GIAC Certified Forensic Analyst (GCFA)

Forensic Analysis of Shared Workstation

Practical assignment

Version 1.3

Michael Kerr

First Steps - Preparation

Toolkit Preparation

Before any forensic investigation can take place some work is involved in order to have confidence that the results produced are consistent, reproducible, and most importantly, correct. In order to have total confidence in the tools I would be using I undertook considerable research in order to choose the most functional and up to date freely available applications. With the small exception of the Winalysis, Sysinternals utilities (and of course Windows), everything else was open source and was digitally signed either by the software publisher or the software distributor.
My investigation would require both a Windows and Linux forensics workstation with large hard drive capacity and good processing power, for this purpose I built the following machine as my main forensics workstation:

AMD Duron 1.3Mhz
256Mb RAM
liteon 52x CDROM
Seagate 13Gb IDE HDD (for OS)
Seagate 80Gb IDE HDD in removable drive bay (for images)
Iomega ATAPI Zip100 disk drive
OS: Redhat 9 Shrike (Workstation install)

And utilised a Toshiba Satellite TE2100 Laptop as an onsite workstation
Intel 1.4Ghz P4
512 RAM
Toshiba 30Gb HDD
OS: Windows 2000 Professional

Main software tools chosen:

<u>Linux</u>
Autopsy 1.73
Sleuthkit 1.62

<u>Windows</u>
Winalysis
The Forensics Acquisition Utilities

In addition to these tools, I chose to use the F.I.R.E (Forensics Incident Response Environment) utility CD. This toolkit packages up many small utilities from both Linux and Windows, creating a trusted environment from which to launch many of the nuts and bolts applications used in information gathering at the scene. As I detail each step of the image acquisition and binary analysis the usefulness of this CD will become apparent.
Included on the F.I.R.E CD and used in my investigation are:

- env (show environment variables)
- fport (enumerate listening ports and map to processes)
- hunt (enumerate shares and local users)

- listdlls (List all dlls currently in memory)
- netstat (List all ports in use)
- ntlast (List all recent logins)
- printenv (show environment variables)
- psinfo (display detailed system information)
- pslist (show running processes)
- psloggeon (show current users logged on and logged on via shares)
- uname (show machine specific information)
- uptime (display how long machine has been up for)
- whoami (display operators login)
- dd (disk imaging tool ported from unix)
- netcat (nc, send data streams over the network)
- md5sum (create md5 hash sums for files)
- binText (extract strings)
- strace (log system calls from an executable)

Building A Trustworthy Forensic Environment.

In order to have total confidence in the tools used, all software sources should be verified as unmodified since being published by the developers. Verification of the windows installation media is reasonably straight forward. I used an original Microsoft Windows 2000 installation CD, resplendent with it's holographic seal burnt into the topside of the disc[1].

My signed Windows 2000 CD

On the other hand the Redhat installation CDs, and all of the Linux tools were downloaded from the internet.
In order to verify an ISO image it is necessary to locate the accompanying md5 checksum file. This in turn is digitally signed by the publisher, guaranteeing its authenticity. In order to verify the checksum file it is first necessary to obtain the signers public pgp/gnupg key. In this case it was security@redhat.com. The concept of pgp/gnupg's web of trust requires the key to be signed by either my own private key, or by someone else who I have chosen to trust[2]. Unfortunately I do not have the good fortune to be well acquainted with any of the signers of the Redhat security key, nor do any of my already trusted public keys in turn trust this key, and so on. My general rule in these situations is to trust a key if I can obtain it identically from three different sources. The public key for security@redhat.com was identical at these different sources;

1. The Redhat Web Site

[1] Microsoft's Website has detailed instructions on examining CD's in order to determine authenticity, http://www.microsoft.com/resources/howtotell/uk/applications/default.mspx.
[2] These explanations are brief, but the larger fields of PGP security and cryptography in general are off the topic of my paper. Interested people should check out the Gnupg Privacy Handbook and RSA's cryptography faq for a every good introduction to cryptography.

2. pgp.mit.edu
3. wwwkeys.pgp.net

Based on this I felt it was reasonable to trust the security@redhat.com public key, and therefore locally signed the key on my key ring. Once the key was signed and trusted the digital signature embedded in the md5 checksum file was evaluated. It checked out fine and meant I was now able to verify the downloaded ISO images against these values by creating my own checksums and comparing.
Below is the output of the session, showing the signing of the public key, the checking of the digital signature on the md5 file, and finally the hash value calculation and comparison. My commands are in bold, everything else is output.

```
kerrm@mandrill:~/isos$ gpg --edit-key security@redhat.com lsign
gpg (GnuPG) 1.2.1; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.


pub  1024D/DB42A60E  created: 1999-09-23 expires: never       trust: -/-
sub  2048g/961630A2  created: 1999-09-23 expires: never
(1). Red Hat, Inc <security@redhat.com>


pub  1024D/DB42A60E  created: 1999-09-23 expires: never      trust: -/-
Primary key fingerprint: CA20 8686 2BD6 9DFC 65F6 ECC4 2191 80CD DB42 A60E

     Red Hat, Inc <security@redhat.com>

How carefully have you verified the key you are about to sign actually belongs
to the person named above?  If you don't know what to answer, enter "0".

   (0) I will not answer. (default)
   (1) I have not checked at all.
   (2) I have done casual checking.
   (3) I have done very careful checking.

Your selection? 3
Are you really sure that you want to sign this key
with your key: "Michael Kerr (Michael Kerr) <zokuju@telstra.com>"

The signature will be marked as non-exportable.

I have checked this key very carefully.

Really sign? yes

You need a passphrase to unlock the secret key for
user: "Michael Kerr (Michael Kerr) <zokuju@telstra.com>"
1024-bit DSA key, ID 15FC8E6E, created 2003-04-27

Enter passphrase:
Command> save

kerrm@mandrill:~/isos$ gpg -verify MD5SUM
gpg: Signature made Wed Apr  2 07:07:31 2003 EST using DSA key ID DB42A60E
gpg: Good signature from "Red Hat, Inc <security@redhat.com>"
gpg: checking the trustdb
gpg: checking at depth 0 signed=1 ot(-/q/n/m/f/u)=0/0/0/0/0/1
gpg: checking at depth 1 signed=0 ot(-/q/n/m/f/u)=1/0/0/0/0/0
kerrm@mandrill:~/isos$ openssl dgst shrike*
MD5(shrike-i386-disc1.iso)= 400c7fb292c73b793fb722532abd09ad
MD5(shrike-i386-disc2.iso)= 6b8ba42f56b397d536826c78c9679c0a
MD5(shrike-i386-disc3.iso)= af38ac4316ba20df2dec5f990913396d
kerrm@mandrill:~/isos$ cat MD5SUM.txt
400c7fb292c73b793fb722532abd09ad  shrike-i386-disc1.iso
6b8ba42f56b397d536826c78c9679c0a  shrike-i386-disc2.iso
```

```
af38ac4316ba20df2dec5f990913396d  shrike-i386-disc3.iso
0727c51ab359dafa9ab31e0c50958aa6  shrike-SRPMS-disc1.iso
2ddd8e6a8502869cd2e78d47590b9be1  shrike-SRPMS-disc2.iso
f378cf68b22c3b9a64c86b5067511630  shrike-SRPMS-disc3.iso
```

This process proved invaluable, as my first attempted download from my local mirror site produced a corrupted ISO image of disk 1. While the disk was usable, and the installer functioned correctly, it would prove to be my downfall later, if scrutinised. I therefore downloaded the image again directly from the Redhat ftp site.

A similar process of verification was followed for the F.I.R.E ISO image, the @tstake Sleuthkit, Autopsy and the FAU archive files. This machine was now dedicated use, its software verified and it was physically located in an area with restricted access. I now had confidence that the lab environment was trustworthy and would produce accurate, reliable and reproducible results.

Part 1 – Binary Analysis

I began my investigation on Linux. The file provided was called binary_v1.3.zip. Using the Gnu unzip utility I extracted a report from the zip file using the following command.

```
unzip -Z -v binary_v1.3.zip
```

The full report is attached as appendix A. Key information reported is as follows:

- File size
  - compressed 5,567 bytes
  - uncompressed 26,793 bytes
- MAC times
  - Last modified date 2003-02-20 12:45:48

Unfortunately without access to the original file system it would not be possible to derive more detailed MAC information from the file, as the full metadata information is not packaged in the zip file, but on the fiesystem.

From the command line I extracted the file using unzip.

```
[kerrm@forensics binary analysis]$ unzip -u binary_v1.3.zip
Archive:       binary_v1.3.zip
 inflating: target2.exe
```

Once the file was extracted I immediately produced a hash value in order to check the integrity of the binary subject during and after the investigation.

```
[kerrm@forensics binary analysis]$md5sum target2.exe > target2.md5; cat target2.md5
848903a92843895f3ba7fb77f02f9bf1  target2.exe

[kerrm@forensics binary analysis]$ file target2.exe
target2.exe: MS-DOS executable (EXE), OS/2 or MS Windows
```

After considering the output from the file utility I moved the investigation the Windows platform.

Windows 2000 Analysis

From Windows I again unzipped the binary and produced a hash value using the md5sum utility supplied with the FIRE CD. The hash value can be seen to match the value obtained from the Linux workstation.

```
kerrm@forensics:~/binary analysis
File  Edit  View  Terminal  Go  Help
kerrm@forensics:~/binary analysis    kerrm@forensics:~
[kerrm@forensics binary analysis]$ ls
binary analysis.sxw  binary_v1.3.zip  target2.exe  target2.md5
[kerrm@forensics binary analysis]$ md5sum target2.exe > target2.md5;cat target2.
md5
848903a92843895f3ba7fb77f02f9bf1  target2.exe
[kerrm@forensics binary analysis]$ file target2.exe
target2.exe: MS-DOS executable (EXE), OS/2 or MS Windows
[kerrm@forensics binary analysis]$ ls -l target2.exe
-rwxrwxr-x    1 kerrm    kerrm       26793 Feb 20 13:45 target2.exe
[kerrm@forensics binary analysis]$
```

MD5 hash creation of unknown binary on the Linux system

```
Forensic Cmd Shell
Ctrl-D or Ctrl-F for Directory and filname completion
The Shell Path has been modified to find trusted cdrom binaries first
Do not navigate away from the CD drive letter.
==================================================================
15:00:32.53 E:\> md5sum "d:\gcfa\binary analysis\target2.exe"
\848903a92843895f3ba7fb77f02f9bf1 *d:\\gcfa\\binary analysis\\target2.exe

15:00:54.39 E:\>
```

MD5 hash creation of unknown binary on the Windows system

The next step was to extract all readable strings from the exe. Using BinText I extracted 150 lines of text, listed in Appendix B, the most interesting are also listed here:

```
Sleep
HeapAlloc
GetProcessHeap
TerminateProcess
ReadFile
PeekNamedPipe
CloseHandle
CreateProcessA
CreatePipe
WriteFile
GetLastError
LocalAlloc
KERNEL32.dll
StartServiceCtrlDispatcherA
SetServiceStatus
RegisterServiceCtrlHandlerA
CloseServiceHandle
ControlService
QueryServiceStatus
OpenServiceA
CreateServiceA
OpenSCManagerA
DeleteService
StartServiceA
ChangeServiceConfigA
QueryServiceConfigA
ADVAPI32.dll
WSAIoctl
WSASocketA
WS2_32.dll
MFC42.DLL
memmove
fprintf
sprintf
perror
strstr
printf
MSVCRT.dll
impossibile creare raw ICMP socket
RAW ICMP SendTo:
======================== Icmp BackDoor V0.1 ========================
========= Code by Spoof. Enjoy Yourself!
Your PassWord:
loki
Hello from MFC!
\winnt\system32\smsses.exe
\\199.107.97.191\C$
\winnt\system32
\winnt\system32\reg.exe
```

Based purely on the banner and the password string I expected the application to be some type of variant of the original Loki ICMP backdoor first documented in 1996 in the whitepaper "Project Loki"[3] by daemon9 & Alhambra, and still available at www.phrack.org. Loki facilitates the transport of data through the ICMP_ECHO standard packet. The version number of 0.1 suggests this is an initial/early attempt of a port to win32. The source code to the original UNIX version is still available at phrack[4].

[3] http://www.phrack.org/show.php?p=49&a=6
[4] Loki2 source available at http://www.phrack.org/show.php?p=51&a=6

Banner

The exe contains the banner

```
======================== Icmp BackDoor V0.1 ========================
========= Code by Spoof. Enjoy Yourself!
```

Which clearly states the applications purpose, or at least its advertised purpose. The alias "Spoof" is the clearest indication of the responsible entity, either one person or a group. Searching of the internet using Google, Altavista, and Teoma failed to find anyone operating under this alias distributing an ICMP tool.

Loki

The two lines

```
Your PassWord:
loki
```

Indicate the application supports some sort of simple authentication, but its usage is not clear from the strings file.

External application dependency

Two external applications are referenced in the exe.

```
\winnt\system32\smsses.exe
\winnt\system32\reg.exe
```

After extensive searching on the internet I could find no reference to any application known as smsses.exe. This suggests the application either creates the file when run, or attempts to create it, or the code which uses this string is unused.
The second program, reg.exe is commonly known as a Microsoft tool used to write registry values, and can be called from the command line. However, reg.exe is not present on most Windows systems, as it is distributed as part of the NT4 resource kit, and in the support tools for Windows 2000[5]. Either the reg.exe referred to by target2.exe is a different application with the same name, or the MS file is bundled in the target2 installation package, or the author has made a fairly large assumption that the file would be present on the target machine; perhaps he/she had detailed information on the intended target host? The only way to know for sure would be to obtain the target2 installation package and compare md5hash values against the MS reg.exe file and the bundled file, if present.

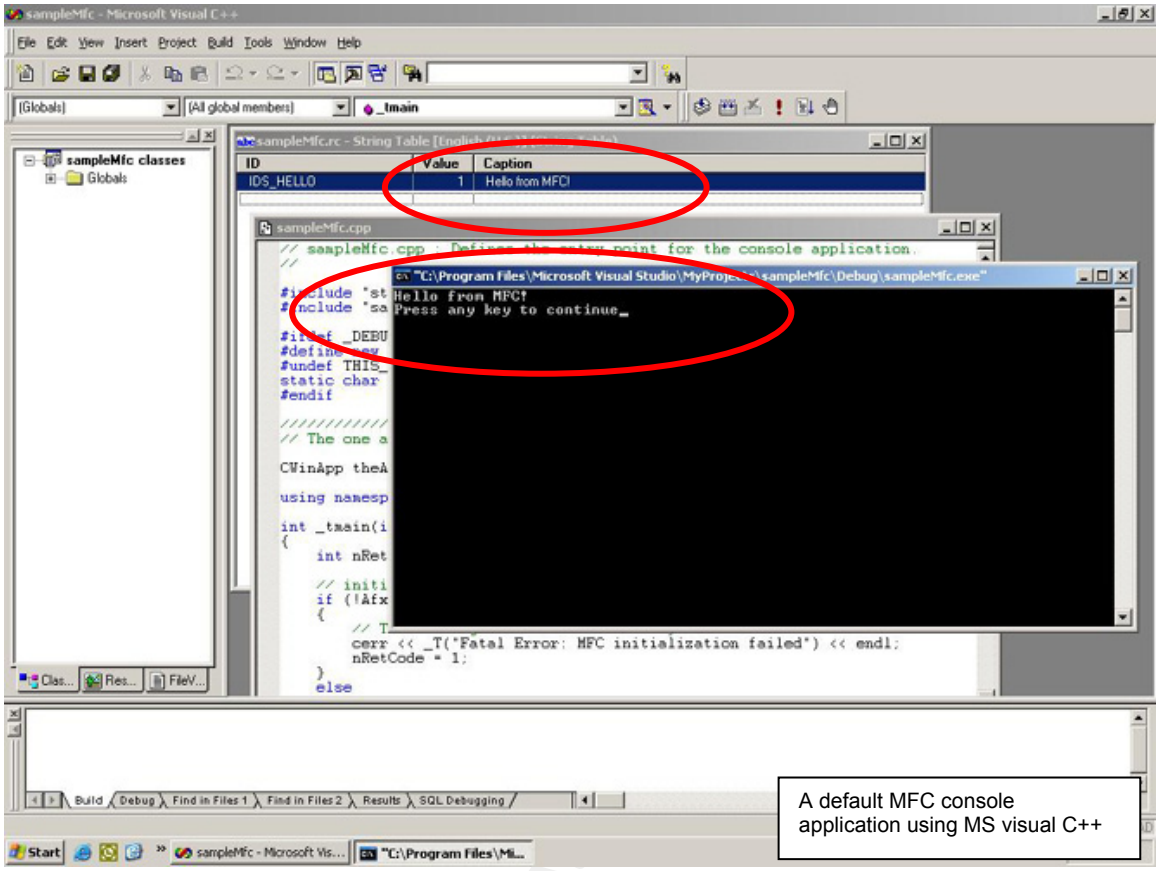
Hello from MFC!

The string "Hello from MFC!" gives away some information on the history of the applications development. This string is used in the default creation of a

---

5 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/scrguide/sas_reg_sgqw.asp

console application in Microsoft's Visual C++, indicating the application started out as a VC++ project supporting Microsoft Foundation Classes.

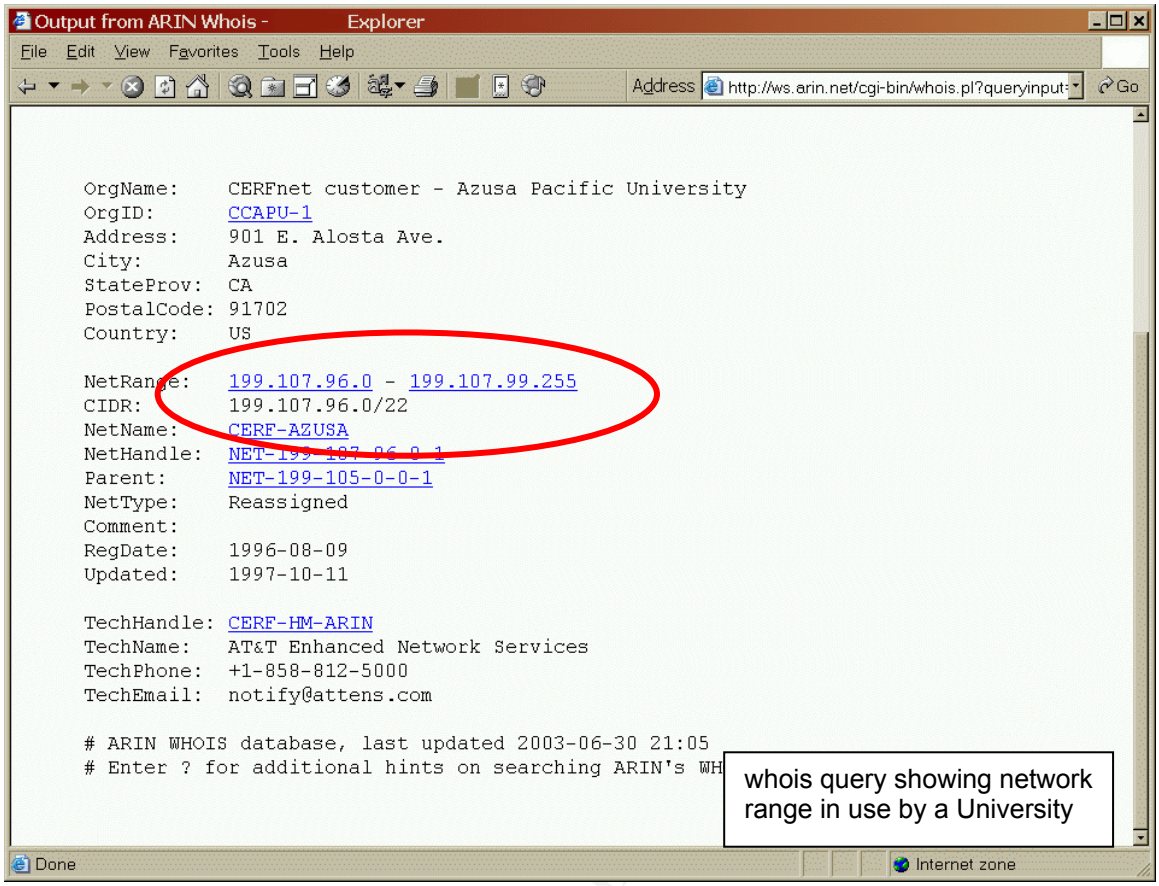


IP Address

The presence of an IP address in the form

```
\\199.107.97.191\C$
```

is hugely useful. In this form it shows the application may attempt to either copy to or from the hidden administrative share on the C drive of the machine 199.107.97.191. A quick whois search on arin.net shows the address range of 197.107.96.0 – 199.107.99.255 to be registered to a Californian University. It's common practice for universities to apply externally routable IP addresses to workstations. With sufficient resources it could be possible to track down the very machine this application connects to.



whois query showing network range in use by a University

System DLLs

The target2.exe contains references to several windows DLLs. The API calls extracted can be linked to each of the DLLS as follows:

KERNEL32.dll

- Handles memory management and I/O
  - CreateProcessA
  - ReadFile
  - Sleep
  - HeapAlloc
  - GetProcessHeap
  - TerminateProcess
  - PeekNamedPipe
  - CloseHandle
  - CreatePipe
  - WriteFile
  - GetLastError
  - LocalAlloc

ADVAPI32.dll

- Handles calls to registry and security related functions.
  - StartServiceCtrlDispatcherA
  - QueryServiceConfigA
  - SetServiceStatus
  - RegisterServiceCtrlHandlerA
  - CloseServiceHandle
  - ControlService
  - QueryServiceStatus
  - OpenServiceA
  - CreateServiceA
  - OpenSCManagerA

```
            o   DeleteService
            o   StartServiceA
            o   ChangeServiceConfigA


WS2_32.dll
    •   Windows sockets function
            o   WSAIoctl
            o   WSASocketA


MSVCRT.dll
    •   console printing and string manipulation
            o   memmove
            o   fprintf
            o   sprintf
            o   perror
            o   strstr
            o   printf


MFC42.DLL
    •   Microsoft foundation Classes
```

The API calls are essentially listed in opposite order to the strings output, making the information more readable.

Running The Application

At this point I decided the only way to learn more would be to run the application in my controlled environment. This step contained some risk, and although the forensics operating system was ultimately expendable I took several precautions before running the application. My internet connection was shut down and I set Ethereal running to report on any traffic sent from my machine.

Based on the examined output of the strings I expected to see the application do one, or several of the following things:

- Install a new service.
- stop a current service
- grab files from the Californian computer
- send files, or a report to the Californian computer
- output the banner to the console
- request a password
- write to the registry
- read from the registry
- open a socket
- access system DLLs

Again I used tools from the FIRE CD, but in addition I required several monitoring tools from the internet.

- Strace (FIRE CD)
- Winalysis [6]
- Filemon[7]
- Regmon[8]

[6] http://www.winalysis.com/
[7] http://www.sysinternals.com

- Ethereal[9]

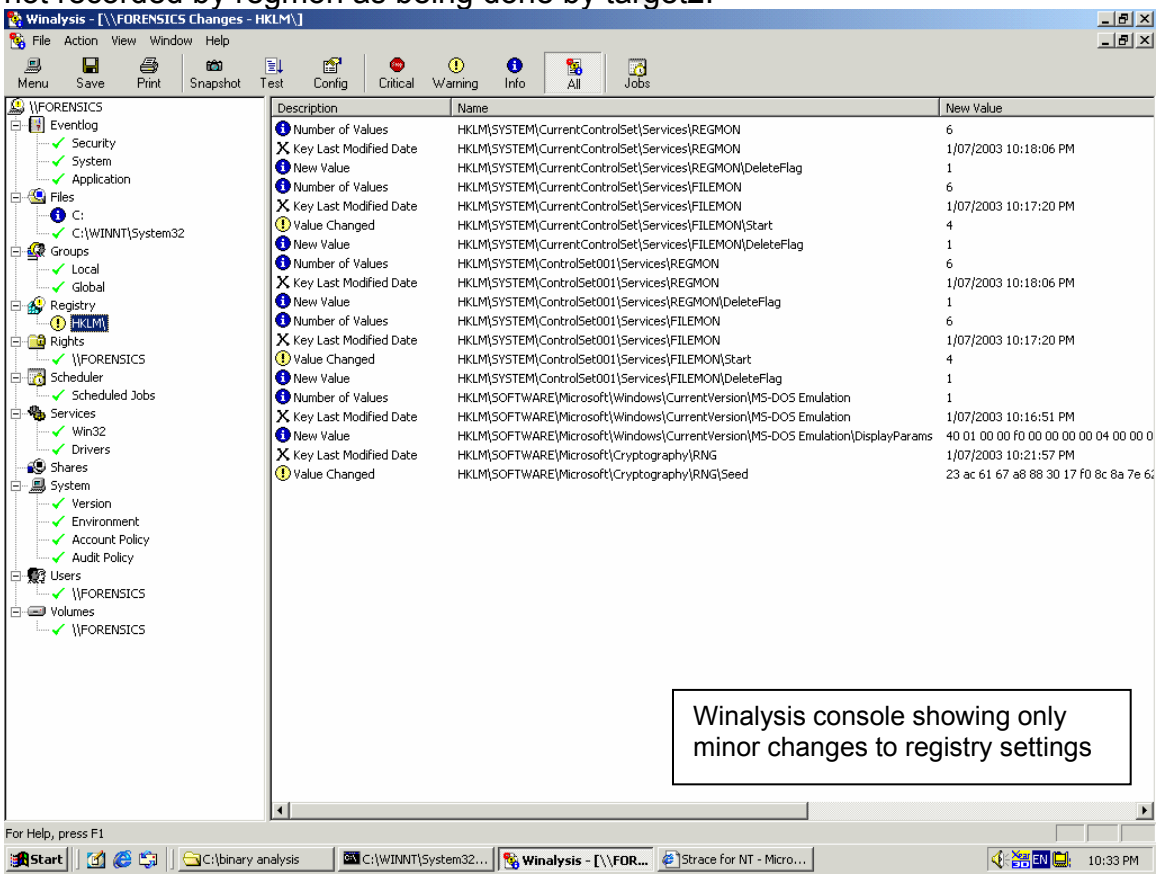
My methodology was as follows:

1. Take Winalysis snapshot of system
2. start Filemon to monitor file system activity
3. start Regmon to monitor registry activity
4. start the target2 executable, but attach the Strace program to log system calls
5. After program exit take Winalysis snapshot and compare
6. examine filemon log
7. examine regmon log
8. examine Strace log

The exe was run from the command line with the command

```
D:\gcfa\binary analysis\strace target2.exe > strace.log
```

Running the executable took approximately 5 seconds, the application exited with no messages.
My first examination was of the Winalysis comparison. The output shows only modification to the filemon and regmon keys, and the access to the systems random number generator seed value, which changes often under normal conditions, I was sure this was not modified as a result of our test, as it was not recorded by regmon as being done by target2.



[8] http://www.sysinternals.com
[9] http://www.ethereal.com

The filemon, regmon and strace log files are attached as Appendix C, D and E respectively.

There were of course many log entries created directly by the monitoring tools, and the system itself. Shown here in concise table form is a listing only of entries directly created by target2.exe for both filemon and regmon. The information, while initially overwhelming, is quite repetitive and describes the applications search for its required DLL. The final table, showing sections of the strace output, shows the application looking for MFC42LOC.DLL, which is not present. Finally the application attempts to open a pipe but returns the status STATUS_ACCESS_DENIED and then exits. Based on this we can see the application is not statically linked, and would probably require the MFC to be bundled with it's distribution in order to run correctly. MFC support files are not readily distributed by Microsoft, it would be moderately difficult to obtain and install the correct version for this application. Based on the information I had gathered so far I felt I could confidently describe the applications purpose without actually successfully running it.

FileMon Log

```
                                                C:\Documents and
10:21:00 PM    IRP_MJ_CREATE                    Settings\Administrator\Desktop
                                                C:\Documents and
10:21:00 PM    FSCTL_IS_VOLUME_MOUNTED          Settings\Administrator\Desktop
                                                C:\Documents and
10:21:00 PM    FASTIO_QUERY_OPEN                Settings\Administrator\Desktop\WS2_32.dll
                                                C:\Documents and
10:21:00 PM    FSCTL_IS_VOLUME_MOUNTED          Settings\Administrator\Desktop
                                                C:\Documents and
10:21:00 PM    FASTIO_QUERY_OPEN                Settings\Administrator\Desktop\WS2_32.dll
                                                C:\Documents and
10:21:00 PM    FSCTL_IS_VOLUME_MOUNTED          Settings\Administrator\Desktop
                                                C:\Documents and
10:21:00 PM    FASTIO_QUERY_OPEN                Settings\Administrator\Desktop\WS2_32.dll
                                                C:\Documents and
10:21:00 PM    FSCTL_IS_VOLUME_MOUNTED          Settings\Administrator\Desktop
                                                C:\Documents and
10:21:00 PM    FSCTL_IS_VOLUME_MOUNTED          Settings\Administrator\Desktop
10:21:00 PM    IRP_MJ_CREATE                    C:\WINNT\System32\WS2_32.dll
10:21:00 PM    IRP_MJ_CLEANUP                   C:\WINNT\System32\WS2_32.dll
10:21:00 PM    IRP_MJ_CLOSE                     C:\WINNT\System32\WS2_32.dll
                                                C:\Documents and
10:21:00 PM    FSCTL_IS_VOLUME_MOUNTED          Settings\Administrator\Desktop
                                                C:\Documents and
10:21:00 PM    FASTIO_QUERY_OPEN                Settings\Administrator\Desktop\WS2_32.dll
                                                C:\Documents and
10:21:00 PM    FSCTL_IS_VOLUME_MOUNTED          Settings\Administrator\Desktop
                                                C:\Documents and
10:21:00 PM    FASTIO_QUERY_OPEN                Settings\Administrator\Desktop\WS2_32.dll
                                                C:\Documents and
10:21:00 PM    FSCTL_IS_VOLUME_MOUNTED          Settings\Administrator\Desktop
                                                C:\Documents and
10:21:00 PM    FASTIO_QUERY_OPEN                Settings\Administrator\Desktop\WS2_32.dll
                                                C:\Documents and
10:21:00 PM    FSCTL_IS_VOLUME_MOUNTED          Settings\Administrator\Desktop
                                                C:\Documents and
10:21:00 PM    FSCTL_IS_VOLUME_MOUNTED          Settings\Administrator\Desktop
10:21:00 PM    IRP_MJ_CREATE                    C:\WINNT\System32\WS2HELP.DLL
10:21:00 PM    IRP_MJ_CLEANUP                   C:\WINNT\System32\WS2HELP.DLL
10:21:00 PM    IRP_MJ_CLOSE                     C:\WINNT\System32\WS2HELP.DLL
                                                C:\Documents and
10:21:00 PM    FSCTL_IS_VOLUME_MOUNTED          Settings\Administrator\Desktop
10:21:00 PM    FASTIO_QUERY_OPEN                C:\Documents and
```

		Settings\Administrator\Desktop\WS2_32.dll
10:21:00 PM	FSCTL_IS_VOLUME_MOUNTED	C:\Documents and Settings\Administrator\Desktop
10:21:00 PM	FASTIO_QUERY_OPEN	C:\Documents and Settings\Administrator\Desktop\WS2_32.dll
10:21:00 PM	FSCTL_IS_VOLUME_MOUNTED	C:\Documents and Settings\Administrator\Desktop
10:21:00 PM	FASTIO_QUERY_OPEN	C:\Documents and Settings\Administrator\Desktop\WS2_32.dll
10:21:00 PM	FSCTL_IS_VOLUME_MOUNTED	C:\Documents and Settings\Administrator\Desktop
10:21:00 PM	FSCTL_IS_VOLUME_MOUNTED	C:\Documents and Settings\Administrator\Desktop
10:21:00 PM	IRP_MJ_CREATE	C:\WINNT\System32\MFC42.DLL
10:21:00 PM	IRP_MJ_CLEANUP	C:\WINNT\System32\MFC42.DLL
10:21:00 PM	IRP_MJ_CLOSE	C:\WINNT\System32\MFC42.DLL
10:21:00 PM	FSCTL_IS_VOLUME_MOUNTED	C:\Documents and Settings\Administrator\Desktop
10:21:00 PM	FASTIO_QUERY_OPEN	C:\Documents and Settings\Administrator\Desktop\WS2_32.dll
10:21:00 PM	FSCTL_IS_VOLUME_MOUNTED	C:\Documents and Settings\Administrator\Desktop
10:21:00 PM	FSCTL_IS_VOLUME_MOUNTED	C:\Documents and Settings\Administrator\Desktop
10:21:00 PM	IRP_MJ_CREATE	C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll
10:21:00 PM	FASTIO_QUERY_STANDARD_INFO	C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll
10:21:00 PM	IRP_MJ_READ*	C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll
10:21:00 PM	IRP_MJ_CLEANUP	C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll
10:21:00 PM	IRP_MJ_READ*	C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll
10:21:00 PM	IRP_MJ_READ*	C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll
10:21:00 PM	IRP_MJ_READ*	C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll
10:21:00 PM	IRP_MJ_READ*	C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll
10:21:00 PM	IRP_MJ_READ*	C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll
10:21:00 PM	FSCTL_IS_VOLUME_MOUNTED	C:\Documents and Settings\Administrator\Desktop
10:21:00 PM	FASTIO_QUERY_OPEN	C:\Documents and Settings\Administrator\Desktop\WS2_32.dll
10:21:00 PM	FSCTL_IS_VOLUME_MOUNTED	C:\Documents and Settings\Administrator\Desktop
10:21:00 PM	FASTIO_QUERY_OPEN	C:\WINNT\System32\MFC42LOC.DLL
10:21:00 PM	FSCTL_IS_VOLUME_MOUNTED	C:\Documents and Settings\Administrator\Desktop
10:21:00 PM	FASTIO_QUERY_OPEN	C:\WINNT\System32\MFC42LOC.DLL
10:21:00 PM	IRP_MJ_READ*	C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll
10:21:00 PM	IRP_MJ_READ*	C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll
10:21:00 PM	IRP_MJ_READ*	C:\Documents and Settings\Administrator\Desktop\target2.exe

Regmon Log

OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\target2.exe	NOTFOUND
OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\target2.exe	NOTFOUND
OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\target2.exe	NOTFOUND
OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\target2.exe	NOTFOUND
OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\target2.exe	NOTFOUND
OpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS
QueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode	NOTFOUND
CloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS
OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
QueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack	NOTFOUND
CloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
OpenKey	HKLM	SUCCESS
OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NOTFOUND
OpenKey	HKLM\System\CurrentControlSet\Control\Error Message Instrument\	NOTFOUND
OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS
QueryValue	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32\target2	NOTFOUND
CloseKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS
OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2	SUCCESS
QueryValue	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2\target20.0	NOTFOUND
CloseKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2	SUCCESS
OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility	SUCCESS
QueryValue	HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility\target2	NOTFOUND
CloseKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility	SUCCESS
OpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility\target2.exe	NOTFOUND
OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS
QueryValue	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs	SUCCESS
CloseKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS
OpenKey	HKCU	SUCCESS
OpenKey	HKLM\System\CurrentControlSet\Control\Nls\MUILanguages	NOTFOUND
OpenKey	HKCU\Control Panel\Desktop	SUCCESS
QueryValue	HKCU\Control Panel\Desktop\MultiUILanguageId	NOTFOUND
CloseKey	HKCU\Control Panel\Desktop	SUCCESS
CloseKey	HKCU	SUCCESS
OpenKey	HKLM\System\CurrentControlSet\Control\ServiceCurrent	SUCCESS
QueryValue	HKLM\System\CurrentControlSet\Control\ServiceCurrent\(Default)	SUCCESS
CloseKey	HKLM\System\CurrentControlSet\Control\ServiceCurrent	SUCCESS
CloseKey	HKLM	SUCCESS

Strace Log
158 912 624 NtFsControlFile (28, 0, 0, 0, 1242152, 589864, 0, 0, 0, 0, ...) == 0x0
159 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0, "\??\C:\binary analysis\MSVCP60.dll"}, 1243076, ...) == 0x0
160 912 624 NtFsControlFile (28, 0, 0, 0, 1242908, 589864, 0, 0, 0, 0, ...) == 0x0
161 912 624 NtFsControlFile (28, 0, 0, 0, 1242352, 589864, 0, 0, 0, 0, ...) == 0x0
162 912 624 NtOpenFile (0x100020, {24, 0, 0x40, 0, 0, "\??\C:\binary analysis\MSVCP60.dll"}, 1243232, 5, 96, ... 36,) == 0x0
356 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0, "\??\C:\WINNT\System32\MFC42LOC.DLL"}, 1241268, ...) == STATUS_OBJECT_NAME_NOT_FOUND
357 912 624 NtFsControlFile (28, 0, 0, 0, 1240904, 589864, 0, 0, 0, 0, ...) == 0x0
358 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0, "\??\C:\WINNT\System32\MFC42LOC.DLL"}, 1241828, ...) == STATUS_OBJECT_NAME_NOT_FOUND
359 912 624 NtTestAlert (...) == 0x0
360 912 624 NtContinue (1244464, 1, ...
361 912 624 NtSetInformationThread (-2, 9, 1245176, 4, ...) == 0x0
362 912 624 NtOpenKey (0x1, {24, 52, 0x40, 0, 0, "System\CurrentControlSet\Control\ServiceCurrent"}, ... 80,) == 0x0
363 912 624 NtQueryValueKey (80, "□", 2, 1244012, 144, 1244164, ...) == 0x0
364 912 624 NtClose (80, ...) == 0x0
365 912 624 NtOpenFile (0x100080, {24, 0, 0x40, 0, 0, "\DosDevices\pipe\"}, 1244232, 3, 32, ... 80,) == 0x0
366 912 624 NtFsControlFile (80, 0, 0, 0, 1244240, 1114136, 1274896, 50, 0, 0, ...) == STATUS_IO_TIMEOUT
367 912 624 NtClose (80, ...) == 0x0
368 912 624 NtCreateFile (0xc0100080, {24, 0, 0x40, 0, 1244208, "\??\pipe\net\NtControlPipe9"}, 1244228, 0, 128, 3, 1, 96, 0, 0, ...) == STATUS_ACCESS_DENIED

Legal Implications

Based on what I have seen so far I will assume the application facilitates the transport of data over a network using a well known application of an ICMP weakness. This can be taken further to assume that, like the Unix based Loki applications, the transmitted data is intended to be executed by the target server. An application such as this really has only one intended purpose, the clandestine execution of code on a remote server which can be performed in such a way as to bypass packet filtering technology intended to manage standard traffic.

Therefore, it seems reasonable to state that any use of this application would be an attempt to gain "unauthorised use of a computer", as described in Australia's *Cybercrime Act 2001*(477.1), which carries a penalty of ten years imprisonment[10].

Unfortunately, a WinZip file contains only a files last accessed timestamp; it is therefore difficult to recover details of the files history. Only an image of the originating machines file system would provide MAC times detailing creation, access, modification or deletion dates. Without this information it cannot be proven that the file was ever run, indeed, my own tests failed to even execute the application, perhaps the file does not run at all.

[10] http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001112/sch1.html

Interview Questions

The circumstances surrounding an opportunity to interview the suspect should begin with some evidence to indicate this individual above others. Perhaps audit logs or modem logs, or the user found at a terminal during a detected breach. Some circumstantial evidence, at least, should place the user on the system at the time of the binaries detection.
Questions should begin vague; asking general questions about the system, how the user accesses it, and what tasks the user performs using it. Care should be taken not to reveal any detailed information on the binary at an early stage. For example:

1. Are you familiar with system X?
2. Do you access system X?
3. How do you access this system?
    a. Dial in?
    b. Web?
    c. Telnet?
    d. Citrix?
    e. Local?
4. What tasks do you perform on this system?
5. What level is your access on this system?
    a. User?
    b. Guest?
    c. Power User?
    d. Administrator?

More specific questions regarding the user's actions during the time in question should be asked. Generally the suspect should be asked if they made any modifications to the system, or installed any software.

6. What tasks did you perform on [date]?
7. Have you ever installed software on this system?
8. Did you install software on [date]?

The suspect could be shown some information regarding the program, its filename, location or permissions. An audit log could be referred to, but not shown; indicating any access to the program by the suspect has been recorded. The suspect could be asked

1. Are you familiar with this program?
2. Do you know what this program does?
3. Do you know how and when this application was installed?
4. Have you ever used this application?

At this stage it would be appropriate to provide evidence linking the user to the software, audit logs showing either access to or installation of the program would be enough. After referring to this evidence more specific questions could be asked.

1. Where did the software come from?
2. Are you/do you know 'spoof'?

And again

1. What does the program do?

2. When did you use it?
3. How did you use it?

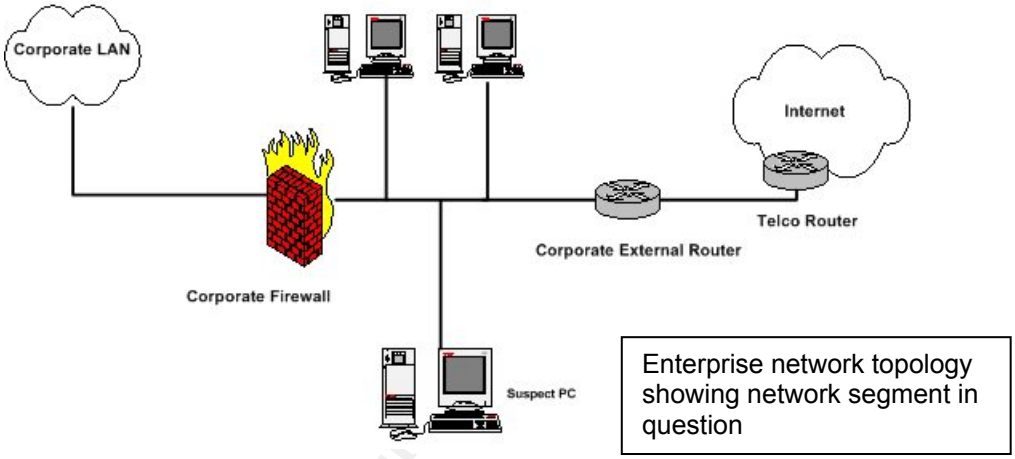
Conclusion

The file target2.exe was obtained in compressed format within a Windows Zip file named binary_v1.3.zip. It is a windows console application which was last modified, possibly compiled, on February 20th 2003. It was created using Microsoft Visual C++ IDE. Its intended use is most likely a Win32 version of the original Loki or Loki 2 applications available on the UNIX platform for many years. It is a networking application possibly installing a service which listens for ICMP_ECHO packets and manipulates the payload of ICMP packets, taking advantage of the lack of ICMP data handling standards. It manipulates Windows services, either installing a new service or replacing an existing one with a trojaned version. It was coded by a person or persons with the alias "Spoof" who most likely has some relationship with a Californian university. The application has some dependency on the Microsoft C++ libraries, and will not run without at least MFC42LOC.DLL. The file is most likely not advertised as available for download from any indexed websites.

Part 2 – Option 1: Perform Forensic Analysis On A System

Background

Our company purchases bandwidth from our telecommunications provider by the megabyte. Recently an exercise was undertaken to graph the amount of data passing through our firewall and reconciling this information with the statistics supplied by the Telco. What we found was disturbing. Between the months of January through to May 2003 there was a clear difference between the amount of data the company was being billed for the amount of data actually passing through our firewall. We keep a small internet segment between our external firewall and our egress router; it was possible that it was here that the data was travelling to and from. There are less than 5 machines in this network segment, a secondary DNS server and two or three workstations used for internet troubleshooting. One of the workstations was mine, one my manager's and one unclaimed desktop machine used by several people. I requested that I be able to take an image of the PC and perform a forensic analysis in order to determine if it was being used for any unauthorised or unintended purpose.



On Site Response

Evidence Collection

Once access to the machine had been approved it was necessary to examine the hardware configuration and put together a plan for capturing data.

The desktop machine was a HP e-Vectra, based on sales material, until I knew otherwise I assumed the specifications to be:

- Intel Pentium III 600Mhz
- 128Mb RAM
- 8Gb HDD

After image capture I physically examined the case and hard drive retrieved the following serial numbers and tagged the items as follows:

Tag # 1: Hard Drive - HP S/N D9919 – XXXXX

Tag # 2: Case - HP S/N D9898A – XXXXX

Catalogue image of HP eVectra

I found the machine to be running, and logged in as local Administrator, I performed a cursory, non obtrusive, examination by right clicking on 'My Computer' icon and selecting properties. Several pieces of general information were available for viewing from this screen; I then entered 'My Computer' and examined the drive configuration. This brief examination indicated the active OS was Windows 2000 Professional, installed on a fat32 partition approximately 8 GB in size.
At this stage I had confidence in the following facts:

- The machine was not in constant use, or the responsibility of any one individual
- The machine was running Windows 2000 Professional
- The machine was logged in as local Administrator (I therefore had very good access to the running os).
- The machine had been running for an unknown period of time.

