



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 permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics
at <http://www.giac.org/registration/gcfa>

Table of Contents.....	1
Ben_Doyle_GCFA.doc.....	2

© SANS Institute 2005, Author retains full rights.

GIAC Certified Forensic Analyst

Practical Assignment

(GCFA) – Version 2.0

By Ben Doyle (25th January 2005)

© SANS Institute 2005, Author retains full rights

Abstract

CC Terminals has requested that a forensic analysis of the provided USB Flashdrive image be done. The disk image [USBFD-64531026-RL-001.img] was created from a USB Flashdrive [USBFD-64531026-RL-001] that CC Terminals had quarantined as evidence in an investigation of one of their employees. The employee in question, Robert Lawrence (name provided by CC Terminals), is suspected of harassing a fellow employee Leila Conlay (name provided by CC Terminals). CC Terminals requires the following:-

- Determine all files that are currently stored on the seized USB Flashdrive [USBFD-64531026-RL-001] using the provided image [USBFD-64531026-RL-001.img]
- Recover any available data that may have been deleted from the USB Flashdrive [USBFD-64531026-RL-001]
- Determine if there is any evidence on the USB Flashdrive [USBFD-64531026-RL-001] that indicates how Robert Lawrence was able to make contact with Leila Conlay using her personal email account.
- Determine if there is any evidence on the USB Flashdrive [USBFD-64531026-RL-001] that indicates how Robert Lawrence was able to make contact with Leila Conlay at a café outside of work hours.

© SANS Institute 2005, Author

Part One:

Analyze an image provided to you from this web site

Forensic Report – Case: CC_Terminals_20050125

Evidence:- 64M Lexar Media JumpDrive
Serial #: JDSP064-04-5000C
(MD5: 338ecf17b7fc85bbb2d5ae2bbc729dd5)

Chain of Evidence Tag #: USBFD-64531026-RL-001

Notes: An image of the USB Flashdrive was provided for our analysis by the security administrator Mark Mawer. The file name of the image was USBFD-64531026-RL-001.img

Assumptions:-

It is assumed that the image provided is a true bit copy of the original USB Flashdrive [USBFD-64531026-RL-001] in evidence, and that the evidence has not been tampered with since being seized.

How this report is organised

This report has been presented in four sections. The Abstract provides an overview of the initial information that was provided to undertake the forensic investigation and the results that were obtained during the investigation are presented in the second section labelled "Summary". At the end of the "Summary" section are some suggested actions the system administrator may take following this incident. The third section explains in detail, the forensic process that was followed to obtain the results presented in the "Summary". The detailed outputs created during the forensic analysis are presented in the final section of Appendixes.

Abstract

CC Terminals has requested that a forensic analysis of the provided USB Flashdrive image be done. The disk image [USBFD-64531026-RL-001.img] was created from a USB Flashdrive [USBFD-64531026-RL-001] that CC Terminals had quarantined as evidence in an investigation of one of their employees. The employee in question, Robert Lawrence (name provided by CC Terminals), is suspected of harassing a fellow employee Leila Conlay (name provided by CC Terminals). CC Terminals requires the following:-

- Determine all files that are currently stored on the seized USB Flashdrive [USBFD-64531026-RL-001] using the provided image [USBFD-64531026-RL-001.img]
- Recover any available data that may have been deleted from the USB Flashdrive [USBFD-64531026-RL-001]
- Determine if there is any evidence on the USB Flashdrive [USBFD-64531026-RL-001] that indicates how Robert Lawrence was able to make contact with Leila Conlay using her personal email account.
- Determine if there is any evidence on the USB Flashdrive [USBFD-64531026-RL-001] that indicates how Robert Lawrence was able to make contact with Leila Conlay at a café outside of work hours.

Summary

Executive Summary of Findings

The Security Administrator, Mike Mawer, of the credit card processing firm CC Terminals, provided us an image [USBFD-64531026-RL-001.img] of a previously seized USB Flashdrive from an internal investigation. An “image” is a true and exact copy of some form of computer data. The “image” is used to undertake forensic analysis with. By using an “image” the original evidence can be securely stored away so it is not able to be modified after the time that it was seized.

Upon forensic investigation of the image [USBFD-64531026-RL-001.img], it was found that the owner of the original USB Flashdrive [USBFD-64531026-RL-001] may have been using computer resources to spy on the network traffic of another employee “Leila”. Documentation was also found that suggest that a Robert Lawrence may have been harassing another employee.

During the detail investigation of the USB Flashdrive image [USBFD-64531026-RL-001.img] it was discovered a number of files had been deleted. Some of those files that were deleted, and then forensically recovered, were related to software used to monitor and capture computer network traffic. The software packaged found on the USB Flashdrive [USBFD-64531026-RL-001]

to undertake this task was called WinDump. The program WinDump was recovered from the USB Flashdrive [USBFD-64531026-RL-001] as well as a file that contained a saved copy of the traffic that was captured using the software package. On investigation, the saved traffic revealed that the person who used the software package WinDump, had monitored another employee sending an email using the web based email provider Hotmail. The monitored employee had a Hotmail email account with the login of flowergirl96@hotmail.com and had signed their name as "Leila". The monitored email was being sent to a SamGuarillo@hotmail.com agreeing to a meet at a coffee shop on the corner of Hollywood and McCadden at 7pm. A computer graphic showing a street map of the location mentioned in the captured email was also recovered also from the USB Flashdrive image [USBFD-64531026-RL-001.img]. This graphic had been deleted previously from the USB Flashdrive.

There were three Microsoft Word 10, from the Microsoft Office 2000 suite, documents found on the USB Flashdrive image [USBFD-64531026-RL-001.img]. The documents are recorded as have been written by a Richard Lawrence on the dates of 26th, 27th and 29th of October 2004. The contents of the documents are letters to an unnamed person. The first letter's contents seem fairly benign, however by the last document the letter that was written was aggressive. The full content of the letters can be found at the end of the third section of this report.

The forensic evidence that was gathered as part of the investigation for CC Terminals into the USB Flashdrive image [USBFD-64531026-RL-001.img] could not be used to determine if any laws were broken. Although we can prove that the software package "WinDump" was used to monitor and capture computer network traffic, this in itself does not break any laws in Australia. The Commonwealth Crimes Act 1914 only has legislation that covers the harassment of another person using a carrier service (Section 85ZE). Under the Commonwealth Telecommunications Act 1997, a carrier service is defined as a service offered by company that has been provisioned with a carrier license.

The information that was recovered, in conjunction with testimony from the targeted employee, may be enough to charge the owner of the USB Flashdrive [USBFD-64531026-RL-001] with sexual harassment.

CC Terminals should review all its network and HR policies to ensure that there are policies that cover the use of computer facilities to harass other employees. The corporate policies should also state that it is unacceptable to use software to monitor computer generate traffic.

Suggested Actions

- 1) Review the network architecture of the facility the incident occurred at. If the facility used network switches, and not hubs, the ability for end-users to easily monitor other employee's traffic would be limited. From the investigation it is likely that hubs are used to connect end-users to

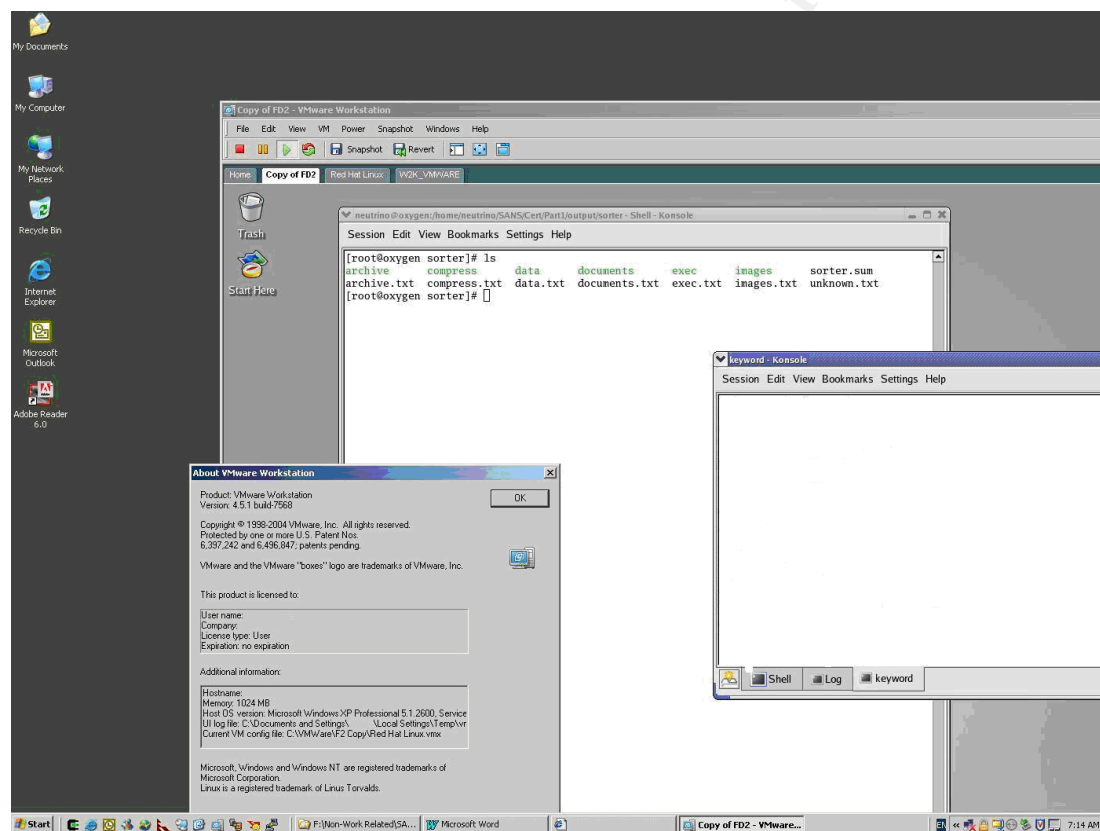
CC Terminals network. Hubs have no segmentation of traffic, and all computers can see the network traffic of all other computers connected to the same hub. A network switch segments the traffic so only intended computer sees its own network traffic. It is suggested that the security administrator at CC Terminals read the following article to familiarise themselves with the risks of unapproved network monitoring on a non-switched and switched network.

(http://www.sans.org/resources/idfaq/switched_network.php) . This document should provide a starting point for the security administrator to be able to analyse the risk to CC Terminals by someone being able to view sensitive data crossing their LAN infrastructure.

- 2) Undertake a risk review and cost benefit justification to determine if software can be employed to limit the use of USB Flashdrives. USB Flashdrives offer the same risks that floppy disks do (uncontrolled data movement), however USB Flashdrives can hold significant more data, and therefore pose a much greater risk. If the owner of the Flashdrive was not able to download the software package at work, they may have download it externally and then used the Flashdrive to use it on CC Terminals computers. If software control is not appropriate, then it is suggested that corporate policy be reviewed, and end-users be re-educated on the acceptability and use of USB Flashdrive at CC Terminals.
- 3) As CC terminals offers its customers a sensitive service (credit card processing), it is suggested that the security administrator captures network traffic at various desktop locations so CC Terminals may determine the risk of comprising sensitive information transversing the corporate LAN. The security administrator can use a software package like Ethereal to undertake this task. A user guide on how to use the Ethereal to monitor and capture traffic can be found at <http://www.ethereal.com/docs/user-guide/chap03.html>
- 4) In the future the security administrator may wish to do an initial analysis on copies of seized media before seeking professional services. The security administrator can review the documents at <http://www.sleuthkit.org/sleuthkit/docs.php> and <http://www.sleuthkit.org/sleuthkit/tools.php> to gain an understanding of the tools that were used during this investigation. It is essential that proper procedures for handling forensic evidence always be followed, and that any analysis is only done on a forensic copy of the seized media.

Forensic Preparation

The forensic analysis of the supplied image [USBFD-64531026-RL-001.img] was done using virtual computing software called VMware. The VMware products allow end users to run multiple copies of the same or different operating systems (as long as they are the same CPU architecture (i.e. x86)) at the same time. The VMware version that was used was VMware Workstation, Version 4.5.1 build -7568 running in a Microsoft Windows XP SP1 environment. VMware was used to run a known good copy (snapshot) of a virtual computer running Redhat Fedora2 Linux. VMware has the capability to share a computer's resources with any virtual computers it is running. To isolate the Fedora2 VMware environment, the VMware hardware mappings for the CDROM, floppy disk drive, network ethernet NIC's, audio and USB devices were disabled. A CD-R was used to transfer files into the system, so the CDROM hardware mappings in VMware were only enabled when data needed to be introduced into the Fedora2 environment.



The VMware Fedora2 Linux environment was a known forensically safe system. All the Linux programs in the Fedora2 snapshot had previously been verified to ensure they had not been changed or tampered with in any way. The forensic programs/toolkits that were installed and utilised from this Fedora2 environment were:-

SleuthKit Toolkit (v1.73) – This toolkit is a collection of forensic programs

that were created to help in the forensic analysis of stored data. The Sleuthkit is an open source project to provide forensic tools that analysts can use without charge. Being open source also allows analysts to examine the source program code to ensure the integrity of the utilities.

