

## **Global Information Assurance Certification Paper**

## Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering "Hacker Tools, Techniques, and Incident Handling (Security 504)" at http://www.giac.org/registration/gcih

### Hunting through Log Data with Excel

#### GIAC GCIH Gold Certification

Author: Greg Lalla, greg.lalla@mail.com Advisor: Christopher Walker, CISSP, GWEB, GCED, CCISO, GCUX, GCWN, GSEC Accepted: March 25, 2017

Abstract

Gathering and analyzing data during an incident can be a long and tedious process. The vast amounts of data involved in even a single system intrusion can be overwhelming. Larger and well-funded incident response teams typically have a Security Information and Event Management (SIEM) product at their disposal to help the responder sift through this data to find artifacts relevant to the intrusion. This paper will demonstrate to the reader how to use Microsoft Excel and some of its more advanced features during an intrusion if a SIEM or similar product is not available to the incident responder.

### 1. Introduction

This document will show you how to use Microsoft Excel to search through dissimilar data to find significant artifacts needed to respond to an intrusion. It may not be ideal to import thousands of log entries into Excel and root through them for a few nuggets that might give you insight into the adversary's exploitation of a network. However, if a SIEM product is not running in the enterprise, with a little knowledge and a small amount of coding, you can use Excel as a suitable substitute. There will still be a manual effort involved as there is no magic button that will produce all the artifacts that you wish to find, but the process described here will make it easier and more intuitive to filter out all the unwanted data.

When examining logs, you will look for indicators of compromise (IOCs) that can point you in the direction of other compromised systems. The examination of logs is not a deep dive forensic type of analysis. During an incident, there is not enough time to look at every log entry from every system. The method shown below will help find the obvious artifacts and identify the next system to examine.

This guide will contain up to three methods for each example presented. First, the paper will show some of the things you can do with Excel by just using the toolbar commands. Second, if available, an Excel Function will be created to show how it can be slightly automated. Third, to enhance the Excel Function process even further, Visual Basic for Applications (VBA) code will be provided. Knowing alternate ways of manipulating different types of data will allow you to incorporate the results into the standard output described below.

To prevent this paper from being overly long and difficult to search through, the VBA code will be made available on the GitHub website to make it easier to replicate. The GitHub URL is https://github.com/gregory-lalla/GCIH\_Gold/.

### 2. Requirements

### 2.1. Excel Version

The Excel Functions and VBA code in this paper were written and executed using Microsoft Excel 2010. Other versions of Microsoft Excel based on the Office Open XML (OOXML) specification (Excel 2007 and later) should have most of the same functionality. There are exceptions, such as "Making a Macro that changes the cell colors and making changes to other aspects of cells may not be backward compatible" ("Microsoft Excel", 2016). Also, the location of some options may be in different menus or locations within a menu.

### 2.2. Developer Toolbar

To use the techniques described in this document, you will need to have the Developer Toolbar added to the Ribbon. For instructions on how to enable the Developer Toolbar, visit https://msdn.microsoft.com/en-us/library/bb608625.aspx/.

### 3. Organizational Concepts

Formatting, filtering, and organization are the core techniques in this paper for finding relevant information needed to respond to an incident. The following are suggestions on how to get Excel to display the data in a way that is easy to analyze. We will use these techniques when looking at each of the different types of logs discussed later in this paper.

### 3.1. System Time

First, depending on the geographic location of your systems, the time zone settings may need to be adjusted. If the location of all the systems is in the same time zone, then you may want to perform all your data correlation in the local time zone. If your systems span time zones, it is best to do all the analysis using the Coordinated Universal Time (UTC) time zone. Using UTC, all the data will line up chronologically. To make the process easier, the system time should be changed to UTC so that applications that use the computer's time to display the timestamp will automatically produce the correct time format.

Another setting to change is the Date and Time format of your analysis computer. Excel uses the Date/Time format of the system when it displays the information in the formula bar. To keep things consistent throughout the investigation and within reporting, have the Date/Time in the 'mm/dd/yyyy hh:mm:ss' format (without the quotes). This setting makes all the date and time values 19 characters long. To make this change, follow these instructions: https://support.office.com/en-us/article/Change-the-Windows-regional-settings-to-modify-the-appearance-of-some-data-types-edf41006-f6e2-4360-bc1b-30e9e8a54989/.

Finally, the dates and times in the Excel spreadsheets need to be formatted to display the same 'mm/dd/yyyy hh:mm:ss' format. In the below example, you change the Date/Time format by selecting Column A which contains the date and time values, then right clicking the column and selecting 'Format Cells...'. This process should bring up a new window titled 'Format Cells' with the 'Number' tab already selected. Under 'Category,' click 'Custom.' In dialogue box labeled 'Type:' enter mm/dd/yyyy hh:mm:ss (Figure 1).

| 금 っ ~ ~  | System Shim vlsm - Microsoft Evcel   | _ 🗆 🗡             |
|--|--|-------------------|
| File Home Insert Page                            | Format Cells   | a 🕜 🗖 🖾           |
| Calibri - 11                                     | Number         Alignment         Font         Border         Fill         Protection           Category:         Category: | Σ                 |
| Paste <b>B</b> <i>I</i> <u>U</u> ·               | General<br>Number Last Modified Date Format  | Filter * Select * |
| Clipboard G Font                                 | Currency<br>Accounting Type:   | Editing           |
| AI ·   | Date middloony bhympisd  | *                 |
| A B  | Percentage General   |                   |
| 1 Last Modified ▼ Last Up                        | Fraction 0<br>Scientific 0.00  |                   |
| 2 03/15/2012 07:01 N/A<br>3 03/13/2012 06:44 N/A | Text #,##0   |                   |
| 4 03/10/2012 18:00 N/A                           | Special         #,##0.00           Custom         #,##0);(#,##0)         26-D0595EFD80E4}\chron  | ma undator ava    |
| 5 03/08/2012 21:44 N/A                           | #,##0_);[Red](#,##0)   | ne_upuater.exe    |
| 6 03/08/2012 21:44 N/A                           | #,##0.00_);[Red[(#,##0.00)   |                   |
| 7 03/08/2012 17:20 N/A                           | \$#,##0_);(\$#,##0)<br>\$#,##0_);[Red](\$#,##0)  | ome_updater.exe   |
| 8 03/08/2012 14:28 N//Cus                        | stom Category ~  |                   |
| 9 03/07/2012 19:43 N/A                           | .6-delta.exe   |                   |
| 10 03/07/2012 06:17 N/A                          | Type the number format code, using one of the existing codes as a starting point.  |                   |
| 11 03/07/2012 00:44 N/A                          | r\setup.exe هاد الم  |                   |
| 12 03/07/2012 00:44 N/A                          |  |                   |
| 13 03/06/2012 17:30 N/A                          |  | me_updater.exe    |
| 14 03/06/2012 11:49 N/A                          | OK Cancel  | -                 |
| 🖪 💶 🕨 System_Shim                                |  |                   |
| Ready 🛅  | Average: 40546.95748 Count: 408 Sum: 16502611.69 🧮 🔲 🛄 100% 🤇  | ∍€_,,             |

Figure 1. Date Format (Lee, 2014, digital case files)

### 3.2. Consistent Results

Other columns displaying data should also have a uniform appearance, which makes it easier to spot trends, inconsistencies, patterns, etc. In this paper, the following column headers will be used across all spreadsheets to achieve that consistent look:

- Column A Header Name = Date/Time
- Column B Header Name = Account
- Column C Header Name = Computer
- Column D Header Name = Description
- Column E Header Name = Details
- Column F Header Name = Properties
- Column G Header Name = Miscellaneous
- Column H Header Name = Artifact

Note that it is acceptable to have empty columns to the spreadsheet if there is not enough data to fill all the suggested columns.

### 3.3. Formatting

To easily read the data, you will freeze the top row and apply a bold font to it; enable filters on the columns; set the column widths to 'Autofit'; and 'left justify' the entire spreadsheet. Reduce the data where possible and sort it by the Date/Time column from oldest to newest. Please see the GitHub page which has an Excel template of the standard format named 'Standard\_Format.xltm' (https://github.com/gregorylalla/GCIH\_Gold/blob/master/Docs/Template/Standard\_Format.xltm).

### 3.4. Keywords, Named Cells, and Filters

One of the common themes repeated in this paper is data reduction. Excel can handle a lot of data, but there is a cost in the time it takes to manipulate and analyze that data. Each log file examined will have unique entries which the responder must understand to reduce the data without losing critical items relevant to the incident.

One method of data reduction is the use of keywords. A list of keywords will be used to help pinpoint known or suspicious activity related to the intrusion. There should be two types of keyword lists maintained. One master list of all the terms discovered during the throughout the investigation and an event list for each type of log analyzed. Tailor the event keyword lists to the log files you are inspecting to minimize the output of the filtered data.

When reducing data, one issue faced is the location of the data you want to keep changes as rows and columns get adjusted. This shifting of data needs to be kept in mind when working with 'Named Cells' (Blue arrow in Figure 2) as the properties assigned to

the cell stay with that cell, even if the data in the cell moves to a new location. Therefore, reduce and adjust all the data before using 'Named Cells.' If the data in a 'Named Cell' will change, a good way to keep track of that data is to use 'Fill Colors.' When a keyword search gets a match, highlight the cell or entire row with a particular color. Using filters, you can locate the 'colored' data with a few clicks of the mouse.

To manually work with keywords, the basic search feature can be used to find each instance of the keyword. Enter a unique identifier in the cell 'Name Box' (Blue arrow in Figure 2) when a keyword is found in a cell. The unique identifier name has the following rules: "The first character of a name must be a letter, an underscore character (\_), or a backslash (\). Remaining characters in the name can be letters, numbers, periods, and underscore characters" ("Define and use names in formulas – Excel", 2017).

| S 🖬 🥱 - C - 🗎 -                     |  | System Shim.xlsm - Microsoft Excel   |                                       | -  |         |
|-------------------------------------|--|--|---------------------------------------|--|---------|
|                                     | e Layout Formulas Data Review  | /iew Developer Team  |                                       | ۵  | ) - # X |
| Paste<br>Clipboard ⊂<br>Clipboard ⊂ | $\begin{array}{c} \mathbf{I} \mathbf{I} \\ \mathbf{I}$ | Image: Second | Cell<br>Insert Delete Format<br>Cells | Σ AutoSum *<br>Fill *<br>Clear * Sort & Find<br>Filter * Sole<br>Editing | 81      |
| Svchost_Evil_1 🚤 👻 🕤                |  | /chost.exe   |                                       | -  |         |
| A                                   | B C D  | E  | F                                     | G H  | H 🖌     |
| 1 Date/Time                         | count 👻 Computer 🝸 Description   | 💌 Details  | <ul> <li>Properties</li> </ul>        | Miscellaneous 💌 Artifa   | ct ·    |
| 234 07/14/2009 015 0:51             | Cell E241  | C:\Windows\system32\wermgr.exe   | TRUE                                  |  |         |
| 235 07/14/2009 01:39:49             | The Part of State of State of State of State   | C:\Windows\System32\vdsldr.exe   | TRUE                                  |  |         |
| 236 07/14/2009 01:39:48             | named  | C:\Windows\system32\TSTheme.exe  | TRUE                                  |  |         |
| 237 07/14/2009 01:39:48             | Svchost_Evil_1   | C:\Windows\system32\unlodctr.exe   | TRUE                                  |  |         |
| 238 07/14/2009 01:39:48             |  | C:\Windows\System32\unregmp2.exe   | TRUE                                  |  |         |
| 239 07/14/2009 01:39:47             |  | C:\Windows\system32\systempropertiesprotection.exe   | TRUE                                  |  |         |
| 240 07/14/2009 01:39:46             | Cell   | C:\Windows\system32\StikyNot.exe   | FALSE                                 |  |         |
| 241 07/14/2009 01:39:46             |  | C:\Windows\System32\svchost.exe  | TRUE                                  |  |         |
| 242 07/14/2009 01:39:42             | E241   | C:\Windows\system32\SoundRecorder.exe  | FALSE                                 |  |         |
| 243 07/14/2009 01:39:41             |  | C:\Windows\system32\SnippingTool.exe   | FALSE                                 |  |         |
| 244 07/14/2009 01:39:40             |  | C:\Windows\system32\shutdown.exe   | TRUE                                  |  |         |
| 245 07/14/2009 01:39:37             |  | C:\Windows\System32\sdiagnhost.exe   | TRUE                                  |  |         |
| 246 07/14/2009 01:39:37             |  | C:\Windows\system32\services.exe   | TRUE                                  |  |         |
| 247 07/14/2009 01:39:35             |  | C:\Windows\system32\sc.exe   | TRUE                                  |  |         |
| K + P H System_Shim 🥂               | J/   |  |                                       |  | •       |
| Ready                               |  |  |                                       | 100% 🕞 👘 🖯   | •       |

Figure 2. Named Cell. (Lee, 2014, digital case files)

After naming the cell, fill the entire row that contains the keyword with a color (Figure 3). For each unique keyword found you can continue to use the same color or change them to different colors distinctively associated with each keyword. Using the fill colors is helpful when using the filter tool, which will be discussed and demonstrated further into the paper.

| <b>a</b> • • • <b>a</b> • |                        |                  |            |        | System_Shim        | .xlsm - Microsoft  | Excel   |                                |               | _ □                        | ×   |
|---------------------------|------------------------|------------------|------------|--------|--------------------|--------------------|---|--------------------------------|---------------|----------------------------|-----|
| File Home Insert          | Page Layout For        | nulas Data       | Review 1   | View   | Developer Team     |                    |   |                                |               | a 🕜 🗆                      | - B |
| Cali                      | ibri + 11              | - A* A* =        | = =        | », -   | Wrap Text          | Custom ~           | k 📝 📝   | i 🏹 📑                          | Σ AutoSum * A |                            |     |
|                           | I <u>U</u> - <u></u> - | 🌺 - <u>A</u> - 🔳 |            | (F (F  | 👬 Merge & Center * | \$ - % • .38 .38   | Conditional Format Cell<br>Formatting * as Table * Styles * | Insert Delete Form             |               | t& Find &<br>er * Select * |     |
| Clipboard 🕓               | Font                   |                  |            | Alignm | ent 🔍              | Number 5           | Styles  | Cells                          | Editing       |                            |     |
| A241 -                    | <i>f</i> = 07          | / 4/2009 01      | :39:46     |        |                    |                    |   |                                |               |                            |     |
| A                         | В                      | С                | D          |        |                    | E                  |   | F                              | G             | н                          |     |
| Date/Time                 | Account - Co           | mputer 🝸 D       | escription | ▼ De   | tails              |                    |   | <ul> <li>Properties</li> </ul> | Miscellaneous | Artifact                   | Ŧ   |
| 4 07/14/2009 01:39:51     |                        |                  |            | C:)    | \Windows\system3   | 2\wermgr.exe       |   | TRUE                           |               |                            |     |
| 5 07/14/2009 01:39:49     |                        |                  |            | C:)    | Windows\System3    | 2\vdsldr.exe       |   | TRUE                           |               |                            |     |
| 6 07/14/2009 01:39:48     | Select*                | Fill Color       | 2          | C:)    | \Windows\system3   | 2\TSTheme.exe      |   | TRUE                           |               |                            |     |
| 7 07/14/2009 01:39:48     | ( ) and ( )            | con              |            | C:)    | \Windows\system3   | 2\unlodctr.exe     |   | TRUE                           |               |                            |     |
| 8 07/14/2009 01:39:48     | 1                      |                  |            | C:     | Windows\System3    | 2\unregmp2.exe     |   | TRUE                           |               |                            |     |
| 9 07/14/2009 01:39:47     |                        | 2                |            | C:     | Windows\system3    | 2\systemproperties | protection.exe  | TRUE                           |               |                            |     |
| 0 07/14/2009 01:39:46     |                        | -                |            | C:     | Windows\system3    | 2\StikyNot.exe     |   | FALSE                          |               |                            |     |
| 1 07/14/2009 01:39:46     |                        |                  |            | C:)    | \Windows\System3   | 32\svchost.exe     |   | TRUE                           |               |                            |     |
| 2 0./ +. /2009 01:39:42   |                        |                  |            | C:     | \Windows\system3   | 2\SoundRecorder.e  | xe  | FALSE                          |               |                            |     |
| 3 07/14/2009 01.29:41     |                        |                  |            | C:     | Windows\system3    | 2\SnippingTool.exe |   | FALSE                          |               |                            |     |
| 4 07/14/2009 01:39:40     |                        |                  |            | C:     | Windows\system3    | 2\shutdown.exe     |   | TRUE                           |               |                            |     |
| 5 07/14/2009 01:39:37     | Sel                    | ect Entire       |            | C:     | Windows\System3    | 2\sdiagnhost.exe   |   | TRUE                           |               |                            |     |
| 6 07/14/2009 01:39:37     |                        | Row              |            | C:     | Windows\system3    | 2\services.exe     |   | TRUE                           |               |                            |     |
| 7 07/14/2009 01:39:35     |                        |                  |            | C:)    | \Windows\system3   | 2\sc.exe           |   | TRUE                           |               |                            |     |
| ↓ ► ► System Shim         | <u>/</u>               |                  |            | - 1    |                    |                    | 14  |                                |               | _                          |     |

Figure 3. Fill Color. (Lee, 2014, digital case files)

Click 'Find Next' in the 'Find and Replace' window to find the next instance of the keyword. Once found, give that cell a similar, but unique name to distinguish it from the first keyword found and give it a 'Fill Color.' As an example, the first unique cell Name would be 'Svchost\_Evil\_1' and the second would be 'Svchost\_Evil\_2' for hits found on keyword 'svchost.exe.' After all the keywords are searched and found in this manner, you can navigate to those cells by clicking the dropdown arrow in the cell 'Name Box' and selecting one of the entries (Figure 4). You can also manage the 'Named Cells' and see their location by going to the 'Formulas' ribbon tab and selecting the 'Name Manager' icon (Figure 5).

| 🖾 🤊 - e - 🗋 🖃            |                             |                                     |                    | System_Sh   | im.xlsm - Microsoft    | Excel   |                                |               | _ 🗆       | ×     |
|--------------------------|-----------------------------|-------------------------------------|--------------------|---|------------------------|---|--------------------------------|---------------|-----------|-------|
| File Home Insert         | Page Layout                 | Formulas Data                       | Review             | View Developer Team   |                        |   |                                |               | a 🕜 c     | - 🗗 🛛 |
| Copy -                   | libri -                     | 11 • A A<br>• <u>A</u> • <u>A</u> • | = = <mark>_</mark> | <ul> <li>♥・・ 営<sup>4</sup>Wrap Text</li> <li>電信 Merge &amp; Center</li> </ul> | General ~              | Conditional Format Cell<br>Formatting * as Table * Styles * | Insert Delete Form             |               | t& Find & |       |
| Clipboard 🕓              | Font                        | T                                   |                    | Alignment   | Number Fill            | Styles  | Cells                          | Editing       |           |       |
| Cleanup_Evil_1           | f <sub>⊻</sub>              | C:\Windows\                         | TEMP\mfe           | ABB5.tmp\cleanup.exe  |                        |   |                                |               |           | *     |
| Cleanup_Evil_1           | В                           | C                                   | D                  |   | E                      |   | F                              | G             | Н         |       |
| Cleanup_Evil_2           | Arcount 👻                   | Computer 🝸                          | Descriptio         | n 🔻 Details   |                        |   | <ul> <li>Properties</li> </ul> | Miscellaneous | Artifact  | *     |
| MRT_Evil_1               | 3                           |                                     |                    | c:\66da7d133db3   | ac3bca7b4fdc55fbf\mr   | tstub.exe   | TRUE                           |               |           | -     |
| MRT_Evil_2               |                             |                                     |                    | c:\95deb80f1a02a  | d2a6ffcb5b70420\Setu   | p.exe   | TRUE                           |               |           |       |
| MRT_Evil_3               | 8                           |                                     |                    | C:\Program Files (:   | (86)\Jetico\BCWipe\bc  | updt.exe  | TRUE                           |               |           |       |
| MRT_Evil_4<br>MRT_Evil_5 | · \                         |                                     |                    | C:\Windows\syste  | m32\MRT.exe            |   | TRUE                           |               |           |       |
| MRT_EVIL5                | ,                           |                                     |                    | C:\Program Files (  | (86)\Jetico\Shared64\B | CShExt.dll  | FALSE                          |               |           |       |
| MRT_EVIL_0               | Dropdo                      | wn to Sele                          | ect                | C:\Users\nfury\Ap   | pData\Local\Temp\CR    | FC5A4.tmp\setup.exe   | TRUE                           |               |           |       |
| MRT_Evil_8               | International International | ned Cell                            |                    | c:\4d9c2772a8479  | fd3574a482ba06b\mrt    | stub.exe  | TRUE                           |               |           |       |
| Skype_Evil_1             | )                           |                                     |                    | C:\Users\nfury\Ap   | pData\Local\Temp\CR    | 3C462.tmp\setup.exe   | TRUE                           |               |           |       |
| Svchost_Evil_1           | L                           |                                     |                    | C:\Program Files\0  | ommon Files\System\    | wab32.dll   | FALSE                          |               |           |       |
| 33 09/29/2011 08:23:32   | 2                           |                                     |                    | C:\Program Files ()   | (86)\Jetico\BCWipe\BC  | Wipe.exe  | TRUE                           |               |           |       |
| 34 09/28/2011 07:02:49   | )                           |                                     |                    | C:\Windows\syste  | m32\MRT.exe            |   | TRUE                           |               |           |       |
| 35 09/21/2011 01:24:09   | )                           |                                     |                    |   |                        | 59C55.tmp\setup.exe   | TRUE                           |               |           |       |
| 36 09/17/2011 22:24:30   | )                           |                                     |                    |   |                        | 7C704.tmp\setup.exe   | TRUE                           |               |           |       |
| 37 09/17/2011 00:22:58   |                             |                                     |                    |   | http://www.cleanu      |   | TRUE                           |               |           |       |
| R + P System_Shir        | n /1                        |                                     |                    |   |                        |   |                                |               |           |       |
| Ready                    |                             |                                     |                    |   |                        |   |                                | 回 円 100% (一)  |           | - ÷ . |

Figure 4. Selecting Named Cells. (Lee, 2014, digital case files)

| S 🔂 🤊 • (* - 🗋 💂                                   | System_S                       | 5him.xlsm - Microsoft Excel   | _ 🗆                  |
|--|--------------------------------|---|----------------------|
| File Home Insert Page Layout Formulas              | Data Review View Developer Tea | Name Manager  | ? × ? - :            |
| fx Σ 👔 🏚 👔 🄶                                       |                                | New Edit Delete Named Cell Locat  | ions <sub>er</sub> . |
| Insert AutoSum Recently Financial Logical 11t Date | 8. Lookup & Math 8. More Name  | Name         Value         Neters to           Cloamup_Evil_1_C:\Windows\TEMP/mfeADD5.tmp\deamup.exe         -System_Shiml\$E\$37   | Scope<br>Workbook    |
| Function Lorary                                    |                                | Ceanup Evil 2 C:\Windows\TEMP\mfeD15C.tmp\cleanup.exe =System Shimi\$E\$39  | Workbook             |
| Cleanup_Evil_1 • fr fr C:\Windo                    | ows\TEMP\mfeABB5.tmp\cleanup.e | MRT_Evil_1 C:\Windows\system32\MRT.exe =System_Shiml\$E\$2  | Workbook             |
| A B C  | D                              | MRT_Evil_2 C:\Windows\system32\MRT.exe =System_Shim!\$E\$8  | Workbook             |
| 1 Date/Time · Account Compute                      | er • Description • Letails     | MRT_Evil_3 C:\Windows\system32\MRT.exe =System_Shim!\$E\$11     System_Shim!\$E\$11   | Workbook<br>Workbook |
| 4 10/28/2011 04:04:58                              | c:\66da7d133db                 | Image: The second sec | Workbook Workbook    |
| 5 10/26/2011 19:41:40                              | c:\95deb80f1a0                 | MRT_Evil_6 C:\Windows\system32\MRT.exe -system_Shiml\$E\$25   | Workbook             |
| 6 10/12/2011 08:05:48                              | C:\Program Files               |   | Workbook             |
| 7 10/12/2011 07:07:07                              | C:\Windows\sys                 | MRT_Evil_8 C:\Windows\system32\MRT.exe -System_Shiml\$E\$65   | Workbook             |
| 8 10/12/2011 04:49:07                              | C:\Program Files               | Skype_Evil_1 C:\Program Files (x86)\Skype\Phone\Skype.exe =System_Shiml\$E\$80  | Workbook             |
| 9 10/07/2011 22:29:30                              | C:\Users\nfury\                | Svchost_Evil_1 C:\Windows\System32\svchost.exe =System_Shimt\$E\$241  | Workbook             |
| 0 10/05/2011 14:42:32 Formulas                     | Name c:\4d9c2772a84            |   |                      |
| 11 10/01/2011 21:29:40 Tob                         | Manager C:\Users\nfury\        |   |                      |
| 12 10/01/2011 05:45:21                             | C:\Program Files               | <   | >                    |
| 3 09/29/2011 08:23:32                              | C:\Program Files               | Befers to:  |                      |
| 4 09/28/2011 07:02:49                              | C:\Windows\sys                 | X V -System_Shim!\$E\$37  | <b>1</b>             |
| 35 09/21/2011 01:24:09                             | C:\Users\nfury\                |   |                      |
| 36 09/17/2011 22:24:30                             | C:\Users\nfury\                |   | Close                |
| 09/17/2011 00:22:58                                | C:\Windows\TE                  | un funeurovanik felesiteksze tutor  |                      |
| ( + > > System Shim                                | a house house                  |   |                      |
| Ready 🛅  |                                | III 10  | 0% 🕞 👘 🗌             |

Figure 5. Name Manager. (Lee, 2014, digital case files)

Using 'Named Cells' is a quick way to locate known artifacts. It is also an excellent way to find more keywords by examining the data around those cells.

Filters are another technique to find data and visually reduced the data to only show those cells that the analyst wishes to view. These are particularly helpful when you know you'll have many hits on your keywords and would like to see them without the clutter of all the other rows not associated with those keywords. There are two ways to use the filters. There is a basic filter where you can have up to two items filtered per column using AND OR operators. To filter on more than two items, there are Advanced Filters which can be used to search for data with more complex options.

We enabled basic filters already in an earlier example. To access them, on the column we are looking to search, click on the dropdown arrow in the header cell. Select the 'Text Filters' option and then choose one of the filter selections (See Figure 6).

| 🖥 🔊 · 🕐 🗋 🚽   |                                |               |               | Sys           | stem_Shim.xlsm - N  |  |                         |                   |                 |         |
|---|--------------------------------|---------------|---------------|---------------|---------------------|--|-------------------------|-------------------|-----------------|---------|
| File Home Insert                                    | Page Layout                    | Formulas Data | Review Vie    | w Develope    | r Team              | Basic Filters                                  | Enabled                 |                   |                 | a 🕜 🗆 🕯 |
| From From From Ot     Sources     Get External Date | <ul> <li>Connection</li> </ul> | Refresh Pr    | it Links      | Sort & Filter | Manced Columns E    | Remove Data Consolie<br>uplicates Validation * | a What-If<br>Analysis • | IP Ungroup Subtor | Hide Detail     |         |
| A2 -  |                                | 03/15/2012 (  | 010           | Sont Germ     | itter               | 0000 10033                                     |                         | Guune             |                 |         |
| A   | B                              | с             | D             |               |                     | E  |                         | F                 | G               | Н       |
|   |                                | Computer -    | Description - | Details       |                     | -  |                         | Properties *      | Miscellaneous ~ |         |
| 03/15/2012 07:01:20                                 |                                |               |               | C:\Windo      | ws\system32\MRT 2   | Sort A to Z                                    |                         | TUE               |                 | -       |
| 03/13/2012 06:44:10                                 |                                |               |               |               | nfury\AppData\Loc 7 |  |                         | TRUE              | <b>T</b>        |         |
| 03/08/2012 21:44:04                                 |                                |               |               | C:\Users\r    | nfury\AppData\Loc   | Sort by Color                                  |                         | TRUE              |                 |         |
| 03/07/2012 00:44:08                                 |                                |               |               | C:\Users\r    | nfury\AppData\Loc   |  |                         | TRUE              |                 |         |
| 03/05/2012 18:46:04                                 |                                |               |               | C:\Users\r    | nfury\AppData\Loc   | Clear Filter From "Details"                    |                         | TRUE              |                 |         |
| 03/04/2012 21:14:18                                 |                                |               |               | c:\25dfc16    | 07c2h41732c15f75    | Filter by Color                                |                         | TRUE              |                 |         |
| 02/15/2012 08:02:13                                 |                                |               |               | C:\W          | Equals              | Text <u>Filters</u>                            |                         | TRUE              | \\//            |         |
| 01/27/2012 05:36:04                                 |                                |               |               | c:\b7         | Does Not Equal      | Search   | م                       | TRUE              | Filter          |         |
| 01/25/2012 06:33:30                                 |                                |               |               | C:\W          | Begins With         | (Select All)                                   |                         | TRU               | Dropdown        |         |
| 01/11/2012 08:08:32                                 |                                |               |               | C:\W          | Ends With           | C:\0b6f6f1e57a76e0c                            |                         | TRUE              | Diopuowii       |         |
| 01/04/2012 23:01:58                                 |                                |               |               | c:\0e         | Contains            | ✓ c:\0e4be682c737e4e ✓ c:\253b615(2dd9d77)     |                         | TRUE              |                 |         |
| 01/04/2012 10:44:20                                 |                                |               |               | C:\W          |                     | ✓ c:\25dfc1607c2b4173                          |                         | FALSE             |                 |         |
| 01/04/2012 08:58:41                                 |                                |               |               | C:\W          | Does Not Contain    | ✓ c:\3476acac3c159a03                          | e5318a0255\Sett         | FALSE T           | ext Filters     |         |
| 12/29/2011 08:06:20                                 | Custom                         | Filters =     |               |               | Custom Eilter       | ✓ c:\/labecc7af24d996d                         | 7070a1\MpMiniSi 🗸       | TRUE              |                 |         |
| 12/26/2011 08:51:18                                 |                                |               |               |               | ac3c159a03e5318a    | <  | >                       | TRUE              |                 |         |
| ↔ → System_Shim                                     | <u>@</u> ]/                    |               |               | a)            | 1                   |  | Consul                  | -                 |                 |         |
| dy 🔚  |                                |               |               |               |                     | OK   | Cancel                  |                   | E 🛄 100% 🕞 —    | 0       |

Figure 6. Filter Dropdown Menu. (Lee, 2014, digital case files)

When the filter window comes up, enter the word(s) you want to locate (or exclude) in the dialogue box. The filter will display only the rows that have (or don't have) the words in the column.

You can also search on the 'Fill Colors' used during the keyword search to filter only on those colors you wish to see (Figure 7).

| 🖬 🤊 🦿 🛄 –             |             |              |               | System_Shim               | .xlsm - M | icrosoft          | Excel                                |                  |              |                                       | _ □        | ×   |
|-----------------------|-------------|--------------|---------------|---------------------------|-----------|-------------------|--------------------------------------|------------------|--------------|---------------------------------------|------------|-----|
| File Home Insert      | Page Layout | Formulas Dat | a Review View | Developer Team            |           |                   |                                      |                  |              |                                       | a 🕜 🗆      | B   |
| Cali                  | bri -       | 11 - A A     | = = _ »·      | Wrap Text                 | General   | ÷.0               | Conditional For                      | mat Cell Inse    |              | Σ AutoSum *<br>Fill *<br>Clear * Sort | Find &     |     |
| Clipboard             | Font        |              |               | nment S                   | Numbe     | 100 100           | Formatting * as Ta<br>Style          | · · ·            | Cells        | Editing                               | * Select * |     |
| E28 - (               |             | C:\Program I |               | \Shared64\BCShExt.d       |           |                   |                                      | -                |              | Loning                                |            | _   |
| A                     | В           | C            | D             |                           |           | E                 |                                      |                  | F            | G                                     | н          |     |
| Date/Time -           | Account -   | Computer -   | Description - | Details                   |           |                   |                                      | -                | Properties - | Miscellaneous -                       | Artifact   | -   |
| 06/06/2011 17:55:30   |             |              |               | C:\Program Files (x86     | )∖Adob 2↓ | Sort A to 2       |                                      |                  | FALSE        |                                       |            |     |
| 06/06/2011 17:55:28   |             |              |               | C:\Program Files (x86     | Comn Z    | Sprt Z to A       |                                      |                  | TRUE         |                                       |            |     |
| 05/25/2011 00:14:10   |             |              |               | C:\Windows\system3        | 2\MpSi    | Sort by Co        | lor                                  |                  | TRUE         |                                       |            |     |
| 05/24/2011 23:14:10   |             |              |               | c:\253b615f2dd9d773       | 31b3835   |                   |                                      |                  | TRUE         |                                       |            |     |
| 05/24/2011 23:14:10   |             |              |               | c:\4aberr7-f74deed        | 7070-1    |                   | From "Details"                       |                  | TRUE         |                                       |            |     |
| 2 05/19/2011 20:05:00 |             |              |               | C:\PROC Filter by Cell Co | lor       | Filter by C       | olor                                 | •                | UE           |                                       |            |     |
| 05/19/2011 20:05:00   |             |              |               | C:\Prog                   |           | Text Eilters      |                                      | •                | TRUL         |                                       |            |     |
| 05/19/2011 20:05:00   |             | -            |               | C:\Prog                   |           | Search            |                                      | Q                | TRUE         |                                       |            |     |
| 05/19/2011 20:05:00   |             | Color of     |               | C:\Prog                   |           | - (m.)            |                                      | ~                | TRUE         |                                       |            |     |
| 05/19/2011 20:05:00   | Rows        | to Filter    |               | CATTOR                    |           | ✓ (Sele<br>✓ C:V0 | scr All)<br>661611e57a76e0cd         | c1b45d0\Selun    | TRUE         | (Citizen la                           |            |     |
| 05/17/2011 12:41:46   |             | ອn           |               | al 00700                  |           |                   | e4be682c737e4ecc                     |                  | TRUE         | Filter b                              | y          |     |
| 05/12/2011 16:50:46   |             |              |               | C:\Wind                   | _         |                   | 53b615f2dd9d773                      |                  | TRUE         | Color                                 |            |     |
| 05/12/2011 15:48:20   |             |              |               | C:\Programmes (Abo        |           |                   | 5dFc1607c2b41732<br>476acac3c159a03e |                  | TRUE         |                                       |            |     |
| 0 05/12/2011 15:48:12 |             |              |               | C:\Program Files (x86     |           |                   |                                      | 070a1\MpMiniSi V | FALSE        |                                       |            |     |
| 1 05/04/2011 05:22:25 |             |              |               | C:\Windows\System3        |           | <                 |                                      | >                | FALSE        |                                       |            |     |
| 05/04/2011 05-10-20   |             |              |               | C.) Mindows (5950000      |           |                   |                                      |                  | TOUL         |                                       |            |     |
| ↔ H System_Shim       | /21/        |              |               |                           |           |                   | OK                                   | Cancel           |              |                                       |            |     |
| ady 🛅                 |             |              |               |                           |           |                   |                                      |                  | E (          | 🗉 🛄 100% 🕞 —                          | 0          | - 6 |

Figure 7. Search on Fill Color. (Lee, 2014, digital case files)

The advanced filters allow you to search for more than two keywords in a column. You enter the keywords into unused cells in the spreadsheet. The first cell is the column header name of the column to search. The cells underneath are the search terms.

Words listed vertically use the OR operator and those listed horizontally use the AND operator. Figure 8 shows an example of an advanced filter, where you are searching the 'Details' column for five keywords. Surrounding the keyword with asterisks finds cells that CONTAIN the word. For details on filters, see https://support.office.com/en-us/article/Filter-by-using-advanced-criteria-4c9222fe-8529-4cd7-a898-3f16abdff32b/.

| 8 8   | 🔊 • (?) - 🗋 📮           | System_Shim.xlsm -  | Microsoft Excel                |                                   |                      | <b>_</b> 🗆 ×  |
|-------|-------------------------|---|--------------------------------|-----------------------------------|----------------------|---------------|
| File  | Home Insert Page La     | yout Formulas Data Review View Developer Team   |                                |                                   |                      | ۵ 🚱 🗖 🚱 ۵     |
| From  |                         | Existing<br>Refresh Properties<br>Refresh → © 2 till Links<br>Refresh → © 2 | Remove Data C                  | Consolidate What-If<br>Analysis - | Ungroup Subtotal     | Hide Detail   |
|       | Get External Data       | Connections State filter  | Data Tools                     |                                   | Outline              | a 🦯           |
|       | J2 🔫 (*                 | ∫∗ Details  |                                |                                   |                      |               |
|       | C D                     | E   | F                              | G                                 | н                    | J K L         |
| 1 C   | omputer 👻 Description 🕚 | Details   | <ul> <li>Properties</li> </ul> | Miscellaneous Y Ar                | tifact 👻             |               |
| 2     |                         | C:\Wind_ws\system32\MRT.exe   | TRUE                           |                                   |                      | Details       |
| 3     |                         | Osers\nfury\AppData\Local\Temp\CR_716FC.tmp\setup.exe   | TRUE                           |                                   |                      | *svchost.exe* |
| 4     |                         | C:\Users\nfury\AppData\Local\Temp\CR_F4244.tmp\setup.exe  | TRUE                           | Advanced Filter                   | ? ×                  | *cleanup.exe* |
| 5     |                         | C:\Users\nfury\AppData\Local\Temp\CR_DE279.tmp\setup.exe  | e TRUE                         | Action                            |                      | *skype.exe*   |
| 6     | Advanced                | C:\Users\nfury\AppData\Local\Temp\CR_1F252.tmp\setup.exe  | TRUE                           | Filter the list. In-place         |                      | *mrt.exe*     |
| 7     | Filter                  | c:\25dfc1607c2b41732c15f75adaf0\mrtstub.exe   | TRUE                           | Copy to another locate            |                      | *setup.exe*   |
| 8     |                         | C:\Windows\system32\MRT.exe   | TRUE                           |                                   |                      |               |
| 9     |                         | c:\b75140d8ef4a4e1bd9439a5ae2d6e3d1\mrtstub.exe   | TRUE                           | List range: \$A\$1:\$H\$2         | 295                  | Range to      |
| LO    |                         | C:\Windows\System32\rdrmemptylst.exe  | TRUE                           | Criteria range: \$1\$2:\$1\$7     | 1                    | Filter        |
| 11    |                         | C:\Windows\system32\MRT.exe   | TRUE                           | Copy to:                          | A COLORED IN COLORED | (Miller)      |
| 12    |                         | c:\0e4be682c737e4eccd01f9435bdc86\mrtstub.exe   | TRUE                           |                                   |                      |               |
| 13    |                         | C:\Windows\System32\ntshrui.dll   | FALSE                          | Unique records only               |                      | Search        |
| 14    |                         | C:\Windows\SysWOW64\ntshrui.dll   | FALSE                          | ОК                                | Cancel               | Criteria      |
| 15    |                         | C:\Program Files (x86)\Jetico\BCWipe\BCWipeTM.exe   | TRUE                           |                                   |                      | Cintena       |
| 16    |                         | c:\3476acac3c159a03e5318a0255\Setup.exe   | TRUE                           |                                   |                      |               |
| 4 4   | 🖂 🕺 System_Shim         |   |                                |                                   |                      | - ·           |
| Point |                         |   |                                | L                                 | Count: 6 FFF E       |               |

#### Figure 8. Advanced Filter. (Lee, 2014, digital case files)

Note the timeframe of the filtered keyword data. When looking at all the log files with tens of thousands of lines of data, this range will be important when deciding what to export for analysis (if given the option). The dropdown menu on the Date/Time column is used to filter by timeframe (Figure 9). Selecting the 'Between...' filter will allow you to capture all the data between two dates narrowing down what data you need to examine.

| Ella    | Home Insert Page                       | Layout Formulas Data Review                     | View De    | System_Si    |          | Microsoft   | Excel   |  |                      |                |                                    | ×  |
|---------|--|---|------------|--------------|----------|-------------|---------|--|----------------------|----------------|------------------------------------|----|
| î î î î | Cut Calibri                            | - 11 - A A = = =                                |            | Wrap Text    | General  |             |         |  | 3- 3× 111            | ∑ AutoSum *    | A7 A                               | B  |
| aste    | In Copy ▼<br>Image: Sormat Painter B I | <u>U</u> •   <u>.</u> • <u>▲</u> • <u>■</u> ≡ ≡ | _          | Merge & Cent | er- \$-9 | 0.0 0.0 •.0 |         | fitional Format Cell<br>atting * as Table * Styles * | Insert Delete Format | 🛃 Fill 🕶       | Sort & Find &<br>Filter * Select * |    |
| (       | Clipboard G                            | Font G  | Alignment  |              | 5 N      | umber 5     |         | Styles   | Cells                | Edit           | ting                               |    |
| N       | MRT_Evil_2 👻 🗧                         | ∫ <sub>x</sub> C:\Windows\system32              | MRT.exe    |              |          |             |         |  |                      |                |                                    |    |
| 4       |  | A   |            | В            | С        | D           |         |  | E                    |                |                                    |    |
| D       | Date/Time                              |   | ¥          | Account -    | Computer | - Descript  | on 👻    | Details  |                      |                |                                    |    |
| 0       | 06/06/2011 17:55:32                    | Sort Oldest to Newest                           |            |              |          | Select      |         | C:\Program Files (x8                                 | 6)\Adobe\Reader      | 10.0\Reader\F  | Reader_sl.exe                      |    |
| 0       | 6/06/2011 17:55:30                     | Sgrt Newest to Oldest                           |            |              |          | Dropdov     | m       | C:\Program Files (x8                                 | 6)\Adobe\Reader      | 10.0\Reader\A  | AcroRd32.exe                       |    |
| 0       | 06/06/2011 17:55:28                    | Sort by Color                                   |            |              |          | Menu o      | and and | C:\Program Files (x8                                 | 6)\Common Files\/    | Adobe\ARM\1    | 1.0\armsvc.exe                     | ,  |
| 0       | 05/25/2011 00:14:10                    | Clear Filter From "Date/Time"                   |            |              |          |             |         | C:\Windows\system                                    | 32\MpSigStub.exe     |                |                                    |    |
| 0       | 5/24/2011 23:14:10                     | 1.  |            |              |          | Date/Tin    | -       | c:\253b615f2dd9d77                                   | /31b383530791e\N     | /IpMiniSigStub | o.exe                              |    |
| 2       |  | Filter by Color                                 |            |              |          | Colum       |         | c:\4abecc7af24d996                                   | d7070a1\MpMiniS      | igStub.exe     |                                    |    |
| 4       | Equals                                 | Date <u>Filters</u>                             | •          |              |          |             |         | C:\PROGRA~2\McAf                                     | ee\COMMON~1\N        | lcScanCheck.e  | exe                                |    |
| ł       | Before                                 | Search (All)                                    | <b>ب</b> و |              |          | -           |         | C:\Program Files (x8                                 | 6)\McAfee\Comm       | on Framework   | k\McTray.exe                       |    |
| ł       | After                                  | (Select All)                                    |            |              |          | Select      |         | C:\Program Files (x8                                 | 6)\McAfee\Comm       | on Framework   | k\msaconfig.ex                     | e  |
|         | Between_                               | · 2012  |            |              |          | Date        |         | C:\Program Files (x8                                 | 6)\McAfee\Comm       | on Framework   | k\naPrdMgr.ex                      | е  |
| 4       |  | 2011  |            |              |          | Filters     |         | C:\Program Files (x8                                 | 6)\McAfee\Comm       | on Framework   | k\udaterui.exe                     |    |
| ł       | Iomorrow                               | 2010<br>2009                                    |            |              |          |             |         | c:\cc7a981a16f7e1d                                   | 482fff3b5d2\Setup    | .exe           |                                    |    |
| ł       | Tgday                                  |   |            |              |          |             |         | C:\Windows\TEMP\                                     | 3.0.0.638.4\setup_   | SAE.exe        |                                    |    |
|         | Yesterday                              |   |            |              |          |             |         | C:\Program Files (x8                                 | 6)\McAfee\SiteAdv    | isor Enterpris | e\McSACore.e                       | xe |
|         | Next Week                              |   |            |              |          |             |         | C:\Program Files (x8                                 | 6)\McAfee\SiteAdv    | isor Enterpris | e\McIEPIg.dll                      |    |
|         | This Week                              |   |            |              |          |             |         | 4  | 22)                  |                |                                    |    |
| d       | Last Week                              | ОК  | Cancel     |              |          |             |         |  | E C                  | 100% 😑         |                                    | _( |
|         |  |   |            |              | -        | _           |         |  |                      |                |                                    |    |
|         | Next Month                             | Filter  | oy I im    | nefram       | •        | States and  |         |  |                      |                |                                    |    |
|         | This Month                             |   |            |              |          |             |         |  |                      |                |                                    |    |

Figure 9. Search by Date/Time. (Lee, 2014, digital case files)

One thing to be aware of when filtering by timeframe is that artifacts may have timestamps that occur outside of the incident timeline. These timestamps can happen when the artifact is showing the file compile time instead of its execution time. Another example would be time-stomping, which is an anti-forensics technique to change the MFT timestamps of a file.

Any new entries found that are related to the intrusion should be 'Named' and 'Filled.' You should then copy off the highlighted rows onto a separate workbook which will contain all the rows of interest from all the logs collected.

### 3.5. Macros

Many of the tasks described above are tedious and repetitive. In such circumstances, it is easier to automate the tasks using VBA macros. You'll be provided with several VBA macros so you do not need to perform the task manually. To use macros, open the exported log file in Excel and then save it as an Excel macro-enabled workbook file with an XLSM file extension. Open the newly created .XLSM file to import the macro into the spreadsheet. Once the spreadsheet is open, you need to launch the VBA Editor window by hitting the Alt-F11 keys. With the VBA window open, select the 'File' dropdown menu and click on 'Import File.' Browse to the .BAS file with the code you are looking to run and select 'Open.' Close the VBA window and head back to

the spreadsheet. Under the 'Developer' tab, select the 'Macros' button, highlight the newly imported macro in the popup window and select 'Run' (See Figure 10).

| X           |           |            |              |                   |           | Syst           | em_Shir                            | m.xlsm - I | Microsoft Ex | cel                           | _ 🗆 🛛           |
|-------------|-----------|------------|--------------|-------------------|-----------|----------------|------------------------------------|------------|--------------|-------------------------------|-----------------|
|             | ile Hom   | e Insert   | Page Layou   | Formulas          | Data F    | keview Vi      | Develo                             | oper Team  |              |                               | ۵ 🕝 🗆 🗗         |
| Vist<br>Bas | al Macros | Macro Secu | e References | Add-Ins CO<br>Add |           | Design<br>Mode | roperties<br>iew Code<br>un Dialog |            |              |                               |                 |
|             | A1        | Code       | -            | Add-Ins           | odified   | Controls       |                                    |            | XML          | Macro                         | ? ×             |
|             | A         | В          | c            | D                 | E         | F              | G                                  | Н          |              | Macro name:                   |                 |
| 1           | Last Modi |            |              | File Size         | Exec Flag |                | _                                  |            |              | Format                        | 🔣 3 <u>R</u> un |
| 2           | ########  | N/A        | C:\Progra    | r N/A             | TRUE      |                |                                    |            |              | Format                        | Step Into       |
| 3           | ########  | N/A        | C:\Windo     | N/A               | TRUE      |                |                                    |            |              |                               | Step Into       |
| 4           | ########  | N/A        | C:\Windo     | N/A               | TRUE      |                |                                    |            |              |                               | Edit            |
| 5           | ########  | N/A        | C:\Windo     | N/A               | TRUE      |                |                                    |            |              |                               | Create          |
| 6           | ########  | N/A        | C:\Windo     | N/A               | TRUE      |                |                                    |            |              |                               |                 |
| 7           | ########  |            | C:\Progra    |                   | TRUE      |                |                                    |            |              |                               | Delete          |
| 8           | ########  |            | C:\Progra    |                   | TRUE      |                |                                    |            |              |                               | Options         |
| 9           | ########  |            | C:\Windo     |                   | TRUE      |                |                                    |            |              |                               |                 |
| 10          | ########  |            | C:\Windo     |                   | TRUE      |                |                                    |            |              | Macros in: All Open Workbooks | $\checkmark$    |
| 11          | ########  |            | C:\Windo     |                   | TRUE      |                |                                    |            |              | Description                   |                 |
| 12          | ########  |            | C:\Windo     |                   | TRUE      |                |                                    |            |              |                               |                 |
| 13          | ########  |            | C:\Windo     |                   | FALSE     |                |                                    |            |              |                               |                 |
|             | ########  |            | C:\Windo     | N/A               | FALSE     |                |                                    |            |              |                               | Consel          |
| M -         | I ► ► Sys | tem_Shir   | n /🞾 /       |                   |           |                |                                    |            | ·            |                               | Cancel          |
| Ente        | r 🛅       |            |              |                   |           |                |                                    |            |              |                               |                 |

#### Figure 10. Run Macro. (Lee, 2014, digital case files)

There are several macros in the GitHub repository that can automate the processes described above. See Appendix C for a list of macros available in the repository and a description of what each one accomplishes.

### 3.6. Pivot Tables

Pivot Tables are an excellent way to sort data in a way that visually allows you to pick out artifacts of interest. "A pivot table allows you to create an interactive view of your dataset. With a pivot table report, you can quickly and easily categorize your data into meaningful information, and perform a wide variety of calculations in a fraction of the time it takes by hand" (Jelen, 2006, p. 9). This categorization of data is particularly true when working with Windows Event Viewer logs. Exporting the data in XML table format provides headers that can be used to categorize the data in ways that will allow you to see trends and commonalities. The GitHub site has a document named "Pivot\_Table\_Example.docx" that shows examples of how you can work with pivot tables to analyze data (https://github.com/gregory-

lalla/GCIH\_Gold/blob/master/Docs/Supplement/ Pivot\_Table\_Example.docx).

### 4. Gathering the Data

Having explained the essentials of organizing logs with Excel, real understanding comes from seeing the techniques demonstrated on specific types of log files. This section will discuss examples of different log files that an incident responder may have to examine while investigating a compromised network. Then in the following section, a case study will be analyzed employing the techniques described in this paper. Appendix D provides a detailed explanation on how the Windows log files in the case study were formatted. A supplement document on the GitHub site named 'Additional\_Log\_Formatting\_Instructions.docx' (https://github.com/gregory-lalla/GCIH\_Gold/blob/master/Docs/Supplement/Additional\_Log\_Formatting\_Instruction s.docx) provides a detailed explanation of the remaining log files mentioned in this section.

### 4.1. Windows Logs

#### 4.1.1. Event Viewer Logs

One of the primary sources of information/data gathered from a Windows operating system will come from Event Viewer logs, especially if recommended auditing settings are configured appropriately (see https://technet.microsoft.com/enus/library/ee513968%28WS.10%29.aspx for recommendations). Unfortunately, a "Microsoft Windows event log is a binary file that consists of special records – Windows events" ("Windows event log essentials", 2017) and parsing the data is not as simple as manipulating the file in a text editor. Also, when exporting the data from the native Windows Event Viewer tool, depending on the format chosen, different data is returned. Last, if you've ever tried to filter or search using the native Windows Event Viewer tool, you know that it has many limitations and is extremely slow.

Because Event Viewer logs can contain hundreds of thousands of entries, it is essential to reduce the data to a manageable level. Since the Event Viewer GUI is extremely slow, the native Windows command line utility named WEVTUTIL.EXE should be used to export the data. This tool comes with its challenges such as producing XML files that Excel cannot open. When running the command, there are several options

to massage the data to a format that Excel accepts. To get the correct results, you may need to mix and match the switches until you get a compatible output.

#### 4.1.2. ShimCache Entries

The ShimCache or Application Compatibility Cache entries show executables that were likely run on the system. "The Windows Shimcache was created by Microsoft beginning in Windows XP to track compatibility issues with executed programs...It is important to understand there may be entries in the Shimcache that were not actually executed" (Parisi, 2015). "Microsoft designed the Shimcache in Windows Vista, 7, Server 2008 and Server 2012 to incorporate a 'Process Execution Flag' category for each entry" (Parisi, 2015). For further details on the Shimcache and the differences between XP/2003 and Vista+, see https://www.fireeye.com/blog/threatresearch/2015/06/caching\_out\_the\_val.html

#### 4.1.3. Shellbags

Shellbags reflect the locations that the user has traversed using Windows Explorer. "Shellbags are found in the Windows Registry and store user preferences for folder display in Windows Explorer, such as the size of the window or how items were listed. For a folder to exist in the shellbags, it must have been opened in Windows Explorer at least one time by the user" (Cowen, 2013, ch. 13). The user's usrclass.dat (Vista+) and NTUSER.DAT registry files contain the Shellbag artifacts.

#### 4.1.4. AutoRun Entries

Autorun entries refer to "software that runs automatically without being intentionally started by the user. These include drivers and services that start when the computer boots; application, utilities and shell extensions that start when a user logs on; and browser extensions that load when Internet Explorer is started" (Russinovich, 2011, ch. 5). To parse autorun data, run the autorunsc.exe command against the registry files of a system. You can run the tool on a live system or offline by mounting an image of the hard drive and pointing the program to the newly mapped location.

#### 4.1.5. Web Browser Logs

The client browser may provide clues on how the adversary initially got onto a system, either through the user browsing the internet or by clicking on a link in an email or document. That information may be quite valuable in targeted attacks against the employees of a company. This section will examine Internet Explorer (IE) history/cache logs in index.dat files (IE 9 and below). Newer versions of IE browsers store their data in an Extensible Storage Engine (ESE) database. There are still other browsers that use SQLite databases. However, the data represented should still be similar once exported out of the database and into a plaintext format.

#### 4.1.6. MFT Entries

"The Master File Table (MFT) is the heart of NTFS because it contains the information about all files and directories. Every file and directory has at least one entry in the table, and the entries by themselves are very simple" (Carrier, 2005, p. 274).

#### 4.1.7. Prefetch Entries

"Application prefetch is intended to enable a better user experience within Windows systems by monitoring an application as it's launched, and then 'prefetching' the necessary code to a single location so that the next time the application is launched, it launches faster. This way, the system doesn't have to seek across the file system for DLLs and other data that it needs to start the application – it knows where to find it" (Carvey, 2014, p. 98).

### 4.2. Other Log File Types

#### 4.2.1. Linux System Logs

The formatting of logs produced by many applications and services in Linux make importing the data into Excel challenging. The manual massaging of the data is not difficult but must be done in several stages using a variety of tools. Many of the tools originated on the UNIX operating system, but the ones used in this document have all been ported over to Windows. These tools are from the GNU utilities run under the Open Source tools package CYGWIN.

Linux produces several plain text system logs that may have value to the incident response analyst and which all have the same log format. In the supplement, we will look specifically at the Syslog, Auth.log and Cron.log files, but we can use the same techniques against the Daemon.log, Boot.log, Mail.log and other system log files. See http://www.thegeekstuff.com/2011/08/linux-var-log-files/ for a listing of system logs that may appear on a Linux host.

The syslog daemon handles messages from the entire system to include many of the system logs mentioned above. Depending on the configuration of the logging in the syslog.conf configuration file, the bulk of the message usually are sent to the 'syslog' (often named 'messages') log file. The Auth.log file contains user authentication information, and the Cron logs record the activity of the cron jobs (scheduled tasks) run on the system.

#### 4.2.2. Apache Access and Error Logs

Another log you may find on a Linux server is the Apache www-access.log file which records connections made from a client to the web services of the system. Web servers are often exploited and could provide the adversary with an initial stepping stone into a network. What gets logged can vary based on the configuration of the web server.

The Apache Error logs contain web server error and resource alerts. The formatting of this log is similarly to the Linux system logs discussed previously. The log should have the dates and delimiters corrected, so each field is in its proper column.

