GIAC Certified Forensic Analyst (GCFA) Practical Assignment (Version 1.2)

Analysis of an Unknown Binary
Analysis of an Unfamiliar Windows 2000 System
Discussion on the Legal Issues of Incident Handling

by

Jeffrey M. Kurasiewicz
April 4, 2003

Introduction

The GIAC GCFA Practical Exam consists of three lengthy exercises related to the field of computer forensics. Part I deals with an unknown binary I obtained via download from www.giac.org. I will show how I performed a full analysis of this binary to determine what it is and why it would be present on a system. Then I will discuss some of the possible legal issues that could arise should someone be suspected of using this binary on an unauthorized system. I will close this section with a mock interrogation of the suspect.

Part II of the practical exam will show how I performed a complete forensic analysis of an unfamiliar Windows 2000 system. I will start by describing what was known about the system prior to analysis, including descriptions of the hardware configurations. I will then show how I was able to create a duplicate image of the system and use it to safely investigate the contents of the hard drive without damaging the original copy. After imaging, I will go through detail on the techniques I used to investigate the system, and document my findings. The list of the forensic techniques I covered includes the analysis of the file system, timeline analysis, string searches, and recovery of any deleted files.

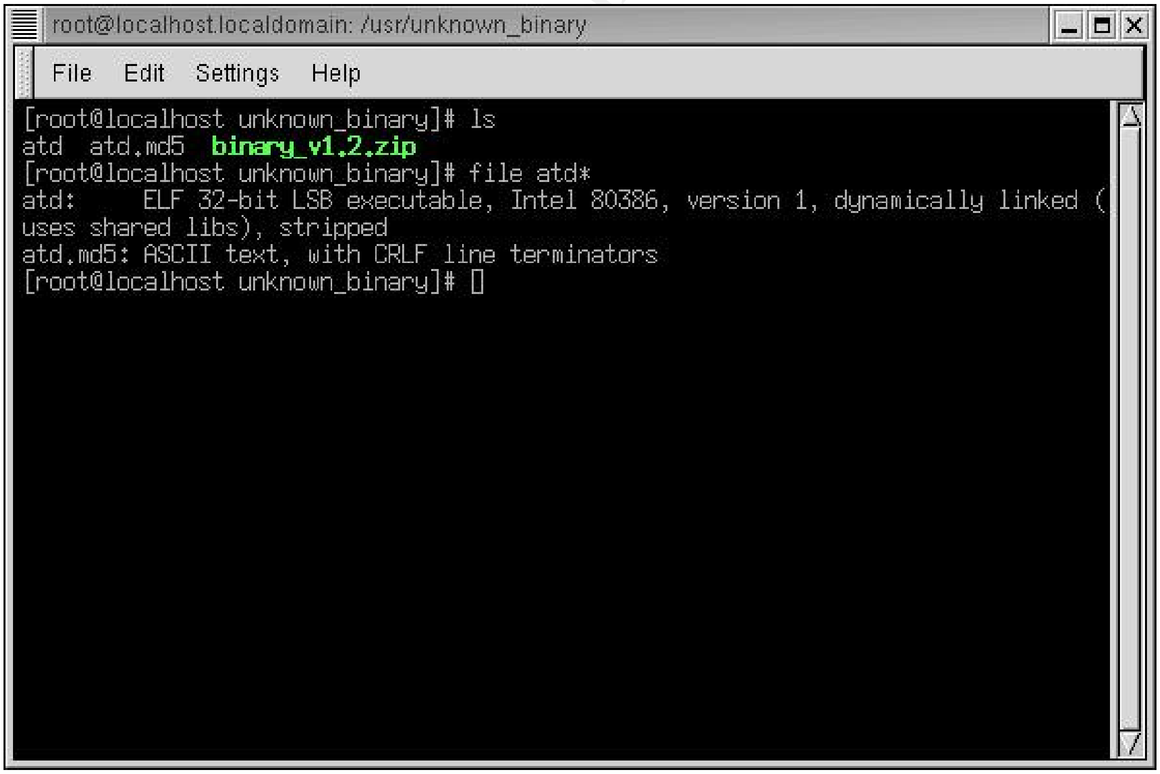
For Part III, I will discuss some of the legal issues that would be involved in a potential situation where a government agent is trying to obtain private information from an ISP system administrator about a certain user's account.

Part I: Analysis of an Unknown Binary

Preliminary Analysis

For the analysis of the unknown binary, I used my IBM T23 laptop, which I specially configured for the purposes of computer forensics examination. I set up a dual partition, the first partition with a Windows 2000 operating system installed and the other with Red Hat Linux 7.1. Both partitions have several forensic tools installed on them including many that I found to be included on the SANS Institute System Forensics, Investigations, and Response CD. Linux is generally the more preferred system to perform forensic examinations on, because of its versatility. Therefore, my initial plan was to dissect the unknown binary using the Linux partition. To ensure safety, the laptop was kept as a stand-alone machine and not connected to any outside network. All work was done logged in as root.

The first step was to unzip the binary that was downloaded off the GIAC web site, and run some preliminary commands on its contents. The zip file contained two files, “atd” and “atd.md5”. After running the **file** command I received the following information:

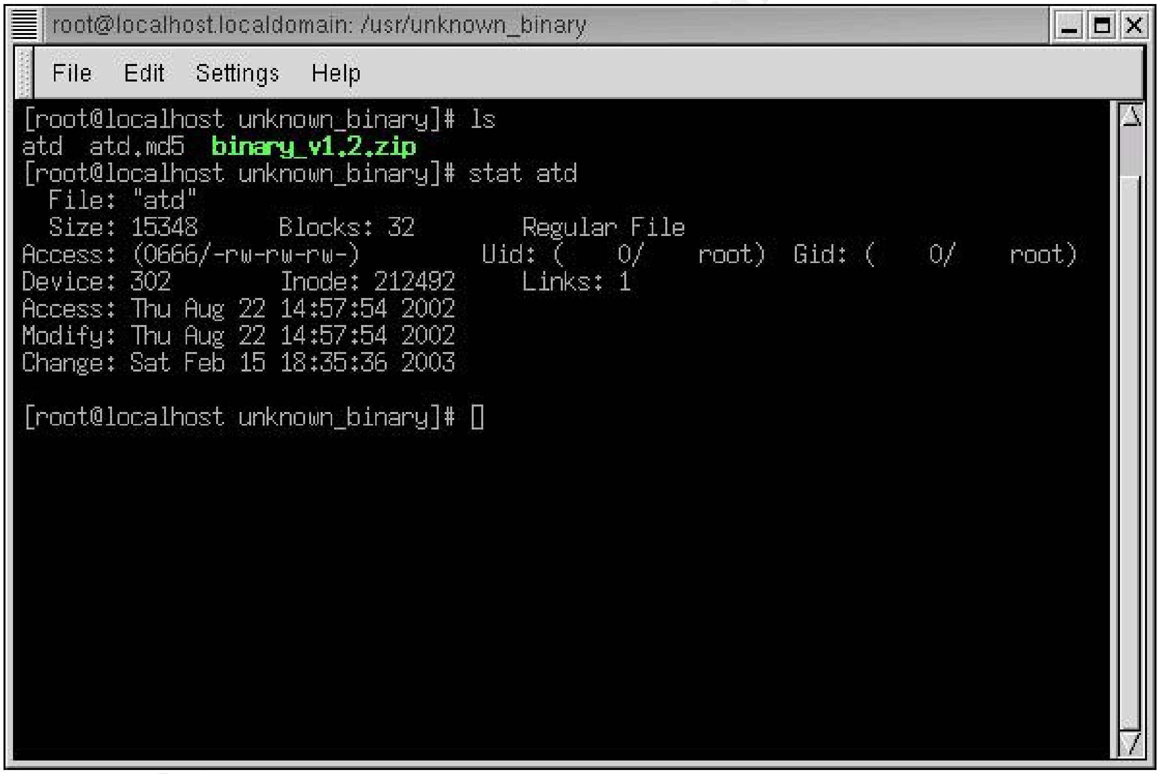


```
[root@localhost unknown_binary]# ls
atd  atd.md5  binary_v1.2.zip
[root@localhost unknown_binary]# file atd*
atd:     ELF 32-bit LSB executable, Intel 80386, version 1, dynamically linked (
uses shared libs), stripped
atd.md5: ASCII text, with CRLF line terminators
[root@localhost unknown_binary]# []
```

The output from **file** told me that atd was in fact the executable that was intended for me to perform analysis on. Of special note was the fact that the executable was compiled to run dynamically linked, so I thought it might be helpful to determine which libraries the executable needs loaded when it is called. The binary was also stripped, so the symbols from the object files were removed, significantly decreasing the file's size after compilation.

Atd.md5 turned out to be an ordinary ASCII text file that contained what was probably the MD5 hash value of the executable.

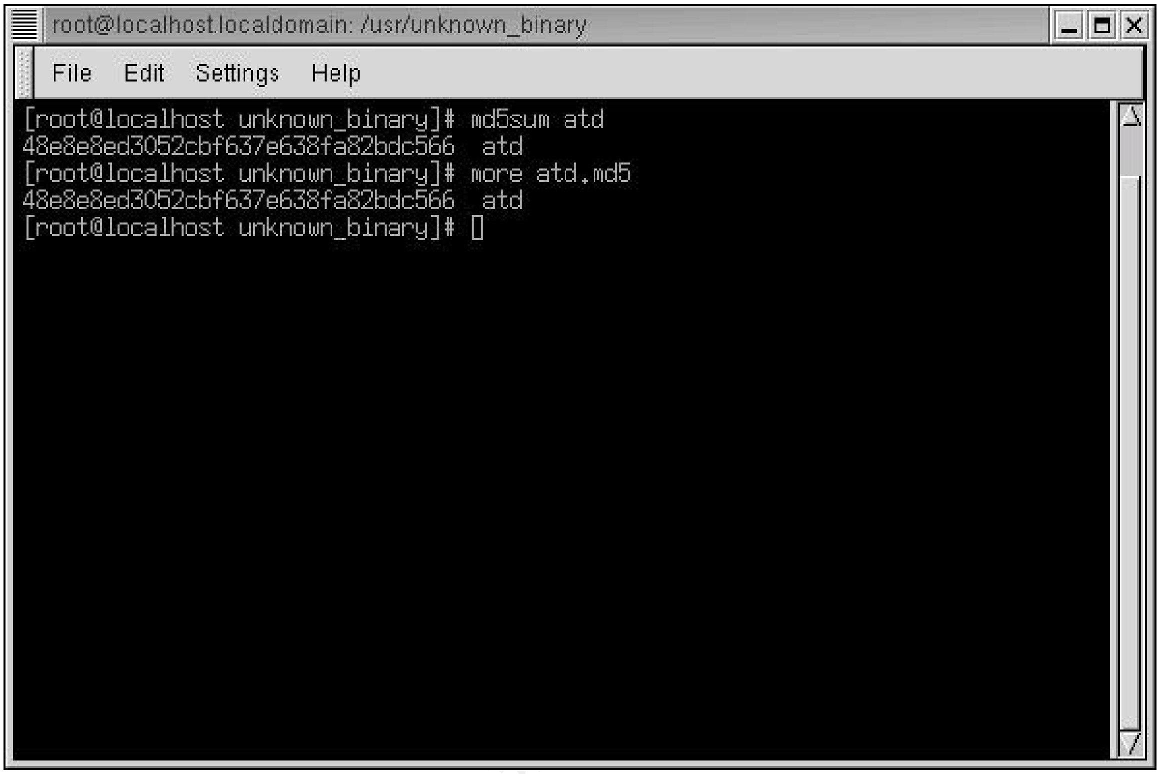
I ran the **stat** command on atd but noticed the access time had already been corrupted by running **file**, so I re-unzipped the binary and ran **stat** on a fresh sample. Normally I would have made a backup copy of the evidence, but in this situation I already had the zip file to work from. The output from **stat** produced the following results:



```
[root@localhost unknown_binary]# ls
atd  atd.md5  binary_v1.2.zip
[root@localhost unknown_binary]# stat atd
  File: "atd"
  Size: 15348      Blocks: 32        Regular File
Access: (0666/-rw-rw-rw-)        Uid: (    0/    root)  Gid: (    0/    root)
Device: 302        Inode: 212492     Links: 1
Access: Thu Aug 22 14:57:54 2002
Modify: Thu Aug 22 14:57:54 2002
Change: Sat Feb 15 18:35:36 2003

[root@localhost unknown_binary]# 
```

The binary was last accessed and modified on Thursday, August 22 2002 at 2:57 PM. Since I had just unzipped the file the creation time was the current time of Saturday, February 15, 2003 at 6:35 PM. The file's size was 15,348 bytes. Unfortunately, the file's owner was found to be myself: root with ID 0. Unlike the tar command, files that are packaged under Zip do not retain the former username or ID. The binary was set with read and write permissions but not execution permissions.

An MD5 hash of the file was produced using Md5sum, and the hash proved to be identical to the hash value found in atd.md5. The evidence had not been altered so far:



```
[root@localhost unknown_binary]# md5sum atd
48e8e8ed3052cbf637e638fa82bdc566  atd
[root@localhost unknown_binary]# more atd.md5
48e8e8ed3052cbf637e638fa82bdc566  atd
[root@localhost unknown_binary]# []
```

To get some clues as to how this executable ran and what it might be used for, I ran the command **strings** to pull out any sets of character data longer than three characters:

```
/lib/ld-linux.so.1
libc.so.5
longjmp
strcpy
ioctl
popen
shmctl
geteuid
_DYNAMIC
getprotobynumber
errno
__strtol_internal
usleep
semget
getpid
fgets
shmat
_IO_stderr_
perror
getuid
semctl
optarg
socket
__environ
bzero
_init
```

```
alarm
__libc_init
environ
fprintf
kill
inet_addr
chdir
shmdt
setsockopt
__fpu_control
shmget
wait
umask
signal
read
strncmp
sendto
bcopy
fork
strdup
getopt
inet_ntoa
getppid
time
gethostbyname
_fini
sprintf
difftime
atexit
_GLOBAL_OFFSET_TABLE_
semop
exit
__setfpucw
open
setsid
close
_errno
_etext
_edata
__bss_start
_end
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
```

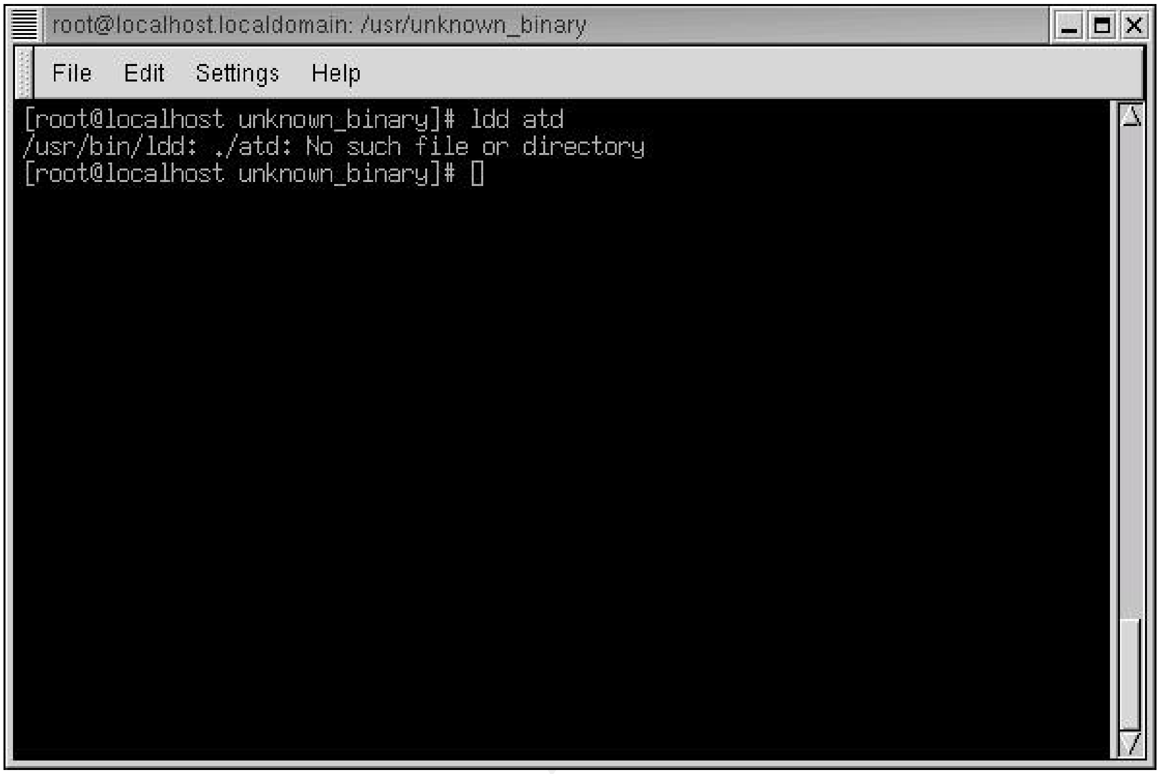
```
lokid: Client database full
DEBUG: stat_client nono
lokid version:        %s
remote interface:     %s
active transport:     %s
active cryptography:  %s
server uptime:        %.02f minutes
client ID:            %d
packets written:      %ld
bytes written:        %ld
requests:             %d
N@[fatal] 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 shmid
[fatal] cannot destroy semaphore
[fatal] name lookup failed
[fatal] cannot catch SIGALRM
[fatal] cannot catch SIGCHLD
[fatal] Cannot go daemon
[fatal] Cannot create session
/dev/tty
[fatal] cannot detach from controlling terminal
/tmp
[fatal] invalid user identification value
v:p:
Unknown transport
lokid -p (i|u) [ -v (0|1) ]
[fatal] socket allocation error
[fatal] cannot catch SIGUSR1
Cannot set IP_HDRINCL socket option
[fatal] cannot register with atexit(2)
LOKI2   route [(c) 1997 guild corporation worldwide]
[fatal] cannot catch SIGALRM
[fatal] cannot catch SIGCHLD
[SUPER fatal] control should NEVER fall here
[fatal] forking error
lokid: server is currently at capacity.  Try again later
lokid: Cannot add key
lokid: popen
[non fatal] truncated write
/quit all
lokid: client <%d> requested an all kill
        sending L_QUIT: <%d> %s
lokid: clean exit (killed at client request)
[fatal] could not signal process group
/quit
lokid: cannot locate client entry in database
lokid: client <%d> freed from list [%d]
/stat
/swapt
[fatal] could not signal parent
lokid: unsupported or unknown command string
lokid: client <%d> requested a protocol swap
        sending protocol update: <%d> %s [%d]
lokid: transport protocol changed to %s
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
01.01
01.01
01.01
```

```
01.01
01.01
01.01
01.01
01.01
.symtab
.strtab
.shstrtab
.interp
.hash
.dynsym
.dynstr
.rel.bss
.rel.plt
.init
.plt
.text
.fini
.rodata
.data
.ctors
.dtors
.got
.dynamic
.bss
.comment
.note
```

Right away I noticed the first two lines of the **strings** output contained the names of a pair of libraries: ld-linux.so.1 and libc.so.5. I searched my system to see if I already had these installed. I found ld-linux.so.2 and libc.so.6, so the libraries listed in the binary were a little outdated. There were also many references to sockets, daemons, and clients, so the executable probably had something to do with network communications. There were also what appeared to be several error/notification messages with the name "lokid:" preceding them. One line in particular looked like the results of running a version check: "LOKI2 route [© 1997 guild corporation worldwide]". I concluded at this point that the name of the program was probably Loki, Loki2, or something similar. Another line looked like a template for how the user might execute the binary from the command line: "lokid –p (I|u) [-v (0|1)]".

The version of **gcc** compiler used (2.7.2.1) was found near the bottom of the list. I typed in "**gcc** –v" to check my own version and saw that I had version 2.96, and this was on RedHat Linux 7.1. From this I figured that the compiler used to create this binary, as well as the libraries, must not be very current.

In order to verify the libraries I found in **strings**, I decided to run **ldd** to obtain a listing of .dlls used by the binary:



```
[root@localhost unknown_binary]# ldd atd
/usr/bin/ldd: ./atd: No such file or directory
[root@localhost unknown_binary]# []
```

The results were inconclusive. I may have received this error because I did not have the libraries mentioned above installed on my system.

I ran the binary through some additional tests just to be thorough in my investigation. By using **objdump** I was able to again verify that the file was an ELF 32-bit executable that required the libc.so.5 library. Also as expected, no object symbols could be extracted. Everything appeared to be normal. The executable entry point address was found at 0x08048db0, which is typical. I checked this because an abnormal starting position can sometimes be a clue that you are dealing with a malevolent binary and someone is trying to make it difficult for investigators to analyze its contents.

```
atd:     file format elf32-i386
atd
architecture: i386, flags 0x00000112:
EXEC_P, HAS_SYMS, D_PAGED
start address 0x08048db0

Program Header:
    PHDR off    0x00000034 vaddr 0x08048034 paddr 0x08048034 align 2**2
         filesz 0x000000a0 memsz 0x000000a0 flags r-x
  INTERP off    0x000000d4 vaddr 0x080480d4 paddr 0x080480d4 align 2**0
         filesz 0x00000013 memsz 0x00000013 flags r--
    LOAD off    0x00000000 vaddr 0x08048000 paddr 0x08048000 align 2**12
         filesz 0x00003524 memsz 0x00003524 flags r-x
    LOAD off    0x00003528 vaddr 0x0804c528 paddr 0x0804c528 align 2**12
         filesz 0x000001a4 memsz 0x000002d0 flags rw-
```

```
 DYNAMIC off    0x00003644 vaddr 0x0804c644 paddr 0x0804c644 align 2**2
         filesz 0x00000088 memsz 0x00000088 flags rw-

Dynamic Section:
  NEEDED      libc.so.5
  INIT        0x8048a70
  FINI        0x804a8e0
  HASH        0x80480e8
  STRTAB      0x80486ac
  SYMTAB      0x804828c
  STRSZ       0x210
  SYMENT      0x10
  DEBUG       0x0
  PLTGOT      0x804c570
  PLTRELSZ    0x190
  PLTREL      0x11
  JMPREL      0x80488dc
  REL         0x80488bc
  RELSZ       0x20
  RELENT      0x8

Sections:
Idx Name          Size      VMA       LMA       File off  Algn
  0 .interp       00000013  080480d4  080480d4  000000d4  2**0
                  CONTENTS, ALLOC, LOAD, READONLY, DATA
  1 .hash         000001a4  080480e8  080480e8  000000e8  2**2
                  CONTENTS, ALLOC, LOAD, READONLY, DATA
  2 .dynsym       00000420  0804828c  0804828c  0000028c  2**2
                  CONTENTS, ALLOC, LOAD, READONLY, DATA
  3 .dynstr       00000210  080486ac  080486ac  000006ac  2**0
                  CONTENTS, ALLOC, LOAD, READONLY, DATA
  4 .rel.bss      00000020  080488bc  080488bc  000008bc  2**2
                  CONTENTS, ALLOC, LOAD, READONLY, DATA
  5 .rel.plt      00000190  080488dc  080488dc  000008dc  2**2
                  CONTENTS, ALLOC, LOAD, READONLY, DATA
  6 .init         00000008  08048a70  08048a70  00000a70  2**4
                  CONTENTS, ALLOC, LOAD, READONLY, CODE
  7 .plt          00000330  08048a78  08048a78  00000a78  2**2
                  CONTENTS, ALLOC, LOAD, READONLY, CODE
  8 .text         00001b28  08048db0  08048db0  00000db0  2**4
                  CONTENTS, ALLOC, LOAD, READONLY, CODE
  9 .fini         00000008  0804a8e0  0804a8e0  000028e0  2**4
                  CONTENTS, ALLOC, LOAD, READONLY, CODE
 10 .rodata       00000c3c  0804a8e8  0804a8e8  000028e8  2**2
                  CONTENTS, ALLOC, LOAD, READONLY, DATA
 11 .data         00000038  0804c528  0804c528  00003528  2**2
                  CONTENTS, ALLOC, LOAD, DATA
 12 .ctors        00000008  0804c560  0804c560  00003560  2**2
                  CONTENTS, ALLOC, LOAD, DATA
 13 .dtors        00000008  0804c568  0804c568  00003568  2**2
                  CONTENTS, ALLOC, LOAD, DATA
 14 .got          000000d4  0804c570  0804c570  00003570  2**2
                  CONTENTS, ALLOC, LOAD, DATA
 15 .dynamic      00000088  0804c644  0804c644  00003644  2**2
                  CONTENTS, ALLOC, LOAD, DATA
 16 .bss          0000012c  0804c6cc  0804c6cc  000036cc  2**3
                  ALLOC
 17 .comment      000000a0  00000000  00000000  000036cc  2**0
                  CONTENTS, READONLY
 18 .note         000000a0  000000a0  000000a0  0000376c  2**0
                  CONTENTS, READONLY
```

Since the binary was an ELF format, I used **readelf** to see if I could gather any more useful information. The **readelf** results matched up with the rest of my analysis so far, and I did not see anything out of the ordinary.

```
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 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 0000d4 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              Symbol's Value  Symbol's Name
  0804c6d8  01005 R_386_COPY              0804c6d8  _IO_stderr_
  0804c72c  01405 R_386_COPY              0804c72c  optarg
  0804c730  02205 R_386_COPY              0804c730  __fpu_control
  0804c6d0  03d05 R_386_COPY              0804c6d0  _errno

Relocation section '.rel.plt' at offset 0x8dc contains 50 entries:
  Offset    Info  Type              Symbol's Value  Symbol's Name
  0804c57c  00107 R_386_JUMP_SLOT         08048a88  longjmp
  0804c580  00207 R_386_JUMP_SLOT         08048a98  strcpy
  0804c584  00307 R_386_JUMP_SLOT         08048aa8  ioctl
  0804c588  00407 R_386_JUMP_SLOT         08048ab8  popen
  0804c58c  00507 R_386_JUMP_SLOT         08048ac8  shmctl
  0804c590  00607 R_386_JUMP_SLOT         08048ad8  geteuid
  0804c594  00807 R_386_JUMP_SLOT         08048ae8  getprotobynumber
  0804c598  00a07 R_386_JUMP_SLOT         08048af8  __strtol_internal
  0804c59c  00b07 R_386_JUMP_SLOT         08048b08  usleep
  0804c5a0  00c07 R_386_JUMP_SLOT         08048b18  semget
  0804c5a4  00d07 R_386_JUMP_SLOT         08048b28  getpid
  0804c5a8  00e07 R_386_JUMP_SLOT         08048b38  fgets
  0804c5ac  00f07 R_386_JUMP_SLOT         08048b48  shmat
  0804c5b0  01107 R_386_JUMP_SLOT         08048b58  perror
  0804c5b4  01207 R_386_JUMP_SLOT         08048b68  getuid
  0804c5b8  01307 R_386_JUMP_SLOT         08048b78  semctl
  0804c5bc  01507 R_386_JUMP_SLOT         08048b88  socket
  0804c5c0  01707 R_386_JUMP_SLOT         08048b98  bzero
  0804c5c4  01907 R_386_JUMP_SLOT         08048ba8  alarm
  0804c5c8  01a07 R_386_JUMP_SLOT         08048bb8  __libc_init
  0804c5cc  01c07 R_386_JUMP_SLOT         08048bc8  fprintf
  0804c5d0  01d07 R_386_JUMP_SLOT         08048bd8  kill
  0804c5d4  01e07 R_386_JUMP_SLOT         08048be8  inet_addr
  0804c5d8  01f07 R_386_JUMP_SLOT         08048bf8  chdir
  0804c5dc  02007 R_386_JUMP_SLOT         08048c08  shmdt
  0804c5e0  02107 R_386_JUMP_SLOT         08048c18  setsockopt
  0804c5e4  02307 R_386_JUMP_SLOT         08048c28  shmget
  0804c5e8  02407 R_386_JUMP_SLOT         08048c38  wait
  0804c5ec  02507 R_386_JUMP_SLOT         08048c48  umask
  0804c5f0  02607 R_386_JUMP_SLOT         08048c58  signal
  0804c5f4  02707 R_386_JUMP_SLOT         08048c68  read
  0804c5f8  02807 R_386_JUMP_SLOT         08048c78  strncmp
  0804c5fc  02907 R_386_JUMP_SLOT         08048c88  sendto
  0804c600  02a07 R_386_JUMP_SLOT         08048c98  bcopy
  0804c604  02b07 R_386_JUMP_SLOT         08048ca8  fork
  0804c608  02c07 R_386_JUMP_SLOT         08048cb8  strdup
  0804c60c  02d07 R_386_JUMP_SLOT         08048cc8  getopt
  0804c610  02e07 R_386_JUMP_SLOT         08048cd8  inet_ntoa
  0804c614  02f07 R_386_JUMP_SLOT         08048ce8  getppid
  0804c618  03007 R_386_JUMP_SLOT         08048cf8  time
  0804c61c  03107 R_386_JUMP_SLOT         08048d08  gethostbyname
  0804c620  03307 R_386_JUMP_SLOT       08048d18  sprintf
  0804c624  03407 R_386_JUMP_SLOT       08048d28  difftime
  0804c628  03507 R_386_JUMP_SLOT       08048d38  atexit
  0804c62c  03707 R_386_JUMP_SLOT       08048d48  semop
  0804c630  03807 R_386_JUMP_SLOT       08048d58  exit
  0804c634  03907 R_386_JUMP_SLOT       08048d68  __setfpucw
  0804c638  03a07 R_386_JUMP_SLOT       08048d78  open
  0804c63c  03b07 R_386_JUMP_SLOT       08048d88  setsid
  0804c640  03c07 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 
     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.
```

Overview of the Loki Program

Before going on to finally execute the binary using tracing options, I felt that I could possibly save some time and effort by researching some of the clues I found in the Strings output. I thought that if the binary turned out to be a particularly nasty virus or something similar, I might have been able to take some extra precautions to save myself from having to create another test system. I decided to search the Internet for any information I could find on Loki, Loki2, or Lokid. Using www.google.com I found several links on the web leading back to two interesting whitepapers from Phrack magazine, an underground publication for hackers. The first whitepaper, entitled “Project Loki: ICMP Tunneling”, gave a general overview of the Loki program and the technology behind it. The second was simply entitled “LOKI2 (the implementation)”, and was meant to be the follow-up how-to guide and source code listing for the first article. According to the Phrack articles, Loki was an ICMP information tunneler, in that it used the ICMP protocol to send and receive information discreetly.

