GIAC
CERTIFICATIONS

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
"Wireless Penetration Testing and Ethical Hacking (Security 617)"
at http://www.giac.org/registration/gawn

Wireless Networks and the Windows Registry - Just where has your computer been?

GIAC (GAWN) Gold Certification

Author: Jonathan Risto, jonathan.risto@hotmail.com
Advisor: Erik Avakian

Accepted: September, 2010

Abstract

Windows keeps track of everything you do on the system, what you have connected to the computer and what you have used on the system. Knowing where to look for this information and what it tells you is one of the great challenges incident responders and analysts have when looking at computers. This paper documents the registry remnants that remain from both hardware connections (NIC's) being inserted into the computer, as well as information within the registry regarding the networks that the computer has connected too in the past for both Windows XP and Windows Vista systems.

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute Author retains full rights.

1. Introduction

The Windows Registry stores all of the information that is needed by the host operating system. This database contains all of the configurations, settings and options that are both created initially by the operating system, as well as user configuring settings and installed software. For example, a 1-year-old Vista system used in this paper has over 800,000 individual keys, as show in a screen capture from the Active Registry Monitor program (About Active Registry Monitor, 2010) shown in Figure 1.

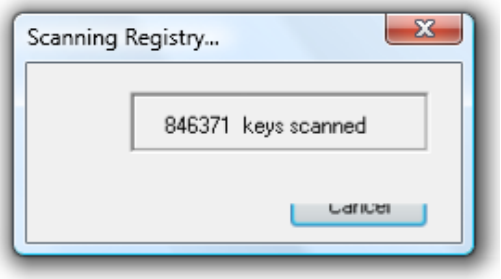

Figure 1 - Registry Key count on Windows Vista

The sheer volume of information stored within the windows registry poses the challenge of finding the right information on the system. Randomly looking through the registry is not practical nor will you likely find the correct information quickly using this approach. Adding to the challenge, Microsoft changes the locations where information is stored within the Windows registry depending on the operating system release (i.e. Windows XP to Windows Vista).

Wireless network configuration settings are not exempted from being stored within the windows registry. Service set identifier's (SSID's) of networks that the computer has connected to, network configuration parameters of those networks, and details relating to the Network Interface Cards on the system are all stored within the Windows Registry.

© 2011 The SANS Institute Author retains full rights.

2. The Windows registry hierarchy

The windows registry is a database that contains the configuration for the system in question. All of this data is stored in one of six hives on the local system. Microsoft describes a hive as "a group of keys, sub keys, and values in the registry that has a set of supporting files that contain backups of its data. " (Windows Registry information for Advanced Users, 2008) The five common root keys found on a system are as follows:

- HKEY_LOCAL_MACHINE or HKLM
- HKEY_CURRENT_CONFIG or HKCC
- HKEY_CLASSES_ROOT or HKCR
- HKEY_CURRENT_USER or HKCU
- HKEY_USERS or HKU

These are shown in Figure 2, as seen through the built in Windows regedit program.

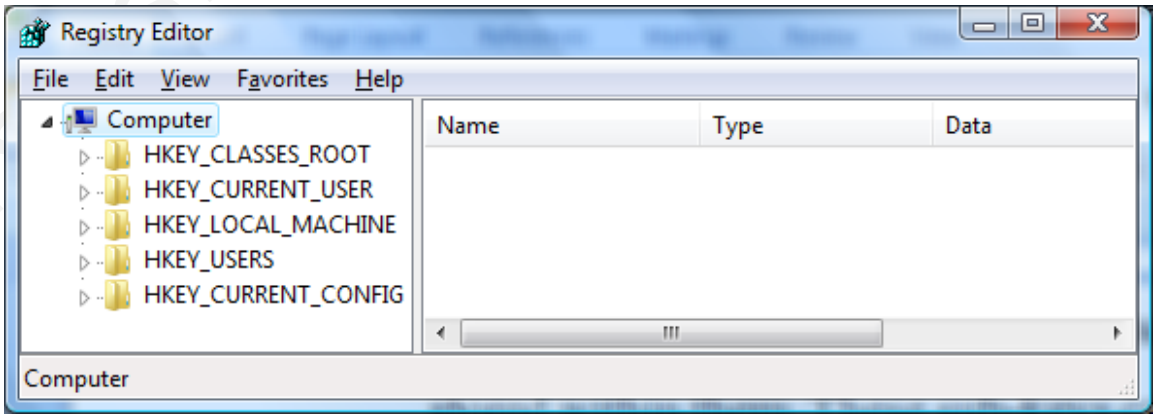

Figure 2 - Root Windows Vista Registry keys

© 2011 The SANS Institute Author retains full rights.

Each of these root keys could be considered similar to a folder, with items pertaining to that key stored there. Each root key can and do have numerous sub-keys stored within them. These sub-keys in turn can store other sub-keys, which can product a long list of folders to access the data you need. An example of a Windows Vista Registry key is:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

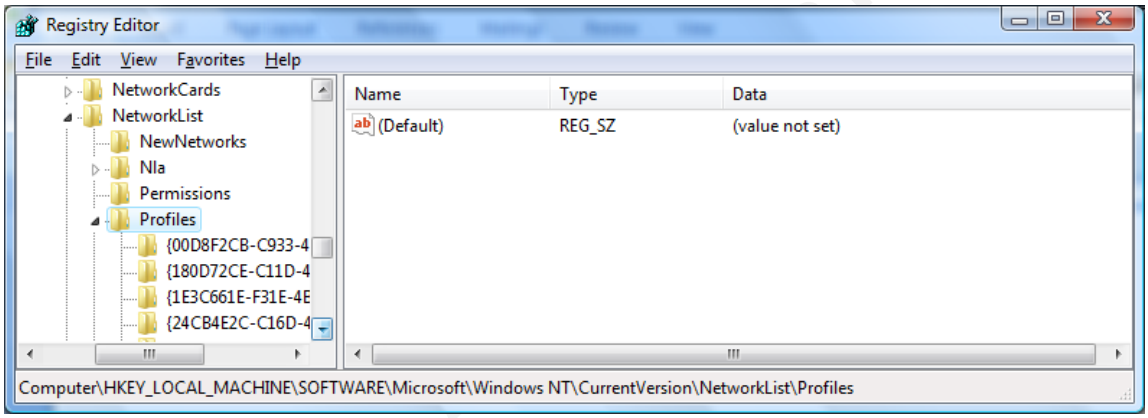

Figure 3 - Example of a Windows Vista registry key

As shown in Figure 3, the registry key can contain only one item or it could contain a large number of items, as shown in Figure 4.

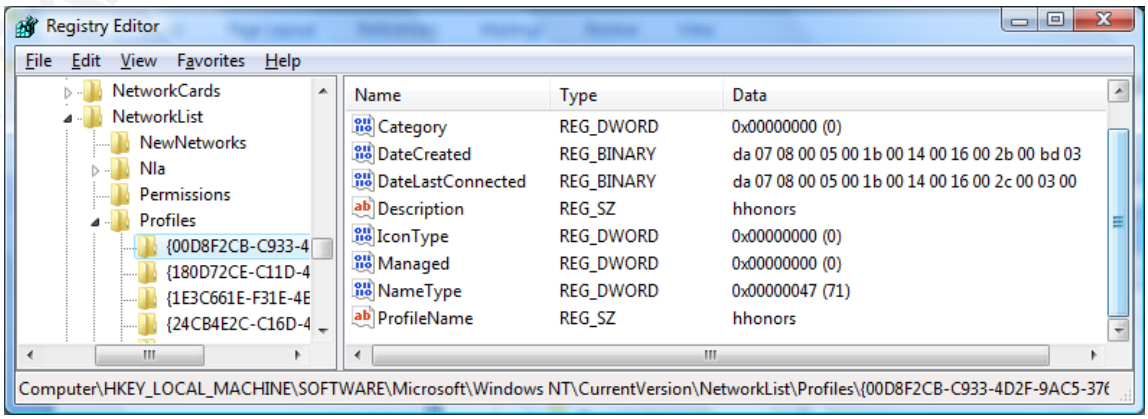

Figure 4 - Example of Windows Vista Registry keys

Jonathan Risto, jonathan.risto@hotmail.com

© 2011 The SANS Institute Author retains full rights.

