



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

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

An Investigative Forensic Examination

By

Charles Fraser

**GCFA Practical
Submission Attempt #2
Version 1.4 (July 2003)**

**Submission Date
03/28/04**

Part 1 Analyze An Unknown Binary

Binary Details-----	3
Program Description-----	12
Forensic Details-----	15
Program Identification-----	20
Legal Implications-----	24
Interview Questions-----	26
Case Information-----	27
Additional Information-----	38

Part 2 Option 1 Perform Forensic Analysis On A System

Synopsis of Case Facts-----	39
System Description-----	40
Hardware-----	40
Image Media-----	41
Media Analysis of System-----	49
Part 1-----	49
Part 2-----	61
Part 3-----	66
Part 4-----	69
Part 5-----	70
Part 6-----	73
Timeline Analysis-----	75
Recover Deleted Files-----	81
String Search-----	85
Conclusions-----	98

Part 3 Legal Issues of Incident Handling

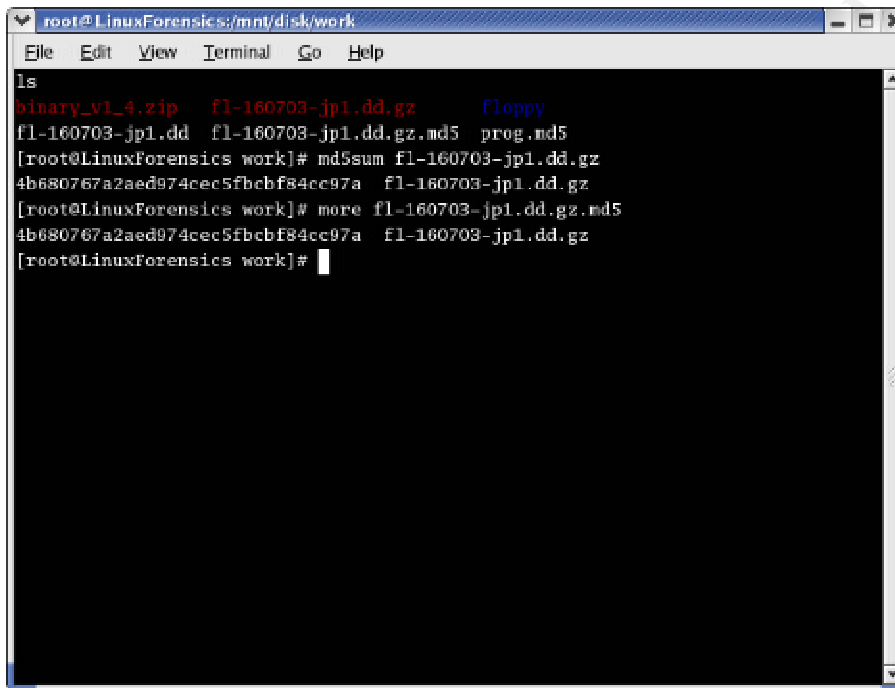
A-----	94
B-----	102
C-----	102
D-----	102

Appendix 1 Useful Links-----	103
Appendix 2 Excerpt of NJ Criminal Code-----	103
Appendix 3 U.S Child Pornography Laws-----	111
Appendix 4 Text File Listing From Part 2-----	120

Part 1 Analyze an Unknown Binary

Binary Details

I began my analysis of the floppy image seized from John Price's computer. I Sterilized the forensic examination partition of my forensic computer which is an 18gb expansion bay hard drive designated as hdc1. I used the dd command to zero out the media then formatted the drive and insure no data exists on the media. I downloaded the file from GIAC web site. I Copied image to sterilized workspace. I unzipped the archived file fl-160703-jp1.dd.gz and verified md5checksum of dd image file.



```
root@LinuxForensics:/mnt/disk/work
File Edit View Terminal Go Help
ls
binary_v1_4.zip  fl-160703-jp1.dd.gz  floppy
fl-160703-jp1.dd  fl-160703-jp1.dd.gz.md5  prog.md5
[root@LinuxForensics work]# md5sum fl-160703-jp1.dd.gz
4b680767a2aed974cec5fbcfb84cc97a  fl-160703-jp1.dd.gz
[root@LinuxForensics work]# more fl-160703-jp1.dd.gz.md5
4b680767a2aed974cec5fbcfb84cc97a  fl-160703-jp1.dd.gz
[root@LinuxForensics work]#
```

Upon comparing the md5sum of the image file and MD5 checksum file I found they match exactly.

The image was mounted using mount o -ro, loop

```
[root@LinuxForensics root]# mount -o ro,loop fl-160703-jp1.dd
/mnt/disk/work/floppy
```

At the root of the mounted image the following files and directories were found:

```
total 552
drwxr-xr-x  2 502    502      1024 Jul 14  2003 Docs
drwxr-xr-x  2 502    502      1024 Feb  3  2003 John
drwx-----  2 root   root    12288 Jul 14  2003 lost+found
drwxr-xr-x  2 502    502      1024 May  3  2003 May03
-rwxr-xr-x  1 502    502     56950 Jul 14  2003 nc-1.10-16.i386.rpm..rpm
-rwxr-xr-x  1 502    502    487476 Jul 14  2003 prog
```


The name of the binary in question as downloaded from the GIAC website is prog binary. After analysis I have identified the true name of the program is bmap. This was determined by searching text strings on the internet and comparing help libraries. I then took strings from the prog binary and inputted them into the Google search engine when I inputted the text string “use block-list knowledge to perform special operations on files”. The search returned reference to a binary called “bmap. Upon comparison of the source code and help file I was able to confirm this.

I Ran GraveRobber on the read only mounted image. Graverobber is found with The Coroner's Toolkit it was written by Dan Farmer and Weitse Venema and can be found at www.fish.com/tct. I am running version 1.11. Graverobber as describe on page 17 of vol 8.3 of the SANS System and Forensics textbook, Investigation and Response text book is a data capture tool which automates gathering of system information. Graverobber can also create MD5 signatures of all output and is most useful on a live system, but it can also be used on a disk image. When using graverobber I used the -M -i -v -V and -t options. As defined on Page 22 of vol 8.8 of the SANS Systems and Forensics textbook

- M md5Sum all files, implies and lstat so inode mactimes are collected too.
- i collect inode info from unallocated portions of the image.
- v do it verbosely.
- V get major and minor numbers from /dev
- t gather trust information

Below is the output from the graverobber command:

```
[root@LinuxForensics work]# /usr/local/src/tct/bin/grave-robber -c
/mnt/disk/work/floppy -o LINUX2 -MivVt
Determining OS (in determine_os())
OS is: LINUX2
Preparing the vault...
... in prepare_config_vault()
Grabbing all free inode info (in &suck_free_inodes())
Trying to find all disks (in &find_disks())
pipe_command: DF df -l
log_item: PIPEFROM_CMD df
grabbing all unallocated inode info in (in &grab_inode_info())
grabbing all unallocated inode info in /root/fl-160703-jp1.dd (in
&grab_inode_info())
Stamping file
/usr/local/src/tct/data//LinuxForensics/command_out/free_inode_info._root_fl-
160703-jp1.dd with date (in &date_stamp())
redirect_command: /bin/date
>/usr/local/src/tct/data//LinuxForensics/command_out/free_inode_info._root_fl-
160703-jp1.dd
```

```

log_item: REDIRECT_CMD
>/usr/local/src/tct/data//LinuxForensics/command_out/free_inode_info._root_fl-
160703-jp1.dd /bin/date
redirect_command: /usr/local/src/tct/bin/ils /root/fl-160703-jp1.dd
>>/usr/local/src/tct/data//LinuxForensics/command_out/free_inode_info._root_fl-
160703-jp1.dd
log_item: REDIRECT_CMD
>>/usr/local/src/tct/data//LinuxForensics/command_out/free_inode_info._root_fl-
160703-jp1.dd /usr/local/src/tct/bin/ils /root/fl-160703-jp1.dd
Making MD5 of file
/usr/local/src/tct/data//LinuxForensics/command_out/free_inode_info._root_fl-
160703-jp1.dd (in &sign_it())
redirect_command: /usr/local/src/tct/bin/md5
/usr/local/src/tct/data//LinuxForensics/command_out/free_inode_info._root_fl-
160703-jp1.dd
>/usr/local/src/tct/data//LinuxForensics/command_out/free_inode_info._root_fl-
160703-jp1.dd.md5
log_item: REDIRECT_CMD
>/usr/local/src/tct/data//LinuxForensics/command_out/free_inode_info._root_fl-
160703-jp1.dd.md5 /usr/local/src/tct/bin/md5
/usr/local/src/tct/data//LinuxForensics/command_out/free_inode_info._root_fl-
160703-jp1.dd
processing dir /mnt/disk/work/floppy// (in process_dir)
crunching dir /mnt/disk/work/floppy/ (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/Docs
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/Docs
processing dir /mnt/disk/work/floppy/Docs (in process_dir)
crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/Docs/Letter.doc
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/Docs/Letter.doc
crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/Docs/Mikemsg.doc
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/Docs/Mikemsg.doc
crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/Docs/Kernel-
HOWTO-html.tar.gz
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/Docs/Kernel-HOWTO-html.tar.gz
crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/Docs/MP3-
HOWTO-html.tar.gz
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/Docs/MP3-HOWTO-html.tar.gz

```

```

crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/Docs/Sound-
HOWTO-html.tar.gz
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/Docs/Sound-HOWTO-html.tar.gz
crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/Docs/DVD-
Playing-HOWTO-html.tar
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/Docs/DVD-Playing-HOWTO-html.tar
crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/lost+found
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/lost+found
crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/John
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/John
crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/prog
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/prog
crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/May03
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/May03
crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/nc-1.10-
16.i386.rpm..rpm
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/nc-
1.10-16.i386.rpm..rpm
crunching dir /mnt/disk/work/floppy/Docs (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/.~5456g.tmp
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/.~5456g.tmp
processing dir /mnt/disk/work/floppy/May03 (in process_dir)
crunching dir /mnt/disk/work/floppy/May03 (in crunch)
command_to_list: /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/May03/ebay300.jpg
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/May03/ebay300.jpg
processing dir /mnt/disk/work/floppy/John (in process_dir)
crunching dir /mnt/disk/work/floppy/John (in crunch)
command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/John/sect-
num.gif
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/John/sect-num.gif
crunching dir /mnt/disk/work/floppy/John (in crunch)

```

```

command_to_list: /usr/local/src/tct/bin/md5 /mnt/disk/work/floppy/John/sectors.gif
log_item: PIPEFROM_CMD /usr/local/src/tct/bin/md5
/mnt/disk/work/floppy/John/sectors.gif
processing dir /mnt/disk/work/floppy/lost+found (in process_dir)
Grabbing all trust-related files (in grab_user_trust_files())
Grabbing all time stuff (at, cron, etc) (in grab_user_time_trust())
Stamping file /usr/local/src/tct/data//LinuxForensics/trust/time with date (in
&date_stamp())
redirect_command: /bin/date >/usr/local/src/tct/data//LinuxForensics/trust/time
log_item: REDIRECT_CMD >/usr/local/src/tct/data//LinuxForensics/trust/time
/bin/date
Making MD5 of file /usr/local/src/tct/data//LinuxForensics/trust/time (in &sign_it())
redirect_command: /usr/local/src/tct/bin/md5
/usr/local/src/tct/data//LinuxForensics/trust/time
>/usr/local/src/tct/data//LinuxForensics/trust/time.md5
log_item: REDIRECT_CMD
>/usr/local/src/tct/data//LinuxForensics/trust/time.md5 /usr/local/src/tct/bin/md5
/usr/local/src/tct/data//LinuxForensics/trust/time
Grabbing some window stuff (in grab_window_trust())
Stamping file /usr/local/src/tct/data//LinuxForensics/trust/window_systems with
date (in &date_stamp())
redirect_command: /bin/date
>/usr/local/src/tct/data//LinuxForensics/trust/window_systems
log_item: REDIRECT_CMD
>/usr/local/src/tct/data//LinuxForensics/trust/window_systems /bin/date
pipe_command: XHOST /usr/X11R6/bin/xhost -|
log_item: PIPEFROM_CMD /usr/X11R6/bin/xhost
pipe_command: XAUTH /usr/X11R6/bin/xauth list -|
log_item: PIPEFROM_CMD /usr/X11R6/bin/xauth list
Making MD5 of file /usr/local/src/tct/data//LinuxForensics/trust/window_systems
(in &sign_it())
redirect_command: /usr/local/src/tct/bin/md5
/usr/local/src/tct/data//LinuxForensics/trust/window_systems
>/usr/local/src/tct/data//LinuxForensics/trust/window_systems.md5
log_item: REDIRECT_CMD
>/usr/local/src/tct/data//LinuxForensics/trust/window_systems.md5
/usr/local/src/tct/bin/md5
/usr/local/src/tct/data//LinuxForensics/trust/window_systems
Closing the vault (in close_config_vault())
Stamping file /usr/local/src/tct/data//LinuxForensics/MD5_all with date (in
&date_stamp())
redirect_command: /bin/date >/usr/local/src/tct/data//LinuxForensics/MD5_all
log_item: REDIRECT_CMD >/usr/local/src/tct/data//LinuxForensics/MD5_all
/bin/date
redirect_command: /usr/bin/find data//LinuxForensics_2004_03_13_14:58:44_-
0500 -print >md5_all.tmp.5767

```

```
log_item: REDIRECT_CMD >md5_all.tmp.5767 /usr/bin/find
data//LinuxForensics_2004_03_13_14:58:44_-0500 -print
Making MD5 of file /usr/local/src/tct/data//LinuxForensics/MD5_all (in &sign_it())
redirect_command: /usr/local/src/tct/bin/md5
/usr/local/src/tct/data//LinuxForensics/MD5_all
>/usr/local/src/tct/data//LinuxForensics/MD5_all.md5
log_item: REDIRECT_CMD >/usr/local/src/tct/data//LinuxForensics/MD5_all.md5
/usr/local/src/tct/bin/md5 /usr/local/src/tct/data//LinuxForensics/MD5_all
```

With the grave robber information I ran mactime against the body file with the following results:

```
[root@LinuxForensics root]# more mac.time
Tue Jan 28 2003 10:56:00 19088 ma. -rwxr-xr-x 502 502 24 /mnt
/hack/floppy/John/sect-num.gif
20680 ma. -rwxr-xr-x 502 502 25 /mnt
/hack/floppy/John/sectors.gif
Mon Feb 03 2003 06:08:00 1024 m.. drwxr-xr-x 502 502 12 /mnt
/hack/floppy/John
Sat May 03 2003 06:10:00 1024 m.. drwxr-xr-x 502 502 14 /mnt
/hack/floppy/May03
Wed May 21 2003 06:09:00 29184 ma. -rwxr-xr-x 502 502 13 /mnt
/hack/floppy/Docs/DVD-Playing-HOWTO-html.tar
27430 ma. -rwxr-xr-x 502 502 19 /mnt
/hack/floppy/Docs/Kernel-HOWTO-html.tar.gz
Wed May 21 2003 06:12:00 32661 ma. -rwxr-xr-x 502 502 20 /mnt
/hack/floppy/Docs/MP3-HOWTO-html.tar.gz
Wed Jun 11 2003 09:09:00 29696 ma. -rw----- 502 502 16 /mnt
/hack/floppy/Docs/Letter.doc
Mon Jul 14 2003 10:08:09 12288 m.c drwx----- 0 0 11 /mnt
/hack/floppy/lost+found
Mon Jul 14 2003 10:11:50 26843 ma. -rwxr-xr-x 502 502 21 /mnt
/hack/floppy/Docs/Sound-HOWTO-html.tar.gz
Mon Jul 14 2003 10:12:02 56950 ma. -rwxr-xr-x 502 502 22 /mnt
/hack/floppy/nc-1.10-16.i386.rpm..rpm
Mon Jul 14 2003 10:12:48 13487 ma. -rwxr-xr-x 502 502 26 /mnt
/hack/floppy/May03/ebay300.jpg
Mon Jul 14 2003 10:13:52 2592 m.c -rw-r--r-- 0 0 28 /mnt
/hack/floppy/.~5456g.tmp
Mon Jul 14 2003 10:22:36 1024 m.. drwxr-xr-x 502 502 15 /mnt
/hack/floppy/Docs
Mon Jul 14 2003 10:24:00 487476 m.. -rwxr-xr-x 502 502 18 /mnt
/hack/floppy/prog
Mon Jul 14 2003 10:43:44 26843 ..c -rwxr-xr-x 502 502 21 /mnt
/hack/floppy/Docs/Sound-HOWTO-html.tar.gz
1024 ..c drwxr-xr-x 502 502 15 /mnt
/hack/floppy/Docs
```

```

Mon Jul 14 2003 10:43:53 13487 ..c -rwxr-xr-x 502 502 26 /mnt
/hack/floppy/May03/ebay300.jpg
Mon Jul 14 2003 10:43:57 56950 ..c -rwxr-xr-x 502 502 22 /mnt
/hack/floppy/nc-1.10-16.i386.rpm..rpm
Mon Jul 14 2003 10:45:48 29184 ..c -rwxr-xr-x 502 502 13 /mnt
/hack/floppy/Docs/DVD-Playing-HOWTO-html.tar
Mon Jul 14 2003 10:46:00 27430 ..c -rwxr-xr-x 502 502 19 /mnt
/hack/floppy/Docs/Kernel-HOWTO-html.tar.gz
Mon Jul 14 2003 10:46:07 32661 ..c -rwxr-xr-x 502 502 20 /mnt
/hack/floppy/Docs/MP3-HOWTO-html.tar.gz
Mon Jul 14 2003 10:47:57 29696 ..c -rw----- 502 502 16 /mnt
/hack/floppy/Docs/Letter.doc
Mon Jul 14 2003 10:48:15 19456 mac -rw----- 502 502 17 /mnt
/hack/floppy/Docs/Mikemsg.doc
Mon Jul 14 2003 10:48:53 19088 ..c -rwxr-xr-x 502 502 24 /mnt
/hack/floppy/John/sect-num.gif
20680 ..c -rwxr-xr-x 502 502 25 /mnt
/hack/floppy/John/sectors.gif
Mon Jul 14 2003 10:49:25 1024 ..c drwxr-xr-x 502 502 12 /mnt
/hack/floppy/John
Mon Jul 14 2003 10:50:15 1024 ..c drwxr-xr-x 502 502 14 /mnt
/hack/floppy/May03
Wed Jul 16 2003 02:05:33 487476 ..c -rwxr-xr-x 502 502 18 /mnt
/hack/floppy/prog
Wed Jul 16 2003 02:06:15 12288 .a. drwx----- 0 0 11 /mnt
/hack/floppy/lost+found
Wed Jul 16 2003 02:09:35 1024 .a. drwxr-xr-x 502 502 12 /mnt
/hack/floppy/John
Wed Jul 16 2003 02:09:49 1024 .a. drwxr-xr-x 502 502 14 /mnt
/hack/floppy/May03
Wed Jul 16 2003 02:10:01 1024 .a. drwxr-xr-x 502 502 15 /mnt
/hack/floppy/Docs
Wed Jul 16 2003 02:11:36 2592 .a. -rw-r--r-- 0 0 28 /mnt
/hack/floppy/.~5456g.tmp
Wed Jul 16 2003 02:12:45 487476 .a. -rwxr-xr-x 502 502 18 /mnt
/hack/floppy/prog

```

The last time the file was modified was 7/14/03 10:24AM.

The last time the file was changed was 7/16/03 2:05AM

The last time the file was accessed was 7/16/03 2:12AM

I ran the stat command on prog with the results in the image below. The stat command supported the mactimes produced from the graverobber information.

```
root@LinuxForensics:/mnt/disk/work/floppy
File Edit View Terminal Go Help

[root@LinuxForensics work]# cd floppy
[root@LinuxForensics floppy]# stat prog
  File: 'prog'
  Size: 487476      Blocks: 960      IO Block: 4096   Regular File
Device: 790h/1792d-- --Inode: 18----   Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (   502/ UNKNOWN)   Gid: (   502/ UNKNOWN)
Access: 2003-07-16 02:12:45.000000000 -0400
Modify: 2003-07-14 10:24:00.000000000 -0400-- -- -- -- --
Change: 2003-07-16 02:05:33.000000000 -0400

[root@LinuxForensics floppy]#
```

Also indicated in the output from the stat command is the owner and group of the file are unknown because there is no passwd or group file to compare it to. The file size is 487476 bytes.

I compared the md5 sum of the prog binary and the prog.md5. The values matched exactly meaning that the binary has been verified to be the actual file packaged with the zipped archive.

```
root@LinuxForensics:/mnt/disk/work
File Edit View Terminal Go Help

ls
Docs John lost+found May03 nc-1.10-16.i386.rpm..rpm prog
[root@LinuxForensics floppy]# md5sum prog
7b80d9aff486c6aa6aa3efa63cc56880 prog
[root@LinuxForensics floppy]# cd ..
[root@LinuxForensics work]# ls
binary_v1_4.zip fl-160703-jp1.dd.gz floppy
fl-160703-jp1.dd fl-160703-jp1.dd.gz.md5 prog.md5
[root@LinuxForensics work]# more prog.md5
7b80d9aff486c6aa6aa3efa63cc56880 prog
[root@LinuxForensics work]#
```

I ran strings on the prog binary and was able to get some key words which I will outline further on in the paper. Some key words of interest include:

+45 3325-6543

+45 3122-6543

keld@dkuug.dk

Keld Simonsen

ISO/IEC 14652 i18n FDCC-set

C/o Keld Simonsen, Skt. Jorgens Alle 8, DK-1615 Kobenhavn V

ISO/IEC JTC1/SC22/WG20 - internationalization

autogenerate document ...

1.0.20 (07/15/03)

newt

LC_IDENTIFICATION

LC_MEASUREMENT

LC_TELEPHONE

LC_ADDRESS

LC_NAME

LC_PAPER

LOCPATH

/usr/lib/locale

LANG

/SYS_

December

November

October

September

August

July

June

April

March

February

January

Saturday

Friday

Thursday

Wednesday

Tuesday

Monday

Sunday

Other strings from the binary which initially were possibly suspicious turned out to just be statically included libraries to make the file self contained.

Unable to open file: %s
Unable to determine blocksize
target file block size: %d
unable to raw open %s
Unable to determine count
Unable to allocate buffer
bmap_get_slack_block
NULL value for slack_block
print number of bytes available
test (returns 0 if exist)
wipe
place data
display data
extract a copy from the raw device
list sector numbers
operation to perform on files
Operation now in progress
Operation already in progress
No route to host
Host is down
Connection refused
Connection timed out
No buffer space available
Connection reset by peer
Network is unreachable
Network is down
Address already in use
Protocol family not supported
Operation not supported
Socket type not supported
Protocol not supported
Protocol not available

Program Description:

After analyzing the file prog is in reality the binary bmap. Bmap is a program which checks, writes, deletes, and wipes to slack space. As defined on page 63 of Vol. 8.2 *Basic Forensic Principles Illustrated With Linux*. Slack space is "Another method for hiding data is to write to areas of the disk that [because of allocation algorithms] are unusable by the kernel. Slack space is unused space in a disk block which can be written to and remain almost totally hidden to the operating system. The disadvantage of using slack space is that if the inode where the slack space is rewritten the data is lost. A good use of slack space in a

corporate or scientific environment would be espionage to get data out of a location undetected.

The blocksize of a typical file system varies from 1K to 4K. Every file takes at least one block. The unused space in that block is slack space. bmap can save data into this slack space, extract data from slack space, and delete data in slack space. The data cannot be accessed using tools unaware of slack space (ie. almost all other tools), does not change existing files, and therefore cannot be detected using checksums or access times.

Bmap was written by in 1998 by Daniel Ridge who was an analyst for NASA's Computer Crime Division. I obtained this information from the readme file of bmap-1.0.20

Excerpt from the read me file:

Written 1998 by Daniel Ridge in support of:

Computer Crime Division, Office of Inspector General,
National Aeronautics and Space Administration.

I ran the prog executable with the `--help` flag which produced the following results which instructed how to use the program. The person who compiled the program modified the commands slightly as compared to the actual bmap 1.0.20 program which I will show further in the program identification section.

```
[root@LinuxForensics floppy]# ./prog --help
prog:1.0.20 (07/15/03) newt
Usage: prog [OPTION]... [<target-filename>]
use block-list knowledge to perform special operations on files
```

`--doc VALUE`

where VALUE is one of:

version display version and exit
help display options and exit
man generate man page and exit
sgml generate SGML invocation info

`--mode VALUE`

where VALUE is one of:

m list sector numbers
c extract a copy from the raw device
s display data
p place data
w wipe
chk test (returns 0 if exist)
sb print number of bytes available
wipe wipe the file from the raw device
frag display fragmentation information for the file
checkfrag test for fragmentation (returns 0 if file is fragmented)

--outfile <filename> write output to ...
--label useless bogus option
--name useless bogus option
--verbose be verbose
--log-thresh <none | fatal | error | info | branch | progress | entryexit> logging threshold ...
--target <filename> operate on ...

The person who compiled this program shortened the options quite possibly to throw off an investigator or systems administrator. For example, to place data into slack space using bmap the correct syntax is "bmap --mode putslack filename" using prog the syntax would be "prog--mode p filename"

To confirm how the prog binary worked I created a text file using the vi text editor called test.txt. The contents of that file are as follows:

```
[root@LinuxForensics root]# echo "This data is secret don't tell anyone!" |  
/mnt/disk/work/floppy/prog --mode p test.txt  
stuffing block 593484  
file size was: 40  
slack size: 4056  
block size: 4096
```

The output confirmed that the slackspace in block 592484 was stuffed with the text I inputted. I confirmed this by using the display data option:

```
[root@LinuxForensics root]# /mnt/disk/work/floppy/prog --mode s test.txt getting  
from block 593484  
file size was: 40  
slack size: 4056  
block size: 4096  
This data is secret don't tell anyone!
```

To further confirm that the data was only readable in the slack space I outputted the contents of the test file I created:

```
[root@LinuxForensics root]# more test.txt
```

The Grey Fox jumped over the red barn.

There is no evidence of my covert message by examining the file system directly, nor has the size of the file changed.

Using the data I gathered from analyzing the mactimes I have determined the last time the program was most likely run was on July 16th at 2:12 AM. However we only have circumstantial evidence that the program was run on Price's computer. Through checking MAC times I was able to determine I was able to establish that the prog binary was last accessed 2:12:45 on 7/16/2003.

Because the hard drive was wiped in system the floppy was found I cannot determine which system the program was last executed. Most likely it was last used on Price's system.

Forensic Details.

The prog binary was compiled statically therefore it does not use any shared libraries The program can run stand alone from the floppy. The most evident footprint of this binary would be data written in the slack space of a file system. to check the slack space of the files in the suspected file system. I examined each file on the floppy for slack space and found some data in the slack space of Sound - H O W T O - h t m l . t a r . g z in the docs directory.

```
[ r o o t @ L i n u x F o r e n s i c s   D o c s ] #
/ m n t / d i s k / w o r k / f l o p p y / p r o g   - -
m o d e s   S o u n d - H O W T O -
h t m l . t a r . g z
g e t t i n g   f r o m   b l o c k   1 9 0
f i l e   s i z e   w a s :   2 6 8 4 3
s l a c k   s i z e :   8 0 5
b l o c k   s i z e :   1 0 2 4

h ? ? d o w n l o a d s M ? ? ?
E w ? ? ? l a p s 4 $ ? ? ? ? ? B R P ? ? m ? \ • ' ?
? ? ? ? / ? ? { ? ? ? \ x ?
? ? ? ? ? Z ? \ ? V % d ? S 6 ? ? A ? ? k W ? ? P ?
W ? d | e # ? ? ? ? ? 3 x ? b ? Z / ? 3 ? ? H ? A ? M ?
$ 3 t B i ? u ] 7 N
? y • [ r o o t @ L i n u x F o r e n s i c s
D o c s ] #
? M 3 ? ? e ? e ? ?
```

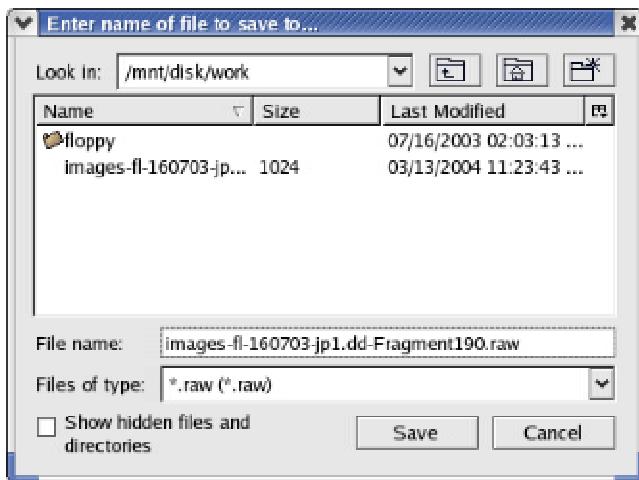
The output looks to be either a piece of file or code. I attempted to reconstruct this piece of data in a new file using a hex editor but when I ran the file command against it the return was it was a gzip archive. I was unable to gunzip the file when I renamed it to a .gz archive.

```
[root@LinuxForensics work]# file test1
```

```
test1: gzip compressed data, was "downloads", from Unix
```

According to the output of the file command as indicated above, It is possible that the original name of the file put in slack was downloads.