Other programs that were used as part of this forensic analysis, but are not specifically designed for forensics were:-

Strings – this program extracts all ASCII characters (ASCII characters includes the English alphabetic characters) from any data. In a lot of cases the extract ASCII characters will provide relevant information.

File – this program attempts to analyse data to determine if it is of a certain format (e.g. gif image, word document, zip file).

In addition to the VMWare Fedora2 Linux environment, a forensically safe copy of Microsoft Windows 2000 was installed into a VMWare environment. This environment was required to analyse any Microsoft Windows executables found on the USB Flashdrive image [USBFD-64531026-RL-001.img].

Detailed Forensic Analysis

Following is a detail explanation of the forensic analysis taken on the image [USBFD-64531026-RL-001.img] provided by CC Terminals. The section is split into four sections. The first section details the image [USBFD-64531026-RL-001.img] integrity checking. In the second section of the forensic analysis we analyse the actual image [USBFD-64531026-RL-001.img] and undertake the initial data extraction held within the image. The third section is dedicated to the detailed forensic analysis of the executable as required by CC Terminals, while the last section details other evidence that was found.

Integrity Checking the Image


A MD5 hash calculation was done to verify that the image that was being analysed was the same that CC Terminals had provided.

- The MD5 hash for the image [USBFD-64531026-RL-001.img] was calculated and compared with the MD5 hash provided by CC Terminals

[MD5 HASH Provided]:- 338ecf17b7fc85bbb2d5ae2bbc729dd5

[Command Used]:- /usr/bin/md5sum ./USBFD-64531026-RL-001.img > ./output/ USBFD-64531026-RL-001.img.md5

[MD5SUM Result]:- 338ecf17b7fc85bbb2d5ae2bbc729dd5

A screenshot of a terminal window titled 'neutrino@oxygen:/home/neutrino/NEWSAN'. The terminal shows a series of commands and their outputs. First, the command '>/usr/bin/md5sum ./USBFD-64531026-RL-001.img > ./output/USBFD-64531026-RL-001.img.md5' is entered, followed by '>' on the next line. Then, the command '>cat ./output/USBFD-64531026-RL-001.img.md5' is entered, and the output '338ecf17b7fc85bbb2d5ae2bbc729dd5 ./USBFD-64531026-RL-001.img' is displayed. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Terminal', 'Tabs', and 'Help'.

```
neutrino@oxygen:/home/neutrino/NEWSAN
File Edit View Terminal Tabs Help
>/usr/bin/md5sum ./USBFD-64531026-RL-001.img > ./output/USBFD-64531026-RL-001.img.md5
>
>cat ./output/USBFD-64531026-RL-001.img.md5
338ecf17b7fc85bbb2d5ae2bbc729dd5 ./USBFD-64531026-RL-001.img
>
```

Initial Image Analysis and Data Extraction

The following steps were undertaken to determine the initial configuration of the data stored on the image, and to extract that data in preparation for further analysis.

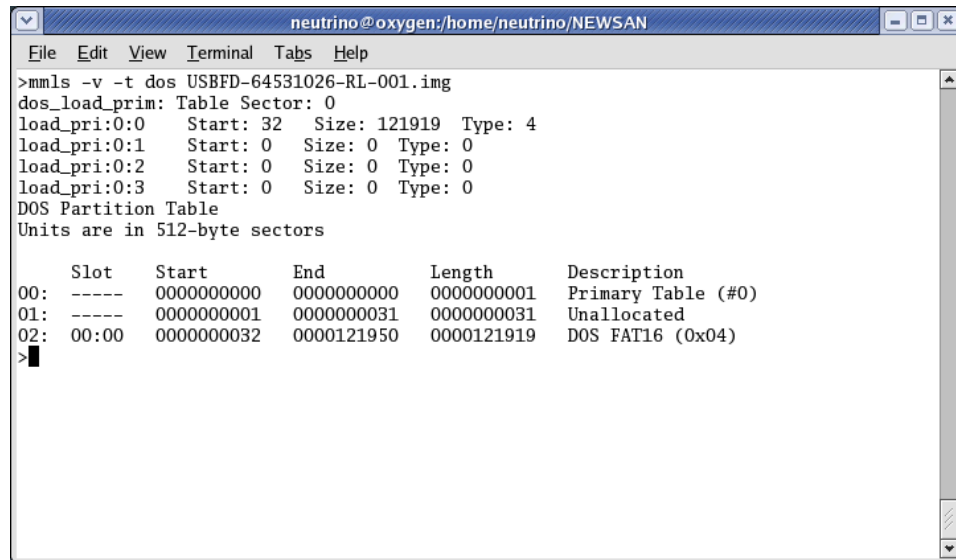
- The command “file” was run to determine what filesystem format the image [USBFD-64531026-RL-001.img] was. In general, all data is written following a template specified by the program creating it. This data may include a small amount of data at the start (header) or end (footer) of the data that is the same for every file created in that format, and therefore identifies the data. The command “file” has a small database of these identifiers, and when run against a file will print out the associated format if an identifier matches one found in the data being analysed.

[Command Used]:- /usr/bin/file ./USBFD-64531026-RL-001.img
[Result]:- x86 boot sector

This result would indicate that the USB Flashdrive [USBFD-64531026-RL-001] was formatted with a dos base file system.

- The “mmls” tool from SleuthKit was used to print the partition table stored in the USB image [USBFD-64531026-RL-001.img]. This showed that the USB image had a large DOS FAT16 partition created on it.

[Command Used]:- mmls -v -t dos USBFD-64531026-RL-001.img



```

neutrino@oxygen:/home/neutrino/NEWSAN
File Edit View Terminal Tabs Help
>mmls -v -t dos USBFD-64531026-RL-001.img
dos_load_prim: Table Sector: 0
load_pri:0:0   Start: 32   Size: 121919   Type: 4
load_pri:0:1   Start: 0    Size: 0      Type: 0
load_pri:0:2   Start: 0    Size: 0      Type: 0
load_pri:0:3   Start: 0    Size: 0      Type: 0
DOS Partition Table
Units are in 512-byte sectors

   Slot   Start      End          Length      Description
00:  -----  0000000000  0000000000  0000000001  Primary Table (#0)
01:  -----  0000000001  0000000031  0000000031  Unallocated
02:  00:00   0000000032  0000121950  0000121919  DOS FAT16 (0x04)
>

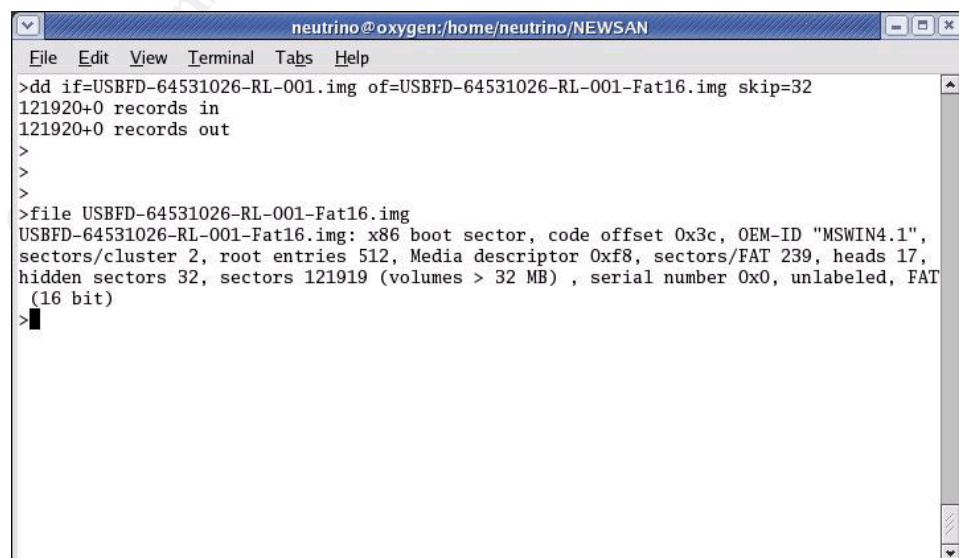
```

- To be able to utilize other forensic tools, it was required that an image of the FAT16 partition table be recovered from the provided image [USBFD-64531026-RL-001.img]. The Unix command “dd” was used to carve out the FAT16 partition from the original image [USBFD-64531026-RL-001.img] and write it to a separate file. As can be seen from the “mmls” output, the FAT16 partition started on sector 32. Therefore when running the command “dd” it was required to skip the first 32 sectors.

[Command]:- dd if= USBFD-64531026-RL-001.img of= USBFD-64531026-RL-001-Fat16.img skip=32

- The “file” command was used on the output of the “dd” command to ensure that the FAT16 partition was extracted successfully. The output from the command showed the partition image created was successful.

[Command]:- file USBFD-64531026-RL-001-Fat16.img



```

neutrino@oxygen:/home/neutrino/NEWSAN
File Edit View Terminal Tabs Help
>dd if=USBFD-64531026-RL-001.img of=USBFD-64531026-RL-001-Fat16.img skip=32
121920+0 records in
121920+0 records out
>
>
>
>file USBFD-64531026-RL-001-Fat16.img
USBFD-64531026-RL-001-Fat16.img: x86 boot sector, code offset 0x3c, OEM-ID "MSWIN4.1",
sectors/cluster 2, root entries 512, Media descriptor 0xf8, sectors/FAT 239, heads 17,
hidden sectors 32, sectors 121919 (volumes > 32 MB) , serial number 0x0, unlabeled, FAT
(16 bit)
>

```

- The “fsstat” command was then used against the partition image [USBFD-64531026-RL-001-Fat16.img] to extract information about the Fat16 filesystem that was created on the USB Flashdrive. The “fsstat” command is one of the tools that is supplied with the open source forensic project called SleuthKit. The information provided by the “fsstat” command may be useful later in the forensic analysis as input for other forensic tools.

[Command]:- fsstat -f fat16 ./USBFD-64531026-RL-001-Fat16.img > ./output/filesystem.details

[Results]:- For full results see Appendix A

- Using the commands “fls”, “ils” and “mactime” from the SleuthKit (v1.73), a MAC (modified, accessed, created) timeline was created of all data found on the FAT16 image [USBFD-64531026-RL-001-Fat16.img].

The “fls” command is used to extract the MAC times for all files that are still allocated in the image. An assumption was made that the USB Flashdrive was originally connected to a Windows system under the directory “D:”.

The “ils” command is used to extract the MAC times for any files that have unallocated (deleted) from the image (and hence the USB Flashdrive). Although the file has been deleted, if the filesystem information has not be written over with new data, then with the appropriate tools, the data may still be recovered.

The “mactime” command is used to format the output from the “fls” and “ils” commands into a more human readable format.

[Command to Find allocated files]:-

fls -f fat16 -m “d:” -r ./ USBFD-64531026-RL-001-Fat16.img > ./output/body

[Results]:- For full results see Appendix B

[Command to Find unallocated data]:-

ils -f fat16 -m ./ USBFD-64531026-RL-001-Fat16.img >> ./output/body

[Results]:- For full results see Appendix C

[Command to format timeline data]:-

mactime -b ./output/body > ./output/mactime.body

[Results]:- For full results see Appendix D

The MAC timeline that was created from the partition image [USBFD-64531026-RL-001-Fat16.img] provided the following information in relation to CC Terminals request for information:-

[Earliest timestamp]:- Mon Oct 25 2004 00:00:00 (d:/her.doc)

[Oldest timestamp]:- Thu Oct 28 2004 19:24:48 (d:/coffee.doc)

File Name	File Size (bytes)	Status
her.doc	19968	Exists
hey.doc	19968	Exists
WinDump.exe	450560	Deleted
WinPcap 3 1 beta 3.exe	485810	Deleted
coffee.doc	19968	Exists

_apture	53056	Deleted
_ap.gif	8814	Deleted

- The MAC timeline could not recover any details on the owner or group credentials of the files in the partition image [USBFD-64531026-RL-001-Fat16.img].
- Using another tool called “sorter”, from the forensic SleuthKit project, all the files were extracted from the partition image [USBFD-64531026-RL-001-Fat16.img] and sorted into file types. The unallocated (deleted) files were also extracted if possible. As the command “sorter” extracted each file, it calculated and recorded both the MD5 and a SHA1 hash. Similar to the previous mentioned command “file”, “sorter” tries to determine the type of file it has extracted, and sorts them into categories.

[Command Used]:- `sorter -md5 -sha1 -s -d ./output/sorter/ -f USBFD-64531026-RL-001-Fat16.img -m “d:”
./ USBFD-64531026-RL-001-Fat16.img`

[Files Extracted]:- 20 Files, (10 allocated, 10 unallocated)

[Categories of Extracted Files]:-

documents (3), exec (2), images (2), unknown (2)

[Files Skipped]:- 11 non-files

[Command Output]:- For full results see Appendix E

[Hash Calculations]:- For full results see Appendix F

Detail Analysis of executable found in Image

Using the data extracted from the previous steps, the analysis was able to focus on the executable found on the partition image on the USB Flashdrive [USBFD-64531026-RL-001].