Regardless of the number of keys stored in any particular location, each key will be one of major types outlined in Table 1.

Name	Data Type	Description
REG_BINARY	Binary Value	Raw binary data. Most hardware component information is stored as binary data and is displayed in Registry Editor in hexadecimal format.
REG_DWORD	DWORD Value	Data represented by a number that is 4 bytes long (a 32-bit integer). Many parameters for device drivers and services are this type and are displayed in Registry Editor in binary, hexadecimal, or decimal format. Related values are DWORD_LITTLE_ENDIAN (least significant byte is at the lowest address) and REG_DWORD_BIG_ENDIAN (least significant byte is at the highest address).
REG_EXPAND_SZ	Expandable String Value	A variable-length data string. This data type includes variables that are resolved when a program or service uses the data.
REG_MULTI_SZ	Multi-String Value	A multiple string. Values that contain lists or multiple values in a form that people can read are generally this type. Entries are separated by spaces, commas, or other marks.
REG_SZ	String Value	A fixed-length text string.

Table 1 – Major data types for Registry keys (Windows Registry information for Advanced Users, 2008)

2.1. Windows Vista Wireless Registry Keys

Windows Vista stores wireless settings and configurations in several distinct locations. The first location to find wireless information is the registry key that stores

© 2011 The SANS Institute Author retains full rights.

data related to network interface cards (NIC's). This information is located in the following location:

HKLM\Y_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards

This can be seen in Figure 5 below.

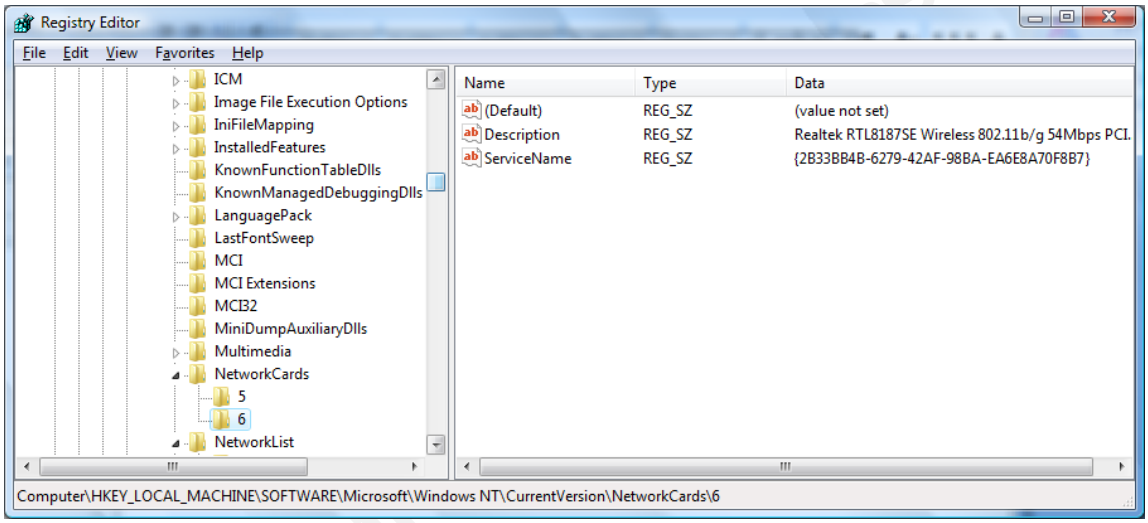

Figure 5 - Network card registry key

Within this key, the Globally Unique Identifier, or GUID, assigned to the interface is found. This information is stored in the ServiceName key. In the example in Figure 5, this value is {2B33BB4B-6279-42AF-98BA-EA6E8A70F8B7}. If there are multiple cards installed on the system, or if an additional card has been placed into the computer, each card will be shown here with a unique identifier. Within Figure 5, it is shown that an additional card, labeled 5, has been installed on this system, and has a separate GUID assigned to it.

Knowing what the GUID assigned to this network interface, the wireless network IP address and associated information are stored within the Vista registry is able to be determined. The registry key associated with this is:

© 2011 The SANS Institute Author retains full rights.

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{GUID}

An example of the information stored within this key location is shown in Figure 6, using the GUID found in the previous step. This GUID value is {2B33BB4B-6279-42AF-98BA-EA6E8A70F8B7}.

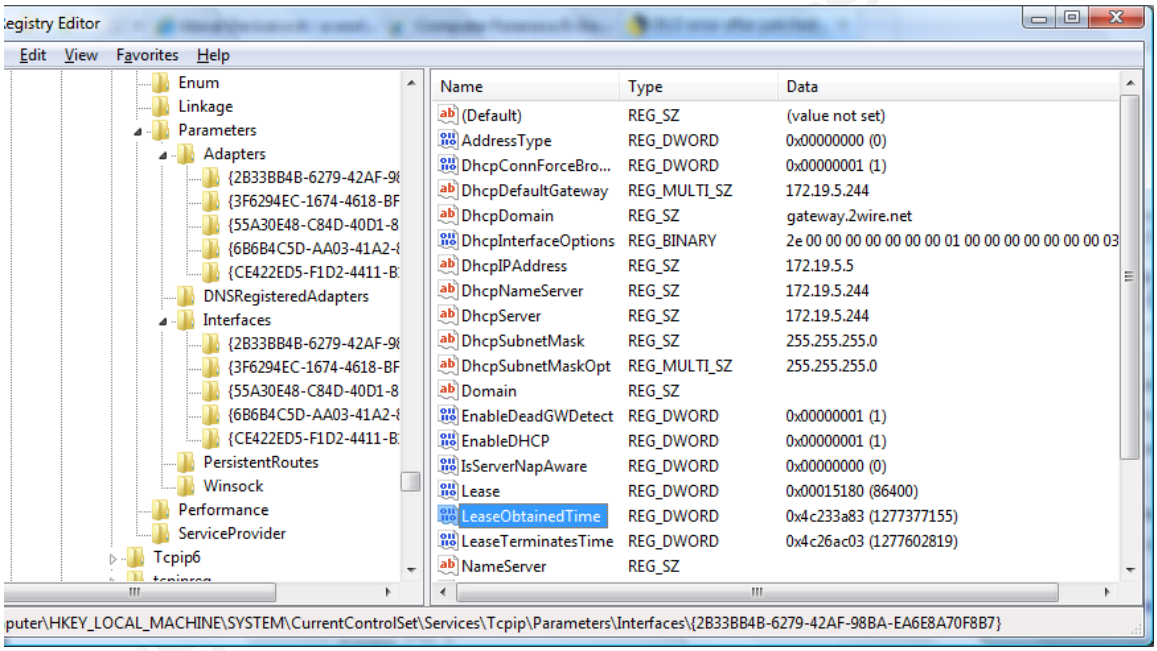

Figure 6 - TCPIP parameters associated with a wireless NIC

From this example, it can be determined what IP address was assigned to the computer (172.19.5.5), what the gateway address was (172.19.5.244), and the domain assigned to the device (gateway.2wire.net). It is also shown that the gateway is the DHCP server, so it may be safe to assume that this was a home gateway device.