I tried renaming the file to and .mp3 extension and playing is as a sound archive with no success. I then attempted reconstructing the data found in the slack space I used Autopsy to export all of the data from fragment 190 where the suspect code is located on the floppy image.



Using a hex editor I tried once again to extract the slack data. I was unsuccessful in recomposing the data to ascertain what type of data was in the slack space. I then tried using bmap to extract the slack data of sound-HOWTO-html.tar.gz to a file.

```

root@LinuxForensics:/mnt/disk/work/floppy/Docs
File Edit View Terminal Go Help
[root@LinuxForensics root]# cd /mnt/disk/work/floppy/Docs
[root@LinuxForensics Docs]# ls
DVD-Playing-HOWTO-html.tar Letter.doc MP3-HOWTO-html.tar.gz
Kernel-HOWTO-html.tar.gz Mikensg.doc Sound-HOWTO-html.tar.gz
[root@LinuxForensics Docs]# /root/temp/bmap-1.0.20/bmap --mode slack --outfile /
root/output2 Sound-HOWTO-html.tar.gz
getting from block 190
file size was: 26843
slack size: 805
block size: 1024
[root@LinuxForensics Docs]#

```

I performed the file command on the output2 file. The file command was reporting the file was a gzip compressed archive.

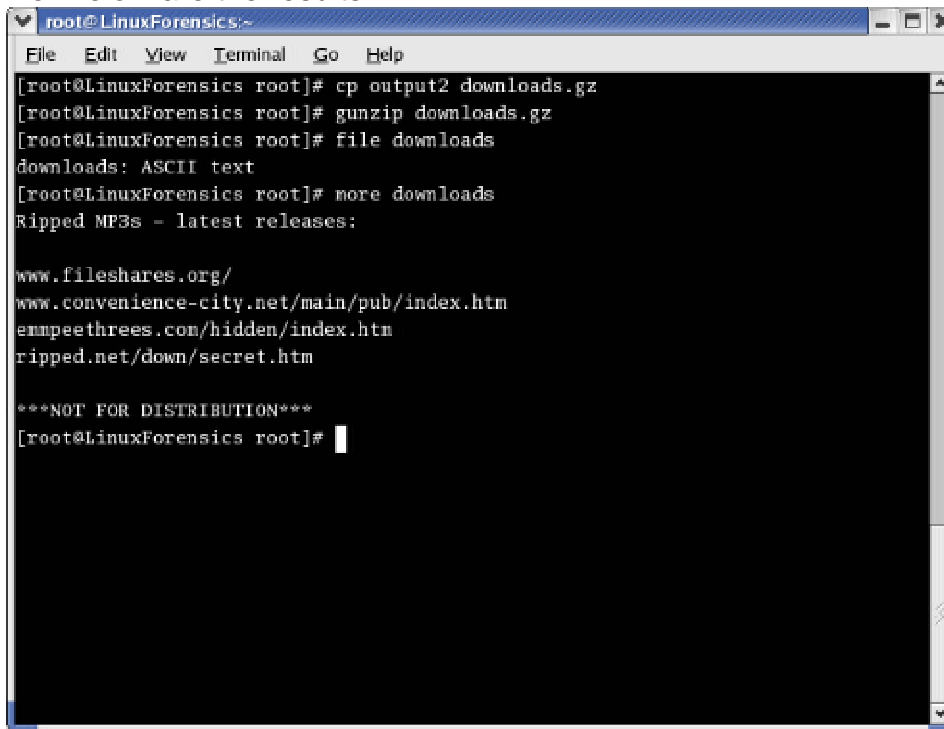
```
[root@LinuxForensics root]# file output2
```

output2: gzip compressed data, was "downloads", from Unix
I then attempted to unzip the file output2.

```
[root@LinuxForensics root]# gunzip output2
```

gunzip: output2: unknown suffix -- ignored

I then copied the output file to a file with a .gz extension. I was successful. I then did a file on the renamed file downloads and it returned to be an ASCII text file. Below are the results.



```
root@LinuxForensics:~  
File Edit View Terminal Go Help  
[root@LinuxForensics root]# cp output2 downloads.gz  
[root@LinuxForensics root]# gunzip downloads.gz  
[root@LinuxForensics root]# file downloads  
downloads: ASCII text  
[root@LinuxForensics root]# more downloads  
Ripped MP3s - latest releases:  
  
www.fileshares.org/  
www.convenience-city.net/main/pub/index.htm  
ennpeethrees.com/hidden/index.htm  
ripped.net/down/secret.htm  
  
***NOT FOR DISTRIBUTION***  
[root@LinuxForensics root]#
```

The file contained lists of download sites to obtain "Ripped MP3s. I was incorrect in my original assumption that the data in the slack space was a partial mp3 file. I visited some of the listed sites. The first three sites could not be resolved and the last site ripped.net/down/secret was a redirection to a travel site <http://www.travelnow.com/index.jsp?cid=58623&home=truedown/secret.htm>

Other evidence found on the disk leads me to believe the type of data Mr. Price is hiding are mp3 audio files. An mp3 file as defined by the Institute of Telecommunication Sciences is "A standard wave file format (with a ".wav" file extension) for digitally encoded and compresses music files (similar to the format used for CD music files). *Note:* MP3 files can be stored or downloaded from the web or other media and played on suitable players".

The forensic footprints that the prog binary would leave is data in the slack space. Since Prog is a statically compiled binary it does not depend on any other libraries, files or programs. Prog does not need to even need to be installed on the file system in question as in this case it can be installed on a floppy. Prog also can be ran from an external file system or other external media. Since there are no log files generated from the program's use data in the slack space of the file system would be the only indicator of it's existence. I also found a the rpm for netcat for Redhat 8 which would enable the user to upload or download

information. The addition of netcat to the floppy makes a neat self contained kit to collect and distribute material.

Upon my initial analysis I discovered the following contact information:

+45 3325-6543

+45 3122-6543

keld@dkuug.dk

Keld Simonsen

ISO/IEC 14652 i18n FDCC-set

C/o Keld Simonsen, Skt. Jorgens Alle 8, DK-1615 Kobenhavn V

ISO/IEC JTC1/SC22/WG20 - internationalization

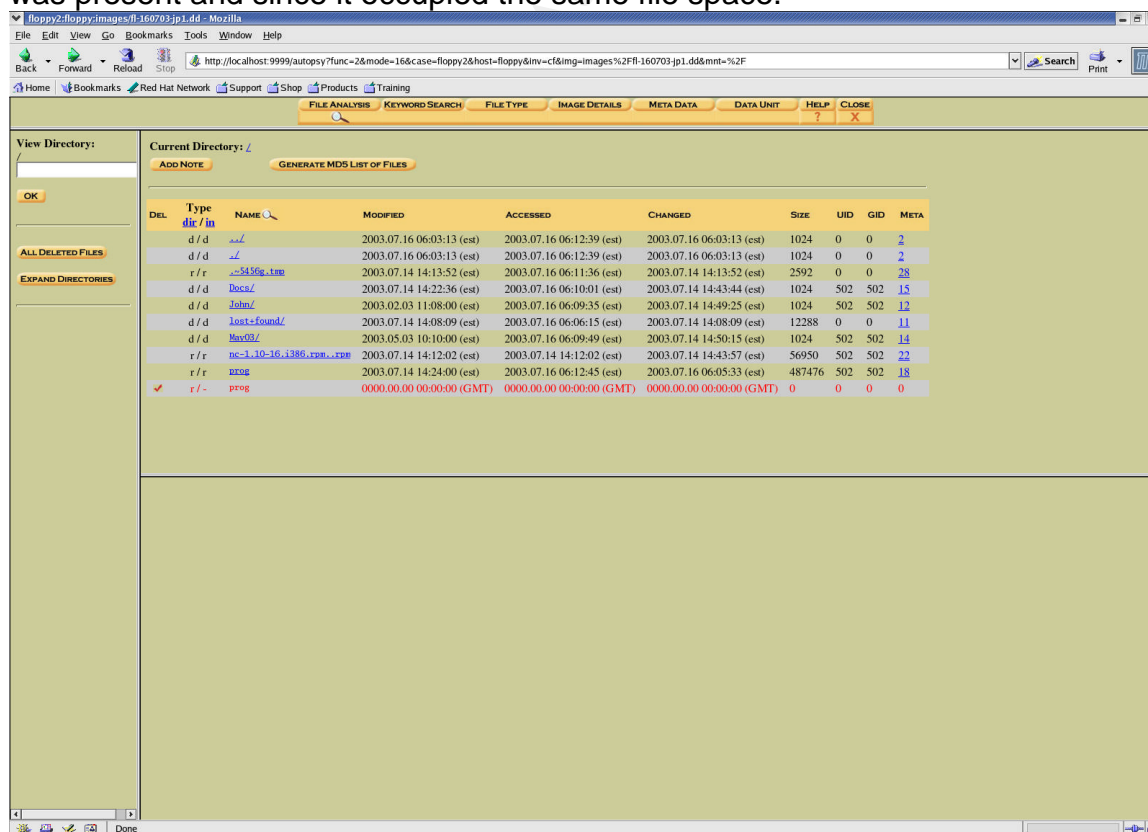
Upon further investigation Keld Simonson is on a ISO committee for localization standards.

Other interesting strings include:

autogenerate document ...

1.0.20 (07/15/03)

From this information I was to determine that the binary version is 1.0.20 and was compiled on 7/15/03. This information conflicts with the modify date/time stamp of 7/14/03. When I ran Autopsy I found an instance of prog was deleted for the floppy as indicated below, however since the inode was rewritten I could obtain no further information. It appears an earlier compiled version of the binary was present and since it occupied the same file space.



DEL	Type	NAME	MODIFIED	ACCESSED	CHANGED	SIZE	UID	GID	META
	d / d	..	2003.07.16 06:03:13 (est)	2003.07.16 06:12:39 (est)	2003.07.16 06:03:13 (est)	1024	0	0	2
	d / d	..	2003.07.16 06:03:13 (est)	2003.07.16 06:12:39 (est)	2003.07.16 06:03:13 (est)	1024	0	0	2
	r / r	..5456p.img	2003.07.14 14:13:52 (est)	2003.07.16 06:11:36 (est)	2003.07.14 14:13:52 (est)	2592	0	0	28
	d / d	Docu/	2003.07.14 14:22:36 (est)	2003.07.16 06:10:01 (est)	2003.07.14 14:43:44 (est)	1024	502	502	15
	d / d	John/	2003.02.03 11:08:00 (est)	2003.07.16 06:09:35 (est)	2003.07.14 14:49:25 (est)	1024	502	502	12
	d / d	lost+found/	2003.07.14 14:08:09 (est)	2003.07.16 06:06:15 (est)	2003.07.14 14:08:09 (est)	12288	0	0	11
	d / d	My00/	2003.05.03 10:10:00 (est)	2003.07.16 06:09:49 (est)	2003.07.14 14:50:15 (est)	1024	502	502	14
	r / r	nc-1.10-16.1386.rpm...	2003.07.14 14:12:02 (est)	2003.07.14 14:12:02 (est)	2003.07.14 14:43:57 (est)	56950	502	502	22
	r / r	prog	2003.07.14 14:24:00 (est)	2003.07.16 06:12:45 (est)	2003.07.16 06:05:33 (est)	487476	502	502	18
✓	r / -	prog	0000.00.00 00:00:00 (GMT)	0000.00.00 00:00:00 (GMT)	0000.00.00 00:00:00 (GMT)	0	0	0	0

newt

Newt refers to Daniel Ridge, the original author of BMAP newt@scyld.com

Daniel Ridge **newt@scyld.com**

I ran the file command on the executable with the following results:

```
[root@LinuxForensics floppy]# file prog
prog: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for GNU/Linux
2.2.5, statically linked, stripped
[root@LinuxForensics floppy]#
```

The prog binary is stripped and statically linked meaning that the libraries are built into the binary and can be run as a stand alone program. I was able to confirm most of these results by running `readelf -h` and the `ldd` command which lists any shared library dependencies.

```
[root@LinuxForensics floppy]# readelf -h prog
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:       0x80480e0
  Start of program headers:  52 (bytes into file)
  Start of section headers:  486796 (bytes into file)
  Flags:                     0x0
  Size of this header:       52 (bytes)
  Size of program headers:   32 (bytes)
  Number of program headers:  3
  Size of section headers:   40 (bytes)
  Number of section headers: 17
  Section header string table index: 16
```

```
[root@LinuxForensics floppy]# ldd prog
not a dynamic executable
```

The output from running `readelf-h` confirms that the prog executable is a Linux (Unix System V) executable in ELF format that was compiled for the Intel

386 chipset. The output from the ldd command confirms the prog executable is not a dynamic executable.

The environment I used to test the prog binary was a Dell C-800 laptop running Redhat 9. By running the prog -help command I was able to ascertain the command switches which almost exactly match the actual bmap binary except the person who compiled this program shortened the options by letter as indicated below.

Program Identification

The latest version of bmap is 1.0.20 and is available on a few ftp sites. I obtained the source code from

<http://ftp.cfu.net/mirrors/garchive.cs.uni.edu/garchive/bmap-1.0.20/>. I compiled

the source code using gcc version 3.2.2. I was only able to compile the binary dynamically using the make command and gcc ver 3.22.

When trying to compile using gcc -static I kept getting the error "bmap.c:103: storage size of 'bmap_info' isn't known. I attempted to contact the author but the email address provided was not valid. After many attempts I went forward and did a comparison between the static prog binary and dynamic bmap. I performed a file and readelf on bmap. The file was compiled for Linux 2.2.5 for use on the Intel processor. I also ran the ldd command on the binary which lists file dependencies.

```
[root@LinuxForensics bmap-1.0.20]# file bmap
bmap: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for GNU/Linux
2.2.5, dynamically linked (uses shared libs), not stripped
[root@LinuxForensics bmap-1.0.20]# readelf -h bmap
```

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: 0x8048a20
Start of program headers: 52 (bytes into file)
Start of section headers: 214932 (bytes into file)
Flags:    0x0
Size of this header: 52 (bytes)
Size of program headers: 32 (bytes)
Number of program headers: 7
Size of section headers: 40 (bytes)
```

Number of section headers: 35
Section header string table index: 32

```
[root@LinuxForensics bmap-1.0.20]# ldd bmap
libc.so.6 => /lib/tls/libc.so.6 (0x42000000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
```

The libc package as defined (obtained from <http://dc.qut.edu.au/rpm2html/local/glibc-2.3.2-11.9.i686.html>). The glibc package contains standard libraries which are used by multiple programs on the system. In order to save disk space and memory, as well as to make upgrading easier, common system code is kept in one place and shared between programs. This particular package contains the most important sets of shared libraries: the standard C library and the standard math library. Without these two libraries, a Linux system will not function.

The file size of bmap is 221985 bytes much smaller than the prog binary because the libraries are not compiled in. I ran strings on bmap and found the base code to match prog. I will also include the full strings from bmap.

Excerpt from bmap.
01/25/04
invalid option: %s
try '--help' for help.
how did we get here?
no filename. try '--help' for help.
target filename: %s
Unable to stat file: %s
%s is not a regular file.
%s has multiple links.
Unable to open file: %s
Unable to determine blocksize
target file block size: %d
unable to raw open %s
Unable to determine count
Unable to allocate buffer
%s has holes in excess of %ld bytes...
error mapping block %d (%s)
nul block while mapping block %d.
seek failure
read error
write error
%s fragmented between %d and %d
%d %s
getting from block %d

Excerpt from prog.
07/15/03
invalid option: %s
try '--help' for help.
how did we get here?
no filename. try '--help' for help.
target filename: %s
Unable to stat file: %s
%s is not a regular file.
%s has multiple links.
Unable to open file: %s
Unable to determine blocksize
target file block size: %d
unable to raw open %s
Unable to determine count
Unable to allocate buffer
%s has holes in excess of %ld bytes...
error mapping block %d (%s)
nul block while mapping block %d.
seek failure
read error
write error
%s fragmented between %d and %d
%d %s
getting from block %d

I also confirmed the identity of prog by comparison of the help file. As I indicated above there was very little difference in the out put of --help.

```
[root@LinuxForensics bmap-1.0.20]# bmap --help
bmap:1.0.20 (05/29/00) newt@scyld.com
Usage: bmap [OPTION]... [<target-filename>]
use block-list knowledge to perform special operations on files
```

```
--doc VALUE
  where VALUE is one of:
  version  display version and exit
  help    display options and exit
  man     generate man page and exit
  sgml    generate SGML invocation info
--mode VALUE
  where VALUE is one of:
  map     list sector numbers
  carve   extract a copy from the raw device
  slack   display data in slack space
```

putslack place data into slack
wipeslack wipe slack
checkslack test for slack (returns 0 if file has slack)
slackbytes print number of slack bytes available
wipe wipe the file from the raw device
frag display fragmentation information for the file
checkfrag test for fragmentation (returns 0 if file is fragmented)
--outfile <filename> write output to ...
--label useless bogus option
--name useless bogus option
--verbose be verbose
--log-thresh <none | fatal | error | info | branch | progress | entryexit> logging threshold ...
--target <filename> operate on ...

The only differences in some of the command options. I ran an md5 sum against both binaries, since they were compiled differently why will be different. I ran the strip command, which discards the symbols, on bmap which changed the md5sum.

```
[root@LinuxForensics bmap-1.0.20]# md5sum bmap
c186fd03c46e710f3c51a87a7226951d bmap
[root@LinuxForensics bmap-1.0.20]# strip bmap
[root@LinuxForensics bmap-1.0.20]# md5sum bmap
0a95ced2800392c61a81d6ff440eb755 bmap
[root@LinuxForensics floppy]# md5sum prog
7b80d9aff486c6aa6aa3efa63cc56880 prog
```

Ran strings on the bmap 1.0.20 binary

Ran strings on the prog 1.0.20 binary

Strings on bmap was 64813

Strings on prog was 54948

I ran FSStat **Define**

```
[root@LinuxForensics root]# fsstat -f linux-ext2 /mnt/disk/floppy.img
FILE SYSTEM INFORMATION
```

```
-----
File System Type: EXT2FS
Volume Name:
Last Mount: Wed Jul 16 02:12:33 2003
Last Write: Wed Jul 16 02:12:58 2003
Last Check: Mon Jul 14 10:08:08 2003
Unmounted properly
```

Last mounted on:
Operating System: Linux
Dynamic Structure
InCompat Features: Filetype,
Read Only Compat Features: Sparse Super,

META-DATA INFORMATION

Inode Range: 1 - 184
Root Directory: 2

CONTENT-DATA INFORMATION

Fragment Range: 0 - 1439
Block Size: 1024
Fragment Size: 1024

BLOCK GROUP INFORMATION

Number of Block Groups: 1
Inodes per group: 184
Blocks per group: 8192
Fragments per group: 8192

Group: 0:
Inode Range: 1 - 184
Block Range: 1 - 1439
Super Block: 1 - 1
Group Descriptor Table: 2 - 2
Data bitmap: 3 - 3
Inode bitmap: 4 - 4
Inode Table: 5 - 27
Data Blocks: 28 - 1439

Legal Implications

I was able to prove that the program was run by finding the data in the slack space of the floppy. However, it can not be proven conclusively what system or systems the program was run on. There are a few potential criminal violations both Federal and State. There is a lot of circumstantial evidence that Mr. Price has been engaged in the distribution and sale of copyrighted music. Since the system he is working on was wiped there is no corroborating evidence such as an mp3 file containing copyrighted material. There is the question of slack space and would it's use constitute a crime under NJ Criminal Code 2C:20-8. Theft of Services? If Mr. Price used the cooperate computer facilities for a commercial enterprise as the circumstantial evidence points to he can be

prosecuted under NJ law as well as federal charges for distributing copyrighted material.

Federal law prohibits distributing copyrighted material. If Mr. Price was charged under federal Statute it would most likely be under Title 17 U.S.C 101 and Title 18 U.S.C Section 2319. Below is an excerpt from the law from the Recording Industry

U.S. Copyright Law {Title 17 U.S.C. Section 101 et seq., Title 18 U.S.C. Section 2319} Federal law protects copyright owners from the unauthorized reproduction, adaptation, performance, display or distribution of copyright protected works.

Penalties for copyright infringement differ in civil and criminal cases. Civil remedies are generally available for any act of infringement without regard to the intention or knowledge of the defendant, or harm to the copyright owner. Criminal penalties are available for intentional acts undertaken for purposes of "commercial advantage" or "private financial gain." "Private financial gain" includes the possibility of financial loss to the copyright holder as well as traditional "gain" by the defendant.

Where the infringing activity is for commercial advantage or private financial gain, sound recording infringements can be punishable by up to five years in prison and \$250,000 in fines. Repeat offenders can be imprisoned for up to 10 years. Violators can also be held civilly liable for actual damages, lost profits, or statutory damages up to \$150,000 per work.

In the state of New Jersey use of slack space may constitute a violation of NJ Criminal Code 2C:20-8. Theft of Services. Under section b it states "b. A person commits theft if, having control over the disposition of services of another, to which he is not entitled, he knowingly diverts such services to his own benefit or to the benefit of another not entitled thereto." Since using slack space would be without the knowledge or permission of the owner. Slack space also is decidedly not a service offered by the owner. In proving whether a crime has been committed it needs to be established who owns the floppy disk. If the floppy disk is owned by the company then a crime possible has been committed. It is evident that the prog binary was executed. Since there is data in the slackspace of one of the files on the floppy. The problem is since Price's system has been wiped and the malware can be run self-contained on the floppy it would be impossible to prove forensically that the program was executed on Mr Price's computer. However, There is enough evidence to prove that data was hidden.

At the institution where I am employed we have a Guidelines for Responsible Computing

Running a program which manipulates slack space could be considered a violation of section 5. Placing data in the slack space bypasses the operating system and would not be detected by any file accounting systems such as quotas.

“5. You must refrain from any unauthorized action which deliberately interferes with the operating system or accounting functions of the systems or that is likely to have such effects.

2. You must not intentionally seek information about, browse, obtain copies of, or modify files, passwords, images, music, sound or tapes belonging to other people, whether at Montclair State or elsewhere, unless specifically authorized to do so by those individuals. (Note: if an individual has explicitly and intentionally established a public server, or explicitly designated a set of files as being for shared public use, others may assume authorization to use that server or those files.)”

Potential Interview Questions

If I had the opportunity to interview the suspect I would ask the following questions:

- What is your job and classification?
- Does anyone else use this computer?
- Who else might have access to the computer?
- You seem to have an interest in computers where do your interests lie?
- Tell me a little about the programs you use on your computer and how you use it.
- What kind of computer do you use at home and how do you use it?
- Do you download music at home?
- Have you ever compiled a program? What programs have you compiled lately?
- Do you know what slack space is and how it works?
- Do you listen to music while your working?
- Mr. Price you maintain that the floppy is not yours yet there is a directory with your first name and documents with your name on them. How do you think they got there?
- On the floppy in the John directory is document called mikemsg.doc does that sound familiar?
- What are your initials please?
- Do you know anyone named Mike?
- Are you familiar with federal copyright laws?
- Let's say I had the floppy disk dusted for fingerprints, would you be willing to supply your fingerprints for comparison?

I started out asking simple questions about Mr. Price's job and progressed with more pointed questions. The last question is meant to intimidate and I would be looking for reactions and possibly for the suspect to break and admit what he

did if anything. Since Mr. Price denied ownership of the floppy no warrant would be needed to obtain fingerprints. Before I questioned the suspect I would run the questions past human resources and the legal department.

Case information

Detecting use of slack space is not something that is generally done. I would recommend to Systems Administrators to implement both policy and procedural changes. There are some commercial packages such as pro-discovery which would detect the use of slack space on a file system. Monitoring utilities like Tripwire would not detect manipulation of slack space. Perhaps script bmap to scan a file system. Random security checks can be performed I would also update the accepted use policy forbidding using forensic tools without written permission of the IT Director. Due to the nature of the files found on the floppy I would suggest monitoring network traffic on all of the computers in the area for large amounts of uploads and downloads.

In addition to the data found in the slack space listing mp3 ripper sites I found other evidence to support the assumption that Mr. Price was using the company's computer resources to distribute copyrighted material possibly for his own financial gain.

I went through these documents and the most compelling is a file "Mikemsg.doc". While the evidence is circumstantial it is a message signed by a person JP indicating that he received the last batch of files and that he had advanced orders. There are also other documents I discovered after copying and uncompressing the other document files in the /Docs directory. I found the following documents in the /Docs directory. Below is a synopsis:

```
[root@LinuxForensics Docs]# ls
DVD-Playing-HOWTO-html.tar Letter.doc MP3-HOWTO-html.tar.gz
Kernel-HOWTO-html.tar.gz Mikemsg.doc Sound-HOWTO-html.tar.gz
```

Sound-HOWTO-html.tar.gz

This was eight html files linked into a document titled "The Linux Sound HOW TO" This document basically outlines how to install a sound card in linux and basics in playing sound on Linux.

Kernel-HOWTO-html.tar.gz

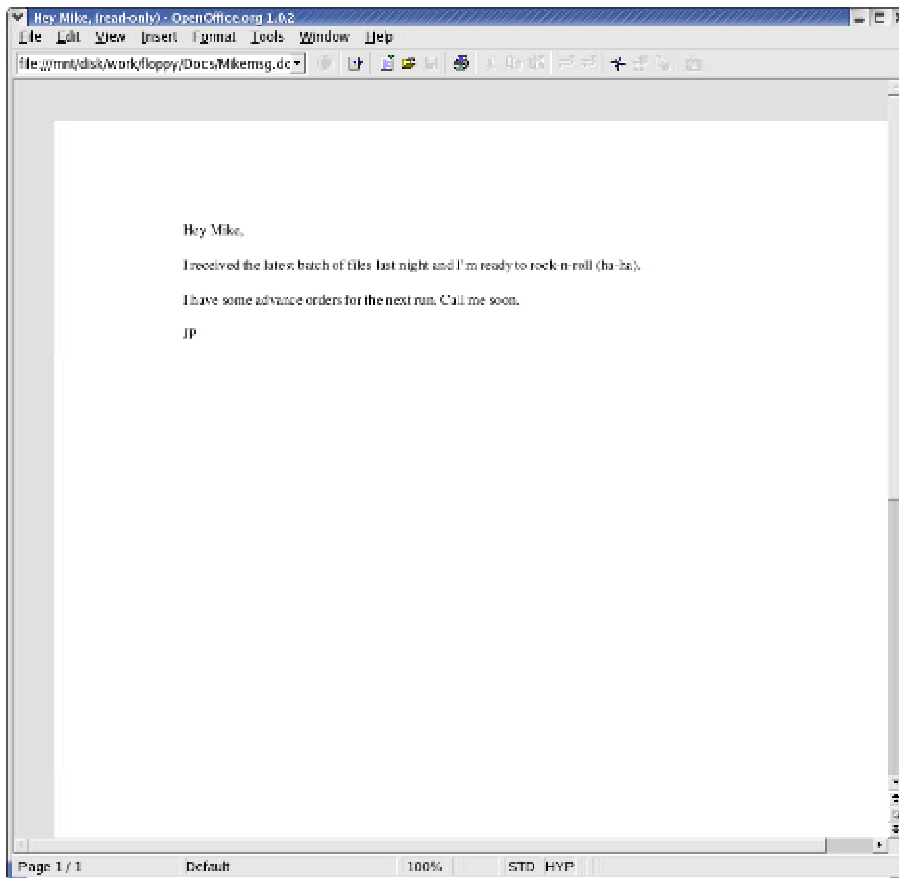
This document is the Linux Kernel HOWTO which outlines how to recompile the Kernel which could have been used in recompiling the bmap statically to create the prog binary found on the suspect floppy disk.

MP3-HOWTO-html.tar.gz

The purpose of this document is how to create, edit, manipulate, and stream mp3 files.

DVD-Playing-HOWTO-html.tar

A document on how to play DVD movies on Linux



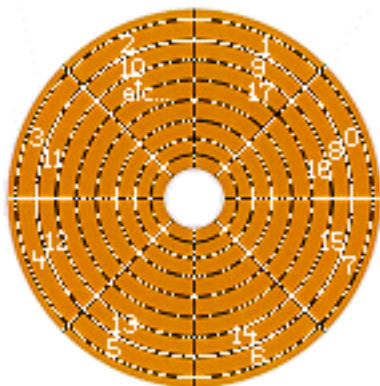
In the /John directory I found 2 graphics files these files were disk sector illustrations.