The ICMP protocol’s intended use is to provide a universal means of relaying error messages and the like across unicast addresses. ICMP packets are generally ignored by firewalls and other security checkpoints, so the information contained within them can be sent back and forth freely. Programs like Ping use the protocol to find out if a particular host is reachable without having to deal with firewalls and other roadblocks. Someone realized this and decided to exploit the weakness by writing Loki. Following a system compromise, Loki can be set up in a client-server fashion and format any desired information to match the ICMP protocol. It will then send it out underneath the firewall of a system without raising any red flags for system administration, acting as a backdoor for the attacker.

Executing the Binary

Before I could run atd, I had to change the file permissions because the access rights were previously set to block execution of the binary, yet read and write access were granted. I thought this was a little odd, as it gave the impression that the binary had never been run before. I also had to obtain the required libraries, ld-linux.so.1 and libc.so.5, from some older Red Hat RPMs. To get a clear picture of what was going on during execution, I decided to use **strace**. **Strace** is a UNIX command that can obtain a detailed trace of the system operations of an executable. I set the –ff option so I could get traces of atd as well as any child processes it might spawn. Upon launching the executable I received the following output, further confirming that this binary was somehow related to the Loki ICMP tunneler:

```
LOKI2   route [© 1997 guild corporation worldwide]
```

A breakdown of the **strace** results follows:

```
execve("./atd", ["./atd"], [/* 40 vars */]) = 0
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40007000
mprotect(0x40000000, 21420, 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=58970, ...}) = 0
open("/etc/ld.so.cache", O_RDONLY)      = 3
old_mmap(NULL, 58970, PROT_READ, MAP_SHARED, 3, 0) = 0x40008000
close(3)                                = 0
stat("/etc/ld.so.preload", 0xbffff8b8)  = -1 ENOENT (No such file or directory)
open("/usr/lib/libc.so.5", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/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\310\'\1"..., 4096) = 4096
old_mmap(NULL, 770048, PROT_NONE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40017000
old_mmap(0x40017000, 536799, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_FIXED, 3, 0) =
0x40017000
old_mmap(0x4009b000, 19404, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED, 3, 0x83000) =
0x4009b000
old_mmap(0x400a0000, 206520, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -
1, 0) = 0x400a0000
close(3)                                = 0
mprotect(0x40017000, 536799, PROT_READ|PROT_WRITE|PROT_EXEC) = 0
munmap(0x40008000, 58970)               = 0
mprotect(0x8048000, 13604, PROT_READ|PROT_EXEC) = 0
mprotect(0x40017000, 536799, PROT_READ|PROT_EXEC) = 0
mprotect(0x40000000, 21420, PROT_READ|PROT_EXEC) = 0
personality(PER_LINUX)                  = 0
geteuid()                               = 0
getuid()                                = 0
getgid()                                = 0
getegid()                               = 0
geteuid()                               = 0
getuid()                                = 0
brk(0x804c820)                          = 0x804c820
brk(0x804d000)                          = 0x804d000
open("/usr/share/locale/locale.alias", O_RDONLY) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=2601, ...}) = 0
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40008000
read(3, "# Locale name alias data base.\n#"..., 4096) = 2601
brk(0x804e000)                          = 0x804e000
read(3, "", 4096)                       = 0
close(3)                                = 0
munmap(0x40008000, 4096)                = 0
```

```
open("/usr/share/i18n/locale.alias", O_RDONLY) = -1 ENOENT (No such file or directory)
open("/usr/share/locale/en_US/LC_MESSAGES", O_RDONLY) = -1 ENOENT (No such file or
directory)
open("/usr/share/locale/en/LC_MESSAGES", O_RDONLY) = -1 ENOENT (No such file or
directory)
stat("/etc/locale/C/libc.cat", 0xbffff3d8) = -1 ENOENT (No such file or directory)
stat("/usr/share/locale/C/libc.cat", 0xbffff3d8) = -1 ENOENT (No such file or directory)
stat("/usr/share/locale/libc/C", 0xbffff3d8) = -1 ENOENT (No such file or directory)
stat("/usr/share/locale/C/libc.cat", 0xbffff3d8) = -1 ENOENT (No such file or directory)
stat("/usr/local/share/locale/C/libc.cat", 0xbffff3d8) = -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},
0x4005c648) = 0
socket(PF_INET, SOCK_RAW, IPPROTO_RAW)  = 4
setsockopt(4, SOL_IP, IP_HDRINCL, [1], 4) = 0
getpid()                                = 1102
getpid()                                = 1102
shmget(1344, 240, IPC_CREAT|0)          = 5242891
semget(1526, 1, IPC_CREAT|0x180|0600)   = 0
shmat(5242891, 0, 0)                    = 0x40008000
write(2, "\nLOKI2\troute [(c) 1997 guild cor"..., 52) = 52
time([1045950450])                      = 1045950450
close(0)                                = 0
sigaction(SIGTTOU, {SIG_IGN}, {SIG_DFL}, 0x4005c648) = 0
sigaction(SIGTTIN, {SIG_IGN}, {SIG_DFL}, 0x4005c648) = 0
sigaction(SIGTSTP, {SIG_IGN}, {SIG_DFL}, 0x4005c648) = 0
fork()                                  = 1103
close(4)                                = 0
close(3)                                = 0
semop(0, 0xbffff854, 2)                 = 0
shmdt(0x40008000)                       = 0
semop(0, 0xbffff854, 1)                 = 0
_exit(0)                                = ?
```

The executable began by accessing /etc/ld.so.cache. Shortly after, I noticed it searched for the required libc.so.5 library and finally accessed it in the /lib directory. Some portions of libc.so.5 were read and stored into memory. The binary then did a series of user ID checks to determine the current user belonging to the process. Then it searched for the alias database in a number of typical default directories. It proceeded to read in my locale information at /usr/share/locale/locale.alias. Several attempts were made to either open or run a **stat** command on a list of other locale-related files, yet all of them failed because these files did not exist on my system. At this point I noticed a common link in the trace between the binary and the Loki program I had researched, as two raw ICMP sockets were opened and the socket settings were configured. I saw the LOKI2 banner being written to output. The program then spawned a child process using **fork**() and terminated itself shortly after. The child process was also recorded by **strace** and produced more data to examine:

```
setsid()                                = 1103
open("/dev/tty", O_RDWR)                = -1 ENXIO (No such device or address)
chdir("/tmp")                           = 0
umask(0)                                = 022
sigaction(SIGALRM, {0x8049218, [], SA_INTERRUPT|SA_NOMASK|SA_ONESHOT}, {SIG_DFL},
0x4005c648) = 0
alarm(3600)                             = 0
sigaction(SIGCHLD, {0x8049900, [], SA_INTERRUPT|SA_NOMASK|SA_ONESHOT}, {SIG_DFL},
0x4005c648) = 0
read(3, 0x804c78c, 84)                  = ? ERESTARTSYS (To be restarted)
--- SIGTERM (Terminated) ---
```

The child process was spawned with a PID of 1103. It first attempted to get the name of the terminal, but failed. The working directory was changed to /tmp and more signal settings were configured. An alarm was set for the delivery of a signal.

To be thorough, I also ran **ltrace** to get a look at the library activity. **Ltrace** produced nearly identical results to **strace**, but in greater detail as all the standard library calls were shown during the file reads, etc.

Upon using **netstat** to observe the current state of my network, I discovered the two raw ICMP sockets still lingering on the system (addresses 0.0.0.0:1 and 0.0.0.0:255):

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:32768           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:32768           0.0.0.0:*
udp        0      0 0.0.0.0:111             0.0.0.0:*
udp        0      0 0.0.0.0:759             0.0.0.0:*
raw        0      0 0.0.0.0:1               0.0.0.0:*               7
raw        0      0 0.0.0.0:255             0.0.0.0:*               7
```

It appeared as if these sockets were listening for incoming ICMP messages, so the binary could have represented the Loki server component. I ran a quick check to see that the child process was still running using **ps** and noted the processes at PID 1101 and 1103:

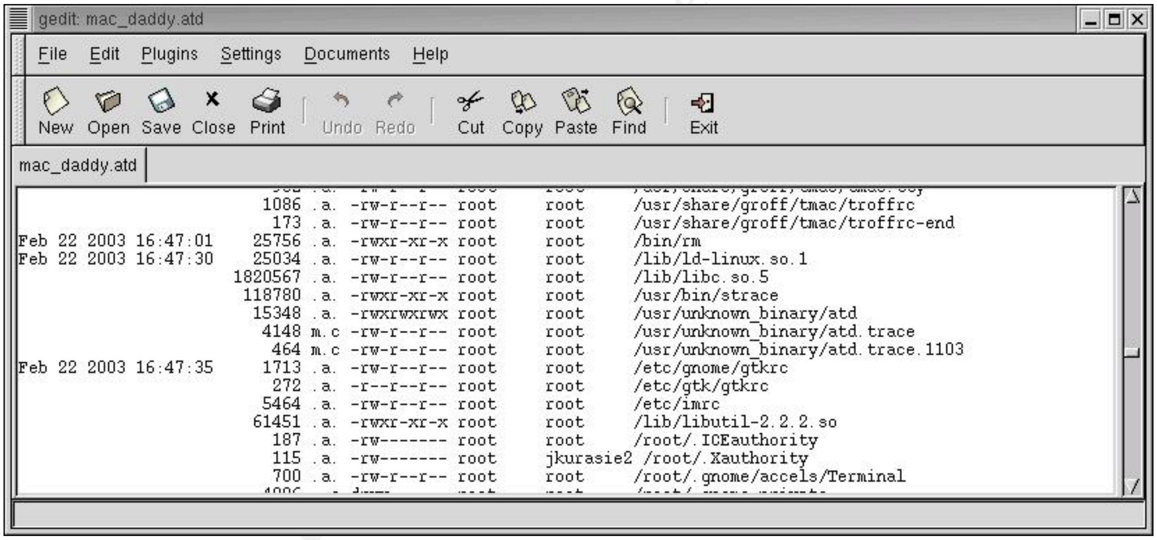
```
UID        PID  PPID  C STIME TTY          TIME CMD
root      1101  1062  0 16:47 pts/0    00:00:00 strace -ff -o atd.trace ./atd
root      1103     1  0 16:47 ?        00:00:00 ./atd
```

In order to discover the footprints left on the file system (if any), I decided to run **lsof** to get a list of the currently open files, followed by a MACtime analysis. I received typical results with **lsof**:

```
COMMAND    PID USER   FD   TYPE     DEVICE    SIZE     NODE NAME
strace    1101 root  cwd    DIR        3,2    4096   212484 /usr/unknown_binary
strace    1101 root  rtd    DIR        3,2    4096        2 /
strace    1101 root  txt    REG        3,2  118780   617421 /usr/bin/strace
strace    1101 root  mem    REG        3,2  471781   113433 /lib/ld-2.2.2.so
strace    1101 root  mem    REG        3,2 5634864   291518 /lib/i686/libc-2.2.2.so
strace    1101 root    0u   CHR      136,0                 2 /dev/pts/0
strace    1101 root    1u   CHR      136,0                 2 /dev/pts/0
strace    1101 root    2u   CHR      136,0                 2 /dev/pts/0
strace    1101 root    3w   REG        3,2    4148   212512 /usr/unknown_binary/atd.trace
strace    1101 root    4w   REG        3,2     464   212513
/usr/unknown_binary/atd.trace.1103
atd       1103 root  cwd    DIR        3,2    4096   178113 /tmp
atd       1103 root  rtd    DIR        3,2    4096        2 /
atd       1103 root  txt    REG        3,2   15348   212492 /usr/unknown_binary/atd
atd       1103 root  mem    REG        3,2   25034   115522 /lib/ld-linux.so.1
atd       1103 root  mem    REG        3,2 1820567   115525 /lib/libc.so.5
atd       1103 root    1u   CHR      136,0                 2 /dev/pts/0
atd       1103 root    2u   CHR       136,0                  2 /dev/pts/0
atd       1103 root    3u   raw                           2977 00000000:0001->00000000:0000
st=07
atd       1103 root    4u   raw                           2978 00000000:00FF->00000000:0000
st=07
```

Lsof showed the **strace** process started at PID 1101 and the child it spawned at PID 1103. The libraries ld-linux.so.1 and libc.so.5 were accessed. The raw ICMP sockets were currently still open and listening through PID 1103. I did not find much else of interest in the remainder of the **lsof** results.

The MACTime analysis also did not give any new clues at this point as well. I essentially used it to verify what I had seen thus far. To get a timeline of the system I used the mac_daddy.pl Perl script, which I have found to be very quick and easy to use. The point of interest occurred at 16:47, when the executable was launched:


gedit: mac_daddy.atd
File Edit Plugins Settings Documents Help
New Open Save Close Print Undo Redo Cut Copy Paste Find Exit
mac_daddy.atd

```
                           1086 .a. -rw-r--r-- root     root     /usr/share/groff/tmac/troffrc
                            173 .a. -rw-r--r-- root     root     /usr/share/groff/tmac/troffrc-end
Feb 22 2003 16:47:01      25756 .a. -rwxr-xr-x root     root     /bin/rm
Feb 22 2003 16:47:30      25034 .a. -rw-r--r-- root     root     /lib/ld-linux.so.1
                        1820567 .a. -rw-r--r-- root     root     /lib/libc.so.5
                         118780 .a. -rwxr-xr-x root     root     /usr/bin/strace
                          15348 .a. -rwxrwxrwx root     root     /usr/unknown_binary/atd
                           4148 m.c -rw-r--r-- root     root     /usr/unknown_binary/atd.trace
                            464 m.c -rw-r--r-- root     root     /usr/unknown_binary/atd.trace.1103
Feb 22 2003 16:47:35       1713 .a. -rw-r--r-- root     root     /etc/gnome/gtkrc
                            272 .a. -r--r--r-- root     root     /etc/gtk/gtkrc
                           5464 .a. -rw-r--r-- root     root     /etc/imrc
                          61451 .a. -rwxr-xr-x root     root     /lib/libutil-2.2.2.so
                            187 .a. -rw------- root     root     /root/.ICEauthority
                            115 .a. -rw------- root     jkurasie2 /root/.Xauthority
                            700 .a. -rw-r--r-- root     root     /root/.gnome/accels/Terminal
```

The mac_daddy output shows that the two libraries were accessed at the time the file was run, and also shows my traces being created. I was surprised that I didn't catch the two other files being accessed in the **strace** report (ld.so.cache and locale.alias). I searched down the mac_daddy listing a bit further and spotted them. The mac_daddy script itself had accessed those two files upon execution, slightly skewing the results of the MACTime analysis. This was a good example of how volatile a UNIX system can be, and why it's important to do timeline analysis as soon as possible before stepping on other parts of the system.

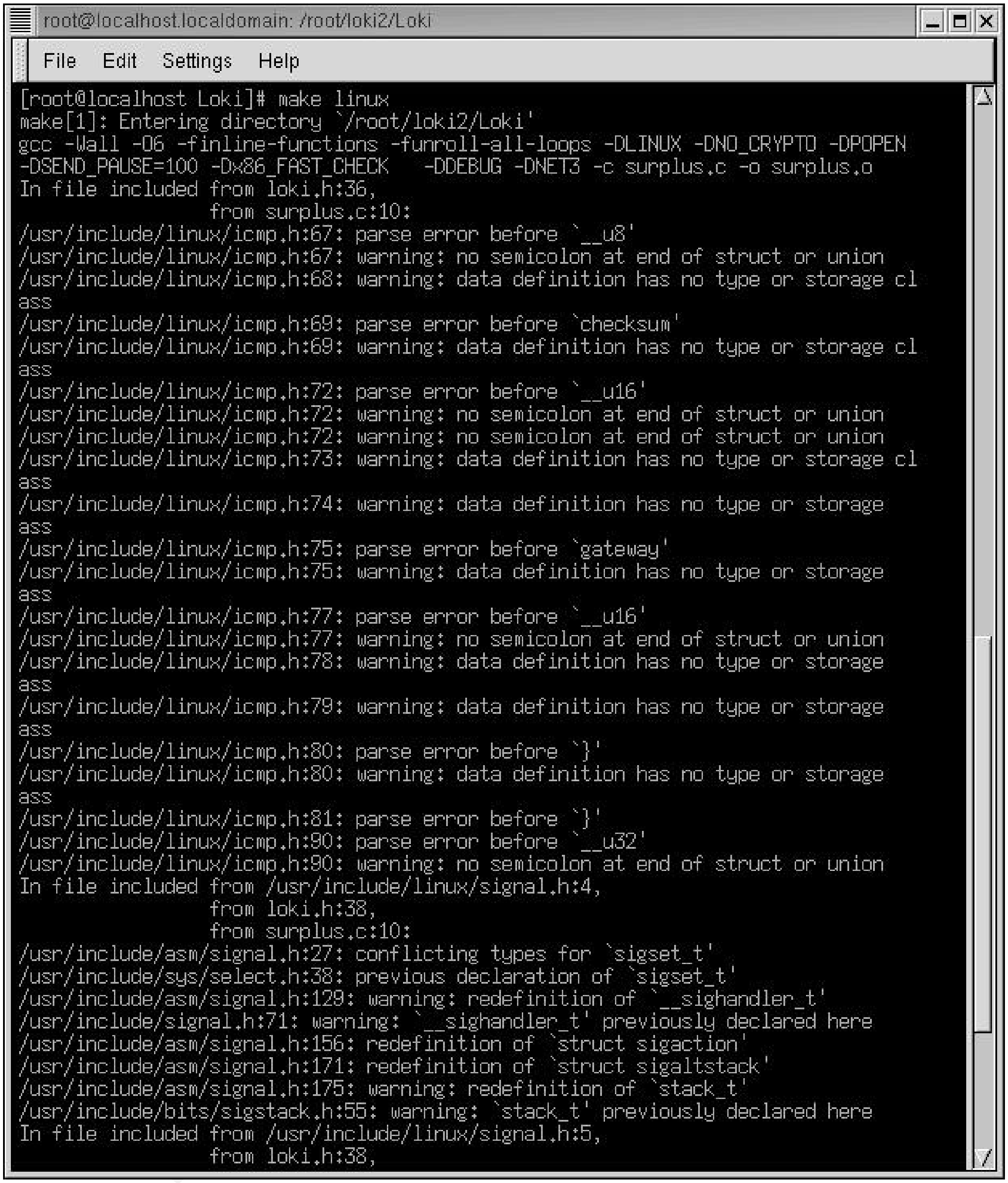
By now it was fairly certain that I was dealing with a component related to the Loki ICMP tunneller. From examination of the results of **strace** and Mac_daddy, atd did not appear to make any modifications to the file system when run. This makes sense, however, as it would be a desired trait of a clandestine communications server.

Compiling Loki

At this time I proceeded to research Loki further in attempt to compile the program and compare my results with atd. After reading “LOKI2 (The Implementation)” off of the Phrack web site, I learned that the Phrack code included with the article was only supported on Linux 2.0.x, OpenBSD 2.1, FreeBSD 2.1.x, and Solaris 2.5.x. I spent a good deal of time searching the web for an old version of Linux, and finally as a last resort for FreeBSD, but nothing that obsolete was easily available anymore. I then decided to just try to force a compile on my Linux 7.1 machine. To make things easier, I downloaded a copy of Loki2 from www.packetstormsecurity.org. After extracting the contents from the .tar.gz file I was presented with the following source code:

```
.:
total 104
-rw-------    1 root     root         6685 Aug 25  1997 client_db.c
-rw-------    1 root     root         1750 Aug 18  1997 client_db.h
-rw-------    1 root     root         3971 Aug 18  1997 crypt.c
-rw-------    1 root     root          470 Aug 11  1997 crypt.h
-rw-------    1 root     root        16718 Aug 27  1997 loki.c
-rw-------    1 root     root        18878 Aug 27  1997 lokid.c
-rw-------    1 root     root        14740 Oct  8  1997 loki.h
-rw-------    1 root     root         2631 Aug 29  1997 Makefile
drwx------    2 root     root         4096 Aug 25  1997 md5
-rw-------    1 root     root         3739 Aug 25  1997 pty.c
-rw-------    1 root     root         2813 Aug 18  1997 shm.c
-rw-------    1 root     root          645 Aug 11  1997 shm.h
-rw-------    1 root     root         8018 Aug 25  1997 surplus.c

./md5:
total 24
-rw-------    1 root     root          933 Jul 22  1997 global.h
-rw-------    1 root     root          125 Jul 22  1997 Makefile
-rw-------    1 root     root        11353 Jul 22  1997 md5c.c
-rw-------    1 root     root         1531 Jul 22  1997 md5.h
```

As evidenced by the file listing, the source code dates matched up with the time frames atd had given through binary analysis. I also discovered that many of the key words found in the **strings** output of atd were also found inside the source. My initial attempt at compilation resulted in the following errors:



```
[root@localhost Loki]# make linux
make[1]: Entering directory `/root/loki2/Loki'
gcc -Wall -O6 -finline-functions -funroll-all-loops -DLINUX -DNO_CRYPTO -DPOPEN
-DSEND_PAUSE=100 -Dx86_FAST_CHECK   -DDEBUG -DNET3 -c surplus.c -o surplus.o
In file included from loki.h:36,
                 from surplus.c:10:
/usr/include/linux/icmp.h:67: parse error before `__u8'
/usr/include/linux/icmp.h:67: warning: no semicolon at end of struct or union
/usr/include/linux/icmp.h:68: warning: data definition has no type or storage cl
ass
/usr/include/linux/icmp.h:69: parse error before `checksum'
/usr/include/linux/icmp.h:69: warning: data definition has no type or storage cl
ass
/usr/include/linux/icmp.h:72: parse error before `__u16'
/usr/include/linux/icmp.h:72: warning: no semicolon at end of struct or union
/usr/include/linux/icmp.h:72: warning: no semicolon at end of struct or union
/usr/include/linux/icmp.h:73: warning: data definition has no type or storage cl
ass
/usr/include/linux/icmp.h:74: warning: data definition has no type or storage
ass
/usr/include/linux/icmp.h:75: parse error before `gateway'
/usr/include/linux/icmp.h:75: warning: data definition has no type or storage
ass
/usr/include/linux/icmp.h:77: parse error before `__u16'
/usr/include/linux/icmp.h:77: warning: no semicolon at end of struct or union
/usr/include/linux/icmp.h:78: warning: data definition has no type or storage
ass
/usr/include/linux/icmp.h:79: warning: data definition has no type or storage
ass
/usr/include/linux/icmp.h:80: parse error before `}'
/usr/include/linux/icmp.h:80: warning: data definition has no type or storage
ass
/usr/include/linux/icmp.h:81: parse error before `}'
/usr/include/linux/icmp.h:90: parse error before `__u32'
/usr/include/linux/icmp.h:90: warning: no semicolon at end of struct or union
In file included from /usr/include/linux/signal.h:4,
                 from loki.h:38,
                 from surplus.c:10:
/usr/include/asm/signal.h:27: conflicting types for `sigset_t'
/usr/include/sys/select.h:38: previous declaration of `sigset_t'
/usr/include/asm/signal.h:129: warning: redefinition of `__sighandler_t'
/usr/include/signal.h:71: warning: `__sighandler_t' previously declared here
/usr/include/asm/signal.h:156: redefinition of `struct sigaction'
/usr/include/asm/signal.h:171: redefinition of `struct sigaltstack'
/usr/include/asm/signal.h:175: warning: redefinition of `stack_t'
/usr/include/bits/sigstack.h:55: warning: `stack_t' previously declared here
In file included from /usr/include/linux/signal.h:5,
                 from loki.h:38,
```

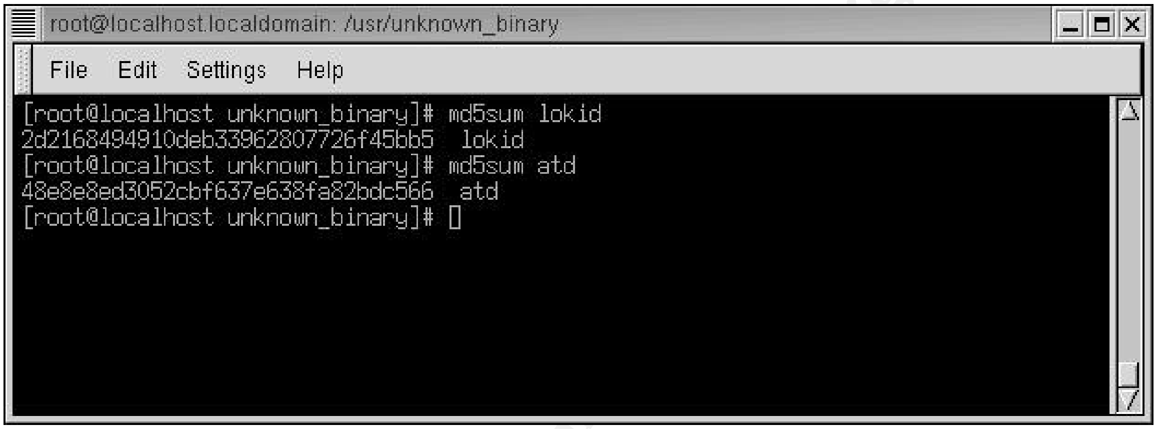
The error at the top of the screen involving icmp.h was easily worked around by playing with some of the gcc configuration settings to recognize the __u8 and __u16 variables. To resolve the error involving signal.h, I simply removed the #include <signal.h> from the loki.h header file. Despite my modification to loki.h, Loki was able to compile successfully.

The compilation produced two binaries, loki and lokid. According to the Phrack article, loki was the client and lokid was the server. I tested out the freshly compiled binaries by launching the lokid daemon to run in the background. I was shown the now familiar “LOKI2” banner. With lokid listening I launched the loki client to connect on localhost. I was able to send simple commands such as “**ls**” across the connection and see the results on client side. **Netstat** showed the connections opened on 0.0.0.0:1 and 0.0.0.0:255. The compilation appeared to be a success.

Next, I attempted to use the loki client to connect to the atd server. Atd did not seem to run properly, as loki couldn’t get a response from the server side. I decided to compare **straces** of lokid and atd to shed some light on the subject. The lokid **strace** follows:

```
execve("./lokid", ["./lokid"], [/* 40 vars */]) = 0
uname({sys="Linux", node="localhost.localdomain", ...}) = 0
brk(0)                                  = 0x804cb1c
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40017000
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=58970, ...}) = 0
old_mmap(NULL, 58970, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40018000
close(3)                                = 0
open("/lib/i686/libc.so.6", O_RDONLY)   = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\0\0\3\0\3\0\1\0\0\0\200\302"..., 1024) = 1024
fstat64(3, {st_mode=S_IFREG|0755, st_size=5634864, ...}) = 0
old_mmap(NULL, 1242920, PROT_READ|PROT_EXEC, MAP_PRIVATE, 3, 0) = 0x40027000
mprotect(0x4014d000, 38696, PROT_NONE)  = 0
old_mmap(0x4014d000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED, 3, 0x125000) =
0x4014d000
old_mmap(0x40153000, 14120, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -
1, 0) = 0x40153000
close(3)                                = 0
munmap(0x40018000, 58970)               = 0
getpid()                                = 1154
geteuid32()                             = 0
getuid32()                              = 0
socket(PF_INET, SOCK_RAW, IPPROTO_ICMP) = 3
rt_sigaction(SIGUSR1, {0x804aa5c, [USR1], SA_RESTART|0x4000000}, {SIG_DFL}, 8) = 0
socket(PF_INET, SOCK_RAW, IPPROTO_RAW)  = 4
write(2, "\nRaw IP socket: ", 16)       = 16
fcntl64(4, F_GETFL)                     = 0x2 (flags O_RDWR)
write(2, " read write", 11)             = 11
write(2, " blocking", 9)                = 9
write(2, "\r\n", 2)                     = 2
setsockopt(4, SOL_IP, IP_HDRINCL, [1], 4) = 0
getpid()                                = 1154
getpid()                                = 1154
shmget(1396, 240, IPC_CREAT|0)          = 6684686
semget(1578, 1, IPC_CREAT|0x180|0600)   = 98307
shmat(6684686, 0, 0)                    = 0x40018000
write(2, "\nLOKI2\troute [(c) 1997 guild cor"..., 52) = 52
time([1048217597])                      = 1048217597
rt_sigaction(SIGALRM, {0x804933c, [ALRM], SA_RESTART|0x4000000}, {SIG_DFL}, 8) = 0
alarm(3600)                             = 0
rt_sigaction(SIGCHLD, {0x8049b24, [CHLD], SA_RESTART|0x4000000}, {SIG_DFL}, 8) = 0
read(3, 0x804ca20, 84)                  = ? ERESTARTSYS (To be restarted)
--- SIGINT (Interrupt) ---
+++ killed by SIGINT +++
```

The lokid program possessed the key similarities to atd but also produced quite a few differences when run, the biggest difference being that the program listened towards the end of the trace rather than first forking off and then listening, as atd did. Lokid also appeared to complain about read/write blocking on the raw IP socket it attempted to open. I did a **strings** compare at this time and found a number of differences, but again also found many of the key similarities, such as the LOKI2 banner and several of the unique error messages. The **strings** differences can easily be attributed to the fact that I was using newer libraries and had to modify the code a little to get the compilation to work. There were also several options available with the included makefile to toggle encryption options, etc, which could also have affected how the binary was compiled. My code modification was most likely not the reason lokid ran differently than atd, as neither program required the specific code I removed from signal.h. As expected, the **md5sum** compare did not match up because of these reasons:



```
[root@localhost unknown_binary]# md5sum lokid
2d2168494910deb33962807726f45bb5  lokid
[root@localhost unknown_binary]# md5sum atd
48e8e8ed3052cbf637e638fa82bdc566  atd
[root@localhost unknown_binary]# 
```

Despite the number of differences between atd and lokid, I believe there were enough similarities between the two to show that they were both incarnations of the LOKI2 daemon.

Legal Implications of Loki

From the information given, I was unable to determine if the atd binary had been executed before. The only thing I knew for sure about atd's possible execution was that the last access date was on August 22, 2002. If I was performing analysis on the system where atd was found and happened to notice a good deal of questionable activity on that date, I would obviously have to acknowledge the possibility that Loki was somehow involved.

Loki is a simple program with a simple concept. Its purpose is to transfer data across networks, although the method it uses is generally viewed as unorthodox. Most of the laws that may be violated with Loki could very well be violated in the same way with more traditional communications programs such as ftp. As the Phrack article suggests, Loki has many uses for those with malicious intent:

> Loki is not a compromise tool. It has many uses, none of which are breaking into a machine. It can be used as a backdoor into a system by providing a covert method of getting commands executed on a target machine. It can be used as a way of clandestinely leeching information off

> of a machine. It can be used as a covert method of user-machine or user-user communication. In essence the channel is simply a way to secretly shuffle data (confidentiality and authenticity can be added by way of cryptography). (Daemon9, Issue 49, Article 6)

On that note, any system administrator who discovers the use of Loki on their system must assume the owner of the binary is up to something, and should go through the proper measures to protect themselves. The fact that Loki uses a covert ICMP channel is a dead giveaway that the user is smart enough to intentionally go out of his way to hide whatever is being transferred. It should also be noted that **atd** is the name of an actual Unix command. Its real purpose is to run jobs that have been queued up with the **at** command. It is very likely that whoever created this binary was planning on hiding the Loki daemon by disguising it as **atd**.

A situation could occur where a hacker could compromise a system with another set of hacker tools and then set up a Loki channel to discreetly relay information from the compromised system back to the hacker. For example, the hacker could use Loki to send back financial information, credit card numbers, credit reports, classified government information, etc. In such a situation, the hacker would be in violation under the Computer Fraud & Abuse Act, 18 U.S.C. 1030(a)(2). Note that the law applies even if the hacker did not damage the system or corrupt any of the involved information. If he is found guilty, possible penalties include a fine and a maximum sentence of one year in prison for first time offenders (U.S.C. 1030(c)(2)(A)). For more serious offenders or for those seeking to acquire personal financial gain or commercial advantage, the penalty is more severe. Those involved can expect to face a fine and up to five years in prison (U.S.C. 1030(c)(2)(B)). Finally, repeat offenders can be charged with a fine and up to ten years in prison (U.S.C. 1030(c)(2)(C)).

Loki could also be used to transmit unauthorized commands, information, or even more potentially dangerous hacker tools with the intention of damaging a protected system. Such an act would be in violation of U.S.C 1030(a)(5)(A)(i). Depending on the type and amount of damage done to the system, a first time offender could face a fine and 10 years in prison (U.S.C. 1030(c)(4)(A). Repeat offenders would be facing a fine and a maximum of 20 years (U.S.C. 1030(c)(4)(C)).

Another potential situation that could come up would be when a hacker's goal is to pipeline restricted government information to unauthorized or foreign organizations with the intent of harming the United States. After a successful compromise of a government system, the hacker could send any amount of classified information under complete secrecy from national defenses. In this case the hacker would be found in violation of U.S.C. 1030(a)(1). The maximum penalties he could face are more serious in this matter, with a fine and 10 years in prison for first time offenders (U.S.C. 1030(c)(1)(A)) and a fine and 20 years in prison for repeat offenders (U.S.C. 1030(c)(1)(B)).

Lastly, if the hacker were to use Loki to relay passwords or other information to gain access to U.S. government systems or to potentially have an affect on interstate or foreign commerce, the guilty parties would be in violation of U.S.C. 1030(a)(6) (A & B). The penalties involved would be similar to U.S.C. 1030(a)(1).

Possible Interview Questions

Let us assume a situation where I was working as a system administrator and discovered Loki running on my system. After performing some of the analysis above, and discovering the owner of the user account that was logged as launching the required executables, it is time to interview the suspect. The objective here is to find out if the owner is the one responsible, and to make him confess up to it. I would generally ask the following questions during my interrogation:

1. Has anyone had access to your account in the past few weeks? Have you ever given your password to anyone?

This question is often the most important and could probably save a lot of time and effort. Quite often, the user is merely a victim of someone who managed to hack into his account.

2. Were you working late at your terminal last Tuesday night? Were you logged into your account?

3. Have you been having/noticing any problems with the system lately? You seem to have the reputation around the office as being a technology whiz. I thought you might be able to provide some insight to some problems we've been having.

4. My system monitors have alerted me to quite a bit of activity under your username involving a tool called Loki. Did you put this tool on the system? Do you know what it's used for?

5. I'm sure you are aware that our internal policy forbids tools of this nature to be installed on our systems. Do you have an interest in network security? I realize you may have just been experimenting as a hobby, and as a system admin, it is part of my job to check these things out. However, this situation could potentially get worse for the both of us if it is not resolved soon. We definitely don't want to get law enforcement involved. Could you please stop running these tools and remove them from the system?

If all goes well, this last question will have eased the suspect's anxiety and invite him to confess. The suspect will hopefully realize this is probably his best option at this point. More often than not however, it will take a second or third interview to get him to reveal the complete story.

References

Daemon9. "Project Loki." Phrack Magazine, Volume 7, Issue 49, Article 6 (August 1996).
URL: http://www.phrack.org/phrack/49/P49-06. (15 March 2003).

Daemon9. "LOKI2 (the implementation)". Phrack Magazine, Volume 7, Issue 51, Article 6 (September 1997).
URL: http://www.phrack.org/phrack/51/P51-06. (15 March 2003).

Department of Justice. "18 U.S.C. 1030. Fraud and Related Activity in Connection with Computers".
URL: http://www.usdoj.gov/criminal/cybercrime/1030_new.html. (15, March 2003)

Internet Security Systems. "ISS X-Force Database: loki (1452): LOKI ICMP tunneling back door". September 1997.
URL: http://www.iss.net/security_center/static/1452.php. (15 March 2003)

Lee, Rob. "Forensics Faq". 1 July 2000.
URL: http://www.deaddrop.org/security/Presentations/2ndqtr/ForensicsFaq.html. (15 March 2003)

Low, C. "ICMP Attacks Illustrated". December 2001.
URL: http://www.sans.org/rr/threats/ICMP_attacks.php. (15 March 2003)

Scambray, J., McClure, S., and Kurtz, G. Hacking Exposed: Network Security Secrets and Solutions Second Edition. New York: Osborne/McGraw Hill, 2001. p. 476, 541.

Part II: Perform Forensic Analysis on a System

Synopsis of Case Facts

The company I work for has an Information Assurance department with a number of security professionals on board. I do not currently work in Information Assurance, although our teams have collaborated with each other in the past, and our work is closely related. I thought it would be a good idea to contact some of the people over there to see if they had a system I could analyze for the GCFA practical. After a few exchanges of emails I learned that part of their job was to routinely set up test systems and study security threats on them. I thought that if I could get a hold of one of their test systems, it would make an excellent specimen to use for my exam. I asked if there were any systems they had lying around that they wouldn't mind my imaging and performing my own forensic analysis on. My contact replied that someone on his team had given a security demonstration the week before on a Windows 2000 system and happily agreed to my request. I set up a meeting time, and on March 18, 2003, I took a visit to their office to collect evidence.

The system had been shut down before I got there. I first took an image of the system's hard drive and noted the hardware setup of the machine. I wanted to collect a few more pieces of evidence and asked if there was any reason why I shouldn't boot up the drive. After verifying from my contact that there was no apparent threat, I started up the machine, ran IRCR (Incident Response Collection Report), collected some registry information using Registrar Lite, performed a quick check for sniffers, and archived some of the log information using the Windows Event Viewer. IRCR is a useful and free tool that collects a wide variety of information off Windows NT/2000 systems so that forensic analysts can study the data later. Registrar Lite is also a free tool that is similar to the Windows regedit program, and allows you to export the registry data to a text format. In order to get copies of all generated reports I mapped the output drive to another local machine on the network, and then copied the contents to my laptop. Unfortunately, they would not let me take possession of any hardware, but I was assured they did not need the machine again for a while and could keep the system secure for me.

System Background

The system was set up in the IAC lab in Falls Church, VA. When I first encountered the system, it had already been shut down. I asked my contact some basic questions about what was on it. I learned that the last known activity on the system took place the week before, but anyone could have booted up the system since then. He said he had no reason to believe it wasn't shut down normally (i.e. Start-> Shutdown). The operating system installed was Windows 2000 Professional. There was no dual boot partition configuration set up to his knowledge. The system was configured for company-wide network and Internet access via Ethernet 10/100 using a NAT IP address of 192.168.5.76.

I asked my contact to briefly describe what the system had been used for in the past. The system had been around for a while, probably for over a year. IAC had been using it as an all-purpose machine, mainly for generating test data and studying exploits as well. The machine had multiple users and they normally logged in under the username "A User". He had no knowledge of any other user names on the system. Other than that he wasn't too sure what software was on it.

Description of Hardware

I was not authorized to seize any hardware. I took notes on all hardware details below.

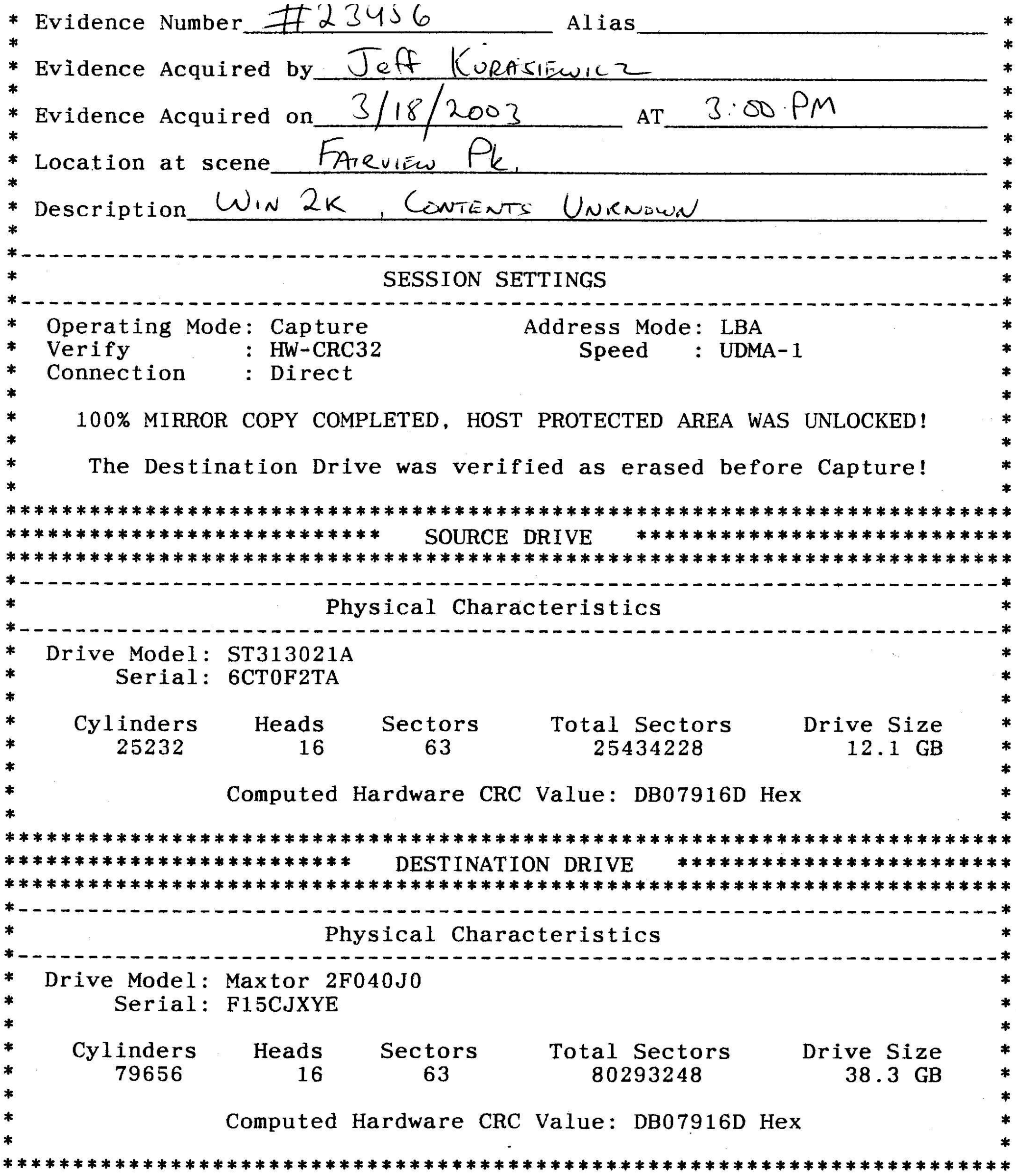
Tag No.	Description
12345	Dell Optiplex GX110 system w/ Pentium III CPU. Serial #6GF8G01. Model# MMP. Two removable drive slots.
23456	Seagate U8 Hard Disk. Serial # 6CT0F2TA. Model # ST313021A. Size: 13.0 Gigabytes.
34567	Generic CD-RW Read/Writer
45678	3Com EtherLink XL 10/100 PCI TX NIC
56789	Generic 3.5" Floppy Drive

Imaging the Media

I thought the easiest way to obtain an image of the system would be to use a disk duplicator. Logicube makes a variety of these duplicator kits, and designs them with the forensic examiner's needs in mind. Along with the actual duplication device, the 5000u model I used also comes with a portable printer, a power distribution panel, a screwdriver and other PC-related tools, a 2.5" drive adaptor (for laptop drives), and a PCMCIA Clonecard (for duplicating difficult-to-reach laptop drives). For image copy verification, the 5000u can perform both software and hardware based CRC-32 calculations. It is a very convenient tool when dealing with forensic investigations, particularly when traveling to other locations and working with unfamiliar systems as I did. The only complaint I have about it is that I have found it can be finicky with some of the newer drives. Logicube comes out with new software for supporting the newer drive models every so often, but some drives will require a bit of experimenting with the jumper settings or toggling the copy speed.

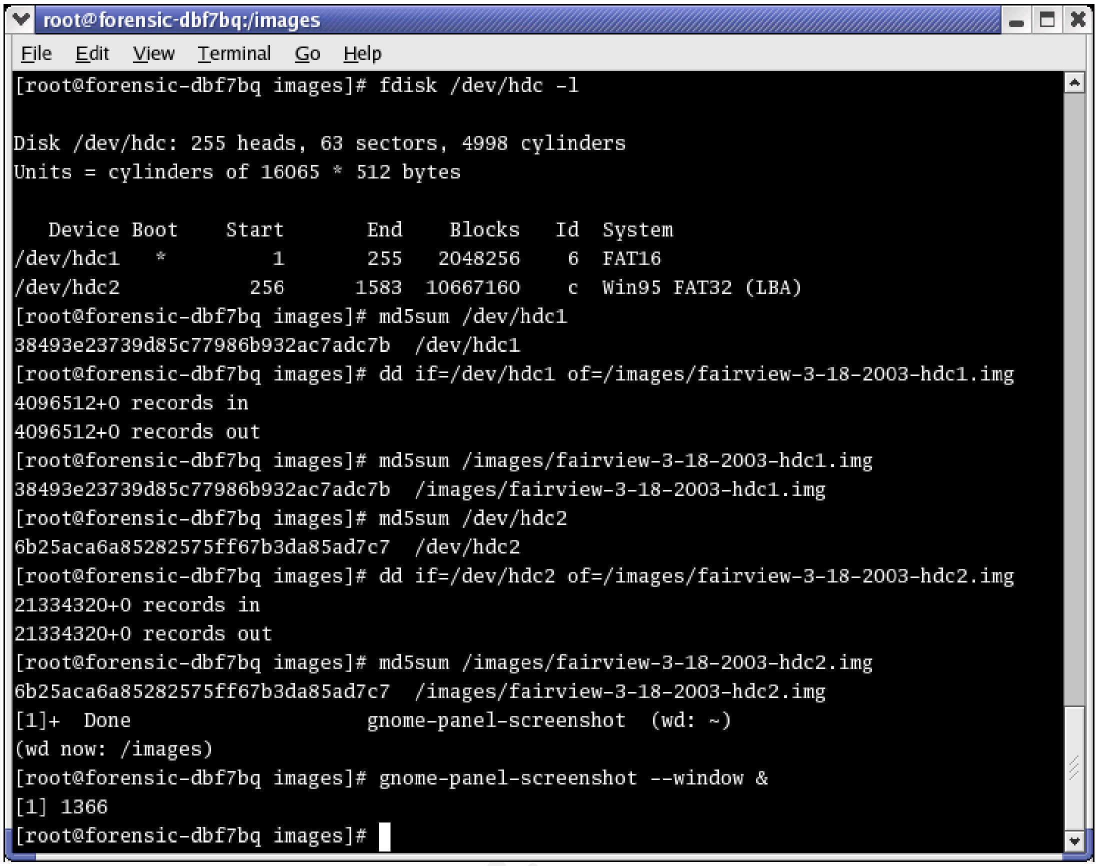
There was no need to start up the suspect system. I opened up the case and removed the hard drive. I brought a 38.3 gigabyte Maxtor 2F040J0 to use as the destination drive. Even though I obtained this disk fresh out of the box, as an added precaution (and always good practice), I had previously sterilized this disk with a fresh coating of zero-bits. In fact, the 5000u will not let you duplicate a disk without first sterilizing it. It has a special WipeClean function that locates zero-filled sectors on the source drive and quickly copies them to the destination. A source drive does not need to be present but it is much faster using the source drive method, according to the manual. The 5000u also writes a digital signature at the end of every sector, consisting of 0xAAAA, 0x5555, and the character string “Logicube”. This is so it can quickly verify that the drive is sterile. So technically, the drive is not completely blanketed in 0 bits, but I can account for the last 12 bytes of each sector.

Imaging went smoothly, at a speed of UDMA-1, or about a gigabyte per minute. I used a Hardware CRC check to verify the copy. The resulting report was generated, providing proof that the drive was erased and the CRC checks matched:



```
* Evidence Number #23456          Alias                              *
*                                                                   *
* Evidence Acquired by Jeff Kurasiewicz                             *
*                                                                   *
* Evidence Acquired on 3/18/2003        AT 3:00 PM                  *
*                                                                   *
* Location at scene Fairview Pk.                                    *
*                                                                   *
* Description Win 2K, Contents Unknown                              *
*                                                                   *
*-------------------------------------------------------------------*
*                          SESSION SETTINGS                         *
*-------------------------------------------------------------------*
*  Operating Mode: Capture          Address Mode: LBA               *
*  Verify        : HW-CRC32             Speed   : UDMA-1            *
*  Connection    : Direct                                           *
*                                                                   *
*    100% MIRROR COPY COMPLETED, HOST PROTECTED AREA WAS UNLOCKED!  *
*                                                                   *
*     The Destination Drive was verified as erased before Capture!  *
*                                                                   *
*********************************************************************
**************************   SOURCE DRIVE   *************************
*********************************************************************
*-------------------------------------------------------------------*
*                      Physical Characteristics                     *
*-------------------------------------------------------------------*
*  Drive Model: ST313021A                                           *
*       Serial: 6CT0F2TA                                            *
*                                                                   *
*    Cylinders    Heads    Sectors     Total Sectors     Drive Size *
*       25232       16       63          25434228          12.1 GB  *
*                                                                   *
*               Computed Hardware CRC Value: DB07916D Hex           *
*                                                                   *
*********************************************************************
************************   DESTINATION DRIVE   **********************
*********************************************************************
*-------------------------------------------------------------------*
*                      Physical Characteristics                     *
*-------------------------------------------------------------------*
*  Drive Model: Maxtor 2F040J0                                      *
*       Serial: F15CJXYE                                            *
*                                                                   *
*    Cylinders    Heads    Sectors     Total Sectors     Drive Size *
*       79656       16       63          80293248          38.3 GB  *
*                                                                   *
*               Computed Hardware CRC Value: DB07916D Hex           *
*                                                                   *
*********************************************************************
```

Later on in my investigation, I wanted to copy an image of the drive onto a Linux forensics workstation I had set up earlier using a Dell machine. This was not the same machine I used for analysis of the binary in Part I of this practical, but my setup was very similar. It had a dual boot for Windows 2000 and Linux 8.0 partitions, and also a removable drive slot (a CRU Dataport IV Storage Cabinet) to ease copying images onto and off the machine. I also loaded many of the same forensic tools from the SANS Disk. The Linux partition had a lot of space on it, so to make things easier I created additional images directly on the drive using dd. As the **fdisk** command shows below, there turned out to be two partitions on the suspect drive. I discovered there was a 2 gigabyte FAT16 boot partition for the Windows 2000 OS, and an additional FAT32 partition that took up the remaining 11 gigs. I will go into this with much more detail in the next section. The **md5sum** hashes below are proof that the Linux images are valid.



```
[root@forensic-dbf7bq images]# fdisk /dev/hdc -l

Disk /dev/hdc: 255 heads, 63 sectors, 4998 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/hdc1   *         1       255   2048256    6  FAT16
/dev/hdc2           256      1583  10667160    c  Win95 FAT32 (LBA)
[root@forensic-dbf7bq images]# md5sum /dev/hdc1
38493e23739d85c77986b932ac7adc7b  /dev/hdc1
[root@forensic-dbf7bq images]# dd if=/dev/hdc1 of=/images/fairview-3-18-2003-hdc1.img
4096512+0 records in
4096512+0 records out
[root@forensic-dbf7bq images]# md5sum /images/fairview-3-18-2003-hdc1.img
38493e23739d85c77986b932ac7adc7b  /images/fairview-3-18-2003-hdc1.img
[root@forensic-dbf7bq images]# md5sum /dev/hdc2
6b25aca6a85282575ff67b3da85ad7c7  /dev/hdc2
[root@forensic-dbf7bq images]# dd if=/dev/hdc2 of=/images/fairview-3-18-2003-hdc2.img
21334320+0 records in
21334320+0 records out
[root@forensic-dbf7bq images]# md5sum /images/fairview-3-18-2003-hdc2.img
6b25aca6a85282575ff67b3da85ad7c7  /images/fairview-3-18-2003-hdc2.img
[1]+  Done                    gnome-panel-screenshot  (wd: ~)
(wd now: /images)
[root@forensic-dbf7bq images]# gnome-panel-screenshot --window &
[1] 1366
[root@forensic-dbf7bq images]# 
```

Mounting the images for analysis was done using the following command to ensure the images were not modified from the original evidence in any way:

```
mount -o ro,loop,nosuid,noexec,nodev,noatime /images/Fairview-3-18-2003-hdc1.img
/mnt/hdc1
```

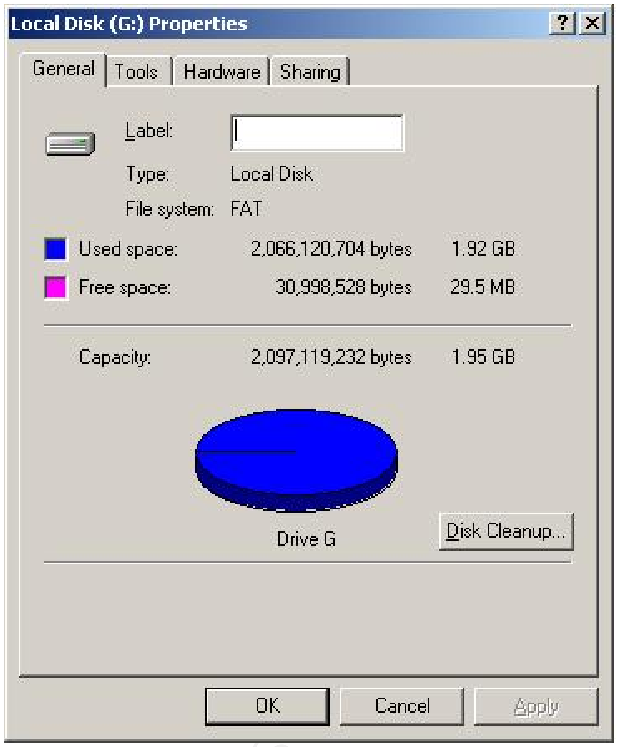
The options after –o make the image:
ro: read-only
loop: mounted on a loop device
nodev: no interpretation of special devices
noexec: no executions of any files allowed
noatime: access times are not changed

Media Analysis of the System

For the media analysis of the system I found it useful to use both my Windows and Linux partitions. Each OS has its own strengths and weaknesses when it comes to forensic work. When examining a Windows based system, the natural choice would be to use a Windows forensic machine, but Linux has some powerful (and free) tools that make it worth checking out as well.

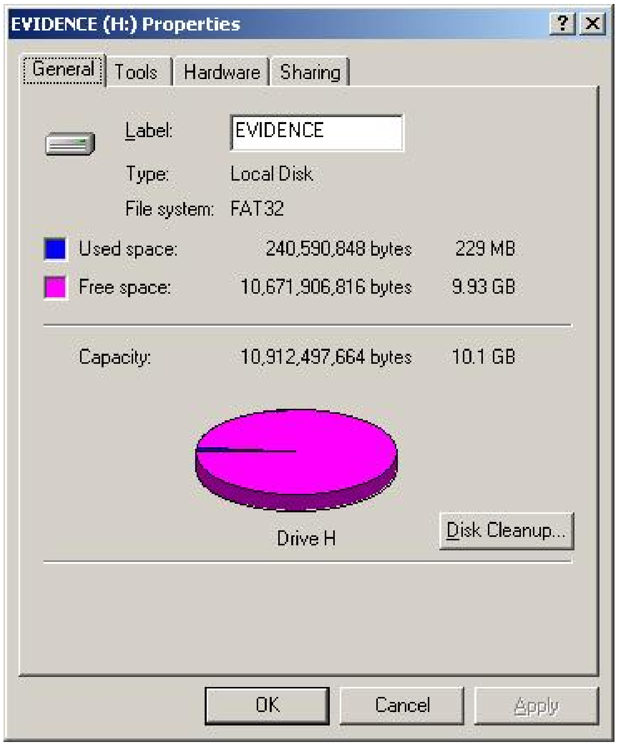
I began my investigation using the Windows partition. Mounting the drive was simple with the setup I had, by simply using the removable drive and making my image the secondary drive. I used a Windows-based tool that some of my colleagues have worked on called WriteBlocker to ensure that my image was not written to. It is very easy to use and can be set to automatically block local drives from write access by default. WriteBlocker is not available to the public at this time as it is still under beta testing, but I will prove through the course of the investigation that the evidence was never altered.

As mentioned during the imaging, there turned out to be two partitions on the suspect drive. I had mounted these as G: and H:. A quick look at the drive properties gave some basic information:



Label:
Type: Local Disk
File system: FAT

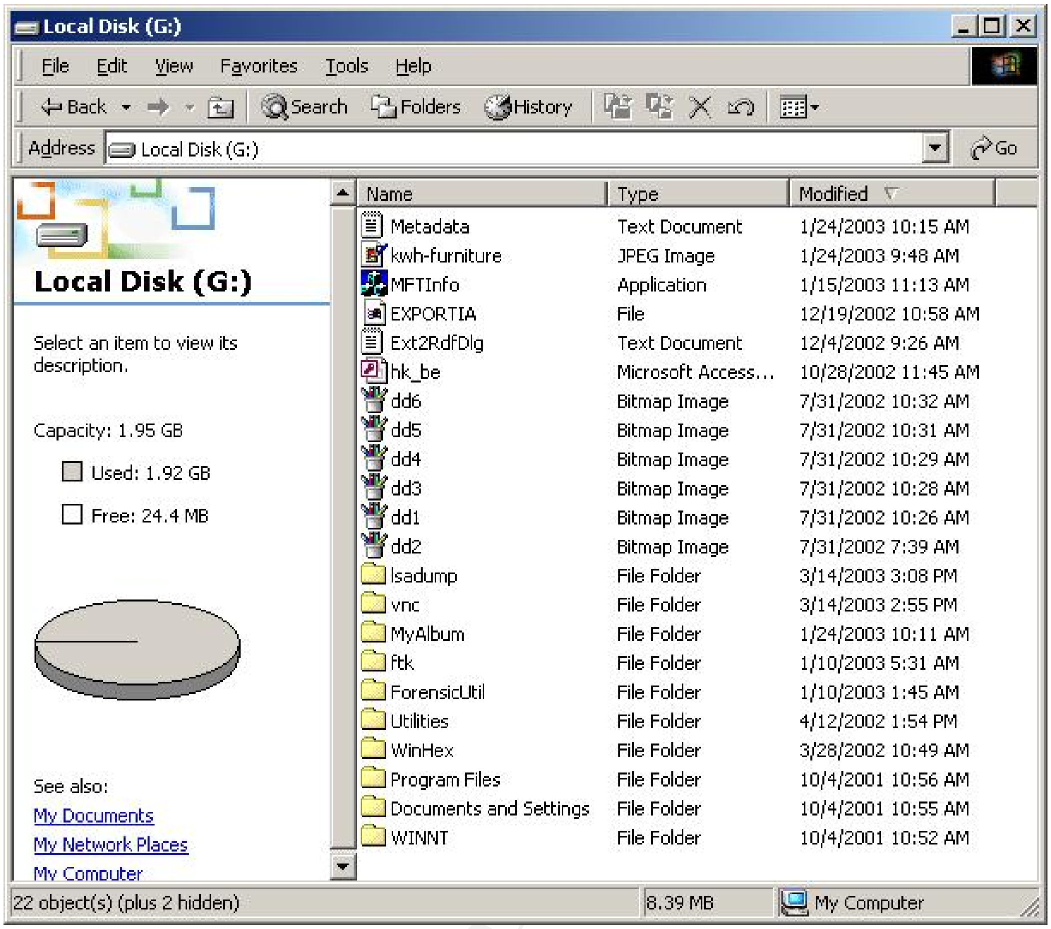
🟦 Used space:	2,066,120,704 bytes	1.92 GB
🟪 Free space:	30,998,528 bytes	29.5 MB
Capacity:	2,097,119,232 bytes	1.95 GB



Label: EVIDENCE
Type: Local Disk
File system: FAT32
Used space: 240,590,848 bytes 229 MB
Free space: 10,671,906,816 bytes 9.93 GB
Capacity: 10,912,497,664 bytes 10.1 GB

The Windows 2000 boot partition was a FAT16 drive and had a size of 2 gigabytes. The Volume label was blank. The drive was taken to nearly full capacity, with a mere 30 megabytes free. I took this as a good indication that the partition had been used quite a bit and hadn't been cleaned out in a while. The other partition was a completely different story, however. With 11 gigabytes allocated to the FAT32 partition labeled EVIDENCE, only 229 megabytes were being used. Out of curiosity, I opened up the H: drive in Winhex and found a good deal of old information sitting in the slack space. Some of it was Unix related, leading me to believe this drive may have housed a Unix-based operating system in its past. Winhex is a tool of many uses, but its main use is to read and write data at the machine, (or binary) level. Here I just wanted to get a quick look at the drive as a whole, to see if I was dealing with a fresh drive (mostly zeros), or a well-used drive. I took note of this and would definitely be sure to examine the slack space on H: further down the road.

To get a basic idea of the contents of both partitions, I used Explorer to look around for a bit. I have included screenshots of the root directories and the Program Files directory from drive G:



Local Disk (G:)

Select an item to view its description.

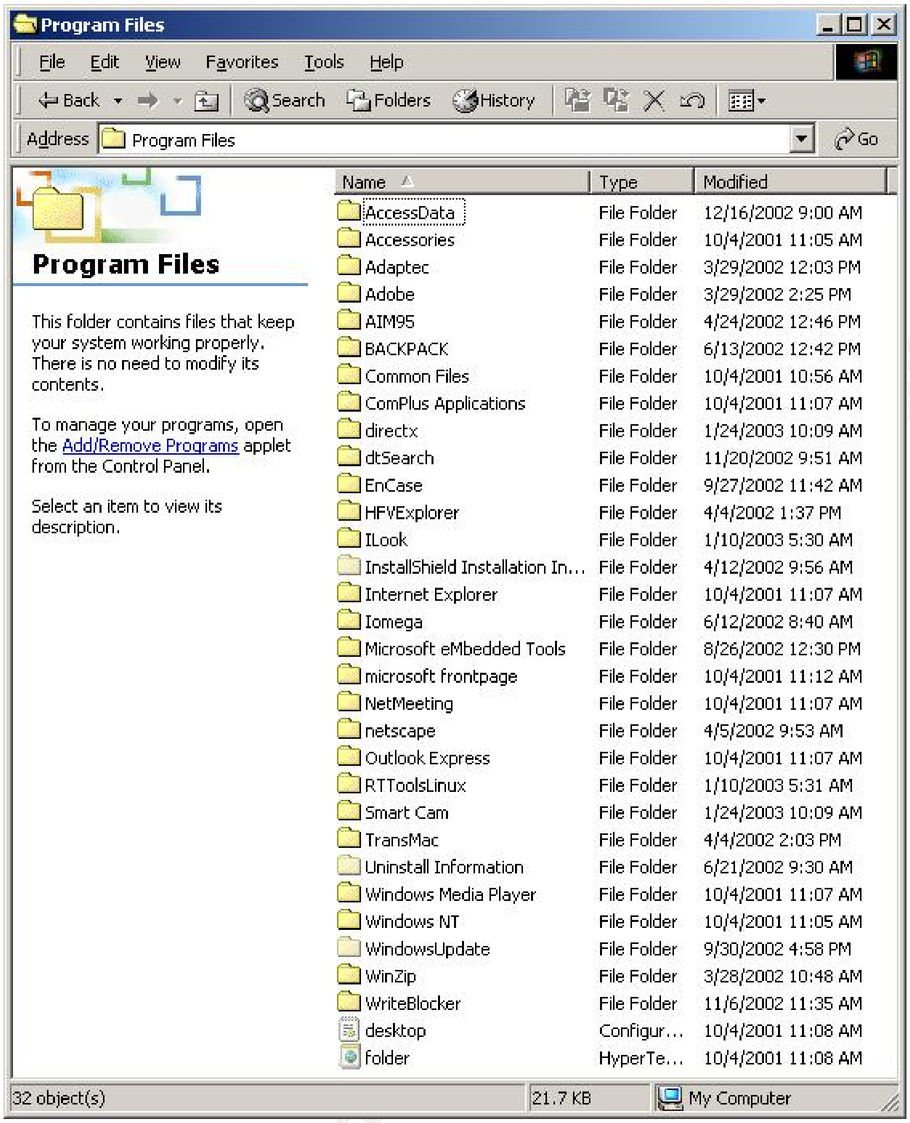
Capacity: 1.95 GB

☐ Used: 1.92 GB

☐ Free: 24.4 MB

Name	Type	Modified
Metadata	Text Document	1/24/2003 10:15 AM
kwh-furniture	JPEG Image	1/24/2003 9:48 AM
MFTInfo	Application	1/15/2003 11:13 AM
EXPORTIA	File	12/19/2002 10:58 AM
Ext2RdfDlg	Text Document	12/4/2002 9:26 AM
hk_be	Microsoft Access...	10/28/2002 11:45 AM
dd6	Bitmap Image	7/31/2002 10:32 AM
dd5	Bitmap Image	7/31/2002 10:31 AM
dd4	Bitmap Image	7/31/2002 10:29 AM
dd3	Bitmap Image	7/31/2002 10:28 AM
dd1	Bitmap Image	7/31/2002 10:26 AM
dd2	Bitmap Image	7/31/2002 7:39 AM
lsadump	File Folder	3/14/2003 3:08 PM
vnc	File Folder	3/14/2003 2:55 PM
MyAlbum	File Folder	1/24/2003 10:11 AM
ftk	File Folder	1/10/2003 5:31 AM
ForensicUtil	File Folder	1/10/2003 1:45 AM
Utilities	File Folder	4/12/2002 1:54 PM
WinHex	File Folder	3/28/2002 10:49 AM
Program Files	File Folder	10/4/2001 10:56 AM
Documents and Settings	File Folder	10/4/2001 10:55 AM
WINNT	File Folder	10/4/2001 10:52 AM

22 object(s) (plus 2 hidden) | 8.39 MB | My Computer


Program Files
File Edit View Favorites Tools Help
Back Search Folders History
Address Program Files
Go

Program Files

This folder contains files that keep your system working properly. There is no need to modify its contents.

To manage your programs, open the Add/Remove Programs applet from the Control Panel.

Select an item to view its description.

Name	Type	Modified
AccessData	File Folder	12/16/2002 9:00 AM
Accessories	File Folder	10/4/2001 11:05 AM
Adaptec	File Folder	3/29/2002 12:03 PM
Adobe	File Folder	3/29/2002 2:25 PM
AIM95	File Folder	4/24/2002 12:46 PM
BACKPACK	File Folder	6/13/2002 12:42 PM
Common Files	File Folder	10/4/2001 10:56 AM
ComPlus Applications	File Folder	10/4/2001 11:07 AM
directx	File Folder	1/24/2003 10:09 AM
dtSearch	File Folder	11/20/2002 9:51 AM
EnCase	File Folder	9/27/2002 11:42 AM
HFVExplorer	File Folder	4/4/2002 1:37 PM
ILook	File Folder	1/10/2003 5:30 AM
InstallShield Installation In...	File Folder	4/12/2002 9:56 AM
Internet Explorer	File Folder	10/4/2001 11:07 AM
Iomega	File Folder	6/12/2002 8:40 AM
Microsoft eMbedded Tools	File Folder	8/26/2002 12:30 PM
microsoft frontpage	File Folder	10/4/2001 11:12 AM
NetMeeting	File Folder	10/4/2001 11:07 AM
netscape	File Folder	4/5/2002 9:53 AM
Outlook Express	File Folder	10/4/2001 11:07 AM
RTToolsLinux	File Folder	1/10/2003 5:31 AM
Smart Cam	File Folder	1/24/2003 10:09 AM
TransMac	File Folder	4/4/2002 2:03 PM
Uninstall Information	File Folder	6/21/2002 9:30 AM
Windows Media Player	File Folder	10/4/2001 11:07 AM
Windows NT	File Folder	10/4/2001 11:05 AM
WindowsUpdate	File Folder	9/30/2002 4:58 PM
WinZip	File Folder	3/28/2002 10:48 AM
WriteBlocker	File Folder	11/6/2002 11:35 AM
desktop	Configur...	10/4/2001 11:08 AM
folder	HyperTe...	10/4/2001 11:08 AM

32 object(s) | 21.7 KB | My Computer

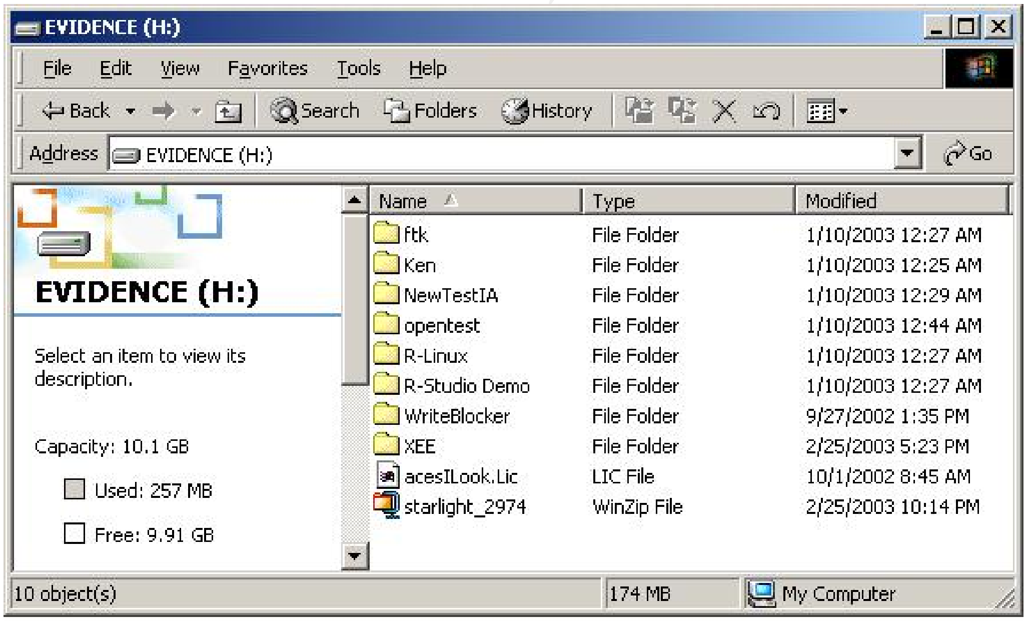
From the command prompt, I verified through **dir /TC** that all modified times shown above matched their creation times. At this point it was likely that the above software components were installed on their respective Modified dates shown in Explorer. It appeared that the system had been installed on 10/4/2001, judging by the typically generated Windows directories “WINNT”, “Documents and Settings”, “Common Files”, “Windows NT”, “Accessories”, etc. From studying the contents of Program Files, where Windows programs are usually installed by default, it appeared there were already several forensic tools installed on the system. Considering the background of the group I obtained the system from, I didn’t think this was at all out of the ordinary, just a little ironic. Looking inside some of the directories, I recognized the popular tools FTK (Forensic Toolkit), Encase, and Ilook had been installed. There was also an older copy of WriteBlocker that had made its way over to IAC at some point. There were several other common software applications that I verified had been installed over the history of the machine:

WinHex
Microsoft Internet Explorer
Microsoft Outlook Express
Microsoft Frontpage
WinZip
Adaptec DirectCD CD-R writing software
Adobe Acrobat
Netscape
AOL Instant Messenger

I will attempt to verify the software versions and upgrade histories of these applications later in this analysis.

Of particular interest were the two directories G:\vnc and G:\lsadump, which had been created/modified recently, on 3/14/2003. The vnc directory appeared to contain a copy of Virtual Network Computing. The lsadump directory appeared to contain a copy of Lsadump2. Both of these tools were created for the purposes of helping Windows NT system administrators, but they have also been considered useful to hackers. They will be covered in greater detail later.

The H: drive was not as interesting, and looked as if it had been used as a “dumping ground” of sorts for the storage of miscellaneous files:



EVIDENCE (H:)

Select an item to view its description.

Capacity: 10.1 GB

☐ Used: 257 MB

☐ Free: 9.91 GB

Name	Type	Modified
ftk	File Folder	1/10/2003 12:27 AM
Ken	File Folder	1/10/2003 12:25 AM
NewTestIA	File Folder	1/10/2003 12:29 AM
opentest	File Folder	1/10/2003 12:44 AM
R-Linux	File Folder	1/10/2003 12:27 AM
R-Studio Demo	File Folder	1/10/2003 12:27 AM
WriteBlocker	File Folder	9/27/2002 1:35 PM
XEE	File Folder	2/25/2003 5:23 PM
acesILook.Lic	LIC File	10/1/2002 8:45 AM
starlight_2974	WinZip File	2/25/2003 10:14 PM

10 object(s) | 174 MB | My Computer

On this drive I was able to find a copy of R-Linux, which is a file recovery utility for Ext2 file systems, and another copy of WriteBlocker. The contents of the other directories shown above did not contain anything particularly noteworthy, but they would be included in string searches, etc. later on.

I decided to take a look at the reports IRCR generated next. For all reports I used IRCR version 1.1. The following system information was verified at this time:

```
Login Name: A User
Computer Name: SECTOR
Domain Name: ACESLAB
File System: FAT
IP Address. . . . . . . . . . . . : 192.168.5.76
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.5.1
DNS Servers . . . . . . . . . . . : 192.168.3.2, 192.168.3.3
```

A look at the md5chk.txt report showed the following files had not been altered:

```
Computer Name: SECTOR
 Domain Name: ACESLAB
 Time/Date: 16:09:57 Tue Mar 18  2003 Eastern Standard Time

-------------------------------------------------------------------------------

 MD5 check on some important files

-------------------------------------------------------------------------------

Verifying data...
c:\winnt\system32\fpnwclnt.dll verified.
C:\WINNT\system32\net.exe verified.
C:\WINNT\system32\arp.exe verified.
C:\WINNT\system32\ipconfig.exe verified.
C:\WINNT\system32\wscript.exe verified.
C:\WINNT\system32\wmi.dll verified.
C:\WINNT\system32\wmicore.dll verified.
C:\WINNT\system32\cmd.exe verified.
```

This report basically performs an md5sum check on some of the more critical Windows system files, providing a good way to verify your OS software has not been tampered with by a malevolent entity.

While at the IAC lab, I used a program called **sniffer** to search the system for any signs of a sniffer, or sniffer drivers. No sniffers were detected:

```
Sniffer Detector, by H. Carvey <keydet89@yahoo.com)

Packet sniffer not detected.
```

Registry Analysis

The Windows system registry offers a great deal of information for the forensic examiner, if he knows where to look. General system information, software and OS version numbers, specific user information, user accounts, user logons, network information, recently searched/used/saved files, commands executed, and internet history information are all commonly found in the registry. I was able to extract the following information from the exported .reg files generated by Registrar Lite.

```
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ComputerName]
"ComputerName"="SECTOR"
```

The computer's identity "ComputerName" was shown as SECTOR.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion]
"CurrentBuild"="1.511.1 () (Obsolete data - do not use)"
"InstallDate"=dword:3bbc41ef
"ProductName"="Microsoft Windows 2000"
"RegDone"=""
"RegisteredOrganization"=""
"RegisteredOwner"="A User"
"SoftwareType"="SYSTEM"
"CurrentVersion"="5.0"
"CurrentBuildNumber"="2195"
"CurrentType"="Uniprocessor Free"
"CSDVersion"="Service Pack 3"
"SystemRoot"="C:\\WINNT"
"SourcePath"="F:\\I386"
"PathName"="C:\\WINNT"
"ProductId"="51873-OEM-0003317-35176"
```

The OS was confirmed here as Microsoft Windows 2000, Version 5.0, Build 2195. Microsoft Service Pack 3 had been installed. The registered owner of the system was "A User".

```
[HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System]
"SystemBiosDate"="09/18/00"
"SystemBiosVersion"=hex(7):50,68,6f,65,6e,69,78,20,52,4f,4d,20,42,49,4f,53,20,\
  50,4c,55,53,20,56,65,72,73,69,6f,6e,20,31,2e,31,30,20,41,30,35,00,00
```

System Bios information.

```
[HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0]
"Component Information"=hex:00,00,00,00,00,00,00,00,00,00,00,00,01,00,00,00
"Identifier"="x86 Family 6 Model 8 Stepping 6"
"Configuration Data"=hex(9):ff,ff,ff,ff,ff,ff,ff,ff,00,00,00,00,00,00,00,00
"VendorIdentifier"="GenuineIntel"
"FeatureSet"=dword:00002fff
"~MHz"=dword:000003a2
```

CPU information. The CPU speed is shown in hex here. Converted to decimal, the machine's speed was 933 MHz.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\HP
LaserJet 4000 Series PCL]
"ChangeID"=dword:0307e227
"Status"=dword:00000180
"Name"="HP LaserJet 4000 Series PCL"
"Share Name"=""
"Print Processor"="WinPrint"
"Datatype"="RAW"
"Parameters"=""
"ObjectGUID"=""
"DsKeyUpdate"=dword:00000000
"Description"=""
"Printer Driver"="HP LaserJet 4000 Series PCL"
```

It appeared that this system had been using an HP LaserJet 4000 Series PCL printer, or at least had the driver for it installed at some point.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Providers\LanMan
Print Services\Servers\EDWIN-LE2\Printers\HP LaserJet 4000 N]
"ChangeID"=dword:0307e297
"Status"=dword:00000080
"Name"="HP LaserJet 4000 N"
"Share Name"="printer"
"Print Processor"="WinPrint"
"Datatype"="RAW"
"Parameters"=""
"ObjectGUID"=""
"DsKeyUpdate"=dword:00000003
"Description"=""
"Printer Driver"="HP LaserJet 4000 Series PS"
```

Location of the HP LaserJet printer on the network.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"DefaultDomainName"="W2K"
"DefaultUserName"="A User"
"AltDefaultUserName"="A User"
"AltDefaultDomainName"="SECTOR"
```

System defaults. There were no surprises here, as the user “A User” was the default user name. However, the system was using an alternate domain name “SECTOR”, instead of “W2K”.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-
1547161642-842925246-1060284298-1000]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q282522]
"InstalledDate"="9/30/2002"
"InstalledBy"="A User"
"UninstallCommand"="C:\\WINNT\\$NtServicePackUninstall$\\spuninst\\spuninst.exe"
"Description"="Windows 2000 Service Pack 3"
"Type"="Service Pack"
```

Windows 2000 Service Pack 3 was installed by the default user “A User” on Sept. 30, 2002.

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{C4EE31F3-4768-
11D2-BE5C-00A0C9A83DA1}\FilesNamedMRU]
"000"="Files*.exe"
"001"="*raptor*.jpg"
"002"="*gold*.jpg"
"003"="*paradise*.jpg"
"004"="*.zip"
"005"="winzip"
"006"="winzip.exe"
"007"="license.txt"
"008"="*.cas"
"009"="winnt.hlp"

[HKEY_USERS\S-1-5-21-1547161642-842925246-1060284298-1000\Software\Microsoft\Internet
Explorer\Explorer Bars\{C4EE31F3-4768-11D2-BE5C-00A0C9A83DA1}\FilesNamedMRU]
"000"="Files*.exe"
"001"="*raptor*.jpg"
"002"="*gold*.jpg"
"003"="*paradise*.jpg"
"004"="*.zip"
"005"="winzip"
"006"="winzip.exe"
"007"="license.txt"
"008"="*.cas"
"009"="winnt.hlp"
```

These registry keys show the recent file search history of the user.

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs]
"url1"="ftp://ftp.pnl.gov/"
"url2"="http://www.buy.com/"
"url3"="http://mail.yahoo.com/"
"url4"="http://www.google.com/"
"url5"="http://www.exif.org/"
"url6"="http://www.accessdata.com/"
"url7"="http://www.dell.com"
"url8"="mal.yahoo.com"
"url9"="My Network Places"
"url10"="http://web.mit.edu/maryr/www/amusements/"
"url11"="http://www.washingtonpost.com/"
"url12"="ftp://ftp.webtrek.com/"
"url13"="http://www.redhat.com/"
"url14"="http://www.download.com/"
"url15"="http://www.redhat.com/download/mirror.html"
"url16"="http://www.microsoft.com/"
"url17"="http://www.encase.com/"
"url18"="http://www.npr.org/"
"url19"="www.encaase.com"
"url20"="http://www.pocketpccity.com/"
"url21"="/Mobile Device"
"url22"="http://das.microsoft.com/activate"
"url23"="http://www.meguiars.com/"
"url24"="http://www.dell.com/"
"url25"="http://www.3com.com/"

[HKEY_USERS\S-1-5-21-1547161642-842925246-1060284298-1000\Software\Microsoft\Internet
Explorer\TypedURLs]
"url1"="ftp://ftp.pnl.gov/"
"url2"="http://www.buy.com/"
"url3"="http://mail.yahoo.com/"
"url4"="http://www.google.com/"
"url5"="http://www.exif.org/"
"url6"="http://www.accessdata.com/"
"url7"="http://www.dell.com"
"url8"="mal.yahoo.com"
"url9"="My Network Places"
"url10"="http://web.mit.edu/maryr/www/amusements/"
"url11"="http://www.washingtonpost.com/"
"url12"="ftp://ftp.webtrek.com/"
"url13"="http://www.redhat.com/"
"url14"="http://www.download.com/"
"url15"="http://www.redhat.com/download/mirror.html"
"url16"="http://www.microsoft.com/"
"url17"="http://www.encase.com/"
"url18"="http://www.npr.org/"
"url19"="www.encaase.com"
"url20"="http://www.pocketpccity.com/"
"url21"="/Mobile Device"
"url22"="http://das.microsoft.com/activate"
"url23"="http://www.meguiars.com/"
"url24"="http://www.dell.com/"
"url25"=http://www.3com.com/
```

These keys show any URLs the user may have recently typed into Internet Explorer. Here I was able to get a good idea of what web sites the user had been browsing through.

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU]
"a"="regedit\\1"
"MRUList"="adcb"
"b"="F:\\Setup.exe\\1"
"c"="H:\\Setup.exe\\1"
"d"="G:\\Setup.exe\\1"
```

```
[HKEY_USERS\S-1-5-21-1547161642-842925246-1060284298-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU]
"a"="regedit\\1"
"MRUList"="adcb"
"b"="F:\\Setup.exe\\1"
"c"="H:\\Setup.exe\\1"
"d"="G:\\Setup.exe\\1"
```

These keys show the last commands executed. From the looks of things, it seems the user had been installing several programs from different locations. I found it interesting that there were three drive letters here, so there may have been several forms of media involved (CD-ROM, Zip disk, Jaz drive), or possibly the user was mapping drive letters to different sources on the network.

```
[HKEY_USERS\S-1-5-21-1547161642-842925246-1060284298-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*]
"a"="C:\\Program Files\\netscape\\communicator\\program\\ftkinstall1-1-29.exe"
"MRUList"="jhfedicagb"
"b"="E:\\NewDataSet11-26-02\\DigitalCameraFiles\\Kodak\\DC240\\EXIF Data.htm"
"c"="C:\\ftk\\kffinstall.exe"
"d"="G:\\Setup.exe"
"e"="C:\\kwh-furniture.jpg"
"f"="C:\\Documents and Settings\\A User\\Desktop\\Thumbnail.pdf"
"g"="C:\\larryslinuxtest.evd"
"h"="K:\\XPHOMEFI.007"
"i"="H:\\Setup.exe"
"j"="C:\\Documents and Settings\\A User\\My Documents\\sysinfo.txt"
```

This key shows the last files saved by the user. I found what appeared to be some installation files (ftkinstall1-1-29.exe, kffinstall.exe, setup.exe) being copied recently.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Products\C8D617F6F8933D11581E000540386890\InstallProperties]
"LocalPackage"="C:\\WINNT\\Installer\\10411.msi"
"RegOwner"="A User"
"RegCompany"=""
"ProductID"="12345-111-1111111-68966"
"AuthorizedCDFPrefix"=""
"Comments"=""
"Contact"=""
"DisplayVersion"="9.00.3907"
"HelpLink"=hex(2):68,74,74,70,3a,2f,2f,77,77,77,2e,6d,69,63,72,6f,73,6f,66,74,\
  2e,63,6f,6d,2f,77,69,6e,64,6f,77,73,00
"HelpTelephone"=""
"InstallDate"="20011004"
```

Here I was able to obtain the OS installation date of Oct. 4, 2001. The product ID was 12345-111-1111111-68966.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Netscape\Netscape Navigator\MAPI]
"CurrentVersion"="4.76.0.11"
"Enabled"=dword:00000000
```

The current version of Netscape.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Acrobat Reader\5.0\InstallPath]
@="C:\\Program Files\\Adobe\\Acrobat 5.0\\Reader"
```

The current version of Adobe Acrobat.

```
[HKEY_USERS\S-1-5-21-1547161642-842925246-1060284298-1000\Software\America Online\AOL
Instant Messenger (TM)\CurrentVersion\AutoUpgrade]
"LatestBetaNum"=dword:00000add
"LatestBetaVersion"="4.8.2781"
"LatestReleaseNum"=dword:00000ae6
"LatestReleaseVersion"="4.8.2790"
```

The current version of AOL Instant Messenger is shown here. I was hoping to find some other traces of AOL software on this system as AOL files can often be a wealth of information (Address books, user downloads, emails, etc…) but unfortunately this was a stand-alone version of IM. This is common these days as there has been a recent explosion of activity with AOL IM.

```
[HKEY_USERS\S-1-5-21-1547161642-842925246-1060284298-1000\Software\America Online\AOL
Instant Messenger (TM)\CurrentVersion\Login]
"Screen Name"="XXXXXXXX"

[HKEY_USERS\S-1-5-21-1547161642-842925246-1060284298-1000\Software\America Online\AOL
Instant Messenger (TM)\CurrentVersion\Users]
"XXXXXXXX"="XXXXXXXX"

[HKEY_USERS\S-1-5-21-1547161642-842925246-1060284298-1000\Software\America Online\AOL
Instant Messenger (TM)\CurrentVersion\Users\XXXXXXXX\recent IM ScreenNames]
"1"="XXXXXXXXX"
"2"="XXXXXXXX"
```

Here I have removed screen name information to ensure privacy but decided to include these keys just to show that AOL IM Screen names and “buddy lists” can be obtained from the registry as well.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinZip]
"DisplayName"="WinZip"
"UninstallString"="\"C:\\Program Files\\WinZip\\WINZIP32.EXE\" /uninstall"
"InstallLocation"="C:\\PROGRA~1\\WINZIP\\"
"Publisher"="WinZip Computing, Inc."
"VersionMajor"=dword:00000008
"VersionMinor"=dword:00000001
"DisplayVersion"=" 8.1  (4331)"
```

Winzip was version 8.1.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"AutoRestartShell"=dword:00000001
"DefaultDomainName"="W2K"
"DefaultUserName"="A User"
"LegalNoticeCaption"=""
"LegalNoticeText"=""
"PowerdownAfterShutdown"="0"
"ReportBootOk"="1"
"Shell"="Explorer.exe"
"ShutdownWithoutLogon"="1"
"System"=""
"Userinit"="C:\\WINNT\\system32\\userinit.exe,"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Synchronization Manager"="mobsync.exe /logon"
"Adaptec DirectCD"="C:\\PROGRA~1\\Adaptec\\DirectCD\\directcd.exe"
"CreateCD"="C:\\PROGRA~1\\Adaptec\\EASYCD~1\\CreateCD\\CreateCD.exe -r"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce]
```

Here I have extracted the registry keys that show startup processes of the Windows 2000 system, in the order they occur. The only process shown here that is worth noting is the Adaptec DirectCD software, as the others are typical Windows system processes.