Using another tool that is available to download for free called DCODE, we are able to decode the time values associated with the various settings. For example, the time that the lease was obtained is able to be determined using the DCODE tool (Free Tool – DCODE,

© 2011 The SANS Institute Author retains full rights.

2009). To calculate the date, place the numeric value of the LeaseObtainedTime key into the tool, and selecting the correct format of UNIX: Numeric Value, we can see that this DHCP lease was obtained on June 24, at 10:59:15 UTC. This output can be seen in Figure 7.

Following a similar calculation, it is determined that the lease for that address expired on June 27 at 01:40:19 UTC. Now it is known that the computer was connected to this network starting on June 24, 2010 at 10:59:15 UTC. We do not know when the computer was disconnected, but we do know it was before June 27, as the auto-renew functionally of DHCP would have renewed the lease prior to expiration.

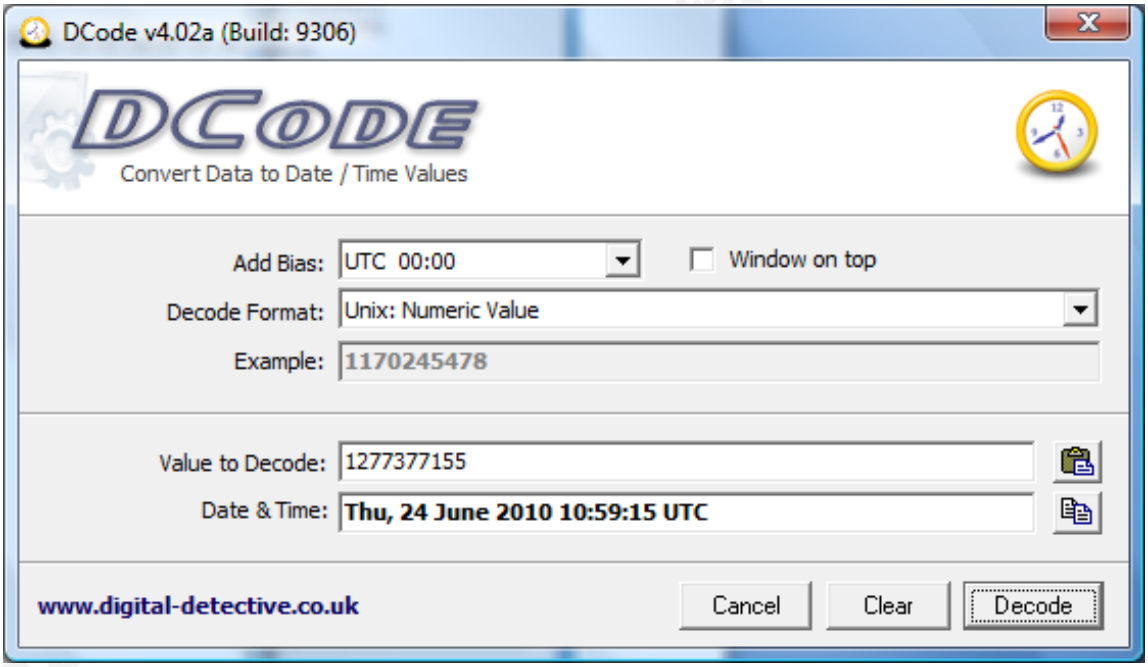

Figure 7 - Date decoding using the DCODE tool

Since it is known what timeframe this interface connected to the network, determining which network it connected to remains to be discovered. Within the following registry key:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\

© 2011 The SANS Institute Author retains full rights.

each of the networks that the computer has connected to is recorded by the system. Each one is identified by a profileGUID, similar to the device GUID seen previously. Within this registry key, the SSID of the network is contained within the Description key. When the computer first connected to the network is recorded in the DateCreated field, as well as the last time the computer connected, which is recorded in the DateLastConnected field. Examples of the registry key values and parameters are shown in Figure 8.

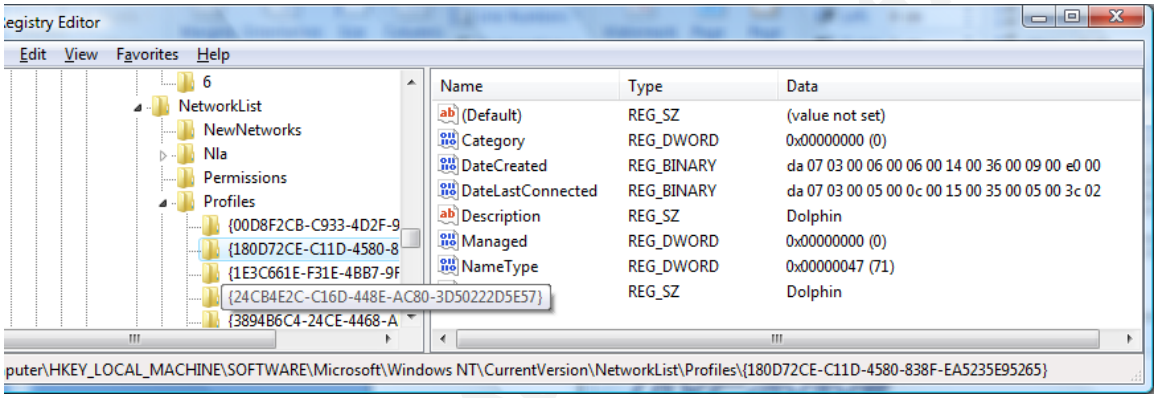

Figure 8 - Wireless profile settings registry key

The date format recorded within this key is different from the format in the TCPIP section. These are in a system binary structure, which can be broken up into 4-byte parts. Each part is in little endian format and corresponds to the following values, in order:

Year, Month, Weekday, Day, Hour, Minutes, Seconds, Thousandths

From the example shown in Figure 8, the Date Created registry key value is:

Da07 0300 0600 0600 1400 3600 0900 e000

To start translating this key, we need to break the key value into 4-byte pieces, as shown above. After breaking it up into these pieces, each piece will need to be changed to a format we can use from little endian. To manually convert this value, the 4 bytes pieces

© 2011 The SANS Institute Author retains full rights.

will need to be converted to a decimal value, and to convert these values, the following is performed.

Year - da07 changes to 07da = 2010

Month = 0300 changes to 0003 = March

Weekday – 0600 changes to 0006 = Saturday

Day - 0600 changes to 0006 = 06

Hour –1400 changes to 0014 = 20

Minutes – 3600 changes to 0036 = 54

Seconds – 0900 changes to 0009 = 09

Thousandths – e000 changes to 00e0 – 224

Based on the above information, the correct date from this translation of the key value is Saturday March 6, 2010 at 20:54:09.224. This is the first time that the computer connected to this network. (Computer Forensics/E-Discovery Tips/Tricks and Information, 2009)

Valid values for this conversation are as follows:

Year – Any valid year

Weekday – Sunday to Saturday, starting from value 0000 to value 0006

Day – from 1 to 31

Hour – from 00 to 23

Minute – from 0 to 59

Second – from 0 to 59

Thousandths – from 000 to 999

To avoid this manual calculation, the DCODE tool provides the ability to translate this date format also as shown in Figure 9.

© 2011 The SANS Institute Author retains full rights.

© 2011 SANS Institute, Author retains full rights.