```
[root@LinuxForensics John]# ls -l
```

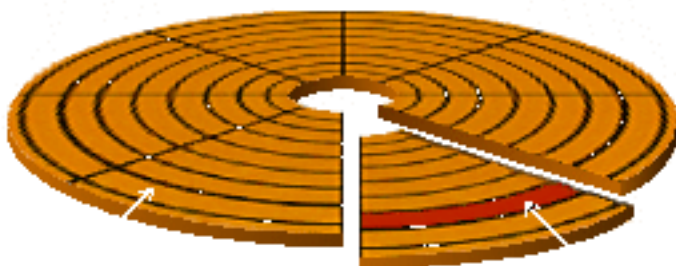
```
total 42
```

```
-rwxr-xr-x 1 502 502 19088 Jan 28 2003 sect-num.gif
-rwxr-xr-x 1 502 502 20680 Jan 28 2003 sectors.gif
```

sect-num.gif



sectors.gif



These illustrations seem to be demonstrating what a track is vs a sector could be graphics attached to one of the How to found.

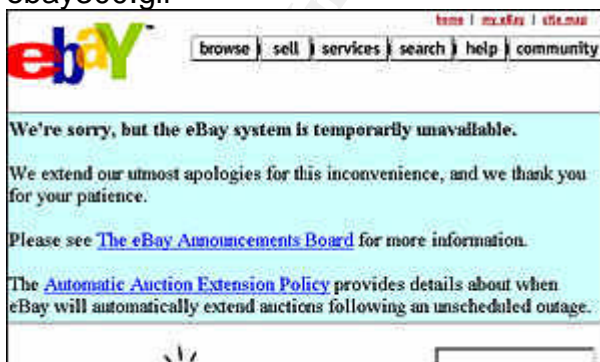
In the /May03 directory there was a graphics file called ebay300.jpg

```
[root@LinuxForensics May03]# ls -l
```

```
total 15
```

```
-rwxr-xr-x  1 502    502    13487 Jul 14  2003 ebay300.jpg
```

ebay300.gif



This file initially looked suspicious by it's name, but after viewing the file it was only a screen shot if an Ebay auction system announcement. It is possible that the graphic images contained steganography but I did not find evidence of this.

testfloppy:images/f1-160703-jp1.dd - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop http://localhost:9999/autopsy7func-z&mode-test&host-floppy&drv-unknown&img-images%2F160703-jp1.d&mnt-%2F Search Print

Home Bookmarks Red Hat Network Support Shop Products Training

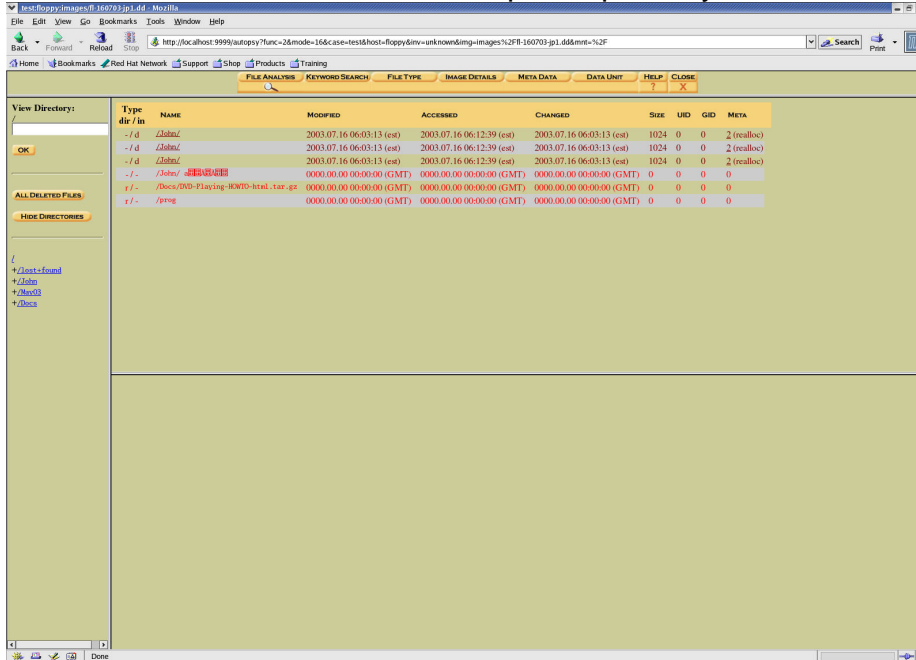
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE ? X

View Directory: /John/

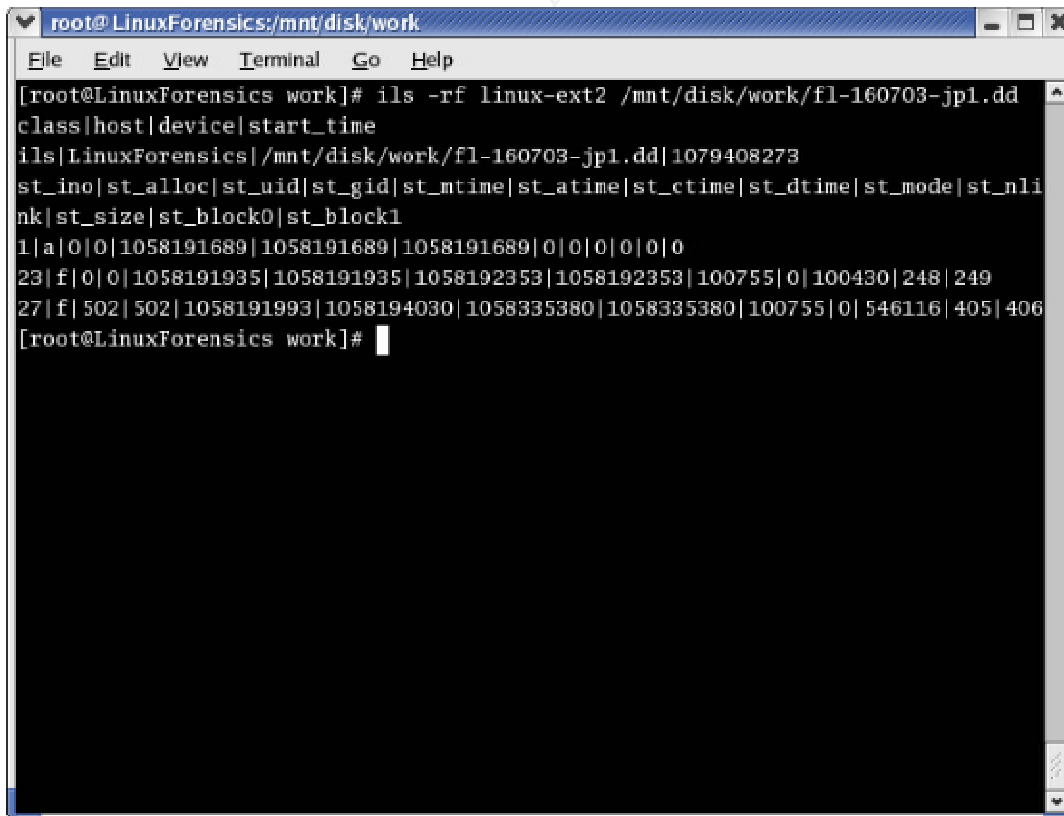
ADD NOTE GENERATE MD5 LIST OF FILES

DEL	Type	NAME	MODIFIED	ACCESSED	CHANGED	SIZE	UID	GID	META
		Error Parsing File (Invalid Characters?):							
		-d * 2(realloc): 2003.07.16 06:03:13 (est) 2003.07.16 06:12:39 (est) 2003.07.16 06:03:13 (est) 1024 0 0							
		Error Parsing File (Invalid Characters?):							
		-d * 2(realloc): 2003.07.16 06:03:13 (est) 2003.07.16 06:12:39 (est) 2003.07.16 06:03:13 (est) 1024 0 0							
		Error Parsing File (Invalid Characters?):							
		-d * 2(realloc): 2003.07.16 06:03:13 (est) 2003.07.16 06:12:39 (est) 2003.07.16 06:03:13 (est) 1024 0 0							
✓	-/-	sect-mm-gif	0000.00.00 00:00:00 (GMT)	0000.00.00 00:00:00 (GMT)	0000.00.00 00:00:00 (GMT)	0	0	0	0
	d/d	sect-mm-gif	2003.07.16 06:03:13 (est)	2003.07.16 06:12:39 (est)	2003.07.16 06:03:13 (est)	1024	0	0	2
	d/d	sect-mm-gif	2003.02.03 11:08:00 (est)	2003.07.16 06:09:35 (est)	2003.07.14 14:49:25 (est)	1024	502	502	12
	r/r	sect-mm-gif	2003.01.28 15:56:00 (est)	2003.01.28 15:56:00 (est)	2003.07.14 14:48:53 (est)	19088	502	502	24
	r/r	sect-px.gif	2003.01.28 15:56:00 (est)	2003.01.28 15:56:00 (est)	2003.07.14 14:48:53 (est)	20680	502	502	25

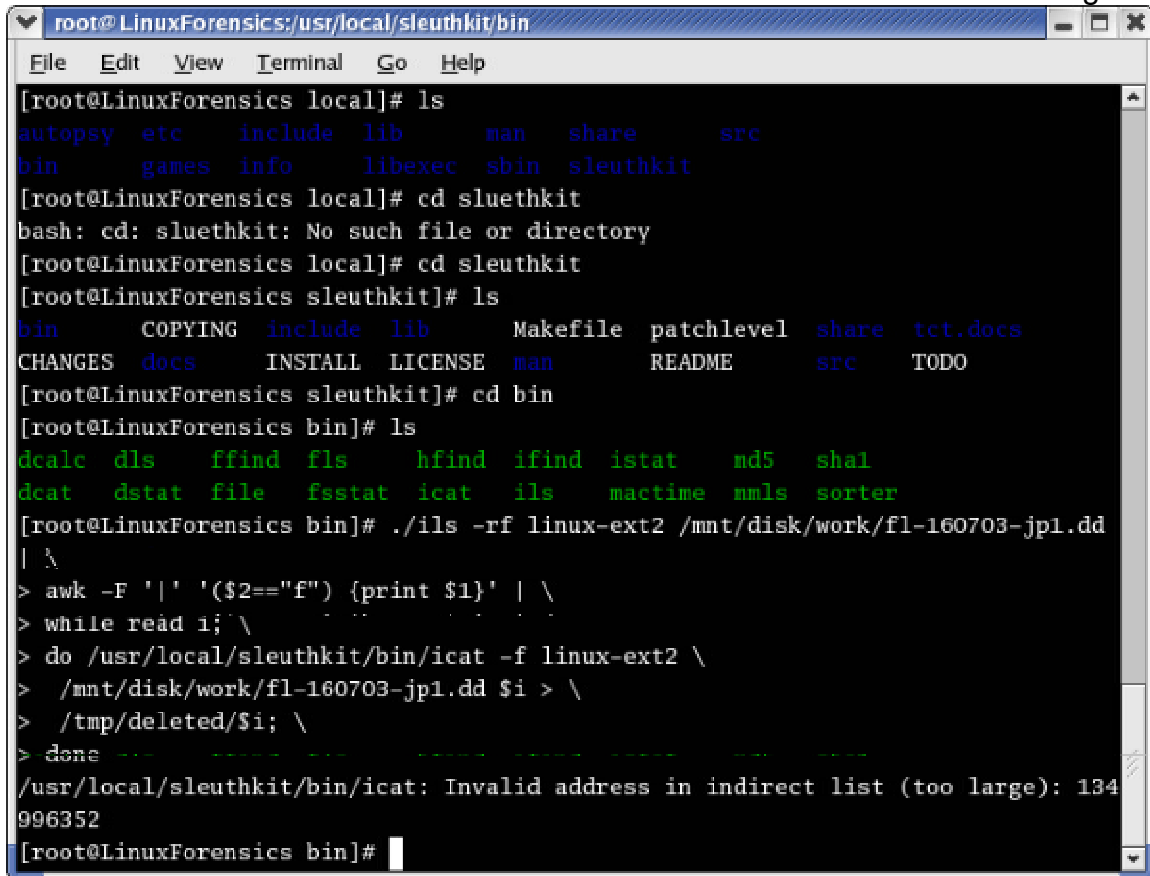
I ran a list of all deleted files and the strange entry is also there and all of the entries are unrecoverable. I suspect it possibly could be a hidden directory.



I then used individual commands in the Sleuthkit to attempt to get more information. I ran the ils command to find inodes of deleted files. I found 3 entries that were not detected by Autopsy.



I then used the icat command to extract the deleted files from the image.



```
root@LinuxForensics:/usr/local/sleuthkit/bin
File Edit View Terminal Go Help
[root@LinuxForensics local]# ls
autopsy  etc      include  lib      man      share    src
bin      games    info     libexec  sbin     sleuthkit
[root@LinuxForensics local]# cd sleuthkit
bash: cd: sleuthkit: No such file or directory
[root@LinuxForensics local]# cd sleuthkit
[root@LinuxForensics sleuthkit]# ls
bin      COPYING  include  lib      Makefile  patchlevel  share  tct.docs
CHANGES docs     INSTALL  LICENSE  man      README      src    TODO
[root@LinuxForensics sleuthkit]# cd bin
[root@LinuxForensics bin]# ls
dcalc  dls      ffind  fls      hfind  ifind  istat  nd5  sha1
dcat   dstat   file   fsstat  icat   ils    mactime  mmls  sorter
[root@LinuxForensics bin]# ./ils -rf linux-ext2 /mnt/disk/work/fl-160703-jp1.dd
| \
> awk -F '|' '($2=="f") {print $1}' | \
> while read i; \
> do /usr/local/sleuthkit/bin/icat -f linux-ext2 \
> /mnt/disk/work/fl-160703-jp1.dd $i > \
> /tmp/deleted/$i; \
> done
/usr/local/sleuthkit/bin/icat: Invalid address in indirect list (too large): 134996352
[root@LinuxForensics bin]#
```

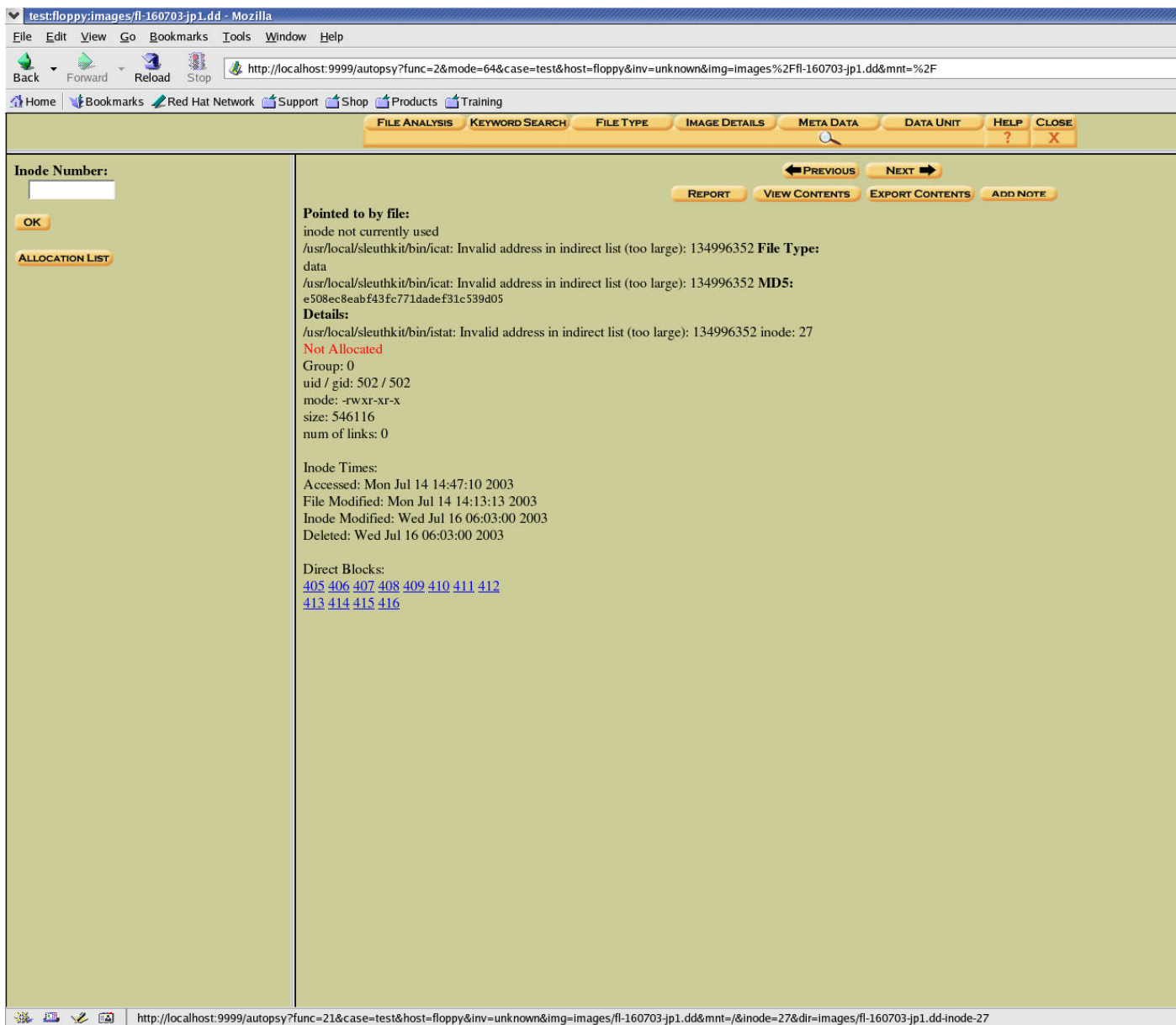
I was able to retrieve two files in this manner that I was not able to with Autopsy. However icat reported that Invalid address in indirect list (too large):134996352. Autopsy reports the same error. Of the two files I did retrieve one was a tar archive and the other was data. I copied the file from inode 23 to test.tar. I then ran tar -tvf to view the contents. It was a deleted copy of the DVD instructional document. I tried to identify the contents of the data file by renaming it with an .mp3 extension and using the Redhat media play and was not successful. Running strings on the file did not produce any useable clues.

© SANS

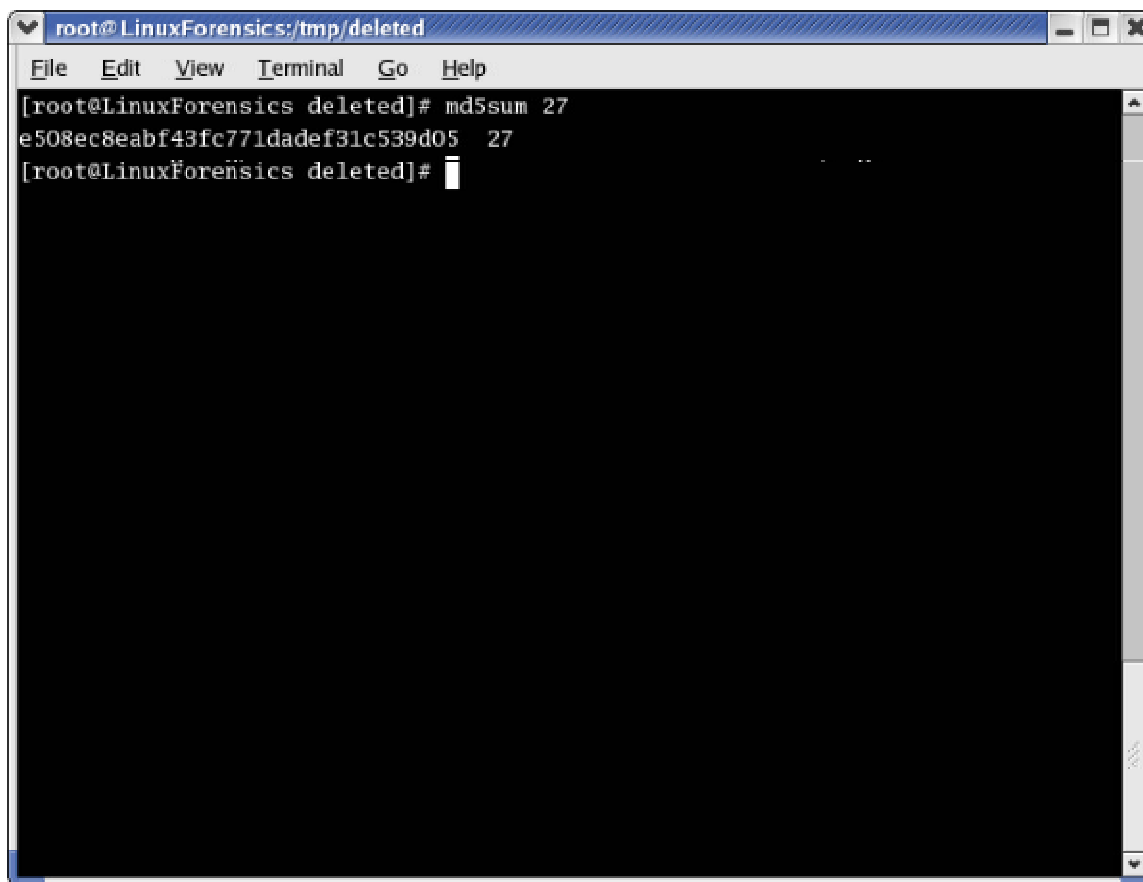
```
root@LinuxForensics:/tmp/deleted
File Edit View Terminal Go Help
[root@LinuxForensics root]# cd /tmp/deleted
[root@LinuxForensics deleted]# ls
23 27
[root@LinuxForensics deleted]# ls -l
total 116
-rw-r--r-- 1 root root 100430 Mar 15 22:47 23
-rw-r--r-- 1 root root 12288 Mar 15 22:47 27
[root@LinuxForensics deleted]# file 23
23: POSIX tar archive
[root@LinuxForensics deleted]# file 27
27: data
[root@LinuxForensics deleted]# cp 23 test.tar
[root@LinuxForensics deleted]# tar -tvf test.tar
-rw-r--r-- gferg/other 3256 2000-06-19 11:54:48 DVD-Playing-HOWTO-1.html
-rw-r--r-- gferg/other 994 2000-06-19 11:54:48 DVD-Playing-HOWTO-2.html
-rw-r--r-- gferg/other 2300 2000-06-19 11:54:48 DVD-Playing-HOWTO-3.html
-rw-r--r-- gferg/other 2763 2000-06-19 11:54:49 DVD-Playing-HOWTO-4.html
-rw-r--r-- gferg/other 1171 2000-06-19 11:54:49 DVD-Playing-HOWTO-5.html
-rw-r--r-- gferg/other 3599 2000-06-19 11:54:49 DVD-Playing-HOWTO-6.html
-rw-r--r-- gferg/other 3809 2000-06-19 11:54:50 DVD-Playing-HOWTO-7.html
-rw-r--r-- gferg/other 920 2000-06-19 11:54:50 DVD-Playing-HOWTO-8.html
-rw-r--r-- gferg/other 2092 2000-06-19 11:54:50 DVD-Playing-HOWTO.html
[root@LinuxForensics deleted]#
```

I then proceeded to examine inode 27 more closely. I ran a report on the file from Autopsy.

© SANS Institute 2004



The md5sum of the deleted file and recovered file from inode 27 match exactly. However, Autopsy is reporting the size of the file as 546116 bytes as opposed to the 12228 bytes extracted from the inode.

A terminal window titled 'root@LinuxForensics:/tmp/deleted'. The window has a menu bar with 'File', 'Edit', 'View', 'Terminal', 'Go', and 'Help'. The terminal content shows a command prompt '[root@LinuxForensics deleted]# md5sum 27' followed by the output 'e508ec8eabf43fc771dadef31c539d05 27'. Below the output is another prompt '[root@LinuxForensics deleted]#' with a cursor.

```
root@LinuxForensics:/tmp/deleted
File Edit View Terminal Go Help
[root@LinuxForensics deleted]# md5sum 27
e508ec8eabf43fc771dadef31c539d05 27
[root@LinuxForensics deleted]#
```

It seems the disk is a victim of what is called anti-forensics. Anti-forensics are techniques used to thwart forensic investigations. There are two types of anti-forensics data-hiding and data-destruction. I found an article on the Phrack Magazine site titled "Defeating Forensic Analysis on Unix". It looks like the technique that was used was to write data into bad blocks, thus hiding it. I suspect a tool called runefs was used to do this. I was unsuccessful in obtaining the tool. I attempted to extract it from the Phrack web site but the file was corrupted.

I ran debugfs with the -R (request) option which causes debugfs to execute the single command request.