With this information I formed the following strategy for obtaining the most information possible whilst having the minimum impact of the machine:

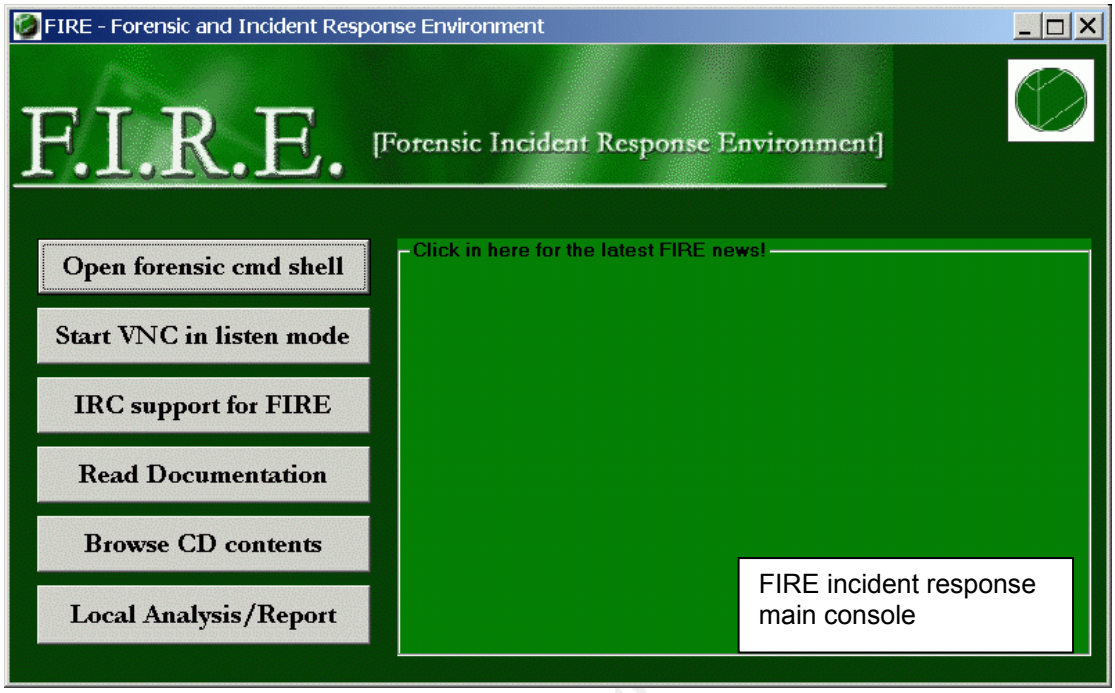
1. Image physical memory
2. Gather information on running processes
3. Power down machine and image hard drive
4. Dismantle machine and obtain drive and case serial numbers
5. Securely store machine.

In preparation I connected my Windows 2000 laptop to the internet segment and manually configured a compatible IP address 192.168.1.2[11]. I inserted the F.I.R.E CD (I had burnt two copies from the iso image) into my laptop and started a command shell by clicking the "Open forensic cmd shell" button on the main menu. The F.I.R.E CD alters the path variable to use binaries from the CD instead of the OSs normal path, this is vital when working on a possibly compromised machine. I then started netcat[12] and configured it to listen on port 40000, and to output data to a file c:\images\pc_mem.img (it's

[11] Obviously a fictitious IP address, but an important point to remember is that IP addresses in this Network Segment are public.
[12] Netcat is a hugely useful program capable of setting up adhoc network connections between hosts, enabling the no fuss transport of data www.insecure.org.

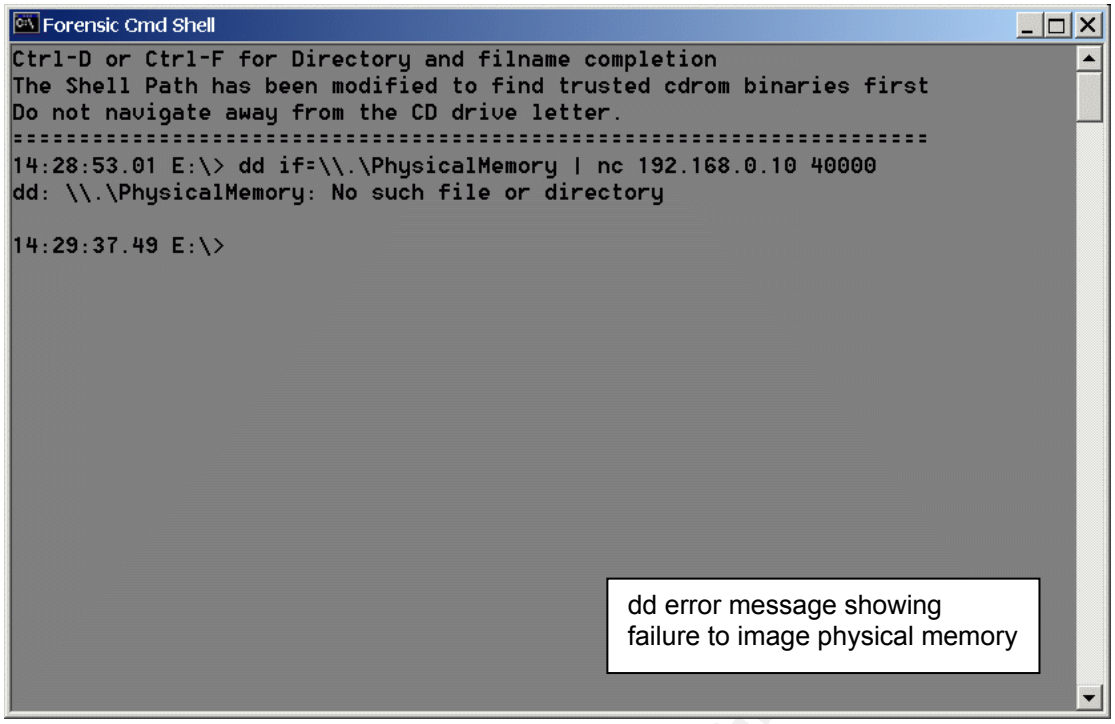
necessary to change the output file for each image). Starting and configuring netcat was done using the command

```
nc -l -p 40000 > c:\images\pc_mem.img
```



Imaging Physical Memory

My first obstacle was a compatibility issue with the tools I had chosen. It became apparent that the only version of dd ported to Windows capable of imaging physical memory was the version distributed in the Forensic Acquisition Utilities Package. The version of dd bundled with F.I.R.E is older, from the UnixUtils package, attempting to image the running machines memory using this version produced only an error.



I had prepared another CD with the Forensic Acquisition Utilities on it. The version on this CD worked perfectly, and dd performed a bit by bit copy of the memory, piping it through netcat to the forensics laptop. Once the image was safe on the notebook I obtained a hash value using md5sum.

```
c:\images>md5sum pc_mem.img > c:\images\eVectra.md5
```

Gathering information on running processes

The F.I.R.E CD provides one click reporting of a Windows operating system. Inserting a floppy disk and clicking on the local analysis/ report runs the 'Fred' batch script, this executes many command line utilities from the CD designed to produce a single file report detailing running processes, loaded dlls etc. Appendix G is the Fred script, appendix H is the report produced from the suspect machine. This script consecutively runs many forensic, and administrative command executables, in order they:

1. Output the system's current time (time /t)
2. Output the system's current date (date /t)
3. Summarise system information (Psinfo)
4. Show information on password policy (net accounts)
5. Show open files (net file)
6. Show any network sessions with other machines (net session)
7. List shared directories (net share)
8. List running services (net start)
9. List current or disconnected network connections (net use)
10. Show local accounts (net user)
11. Show any other machines in the same domain (net view)
12. Show any entries in the arp cache (Arp –a)
13. Show all listening ports, and display routing table (netstat –anr)

14. Show any logged on sessions (psloggedon)
15. List all running processes, and any dlls associated (procinterrogate –list)
16. Map listening ports to running processes (fport /p)
17. List processes in detail, record kernel itmes and thread information (pslist –x)
18. List contents of netbios name cache (nbtstat –c)
19. List hidden files on C drive (dir /s /a:h /t:a c)
20. List hidden files on D drive (**redundant**) (dir /s /a:h /t:a d)
21. List any jobs configured in the at service (at)
22. Print the finish time (time /t)
23. Print the finish date (date /t)

The script also attempted to generate md5 hash values for system directories on the machine. Unfortunately the results returned were not useful. All attempts to perform md5 hashing within the Fred script failed, this was hardly an issue though, I simply hashed the file manually, producing the following MD5 sum.
report.log MD5 hash:
1daa807267731a339adcb7410eeb71f5

Once hashed I write protected the floppy disk and stored it for later reference.

The Fred script is very convenient, saving me having to write and store separately my own batch script.

After running the report I briefly examined the output, and decided it was time to reboot the machine.

Imaging the hard drive

The machine was rebooted with the FIRE CD loaded in the drive. FIRE is bootable and runs a minimal Linux kernel providing command line and X as well as preconfigured text menus for performing networking setup and standard forensic tasks quickly.

The first task on the FIRE menu is to set up an IP address for copying data to another machine. I chose to hardcode an IP address of 192.168.1.3 before continuing on with my examination. I ran fdisk from the command line to examine the hard disk.

```
[root@FIRE root]>fdisk /dev/hda
The number of cylinders for this machine is set to 1027.  There is nothing wrong with
that, but this is larger than 1024 and could on certain setups cause problems with:
1) software that runs at boot time (eg., old versions of lilo)
2) booting and partition software from other OSs
(eg., DOS FDISK, OS/2 FDISK)

Command (m for help):p
Disk /dev/hda: 255 heads, 63 sectors, 1027 cylinders
Units = cylinders of 16055 * 512 bytes

Device  Boot    Start   End     Block   Id      System
/dev/hda1       1       2       16033+  12      Compaq Diagnostics
/dev/hda2 *     3       1027    8233312+c       Win95 FAT32 (LBA)
```

The results from this were interesting, but not altogether surprising. Compaq (HP) machines have for many years created a small hidden partition at the start of a hard drive and used it to store recovery and configuration applications. This machine had a 16Mb hidden partition which was not reported by the Fred script earlier. I would need to image and analyse this partition as well.
Prior to extracting images it was necessary to create hash values from the raw partitions. As I stated earlier, the version of dd on the FIRE CD is not as advanced as the FAU version available, the same can be said for the netcat executable. FAU netcat allows for computing hash values for data file on the fly. This is convenient and hopefully will become a feature in the future, but for now I was required to first hash the partitions on the suspect system, then compare those values to my netcated images captured to the notebook.

```
[root@FIRE root]>md5sum /dev/hda1
f319e102207902f3eec8ceeddbb792a1  /dev/hda1

[root@FIRE root]>md5sum /dev/hda2
d73412ea5ab865e55d0e7937901ed0a4  /dev/hda2
```

Using netcat I again set up my laptop to listen for data and output it to an image file. I first imaged the Compaq Utilities partition, then the actual Windows 2000 system partition.

On the laptop:
```
nc -l -p 40000 > c:\images\pc_utils.img
```

On the suspect PC:
```
dd if=/dev/hda1 | nc 192.168.1.2 40000
```

And then

On the laptop:
```
nc -l -p 40000 > c:\images\pc.img
```

On the suspect PC:
```
dd if=/dev/hda2 | nc 192.168.1.2 40000
```

With all images on the notebook I produced a file containing all md5 hash values for the e-Vectra PC.

```
[root@FIRE root]>md5sum /mnt/ext/*.img > /home/kerrm/supporting \forensic
\work/eVectra.md5
[root@FIRE root]>cat /home/kerrm/supporting \forensic \work/eVectra.md5
d73412ea5ab865e55d0e7937901ed0a4  /mnt/ext/pc.img
5d004eebc40cb78a6229bd25271a3dd9  /mnt/ext/pc_mem.img
f319e102207902f3eec8ceeddbb792a1  /mnt/ext/pc_utils.img
```

This indicates perfect copies of the two partitions from the suspect machine. With all data collected I chose to secure the PC until a decision could be made regarding its future. Small form factor PCs are convenient, in this case I was able to lock the PC in my drawer!

Offsite Image Analysis

At the forensic lab I connected the notebook to the analysis machine via crossover cable, configured an IP address and transferred the images one by one via netcat again. Once copied it was necessary to calculate and compare hash values of the images to ensure they remained unaltered by the network copy.
Using the already created md5 file, it was easy to at once calculate and compare the three images to the values in the file.

```
[kerrm@forensics ext]$ ls
lost+found  pc.img  pc_mem.img  pc_utils.img
[kerrm@forensics ext]$ md5sum --check /home/kerrm/supporting \forensic
\work/eVectra.md5
/mnt/ext/pc.img: OK
/mnt/ext/pc_mem.img: OK
/mnt/ext/pc_utils.img: OK
```

I had loaded the images onto a dedicated partition. I could further ensure their integrity during the investigation by modifying the fstab table to mount the dedicated partition in read only mode on start up. Appendix J shows the modified fstab file directing /dev/hdd2 to be mounted read only (ro) to /mnt/ext on start up. After a reboot the images were now ready and the analysis began.

Analysis of Reports

My first step was to examine the FRED report and gain preliminary information which may provide some clues on the machines current activity. The following is excerpts of the report, with brief explanations. The entire report is included as Appendix H.

```
FRED v1.1 - 2 April 2002 [modified for fire 10/2002]


-------------------------------------------------
START TIME
-------------------------------------------------
11:50a
Fri 05/02/2003


-------------------------------------------------
PSINFO
-------------------------------------------------

PsInfo v1.31 - local and remote system information viewer
Copyright (C) 2001-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Querying information for ...

System information for \\HP1:
Uptime:                    1 day, 1 hour, 14 minutes, 0 seconds
Kernel version:            Microsoft Windows 2000, Uniprocessor Free
Product type:              Professional
Product version:           5.0
Service pack:              2
Kernel build number:       2195
Registered organization:
Registered owner:          administrator
Install date:              5/10/2000, 3:46:07 PM
IE version:                6.0000
System root:               C:\WINNT
```

```
Processors:                1
Processor speed:           605 MHz
Processor type:            Intel Pentium III
Physical memory:           126 MB
Volume Type       Format     Label                       Size       Free   Free
    A: Removable  FAT                                   1.4 MB     1.4 MB   100%
    C: Fixed      FAT32      ATRYP00ABK                 7.8 GB     5.2 GB    66%
    E: CD-ROM     CDFS       FIRE-0.3.5b              220.1 MB                0%
```

This information is very generic; it does little other than to confirm my original assumptions regarding the machine specification. It does however show the installation date of 10th of June 2000. Note that the Compaq diagnostic partition is not listed here; it is marked as hidden and is not visible to Windows.

```
-------------------------------------------------
NET SHARE
-------------------------------------------------

Share name   Resource                        Remark


-------------------------------------------------------------------------------
ADMIN$       C:\WINNT                        Remote Admin
C$           C:\                             Default share
IPC$                                         Remote IPC
The command completed successfully.
```

These shares are all automatically created by the operating system, there is nothing unexpected here.

```
-------------------------------------------------
NET START
-------------------------------------------------
These Windows 2000 services are started:


   COM+ Event System
   Computer Browser
   DHCP Client
   Distributed Link Tracking Client
   Event Log
   IPSEC Policy Agent
   Logical Disk Manager
   Messenger
   Network Connections
   Plug and Play
   Print Spooler
   Protected Storage
   Remote Access Connection Manager
   Remote Procedure Call (RPC)
   Remote Registry Service
   Removable Storage
   RunAs Service
   Security Accounts Manager
   Server
   Still Image Service
   System Event Notification
   Task Scheduler
   TCP/IP NetBIOS Helper Service
   Telephony
   Windows Management Instrumentation
   Windows Management Instrumentation Driver Extensions
   WMDM PMSP Service
   Workstation

The command completed successfully.
```

These are all Windows 2000 services. Note however the "Still Image Service", it is a Microsoft service, but is only installed when an usb imaging device such as Digital Camera or Scanner is attached to the machine. Therefore, at some stage this machine has been attached to an imaging device. With this in mind it will be worthwhile conducting a thorough image search later on in the analysis.

```
-------------------------------------------------
NET USER
-------------------------------------------------

User accounts for \\HP1


-------------------------------------------------------------------------------
Administrator            Fooman                   Guest
The command completed successfully.
```

Fooman doesn't sound like a corporate account. This is a local account, as this machine is not a member of any domain it is reasonable to expect someone to create their own account. I made a note to examine the user directory later.

```
-------------------------------------------------
LOGGED ON
-------------------------------------------------

PsLoggedOn v1.21 - Logon Session Displayer
Copyright (C) 1999-2000 Mark Russinovich
SysInternals - www.sysinternals.com

Users logged on locally:
     5/1/2003 10:37:24 AM    HP1\Administrator

No one is logged on via resource shares.
```

This is good.

```
-------------------------------------------------
ProcInterrogate
-------------------------------------------------
ProcInterrogate Version 0.0.1 by Kirby Kuehl vacuum@users.sourceforge.net
-------------------------------------------------------------------------

-------------------------------------------------------------------------
C:\WINNT\System32\smss.exe (Process ID: 140)
-------------------------------------------------------------------------
C:\WINNT\System32\winlogon.exe (Process ID: 160)
-------------------------------------------------------------------------
C:\WINNT\System32\services.exe (Process ID: 212)
-------------------------------------------------------------------------
C:\WINNT\System32\lsass.exe (Process ID: 224)
-------------------------------------------------------------------------
C:\WINNT\System32\svchost.exe (Process ID: 384)
-------------------------------------------------------------------------
C:\WINNT\System32\spoolsv.exe (Process ID: 412)
-------------------------------------------------------------------------
C:\WINNT\System32\svchost.exe (Process ID: 444)
-------------------------------------------------------------------------
C:\WINNT\System32\regsvc.exe (Process ID: 480)
-------------------------------------------------------------------------
C:\WINNT\System32\MSTask.exe (Process ID: 496)
-------------------------------------------------------------------------
C:\WINNT\System32\stisvc.exe (Process ID: 524)
-------------------------------------------------------------------------
C:\WINNT\System32\Wbem\WinMgmt.exe (Process ID: 572)
-------------------------------------------------------------------------
C:\WINNT\System32\mspmspsv.exe (Process ID: 592)
-------------------------------------------------------------------------
C:\WINNT\Explorer.EXE (Process ID: 792)
```

```
---------------------------------------------------------------------------
popupkiller.EXE (Process ID: 852)
---------------------------------------------------------------------------
qttask.exe (Process ID: 864)
---------------------------------------------------------------------------
SETI@home.exe (Process ID: 880)
---------------------------------------------------------------------------
E:\win32\fire.exe (Process ID: 936)
---------------------------------------------------------------------------
E:\win32\cmd.exe (Process ID: 1172)
---------------------------------------------------------------------------
E:\win32\procinterrogate.exe (Process ID: 1156)
```

Procinterrogate lists alls executables currently running. It also lists any DLLS in use by the exe, but here I've removed them for readability. Most of the exes here are from Windows, but also listed are; a pop up ad killer, the Quicktime tray launcher, SETI@home, the FIRE CD (in use by me), our trusted cmd binary from the CD and procinterrogate itself.

```
-------------------------------------------------
FPORT (fport /p)
-------------------------------------------------
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com


Pid   Process            Port  Proto Path
384   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  445   TCP
496   MSTask         ->  1025  TCP   C:\WINNT\system32\MSTask.exe
8     System         ->  1028  TCP

384   svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System         ->  445   UDP
212   services       ->  1027  UDP   C:\WINNT\system32\services.exe
792   Explorer       ->  1088  UDP   C:\WINNT\Explorer.EXE
936   fire           ->  1142  UDP   E:\win32\fire.exe
```

Fport lists very few open ports listening, this is also a relief. The last entry, fire, is my toolkit.

Memory Image Interrogation

I found the memory image file unmountable. To examine it I created a strings file from the image and perused the contents for suspicious text. The command used was

```
[kerrm@forensics kerrm]$ strings pc_mem.img > mem_strings
```

The output of which was over 10Mb of pure text. To make the file more manageable the strings file was grepped, looking for instances of ".exe". This would give a good indication of applications which were in some way associated with the machine.

```
[kerrm@forensics kerrm]$ fgrep -e exe -i -n mem_strings > fgrepped_mem_strings
```

Fgrep, with these options performed a case insensitive search for instances of exe, outputting the matching line with their original line number into a new file, fgrepped_mem_strings.
Viewing this file was much easier, and almost immediately gratifying. Held in memory were references to dozens of non OS related executables. Common

downloads such as SETI, game demos and possibly warez-like files were also mentioned. The following sample output shows executable names of game demos, and the Microsoft Direct X 8 distribution for Windows 2000, necessary to play most modern 3D games. It would not be likely these files were downloaded for any business reason.

```
100719:DX80NTeng.exe
100720:DX80NT~1.EXE
100724:LegendsFirstLook.exe
100725:LEGEND~1.EXE
100746:setiathome_win_3_03.exe
100747:SETIAT~1.EXE
100750:startrekawayteamdemo.exe
100751:STARTR~1.EXE
100753:thmpls410_s.exe
100754:THMPLS~1.EXE
100758:winzip80.exe
100788:Tribes2.exe
100789:TRIBES2.EXE
100790:UNWISE.EXE
102531:"C:\Program Files\SETI@home\SETI@home.exe" -min
102725:arcanum_en_1074.exe
```

The internal workings of an application can be very handy to a forensic investigation. The win32 function FindExecutableImage and FindExecutableImageEx are both called by an application wishing to find all executables in a given location[13]. The following output from the grepped strings file show a call to both FindExecutableImage and FindExecutableImageex which in turn lists all executables from the a directory. Note the seti@home exe, and the BRYCE_~1EXE entry, probably Bryce 3D. Also in this list is eye.exe, this is probably the All Seeing Eye from Udpsoft[14], a multiplayer game server browser.

```
849847:FindExecutableImage
849848:FindExecutableImageEx
851035:SYSOCMGREXE
851053:TWUNK_16EXE
851057:TWUNK_32EXE
851081:VCMD    EXE
851086:MSTASK  EXE
851100:ODBCAD32EXE
851102:ODBCCONFEXE
851107:WINLOGONEXE
851111:WJVIEW  EXE
851127:UNREGMP2EXE
851137:ACCWIZ  EXE
851401:SETI@HOME.EXE
851663:MSIEXEC EXE
851668:MRINFO  EXE
851670:MSINFO32EXE
851689:MSPAINT EXE
851692:PROCTEXEOCX
851703:MSCDEXNTEXE
851706:MSSWCHX EXE
851713:MSTINIT EXE
851717:MSDTC   EXE
851748:MWCLOAD EXE
851750:MWCLOADWEXE
851757:NETDDE  EXE
851758:MWCPYRT EXE
851759:MWCSW32 EXE
851761:MWMDMSVCEXE
```

[13] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/findexecutableimage.asp
[14] http://www.udpsoft.com/eye2/index.html

```
851768:MWRCOV16EXE
851770:MWREMINDEXE
851772:MWSSW32 EXE
851784:NARRATOREXE
854194:C:\WINNT\System32\cmd.exe
854397:BRYCE_~1EXE
854403:KMD171~1EXE
854405:OLWAR~1EXE
855215:RAR     EXE
855218:UNINST~1EXE
855219:UNRAR   EXE
855221:WINRAR  EXE
855726:AUTOEXECBAT 4.0
857597:_execvp
857788:NBTSTAT EXE
857790:NLSFUNC EXE
857796:NDDEAPIREXE
857802:NOTEPAD EXE
857804:NSLOOKUPEXE
857808:NPPAGENTEXE
857818:NET     EXE
857821:NET1    EXE
857831:NTDSUTILEXE
857842:NTSD    EXE
857853:NTVDM   EXE
857869:NW16    EXE
857875:NWSCRIPTEXE
857883:OSK     EXE
857884:PACKAGEREXE
857892:NETSH   EXE
857901:NETSTAT EXE
857904:PRINT   EXE
858922:_18be6784.exe
858937:Slingo.exe
861017:SMSS    EXE
861116:eye.exe
861307:BSC4.exe
861862:WINMSD  EXE
861876:WINSPOOLEXE
861884:WINVER  EXE
861889:WANGIMG EXE
861892:WORDPAD EXE
861894:WOWDEB  EXE
861895:WOWEXEC EXE
861896:WB32    EXE
861898:WPNPINSTEXE
861903:WRITE   EXE
861914:WSCRIPT EXE
861923:XCOPY   EXE
861928:WABMIG  EXE
861929:WUPDMGR EXE
861932:MSIMN   EXE
861936:WBEMTESTEXE
861939:OEMIG50 EXE
861941:WELCOME EXE
861942:WEXTRACTEXE
861947:WINCHAT EXE
861949:WINHELP EXE
861951:SETUP50 EXE
861977:WAB     EXE
863490:CMSTP   EXE
863503:COMPACT EXE
863506:COMP    EXE
863507:CDPLAYEREXE
863515:COMCLUSTEXE
863522:CONF    EXE
863523:CHARMAP EXE
863526:COMREPL EXE
863529:COMREREGEXE
863532:CLUSTER EXE
863537:CONIME  EXE
863540:CONTROL EXE
863542:CONVERT EXE
863544:CONVLOG EXE
863548:CIDAEMONEXE
863559:CMD     EXE
863566:CSRSS   EXE
```

```
863571:CIPHER  EXE
863576:CISVC   EXE
863580:CKCNV   EXE
863585:DDESHAREEXE
863586:DDMPRXY EXE
863594:DCOMCNFGEXE
863600:DFRGFAT EXE
863603:DFRGNTFSEXE
863606:DEBUG   EXE
863607:DPLAYSVREXE
863608:CLEANMGREXE
863614:CLIPBRD EXE
863618:CLIPSRV EXE
863623:CLSPACK EXE
863634:DISKPERFEXE
863639:DLLHOST EXE
863642:DLLHST3GEXE
863645:DMADMIN EXE
863647:DIALER  EXE
863648:DIANTZ  EXE
863649:IE4UINITEXE
863655:DISCOVEREXE
863656:CMDL32  EXE
863764:COGS_1~1EXE
864542:eXeh
```

My initial impressions are that there have been or still are non work related files on this machine, some of them, such as game demos, or the SETI daemon are capable of consuming large amounts of bandwidth and may be responsible for our traffic discrepancy. At this stage I didn't know if the files had simply been downloaded, or were in fact installed on the machine.

C Drive Image Interrogation

Before utilising the Sleuthkit I did some simple searches to look for anything which could provide quick clues to help the investigation. The partition storing the image files was already mounted read only; therefore it was a simple matter to mount the drive image in loop back mode to gain access to the file system without compromising the integrity on the image

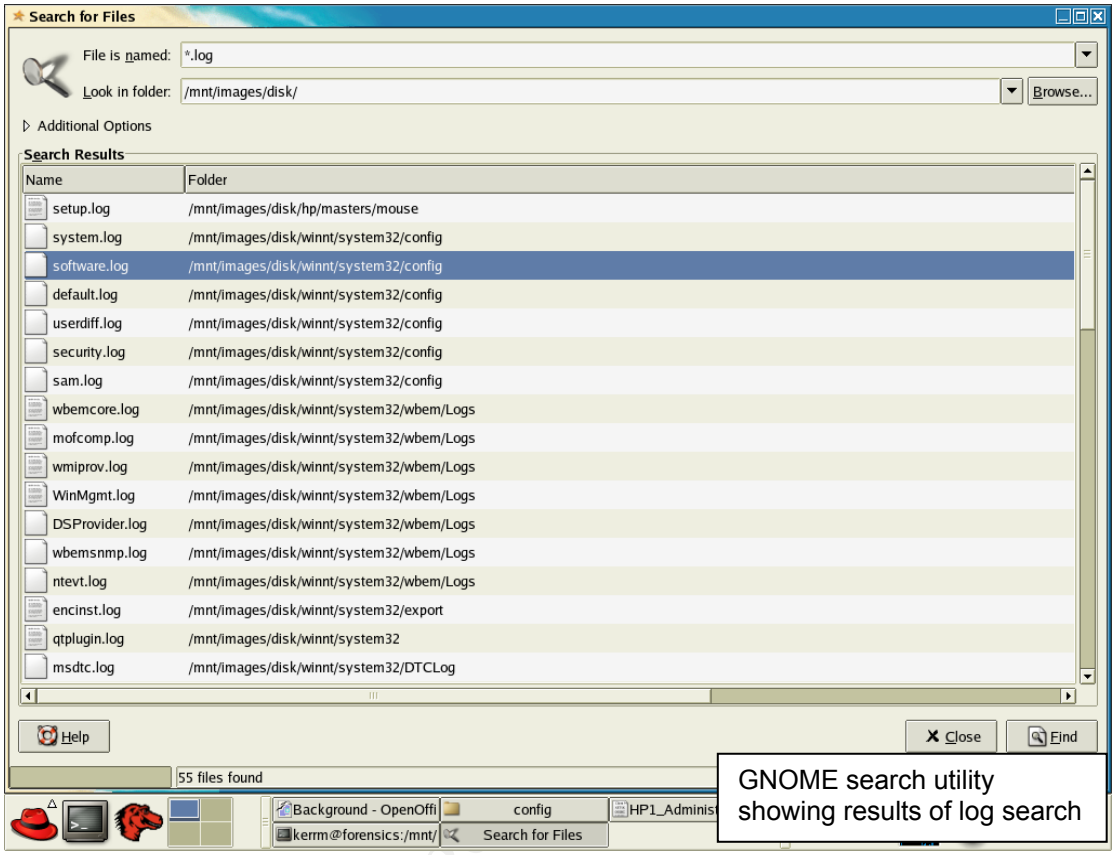
```
[kerrm@forensics kerrm]$ mount -t vfat -o loop /mnt/ext/pc.img /mnt/images/disk
```

I performed several high level searches, similar to what I would do if I was operating within the OS, as well as a couple of tricks I couldn't do in Windows as well. My method was:

- Search for .log files, follow clues
- Search for .txt files, follow clues
- Search for EXEs, follow clues
- View contents of recycle bin
- Extract strings from internet history files (index.dat)
- Examine cookies

Search for Log Files

From the Gnome Find utility it was trivial to search for some easy sources of information. My first search was for the term *.log, this returned over 50 matches.



GNOME search utility showing results of log search

The search returned these files:

```
/mnt/images/disk/hp/masters/mouse/setup.log
/mnt/images/disk/winnt/system32/config/system.log
/mnt/images/disk/winnt/system32/config/software.log
/mnt/images/disk/winnt/system32/config/default.log
/mnt/images/disk/winnt/system32/config/userdiff.log
/mnt/images/disk/winnt/system32/config/security.log
/mnt/images/disk/winnt/system32/config/sam.log
/mnt/images/disk/winnt/system32/wbem/Logs/wbemcore.log
/mnt/images/disk/winnt/system32/wbem/Logs/mofcomp.log
/mnt/images/disk/winnt/system32/wbem/Logs/wmiprov.log
/mnt/images/disk/winnt/system32/wbem/Logs/WinMgmt.log
/mnt/images/disk/winnt/system32/wbem/Logs/DSProvider.log
/mnt/images/disk/winnt/system32/wbem/Logs/wbemsnmp.log
/mnt/images/disk/winnt/system32/wbem/Logs/ntevt.log
/mnt/images/disk/winnt/system32/export/encinst.log
/mnt/images/disk/winnt/system32/qtplugin.log
/mnt/images/disk/winnt/system32/DTCLog/msdtc.log
/mnt/images/disk/winnt/system32/QuickTime/Uninstall.log
/mnt/images/disk/winnt/repair/setup.log
/mnt/images/disk/winnt/security/logs/scesetup.log
/mnt/images/disk/winnt/security/logs/backup.log
/mnt/images/disk/winnt/security/logs/scesrv.log
/mnt/images/disk/winnt/security/res2.log
/mnt/images/disk/winnt/security/res1.log
/mnt/images/disk/winnt/security/edb.log
/mnt/images/disk/winnt/security/edb00004.log
```

```
/mnt/images/disk/winnt/Debug/UserMode/userenv.log
/mnt/images/disk/winnt/Debug/passwd.log
/mnt/images/disk/winnt/Debug/oakley.log
/mnt/images/disk/winnt/Debug/ipsecpa.log
/mnt/images/disk/winnt/wmsetup.log
/mnt/images/disk/winnt/setupact.log
/mnt/images/disk/winnt/setuperr.log
/mnt/images/disk/winnt/iis5.log
/mnt/images/disk/winnt/comsetup.log
/mnt/images/disk/winnt/ockodak.log
/mnt/images/disk/winnt/ocgen.log
/mnt/images/disk/winnt/mmdet.log
/mnt/images/disk/winnt/setupapi.log
/mnt/images/disk/winnt/COM+.log
/mnt/images/disk/winnt/Directx.log
/mnt/images/disk/winnt/DtcInstall.log
/mnt/images/disk/winnt/Sti_Trace.log
/mnt/images/disk/winnt/imsins.log
/mnt/images/disk/winnt/coder.log
/mnt/images/disk/winnt/svcpack.log
/mnt/images/disk/winnt/Windows Update.log
/mnt/images/disk/Documents and Settings/All
/mnt/images/diskUsers/Documents/DrWatson/drwtsn32.log
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Application
Data/Identities/{7BFA2DFB-B5B6-497B-A008-9996A0C2600C}/Microsoft/Outlook
Express/cleanup.log
/mnt/images/disk/Program Files/Thumbs4/install.log
/mnt/images/disk/Program Files/WindowsUpdate/wuhistv3.log
/mnt/images/disk/Program Files/install.log
/mnt/images/disk/Program Files/Lavasoft Ad-Aware/install.log
/mnt/images/disk/Program Files/SpyBlocker Software/UnInst.log
/mnt/images/disk/games/Microsoft Golf 2001/crash.log
```

We can see here many Windows related log files, but at least seven stand out.

Firstly winnt/IIS.log indicates this machine had at one time IIS installed and running. Running the tail command on this file indicates it has not been active for some time, the 26th of November in 2001 in fact.

```
[root@forensics images]# tail /mnt/images/disk/winnt/iis5.log
[11/26/2001 16:48:48] OC_CLEANUP:Final Check:OC_NEED_MEDIA Called=0
[11/26/2001 16:48:48] OC_CLEANUP:Final Check:OC_NOTIFICATION_FROM_QUEUE
Called=0[11/26/2001 16:48:48] OC_CLEANUP:Final Check:OC_QUERY_STEP_COUNT Called=0
[11/26/2001 16:48:48] OC_CLEANUP:Final Check:OC_ABOUT_TO_COMMIT_QUEUE Called=0
[11/26/2001 16:48:48] OC_CLEANUP:Final Check:OC_FILE_BUSY Called=0
[11/26/2001 16:48:48] OC_CLEANUP:Final Check:OC_COMPLETE_INSTALLATION Called=0
[11/26/2001 16:48:48] OC_CLEANUP:Final Check:OC_CLEANUP Called=1
[11/26/2001 16:48:48] OC_CLEANUP:Final Check:OC_DEFAULT Called=0
[11/26/2001 16:48:48] OC_CLEANUP:Final Check:RtlValidateHeap(): Good.
[11/26/2001 16:48:48] OC_CLEANUP:Final Check:LogFile Close.
```

Secondly, the file install.log has been just dumped in the Program Files directory; this alone draws attention to it. Running tail on this log produces this output

```
[root@forensics images]# tail disk/Program\ Files/install.log
***  Installation Started 08/28/2001 14:36  ***
Title: Virtua Girl Installation
Source: E:\MODRIV~9\NAUGHTY\VIRTUA~A\VIRGIRL\ADDON_~3\STRIP.EXE | 07-21-2001 |
21:24:36 | 2324647
Installation Aborted!
```

Virtua Girl is a popular piece of free software, and also a well known Trojan. This log file indicates the installation was aborted for some reason, this is good. Interestingly enough the installation seems to have been run from a CD.

Next, the file /mnt/images/disk/games/Microsoft Golf 2001/crash.log of course indicates that games have been installed on this machine (already suggested by the presence of a DirectX setup log as well).

Many of the Windows logs in the security and debug directories are empty (I would need to check the MAC times later to detect any unexpected modifcation), but one /winnt/Debug/NetSetup.log has some interesting information. This log shows the process of a machine joining and rejoining the workgroup named "workgroup" three times, each as a different machine name. The machine started out as HP-6DDLBKHXXXXX, was renamed EVECTRA01 and then finally HP1. Was this an attempt to assume some anonaminity? The full log is attached as Appendix I.

The file /winnt/coder.log provided some alarming information. Running tail on this file produces only two lines.

```
www.hacker.ag  03/13/03 15:49:36     dialer start
www.hacker.ag  04/09/03 12:04:15     dialer start
```

This indicates some type of dialling software, which, although the machine has no modem, could be a real problem and deserves more investigation. Next I browsed to the location of the log file in the file manager, and found that in addition to the log file there was also an ini file and a directory by the same name. The directory was empty, but the contents of the ini file were as follows;

```
[cfg]
country=3
ln_2-hags-1-0-.exe=2-hags-1-0-
user=CILABYALZRJHDOSVWAXEFWYNDJXXXX
modem=
prefix=
tone=yes
```

A visit to the www.hacker.ag website showed the site to be offering cracked software, keys and tuition in hacking techniques. The visitor is required to disconnect from the internet and reconnect using the dialup software. The service is charged by the minute. The user on this machine probably did not realise they would require a modem to use the software, after running it once deleted it. The coder.log file supports this theory, with only two entries.

Not a concern, but of note is the Ad-aware and Spy Blocker installation logs. This indicates the user was trying to clean the machine and may have already dealt with the above software, which would also explain why there is no executable. I made a note to attempt to recover the "hag" exe later on.

Search for Text Files

My next search was for text files in general. This search returned over nine hundred results. I was able to quickly eliminate many of these as Microsoft files by their location in the i386 directory, which contained the Windows 2000

installation files. This was of course pending the examination later on in Autopsy. The search for text files also returned all user's cookies. I could ignore them for the moment, as they would be the subject of my next search. The remainder were almost entirely application readme files, data files or License files. Again, this search indicated the installation of several game demos. The following is a sample of the returned search:

```
 1.0/cogsdata/lists.txt
/mnt/images/disk/Program Files/GameArena/COGS 1.0/cogsdata/sounds/cogs.txt
/mnt/images/disk/Program Files/GameArena/COGS 1.0/readme.txt
/mnt/images/disk/Program Files/GameArena/COGS 1.0/development.txt
/mnt/images/disk/Program Files/Winamp/whatsnew.txt
/mnt/images/disk/Program Files/Winamp/readme.txt
/mnt/images/disk/Program Files/Thumbs4/readme.txt
/mnt/images/disk/Program Files/The All-Seeing Eye/filters.txt
/mnt/images/disk/Program Files/The All-Seeing Eye/countries.txt
/mnt/images/disk/Program Files/The All-Seeing Eye/history.txt
/mnt/images/disk/Program Files/The All-Seeing Eye/buddylog.txt
/mnt/images/disk/Program Files/Lionhead Studios Ltd/Black & White/unin.txt
/mnt/images/disk/Program Files/Lionhead Studios Ltd/Black & White/MemoryLeaks.txt
/mnt/images/disk/Program Files/The Playa/PLAYA-LICENSE.txt
/mnt/images/disk/Program Files/The Playa/README-PLAYA.txt
/mnt/images/disk/Program Files/WinRAR/ReadMe.txt
/mnt/images/disk/Program Files/WinRAR/License.txt
/mnt/images/disk/Program Files/WinRAR/Rar.txt
/mnt/images/disk/Program Files/WinRAR/Rar_Site.txt
/mnt/images/disk/Program Files/WinRAR/Register.txt
/mnt/images/disk/Program Files/WinRAR/TechNote.txt
/mnt/images/disk/Program Files/WinRAR/UnrarSrc.txt
/mnt/images/disk/Program Files/WinRAR/WhatsNew.txt
/mnt/images/disk/Program Files/WindowsUpdate/v4/iuident.txt
/mnt/images/disk/Program Files/Adobe/Acrobat 5.0/Reader/Optional/readme.txt
/mnt/images/disk/Program Files/Adobe/Acrobat 5.0/Reader/Legal/License.txt
/mnt/images/disk/Program Files/DivXCodec/license.txt
/mnt/images/disk/Program Files/DivXCodec/readme.txt
/mnt/images/disk/Program Files/Lavasoft Ad-Aware/License Agreement.txt
/mnt/images/disk/Program Files/Lavasoft Ad-Aware/Readme.txt
/mnt/images/disk/Program Files/Lavasoft Ad-Aware/ad-aware log29-08-02-151103.txt
/mnt/images/disk/Program Files/SpyBlocker Software/agreement.txt
 Software/pone.txt
/mnt/images/disk/Program Files/SpyBlocker Software/readme.txt
/mnt/images/disk/Program Files/SpyBlocker Software/License.txt
/mnt/images/disk/Program Files/WinMX/license.txt
/mnt/images/disk/Sierra/Arcanum/Documents/portrait.txt
/mnt/images/disk/Sierra/Arcanum/PatchReadme.txt
/mnt/images/disk/Sierra/Arcanum/Version.txt
/mnt/images/disk/Sierra/Arcanum/EULA PATCH.txt
/mnt/images/disk/Test/incomplete downloads.txt
/mnt/images/disk/Kazaa/XXXXXXXXXXXX_key.txt
```

This list show's lots of game directories, as well as the All Seeing Eye there is also a directory for COGS, another game server management application. The last entry shows a download directory for the Peer to Peer application Kazaa. If Kazaa has been running on this machine it could definitely be related to our bandwidth issues. Later I would try to find the Kazaa executable.