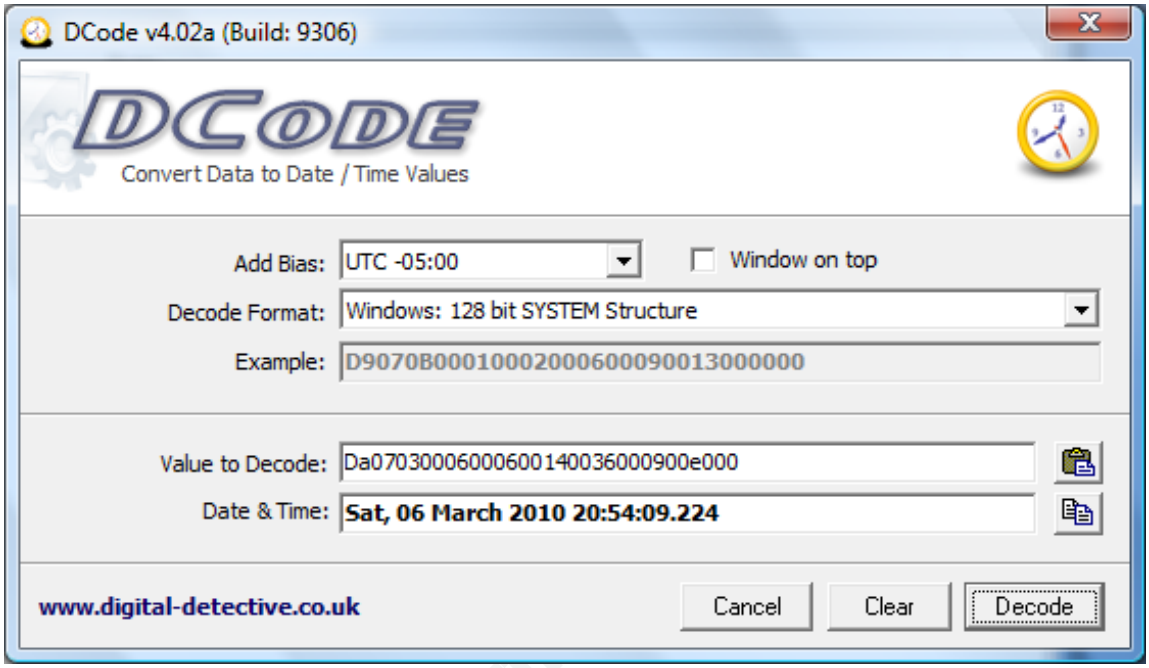

Figure 9 - DCODE of the DateCreated registry key

By using the tool, or performing the task manually, the last access date is determined which is found to be Friday March 12th, 2010 at 21:53:05.572. From the information gained from the interface settings, this is before the network connection time that is being looked for.

Selecting another key, we see the data shown in Figure 10.

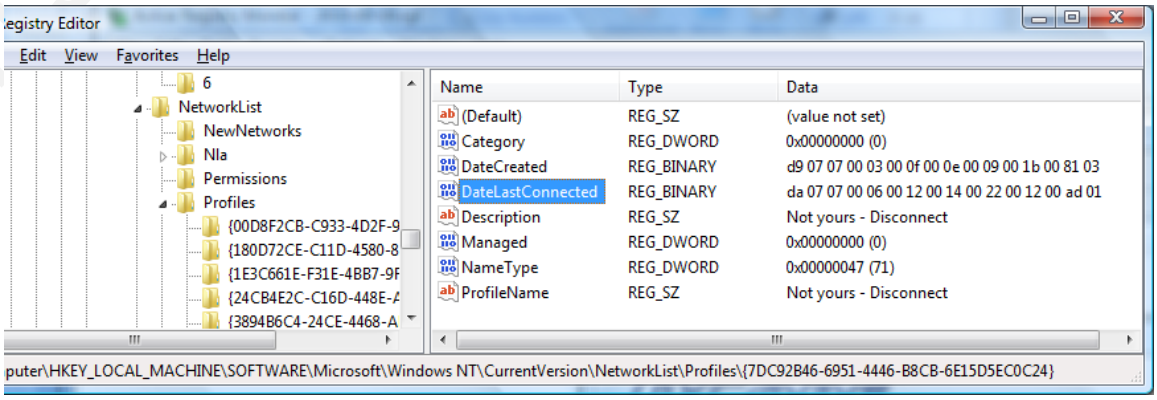

Figure 10 - Wireless profile settings registry key

Jonathan Risto, jonathan.risto@hotmail.com

© 2011 The SANS Institute Author retains full rights.

Using the same technique, it is found that this network, with the SSID of (Not Yours – Disconnect), was first connected to this network on Wed, 15 July 2009 14:09:27.897 and the last time the system was connected was on Sun, 18 July 2010 20:34:18.429. This network falls within the range of the dates in question, so it would be a possibility to consider. The remaining registry keys would need to be examined to determine if this is the only network that was accessed.

One final piece of wireless network information that is stored within the registry keys is found in the following registry key location:

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Signatues\Unmanaged\{ProfileGUID}

This registry key contains the MAC address of the wireless access point that the system connected to. It also contains the DNS suffix assigned to this network, the SSID, and the ProfileGUID is assigned in this registry. By searching for this GUID, you would be able to find either this key or the registry key containing the IP address information.

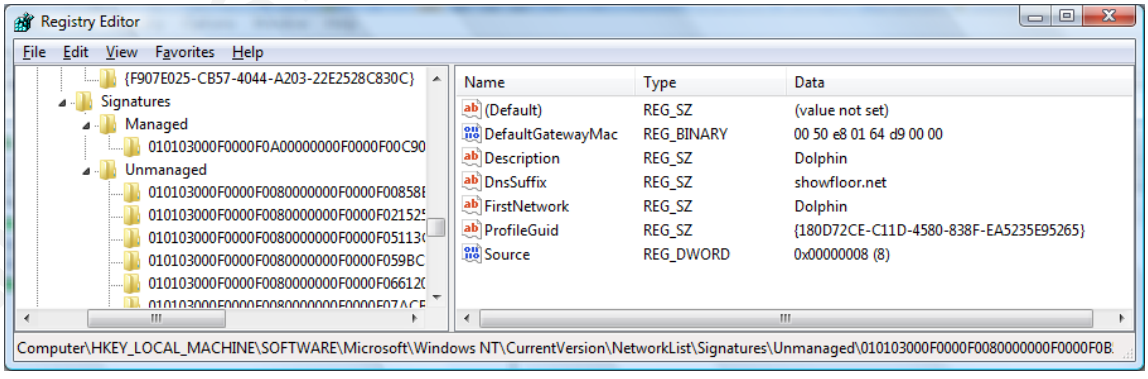

Figure 11 - Wireless access point information

© 2011 The SANS Institute Author retains full rights.

Once the MAC address is known, pin pointing down the exact access point that the computer has connected to becomes easier. Geolocation may also be possible using tools such as those provided by Skyhook (Skyhook, 2010). Skyhook has mapped out wireless access points within major cities and their associated MAC addresses. If the geographical location of the access point is important to know, then the use of such a site to help determine locations may be warranted.

