Global Information Assurance Certification Paper

GIAC Certified Forensic Analyst (GCFA) Practical

Version 1.1b:

Submitted by: Brad Bowers

Date submitted: 4/10/03

Part 1 – Analyze an Unknown Binary

Name: atd
The file being analyzed is an unknown binary called atd. From my analysis of the unknown binary (atd), it is a renamed version of a Unix based Trojan application called *Loki2.* A thorough description of the Trojan application and its functions is discussed later in the paper. The binary is the server portion of the loki2 trojan more commonly known as lokid. The Trojan application has simply been renamed as atd. This was most likely done in an attempt to replace and masquerade the Trojan for the "at" daemon. Atd is a Linux command scheduling service used for running job queries at specified times. The following sections below will discuss in detail the findings and evidence that lead to the conclusion that the atd binary is in fact the server portion of the Loki2 Trojan application.

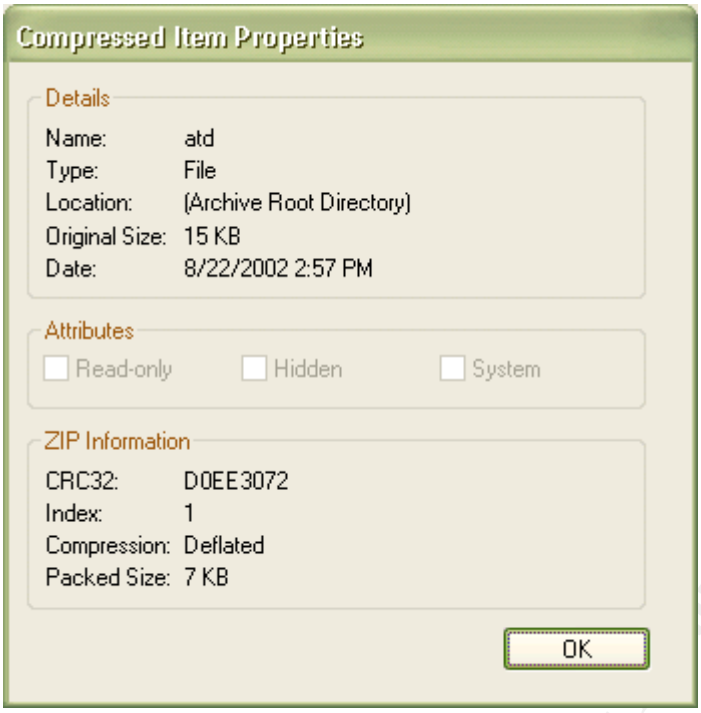
File information: To generate additional information about the binary the Unix "file" command was used. The "file" command is a tool that looks at a file's header information and provides information as to what type of file is being analyzed. The file command compares files to a list of known file types stored in /etc/magic. The following file output was received from the atd binary:

atd: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), stripped

The file command shows that the binary is a known type and is a Linux executable that requires link libraries. The "stripped" in the file output show that all symbol information has been stripped from the executable.

MAC times: The binary file that was given for this part of the practical was compressed in a Windows zip file. The fact that the file is not being analyzed on the original system has a significant impact on the MAC information. The original file creation date has been changed since the file has been packaged and transmitted in a zip file. From the information that is available it appears that the atd file was last accessed and modified on August 22nd, 2002 at 2:57pm. I derived this information by analyzing the atd file from within the zip file on a windows system.

Using Microsoft's zip/compression application I was able to view inside the zip file and gather file information without corrupting or modifying the file in anyway. The following screen shot depicts the information that was retrieved:



Unfortunately, there is no sure way of identifying the creation time of the atd file. If this binary was being investigated on the compromised system or a dd bit-for-bit image of the file system it would be possible to complete a more thorough mac time analysis. This would have been done by getting the inode information for the file, then running the debugfs stat command with the atd file's inode number. An **example** of how this could be done is:

 # ls – i atd
472546 atd
 # debugfs
debugfs 1.27 (8-Mar-2002)
 # debugfs open /dev/hda2
#debugfs: stat <472546>
Inode: 472546 Type: regular Mode: 0644 Flags: 0x0 Generation: 79014
User: 0 Group: 0 Size: 15348
File ACL: 0 Directory ACL: 0
Links: 1 Blockcount: 32
Fragment: Address: 0 Number: 0 Size: 0
ctime: 0x3dfbc590 -- Sat Dec 14 18:58:08 2002
atime: 0x3dfbd8d0 -- Sat Dec 14 20:20:16 2002
mtime: 0x3dfbc590 -- Sat Dec 14 18:58:08 2002
BLOCKS:
(0-3):559574-559577

The ctime, atime, and mtime show the creation, last accessed and last modified time respectfully of the file.

It is important to note that MAC times can easily be changed by an attacker. MAC time information is stored in inodes. By using the debugfs command, a

command that comes standard with most distributions of Unix and Linux, it is simple to modify the creation, modified, and accessed times. While MAC information taken from inodes can be invaluable in an investigation it is important to use common sense.

File owner(s): Since the file being analyzed is not on a bit-for-bit image of the system or being analyzed on the compromised system itself, it is not possible to be 100 percent positive who the owner of the file was. The file does however provide us with some important information that enables us to make an educated guess as to who owned the file. We are unable to determine who originally owned the file, but since the file is a Trojanized version of the at daemon executable that requires root privileges to run we can deduce that the owner of the file was "root" at some point. It should be mentioned that the file could have been originally owned by a less privileged user account but most likely could not be executed without root privileges.

File size: 14.9 kilobytes

MD5 Hash: The provided MD5 hash for this file was 48e8e8ed3052cbf637e638fa82bdc566 atd. This value was again verified with the following command:

 # md5sum atd
48e8e8ed3052cbf637e638fa82bdc566 atd

This was done to ensure that the file was not manipulated or corrupted during download and that I'm working with a file that is an exact copy of the original.

Key words found: The method I used to identify keywords for the atd binary was to use the unix "strings" command. Strings is a program that parses through a file(s) and pulls out all ascii (plain text) information of four characters or more. As you can see below this can provide some excellent forensic information about what the program is and how the program works.

The command to run this strings search was:

C:\strings –a atd >> temp.txt

The following plain text strings were found in the atd binary:

/lib/ld-linux.so.1
libc.so.5
longjmp
strcpy
ioctl
popen
shmctl
geteuid
_DYNAMIC
getprotobynumber
errno

__strtol_internal
usleep
semget
getpid
fgets
shmat
*_IO_stderr_*
perror
getuid
semctl
optarg
socket
__environ
bzero
_init
alarm
__libc_init
environ
fprintf
kill
inet_addr
chdir
shmdt
setsockopt
__fpu_control
shmget
wait
umask
signal
read
strncmp
sendto
bcopy
fork
strdup
getopt
inet_ntoa
getppid
time
gethostbyname
_fini
sprintf
difftime
atexit
*_GLOBAL_OFFSET_TABLE_*
semop
exit
__setfpucw
open
setsid
close
_errno
_etext
_edata
__bss_start
_end

lokid: Client database full
DEBUG: stat_client nono
lokid version: %s
remote interface: %s
active transport:%s
active cryptography: %s
server uptime: %.02f minutes
client ID: %d
packets written: %ld
bytes written: %ld
requests: %d
N@[fatal] cannot catch SIGALRM
lokid: inactive client <%d> expired from list [%d]
@[fatal] shared mem segment request error
[fatal] semaphore allocation error
[fatal] could not lock memory
[fatal] could not unlock memory
[fatal] shared mem segment detach error
[fatal] cannot destroy shmid
[fatal] cannot destroy semaphore
[fatal] name lookup failed
[fatal] cannot catch SIGALRM
[fatal] cannot catch SIGCHLD
[fatal] Cannot go daemon
[fatal] Cannot create session
/dev/tty
[fatal] cannot detach from controlling terminal
/tmp
[fatal] invalid user identification value
v:p:
Unknown transport
lokid -p (i|u) [-v (0|1)]
[fatal] socket allocation error
[fatal] cannot catch SIGUSR1
Cannot set IP_HDRINCL socket option
[fatal] cannot register with atexit(2)
LOKI2 route [(c) 1997 guild corporation worldwide]
[fatal] cannot catch SIGALRM
[fatal] cannot catch SIGCHLD
[SUPER fatal] control should NEVER fall here
[fatal] forking error
lokid: server is currently at capacity. Try again later
lokid: Cannot add key
lokid: popen
[non fatal] truncated write
/quit all
lokid: client <%d> requested an all kill
sending L_QUIT: <%d> %s
lokid: clean exit (killed at client request)
[fatal] could not signal process group
/quit
lokid: cannot locate client entry in database
lokid: client <%d> freed from list [%d]
/stat
/swapt
[fatal] could not signal parent

lokid: unsupported or unknown command string
lokid: client <%d> requested a protocol swap
sending protocol update: <%d> %s [%d]
lokid: transport protocol changed to %s
<End of file>

The strings information that was gathered from the atd file provided a tremendous amount of forensic data. To start with the first two lines that strings found "/lib/ld-linux.so.1" and "libc.so.5" shows that the binary was designed to work on fairly old versions of the Linux operating systems. These two libraries are dependencies that the binary calls upon during execution. Other strings information such as "_DYNAMIC" and "fatal] socket allocation error" shows that the binary can run in memory and utilizes network connectivity as part of its functionality. This is also seen throughout the strings dump; "packets written: %ld", "bytes written: %ld", "[fatal] socket allocation error" and " server uptime: %.02f minutes".

Another interesting piece of text that was captured in the strings dump is "active cryptography: %s". This is interesting because it seems to allude to the fact that the binary does or can use some form of encryption as part of its functionality.

The keyword that stands out the most in the strings text is "LOKI2route [(c) 1997 guild corporation worldwide]". This piece of text strongly suggests that the binary is actually the loki2 Trojan. Further findings illustrated later in this paper will show that this piece of text was very valuable in identifying the binary and its uses.

Program description: The binary (atd) turned out to be a Trojan application called Loki2. More specifically, atd is the server portion of Loki2 that is designed to sit on a compromised host and listen for connection attempts. Loki2 was originally created as a proof of concept program to demonstrate some of the potential insecurities associated with network protocols[1]. The best way to describe the application is a network command tunnel that allows a user to transmit commands through ICMP echo and ICMP echo replies. ICMP is short for Internet control messaging protocol. ICMP is used for trouble shooting and error reporting between a host server and a gateway to the Internet[2]. ICMP's echo datagrams are used to test that a system is responsive for requests. The ICMP echo (also known as ICMP type 8) is sent to a target host. If the host is live and can accept ICMP echo datagrams it will reply by sending an echo reply (ICMP type 0). It is this communication path that the Loki Trojan uses to send and receive data. What's the value of this? Since the application uses ICMP packets as its form of transmitting the data it can elude applications such as IDS systems. Most IDS systems are designed to look for and analyze active TCP port connections for potential malicious activity. Since the application utilizes ICMP

[1] The Phrack Home page http://www.phrack.com/phrack/51/P51-06
[2] http://searchsystemsmanagement.techtarget.com/sDefinition/0,,sid20_gci214012,00.html

packets it is essentially able to hide below radar. Even packet analyzing IDS systems may not identify the tunnel since most do not analyze ICMP packets for malicious content.

Here is a synopsis of how it would be installed and how it works. For a full description and breakdown of the software's functionality go to http://www.phrack.com/phrack/51/P51-06.

The program sets up an active listener on a target host. This is done when the loki2 daemon (lokid) is executed on the system. The listener acts as a packet analyzer for all inbound ICMP echo packets. Machines with the Loki2 daemon running will pull Loki2 commands from the ICMP packets.

An interesting capability of the Loki2 program is the ability to encrypt the information encapsulated in the ICMP echo packets. The daemon can be configured to use Diffie-Hillman or Blowfish encryption methods to further obfuscate the information being transmitted.

Once the daemon has completed the requested commands the output of the commands is sent back to the client as ICMP_ECHOREPLY packets.

Logical step-by-step breakdown of the actions Loki2 takes:

1. Lokid (server portion of the application) is initiated on the target system.
2. Remote user initiates Loki client with command "./loki –d host ip".
3. Requested commands are encapsulated in ICMP echo datagram which are then sent to the target host.
4. Lokid watches incoming traffic and specifically looks for ICMP echo requests. When an echo request datagram is detected the application captures it and parses out command information.
5. Loki then passes the command requests to the system for execution.
6. Output from command execution is then encapsulated in an ICMP echo reply datagram that is sent back to the originating host.
7. The originating host goes through the process of parsing the received ICMP echo replies and returns the command output to the user's screen (standard out).

As mentioned above, the stings dump information played a big part in my conclusion that the binary was the loki2 tunneling program. The "LOKI2route [(c) 1997 guild corporation worldwide]" seemed like it was a name. To test my hypothesis I entered the word LOKI2 into the Google search engine. The 2,680 hits made clear that the file was known and publicized. The top hit was "Phrack", a known underground e-text magazine for all sorts of interesting computer hacks. Phrack issue 51 discussed the Loki and Loki2 application in great detail and provided me enough information that I was confident that the binary the server portion of the loki2 Trojan.

Forensic details: The loki2 trojan is specifically designed to leave as little of a foot print as possible. This is evident in the way the application works and was designed. Despite the attempts to make the applications as invisible as possible there are still several forensic footprints that are left behind that can allude to the fact that the daemon has been installed and is running on the system.
The first forensic evidence that could be potentially left behind is the loki2 installation files:

L2/Makefile
L2/client_db.c
L2/client_db.h
L2/crypt.c
L2/crypt.h
L2/loki.c
L2/loki.h
L2/lokid.c
L2/md5/Makefile
L2/md5/global.h
L2/md5/md5.h
L2/md5/md5c.c
L2/pty.c
L2/shm.c
L2/shm.h
L2/surplus.c

The above files are included in the Loki2's default tar ball. It is important to mention that these directories and filenames could easily be changed, but if an analyst suspects that Loki2 is potentially on the system this would be a good starting point. Checking deleted inode md5 checksums with the checksums of the above files would be another tactic a forensic analyst should take.

A strace of the application provided some good forensic information on what the binary uses and touches during execution (A complete strace dump is located in Appendix A). Some of the more interesting pieces that were found in the strace are:

rt_sigaction(SIGUSR1, {0x804a76c, [USR1], SA_RESTART|0x4000000},
{SIG_DFL}, 8) = 0
socket(PF_INET, SOCK_RAW, IPPROTO_RAW) = 4

setsockopt(4, SOL_IP, IP_HDRINCL, [1], 4) = 0

The above strace text shows the binary's ability to create raw sockets. This gives the application the ability to create IP headers.

getpid() = 1138

Binary gets a process id of 1138.

write(2, "\nLOKI2\troute [(c) 1997 guild cor"..., 52 LOKI2 route [(c) 1997 guild corporation worldwide]) = 52

The above strace information shows that loki2 is written as output. This also provides evidence as to what the program is.

time([1047223425]) = 1047223425
close(0) = 0
fork() = 1139
[pid 1138] close(4) = 0
[pid 1138] close(3) = 0
[pid 1138] semop(262152, 0xbffff9d0, 2) = 0
[pid 1138] shmdt(0x40014000) = 0
[pid 1138] semop(262152, 0xbffff9c0, 1) = 0
[pid 1138] _exit(0) = ?

The above strace data shows that atd creates a child process "pid id 1139".

Other files that are used by the Loki program include encryption libraries. Depending on how Loki2 is configured forensic evidence of SSLeay or other encryption packages may also be found on the system. An analysis of deleted inodes should be done to determine if there is evidence of encryption software being installed on the system around the same time as the malicious software. A quick review of the system's "message", "syslog" and "history log" should also be done to determine if any encryption libraries have been ftped to the system.

An analysis of all running programs in memory may reveal that the application is running. The loki2 application does show up in a ps-aux command output, though as seen in this example it can easily be renamed as a legitimate binary. An analysis and thorough understanding of all running process should be initiated.

Depending on how the application was configured there may be other evidence left behind when the application is executed. Loki2 has an unusual way of handling the commands that are handed down to the kernel for execution. Loki2 can be configured to use either POPEN or PTYs. If the application is configured to use PTY (pseudo terminal) evidence may be found in the form of numerous program forks. Loki2d forks at least twice on every client request[3]. This in a

[3]quote from http://www.phrack.com/phrack/51/P51-06

way, acts like a memory leak and may leave evidence in the memory and processes.

Program Identification:
A copy of Loki2 was downloaded and extracted from the Phrack website and moved to a testing environment.[4] Attempts to execute the binaries were only done from a controlled testing and analysis environment so there would be no chance of corrupting production data or compromising other network devices.

The testing environment used for analysis of the system consisted of a small isolated network made up of several systems each with specific functions and installed tools. The following provides a breakdown of the systems on this isolated network and their functions:

IBM Intellastation
Processor:1.2 Ghz
Ram: 1GB ram
Capacity: 20GB
Network setup: DHCP
OS: Windows 2000 server service pack 2
The server is configured with DHCP service enabled and has Norton CE antivirus software installed. The server's primary function is to provide ip address and name resolution for the isolated network. The server also acts as a proving ground for the security team's testing of configurations and tools.

IBM clone
Processor: 550mhz
Ram: 256mb
Capacity: 20 GB (2 x 10gb harddrives)
Network setup: DHCP
OS: Winodws professional service pack 2 with security rollup patch.
This system is used for gathering forensic images and testing of security tools. The system is configured with several major applications including Encase 3.19 (forensic imaging and analysis tool), eEye's Iris 3.80.9 (Packet capturing and analysis tool), eEye's Retina Security Scanner 4.8.0 and Norton Antivirus. The system also contains a large assortment of security and system enumeration tools including those discussed on appendix B. This system is frequently rebuilt from an image to ensure the integrity of executables and system files.

IBM clone
Processor: 900mhz
Ram:512mb
Capacity: 10GB
Network setup: DHCP

[4] file site http://www.phrack.com/phrack/51/P51-06

OS: Redhat Linux 7.3
This system is used for the testing and analysis of Unix and Linux based applications and tools. The system is configured with an assortment of network and security related tools including Nessus 2.0.3 (security scanner), Ethereal (packet sniffer and analysis tool), Snort 1.8.5 (light weight intrusion detection system) and tools from the SANS' GCFA cdrom. This system is frequently rebuilt from an image to ensure integrity of executables and system files.

Attempts to compile and execute loki2 source code were at first unsuccessful. The binary indicated that I was missing a required link library needed by the program. The file specified was "ld-linux.so.1". Ld-linux.so.1 is an older Linux library that has since been replaced by ld-linux.so.2. I downloaded a copy of the ld-linux.so.1 library from the Internet and attempted to compile and execute the binary again.

The binary appeared to execute without an issue and returned the following output:

LOKI2 route [(c) 1997 guild corporation worldwide]

I performed a ps –aux which showed that the lokid was in fact running:

root 1018 0.0 0.2 1360 356 ? S 11:48 0:00 ./lokid

The next command I ran was netstat –anp which produced the follow output:

```
Proto Recv-Q Send-Q Local Address       Foreign Address     State       PID/Program name
tcp        0      0 0.0.0.0:32768       0.0.0.0:*           LISTEN      489/rpc.statd
tcp        0      0 127.0.0.1:32769     0.0.0.0:*           LISTEN      789/xinetd
tcp        0      0 0.0.0.0:111         0.0.0.0:*           LISTEN      461/portmap
tcp        0      0 0.0.0.0:21          0.0.0.0:*           LISTEN      789/xinetd
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN      756/sshd
tcp        0      0 0.0.0.0:23          0.0.0.0:*           LISTEN      789/xinetd
tcp        0      0 127.0.0.1:25        0.0.0.0:*           LISTEN      855/sendmail: accep
udp        0      0 0.0.0.0:32768       0.0.0.0:*                       489/rpc.statd
udp        0      0 0.0.0.0:111         0.0.0.0:*                       461/portmap
raw        0      0 0.0.0.0:1           0.0.0.0:*           7           1018/lokid
raw        0      0 0.0.0.0:255         0.0.0.0:*           7           1018/lokid
```

Next the atd binary was executed and netstat –anp was run again. The results show compelling evidence that the executables are one in the same. Both the downloaded loki2 code and the atd binary create the same raw mode network connections. The following shows the netstat output for atd:

```
raw        0      0 0.0.0.0:1           0.0.0.0:*           7           1027/atd
raw        0      0 0.0.0.0:255         0.0.0.0:*           7           1027/atd
```

The next analysis performed was a comparison of the strings information taken from the atd binary and the lokid binary. Diff was used to compare the strings output from atd and lokid (complete string diff information is in appendix A). The results show that both binaries were very similar. One difference between the files is that atd uses lib/ld-linux.so1 and libc.so.5 while the downloaded version of lokid uses /lib/ld-linux.so.2 and libc.so.6. The following is a snippet from the diff dump:

< /lib/ld-linux.so.1
< libc.so.5

> libc.so.6
> /lib/ld-linux.so.2

The differences in the files are most likely contributed to being compiled on different machines and/or with slightly different options at compile time. The differences in the link libraries as shown above, is contributed to a newer version of the sources code than the atd binary.

The keyword “loki” was found in the same locations in the lokid strings dump as in the atd. The String “LOKI2 route [(c) 1997 guild corporation worldwide]” was also found in both string dumps.

The fact that both binaries contain a very high percentage of the same strings information provides compelling evidence that the files are slightly different versions of the same executable.

The next step was to perform md5 checksums on the two files for comparison.

 # md5sum atd
48e8e8ed3052cbf637e638fa82bdc566 atd
#md5sum lokid
b000abaf9af5bfa7d03b15a650c9ce87 lokid

Md5 checksum matches were not expected since the files were not compiled on the same system and with the same options. To understand why these differences occurred it is important to understand how the application is compiled. When “make” is run on the source code of Loki the user must choose whether the code should be configured as linux, openbsd, freebsd, solaris or clean. The source code can also be configured whether to use encryption or not. When the source code is compiled with these different options it pulls information from various libraries and system configuration files. This process makes the compiled binary vary slightly from one system to another.

Legal Implications: Since the file was received as a binary in a Winzip file there is not definitive way to prove that the file was executed on the originating system. If the investigation was conducted on the original system where the binary came

from there is a very good chance that analysis would be able to determine if the binary was executed along with MAC and other information. In this situation we are not able to determine if any laws where broken since we do not know how the file got onto the system and whether it was executed. We can speculate that if the system was intentionally compromised by a hacker, and the hacker had installed the Trojan and in so doing caused damage to the system (greater than $5000), that it would be considered a felony under 18 U.S.C. §1030(a)(5)(A)(i). The act would be a felony regardless of whether it was an outside hacker or a disgruntled employee as long as it can be proven to been done intentionally.

Since we can not conclude that any laws were broken I'll focus on the violation to corporate policies. We can conclude that the file would be in violation of most company's policies. To use my organization as an example, we have stringent policies that prohibit users from downloading and installing executables from the Internet. We have this policy for the specific purpose of avoid unknown binaries from residing and being executed on our production systems. To enforce this policy, the company tracks all binaries that are on production systems. All binaries that are not needed for the system's and user's functionality are removed. Once these steps are down, an image of the system is created and used to build similar systems.

On the people side, we utilize aggressive logging of key system functions and access to ensure that policies are being adhered to. Our company's security team routinely reviews access and system logs looking for inconsistencies. All employees are required to sign an employee handbook and participate in periodic security awareness training. In these classes we reiterate the company's acceptable use policies and solidify the fact that unknown binaries are not be downloaded or executed on production systems.

Interview Questions: The questions I would ask in this situation significantly depend on the type of incident, the incident circumstances and the person being questioned. If the suspect that is being questioned is expected of installing and using the application for malicious purposes I would gear my attitude and questioning toward proving that he/she was the person to execute the program and attempt to gain how they did it. If the person being questioned was simply social engineered into running the application I would gear my questioning toward how they received the app, why they installed it, and exactly what steps they took. Assuming that I'm questioning a malicious user suspected of installing and executing the application I would take the follow preparation steps and ask the following questions:

Preparation steps:

1. The first thing I would do is prepare the information that I already have and structure it in a way that will allow me to ask questions that will be meaningful and concise. I want to be able to confirm the things I think I know, and get

answers to the things I don't know. Interviewing is an art and takes lots of practice to get right. The interviewer must plan ahead as much as possible, but also must be able to build affective questions from answers given by the interviewee.

2. My next preparation step would be to determine the best way to gain some of the interviewees trust. To do this I would try to sympathize with the person. Let them know I understand where they are coming from. This can be very valuable and can help the interviewee create an "acceptable rationalization[5]". If done correctly this process can help the interviewee through a confession process.

3. Prepare open ended questions to be asked. I would do this in the most non-accusing fashion as possible. It has been my experience that people being questioned are much more open to answering questions if they think they are not suspected of anything and are simply being questioned for help in resolving a problem.

4. Questions I would start off with would be qualifying questions such as "what is your job here"? How long have you been in your position? Who are the people you work with? How do you think things are going with the company? These questions are meant to get information about the person, but at the same time they are meant to relax and start a rapport with the person.

5. The next phase of questions would dig a little bit deeper such as, What hours do you work? Do you have a VPN/dialup id? How often do you login from home? What access do you have? These questions are geared towards answering the investigation questions, but at the same time seeming innocent as possible.
6. As the questioning continues I would start to get admission to general things and work up to more serious issues. This type of questioning gets the interviewee into the frame of mind of admitting to some things. This is progressively built upon, while continually reassuring the person that you are on their side and simply want to get to the bottom of the problem.

Example questions:
1. I noticed that you like to test security applications and tools. I like to keep on top of the latest exploits and tools too. I see that you were testing with a tunneling program called Loki. How did it go? Were you able to get it working correctly?

2. I know that you sometimes have to go around the system to get things done, like using the NOC's root account when they aren't available. There's nothing really wrong with that, you were just trying to get the job done right?

[5] The Kubark Interrogation Manual http://www.parascope.com/articles/0397/kubarkin.htm

3. I know that you are required to connect remotely sometimes to get work done. Did you install Loki to test its remote control capabilities?

4. My boss wants this matter cleared up as soon as possible so security doesn't have to get involved. I don't want this to go any farther. Will you help me help you by telling me everything that was done?
5. I know that you sometimes test the security of our internal systems. Is this what you were trying to do with Loki? How exactly does it work?

Additional Information: The following are some good links for additional information on the Loki tunneling program and other forensic practices that I used for this section of the paper.
Loki source code, usage and functionality
http://www.phrack.com/phrack/51/P51-06

ICMP attacks and applications
http://rr.sans.org/threats/ICMP_attacks.php

ICMP tunneling article
http://www.networkmagazine.com/article/NMG20000515S0048

IDS signatures and information about ICMP attacks
http://www.shmoo.com/mail/fw1/mar01/msg00042.shtml

Forensic interrogation practices
http://www.parascope.com/articles/0397/kub_ix.htm

MAC time resources
http://www.cert.org/security-improvement/implementations/i046.01.html

Strings command references
http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/cmds/aixcmds5/strings.htm

Part II – Option 1: Perform Forensic Analysis on a System

Synopsis of Case Facts -
On May 8th, 2002 the PC maintenance techs received a Think pad 600 laptop running Windows 2000 server from a corporate web developer. The developer said that the machine was his old production laptop and was being used as a testing server and developing machine. The developer also stated that the laptop did not have a company system image and he frequently transported the machine between his office and home.

The developer complained that the laptop was not working correctly and was acting oddly. He also mentioned that the laptop seemed to be running considerable slower than expected. When technicians questioned the developer on the specifics of the problem, the developer said that he thought there may be corrupted system files or a virus, since he was noticing unusual activity and changes that he didn't remember making. After gathering administrator password information the PC maintenance techs issued the developer a different laptop and place the developer's old laptop in there equipment locker.

On May 13th, 2002 PC maintenance techs contacted the company's Security Operations team and informed them about the laptop and the situation surrounding it. The laptop was picked up and signed for that day by the security operations team. Since the laptop was not a production machine and was not considered a threat, it was secured in a storage locker until time could be allocated to inspect the system.

The storage locker has a sign-in/sign-out sheet that must be filled out each time something is added or removed from storage. The sheet requires times, dates, description of action performed, and initials of person performing the actions. This chain of custody process is enforced and documented in our company's policies. All equipment received from the PC maintenance techs was signed-in on May 13th, 2002.

The laptop would remain untouched until Oct 11th, 2002 when a junior member of the Security Operations team signed-out the laptop. The junior analyst powered on the system, login as administrator and reviewed the laptops configuration (evidence of these actions is seen in the system's security logs and is discussed later in the paper). The junior analyst concluded that the laptop showed potentially malicious processes and accounts on the system. At this point the system was shutdown for later inspection and formally labeled with case id # 101203-02. The laptop was placed back in the storage locker and required sign-in information was documented. I received initial information about the system during a team meeting and thought it could be a potential "compromised host" for my GIAC practical. I signed-out the system on Dec 2nd, 2002 to perform a forensic analysis.

When I received the system, my first thoughts were to get as much information from the original system owner as possible. Since the laptop wasn't being used as a production system and didn't have an organization approved build I wanted to gather as much detail about how the system was configured as I could. My main concerns were around what applications, accounts, and services were installed on the system. I know these pieces of information could prove invaluable and dramatically limit the amount of time it would take for me to determine if the system was compromised, had a virus, or simply had an application that was causing problems. My attempts to contact the original owner and glean valuable information turned out fruitless since the original owner was

no longer with the company. Other attempts to gain information about the system from remaining members of the development team also failed to provide meaningful results.

Unfortunately, I was not available when the original analyst reviewed the system. Since the company didn't have any intention of pursuing legal action in this instance and the state of the machine was unknown; I made the decision to start the computer and determine if the box did indeed show signs of compromise or malicious use and if it would be suitable for my practical. (**I was aware that this could potentially change valuable data, but I needed to determine the state of the machine and its potential value as a compromised system to use for my practical. The restarting of a system should never be done in a real investigation**. **As Robert Lee says, "Some times you have a powered off computer and have to make a choice, evidence a 40 gigabyte hard drive or power on to verify an incident before you spend hours backing up a system that really isn't involved in an incident anyway. Touch choices."**)

My first step was to take a preliminary look at the system while manipulating as little data as possible. The machine was placed in a non-production testing environment where it could be analyzed without the fear of it affecting other network devices. (The same isolated non-production testing environment that was discussed earlier in the paper was used for this part of the investigation.)

The laptop was network enabled, but was not connected into the network at this time. In order to record and collect as much information as possible, I used a hardback notebook to take notes as I went through the investigation. All members of the Security Operations Team are given hardback notebooks because they provide a bit more validity and integrity if used as evidence in a case. Hardback note books have threaded pages. It is easy to determine if pages have been removed from a hardback notebook, as opposed to ring notebooks where pages can easily be removed with no evidence of tampering.

In an attempt to plan ahead a bit, I contacted the PC maintenance techs for a spare PCMCIA NIC card that is distributed with the model of laptop being investigated (3com model 3CCE589ET 10/100). I wanted this in the event that I needed to connect the system to the test network for investigation. The laptop does not have a built-in network card and did not come with one when it was originally received from the PC maintenance techs. I did not want to put a different make/model of network card into the laptop as I didn't want to have to install and configure software on the system. Doing so could alter valuable system data unnecessarily.

I started the laptop and immediately went into the system's bios by press "F1" as soon as the system started to boot. This allowed me to get detailed bios information off the system including bios part number, system unit serial number, system board serial number, time & date information and network wake on LAN

configuration. The following table details the specifics that were gleaned from the system's bios:

Description	Value
Bios part # and date	97H4112, 06/23/98
System-unit Serial #	264551U78HN950
System board serial	J16QR5981FS
Micro Processor	Pentium II 266mhz
Bios date	12/3/2002
Ram Installed	163840KB
Ram Usable	163264KB
Network Wake on LAN	Enabled

Information gathered from the bios can be very valuable since information such as the system unit and system board serial numbers are burned in by most manufactures and can not be changed. This provides an iron clad way of identify and tracking a system, unlike physical casing serial numbers which can be scratched off or replaced.

My next step was to allow the system to boot normally. As the system started to boot it went into the Windows NT selection screen showing that Windows 2000 Advanced server was installed on the system. I logged in to the system as administrator and conducted a preliminary view of the applications that were installed on the system and those that started automatically. In order to manipulate as little data as possible I refrained from executing any programs. As soon as I logged in the "Windows 2000 configure your server" wizard popped up along with "Yahoo! Messenger". In the box "Yahoo ID" an apparent id "rbadg" was displayed. A comparison of the bios time and windows system time was consistent. Other programs that appeared to be running in the system tray included one called "Net.medic", volume control, and Microsoft's hardware ejection wizard. A view of my computer showed that the C drive was 1.95 gigabits formatted as NTFS and the D drive was 1.86GB and was unformatted space. The two partitions made up the entire capacity of the hard drive.