Search for Executables

Using the same method I searched for files with an EXE extension. Again a huge list was returned, over nine hundred. I quickly discounted Windows exes for the moment, focussing on large files such as installers and looking for some of the applications I believed existed somewhere. Finding many of

the installation files was surprisingly easy; at least one copy still resided in the Administrators temporary internet files directory. Sections of the search results are printed here. The first section shows a selection of installers, the second section shows some of the garbage installed into the Program files directory. File types include more games, Seti@home, the COGS application and the All Seeing Eye, as well as another dialler called "hotporn.exe", charming. Listed also is the installer for Kazaa 1.71, and another installed peer to peer application called winmx. Kazaa itself seems to be uninstalled. Also in the Administrators profile was the hackers.ag "hag" dialler setup. If I had more time it would make an interesting binary analysis.

```
/mnt/images/disk/winnt/Windows Update Setup Files/ie6setup.exe
/mnt/images/disk/Documents and Settings/Administrator/Local
Settings/Temp/pft20F~tmp/Reader/AcroRd32.exe
/mnt/images/disk/Documents and Settings/Administrator/Local
Settings/Temp/pft20F~tmp/Setup.exe
/mnt/images/disk/Documents and Settings/Administrator/Local
Settings/Temp/pft20F~tmp/_ISDel.exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temp/setup_wm.exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temporary
Internet Files/Content.IE5/0ssbo0es/movenrun[1].exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temporary
Internet Files/Content.IE5/s7ynavi1/SP20953[1].exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temporary
Internet Files/Content.IE5/wxurod2j/QuickTimeInstaller[1].exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temporary
Internet Files/Content.IE5/ghct0zw1/SP19474[1].exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temporary
Internet Files/Content.IE5/ghct0zw1/EyeInstaller[1].exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temporary
Internet Files/Content.IE5/65grgjw9/cogs[1].exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temporary
Internet Files/Content.IE5/wd2r05un/ar500enu[1].exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temporary
Internet Files/Content.IE5/kxa3otaj/SP21494[1].exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temporary
Internet Files/Content.IE5/kxa3otaj/Hacker AG SE(2-hags-1-0-#)[1].exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temporary
Internet Files/Content.IE5/mriruny9/SP20954[1].exe
/mnt/images/disk/Documents and Settings/Administrator/Local Settings/Temporary
Internet Files/Content.IE5/xrvfhtse/cogs[1].exe
/mnt/images/disk/Documents and Settings/Administrator/My
Documents/setiathome_win_3_0.exe
/mnt/images/disk/Documents and Settings/Administrator/My Documents/wmp7.exe


/mnt/images/disk/Program Files/WinZip/wzsepe32.exe
/mnt/images/disk/Program Files/WinZip/winzip32.exe
/mnt/images/disk/Program Files/GameArena/COGS 1.0/cogs.exe
/mnt/images/disk/Program Files/GameArena/COGS 1.0/movenrun.exe
/mnt/images/disk/Program Files/QuickTime/qttask.exe
/mnt/images/disk/Program Files/QuickTime/QuickTimeUpdater.exe
/mnt/images/disk/Program Files/QuickTime/QTInfo.exe
/mnt/images/disk/Program Files/QuickTime/QuickTimePlayer.exe
/mnt/images/disk/Program Files/QuickTime/Plugins/DeleteMe1.exe
/mnt/images/disk/Program Files/Winamp/Winamp.exe
/mnt/images/disk/Program Files/Sierra On-Line/SIGSPat.exe
/mnt/images/disk/Program Files/Thumbs4/unwise.exe
/mnt/images/disk/Program Files/Thumbs4/Thumbs.exe
/mnt/images/disk/Program Files/Thumbs4/helpshel.exe
/mnt/images/disk/Program Files/Thumbs4/TPView.exe
/mnt/images/disk/Program Files/The All-Seeing Eye/movenrun.exe
/mnt/images/disk/Program Files/The All-Seeing Eye/eye.exe
/mnt/images/disk/Program Files/The Playa/uninstall.exe
/mnt/images/disk/Program Files/The Playa/ThePlaya.exe
/mnt/images/disk/Program Files/The Playa/validator.exe
/mnt/images/disk/Program Files/WinRAR/Rar.exe
/mnt/images/disk/Program Files/WinRAR/Uninstall.exe
/mnt/images/disk/Program Files/WinRAR/UnRAR.exe
/mnt/images/disk/Program Files/WinRAR/WinRAR.exe
/mnt/images/disk/Program Files/DiallerProgram/hotporn.exe
```

```
/mnt/images/disk/Program Files/Adobe/Acrobat 5.0/Reader/AcroRd32.exe
/mnt/images/disk/Program Files/DivXCodec/uninstall.exe
/mnt/images/disk/Program Files/Adaptec/Shared/ECDC Engine/wmburn.exe
/mnt/images/disk/Program Files/My application/C-a-s-i-n-o.exe
/mnt/images/disk/Program Files/My application/dome.exe
/mnt/images/disk/Program Files/Lavasoft Ad-Aware/unwise.exe
/mnt/images/disk/Program Files/Lavasoft Ad-Aware/Ad-aware.exe
/mnt/images/disk/Program Files/Lavasoft Ad-Aware/Ad-watch.exe
/mnt/images/disk/Program Files/Lavasoft Ad-Aware/lvdel.exe
/mnt/images/disk/Program Files/SpyBlocker Software/sbuninst.exe
/mnt/images/disk/Program Files/SpyBlocker Software/spyblocker.exe
/mnt/images/disk/Program Files/SpyBlocker Software/regdns.exe
/mnt/images/disk/Program Files/PopUp Killer/PopUpKiller.exe
/mnt/images/disk/Program Files/WinMX/WinMX.exe
/mnt/images/disk/Program Files/WinMX/uninstall.exe
/mnt/images/disk/Program Files/KaZaA/My Shared Folder/XXXXXXXXX.exe
/mnt/images/disk/Program Files/KaZaA/My Shared Folder/XXXXXXXXX.exe
/mnt/images/disk/Downloads/mp71.exe
/mnt/images/disk/Downloads/quicktime/QuickTime403/QuickTimeInstaller.exe
/mnt/images/disk/Downloads/quicktime/QuickTimeInstaller.exe
/mnt/images/disk/Downloads/setiathome_win_3_03.exe
/mnt/images/disk/Downloads/kmd.exe
/mnt/images/disk/Downloads/network/Netboot_detectcards.exe
/mnt/images/disk/Downloads/DivX4FullInstaller.exe
/mnt/images/disk/Downloads/ydsxgw9x/audio/yamaha/Win9X/dsuninst.exe
/mnt/images/disk/Downloads/ydsxgw9x/audio/yamaha/Win9X/setup.exe
/mnt/images/disk/Downloads/ydsxgw9x/audio/yamaha/Win9X/_isdel.exe
/mnt/images/disk/Downloads/arcanum30.exe
/mnt/images/disk/Downloads/puksetup.exe
/mnt/images/disk/Downloads/arcanum_en_1074.exe
/mnt/images/disk/Downloads/QTrax/setup.exe
/mnt/images/disk/Downloads/sb/spyblock.exe
/mnt/images/disk/Downloads/XXXXXXX.exe
/mnt/images/disk/Downloads/RealArcade.exe
/mnt/images/disk/Downloads/setiathome_win_3_07.exe
/mnt/images/disk/Downloads/lego chess.exe
/mnt/images/disk/Downloads/cogs-1.0-setup.exe
/mnt/images/disk/Kazaa/BRYCE_5.exe
/mnt/images/disk/Kazaa/kmd171gu_en.exe
```

View Recycle Bin

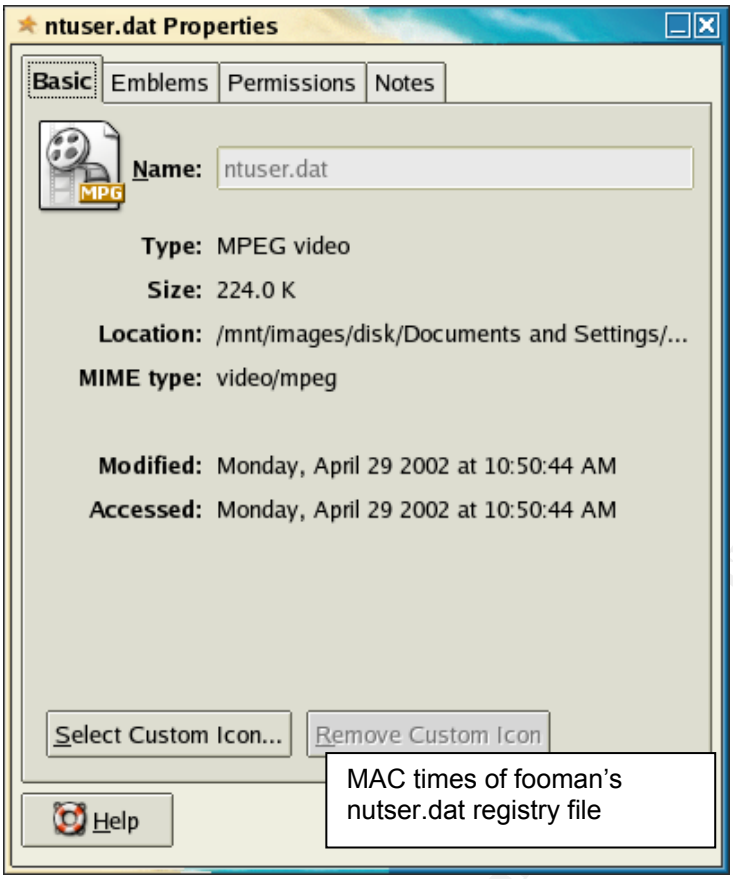
Next I viewed the contents of /mnt/images/disk/Recycled. Disappointingly, the recycle bin was empty, and looked as if it had been recently emptied. I made a note to examine it again later in Autopsy.

Extract Strings from Internet History Data files

Within the "Documents and Settings" directory is a directory for each user that has logged onto this machine.

```
[kerrm@forensics kerrm]$ cd /mnt/images/disk/Documents\ and\ Settings/
[kerrm@forensics Documents and Settings]$ ls
Administrator  All Users  Default User  fooman
```

The Documents and Settings folder contained four directories. All Users is for sharing common settings across all users. The Default User directory is copied each time a new user logs onto the machine. The directories Administrator and fooman are actual user directories, containing tmp files, internet history, start menu and individual registry information for the user. Firstly, from the Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5 directory I created a strings file from the index.dat file. This file shows in text format the history of requested



web sites by this user. The following command was used to create the text file of the Administrators history file.

```
[kerrm@forensics Content.IE5]$ strings index.dat > /home/kerrm/supporting\ forensic\
work/Administrator_index_dat_strings.txt
```

And the same from fooman's Content.IE5 directory

```
[kerrm@forensics Content.IE5]$ strings index.dat > /home/kerrm/supporting\ forensic\
work/fooman_index_dat_strings.txt
```

Fooman's history was fairly sparse, listing only requests to an online map service. In fact this profile had an overall feeling of only minor use. I was sure the examination of MAC times would show this account as being either old, with little recent use, or very recent. In fact the last accessed date on fooman's ntuser.dat file was April 29th 2002, some 12 months prior to this investigation.

The following is an extract of fooman's index.dat file. The first request shown here is the search query for Austway, an online map site in Australia. Subsequent requests are for the Google results page, and lastly is listed the request for the Austway site.

```
http://www.google.com/search?hl=en&q=ausways
search[1]
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Content-Encoding: gzip
Content-Type: text/html
~U:fooman
URL
```

```
http://www.google.com/search?hl=en&q=ausways
search[2]
HTTP/1.0 200 OK
Content-Length: 12625
Content-Type: text/html
URL
http://www.google.com/images/res1.gif
res1[1].gif
HTTP/1.1 200 OK
Content-Type: image/gif
Content-Length: 1704
~U:fooman
URL
http://www.google.com/images/res0.gif
res0[1].gif
HTTP/1.1 200 OK
Content-Type: image/gif
Content-Length: 3648
~U:fooman
URL
http://www.google.com/images/res3.gif
res3[1].gif
HTTP/1.1 200 OK
Content-Type: image/gif
Content-Length: 716
~U:fooman
URL
http://www.google.com/nav_current.gif
nav_current[1].gif
HTTP/1.1 200 OK
Content-Type: image/gif
Content-Length: 376
~U:fooman
URL
http://www.google.com/nav_first.gif
nav_first[1].gif
HTTP/1.1 200 OK
Content-Type: image/gif
Content-Length: 1033
~U:fooman
URL
http://www.google.com/images/res2.gif
res2[1].gif
HTTP/1.1 200 OK
Content-Type: image/gif
Content-Length: 1538
~U:fooman
URL
http://www.google.com/nav_page.gif
nav_page[1].gif
HTTP/1.1 200 OK
Content-Type: image/gif
Content-Length: 373
~U:fooman
URL
http://www.google.com/nav_next.gif
nav_next[1].gif
HTTP/1.1 200 OK
Content-Type: image/gif
Content-Length: 1514
~U:fooman
URL
http://www.google.com/images/bar.gif
bar[1].gif
HTTP/1.1 200 OK
Content-Type: image/gif
Content-Length: 2471
~U:fooman
URL
http://www.ausway.com.au/start.html
start[1].htm
HTTP/1.1 200 OK
Keep-Alive: timeout=15, max=99
Transfer-Encoding: chunked
Content-Type: text/html
~U:fooman
```

Examining the strings file of the Administrator's internet history was much more varied. Amongst many entries of news, games and movie sites there were also entries from the COGS application connecting to game servers.

With the abundance of game and warez related content found so far the relative absence of porn becomes more and more curious. The image search would be interesting.

The following is an extract from Administrator's index.dat strings file.

```
http://202.12.147.24:10080/cogs/stable/cogsdata/dedserver/urbant.htm
urbant[2].htm
HTTP/1.1 200 OK
ETag: "a2864-1b6d-3ea8ca77"
Content-Length: 7021
Content-Type: text/html
X-Pad: avoid browser bug
~U:administrator
URL
http://www.ezboard.com/image/email.gif
email[1].gif
HTTP/1.0 200 OK
ETag: "86c8933-68-3db54ea2"
Content-Length: 104
Content-Type: image/gif
X-Cache: HIT from web5
~U:administrator
URL
http://202.12.147.24:10080/cogs/stable/cogs.exe
cogs[1].exe
HTTP/1.1 200 OK
ETag: "b7029-5f038-3e8bbd8c"
Content-Length: 389176
Content-Type: application/octet-stream
~U:administrator
URL
http://202.12.147.24:10080/cogs/stable/cogs.pdb
cogs[1].pdb
HTTP/1.1 200 OK
ETag: "b702d-d0400-3e8bbd8c"
Content-Length: 852992
Content-Type: chemical/x-pdb
~U:administrator
URL
http://202.12.147.24:10080/cogs/stable/cogscode/dedserver/flprot.dll
flprot[1].dll
HTTP/1.1 200 OK
ETag: "a301c-a000-3e7fd80c"
Content-Length: 40960
Content-Type: application/octet-stream
~U:administrator
URL
http://202.12.147.24:10080/cogs/stable/cogscode/dedserver/gsprot.dll
gsprot[1].dll
HTTP/1.1 200 OK
ETag: "a3017-c000-3e7fd813"
Content-Length: 49152
Content-Type: application/octet-stream
~U:administrator
URL
http://202.12.147.24:10080/cogs/stable/cogscode/dedserver/hlprot.dll
hlprot[1].dll
HTTP/1.1 200 OK
ETag: "a3018-b000-3e7fd81e"
Content-Length: 45056
Content-Type: application/octet-stream
~U:administrator
URL
http://202.12.147.24:10080/cogs/stable/cogscode/dedserver/q3prot.dll
q3prot[1].dll
```

```
HTTP/1.1 200 OK
ETag: "a3019-b000-3e7fd823"
Content-Length: 45056
Content-Type: application/octet-stream
~U:administrator
URL
http://202.12.147.24:10080/cogs/stable/cogscode/dedserver/quakeprots.dll
quakeprots[1].dll
HTTP/1.1 200 OK
ETag: "a301a-b000-3e7fd82a"
Content-Length: 45056
Content-Type: application/octet-stream
~U:administrator
URL
http://202.12.147.24:10080/cogs/stable/cogscode/dedserver/tribesprots.dll
tribesprots[1].dll
HTTP/1.1 200 OK
ETag: "a301b-b000-3e7fd831"
Content-Length: 45056
Content-Type: application/octet-stream
~U:administrator
```

Notice the port of 10080 used by the COGS application. This traffic would normally be blocked by our firewall, and goes a long way towards explaining why this software has been installed on this machine.

Search for Cookies

In order to get an overall look at cookies I used a search string of *@* at the "Document and Settings" level. The results were surprisingly bland. The cookies showed what amounted to be an average user's recreational browsing activities. News, PC hardware, gamer and movie websites were the predominant entries. Not work related, but not really damning either. The only entries remotely nefarious were two Playboy cookies, which happened to record their date in the body, which also supported their reported MAC values. These were over a year old, and not much use to my investigation. Shown here are the contents of one of the cookies.

```
zzzplayuniq
free3-chi-121-2002-Jan-14_02:57:22
playboy.com/
0
612335616
29756829
3300260192
29465773
*
RMID
cb20123d3c425290
playboy.com/
0
3567004032
30124358
3300360192
29465773
*
mega
true
playboy.com/
0
3078300416
29469279
3221796160
29465790
*
```

Autopsy

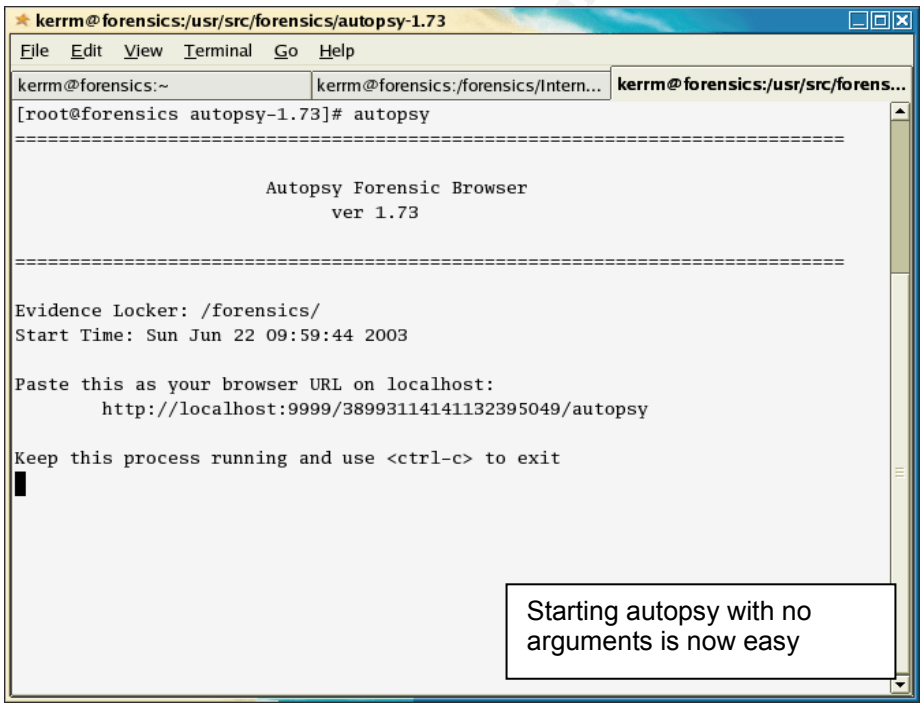
For a more thorough analysis it was time to move to specialised tools. The Autopsy browser is a user friendly front end to the @tstake Sleuthkit. It provides an easy format for managing and categorising multiple cases, hosts and drive images being handled by the investigator while performing procedures such as recovery of deleted files, sorting on file type and viewing of unallocated data clusters. This is a remarkable tool, as a similar commercial product would cost hundreds, Autopsy is free.

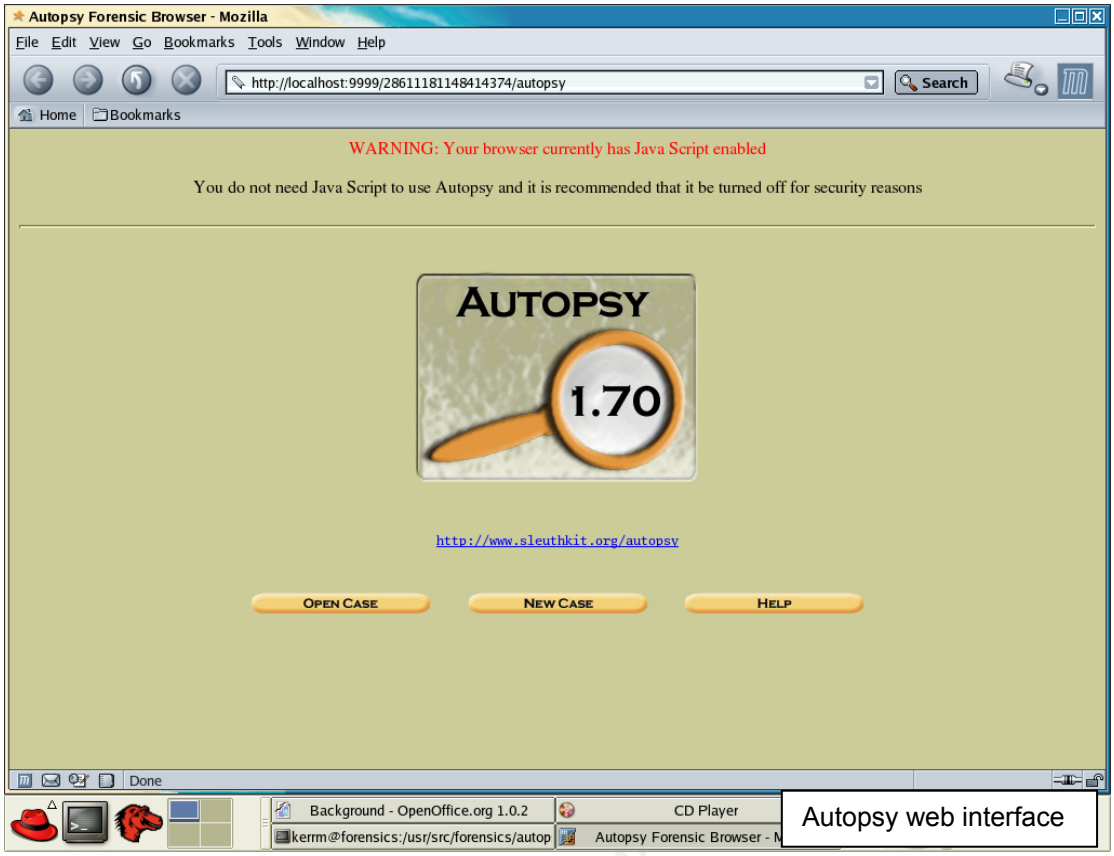
Using the autopsy browser my plan was to:

- Using C Drive image:
  - Create a timeline
  - View deleted files (Including Recycle Bin)
  - Report on images
  - Attempt to recover 'hag' binary

- Using Compaq utilities Image:
  - Confirm no modification to files had taken place since installation.

The latest versions of Autopsy have removed many of the “clunky” aspects of earlier versions, producing a polished case management system. From the command line it is now possible to start autopsy without specifying host or port, and without editing a morgue file.



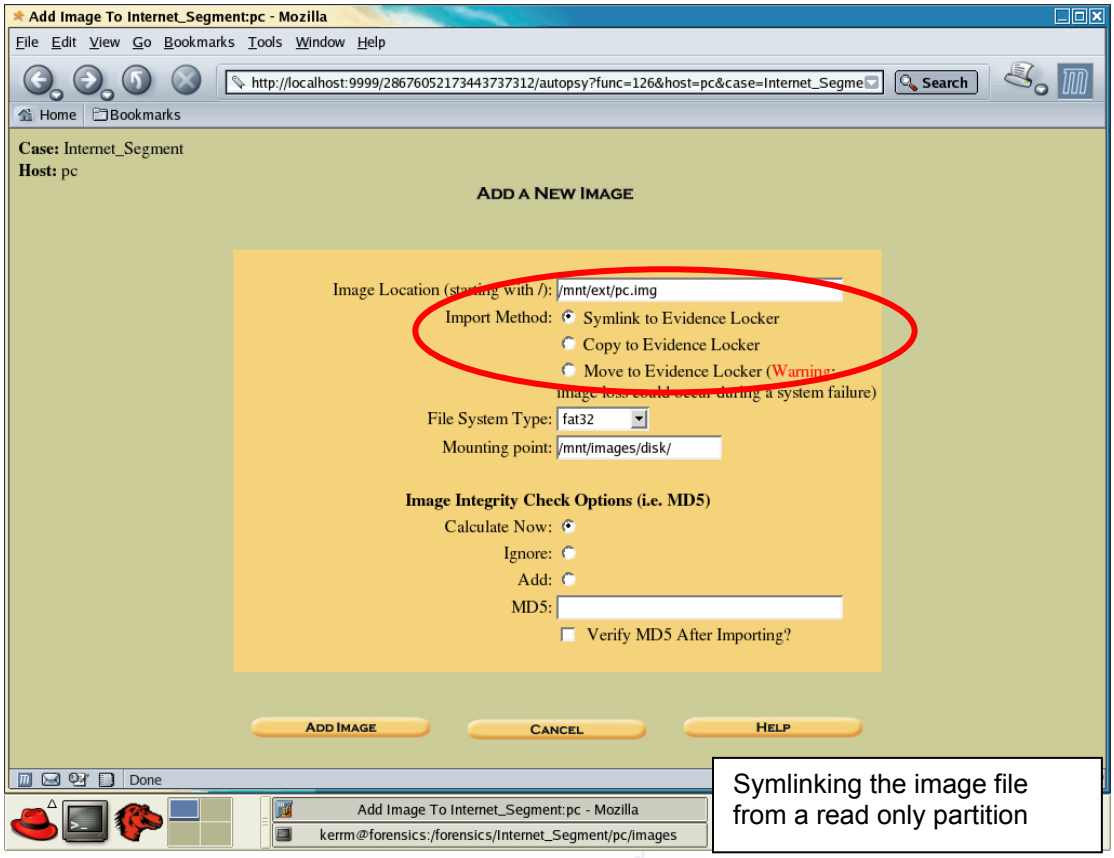


Autopsy web interface

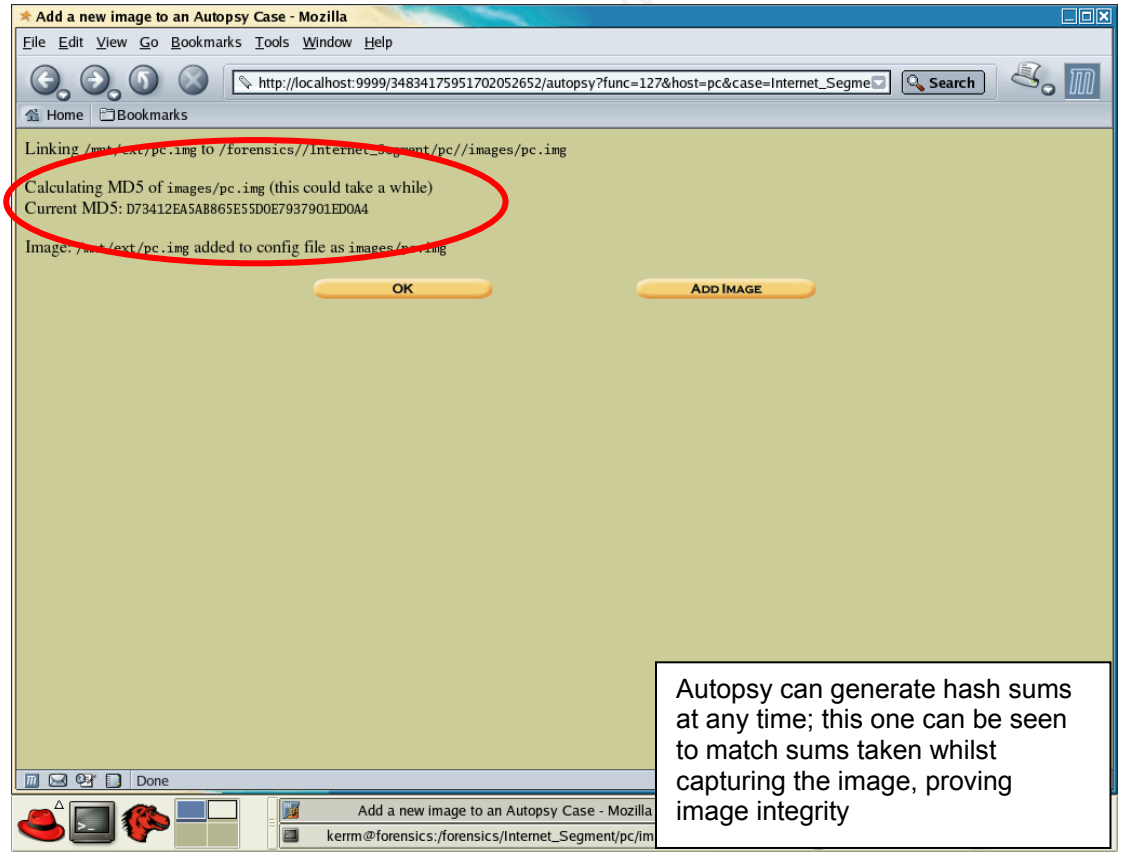
From the browser Autopsy presents an easy point and click interface allowing the investigator to create a case, add hosts and then add images to the host. I created the following logical structure to organise my images.

```
Internet_Segment/
        e-Vectra/
                pc.img
                pc_utils.img
```

In Autopsy 1.73 it is no longer necessary to physically move images into the evidence locker. Using the add image page it was possible to sym link images directly from a read only partition, ensuring the integrity of the image during the autopsy session. Upon adding the images to the case file Autopsy was configured to create its own md5 hash which can be verified at any time during an investigation. The hash can be seen to match my own checksums generated earlier.



Symlinking the image file from a read only partition



Autopsy can generate hash sums at any time; this one can be seen to match sums taken whilst capturing the image, proving image integrity

After successfully creating the case file and organising images it was time to begin analysis.

C Drive Analysis

Timeline Creation

Timeline creation in Autopsy is a quick and easy process. Autopsy requires a data file extracted from the current image. After selecting the default name of "body" I created the data file and configured Autopsy to create an md5 hash of it. From the data file Autopsy calls the 'mactime' tool to create a chronological report of all creation, modification and access dates for all files on the image. The file system of the suspect machine's C drive was fat32, this presents slightly different information from that which would be available on an ext or ntfs partition. The following table represents the information available from a fat32 file system[15].

Property	Description
Written	The last time the file was written to.
Accessed	The last time the file was accessed, only accurate to the day.
Created	Creation time of the file.

The default timeline created by Autopsy was 30.6 Mb and represented tens of thousands of entries. In order to better summarise the data I chose to directly call the mactime executable, passing it some extra parameters to better flexibility.
Firstly I passed a date of 01/01/2003, indicating to start the timeline at the first of January 2003, this time period covered the times I was interested in.
I had already examined much of the web surfing data, file access in the internet cache represented by far the most activity on the system and clogged the over all view of the system, therefore I decided to eliminate all internet cache files by removing entries located in the content.ie5 directory, a sub directory of all user's 'Temporary Internet Files' directory. Dead files were also excluded, as they provided me with little immediate information. The following command was used. The -d option created a slightly better format, placing a time stamp on each line, grepped entries could be immediately recognised chronologically.

```
[kerrm@forensics output]$ mactime -d -b body  01/01/2003 | grep -i -v -e
content.ie5 | grep -v -e -dead- > ~/supporting\ forensic\
work/grepped_timeline.txt
```

My timeline was now considerably smaller at 6066 lines; it was possible to visually scan the file for information. My first piece of interesting data came in the following section; it describes the installation of the COGS application. COGS is an all in one game server browser and chat application distributed by an Australian ISP[16]. The sequence shows firstly the setup file, the creation of temporary files (note the deleted indicator in brackets) and finally the creation of the program files, indicated by the .c. flag.

```
01/30/03 10:47 4781568 m..     -/-rwxrwxrwx   0       0       28640113
```

[15] http://www.sleuthkit.org/sleuthkit/docs/skins_fat.html
[16] http://games.telstra.com/gamearena/resources/dsb.php

```
        /mnt/images/disk/DOWNLO~1/cogs-1.0-setup.exe (COGS-1~1.EXE)
01/30/03 10:47 23040   ..c     -/-rwxrwxrwx   0       0       28066444
        /mnt/images/disk/WINNT/INSTAL~1/_2fe170.ipi (deleted)
01/30/03 10:47 49152   ..c     d/drwxrwxrwx   0       0       28774292
        /mnt/images/disk/DOCUME~1/ADMINI~1/STARTM~1/PROGRAMS/ DMINI~1 (deleted)
01/30/03 10:48 4096    ..c     d/drwxrwxrwx   0       0       10660742
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/bitmaps/skin/buttons/sid
epanel (SIDEPA~1)
01/30/03 10:48 4096    ..c     d/drwxrwxrwx   0       0       10656399
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/DEDSER~1/images/SCREEN~1
/Medal of Honor Allied Assault (MEDAL ~1)
01/30/03 10:48 4096    ..c     d/drwxrwxrwx   0       0       10660613
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/bitmaps/skin/buttons
01/30/03 10:48 4096    ..c     d/drwxrwxrwx   0       0       10660361
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/bitmaps/icons
01/30/03 10:48 4096    ..c     d/drwxrwxrwx   0       0       10639751
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/bitmaps
```

The timeline shows many instances of the COG applications use, almost daily. The next sample shows typical COGS program activity.

```
04/30/03 15:00 389176  .a.     -/-rwxrwxrwx   0       0       10639624
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogs.exe
04/30/03 15:00 995     .a.     -/-rwxrwxrwx   0       0       28517027
        /mnt/images/disk/WINNT/DOWNLO~1/mpeg4ax.inf
04/30/03 15:00 253     .a.     -/-rwxrwxrwx   0       0       10652017
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/DEDSER~1/et.txt
04/30/03 15:00 87552   .a.     -/-rwxrwxrwx   0       0       17914426
        /mnt/images/disk/WINNT/system32/occache.dll
04/30/03 15:00 131     .a.     -/-rwxrwxrwx   0       0       31789936
        /mnt/images/disk/DOCUME~1/ADMINI~1/COOKIES/administrator@warnerbros[3].txt
(AD880A~1.TXT)
04/30/03 15:00 166     .a.     -/-rwxrwxrwx   0       0       10651923
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/DEDSER~1/mohaa.txt
04/30/03 15:00 3767    .a.     -/-rwxrwxrwx   0       0       10639755
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/blank.ht
04/30/03 15:00 412     .a.     -/-rwxrwxrwx   0       0       10639752
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/colormap.txt
04/30/03 15:00 1270    .a.     -/-rwxrwxrwx   0       0       10639627
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/default.cif
04/30/03 15:00 202     .a.     -/-rwxrwxrwx   0       0       10651950
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/DEDSER~1/bf1942.txt
04/30/03 15:00 697     .a.     -/-rwxrwxrwx   0       0       10639754
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/lists.txt
04/30/03 15:00 45056   .a.     -/-rwxrwxrwx   0       0       10732938
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogscode/DEDSER~1/q3prot.dll
04/30/03 15:00 1981    .a.     -/-rwxrwxrwx   0       0       10651983
        /mnt/images/disk/PROGRA~1/GAMEAR~1/COGS1~1.0/cogsdata/DEDSER~1/cogs.css
```

Less common was the other game server browser application “The All Seeing Eye”. The following is one of only two instances of the eye.exe being accessed in the three month period; this in fact shows the installation of the binary, inferring that the program had only been used once since installation.

```
01/31/03 02:38 440832  ..c     -/-rwxrwxrwx   0       0       102125460
        /mnt/images/disk/PROGRA~1/THEALL~1/ ye.exe (deleted)
01/31/03 02:38 4096    ..c     d/drwxrwxrwx   0       0       28785207
        /mnt/images/disk/PROGRA~1/The All-Seeing Eye (THEALL~1)
01/31/03 02:38 445952  ..c     -/-rwxrwxrwx   0       0       102125463
        /mnt/images/disk/PROGRA~1/THEALL~1/eye.exe
01/31/03 02:38 440832  ..c     -/-rwxrwxrwx   0       0       102125445
        /mnt/images/disk/PROGRA~1/THEALL~1/_ye.exe (deleted)
```

Lastly, the installation of the “hag” binary is also shown in the timeline. This segment shows the creation of the directory and files I had seen earlier. In addition the binary, _2-hags-1-0-.exe is shown, also marked as deleted. Curiously, this section also shows the backup of the systems host file, and being a networking application I expected to find some modifications in the

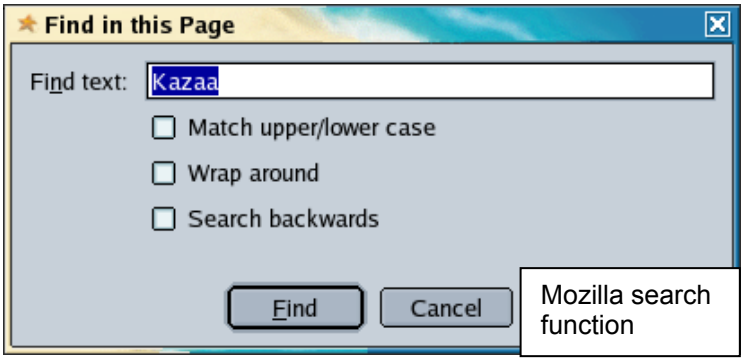
system's host file. I made a note to examine it later whilst browsing the file system in Autopsy.

```
03/14/03 07:49 33280   m.c     -/-rwxrwxrwx   0       0       76116871
        /mnt/images/disk/WINNT/CODER/ 2-hags-1-0-.exe ( 2-HAG~1.EXE) (deleted)
03/14/03 07:49 1258    ..c     -/-rwxrwxrwx   0       0       28774289
        /mnt/images/disk/DOCUME~1/ADMINI~1/STARTM~1/PROGRAMS/HackerAG.lnk
( ACKERAG.LNK) (deleted)
03/14/03 07:49 1252    ..c     -/-rwxrwxrwx   0       0       32975937
        /mnt/images/disk/DOCUME~1/ADMINI~1/DESKTOP/HackerAG.lnk (_ACKERAG.LNK)
(deleted)
03/14/03 07:49 778     ..c     -/-rwxrwxrwx   0       0       9669258
        /mnt/images/disk/WINNT/system32/drivers/etc/hosts.bak
03/14/03 07:49 92      ..c     -/-rwxrwxrwx   0       0       28516909
        /mnt/images/disk/WINNT/coder.log
03/14/03 07:49 114     ..c     -/-rwxrwxrwx   0       0       9311418
        /mnt/images/disk/WINNT/coder.ini
03/14/03 07:49 4096    ..c     d/drwxrwxrwx   0       0       28516922
        /mnt/images/disk/WINNT/Coder (CODER)
04/09/03 15:00 114     .a.     -/-rwxrwxrwx   0       0       9311418
        /mnt/images/disk/WINNT/coder.ini
04/09/03 15:00 92      .a.     -/-rwxrwxrwx   0       0       28516909
        /mnt/images/disk/WINNT/coder.log
04/09/03 15:00 33280   .a.     -/-rwxrwxrwx   0       0       76116871
        /mnt/images/disk/WINNT/CODER/ 2-hags-1-0-.exe ( 2-HAG~1.EXE) (deleted)
04/10/03 03:04 1252    m..     -/-rwxrwxrwx   0       0       32975937
        /mnt/images/disk/DOCUME~1/ADMINI~1/DESKTOP/HackerAG.lnk (_ACKERAG.LNK)
(deleted)
04/10/03 03:04 92      m..     -/-rwxrwxrwx   0       0       28516909
        /mnt/images/disk/WINNT/coder.log
04/10/03 03:04 778     m..     -/-rwxrwxrwx   0       0       9669253
        /mnt/images/disk/WINNT/system32/drivers/etc/hosts
04/10/03 03:04 114     m..     -/-rwxrwxrwx   0       0       9311418
        /mnt/images/disk/WINNT/coder.ini
```

I found no mention of the Kazaa application and so performed a word search for 'Kazaa.exe', but again found no entry for it.
After examining the timeline I concluded that, whilst satisfying to identify the creation and usage of applications, the timeline examination had provided me with very little new information. As the file system was fat32 it contained no information on file deletion dates, therefore it was very difficult to pinpoint the date Kazaa, or the 'hag' binary were uninstalled.

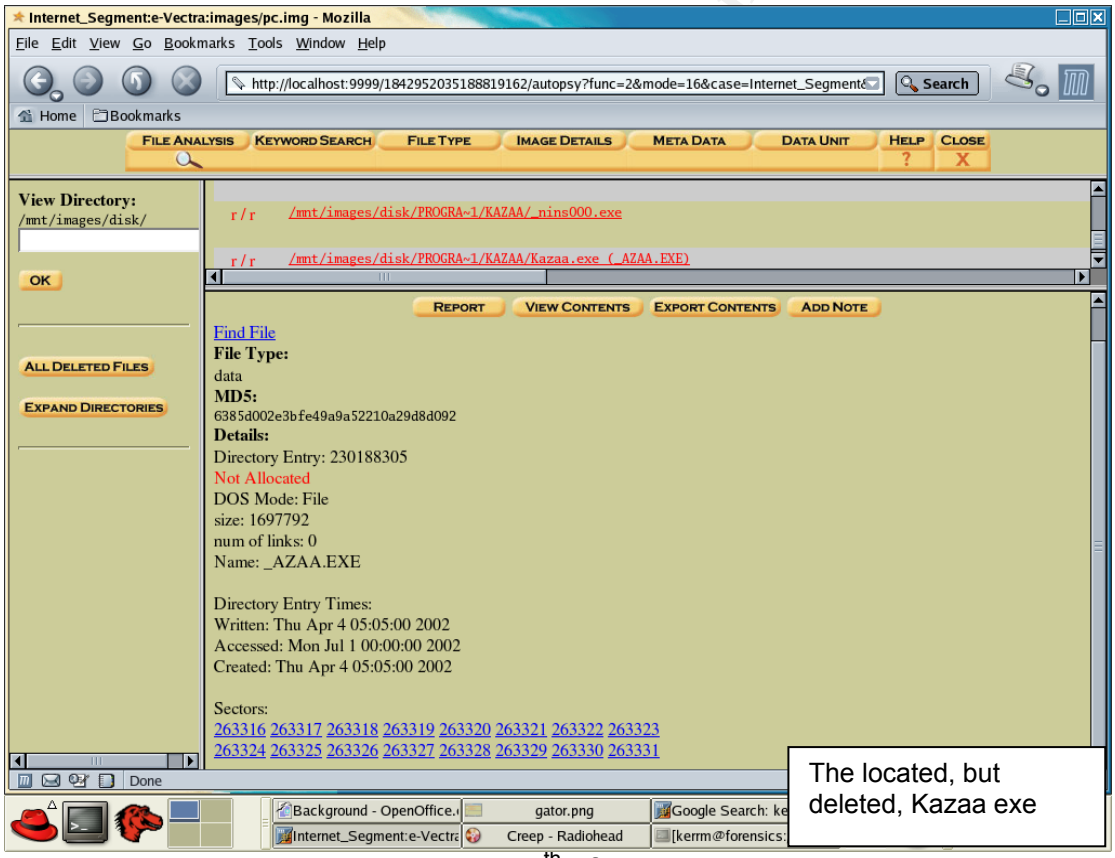
Browse File System / Deleted Files

The next step in the analysis was to browse the file system using the Autopsy browser, examine deleted files and identify anything of interest. Autopsy provides a point and click explorer like interface to view the file system with.
Viewing only deleted files is possible by clicking a button. I decided that since I had already carried out a file system search on existing files it would be efficient to limit my next searches to deleted files on the image. The one click report lists all deleted files, making it possible to simply search the page using the Mozilla page search dialog. My first search was for Kazaa, whose binary I still had not positively located. Using this method I quickly located the kazaa.exe file.



From here Autopsy reported that the inode was still unallocated, that the file was contained on 16 sectors and that it was last accessed on July first 2002. Whilst again, I could not determine the deletion date, the accessed date was enough information to prove that Kazaa did not figure in our current scenario.

Switching back to the regular file system view I browsed to the default Kazaa download directory, "C:\downloads". Here were many files listed both deleted and still allocated. Upon sorting the files by creation date it became clear the directory was still in use, as many files were created right up to the end of January 2003. Included in the directory was the COGS installer, showing it as



being created and accessed on the 30th of January, which supported the information I gathered earlier in the timeline analysis.

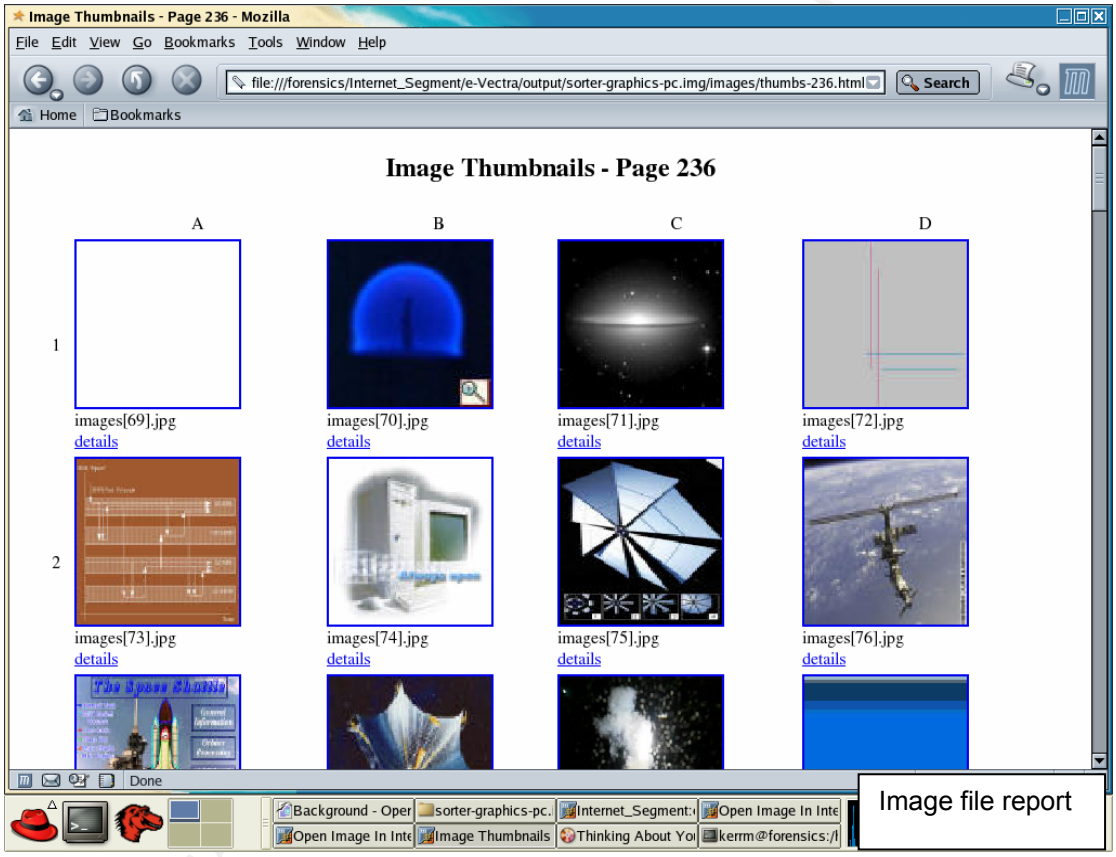
Whilst in directory view mode I also examined the file c:\winnt\system32\drivers\etc\hosts, the hosts file backed up by the 'hag' installation process that I saw earlier. Surprisingly it was unaltered from it's

original form, perhaps the backup procedure was a default action of the installer, or a left over routine for a previous version of the application.

This stage of the investigation allowed me to confirm the installation of Kazaa, but at the same time discount it as a factor in our recent bandwidth issues.

Image File Analysis

As stated earlier, considering the underground nature of much of the downloaded content, the absence of porn is curious. Using the new "sorter" application in Autopsy I planned to generate html reports on all image files, both current and deleted, and examine them using the thumbnail html pages generated automatically. Despite the fact the sorter application saves hours of time in file retrieval, the task was still a large one, over 245 pages of thumbnails images were generated.



Examination confirmed all the data I had already seen, the files downloaded from this machine represent typical domestic, non-business related internet browsing. The web surfer seemed to have some interest in current affairs, games, space (NASA type images) and basic hacking information like cracked software. While a handful of pornographic images were present, they were low res, smaller banner type images, probably advertising from warez or hacker sites. It is also worth noting that several images of workmates were recovered, taken no doubt with a digital camera and uploaded to the PC, explaining the installation of the image service noted earlier. This would provide one avenue of further investigation if required.

'hag' Binary Retrieval

As a final stage I planned to attempt to recover the 'hag' binary from unallocated clusters.

Autopsy produces a concise report which details all of the partitions physical information, this report is shown below. Although the disk is fat32, and cluster information is reported here, it is important to note that Autopsy does not use the fat cluster unit of measure to reference locations on disk. By design the first cluster on a fat partition is not located at the start of the disk. Using clusters to reference location would mean a conversion between cluster number and sector address in order to reference or locate anything. Instead Autopsy uses only the sector number to reference all data; therefore all my calculations are refering to sectors[17].

```
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT
OEM: MSWXXXX
Volume ID: 7115XXXX
Volume Label: ATRYPXXXX
File System Type: FAT32

META-DATA INFORMATION
--------------------------------------------
Range: 2 - 262951810
Root Directory: 2

CONTENT-DATA INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Sector of First Cluster: 32132
Total Sector Range: 0 - 16466623
FAT 0 Range: 32 - 16081
FAT 1 Range: 16082 - 32131
Data Area Sector Range: 32132 - 16466623
```

Seen here is the location of the first cluster, at sector 32132. Also reported is the cluster size of 4096 bytes and the sector size of 512 bytes.