```
[root@LinuxForensics work]# debugfs -R "stat <27>" /mnt/disk/work/fl-160703-jp1.dd
debugfs 1.35 (28-Feb-2004)
Inode: 27  Type: regular  Mode: 0755  Flags: 0x0  Generation: 22184
User: 502  Group: 502  Size: 546116
File ACL: 0  Directory ACL: 0
Links: 0  Blockcount: 1076
Fragment: Address: 0  Number: 0  Size: 0
ctime: 0x3f14ea94 -- Wed Jul 16 02:03:00 2003
atime: 0x3f12c26e -- Mon Jul 14 10:47:10 2003
mtime: 0x3f12ba79 -- Mon Jul 14 10:13:13 2003
dtime: 0x3f14ea94 -- Wed Jul 16 02:03:00 2003
BLOCKS:
```


(0-11):405-416, (IND):417, (12):134996352, (13):1157868407, (14):205912032, (15):1, (16):265831817, (17):201605, (18):-260732160, (19):326432389, (20):259312005, (21):266093963, (22):-2062921545, (23):-1719332910, (24):-2063597567, (25):-1961986826, (26):-2090410931, (27):251659385, (28):-37756, (29):-330986497, (30):242532485, (31):1725463947, (32):556931, (33):-11041777, (34):-158990337, (35):22709263, (36):-326959104, (37):-395286004, (38):-48552, (39):-997996919, (40):-1191803632, (41):3, (42):-13073393, (43):1166802943, (44):-1959753240, (45):46598229, (47):-2047849077, (48):-1957661495, (49):-1223697331, (50):-465239295, (51):-955496823, (52):-145682362, (53):1187448841, (54):264, (55):877053696, (57):104969999, (58):-2132509301, (59):251672636, (60):57220, (61):1370951424, (62):33161480, (63):-386823688, (64):-652, (65):-611990647, (66):11699471, (67):1300955136, (68):-1962803448, (69):-762975147, (70):34112527, (71):2106261504, (72):-1927312632, (73):56580, (74):-668401664, (75):12915853, (76):-956301312, (77):1359746628, (78):-1962407433, (79):-1223698355, (80):-465239295, (81):269894793, (82):135677127, (83):1, (84):873874631, (86):37861135, (87):-2132509301, (88):1946171452, (89):-662860985, (90):254938253, (91):50616247, (92):1157882965, (93):-50403100, (94):-947257345, (95):209059717, (96):-16220789, (97):27060487, (98):-158793728, (99):125098885, (100):1575547017, (101):-2080374870, (102):-397013780, (103):-35588, (104):-1995389821, (105):-29562376, (106):-158728193, (107):265833867, (108):-1929100873, (109):1157837332, (110):-1184962332, (111):-1058275329, (112):1443687555, (113):-9120792, (114):281314303, (115):334092425, (116):-1862270978, (117):266098059, (118):50873015, (119):-225844155, (120):-4638744, (121):-14358017, (122):-158728193, (123):-2062565243, (124):-354, (125):-136983, (126):7769599, (127):205764367, (128):-385874685, (129):344786955, (130):2055431682, (131):1519190271, (132):255096063, (133):-1912651081, (134):-1223737340, (135):972767812, (136):-1876659000, (137):-1929136369, (138):344801284, (139):2055431747, (140):1519190018, (141):252736514, (142):-1929231689, (143):-1223737340, (144):972964420, (145):1725789640, (146):251673475, (147):-126332, (148):330764287, (149):13960333, (150):687865856, (151):139299792, (152):-1056117629, (153):294192096, (154):1082583120, (155):-964034561, (156):-2081915509, (157):-159051580, (158):-1194560119, (159):3, (160):-2079377527, (161):-674, (162):266098059, (163):1157825207, (164):-733640220, (165):13649351, (166):-956301312, (167):51269, (168):-142016512, (169):12862919, (170):-1879048192, (171):-1949018741, (172):1166787661, (173):139758028, (174):-934442228, (175):423933711, (176):-531264766, (177):255853709, (178):58852535, (179):1301013573, (180):239372740, (181):-733640432, (182):-942914165, (183):17303620, (184):-956301312, (185):3409988, (186):-1962934272, (187):-1223702443, (188):-1962665404, (189):1015080013, (190):1282670600, (191):324318991, (192):30015750, (193):-386299448, (194):-1172, (195):544587909, (196):113788291, (197):952386947, (198):265307647, (199):-947715145, (200):-800769736, (201):-1070496132, (202):-214551, (203):7769599, (204):-15930237, (205):1642646645, (206):-2080374925,

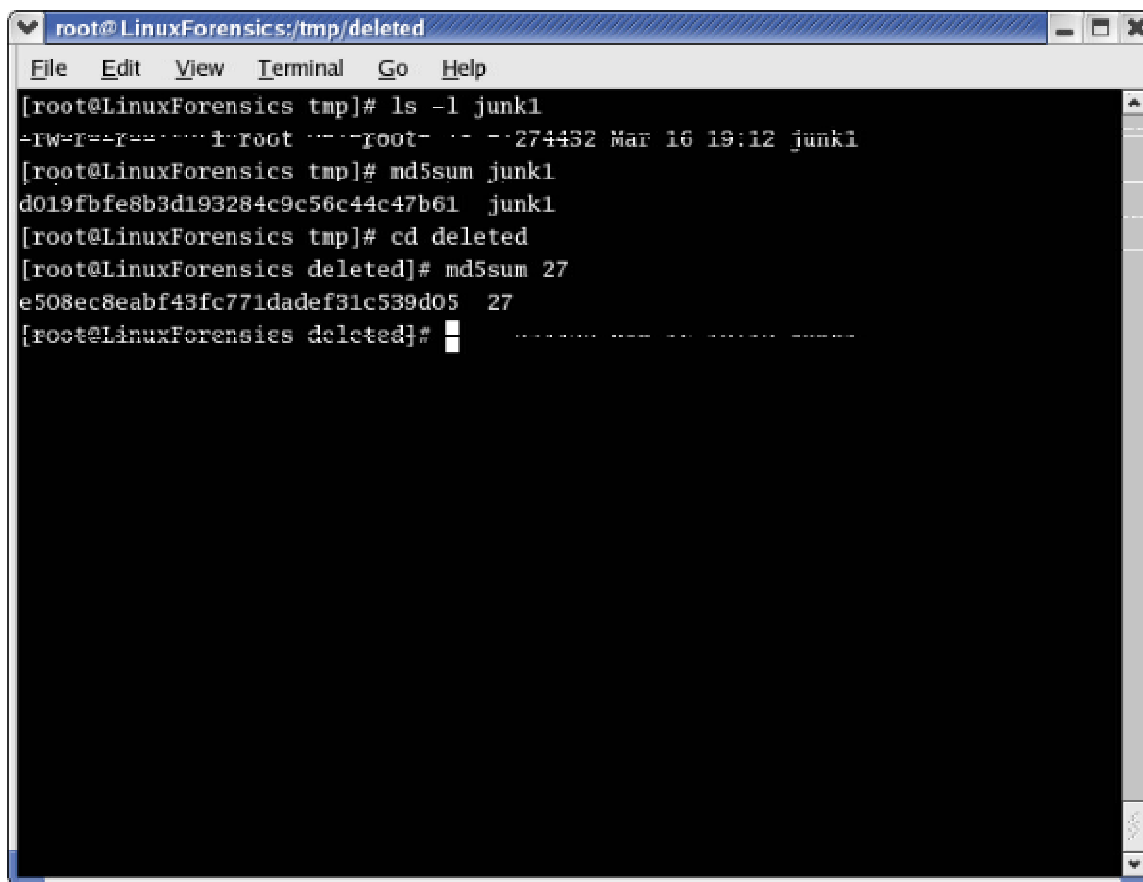
(207):1972048068, (208):-48371216, (209):-158728193, (210):264787339,
 (211):101926071, (212):-1981528829, (213):-1211963142, (214):-1259601921,
 (215):972060043, (216):-444264498, (217):-369098756, (218):-907, (219):-
 2082109099, (220):361433324, (221):134998272, (222):208982661, (223):13
 43024259, (224):-9234456, (225):281314303, (226):-158743607, (227):-
 2082109099, (228):227215596, (229):134996356, (230):343198085, (231):-
 15930237, (232):199819317, (233):1928521736, (234):-997982209, (235):-
 1866217200, (236):-16192381, (237):199327797, (238):3538696, (239):-
 402125847, (240):-27524, (241):-158735125, (242):-2082109099,
 (243):1166741740, (244):-1959723252, (245):855574613, (246):-8691736,
 (247):281314303, (248):-158743607, (249):1474660693, (250):-326937770, (
 251):-946313200, (252):-2006448123, (253):-1995961375, (254):1166929989,
 (255):-35106576, (256):-2097151680, (257):-1065021244, (258):10388495,
 (259):411762688, (260):1668602757, (261):-2096872565, (262):1954414328,
 (263):-15930237, (264):-1735727053, (265):-998047743, (266):-1983871728,
 (267):1534330947, (DIND):674, (IND):959606116

TOTAL: 268

I then ran fsgrab to try to piece together the file again. I was only able to recover the first 2 blocks. When I tried reading block 134996352 I received errors as indicated below.

```
[root@LinuxForensics work]# fsgrab -c 12 -s 405 /mnt/disk/work/fl-160703-jp1.dd
> /tmp/junk1
[root@LinuxForensics work]# fsgrab -c 256 -s 417 /mnt/disk/work/fl-160703-
jp1.dd > /tmp/junk1
[root@LinuxForensics work]# fsgrab -c 12 -s 405 /mnt/disk/work/fl-160703-jp1.dd
> /tmp/junk1
[root@LinuxForensics work]# fsgrab -c 256 -s 417 /mnt/disk/work/fl-160703-
jp1.dd >> /tmp/junk1
[root@LinuxForensics work]# fsgrab -c 1 -s 134996352 /mnt/disk/work/fl-160703-
jp1.dd >> /tmp/junk1
fsgrab: /mnt/disk/work/fl-160703-jp1.dd: warning: unexpected end of file after 0
chars
[root@LinuxForensics work]# fsgrab -c 256 -s 134996352 /mnt/disk/work/fl-
160703-jp1.dd >> /tmp/junk1
fsgrab: /mnt/disk/work/fl-160703-jp1.dd: warning: unexpected end of file after 0
chars
```

I suspect there was anti-forensics with all of the negative block numbers. I was able to recover 272432 bytes. I ran strings on the file and I got data relating to the prog binary which also showed up as deleted and unrecoverable in Autopsy. I compared md5sums on junk1 and 27 which I recovered earlier and they did not match.

A terminal window titled 'root@LinuxForensics:/tmp/deleted'. The window contains the following commands and output:

```
[root@LinuxForensics tmp]# ls -l junk1
-rw-r--r-- 1 root root 274432 Mar 16 19:12 junk1
[root@LinuxForensics tmp]# md5sum junk1
d019fbfe8b3d193284c9c56c44c47b61  junk1
[root@LinuxForensics tmp]# cd deleted
[root@LinuxForensics deleted]# md5sum 27
e508ec8eabf43fc771dade31c539d05  27
[root@LinuxForensics deleted]#
```

Since the suspect's computer was wiped I suspect he also ran a utility like `runefs` to hide the data or a utility like the defiler's toolkit also talked about in the Phrack article to sanitize the data.

If there was a backup to Price's computer it may be possible to track the owner of the file back to Price. If user id 502 is the standard user id in the work place it may be possible to leverage that as potential evidence and in any questioning. The last time `prog` was run was most likely July 16th at 2:12AM. Again because the binary was found on a floppy I cannot conclusively determine on what system the binary was executed. Since the floppy was found in Price's computer there is reasonable suspicion that computer was the last system it was run on.

Additional Information

<http://www.forinsect.de/forensics/forensics-tools.php>
http://www.its.bldrdoc.gov/projects/devglossary/_mp3.html
http://www.linuxsecurity.com/feature_stories/data-hiding-forensics.html
<http://build.lnx-bbc.org/packages/fs/bmap.html>
<http://www.e-evidence.info/other.html>
<http://www.phrack.org/show.php?p=59&a=6>

Legal Resources

<http://www.riaa.com/issues/copyright/laws.asp#uscopyright>
<http://www.cybergov.gov>

Part2 Option 1 Perform Forensic Analysis on a System

Synopsis of Case Facts

A system in our MIS department has been exhibiting some strange behavior including the inability to be updated remotely and remote administrator functions are being denied. The workstation runs middleware between our administrative system, a VMS Alpha cluster and a Windows 2000 server running SQL. The system is set to be replaced but is currently critical to MIS operations and our Associate VP has requested it be kept online unless it is deemed absolutely necessary to take it offline. I was asked by my supervisor to do a forensics exam and give him a risk assessment. We have good evidence that the system has been previously compromised. It has been previously infected with the "My Doom" virus and possibly one other virus or trojan which was cleaned by the systems staff. The network environment at my Institution is open to the internet. while some key at-risk ports are blocked there is still no real firewall implemented yet in our enterprise. The current desktop workstations have been implemented without many standards and very loose security procedures. There have been many systems compromised especially Windows 2000 systems. Standard Operating Procedure thus far has been to format and reload the potentially compromised system, however, in this case we are going to do that only if absolutely necessary. Goals of the investigation:

- Perform an initial evaluation to ascertain if the system has been compromised.
- Determine inconclusively whether the system has been compromised and exactly how.
- Establish a timeline
- Retrieve any suspicious files or malware.
- Submit a report to management with recommendations for a decision on whether the replacement of the system is to be accelerated.

Approach

- Gather evidence while system is still online.
- With the assistance of the network department monitor network traffic to ascertain if there is any suspicious network traffic.
- Analyze evidence in laboratory conditions to assess and investigate the system for wrongdoing

System Description

The system is Dell GX110 Running Microsoft Windows 2000 Professional with SP 4. The system's primary use is to run the Connx Data Synchronization software and Ascential Software's DataStage product. Connx Data Sync product provides a data connector between our VMS cluster running SCT's Plus product for FRS (Financial Record System), HRS (Human Resource Record System) and SIS (Student Information System). Ascential's DataStage product's function is to transform data from formats like Cobol, JCL, etc..... For further information on these products I have included the websites of the vendors in my useful links section.

The suspect system has 512 megs of ram and a 10gb hard drive. Currently, there are 3 MIS employees who have access to this system, the DBA and two programmers. At this time there is no reason to suspect any wrong doing on their part. Since almost all of our corporate data runs through this system there are huge implications of this system being compromised. Part of the problem is critical systems are just thrown together without regard for security or maintenance. The system was originally installed Feb of 2003, but antivirus software was not installed on the system until July of 2003 after being infected with the My Doom virus.

Hardware

Since the system itself must be kept running and cannot be seized I used a hard drive to store the image. This method is just as good in maintaining the chain of evidence. In the event this case is prosecuted criminally I would turn the hard drive sealed and signed by myself, and receiving a receipt from the law enforcement agency.

Evidence ID	Tag 001
Make	Dell
Model	GX110
Serial Number	73S2XXX (Masked Intentionally)
Drives	Maxtor Model 51024H2 10.2 GB IDE Hard Drive
	A: 3.5" 1.44 MB Floppy Drive
	250MB Zip Drive
	DVD 48X CD Rom
Memory	512 MB
Modem	No
Nic	3-Com 3C905C-TX 10/100 Ethernet RJ-45
USB	2
Serial Port	2-9Pin
Parallel Port	1-RS232
Microphone	1-Mini Phono

Speaker	1- Mini Phono
Mouse	PS2
Keyboard	PS2
Video	Standard VGA Adapter

Evidence ID	Tag 002
Make	Western Digital
Model	WD200
Serial #	WCAFD168XXXXX
Description	20.08 GB Hard Drive used to store Gathered Evidence.

Image Media

Since the system is live and cannot be taken offline, there are some steps that need to be taken to insure the forensic integrity of the evidence. Care must be taken to insure the minimum is done to change the state of the system. My plan is to use my incident response CD to run the dd command and copy the images to a SMB share to one of my forensics machines. For purposes of the investigation I will be using 3 pieces of equipment.

System 1: Dell Latitude C-810 laptop with a P III 1.2 GHz processor, 512mb RAM and 2 hard drives a 30GB internal drive and a 18GB removable expansion bay drive. This system is running Redhat Linux 9 and Vmware 4. Laptop is portable and allows for on-site investigations and portability to be mobile between lab and jobsite.

System 2: Dell Optiplex GX110 P III 667 MHz processor 512 MB ram and 2 hard drives both 20GB, one as a system drive and the second to be removed from the system to be secured as the evidence disk. This system is running Windows 2000 Server SP4.

System 3: Dell Optiplex GX240 P4 2 GHz Processor 1MB Ram 1 60 GB hard drive and 1 20 GB hard drive. The system is running Redhat Linux 9 and VM Ware. System also to be used for examination because it has more power than the laptop and will be used for intense searches and computations.

Before imaging the media of the suspect workstation, the media where the image is to be stored must be sterilized. For capturing this media I will be using two storage devices.

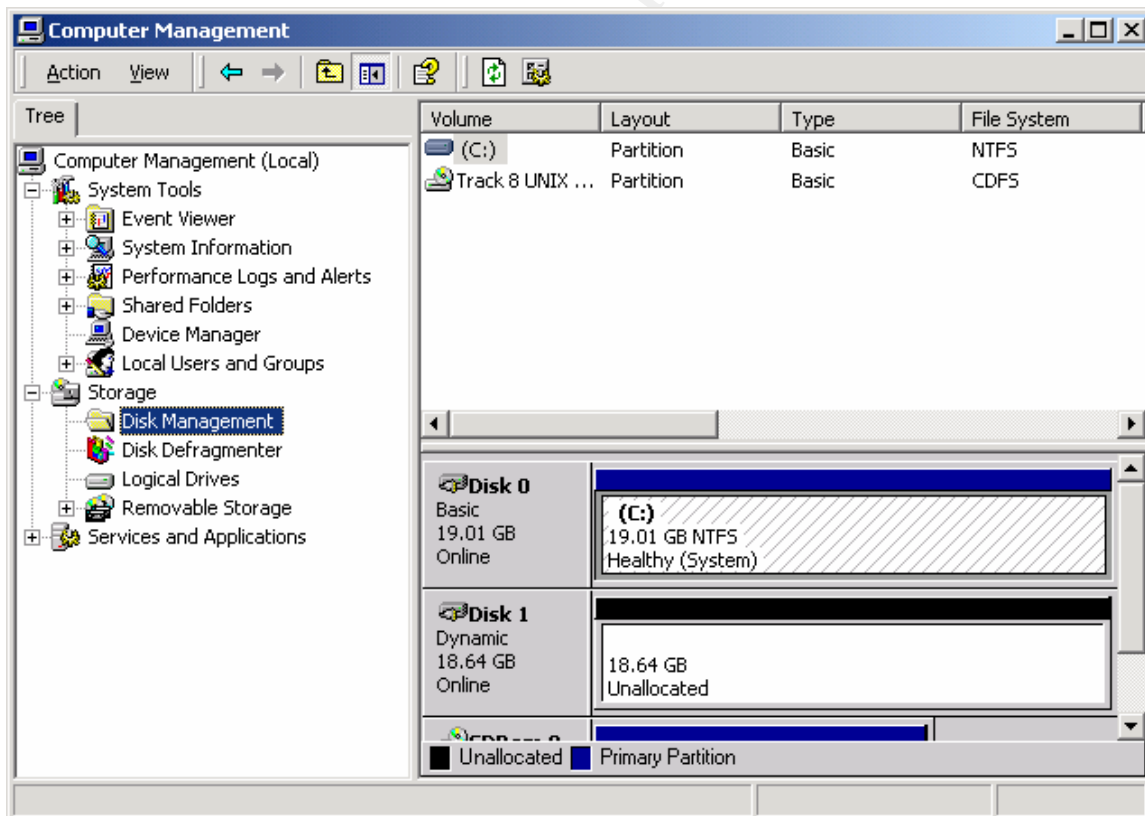
- a) A 20 GB Western Digital hard drive currently connected to system 2 the image will be transferred using the dd command and disconnected to be stored in a secure area in a sealed envelope in the evidence safe which myself and my supervisor have the combination.
- b) A 18GB Dell expansion bay hard drive currently connected to system 1. The image will be transferred from system 2 before disconnection. This is

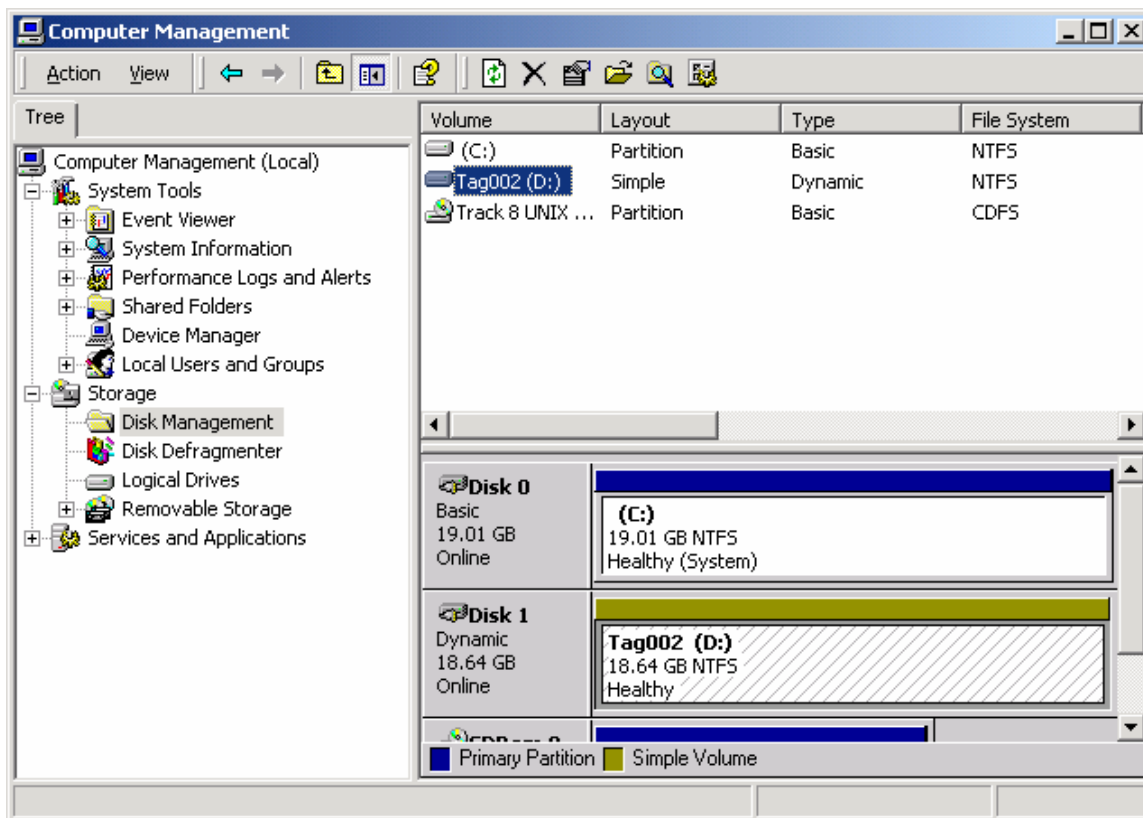
done to maintain the chain of evidence and to work from a copy of the evidence not the actual evidence itself.

Sterilization of Media System 2:

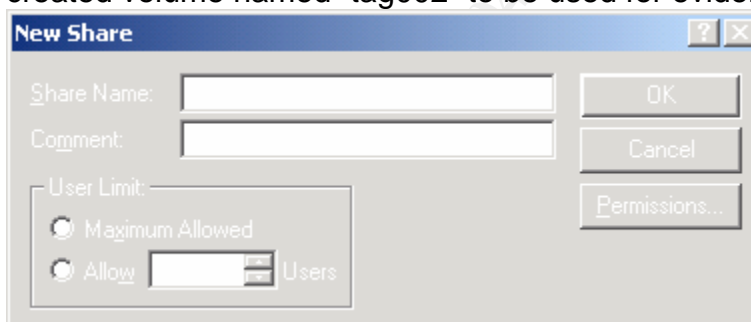
From my incident response CD I ran the wipe command on the 20GB Western Digital hard drive. Wipe is included in the Forensic Acquisition Utilities by George M. Garner Jr. The documentation states that “wipe.exe is an original utility to sterilize media prior to forensic duplication.” According to page 66 of volume 8.4 of the SANS forensic textbook “It will wipe standard disk files, alternate streams and tapes in addition to logical volumes and disk drives. Files, drives, volumes, streams and directories are wiped by writing successively FF, random data and zeros to the object being wiped.”

As indicated below I ran the wipe command with no switches to physicaldrive1. The program proceeded to write FF, random and zero bits to the device. I deleted the original wiped partition because it was un-writeable in this state and created a clean 19092MB simple volume partition and formatted it with NTFS. I labeled the volume Tag002.





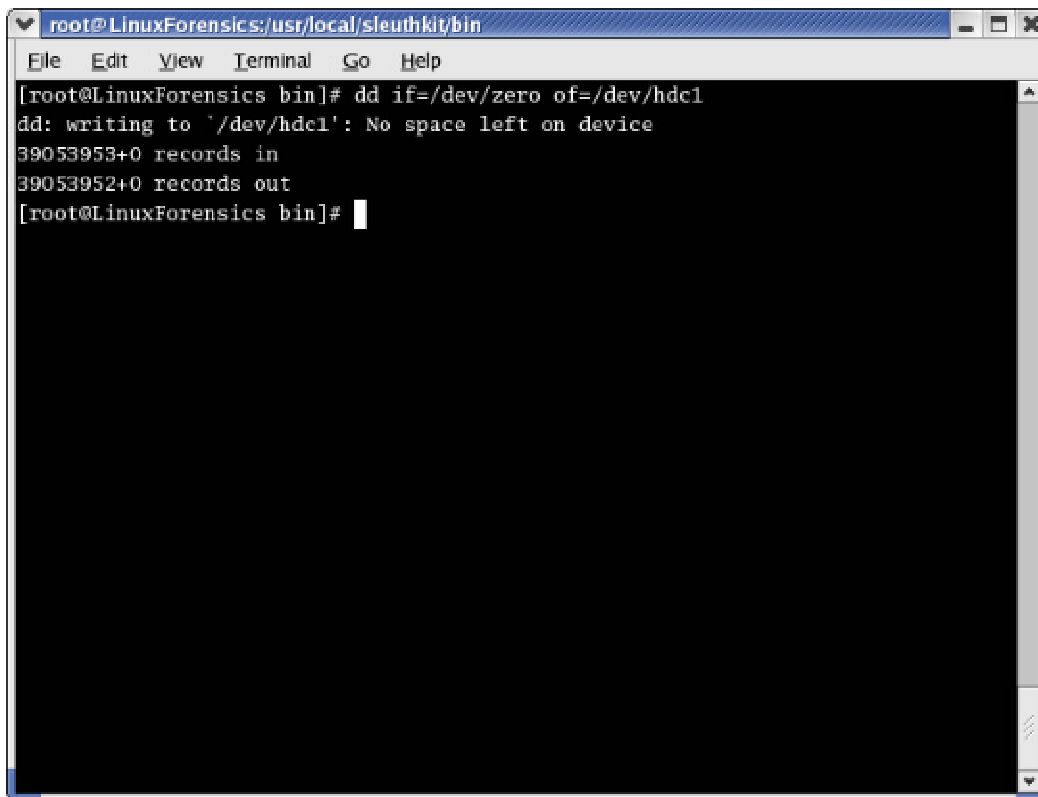
I created a share on the system called forensics, which shared the newly created volume named "tag002" to be used for evidence collection.



System 2 is now ready to receive the images of the suspect workstation.

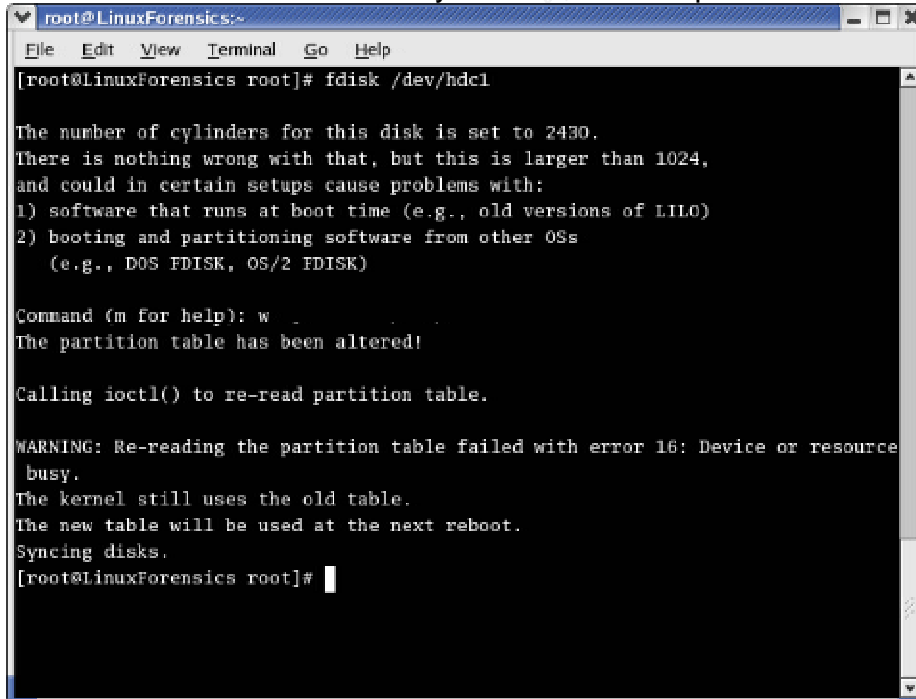
Sterilization of Media System 1.

Since this was a Linux system I used the dd command to write zeros to the 18 gig expansion bay hard drive to be used to store the working copy of the images for the investigation. DD is utility that reads input block by block. DD can also be used to write an entire device with zeros to sterilize a device. As indicated below I sterilized the device-designated hdc1, the 18GB expansion hard drive connected to System 1.

A terminal window titled 'root@LinuxForensics:/usr/local/sleuthkit/bin'. The window has a menu bar with 'File', 'Edit', 'View', 'Terminal', 'Go', and 'Help'. The terminal output shows the command '[root@LinuxForensics bin]# dd if=/dev/zero of=/dev/hdc1' being executed. The response is 'dd: writing to `/dev/hdc1': No space left on device', followed by '39053953+0 records in' and '39053952+0 records out'. The prompt returns to '[root@LinuxForensics bin]#'.

```
root@LinuxForensics:/usr/local/sleuthkit/bin
File Edit View Terminal Go Help
[root@LinuxForensics bin]# dd if=/dev/zero of=/dev/hdc1
dd: writing to `/dev/hdc1': No space left on device
39053953+0 records in
39053952+0 records out
[root@LinuxForensics bin]#
```

I then used the fdisk command to create a partition which will be mounted as /mnt/disk1. I rebooted the system to flush the partition table.

A terminal window titled 'root@LinuxForensics:~'. The window has a menu bar with 'File', 'Edit', 'View', 'Terminal', 'Go', and 'Help'. The terminal output shows the command '[root@LinuxForensics root]# fdisk /dev/hdc1' being executed. The response is 'The number of cylinders for this disk is set to 2430. There is nothing wrong with that, but this is larger than 1024, and could in certain setups cause problems with: 1) software that runs at boot time (e.g., old versions of LILO) 2) booting and partitioning software from other OSs (e.g., DOS FDISK, OS/2 FDISK)'. The prompt returns to '[root@LinuxForensics root]#'.

```
root@LinuxForensics:~
File Edit View Terminal Go Help
[root@LinuxForensics root]# fdisk /dev/hdc1

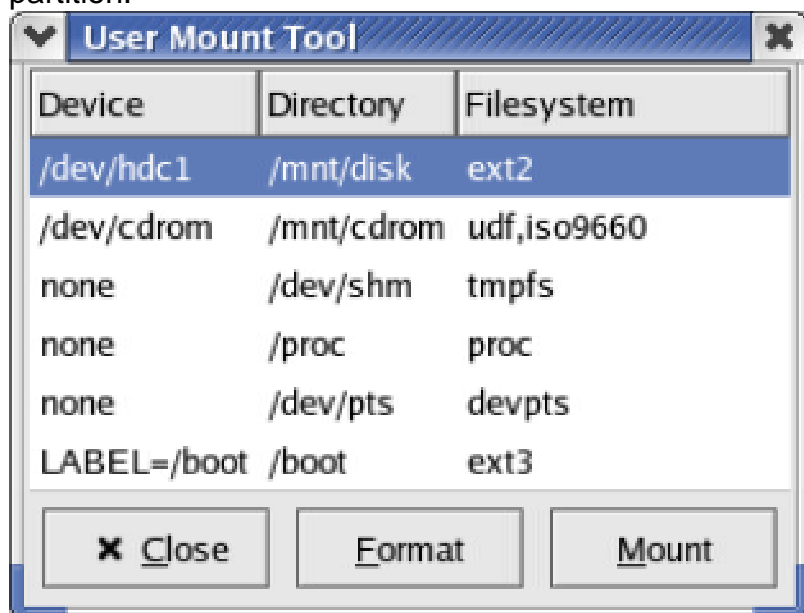
The number of cylinders for this disk is set to 2430.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
 1) software that runs at boot time (e.g., old versions of LILO)
 2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource
busy.
The kernel still uses the old table.
The new table will be used at the next reboot.
Syncing disks.
[root@LinuxForensics root]#
```

I then used the Gnome User Mount Tool to reformat and mount the partition.



I ran the `df -k` command to verify that the partition is indeed mounted.