In order to confirm the findings of the junior security analyst, and to determine if there was any validity to the notion that the system had been compromised I wanted to perform specific discovery tasks. I first pressed ctr+alt+delete to engage the task manager and to view the applications and processes that were running. The following table lists the processes that were found running.

Image Name	PID	CPU	CPU time	Memory Usage
svchost.exe	472	0	0:00:01	3,332K
svchost.exe	516	0	0:00:00	5,376K
mwmdmsvc.exe	564	0	0:00:00	1,500K
mwssw32.exe	588	0	0:00:00	4,244K

msdtc.exe	612	0	0:00:00	5,168K
LLSSRV.exe	756	0	0:00:00	2,224K
regsvc.exe	796	0	0:00:00	884K
WinMgmt.exe	920	0	0:00:00	148K
dfsscv.exe	956	0	0:00:00	1,420K
inetinfo.exe	976	0	0:00:00	1,892K
syshook.exe	1112	0	0:00:00	728K
fastfindeng.exe	1184	0	0:00:00	1,892K
docmanager.exe	1200	0	0:00:00	2,748K
Tp4mon.exe	1204	0	0:00:00	1,056K
netMedic.exe	1220	0	0:00:00	3,742K
Ypager.exe	1228	0	0:00:00	5,552K
svchost.exe	1244	0	0:00:00	3,568K
explorer.exe	1364	0	0:00:20	3,604K

At first glance I was able to identify what most of the processes running were. There were a couple processes that I wasn't sure about and thought warranted additional scrutiny. These were:

syshook.exe
fastfindeng.exe
docmanager.exe
Tp4mon.exe

Next I opened event viewer and looked at the security, application and system event logs. At first glance nothing seemed to standout as unusual or malicious activity. From previous experience of looking at NT log files, I could tell that the system wasn't setup to conduct proper logging and that the auditing policies were for the most part system defaults. At this time I was not able to determine if the auditing settings were setup this way when the system was originally built or if they were changed at a later date.

My next step was to look at user accounts that exist on the laptop. The driving factor for doing this was to look for accounts that look as though they do not belong on the system, specifically user accounts that belong to the administrator's group. (Accounts that exist in the administrator's group have complete control over the system and are the typical target for malicious users.) To do this I opened "computer management" from "administrator tools" then opened the "Local Users and Groups" followed by the "Administrator" group. Three accounts existed in the administrators group:

Administrator
rbadg
supportadmin

One seemed unusual, "support admin". Since this machine was not running a company approved OS build and was not configured to company standards, I wasn't sure if the account was added by some application or added as part of some development application. Regardless, I felt that between the unusual

processes and the accounts I had enough information to warrant conducting a complete investigation of the system.

System being analyzed –
The system being analyzed is an IBM Thinkpad 600 series laptop. The system is a company purchased laptop that was originally configured with Windows NT, but was reconfigured with windows 2000 server. When I received the laptop it had all its standard parts, but did not have a network adapter (it was probably kept, by the original user for a different laptop). The laptop physically appears to be in good working order.

Hardware –
The following items were received from the Security Operation's storage locker and tagged as evidence on 12/03/02:

Tag #'s	Description	Serial #
010603-00	IBM DTCA-24090 4GB hard drive	K34V9327
010603-01	IBM thinkpad 600	78-HN950
010603-02	IBM thinkpad 600 external floppy	10502956
010603-03	IBM thinkpad 600 Power adapter	J14FQ510AT0
010603-04	Toshiba cd-rom XM-1702BC	8X7V605128
010603-05	IBM thinkpad 600 series battery Li-Ion	J15VD5567GS

The laptop has integrated video, sound and 56.6k modem. (A 3Com PCMICA 10/100 network card was signed out from Company's storage.)
The following are several images taken of the main pieces of the laptop. The images show serial numbers and illustrate system's physical condition. (Some information has been blanked out to protect the company.)

*Company proprietary information has been masked.

Evidence Gathering –

Now that I had reason to suspect that the system may have been compromised; my first objective was to ensure that I didn't chance any information on the system. I also wanted to get a complete image of both the system's drive and memory. The tactic I decided to use was to connect the laptop to the isolated testing and forensic network. This was done to provide a fast means of moving forensic data to the analysis machine while not further manipulating the data on the laptop.

To ensure that I didn't cause further damage to the system or use trojan applications I used a cdrom with a collection of dos forensic commands including those contained on the SANS' forensic cdrom (see appendix B for complete list of tools and corresponding MD5checksums). Using the tools from a cdrom prevents commands from being overwritten by viruses or trojaned applications that may be running in memory.

I plugged the NIC card into the laptop and connected it to the isolated network.
From the cdrom I started a command window with the CD's "cmd.exe."
From the command window I typed "ipconfig /renew" to gain an ip address.
Next I used the "net" command from the cd to connect to the forensic workstation's d$ share. This was done to provide a storage ground for output of the evidence gathering commands. This was also done because one particular tool, the Incident response collection reporting tool (IRCR), does not support server share naming.

```
E:\evidence gathering tools\response_kit\win2k_xp\net use * \\192.168.1.104\d$
Drive F: is now connected to \\192.168.1.104\d$
The command completed successfully.
```

My next step was to gather volatile memory from the system. To do this I used the Windows port of the "dd" command from my forensics cdrom to dump the system's ram to the mapped drive. The dd command is a great tool that is capable of copying raw data from one place to another. Dd is capable of copying

a single file, partitions, logical drives, memory and swap files. Dd also has built in integrity checking which can generate md5 checksums for input and output data. This is an important feature and helps illustrate and prove that the output data is an exact replica of the data being imaged. For gathering the memory from the laptop I used the dd command as follows:

```
E:\evidence gathering tools\response_kit\win2k_xp>dd if=//./PhysicalMemory of=f:
\101203-02_memory.dmp --md5sum --verifymd5 --md5out=f:\memorymd5.dmp
Forensic Acquisition Utilities, 3, 16, 2, 1029
dd, 3, 16, 2, 1029
Copyright (C) 2002 George M. Garner Jr.

Command Line: dd if=//./PhysicalMemory of=f:\ 101203-02_memory.dmp --md5sum --verifymd5 -
-md5out=f:\ 101203-02_memorymd5.dmp
Based on original version developed by Paul Rubin, David MacKenzie, and Stuart Kemp
Microsoft Windows: Version 5.0 (Build 2195.Professional Service Pack 2)

03/12/2002  16:15:55 (UTC)
03/12/2002  11:15:55 (local time)

Current User: NE-PRODUCTION-T \administrator

Total physical memory reported: 523184 KB
Copying physical memory...
E:\evidence gathering tools\response_kit\win2k_xp\dd.exe:
      Stopped reading physical memory:

The parameter is incorrect.
\13b091b78e2756edb471c18c41054045 [\\\\.\\PhysicalMemory] *f:\\  101203-02_memory.dmp

Verifying output file...
\13b091b78e2756edb471c18c41054045 [f:\\memory.dmp] *f:\\ 101203-02_memory.dmp
The checksums do match.
The operation completed successfully.

Output c:\memory.dmp 536211456/536211456 bytes (compressed/uncompressed)
130911+0 records in
130911+0 records out
```

*note: The “Parameter is incorrect” message seen in the above screen dump is a normal (benign) message and is expected. It does not refer to integrity of the data or an incorrect setting. The message is received during normal operation and is generated by an offset of the memory being read going beyond the range of addressable memory.

Once this was done I ran an assortment of tools to collect system information, configuration settings, and volatile data. The files were run from the forensic tool cdrom and were configured to dump to the share drive that had already been configured. The following will provide a description of what each tool does and how it was executed (outputs and screenshots of the commands will be discussed later in the paper).

The first tool I used is called pslist.exe. Pslist is a System Internal’s tool that provides a dump all the processes that are running on the system. Pslist also

provides a wealth of other information including PID (process ID), priority, thread, and memory usage statistics. This data can be very useful in determining if there are rogue processes or applications that are using a significant amount of the system's resources. The command was executed as follows:

```
Pslist >> f:\pslist_dump.txt
```

The next tool I ran is called "fport.exe". Fport is a utility created by Foundstone which maps processes to tcp/udp port numbers. This comes in very handy when attempting to determine ports that are being used running processes. Additional information about fport can be received at www.foundstone.com The command was run as follows:

```
Fport >> f:\fport_dump.txt
```

After running fport I ran a tool called "listdlls.exe". Listdlls is another System Internals tool which enumerates all DLLs that are loaded by a process. The value that this provides is a detailed list of files that are being used by an executable. The output also provides information such as dll version number, and path to the dll. Listdlls was executed as follows:

```
Listdlls >> f:\listdlls_dump.txt
```

Next I ran "psservice.exe". Psservice is another System Internal's tool which provides detailed local and remote service information about a target system. One nice benefit of this tool is that it provides descriptive information about a service's functionality alone with its state and its configuration. The command was executed as follows:

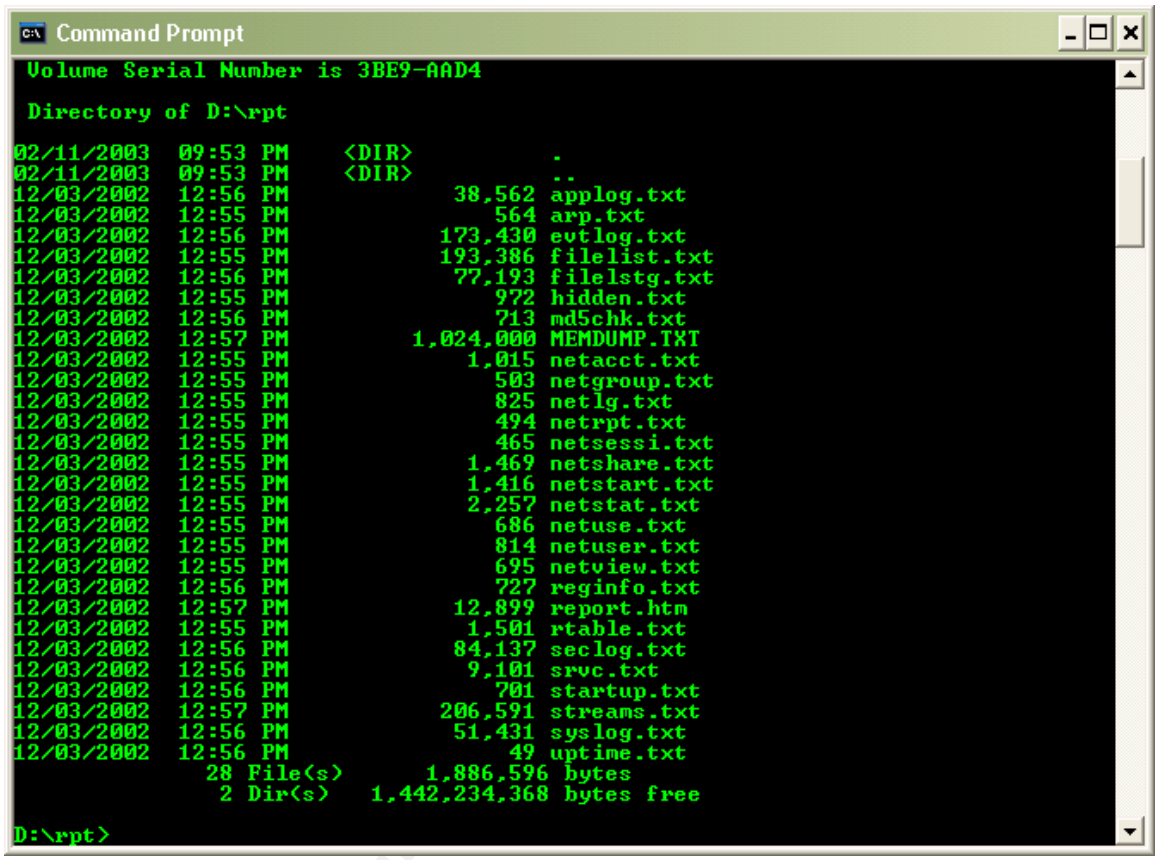
```
Psservice >> f:\psservice_dump.txt
```

Next I used the Incident response collection reporting tool (IRCR). This tool is a powerful collection of system utilities that have been wrapped up into a perl executable. The tool polls a myriad of system vital signs, configuration and statistics. When the tool is complete it provides a user friendly html page with links to the pertinent information. Some of the essential pieces of information the tool pulls includes:

Accounts
groups
Log files
Shares
Local network device
Registry info
Start up files
Alternate data streams
Uptime
Services

File listings
General network configurations

The follow is a screen shoot of the files created by IRCR and their creation date and time:



*Screenshot taken from system which IRCR data was directed to

More information about the findings from the IRCR and the previous commands will be provided later in the paper. With the physical memory dump and the information gathered from the IRCR tool, I had enough information to shutdown the machine and image the drives.

*(The decision to shutdown the system for future imaging was driven by work related factor and lack of corporate support for an investigation on this system. Under normal circumstances this would **never** be done! A more appropriate solution for this situation would have been to continue to use “dd” and the existing net share to the forensic machine or use a tool like Forensic Netcat. Examples of how this can be done are provided at the end of the imaging section.)

Because of other work assignments and the fact that my company did not see this investigation as a critical endeavor I would not get the chance to continue

working on the imaging and investigation of the system for several weeks. The laptop, harddrive and other pieces of the system being investigated were signed back into the storage locker until I could continue working on them.

Imaging of Media –
I signed-out all the laptop hardware on Jan 27th, 2003 at 4:20pm.
In order to preserve the data on the hard drive as best as possible, I wanted refrained from touching any additional data on the system until I had a complete image of the partitions from the drive. I removed the laptop hard drive and physically mounted it into another machine that is used for analysis and imaging.

The Analysis machine used to perform the imaging is a PC clone running Windows 2000 Professional service pack 2. The system has an Intel 550mhz processor and 256megs RAM. This forensic system has 2, 10 GB, 7200 rpm drives. The first drive contains the operating system and an array of system and forensic tools. The second hard drive is used to hold forensic data. All system executables and forensic tools that exist on the system are periodically checked against a cdrom containing md5 checksums. This is done to ensure the integrity of the system executables and installed forensic tools. Another reason the imaging was done on this machine was because it has an adapter that converts laptop 2.5" hard drives to standard IDE.

The following is a screen dump of the commands that were used to perform the imagining of the drive and to ensure data integrity. MD5checksum verification was used to ensure that the images made are identical copies of the imaged drive partitions:

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>cd zip\temp

C:\zip\temp>dd if=\\.\h: of=c:\101203-02_c-drive.img --md5sum --
verifymd5 --md5out=c:\101203-02_c-drive.md5
Forensic Acquisition Utilities, 3, 16, 2, 1029
dd, 3, 16, 2, 1029
Copyright (C) 2002 George M. Garner Jr.

Command Line: dd if=\\.\h: of=c:\101203-02_c-drive.img --md5sum --
verifymd5 --md
5out=c:\101203-02_c-drive.md5
Based on original version developed by Paul Rubin, David MacKenzie, and
Stuart Kemp
Microsoft Windows: Version 5.0 (Build 2195.Professional Service Pack 2)

28/01/2003  04:38:16 (UTC)
27/01/2003  23:38:16 (local time)
```

```
Current User: VDC30667\bbowers

Statistics for logical volume \\.\h:
               524292096 bytes available
               524292096 bytes free
               2097381376 bytes total

Volume Name:            \\.\h:
Volume Label:
Drive Type:             fixed
Volume Serial Number:           6E46-461A
Maximum Component Length:       255
Volume Characteristics:

                        File system preserves case
                        File system supports case sensitive file names
                        File system supports Unicode file names
                        File system preserves and supports persistent
ACL's
                        File system supports file level compression
                        File system supports named streams
                        File system supports encryption
                        File system supports object identifiers
                        File system supports reparse points
                        File system supports sparse files
                        File system supports quotas
File System:            NTFS
Clustered:              No

Volume Extents:

        Disk Number:            1
        Starting Offset:        0x0000000000007e00
        Extent Length:          0000002097381888
Copying \\.\h: to c:\101203-02_c-drive.img...
\dfa54408ab09651b7c9dd5f85548097b [\\\\.\\h:] *c:\\101203-02_c-
drive.img

Verifying output file...
\dfa54408ab09651b7c9dd5f85548097b [\\\\.\\h:] *c:\\101203-02_c-
drive.img
The checksums do match.

Output c:\101203-02_c-drive.img 2097381376/2097381376 bytes
(compressed/uncompressed)
512056+0 records in
512056+0 records out


C:\zip\temp>dd if=\\.\i: of=c:\101203-02_d-drive.img --md5sum --
verifymd5 --md5out=c:\101203-02_d-drive.md5
Forensic Acquisition Utilities, 3, 16, 2, 1029
dd, 3, 16, 2, 1029
Copyright (C) 2002 George M. Garner Jr.
```

```
Command Line: dd if=\\.\i: of=c:\101203-02_d-drive.img --md5sum --
verifymd5 --md5out=c:\101203-02_d-drive.md5
Based on original version developed by Paul Rubin, David MacKenzie, and
Stuart Kemp
Microsoft Windows: Version 5.0 (Build 2195.Professional Service Pack 2)

28/01/2003  05:00:45 (UTC)
28/01/2003  00:00:45 (local time)

Current User: VDC30667\bbowers

Statistics for logical volume \\.\i:
               1988229120 bytes available
               1988229120 bytes free
               2002419712 bytes total

Volume Name:            \\.\i:
Volume Label:
Drive Type:             fixed
Volume Serial Number:           DA70-70A6
Maximum Component Length:       255
Volume Characteristics:

                        File system preserves case
                        File system supports case sensitive file names
                        File system supports Unicode file names
                        File system preserves and supports persistent
ACL's
                        File system supports file level compression
                        File system supports named streams
                        File system supports encryption
                        File system supports object identifiers
                        File system supports reparse points
                        File system supports sparse files
                        File system supports quotas
File System:            NTFS
Clustered:              No

Volume Extents:

        Disk Number:            1
        Starting Offset:        0x000000007d047e00
        Extent Length:          0000002002420224
Copying \\.\i: to c:\101203-02_d-drive.img...
\5854695e5e7e7eb8ab03a73a0c21de7d [\\\\.\\i:] *c:\\101203-02_d-
drive.img

Verifying output file...
\5854695e5e7e7eb8ab03a73a0c21de7d [\\\\.\\i:] *c:\\101203-02_d-
drive.img
The checksums do match.

Output c:\101203-02_d-drive.img 2002419712/2002419712 bytes
(compressed/uncompressed)
488872+0 records in
488872+0 records out
```

MD5 checksum outputs prove that the images are identical copies of the drive partitions. The checksum also proves that the data was not manipulated or changed in anyway.

MD5checksums of the partitions:
```
\dfa54408ab09651b7c9dd5f85548097b C:
\5854695e5e7e7eb8ab03a73a0c21de7d D:
```

MD5checksums of the image files:
```
\dfa54408ab09651b7c9dd5f85548097b C:
\5854695e5e7e7eb8ab03a73a0c21de7d D:
```

The original hard drive was removed from the forensic machine and was placed back in the storage locker along with the other items that were labeled as evidence on Jan 28th, at 8:11am.

*(As discussed previously this was not the normal corporate approved process for imaging the drive. The above discussed steps were taken because the investigation was not sanctioned by the company and therefore didn't warrant the time and use of company resources. Under normal circumstances a live system would not have be shutdown and the drive(s) would have been imaged at the moment the system was considered potentially compromised. A more effective way to image the drives would have been to continue using the previously established net share drive before the system was shutdown. Tools such as "dd" or Forensic Netcat could have been used to perform the imaging.

The following examples are provided to demonstrate how the image could have been done using "dd" and Forensic Netcat:
Using the "dd" command and the established network share a forensically sound image of the drive could have been performed by using the same method used in the collection of the physical memory. This would create a complete image of the drive while maintaining data integrity. This process would also allow for MD5sums of the image to be made and verified. The following is an example of how the command could be run:

```
E:\evidence gathering tools\response_kit\win2k_xp>dd if=//./c:
of=f:\101203-02_c-drive.img --md5sum --verifymd5 --md5out=c:\101203-
02_c-drive.md5
```
In this example "f:\101203-02" represents the network share and file name that the dd image will be outputted to. This process also creates a md5sum of the image and verifies it.

Forensic Netcat could have also been used for creating the images. Forensic Netcat works in much the same way as the "dd" command except it has the ability to write to raw socket connections. Raw socket connections are established TCP network connections. This allows the tool to direct the dd image bit stream to a specified network devices such as another machine. Forensic

Netcat has many of the same integrity features as the “dd” command including the ability to lock file from changing and performing md5sums. An example of how Forensic Netcat could have been used in this situation is:

```
d:\>nc –v –n –l –p 5050 –k md5 --verify –O 101203-02.img
```

This command would be run on the system that will be storing the forensic image. The command configures the system to actively listen on port tcp/5050 for connections and data transmission. The included command switches configure the application to provided verbose output, generate and verify md5sum data and direct the bit stream image to a file called “101203-02.img”. In order for this part of Forensic Netcat to work it must have another command run on the system which the data to be imaged resides. The function of the command is to transmit via network connection, all the data to be imaged. An example of the command would be:

```
E:\evidence gathering tools\response_kit\win2k_xp>nc –v –n –I \\.\c:
192.168.1.104 5050
```

This command instructs Forensic Netcat to perform a dd image of the system’s C: drive and send it via network connection to 192.168.1.104 over port tcp/5050.

The two described Forensic Netcat commands work in unison with each other. The first command listens for incoming dd image data while the other command collects the data and performs a md5sum on it.

The above described solutions would have allowed dd imaging of the system’s drive without having to chance manipulating data by shutting down the machine and connecting the drive to another system.)

Media Analysis of System – (Operating System/Configuration/Back doors)

Media analysis of the system was done from the images that were made from the original hard drive partitions and data collected from the system when it was live. As stated earlier, md5sums were done of the images to ensure that I was working on identical copies of the system partitions. My first step in analyzing the collected data was to go through the IRCR report and other previously collected data and see if there were any tidbits of information that would help focus where I should start looking for abnormalities.

The first files analyzed were system files that would provide general information about the system and its structure. The following is a dump of some of the key information provided on the main report screen of IRCR:

Caption: Microsoft Windows 2000 Advanced Server
Manuf: Microsoft Corporation
BootDevice: \Device\Harddisk0\Partition1
System Dir: C:\WINNT\System32
Organization:

BuildNum: 2195
Build: Uniprocessor Free
Version: 5.0.2195
CSDVersion: Service Pack 2
Locale: 0409
WinDir: C:\WINNT
TotMem: 163184 bytes
SerNum: 51879-000-0000007-05097
Windows 2000 IP Configuration
Host Name . . . . . : ne-production-t
Primary DNS Suffix . . . . . :
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . :
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . :
Description . . . . . : 3Com Megahertz LAN PC Card (589E) (Ethernet)
Physical Address. . . . . : 00-01-02-F8-4B-93
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.104
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.100
Lease Obtained. . . . . : Tuesday, December 03, 2002 11:07:37 AM
Lease Expires . . . . . : Wednesday, December 04, 2002 11:07:37 AM

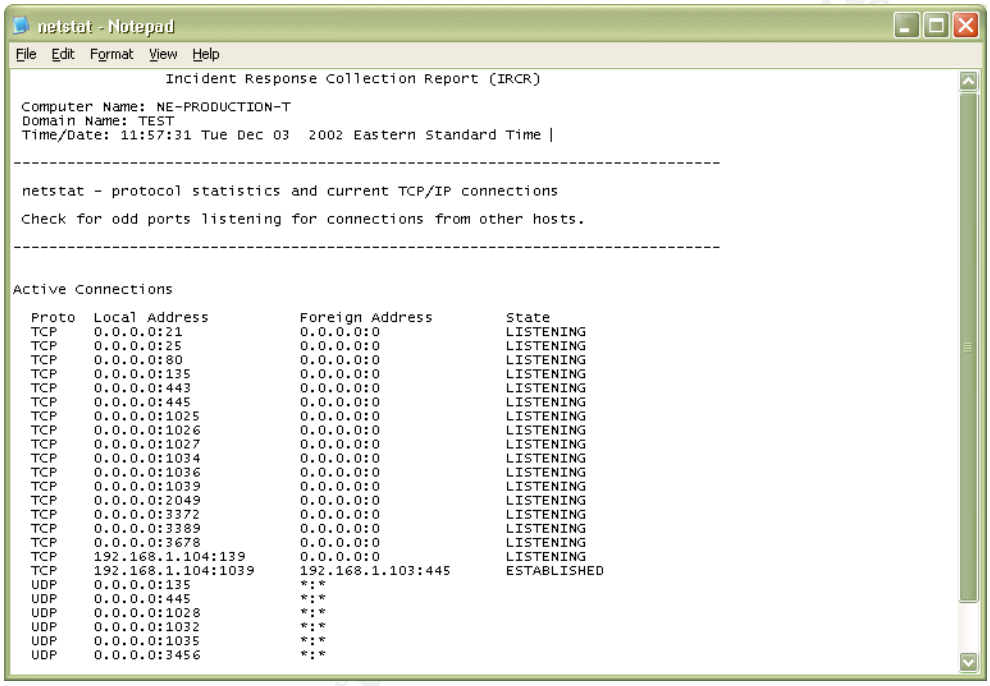
The above screen dump provides a wealth of information about the system and it configuration. Some of the key pieces of information this provides is OS, system build, service pack levels, system software serial number, and hardware information such as boot device and memory. While this data doesn't go a long way in telling what could be wrong with the machine it does provides background information and helps determine next course of action.

Next, I proceeded to review the file structure of the system looking for data streams, hidden files and unusual executables. As part of its collection, ICRC collects all these pieces of information. I reviewed the ICRC file called streams.txt. This file contains all the data streams that are contained on the system. Alternate data streams are a poorly documented feature that exists in NFTS file systems to support Macintosh files. Alternate data streams are an excellent place to store malicious information since they are virtually invisible to the filesystem and special software is required to detect them.
The ICRC streams.txt file should that there were no alternate data streams found on the system.

I proceeded to analyze the hidden.txt file which contained all the hidden files stored on the system. Many files are hidden by the system automatically. This is done to protect important system files from accidental deletion or corruption. In my analysis of the system's hidden files I was looking for apparent malicious executables or suspicious log files. My analysis of the hidden files did not reveal

any files that where obviously malicious. Further I didn't find any file MAC times that seemed obviously out of place.

My next step was to review the Netstat.txt. Netstat is a tool that gathers all the active connections and listening ports on a host. In this file I was looking for any unusual ports that were listening for connections. Unusual ports listening for connections could be an indication of viruses or Trojan software. The difficulty here is that many applications will use random high ports (port numbers over 1024) and it is difficult to determine which application they are tied to. The following shows the text that was collected from the netstat command:



Most of the ports I was able to immediately identify as typical server system ports (21/ftp, 25/smtp, 80web, 443/https, 135/netbios, 3389/Terminal services, etc.), though I was keeping in mind that the ports could easily be utilized by other malicious applications. An example would be configuring a Trojan application to use port tcp/443. This port is usually used by HTTPS, but if the server doesn't have https service enabled the port could easily be commandeered by a malicious application. This may appear by someone unfamiliar with the box as simply https services running on the box and not raise any flags.

There were a couple ports that I was unable to readily identify so I used a port lookup site at http://www.treachery.net/tools/ports/lookup.cgi to gather more information about the ports. The site performs a database search based off the provided port number and protocol types selected. I used the lookup tool for TCP ports 2049,3678, 1027 and UDP port 3456. The below table shows the output the database retrieved for these ports.

Protocol	Port#	Description

TCP	2049	NFS – shilp
TCP	3678	Unknown port
TCP	1027	ICKiller Trojan
UDP	3456	Vat default data

The port lockup tool provided some interesting information. Ports tcp/2049 and udp/3456 are most commonly used by Unix based systems. Since this was an NT box, the results raised an eyebrow. The other two port tcp 3678 & 1027 also seem to be alarming. Tcp port 1027 is the common port used by a Trojan application called ICKiller. While I wanted to be sure that I thoroughly checked what each of these ports was being used for, I also wanted to keep in mind that many Windows based applications pick high ports at random for everything from netbios connections to temporary DNS communication ports. To dig deeper into the functions behind the ports I next reviewed the fport and psservice data that was collected.

The following is a screen dump of the data collected from fport:

```
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process          Port  Proto Path
976   inetinfo      -> 21    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
976   inetinfo      -> 25    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
976   inetinfo      -> 80    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
472   svchost       -> 135   TCP   C:\WINNT\system32\svchost.exe
8     System        -> 139   TCP
976   inetinfo      -> 443   TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
8     System        -> 445   TCP
612   msdtc         -> 1025  TCP   C:\WINNT\System32\msdtc.exe
812   MSTask        -> 1026  TCP   C:\WINNT\system32\MSTask.exe
252   services      -> 1027  TCP   C:\WINNT\system32\services.exe
976   inetinfo      -> 1034  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
8     System        -> 1036  TCP
8     System        -> 1039  TCP
1200  docmanager    -> 2049  TCP   C:\WINNT\docmanager.exe
612   msdtc         -> 3372  TCP   C:\WINNT\System32\msdtc.exe
384   termsrv       -> 3389  TCP   C:\WINNT\System32\termsrv.exe
976   inetinfo      -> 3678  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe

472   svchost       -> 135   UDP   C:\WINNT\system32\svchost.exe
8     System        -> 137   UDP
8     System        -> 138   UDP
8     System        -> 445   UDP
264   lsass         -> 500   UDP   C:\WINNT\system32\lsass.exe
252   services      -> 1028  UDP   C:\WINNT\system32\services.exe
252   services      -> 1032  UDP   C:\WINNT\system32\services.exe
976   inetinfo      -> 1035  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe
976   inetinfo      -> 3456  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe
```

Fport provided me more detail around what was using the unidentified ports. After asking several questions to the company's NT gurus and reviewing the fport

data I was able to determine that udp/3456 is commonly seen on Windows 2000 servers. As seen above udp/3456 is tied to the inetinfo.exe process. I validated this against several other systems running NT advanced server and found that the inetinfo.exe quite commonly grabs udp/3456 as its port. Another one of the unknown ports that I felt more comfortable with was tcp/3678. Tcp/3678 as shown above is associated with inetinfo.exe. This is most likely the random high port that is being used by the administrative webadmin site. Although I felt more comfortable about these ports I still wanted to keep them in mind since it was possible that they were some form of trojanized application that is setup to look like a legitimate service.

The other two ports tcp 2049 and 1027 were still a bit of a mystery at this point.

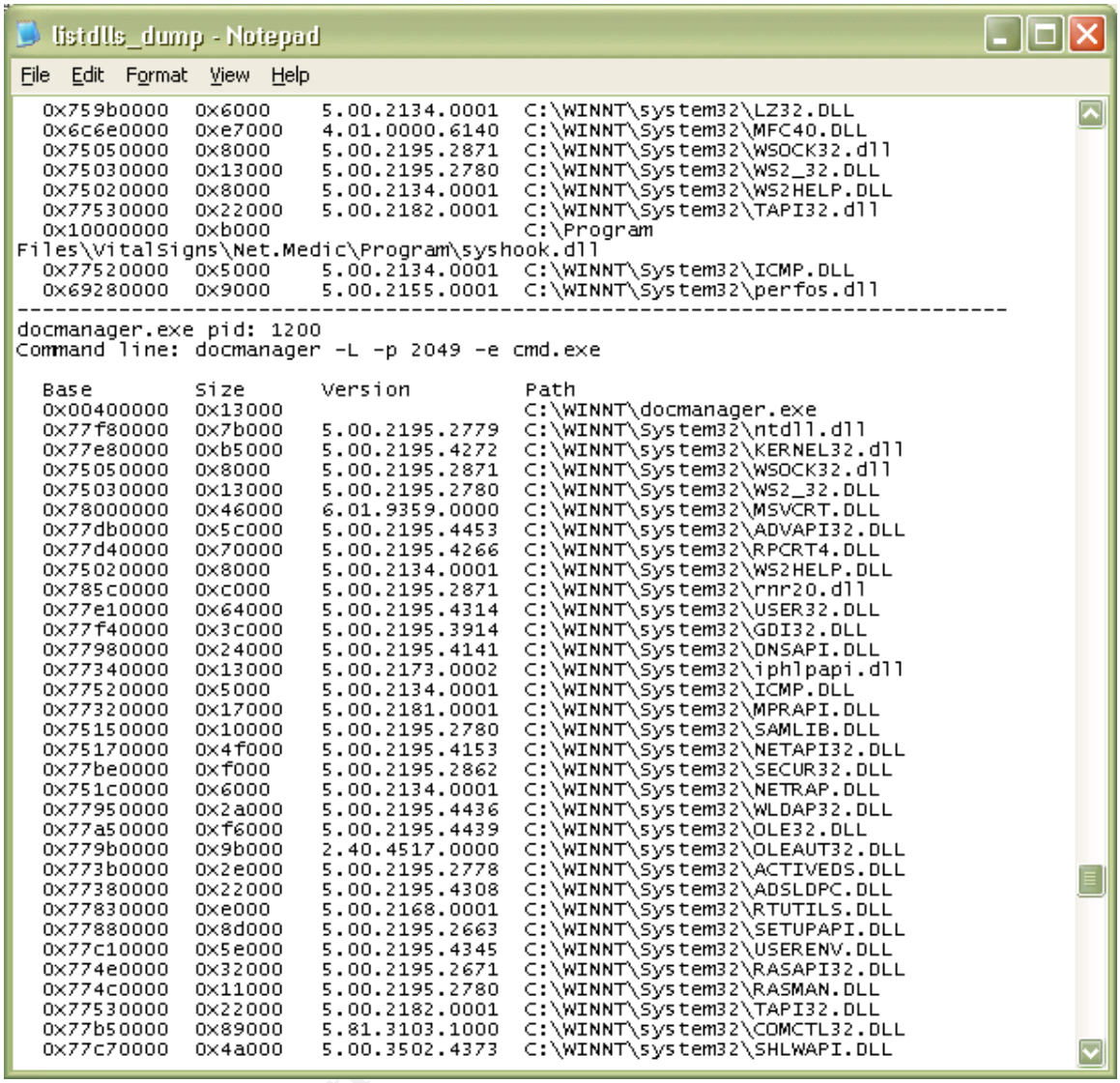
```
252  services      ->  1027  TCP   C:\WINNT\system32\services.exe
1200  docmanager    ->  2049  TCP   C:\WINNT\docmanager.exe
```

Fport showed that port tcp/1027 was being used by the services.exe process. The services.exe process commonly shows up in the process list as it is the engine that runs NT's services. I still felt uncomfortable that it was using a port that was commonly associated with the ICKiller Trojan. This could be simply coincidence, but I wanted to continue digging on this port until I was sure that there were no signs of a Trojan on the system. Since the system was not connected to the Internet or other network during the time Netstat was run there were no established connections that would glen additional information.

Port tcp/2049 showed up as being used by docmanager.exe. This seemed innocent enough since the system was being used as some form of development box. One thing I thought was unusual about the docmanager.exe process was that it started from c:\WINNT were all the other process started from c:\WINNT\system32\. With these things in mind I moved on to the psservice dump file.

An examination of the psservice_dump.txt did not provide any alarming information. The local and remote services that were collected by psservice seemed to be inline. The analysis also didn't provide any additional information about the unusual process and ports other than the fact that the one process 1200, (1200 docmanager -> 2049 TCP C:\WINNT\docmanager.exe) was not a service.

Next I moved onto an examination of the output from listdlls. As stated above the output was directed to a file called listdlls_dump.txt. Information found within the listdlls_dump file would lead to possible evidence that the system being investigation was compromised. The following screenshot taken from the file shows that one process 2000, using port 2049 was calling "cmd.exe" (a complete dump of the listdlls_dump.txt file is in appendix C).



What was even more alarming was the fact that the configuration of the command looked very similar to a hacker tool I'm familiar with called netcat.

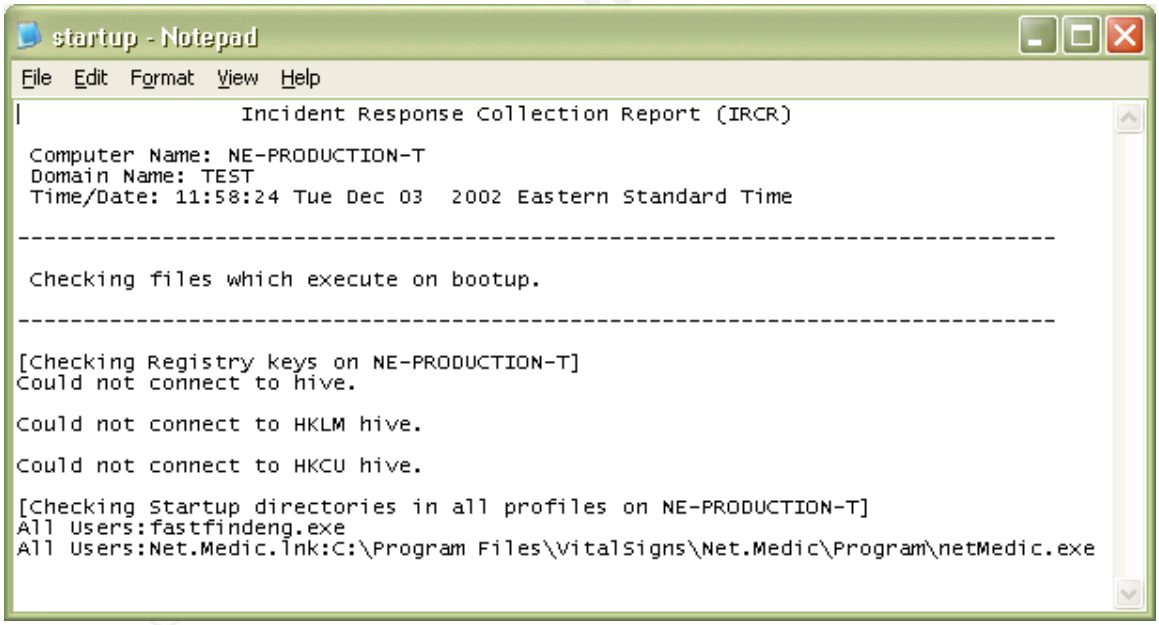
Netcat is an old tool which is commonly referred to as the Hacker's swiss army knife. Netcat is widely used and publicized and has many functions one of which is the capability to act as a kind of telnet program by send commands to a target system. The original version of netcat was created by a hacker named Hobbit for Unix based systems. A windows port of the program was created by Weld Pond of L0pht[6].

Further analysis of the listdlls did not show anything else unusual. I thoroughly documented my findings and suspicions in my notebook and continued on with the rest of the analysis of the system. Now that I had some strong indication that

[6] http://www.zoran.net/wm_resources/netcat_ntclient.asp

the system was compromised I wanted to look for other pieces of evidence that would shine some light on how and when the system was compromised. I also wanted to look for other pieces of software such as sniffers or Trojan that may reside on the system. In order for these types of programs to execute they would have to be either started by a valid system command that had trojanized, started automatically by the system during startup, or started by the user. When I originally started the system I was very careful to only use commands that were being ran from my forensic cdrom and not from the system. I was confident that any commands/processes that were running on the system had to be started automatically when the system started. This lead to an analysis of the systems startup files.

One of the files that IRCR creates when it runs on a system is a dump of several registry keys that are accessed whenever the system starts. These keys are:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run[7]
These keys contain paths to applications that will start automatically without prompting or requiring input from the user. Because of these facts these registry keys are common hiding placed for sniffers, Trojans, and other malicious software. The following screenshot is what was recorded by IRCR:



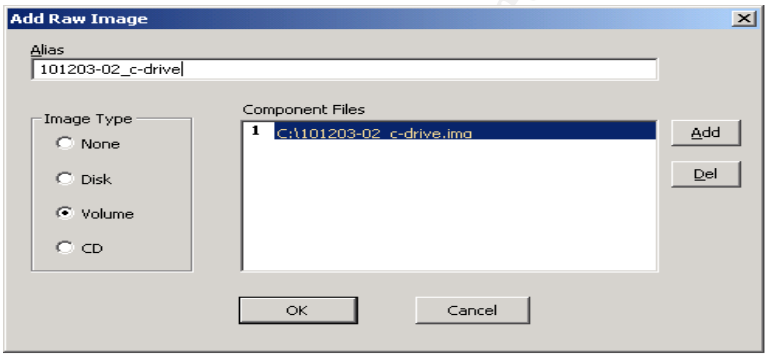
This shows that two programs were started by the registry keys, fastfindeng.exe and netmedic.exe. Neither of these applications sounded ominous, but I wanted to check them both out and ensure they were not sniffers or some other form of malicious program. I performed a google search on both executable names. Netmedic.exe came back with 83 hits about a tool from Vitalsigns. This seemed

[7] http://support.microsoft.com/?kbid=179365

to checkout since I noted that netmedic started automatically when I originally started the system. The other executable, fastfindeng.exe turned up 0 hits. This seemed unusual, but didn't prove that anything was wrong with the executable.

Time line analysis –
To build a timeline for the system I used a combination of the system's logs collected by ICRC and MAC time information analyzed in Encase 3.19. Encase is a well know and respected Windows forensic tool created by Guidance Software[8]. Encase is capable of creating image files as well as conducting detailed analysis of existing image files. Encase is well respected as a forensic tool because of its ease of use, analysis capabilities and its built in chain of custody features.

My first step in analyzing the timeline data was to create a new Encase case and import the image file by using "add Raw image". Encase typically uses its own proprietary format for creating image files, but versions 3.0 and higher are capable of importing and analyzing dd created images.



Once this was completed I had read only access to the image's files, file structure and MAC time information.

The first pieces of information I was after was the time and date of the system installation. To find this I analyzed the system log looking for the first entry that showed an event id 6009 (operating system and build information).

Microsoft uses an elaborate system of "Event Identification" numbers to detail specific actions that have taken place on a system. The value of these event id numbers is that they provide a detailed unambiguous means of identifying actions and problems. Events generally breakdown into three major groups, Security, System and Application. Each event generated is made up of several parts including:

[8] Guidance Software www.encase.com

Record number ← Incremental number assigned to an event. The record number provides identifying and auditing functionality.

Source ← What generated the event.

Computer ← This identifies the name of the system generating the event or on which system the event happened on.

Category: ← This field breaks down different groupings of events such as security, system, hardware, and software.

Event ID ← This is the identifier that is associated with a particular event.

Event type ← This field specifies the criticality of the event. For example some event types include informational, security, warning and error.

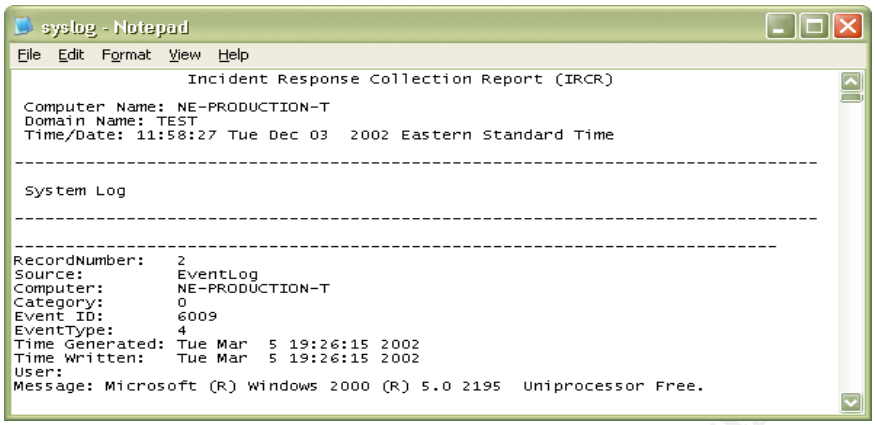
Time Generated ← This is the actual time the event happened.

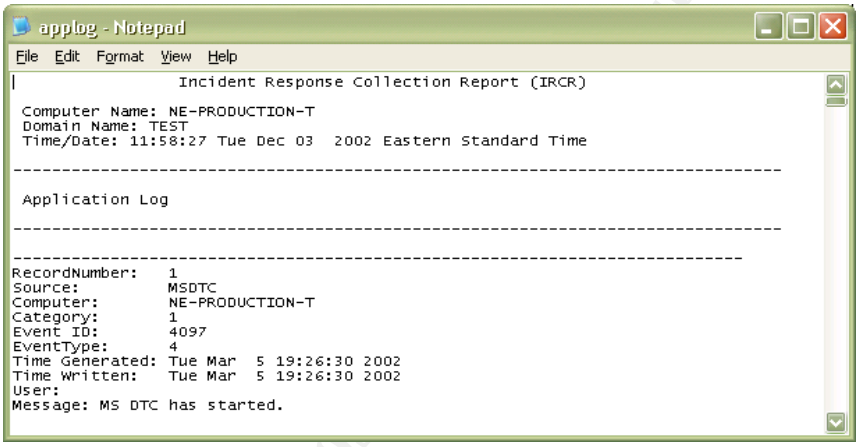
Time Written ← This is the time the event was written to the log. This sometimes differs from time generated because system processes may be consumed by other system functions.

User ← When available, this is the name of the user that is involved or caused the event.

Message ← This is the detailed text that is provided about a particular event.

An Event 6009 is generated every time a system is started. This shows the first time the system was started after installation. From the information collected it appears that the system was installed and on March 5th, 2002 at 7:26pm. To further validate this information I reviewed the application log which showed its first entry as a service starting at the exact same time. (Services starting is conducive of a system starting up.)
The follow screen shots show the first entries in the system and application log files:



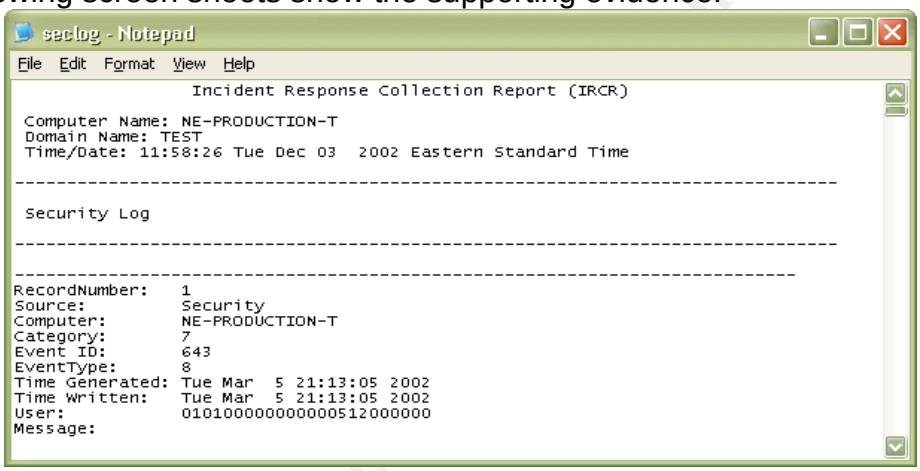


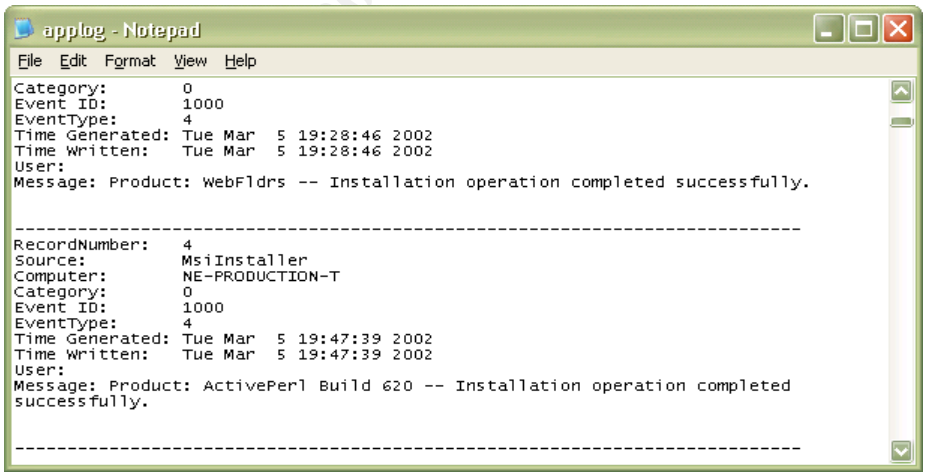
An analysis of Encase's timeline shows that the first file creation time on the system was:

File Name	oschoice.exe
File Ext	exe
Description	File, Archive
Last Accessed	10/11/02 02:35:00PM
Last Written	12/07/99 07:00:00AM
File Created	03/05/02 06:12:45PM
Entry Modified	03/05/02 06:12:45PM
Logical Size	170,768
Physical Size	196,608
File Type	EXE File
File Category	Executable
File Identifier	8,620
Starting Extent	0C549492
Physical Location	PS:2197968, SO:0
Evidence File	101203-02_c-drive
Full Path	101203-02_c-drive\WINNT\system32\dllcache\oschoice.exe

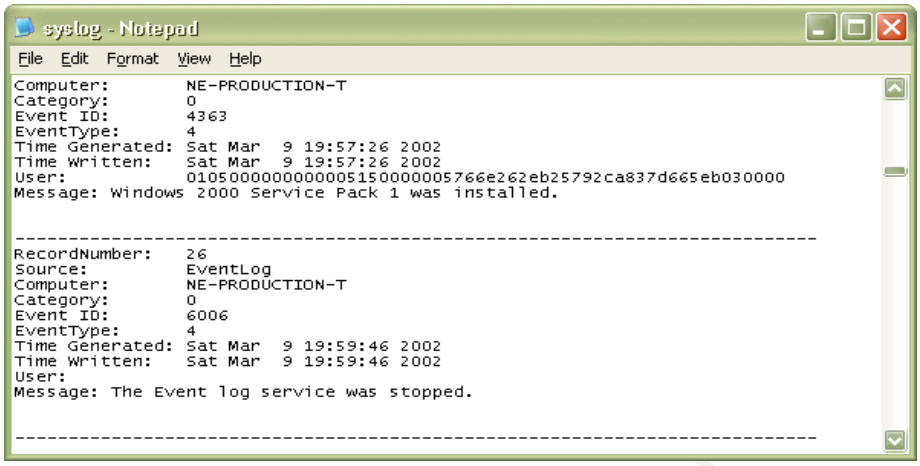
This is another indication of when the system was first installed.

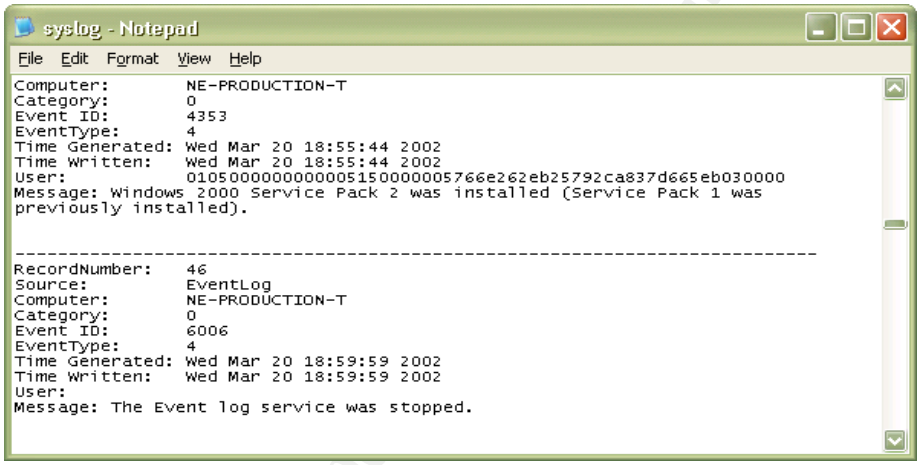
Next I worked on gathering the first user logon time. Getting accurate logon time information is a bit more difficult since the system is configured by default to "not" log any security events. The security log shows that the first official log (event id 680) on was on March 8th 2002 at 6:25pm. Obviously there must have been an earlier login since someone had to logon before that to change the auditing settings to log login success/failures. My analysis of the logs concludes that the first logon was done on March 5th, 2002 around 7:27pm. This was determined by the fact that event ids 643's were found as the second and third security events and were generated on the above date. Event 643 is account management. Other supporting evidence is found in the application log showing that web folders where installed in the surrounding minutes of 7:27pm on March 5th, 2002. The following screen shoots show the supporting evidence:

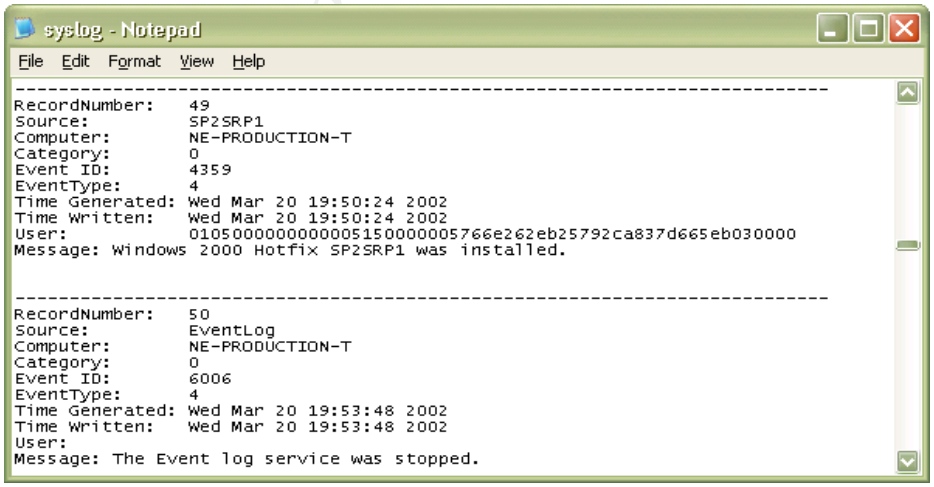




Other pieces of information pulled from the event logs was service pack information. An analysis of the system log shows that service pack 1 was installed on March 9th, 2002 and Service pack 2 was installed on March 20th, 2002. It appears that hotfix sp2srp1 was also installed on March 20th, 2002 at 7:50pm. The following screen shots show the system log entries:

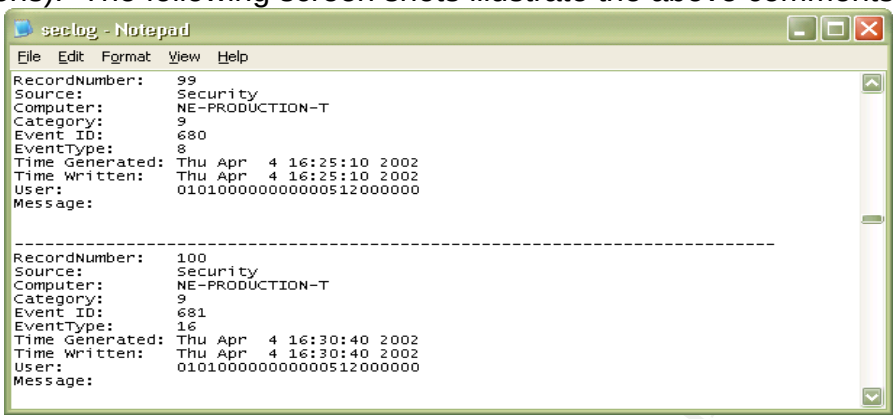


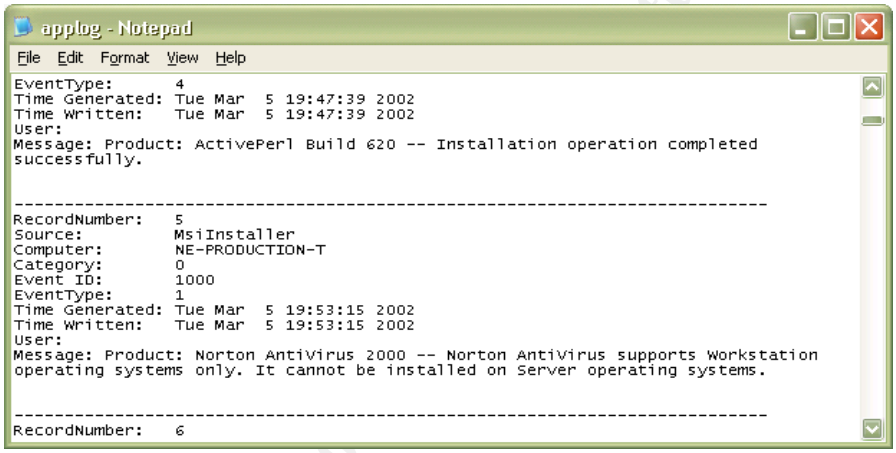




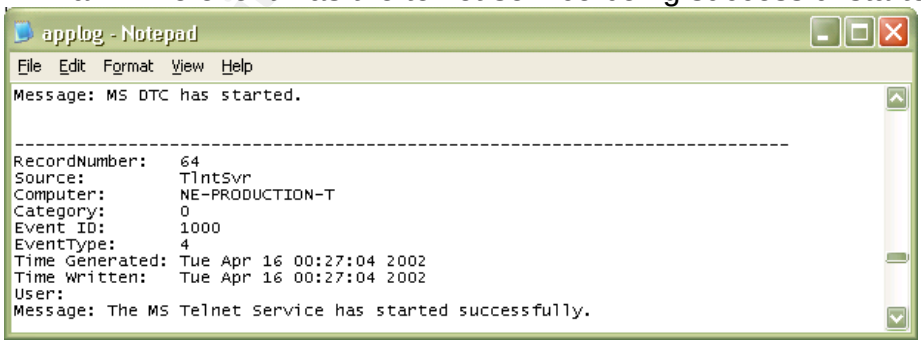
There were a couple of other events in the logs that seemed unusual and interesting which I felt should be commented on. These include a failure event in the application log showing that Norton Antivirus was not successfully installed and a group of failed log-in attempts on April 4th, 2002. The failed attempts are from someone attempting to connect to the system's resources through network

connections (Most likely IUSR_, which is the account used by remote web based connections). The following screen shots illustrate the above comments:

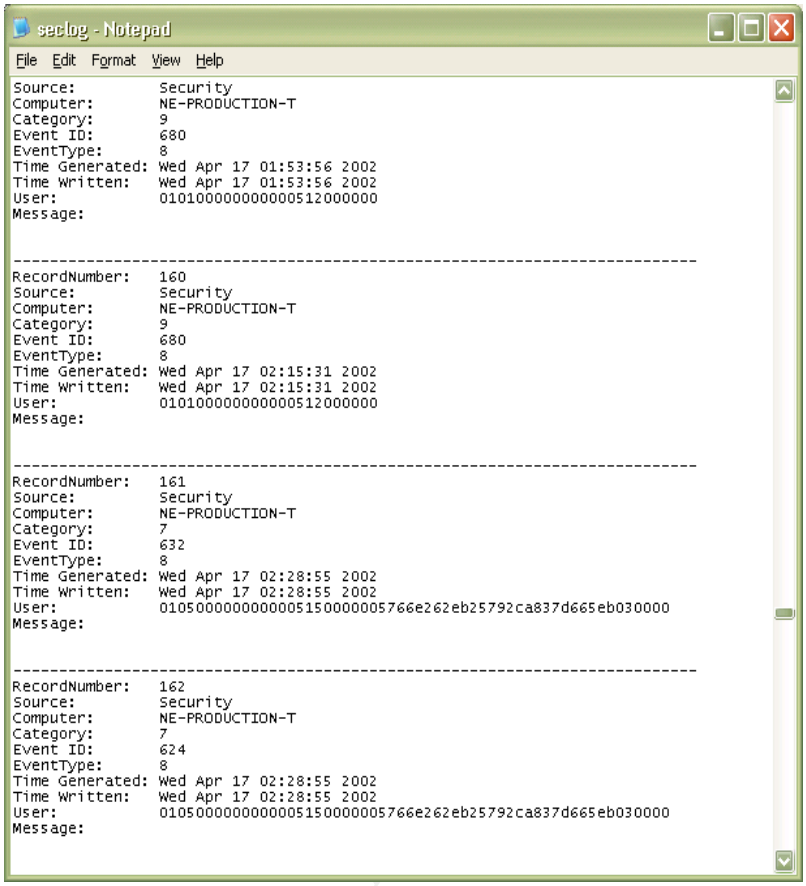


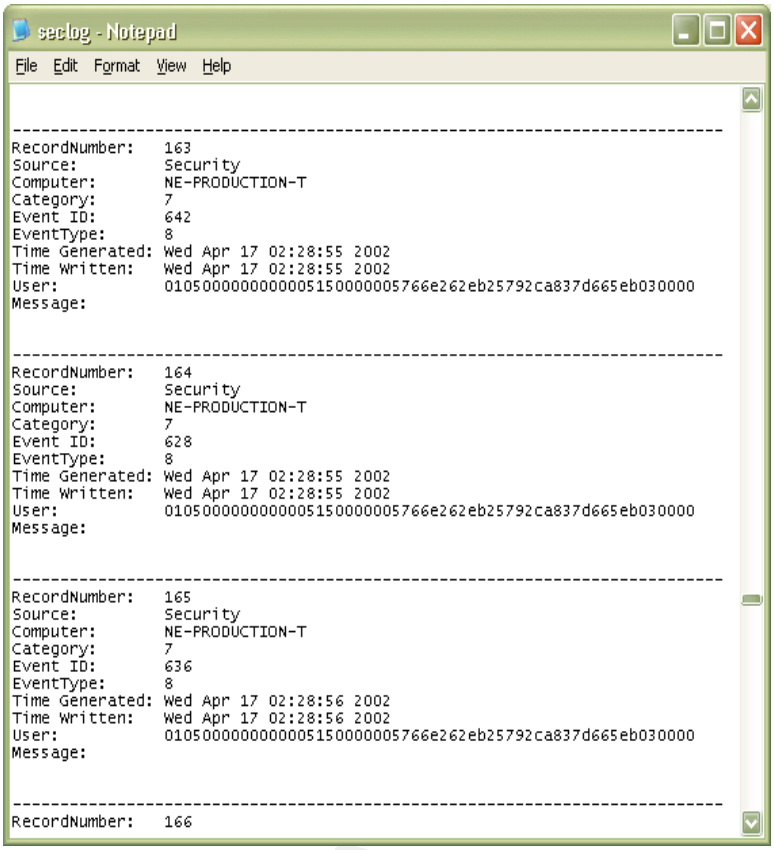


Another interesting event found in the application log was one generated on April 16th, at 12:27am. The event was the telnet service being successful started.



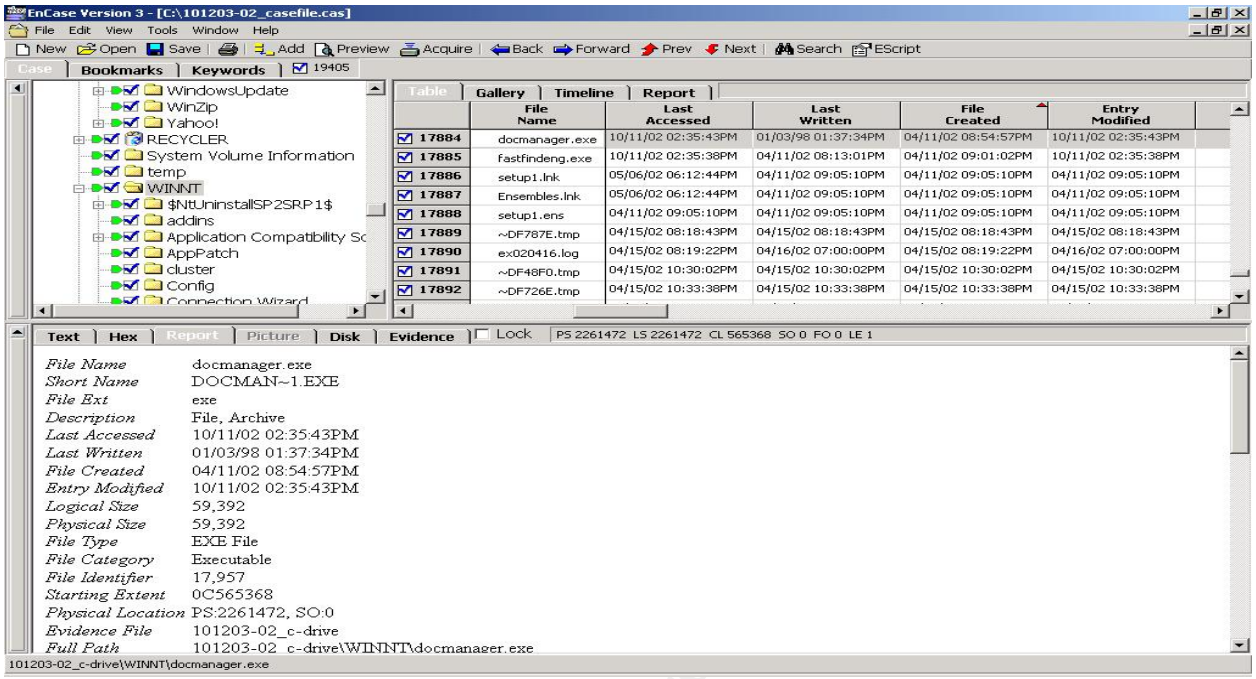
This led me to review the security log around the same time which shows several unusual activities. The security log showed that starting at 1:28am on Apr 17th there were several account management activities. These activities include accounts being created and additions to groups. The following screen shots show the events:





There are two things that make these events alarming. The first is the fact that they are created very late at night, which deviants from the norm of usual activity. The other alarming element is the fact that the activity is the creation of accounts and assigning of permissions. Since this system was allegedly used by only one person and for development work it is not conducive that there would be an additional accounts or permissions added to the system. These events do not prove the system has been compromised, but provide evidence of unusual activity that could lead up to or could be part of a system compromise.

To dig a bit deeper I used Encase to analyze all file MAC times information between the dates of 4/10/02 thru 4/20/02. I picked these dates for an in depth analysis because of the unusual activity that was seen in the log files. The analysis revealed that on 4/11/02 around 8:54:57pm four files were created. Two of these files were called docmanager.exe and fastfindeng.exe. As discussed earlier the file “docmanager.exe” was considered very suspicious. The other file “fastfindeng.exe” was also suspicious since it was configured as described above to execute automatically when the system starts. The following screenshot shows the file and MAC time information for the two files:



Another piece of evidence found in the analysis was the creation of the file "fastfindeng.exe" again on 4/15/02 at 10:52:18pm in the c:\winnt\ directory.

The follow is a complete timeline of system specific events and unusual activities.

03/05/02, 7:26pm	03/05/02, 7:26pm	03/05/02, 7:51pm	3/9/2002	3/20/2002	03/20/200	04/04/02, 4:30pm	04/16/02, 12:27am	04/17/02, 2:20am	10/11/02, 3:35pm
System install	Fist login event	Norton install fails	srv pk1 install	srv pk2 install	sp2srp1 Install	login failures	Telnet serv. started	acct. creation anomalies	Last login

Recover Deleted Files –
To perform the deleted file recovery I imported the forensic dd image file (101203-02_cdrive) into Encase 3.19. Encase allowed me to analyze the dd image file without manipulating or changing the image's data in any way.

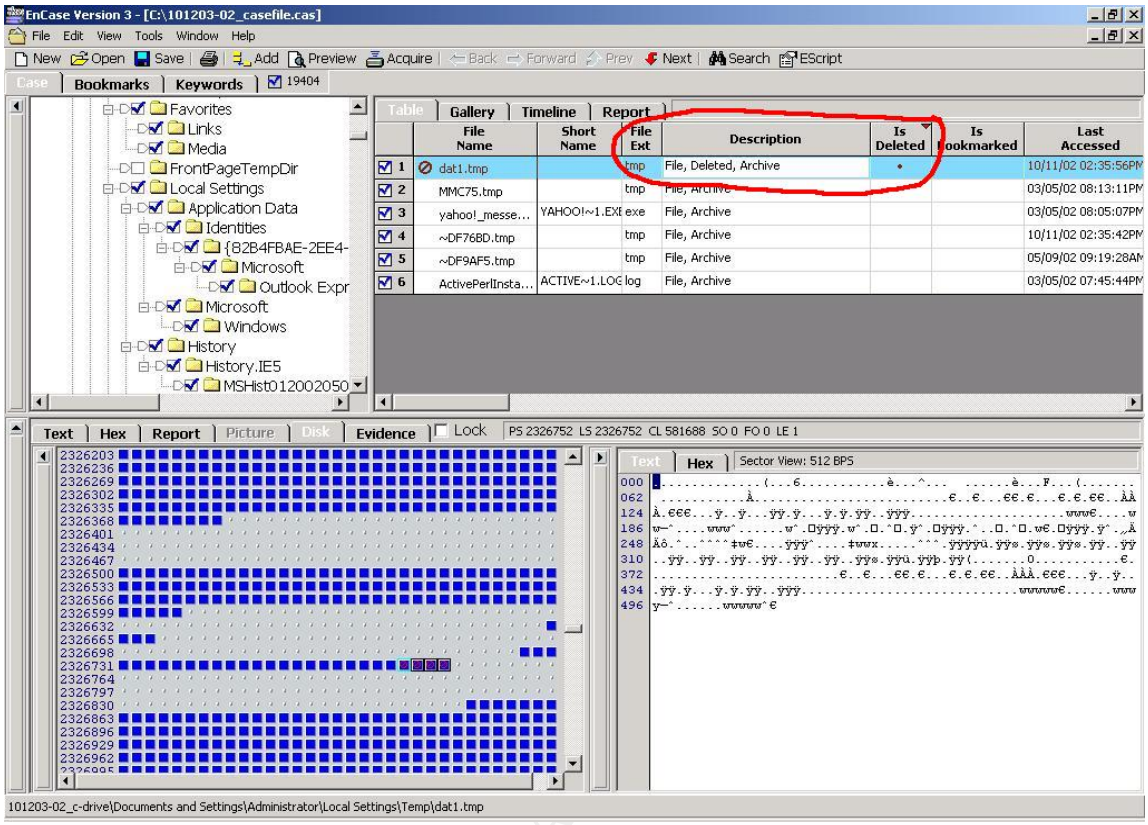
Encase has a sophisticated way of recovering files that have been deleted, but before going into the details it's important to have a high level overview of what happens on a windows NT & 2000 system when files are deleted. When a file is deleted on a Windows NT & 2000 system it is not truly being deleted. The operating system simply removes the pointer (location on the disk were the file resides) reference from the Master File Table (MFT). The MFT is a form of map

that tells the system where files are located and where new files can most effectively be placed. By removing the file's pointer, the operating system can use the disk space previously allocated to the file for other new files. What makes files able to be recovered is the fact that the operating system may not use the freed up space for some time. It is also possible to recover parts of files that have been deleted. This is due to the fact that some files take up multiple clusters. A cluster on a Windows NT & 2000 system is fairly small, usually 512 bytes. When the file is deleted the operating system may allocate only a couple of the clusters that were previously being used by the deleted file. The remaining non-overwritten clusters may be recoverable.

Windows NT & 2000 systems also have a "recycle bin" which acts as a logical way of deleting files. When files are sent to the recycle bin they are not deleted. They are simply marked by the Operating system as "INFO2" files. The operating system keeps track of these files in case the user decides that they want to recovery them. Once the files are removed (emptied) from the recycle bin the INFO information and pointer information is deleted.

Encase locates deleted files by systematically looking at every part of the drive including slack and unallocated space for clusters that are identified as deleted. As stated above, Encase may find complete deleted files or only portions of deleted files. Encase enumerates these files in different ways. Files that are deleted and have not been overwritten are indicated as "file, deleted, archive". These files can typically recovered. Deleted files that have been partially overwritten are indicated as "file, deleted, overwritten, archive. These files can usually be recovered though the value and completeness of the file will vary. The last type of deleted files Encase enumerates is "file, invalid cluster, deleted". This type of deleted files can not be recovered. There is a significant amount of information that is included with all the deleted file types. This includes file type (exe, com, txt, ect.), MAC time information, and the files complete path. All this information helps a forensic analyst put together when, what, and how files on the system were changed.

On the system being analyzed I searched for deleted files by systematically going through the directory structure looking for files that had the deleted flag set. The search for deleted files was virtually fruitless. A search of the entire image revealed only six deleted recoverable files. To validate that the deleted files didn't contain malicious data or information that would add value to the investigation I recovered each file and analyzed the contents. The following is a screenshot of how deleted files are identified within Encase:



The screenshot also shows how Encase displays the contents of the file and where the file resides on the image. The next shot shows reporting information that was collected by encase detailing one of the deleted file. The report information shows a description of the file, file creation and last accessed times, and when the file was deleted:

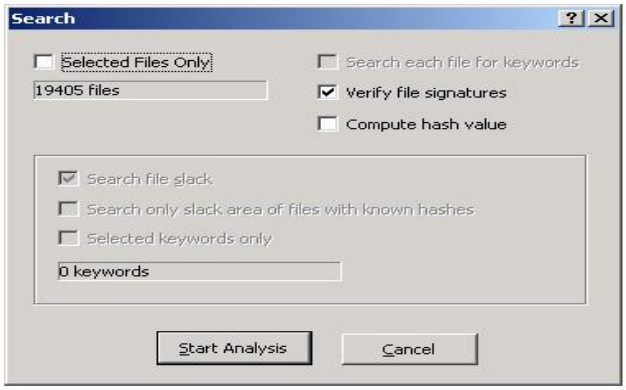
File Name	Setup.ini
Short Name	Setup.ini
File Ext	ini
Description	File, Recycled, Archive
Last Accessed	03/05/02 07:52:57PM
Last Written	08/21/01 10:37:02PM
File Created	08/21/01 10:37:02PM
Entry Modified	03/05/02 07:51:46PM
Logical Size	807
Physical Size	2,048
File Type	Initialization File
File Category	Windows
File Identifier	11,076
Starting Extent	0C950123

Since I already had a good understanding of when the system was compromised I was looking for files that were deleted around April 4th-20th. None of the deleted

files matched the timeline nor did they contain any information that would benefit the investigation. The lack of deleted files by the malicious user seemed odd and I wanted to dig deeper. To do this I wanted to perform a file signature/integrity check on all the files that were deleted and the entire image. My intention was to ensure that a malicious user didn't attempt to rename or manipulate files to hide data instead of deleting them.

Encase's file signature check is a power tool that allow files within an image to be validated against a list of valid known file headers. This is important because Windows interprets file types by the file's suffixes. A malicious user could temporarily rename executable files to some other file name to disguise them. When the malicious user wants to execute the file they would simply have to rename the suffix of the file to .exe, .com, or .bat.

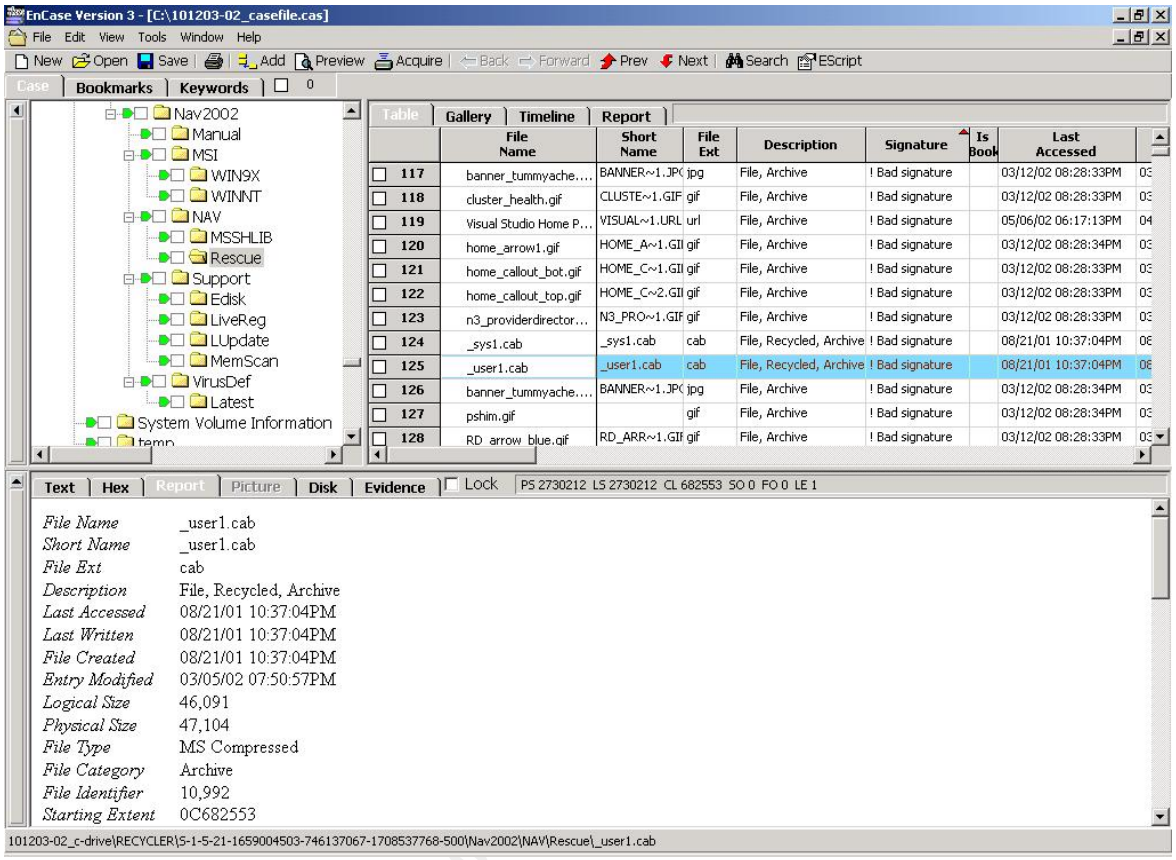
I wanted to use the file integrity tool to identify any mismatch files, analyze their contents and validate their MAC information. The file signature check was engaged by using the search command and selecting "verify file signatures".



The search returned a large number of unknown and mismatch file signatures. These mismatches needed to be investigated, but it's important to remember that this doesn't mean that there are a significant number of files that have been maliciously manipulated. Encase does not have a complete list of known file headers. Encase comes with a large list of standard file headers, but there are always new ones being developed and incorporated into applications. Another contributing factor leading to mismatches is that numerous developer's and applications use the same file suffixes for different types of files. An example is .dat files. Many applications use .dat files, but header information can (and often is) different amongst different applications and vendors.

I analyzed all the reported files looking for unusual MAC information and files that appeared to contain data or executable code. I was also looking for mismatch files that were in strategically significant or obscure locations on the image. An example of what I was looking for would be a renamed executable file residing in the Winnt directory. The following screenshot is an example of the search output

and report information that is returned on files with mismatch and bad file signatures.



The analysis provided some useful information about when and how files were created and deleted, but ultimately didn't provide any additional data that would benefit the investigation at this time.