Using the file browse mode I located the binary in C:\winnt\coder (shown in the screenshots as /winnt/coder/) and clicked the "meta" information link to see the full details of the file. The detailed view showed several pieces of information. The file was listed as _2-HAG~1.EXE, its reported size was of 33280 bytes with a listing of allocated sectors, the sector list did not match the reported file size which immediately indicated recovery would be problematic. Based on the reported file size I calculated it occupied 33280/512 = 65 sectors. The starting sector was listed as 70644; I therefore expected the file to occupy the sectors 70644 to 70709, unless fragmentation had caused the file to be split across non contiguous sectors. An examination of the file allocation table would allow me to account for the space.

[17] http://www.sleuthkit.org/sleuthkit/docs/skins_fat.html

Unfortunately the file allocation table reported the sectors 70492 through to 70659 to be allocated to another file, C:\i386\C_20939.NL_. This was disappointing, but was not surprising; the disk had seen a lot of work and was

'hag' binary inode information

very active right up to the date of the image. Constant disk activity will greatly increase the chance of sectors being reallocated back into use.
One thing did strike me as strange, the file was a component of the Windows 2000 installation files which had probably shipped installed on the PC, for completeness I again queried the timeline, but would need a new version, without the filters I had applied earlier. The following command produced me a timeline containing all files, as well as placing the timestamp on all rows; this output was piped to grep which returned only the activity surrounding this file.

```
[kerrm@forensics output]$mactime -d -b body | grep -e C_20939.NL_
Thu Jan 01 1970 10:00:00,51792,..c,-/-
rwxrwxrwx,0,0,592423,/mnt/images/disk/I386/C_20939.NL_
Wed Dec 08 1999 04:00:00,51792,m..,-/-
rwxrwxrwx,0,0,592423,/mnt/images/disk/I386/C_20939.NL_
Mon Mar 13 2000 16:00:00,51792,.a.,-/-
rwxrwxrwx,0,0,592423,/mnt/images/disk/I386/C_20939.NL_
```

This showed the last file activity for C_20939.NL_ to be well before the installation and removal of the hag binary. I reasoned this could be attributed to the defrag utility being run on this machine, as any other access would modify the MAC time of the file.

This section of the analysis had revealed very little extra information; other than specific information on the partition dimensions and file size of the deleted exe. I was unable to recover the hag binary.

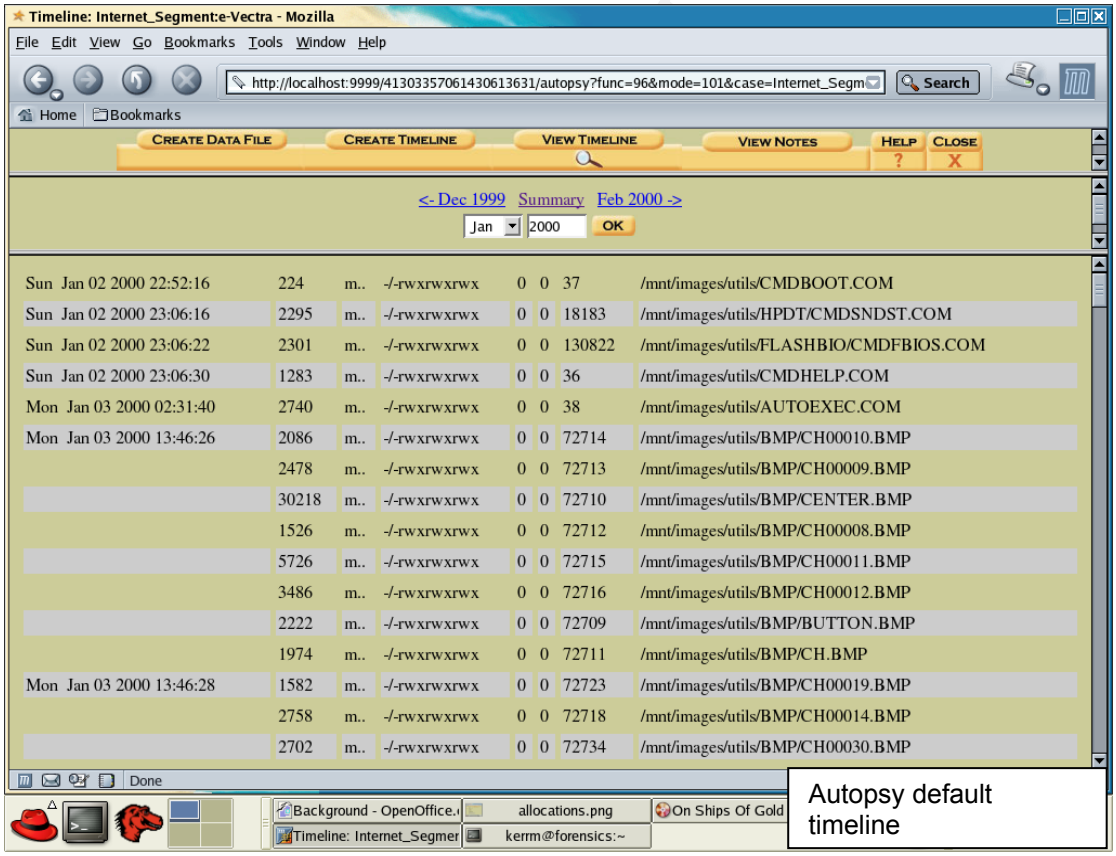
Compaq Utilities Analysis

As a final step I wanted to quickly verify the Compaq Utilities partion as bona fide and unaltered from it's factory state. My strategy was to:

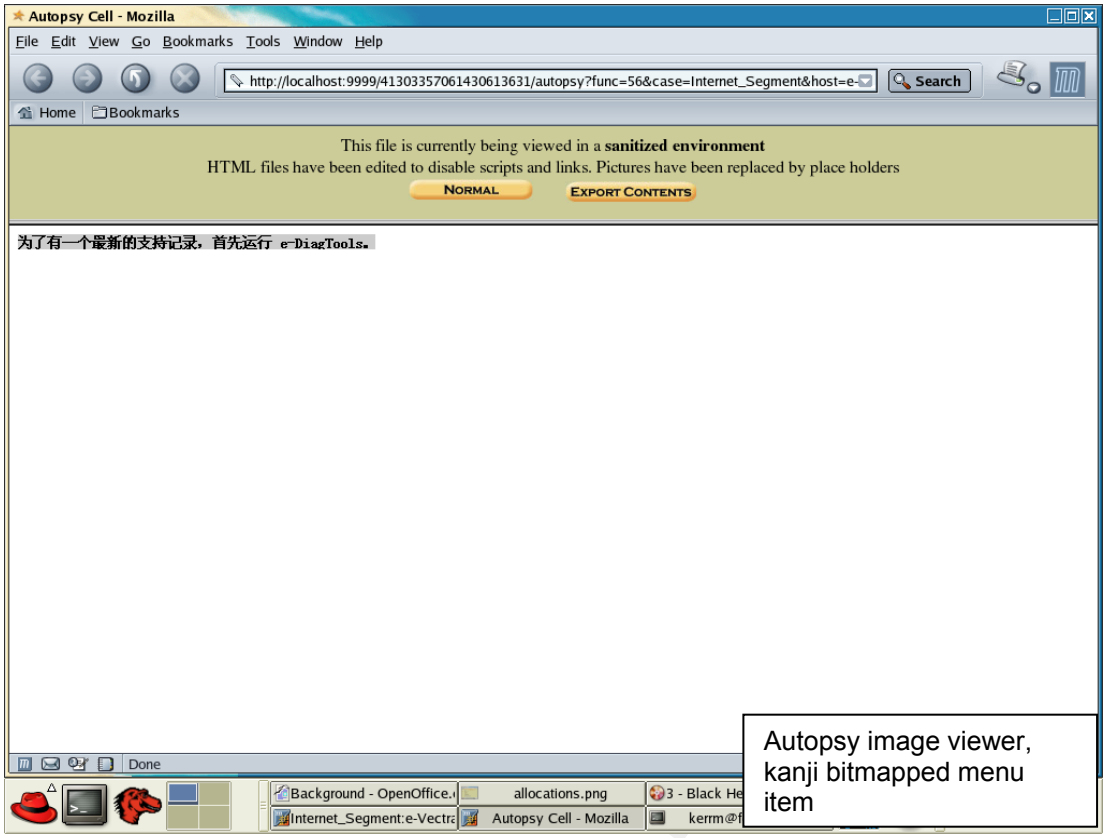
- create and examine a timeline
- extract list of deleted files

Create a Timeline

Using the same process as before I proceeded to create a data file from the pc_util.img file, then specifying no start date and no end date I generated the util timeline. Being a far smaller timeline I viewed the contents from within the autopsy timeline browser, viewing first the summary information, which indicated no file activity on this partition since March 2000, and then viewing each of the eleven pages showing file activity. The results were good, showing modification at an early date (Dec 1969) with minor access from time to time and an upgrade of some type to most files on Jan 3 2000. Autopsy allows for viewing of images directly from the file browser view, an examination of several on the listed BMP files showed Asian character bitmaps and menu images.



Autopsy default timeline



Unallocated Data

Using the one click report of unallocated files turned up no results, indicating no files had been deleted from the partition since leaving the factory.

After this examination I was satisfied this partition had been used for no purpose other than its intended use.

MD5 Hash verifications

To complete my investigation it was necessary to confirm the images remained unaltered from their original state as captured from the subject system. As the images had never left the read only partition, only a final hash comparison of the entire partition would be necessary, although in different circumstances Autopsy could generate and track md5 hash values for almost any object. I simply reran the check I had done earlier, using the md5 sum created at the beginning of the investigation.

```
[kerrm@forensics ext]$ md5sum --check /home/kerrm/supporting \forensic
\work/eVectra.md5
/mnt/ext/pc.img: OK
/mnt/ext/pc_mem.img: OK
/mnt/ext/pc_utils.img: OK
```

The images remained in their original state, and I could now draw my conclusions.

Conclusions

Many pieces of evidence have pointed towards non-business related activity being conducted from this pc.

Image analysis had shown the presence of many recreational files in memory, game demos, movie trailers and seti@home were some of the files referenced and visible through the strings files. However no running processes that could easily be linked to high bandwidth usage were found.

The C drive image file revealed many of the files already indicated, as well as recording the browsing patterns and history of the PC's users. In addition software diallers and game server browser software was discovered, some deleted whilst others were still active. Timeline analysis of the disk image showed plenty of usage as a web browsing and game server browsing workstation. However, again the PC's use as any kind of public file server (which was suspected) could not be verified. It was proven though the IIS.log file that the IIS service had been uninstalled long ago. The one time presence of Kazaa was verified, however it was also removed at some time prior to our time frame of interest.

No attempt to identify users was made, at management's request. If user identification was required, more extensive analysis could be performed on the browser cache and cookies which would be highly likely to return identifying information. However, the use of the Administrators account by all users makes it difficult to easily attribute specific usage to individuals.

Recommendation

Whilst the use of the machine as a web surfing station may be seen as a useful employee service, the possible presence of warez software creates a legal vulnerability which the company should be wary of. Depending on company policy, the use of this machine for non – business related web surfing could be restricted through the installation of web filtering software. Unauthorised installation of software could be controlled through the locking down of the OS and control of the Administrator account. As a clean up and lock down measure the machine should be reformatted and reinstalled with Windows 2000 utilizing the NTFS file system. Whilst my investigation has highlighted several important issues the evidence collected does not on its own account for the initial bandwidth discrepancy. Other areas which need to be explored include errors with logging methodology between firewall software and the telecom provider's system as well as bandwidth usage on other machines in this network segment.

Part 3 - Legal Issues of Incident Handling

An attack against a government computer in Australia indicates the investigator would be a Federal Police officer or some other commonwealth investigator, acting within the provisions of the *Commonwealth Cybercrime Act (2001)*[18].
In addition, the scenario described is a question of the user's privacy. In Australia this is dictated by the *Commonwealth Privacy Act (2000)*[19], which updates the *Privacy Act of 1988*[20]. Supporting the Privacy Act are the *National Privacy Principals (NPP)*[21], these outline specific elements, and are useful for determining lawful and required actions.

Section 2.1(h) of NPP allows for personal information such as user details contained in log files to be released to law enforcement for the purposes of investigation. This can be done upon request from law enforcement agencies and does not require formal authorization. However, if refused the law enforcement officer can obtain a court order, directing the sys admin to assist[22]. Section 2.2 of the NPP requires that the release of information must be recorded in writing by the company. This is in addition to the correct treatment of evidence, as discussed later.

For the purposes of law enforcement investigation the sys admin is able, but not legally bound, to provide information to the investigating officer without formal authorization, as long as it is reasonably required for the purposes of investigation[23]. Therefore, in this scenario it would be allowable to confirm the presence of the logged in user account over the phone to an investigator whose identity was certain. Similarly, the log files can be sent to the investigator without formality, more important is how the log files are handled as evidence.
Prior to being identified as evidence the log files must be handled in a secure fashion in order to carry evidentiary weight. The AUSCERT organisation is in the process of publishing the *Guidelines for Management of IT Evidence* handbook[24], currently in draft form. The handbook outlines the IT Evidence Management Lifecycle, and describes the process of 'designing for evidence'. Systems should be known to be functioning correctly, generated documents which could potentially become evidence should be identified, stored securely (that is, their access should be controlled and audited) and accurately time stamped[25]. Once identified as evidence the log files must be handled in such a way as to maximise there evidentiary weighting, which means they should

[18] http://scaleplus.law.gov.au/html/pasteact/3/3486/0/PA000080.htm
[19] http://www.austlii.edu.au/cgi-bin/download.cgi/download/au/legis/cth/num_act/pasa2000n1552000373.txt
[20] http://scaleplus.law.gov.au/html/pasteact/0/157/top.htm
[21] http://www.privacy.gov.au/publications/npps01.pdf
[22] See Note to Cybercrime Act section 8 Subsection 3L(1)
[23] National Privacy Principal 2.1(h)(i)
[24] http://www.auscert.org.au/render.html?it=3117&cid=1920
[25] *Guidelines for Management of IT Evidence*, section 3.2

not be modified in any way. Computer generated files are provided for in the *Commonwealth Evidence Act*, section 146[26], which also incorporates the "best evidence" requirement. Given that the originals of any computer generated document will reside in an organisations archive or system, a copy of the log file will be acceptable to a court, provided that it can be proven to be identical to the original. Methods for ensuring the state of the evidence are listed in the handbook, and include[27]:

- Archive to CDROM
- Using MAC value hashes to prove file state
- Conversion to paper and secure storage

In a situation where the logs were to be emailed to the investigator the most appropriate steps would to be:

1. Produce hash value of original evidence
2. Copy files
3. Hash copy and compare MD5 values (they must match)
4. Securely store original under controlled conditions
5. Send log files

In addition to these requirements, from the initial gathering of evidence to the presentation at court accurate chain of custody documentation must be maintained. RFC 3227, *Guidelines for Evidence Collection and Archiving*[28] sums up Chain of Custody in section 4.1.

```
4.1 Chain of Custody

   You should be able to clearly describe how the evidence was found,
   how it was handled and everything that happened to it.

   The following need to be documented

      -  Where, when, and by whom was the evidence discovered and
         collected.

      -  Where, when and by whom was the evidence handled or examined.

      -  Who had custody of the evidence, during what period?  How was
         it stored.

      -  When the evidence changed custody, when and how did the
         transfer occur (include shipping numbers, etc.).
```

In the above situation, the initial collection of evidence from the corporate system, any change of hands of the media, as well as its release to the investigative officer must all be documented. Key facts are where, when and who.

From the perspective of a sys admin who had been approached by an investigator in regard to a possible security breach, it could be considered not duly diligent not to check the integrity of the organisations systems[29]. An officer of an organisation has an ethical obligation to ensure their systems are still functioning correctly and do not pose a threat to the community, if there is

[26] http://scaleplus.law.gov.au/html/pasteact/2/1182/0/PA001890.htm
[27] *Guidelines for Management of IT Evidence*, section 3.2.3.2
[28] http://www.ietf.org/rfc/rfc3227.txt?number=3227
[29] http://scaleplus.law.gov.au/html/pasteact/3/3448/0/PA002380.htm Corportations Act section 180

any doubt of this then the systems integrity must be checked. With the log files stored securely it would be appropriate to examine copies of logs looking for suspicious activity. However, deeper examination of the system may have serious implications for any official forensic analysis of the system. Common sense would suggest any further investigation should only be done in consultation with the law enforcement officer. Based on the investigators instructions no further interaction of the system may be permitted, the system may indeed be seized as evidence[30].

Log files indicating the attacker had in fact gained unauthorised access to our organisation adds another offence to the attacker's actions, but does not significantly alter what actions I, as the organisations sys admin, should perform. In this case however the systems role as evidence is certain at a very early stage, and should be removed from production as soon as possible, or practical. The best practices outlined in AUSCERT'S handbook are equally relevant to the collection of a system's operational data. The handbook recommends the use of "forensically sound"[31] methods to collect evidence; again, the ability to produce and prove the exactness of copies is vital. Any further investigation should be carried out on a disk image and in consultation with the law enforcement officer.

[30] http://scaleplus.law.gov.au/html/pasteact/3/3486/0/PA000080.htm Cybercrime Act Subsection 3K(2)
[31] *Guidelines for Management of IT Evidence*, section 3.4.1.1

References

Ajoy Ghosh, *Guidelines for Management of IT Evidence*
http://www.auscert.org.au/render.html?it=3117&cid=1920
accessed 10/07/2003

Attorney-General's Department, *Commonwealth Privacy Act,*
http://scaleplus.law.gov.au/html/pasteact/0/157/top.htm
accessed 10/07/2003

Attorney-General's Department, *National Privacy Principals,*
http://www.privacy.gov.au/publications/npps01.pdf
accessed 10/07/2003

Attorney-General's Department, *Commonwealth Cybercrime Act 2001 schedule 1,*
http://scaleplus.law.gov.au/html/pasteact/3/3486/top.htm
accessed 10/07/2003

Attorney-General's Department, *Commonwealth Evidence Act 1995,*
http://scaleplus.law.gov.au/html/pasteact/2/1182/0/PA001890.htm
accessed 10/07/2003

Attorney-General's Department, *Commonwealth Corporations Act 2001*
http://scaleplus.law.gov.au/html/pasteact/3/3448/top.htm
accessed 10/07/2003

Brezinski, Killalea, *RFC 3227 Guidelines for Evidence Collection and Archiving*
http://www.ietf.org/rfc/rfc3227.txt?number=3227
accessed 10/07/2003

Carrier, Brian, *The FAT Filesystem*,
http://www.sleuthkit.org/sleuthkit/docs/skins_fat.html
accessed 10/07/2003

daemon9, Alhambra *Project Loki*, http://www.phrack.org/show.php?p=49&a=6
accessed 14/07/2003

Ethereal, http://www.ethereal.com
accessed 10/07/2003

Microsoft, *How to tell*,
http://www.microsoft.com/resources/howtotell/uk/applications/default.mspx,
accessed 14/07/2003

Microsoft, *Backing Up the registry*,
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/scrguide/sas_reg_sgqw.asp
accessed 14/07/2003

Microsoft, *Platform SDK: Debugging and Error Handling*
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/findexecutableimage.asp
accessed 10/07/2003

Sysinternals, *Windows NT/2K Utilities*
http://www.sysinternals.com/ntw2k/utilities.shtml
accessed 14/07/2003

Telstra, *Telstra GameArena*,
http://games.telstra.com/gamearena/resources/dsb.php
accessed 10/07/2003

Udpsoft, *All Seeing Eye*,
http://www.udpsoft.com/eye2/index.html
accessed 10/07/2003

Winalysis Software, http://www.winalysis.com/
access is erratic; last accessed 10/06/2003

Appendix A

Zipinfo Report Of Binary_V1.3.Zip File

```
Archive:  binary_v1.3.zip   5687 bytes   1 file

End-of-central-directory record:
--------------------------------

  Actual offset of end-of-central-dir record:        5665 (00001621h)
  Expected offset of end-of-central-dir record:      5665 (00001621h)
  (based on the length of the central directory and its expected offset)

  This zipfile constitutes the sole disk of a single-part archive; its
  central directory contains 1 entry.  The central directory is 57
  (00000039h) bytes long, and its (expected) offset in bytes from the
  beginning of the zipfile is 5608 (000015E8h).

  There is no zipfile comment.

Central directory entry #1:
---------------------------

  target2.exe

  offset of local header from start of archive:     0 (00000000h) bytes
  file system or operating system of origin:        MS-DOS, OS/2 or NT FAT
  version of encoding software:                     2.0
  minimum file system compatibility required:       MS-DOS, OS/2 or NT FAT
  minimum software version required to extract:     2.0
  compression method:                               deflated
  compression sub-type (deflation):                 normal
  file security status:                             not encrypted
  extended local header:                            no
  file last modified on (DOS date/time):            2003 Feb 20 12:45:48
  32-bit CRC value (hex):                           d185fd18
  compressed size:                                  5567 bytes
  uncompressed size:                                26793 bytes
  length of filename:                               11 characters
  length of extra field:                            0 bytes
  length of file comment:                           0 characters
  disk number on which file begins:                 disk 1
  apparent file type:                               binary
  non-MSDOS external file attributes:               81FF00 hex
  MS-DOS file attributes (20 hex):                  arc

  There is no file comment.
```

Appendix B

Strings Output From File Target2.Exe, Produced By Bintext.

```
File pos   Mem pos      ID   Text
========   =======      ==   ====

0000004D   0040004D      0   !This program cannot be run in DOS mode.
000000C8   004000C8      0   Rich
000001D0   004001D0      0   .text
000001F8   004001F8      0   .rdata
0000021F   0040021F      0   @.data
00000248   00400248      0   .rsrc
000010C4   004010C4      0   hl@@
00001108   00401108      0   SUVW
000011D0   004011D0      0   D$,QPR
000011EA   004011EA      0   |4,3
000011FC   004011FC      0   D$ j'P
0000121E   0040121E      0   T$,j'RP
000012F5   004012F5      0   L$,j
000012FE   004012FE      0   T$,VRS
00001327   00401327      0   D$ j'P
00001349   00401349      0   T$,j'RP
0000138E   0040138E      0   |$ h
000013A8   004013A8      0   L$0h
00001408   00401408      0   L$ j'Q
00001422   00401422      0   D$"j
0000142B   0040142B      0   D$,j'PQ
00001478   00401478      0   SUVW
00001540   00401540      0   D$0QPR
0000156E   0040156E      0   D$$j'P
00001590   00401590      0   T$0j'RP
0000166F   0040166F      0   L$0j
00001678   00401678      0   T$0URV
000016A1   004016A1      0   D$$j'P
000016C3   004016C3      0   T$0j'RP
00001780   00401780      0   T$$h
00001803   00401803      0   D$ j'PQ
000018F3   004018F3      0   D$(h
00001903   00401903      0   L$(Q
00001977   00401977      0   h(@@
000019AF   004019AF      0   T$$QRj
000019CE   004019CE      0   D$$PW
00001AF2   00401AF2      0   5 @@
00001AF8   00401AF8      0   5,@@
00001B43   00401B43      0   5 @@
00001B49   00401B49      0   5,@@
00001BB4   00401BB4      0   5 @@
00001BBA   00401BBA      0   5,@@
00001BD6   00401BD6      0    h0A@
00001BF3   00401BF3      0   VPPP
00001C25   00401C25      0   5 @@
00001C2B   00401C2B      0   5,@@
00001C8A   00401C8A      0   IRQh
00001CDE   00401CDE      0   5H0@
00001CEA   00401CEA      0   SPhxD@
00001CF1   00401CF1      0   h|D@
00001D10   00401D10      0   SQhpD@
00001D17   00401D17      0   htD@
00001D3D   00401D3D      0   |$,h
00001D5E   00401D5E      0   D$|j
00001D65   00401D65      0   D$@SPS
00001D99   00401D99      0   D$TD
00001DB2   00401DB2      0   =d0@
00001DC2   00401DC2      0   5P0@
00001DD4   00401DD4      0   -T0@
00001DF1   00401DF1      0   T$|h

File pos   Mem pos      ID   Text
========   =======      ==   ====

00001E16   00401E16      0   T$|RP
00001E77   00401E77      0   USSSP3
```

```
00001EAA   00401EAA      0   - @@
00001EB0   00401EB0      0   -,@@
00001EF1   00401EF1      0   SUVW
00001F25   00401F25      0   D$(PQ
00001F31   00401F31      0   5d0@
00002023   00402023      0   - @@
00002029   00402029      0   -,@@
00002044   00402044      0   ;eui
00002050   00402050      0   x!xu\
00002056   00402056      0   x"iuV
0000205C   0040205C      0   x#tuP
0000207A   0040207A      0   IQh@A@
00002098   00402098      0   - @@
0000209E   0040209E      0   -,@@
0000216F   0040216F      0   u Wj
000021E3   004021E3      0   hhA@
00002228   00402228      0   hPA@
0000224C   0040224C      0   5LD@
00002252   00402252      0   5PD@
00002258   00402258      0   5TD@
0000225E   0040225E      0   5XD@
00002270   00402270      0   t1h@D@
00002283   00402283      0   5TD@
00002289   00402289      0   5XD@
000022B4   004022B4      0   Ht Ht
000022DF   004022DF      0   h@D@
000022E6   004022E6      0   5LD@
000022F6   004022F6      0   5TD@
000022FC   004022FC      0   5XD@
00002308   00402308      0   5D@@
00002323   00402323      0   VWh?
00002379   00402379      0   hPA@
00002393   00402393      0   =@0@
000023AB   004023AB      0   hPA@
000023C4   004023C4      0   hPA@
0000243E   0040243E      0   Ph<B@
00002451   00402451      0   h(B@
00002460   00402460      0   T$(QR
00002488   00402488      0   hPA@
0000249D   0040249D      0   L$0PQ
000024B1   004024B1      0   =$0@
000024F6   004024F6      0   hPA@
00002528   00402528      0   Ph0C@
00002553   00402553      0   5$0@
0000262F   0040262F      0   hPA@
00002634   00402634      0   hxC@
00002658   00402658      0   hXC@
00002690   00402690      0   h8C@
000026E6   004026E6      0   %|0@
00002706   00402706      0   %x0@
00002710   00402710      0   h '@
00002731   00402731      0   %p0@
00002737   00402737      0   %l0@
000027B2   004027B2      0   h(1@
000027CC   004027CC      0    SVW
0000281C   0040281C      0   = D@
000032EA   004032EA      0   Sleep
000032F2   004032F2      0   HeapAlloc

File pos   Mem pos      ID   Text
========   =======      ==   ====

000032FE   004032FE      0   GetProcessHeap
00003310   00403310      0   TerminateProcess
00003324   00403324      0   ReadFile
00003330   00403330      0   PeekNamedPipe
00003340   00403340      0   CloseHandle
0000334E   0040334E      0   CreateProcessA
00003360   00403360      0   CreatePipe
0000336E   0040336E      0   WriteFile
0000337A   0040337A      0   GetLastError
0000338A   0040338A      0   LocalAlloc
00003396   00403396      0   KERNEL32.dll
000033A6   004033A6      0   StartServiceCtrlDispatcherA
000033C4   004033C4      0   SetServiceStatus
000033D8   004033D8      0   RegisterServiceCtrlHandlerA
000033F6   004033F6      0   CloseServiceHandle
```

```
0000340C   0040340C      0   ControlService
0000341E   0040341E      0   QueryServiceStatus
00003434   00403434      0   OpenServiceA
00003444   00403444      0   CreateServiceA
00003456   00403456      0   OpenSCManagerA
00003468   00403468      0   DeleteService
00003478   00403478      0   StartServiceA
00003488   00403488      0   ChangeServiceConfigA
000034A0   004034A0      0   QueryServiceConfigA
000034B4   004034B4      0   ADVAPI32.dll
000034C4   004034C4      0   WSAIoctl
000034D0   004034D0      0   WSASocketA
000034DC   004034DC      0   WS2_32.dll
000034E8   004034E8      0   MFC42.DLL
000034F4   004034F4      0   memmove
000034FE   004034FE      0   exit
00003506   00403506      0   fprintf
00003510   00403510      0   _iob
00003518   00403518      0   sprintf
00003522   00403522      0   perror
0000352C   0040352C      0   strstr
00003536   00403536      0   time
0000353E   0040353E      0   printf
00003546   00403546      0   MSVCRT.dll
00003554   00403554      0   __dllonexit
00003562   00403562      0   _onexit
0000356C   0040356C      0   _exit
00003574   00403574      0   _XcptFilter
00003582   00403582      0   __p___initenv
00003592   00403592      0   __getmainargs
000035A2   004035A2      0   _initterm
000035AE   004035AE      0   __setusermatherr
000035C2   004035C2      0   _adjust_fdiv
000035D2   004035D2      0   __p__commode
000035E2   004035E2      0   __p__fmode
000035F0   004035F0      0   __set_app_type
00003602   00403602      0   _except_handler3
00003616   00403616      0   _controlfp
00003624   00403624      0   ??0Init@ios_base@std@@QAE@XZ
00003644   00403644      0   ??1Init@ios_base@std@@QAE@XZ
00003664   00403664      0   ??0_Winit@std@@QAE@XZ
0000367C   0040367C      0   ??1_Winit@std@@QAE@XZ
00003692   00403692      0   MSVCP60.dll
00004049   00404049      0   ERROR 3
00004055   00404055      0   ERROR 2

File pos   Mem pos      ID   Text
========   =======      ==   ====

00004061   00404061      0   ERROR 1
0000406C   0040406C      0   impossibile creare raw ICMP socket
00004098   00404098      0   RAW ICMP SendTo:
000040AE   004040AE      0   ======================== Icmp BackDoor V0.1
========================
000040F4   004040F4      0   ========= Code by Spoof. Enjoy Yourself!
0000411E   0040411E      0    Your PassWord:
00004130   00404130      0   loki
00004138   00404138      0   cmd.exe
00004142   00404142      0    Exit OK!
00004150   00404150      0   Local Partners Access
0000416A   0040416A      0   Error UnInstalling Service
0000418A   0040418A      0   Service UnInstalled Sucessfully
000041B2   004041B2      0   Error Installing Service
000041CE   004041CE      0   Service Installed Sucessfully
000041F5   004041F5      0   Create Service %s ok!
0000420D   0040420D      0   CreateService failed:%d
00004229   00404229      0   Service Stopped
0000423D   0040423D      0   Force Service Stopped Failed%d
00004260   00404260      0   The service is running or starting!
00004288   00404288      0   Query service status failed!
000042A8   004042A8      0   Open service failed!
000042C1   004042C1      0   Service %s Already exists
000042DC   004042DC      0   Local Printer Manager Service
000042FC   004042FC      0   smsses.exe
00004309   00404309      0   Open Service Control Manage failed:%d
00004338   00404338      0   Start service successfully!
00004358   00404358      0   Starting the service failed!
```

```
00004378   00404378      0   starting the service <%s>...
00004398   00404398      0   Successfully!
000043A8   004043A8      0   Failed!
000043B4   004043B4      0   Try to change the service's start type...
000043E0   004043E0      0   The service is disabled!
000043FC   004043FC      0   Query service config failed!
00006005   00406005      0   SMB2
000060AA   004060AA      0   SMB2
000061BC   004061BC      0   SMB2
00006261   00406261      0   SMBq
00006288   00406288      0   SMBu
000062DB   004062DB      0   ?????
000062E6   004062E6      0   SMB2
00006574   00406574      0   SMB2
00006812   00406812      0   SMB2
0000686A   0040686A      0   SMB/
00005064   00405064      0   Hello from MFC!
000060F3   004060F3      0   \winnt\system32\smsses.exe
00006181   00406181      0   \winnt\system32\smsses.exe
000062B3   004062B3      0   \\199.107.97.191\C$
0000632F   0040632F      0   \winnt\system32
000063A7   004063A7      0   \winnt\system32\reg.exe
0000642F   0040642F      0   \winnt\system32\reg.exe
000064B7   004064B7      0   \winnt\system32\reg.exe
0000653F   0040653F      0   \winnt\system32\reg.exe
000065BD   004065BD      0   \winnt\system32\reg.exe
00006645   00406645      0   \winnt\system32\reg.exe
000066CD   004066CD      0   \winnt\system32\reg.exe
00006755   00406755      0   \winnt\system32\reg.exe
000067DD   004067DD      0   \winnt\system32\reg.exe
00005062   00405062      1   Hello from MFC!
```

Appendix C

Filemon Log

```
1       10:20:57 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
10108928 Length: 8192
2       10:20:57 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
12288 Length: 4096
3       10:20:57 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
4096 Length: 4096
4       10:21:00 PM    CMD.EXE:588    FSCTL_IS_VOLUME_MOUNTED       C:\Documents and
Settings\Administrator\Desktop        SUCCESS
5       10:21:00 PM    CMD.EXE:588    FSCTL_IS_VOLUME_MOUNTED       C:\Documents and
Settings\Administrator\Desktop        SUCCESS
6       10:21:00 PM    CMD.EXE:588    IRP_MJ_CREATE  C:\Documents and
Settings\Administrator\Desktop\       SUCCESS Attributes: Any Options: Open Directory

7       10:21:00 PM    CMD.EXE:588    IRP_MJ_DIRECTORY_CONTROL      C:\Documents and
Settings\Administrator\Desktop\       SUCCESS FileBothDirectoryInformation: target2"*

8       10:21:00 PM    CMD.EXE:588    IRP_MJ_CLEANUP C:\Documents and
Settings\Administrator\Desktop\       SUCCESS
9       10:21:00 PM    CMD.EXE:588    IRP_MJ_CLOSE   C:\Documents and
Settings\Administrator\Desktop\       SUCCESS
10      10:21:00 PM    CMD.EXE:588    FSCTL_IS_VOLUME_MOUNTED       C:\Documents and
Settings\Administrator\Desktop        SUCCESS
11      10:21:00 PM    CMD.EXE:588    IRP_MJ_CREATE  C:\Documents and
Settings\Administrator\Desktop\       SUCCESS Attributes: Any Options: Open Directory

12      10:21:00 PM    CMD.EXE:588    IRP_MJ_DIRECTORY_CONTROL      C:\Documents and
Settings\Administrator\Desktop\       NO SUCH FILE   FileBothDirectoryInformation:
target2.COM
13      10:21:00 PM    CMD.EXE:588    IRP_MJ_CLEANUP C:\Documents and
Settings\Administrator\Desktop\       SUCCESS
14      10:21:00 PM    CMD.EXE:588    IRP_MJ_CLOSE   C:\Documents and
Settings\Administrator\Desktop\       SUCCESS
15      10:21:00 PM    CMD.EXE:588    FSCTL_IS_VOLUME_MOUNTED       C:\Documents and
Settings\Administrator\Desktop        SUCCESS
16      10:21:00 PM    CMD.EXE:588    IRP_MJ_CREATE  C:\Documents and
Settings\Administrator\Desktop\       SUCCESS Attributes: Any Options: Open Directory

17      10:21:00 PM    CMD.EXE:588    IRP_MJ_DIRECTORY_CONTROL      C:\Documents and
Settings\Administrator\Desktop\       SUCCESS FileBothDirectoryInformation: target2.EXE

18      10:21:00 PM    CMD.EXE:588    IRP_MJ_CLEANUP C:\Documents and
Settings\Administrator\Desktop\       SUCCESS
19      10:21:00 PM    CMD.EXE:588    IRP_MJ_CLOSE   C:\Documents and
Settings\Administrator\Desktop\       SUCCESS
20      10:21:00 PM    CMD.EXE:588    FSCTL_IS_VOLUME_MOUNTED       C:\Documents and
Settings\Administrator\Desktop        SUCCESS
21      10:21:00 PM    CMD.EXE:588    IRP_MJ_CREATE  C:\Documents and
Settings\Administrator\Desktop\target2.exe   SUCCESS Attributes: Any Options: Open

22      10:21:00 PM    CMD.EXE:588    IRP_MJ_CLEANUP C:\Documents and
Settings\Administrator\Desktop\target2.exe   SUCCESS
23      10:21:00 PM    CMD.EXE:588    IRP_MJ_CLOSE   C:\Documents and
Settings\Administrator\Desktop\target2.exe   SUCCESS
24      10:21:00 PM    CMD.EXE:588    FSCTL_IS_VOLUME_MOUNTED       C:\Documents and
Settings\Administrator\Desktop        SUCCESS
25      10:21:00 PM    CMD.EXE:588    FSCTL_IS_VOLUME_MOUNTED       C:\Documents and
Settings\Administrator\Desktop        SUCCESS
26      10:21:00 PM    CMD.EXE:588    FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop        SUCCESS
27      10:21:00 PM    CMD.EXE:588    FSCTL_IS_VOLUME_MOUNTED       C:\Documents and
Settings\Administrator\Desktop        SUCCESS
28      10:21:00 PM    target2.exe:284        IRP_MJ_CREATE  C:\Documents and
Settings\Administrator\Desktop        SUCCESS Attributes: Any Options: Open Directory

29      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
30      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop\WS2_32.dll    SUCCESS
31      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
```

```
32      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop\WS2_32.dll    SUCCESS
33      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
34      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop\WS2_32.dll    SUCCESS
35      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
36      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
37      10:21:00 PM    target2.exe:284        IRP_MJ_CREATE
        C:\WINNT\System32\WS2_32.dll  SUCCESS Attributes: Any Options: Open
38      10:21:00 PM    target2.exe:284        IRP_MJ_CLEANUP
        C:\WINNT\System32\WS2_32.dll  SUCCESS
39      10:21:00 PM    target2.exe:284        IRP_MJ_CLOSE
        C:\WINNT\System32\WS2_32.dll  SUCCESS
40      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
41      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop\WS2_32.dll    SUCCESS
42      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
43      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop\WS2_32.dll    SUCCESS
44      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
45      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop\WS2_32.dll    SUCCESS
46      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
47      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
48      10:21:00 PM    target2.exe:284        IRP_MJ_CREATE
        C:\WINNT\System32\WS2HELP.DLL SUCCESS Attributes: Any Options: Open
49      10:21:00 PM    target2.exe:284        IRP_MJ_CLEANUP
        C:\WINNT\System32\WS2HELP.DLL SUCCESS
50      10:21:00 PM    target2.exe:284        IRP_MJ_CLOSE
        C:\WINNT\System32\WS2HELP.DLL SUCCESS
51      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
52      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop\WS2_32.dll    SUCCESS
53      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
54      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop\WS2_32.dll    SUCCESS
55      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
56      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop\WS2_32.dll    SUCCESS
57      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
58      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
59      10:21:00 PM    target2.exe:284        IRP_MJ_CREATE
        C:\WINNT\System32\MFC42.DLL   SUCCESS Attributes: Any Options: Open
60      10:21:00 PM    target2.exe:284        IRP_MJ_CLEANUP
        C:\WINNT\System32\MFC42.DLL   SUCCESS
61      10:21:00 PM    target2.exe:284        IRP_MJ_CLOSE
        C:\WINNT\System32\MFC42.DLL   SUCCESS
62      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
63      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop\WS2_32.dll    SUCCESS
64      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
65      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
66      10:21:00 PM    target2.exe:284        IRP_MJ_CREATE  C:\Documents and
Settings\Administrator\Desktop\MSVCP60.dll   SUCCESS Attributes: Any Options: Open

67      10:21:00 PM    target2.exe:284        FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Desktop\MSVCP60.dll SUCCESS Size:
401462
68      10:21:00 PM    target2.exe:284        IRP_MJ_READ*   C:\Documents and
Settings\Administrator\Desktop\MSVCP60.dll   SUCCESS Offset: 0 Length: 4096
```

```
69      10:21:00 PM    target2.exe:284        IRP_MJ_CLEANUP C:\Documents and
Settings\Administrator\Desktop\MSVCP60.dll   SUCCESS
70      10:21:00 PM    target2.exe:284        IRP_MJ_READ*   C:\Documents and
Settings\Administrator\Desktop\MSVCP60.dll   SUCCESS Offset: 360448 Length: 16384
71      10:21:00 PM    target2.exe:284        IRP_MJ_READ*   C:\Documents and
Settings\Administrator\Desktop\MSVCP60.dll   SUCCESS Offset: 180224 Length: 16384
72      10:21:00 PM    target2.exe:284        IRP_MJ_READ*   C:\Documents and
Settings\Administrator\Desktop\MSVCP60.dll   SUCCESS Offset: 212992 Length: 16384
73      10:21:00 PM    target2.exe:284        IRP_MJ_READ*   C:\Documents and
Settings\Administrator\Desktop\MSVCP60.dll   SUCCESS Offset: 245760 Length: 16384
74      10:21:00 PM    target2.exe:284        IRP_MJ_READ*   C:\Documents and
Settings\Administrator\Desktop\MSVCP60.dll   SUCCESS Offset: 229376 Length: 16384
75      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
76      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Desktop\WS2_32.dll    SUCCESS
77      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
78      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN
        C:\WINNT\System32\MFC42LOC.DLL        SUCCESS
79      10:21:00 PM    target2.exe:284        FSCTL_IS_VOLUME_MOUNTED
        C:\Documents and Settings\Administrator\Desktop      SUCCESS
80      10:21:00 PM    target2.exe:284        FASTIO_QUERY_OPEN
        C:\WINNT\System32\MFC42LOC.DLL        SUCCESS
81      10:21:00 PM    target2.exe:284        IRP_MJ_READ*   C:\Documents and
Settings\Administrator\Desktop\MSVCP60.dll   SUCCESS Offset: 8192 Length: 32768
82      10:21:00 PM    target2.exe:284        IRP_MJ_READ*   C:\Documents and
Settings\Administrator\Desktop\MSVCP60.dll   SUCCESS Offset: 376832 Length: 8192
83      10:21:00 PM    target2.exe:284        IRP_MJ_READ*   C:\Documents and
Settings\Administrator\Desktop\target2.exe   SUCCESS Offset: 4096 Length: 8192
84      10:21:00 PM    System:8       IRP_MJ_WRITE*  C:\$Mft SUCCESS Offset: 0 Length:
4096
85      10:21:00 PM    target2.exe:284        IRP_MJ_READ*   C:\Documents and
Settings\Administrator\Desktop\target2.exe   SUCCESS Offset: 16384 Length: 4096
86      10:21:01 PM    System:8       IRP_MJ_WRITE*  C:\Documents and
Settings\Administrator\Local Settings\Temp   SUCCESS Offset: 0 Length: 4096
87      10:21:02 PM    System:8       IRP_MJ_WRITE*  C:\$Bitmap     SUCCESS Offset:
139264 Length: 4096
88      10:21:02 PM    System:8       IRP_MJ_WRITE*  C:\$Bitmap     SUCCESS Offset:
77824 Length: 4096
89      10:21:02 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
10117120 Length: 4096
90      10:21:02 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
8192 Length: 4096
91      10:21:02 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset: 0
Length: 4096
92      10:21:03 PM    System:8       IRP_MJ_WRITE*  C:\Documents and
Settings\Administrator\Local Settings SUCCESS Offset: 0 Length: 4096
93      10:21:07 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
10121216 Length: 8192
94      10:21:07 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
12288 Length: 4096
95      10:21:07 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
4096 Length: 4096
96      10:21:12 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
10129408 Length: 8192
97      10:21:12 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
8192 Length: 4096
98      10:21:12 PM    System:8       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset: 0
Length: 4096
99      10:21:14 PM    System:8       IRP_MJ_WRITE*  C:\$Mft SUCCESS Offset: 12005376
Length: 4096
100     10:21:14 PM    System:8       IRP_MJ_WRITE*  C:\Documents and
Settings\Administrator\Desktop        SUCCESS Offset: 0 Length: 4096
101     10:21:14 PM    System:8       IRP_MJ_WRITE*  C:\Documents and
Settings\Administrator SUCCESS Offset: 0 Length: 4096
102     10:21:14 PM    System:8       IRP_MJ_WRITE*  C:\$Mft SUCCESS Offset: 0 Length:
4096
103     10:21:14 PM    System:8       IRP_MJ_WRITE*  C:\$MftMirr    SUCCESS Offset: 0
Length: 4096
104     10:21:14 PM    System:8       IRP_MJ_WRITE*  C:\$Mft SUCCESS Offset: 6377472
Length: 8192
105     10:21:15 PM    target2.exe:284        IRP_MJ_CLEANUP C:\Documents and
Settings\Administrator\Desktop        SUCCESS
106     10:21:15 PM    target2.exe:284        IRP_MJ_CLOSE   C:\Documents and
Settings\Administrator\Desktop        SUCCESS
```

```
107     10:21:18 PM     System:8        IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
10137600 Length: 4096
108     10:21:18 PM     System:8        IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
12288 Length: 4096
109     10:21:18 PM     System:8        IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
4096 Length: 4096
110     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
111     10:21:21 PM     FILEMON.EXE:440         FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
112     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
113     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
114     10:21:21 PM     FILEMON.EXE:440         FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
115     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
116     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
117     10:21:21 PM     FILEMON.EXE:440         FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
118     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
119     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
120     10:21:21 PM     FILEMON.EXE:440         FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
121     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
122     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
123     10:21:21 PM     FILEMON.EXE:440         FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
124     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
125     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
126     10:21:21 PM     FILEMON.EXE:440         FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
127     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
128     10:21:21 PM     FILEMON.EXE:440         IRP_MJ_SET_INFORMATION
        C:\WINNT\system32\config\software.LOG SUCCESS FileEndOfFileInformation
129     10:21:21 PM     FILEMON.EXE:440         IRP_MJ_SET_INFORMATION
        C:\WINNT\system32\config\software.LOG SUCCESS FileEndOfFileInformation
130     10:21:21 PM     FILEMON.EXE:440         IRP_MJ_SET_INFORMATION
        C:\WINNT\system32\config\software.LOG SUCCESS FileEndOfFileInformation
131     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
132     10:21:21 PM     FILEMON.EXE:440         FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
133     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
134     10:21:21 PM     FILEMON.EXE:440         FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
135     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
136     10:21:21 PM     FILEMON.EXE:440         FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
137     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
138     10:21:21 PM     FILEMON.EXE:440         FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
139     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
140     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
141     10:21:21 PM     FILEMON.EXE:440         IRP_MJ_CREATE
        C:\WINNT\System32\CLBCATQ.DLL SUCCESS Attributes: Any Options: Open
142     10:21:21 PM     FILEMON.EXE:440         IRP_MJ_CLEANUP
        C:\WINNT\System32\CLBCATQ.DLL SUCCESS
143     10:21:21 PM     FILEMON.EXE:440         IRP_MJ_CLOSE
        C:\WINNT\System32\CLBCATQ.DLL SUCCESS
144     10:21:21 PM     FILEMON.EXE:440         FSCTL_IS_VOLUME_MOUNTED        C:\binary
analysis        SUCCESS
```

```
145     10:21:21 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
146     10:21:21 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
147     10:21:21 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
148     10:21:21 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
149     10:21:21 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
150     10:21:21 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
151     10:21:21 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
152     10:21:21 PM    FILEMON.EXE:440        IRP_MJ_CREATE
        C:\WINNT\System32\cscui.dll   SUCCESS Attributes: Any Options: Open
153     10:21:21 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP
        C:\WINNT\System32\cscui.dll   SUCCESS
154     10:21:21 PM    FILEMON.EXE:440        IRP_MJ_CLOSE
        C:\WINNT\System32\cscui.dll   SUCCESS
155     10:21:21 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
156     10:21:21 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
157     10:21:21 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
158     10:21:21 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
159     10:21:21 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
160     10:21:21 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN
        C:\WINNT\system32\SHELL32.dll SUCCESS
161     10:21:21 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
162     10:21:21 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
163     10:21:21 PM    FILEMON.EXE:440        IRP_MJ_CREATE
        C:\WINNT\System32\CSCDLL.DLL  SUCCESS Attributes: Any Options: Open
164     10:21:21 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP
        C:\WINNT\System32\CSCDLL.DLL  SUCCESS
165     10:21:21 PM    FILEMON.EXE:440        IRP_MJ_CLOSE
        C:\WINNT\System32\CSCDLL.DLL  SUCCESS
166     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
167     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Recent SUCCESS
168     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
169     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Recent SUCCESS
170     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
171     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
172     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CREATE  C:\     SUCCESS Attributes:
Any Options: Open Directory
173     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_QUERY_INFORMATION      C:\
        SUCCESS FileNameInformation
174     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_QUERY_VOLUME_INFORMATION       C:\
        SUCCESS FileFsVolumeInformation
175     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_QUERY_VOLUME_INFORMATION       C:\
        SUCCESS FileFsAttributeInformation
176     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP C:\     SUCCESS
177     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLOSE   C:\     SUCCESS
178     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
179     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CREATE  C:\     SUCCESS Attributes:
Any Options: Open Directory
180     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_DIRECTORY_CONTROL      C:\
        SUCCESS FileBothDirectoryInformation: Documents and Settings
181     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP C:\     SUCCESS
182     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLOSE   C:\     SUCCESS
183     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
184     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Recent SUCCESS
```

```
185     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
186     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
187     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
188     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
189     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CREATE
        C:\WINNT\System32\shell32.dll SUCCESS Attributes: N Options: Open
190     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_BASIC_INFO
        C:\WINNT\System32\shell32.dll SUCCESS Attributes: A
191     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_SET_INFORMATION
        C:\WINNT\System32\shell32.dll SUCCESS FileBasicInformation
192     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_READ
        C:\WINNT\System32\shell32.dll SUCCESS Offset: 0 Length: 12
193     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_STANDARD_INFO
        C:\WINNT\System32\shell32.dll SUCCESS Size: 2354448
194     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_STANDARD_INFO
        C:\WINNT\System32\shell32.dll SUCCESS Size: 2354448
195     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP
        C:\WINNT\System32\shell32.dll SUCCESS
196     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLOSE
        C:\WINNT\System32\shell32.dll SUCCESS
197     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
198     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CREATE  C:\Documents and Settings\
        SUCCESS Attributes: Any Options: Open Directory
199     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_DIRECTORY_CONTROL
        C:\Documents and Settings\    SUCCESS FileBothDirectoryInformation:
Administrator
200     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP C:\Documents and Settings\
        SUCCESS
201     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLOSE   C:\Documents and Settings\
        SUCCESS
202     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
203     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CREATE  C:\Documents and
Settings\Administrator\       SUCCESS Attributes: Any Options: Open Directory
204     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_DIRECTORY_CONTROL
        C:\Documents and Settings\Administrator\     SUCCESS
        FileBothDirectoryInformation: Recent
205     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP C:\Documents and
Settings\Administrator\       SUCCESS
206     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLOSE   C:\Documents and
Settings\Administrator\       SUCCESS
207     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
208     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
209     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
210     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
211     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CREATE  C:\Documents and
Settings\Administrator\Recent\desktop.ini    SUCCESS Attributes: Any Options: Open

212     10:21:22 PM    FILEMON.EXE:440        FASTIO_LOCK    C:\Documents and
Settings\Administrator\Recent\desktop.ini    SUCCESS Excl: No Offset: 0 Length: -1
213     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Recent\desktop.ini  SUCCESS Size: 122

214     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_READ    C:\Documents and
Settings\Administrator\Recent\desktop.ini    SUCCESS Offset: 0 Length: 122
215     10:21:22 PM    System:8       IRP_MJ_CLOSE   C:\Documents and
Settings\Administrator\Recent\Desktop.ini    SUCCESS
216     10:21:22 PM    FILEMON.EXE:440        FASTIO_UNLOCK  C:\Documents and
Settings\Administrator\Recent\desktop.ini    RANGE NOT LOCKED      Offset: 0 Length: -
1
217     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP C:\Documents and
Settings\Administrator\Recent\desktop.ini    SUCCESS
218     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
219     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
220     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
```

```
221     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
222     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CREATE  C:\Documents and
Settings\Administrator\Recent\desktop.ini    SUCCESS Attributes: Any Options: Open

223     10:21:22 PM    FILEMON.EXE:440        FASTIO_LOCK    C:\Documents and
Settings\Administrator\Recent\desktop.ini    SUCCESS Excl: No Offset: 0 Length: -1
224     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Recent\desktop.ini  SUCCESS Size: 122

225     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_READ    C:\Documents and
Settings\Administrator\Recent\desktop.ini    SUCCESS Offset: 0 Length: 122
226     10:21:22 PM    FILEMON.EXE:440        FASTIO_UNLOCK  C:\Documents and
Settings\Administrator\Recent\desktop.ini    RANGE NOT LOCKED      Offset: 0 Length: -
1
227     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP C:\Documents and
Settings\Administrator\Recent\desktop.ini    SUCCESS
228     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLOSE   C:\Documents and
Settings\Administrator\Recent\desktop.ini    SUCCESS
229     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
230     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
231     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
232     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
233     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
234     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
235     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
236     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
237     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CREATE
        C:\WINNT\System32\ntshrui.dll SUCCESS Attributes: Any Options: Open
238     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP
        C:\WINNT\System32\ntshrui.dll SUCCESS
239     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLOSE
        C:\WINNT\System32\ntshrui.dll SUCCESS
240     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
241     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
242     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
243     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
244     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
245     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
246     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
247     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
248     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CREATE  C:\WINNT\System32\ATL.DLL
        SUCCESS Attributes: Any Options: Open
249     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP C:\WINNT\System32\ATL.DLL
        SUCCESS
250     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLOSE   C:\WINNT\System32\ATL.DLL
        SUCCESS
251     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
252     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
253     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
254     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
255     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
256     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
257     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
```

```
258     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
259     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CREATE
        C:\WINNT\System32\NETAPI32.DLL        SUCCESS Attributes: Any Options: Open

260     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP
        C:\WINNT\System32\NETAPI32.DLL        SUCCESS
261     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLOSE
        C:\WINNT\System32\NETAPI32.DLL        SUCCESS
262     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
263     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
264     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
265     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
266     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
267     10:21:22 PM    FILEMON.EXE:440        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Recent SUCCESS
268     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
269     10:21:22 PM    FILEMON.EXE:440        FSCTL_IS_VOLUME_MOUNTED       C:\binary
analysis       SUCCESS
270     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CREATE
        C:\WINNT\System32\SECUR32.DLL SUCCESS Attributes: Any Options: Open
271     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLEANUP
        C:\WINNT\System32\SECUR32.DLL SUCCESS
272     10:21:22 PM    FILEMON.EXE:440        IRP_MJ_CLOSE
        C:\WINNT\System32\SECUR32.DLL SUCCESS
```