Analysis of the Log Files

I felt at this time I had gotten a good general picture of the system and what kind of usage it had in the past. I decided to study the log files, particularly for the week prior to my visit to the IAC lab (approximately 3/8/2003 to 3/15/2003). From looking at the file access times generated by IRCR (covered later in Timeline Analysis), I thought it was very probable at this point that WinVNC and lsadump were somehow a part of their security demonstration the week before.

While IRCR is a decent tool for recovering useful Windows information on the fly, it does not record binary data when retrieving critical Windows log files. IRCR only records the text format, leaving out the Event Details. To be sure that I took back all the information I needed from the lab, I saved all log files in the .evt format, via Windows Event Viewer (located in Control Panel->Administrative Tools). By archiving the logs this way, I was able to import the exact contents of the logs into my own Event Viewer and bring up the Information Properties of whichever events I desired. In a real scenario where your system has been compromised, you can sometimes get details of the hacker's system such as domain name, workstation name, user name, etc. by looking at the event details.

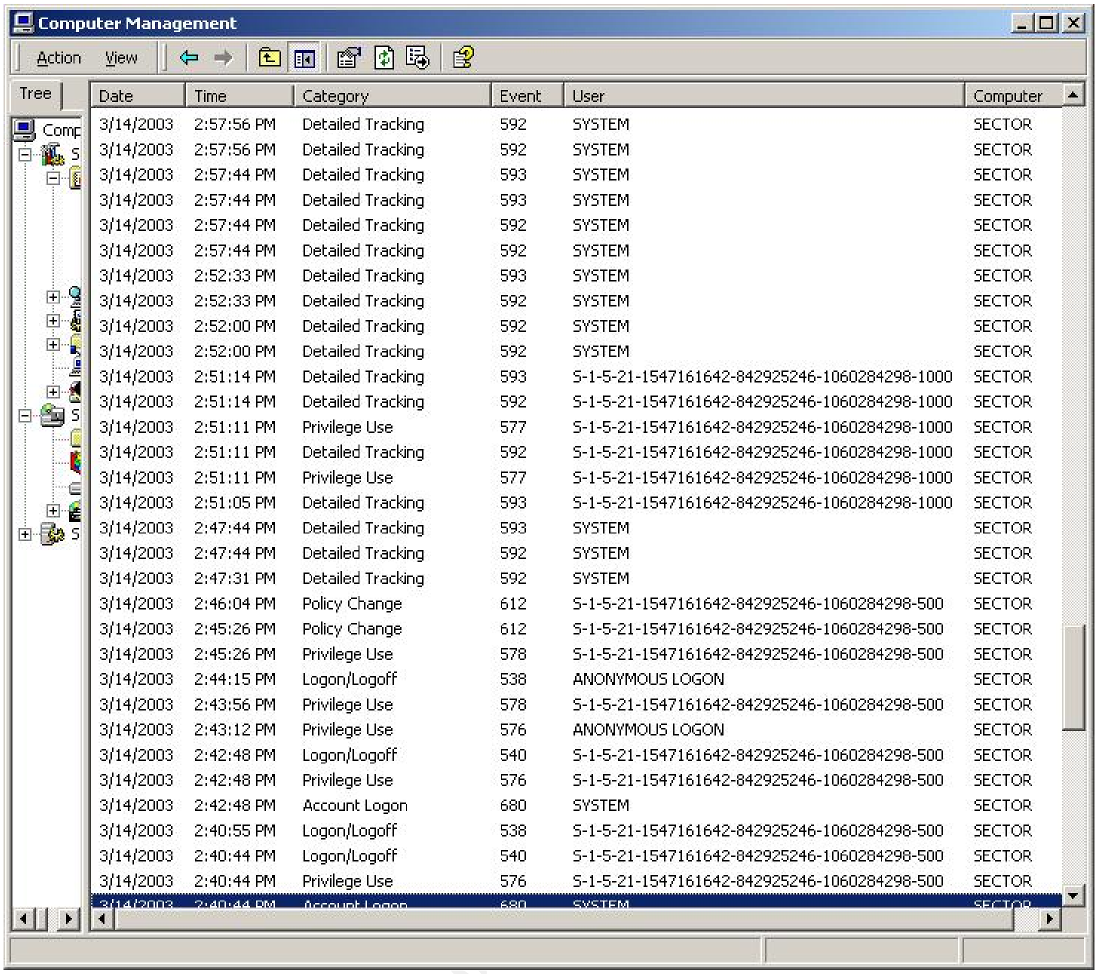
To get a starting point, I obtained the creation time of the G:\lsadump directory from my command prompt by using "**dir** lsadump /tc". The time was listed as 3/14/2003 3:08pm. I pulled up the system and security logs in Event Viewer to look for any interesting activity during that period.

From glancing at the system log, I was able to see that the machine had been start up and shutdown on 3/14/2003, and that was the last time it appeared the machine had been used. Prior to that, the machine had been start up and shutdown on 3/7/2003, and several times in the week prior to that. Paging down the log, it appeared that this was not really intended to be an "always on" server-type system. Most of the entries in the system file contained event IDs of 6005 and 6006, showing the start and stop of the event logging, or 6009 showing Service Pack 3 starting up. There were also many 2013 IDs, which simply mean the drive is nearly full to capacity. There wasn't much else to be said about the system logs.

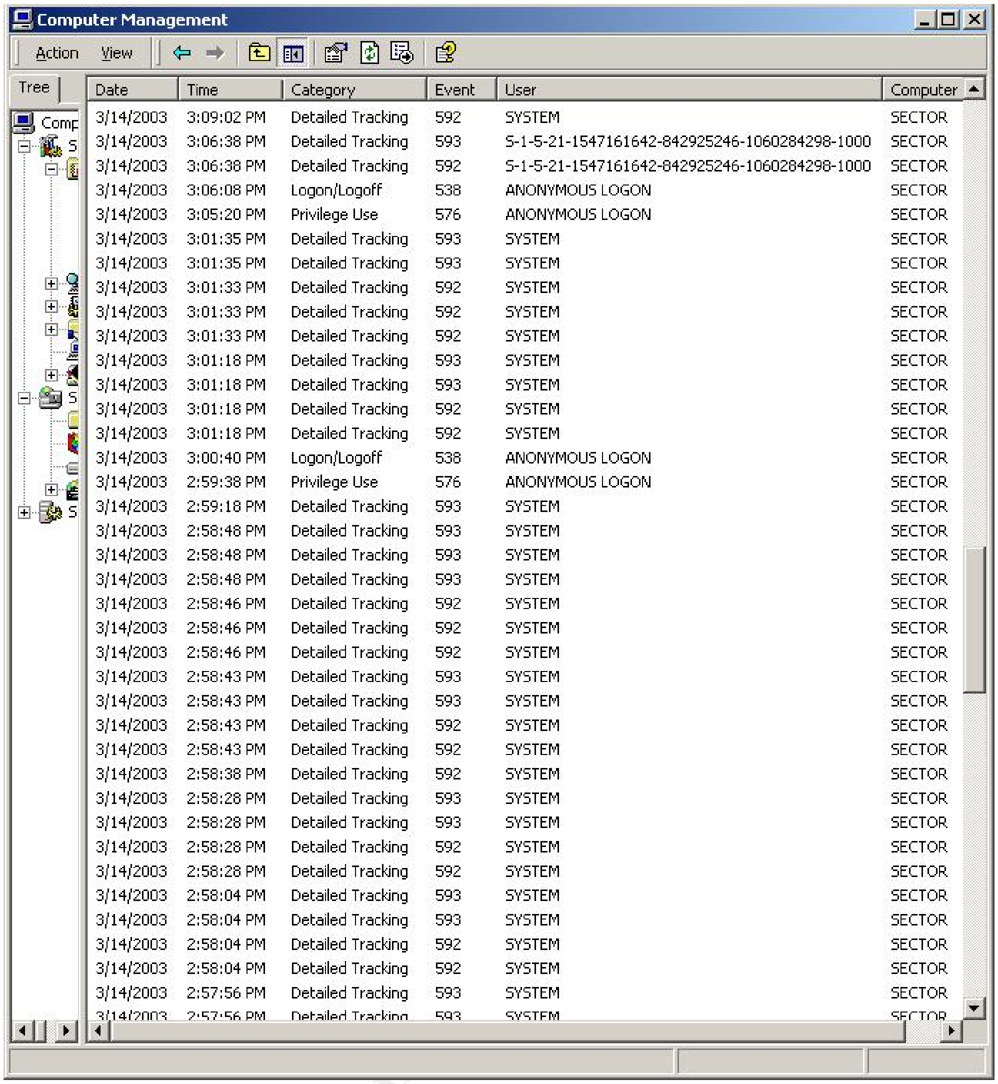
The security logs proved to be a little more interesting. I found a good amount of system activity on the afternoon of 3/14/2003. Two other remote machines had logged in and it appeared that one of them was being used to demonstrate a couple of NT Resource Kit capabilities, plus the lsadump2 program. I have constructed the following timeline outlining what I was able to learn.

Timeline

14:40:44	User at workstation SQLSERVER logs into SECTOR with administrator rights.
14:40:55	Workstation SQLSERVER logs out.
14:42:48	User at workstation FOO logs into SECTOR with administrator rights.
14:43:12	SECTOR accepts an anonymous logon.
14:43:56	Special privileges are assigned with SeTakeOwnershipPrivilege. This is indicative of the attacker (FOO) bypassing present security settings in order to attempt to take control of a file ownership.
14:44:15	Anonymous login logs off with NT Authority.
14:45:26	All auditing policies are turned off.
14:46:04	All auditing policies are turned back on.
14:51:14	The at.exe scheduler is run.
14:52:00	Remote.exe is started.
14:52:33	Ipconfig.exe is run.
14:57:44	4 net commands are seen run.
14:58:38	\vnc\WinVNC.exe is run.
14:58:43	2 more net commands seen are seen.
14:58:46	\vnc\WinVNC.exe is run again.
14:58:48	The first WinVNC exits.
14:59:18	The next WinVNC exits.
14:59:38	Special privileges assigned again via anonymous logon, with SeChangeNotifyPrivilege. This allows a user to traverse a directory tree without having the required access permissions.
15:01:18	2 more net commands seen.
15:01:33	\vnc\WinVNC.exe is run again.
15:05:20	Special privileges assigned again via anonymous logon, with SeChangeNotifyPrivilege.
15:06:38	"A User" runs ipconfig.exe.
15:09:02	\lsadump\lsadump2.exe is run



Date	Time	Category	Event	User	Computer
3/14/2003	2:57:56 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:57:56 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:57:44 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:57:44 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:57:44 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:57:44 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:52:33 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:52:33 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:52:00 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:52:00 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:51:14 PM	Detailed Tracking	593	S-1-5-21-1547161642-842925246-1060284298-1000	SECTOR
3/14/2003	2:51:14 PM	Detailed Tracking	592	S-1-5-21-1547161642-842925246-1060284298-1000	SECTOR
3/14/2003	2:51:11 PM	Privilege Use	577	S-1-5-21-1547161642-842925246-1060284298-1000	SECTOR
3/14/2003	2:51:11 PM	Detailed Tracking	592	S-1-5-21-1547161642-842925246-1060284298-1000	SECTOR
3/14/2003	2:51:11 PM	Privilege Use	577	S-1-5-21-1547161642-842925246-1060284298-1000	SECTOR
3/14/2003	2:51:05 PM	Detailed Tracking	593	S-1-5-21-1547161642-842925246-1060284298-1000	SECTOR
3/14/2003	2:47:44 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:47:44 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:47:31 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:46:04 PM	Policy Change	612	S-1-5-21-1547161642-842925246-1060284298-500	SECTOR
3/14/2003	2:45:26 PM	Policy Change	612	S-1-5-21-1547161642-842925246-1060284298-500	SECTOR
3/14/2003	2:45:26 PM	Privilege Use	578	S-1-5-21-1547161642-842925246-1060284298-500	SECTOR
3/14/2003	2:44:15 PM	Logon/Logoff	538	ANONYMOUS LOGON	SECTOR
3/14/2003	2:43:56 PM	Privilege Use	578	S-1-5-21-1547161642-842925246-1060284298-500	SECTOR
3/14/2003	2:43:12 PM	Privilege Use	576	ANONYMOUS LOGON	SECTOR
3/14/2003	2:42:48 PM	Logon/Logoff	540	S-1-5-21-1547161642-842925246-1060284298-500	SECTOR
3/14/2003	2:42:48 PM	Privilege Use	576	S-1-5-21-1547161642-842925246-1060284298-500	SECTOR
3/14/2003	2:42:48 PM	Account Logon	680	SYSTEM	SECTOR
3/14/2003	2:40:55 PM	Logon/Logoff	538	S-1-5-21-1547161642-842925246-1060284298-500	SECTOR
3/14/2003	2:40:44 PM	Logon/Logoff	540	S-1-5-21-1547161642-842925246-1060284298-500	SECTOR
3/14/2003	2:40:44 PM	Privilege Use	576	S-1-5-21-1547161642-842925246-1060284298-500	SECTOR
3/14/2003	2:40:44 PM	Account Logon	680	SYSTEM	SECTOR



Date	Time	Category	Event	User	Computer
3/14/2003	3:09:02 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	3:06:38 PM	Detailed Tracking	593	S-1-5-21-1547161642-842925246-1060284298-1000	SECTOR
3/14/2003	3:06:38 PM	Detailed Tracking	592	S-1-5-21-1547161642-842925246-1060284298-1000	SECTOR
3/14/2003	3:06:08 PM	Logon/Logoff	538	ANONYMOUS LOGON	SECTOR
3/14/2003	3:05:20 PM	Privilege Use	576	ANONYMOUS LOGON	SECTOR
3/14/2003	3:01:35 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	3:01:35 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	3:01:33 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	3:01:33 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	3:01:33 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	3:01:18 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	3:01:18 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	3:01:18 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	3:01:18 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	3:00:40 PM	Logon/Logoff	538	ANONYMOUS LOGON	SECTOR
3/14/2003	2:59:38 PM	Privilege Use	576	ANONYMOUS LOGON	SECTOR
3/14/2003	2:59:18 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:58:48 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:58:48 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:58:48 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:58:46 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:58:46 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:58:46 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:58:43 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:58:43 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:58:43 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:58:43 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:58:38 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:58:28 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:58:28 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:58:28 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:58:28 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:58:04 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:58:04 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:58:04 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:58:04 PM	Detailed Tracking	592	SYSTEM	SECTOR
3/14/2003	2:57:56 PM	Detailed Tracking	593	SYSTEM	SECTOR
3/14/2003	2:57:56 PM	Detailed Tracking	593	SYSTEM	SECTOR

First, I will give a little background on some of the tools and commands that are seen being run here. **At** is a Windows command that can be used to schedule other commands to be run at a certain time. It looks quite possible here that **at** was used at 2:51:14 to schedule the next command seen, remote.exe, to run at exactly 2:52pm.

Remote.exe, also known as the Remote Command Line, is a tool found in the NT Resource Kit. The name of the tool is a good description for what it does, as it allows users to gain a command prompt from a remote machine. The NT Resource Kit has sometimes been called the NT Hacking Kit, because while the tools provided can do a lot to help out system administrators, they have also been proven to have malicious qualities to them when put in the wrong hands. An attacker with a full command prompt of another machine at his disposal can be a dangerous thing.

WinVNC.exe, or Virtual Network Computing, is a tool developed by AT&T Research Labs that takes Remote.exe one step further by supplying the user with a full graphical user interface of the remote system. It is much like having full control of the remote Windows GUI interface, mouse clicks and all. Once again, this could be very helpful for administrators, or extremely dangerous if used by a malicious user. An attacker could even reboot the system or have access to Task Manager via Ctrl-Alt-Del.

Lsadump2.exe is a tool that can extract Local Security Authority Secrets from an NT system. In the hacker's eyes, it is considered to be an extremely powerful tool because the LSA gives access to a plethora of passwords, such as service account passwords, cached user passwords, and web passwords.

Net is a powerful command run from the Windows Command Prompt that has a large number of network-related uses, including logins, retrieval of network stats, configuring network shares, etc. It is a little outdated these days because everything that used to be done with **net** is now done through the Windows GUI.

While studying the timeline above, it appears that the "attacker" using the workstation FOO was attempting to run the tools mentioned above on our target machine, SECTOR. It will be interesting to see how the file system's history matches up with the above timeline later in this analysis.

Some notes of interest:

- It is unclear as to what role the user at workstation SQLSERVER played in this demonstration, but I have included its login with the timeline because of its close proximity to the other activity.

- According to log details, all auditing policies were shut off briefly at 14:45:26. In a normal attack scenario this small time frame would definitely be worth investigating, as the attacker could be trying to hide a password change or the creation of a new user.

- SECTOR does not restrict anonymous logins, so the attacker was able to open a null session at various points to change access permissions. This is a little strange to see this however, because FAT16 partitions have little support for object security features.

- The **net** commands seen near the WinVNC runs could likely signify the attacker attempting to install or configure WinVNC.

- The attacker may have had trouble getting WinVNC to work initially, as we see two WinVNC runs occur only 8 seconds apart and end very shortly after.

Network Processes

The following is a list of network services generated by IRCR. Note VNC server is still active.

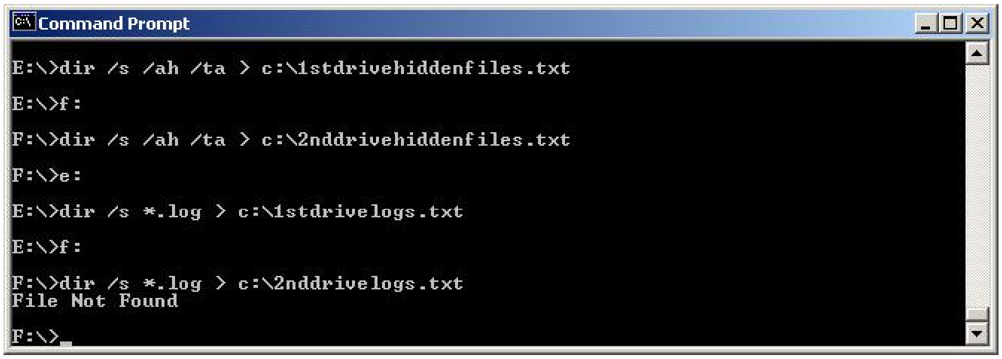
```
 Computer Name: SECTOR
 Domain Name: ACESLAB
 Time/Date: 19:09:32 Sun Mar 23  2003 Eastern Standard Time

-------------------------------------------------------------------------------
 net start - displays a list of running services.
-------------------------------------------------------------------------------

These Windows 2000 services are started:
   Automatic Updates
   COM+ Event System
   Computer Browser
   DHCP Client
   Distributed Link Tracking Client
   DNS Client
   Event Log
   IPSEC Policy Agent
   Logical Disk Manager
   Messenger
   Network Connections
   Plug and Play
   Print Spooler
   Protected Storage
   Remote Procedure Call (RPC)
   Remote Registry Service
   Removable Storage
   RunAs Service
   Security Accounts Manager
   Server
   Still Image Service
   System Event Notification
   Task Scheduler
   TCP/IP NetBIOS Helper Service
   Telephony
   VNC Server
   Windows Management Instrumentation
   Windows Management Instrumentation Driver Extensions
   Workstation

The command completed successfully.
```

From IRCR’s detailed services report:

```
VNC Server
       Name    winvnc
       State   Running
       Account LocalSystem
       File    "C:\vnc\WinVNC.exe" -service
       Start       Automatic
```

Hidden Files

At this time I wanted to get a listing of all hidden files and other log files. This was easily done from the Windows command prompt. At this point I had changed some configuration settings on my forensic machine, so the drives were mounted as E: and F:



```
E:\>dir /s /ah /ta > c:\1stdrivehiddenfiles.txt

E:\>f:

F:\>dir /s /ah /ta > c:\2nddrivehiddenfiles.txt

F:\>e:

E:\>dir /s *.log > c:\1stdrivelogs.txt

E:\>f:

F:\>dir /s *.log > c:\2nddrivelogs.txt
File Not Found

F:\>_
```