2.2. Windows XP Wireless Registry Keys

Registry analysis on a Windows XP system is easier to do than on Windows Vista. This is not due to a better registry setup, but rather due to the numerous tools widely available that have the ability to parse through the hives and pull out the data. One tool that does an excellent job, puts the data into a useful text file and still provides you with the locations of the keys is the program regripper by Harlan Carvey. (Carvey, 2010)

XP registry entries for wireless network connections are stored in the following location (Carvey, 2009) :

HKLM|SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID}

An example of this registry is shown in Figure 12

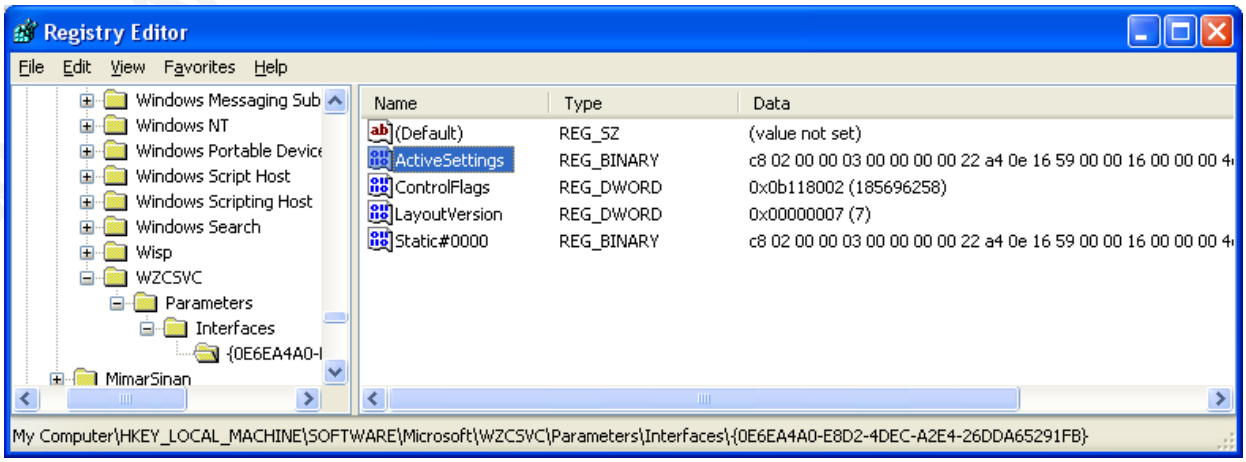

Figure 12 - Windows XP wireless registry example

© 2011 The SANS Institute Author retains full rights.

Within this registry key, the important information is shown in several locations. First, the ActiveSettings contains the information for the active wireless profile on the system. When this key is opened, the SSID of the network is shown. An example is of a network SSID (Not yours – Disconnect) is shown in Figure 13

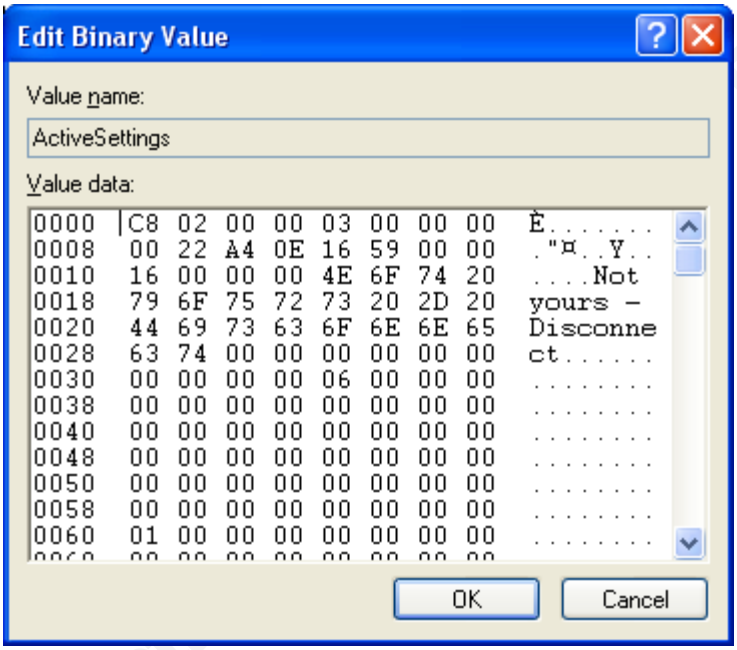

Figure 13 - SSID within the ActiveSettings registry key

The other important information within this key is found within the Static#000 value. This location shows each of the wireless networks that the system has connected to on this interface. If you open this registry key, you will see the SSID, which is the same as the active session. This is shown in Figure 14

© 2011 The SANS Institute Author retains full rights.

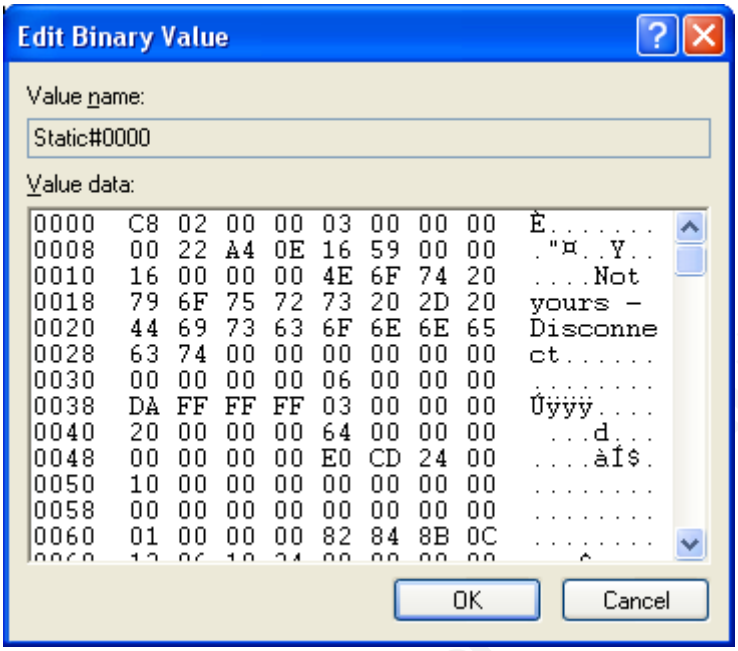

Figure 14 - Static#000 registry details

Most systems have connected to many wireless networks on the wireless interface installed. A laptop system that has been active for a longer period would likely display multiple values, such as seen in Figure 15.

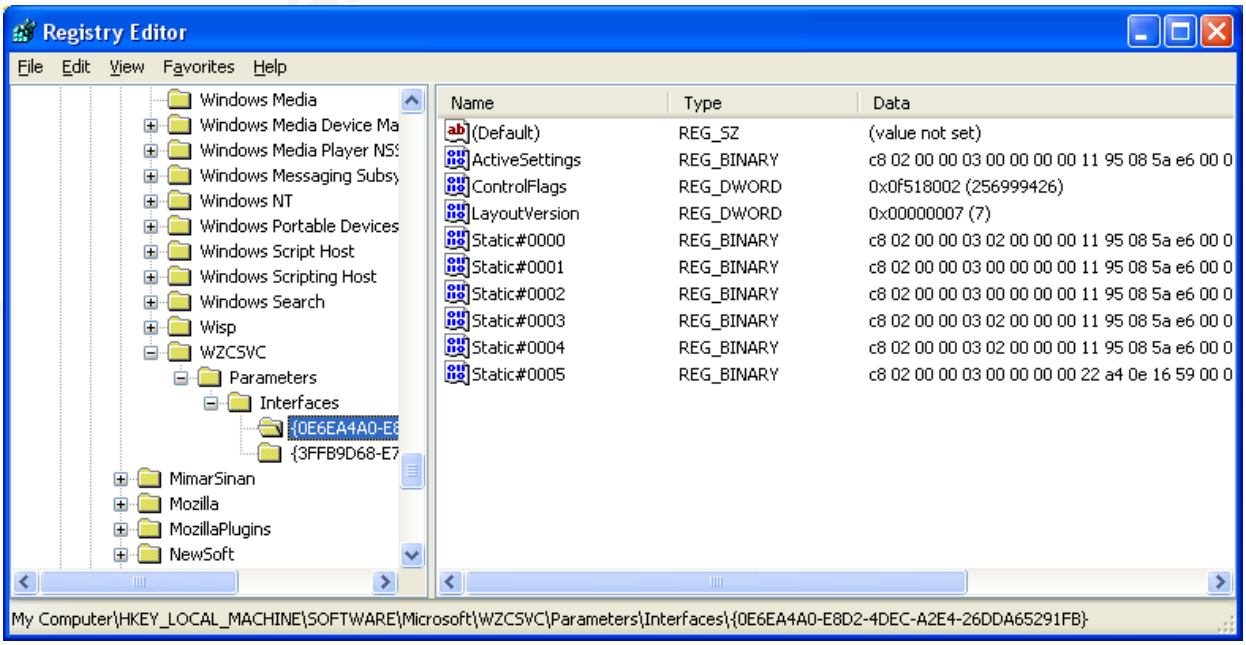

Figure 15 - Typical wireless settings view

Jonathan Risto, jonathan.risto@hotmail.com

© 2011 The SANS Institute Author retains full rights.