String Search –

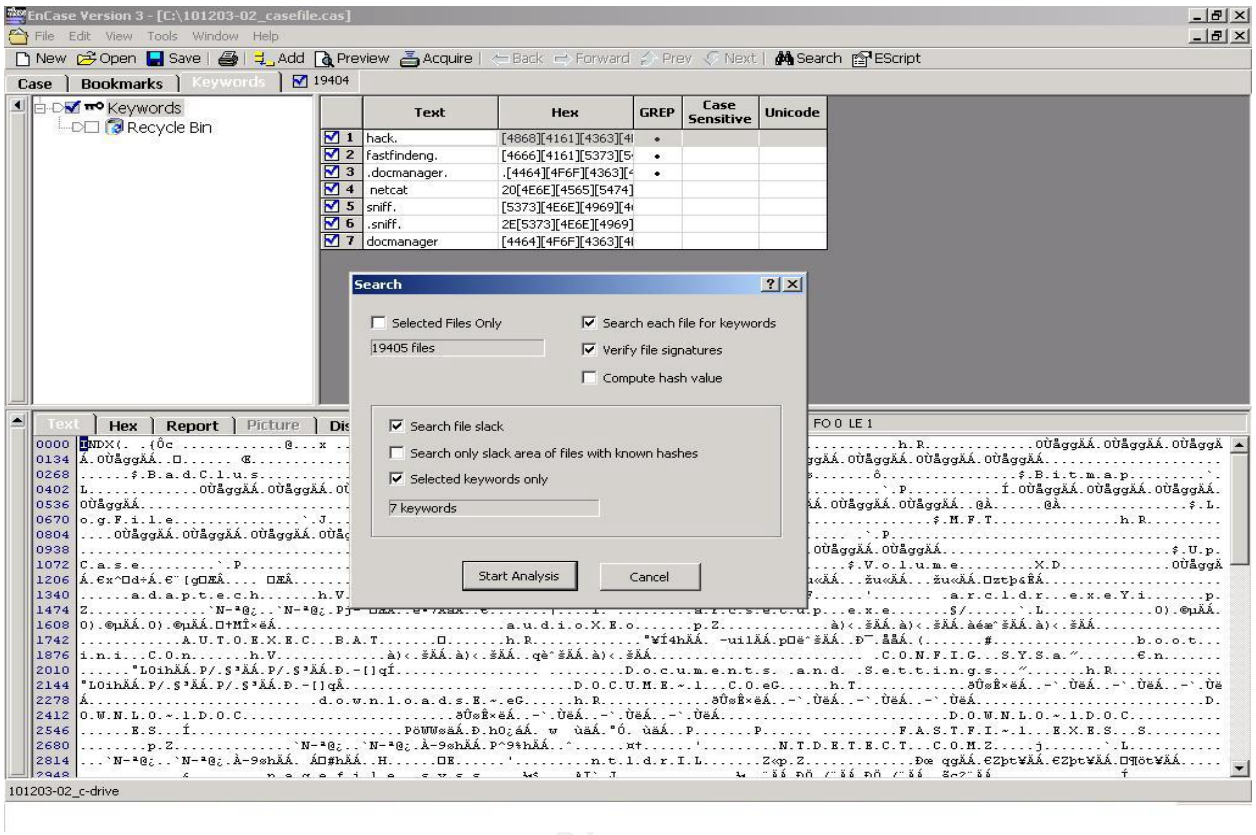
For this part of the investigation I used Encase's keyword search functionality to perform string searches through the entire image file. Since I already had an abundance of information as to what was going on with the system I wanted to use the keyword search functionality to help me extrapolate additional proof that malicious software resided on the system. I also wanted to prove that a Windows port of Netcat resided on the system. Based on evidence found and documented throughout the paper I had a short list of keywords that I wanted to look for. These included:

netcat
docmanager
netmedic
fastfindeng
sniffer

hack

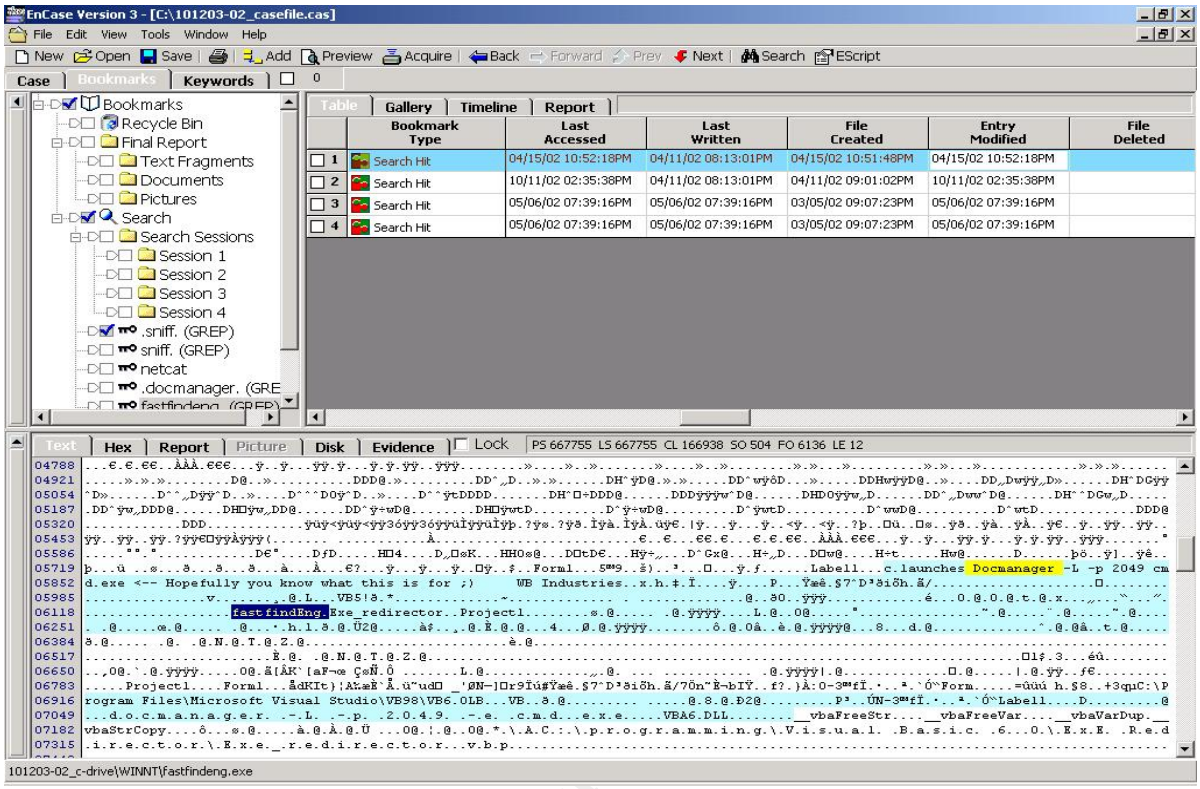
Encase is a superb tool for performing string searches on Windows NT & 2000 because of the manner in which it handles clusters (chunks of disk space). Windows NT & 2000 usually use smaller cluster sizes around 512k. This small amount of space mixed with the fact that clusters may not necessarily be contiguous, leaves a higher probability that keywords could be missed by many string searching programs. For example, if a keyword search for the words "private document" was performed on a system which had the word "private" located at the end of one physical cluster and the word "document" at the beginning of the next cluster, some string searching programs may not be able to find them. Encase searches file by file and logically looks at a file's physical structure on a disk to avoid this problem. The result is a more comprehensive search of a drive.

I setup and engaged Encase's keyword search so it would search the entire image including slack space. The keywords hack, fastfindeng and docmanager were configured as grep searches and appended with a ".", which instructs Encase to look for variations of a keyword (e.g. from the keyword "hack" the search would also return hacker, hackers, hacked). I also engaged the "verify file signatures" to ensure that all the files found with keywords in them have not been manipulated to disguise malicious data. This was redundancy, as it was done earlier, but was performed for good measure. The following screenshot shows the keyword and configuration settings that were enabled for the search:



The search took about 20 minutes to complete and returned over 2000 hit for the keywords that I provided. The keyword search provided a tremendous amount of information. I analyzed all the results, but I focused my analysis on keyword hits that were found in files executed automatically when the system starts. The results validated what I expected.

Search results on Fastfindeng –
Four hits were found for the keyword “fastfindeng”. Two were found within the executable file “fastfindeng.exe” and the other two were found in a file called “ntuser.dat”. The returned text indicates that fastfindeng.exe was some form of catalysis program to start another program called “docmanger.exe.” The MAC information of the file “fastfindeng.exe” also provided valuable timeline information and indicated that the file was created on “04/14/02 10:51:18pm.” This time and date falls inline with the suspected time of system compromise as outlined above. The following is a screenshot of the found text and timeline information:



Search results on Docmanager –
There was a significant amount of information returned on the keyword “Docmanager”. In the fastfindeng.exe file itself was alarming evidence that the system contained malicious software. The following is a portion of the string information returned for docmanger:

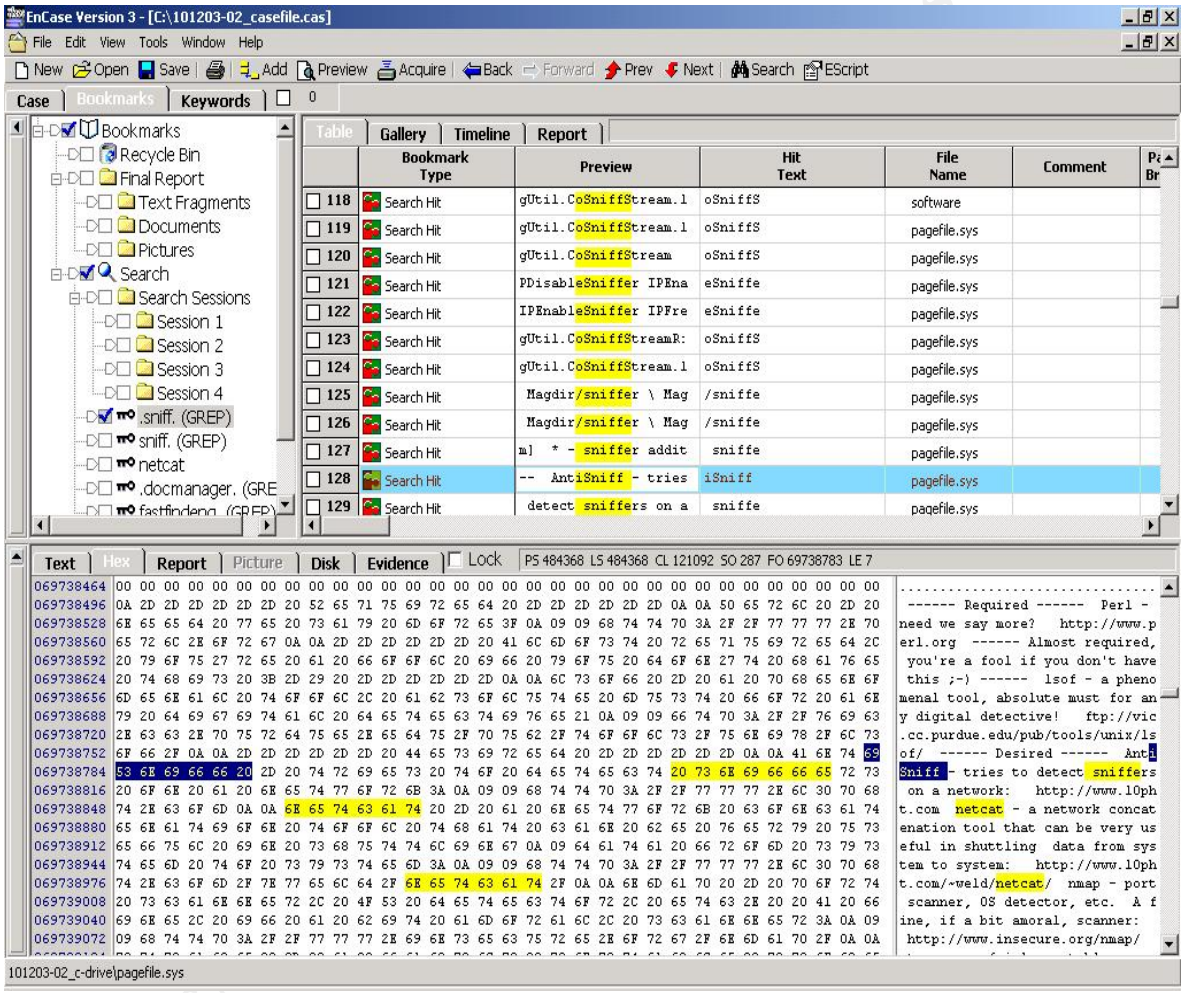
c.launches Docmanager -L -p 2049 cmd.exe <-- Hopefully you know what this is for ;) WB Industries..x.h.‡.Ï....ÿ....P...Ÿæê.§7^D³ðiõh.ã/..... .....v.....¸.@.L...VB5!ð.*.....~..... .....
program Files\Microsoft Visual Studio\VB98\VB6.OLB...VB..ð.@.....
.....@.8.@.Ð2@.....P³..ÚN-3™fÏ..ª.`Ó“Label1....D.....@...d.o.c.m.a.n.a.g.e.r. .-.L. .-.p. .2.0.4.9. .-.e. .c.m.d...e.x.e.....VBA6.DLL.....

The string information shows that the file fastfindeng.exe is designed to execute the docmanager.exe program. The string information indicates that the fastfindeng.exe application is a Visional Basic application and was written in Microsoft Visual Studio. The string information also provides some indication of who originally created the application:

<-- Hopefully you know what this is for ;) WB Industries

This string information appears to be comments about the code. This suggests that the malicious code wasn’t written by the person who is using it. It also indicates that the code was written by a person or group called “WB Industries”.

Search results on netcat, sniff & hack –
The keywords “netcat’, “netmedic”, “sniff” & “hack” returned numerous hits. The vast majority of hits didn’t show any relevant investigation information, but a couple instances of netcat, sniff and sniffer were found in “pagefile.sys.” As state above the pagefile.sys is the area on disk that Windows based machines use as a form of ram. The text appeared to be code comments and application usage for netcat. The following screenshot shows a snippet of the returned string information:



The strings information shows that it was possible that some form of sniffer application was running on the system. The strings information along provided enough evidence that the malicious application Netcat was configured and running on the system.

Conclusions –
In conclusion the investigation showed a considerable amount of information about the habits of the user, when the system was compromised and in what way.

User habits -
The investigation shows that the user did not have security in mind when they were setting up and using the system. This is evident in numerous ways. Firstly, the user didn't have significant logging enabled on the system. The system for the most part appears to have the default auditing and security features enabled. This leaves the system is a bad state since default security settings do not provide means for tracking and recording events on the system. Further, the user did not configure any type of user policies that would inhibit a malicious user from brute forcing passwords or grinding system weaknesses.

Other evidence that the user did not have security in mind is the fact that there doesn't appear to be any anti-virus software installed on the system. The application log shows that the user attempted to install a workstation version of Norton Anti-virus but the install was unsuccessful. This meager attempt to protect the system leave it open to countless numbers of file and internet related virus and worms. It also leaves the system open to trojaned applications which appears to be the cause of the system being compromised.

Another piece of evidence showing the users lack of concern over security is evident by the fact there the system was not kept up to date with the lastest service packs and hot fixes. The timeline shows that service packs were not implemented on the system until months after the system was built. The timeline further showed that there was only one security rollup patch implemented on the system. Since the system was a server running numerous services it would be critical for the system to be routinely upgraded with the latest hot fixes and security patches.

One final example of the user's lack of secure computing habits is evident by the fact that there is no form of firewall application installed on the system. The PC maintenance techs reported that the user said he was using the system for personal use and application development. The user also stated that he frequently took the system home with him. Since all company developer are given remote access accounts it is very likely that the user had the system connected to the internet from time-to-time. The lack of some form of firewall software could leave the system exposed to malicious Internet users. This compounded with the fact that minimal security settings were enabled on the system shows that security was not a primary concern to the user.

Compromised system –
There is a tremendous amount of evidence to support that the system was compromised. The most compelling of the evidence is the fact that a ported copy of the hacker tool Netcat was configured to run on the system as an application called docmanager.exe. It appears that the program was slightly modified and configured to run in listening mode on port tcp/2049. The hacker tool was configured in a form of telnet mode where a remote user could connect to port

2049 and send commands to the system. The received commands would be interrupted by the system's cmd.exe with the output being transmitted back to the malicious user. The docmanager.exe (netcat) command was executed by another program (fastfindeng.exe) that was configured in the registry of the system to start at boot time. I'm not sure if docmanager.exe was originally a legitimate application or why it was used to start the docmanager.exe application, but the docmanager.exe applications was configured to start the trojaned application with the switches needed to enable a malicious user to control the system.

Other evidence shown in the security logs and Encase MAC time information shows evidence that the system was compromised on 4/11/02 around 8:54:57pm. The security log also shows two accounts being added to the system followed by permission additions on 4/17/02 around 1:30am. One of the accounts (supportadmin) was added to the "Administrators group". The activity trend of the user shows that he would typically logon around 5:00pm on weekday and log off around 8-9pm. The fact that accounts were added at 1:30am in the morning significantly deviates from the user's norm. The fact that additional accounts were added to the administrators group also deviates from the norm since the user was the only person to use the system.

Conclusions on how the system was compromised –
The nefarious applications and unusual security log entries provide a strong case that the system was compromised by some form of remote attack that was conducted while the user had his system connected to the Internet. Since the attacker seemed to space various parts of the compromise over several days it is assumed that the system was connected to a static Internet addressable ip address. The system was likely originally compromised by a brute force password attack to one of the system's default shares or by some form of buffer overflow attack to one the system's services. The fact that there was no firewall software configured would leave the system open to Internet attacks. The evidence shows that the attacker then copied several files to strategic places on the system. One file "docmanager.exe" was added to the system startup and configured to start another program called "fastfindeng.exe". Once the system was rebooted the attacker would have command shell access to the system. From there the attacker added several accounts to the system, one of them to the administrators group. By this time the attacker already had full control of the system and could perform any function that the system owner could.

PART III – Legal Issues of Incident handling

A. What if any, information can you provide to the law enforcement officer over the phone during the initial contact?

According to the Electronic Communications Privacy Act (ECPA) the disclosure of contents of communication stored electronically by a public provider to government are forbidden unless a legal request has been made such as a search warrant or subpoena. Before disclosing a user's content or non-content, the public provider must look into statutory exceptions. The public provider may voluntarily disclose non-content information concerning a customer under where these exceptions permit disclosure. The ECPA is finely balanced to help to protect the rights and privacy of the public consumer, while allowing public service providers to assist the government in law enforcement. So long as the proper permission is provided by the authorities, and a good faith reliance has been noted on that documentation (court order, warrant, grand subpoena) it has the ability to offer immunity to civil or criminal action brought against the public service provider.

B. What must the law enforcement officer do to ensure you preserve this evidence if there is a delay in obtaining any required legal authority?

The law enforcement officer is to take immediate action to preserve existing records using the ECPA *Preservation of Evidence under 18 U.S.C. § 2703(f)*[9] Timing is crucial on this step due to the fact that there is no law regulating how long the provider must retain this information and the evidence could easily be lost if not required to hold this information under law. This may be achieved by a phone call, however a fax or email would better provide documentation of the § 2703(f) requests[10]. This section is limiting only in that it will require the provider to only store the information that currently exists and will not include any future electronic communications. In order to acquire any real time electronic communications the law officer must provide proof of probable cause to the courts then acquire permission through the court with a subpoena or court order to intercept this information. Even so only email received that has been open would be considered real time under the court definitions.

C. What legal authority, if any, does the law enforcement officer need to provide to you in order for you send him your logs?

The 18 *U.S.C. § 2703* offers five levels of compelled disclosure under the ECPA. Each of the five mechanisms offers a different level of disclosure information and are in proportion to the difficulty in obtaining them. The minimum requirement for an officer to request log information would be a § 2703d court order with or without prior notice to the subscriber or customer. Depending upon the extent of information needed the officer may provide a search warrant. If a officer provides a section § 2703d court order, the agent may attain anything that can be obtained using a subpoena without notice such as basic subscriber information

8 http://www.cybercrime.gov/s&smanual2002.htm#_IIIG_

as well as information that is outside the scope of ECPA. For example: if a certain email is found to be sent to a company that does not fall under the ECPA protection, an officer could contact the company, provide a subpoena and request the communication that was found to be sent to them. The point here is anything found to be sent to a non-public subscriber which doesn't fall under the protection of the ECPA the agent could bypass the requirements of the ECPA.

Additionally, courts order will also allow officers to obtain all record(s) or other information pertaining to a subscriber to or customer of such service (not including the contents of communications that are held by providers of electronic communications and remote computing service) as stated in 18 U.S.C. § 2703(c)(1). The court order must be issued by an approved governmental agent such as a district court or federal magistrate, or other approved government sources. In addition to the information permitted in § 2703(d), if the officer has a search warrant allowed by § 2703(d), he can obtain full contents of an account without notification to the customer or service subscriber. This includes the contents of a "wire or electronic communication" that is in electronic storage in an electronic communications system although not a remote computing service for 180 days or less. The only limitation to the search warrant is that an officer may not obtain the contents of unopened email. Special care must be taken when presented with a Search warrant.

In United States v. Bach a problem arose when a law enforcement officer obtained a warrant and faxed it to an ISP who in turn provided the appropriate documents. Traditional search warrants call for the presence of the official who would in turn carry out the search and the information provided was deemed a violation of the Fourth Amendment. Since then the ruling has been appealed and the ECPA has shown that § 2705 doesn't require the presence of an officer due to the fact that this type of search warrant is considered non-traditional. However, until the matter in Bach is finalized it would be considered sensible for the warrant issuer to specially permit faxing the warrant to the ISP and noting that an officer need not be present during the execution of the warrant.

D. What other investigative activity are you permitted to conduct at this time?

When presented with a subpoena or court order the ECPA provides the legal ability to provide only the information that is specially requested in that document. The exceptions would be if the provider does not offer their service to the public. There are voluntary discloser provisions that would apply in 18 U.S.C. § 2702 and allow the provider the choice as to whether or not they choose to disclose the information. Otherwise, a public provider may only voluntarily disclose the content of communications to law enforcement when consent to do so exist via banners or other contractual agreements. Without these, rights and property must be protected unless they fall under certain exceptions listed under the

ECPA such as immediate danger to an individual or a serious threat of bodily injury.

E. How would your actions change if your logs disclosed a hacker gained unauthorized access to your system at some point, created an account for him/her to use, and used that account to hack into the government system?

Initially, the ECPA imposed a tremendous obstacle in investigating computer hacker cases because it didn't allow the victims of hackers to ask government agencies for assistance. During the fall of 2001 Congress enacted a new exception in the USA Patriot Act[11]. This exception (§ 2511(2)(i)) called the "computer trespasser" exception allows the law enforcement to assist the victims of hacking in an investigation of a crime. A Hacker by definition according to the ECPA is anyone who the provider has no existing user knowledge of a contractual relationship for their service as noted in 18 U.S.C. § 2510(21). Because a hacker gained unauthorized access to our system and we had no contractual relationship, the hacker would not be protected under the ECPA and would lose his "reasonable expectation of privacy" provided by the fourth amendment. We would then be able to provide the law officer with the information requested without threat of violation of ECPA. It is important to note that a customer that abuses or violates his contract doesn't fall under the definition of a hacker even if he were to create an unauthorized account. When the company has any knowledge of this user then the customer although violating the terms of his contract, would still have privacy rights that fall under the ECPA.

From this point, in order for the computer trespasser exception to apply all actions of the investigation would have to be preformed by the government official or an agent acting under the color of law with our consent in order to pursue the investigation. Also the rights of protected individuals can't be superceded in the pursuit of the hacker. All information acquired by the communication intercepted may only be to-and-from the computer trespasser. Any prior exceptions with the wiretap statue may also be used.

Additional Information and Sources

Computer Crime and Intellectual Property Section Criminal Division
United States Department of Justice:
http://www.cybercrime.gov/s&smanual2002.htm#_IVD_

[11] http://www.cybercrime.gov/s&smanual2002.htm

The Provisions of the USA Patriot Act:
http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html

US code collection:
http://www4.law.cornell.edu/uscode/18/pIch119.html

Sans Institute, Forensics Frameworks and Best Practices:
Managerial and Legal Issues 2002

Communication Security:
http://nsi.org/Computer/comm.html

Consumer Privacy Guide:
http://www.consumerprivacyguide.org/law/ecpa.shtml

Reference

Phrack home page: http://www.phrack.com/phrack/51/P51-06. Jan. 5, 2003

Guidance Software: http://www.guidancesoftware.com/support/v4support.shtm Nov. 25, 2002.

CERT. Intruder Detection Checklist. CERT website. http://www.cert.org/tech_tips/intruder_detection_checklist.html. Nov. 25, 2002

"Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations": http://www.cybercrime.gov/s&smanual2002.htm Feb 12th, 2003

Electronic Privacy Information Center:
http://www.epic.org/privacy/terrorism/hr3162.html Feb12th, 2003

McClure, Scambary, Kurtz,. "Hacking Exposed:netcat" ch. 8 pg. 381-382. Mc Graw Hill, Osborne Press, 1999.

United States Congress. "Wire and Electronic Communications Interception and Interception of Oral communications" 13th Feb. 2003.
http://www.usdoj.gov/crimal/cybercrime/18usc2511.htm

United States Congress. “Unlawful Access to Stored Communications” http://www.usdoj.gov/crimal/cybercrime/usc2701.htm

SANS Institute Information Security Reading Room – Netcat: The TCP/IP Swiss Army Knife. Tom Armstrong; Feb 15, 2001

Kubark, The Kubark Interrogation Manual, http://www.parascope.scom/articles/0397/kubarkin.htm Dec 10, 2002.

ICMP attacks and applications http://rr.sans.org/threats/ICMP_attacks.php; Dec 8, 2002.

ICMP tunneling article http://www.networkmagazine.com/article/NMG20000515S0048; Dec 8, 2002.

IDS signatures and information about ICMP attacks http://www.shmoo.com/mail/fw1/mar01/msg00042.shtml; Dec 8, 2002.

Forensic interrogation practices http://www.parascope.com/articles/0397/kub_ix.htm Dec. 8, 2002.

MAC time resources http://www.cert.org/security-improvement/implementations/i046.01.html Dec. 8, 2002.

Strings command references http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/cmds/aixcmds5/strings.htm; Dec. 8, 2002.

Appendix A

The following is a strace dump with the follow option engaged:

```
Strace –ff –e trace=read
execve("/usr/sbin/atd", ["atd", "-ff", "-e", "trace=read"], [/* 35 vars */]) = 0
uname({sys="Linux", node="localhost.localdomain", ...}) = 0
brk(0)                                  = 0x804c584
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=98907, ...}) = 0
old_mmap(NULL, 98907, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40014000
close(3)                                = 0
open("/lib/i686/libc.so.6", O_RDONLY)   = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\0\0\3\0\3\0\1\0\0\0`u\1B4\0"..., 1024) = 1024
```

```
fstat64(3, {st_mode=S_IFREG|0755, st_size=1401027, ...}) = 0
old_mmap(0x42000000, 1264928, PROT_READ|PROT_EXEC, MAP_PRIVATE, 3, 0) =
0x42000000
mprotect(0x4212c000, 36128, PROT_NONE)  = 0
old_mmap(0x4212c000, 20480, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED, 3,
0x12c000) = 0x4212c000
old_mmap(0x42131000, 15648, PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x42131000
close(3)                                = 0
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1,
0) = 0x4002d000
munmap(0x40014000, 98907)               = 0
brk(0)                                  = 0x804c584
brk(0x804c5b4)                          = 0x804c5b4
brk(0x804d000)                          = 0x804d000
socket(PF_UNIX, SOCK_STREAM, 0)         = 3
connect(3, {sin_family=AF_UNIX, path="/var/run/.nscd_socket"}, 110) = -1 ENOENT (No such file
or directory)
close(3)                                = 0
open("/etc/nsswitch.conf", O_RDONLY)    = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=1750, ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0)
= 0x40014000
read(3, "#\n# /etc/nsswitch.conf\n#\n# An ex"..., 4096) = 1750
brk(0x804e000)                          = 0x804e000
read(3, "", 4096)                       = 0
close(3)                                = 0
munmap(0x40014000, 4096)                = 0
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=98907, ...}) = 0
old_mmap(NULL, 98907, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40014000
close(3)                                = 0
open("/lib/libnss_files.so.2", O_RDONLY) = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\0\0\3\0\3\0\1\0\0\0\0\0\35\0"..., 1024) = 1024
fstat64(3, {st_mode=S_IFREG|0755, st_size=45415, ...}) = 0
old_mmap(NULL, 37848, PROT_READ|PROT_EXEC, MAP_PRIVATE, 3, 0) = 0x4002e000
mprotect(0x40037000, 984, PROT_NONE)    = 0
old_mmap(0x40037000, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED, 3,
0x9000) = 0x40037000
close(3)                                = 0
munmap(0x40014000, 98907)               = 0
open("/etc/passwd", O_RDONLY)           = 3
fcntl64(3, F_GETFD)                     = 0
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
fstat64(3, {st_mode=S_IFREG|0644, st_size=1383, ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0)
= 0x40014000
read(3, "root:x:0:0:root:/root:/bin/bash\n"..., 4096) = 1383
close(3)                                = 0
munmap(0x40014000, 4096)                = 0
socket(PF_UNIX, SOCK_STREAM, 0)         = 3
connect(3, {sin_family=AF_UNIX, path="/var/run/.nscd_socket"}, 110) = -1 ENOENT (No such file
or directory)
close(3)                                = 0
open("/etc/group", O_RDONLY)            = 3
fcntl64(3, F_GETFD)                     = 0
```

```
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
fstat64(3, {st_mode=S_IFREG|0644, st_size=610, ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0)
= 0x40014000
read(3, "root:x:0:root,bbowers\nbin:x:1:ro"..., 4096) = 610
close(3)                                = 0
munmap(0x40014000, 4096)                = 0
geteuid32()                             = 0
getegid32()                             = 0
setregid32(0, 0x2)                      = 0
setreuid32(0, 0x2)                      = 0
brk(0x8051000)                          = 0x8051000
time([1040325951])                      = 1040325951
open("/etc/localtime", O_RDONLY)        = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=1267, ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0)
= 0x40014000
read(3, "TZif\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\4\0\0\0\4\0"..., 4096) = 1267
close(3)                                = 0
munmap(0x40014000, 4096)                = 0
getpid()                                = 2161
rt_sigaction(SIGPIPE, {0x420e4570, [], 0x4000000}, {SIG_DFL}, 8) = 0
socket(PF_UNIX, SOCK_DGRAM, 0)          = 3
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
connect(3, {sin_family=AF_UNIX, path="/dev/log"}, 16) = 0
send(3, "<75>Dec 19 14:25:51 atd[2161]: u"..., 45, 0) = 45
rt_sigaction(SIGPIPE, {SIG_DFL}, NULL, 8) = 0
_exit(1)                                = ?
```

The following is a complete diff dump of the strings information retrieved from the atd binary and lokid:

```
 1,2c1,2
< /lib/ld-linux.so.1
< libc.so.5
---
> /lib/ld-linux.so.2
> libc.so.6
6,7d5
< popen
< shmctl
9d6
< _DYNAMIC
11d7
< errno
18d13
< _IO_stderr_
21d15
< semctl
24,26d17
< __environ
< bzero
< _init
```

```
28,29c19
< __libc_init
< environ
---
> popen
32a23
> __deregister_frame_info
36d26
< __fpu_control
43a34
> __strdup
46d36
< strdup
47a38
> memset
50d40
< time
52d41
< _fini
55,56c44,46
< atexit
< _GLOBAL_OFFSET_TABLE_
---
> stderr
> shmctl
> semctl
58,60c48,49
< exit
< __setfpucw
< open
---
> _IO_stdin_used
> __libc_start_main
61a51
> __register_frame_info
64,67c54,94
< _etext
< _edata
< __bss_start
< _end
---
> __cxa_atexit
> __gmon_start__
> GLIBC_2.2
> GLIBC_2.1
> GLIBC_2.1.3
> GLIBC_2.0
> PTRh
> [^_]
> [^_]
> [^_]
> [^_]
> f;4:u
> [^_]
> [^_]
> u[Wj
```

```
> ZYPS
> xFRj
> JIt
> vuRj
> vuQj
> j@ht
> Kuqf
> j@ht
> Ku.f
> @uGj
> Sj7j
> Rj8SW
>  PVj7W
> Qj8SW
> Vj7W
> tdRj8SW
> Vj7W
> t4Pj8SW
> Vj7W
> PVj7j
> Wj7h
> [^_]
> j        ht
> }`Rj7
> }2Pj7
> [^_]
69,97c96,97
< f91u
< WVS1
< pWVS
< vuWj
< <it     <ut
< vudj
< <it     <ut
< 3jTh
< j7Wh
< Wj7j
< Vj7S
< j8WS
< Vj7S
< j8WS
< Vj7S
< tVj8WS
< Vj7S
< t'j8WS
< jTh8
< Wj7j
< j7hU
< j@hL
< @j@hL
< jTh8
< j        h@
< }^j7
< }1j7
< <WVS
< tDWS
```

```
---
> ZYhl
> [^_]
104d103
< server uptime:            %.02f minutes
109c108,109
< N@[fatal] cannot catch SIGALRM
---
> [fatal] cannot catch SIGALRM
> server uptime:            %.02f minutes
111c111
< @[fatal] shared mem segment request error
---
> [fatal] shared mem segment request error
113d112
< [fatal] could not lock memory
116d114
< [fatal] cannot destroy shmid
117a116,117
> [fatal] could not lock memory
> [fatal] cannot destroy shmid
119d118
< [fatal] cannot catch SIGALRM
124d122
< [fatal] cannot detach from controlling terminal
125a124
> [fatal] cannot detach from controlling terminal
127,129d125
< v:p:
< Unknown transport
< lokid -p (i|u) [ -v (0|1) ]
131d126
< [fatal] cannot catch SIGUSR1
135,136d129
< [fatal] cannot catch SIGALRM
< [fatal] cannot catch SIGCHLD
138d130
< [fatal] forking error
140,143d131
< lokid: Cannot add key
< lokid: popen
< [non fatal] truncated write
< /quit all
145d132
<           sending L_QUIT: <%d> %s
148d134
< /quit
151,152d136
< /stat
< /swapt
157a142,154
> v:p:
> Unknown transport
> lokid -p (i|u) [ -v (0|1) ]
> [fatal] cannot catch SIGUSR1
> [fatal] forking error
```

> lokid: Cannot add key
> lokid: popen
> [non fatal] truncated write
> /quit all
> sending L_QUIT: <%d> %s
> /quit
> /stat
> /swapt

Appendix B

\d020bb04b3299913a8958ef8102ebecc *g:\\forensic_tools\\ads.exe
\996368b900e1a5f416ebe6d9ce0ab936 *g:\\forensic_tools\\AFind.exe
\d6d9ba7cf601dea64d4a8cf0ee857e6a *g:\\forensic_tools\\ar.exe
\4db533f44112e9a8aab1a2bfc9de4058 *g:\\forensic_tools\\ARP.EXE
\825117283877a346e9ba8535acb7e680 *g:\\forensic_tools\\as.exe
\c2937180dd68c664e72398a05f4a30ac *g:\\forensic_tools\\Audited.exe
\47b2355d13884c9558253b7e7303d4f5 *g:\\forensic_tools\\awk.exe
\e2d152b18786cdd19119f585a407a8b7 *g:\\forensic_tools\\bintext.exe
\7efabbd8356b2e3168d09abd0b137a61 *g:\\forensic_tools\\bunzip2.exe
\840073d380c4c45a2f57de5584e1b36a *g:\\forensic_tools\\bzcat.exe
\840073d380c4c45a2f57de5584e1b36a *g:\\forensic_tools\\bzip2.exe
\876d82e2940bea7228071c23c7993e99 *g:\\forensic_tools\\bzip2recover.exe
\ebdc3a61996501c773f941b22926be16 *g:\\forensic_tools\\cat.exe
\e0404e18c24b474c2499d52794ec4718 *g:\\forensic_tools\\chgrp.exe
\f9945b41f492068c11ca25a52ef2cf53 *g:\\forensic_tools\\chmod.exe
\d34ed8b1571fdbb54ab12d00bd4be75f *g:\\forensic_tools\\chown.exe
\f488f33ef4973568c1fb9f1784a7bc1f *g:\\forensic_tools\\chroot.exe
\4c84ebae362030b838814af9b7f285e0 *g:\\forensic_tools\\cjpeg.exe
\16b43945a9d671802d0ea18bfa4b4ed9 *g:\\forensic_tools\\cksum.exe
\6c9b72e5cbc6fe1161ec1b58d1e2f1ee *g:\\forensic_tools\\clear.exe
\7644ae3bcadae89e7160e3aff2e7d2bc *g:\\forensic_tools\\CMD.EXE
\b829ea9c8d88429bb329f2c6606cbd1e *g:\\forensic_tools\\cp.exe
\f66f141294f1cd415a130a4ec90f7f4f *g:\\forensic_tools\\cpio.exe
\1810315656724f5f547eeb57ae9e1c60 *g:\\forensic_tools\\cpp.exe
\6ccaecc0f803ab9b5bb9c9a747eca8c9 *g:\\forensic_tools\\crypt.exe
\2b4eef60434538e480ddbea1f209506f *g:\\forensic_tools\\ctags.exe
\1206acec495dbc9db1e27966cdcc0e1b *g:\\forensic_tools\\cut.exe
\96e9baabf3168e5c3b51e089d1b7ed51 *g:\\forensic_tools\\DACLchk.exe
\befa15863e0bb831b0daa7a0b689b117 *g:\\forensic_tools\\date.exe
\1bcf2f24d761db7565690c91e0c0506b *g:\\forensic_tools\\dd.exe
\4e466029684bb2131ec2a4b23fa56035 *g:\\forensic_tools\\ddNT.exe
\49ee1e66a324c45804271acfe277e999 *g:\\forensic_tools\\df.exe
\c0555070f3c843438439758c54c59371 *g:\\forensic_tools\\diff.exe
\a3a9f784e7c9bb3b716c790de3f72dd3 *g:\\forensic_tools\\diff3.exe
\1e82062954af63192aefb5929c9e0e43 *g:\\forensic_tools\\dir.exe
\e77147ff2f5156523617ce8b619213e3 *g:\\forensic_tools\\dircolors.exe
\49ec63eeb2e59aab2f3ef80a947db211 *g:\\forensic_tools\\dirname.exe
\5545311a5c8ba4228a8a6f7de533c15d *g:\\forensic_tools\\doskey.exe
\6717d1d7d502139227f484f81faa7861 *g:\\forensic_tools\\du.exe
\760ca7e134e7f367e263a14dee41d983 *g:\\forensic_tools\\DUMPACL.EXE
\b214c4ac1f53faa7bfbd02402519c23b *g:\\forensic_tools\\echo.exe

\fefbed6ace30d2ea78eb38adf1b88fbe *g:\\forensic_tools\\egrep.exe
\73f85b456ebdbb2e5b0f835e25a0827e *g:\\forensic_tools\\enum.exe
\363c7a2f3c49b94d3f1a2618d788dd89 *g:\\forensic_tools\\env.exe
\df1d9a2c20135f2f33fcbd1aaa05fa43 *g:\\forensic_tools\\fgrep.exe
\9b86f2ef90962057a64acc054604826a *g:\\forensic_tools\\file.exe
\d099b4d399874f55f44be4601eb662a1 *g:\\forensic_tools\\FILEMON.EXE
\d9027a03653dcbdccf47bd4a2e165b13 *g:\\forensic_tools\\FileStat.exe
\f00ff20c4d6466a9d42e25fff3158095 *g:\\forensic_tools\\find.exe
\7150d8016a5b6e0b985e921f1f98817d *g:\\forensic_tools\\finfo.exe
\544e746b267808ec0f76d904c739bd0d *g:\\forensic_tools\\fport.exe
\b4f430017c9bf7a4c58dd01cda48e308 *g:\\forensic_tools\\grep.exe
\fa6dcbda15b99c817db83613050246c5 *g:\\forensic_tools\\gunzip.exe
\fa6dcbda15b99c817db83613050246c5 *g:\\forensic_tools\\gzip.exe
\e150207c843e52224071fe6e86c877fe *g:\\forensic_tools\\handle.exe
\9876f3f8f26260432c7dd21b440e4d99 *g:\\forensic_tools\\head.exe
\ec531a7bb577bf938d3a76dd6a0bb6b9 *g:\\forensic_tools\\HexDiff.exe
\5125ddd2568378310fb0bc4f9994bfc4 *g:\\forensic_tools\\HFind.exe
\4e0db46827176a066e2757309a9c9b3a *g:\\forensic_tools\\hostname.exe
\81c473dc0d266dfe7c275af12db0327a *g:\\forensic_tools\\Hunt.exe
\d01378f0a6141373e78433f048081dde *g:\\forensic_tools\\id.exe
\a60b9bfc975a71e528fb977f0c2983c5 *g:\\forensic_tools\\IeHistory.exe
\823722f2b6588db66296eded1c90df83 *g:\\forensic_tools\\ifids.exe
\4a1c9188d2633926b955584406f9d04d *g:\\forensic_tools\\ircr11.exe
\3e37c1c1d736ad3aac1f1e5aadec40de *g:\\forensic_tools\\keytime.exe
\9f51b451b4df92e4085da8ce27208426 *g:\\forensic_tools\\kill.exe
\5645bcb1b00d5f4e1f2a9eceac40deb6 *g:\\forensic_tools\\ld.exe
\01b5d56602370685f895b075dc02de08 *g:\\forensic_tools\\less.exe
\3a5e441b07f398977fca97db18fecc0a *g:\\forensic_tools\\lessecho.exe
\7b591001cc00ea60b44242d1f39f4455 *g:\\forensic_tools\\lesskey.exe
\7ca844ce3df71df241cbe0a1d1741b08 *g:\\forensic_tools\\listdlls.exe
\78a9164b632a8d2d4a8cb6b2a9aa0584 *g:\\forensic_tools\\lsaacl.exe
\1b5571a62e590885da19dd17ebd54094 *g:\\forensic_tools\\lsadump2.exe
\388631fc7dd59959a26f246fc37034fa *g:\\forensic_tools\\mac.exe
\01ccdb12282dd542182fef660cc2a574 *g:\\forensic_tools\\md5sum.exe
\0633b72ec8e8ef515b33ef882acf955d *g:\\forensic_tools\\mdmchk.exe
\41dfd71fa18804847eb411f2c6ca5aca *g:\\forensic_tools\\memdump.exe
\0b30f70235af7cf9d932f69754a1826e *g:\\forensic_tools\\mkdir.exe
\7ab9db9514f06f053274c7e249ad303f *g:\\forensic_tools\\mount.exe
\d1e0269b75681e99451b7ace4423e540 *g:\\forensic_tools\\nbname.exe
\402a307f8121977b3f74b2316b9ec60e *g:\\forensic_tools\\nc.exe
\e0fb946c00b140693e3cf5de258c22a1 *g:\\forensic_tools\\nc_orig.exe
\24804c086cd28be1795eed24e60d214f *g:\\forensic_tools\\NET.EXE
\40b3d919e08b5ebcd4b44eb369e169f8 *g:\\forensic_tools\\NETSTAT.EXE
\b485fef42ca1d659ecb41b88aca9de72 *g:\\forensic_tools\\NTFSINFO.EXE
\1128a558328023f6006327570c4d201f *g:\\forensic_tools\\NTLast.exe
\f996fc1c349793c8c78a5877bbc95538 *g:\\forensic_tools\\NTPMON.EXE
\ce2a33505a81936c7056a111ac01f9c4 *g:\\forensic_tools\\od.exe
\a67eda792c12d5793522d9cf26f9f1d1 *g:\\forensic_tools\\patchit.exe
\8eddf8f2db452b6dba8fbce35c464131 *g:\\forensic_tools\\pd.exe
\d09011bc7af7aae3b0b2f3011e1cc2a4 *g:\\forensic_tools\\pdd.exe
\f989d12eb87df1342a917792a77e6053 *g:\\forensic_tools\\pslist.exe
\9c6d6542908a8fec64063489344722c5 *g:\\forensic_tools\\psservice.exe
\32913dec9ff17aa115383bf1805265b2 *g:\\forensic_tools\\RITEDISK.EXE
\959541bc0790abdc097753324bbf5466 *g:\\forensic_tools\\rl.exe
\f35a2eb2e0db54b7d3bb55f17f11df62 *g:\\forensic_tools\\rm.exe
\0360513d6994bdda673d596aee43bbbd *g:\\forensic_tools\\rmdir.exe

\a56b39b43b7b9d676d6463e268b415f1 *g:\\forensic_tools\\rsh.exe
\df8bc69d9f501a0e88c9814011267753 *g:\\forensic_tools\\rsync.exe
\83c7b69ca4bb9e46448377d3012e49c2 *g:\\forensic_tools\\scp.exe
\c9bfe75941cabe2a90036b6d60007e02 *g:\\forensic_tools\\sdiff.exe
\56d8cc07aee23211942a79c652f180d6 *g:\\forensic_tools\\sed.exe
\88d999319a87a17b1884224810944e3d *g:\\forensic_tools\\seq.exe
\a21a4542cc132b2ac9cc5df3fff7d980 *g:\\forensic_tools\\service.exe
\6545b392a18bb17ef331dbc19d75a2ae *g:\\forensic_tools\\SFind.exe
\a2f597ba9edba04095fff610217ea7d0 *g:\\forensic_tools\\showin.exe
\21e8140d75ee962a1e87383715b8f4a4 *g:\\forensic_tools\\sid2user.exe
\dc8fdfdd099de41f6d83cd8519ef0d85 *g:\\forensic_tools\\sigs.exe
\63edfc1241bf2a6bbe9b79bff6e7435d *g:\\forensic_tools\\size.exe
\ef13b9506e76689b250c33d4f477035f *g:\\forensic_tools\\sniffer.exe
\bf82b16fa986572f1f2bb9a5a1ec2c04 *g:\\forensic_tools\\sort.exe
\0e4fab08c1cdd8004975b5b0471aa45c *g:\\forensic_tools\\split.exe
\06ecc5909d0fe6e730154a09116dc115 *g:\\forensic_tools\\ssh-add.exe
\41dbed87b7ebeb3cb6c8dfd7c63edb97 *g:\\forensic_tools\\ssh-agent.exe
\304214d274dbebe6592def0aa3f6caa1 *g:\\forensic_tools\\ssh-keygen.exe
\72e11e82dddd4a8abedb509c6e591f43 *g:\\forensic_tools\\ssh-keyscan.exe
\04f37d2a7a8d37d333f369c85818a630 *g:\\forensic_tools\\ssh.exe
\d9dc7e3eafba5f5e1b9819b168d55567 *g:\\forensic_tools\\strace.exe
\9e5f272e010be683bb42430a9609426d *g:\\forensic_tools\\STREAMS.EXE
\c297e8f2fc6744e02d71860cda706458 *g:\\forensic_tools\\strings.exe
\2189f62f76fa18eb73d6fed66747ed65 *g:\\forensic_tools\\strip.exe
\28102bdf7185cd389c9a48bb2b6da197 *g:\\forensic_tools\\tail.exe
\f16165d814d6aa9a6c4439cd166cdfb2 *g:\\forensic_tools\\TCPVIEW.EXE
\c31e927903f01d0776e3691d4b57bd96 *g:\\forensic_tools\\TDIMON.EXE
\a85401fa6f6a895c4b09d18fd4f43960 *g:\\forensic_tools\\TOKENMON.EXE
\5e93eb01a8fb1cb41e03a322080b8250 *g:\\forensic_tools\\touch.exe
\20bfba1e7b6fcce6cf1ddba49c274248 *g:\\forensic_tools\\tput.exe
\f47bc77f558ee1dce1836ab8bd3d71bb *g:\\forensic_tools\\tr.exe
\5c5d3c6e54767bd4b2abc0b8c93ccd18 *g:\\forensic_tools\\umount.exe
\da2a3776404aa24685e0d4092f306420 *g:\\forensic_tools\\uname.exe
\6655b2b14e8eab800bb0cd8689e0d10f *g:\\forensic_tools\\uniq.exe
\bfd530d1972e59768c5c7942c6e8b040 *g:\\forensic_tools\\unzip.exe
\415eda8d64e4b487a78218212f5db282 *g:\\forensic_tools\\uptime.exe
\e59a5b0886a9a7681b247897a2872bcd *g:\\forensic_tools\\user2sid.exe
\754fe4f1f35c193f3080c368320b3890 *g:\\forensic_tools\\volume_dump.exe
\1031e361396a744447ddc9194d16ce2c *g:\\forensic_tools\\walksam.exe
\ed11260ac9099846879329b06c81c0dd *g:\\forensic_tools\\wc.exe
\d8670289a1b781e2dd361c1507321b64 *g:\\forensic_tools\\wget.exe
\81668d19667365f380ff4bfb04453b09 *g:\\forensic_tools\\which.exe
\f1b801b30c27a8c0e2b3c2759a9c043b *g:\\forensic_tools\\whoami.exe
\215449a456f895f15425c82465862816 *g:\\forensic_tools\\WinHex.exe
\0fc7636391a972440973cc827e61fdeb *g:\\forensic_tools\\wipe.exe
\ab41a77f5fbeb9da2701a9a544d6834b *g:\\forensic_tools\\xargs.exe
\fa6dcbda15b99c817db83613050246c5 *g:\\forensic_tools\\zcat.exe
\7f54d7eabaf4a4db146aa52269154329 *g:\\forensic_tools\\zip.exe

Appendix C

ListDLLs V2.23 - DLL lister for Win9x/NT
Copyright (C) 1997-2000 Mark Russinovich
http://www.sysinternals.com

```
--------------------------------------------------------------------------------
System pid: 8
Command line: <no command line>
--------------------------------------------------------------------------------
SMSS.EXE pid: 172
Command line: \SystemRoot\System32\smss.exe

  Base        Size      Version                  Path
  0x48580000  0xe000                 \SystemRoot\System32\smss.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x68010000  0xf0000   5.00.2195.2967  C:\WINNT\System32\sfcfiles.dll
--------------------------------------------------------------------------------
CSRSS.EXE pid: 200
Command line: C:\WINNT\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,3072,512,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2
ProfileControl=Off MaxRequestThreads=16

  Base        Size      Version                  Path
  0x5fff0000  0x4000                \??\C:\WINNT\system32\csrss.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x5ff90000  0xc000    5.00.2195.2581  C:\WINNT\system32\CSRSRV.dll
  0x5ffa0000  0xd000    5.00.2195.2581  C:\WINNT\system32\basesrv.dll
  0x5ffb0000  0x40000   5.00.2195.4121  C:\WINNT\system32\winsrv.dll
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.DLL
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
--------------------------------------------------------------------------------
WINLOGON.EXE pid: 224
Command line: winlogon.exe