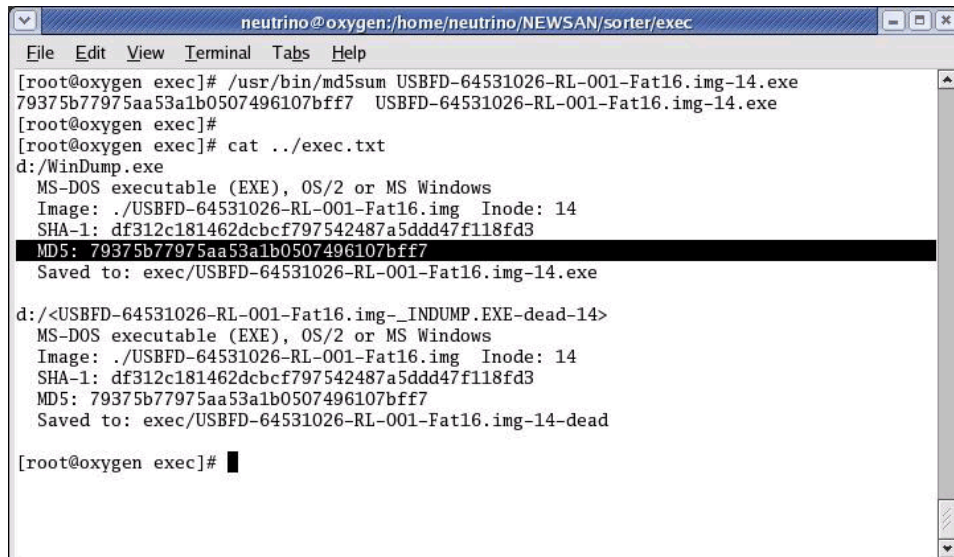
The following steps were followed to identify the unknown executables. As both the SHA1 and MD5 hash were the same for the two executables the tool “sorter” extracted (USBFD-64531026-RL-001-Fat16.img-14.exe and USBFD-64531026-RL-001-Fat16.img-14-dead), we can assume they are the same file. Also, we know that sorter extracted the data starting from the same inode (14) in the image (same starting point) for both executables.

- Using the file “USBFD-64531026-RL-001-Fat16.img-14.exe” created by the tool “sorter” previously the MD5 Hash was calculated. This was compared to the MD5 Hash calculated when the command “sorted” extracted the same program from the image earlier in the analysis.

[Command Used]:- `/usr/bin/md5sum USBFD-64531026-RL-001-Fat16.img-14.exe`

[MD5 Hash using md5sum]:- 79375b77975aa53a1b0507496107bff7

[MD5 Hash of Extracted with sorter]:- 79375b77975aa53a1b0507496107bff7



```

neutrino@oxygen:/home/neutrino/NEWSAN/sorter/exec
File Edit View Terminal Tabs Help
[root@oxygen exec]# /usr/bin/md5sum USBFD-64531026-RL-001-Fat16.img-14.exe
79375b77975aa53a1b0507496107bff7 USBFD-64531026-RL-001-Fat16.img-14.exe
[root@oxygen exec]#
[root@oxygen exec]# cat ../exec.txt
d:/WinDump.exe
MS-DOS executable (EXE), OS/2 or MS Windows
Image: ./USBFD-64531026-RL-001-Fat16.img Inode: 14
SHA-1: df312c181462dcbcf797542487a5ddd47f118fd3
MD5: 79375b77975aa53a1b0507496107bff7
Saved to: exec/USBFD-64531026-RL-001-Fat16.img-14.exe

d:/<USBFD-64531026-RL-001-Fat16.img-_INDUMP.EXE-dead-14>
MS-DOS executable (EXE), OS/2 or MS Windows
Image: ./USBFD-64531026-RL-001-Fat16.img Inode: 14
SHA-1: df312c181462dcbcf797542487a5ddd47f118fd3
MD5: 79375b77975aa53a1b0507496107bff7
Saved to: exec/USBFD-64531026-RL-001-Fat16.img-14-dead

[root@oxygen exec]#

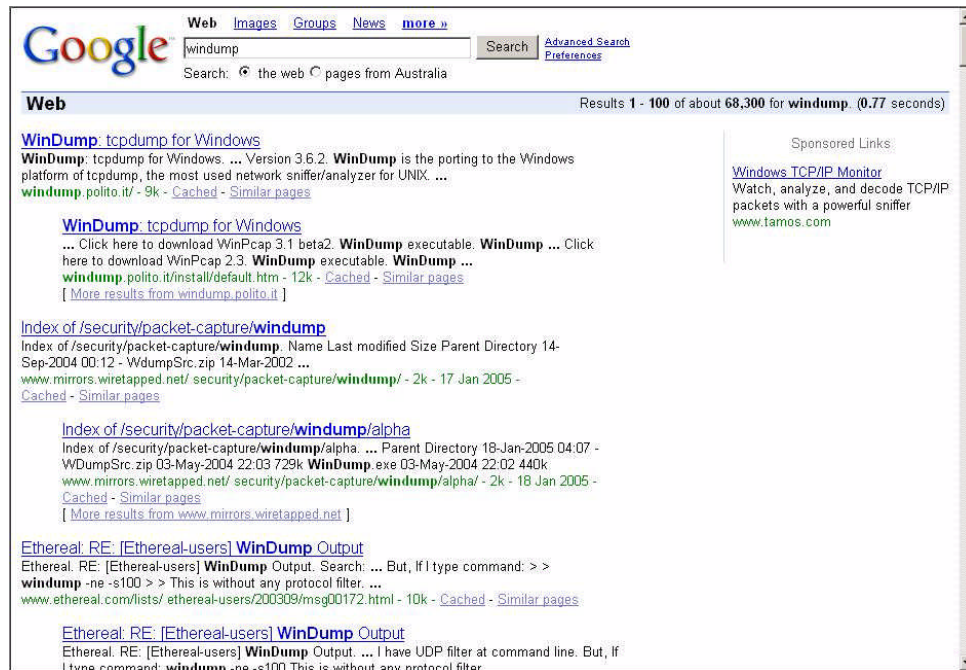
```

- Next, the standard Linux command “strings” was use to extract all ASCII character sequences from the program. The command “strings” steps through a data file of any type, and will print out any sequences of ASCII characters that it finds (ASCII characters includes the English alphabetic characters). On a program file, the use of the command “strings” may produce a list of useful search terms (keywords) that can be used to try identify the executable. This is because any output the executable is programed to supply to an end user when run, is stored in normal ASCII as part of the binary data for the file.

[Command Used]:- /usr/bin/strings USBFD-64531026-RL-001-Fat16.img-14.exe
[Lines produced]:- 8783

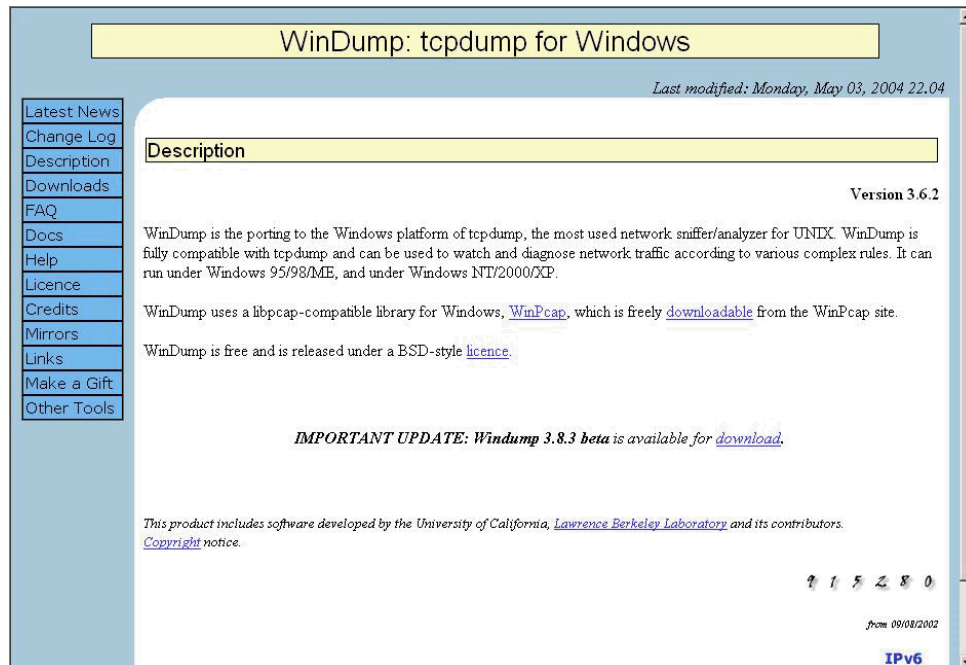
- The list of ASCII characters produced from running the “strings” command on the executable “USBFD-64531026-RL-001-Fat16.img-14.exe” was reviewed and the non-words removed. This left a sizeable list of 5943 lines.
- Reviewing the “string” list again, the following can be noted:-
 - 1) It contains a large number tcpdump headers. For example:
 ”@(#) \$Header: /tcpdump/master/tcpdump/addrtoname.c,v 1.96.2.6 2004/03/24 04:14:31 guy Exp \$ (LBL)
 @(#) \$Header: /tcpdump/master/tcpdump/bpf_dump.c,v 1.14.2.2 2003/11/16 08:51:04 guy Exp \$ (LBL)
 @(#) \$Header: /tcpdump/master/tcpdump/missing/datalinks.c,v 1.1.2.3 2003/11/16 09:29:48 guy Exp \$ (LBL)”
 - 2) It contains a large number of network protocol names. For example:
 ”Linux Classical IP-over-ATM
 DLT_ATM_CLIP
 BSD/OS PPP
 DLT_PPP BSDOS
 BSD/OS SLIP
 DLT_SLIP_BSDOS
 Raw IP”
 - 3) It contains the string “%s version %s, based on tcpdump version %s”
 - 4) contains the following strings that may be version numbers: 3.8.3 beta, 3.8.3, 0.8.1, 3.1 beta2
 - 5) Likely compiled after 28th April 2004 as the oldest tcpdump header reference is to
 ”/tcpdump/master/tcpdump/util.c,v 1. 87.2.4 2004/04/28 22:09:23 guy”

- From the previous forensic steps (MAC timeline and sorter), it is known that the executable was named WinDump on the USB Flashdrive [USBFD-64531026-RL-001].
- The next step in the investigation involved searching for information about the executable, called WinDump.exe in the partition image [USBFD-64531026-RL-001-Fat16.img], on the Internet. The web search engine Google was used initially to find terms relating to “WinDump”.

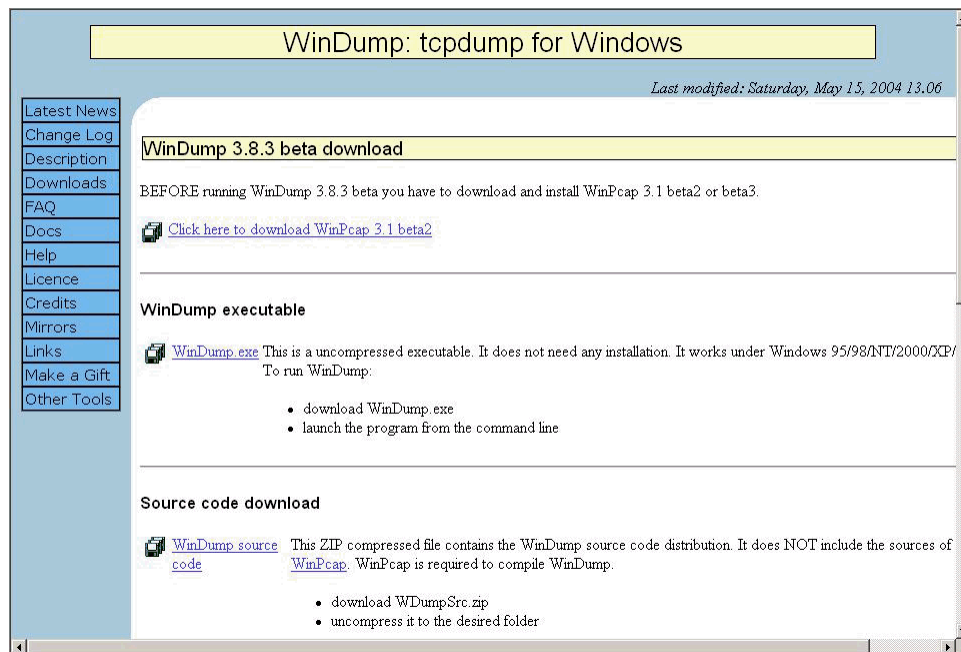


The first two websites found by Google mention WinDump and tcpdump. Interesting the second website returned by Google also listed the term “WinPcap 3.1 beta2” in the summary. We know that a file called “WinPcap_3_1_beta_3.exe” was deleted from the USB Flashdrive. The first two search results both reference the same website of <http://windump.polito.it>