```
root@LinuxForensics:~  
File Edit View Terminal Go Help  
[root@LinuxForensics root]# df -k  
Filesystem            1K-blocks    Used Available Use% Mounted on  
/dev/hda3              27680468 15978868 10295512  61% /  
/dev/hda1              124427    9405   108598    8% /boot  
none                   256892      0   256892    0% /dev/shm  
[root@LinuxForensics root]# df -k  
Filesystem            1K-blocks    Used Available Use% Mounted on  
/dev/hda3              27680468 15979888 10294492  61% /  
/dev/hda1              124427    9405   108598    8% /boot  
none                   256892      0   256892    0% /dev/shm  
/dev/hdc1             19220500     20 18244132    1% /mnt/disk  
[root@LinuxForensics root]#
```

System 1 is now ready to receive the working copy of the suspect image.

Capturing Image.

As I indicated above there are advantages and disadvantages to performing an examination of a running system. The advantages are that the examiner will be able to gather volatile memory such as memory, the contents of the swap file and running processes. The disadvantage is that anything that is done to the system will change the system. I will touch the system as minimally as possible to insure the integrity of the system. I will carefully note any procedures that I perform on the live image. Also to preserve the state of the system I will not be getting screen shots on the suspect workstation.

I used the dd command to image the suspect system and create an md5sum of the file and an md5 file. The command to image the machine I used was.

```
"dd if=\\.\c: of=\\130.XX.X.143\forensics\odshd.img -md5sum -verifymd5 -md5out=\\130.XX.X.143\forensics\odshd.md5"
```

I was asked to enter my network credentials to access the share on the forensic station. Following this procedure and not mapping a drive there is very minimal information being changed on the suspect system that would alter its state. Most notably would be key strokes.

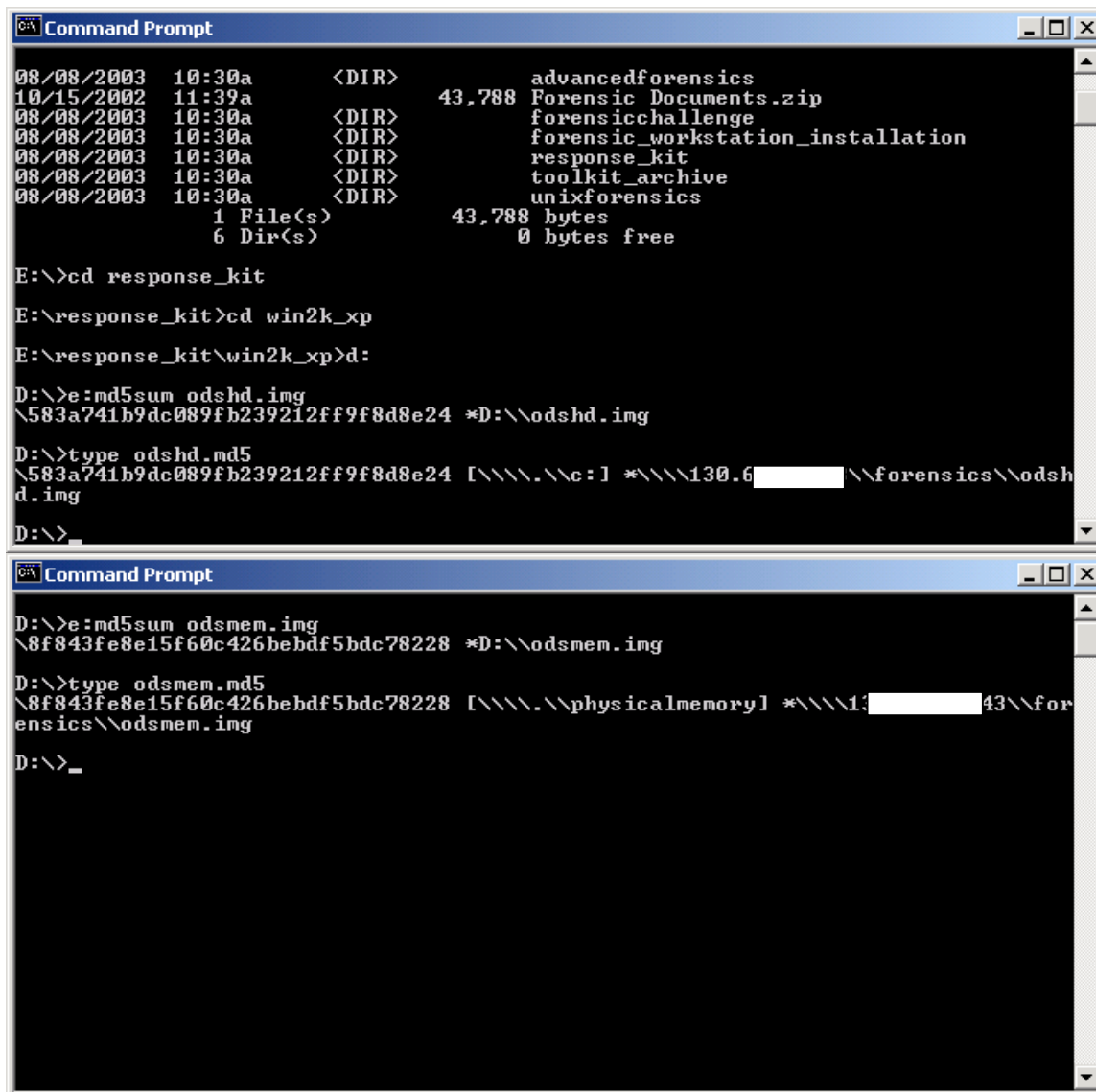
The dd command will perform a bit level image of the system and save the image file to a SMB share on another system, which contains the sterilized media, and then it will also calculate an md5 algorithm of the image and verify that md5 algorithm. So, the image file may be verified during the investigation and in a court of law if necessary.

The dd process completed successfully with 2496091+0 records in and 2496091+0 records out. The output of the dd command also returned that the checksums do match.

I then used the dd command to copy the contents of the volatile system memory and calculate an md5sum. The command syntax I used was:
"dd if=\\.\physicalmemory of=\\130.XX.X.143\forensics\odsmem.img -md5sum -verifymd5 -md5out=\\130.XX.X.143\forensics\odsmem.md5"

The operation completed successfully with 130733+0 records in and 130733+0 records out. The checksums do match.

From System 2 I used the md5sum command from my incident response CD to verify the md5sum of the images I just created. Both the hard disk image and memory image checksums matched as indicated below. I verified this by running md5sum against the images and compared them to the contents of the md5 files.



```
08/08/2003 10:30a <DIR> advancedforensics
10/15/2002 11:39a 43,788 Forensic Documents.zip
08/08/2003 10:30a <DIR> forensicchallenge
08/08/2003 10:30a <DIR> forensic_workstation_installation
08/08/2003 10:30a <DIR> response_kit
08/08/2003 10:30a <DIR> toolkit_archive
08/08/2003 10:30a <DIR> unixforensics
                1 File(s)      43,788 bytes
                6 Dir(s)        0 bytes free

E:\>cd response_kit
E:\response_kit>cd win2k_xp
E:\response_kit\win2k_xp>d:
D:\>e:md5sum odshd.img
\583a741b9dc089fb239212ff9f8d8e24 *D:\odshd.img

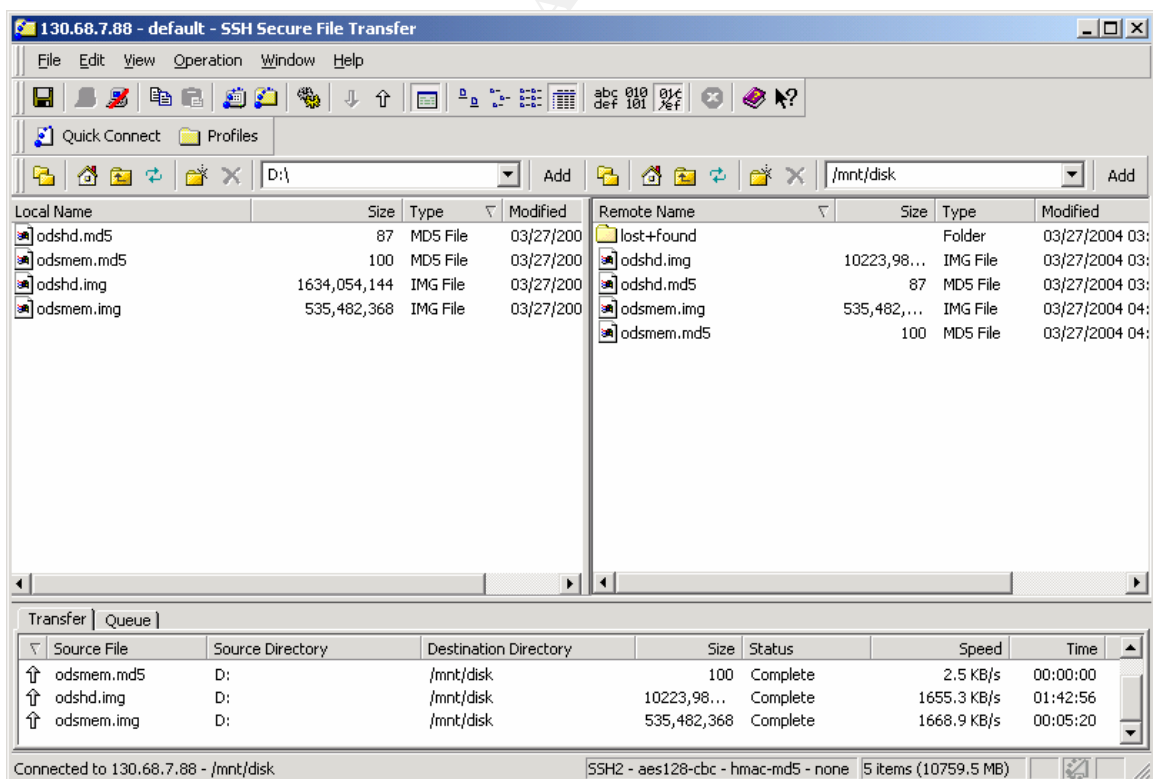
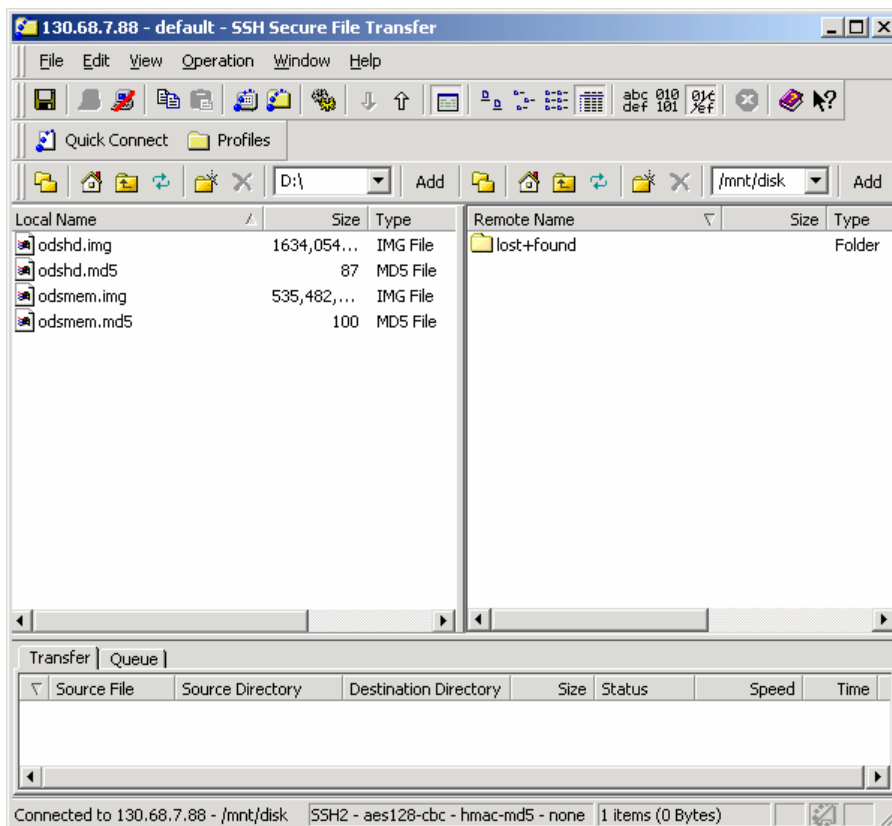
D:\>type odshd.md5
\583a741b9dc089fb239212ff9f8d8e24 [\\.\c:] *\\130.6[redacted] \forensics\odsh
d.img
D:\>_

D:\>e:md5sum odsmem.img
\8f843fe8e15f60c426bebdf5bdc78228 *D:\odsmem.img

D:\>type odsmem.md5
\8f843fe8e15f60c426bebdf5bdc78228 [\\.\physicalmemory] *\\1[redacted]43\for
ensics\odsmem.img
D:\>_
```

Now that the evidence has been verified I then used sftp which is part of the SSH protocol to copy the working copies of the hard drive image and memory contents image and corresponding md5 files from system 2 to system 1. Because of the security on system 2 I needed to add system 1 to the exception list in IPsec. IPsec is configured on our Windows hosts for host level IP security above our firewall.

I used the SSH Secure Shell Windows client version 3.2.0 to upload the working data to the sanitized media on System 1. Secure copy is sometimes an easier way to move files between hosts. SSH has a port for almost every OS and is a more secure copy method than FTP or Windows SMB.



I changed the permissions to the image files to read only.

```

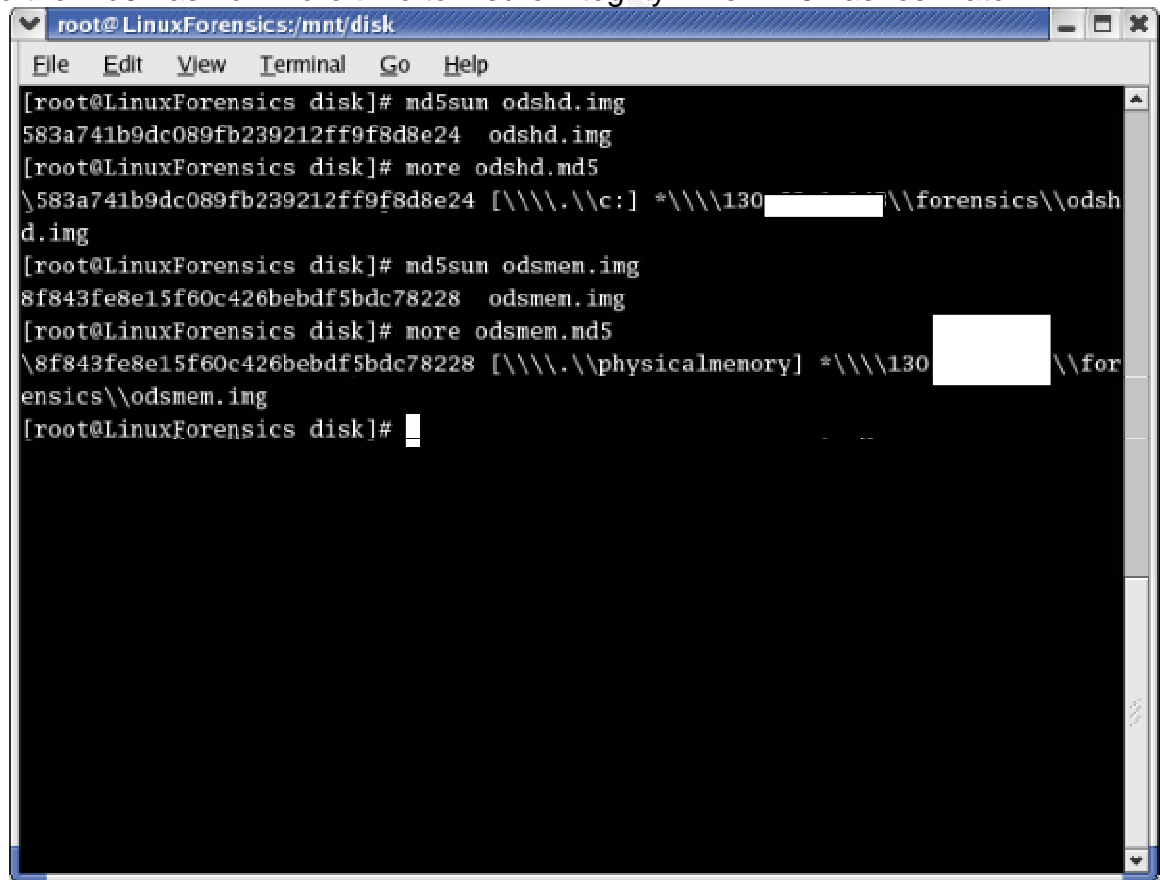
-r----- 1 root  root  10223988736 Mar 27 15:48 odshd.img
-r----- 1 root  root    87 Mar 27 15:48 odshd.md5
-r----- 1 root  root  535482368 Mar 27 16:28 odsmem.img
-r----- 1 root  root   100 Mar 27 16:28 odsmem.md5

```

I powered down system 2 and removed physicaldrive1 the Western Digital 20 GB hard drive. I tagged the evidence Tag002 and noted the case date contents. I also noted all of the file sizes and md5 sums on a piece of paper and placed it in the envelope with the gathered evidence. I sealed and signed the back of the envelope and put the evidence in my safe.

Media Analysis of System

Back in my forensic lab I powered up System 1, my Dell C810 laptop and verified the md5 hash on more time to insure integrity. The MD5 hashes match.



```

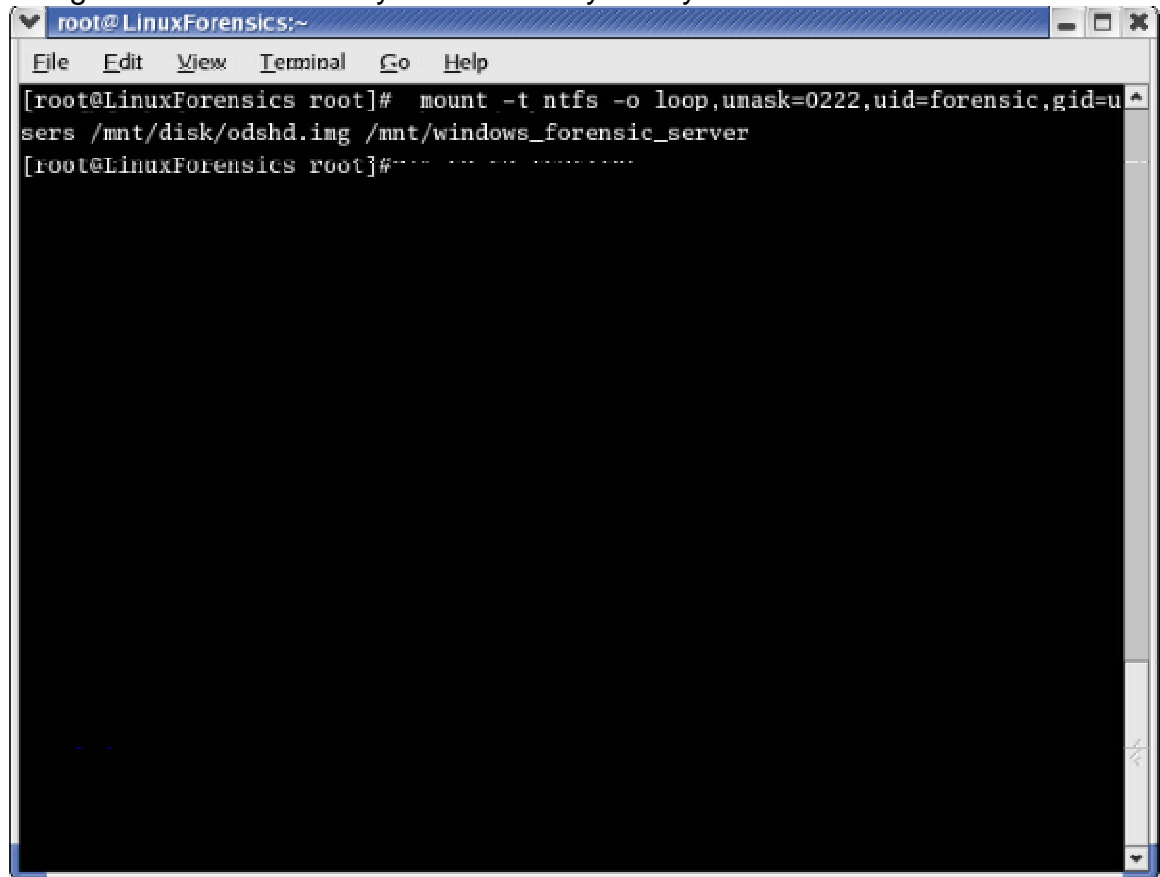
root@LinuxForensics:/mnt/disk
File Edit View Terminal Go Help
[root@LinuxForensics disk]# md5sum odshd.img
583a741b9dc089fb239212ff9f8d8e24 odshd.img
[root@LinuxForensics disk]# more odshd.md5
583a741b9dc089fb239212ff9f8d8e24 [\\.\c:] *\\.\130 [redacted] \\forensics\odshd.img
[root@LinuxForensics disk]# md5sum odsmem.img
8f843fe8e15f60c426bebd5bdc78228 odsmem.img
[root@LinuxForensics disk]# more odsmem.md5
8f843fe8e15f60c426bebd5bdc78228 [\\.\physicalmemory] *\\.\130 [redacted] \\forensics\odsmem.img
[root@LinuxForensics disk]#

```

Image Part 1: File System

The suspect hard disk was formatted NTFS. I used Autopsy to perform my file analysis. Autopsy is an graphic interface of the Sleuthkit and was written by Brian Carrier. This tool was chosen because it is freely available and widely recognized in the computer forensic community. I opened the image file in

Autopsy for an initial examination. The first thing that glared at me is NTDetect and Ntldr were replaced. I could have been from service packs and hotfixes but worth noting. I mounted the file system read only on my forensic station.

A screenshot of a Linux terminal window titled 'root@LinuxForensics:~'. The window has a menu bar with 'File', 'Edit', 'View', 'Terminal', 'Go', and 'Help'. The terminal shows the following command and its output: [root@LinuxForensics root]# mount -t ntfs -o loop,unask=0222,uid=forensic,gid=users /mnt/disk/odshd.img /mnt/windows_forensic_server [root@LinuxForensics root]#

```
root@LinuxForensics:~
File Edit View Terminal Go Help
[root@LinuxForensics root]# mount -t ntfs -o loop,unask=0222,uid=forensic,gid=users /mnt/disk/odshd.img /mnt/windows_forensic_server
[root@LinuxForensics root]#
```

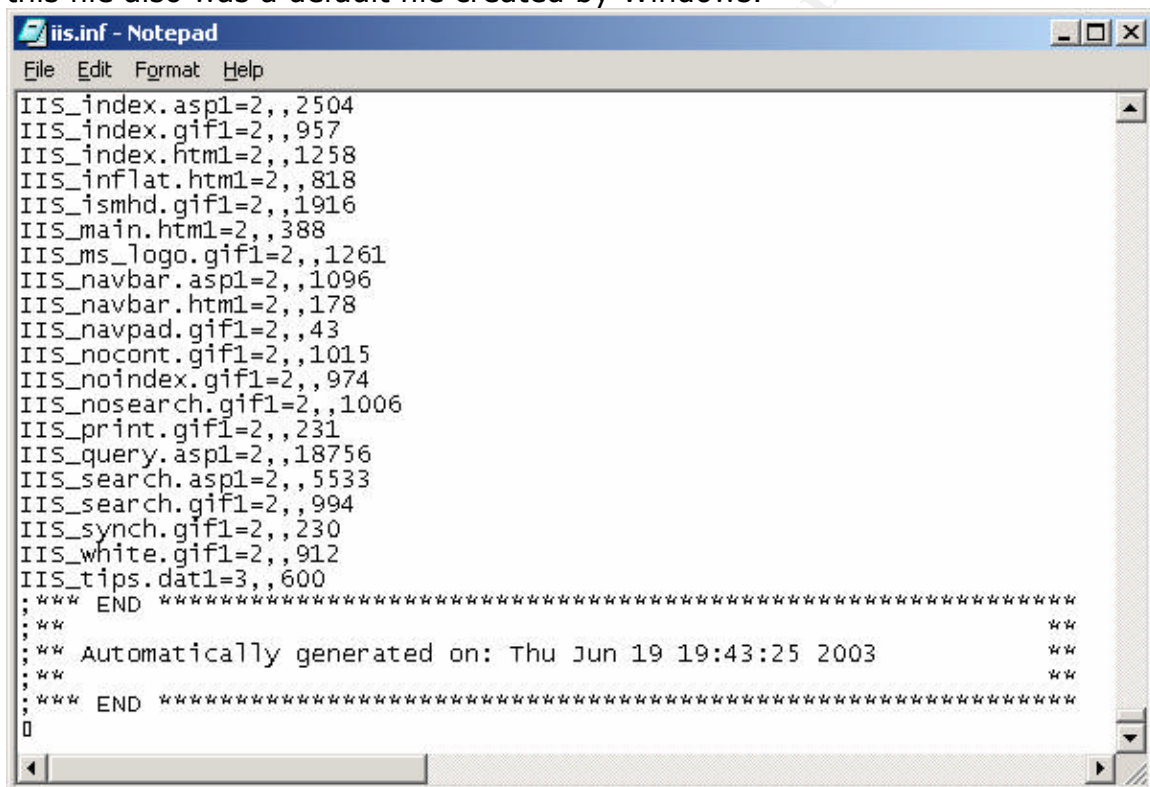
As indicated above. I mounted the image using the Linux mount command with the loop option which allows me to mount a dd image. I used /mnt/windows_forensic_server to mount the image. This mountpoint is configured as a share in my Samba configuration.

I accessed the file system through the Samba windows share. I performed a search for *.log. One important fact to note The security log was empty. Most likely there was no auditing set which is a Windows default but worth following up. Because the event log settings were not changed from their defaults the log files size were set to 512K and to overwrite as needed. Consequently, the oldest application log entry was 9/20/2003 and the farthest system log entry was 12/17/2003. The search for *.log files returned 217 files 9 of which returned a 0 byte size. Some log files were from the Connx data tool. The Timbuktu activity log was checked and all that was found was access from the sysadmin and DBA. IP addresses were confirmed to be their cable modem IP. A log file called iis5.log was found in c:\winnt. After looking through the log it was determined to be a default from the windows2000 install. The IIS service was not installed or running on the system in question. The log was also compared with a log on another installation of Windows 2000 Professional. As explained by Microsoft the iis5.log is an installation log for IIS.

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/tips/setuplog.msp>

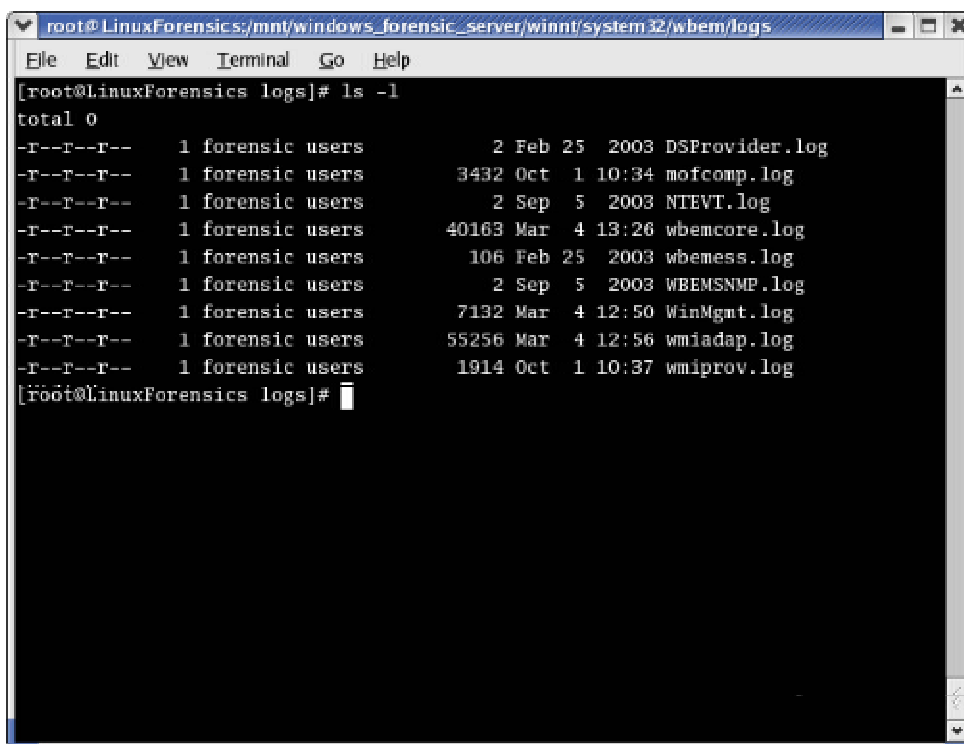
"The %windir%\iis5.log file is simply a log of the activities of setup. Any failures within setup are reported here. The log file's operations are controlled by the setup .inf file, located at %windir%\inf. (Iis.inf is specified in the %windir%\inf\sysoc.inf)."

I did a search for *.inf files which returned 813 files and found an iis.inf file. At one time IIS could have been installed on the system. Towards the bottom of the document it states it was auto generated on June 19th 2003 which does not coincide with the system installation and service pack installation. However, it does match with the date of the file as included with servicepack4. I confirmed this by checking the file on another working installation of Windows 2000 Pro SP 4. IIS was not installed on the system this file also was a default file created by Windows.