#### 4.2.3. IIS Web and FTP Logs

The native format of the IIS Web log allows for easy importing of data into Excel. However, the scattering of headers throughout a log file presents the only real issue. By filtering on the Date/Time column for entries that are not in the Date/Time format, the extra headings can be found and removed.

#### 4.2.4. IPTables Firewall Logs

Scrutinizing network traffic when combined with other types of artifacts may also be beneficial to your investigation by identifying communications associated with the event and adding those IP addresses to your keywords for further examination.

IPTables and most other firewalls will produce logs that can be exported and examined. IPTables is run on Unix/Linux systems and has logs similar in format to the Linux system logs discussed earlier in this paper. Therefore, the same steps are used to fix the dates and set the delineation of the fields.

#### 4.2.5. Packet Captures

Packet Captures can be included as well into the analysis of the incident. For the packets to get formatted correctly when exported, the columns in Wireshark need to be changed to produce the results desired.

#### 4.2.6. Snort and Bro IDS Logs

Host-based and network-based IDS logs are critical to incorporate into the analysis as it may be the primary reason you are aware of the intrusion in the first place. These logs usually contain data from the best vantage point, either from the network or host perspective.

Snort is an open source product that "supports sending real-time alerts when an intrusion event is detected and can even be used as an inline 'intrusion prevention system' that enables you to receive alerts in real time and in several different medium, rather than having to continuously sit at a desk monitoring your Snort system 24 hours a day" (Caswell, 2007, ch. 2).

The supplement will look at the logs produced by running snort in Fast alert mode which "writes the alert in a simple format with a timestamp, alert message, source and destination IPs/ports" (Roesch, 2003).

Bro is another open source intrusion detection system. "Bro inspects all traffic flowing into and out of a network. It can operate in passive mode, in which it generates alerts for suspicious activity, or in active mode, in which it injects traffic to disrupt malicious activity ... Unlike other NIDSs, Bro monitors traffic flows rather than just matching patterns inside individual packets. This method of operation means that Bro can detect suspicious activity based on who talks to whom, even without matching any particular string or pattern" (Nemeth, 2010, ch. 22). Bro produces several logs, each of which can use the technique described in the supplement to achieve our standard layout.

Here are some of the logs Bro generates: Conn, DHCP, DNS, Files, HTTP, Weird, etc. The supplement will examine the Bro Connect log (conn.log) which records TCP, UDP and ICMP connections.

### 5. Case Study

#### 5.1. SANS Stark Research Labs

The techniques for extracting and importing the relevant log files in this Case Study are shown in Appendix D. Macros to automate the manipulation of the data are listed in Appendix C. The application of these tools and techniques will be demonstrated by examining an incident presented in the SANS Forensic 508 Advanced Computer Forensic Analysis and Incident Response exercise workbook titled 'Stark Research Labs Intrusion.' The scenario describes how a company received a phone call on April 06, 2012 @ 5 PM EDT from a 3-4 letter government agency stating "We have seen a few hundred megabytes of sensitive data leave your network bound for a foreign country. Don't ask how we know, but you might want to check 10.3.58.7 on your network" (Lee, 2014, ex. 0 p. 2).

Given other information about the company and its assets, a preliminary keyword list is compiled by the incident response team to include the following terms: hydra, star fury, agents, secret and formula. When discussing log files and artifacts below, you can assume that the files have already been imported into Excel with the standard format.

#### 5.1.1. WinXP-TDugan (WKS-WINXP32BIT)

The host reported as leaking data (IP address of 10.3.58.7) is a machine running Windows XP. Since data appears to be actively leaving the host, the first step would be to see what applications have been running on the system. There are two artifacts made available to us that can show what was running on the workstation. The first is the Prefetch files. Applying our initial keyword list against the output gives us one hit on HYDRAKATZ.EXE. The name of the file is similar to Mimikatz, which is a post exploitation tool to capture user credentials. We will flag this suspicious executable by giving the hit a 'Named Cell' of 'HYDRAKATZ\_1' and highlighting the row in yellow (Figure 11).

| F  | FILE HOM                  | /IE IN   | SERT PA      | GE LAYOUT  | FORMULAS DATA REVIEW W           |   | Named                | Cell and        | High     | nlighted       |            |       |   |
|----|---------------------------|----------|--------------|------------|----------------------------------|---|----------------------|-----------------|----------|----------------|------------|-------|---|
| H  | YDRAKA                    |          |              | x HYDRA    | KATZ.EXE                         |   |                      |                 |          | -              |            |       |   |
|    | А                         |          | В            | С          | D                                |   | E                    | E E             |          | G              | н          |       | 1 |
| 1  | Date/Time                 | v        | Account ~    | Computer 💌 | Description                      | • | Details              | Pror .rties     | -        | Miscellaneou 👻 | Artifacts  | T     |   |
| 3  | 04/02/2012                | 22:24:04 | N/A          | TDUNGAN    | HELPER.EXE-0415776D.pf           |   | HELPER.EXE           | Ny ober of Time | Run: 1   |                | Prefetch B | Intry |   |
| 24 | 04/03/2012                | 00:33:17 | N/A          | TDUNGAN    | PKXEZY1TJI98.EXE-0BCBF29B.pf     |   | PKXEZY1TJI98.EXE     | umber of Time   | Run: 1   |                | Prefetch B | Intry |   |
| 25 | 04/03/2012                | 01:03:30 | N/A          | TDUNGAN    | FIREFOX.EXE-28641590.pf          |   | FIREFOX.EXE          | Number of Time  | Run: 17  |                | Prefetch B | Entry |   |
| 6  | 04/03/2012                | 01:05:20 | N/A          | TDUNGAN    | PLUGIN-CONTAINER.EXE-15EDC9DD.pf |   | PLUGIN-CONTAINER.EXE | Number of Time  | Run: 4   |                | Prefetch B | Intry |   |
| 7  | 04/03/2012                | 14:44:02 | N/A          | TDUNGAN    | SLLAUNCHER.EXE-0E3D1802.pf       |   | SLLAUNCHER.EXE       | Number of Time  | Run: 18  |                | Prefetch B | Intry |   |
| 28 | 04/03/2012                | 16:07:49 | N/A          | TDUNGAN    | FTP.EXE-0FFFB5A3.pf              |   | FTP.EXE              | Number of Time  | Run: 1   |                | Prefetch B | Intry |   |
| 9  | 04/03/2012                | 17:15:10 | N/A          | TDUNGAN    | HYVY.EXE-2A94EF14.pf             |   | HYVY.EXE             | Number of Time  | Run: 5   |                | Prefetch B | Intry |   |
| 0  | 04/03/2012                | 18:22:55 | N/A          | TDUNGAN    | RUNDLL32.EXE-2576181F.pf         |   | RUNDLL32.EXE         | Number of Time  | Run: 1   |                | Prefetch B | Entry |   |
| 31 | 04/03/2012                | 18:22:59 | N/A          | TDUNGAN    | SSSTARS.SCR-2D6FC20D.pf          |   | SSSTARS.SCR          | Number of Time  | Run: 1   |                | Prefetch B | Intry |   |
| 32 | 04/03/2012                | 23:30:35 | N/A          | TDUNGAN    | HYDRAKATZ.EXE-27B49502.pf        |   | HYDRAKATZ.EXE        | Number of Time  | Run: 4   |                | Prefetch B | Intry |   |
| 33 | 04/04/2012                | 03:31:07 | N/A          | TDUNGAN    | RUNDLL32.EXE-48E4BF0A.pf         |   | RUNDLL32.EXE         | Number of Time  | Run: 1   |                | Prefetch B | Entry |   |
| 34 | 04/04/2012                | 12:16:00 | N/A          | TDUNGAN    | MSFEEDSSYNC.EXE-25E13438.pf      |   | MSFEEDSSYNC.EXE      | Number of Time  | Run: 242 |                | Prefetch B | Intry |   |
| 35 | 04/04/2012                | 12:22:40 | N/A          | TDUNGAN    | A.EXE-0F3A0E12.pf                |   | A.EXE                | Number of Time  | Run: 67  |                | Prefetch B | Intry |   |
| 36 | 04/04/2012                | 12:22:56 | N/A          | TDUNGAN    | RUNDLL32.EXE-13CC3015.pf         |   | RUNDLL32.EXE         | Number of Time  | Run: 1   |                | Prefetch B | Intry |   |
| 87 | 04/04/2012                | 12.22.57 | Ν/Δ          | TDUNGAN    | RUNDLI 32 EXE-2001189D of        |   | RUNDLI 32 EXE        | Number of Time  | Run: 1   |                | Prefetch F | ntry  | _ |
|    | $\prec  \models  \ldots $ | prefete  | :h_file_info | +          |                                  |   | : 4                  |                 |          |                |            |       | Þ |

Figure 11. Named Cell and Highlight keyword hits. (Lee, 2014, digital case files)

This keyword hit also gives us an initial timeframe of the incident. The file Hydrakatz ran on 04/03/2012, and a notification was sent to the company regarding a data leak on 04/06/2012. Looking at the Prefetch entries around that timeframe gives us addition clues. Right around hydrakatz.exe, there is a file that appears to be a randomly generated name, PKXEZY1TJI98.EXE; two files with unusual names, HYVY.EXE and A.EXE; and the execution of FTP.EXE. These are all 'Named' and highlighted (Figure 12).

| X  | 1 🗄 🔊 🤆        | > □ =             |                      | TDUNGAN_Pre                      | fetch_Results.xlsx - Excel |                         | ? 🖅 — 🗆                      |
|----|----------------|-------------------|----------------------|----------------------------------|----------------------------|-------------------------|------------------------------|
| F  | FILE HOME      | INSERT P          | AGE LAYOUT           | FORMULAS DATA REVIEW VIEW        | N                          | Unusual File            | Names                        |
| PI | KXEZY1T 🔻      | : X 🗸             | ƒ <sub>X</sub> pkxez | Y1TJI98.EXE                      |                            | //                      | //                           |
|    | Α              | В                 | С                    | D                                | E                          | F                       | G H                          |
|    | Date/Time      | Account           | Computer 💌           |                                  | 🖌 Details 🛛 🖊 🗹            | Tropertie               | niscellaneou 💌 Artifacts 🛛 💌 |
| ļ  | 04/03/2012 00: |                   | TDUNGAN              | PKXEZY1TJI98.EXE-0BCBF29B.pf     | PKXEZY1TJI98.EXE           | Num' ar of Time Run     | Prefetch Entry               |
|    | 04/03/2012 01: | 03:30 N/A         | TDUNGAN              | FIREFOX.EXE-28641590.pf          | FIREFOX.EXE                | .amber of Time Plan: 17 | Prefetch Entry               |
| 5  |                |                   | TDUNGAN              | PLUGIN-CONTAINER.EXE-15EDC9DD.pf | PLUGIN-CONTAINER.FY        | Number of Till.e Run: 4 | Prefetch Entry               |
|    | 04/03/2012 14: | 44:02 N/A         | TDUNGAN              | SLLAUNCHER.EXE-0E3D1802.pf       | SLLAUNCHER, EXF            | Number Fime Run: 18     | Prefetch Entry               |
| 3  | 04/03/2012 16: | 07:49 N/A         | TDUNGAN              | FTP.EXE-0FFFB5A3.pf              | FTP.EXE                    | Num'⊿r of Time Run: 1   | Prefetch Entry               |
| 9  | 04/03/2012 17: | 15:10 N/A         | TDUNGAN              | HYVY.EXE-2A94EF14.pf             | HYVY.EXE                   | Mumber of Time Run: 5   | Prefetch Entry               |
| 0  | 04/03/2012 18: | 22:55 N/A         | TDUNGAN              | RUNDLL32.EXE-2576181F.pf         | RUNDLL32.EXE               | Number of Time Run: 1   | Prefetch Entry               |
| 1  | 04/03/2012 18: | 22:59 N/A         | TDUNGAN              | SSSTARS.SCR-2D6FC20D.pf          | SSSTARS.SCR                | Number of Time Run: 1   | Prefetch Entry               |
| 2  | 04/03/2012 23: | 30:35 N/A         | TDUNGAN              | HYDRAKATZ.EXE-27B49502.pf        | HYDRAKATZ.EXE              | Number of Time Run: 4   | Prefetch Entry               |
| 3  | 04/04/2012 03: | 31:07 N/A         | TDUNGAN              | RUNDLL32.EXE-48E4BF0A.pf         | RUNDLL32-EX                | Number of Time Run: 1   | Prefetch Entry               |
| 4  | 04/04/2012 12: | 16:00 N/A         | TDUNGAN              | MSFEEDSSYNC.EXE-25E13438.pf      | MSFEEDS C.EXE              | Number of Time Run: 242 | Prefetch Entry               |
| 85 | 04/04/2012 12: | 22:40 N/A         | TDUNGAN              | A.EXE-0F3A0E12.pf                | A.EXE                      | Number of Time Run: 67  | Prefetch Entry               |
| 86 | 04/04/2012 12: | 22:56 N/A         | TDUNGAN              | RUNDLL32.EXE-13CC3015.pf         | RUNDLL32.EXE               | Number of Time Run: 1   | Prefetch Entry               |
| 87 | 04/04/2012 12: | 22:57 N/A         | TDUNGAN              | RUNDLL32.EXE-2CC11B9D.pf         | RUNDLL32.EXE               | Number of Time Run: 1   | Prefetch Entry               |
| 8  | 04/04/2012 12  | 25-54 N/A         | TDUNGAN              | RUNDU 32 EXE-470E11BD of         | RUNDLI 32 EXE              | Number of Time Run: 1   | Prefetch Entry               |
|    |                | refetch_file_info | +                    |                                  | E 4                        |                         |                              |

Figure 12. Unusual File Names. (Lee, 2014, digital case files)

Looking within the timeframe, we see activities that suggest the adversary ran commands on the system (Figure 13). There is also another suspicious file named PE.EXE. These are all 'Named' and highlighted as well (Figure 13).

| 185      | ) •<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>· <b< th=""><th></th><th>1</th><th>DUNGAN_Prefetch_Results.xlsx - Excel</th><th></th><th>? 🗹 — 🗆</th></b<> |                 | 1                        | DUNGAN_Prefetch_Results.xlsx - Excel |                         | ? 🗹 — 🗆           |
|----------|---|-----------------|--------------------------|--------------------------------------|-------------------------|-------------------|
| FILE H   | HOME INSERT   | PAGE LAYOUT     | FORMULAS DATA RE         | VIEW VIEW                            | Suspicious Activity     | U                 |
| e_1      |   | $f_x$ pe.ex     | E                        |                                      |                         |                   |
|          | A B   | С               | D                        | E                                    | F G                     | Н                 |
| Date/Tin | ne 💌 Accou  | nt 🔹 Computer 🕚 | Description              | ✓ Details                            | Pr perties 💽 Miscellan  | eou 👻 Artifacts 💽 |
| 04/04/20 | 012 12:22:40 N/A  | TDUNGAN         | A.EXE-0F3A0E12.pf        | A.EXE                                | Jumber of Time Run: 67  | Prefetch Entry    |
| 04/04/20 | 012 14:01:32 N/A  | TDUNGAN         | A.EXE-0FBE37C1.pf        | A.EXE                                | Number of Time Run: 390 | Prefetch Entry    |
| 04/04/20 | 012 18:05:29 N/A  | TDUNGAN         | WMIC.EXE-3B772CC6.pf     | WMIC.EXE                             | Number of Time Run: 6   | Prefetch Entry    |
| 04/05/20 | 012 13:28:01 N/A  | TDUNGAN         | A.EXE-2E0C27A0.pf        | A.EXE                                | Number of Time Run: 490 | Prefetch Entry    |
| 04/05/20 | )12 14:18:24 N/A  | TDUNGAN         | FIND.EXE-0EC32F1E.pf     | FIND.EXE                             | Number of Time Run: 1   | Prefetch Entry    |
| 04/05/20 | )12 17:12:12 N/A  | TDUNGAN         | IPCONFIG.EXE-2395F30B.pf | IPCONFIG.EXE                         | Number of Time Run: 4   | Prefetch Entry    |
| 04/05/20 | )12 17:38:21 N/A  | TDUNGAN         | REG.EXE-0D2A95F7.pf      | REG.EXE                              | Number of Time Run: 16  | Prefetch Entry    |
| 04/05/20 | )12 17:44:17 N/A  | TDUNGAN         | NET1.EXE-029B9DB4.pf     | NET1.EXE                             | Number of Time Run: 23  | Prefetch Entry    |
| 04/05/20 | )12 17:46:11 N/A  | TDUNGAN         | TASKLIST.EXE-10D94B23.pf | TASKLIST.EXE                         | Number of Time Run: 8   | Prefetch Entry    |
| 04/06/20 | 012 18:55:35 N/A  | TDUNGAN         | AT.EXE-2770DD18.pf       | AT.EXE                               | Number of Time Run: 14  | Prefetch Entry    |
| 04/06/20 | )12 19:20:22 N/A  | TDUNGAN         | CMD.EXE-087B4001.pf      | CMD.EXE                              | Number of Time Run: 60  | Prefetch Entry    |
| 04/06/20 | )12 19:21:27 N/A  | TDUNGAN         | NET.EXE-01A53C2F.pf      | NET.EXE                              | Number of Time Run: 66  | Prefetch Entry    |
| 04/06/20 | 012 19:22:20 N/A  | TDUNGAN         | PE.EXE-0DC593C2.pf       | PE.EXE                               | Number of Time Run: 30  | Prefetch Entry    |
| 04/07/20 | 012 01:23:52 N/A  | TDUNGAN         | A.EXE-239305EA.pf        | A.EXE                                | Number of Time Run: 174 | Prefetch Entry    |
|          |   |                 |                          |                                      |                         |                   |
|          | prefetch_file   | info 🕂          |                          |                                      | 4                       | •                 |
| ADY 18 O | F 111 RECORDS FOUR  | ID 🔠            |                          |                                      |                         | + 100             |

Figure 13. Suspicious activity. (Lee, 2014, digital case files)

The keyword lists should contain the newly found keywords identified in the Prefetch output. As new ones get found, those will be added as well to help locate other indicators of compromise. The second artifact containing the execution of files is the ShimCache entries from the registry.

Running the keywords against the ShimCache artifacts produced one hit on file PE.EXE. Though the dates of the artifact don't show the time of execution, executables with the same write timestamp may be related. In this output, there is another executable, located in a strange location, which has the same timestamp as PE.EXE. Normally svchost.exe will reside in C:\Windows\System32. Its location in

C:\Windows\System32\dllhost, makes it suspicious. Since the legitimate svchost.exe file shows up in a lot of logs, the keyword for this IOC will be '\dllhost\'. Both entries are 'Named' and highlighted (Figure 14).

| x∎  |          | <b>)</b> . ⊜. | <b></b> =           |             |                     | TDUNGAN          | N_ShimCache_Results.xlsx - Excel |              |               | ? 📧      | - 0       | ×  |
|-----|----------|---------------|---------------------|-------------|---------------------|------------------|----------------------------------|--------------|---------------|----------|-----------|----|
| FI  | LE       | HOME          | INSERT              | PAGE LAYOUT | FORMULAS D          | ATA REVIEW       | VIEW                             | Same Timesta | amp           |          |           |    |
| dll | host_1   | • :           | $\times \checkmark$ | $f_x$ C:\\  | WINDOWS\system32    | dllhost\svchost. | .exe                             |              |               |          |           | ٧  |
|     |          | Α             | В                   | С           | D                   |                  | E                                |              | F             | G        | н         |    |
| 1   | Date/Tir | me            | Accol -             | Computer 👻  | Description 🔹       | Detail           |                                  | -            | Properties 💌  | Miscel 💌 | Artifacts | -  |
| 29  | 04/14/20 | 008 00:12:1   | 1 N/A               | TDUNGAN     | User ShimCache      | , c:\WINDOWS\S   | System32\zipfldr.dll             |              | Executed: N/A |          | ShimCach  | he |
| 30  | 04/14/20 | 008 00:12:1   | 7 N/A               | TDUNGAN     | User Shi Lache Entr | C:\WINDOWS\s     | system32\dmremote.exe            |              | Executed: N/A |          | ShimCach  | he |
| 31  | 04/14/20 | 008 00:12:1   | 7 N/A               | TDUNGAN     | Jer ShimCache Entr  | C:\WINDOWS\s     | system32\dmadmin.exe             |              | Executed: N/A |          | ShimCach  | he |
| 32  | 04/14/20 | 008 00:12:3   | 4 N/A               | LINGAN      | User ShimCache Entr | C:\Program File  | es\Outlook Express\setup50.exe   |              | Executed: N/A |          | ShimCach  | he |
| 33  | 04/14/20 | 008 00:12:3   | 6 N/A               | TDUNGAN     | User ShimCache Entr | C:\WINDOWS\s     | system32\dllhost\svchost.exe     |              | Executed: N/A |          | ShimCach  | he |
| 34  | 04/14/20 | 008 00:12:3   | 6 N/A               | TDUNGAN     | User ShimCache Entr | C:\WINDOWS\s     | system32\pe.exe                  |              | Executed: N/A |          | ShimCach  | he |
| 35  | 04/14/20 | 008 00:12:3   | 8 N/A               | TDUNGAN     | User ShimCache Entr | C:\WINDOWS\s     | system32\verclsid.exe            |              | Executed: N/A |          | ShimCach  | he |

Figure 14. Identical Timestamps. (Lee, 2014, digital case files)

Next, we'll look at the MFT file. After running our keywords against this file's output, we can now see the full paths of the suspicious artifacts (Figure 15).

| x∎    | 5 - ∃      | ð - 🗋      | ÷      |             |                       | TDUNGAN_MFT_Results.xlsx - Excel                                      | ? 🗹 — 🗆 🗙                                |
|-------|------------|------------|--------|-------------|-----------------------|---|--|
| FILE  | HOM        | e inse     | RT     | PAGE LAYOUT | FORMULAS DA           | FA REVIEW VIEW  |  |
|       |            |            |        |             |                       |   |  |
| pkxe  | ezy1tji ▼  | : X        | $\sim$ | $f_x$ C:\D  | ocuments and Setting  | s\tdungan\Local Settings\Temp\pkxezy1tji98.exe                        | ×  |
|       | ۵          |            | В      | С           | D                     | E   |  |
| 1     | Date/Time  | , a        | Acco   | Compute 👻   | Description           | Details   | T Properties                             |
| 50030 | 04/03/2012 | 2 00:33:15 | N/A    | TDUNGAN     | Create Date (FN Info) | C:\Documents and Settings\tdungan\Local Settings\Temp\pkxezy1tji98.ex | e Std Info - Create: 04/03/2012 00:33:15 |
| 50070 | 04/03/2012 | 2 01:03:04 | N/A    | TDUNGAN     | Create Date (FN Info) | C:\Documents and Settings\tdungan\Local Settings\Temp\a.exe           | Std Info - Create: 04/03/2012 01:03:04   |
| 50604 | 04/03/2012 | 2 15:19:50 | N/A    | TDUNGAN     | Create Date (FN Info) | C:\WINDOWS\system32\hydrakatz.exe                                     | Std Info - Create: 03/31/2003 12:00:00   |
| 50605 | 04/03/2012 | 2 15:26:01 | N/A    | TDUNGAN     | Create Date (FN Info) | C:\WINDOWS\system32\pe.exe  | Std Info - Create: 03/31/2003 12:00:00   |
| 50616 | 04/03/2012 | 2 16:30:02 | N/A    | TDUNGAN     | Create Date (FN Info) | C:\WINDOWS\system32\hyvy.exe  | Std Info - Create: 03/31/2003 12:00:00   |
| 50617 | 04/03/2012 | 2 16:30:02 | N/A    | TDUNGAN     | Create Date (FN Info) | C:\WINDOWS\system32\hyvy.exe:Zone.Identifier                          | Std Info - Create: 03/31/2003 12:00:00   |
| 50714 | 04/03/2012 | 2 20:43:44 | N/A    | TDUNGAN     | Create Date (FN Info) | C:\Documents and Settings\RSydow\Local Settings\Temp\a.exe            | Std Info - Create: 04/03/2012 20:43:44   |
| 50953 | 04/04/2012 | 2 12:26:24 | N/A    | TDUNGAN     | Create Date (FN Info) | C:\Documents and Settings\SRL-Helpdesk\Local Settings\Temp\a.exe      | Std Info - Create: 04/04/2012 12:26:24   |
| 51200 | 04/04/2012 | 2 16:41:47 | N/A    | TDUNGAN     | Create Date (FN Info) | C:\Documents and Settings\vibranium\Local Settings\Temp\a.exe         | Std Info - Create: 04/04/2012 16:41:47   |
| 52211 |            |            |        |             |                       |   |  |

Figure 15. Paths of suspicious files are displayed. (Lee, 2014, digital case files)

When looking at the keyword hits, you'll notice that they often appear in clusters. Looking at one of the clusters, we see a new artifact named SEKURLSA.DLL in the middle of several suspicious executables (Figure 16). Googling this file name shows us that it belongs to the Mimikatz tool mentioned previously. This discovery substantiates our guess that file hydrkatz.exe is Mimikatz in disguise. Therefore, we'll add Sekurlsa.dll to our keyword list.

| 🚺 🗄 🏷 🖓 🗋 Ŧ                   | TDUNGAN_MFT_Results.xlsx - Excel  | ? 🗹 – 🗆 🗙                                      |
|-------------------------------|---|--|
| FILE HOME INSERT              | PAGE LAVOUT FORMULAS DATA REVIEW VIEW Suspicious File in  | Keyword Grouping                               |
| sekurlsa_1 🔹 : 🗙 🗸            | fx C:\WINDOWS\system32\sekurlsa.dll   | V  |
| A B                           | C D E   |  |
| 1 Date/Time Acco              | Compute Description     Details   | <ul> <li>Properties</li> </ul>                 |
| 50604 04/03/2012 15:19:50 N/A | TDUNGAN Create Date (FN Inf.) C:\WINDOWS\system32\hydrakatz.e                                   | Stil Info - Create: 03/31/2003 12:00:00        |
| 50605 04/03/2012 15:26:01 N/A | TDUNGAN Create Date (FN Inf)) _C:\WINDOWS\system32\pe.exe                                       | Stil Info - Create: 03/31/2003 12:00:00        |
| 50606 04/03/2012 15:30:13 N/A | TDUNGAN Create Date (FN Info) C:\WINDOWS\system32\sekurlsa.dll                                  | St. Info - Create: 03/31/2003 12:00:00         |
| 50607 04/03/2012 15:33:20 N/A | TDUNGAN Create Date (FN Inf.) C:\WINDOWS\Prefetch\HYDRAKATZ.EXE-27B49502.pf                     | Std Info - Create: 04/03/2012 15:33:20         |
| 50608 04/03/2012 15:40:31 N/A | TDUNGAN Create Date (FN Inf.) C:\WINDOWS\Prefetch\NET.EXE-01A53C2F.pf                           | Std Info - Create: 04/03/2012 15:40:31         |
| 50609 04/03/2012 15:40:31 N/A | TDUNGAN Create Date (FN Inf)) C:\WINDOWS\Prefetch\NET1.EXE-029B9DB4.pf                          | Styl Info - Create: 04/03/2012 15:40:31        |
| 50610 04/03/2012 16:02:15 N/A | TDUNGAN Create Date (FN Inf.) C:\WINDOWS\Prefetch\HYVY.EXE-2A94EF14.pf                          | Stil Info - Create: 04/03/2012 16:02:15        |
| 50611 04/03/2012 16:06:55 N/A | TDUNGAN Create Date (FN Infb) C:\Documents and Settings\tdungan\Application Data\Skype\shared   | .xml Std Info - Create: 08/25/2011 21:55:40    |
| 50612 04/03/2012 16:08:00 N/A | TDUNGAN Create Date (FN Info) C:\WINDOWS\Prefetch\FTP.EXE-0FFFB5A3.pf                           | Std Info - Create: 04/03/2012 16:08:00         |
| 50613 04/03/2012 16:09:29 N/A | TDUNGAN Create Date (FN Info) C:\Documents and Settings\tdungan\Local Settings\Application Data | \Mozill Std Info - Create: 04/03/2012 16:09:29 |
| 50614 04/03/2012 16:09:29 N/A | TDUNGAN Create Date (FN Info) C:\Documents and Settings\tdungan\Local Settings\Application Data | \Mozill.Std Info - Create: 04/03/2012 16:09:29 |
| 50615 04/03/2012 16:29:56 N/A | TDUNGAN Create Date (FN Info) C:\Documents and Settings\tdungan\Application Data\Dropbox\shell  |  |
| 50616 04/03/2012 16:30:02 N/A | TDUNGAN Create Date (FN Info) C:\WINDOWS\system32\hyvy.exe                                      | Std Info - Create: 03/31/2003 12:00:00         |
| 50617 04/03/2012 16:30:02 N/A | TDUNGAN Create Date (FN Info) C:\WINDOWS\system32\hyvy.exe:Zone.Identifier                      | Std Info - Create: 03/31/2003 12:00:00         |
| 50618 04/03/2012 16:39:28 N/A | TDUNGAN Create Date (EN Info) C·\Documents and Settings\tdungan\Local Settings\Application Data |  |
| MFT_TDungan                   | +   | ×  |
| READY 🛗                       |   | Ⅲ □+ 100%                                      |

Figure 16. Mimikatz .dll file. (Lee, 2014, digital case files)

Finally, it is easy to filter the data on a particular path to see if there are any other files of interest in the same directories. Looking at c:\windows\system32\dllhost\, we find the file WINCLIENT.REG, which we'll add to the keyword list (Figure 17).

| 🕼 🖯 🕈 🖓 · 🗋 🗧               |                         | TDUNGAN_MFT_Results.xlsx - Excel                  | ? 🗹 — 🗖                                |
|-----------------------------|-------------------------|---|--|
| FILE HOME INSERT P          | AGE LAYOUT FORMULAS     | DATA REVIEW VIEW                                  |  |
| vinclient_1 🔻 🗄 🗙 🗸         | fx C:\WINDOWS\syste     | m32\dllhost\winclient.reg                         |  |
| A B                         | C D                     | E   |  |
| Date/Time 🔹 Accc 💌          | Compute   Description   | <ul> <li>Details</li> </ul>                       | T Properties                           |
| 34 04/03/2012 00:34:26 N/A  | TDUNGAN Create Date (F  | N Info) C:\WINDOWS\system32\dllhost               | Std Info - Create: 04/03/2012 00:34:26 |
| 35 04/03/2012 00:35:03 N/A  | TDUNGAN Create Date (F  | N Info) C:\WINDOWS\system32\dllhost\svchost.exe   | Std Info - Create: 03/31/2003 12:00:00 |
|                             | TOUNCAN, Create Date (F | N Info) C:\WINDOWS\system32\dllhost\winclient.reg | Std Info - Create: 04/03/2012 00:35:10 |
| 136 04/03/2012 00:35:10 N/A | TDUNGAN Create Date (F  |   |  |

Figure 17. Winclient artifact. (Lee, 2014, digital case files)

Using the keywords or IOCs discovered so far, we can start to look for other compromised systems on the network.

### 5.1.2. Win7-32-NROMANOFF (WKS-WIN732BITA)

Running our keyword list against workstation WKS-WIN732BITA (10.3.58.7) prefetch files generates hits on A.EXE and HYDRAKATX.EXE. Within the intrusion timeframe established earlier, we see the adversary possibly using native Windows tools to explore the host and network (Figure 18).

| xII 🔒     | <b>5</b> -∂-[  | ] ÷          |              | •            |             | NROMAN | OFF_Prefetch_ | Results.xlsx - Excel | N. Out the A                 | ? 🗷 -                            | - 🗆 X   |
|-----------|----------------|--------------|--------------|--------------|-------------|--------|---------------|----------------------|------------------------------|----------------------------------|---------|
| FILE      | HOME IN:       | SERT PA      | AGE LAYOUT   | FORMULAS     | DATA        | REVIEW | VIEW          |                      | More Suspicious Ac           | tivity                           |         |
|           |                |              | C            |              |             |        |               |                      |                              |                                  |         |
| AT_1      |                | X 🗸 .        | $f_x$ AT.EXE |              |             |        |               |                      |                              |                                  | ~       |
|           | А              | в            | С            |              | D           |        |               |                      |                              | G                                | E F     |
| 1 Date/   | Time 💌         | Account -    | Computer 👻   | Description  |             |        |               | Details              | T Propertic                  | <ul> <li>Miscellaneou</li> </ul> | Artifac |
| 17 04/03/ | /2012 21:50:44 | N/A          | NROMANOF     | WMIC.EXE-B7  | 7E8CD6.pf   |        |               | WMIC.EXE             | Numb , of Time Run: 2        |                                  | Prefete |
| 22 04/03/ | /2012 23:10:02 | N/A          | NROMANOFF    | NETSTAT.EXE- | -6D34D712.p | of     |               | NETSTAT.EXE          | Nr aber of Time Run: 3       |                                  | Prefete |
| 25 04/04/ | /2012 00:43:06 | N/A          | NROMANOFF    | A.EXE-8D56B1 | LC4.pf      |        |               | A.EXE                | 🗧 🦾 💦 Number of Time Run: 26 | 5                                | Prefete |
|           | /2012 01:52:26 |              | NROMANOFF    | SC.EXE-BC6DA | AF49.pf     |        |               | SC.EXE               | Number of Time Run: 12       | 2                                | Prefeto |
|           | /2012 01:55:42 |              | NROMANOFF    |              |             |        |               | REG.EXE              | Number of Time Run: 9        |                                  | Prefeto |
|           | /2012 15:48:46 |              | NROMANOFF    | TASKLIST.EXE | -9811F41E.p | f      |               | TASKLIST.EXE         | Number of Time Run: 1        |                                  | Prefeto |
|           | /2012 13:20:48 |              | NROMANOFF    |              |             |        |               | HYDRAKATZ.EX         |                              |                                  | Prefeto |
|           | /2012 13:24:24 |              | NROMANOFF    |              |             | of     |               | IPCONFIG.EXE         | Number of Time Run: 6        |                                  | Prefeto |
|           | /2012 13:25:06 |              | NROMANOFF    |              |             |        |               | NET1.EXE             | Number of Time Run: 9        |                                  | Prefeto |
|           | /2012 13:41:09 |              | NROMANOFF    |              |             |        |               | AT.EXE               | Number of Time Run: 9        |                                  | Prefeto |
|           | /2012 14:03:14 |              | NROMANOFF    |              |             |        |               | NET.EXE              | Number of Time Run: 14       |                                  | Prefeto |
|           | /2012 19:00:47 |              | NROMANOFF    |              |             |        |               | CMD.EXE              | Number of Time Run: 25       |                                  | Prefeto |
|           | /2012 19:00:55 |              | NROMANOFF    |              |             |        |               | PING.EXE             | Number of Time Run: 14       |                                  | Prefet  |
|           | /2012 16:22:10 | N/A          | NROMANOF     | A.EXE-F91CBA | VOE.pf      |        |               | A.EXE                | Number of Time Run: 15       | 641                              | Prefet  |
| 122       | prefeto        | h file info: | (+)          |              |             |        |               | :                    | •                            |                                  |         |
| D54.DX 44 |                |              | -            |              |             |        |               |                      |                              | _                                | + 100%  |
| READY 14  | OF 120 RECORD  | IS FOUND     | 1            |              |             |        |               |                      |                              |                                  | + 100%  |

Figure 18. Possible native Windows tools used by the adversary. (Lee, 2014, digital case files)

Executing one after the other are two suspicious files with randomly generated names (Figure 19).

| X  | <b>₽ 5</b> • ♂-     | <b>-</b> - |            | NROMANC                    | FF_Prefetch_R | esults.xlsx - Excel |   |                       | ? 📧 -        | - 🗆     |
|----|---------------------|------------|------------|----------------------------|---------------|---------------------|---|-----------------------|--------------|---------|
| E  | TLE HOME IN         | ISERT PA   | AGE LAYOUT | FORMULAS DATA REVIEW       | VIEW          |                     |   |                       |              |         |
| тс | OPLZAG 🔻 :          | X 🗸 .      | fx TOPLZ   | AGU.EXE                    |               |                     |   |                       |              |         |
| 4  | А                   | В          | С          | D                          |               | E                   |   | F                     | G            | F       |
| 1  | Date/Time           | Account -  | Computer 👻 | Description                | Ŧ             | Details             | - | Properties            | Miscellaneou | Artifac |
| 5  | 03/26/2012 04:00:00 | N/A        | NROMANOF   | WSQMCONS.EXE-E2CE6542.pf   |               | WSQMCONS.EXE        |   | Number of Time Run: 1 |              | Prefete |
| 6  | 03/29/2012 22:44:42 | N/A        | NROMANOF   | NAPRDMGR.EXE-55F08014.pf   |               | NAPRDMGR.EXE        |   | Number of Time Run: 2 |              | Prefete |
| 7  | 03/31/2012 17:18:51 | N/A        | NROMANOF   | SCRNSAVE.SCR-225A7D32.pf   |               | SCRNSAVE.SCR        |   | Number of Time Run: 1 | 2            | Prefete |
| 8  | 04/01/2012 05:00:02 | N/A        | NROMANOF   | SDIAGNHOST.EXE-67CD1457.pf |               | SDIAGNHOST.EXE      |   | Number of Time Run: 2 |              | Prefete |
| 9  | 04/01/2012 05:00:38 | N/A        | NROMANOF   | CSC.EXE-4EF173D0.pf        |               | CSC.EXE             |   | Number of Time Run: 4 |              | Prefete |
| 10 | 04/01/2012 05:00:38 | N/A        | NROMANOF   | CVTRES.EXE-419E4E46.pf     |               | CVTRES.EXE          |   | Number of Time Run: 4 |              | Prefete |
| 11 | 04/01/2012 14:17:38 | N/A        | NROMANOF   | ACRORD32.EXE-33939BD1.pf   |               | ACRORD32.EXE        |   | Number of Time Run: 4 |              | Prefeto |
| 12 | 04/03/2012 20:38:05 | N/A        | NROMANOF   | MMC.EXE-2E157AE5.pf        |               | MMC.EXE             |   | Number of Time Run: 1 |              | Prefeto |
| 13 | 04/03/2012 21:03:30 | N/A        | NROMANOF   | TOPLZAGU.EXE-4EFD8FD3.pf   |               | TOPLZAGU.EXE        |   | Number of Time Run: 1 |              | Prefet  |
| L4 | 04/03/2012 21:18:21 | N/A        | NROMANOF   | OSCMPGPK.EXE-DDCC6901.pf   |               | OSCMPGPK.EXE        |   | Number of Time Run: 1 |              | Prefet  |
| 15 | 04/03/2012 21:18:21 | N/A        | NROMANOF   | RUNDLL32.EXE-6706170E.pf   |               | RUNDLL32.EXE        |   | Number of Time Run: 2 |              | Prefeto |

Figure 19. Randomly generated file names. (Lee, 2014, digital case files)

Finally, there is a well-known artifact associated with the remote administrative command tool named PSEXEC by Microsoft. Administrators of the system could have used this tool to manage the system, but since it appears in our timeframe and may be an indication of lateral movement of the adversary, the keyword PSEXE will be added to our list to spot the 'Client' executable of PSEXEC.EXE and the 'Service' executable of PSEXESRV.EXE. Right below PSEXESRV.EXE is another artifact observed on workstation WKS-WINXP32BIT (but not noted), named SPINLOCK.EXE. Since this executable was run two minutes after PSEXEC and since the name of the file is not familiar to us, it will be added to the keyword list as well (Figure 20).

| x  | 🔒 🔊 🖓               | <b>–</b>  |              | NROMANOFF_Pref            | etch_F | esults.xlsx - Excel |                        | ? 🖅 —          |         |
|----|---------------------|-----------|--------------|---------------------------|--------|---------------------|------------------------|----------------|---------|
| F  | ILE HOME IN         | ISERT P.A | AGE LAYOUT   | FORMULAS DATA REVIEW VIEW |        |                     |                        |                |         |
| ps | exe_1 •             | ×         | $f_x$ psexes | VC.EXE                    |        |                     |                        |                | v       |
|    | А                   | В         | С            | D                         |        | E                   | F                      | G              | E e     |
| 1  | Date/Time           | Account - | Computer 👻   | Description               | -      | Details 🔹           | Properties 🔹           | Miscellaneou 👻 | Artifac |
| 62 | 04/04/2012 15:48:46 | N/A       | NROMANOF     | TASKLIST.EXE-9811F41E.pf  |        | TASKLIST.EXE        | Number of Time Run: 1  |                | Prefete |
| 63 | 04/04/2012 18:51:15 | N/A       | NROMANOF     | SVCHOST.EXE-CD257EB2.pf   |        | SVCHOST.EXE         | Number of Time Run: 1  |                | Prefete |
| 64 | 04/04/2012 18:52:11 | N/A       | NROMANOF     | PSEXESVC.EXE-51BA46F2.pf  |        | PSEXESVC.EXE        | Number of Time Run: 9  |                | Prefeto |
| 65 | 04/04/2012 18:54:51 | N/A       | NROMANOF     | SPINLOCK.EXE-1610A75A.pf  |        | SPINLOCK.EXE        | Number of Time Run: 16 |                | Prefet  |
| 66 | 04/04/2012 19:40:29 | N/A       | NROMANOF     | FIRETRAY.EXE-83604477.pf  |        | FIRFTRAY, FXF       | Number of Time Run: 3  |                | Prefeto |

Figure 20. The keyword list has two more files added to it. (Lee, 2014, digital case files)

Keywords run against the Autoruns output gives us two hits. One on PSEXESRV.EXE and one for C:\Windows\System32\dllhost\svchost.exe (Figure 21).

| 🗱 🔒 5 · C · 🗋 -                                       | NROMANOFF_Autorun       | ns_Results.xlsx - Excel |   | ? 📧 – 🗆 🗙                 |
|---|-------------------------|-------------------------|---|---------------------------|
| FILE HOME INSERT PAGE LAYOUT FORMULAS DA              | TA REVIEW VIEW          |                         |   |                           |
| dllhost_1 • : X v $f_x$ c:\windows\system32\dll       | host\svchost.exe        |                         |   | ~                         |
| A B C D   |                         | E                       | F                                       |                           |
| 1 Date Acc Computer Description                       | ▼ D                     | Details 💽               | Properties 🧊                            | Miscellaneous             |
| 194 N/A N/A NROMANOFF HKLM\SOFTWARE\Microsoft\Windd   | ws\CurrentVersion\Run - | svchost                 | c:\windows\system32\dllhost\svchost.exe | Launch String: c:\windows |
| 485 N/A N/A NROMANOFF HKLM\System\CurrentControlSet\S | ervices - PSEXESVC P    | sExec Service           | c:\windows\psexesvc.exe                 | Launch String: %SystemRo  |
| 762   |                         |                         |   |                           |

Figure 21. Two keyword hits on Autorun entries. (Lee, 2014, digital case files)

We find two additional hits when examining the Shellbag entries of user Vibranium (Figure 22).

| XI 🔒 🕤 🤄           | - 🗋 =         |              |                | viranium_NROMAONOFF_Shellbag_Results.xlsx - Excel |                | ?               | * - I       | × |
|--------------------|---------------|--------------|----------------|---|----------------|-----------------|-------------|---|
| FILE HOME          | INSERT PAG    | SE LAYOUT FC | RMULAS DAT     | A REVIEW VIEW                                     |                |                 |             |   |
| -                  | × 4 .         | C            |                |   |                |                 |             |   |
| E75 👻 🗄            | X 🗸 j         | x            |                |   |                |                 |             | ~ |
| A                  | В             | С            | D              | E   | F              | G               | н           | ۸ |
| 1 Date/Time        | ▼ Account ▼   | Computer 🛛 💌 | Description 💌  | Details   | 🖵 Properties 🔽 | Miscellaneous 💌 | Artifacts 👻 |   |
| 33 04/03/2012 23:3 | 8:38 viranium | NROMAONOFF   | First Accessed | My Computer\C:\Windows\System32\dllhost\          |                |                 | Shellbags   |   |
| 40 04/04/2012 02:2 | 3:59 viranium | NROMAONOFF   | Last Accessed  | My Computer\C:\Windows\System32\dllhost\          |                |                 | Shellbags   |   |
| 72                 |               |              |                |   |                |                 |             |   |
|                    |               |              |                |   |                |                 |             |   |



Running the keywords against the ShimCache entries yields several interesting artifacts. First, we see that C:\Windows\Temp\a.exe is executed 47 times in one hour. Next, we find an entry with a file name from our keyword list, but with a different file extension. Recall that we saw a suspicious file called WINCLIENT.REG. The keyword list contained only the word WINCLIENT as the search term. This shortened keyword produced a hit on WINCLIENT.EXE which we found in user Vibranium's download folder (Figure 23). This user account is the same one seen above accessing the C:\Windows\System32\dllhost\ directory which contained the WINCLIENT.REG file from before.

| ] 🖯 🏷 🖓 🗋 🗧               | NROMANOFF_ShimCache_Results.xlsx - Excel                                  | ? 📧                  | - 🗆                         |
|---------------------------|---|----------------------|-----------------------------|
| FILE HOME INSERT          | PAGE LAYOUT FORMULAS DATA REVIEW VIEW                                     |                      |                             |
| vinclient_1 🔹 🗄 📉         | / $f_x$ C:\Users\vibranium\Downloads\winclient.exe                        |                      |                             |
| AB                        | C D E   | F G                  | н                           |
| Date/Time J Acco          | Computer Description Details  | 🐨 Properties 💌 Misce | <ul> <li>Artifac</li> </ul> |
| 2 04/03/2012 21:03:23 N/A | NROMANOFF User ShimCache Entry C:\Windows\TopLZAGU.exe                    | Executed: True       | ShimC                       |
| 8 04/03/2012 21:11:07 N/A | NROMANOFf User ShimCache Entry C:\Windows\PSEXESVC.EXE                    | Executed: True       | ShimC                       |
| 04/03/2012 21:12:04 N/A   | NROMANOFF User ShimCache Entry C:\Windows\PSEXESVC.EXE                    | Executed: True       | Shim                        |
| 04/03/2012 21:13:07 N/A   | NROMANOFF User ShimCache Entry C:\Windows\PSEXESVC.EXE                    | Executed: True       | Shim                        |
| 04/03/2012 21:13:29 N/A   | NROMANOFf User ShimCache Entry C:\Windows\PSEXESVC.EXE                    | Executed: True       | Shim                        |
| 04/03/2012 21:14:56 N/A   | NROMANOFF User ShimCache Entry C:\Windows\PSEXESVC.EXE                    | Executed: True       | Shim                        |
| 04/03/2012 21:18:14 N/A   | NROMANOFF User ShimCache Entry C:\Windows\oSCMpGpk.exe                    | Executed: True       | Shim                        |
| 04/03/2012 21:19:52 N/A   | NROMANOFF User ShimCache Entry C:\Windows\PSEXESVC.EXE                    | Executed: True       | Shim                        |
| 04/03/2012 22:40:25 N/A   | NROMANOFF User ShimCache Entry c:\windows\system32\dllhost\svchost.exe    | Executed: True       | Shim                        |
| 04/03/2012 22:40:25 N/A   | NROMANOFF User ShimCache Entry C:\Users\vibranium\Downloads\winclient.exe | Executed: False      | Shim                        |
| 04/03/2012 22:53:39 N/A   | NROMANOFFUser ShimCache Entry C:\Windows\system32\spinlock.exe            | Executed: True       | Shim                        |
| 04/04/2012 01:00:45 N/A   | NROMANOFF User ShimCache Entry C:\windows\system32\hydrakatz.exe          | Executed: True       | Shim                        |
| 04/04/2012 01:46:37 N/A   | NROMANOFF User ShimCache Entry C:\Windows\PSEXESVC.EXE                    | Executed: True       | Shim                        |
| 2                         |   |                      |                             |
| System Shir               |   |                      |                             |
| ADY 13 OF 330 RECORDS FOU |   | ∎ <b>™ -</b>         | -+ 100                      |

*Figure 23. Winclient keyword hit. (Lee, 2014, digital case files)* 

Last, every entry from 04/03/2012 onward is a hit, except three files. Looking at these three files, they appear suspicious and are flagged (Figure 24).

| 🚺 🔒 🐬 👌 🗋 👳                            | NROMANOFF_ShimCache_Results.xtsx - Excel   | ? 📧                                   |                             |
|--|--|---------------------------------------|-----------------------------|
| FILE HOME INSERT                       | PAGE LAYOUT FORMULAS DATA REVIEW VIEW Suspicious Entries in Time F   | rame                                  |                             |
| TopLZAGU 👻 🗄 🗙 🐧                       | fx C:\Windows\TopLZAGU.exe   |                                       |                             |
| A B                                    | C D E  | F G                                   | н                           |
| Date/Time 🔹 Acco                       | Computer Description Justialis   | Properties 💌 Misce                    | <ul> <li>Artifac</li> </ul> |
| 68 03/16/2012 21:36:21 N/A             | NROMANOE"mCache Entry C:\Users\NROMAN~1\AppData\I ocal\Temp\AIR4C32.tmp\Adobe AIR Installer.exe              | Executed: True                        | ShimCa                      |
| 04/03/2012 18:08:50 IV/A               | MANOFF User ShimCache Enin C:\\$Recycle.Bin\S-1-5-21-2036804247-3058324640-2116585241-1673\\$RR3GW21.exe الم | Executed: False                       | ShimC                       |
| ) 04/03/2012 18:08:50 N/A              | NROMANOFI User ShimCache Entry C:\dllhot.exe   | Executed: True                        | ShimC                       |
| 1 04/03/2012 18:08:50 N/A              | NROMANOFF User ShimCache Entry C:\dllhost.exe  | Executed: True                        | ShimC                       |
| 2 04/03/2012 21:03:23 N/A              | NROMANOFF User ShimCache Entry C:\Windows\TopLZAGU.exe   | Executed: True                        | ShimC                       |
| 3 04/03/2012 21:11:07 N/A              | NROMANOFF User ShimCache Entry C:\Windows\PSEXESVC.EXE   | Executed: True                        | ShimC                       |
| 4 04/03/2012 21:12:04 N/A              | NROMANOFI User ShimCache Entry C:\Windows\PSEXESVC.EXE   | Executed: True                        | ShimC                       |
| 5 04/03/2012 21:13:07 N/A              | NROMANOFI User ShimCache Entry C:\Windows\PSEXESVC.EXE   | Executed: True                        | ShimC                       |
| 5 <mark>04/03/2012 21:13:29 N/A</mark> | NROMANOFI User ShimCache Entry C:\Windows\PSEXESVC.EXE   | Executed: True                        | ShimC                       |
| 7 04/03/2012 21:14:56 N/A              | NROMANOFI User ShimCache Entry C:\Windows\PSEXESVC.EXE   | Executed: True                        | ShimC                       |
| 8 <mark>04/03/2012 21:18:14 N/A</mark> | ······································   | Executed: True                        | ShimC                       |
| 9 <mark>04/03/2012 21:19:52 N/A</mark> |  | Executed: True                        | ShimC                       |
| 0 <mark>04/03/2012 22:40:25 N/A</mark> |  | Executed: True                        | ShimC                       |
| 1 04/03/2012 22:40:25 N/A              |  | Executed: False                       | ShimC                       |
| 2 04/03/2012 22:53:39 N/A              |  | Executed: True                        | ShimC                       |
| System_Shim                            | ÷ : •  |                                       | •                           |
| EADY 🔠                                 |  | • • • • • • • • • • • • • • • • • • • | <b>+</b> 100                |

Figure 24. Suspicious Entries found in the Time Frame. (Lee, 2014, digital case files)

Running the keywords against the MFT file shows us the paths of the artifacts of interest on this system (Figure 25).

|        |                                       | -            |             |               |   |                    |                    |
|--------|---------------------------------------|--------------|-------------|---------------|---|--------------------|--------------------|
| ×      | <b>. 5</b> , 9,                       | r 🗋 🜩        |             |               | NROMANOFF_MFT_Results.xlsx - Excel  | ? 📧 – 🗆            | = ×                |
| FILE   | HOME                                  | INSERT F     | PAGE LAYOUT | FORMULAS      | DATA REVIEW VIEW  |                    |                    |
|        | _                                     |              |             |               |   |                    |                    |
| sekur  | rlsa 1 🔻 🗄                            | XV           | fx \Win     | ndows\System  | 132\sekurisa.dll  |                    | ~                  |
|        |                                       |              |             |               | _   |                    |                    |
|        | A                                     | В            | С           | D             | E   |                    |                    |
| 1      | Date/Time                             |              |             | Descriptic 🔻  |   |                    | -                  |
| 114162 | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 |              |             |               |   | Create: 04/03/2012 |                    |
| 114166 | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 |              | NROMANO     | I Create Date | \Windows\Prefetch\PSEXESVC.EXE-51BA46F2.pf Std Info -                           | Create: 04/03/2012 | 21:                |
| 114167 | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 |              | NROMANO     | I Create Date | \Windows\oSCMpGpk.exe Std Info -  | Create: 04/03/2012 | 21:                |
| 114168 | 04/03/2012 2                          | 1:18:21 N/A  | NROMANO     | I Create Date | \Windows\Prefetch\OSCMPGPK.EXE-DDCC6901.pf Std Info -                           | Create: 04/03/2012 | 21:                |
| 114826 | 04/03/2012 2                          | 2:59:43 N/A  | NROMANO     | I Create Date | \Windows\System32\spinlock.exe Std Info -                                       | Create: 04/03/2012 | <mark>22:</mark>   |
| 114835 | 04/03/2012 2                          | 3:09:17 N/A  | NROMANO     | I Create Date | \Users\vibranium\AppData\Local\Temp\_MEI138842\spinlock.exe.manifest Std Info - | Create: 04/03/2012 | <mark>23:</mark>   |
| 114836 | 04/03/2012 2                          | 3:09:26 N/A  | NROMANO     | I Create Date | \Windows\Prefetch\SPINLOCK.EXE-1610A75A.pf Std Info -                           | Create: 04/03/2012 | <mark>23:</mark>   |
| 114843 | 04/03/2012 2                          | 3:54:46 N/A  | NROMANO     | I Create Date | \Windows\Temp\a.exe Std Info -  | Create: 04/03/2012 | <mark>23:</mark>   |
| 114844 | 04/03/2012 2                          | 3:54:48 N/A  | NROMANO     | I Create Date | \Windows\Prefetch\A.EXE-8D56B1C4.pf Std Info -                                  | Create: 04/03/2012 | 23:                |
| 114856 | 04/04/2012 0                          | 0:01:45 N/A  | NROMANO     | I Create Date | \Users\vibranium\AppData\Local\Temp\_MEI57722\spinlock.exe.manifest Std Info -  | Create: 04/04/2012 | . <mark>00:</mark> |
| 114866 | 04/04/2012 0                          | 0:06:41 N/A  | NROMANO     | I Create Date | \Users\vibranium\AppData\Local\Temp\_MEI111242\spinlock.exe.manifest Std Info - | Create: 04/04/2012 | 00:                |
| 114877 | 04/04/2012 0                          | 1:00:07 N/A  | NROMANO     | I Create Date | \Windows\System32\hydrakatz.exe Std Info -                                      | Create: 04/04/2012 | 01:                |
| 114878 | 04/04/2012 0                          | 1:01:15 N/A  | NROMANO     | I Create Date | \Windows\System32\pe.exe Std Info -   | Create: 04/04/2012 | 01:                |
| 114879 | 04/04/2012 0                          | 1:02:10 N/A  | NROMANO     | I Create Date | \Windows\System32\sekurlsa.dll Std Info -                                       | Create: 04/04/2012 | 01:                |
| 114880 | 04/04/2012 0                          | 1.09.03 N/A  | NROMANO     | Create Date   | \Windows\Prefetch\HYDRAKAT7 FXF-A0DADA85 nf                                     | Create: 04/04/2012 | 01.                |
|        | → MF                                  | T_NRomanof   | f 🕂         |               |   |                    | ▶                  |
| READY  | 22 OF 115585 F                        | RECORDS FOUN | ID 🔚        |               | ₩ <b>0 1</b>  | + 1                | 100%               |
|        |                                       |              |             |               |   |                    |                    |