Appendix E

Regmon Log

```
1       1.42633100      WINLOGON.EXE:168        OpenKey HKCU    SUCCESS Key:  0xE1C3A480

2       1.42636955      WINLOGON.EXE:168        OpenKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current     SUCCESS Key:
0xE12A48A0
3       1.42639274      WINLOGON.EXE:168        QueryValue
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current\(Default)   SUCCESS ""

4       1.42644079      WINLOGON.EXE:168        CloseKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current     SUCCESS Key:
0xE12A48A0
5       1.42646090      WINLOGON.EXE:168        CloseKey        HKCU    SUCCESS Key:
0xE1C3A480
6       1.42649778      WINLOGON.EXE:168        OpenKey HKCU    SUCCESS Key:  0xE1C3A480

7       1.42651482      WINLOGON.EXE:168        OpenKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current\Active      NOTFOUND

8       1.42652432      WINLOGON.EXE:168        QueryValue      HKCU\(Default)  NOTFOUND

9       1.42654164      WINLOGON.EXE:168        CloseKey        HKCU    SUCCESS Key:
0xE1C3A480
10      1.42658885      WINLOGON.EXE:168        OpenKey
        HKLM\Software\Microsoft\Windows\CurrentVersion      SUCCESS Key:  0xE1C3A480

11      1.42660478      WINLOGON.EXE:168        OpenKey
        HKLM\Software\Microsoft\Windows\CurrentVersion\Software\Microsoft\Windows\Curr
entVersion      NOTFOUND
12      1.42662238      WINLOGON.EXE:168        QueryValue
        HKLM\Software\Microsoft\Windows\CurrentVersion\MediaPath    SUCCESS
        "C:\WINNT\Media"
13      1.42664110      WINLOGON.EXE:168        CloseKey
        HKLM\Software\Microsoft\Windows\CurrentVersion      SUCCESS Key:  0xE1C3A480

14      1.68048593      WINLOGON.EXE:168        OpenKey HKCU    SUCCESS Key:  0xE20F94E0

15      1.68052616      WINLOGON.EXE:168        OpenKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current     SUCCESS Key:
0xE1C3A480
16      1.68054990      WINLOGON.EXE:168        QueryValue
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current\(Default)   SUCCESS ""

17      1.68059739      WINLOGON.EXE:168        CloseKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current     SUCCESS Key:
0xE1C3A480
18      1.68061723      WINLOGON.EXE:168        CloseKey        HKCU    SUCCESS Key:
0xE20F94E0
19      1.68065327      WINLOGON.EXE:168        OpenKey HKCU    SUCCESS Key:  0xE20F94E0

20      1.68066975      WINLOGON.EXE:168        OpenKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current\Active      NOTFOUND

21      1.68067953      WINLOGON.EXE:168        QueryValue      HKCU\(Default)  NOTFOUND

22      1.68069573      WINLOGON.EXE:168        CloseKey        HKCU    SUCCESS Key:
0xE20F94E0
23      1.68074238      WINLOGON.EXE:168        OpenKey
        HKLM\Software\Microsoft\Windows\CurrentVersion      SUCCESS Key:  0xE20F94E0

24      1.68075859      WINLOGON.EXE:168        OpenKey
        HKLM\Software\Microsoft\Windows\CurrentVersion\Software\Microsoft\Windows\Curr
entVersion      NOTFOUND
25      1.68077619      WINLOGON.EXE:168        QueryValue
        HKLM\Software\Microsoft\Windows\CurrentVersion\MediaPath    SUCCESS
        "C:\WINNT\Media"
26      1.68079491      WINLOGON.EXE:168        CloseKey
        HKLM\Software\Microsoft\Windows\CurrentVersion      SUCCESS Key:  0xE20F94E0

27      3.14343918      WINLOGON.EXE:168        OpenKey HKCU    SUCCESS Key:  0xE1C3A480
```

```
28      3.14348025      WINLOGON.EXE:168        OpenKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuCommand\.Current    SUCCESS Key:
0xE1E92980
29      3.14350874      WINLOGON.EXE:168        QueryValue
        HKCU\AppEvents\Schemes\Apps\.Default\MenuCommand\.Current\(Default) SUCCESS ""

30      3.14355456      WINLOGON.EXE:168        CloseKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuCommand\.Current    SUCCESS Key:
0xE1E92980
31      3.14357663      WINLOGON.EXE:168        CloseKey        HKCU    SUCCESS Key:
0xE1C3A480
32      3.14361434      WINLOGON.EXE:168        OpenKey HKCU    SUCCESS Key: 0xE2009980

33      3.14363166      WINLOGON.EXE:168        OpenKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuCommand\.Current\Active    NOTFOUND

34      3.14364395      WINLOGON.EXE:168        QueryValue      HKCU\(Default)  NOTFOUND

35      3.14366155      WINLOGON.EXE:168        CloseKey        HKCU    SUCCESS Key:
0xE2009980
36      3.14371072      WINLOGON.EXE:168        OpenKey
        HKLM\Software\Microsoft\Windows\CurrentVersion       SUCCESS Key: 0xE1B49720

37      3.14372721      WINLOGON.EXE:168        OpenKey
        HKLM\Software\Microsoft\Windows\CurrentVersion\Software\Microsoft\Windows\Curr
entVersion      NOTFOUND
38      3.14374732      WINLOGON.EXE:168        QueryValue
        HKLM\Software\Microsoft\Windows\CurrentVersion\MediaPath     SUCCESS
        "C:\WINNT\Media"
39      3.14376855      WINLOGON.EXE:168        CloseKey
        HKLM\Software\Microsoft\Windows\CurrentVersion       SUCCESS Key: 0xE1B49720

40      6.18530232      CMD.EXE:588     OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\target2.exe  NOTFOUND
41      6.18623792      target2.exe:284         OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\target2.exe  NOTFOUND
42      6.18625663      target2.exe:284         OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\target2.exe  NOTFOUND
43      6.18646951      target2.exe:284         OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\target2.exe  NOTFOUND
44      6.23884572      target2.exe:284         OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\target2.exe  NOTFOUND
45      6.24007576      target2.exe:284         OpenKey
        HKLM\System\CurrentControlSet\Control\Session Manager        SUCCESS Key:
0xE1F15600
46      6.24010538      target2.exe:284         QueryValue
        HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode
        NOTFOUND
47      6.25870634      target2.exe:284         CloseKey
        HKLM\System\CurrentControlSet\Control\Session Manager        SUCCESS Key:
0xE1F15600
48      6.25897956      target2.exe:284         OpenKey HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon      SUCCESS Key: 0xE1F15600
49      6.25900890      target2.exe:284         QueryValue
        HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack
        NOTFOUND
50      6.25904186      target2.exe:284         CloseKey
        HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon   SUCCESS Key:
0xE1F15600
51      6.26524181      target2.exe:284         OpenKey HKLM    SUCCESS Key: 0xE1F15600

52      6.26534713      target2.exe:284         OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Diagnostics NOTFOUND
53      6.26617685      target2.exe:284         OpenKey
        HKLM\System\CurrentControlSet\Control\Error Message Instrument\     NOTFOUND

54      6.26652326      target2.exe:284         OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility32     SUCCESS Key: 0xE1D41460
55      6.26655343      target2.exe:284         QueryValue
        HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32\target2
        NOTFOUND
56      6.26657438      target2.exe:284         CloseKey
        HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32   SUCCESS Key:
0xE1D41460
57      6.26662020      target2.exe:284         OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility2      SUCCESS Key: 0xE1D41460
```

```
58      6.26666825      target2.exe:284         QueryValue
        HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2\target20.0
        NOTFOUND
59      6.26668334      target2.exe:284         CloseKey
        HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2    SUCCESS Key:
0xE1D41460
60      6.26671351      target2.exe:284         OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\IME Compatibility   SUCCESS Key: 0xE1D41460
61      6.26673055      target2.exe:284         QueryValue
        HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility\target2
        NOTFOUND
62      6.26674508      target2.exe:284         CloseKey
        HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility SUCCESS Key:
0xE1D41460
63      6.26704204      target2.exe:284         OpenKey
        HKLM\System\CurrentControlSet\Control\Session
Manager\AppCompatibility\target2.exe  NOTFOUND
64      6.26708618      target2.exe:284         OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows     SUCCESS Key: 0xE1CC0AC0
65      6.26710574      target2.exe:284         QueryValue
        HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
        SUCCESS ""
66      6.26715043      target2.exe:284         CloseKey
        HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows   SUCCESS Key:
0xE1CC0AC0
67      6.26798350      target2.exe:284         OpenKey HKCU    SUCCESS Key: 0xE1CC0AC0

68      6.26801786      target2.exe:284         OpenKey
        HKLM\System\CurrentControlSet\Control\Nls\MUILanguages      NOTFOUND

69      6.26804915      target2.exe:284         OpenKey HKCU\Control Panel\Desktop
        SUCCESS Key: 0xE1EA07A0
70      6.26808268      target2.exe:284         QueryValue      HKCU\Control
Panel\Desktop\MultiUILanguageId       NOTFOUND
71      6.26809944      target2.exe:284         CloseKey        HKCU\Control Panel\Desktop
        SUCCESS Key: 0xE1EA07A0
72      6.26811396      target2.exe:284         CloseKey        HKCU    SUCCESS Key:
0xE1CC0AC0
73      6.30466358      target2.exe:284         OpenKey
        HKLM\System\CurrentControlSet\Control\ServiceCurrent SUCCESS Key: 0xE1CC0AC0

74      6.30469599      target2.exe:284         QueryValue
        HKLM\System\CurrentControlSet\Control\ServiceCurrent\(Default)      SUCCESS 0x9

75      6.30474571      target2.exe:284         CloseKey
        HKLM\System\CurrentControlSet\Control\ServiceCurrent SUCCESS Key: 0xE1CC0AC0

76      21.30137015     target2.exe:284         CloseKey        HKLM    SUCCESS Key:
0xE1F15600
77      26.55605084     WINLOGON.EXE:168        OpenKey HKCU    SUCCESS Key: 0xE1D05180

78      26.55609107     WINLOGON.EXE:168        OpenKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current     SUCCESS Key:
0xE1DF5FC0
79      26.55611342     WINLOGON.EXE:168        QueryValue
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current\(Default)   SUCCESS ""

80      26.55616063     WINLOGON.EXE:168        CloseKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current     SUCCESS Key:
0xE1DF5FC0
81      26.55618130     WINLOGON.EXE:168        CloseKey        HKCU    SUCCESS Key:
0xE1D05180
82      26.55621874     WINLOGON.EXE:168        OpenKey HKCU    SUCCESS Key: 0xE1D05180

83      26.55623578     WINLOGON.EXE:168        OpenKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuPopup\.Current\Active      NOTFOUND

84      26.55624472     WINLOGON.EXE:168        QueryValue      HKCU\(Default)  NOTFOUND

85      26.55626148     WINLOGON.EXE:168        CloseKey        HKCU    SUCCESS Key:
0xE1D05180
86      26.55630841     WINLOGON.EXE:168        OpenKey
        HKLM\Software\Microsoft\Windows\CurrentVersion      SUCCESS Key: 0xE1D05180

87      26.55632406     WINLOGON.EXE:168        OpenKey
        HKLM\Software\Microsoft\Windows\CurrentVersion\Software\Microsoft\Windows\Curr
entVersion     NOTFOUND
```

```
88      26.55634138    WINLOGON.EXE:168       QueryValue
        HKLM\Software\Microsoft\Windows\CurrentVersion\MediaPath    SUCCESS
        "C:\WINNT\Media"
89      26.55636093    WINLOGON.EXE:168       CloseKey
        HKLM\Software\Microsoft\Windows\CurrentVersion       SUCCESS Key: 0xE1D05180

90      27.97856487    WINLOGON.EXE:168       OpenKey HKCU    SUCCESS Key: 0xE1EA07A0

91      27.97860426    WINLOGON.EXE:168       OpenKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuCommand\.Current   SUCCESS Key:
0xE1D05180
92      27.97862745    WINLOGON.EXE:168       QueryValue
        HKCU\AppEvents\Schemes\Apps\.Default\MenuCommand\.Current\(Default) SUCCESS ""

93      27.97867271    WINLOGON.EXE:168       CloseKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuCommand\.Current   SUCCESS Key:
0xE1D05180
94      27.97869282    WINLOGON.EXE:168       CloseKey       HKCU    SUCCESS Key:
0xE1EA07A0
95      27.97872886    WINLOGON.EXE:168       OpenKey HKCU    SUCCESS Key: 0xE1EA07A0

96      27.97874590    WINLOGON.EXE:168       OpenKey
        HKCU\AppEvents\Schemes\Apps\.Default\MenuCommand\.Current\Active    NOTFOUND

97      27.97875568    WINLOGON.EXE:168       QueryValue     HKCU\(Default)  NOTFOUND

98      27.97877216    WINLOGON.EXE:168       CloseKey       HKCU    SUCCESS Key:
0xE1EA07A0
99      27.97881742    WINLOGON.EXE:168       OpenKey
        HKLM\Software\Microsoft\Windows\CurrentVersion       SUCCESS Key: 0xE1EA07A0

100     27.97883390    WINLOGON.EXE:168       OpenKey
        HKLM\Software\Microsoft\Windows\CurrentVersion\Software\Microsoft\Windows\Curr
entVersion     NOTFOUND
101     27.97885206    WINLOGON.EXE:168       QueryValue
        HKLM\Software\Microsoft\Windows\CurrentVersion\MediaPath    SUCCESS
        "C:\WINNT\Media"
102     27.97887106    WINLOGON.EXE:168       CloseKey
        HKLM\Software\Microsoft\Windows\CurrentVersion       SUCCESS Key: 0xE1EA07A0

103     27.97931944    FILEMON.EXE:440        OpenKey
        HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32    NOTFOUND

104     27.97934291    FILEMON.EXE:440        OpenKey
        HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32    NOTFOUND

105     27.97946583    FILEMON.EXE:440        OpenKey HKCU    SUCCESS Key: 0xE1DF5FC0

106     27.97949488    FILEMON.EXE:440        OpenKey
        HKLM\System\CurrentControlSet\Control\Nls\MUILanguages      NOTFOUND

107     27.97952617    FILEMON.EXE:440        OpenKey HKCU\Control Panel\Desktop
        SUCCESS Key: 0xE1E4C460
108     27.97955969    FILEMON.EXE:440        QueryValue     HKCU\Control
Panel\Desktop\MultiUILanguageId       NOTFOUND
109     27.97957506    FILEMON.EXE:440        CloseKey       HKCU\Control Panel\Desktop
        SUCCESS Key: 0xE1E4C460
```

Appendix F

Strace log from target2.exe

```
1 912 624 NtOpenKey (0x80000000, {24, 0, 0x40, 0, 0,
"\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\target2.exe"}, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
2 912 624 NtOpenKey (0x80000000, {24, 0, 0x40, 0, 0,
"\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\target2.exe"}, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
3 912 624 NtCreateEvent (0x100003, 0x0, 1, 0, ... 12, ) == 0x0
4 912 624 NtCreateEvent (0x100003, 0x0, 1, 0, ... 16, ) == 0x0
5 912 624 NtQuerySystemInformation (0, 1243348, 44, 0, ... ) == 0x0
6 912 624 NtAllocateVirtualMemory (-1, 1243292, 0, 1243512, 8192, 4, ... ) == 0x0
7 912 624 NtAllocateVirtualMemory (-1, 1243464, 0, 1243516, 4096, 4, ... ) == 0x0
8 912 624 NtCreateEvent (0x100003, 0x0, 1, 0, ... 20, ) == 0x0
9 912 624 NtAllocateVirtualMemory (-1, 1242760, 0, 1242792, 4096, 4, ... ) == 0x0
10 912 624 NtOpenKey (0x80000000, {24, 0, 0x40, 0, 0,
"\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\target2.exe"}, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
11 912 624 NtOpenDirectoryObject (0x3, {24, 0, 0x40, 0, 0, "\KnownDlls"}, ... 24, ) ==
0x0
12 912 624 NtOpenSymbolicLinkObject (0x1, {24, 24, 0x40, 0, 0, "KnownDllPath"}, ...
28, ) == 0x0
13 912 624 NtQuerySymbolicLinkObject (28, ... "C:\WINNT\system32", 0x0, ) == 0x0
14 912 624 NtClose (28, ... ) == 0x0
15 912 624 NtFsControlFile (0, 0, 0, 0, 1243132, 589864, 0, 0, 0, 0, ... ) ==
STATUS_INVALID_HANDLE
16 912 624 NtFsControlFile (0, 0, 0, 0, 1242448, 589864, 0, 0, 0, 0, ... ) ==
STATUS_INVALID_HANDLE
17 912 624 NtOpenFile (0x100020, {24, 0, 0x42, 0, 0, "\??\C:\binary analysis\"},
1243404, 3, 33, ... 28, ) == 0x0
18 912 624 NtQueryVolumeInformationFile (28, 1243404, 1243436, 8, 4, ... ) == 0x0
19 912 624 NtOpenSection (0xe, {24, 24, 0x40, 0, 0, "KERNEL32.dll"}, ... 32, ) == 0x0
20 912 624 NtMapViewOfSection (32, -1, 1243364, 0, 0, 0, 1243356, 1, 0, 4, ... ) ==
0x0
21 912 624 NtClose (32, ... ) == 0x0
22 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
23 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 32, 1243220, ... ) == 0x0
24 912 624 NtFlushInstructionCache (-1, 2011697152, 1324, ... ) == 0x0
25 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 4, 1243344, ... ) == 0x0
26 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 2, 1243344, ... ) == 0x0
27 912 624 NtFlushInstructionCache (-1, 4206592, 296, ... ) == 0x0
28 912 624 NtOpenSection (0xe, {24, 24, 0x40, 0, 0, "ADVAPI32.dll"}, ... 32, ) == 0x0
29 912 624 NtMapViewOfSection (32, -1, 1243364, 0, 0, 0, 1243356, 1, 0, 4, ... ) ==
0x0
30 912 624 NtClose (32, ... ) == 0x0
31 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
32 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 32, 1243220, ... ) == 0x0
33 912 624 NtFlushInstructionCache (-1, 2010845184, 1428, ... ) == 0x0
34 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
35 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 32, 1243220, ... ) == 0x0
36 912 624 NtFlushInstructionCache (-1, 2010845184, 1428, ... ) == 0x0
37 912 624 NtOpenSection (0xe, {24, 24, 0x40, 0, 0, "RPCRT4.DLL"}, ... 32, ) == 0x0
38 912 624 NtMapViewOfSection (32, -1, 1243240, 0, 0, 0, 1243232, 1, 0, 4, ... ) ==
0x0
39 912 624 NtClose (32, ... ) == 0x0
40 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 4, 1243096, ... ) == 0x0
41 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 32, 1243096, ... ) == 0x0
42 912 624 NtFlushInstructionCache (-1, 2010320896, 784, ... ) == 0x0
43 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 4, 1243096, ... ) == 0x0
44 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 32, 1243096, ... ) == 0x0
45 912 624 NtFlushInstructionCache (-1, 2010320896, 784, ... ) == 0x0
46 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 4, 1243096, ... ) == 0x0
47 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 32, 1243096, ... ) == 0x0
48 912 624 NtFlushInstructionCache (-1, 2010320896, 784, ... ) == 0x0
49 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
50 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 32, 1243220, ... ) == 0x0
51 912 624 NtFlushInstructionCache (-1, 2010845184, 1428, ... ) == 0x0
52 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 4, 1243344, ... ) == 0x0
53 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 2, 1243344, ... ) == 0x0
54 912 624 NtFlushInstructionCache (-1, 4206592, 296, ... ) == 0x0
55 912 624 NtOpenSection (0xe, {24, 24, 0x40, 0, 0, "WS2_32.dll"}, ... ) ==
STATUS_OBJECT_NAME_NOT_FOUND
```

```
56 912 624 NtFsControlFile (28, 0, 0, 0, 1242152, 589864, 0, 0, 0, 0, ... ) == 0x0
57 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0, "\??\C:\binary
analysis\WS2_32.dll"}, 1243076, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
58 912 624 NtFsControlFile (28, 0, 0, 0, 1242152, 589864, 0, 0, 0, 0, ... ) == 0x0
59 912 624 NtQueryAttributesFile ({24, 28, 0x40, 0, 0, "WS2_32.dll"}, 1243076, ... )
== STATUS_OBJECT_NAME_NOT_FOUND
60 912 624 NtFsControlFile (28, 0, 0, 0, 1242152, 589864, 0, 0, 0, 0, ... ) == 0x0
61 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0,
"\??\C:\WINNT\System32\WS2_32.dll"}, 1243076, ... ) == 0x0
62 912 624 NtFsControlFile (28, 0, 0, 0, 1242908, 589864, 0, 0, 0, 0, ... ) == 0x0
63 912 624 NtFsControlFile (28, 0, 0, 0, 1242352, 589864, 0, 0, 0, 0, ... ) == 0x0
64 912 624 NtOpenFile (0x100020, {24, 0, 0x40, 0, 0,
"\??\C:\WINNT\System32\WS2_32.dll"}, 1243232, 5, 96, ... 32, ) == 0x0
65 912 624 NtCreateSection (0xf, 0x0, 0, 16, 16777216, 32, ... 36, ) == 0x0
66 912 624 NtClose (32, ... ) == 0x0
67 912 624 NtMapViewOfSection (36, -1, 1243364, 0, 0, 0, 1243356, 1, 0, 4, ... ) ==
0x0
68 912 624 NtClose (36, ... ) == 0x0
69 912 624 NtOpenSection (0xe, {24, 24, 0x40, 0, 0, "MSVCRT.DLL"}, ... 36, ) == 0x0
70 912 624 NtMapViewOfSection (36, -1, 1243240, 0, 0, 0, 1243232, 1, 0, 4, ... ) ==
0x0
71 912 624 NtClose (36, ... ) == 0x0
72 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 4, 1243096, ... ) == 0x0
73 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 2, 1243096, ... ) == 0x0
74 912 624 NtFlushInstructionCache (-1, 2013474816, 564, ... ) == 0x0
75 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
76 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 32, 1243220, ... ) == 0x0
77 912 624 NtFlushInstructionCache (-1, 1963134976, 388, ... ) == 0x0
78 912 624 NtOpenSection (0xe, {24, 24, 0x40, 0, 0, "WS2HELP.DLL"}, ... ) ==
STATUS_OBJECT_NAME_NOT_FOUND
79 912 624 NtFsControlFile (28, 0, 0, 0, 1242028, 589864, 0, 0, 0, 0, ... ) == 0x0
80 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0, "\??\C:\binary
analysis\WS2HELP.DLL"}, 1242952, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
81 912 624 NtFsControlFile (28, 0, 0, 0, 1242028, 589864, 0, 0, 0, 0, ... ) == 0x0
82 912 624 NtQueryAttributesFile ({24, 28, 0x40, 0, 0, "WS2HELP.DLL"}, 1242952, ... )
== STATUS_OBJECT_NAME_NOT_FOUND
83 912 624 NtFsControlFile (28, 0, 0, 0, 1242028, 589864, 0, 0, 0, 0, ... ) == 0x0
84 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0,
"\??\C:\WINNT\System32\WS2HELP.DLL"}, 1242952, ... ) == 0x0
85 912 624 NtFsControlFile (28, 0, 0, 0, 1242784, 589864, 0, 0, 0, 0, ... ) == 0x0
86 912 624 NtFsControlFile (28, 0, 0, 0, 1242228, 589864, 0, 0, 0, 0, ... ) == 0x0
87 912 624 NtOpenFile (0x100020, {24, 0, 0x40, 0, 0,
"\??\C:\WINNT\System32\WS2HELP.DLL"}, 1243108, 5, 96, ... 36, ) == 0x0
88 912 624 NtCreateSection (0xf, 0x0, 0, 16, 16777216, 36, ... 32, ) == 0x0
89 912 624 NtClose (36, ... ) == 0x0
90 912 624 NtMapViewOfSection (32, -1, 1243240, 0, 0, 0, 1243232, 1, 0, 4, ... ) ==
0x0
91 912 624 NtClose (32, ... ) == 0x0
92 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 4, 1243096, ... ) == 0x0
93 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 32, 1243096, ... ) == 0x0
94 912 624 NtFlushInstructionCache (-1, 1963069440, 308, ... ) == 0x0
95 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 4, 1243096, ... ) == 0x0
96 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 32, 1243096, ... ) == 0x0
97 912 624 NtFlushInstructionCache (-1, 1963069440, 308, ... ) == 0x0
98 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 4, 1243096, ... ) == 0x0
99 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 32, 1243096, ... ) == 0x0
100 912 624 NtFlushInstructionCache (-1, 1963069440, 308, ... ) == 0x0
101 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
102 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 32, 1243220, ... ) == 0x0
103 912 624 NtFlushInstructionCache (-1, 1963134976, 388, ... ) == 0x0
104 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 4, 1243344, ... ) == 0x0
105 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 2, 1243344, ... ) == 0x0
106 912 624 NtFlushInstructionCache (-1, 4206592, 296, ... ) == 0x0
107 912 624 NtOpenSection (0xe, {24, 24, 0x40, 0, 0, "MFC42.DLL"}, ... ) ==
STATUS_OBJECT_NAME_NOT_FOUND
108 912 624 NtFsControlFile (28, 0, 0, 0, 1242152, 589864, 0, 0, 0, 0, ... ) == 0x0
109 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0, "\??\C:\binary
analysis\MFC42.DLL"}, 1243076, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
110 912 624 NtFsControlFile (28, 0, 0, 0, 1242152, 589864, 0, 0, 0, 0, ... ) == 0x0
111 912 624 NtQueryAttributesFile ({24, 28, 0x40, 0, 0, "MFC42.DLL"}, 1243076, ... )
== STATUS_OBJECT_NAME_NOT_FOUND
112 912 624 NtFsControlFile (28, 0, 0, 0, 1242152, 589864, 0, 0, 0, 0, ... ) == 0x0
113 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0,
"\??\C:\WINNT\System32\MFC42.DLL"}, 1243076, ... ) == 0x0
114 912 624 NtFsControlFile (28, 0, 0, 0, 1242908, 589864, 0, 0, 0, 0, ... ) == 0x0
115 912 624 NtFsControlFile (28, 0, 0, 0, 1242352, 589864, 0, 0, 0, 0, ... ) == 0x0
```

```
116 912 624 NtOpenFile (0x100020, {24, 0, 0x40, 0, 0,
"\??\C:\WINNT\System32\MFC42.DLL"}, 1243232, 5, 96, ... 32, ) == 0x0
117 912 624 NtCreateSection (0xf, 0x0, 0, 16, 16777216, 32, ... 36, ) == 0x0
118 912 624 NtClose (32, ... ) == 0x0
119 912 624 NtMapViewOfSection (36, -1, 1243364, 0, 0, 0, 1243356, 1, 0, 4, ... ) ==
0x0
120 912 624 NtClose (36, ... ) == 0x0
121 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
122 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 2, 1243220, ... ) == 0x0
123 912 624 NtFlushInstructionCache (-1, 1816178688, 2076, ... ) == 0x0
124 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
125 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 2, 1243220, ... ) == 0x0
126 912 624 NtFlushInstructionCache (-1, 1816178688, 2076, ... ) == 0x0
127 912 624 NtOpenSection (0xe, {24, 24, 0x40, 0, 0, "GDI32.dll"}, ... 36, ) == 0x0
128 912 624 NtMapViewOfSection (36, -1, 1243240, 0, 0, 0, 1243232, 1, 0, 4, ... ) ==
0x0
129 912 624 NtClose (36, ... ) == 0x0
130 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 4, 1243096, ... ) == 0x0
131 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 32, 1243096, ... ) == 0x0
132 912 624 NtFlushInstructionCache (-1, 2012483584, 440, ... ) == 0x0
133 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 4, 1243096, ... ) == 0x0
134 912 624 NtProtectVirtualMemory (-1, 1243152, 1243092, 32, 1243096, ... ) == 0x0
135 912 624 NtFlushInstructionCache (-1, 2012483584, 440, ... ) == 0x0
136 912 624 NtOpenSection (0xe, {24, 24, 0x40, 0, 0, "USER32.DLL"}, ... 36, ) == 0x0
137 912 624 NtMapViewOfSection (36, -1, 1243116, 0, 0, 0, 1243108, 1, 0, 4, ... ) ==
0x0
138 912 624 NtClose (36, ... ) == 0x0
139 912 624 NtProtectVirtualMemory (-1, 1243028, 1242968, 4, 1242972, ... ) == 0x0
140 912 624 NtProtectVirtualMemory (-1, 1243028, 1242968, 32, 1242972, ... ) == 0x0
141 912 624 NtFlushInstructionCache (-1, 2011238400, 1200, ... ) == 0x0
142 912 624 NtProtectVirtualMemory (-1, 1243028, 1242968, 4, 1242972, ... ) == 0x0
143 912 624 NtProtectVirtualMemory (-1, 1243028, 1242968, 32, 1242972, ... ) == 0x0
144 912 624 NtFlushInstructionCache (-1, 2011238400, 1200, ... ) == 0x0
145 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
146 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 2, 1243220, ... ) == 0x0
147 912 624 NtFlushInstructionCache (-1, 1816178688, 2076, ... ) == 0x0
148 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
149 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 2, 1243220, ... ) == 0x0
150 912 624 NtFlushInstructionCache (-1, 1816178688, 2076, ... ) == 0x0
151 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 4, 1243344, ... ) == 0x0
152 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 2, 1243344, ... ) == 0x0
153 912 624 NtFlushInstructionCache (-1, 4206592, 296, ... ) == 0x0
154 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 4, 1243344, ... ) == 0x0
155 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 2, 1243344, ... ) == 0x0
156 912 624 NtFlushInstructionCache (-1, 4206592, 296, ... ) == 0x0
157 912 624 NtOpenSection (0xe, {24, 24, 0x40, 0, 0, "MSVCP60.dll"}, ... ) ==
STATUS_OBJECT_NAME_NOT_FOUND
158 912 624 NtFsControlFile (28, 0, 0, 0, 1242152, 589864, 0, 0, 0, 0, ... ) == 0x0
159 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0, "\??\C:\binary
analysis\MSVCP60.dll"}, 1243076, ... ) == 0x0
160 912 624 NtFsControlFile (28, 0, 0, 0, 1242908, 589864, 0, 0, 0, 0, ... ) == 0x0
161 912 624 NtFsControlFile (28, 0, 0, 0, 1242352, 589864, 0, 0, 0, 0, ... ) == 0x0
162 912 624 NtOpenFile (0x100020, {24, 0, 0x40, 0, 0, "\??\C:\binary
analysis\MSVCP60.dll"}, 1243232, 5, 96, ... 36, ) == 0x0
163 912 624 NtCreateSection (0xf, 0x0, 0, 16, 16777216, 36, ... 32, ) == 0x0
164 912 624 NtClose (36, ... ) == 0x0
165 912 624 NtMapViewOfSection (32, -1, 1243364, 0, 0, 0, 1243356, 1, 0, 4, ... ) ==
0x0
166 912 624 NtClose (32, ... ) == 0x0
167 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
168 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 2, 1243220, ... ) == 0x0
169 912 624 NtFlushInstructionCache (-1, 2014228480, 360, ... ) == 0x0
170 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 4, 1243220, ... ) == 0x0
171 912 624 NtProtectVirtualMemory (-1, 1243276, 1243216, 2, 1243220, ... ) == 0x0
172 912 624 NtFlushInstructionCache (-1, 2014228480, 360, ... ) == 0x0
173 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 4, 1243344, ... ) == 0x0
174 912 624 NtProtectVirtualMemory (-1, 1243400, 1243340, 2, 1243344, ... ) == 0x0
175 912 624 NtFlushInstructionCache (-1, 4206592, 296, ... ) == 0x0
176 912 624 NtOpenKey (0x80000000, {24, 0, 0x40, 0, 0,
"\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\target2.exe"}, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
177 912 624 NtQuerySystemInformation (50, 2012088280, 4, 0, ... ) == 0x0
178 912 624 NtQuerySystemInformation (0, 2013060640, 44, 0, ... ) == 0x0
179 912 624 NtCreateSection (0xf001f, 0x0, 1242536, 4, 67108864, 0, ... 32, ) == 0x0
180 912 624 NtSecureConnectPort ("\Windows\ApiPort", 1242524, 1242488, 1254584,
1242512, 1242552, 1242448, 1242556, ... 40, ) == 0x0
181 912 624 NtClose (32, ... ) == 0x0
```

```
182 912 624 NtQueryObject (40, 4, 1242426, 2, 0, ... ) == 0x0
183 912 624 NtSetInformationObject (40, 4, 1242426, 2, ... ) == 0x0
184 912 624 NtQuerySystemInformation (0, 1242260, 44, 0, ... ) == 0x0
185 912 624 NtQueryVirtualMemory (-1, 2293760, 0, 1242328, 28, 0, ... ) == 0x0
186 912 624 NtAllocateVirtualMemory (-1, 1242376, 0, 1242428, 4096, 4, ... ) == 0x0
187 912 624 NtCreateEvent (0x100003, 0x0, 1, 0, ... 32, ) == 0x0
188 912 624 NtRequestWaitReplyPort (40, {28, 52, 0, 1256860, 1243332, 2013060448,
2012788137}, ... {28, 52, 2, 912, 624, 13203, 0}, ) == 0x0
189 912 624 NtRegisterThreadTerminatePort (40, ... ) == 0x0
190 912 624 NtFsControlFile (28, 0, 0, 0, 1241784, 589864, 0, 0, 0, 0, ... ) == 0x0
191 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0, "\??\C:\binary
analysis\target2.exe.Local"}, 1242708, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
192 912 624 NtAllocateVirtualMemory (-1, -1092756228, 0, -1092756232, 4096, 260, ... )
== 0x0
193 912 624 NtOpenMutant (0x1, {24, 0, 0x40, 0, 0, "\NlsCacheMutant"}, ... 44, ) ==
0x0
194 912 624 NtAllocateVirtualMemory (-1, 1242272, 0, 1242304, 4096, 4, ... ) == 0x0
195 912 624 NtOpenSection (0x4, {24, 0, 0x40, 0, 0, "\NLS\NlsSectionUnicode"}, ... 48,
) == 0x0
196 912 624 NtMapViewOfSection (48, -1, 1242756, 0, 0, 0, 1242632, 2, 0, 2, ... ) ==
0x0
197 912 624 NtClose (48, ... ) == 0x0
198 912 624 NtQueryDefaultLocale (0, 2012087320, ... ) == 0x0
199 912 624 NtOpenSection (0x4, {24, 0, 0x40, 0, 0, "\NLS\NlsSectionLocale"}, ... 48,
) == 0x0
200 912 624 NtMapViewOfSection (48, -1, 1242744, 0, 0, 0, 1242656, 2, 0, 2, ... ) ==
0x0
201 912 624 NtClose (48, ... ) == 0x0
202 912 624 NtOpenSection (0x5, {24, 0, 0x40, 0, 0, "\NLS\NlsSectionSortkey"}, ... 48,
) == 0x0
203 912 624 NtMapViewOfSection (48, -1, 1242752, 0, 0, 0, 1242644, 2, 0, 2, ... ) ==
0x0
204 912 624 NtQuerySection (48, 0, 1242728, 16, 0, ... ) == 0x0
205 912 624 NtClose (48, ... ) == 0x0
206 912 624 NtOpenSection (0x4, {24, 0, 0x40, 0, 0, "\NLS\NlsSectionSortTbls"}, ...
48, ) == 0x0
207 912 624 NtMapViewOfSection (48, -1, 1242756, 0, 0, 0, 1242664, 2, 0, 2, ... ) ==
0x0
208 912 624 NtClose (48, ... ) == 0x0
209 912 624 NtQueryVirtualMemory (-1, 2147295232, 0, 1242716, 28, 0, ... ) == 0x0
210 912 624 NtOpenSection (0x4, {24, 0, 0x40, 0, 0, "\NLS\NlsSectionSortkey00000C09"},
... ) == STATUS_OBJECT_NAME_NOT_FOUND
211 912 624 NtRequestWaitReplyPort (40, {28, 52, 0, 2013060256, 1241604, 2012088192,
2013057856}, ... {28, 52, 2, 912, 624, 13204, 0}, ) == 0x0
212 912 624 NtWaitForMultipleObjects (2, 1240708, 1, 0, 0, ... ) == 0x0
213 912 624 NtClose (48, ... ) == 0x0
214 912 624 NtClose (52, ... ) == 0x0
215 912 624 NtRequestWaitReplyPort (40, {24, 48, 0, 0, 1048579, 1240464, 1241540}, ...
{24, 48, 2, 912, 624, 13205, 0}, ) == 0x0
216 912 624 NtAllocateVirtualMemory (-1, 1242824, 0, 1242856, 4096, 4, ... ) == 0x0
217 912 624 NtOpenKey (0x1, {24, 0, 0x40, 0, 0,
"\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager"}, ... 52, ) ==
0x0
218 912 624 NtQueryValueKey (52, "SafeDllSearchMode", 2, 1243088, 16, 1243112, ... )
== STATUS_OBJECT_NAME_NOT_FOUND
219 912 624 NtClose (52, ... ) == 0x0
220 912 624 NtOpenProcessToken (-1, 0x8, ... 52, ) == 0x0
221 912 624 NtQueryInformationToken (52, 11, 0, 0, 1242624, ... ) ==
STATUS_BUFFER_TOO_SMALL
222 912 624 NtQueryInformationToken (52, 11, 1264600, 4, 1242624, ... ) == 0x0
223 912 624 NtClose (52, ... ) == 0x0
224 912 624 NtOpenKey (0x20019, {24, 0, 0x40, 0, 0,
"\Registry\Machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"}, ... 52, )
== 0x0
225 912 624 NtQueryValueKey (52, "LeakTrack", 2, 1242560, 144, 1242712, ... ) ==
STATUS_OBJECT_NAME_NOT_FOUND
226 912 624 NtClose (52, ... ) == 0x0
227 912 624 NtOpenKey (0x2000000, {24, 0, 0x40, 0, 0, "\REGISTRY\MACHINE"}, ... 52, )
== 0x0
228 912 624 NtOpenKey (0x20019, {24, 52, 0x40, 0, 0, "Software\Microsoft\Windows
NT\CurrentVersion\Diagnostics"}, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
229 912 624 NtQuerySystemInformation (0, 1242992, 44, 0, ... ) == 0x0
230 912 624 NtAllocateVirtualMemory (-1, 1242936, 0, 1243156, 8192, 4, ... ) == 0x0
231 912 624 NtAllocateVirtualMemory (-1, 1243108, 0, 1243160, 4096, 4, ... ) == 0x0
232 912 624 NtCreateEvent (0x100003, 0x0, 1, 0, ... 48, ) == 0x0
233 912 624 NtAllocateVirtualMemory (-1, 1242404, 0, 1242436, 4096, 4, ... ) == 0x0
```

```
234 912 624 NtRequestWaitReplyPort (40, {28, 52, 0, 65536, 1265304, 3080192, 1245944},
... {28, 52, 2, 912, 624, 13206, 0}, ) == 0x0
235 912 624 NtQueryVolumeInformationFile (8, 1243084, 1243092, 8, 4, ... ) == 0x0
236 912 624 NtRequestWaitReplyPort (40, {28, 52, 0, 912, 624, 13206, 0}, ... {28, 52,
2, 912, 624, 13207, 0}, ) == 0x0
237 912 624 NtOpenSection (0x4, {24, 0, 0x40, 0, 0, "\NLS\NlsSectionCType"}, ... 64, )
== 0x0
238 912 624 NtMapViewOfSection (64, -1, 1241636, 0, 0, 0, 1241540, 2, 0, 2, ... ) ==
0x0
239 912 624 NtClose (64, ... ) == 0x0
240 912 624 NtAllocateVirtualMemory (-1, 1242628, 0, 1242660, 4096, 4, ... ) == 0x0
241 912 624 NtQuerySystemInformation (0, 1243196, 44, 0, ... ) == 0x0
242 912 624 NtQuerySystemInformation (1, 1243240, 12, 0, ... ) == 0x0
243 912 624 NtQuerySystemInformation (0, 1243304, 44, 0, ... ) == 0x0
244 912 624 NtRequestWaitReplyPort (40, {28, 52, 0, 2097224, 2097184, 2097184,
2097184}, ... {28, 52, 2, 912, 624, 13208, 0}, ) == 0x0
245 912 624 NtOpenKey (0x20019, {24, 0, 0x40, 0, 0,
"\Registry\Machine\System\CurrentControlSet\Control\Error Message Instrument\"}, ... )
== STATUS_OBJECT_NAME_NOT_FOUND
246 912 624 NtMapViewOfSection (64, -1, -1096348376, 0, 0, 0, -1096348388, 2, 0, 2,
... ) == 0x0
247 912 624 NtCreateEvent (0x1f0003, 0x0, 1, 0, ... 68, ) == 0x0
248 912 624 NtQueryObject (68, 4, -1096348498, 2, 0, ... ) == 0x0
249 912 624 NtSetInformationObject (68, 4, -1096348498, 2, ... ) == 0x0
250 912 624 NtOpenThreadToken (-2, 0x8, 1, ... ) == STATUS_NO_TOKEN
251 912 624 NtOpenProcessToken (-1, 0x8, ... 72, ) == 0x0
252 912 624 NtQueryInformationToken (72, 10, 0, 0, -1096348860, ... ) ==
STATUS_BUFFER_TOO_SMALL
253 912 624 NtQueryInformationToken (72, 10, -504580952, 56, -1096348860, ... ) == 0x0
254 912 624 NtClose (72, ... ) == 0x0
255 912 624 NtAllocateVirtualMemory (-1, -1096348616, 0, -1096348688, 4096, 4, ... )
== 0x0
256 912 624 NtFreeVirtualMemory (-1, -1096348616, -1096348688, 32768, ... ) == 0x0
257 912 624 NtOpenKey (0x20019, {24, 0, 0x240, 0, 0,
"\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32"}, ...
-2147483388, ) == 0x0
258 912 624 NtQueryValueKey (-2147483388, "target2", 2, -504584600, 332, -1096349012,
... ) == STATUS_OBJECT_NAME_NOT_FOUND
259 912 624 NtClose (-2147483388, ... ) == 0x0
260 912 624 NtOpenKey (0x20019, {24, 0, 0x240, 0, 0,
"\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2"}, ...
-2147483388, ) == 0x0
261 912 624 NtQueryValueKey (-2147483388, "target20.0", 2, -516371928, 32, -
1096349008, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
262 912 624 NtClose (-2147483388, ... ) == 0x0
263 912 624 NtOpenKey (0x20019, {24, 0, 0x240, 0, 0,
"\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility"},
... -2147483388, ) == 0x0
264 912 624 NtQueryValueKey (-2147483388, "target2", 2, -507912920, 332, -1096349236,
... ) == STATUS_OBJECT_NAME_NOT_FOUND
265 912 624 NtClose (-2147483388, ... ) == 0x0
266 912 624 NtQueryDefaultLocale (0, -1096349008, ... ) == 0x0
267 912 624 NtGdiQueryFontAssocInfo (0, ... ) == 0x0
268 912 624 NtUserCallNoParam (18, ... ) == 0x0
269 912 624 NtGdiCreateCompatibleDC (0, ...
270 912 624 NtAllocateVirtualMemory (-1, -1096350628, 0, -1096350632, 12288, 4, ... )
== 0x0
269 912 624 NtGdiCreateCompatibleDC ) == 0xd7010443
271 912 624 NtGdiGetStockObject (0, ... ) == 0x1900010
272 912 624 NtGdiGetStockObject (4, ... ) == 0x1900011
273 912 624 NtGdiCreateBitmap (8, 8, 1, 1, 2011347328, ... ) == 0x4d05020f
274 912 624 NtGdiCreateSolidBrush (0, 0, ...
275 912 624 NtAllocateVirtualMemory (-1, -1096350616, 0, -1096350620, 12288, 4, ... )
== 0x0
274 912 624 NtGdiCreateSolidBrush ) == 0xf810024f
276 912 624 NtGdiGetStockObject (13, ... ) == 0x18a0021
277 912 624 NtGdiCreateCompatibleDC (0, ... ) == 0x77010424
278 912 624 NtGdiSelectBitmap (1996555300, 1292173839, ... ) == 0x185000f
279 912 624 NtUserGetThreadDesktop (624, 0, ... ) == 0x4c
280 912 624 NtOpenKey (0x80000000, {24, 0, 0x40, 0, 0,
"\Registry\Machine\System\CurrentControlSet\Control\Session
Manager\AppCompatibility\target2.exe"}, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
281 912 624 NtOpenKey (0x20019, {24, 0, 0x40, 0, 0,
"\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Windows"}, ... 80, )
== 0x0
282 912 624 NtQueryValueKey (80, "AppInit_DLLs", 2, 1241552, 64, 1241656, ... ) == 0x0
283 912 624 NtClose (80, ... ) == 0x0
```

```
284 912 624 NtUserFindExistingCursorIcon (1240952, 1240968, 1241536, ... ) == 0x10011
285 912 624 NtUserRegisterClassExWOW (1241492, 1241556, 1241572, 2011300511, 128, 0,
... ) == 0x815cc017
286 912 624 NtUserFindExistingCursorIcon (1240952, 1240968, 1241536, ... ) == 0x10011
287 912 624 NtUserRegisterClassExWOW (1241492, 1241556, 1241572, 2011300512, 128, 0,
... ) == 0x815cc01c
288 912 624 NtUserFindExistingCursorIcon (1240952, 1240968, 1241536, ... ) == 0x10011
289 912 624 NtUserRegisterClassExWOW (1241492, 1241556, 1241572, 2011300513, 128, 0,
... ) == 0x815cc01e
290 912 624 NtUserFindExistingCursorIcon (1240952, 1240968, 1241536, ... ) == 0x10011
291 912 624 NtUserRegisterClassExWOW (1241492, 1241556, 1241572, 674, 128, 0, ... ) ==
0x815c8002
292 912 624 NtUserFindExistingCursorIcon (1240952, 1240968, 1241536, ... ) == 0x10013
293 912 624 NtUserRegisterClassExWOW (1241492, 1241556, 1241572, 2011300515, 128, 0,
... ) == 0x815cc018
294 912 624 NtUserFindExistingCursorIcon (1240952, 1240968, 1241536, ... ) == 0x10011
295 912 624 NtUserRegisterClassExWOW (1241492, 1241556, 1241572, 2011300516, 128, 0,
... ) == 0x815cc01a
296 912 624 NtUserFindExistingCursorIcon (1240952, 1240968, 1241536, ... ) == 0x10011
297 912 624 NtUserRegisterClassExWOW (1241492, 1241556, 1241572, 2011300517, 128, 0,
... ) == 0x815cc01d
298 912 624 NtUserFindExistingCursorIcon (1240952, 1240968, 1241536, ... ) == 0x10011
299 912 624 NtUserRegisterClassExWOW (1241492, 1241556, 1241572, 2011300519, 128, 0,
... ) == 0x815cc026
300 912 624 NtUserFindExistingCursorIcon (1240952, 1240968, 1241536, ... ) == 0x10011
301 912 624 NtUserRegisterClassExWOW (1241492, 1241556, 1241572, 2011300518, 128, 0,
... ) == 0x815cc019
302 912 624 NtUserRegisterClassExWOW (1241444, 1241508, 1241524, 0, 128, 0, ... ) ==
0x815cc020
303 912 624 NtUserRegisterClassExWOW (1241444, 1241508, 1241524, 0, 130, 0, ... ) ==
0x815cc022
304 912 624 NtUserRegisterClassExWOW (1241444, 1241508, 1241524, 0, 128, 0, ... ) ==
0x815cc023
305 912 624 NtUserRegisterClassExWOW (1241444, 1241508, 1241524, 0, 130, 0, ... ) ==
0x815cc024
306 912 624 NtUserRegisterClassExWOW (1241444, 1241508, 1241524, 0, 128, 0, ... ) ==
0x815cc025
307 912 624 NtCallbackReturn (0, 0, 0, ...
308 912 624 NtGdiInit (... ) == 0x1
309 912 624 NtGdiGetStockObject (18, ... ) == 0x290001c
310 912 624 NtGdiGetStockObject (19, ... ) == 0x1b00019
311 912 624 NtQueryInformationProcess (-1, 12, 1243292, 4, 0, ... ) == 0x0
312 912 624 NtSetInformationProcess (-1, 12, 1243308, 4, ... ) == 0x0
313 912 624 NtQueryInformationProcess (-1, 12, 1243292, 4, 0, ... ) == 0x0
314 912 624 NtSetInformationProcess (-1, 12, 1243308, 4, ... ) == 0x0
315 912 624 NtAllocateVirtualMemory (-1, 1242768, 0, 1242800, 4096, 4, ... ) == 0x0
316 912 624 NtAllocateVirtualMemory (-1, 1243148, 0, 1243144, 8192, 4, ... ) == 0x0
317 912 624 NtAllocateVirtualMemory (-1, 1243156, 0, 1243152, 4096, 4, ... ) == 0x0
318 912 624 NtUserRegisterWindowMessage (1243280, ... ) == 0xc04e
319 912 624 NtUserGetDC (0, ... ) == 0x1010051
320 912 624 NtUserCallOneParam (16842833, 41, ... ) == 0x1
321 912 624 NtUserFindExistingCursorIcon (1242620, 1242636, 1243204, ... ) == 0x10015
322 912 624 NtUserFindExistingCursorIcon (1242620, 1242636, 1243204, ... ) == 0x10011
323 912 624 NtUserRegisterWindowMessage (1243280, ... ) == 0xc04f
324 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc004
325 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc003
326 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc002
327 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc00a
328 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc00b
329 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc00d
330 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc00e
331 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc00f
332 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc006
333 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc007
334 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc050
335 912 624 NtUserRegisterWindowMessage (1243272, ... ) == 0xc051
336 912 624 NtUserRegisterWindowMessage (1243280, ... ) == 0xc04f
337 912 624 NtQueryInformationProcess (-1, 12, 1242980, 4, 0, ... ) == 0x0
338 912 624 NtSetInformationProcess (-1, 12, 1242996, 4, ... ) == 0x0
339 912 624 NtQueryInformationProcess (-1, 12, 1242980, 4, 0, ... ) == 0x0
340 912 624 NtSetInformationProcess (-1, 12, 1242996, 4, ... ) == 0x0
341 912 624 NtQueryDefaultUILanguage (2013063980, ...
342 912 624 NtOpenThreadToken (-2, 0x20008, 1, ... ) == STATUS_NO_TOKEN
343 912 624 NtOpenProcessToken (-1, 0x20008, ... 80, ) == 0x0
344 912 624 NtQueryInformationToken (80, 1, -1096350048, 80, -1096349960, ... ) == 0x0
345 912 624 NtClose (80, ... ) == 0x0
```

```
346 912 624 NtOpenKey (0x2000000, {24, 0, 0x40, 0, 0, "\REGISTRY\USER\S-1-5-21-
515967899-1078145449-1343024091-500"}, ... 80, ) == 0x0
347 912 624 NtOpenKey (0x80000000, {24, 0, 0x240, 0, 0,
"\Registry\Machine\System\CurrentControlSet\Control\Nls\MUILanguages"}, ... ) ==
STATUS_OBJECT_NAME_NOT_FOUND
348 912 624 NtOpenKey (0x80000000, {24, 80, 0x240, 0, 0, "Control Panel\Desktop"}, ...
-2147483388, ) == 0x0
349 912 624 NtQueryValueKey (-2147483388, "MultiUILanguageId", 2, -1096349868, 256, -
1096349604, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
350 912 624 NtClose (-2147483388, ... ) == 0x0
351 912 624 NtClose (80, ... ) == 0x0
341 912 624 NtQueryDefaultUILanguage ) == 0x0
352 912 624 NtQueryInstallUILanguage (2013063982, ... ) == 0x0
353 912 624 NtQueryDefaultLocale (1, 1241928, ... ) == 0x0
354 912 624 NtQueryDefaultLocale (1, 1241848, ... ) == 0x0
355 912 624 NtFsControlFile (28, 0, 0, 0, 1240344, 589864, 0, 0, 0, 0, ... ) == 0x0
356 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0,
"\??\C:\WINNT\System32\MFC42LOC.DLL"}, 1241268, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
357 912 624 NtFsControlFile (28, 0, 0, 0, 1240904, 589864, 0, 0, 0, 0, ... ) == 0x0
358 912 624 NtQueryAttributesFile ({24, 0, 0x40, 0, 0,
"\??\C:\WINNT\System32\MFC42LOC.DLL"}, 1241828, ... ) == STATUS_OBJECT_NAME_NOT_FOUND
359 912 624 NtTestAlert (... ) == 0x0
360 912 624 NtContinue (1244464, 1, ...
361 912 624 NtSetInformationThread (-2, 9, 1245176, 4, ... ) == 0x0
362 912 624 NtOpenKey (0x1, {24, 52, 0x40, 0, 0,
"System\CurrentControlSet\Control\ServiceCurrent"}, ... 80, ) == 0x0
363 912 624 NtQueryValueKey (80, "□", 2, 1244012, 144, 1244164, ... ) == 0x0
364 912 624 NtClose (80, ... ) == 0x0
365 912 624 NtOpenFile (0x100080, {24, 0, 0x40, 0, 0, "\DosDevices\pipe\"}, 1244232,
3, 32, ... 80, ) == 0x0
366 912 624 NtFsControlFile (80, 0, 0, 0, 1244240, 1114136, 1274896, 50, 0, 0, ... )
== STATUS_IO_TIMEOUT
367 912 624 NtClose (80, ... ) == 0x0
368 912 624 NtCreateFile (0xc0100080, {24, 0, 0x40, 0, 1244208,
"\??\pipe\net\NtControlPipe9"}, 1244228, 0, 128, 3, 1, 96, 0, 0, ... ) ==
STATUS_ACCESS_DENIED
369 912 624 NtTerminateProcess (0, 0, ... ) == 0x0
370 912 624 NtSetInformationThread (-2, 10, 1244636, 4, ... ) == 0x0
371 912 624 NtRequestWaitReplyPort (40, {20, 44, 0, 1244676, 1266856, 1244988,
2012964084}, ... {20, 44, 2, 912, 624, 13223, 0}, ) == 0x0
372 912 624 NtTerminateProcess (-1, 0, ...
373 912 624 NtQueryObject (68, 4, -1096349798, 2, 0, ... ) == 0x0
374 912 624 NtSetInformationObject (68, 4, -1096349798, 2, ... ) == 0x0
375 912 624 NtClose (68, ... ) == 0x0
376 912 624 NtClose (76, ... ) == 0x0
377 912 624 NtClose (4, ... ) == 0x0
378 912 624 NtClose (8, ... ) == 0x0
379 912 624 NtClose (12, ... ) == 0x0
380 912 624 NtClose (16, ... ) == 0x0
381 912 624 NtClose (20, ... ) == 0x0
382 912 624 NtClose (24, ... ) == 0x0
383 912 624 NtClose (28, ... ) == 0x0
384 912 624 NtClose (32, ... ) == 0x0
385 912 624 NtClose (36, ... ) == 0x0
386 912 624 NtClose (40, ... ) == 0x0
387 912 624 NtClose (44, ... ) == 0x0
388 912 624 NtClose (48, ... ) == 0x0
389 912 624 NtClose (52, ... ) == 0x0
390 912 624 NtClose (56, ... ) == 0x0
391 912 624 NtClose (60, ... ) == 0x0
392 912 624 NtClose (64, ... ) == 0x0
393 912 624 NtClose (72, ... ) == 0x0
```