Within figure 15, each of the Static#xxx lines is a separate wireless network that the computer has connected to. The more entries located here, the more wireless networks the computer has connected to.

Because the system locks the hives when active, analysis on an active system is not possible, and so creting a copy is required.

To quickly find and determine all of this information, we can use the previously mentioned tool Regripper to create a copy of the registry hives. When launching regripper, you will be presented with a screen similar to the following:

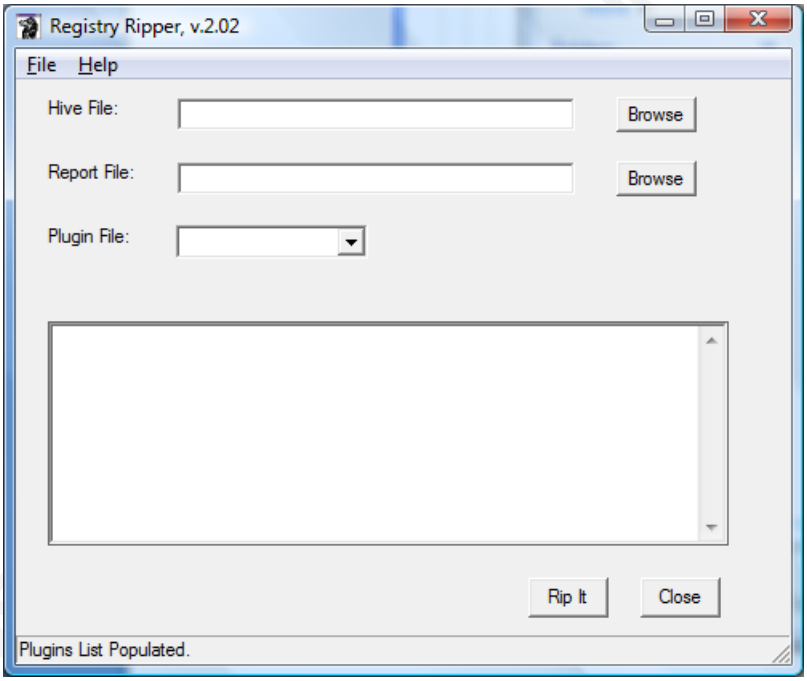

Figure 16 - Regripper main screen

To run the program, 3 pieces of information are needed: the hive location, the output filename, and the hive type (plugin file). With this information, click on the "Rip It" button and the output file will be created. A sample output screen using the system registry hive is shown in Figure 17.

© 2011 The SANS Institute Author retains full rights.

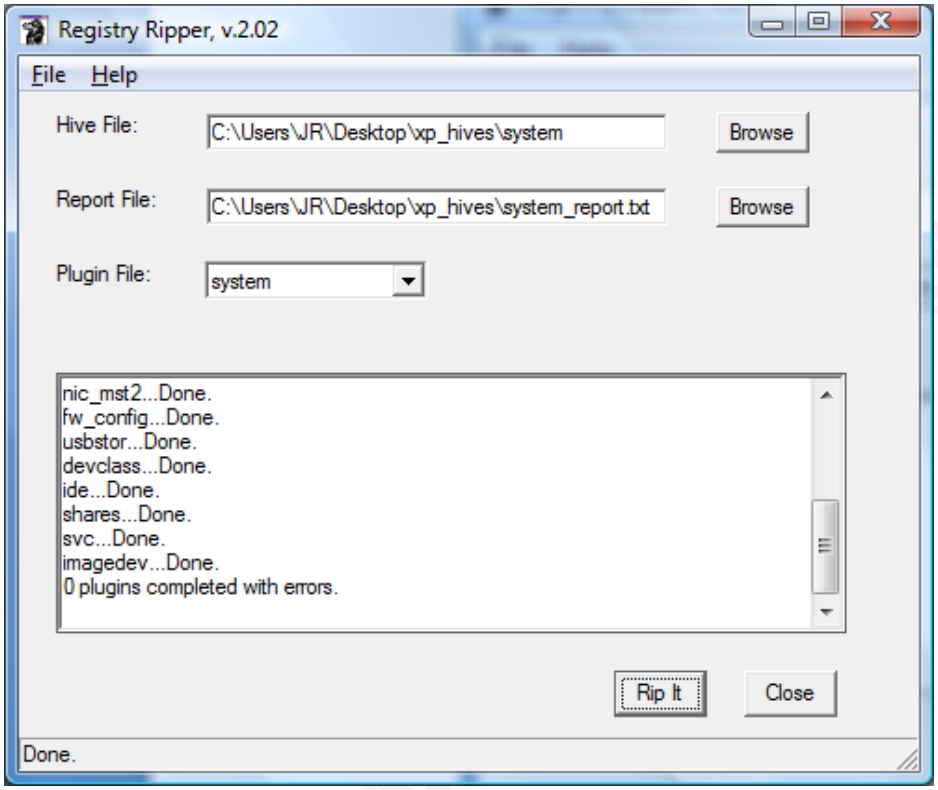

Figure 17 - regripper output

After the program has completed running, the text file output contains all of the information that was contained within the hive. It provides the key location, as well as the details surrounding the data stored within those keys, in text format, with all values decoded. An examples of information provided in the system hive relative to wireless settings is as follows:

Network key
ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}
Interface {0E6EA4A0-E8D2-4DEC-A2E4-26DDA65291FB}
LastWrite time Sat Aug 22 14:30:50 2009 (UTC)
Name = Wireless Network Connection
PnpInstanceID =
PCI\VEN_168C&DEV_0013&SUBSYS_3A131186&REV_01\4&5855BE9&0&10F0
MediaSubType = 2

© 2011 The SANS Institute Author retains full rights.

IpCheckingEnabled = 1

Interface {3FFB9D68-E701-40DE-ADAC-1F69A4EEA438}
LastWrite time Sun June 13 12:20:55 2010 (UTC)
Name = Wireless Network Connection 2
PnpInstanceID = USB\VID_07B8&PID_6001\5&30589810&0&7
MediaSubType = 2

This provides the {GUID} of each interface, what each interface is called, as well as when each interface was last changed. Details surrounding the IP data for that network are also found within the report.

Interface {3FFB9D68-E701-40DE-ADAC-1F69A4EEA438}
Name: Wireless Network Connection 2
Control\Network key LastWrite time Sun June 13 12:20:55 2010 (UTC)
Services\Tcpip key LastWrite time Sun June 13 16:30:57 2010 (UTC)
DhcpDomain =
DhcpIPAddress = 172.18.0.100
DhcpSubnetMask = 255.255.255.0
DhcpNameServer =
DhcpServer = 172.18.0.240

Interface {0E6EA4A0-E8D2-4DEC-A2E4-26DDA65291FB}
Name: Wireless Network Connection
Control\Network key LastWrite time Sat Aug 22 14:30:50 2009 (UTC)
Services\Tcpip key LastWrite time Sun June 13 18:27:30 2010 (UTC)
DhcpDomain = gateway.2wire.net
DhcpIPAddress = 172.19.5.6
DhcpSubnetMask = 255.255.255.0
DhcpNameServer = 172.19.5.244
DhcpServer = 172.19.5.244

© 2011 The SANS Institute Author retains full rights.