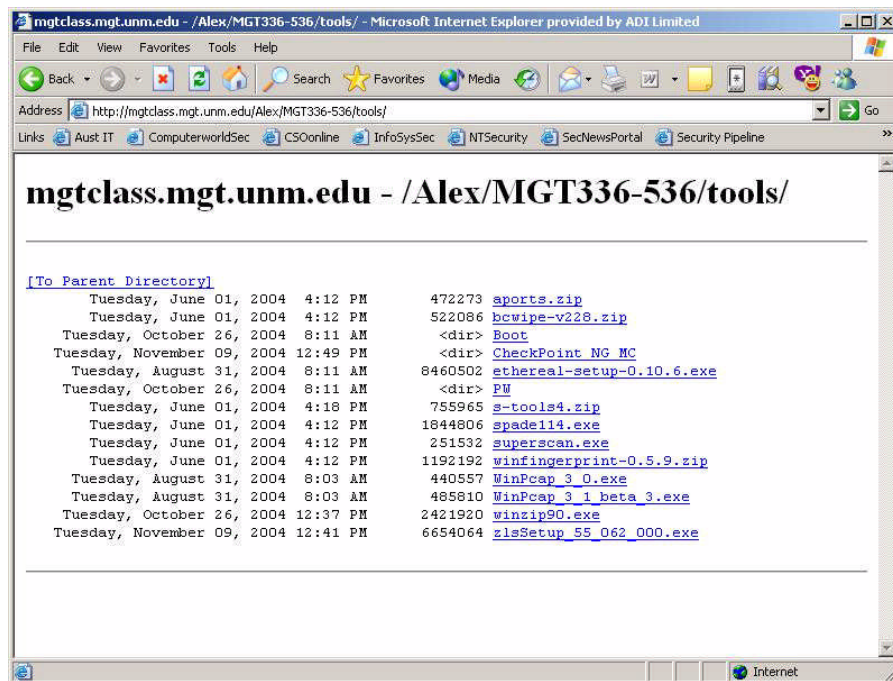
- The homepage for the website <http://windump.polito.it> explains that WinDump is a port of the program tcpdump. A “port” is a term used when a program is modified to run on a different operating system than it was originally programmed for.
- The website then explains that tcpdump is a network sniffer for the Unix environment. The term “sniffer” is used to describe a program that is able to monitor and/or record traffic that is flowing across a network.
- Therefore, WinDump is a network sniffer used to capture network traffic. The homepage also lists that WinDump was ported to run on the operation systems Microsoft Windows 95/98/ME/NT/2000/XP.



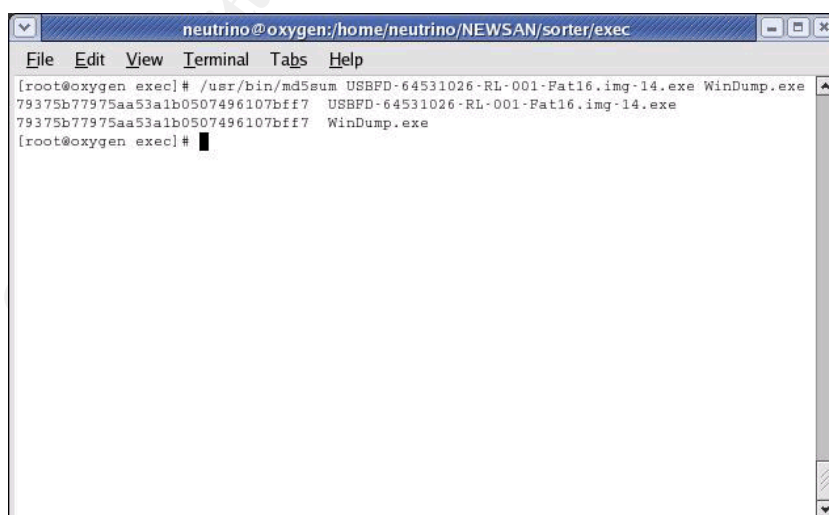
- The final bit of important information found on the homepage of <http://windump.polito.it> was the current version of WinDump. The webpage says that version 3.8.3 beta is available. This version corresponds with the string found in the "USBFD-64531026-RL-001-Fat16.img-14.exe" executable that was thought to be version numbers. The strings were: "3.8.3 beta" and "3.8.3".
- When the link to download the 3.8.3 beta version of WinDump was followed, we were directed to the second webpage that the Google search returned. This webpage tells the end user that before you can run the version 3.8.3 beta of WinDump, you must install WinPcap 3.1 beta2 or beta3. The term "3.1 beta2" is another string that was thought to be a version number when analysing the "USBFD-64531026-RL-001-Fat16.img-14.exe" executable in the partition image [USBFD-64531026-RL-001-Fat16.img].



- The program WinDump.exe was downloaded from the website <http://www.polito.it> to compare it against the executable [USBFD-64531026-RL-001-Fat16.img-14.exe] that was extracted from the partition image [USBFD-64531026-RL-001-Fat16.img].
- Reviewing the rest of the website <http://www.polito.it> we could not find a link to be able to download WinPcap_3_1_beta_3.exe which is the same filename as that found to be deleted from the USB Flashdrive. Therefore, the exact filename was entered into the Google website search engine to try find a copy of the file on the Internet. One of the webpages returned from Google was <http://mgtclass.mgt.unm.edu/Alex/MGT336-536/tools/>. This webpage was a directory listing of files, including the filename we were searching for. For further confirmation, the size of the link corresponding to the filename WinPcap_3_1_beta_3.exe was 485810. This was the same filesize that was still recorded in the data recovered from the USB Flashdrive for the corresponding file. The file was downloaded from the website to help with the analysis of the USB Flashdrive image [USBFD-64531026-RL-001.img].



- The two files, WinDump.exe and WinPcap_3_1_beta_3.exe, were recorded onto a CD-R. The CD-R was used to copy the programs into the Fedora2 Linux and Microsoft Windows 2000 VMWare environments for analysis. Using a CD-R ensured that files on the CD could not be modified once they were recorded.
- In the Fedora2 Linux environment the md5sum program was used to calculate the MD5 Hash for the downloaded WinDump.exe. The MD5 Hash was found to match the MD5 Hash of the extracted executable from the partition image [USBFD-64531026-RL-001-Fat16.img]. This means the version of WinDump.exe that was downloaded from the Internet was the same file that was stored on the USB Flashdrive.



- The two executables were there transferred into the Microsoft

Windows 2000 VMWare environment.

- The installation instructions on the website <http://www.polito.it> specified that package WinPcap had to be installed prior to the WinDump program being used.
- The WinPcap_3_1_beta_3.exe package was installed by executing the file. To monitor any changes that occur in Windows 2000 environment a program called Winalysis (Version 3) was used. The Winalysis program will take a “snapshot” of the operating system environment. This snapshot can be used in the future (e.g. after an installation) as a comparison to determine what changes had taken place.

[Winalysis Output]:- For full results see Appendix G

- The installation of WinPcap caused 4 files (packet.dll, pthreadvc.dll, wanpacket.dll and wpcap.dll) to be installed in the directory c:\winnt\system32. The c:\winnt directory is where the main operating system files/programs are stored in the Windows 2000 VMWare environment.
- The Windows 2000 registry was also modified by the installation of WinPcap. Windows uses its registry as a central point for storing parameters and their values that can be used by the operating system or programs running in the operating system environment. The full log of registry changes is listed in the appendix.
- Also part of the installation of WinPcap, was the introduction of two new drivers (“NetGroup Packet Filter Driver” and “Network Monitor Driver”). Along with these drivers a new service (“Remote Packet Capture Protocol v0 (experimental)”) was installed and activated.
- Following the installation of WinPcap we ran the WinDump.exe program. The Winalysis program was used again to monitor any system changes. However, the WinDump.exe program did not modify any files or services. It did make small registry changes during its execution. The parameters that were changed were:-

HKLM\SOFTWARE\Microsoft\Cryptography\ RNG – [Key Last Modified Date]
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\seed

- The WinDump.exe program was first run with the command switch of “-h”. This produced a usage help instruction on what all the command switches were available for WinDump.exe. The instruction also shows what information is required for the program to run correctly.

```

Select C:\WINNT\System32\CMD.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>windump -h
windump version 3.8.3 beta, based on tcpdump version 3.8.3
WinPcap version 3.1 beta3 (packet.dll version 3.1.0.23), based on libpcap ver
sion 0.8.1
Usage: windump [-aAddDeflLnNOpgRStuUvxX] [-B size] [-c count] [-C file_size]
               [-E algo:secret] [-F file] [-i interface] [-r file]
               [-s snaplen] [-T type] [-w file] [-y datalinktype]
               [expression]

C:\>_

```

- From the previous step, it was found that WinDump.exe does not require any additional options or arguments on the command line to execute correctly. Therefore, we ran WinDump.exe without any arguments. This showed that the WinDump.exe does monitor all network traffic.

```

C:\WINNT\System32\CMD.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>windump -h
windump version 3.8.3 beta, based on tcpdump version 3.8.3
WinPcap version 3.1 beta3 (packet.dll version 3.1.0.23), based on libpcap ver
sion 0.8.1
Usage: windump [-aAddDeflLnNOpgRStuUvxX] [-B size] [-c count] [-C file_size]
               [-E algo:secret] [-F file] [-i interface] [-r file]
               [-s snaplen] [-T type] [-w file] [-y datalinktype]
               [expression]

C:\>windump
windump: listening on \Device\NPF_{...}GenericNdisWanAdapter
07:23:01.531250 c4:64:20:52:41:53 802.1b-gsap > 03:00:00:00:00:02 802.1b-isap ui
/C len=180
07:23:11.546875 c4:64:20:52:41:53 802.1b-gsap > 03:00:00:00:00:02 802.1b-isap ui
/C len=180

2 packets captured
2 packets received by filter
0 packets dropped by kernel
-

```

- From the MAC time analysis of the partition image [USBFD-64531026-RL-001-Fat16.img] we can see that the WinDump.exe program was accessed a number of time. When a program is showed to be accessed, it corresponds to an end-user running the program. This means that we know that the end-user of the USB Flashdrive [USBFD-64531026-RL-001] was running the WinDump.exe program at these times:-

- 1) Wed Oct 27 2004 00:00:00
- 2) Thu Oct 28 2004 00:00:00

- One of the abilities of the WinDump program is to store all monitored traffic into a file. This is done by:-

[Command Needed]:- WinDump.exe -w <filename>

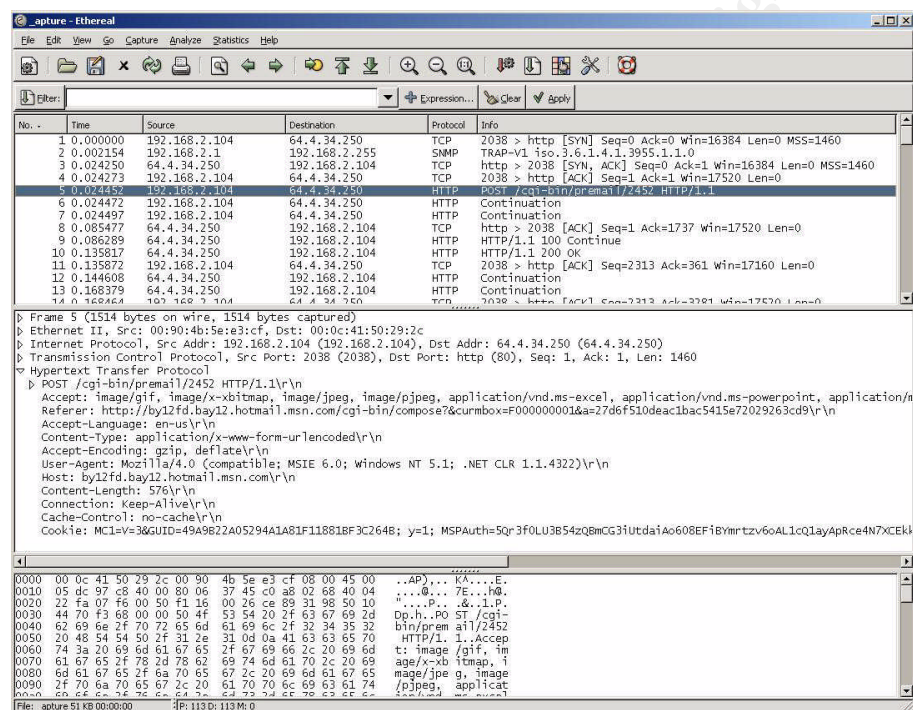
In the analysis of the partition image [USBFD-64531026-RL-001-

Fat16.img] a file “_apture” was found to have been deleted. This file was also recognized by the SleuthKit tool “sorter” as being a tcpdump capture file.

- The “icat” utility from the SleuthKit project was used to extract the deleted file “_apture” from the partition image [USBFD-64531026-RL-001-Fat16.img].