Figure 25. File paths for keyword hits. (Lee, 2014, digital case files)

Running the keywords against the Application Event Viewer log produced two hits (Figure 26).

| XI    | <b>5</b> • 0 | ⇒ 🗋 ∓      |                 | High                            | lighted_NROMAN | IOFF_Application_XML_Standard_Results.xlsx - Excel |                                   | ? 🖻 – 🗆 X             |
|-------|--------------|------------|-----------------|---------------------------------|----------------|--|-----------------------------------|-----------------------|
| FILE  | HOME         | INSERT     | PAGE LAYOUT     | FORMULAS [                      | DATA REVIEW    | / VIEW   |                                   |                       |
| E1358 | 87 -         | : X v      | fx              |                                 |                |  |                                   |                       |
|       | А            |            | B C             | D                               | E              | F  | G                                 | н                     |
| 1     | Date/Time    | Accord     | ount 🔻 Computer | <ul> <li>Description</li> </ul> | 🔻 Details 👻    | Properties   | T Miscellaneous                   | Artifact 💌            |
| 12985 | 04/04/2012   | 01:18:15 - | NROMANO         | F Application E                 | irror -        | c:\windows\system32\dllhost\svchost.exe            | Evt ID: 1000   Evt Record #: 6103 | Application Event Log |
| 12986 | 04/04/2012   | 01:18:15 - | NROMANO         | F Application E                 | rror -         | c:\windows\system32\dllhost\svchost.exe            | Evt ID: 1000   Evt Record #: 6103 | Application Event Log |
| 13581 |              |            |                 |                                 |                |  |                                   |                       |

Figure 26. The keyword hits in the Application Event Viewer log. (Lee, 2014, digital case files)

| FILEHOMEINSERTPAGE LAYOUTFORMULASDATAREVIEWVIEW225157Image: Compute DescriptionDetailsImage: Compute DescriptionDetailsImage: Compute DescriptionDetailsImage: Compute DescriptionDetailsImage: Compute DescriptionDetailsImage: Compute DescriptionImage: Compute DescriptionImage: Compute DescriptionDetailsImage: Compute DescriptionImage: Compute DescriptionImage   |                    |          |           |      |                  |              |  |             |                      |               |                     |
|--|--------------------|----------|-----------|------|------------------|--------------|--|-------------|----------------------|---------------|---------------------|
| $ \begin{array}{c c c c c c c c c c c c c c c c c c c $  | XII.               | 5-       | ¢ - [     | _] ≐ |                  |              | Highlighted_NROMANOFF_Security_EventLog_XML_Standard_Format.xlsx - Excel |             |                      | ? 🗹 –         |                     |
| A       B       C       D       E       G         1       Date/Time       \[Adv]       Computer       Descriptior       Details       \[Adv]       ProcessNam Evt ID: 4625       Evt Record #: 526080 Se         168       04/03/2012 21:12:07       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526080 Se         228       04/03/2012 21:12:07       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526080 Se         320       04/03/2012 21:13:29       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526097 Se         59       04/03/2012 21:13:29       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 52607 Se         59       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526101 Se         539       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 526101 Se         539       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 527370 Se         730       04/05/2012 05:19:11       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 16464   | FILE               | HOM      | IE INS    | SERT | PAGE LAYO        | UT FORMUL    | AS DATA REVIEW VIEW  |             |                      |               |                     |
| A       B       C       D       E       G         1       Date/Time       \[Adv]       Computer       Descriptior       Details       \[Adv]       ProcessNam Evt ID: 4625       Evt Record #: 526080 Se         168       04/03/2012 21:12:07       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526080 Se         228       04/03/2012 21:12:07       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526080 Se         320       04/03/2012 21:13:29       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526097 Se         59       04/03/2012 21:13:29       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 52607 Se         59       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526101 Se         539       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 526101 Se         539       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 527370 Se         730       04/05/2012 05:19:11       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 16464   |                    |          |           |      |                  |              |  |             |                      |               |                     |
| 1       Date/Time       A       Computé < Descriptiof < Details       Image: Computé < Miscellaneous       Ar         168       04/03/2012 21:11:08       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526080 5e         249       04/03/2012 21:12:07       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526080 5e         230       04/03/2012 21:13:09       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526097 5e         230       04/03/2012 21:13:29       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526102 5e         230       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526102 5e         230       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526102 5e         230       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4642       Evt Record #: 526102 5e         230       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4644       Evt Record #: 527370 5e         230       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       Proce   | E2515              | 7 -      | : >       | < 🗸  | f <sub>x</sub> 0 | xc000006d    |  |             |                      |               |                     |
| 1       Date/Time       A       Computé < Descriptiof < Details       Image: Computé < Miscellaneous       Ar         168       04/03/2012 21:11:08       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526080 5e         249       04/03/2012 21:12:07       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526080 5e         230       04/03/2012 21:13:09       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526097 5e         230       04/03/2012 21:13:29       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526102 5e         230       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526102 5e         230       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526102 5e         230       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4642       Evt Record #: 526102 5e         230       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4644       Evt Record #: 527370 5e         230       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       Proce   |                    |          |           |      |                  | -            |  |             |                      | _             |                     |
| 168       04/03/2012 21:11:08       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526086 Se         248       04/03/2012 21:12:07       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526086 Se         320       04/03/2012 21:13:29       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526097 Se         320       04/03/2012 21:13:29       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526097 Se         430       04/03/2012 21:13:29       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526111 Se         539       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526110 Se         539       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 526107 Se         530       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 527370 Se         730       04/05/2012 05:19:11       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       Application Evt ID: 5156       Evt Record #: 527370 Se         751       04/05/2012 05:19:11       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC   |                    | 4        | 4         | -    | С                |              |  | F           |                      | 3             | _                   |
| 248       04/03/2012 21:12:07       NROMANO! Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526092 Se         230       04/03/2012 21:13:08       NROMANO! Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526092 Se         375       04/03/2012 21:13:08       NROMANO! Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526092 Se         470       04/03/2012 21:13:05       NROMANO! Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526101 Se         530       04/03/2012 21:19:33       NROMANO! Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526101 Se         539       04/03/2012 21:19:33       NROMANO! Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 46484       Evt Record #: 526101 Se         539       04/03/2012 21:19:33       NROMANO! Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 52710 Se         530       04/03/2012 21:19:33       NROMANO! Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 527370 Se         730       04/05/2012 05:19:11       NROMANO! Microsoft-Wii C:\Windows\PSEXESVC.EXE       Application Evt ID: 5156       Evt Record #: 527367 Se         710       04/05/2012 05:19:11       NROMANO! Microsoft-Wii C:\Windows\PSEXESVC   |                    |          |           |      | • •              |              |  | • •         |                      |               |                     |
| 320       04/03/2012 21:13:08 -       NROMANOI Microsoft-Wii C;Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526092 Se         325       04/03/2012 21:13:09 -       NROMANOI Microsoft-Wii C;Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526012 Se         329       04/03/2012 21:13:09 -       NROMANOI Microsoft-Wii C;Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4625       Evt Record #: 526012 Se         329       04/03/2012 21:19:53 -       NROMANOI Microsoft-Wii C;Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526102 Se         539       04/03/2012 21:19:53 -       NROMANOI Microsoft-Wii C;Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526102 Se         539       04/03/2012 21:19:53 -       NROMANOI Microsoft-Wii C;Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 5273010 Se         730       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii ; device\harddiskvolume1\windows\system32\dilhost\svchost.exe       Application Evt ID: 5156       Evt Record #: 5273070 Se         761       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii ; device\harddiskvolume1\windows\system32\dilhost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527307 Se         771       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii ; device\harddiskvolume1\windows\system32\dilhost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527367 Se<   |                    |          |           |      |                  |              |  |             |                      |               |                     |
| 375       04/03/2012 21:13:29       NROMANO! Microsoft-Wir C:\Windows\PSEXESVC.EXE       ProcessNam Evt 10: 4625       Evt Record #: 526097 Set         430       04/03/2012 21:13:53       NROMANO! Microsoft-Wir C:\Windows\PSEXESVC.EXE       ProcessNam Evt 10: 4625       Evt Record #: 526102 Set         550       04/03/2012 21:19:53       NROMANO! Microsoft-Wir C:\Windows\PSEXESVC.EXE       ProcessNam Evt 10: 4624       Evt Record #: 526109 Set         553       04/03/2012 21:19:53       NROMANO! Microsoft-Wir C:\Windows\PSEXESVC.EXE       ProcessNam Evt 10: 4624       Evt Record #: 526109 Set         553       04/03/2012 21:19:53       NROMANO! Microsoft-Wir C:\Windows\PSEXESVC.EXE       ProcessNam Evt 10: 4624       Evt Record #: 526109 Set         720       04/05/2012 05:19:11       NROMANO! Microsoft-Wir C:\Windows\PSEXESVC.EXE       ProcessNam Evt 10: 5156       Evt Record #: 527309 Set         721       04/05/2012 05:19:11       NROMANO! Microsoft-Wir \device\harddiskvolume1\windows\system32\dlihost\svchost.eve       Application Evt 10: 5156       Evt Record #: 527309 Set         721       04/05/2012 05:19:11       NROMANO! Microsoft-Wir \device\harddiskvolume1\windows\system32\dlihost\svchost.eve       Application Evt 10: 5156       Evt Record #: 527369 Set         721       04/05/2012 05:19:11       NROMANO! Microsoft-Wir \device\harddiskvolume1\windows\system32\dlihost\svchost.eve       Application Evt 10: 5156       Evt Record #: 527367 Set  |                    |          |           |      | NROMANC          | Microsoft-Wi | C:\Windows\PSEXESVC.EXE  | ProcessNan  | n Evt ID: 4625   Evt | Record #: 526 | 086 Se              |
| 130       04/03/2012 21:14:56 -       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4622       Evt Record #: 526102 Se         130       04/03/2012 21:19:35 -       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526110 Se         130       04/03/2012 21:19:35 -       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526110 Se         130       04/05/2012 21:19:35 -       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 526100 Se         130       04/05/2012 21:19:35 -       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 527370 Se         130       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dllhost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527369 Se         14       V       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5156       Evt Record #: 527369 Se         1777       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5156       Evt Record #: 527369 Se         1777       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158  | 320 <mark>0</mark> | 4/03/201 | 2 21:13:0 | 8 -  | NROMANC          | Microsoft-Wi | C:\Windows\PSEXESVC.EXE  | ProcessNan  | n Evt ID: 4625   Evt | Record #: 526 | 092 Se              |
| 119       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526110 Se         539       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 526110 Se         539       04/03/2012 21:19:53       NROMANOI Microsoft-Wii C:\Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 526110 Se         730       04/05/2012 05:19:11       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dllhost\svchost.exe       Application Evt ID: 5158       Evt Record #: 52730 Se         730       04/05/2012 05:19:11       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dllhost\svchost.exe       Application Evt ID: 5156       Evt Record #: 52730 Se         751       04/05/2012 05:19:11       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dllhost\svchost.exe       Application Evt ID: 5156       Evt Record #: 52730 Se         752       04/05/2012 05:19:11       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dllhost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527367 Se         752       04/05/2012 05:19:11       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158       Evt Record #: 527367 Se         777       04/05/2012 05:19:11       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\ap   | 375 <mark>0</mark> | 4/03/201 | 2 21:13:2 | 9 -  | NROMANC          | Microsoft-Wi | C:\Windows\PSEXESVC.EXE  | ProcessNan  | n Evt ID: 4625   Evt | Record #: 526 | <mark>097 Se</mark> |
| 339       04/03/2012 21:19:53 -       NROMANOI Microsoft-Wii C;Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4624       Evt Record #: 526110 Se         539       04/03/2012 21:19:53 -       NROMANOI Microsoft-Wii C;Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 526110 Se         730       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dllhost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527370 Se         731       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dllhost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527370 Se         751       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dllhost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527367 Se         751       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5156       Evt Record #: 527367 Se         777       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5156       Evt Record #: 527367 Se         777       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158       Evt Record #: 527367 Se         7777       04/05/2012 05:19:11 - <td< td=""><td>430 <mark>0</mark></td><td>4/03/201</td><td>2 21:14:5</td><td>6 -</td><td>NROMANC</td><td>Microsoft-Wi</td><td>C:\Windows\PSEXESVC.EXE</td><td>ProcessNan</td><td>n Evt ID: 4625   Evt</td><td>Record #: 526</td><td>102 Se</td></td<> | 430 <mark>0</mark> | 4/03/201 | 2 21:14:5 | 6 -  | NROMANC          | Microsoft-Wi | C:\Windows\PSEXESVC.EXE  | ProcessNan  | n Evt ID: 4625   Evt | Record #: 526 | 102 Se              |
| 553       04/03/2012 21:19:53 -       NROMANOI Microsoft-Wii Cl;Windows\PSEXESVC.EXE       ProcessNam Evt ID: 4648       Evt Record #: 526109 Set         720       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii Clevice\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527309 Set         721       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii Clevice\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527309 Set         7261       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii Clevice\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527369 Set         7270       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii Clevice\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527369 Set         7277       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii Clevice\harddiskvolume1\windows\system32\ullibast\svchost.exe       Application Evt ID: 5156       Evt Record #: 527369 Set         7277       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii Clevice\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158       Evt Record #: 527369 Set         7333  | 519 <mark>0</mark> | 4/03/201 | 2 21:19:5 | 3 -  | NROMANC          | Microsoft-Wi | C:\Windows\PSEXESVC.EXE  | ProcessNan  | n Evt ID: 4624   Evt | Record #: 526 | 111 Se              |
| 730       04/05/2012 05:19:11 -       NROMANO! Microsoft-Wii \device\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527369 Se         731       04/05/2012 05:19:11 -       NROMANO! Microsoft-Wii \device\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527369 Se         751       04/05/2012 05:19:11 -       NROMANO! Microsoft-Wii \device\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527369 Se         764       04/05/2012 05:19:11 -       NROMANO! Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5156       Evt Record #: 527369 Se         777       04/05/2012 05:19:11 -       NROMANO! Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158       Evt Record #: 527369 Se         777       04/05/2012 05:19:11 -       NROMANO! Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158       Evt Record #: 527369 Se         773       04/05/2012 05:19:11 -       NROMANO! Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158       Evt Record #: 527369 Se         773       04/05/2012 05:19:11 -       NROMANO! Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158       Evt Record #: 52736 Se   | 539 0              | 4/03/201 | 2 21:19:5 | 3 -  | NROMANC          | Microsoft-Wi | C:\Windows\PSEXESVC.EXE  | ProcessNan  | n Evt ID: 4624   Evt | Record #: 526 | 110 Se              |
| 743       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5158       Evt Record #: 527369 Se         751       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527369 Se         764       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5156       Evt Record #: 527367 Se         777       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158       Evt Record #: 527367 Se         933  | 553 0              | 4/03/201 | 2 21:19:5 | 3 -  | NROMANC          | Microsoft-Wi | C:\Windows\PSEXESVC.EXE  | ProcessNan  | n Evt ID: 4648   Evt | Record #: 526 | 109 Se              |
| 743       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5158       Evt Record #: 527369 Se         751       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5158       Evt Record #: 527369 Se         764       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158       Evt Record #: 527367 Se         777       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158       Evt Record #: 527367 Se         933  | 730 0              | 4/05/201 | 2 05:19:1 | 1 -  | NROMANC          | Microsoft-Wi | \device\harddiskvolume1\windows\system32\dllhost\svchost.exe             | Application | Evt ID: 5156   Evt   | Record #: 527 | 370 Se              |
| 751       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\windows\system32\dlihost\svchost.exe       Application Evt ID: 5156       Evt Record #: 527368 Set         764       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5156       Evt Record #: 527367 Se         777       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application Evt ID: 5158       Evt Record #: 527367 Se         933  | 743 0              | 4/05/201 | 2 05:19:1 | 1 -  |                  |              |  |             |                      |               |                     |
| 764       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application       Evt Record #: 527367 Set         777       04/05/2012 05:19:11 -       NROMANOI Microsoft-Wii \device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application       Evt Record #: 527366 Set         933  |                    |          |           |      |                  |              |  |             |                      |               |                     |
| Od/05/2012 05:19:11 -       NROMANO! Microsoft-Wir\device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe       Application       Evt Record #: 527366       See         933  |                    |          |           |      |                  |              |  |             |                      |               |                     |
| 933<br>q34<br>← → Sheet1 Sheet3 ⊕ : 4  |                    |          |           |      |                  |              |  |             |                      |               |                     |
| G34  | 933                |          |           |      |                  |              |  |             |                      |               |                     |
| Sheet1     Sheet3     Image: Head of the sheet3  | 934                |          |           |      |                  |              |  |             |                      |               |                     |
|  |                    | •        | Sheet1    | She  | eet2 Shee        | et3 (+)      | : 4  |             |                      |               | Þ                   |
|  | EADY               | 13 OF 63 | ARECOR    |      | JND 🔚            |              |  | Ħ           | B M                  |               | + 1009              |

The Security Event Viewer log has several keywords in it (Figure 27).

Figure 27. The keyword hits in the Security Event Viewer log. (Lee, 2014, digital case files)

#### And finally, the System Event Viewer log has a bunch of hits (Figure 28).

| X∎    | 🗄 🕤 d        | • - D   | Ŧ           |                    | Highlighted      | NROMA  | NOFF_System_EventLog_XML_Standard_Format.xlsx - Excel      |                | ? 📧 🗕               |       |
|-------|--------------|---------|-------------|--------------------|------------------|--------|--|----------------|---------------------|-------|
| FILE  | E HOME       | INSE    | RT PAGE     | LAYOUT FOR         | RMULAS DATA      | RE     | VIEW VIEW  |                |                     |       |
|       |              |         |             |                    |                  |        |  |                |                     |       |
| dllh  | ost_1 💌      | : 🗙     | s fx        | c:\windows         | system32\cmd     | .exe/k | c:\windows\system32\dllhost\svchost.exe                    |                |                     |       |
|       |              | _       | -           | -                  | _                | _      | -  |                | _                   |       |
|       | A            |         | В           | C                  | D                | E      | P  |                | G                   |       |
| 1     | Date/Time    | -       | Account     | Computer *         | Description 💌    | Deta 🔻 | Properties   | Miscellaneo    | us 🔹                | Artif |
| 8882  | 04/03/2012 2 | 1:03:27 | S-1-5-21-20 | <b>36 NROMANOF</b> | FService Control | -      | %SYSTEMROOT%\TopLZAGU.exe                                  | Evt ID: 7045   | Evt Record #: 14789 | Syste |
| 8899  | 04/03/2012 2 | 1:11:07 | S-1-5-21-20 | B6 NROMANOF        | FService Control | -      | %SystemRoot%\PSEXESVC.EXE                                  | Evt ID: 7045   | Evt Record #: 14794 | Syste |
| 8910  | 04/03/2012 2 | 1:12:04 | S-1-5-21-20 | B6 NROMANOF        | FService Control | -      | %SystemRoot%\PSEXESVC.EXE                                  | Evt ID: 7045   | Evt Record #: 14797 | Syste |
| 3924  | 04/03/2012 2 | 1:13:08 | S-1-5-21-20 | B6 NROMANOF        | FService Control | -      | %SystemRoot%\PSEXESVC.EXE                                  | Evt ID: 7045   | Evt Record #: 14800 | Syste |
| 3935  | 04/03/2012 2 | 1:13:29 | S-1-5-21-20 | B6 NROMANOF        | FService Control | -      | %SystemRoot%\PSEXESVC.EXE                                  | Evt ID: 7045   | Evt Record #: 14803 | Syste |
| 3946  | 04/03/2012 2 | 1:14:56 | S-1-5-21-20 | B6 NROMANOF        | FService Control | -      | %SystemRoot%\PSEXESVC.EXE                                  | Evt ID: 7045   | Evt Record #: 14806 | Syste |
| 3952  | 04/03/2012 2 | 1:18:18 | S-1-5-21-20 | B6 NROMANOF        | FService Control | -      | %SYSTEMROOT%\oSCMpGpk.exe                                  | Evt ID: 7045   | Evt Record #: 14809 | Syste |
| 3966  | 04/03/2012 2 | 1:19:53 | S-1-5-21-20 | B6 NROMANOF        | FService Control | -      | %SystemRoot%\PSEXESVC.EXE                                  | Evt ID: 7045   | Evt Record #: 14813 | Syste |
| 9071  | 04/03/2012 2 | 3:52:47 | S-1-5-21-20 | B6 NROMANOF        | FService Control | -      | c:\windows\system32\cmd.exe /k c:\windows\system32\dllhost | s Evt ID: 7045 | Evt Record #: 14848 | Syste |
| 9092  | 04/04/2012 0 | 0:07:23 | S-1-5-21-20 | 36 NROMANOF        | FUSER32          | -      | spinlock.exe   | Evt ID: 1074   | Evt Record #: 14856 | Syste |
| .0485 | 04/04/2012 1 | 8:52:11 | S-1-5-21-20 | 36 NROMANOF        | FService Control | -      | %SystemRoot%\PSEXESVC.EXE                                  | Evt ID: 7045   | Evt Record #: 15316 | Syste |
| 0904  |              |         |             |                    |                  |        |  |                |                     |       |

Figure 28. The keyword hits in the System Event Viewer log. (Lee, 2014, digital case files)

Examining the Event Viewer logs using Event IDs instead of keywords, also yields some information that was not previously known. Pivoting on Event ID 5156 ("The Windows Filtering Platform has permitted a connection") shows an outbound connection from one of the suspicious executables to IP address 12.190.135.235 (Figure 29). This address will be added to the keyword list and possibly added to the company's network devices to log or block any connections still going to this location.

|                  |  |       |          |          | _     |    |   |                      |              |               |
|------------------|--|-------|----------|----------|-------|----|---|----------------------|--------------|---------------|
| 🛛 🖯 🕤            | ▶ < C = Divot_NROMANOFF_Security_EventLog_XML_Standard_Format                          | .xlsx | PIVOTTAB | LE TOOLS |       |    |   |                      | ? 街 –        | • ×           |
| FILE H           | HOME INSERT PAGE LAYOUT FORMULAS DATA REVIEW   | VIEW  | ANALYZE  | DESIGN   |       |    |   |                      |              |               |
| A58              | • : $\times \int f_x$ LayerRTID   -  |       |          |          |       |    |   |                      |              | v             |
|                  | А  | В     | С        | D        | E     | F  |   |                      |              |               |
| 44 🗆 Evt ID:     | : 5156   |       |          |          |       |    |   | PivotTable F         | ields        | - ×           |
| 46 \d            | lication   -<br>device\harddiskvolume1\users\vibranium\appdata\local\temp\a.exe        |       |          |          |       |    |   | Choose fields to add | to report:   | -\$} <b>v</b> |
| 48 Dest          | device\harddiskvolume1\windows\system32\dllhost\svchost.exe tAddress   - 2.190.135.235 |       |          |          |       |    |   | Date/Time            |              | *<br>*        |
| 50 12            | 27.0.0.1   |       |          |          |       |    |   | Drag fields between  | areas below: |               |
|                  | 2924   |       |          |          |       |    |   | ▼ FILTERS            | COLUN        | INS           |
| 53 <b>56</b>     | 578  | 000   |          |          |       |    |   |                      |              |               |
| 54 80            |  | Net   | work     | Conn     | ectio | ns |   |                      |              |               |
|                  | ection   -   |       |          |          |       |    |   | ROWS                 | Σ VALUES     | \$            |
|                  | erRTID   -   |       |          |          |       |    |   | Miscellan •          | ~ VALUE.     | ,             |
|                  | erName -   |       |          |          |       |    |   | Properties V         |              |               |
|                  | erRTID   -   |       |          |          |       |    |   | Properties •         |              |               |
| 59 <b>+ Proc</b> | Sheet4 Sheet1 Sheet2 Sheet3 +  | :     |          |          |       |    | • | Defer Layout Upo     | late         | UPDATE        |
| READY CALC       | CULATE 🔠   |       |          |          |       |    | Ħ | ▣ ॻ                  | ++           | <b>-</b> 100% |
|                  |  |       |          |          |       |    |   |                      |              |               |

Figure 29. Outbound connection. (Lee, 2014, digital case files)

Examining the Event IDs in the CSV output of the Event Viewer Security log shows us some other activity that could be related to the intrusion. First, we filter on Event ID 4624 ("An account was successfully logged on") Type 10 ("RemoteInteractive"), which shows us possible lateral movement using the Remote Desktop protocol (Figure 30).

| X∎  | 🖯 🎝 - 🗟 - 🗋         | ÷            |               | NROMANOFF_Security_EventLog_CSV_Export.xlsx | - Excel                     | PP-0-P-        | TIME            | ? 🗹 – 🗆            |
|-----|---------------------|--------------|---------------|---|-----------------------------|----------------|-----------------|--------------------|
| FIL | E HOME INSE         | RT PAGE LA   | YOUT FORM     | JLAS DATA REVIEW VIEW                       | Possi                       | ble Latel      | ral Moven       | nent               |
| D26 | i95 - : 🗙           | ✓ fx         | An account wa | s successfully logged on.                   |                             |                |                 |                    |
|     | А                   | В            | С             | D   | F                           | F              | G               | Н                  |
| 1   | Date/Time 🔹         | Account 💌    | Computer 💌    | Description                                 | <ul> <li>Details</li> </ul> | Properties 🛛 💌 | Miscellaneous J | Artifact           |
|     | 04/03/2012 20:37:40 |              | NROMANOFF     | An account was successfully logged on.      | 10.3.58.4                   | ogon Type: 10  | Evt ID: 4624    | Security Event Log |
| 569 | 04/03/2012 20:47:39 | nromanoff    | NROMANOFF     | An account was successfully logged on.      | 10.3.16.5                   | ogon Type: 10  | Evt ID: 4624    | Security Event Log |
| 695 | 04/03/2012 22:08:05 | vibranium    | NROMANOFF     | An account was successfully logged on.      | 10.3.58.7                   | ogon Type: 10  | Evt ID: 4624    | Security Event Log |
| 696 | 04/03/2012 22:08:05 | vibranium    | NROMANOFF     | An account was successfully logged on.      | 10.3.58.7                   | ogon Type: 10  | Evt ID: 4624    | Security Event Log |
| 063 | 04/04/2012 02:03:59 | nromanoff    | NROMANOFF     | An account was successfully logged on.      | 10.3.16.5                   | ogon Type: 10  | Evt ID: 4624    | Security Event Log |
| 103 | 04/04/2012 02:17:48 | vibranium    | NROMANOFF     | An account was successfully logged on.      | 10.3.58.7                   | ogon Type: 10  | Evt ID: 4624    | Security Event Log |
| 104 | 04/04/2012 02:17:48 | vibranium    | NROMANOFF     | An account was successfully logged on.      | 10.3.58.7                   | ogon Type: 10  | Evt ID: 4624    | Security Event Log |
| 167 | 04/04/2012 03:31:50 | rsydow       | NROMANOFF     | An account was successfully logged on.      | 10.3.58.4                   | ogon Type: 10  | Evt ID: 4624    | Security Event Log |
| 168 | 04/04/2012 03:31:50 | rsydow       | NROMANOFF     | An account was successfully logged on.      | 10.3.58.4                   | .ogon Type: 10 | Evt ID: 4624    | Security Event Log |
| 293 | 04/04/2012 12:20:42 | rsydow       | NROMANOFF     | An account was successfully logged on.      | 10.3.58.4                   | ogon Type: 10  | Evt ID: 4624    | Security Event Log |
| 294 | 04/04/2012 12:20:42 | rsydow       | NROMANOFF     | An account was successfully logged on.      | 10.3.58.4                   | ogon Type: 10  | Evt ID: 4624    | Security Event Log |
| 330 | 04/04/2012 12:29:11 | SRL-Helpdesk | NROMANOFF     | An account was successfully logged on.      | 10.3.58.4                   | .ogon Type: 10 | Evt ID: 4624    | Security Event Log |
| 331 | 04/04/2012 12:29:11 | SRL-Helpdesk | NROMANOFF     | An account was successfully logged on.      | 10.3.58.4                   | .ogon Type: 10 | Evt ID: 4624    | Security Event Log |
| 479 | 04/04/2012 12:42:03 | SRL-Helpdesk | NROMANOFF     | An account was successfully logged on.      | 10.3.58.4                   | .ogon Type: 10 | Evt ID: 4624    | Security Event Log |
| 480 | 04/04/2012 12:42:03 |              | NROMANOFE     | An account was successfully logged on       | 10 3 58 4                   | ogon Tyne: 10  | Evt ID: 4624    | Security Event Log |
| 4   | Security            | +            |               |   | : •                         |                |                 | Þ                  |
| FAD | y 35 OF 6184 RECORD | S FOUND      |               |   |                             | Ħ              | III             | + 100              |



Next, we apply a filter on Event IDs 4717, 4724, 4732, 4733, and 4738. These Event IDs relate to changes made to user accounts. The results of the filter show activity by account RSYDOW against account SRL-Helpdesk (Figure 31).

| X∎   | <b>□ 5</b> · ♂ □    | ) ÷                  |                | NROMANOFF Security EventLog CSV Export.xlsx               | - Excel                     | ? 📧                          | 1 - 0       | ×  |
|------|---------------------|----------------------|----------------|---|-----------------------------|------------------------------|-------------|----|
| FIL  | _                   | ERT PA               | AGE LAYOUT     | FORMULAS DATA REVIEW VIEW                                 |                             |                              |             |    |
| F61  | 90 - : >            | $\langle \checkmark$ | f <sub>x</sub> |   |                             |                              |             | v  |
|      | А                   | В                    | С              | D   | E                           | F                            | G           | 4  |
| 1    | Date/Time           | Accou 👻              | Computer 💌     | Description   | Details 💌                   | Properties 🔹                 | Miscellan   | e  |
| 2531 | 04/03/2012 20:26:18 | rsydow               | NROMANOFF      | A member was added to a security-enabled local group.     | BUILTIN\Administrators      | Target Account: SRL-Helpdesk | Evt ID: 473 | 12 |
| 2532 | 04/03/2012 20:26:18 | rsydow               | NROMANOFF      | A member was removed from a security-enabled local group. | BUILTIN\Users               | Target Account: SRL-Helpdesk | Evt ID: 473 | в  |
| 2533 | 04/03/2012 20:26:18 | rsydow               | NROMANOFF      | A member was removed from a security-enabled local group. | BUILTIN\Administrators      | Target Account: SRL-Helpdesk | Evt ID: 473 | в  |
| 2561 | 04/03/2012 20:40:38 | SYSTEM               | NROMANOFF      | System security access was granted to an account.         | SeRemoteInteractiveLogon    | Target Account: Everyone     | Evt ID: 471 | 7  |
| 3314 | 04/04/2012 12:22:15 | rsydow               | NROMANOFF      | An attempt was made to reset an account's password.       |                             | Target Account: SRL-Helpdesk | Evt ID: 472 | 4  |
| 3315 | 04/04/2012 12:22:15 | rsydow               | NROMANOFF      | A user account was changed.                               | Password Last Set: 4/4/2012 | Target Account: SRL-Helpdesk | Evt ID: 473 | 8  |
| 3466 | 04/04/2012 12:35:57 | rsydow               | NROMANOFF      | An attempt was made to reset an account's password.       |                             | Target Account: SRL-Helpdesk | Evt ID: 472 | 4  |
| 3467 | 04/04/2012 12:35:57 | rsydow               | NROMANOFF      | A user account was changed.                               | Password Last Set: 4/4/2012 | Target Account: SRL-Helpdesk | Evt ID: 473 | 8  |
| 6186 |                     |                      |                |   |                             |                              |             |    |



Finally, examining the System Event Viewer log by Event ID produces several more keywords. The Event ID filtered on is 7045 ("A service was installed in the system"). This filter shows us hits on several suspicious executables that we've already seen, but also provides us with unique Service Names of Mys, winsvchost, and MqlXmtLRaYQDMsvljY (Figure 32). We added these three new terms to the keyword list.

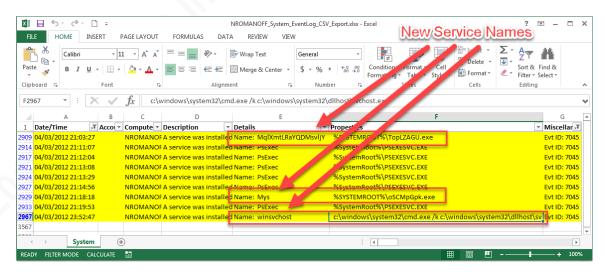


Figure 32. The keyword list has Service names added to it. (Lee, 2014, digital case files)

### 5.1.3. Win7-64-NFURRY (WKS-WIN764BITB)

Running our keyword list against workstation WKS-WIN764BITB (10.3.58.6) Autorun entries shows us Scheduled Tasks that run two of the suspicious executables that we have seen on other machines on this network (Figure 33).

| KII → ↔ □<br>FILE HOME INSE                      |                       | NFUR<br>FORMULAS DATA REVIEW | Y_Autoruns_Results.xlsx - Excel<br>VIEW | Scheduled Tasks   | ? 🗹 — 🗆                              | ×   |
|--|-----------------------|------------------------------|---|---|--------------------------------------|-----|
| Calibri<br>Paste *<br>Clipboard 5<br>Clipboard 5 | Font ry               | = = ≫ -                      | کا Number                               | Conditional Format as Cell<br>Formatting * Table * Styles *<br>Styles | - Z <sup>™</sup> ■■<br>Sort & Find & | < > |
| A B C  | D                     | E                            | F                                       | G   |                                      |     |
| 1 Date T Acc Comp                                | Description           | Dr s 💌                       | Properties                              | <ul> <li>Miscellaneous</li> </ul>                                     |                                      |     |
| 576 N/A N/A NFURY                                | Task Scheduler - \At1 | Windows Command Processor    | c:\windows\system32\cmd.ex              | Launch String: "cmd" /c c:\windows\s                                  | ystem32\spinlock.exe                 |     |
| 577 N/A N/A NFURY                                | Task Scheduler - \At2 | Windows Command Processor    | c:\windows\system32\cmd.ex              | Launch String: "cmd" /c c:\windows\s                                  | ystem32\dllhost\svchost.ex           | e   |
| 921  | -                     |                              |   |   |                                      |     |
|  |                       |                              |   |   |                                      |     |

Figure 33. Suspicious scheduled tasks. (Lee, 2014, digital case files)

A search against NFurry's Shellbag entries shows the directory

C:\Windows\System32\dllhost\ where several suspicious executables reside (Figure 34).

| 🚺 🖯 🎝 d             | - D -       |          |                | NFury_NFURY_Sh     | ellbag_Results.xlsx - Exce | I   |            | ? 📧 –   | <b>—</b> × |
|---------------------|-------------|----------|----------------|--------------------|----------------------------|---|------------|---|------------|
| FILE HOME           | INSERT PAG  | E LAYOUT | FORMULAS DA    | TA REVIEW VIEW     | v                          |   |            |   |            |
| Paste V B           |             |          |                | ₩ Wrap Text        | General                    | Conditional Format as<br>Formatting ▼ Table ▼ |            | ∑ · A<br>Z · A<br>Z · A<br>Sort & Find &<br>Filter • Select • |            |
| Clipboard 🕞         | Font        | Es.      | Alignr         | nent G             | Number                     | Styles  | Cells      | Editing   | ~          |
| G161 ·              | × 🗸 f.      | x        |                |                    |                            |   |            |   | ~          |
| A                   | В           | С        | D              |                    | E                          |   | F          | G   | H 🔺        |
| 1 Date/Time         | T Account   | Computer | Description    | Details            |                            |   | Properties | Miscellaneous 💌 Art   | facts 💌    |
| 118 04/05/2012 17:  | L3:58 NFury | NFURY    | First Accessed | My Computer\C:\Win | dows\System32\dllh         | ost\  |            | She   | llbags     |
| 131 04/06/2012 18:4 | 43:43 NFury | NFURY    | Last Accessed  | My Computer\C:\Win | idows\System32\dllh        | ost\  |            | She   | llbags     |
| 158                 |             |          |                |                    |                            |   |            |   |            |

Figure 34. Shellbag keyword hits. (Lee, 2014, digital case files)

A keyword search against the MFT entries on the system shows the suspicious WINCLIENT.REG file in a user's Recycle Bin (Figure 35).

| ×     | H           | 5              | - (       | ⇒.    | Ľ          | Ŧ            |                |        |            |        |            |         | NF                     | URY_M   | FT_Res | sults.xlsx -   | xcel         |      |                             |           |         |                 |       |         | ?       | <b>T</b> –         |        | ×               |
|-------|-------------|----------------|-----------|-------|------------|--------------|----------------|--------|------------|--------|------------|---------|------------------------|---------|--------|----------------|--------------|------|-----------------------------|-----------|---------|-----------------|-------|---------|---------|--------------------|--------|-----------------|
| FILE  | E           | Н              | OME       |       | INSER      | T F          | PAGE LA        | YOUT   | FORM       | ULAS   | DA         | ATA     | REVIEW                 | VIE     | W      |                |              |      |                             |           |         |                 |       |         |         |                    |        |                 |
| Paste | ] [         | %<br>È∎ -<br>≶ | Cali<br>B |       | <u>U</u> - | • 1          |                | A A    | = =        | -      | %-<br>∈ +≘ |         | /rap Text<br>lerge & C | enter 🔻 |        | neral<br>• % • | ▼<br>0.0 0.0 |      | Conditional<br>Formatting ▼ |           |         | Enseri<br>Tolet | e -   |         |         | Find &<br>Select * |        |                 |
| Clipb | oard        | d 🕞            |           |       | 1          | Font         |                | E.     |            |        | Aligr      | nment   |                        | r       | 5      | Numbe          | r I          | G l  |                             | Styles    |         | Cells           |       |         | Editing |                    |        | ^               |
| wind  | clie        | ent_1          | *         | : [   | $\times$   | $\checkmark$ | f <sub>x</sub> | C:\\$F | ecycle.B   | in\S-: | 1-5-21     | -20368  | 04247-30               | 583246  | 540-21 | 11658524       | 1673\\$      | R6S  | ODDB\win                    | client.re | B       |                 |       |         |         |                    |        | ¥               |
|       |             |                | А         |       |            | В            | С              |        | D          |        |            |         |                        |         |        |                | E            |      |                             |           |         |                 |       |         | F       |                    |        |                 |
| 1     | D           | ate/           | Time      |       |            | Acc 🔻        | Comp           | ▼ De   | scriptic 💵 | Deta   | ails       |         |                        |         |        |                |              |      |                             |           |         |                 | Prop  | erties  |         |                    | - M    | ise             |
| 14723 | 32 0        | 04/05,         | 201       | 2 16: | 54:26      | N/A          | NFUR           | ( Cre  | ate Date   | C:\V   | Vindo      | ws\Sys  | tem32\s                | pinloc  | k.exe  |                |              |      |                             |           |         |                 | Std I | nfo - C | reate:  | 04/05/             | 20: FN | <mark>11</mark> |
| 14734 | <b>14</b> 0 | 04/05,         | 201       | 2 17: | 13:57      | N/A          | NFUR           | ( Cre  | ate Date   | C:\\$  | Recyc      | le.Bin\ | <mark>S-1-5-21</mark>  | 20368   | 04247  | -3058324       | 540-2116     | 5585 | 5241-1673\                  | \$R6SODD  | B\wincl | ient.reg        | Std I | nfo - C | reate:  | 04/05/             | 20: FN | <mark>11</mark> |
| 14734 | 17 0        | 04/05,         | 201       | 2 17: | 47:01      | N/A          | NFUR           | ( Cre  | ate Date   | C:\V   | Vindo      | ws\Ten  | np\a.exe               | 2       |        |                |              |      |                             |           |         |                 | Std I | nfo - C | reate:  | 04/05/             | 20: FN | <mark>11</mark> |
| 14764 | 14 0        | 04/06,         | 201       | 2 13: | 43:22      | N/A          | NFUR           | ( Cre  | ate Date   | C:\U   | sers\\     | vibrani | um\App                 | Data\L  | ocal\1 | Гemp\a.e       | xe           |      |                             |           |         |                 | Std I | nfo - C | reate:  | 04/06/             | 20: FN | <mark>11</mark> |
| 14786 | 63          |                |           |       |            |              |                |        |            |        |            |         |                        |         |        |                |              |      |                             |           |         |                 |       |         |         |                    |        |                 |

Figure 35. Winclient in user's recycle bin. (Lee, 2014, digital case files)

When we look at the Application Event Viewer log, two entries show up for the suspicious SVCHOST.EXE file (Figure 36).

| 🚺 🔒 🐬 👌                | <b>-</b> =           |                   | High              | lighted_NFURY_Applicati | on_XML_Standard_Results. | xlsx - Excel                | ?   | 团 – □ ×       |
|------------------------|----------------------|-------------------|-------------------|-------------------------|--------------------------|-----------------------------|---|---------------|
| FILE HOME I            | NSERT PAG            | E LAYOUT          | FORMULAS DAT      | A REVIEW VIEW           |                          |                             |   |               |
| Paste                  |                      | T A A             |                   | 🖶 Wrap Text             | General -                | Conditional Format as Cell  | Insert ▼<br>∑ ▼ Delete ▼<br>↓ ▼<br>Sort & | Find &        |
| Paste B I L            | <u>1</u> •   🖽 •   🕹 | <u>&gt; - A</u> - | E E E E           | 🖽 Merge & Center 🔹      | \$ - % '                 | Formatting * Table * Styles |   | Select *      |
| Clipboard 🗔            | Font                 | Fa                | Alignm            | ient 🗔                  | Number 🗔                 | Styles                      | Cells Editin                              | g 🔥 🔨         |
| D937 - :               | × 🗸 f.               | x                 |                   |                         |                          |                             |   | ~             |
| A                      | В                    | С                 | D                 | E                       |                          | F                           | G   | H 🔺           |
| 1 Date/Time            | Account 💌            | Computer 💌        | Description       | 💌 Details 💽 💌           | Properties               | J. M                        | iscellaneous                              | Artifact      |
| 11 04/05/2012 19:30:40 | ) -                  | NFURY             | Application Error | -                       | c:\windows\system32      | \dllhost\svchost.exe   Ev   | t ID: 1000   Evt Record #: 7697           | Application E |
| 12 04/05/2012 19:30:40 | ) -                  | NFURY             | Application Error | -                       | c:\windows\system32      | dllhost\svchost.exe   Ev    | t ID: 1000   Evt Record #: 7697           | Application E |
| 34                     |                      |                   |                   |                         |                          |                             |   |               |
|                        |                      |                   |                   |                         |                          |                             |   |               |

*Figure 36. Keyword hits in the Application Event Viewer log. (Lee, 2014, digital case files)* 

And finally for this host, in the System Event Viewer log, several instances of PSEXEC and PSEXESVC are found running as services (Figure 37).

| 🕅 🔒 5 - 🖓 - 🗋 - Highlighted_NFURY_System_EventLog_XML_Stan   | andard_Format.xlsx - Excel ? 📧 🗕 🗖                                |
|--|---|
| FILE HOME INSERT PAGE LAYOUT FORMULAS DATA REVIEW VIEW   |   |
| $ \begin{array}{c c} & & & \\ & & & \\ & & & \\ Paste \\ & & & \\ & & & \\ \end{array}  \\ & & & \\ \end{array} \begin{array}{c c} Calibiri & & & \\ & & & \\ Till & & & \\ & & & \\ \end{array} \begin{array}{c c} A^* & A^* \\ & & \\ \hline & & \\ \end{array} \begin{array}{c c} = & & \\ \hline & & \\ \hline & & \\ \end{array} \begin{array}{c c} Wrap Text \\ \hline & & \\ \hline & & \\ Wrap Text \\ \hline & & \\ \hline & & \\ \end{array} \begin{array}{c c} Text \\ \hline & \\ \hline & & \\ \hline & & \\ \end{array} \begin{array}{c c} \\ Text \\ \hline & \\ \hline & & \\ \end{array} \begin{array}{c c} \\ \hline & & \\ \end{array} \end{array}$ |   |
| Clipboard 🗤 Font 🖓 Alignment 🖓 Number  | r 🖓 Styles Cells Editing  |
| F3957 $\checkmark$ : X $\checkmark$ $f_X$ PsExec   |   |
| A B C D  | D E F G   |
| 1 Date/Time   Account  Computer  Description   | J Details Properties Miscellaneous                                |
| 949 04/05/2012 17:03:51 S-1-5-21-2036804247-3058324640-2116585241-1673 NFURY Service Contro  | rol Manager - PsExec   Evt ID: 7045   Evt Record                  |
| 950 04/05/2012 17:03:51 S-1-5-21-2036804247-3058324640-2116585241-1673 NFURY Service Control   | rol Manager - %SystemRoot%\PSEXESVC.EXE_Evt ID: 7045   Evt Record |
| 954 04/05/2012 17:03:52 - NFURY Service Contro   | rol Manager - PsExec Evt ID: 7036 Evt Record                      |
| 956 04/05/2012 17:03:52 - NFURY Service Contro   | rol Manager PSEXESVC/4 Evt ID: 7036   Evt Record                  |
| 1957 04/05/2012 17:03:55 - NFURY Service Contro  | rol Manager - PsExec  Evt ID: 7036   Evt Record                   |
| 959 04/05/2012 17:03:55 - NFURY Service Contro   | rol Manager   PSEXESVC/1 Evt ID: 7036   Evt Record                |
| 1962 04/05/2012 17:07:15 - NFURY Service Contro  | rol Manager   PSEXESVC/4 Evt ID: 7036   Evt Record                |
| 963 04/05/2012 17:07:15 S-1-5-21-2036804247-3058324640-2116585241-1673 NFURY Service Contro  | rol Manager - PsExec   Evt ID: 7045   Evt Record                  |
| 8964 04/05/2012 17:07:15 S-1-5-21-2036804247-3058324640-2116585241-1673 NFURY Service Contro   | rol Manager - %SystemRoot%\PSEXESVC.EXE_Evt ID: 7045   Evt Record |
| 8971 04/05/2012 17:22:41 - NFURY Service Control   | rol Manager - PsExec   Evt ID: 7036   Evt Record                  |
| Sheet1 Sheet3  | : 4   |
| READY 24 OF 5049 RECORDS FOUND CALCULATE 🔚   | III II  |

Figure 37. Keyword hits in the System Event Viewer log. (Lee, 2014, digital case files)

### 5.1.4. Win2008R2-Controller (CONTROLLER)

The last host (IP Address 10.3.58.4) examined in this case study is the domain controller. When we look at the Autorun entries, we discover a scheduled task to run SPINLOCK.EXE (Figure 38).

| 🕅 🔒 🐤 🔿 · 🗋 📼  | Controlle                               | r_Autoruns_Results.xlsx - Excel |   | ? 🗈 – 🗆 🗙                          |
|--|---|---------------------------------|---|------------------------------------|
| FILE HOME INSERT PAGE LAYOUT F   | DRMULAS DATA REVIEW                     | VIEW                            |   |                                    |
| Paste $\checkmark$ $B I \underline{U} \checkmark \square \checkmark \Delta \checkmark \Delta \checkmark$ | = ► I I I I I I I I I I I I I I I I I I | er ↓ ⊅ √ % ,00 →.0 For          | rmatting 👻 Table 👻 Styles 👻 📰 Format 👻 🗶 👻  | Sort & Find &<br>Filter - Select - |
| Clipboard 5 Font 5   | Alignment                               | Fa Number Fa                    | Styles Cells                                | Editing A                          |
| spinlock_1 $\cdot$ : $\times$ $\checkmark$ $f_x$ Launch St   | ring: "cmd" /c c:\windows\syster        | n32\spinlock.exe                |   | ~                                  |
| A B C D  | E                                       | F                               | G   | *                                  |
| 1 Date Acco Comput Description   | Details 🔹                               | Properties 🔹                    | Miscellaneous                               | 💌 Arti                             |
| 573 N/A N/A Controller Task Scheduler - \At2   | Windows Command Processor               | c:\windows\system32\cmd.exe     | Launch String: "cmd" /c c:\windows\system32 | 2\spinlock.exe Aut                 |
| 790  |   |                                 |   | ⊺ II I                             |

Figure 38. Suspicious scheduled task. (Lee, 2014, digital case files)

Examining the MFT log shows PSEXEC and Spinlock on the system (Figure 39).

| 🚺 🖯 🏷 🖓 🖓 🗧   | CONTROLLER_MFT_Results.xlsx - Excel   | ? 🛧 –   | • ×   |
|---|---|---|---|
| FILE HOME INSERT PAG  | E LAYOUT FORMULAS DATA REVIEW VIEW  |   |   |
|   | · A · A · = = · · · · · · · · · · · · ·   | Sort & Find &   |   |
| Clipboard 🖓 Font  | rs Alignment rs Number rs Styles Cells  | Editing   | ~   |
| and a local state of the state |   | 0404-1104-1-1-1 42  | chooo .   |
| spinlock_1  |   | 20484d134edcb1_cab_43<br>F  | 6b900 🔻   |
|   |   | F   | 6b900 💊   |
| A B<br>1 Date/Time J Accour   | C D E<br>Computer Description Details Properti  | F   | ▼ M   |
| A B<br>1 Date/Time J Accour<br>66014 04/27/2010 19:04:06 N/A  | C D E<br>Computer Description Details Properti  | F<br>F<br>ties<br>0 - Create: 04/27/2010 19   | <b>M</b><br>0:04:(FN  |
| A B<br>1 Date/Time J Accourt<br>66014 04/27/2010 19:04:06 N/A<br>175055 04/04/2012 18:28:42 N/A   | Computer v Descriptio v Details v Properti<br>CONTROLLER Create Date (\Tools\SysInternals\PsExec.exe Std Info   | F<br>F<br>c Create: 04/27/2010 19<br>c - Create: 04/04/2012 18  | <b>M</b><br>0:04:(FN<br>0:28:4 FN                                 |
| A B<br>1 Date/Time J Accourty<br>66014 04/27/2010 19:04:06 N/A<br>175055 04/04/2012 18:28:42 N/A<br>175056 04/04/2012 18:28:42 N/A  | C D E Propertie<br>Computer Description Details Potence Std Info<br>CONTROLLER Create Date (\Tools\SysInternals\PsExec.exe Std Info<br>CONTROLLER Create Date (\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_spinlock.estd Info  | F<br>F<br>c- Create: 04/27/2010 19<br>c - Create: 04/04/2012 18<br>c - Create: 04/04/2012 18                                  | ▼ M<br>):04:( FN<br>):28:4 FN<br>):28:4 FN                        |
| A 8<br>1 Date/Time J Accour<br>66014 04/27/2010 19:04:06 N/A<br>175055 04/04/2012 18:28:42 N/A<br>175055 04/04/2012 18:28:42 N/A  | CONTROLLER Create Date (\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_spinlock.eStd Info<br>CONTROLLER Create Date (\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_spinlock.eStd Info  | F<br>ties<br>o - Create: 04/27/2010 19<br>o - Create: 04/04/2012 18<br>o - Create: 04/04/2012 18<br>o - Create: 04/04/2012 18 | M<br>0:04:(FN<br>0:28:4 FN<br>0:28:4 FN<br>0:28:4 FN<br>0:28:4 FN |
| A B   | C         D         E           Computer         Descriptio         Details         Y           CONTROLLER         Create Date (\Tools\SysInternals\PsExec.exe         Std Info           CONTROLLER         Create Date (\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_spinlock.elstd Info | F<br>ties<br>o - Create: 04/27/2010 19<br>o - Create: 04/04/2012 18<br>o - Create: 04/04/2012 18<br>o - Create: 04/04/2012 18 | M<br>0:04:(FN<br>0:28:4FN<br>0:28:4FN<br>0:28:4FN<br>0:28:4FN     |

Figure 39. Keyword hits in MFT file. (Lee, 2014, digital case files)

The Application Event Viewer records the same SPINLOCK.EXE file in Windows Error Reporting (WER) (Figure 40).

| XI 🔒 🗧      | 5 ° °                    | <b>-</b> =        |            | highlig           | hted_CONTR(        | OLLER_Appli | ation_XML_Sta    | ndard_Res          | ults.xlsx - Excel             |                        |          |                      | 3            | ?                       | - 🗆 X      |
|-------------|--------------------------|-------------------|------------|-------------------|--------------------|-------------|------------------|--------------------|-------------------------------|------------------------|----------|----------------------|--------------|-------------------------|------------|
| FILE        | HOME I                   | NSERT PA          | AGE LAYOUT | FORMULAS DA       | TA REVIE           | W VIEW      |                  |                    |                               |                        |          |                      |              |                         |            |
| Paste       | Calibri<br>B I L         | - 11<br>J - 8 - 1 | • A A      |                   | 🔐 Wrap Te          |             | Text<br>\$ ~ % > | ₹.0 .00<br>.00 →.0 | Conditional F<br>Formatting ▼ | Format as<br>Table + S | Cell     | Ensert •<br>Delete • |              | t & Find<br>er * Select |            |
| Clipboard r | G                        | Font              | G.         | Alignn            | nent               | Fa          | Number           | Es.                | S                             | tyles                  |          | Cells                | Ed           | iting                   | ~          |
| spinlock_2  |                          |                   | fx C:\Prog | gramData\Microsof | t <b>\W</b> indows | \WER\Repo   | ortQueue\Noi     | nCritical_         | _spinlock.exe_                | f55bbffa8              | Sebc6a99 |                      |              | dcb1_ca                 | -          |
|             | A                        | В                 | C          | D                 |                    |             | E                |                    |                               | F                      |          | G                    | i            | _                       | H ▲        |
| 1 Date/     |                          |                   | Computer 💌 |                   |                    | Details     |                  |                    | Ŧ                             | Proper                 |          |                      |              |                         | rtifact    |
| 13315 04/04 | <mark>/2012 18:28</mark> | :42 -             | CONTROLLER | Windows Error Re  | porting            | spinlock.e  | xe               |                    |                               | -1                     | Evt ID:  | 1001   Evt F         | Record #: 22 | 21250 A                 | pplicatior |
| 13317 04/04 | /2012 18:28              | :42 -             | CONTROLLER | Windows Error Re  | porting            | spinlock.e  | xe               |                    |                               | -1                     | Evt ID:  | 1001   Evt F         | Record #: 22 | 21250 A                 | pplicatior |
| 13326 04/04 | /2012 18:28              | :42 -             | CONTROLLER | Windows Error Re  | porting            | C:\Program  | nData\Micros     | oft\Wind           | dows\WER\Re                   | i-1                    | Evt ID:  | 1001   Evt F         | ecord #: 22  | 21250 A                 | pplicatior |
| 13336 04/04 | /2012 18:28              | :42 -             | CONTROLLER | Windows Error Re  | porting            | spinlock.e  | xe               |                    |                               | -                      | Evt ID:  | 1001   Evt F         | ecord #: 22  | 21249 A                 | pplicatior |
| 13338 04/04 | /2012 18:28              | :42 -             | CONTROLLER | Windows Error Re  | porting            | spinlock.e  | xe               |                    |                               | -1                     | Evt ID:  | 1001   Evt F         | ecord #: 22  | 21249 A                 | pplicatior |
| 22390       |                          |                   |            |                   |                    |             |                  |                    |                               |                        |          |                      |              |                         |            |

Figure 40. Keyword hits in the Application Event Viewer log. (Lee, 2014, digital case files)

The Security Event Viewer log (Figure 41) and the System Event Viewer log (Figure 42), both show the PSEXESVC.EXE service running.