```
iis.inf - Notepad
File Edit Format Help
IIS_index.asp1=2,,2504
IIS_index.gif1=2,,957
IIS_index.htm1=2,,1258
IIS_inflat.htm1=2,,818
IIS_ismhd.gif1=2,,1916
IIS_main.htm1=2,,388
IIS_ms_logo.gif1=2,,1261
IIS_navbar.asp1=2,,1096
IIS_navbar.htm1=2,,178
IIS_navpad.gif1=2,,43
IIS_nocont.gif1=2,,1015
IIS_noindex.gif1=2,,974
IIS_nosearch.gif1=2,,1006
IIS_print.gif1=2,,231
IIS_query.asp1=2,,18756
IIS_search.asp1=2,,5533
IIS_search.gif1=2,,994
IIS_synch.gif1=2,,230
IIS_white.gif1=2,,912
IIS_tips.dat1=3,,600
; *** END *****
; **
; ** Automatically generated on: Thu Jun 19 19:43:25 2003 **
; **
; *** END *****
0
```

A discrepancy found was in the Gnome search tool only 173 files were found while in the windows search 217 files were discovered. What the cause of this was that Windows is not case sensitive and Linux is. A windows search will ignore case and return all characters matching the query both upper and lower case. I subsequently did a search for *.LOG and received 45 hits. There is still a discrepancy of one file, I then did a side by side search by name to find the extra file. The uppercase *.LOG match at 45. However, there is an extra file in *.log. The file was Dc1.log which was in the recycler. I tailed the file which turned out to be a log file from either a DataStage or SQL query. Other logs which should be checked include log files in the c:\winnt\system32\wbem\logs directory.



```
root@LinuxForensics:/mnt/windows_forensic_server/winnt/system32/wbem/logs
File Edit View Terminal Go Help
[root@LinuxForensics logs]# ls -l
total 0
-r--r--r-- 1 forensic users 2 Feb 25 2003 DSProvider.log
-r--r--r-- 1 forensic users 3432 Oct 1 10:34 mofcomp.log
-r--r--r-- 1 forensic users 2 Sep 5 2003 NTEVT.log
-r--r--r-- 1 forensic users 40163 Mar 4 13:26 wbemcore.log
-r--r--r-- 1 forensic users 106 Feb 25 2003 wbemess.log
-r--r--r-- 1 forensic users 2 Sep 5 2003 WBEMSNMP.log
-r--r--r-- 1 forensic users 7132 Mar 4 12:50 WinMgmt.log
-r--r--r-- 1 forensic users 55256 Mar 4 12:56 wmiadap.log
-r--r--r-- 1 forensic users 1914 Oct 1 10:37 wmiprov.log
[roöt@LinuxForensics logs]#
```

The logs contained in this directory were for Windows Management Instrumentation. The wbemcore.log provides some interesting but inconclusive information. However, some good leads when checking deleted files.

(Tue Feb 25 16:55:47 2003) : CAsyncReq_GetObjectAsync, Path=WmiBinaryMofResource.HighDateTime=29311104,LowDateTime=2910345216, Name="C:\\WINNT\\system32\\wmi\\core.dll[MofResource]" in namespace Root\\WMI using flags 0x0

(Tue Feb 25 16:55:48 2003) : Error 80041002 occurred executing queued request

(Tue Feb 25 16:55:48 2003) : CAsyncReq_GetObjectAsync, Path=WmiBinaryMofResource.HighDateTime=29311104,LowDateTime=2910345216, Name="C:\\WINNT\\system32\\Services.exe[MofResourceName]" in namespace Root\\WMI using flags 0x0

(Tue Feb 25 16:55:49 2003) : Error 80041002 occurred executing queued request

(Tue Feb 25 16:55:49 2003) : CAsyncReq_GetObjectAsync, Path=WmiBinaryMofResource.HighDateTime=29311104,LowDateTime=2910345216, Name="C:\\WINNT\\System32\\Drivers\\atapi.SYS[MofResourceName]" in namespace Root\\WMI using flags 0x0

(Tue Feb 25 16:55:49 2003) : Error 80041002 occurred executing queued request

(Tue Feb 25 16:55:49 2003) : CAsyncReq_GetObjectAsync, Path=WmiBinaryMofResource.HighDateTime=29311104,LowDateTime=2910345216, Name="C:\\WINNT\\System32\\Drivers\\Disk.SYS[MofResourceName]" in namespace Root\\WMI using flags 0x0

(Tue Feb 25 16:55:49 2003) : Error 80041002 occurred executing queued request

(Tue Feb 25 16:55:49 2003) : CAsyncReq_GetObjectAsync, Path=WmiBinaryMofResource.HighDateTime=29311104,LowDateTime=2910345216, Name="C:\\WINNT\\system32\\lsass.exe[LsaMofResource]" in namespace Root\\WMI using flags 0x0

I checked the error messages on the Microsoft knowledge base with the following result from Article#316753 which states:

"Excessive error entries may be recorded in the Wbemcore.log file if you are using Network Load Balancing (NLB). When this occurs, error entries that are similar to these are recorded:"

The error only occurred on the day the system was installed. I attribute the error to be pre hot fixes and service packs.

I will include a list of log files discovered in the appendix, but there was no evidence to suggest system compromise.

I ran a search on *.txt files and received 304 hits in VMware and 171 files in Linux with 133 with the string *.TXT. Of these there were some things that stood out. The first was a file c:\\comcheck\\getdata.txt. The contents brought up a red flag because it looks like the text of a script collects system data such as registry settings. The streams directory is an output directory with a lot of information about the computer including location of files and registry information. I installed the latest version of comcheck and installed it on a test system and it did not behave this way. However, the information gathered only relates to the installation of the MDAC 2.5 checking tool beta1. I verified that the scripts did not send data out. Below is an excerpt of the file getdata.txt.

```
// "ForReal_File.TXT"
// 05/21/99 JTH "39360 DD Expects that the system drive is drive C:"
```

```
// P0_0
// Collect file data
```

```
FileObject.   InputFileName       = %InputDir%\\AllFiles.txt
FileObject.   OutputFileName      = OutputData\\JustFile.CSV
FileObject.   FieldDefinitions    = FileNew.DSC
FileObject.   GenearlOutputFormat = CSV
FileObject.   CollectData
```

```
// "ForReal_Registry.TXT"
```

```
// P1_2
```

```
RegistryObject. InputFileName      = %InputDir%\RegistryKeyValue.txt
RegistryObject. FieldDefinitions   = RegistryKeyValue.DSC
RegistryObject. OutputFileName     = OutputData\RegistryKeyValue.CSV
RegistryObject. GenearlOutputFormat = CSV
RegistryObject. RegistrySearchMethod = RegistryKeyValue
RegistryObject. CollectData
```

```
// "ForReal_ComReg.TXT"
```

```
// P1_3
```

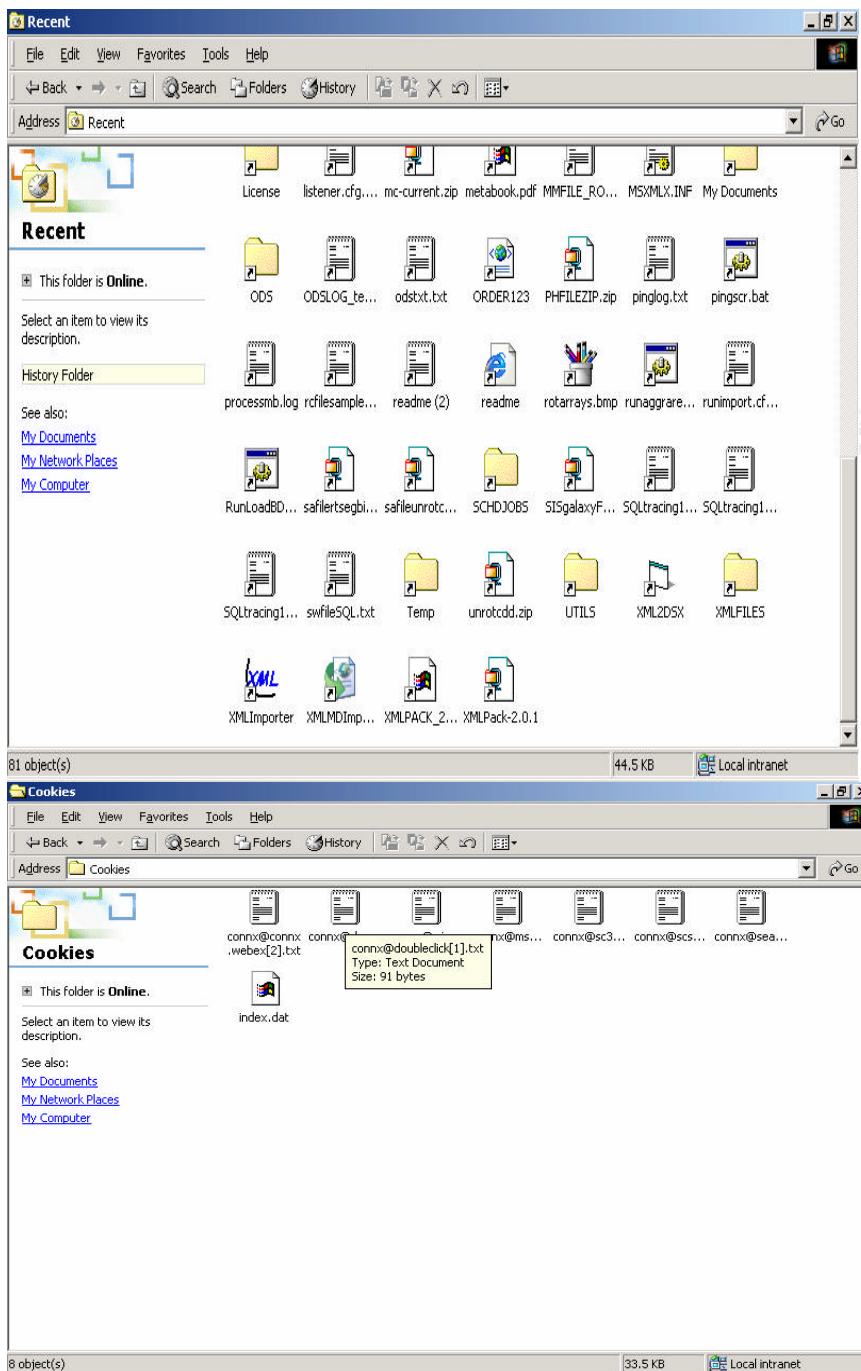
```
RegistryObject. InputFileName      = %InputDir%\RegKeysNew.TXT
RegistryObject. OutputFileName     = OutputData\RegKeysOut.CSV
RegistryObject. GenearlOutputFormat = CSV
RegistryObject. RegistrySearchMethod = RegistryKeyFileName
RegistryObject. CollectData
```