  Base        Size      Version                  Path
  0x01000000  0x2e000               \??\C:\WINNT\SYSTEM32\winlogon.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.DLL
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.DLL
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.DLL
  0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\system32\USERENV.DLL
  0x769a0000  0x7000    5.00.2195.3669  C:\WINNT\system32\NDDEAPI.DLL
  0x76980000  0x1b000   5.00.2195.2896  C:\WINNT\system32\SFC.DLL
  0x68010000  0xf0000   5.00.2195.2967  C:\WINNT\system32\sfcfiles.dll
  0x77be0000  0xf000    5.00.2195.2862  C:\WINNT\system32\SECUR32.DLL
  0x690f0000  0xb000    5.00.2181.0001  C:\WINNT\system32\PROFMAP.DLL
  0x75170000  0x4f000   5.00.2195.4153  C:\WINNT\system32\NETAPI32.dll
  0x751c0000  0x6000    5.00.2134.0001  C:\WINNT\system32\NETRAP.DLL
  0x75150000  0x10000   5.00.2195.2780  C:\WINNT\system32\SAMLIB.DLL
  0x75030000  0x13000   5.00.2195.2780  C:\WINNT\system32\WS2_32.DLL
  0x75020000  0x8000    5.00.2134.0001  C:\WINNT\system32\WS2HELP.DLL
  0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.DLL
  0x77980000  0x24000   5.00.2195.4141  C:\WINNT\system32\DNSAPI.DLL
  0x75050000  0x8000    5.00.2195.2871  C:\WINNT\system32\WSOCK32.DLL
  0x65780000  0xc000    5.00.2195.2386  C:\WINNT\SYSTEM32\winsta.dll
  0x77570000  0x30000   5.00.2161.0001  C:\WINNT\SYSTEM32\WINMM.dll
  0x681a0000  0x7000    5.00.2134.0001  C:\WINNT\SYSTEM32\serwvdrv.dll
  0x66740000  0x7000    5.00.2134.0001  C:\WINNT\SYSTEM32\umdmxfrm.dll
  0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\SYSTEM32\setupapi.dll
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.dll
  0x76b90000  0x54000   5.00.2195.2779  C:\WINNT\SYSTEM32\msgina.dll
  0x782f0000  0x242000  5.00.3315.2902  C:\WINNT\system32\SHELL32.DLL
```

```
  0x77c70000  0x4a000   5.00.3502.4373  C:\WINNT\system32\SHLWAPI.DLL
  0x76930000  0x2b000   5.131.2195.2779  C:\WINNT\system32\wintrust.dll
  0x77440000  0x75000   5.131.2195.2833  C:\WINNT\system32\CRYPT32.dll
  0x77430000  0x10000   5.00.2195.4067  C:\WINNT\system32\MSASN1.DLL
  0x77920000  0x23000   5.00.2195.2778  C:\WINNT\system32\IMAGEHLP.dll
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\ole32.dll
  0x76a00000  0x5000    5.131.2134.0001  C:\WINNT\system32\mscat32.dll
  0x7ca00000  0x23000   5.00.2195.2228  C:\WINNT\SYSTEM32\rsaenh.dll
  0x77560000  0x9000    5.00.2195.2669  C:\WINNT\SYSTEM32\wdmaud.drv
  0x77820000  0x7000    5.00.2134.0001  C:\WINNT\system32\VERSION.dll
  0x759b0000  0x6000    5.00.2134.0001  C:\WINNT\system32\LZ32.DLL
  0x770c0000  0x23000   5.00.2195.2401  C:\WINNT\SYSTEM32\cscdll.dll
  0x76920000  0xf000    5.00.2195.2780  C:\WINNT\SYSTEM32\WlNotify.dll
  0x76960000  0x17000   5.00.2134.0001  C:\WINNT\SYSTEM32\WINSCARD.DLL
  0x77800000  0x1d000   5.00.2195.2780  C:\WINNT\SYSTEM32\WINSPOOL.DRV
  0x77840000  0x3c000   5.00.2195.2959  C:\WINNT\SYSTEM32\cscui.dll
  0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.DLL
  0x775a0000  0x85000   2000.02.3488.0000  C:\WINNT\System32\CLBCATQ.DLL
  0x782d0000  0x1e000   5.00.2195.4436  C:\WINNT\system32\msv1_0.dll
  0x77400000  0x8000    5.00.2134.0001  C:\WINNT\SYSTEM32\msacm32.drv
  0x77410000  0x13000   5.00.2134.0001  C:\WINNT\SYSTEM32\MSACM32.dll
--------------------------------------------------------------------------------
SERVICES.EXE pid: 252
Command line: C:\WINNT\system32\services.exe

  Base        Size      Version                  Path
  0x01000000  0x18000   5.00.2195.2780  C:\WINNT\system32\services.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.DLL
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.DLL
  0x75170000  0x4f000   5.00.2195.4153  C:\WINNT\system32\NETAPI32.DLL
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.DLL
  0x77be0000  0xf000    5.00.2195.2862  C:\WINNT\system32\SECUR32.DLL
  0x751c0000  0x6000    5.00.2134.0001  C:\WINNT\system32\NETRAP.DLL
  0x75150000  0x10000   5.00.2195.2780  C:\WINNT\system32\SAMLIB.DLL
  0x75030000  0x13000   5.00.2195.2780  C:\WINNT\system32\WS2_32.DLL
  0x75020000  0x8000    5.00.2134.0001  C:\WINNT\system32\WS2HELP.DLL
  0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.DLL
  0x77980000  0x24000   5.00.2195.4141  C:\WINNT\system32\DNSAPI.DLL
  0x75050000  0x8000    5.00.2195.2871  C:\WINNT\system32\WSOCK32.DLL
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x767a0000  0x18000   5.00.2182.0001  C:\WINNT\system32\UMPNPMGR.DLL
  0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\system32\USERENV.DLL
  0x76460000  0x40000   5.00.2195.3649  C:\WINNT\system32\SCESRV.DLL
  0x77bf0000  0x11000   5.00.2195.2661  C:\WINNT\system32\NTDSAPI.DLL
  0x76890000  0xe000    5.00.2178.0001  C:\WINNT\system32\eventlog.dll
  0x77360000  0x19000   5.00.2195.2778  C:\WINNT\system32\dhcpcsvc.dll
  0x77520000  0x5000    5.00.2134.0001  C:\WINNT\system32\ICMP.DLL
  0x77340000  0x13000   5.00.2173.0002  C:\WINNT\system32\IPHLPAPI.DLL
  0x77320000  0x17000   5.00.2181.0001  C:\WINNT\system32\MPRAPI.DLL
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\OLE32.DLL
  0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.DLL
  0x773b0000  0x2e000   5.00.2195.2778  C:\WINNT\system32\ACTIVEDS.DLL
  0x77380000  0x22000   5.00.2195.4308  C:\WINNT\system32\ADSLDPC.DLL
  0x77830000  0xe000    5.00.2168.0001  C:\WINNT\system32\RTUTILS.DLL
  0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\system32\SETUPAPI.DLL
  0x774e0000  0x32000   5.00.2195.2671  C:\WINNT\system32\RASAPI32.DLL
  0x774c0000  0x11000   5.00.2195.2780  C:\WINNT\system32\RASMAN.DLL
  0x77530000  0x22000   5.00.2182.0001  C:\WINNT\system32\TAPI32.DLL
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.DLL
```

0x77c70000 0x4a000 5.00.3502.4373 C:\WINNT\system32\SHLWAPI.DLL
0x775a0000 0x85000 2000.02.3488.0000 C:\WINNT\system32\CLBCATQ.DLL
0x768a0000 0x19000 5.00.2195.4379 C:\WINNT\system32\dnsrslvr.dll
0x76880000 0x6000 5.00.2195.2778 C:\WINNT\system32\lmhsvc.dll
0x65780000 0xc000 5.00.2195.2386 C:\WINNT\system32\WINSTA.DLL
0x70170000 0x11a000 6.00.3940.0013 C:\WINNT\system32\ESENT.dll
0x768c0000 0x6000 2195.2778.0297.0003 C:\WINNT\system32\dmserver.dll
0x770b0000 0x7000 5.00.2134.0001 C:\WINNT\system32\CFGMGR32.DLL
0x767e0000 0x16000 5.00.2195.2904 C:\WINNT\system32\Srvsvc.dll
0x77800000 0x1d000 5.00.2195.2780 C:\WINNT\system32\WINSPOOL.DRV
0x76770000 0x1a000 5.00.2195.2780 C:\WINNT\system32\wkssvc.dll
0x76670000 0xe000 5.00.2135.0001 C:\WINNT\system32\CRYPTDLL.DLL
0x768d0000 0x12000 5.00.2181.0001 C:\WINNT\system32\cryptsvc.dll
0x76850000 0x1f000 5.00.2195.2779 C:\WINNT\system32\psbase.dll
0x7ca00000 0x23000 5.00.2195.2228 C:\WINNT\system32\rsaenh.dll
0x77440000 0x75000 5.131.2195.2833 C:\WINNT\system32\CRYPT32.dll
0x77430000 0x10000 5.00.2195.4067 C:\WINNT\system32\MSASN1.DLL
0x76800000 0x7000 5.00.2135.0001 C:\WINNT\system32\seclogon.dll
0x66b70000 0x10000 5.00.2195.3753 C:\WINNT\system32\trksvr.dll
0x767c0000 0x19000 5.00.2166.0001 C:\WINNT\system32\trkwks.dll
0x74ff0000 0x12000 5.00.2195.2871 C:\WINNT\system32\mswsock.dll
0x74fd0000 0x1f000 5.00.2195.2779 C:\WINNT\system32\msafd.dll
0x75010000 0x7000 5.00.2195.2104 C:\WINNT\System32\wshtcpip.dll
0x785c0000 0xc000 5.00.2195.2871 C:\WINNT\System32\rnr20.dll
0x777e0000 0x8000 5.00.2160.0001 C:\WINNT\System32\winrnr.dll
0x777f0000 0x5000 5.00.2168.0001 C:\WINNT\system32\rasadhlp.dll
0x74b40000 0x8000 5.00.2134.0001 C:\WINNT\system32\alrsvc.dll
0x768f0000 0xf000 5.00.2195.2778 C:\WINNT\system32\browser.dll
0x76870000 0xb000 5.00.2195.2939 C:\WINNT\system32\msgsvc.dll
0x76750000 0x15000 5.00.2195.2842 C:\WINNT\system32\wmicore.dll

---

LSASS.EXE pid: 264
Command line: C:\WINNT\system32\lsass.exe

Base Size Version Path
0x01000000 0xa000 5.00.2195.4436 C:\WINNT\system32\lsass.exe
0x77f80000 0x7b000 5.00.2195.2779 C:\WINNT\System32\ntdll.dll
0x77e80000 0xb5000 5.00.2195.4272 C:\WINNT\system32\KERNEL32.dll
0x78540000 0x7f000 5.00.2195.4436 C:\WINNT\system32\LSASRV.dll
0x78000000 0x46000 6.01.9359.0000 C:\WINNT\system32\MSVCRT.DLL
0x76670000 0xe000 5.00.2135.0001 C:\WINNT\system32\CRYPTDLL.DLL
0x77db0000 0x5c000 5.00.2195.4453 C:\WINNT\system32\ADVAPI32.DLL
0x77d40000 0x70000 5.00.2195.4266 C:\WINNT\system32\RPCRT4.DLL
0x77be0000 0xf000 5.00.2195.2862 C:\WINNT\system32\SECUR32.DLL
0x77e10000 0x64000 5.00.2195.4314 C:\WINNT\system32\USER32.DLL
0x77f40000 0x3c000 5.00.2195.3914 C:\WINNT\system32\GDI32.DLL
0x77cc0000 0x60000 5.00.2195.4453 C:\WINNT\system32\SAMSRV.DLL
0x77980000 0x24000 5.00.2195.4141 C:\WINNT\system32\DNSAPI.DLL
0x75050000 0x8000 5.00.2195.2871 C:\WINNT\system32\WSOCK32.DLL
0x75030000 0x13000 5.00.2195.2780 C:\WINNT\system32\WS2_32.DLL
0x75020000 0x8000 5.00.2134.0001 C:\WINNT\system32\WS2HELP.DLL
0x77430000 0x10000 5.00.2195.4067 C:\WINNT\system32\MSASN1.DLL
0x75170000 0x4f000 5.00.2195.4153 C:\WINNT\system32\NETAPI32.DLL
0x751c0000 0x6000 5.00.2134.0001 C:\WINNT\system32\NETRAP.DLL
0x75150000 0x10000 5.00.2195.2780 C:\WINNT\system32\SAMLIB.DLL
0x77950000 0x2a000 5.00.2195.4436 C:\WINNT\system32\WLDAP32.DLL
0x765e0000 0xd000 5.00.2154.0001 C:\WINNT\system32\msprivs.dll
0x78280000 0x34000 5.00.2195.4439 C:\WINNT\system32\kerberos.dll
0x782d0000 0x1e000 5.00.2195.4436 C:\WINNT\system32\msv1_0.dll
0x76580000 0x5d000 5.00.2195.4357 C:\WINNT\system32\netlogon.dll
0x77bf0000 0x11000 5.00.2195.2661 C:\WINNT\system32\NTDSAPI.DLL
0x78160000 0x26000 5.01.2195.0000 C:\WINNT\system32\schannel.dll

0x77440000 0x75000 5.131.2195.2833 C:\WINNT\system32\CRYPT32.DLL
0x77c10000 0x5e000 5.00.2195.4345 C:\WINNT\system32\USERENV.DLL
0x7ca00000 0x22000 5.00.2195.2228 C:\WINNT\system32\rsabase.dll
0x77a50000 0xf6000 5.00.2195.4439 C:\WINNT\system32\ole32.dll
0x75090000 0x10000 5.00.2195.2779 C:\WINNT\system32\mpr.dll
0x77880000 0x8d000 5.00.2195.2663 C:\WINNT\system32\setupapi.dll
0x77b50000 0x89000 5.81.3103.1000 C:\WINNT\system32\COMCTL32.dll
0x68b20000 0x9000 5.00.2195.2671 C:\WINNT\system32\RASSFM.dll
0x77320000 0x17000 5.00.2181.0001 C:\WINNT\system32\MPRAPI.dll
0x779b0000 0x9b000 2.40.4517.0000 C:\WINNT\system32\OLEAUT32.DLL
0x773b0000 0x2e000 5.00.2195.2778 C:\WINNT\system32\ACTIVEDS.DLL
0x77380000 0x22000 5.00.2195.4308 C:\WINNT\system32\ADSLDPC.DLL
0x77830000 0xe000 5.00.2168.0001 C:\WINNT\system32\RTUTILS.DLL
0x68000000 0xd000 5.00.2134.0001 C:\WINNT\system32\SFMAPI.dll
0x775a0000 0x85000 2000.02.3488.0000 C:\WINNT\system32\CLBCATQ.DLL
0x6cef0000 0x26000 5.00.2195.4450 C:\WINNT\system32\KDCSVC.dll
0x75770000 0xfb000 5.00.2195.4445 C:\WINNT\system32\NTDSA.DLL
0x755f0000 0xb000 5.00.2195.2878 C:\WINNT\system32\NTDSATQ.DLL
0x74ff0000 0x12000 5.00.2195.2871 C:\WINNT\system32\MSWSOCK.DLL
0x70170000 0x11a000 6.00.3940.0013 C:\WINNT\system32\ESENT.DLL
0x75570000 0x24000 5.00.2195.2778 C:\WINNT\system32\CERTCLI.DLL
0x773e0000 0x12000 3.00.8449.0000 C:\WINNT\system32\ATL.DLL
0x76430000 0x1e000 5.00.2195.4117 C:\WINNT\system32\scecli.dll
0x764e0000 0x1e000 5.00.2183.0001 C:\WINNT\system32\polagent.dll
0x76fb0000 0xf2000 6.00.8665.0000 C:\WINNT\system32\MFC42U.DLL
0x76500000 0x77000 5.00.2195.2785 C:\WINNT\system32\OAKLEY.DLL
0x77340000 0x13000 5.00.2173.0002 C:\WINNT\system32\IPHLPAPI.DLL
0x77520000 0x5000 5.00.2134.0001 C:\WINNT\system32\ICMP.DLL
0x774e0000 0x32000 5.00.2195.2671 C:\WINNT\system32\RASAPI32.DLL
0x774c0000 0x11000 5.00.2195.2780 C:\WINNT\system32\RASMAN.DLL
0x77530000 0x22000 5.00.2182.0001 C:\WINNT\system32\TAPI32.DLL
0x77c70000 0x4a000 5.00.3502.4373 C:\WINNT\system32\SHLWAPI.DLL
0x77360000 0x19000 5.00.2195.2778 C:\WINNT\system32\DHCPCSVC.DLL
0x74fd0000 0x1f000 5.00.2195.2779 C:\WINNT\system32\msafd.dll
0x75010000 0x7000 5.00.2195.2104 C:\WINNT\System32\wshtcpip.dll
0x00910000 0x23000 5.00.2195.2228 C:\WINNT\system32\rsaenh.dll
0x67400000 0x27000 5.00.2195.2228 C:\WINNT\system32\dssenh.dll

---

termsrv.exe pid: 384
Command line: C:\WINNT\System32\termsrv.exe

Base	Size	Version	Path
0x01000000	0x27000	5.00.2195.3895	C:\WINNT\System32\termsrv.exe
0x77f80000	0x7b000	5.00.2195.2779	C:\WINNT\System32\ntdll.dll
0x77db0000	0x5c000	5.00.2195.4453	C:\WINNT\system32\ADVAPI32.dll
0x77e80000	0xb5000	5.00.2195.4272	C:\WINNT\system32\KERNEL32.DLL
0x77d40000	0x70000	5.00.2195.4266	C:\WINNT\system32\RPCRT4.DLL
0x68a80000	0xb000	5.00.2155.0001	C:\WINNT\System32\REGAPI.dll
0x78000000	0x46000	6.01.9359.0000	C:\WINNT\system32\MSVCRT.dll
0x75150000	0x10000	5.00.2195.2780	C:\WINNT\System32\SAMLIB.dll
0x77e10000	0x64000	5.00.2195.4314	C:\WINNT\system32\USER32.dll
0x77f40000	0x3c000	5.00.2195.3914	C:\WINNT\system32\GDI32.DLL
0x75170000	0x4f000	5.00.2195.4153	C:\WINNT\System32\NETAPI32.dll
0x77be0000	0xf000	5.00.2195.2862	C:\WINNT\System32\SECUR32.DLL
0x751c0000	0x6000	5.00.2134.0001	C:\WINNT\System32\NETRAP.DLL
0x75030000	0x13000	5.00.2195.2780	C:\WINNT\System32\WS2_32.DLL
0x75020000	0x8000	5.00.2134.0001	C:\WINNT\System32\WS2HELP.DLL
0x77950000	0x2a000	5.00.2195.4436	C:\WINNT\system32\WLDAP32.DLL
0x77980000	0x24000	5.00.2195.4141	C:\WINNT\System32\DNSAPI.DLL
0x75050000	0x8000	5.00.2195.2871	C:\WINNT\System32\WSOCK32.DLL
0x65780000	0xc000	5.00.2195.2386	C:\WINNT\System32\WINSTA.dll
0x6ea50000	0x22000	5.00.2195.3895	C:\WINNT\System32\ICAAPI.dll

```
  0x6ac10000  0xa000    5.00.2195.3895  C:\WINNT\System32\mstlsapi.dll
  0x773b0000  0x2e000   5.00.2195.2778  C:\WINNT\System32\ACTIVEDS.dll
  0x77380000  0x22000   5.00.2195.4308  C:\WINNT\System32\ADSLDPC.DLL
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\OLE32.DLL
  0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.DLL
  0x77bf0000  0x11000   5.00.2195.2661  C:\WINNT\System32\NTDSAPI.dll
  0x77440000  0x75000   5.131.2195.2833  C:\WINNT\System32\CRYPT32.dll
  0x77430000  0x10000   5.00.2195.4067  C:\WINNT\System32\MSASN1.DLL
  0x77920000  0x23000   5.00.2195.2778  C:\WINNT\system32\IMAGEHLP.dll
  0x77820000  0x7000    5.00.2134.0001  C:\WINNT\system32\VERSION.dll
  0x759b0000  0x6000    5.00.2134.0001  C:\WINNT\system32\LZ32.DLL
  0x756e0000  0x5000    5.00.2195.4450  C:\WINNT\System32\ntlsapi.dll
  0x775a0000  0x85000   2000.02.3488.0000  C:\WINNT\System32\CLBCATQ.DLL
  0x7ca00000  0x22000   5.00.2195.2228  C:\WINNT\System32\rsabase.dll
  0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\System32\USERENV.dll
  0x782f0000  0x242000  5.00.3315.2902  C:\WINNT\system32\shell32.dll
  0x77c70000  0x4a000   5.00.3502.4373  C:\WINNT\system32\SHLWAPI.DLL
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.DLL
  0x68a60000  0x1b000   5.00.2195.4307  C:\WINNT\System32\rdpwsx.dll
  0x77800000  0x1d000   5.00.2195.2780  C:\WINNT\System32\WINSPOOL.DRV
--------------------------------------------------------------------------------
svchost.exe pid: 472
Command line: C:\WINNT\system32\svchost -k rpcss

  Base        Size      Version                  Path
  0x01000000  0x5000    5.00.2134.0001  C:\WINNT\system32\svchost.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.DLL
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.DLL
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\OLE32.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.DLL
  0x76190000  0x3d000   5.00.2195.4445  c:\winnt\system32\rpcss.dll
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.DLL
  0x77c10000  0x5e000   5.00.2195.4345  c:\winnt\system32\USERENV.DLL
  0x75030000  0x13000   5.00.2195.2780  c:\winnt\system32\WS2_32.DLL
  0x75020000  0x8000    5.00.2134.0001  c:\winnt\system32\WS2HELP.DLL
  0x77be0000  0xf000    5.00.2195.2862  c:\winnt\system32\SECUR32.DLL
  0x74ff0000  0x12000   5.00.2195.2871  C:\WINNT\system32\mswsock.dll
  0x77980000  0x24000   5.00.2195.4141  C:\WINNT\system32\DNSAPI.DLL
  0x75050000  0x8000    5.00.2195.2871  C:\WINNT\system32\WSOCK32.DLL
  0x74fd0000  0x1f000   5.00.2195.2779  C:\WINNT\system32\msafd.dll
  0x75010000  0x7000    5.00.2195.2104  C:\WINNT\System32\wshtcpip.dll
  0x785c0000  0xc000    5.00.2195.2871  C:\WINNT\System32\rnr20.dll
  0x77340000  0x13000   5.00.2173.0002  C:\WINNT\system32\iphlpapi.dll
  0x77520000  0x5000    5.00.2134.0001  C:\WINNT\system32\ICMP.DLL
  0x77320000  0x17000   5.00.2181.0001  C:\WINNT\system32\MPRAPI.DLL
  0x75150000  0x10000   5.00.2195.2780  C:\WINNT\system32\SAMLIB.DLL
  0x75170000  0x4f000   5.00.2195.4153  C:\WINNT\system32\NETAPI32.DLL
  0x751c0000  0x6000    5.00.2134.0001  C:\WINNT\system32\NETRAP.DLL
  0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.DLL
  0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.DLL
  0x773b0000  0x2e000   5.00.2195.2778  C:\WINNT\system32\ACTIVEDS.DLL
  0x77380000  0x22000   5.00.2195.4308  C:\WINNT\system32\ADSLDPC.DLL
  0x77830000  0xe000    5.00.2168.0001  C:\WINNT\system32\RTUTILS.DLL
  0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\system32\SETUPAPI.DLL
  0x774e0000  0x32000   5.00.2195.2671  C:\WINNT\system32\RASAPI32.DLL
  0x774c0000  0x11000   5.00.2195.2780  C:\WINNT\system32\RASMAN.DLL
  0x77530000  0x22000   5.00.2182.0001  C:\WINNT\system32\TAPI32.DLL
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.DLL
  0x77c70000  0x4a000   5.00.3502.4373  C:\WINNT\system32\SHLWAPI.DLL
```

0x77360000 0x19000 5.00.2195.2778 C:\WINNT\system32\DHCPCSVC.DLL
0x775a0000 0x85000 2000.02.3488.0000 C:\WINNT\system32\CLBCATQ.DLL
0x777e0000 0x8000 5.00.2160.0001 C:\WINNT\System32\winrnr.dll
0x777f0000 0x5000 5.00.2168.0001 C:\WINNT\system32\rasadhlp.dll
0x782d0000 0x1e000 5.00.2195.4436 C:\WINNT\system32\msv1_0.dll

---

svchost.exe pid: 516
Command line: C:\WINNT\System32\svchost.exe -k netsvcs

Base Size Version Path
0x01000000 0x5000 5.00.2134.0001 C:\WINNT\System32\svchost.exe
0x77f80000 0x7b000 5.00.2195.2779 C:\WINNT\System32\ntdll.dll
0x77db0000 0x5c000 5.00.2195.4453 C:\WINNT\system32\ADVAPI32.DLL
0x77e80000 0xb5000 5.00.2195.4272 C:\WINNT\system32\KERNEL32.DLL
0x77d40000 0x70000 5.00.2195.4266 C:\WINNT\system32\RPCRT4.DLL
0x77a50000 0xf6000 5.00.2195.4439 C:\WINNT\system32\OLE32.DLL
0x77f40000 0x3c000 5.00.2195.3914 C:\WINNT\system32\GDI32.DLL
0x77e10000 0x64000 5.00.2195.4314 C:\WINNT\system32\USER32.DLL
0x6d7b0000 0x16000 5.00.2195.2104 c:\winnt\system32\irmon.dll
0x78000000 0x46000 6.01.9359.0000 C:\WINNT\system32\MSVCRT.dll
0x782f0000 0x242000 5.00.3315.2902 C:\WINNT\system32\SHELL32.dll
0x77c70000 0x4a000 5.00.3502.4373 C:\WINNT\system32\SHLWAPI.DLL
0x77b50000 0x89000 5.81.3103.1000 C:\WINNT\system32\COMCTL32.DLL
0x75030000 0x13000 5.00.2195.2780 c:\winnt\system32\WS2_32.dll
0x75020000 0x8000 5.00.2134.0001 c:\winnt\system32\WS2HELP.DLL
0x77880000 0x8d000 5.00.2195.2663 c:\winnt\system32\SETUPAPI.dll
0x77c10000 0x5e000 5.00.2195.4345 c:\winnt\system32\USERENV.DLL
0x74ff0000 0x12000 5.00.2195.2871 c:\winnt\system32\MSWSOCK.dll
0x77980000 0x24000 5.00.2195.4141 c:\winnt\system32\DNSAPI.DLL
0x75050000 0x8000 5.00.2195.2871 c:\winnt\system32\WSOCK32.DLL
0x74fd0000 0x1f000 5.00.2195.2779 C:\WINNT\system32\msafd.dll
0x655f0000 0x5000 5.00.2195.2104 C:\WINNT\System32\wshirda.dll
0x77be0000 0xf000 5.00.2195.2862 C:\WINNT\System32\secur32.dll
0x782d0000 0x1e000 5.00.2195.4436 C:\WINNT\system32\msv1_0.dll
0x76290000 0x3b000 2000.02.3488.0000 c:\winnt\system32\es.dll
0x6de80000 0x63000 2000.02.3488.0000 c:\winnt\system32\TXFAUX.DLL
0x779b0000 0x9b000 2.40.4517.0000 C:\WINNT\system32\OLEAUT32.DLL
0x761d0000 0x64000 5.00.2195.2779 c:\winnt\system32\ntmssvc.dll
0x775a0000 0x85000 2000.02.3488.0000 C:\WINNT\System32\CLBCATQ.DLL
0x76180000 0xc000 5.00.2163.0001 c:\winnt\system32\sens.dll
0x773e0000 0x12000 3.00.8449.0000 C:\WINNT\System32\ATL.DLL
0x76240000 0x2c000 5.00.2195.2779 C:\WINNT\System32\NTMSDBA.dll
0x75710000 0x29000 5.00.2195.2728 c:\winnt\system32\rasmans.dll
0x77830000 0xe000 5.00.2168.0001 c:\winnt\system32\rtutils.dll
0x77440000 0x75000 5.131.2195.2833 c:\winnt\system32\CRYPT32.dll
0x77430000 0x10000 5.00.2195.4067 c:\winnt\system32\MSASN1.DLL
0x6a4b0000 0x89000 5.00.2195.2228 c:\winnt\system32\netcfgx.dll
0x774e0000 0x32000 5.00.2195.2671 c:\winnt\system32\RASAPI32.dll
0x774c0000 0x11000 5.00.2195.2780 c:\winnt\system32\RASMAN.DLL
0x77530000 0x22000 5.00.2182.0001 c:\winnt\system32\TAPI32.DLL
0x75870000 0x83000 5.00.2195.2671 c:\winnt\system32\RASDLG.dll
0x77320000 0x17000 5.00.2181.0001 c:\winnt\system32\MPRAPI.dll
0x75150000 0x10000 5.00.2195.2780 c:\winnt\system32\SAMLIB.DLL
0x75170000 0x4f000 5.00.2195.4153 c:\winnt\system32\NETAPI32.DLL
0x751c0000 0x6000 5.00.2134.0001 c:\winnt\system32\NETRAP.DLL
0x77950000 0x2a000 5.00.2195.4436 C:\WINNT\system32\WLDAP32.DLL
0x773b0000 0x2e000 5.00.2195.2778 c:\winnt\system32\ACTIVEDS.DLL
0x77380000 0x22000 5.00.2195.4308 c:\winnt\system32\ADSLDPC.DLL
0x77360000 0x19000 5.00.2195.2778 C:\WINNT\System32\dhcpcsvc.dll
0x77520000 0x5000 5.00.2134.0001 C:\WINNT\System32\ICMP.DLL
0x77340000 0x13000 5.00.2173.0002 C:\WINNT\System32\IPHLPAPI.DLL
0x76270000 0x19000 5.00.2195.2779 c:\winnt\system32\netman.dll

```
  0x76f20000  0x75000   5.00.2195.2779  C:\WINNT\system32\NETSHELL.dll
  0x76110000  0x4000    5.00.2191.0001  C:\WINNT\System32\WMI.dll
  0x75010000  0x7000    5.00.2195.2104  C:\WINNT\System32\wshtcpip.dll
--------------------------------------------------------------------------------
mwmdmsvc.exe pid: 564
Command line: C:\WINNT\MWW32\MANAGER\MWMDMSVC.EXE

  Base        Size      Version                   Path
  0x00400000  0x10000   2.60.0035.0000  C:\WINNT\MWW32\MANAGER\MWMDMSVC.EXE
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x10000000  0xc000    2.60.0035.0000  C:\WINNT\MWWDMHLP.dll
  0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\SYSTEM32\SETUPAPI.dll
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.DLL
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.DLL
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.DLL
  0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\SYSTEM32\USERENV.DLL
  0x770b0000  0x7000    5.00.2134.0001  C:\WINNT\SYSTEM32\CFGMGR32.dll
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.dll
--------------------------------------------------------------------------------
mwssw32.exe pid: 588
Command line:  -2147483648

  Base        Size      Version                   Path
  0x00400000  0xb000    2.60.0035.0000  C:\WINNT\MWW32\MANAGER\MWSSW32.EXE
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x10000000  0x1a000   2.60.0035.0000  C:\WINNT\MWCLW32.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.dll
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.dll
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x011c0000  0x24000   2.60.0035.0000  C:\WINNT\MWW32\MODEM\MWMW32.DLL
  0x011f0000  0x2d000   2.60.0035.0000  C:\WINNT\MWW32\MODEM\MWMPW32.dll
  0x10030000  0x22000   2.60.0035.0000  C:\WINNT\MWW32\MANAGER\mwave.dll
  0x01220000  0x24000   2.60.0035.0000  C:\WINNT\MWW32\MANAGER\mwavesrv.dll
  0x01250000  0xc000    2.60.0035.0000  C:\WINNT\MWWDMHLP.dll
  0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\System32\SETUPAPI.dll
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.DLL
  0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\System32\USERENV.DLL
  0x770b0000  0x7000    5.00.2134.0001  C:\WINNT\System32\CFGMGR32.dll
  0x01260000  0x45000   2.60.0035.0000  C:\WINNT\MWW32\MODEM\MWMLW32.dll
  0x012b0000  0x14000   2.60.0035.0000  C:\WINNT\MWW32\MODEM\MWBLW32.dll
  0x012d0000  0x20000   2.60.0035.0000  C:\WINNT\MWW32\MODEM\MWWTT32.dll
  0x012f0000  0xc000    2.60.0035.0000  C:\WINNT\MWW32\MODEM\MWCNAM32.dll
  0x01300000  0xc000    2.60.0035.0000  C:\WINNT\MWW32\MANAGER\MEI32API.dll
  0x76b30000  0x3e000   5.00.3103.1000  C:\WINNT\system32\comdlg32.dll
  0x77c70000  0x4a000   5.00.3502.4373  C:\WINNT\system32\SHLWAPI.DLL
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.DLL
  0x782f0000  0x242000  5.00.3315.2902  C:\WINNT\system32\SHELL32.DLL
  0x77570000  0x30000   5.00.2161.0001  C:\WINNT\System32\WINMM.dll
  0x681a0000  0x7000    5.00.2134.0001  C:\WINNT\System32\serwvdrv.dll
  0x66740000  0x7000    5.00.2134.0001  C:\WINNT\System32\umdmxfrm.dll
  0x03e40000  0xe000    2.60.0035.0000  C:\WINNT\MWW32\MODEM\MWMMW32.DLL
  0x04360000  0x1a000   2.60.0035.0000  C:\WINNT\MWW32\MANAGER\meiw0439.dll
--------------------------------------------------------------------------------
msdtc.exe pid: 612
Command line: C:\WINNT\System32\msdtc.exe