| XI     | 5-         | €.             | <u> </u>                   |           |        | Highli     | ghted_COM | NTROLLER_Secu               | rity_Even | tLog_XN        | IL_Stand | dard_Form               | at_20120404.xls             | ax - Excel           |                           |                                  |                   | ?                         | <b>*</b> - | - 🗆    | ×   |
|--------|------------|----------------|----------------------------|-----------|--------|------------|-----------|-----------------------------|-----------|----------------|----------|-------------------------|-----------------------------|----------------------|---------------------------|----------------------------------|-------------------|---------------------------|------------|--------|-----|
| FILE   | HO         | ИE             | INSERT                     | PAGE LAYO | TUC    | FORMULA    | DAT       | A REVIEW                    | VIEV      | /              |          |                         |                             |                      |                           |                                  |                   |                           |            |        |     |
| Paste  | Ē <u>₽</u> | Calibri<br>B I | -<br><u>U</u> - <u>U</u> - |           |        | _ =        |           | F Wrap Text<br>🗮 Merge & Ce | nter 🝷    | Genera<br>\$ + | I<br>%   | ▼<br>00. 00.<br>0.€ 00. | Conditional<br>Formatting → | Format as<br>Table • |                           | Insert ▼<br>Delete ▼<br>Format ▼ | ∑ -<br>↓ -<br>∢ - | AZT<br>Sort &<br>Filter * |            |        |     |
| Clipbo | ard 🗔      |                | Font                       |           | Es .   |            | Alignm    | ent                         | G.        |                | Number   | G,                      |                             | Styles               |                           | Cells                            |                   | Editing                   | I          |        | ^   |
| E1434  | 184 .      | ·              | $\times \checkmark$        | $f_x$     |        |            |           |                             |           |                |          |                         |                             |                      |                           |                                  |                   |                           |            |        | ٧   |
|        |            | А              | В                          |           | с      |            | D         |                             | E         |                |          |                         | F                           |                      |                           | G                                |                   |                           |            |        | F 🔺 |
| 1      | Date/Ti    | ne             | T Acco                     | Comp      | uter 👻 | Descriptio | n         | <ul> <li>Details</li> </ul> |           |                | v        | Propert                 | ies                         |                      | <ul> <li>Misce</li> </ul> | llaneous                         |                   |                           | ▼ Ar       | tifact |     |
| 44908  | 04/04/2    | 012 18         | :00:44 -                   | CONT      | ROLLER | Microsoft- | Window    | s-S C:\Windov               | /s\PSEX   | ESVC.E         | ХE       | Process                 | Name   -                    |                      | Evt ID                    | <mark>: 4648   Evt R</mark>      | ecord #           | : 12509                   | 850 Se     | curity | Ev  |
| 44928  | 04/04/2    | 012 18         | :00:44 -                   | CONT      | ROLLER | Microsoft  | Window    | s-S C:\Windov               | /s\PSEX   | ESVC.E         | XE       | Process                 | Name   -                    |                      | Evt ID                    | : 4624   Evt R                   | ecord #           | : 12509                   | 851 Se     | curity | Ev  |
| 44948  | 04/04/2    | 012 18         | :00:44 -                   | CONT      | ROLLER | Microsoft- | Window    | s-S C:\Windov               | s\PSEX    | ESVC.E         | ХE       | Process                 | Name   -                    |                      | Evt ID                    | : 4624   Evt R                   | ecord #           | : 12509                   | 852 Se     | curity | Ev  |
| 143482 |            |                |                            |           |        |            |           |                             |           |                |          |                         |                             |                      |                           |                                  |                   |                           |            |        |     |

Figure 41. Keyword hits in the Security Event Viewer log. (Lee, 2014, digital case files)

|       |                        |                     |               |             |                |                              |           |            |                |                          |           |          |                                  |                   |                             |          | _      | _   |
|-------|------------------------|---------------------|---------------|-------------|----------------|------------------------------|-----------|------------|----------------|--------------------------|-----------|----------|----------------------------------|-------------------|-----------------------------|----------|--------|-----|
| x∎    | <mark>සු 5</mark> -  ි | - 🗋 -               |               | Н           | ighlighted_CON | TROLLER_Syster               | n_EventLo | og_XML_Sta | andard_F       | ormat.xlsx - E           | xcel      |          |                                  |                   | ?                           | <u> </u> |        | х   |
| FILE  | HOME                   | INSERT P.           | AGE LAYOUT    | FORMULAS    | DATA           | REVIEW VI                    | W         |            |                |                          |           |          |                                  |                   |                             |          |        |     |
| Paste | Calibri                | i •  11             | • A A         |             |                | rap Text<br>erge & Center    | Text      | % ,        | ▼<br>0.00, 0.0 | Conditiona<br>Formatting |           |          | Insert •<br>Delete •<br>Format • | ∑ -<br>↓ -<br>∢ - | AZT<br>Sort &<br>Filter * S |          |        |     |
| Clipb | oard 🖓                 | Font                | Fai           |             | Alignment      |                              | 5         | Number     | Fai            |                          | Styles    |          | Cells                            |                   | Editing                     |          |        | ^   |
| E519  | 921 -                  | $\times \checkmark$ | fx -          |             |                |                              |           |            |                |                          |           |          |                                  |                   |                             |          |        | v   |
|       | А                      |                     |               | в           |                | С                            |           |            | D              |                          | E         |          | F                                |                   |                             |          | G      | -   |
| 1     | Date/Time              | - Accoun            | t             |             |                | <ul> <li>Computer</li> </ul> | - Desc    | ription    |                | ,∓ De                    | tails 🔻 P | ropertie | s                                | Ŧ                 | Miscel                      | laneou   | s      | ٦٦  |
| 51903 | 04/04/2012 17          | .29:33 -            |               |             |                | CONTROL                      |           | •          | ol Mana        |                          |           |          | PSEXESVC/4                       |                   | Evt ID:                     | 7036     | Evt Re | c   |
|       | 04/04/2012 17          |                     |               |             |                | CONTROL                      |           |            |                | -                        |           |          | PSEXESVC/4                       |                   | Evt ID:                     |          |        |     |
|       |                        |                     | L-2036804247- | 3058324640- | 2116585241-16  | 73 CONTROL                   | ER Serv   | ice Contro | ol Mana        | zer -                    |           | sExec    |                                  |                   | Evt ID:                     |          |        |     |
| 51906 | 04/04/2012 17          |                     | L-2036804247- | 3058324640- | 2116585241-16  | 73 CONTROL                   | ER Serv   | ice Contro | ol Mana        | zer -                    | %         | System   | Root%\PSEXES                     | VC.EXE            | Evt ID:                     | 7045     | Evt Re | с   |
| 51910 | 04/04/2012 17          | /:29:34 -           |               |             |                | CONTROL                      | ER Serv   | ice Contro | ol Mana        | zer -                    |           |          | PSEXESVC/1                       |                   | Evt ID:                     |          |        |     |
| 51911 | 04/04/2012 17          | /:29:34 -           |               |             |                | CONTROL                      | ER Serv   | ice Contro | ol Mana        | zer -                    | S         | opped    | PSEXESVC/1                       |                   | Evt ID:                     | 7036     | Evt Re | с   |
| 51920 | 04/04/2012 17          | /:30:09 -           |               |             |                | CONTROL                      | ER Serv   | ice Contro | ol Mana        | zer -                    | Р         | sExec    | PSEXESVC/4                       |                   | Evt ID:                     | 7036     | Evt Re | с   |
| 51921 | 04/04/2012 17          | /:30:09 -           |               |             |                | CONTROL                      | ER Serv   | ice Contro | ol Mana        | zer -                    | r         | Inning   | PSEXESVC/4                       |                   | Evt ID:                     | 7036     | Evt Re | с _ |
| 51922 | 04/04/2012 17          |                     | L-2036804247- | 3058324640- | 2116585241-16  | 73 CONTROL                   | ER Serv   | ice Contro | ol Mana        | ger -                    |           | sExec    |                                  |                   | Evt ID:                     | 7045     | Evt Re | c   |
| 51923 | 04/04/2012 17          |                     | L-2036804247- | 3058324640- | 2116585241-16  | 73 CONTROL                   | ER Serv   | ice Contro | ol Mana        | ger -                    | %         | System   | Root%\PSEXES                     | VC.EXE            | Evt ID:                     | 7045     | Evt Re | c _ |
| 4     | > Sh                   | eet1 Sheet2         | Sheet3        | +           |                |                              |           | <u> </u>   |                | 4                        | -         |          |                                  |                   |                             |          | •      |     |
| READ  | / 36 OF 64509 P        | RECORDS FOUND       | CALCULATE     | 1           |                |                              |           |            |                |                          |           | E        | 8 8 8                            |                   |                             |          | - 100  | %   |
|       |                        |                     |               |             |                |                              |           |            |                |                          |           |          |                                  |                   |                             |          |        |     |

Figure 42. Keyword hits in the System Event Viewer log. (Lee, 2014, digital case files)

#### 5.1.5. Master IOC Spreadsheet

Taking all the hits found from each of the workstations and combining them into one master spreadsheet allows the responder to see, among other benefits, what the adversary is doing chronologically; what artifacts they used across systems; and what capabilities they deployed. To demonstrate the techniques outlined in this paper, the standard output in the below images have been manipulated to fit the relevant information into the screenshots.

When we look at the timeline of events, the incident appears to have started on 04/03/2012 with the exploitation of host TGUNGAN (WKS-WINXP32BIT), then laterally moving to host NROMANOFF (WKS-WIN732BITA), then on to the Domain Controller (CONTROLLER) and finally to NFURY (WKS-WIN764BITB) (Figure 43).

|      | 19 e  - 15  |                 |   |  |  | a 🕜 🗆 i                          |
|------|---|-----------------|---|--|--|----------------------------------|
| File |   | Page Layout For | mulas Data Review View Team             |  |  | a 🕜 🗆 (                          |
| aste | X Cut Cali<br>Copy +<br>I Gopy +<br>I Gali<br>Copy +<br>B |                 | · A` A` ≡ = = ≫ ·<br>. Wrap Lev<br>     | - <u> </u>                               | Cell Insert Delete Format                  | ort & Find &<br>itter - Select - |
|      | Clipboard 5   | Font            | Alignment                               | S Number S Styles                        | Cells Editio                               | 9                                |
|      | C16 -   | fx C:           | \\$Recycle.Bin\S-1-5-21-2036804247-3058 | 324640-2116585241-1673\\$R6SODDB\winclie | ent.reg                                    |                                  |
| 4    | A   | В               |   | с  | D  | E                                |
| C    | ate/Time  | Computer *      | Details                                 |  | Properties                                 | · Artifacts                      |
| 0    | 4/03/2012 00:33:15  | TDUNGAN         | C:\Documents and Settings\tdungan\Lo    | cal Settings\Temp\pkxezy1tji98.exe       | FN Info - Modify: 04/03/2012 00:33:15, Er  | ntry: 04/03/20 MFT Entry         |
| C    | 4/03/2012 00:33:17  | TDUNGAN         | PKX57Y1TJI98.EXE-0BCBF29B.pf            |  | Number of Time Run: 1                      | Prefetch Entry                   |
|      | 4/03/2012 00:34:26  | TDUNGAN         | C:\WIN POWS\system32\dllhost            |  | FN Info - Modify: 04/03/2012 00:34:26, Er  | ntry: 04/03/20 MFT Entry         |
| C    | 4/03/2012 18:08:50  | NROMANOFF       | C:\\$Recycle.Bi.\5-1-5-21-2036804247-3  | 058324640-2116585241-1673\\$RR3GW21.exe  | Executed: False                            | ShimCache                        |
| ¢    | 4/03/2012 18:08:50  | NROMANOFF       | C:\dllhot.exe                           |  | Executed: True                             | ShimCache                        |
| ¢    | 4/03/2012 18:08:50  | NROMANOFF       | ::\c_bost.exe                           |  | Executed: True                             | ShimCache                        |
| ¢    | 4/03/2012 20:26:18  | NROMANOFF       | A member was added to a security-enab   | bled local group.                        | BUILTIN\Administrators                     | Security Event                   |
|      |   |                 |   |  |  |                                  |
| C    | 4/04/2012 18:00:44  | CONTROLLER      | C:\Windows\PSEXEs.C.EXE                 |  | ProcessName                                | Security Event                   |
|      | 4/04/2012 18:28:42  |                 | spin vck.exe                            |  | Windows Error Reporting                    | Application Ev                   |
| C    | 4/05/2012 16:54:26  | NFURY           | C:\Windows\Systems_ minlock.exe         |  | FN Info - Modify: 04/05/2012 16:54:26, Er  | ntry: 04/05/20 MFT Entry         |
|      | 4/05/2012 17:07:15  |                 | %SwitemRoot%\PSEXESVC.EXE               |  | Service Control Manager                    | Application Ev                   |
|      | 4/05/2012 17:13:57  |                 | C:\\$Recycle.8m\s = 21_2036804247-3     |  | dFN Info - Modify: 04/05/2012 17:13:57, Er |                                  |
| ¢    | 4/05/2012 17:13:58  | NFURY           | My Computer\C:\Windows\System32\a       | innos.                                   | First Accessed                             | Shellbags                        |
| F    |   |                 | Time                                    | line of Lateral Movement                 |  |                                  |
| i    | >> Sheet1   |                 |   | 14                                       |  |                                  |

Figure 43. A timeline of events. (Lee, 2014, digital case files)

Tools used across hosts by the adversary include svchost.exe (Figure 44), a.exe (Figure 45), spinlock.exe (Figure 46), winclient (Figure 47), and psexesvc (Figure 48).

| 8   | <b>∃</b> •>• @• =   |                        | Stark_IOC_                              | All_Modified.xlsx -    | Microsoft Excel   |                      |  | _ 🗆 🗙                         |
|-----|---------------------|------------------------|---|------------------------|---|----------------------|--|-------------------------------|
| F   |                     | ൾ<br>Page Layout Formu | las Data Review View Team               |                        |   |                      |  | 23 🖷 🗕 🕥 ۵                    |
| ľ   | Cut Calil           | bri - 11 -             | A A S S S Wrap Text                     | General 👻              | 🛃 📝 📝   | i 👬 👘                | ∑ AutoSum * 😿 👬                            |                               |
| Pas |                     | I U -   🔤 -   🗳        | 💽 🚣 🔹 📰 📰 🐨 🖬 Merge & Center 🕶          |                        | Conditional Format Cell<br>Formatting + as Table + Styles + | Insert Delete Format | Clear * Sort & Find &<br>Filter * Select * |                               |
|     | Clipboard 🕞         | Font                   | G Alignment G                           | Number 🖓               | Styles  | Cells                | Editing                                    |                               |
|     | C129 -              | <i>f</i> ∗ HKLM        | //SOFTWARE\Wow6432Node\Microsoft\Wir    | ndows\CurrentVersion   | \Run - svchost  |                      |  | ¥                             |
|     | A                   | В                      |   | С                      |   |                      | D  | E 🔺                           |
| 1   | Date/Time           | Computer 🛛 👻           | Details                                 |                        | .7  | Properties           |  | <ul> <li>Artifacts</li> </ul> |
| 5   | 04/03/2012 00:35:03 | TDUNGAN                | C:\WINDOWS\system32\dllhost\svchost.exe | •                      |   | FN Info - Modify: 04 | 1/03/2012 00:35:04, Entry: 04/             | 03/20 MFT Entry               |
| 39  | 04/03/2012 22:40:25 | NROMANOFF              | c:\windows\system32\dllhost\svchost.exe |                        |   | Executed: True       |  | ShimCache                     |
| 47  | 04/03/2012 23:52:47 | NROMANOFF              | Service Name: winsvchost                |                        |   | c:\windows\system    | 32\cmd.exe /k c:\windows\sy                | /stem:System Ev               |
| 63  | 04/04/2012 01:18:15 | NROMANOFF              | c:\windows\system32\dllhost\svchost.exe |                        |   | Application Error    |  | Applicatio                    |
| 94  | 04/05/2012 05:19:11 | NROMANOFF              | C:\windows\system32\dllhost\svchost.exe |                        |   | Microsoft-Window     | s-Security-Auditing                        | Applicatio                    |
| 96  | 04/05/2012 05:19:11 | NROMANOFF              | C:\windows\system32\dllhost\svchost.exe |                        |   | Dst IP: 12.190.135.2 | 235   Dst Prt: 80                          | Security Ev                   |
| 111 | 04/05/2012 19:30:40 | NFURY                  | c:\windows\system32\dllhost\svchost.exe |                        |   | Application Error    |  | Applicatio                    |
| 127 | N/A                 | NROMANOFF              | HKLM\SOFTWARE\Microsoft\Windows\Curr    | rentVersion\Run - svch | nost  | c:\windows\system    | 32\dllhost\svchost.exe                     | Autoruns                      |
| 129 | N/A                 | NFURY                  | HKLM\SOFTWARE\Wow6432Node\Microsof      | t\Windows\CurrentVe    | ersion\Run - svchost  | c:\windows\system    | 32\dllhost\svchost.exe                     | Autoruns                      |
| 133 |                     |                        |   |                        |   |                      |  |                               |

Figure 44. SVCHOST.EXE keyword hits. (Lee, 2014, digital case files)

| File Home Insert    | Page Layout For       | mulas Data Review   | View Team        |                         |             |              |             |  |             |                |               |                          | _ <b>○</b> ⊂                  | ) (j |
|---------------------|-----------------------|---------------------|------------------|-------------------------|-------------|--------------|-------------|--|-------------|----------------|---------------|--------------------------|-------------------------------|------|
| Cali                | bri • 11<br>I Ц • — • |                     | ≫ → 書 Wrap       | o Text<br>je & Center • | General     | ▼<br>0.* 0.* | Conditional |  | ell Insert  |                | ∑ AutoSum •   | Zí mini<br>Sort & Find & |                               |      |
| Clipboard           | Font                  |                     | Alignment        | 6                       | Numbe       | r G          | Formatting  | <ul> <li>as Table - Sty</li> <li>Styles</li> </ul> | les * *     | Cells          | -             | Filter • Select •        |                               |      |
| C7 •                |                       | Documents and Setti |                  | ocal Setting            | s\Temp\a.e  | xe           |             |  |             |                |               |                          |                               | _    |
| A                   | В                     |                     | С                | -                       |             |              |             |  |             | D              |               |                          | E                             |      |
| Date/Time 🔹         | Computer 🔻            | Details             |                  |                         |             |              | J Prope     | rties  |             |                |               |                          | <ul> <li>Artifacts</li> </ul> |      |
| 04/03/2012 20:43:54 | TDUNGAN               | C:\WINDOWS\Prefet   | ch\A.EXE-0F3A    | )E12.pf                 |             |              | FN Inf      | o - Modify: I                                      | 04/03/201   | 2 20:43:54, Er | ntry: 04/03/2 | 012 20:43:54             | MFT Entry                     | _    |
| 04/03/2012 23:54:46 | NROMANOFF             | C:\Windows\Temp\a   | a.exe            |                         |             |              | FN Inf      | o - Modify: I                                      | 04/03/201   | 2 23:54:46, Er | ntry: 04/03/2 | 012 23:54:46             | MFT Entry                     |      |
| 04/03/2012 23:54:48 | NROMANOFF             | C:\Windows\Prefetc  | h\A.EXE-8D56B    | LC4.pf                  |             |              | FN Inf      | o - Modify: I                                      | 04/03/201   | 2 23:54:48, Er | ntry: 04/03/2 | 012 23:54:48             | MFT Entry                     |      |
| 04/04/2012 00:01:20 | NROMANOFF             | C:\Windows\TEMP\a   | a.exe            |                         |             |              | Execut      | ted: True  |             |                |               |                          | ShimCache                     |      |
| 04/04/2012 00:43:06 | NROMANOFF             | A.EXE-8D56B1C4.pf   |                  |                         |             |              | Numb        | er of Time F                                       | lun: 26     |                |               |                          | Prefetch En                   | ıtr  |
| 04/04/2012 00:44:11 | NROMANOFF             | C:\Windows\TEMP\a   | a.exe            |                         |             |              | Execut      | ted: True  |             |                |               |                          | ShimCache                     |      |
| 04/04/2012 02:22:00 | NROMANOFF             | C:\Users\vibranium\ | AppData\Local    | Temp\a.e                | (e          |              | FN Inf      | o - Modify: I                                      | 04/04/201   | 2 02:22:00, Er | ntry: 04/04/2 | 012 02:22:00             | MFT Entry                     |      |
| 04/04/2012 02:22:02 | NROMANOFF             | C:\Windows\Prefetc  | h\A.EXE-F91CBA   | OE.pf                   |             |              | FN Inf      | o - Modify: (                                      | 04/04/201   | 2 02:22:02, Er | ntry: 04/04/2 | 012 02:22:02             | MFT Entry                     |      |
| 04/04/2012 12:22:40 | TDUNGAN               | A.EXE-0F3A0E12.pf   |                  |                         |             |              | Numb        | er of Time F                                       | lun: 67     |                |               |                          | Prefetch En                   | iti  |
| 04/04/2012 12:26:24 | TDUNGAN               | C:\Documents and S  | ettings\SRL-Help | odesk\Loca              | Settings\T  | emp\a.e      | e FN Inf    | o - Modify: I                                      | 04/04/201   | 2 12:26:24, Er | ntry: 04/04/2 | 012 12:26:24             | MFT Entry                     |      |
| 04/04/2012 12:26:30 | TDUNGAN               | C:\WINDOWS\Prefet   | ch\A.EXE-23930   | 05EA.pf                 |             |              | FN Inf      | o - Modify: I                                      | 04/04/201   | 2 12:26:30, Er | ntry: 04/04/2 | 012 12:26:30             | MFT Entry                     |      |
| 04/04/2012 14:01:32 | TDUNGAN               | A.EXE-OFBE37C1.pf   |                  |                         |             |              | Numb        | er of Time F                                       | lun: 390    |                |               |                          | Prefetch En                   | itr  |
| 04/04/2012 16:41:47 | TDUNGAN               | C:\Documents and S  | ettings\vibraniu | m\Local Se              | ettings\Tem | p∖a.exe      | FN Inf      | o - Modify: I                                      | 04/04/201   | 2 16:41:47, Er | ntry: 04/04/2 | 012 16:41:47             | MFT Entry                     |      |
| 04/04/2012 16:41:58 | TDUNGAN               | C:\WINDOWS\Prefet   | ch\A.EXE-2E0C    | 27A0.pf                 |             |              | FN Inf      | o - Modify: I                                      | 04/04/201   | 2 16:41:58, Er | ntry: 04/04/2 | 012 16:41:58             | MFT Entry                     |      |
| 04/05/2012 05:19:11 | NROMANOFF             | C:\users\vibranium\ | appdata\local\t  | emp\a.exe               |             |              | Micro       | soft-Windo   | vs-Security | y-Auditing     |               |                          | Application                   | E    |
| 04/05/2012 13:28:01 | TDUNGAN               | A.EXE-2E0C27A0.pf   |                  |                         |             |              | Numb        | er of Time F                                       | lun: 490    |                |               |                          | Prefetch En                   | ıtr  |
| 04/05/2012 17:47:01 | NFURY                 | C:\Windows\Temp\a   | a.exe            |                         |             |              | FN Inf      | o - Modify: I                                      | 04/05/201   | 2 17:47:01, Er | ntry: 04/05/2 | 012 17:47:01             | MFT Entry                     |      |
| 04/06/2012 13:43:22 | NFURY                 | C:\Users\vibranium\ | AppData\Local    | Temp\a.e                | ke          |              | FN Inf      | o - Modify: I                                      | 04/06/201   | 2 13:43:22, Er | ntry: 04/06/2 | 012 13:43:22             | MFT Entry                     |      |
| \mapsto 🖻 Sheet1 😕  |                       |                     |                  |                         |             |              |             |  |             |                |               |                          |                               |      |

Figure 45. A.EXE keyword hits. (Lee, 2014, digital case files)

| 🖾   🚽 🤊 • 🔗 -   = 🛛 📐           | Stark_IOC_A  | II_Modified.xlsx - Microsoft I | Excel  | _ 🗆 🗙                                   |
|---------------------------------|--|--------------------------------|--|---|
| File Home Insert Page Layout    | Formulas Data Review View Team   |                                |  | ۵ 🕝 🗖 🖓                                 |
| Calibri                         | • 11 • <b>A A E E S</b> • <b>E</b> Wrap Text                           | General 🗸                      | 🗾 📑 🚰 🔆 🛄 Σ Aut  | • 🦅 🖍                                   |
| Paste Sermat Painter B I U      | 🛄 🔹 🌺 🗙 🚣 🐂 🧱 🗮 🖉 Merge & Center 🔹                                     | \$ • % •                       | format Cell Insert Delete Format Q Cle<br>Table * Styles * * * * | ar * Sort & Find &<br>Filter * Select * |
| Clipboard 💈 For                 | t 💈 Alignment 🖾  | Number 🕞 Sty                   | /les Cells   | Editing                                 |
| C105 - ß                        | <ul> <li>C:\Documents and Settings\vibranium\Local Settings</li> </ul> | gs\Temp\_MEI122362\spinlock.e  | exe.manifest   | ,                                       |
| A B                             | С  |                                | D  | E                                       |
| 1 Date/Time  Compute            |  |                                | Properties   | <ul> <li>Artifacts</li> </ul>           |
| 41 04/03/2012 22:53:39 NROMAN   | IOFF C:\Windows\system32\spinlock.exe                                  |                                | Executed: True   | ShimCache                               |
| 42 04/03/2012 22:59:43 NROMAN   | OFF C:\Windows\System32\spinlock.exe                                   |                                | FN Info - Modify: 04/03/2012 22:59:43,                           | Entry: 04/03/201 MFT Entry              |
| 43 04/03/2012 23:09:26 NROMAN   | OFF C:\Windows\Prefetch\SPINLOCK.EXE-1610A75A                          | pf                             | FN Info - Modify: 04/03/2012 23:09:26,                           | Entry: 04/03/201 MFT Entry              |
| 51 04/04/2012 00:01:45 NROMAN   | OFF C:\Users\vibranium\AppData\Local\Temp\_ME                          | 157722\spinlock.exe.manifest   | FN Info - Modify: 04/04/2012 00:01:45,                           | Entry: 04/04/201 MFT Entry              |
| 53 04/04/2012 00:06:41 NROMAN   | OFF C:\Users\vibranium\AppData\Local\Temp\_ME                          | 1111242\spinlock.exe.manifest  | FN Info - Modify: 04/04/2012 00:06:41,                           | Entry: 04/04/201 MFT Entry              |
| 55 04/04/2012 00:07:23 NROMAN   | OFF spinlock.exe   |                                | USER32   | Application Event Log                   |
| 65 04/04/2012 01:46:40 NROMAN   | OFF C:\Users\vibranium\AppData\Local\Temp\_ME                          | 139242\spinlock.exe.manifest   | FN Info - Modify: 04/04/2012 01:46:40,                           | Entry: 04/04/201 MFT Entry              |
| 81 04/04/2012 15:07:33 NROMAN   | OFF C:\Users\vibranium\AppData\Local\Temp\_ME                          | 125602\spinlock.exe.manifest   | FN Info - Modify: 04/04/2012 15:07:33,                           | Entry: 04/04/201 MFT Entry              |
| 84 04/04/2012 17:04:44 TDUNGAI  | N C:\WINDOWS\system32\spinlock.exe                                     |                                | FN Info - Modify: 04/04/2012 17:04:44,                           | Entry: 04/04/201 MFT Entry              |
| 85 04/04/2012 17:06:37 TDUNGAI  | N C:\WINDOWS\system32\spinlock.exe                                     |                                | Executed: N/A  | ShimCache                               |
| 89 04/04/2012 18:28:42 CONTROL  | LER spinlock.exe   |                                | Windows Error Reporting  | Application Event Log                   |
| 92 04/04/2012 18:54:51 NROMAN   | OFF SPINLOCK.EXE-1610A75A.pf   |                                | Number of Time Run: 16   | Prefetch Entry                          |
| 93 04/04/2012 18:54:52 NROMAN   | OFF C:\Users\vibranium\AppData\Local\Temp\_ME                          | 129562\spinlock.exe.manifest   | FN Info - Modify: 04/04/2012 18:54:52,                           | Entry: 04/04/201 MFT Entry              |
| 100 04/05/2012 16:54:26 NFURY   | C:\Windows\System32\spinlock.exe                                       |                                | FN Info - Modify: 04/05/2012 16:54:26,                           | Entry: 04/05/201 MFT Entry              |
| 104 04/05/2012 17:15:57 TDUNGAI | N C:\WINDOWS\Prefetch\SPINLOCK.EXE-1F9810CF                            | .pf                            | FN Info - Modify: 04/05/2012 17:15:57,                           | Entry: 04/05/201 MFT Entry              |
| 105 04/05/2012 17:16:02 TDUNGAI | N C:\Documents and Settings\vibranium\Local Set                        | tings\Temp\_MEI122362\spinlc   | FN Info - Modify: 04/05/2012 17:16:02,                           | Entry: 04/05/201 MFT Entry              |
| 112 04/06/2012 13:25:01 TDUNGAI | N SPINLOCK.EXE-1F9810CF.pf   |                                | Number of Time Run: 4  | Prefetch Entry                          |
| 133                             |  |                                |  |   |
| H + > > Sheet1                  |  |                                | 4  | •                                       |
| Ready 17 of 131 records found   |  |                                |  |   |
|                                 |  |                                |  |   |

Figure 46. SPINLOCK.EXE keyword hits. (Lee, 2014, digital case files)

| 25  | <b>a</b> • • •   = 1   | S                                     |  | Stark_IOC_   | All_Modified.xlsx       | Microsoft Excel   |                                     |  | _ 🗆 🗙                      |
|-----|------------------------|---------------------------------------|--|--|-------------------------|---|-------------------------------------|--|----------------------------|
| F   | File Home Insert #     | o<br>Page Layout Forr                 | mulas Data Review                                    | View Team  |                         |   |                                     |  | a 🕜 🗆 🕼 🛙                  |
|     | Cut Calib              | - 11                                  | · A` A` = = =  | 🗞 - 📑 Wrap Text                                      | General +               | 🛃 📝 📝   | i= ik 🗊                             | Σ AutoSum * 🖅 🏦                            |                            |
| Pat | ste 🛷 Format Painter B | I <u>U</u> • <u>⊡</u> •               | <u>▲· ▲</u> · ■ ≡ ≡                                  | 🗱 🗱 🌆 Merge & Center *                               | \$ - % • 38.38          | Conditional Format Cell<br>Formatting * as Table * Styles * | Insert Delete Format                | Clear * Sort & Find &<br>Filter * Select * |                            |
|     | Clipboard 5            | Font                                  |  | Alignment  | Number G                | Styles  | Cells                               | Editing                                    |                            |
|     |                        |                                       |  |  |                         |   |                                     |  |                            |
|     | C102 👻 (*              | ∫ <sub>∞</sub> C:                     | \$Recycle.Bin\S-1-5-21                               | 1-2036804247-305832464                               | 0-2116585241-1673\      | \$R6SODDB\winclient.reg                                     |                                     |  | ~                          |
|     | C102 • (*              | ∫ <sub>×</sub> C:∖<br>B               | \$Recycle.Bin\S-1-5-21                               | 1-2036804247-305832464                               | 0-2116585241-1673\<br>C | \$R6SODDB\winclient.reg                                     |                                     | D  | ¥<br>4                     |
| 1   | A                      | В                                     | \$Recycle.Bin\\$-1-5-21                              | 1-2036804247-305832464                               | 0-2116585241-1673\<br>C |   | र<br>ग Properties                   | D  | v<br>▲<br>× Artifa         |
| 1   | A                      | B<br>Computer 👻                       | Details  | 1-2036804247-305832464                               | с                       |   |                                     | D<br>: 04/03/2012 00:35:10, Entry:         |                            |
|     | A<br>Date/Time         | B<br>Computer *<br>TDUNGAN            | Details<br>C:\WINDOWS\system                         |  | с                       |   |                                     | -  |                            |
| 40  | A Date/Time            | B<br>Computer<br>TDUNGAN<br>NROMANOFF | Details<br>C:\WINDOWS\system<br>C:\Users\vibranium\I | n32\dllhost\winclient.reg<br>Downloads\winclient.exe | с                       |   | FN Info - Modify<br>Executed: False | -  | : 04/03/201 MFT E<br>ShimC |

*Figure 47. WINCLIENT keyword hits. (Lee, 2014, digital case files)* 

| S  🛃 🤊 • 🥐 ·   =                     |                                 | Stark_IOC_All_Modified.xlsx - Microsoft Excel   | _ 🗆 >                     |
|--------------------------------------|---------------------------------|---|---------------------------|
| File Home Insert                     | -                               | mulas Data Review View Team   | a 🕜 🗖 🗗                   |
| Cut Cali<br>Paste ✓ Format Painter B | bri • 11<br><i>I</i> <u>U</u> • | · A · A       = = = ≫·       Wrap Text       General       Image: A = A = B = B = B = B = B = B = B = B = |                           |
| Clipboard 🕞                          | Font                            | Alignment G Number Styles Cells Editing   |                           |
| C87 -                                | ∫x C:                           | \Windows\PSEXESVC.EXE   |                           |
| A                                    | В                               | C D   |                           |
| 1 Date/Time -                        | Computer -                      | Details J Properties  | <ul> <li>Artit</li> </ul> |
| 1 04/03/2012 21:11:09                | NROMANOFF                       | C:\Windows\Prefetch\PSEXESVC.EXE-51BA46F2.pf FN Info - Modify: 04/03/2012 21:11:09, Entry                 | : 04/03/201 MFT           |
| 2 04/03/2012 21:14:56                | NROMANOFF                       | C:\Windows\PSEXESVC.EXE Executed: True  | Shir                      |
| 7 04/03/2012 21:19:52                | NROMANOFF                       | C:\Windows\PSEXESVC.EXE Executed: True  | Shir                      |
| 8 04/03/2012 21:19:53                | NROMANOFF                       | Service Name: PsExec %SystemRoot%\PSEXESVC.EXE  | Syst                      |
| 4 04/04/2012 01:46:37                | NROMANOFF                       | C:\Windows\PSEXESVC.EXE Executed: True  | Shir                      |
| 6 04/04/2012 01:48:01                | NROMANOFF                       | PsExec Service Control Manager  | App                       |
| 04/04/2012 14:37:19                  | NROMANOFF                       | PSEXESVC Service Control Manager  | App                       |
| 7 04/04/2012 18:00:44                | CONTROLLER                      | C:\Windows\PSEXESVC.EXE ProcessName   | Sec                       |
|                                      |                                 | C:\Windows\PSEXESVC.EXE FN Info - Modify: 04/04/2012 18:52:11, Entry                                      | : 04/04/201 MFT           |
|                                      |                                 | PSEXESVC.EXE-51BA46F2.pf Number of Time Run: 9  | Pref                      |
| 01 04/05/2012 17:07:15               |                                 | %SystemRoot%\PSEXESVC.EXE Service Control Manager   | App                       |
| 06 04/05/2012 17:23:04               |                                 | %SystemRoot%\PSEXESVC.EXE Service Control Manager   | App                       |
| 17 04/06/2012 18:09:48               |                                 | %SystemRoot%\PSEXESVC.EXE Service Control Manager   | App                       |
| .28 N/A                              | NROMANOFF                       | PsExec Service %SystemRoot%\PSEXESVC.EXE  | Auto                      |

*Figure 48. PSEXESVC.EXE keyword hits. (Lee, 2014, digital case files)* 

The capabilities of the adversary are also significant to know to defend and respond to the intrusion. Figure 48 has already shown that the intruder is likely using PSEXEC from Microsoft to assist in moving laterally. There is also evidence that the adversary is running malware through Scheduled Tasks (Figure 49) and is using the tool Mimiatz tool to steal user credentials (Figure 50).

| 7     | 0.0.1-          | n.    |                   |                            | Star             |               | lodified.xlsx | Microso                   | ft Evcel                 |                  |           |             |              |                              |      | _ 0           | ×    |
|-------|-----------------|-------|-------------------|----------------------------|------------------|---------------|---------------|---------------------------|--------------------------|------------------|-----------|-------------|--------------|------------------------------|------|---------------|------|
| File  |                 |       | Page Lavout For   | mulas Data Review          | View Team        | CIOC_AII_IV   | ioumeu.xisx   | - WICTOSO                 | IT EXCEI                 |                  |           |             |              |                              |      | a 🕜 🗖         |      |
| FIR   | Home Ins        | ert i | Page Layout For   | mulas Data Keview          | view learn       |               |               |                           |                          |                  |           |             |              |                              |      | ω 🕜 🗖         | 9° ' |
| Ĉ     | 🔏 Cut           | Calib | ori - 11          | - A* A* = = =              | 🏶 - 📑 Wrap Ter   | t Gener       | al            |                           |                          |                  | - 1       | × 🗊         | Σ AutoSum    | · 🆅 💣                        |      |               |      |
| Paste | Copy *          | в     | I <u>U</u> • 🔟 •  | <u>▲· ▲</u> · <b>≡</b> ≡ ≡ | 🗱 🗊 Merge &      | Center * \$ * | % • % .       | Conditional<br>Formatting | Format<br>• as Table • ! | Cell<br>Styles * | Insert De | lete Format | Clear *      | Sort & Find<br>Filter ▼ Sele |      |               |      |
|       | Clipboard 5     |       | Font              | 6                          | Alignment        | 6             | Number        |                           | Styles                   |                  | G         | ells        | Ð            | diting                       |      |               |      |
|       | C86             | + (*  | f <sub>x</sub> C: | \WINDOWS\Prefetch\         | AT.EXE-2770DD18  | pf            |               |                           |                          |                  |           |             |              |                              |      |               |      |
|       | A               |       | В                 |                            | С                |               |               |                           |                          |                  |           | D           |              |                              |      | E             |      |
| 1 [   | Date/Time       |       | Computer 👻        | Details                    |                  |               |               | JT Prope                  | erties                   |                  |           |             |              |                              | ~ A  | rtifacts      |      |
| 6 0   | 04/04/2012 17:2 | 4:44  | TDUNGAN           | C:\WINDOWS\Prefet          | ch\AT.EXE-2770DD | 18.pf         |               | FN In                     | fo - Modi                | fy: 04/(         | 04/2012 1 | 7:24:44, E  | ntry: 04/04/ | 2012 17:24                   | 44 N | AFT Entry     |      |
| 14 (  | 04/06/2012 13:4 | 1:09  | NROMANOFF         | AT.EXE-E3131BD4.pf         |                  |               |               | Numi                      | ber of Tim               | e Run:           | 9         |             |              |                              | P    | refetch Entry |      |
| 19 (  | 04/06/2012 18:5 | 5:35  | TDUNGAN           | AT.EXE                     |                  |               |               | Numi                      | ber of Tim               | e Run:           | 14        |             |              |                              | P    | refetch Entry |      |
| 30 N  | N/A             |       | NFURY             | Task Scheduler - \At1      |                  |               |               | "cmd                      | " /c c:\wi               | ndows            | system3   | 2\spinlock  | .exe         |                              | A    | utoruns       |      |
| 31 M  | A/A             |       | NFURY             | Task Scheduler - \At2      |                  |               |               | "cmd                      | " /c c:\wi               | ndows            | system3   | 2\dllhost\  | svchost.exe  |                              | A    | utoruns       |      |
|       | N/A             |       | Controller        | Task Scheduler - \At2      |                  |               |               | "cmd                      | " /c c:\wi               | ndows            | system3   | 2\spinlock  | .exe         |                              | A    | utoruns       |      |
| 32 1  |                 |       |                   |                            |                  |               |               |                           |                          |                  |           |             |              |                              |      |               |      |

Figure 49. Scheduled Tasks. (Lee, 2014, digital case files)

|                      | 🚽 🤊 • 🗠   = 💦 🙀   | 5  | Stark_IOC_AII_M  | Iodified.xlsx - Microsoft Excel  | - 🗆 🗙   |  |
|----------------------|---|--|--|--|---------|--|
| F                    | File Home Insert  | Page Layout Forr                             | mulas Data Review View Team  | 2  | x 🖷 🗕 🕜 |  |
| ľ                    | Calil   | bri v 11                                     | · A A ≡ ≡ 🕳 ≫ · 📑 Wrap Text Genera   | al 🔹 📑 📑 📑 🚰 🛄 🔀 AutoSum * 🔊 🖍   |         |  |
| Pas<br>*             |   | I <u>U</u> • <u> </u>                        | <u>∧</u> • <u>►</u> = = : : : : : : : : : : : : : : : : :  | % • *.*** **** Conditional Format Cell Insert Delete Format<br>Formatting * as Table * Styles * * * * * * * * * * * * * * * * * * *  |         |  |
|                      | Clipboard 5   | Font   | S Alignment S I  | Number 🕫 Styles Cells Editing  |         |  |
|                      | C9 v (* fr C/WINDOWS/system32/hydrakatz.exe v   |  |  |  |         |  |
|                      | A   | В  | С  | D  |         |  |
| 1                    | Date/Time 🔹   | Computer 💌                                   | Details  | T Properties Artifacts   | ¥       |  |
| 9                    | 04/03/2012 15:19:50   | TDUNGAN                                      | C:\WINDOWS\system32\hydrakatz.exe  | FN Info - Modify: 04/03/2012 15:20:27, Entry: 04/03/2012 15:20:27 MFT Entry  |         |  |
| 11                   |   |  |  | FN Into - Modity: 04/05/2012 15:20:27, Entry: 04/05/2012 15:20:27 MIFT Entry   |         |  |
|                      | 04/03/2012 15:30:13   | TDUNGAN                                      | C:\WINDOWS\system32\sekurlsa.dll   | FN Info - Modify: 04/03/2012 15:20:27, Entry: 04/03/2012 15:20:27 MIFT Entry<br>FN Info - Modify: 04/03/2012 15:30:13, Entry: 04/03/2012 15:30:13 MFT Entry  |         |  |
| 12                   | 04/03/2012 15:30:13<br>04/03/2012 15:33:20  |  | , .,   | FN Info - Modify: 04/03/2012 15:30:13, Entry: 04/03/2012 15:30:13 MFT Entry  |         |  |
|                      |   | TDUNGAN                                      | C:\WINDOWS\system32\sekurlsa.dll   | FN Info - Modify: 04/03/2012 15:30:13, Entry: 04/03/2012 15:30:13 MFT Entry  | y       |  |
| 45                   | 04/03/2012 15:33:20<br>04/03/2012 23:30:35  | TDUNGAN<br>TDUNGAN                           | C:\WINDOWS\system32\sekurlsa.dll<br>C:\WINDOWS\Prefetch\HYDRAKATZ.EXE-27B49502.p   | FN Info - Modify: 04/03/2012 15:30:13, Entry: 04/03/2012 15:30:13         MFT Entry           of         FN Info - Modify: 04/03/2012 15:33:20, Entry: 04/03/2012 15:33:20         MFT Entry   | y       |  |
| 45<br>59             | 04/03/2012 15:33:20<br>04/03/2012 23:30:35<br>04/04/2012 01:00:45   | TDUNGAN<br>TDUNGAN<br>NROMANOFF              | C:\WINDOWS\system32\sekurlsa.dll<br>C:\WINDOWS\Prefetch\HYDRAKATZ.EXE-27B49502.p<br>HYDRAKATZ.EXE-27B49502.pf  | FN Info - Modify: 04/03/2012 15:30:13, Entry: 04/03/2012 15:30:13         MFT Entry           of         FN Info - Modify: 04/03/2012 15:33:20, Entry: 04/03/2012 15:33:20         MFT Entry           Number of Time Run: 4         Prefetch Entry  | y       |  |
| 45<br>59<br>61       | 04/03/2012 15:33:20<br>04/03/2012 23:30:35<br>04/04/2012 01:00:45<br>04/04/2012 01:02:10                        | TDUNGAN<br>TDUNGAN<br>NROMANOFF<br>NROMANOFF | C:\WINDOWS\system32\sekurisa.dll<br>C:\WINDOWS\Prefetch\HYDRAKATZ.EXE-27B49502.p<br>HYDRAKATZ.EXE-27B49502.pf<br>C:\windows\system32\hydrakatz.exe                                     | FN Info - Modify: 04/03/2012 15:30:13, Entry: 04/03/2012 15:30:13         MFT Entry           of         FN Info - Modify: 04/03/2012 15:33:20, Entry: 04/03/2012 15:33:20         MFT Entry           Number of Time Run: 4         Prefetch Entry           Executed: True         ShimGache           FN Info - Modify: 04/04/2012 01:02:10, Entry: 04/04/2012 01:02:10         MFT Entry | y       |  |
| 45<br>59<br>61<br>62 | 04/03/2012 15:33:20<br>04/03/2012 23:30:35<br>04/04/2012 01:00:45<br>04/04/2012 01:02:10<br>04/04/2012 01:09:03 | TDUNGAN<br>TDUNGAN<br>NROMANOFF<br>NROMANOFF | C.\WINDOWS\system32\sekurlsa.dll<br>C.\WINDOWS\Prefetch\HYDRAKATZ.EXE-27B49502.p<br>HYDRAKATZ.EXE-27B49502.pf<br>C.\Windows\system32\hydrakatz.exe<br>C.\Windows\System32\sekurlsa.dll | FN Info - Modify: 04/03/2012 15:30:13, Entry: 04/03/2012 15:30:13         MFT Entry           of         FN Info - Modify: 04/03/2012 15:33:20, Entry: 04/03/2012 15:33:20         MFT Entry           Number of Time Run: 4         Prefetch Entry           Executed: True         ShimGache           FN Info - Modify: 04/04/2012 01:02:10, Entry: 04/04/2012 01:02:10         MFT Entry | ,<br>   |  |

Figure 50. Mimikatz artifacts. (Lee, 2014, digital case files)

### 6. Conclusion

Using Microsoft Excel in your investigation during an incident can help bring lots of different data sources together into one location with a standard format for quick and easy analysis of the data. It also allows the analyst to manipulate the data in ways that can bring out indicators of compromise missed when buried in unrelated events contained in the original log files. This paper only touched on a few of Microsoft Excel's features and capabilities. The more you can automate the processes involved in analyzing the data, the better the tool becomes. To take it to a higher level, consider learning more advanced concepts in programming in VBA and taking advantage of add-ins/plugins that Microsoft and third party entities offer that can expand the analysis of your data even further.

### 7. References

### References

Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional

- Carvey, H. (2014). Windows Forensic Analysis Toolkit, 4th Edition. Syngress
- Caswell, B., Beale, J., & Baker, A. (2007). Snort Intrusion Detection and Prevention Toolkit. Syngress

Cowen, D. (2013). Computer Forensic InfoSec Pro Guide. McGraw-Hill

Define and use names in formulas - Excel. (n.d.). Retrieved from https://support.office.com/en-us/article/Define-and-use-names-in-formulas-4d0f13ac-53b7-422e-afd2-abd7ff379c64

- Jelen, B., & Alexander, M. (2006). *Pivot Table Data Crunching*. Indianapolis, IN: Que Publishing
- Lee, R. (2014). SANS Forensic 508 Advanced Computer Forensic Analysis and Incident Response, Stark Research Labs Intrusion: Exercise Workbook.

Microsoft Excel. (n.d.). In Wikipedia. Retrieved November 18, 2016, from https://en.wikipedia.org/wiki/Microsoft\_Excel#Macro\_programming

- Nemeth, E., Snyder, G., Hein, T., & Whaley, B. (2010). Unix and Linux System Administration Handbook, Fourth Edition. Prentice Hill
- Parisi, T. (2015, June 17). *Caching out: The value of shimcache for investigators « Threat Research Blog | FireEye Inc.* Retrieved from https://www.fireeye.com/blog/threat-research/2015/06/caching out the val.html
- Roesch, M. (2003). *Network intrusion detection system mode* | *NIDS mode output options*. Retrieved from http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node6.html
- Russinovich, M., & Margosis, A. (2011). Windows Sysinternals Administrator's *Reference*. McGraw-Hill
- Windows event log essentials Windows event log FAQ. Basic explanation of Windows event logs. (n.d.). Retrieved from

https://eventlogxp.com/essentials/windowseventlog.html

### 8. Appendix

### 8.1. Appendix A - Open Source Tools

Here is a listing of the tools used in this document:

- NOTEPAD++, v7.3.2 (https://notepad-plus-plus.org/)
- Shellbags Explorer, v0.7.0.0 (http://binaryforay.blogspot.com/p/software.html)
- Bro, v2.5 (https://www.bro.org/)
- Snort, v2.9.9.0 (https://www.snort.org/)
- IPTables, v1.6.1 (https://git.netfilter.org/iptables/)
- Wevtutil.exe, v6.1.7600.16385 (Native Windows 7 tool)
- Autorunsc.exe, v13.7 (https://technet.microsoft.com/en-us/sysinternals/bb842062)
- Shimcacheparser.py, v1.0 (https://github.com/mandiant/ShimCacheParser)
- Pasco.exe, v1.0 (https://www.mcafee.com/us/downloads/free-tools/pasco.aspx)
- analyzeMFT, v2.0.18 (https://github.com/dkovar/analyzeMFT)
- parse\_prefetch\_info, v1.5 (http://redwolfcomputerforensics.com dead link)
- Wireshark, v2.2.4 (https://www.wireshark.org/)
- CYGWIN, v2.7.0. (https://www.cygwin.com/)

Within CYGWIN Environment:

- o SED https://www.gnu.org/software/sed/
- CUT part of https://www.gnu.org/software/coreutils/coreutils.html
- $\circ \quad CAT-part \ of \ https://www.gnu.org/software/coreutils/coreutils.html$

### 8.2. Appendix B – Resources

Here is a listing of books and blog web sites that I have found beneficial in learning Excel and VBA Programming:

- Excel 2013 Power Programming with VBA by John Walkenback
- Excel 2013 Bible by John Walkenback
- http://analysistabs.com/
- https://powerspreadsheets.com/
- http://stackoverflow.com/
- http://wellsr.com/
- https://www.ablebits.com/
- http://www.mrexcel.com/
- https://www.techonthenet.com/excel/index.php
- https://www.thespreadsheetguru.com

### 8.3. Appendix C – Files Available on GitHub

I have provided code to automate much of the processes described in this document. If there are issues running the code, check to make sure you are using the same version of software listed in Appendix A.

The VBA code is separated up into two categories. One category contains individual code for each of the log files mentioned in this document along with a few miscellaneous scripts for specific tasks. The other category contains two 'Master' spreadsheets that comprise many of the individual scripts into one document for ease of execution. You can find the code at https://github.com/gregory-lalla/GCIH\_Gold under the 'Code' directory. Each category has two sub-categories. The sub-categories are explained below.

### **Module Files:**

The files under this sub-category are individual modules that can be added to macro-enabled spreadsheets (see Section 3.5 for directions on adding macros to a spreadsheet). You can find the code at GitHub site under the Code/Singles/Module\_BAS\_Files directory. Each log file has code designed specifically for the output shown in this paper. There are four types of modules. The first type will search the data for specific keywords and will have the word 'keyword' in the file name. The second type will search the data for specific Event IDs and will have the word 'EventID' in the file name. The third type will format the data per the instructions provide in this paper and will contain the words 'Standard\_Format' in the file name. The last type will be code which is designed to perform a specific task and will not have any of the words mentioned above in the file name. The following is a list of the task specific macros and a description of each:

• Binary\_Hex2Ascii\_Conversion\_Module:

This script will convert a column of hexadecimal encoded characters to human readable ASCII encoding. This script will work on an XML export of Microsoft Event Viewer data.

• Insert\_Headers\_Module:

This script will insert the standard headers described in this paper to the spreadsheets first row.

- EventLogs\_Application\_CSV\_Unique\_IDs\_per\_Sheet\_Module: This script will take each unique Event ID and create an individual spreadsheet (tab) containing only those Event IDs. This script will work on a CSV export of Microsoft Event Viewer Application log data.
- EventLogs\_Security\_CSV\_Unique\_IDs\_per\_Sheet\_Module:

This script will take each unique Event ID and create an individual spreadsheet (tab) containing only those Event IDs. This script will work on a CSV export of Microsoft Event Viewer Security log data.

• EventLogs\_System\_CSV\_Unique\_IDs\_per\_Sheet\_Module:

This script will take each unique Event ID and create an individual spreadsheet (tab) containing only those Event IDs. This script will work on a CSV export of Microsoft Event Viewer System log data.

#### **Macro Files:**

The files under this sub-category also contain individual scripts designed specifically for each log file. The scripts here, however, are contained within a Macro-enabled Excel file. There is a button on the first spreadsheet that will prompt the user to specify the log file they wish to process. The script will then run and produce a unique output file name based on the hostname that produced the log. These Excel files contain the same types of scripts mentioned above, except there are no task-specific modules for hexadecimal to ASCII conversion or inserting of headers. You can find the code at the GitHub site under the Code/Singles/Excel Macro Files directory.

#### **Singles Combined:**

The file under this sub-category is named 'Master-Single.xlsm' and combines all the code from the Macro Files sub-category. Each log file has its own button that when pushed will run the same code as the Macro Files sub-category. This file is available on the GitHub site at https://github.com/gregory-

lalla/GCIH\_Gold/blob/master/Code/Combined/Singles\_Combined/Master -Single.xlsm.

#### Master IOC Combined:

The file under this sub-category is named 'Master-IOC.xlsm' and has two differences from the 'Master-Single.xlsm' document. First, the result of the script not only writes to a unique file, but is appended to an overall Master IOC Excel file. When opening the document, the user is prompted to either select a previously created Master IOC file or to create a new one. This file is then used to hold the results of all the scripts run. The other difference is that instead of a standard format button, there is a button to filter the results of each log file by date to remove data that is outside the timeframe of an incident. This file is available on the GitHub site at https://github.com/gregory-

lalla/GCIH\_Gold/blob/master/Code/Combined/Master\_IOC\_Combined/M aster-IOC.xlsm.

There is also a documents directory located at https://github.com/gregorylalla/GCIH\_Gold/blob/master/Docs with several subdirectories. The 'Supplement' subdirectory contains a document named

'Additional\_Log\_Formatting\_Instructions.docx' which covers instructions for formatting the logs mentioned in Section 4.2 of this paper. It also contains a file named 'Pivote\_Table\_Example.docx' which shows examples of the content discussed in Section 3.6 of this paper. Last, there is a file named

'Complete\_GIAC\_GCIH\_Gold\_Paper\_Greg\_Lalla.docx' which is the original document before it was edited to fit the requirements of a GIAC Gold Paper (Because of file size limits on Github, the document has been compressed and split into three files. You can recombine the compressed files with 7-zip). The 'Template' subdirectory contains an Excel Macro-Enabled Template named 'standard\_format.xltm' you can use when manipulating data from log files not discussed in this paper. The last subdirectory in the 'Docs' folder is 'Worksheet\_Functions.' This folder contains a document named 'Worksheet\_Functions\_in\_Paper.docx' which contains the worksheet functions used in this paper, along with a description of what each one accomplishes.

The last directory at the root of the GitHub page is named 'Misc' and contains the SED script file named 'months.sed,' which fixes the Date/Time fields of Linux system

logs. You can find the SED script at https://github.com/gregory-

lalla/GCIH\_Gold/blob/master/Misc/SED\_Month\_Replacement\_Filter/months.sed.

### 8.4. Appendix D: Windows Logs Explained

For brevity, anything discussed previously will be not be explained again but only referenced.

### 8.4.1. Event Viewer Logs

Because Event Viewer logs can contain hundreds of thousands of entries, it is essential to reduce the data to a manageable level before importing it into Excel. One way to do this is to use XML filtering in Event Viewer Custom Views which is more efficient than filtering through the GUI. There are many types of expressions you can use, but two of the more useful are sorting by timeframe and sorting by a username (See Figure 51 and 52). For more information about XML filtering, see the article at

https://blogs.technet.microsoft.com/askds/2011/09/26/advanced-xml-filtering-in-the-windows-event-viewer/.