[Command]:- icat -r -f fat16 USBFD-64531026-RL-001-Fat16.img 15 > _apture

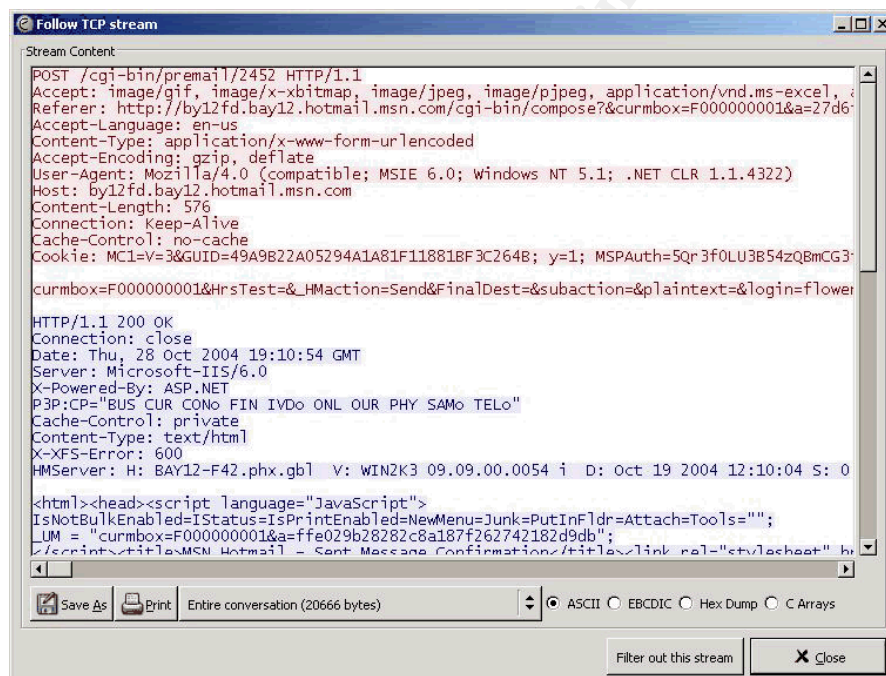
- A graphical interface that is able to read and display tcpdump capture files was used to analyse the file “_apture”. The program that provided the graphical interface was called “Ethereal” (Version 0.10.5a).



- The Ethereal program has many added features to enable the end-user to better analyse capture network traffic, rather than just view it. One of these features automatically sorts capture data packets into conversations between two computers. This feature was used to analyse the web conversations that could be seen in the capture data.

Address A	Port A	Address B	Port B	Packets	Bytes	-> Packets	-> Bytes	<- Packets	<- Bytes
192.168.2.104	2038	64.4.34.250	80	16	22578	16	3232	18	19346
192.168.2.104	2039	207.68.178.1	80	8	7764	8	4013	10	3751
192.168.2.104	2040	207.68.178.1	80	6	5365	6	2716	7	2649
192.168.2.104	2042	63.209.188.6	80	6				6	3774
192.168.2.104	2045	216.73.86.40	80	5				5	4411
192.168.2.104	2041	207.68.177.1	80	3				3	560
192.168.2.104	2043	63.209.188.62	80	3				3	1307
192.168.2.104	2044	216.73.86.40	80	2	178	2		1	62
192.168.2.104	2046	63.166.13.75	80	1	62	1		0	0

- For each web conversation found, the associated data packet was found in the file “_apture”, and another Ethereal feature (Follow TCP Stream) was used to display the conversations.



- On reviewing the conversations, we found that one of the conversations was an end-user posting an email to hotmail. The key HTML (web language) data is show below with important information bolded:-

```
curmbox=F000000001&HrsTest=&_HMAction=Send&FinalDest=&subaction=&plaintext=&login=flowerg
ir196&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&msgid=b16479b18bee
c291196189c78555223c_1098692452&RTebgcolor=&encodedto=SamGuarillo@hotmail.com&encode
dcc=&encodedbcc=&deleteUponSend=0&importance=&sigflag=&newmail=new&to=SamGuarillo@hotm
ail.com&cc=&bcc=&subject=RE%3Acoffee&body=Sure%2C+coffee+sounds+great.++Let%27s+mee
t+at+the+coffee+shop+on+the+corner+Hollywood+and+McCadden.++It%27s+a+nice+out+of+the+w
ay+spot.%0D%0A%0D%0ASee+you+at+7pm%21%0D%0A%0D%0A-LeilaHTTP/1.1 100 Continue
```

From this data we can see that:

- 1) flowergirl96@hotmail.com (from login= fields) sent an email
- 2) to SamGuarillo@hotmail.com (from encodedto= and to= fields)
- 3) with the Subject of "**Re:A coffee**" (from subject= field) and
- 4) a body (from body= field) of "**Sure, coffee sounds great. Let's meet at the coffee shop on the corner Hollywood and McCadden. It's a nice out of the way spot. See you at 7pm!-Leila**"

Other Forensic Evidence Found

While analyzing the contents of the USB Flashdrive [USBFD-64531026-RL-001.img] provided there were other files found other than the executables. The analysis of these files shows the following:-

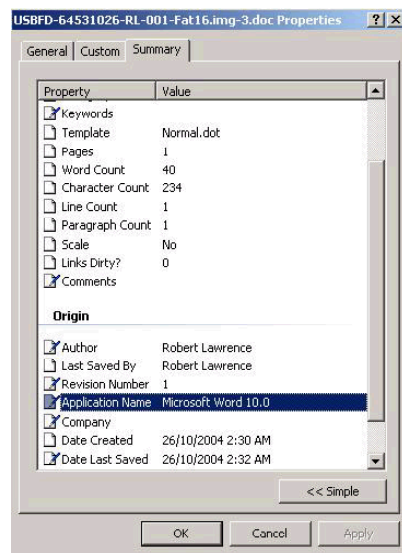
- There are three documents stored in the USB Flashdrive [USBFD-64531026-RL-001]. The three documents were examined using the Unix command "strings". In each of the documents it was the term "Microsoft Word 10.0" was found. This tells us that the documents were created in the Microsoft Word program that came with the Microsoft Office 2002 Suite.
- The first document, in chronological order, on the USB Flashdrive [USBFD-64531026-RL-001] was name "her.doc". The contents of the document were:

Hey I saw you the other day. I tried to say "hi", but you disappeared??? That was a nice blue dress you were wearing. I heard that your car was giving you some trouble. Maybe I can give you a ride to work sometime, or maybe we can get dinner sometime?

Have a nice day

Using Windows Explorer, a copy of the document that was extracted previously using the SleuthKit "sorter" tool was examined. The properties of the documents were review by selecting the document and using the right mouse button to select Properties. The Summary tab was chosen and then the Advance button clicked. This provided us with the following information on the document "her.doc":-

[Title]:- Hey I saw you the other day
[Author]:- Robert Lawrence
[Last Saved By]:- Robert Lawrence
[Application Name]:- Microsoft Word 10.0
[Date Created]:- 26/10/2004 2:30 AM
[Date Last Saved]:- 26/10/2004 2:32 AM



- The second document on the USB Flashdrive [USBFD-64531026-RL-001] was named "hey.doc". The contents of this document were:

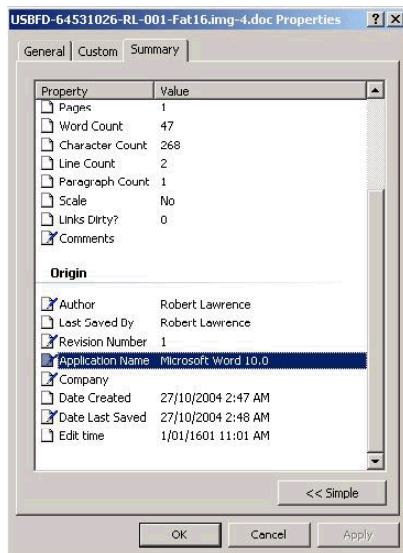
Hey! Why are you being so mean? I was just offering to help you out with your car! Don't tell me to get lost! You should give me a chance. I'm a nice guy just trying to help you out, just because I think you're cute doesn't mean I'm weird. Perhaps coffee would be better, when would be a good time for you?

Using the same procedure as the previous file, the properties of the document was analysed and the following information was found:-

[Title]:- Hey
[Author]:- Robert Lawrence
[Last Saved By]:- Robert Lawrence
[Application Name]:- Microsoft Word 10.0
[Date Created]:- 27/10/2004 2:47 AM
[Date Last Saved]:- 27/10/2004 2:48 AM

- The last document found on the USB Flashdrive [USBFD-64531026-RL-001] was named "coffee.doc". The contents of this document were:

Hey what gives? I was drinking a coffee on thursday and saw you stop buy with some guy! You said you didn't want coffee with me, but you'll go have it with some random guy??? He looked like a loser! Guys like that are nothing but trouble. I can't believe you did this to me! You should stick to your word, if you're not interested in going to coffee with me then you shouldn't be going with anyone! I heard rumors about a "bad batch" of

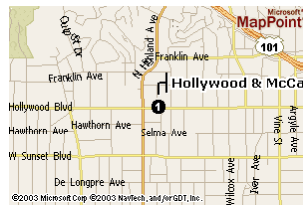
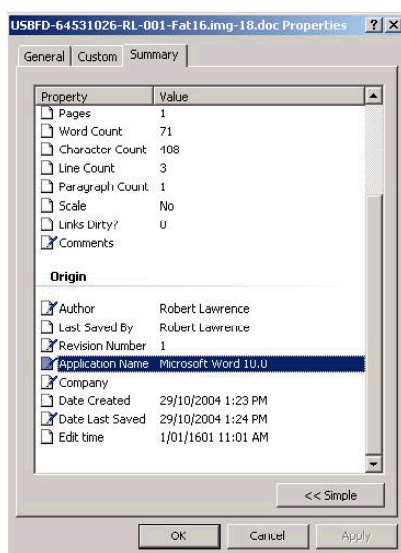


coffee, hope you don't get any...

Using the same procedure as the previous file, the properties of the document was analysed and the following information was found:-

[Title]:- Hey what gives
[Author]:- Robert Lawrence
[Last Saved By]:- Robert Lawrence
[Application Name]:- Microsoft Word 10.0
[Date Created]:- 29/10/2004 1:23 PM
[Date Last Saved]:- 29/10/2004 1:24 PM

-
- The last file that was able to be recovered from the USB Flashdrive image [USBFD-64531026-RL-001.img] was a GIF89a formatted image. The image named found during the analysis was _ap.gif. The use of an underscore character at the beginning of the name suggests that it was deleted in a Windows based system. In Windows, when you delete a file, it just renames the file from the original by replacing the first letter with an underscore. Recovery of the data was automatically done during the previous analysis work when the SleuthKit tool “sorter” was used. The image recovered is shown below.



References

Brian Carter, “The Sleuth Kit”, version 1.73, 3 November 2004, URL: <http://www.sleuthkit.org/sleuthkit/desc.php>

University of California, Lawrence Berkeley Laboratory, “WinDump”, version 3.8.3 beta, 3 May 2004, URL: <http://windump.polito.it/> (3 May 2004)

University of California, Lawrence Berkeley Laboratory, “WinPcap”, version 3.1 beta 3, 4 November 2004, URL: <http://winpcap.polito.it/default.htm> (4 November 2004)

“tcpdump/libpcap”, URL: <http://www.tcpdump.org> (22 June 2004)

Australian Commonwealth Government, "Crimes Act 1914", Attorney
Generals Department, Canberra, prepared 6 July 2004

Australian Commonwealth Government, "Telecommunications Act 1997",
Attorney Generals Department, Canberra, prepared 1 November 2004

Winalysis Software Inc., "Winalysis", version 3.0, 1 August 2002, URL: [http://
www.winalysis.com](http://www.winalysis.com)

Albion Research Ltd, "The URLEncode and URLDecode Page", URL:
<http://www.albionresearch.com/misc/urlencode.php> (24 January 2005)

© SANS Institute 2005, Author retains full rights.