This provides us with all of the IP address information associated with the wireless interfaces, collected all together in an easy to read format. Next, performing the same task with the software hive, the following additional wireless information is found:

NetworkCards
Microsoft\Windows NT\CurrentVersion\NetworkCards

Intel(R) PRO/100 VE Network Connection [Sat Aug 15 00:32:55 2009]
XPC 802.11b/g Wireless Kit [Sun June 13 12:20:55 2010]
D-Link AirPlus DWL-G520 Wireless PCI Adapter(rev.B) [Tue Aug 11 00:58:08 2009]

SSID
Microsoft\WZCSVC\Parameters\Interfaces

NIC: D-Link AirPlus DWL-G520 Wireless PCI Adapter(rev.B)
Static#0000 SSID : rocky - go away :) [Sun June 13 03:47:36 2010]
Static#0001 SSID : Not yours - Disconnect [Sun June 13 18:26:09 2010]
NIC: XPC 802.11b/g Wireless Kit
Static#0000 SSID : Not your AP - go away :) [Sun June 13 16:30:33 2010]
Static#0001 SSID : Not yours - Disconnect [Sun June 13 13:10:15 2010]
Static#0002 SSID : New rocky - go away :) [Sun June 13 14:08:54 2010]

From this information, it can be determined that both network cards were connected to the same SSID at one point, and, in total, there are 4 different networks that have been connected. This tool removes the need to go manually into the registry and calculate values and parameters. An excellent time saver for sure, but if the raw registry format needs to be examined, an example of the information contained within the TCPIP parameters is shown in Figure 18

© 2011 The SANS Institute Author retains full rights.

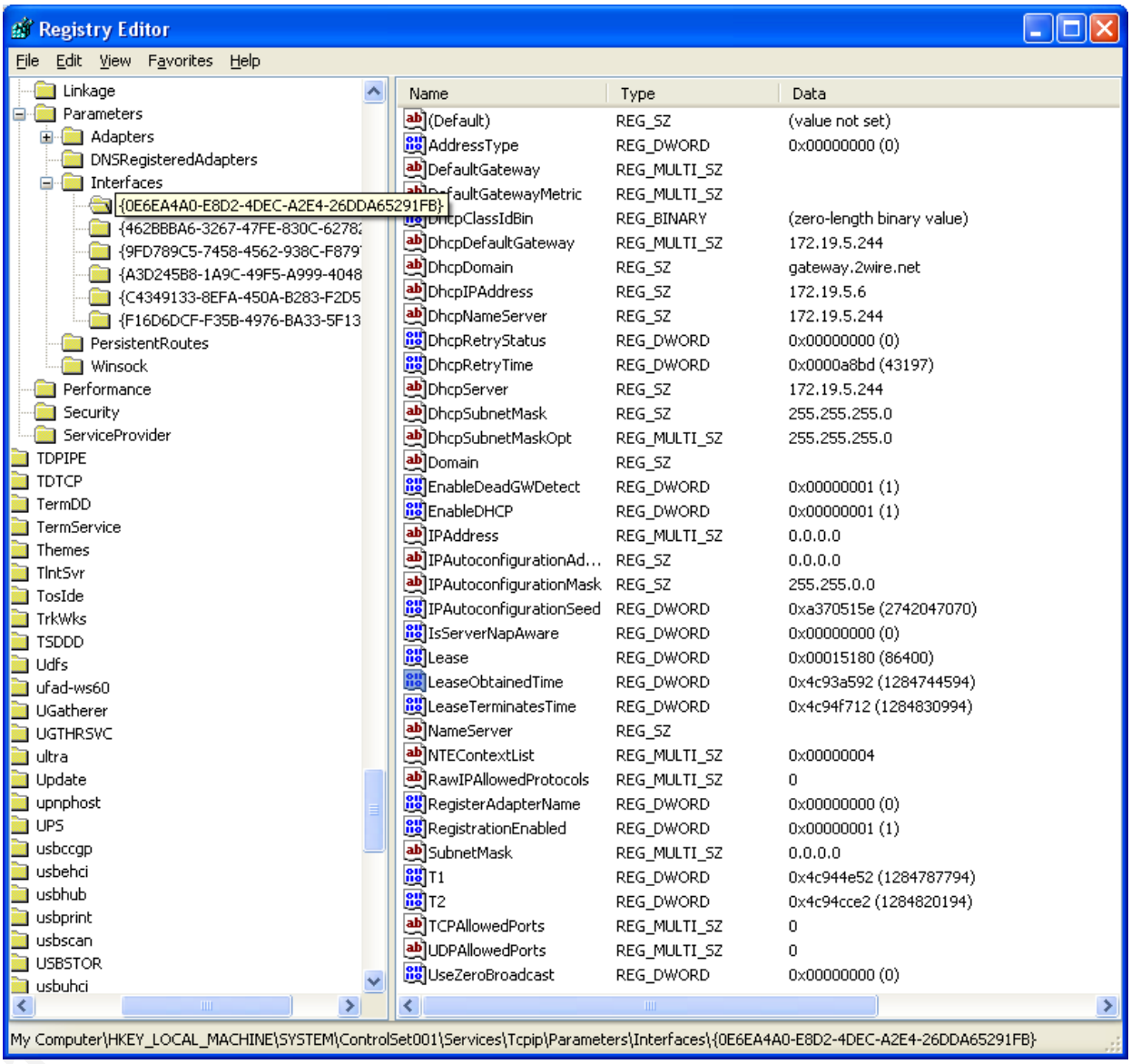

Figure 18 - Example TCPIP parameters registry key

2.3. Automating Registry Analysis

A simple tool, Active Registry Monitor (About Active Registry Monitor, 2010), was used to perform registry comparisons throughout this paper to help determine registry key locations. With this tool, changes made from one registry scan to the next

© 2011 The SANS Institute Author retains full rights.

can be compared to view which keys and values have changed. For example, when a new USB wireless device is connected to a Windows Vista system, the following information is displayed:

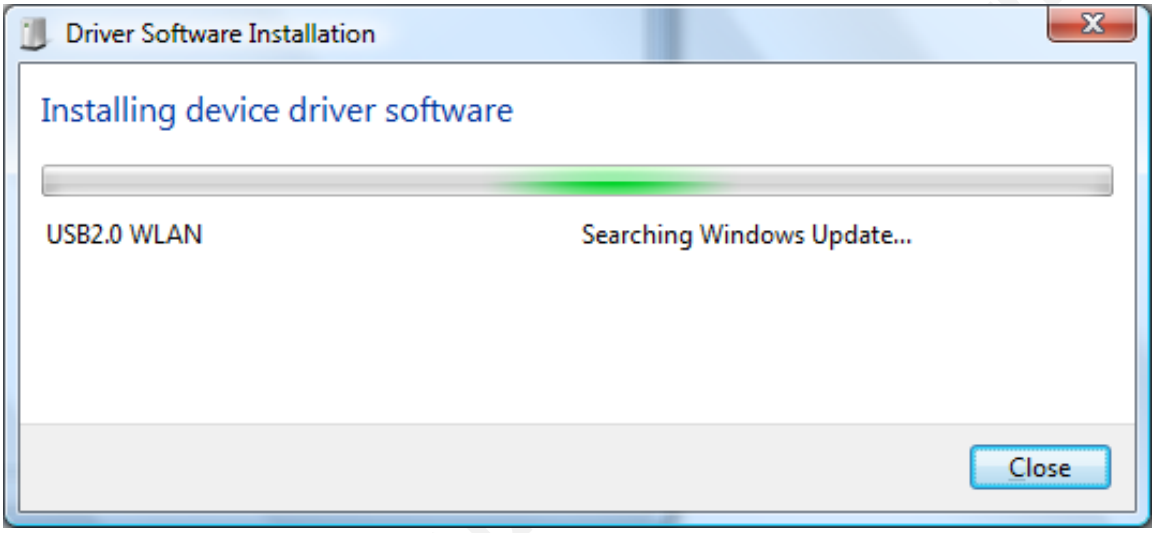

Figure 19 - Installing a new device on Windows Vista

This installation creates a large number of registry key, and by using the Active Registry Monitor program, it is easy to determine which keys have changed. In this example, a new USB wireless NIC was inserted into the computer in question. A scan was performed prior to inserting the USB device and again immediately after the system installation was completed. As shown in Figure 21, there were 259 additions to the registry from this task. Some wireless specific key data is shown in Figures 21 and 22.