The following is a list of hidden files found. Unfortunately, since we are dealing with a FAT16 system, there are no access times given. We only have the access dates. However, by noting all the hidden system files that were last accessed on 3/14/2003, there is sufficient evidence that the system was last used on that date:

```
Volume in drive E has no label.
 Volume Serial Number is 7898-3AAB

 Directory of E:\

03/14/2003  12:00a           214,432 ntldr
03/14/2003  12:00a            34,724 NTDETECT.COM
03/14/2003  12:00a               192 boot.ini
10/04/2001  12:00a                 0 CONFIG.SYS
10/04/2001  12:00a                 0 AUTOEXEC.BAT
10/04/2001  12:00a                 0 IO.SYS
10/04/2001  12:00a                 0 MSDOS.SYS
03/25/2002  12:00a      <DIR>          System Volume Information
03/14/2003  12:00a               528 VDATA.SAV
04/04/2002  12:00a      <DIR>          Recycled
03/14/2003  12:00a           150,528 arcldr.exe
03/14/2003  12:00a           163,840 arcsetup.exe
03/14/2003  12:00a       201,326,592 pagefile.sys
01/21/2003  12:00a      <DIR>          Config.Msi
              11 File(s)    201,890,836 bytes

 Directory of E:\WINNT

10/04/2001  12:00a      <DIR>          inf
03/14/2003  12:00a            24,076 winnt.bmp
03/14/2003  12:00a            48,540 winnt256.bmp
03/14/2003  12:00a            21,692 folder.htt
03/14/2003  12:00a               271 desktop.ini
```

```
10/04/2001  12:00a      <DIR>          CSC
10/04/2001  12:00a      <DIR>          Installer
03/14/2003  12:00a             643,524 ShellIconCache
09/30/2002  12:00a      <DIR>          $NtServicePackUninstall$
               5 File(s)        738,103 bytes

 Directory of E:\WINNT\system32

10/04/2001  12:00a      <DIR>          dllcache
03/14/2003  12:00a              21,692 folder.htt
03/14/2003  12:00a                 271 desktop.ini
10/04/2001  12:00a      <DIR>          GroupPolicy
               2 File(s)         21,963 bytes

 Directory of E:\WINNT\system32\config

03/14/2003  12:00a               1,024 system.LOG
03/14/2003  12:00a               1,024 software.LOG
03/14/2003  12:00a               1,024 default.LOG
03/14/2003  12:00a               1,024 userdiff.LOG
10/04/2001  12:00a                   0 TempKey.LOG
03/14/2003  12:00a               1,024 SECURITY.LOG
03/14/2003  12:00a               1,024 SAM.LOG
               7 File(s)          6,144 bytes

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

03/14/2003  12:00a                 336 d06e3957-96ec-43f4-b5d0-410e2057f2b9
03/14/2003  12:00a                  24 Preferred
               2 File(s)            360 bytes

 Directory of E:\WINNT\repair

03/14/2003  12:00a             122,880 ntuser.dat
               1 File(s)        122,880 bytes

 Directory of E:\WINNT\Help

03/14/2003  12:00a              10,820 nocontnt.GID
               1 File(s)         10,820 bytes

 Directory of E:\WINNT\Fonts

03/14/2003  12:00a              36,672 app850.fon
03/14/2003  12:00a               6,352 cga40850.fon
03/14/2003  12:00a               6,336 cga40woa.fon
03/14/2003  12:00a               4,320 cga80850.fon
03/14/2003  12:00a               4,304 cga80woa.fon
03/14/2003  12:00a              23,408 coure.fon
03/14/2003  12:00a              31,712 courf.fon
03/14/2003  12:00a                  67 desktop.ini
03/14/2003  12:00a              36,656 dosapp.fon
03/14/2003  12:00a               8,384 ega40850.fon
03/14/2003  12:00a               8,368 ega40woa.fon
03/14/2003  12:00a               5,328 ega80850.fon
03/14/2003  12:00a               5,312 ega80woa.fon
03/14/2003  12:00a              24,480 marlett.ttf
03/14/2003  12:00a              57,936 serife.fon
03/14/2003  12:00a              81,728 seriff.fon
03/14/2003  12:00a              26,112 smalle.fon
03/14/2003  12:00a              64,656 sserife.fon
03/14/2003  12:00a              89,856 sseriff.fon
03/14/2003  12:00a              56,336 symbole.fon
03/14/2003  12:00a               5,232 vga850.fon
03/14/2003  12:00a               5,360 vgafix.fon
03/14/2003  12:00a               5,168 vgaoem.fon
03/14/2003  12:00a               7,280 vgasys.fon
03/14/2003  12:00a              10,976 8514fix.fon
03/14/2003  12:00a              12,288 8514oem.fon
03/14/2003  12:00a               9,280 8514sys.fon
03/14/2003  12:00a              21,504 smallf.fon
```

```
03/14/2003  12:00a               5,184 vga860.fon
03/14/2003  12:00a               5,200 vga863.fon
03/14/2003  12:00a               5,184 vga865.fon
              31 File(s)        670,979 bytes

 Directory of E:\WINNT\Web

03/14/2003  12:00a               1,316 webview.css
03/14/2003  12:00a               4,659 controlp.htt
03/14/2003  12:00a               5,296 default.htt
03/14/2003  12:00a               3,210 folder.htt
03/14/2003  12:00a              13,280 nethood.htt
03/14/2003  12:00a              13,798 printers.htt
03/14/2003  12:00a              11,149 recycle.htt
03/14/2003  12:00a               6,489 schedule.htt
03/14/2003  12:00a               8,898 dialup.htt
03/14/2003  12:00a               8,248 wvleft.bmp
03/14/2003  12:00a                  54 wvline.gif
03/14/2003  12:00a              14,865 wvlogo.gif
03/14/2003  12:00a              90,056 classic.bmp
03/14/2003  12:00a                 634 classic.htt
03/14/2003  12:00a              31,080 folder.bmp
03/14/2003  12:00a               1,024 starter.htt
03/14/2003  12:00a              31,080 starter.bmp
03/14/2003  12:00a              31,080 preview.bmp
03/14/2003  12:00a              16,981 imgview.htt
03/14/2003  12:00a                 830 deskmovr.htt
03/14/2003  12:00a               2,913 safemode.htt
03/14/2003  12:00a              19,355 fsresult.htt
03/14/2003  12:00a              28,565 standard.htt
03/14/2003  12:00a              31,438 webview.js
03/14/2003  12:00a              12,403 wvnet.gif
03/14/2003  12:00a               2,642 exclam.gif
03/14/2003  12:00a                 842 bullet.gif
03/14/2003  12:00a                  80 plushot.gif
03/14/2003  12:00a                  59 pluscold.gif
03/14/2003  12:00a                  77 minhot.gif
03/14/2003  12:00a                  56 mincold.gif
03/14/2003  12:00a              11,009 ftp.htt
              32 File(s)        403,466 bytes

 Directory of E:\WINNT\security\templates

03/14/2003  12:00a      <DIR>          policies
               0 File(s)              0 bytes

 Directory of E:\WINNT\Tasks

03/14/2003  12:00a                  65 desktop.ini
03/14/2003  12:00a                   6 SA.DAT
               2 File(s)             71 bytes

 Directory of E:\WINNT\Downloaded Program Files

03/14/2003  12:00a                  65 desktop.ini
               1 File(s)             65 bytes

 Directory of E:\WINNT\Offline Web Pages

03/14/2003  12:00a                  65 desktop.ini
               1 File(s)             65 bytes

 Directory of E:\Documents and Settings

10/04/2001  12:00a      <DIR>          Default User
               0 File(s)              0 bytes

 Directory of E:\Documents and Settings\Default User

10/04/2001  12:00a      <DIR>          Application Data
10/04/2001  12:00a      <DIR>          NetHood
```

```
10/04/2001  12:00a      <DIR>          PrintHood
10/04/2001  12:00a      <DIR>          Recent
10/04/2001  12:00a      <DIR>          SendTo
10/04/2001  12:00a      <DIR>          Templates
10/04/2001  12:00a      <DIR>          Local Settings
03/14/2003  12:00a             122,880 NTUSER.DAT
               1 File(s)        122,880 bytes

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

03/14/2003  12:00a                 438 Desktop.ini
               1 File(s)            438 bytes

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

10/04/2001  12:00a      <DIR>          Application Data
               0 File(s)              0 bytes

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

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

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

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of E:\Documents and Settings\Default User\Local Settings\Temporary Internet
Files\Content.IE5\Q3UBMV87

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of E:\Documents and Settings\Default User\Local Settings\Temporary Internet
Files\Content.IE5\NSZLRMZ5

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

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

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of E:\Documents and Settings\Default User\Local Settings\Temporary Internet
Files\Content.IE5\EBKW63RM

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

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

03/14/2003  12:00a                 113 desktop.ini
               1 File(s)            113 bytes

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

03/14/2003  12:00a                 113 desktop.ini
               1 File(s)            113 bytes

 Directory of E:\Documents and Settings\All Users

10/04/2001  12:00a      <DIR>          Application Data
10/04/2001  12:00a      <DIR>          Templates
10/04/2001  12:00a      <DIR>          DRM
03/14/2003  12:00a               2,342 ntuser.pol
               1 File(s)          2,342 bytes
 Directory of E:\Documents and Settings\All Users\Application Data\Microsoft\Windows
NT\MSFax

10/04/2001  12:00a      <DIR>          faxreceive
10/04/2001  12:00a      <DIR>          queue
               0 File(s)              0 bytes

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

10/04/2001  12:00a      <DIR>          My Faxes
               0 File(s)              0 bytes

 Directory of E:\Documents and Settings\A User

03/14/2003  12:00a             811,008 NTUSER.DAT
10/04/2001  12:00a      <DIR>          Local Settings
10/04/2001  12:00a      <DIR>          Templates
10/04/2001  12:00a      <DIR>          SendTo
10/04/2001  12:00a      <DIR>          Recent
10/04/2001  12:00a      <DIR>          PrintHood
10/04/2001  12:00a      <DIR>          NetHood
10/04/2001  12:00a      <DIR>          Application Data
03/14/2003  12:00a               1,024 ntuser.dat.LOG
03/14/2003  12:00a                 180 ntuser.ini
               3 File(s)        812,212 bytes

 Directory of E:\Documents and Settings\A User\Local Settings

10/04/2001  12:00a      <DIR>          Application Data
               0 File(s)              0 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\History

03/14/2003  12:00a                 113 desktop.ini
               1 File(s)            113 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\History\History.IE5

03/14/2003  12:00a                 113 desktop.ini
               1 File(s)            113 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\Temporary Internet Files

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\Temporary Internet
Files\Content.IE5

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\Temporary Internet
Files\Content.IE5\RKRRWQAH

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\Temporary Internet
Files\Content.IE5\40G3A8GJ

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\Temporary Internet
Files\Content.IE5\YH9ST3VW

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes
 Directory of E:\Documents and Settings\A User\Local Settings\Temporary Internet
Files\Content.IE5\VD6YW10S

03/14/2003  12:00a                  67 desktop.ini
               1 File(s)             67 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\Application
Data\Microsoft\Windows

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

 Directory of E:\Documents and Settings\A User\Recent

03/14/2003  12:00a                 122 Desktop.ini
               1 File(s)            122 bytes

 Directory of E:\Documents and Settings\A User\My Documents\My Pictures

03/14/2003  12:00a                 438 Desktop.ini
03/14/2003  12:00a               7,168 Thumbs.db
               2 File(s)          7,606 bytes

 Directory of E:\Documents and Settings\A User\NetHood\Computers Near Me

03/14/2003  12:00a                  92 Desktop.ini
               1 File(s)             92 bytes

 Directory of E:\Documents and Settings\A User\NetHood\My Web Sites on MSN

03/14/2003  12:00a                  92 Desktop.ini
               1 File(s)             92 bytes

 Directory of E:\Documents and Settings\A User\Favorites

03/14/2003  12:00a                  83 Desktop.ini
               1 File(s)             83 bytes

 Directory of E:\Documents and Settings\A User\Application Data\Microsoft\Internet
Explorer

03/14/2003  12:00a               2,656 Desktop.htt
               1 File(s)          2,656 bytes

 Directory of E:\Documents and Settings\A User\Application Data\Microsoft\Protect\S-1-5-
21-1547161642-842925246-1060284298-1000

03/14/2003  12:00a                 456 a29c66eb-a542-48e8-8357-919d13a602c8
03/14/2003  12:00a                  24 Preferred
03/14/2003  12:00a                 456 fc1630fb-7992-4dd2-b040-74b8ec3804aa
               3 File(s)            936 bytes

 Directory of E:\Documents and Settings\A User\Application Data\Microsoft\Office\Recent

03/14/2003  12:00a                  77 index.dat
               1 File(s)             77 bytes

 Directory of E:\Program Files

03/14/2003  12:00a              21,952 folder.htt
03/14/2003  12:00a                 271 desktop.ini
04/12/2002  12:00a      <DIR>          InstallShield Installation Information
06/21/2002  12:00a      <DIR>          Uninstall Information
09/30/2002  12:00a      <DIR>          WindowsUpdate
               2 File(s)         22,223 bytes

 Directory of E:\Program Files\Common Files\Microsoft Shared\Web Folders

03/14/2003  12:00a               7,994 PUBPLACE.HTT
               1 File(s)          7,994 bytes
 Directory of E:\Program Files\Common Files\Microsoft Shared\VS98

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Common Files\Microsoft Shared\VS98\resources

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Common Files\Microsoft Shared\VS98\resources\1033

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Uninstall Information

06/21/2002  12:00a      <DIR>          MDAC_CORE
06/21/2002  12:00a      <DIR>          MSXML
06/21/2002  12:00a      <DIR>          SQLXMLX
06/21/2002  12:00a      <DIR>          SQLNET
06/21/2002  12:00a      <DIR>          SQLODBC
06/21/2002  12:00a      <DIR>          SQLOLEDB
               0 File(s)              0 bytes

 Directory of E:\Program Files\Uninstall Information\MDAC_CORE

03/14/2003  12:00a           2,518,427 MDAC_CORE.DAT
03/14/2003  12:00a               7,426 MDAC_CORE.INI
               2 File(s)      2,525,853 bytes

 Directory of E:\Program Files\Uninstall Information\MSXML

06/21/2002  12:00a                   0 MSXML.DAT
03/14/2003  12:00a                 232 MSXML.INI
               2 File(s)            232 bytes

 Directory of E:\Program Files\Uninstall Information\SQLXMLX

06/21/2002  12:00a                   0 SQLXMLX.DAT
03/14/2003  12:00a                 240 SQLXMLX.INI
               2 File(s)            240 bytes

 Directory of E:\Program Files\Uninstall Information\SQLNET

03/14/2003  12:00a             162,852 SQLNET.DAT
03/14/2003  12:00a                 895 SQLNET.INI
               2 File(s)        163,747 bytes

 Directory of E:\Program Files\Uninstall Information\SQLODBC

03/14/2003  12:00a             287,687 SQLODBC.DAT
03/14/2003  12:00a                 335 SQLODBC.INI
               2 File(s)        288,022 bytes

 Directory of E:\Program Files\Uninstall Information\SQLOLEDB

03/14/2003  12:00a             314,210 SQLOLEDB.DAT
03/14/2003  12:00a                 340 SQLOLEDB.INI
               2 File(s)        314,550 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\Common

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes
 Directory of E:\Program Files\Microsoft eMbedded Tools\Common\Setup

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\Common\Setup\1033

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\Common\Tools

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\Common\EVC

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\Common\EVC\Bin

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\Common\EVC\Bin\IDE

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\Common\EVC\AddIns

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\Common\EVC\Template

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\Common\EVC\Template\ATLCE

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\Common\EVC\Macros

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\Include

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\Include\ObjModel

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\Include\Win32

08/26/2002  12:00a                 0 MSCREATE.DIR
               1 File(s)             0 bytes
 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE200

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE200\TARGET

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE200\TARGET\MIPS

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE200\TARGET\SH3

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE200\BIN

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE201

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE201\TARGET

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE201\TARGET\SH3

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE201\TARGET\MIPS

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE201\BIN

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE210

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE210\TARGET

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE210\TARGET\ARM

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE210\TARGET\SH4

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE210\TARGET\SH3
```

```
08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE210\TARGET\MIPS

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE210\TARGET\MIPFP

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE210\TARGET\X86

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE210\TARGET\PPC

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE210\BIN

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE211

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE211\TARGET

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE211\TARGET\PPC

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE211\TARGET\X86

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE211\TARGET\MIPFP

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE211\TARGET\ARM

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE211\TARGET\SH4

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE211\TARGET\SH3

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE211\TARGET\MIPS
```

```
08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE211\BIN

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE212

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE212\TARGET

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE212\TARGET\PPC

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE212\TARGET\X86

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE212\TARGET\MIPFP

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE212\TARGET\ARM

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE212\TARGET\THUMB

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE212\TARGET\SH4

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE212\TARGET\SH3

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE212\TARGET\MIPS

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE212\BIN

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE300

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE300\TARGET

08/26/2002  12:00a                   0 MSCREATE.DIR
```

```
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE300\TARGET\ARM

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE300\TARGET\SH3

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE300\TARGET\SH4

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE300\TARGET\THUMB

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE300\TARGET\MIPS

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE300\TARGET\MIPFP

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE300\TARGET\PPC

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE300\TARGET\X86

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\Program Files\Microsoft eMbedded Tools\EVC\WCE300\BIN

08/26/2002  12:00a                   0 MSCREATE.DIR
               1 File(s)              0 bytes

 Directory of E:\WinHex

03/14/2003  12:00a              19,062 WinHex.GID
               1 File(s)         19,062 bytes

 Directory of E:\Recycled

03/14/2003  12:00a                 820 INFO2
03/14/2003  12:00a                 820 INFO
03/14/2003  12:00a                  65 desktop.ini
               3 File(s)          1,705 bytes

     Total Files Listed:
             221 File(s)    208,169,388 bytes
              42 Dir(s)      30,998,528 bytes free

Volume in drive F is EVIDENCE
 Volume Serial Number is A8D1-BCA4

 Directory of F:\

04/04/2002  12:00a      <DIR>          Recycled
               0 File(s)              0 bytes
 Directory of F:\Recycled

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

     Total Files Listed:
               2 File(s)             85 bytes
               1 Dir(s)  10,671,906,816 bytes free
```

Other Log Files

Other log files found on the system, with modified times, are shown:

```
Volume in drive E has no label.
 Volume Serial Number is 7898-3AAB

 Directory of E:\

12/04/2002  09:26a               4,290 Ext2RdfDlg.log
               1 File(s)          4,290 bytes

 Directory of E:\WINNT

10/04/2001  11:17a             100,060 setupact.log
10/04/2001  10:55a                   0 setuperr.log
03/14/2003  02:33p             527,726 setupapi.log
09/30/2002  04:56p              59,339 iis5.log
09/30/2002  04:56p              49,278 comsetup.log
09/30/2002  04:51p                 971 ockodak.log
09/30/2002  04:51p              13,741 ocgen.log
10/04/2001  10:59a                  96 mmdet.log
10/04/2001  11:07a                 384 COM+.log
01/24/2003  11:04a               1,562 Sti_Trace.log
06/21/2002  09:31a              22,149 dasetup.log
06/21/2002  09:31a                 354 muisetup.log
09/30/2002  04:51p             164,521 svcpack.log
09/30/2002  04:51p                 339 msmqprop.log
09/30/2002  04:51p                 194 sptsupd.log
09/30/2002  04:56p               1,429 imsins.log
01/24/2003  10:09a                 461 Directx.log
              17 File(s)        942,604 bytes

 Directory of E:\WINNT\system32\wbem\Logs

03/14/2003  03:25p              49,035 wbemcore.log
09/30/2002  04:51p               3,032 mofcomp.log
04/03/2002  09:49a               1,468 wmiprov.log
03/14/2003  03:25p              20,236 WinMgmt.log
04/03/2002  09:38a                   2 DSProvider.log
03/14/2003  02:33p               9,470 wmiadap.log
09/30/2002  04:51p                 106 wbemess.log
02/05/2003  09:06a                   2 WBEMSNMP.log
02/05/2003  09:06a                   2 NTEVT.log
               9 File(s)         83,353 bytes

 Directory of E:\WINNT\system32\export

09/30/2002  04:47p              10,552 encinst.log
               1 File(s)         10,552 bytes

 Directory of E:\WINNT\system32\DTCLog

10/04/2001  11:06a           4,194,304 MSDTC.LOG
               1 File(s)      4,194,304 bytes

 Directory of E:\WINNT\repair
```

```
10/04/2001  11:07a             140,887 setup.log
               1 File(s)        140,887 bytes

 Directory of E:\WINNT\security

10/04/2001  10:56a           1,048,576 res2.log
10/04/2001  10:56a           1,048,576 res1.log
03/14/2003  02:52p           1,048,576 edb.log
10/04/2001  11:12a           1,048,576 edb00004.log
               4 File(s)      4,194,304 bytes

 Directory of E:\WINNT\security\logs

10/04/2001  11:10a             109,874 scesetup.log
10/04/2001  11:10a               2,576 backup.log
09/30/2002  04:51p               4,440 scesrv.log
09/30/2002  04:58p             188,200 scepol.log
               4 File(s)        305,090 bytes

 Directory of E:\WINNT\Debug

03/14/2003  02:33p                   0 PASSWD.LOG
03/21/2002  09:23a               5,887 NetSetup.LOG
03/14/2003  02:33p                   0 ipsecpa.log
03/14/2003  02:33p                   0 oakley.log
               4 File(s)          5,887 bytes

 Directory of E:\WINNT\Debug\UserMode

03/14/2003  02:33p              11,184 userenv.log
               1 File(s)         11,184 bytes

 Directory of E:\Documents and Settings\All Users\Documents\DrWatson

01/28/2003  03:24p              64,269 drwtsn32.log
               1 File(s)         64,269 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\Temp

01/21/2003  10:48a               8,464 dtSearch_Setup.log
11/20/2002  09:51a             203,932 dtSearch_Setup_MSI.log
11/22/2002  09:43a                   0 WPI7.log
11/22/2002  09:40a              31,525 offcln9.log
12/20/2002  01:18p              33,333 offcln10.log
09/30/2002  03:13p               2,035 outstore.log
               6 File(s)        279,289 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\Application
Data\Identities\{3D481FC2-7D7C-4FCD-980B-A885B88EC920}\Microsoft\Outlook Express

12/06/2002  01:56p               3,884 cleanup.log
               1 File(s)          3,884 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\Application
Data\Identities\{100275A7-AEAD-4ADA-A1B1-C7AE47246B70}\Microsoft\Outlook Express

12/06/2002  01:55p               2,088 cleanup.log
               1 File(s)          2,088 bytes

 Directory of E:\Documents and Settings\A User\Local Settings\Application
Data\Identities\{0835AFE8-1D4A-4668-9587-F08B3D587BE0}\Microsoft\Outlook Express

12/06/2002  02:02p                 937 cleanup.log
               1 File(s)            937 bytes

 Directory of E:\Program Files\Adaptec\Shared\Web-Checkup

01/19/2000  01:01a                   0 updates.log
               1 File(s)              0 bytes
 Directory of E:\Program Files\TransMac

04/04/2002  02:03p               1,583 INSTALL.LOG
               1 File(s)          1,583 bytes

 Directory of E:\Program Files\AIM95

04/24/2002  12:46p              11,571 INSTALL.LOG
               1 File(s)         11,571 bytes

 Directory of E:\Program Files\AccessData\AccessData Forensic Toolkit\Program

12/16/2002  09:30a                   0 FTKTrace000.log
               1 File(s)              0 bytes

 Directory of E:\Program Files\ILook

10/01/2002  09:44a              50,086 ST6UNST.LOG
               1 File(s)         50,086 bytes

 Directory of E:\Program Files\RTToolsLinux\OutlookExpress97

10/30/2002  10:20a              77,309 cleanup.log
               1 File(s)         77,309 bytes

 Directory of E:\Program Files\RTToolsLinux\OutlookExpress5

10/30/2002  10:20a              12,370 cleanup.log
               1 File(s)         12,370 bytes

     Total Files Listed:
              60 File(s)     10,395,841 bytes
               0 Dir(s)      30,998,528 bytes free
```

From studying the other log files I was able to verify the following:

- C:\WINNT\Setupact.log was created 10/4/2001 marking the near exact time of OS installation.

- Several log files in C:\WINNT were created on 10/4/2001 but modified 9/30/2002 at around 4:51pm, marking the installation of Windows 2000 Service Pack 3.

- C:\WINNT\dasetup.log contained the install log of Microsoft Access Data Components version 2.6, installed 6/21/2002 at 9:30am.

- C:\WINNT\Directx.log showed the user attempted to install DirectX on 1/24/2003 but the installation failed due to lack of drive space.

- Several system logs were last modified on 3/14/2003, providing further evidence that the machine was last used on that date.

- C:\WINNT\Debug\NetSetup.log contained evidence that the machine's name was initially WORKGROUP, and the domain was ACES9THFLOOR. These were changed to SECTOR and ACESLAB, respectfully, on 3/21/2002.

- C:\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log showed that Dr. Watson was installed on the machine and was last used 1/28/2003.

- C:\Documents and Settings\A User\Local Settings\Temp\dtSearch_Setup.log was created on 11/20/2002 which marks the installation date of dtSearch. From the contents of the log and the modification date, it also appears dtSearch was upgraded on 1/21/2003.

- The three files named cleanup.log contained cleanup information for Microsoft Outlook, but there didn't appear to be an awful lot of activity.

- C:\Program Files\TransMac\INSTALL.log marked the installation of TransMac on 4/4/2002.

- C:\Program Files\AIM95\INSTALL.log marked the installation of AOL Instant Messenger on 4/4/2002.

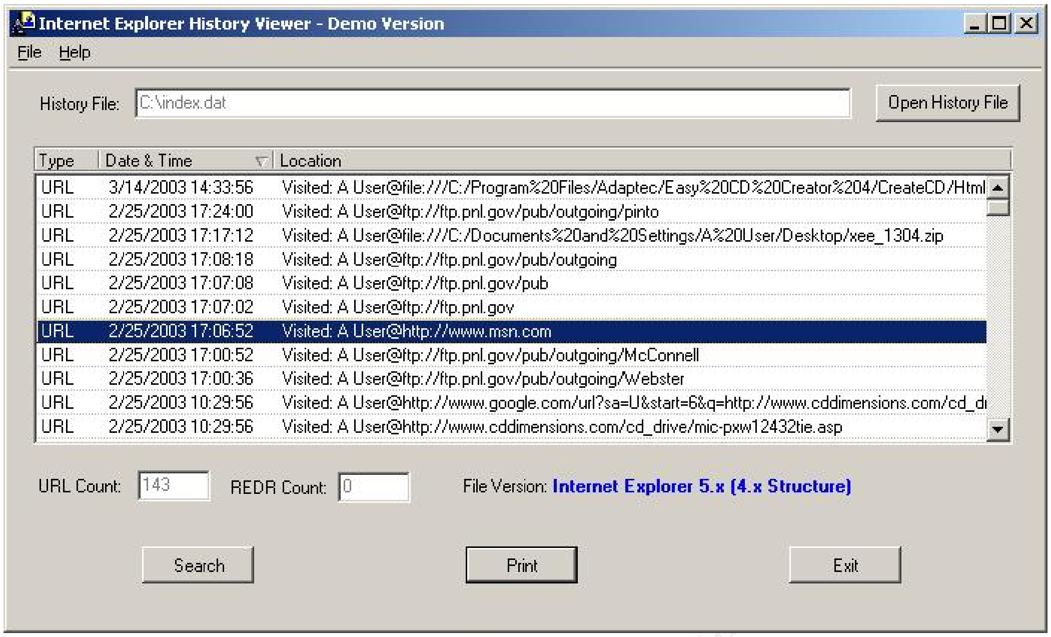
Analysis of Internet Activity

By looking in the installation directories of Internet Explorer and Netscape, I was able to retrieve some evidence of Internet activity. Also, the "Documents and Settings" folder held a good amount of information on the surfing habits of the user "A User".

Internet Explorer histories are commonly found by locating the index.dat files, which in this case were found in the hidden directory:

C:\Documents and Settings\A User\Local Settings\History\History.IE5\index.dat

By running this file through another tool called Internet Explorer History Viewer, I was able to browse through the URL history of "A User":



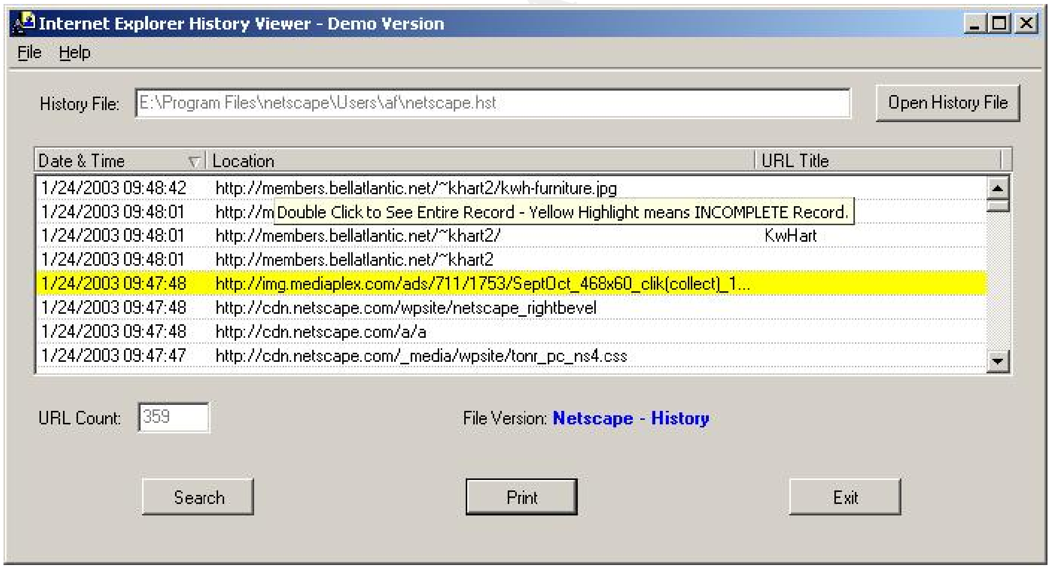
History File: C:\index.dat

Type	Date & Time	Location
URL	3/14/2003 14:33:56	Visited: A User@file:///C:/Program%20Files/Adaptec/Easy%20CD%20Creator%204/CreateCD/Html
URL	2/25/2003 17:24:00	Visited: A User@ftp://ftp.pnl.gov/pub/outgoing/pinto
URL	2/25/2003 17:17:12	Visited: A User@file:///C:/Documents%20and%20Settings/A%20User/Desktop/xee_1304.zip
URL	2/25/2003 17:08:18	Visited: A User@ftp://ftp.pnl.gov/pub/outgoing
URL	2/25/2003 17:07:08	Visited: A User@ftp://ftp.pnl.gov/pub
URL	2/25/2003 17:07:02	Visited: A User@ftp://ftp.pnl.gov
URL	2/25/2003 17:06:52	Visited: A User@http://www.msn.com
URL	2/25/2003 17:00:52	Visited: A User@ftp://ftp.pnl.gov/pub/outgoing/McConnell
URL	2/25/2003 17:00:36	Visited: A User@ftp://ftp.pnl.gov/pub/outgoing/Webster
URL	2/25/2003 10:29:56	Visited: A User@http://www.google.com/url?sa=U&start=6&q=http://www.cddimensions.com/cd_dı
URL	2/25/2003 10:29:56	Visited: A User@http://www.cddimensions.com/cd_drive/mic-pxw12432tie.asp

URL Count: 143 REDR Count: 0 File Version: **Internet Explorer 5.x (4.x Structure)**

I also found the Netscape history file, which is commonly found as netscape.hst, at:

C:\Program Files\netscape\Users\af\netscape.hst



History File: E:\Program Files\netscape\Users\af\netscape.hst

Date & Time	Location	URL Title
1/24/2003 09:48:42	http://members.bellatlantic.net/~khart2/kwh-furniture.jpg	
1/24/2003 09:48:01	http://m Double Click to See Entire Record - Yellow Highlight means INCOMPLETE Record.	
1/24/2003 09:48:01	http://members.bellatlantic.net/~khart2/	KwHart
1/24/2003 09:48:01	http://members.bellatlantic.net/~khart2	
1/24/2003 09:47:48	http://img.mediaplex.com/ads/711/1753/SeptOct_468x60_clik(collect)_1...	
1/24/2003 09:47:48	http://cdn.netscape.com/wpsite/netscape_rightbevel	
1/24/2003 09:47:48	http://cdn.netscape.com/a/a	
1/24/2003 09:47:47	http://cdn.netscape.com/_media/wpsite/tonr_pc_ns4.css	

URL Count: 359 File Version: **Netscape - History**

For this exercise, there was entirely too much Internet history data to list here. Basically, I found histories dating back to April 4, 2002, and also noticed one history entry on October 4, 2001 which appeared to be some kind of generic welcome message, further signifying that that was the machine's install date. The last time Netscape had been used was on January 24, 2003, while Internet Explorer had been used more recently. The most popular web sites found (from both history files) were:

www.buy.com
www.dell.com
www.forensics-intl.com
www.google.com
www.netscape.com
www.aol.com

I was also able to easily locate and confirm the Internet Explorer directories for cookies, favorites (bookmarks), and cache files by performing simple searches in Explorer and looking at my hidden files listing:

C:\Documents and Settings\A User\Cookies\*.txt
C:\Documents and Settings\A User\Local Settings\Temporary Internet Files\Content.IE5\*.*
C:\Documents and Settings\A User\Favorites\*.url

Also, the Netscape cache files were found at:

C:\Program Files\netscape\Users\af\Cache\*.*

Netscape cookies are all stored in one file. The Netscape cookie file was found at:

C:\Program Files\netscape\Users\af\cookies.txt

Like cookies, Netscape bookmarks are all stored in one HTML formatted file. The bookmark.htm file I found didn't contain any other bookmarks other than the bookmarks generated by default at installation. The Netscape bookmark file was found at:

C:\Program Files\netscape\Users\af\bookmarks.htm

Again, I am not listing the contents of the directories and files because it is simply too much to list. I located these Internet findings to show that a great deal of information is available here and the files saved by Internet Explorer and Netscape can supply the forensic examiner with a useful timeline of web activity.

Additionally, I found there was very little email activity on the system. The email files for Outlook (*.dbx) and Netscape (C:\Program Files\netscape\Users\af\Mail\Sent.) were nearly empty, with only some generic messages.

Timeline Results

I was able to create a timeline of the entire system by mounting the image on my Linux partition and using the mac_daddy perl script mentioned in the "Unknown Binary" section:

```
#perl mac_daddy.pl /mnt/hdc1 > /images/mac_daddy.hdc1
```

By coupling the MACTime analysis with the previous media analysis I had done, I was able to list the highlights of the system's history:

```
Oct 04 2001 11:52:08
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/winnt
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/winnt/AppPatch
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/winnt/Config
  ...............
```

- Creation times of the WinNT directories, plus evidence found in the registry, log files, etc. mark the system installation.

Mar 21 2002 12:34:22

- C:\WINNT\Debug\NetSetup.log contained evidence that the machine's name was initially WORKGROUP, and the domain was ACES9THFLOOR. These were changed to SECTOR and ACESLAB, respectfully, on 3/21/2002

```
Mar 28 2002 10:48:36
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/WinZip
 546764 ..c -rwxr-xr-x root     root     /mnt/hdc1/Program Files/WinZip/winzip.hlp
2076739 ..c -rwxr-xr-x root     root     /mnt/hdc1/Program Files/WinZip/winzip32.exe
```

- WinZip is installed.

```
Mar 28 2002 10:49:10
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/WinHex
 552960 ..c -rwxr-xr-x root     root     /mnt/hdc1/WinHex/WinHex.exe
```

- WinHex is installed.

```
Mar 29 2002 12:03:32
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/Adaptec
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/Adaptec/Easy CD Creator
4
```

- Adaptec Easy CD Creator 4 software is installed.

```
Mar 29 2002 14:25:34
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/Adobe
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/Adobe/Acrobat 5.0
```

- Adobe Acrobat 5.0 is installed.

```
Apr 04 2002 13:37:36
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/HFVExplorer
 734720 ..c -rwxr-xr-x root     root     /mnt/hdc1/Program
Files/HFVExplorer/HFVExplorer.exe
```

- HFVExplorer is installed.

```
Apr 04 2002 14:03:36
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Documents and Settings/A User/Start
Menu/Programs/TransMac
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/TransMac
```

- TransMac is installed (verified by *.log file).