Appendix G

FRED1.1 Script Source (Reproduced In It's Entirety From The FIRE CD)

```
title Obtaining live response details
echo off
@echo FRED v1.1 is running...
@echo FRED v1.1 - 2 April 2002 [modified for fire 10/2002] > a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo START TIME >> a:\audit.txt
@call \win32\makeline
time /t >> a:\audit.txt
@time /t
date /t >> a:\audit.txt
@date /t
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo PSINFO >> a:\audit.txt
@call \win32\makeline
\win32\sysinternals\Psinfo >> a:\audit.txt
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo NET ACCOUNTS >> a:\audit.txt
@call \win32\makeline
echo on
net accounts >> a:\audit.txt
echo off
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo NET FILE >> a:\audit.txt
@call \win32\makeline
echo on
net file >> a:\audit.txt
echo off
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo NET SESSION >> a:\audit.txt
@call \win32\makeline
echo on
net session >> a:\audit.txt
echo off
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo NET SHARE >> a:\audit.txt
@call \win32\makeline
echo on
net share >> a:\audit.txt
echo off
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo NET START >> a:\audit.txt
@call \win32\makeline
echo on
net start >> a:\audit.txt
echo off
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo NET USE >> a:\audit.txt
@call \win32\makeline
echo on
net use >> a:\audit.txt
echo off
@echo. >> a:\audit.txt
```

```
@echo. >> a:\audit.txt
@call \win32\makeline
@echo NET USER >> a:\audit.txt
@call \win32\makeline
echo on
net user >> a:\audit.txt
echo off
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo NET VIEW >> a:\audit.txt
@call \win32\makeline
echo on
net view >> a:\audit.txt
echo off
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo ARP (arp -a) >> a:\audit.txt
@call \win32\makeline
arp -a >> a:\audit.txt
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo NETSTAT (netstat -anr) >> a:\audit.txt
@call \win32\makeline
netstat -anr >> a:\audit.txt
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo LOGGED ON >> a:\audit.txt
@call \win32\makeline
\win32\sysinternals\psloggedon >> a:\audit.txt
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo ProcInterrogate >> a:\audit.txt
@call \win32\makeline
\win32\procinterrogate -list >> a:\audit.txt
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo FPORT (fport /p)>> a:\audit.txt
@call \win32\makeline
\win32\foundstone\fport /p >> a:\audit.txt
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo PSLIST (pslist -x) >> a:\audit.txt
@call \win32\makeline
\win32\sysinternals\pslist -x >> a:\audit.txt
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo NBTSTAT >> a:\audit.txt
@call \win32\makeline
nbtstat -c >> a:\audit.txt
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo HIDDEN FILES (dir /s /a:h /t:a c: d:) >> a:\audit.txt
@call \win32\makeline
dir /s /a:h /t:a c: >> a:\audit.txt
dir /s /a:h /t:a d: >> a:\audit.txt
@echo. >> a:\audit.txt
@echo. >> a:\audit.txt
@call \win32\makeline
@echo MD5SUM >> a:\audit.txt
@call \win32\makeline
md5sum c:/*.* >> a:\audit.txt
md5sum c:/winnt/*.* >> a:\audit.txt
md5sum c:/winnt/system/*.* >> a:\audit.txt
md5sum c:/winnt/system32/*.* >> a:\audit.txt
md5sum d:/*.* >> a:\audit.txt
md5sum d:/winnt/*.* >> a:\audit.txt
md5sum d:/winnt/system/*.* >> a:\audit.txt
md5sum d:/winnt/system32/*.* >> a:\audit.txt
```

```
@call \win32\makeline
@echo AT scheduler list >> a:\audit.txt
at >> a:\audit.txt
@call \win32\makeline
@echo END TIME >> a:\audit.txt
@call \win32\makeline
time /t >> a:\audit.txt
@time /t
date /t >> a:\audit.txt
@date /t
@echo.
@echo.
@echo.
@echo.
@echo.
@echo FRED is done.
@echo.
@echo The MD5 sum of the audit log is:
@md5sum a:\audit.txt > a:\audit.md5
@type a:\audit.md5
@echo.
@echo ** WRITE THIS NUMBER DOWN AND INCLUDE IT ON THE EVIDENCE TAG **
@echo (this value also saved to a:\audit.md5)
@echo.
@echo Remove your audit floppy from the computer and write protect it NOW.
echo on
```