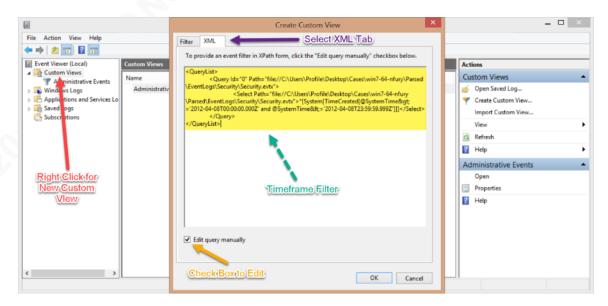


Figure 51. Event Viewer XML Timeframe Filter. (Lee, 2014, digital case files)

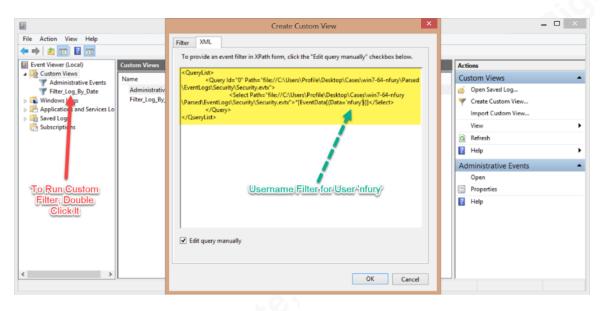


Figure 52. Event Viewer XML Username Filter. (Lee, 2014, digital case files)

An even easier method, avoiding the slow GUI, is to use the native command line utility called WEVTUTIL.EXE to export the logs. This tool comes with its challenges such as producing XML files that Excel cannot open. When running the command, there are several options to massage the data to a format that Excel accepts. To get the correct results, you may need to mix and match the switches until you get an XML file that imports into Excel. Here is an example of a command that you can run which filters the data based on a timeframe:

### wevtutil qe "<path\_to\_system.evtx>" /lf:true /q: "\*[System[TimeCreated[@SystemTime>='2015-07-10T00:00:00.000Z' and @SystemTime<='2015-07-13T23:59:59.999Z']]]" /f:RenderedXML /e:root > System.xml

A final way to get the output you want from Event Viewer logs is to use Powershell, which is a topic beyond this paper, but well worth the effort to try and learn.

Once you have reduced the data, you should then export it from the utility. Event Viewer offers four different formats to export the data: .EVTX, .TXT, .CSV, and .XML (See Figure 33). This paper will look at the .CSV format and the .XML format. Neither of these formats includes all the information from the Event Viewer logs, and the data may need to be combined to get a full picture of what occurred during each event.

|  |  | Event Viewer   |  | _ 🗆 🗙   |
|--|--|--|--|---|
| 4  | Save As  | ×  |  |   |
| 🛞 🍥 👻 🕆 👗 > This PC > Local Disk (   | (C:) <   | rch Local Disk (C:)  |  | Actions   |
| Organize 👻 New folder  |  | 1 🖬 👻 🔞  |  | Filter_Log_By_Date  |
| This PC     Cases     Desktop     Documents     Music     Pictures     Videos     Local Disk (Ci)  | ram Files 10/10/2014<br>12/05/2016<br>08/22/2013<br>10/09/2014 | 11/200         File folder           12/201         File folder           14/433         File folder           14/455         File folder           12/200         File folder           12/200         File folder           12/200         File folder           12/201         File folder           12/202         File folder           12/2025         File folder | t ID Task Category<br>1674 Sensitive Privile<br>1674 Sensitive Privile<br>1672 Cascitive Brivile<br>X<br>X |   |
| Image: Save as type:     Event Files (*.evta)       File name:     Save as type:       Save as type:     Event Files (*.evta)       Image: Save as type: Sav | (#8) 12/07/2016  | 522:19 File folder v   | Save Filtered<br>Events<br>selecal   | Attach Task To This Custom View<br>View  Celete Rename Refresh Help Event 4674, Microsoft Window  V |

#### Figure 53. Save Filtered Event Viewer logs. (Lee, 2014, digital case files)

In this section, two event logs are shown, each with a slightly different output. With these two examples, you can manipulate other Event Viewer logs in a similar manner. First, the Security.evtx log, when exported as a .CSV file produces cells with newline and carriage returns, which makes the data unwieldy. You will remove the carriage return character (ASCII Code 13), and replace the newline character (ASCII Code 10) with the '#' character which will be used as a delimiter to split the data into columns. You can automate this task with the following Excel Function:

#### =SUBSTITUTE(SUBSTITUTE(F2,CHAR(13),""),CHAR(10),"#")

Place the above function in an empty cell adjacent to the cell that needs to have the newline and carriage return characters replaced (Figure 54). The blank cell will then contain the new contents as its value, but will also contain the formula used in the function.

| 83  | <b>.</b> | × - □   =                                      | Security_Function.xlsx - Micro   | osoft Excel 💶 🗖 🗙  | ×          |
|-----|----------|--|--|--|------------|
|     | ile H    | ome Insert Page Layout                         | Formulas Data Review View Developer Team   | a 🕜 🗗 🖗  | 23         |
| Nor | Layout   | Page Break Custom Full<br>Preview Views Screen | Kuler V Formula Bar     Zoom 100% Zoom to New Arrange Freeze Hide     Gridlines Z Headings     Zoom 100% Zoom to New Arrange Freeze Hide   | Unter Side by Side<br>Synchronous Stratiling<br>Save Switch<br>Werkspace Windows - Macros  |            |
| E   | 62       |  | =SUBSTITUTE(SUBSTITUTE(F2,CHAR(13),""),CHAR(10),"#")   | Indow Macros   |            |
|     | D        | E  | 308311012(308311012(12);CIAR(13); 7,CIAR(10); # )  | G H I  |            |
| 1   | -        | Task Category                                  |  |  | 10         |
|     |          |  | An operation was attempted on a privileged object. Subject: Security ID-LOCAL SERVICE Account Domain:NT AUTHORITY Logon ID:0x3E5 Object: Object: Object:SA Object Server:LSA Object Type:- Object Name:- Cheven of the content of the c | Excel Function to Replace<br>Newline (CHAR(13)) and<br>Carriage Returns (CHAR(10))<br>with a # Character to Act as<br>a Delimiter  |            |
| 2   | 4674     | Sensitive Privilege Use                        | Object Handle:DxD<br>Process Information:<br>Process ID:Dx228<br>Process Name:C:\Windows\System32\Isass.exe<br>Requested Operation:<br>Desired Access:1677216<br>Privileges:SaSacurityPrivilege  | An operation was attempted on a privileged<br>object.##Subject.#Security ID:LOCAL SERVICE#Account<br>Name:LOCAL SERVICE#Account Domain:NT<br>AUTHORITY#Logon ID:0x365##D0ject.#D0ject<br>Server:LSA#Object Type::#Object Name:#Object<br>Handle::\DifferProcess Information:#Process ID 0x228#Process<br>Name:C_\Window:System32\sss.exe##Requested<br>Operation:#Desired<br>Access:1677216#Privileges:SeSecurityPrivilege |            |
|     |          | ecurity 🔔                                      | A  |  | , <b>*</b> |
| Rea | dy 🛅     |  |  | la 🖂 🖂 💭 🕹   | Ð          |

Figure 54. Remove Newline and Carriage Return Characters from Cell Contents. (Lee, 2014, digital case files)

To produce a similar result in every cell in the column, highlight the cell with the function and double-click on the bottom right-hand corner of the cell. This action will copy the function to every cell in the column. The arguments used by the function will be updated to reflect the correct cell locations (Figure 55).

| 16            | 9.0                  | - 🗋 📼                   | Security_Function.xlsx - Microsoft Excel  |              |
|---------------|----------------------|-------------------------|---|--------------|
| File<br>Paste | Hor<br>K Cut<br>Cupy | Calibri - 1             | Hormulas Data Review View Developer Learn<br>11 - A' A' = = - ⊗ - Constrained<br>1 - A' A' = = = E E E Marganian Strained & Constrained Format Coll Insert Deter Format Coll Insert Deter Format Coll Insert Deter Format Coll Constrained Format Coll Insert Deter Format Coll In | ئ ص 🚱 ھ      |
|               | Clipboard            | 5 Font                  | Celes      Alignment      Number      Subler Styles     Cels     Editing  |              |
|               | G2                   | ▼ (*                    | =SUBSTITUTE(SUBSTITUTE(F2,CHAR(13),""),CHAR(10),"#")  |              |
| 4             | D                    | E                       | F G   |              |
| E             | vent ID              | Task Category           |   |              |
| 2             |                      | Sensitive Privilege Use | Account Name:LOCAL SERVICE Account Domain:NT AUTHORITY Logon ID:0x355 Object: Object Server:LSA Object Type:- Object Type:- Object Handle:Dx0 Process Information: Process Information: Process ID:0x228 Process Name:C:\Windows\System32\sass.exe Requested Operation: Requested Operatio    |              |
|               |                      | ecurity શ               |   |              |
| ady           | 2                    |                         |   | 100% 😑 — 🖓 ( |

Figure 55. Copy Function to All Cells in Column. (Lee, 2014, digital case files)

To prevent the function from being accidently changed and to make it easier to manipulate the contents of the cell, the values within the new cells will be copied and

pasted over the formula. To perform this action, select the entire column that contains the functions, right click the highlighted cells, select 'Copy,' right click the highlighted cells again and select the 'Paste Value' icon which has the numbers 123 in the image (Figure 56).

| 🔁 📑 🐐  | - 🗆 🗙      |
|--|------------|
| Hie Home Insert PageLayout Formulas Data Review View Developer Learn   | 23 🖬 🖬 🚱 a |
| Image: |            |
| Normal Page Page Ricak Custom Full 📝 Gridilives 🕼 Headings<br>Layout Preview Views Screen  |            |
| Workbook Views Show Zoom Window Macros   |            |
| G2 v fsc =SUBSTITUTE(SUBSTITUTE(F2,CHAR(13),"*),CHAR(10),"#")  | *          |
| D E F Calibri - 11 - A A S - % - 30  | A          |
| 1 Event ID Task Category B / = 🚴 🛆 👘 🐄 🕹 🚽   | -          |
| An operation was attempted on a privileged object.   |            |
|  |            |
| Subject:   |            |
| Security ID:LOCAL SERVICE Page Options:  |            |
| Account Name: LOCAL SERVICE  |            |
| Account Domain VI AD HORITY  |            |
|  |            |
| Object: Linear Capied Calls.   |            |
| Object Server: LSA   |            |
| Object Type;- Clear Cogtents   |            |
| Object Name:- Filter > Paste Value   |            |
| Object Handle:0x0 An operation w Sart > (2)  |            |
| object.##Subject 🔤 Insert Comment Count  |            |
| Process Information: Name:LOCAL SE   |            |
| Process ID:0x228 AUTHORITY#Log   |            |
| Process Name:C:\windows\system32\isass.exe iserver:LSA#Obje  |            |
| Handle.oxometric   |            |
| Requested Operation: Name:C:\Windo 🐘 Hyperlink.sted Desired Access:16777216 Operation:#Desired   |            |
| 2 4674 Sensitive Privilege Use PrivilegesSescurityPrivilege (Access:1677/216)  |            |
|  | <b>v</b>   |
| H (+) H Security 2   |            |
| Select destination and press PNTFR or chaose Paste   | ∋          |

Figure 56. Copy and Paste Value of cell over the Function in the cell. (Lee, 2014, digital case files)

With the data copied to a new column in the correct format, you can delete the original column. Since the new column has a delimiter of '#' in the data, the 'Text to Column' feature on the 'Data' ribbon can be used to separate the data into multiple columns (Figure 57).

| 🔀 🔚 🔿 + 🕐 + 🛄 =  | Security_Function.xlsx - Micro  | osoft Excel – 🗆 🔺  |
|--|---|--|
| File Home Insert Page Layout F                               | ormulas Data Review View Developer Team   | Text to Columns Icon 3   |
| From From From Other<br>Access Web Text Sources* Connections | Convections<br>Properties<br>Refer was Edit Links<br>Convections<br>Refer was Edit Links<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections<br>Convections | Censolidate What If Group Ungroup Subtrotal<br>Analysis  |
| Get External Data  | Connections Sort & Filter Data Tools  | Outline 5  |
| G1 ▼ (^∫_*   |   |  |
| D E  | F   | G  |
| 1 Event ID Task Category                                     | An operation was attempted on a privileged object.  |  |
| Data Tab   | Subject:<br>Security ID:LOCAL SERVICE<br>Account Domain:NT AUTHORITY<br>Logon ID:XAES<br>Object:<br>Object Server:LSA<br>Object Type:-<br>Object Mame:-<br>Object Handle:DxO  | An operation was attempted on a privileged<br>object.##Subject.#Security ID:LOCAL SERVICE#Account          |
|  | Process Information:  | Name:LOCAL SERVICE#Account Domain:NT   |
|  | Process ID:0x228  | AUTHORITY#Logon ID:0x3E5##Object:#Object   |
|  | Process Name:C:\Windows\System32\Isass.exe  | Server:LSA#Object Type::#Object Name::#Object<br>Handle:0x0##Process Information:#Process ID:0x228#Process |
|  | Requested Operation:  | Handle:UxU##Process Information:#Process ID:Ux228#Process<br>Name:C:\Windows\System32\Isass.exe##Requested |
|  | Desired Access:16777216   | Operation:#Desired   |
| 2 4674 Sensitive Privilege Use                               | Privileges:SeSecurityPrivilege  | Access:16777216#Privileges:SeSecurityPrivilege   |
| H 4 > H Security   | A   |  |
| Ready Calculate 🔚  |   | Count: 952 🔠 🗖 🛄 100% 🕞 – 🤇 🛨  |

Figure 57. Text to Columns. (Lee, 2014, digital case files)

On the 'Text to Columns' wizard, select the defaults on Step 1 and 3. On 'Convert Text to Columns Wizard – Step 2 of 3' only check 'Other:' under 'Delimiters.' In the box next to 'Other:' type the '#' character. Also, make sure the 'Treat consecutive delimiters as one' checkbox is unchecked to keep data of a similar nature in the same columns (Figure 58).

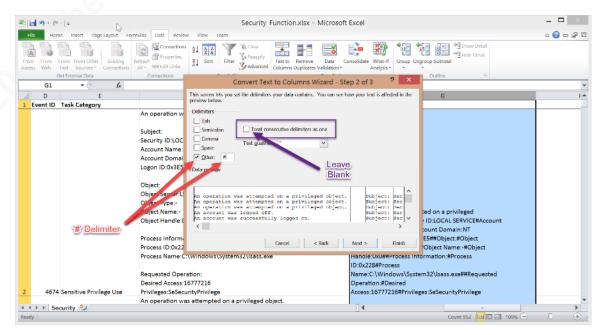


Figure 58. Text to Columns Delimited (Lee, 2014, digital case files)

The result should look like Figure 59 after 'Wrap Text' has been removed from the worksheet cells.

| 🔊 🚽 🖉 - 🖉 📄 🚽                  | Securit   | y_Function.xlsx - Microsoft Excel      |   |
|--------------------------------|---|--|---|
| File Home Insert Pag           | e Layout Formulas Data Review View Developer Team   |  | a 🕜 🗆 🧉   |
| Cut Calibri                    | - 11 - <b>A</b> <sup>*</sup> <b>A</b> <sup>*</sup> ≡ = → Wrap Text G                      | eneral 🗸 🛃 📑 📑                         | K I AutoSum * 🎢 👬   |
| aste<br>→ ✓ Format Painter B I | <u>U</u> ×   <u>→</u> × <u>→</u> × <u>→</u> × ≡ ≡ ≡   ; ; ; ; <u>→</u> Merge & Center × ! | * % * ******************************** | te Format<br>Clear * Sort & Find &<br>Filter * Select *     |
| Clipboard 5                    | Font 🕫 Alignment 🕫  | Number 5 Styles Cell                   | ls Editing  |
| F2 👻 🕤                         | $f_{\rm sc}$ An operation was attempted on a privileged object.                           |  |   |
| E                              | F   | G                                      | H I J K L   |
| Task Category                  |   |  |   |
| Sensitive Privilege Use        | An operation was attempted on a privileged object.  | Subject:                               | Security IE Account N Account D Logon ID:( Object           |
| Sensitive Privilege Use        | An operation was attempted on a privileged object.  | Subject:                               | Security IE Account N Account D Logon ID:( Object           |
| Sensitive Privilege Use        | An operation was attempted on a privileged object.  | Subject:                               | Security IE Account N Account D Logon ID:( Object           |
| Logoff                         | An account was logged off.  | Subject:                               | Security IE Account N Account D Logon ID:( Logon            |
| Logon                          | An account was successfully logged on.  | Subject:                               | Security IE Account N Account D Logon ID:(Logon             |
| Special Logon                  | An account was successfully logged on.  | Subject:                               | Security IE Account N Account D Logon ID:( Logon            |
| Logoff                         | Special privileges assigned to new logon.   | Subject:                               | Security IE Account N Account D Logon ID:(Privile           |
| Logon                          | An account was logged off.  | Subject:                               | Security IE Account N Account D Logon ID:( Logon            |
| 0 Special Logon                | An account was successfully logged on.  | Subject:                               | Security IE Account N Account D Logon ID:( Logon            |
| 1 Logon                        | Special privileges assigned to new logon.   | Subject:                               | Security IE Account N Account D Logon ID:( Privile)         |
| 2 Logoff                       | A logon was attempted using explicit credentials.   | Subject:                               | Security IE Account N Account D Logon ID: (Logon            |
| 3 Logon                        | An account was logged off.  | Subject:                               | Security IE Account N Account D Logon ID: (Logon            |
| Special Logon                  | An account was successfully logged on.  | Subject:                               | Security IE Account N Account D Logon ID:( Logon            |
| 5 Logon                        | Special privileges assigned to new logon.   | Subject:                               | Security IE Account N Account D Logon ID:( Privile)         |
| 6 File System                  | A logon was attempted using explicit credentials.   | Subject:                               | Security IE Account N Account D Logon ID:( Logon            |
| 7 File System                  | The state of a transaction has changed.   | Subject:                               | Security IE Account N Account D Logon ID:(Transa            |
| 8 File System                  | The state of a transaction has changed.   | Subject:                               | Security IE Account N Account D Logon ID:(Transa            |
| 9 File System                  | The state of a transaction has changed.   | Subject:                               | Security IE Account N Account D Logon ID:( Transa           |
| 0 Sensitive Privilege Use      | The state of a transaction has changed.   | Subject:                               | Security IE Account N Account D Logon ID:(Transa            |
| 1 Sensitive Privilege Use      | An operation was attempted on a privileged object.  | Subject:                               | Security IE Account N Account D Logon ID:( Object           |
| 2 Sensitive Privilege Use      | An operation was attempted on a privileged object.  | Subject:                               | Security IE Account N Account D Logon ID:( Object           |
| Security 😓                     | An encodered and address and an encodered address   | Cubicati                               | Consider IE A constant NI A constant D I constant D Cohicot |
| eady 🛅                         |   |  | ■ □ □ 100% (-)((  |

Figure 59. Text to Columns Result. (Lee, 2014, digital case files)

These actions should line up most of the data correctly, but you will find there are some columns with extra data or missing data. Here you'll need to do some manual work to get the data correctly aligned. First, run the Standard Format macro to better view the data. You need to keep in mind the data you want to retain, relative the Column Header names. Of the five headers already present, keep the 'Date and Time'; 'Source'; and 'Event ID' columns. The other two columns can be deleted (Figure 60).

|          | <b>-</b> | @ - ]]  -                | Ŧ                     |           |                  |         |      |     |        |               | Sec      | curity  | Fui  | nctio | on.xls | 5x - | Micr           | osoft E               | kcel   | I        |                    |             |            |   |             |        | _ 0                | ×      |
|----------|----------|--------------------------|-----------------------|-----------|------------------|---------|------|-----|--------|---------------|----------|---------|------|-------|--------|------|----------------|-----------------------|--------|----------|--------------------|-------------|------------|---|-------------|--------|--------------------|--------|
|          | File H   | Home Ins                 | sert Pa               | ige Layou | : Fo             | rmulas  | Da   | ita | Review | Vi            | iew      | Devel   | oper | Tea   | m      |      |                |                       |        |          |                    |             |            |   |             |        | a 🕜 =              | - @ 23 |
| ľ        | ₿.₩      | Calibri                  | Ŧ                     | 11 -      | λ Λ <sup>*</sup> | = ;     | =    | *   | · •    | <b>≣</b> • w  | Vrap Te  | ext     | 0    | Sener | al     |      | Ŧ              |                       |        |          |                    | ÷           |            |   | AutoSum     | Ż      | ñ                  |        |
| Pa       | ste 🝼    | В І Ц                    | <u>U</u> •   <u>—</u> | *   🏄 ·   | <u>A</u> *       | <b></b> | E I  | 1   | •      | • <b>a•</b> N | lerge 8  | & Cente |      | \$-   | % *    | 1    | .0 <b>.</b> 00 | Conditio<br>Formattir | ng • a |          | Cell<br>• Styles • | Insert<br>• | Delet<br>* | * | <br>Clear • |        | Find &<br>Select • |        |
| Clip     | board 🕞  |                          | Font                  |           | F3               |         |      |     | lignme |               |          |         | Γs.  |       | Numbe  | er   | G.             |                       | S      | ityles   |                    |             | Cells      | ; | E           | liting |                    |        |
| -        | D5       | 5                        | <b>•</b> (*           |           | f∞ A             | n acco  | ount | was | ogge   | d off         | <u> </u> |         |      |       |        |      |                |                       |        |          |                    |             |            |   |             |        |                    | 4      |
|          |          | А                        |                       |           |                  | В       | 1    |     |        |               |          | С       |      |       |        |      |                |                       |        |          |                    |             |            |   |             |        |                    |        |
| 1        | Date ar  | nd Time                  | ⊻ S                   | ource     |                  |         |      |     |        | ٣             | Ever     | nt ID   |      |       |        |      |                |                       |        |          |                    |             |            |   |             |        |                    |        |
|          | 04/00/   | 2012 11                  | 10.07 1               | 4         |                  |         | -    |     | -      |               |          |         |      |       |        |      |                | empted                |        |          |                    |             |            |   |             |        |                    |        |
| 3        |          | 2012 11:                 |                       |           |                  |         |      |     |        | -             |          |         |      |       |        |      |                | empted                |        |          |                    |             |            |   |             |        |                    |        |
| 4        |          | 2012 11:                 |                       |           |                  |         |      |     |        | -             |          |         |      | _     |        |      |                | empted                | on     | a priv   | leged c            | bject.      |            |   |             |        |                    |        |
| 5        |          | 2012 11:                 |                       |           |                  |         |      |     |        |               |          |         |      |       |        |      |                | ed off.               |        |          |                    |             |            |   |             |        |                    |        |
| 6        |          | 2012 11:                 |                       |           |                  |         |      |     |        | -             |          |         |      |       |        |      |                | essfully              |        |          |                    |             |            |   |             |        |                    |        |
| 7        |          | 2012 11:                 |                       |           |                  |         |      |     |        | -             |          |         |      |       |        |      |                | essfully              |        |          |                    |             |            |   |             |        |                    |        |
| 8        |          | 2012 11:                 |                       |           |                  |         |      |     |        |               |          |         |      |       |        |      |                | igned to              | nev    | N logo   | n.                 |             |            |   |             |        |                    |        |
| 9        |          | 2012 11::                |                       |           |                  |         |      |     |        | -             |          |         |      |       |        |      |                | ed off.               |        |          |                    |             |            |   |             |        |                    |        |
| 10       |          | 2012 11:                 |                       |           |                  |         |      |     |        |               |          |         |      |       |        |      |                | essfully              |        |          |                    |             |            |   |             |        |                    |        |
| 11       |          | 2012 11::                |                       |           |                  |         |      |     |        |               |          |         |      |       |        | -    |                | igned to              |        | -        |                    |             |            |   |             |        |                    |        |
| 12       |          | 2012 11:                 |                       |           |                  |         |      |     |        | -             |          |         |      |       |        |      |                | ed using              | exp    | pilcit c | reaenti            | ais.        |            |   |             |        |                    |        |
| 13       |          | 2012 11:                 |                       |           |                  |         |      |     |        |               |          |         |      |       |        |      | 00             | ed off.               |        |          |                    |             |            |   |             |        |                    |        |
| 14       |          | 2012 11:                 |                       |           |                  |         |      |     |        |               |          |         |      |       |        |      |                | essfully              |        |          |                    |             |            |   |             |        |                    |        |
| 15<br>16 |          | 2012 11::<br>2012 11::   |                       |           |                  |         |      |     |        | -             |          |         |      |       |        |      |                | igned to              |        |          |                    | -1-         |            |   |             |        |                    |        |
| 10       |          |                          |                       |           |                  |         |      |     |        | •             |          |         |      | -     |        |      |                | ed using<br>ction ha  |        |          |                    | ais.        |            |   |             |        |                    |        |
| 17       |          | '2012 11::<br>'2012 11:: |                       |           |                  |         |      |     |        |               |          |         |      |       |        |      |                | ction na<br>ction ha  |        |          |                    |             |            |   |             |        |                    |        |
| 18       |          | 2012 11:                 |                       |           |                  |         |      |     |        |               |          |         |      |       |        |      |                | ction ha              |        |          |                    |             |            |   |             |        |                    | -      |
| H        |          | Security                 |                       |           |                  |         | et   |     |        |               |          |         |      | .e al |        |      |                |                       | •      |          |                    |             |            |   |             |        |                    | •      |
| Rea      | idy 🛅    |                          |                       |           |                  |         |      |     |        |               |          |         |      |       |        |      |                |                       |        |          |                    |             |            |   | 100% 😑      |        | 0                  | -+     |

Figure 60. Keep the 'Date and Time' column and 'Event ID' column. (Lee, 2014, digital case files)

Change the 'Date and Time' column header to 'Date/Time,' the 'Source' header to 'Artifact' and the 'Event ID' header to 'Properties.' To understand what the value of the cells under 'Properties' represent, prefix each cell with the string 'Event ID: ' (Figure 61). You can do this by using the following function:

| 3            | 🄊 • (° • 🗋   👳 |                            |                     | Security_F      | unction.xlsx   | Microsoft Excel – 🗖   | ×     |
|--------------|----------------|----------------------------|---------------------|-----------------|----------------|---|-------|
| File         | Home Inser     | t Page Layout F            | ormulas Data Review | w View Develope | er Team        | a 🕜 =   | - @ X |
|              | Calibri        | - 11 - <b>A A</b>          | · = = = »··         | Wrap Text       | General        | ▼         ↓ |       |
|              | →              |                            |                     |                 |                | Formatting * as Table * Styles * * * * Filter * Select *  |       |
| lipboard     |                | Tone                       | Alignm              | ent 🕞           | Number         | Function to Prefix Cells Editing  |       |
|              | D2             | • (* <b>f</b> *            | ="Event ID: "&C2 🚽  |                 |                | String to Cell Data   | 1     |
|              | A              |                            | В                   | С               | D              | Carrig to Constraint  |       |
|              | te and Time    | <ul> <li>Source</li> </ul> |                     | Event ID        |                |   | -     |
|              |                |                            | indows-Security-Aud |                 | Event ID: 4674 | An operation was attempted on a privileged object.  |       |
|              |                |                            | indows-Security-Aud | -               |                | An operation was attempted on a privileged object.  |       |
| 4 04         | /08/2012 11:32 | :37 Microsoft-W            | indows-Security-Aud | iting 4674      |                | An operation was attempted on a privileged object.  |       |
|              |                |                            | indows-Security-Aud |                 |                | An account was logged off.  |       |
|              |                |                            | indows-Security-Aud |                 |                | An account was successfully logged on.  |       |
| 7 04         | /08/2012 11:32 | :36 Microsoft-W            | indows-Security-Aud | iting 4672      |                | An account was successfully logged on.  |       |
|              |                |                            | indows-Security-Aud |                 |                | Special privileges assigned to new logon.   |       |
| 9 04         | /08/2012 11:12 | :35 Microsoft-W            | indows-Security-Aud | iting 4624      |                | An account was logged off.  |       |
|              |                |                            | indows-Security-Aud | -               |                | An account was successfully logged on.  |       |
| 1 04         | /08/2012 11:12 | :35 Microsoft-W            | indows-Security-Aud | iting 4648      |                | Special privileges assigned to new logon.   |       |
|              |                |                            | indows-Security-Aud |                 |                | A logon was attempted using explicit credentials.   |       |
| l3 <b>04</b> | /08/2012 11:12 | :34 Microsoft-W            | indows-Security-Aud | iting 4624      |                | An account was logged off.  |       |
|              |                |                            | indows-Security-Aud |                 |                | An account was successfully logged on.  |       |
|              |                |                            | indows-Security-Aud | -               |                | Special privileges assigned to new logon.   |       |
|              |                |                            | indows-Security-Aud | •               |                | A logon was attempted using explicit credentials.   |       |
| l7 04        | /08/2012 11:12 | :31 Microsoft-W            | indows-Security-Aud | iting 4985      |                | The state of a transaction has changed.   |       |
|              |                |                            | indows-Security-Aud | •               |                | The state of a transaction has changed.   |       |
|              | /08/2012 11·12 |                            | indows-Security-Aud | iting 4985      |                | The state of a transaction has changed.   | •     |

="Event ID: "&B2

*Figure 61. Prefix cell value with a string. (Lee, 2014, digital case files)* 

Follow the steps outlined previously (the substitute function instructions near Figure 54) to get the desired results as shown in Figure 62.

| 💌 🔚 🖬     | 9 • @ • 🗋   <del>-</del>           |                              |                         | Security_Fu       | nction.xlsx - Mic  | rosoft Excel  |             |           |         | _ 🗆                                  | ×        |
|-----------|------------------------------------|------------------------------|-------------------------|-------------------|--------------------|---|-------------|-----------|---------|--------------------------------------|----------|
| File      | Home Insert                        | Page Layout                  | Formulas Data Review    | View Developer    | Team               |   |             |           |         | a 🕜 🗆                                | JP 23    |
|           | Calibri                            | - 11 - A                     |                         | - white low       | General 🗸          |   |             | <         | ∑ Autos | ZY                                   |          |
| Paste     | <sub>≱</sub> B <i>I</i> <u>U</u> - | 😐 •   🖄 • 🔒                  | ▲ ·  ■ = =   :: :: :: : | Merge & Center 🔻  | \$ - % •           | Conditional Format Cell<br>Formatting • as Table • Styles • | Insert Dele | te Format | Clear   | ▼ Sort & Find &<br>Filter ▼ Select ▼ |          |
| Clipboard | G <sub>2</sub>                     | Font                         | ন Alignment             | 5                 | Number 🕞           | Styles  | Cell        | s         |         | Editing                              |          |
|           | C2 -                               | (* <b>f</b> <sub>x</sub>     | Event ID: 4674          |                   |                    |   |             |           |         |                                      | 1        |
|           | А                                  |                              | В                       | С                 |                    | D   |             | E         |         |                                      | -        |
| 1 Dat     | e/Time                             | <ul> <li>Artifact</li> </ul> |                         | • Properties      | ·                  |   |             |           | *       |                                      | F        |
| 2 04/0    | 08/2012 11:32:                     | 37 Microsoft-                | Windows-Security-Auditi | ng Event ID: 467  | An operation wa    | s attempted on a privilege                                  | d object.   | Subject:  | Se      | ecurity ID:LOCAL SE                  | RVI      |
| 3 04/0    | 08/2012 11:32:                     | 37 Microsoft-                | Windows-Security-Auditi | ng Event ID: 4674 | An operation wa    | s attempted on a privilege                                  | d object.   | Subject:  | Se      | ecurity ID:LOCAL SE                  | RVI      |
| 4 04/0    | 08/2012 11:32:                     | 37 Microsoft-                | Windows-Security-Auditi | ng Event ID: 4674 | An operation wa    | s attempted on a privilege                                  | d object.   | Subject:  | Se      | ecurity ID:LOCAL SE                  | ERVI     |
| 5 04/0    | 08/2012 11:32:                     | 36 Microsoft-                | Windows-Security-Auditi | ng Event ID: 463  | An account was l   | ogged off.  |             | Subject:  | Se      | ecurity ID:SYSTEM                    |          |
| 6 04/0    | 08/2012 11:32:                     | 36 Microsoft-                | Windows-Security-Auditi | ng Event ID: 462  | An account was s   | successfully logged on.                                     |             | Subject:  | Se      | ecurity ID:NULL SID                  | )        |
| 7 04/0    | 08/2012 11:32:                     | 36 Microsoft-                | Windows-Security-Auditi | ng Event ID: 467  | An account was s   | successfully logged on.                                     |             | Subject:  | Se      | ecurity ID:NULL SID                  | )        |
| 8 04/0    | 08/2012 11:12:                     | 35 Microsoft-                | Windows-Security-Auditi | ng Event ID: 4634 | Special privileges | assigned to new logon.                                      |             | Subject:  | S       | ecurity ID:SYSTEM                    |          |
| 9 04/0    | 08/2012 11:12:                     | 35 Microsoft-                | Windows-Security-Auditi | ng Event ID: 462  | An account was l   | ogged off.  |             | Subject:  | Se      | ecurity ID:SYSTEM                    |          |
| 10 04/0   | 08/2012 11:12:                     | 35 Microsoft-                | Windows-Security-Auditi | ng Event ID: 467  | An account was s   | successfully logged on.                                     |             | Subject:  | Se      | ecurity ID:NULL SID                  | )        |
| 11 04/0   | 08/2012 11:12:                     | 35 Microsoft-                | Windows-Security-Auditi | ng Event ID: 464  | Special privileges | assigned to new logon.                                      |             | Subject:  | Se      | ecurity ID:SYSTEM                    |          |
| 12 04/0   | 08/2012 11:12:                     | 34 Microsoft-                | Windows-Security-Auditi | ng Event ID: 4634 | A logon was atte   | mpted using explicit crede                                  | ntials.     | Subject:  | Se      | ecurity ID:SYSTEM                    |          |
| 13 04/0   | 08/2012 11:12:                     | 34 Microsoft-                | Windows-Security-Auditi | ng Event ID: 462  | An account was l   | ogged off.  |             | Subject:  | Se      | ecurity ID:SYSTEM                    |          |
| 14 04/0   | 08/2012 11:12:                     | 34 Microsoft-                | Windows-Security-Auditi | ng Event ID: 467  | 2 An account was s | successfully logged on.                                     |             | Subject:  | Se      | ecurity ID:NULL SID                  | )        |
|           |                                    |                              | Windows-Security-Auditi | •                 |                    |   |             | Subject:  | Se      | ecurity ID:SYSTEM                    |          |
| 16 04/0   | 08/2012 11:12:                     | 31 Microsoft-                | Windows-Security-Auditi | ng Event ID: 498  | A logon was atte   | mpted using explicit crede                                  | ntials.     | Subject:  | S       | ecurity ID:SYSTEM                    |          |
|           |                                    |                              | Windows-Security-Auditi | •                 |                    |   |             | Subject:  |         | ecurity ID:SYSTEM                    |          |
|           |                                    |                              | Windows-Security-Auditi | -                 |                    | -   |             | Subject:  |         | ecurity ID:SYSTEM                    |          |
| ₩ 4 ►     | 🗵 Security 🥂                       |                              | Windows-Security-Auditi | ng Event ID: 498  | The state of a tra | nsaction has changed.                                       |             | Subject:  |         | ecurity ID:SYSTEM                    | •        |
| Ready     |                                    |                              |                         |                   |                    |   |             |           | 100%    | · ────                               | - (+ ) , |

Figure 62. Date/Time and Properties columns. (Lee, 2014, digital case files)

Using the filter dropdown arrows in each column header cell, delete columns that clearly don't contain information of value. Next, find the columns that correspond to the remaining Column Headers and label them accordingly. Finally, delete the columns that are not labeled. Remember, to make this process immensely easier, reduce as much data first by getting rid of rows based off the timeframe, keywords, and Event IDs you know will not contain information related to the intrusion. The final output would look like Figure 63 after putting the columns in the correct order.

| S 🔚 🔊 • 🗠 🗋 📼                                  |                              | Security_Function.xlsx - Micros          | oft Excel  | _ 🗆 🗙   |
|--|------------------------------|--|--|---|
| File Home Insert Pa                            | age Layout Formulas Data F   | eview View Developer Team                |  | a 🕜 🗖 🗟                                       |
| Paste  |                              |  | nditional Format Cell<br>Insert Delete Format Q<br>2 Clear v | m * 🖅 👬<br>Sort & Find &<br>Filter * Select * |
| Clipboard 🕤 Font                               | G AI                         | gnment 🕞 Number 🕞                        | Styles Cells   | Editing                                       |
| B6 👻 (*  | <i>f</i> <sub>≠</sub> SYSTEM |  |  |   |
| A  | ВС                           | D  | E  | F   |
|  | ccount · Computer            | Description                              | Details  | Properties 🔹 Misc                             |
| 2 04/08/2012 11:12:31 S                        | YSTEM WKS-WIN764BITB         | The state of a transaction has changed.  | Process Name:C:\Windows\System32\svchost.exe                 | Event ID: 4985                                |
| 3 04/08/2012 11:12:31 S                        | YSTEM WKS-WIN764BITB         | The state of a transaction has changed.  | Process Name:C:\Windows\System32\svchost.exe                 | Event ID: 4985                                |
| 4 04/08/2012 11:12:31 S                        | YSTEM WKS-WIN764BITB         | The state of a transaction has changed.  | Process Name:C:\Windows\System32\svchost.exe                 | Event ID: 4985                                |
| 5 04/08/2012 09:45:36 S                        | YSTEM WKS-WIN764BITB         | The state of a transaction has changed.  | Process Name:C:\Windows\System32\svchost.exe                 | Event ID: 4674                                |
| 6 04/08/2012 05:00:26 S                        | YSTEM WKS-WIN764BITB         | An attempt was made to access an object. | Process ID:0x6b8   | Event ID: 4663 Proce                          |
| 7 04/08/2012 05:00:26 S                        | YSTEM WKS-WIN764BITB         | An attempt was made to access an object. | Process ID:0x6b8   | Event ID: 4663 Proce                          |
| 8 04/08/2012 05:00:23 S                        | YSTEM WKS-WIN764BITB         | An attempt was made to access an object. | Process ID:0x6b8   | Event ID: 4663 Proce                          |
| 9 04/08/2012 05:00:21 S                        | YSTEM WKS-WIN764BITB         | An attempt was made to access an object. | Process ID:0x6b8   | Event ID: 4663 Proce                          |
| 10 04/08/2012 05:00:17 S                       | YSTEM WKS-WIN764BITB         | An attempt was made to access an object. | Process ID:0x6b8   | Event ID: 4663 Proce                          |
| 11 04/08/2012 05:00:16 S                       | YSTEM WKS-WIN764BITB         | An attempt was made to access an object. | Process ID:0x6b8   | Event ID: 4663 Proce                          |
| 12 04/08/2012 05:00:14 S                       | YSTEM WKS-WIN764BITB         | An attempt was made to access an object. | Process ID:0x6b8   | Event ID: 4663 Proce                          |
| 13 04/08/2012 05:00:14 S                       | YSTEM WKS-WIN764BITB         | An attempt was made to access an object. | Process ID:0x6b8   | Event ID: 4663 Proce                          |
| 14 04/08/2012 05:00:12 S                       | YSTEM WKS-WIN764BITB         | An attempt was made to access an object. | Process ID:0x6b8   | Event ID: 4663 Proce                          |
| 15 04/08/2012 05:00:12 S                       | YSTEM WKS-WIN764BITB         | An attempt was made to access an object. | Process ID:0x6b8   | Event ID: 4663 Proce                          |
| 16 04/08/2012 03:12:30 S                       | YSTEM WKS-WIN764BITB         | The state of a transaction has changed.  | Process Name:C:\Windows\System32\svchost.exe                 | Event ID: 4985                                |
| 17 04/08/2012 03:12:30 S                       | YSTEM WKS-WIN764BITB         | The state of a transaction has changed.  | Process Name:C:\Windows\System32\svchost.exe                 | Event ID: 4985                                |
| 18 04/08/2012 02:49:31 S                       | YSTEM WKS-WIN764BITB         | The state of a transaction has changed.  | Process Name:C:\Windows\System32\svchost.exe                 | Event ID: 4674                                |
| 19 04/08/2012 01·12·03 S<br>▲ ▲ ▶ ₱ Security 🚱 | YSTEM WKS-WIN764BITB         | The state of a transaction has changed.  | Process Name:C:\Windows\Svstem32\svchost.exe                 | Event ID: 4985                                |
| Ready 🛅  |                              |  | 🖽 🔲 🛄 100% (   | -)(+)   |

Figure 63. The final output of the CSV export data. (Lee, 2014, digital case files)

The second type of export from an Event Viewer log that we will look at is the XML format. This output is a lot easier to examine since there are already tags defining each column. As before, you export Event Viewer logs in the XML format by selecting 'Save All Events As...' or 'Save Filtered Log File As...' and choosing XML in the 'Save as type' dropdown list (Figure 53). Import the resulting .XML file into Microsoft Excel. You will get a popup box asking how to import the data. Select 'As an XML Table' and click on the 'OK' button (Figure 64).

| 2                               | ii) -    | e -    | )   =        |          |                         |        |        |                | Во             | ok1 - M | icrosoft | t Ex        | cel                       |                          |                 |               |           |          |           |        |                    | ×    |
|---------------------------------|----------|--------|--------------|----------|-------------------------|--------|--------|----------------|----------------|---------|----------|-------------|---------------------------|--------------------------|-----------------|---------------|-----------|----------|-----------|--------|--------------------|------|
| File                            | -        | lome   | Insert       | Page Lay | yout Formula            | s Data | Review | v Viev         | N Developer    | r Team  |          |             |                           |                          |                 |               |           |          |           | 6      | a 🕜 🗖              | a X3 |
| Ê                               | X        | Calibr | i            | - 11     | - A* A* =               | = _    | ð) -   | <b>≣</b> • Wra | ap Text        | General |          | Ŧ           |                           |                          | J               |               | *         |          | Σ AutoSum | Ż      | ñ                  |      |
| Paste                           | ۰۳.<br>ا | в      | <i>I</i> ∐ - | 188 • 1  | <u>≫</u> - <u>A</u> - ≡ | ≡ ≡    | ¢ ¢    | 😐 Mer          | rge & Center + | \$ - %  | • .0     | 0.**<br>00. | Conditional<br>Formatting | Format<br>• as Table • S | Cell<br>tyles * | Insert        |           | Format   | Clear -   |        | Find &<br>Select = |      |
| Clipboa                         | nd 🕞     |        | F            | ont      | 15                      |        | Alignm | ent            | G.             | Nun     | iber     | - 54        |                           | Styles                   |                 |               | Cells     |          | E         | diting |                    |      |
|                                 | A1       |        | -            | 6        | fs:                     |        |        |                |                |         |          |             |                           |                          |                 |               |           |          |           |        |                    | ~    |
|                                 | Α        |        | в            | С        | D                       | E      |        | F              | G              | н       | 1        |             | J                         | V                        |                 | 1             |           | ?        | ×         | 0      | P                  |      |
| 1                               |          |        |              |          |                         |        |        |                |                |         |          |             |                           |                          |                 | Open          | XML       | r        | <u> </u>  |        |                    |      |
| 2                               |          |        |              |          |                         |        |        |                |                |         |          |             |                           | Please sele              | t how           | you wou       | d like to | open thi | is file:  |        |                    |      |
| 2<br>3<br>4<br>5<br>6<br>7<br>8 |          |        |              |          |                         |        |        |                |                |         |          |             |                           | As an X                  | ML ţab          | le            |           |          |           |        |                    |      |
| 4                               |          |        |              |          |                         |        |        |                |                |         |          |             |                           | 0.444                    | ni uniy         | <u>no ita</u> | k         |          |           |        |                    |      |
| 5                               |          |        |              |          |                         |        |        |                |                |         |          |             |                           | 🔘 Use the                | XML S           | ource tas     | k pane    |          |           |        |                    |      |
| 6                               |          |        |              |          |                         |        |        |                |                |         |          |             |                           | OK                       |                 | Cano          | el        | He       | 4p        |        |                    |      |
| 7                               |          |        |              |          |                         |        |        |                |                |         |          |             |                           |                          |                 | · · · · · ·   |           |          |           |        |                    |      |
| 8                               |          |        |              |          |                         |        |        |                |                |         |          |             |                           |                          |                 |               |           |          |           |        |                    |      |

Figure 64. Open .xml file as an XML Table. (Lee, 2014, digital case files)

Once you have imported the data, it will look like Figure 65.

|            | <b></b>  | Book2 -      | Microsoft Excel   |                  |   |    |   |       |          |          | - 🗆 ×             |
|------------|--|--------------|-------------------|------------------|---|----|---|-------|----------|----------|-------------------|
| File Home  | Insert Page Layout Fo  | rmulas D     | ata Review View   | Developer Team   | Design                                    |    |   |       |          |          | a 🕜 🗖 🗗           |
| able1      | Summarize with PivotTable<br>Remove Duplicates<br>Convert to Range | Export Refre | Open in Browser   |                  | rst Column<br>ist Column<br>anded Columns |    |   |       |          |          |                   |
| Properties | Tools  | Exte         | ernal Table Data  | Table Style Op   | tions                                     |    |   | Table | e Styles |          |                   |
| A1         | <b>▼</b> (° <b>f</b> x N   | ame          |                   |                  |   |    |   |       |          |          |                   |
|            | A  |              | В                 |                  | С   |    | D | E     | F        | G        | Н                 |
| 1 Name     |  | ▼ Guid       |                   | ×                | ns1:EventID                               |    |   |       |          |          | ns1:Keywor        |
|            | /indows-Security-Auditir   | •••          |                   | ,                |   | 74 | 0 | 0     | 13056    |          | 0 0x80100000      |
|            | /indows-Security-Auditin   | • •          |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x80100000      |
|            | /indows-Security-Auditir   |              |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x80100000      |
|            | /indows-Security-Auditin   |              |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditin   | •••          |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditin   | •••          |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditin   |              |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditir   |              |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditin   | •••          |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditin   | • •          |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditir   | •••          |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditin   | • •          |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditir   |              |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditin   | • •          |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditin   | •••          |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditir   | •••          |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
|            | /indows-Security-Auditin   | •••          |                   |                  |   | 74 | 0 | 0     | 13056    |          | 0 0x8010000       |
| Shee       | vindows-Security-Auditin<br>t1 Sheet2 Sheet3                       |              | 9625-5478-4994-A5 | BA-3E3B0328C30D} | 46  | 74 |   | 0     | 13056    |          | 0 0x80100000<br>▶ |
| eady 🛅     |  |              |                   |                  |   |    |   |       |          | 100% 😑 🛁 | -0(+              |

Figure 65. Imported XML file as a Table. (Lee, 2014, digital case files)

One issue is the Date/Time format, which separates the date and time with the letter 'T' and includes milliseconds followed by the letter 'Z.' A function will be used to get the correct format of 'mm/dd/yyyy hh:mm:ss'. To make manipulating the data easier, you will convert the table to a normal range. This conversion can be done by selecting the 'Convert to Range' button on the 'Table Tools' ribbon and selecting 'Yes' on the popup window (Figure 66).

| 3 🖬 🤊              | - (° - 🗋   -        |                    | Book2 -      | Microsoft       | Excel   |                         | Table Tools              |            |               |          |                     | _ □               | ~      |
|--------------------|---------------------|--------------------|--------------|-----------------|---------|-------------------------|--------------------------|------------|---------------|----------|---------------------|-------------------|--------|
| File               | Home Insert         | Page Layout For    | mulas Dat    | a Review        | View    | Developer Team          | Design                   |            |               |          |                     | a 🕜 =             | - #P 2 |
| able Name<br>able1 | Remove D            | upileates -        | xport Refres | Properti        |         |                         | rst Column<br>ast Column |            |               |          |                     | · · · · · · · · · |        |
| Resize 1           |                     | Range              | ÷ ÷          | ဖွဲ့ခ်္ဆ Unlink |         | Banded Rows B           |                          | ,          |               |          |                     | <del>-</del>      |        |
| Propertie          | es 💦                | pols               |              | nal Table Data  |         | Table Style Op          | otions                   |            |               | Tab      | le Styles           |                   | _      |
|                    | -                   | <i>f</i> ∗ 20      | 12-04-08T    | 11:32:37.2      | 8463760 | 00Z                     |                          |            |               |          |                     |                   |        |
|                    | С                   | 5                  | E            | F               | G       |                         |                          |            | 1             |          | J                   | К                 |        |
|                    |                     | ersion 💌 ns1:L     |              | 1:Task 💌 I      | ns1:Opc |                         |                          | SystemTin  |               |          | ns1:EventRecordID 💌 | ns1:Correlat      | tion   |
| 2                  | 4674                | 0                  | 0            | 13056           |         | 0 0x80100000            |                          |            |               |          | 981779              |                   |        |
| 3                  | 4674                | 0                  | 0            | 13056           |         | 0 0x80100000            |                          |            |               |          | 981779              |                   |        |
|                    | 4674                | 0                  | 0            | 13056           |         | 0 0x8010000             |                          |            |               |          | 981779              |                   |        |
|                    | 4674                | nvert 0            | 0            | 13056           |         | 0 0x8010000             |                          |            |               |          | 981779              |                   |        |
| ;<br>,             | Tak                 | le to a            | 0            | 13056           |         | 0 0x80100000            |                          |            |               |          | 981779              |                   |        |
|                    |                     |                    | 0            | 13              |         | Microsoft E>            | cel                      |            | T11:32:37.28  |          | 981779              |                   |        |
|                    | 4674                |                    | 0            | 13              |         |                         |                          |            | T11:32:37.28  |          | 981779<br>981779    |                   |        |
| )                  | 4674                |                    | 0            | 13              | Do      | you want to convert the | table to a norm          | nal range? | T11:32:37.28  |          | 981779              |                   |        |
| 1                  | 4674                | 0                  | 0            | 13              |         |                         |                          |            | T11:32:37.28  |          | 981779              |                   |        |
| 2                  | 4674                | 0                  | 0            | 13              |         | Yes                     | No                       |            | T11:32:37.28  |          | 981779              |                   |        |
| 3                  | 4674                | 0                  | 0            | 13056           |         | 70 0x80100000           | 0000000                  |            |               |          | 981779              |                   |        |
| 1                  | 4674                | 0                  | 0            | 13056           |         | 0 0x80100000            |                          |            |               |          | 981778              |                   |        |
| 5                  | 4674                | 0                  | 0            | 13056           |         | 0 0x80100000            |                          |            |               |          | 981778              |                   |        |
| 6                  | 4674                | 0                  | 0            | 13056           | 2       | 0 0x80100000            |                          |            |               |          | 981778              |                   |        |
| 7                  | 4674                | 0                  | 0            | 13056           | 2       | 0 0x8010000             | 00000000                 | 2012-04-0  | 8T11:32:37.28 | 4637600Z | 981778              |                   |        |
| 8                  | 4674                | 0                  | 0            | 13056           |         | 0 0x80100000            | 00000000                 | 2012-04-0  | 8T11:32:37.28 | 4637600Z | 981778              |                   |        |
| 9                  | 4674<br>Sheet1 Shee | 0<br>t2 / Sheet3 😤 | 0            | 13056           |         | 0 0x8010000             | 00000000                 | 2012-04-0  | 8T11-32-37.28 | 46376007 | 981778              |                   |        |
| eady               | 1                   |                    | ,            |                 |         |                         |                          |            |               |          | ■□□ 100% (-)-       |                   | (+     |

Figure 66. Convert Table to a Range. (Lee, 2014, digital case files)

In order prevent confusion from the highlighting of artifacts related to the incident, you should remove the formatting left over from the table layout (Figure 67).

| 🛃 🔊 • (e    | ×   <del>↓</del>           |                   |                     | Boo                 | k2 - Microsoft E        | cel                    |   |                             |                                    |
|-------------|----------------------------|-------------------|---------------------|---------------------|-------------------------|------------------------|---|-----------------------------|------------------------------------|
| File Hor    | ne Insert Page Layout      | Formulas Data     | Review View         | Team                |                         |                        |   |                             | ۵ 😮 🗆 و                            |
| Cut         | -                          | 11 × A ∧ =        |                     |                     | neral -                 | 5                      |   | 📺 🖆 🚛 📑 🖬                   | toSum - 🔊 🕅                        |
| aste 🛷 Form | at Painter B Z U *         | ] •   🌺 • 🛕 •   🗏 | : = = :: :: :       | Merge & Center * \$ | × % , .0 .00<br>.00 →.0 | Condition<br>Formattin | nal Format Cell<br>g * as Table * Styles *    | Insert Delete Format        | sort & Find &<br>Filter * Select * |
| Clipboard   | G Font                     | Es .              | Alignment           | Fa                  | Number 🕞                |                        | Styles  | Clear All                   | ng                                 |
| A1          | ▼ (° <i>f</i> x N          | ame               |                     |                     |                         |                        |   | 🦢 Clear <u>F</u> ormats     |                                    |
|             | A                          |                   | В                   | С                   | D                       | E                      | c   | G Clear Con                 | I I                                |
| me          |                            | Guid              |                     | ns1:EventID         | ns1:Version ns          | 1:Level                | Clear Formats                                 | ear Co <u>m</u> me          | ystemTime ns1:                     |
| Mic, soft-  | Windows-Security-Auditing  | {54849625-5478-4  | 994-A5BA-3E3B0328C  | 0D} 4674            | 0                       |                        | Clear only the forma<br>applied to the select |                             | 012-04-08T11. 2:37.284637600Z      |
| Micros, 4-  | Windows-Security-Auditing  | {54849625-5478-4  | 1994-A5BA-3E3B0328C | 0D} 4674            | 0                       | l                      | applied to the select                         | Remove Hyperlinks           | 012-04-08T11:32. 7.284637600Z      |
| Microsoft   | Vindows-Security-Auditing  | {54849625-5478-4  | 1994-A5BA-3E3B0328C | 0D} 4674            | 0                       | 0                      | 13056   | - Seniove Hypernins         | 12-04-08T11:32:37.284637600Z       |
| -           | Wi. dows-Security-Auditing |                   | 1994-A5BA-3E3B0328C | 0D} 4674            |                         | 0                      |   | 0 0x80100000000000          |                                    |
| Microsoft-  | Windeys-Security-Auditing  | {54849625-5478-4  | 1994-A5BA-3E3B0328C | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 00 2012-0-08T11:3>->7.20405/6002   |
|             | Windows-Security-Auditing  |                   | 1994-A5BA-3E3B0328C | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x8010000000000           | 2012-04- 3T11: Button 302          |
| Microso     | Select All Auditing        | {54849625-5478-4  | 1994-A5BA-3E3B0328C | IOD} 4674           | 0                       | 0                      | 13056   | 0 0x8010000000000           |                                    |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 1994-A5BA-3E3B0328C | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:37 24637500Z       |
| Microsoft-  |                            |                   | 1994-A5BA-3E3B0328C | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x8010000000000           | 0 2012-04-08T11:32                 |
| Microsoft-  | Windov. ecurity-Auditing   | {54849625-5478-4  | 1994-A5BA-3E3B0328C | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x8010000000000           | INVITIALS                          |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 1994-A5BA-3E3B0328C | IOD} 4674           | 0                       | 0                      | 13056   | 0 0x80100000000000          | 00 2012-04-08T11:32:37.284637600Z  |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 1994-A5BA-3E3B0328C | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:32:37 2 7600Z      |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 994-A5BA-3E3B0328C  | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:32:37. 37600Z      |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 994-A5BA-3E3B0328C  | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 00 2012-04-08T11:32:37.284637600Z  |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 994-A5BA-3E3B0328C  | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:32:37.284637600Z   |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 994-A5BA-3E3B0328C  | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:32:37.284637600Z   |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 1994-A5BA-3E3B0328C | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:32:37.284637600Z   |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 1994-A5BA-3E3B0328C | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:32:37.284637600Z   |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 994-A5BA-3E3B0328C  | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:32:37.284637600Z   |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 994-A5BA-3E3B0328C  | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:32:37.284637600Z   |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 994-A5BA-3E3B0328C  | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:32:37.284637600Z   |
| Microsoft-  | Windows-Security-Auditing  | {54849625-5478-4  | 994-A5BA-3E3B0328C  | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:32:37.284637600Z   |
|             | Windows-Security-Auditing  | {54849625-5478-4  | 994-A5BA-3E3B0328C  | 0D} 4674            | 0                       | 0                      | 13056   | 0 0x80100000000000          | 0 2012-04-08T11:32:37.284637600Z   |
|             | et1 / Sheet2 / Sheet3 / 🕈  | 2/                |                     |                     |                         |                        | I 4   |                             |                                    |
| eady        |                            |                   |                     |                     |                         |                        | Average: 124891.6966                          | Count: 178379 Sum: 11139340 | )205 🔠 🗉 100% 😑 🗸 🗸                |

Figure 67. Clear Table Formatting. (Lee, 2014, digital case files)

To fix the Date/Time formatting, you can use the following function (Figure 68):

=0+SUBSTITUTE(SUBSTITUTE((MID(12,1,19)), "T", " "), "-", "/")

| X   🖬  | <b>n) -</b> (n - | -   <del>-</del> |                          |                 |                       | Bool                                       | k2 - Microsof    | Excel              |                             |                      |                  |                    |           | - • ×               |
|--------|------------------|------------------|--------------------------|-----------------|-----------------------|--|------------------|--------------------|-----------------------------|----------------------|------------------|--------------------|-----------|---------------------|
| File   | Home             | Insert           | Page Layout              | Formulas Dat    | a Re                  | view View Tea                              | am               |                    |                             |                      |                  |                    | ۵         | () — d <sup>2</sup> |
| Ê      | K Cal            | libri            | • 11 • A                 | <b>≡ ≡</b>      | ≫                     | Wrap Text                                  | General          | *                  | <b>≦</b> ≸                  |                      |                  | Σ                  | <b>CR</b> | A                   |
| Paste  | 🧳 В              | ΙŪ·              | 🔄 •  🔕 • 🗛               | • = = =         | <b>€</b> ≣ <b>€</b> ≣ | Merge & Center                             | · \$ · % ,       | €.0 .00<br>0.€ 00. | Conditional<br>Formatting * | Format<br>as Table ≠ | Cell<br>Styles * | Function to        | Sort &    |                     |
| lipboa | ird G            | For              | nt                       | - Fai           | Alignm                | ient                                       | S Numbe          | r G                |                             | Styles               |                  | Lens               | Editing   |                     |
|        | J2               | <b>-</b>         | <i>f<sub>x</sub></i> =0- | +SUBSTITUTE(SUB | STITUTE               | E((MID(I2,1,19)),"T"                       | ," "),"-","/") 📹 |                    |                             |                      |                  | Convert            |           |                     |
|        | E                | F                | G                        | н               |                       | 1  |                  |                    |                             |                      |                  | Date/Time          | L         | М                   |
| ns     | 1:Level          | ns1:Task         | ns1:Opcode               | ns1:Keywords    | 5                     | SystemTime                                 |                  |                    |                             |                      | 1:E              | entReardID ns) Cor | relation  | ProcessID           |
|        | 0                | 13056            |                          | 0 0x8010000000  | 00000 2               | 2012-04-08T11:32:37                        | .28463700.Z      |                    | 41                          | 007.4809             | 8                | Format             |           |                     |
|        | 0                | 13056            |                          | 0 0x8010000000  | 00000 2               | 2012-04-08T11:32:37                        | .284637600Z      |                    |                             |                      |                  | 981779             |           |                     |
| L .    | 0                | 13056            |                          | 0 0x8010000000  | 00000 2               | 2012-04-08T11:32:37                        | .284637600Z      |                    |                             | <b>-</b>             |                  | 9 1 9              |           |                     |
|        | 0                | 13056            |                          | 0 0x8010000000  | 00000 2               | 2012-04-08T11:32:37                        | .284637600Z      |                    |                             |                      |                  | 981.19             |           |                     |
| 5      | 0                | 13056            |                          | 0 0x8010000000  | 00000 2               | 2012-04-08T11:32:37                        | .284637600Z      |                    |                             |                      |                  | 981779             |           |                     |
| '      | 0                |                  |                          | 0 0x8010000000  |                       | 2012-04-08T11:32:37                        |                  |                    |                             |                      |                  | 981779             |           |                     |
|        | 0                |                  |                          | 0 0x8010000000  |                       | 2012-04-08T11:32:37                        |                  |                    |                             |                      |                  | 981779             |           |                     |
|        | 0                |                  |                          |                 |                       | 2012-04-08T11:32:37                        |                  |                    | For                         | mat                  | to               | 981779             |           |                     |
| D      | 0                |                  |                          | 0 0x8010000000  |                       | 2012-04-08T11:32:37                        |                  |                    |                             |                      |                  | 981779             |           |                     |
| 1      | 0                |                  |                          |                 |                       | 2012-04-08T11:32:37                        |                  |                    | mm/                         | dd/y                 | VVV              | 981779             |           |                     |
| 2      | 0                |                  |                          |                 |                       | 2012-04-08T11:32:37                        |                  |                    | hhu                         | mm:                  | 200              | 981779             |           |                     |
| 3      | 0                |                  |                          |                 |                       | 2012-04-08T11:32:37<br>2012-04-08T11:32:37 |                  |                    |                             | IIIII:               | 22               | 981779<br>981778   |           |                     |
| 4<br>5 | 0                |                  |                          | 0 0x80100000000 |                       | 2012-04-08111:32:37<br>2012-04-08T11:32:37 |                  |                    |                             | 2                    |                  | 981778             |           |                     |
| 5      | 0                |                  |                          |                 |                       | 2012-04-08111:32:37<br>2012-04-08T11:32:37 |                  |                    | -                           | 6                    |                  | 981778             |           |                     |
| 7      | 0                |                  |                          |                 |                       | 2012-04-08T11:32:37                        |                  |                    |                             |                      |                  | 981778             |           |                     |
| ,<br>B | 0                |                  |                          |                 |                       | 2012-04-08T11:32:37                        |                  |                    |                             |                      |                  | 981778             |           |                     |
| 9      | 0                |                  |                          |                 |                       | 2012-04-08T11:32:37                        |                  |                    |                             |                      |                  | 981778             |           |                     |
| • •    | N Sheet          |                  | /Sheet3 / 🞾              |                 |                       |  |                  |                    | 1                           |                      |                  |                    |           | Þ                   |
| eady   | 0.000            | - A DIROCLE      |                          |                 |                       |  |                  |                    | <b>.</b>                    |                      |                  | III III 100%       | 0         |                     |

*Figure 68. Function for Date/Time Formatting. (Lee, 2014, digital case files)* 

This function will display the Date/Time in number format. Apply the 'mm/dd/yyyy hh:mm:ss' format to the column for proper display.