```
// P1_4
```

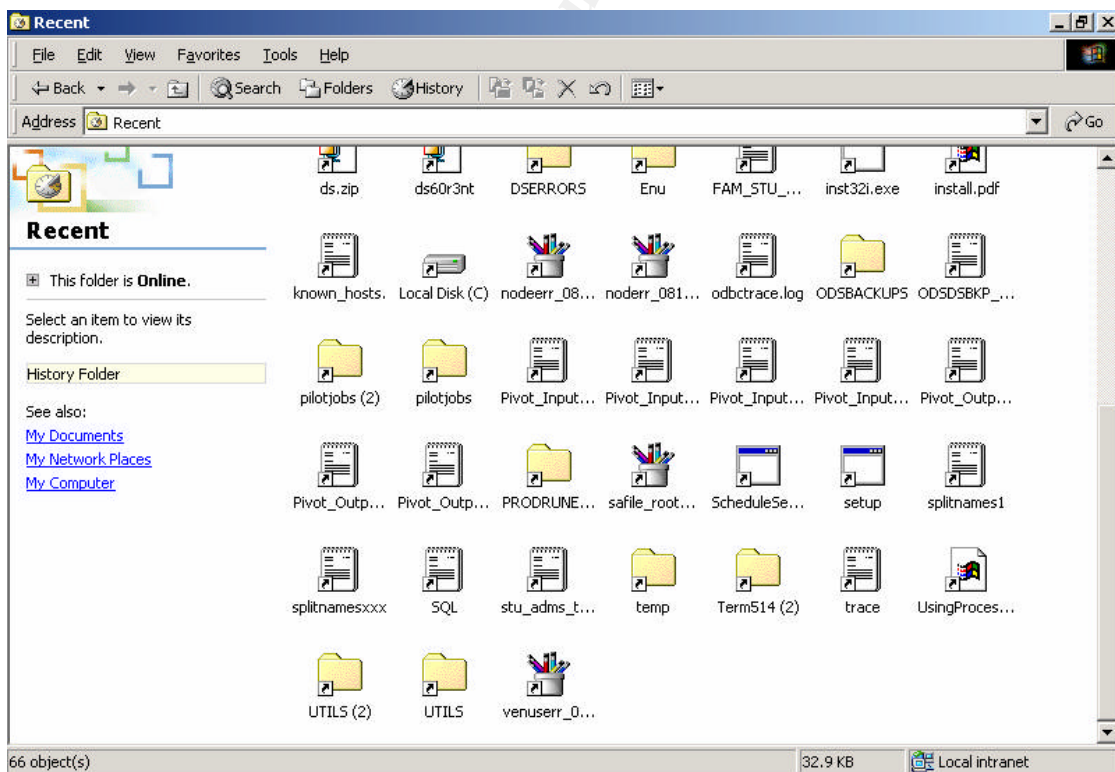
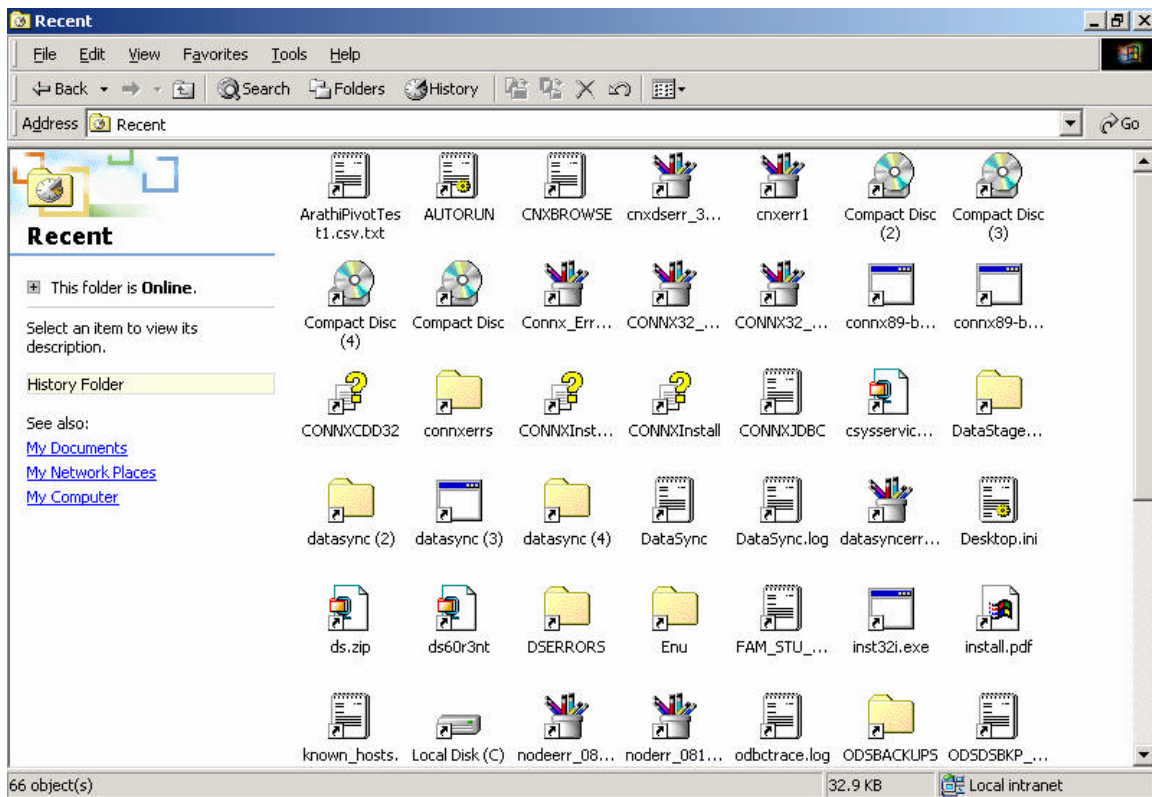
```
CSVObject. InputFileName      = OutputData\RegKeysOut.CSV
CSVObject. OutputFileName     = OutputData\CompFile.TXT
CSVObject. FieldDefinitions   = FileJustName.DSC
CSVObject. GenearlOutputFormat = CSV
CSVObject. CreateCompositeFieldFile
I checked the recent and cookies folders in the document and settings directory.
There were two users that had information in those folders Connx and
Administrator
```

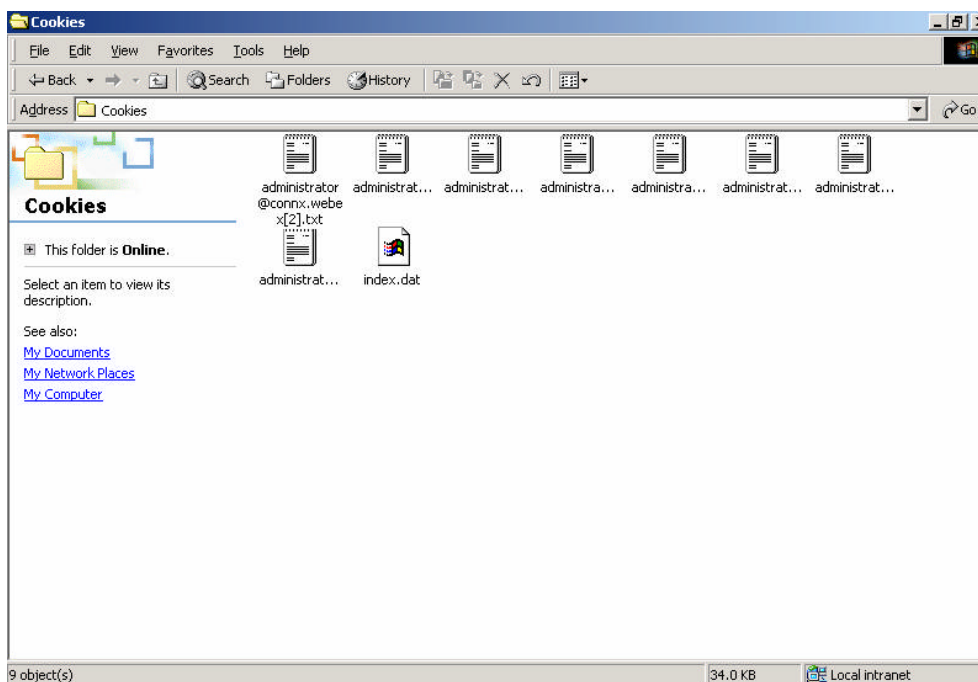
Connx Cookies and recent files.

© SANS Institute 2004. Author retains full rights.



Administrator Recent files and cookies.





The accessed files in the recent file folder were mostly related to the Connx and DataStage programs. In the cookies directory almost all of them were related to webex and a couple of yahoo sites and sites at out location. There was nothing suspicious or out of the ordinary in these directories.

Tripwire was running on this system as of approximately October of 2003. Tripwire is a monitoring system which runs daily scans of a system and check the system's baseline database for any changes in the file system and registry. Tripwire is made by the company Tripwire. If used correctly Tripwire can be an effective intrusion detection tool. One advantage as in this case Tripwire's logs are kept on a separate server, which prevents compromise of the Tripwire data. Tripwire only can detect changes from the time it is first installed and the initial database is created. Tripwire will not help in detecting intrusions prior to the first time it is scanned. I pulled the tripwire log as indicated below and found nothing suspicious. There were 78 violations found. What I mostly discovered was service pack updates, logs, and some changes in the network interface and DHCP leases. As I said this does say that the system was not compromised prior to Tripwire's installation in October of 2003.

- * Added: C:\WINNT\\$NtUninstallKB828028\$
- * Added: C:\WINNT\KB828028.log
- * Modified: C:\WINNT\comsetup.log
- * Modified: C:\WINNT\ieuninst.exe
- * Modified: C:\WINNT\iis5.log
- * Modified: C:\WINNT\imsins.BAK
- * Modified: C:\WINNT\imsins.log

- * Modified: C:\WINNT\ocgen.log
- * Modified: C:\WINNT\ockodak.log
- * Modified: C:\WINNT\randseed.rnd
- * Modified: C:\WINNT\Windows Update.log
- * Modified: C:\WINNT\System32\BROWSEUI.DLL
- * Modified: C:\WINNT\System32\msasn1.dll
- * Modified: C:\WINNT\System32\MSHTML.DLL
- * Modified: C:\WINNT\System32\SHDOCVW.DLL
- * Modified: C:\WINNT\System32\SHLWAPI.DLL
- * Modified: C:\WINNT\System32\spmsg.dll
- * Modified: C:\WINNT\System32\URLMON.DLL
- * Modified: C:\WINNT\System32\WININET.DLL
- * Added: C:\WINNT\System32\dllcache\msasn1.dll
- * Modified: C:\WINNT\System32\dllcache\BROWSEUI.DLL
- * Modified: C:\WINNT\System32\dllcache\MSHTML.DLL
- * Modified: C:\WINNT\System32\dllcache\SHDOCVW.DLL
- * Modified: C:\WINNT\System32\dllcache\SHLWAPI.DLL
- * Modified: C:\WINNT\System32\dllcache\URLMON.DLL
- * Modified: C:\WINNT\System32\dllcache\WININET.DLL
- * Added: C:\WINNT\security\edb00002.log
- * Removed: C:\WINNT\security\edb00001.log
- * Modified: C:\WINNT\security\Database\secedit.sdb
- * Modified: C:\WINNT\security\edb.chk
- * Modified: C:\WINNT\security\edb.log
- * Modified: C:\WINNT\security\logs\scepol.log
- * Modified: C:\WINNT\security\logs\winlogon.log
- * Modified: C:\WINNT\security\logs\winlogon.old
- * Added: C:\WINNT\inf\q832894.inf
- * Added: C:\WINNT\inf\q832894.PNF
- * Removed: C:\WINNT\inf\q824145.inf
- * Modified: C:\PROGRAM FILES\TRIPWIRE\TFS\Key\authentication.dat
- * Modified:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dhcp\Parameters\+{B5E2AB0F-0062-4538-8517-DE1AB13E0257}

- * Modified:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\+Sources

- * Modified:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\+Sources

- * Modified:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrkWks\Parameters\+NextRefreshTime

- * Modified:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrkWks\Parameters\+NextVolFrequentTask

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrkWks\Parameters\+NextVollnfrequentTask

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\+msSkewPerDay

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{B5E2AB0F-0062-4538-8517-DE1AB13E0257}\Parameters\Tcpip\+LeaseObtainedTime

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{B5E2AB0F-0062-4538-8517-DE1AB13E0257}\Parameters\Tcpip\+LeaseTerminatesTime

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{B5E2AB0F-0062-4538-8517-DE1AB13E0257}\Parameters\Tcpip\+T1

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{B5E2AB0F-0062-4538-8517-DE1AB13E0257}\Parameters\Tcpip\+T2

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\parameters\+Guid

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\+Hostname

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\+NV Hostname

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{B5E2AB0F-0062-4538-8517-DE1AB13E0257}\+IPAutoconfigurationSeed

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{B5E2AB0F-0062-4538-8517-DE1AB13E0257}\+LeaseObtainedTime

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{B5E2AB0F-0062-4538-8517-DE1AB13E0257}\+LeaseTerminatesTime

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{B5E2AB0F-0062-4538-8517-DE1AB13E0257}\+T1

* Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{B5E2AB0F-0062-4538-8517-DE1AB13E0257}\+T2

- * Modified:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule\+Next
AtJobId
- * Added:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Applic
ation\Tripwire Agent\+TypesSupported
- * Added:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Applic
ation\Tripwire Agent\+EventMessageFile
- * Modified: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\+AltDefaultDomainName
- * Modified: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\+DCacheUpdate
- * Modified: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\+DefaultDomainName
- * Modified: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\GPEExtensions\{827D319E-6EAC-11D2-A4EA-
00C04F79F83A}\+LastPolicyTime
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\File 1
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\File 1\+New File
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\File 1\+New Link Date
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\File 1\+Old Link Date
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\File 1\+Flags
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\+Installed
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\+Comments
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\+Backup Dir
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\+Fix Description
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\+Installed By
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\+Installed On
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\+Service Pack
- * Added: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Hotfix\KB828028\+Valid

Total violations found: 78

Image Part 2

I ran a listing of the running processes and found nothing out of the ordinary or that I could not account for. I used the taskmgr.exe command from my incident response CD. While running the taskmgr command on a live system will change that data on the disk this is the best method to get accurate information on running processes. The disk has been imaged and secured as evidence. If anything is found from running diagnostics on the suspect system it can be used as clues. However, I must then prove my findings from the secured image to be used as evidence.

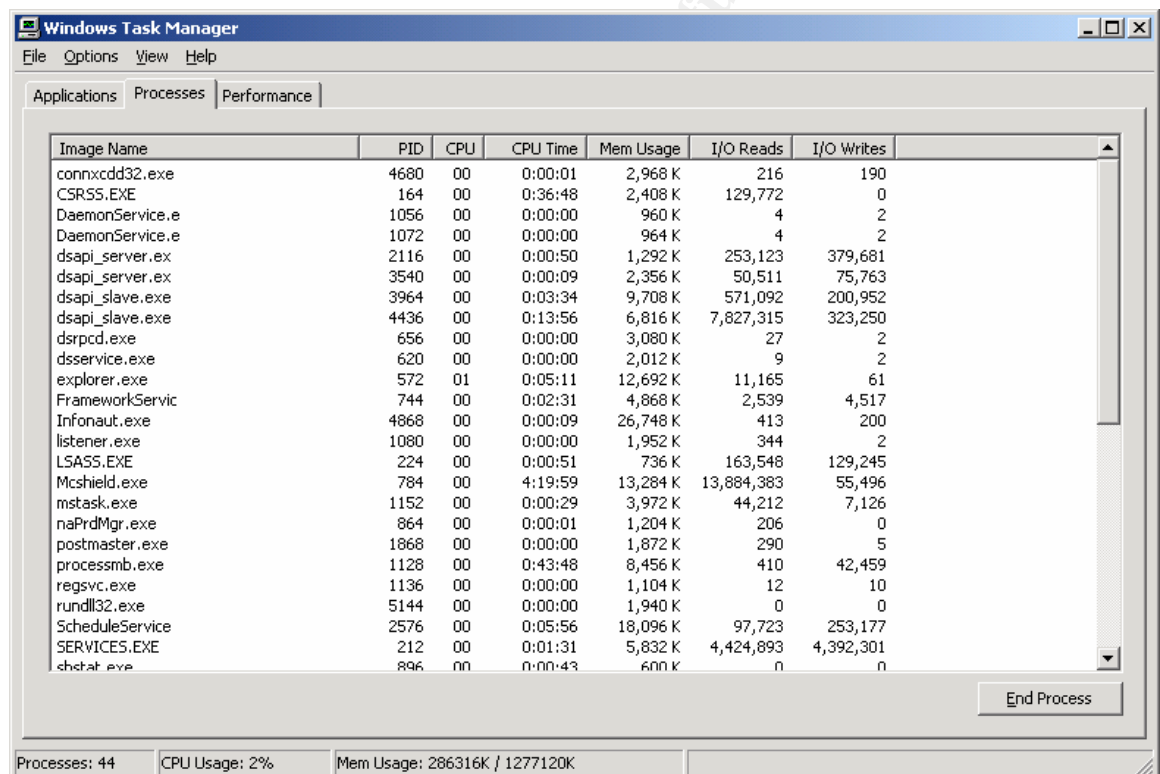
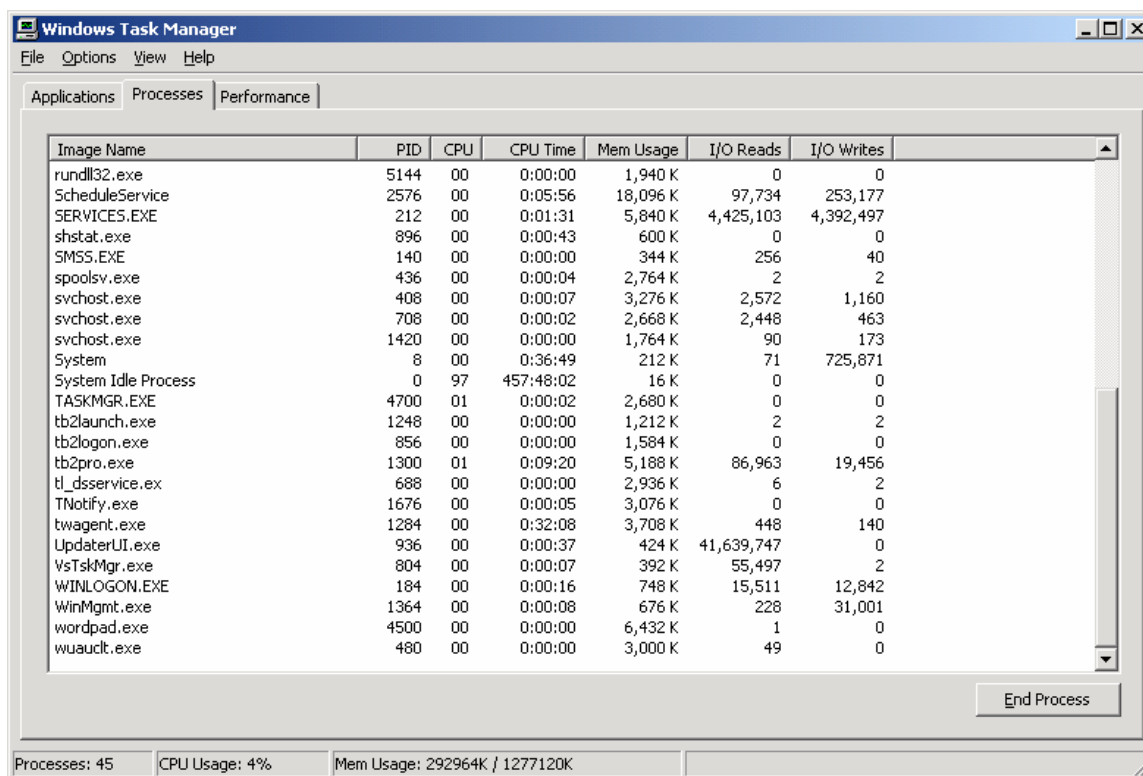


Image Name	PID	CPU	CPU Time	Mem Usage	I/O Reads	I/O Writes
connxddd32.exe	4680	00	0:00:01	2,968 K	216	190
CSRSS.EXE	164	00	0:36:48	2,408 K	129,772	0
DaemonService.e	1056	00	0:00:00	960 K	4	2
DaemonService.e	1072	00	0:00:00	964 K	4	2
dsapi_server.ex	2116	00	0:00:50	1,292 K	253,123	379,681
dsapi_server.ex	3540	00	0:00:09	2,356 K	50,511	75,763
dsapi_slave.exe	3964	00	0:03:34	9,708 K	571,092	200,952
dsapi_slave.exe	4436	00	0:13:56	6,816 K	7,827,315	323,250
dsrpsd.exe	656	00	0:00:00	3,080 K	27	2
dsservice.exe	620	00	0:00:00	2,012 K	9	2
explorer.exe	572	01	0:05:11	12,692 K	11,165	61
FrameworkServic	744	00	0:02:31	4,868 K	2,539	4,517
Infonaut.exe	4868	00	0:00:09	26,748 K	413	200
listener.exe	1080	00	0:00:00	1,952 K	344	2
LSASS.EXE	224	00	0:00:51	736 K	163,548	129,245
Mcshield.exe	784	00	4:19:59	13,284 K	13,884,383	55,496
mstask.exe	1152	00	0:00:29	3,972 K	44,212	7,126
naPrdMgr.exe	864	00	0:00:01	1,204 K	206	0
postmaster.exe	1868	00	0:00:00	1,872 K	290	5
processmb.exe	1128	00	0:43:48	8,456 K	410	42,459
regsvc.exe	1136	00	0:00:00	1,104 K	12	10
rundll32.exe	5144	00	0:00:00	1,940 K	0	0
ScheduleService	2576	00	0:05:56	18,096 K	97,723	253,177
SERVICES.EXE	212	00	0:01:31	5,832 K	4,424,893	4,392,301
shstat.exe	896	00	0:00:43	600 K	0	0

Processes: 44 CPU Usage: 2% Mem Usage: 286316K / 1277120K



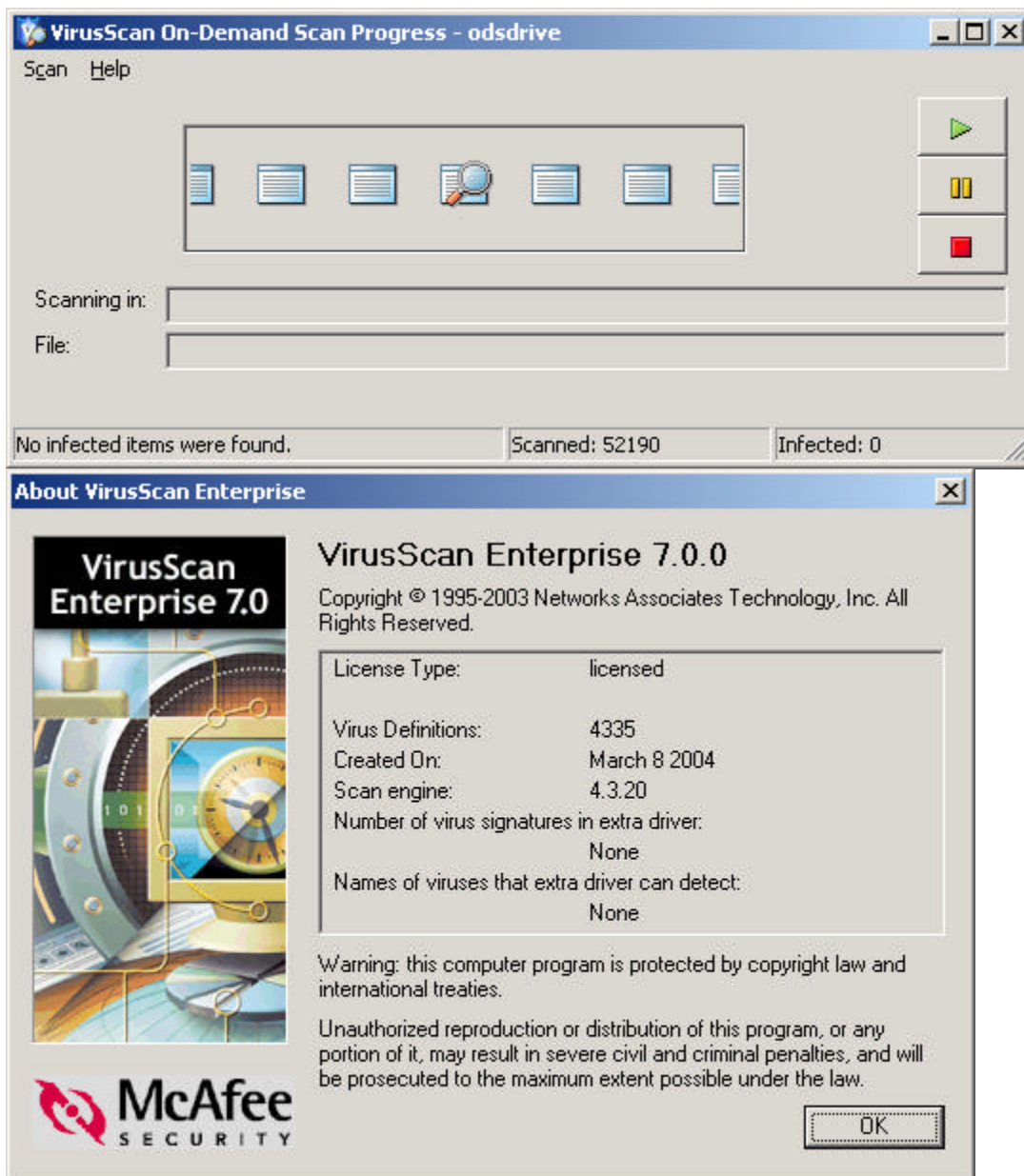
The screenshot shows the Windows Task Manager Performance tab. The 'Processes' tab is selected, displaying a list of running processes. The status bar at the bottom indicates 45 processes, 4% CPU usage, and 292964K / 1277120K memory usage.

Image Name	PID	CPU	CPU Time	Mem Usage	I/O Reads	I/O Writes
rundll32.exe	5144	00	0:00:00	1,940 K	0	0
ScheduleService	2576	00	0:05:56	18,096 K	97,734	253,177
SERVICES.EXE	212	00	0:01:31	5,840 K	4,425,103	4,392,497
shstat.exe	896	00	0:00:43	600 K	0	0
SMSS.EXE	140	00	0:00:00	344 K	256	40
spoolsv.exe	436	00	0:00:04	2,764 K	2	2
svchost.exe	408	00	0:00:07	3,276 K	2,572	1,160
svchost.exe	708	00	0:00:02	2,668 K	2,448	463
svchost.exe	1420	00	0:00:00	1,764 K	90	173
System	8	00	0:36:49	212 K	71	725,871
System Idle Process	0	97	457:48:02	16 K	0	0
TASKMGR.EXE	4700	01	0:00:02	2,680 K	0	0
tb2launch.exe	1248	00	0:00:00	1,212 K	2	2
tb2logon.exe	856	00	0:00:00	1,584 K	0	0
tb2pro.exe	1300	01	0:09:20	5,188 K	86,963	19,456
tl_dsservice.ex	688	00	0:00:00	2,936 K	6	2
TNotify.exe	1676	00	0:00:05	3,076 K	0	0
twagent.exe	1284	00	0:32:08	3,708 K	448	140
UpdaterUI.exe	936	00	0:00:37	424 K	41,639,747	0
VsTskMgr.exe	804	00	0:00:07	392 K	55,497	2
WINLOGON.EXE	184	00	0:00:16	748 K	15,511	12,842
WinMgmt.exe	1364	00	0:00:08	676 K	228	31,001
wordpad.exe	4500	00	0:00:00	6,432 K	1	0
wuauct.exe	480	00	0:00:00	3,000 K	49	0

Some processes that stood out included postmaster.exe but that was part of the ConnX product and located in the c:\connx32\connxstore\bin DaemonService also refers to the ConnX product as does listener. as is dsapi_slave. I checked to see if these files were deleted dsapi.slave was but it coincides with a update of the ConnX software. The other running processes were accounted for and mostly attributed to Windows itself.

Virus Check

To both check for any running viruses or trojans and backdoors I did a complete virus check on the image of the system. I created a custom scan called odsdrive and scanned all files. I used McAfee Anti Virus ver 7 to scan the hard drive image with the latest dat files. Historically this system has had previous problems with viruses and is auto updated at this time. I also checked the McAfee log for any viruses. No viruses were found on the disk in question.



From the mcscript.log I was able to ascertain that McAfee Antivirus was first installed in August of 2003.

20030814101420: MONTCLAI-5KWJJC: ScriptEngine: MONTCLAI-5KWJJC
Initializing update ...

I was not able to find evidence that the system has been previously infected.

Also from the log file mcscript.log I was able to confirm that the latest dat file was running at the time of gathering the evidence. The virus scanner is set to check for updates daily.

20040304170915: ODS-TEST: ScriptEngine: ODS-TEST session.	Closing update
20040305173305: ODS-TEST: ScriptEngine: ODS-TEST	Initializing update ...
20040305173305: ODS-TEST: ScriptEngine: ODS-TEST catalog.z.	Downloading
20040305173306: ODS-TEST: ScriptEngine: ODS-TEST	Verifying catalog.z.
20040305173306: ODS-TEST: ScriptEngine: ODS-TEST	Replacing file
C:\Documents and Settings\All Users\Application Data\Network Associates\Common Framework\catalog.ztp with C:\Documents and Settings\All Users\Application Data\Network Associates\Common Framework\catalog.z	
20040305173307: ODS-TEST: ScriptEngine: ODS-TEST catalog.z.	Extracting
20040305173307: ODS-TEST: ScriptEngine: ODS-TEST configuration from: Catalog.xml	Loading update
20040305173308: ODS-TEST: ScriptEngine: ODS-TEST updates for Engine.	Searching available
20040305173309: ODS-TEST: ScriptEngine: ODS-TEST latest Engine.	Product(s) running
20040305173310: ODS-TEST: ScriptEngine: ODS-TEST updates for DATs.	Searching available
20040305173311: ODS-TEST: ScriptEngine: ODS-TEST PkgCatalog.z.	Downloading
20040305173312: ODS-TEST: ScriptEngine: ODS-TEST PkgCatalog.z.	Verifying
20040305173312: ODS-TEST: ScriptEngine: ODS-TEST PkgCatalog.z.	Extracting
20040305173312: ODS-TEST: ScriptEngine: ODS-TEST configuration from: PkgCatalog.xml	Loading update
20040305173314: ODS-TEST: ScriptEngine: ODS-TEST update.	Starting DAT
20040305173314: ODS-TEST: ScriptEngine: ODS-TEST DAT update.	Pre-notifying for
20040305173316: ODS-TEST: ScriptEngine: ODS-TEST	Downloading DAT.
20040305173316: ODS-TEST: ScriptEngine: ODS-TEST delta.ini.	Downloading
20040305173317: ODS-TEST: ScriptEngine: ODS-TEST 43304331.upd.	Downloading
20040305173317: ODS-TEST: ScriptEngine: ODS-TEST	Replacing file
C:\WINNT\TEMP\23DB\43304331.upd with C:\Documents and Settings\All Users\Application Data\Network Associates\Common Framework\Current\VSCANDAT1000\DAT\0000\43304331.upd	
20040305173318: ODS-TEST: ScriptEngine: ODS-TEST 43314332.upd.	Downloading
20040305173318: ODS-TEST: ScriptEngine: ODS-TEST	Replacing file
C:\WINNT\TEMP\23DB\43314332.upd with C:\Documents and Settings\All	

Users\Application Data\Network Associates\Common
 Framework\Current\VSCANDAT1000\DAT\0000\43314332.upd
 20040305173318: ODS-TEST: ScriptEngine: ODS-TEST Downloading
 43324333.upd.
 20040305173319: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\WINNT\TEMP\23DB\43324333.upd with C:\Documents and Settings\All
 Users\Application Data\Network Associates\Common
 Framework\Current\VSCANDAT1000\DAT\0000\43324333.upd
 20040305173319: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\WINNT\TEMP\23DB\SCAN.DAT with C:\Program Files\Common
 Files\Network Associates\Engine\SCAN.DAT
 20040305173319: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\WINNT\TEMP\23DB\NAMES.DAT with C:\Program Files\Common
 Files\Network Associates\Engine\NAMES.DAT
 20040305173319: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\WINNT\TEMP\23DB\CLEAN.DAT with C:\Program Files\Common
 Files\Network Associates\Engine\CLEAN.DAT
 20040305173340: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\Documents and Settings\All Users\Application Data\Network
 Associates\Common
 Framework\Current\VSCANDAT1000\DAT\0000\SCAN.DAT with
 C:\WINNT\TEMP\23DB\SCAN.DAT
 20040305173340: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\Documents and Settings\All Users\Application Data\Network
 Associates\Common
 Framework\Current\VSCANDAT1000\DAT\0000\NAMES.DAT with
 C:\WINNT\TEMP\23DB\NAMES.DAT
 20040305173340: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\Documents and Settings\All Users\Application Data\Network
 Associates\Common
 Framework\Current\VSCANDAT1000\DAT\0000\CLEAN.DAT with
 C:\WINNT\TEMP\23DB\CLEAN.DAT
 20040305173341: ODS-TEST: ScriptEngine: ODS-TEST Deleting
 C:\WINNT\TEMP\23DB
 20040305173341: ODS-TEST: ScriptEngine: ODS-TEST Backing up file(s)
 SCAN.DAT, NAMES.DAT, CLEAN.DAT
 20040305173341: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\Program Files\Common Files\Network Associates\Engine\OldDats\SCAN.DAT
 with C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT
 20040305173341: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\Program Files\Common Files\Network
 Associates\Engine\OldDats\NAMES.DAT with C:\Program Files\Common
 Files\Network Associates\Engine\NAMES.DAT
 20040305173341: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\Program Files\Common Files\Network
 Associates\Engine\OldDats\CLEAN.DAT with C:\Program Files\Common

Files\Network Associates\Engine\CLEAN.DAT
 20040305173341: ODS-TEST: ScriptEngine: ODS-TEST Copying
 SCAN.DAT, NAMES.DAT, CLEAN.DAT.
 20040305173341: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT with
 C:\Documents and Settings\All Users\Application Data\Network
 Associates\Common
 Framework\Current\VSCANDAT1000\DAT\0000\SCAN.DAT
 20040305173341: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\Program Files\Common Files\Network Associates\Engine\NAMES.DAT with
 C:\Documents and Settings\All Users\Application Data\Network
 Associates\Common
 Framework\Current\VSCANDAT1000\DAT\0000\NAMES.DAT
 20040305173341: ODS-TEST: ScriptEngine: ODS-TEST Replacing file
 C:\Program Files\Common Files\Network Associates\Engine\CLEAN.DAT with
 C:\Documents and Settings\All Users\Application Data\Network
 Associates\Common
 Framework\Current\VSCANDAT1000\DAT\0000\CLEAN.DAT
 20040305173343: ODS-TEST: ScriptEngine: ODS-TEST Post-notifying for
 DAT update.
 20040305173345: ODS-TEST: ScriptEngine: ODS-TEST Update succeeded
 to version 4.0.4333.
 20040305173345: ODS-TEST: ScriptEngine: ODS-TEST Deleting
 C:\Documents and Settings\All Users\Application Data\Network
 Associates\Common Framework\Current\VSCANDAT1000\DAT
 20040305173347: ODS-TEST: ScriptEngine: ODS-TEST Update Finished

Image Part 3

I began analyzing the event logs for any suspicious activity. There were a few entries that stood out.

Event Type: Information

Event Source: Windows File Protection

Event Category: None

Event ID: 64001

Date: 3/5/2004

Time: 12:10:39 PM

User: N/A

Computer: ODS-TEST

Description:

File replacement was attempted on the protected system file c:\program files\common files\system\ado\msado21.tlb. This file was restored to the original version to maintain system stability. The file version of the bad file is 2.51.5303.0, the version of the system file is 2.71.9030.0.

It is possible that an update was performed but the system was not rebooted as stated in Microsoft's KB article 236995, If a file in the dll cache is manually replaced the dll cache will not be updated until next reboot. I have noted this and will discuss it with the DBA.

Event Type: Error
Event Source: Service1
Event Category: None
Event ID: 0
Date: 3/4/2004
Time: 12:54:55 PM
User: N/A
Computer: ODS-TEST

Description

The description for Event ID (0) in Source (Service1) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. The following information is part of the event: Service cannot be started. System.InvalidCastException: QueryInterface for interface CNXLicense.ILicenseServer failed.

at System.RuntimeType.InvokeDispMethod(String name, BindingFlags invokeAttr, Object target, Object[] args, Boolean[] byrefModifiers, Int32 culture, String[] namedParameters)
at System.RuntimeType.InvokeMember(String name, BindingFlags invokeAttr, Binder binder, Object target, Object[] args, ParameterModifier[] modifiers, CultureInfo culture, String[] namedParameters)
at System.RuntimeType.ForwardCallToInvokeMember(String memberName, BindingFlags flags, Object target, Int32[] aWrapperTypes, MessageData& msgData)
at CNXLicense.LicenseServerClass.ReleaseLicense()
at ScheduleService.CONNXScheduleService.OnStart(String[] args)
at System.ServiceProcess.ServiceBase.ServiceQueuedMainCallback(Object state).

Service1 looked suspicious but after examining it closer it was also connected to the Connx product.

Event Type: Warning
Event Source: EventSystem
Event Category: Event Service
Event ID: 4106
Date: 3/4/2004
Time: 12:50:39 PM

User: N/A
Computer: ODS-TEST
Description:

The COM+ Event System detected a corrupt IEventSubscription object. The COM+ Event System has removed object ID {2F519218-754D-4CFE-8DAA-5215CD0DE0EB}. The subscriber will no longer be notified when the event occurs.

Initially this log entry also looked suspicious but I found it was also a bug in Windows 2000 which a hotfix is available. The article number is 819995. I have noted this and will report it to the system administrator for resolution. Below is an excerpt of the article.

“When a publisher fires an event, the COM+ event system enumerates all subscribers to trigger the event on all subscribers. If a subscriber unregisters a transient subscription during this enumeration, the whole enumeration can fail, and the publishing fails altogether.”

“This issue is fixed in the Microsoft Windows 2000 Post-Service Pack 4 (SP4) COM+ 1.0 Hotfix Package 27. “

Event Type: Information
Event Source: McLogEvent
Event Category: None
Event ID: 5000
Date: 9/20/2003
Time: 4:38:16 PM
User: NT AUTHORITY\SYSTEM
Computer: MONTCLAI-5KWJJC
Event Type: Information
Event Source: Service1
Event Category: None
Event ID: 0
Date: 9/22/2003
Time: 11:35:21 AM
User: N/A
Computer: MONTCLAI-5KWJJC
Description:

The description for Event ID (0) in Source (Service1) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. The following information is part of the event: Service has been successfully shut down..

Description

The description for Event ID (5000) in Source (McLogEvent) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. The following information is part of the event: 80178, None, None, None, VirusScan Enterprise, 4.2.60, 4294.

The message proved interesting since the system will not allow for remote management.

Event Type: Warning
Event Source: ASP.NET 1.1.4322.0
Event Category: (1)
Event ID: 1020
Date: 10/1/2003
Time: 9:35:20 AM
User: N/A
Computer: MONTCLAI-5KWJJC

Description:

The description for Event ID (1020) in Source (ASP.NET 1.1.4322.0) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. The following information is part of the event: .

Event Type: Error
Event Source: ESENT
Event Category: Logging/Recovery
Event ID: 439
Date: 2/10/2004
Time: 6:17:43 PM
User: N/A
Computer: ODS-TEST

Description:

services (212) Unable to write a shadowed header for file
C:\WINNT\Security\tmp.edb.

The c:\winnt\security\tmp.edb file has been deleted and is not recoverable.
Tmp.edb is an MS Exchange temporary file.

Image Part 4

I used the Internet Explorer history viewer to check for IE history files. The IE history viewer is a useful tool in checking visited web sites and was written by Scott Ponder in 1999 and is distributed by the Phillips Ponder Company. Out of 11 index.dat files there was one that was useful with 590 url's and 14 redirects. There was not that much in the way of links to trace most were the Microsoft update site and our corporate mail and web server. There were some interesting *.gifs including a gif from yahoo.com which was a picture of Cristina Aquilera.
8/12/2003 http://us.i1.yimg.com/us.yimg.com/i/us/pi/50/2003/07/c_aguile_1.jpg

11:33:18

URL 2/27/2003 http://us.i1.yimg.com/us.yimg.com/i/mc/mc2.js
08:20:46

I also found several url's leading to javascript. All looked like normal web sites. Below is a sample of one file mc1.js.