Appendix A – Output of “fsstat” command

```
FILE SYSTEM INFORMATION
-----
File System Type: FAT

OEM Name: MSWIN4.1
Volume ID: 0x0
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT16

Sectors before file system: 32

File System Layout (in sectors)
Total Range: 0 - 121918
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 0: 1 - 239
* FAT 1: 240 - 478
* Data Area: 479 - 121918
** Root Directory: 479 - 510
** Cluster Area: 511 - 121918

METADATA INFORMATION
-----
Range: 2 - 1942530
Root Directory: 2

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 1024
Total Cluster Range: 2 - 60705

FAT CONTENTS (in sectors)
-----
511-550 (40) -> EOF
551-590 (40) -> EOF
591-630 (40) -> EOF
```

Appendix B – Output of the “fls” command for MAC time creation

```
0|d:/her.doc|0|3|33279|-/-rwxxrwxrwx|1|0|0|0|19968|1098626400|1098657128|1098657126|512|0
0|d:/hey.doc|0|4|33279|-/-rwxxrwxrwx|1|0|0|0|19968|1098712800|1098744490|1098744486|512|0
0|d:/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)|0|7|33279|-/-rwxxrwxrwx|0|0|0|0|1098799200|1098858236|1098858234|512|0
0|d:/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)|0|10|33279|-/-rwxxrwxrwx|0|0|0|0|485810|1098885600|1098858230|1098858234|512|0
0|d:/WinDump.exe (_INDUMP.EXE) (deleted)|0|12|33279|-/-rwxxrwxrwx|0|0|0|0|1098799200|1098858246|1098858244|512|0
0|d:/WinDump.exe (_INDUMP.EXE) (deleted)|0|14|33279|-/-rwxxrwxrwx|0|0|0|0|450560|1098885600|1098858242|1098858244|512|0
0|d:/_apture (deleted)|0|15|33279|-/-rwxxrwxrwx|0|0|0|0|53056|1098885600|1098925860|1098925704|512|0
0|d:/_ap.gif (deleted)|0|16|33279|-/-rwxxrwxrwx|0|0|0|0|1098885600|1098926266|1098926264|512|0
0|d:/_ap.gif (deleted)|0|17|33279|-/-rwxxrwxrwx|0|0|0|0|8814|1098885600|1098926266|1098926264|512|0
0|d:/coffee.doc|0|18|33279|-/-rwxxrwxrwx|1|0|0|0|19968|1098885600|1098955488|1098955486|512|0
```

Appendix C – Output of the “ils” command for MAC time creation

```
0|<USBFD-64531026-RL-001-Fat16.img-_INPCA~1.EXE-dead-7>|0|7|33279|-rwxxrwxrwx|0|0|0|0|1098799200|1098858236|1098858234|512|0
0|<USBFD-64531026-RL-001-Fat16.img-_INPCA~1.EXE-dead-10>|0|10|33279|-rwxxrwxrwx|0|0|0|0|485810|1098885600|1098858230|1098858234|512|0
0|<USBFD-64531026-RL-001-Fat16.img-_INDUMP.EXE-dead-12>|0|12|33279|-rwxxrwxrwx|0|0|0|0|1098799200|1098858246|1098858244|512|0
0|<USBFD-64531026-RL-001-Fat16.img-_INDUMP.EXE-dead-14>|0|14|33279|-rwxxrwxrwx|0|0|0|0|450560|1098885600|1098858242|1098858244|512|0
0|<USBFD-64531026-RL-001-Fat16.img-_apture-dead-15>|0|15|33279|-rwxxrwxrwx|0|0|0|0|53056|1098885600|1098925860|1098925704|512|0
0|<USBFD-64531026-RL-001-Fat16.img-_ap.gif-dead-16>|0|16|33279|-rwxxrwxrwx|0|0|0|0|1098885600|1098926266|1098926264|512|0
0|<USBFD-64531026-RL-001-Fat16.img-_ap.gif-dead-17>|0|17|33279|-rwxxrwxrwx|0|0|0|0|8814|1098885600|1098926266|1098926264|512|0
```

Appendix D – Output of the “mactime” command to reformat MAC time output

Mon Oct 25 2004 00:00:00	19968 .a. -/-rwxrwxrwx	0	3	d:/her.doc
Mon Oct 25 2004 08:32:06	19968 .c -/-rwxrwxrwx	0	3	d:/her.doc
Mon Oct 25 2004 08:32:08	19968 m.. -/-rwxrwxrwx	0	3	d:/her.doc
Tue Oct 26 2004 00:00:00	19968 .a. -/-rwxrwxrwx	0	4	d:/hey.doc
Tue Oct 26 2004 08:48:06	19968 .c -/-rwxrwxrwx	0	4	d:/hey.doc
Tue Oct 26 2004 08:48:10	19968 m.. -/-rwxrwxrwx	0	4	d:/hey.doc
Wed Oct 27 2004 00:00:00	450560 .a. -/-rwxrwxrwx	0	12	d:/WinDump.exe (_INDUMP.EXE) (deleted)
	0 .a. -rwxrwxrwx	0	7	<USBFD-64531026-RL-001-Fat16.img-_INPCA~1.EXE-dead-7>
	0 .a. -rwxrwxrwx	0	12	<USBFD-64531026-RL-001-Fat16.img-_INDUMP.EXE-dead-12>
	485810 .a. -/-rwxrwxrwx	0	7	d:/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:23:50	485810 m.. -/-rwxrwxrwx	0	10	d:/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
	485810 m.. -rwxrwxrwx	0	10	<USBFD-64531026-RL-001-Fat16.img-_INPCA~1.EXE-dead-10>
Wed Oct 27 2004 16:23:54	0 .c -rwxrwxrwx	0	7	<USBFD-64531026-RL-001-Fat16.img-_INPCA~1.EXE-dead-7>
	485810 .c -/-rwxrwxrwx	0	10	d:/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
	485810 .c -/-rwxrwxrwx	0	7	d:/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
	485810 .c -rwxrwxrwx	0	10	<USBFD-64531026-RL-001-Fat16.img-_INPCA~1.EXE-dead-10>
Wed Oct 27 2004 16:23:56	0 m.. -rwxrwxrwx	0	7	<USBFD-64531026-RL-001-Fat16.img-_INPCA~1.EXE-dead-7>
	485810 m.. -/-rwxrwxrwx	0	7	d:/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:24:02	450560 m.. -rwxrwxrwx	0	14	<USBFD-64531026-RL-001-Fat16.img-_INDUMP.EXE-dead-14>
	450560 m.. -/-rwxrwxrwx	0	14	d:/WinDump.exe (_INDUMP.EXE) (deleted)
Wed Oct 27 2004 16:24:04	450560 .c -rwxrwxrwx	0	14	<USBFD-64531026-RL-001-Fat16.img-_INDUMP.EXE-dead-14>
	0 .c -rwxrwxrwx	0	12	<USBFD-64531026-RL-001-Fat16.img-_INDUMP.EXE-dead-12>
	450560 .c -/-rwxrwxrwx	0	14	d:/WinDump.exe (_INDUMP.EXE) (deleted)
	450560 .c -/-rwxrwxrwx	0	12	d:/WinDump.exe (_INDUMP.EXE) (deleted)
Wed Oct 27 2004 16:24:06	450560 m.. -/-rwxrwxrwx	0	12	d:/WinDump.exe (_INDUMP.EXE) (deleted)
	0 m.. -rwxrwxrwx	0	12	<USBFD-64531026-RL-001-Fat16.img-_INDUMP.EXE-dead-12>
Thu Oct 28 2004 00:00:00	19968 .a. -/-rwxrwxrwx	0	18	d:/coffee.doc
	8814 .a. -rwxrwxrwx	0	17	<USBFD-64531026-RL-001-Fat16.img-_ap.gif-dead-17>
	53056 .a. -rwxrwxrwx	0	15	<USBFD-64531026-RL-001-Fat16.img-_apture-dead-15>
	53056 .a. -/-rwxrwxrwx	0	15	d:/_apture (deleted)
	8814 .a. -/-rwxrwxrwx	0	16	d:/_ap.gif (deleted)
	450560 .a. -/-rwxrwxrwx	0	14	d:/WinDump.exe (_INDUMP.EXE) (deleted)
	8814 .a. -/-rwxrwxrwx	0	17	d:/_ap.gif (deleted)
	485810 .a. -rwxrwxrwx	0	10	<USBFD-64531026-RL-001-Fat16.img-_INPCA~1.EXE-dead-10>
	485810 .a. -/-rwxrwxrwx	0	10	d:/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
	450560 .a. -rwxrwxrwx	0	14	<USBFD-64531026-RL-001-Fat16.img-_INDUMP.EXE-dead-14>
	0 .a. -rwxrwxrwx	0	16	<USBFD-64531026-RL-001-Fat16.img-_ap.gif-dead-16>
Thu Oct 28 2004 11:08:24	53056 .c -rwxrwxrwx	0	15	<USBFD-64531026-RL-001-Fat16.img-_apture-dead-15>
	53056 .c -/-rwxrwxrwx	0	15	d:/_apture (deleted)
Thu Oct 28 2004 11:11:00	53056 m.. -/-rwxrwxrwx	0	15	d:/_apture (deleted)
	53056 m.. -rwxrwxrwx	0	15	<USBFD-64531026-RL-001-Fat16.img-_apture-dead-15>
Thu Oct 28 2004 11:17:44	0 .c -rwxrwxrwx	0	16	<USBFD-64531026-RL-001-Fat16.img-_ap.gif-dead-16>
	8814 .c -/-rwxrwxrwx	0	16	d:/_ap.gif (deleted)
	8814 .c -/-rwxrwxrwx	0	17	d:/_ap.gif (deleted)
	8814 .c -rwxrwxrwx	0	17	<USBFD-64531026-RL-001-Fat16.img-_ap.gif-dead-17>
Thu Oct 28 2004 11:17:46	0 m.. -rwxrwxrwx	0	16	<USBFD-64531026-RL-001-Fat16.img-_ap.gif-dead-16>
	8814 m.. -rwxrwxrwx	0	17	<USBFD-64531026-RL-001-Fat16.img-_ap.gif-dead-17>

	8814	m..	-/-rwxrwxrwx	0	0	16	d:/_ap.gif (deleted)
	8814	m..	-/-rwxrwxrwx	0	0	17	d:/_ap.gif (deleted)
Thu Oct 28 2004 19:24:46	19968	..c	-/-rwxrwxrwx	0	0	18	d:/coffee.doc
Thu Oct 28 2004 19:24:48	19968	m..	-/-rwxrwxrwx	0	0	18	d:/coffee.doc

© SANS Institute 2005, Author retains full rights.

Appendix E – Output of the “sorter” command

```
Images
- ./USBFD-64531026-RL-001-Fat16.img

Files (20)
- Allocated (10)
- Unallocated (10)

Files Skipped (11)
- Non-Files (11)
- 'ignore' category (0)

Extensions
- Extension Mismatches (0)

Categories (9)
- archive (0)
- audio (0)
- compress (0)
- crypto (0)
- data (0)
- disk (0)
- documents (3)
- exec (2)
- images (2)
- system (0)
- text (0)
- unknown (2)
- video (0)
```

Appendix F – Hash calculations from the running of the “sorter” command.

Documents:-

```
d:/her.doc
Microsoft Office Document
Image: ./USBFD-64531026-RL-001-Fat16.img Inode: 3
SHA-1: 3bd04282d18f99a30267ef95fbc9fe7c923068f6
MD5: 9785a777c5286738f9deb73d8bc57978
Saved to: documents/USBFD-64531026-RL-001-Fat16.img-3.doc
```

```
d:/hey.doc
Microsoft Office Document
Image: ./USBFD-64531026-RL-001-Fat16.img Inode: 4
SHA-1: 1b9bb523410406485e3321b1d93e65f497b6fe2d
MD5: ca601d4f8138717dca4de07a8ec19ed1
Saved to: documents/USBFD-64531026-RL-001-Fat16.img-4.doc
```

```
d:/coffee.doc
Microsoft Office Document
Image: ./USBFD-64531026-RL-001-Fat16.img Inode: 18
SHA-1: 18b50dfadd3c2e24fbc4a398f70566ab309e958a
MD5: a833c58689596eda15a27c931e0c76d1
Saved to: documents/USBFD-64531026-RL-001-Fat16.img-18.doc
```

Exec:-

```
d:/WinDump.exe
MS-DOS executable (EXE), OS/2 or MS Windows
Image: ./USBFD-64531026-RL-001-Fat16.img Inode: 14
SHA-1: df312c181462dcbcf797542487a5ddd47f118fd3
MD5: 79375b77975aa53a1b0507496107bff7
Saved to: exec/USBFD-64531026-RL-001-Fat16.img-14.exe
```

```
d:/<USBFD-64531026-RL-001-Fat16.img- INDUMP.EXE-dead-14>
MS-DOS executable (EXE), OS/2 or MS Windows
Image: ./USBFD-64531026-RL-001-Fat16.img Inode: 14
SHA-1: df312c181462dcbcf797542487a5ddd47f118fd3
MD5: 79375b77975aa53a1b0507496107bff7
Saved to: exec/USBFD-64531026-RL-001-Fat16.img-14-dead
```

Images:-

```
d:/_ap.gif
GIF image data, version 89a, 300 x 200
Image: ./USBFD-64531026-RL-001-Fat16.img Inode: 17
SHA-1: 4301b120a91fe66f19af80d9984203cdf57a2470
MD5: 9bc3923cf8e72fd405d7cea8c8781011
Saved to: images/USBFD-64531026-RL-001-Fat16.img-17.gif
```

```
d:/<USBFD-64531026-RL-001-Fat16.img-_ap.gif-dead-17>
GIF image data, version 89a, 300 x 200
Image: ./USBFD-64531026-RL-001-Fat16.img Inode: 17
SHA-1: 4301b120a91fe66f19af80d9984203cdf57a2470
MD5: 9bc3923cf8e72fd405d7cea8c8781011
Saved to: images/USBFD-64531026-RL-001-Fat16.img-17-dead
```

Unknown:-

```
d:/_apture
tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 4096)
Image: ./USBFD-64531026-RL-001-Fat16.img Inode: 15
```

```
d:/<USBFD-64531026-RL-001-Fat16.img-_apture-dead-15>
tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 4096)
```

Image: ./USBFD-64531026-RL-001-Fat16.img Inode: 15

Appendix G – Output from Winalysis when installing WinPcap

Changes on \\WINFORENSICS
(All Changes -- No Severity Filters)