Another issue you may run into is that some of the data is hex encoded (Figure 69). To convert the hex data to human readable ASCII data, you can run the 'Binary\_Hex2Ascii\_Conversion\_Module.bas' code (https://github.com/gregory-lalla/GCIH\_Gold/blob/master/Code/Singles/Module\_BAS\_Files/Misc/Binary\_Hex2Ascii\_Conversion\_Module.bas) (Figure 70).

|                                      |                                   |   | _   |
|--------------------------------------|-----------------------------------|---|---|
| X   🛃 🤊 • (°- ×   = Bo               | ook2 - Microsoft Excel            |   | ×   |
| File Home Insert Page Layout F       | Formulas Data Review View Team    | Design  | a 😮 🗆 🗗                                     |
| Calibri • 11 • A A                   | r ≡ = ⊗ v ∰ Wrap Text G           | eneral 🔹 🛃 🗾  | Σ AutoSum · T                               |
| Paste 🦪 B Z U - 🖽 - 🌆 - 🗛            | * 王 王 王 詳 詳 譯 Merge & Center * \$ | * %      * | Insert Delete Format                        |
| Clipboard 🛱 Font 🗆                   | Fa Alignment Fa                   | Number 🖓 Styles   | Cells Editing                               |
| R1 • 🥑 🎜 ns2:1                       | Binary                            |   |   |
| N O P                                | P Q                               |   |   |
|                                      | elation VerocessID VerocessID     |   |   |
| 16                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 51                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| i6                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 26                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 39                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 27                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 64                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 66                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 76                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 83                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 94                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 26                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 01                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 39                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 87                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 32                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 74                                   | 2D20436F64653A202043              | 4F525356434330303030303737332D2043616C6C3A  | 2020434F525356434330303030303735352D2050494 |
| 15                                   | 2D20436F64653A202043              |   | 2020434F525356434330303030303735352D2050494 |
| 🖬 🔸 🕨 Sheet1 / Sheet2 / Sheet3 / 🤧 / | 7                                 | 1 4   |   |
| Ready 23 of 932 records found        |                                   |   | Count: 24 🔲 🗉 🛄 100% 😑 —— 🕂 🕂               |

Figure 69. Hex Encoded Data. (Lee, 2014, digital case files)

| () 🛄 🔊 • 🕅 •           | 1.   |                                   |             | P              | ook2 - Micr   | osoft Excel   |                             |                     |                 | _ 0              | ×     |
|------------------------|--|-----------------------------------|-------------|----------------|---------------|---|-----------------------------|---------------------|-----------------|------------------|-------|
| 🛛 🔚 🤊 • (° -           | -   <del>-</del>   |                                   |             | he             | x_data.xlsm   | - Microsoft Excel   |                             |                     |                 | -                |       |
| File Home              | Insert Page  | e Layout Formulas                 | Data R      | eview View     | Developer     | Team  |                             |                     |                 | ۵ 😭              | 2 -   |
| Visual Macros<br>Basic | Record Macro<br>Use Relative Referen<br>Macro Security<br>Code | Add-Ins COM<br>Add-Ins<br>Add-Ins |             | e 🖞 Run Dialog | Source Source | ap Properties 📑 Im<br>(pansion Packs 📑 Ex<br>efresh Data<br>XML | Document<br>Panel<br>Modify |                     |                 |                  |       |
| R16                    | • (=   | Jx - Code: CORS                   | Q           | - call: CORSVC | 200000755- PI | D: 00002872- 11D: 1   | 0000912- CMD:               | C:\Windows\syste    |                 | - User: Name: NI |       |
|                        |  |                                   | ProcessID 🔻 |                |               |   |                             |                     | R               |                  |       |
|                        | Insz:Opcode  | nsz:correlation *                 | ProcessiD * | · · · · ·      | 00000770      |   | 00755 010.000               | 02872- TID: 000009: |                 |                  |       |
| 16                     |  |                                   |             |                |               |   |                             |                     |                 |                  |       |
| 51                     |  |                                   |             |                |               |   |                             | 02112- TID: 0000174 |                 |                  |       |
|                        |  |                                   |             |                |               |   |                             | 02644- TID: 0000030 |                 |                  |       |
| 26                     |  |                                   |             |                |               |   |                             | 03004- TID: 000029: |                 |                  |       |
| 39                     |  |                                   |             |                |               |   |                             | 00944- TID: 000021: |                 |                  |       |
| 27                     |  |                                   |             |                |               |   |                             | 03476- TID: 0000675 |                 | ., .             |       |
| 64                     |  |                                   |             |                |               |   |                             | 05292- TID: 0000403 |                 |                  |       |
| 66                     |  |                                   |             |                |               |   |                             | 07308- TID: 0000460 |                 |                  |       |
| 76                     |  |                                   |             |                |               |   |                             | 04088- TID: 0000803 |                 |                  |       |
| 83                     |  |                                   |             |                |               |   |                             | 09112- TID: 0000914 |                 |                  |       |
| 94                     |  |                                   |             |                |               |   |                             | 06888- TID: 0000754 |                 |                  |       |
| 26                     |  |                                   |             |                |               |   |                             | 07752- TID: 0000413 |                 |                  |       |
| 01                     |  |                                   |             |                |               |   |                             | 08120- TID: 0000746 |                 |                  |       |
| 39                     |  |                                   |             |                |               |   |                             | 07784- TID: 0000738 |                 |                  |       |
| 87                     |  |                                   |             |                |               |   |                             | 06828- TID: 0000612 |                 |                  |       |
| 32                     |  |                                   |             |                |               |   |                             | 06344- TID: 0000655 |                 |                  |       |
| 74                     |  |                                   |             |                |               |   |                             | 06776- TID: 0000698 |                 |                  |       |
| 15                     |  |                                   |             | - Code: CORS   | CC00000773-   |   |                             | 06840- TID: 0000652 | 28- CMD: C:\Win | dows\system32\   | vssvc |
| A A F FL Sheet         | 1 Sheet2 She   | eet3 / 🞾 /                        |             |                |               |   |                             |                     |                 |                  |       |

Figure 70. Hex Data Converted to ASCII Data. (Lee, 2014, digital case files)

Once you have fixed all the data conversion issues, it is a simple matter of finding the columns to keep, applying the headers, formatting the spreadsheet and putting the columns in the correct order (Figure 71). Once complete, you can begin to search for artifacts of interest.

|     | <b>, ⊔) •</b> (≥ -   <del>-</del> |            |                   |                                | VML Soc            | urity_Events.xlsx - | N.41 | crocoft Evcal  |              |                 | - 🗆 🗙                            |
|-----|-----------------------------------|------------|-------------------|--------------------------------|--------------------|---------------------|------|--|--------------|-----------------|----------------------------------|
|     |                                   |            |                   |                                |                    |                     |      |  |              |                 |                                  |
| Fi  | le Home Insert                    |            |                   | Data Review                    | View               | Developer Tear      | n    |  |              |                 | ۵ 🕜 🗆 🗗 ۵                        |
| Fro | m From From From                  | Other Ex   | xisting Refresh   | Connections ≵↓<br>roperties X↓ | A Z<br>Z A<br>Sort | Filter              | Te   | xt to Remove Data Consolidate Wha<br>lumns Duplicates Validation - Analy | t-If Group U | ngroup Subtotal | ♥클 Show Detail<br>■∃ Hide Detail |
|     | Get External                      | Data       | Connec            | tions                          | Sor                | t & Filter          |      | Data Tools   |              | Outline         | Fa                               |
|     | D9 🔻                              | e .        | fx Handleld       |                                |                    |                     |      |  |              |                 | •                                |
|     | А                                 | В          | C                 |                                |                    | D                   |      |  |              |                 |                                  |
| 1   | Date/Time 🗾                       | Account 🔻  | Computer          | -                              | Descript           | ion                 | -    | Details  |              |                 |                                  |
| 2   | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh | nieldbase.local                | Subject            | JserSid             |      | S-1-5-19   |              |                 |                                  |
| 3   | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh | nieldbase.local                | Subject            | JserName            |      | LOCAL SERVICE  |              |                 |                                  |
| 4   | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh | nieldbase.local                | Subject            | omainName           |      | NT AUTHORITY   |              |                 |                                  |
| 5   | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh | nieldbase.local                | SubjectL           | ogonId              |      | 0x3e5  |              |                 |                                  |
|     | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh | nieldbase.local                | ObjectSe           | erver               |      | LSA  |              |                 |                                  |
| -   | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh | nieldbase.local                | ObjectTy           | /pe                 |      | -  |              |                 |                                  |
| _   | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh |                                | ObjectN            |                     | _    | -  |              |                 |                                  |
|     | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh |                                | Handlei            |                     |      | 0x0  |              |                 |                                  |
|     | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh |                                | AccessM            |                     |      | 16777216   |              |                 |                                  |
|     | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh |                                | Privilege          |                     |      | SeSecurityPrivilege  |              |                 |                                  |
|     | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh |                                | Processi           |                     |      | 0x228  |              |                 |                                  |
|     | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh |                                | Process            |                     |      | C:\Windows\System32\Isass.exe  |              |                 |                                  |
|     | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh |                                | Subject            |                     |      | S-1-5-19   |              |                 |                                  |
|     | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh |                                |                    | JserName            |      | LOCAL SERVICE  |              |                 |                                  |
| _   | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh |                                |                    | DomainName          |      | NT AUTHORITY   |              |                 |                                  |
|     | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh |                                | SubjectL           | •                   |      | 0x3e5  |              |                 |                                  |
|     | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh |                                | ObjectSe           |                     |      | LSA  |              |                 |                                  |
|     | 04/08/2012 11:32:37               |            | WKS-WIN764BITB.sh | nieldbase.local                | ObjectT            | /pe                 |      | -  |              |                 |                                  |
|     | H Sheet1 Sheet                    | t2 / Sheet | 13 / 🔁 /          |                                |                    |                     |      | i 4  |              |                 | •                                |
| Rea | dy 🎦                              |            |                   |                                |                    |                     |      |  |              | 100% 😑 📉        |                                  |

Figure 71. Final Formatted Spreadsheet from XML Data. (Lee, 2014, digital case files)

One last note on XML exported data. Each row does not correspond with only one Event Viewer log entry. There are multiple rows for each Event Viewer log entry identified by an 'EventRecordID' as shown in Figure 72. Therefore, when there is a hit on a keyword search, don't just copy over that one row to the master IOC file, but all the rows that have the same 'EventRecordID' number.

|                            | 0.10   | 10 0 C 1                  |  | - <b>D</b> X                          |
|----------------------------|--|---------------------------|--|---------------------------------------|
| X . · · · · · ·            | BOOK2 -  | Microsoft Excel           |  |                                       |
| File Home Insert Page      | e Layout Formulas Data Review View Develo  | per Team                  |  |                                       |
| Calibri • 1                | 1 · A · A ≡ ≡ 😸 ≫·· 🐨 Wrap Text  | General 🔹                 |  | = 🖹 📜 Σ΄ 🔭 🕅                          |
| Paste 🥃 🖪 I 🗓 -            | 🂁 * 🛕 * 📕 喜 🗐 🇊 镡 💷 Merge & Center *   | \$ ~ % , .0 .00 Condition | onal Format Cell Inse<br>ing * as Table * Styles * | ert Delete Format                     |
| Clipboard 😨 Font           | G Alignment G  | Number 🕞                  | Styles   | Cells Editing                         |
| G1 🔹 🖱                     | <i>f</i> <sub>x</sub> Miscellaneous  |                           |  | ~                                     |
| D                          | E  | F                         | G  | H                                     |
| 1 Description              | Details  | Properties                | Miscellaneous                                      | Artifact 🗾 📃                          |
| 104 TargetDomainName       | SHIELDBASE.LOCAL   | Event ID: 4648            | EventRecordID: 981770                              | Microsoft-Windows-Security-Auditing   |
| 105 TargetLogonGuid        | {E8809E1A-5ABD-2B38-DF63-943347931D69}   | Event ID: 4648            | EventRecordID: 981770                              | Microsoft-Windows-Security-Auditing   |
| 106 TargetServerName       | wks-win764bitb\$   | Event ID: 4648            | rect. dID: 981770                                  | Microsoft-Windows-Security-Auditing   |
| 107 TargetInfo             | wks-win764bitb\$   | Event ID: 10              | EventRecordID: 981770                              | Microsoft-Windows-Security-Auditing   |
| 108 ProcessId              | 0x514  | _vent ID: 4648            | EventRecordID: 981770                              | Microsoft-Windows-Security-Auditing   |
| 109 ProcessName            | C:\Windows\System32\taskhost.exe   | Event ID: 4648            | EventRecordID: 981770                              | Microsoft-Windows-Security-Auditing   |
| 110 IpAddress              | Different Event  | Event ID: 4648            | EventRecordID: 981770                              | Microsoft-Windows-Security-Auditing   |
| 111 IpPort                 | and the state of t | Event ID: 4648            | EventRecordID: 981770                              | Microsoft-Windows-Security-Auditing   |
| 112 TargetUserSid          | s-1-5-18 Record IDs  | 10.4634                   | EventRecordID: 981769                              | Microsoft-Windows-Security-Auditing   |
| 113 TargetUserName         | WKS-WIN764BITB\$   | Event ID: 4634            | EventRecordID: 981769                              | Microsoft-Windows-Security-Auditing   |
| 114 TargetDomainName       | SHIELDBASE   | Event ID: 4634            | EventRecc: 981769                                  | Microsoft-Windows-Security-Auditing   |
| 115 TargetLogonId          | 0x881120   | nt ID: 4634               | EventRecordID: 981769                              | Microsoft-Windows-Security-Auditing   |
| 116 LogonType              | 3  | Event ID 24               | EventRecordID: 981769                              | Microsoft-Windows-Security-Auditing   |
| 117 SubjectUserSid         | S-1-0-0  | Event ID: 4624            | EventRecordID: 981768                              | Microsoft-Windows-Security-Auditing   |
| 118 SubjectUserName        | -  | Event ID: 4624            | Even. or dID: 981768                               | Microsoft-Windows-Security-Auditing   |
| 119 SubjectDomainName      | -  | Event ID: 4624            | EventRecordID: 981768                              | Microsoft-Windows-Security-Auditing   |
| 120 SubjectLogonId         | 0x0  | Event ID: 4624            | EventRecordID: 981768                              | Microsoft-Windows-Security-Auditing   |
| 121 TargetUserSid          | S-1-5-18   | Event ID: 4624            | EventRecordID: 981768                              | Microsoft-Windows-Security-Auditing 🚽 |
| H + H Sheet1 / Sheet2 / Sh | eet3 / 🔁 /   | I 4                       |  | • • • • • • • • • • • • • • • • • • • |
| Ready 🛅                    |  |                           | Count: 1115  | 50 🔲 💷 100% 😑 —— 🖓 —— 🕂 🤃             |

*Figure 72. Event Record IDs in XML Exported Data. (Lee, 2014, digital case files)* 

### 8.4.2. ShimCache Entries

We produced the ShimCache output used in this example by running the ShimCacheParser python tool against a Windows 7 SYSTEM registry file:

### ShimCacheParser.py -i system -o System\_Shim.csv

Open the .CSV output file in Excel and then save it as an Excel macro-enabled workbook file with an .XLSM file extension. Apply the Standard Format macro for a consistent look. (Figure 73).

| 🛃 👘 ▼ (?? -   ╤           |                           | System_Shim            | .xlsm - Microso  | ft Excel  |                         |                     |           |               | × |
|---------------------------|---------------------------|------------------------|------------------|---|-------------------------|---------------------|-----------|---------------|---|
| File Home Insert Pa       | ige Layout Formulas Data  | Review View Devel      | oper Team        |   |                         |                     |           | ے 😮 ۵         | đ |
|                           |                           | 🗐 Wrap Text            | General          | -<br>   |                         |                     | Σ - Α     | 7 🗥           |   |
| aste 🚽 B I U -            | · (A)· A· E = = (# *      | Merge & Center 🔻       | \$ - % , 5       | Call of the second s | al Format Cell          | Insert Delete Forma | at Sol    | t& Find &     |   |
| ₩ <b>₽</b> ⊻ <u></u> ₩    | · · · · · = = = · · ·     | Merge & Center         | 3 70 9 .0        | o →.0 Formattin   | g * as Table * Styles * | * * *               |           | er * Select * |   |
| pboard 😨 Font             | Ta Alig                   | iment 🔤                | Number           | Fai   | Styles                  | Cells               | Ed        | liting        |   |
| E8 🔻 💿                    | <i>f</i> ∗ TRUE           |                        |                  |   |                         |                     |           |               |   |
| A                         | B                         |                        | С                |   |                         |                     | D         | E             |   |
| Last Modified 🛛 👻 Last Up | odate 💌 Path              |                        |                  |   |                         |                     | File Size | Exec Flag     | ¥ |
| 01/12/2011 12:08:00 N/A   | C:\Program Files (x86)\N  | cAfee\VirusScan Enterp | orise\mfeann.exe |   |                         |                     | N/A       | TRUE          |   |
| 11/20/2010 13:24:52 N/A   | C:\Windows\system32\L     | ogonUI.exe             |                  |   |                         |                     | N/A       | TRUE          |   |
| 05/04/2011 05:19:28 N/A   | C:\Windows\system32\S     | earchFilterHost.exe    |                  |   |                         |                     | N/A       | TRUE          |   |
| 05/04/2011 05:19:28 N/A   | C:\Windows\system32\S     | earchProtocolHost.exe  |                  |   |                         |                     | N/A       | TRUE          |   |
| 07/14/2009 01:39:11 N/A   | C:\Windows\system32\g     | pscript.exe            |                  |   |                         |                     | N/A       | TRUE          |   |
| 12/29/2011 08:06:20 N/A   | C:\Program Files (x86)\Je | tico\BCWipe\BCWipeTI   | M.exe            |   |                         |                     | N/A       | TRUE          |   |
| 03/28/2011 11:26:14 N/A   | C:\Program Files (x86)\Je |                        | vc.exe           |   |                         |                     | N/A       | TRUE          |   |
| 06/23/2011 03:08:24 N/A   | C:\Windows\BCUnInstal     |                        |                  |   |                         |                     | N/A       | TRUE          |   |
| 07/14/2009 01:14:18 N/A   | C:\Windows\SysWOW64       | DIIHost.exe            |                  |   |                         |                     | N/A       | TRUE          |   |
| 07/14/2009 01:39:06 N/A   | C:\Windows\system32\E     | llHost.exe             |                  |   |                         |                     | N/A       | TRUE          |   |
| 11/20/2010 13:32:57 N/A   | C:\Windows\system32\c     | onsent.exe             |                  |   |                         |                     | N/A       | TRUE          |   |
| 11/20/2010 13:24:22 N/A   | C:\Windows\System32\a     |                        |                  |   |                         |                     | N/A       | FALSE         |   |
| 01/04/2012 10:44:20 N/A   | C:\Windows\System32\r     |                        |                  |   |                         |                     | N/A       | FALSE         |   |
| 11/20/2010 13:25:59 N/A   | C:\Windows\System32\o     |                        |                  |   |                         |                     | N/A       | FALSE         |   |
| 07/14/2009 01:40:36 N/A   | C:\Windows\System32\E     |                        |                  |   |                         |                     | N/A       | FALSE         |   |
| 07/14/2009 01:39:46 N/A   | C:\Windows\System32\s     |                        |                  |   |                         |                     | N/A       | TRUE          |   |
| 11/20/2010 13:25:27 N/A   | C:\Windows\system32\v     |                        |                  |   |                         |                     | N/A       | TRUE          |   |
| 11/20/2010 13:27:24 N/A   | C:\Windows\System32\r     | emotepg.dll            |                  |   |                         |                     | N/A       | FALSE         |   |
| ◆ ▶ ► System_Shim / 💱 /   |                           |                        |                  |   |                         |                     |           |               |   |



In this data, there are a few things to note. First, since the date and time represent the Last Modified date of the executable, in the 'Miscellaneous' column it will be noted as such so that there is less confusion when looking at the final data in a timeline of events. Second, the 'Exec Flag' column needs to express that statement to understand what the 'TRUE' and 'FALSE' entries represent. Third, since there are not enough columns to match the headers we want, it is OK to leave the cells blank under those extra headers. Finally, we need to insert a column for the name of the computer. The final view of the ShimCache Excel spreadsheet should look like Figure 74.

| F   | ile Home        | Inser | t PageLa  | ayout  | Formulas  | Di    | ata Rei    | riew Vie  | ew Deve    | loper      | Team    |                    |                           |         |                    |        |        |         |              |            | ۵ 🕜                | - 7    |
|-----|-----------------|-------|-----------|--------|-----------|-------|------------|-----------|------------|------------|---------|--------------------|---------------------------|---------|--------------------|--------|--------|---------|--------------|------------|--------------------|--------|
| ľ   | Calibri         |       |           | · A    |           | -     | ≫,-        | 📑 Wrap 1  |            | General    |         | •                  |                           |         |                    |        | *      |         | Σ AutoSum    | Ż          | ñ                  |        |
| 'as | ste 🧹 🏼 🖪 🖌     | Ū     | •   🖽 •   | 🔅 - 🗛  | · = =     | 1     |            | -a- Merge | & Center * | \$ - %     | 6 ,     | 00. 0.<br>0. ♦ 00. | Conditional<br>Formatting |         | Cell<br>• Styles • | Insert | Delete | Format  | Clear *      |            | Find &<br>Select ₹ |        |
| ip  | board 🗔         |       | Font      |        | Gi        |       | Alignm     | ent       | - Fa       | Nu         | umber   | - Gr               |                           | Styles  |                    |        | Cells  |         | E            | diting     |                    |        |
|     | E19             | -     | (=        | fx C:\ | Windows\  | Syste | em32\wsd   | ui.cpl    |            |            |         |                    |                           |         |                    |        |        |         |              |            |                    |        |
| đ   | А               |       | В         |        | С         |       | D          |           |            |            |         |                    | E                         |         |                    |        |        | F       |              |            |                    | G      |
|     | Date/Time       | -     | Account - | Compu  | iter      | - De  | scription  | -         | Details    |            |         |                    |                           |         |                    | -      | Prope  | rties 🔻 | Miscellaneo  | JS         |                    |        |
|     | 07/14/2009 01:: | 4:31  |           | WKS-V  | VIN764BIT | B Fil | e Executio | on: TRUE  | C:\Windo   | ws\SysW    | OW64\r  | rundll32           | .exe                      |         |                    |        |        |         | Date/Time re | eflects La | st Modi            | ied d  |
|     | 07/14/2009 01:: | 4:42  |           | WKS-V  | VIN764BIT | B Fil | e Executio | on: TRUE  | C:\Windo   | ws\SysW    | OW64\t  | tasklist.          | exe                       |         |                    |        |        |         | Date/Time re | eflects La | st Modi            | fied d |
|     | 07/14/2009 01:  | 4:42  |           | WKS-V  | VIN764BIT | B Fil | e Executio | on: FALSE | C:\Windo   | ws\syste   | m32\tas | sklist.ex          | e                         |         |                    |        |        |         | Date/Time re | eflects La | st Modi            | fied d |
|     | 07/14/2009 01:: | 4:45  |           | WKS-V  | VIN764BIT | B Fil | e Executio | on: TRUE  | C:\Program | m Files (x | :86)\Wi | ndows M            | /ail\WinM                 | ail.exe |                    |        |        |         | Date/Time re | eflects La | st Modi            | fied o |
|     | 07/14/2009 01:: | 15:14 |           |        |           |       |            |           | C:\Windo   |            |         |                    | nell.dll                  |         |                    |        |        |         | Date/Time re | eflects La | ist Modi           | fied d |
|     | 07/14/2009 01:  | 88:52 |           | WKS-V  | VIN764BIT | B Fil | e Executio | on: FALSE | C:\Windo   | ws\Syste   | m32\ws  | scui.cpl           |                           |         |                    |        |        |         | Date/Time re | eflects La | ist Modi           | fied o |
| )   | 07/14/2009 01:  | 8:53  |           | WKS-V  | VIN764BIT | B Fil | e Executio | on: TRUE  | C:\Windo   | ws\syste   | m32\scr | rnsave.s           | cr                        |         |                    |        |        |         | Date/Time re | eflects La | ist Modi           | fied d |
|     | 07/14/2009 01:  |       |           |        |           |       |            |           | C:\Windo   |            |         |                    |                           |         |                    |        |        |         | Date/Time re |            |                    |        |
| 2   | 07/14/2009 01:  |       |           |        |           |       |            |           | C:\Windo   |            |         |                    |                           |         |                    |        |        |         | Date/Time re |            |                    |        |
| 3   | 07/14/2009 01:  |       |           | WKS-V  | VIN764BIT | B Fil | e Executio | on: TRUE  | C:\Windo   | ws\syste   | m32\de  | frag.ex            | 2                         |         |                    |        |        |         | Date/Time re |            |                    |        |
| ŀ   | 07/14/2009 01:  |       |           |        |           |       |            |           | C:\Windo   |            |         |                    |                           |         |                    |        |        |         | Date/Time re |            |                    |        |
| 5   | 07/14/2009 01:  |       |           |        |           |       |            |           | C:\Windo   |            |         |                    |                           |         |                    |        |        |         | Date/Time re |            |                    |        |
| 5   | 07/14/2009 01:  |       |           |        |           |       |            |           | C:\Windo   |            |         |                    | e                         |         |                    |        |        |         | Date/Time re |            |                    |        |
| 7   | 07/14/2009 01:  |       |           |        |           |       |            |           | C:\Windo   |            |         |                    |                           |         |                    |        |        |         | Date/Time re |            |                    |        |
| 8   | 07/14/2009 01:  |       |           |        |           |       |            |           | C:\Program |            |         |                    | Maker.exe                 | 2       |                    |        |        |         | Date/Time re |            |                    |        |
| 9   | 07/14/2009 01:  |       |           |        |           |       |            |           | C:\Windo   |            |         |                    |                           |         |                    |        |        |         | Date/Time re |            |                    |        |
| )   | 07/14/2009 01:  |       |           |        |           |       |            |           | C:\Windo   |            |         |                    |                           |         |                    |        |        |         | Date/Time re |            |                    |        |
|     | 07/14/2009 01:  |       | (7        | WKS-V  | VIN764BIT | B Fil | e Executio | on: FALSE | C:\Windo   | ws\syste   | m32\isc | sicpl.ex           |                           |         |                    |        |        |         | Date/Time re | effects La | ist Modi           | ried d |
|     | I 🕨 H System_   | Shim  | <u></u>   |        |           |       |            |           |            |            |         |                    | I 4                       |         |                    |        |        |         |              |            |                    |        |

Figure 74. ShimCache Final Formatting. (Lee, 2014, digital case files)

### 8.4.3. Shellbags

We produced the Shellbags output used in this example by running the Shellbags Explorer tool against a Windows 7 USRCLASS.DAT registry file:

*Sbecmd.exe --timezone="UTC" –d <path to directory containing usrclass.dat>* 

The output of the above command produces a tab delimited file with a .TSV extension. Import the file into Excel, choose TAB as the delimiter in the 'Text Import Wizard' and save it as an .XLSM file to run Macro's against the data (Figure 75).

|             |       | rt Pagel | Layout             | Formulas      | Data R      | eview \    | /iew De     | veloper  | Team          |        |                                    |   |   |             |           |             | 2 م                            | - 6     |
|-------------|-------|----------|--------------------|---------------|-------------|------------|-------------|----------|---------------|--------|------------------------------------|---|---|-------------|-----------|-------------|--------------------------------|---------|
| 🗋 🚆 Cal     | libri | * 11     | · A A              | = =           | ₩           | 📑 Wra      | p Text      | General  |               | -      |                                    |   | + | P 🚺         | Σ Au      | toSum • 🛔   | 7 🗥                            |         |
|             | ΙŪ    | • 🔛 •    | 🆄 - <u>A</u>       | • E =         | ≡ 律様        | E 🔤 Merg   | ge & Center | - \$ - 9 | % , 50        |        | onditional For<br>rmatting × as Ta |   |   | Delete Form |           | Sc          | ort & Find &<br>ter ∗ Select ∗ |         |
| oard G      |       | Font     |                    | Ga            | Align       | ment       |             | 5 N      | lumber        | 5      | Styles                             |   |   | Cells       | -         | Editin      |                                |         |
| A1          |       | . (=     | f <sub>*</sub> Bag | Path          |             |            |             |          |               |        |                                    |   |   |             |           |             | -                              |         |
| A           | В     | С        |                    | F             | F           | G          | Н           | 1        | 1             | K      | 1                                  | М | N | 0           | Р         | Q           | R                              | S       |
| BagPath Slo |       | NodeSlot | MRUPosit           | -<br>Absolute | F ShellType | Value      |             | CreatedO | -<br>Modified | Access | ed(LastWrite                       |   |   |             | FirstExpl |             | or Miscellan                   | eous    |
| BagMRU      | 0     |          |                    |               | (Root folde |            | •           |          |               |        | 4/6/20127                          |   |   | 0           |           |             |                                |         |
| BagMRU      | 1     | 0        | 5                  | Desktop       | SRoot folde | Shared Do  | 3           |          |               |        | 4/6/20127                          |   |   | 0           |           |             |                                |         |
| BagMRU      | 2     | 0        | 7                  | Desktop       | (Root folde | Computer   | 3           |          |               |        | 4/6/2012 7                         |   |   | 0           |           |             |                                |         |
| BagMRU      | 3     | 0        | 0                  | Desktop       | Root folde  | My Compi   | 3           |          |               |        | 4/6/20127                          |   |   | 0           |           | 4/6/2012    | 7:52:10 PM                     | +01:00  |
| BagMRU      | 4     | 0        | 1                  | Desktop\      | Root folde  | User Libra | 7           |          |               |        | 4/6/2012 7                         |   |   | 0           |           |             |                                |         |
| BagMRU      | 5     | 0        | 8                  | Desktop\      | FRoot folde | Recycle bi | 0           |          |               |        | 4/6/2012 7                         |   |   | 0           | 8/22/201  | 1 5:59:13 P | M +01:00                       |         |
| BagMRU      | 6     | 0        | 6                  | i Desktop\    | FRoot folde | Recent Pla | 0           |          |               |        | 4/6/2012 7                         |   |   | 0           | 4/1/2012  | 2:35:32 PN  | / +01:00                       |         |
| BagMRU      | 7     | 0        | 4                  | Desktop\      | (Root folde | Common I   | 0           |          |               |        | 4/6/2012 7                         |   |   | 0           | 4/1/2012  | 2:36:20 PN  | / +01:00                       |         |
| BagMRU      | 8     | 0        | 2                  | Desktop       | Users prop  | Search Fol | 0           |          |               |        | 4/6/20127                          |   |   | 3           | 4/6/2012  | 7:42:33 PN  | / +01:00                       |         |
| BagMRU\(    | 0     | 5        | 1                  | Desktop\      | Control Pa  | Appearan   | 2           |          |               |        | 4/6/2012 2                         |   |   | 0           |           |             |                                |         |
| BagMRU\(    | 1     | 8        | 4                  | Desktop\      | Control Pa  | All Contro | 2           |          |               |        | 4/6/2012 2                         |   |   | 0           |           |             |                                |         |
| BagMRU\(    | 2     |          | 0                  | Desktop\      | Control Pa  | System an  | 2           |          |               |        | 4/6/2012 2                         |   |   | 0           |           | 4/6/2012    | 2:10:45 PM                     | +01:00  |
| BagMRU\(    | 3     | 33       |                    |               | (Control Pa |            |             |          |               |        | 4/6/2012 2                         |   |   | 0           |           |             |                                |         |
| BagMRU\(    | 4     | 32       | 3                  | Desktop\      | Control Pa  | Hardware   | 0           |          |               |        | 4/6/2012 2                         |   |   | 0           | 9/8/2011  | 9:48:12 PN  | / +01:00                       |         |
| BagMRU\(    | 0     | 1        |                    |               | GUID: Con   |            | 1           |          |               |        | 3/15/2012                          |   |   | 0           |           | 3/15/201    | 2 10:12:38 F                   | PM +00: |
| BagMRU\(    | 1     | 0        |                    |               | GUID: Con   |            | 1           |          |               |        | 3/15/2012                          |   |   | 0           |           |             |                                |         |
| BagMRU\(    | 0     | -        |                    |               | (Variable:  |            |             |          |               |        | 11/10/201                          |   |   |             |           |             | 10 7:53:42 /                   |         |
| BagMRU\(    | 0     | 6        | 0                  | Desktop\      | (Variable:  | Screen Re  | 0           |          |               |        | 11/10/201                          |   |   | 0           | 11/10/20  | 1 11/10/20  | 10 7:59:38 /                   | AM +00: |

Figure 75. Shellbags .TSV file imported into Excel. (Lee, 2014, digital case files)

Apply the Standard Format macro and delete the following columns in this order: R, O, N, M, J, I, H, G, F, D, C, B, A. You'll notice that the dates include a UTC offset value of '+00:00' (Figure 76). This value will need to be removed to have the Date/Time column properly formatted. The removal of the offset can be done with a simple search and replace.

| 🔟 🔚 🤊 • 🔍 - 💷 nfury.x   | Ism - Microsoft Excel                  |                            |                            | - 🗆 🗙                           |
|---|--|----------------------------|----------------------------|---------------------------------|
| File Home Insert Page Layout Formulas Data Review View Developer  | Team                                   |                            |                            | a 🕜 🗖 🖾                         |
| A     Calibri     11     A     A     =     ●     Wrap Text     Get       Pate     B     I     I     •     A     ●     ●     ●     ●     ●     Image: A transformed and tran | neral ▼<br>* % * *.00 .000<br>Number 5 | ng * as Table * Styles * * | elete Format               | ort & Find &<br>Iter * Select * |
| B29 • fx 11/10/2010 07:50:38 +00:00   |  |                            |                            |                                 |
| A   | В                                      | С                          | D                          | E 🔺                             |
| 1 AbsolutePath  | CreatedOn                              |                            | AccessedOn                 | LastWriteTime                   |
| 23 Desktop\Control Panel\System and Security\Windows Update   |  | Remove                     |                            | 03/05/2012 13:41:3:             |
| 24 Desktop\Control Panel\System and Security\System   |  | UTC Offset                 |                            | 03/05/2012 13:41:32             |
| 25 Desktop\Control Panel\System and Security\Windows Update\Change settings   |  | Olecinser                  |                            | 09/08/2011 20:54:3(             |
| 26 Desktop\Control Panel\System and Security\Windows Update\Select updates to install   |  |                            |                            | 09/08/2011 20:54:30             |
| 27 Desktop\Control Panel\Programs\Programs and Features   |  |                            |                            | 09/08/2011 20:48:15             |
| 28 Desktop\Shared Documents Folder (Users Files)\Downloads  |  |                            |                            | 04/01/2012 13:33:2              |
| 29 Desktop\Shared Documents Folder (Users Files)\AppData  | 11/10/2010 07:50:38 +00:00             | 11/10/2010 07:50:40 +00:00 | 11/10/2010 07:50:40 +00:00 | 04/01/2012 13:33:2              |
| 30 Desktop\Shared Documents Folder (Users Files)\Documents  |  |                            |                            | 04/01/2012 13:33:2              |
| 31 Desktop\Shared Documents Folder (Users Files)\AppData\Roaming  | 11/10/2010 07:50:38 +00:00             | 08/28/2011 20:38:04 +00:00 | 08/28/2011 20:38:04 +00:00 | 08/28/2011 22:42:0:             |
| 32 Desktop\Shared Documents Folder (Users Files)\AppData\Roaming\Skype  | 08/25/2011 21:52:38 +00:00             | 08/28/2011 22:41:58 +00:00 | 08/28/2011 22:41:58 +00:00 | 08/28/2011 22:42:0:             |
| 33 Desktop\Shared Documents Folder (Users Files)\AppData\Roaming\Skype\Pictures   | 08/25/2011 21:56:24 +00:00             | 08/25/2011 21:56:24 +00:00 | 08/25/2011 21:56:24 +00:00 | 08/28/2011 22:42:0:             |
| 34 Desktop\Shared Documents Folder (Users Files)\Documents\StarFury   |  |                            |                            | 04/01/2012 13:34:5              |
| 35 Desktop\Shared Documents Folder (Users Files)\Documents\StarFury\StarFury  | 03/12/2012 20:50:08 +00:00             | 03/12/2012 20:50:16 +00:00 | 03/12/2012 20:50:16 +00:00 | 03/12/2012 20:50:19             |
| 36 Desktop\Computers and Devices\controller   |  |                            |                            | 03/15/2012 22:12:38             |
| 37 Desktop\Computers and Devices\System and Security  |  |                            |                            | 03/15/2012 22:12:38             |
| 38 Desktop\Computers and Devices\All Control Panel Items  |  |                            |                            | 03/15/2012 22:12:38             |
| 39 Desktop\Computers and Devices\controller\controller\WebDavShare  |  |                            |                            | 03/15/2012 22:12:38             |
| 40 Desktop\Computers and Devices\controller\Network Connections   |  |                            |                            | 03/15/2012 22:12:38 🖉           |
| UsrClass_win7-64_nfury.dat  |  | 4                          |                            | • •                             |
| Ready 🛅   |  |                            | 🔳 🗆 🛄 100% 🤆               |                                 |
|   |  |                            |                            |                                 |

Figure 76. Dates contain a UTC Offset. (Lee, 2014, digital case files)

After removing the offset and formatting the date and times correctly, the result should look like Figure 77.

| 🔣   🛃 🧐 🕶 🔍 -   ਦ nfu  | ıry.xlsm - Microsoft Ex                       | cel   |                     |                         | - 🗆 🗙                                      |
|--|---|---|---------------------|-------------------------|--|
| File Home Insert Page Layout Formulas Data Review View Devel   | loper Team                                    |   |                     |                         | a 🕜 🗕 🗗 🛛                                  |
| Calibri     11     A*     = = =     ⊗+     = Wrap Text       Paste     Image: Calibria     Image: Calibria     Image: Calibria     Image: Calibria       B     Image: Image: Calibria     Image: Calibria     Image: Calibria     Image: Calibria       Composed rs     Font     Image: Calibria     Image: Calibria | Custom ▼<br>\$ ▼ % \$ \$.00 \$.00<br>Number ☞ | Conditional Format<br>Formatting + as Table + S<br>Styles |                     | Format<br>▼ Clear ▼ Edi | Sort & Find &<br>Filter * Select *<br>ting |
| B22 • (* J* 03/15/2012 22:07:00  |   |   |                     |                         | >  |
| A  | В   | С   | D                   | E                       | F 🗖  |
| 1 AbsolutePath   | 💌 CreatedOn 🖉                                 | ModifiedOn 🛛  | AccessedOn 🛛        | LastWriteTime           | FirstExplored 🛛 💌 L                        |
| 20 Desktop\Control Panel\All Control Panel Items\System  |   |   |                     | 03/15/2012 22:12:38     | 11/10/2010 08:16:02 0                      |
| 21 Desktop\Control Panel\All Control Panel Items\Security Tools  | 08/24/2011 16:47:00                           | 03/15/2012 22:07:04                                       | 03/15/2012 22:07:04 | 03/15/2012 22:12:38     |  |
| 22 Desktop\Control Panel\All Control Panel Items\Security Tools\BC Wipe  | 03/15/2012 22:07:00                           | 03/15/2012 22:07:08                                       | 03/15/2012 22:07:08 | 03/15/2012 22:12:38     | 03/15/2012 22:12:38 0                      |
| 23 Desktop\Control Panel\System and Security\Windows Update  |   |   |                     | 03/05/2012 13:41:32     |  |
| 24 Desktop\Control Panel\System and Security\System  |   |   |                     | 03/05/2012 13:41:32     | 03/05/2012 13:41:32 0                      |
| 25 Desktop\Control Panel\System and Security\Windows Update\Change settings  |   |   |                     | 09/08/2011 20:54:30     | 08/15/2011 14:32:06 0                      |
| 26 Desktop\Control Panel\System and Security\Windows Update\Select updates to inst   | all   |   |                     | 09/08/2011 20:54:30     | 09/08/2011 20:52:24                        |
| 27 Desktop\Control Panel\Programs\Programs and Features  |   |   |                     | 09/08/2011 20:48:15     | 08/28/2011 22:57:34 0                      |
| 28 Desktop\Shared Documents Folder (Users Files)\Downloads   |   |   |                     | 04/01/2012 13:33:27     | 03/15/2012 22:12:38                        |
| 29 Desktop\Shared Documents Folder (Users Files)\AppData   | 11/10/2010 07:50:38                           | 11/10/2010 07:50:40                                       | 11/10/2010 07:50:40 | 04/01/2012 13:33:27     |  |
| 30 Desktop\Shared Documents Folder (Users Files)\Documents   |   |   |                     | 04/01/2012 13:33:27     | 0  |
| 31 Desktop\Shared Documents Folder (Users Files)\AppData\Roaming   | 11/10/2010 07:50:38                           | 08/28/2011 20:38:04                                       | 08/28/2011 20:38:04 | 08/28/2011 22:42:03     | 0  |
| 32 Desktop\Shared Documents Folder (Users Files)\AppData\Roaming\Skype   | 08/25/2011 21:52:38                           | 08/28/2011 22:41:58                                       | 08/28/2011 22:41:58 | 08/28/2011 22:42:03     | 0  |
| 33 Desktop\Shared Documents Folder (Users Files)\AppData\Roaming\Skype\Pictures  | 08/25/2011 21:56:24                           | 08/25/2011 21:56:24                                       | 08/25/2011 21:56:24 | 08/28/2011 22:42:03     | 08/28/2011 22:42:03 0                      |
| 34 Desktop\Shared Documents Folder (Users Files)\Documents\StarFury  |   |   |                     | 04/01/2012 13:34:55     | 0  |
| 35 Desktop\Shared Documents Folder (Users Files)\Documents\StarFury\StarFury   | 03/12/2012 20:50:08                           | 03/12/2012 20:50:16                                       | 03/12/2012 20:50:16 | 03/12/2012 20:50:19     | 03/12/2012 20:50:19 0                      |
| 36 Desktop\Computers and Devices\controller  |   |   |                     | 03/15/2012 22:12:38     | 0  |
| 37 Desktop\Computers and Devices\System and Security   |   |   |                     | 03/15/2012 22:12:38     |  |
| H ◀ → H UsrClass_win7-64_nfury.dat   |   | I 4   | 1                   |                         |  |
| Ready 🛅  |   |   |                     | 🖽 🗆 🛄 100%              |  |

Figure 77. Standard Format with Dates and Times fixed. (Lee, 2014, digital case files)

There are six columns of Dates and Times. For this paper, the information sought is the first date the resource was accessed and the last date the resource was accessed. Manually going through all the entries and getting those two dates for each resource would consume too much time. To make finding the two dates and sorting the Date/Time column easier, we have provided VBA code on the GitHub site called 'Shellbags\_Standard\_Format\_Module.bas' (https://github.com/gregorylalla/GCIH\_Gold/blob/master/Code/Singles/Module\_BAS\_Files/Shellbags/Shellbags\_Sta ndard\_Format\_Module.bas) which will automatically do the work for you. The script will produce two rows for each entry. One for the first time it was accessed and one for the last time it was accessed. If there is only one date for the entry or the dates shown are the same or within 3 seconds of each other, then only one row will be produced for that entry. Figure 78 shows the result of running the VBA code.

| 🔚 🤊 - 🗠 📄                          |  | nfury.xlsm - Microsoft Excel   | _ 🗆        | ×   |
|------------------------------------|--|--|------------|-----|
| File Home Insert Page Layout       | Formulas Data Review Vie                                 | w learn  | a 🕜 🗆      | æ   |
| aste<br>→ ✓ Format Painter B I U → | $\frac{11}{2} \cdot \Delta^* \Delta^* = = = \Rightarrow$ | Conditional Fermat Cell Insert Delete Format 2 Celler - Solt € Sol |            |     |
| Clipboard 5 Eon                    |  | gement 🗟 Number 🗟 Styles Cells Editing   |            |     |
| D4 • (* <i>f</i> <sub>N</sub>      |  |  |            | _   |
| A B                                | C D  | E F G  | H          |     |
| Date/Time Account                  | Computer V Description                                   | Details  | Artifact 🝸 | _   |
| 04/06/2012 18:52:10 nfury          |  | Desktop\Control Panel  | Shellbags  |     |
| 04/06/2012 18:52:10 nfury          |  | Desktop\Shared Documents Folder (Users Files)  | Shellbags  |     |
| 04/06/2012 18:52:10 nfury          |  | Desktop\Computers and Devices  | Shellbags  |     |
| 04/06/2012 18:52:10 nfury          |  | Desktop\My Computer  | Shellbags  |     |
| 04/06/2012 18:52:10 nfury          | Win764bitb Last Accessed                                 |  | Shellbags  |     |
| 04/05/2012 18:52:10 nfury          | Win764bitb Last Accessed                                 |  | Shellbags  |     |
| 08/22/2011 16:59:13 nfury          | Win764bitb First Accessed                                |  | Shellbags  |     |
| 04/06/2012 18:52:10 nfury          | Win764bitb Last Accessed                                 |  | Shellbags  |     |
| 0 04/01/2012 13:35:32 nfury        | Win764bitb First Accessed                                |  | Shellbags  |     |
| 1 04/06/2012 18:52:10 nfury        | Win764bitb Last Accessed                                 |  | Shellbags  |     |
| 2 04/01/2012 13:36:20 nfury        | Win764bitb First Accessed                                |  | Shellbags  |     |
| 3 04/06/2012 18:52:10 nfury        | Win764bitb Last Accessed                                 | Desktop\Search Folder  | Shellbags  |     |
| 4 04/06/2012 18:42:33 nfury        | Win764bitb First Accessed                                |  | Shellbags  |     |
| 5 04/06/2012 13:10:45 nfury        | Win764bitb Last Accessed                                 |  | Shellbags  |     |
| 6 04/06/2012 13:10:45 nfury        | Win764bitb Last Accessed                                 |  | Shellbags  |     |
| 7 04/06/2012 13:10:45 nfury        | Win764bitb Last Accessed                                 |  | Shellbags  |     |
| 8 04/06/2012 13:10:45 nfury        | Win764bitb Last Accessed                                 |  | Shellbags  |     |
| 9 04/06/2012 13:10:45 nfury        | Win764bitb 📑 t Accessed                                  | Desktop\Control Panel\Hardware and Sound   | Shellbags  |     |
| → → I nfury 🔩                      |  |  |            | 1 b |

*Figure 78. Shellbags View after running Shellbags\_Date\_Sorter code. (Lee, 2014, digital case files)* 

### 8.4.4. AutoRun Entries

To parse autorun data, we run the autorunsc.exe command against the registry files of a system. This parsing can be done offline by mounting an image of the system and pointing the tool to the mapped drive:

```
Autorunsc.exe -a * -c -m -s -z M:\Windows M:\Users\<profilename> >
```

autoruns\_profilename.csv

The options in the above command are:

- -a \*: Check All
- -c: CVS output need to direct to a file
- -m: Hide Microsoft Verified Signed
- -s: Check signature
- -z: offline analysis

Open the resulting .CSV file in Excel and apply the standard formatting (Figure

79).