  Base        Size      Version                   Path
```

```
  0x00400000  0x4000    1999.09.3421.0003  C:\WINNT\System32\msdtc.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.dll
  0x730a0000  0x126000  2000.02.3488.0000  C:\WINNT\System32\MSDTCTM.dll
  0x6de80000  0x63000   2000.02.3488.0000  C:\WINNT\System32\TxfAux.Dll
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.dll
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\ole32.dll
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.DLL
  0x68c60000  0xaf000   2000.02.3488.0000  C:\WINNT\System32\MSDTCPRX.dll
  0x6a7a0000  0x10000   2000.02.3488.0000  C:\WINNT\System32\MTXCLU.DLL
  0x77820000  0x7000    5.00.2134.0001  C:\WINNT\system32\VERSION.dll
  0x759b0000  0x6000    5.00.2134.0001  C:\WINNT\system32\LZ32.DLL
  0x75050000  0x8000    5.00.2195.2871  C:\WINNT\System32\WSOCK32.dll
  0x75030000  0x13000   5.00.2195.2780  C:\WINNT\System32\WS2_32.DLL
  0x75020000  0x8000    5.00.2134.0001  C:\WINNT\System32\WS2HELP.DLL
  0x6b6f0000  0x19000   1999.09.3421.0003  C:\WINNT\System32\MSDTCLOG.dll
  0x65450000  0x8000    1999.09.3421.0003  C:\WINNT\System32\XOLEHLP.dll
  0x74ff0000  0x12000   5.00.2195.2871  C:\WINNT\System32\MSWSOCK.dll
  0x77980000  0x24000   5.00.2195.4141  C:\WINNT\System32\DNSAPI.DLL
  0x77570000  0x30000   5.00.2161.0001  C:\WINNT\System32\WINMM.dll
  0x780c0000  0x8d000   5.00.0000.7051  C:\WINNT\System32\MSVCP50.dll
  0x73930000  0x10000   5.00.2195.2104  C:\WINNT\System32\CLUSAPI.DLL
  0x689d0000  0xd000    5.00.2195.2787  C:\WINNT\System32\RESUTILS.DLL
  0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\System32\USERENV.dll
  0x681a0000  0x7000    5.00.2134.0001  C:\WINNT\System32\serwvdrv.dll
  0x66740000  0x7000    5.00.2134.0001  C:\WINNT\System32\umdmxfrm.dll
  0x76810000  0x23000   2000.02.3488.0000  C:\WINNT\System32\MTxOCI.Dll
  0x74fd0000  0x1f000   5.00.2195.2779  C:\WINNT\system32\msafd.dll
  0x75010000  0x7000    5.00.2195.2104  C:\WINNT\System32\wshtcpip.dll
  0x785c0000  0xc000    5.00.2195.2871  C:\WINNT\System32\rnr20.dll
  0x77340000  0x13000   5.00.2173.0002  C:\WINNT\System32\iphlpapi.dll
  0x77520000  0x5000    5.00.2134.0001  C:\WINNT\System32\ICMP.DLL
  0x77320000  0x17000   5.00.2181.0001  C:\WINNT\System32\MPRAPI.DLL
  0x75150000  0x10000   5.00.2195.2780  C:\WINNT\System32\SAMLIB.DLL
  0x75170000  0x4f000   5.00.2195.4153  C:\WINNT\System32\NETAPI32.DLL
  0x77be0000  0xf000    5.00.2195.2862  C:\WINNT\System32\SECUR32.DLL
  0x751c0000  0x6000    5.00.2134.0001  C:\WINNT\System32\NETRAP.DLL
  0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.DLL
  0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.DLL
  0x773b0000  0x2e000   5.00.2195.2778  C:\WINNT\System32\ACTIVEDS.DLL
  0x77380000  0x22000   5.00.2195.4308  C:\WINNT\System32\ADSLDPC.DLL
  0x77830000  0xe000    5.00.2168.0001  C:\WINNT\System32\RTUTILS.DLL
  0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\System32\SETUPAPI.DLL
  0x774e0000  0x32000   5.00.2195.2671  C:\WINNT\System32\RASAPI32.DLL
  0x774c0000  0x11000   5.00.2195.2780  C:\WINNT\System32\RASMAN.DLL
  0x77530000  0x22000   5.00.2182.0001  C:\WINNT\System32\TAPI32.DLL
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.DLL
  0x77c70000  0x4a000   5.00.3502.4373  C:\WINNT\system32\SHLWAPI.DLL
  0x77360000  0x19000   5.00.2195.2778  C:\WINNT\System32\DHCPCSVC.DLL
  0x775a0000  0x85000   2000.02.3488.0000  C:\WINNT\System32\CLBCATQ.DLL
  0x777e0000  0x8000    5.00.2160.0001  C:\WINNT\System32\winrnr.dll
  0x777f0000  0x5000    5.00.2168.0001  C:\WINNT\System32\rasadhlp.dll
--------------------------------------------------------------------------------
LLSSRV.EXE pid: 756
Command line: C:\WINNT\System32\llssrv.exe

  Base        Size      Version                  Path
  0x01000000  0x1a000   5.00.2195.4450  C:\WINNT\System32\llssrv.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
```

0x773b0000 0x2e000 5.00.2195.2778 C:\WINNT\System32\ACTIVEDS.dll
0x77380000 0x22000 5.00.2195.4308 C:\WINNT\System32\ADSLDPC.DLL
0x78000000 0x46000 6.01.9359.0000 C:\WINNT\system32\MSVCRT.DLL
0x77e80000 0xb5000 5.00.2195.4272 C:\WINNT\system32\KERNEL32.dll
0x75170000 0x4f000 5.00.2195.4153 C:\WINNT\System32\NETAPI32.DLL
0x77be0000 0xf000 5.00.2195.2862 C:\WINNT\System32\SECUR32.DLL
0x77db0000 0x5c000 5.00.2195.4453 C:\WINNT\system32\ADVAPI32.DLL
0x77d40000 0x70000 5.00.2195.4266 C:\WINNT\system32\RPCRT4.DLL
0x751c0000 0x6000 5.00.2134.0001 C:\WINNT\System32\NETRAP.DLL
0x75150000 0x10000 5.00.2195.2780 C:\WINNT\System32\SAMLIB.DLL
0x75030000 0x13000 5.00.2195.2780 C:\WINNT\System32\WS2_32.DLL
0x75020000 0x8000 5.00.2134.0001 C:\WINNT\System32\WS2HELP.DLL
0x77950000 0x2a000 5.00.2195.4436 C:\WINNT\system32\WLDAP32.DLL
0x77980000 0x24000 5.00.2195.4141 C:\WINNT\System32\DNSAPI.DLL
0x75050000 0x8000 5.00.2195.2871 C:\WINNT\System32\WSOCK32.DLL
0x77e10000 0x64000 5.00.2195.4314 C:\WINNT\system32\USER32.DLL
0x77f40000 0x3c000 5.00.2195.3914 C:\WINNT\system32\GDI32.DLL
0x77a50000 0xf6000 5.00.2195.4439 C:\WINNT\system32\OLE32.DLL
0x779b0000 0x9b000 2.40.4517.0000 C:\WINNT\system32\OLEAUT32.DLL
0x77bf0000 0x11000 5.00.2195.2661 C:\WINNT\System32\NTDSAPI.dll
0x775a0000 0x85000 2000.02.3488.0000 C:\WINNT\System32\CLBCATQ.DLL
0x6cc10000 0xe000 5.00.2195.4450 C:\WINNT\System32\LLSRPC.DLL

---

regsvc.exe pid: 796
Command line: C:\WINNT\system32\regsvc.exe

Base Size Version Path
0x01000000 0x14000 5.00.2195.2104 C:\WINNT\system32\regsvc.exe
0x77f80000 0x7b000 5.00.2195.2779 C:\WINNT\System32\ntdll.dll
0x77db0000 0x5c000 5.00.2195.4453 C:\WINNT\system32\ADVAPI32.dll
0x77e80000 0xb5000 5.00.2195.4272 C:\WINNT\system32\KERNEL32.DLL
0x77d40000 0x70000 5.00.2195.4266 C:\WINNT\system32\RPCRT4.DLL
0x77be0000 0xf000 5.00.2195.2862 C:\WINNT\system32\secur32.dll

---

mstask.exe pid: 812
Command line: C:\WINNT\system32\MSTask.exe

Base Size Version Path
0x01000000 0x1e000 4.71.2195.0001 C:\WINNT\system32\MSTask.exe
0x77f80000 0x7b000 5.00.2195.2779 C:\WINNT\System32\ntdll.dll
0x78000000 0x46000 6.01.9359.0000 C:\WINNT\system32\MSVCRT.dll
0x77e80000 0xb5000 5.00.2195.4272 C:\WINNT\system32\KERNEL32.dll
0x77db0000 0x5c000 5.00.2195.4453 C:\WINNT\system32\ADVAPI32.dll
0x77d40000 0x70000 5.00.2195.4266 C:\WINNT\system32\RPCRT4.DLL
0x77f40000 0x3c000 5.00.2195.3914 C:\WINNT\system32\GDI32.dll
0x77e10000 0x64000 5.00.2195.4314 C:\WINNT\system32\USER32.DLL
0x75170000 0x4f000 5.00.2195.4153 C:\WINNT\system32\NETAPI32.dll
0x77be0000 0xf000 5.00.2195.2862 C:\WINNT\system32\SECUR32.DLL
0x751c0000 0x6000 5.00.2134.0001 C:\WINNT\system32\NETRAP.DLL
0x75150000 0x10000 5.00.2195.2780 C:\WINNT\system32\SAMLIB.DLL
0x75030000 0x13000 5.00.2195.2780 C:\WINNT\system32\WS2_32.DLL
0x75020000 0x8000 5.00.2134.0001 C:\WINNT\system32\WS2HELP.DLL
0x77950000 0x2a000 5.00.2195.4436 C:\WINNT\system32\WLDAP32.DLL
0x77980000 0x24000 5.00.2195.4141 C:\WINNT\system32\DNSAPI.DLL
0x75050000 0x8000 5.00.2195.2871 C:\WINNT\system32\WSOCK32.DLL
0x77bf0000 0x11000 5.00.2195.2661 C:\WINNT\system32\NTDSAPI.dll
0x77c70000 0x4a000 5.00.3502.4373 C:\WINNT\system32\SHLWAPI.dll
0x782f0000 0x242000 5.00.3315.2902 C:\WINNT\system32\SHELL32.dll
0x77b50000 0x89000 5.81.3103.1000 C:\WINNT\system32\COMCTL32.DLL
0x77c10000 0x5e000 5.00.2195.4345 C:\WINNT\system32\USERENV.dll
0x74ff0000 0x12000 5.00.2195.2871 C:\WINNT\system32\mswsock.dll
0x74fd0000 0x1f000 5.00.2195.2779 C:\WINNT\system32\msafd.dll

```
  0x75010000  0x7000    5.00.2195.2104  C:\WINNT\System32\wshtcpip.dll
  0x785c0000  0xc000    5.00.2195.2871  C:\WINNT\System32\rnr20.dll
  0x77340000  0x13000   5.00.2173.0002  C:\WINNT\system32\iphlpapi.dll
  0x77520000  0x5000    5.00.2134.0001  C:\WINNT\system32\ICMP.DLL
  0x77320000  0x17000   5.00.2181.0001  C:\WINNT\system32\MPRAPI.DLL
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\OLE32.DLL
  0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.DLL
  0x773b0000  0x2e000   5.00.2195.2778  C:\WINNT\system32\ACTIVEDS.DLL
  0x77380000  0x22000   5.00.2195.4308  C:\WINNT\system32\ADSLDPC.DLL
  0x77830000  0xe000    5.00.2168.0001  C:\WINNT\system32\RTUTILS.DLL
  0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\system32\SETUPAPI.DLL
  0x774e0000  0x32000   5.00.2195.2671  C:\WINNT\system32\RASAPI32.DLL
  0x774c0000  0x11000   5.00.2195.2780  C:\WINNT\system32\RASMAN.DLL
  0x77530000  0x22000   5.00.2182.0001  C:\WINNT\system32\TAPI32.DLL
  0x77360000  0x19000   5.00.2195.2778  C:\WINNT\system32\DHCPCSVC.DLL
  0x775a0000  0x85000   2000.02.3488.0000  C:\WINNT\system32\CLBCATQ.DLL
  0x777e0000  0x8000    5.00.2160.0001  C:\WINNT\System32\winrnr.dll
  0x777f0000  0x5000    5.00.2168.0001  C:\WINNT\system32\rasadhlp.dll
  0x76a40000  0x6000    5.00.2920.0000  C:\WINNT\system32\MSIDLE.DLL
---------------------------------------------------------------------------
WinMgmt.exe pid: 920
Command line: C:\WINNT\System32\WBEM\WinMgmt.exe

  Base        Size      Version                   Path
  0x00400000  0x30000   1.50.1085.0029  C:\WINNT\System32\WBEM\WinMgmt.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x65c20000  0xad000   1.50.1085.0021  C:\WINNT\System32\WBEM\wbemcomn.dll
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.dll
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.dll
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.dll
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\ole32.dll
  0x775a0000  0x85000   2000.02.3488.0000  C:\WINNT\SYSTEM32\CLBCATQ.DLL
  0x69280000  0x9000    5.00.2155.0001  C:\WINNT\SYSTEM32\perfos.dll
  0x75030000  0x13000   5.00.2195.2780  C:\WINNT\SYSTEM32\WS2_32.DLL
  0x75020000  0x8000    5.00.2134.0001  C:\WINNT\SYSTEM32\WS2HELP.DLL
---------------------------------------------------------------------------
dfssvc.exe pid: 956
Command line: C:\WINNT\system32\Dfssvc.exe

  Base        Size      Version                   Path
  0x01000000  0x1b000   5.00.2195.2841  C:\WINNT\system32\Dfssvc.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.dll
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.dll
  0x75170000  0x4f000   5.00.2195.4153  C:\WINNT\system32\NETAPI32.dll
  0x77be0000  0xf000    5.00.2195.2862  C:\WINNT\system32\SECUR32.DLL
  0x751c0000  0x6000    5.00.2134.0001  C:\WINNT\system32\NETRAP.DLL
  0x75150000  0x10000   5.00.2195.2780  C:\WINNT\system32\SAMLIB.DLL
  0x75030000  0x13000   5.00.2195.2780  C:\WINNT\system32\WS2_32.DLL
  0x75020000  0x8000    5.00.2134.0001  C:\WINNT\system32\WS2HELP.DLL
  0x77980000  0x24000   5.00.2195.4141  C:\WINNT\system32\DNSAPI.DLL
  0x75050000  0x8000    5.00.2195.2871  C:\WINNT\system32\WSOCK32.DLL
  0x73930000  0x10000   5.00.2195.2104  C:\WINNT\system32\CLUSAPI.dll
  0x689d0000  0xd000    5.00.2195.2787  C:\WINNT\system32\RESUTILS.dll
  0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\system32\USERENV.dll
```

```
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77bf0000  0x11000   5.00.2195.2661  C:\WINNT\system32\NTDSAPI.dll
--------------------------------------------------------------------------------
inetinfo.exe pid: 976
Command line: C:\WINNT\System32\inetsrv\inetinfo.exe

  Base        Size      Version                  Path
  0x01000000  0x6000    5.00.2195.2966  C:\WINNT\System32\inetsrv\inetinfo.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.dll
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.dll
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\ole32.dll
  0x6e5a0000  0x21000   5.00.2195.4386  C:\WINNT\SYSTEM32\IisRTL.DLL
  0x75030000  0x13000   5.00.2195.2780  C:\WINNT\SYSTEM32\WS2_32.DLL
  0x75020000  0x8000    5.00.2134.0001  C:\WINNT\SYSTEM32\WS2HELP.DLL
  0x68920000  0x5000    5.00.2195.2966  C:\WINNT\System32\inetsrv\rpcref.dll
  0x6e6f0000  0x7000    5.00.2195.2966  C:\WINNT\System32\inetsrv\iisadmin.dll
  0x73330000  0xd000    5.00.2195.2966  C:\WINNT\System32\inetsrv\COADMIN.DLL
  0x782f0000  0x242000  5.00.3315.2902  C:\WINNT\system32\SHELL32.DLL
  0x77c70000  0x4a000   5.00.3502.4373  C:\WINNT\system32\SHLWAPI.DLL
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.DLL
  0x74e30000  0xc000    5.00.2185.0001  C:\WINNT\SYSTEM32\ADMWPROX.DLL
  0x76110000  0x4000    5.00.2191.0001  C:\WINNT\SYSTEM32\WMI.dll
  0x775a0000  0x85000   2000.02.3488.0000  C:\WINNT\SYSTEM32\CLBCATQ.DLL
  0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.dll
  0x69d00000  0xd000    5.00.2195.2966  C:\WINNT\System32\inetsrv\nsepm.dll
  0x6e5e0000  0x11000   5.00.2195.2966  C:\WINNT\SYSTEM32\IISMAP.dll
  0x78160000  0x26000   5.01.2195.0000  C:\WINNT\SYSTEM32\schannel.dll
  0x77be0000  0xf000    5.00.2195.2862  C:\WINNT\SYSTEM32\SECUR32.DLL
  0x77430000  0x10000   5.00.2195.4067  C:\WINNT\SYSTEM32\MSASN1.DLL
  0x77440000  0x75000   5.131.2195.2833  C:\WINNT\SYSTEM32\CRYPT32.DLL
  0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\SYSTEM32\USERENV.DLL
  0x75050000  0x8000    5.00.2195.2871  C:\WINNT\SYSTEM32\WSOCK32.DLL
  0x77980000  0x24000   5.00.2195.4141  C:\WINNT\SYSTEM32\DNSAPI.DLL
  0x6c7e0000  0x14000   5.00.2195.2966  C:\WINNT\System32\inetsrv\metadata.dll
  0x65d60000  0xe000    5.00.2195.2966  C:\WINNT\System32\inetsrv\wamreg.dll
  0x7ca00000  0x22000   5.00.2195.2228  C:\WINNT\SYSTEM32\rsabase.dll
  0x74e40000  0xa000    5.00.2195.2966  C:\WINNT\System32\inetsrv\admexs.dll
  0x671b0000  0xc000    5.00.2195.2966  C:\WINNT\System32\inetsrv\svcext.dll
  0x75500000  0x4000    5.00.2154.0001  C:\WINNT\SYSTEM32\Security.dll
  0x75170000  0x4f000   5.00.2195.4153  C:\WINNT\SYSTEM32\NETAPI32.dll
  0x751c0000  0x6000    5.00.2134.0001  C:\WINNT\SYSTEM32\NETRAP.DLL
  0x75150000  0x10000   5.00.2195.2780  C:\WINNT\SYSTEM32\SAMLIB.DLL
  0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.DLL
  0x6fc60000  0x1f000   5.00.2195.2966  C:\WINNT\System32\inetsrv\ftpsvc2.dll
  0x6d700000  0x12000   5.00.2195.4430  C:\WINNT\System32\inetsrv\ISATQ.dll
  0x769b0000  0x42000   5.00.2195.4430  C:\WINNT\System32\inetsrv\INFOCOMM.dll
  0x6e620000  0x5000    5.00.2185.0001  C:\WINNT\System32\inetsrv\IISFECNV.DLL
  0x67810000  0x70000   5.00.2195.4453  C:\WINNT\System32\inetsrv\SMTPSVC.dll
  0x773e0000  0x12000   3.00.8449.0000  C:\WINNT\SYSTEM32\ATL.DLL
  0x77820000  0x7000    5.00.2134.0001  C:\WINNT\system32\VERSION.dll
  0x759b0000  0x6000    5.00.2134.0001  C:\WINNT\system32\LZ32.DLL
  0x6ff20000  0xe000    5.00.2159.0001  C:\WINNT\SYSTEM32\FCACHDLL.dll
  0x68510000  0x6000    5.00.2159.0001  C:\WINNT\SYSTEM32\RWNH.dll
  0x70120000  0xc000    5.06.2159.0001  C:\WINNT\SYSTEM32\exstrace.dll
  0x67390000  0x6000    5.00.2159.0001  C:\WINNT\SYSTEM32\STAXMEM.dll
  0x77bf0000  0x11000   5.00.2195.2661  C:\WINNT\SYSTEM32\NTDSAPI.dll
```

```
  0x65f00000  0x59000   5.00.2195.4431  C:\WINNT\System32\inetsrv\w3svc.dll
  0x6e2b0000  0x8000    5.00.2195.2966  C:\WINNT\SYSTEM32\inetsloc.dll
  0x74ff0000  0x12000   5.00.2195.2871  C:\WINNT\SYSTEM32\MSWSOCK.dll
  0x6ca80000  0x6000    5.00.2195.2966  C:\WINNT\System32\inetsrv\lonsint.dll
  0x74fd0000  0x1f000   5.00.2195.2779  C:\WINNT\system32\msafd.dll
  0x75010000  0x7000    5.00.2195.2104  C:\WINNT\System32\wshtcpip.dll
  0x76930000  0x2b000   5.131.2195.2779  C:\WINNT\SYSTEM32\wintrust.dll
  0x77920000  0x23000   5.00.2195.2778  C:\WINNT\system32\IMAGEHLP.dll
  0x785c0000  0xc000    5.00.2195.2871  C:\WINNT\System32\rnr20.dll
  0x77340000  0x13000   5.00.2173.0002  C:\WINNT\SYSTEM32\iphlpapi.dll
  0x77520000  0x5000    5.00.2134.0001  C:\WINNT\SYSTEM32\ICMP.DLL
  0x77320000  0x17000   5.00.2181.0001  C:\WINNT\SYSTEM32\MPRAPI.DLL
  0x773b0000  0x2e000   5.00.2195.2778  C:\WINNT\SYSTEM32\ACTIVEDS.DLL
  0x77380000  0x22000   5.00.2195.4308  C:\WINNT\SYSTEM32\ADSLDPC.DLL
  0x77830000  0xe000    5.00.2168.0001  C:\WINNT\SYSTEM32\RTUTILS.DLL
  0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\SYSTEM32\SETUPAPI.DLL
  0x774e0000  0x32000   5.00.2195.2671  C:\WINNT\SYSTEM32\RASAPI32.DLL
  0x774c0000  0x11000   5.00.2195.2780  C:\WINNT\SYSTEM32\RASMAN.DLL
  0x77530000  0x22000   5.00.2182.0001  C:\WINNT\SYSTEM32\TAPI32.DLL
  0x77360000  0x19000   5.00.2195.2778  C:\WINNT\SYSTEM32\DHCPCSVC.DLL
  0x777e0000  0x8000    5.00.2160.0001  C:\WINNT\System32\winrnr.dll
  0x777f0000  0x5000    5.00.2168.0001  C:\WINNT\SYSTEM32\rasadhlp.dll
  0x6d6f0000  0xa000    5.00.2195.2966  C:\WINNT\System32\inetsrv\iscomlog.dll
  0x681e0000  0x3c000   5.00.2195.2966  C:\WINNT\System32\inetsrv\seo.dll
  0x67400000  0xe000    5.00.2195.2966  C:\WINNT\System32\inetsrv\sspifilt.dll
  0x732c0000  0x9000    5.00.2195.2966  C:\WINNT\System32\inetsrv\compfilt.dll
  0x6fa20000  0xb000    5.00.2195.2966  C:\WINNT\system32\inetsrv\gzip.dll
  0x754b0000  0x5000    5.00.2134.0001  C:\WINNT\System32\wshnetbs.dll
  0x6e600000  0x15000   5.00.2195.2966  C:\WINNT\System32\inetsrv\iislog.dll
  0x6c850000  0xc000    5.00.2195.2966  C:\WINNT\System32\inetsrv\md5filt.dll
  0x01860000  0x23000   5.00.2195.2228  C:\WINNT\SYSTEM32\rsaenh.dll
  0x74a60000  0x50000   5.00.2195.4386  C:\WINNT\System32\inetsrv\aqueue.dll
  0x67e70000  0x5000    4.00.0002.5526  C:\Program Files\Common Files\Microsoft Shared\Web Server
Extensions\40\bin\fpexedll.dll
  0x6eeb0000  0x42000   5.00.2195.4386  C:\WINNT\System32\inetsrv\httpext.dll
  0x756e0000  0x5000    5.00.2195.4450  C:\WINNT\SYSTEM32\NTLSAPI.DLL
  0x69c20000  0xc000    5.00.2195.4386  C:\WINNT\System32\inetsrv\ntfsdrv.dll
-------------------------------------------------------------------------------
svchost.exe pid: 1244
Command line: C:\WINNT\System32\svchost.exe -k tapisrv

  Base        Size      Version                  Path
  0x01000000  0x5000    5.00.2134.0001  C:\WINNT\System32\svchost.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.DLL
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.DLL
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\OLE32.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.DLL
  0x66df0000  0x2c000   5.00.2195.2955  c:\winnt\system32\tapisrv.dll
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.dll
  0x77be0000  0xf000    5.00.2195.2862  C:\WINNT\System32\secur32.dll
  0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\System32\SETUPAPI.dll
  0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\System32\USERENV.DLL
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.dll
  0x69bf0000  0x1d000   5.00.2195.2862  C:\WINNT\System32\NTMARTA.DLL
  0x77800000  0x1d000   5.00.2195.2780  C:\WINNT\System32\WINSPOOL.DRV
  0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.dll
  0x77bf0000  0x11000   5.00.2195.2661  C:\WINNT\System32\NTDSAPI.dll
  0x77980000  0x24000   5.00.2195.4141  C:\WINNT\System32\DNSAPI.DLL
  0x75050000  0x8000    5.00.2195.2871  C:\WINNT\System32\WSOCK32.DLL
```

0x75030000 0x13000 5.00.2195.2780 C:\WINNT\System32\WS2_32.DLL
0x75020000 0x8000 5.00.2134.0001 C:\WINNT\System32\WS2HELP.DLL
0x75170000 0x4f000 5.00.2195.4153 C:\WINNT\System32\NETAPI32.DLL
0x751c0000 0x6000 5.00.2134.0001 C:\WINNT\System32\NETRAP.DLL
0x75150000 0x10000 5.00.2195.2780 C:\WINNT\System32\SAMLIB.DLL
0x77c70000 0x4a000 5.00.3502.4373 C:\WINNT\system32\SHLWAPI.dll
0x77340000 0x13000 5.00.2173.0002 C:\WINNT\System32\iphlpapi.dll
0x77520000 0x5000 5.00.2134.0001 C:\WINNT\System32\ICMP.DLL
0x77320000 0x17000 5.00.2181.0001 C:\WINNT\System32\MPRAPI.DLL
0x779b0000 0x9b000 2.40.4517.0000 C:\WINNT\system32\OLEAUT32.DLL
0x773b0000 0x2e000 5.00.2195.2778 C:\WINNT\System32\ACTIVEDS.DLL
0x77380000 0x22000 5.00.2195.4308 C:\WINNT\System32\ADSLDPC.DLL
0x77830000 0xe000 5.00.2168.0001 C:\WINNT\System32\RTUTILS.DLL
0x774e0000 0x32000 5.00.2195.2671 C:\WINNT\System32\RASAPI32.DLL
0x774c0000 0x11000 5.00.2195.2780 C:\WINNT\System32\RASMAN.DLL
0x77530000 0x22000 5.00.2182.0001 C:\WINNT\System32\TAPI32.DLL
0x77360000 0x19000 5.00.2195.2778 C:\WINNT\System32\DHCPCSVC.DLL
0x775a0000 0x85000 2000.02.3488.0000 C:\WINNT\System32\CLBCATQ.DLL
0x644d0000 0x34000 5.00.2175.0001 C:\WINNT\System32\unimdm.tsp
0x75600000 0x7000 5.00.2151.0001 C:\WINNT\System32\uniplat.dll
0x770b0000 0x7000 5.00.2134.0001 C:\WINNT\System32\CFGMGR32.dll
0x66720000 0x13000 5.00.2134.0001 C:\WINNT\System32\unimdmat.dll
0x77820000 0x7000 5.00.2134.0001 C:\WINNT\system32\VERSION.dll
0x759b0000 0x6000 5.00.2134.0001 C:\WINNT\system32\LZ32.DLL
0x6bdb0000 0x1b000 5.00.2146.0001 C:\WINNT\System32\modemui.dll
0x782f0000 0x242000 5.00.3315.2902 C:\WINNT\system32\SHELL32.dll
0x64540000 0x8000 5.00.2150.0001 C:\WINNT\System32\kmddsp.tsp
0x64530000 0xc000 5.00.2143.0001 C:\WINNT\System32\ndptsp.tsp
0x64550000 0x6000 5.00.2143.0001 C:\WINNT\System32\ipconf.tsp
0x64560000 0x44000 5.00.2195.2283 C:\WINNT\System32\h323.tsp
0x77430000 0x10000 5.00.2195.4067 C:\WINNT\System32\MSASN1.dll

---

explorer.exe pid: 1364
Command line: C:\WINNT\Explorer.EXE

Base Size Version Path
0x00400000 0x3e000 5.00.3315.2846 C:\WINNT\Explorer.EXE
0x77f80000 0x7b000 5.00.2195.2779 C:\WINNT\System32\ntdll.dll
0x77db0000 0x5c000 5.00.2195.4453 C:\WINNT\system32\ADVAPI32.DLL
0x77e80000 0xb5000 5.00.2195.4272 C:\WINNT\system32\KERNEL32.DLL
0x77d40000 0x70000 5.00.2195.4266 C:\WINNT\system32\RPCRT4.DLL
0x77f40000 0x3c000 5.00.2195.3914 C:\WINNT\system32\GDI32.DLL
0x77e10000 0x64000 5.00.2195.4314 C:\WINNT\system32\USER32.DLL
0x77c70000 0x4a000 5.00.3502.4373 C:\WINNT\system32\SHLWAPI.DLL
0x77b50000 0x89000 5.81.3103.1000 C:\WINNT\system32\COMCTL32.DLL
0x782f0000 0x242000 5.00.3315.2902 C:\WINNT\system32\SHELL32.dll
0x77a50000 0xf6000 5.00.2195.4439 C:\WINNT\system32\OLE32.DLL
0x775a0000 0x85000 2000.02.3488.0000 C:\WINNT\System32\CLBCATQ.DLL
0x779b0000 0x9b000 2.40.4517.0000 C:\WINNT\system32\OLEAUT32.dll
0x78000000 0x46000 6.01.9359.0000 C:\WINNT\system32\MSVCRT.dll
0x76c80000 0x110000 5.00.3315.2879 C:\WINNT\System32\SHDOCVW.DLL
0x76e10000 0xc7000 5.00.3502.4373 C:\WINNT\System32\browseui.dll
0x77c10000 0x5e000 5.00.2195.4345 C:\WINNT\System32\USERENV.DLL
0x76df0000 0x11000 5.00.2920.0000 C:\WINNT\System32\mydocs.dll
0x76fa0000 0xf000 5.00.2134.0001 C:\WINNT\System32\ntshrui.dll
0x773e0000 0x12000 3.00.8449.0000 C:\WINNT\System32\ATL.DLL
0x75170000 0x4f000 5.00.2195.4153 C:\WINNT\System32\NETAPI32.DLL
0x77be0000 0xf000 5.00.2195.2862 C:\WINNT\System32\SECUR32.DLL
0x751c0000 0x6000 5.00.2134.0001 C:\WINNT\System32\NETRAP.DLL
0x75150000 0x10000 5.00.2195.2780 C:\WINNT\System32\SAMLIB.DLL
0x75030000 0x13000 5.00.2195.2780 C:\WINNT\System32\WS2_32.DLL
0x75020000 0x8000 5.00.2134.0001 C:\WINNT\System32\WS2HELP.DLL