Apr 05 2002 09:53:08

```
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/netscape
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/netscape/communicator
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program
Files/netscape/communicator/program
```

- Netscape is installed.

Apr 05 2002 09:54:30

```
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/netscape/Users
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/netscape/Users/af
```

- The Netscape user "af" is added.

Apr 22 2002 11:22:28

```
  13072 ..c -rwxr-xr-x root     root     /mnt/hdc1/winnt/system32/pjlmon.dll
 134416 ..c -rwxr-xr-x root     root
/mnt/hdc1/winnt/system32/spool/drivers/w32x86/3/hpc4500u.dll
  35613 ..c -rwxr-xr-x root     root
/mnt/hdc1/winnt/system32/spool/drivers/w32x86/3/hplj4000.gpd
  13220 ..c -rwxr-xr-x root     root
/mnt/hdc1/winnt/system32/spool/drivers/w32x86/3/hplj5si.hlp
```

- The system is configured for an HP LaserJet printer.

Apr 24 2002 13:46:30

```
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/aim95
```

- AOL Instant Messenger is installed. This is odd because the AOL log file shows it was installed April 4 2002. It is possible AOL IM was either upgraded or reinstalled.

Jun 21 2002 9:30:13

- C:\WINNT\dasetup.log contained the install log of Microsoft Access Data Components version 2.6, installed 6/21/2002 at 9:30am.

Sep 27 2002 12:42:08

```
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/EnCase
```

- EnCase is installed.

Sep 27 2002 14:35:46

```
   8192 ..c drwxr-xr-x root     root     /mnt/hdc2/WriteBlocker
```

Sep 27 2002 14:35:48

```
   8192 ma. drwxr-xr-x root     root     /mnt/hdc2/WriteBlocker
```

Sep 27 2002 14:39:30

```
   8192 ..c drwxr-xr-x root     root     /mnt/hdc2/WriteBlocker/Drivers
 160880 ..c -rwxr-xr-x root     root     /mnt/hdc2/WriteBlocker/Drivers/ntwbfs.sys
```

- WriteBlocker is copied to the EVIDENCE partition.

Sep 30 2002 17:20:50

```
    494 ..c -rwxr-xr-x root     root     /mnt/hdc1/Documents and Settings/A
User/Recent/sp3express.lnk
```

Sep 30 2002 17:22:54

```
  30160 ..c -rwxr-xr-x root     root
/mnt/hdc1/winnt/ServicePackFiles/i386/compobj.dll
  16113 ..c -rwxr-xr-x root     root
/mnt/hdc1/winnt/ServicePackFiles/i386/dsclient.hlp
.................
```

- Windows 2000 Service Pack 3 is installed.

Nov 06 2002 11:35:14

```
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/WriteBlocker
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/WriteBlocker/Drivers
```

- WriteBlocker is installed.

Nov 20 2002 09:51:12

```
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/dtSearch
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/dtSearch/bin
```

- dtSearch is installed.

```
Dec 16 2002 09:29:52
    701 ..c -rwxr-xr-x root     root     /mnt/hdc1/Documents and Settings/All
Users/Desktop/Forensic Toolkit.lnk
```

- Forensic Toolkit is installed.

```
Jan 10 2003 05:30:34
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/ILook
```

- ILook is installed.

```
Jan 10 2003 00:27:28
   8192 ..c drwxr-xr-x root     root     /mnt/hdc2/R-Linux
Jan 10 2003 00:27:36
   8192 ..c drwxr-xr-x root     root     /mnt/hdc2/R-Studio Demo
```

- R-Linux tools are copied to the EVIDENCE partition.

```
Jan 10 2003 05:31:26
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/RTToolsLinux
```

- R-Linux tools are installed.

```
Jan 24 2003 09:06:20
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/Adaptec/DirectCD
```

- Adaptec DirectCD software is added.

```
Jan 24 2003 10:09:02
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/Program Files/Smart Cam
```

- Smart Cam software is installed. There were also a group of .jpg images and thumbnails created about an hour after this.

```
Mar 14 2003 14:49:16
  60688 ..c -rwxr-xr-x root     root     /mnt/hdc1/winnt/system32/remote.exe
```

- Remote from NT Resource Kit found in WinNT system directory.

```
Mar 14 2003 14:51:10
    831 ..c -rwxr-xr-x root     root     /mnt/hdc1/Documents and Settings/All
Users/Application Data/Microsoft/Crypto/rsa/s-1-5-
18/d42cc0c3858a58db2db37658219e6400_86e541d4-4431-4df4-87be-b86271056ee4
    326 ..c -rwxr-xr-x root     root     /mnt/hdc1/winnt/Tasks/At1.job
Mar 14 2003 14:51:12
    831 ma. -rwxr-xr-x root     root     /mnt/hdc1/Documents and Settings/All
Users/Application Data/Microsoft/Crypto/rsa/s-1-5-
18/d42cc0c3858a58db2db37658219e6400_86e541d4-4431-4df4-87be-b86271056ee4
Mar 14 2003 14:52:00
 102616 ..c -rwxr-xr-x root     root     /mnt/hdc1/winnt/Temp/reme.tmp
Mar 14 2003 14:52:02
    326 ma. -rwxr-xr-x root     root     /mnt/hdc1/winnt/Tasks/At1.job

 102616 ma. -rwxr-xr-x root     root     /mnt/hdc1/winnt/Temp/reme.tmp
Mar 14 2003 14:52:06
1048576 ma. -rwxr-xr-x root     root     /mnt/hdc1/winnt/security/edb.log
```

- Some files possibly related to Remote are created.

```
Mar 14 2003 14:55:28
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/vnc
Mar 14 2003 14:55:30
  32768 ma. drwxr-xr-x root     root     /mnt/hdc1/vnc
Mar 14 2003 14:56:16
  11776 ..c -rwxr-xr-x root     root     /mnt/hdc1/vnc/VNCHooks.dll
 161280 ..c -rwxr-xr-x root     root     /mnt/hdc1/vnc/WinVNC.exe
  71168 ..c -rwxr-xr-x root     root     /mnt/hdc1/vnc/omnithread_rt.dll
  68880 ..c -rwxr-xr-x root     root     /mnt/hdc1/vnc/regini.exe
    138 ..c -rwxr-xr-x root     root     /mnt/hdc1/vnc/vnc.ini

- WinVNC is installed.  Unfortunately I could not pinpoint the exact last time WinVNC.exe
was executed because of the FAT16 file system.  The evidence in the log files will have
to suffice.

Mar 14 2003 15:08:46
  32768 ..c drwxr-xr-x root     root     /mnt/hdc1/lsadump
    787 ..c -rwxr-xr-x root     root     /mnt/hdc1/lsadump/DISCLAIMER
   2379 ..c -rwxr-xr-x root     root     /mnt/hdc1/lsadump/README.html
   9655 ..c -rwxr-xr-x root     root     /mnt/hdc1/lsadump/dumplsa.c
  36864 ..c -rwxr-xr-x root     root     /mnt/hdc1/lsadump/dumplsa.dll
   4111 ..c -rwxr-xr-x root     root     /mnt/hdc1/lsadump/dumplsa.dsp
   3442 ..c -rwxr-xr-x root     root     /mnt/hdc1/lsadump/getpid.c
  10074 ..c -rwxr-xr-x root     root     /mnt/hdc1/lsadump/lsadump2.c
   4353 ..c -rwxr-xr-x root     root     /mnt/hdc1/lsadump/lsadump2.dsp
  32768 ..c -rwxr-xr-x root     root     /mnt/hdc1/lsadump/lsadump2.exe
   1622 ..c -rwxr-xr-x root     root     /mnt/hdc1/lsadump/lsadump2.h

- LSADump2 is installed.  Again, without access times I could not determine the last time
lsadump2 was run.

Mar 14 2003 15:10:38
      0 ..c -rwxr-xr-x root     root     /mnt/hdc1/Documents and Settings/A User/My
Documents/Security/Database/sct10.tmp
1056768 ..c -rwxr-xr-x root     root     /mnt/hdc1/winnt/security/tmp.edb
Mar 14 2003 15:10:40
      0 ma. -rwxr-xr-x root     root     /mnt/hdc1/Documents and Settings/A User/My
Documents/Security/Database/sct10.tmp
    311 ma. -rwxr-xr-x root     root     /mnt/hdc1/winnt/system32/GroupPolicy/gpt.ini

- Security policies are possibly altered.

Mar 14 2003 17:25:28
   1024 ma. -rwxr-xr-x root     root     /mnt/hdc1/winnt/system32/config/system.alt

- The last files are modified, marking the last time the system was used.
```

Deleted File Recovery

To aid in my attempt at recovering any deleted files, I installed the Autopsy Forensic Browser, which is part of the @stake Sleuth Kit (TASK). Autopsy is a powerful UNIX tool that can be used to examine MAC times, recover deleted files, and perform string searches. It operates by creating a browser-based interface through your localhost (or remotely if necessary) that you can point and click through a web browser.

Upon running Autopsy on my localhost, I obtained a list of thousands of deleted files on the boot partition mounted on /mnt/hdc1. I quickly realized that most of the file listings were just dead file entries still lingering around in the FAT. From this I was able to get a good look at some more history of the system, as I noticed old links to temporary system files, installation files, many Internet caches, and other files with short life spans. I also found links to what could likely have been former exploits residing on the system. In particular, I found a directory link "_wdump2\" and executable "_wdump2.exe". Pwdump is a common tool for extracting password hashes. I was not able to extract the data for these files as it had been overwritten.

Overall, it was difficult to figure out which file entries led to deleted files that were still intact and which ones led to overwritten data; very comparable to trying to find a needle in a haystack. This could be attributed to the nature of the FAT16 partition. FAT deleted files are recoverable if you know what you're looking for, but no tool can list for the examiner which ones are actually recoverable on a FAT16 drive.

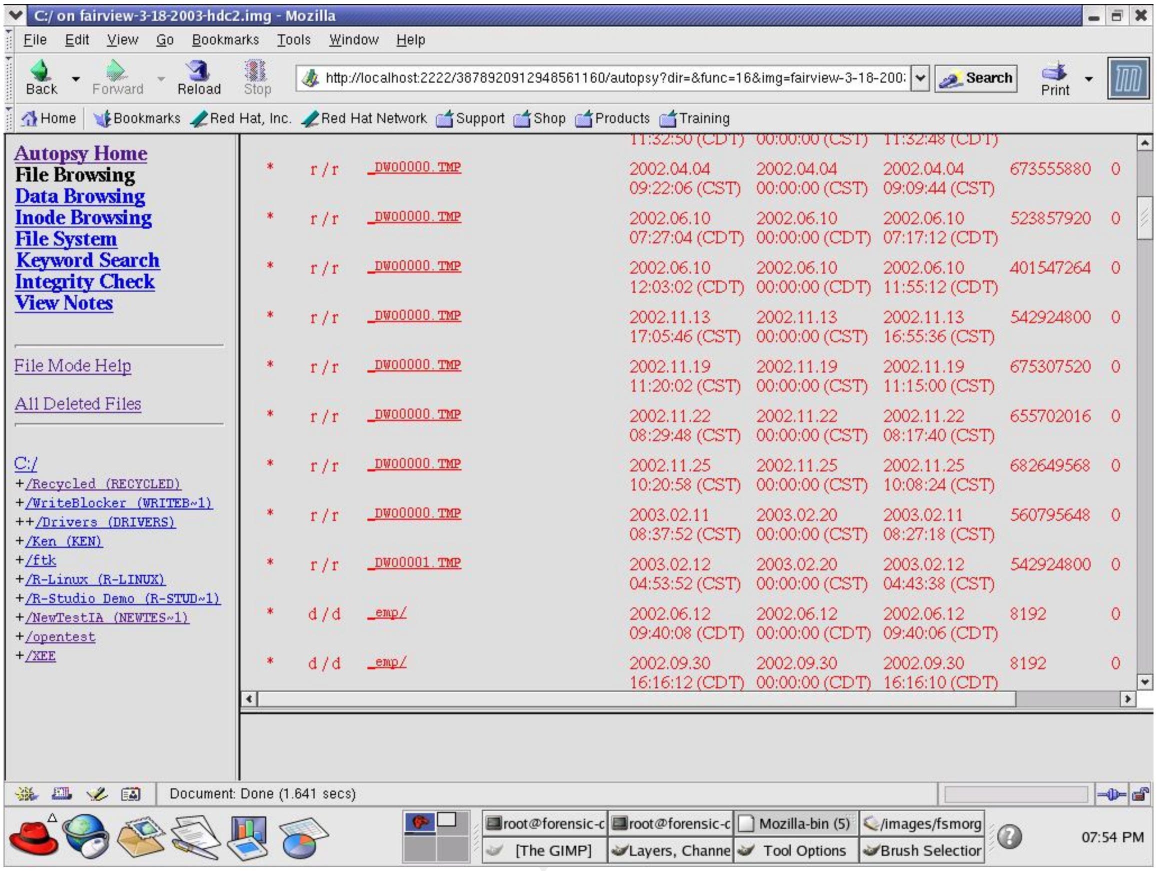
I checked the lsadump and winvnc directories for deleted files but came up empty.

The Recycle Bin, which technically doesn't contain any deleted files but rather files that have been moved and renamed, contained only one directory and no files:

C:\Dc1\Express\CD_ROM\DiskImages\

The root directory was renamed Dc1 because of the naming convention of Recycle Bin. "D" stands for Deleted, "c" is the drive letter the file or directory came from, and "1" is the index number Windows uses to look up what the file's former name was. I was a little disappointed by the lack of files residing here, but I figured the Recycle Bin would have to be emptied quite often by a user whose system was always low on disk space, as the system log history suggested.

I checked the other partition hoping to find some other deleted information. Unfortunately, the EVIDENCE drive did not appear to have gotten a lot of use in the past. There were only about 200 deleted file entries on the whole partition, which was nearly insignificant compared to the activity on the boot partition. The Recycle Bin was empty. However, I was able to find traces of some extremely large .tmp files. The file sizes for some of these files were as large as 650 MB – evidence that these files were originally stored on CD-ROM. Since I had also found a copy of R-Linux on this drive, and I had remembered seeing a large amount of UNIX-related data when I glanced at the partition with WinHex at the beginning of my analysis, I figured these files used to be image copies of a Linux partition:



			11:32:50 (CDT)	00:00:00 (CST)	11:32:48 (CDT)		
*	r / r	_DW00000.TMP	2002.04.04 09:22:06 (CST)	2002.04.04 00:00:00 (CST)	2002.04.04 09:09:44 (CST)	673555880	0
*	r / r	_DW00000.TMP	2002.06.10 07:27:04 (CDT)	2002.06.10 00:00:00 (CDT)	2002.06.10 07:17:12 (CDT)	523857920	0
*	r / r	_DW00000.TMP	2002.06.10 12:03:02 (CDT)	2002.06.10 00:00:00 (CDT)	2002.06.10 11:55:12 (CDT)	401547264	0
*	r / r	_DW00000.TMP	2002.11.13 17:05:46 (CST)	2002.11.13 00:00:00 (CST)	2002.11.13 16:55:36 (CST)	542924800	0
*	r / r	_DW00000.TMP	2002.11.19 11:20:02 (CST)	2002.11.19 00:00:00 (CST)	2002.11.19 11:15:00 (CST)	675307520	0
*	r / r	_DW00000.TMP	2002.11.22 08:29:48 (CST)	2002.11.22 00:00:00 (CST)	2002.11.22 08:17:40 (CST)	655702016	0
*	r / r	_DW00000.TMP	2002.11.25 10:20:58 (CST)	2002.11.25 00:00:00 (CST)	2002.11.25 10:08:24 (CST)	682649568	0
*	r / r	_DW00000.TMP	2003.02.11 08:37:52 (CST)	2003.02.20 00:00:00 (CST)	2003.02.11 08:27:18 (CST)	560795648	0
*	r / r	_DW00001.TMP	2003.02.12 04:53:52 (CST)	2003.02.20 00:00:00 (CST)	2003.02.12 04:43:38 (CST)	542924800	0
*	d / d	_emp/	2002.06.12 09:40:08 (CDT)	2002.06.12 00:00:00 (CDT)	2002.06.12 09:40:06 (CDT)	8192	0
*	d / d	_emp/	2002.09.30 16:16:12 (CDT)	2002.09.30 00:00:00 (CDT)	2002.09.30 16:16:10 (CDT)	8192	0

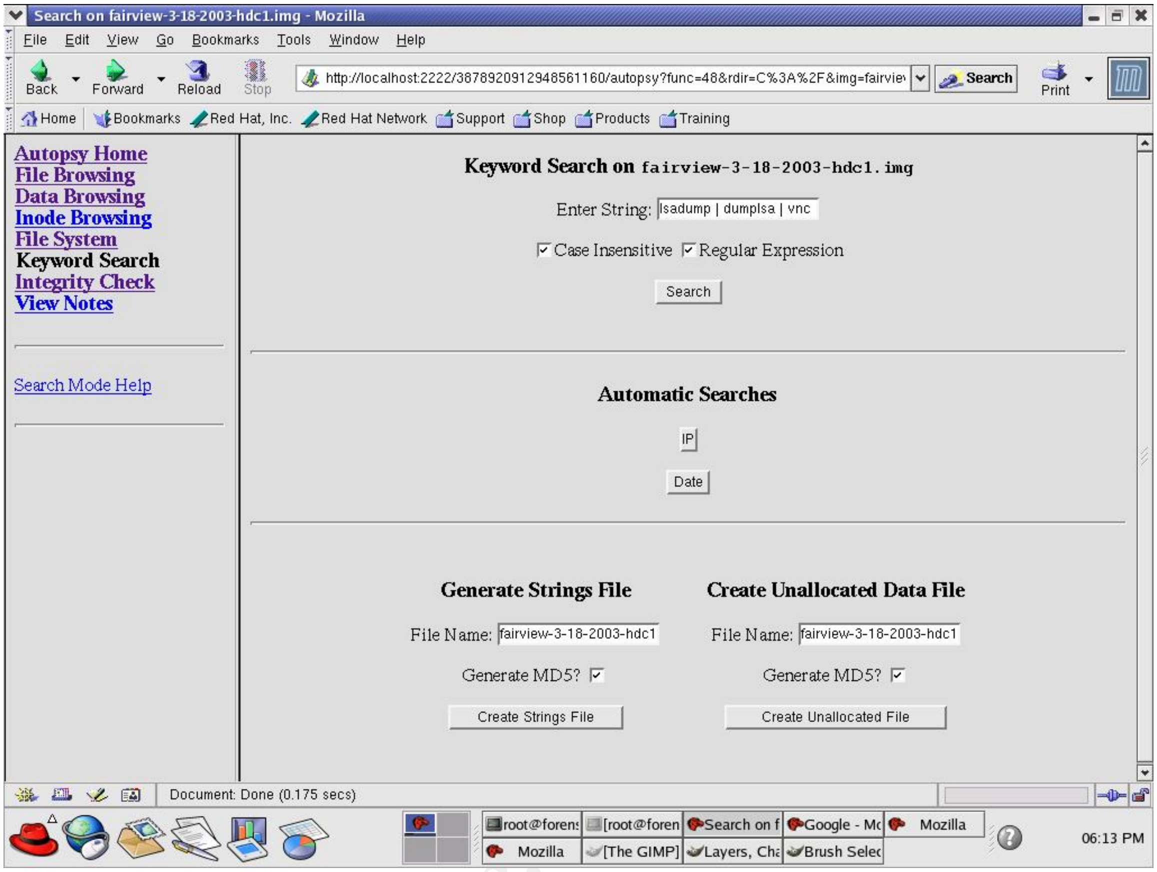
Finally, I created a small timeline with Autopsy to look for any deleted files around the time of the demonstration. I managed to locate some .tmp files deleted by the system but nothing that looked to be related to VNC, remote, or lsadump.

String Searches

One very useful aspect of Autopsy is its ability to perform **grep**-style string searches. It can even search through the slack space of an image. From the information I had gathered up to this point, I felt that the following keywords might lead to something interesting on this system:

Lsadump
dumplsa
vnc
Pwdump
Sqlserver
Larry

I was able to perform a search on all keywords at once by concatenating them together: “lsadump | dumplsa | vnc | pwdump | sqlserver | larry”. The search was case insensitive.



Search on fairview-3-18-2003-hdc1.img - Mozilla

http://localhost:2222/38789209129485611 60/autopsy?func=4&&rdir=C%3A%2F&img=fairviev

Keyword Search on `fairview-3-18-2003-hdc1.img`

Enter String: lsadump | dumplsa | vnc

☑ Case Insensitive ☑ Regular Expression

Automatic Searches

Generate Strings File

File Name: fairview-3-18-2003-hdc1

Generate MD5? ☑

Create Unallocated Data File

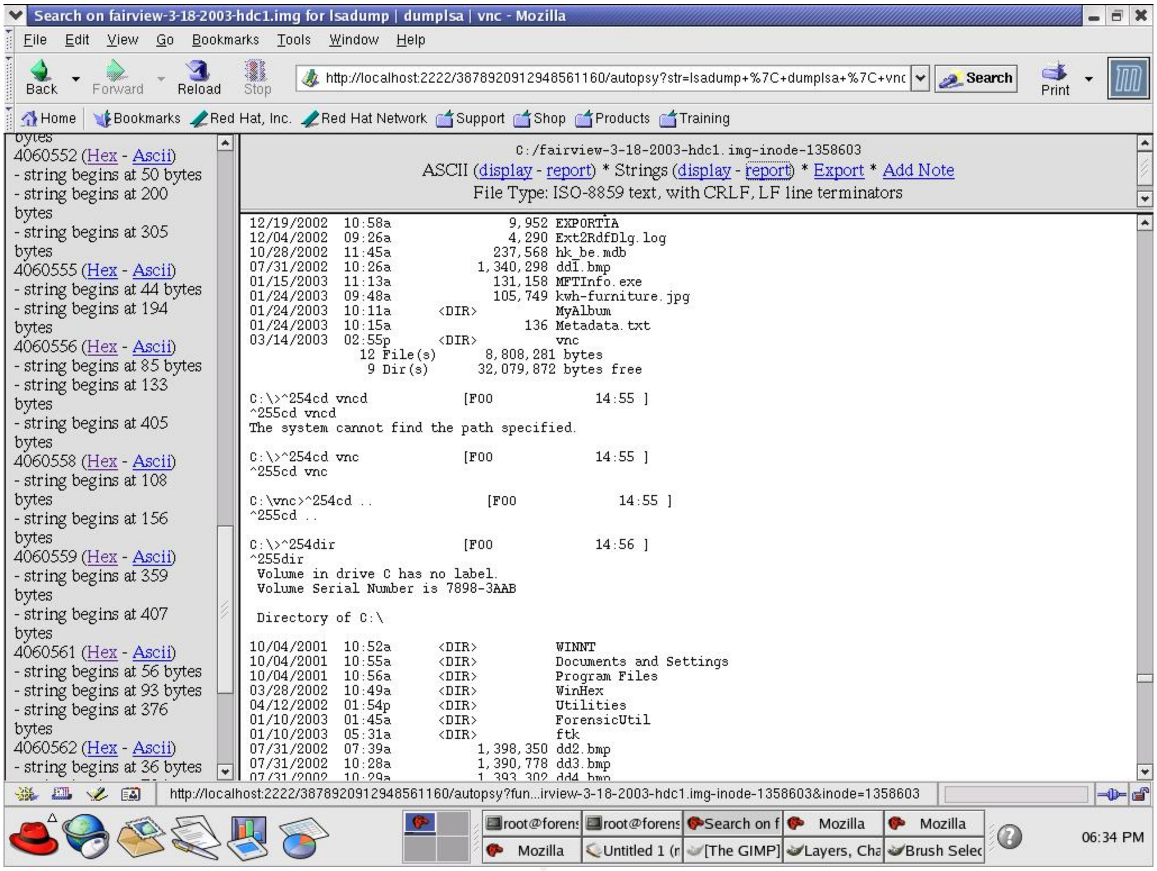
File Name: fairview-3-18-2003-hdc1

Generate MD5? ☑

Document: Done (0.175 secs)

The results of the first search produced an overwhelming number of results for the keyword “larry”. Apparently “Larry” had been the one using R-Linux as his name appeared all over the EVIDENCE partition, as well as the boot partition.

To shorten my results list, I removed “larry” and ran again. This time I was able to locate the winvnc.exe executable, and lsadump came up in some of the .c files, which was expected. As I scrolled down the list I also found actual command prompt listings of the workstation FOO running WinVNC and lsadump in C:\Winnt\temp\REME.tmp:


Search on fairview-3-18-2003-hdc1.img for lsadump | dumplsa | vnc - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://localhost:2222/38789209129485611 60/autopsy?str=lsadump+%7C+dumplsa+%7C+vnc
Search
Print
Home Bookmarks Red Hat, Inc. Red Hat Network Support Shop Products Training
http://localhost:2222/38789209129485611 60/autopsy?fun...irview-3-18-2003-hdc1.img-inode-1358603&inode=1358603
root@forens root@forens Search on f Mozilla Mozilla
Mozilla Untitled 1 (r [The GIMP] Layers, Cha Brush Selec
06:34 PM

```
bytes
4060552 (Hex - Ascii)
- string begins at 50 bytes
- string begins at 200
bytes
- string begins at 305
bytes
4060555 (Hex - Ascii)
- string begins at 44 bytes
- string begins at 194
bytes
4060556 (Hex - Ascii)
- string begins at 85 bytes
- string begins at 133
bytes
- string begins at 405
bytes
4060558 (Hex - Ascii)
- string begins at 108
bytes
- string begins at 156
bytes
4060559 (Hex - Ascii)
- string begins at 359
bytes
- string begins at 407
bytes
4060561 (Hex - Ascii)
- string begins at 56 bytes
- string begins at 93 bytes
- string begins at 376
bytes
4060562 (Hex - Ascii)
- string begins at 36 bytes
```