Appendix H

FRED Output As Written To A:\Audit.Txt

```
FRED v1.1 - 2 April 2002 [modified for fire 10/2002]

--------------------------------------------------
START TIME
--------------------------------------------------
11:50a
Fri 05/02/2003


--------------------------------------------------
PSINFO
--------------------------------------------------

PsInfo v1.31 - local and remote system information viewer
Copyright (C) 2001-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Querying information for ...

System information for \\HP1:
Uptime:                    1 day, 1 hour, 14 minutes, 0 seconds
Kernel version:            Microsoft Windows 2000, Uniprocessor Free
Product type:              Professional
Product version:           5.0
Service pack:              2
Kernel build number:       2195
Registered organization:
Registered owner:          administrator
Install date:              5/10/2000, 3:46:07 PM
IE version:                6.0000
System root:               C:\WINNT
Processors:                1
Processor speed:           605 MHz
Processor type:            Intel Pentium III
Physical memory:           126 MB
Volume Type       Format     Label                      Size       Free   Free
    A: Removable  FAT                                  1.4 MB     1.4 MB   100%
    C: Fixed      FAT32      ATRYP00ABK                7.8 GB     5.2 GB    66%
    E: CD-ROM     CDFS       FIRE-0.3.5b             220.1 MB                0%



--------------------------------------------------
NET ACCOUNTS
--------------------------------------------------
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.



--------------------------------------------------
NET FILE
--------------------------------------------------
There are no entries in the list.



--------------------------------------------------
NET SESSION
```

```
-------------------------------------------------
There are no entries in the list.


-------------------------------------------------
NET SHARE
-------------------------------------------------

Share name   Resource                        Remark


-------------------------------------------------------------------------------
ADMIN$       C:\WINNT                        Remote Admin
C$           C:\                             Default share
IPC$                                         Remote IPC
The command completed successfully.


-------------------------------------------------
NET START
-------------------------------------------------
These Windows 2000 services are started:


   COM+ Event System
   Computer Browser
   DHCP Client
   Distributed Link Tracking Client
   Event Log
   IPSEC Policy Agent
   Logical Disk Manager
   Messenger
   Network Connections
   Plug and Play
   Print Spooler
   Protected Storage
   Remote Access Connection Manager
   Remote Procedure Call (RPC)
   Remote Registry Service
   Removable Storage
   RunAs Service
   Security Accounts Manager
   Server
   Still Image Service
   System Event Notification
   Task Scheduler
   TCP/IP NetBIOS Helper Service
   Telephony
   Windows Management Instrumentation
   Windows Management Instrumentation Driver Extensions
   WMDM PMSP Service
   Workstation

The command completed successfully.


-------------------------------------------------
NET USE
-------------------------------------------------
New connections will be remembered.


There are no entries in the list.


-------------------------------------------------
NET USER
-------------------------------------------------
```

```
User accounts for \\HP1


-------------------------------------------------------------------------------
Administrator            Fooman                   Guest
The command completed successfully.




-------------------------------------------------
NET VIEW
-------------------------------------------------
There are no entries in the list.




-------------------------------------------------
ARP (arp -a)
-------------------------------------------------
No ARP Entries Found


-------------------------------------------------
NETSTAT (netstat -anr)
-------------------------------------------------
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 01 02 00 0e 15 ...... 3Com EtherLink PCI
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1   1
  255.255.255.255  255.255.255.255  255.255.255.255         1000003   1
===========================================================================
Persistent Routes:
  None

Route Table


-------------------------------------------------
LOGGED ON
-------------------------------------------------

PsLoggedOn v1.21 - Logon Session Displayer
Copyright (C) 1999-2000 Mark Russinovich
SysInternals - www.sysinternals.com

Users logged on locally:
     5/1/2003 10:37:24 AM     HP1\Administrator

No one is logged on via resource shares.


-------------------------------------------------
ProcInterrogate
-------------------------------------------------
ProcInterrogate Version 0.0.1 by Kirby Kuehl vacuum@users.sourceforge.net
-----------------------------------------------------------------------
unknown (Process ID: 0)

        Entry Point  Base      Size       Module
-----------------------------------------------------------------------
unknown (Process ID: 8)

        Entry Point  Base      Size       Module
-----------------------------------------------------------------------
C:\WINNT\System32\smss.exe (Process ID: 140)

        Entry Point  Base      Size       Module
        0x48589586   0x48580000       0000E000   \SystemRoot\System32\smss.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x68011080   0x68010000       000F0000   C:\WINNT\System32\sfcfiles.dll
```

```
---------------------------------------------------------------------------
unknown (Process ID: 164)

        Entry Point  Base      Size       Module
---------------------------------------------------------------------------
C:\WINNT\System32\winlogon.exe (Process ID: 160)

        Entry Point  Base      Size       Module
        0x01001678   0x01000000       0002D000   \??\C:\WINNT\system32\winlogon.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.DLL
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.dll
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.DLL
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.DLL
        0x77C1D43C   0x77C10000       0005D000   C:\WINNT\system32\USERENV.DLL
        0x769A1084   0x769A0000       00007000   C:\WINNT\system32\NDDEAPI.DLL
        0x7698671B   0x76980000       0001B000   C:\WINNT\system32\SFC.DLL
        0x68011080   0x68010000       000F0000   C:\WINNT\system32\sfcfiles.dll
        0x77BE56C2   0x77BE0000       0000F000   C:\WINNT\system32\SECUR32.DLL
        0x690F5D00   0x690F0000       0000B000   C:\WINNT\system32\PROFMAP.DLL
        0x75173309   0x75170000       0004F000   C:\WINNT\system32\NETAPI32.dll
        0x00000000   0x751C0000       00006000   C:\WINNT\system32\NETRAP.DLL
        0x75153777   0x75150000       00010000   C:\WINNT\system32\SAMLIB.DLL
        0x750312D4   0x75030000       00013000   C:\WINNT\system32\WS2_32.DLL
        0x750211AE   0x75020000       00008000   C:\WINNT\system32\WS2HELP.DLL
        0x779536C2   0x77950000       00029000   C:\WINNT\system32\WLDAP32.DLL
        0x77987CC5   0x77980000       00024000   C:\WINNT\system32\DNSAPI.DLL
        0x00000000   0x75050000       00008000   C:\WINNT\system32\WSOCK32.DLL
        0x76B914A8   0x76B90000       00054000   C:\WINNT\system32\msgina.dll
        0x782F7238   0x782F0000       00242000   C:\WINNT\system32\SHELL32.DLL
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.DLL
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.DLL
        0x77574164   0x77570000       00030000   C:\WINNT\system32\WINMM.dll
        0x77882AB8   0x77880000       0008D000   C:\WINNT\system32\setupapi.dll
        0x76952F60   0x76930000       0002B000   C:\WINNT\system32\wintrust.dll
        0x77444ACC   0x77440000       00075000   C:\WINNT\system32\CRYPT32.dll
        0x774333F0   0x77430000       00010000   C:\WINNT\system32\MSASN1.DLL
        0x77921158   0x77920000       00023000   C:\WINNT\system32\IMAGEHLP.dll
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\ole32.dll
        0x76A01380   0x76A00000       00005000   C:\WINNT\system32\mscat32.dll
        0x7CA0D2BA   0x7CA00000       00023000   C:\WINNT\system32\rsaenh.dll
        0x77563789   0x77560000       00009000   C:\WINNT\system32\wdmaud.drv
        0x77821114   0x77820000       00007000   C:\WINNT\system32\VERSION.dll
        0x759B1A3F   0x759B0000       00006000   C:\WINNT\system32\LZ32.DLL
        0x770C6B43   0x770C0000       00023000   C:\WINNT\system32\cscdll.dll
        0x76921388   0x76920000       0000F000   C:\WINNT\system32\WlNotify.dll
        0x769611DD   0x76960000       00017000   C:\WINNT\system32\WINSCARD.DLL
        0x77801AFC   0x77800000       0001D000   C:\WINNT\system32\WINSPOOL.DRV
        0x7784288A   0x77840000       0003C000   C:\WINNT\system32\cscui.dll
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.DLL
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\System32\CLBCATQ.DLL
        0x77402638   0x77400000       00008000   C:\WINNT\system32\msacm32.drv
        0x7741DA10   0x77410000       00013000   C:\WINNT\system32\MSACM32.dll
        0x00000000   0x782D0000       0001E000   C:\WINNT\system32\msv1_0.dll
---------------------------------------------------------------------------
C:\WINNT\System32\services.exe (Process ID: 212)

        Entry Point  Base      Size       Module
        0x010014F8   0x01000000       00018000   C:\WINNT\system32\services.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.DLL
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.DLL
        0x75173309   0x75170000       0004F000   C:\WINNT\system32\NETAPI32.DLL
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.DLL
        0x77BE56C2   0x77BE0000       0000F000   C:\WINNT\system32\SECUR32.DLL
        0x00000000   0x751C0000       00006000   C:\WINNT\system32\NETRAP.DLL
        0x75153777   0x75150000       00010000   C:\WINNT\system32\SAMLIB.DLL
        0x750312D4   0x75030000       00013000   C:\WINNT\system32\WS2_32.DLL
        0x750211AE   0x75020000       00008000   C:\WINNT\system32\WS2HELP.DLL
        0x779536C2   0x77950000       00029000   C:\WINNT\system32\WLDAP32.DLL
        0x77987CC5   0x77980000       00024000   C:\WINNT\system32\DNSAPI.DLL
        0x00000000   0x75050000       00008000   C:\WINNT\system32\WSOCK32.DLL
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.DLL
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
```

```
        0x767A3C6C   0x767A0000       00018000   C:\WINNT\system32\UMPNPMGR.DLL
        0x77C1D43C   0x77C10000       0005D000   C:\WINNT\system32\USERENV.DLL
        0x76812A40   0x76810000       0003B000   C:\WINNT\system32\SCESRV.DLL
        0x77BF39C5   0x77BF0000       00011000   C:\WINNT\system32\NTDSAPI.DLL
        0x00000000   0x76890000       0000E000   C:\WINNT\system32\eventlog.dll
        0x7736727A   0x77360000       00019000   C:\WINNT\system32\dhcpcsvc.dll
        0x775218B2   0x77520000       00005000   C:\WINNT\system32\ICMP.DLL
        0x77342C35   0x77340000       00013000   C:\WINNT\system32\IPHLPAPI.DLL
        0x77321290   0x77320000       00017000   C:\WINNT\system32\MPRAPI.DLL
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\OLE32.DLL
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.DLL
        0x773B123C   0x773B0000       0002E000   C:\WINNT\system32\ACTIVEDS.DLL
        0x773812A8   0x77380000       00022000   C:\WINNT\system32\ADSLDPC.DLL
        0x77831D22   0x77830000       0000E000   C:\WINNT\system32\RTUTILS.DLL
        0x77882AB8   0x77880000       0008D000   C:\WINNT\system32\SETUPAPI.DLL
        0x774E24E0   0x774E0000       00032000   C:\WINNT\system32\RASAPI32.DLL
        0x774C2170   0x774C0000       00011000   C:\WINNT\system32\RASMAN.DLL
        0x77532E60   0x77530000       00022000   C:\WINNT\system32\TAPI32.DLL
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.DLL
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.DLL
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\system32\CLBCATQ.DLL
        0x00000000   0x76880000       00006000   C:\WINNT\system32\lmhsvc.dll
        0x65782421   0x65780000       0000C000   C:\WINNT\system32\WINSTA.DLL
        0x74FD182C   0x74FD0000       0001F000   C:\WINNT\system32\msafd.dll
        0x750111A4   0x75010000       00007000   C:\WINNT\System32\wshtcpip.dll
        0x768C1854   0x768C0000       00006000   C:\WINNT\system32\dmserver.dll
        0x00000000   0x770B0000       00007000   C:\WINNT\system32\CFGMGR32.DLL
        0x00000000   0x767E0000       00016000   C:\WINNT\system32\Srvsvc.dll
        0x77801AFC   0x77800000       0001D000   C:\WINNT\system32\WINSPOOL.DRV
        0x00000000   0x76770000       0001A000   C:\WINNT\system32\wkssvc.dll
        0x76674054   0x76670000       0000E000   C:\WINNT\system32\CRYPTDLL.DLL
        0x768D1250   0x768D0000       00012000   C:\WINNT\system32\cryptsvc.dll
        0x768512D4   0x76850000       0001F000   C:\WINNT\system32\psbase.dll
        0x7CA0D2BA   0x7CA00000       00023000   C:\WINNT\system32\rsaenh.dll
        0x77444ACC   0x77440000       00075000   C:\WINNT\system32\CRYPT32.dll
        0x774333F0   0x77430000       00010000   C:\WINNT\system32\MSASN1.DLL
        0x00000000   0x76800000       00007000   C:\WINNT\system32\seclogon.dll
        0x767C4B9C   0x767C0000       00019000   C:\WINNT\system32\trkwks.dll
        0x00000000   0x768F0000       0000F000   C:\WINNT\system32\browser.dll
        0x00000000   0x76870000       0000B000   C:\WINNT\system32\msgsvc.dll
        0x74FF122C   0x74FF0000       00012000   C:\WINNT\system32\mswsock.dll
        0x785C11E9   0x785C0000       0000C000   C:\WINNT\System32\rnr20.dll
        0x777E10C5   0x777E0000       00008000   C:\WINNT\System32\winrnr.dll
        0x777F1380   0x777F0000       00005000   C:\WINNT\system32\rasadhlp.dll
        0x76753FD4   0x76750000       00015000   C:\WINNT\system32\wmicore.dll
        0x76952F60   0x76930000       0002B000   C:\WINNT\system32\WINTRUST.dll
        0x77921158   0x77920000       00023000   C:\WINNT\system32\IMAGEHLP.dll
        0x782F7238   0x782F0000       00242000   C:\WINNT\system32\SHELL32.DLL
---------------------------------------------------------------------------
C:\WINNT\System32\lsass.exe (Process ID: 224)

        Entry Point  Base     Size       Module
        0x01001258   0x01000000       0000A000   C:\WINNT\system32\lsass.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.dll
        0x00000000   0x78540000       0007D000   C:\WINNT\system32\LSASRV.dll
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.DLL
        0x76674054   0x76670000       0000E000   C:\WINNT\system32\CRYPTDLL.DLL
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.DLL
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x77BE56C2   0x77BE0000       0000F000   C:\WINNT\system32\SECUR32.DLL
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.DLL
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x00000000   0x77CC0000       0005E000   C:\WINNT\system32\SAMSRV.DLL
        0x77987CC5   0x77980000       00024000   C:\WINNT\system32\DNSAPI.DLL
        0x00000000   0x75050000       00008000   C:\WINNT\system32\WSOCK32.DLL
        0x750312D4   0x75030000       00013000   C:\WINNT\system32\WS2_32.DLL
        0x750211AE   0x75020000       00008000   C:\WINNT\system32\WS2HELP.DLL
        0x774333F0   0x77430000       00010000   C:\WINNT\system32\MSASN1.DLL
        0x75173309   0x75170000       0004F000   C:\WINNT\system32\NETAPI32.DLL
        0x00000000   0x751C0000       00006000   C:\WINNT\system32\NETRAP.DLL
        0x75153777   0x75150000       00010000   C:\WINNT\system32\SAMLIB.DLL
        0x779536C2   0x77950000       00029000   C:\WINNT\system32\WLDAP32.DLL
        0x00000000   0x765E0000       0000D000   C:\WINNT\system32\msprivs.dll
        0x78282F14   0x78280000       00033000   C:\WINNT\system32\kerberos.dll
        0x00000000   0x782D0000       0001E000   C:\WINNT\system32\msv1_0.dll
        0x7658DD61   0x76580000       0005C000   C:\WINNT\system32\netlogon.dll
```

```
        0x77BF39C5   0x77BF0000       00011000   C:\WINNT\system32\NTDSAPI.DLL
        0x78161581   0x78160000       00026000   C:\WINNT\system32\schannel.dll
        0x77444ACC   0x77440000       00075000   C:\WINNT\system32\CRYPT32.DLL
        0x77C1D43C   0x77C10000       0005D000   C:\WINNT\system32\USERENV.DLL
        0x7CA0C9BD   0x7CA00000       00022000   C:\WINNT\system32\rsabase.dll
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\ole32.dll

        0x750915EB   0x75090000       00010000   C:\WINNT\system32\mpr.dll
        0x77882AB8   0x77880000       0008D000   C:\WINNT\system32\setupapi.dll
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.dll
        0x764316BC   0x76430000       0001C000   C:\WINNT\system32\scecli.dll
        0x764E12B8   0x764E0000       0001E000   C:\WINNT\system32\polagent.dll
        0x76FB5E9A   0x76FB0000       000F2000   C:\WINNT\system32\MFC42U.DLL
        0x7650374C   0x76500000       00077000   C:\WINNT\system32\OAKLEY.DLL
        0x77342C35   0x77340000       00013000   C:\WINNT\system32\IPHLPAPI.DLL
        0x775218B2   0x77520000       00005000   C:\WINNT\system32\ICMP.DLL
        0x77321290   0x77320000       00017000   C:\WINNT\system32\MPRAPI.DLL
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.DLL
        0x773B123C   0x773B0000       0002E000   C:\WINNT\system32\ACTIVEDS.DLL
        0x773812A8   0x77380000       00022000   C:\WINNT\system32\ADSLDPC.DLL
        0x77831D22   0x77830000       0000E000   C:\WINNT\system32\RTUTILS.DLL
        0x774E24E0   0x774E0000       00032000   C:\WINNT\system32\RASAPI32.DLL
        0x774C2170   0x774C0000       00011000   C:\WINNT\system32\RASMAN.DLL
        0x77532E60   0x77530000       00022000   C:\WINNT\system32\TAPI32.DLL
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.DLL
        0x7736727A   0x77360000       00019000   C:\WINNT\system32\DHCPCSVC.DLL
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\system32\CLBCATQ.DLL
        0x74FD182C   0x74FD0000       0001F000   C:\WINNT\system32\msafd.dll
        0x750111A4   0x75010000       00007000   C:\WINNT\System32\wshtcpip.dll
        0x00FAD2BA   0x00FA0000       00023000   C:\WINNT\system32\rsaenh.dll
        0x67405829   0x67400000       00027000   C:\WINNT\system32\dssenh.dll
-----------------------------------------------------------------------
C:\WINNT\System32\svchost.exe (Process ID: 384)

        Entry Point  Base      Size       Module
        0x010010B8   0x01000000       00005000   C:\WINNT\system32\svchost.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.DLL
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.DLL
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\OLE32.DLL
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.DLL
        0x76196CA4   0x76190000       0003D000   c:\winnt\system32\rpcss.dll
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.DLL
        0x77C1D43C   0x77C10000       0005D000   c:\winnt\system32\USERENV.DLL
        0x750312D4   0x75030000       00013000   c:\winnt\system32\WS2_32.DLL
        0x750211AE   0x75020000       00008000   c:\winnt\system32\WS2HELP.DLL
        0x77BE56C2   0x77BE0000       0000F000   c:\winnt\system32\SECUR32.DLL
        0x74FF122C   0x74FF0000       00012000   C:\WINNT\system32\mswsock.dll
        0x77987CC5   0x77980000       00024000   C:\WINNT\system32\DNSAPI.DLL
        0x00000000   0x75050000       00008000   C:\WINNT\system32\WSOCK32.DLL
        0x74FD182C   0x74FD0000       0001F000   C:\WINNT\system32\msafd.dll
        0x750111A4   0x75010000       00007000   C:\WINNT\System32\wshtcpip.dll
        0x785C11E9   0x785C0000       0000C000   C:\WINNT\System32\rnr20.dll
        0x77342C35   0x77340000       00013000   C:\WINNT\system32\iphlpapi.dll
        0x775218B2   0x77520000       00005000   C:\WINNT\system32\ICMP.DLL
        0x77321290   0x77320000       00017000   C:\WINNT\system32\MPRAPI.DLL
        0x75153777   0x75150000       00010000   C:\WINNT\system32\SAMLIB.DLL
        0x75173309   0x75170000       0004F000   C:\WINNT\system32\NETAPI32.DLL
        0x00000000   0x751C0000       00006000   C:\WINNT\system32\NETRAP.DLL
        0x779536C2   0x77950000       00029000   C:\WINNT\system32\WLDAP32.DLL
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.DLL
        0x773B123C   0x773B0000       0002E000   C:\WINNT\system32\ACTIVEDS.DLL
        0x773812A8   0x77380000       00022000   C:\WINNT\system32\ADSLDPC.DLL
        0x77831D22   0x77830000       0000E000   C:\WINNT\system32\RTUTILS.DLL
        0x77882AB8   0x77880000       0008D000   C:\WINNT\system32\SETUPAPI.DLL
        0x774E24E0   0x774E0000       00032000   C:\WINNT\system32\RASAPI32.DLL
        0x774C2170   0x774C0000       00011000   C:\WINNT\system32\RASMAN.DLL
        0x77532E60   0x77530000       00022000   C:\WINNT\system32\TAPI32.DLL
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.DLL
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.DLL
        0x7736727A   0x77360000       00019000   C:\WINNT\system32\DHCPCSVC.DLL
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\system32\CLBCATQ.DLL
        0x777E10C5   0x777E0000       00008000   C:\WINNT\System32\winrnr.dll
        0x777F1380   0x777F0000       00005000   C:\WINNT\system32\rasadhlp.dll
        0x00000000   0x782D0000       0001E000   C:\WINNT\system32\b
```

```
---------------------------------------------------------------------------
C:\WINNT\System32\spoolsv.exe (Process ID: 412)

        Entry Point  Base      Size       Module
        0x01001124   0x01000000       0000D000   C:\WINNT\system32\spoolsv.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.DLL
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.dll
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.DLL
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.dll
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.DLL
        0x76A922BC   0x76A90000       00012000   C:\WINNT\system32\SPOOLSS.DLL
        0x750312D4   0x75030000       00013000   C:\WINNT\system32\WS2_32.DLL
        0x750211AE   0x75020000       00008000   C:\WINNT\system32\WS2HELP.DLL
        0x77987CC5   0x77980000       00024000   C:\WINNT\system32\DNSAPI.DLL
        0x00000000   0x75050000       00008000   C:\WINNT\system32\WSOCK32.DLL
        0x77342C35   0x77340000       00013000   C:\WINNT\system32\iphlpapi.dll
        0x775218B2   0x77520000       00005000   C:\WINNT\system32\ICMP.DLL
        0x77321290   0x77320000       00017000   C:\WINNT\system32\MPRAPI.DLL
        0x75153777   0x75150000       00010000   C:\WINNT\system32\SAMLIB.DLL
        0x75173309   0x75170000       0004F000   C:\WINNT\system32\NETAPI32.DLL
        0x77BE56C2   0x77BE0000       0000F000   C:\WINNT\system32\SECUR32.DLL
        0x00000000   0x751C0000       00006000   C:\WINNT\system32\NETRAP.DLL
        0x779536C2   0x77950000       00029000   C:\WINNT\system32\WLDAP32.DLL
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\OLE32.DLL
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.DLL
        0x773B123C   0x773B0000       0002E000   C:\WINNT\system32\ACTIVEDS.DLL
        0x773812A8   0x77380000       00022000   C:\WINNT\system32\ADSLDPC.DLL
        0x77831D22   0x77830000       0000E000   C:\WINNT\system32\RTUTILS.DLL
        0x77882AB8   0x77880000       0008D000   C:\WINNT\system32\SETUPAPI.DLL
        0x77C1D43C   0x77C10000       0005D000   C:\WINNT\system32\USERENV.DLL
        0x774E24E0   0x774E0000       00032000   C:\WINNT\system32\RASAPI32.DLL
        0x774C2170   0x774C0000       00011000   C:\WINNT\system32\RASMAN.DLL
        0x77532E60   0x77530000       00022000   C:\WINNT\system32\TAPI32.DLL
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.DLL
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.DLL
        0x7736727A   0x77360000       00019000   C:\WINNT\system32\DHCPCSVC.DLL
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\system32\CLBCATQ.DLL
        0x777F1380   0x777F0000       00005000   C:\WINNT\system32\rasadhlp.dll
        0x76AC5002   0x76AC0000       00040000   C:\WINNT\system32\localspl.dll
        0x77821114   0x77820000       00007000   C:\WINNT\system32\VERSION.DLL
        0x759B1A3F   0x759B0000       00006000   C:\WINNT\system32\LZ32.DLL
        0x7698671B   0x76980000       0001B000   C:\WINNT\system32\SFC.DLL
        0x68011080   0x68010000       000F0000   C:\WINNT\system32\sfcfiles.dll
        0x77801AFC   0x77800000       0001D000   C:\WINNT\system32\winspool.drv
        0x733E1480   0x733E0000       0000E000   C:\WINNT\system32\cnbjmon.dll
        0x76AB1162   0x76AB0000       00007000   C:\WINNT\system32\pjlmon.dll
        0x76A8119C   0x76A80000       0000D000   C:\WINNT\system32\tcpmon.dll
        0x76A710CC   0x76A70000       00006000   C:\WINNT\system32\usbmon.dll
        0x785C11E9   0x785C0000       0000C000   C:\WINNT\System32\rnr20.dll
        0x777E10C5   0x777E0000       00008000   C:\WINNT\System32\winrnr.dll
        0x76A512A4   0x76A50000       0001F000   C:\WINNT\system32\win32spl.dll
        0x76B017C2   0x76B00000       00013000   C:\WINNT\system32\inetpp.dll
---------------------------------------------------------------------------
C:\WINNT\System32\svchost.exe (Process ID: 444)

        Entry Point  Base      Size       Module
        0x010010B8   0x01000000       00005000   C:\WINNT\System32\svchost.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.DLL
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.DLL
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\OLE32.DLL
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.DLL
        0x76293B2C   0x76290000       0003A000   c:\winnt\system32\es.dll
        0x004944E0   0x00440000       00061000   c:\winnt\system32\TXFAUX.DLL
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.dll
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.DLL
        0x761D94DE   0x761D0000       00064000   c:\winnt\system32\ntmssvc.dll
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\System32\CLBCATQ.DLL
        0x7618401A   0x76180000       0000C000   c:\winnt\system32\sens.dll
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.dll
        0x750312D4   0x75030000       00013000   C:\WINNT\System32\WS2_32.dll
        0x750211AE   0x75020000       00008000   C:\WINNT\System32\WS2HELP.DLL
        0x77342C35   0x77340000       00013000   C:\WINNT\System32\iphlpapi.dll
```

```
        0x775218B2   0x77520000       00005000   C:\WINNT\System32\ICMP.DLL
        0x77321290   0x77320000       00017000   C:\WINNT\System32\MPRAPI.DLL
        0x75153777   0x75150000       00010000   C:\WINNT\System32\SAMLIB.DLL
        0x75173309   0x75170000       0004F000   C:\WINNT\System32\NETAPI32.DLL
        0x77BE56C2   0x77BE0000       0000F000   C:\WINNT\System32\SECUR32.DLL
        0x00000000   0x751C0000       00006000   C:\WINNT\System32\NETRAP.DLL
        0x779536C2   0x77950000       00029000   C:\WINNT\system32\WLDAP32.DLL
        0x77987CC5   0x77980000       00024000   C:\WINNT\System32\DNSAPI.DLL
        0x00000000   0x75050000       00008000   C:\WINNT\System32\WSOCK32.DLL
        0x773B123C   0x773B0000       0002E000   C:\WINNT\System32\ACTIVEDS.DLL
        0x773812A8   0x77380000       00022000   C:\WINNT\System32\ADSLDPC.DLL
        0x77831D22   0x77830000       0000E000   C:\WINNT\System32\RTUTILS.DLL
        0x77882AB8   0x77880000       0008D000   C:\WINNT\System32\SETUPAPI.DLL
        0x77C1D43C   0x77C10000       0005D000   C:\WINNT\System32\USERENV.DLL
        0x774E24E0   0x774E0000       00032000   C:\WINNT\System32\RASAPI32.DLL
        0x774C2170   0x774C0000       00011000   C:\WINNT\System32\RASMAN.DLL
        0x77532E60   0x77530000       00022000   C:\WINNT\System32\TAPI32.DLL
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.DLL
        0x7736727A   0x77360000       00019000   C:\WINNT\System32\DHCPCSVC.DLL
        0x5F3E2D3C   0x5F3E0000       00012000   C:\WINNT\System32\ATL.DLL
        0x7624117C   0x76240000       0002C000   C:\WINNT\System32\NTMSDBA.dll
        0x782F7238   0x782F0000       00242000   C:\WINNT\system32\Shell32.dll
        0x66E10ED0   0x66DF0000       0002C000   c:\winnt\system32\tapisrv.dll
        0x7571B878   0x75710000       00029000   c:\winnt\system32\rasmans.dll
        0x77444ACC   0x77440000       00075000   C:\WINNT\system32\CRYPT32.dll
        0x774333F0   0x77430000       00010000   C:\WINNT\system32\MSASN1.DLL
        0x6A4E5370   0x6A4B0000       00089000   c:\winnt\system32\netcfgx.dll
        0x7588FF96   0x75870000       00083000   c:\winnt\system32\RASDLG.dll
        0x76271228   0x76270000       00019000   c:\winnt\system32\netman.dll
        0x76F24A0A   0x76F20000       00075000   C:\WINNT\system32\NETSHELL.dll
        0x00000000   0x76110000       00004000   C:\WINNT\System32\WMI.dll
        0x75674F29   0x75670000       00010000   C:\WINNT\System32\rastapi.dll
        0x644F2CE0   0x644D0000       00034000   C:\WINNT\System32\unimdm.tsp
        0x756012C0   0x75600000       00007000   C:\WINNT\System32\uniplat.dll
        0x00000000   0x770B0000       00007000   C:\WINNT\System32\CFGMGR32.dll
        0x69C04BA0   0x69BF0000       0001D000   C:\WINNT\System32\NTMARTA.DLL
        0x77801AFC   0x77800000       0001D000   C:\WINNT\System32\WINSPOOL.DRV
        0x77BF39C5   0x77BF0000       00011000   C:\WINNT\System32\NTDSAPI.dll
        0x645411F0   0x64540000       00008000   C:\WINNT\System32\kmddsp.tsp
        0x64531460   0x64530000       0000C000   C:\WINNT\System32\ndptsp.tsp
        0x64552060   0x64550000       00006000   C:\WINNT\System32\ipconf.tsp
        0x64567220   0x64560000       00044000   C:\WINNT\System32\h323.tsp
        0x75910822   0x75900000       00033000   C:\WINNT\System32\rasppp.dll
        0x756E1738   0x756E0000       00005000   C:\WINNT\System32\ntlsapi.dll
        0x00000000   0x68C30000       0000C000   C:\WINNT\System32\raschap.dll
        0x68B18750   0x68B10000       0000F000   C:\WINNT\System32\rastls.dll
        0x78161581   0x78160000       00026000   C:\WINNT\System32\SCHANNEL.dll
        0x769611DD   0x76960000       00017000   C:\WINNT\System32\WinSCard.dll
        0x695C9140   0x694F0000       00162000   C:\WINNT\System32\COMSVCS.DLL
        0x69A40040   0x699E0000       000AF000   C:\WINNT\System32\MSDTCPRX.dll
        0x6A7AAB00   0x6A7A0000       00010000   C:\WINNT\System32\MTXCLU.DLL
        0x77821114   0x77820000       00007000   C:\WINNT\system32\VERSION.dll
        0x759B1A3F   0x759B0000       00006000   C:\WINNT\system32\LZ32.DLL
        0x00000000   0x73930000       00010000   C:\WINNT\System32\CLUSAPI.DLL
        0x689D2420   0x689D0000       0000D000   C:\WINNT\System32\RESUTILS.DLL
----------------------------------------------------------------------
C:\WINNT\System32\regsvc.exe (Process ID: 480)

        Entry Point  Base      Size       Module
        0x01002E80   0x01000000       00014000   C:\WINNT\system32\regsvc.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.dll
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.DLL
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x77BE56C2   0x77BE0000       0000F000   C:\WINNT\system32\secur32.dll
----------------------------------------------------------------------
C:\WINNT\System32\MSTask.exe (Process ID: 496)

        Entry Point  Base      Size       Module
        0x01002F10   0x01000000       0001E000   C:\WINNT\system32\MSTask.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.dll
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.dll
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.dll
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.dll
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.DLL
```

```
        0x75173309   0x75170000       0004F000   C:\WINNT\system32\NETAPI32.dll
        0x77BE56C2   0x77BE0000       0000F000   C:\WINNT\system32\SECUR32.DLL
        0x00000000   0x751C0000       00006000   C:\WINNT\system32\NETRAP.DLL
        0x75153777   0x75150000       00010000   C:\WINNT\system32\SAMLIB.DLL
        0x750312D4   0x75030000       00013000   C:\WINNT\system32\WS2_32.DLL
        0x750211AE   0x75020000       00008000   C:\WINNT\system32\WS2HELP.DLL
        0x779536C2   0x77950000       00029000   C:\WINNT\system32\WLDAP32.DLL
        0x77987CC5   0x77980000       00024000   C:\WINNT\system32\DNSAPI.DLL
        0x00000000   0x75050000       00008000   C:\WINNT\system32\WSOCK32.DLL
        0x77BF39C5   0x77BF0000       00011000   C:\WINNT\system32\NTDSAPI.dll
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.dll
        0x782F7238   0x782F0000       00242000   C:\WINNT\system32\SHELL32.dll
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.DLL
        0x77C1D43C   0x77C10000       0005D000   C:\WINNT\system32\USERENV.dll
        0x74FF122C   0x74FF0000       00012000   C:\WINNT\system32\mswsock.dll
        0x74FD182C   0x74FD0000       0001F000   C:\WINNT\system32\msafd.dll
        0x750111A4   0x75010000       00007000   C:\WINNT\System32\wshtcpip.dll
        0x785C11E9   0x785C0000       0000C000   C:\WINNT\System32\rnr20.dll
        0x77342C35   0x77340000       00013000   C:\WINNT\system32\iphlpapi.dll
        0x775218B2   0x77520000       00005000   C:\WINNT\system32\ICMP.DLL
        0x77321290   0x77320000       00017000   C:\WINNT\system32\MPRAPI.DLL
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\OLE32.DLL
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.DLL
        0x773B123C   0x773B0000       0002E000   C:\WINNT\system32\ACTIVEDS.DLL
        0x773812A8   0x77380000       00022000   C:\WINNT\system32\ADSLDPC.DLL
        0x77831D22   0x77830000       0000E000   C:\WINNT\system32\RTUTILS.DLL
        0x77882AB8   0x77880000       0008D000   C:\WINNT\system32\SETUPAPI.DLL
        0x774E24E0   0x774E0000       00032000   C:\WINNT\system32\RASAPI32.DLL
        0x774C2170   0x774C0000       00011000   C:\WINNT\system32\RASMAN.DLL
        0x77532E60   0x77530000       00022000   C:\WINNT\system32\TAPI32.DLL
        0x7736727A   0x77360000       00019000   C:\WINNT\system32\DHCPCSVC.DLL
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\system32\CLBCATQ.DLL
        0x777E10C5   0x777E0000       00008000   C:\WINNT\System32\winrnr.dll
        0x777F1380   0x777F0000       00005000   C:\WINNT\system32\rasadhlp.dll
        0x76A4127B   0x76A40000       00006000   C:\WINNT\system32\MSIDLE.DLL
----------------------------------------------------------------------
C:\WINNT\System32\stisvc.exe (Process ID: 524)

        Entry Point  Base      Size       Module

        0x010086D0   0x01000000       00011000   C:\WINNT\system32\stisvc.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.dll
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.dll
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.dll
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.dll
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x77882AB8   0x77880000       0008D000   C:\WINNT\system32\SETUPAPI.dll
        0x77C1D43C   0x77C10000       0005D000   C:\WINNT\system32\USERENV.DLL
        0x67335351   0x67330000       0000D000   C:\WINNT\system32\STI.dll
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.dll
----------------------------------------------------------------------
C:\WINNT\System32\Wbem\WinMgmt.exe (Process ID: 572)

        Entry Point  Base      Size       Module
        0x0041EF26   0x00400000       00030000   C:\WINNT\System32\WBEM\WinMgmt.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x65C8862C   0x65C20000       000AD000   C:\WINNT\System32\WBEM\wbemcomn.dll
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.dll
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.DLL
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.dll
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.dll
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.dll
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\ole32.dll
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\system32\CLBCATQ.DLL
----------------------------------------------------------------------
C:\WINNT\System32\mspmspsv.exe (Process ID: 592)

        Entry Point  Base      Size       Module
        0x01007C20   0x01000000       0000D000   C:\WINNT\System32\mspmspsv.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.dll
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.DLL
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
```

```
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.dll
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.dll
        0x69C04BA0   0x69BF0000       0001D000   C:\WINNT\System32\NTMARTA.DLL
        0x77801AFC   0x77800000       0001D000   C:\WINNT\System32\WINSPOOL.DRV
        0x779536C2   0x77950000       00029000   C:\WINNT\system32\WLDAP32.dll
        0x77BF39C5   0x77BF0000       00011000   C:\WINNT\System32\NTDSAPI.dll
        0x77987CC5   0x77980000       00024000   C:\WINNT\System32\DNSAPI.DLL
        0x00000000   0x75050000       00008000   C:\WINNT\System32\WSOCK32.DLL
        0x750312D4   0x75030000       00013000   C:\WINNT\System32\WS2_32.DLL
        0x750211AE   0x75020000       00008000   C:\WINNT\System32\WS2HELP.DLL
        0x75173309   0x75170000       0004F000   C:\WINNT\System32\NETAPI32.DLL

        0x77BE56C2   0x77BE0000       0000F000   C:\WINNT\System32\SECUR32.DLL
        0x00000000   0x751C0000       00006000   C:\WINNT\System32\NETRAP.DLL
        0x75153777   0x75150000       00010000   C:\WINNT\System32\SAMLIB.DLL
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\ole32.dll
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.dll
-----------------------------------------------------------------------
C:\WINNT\Explorer.EXE (Process ID: 792)

        Entry Point  Base      Size       Module
        0x004015A8   0x00400000       0003E000   C:\WINNT\Explorer.EXE
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.DLL
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.DLL
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.DLL
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.DLL
        0x78001000   0x78000000       00046000   C:\WINNT\system32\msvcrt.dll
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.DLL
        0x732E520F   0x732E0000       00020000   C:\WINNT\System32\shim.dll
        0x77821114   0x77820000       00007000   C:\WINNT\system32\version.dll
        0x759B1A3F   0x759B0000       00006000   C:\WINNT\system32\LZ32.DLL
        0x4000421C   0x40000000       00009000   C:\WINNT\AppPatch\_W2KPLYR.DLL
        0x782F7238   0x782F0000       00242000   C:\WINNT\system32\SHELL32.dll
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\OLE32.DLL
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\System32\CLBCATQ.DLL
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.dll
        0x7784288A   0x77840000       0003C000   C:\WINNT\System32\cscui.dll
        0x770C6B43   0x770C0000       00023000   C:\WINNT\System32\CSCDLL.DLL
        0x71019B2E   0x71000000       00148000   C:\WINNT\System32\SHDOCVW.DLL
        0x7118485C   0x71160000       000FD000   C:\WINNT\System32\browseui.dll
        0x750915EB   0x75090000       00010000   C:\WINNT\system32\MPR.DLL
        0x77C1D43C   0x77C10000       0005D000   C:\WINNT\System32\USERENV.DLL
        0x702BF821   0x702B0000       00078000   C:\WINNT\system32\URLMON.DLL
        0x704433D3   0x70440000       0008F000   C:\WINNT\System32\mlang.dll
        0x70D7ED52   0x70C50000       002A3000   C:\WINNT\System32\mshtml.dll
        0x702018CB   0x70200000       00094000   C:\WINNT\system32\WININET.DLL
        0x77444ACC   0x77440000       00075000   C:\WINNT\system32\CRYPT32.dll
        0x774333F0   0x77430000       00010000   C:\WINNT\system32\MSASN1.DLL
        0x774E24E0   0x774E0000       00032000   C:\WINNT\System32\RASAPI32.DLL
        0x774C2170   0x774C0000       00011000   C:\WINNT\System32\RASMAN.DLL
        0x750312D4   0x75030000       00013000   C:\WINNT\System32\WS2_32.DLL
        0x750211AE   0x75020000       00008000   C:\WINNT\System32\WS2HELP.DLL
        0x77532E60   0x77530000       00022000   C:\WINNT\System32\TAPI32.DLL
        0x77831D22   0x77830000       0000E000   C:\WINNT\System32\RTUTILS.DLL
        0x75AB1641   0x75AB0000       00005000   C:\WINNT\System32\sensapi.dll
        0x76FA1936   0x76FA0000       0000F000   C:\WINNT\System32\ntshrui.dll
        0x5F3E2D3C   0x5F3E0000       00012000   C:\WINNT\System32\ATL.DLL
        0x75173309   0x75170000       0004F000   C:\WINNT\System32\NETAPI32.DLL
        0x77BE56C2   0x77BE0000       0000F000   C:\WINNT\System32\SECUR32.DLL
        0x00000000   0x751C0000       00006000   C:\WINNT\System32\NETRAP.DLL
        0x75153777   0x75150000       00010000   C:\WINNT\System32\SAMLIB.DLL
        0x779536C2   0x77950000       00029000   C:\WINNT\system32\WLDAP32.DLL
        0x77987CC5   0x77980000       00024000   C:\WINNT\System32\DNSAPI.DLL
        0x00000000   0x75050000       00008000   C:\WINNT\System32\WSOCK32.DLL
        0x00000000   0x71930000       00088000   C:\WINNT\System32\shdoclc.dll
        0x00000000   0x75AC0000       00028000   C:\WINNT\System32\MSLS31.DLL
        0x75E61264   0x75E60000       0001A000   C:\WINNT\System32\IMM32.DLL
        0x75161358   0x75160000       0000C000   C:\WINNT\System32\ntlanman.dll
        0x75211323   0x75210000       00015000   C:\WINNT\System32\NETUI0.DLL
        0x751D15F4   0x751D0000       00038000   C:\WINNT\System32\NETUI1.DLL
        0x76F24A0A   0x76F20000       00075000   C:\WINNT\system32\NETSHELL.dll
        0x7034219D   0x70340000       00041000   C:\WINNT\System32\webcheck.dll
        0x766D2716   0x766D0000       00018000   C:\WINNT\System32\stobject.dll
```

```
        0x767410E1   0x76740000       00008000   C:\WINNT\System32\BATMETER.DLL
        0x77882AB8   0x77880000       0008D000   C:\WINNT\System32\SETUPAPI.DLL
        0x766F108C   0x766F0000       00007000   C:\WINNT\System32\POWRPROF.DLL
        0x77574164   0x77570000       00030000   C:\WINNT\System32\WINMM.DLL
        0x7722888D   0x770F0000       001FD000   C:\WINNT\System32\MSI.DLL
        0x77563789   0x77560000       00009000   C:\WINNT\System32\wdmaud.drv
        0x77402638   0x77400000       00008000   C:\WINNT\System32\msacm32.drv
        0x7741DA10   0x77410000       00013000   C:\WINNT\System32\MSACM32.dll
        0x00000000   0x719D0000       00012000   C:\WINNT\System32\browselc.dll
        0x70511C9A   0x70510000       0000A000   C:\WINNT\System32\imgutil.dll
        0x6665DE8C   0x66650000       00054000   C:\WINNT\System32\USP10.DLL
        0x74FD182C   0x74FD0000       0001F000   C:\WINNT\system32\msafd.dll
        0x750111A4   0x75010000       00007000   C:\WINNT\System32\wshtcpip.dll
        0x785C11E9   0x785C0000       0000C000   C:\WINNT\System32\rnr20.dll
        0x77342C35   0x77340000       00013000   C:\WINNT\System32\iphlpapi.dll
        0x775218B2   0x77520000       00005000   C:\WINNT\System32\ICMP.DLL
        0x77321290   0x77320000       00017000   C:\WINNT\System32\MPRAPI.DLL
        0x773B123C   0x773B0000       0002E000   C:\WINNT\System32\ACTIVEDS.DLL
        0x773812A8   0x77380000       00022000   C:\WINNT\System32\ADSLDPC.DLL
        0x7736727A   0x77360000       00019000   C:\WINNT\System32\DHCPCSVC.DLL
        0x777E10C5   0x777E0000       00008000   C:\WINNT\System32\winrnr.dll
        0x777F1380   0x777F0000       00005000   C:\WINNT\System32\rasadhlp.dll
        0x00000000   0x770B0000       00007000   C:\WINNT\System32\CfgMgr32.dll
        0x044EE8F0   0x044E0000       00029000   C:\WINNT\System32\dsquery.dll
        0x76B31DE5   0x76B30000       0003E000   C:\WINNT\system32\comdlg32.dll
        0x0451A080   0x04510000       0001E000   C:\WINNT\System32\dsuiext.dll
        0x77BF39C5   0x77BF0000       00011000   C:\WINNT\System32\NTDSAPI.dll
        0x77801AFC   0x77800000       0001D000   C:\WINNT\System32\WINSPOOL.DRV
        0x6B72BF3C   0x6B700000       00090000   C:\WINNT\System32\jscript.dll
        0x69B29278   0x69B10000       00114000   C:\WINNT\System32\msxml3.dll
        0x6AC3C530   0x6AC20000       00037000   C:\WINNT\System32\mstask.dll
        0x68D48B40   0x68C60000       00160000   C:\WINNT\System32\query.dll
        0x76711840   0x76710000       00009000   C:\WINNT\System32\LINKINFO.DLL
        0x16201120   0x16200000       00006000   C:\PROGRA~1\WinZip\WZSHLSTB.DLL
        0x379CC0A3   0x379B0000       0008C000
C:\PROGRA~1\COMMON~1\MICROS~1\WEBFOL~1\MSONSEXT.DLL
        0x05BC1000   0x05BC0000       00024000   C:\Program Files\WinRAR\rarext.dll
        0x76952F60   0x76930000       0002B000   C:\WINNT\system32\WINTRUST.dll
        0x77921158   0x77920000       00023000   C:\WINNT\system32\IMAGEHLP.dll
        0x71F017E7   0x71F00000       0004D000   C:\WINNT\System32\docprop2.dll
        0x6A8F442A   0x6A8F0000       00020000   C:\WINNT\System32\MSVFW32.DLL
        0x74874EB2   0x74870000       00016000   C:\WINNT\System32\AVIFIL32.DLL
        0x700214F0   0x70020000       00005000   C:\WINNT\system32\faxshell.dll
        0x72211F49   0x72210000       00007000   C:\WINNT\System32\diskcopy.dll
        0x71C940C0   0x71C80000       00026000   C:\WINNT\System32\dskquoui.dll
        0x10001000   0x10000000       00008000   C:\Program Files\Adobe\Acrobat
5.0\Reader\ActiveX\AcroIEHelper.ocx
        0x658F2374   0x658F0000       00114000   C:\WINNT\System32\webvw.dll
        0x76DF1A8C   0x76DF0000       00011000   C:\WINNT\System32\mydocs.dll
        0x70F89613   0x70F30000       0006E000   C:\WINNT\System32\mshtmled.dll
----------------------------------------------------------------------------
popupkiller.EXE (Process ID: 852)

        Entry Point  Base      Size       Module
        0x00455000   0x00400000       0005A000   C:\Program Files\PopUp
Killer\popupkiller.EXE
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.DLL
        0x73421AD8   0x73420000       00153000   C:\WINNT\System32\MSVBVM60.DLL
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.dll
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.dll
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\ole32.dll
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.dll
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\System32\CLBCATQ.DLL
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.dll
        0x110011E4   0x11000000       00006000   C:\WINNT\System32\Line3D.ocx
        0x01701A64   0x01700000       0000E000   C:\WINNT\System32\hRef.ocx
        0x749AFF40   0x749A0000       00024000   C:\WINNT\System32\asycfilt.dll
        0x27588820   0x27580000       00105000   C:\WINNT\System32\mscomctl.ocx
        0x76B31DE5   0x76B30000       0003E000   C:\WINNT\system32\comdlg32.dll
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.DLL
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.DLL
        0x782F7238   0x782F0000       00242000   C:\WINNT\system32\SHELL32.DLL
        0x217A14B0   0x217A0000       00023000   C:\WINNT\System32\COMDLG32.OCX
        0x02101344   0x02100000       00009000   C:\WINNT\System32\xFXSysTray.ocx
```

```
        0x234C12FC   0x234C0000       0001E000   C:\WINNT\System32\MSINET.OCX
        0x702018CB   0x70200000       00094000   C:\WINNT\system32\WININET.dll
        0x77444ACC   0x77440000       00075000   C:\WINNT\system32\CRYPT32.dll
        0x774333F0   0x77430000       00010000   C:\WINNT\system32\MSASN1.DLL
        0x02196000   0x02190000       0000B000   C:\Program Files\PopUp Killer\fgeo.dll
        0x77801AFC   0x77800000       0001D000   C:\WINNT\System32\WINSPOOL.DRV
        0x760211C8   0x76020000       00033000
C:\WINNT\System32\spool\DRIVERS\W32X86\3\UNIDRVUI.DLL
        0x76EF119C   0x76EF0000       0002B000
C:\WINNT\System32\spool\DRIVERS\W32X86\3\UNIDRV.DLL
        0x6B7724A0   0x6B770000       00013000   C:\WINNT\System32\mscms.dll
-----------------------------------------------------------------------
qttask.exe (Process ID: 864)

        Entry Point  Base      Size       Module
        0x0040578E   0x00400000       00014000   C:\Program Files\QuickTime\qttask.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.dll
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.dll
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.dll
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x782F7238   0x782F0000       00242000   C:\WINNT\system32\SHELL32.dll
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.DLL
        0x78001000   0x78000000       00046000   C:\WINNT\system32\msvcrt.dll
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.DLL
        0x66AB1009   0x66800000       0041C000   C:\WINNT\System32\QuickTime.qts
        0x77574164   0x77570000       00030000   C:\WINNT\System32\WINMM.dll
        0x76B31DE5   0x76B30000       0003E000   C:\WINNT\system32\comdlg32.dll
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\ole32.dll
        0x77821114   0x77820000       00007000   C:\WINNT\system32\VERSION.dll
        0x759B1A3F   0x759B0000       00006000   C:\WINNT\system32\LZ32.DLL
        0x702018CB   0x70200000       00094000   C:\WINNT\system32\WININET.DLL
        0x77444ACC   0x77440000       00075000   C:\WINNT\system32\CRYPT32.dll
        0x774333F0   0x77430000       00010000   C:\WINNT\system32\MSASN1.DLL
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.dll
        0x51038811   0x51000000       0004A000   C:\WINNT\System32\ddraw.dll
        0x728A112C   0x728A0000       00006000   C:\WINNT\System32\DCIMAN32.dll
        0x673110D9   0x672D0000       00079000
C:\WINNT\system32\QuickTime\QuickTimeEssentials.qtx
        0x66E77919   0x66DF0000       000CD000
C:\WINNT\system32\QuickTime\QuickTimeInternetExtras.qtx
        0x672ABA69   0x67260000       00068000
C:\WINNT\system32\QuickTime\QuickTimeMPEG.qtx
        0x6738B329   0x67350000       00064000
C:\WINNT\system32\QuickTime\QuickTimeMPEG4.qtx
        0x66CA3260   0x66C20000       000B7000
C:\WINNT\system32\QuickTime\QuickTimeStreaming.qtx
        0x00000000   0x75050000       00008000   C:\WINNT\System32\WSOCK32.dll
        0x750312D4   0x75030000       00013000   C:\WINNT\System32\WS2_32.DLL
        0x750211AE   0x75020000       00008000   C:\WINNT\System32\WS2HELP.DLL
        0x6764A480   0x67640000       0001C000
C:\WINNT\system32\QuickTime\QuickTimeStreamingExtras.qtx
-----------------------------------------------------------------------
SETI@home.exe (Process ID: 880)

        Entry Point  Base      Size       Module
        0x00423C0D   0x00400000       0007F000   C:\Program
Files\SETI@home\SETI@home.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.dll
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.dll
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.dll
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x782F7238   0x782F0000       00242000   C:\WINNT\system32\SHELL32.dll
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.DLL
        0x78001000   0x78000000       00046000   C:\WINNT\system32\msvcrt.dll
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.DLL
        0x00000000   0x75050000       00008000   C:\WINNT\System32\WSOCK32.dll
        0x750312D4   0x75030000       00013000   C:\WINNT\System32\WS2_32.DLL
        0x750211AE   0x75020000       00008000   C:\WINNT\System32\WS2HELP.DLL
        0x702018CB   0x70200000       00094000   C:\WINNT\system32\wininet.dll
        0x77444ACC   0x77440000       00075000   C:\WINNT\system32\CRYPT32.dll
        0x774333F0   0x77430000       00010000   C:\WINNT\system32\MSASN1.DLL
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.dll
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\ole32.dll
```

```
        0x774E24E0   0x774E0000       00032000   C:\WINNT\System32\RASAPI32.DLL
        0x774C2170   0x774C0000       00011000   C:\WINNT\System32\RASMAN.DLL
        0x77532E60   0x77530000       00022000   C:\WINNT\System32\TAPI32.DLL
        0x77831D22   0x77830000       0000E000   C:\WINNT\System32\RTUTILS.DLL
        0x75AB1641   0x75AB0000       00005000   C:\WINNT\System32\sensapi.dll
        0x77C1D43C   0x77C10000       0005D000   C:\WINNT\System32\USERENV.DLL
        0x75173309   0x75170000       0004F000   C:\WINNT\System32\netapi32.dll
        0x77BE56C2   0x77BE0000       0000F000   C:\WINNT\System32\SECUR32.DLL
        0x00000000   0x751C0000       00006000   C:\WINNT\System32\NETRAP.DLL
        0x75153777   0x75150000       00010000   C:\WINNT\System32\SAMLIB.DLL
        0x779536C2   0x77950000       00029000   C:\WINNT\system32\WLDAP32.DLL
        0x77987CC5   0x77980000       00024000   C:\WINNT\System32\DNSAPI.DLL
        0x74FD182C   0x74FD0000       0001F000   C:\WINNT\system32\msafd.dll
        0x750111A4   0x75010000       00007000   C:\WINNT\System32\wshtcpip.dll
        0x785C11E9   0x785C0000       0000C000   C:\WINNT\System32\rnr20.dll
        0x77342C35   0x77340000       00013000   C:\WINNT\System32\iphlpapi.dll
        0x775218B2   0x77520000       00005000   C:\WINNT\System32\ICMP.DLL
        0x77321290   0x77320000       00017000   C:\WINNT\System32\MPRAPI.DLL
        0x773B123C   0x773B0000       0002E000   C:\WINNT\System32\ACTIVEDS.DLL
        0x773812A8   0x77380000       00022000   C:\WINNT\System32\ADSLDPC.DLL
        0x77882AB8   0x77880000       0008D000   C:\WINNT\System32\SETUPAPI.DLL
        0x7736727A   0x77360000       00019000   C:\WINNT\System32\DHCPCSVC.DLL
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\System32\CLBCATQ.DLL
        0x777E10C5   0x777E0000       00008000   C:\WINNT\System32\winrnr.dll
        0x777F1380   0x777F0000       00005000   C:\WINNT\System32\rasadhlp.dll
-----------------------------------------------------------------------
E:\win32\fire.exe (Process ID: 936)

        Entry Point  Base      Size       Module
        0x00401454   0x00400000       0003B000   E:\win32\fire.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x73421AD8   0x73420000       00153000   C:\WINNT\System32\MSVBVM60.DLL
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.dll
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.dll
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.dll
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\ole32.dll
        0x77A23A50   0x779B0000       0009B000   C:\WINNT\system32\OLEAUT32.dll
        0x7760EAE0   0x775A0000       00085000   C:\WINNT\System32\CLBCATQ.DLL
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.dll
        0x71019B2E   0x71000000       00148000   C:\WINNT\System32\shdocvw.dll
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.dll
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\comctl32.dll
        0x782F7238   0x782F0000       00242000   C:\WINNT\system32\SHELL32.dll
        0x702018CB   0x70200000       00094000   C:\WINNT\system32\WININET.dll
        0x77444ACC   0x77440000       00075000   C:\WINNT\system32\CRYPT32.dll
        0x774333F0   0x77430000       00010000   C:\WINNT\system32\MSASN1.DLL
        0x749AFF40   0x749A0000       00024000   C:\WINNT\System32\asycfilt.dll
        0x00000000   0x71930000       00088000   C:\WINNT\System32\shdoclc.dll
        0x702BF821   0x702B0000       00078000   C:\WINNT\system32\urlmon.dll
        0x77821114   0x77820000       00007000   C:\WINNT\system32\VERSION.dll
        0x759B1A3F   0x759B0000       00006000   C:\WINNT\system32\LZ32.DLL
        0x70416E7B   0x70400000       00023000   C:\WINNT\System32\MSRATING.dll
        0x00000000   0x75050000       00008000   C:\WINNT\System32\WSOCK32.dll
        0x750312D4   0x75030000       00013000   C:\WINNT\System32\WS2_32.DLL

        0x750211AE   0x75020000       00008000   C:\WINNT\System32\WS2HELP.DLL
        0x00000000   0x30000000       00011000   C:\WINNT\System32\msratelc.dll
        0x704433D3   0x70440000       0008F000   C:\WINNT\System32\mlang.dll
        0x74FD182C   0x74FD0000       0001F000   C:\WINNT\system32\msafd.dll
        0x70D7ED52   0x70C50000       002A3000   C:\WINNT\System32\mshtml.dll
        0x750111A4   0x75010000       00007000   C:\WINNT\System32\wshtcpip.dll
-----------------------------------------------------------------------
E:\win32\cmd.exe (Process ID: 1172)


        Entry Point  Base      Size       Module
        0x4AD1A420   0x4AD00000       00048000   E:\win32\cmd.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.dll
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.dll
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.dll
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.dll
-----------------------------------------------------------------------
```

```
E:\win32\procinterrogate.exe (Process ID: 1156)

        Entry Point  Base      Size       Module
        0x004031C4   0x00400000       0000E000   E:\win32\procinterrogate.exe
        0x00000000   0x77F80000       0007B000   C:\WINNT\System32\ntdll.dll
        0x77E874CA   0x77E80000       000B5000   C:\WINNT\system32\KERNEL32.dll
        0x77E2FE7E   0x77E10000       00064000   C:\WINNT\system32\USER32.dll
        0x00000000   0x77F40000       0003C000   C:\WINNT\system32\GDI32.DLL
        0x77DB7CDA   0x77DB0000       0005B000   C:\WINNT\system32\ADVAPI32.dll
        0x77D43905   0x77D40000       00070000   C:\WINNT\system32\RPCRT4.DLL
        0x690A10BC   0x690A0000       0000B000   C:\WINNT\System32\PSAPI.DLL
        0x77821114   0x77820000       00007000   C:\WINNT\system32\VERSION.dll
        0x759B1A3F   0x759B0000       00006000   C:\WINNT\system32\LZ32.DLL
        0x7CA0C9BD   0x7CA00000       00022000   C:\WINNT\System32\rsabase.dll
        0x77A52804   0x77A50000       000F6000   C:\WINNT\system32\ole32.dll
        0x77C1D43C   0x77C10000       0005D000   C:\WINNT\System32\USERENV.dll
        0x78001000   0x78000000       00046000   C:\WINNT\system32\MSVCRT.DLL
        0x77444ACC   0x77440000       00075000   C:\WINNT\system32\CRYPT32.dll
        0x774333F0   0x77430000       00010000   C:\WINNT\system32\MSASN1.DLL
        0x782F7238   0x782F0000       00242000   C:\WINNT\system32\shell32.dll
        0x70BEE493   0x70BD0000       00064000   C:\WINNT\system32\SHLWAPI.DLL
        0x717889EC   0x71780000       0008A000   C:\WINNT\system32\COMCTL32.DLL
        0x75173309   0x75170000       0004F000   C:\WINNT\System32\netapi32.dll
        0x77BE56C2   0x77BE0000       0000F000   C:\WINNT\System32\SECUR32.DLL
        0x00000000   0x751C0000       00006000   C:\WINNT\System32\NETRAP.DLL
        0x75153777   0x75150000       00010000   C:\WINNT\System32\SAMLIB.DLL
        0x750312D4   0x75030000       00013000   C:\WINNT\System32\WS2_32.DLL
        0x750211AE   0x75020000       00008000   C:\WINNT\System32\WS2HELP.DLL
        0x779536C2   0x77950000       00029000   C:\WINNT\system32\WLDAP32.DLL
        0x77987CC5   0x77980000       00024000   C:\WINNT\System32\DNSAPI.DLL
        0x00000000   0x75050000       00008000   C:\WINNT\System32\WSOCK32.DLL


-------------------------------------------------
FPORT (fport /p)
-------------------------------------------------
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com


Pid   Process            Port  Proto Path
384   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  445   TCP
496   MSTask         ->  1025  TCP   C:\WINNT\system32\MSTask.exe
8     System         ->  1028  TCP

384   svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System         ->  445   UDP
212   services       ->  1027  UDP   C:\WINNT\system32\services.exe
792   Explorer       ->  1088  UDP   C:\WINNT\Explorer.EXE
936   fire           ->  1142  UDP   E:\win32\fire.exe



-------------------------------------------------
PSLIST (pslist -x)
-------------------------------------------------

PsList v1.2 - Process Information Lister
Copyright (C) 1999-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Process and thread information for HP1:

Name          Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
Idle            0   0   1    0     16   0:00:00.000   0:25:41.025   25:14:34.360
                      VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                       0      16      16       0        1    0    0        0
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
   0   0    195625          Running   0:00:00.000   0:25:41.025    0:00:00.000

Name          Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
System          8   8  33  100    212   0:00:00.000   0:00:12.908   25:14:34.360
                      VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                    1668     212     644      24     2225    0    0       24
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
```

```
   4   0      4299            Ready   0:00:00.000   0:00:06.409    0:00:00.000
  12  14       157       Wait:Queue   0:00:00.000   0:00:00.000   25:14:53.097
  16  13     73539       Wait:Queue   0:00:00.000   0:00:00.210   25:14:53.097
  20  14    603259       Wait:Queue   0:00:00.000   0:00:00.811   25:14:53.097
  24  13    535444       Wait:Queue   0:00:00.000   0:00:00.660   25:14:53.097
  28  13    656660       Wait:Queue   0:00:00.000   0:00:00.841   25:14:53.097
  32  12    187590       Wait:Queue   0:00:00.000   0:00:00.460   25:14:53.097
  36  12        58       Wait:Queue   0:00:00.000   0:00:00.020   25:14:53.097
  40  12      4842       Wait:Queue   0:00:00.000   0:00:00.170   25:14:53.097
  44  15      3162       Wait:Queue   0:00:00.000   0:00:00.000   25:14:53.097
  48  14     90874   Wait:Executive   0:00:00.000   0:00:00.000   25:14:53.097
  52  18      3199  Wait:VirtualMem   0:00:00.000   0:00:00.160   25:14:53.077
  56  17     47634    Wait:FreePage   0:00:00.000   0:00:00.150   25:14:53.077
  60  16   1038544   Wait:Executive   0:00:00.000   0:00:00.000   25:14:53.077
  64  23   1031758   Wait:Executive   0:00:00.000   0:00:00.070   25:14:53.077
  68  16         1       Wait:Queue   0:00:00.000   0:00:00.000   25:14:52.957
  72  17         1       Wait:Queue   0:00:00.000   0:00:00.000   25:14:52.957
  76   8       343   Wait:Executive   0:00:00.000   0:00:00.000   25:14:52.777
  80  17       151  Wait:VirtualMem   0:00:00.000   0:00:00.000   25:14:52.767
  84   8         1   Wait:Executive   0:00:00.000   0:00:00.000   25:14:52.436
  88   8        15       Wait:Queue   0:00:00.000   0:00:00.000   25:14:42.562
  92   9        44   Wait:Executive   0:00:00.000   0:00:00.000   25:14:40.669
  96   8         3   Wait:Executive   0:00:00.000   0:00:00.000   25:14:35.472
 104   8         1   Wait:Executive   0:00:00.000   0:00:00.000   25:14:35.472
 108   8         1   Wait:Executive   0:00:00.000   0:00:00.000   25:14:34.731
 116   8       499       Wait:Queue   0:00:00.000   0:00:00.000   25:14:34.521
 112   8      3534       Wait:Queue   0:00:00.000   0:00:00.000   25:14:34.521
 120   8       131       Wait:Queue   0:00:00.000   0:00:00.000   25:14:34.521
 124   8      1614   Wait:Executive   0:00:00.000   0:00:00.000   25:14:34.521
 132   8        60  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:34.380
 640   9        36       Wait:Queue   0:00:00.000   0:00:00.000   25:14:18.057
 644   9        43       Wait:Queue   0:00:00.000   0:00:00.000   25:14:18.047
 268   8    362147     Wait:UserReq   0:00:00.000   0:00:00.030   25:13:43.848

Name          Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
smss          140  11   6   33    336   0:00:00.020   0:00:00.460   25:14:34.360
                       VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                     5248     336    2004    1068      626    1    5     1068
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 136  13       480     Wait:UserReq   0:00:00.010   0:00:00.470   25:14:34.360
 144  13         7  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:34.220
 148  13         3  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:34.220
 100  13         2  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:30.915
 156  13         4  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:30.915
 152  13         2  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:30.915

Name          Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
csrss         164  13  10  273   1744   0:00:00.120   0:00:13.108   25:14:30.915
                       VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                    17404    1744    1752    1148     1730    4   33     1148
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 168  15       125     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:29.894
 172  14      3241  Wait:LpcReceive   0:00:00.030   0:00:00.090   25:14:29.784
 176  15         2  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:29.684
 180  15         4  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:29.684
 184  14      3217  Wait:LpcReceive   0:00:00.040   0:00:00.120   25:14:29.283
 188  19  10805973     Wait:UserReq   0:00:00.000   0:00:01.522   25:14:28.572
 192  16     58018     Wait:UserReq   0:00:00.000   0:00:10.314   25:14:28.572
 228  16         5     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:27.821
 504  14      3190  Wait:LpcReceive   0:00:00.040   0:00:00.080   25:14:21.892
1064  15       205     Wait:UserReq   0:00:00.000   0:00:00.020    0:01:02.029

Name          Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
winlogon      160  13  16  359   3040   0:00:00.610   0:00:02.523   25:14:29.674
                       VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                    33436    3040   11136    5480     5881   59   35     5480
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 128  15    264576     Wait:UserReq   0:00:00.290   0:00:01.381   25:14:29.674
 200  13      3036   Wait:DelayExec   0:00:00.000   0:00:00.000   25:14:28.232
 204  13       356       Wait:Queue   0:00:00.000   0:00:00.010   25:14:28.202
 216  13        46     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:28.192
 248  15       122     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:27.280
 264  15      2698     Wait:UserReq   0:00:00.020   0:00:00.180   25:14:26.289
 560  15         6     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:17.676
 660  15        11     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:16.635
 664  14      2685     Wait:UserReq   0:00:00.050   0:00:00.200   25:14:16.635
 668  14        55     Wait:UserReq   0:00:00.020   0:00:00.070   25:14:11.097
```

```
 252  13       753     Wait:UserReq   0:00:00.000   0:00:00.010   25:14:11.067
 328  11      1523     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:11.027
 672  15       107     Wait:UserReq   0:00:00.000   0:00:00.010   25:14:10.746
 196  15        45     Wait:UserReq   0:00:00.000   0:00:00.030   25:13:59.020
 744  15         2     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:58.929
 772  15         3  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:13:58.859

Name          Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
services      212   9  35  549  15320   0:00:13.379   0:00:08.492   25:14:28.192
                       VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                    55936   15320   20988   12492    65069  212   32    12492
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 236   9      8802     Wait:UserReq   0:00:00.010   0:00:00.020   25:14:27.581
 304  10      1551       Wait:Queue   0:00:00.010   0:00:00.050   25:14:25.708
 308   9      1809       Wait:Queue   0:00:00.060   0:00:00.080   25:14:25.698
 312   9      3064   Wait:DelayExec   0:00:00.000   0:00:00.000   25:14:25.588
 320  10       157   Wait:Executive   0:00:00.000   0:00:00.000   25:14:25.548
 332  11         5  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:25.057
 336   9     12081   Wait:DelayExec   0:00:00.610   0:00:01.702   25:14:25.057
 324  10       150     Wait:UserReq   0:00:00.030   0:00:00.010   25:14:24.817
 340  11        13     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:24.817
 356  11         8     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:23.605
 360   9        12     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:23.505
 364  11         2     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:23.505
 368  11        39     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:23.505
 392   9       606   Wait:Executive   0:00:00.000   0:00:00.010   25:14:23.345
 396   9     10820     Wait:UserReq   0:00:12.277   0:00:05.437   25:14:23.345
 436  11        86     Wait:UserReq   0:00:00.000   0:00:00.010   25:14:22.994
 456   9       718     Wait:UserReq   0:00:00.010   0:00:00.010   25:14:22.814
 484   9       534       Wait:Queue   0:00:00.000   0:00:00.000   25:14:21.892
 516  11        28       Wait:Queue   0:00:00.000   0:00:00.000   25:14:21.362
 544  10      5856       Wait:Queue   0:00:00.070   0:00:00.330   25:14:20.901
 944  10      5826       Wait:Queue   0:00:00.080   0:00:00.220   25:13:36.107
 952  10      3561       Wait:Queue   0:00:00.030   0:00:00.280   25:13:35.516
 956   9       360       Wait:Queue   0:00:00.000   0:00:00.000   25:13:34.985
 968   9       355       Wait:Queue   0:00:00.000   0:00:00.000   25:13:34.855
 460  10      1587     Wait:UserReq   0:00:00.070   0:00:00.080   25:13:28.996
 796  11         4     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:28.876
1008  11      1480     Wait:UserReq   0:00:00.020   0:00:00.080   25:13:28.846
 784  11        15     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:13.835
 756  11         4     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:13.795
1104  11        17  Wait:LpcReceive   0:00:00.000   0:00:00.000   24:49:29.436
 692   9         4     Wait:UserReq   0:00:00.000   0:00:00.000   24:49:27.273
 632  11        22  Wait:LpcReceive   0:00:00.010   0:00:00.000    0:03:12.286
 820  10         3     Wait:UserReq   0:00:00.000   0:00:00.000    0:02:56.654
 948  10         5  Wait:LpcReceive   0:00:00.000   0:00:00.000    0:00:52.335
 316   9         3       Wait:Queue   0:00:00.000   0:00:00.000    0:00:00.220

Name          Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
lsass         224   9  15  277   1060   0:00:00.370   0:00:00.550   25:14:28.121
                       VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                    28292    1060    4864    2128     2425   35   27     2128
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 232  11        19   Wait:Executive   0:00:00.000   0:00:00.000   25:14:27.601
 240  10        42     Wait:UserReq   0:00:00.000   0:00:00.010   25:14:27.320
 244  11         3  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:27.310
 256   9      5077   Wait:DelayExec   0:00:00.000   0:00:00.000   25:14:27.070
 260   9      4208       Wait:Queue   0:00:00.010   0:00:00.000   25:14:26.970
 272  10      5080       Wait:Queue   0:00:00.090   0:00:00.260   25:14:25.938
 276   9       253  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:25.918
 288   9       340       Wait:Queue   0:00:00.000   0:00:00.000   25:14:25.908
 292  11         3     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:25.908
 468  10       190     Wait:UserReq   0:00:00.210   0:00:00.050   25:14:22.804
 508  11         3     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:21.372
 648  10       150     Wait:UserReq   0:00:00.020   0:00:00.020   25:14:18.037
1000  11         3  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:13:13.755
1052  13         3     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:13.094
 616   9        18     Wait:UserReq   0:00:00.000   0:00:00.000    0:00:27.389

Name          Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
svchost       384   8   8  242   3192   0:00:00.230   0:00:00.330   25:14:23.475
                       VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                    20620    3192    3312    1220     2848   17   25     1220
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 380  10        24   Wait:Executive   0:00:00.000   0:00:00.010   25:14:23.475
 388   8       911   Wait:DelayExec   0:00:00.020   0:00:00.030   25:14:23.445
 400  10       521  Wait:LpcReceive   0:00:00.060   0:00:00.090   25:14:23.315
```

```
 372   9         5     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:23.224
 404   8       326       Wait:Queue   0:00:00.010   0:00:00.000   25:14:23.104
1112   8      1341   Wait:DelayExec   0:00:00.020   0:00:00.000   25:12:22.050
 752   8        39  Wait:LpcReceive   0:00:00.000   0:00:00.000    2:51:22.315
 488   9        51  Wait:LpcReceive   0:00:00.000   0:00:00.010    0:08:29.482

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
spoolsv      412   8  11  147   3436   0:00:00.060   0:00:00.180   25:14:23.024
                      VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                   25248    3436    3460    2296     1253  693   22     2296
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 408  10        27   Wait:Executive   0:00:00.000   0:00:00.010   25:14:23.024
 416  10        17     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:23.014
 420   8       306       Wait:Queue   0:00:00.000   0:00:00.000   25:14:23.014
 432   8       153   Wait:Executive   0:00:00.000   0:00:00.000   25:14:23.014
 900   9       215     Wait:UserReq   0:00:00.030   0:00:00.100   25:13:45.240
 428  10         4     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:45.210
 376  10         3     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:44.328
 904   8      1066     Wait:UserReq   0:00:00.010   0:00:00.040   25:13:44.278
 908  10         2     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:44.278
 920  10         3  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:13:44.208
 916   8         4  Wait:LpcReceive   0:00:00.000   0:00:00.000    0:00:53.296

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
svchost      444   8  30  396   6884   0:00:00.150   0:00:00.340   25:14:22.984
                      VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                   38336    6884    6964    2888     2183   62  38     2888
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 440   9        94   Wait:Executive   0:00:00.000   0:00:00.010   25:14:22.984
 452  10        44     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:22.934
 464  10       576     Wait:UserReq   0:00:00.010   0:00:00.040   25:14:22.804
 600  10       157     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:18.948
 612   8      3039   Wait:DelayExec   0:00:00.000   0:00:00.010   25:14:18.758
 624  10        22     Wait:UserReq   0:00:00.010   0:00:00.010   25:14:18.488
 628  10         3     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:18.488
 296  10        18     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:55.134
1016   9         8     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:28.756
 208  10        26     Wait:UserReq   0:00:00.000   0:00:00.010   25:13:13.755
1020   9      3030     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:13.604
1036   9       658       Wait:Queue   0:00:00.010   0:00:00.000   25:13:13.604
1044  10       201       Wait:Queue   0:00:00.000   0:00:00.050   25:13:13.594
1048  10        36     Wait:UserReq   0:00:00.000   0:00:00.010   25:13:13.594
 896  10       155     Wait:UserReq   0:00:00.000   0:00:00.010   25:13:12.723
1072  11         4     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:12.623
1076  10        59     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:12.533
1080  10         4       Wait:Queue   0:00:00.000   0:00:00.000   25:13:12.523
1084  10         4       Wait:Queue   0:00:00.000   0:00:00.000   25:13:12.503
1088  10         3     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:12.413
1092  10         3     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:12.413
1100  10         6     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:12.202
1116   8       314       Wait:Queue   0:00:00.000   0:00:00.000   25:13:12.022
 636   9       555   Wait:DelayExec   0:00:00.020   0:00:00.040   24:43:08.829
 548   8       197  Wait:LpcReceive   0:00:00.010   0:00:00.010   24:25:40.622
1024   8        65       Wait:Queue   0:00:00.000   0:00:00.000    0:03:20.288
 988   9        40  Wait:LpcReceive   0:00:00.010   0:00:00.000    0:03:20.217
 928   8         7  Wait:LpcReceive   0:00:00.000   0:00:00.000    0:03:20.107
 748   8        12  Wait:LpcReceive   0:00:00.000   0:00:00.000    0:00:53.216
1164   8         2  Wait:LpcReceive   0:00:00.010   0:00:00.000    0:00:52.435

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
regsvc       480   8   2   30    740   0:00:00.010   0:00:00.020   25:14:22.734
                      VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                    9664     740     748     240      188    9    7      240
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 476  10        29   Wait:Executive   0:00:00.000   0:00:00.010   25:14:22.734
 500   8       307       Wait:Queue   0:00:00.000   0:00:00.000   25:14:22.383

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
MSTask       496   8   6  143   3080   0:00:00.040   0:00:00.060   25:14:22.393
                      VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                   25188    3080    3088    1008      852   14   25     1008
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 492  10        43   Wait:Executive   0:00:00.020   0:00:00.010   25:14:22.393
 512   8        98     Wait:UserReq   0:00:00.010   0:00:00.040   25:14:21.362
 528  10         3  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:21.262
 532  10         3     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:21.242
 536   8       307       Wait:Queue   0:00:00.000   0:00:00.000   25:14:21.222
```

```
 540  10      1656     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:21.222

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
stisvc       524   8   4   59   1444   0:00:00.030   0:00:00.040   25:14:21.312
                     VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                  12616    1444    1456     432      364    2   15      432
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 520  10        39   Wait:Executive   0:00:00.010   0:00:00.010   25:14:21.312
 552  10         5     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:20.801
 556  10        47     Wait:UserReq   0:00:00.000   0:00:00.000   25:14:20.791
 564  10         3  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:14:20.711

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
WinMgmt      572   8   3   94    172   0:00:06.359   0:00:00.350   25:14:20.701
                     VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                  19168     172    4496     672     5547    3   15      672
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 568  10        57   Wait:Executive   0:00:00.000   0:00:00.020   25:14:20.701
 580   8       137     Wait:UserReq   0:00:00.000   0:00:00.020   25:14:19.579
 596   9       246  Wait:LpcReceive   0:00:00.020   0:00:00.040   25:14:18.988

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
mspmspsv     592   8   2   48   1340   0:00:00.020   0:00:00.020   25:14:19.509
                     VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                  12184    1340    1340     412      334    2   13      412
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 588  10        27   Wait:Executive   0:00:00.000   0:00:00.010   25:14:19.509
 472  10        22   Wait:Executive   0:00:00.010   0:00:00.000   25:14:18.958

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
Explorer     792   8  18  395  12200   0:00:12.087   0:00:24.945   25:13:58.439
                     VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                  90308   12200   16096    9348   124429   22   65     9348
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 788  10    648479     Wait:UserReq   0:00:02.914   0:00:07.891   25:13:58.439
 800  11    205829     Wait:UserReq   0:00:02.483   0:00:05.347   25:13:57.638
 804   8       498     Wait:UserReq   0:00:00.030   0:00:00.030   25:13:56.977
 696   8         3     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:55.214
 828   8      3031   Wait:DelayExec   0:00:00.000   0:00:00.000   25:13:53.241
 832  10    103978     Wait:UserReq   0:00:00.090   0:00:00.751   25:13:53.041
 836   8      5652     Wait:UserReq   0:00:00.070   0:00:00.370   25:13:52.831
 856  15         2     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:52.440
1140   8       365       Wait:Queue   0:00:00.000   0:00:00.000   25:13:11.431
 620  10     32866     Wait:UserReq   0:00:00.000   0:00:00.000   22:49:16.505
1132   8      2795     Wait:UserReq   0:00:00.030   0:00:00.050   22:49:16.505
 676   8        31  Wait:LpcReceive   0:00:00.000   0:00:00.000    0:19:36.411
 868   8        25  Wait:LpcReceive   0:00:00.000   0:00:00.010    0:13:35.412
 448   8        23   Wait:DelayExec   0:00:00.000   0:00:00.000    0:08:29.472
 808   8        37     Wait:UserReq   0:00:00.000   0:00:00.000    0:08:28.371
1068   8       118     Wait:UserReq   0:00:00.010   0:00:00.010    0:05:09.394
 300   9         3  Wait:LpcReceive   0:00:00.000   0:00:00.000    0:03:20.097
 700  10      1148     Wait:UserReq   0:00:00.150   0:00:00.330    0:01:43.188

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
popupkiller  852   8   2   97   6236   0:00:09.733   0:00:01.011   25:13:52.620
                     VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                  50620    6236    6236    2540     1745    5   31     2540
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 848  10   3677634     Wait:UserReq   0:00:09.723   0:00:01.001   25:13:52.620
1060   8         2  Wait:LpcReceive   0:00:00.000   0:00:00.000   25:07:47.535

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
qttask       864   8   5  170   4248   0:00:00.650   0:00:00.220   25:13:52.420
                     VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                 109364    4248    4248    2332     1267    4   92     2332
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 860  10       523     Wait:UserReq   0:00:00.640   0:00:00.190   25:13:52.420
 844  11         2     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:49.606
 888  12         2     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:45.730
 892  11         2     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:45.730
 912   9         3     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:43.077

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
SETI@home    880   4   3  132  13608  24:38:30.619   0:03:10.073   25:13:52.120
                     VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                  54120   13608   17036   16104 11681535    4   33    16104
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
```

```
 876   6   5309641     Wait:UserReq   0:00:01.902   0:00:11.105   25:13:52.120
 840   4         7     Wait:UserReq   0:00:00.000   0:00:00.000   25:13:48.895
 824   2  13485635            Ready  24:38:28.636   0:02:58.857   24:49:09.828

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
fire         936   8   4  129   1360   0:00:00.090   0:00:00.170    0:03:45.163
                     VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                  61176    1360    6248    1724     1989    6   44     1724
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
1096  10       980     Wait:UserReq   0:00:00.080   0:00:00.160    0:03:45.163
 960   8         1  Wait:LpcReceive   0:00:00.000   0:00:00.000    0:03:44.883
 424   9        94     Wait:UserReq   0:00:00.000   0:00:00.000    0:03:44.683
 652   8         8     Wait:UserReq   0:00:00.000   0:00:00.010    0:03:44.653

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
CMD         1172   8   1   24    820   0:00:00.060   0:00:00.410    0:01:02.089
                     VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                  11300     820     824     256      219    1   13      256
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 884  10      3345     Wait:UserReq   0:00:00.050   0:00:00.410    0:01:02.059

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
PSLIST      1156   8   2   71   1160   0:00:00.020   0:00:00.040    0:00:00.160
                     VM      WS   WS Pk    Priv   Faults NonP Page PageFile
                  14416    1160    1160     532      289    2   13      532
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
 740  14        77          Running   0:00:00.010   0:00:00.040    0:00:00.160
1168   8         0            Ready   0:00:00.000   0:00:00.000    0:00:00.000


--------------------------------------------------
NBTSTAT
--------------------------------------------------

Local Area Connection:
Node IpAddress: [0.0.0.0] Scope Id: []



    No names in cache



--------------------------------------------------
HIDDEN FILES (dir /s /a:h /t:a c: d:)
--------------------------------------------------
 Volume in drive C is ATRYP00ABK
 Volume Serial Number is 2A69-1EE3

 Directory of C:\

03/13/2000  12:00a          214,836 IO.SYS
05/10/2000  12:00a            1,553 MSDOS.SYS
08/05/2002  12:00a           93,812 COMMAND.COM
03/13/2000  12:00a      <DIR>       PARATOOL
10/27/2000  12:00a                0 BOOTLOG.TXT
05/02/2003  12:00a               84 AUTOEXEC.BAT
05/10/2000  12:00a              810 BOOTLOG.PRV
04/30/2001  12:00a                1 CONFIG.SYS
03/13/2000  12:00a              512 BOOTSECT.DOS
03/25/2002  12:00a          214,432 ntldr
03/25/2002  12:00a           34,468 NTDETECT.COM
08/08/2002  12:00a              206 BOOT.INI
05/01/2003  12:00a      201,326,592 pagefile.sys
05/10/2000  12:00a      <DIR>       Recycled
              12 File(s)    201,887,306 bytes

 Directory of C:\WINNT

05/10/2000  12:00a      <DIR>       inf
03/13/2000  12:00a           24,076 winnt.bmp
03/13/2000  12:00a           48,540 winnt256.bmp
03/25/2003  12:00a           21,692 folder.htt
03/25/2003  12:00a              271 desktop.ini
03/14/2000  12:00a      <DIR>       CSC
05/10/2000  12:00a      <DIR>       Installer
```

```
05/01/2003  12:00a             930,172 ShellIconCache
10/24/2001  12:00a      <DIR>          msdownld.tmp
05/01/2003  12:00a              54,156 QTFont.qfn
03/25/2002  12:00a      <DIR>          $NtServicePackUninstall$
07/01/2002  12:00a      <DIR>          PIF
03/25/2002  12:00a      <DIR>          $NtUninstallQ280838$
03/25/2002  12:00a      <DIR>          $NtUninstallQ259728$
03/25/2002  12:00a      <DIR>          $NtUninstallQ253934$
               6 File(s)      1,078,907 bytes

 Directory of C:\WINNT\system32

03/13/2000  12:00a      <DIR>          dllcache
04/30/2001  12:00a              21,692 folder.htt
10/25/2001  12:00a                 271 desktop.ini
03/14/2000  12:00a      <DIR>          GroupPolicy
               2 File(s)         21,963 bytes

 Directory of C:\WINNT\system32\config

03/13/2000  12:00a               1,024 system.LOG
05/02/2003  12:00a               1,024 software.LOG
05/01/2003  12:00a               1,024 default.LOG
03/13/2000  12:00a               1,024 userdiff.LOG
03/13/2000  12:00a                   0 TempKey.LOG
05/01/2003  12:00a               1,024 SECURITY.LOG
05/02/2003  12:00a               1,024 SAM.LOG
               7 File(s)          6,144 bytes

 Directory of C:\WINNT\system32\dllcache

05/01/2003  12:00a             626,960 oleaut32.dll
05/01/2003  12:00a             143,632 asycfilt.dll
05/01/2003  12:00a              16,896 stdole2.tlb
03/25/2002  12:00a           1,411,344 query.dll.tmp
03/25/2002  12:00a              42,768 webhits.dll.tmp
03/25/2002  12:00a             121,104 idq.dll.tmp
03/25/2002  12:00a             164,112 olepro32.dll.tmp
               7 File(s)      2,526,816 bytes

 Directory of C:\WINNT\system32\Microsoft\Protect\S-1-5-18\User

02/14/2002  12:00a                 336 0541ff9c-2a66-4420-bb86-a633f52274a1
02/14/2002  12:00a                  24 Preferred
               2 File(s)           360 bytes

 Directory of C:\WINNT\repair

03/14/2000  12:00a             122,880 ntuser.dat
               1 File(s)       122,880 bytes

 Directory of C:\WINNT\inf

03/25/2002  12:00a                   0 oem6.inf
03/25/2002  12:00a                   0 oem7.inf
               2 File(s)             0 bytes

 Directory of C:\WINNT\Fonts

03/13/2000  12:00a              36,672 app850.fon
03/13/2000  12:00a               6,352 cga40850.fon
03/13/2000  12:00a               4,320 cga80850.fon
05/02/2003  12:00a                  67 desktop.ini
05/02/2003  12:00a              36,656 dosapp.fon
03/13/2000  12:00a               8,384 ega40850.fon
03/13/2000  12:00a               5,328 ega80850.fon
05/01/2003  12:00a              24,480 marlett.ttf
05/01/2003  12:00a              26,112 smalle.fon
05/01/2003  12:00a              56,336 symbole.fon
03/13/2000  12:00a               5,232 vga850.fon
05/01/2003  12:00a               5,360 vgafix.fon
05/02/2003  12:00a               5,168 vgaoem.fon
05/02/2003  12:00a               7,280 vgasys.fon
03/13/2000  12:00a              10,976 8514fix.fon
03/13/2000  12:00a              12,288 8514oem.fon
03/13/2000  12:00a               9,280 8514sys.fon
03/13/2000  12:00a              21,504 smallf.fon
```

```
03/13/2000  12:00a               5,184 vga860.fon
03/13/2000  12:00a               5,200 vga863.fon
03/13/2000  12:00a               5,184 vga865.fon
              21 File(s)        297,363 bytes

 Directory of C:\WINNT\Web

04/09/2003  12:00a               1,316 webview.css
04/09/2003  12:00a               4,659 controlp.htt
11/06/2002  12:00a               5,296 default.htt
05/02/2003  12:00a               3,210 folder.htt
11/27/2002  12:00a              13,280 nethood.htt
07/23/2001  12:00a              13,798 printers.htt
11/06/2002  12:00a              11,149 recycle.htt
03/14/2000  12:00a               6,489 schedule.htt
08/05/2002  12:00a               8,898 dialup.htt
05/01/2003  12:00a               8,248 wvleft.bmp
05/01/2003  12:00a                  54 wvline.gif
03/25/2003  12:00a              14,865 wvlogo.gif
08/07/2002  12:00a              90,056 classic.bmp
08/07/2002  12:00a                 634 classic.htt
08/07/2002  12:00a              31,080 folder.bmp
03/14/2000  12:00a               1,024 starter.htt
03/14/2000  12:00a              31,080 starter.bmp
03/14/2000  12:00a              31,080 preview.bmp
08/14/2002  12:00a              16,981 imgview.htt
05/01/2003  12:00a                 830 deskmovr.htt
03/14/2000  12:00a               2,913 safemode.htt
05/02/2003  12:00a              19,355 fsresult.htt
08/07/2002  12:00a              28,565 standard.htt
11/06/2002  12:00a              31,438 webview.js
11/27/2002  12:00a              12,403 wvnet.gif
03/14/2000  12:00a               2,642 exclam.gif
03/14/2000  12:00a                 842 bullet.gif
03/14/2000  12:00a                  80 plushot.gif
03/14/2000  12:00a                  59 pluscold.gif
03/14/2000  12:00a                  77 minhot.gif
03/14/2000  12:00a                  56 mincold.gif
04/29/2002  12:00a              11,083 ftp.htt
              32 File(s)        403,540 bytes

 Directory of C:\WINNT\Temp

10/23/2001  12:00a               6,336 OLD12.tmp
10/23/2001  12:00a               4,304 OLD14.tmp
10/23/2001  12:00a              23,408 OLD16.tmp
10/23/2001  12:00a              31,712 OLD18.tmp
10/23/2001  12:00a               8,368 OLD1A.tmp
10/23/2001  12:00a               5,312 OLD1C.tmp
10/23/2001  12:00a              57,936 OLD25.tmp
10/23/2001  12:00a              81,728 OLD27.tmp
10/23/2001  12:00a              64,656 OLD29.tmp
10/23/2001  12:00a              89,856 OLD2B.tmp
              10 File(s)        373,616 bytes

 Directory of C:\WINNT\Tasks

05/02/2003  12:00a                  65 desktop.ini
05/01/2003  12:00a                   6 SA.DAT
05/02/2003  12:00a                 396 {842CA231-A137-4998-B7F8-
4F7D9C2CA493}_HP1_Administrator.job
               3 File(s)            467 bytes

 Directory of C:\WINNT\Downloaded Program Files

05/02/2003  12:00a                  65 desktop.ini
               1 File(s)             65 bytes

 Directory of C:\WINNT\Offline Web Pages

05/02/2003  12:00a                  65 desktop.ini
               1 File(s)             65 bytes

 Directory of C:\Documents and Settings

03/13/2000  12:00a      <DIR>          Default User
               0 File(s)              0 bytes
```

```
 Directory of C:\Documents and Settings\Default User

03/13/2000  12:00a      <DIR>          Application Data
03/13/2000  12:00a      <DIR>          NetHood
03/13/2000  12:00a      <DIR>          PrintHood
03/13/2000  12:00a      <DIR>          Recent
03/13/2000  12:00a      <DIR>          SendTo
03/13/2000  12:00a      <DIR>          Templates
03/13/2000  12:00a      <DIR>          Local Settings
05/10/2000  12:00a             122,880 NTUSER.DAT
05/10/2000  12:00a               1,024 NTUSER.DAT.LOG
               2 File(s)        123,904 bytes

 Directory of C:\Documents and Settings\Default User\My Documents\My Pictures

05/02/2003  12:00a                 438 Desktop.ini
               1 File(s)            438 bytes

 Directory of C:\Documents and Settings\Default User\Local Settings

03/13/2000  12:00a      <DIR>          Application Data
               0 File(s)              0 bytes

 Directory of C:\Documents and Settings\Default User\Local Settings\Temporary Internet
Files

05/02/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Default User\Local Settings\Temporary Internet
Files\Content.IE5

05/02/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Default User\Local Settings\Temporary Internet
Files\Content.IE5\UP88TB8V

05/02/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Default User\Local Settings\Temporary Internet
Files\Content.IE5\DEIPPZXX

05/02/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Default User\Local Settings\Temporary Internet
Files\Content.IE5\NUGVFTZQ

05/02/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Default User\Local Settings\Temporary Internet
Files\Content.IE5\3WL0TNHB

05/02/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Default User\Local Settings\History

05/02/2003  12:00a                 113 desktop.ini
               1 File(s)            113 bytes

 Directory of C:\Documents and Settings\Default User\Local
Settings\History\History.IE5

06/27/2002  12:00a                 113 desktop.ini
               1 File(s)            113 bytes

 Directory of C:\Documents and Settings\All Users

03/13/2000  12:00a      <DIR>          Application Data
03/13/2000  12:00a      <DIR>          Templates
09/21/2001  12:00a      <DIR>          DRM
05/10/2000  12:00a               1,024 NTUSER.DAT.LOG
```

```
05/10/2000  12:00a               2,370 ntuser.pol
               2 File(s)          3,394 bytes

 Directory of C:\Documents and Settings\All Users\Application Data\Microsoft\Windows
NT\MSFax

03/14/2000  12:00a      <DIR>          faxreceive
03/14/2000  12:00a      <DIR>          queue
               0 File(s)              0 bytes

 Directory of C:\Documents and Settings\All Users\Documents

03/14/2000  12:00a      <DIR>          My Faxes
               0 File(s)              0 bytes

 Directory of C:\Documents and Settings\All Users\DRM

09/21/2001  12:00a               1,536 drmv2.lic
09/21/2001  12:00a               1,536 drmv2.sst
               2 File(s)          3,072 bytes

 Directory of C:\Documents and Settings\Administrator

05/02/2003  12:00a           1,048,576 NTUSER.DAT
04/22/2002  12:00a      <DIR>          Local Settings
03/14/2000  12:00a      <DIR>          Templates
03/14/2000  12:00a      <DIR>          SendTo
03/14/2000  12:00a      <DIR>          Recent
03/14/2000  12:00a      <DIR>          PrintHood
03/14/2000  12:00a      <DIR>          NetHood
03/14/2000  12:00a      <DIR>          Application Data
05/02/2003  12:00a               1,024 ntuser.dat.LOG
05/01/2003  12:00a                 180 ntuser.ini
               3 File(s)      1,049,780 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings

03/14/2000  12:00a      <DIR>          Application Data
               0 File(s)              0 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\History

05/02/2003  12:00a                 113 desktop.ini

               1 File(s)            113 bytes

 Directory of C:\Documents and Settings\Administrator\Local
Settings\History\History.IE5

03/14/2000  12:00a                 113 desktop.ini
               1 File(s)            113 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files

04/08/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5

04/08/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\WXUROD2J


08/21/2002  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\GHCT0ZW1

01/30/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes
```

```
 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\OH274X2Z

06/27/2002  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\4PA3OXIF

06/27/2002  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\C5IRGPUR

06/27/2002  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\65GRGJW9

04/08/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\WD2R05UN

01/13/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\KXA3OTAJ

03/13/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\2484M309

06/27/2002  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\8LQ34PE3

06/27/2002  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\GPYJO1AB

06/27/2002  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\MRIRUNY9

06/27/2002  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\XWS3LHK5

03/17/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\6HH2NMTO

03/17/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\XRVFHTSE

03/17/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes
```

```
 Directory of C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files\Content.IE5\O7TZEABX

03/17/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of C:\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Windows

05/01/2003  12:00a               8,192 UsrClass.dat
03/14/2000  12:00a               1,024 UsrClass.dat.LOG
               2 File(s)          9,216 bytes

 Directory of C:\Documents and Settings\Administrator\Recent

05/02/2003  12:00a                 122 Desktop.ini
               1 File(s)            122 bytes

 Directory of C:\Documents and Settings\Administrator\My Documents\My Pictures

05/02/2003  12:00a                 438 Desktop.ini
05/11/2000  12:00a               7,168 Thumbs.db
               2 File(s)          7,606 bytes

 Directory of C:\Documents and Settings\Administrator\Favorites

05/02/2003  12:00a                  83 Desktop.ini
               1 File(s)             83 bytes

 Directory of C:\Documents and Settings\Administrator\Application
Data\Microsoft\Internet Explorer

05/01/2003  12:00a               2,526 Desktop.htt
               1 File(s)          2,526 bytes

 Directory of C:\Documents and Settings\Administrator\Application
Data\Microsoft\Protect\S-1-5-21-1078081533-842925246-1708537768-500

03/14/2000  12:00a                 456 481efaca-4e99-45bc-b796-eedaf04d1038
03/14/2000  12:00a                  24 Preferred
               2 File(s)            480 bytes

 Directory of C:\Documents and Settings\Administrator\Application
Data\Microsoft\Protect\S-1-5-21-940727086-1440894624-411895618-500

05/10/2000  12:00a                 456 4e0140b6-4ff7-466b-aaf1-8c5371e69970
05/02/2003  12:00a                  24 Preferred
04/22/2002  12:00a                 456 0c4a33a8-e733-4b23-956b-292238d853e7
05/02/2003  12:00a                 456 ccb97d40-4e29-4d15-b3d1-9e032b11375d
               4 File(s)          1,392 bytes

 Directory of C:\Documents and Settings\fooman

04/29/2002  12:00a             229,376 NTUSER.DAT
04/29/2002  12:00a               1,024 NTUSER.DAT.LOG
04/29/2002  12:00a      <DIR>          Local Settings
04/29/2002  12:00a      <DIR>          Templates
04/29/2002  12:00a      <DIR>          SendTo
04/29/2002  12:00a      <DIR>          Recent
04/29/2002  12:00a      <DIR>          PrintHood
04/29/2002  12:00a      <DIR>          NetHood
04/29/2002  12:00a      <DIR>          Application Data
08/05/2002  12:00a                 180 ntuser.ini
               3 File(s)        230,580 bytes

 Directory of C:\Documents and Settings\fooman\Local Settings

04/29/2002  12:00a      <DIR>          Application Data
               0 File(s)              0 bytes

 Directory of C:\Documents and Settings\fooman\Local Settings\History

05/02/2003  12:00a                 113 desktop.ini
               1 File(s)            113 bytes

 Directory of C:\Documents and Settings\fooman\Local Settings\History\History.IE5
```

```
06/27/2002  12:00a                113 desktop.ini
               1 File(s)           113 bytes

 Directory of C:\Documents and Settings\fooman\Local Settings\Temporary Internet Files

05/02/2003  12:00a                 67 desktop.ini
               1 File(s)            67 bytes

 Directory of C:\Documents and Settings\fooman\Local Settings\Temporary Internet
Files\Content.IE5

05/02/2003  12:00a                 67 desktop.ini
               1 File(s)            67 bytes

 Directory of C:\Documents and Settings\fooman\Local Settings\Temporary Internet
Files\Content.IE5\3WL0TNHB

05/02/2003  12:00a                 67 desktop.ini
               1 File(s)            67 bytes

 Directory of C:\Documents and Settings\fooman\Local Settings\Temporary Internet
Files\Content.IE5\NUGVFTZQ

05/02/2003  12:00a                 67 desktop.ini
               1 File(s)            67 bytes

 Directory of C:\Documents and Settings\fooman\Local Settings\Temporary Internet
Files\Content.IE5\DEIPPZXX

05/02/2003  12:00a                 67 desktop.ini
               1 File(s)            67 bytes

 Directory of C:\Documents and Settings\fooman\Local Settings\Temporary Internet
Files\Content.IE5\UP88TB8V

05/02/2003  12:00a                 67 desktop.ini
               1 File(s)            67 bytes

 Directory of C:\Documents and Settings\fooman\Local Settings\Application
Data\Microsoft\Windows

04/29/2002  12:00a              8,192 UsrClass.dat
04/29/2002  12:00a              1,024 UsrClass.dat.LOG
               2 File(s)        9,216 bytes

 Directory of C:\Documents and Settings\fooman\Recent

05/02/2003  12:00a                122 Desktop.ini
               1 File(s)           122 bytes

 Directory of C:\Documents and Settings\fooman\My Documents\My Pictures

05/02/2003  12:00a                438 Desktop.ini
               1 File(s)           438 bytes

 Directory of C:\Documents and Settings\fooman\Favorites

05/02/2003  12:00a                 83 Desktop.ini
               1 File(s)            83 bytes

 Directory of C:\Documents and Settings\fooman\Application Data\Microsoft\Internet
Explorer

04/29/2002  12:00a              2,656 Desktop.htt
               1 File(s)        2,656 bytes

 Directory of C:\Program Files

01/30/2003  12:00a             21,952 folder.htt
05/02/2003  12:00a                271 desktop.ini
03/14/2000  12:00a      <DIR>         InstallShield Installation Information
10/24/2001  12:00a      <DIR>         Uninstall Information
               2 File(s)       22,223 bytes

 Directory of C:\Program Files\Common Files\Microsoft Shared\Web Folders
```

```
05/10/2000  12:00a               7,994 PUBPLACE.HTT
               1 File(s)          7,994 bytes

 Directory of C:\Program Files\Internet Explorer

10/24/2001  12:00a      <DIR>          Backup Data
10/24/2001  12:00a      <DIR>          Uninstall Information
               0 File(s)              0 bytes

 Directory of C:\Program Files\Internet Explorer\Backup Data

04/29/2002  12:00a          17,158,756 IE5BAK.DAT
04/29/2002  12:00a              11,128 IE5BAK.INI
               2 File(s)     17,169,884 bytes

 Directory of C:\Program Files\Internet Explorer\Uninstall Information

04/29/2002  12:00a              17,403 IEEX.DAT
04/29/2002  12:00a                 431 IEEX.INI
04/29/2002  12:00a              27,207 IEREADME.DAT
04/29/2002  12:00a                 359 IEREADME.INI
               4 File(s)         45,400 bytes

 Directory of C:\Program Files\Thumbs4

04/23/2001  12:00a              10,860 THUMBS4.GID
               1 File(s)         10,860 bytes

 Directory of C:\Program Files\Uninstall Information

10/24/2001  12:00a      <DIR>          OutlookExpress
04/29/2002  12:00a      <DIR>          IE UserData NT
               0 File(s)              0 bytes

 Directory of C:\Program Files\Uninstall Information\OutlookExpress

04/29/2002  12:00a           4,797,900 OutlookExpress.DAT
04/29/2002  12:00a               8,535 OutlookExpress.INI
               2 File(s)      4,806,435 bytes

 Directory of C:\Program Files\Uninstall Information\IE UserData NT

04/29/2002  12:00a                 346 IE UserData NT.DAT
04/29/2002  12:00a                 329 IE UserData NT.INI
               2 File(s)            675 bytes

 Directory of C:\Recycled

05/02/2003  12:00a                  65 desktop.ini
04/14/2003  12:00a                  20 INFO2
               2 File(s)            85 bytes

     Total Files Listed:
             191 File(s)    230,230,844 bytes
              50 Dir(s)   5,544,497,152 bytes free


-------------------------------------------------
MD5SUM
-------------------------------------------------
-------------------------------------------------
AT scheduler list
There are no entries in the list.
-------------------------------------------------
END TIME
-------------------------------------------------
11:51a
Fri 05/02/2003
```