```
0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.DLL
0x77980000  0x24000   5.00.2195.4141  C:\WINNT\System32\DNSAPI.DLL
0x75050000  0x8000    5.00.2195.2871  C:\WINNT\System32\WSOCK32.DLL
0x75090000  0x10000   5.00.2195.2779  C:\WINNT\system32\MPR.DLL
0x75160000  0xc000    5.00.2157.0001  C:\WINNT\System32\ntlanman.dll
0x75210000  0x15000   5.00.2134.0001  C:\WINNT\System32\NETUI0.DLL
0x751d0000  0x38000   5.00.2134.0001  C:\WINNT\System32\NETUI1.DLL
0x76f20000  0x75000   5.00.2195.2779  C:\WINNT\system32\NETSHELL.dll
0x76680000  0x41000   5.00.3315.1000  C:\WINNT\System32\webcheck.dll
0x766d0000  0x18000   5.00.2195.2780  C:\WINNT\System32\stobject.dll
0x76740000  0x8000    5.00.3103.1000  C:\WINNT\System32\BATMETER.DLL
0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\System32\SETUPAPI.DLL
0x766f0000  0x7000    5.00.3103.1000  C:\WINNT\System32\POWRPROF.DLL
0x77570000  0x30000   5.00.2161.0001  C:\WINNT\System32\WINMM.DLL
0x681a0000  0x7000    5.00.2134.0001  C:\WINNT\System32\serwvdrv.dll
0x66740000  0x7000    5.00.2134.0001  C:\WINNT\System32\umdmxfrm.dll
0x20280000  0xd000                    C:\WINNT\qvphook.dll
0x770f0000  0x1b7000  1.11.2405.0000  C:\WINNT\System32\MSI.DLL
0x77840000  0x3c000   5.00.2195.2959  C:\WINNT\System32\cscui.dll
0x770c0000  0x23000   5.00.2195.2401  C:\WINNT\System32\CSCDLL.DLL
0x77560000  0x9000    5.00.2195.2669  C:\WINNT\System32\wdmaud.drv
0x77400000  0x8000    5.00.2134.0001  C:\WINNT\System32\msacm32.drv
0x77410000  0x13000   5.00.2134.0001  C:\WINNT\System32\MSACM32.dll
0x76710000  0x9000    5.00.2134.0001  C:\WINNT\System32\LINKINFO.DLL
0x770b0000  0x7000    5.00.2134.0001  C:\WINNT\System32\CfgMgr32.dll
0x71f00000  0x4d000   5.00.2178.0001  C:\WINNT\System32\docprop2.dll
0x6a8f0000  0x20000   5.00.2134.0001  C:\WINNT\System32\MSVFW32.DLL
0x74870000  0x16000   5.00.2134.0001  C:\WINNT\System32\AVIFIL32.DLL
0x70020000  0x5000    5.00.2134.0001  C:\WINNT\system32\faxshell.dll
0x10000000  0xb000                    C:\Program Files\VitalSigns\Net.Medic\Program\syshook.dll
0x01bb0000  0x7000    1.00.0000.0001  C:\Program Files\Yahoo!\Messenger\idle.dll
0x76c00000  0x73000   5.00.3502.4449  C:\WINNT\system32\WININET.DLL
0x76700000  0x9000    5.00.2153.0001  C:\WINNT\System32\mmcshext.dll
0x76fb0000  0xf2000   6.00.8665.0000  C:\WINNT\System32\MFC42u.DLL
0x780c0000  0x8d000   5.00.0000.7051  C:\WINNT\System32\MSVCP50.dll
0x76720000  0x14000   4.74.8702.0000  C:\WINNT\System32\hhsetup.dll
0x76ee0000  0xb000    5.00.3315.2846  C:\WINNT\System32\browselc.dll
0x77640000  0x72000   5.00.3502.4448  C:\WINNT\System32\urlmon.dll
0x77820000  0x7000    5.00.2134.0001  C:\WINNT\system32\VERSION.DLL
0x759b0000  0x6000    5.00.2134.0001  C:\WINNT\system32\LZ32.DLL
0x75d50000  0x82000   5.00.3103.1000  C:\WINNT\System32\mlang.dll
0x4a000000  0x2c000   6.00.0000.8424  C:\WINNT\System32\pdm.dll
0x4aa00000  0x15000   6.00.0000.8424  C:\WINNT\System32\msdbg.dll
0x75e60000  0x1a000   5.00.2195.2821  C:\WINNT\System32\IMM32.DLL
0x75de0000  0x77000   5.01.0000.5907  C:\WINNT\System32\jscript.dll
0x65050000  0x1b000   5.00.3103.1000  C:\WINNT\System32\powercfg.cpl
0x65150000  0x10000   5.00.2195.2104  C:\WINNT\System32\LICCPA.CPL
0x6cc10000  0xe000    5.00.2195.4450  C:\WINNT\System32\LLSRPC.dll
0x74160000  0x11000   5.00.2195.4450  C:\WINNT\System32\CCFAPI32.dll
0x75d40000  0x6000    5.00.2134.0001  C:\WINNT\System32\msadp32.acm
0x69bf0000  0x1d000   5.00.2195.2862  C:\WINNT\System32\NTMARTA.DLL
0x77800000  0x1d000   5.00.2195.2780  C:\WINNT\System32\WINSPOOL.DRV
0x77bf0000  0x11000   5.00.2195.2661  C:\WINNT\System32\NTDSAPI.dll
0x75af0000  0x23f000  5.00.3502.4373  C:\WINNT\System32\mshtml.dll
0x76d90000  0x53000   5.00.3315.2879  C:\WINNT\System32\shdoclc.dll
0x75ac0000  0x28000   3.10.0337.0000  C:\WINNT\System32\MSLS31.DLL
0x658f0000  0x114000  5.00.2920.0000  C:\WINNT\System32\webvw.dll
0x6e490000  0xa000    5.00.3315.2870  C:\WINNT\System32\imgutil.dll
0x6b3d0000  0x3c000   5.00.3315.2870  C:\WINNT\System32\mshtmled.dll
0x66650000  0x54000   1.325.2195.2104  C:\WINNT\System32\USP10.DLL
0x66d20000  0x31000   5.00.2920.0000  C:\WINNT\System32\thumbvw.dll
0x717f0000  0x29000   5.00.2195.4445  C:\WINNT\System32\dsquery.dll
```

0x76b30000 0x3e000 5.00.3103.1000 C:\WINNT\system32\comdlg32.dll
0x717c0000 0x1e000 5.00.2195.4445 C:\WINNT\System32\dsuiext.dll
0x773b0000 0x2e000 5.00.2195.2778 C:\WINNT\System32\ACTIVEDS.dll
0x77380000 0x22000 5.00.2195.4308 C:\WINNT\System32\ADSLDPC.DLL
0x6a830000 0x7f000 8.00.5718.0001 C:\WINNT\System32\msxml.dll
0x6ac20000 0x37000 4.71.2137.0001 C:\WINNT\System32\mstask.dll
0x68c60000 0x160000 5.00.2195.2495 C:\WINNT\System32\query.dll
0x16200000 0x6000 4.01.0000.0000 C:\PROGRA~1\WINZIP\WZSHLSTB.DLL
0x379b0000 0x8c000 9.00.0000.3503
C:\PROGRA~1\COMMON~1\MICROS~1\WEBFOL~1\MSONSEXT.DLL
0x05990000 0xe000 4.00.0001.0957 C:\PROGRA~1\QUICKV~1\PROGRAM\QVPSE2.DLL
0x75230000 0x15000 5.00.3103.1000 C:\WINNT\System32\actxprxy.dll
---
tp4mon.exe pid: 1204
Command line: "C:\WINNT\System32\tp4mon.exe"

Base Size Version Path
0x00400000 0x1b000 5.00.2134.0001 C:\WINNT\System32\tp4mon.exe
0x77f80000 0x7b000 5.00.2195.2779 C:\WINNT\System32\ntdll.dll
0x782f0000 0x242000 5.00.3315.2902 C:\WINNT\system32\SHELL32.dll
0x77f40000 0x3c000 5.00.2195.3914 C:\WINNT\system32\GDI32.DLL
0x77e80000 0xb5000 5.00.2195.4272 C:\WINNT\system32\KERNEL32.DLL
0x77e10000 0x64000 5.00.2195.4314 C:\WINNT\system32\USER32.DLL
0x77db0000 0x5c000 5.00.2195.4453 C:\WINNT\system32\ADVAPI32.DLL
0x77d40000 0x70000 5.00.2195.4266 C:\WINNT\system32\RPCRT4.DLL
0x77c70000 0x4a000 5.00.3502.4373 C:\WINNT\system32\SHLWAPI.DLL
0x77b50000 0x89000 5.81.3103.1000 C:\WINNT\system32\COMCTL32.DLL
0x66cb0000 0x9000 5.00.2134.0001 C:\WINNT\System32\tp4res.dll
---
YPager.exe pid: 1228
Command line: "C:\Program Files\Yahoo!\Messenger\ypager.exe" -quiet

Base Size Version Path
0x00400000 0x164000 5.05.0000.1246 C:\Program Files\Yahoo!\Messenger\ypager.exe
0x77f80000 0x7b000 5.00.2195.2779 C:\WINNT\System32\ntdll.dll
0x77820000 0x7000 5.00.2134.0001 C:\WINNT\system32\VERSION.dll
0x77e80000 0xb5000 5.00.2195.4272 C:\WINNT\system32\KERNEL32.DLL
0x759b0000 0x6000 5.00.2134.0001 C:\WINNT\system32\LZ32.DLL
0x77e10000 0x64000 5.00.2195.4314 C:\WINNT\system32\USER32.dll
0x77f40000 0x3c000 5.00.2195.3914 C:\WINNT\system32\GDI32.DLL
0x77b50000 0x89000 5.81.3103.1000 C:\WINNT\system32\COMCTL32.dll
0x77db0000 0x5c000 5.00.2195.4453 C:\WINNT\system32\ADVAPI32.DLL
0x77d40000 0x70000 5.00.2195.4266 C:\WINNT\system32\RPCRT4.DLL
0x77570000 0x30000 5.00.2161.0001 C:\WINNT\System32\WINMM.dll
0x75050000 0x8000 5.00.2195.2871 C:\WINNT\System32\WSOCK32.dll
0x75030000 0x13000 5.00.2195.2780 C:\WINNT\System32\WS2_32.DLL
0x78000000 0x46000 6.01.9359.0000 C:\WINNT\system32\MSVCRT.DLL
0x75020000 0x8000 5.00.2134.0001 C:\WINNT\System32\WS2HELP.DLL
0x10000000 0x10000 3.04.0000.0006 C:\Program Files\Yahoo!\Messenger\D32-FW.DLL
0x00230000 0x7000 1.00.0000.0001 C:\Program Files\Yahoo!\Messenger\idle.dll
0x00240000 0x19000 2000.10.0009.0001 C:\Program Files\Yahoo!\Messenger\ygxa_2.dll
0x76c00000 0x73000 5.00.3502.4449 C:\WINNT\system32\WININET.dll
0x77c70000 0x4a000 5.00.3502.4373 C:\WINNT\system32\SHLWAPI.DLL
0x20000000 0xd000 C:\Program Files\Yahoo!\Messenger\xmlparse.dll
0x00260000 0x14000 C:\Program Files\Yahoo!\Messenger\xmltok.dll
0x65ec0000 0xe000 3.09.0000.0000 C:\Program Files\Yahoo!\Messenger\pcre.dll
0x76b30000 0x3e000 5.00.3103.1000 C:\WINNT\system32\comdlg32.dll
0x782f0000 0x242000 5.00.3315.2902 C:\WINNT\system32\SHELL32.DLL
0x77a50000 0xf6000 5.00.2195.4439 C:\WINNT\system32\ole32.dll
0x779b0000 0x9b000 2.40.4517.0000 C:\WINNT\system32\OLEAUT32.dll
0x681a0000 0x7000 5.00.2134.0001 C:\WINNT\System32\serwvdrv.dll
0x66740000 0x7000 5.00.2134.0001 C:\WINNT\System32\umdmxfrm.dll

0x017b0000 0x81000 5.05.0000.1200 C:\Program Files\Yahoo!\Messenger\res_msgr.dll
0x01a50000 0xb000 C:\Program Files\VitalSigns\Net.Medic\Program\syshook.dll
0x775a0000 0x85000 2000.02.3488.0000 C:\WINNT\System32\CLBCATQ.DLL
0x01b90000 0x10000 1.00.0000.0001 C:\PROGRA~1\Yahoo!\MESSEN~1\ycrwin32.dll
0x01be0000 0x2c000 5.05.0000.0454 C:\Program Files\Yahoo!\Messenger\MyYahoo.dll
0x76c80000 0x110000 5.00.3315.2879 C:\WINNT\System32\shdocvw.dll
0x76b20000 0x5000 5.00.2134.0001 C:\WINNT\System32\riched32.dll
0x772b0000 0x6c000 5.30.0023.1205 C:\WINNT\System32\RICHED20.dll
0x77640000 0x72000 5.00.3502.4448 C:\WINNT\System32\urlmon.dll
0x774e0000 0x32000 5.00.2195.2671 C:\WINNT\System32\RASAPI32.DLL
0x774c0000 0x11000 5.00.2195.2780 C:\WINNT\System32\RASMAN.DLL
0x77530000 0x22000 5.00.2182.0001 C:\WINNT\System32\TAPI32.DLL
0x77830000 0xe000 5.00.2168.0001 C:\WINNT\System32\RTUTILS.DLL
0x77520000 0x5000 5.00.2134.0001 C:\WINNT\System32\ICMP.DLL
0x75ab0000 0x5000 5.00.2163.0001 C:\WINNT\System32\sensapi.dll
0x77c10000 0x5e000 5.00.2195.4345 C:\WINNT\System32\USERENV.DLL
0x75170000 0x4f000 5.00.2195.4153 C:\WINNT\System32\netapi32.dll
0x77be0000 0xf000 5.00.2195.2862 C:\WINNT\System32\SECUR32.DLL
0x751c0000 0x6000 5.00.2134.0001 C:\WINNT\System32\NETRAP.DLL
0x75150000 0x10000 5.00.2195.2780 C:\WINNT\System32\SAMLIB.DLL
0x77950000 0x2a000 5.00.2195.4436 C:\WINNT\system32\WLDAP32.DLL
0x77980000 0x24000 5.00.2195.4141 C:\WINNT\System32\DNSAPI.DLL

---

fastfindeng.exe pid: 1184
Command line: "C:\Documents and Settings\All Users\Start Menu\Programs\Startup\fastfindeng.exe"

Base Size Version Path
0x00400000 0x5000 1.00.0000.0000 C:\Documents and Settings\All Users\Start Menu\Programs\Startup\fastfindeng.exe
0x77f80000 0x7b000 5.00.2195.2779 C:\WINNT\System32\ntdll.dll
0x6a9d0000 0x152000 6.00.0084.0095 C:\WINNT\System32\MSVBVM60.DLL
0x77e80000 0xb5000 5.00.2195.4272 C:\WINNT\system32\KERNEL32.dll
0x77e10000 0x64000 5.00.2195.4314 C:\WINNT\system32\USER32.dll
0x77f40000 0x3c000 5.00.2195.3914 C:\WINNT\system32\GDI32.DLL
0x77db0000 0x5c000 5.00.2195.4453 C:\WINNT\system32\ADVAPI32.dll
0x77d40000 0x70000 5.00.2195.4266 C:\WINNT\system32\RPCRT4.DLL
0x77a50000 0xf6000 5.00.2195.4439 C:\WINNT\system32\ole32.dll
0x779b0000 0x9b000 2.40.4517.0000 C:\WINNT\system32\OLEAUT32.dll

---

netMedic.exe pid: 1220
Command line: "C:\Program Files\VitalSigns\Net.Medic\Program\netMedic.exe"

Base Size Version Path
0x00400000 0x105000 1.02.0002.0001 C:\Program Files\VitalSigns\Net.Medic\Program\netMedic.exe
0x77f80000 0x7b000 5.00.2195.2779 C:\WINNT\System32\ntdll.dll
0x20000000 0x41000 1.00.0000.0000 C:\Program Files\VitalSigns\Net.Medic\Program\olch2d32.dll
0x77e80000 0xb5000 5.00.2195.4272 C:\WINNT\system32\KERNEL32.dll
0x77e10000 0x64000 5.00.2195.4314 C:\WINNT\system32\USER32.dll
0x77f40000 0x3c000 5.00.2195.3914 C:\WINNT\system32\GDI32.DLL
0x76b30000 0x3e000 5.00.3103.1000 C:\WINNT\system32\comdlg32.dll
0x77c70000 0x4a000 5.00.3502.4373 C:\WINNT\system32\SHLWAPI.DLL
0x77db0000 0x5c000 5.00.2195.4453 C:\WINNT\system32\ADVAPI32.DLL
0x77d40000 0x70000 5.00.2195.4266 C:\WINNT\system32\RPCRT4.DLL
0x77b50000 0x89000 5.81.3103.1000 C:\WINNT\system32\COMCTL32.DLL
0x782f0000 0x242000 5.00.3315.2902 C:\WINNT\system32\SHELL32.DLL
0x78000000 0x46000 6.01.9359.0000 C:\WINNT\system32\MSVCRT.DLL
0x78080000 0x15000 4.2000.0000.6201 C:\WINNT\System32\MSVCRT40.dll
0x780a0000 0x12000 6.01.8637.0000 C:\WINNT\System32\MSVCIRT.dll
0x77820000 0x7000 5.00.2134.0001 C:\WINNT\system32\VERSION.dll
0x759b0000 0x6000 5.00.2134.0001 C:\WINNT\system32\LZ32.DLL
0x6c6e0000 0xe7000 4.01.0000.6140 C:\WINNT\System32\MFC40.DLL
0x75050000 0x8000 5.00.2195.2871 C:\WINNT\System32\WSOCK32.dll

```
  0x75030000  0x13000   5.00.2195.2780  C:\WINNT\System32\WS2_32.DLL
  0x75020000  0x8000    5.00.2134.0001  C:\WINNT\System32\WS2HELP.DLL
  0x77530000  0x22000   5.00.2182.0001  C:\WINNT\System32\TAPI32.dll
  0x10000000  0xb000                    C:\Program Files\VitalSigns\Net.Medic\Program\syshook.dll
  0x77520000  0x5000    5.00.2134.0001  C:\WINNT\System32\ICMP.DLL
  0x69280000  0x9000    5.00.2155.0001  C:\WINNT\System32\perfos.dll
-------------------------------------------------------------------------------
docmanager.exe pid: 1200
Command line: docmanager -L -p 2049 -e cmd.exe

  Base        Size      Version                   Path
  0x00400000  0x13000                   C:\WINNT\docmanager.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
  0x75050000  0x8000    5.00.2195.2871  C:\WINNT\System32\WSOCK32.dll
  0x75030000  0x13000   5.00.2195.2780  C:\WINNT\System32\WS2_32.DLL
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.DLL
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.DLL
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x75020000  0x8000    5.00.2134.0001  C:\WINNT\System32\WS2HELP.DLL
  0x785c0000  0xc000    5.00.2195.2871  C:\WINNT\System32\rnr20.dll
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77980000  0x24000   5.00.2195.4141  C:\WINNT\System32\DNSAPI.DLL
  0x77340000  0x13000   5.00.2173.0002  C:\WINNT\System32\iphlpapi.dll
  0x77520000  0x5000    5.00.2134.0001  C:\WINNT\System32\ICMP.DLL
  0x77320000  0x17000   5.00.2181.0001  C:\WINNT\System32\MPRAPI.DLL
  0x75150000  0x10000   5.00.2195.2780  C:\WINNT\System32\SAMLIB.DLL
  0x75170000  0x4f000   5.00.2195.4153  C:\WINNT\System32\NETAPI32.DLL
  0x77be0000  0xf000    5.00.2195.2862  C:\WINNT\System32\SECUR32.DLL
  0x751c0000  0x6000    5.00.2134.0001  C:\WINNT\System32\NETRAP.DLL
  0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.DLL
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\OLE32.DLL
  0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.DLL
  0x773b0000  0x2e000   5.00.2195.2778  C:\WINNT\System32\ACTIVEDS.DLL
  0x77380000  0x22000   5.00.2195.4308  C:\WINNT\System32\ADSLDPC.DLL
  0x77830000  0xe000    5.00.2168.0001  C:\WINNT\System32\RTUTILS.DLL
  0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\System32\SETUPAPI.DLL
  0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\System32\USERENV.DLL
  0x774e0000  0x32000   5.00.2195.2671  C:\WINNT\System32\RASAPI32.DLL
  0x774c0000  0x11000   5.00.2195.2780  C:\WINNT\System32\RASMAN.DLL
  0x77530000  0x22000   5.00.2182.0001  C:\WINNT\System32\TAPI32.DLL
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.DLL
  0x77c70000  0x4a000   5.00.3502.4373  C:\WINNT\system32\SHLWAPI.DLL
  0x77360000  0x19000   5.00.2195.2778  C:\WINNT\System32\DHCPCSVC.DLL
  0x775a0000  0x85000   2000.02.3488.0000  C:\WINNT\System32\CLBCATQ.DLL
  0x777e0000  0x8000    5.00.2160.0001  C:\WINNT\System32\winrnr.dll
  0x777f0000  0x5000    5.00.2168.0001  C:\WINNT\System32\rasadhlp.dll
  0x74fd0000  0x1f000   5.00.2195.2779  C:\WINNT\system32\msafd.dll
  0x75010000  0x7000    5.00.2195.2104  C:\WINNT\System32\wshtcpip.dll
-------------------------------------------------------------------------------
syshook.exe pid: 1112
Command line: "\Program Files\VitalSigns\Net.Medic\Program\syshook.exe"

  Base        Size      Version                   Path
  0x00400000  0xb000                    C:\Program Files\VitalSigns\Net.Medic\Program\syshook.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x10000000  0xb000                    C:\Program Files\VitalSigns\Net.Medic\Program\syshook.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.dll
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.dll
```

```
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
---------------------------------------------------------------------------
CMD.EXE pid: 1416
Command line: "E:\evidence gathering tools\response_kit\win2k_xp\CMD.EXE"

  Base        Size      Version                  Path
  0x01360000  0x42000                E:\evidence gathering tools\response_kit\win2k_xp\CMD.EXE
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x782f0000  0x242000  5.00.3315.2902  C:\WINNT\system32\SHELL32.dll
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.DLL
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77c70000  0x4a000   5.00.3502.4373  C:\WINNT\system32\SHLWAPI.DLL
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.DLL
  0x75090000  0x10000   5.00.2195.2779  C:\WINNT\system32\MPR.dll
---------------------------------------------------------------------------
NTVDM.EXE pid: 320
Command line: "C:\WINNT\system32\ntvdm.exe" -f

  Base        Size      Version                  Path
  0x0f000000  0xa1000   5.00.2195.2563  C:\WINNT\system32\ntvdm.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.dll
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.dll
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.DLL
  0x69b00000  0x7000    5.00.2134.0001  C:\WINNT\system32\NTVDMD.DLL
---------------------------------------------------------------------------
msiexec.exe pid: 616
Command line: C:\WINNT\system32\msiexec.exe /V

  Base        Size      Version                  Path
  0x00400000  0xe000    1.11.2405.0000  C:\WINNT\system32\msiexec.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.dll
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.dll
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\ole32.dll
  0x770f0000  0x1b7000  1.11.2405.0000  C:\WINNT\system32\Msi.dll
  0x775a0000  0x85000   2000.02.3488.0000  C:\WINNT\system32\CLBCATQ.DLL
  0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.dll
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.dll
  0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\System32\COMCTL32.DLL
  0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\System32\USERENV.DLL
  0x77be0000  0xf000    5.00.2195.2862  C:\WINNT\system32\secur32.dll
  0x75170000  0x4f000   5.00.2195.4153  C:\WINNT\system32\netapi32.dll
  0x751c0000  0x6000    5.00.2134.0001  C:\WINNT\system32\NETRAP.DLL
  0x75150000  0x10000   5.00.2195.2780  C:\WINNT\system32\SAMLIB.DLL
  0x75030000  0x13000   5.00.2195.2780  C:\WINNT\system32\WS2_32.DLL
  0x75020000  0x8000    5.00.2134.0001  C:\WINNT\system32\WS2HELP.DLL
  0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.DLL
  0x77980000  0x24000   5.00.2195.4141  C:\WINNT\system32\DNSAPI.DLL
  0x75050000  0x8000    5.00.2195.2871  C:\WINNT\system32\WSOCK32.DLL
  0x782f0000  0x242000  5.00.3315.2902  C:\WINNT\System32\SHELL32.DLL
  0x77c70000  0x4a000   5.00.3502.4373  C:\WINNT\system32\SHLWAPI.DLL
  0x7ca00000  0x23000   5.00.2195.2228  C:\WINNT\system32\rsaenh.dll
  0x77440000  0x75000   5.131.2195.2833  C:\WINNT\system32\CRYPT32.dll
```

```
 0x77430000  0x10000   5.00.2195.4067  C:\WINNT\system32\MSASN1.DLL
--------------------------------------------------------------------------------
spoolsv.exe pid: 1532
Command line: C:\WINNT\system32\spoolsv.exe

  Base        Size      Version                  Path
 0x01000000  0xd000    5.00.2195.4299  C:\WINNT\system32\spoolsv.exe
 0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
 0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.DLL
 0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
 0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.DLL
 0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
 0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.dll
 0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.DLL
 0x76a90000  0x12000   5.00.2195.4426  C:\WINNT\system32\SPOOLSS.DLL
 0x75030000  0x13000   5.00.2195.2780  C:\WINNT\system32\WS2_32.DLL
 0x75020000  0x8000    5.00.2134.0001  C:\WINNT\system32\WS2HELP.DLL
 0x77980000  0x24000   5.00.2195.4141  C:\WINNT\system32\DNSAPI.DLL
 0x75050000  0x8000    5.00.2195.2871  C:\WINNT\system32\WSOCK32.DLL
 0x77340000  0x13000   5.00.2173.0002  C:\WINNT\system32\iphlpapi.dll
 0x77520000  0x5000    5.00.2134.0001  C:\WINNT\system32\ICMP.DLL
 0x77320000  0x17000   5.00.2181.0001  C:\WINNT\system32\MPRAPI.DLL
 0x75150000  0x10000   5.00.2195.2780  C:\WINNT\system32\SAMLIB.DLL
 0x75170000  0x4f000   5.00.2195.4153  C:\WINNT\system32\NETAPI32.DLL
 0x77be0000  0xf000    5.00.2195.2862  C:\WINNT\system32\SECUR32.DLL
 0x751c0000  0x6000    5.00.2134.0001  C:\WINNT\system32\NETRAP.DLL
 0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.DLL
 0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\OLE32.DLL
 0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.DLL
 0x773b0000  0x2e000   5.00.2195.2778  C:\WINNT\system32\ACTIVEDS.DLL
 0x77380000  0x22000   5.00.2195.4308  C:\WINNT\system32\ADSLDPC.DLL
 0x77830000  0xe000    5.00.2168.0001  C:\WINNT\system32\RTUTILS.DLL
 0x77880000  0x8d000   5.00.2195.2663  C:\WINNT\system32\SETUPAPI.DLL
 0x77c10000  0x5e000   5.00.2195.4345  C:\WINNT\system32\USERENV.DLL
 0x774e0000  0x32000   5.00.2195.2671  C:\WINNT\system32\RASAPI32.DLL
 0x774c0000  0x11000   5.00.2195.2780  C:\WINNT\system32\RASMAN.DLL
 0x77530000  0x22000   5.00.2182.0001  C:\WINNT\system32\TAPI32.DLL
 0x77b50000  0x89000   5.81.3103.1000  C:\WINNT\system32\COMCTL32.DLL
 0x77c70000  0x4a000   5.00.3502.4373  C:\WINNT\system32\SHLWAPI.DLL
 0x77360000  0x19000   5.00.2195.2778  C:\WINNT\system32\DHCPCSVC.DLL
 0x775a0000  0x85000   2000.02.3488.0000  C:\WINNT\system32\CLBCATQ.DLL
 0x777f0000  0x5000    5.00.2168.0001  C:\WINNT\system32\rasadhlp.dll
 0x76ac0000  0x40000   5.00.2195.2793  C:\WINNT\system32\localspl.dll
 0x77820000  0x7000    5.00.2134.0001  C:\WINNT\system32\VERSION.DLL
 0x759b0000  0x6000    5.00.2134.0001  C:\WINNT\system32\LZ32.DLL
 0x76980000  0x1b000   5.00.2195.2896  C:\WINNT\system32\SFC.DLL
 0x68010000  0xf0000   5.00.2195.2967  C:\WINNT\system32\sfcfiles.dll
 0x77800000  0x1d000   5.00.2195.2780  C:\WINNT\system32\winspool.drv
 0x733e0000  0xe000    0.03.0000.0000  C:\WINNT\system32\cnbjmon.dll
 0x74fd0000  0x1f000   5.00.2195.2779  C:\WINNT\system32\msafd.dll
 0x76ab0000  0x7000    5.00.2165.0001  C:\WINNT\system32\pjlmon.dll
 0x76a80000  0xd000    5.00.2195.2780  C:\WINNT\system32\tcpmon.dll
 0x76a70000  0x6000    5.00.2195.2780  C:\WINNT\system32\usbmon.dll
 0x6b460000  0x7000    5.00.2134.0001  C:\WINNT\system32\msfaxmon.dll
 0x785c0000  0xc000    5.00.2195.2871  C:\WINNT\System32\rnr20.dll
 0x777e0000  0x8000    5.00.2160.0001  C:\WINNT\System32\winrnr.dll
 0x76a50000  0x1f000   5.00.2195.2780  C:\WINNT\system32\win32spl.dll
 0x76b00000  0x13000   5.00.2195.2842  C:\WINNT\system32\inetpp.dll
 0x74e30000  0xc000    5.00.2185.0001  C:\WINNT\system32\ADMWPROX.DLL
 0x76110000  0x4000    5.00.2191.0001  C:\WINNT\system32\WMI.dll
 0x7ca00000  0x22000   5.00.2195.2228  C:\WINNT\system32\rsabase.dll
 0x77440000  0x75000   5.131.2195.2833  C:\WINNT\system32\CRYPT32.dll
```

```
  0x77430000  0x10000   5.00.2195.4067  C:\WINNT\system32\MSASN1.DLL
  0x782f0000  0x242000  5.00.3315.2902  C:\WINNT\system32\shell32.dll
-------------------------------------------------------------------------------
mdm.exe pid: 1168
Command line: C:\WINNT\System32\mdm.exe -Embedding

  Base        Size      Version                   Path
  0x00400000  0x1f000   6.00.0000.8424  C:\WINNT\System32\mdm.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.DLL
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77a50000  0xf6000   5.00.2195.4439  C:\WINNT\system32\ole32.dll
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.DLL
  0x779b0000  0x9b000   2.40.4517.0000  C:\WINNT\system32\OLEAUT32.dll
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.dll
  0x75170000  0x4f000   5.00.2195.4153  C:\WINNT\System32\netapi32.dll
  0x77be0000  0xf000    5.00.2195.2862  C:\WINNT\System32\SECUR32.DLL
  0x751c0000  0x6000    5.00.2134.0001  C:\WINNT\System32\NETRAP.DLL
  0x75150000  0x10000   5.00.2195.2780  C:\WINNT\System32\SAMLIB.DLL
  0x75030000  0x13000   5.00.2195.2780  C:\WINNT\System32\WS2_32.DLL
  0x75020000  0x8000    5.00.2134.0001  C:\WINNT\System32\WS2HELP.DLL
  0x77950000  0x2a000   5.00.2195.4436  C:\WINNT\system32\WLDAP32.DLL
  0x77980000  0x24000   5.00.2195.4141  C:\WINNT\System32\DNSAPI.DLL
  0x75050000  0x8000    5.00.2195.2871  C:\WINNT\System32\WSOCK32.DLL
  0x10000000  0xb000                    C:\Program Files\VitalSigns\Net.Medic\Program\syshook.dll
  0x775a0000  0x85000   2000.02.3488.0000  C:\WINNT\System32\CLBCATQ.DLL
  0x690a0000  0xb000    5.00.2134.0001  C:\WINNT\System32\psapi.dll
  0x4aa00000  0x15000   6.00.0000.8424  C:\WINNT\System32\msdbg.dll
-------------------------------------------------------------------------------
listdlls.exe pid: 1644
Command line: listdlls

  Base        Size      Version                   Path
  0x00400000  0xe000    2.20.0000.0000  E:\evidence gathering tools\listdlls.exe
  0x77f80000  0x7b000   5.00.2195.2779  C:\WINNT\System32\ntdll.dll
  0x77e80000  0xb5000   5.00.2195.4272  C:\WINNT\system32\KERNEL32.dll
  0x77820000  0x7000    5.00.2134.0001  C:\WINNT\system32\VERSION.dll
  0x759b0000  0x6000    5.00.2134.0001  C:\WINNT\system32\LZ32.DLL
  0x77e10000  0x64000   5.00.2195.4314  C:\WINNT\system32\USER32.dll
  0x77f40000  0x3c000   5.00.2195.3914  C:\WINNT\system32\GDI32.DLL
  0x77db0000  0x5c000   5.00.2195.4453  C:\WINNT\system32\ADVAPI32.dll
  0x77d40000  0x70000   5.00.2195.4266  C:\WINNT\system32\RPCRT4.DLL
  0x77920000  0x23000   5.00.2195.2778  C:\WINNT\system32\IMAGEHLP.dll
  0x78000000  0x46000   6.01.9359.0000  C:\WINNT\system32\MSVCRT.DLL
```