© 2011 The SANS Institute Author retains full rights.

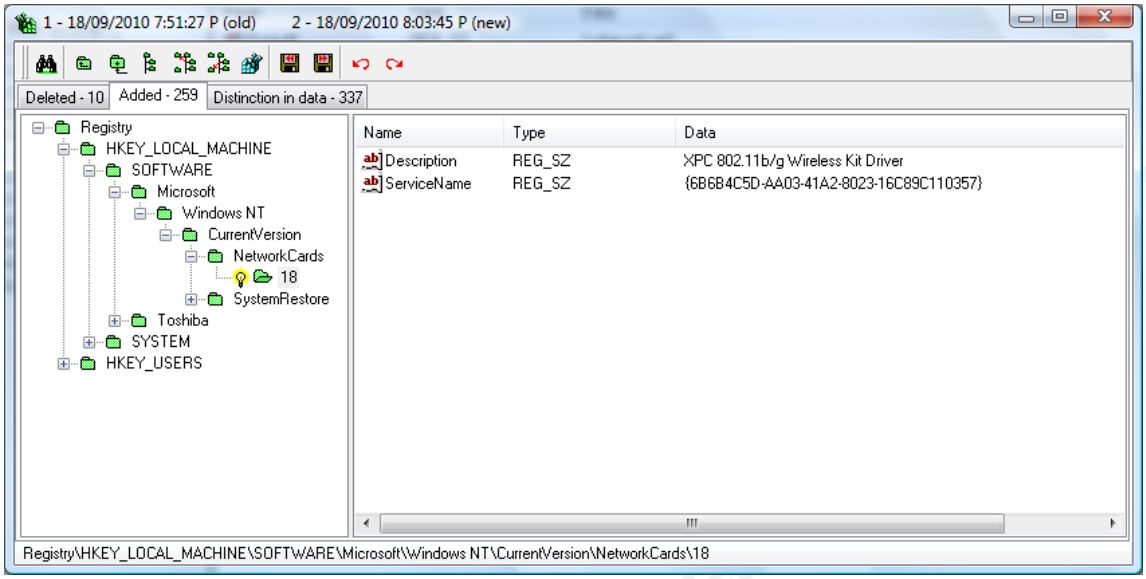

Figure 20 - Keys added from installing a new USB Wireless NIC

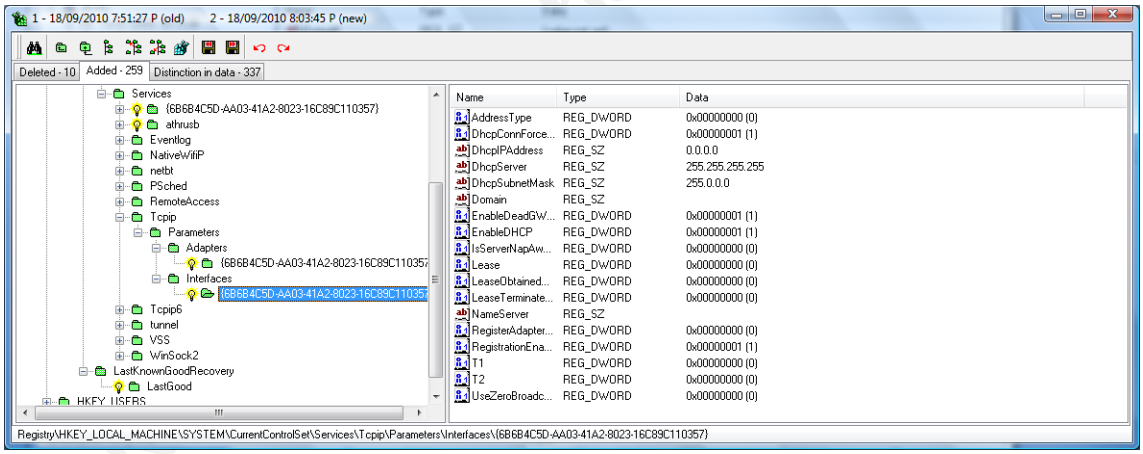

Figure 21 - TCPIP parameters created with the installation of a new NIC

With this program, it is possible to determine exactly what registry keys are changed when certain activities occur on a specific computer. For example, when a system connects to a network or when a system is connecting to a new network, this tool can quickly map out all this information to show exactly which registry keys are impacted and to aid the examiner during future investigations.

Jonathan Risto, jonathan.risto@hotmail.com

© 2011 The SANS Institute Author retains full rights.

3. Conclusions

A Windows registry contains most of the configuration settings for the specific computer. With some knowledge of key locations as well as some basic analysis of the registry keys shown within this paper, an examiner is able to discover wireless network connection information, including when and where these networks were connected to, the IP addresses assigned, and the identification of these networks, either by SSID or by MAC addresses. It has been shown where this information is stored within the registry, as well as providing some tools that can assist in locating and decoding the various registry values more efficiently that via manual methods. Understanding the location of the registry keys, and the means to decode the values contained within provides the incident responder and analyst a powerful avenue for determining possible vectors for infection as well as verifying compliance with wireless polices that may be in place.

© 2011 SANS Institute, Author retains full rights.

Jonathan Risto, jonathan.risto@hotmail.com

© 2011 The SANS Institute Author retains full rights.

4. References

About Active Registry Monitor. (2010). Retrieved April 10th, 2010 from Device Lock website: http://www.devicelock.com/arm/

Windows Registry information for Advanced Users. (2008). Retrieved March 20,2010 from Microsoft Support website: http://support.microsoft.com/kb/256986

Windows Registry information for Advanced Users. (2008). Retrieved March 20,2010 from Microsoft Support website: http://support.microsoft.com/kb/256986

Free Tool – DCODE. (2009). Retrieved April 4th, 2010 from Digital Detective website: http://www.digital-detective.co.uk/freetools/decode.asp

Computer Forensics/E-Discovery Tips/Tricks and Information. (2009). Retrieved April 4th, 2010 from Computer Forensics/E-Discovery Tips/Tricks and Information website: http://cfed-ttf.blogspot.com/2009/08/decoding-datecreated-and.html

Skyhook. (2010). Retrieved August 19th, 2010 from Skyhook website: http://www.skyhookwireless.com/

Carvey, Harlan. (2010). *RegRipper*. Retrieved June 10, 2010 from RegRipper website: http://regripper.net/

Carvey, Harlan. (2009). *Windows Forensics Analysis*. Burlington, MA: Syngress Publishing

Jonathan Risto, jonathan.risto@hotmail.com

© 2011 The SANS Institute Author retains full rights.