Appendix I

Netsetup.Log (Sanitized)

```
03/14 00:00:53 ----------------------------------------------------------------
03/14 00:00:53 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
03/14 00:00:53 NetpCheckNetBiosNameNotInUse: for 'WORKGROUP' returned: 0x858
03/14 00:00:53 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x858
03/14 00:00:53 NetpValidateName: name 'WORKGROUP' is valid for type 2
03/14 00:00:53 ----------------------------------------------------------------
03/14 00:00:53 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
03/14 00:00:53 NetpCheckNetBiosNameNotInUse: for 'WORKGROUP' returned: 0x858
03/14 00:00:53 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x858
03/14 00:00:53 NetpValidateName: name 'WORKGROUP' is valid for type 2
03/14 00:00:54 ----------------------------------------------------------------
03/14 00:00:54 NetpDoDomainJoin
03/14 00:00:54 NetpMachineValidToJoin: 'HP-6DDLBKHD7P4T'
03/14 00:00:54 NetpGetLsaPrimaryDomain: status: 0x0
03/14 00:00:54 NetpMachineValidToJoin: status: 0x0
03/14 00:00:54 NetpJoinWorkgroup: joining computer 'HP-6DDLBKHXXXXX' to workgroup
'WORKGROUP'
03/14 00:00:54 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
03/14 00:00:54 NetpCheckNetBiosNameNotInUse: for 'WORKGROUP' returned: 0x858
03/14 00:00:54 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x858
03/14 00:00:54 NetpValidateName: name 'WORKGROUP' is valid for type 2
03/14 00:00:54 NetpSetLsaPrimaryDomain: for 'WORKGROUP' status: 0x0
03/14 00:00:54 NetpControlServices: open service 'NETLOGON' failed: 0x424
03/14 00:00:54 NetpJoinWorkgroup: status:  0x0
03/14 00:00:54 NetpDoDomainJoin: status: 0x0
03/14 00:01:39 ----------------------------------------------------------------
03/14 00:01:39 NetpValidateName: checking to see if 'HP-6DDLBKHXXXXX' is valid as type
1 name
03/14 00:01:51 NetpCheckNetBiosNameNotInUse for 'HP-6DDLBKHXXXXX' [MACHINE] returned
0x0
03/14 00:01:51 NetpValidateName: name 'HP-6DDLBKHXXXXX' is valid for type 1
03/14 00:01:51 ----------------------------------------------------------------
03/14 00:01:51 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
03/14 00:01:51 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x0
03/14 00:01:51 NetpValidateName: name 'WORKGROUP' is valid for type 2
03/14 00:01:51 ----------------------------------------------------------------
03/14 00:01:51 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
03/14 00:01:51 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x0
03/14 00:01:51 NetpValidateName: name 'WORKGROUP' is valid for type 2
03/14 00:01:51 ----------------------------------------------------------------
03/14 00:01:51 NetpDoDomainJoin
03/14 00:01:51 NetpMachineValidToJoin: 'HP-6DDLBKHXXXXX'
03/14 00:01:51 NetpGetLsaPrimaryDomain: status: 0x0
03/14 00:01:51 NetpMachineValidToJoin: status: 0x0
03/14 00:01:51 NetpJoinWorkgroup: joining computer 'HP-6DDLBKHXXXXX' to workgroup
'WORKGROUP'
03/14 00:01:51 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
03/14 00:01:51 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x0
03/14 00:01:51 NetpValidateName: name 'WORKGROUP' is valid for type 2
03/14 00:01:51 NetpSetLsaPrimaryDomain: for 'WORKGROUP' status: 0x0
03/14 00:01:51 NetpJoinWorkgroup: status:  0x0
03/14 00:01:51 NetpDoDomainJoin: status: 0x0
05/10 13:46:02 ----------------------------------------------------------------
05/10 13:46:02 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
05/10 13:46:02 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x0
05/10 13:46:02 NetpValidateName: name 'WORKGROUP' is valid for type 2
```

```
05/10 13:46:02 ----------------------------------------------------------------
05/10 13:46:02 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
05/10 13:46:02 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x0
05/10 13:46:02 NetpValidateName: name 'WORKGROUP' is valid for type 2
05/10 13:46:02 ----------------------------------------------------------------
05/10 13:46:02 NetpDoDomainJoin
05/10 13:46:02 NetpMachineValidToJoin: 'EVECTRA01'
05/10 13:46:02 NetpGetLsaPrimaryDomain: status: 0x0
05/10 13:46:02 NetpMachineValidToJoin: status: 0x0
05/10 13:46:02 NetpJoinWorkgroup: joining computer 'EVECTRA01' to workgroup
'WORKGROUP'
05/10 13:46:02 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
05/10 13:46:02 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x0
05/10 13:46:02 NetpValidateName: name 'WORKGROUP' is valid for type 2
05/10 13:46:02 NetpSetLsaPrimaryDomain: for 'WORKGROUP' status: 0x0
05/10 13:46:02 NetpJoinWorkgroup: status:  0x0
05/10 13:46:02 NetpDoDomainJoin: status: 0x0
05/10 13:46:03 ----------------------------------------------------------------
05/10 13:46:03 NetpValidateName: checking to see if 'EVECTRA01' is valid as type 1
name
05/10 13:46:03 NetpCheckNetBiosNameNotInUse for 'EVECTRA01' [MACHINE] returned 0x0
05/10 13:46:03 NetpValidateName: name 'EVECTRA01' is valid for type 1
05/10 13:46:03 ----------------------------------------------------------------
05/10 13:46:03 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
05/10 13:46:03 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x0
05/10 13:46:03 NetpValidateName: name 'WORKGROUP' is valid for type 2
05/10 13:46:03 ----------------------------------------------------------------
05/10 13:46:03 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
05/10 13:46:03 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x0
05/10 13:46:03 NetpValidateName: name 'WORKGROUP' is valid for type 2
05/10 13:46:03 ----------------------------------------------------------------
05/10 13:46:03 NetpDoDomainJoin
05/10 13:46:03 NetpMachineValidToJoin: 'EVECTRA01'
05/10 13:46:03 NetpGetLsaPrimaryDomain: status: 0x0
05/10 13:46:03 NetpMachineValidToJoin: status: 0x0
05/10 13:46:03 NetpJoinWorkgroup: joining computer 'EVECTRA01' to workgroup
'WORKGROUP'
05/10 13:46:03 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
05/10 13:46:03 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x0
05/10 13:46:03 NetpValidateName: name 'WORKGROUP' is valid for type 2
05/10 13:46:03 NetpSetLsaPrimaryDomain: for 'WORKGROUP' status: 0x0
05/10 13:46:03 NetpJoinWorkgroup: status:  0x0
05/10 13:46:03 NetpDoDomainJoin: status: 0x0
11/22 14:21:40 ----------------------------------------------------------------
11/22 14:21:40 NetpValidateName: checking to see if 'HP1' is valid as type 1 name
11/22 14:21:47 NetpCheckNetBiosNameNotInUse for 'HP1' [MACHINE] returned 0x0
11/22 14:21:47 NetpValidateName: name 'HP1' is valid for type 1
11/22 14:21:47 ----------------------------------------------------------------
11/22 14:21:47 NetpValidateName: checking to see if 'hp1.' is valid as type 5 name
11/22 14:21:47 NetpValidateName: name 'hp1.' is valid for type 5
11/22 14:24:48 ----------------------------------------------------------------
11/22 14:24:48 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
11/22 14:24:48 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x0
11/22 14:24:48 NetpValidateName: name 'WORKGROUP' is valid for type 2
11/22 14:24:48 ----------------------------------------------------------------
11/22 14:24:48 NetpDoDomainJoin
11/22 14:24:48 NetpMachineValidToJoin: 'HP1'
11/22 14:24:48 NetpGetLsaPrimaryDomain: status: 0x0
11/22 14:24:48 NetpMachineValidToJoin: status: 0x0
11/22 14:24:48 NetpJoinWorkgroup: joining computer 'HP1' to workgroup 'WORKGROUP'
11/22 14:24:48 NetpValidateName: checking to see if 'WORKGROUP' is valid as type 2
name
11/22 14:24:48 NetpCheckNetBiosNameNotInUse for 'WORKGROUP' [ Workgroup as MACHINE]
returned 0x0
11/22 14:24:48 NetpValidateName: name 'WORKGROUP' is valid for type 2
```

```
11/22 14:24:48 NetpSetLsaPrimaryDomain: for 'WORKGROUP' status: 0x0
11/22 14:24:48 NetpJoinWorkgroup: status:  0x0
11/22 14:24:48 NetpDoDomainJoin: status: 0x0
```

Appendix J

Forensics (Hostname) Fstab File Showing The Partition Configured To Mount In Read Only Mode.

```
LABEL=/                 /                       ext3    defaults        1 1
none                    /dev/pts                devpts  gid=5,mode=620  0 0
none                    /proc                   proc    defaults        0 0
none                    /dev/shm                tmpfs   defaults        0 0
/dev/hda3               swap                    swap    defaults        0 0
/dev/cdrom              /mnt/cdrom              udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/hdd2               /mnt/ext                ext2    ro              0 0
/dev/hdd3               /forensics              ext2    defaults        0 0
/dev/fd0                /mnt/floppy             auto    noauto,owner,kudzu 0 0
/dev/hdb4               /mnt/zip                auto    noauto,owner,kudzu 0 0
```