Changes from Snapshot Summary

Name

Files

Groups

RegistryRRights 0

Scheduler 0

Services 3

Shares 0

System 0

Users 0

Volumes 0

Changes from Snapshot Summary for Files

Snapshot:

Tested:

Name

C:

C:\WINNT\System32\oredshot

Changes from Snapshot Details for Files

Snapshot:

Tested:

Name

C:\WINNT\System32\packet.dll

New File

C:\WINNT\System32\pthreadVC.dll

New File

C:\WINNT\System32\wanpacket.dll

New File

C:\WINNT\System32\wpcap.dll

New File

Changes from Snapshot Summary for Registry

Snapshot:a01/18/05 10:57:09Tested: 01/18/05 10:59:18

Name

HKLM\

Changes from Snapshot Details for Registry

Snapshot:

Tested:

Name

HKLM\SYSTEM\CurrentControlSet\Services

HKLM\SYSTEM\CurrentControlSet\Services\nm
HKLM\SYSTEM\CurrentControlSet\Services\nm\Type
HKLM\SYSTEM\CurrentControlSet\Services\nm\Start
HKLM\SYSTEM\CurrentControlSet\Services\nm>ErrorControl
HKLM\SYSTEM\CurrentControlSet\Services\nm\ImagePath
HKLM\SYSTEM\CurrentControlSet\Services\nm\DisplayName
HKLM\SYSTEM\CurrentControlSet\Services\nm\Security
HKLM\SYSTEM\CurrentControlSet\Services\nm\Security\Security
HKLM\SYSTEM\CurrentControlSet\Services\nm\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\nm\Linkage
HKLM\SYSTEM\CurrentControlSet\Services\nm\Linkage\Bind
HKLM\SYSTEM\CurrentControlSet\Services\nm\Linkage\Route
HKLM\SYSTEM\CurrentControlSet\Services\nm\Linkage\Export

HKLM\SYSTEM\CurrentControlSet\Services\NPF
HKLM\SYSTEM\CurrentControlSet\Services\NPF\Type
HKLM\SYSTEM\CurrentControlSet\Services\NPF\Start
HKLM\SYSTEM\CurrentControlSet\Services\NPF>ErrorControl
HKLM\SYSTEM\CurrentControlSet\Services\NPF\ImagePath
HKLM\SYSTEM\CurrentControlSet\Services\NPF\DisplayName
HKLM\SYSTEM\CurrentControlSet\Services\NPF\Security
HKLM\SYSTEM\CurrentControlSet\Services\NPF\Security\Security

HKLM\SYSTEM\CurrentControlSet\Services\rpcapd
HKLM\SYSTEM\CurrentControlSet\Services\rpcapd\Type
HKLM\SYSTEM\CurrentControlSet\Services\rpcapd\Start
HKLM\SYSTEM\CurrentControlSet\Services\rpcapd>ErrorControl
HKLM\SYSTEM\CurrentControlSet\Services\rpcapd\ImagePath
HKLM\SYSTEM\CurrentControlSet\Services\rpcapd\DisplayName
HKLM\SYSTEM\CurrentControlSet\Services\rpcapd\ObjectName
HKLM\SYSTEM\CurrentControlSet\Services\rpcapd>Description
HKLM\SYSTEM\CurrentControlSet\Services\rpcapd\Security
HKLM\SYSTEM\CurrentControlSet\Services\rpcapd\Security\Security

HKLM\SYSTEM\CurrentControlSet\Services\NdisWan\Enum
HKLM\SYSTEM\CurrentControlSet\Services\NdisWan\Enum\Count
HKLM\SYSTEM\CurrentControlSet\Services\NdisWan\Enum\NextInstance

```
HKLM\SYSTEM\CurrentControlSet\Services\NdisWan\Enum\1
HKLM\SYSTEM\CurrentControlSet\Services\NdisTapi\Enum
HKLM\SYSTEM\CurrentControlSet\Services\NdisTapi\Enum\Count
HKLM\SYSTEM\CurrentControlSet\Services\NdisTapi\Enum\NextInstance
HKLM\SYSTEM\CurrentControlSet\Services\NdisTapi\Enum\2
```

```
HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current\System\CurrentControlSet\Enum\ROOT
HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current\System\CurrentControlSet\Enum\ROOT\MS_NDISWANBH
HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current\System\CurrentControlSet\Enum\ROOT\MS_NDISWANBH\0000
```

```
HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\0001\System\CurrentControlSet\Enum\ROOT
HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\0001\System\CurrentControlSet\Enum\ROOT\MS_NDISWANBH
HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\0001\System\CurrentControlSet\Enum\ROOT\MS_NDISWANBH\0000
```

```

HKLM\SYSTEM\CurrentControlSet\Enum\Root
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\ClassGUID      New Value      {4D36E972-E325-11CE-B C1-08002BE10318}
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\Class          New Value      Net
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\HardwareID      New Value      ms_ndiswanbh
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\Driver          New Value      {4D36E972-E325-11CE-B C1-08002BE10318}\0006
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\LowerFilters    New Value      NdisTapi
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\Mfg             New Value      Microsoft
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\Service         New Value      NdisWan
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\DeviceDesc      New Value      WAN Miniport (Network Monitor)
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\ConfigFlags     New Value      0
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\Capabilities    New Value      0
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\Control         New Key
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\Control\DeviceReference New Value      -2124777968
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\LogConf         New Key
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\Device Parameters New Key
HKLM\SYSTEM\CurrentControlSet\Enum\Root\MS_NDISWANBH\0000\Device Parameters\InstanceIndex New Value      1

HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network                    Number of Subkeys      69
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\nm                New Key
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\nm.sys             New Value      Service
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\nm.sys             New Key
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\nm.sys             New Value      Driver

HKLM\SYSTEM\CurrentControlSet\Control\Network                            Key Last Modified Date 1/18/2005 10:58:56 AM3/31/2004 1:45:29 AM
HKLM\SYSTEM\CurrentControlSet\Control\Network\Config                     Value Changed          00 00 00 00 17 00 00 00 00 00 00 15 00 00 00 9a 9a c4 dd ef fb dc 4e
92 24                                                                    4c e2 2e 32 5b e6 04 00 00 00 28 00 00 00 ...

HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318} Number of Subkeys      7
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA} New Key
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Characteristics New Value      0
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\InfPath New Value      netnm.inf
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\InfSection New Value
NETMON.PrimaryInstall
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Description New Value      Network Monitor
Drive
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\ComponentId New Value      MS_NetMon
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi New Key
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi\HelpText New Value      Netmon Packet
capture                                                                    driver that allows the
                                                                    Netmon UI to acquire
                                                                    packets from the local
                                                                    network.
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi\Service New Value      NM
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi\Interfaces New Key
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi\Interfaces\UpperRange New Value      noupper

```

```
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi\Interfaces\LowerRange New Value
ndis5,ndiswanbh,ndisa m
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}\Descriptions Number of Values 7
6
Key Last Modified Date 1/18/2005 10:58:54
AM3/31/2004 1:45:28 AM
HKLM\SYSTEM\CurrentControlSet\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}\Descriptions\WAN Miniport (Network Monitor) New Value 1
```

```

HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}
7
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
New Key
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\DeviceInstance
New Value ROOT\MS_NDISWANBH\000
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\Control
New Key
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\Control\ReferenceCount
New Value 1
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#NDISWANBH
New Key
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#NDISWANBH\SymbolicLink
New Value \\?\ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\
NDISWANBH
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#NDISWANBH\Control
New Key
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#NDISWANBH\Control\Linked
New Value 1

HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}
Number of Subkeys 7 6
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006
New Key
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\EnumExportPref
New Value 0
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Characteristics
New Value 41
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\ComponentId
New Value ms_ndiswanbh
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\InfPath
New Value netrasa.inf
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\InfSection
New Value Ndi-Mp-Bh
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\ProviderName
New Value Microsoft
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\DriverDateData
New Value 00 40 4b de e9 27 bf 1
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\DriverDate
New Value 11-6-1999
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\DriverVersion
New Value 5.0.2175.1
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\MatchingDeviceId
New Value ms_ndiswanbh
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\DriverDesc
New Value WAN Miniport (Network Monitor)
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\NetCfgInstanceId
New Value {68A221DC-ED1B-4507-A FB-787AB946F7CF}
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi
New Key
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi\BindForm
New Value NdisWanBh
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi\Service
New Value NdisWan
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi\Interfaces
New Key
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi\Interfaces\UpperRange
New Value ndiswanbh
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi\Interfaces\LowerRange
New Value wan
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Linkage
New Key
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Linkage\RootDevice
New Value NdisWanBh
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Linkage\UpperBind
New Value NM
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Linkage\Export
New Value \Device\NdisWanBh
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0000\Linkage
Key Last Modified Date 1/18/2005 10:58:58 AM3/31/2004 1:45:16 AM
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0000\Linkage\UpperBind
Value Changed NM Tcpip

```


HKLM\SYSTEM\ControlSet001\Services	Number of Subkeys	210	207
HKLM\SYSTEM\ControlSet001\Services\nm	New Key		
HKLM\SYSTEM\ControlSet001\Services\nm\Type	New Value	1	
HKLM\SYSTEM\ControlSet001\Services\nm\Start	New Value	3	
HKLM\SYSTEM\ControlSet001\Services\nm\ErrorControl	New Value	1	
HKLM\SYSTEM\ControlSet001\Services\nm\ImagePath	New Value		System32\DRIVERS\NMnt sys
HKLM\SYSTEM\ControlSet001\Services\nm\DisplayName	New Value		Network Monitor Drive
HKLM\SYSTEM\ControlSet001\Services\nm\Security	New Key		
HKLM\SYSTEM\ControlSet001\Services\nm\Security\Security	New Value		01 00 14 80 a0 00 00 0 ac 00 00 00 14 00 00 00 30 00 00 00 02 00 1c 00 01 00 00 00 02 80 14 00 ...
HKLM\SYSTEM\ControlSet001\Services\nm\Parameters	New Key		
HKLM\SYSTEM\ControlSet001\Services\nm\Linkage	New Value		
HKLM\SYSTEM\ControlSet001\Services\nm\Linkage\Bind	New Key		
HKLM\SYSTEM\ControlSet001\Services\nm\Linkage\Route	New Value		\Device\{5280E404-268 -42DB-A5FD-00839AA4395F}
HKLM\SYSTEM\ControlSet001\Services\nm\Linkage\Export	New Value		"{5280E404-2685-42DB- 5FD-00839AA4395F}" \Device\NM_{5280E404- 685-42DB-A5FD-00839AA4395F}
HKLM\SYSTEM\ControlSet001\Services\NPF	New Key		
HKLM\SYSTEM\ControlSet001\Services\NPF\Type	New Value	1	
HKLM\SYSTEM\ControlSet001\Services\NPF\Start	New Value	3	
HKLM\SYSTEM\ControlSet001\Services\NPF\ErrorControl	New Value	1	
HKLM\SYSTEM\ControlSet001\Services\NPF\ImagePath	New Value		system32\drivers\npf. ys
HKLM\SYSTEM\ControlSet001\Services\NPF\DisplayName	New Value		NetGroup Packet Filte Driver
HKLM\SYSTEM\ControlSet001\Services\NPF\Security	New Key		
HKLM\SYSTEM\ControlSet001\Services\NPF\Security\Security	New Value		01 00 14 80 a0 00 00 0 ac 00 00 00 14 00 00 00 30 00 00 00 02 00 1c 00 01 00 00 00 02 80 14 00 ...
HKLM\SYSTEM\ControlSet001\Services\rpcapd	New Key		
HKLM\SYSTEM\ControlSet001\Services\rpcapd\Type	New Value	16	
HKLM\SYSTEM\ControlSet001\Services\rpcapd\Start	New Value		3
HKLM\SYSTEM\ControlSet001\Services\rpcapd\ErrorControl	New Value	1	
HKLM\SYSTEM\ControlSet001\Services\rpcapd\ImagePath	New Value		"%ProgramFiles%\WinPc p\ rpcapd.exe" -d -f "%ProgramFiles%\WinPcap\rpcapd.ini"
HKLM\SYSTEM\ControlSet001\Services\rpcapd\DisplayName	New Value		Remote Packet Capture Protocol v.0 (experimental)
HKLM\SYSTEM\ControlSet001\Services\rpcapd\ObjectName	New Value		LocalSystem
HKLM\SYSTEM\ControlSet001\Services\rpcapd>Description	New Value		Allows to capture tra fic on this machine from a remote machine.
HKLM\SYSTEM\ControlSet001\Services\rpcapd\Security	New Key		
HKLM\SYSTEM\ControlSet001\Services\rpcapd\Security\Security	New Value		01 00 14 80 a0 00 00 0 ac 00 00 00 14 00 00 00 30 00 00 00 02 00 1c 00 01 00 00 00 02 80 14 00 ...
HKLM\SYSTEM\ControlSet001\Services\NdisWan\Enum	Number of Values	4	3
HKLM\SYSTEM\ControlSet001\Services\NdisWan\Enum\Count	Key Last Modified Date	1/18/2005 10:58:58 AM	1/18/2005 10:30:50 AM
HKLM\SYSTEM\ControlSet001\Services\NdisWan\Enum\NextInstance	Value Changed	2	1
HKLM\SYSTEM\ControlSet001\Services\NdisWan\Enum\1	Value Changed	2	1
	New Value		ROOT\MS_NDISWANBH\000
HKLM\SYSTEM\ControlSet001\Services\NdisTapi\Enum	Number of Values	5	4
HKLM\SYSTEM\ControlSet001\Services\NdisTapi\Enum\Count	Key Last Modified Date	1/18/2005 10:58:58 AM	1/18/2005 10:30:50 AM
	Value Changed	3	2