| 🗙   🛃 🍤 🕶 (🗠 –   | Ŧ                           |          |   | auto        | runs-win7 | -64-nfury.x                  | dsm - M                 | icrosoft Exc   | el   |               |            |                                  |                    | -        |     | ×    |
|------------------|-----------------------------|----------|---|-------------|-----------|------------------------------|-------------------------|----------------|--|---------------|------------|----------------------------------|--------------------|----------|-----|------|
| File Home        | Insert Page Layout Fo       | ormulas  | Data Revi                                     | ew View     | Develop   | er Team                      |                         |                |  |               |            |                                  |                    | ۵ 🕜      | - ( | de ک |
| Paste of B.      |                             |          | E III (III (IIII))<br>E III (IIII)<br>Alianme | 📑 Wrap Text |           | seneral<br>\$ - % •          | ▼<br>00. 00.<br>00. 00. |                | Format Cell<br>as Table + Styles +<br>Styles | Insert Delete | Format     | Σ AutoSum *<br>Fill *<br>Clear * | Sort &<br>Filter * |          |     |      |
| H543             |                             |          | {79eac9e3-baf9                                |             |           |                              |                         |                | Styles                                       | cens          |            | Edi                              | iting              |          | _   | -    |
| 11545            | A                           | (02515)( | B   | 1100 0002 1 | C C       | D                            |                         |                | F  |               |            |                                  |                    | F        | _   |      |
| 1 Entry Location | A                           |          | intry   |             | Enabled   | <ul> <li>Category</li> </ul> |                         | escription     | E  |               | • Publishe | er.                              |                    | r        |     |      |
|                  | .RE\Classes\Protocols\Filte |          | pplication/octe                               | t-stream    | enabled   | Explorer                     |                         |                | r Runtime Execu                              |               |            | d) Microsoft                     | Window             | vs       |     |      |
|                  | RE\Classes\Protocols\Filte  |          | pplication/x-co                               |             | enabled   | Explorer                     |                         |                | r Runtime Execu                              |               |            | d) Microsoft                     |                    |          |     |      |
|                  | RE\Classes\Protocols\Filte  |          | pplication/x-m                                |             | enabled   | Explorer                     |                         |                | F Runtime Execu                              |               |            | d) Microsoft                     |                    |          |     |      |
|                  | RE\Classes\Protocols\Filte  |          | ext/xml                                       |             | enabled   | Explorer                     | N                       | licrosoft Offi | ce XML MIME Fi                               | lter          | (Verifie   | ,<br>d) Microsoft                | Corpora            | ation    |     |      |
| 39 HKLM\SOFTWA   | RE\Classes\Protocols\Hand   | ller a   | bout  |             | enabled   | Explorer                     | N                       | licrosoft (R)  | HTML Viewer                                  |               | (Verifie   | d) Microsoft                     | Window             | vs       |     |      |
| 40 HKLM\SOFTWA   | RE\Classes\Protocols\Hand   | ller o   | dl  |             | enabled   | Explorer                     | c                       | LE32 Extensi   | ons for Win32                                |               | (Verifie   | d) Microsoft                     | Window             | vs       |     |      |
| 41 HKLM\SOFTWA   | RE\Classes\Protocols\Hand   | iler d   | ivd   |             | enabled   | Explorer                     | А                       | ctiveX contro  | ol for streaming                             | video         | (Verifie   | d) Microsoft                     | Window             | vs       |     |      |
| 42 HKLM\SOFTWA   | RE\Classes\Protocols\Hand   | ller f   | ile   |             | enabled   | Explorer                     | C                       | LE32 Extensi   | ons for Win32                                |               | (Verifie   | d) Microsoft                     | Window             | VS       |     |      |
| 43 HKLM\SOFTWA   | RE\Classes\Protocols\Hand   | ller f   | tp  |             | enabled   | Explorer                     | C                       | LE32 Extensi   | ons for Win32                                |               | (Verifie   | d) Microsoft                     | Window             | vs       |     |      |
|                  | RE\Classes\Protocols\Hanc   |          | nttp  |             | enabled   | Explorer                     | C                       | LE32 Extensi   | ons for Win32                                |               | (Verifie   | d) Microsoft                     | Window             | vs       |     |      |
|                  | RE\Classes\Protocols\Hanc   |          | nttps   |             | enabled   | Explorer                     | -                       |                | ons for Win32                                |               |            | d) Microsoft                     |                    |          |     |      |
|                  | RE\Classes\Protocols\Hanc   |          | ts  |             | enabled   | Explorer                     |                         |                | oTech Storage S                              | ystem Library |            | d) Microsoft                     |                    |          |     |      |
|                  | RE\Classes\Protocols\Hanc   |          | avascript                                     |             | enabled   | Explorer                     |                         |                | HTML Viewer                                  |               |            | d) Microsoft                     |                    |          |     |      |
|                  | RE\Classes\Protocols\Hanc   |          | ocal  |             | enabled   | Explorer                     | -                       |                | ons for Win32                                |               |            | d) Microsoft                     |                    |          |     |      |
|                  | RE\Classes\Protocols\Hanc   |          | nailto  |             | enabled   | Explorer                     |                         |                | HTML Viewer                                  |               |            | d) Microsoft                     |                    |          |     |      |
|                  | RE\Classes\Protocols\Hanc   |          | nhtml   |             | enabled   | Explorer                     |                         |                | rnet Messaging                               | API Resources |            | d) Microsoft                     |                    |          |     |      |
|                  | RE\Classes\Protocols\Hand   |          | nk  |             | enabled   | Explorer                     |                         |                | ons for Win32                                |               |            | d) Microsoft                     |                    |          |     |      |
|                  | RE\Classes\Protocols\Hanc   | lier n   | ns-help                                       |             | enabled   | Explorer                     | N                       |                | lp Data Services                             | Module        | (Not ver   | ified) Micro                     | soft Cor           | poration | 1   |      |
| Ready Sautorur   | s-win7-64-nfury 🕲           |          |   |             |           |                              |                         | 14             |  |               |            | 回 円 100%                         |                    |          |     | +    |

Figure 79. Autoruns Standard Formatting. (Lee, 2014, digital case files)

You should delete the following columns: Enabled, Category, Publisher, MD5, SHA-1, and SHA-256. Two columns, 'Entry Location' and 'Entry' can be combined into one column to preserve data that might not fit into the suggested columns used in this paper (Figure 80).

| <b>⊡ 10 ×</b> (0 ×   <del>-</del>  | autoruns-win7-64-nfury.xlsm - Microsoft Excel   | >                                  |
|--|---|------------------------------------|
| File Home Insert Page Layout Form  | nulas Data Review View Developer Team   | a 😮 🗆 🖬                            |
| $ \begin{array}{c c} & & \\ & & \\ & & \\ & & \\ aste \\ & & \\ & & \\ \end{array}                       $ | E = = 2 2 2 2 Merce & Center × \$ × % \$ , *% % Conditional Format Cell Insert Delete Format                    | Sort & Find &<br>Filter * Select * |
| ipboard 🗊 Font 🕞   | Alignment Function to Combine Columns   | ing                                |
| C2 • (* 5x =A2 & "   |   |                                    |
| A  | Seperated by a Colon  |                                    |
| Entry Location   | ▼ Entry ▼   | <ul> <li>Description</li> </ul>    |
| HKLM\System\CurrentControlSet\Control\Se   | essi autocheck autochk * HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute: autocheck autochk * | Auto Check Utility                 |
| HKLM\System\CurrentControlSet\Control\S  | %systemroot%\syste 22\scext.dll   | Service Control Ma                 |
| HKLM\System\CurrentControlSet\Services   | TheLookupSvc  | Processes applicat                 |
| HKLM\System\CurrentControlSet\Services   | ALG   | Provides support                   |
| HKLM\System\CurrentControlSet\Services   | AppIDS  | Determines and v                   |
| HKLM\System\CurrentControlSet\Services   | Appinfo   | Facilitates the run                |
| HKLM\System\CurrentControlSet\Services   | AppMgmt   | Processes installa                 |
| HKLM\System\CurrentControlSet\Services   | AudioEndpointBuilder  | Manages audio de                   |
| HKLM\System\CurrentControlSet\Services   | AudioSrv  | Manages audio fo                   |
| HKLM\System\CurrentControlSet\Services   | Axinstsv Combine Values   | Provides User Acc                  |
| 2 HKLM\System\CurrentControlSet\Services   | BDESVC of Column A & B  | BDESVC hosts the                   |
| B HKLM\System\CurrentControlSet\Services   | BFE   | The Base Filtering                 |
| HKLM\System\CurrentControlSet\Services   | BITS  | Transfers files in t               |
| HKLM\System\CurrentControlSet\Services   | Browser   | Maintains an upda                  |
| 5 HKLM\System\CurrentControlSet\Services   | bthserv   | The Bluetooth ser                  |
| 7 HKLM\System\CurrentControlSet\Services   | CertPropSvc   | Copies user certifi                |
| 3 HKLM\System\CurrentControlSet\Services   | clr_optimization_v4.0.30319_32  | Microsoft .NET Fra                 |
| HKLM\System\CurrentControlSet\Services   | clr_optimization_v4.0.30319_64  | Microsoft .NET Fra                 |
| 💶 🕨 autoruns-win7-64-nfury   |   |                                    |
| eady 🛅   | 100%  |                                    |

Figure 80. Combine Entry Location and Entry. (Lee, 2014, digital case files)

The combined columns should look like Column A in Figure 81.

| 🔟 🔛 🧐 • (° • ) =  | autoruns-win7-64-nfury.xlsm - Micro                               | soft Excel                                     | ×  |
|---|---|--|--|
| File Home Insert Page Layout Formulas Data  | Review View Developer Team  | Result of Comb                                 | ining 🗠 😗 🖬 🖾  |
| $\beta$ Calibri $11 \rightarrow A^* A^* \equiv = =$ Paste $\beta$ $I \perp \forall = = A^* A^*$ | ≫ → 🔐 Wrap Text General ×<br>律律 魏 Merge & Center × \$ × % > → 🛲 👯 | Inditional Format Cell<br>Insert Delete Format | ∑ AutoSum ×<br>Fill × Sort & Find &<br>Clear × Filter × Select × |
| Clipboard 🕞 Font  | Alignment G wember G  | Styles Cells                                   | Editing  |
| D4 - f %SystemRoot%\Syst  |   |  | v  |
| A   | В   | С  | D  |
| 1 Details   | Desption  | Properties 🗸                                   | Miscellaneous  |
| 231 HKLM\System\CurrentControlSet\Services: intelide  | ntel PCI IDE Driver   | c:\windows\system32\drivers\intelide.sys       | system32\drivers\intelide.sys                                    |
| 232 HKLM\System\CurrentControlSet\Services: intelppm  | Processor Device Driver   | c:\windows\system32\drivers\intelppm.sys       | system32\DRIVERS\intelppm.sys                                    |
| 233 HKLM\System\CurrentControlSet\Services: IpFilterDriver                                      | P Traffic Filter Driver   | c:\windows\system32\drivers\ipfltdrv.sys       | system32\DRIVERS\ipfltdrv.sys                                    |
| 234 HKLM\System\CurrentControlSet\Services: IPMIDRV   | WMI IPMI DRIVER   | c:\windows\system32\drivers\ipmidrv.sys        | \SystemRoot\system32\drivers\IPMI                                |
| 235 HKLM\System\CurrentControlSet\Services: IPNAT   | P Network Address Translator                                      | c:\windows\system32\drivers\ipnat.sys          | System32\drivers\ipnat.sys                                       |
| 236 HKLM\System\CurrentControlSet\Services: IRENUM  | R Bus Enumerator  | c:\windows\system32\drivers\irenum.sys         | system32\drivers\irenum.sys                                      |
| 237 HKLM\System\CurrentControlSet\Services: isapnp  | PNP ISA Bus Driver  | c:\windows\system32\drivers\isapnp.sys         | \SystemRoot\system32\drivers\isapr                               |
| 238 HKLM\System\CurrentControlSet\Services: iScsiPrt  | Microsoft iSCSI Initiator Driver                                  | c:\windows\system32\drivers\msiscsi.sys        | \SystemRoot\system32\drivers\msis                                |
| 239 HKLM\System\CurrentControlSet\Services: kbdclass  | Keyboard Class Driver   | c:\windows\system32\drivers\kbdclass.sys       | \SystemRoot\system32\drivers\kbdc                                |
| 240 HKLM\System\CurrentControlSet\Services: kbdhid  | HID Keyboard Filter Driver  | c:\windows\system32\drivers\kbdhid.sys         | \SystemRoot\system32\drivers\kbdh                                |
| 241 HKLM\System\CurrentControlSet\Services: KSecDD  | Kernel Security Support Provider Interface                        | c:\windows\system32\drivers\ksecdd.sys         | System32\Drivers\ksecdd.sys                                      |
| 242 HKLM\System\CurrentControlSet\Services: KSecPkg   | Kernel Security Support Provider Interface Packages               | c:\windows\system32\drivers\ksecpkg.sys        | System32\Drivers\ksecpkg.sys                                     |
| 243 HKLM\System\CurrentControlSet\Services: ksthunk   | Kernel Streaming WOW Thunk Service                                | c:\windows\system32\drivers\ksthunk.sys        | \SystemRoot\system32\drivers\ksth                                |
| 244 HKLM\System\CurrentControlSet\Services: Iltdio  | Link-Layer Topology Mapper I/O Driver                             | c:\windows\system32\drivers\lltdio.sys         | system32\DRIVERS\IItdio.sys                                      |
| 245 HKLM\System\CurrentControlSet\Services: LSI_FC  | SI Fusion-MPT FC Driver (StorPort)                                | c:\windows\system32\drivers\lsi_fc.sys         | \SystemRoot\system32\DRIVERS\Isi_                                |
| 246 HKLM\System\CurrentControlSet\Services: LSI_SAS   | SI Fusion-MPT SAS Driver (StorPort)                               | c:\windows\system32\drivers\lsi_sas.sys        | \SystemRoot\system32\drivers\lsi_s                               |
| 247 HKLM\System\CurrentControlSet\Services: LSI_SAS2  | SI SAS Gen2 Driver (StorPort)                                     | c:\windows\system32\drivers\lsi_sas2.sys       | \SystemRoot\system32\DRIVERS\Isi_                                |
| 248 HKLM\System\CurrentControlSet\Services: LSI_SCSI  | SI Fusion-MPT SCSI Driver (StorPort)                              | c:\windows\system32\drivers\lsi_scsi.sys       | system32\drivers\lsi_scsi.sys 🚽                                  |
| H + H autoruns-win7-64-nfury  | 1   | II 4   | •  |
| Ready 🛅   |   |  | III I 100% — V   |
|   |   |  |  |

Figure 81. The result of Combining Columns. (Lee, 2014, digital case files)

#### 8.4.5. Web Browser Logs

The example in this section will use the tool PASCO to parse the Internet

Explorer files:

pasco.exe <path>

After you run the above command, open the resulting TSV file in Excel using tab as the delimiter. You should manually delete the first two rows which are not needed (Figure 82).

| l 🖬 🤊   | • @ -  ∓  |                                       |  |                       |          |                    |            | nromar                     | noff_temp  | int.tsv - | Micros                  | oft Excel                        |                              |          |            |          |             |                                 | - 1       |        |
|---|---|---------------------------------------|--|-----------------------|----------|--------------------|------------|----------------------------|------------|-----------|-------------------------|----------------------------------|------------------------------|----------|------------|----------|-------------|---------------------------------|-----------|--------|
| File  | Home Inse   | ert Pag                               | e Layout                               | Formulas              | Data     | Review             | View E     | Developer                  | Team       |           |                         |                                  |                              |          |            |          |             |                                 | ۵ 🕜       | - 7    |
| Paste   | Cut<br>Copy ~<br>Format Painter                                     | Calibri<br>B                          | • 1<br><u>U</u> •   = •                | 1 · A A               | · = =    | <b>_</b> ≫<br>≡ (# | _          | /rap Text<br>lerge & Cente | Genera     |           | *<br>00. 00.<br>0.♦ 00. | Conditional I<br>Formatting * a: | ormat Cell<br>Table + Styles | insert   | Delete For | 📕 😺 Fi   | So          | ort & Find &<br>Iter * Select * |           |        |
| Clipb   | oard 5  |                                       | Font                                   |                       | 6        | Ali                | gnment     |                            | Gi .       | Number    | G.                      | St                               | les                          |          | Cells      |          | Editing     | g                               |           |        |
| 4   | 42 •  | • (=                                  | f <sub>x</sub>                         |                       |          |                    |            |                            |            |           |                         |                                  |                              |          |            |          |             |                                 |           |        |
| A   | В   | С                                     | D                                      | E                     | F        | G                  | Н          | 1                          | J          | К         | L                       | M                                | N                            | 0        | Р          | Q        | R           | S                               | т         | U      |
|   | y File: C:\User   | s\User\D                              | asktop\Case                            | es\win7-32            | -nromano | ff-10.3.58.        | 5\Artifact | s\ie\nroma                 | noff\inde> | .dat Vers | ion: 5.2                |                                  |                              |          |            |          |             |                                 |           |        |
| A-2   |   |                                       |  |                       |          |                    |            |                            |            |           |                         |                                  |                              |          |            |          |             |                                 |           |        |
| Ti  | PL I  |                                       | D ACCESS TI                            |                       |          |                    |            |                            |            |           |                         |                                  |                              |          |            |          |             |                                 |           |        |
| URL   | · · · · //ie  |                                       |  |                       |          |                    |            |                            |            |           |                         | B00000627E                       |                              |          |            |          | a DEVa PSA  | a PSDa OUR                      | IND", pol | cyref= |
| URL   | https://  |                                       |  |                       |          |                    |            |                            |            |           |                         | th: 103 X-Ser                    |                              |          |            |          |             |                                 |           |        |
| URL   |   |                                       |  |                       |          |                    |            |                            |            |           |                         | th: 10856 X-S                    |                              |          |            |          |             |                                 |           |        |
| URL   |   |                                       |  |                       |          |                    |            |                            |            |           |                         | 781cc0c9390f                     |                              |          |            |          |             |                                 |           |        |
| URL   |   |                                       |  |                       |          |                    |            |                            |            |           |                         | IngibECRwYo                      |                              |          |            |          |             |                                 |           |        |
| URL   |   |                                       |  |                       |          |                    |            |                            |            |           |                         | 4n8sVKe4XR                       |                              |          |            |          |             |                                 |           |        |
| URL   |   |                                       |  |                       |          |                    |            |                            |            |           |                         | lo47A13gycIY                     |                              |          |            |          | equest-id:  | 5A92C09357                      | 333954 ET | ag: "c |
| URL   |   |                                       |  |                       |          |                    |            |                            |            |           |                         | th: 347 X-Ser                    |                              | r-web-ap | ps2 ~U:n   | romanoff |             |                                 |           |        |
| URL   |   |                                       |  |                       |          |                    |            |                            |            |           |                         | n: 43 ~U:nro                     |                              |          |            |          |             |                                 |           |        |
| URL   |   |                                       |  |                       |          |                    |            |                            |            |           |                         | n: 43 ~'U:nro                    |                              |          |            |          |             |                                 |           |        |
|   |   |                                       |  |                       |          |                    |            |                            |            |           |                         | -MUHpQq2kk                       |                              |          |            |          |             |                                 |           |        |
|   | http://a0   |                                       |  |                       |          |                    |            |                            |            |           |                         | tC+x9XwLg0b                      |                              |          |            |          |             |                                 |           |        |
| URL   |   |                                       |  | 3NYqQ nr              | 201RVRN  |                    |            |                            |            |           |                         | gCNz7uHYhM                       |                              |          |            |          |             |                                 |           |        |
| URL<br>URL                                    | http://a0.  |                                       |  |                       |          |                    | 200 04 4   | -amz-id-2: c               | dmjZUJ8w+  | SKR/ug08  |                         |                                  |                              |          |            |          |             |                                 |           | С ЕТа  |
| URL<br>URL<br>URL                             | http://a0.<br>http://a0.  | . <b>""""""</b> "                     | " """"""""                             | image_no              |          |                    |            |                            |            |           |                         |                                  |                              |          |            |          |             |                                 |           |        |
| URL<br>URL<br>URL<br>URL                      | http://a0.<br>http://a0.<br>http://a3.                              | . #########<br>: #########            | # #################################### | image_no<br>default_p | OWEBFPC  | HTTP/1.1           | 200 OK x   | -amz-id-2: t               |            |           |                         | /XcWu/yzmll                      |                              |          |            |          | nz-request- | -id: 635523C                    | 50D72EC27 | ETag   |
| URL<br>URL<br>URL<br>URL                      | http://a0.<br>http://a0.<br>http://a3.                              | . #########<br>: #########            | # #################################### | image_no<br>default_p | OWEBFPC  | HTTP/1.1           | 200 OK x   | -amz-id-2: t               |            |           |                         | /IXcWu/yzmll<br>or-web-apps      |                              |          |            |          | nz-request- | -id: 635523C                    | 50D72EC2  | ETag   |
| URL<br>URL<br>URL<br>URL<br>URL<br>URL<br>URL | http://a0.<br>http://a0.<br>http://a3.<br>https://ag<br>nromanoff_t | . ########<br>#########<br>: ######## | # #################################### | image_no<br>default_p | OWEBFPC  | HTTP/1.1           | 200 OK x   | -amz-id-2: t               |            |           |                         |                                  |                              |          |            |          |             | -id: 635523C                    | 50D72EC27 | ETag   |

Figure 82. Delete first two rows. (Lee, 2014, digital case files)

You should delete the following columns: Modified Time, and Directory. Change the 'ACCESS TIME' column formatting to 'mm/dd/yyyy hh:mm:ss' and move that column to Column 'A.' Apply the standard formatting and headers and then manually fill in the missing values in the empty columns. Once complete, it should appear like Figure 83.

| X    | 🛃 🎝 • 🖓 •      | Ŧ        |                       |                 |                                 |                             | nromanoff_           | temp_int.xlsm   | - Micro             | osoft Excel                 |            |                  |           |        |         |                      |           |                 | -         |         |
|------|----------------|----------|-----------------------|-----------------|---------------------------------|-----------------------------|----------------------|-----------------|---------------------|-----------------------------|------------|------------------|-----------|--------|---------|----------------------|-----------|-----------------|-----------|---------|
| Fi   | ile Home       | Insert   | Page Lay              | out Formulas    | Data Rev                        | ew Viev                     | v Developer Tea      | im              |                     |                             |            |                  |           |        |         |                      |           |                 | ۵ 🕜       | - 5     |
| ľ    | 📕 🔏 Cut        | Ca       | alibri                | * 11 * A        | ۸ <sup>×</sup> = =              | ₽ ≫                         | 📑 Wrap Text          | General         | •                   | <b>S</b>                    | J.         |                  |           | *      |         | Σ AutoSu<br>↓ Fill ▼ | " · 🎦     | A               |           |         |
| Pas  | te 🛷 Format Pa | inter B  | 3 <i>I</i> <u>U</u> ∗ | ·   🖽 +   🌺 + 🛓 | 🛓 · 🔳 🗏 🕸                       | ÷ •                         | 🙀 Merge & Center 🔻   | \$ - % ,        | 00. 0,<br>00. ♦ 00. | Conditional<br>Formatting * | Format     | Cell<br>Styles T | Insert    | Delete | Format  | Q Clear ▼            |           | Find & Select * |           |         |
|      | Clipboard      | 5        |                       | Font            | 5                               | Alignm                      | ent G                | Number          | G.                  |                             | Styles .   | Styles           |           | Cells  |         | -                    | Editing   | Jereet          |           |         |
|      | E4             | • (      | f                     | https://apps.   | .skype.com/ho                   | ne/images                   | /buttons/GreenButt   | ons_transparer  | nt_bg.pn            | g                           |            |                  |           |        |         |                      |           |                 |           |         |
| 1    | А              |          | В                     | С               | D                               |                             | E                    |                 |                     | F                           |            |                  |           |        |         | G                    |           |                 | н         |         |
| 1    | Date/Time      | - A      | ccount 👻              | Computer        | <ul> <li>Description</li> </ul> | <ul> <li>Details</li> </ul> |                      |                 | - Prop              | erties                      |            | - N              | iscellan  | eous   |         |                      |           | -               | Artifact  |         |
| 2    | 11/10/2010 08: | 44:11 nr | romanoff              | WKS-WIN732BIT   | A URL                           | https://                    | ieonline.microsoft.c | om/favicon.ico  | favio               | on[1].ico                   |            | H                | TTP/1.1 2 | 00 OK  | ETag: A | 2B3D508B9            | 64F05DEE  | 9225 01         | E Browse  | er Cach |
| 3    | 04/06/2012 19: | 43:57 nr | romanoff              | WIN732BIT       | A                               | https://                    | apps.skype.com/hor   | ne/images/fan   | cyŁ fancy           | _shadow_w                   | [1].png    | н                | TTP/1.1 2 | 00 OK  | Conten  | t-Type: im           | ago/      | content         | IE Browse | er Cacl |
| 4    | 09/17/2011 12: | 57:56 nr | romanoff              | WKS-WIN, PBIT   | A URL                           | https://                    | apps.skype.com/hor   | ne/images/but   | torGree             | nButtons_tra                | ansparent. | _bg[ H           | TTP/1.1 2 | 00 OK  | Conter  |                      | age/png   | Content         | IE Browse | er Cacl |
| 5    | 08/28/2011 21: | 27:32 nr | romanoff              | WKS-WIN732BI1   | A TRL                           | to://a                      | 1.twimg.com/profile  | _images/14954   | 166 IMG             | 9265_norma                  | l[1].jpg   | H                | TTP/1.1   | 00     | conten  | t-Type: im           | age/jpeg  | ETag: "1        | IE Browse | er Cacl |
| 6    | 09/17/2011 16: | 03:54 nr | romanoff              | WKS-WIN732BIT   | A URL                           |                             | twimg.com/profile    |                 |                     |                             | nal[1].jpg |                  |           | 00 OK  | x-amz-  | d-2: i+VDX           | NDqK2DI   | EYA/MQ          | IE Browse | er Cad  |
| 7    | 09/17/2011 16: | 03:56 nr | romanoff              | WKS-WIN732BIT   | A URL                           |                             | 0.twimg.(Vanu        |                 |                     |                             |            |                  | TTP/1.1 2 | 00 OK  | x-amz-  | id-2: GDgpJ          | fiBKzhhi  | 'QYi/aht        | IE Browse | er Cad  |
| 8    | 09/17/2011 16: | 04:02 nr | romanoff              | WKS-WIN732BIT   | A URL                           | http.,,                     | apps.sky Value       | "in"the         | 220 adfs            | _erw_nor                    | mal[1].jpg | H                | TTP/1.12  | 00 OK  | x-amz-  | id-2: guPM           | ytweSGoy  | EX+40FJ         | IE Browse | er Caci |
| 9    | 04/06/2012 19: | 43:57 nr | romanoff              | WKS-WIN732BIT   | A URL                           | https://                    | apps.sky             |                 | S.C.ancy            | _shadow_n                   | e[1].png   | H                | TTP/1.12  | 00 OK  | Conten  | t-Type: im           | age/png   | Content         | IE Browse | er Cacl |
| 10   | 09/17/2011 17: | 27:54 nr | romanoff              | WKS-WIN732BIT   | A URL                           | https://                    | ping.chartbeat 💽 🔿   | lumns           | eck ping[           | 5].gif                      |            | H                | TTP/1.1 2 | 00 OK  | Conten  | t-Type: im           | age/gif C | ontent-l        | IE Browse | er Cacl |
| 11   | 09/17/2011 17: | 32:10 nr | romanoff              | WKS-WIN732BIT   | A URL                           | https://                    | ping.chartbeat.net/p | ing?h=tweetd    | eck ping[           | 5].gif                      |            | H                | TTP/1.12  | 00 OK  | Conten  | t-Type: im           | age/gif C | ontent-l        | IE Browse | er Cach |
| 12   | 09/18/2011 01: | 24:38 nr | romanoff              | WKS-WIN732BIT   | A URL                           | http://a                    | 3.twimg.com/profile  | _images/12581   | L15 youn            | gadult_norn                 | nal[1].jpg | H                | TTP/1.12  | 00 OK  | x-amz-  | id-2: k5STU          | Gzc7FPrd  | e7hQbb          | IE Browse | er Cacl |
| 13   | 09/18/2011 07: | 15:05 nr | romanoff              | WKS-WIN732BIT   | A URL                           | http://a                    | 0.twimg.com/profile  | _images/15462   | 205 book            | s-2_normal[                 | 1].jpg     | H                | TTP/1.1 2 | 00 OK  | x-amz-  | id-2: fps+4e         | ≘J/I4Kq7d | jJw6j5ril       | IE Browse | er Cacl |
| 14   | 03/05/2012 20: | 37:30 nr | romanoff              | WKS-WIN732BIT   | A URL                           | http://a                    | 0.twimg.com/profile  | _images/18634   | 104 3NYq            | Q_normal[2                  | l.gif      | H                | TTP/1.12  | 00 OK  | x-amz-  | d-2: Lbb9/           | 55jVjaAau | i0Tv3iea        | IE Browse | er Cacl |
| 15   | 03/05/2012 23: | 15:26 nr | romanoff              | WKS-WIN732BIT   | A URL                           | http://a                    | 0.twimg.com/profile  | _images/18593   | 327 imag            | e_normalCA                  | 4NCVXA.j   | pg H             | TTP/1.1 2 | 00 OK  | x-amz-  | id-2: dmjZl          | JJ8w+SKR  | /ug08jxk        | IE Browse | er Cach |
| 16   | 09/17/2011 16: | 46:16 nr | romanoff              | WKS-WIN732BIT   | A URL                           | http://a                    | 3.twimg.com/sticky/  | default_profile | e_ii defai          | ult_profile_0               | _normal[1  | 1].pr H          | TTP/1.1 2 | 00 OK  | x-amz-  | id-2: tp/ILY         | +1dm+AD   | yWt+2V          | IE Browse | er Caci |
|      |                |          |                       | WKS-WIN732BIT   |                                 | https://                    | apps.skype.com/hor   | ne/production,  | /in(inde)           | -combined                   | 1].css     | H                | TTP/1.1 2 | 00 OK  | Conten  | t-Type: te>          | t/css X-S | erverNa         | IE Browse | er Cach |
| 18   | 04/06/2012 19: | 43:31 nr | romanoff              | WKS-WIN732BIT   | A URL                           | https://                    | apps.skype.com/hor   | ne/images/Spi   | nneSpinn            | er_light[1].                | gif        | H                | TTP/1.1 2 | 00 OK  | Conten  | t-Type: im           | age/gif C | ontent-l        | IE Browse | er Cach |
| 19   | 04/06/2012 19: | 43:57 nr | romanoff              | WKS-WIN732BIT   | A URL                           | https://                    | apps.skype.com/hor   | ne/images/fan   | cyt fancy           | _shadow_e                   | 1].png     | H                | TTP/1.1 2 | 00 OK  | Conten  | t-Type: im           | age/png   | Content         | IE Browse | er Cach |
| 14 4 | ► ► nroman     | off tem  | n int 🥠               | 1/              |                                 |                             |                      |                 |                     | 14                          |            |                  |           |        |         |                      |           |                 |           |         |

Figure 83. Final look. (Lee, 2014, digital case files)

### 8.4.6. MFT Entries

We produced the MFT output used in this example by running the analyzeMFT python tool against a Windows 7 \$MFT file:

### C:\Python27\python.exe analyzeMFT.py -f \$MFT -w -o MFT.csv

After running this command and importing the .CSV output file into Excel, you'll notice that there is a lot of data. You'll also notice that the Date/Time values are not in the correct format which will need to be corrected (Figure 84).

| File   |                  |                          |                     |                    |              | N         | /IFT.csv | - Microso    | ft Excel      |                |                |          |             |            | -         | >         |
|--------|------------------|--------------------------|---------------------|--------------------|--------------|-----------|----------|--------------|---------------|----------------|----------------|----------|-------------|------------|-----------|-----------|
|        | Home Insert      | Page Layo                | ut Formulas         | Data Review        | View D       | Developer | Team     |              |               |                |                |          |             |            | ۵         | () — #    |
| aste   | Copy *           | alibri<br><b>B /</b> U - | • 11 • A            |                    |              | Wrap Te   |          | General      | *.0<br>0.0    | Conditional    | Format Ce      | Insert   | Delete Form | Late Autos | Zľ        | Find &    |
|        | Format Painter   |                          | ·····               |                    | -/ -/        |           |          |              |               | Formatting * a |                | es * *   | * *         | Clear      | Filter *  | Select *  |
| Clipbo |                  | 6                        | Font<br>fr Record I | la .               | Alignme      | nt        | Fa.      | Numbe        | at 🖻          | 2              | tyles          |          | Cells       |            | Editing   |           |
|        | 11               |                          | -                   |                    | -            |           |          |              |               |                |                |          |             |            |           |           |
| A      | d NuGood         | C<br>Active              | D                   | E<br>Sequence Pare | F            | G         | н        | chilling out | ر<br>معالية م |                | Challander Fri | IVI      | ENLING AN   |            |           | Q         |
|        | 0 Good           | Active                   | File                | Sequence Pare      | nt File Pari |           |          | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | 37:26.5  | 37:26.5     | 37:26.5    | 37:26.5   | bject ID  |
| 3      | 1 Good           | Active                   | File                | 1                  | 5            |           | MFTM     | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | 37:26.5  | 37:26.5     | 37:26.5    | 37:26.5   |           |
| I      | 2 Good           | Active                   | File                | 2                  | 5            |           | LogFile  | 37.20.3      | 37.20.3       | 37.20.3        | 37.20.3        | 37.20.3  | 37.20.3     | 37.20.3    | 37.20.3   |           |
|        | 2 0000<br>3 Good | Active                   | File                | 3                  | 5            |           | Volume   | 37:26.5      | 37:20.5       | 37-26.5        | 37:20.5        | 27:26.5  | _37:26.5    | 37:26.5    | 37:26.5   | 563224a8- |
| 5      | 4 Good           | Active                   | File                | 4                  | 5            |           | AttrDef  | 37:26.5      | 37:20.5       | nvert N        | umeric V       | alueto   | Date/Ti     | me         | 37:26.5   | 00022-100 |
|        | 5 Good           | Active                   | Folder              | 5                  | 5            | 5 \.      |          | 07:54.9      | 47:38.9       | 47:38.9        | 47 For         | mat 26.5 | 37:26.5     | 37:26.5    | 37:26.5   |           |
|        | 6 Good           | Active                   | File                | 6                  | 5            |           | Bitmap   | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | 37:26.5  | 37:26.5     | 37:26.5    | 37:26.5   |           |
|        | 7 Good           | Active                   | File                | 7                  | 5            | 5 \\$     | Boot     | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | 37:26.5  | 37:26.5     | 37:26.5    | 37:26.5   |           |
| D      | 8 Good           | Active                   | File                | 8                  | 5            | 5 \\$     | BadClus  | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | 37:26.5  | 37:26.5     | 37:26.5    | 37:26.5   |           |
| 1      | 8 Good           | Active                   | File                | 8                  | 5            | 5 \\$     | BadClus  | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | 37:26.5  | 37:26.5     | 37:26.5    | 37:26.5   |           |
| 2      | 9 Good           | Active                   | File + Unkı         | 9                  | 5            | 5 \\$     | Secure   | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | 37:26.5  | 37:26.5     | 37:26.5    | 37:26.5   |           |
| 3      | 9 Good           | Active                   | File + Unkı         | 9                  | 5            | 5 \\$     | Secure:  | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | 37:26.5  | 37:26.5     | 37:26.5    | 37:26.5   |           |
| 4      | 10 Good          | Active                   | File                | 10                 | 5            | 5 \\$     | UpCase   | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | 37:26.5  | 37:26.5     | 37:26.5    | 37:26.5   |           |
| 5      | 11 Good          | Active                   | Folder              | 11                 | 5            | 5 \\$     | Extend   | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | 37:26.5  | 37:26.5     | 37:26.5    | 37:26.5   |           |
| 6      | 12 Good          | Active                   | File                | 12 NoPa            | arent NoF    | Parent No | FNReco   | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | NoFNReco | NoFNRecol   | NoFNReco   | NoFNRecor | d         |
| 7      | 13 Good          | Active                   | File                | 13 NoPa            | arent NoF    | Parent No | FNReco   | 37:26.5      | 37:26.5       | 37:26.5        | 37:26.5        | NoFNReco | NoFNRecol   | NoFNReco   | NoFNRecor | d         |
| eady   |                  |                          |                     |                    |              |           |          |              |               |                |                |          |             |            |           |           |

Figure 84. Correct Date/Time values. (Lee, 2014, digital case files)

You will delete most of the columns in this spreadsheet as they will not be used in the analysis. The only columns you should keep are those titled: Record Number; Filename #1; Std Info Creation date; Std Info Modification date; Std Info Entry date; FN Info Creation date; FN Info Modification date; and FN Info Entry date (Figure 85).

| <b>1</b>           | @ -   ≠                |                          |                           | These Columi        | າຮ່                   |                           |   |     |
|--------------------|------------------------|--------------------------|---------------------------|---------------------|-----------------------|---------------------------|---|-----|
| File               | Home Insert Page Layou | it Formulas Data Review  | w View Develop Team       | 1 · · · ·           |                       |                           | a 🕜 c                                     | - F |
| aste               | opy *                  | • 11 • A • = =           | Wrap xt                   | Custor              | Conditional Format    | Coll ort Delate Format    | Σ AutoSum * 27 mm<br>Fill * Sort & Find & |     |
| Clipboa            | ormat Painter B I U -  |                          | 二 「記 記」」 Merge & Cerve    | er • \$ • 9 •       |                       | Etyles • • • • • • • •    | Clear * Filter * Select *<br>Editing      |     |
| C2                 | 2                      | f= 11, 10/2010 17:37:2   |                           |                     |                       |                           |   | _   |
|                    | АВ                     | С                        | D                         | E                   |                       | G                         | Н   |     |
| Record             | Number Filename #1     | Std Info Creation date S | td Info Modification date | Std Info Entry date | FN Info Creation date | FN Info Modification date | FN Info Entry date                        |     |
|                    | 0 \\$MFT               | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | i 11/10/2010 17:37:20     | 5 11/10/2010 17:37:26                     | _   |
|                    | 1 \\$MFTMirr           | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | i 11/10/2010 17:37:20     | 5 11/10/2010 17:37:26                     |     |
|                    | 2 \\$LogFile           | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | 11/10/2010 17:37:20       | 5 11/10/2010 17:37:26                     |     |
|                    | 3 \\$Volume            | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | i 11/10/2010 17:37:20     | 5 11/10/2010 17:37:26                     |     |
|                    | 4 \\$AttrDef           | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | 5 11/10/2010 17:37:20     | 5 11/10/2010 17:37:26                     |     |
|                    | 5 \.                   | 07/14/2009 02:07:55      | 04/04/2012 11:47:39       | 04/04/2012 11:47:39 | 11/10/2010 17:37:26   | i 11/10/2010 17:37:20     | 5 11/10/2010 17:37:26                     |     |
|                    | 6 \\$Bitmap            | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | i 11/10/2010 17:37:20     | 5 11/10/2010 17:37:26                     |     |
|                    | 7 \\$Boot              | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | i 11/10/2010 17:37:20     | 5 11/10/2010 17:37:26                     |     |
|                    | 8 \\$BadClus           | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | 11/10/2010 17:37:20       | 5 11/10/2010 17:37:26                     |     |
|                    | 8 \\$BadClus:\$E       | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | 11/10/2010 17:37:20       | 5 11/10/2010 17:37:26                     |     |
|                    | 9 \\$Secure            | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | i 11/10/2010 17:37:20     | 5 11/10/2010 17:37:26                     |     |
|                    | 9 \\$Secure:\$SE       | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | i 11/10/2010 17:37:20     | 5 11/10/2010 17:37:26                     |     |
|                    | 10 \\$UpCase           | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | 11/10/2010 17:37:26   | 11/10/2010 17:37:20       | 5 11/10/2010 17:37:26                     |     |
|                    | 11 \\$Extend           | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       |                     |                       |                           | 5 11/10/2010 17:37:26                     |     |
|                    | 12 NoFNRecord          | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | NoFNRecord            | NoFNRecord                | NoFNRecord                                |     |
|                    | 13 NoFNRecord          | 11/10/2010 17:37:26      | 11/10/2010 17:37:26       | 11/10/2010 17:37:26 | NoFNRecord            | NoFNRecord                | NoFNRecord                                |     |
| 4 <b>&gt; &gt;</b> | MFT                    | / /                      | / /                       |                     |                       |                           |   | •   |
| ady Calcu          |                        |                          |                           |                     |                       |                           | □ 100%                                    | -(- |

Figure 85. Columns to keep. (Lee, 2014, digital case files)

The output from parsing the MFT file will most likely contain missing or corrupt information. You can identify rows containing this bad data by examining the 'Filename #1' column for cells that contain either the string "NoFNRecord" or "Corrupt MFT Record" (Figure 86).

| S 🔚 🤊 - 🤆 🖓 🖬                          | Iter Out Mis          | sing File Names       | MFT.xls                   | k - Microsoft Excel   |   |  |  | ×          |
|--|-----------------------|-----------------------|---------------------------|-----------------------|---|--|--|------------|
| File Home Inse                         |                       | ormulas Data Review   | View Developer Team       |                       |   |  | a 🕜 🗆 g                                      | <b>a</b> 1 |
| Cut                                    | Calibri 🚽             | 11 • A • = = =        | Wrap Text                 | General +             | k 📝 🗖   |  | AutoSum * 🔊 👬                                |            |
| Paste V Format Painter                 | В <i>I</i> <u>U</u> - | 🛯 • 💽 • 📥 • 🔳 🔳 🗏     | Merge & Center 🕶          | \$ ~ % •              | Conditional Format Cell<br>Formatting * as Table * Styles |  | 2 Clear • Sort & Find &<br>Filter • Select • |            |
| Clipboard 🛛                            | ont                   | 6                     | Alignment 🕞               | Number 🕞              | Styles  | Cells                                      | Editing                                      |            |
| B16                                    | ▼ (^ <b>f</b> x       | NoFNRecord            |                           |                       |   |  |  |            |
| A                                      | В                     | С                     | D                         | E                     | F   | G  | Н  |            |
| 1 Record Number                        | 👻 Filename 🕯 👻        | Std Info Creation dat | Std Info Modification day | Std Info Entry date 👻 | FN Info Creation de 👻                                     | FN Info Modification dat                   | 👻 FN Info Entry date 💌                       |            |
| 8 6                                    | \\$Bitmap             | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | 11/10/2010 17:37:26                                       | 11/10/2010 17:37:26                        | 11/10/2010 17:37:26                          |            |
| 9 7                                    | \\$Boot               | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | 11/10/2010 17:37:26                                       | 11/10/2010 17:37:26                        | 11/10/2010 17:37:26                          |            |
| 10 8                                   | \\$BadClus            | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | 11/10/2010 17:37:26                                       | 11/10/2010 17:37:26                        | 11/10/2010 17:37:26                          |            |
| 11 8                                   | \\$BadCl_s:\$B        | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | 11/10/2010 17:37:26                                       | 11/10/2010 17:37:26                        | 11/10/2010 17:37:26                          |            |
| 12 9                                   | \\$Secur              | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | 11/10/2010 17:37:26                                       | 11/10/2010 17:37:26                        | 11/10/2010 17:37:26                          |            |
| 13 9                                   | \\$Secure:\$SD        | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | 11/10/2010 17:37:26                                       | 11/10/2010 17:37:26                        | 11/10/2010 17:37:26                          |            |
| 14 10                                  | \\$UpCale             | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | 11/10/2010 17:37:26                                       | 11/10/2010 17:37:26                        | 11/10/2010 17:37:26                          |            |
| 15 11                                  | \\$Extor.d            | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | 11/10/2010 17:37:26                                       | 11/10/2010 17:37:26                        | 11/10/2010 17:37:26                          |            |
| 16 12                                  | NoFNRecord            | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | NoFNRecord  | NoFNRecord                                 | NoFNRecord                                   |            |
| 17 13                                  | NoFNRecord            | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | NoFNRecord  | NoFNRecord                                 | NoFNRecord                                   |            |
| 18 14                                  | NoFNRecord            | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | NoFNRecord  | NoFNRecord                                 | NoFNRecord                                   |            |
| 19 15                                  | NoFNRecord            | 11/10/2010 17:37:26   | 11/10/2010 17:37:26       | 11/10/2010 17:37:26   | NoFNRecord  | NoFNRecord                                 | NoFNRecord                                   |            |
| 20 16                                  | NoFNRecord            | NoSIRecord            | NoSIRecord                | NoSIRecord            | NoFNRecord  | NoFNRecord                                 | NoFNRecord                                   |            |
| 21 17                                  | NoFNRecord            | NoSIRecord            | NoSIRecord                | NoSIRecord            | NoFNRecord  | NoFNRecord                                 | NoFNRecord                                   |            |
| 22 18                                  | NoFNRecord            | NoSIRecord            | NoSIRecord                | NoSIRecord            | NoFNRecord  | NoFNRecord                                 | NoFNRecord                                   |            |
| 23 19                                  | NoFNRecord            | NoSIRecord            | NoSIRecord                | NoSIRecord            | NoFNRecord  | NoFNRecord                                 | NoFNRecord                                   |            |
| •••••••••••••••••••••••••••••••••••••• |                       |                       |                           |                       | 14  |  |  | •          |
| Ready Calculate                        |                       |                       |                           |                       |   | <br>[] [] [] [] [] [] [] [] [] [] [] [] [] | 100% (-)                                     | (+         |

Figure 86. Corrupt data. (Lee, 2014, digital case files)

These entries can easily be removed by using the filter button on the 'Filename

#1' column and filtering on those two phrases (Figure 87).

| S 🛃 🤊 • (ལ ·   ∓<br>File Home I | nsert Page Layout | Formulas Data R                                | leview View         | Developer Tear  | n                     | FILEPOITFI         | ename Column             | ۵ 🕜 د                 | - 7 |
|---------------------------------|-------------------|--|---------------------|-----------------|-----------------------|--------------------|--------------------------|-----------------------|-----|
| Paste                           |                   |  | = <mark>_</mark>    | 🖃 Wrap Text     |                       | enditional Format  | *                        | Filter * Select *     |     |
| Clipboard                       | 5 Font            |  | aughm               | ent             | Number                | Styles             | Cells                    | Editing               |     |
| B16                             | ▼ (° ∫•           | NoFNRecord                                     |                     | D               | - F                   | F                  | G                        | Н                     | _   |
| Record Number                   |                   | Call Inda Counting                             | dad - Chid Inda     | -               |                       |                    | di ▼ FN Info Modificatio |                       | _   |
|                                 |                   | Std Into Creation (                            | al • Std Info       | viodification d | . Starinio Er ry date | · FN Into Creation |                          |                       | _   |
| 6                               | \\$Bitmap         |  |                     |                 | Custon AutoFilte      | r                  | ?                        | × 11/10/2010 17:37:26 |     |
|                                 | \\$Boot           | Show rows where:                               |                     |                 |                       |                    |                          | 11/10/2010 17:37:26   |     |
| 8                               | \\$BadClus        |  |                     |                 |                       |                    |                          | 11/10/2010 17:37:26   |     |
| 18                              | \\$BadClus:\$E    |  | ~                   | NoFNRecord      |                       |                    |                          | 11/10/2010 17:37:26   |     |
| 2 9                             | \\$Secure         | contains                                       |                     | NOFNRECORD      |                       |                    |                          | 14/ 10/ 2010 1/.0/.20 |     |
| 3 9                             | \\$Secure:\$SE    |  |                     |                 |                       |                    |                          | 11/10/2010 17:37:26   |     |
| 4 10                            | \\$UpCase         | contains                                       | ~                   | Corrupt MFT Re  | xord                  |                    |                          | 11/10/2010 17:37:26   |     |
| 5 11                            | \\$Extend         |  |                     |                 |                       |                    |                          | 11/10/2010 17:37:20   | 5   |
| 5 12                            | NoFNRecord        | Use ? to represent an<br>Use * to represent an |                     | ers             |                       |                    |                          | NoFNRecord            |     |
| 7 13                            | NoFNRecord        | - use to represent a                           | ry series or charac | cia.            |                       |                    |                          | NoFNRecord            |     |
| 3 14                            | NoFNRecord        |  |                     |                 |                       |                    | OK Cance                 |                       |     |
| 9 15                            | NoFNRecord        |  |                     |                 |                       |                    |                          | NoFNRecord            |     |
| 16                              | NoFNRecord        |  | NoSIReco            |                 | NoSIRecord            | NoFNRecord         | NoFNRecord               | NoFNRecord            |     |
| 1 17                            | NoFNRecord        |  | NoSIReco            |                 | NoSIRecord            | NoFNRecord         | NoFNRecord               | NoFNRecord            |     |
| 2 18                            | NoFNRecord        |  | NoSIReco            |                 | NoSIRecord            | NoFNRecord         | NoFNRecord               | NoFNRecord            |     |
| 3 19                            | NoFNRecord        | NoSIRecord                                     | NoSIReco            | ord             | NoSIRecord            | NoFNRecord         | NoFNRecord               | NoFNRecord            |     |
| 🗘 🖂 MET 🥂                       | a/                |  |                     |                 |                       | 1                  |                          |                       |     |

Figure 87. Filter out corrupt data. (Lee, 2014, digital case files)

Once you identify all the rows with those phrases, merely select them all and delete them (Figure 88).

| <b>8</b>   <del>   </del> | <b>●</b> • @ •   =    | Select          | All and Delete                    | MFT.xlsx                   | - Microsoft Excel     |   |                          |  | ×    |
|---------------------------|-----------------------|-----------------|-----------------------------------|----------------------------|-----------------------|---|--------------------------|--|------|
| File                      | Home Insert           | Page Layout F   |                                   | View Developer Team        |                       |   |                          | a 🕜 🗖 á                                    | J X3 |
| ħ                         | X Cut Ca              | libri - 1       | 1 • A* A* ≡ ≡ <b>≡</b>            | ≫ - <sup>™</sup> Wrap Text | General -             |   | ) 🖅 🖆 🛃 🥫                | AutoSum * 🖅 👬                              |      |
| Paste                     | I Format Painter      | /1 ∐ -   ⊡      | <u>}</u> · <u>A</u> · <b>≣</b> ≡≡ | 📰 📰 Merge & Center 🔻       |                       | Conditional Format Cell<br>Formatting • as Table • Styles • | Insert Delete Format     | Clear * Sort & Find &<br>Filter * Select * |      |
|                           | Clipboard             | Font            | F9                                | Alignment 💿                | Number 🕞              | Styles  | Cells                    | Editing                                    |      |
|                           | B16 🗸                 | e 🦸 1           | NoFNRecord                        |                            |                       |   |                          |  | •    |
|                           | A                     | в               | С                                 | D                          | E                     | F   | G                        | Н  |      |
| 1                         | Necord Number 💌       | Filenam # 🖛     | Std Info Creation da              | Std Info Modification d    | Std Info Entry date 👻 | FN Info Creation de 👻                                       | FN Info Modification dat | <ul> <li>FN Info Entry date</li> </ul>     |      |
| 16                        | 12                    | NoFNR cord      | 11/10/2010 17:37:26               | 11/10/2010 17:37:26        | 11/10/2010 17:37:26   | NoFNRecord  | NoFNRecord               | NoFNRecord                                 |      |
| 17                        | 13                    | NoFN ecord      | 11/10/2010 17:37:26               | 11/10/2010 17:37:26        | 11/10/2010 17:37:26   | NoFNRecord  | NoFNRecord               | NoFNRecord                                 |      |
| 18                        | 14                    | NoFt Record     | 11/10/2010 17:37:26               | 11/10/2010 17:37:26        | 11/10/2010 17:37:26   | NoFNRecord  | NoFNRecord               | NoFNRecord                                 |      |
| 19                        | 15                    | NoF NRecord     | 11/10/2010 17:37:26               | 11/10/2010 17:37:26        | 11/10/2010 17:37:26   | NoFNRecord  | NoFNRecord               | NoFNRecord                                 |      |
| 20                        | 16                    | Nc NRecord      | NoSIRecord                        | NoSIRecord                 | NoSIRecord            | NoFNRecord  | NoFNRecord               | NoFNRecord                                 |      |
| 21                        | 17                    | NoFNRecord      | NoSIRecord                        | NoSIRecord                 | NoSIRecord            | NoFNRecord  | NoFNRecord               | NoFNRecord                                 |      |
| 22                        | 18                    | oFNRecord       | NoSIRecord                        | NoSIRecord                 | NoSIRecord            | NoFNRecord  | NoFNRecord               | NoFNRecord                                 |      |
| 23                        | 19                    | NoFNRecord      | NoSIRecord                        | NoSIRecord                 | NoSIRecord            | NoFNRecord  | NoFNRecord               | NoFNRecord                                 |      |
| 24                        | 20                    | NoFNRecord      | NoSIRecord                        | NoSIRecord                 | NoSIRecord            | NoFNRecord  | NoFNRecord               | NoFNRecord                                 |      |
|                           | 21                    | NoFNRecord      |                                   | NoSIRecord                 | NoSIRecord            |   | NoFNRecord               | NoFNRecord                                 |      |
|                           | 22                    | NoFNRecord      | NoSIRecord                        | NoSIRecord                 | NoSIRecord            | NoFNRecord  | NoFNRecord               | NoFNRecord                                 |      |
|                           | 23                    | NoFNRecord      | NoSIRecord                        | NoSIRecord                 | NoSIRecord            |   | NoFNRecord               | NoFNRecord                                 |      |
| 1281                      |                       | NoFNRecord      |                                   | NoSIRecord                 | NoSIRecord            |   | NoFNRecord               | NoFNRecord                                 |      |
| 1286                      |                       | NoFNRecord      |                                   | NoSIRecord                 | NoSIRecord            |   | NoFNRecord               | NoFNRecord                                 |      |
| 1601                      |                       | NoFNRecord      |                                   | NoSIRecord                 | NoSIRecord            |   | NoFNRecord               | NoFNRecord                                 |      |
| 2837                      | 2831                  | NoFNRecord      | NoSIRecord                        | NoSIRecord                 | NoSIRecord            | NoFNRecord  | NoFNRecord               | NoFNRecord                                 |      |
| 14 4                      | ▶ н м ∕/ / / / /      |                 |                                   | //                         |                       |   |                          |  |      |
| Ready                     | 422 of 116007 records | found Calculate | 2                                 |                            |                       |   |                          | 100% 🕞 🛛 🗍 🤇                               | +    |

Figure 88. Delete corrupt data. (Lee, 2014, digital case files)

There are still too many columns to fit into our standard layout and too many timestamps to incorporate them all in a timeline chronology. To fix the layout, we select the 'FN Info Creation date' column to represent the chronology of the MFT entries, and we combine the remaining timestamps into two columns, one for the 'Std Info' timestamps and one for the remaining 'FN Info' timestamps (Figure 89).

| ile Home Inse        | rt Page Layout        | Formulas Data     | Review     | View Deve   | eloper Team     |            |                                       |                           |                                |           |                          |                    | ۵ 🕜 🗖                              | . 7 |
|----------------------|-----------------------|-------------------|------------|-------------|-----------------|------------|---------------------------------------|---------------------------|--------------------------------|-----------|--------------------------|--------------------|------------------------------------|-----|
| Cut                  | Calibri               | • 11 • <b>A A</b> | = = _      | ≫- ≣        | Wrap Text       | General    | Ŧ                                     | 1                         |                                |           | *                        | ∑ AutoSur          | ** 27 👬                            |     |
| ste 💞 Format Painter | В <i>I</i> <u>U</u> - | 🗉 *   🌺 * 🗛 * 🚺   |            |             | Merge & Center  | · \$ · %   | • • • • • • • • • • • • • • • • • • • | Conditional<br>Formatting | Format Cel<br>as Table * Style |           | Delete Format            | 🖉 Clear 🔻          | Sort & Find &<br>Filter * Select * |     |
| Clipboard 5          | Fon                   | t G               |            | Alignment   |                 | Num        | nber 🗔                                | 5                         | Styles                         |           | Cells                    |                    | Editing                            |     |
| A2                   | ▼ (~ f <sub>x</sub>   | r 0               |            |             |                 |            | M                                     | ove to F                  | irst Colu                      | mn        |                          |                    |                                    |     |
| Α 📥                  |                       |                   | _          |             | _               |            |                                       |                           | -                              |           | G                        |                    | н                                  |     |
| Record Number        | - Filename # -        | Std Info Creation | on dat - S | td Info Mod | dification da 🔻 | Std Info E | ntry date 🕤                           | FN Info C                 | reation da 🔻                   | FN Info N | Aodification d           | at 🕆 FN In         | nfo Entry date 👻                   |     |
| 0                    | \\$MFT                | 11/10/2010 1      | 37:26 1    | 1/10/2010   | 17:37:26        | 11/10/20   | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 17:37:26             | 11/1               | 0/2010 17:37:26                    | 1   |
| 1                    | \\$MFTMirr            | 11/10/2010 1      | 37:26 1    | 1/10/2010   | .7:37:26        | 11/10/     | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 7:37:26              | 11/1               | 0/10 17:37:26                      | ;   |
| 2                    | \\$LogFile            | 11/10/2010 17     | 87:26 1    | 1/10/2010   | .7:37:26        | 11/10/20   | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 1 :37:26             | 11/1               | 0/ .010 17:37:26                   | 1   |
| 3                    | \\$Volume             | 11/10/2010 17     | 7:26 1     | 1/10/2010   | .7:37:26        | 11/1/20    | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 17 37:26             | 11/1               | 0 2010 17:37:26                    | 5   |
| 4                    | \\$AttrDef            | 11/10/2010 17:    | 37:26 1    | 1/10/2010   | .7:37:26        | 11/ 0/20   | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 17: 7:26             | 11/1               | 2010 17:37:26                      | ;   |
| 5                    | ٨.                    | 07/14/2009 02:    | 0)55 0     | 4/04/2012   | 1:47:39         | 04/04/20   | 12 11:47:39                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 17:37:26             | 11/1               | /2010 17:37:26                     | )   |
| 6                    | \\$Bitmap             | 11/10/2010 17:    | 3726 1     | 1/10/2010   | 17:37:26        | 1/10/20    | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 17:37 26             | 11/                | 0/2010 17:37:26                    | i - |
| 7                    | \\$Boot               | 11/10/2010 17:    | 37:6 1     | 1/10/2010   | 17:37:26        | 1/10/20    | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 17:37:26             | 11/ <mark>.</mark> | 0/2010 17:37:26                    | j – |
| 8                    | \\$BadClus            | 11/10/2010 17:    | 37:25 1    | 1/10/2010   | 17:37:26        | 11/10/20   | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 17:37:25             | 11 1               | 0/2010 17:37:26                    | )   |
| 8                    | \\$BadClus:\$         | B 11/10/2010 17:  | 37:20 1    | 1/10/2010   | 17:37:26        | 11/10/20   | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 17:37:2              | 1/1                | 0/2010 17:37:26                    | 1   |
| 9                    | \\$Secure             | 11/10/2010 17:    | 37:26 1    | 1/10/2010   | 17:37:26        | 11/10/20   | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 17:37:26             | 1/1                | 0/2010 17:37:26                    | i – |
| 9                    | \\$Secure:\$SI        | D 11/10/2010 17:  | 37:26 1    | 1/10/2010   | 17:37:26        | 11/10/20   | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 17:37:26             | 1/1                | 0/2010 17:37:26                    | i – |
| 10                   | \\$UpCase             | 11/10/2010 17:    | 37:26 1    | 1/10/2010   | 17:37:26        | 11/10/20   | 10 17:37:26                           | 11/10/20                  | 10 17:37:26                    | 11/10/20  | 010 17:37:26             | 11/1               | 0/2010 17:37:26                    | i – |
| 11                   | \\$Extend             | 11/10/2010 17:    |            | 1/10/2010   |                 |            |                                       |                           |                                |           | 010 17:37:2 <del>6</del> |                    | 0/2010 17:37:26                    |     |
| 24                   | \\$Extend\\$C         | Q 11/10/20 Con    | ibine T    | hesepTit    | ree Colu        |            |                                       |                           |                                |           |                          | 250 11/1           | 0,2010 17.57.36                    | 1   |
| 25                   | \\$Extend\\$C         | 0 11/10/2010 17:  | 37:58 1    | 1/10/2010   | 17:37:58        | 11/10/20   | 10 17:37:58                           | 11/10/20                  | 10 17:37:58                    | 11/10/20  | 010 17:37:58             | 11/1               | 0/2010 17:37:58                    | 1   |
| 🗘 🖂 MFT /💷 /         |                       |                   |            |             |                 |            |                                       | 14                        |                                |           |                          |                    | - '                                |     |

*Figure 89. Combining Date/Time columns. (Lee, 2014, digital case files)* 

To combine the columns of timestamps and to display those timestamps in the correct format, a function will be used that specifically tells Excel how the values should look. The first function will combine the 'Std Info' timestamps (Figure 90).