C:/fairview-3-18-2003-hdc1.img-inode-1358603
ASCII (display - report) * Strings (display - report) * Export * Add Note
File Type: ISO-8859 text, with CRLF, LF line terminators

```
12/19/2002  10:58a               9,952 EXPORTIA
12/04/2002  09:26a               4,290 Ext2RdfDlg.log
10/28/2002  11:45a             237,568 hk_be.mdb
07/31/2002  10:26a           1,340,298 dd1.bmp
01/15/2003  11:13a             131,158 MFTInfo.exe
01/24/2003  09:48a             105,749 kwh-furniture.jpg
01/24/2003  10:11a      <DIR>          MyAlbum
01/24/2003  10:15a                 136 Metadata.txt
03/14/2003  02:55p      <DIR>          vnc
              12 File(s)      8,808,281 bytes
               9 Dir(s)      32,079,872 bytes free

C:\>^254cd vncd            [F00            14:55 ]
^255cd vncd
The system cannot find the path specified.

C:\>^254cd vnc             [F00            14:55 ]
^255cd vnc

C:\vnc>^254cd ..              [F00            14:55 ]
^255cd ..

C:\>^254dir                [F00            14:56 ]
^255dir
 Volume in drive C has no label.
 Volume Serial Number is 7898-3AAB

 Directory of C:\

10/04/2001  10:52a      <DIR>          WINNT
10/04/2001  10:55a      <DIR>          Documents and Settings
10/04/2001  10:56a      <DIR>          Program Files
03/28/2002  10:49a      <DIR>          WinHex
04/12/2002  01:54p      <DIR>          Utilities
01/10/2003  01:45a      <DIR>          ForensicUtil
01/10/2003  05:31a      <DIR>          ftk
07/31/2002  07:39a           1,398,350 dd2.bmp
07/31/2002  10:28a           1,390,778 dd3.bmp
```

```
C:\WINNT\system32>þipconfig           [FOO            14:52 ]
ÿipconfig
 Windows 2000 IP Configuration  Ethernet adapter Local Area Connection 2:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.5.76     Subnet Mask . . . . . . . . .
. . : 255.255.255.0    Default Gateway . . . . . . . . . : 192.168.5.1
C:\WINNT\system32>þcd ..              [FOO            14:53 ]
ÿcd ..



C:\>þmkdir vnc           [FOO            14:55 ]
ÿmkdir vnc

C:\>þdir                 [FOO            14:55 ]
ÿdir
 Volume in drive C has no label.
 Volume Serial Number is 7898-3AAB

 Directory of C:\

10/04/2001  10:52a      <DIR>          WINNT
10/04/2001  10:55a      <DIR>          Documents and Settings
10/04/2001  10:56a      <DIR>          Program Files
03/28/2002  10:49a      <DIR>          WinHex
04/12/2002  01:54p      <DIR>          Utilities
01/10/2003  01:45a      <DIR>          ForensicUtil
01/10/2003  05:31a      <DIR>          ftk
07/31/2002  07:39a           1,398,350 dd2.bmp
07/31/2002  10:28a           1,390,778 dd3.bmp
07/31/2002  10:29a           1,393,302 dd4.bmp
07/31/2002  10:31a           1,398,350 dd5.bmp
07/31/2002  10:32a           1,398,350 dd6.bmp
12/19/2002  10:58a               9,952 EXPORTIA
```

```
12/04/2002  09:26a               4,290 Ext2RdfDlg.log
10/28/2002  11:45a             237,568 hk_be.mdb
07/31/2002  10:26a           1,340,298 dd1.bmp
01/15/2003  11:13a             131,158 MFTInfo.exe
01/24/2003  09:48a             105,749 kwh-furniture.jpg
01/24/2003  10:11a      <DIR>          MyAlbum
01/24/2003  10:15a                 136 Metadata.txt
03/14/2003  02:55p      <DIR>          vnc
              12 File(s)      8,808,281 bytes
               9 Dir(s)      32,079,872 bytes free

C:\>þcd vncd            [FOO             14:55 ]
ÿcd vncd
The system cannot find the path specified.

C:\>þcd vnc             [FOO             14:55 ]
ÿcd vnc

C:\vnc>þcd ..              [FOO             14:55 ]
ÿcd ..

C:\>þdir                [FOO             14:56 ]
ÿdir
 Volume in drive C has no label.
 Volume Serial Number is 7898-3AAB

 Directory of C:\

10/04/2001  10:52a      <DIR>          WINNT
10/04/2001  10:55a      <DIR>          Documents and Settings
10/04/2001  10:56a      <DIR>          Program Files
03/28/2002  10:49a      <DIR>          WinHex
04/12/2002  01:54p      <DIR>          Utilities
01/10/2003  01:45a      <DIR>          ForensicUtil
01/10/2003  05:31a      <DIR>          ftk
07/31/2002  07:39a           1,398,350 dd2.bmp
07/31/2002  10:28a           1,390,778 dd3.bmp
07/31/2002  10:29a           1,393,302 dd4.bmp
07/31/2002  10:31a           1,398,350 dd5.bmp
07/31/2002  10:32a           1,398,350 dd6.bmp
12/19/2002  10:58a               9,952 EXPORTIA
12/04/2002  09:26a               4,290 Ext2RdfDlg.log
10/28/2002  11:45a             237,568 hk_be.mdb
07/31/2002  10:26a           1,340,298 dd1.bmp
01/15/2003  11:13a             131,158 MFTInfo.exe
01/24/2003  09:48a             105,749 kwh-furniture.jpg
01/24/2003  10:11a      <DIR>          MyAlbum
01/24/2003  10:15a                 136 Metadata.txt
03/14/2003  02:55p      <DIR>          vnc
              12 File(s)      8,808,281 bytes
               9 Dir(s)      31,653,888 bytes free

C:\>þcd vnc             [FOO             14:56 ]
ÿcd vnc

C:\vnc>þdir                [FOO             14:56 ]
ÿdir
 Volume in drive C has no label.
 Volume Serial Number is 7898-3AAB

 Directory of C:\vnc

03/14/2003  02:55p      <DIR>          .
03/14/2003  02:55p      <DIR>          ..
05/18/1998  06:24a              71,168 omnithread_rt.dll
02/29/1996  08:00p              68,880 REGINI.EXE
01/31/2001  04:53p                 138 vnc.ini
05/18/1998  06:24a              11,776 VNCHooks.dll
05/18/1998  06:28a             161,280 WinVNC.exe
               5 File(s)        313,242 bytes
               2 Dir(s)      31,653,888 bytes free
```

```
C:\vnc>þcd ..              [FOO             14:56 ]
ÿcd ..

C:\>þcd vnc             [FOO             14:57 ]
ÿcd vnc

C:\vnc>þnet start winvnc    [FOO             14:57 ]
ÿnet start winvnc
The service name is invalid.
More help is available by typing NET HELPMSG 2185.

C:\vnc>þnet start winvnc    [FOO             14:57 ]
ÿnet start winvnc
The service name is invalid.
More help is available by typing NET HELPMSG 2185.

C:\vnc>þdir                [FOO             14:57 ]
ÿdir
 Volume in drive C has no label.
 Volume Serial Number is 7898-3AAB

 Directory of C:\vnc

03/14/2003  02:55p      <DIR>          .
03/14/2003  02:55p      <DIR>          ..
05/18/1998  06:24a              71,168 omnithread_rt.dll
02/29/1996  08:00p              68,880 REGINI.EXE
01/31/2001  04:53p                 138 vnc.ini
05/18/1998  06:24a              11,776 VNCHooks.dll
05/18/1998  06:28a             161,280 WinVNC.exe
               5 File(s)        313,242 bytes
               2 Dir(s)      31,653,888 bytes free

C:\vnc>þnet start WinVNC    [FOO             14:58 ]
ÿnet start WinVNC
The service name is invalid.
More help is available by typing NET HELPMSG 2185.

C:\vnc>þdir                [FOO             14:58 ]
ÿdir
 Volume in drive C has no label.
 Volume Serial Number is 7898-3AAB

 Directory of C:\vnc

03/14/2003  02:55p      <DIR>          .
03/14/2003  02:55p      <DIR>          ..
05/18/1998  06:24a              71,168 omnithread_rt.dll
02/29/1996  08:00p              68,880 REGINI.EXE
01/31/2001  04:53p                 138 vnc.ini
05/18/1998  06:24a              11,776 VNCHooks.dll
05/18/1998  06:28a             161,280 WinVNC.exe
               5 File(s)        313,242 bytes
               2 Dir(s)      31,653,888 bytes free

C:\vnc>þnet start winvnc    [FOO             14:58 ]
ÿnet start winvnc
The service name is invalid.
More help is available by typing NET HELPMSG 2185.

C:\vnc>þwinvnc -install    [FOO             14:58 ]
ÿwinvnc -install

C:\vnc>þnet start winvnc    [FOO             14:58 ]
ÿnet start winvnc
The service name is invalid.
More help is available by typing NET HELPMSG 2185.

C:\vnc>þnet start winvnc    [FOO             14:58 ]
ÿnet start winvnc
```

```
The VNC Server service is starting.
The VNC Server service was started successfully.

C:\vnc>þtlist              [FOO             15:01 ]
ÿtlist
'tlist' is not recognized as an internal or external command,
operable program or batch file.

C:\vnc>þnet stop winvnc    [FOO             15:01 ]
ÿnet stop winvnc
The VNC Server service is not started.
More help is available by typing NET HELPMSG 3521.

C:\vnc>þnet start winvnc    [FOO             15:01 ]
ÿnet start winvnc
The VNC Server service is starting.
The VNC Server service was started successfully.

C:\vnc>þcd ..              [FOO             15:08 ]
ÿcd ..

C:\>þdir                [FOO             15:08 ]
ÿdir
 Volume in drive C has no label.
 Volume Serial Number is 7898-3AAB

 Directory of C:\

10/04/2001  10:52a      <DIR>          WINNT
10/04/2001  10:55a      <DIR>          Documents and Settings
10/04/2001  10:56a      <DIR>          Program Files
03/28/2002  10:49a      <DIR>          WinHex
04/12/2002  01:54p      <DIR>          Utilities
01/10/2003  01:45a      <DIR>          ForensicUtil
01/10/2003  05:31a      <DIR>          ftk
07/31/2002  07:39a           1,398,350 dd2.bmp
07/31/2002  10:28a           1,390,778 dd3.bmp
07/31/2002  10:29a           1,393,302 dd4.bmp
07/31/2002  10:31a           1,398,350 dd5.bmp
07/31/2002  10:32a           1,398,350 dd6.bmp
12/19/2002  10:58a               9,952 EXPORTIA
12/04/2002  09:26a               4,290 Ext2RdfDlg.log
10/28/2002  11:45a             237,568 hk_be.mdb
07/31/2002  10:26a           1,340,298 dd1.bmp
01/15/2003  11:13a             131,158 MFTInfo.exe
01/24/2003  09:48a             105,749 kwh-furniture.jpg
01/24/2003  10:11a      <DIR>          MyAlbum
01/24/2003  10:15a                 136 Metadata.txt
03/14/2003  02:55p      <DIR>          vnc
03/14/2003  03:08p      <DIR>          lsadump
              12 File(s)      8,808,281 bytes
              10 Dir(s)      31,260,672 bytes free

C:\>þcd lsadump         [FOO             15:08 ]
ÿcd lsadump

C:\lsadump>þdir                [FOO             15:08 ]
ÿdir
 Volume in drive C has no label.
 Volume Serial Number is 7898-3AAB

 Directory of C:\lsadump

03/14/2003  03:08p      <DIR>          .
03/14/2003  03:08p      <DIR>          ..
04/06/2000  07:48p                 787 DISCLAIMER
03/29/2000  03:18p               9,655 dumplsa.c
03/29/2000  03:19p              36,864 dumplsa.dll
03/29/2000  03:18p               4,111 dumplsa.dsp
03/29/2000  03:18p               3,442 getpid.c
03/29/2000  03:18p              10,074 lsadump2.c
```

```
03/29/2000  03:18p               4,353 lsadump2.dsp
03/29/2000  03:19p              32,768 lsadump2.exe
03/29/2000  03:18p               1,622 lsadump2.h
04/06/2000  07:48p               2,379 README.html
              10 File(s)        106,055 bytes
               2 Dir(s)      31,260,672 bytes free

C:\lsadump>þlsadump2           [FOO             15:09 ]
ÿlsadump2
DefaultPassword
DPAPI_SYSTEM
 01 00 00 00 76 8E 86 EA 0A 13 C9 9D 3A 21 B5 EB  ....v.......:!..
 ED 74 21 06 CA 46 AF 9C 57 76 0D 69 03 AA 06 75  .t!..F..Wv.i...u
 A0 12 A9 EE 35 5B F3 04 FD 06 8E 52              ....5[.....R
SAC
 02 00 00 00                                      ....
SAI
 02 00 00 00                                      ....
XATM:a19ef4bc-42b6-4a29-ba94-c6e921ccd82f
 A0 00 49 00 17 00 2E 00 D3 00 39 00 1A 00 B2 00  ..I.......9.....
 BF 00 5A 00 52 01 79 00 6B 00 AA 00 53 00 4C 00  ..Z.R.y.k...S.L.
 2A 00 CE 00 69 00 C8 00 3B 00 3D 00 F2 00 B9 00  *...i...;.=.....
 18 20 64 00 1F 00 3F 00 1F 00 D8 00 77 00 CD 00  . d...?.....w...
 30 20 B1 00 EC 00 30 20 B7 00 1D 00 EF 00 D6 00  0 ....0 ........
 2F 00 11 00 2A 00 50 00 C4 00 30 00 B4 00 02 00  /...*.P...0.....
 1F 00 11 00 E7 00 51 00 CA 00 2B 00 33 00 7D 01  ......Q...+.3.}.
 76 00 72 00 38 00 AA 00 C8 00 58 00 C7 00 B3 00  v.r.8.....X.....
 B7 00 17 00 EE 00 02 00 BA 00 56 00 75 00 DF 00  ..........V.u...
 FF 00 F0 00 F9 00 25 00 3E 00 52 01 11 00 51 00  ......%.>.R...Q.
 22 20 FD 00 10 00 1D 00 EF 00 AF 00 5B 00 E7 00  " ..........[...
 56 00 09 00 3E 00 E6 00 1A 00 C4 00 65 00 3B 00  V...>.......e.;.
 7D 00 6F 00 16 00 08 00 76 00 EB 00 62 00 CA 00  }.o.....v...b...
 76 00 C2 00 68 00 DB 00 5E 00 AD 00 2F 00 AD 00  v...h...^.../...
 A0 00 02 00 ED 00 C0 00 28 00 5B 00 CD 00 14 00  ........(.[.....
 B4 00 F5 00 C8 00 A1 00 48 00 3A 00 EC 00 E5 00  ........H.:.....
 E7 00 D2 00 0E 00 13 00 53 01 18 20 AC 00 49 00  ........S.. ..I.
 BB 00 E7 00 68 00 34 00 9D 00 BD 00 AF 00 79 00  ....h.4.......y.
 6C 00 47 00 5A 00 65 00 5E 00 42 00 30 20 69 00  l.G.Z.e.^.B.0 i.
 59 00 ED 00 62 00 3A 20 6F 00 F1 00 63 00 FD 00  Y...b.: o...c...
 11 00 0F 00 CA 00 09 00 CB 00 EF 00 10 00 5B 00  ..............[.
 78 00 31 00 D4 00 C7 00 11 00 35 00 81 00 2B 00  x.1.......5...+.
 0F 00 30 20 7E 01 BA 00 7A 00 10 00 5B 00 B0 00  ..0 ~...z...[...
 60 00 2B 00 01 00 D1 00 14 00 75 00 20 20 CC 00  `.+.......u.  ..
 30 00 B9 00 20 00 A4 00 81 00 2D 00 09 00 1C 00  0... .....-.....
 F4 00 A0 00 E2 00 3D 00 A8 00 D1 00 21 20 2A 00  ......=.....! *.
 C6 00 EB 00 5A 00 05 00 7D 01 0D 00 01 00 14 00  ....Z...}.......
 39 20 56 00 F7 00 50 00 F2 00 C9 00 F9 00 79 00  9 V...P.......y.
 58 00 24 00 69 00 4F 00 A9 00 F8 00 DE 00 18 20  X.$.i.O........
 1F 00 58 00 F1 00 7E 01 E8 00 4C 00 22 21 1F 00  ..X...~...L."!..
 52 00 4E 00 D9 00 05 00 A5 00 77 00 20 20 11 00  R.N.......w.  ..
 24 00 11 00 12 00 6F 00 E4 00 51 00 D7 00 1A 20  $.....o...Q....

C:\lsadump>þcd ..              [FOO             15:10 ]
ÿcd ..

C:\>þrmdir lsadump      [FOO             15:10 ]
ÿrmdir lsadump
The directory is not empty.

C:\>þrmdir /F lsadump    [FOO             15:10 ]
ÿrmdir /F lsadump
Invalid switch - "F".

C:\>þrmdir              [FOO             15:10 ]
ÿrmdir
The syntax of the command is incorrect.

C:\>þrmdir ?            [FOO             15:10 ]
ÿrmdir ?
The filename, directory name, or volume label syntax is incorrect.
```

```
C:\>þcls                [FOO             15:10 ]
ÿcls


C:\>þclear              [FOO             15:10 ]
ÿclear
'clear' is not recognized as an internal or external command,
operable program or batch file.

C:\>þnet stop vnc       [FOO             15:11 ]
ÿnet stop vnc
System error 1060 has occurred.
The specified service does not exist as an installed service.

C:\>þwinvnc -remove     [FOO             15:11 ]
ÿwinvnc -remove
'winvnc' is not recognized as an internal or external command,
operable program or batch file.

C:\>þtlist              [FOO             15:12 ]
ÿtlist
   0 System Process
   8 System
 184 smss.exe
 212 csrss.exe
 232 winlogon.exe
 260 services.exe
 272 lsass.exe
 456 svchost.exe
 488 spoolsv.exe
 520 svchost.exe
 556 regsvc.exe
 572 MSTask.exe
 596 stisvc.exe
 632 WinMgmt.exe
 652 svchost.exe
 800 Explorer.EXE      Program Manager
 892 directcd.exe
 904 CreateCD.exe
1156 wuauclt.exe
 300 cmd.exe           Command Prompt
 760 remote.exe
 368 cmd.exe
 968 WinVNC.exe
 876 mmc.exe           Local Security Settings
 936 mmc.exe           Event Viewer
 896 TLIST.EXE

C:\>
```

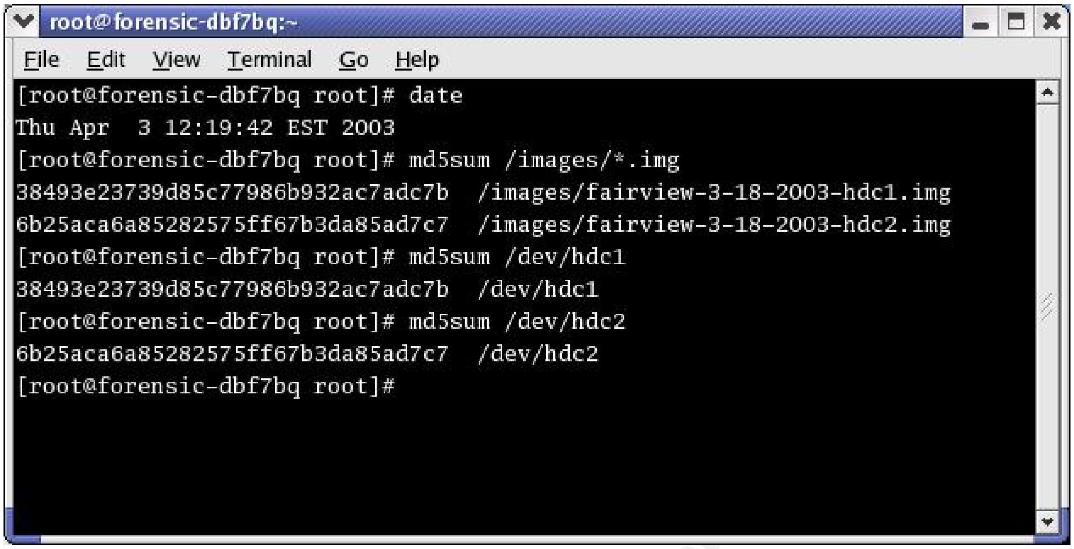
This looked like a forensic examiner's dream come true. Looking back at the log timeline, the attacker from FOO was probably using remote.exe to try and get WinVNC running, and this was a temporary file that was created by remote to hold the contents of any outgoing information. Looking at the file, I was able to verify the multiple attempts to run VNC, and see that the first three attempts did not take. After some initial trouble, the user finally got it working. The lsadump run appears at the bottom of the listing. This file also exposed the reckless habits of the attacker, and it was obvious he was either not trying to run these programs discreetly or not a very skilled NT hacker. Then again, I had to take into account that this was only meant to be a demonstration.

Conclusions

After analysis of the Windows 2000 image I obtained from the IAC lab, I was able to get a general idea of what the machine had been used for in the past. The image contained a FAT16 boot partition and another FAT32 partition labeled "EVIDENCE". The Windows operating system had been installed on October 4, 2001. Since then, several commercial forensic tools had been installed, but judging from deleted files and MAC timeline analysis, none of them were used very frequently. A user named Larry was using the machine at one time to examine Linux images. The EVIDENCE partition remained mostly untouched, and may have been originally created for the sole purpose of having enough disk space to hold the large Linux images. There was some evidence in the form of deleted file entries that the boot partition had been used to study common security risks in the past. The system had also been used as a general web-surfing machine, as evidenced by numerous Internet histories, and thousands of both present and deleted cache/cookie files created over the past 18 months.

I was also able to generate an accurate timeline of the events of March 14, 2003, which was the last time the system was used. A demonstration had been given that afternoon starting around 2:30pm. The demonstration covered the NT Resource Kit tools **remote** and **WinVNC**, as well as **lsadump**. From the MAC timeline evidence, it appeared that the user's main goal was to simply get the tools to work from the workstation FOO. First **remote** was set up, and then **WinVNC** and **lsadump** were run through **remote**. Once the tools were working, there was very little activity afterwards. The user at FOO did not make any reasonable attempt to cover up his tracks, although there was one point during the demonstration where security auditing was turned off for 30 seconds. Due to activity witnessed very close to the time of the demo, the workstation SQLSERVER may have been involved somehow, although it is unclear as to what role it played.

A final md5sum check proved no evidence was modified during the course of the investigation:



```
[root@forensic-dbf7bq root]# date
Thu Apr  3 12:19:42 EST 2003
[root@forensic-dbf7bq root]# md5sum /images/*.img
38493e23739d85c77986b932ac7adc7b  /images/fairview-3-18-2003-hdc1.img
6b25aca6a85282575ff67b3da85ad7c7  /images/fairview-3-18-2003-hdc2.img
[root@forensic-dbf7bq root]# md5sum /dev/hdc1
38493e23739d85c77986b932ac7adc7b  /dev/hdc1
[root@forensic-dbf7bq root]# md5sum /dev/hdc2
6b25aca6a85282575ff67b3da85ad7c7  /dev/hdc2
[root@forensic-dbf7bq root]#
```

References

Logicube. Forensic SF-5000u User's Manual.

RegRun 3 Security Suite. "Specify an order of the startup programs".
URL: http://www.greatis.com/regrun3startuporder.htm. (22 March 2003)

Microsoft TechNet. "Chapter 6 – Auditing and Intrusion Detection".
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/prodtech/windows/windows2000/staysecure/secops06.asp. (22 March 2003)

Microsoft. "How the Recycle Bin Stores Files".
URL: http://support.microsoft.com/?kbid=136517. (22 March 2003)

Posey, Brien M. "Using the Net command in Windows 2000". 20 February 2001.
URL: http://www.shell.linux.se/jake/net_command.html. (22 March 2003)

Where to obtain forensic tools used in the examination:

IRCR was obtained from http://www.incident-response.org/IRCR/htm.

Registrar Lite was obtained from Resplendence Software from http://www.resplendence.com/registry/reglite.htm.

Sniffer was obtained from the SANS System Forensics Track 8 CD.

Mac_daddy was obtained from http://www.incident-response.org/mac_daddy.html.

Autopsy was obtained from http://www.atstake.com/research/tools/autopsy/.

Internet Explorer History Viewer was obtained from the SANS System Forensics Track 8 CD.

Part III: Legal Issues of Incident Handling

For this section of the practical exam, I will assume the role of a system administrator for a public Internet service provider who has recently received a call from a government agent. The agent informs me that one of my user accounts was used to hack into a government system, and he would like me to check my logs for any suspicious activity during the times the system was hacked. From my logs, I can only see that a valid user was logged into his account during the notified times.

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

The answer to this question is basically nothing, assuming the officer is making a quick, informal check-up call. At the most, I can tell him about general activity on my system, but I cannot give away subscriber information, access to user stored content, log details (transactional data), or session information. The Electronic Communications Privacy Act of 1986 (ECPA) protects public system users from having their content and activity being disclosed to the government. Normally, for a government agent to have access to such records, he would have to produce a warrant, subpoena, or court order following ECPA regulations. There are several other exceptions to this rule, and with the hasty introduction of the USA-PATRIOT Act shortly after the events of 9/11/2001, the exceptions have since grown in number and given government officials more flexibility. The details of the ECPA and the USA-PATRIOT Act will be discussed in greater detail later in this section.

The only other way an officer could lawfully obtain this information under the scenario illustrated above were if I had gotten the user's consent beforehand. Since I am running a public ISP, this is most likely not the case. Most ISPs have privacy policies set in place to protect their customers' information from being accessed by others, spread across the web, etc. It can be a serious issue, as AOL demonstrated in 1997 when their violation of their own privacy policy resulted in a U.S. Navy sailor having to face discharge and an ugly publicized court case to follow (Kornblum).

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

The field of computer forensics demands that media evidence be collected as quickly as possible when a possible compromise has been detected. A delay with obtaining the necessary legal authority could prove catastrophic to a case if it results in key evidence being written over, or removed by the hacker in time. Fortunately for law enforcement officials, ISPs are required by law to preserve any requested evidence by whatever means necessary and without a court order, etc., according to 18 U.S.C 2703 (f). In this case, a simple phone call would be enough to request the preservation, although in order to minimize miscommunications, an email or fax request would be better practice.

Government agents must take care when using 18 U.S.C. 2703 (f) to request preservation of evidence. Some ISPs may have certain policies in place that, when put into effect, could tip off the hacker that his activity has been discovered. For example, AOL has a policy that resets a user's password when his email content is preserved. In cases like this, it may be a better idea to simply not make the request.

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

Under the ECPA, 18 U.S.C. 2702 "Voluntary disclosure of customer communications and records" contains the general guidelines for accepting legal authority to disclose evidence. More specifically for this scenario, government officials need to follow the ruling under 18 U.S.C. 2703 "Required disclosure of customer communications and records". In order for a government official to have access to logs or any other records associated with a subscriber or his stored communications without consent of the user, he must comply with the regulations stated in 18 U.S.C 2703(c). According to 2703(c), the official could supply a warrant issued by the court in the related jurisdiction of the investigation or supply an equivalent State warrant. Secondly, he could obtain a court order under the requirements found in 18 U.S.C. 2703(d). Thirdly, if the case is related to telemarketing fraud, he can provide a formal written request for the name, address, and place of business of the subscriber.

Lastly, a government agent can use an administrative subpoena to obtain the user's name, address, records of session times and durations, length of service and type of service used, telephone number or related subscriber identity, and means of payment including credit card numbers and bank accounts. This last exception was significantly modified due to section 210 of the USA-PATRIOT Act, effectively giving government officials a broader set of record types they can have access to. Before the PATRIOT Act was put into effect, government investigators had to obtain a court order before gaining access to a customer's payment information. The change was made to make it easier for the investigator to determine the true identity of the user, as it can sometimes be easy for a hacker to set up accounts under false names.

If the investigator wanted me to provide access to the user's stored content, 18 U.S.C 2703(a) states that in order for a government official to require access to communications that have been stored on an electronic system for less than 180 days, he must supply a warrant issued by the court in the related jurisdiction of the investigation or supply an equivalent State warrant. If the content is more than 180 days old, he can follow the guidelines presented for remote computing services in 18 U.S.C. 2703(b).

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

At this point, I would be at least somewhat concerned with the officer's call. This would prompt me to do some light investigative work. I would probably check the validity of my critical system binaries and check out my logs for suspicious activity. Depending on the situation, I may want to be selective about the tests I run because experienced hackers will be able to monitor what I'm doing and could take actions accordingly.

If I have reason to believe that my system is in potential danger, which is most likely the case here, I can utilize my rights under the Wiretap Act by conducting a surveillance of communications through my system. 18 U.S.C. 2511(2)(a)(i) states that in the case of provider exception, where as the provider I am trying to protect my rights or property in self-defense, I am allowed to perform a wiretap of the accounts relevant to my investigation. When doing this, I must be careful to intercept only communications related to the investigation. The statute does not permit providers to set up unlimited wiretaps. There must be a clear buffer zone with respect to relevant and non-relevant communications.

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

The hacker has committed a crime on my system by trespassing and creating an unauthorized account. According to 18 U.S.C. 1030(a)(5)(A)(i), it is illegal to gain authorized access and intentionally cause the transmission of a program, information, code, or command that will cause damage to a protected system. Also, under the Virginia Computer Crimes Act of 1984, he is in violation of 18.2-152.4(3), which states it is illegal to trespass without authority to alter protected data. With the knowledge that the hacker is suspect to illegal activity, it becomes much easier to get law enforcement officials involved.

I may now disclose to law enforcement officials the suspect's stored data pertaining to his communications with the system. According to 18 U.S.C. 2702(b)(6)(A)(ii), it is lawful to disclose such information if a crime has been committed. 18 U.S.C. 2702(b)(5) strengthens this argument further by stating that I can disclose the communications to protect my system, acting as the ISP.

Also, I can disclose the suspect's customer records to law enforcement. A recent change was made due to the PATRIOT Act where 18 U.S.C. 2702(c)(3) states it is lawful for an ISP to do so if they are protecting their system in self-defense. Government officials still need to comply with the regulations in 18 U.S.C. 2703 before being granted access to customer records, unless somebody could potentially suffer death or serious injury (18 U.S.C. 2702(c)(4)).

Tracking the hacker's actions becomes a lot easier because I can now bring in the help of law enforcement according to the Computer trespasser exception in the Wiretap Act. Under new changes from the PATRIOT Act, section 202, law enforcement can assist with wiretapping if they gain the ISP's consent to do so, they are engaged in the investigation, they have reasonable grounds to believe the intercepted content is related to the investigation, and they limit their wiretaps only to communications relevant to their case (18 U.S.C. 2511(2)(i)(I – IV)).

References

Department of Justice. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations".
URL: http://www.cybercrime.gov/s&smanual2002.htm (15 March 2003)

Department of Justice. "18 U.S.C. 2703. Requirements for Governmental Access".
URL: http://www.usdoj.gov/criminal/cybercrime/usc2703.htm (15 March 2003)

Department of Justice. "Computer Crime and Intellectual Property Section (CCIPS)".
URL: http://www.usdoj.gov/criminal/cybercrime/Patriot_redline.htm (15 March 2003)

Electronic Privacy Information Center. "The USA PATRIOT Act".
URL: http://www.epic.org/privacy/terrorism/usapatriot/ (15 March 2003)

Kornblum, Janet. "AOL accused of privacy violation". CNET News.com. 9 January 1998.
URL: http://news.com.com/2100-1023-206960.html?legacy=cnet (15 March 2003)

Leahy, Patrick. "(USA PATRIOT) Act of 2001, H.R. 3162 Section-by-section Analysis".
URL: http://www.senate.gov/~leahy/press/200110/102401a.html (15 March 2003)

Michie Company. "Virginia Computer Crimes Act".
URL: http://courses.cs.vt.edu/~cs3604/lib/Crime/virginia.law.full (15 March 2003)