HKLM\SYSTEM\ControlSet001\Services\NdisTapi\Enum\NextInstance
HKLM\SYSTEM\ControlSet001\Services\NdisTapi\Enum\2

Value Changed
New Value

3 2
ROOT\MS_NDISWANBH\000

HKLM\SYSTEM\ControlSet001\Hardware Profiles\Current\System\CurrentControlSet\Enum\ROOT	Number of Subkeys	5	4
HKLM\SYSTEM\ControlSet001\Hardware Profiles\Current\System\CurrentControlSet\Enum\ROOT\MS_NDISWANBH	New Key		
HKLM\SYSTEM\ControlSet001\Hardware Profiles\Current\System\CurrentControlSet\Enum\ROOT\MS_NDISWANBH\0000	New Key		
HKLM\SYSTEM\ControlSet001\Hardware Profiles\0001\System\CurrentControlSet\Enum\ROOT	Number of Subkeys	5	4
HKLM\SYSTEM\ControlSet001\Hardware Profiles\0001\System\CurrentControlSet\Enum\ROOT\MS_NDISWANBH	New Key		
HKLM\SYSTEM\ControlSet001\Hardware Profiles\0001\System\CurrentControlSet\Enum\ROOT\MS_NDISWANBH\0000	New Key		
HKLM\SYSTEM\ControlSet001\Enum\Root	Number of Subkeys	78	77
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH	New Key		
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000	New Key		
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\ClassGUID	New Value	{4D36E972-E325-11CE-B C1-08002BE10318}	
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\Class	New Value	Net	
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\HardwareID	New Value	ms_ndiswanbh	
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\Driver	New Value	{4D36E972-E325-11CE-B C1-08002BE10318}\0006	
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\LowerFilters	New Value	NdisTapi	
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\Mfg	New Value	Microsoft	
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\Service	New Value	NdisWan	
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\DeviceDesc	New Value	WAN Miniport (Network Monitor)	
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\ConfigFlags	New Value	0	
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\Capabilities	New Value	0	
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\Control	New Key		
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\Control\DeviceReference	New Value	-2124777968	
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\LogConf	New Key		
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\Device Parameters	New Key		
HKLM\SYSTEM\ControlSet001\Enum\Root\MS_NDISWANBH\0000\Device Parameters\InstanceIndex	New Value	1	
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Network	Number of Subkeys	69	67
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Network\nm	New Key		
	New Value	Service	
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Network\nm.sys	New Key		
	New Value	Driver	
HKLM\SYSTEM\ControlSet001\Control\Network	Key Last Modified Date	1/18/2005 10:58:56 AM3/31/2004 1:45:29 AM	
HKLM\SYSTEM\ControlSet001\Control\Network\Config	Value Changed	00 00 00 00 17 00 00 00 00 00 00 15 00 00 00 9a 9a c4 dd ef fb dc 4e 92 24 4c e2 2e 32 5b e6 04 00 00 00 28 00 00 00 ...	
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}	Number of Subkeys	7	6
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}	New Key		
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Characteristics	New Value	0	
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\InfPath	New Value	netnm.inf	
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\InfSection	New Value		
NETMON.PrimaryInstall			
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Description	New Value	Network Monitor	
Drive			
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\ComponentId	New Value	MS_NetMon	
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi	New Key		
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi\HelpText	New Value	Netmon Packet	
capture driver			

that allows the Netmon UI
to

```
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi\Service      New Value
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi\Interfaces  New Key
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi\Interfaces\UpperRange
                                                                    New Value
                                                                    noupper
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E975-E325-11CE-BFC1-08002BE10318}\{4EEE1DEC-38F6-46BD-9087-9E6C9517CCFA}\Ndi\Interfaces\LowerRange
                                                                    New Value
                                                                    ndis5,ndiswanbh,ndisa m
```

HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}\Descriptions	Number of Values	7	6
	Key Last Modified Date	1/18/2005 10:58:54	
HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}\Descriptions\WAN Miniport (Network Monitor)	New Value	AM3/31/2004 1:45:28 AM	1
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}	Number of Subkeys		8
7			
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}	New Key		
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\DeviceInstance	New Value	ROOT#MS_NDISWANBH\000	
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\Control	New Key		
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\Control\ReferenceCount	New Value	1	
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#NDISWANBH	New Key		
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#NDISWANBH\SymbolicLink	New Value	\\?#ROOT#MS_NDISWANBH	
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#NDISWANBH\Control		0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\NDISWANBH	
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#NDISWANBH\Control\Linked	New Key		
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#ROOT#MS_NDISWANBH#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#NDISWANBH\Control\Linked	New Value	1	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}	Number of Subkeys	7	6
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006	New Key		
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\EnumExportPref	New Value	0	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Characteristics	New Value	41	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\ComponentId	New Value	ms_ndiswanbh	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\InfPath	New Value	netrasa.inf	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\InfSection	New Value	Ndi-Mp-Bh	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\ProviderName	New Value	Microsoft	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\DriverDateData	New Value	00 40 4b de e9 27 bf 1	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\DriverDate	New Value	11-6-1999	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\DriverVersion	New Value	5.0.2175.1	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\MatchingDeviceId	New Value	ms_ndiswanbh	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\DriverDesc	New Value	WAN Miniport (Network Monitor)	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\NetCfgInstanceId	New Value	{68A221DC-ED1B-4507-A FB-787AB946F7CF}	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi	New Key		
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi\BindForm	New Value	NdisWanBh	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi\Service	New Value	NdisWan	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi\Interfaces	New Key		
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi\Interfaces\UpperRange	New Value	ndiswanbh	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Ndi\Interfaces\LowerRange	New Value	wan	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Linkage	New Key		
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Linkage\RootDevice	New Value	NdisWanBh	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Linkage\UpperBind	New Value	NM	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0006\Linkage\Export	New Value	\Device\NdisWanBh	
HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0000\Linkage	Key Last Modified Date	1/18/2005 10:58:58 AM3/31/2004 1:45:16 AM	

HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0000\Linkage\UpperBind Value Changed NM Tcpip

© SANS Institute 2005, Author retains full rights

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	Number of Subkeys	27	26
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst	New Key		
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\DisplayName	New Value	WinPcap 3.1 beta3	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\UninstallString	New Value	"C:\Program Files\WinPcap\Uninstall.exe"	
		"C:\Program Files\WinPcap\install.log"	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\InstallLocation	New Value	C:\Program Files\WinP ap	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\InstallSource	New Value	C:\temp\SANS	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\InstallSourceFile	New Value	C:\temp\SANS\WinPcap_ _1_beta_3.exe	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\InstallDate	New Value	01/18/2005	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\Publisher	New Value	Politecnico di Torino	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs	Number of Values	44	43
	Key Last Modified Date	1/18/2005 10:58:40 AM	1/18/2005 10:21:29 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\C:\Program Files\WinPcap\Uninstall.exe	New Value	1	
HKLM\SOFTWARE\Microsoft\Cryptography\ RNG	Key Last Modified Date	1/18/2005 10:59:18 AM	1/18/2005 10:56:56 AM
HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed	Value Changed	88 d5 8b 0e b2 78 fe 2f 51 19 1a 89 f2 be 7c ed f0 78 b9 cd 25 58 db 44 ea 3e ac 23 3c ae 9f 71 f5 8c de 44 c5 b7 87	
		...	
HKLM\SOFTWARE\Classes\Interface	Number of Subkeys	2085	2080
HKLM\SOFTWARE\Classes\Interface\{394540A0-6FCF-11D0-ACE0-0000F80114D3}	New Key		
	New Value	IRemoteDelaydC	
HKLM\SOFTWARE\Classes\Interface\{394540A0-6FCF-11D0-ACE0-0000F80114D3}\ProxyStubClsid32	New Key		
	New Value	{944AD531-B09D-11CE-B 9C-00AA006CB37D}	
HKLM\SOFTWARE\Classes\Interface\{394540A0-6FCF-11D0-ACE0-0000F80114D3}\NumMethods	New Key		
	New Value	16	
HKLM\SOFTWARE\Classes\Interface\{8947C648-3833-11D1-8682-00C04FBFE171}	New Key		
	New Value	IRemoteCallBack	
HKLM\SOFTWARE\Classes\Interface\{8947C648-3833-11D1-8682-00C04FBFE171}\ProxyStubClsid32	New Key		
	New Value	{944AD531-B09D-11CE-B 9C-00AA006CB37D}	
HKLM\SOFTWARE\Classes\Interface\{8947C648-3833-11D1-8682-00C04FBFE171}\NumMethods	New Key		
	New Value	4	
HKLM\SOFTWARE\Classes\Interface\{944AD531-B09D-11CE-B59C-00AA006CB37D}	New Key		
	New Value	IRemoteStats	
HKLM\SOFTWARE\Classes\Interface\{944AD531-B09D-11CE-B59C-00AA006CB37D}\ProxyStubClsid32	New Key		
	New Value	{944AD531-B09D-11CE-B 9C-00AA006CB37D}	
HKLM\SOFTWARE\Classes\Interface\{944AD531-B09D-11CE-B59C-00AA006CB37D}\NumMethods	New Key		
	New Value	16	
HKLM\SOFTWARE\Classes\Interface\{944AD532-B09D-11CE-B59C-00AA006CB37D}	New Key		
	New Value	IRemoteFinder	
HKLM\SOFTWARE\Classes\Interface\{944AD532-B09D-11CE-B59C-00AA006CB37D}\ProxyStubClsid32	New Key		
	New Value	{944AD531-B09D-11CE-B 9C-00AA006CB37D}	
HKLM\SOFTWARE\Classes\Interface\{944AD532-B09D-11CE-B59C-00AA006CB37D}\NumMethods	New Key		
	New Value	4	
HKLM\SOFTWARE\Classes\Interface\{E99A04AB-AB95-11D0-BE96-00A0C94989DE}	New Key		
	New Value	IRemoteESP	
HKLM\SOFTWARE\Classes\Interface\{E99A04AB-AB95-11D0-BE96-00A0C94989DE}\ProxyStubClsid32	New Key		
	New Value	{944AD531-B09D-11CE-B 9C-00AA006CB37D}	
HKLM\SOFTWARE\Classes\Interface\{E99A04AB-AB95-11D0-BE96-00A0C94989DE}\NumMethods	New Key		

New Value

13

© SANS Institute 2005, Author retains full rights


```
HKLM\SOFTWARE\Classes\CLSID
HKLM\SOFTWARE\Classes\CLSID\{944AD531-B09D-11CE-B59C-00AA006CB37D}
HKLM\SOFTWARE\Classes\CLSID\{944AD531-B09D-11CE-B59C-00AA006CB37D}\InProcServer32
HKLM\SOFTWARE\Classes\CLSID\{944AD531-B09D-11CE-B59C-00AA006CB37D}\InProcServer32\ThreadingModel
HKLM\SOFTWARE\Classes\CLSID\{D413C502-3FAA-11D0-B254-444553540000}
HKLM\SOFTWARE\Classes\CLSID\{D413C502-3FAA-11D0-B254-444553540000}\AppID
HKLM\SOFTWARE\Classes\CLSID\{D413C502-3FAA-11D0-B254-444553540000}\LocalServer32
HKLM\SOFTWARE\Classes\CLSID\{D413C502-3FAA-11D0-B254-444553540000}\LocalServer32\ThreadingModel

HKLM\SOFTWARE\Classes\AppID
HKLM\SOFTWARE\Classes\AppID\{D413C502-3FAA-11D0-B254-444553540000}
```

	Number of Subkeys		
	1892		1890
	New Key		
	New Value	PSFactoryBuffer	
	New Key		
	New Value	C:\WINNT\System32\PsN PAgn.dll	
	New Value	Both	
	New Key		
	New Value	NPPAgent	
	New Value	{D413C502-3FAA-11D0-B 54-444553540000}	
	New Key		
	New Value	C:\WINNT\System32\NPP NPPAgent.exe	
	New Value	Both	
	Number of Subkeys	36	35
	New Key		
	New Value		

Changes from Snapshot Summary for Services
Snapshot: 01/18/05 10:57:09
Tested: 01/18/05 10:59:18

Name	Critical	Warning	Info	Ignored
Win32	1	0	0	0
Drivers	2	0	0	0

Changes from Snapshot Details for Services
Snapshot:
Tested:

Name

Remote Packet Capture Protocol v.0 (experimental)

NetGroup Packet Filter Driver

Network Monitor Driver