="Std Info - Create: " & TEXT(D2, "mm/dd/yyyy hh:mm:ss") & ", Modify: " & TEXT(E2, "mm/dd/yyyy hh:mm:ss") & ", Entry: " & TEXT(F2, "mm/dd/yyyy hh:mm:ss")

| 5 🚽 🔊 • (° - 🖃          |                       |                    |                |           | MFT.xl             | sx - Micro      | soft Excel         |                             |                                    |               |                     | _ □                              | 1 ×    |
|-------------------------|-----------------------|--------------------|----------------|-----------|--------------------|-----------------|--------------------|-----------------------------|------------------------------------|---------------|---------------------|----------------------------------|--------|
| File Home Insert        | Page Layout           | Formulas E         | Data Review    | View D    | eveloper Team      |                 |                    |                             |                                    |               |                     | ۵ 🕜                              | - 7 23 |
| Copy -                  | alibri                | - 11 - <b>A</b> A  | . = = =        | ≫⁄-       | Wrap Text          | Custom          | -                  |                             |                                    | -             | Σ AutoSu            |                                  |        |
| Paste<br>Format Painter | B <i>I</i> <u>U</u> - | 🗄 •   🌺 • <u>A</u> | · <b>F</b> = = |           | •a• Merge & Center | • <b>\$</b> • % | •.0 •.0<br>00. 00. | Conditional<br>Formatting * | Format Cell<br>as Table - Styles - | Insert Delete | Format              | Sort & Find &<br>Filter * Select |        |
| Clipboard 🕞             | Fo                    | nt                 | 6              | Alignmer  | nt                 | 🗟 Nun           | nber 🕞             |                             | ityles                             | Cells         |                     | Editing                          | _      |
| G2 🔻                    | (- )                  | e ="Std Info       | - Create: " &  | TEXT(D2,  | "mm/dd/yyyy        | hh:mm:ss")      | & ", Modif         | y: " & TEXT(                | E2, "mm/dd/y                       | yyy hh:mm:ss  | s") & ", Entry: " & | TEXT(F2, "mm                     | / 🗘 '  |
| Α                       | В                     | С                  | D              |           | E                  |                 |                    | F                           |                                    |               | G                   |                                  |        |
| 1 FN Info Creation da   | te Recor 👻            | Filename # 👻       | Std Info Crea  | tion da 👻 | Std Info Modi      | fication d      | Std In. 1          | Entry date 🔻                |                                    |               |                     |                                  | FN Int |
| 2 11/10/2010 17:37:2    | 60                    | \\$MFT             | 11/10/2010 1   | 7:37:26   | 11/10/2010 1       | 7:37:26         | 11/10/20           | 10 17:37:26                 | Std Info - Cre                     | ate: 11/10/20 | 010 17:37:26, Mo    | dify: 11/10/20                   | 111/10 |
| 3 11/10/2010 17:37:2    | 6 1                   | \$MFTMirr          | 11/10/2010 1   | 7:37:26   | 11/10/2010 1       | 7:37:26         | 11/10/20           | 10 17:37:26                 |                                    |               |                     |                                  | 11/10  |
| 4 11/10/2010 17:37:2    | 6 2                   | \\$LogFile         | 11/10/2010 1   | 7:37:26   | 11/10/2010 1       | 7:37:26         | 11/10/20           | 010 1. 37:26                |                                    | - <b>T</b>    |                     |                                  | 11/10  |
| 5 11/10/2010 17:37:2    | 63                    | \\$Volume          | 11/10/2010 1   | 7:37:26   | 11/10/2010 1       | 7:37:26         | 11/10/20           | 010 17:3 <sup>-26</sup>     |                                    |               |                     |                                  | 11/10  |
| 6 11/10/2010 17:37:2    | 64                    | \\$AttrDef         | 11/10/2010 1   | 7:37:26   | 11/10/2010 1       | 7:37:26         | 11/10/20           | 010 17:37:26                |                                    |               |                     |                                  | 11/10  |
| 7 11/10/2010 17:37:2    | 6 5                   | λ.                 | 07/14/2009 0   | 2:07:55   | 04/04/2012 1       | 1:47:39         | 04/04/20           | 012 11:47:39                |                                    |               |                     |                                  | 11/10  |
| 8 11/10/2010 17:37:2    | 6 6                   | \\$Bitmap          | 11/10/2010 1   | 7:37:26   | 11/10/2010 1       | 7:37:26         | 11/10/20           | 10 17:37:26                 |                                    |               |                     |                                  | 11/10  |
| 9 11/10/2010 17:37:2    | 6 7                   | \\$Boot            | 11/10/2010 1   | 7:37:26   | 11/10/2010 1       | 7:37:26         | 11/10/20           | 10 17:37:26                 |                                    |               |                     |                                  | 11/10  |
| 10 11/10/2010 17:37:2   | 68                    | \\$BadClus         | 11/10/2010 1   | 7:37:26   | 11/10/2010 1       | 7:37:26         | 11/10/20           | 10 17:37:26                 |                                    |               |                     |                                  | 11/10  |
| 11 11/10/2010 17:37:2   | 68                    | \\$BadClus:\$B     | 11/10/2010 1   | 7:37:26   | 11/10/2010 1       | 7:37:26         | 11/10/20           | 10 17:37:26                 |                                    |               |                     |                                  | 11/10  |
| 12 11/10/2010 17:37:2   | 69                    | \\$Secure          | 11/10/2010 1   | 7:37:26   | 11/10/2010 1       |                 | 11/10/20           | 10 17:37:26                 |                                    |               |                     |                                  | 11/10  |
| 13 11/10/2010 17:37:2   |                       | \\$Secure:\$SD     |                |           | 11/10/2010 1       |                 |                    | 10 17:37:26                 | Camalain                           | in a Calu     | an a suith a F      |                                  | 11/10  |
| 14 11/10/2010 17:37:2   | 6 10                  | \\$UpCase          | 11/10/2010 1   | 7:37:26   | 11/10/2010 1       | 7:37:26         |                    | 10 17:37:26                 |                                    | ling Colum    | nns with a F        | unction                          | 11/10  |
| 15 11/10/2010 17:37:2   |                       |                    | 11/10/2010 1   |           | 11/10/2010 1       |                 |                    | 10 17:37:26                 |                                    |               |                     |                                  | 11/10  |
| 16 11/10/2010 17:37:5   |                       | \\$Extend\\$Q      |                |           | 11/10/2010 1       |                 |                    | 10 17:37:58                 |                                    |               |                     |                                  | 11/10  |
| 17 11/10/2010 17:37:5   | 8 25                  | \\$Extend\\$OI     | 11/10/2010 1   | 7:37:58   | 11/10/2010 1       | 7:37:58         | 11/10/20           | 10 17:37:58                 |                                    |               |                     |                                  | 11/10  |
| H A P H MFT 🕼           |                       |                    | / /            |           |                    |                 |                    |                             | н                                  |               |                     |                                  | •••    |
| Ready Calculate 🎦       |                       |                    |                |           |                    |                 |                    |                             |                                    |               | 🖽 🔲 🛄 100% (        | 9-0-                             | (+)    |

*Figure 90. A function to combine columns. (Lee, 2014, digital case files)* 

The second function performs the same action, just on the 'FN Info' timestamps:

="FN Info - Modify: " & TEXT(G2, "mm/dd/yyyy hh:mm:ss") & ", Entry: " & TEXT(H2, "mm/dd/yyyy hh:mm:ss")

When dealing with a large set of data and filling a column with a function, you may run into an issue where the values in the cells do not match the formula applied to that cell (Figure 91 – Number 1). To fix this issue, on the 'Formula' ribbon, select the 'Calculate Now' button to refresh/recalculate the function formulas (Figure 91 – Number 2).

| 8 🔒 🤊                    | • @ ·          | Ŧ                     |          |                |                 |        |        |                      |                |       |                  |           | MF         | T.xlsx - Microsoft  | Exc  | cel Recalc  | ulate            | etol                | Refr          | esh          | Eun    | ctio   | n 🛛        |       |     |       | ×   |
|--------------------------|----------------|-----------------------|----------|----------------|-----------------|--------|--------|----------------------|----------------|-------|------------------|-----------|------------|---|------|---|------------------|---------------------|---------------|--------------|--------|--------|------------|-------|-----|-------|-----|
| File                     | Home           | Insert                | Page Lay | /out           | Formu           | ulas   | Data   | Revi                 | ew             | View  | Deve             | loper     | Te         | am  |      | 01222200  |                  |                     |               |              |        |        |            |       | 6   | s 🕜 = |     |
| fx<br>Insert<br>Function | Σ<br>AutoSum R | ecently Fin<br>Jsed * | ٣        | *              | Text<br>Library |        |        | kup & rence •        | Math a<br>Trig |       | Nore<br>ctions • | Na<br>Man | me<br>ager | 🔁 Define Name ▾<br>📌 Use in Formula ▾<br>🐨 Create from Selection<br>Defined Names | R    | Trace Precedents<br>Trace Dependents<br>Remove Arrows | s 🚸 Er<br>• @ Ev | ror Che<br>aluate F | cking *       | Wate<br>Wind | ch Ci  | ptions | Calculatio |       |     |       |     |
|                          |                |                       | ~        |                | · · · · ·       | ·      |        |                      |                |       |                  |           |            |   |      |   | rmula A          |                     |               |              |        |        | Calculatio | n     |     |       |     |
| -                        | G2             | • (                   |          | J <sub>x</sub> | ="FN            | N Info | - Mo   | odify:               | "& II          | :XI(I | =2, "m           | m/do      | d/yy       | yy hh:mm:ss") & ",  | Entr | ry: " & TEXT(F2                                       | , "mm            | ,                   | yyy hi        | h:mm         | :ss'') |        |            |       |     |       |     |
|                          |                |                       | D        |                |                 |        |        |                      |                | E     |                  |           |            | F   |      |   |                  | G                   |               |              |        |        | H          |       |     |       | J   |
| 1                        |                |                       |          |                |                 |        |        |                      |                |       | icatio           |           |            | N Info Entry date   |      |   |                  |                     |               |              |        |        |            |       |     |       |     |
|                          | nfo - Cre      |                       |          |                |                 |        |        |                      |                |       |                  |           |            | 4/04/2012 00:12:1   |      |   |                  |                     |               |              |        |        |            |       |     |       |     |
|                          | nfo - Cre      |                       |          |                |                 |        |        |                      |                |       |                  |           |            | 4/04/2012 12:35:5   |      |   |                  |                     |               |              |        |        |            |       |     |       |     |
|                          | nfo - Cre      |                       |          |                |                 |        |        |                      |                |       |                  |           |            | 4/04/2012 00:07:3   |      |   |                  |                     |               |              |        |        |            |       |     |       |     |
|                          | nfo - Cre      |                       |          |                |                 |        |        |                      |                |       |                  |           |            | 3/15/2012Date/  |      |   |                  |                     |               |              |        |        |            |       |     |       |     |
| 899 Std I                | nfo - Cre      | ate: 07/              | 05/201   | 1 20:          | 29:52,          | , Mod  | ify: 0 | e <b>03/</b> :       | 15/20          | 12 22 | 2:31:5           | 7         | C          | 3/15/2012 22:31:5   | 7 FN | N Info - Modify                                       | : 11/1           | 0/201               | 0 17:3        | 37:26,       | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
| IOO Std I                | nfo - Cre      | ate: 03/              | 22/201   | 2 14:          | 50:19,          | , Mod  | ify: 0 | e <b>03/</b> 2       | 22/20          | 12 14 | 4:50:1           | 9         | C          | 3/22/2012 14.50:1   | 9 FN | N Info 🚺 odify  | : 11/1           | 0/201               | <b>u</b> 17:3 | 37:26,       | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
| 01 Std I                 | nfo - Cre      | ate: 03/              | 15/201   | 2 22:          | 36:50,          | , Mod  | ify: 0 | 3 <b>03/</b> 3       | 15/20          | 12 22 | 2:36:5           | 0         | C          | 3/15/2012 22:36:5   | DFN  | N Info - Modify                                       | : 11/1           | 0/201               | 0 17:5        | 26,          | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
| 02 Std I                 | nfo - Cre      | ate: 03/              | 15/201   | 2 22:          | 36:54,          | , Mod  | ify: 0 | :03/                 | 15/20          | 12 22 | 2:36:5           | 4         | C          | 3, 15/2012 22:36:5  | 4 FN | N Info - Modify                                       | : 11/1           | 0/201               | 0 17:3        | 37:26,       | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
| 03 Std I                 | nfo - Cre      | ate: 04/              | 04/201   | 2 15:          | 20:56,          | , Mod  | ify: 0 | 404/0                | 04/20          | 12 15 | 5:20:5           | 6         | C          | 4/04/2012 15:20:5   | 6 FN | N Info - Modify                                       | : 11/1           | 0/201               | 017:3         | 37:26,       | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
| 04 Std I                 | nfo - Cre      | ate: 04/              | 01/201   | 2 00:          | 06:46,          | , Mod  | ify: 0 | 404/0                | 01/20          | 12 00 | 0:06:4           | 6         | C          | 4/01/2012 00:06:4   | 6 FN | N Info - Modify                                       | : 11/1           | 0/201               | 0 17:3        | 37:26,       | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
| 05 Std I                 | nfo - Cre      | ate: 03/              | 22/201   | 2 06:4         | 42:29,          | , Mod  | ify: 0 | 3 <mark>03/</mark> 2 | 22/20          | 12 06 | 5:42:2           | 9         | C          | 3/22/2012 06:42:2   | 9 FI | Ninto - Mourty  | : 11/1           | 0/201               | 0 17:3        | 37:26,       | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
| 06 Std I                 | nfo - Cre      | ate: 09/              | 08/201   | 1 20:          | 57:55,          | , Mod  | ify: 0 | :03/:                | 15/20          | 12 22 | 2:32:4           | 3         | C          | 3/15/2012 22:32:4   | 3 FN | N Info - Modify                                       | : 11/1           | 0/201               | 0 17:3        | 37:26,       | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
| 107 Std I                | nfo - Cre      | ate: 03/              | 15/201   | 2 23:          | 13:28,          | , Mod  | ify: 0 | :03/:                | 15/20          | 12 23 | 3:13:2           | 9         | C          | 3/15/2012 23:13:2   | 9 FN | N Info - Modify                                       | : 11/1           | 0/201               | 0 17:3        | 37:26,       | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
| 108 Std I                | nfo - Cre      | ate: 03/              | 15/201   | 2 23:          | 12:01,          | , Mod  | ify: 0 | :03/:                | 15/20          | 12 23 | 3:12:0           | 1         | C          | 3/15/2012 23:12:0   | 1 FN | N Info - Modify                                       | : 11/1           | 0/201               | 0 17:3        | 37:26,       | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
| 109 Std I                | nfo - Cre      | ate: 03/              | 22/201   | 2 07:          | 13:20,          | , Mod  | ify: 0 | :03/:                | 22/20          | 12 07 | 7:13:2           | 0         | C          | 3/22/2012 07:13:2   | D FN | N Info - Modify                                       | : 11/1           | 0/201               | 0 17:3        | 37:26,       | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
| 410 Std I                | nfo - Cre      | ate: 03/              | 22/201   | 2 13:4         | 48:05,          | , Mod  | ify: 0 | 03/2                 | 22/20          | 12 13 | 3:48:0           | 5         | C          | 3/22/2012 13:48:0   | 5 FN | N Info - Modify                                       | : 11/1           | 0/201               | 0 17:3        | 37:26,       | Entry  | : 11/1 | 0/2010     | 17:37 | :26 |       |     |
|                          | MFT /          |                       |          |                | · · • ·         |        | . · ·  |                      | - /            |       |                  | •         |            | - / /   |      | i i na ni   |                  | - /                 |               | -            | - • •  |        |            |       |     |       | •   |
|                          | alculate       |                       |          |                |                 |        |        |                      |                |       |                  |           |            |   |      |   |                  |                     | Cou           | int: 115     | E 0 E  |        | 100%       | 0     |     |       | -(+ |

*Figure 91. Recalculate function values. (Lee, 2014, digital case files)* 

The recalculated combined columns should look like Figure 92.

| S 🖬 🤊 • (° - 🖡                     | MFT.xlsx - Micros   | oft Excel   | _ 🗆     | ×    |
|------------------------------------|---|---|---------|------|
| File Home Insert Page Layout       | Formulas Data Review View Developer Team  |   | ا 🗆 🕥 ۵ | æ 23 |
| fx<br>Insert<br>unction            | al Text Date & Lookup & Math & More<br>• Time • Reference • Trig • Functions • Manager 🔐 Create from Sele<br>O Ubrary | S → Trace Precedents S Show Formulas<br>= Trace Dependents ↔ Error Checking +<br>∴ Remove Arrows ↔ Q Evaluate Formula<br>Formula Auditina<br>Formula Auditina | t       |      |
|                                    | Std Info - Create: 11/10/2010 17:37:26, Modify: 11/10/2010  |   |         | ~    |
|                                    | D   | E   | F       |      |
| 1                                  | 6   |   |         | -    |
| 2 Std Info - Create: 11/10/2010 1  | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  | 26 FN Info - Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:26  | ;       | -    |
|                                    | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  |   |         |      |
| 4 Std Info - Create: 11/10/2010 1  | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  | 26 FN Info - Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:26  | ;       |      |
| 5 Std Info - Create: 11/10/2010 1  | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  | 26 FN Info - Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:26  | i       |      |
| 6 Std Info - Create: 11/10/2010 1  | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  | 26 FN Info - Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:26  | i -     |      |
| 7 Std Info - Create: 07/14/2009 0  | 2:07:55, Modify: 04/04/2012 11:47:39, Entry: 04/04/2012 11:47:  | 89 FN Info - Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:26  | i       |      |
| 8 Std Info - Create: 11/10/2010 1  | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  | 26 FN Info - Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:26  | i       |      |
| 9 Std Info - Create: 11/10/2010 1  | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  | 26 FN Info - Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:26  | i l     |      |
| 10 Std Info - Create: 11/10/2010 1 | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  | 26 FN Info - Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:26  | i       |      |
|                                    | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  |   |         |      |
|                                    | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  |   | i       |      |
|                                    | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  |   |         |      |
|                                    | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  |   |         |      |
|                                    | 7:37:26, Modify: 11/10/2010 17:37:26, Entry: 11/10/2010 17:37:  |   |         |      |
|                                    | 7:37:58, Modify: 11/10/2010 17:37:58, Entry: 11/10/2010 17:37:  |   |         |      |
| 17 Std Info - Create: 11/10/2010 1 | 7:37:58, Modify: 11/10/2010 17:37:58, Entry: 11/10/2010 17:37:  | 58 FN Info - Modify: 11/10/2010 17:37:58, Entry: 11/10/2010 17:37:58  |         |      |
| C C D D MFT 🕼                      |   |   |         |      |
| Ready Calculate 🔚                  |   | 🔲 🔲 100% 😑 —  | 0       | +    |

Figure 92. Date/Time column results. (Lee, 2014, digital case files)

A few final changes need to be made such as entering in the standard headers; creating and filling in the Artifacts column; moving the old 'Record Number' column to the 'Miscellaneous' column; and adding a prefix to the 'Miscellaneous' column for clarity (Figure 93).

| File         Insert         Page Layout           Pase         Conjert         Calibri           Pase         Conjert         B         I         U           Pase         Conjert         B         I         U         Ho           I         Properties         I         I         Properties         I         I           2         FN Info - Modify: 11/10/2010 1         I         S         FN Info - Modify: 11/10/2010 1         I           5         FN Info - Modify: 11/10/2010 1         S         FN Info - Modify: 11/10/2010 1         S           7         FN Info - Modify: 11/10/2010 1         S         FN Info - Modify: 11/10/2010 1         S           8         FN Info - Modify: 11/10/2010 1         S         FN Info - Modify: 11/10/2010 1         S | 11       A* A*       = = = # %         11       A* A*       = # %         12       A* A*       = # % <th>Alignment<br/>7:37:26<br/>7:37:26<br/>7:37:26</th> <th>G<br/>Miscellaneou<br/>0<br/>1<br/>2</th> <th>s v</th> <th>* % * 1.58 .68<br/>Number 5<br/>H</th> <th><ul> <li>Artifa</li> </ul></th> <th>I Format Cell<br/>* as Table &gt; Styles -<br/>Styles<br/>I<br/>tts<br/>ile Create Date</th> <th></th> <th>K</th> <th>∑ AutoSum *</th> <th>۵ 🕜 🖻<br/>Sort &amp; Find &amp;<br/>Filter - Select -<br/>fitting</th> <th>N</th> | Alignment<br>7:37:26<br>7:37:26<br>7:37:26            | G<br>Miscellaneou<br>0<br>1<br>2 | s v | * % * 1.58 .68<br>Number 5<br>H | <ul> <li>Artifa</li> </ul> | I Format Cell<br>* as Table > Styles -<br>Styles<br>I<br>tts<br>ile Create Date |             | K | ∑ AutoSum * | ۵ 🕜 🖻<br>Sort & Find &<br>Filter - Select -<br>fitting  | N |
|---|--|---|----------------------------------|-----|---------------------------------|----------------------------|---|-------------|---|-------------|---|---|
| Paste         Copy *         B         I         U *           Clipboard         rs         F0         F0         F0           1         Properties         r         F0         F0           2         FN Info - Modify: 11/10/2010 1         F0         F0           3         FN Info - Modify: 11/10/2010 1         F0         F0           5         FN Info - Modify: 11/10/2010 1         F0         F0           6         F0 Info - Modify: 11/10/2010 1         F0         F0           7         F0         F0         Modify: 11/10/2010 1           8         F0         F0         Modify: 11/10/2010 1   | minite         r           6         ="Record #: " & G2           F         r           7:37:26, Entry: 11/10/2010 17         r           7:37:26, Entry: 11/10/2010 17         r           7:37:26, Entry: 11/10/2010 17         r  | Alignment<br>7:37:26<br>7:37:26<br>7:37:26<br>7:37:26 | G<br>Miscellaneou<br>1<br>2      | s v | • % • .58 .68<br>Number •       | <ul> <li>Artifa</li> </ul> | Styles  | -           |   | Fill ▼      | Sort & Find &<br>Filter * Select *<br>diting  | N |
| H2         J           Properties         FN Info - Modify: 11/10/2010 1           5 FN Info - Modify: 11/10/2010 1         FN Info - Modify: 11/10/2010 1           5 FN Info - Modify: 11/10/2010 1         FN Info - Modify: 11/10/2010 1           6 FN Info - Modify: 11/10/2010 1         FN Info - Modify: 11/10/2010 1           7 FN Info - Modify: 11/10/2010 1         FN Info - Modify: 11/10/2010 1  | #"Record #: " & G2           F           7:37:26, Entry: 11/10/2010 17           7:37:26, Entry: 11/10/2010 17           7:37:26, Entry: 11/10/2010 17   | 7:37:26<br>7:37:26<br>7:37:26                         | G<br>Miscellaneou<br>0<br>1<br>2 | s 🔻 | н                               |                            | l<br>ts 1   | о<br>1<br>- |   | L           |   | N |
| Properties           2         FN Info - Modify: 11/10/2010 1           3         FN Info - Modify: 11/10/2010 1           4         FN Info - Modify: 11/10/2010 1           5         FN Info - Modify: 11/10/2010 1           6         FN Info - Modify: 11/10/2010 1           7         FN Info - Modify: 11/10/2010 1           8         FN Info - Modify: 11/10/2010 1           8         FN Info - Modify: 11/10/2010 1  | F<br>7:37:26, Entry: 11/10/2010 17<br>7:37:26, Entry: 11/10/2010 17<br>7:37:26, Entry: 11/10/2010 17<br>7:37:26, Entry: 11/10/2010 17  | 7:37:26<br>7:37:26<br>7:37:26                         | Miscellaneou<br>0<br>1<br>2      | -   |                                 |                            |   |             | К | L           | M   | N |
| 2         FN Info - Modify: 11/10/2010 1           3         FN Info - Modify: 11/10/2010 1           4         FN Info - Modify: 11/10/2010 1           5         FN Info - Modify: 11/10/2010 1           6         FN Info - Modify: 11/10/2010 1           7         FN Info - Modify: 11/10/2010 1           7         FN Info - Modify: 11/10/2010 1           8         FN Info - Modify: 11/10/2010 1   | 7:37:26, Entry: 11/10/2010 17<br>7:37:26, Entry: 11/10/2010 17<br>7:37:26, Entry: 11/10/2010 17  | 7:37:26<br>7:37:26<br>7:37:26                         | Miscellaneou<br>0<br>1<br>2      | -   |                                 |                            |   |             | К | L           | M   | N |
| 2         FN Info - Modify: 11/10/2010 1           3         FN Info - Modify: 11/10/2010 1           4         FN Info - Modify: 11/10/2010 1           5         FN Info - Modify: 11/10/2010 1           6         FN Info - Modify: 11/10/2010 1           7         FN Info - Modify: 11/10/2010 1           7         FN Info - Modify: 11/10/2010 1           8         FN Info - Modify: 11/10/2010 1   | 7:37:26, Entry: 11/10/2010 17<br>7:37:26, Entry: 11/10/2010 17<br>7:37:26, Entry: 11/10/2010 17  | 7:37:26<br>7:37:26<br>7:37:26                         |                                  | -   |                                 |                            |   |             |   |             |   |   |
| 3         FN Info - Modify: 11/10/2010 1           4         FN Info - Modify: 11/10/2010 1           5         FN Info - Modify: 11/10/2010 1           6         FN Info - Modify: 11/10/2010 1           7         FN Info - Modify: 11/10/2010 1           8         FN Info - Modify: 11/10/2010 1   | 7:37:26, Entry: 11/10/2010 17<br>7:37:26, Entry: 11/10/2010 17<br>7:37:26, Entry: 11/10/2010 17  | 7:37:26<br>7:37:26<br>7:37:26                         | 1                                |     | Record #: 0                     | MFT F                      | ile Create Date   |             |   |             |   |   |
| 4 FN Info - Modify: 11/10/2010 1<br>5 FN Info - Modify: 11/10/2010 1<br>6 FN Info - Modify: 11/10/2010 1<br>7 FN Info - Modify: 11/10/2010 1<br>8 FN Info - Modify: 11/10/2010 1  | 7:37:26, Entry: 11/10/2010 17<br>7:37:26, Entry: 11/10/2010 17   | 7:37:26<br>7:37:26                                    | 2                                |     | <b>+</b>                        |                            |   | -           |   |             |   |   |
| 5 FN Info - Modify: 11/10/2010 1<br>6 FN Info - Modify: 11/10/2010 1<br>7 FN Info - Modify: 11/10/2010 1<br>8 FN Info - Modify: 11/10/2010 1  | 7:37:26, Entry: 11/10/2010 17  | 7:37:26   |                                  |     | - T                             |                            |   | -           |   |             |   |   |
| 5 FN Info - Modify: 11/10/2010 1<br>7 FN Info - Modify: 11/10/2010 1<br>3 FN Info - Modify: 11/10/2010 1  |  |   | 3                                |     |                                 |                            |   |             |   |             |   |   |
| 7 FN Info - Modify: 11/10/2010 1<br>8 FN Info - Modify: 11/10/2010 1  | 7:37:26, Entry: 11/10/2010 17  | 2.07.00   |                                  |     |                                 |                            |   |             | - | Fill Art    | and the second se |   |
| B FN Info - Modify: 11/10/2010 1  |  | 37:20   | 4                                |     |                                 |                            |   |             |   | Colu        | Imn   |   |
| 1 1 1   | 7:37:26, Entry: 11/10/2010 17  | 7:37:26   | 5                                | Ide | tify Value as                   | sa                         |   |             |   |             |   |   |
|   | 7:37:26, Entry: 11/10/2010 17  | 7:37:26   | 6                                | "E  | ecord #" wit                    | h                          |   |             |   |             |   |   |
| 9 FN Info - Modify: 11/10/2010 1  | 7:37:26, Entry: 11/10/2010 17  | 7:37:26   | 7                                | 0   | Function                        |                            |   |             |   |             |   |   |
| 0 FN Info - Modify: 11/10/2010 1  | 7:37:26, Entry: 11/10/2010 17  | 7:37:26   | 8                                |     | unonon                          |                            |   |             |   |             |   |   |
| 1 FN Info - Modify: 11/10/2010 1  | 7:37:26, Entry: 11/10/2010 17  | 7:37:26   | 8                                |     |                                 |                            |   |             |   |             |   |   |
| 2 FN Info - Modify: 11/10/2010 1  | 7:37:26, Entry: 11/10/2010 17  | 7:37:26   | 9                                |     |                                 |                            |   |             |   |             |   |   |
| 3 FN Info - Modify: 11/10/2010 1  | 7:37:26, Entry: 11/10/2010 17  | 7:37:26   | 9                                |     |                                 |                            |   |             |   |             |   |   |
| 4 FN Info - Modify: 11/10/2010 1  | 7:37:26, Entry: 11/10/2010 17  | 7:37:26   | 10                               |     |                                 |                            |   |             |   |             |   |   |
| 5 FN Info - Modify: 11/10/2010 1  | 7:37:26, Entry: 11/10/2010 17  | 7:37:26   | 11                               |     |                                 |                            |   |             |   |             |   |   |
| 6 FN Info - Modify: 11/10/2010 1  | 7:37:58, Entry: 11/10/2010 17  | 7:37:58   | 24                               |     |                                 |                            |   |             |   |             |   |   |
| 7 FN Info - Modify: 11/10/2010 1  | 7:37:58, Entry: 11/10/2010 17  | 7:37:58   | 25                               |     |                                 |                            |   |             |   |             |   |   |
|   |  |   |                                  |     |                                 | 14                         |   | _           |   |             |   |   |

Figure 93. Moving 'Record Number' column and adding a prefix to columns. (Lee, 2014, digital case files)

The final output should look like Figure 94.

| Fi  | e Home Insert       | Page Layout | Formulas [       | Data Review     | View D    | eveloper   | Team   |        |         |         |                        |                          |                      |             |               |    | ۵ 🕜 د                                      | - # |
|-----|---------------------|-------------|------------------|-----------------|-----------|------------|--------|--------|---------|---------|------------------------|--------------------------|----------------------|-------------|---------------|----|--|-----|
| Â   | Cut Cali            | ~ ~         | 11 - A A         | _               |           | Wrap Te    |        | Custor | n       | ¥       | 5                      |                          |                      | •<br>•      | *             | ΣA | utoSum • 灯 🏔                               |     |
| ast | e                   | ΙŪ·Ι        | -   🌺 - <u>A</u> | • 🔳 🖬 🗐 •       |           | 🙀 Merge 8  | Center | - \$ - | % ,     | .00 .00 | Condition<br>Formattin | al Forma<br>a ∗ as Table | t Cell<br>• Styles • | Insert<br>* | Delete Format |    | llear * Sort & Find &<br>Filter * Select * |     |
|     | Clipboard 5         | Font        |                  | rs.             | Alignmen  | it         |        | a I    | Number  | F2      |                        | Styles                   | -                    |             | Cells         |    | Editing                                    |     |
|     | A2 👻                | $f_{x}$     | 11/10/201        | 0 17:37:26      |           |            |        |        |         |         |                        |                          |                      |             |               |    |  |     |
|     | А                   | В           | С                | D               |           |            | E      |        |         |         |                        | F                        |                      |             | G             |    | Н  |     |
|     | Date/Time           | Accoun -    | Compute -        | Description 🔻   | Details   |            |        |        |         | -       | Propert                | es                       |                      | -           | Miscellaneous |    | Artifacts                                  | -   |
|     | 11/10/2010 17:37:26 |             |                  | \\$MFT          | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify                   | 11/10/2              | 2010 1      | Record #: 0   |    | MFT File Create Dat                        | e   |
|     | 11/10/2010 17:37:26 |             |                  | \\$MFTMirr      | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 1   |    | MFT File Create Dat                        | e   |
|     | 11/10/2010 17:37:26 |             |                  | \\$LogFile      | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 2   |    | MFT File Create Dat                        | е   |
|     | 11/10/2010 17:37:26 |             |                  | \\$Volume       | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 3   |    | MFT File Create Dat                        | e   |
|     | 11/10/2010 17:37:26 |             |                  | \\$AttrDef      | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify                   | 11/10/2              | 2010 1      | Record #: 4   |    | MFT File Create Dat                        | e   |
|     | 11/10/2010 17:37:26 |             |                  | λ.              | Std Inf   | o - Create | : 07/1 | 4/2009 | 02:07:5 | 5, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 5   |    | MFT File Create Dat                        | e   |
|     | 11/10/2010 17:37:26 |             |                  | \\$Bitmap       | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 6   |    | MFT File Create Dat                        | е   |
|     | 11/10/2010 17:37:26 |             |                  | \\$Boot         | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 7   |    | MFT File Create Dat                        | e   |
|     | 11/10/2010 17:37:26 |             |                  | \\$BadClus      | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 8   |    | MFT File Create Dat                        | e   |
|     | 11/10/2010 17:37:26 |             |                  | \\$BadClus:\$Ba | a Std Inf | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 8   |    | MFT File Create Dat                        | e   |
|     | 11/10/2010 17:37:26 |             |                  | \\$Secure       | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 9   |    | MFT File Create Dat                        | е   |
|     | 11/10/2010 17:37:26 |             |                  | \\$Secure:\$SD  | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 9   |    | MFT File Create Dat                        | e   |
|     | 11/10/2010 17:37:26 |             |                  | \\$UpCase       | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 10  |    | MFT File Create Dat                        | е   |
|     | 11/10/2010 17:37:26 |             |                  | \\$Extend       | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:2 | 6, Mod  | FN Info                | Modify                   | 11/10/2              | 2010 1      | Record #: 11  |    | MFT File Create Dat                        | e   |
|     | 11/10/2010 17:37:58 |             |                  | \\$Extend\\$Qu  | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:5 | 8, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 24  |    | MFT File Create Dat                        | е   |
|     | 11/10/2010 17:37:58 |             |                  | \\$Extend\\$Ob  | Std Inf   | o - Create | : 11/1 | 0/2010 | 17:37:5 | 8, Mod  | FN Info                | Modify:                  | 11/10/2              | 2010 1      | Record #: 25  |    | MFT File Create Dat                        | e   |
| 1   | • • MET /2          |             |                  |                 |           |            |        | - /    |         |         |                        |                          |                      |             |               |    |  |     |

Figure 94. Final output. (Lee, 2014, digital case files)

#### 8.4.7. Prefetch Entries

We produced the Prefetch output used in this example by running the parse\_prefetch\_info tool against the prefetch directory of a Windows 7 system:

*parse\_prefetch\_info.exe –p <Path to Prefetch Directory> -d <database\_name> w Vista -o <Path to Output Directory> -r csv* 

One of the files generated when running the above command is prefetch\_file\_info.csv which contains a nice summary of the prefetch file activities on the system. When you open the file and apply the standard formatting, you'll notice that the 'UTC time' column is not formatted properly (Figure 95).

| X 🛃 🧐 • 🔍 - 🖙                         | prefetch_fi             | ile_info.xlsm - Microsc                     | oft Excel   |                      |  | - 🗆 🗙     |
|---------------------------------------|-------------------------|---|---|----------------------|--|-----------|
| File Home Insert Page Layout Formulas | Data Review View Develo | per Team                                    |   |                      |  | a 🕜 🗕 🗗 🛛 |
|                                       |                         | General ▼<br>\$ ▼ % • 5.00 .000<br>Number 5 | Conditional Format Cell<br>formatting * as Table * Styles * | Insert Delete Format | Σ AutoSum *<br>Fill *<br>Clear * Filter *<br>Editing |           |
| A6 - fx AT.EXE-E313                   | -                       |   | syles   |                      |  |           |
| Α                                     | B                       | С   | D   | F F                  | G H  | 1 14      |
|                                       | Actual File Name        | Number Time Run 🔻                           | -   |                      | 5 II   |           |
| 2 A.EXE-8D56B1C4.pf                   | A.EXE                   | 26  | Wed Apr 4 00:43:06 2012                                     |                      |  | =         |
| 3 A.EXE-F91CBA0E.pf                   | A.EXE                   | 1541  | Sat Apr 7 16:22:10 2012                                     |                      |  |           |
| 4 ACRORD32.EXE-33939BD1.pf            | ACRORD32.EXE            | 4   | Sun Apr 1 14:17:38 2012                                     |                      |  |           |
| 5 ADOBEARM.EXE-ACA00A4A.pf            | ADOBEARM.EXE            | 6   | Fri Apr 6 19:43:04 2012                                     |                      |  |           |
| 6 AT.EXE-E3131BD4.pf                  | AT.EXE                  | 9   | Fri Apr 6 13:41:09 2012                                     |                      |  |           |
| 7 ATBROKER.EXE-FF58B71D.pf            | ATBROKER.EXE            | 4   | Wed Apr 4 12:21:04 2012                                     |                      |  |           |
| 8 AUDIODG.EXE-D0D776AC.pf             | AUDIODG.EXE             | 484   | Fri Apr 6 19:42:18 2012                                     |                      |  |           |
| 9 CMD.EXE-89305D47.pf                 | CMD.EXE                 | 25  | Fri Apr 6 19:00:47 2012                                     |                      |  |           |
| 10 CONHOST.EXE-3218E401.pf            | CONHOST.EXE             | 1436  | Sat Apr 707:00:13 2012                                      |                      |  |           |
| 11 CONSENT.EXE-65F6206D.pf            | CONSENT.EXE             | 27  | Wed Apr 4 20:05:23 2012                                     |                      |  |           |
| 12 CONTROL.EXE-9459D5A0.pf            | CONTROL.EXE             | 1   | Wed Apr 4 20:03:16 2012                                     |                      |  |           |
| 13 CSC.EXE-4EF173D0.pf                | CSC.EXE                 | 4   | Sun Apr 1 05:00:38 2012                                     |                      |  |           |
| 14 CSRSS.EXE-8C04D631.pf              | CSRSS.EXE               | 39  | Fri Apr 6 19:42:07 2012                                     |                      |  |           |
| 15 CVTRES.EXE-419E4E46.pf             | CVTRES.EXE              | 4   | Sun Apr 1 05:00:38 2012                                     |                      |  |           |
| 16 DEFRAG.EXE-738093E8.pf             | DEFRAG.EXE              | 67  | Thu Apr 5 11:54:26 2012                                     |                      |  |           |
| 17 DLLHOST.EXE-6202E8F2.pf            | DLLHOST.EXE             | 2   | Wed Apr 4 15:37:11 2012                                     |                      |  |           |
| 18 DLLHOST.EXE-6D52477E.pf            | DLLHOST.EXE             | 1   | Wed Apr 4 02:25:39 2012                                     |                      |  |           |
| 19 DLLHOST.EXE-71214090.pf            | DLLHOST.EXE             | 21  | Thu Apr 5 15:51:47 2012                                     |                      |  |           |
| H + F prefetch_file_info              |                         |   |   |                      |  | •         |
| Ready 🔚                               |                         |   |   |                      | 🔳 💷 🛛 100% 😑 —                                       | + 🕂       |

Figure 95. Fix date and times to match our standard format. (Lee, 2014, digital case files)

Unfortunately, Excel does not recognize these values as Dates or Times, so we'll need to fix it so that it does. All the information is there, but the order in which it appears is not quite right. To correct this, we will reorder the data. First, we highlight the 'UTC time' column and then click the 'Text to Columns' button on the 'Data' ribbon to separate the items using a 'Space' character as the delimiter (Figure 96).

| 🛃 19 - (°1 - | -   <del>-</del>                                 |   | prefeto   | h_file_info.xlsm - | Microsoft Excel                     |            |            |              |           |           |   | - 0   | 1 × |
|--------------|--|---|-----------|--------------------|-------------------------------------|------------|------------|--------------|-----------|-----------|---|-------|-----|
| File Home    | Insert Page Layout                               | Formulas Data Review View                         | Developer | Team               |                                     |            |            |              |           |           |   | a 🕜 = | - # |
|              | Convert Te                                       | xt to Columns Wizard - Step 1 of 3                | ? ×       |                    | 1 1                                 | <b>5</b> 2 | ****       |              | ⊕∃ Show I | Detail    |   |       |     |
|              | The Text Wizard has determined th                | at your data is Fixed Width.                      |           | Text to            | _                                   |            |            |              | "] Hide D | etail     |   |       |     |
| cess Web     | If this is correct, choose Next, or c            | hoose the data type that best describes your data |           | Columns Duplie     | ve Data Consolidate<br>Validation A | nalysis *  | Group Ungr | oup Subtotal |           |           |   |       |     |
|              | Original data type                               |   |           |                    | ta Tools                            |            |            | Outline      |           | Gi .      |   |       |     |
| D1           | Choose the file type that best de                | scribes your data:                                |           |                    |                                     |            |            |              |           |           |   |       |     |
| 1            | Delimited     Aracter                            | s such as commas or tabs separate each field.     |           | С                  | D                                   | E          | F          | G            | н         | 1         | 1 | К     |     |
| Prefetch Fi  | Fixed width - vields unit                        | n columns with spaces between each field.         |           | er Time Run 🔻      | UTC time                            |            | 'Toy       |              | alum      | nol       |   |       | -   |
| A.EXE-8D56   |  |   |           |                    | Wed Apr 4 00:43:06 2012             |            | lex        | t to C       | oluli     |           |   |       |     |
| A.EXE-F910   |  |   |           |                    | Sat Apr 7 16:22:10 2012             |            |            | Butt         | on        |           |   |       |     |
| ACRORD32     |  |   |           |                    | Sun Apr 1 14:17:38 2012             |            |            |              |           |           |   |       |     |
| ADOBEARN     | Preview of selected data:                        |   |           |                    | Fri Apr 6 19:43:04 2012             |            |            | 1            |           |           |   |       |     |
| AT.EXE-E31   | 1 UTC time                                       |   |           |                    | Fri Apr 6 13:41:09 2012             |            |            |              |           |           |   |       |     |
| ATBROKER.    | 2 Wed Apr 4 00:43:06 2                           | 012   | <u>^</u>  |                    | Wee 4 12:21:04 2012                 |            |            |              |           |           |   |       |     |
| AUDIODG.E    | 3 Sat Apr 7 16:22:10 2<br>4 Sun Apr 1 14:17:38 2 |   |           |                    | Fri Apr 6 19:42.1. 1012             |            |            |              |           |           |   |       |     |
| CMD.EXE-8    | 5 Fri Apr 6 19:43:04 2                           |   | v         |                    | Fri Apr 6 19:00:47 2012             |            | D          | 0.00         |           | 0         |   |       |     |
| CONHOST.     | <  |   | >         |                    | Sat Apr 707:00:13 2012              |            | - De       | limite       | d by      | Spac      | е |       |     |
| CONSENT.E    |  |   |           |                    | Wed Apr 4 20:05:23 2012             |            |            |              |           |           | - |       |     |
| CONTROL.E    |  | Cancel < Back <u>N</u> ext >                      | Einish    |                    | Wed Apr 4 20:03:16 2012             |            |            |              | <u> </u>  |           |   |       |     |
| CSC.EXE-4E   |  |   |           |                    | Sun Apr 1 05:00:38 2012             |            |            |              |           |           |   |       |     |
| CSRSS.EXE-8  |  | CSRSS.EXE   | 39        |                    | Fri Apr 6 19:42:07 2012             |            |            |              |           |           |   |       |     |
| CVTRES.EXE-  |  | CVTRES.EXE  | 4         |                    | Sun Apr 1 05:00:38 2012             |            |            |              |           |           |   |       |     |
| DEFRAG.EXE   |  | DEFRAG.EXE  | 67        |                    | Thu Apr 5 11:54:26 2012             |            |            |              |           |           |   |       |     |
| DLLHOST.EXE  |  | DLLHOST.EXE                                       | 2         |                    | Wed Apr 4 15:37:11 2012             |            |            |              |           |           |   |       |     |
| -            | E-6D52477E.pf                                    | DLLHOST.EXE<br>DLLHOST.EXE                        | 1 21      |                    | Wed Apr 4 02:25:39 2012             |            |            |              |           |           |   |       |     |
| DLLHOST.EXE  |  | DILHOST.EXE                                       | 21        |                    | Thu Apr 5 15:51:47 2012             |            |            |              |           |           |   | -     | 1   |
| ady          | etch_file_info 🖄                                 |   |           |                    |                                     |            |            |              |           | B 🛄 🛄 100 | ~ |       | -4  |

Figure 96. Text to columns to fix Date/Time. (Lee, 2014, digital case files)

Once each Date/Time item is in its own column, the following formula can be used to add them back together in the proper order (Figure 97):

=DATE(H2,MONTH(1&E2),F2) + G2

| <b>∐ 🔄 🕫 •</b> (° • ( <del>-</del>        |   | pretetch_file_info.x               | Ism - Microsoft Excel  |                       |                             | >       |
|---|---|------------------------------------|--|-----------------------|-----------------------------|---------|
| File Home Insert Page Layout Formulas     | Data Review View  | Developer Team                     |  |                       |                             | a 🕜 🗆 🗟 |
| From From Prom Other<br>Get External Data | Connections     2↓     2⊥            Properties          £↓          ∑⊥            ∞ Edit Links           Sort           Sort | Filter                             | Remove Data Consolidate<br>Duplicates Validation ~<br>Data Tools | What-If<br>Analysis * |                             |         |
| 12 - fx =DATE(H2,N                        | 1ONTH(1&E2),F2) + G2  |                                    | Function   | to Form               | at Date                     |         |
| A   | В   | с                                  | D  | E F                   | G H                         | I J     |
| Prefetch File Name                        | <ul> <li>Actual File Name</li> </ul>  | <ul> <li>Number Time Ru</li> </ul> | in 🔻   | ▼ UTC time            |                             |         |
| 2 A.EXE-8D56B1C4.pf                       | A.EXE   | 26                                 | Wed  | Apr 4                 | 00:43:06 2012 04/04/2012 00 | 0:43:06 |
| A.EXE-F91CBA0E.pf                         | A.EXE   | 1541                               | Sat  | Apr 7                 | 16:22:10 2012               |         |
| ACRORD32.EXE-33939BD1.pf                  | ACRORD32.EXE  | 4                                  | Sun  | Apr 1                 | 14:17:3 2012                |         |
| ADOBEARM.EXE-ACA00A4A.pf                  | ADOBEARM.EXE  | 6                                  | Fri  | Apr 6                 | 19:43:04 12                 |         |
| AT.EXE-E3131BD4.pf                        | AT.EXE  | 9                                  | Fri  | Α. 6                  | 13:41:09 201 Year           |         |
| ATBROKER.EXE-FF58B71D.pf                  | ATBROKER.EXE  | 4                                  | wed Month  | kpr 4                 | 12:21:04 2012               |         |
| AUDIODG.EXE-D0D776AC.pf                   | AUDIODG.EXE   | 484                                | Fri  | Apr 6                 | 19:42:18 2012               |         |
| CMD.EXE-89305D47.pf                       | CMD.EXE   | 25                                 | Fri  | Apr 6                 | 19:00:47 2012               |         |
| 0 CONHOST.EXE-3218E401.pf                 | CONHOST.EXE   | 1436                               | Sat 🧹  | Apr 7                 | 07:00:13 2012               |         |
| 1 CONSENT.EXE-65F6206D.pf                 | CONSENT.EXE   | 27                                 | Wed Day  | Apr 4                 | 20:05:23 2012 Time          |         |
| 2 CONTROL.EXE-9459D5A0.pf                 | CONTROL.EXE   | 1                                  | weu  | Apr 4                 | 20:03:16 2012               |         |
| 3 CSC.EXE-4EF173D0.pf                     | CSC.EXE   | 4                                  | Sun  | Apr 1                 | 05:00:38 2012               |         |
| 4 CSRSS.EXE-8C04D631.pf                   | CSRSS.EXE   | 39                                 | Fri  | Apr 6                 | 19:42:07 2012               |         |
| 5 CVTRES.EXE-419E4E46.pf                  | CVTRES.EXE  | 4                                  | Sun  | Apr 1                 | 05:00:38 2012               |         |
| 6 DEFRAG.EXE-738093E8.pf                  | DEFRAG.EXE  | 67                                 | Thu  | Apr 5                 | 11:54:26 2012               |         |
| 7 DLLHOST.EXE-6202E8F2.pf                 | DLLHOST.EXE   | 2                                  | Wed  | Apr 4                 | 15:37:11 2012               |         |
| 8 DLLHOST.EXE-6D52477E.pf                 | DLLHOST.EXE   | 1                                  | Wed  | Apr 4                 | 02:25:39 2012               |         |
| 9 DLLHOST.EXE-71214090.pf                 | DLLHOST.EXE   | 21                                 | Thu  | Apr 5                 | 15:51:47 2012               |         |
| ↔ M_prefetch_file_info / 🎾 /<br>eady 🔚    |   |                                    | [ ∢  |                       | III III III III III III III |         |

Figure 97. Reorder date and time fields. (Lee, 2014, digital case files)

After copying the cell values over the functions in the new column, you can delete the delimited columns you just created. Next, move the new Date/Time column to the beginning of the spreadsheet, insert columns where needed and modify the column headers to match our standard headers. Finally, prepend 'Number Time Runs' to the new 'Properties' column entries and manually enter the Artifact and Computer column values for a final result (Figure 98).

| 🛃 🔊 • (° -   =                       |                        | prefetch_file_ir             | nfo.xlsm - Microsoft Excel |                           |   |         |
|--------------------------------------|------------------------|------------------------------|----------------------------|---------------------------|---|---------|
| File Home Insert Page                | Layout Formulas Data   | a Review View Developer Team |                            |                           |   | a 🕜 🗆 🗟 |
| Cut Calibri                          | - 11 - A' A' -         | = = ≥ ≫·· = Wrap Text Cust   | om · ·                     | Cell Insert Delete Format | Σ AutoSum * Ž hit<br>Fill * Sort & Find & |         |
| <ul> <li>V Format Painter</li> </ul> |                        |                              | Formatting * as Table      |                           | Clear * Filter * Select *                 |         |
| Clipboard G                          | Font G                 | Alignment 5                  | Number 🕞 Styles            | Cells                     | Editing                                   |         |
| A4 • (*                              | fx 03/21/2012 15:15:01 | 1                            |                            |                           |   |         |
| A B                                  | С                      | D                            | E                          | F                         | G H                                       | 1 J     |
| 1 Date/Time   Account                |                        |                              | P Details                  | Properties Vis            | scellaneous 🝸 Artifact 👻                  |         |
| 2 03/15/2012 21:17:39                |                        | AUCLT.EXE-830BCC14.pf        | WUAUCLT.EXE                | Number Time Run: 25       | Prefetch                                  |         |
| 3 03/21/2012 15:14:45                | WKS-WIN732BITA MM      |                              | MMC.EXE                    | Number Time Run: 2        | Prefetch                                  |         |
| 4 03/21/2012 15:15:01                | WKS-WIN732BITA VD.     |                              | VDS.EXE                    | Number Time Run: 2        | Prefetch                                  |         |
| 5 03/26/2012 04:00:00                |                        | QMC_NS.EXE-E2CE6542.pf       | WSQMCONS.EXE               | Number Time Run: 1        | Prefetch                                  |         |
| 5 03/29/2012 22:44:42                |                        | PRDMGR. KE-55F08014.pf       | NAPRDMGR.EXE               | Number Time Run: 2 🥒      | Prefetch                                  |         |
| 7 03/31/2012 17:18:51                |                        | NSAVE.SCR-205A7D32.pf        | SCRNSAVE.SCR               | Number Time Rupp 2        | Prefetch                                  |         |
| 8 04/01/2012 05:00:02                |                        | AGNHOST.EXE-67CD1457.pf      | SDIAGNHOST.EXE             | Number Time Sun: 2        | Prefetch                                  |         |
| 9 04/01/2012 05:00:38                | WKS-WIN732BITA CSC.    |                              | CSC.EXE                    | Number Time Run: 4        | Prefetch                                  |         |
| 0 04/01/2012 05:00:38                | WKS-WIN732BITA CVT     |                              | CVTRES.EXE                 | Numb a Time Run: 4        | Prefetch                                  |         |
| 1 04/01/2012 14:17:38                |                        | RORD32.EXE-33939BD1.pf       | ACRORD32.EXE               | Number Time Run: 4        | Prefetch                                  |         |
| 2 04/03/2012 20:38:05                | WKS-WIN732BITA MM      |                              | MMC.EXE                    | Number Time Run: 1        | Prefetch                                  |         |
| 3 04/03/2012 21:03:30                |                        | PLZAGU.EXE-4EFD8FD3.pf       | TOPLZAGU.EXE               | Number Time Run: 1        | Prefetch                                  |         |
| 4 04/03/2012 21:18:21                |                        |                              | d to Columns               | Number Time Run: 1        | Prefetch                                  |         |
| 5 04/03/2012 21:18:21                | WKS-WIN732BITA RUN     |                              | RUNDLL32.EXE               | Number Time Run: 2        | Prefetch                                  |         |
| 6 04/03/2012 21:36:56                |                        | HOST.EXE-C85DDD7D.pf         | DLLHOST.EXE                | Number Time Run: 2        | Prefetch                                  |         |
| 7 04/03/2012 21:50:44                | WKS-WIN732BITA WM      |                              | WMIC.EXE                   | Number Time Run: 2        | Prefetch                                  |         |
| 8 04/03/2012 22:12:42                | WKS-WIN732BITA DLLF    |                              | DLLHOT.EXE                 | Number Time Run: 4        | Prefetch                                  |         |
| 9 04/03/2012 22:17:59                | WKS-WIN732BITA DLLF    | HOST.EXE-7D2183B8.pt         | DLLHOST.EXE                | Number Time Run: 1        | Prefetch                                  |         |

Figure 98. Prefetch results. (Lee, 2014, digital case files)