```
document.write('<span style="behavior:url(#default#clientCaps)" id=cc></span>');
```

I confirmed that the javascript was from Yahoo.

<http://us.i1.yimg.com/us.yimg.com/i/mc/mc1.js>.

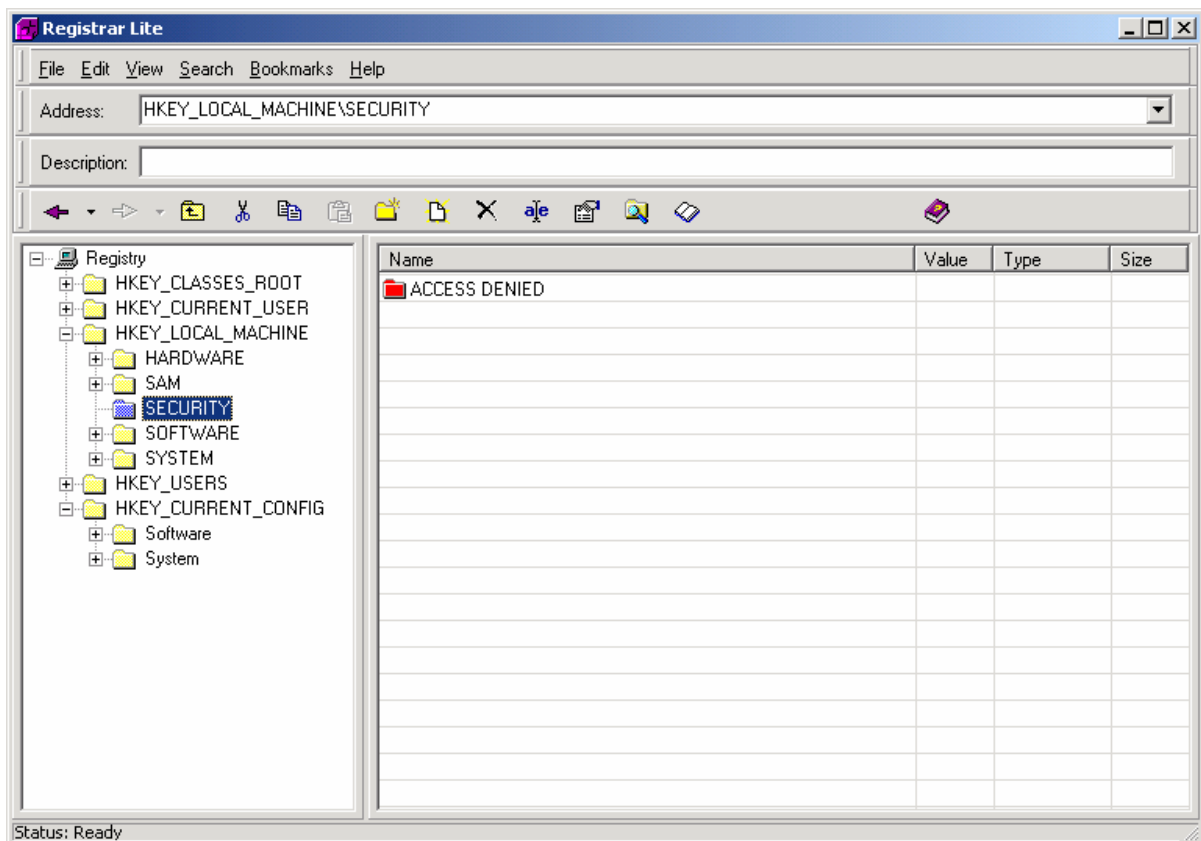
The code is used to format text. It is possible to use this java script for malicious purposes but I verified the code found on the system with the code found on the website.

I found no evidence of a sniffer program on the system I ran a check of *.exe files and found no evidence. However, as I will get into later in the paper I found a lot of trojan and IRC bot code.

Image Part 5

Registry Examination

Since the system is live I decided to start with a live examination of the registry and would use the registry files on the read only evidence image to support my findings. I used Registrar Lite version 1.01- November 11th 1999. from Resplendence Software Projects First thing off the bat I noticed in HKEY_Local_Machine\Security had access denied.

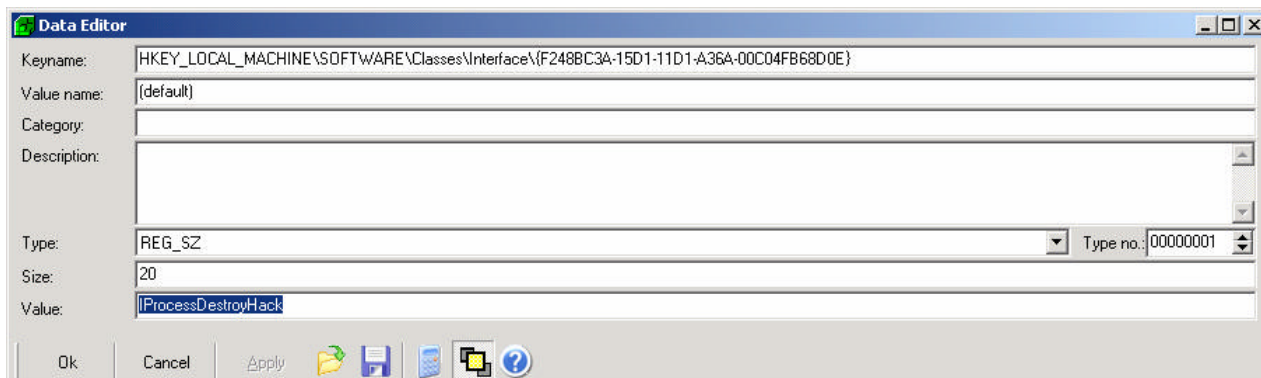


I further looked into this and it was the default permissions registry of Windows. Since this is a running system I did not want to change the registry permissions and further expose the system. I would have to rely on string searches of the registry files for Security and SAM. What I did instead was to download the trial version of Resplendent Registrar version 3.30, build 330.30108. I tried it on my test machine and it allowed me to access the inaccessible registry entries. I put it on my read only share and ran it on the victim machine and I was then able to browse the entries. I found nothing noteworthy in the security and SAM registryhive.

I started running search strings. I ran mail with XXX returns I did a search on hack and found a value of IPROCESSDESTROYHACK. I found no information on this on the web. I performed a file search and search in Autopsy with no results. I found an article on Trend Micro which points to a possible virus regarding HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface. The article points to a trojan by the aliases TrojanDownloader.Win32.Wintrim, W32/Downloader.Persis, Trojan.Wintrim, Downloader.Wintrim.B.

I found no results for files or registry entries for wintrim. I did find a registry entry for uninstall.exe. I ran searches in Autopsy for wintrim, uninstall.exe, Since the virus reported was my doom I looked that up on the trend micro site for more information. I did a search in Autopsy for wintrim and got 12 hits. In cluster 181794 which points to

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_WINT RIM.A&Vsect=T



I performed a registry search for service1 and received a few matches. I was able to account for all of them. Most of the matches were for .net framework and 2 for Windows Backup as indicated in my registry search below.

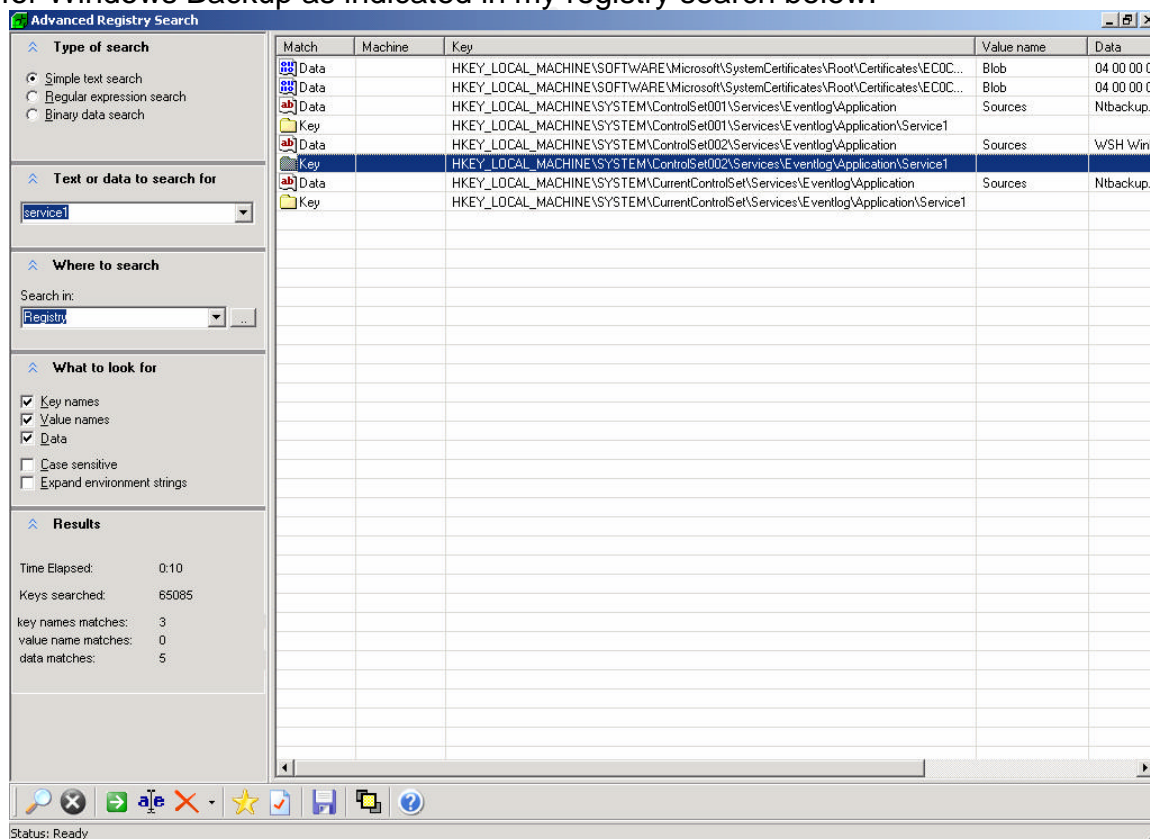
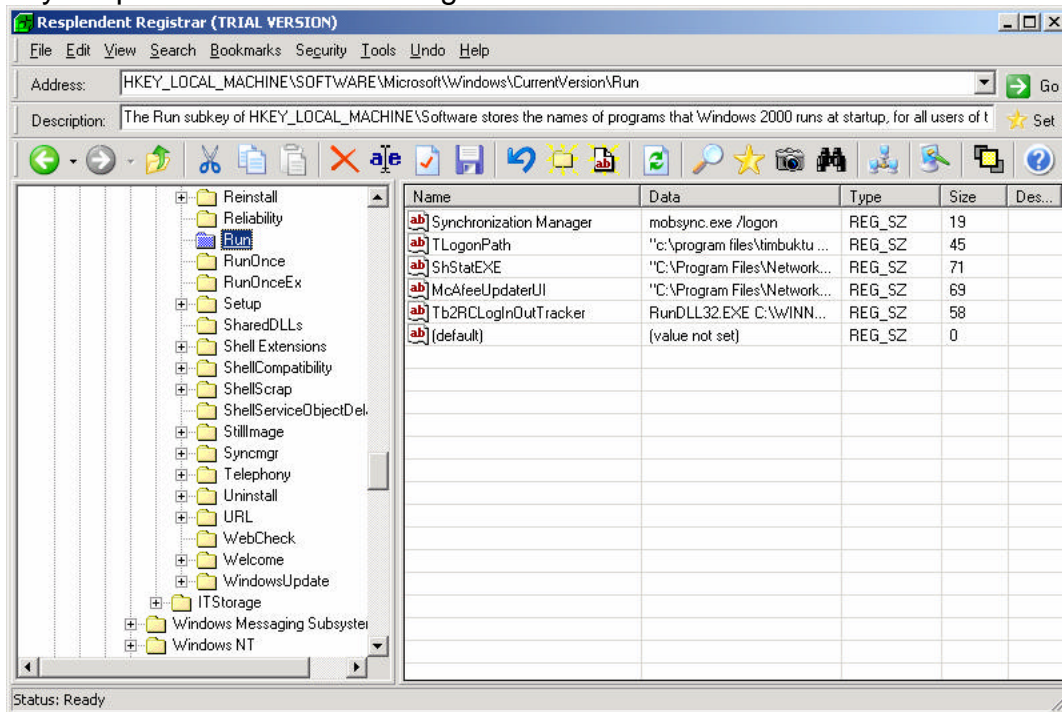


Image Part 6

I ran a check on the start up processes and services to see if there were any suspicious services running.



The above services are set to start when any user logs in. There were no suspicious programs in the run section of HKEY_LOCAL_MACHINE. There were no entries in the runonce or runonceex keys.

© SANS Institute 2004

Services					
Action View					
Tree	Name	Description	Status	Startup Type	Log On As
Services (Local)	Alerter	Notifies sel...		Manual	LocalSystem
	Application Manage...	Provides s...	Started	Manual	LocalSystem
	ASP.NET State Serv...	Provides s...		Manual	ASPNET
	Automatic Updates	Enables th...	Started	Automatic	LocalSystem
	Background Intellig...	Transfers f...		Manual	LocalSystem
	ClipBook	Supports C...		Manual	LocalSystem
	COM+ Event System	Provides a...	Started	Manual	LocalSystem
	Computer Browser	Maintains a...	Started	Automatic	LocalSystem
	CONNIX Enterprise S...			Automatic	.\administ...
	CONNIX JDBC Serve...			Automatic	.\Administ...
	CONNIXSchedule		Started	Automatic	.\connx
	CONNIXStore Datab...		Started	Automatic	.\connx
	DataStage Engine R...		Started	Automatic	LocalSystem
	DataStage Telnet S...		Started	Automatic	LocalSystem
	DHCP Client	Manages n...	Started	Automatic	LocalSystem
	Distributed Link Tra...	Sends notif...	Started	Automatic	LocalSystem
	Distributed Transac...	Coordinate...		Manual	LocalSystem
	DNS Client	Resolves a...	Started	Automatic	LocalSystem
	DSRPC Service		Started	Automatic	LocalSystem
	Event Log	Logs event...	Started	Automatic	LocalSystem
	Fax Service	Helps you ...		Manual	LocalSystem
	Indexing Service			Manual	LocalSystem
	Internet Connectio...	Provides n...		Manual	LocalSystem
	IPSEC Policy Agent	Manages I...	Started	Automatic	LocalSystem
	Logical Disk Manager	Logical Disk...	Started	Automatic	LocalSystem
	Logical Disk Manage...	Administrat...		Manual	LocalSystem
	McAfee Framework ...	Shared co...	Started	Automatic	LocalSystem
	Messenger	Sends and ...	Started	Automatic	LocalSystem
	MetaStage Listener		Started	Automatic	LocalSystem
	MetaStage Process ...		Started	Automatic	LocalSystem
	Net Logon	Supports p...	Started	Automatic	LocalSystem
	NetMeeting Remote...	Allows aut...		Manual	LocalSystem
	Network Associates...		Started	Automatic	LocalSystem
	Network Associates...		Started	Automatic	LocalSystem
	Network Connections	Manages o...	Started	Manual	LocalSystem
	Network DDE	Provides n...		Manual	LocalSystem
	Network DDE DSDM	Manages s...		Manual	LocalSystem
	NT LM Security Sup...	Provides s...		Manual	LocalSystem

Services					
Action View					
Tree	Name	Description	Status	Startup Type	Log On As
Services (Local)	Network Associates...		Started	Automatic	LocalSystem
	Network Associates...		Started	Automatic	LocalSystem
	Network Connections	Manages o...	Started	Manual	LocalSystem
	Network DDE	Provides n...		Manual	LocalSystem
	Network DDE DSDM	Manages s...		Manual	LocalSystem
	NT LM Security Sup...	Provides s...		Manual	LocalSystem
	Performance Logs a...	Configures...		Manual	LocalSystem
	Plug and Play	Manages d...	Started	Automatic	LocalSystem
	Print Spooler	Loads files ...	Started	Automatic	LocalSystem
	Protected Storage	Provides pr...	Started	Automatic	LocalSystem
	QoS RSVP	Provides n...		Manual	LocalSystem
	Remote Access Aut...	Creates a ...		Manual	LocalSystem
	Remote Access Con...	Creates a ...	Started	Manual	LocalSystem
	Remote Procedure ...	Provides th...	Started	Automatic	LocalSystem
	Remote Procedure ...	Manages t...		Manual	LocalSystem
	Remote Registry Se...	Allows rem...	Started	Automatic	LocalSystem
	Removable Storage	Manages r...	Started	Automatic	LocalSystem
	Routing and Remot...	Offers rout...		Disabled	LocalSystem
	RunAs Service	Enables st...	Started	Automatic	LocalSystem
	Security Accounts ...	Stores sec...	Started	Automatic	LocalSystem
	Server	Provides R...	Started	Automatic	LocalSystem
	Smart Card	Manages a...		Manual	LocalSystem
	Smart Card Helper	Provides s...		Manual	LocalSystem
	System Event Notifi...	Tracks syst...	Started	Automatic	LocalSystem
	Task Scheduler	Enables a ...	Started	Automatic	LocalSystem
	Tb2 Launch		Started	Automatic	LocalSystem
	TCP/IP NetBIOS Hel...	Enables su...	Started	Automatic	LocalSystem
	Telephony	Provides T...	Started	Manual	LocalSystem
	Telnet	Allows a re...		Disabled	LocalSystem
	Tripwire Agent	The Tripwir...	Started	Automatic	LocalSystem
	Uninterruptible Pow...	Manages a...		Manual	LocalSystem
	Utility Manager	Starts and ...		Manual	LocalSystem
	Windows Installer	Installs, re...		Manual	LocalSystem
	Windows Managem...	Provides s...	Started	Automatic	LocalSystem
	Windows Managem...	Provides s...	Started	Manual	LocalSystem
	Windows Time	Sets the co...	Started	Automatic	LocalSystem
	Wireless Configuration	Provides a...		Manual	LocalSystem
	Workstation	Provides n...	Started	Automatic	LocalSystem

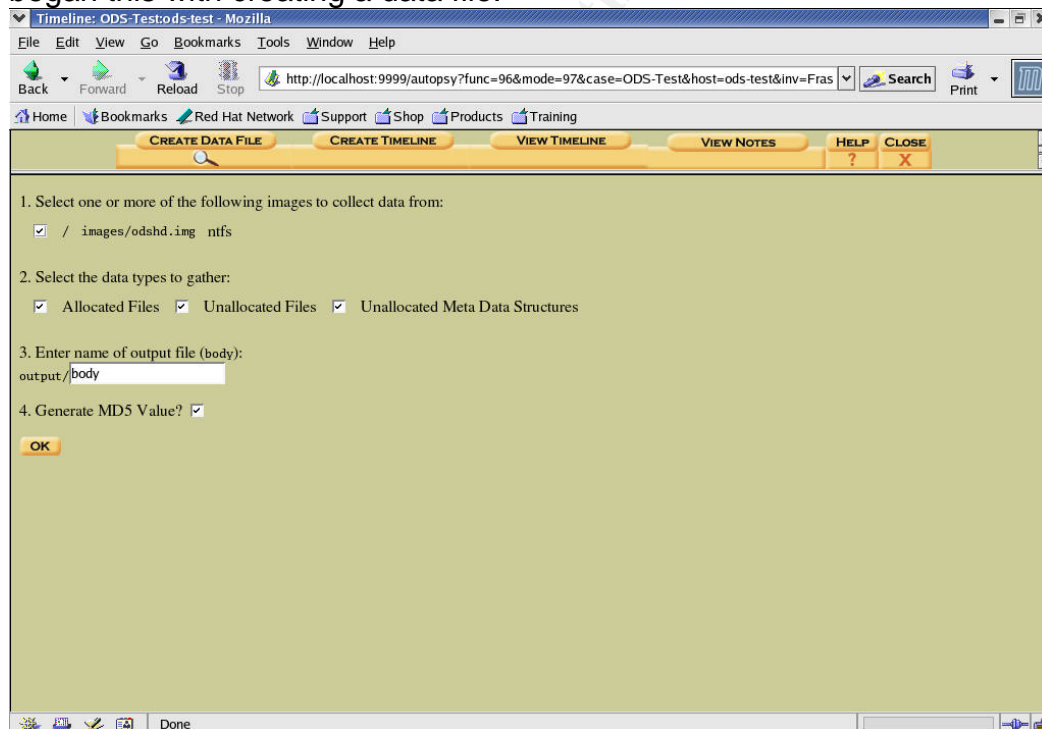
Out of services set to start automatically as indicated above nothing stood out as being suspicious. While this data is not absolute this in cooperation with the results from taskmgr.exe there seems to be no suspicious services running or set to run at startup. I checked to insure that the corresponding services were running the proper executables.

```
[root@LinuxForensics windows_forensic_server]# more boot.ini
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows 2000 Professional"
/fastdetect
```

I checked the boot.ini which loads the operating system partition and it has not been modified and is only pointing to one OS partition.

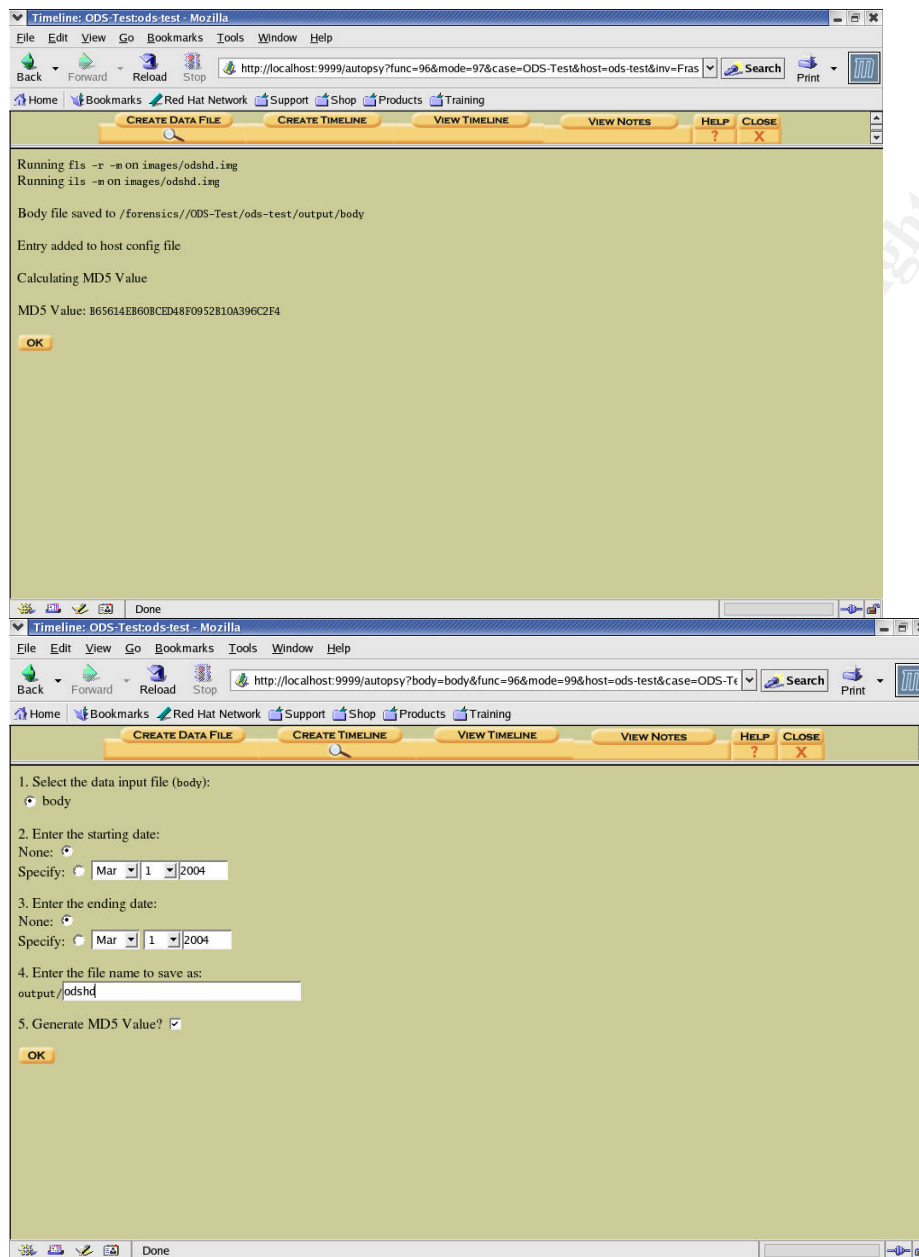
Time Line Analysis

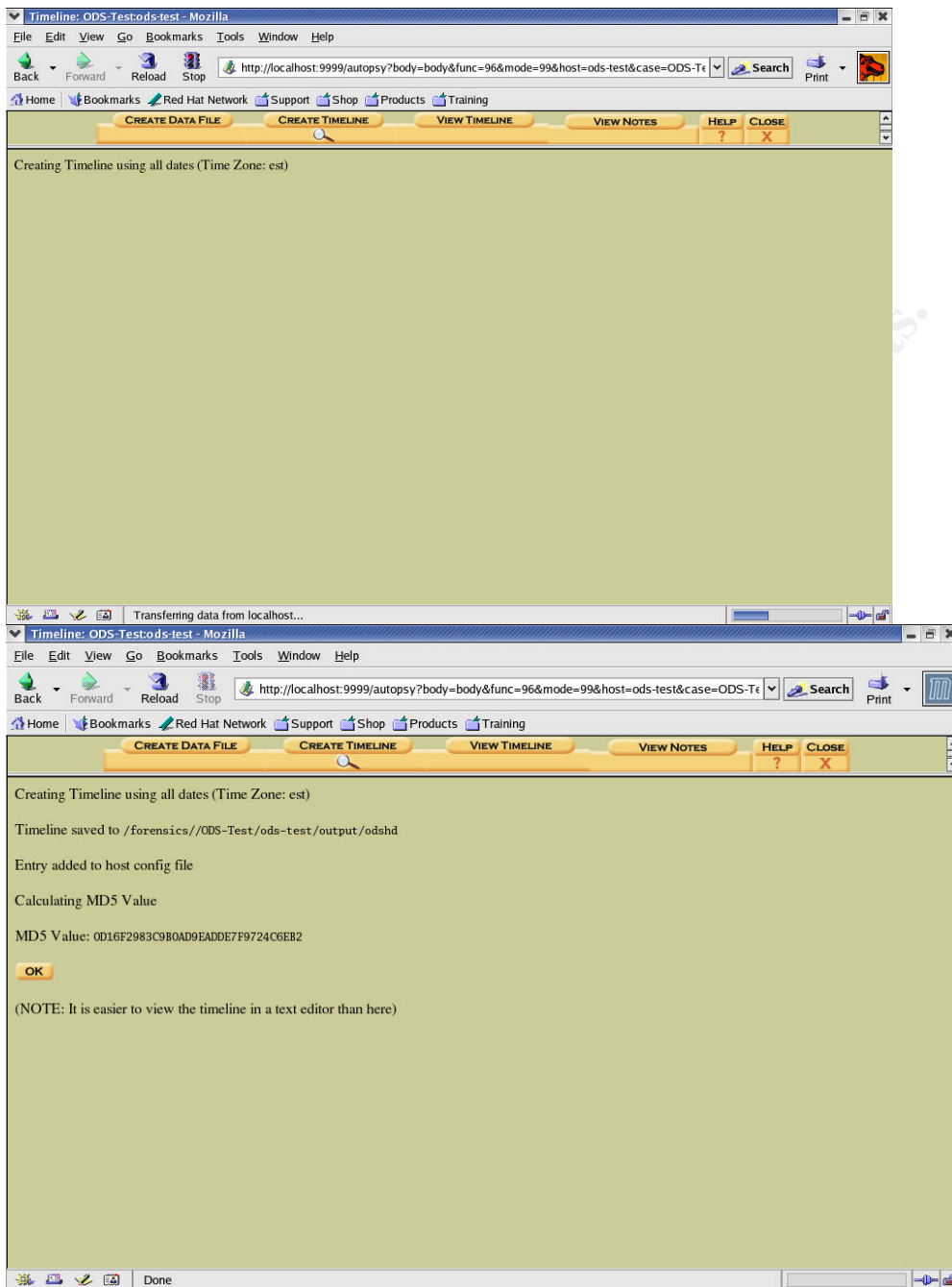
The system was originally installed on February 25th 2003 at 11:36AM EST as per the creation of the setuplog.txt
I decided that the most reliable method was to create the timeline in Autopsy. I began this with creating a data file:



I selected all available options which selected allocated files, unallocated files and unallocated Meta Data Structures . What this procedure does is provides a graphical interface to run the fls -r -m on the image file odshd.img. The fls command as diecribed on page 73 Sans Track 8 manual 8.3 allows

interaction with a forensic image as though it were a normal file system. It takes the inode value of a directory, processes the contents, and displays the file names in the directory (including deleted names).





I then opened the odshd timeline file in a text editor and began analyzing. The first entry is from 1995. The references in question point to older terminal emulation software which we use called QVTNet.

```
Tue Jul 11 1995 12:50:00 557664 m.. -/rwxrwxrwx 0 0 22237-128-3
/QPC/QVTNet/System/LT/OLE32.DLL
Tue Jul 11 1995 13:50:00 24576 m.. -/rwxrwxrwx 0 0 22193-128-3
/QPC/QVTNet/System/LT/AWCODC32.DLL
Mon Jul 31 1995 17:44:46 212480 m.. -/rwxrwxrwx 0 0 22240-128-3
/QPC/QVTNet/System/LT/PCDLIB32.DLL
```

```

Mon Oct 09 1995 20:58:32 10240 m.. -/rwxrwxrwx 0 0 22195-128-3
/QPC/QVTNet/System/LT/AWVIEW32.DLL
Sat Oct 28 1995 21:04:24 115796 m.. -/rwxrwxrwx 0 0 22188-128-3
/QPC/QVTNet/System/COMPLETE.WAV
Thu Nov 16 1995 22:39:50 11776 m.. -/rwxrwxrwx 0 0 22194-128-3
/QPC/QVTNet/System/LT/AWDENC32.DLL

```

Most of the other entries before the system was installed fall along the same lines. I saw nothing out of the ordinary. I then decided to concentrate on February 25th 2003 when the system was most likely installed. This is also supported by the creation of the base files: Tue Feb 25 2003 16:31:47 8192

```

mac -/r-xr-xr-x 48 0 7-128-1 /$Boot
224 mac -/r-xr-xr-x 0 0 9-144-1 /$Secure:$SDH
2560 mac -/r-xr-xr-x 48 0 4-128-4
/Ascential/DataStage/Engine/BP.O/CATALOG.PGMS (deleted-realloc)
0 mac -/r-xr-xr-x 0 0 8-128-2 /$BadClus
131072 mac -/r-xr-xr-x 0 0 10-128-1 /$UpCase
1634054144 mac -/r-xr-xr-x 0 0 8-128-1
/$BadClus:$Bad
0 mac -/r-xr-xr-x 48 0 3-128-3 /$Volume
328788 mac -/r-xr-xr-x 0 0 9-128-0 /$Secure:$SDS
200 mac -/r-xr-xr-x 0 0 9-144-2 /$Secure:$SII
4096 mac -/r-xr-xr-x 0 0 1-128-1 /$MFTMirr
53231616 mac -/r-xr-xr-x 0 0 2-128-1 /$LogFile

```

And this is also supported by the creation of the boot.ini file which is created dynamically. Tue Feb 25 2003 16:46:55 192 m.. -/r-xr-xr-x 0 0 2714-128-4 /boot.ini

There is a discrepancy of 5 hours from the creation of the setuplog.txt file. I then checked the creation of the setuplog.txt file in the timeline file. Tue Feb 25 2003 22:01:29 216338 ma. -/rwxrwxrwx 0 0 2727-128-4 /WINNT/setuplog.txt

The most likely creation time of the setuplog.txt was 10:01PM on Feb 25th 2003. I also confirmed on the live system that it was set to the right time zone. May factors could be contributed to the discrepancy including a faulty battery or incorrect time zone. This was duly noted but evidence does support that the system was originally was installed on Feb 25th 2003.

On June 24th 2003 there was some interesting activity: ServiceAnim.gif (deleted-realloc)

```

1398 ..c -/rwxrwxrwx 0 0 23114-128-3
/unzipped/csyservice/res/srvstate.bmp
4826 ..c -/rwxrwxrwx 0 0 22994-128-4
/unzipped/XMLPack-2.0.1/DialogSplash.cpp (deleted-realloc)
9718 ..c -/rwxrwxrwx 0 0 23106-128-4
/unzipped/csyservice/res/EarthWalkSoftware20.bmp

```

```

43104 ..c -/rwxrwxrwx 0 0 23002-128-3
/unzipped/csyservice/NTSERVIC.JPG
9164 ..c -/rwxrwxrwx 0 0 22996-128-4
/unzipped/csyservice/EditServiceDlg.cpp
6890 ..c -/rwxrwxrwx 0 0 23001-128-3
/unzipped/csyservice/NTSERVIC.HTM (deleted-realloc)
34769 ..c -/rwxrwxrwx 0 0 22993-128-4
/unzipped/XMLPack-2.0.1/CSysServicep.html (deleted-realloc)
3278 ..c -/rwxrwxrwx 0 0 23099-128-4
/unzipped/csyservice/NTServiceSetupDlg.h
2479 ..c -/rwxrwxrwx 0 0 23116-128-3
/unzipped/csyservice/resource.h
3258 ..c -/rwxrwxrwx 0 0 22989-128-4
/unzipped/csyservice/res/SysSecurity.h (deleted-realloc)
5900 ..c -/rwxrwxrwx 0 0 22991-128-4
/unzipped/csyservice/res/SysService.h (deleted-realloc)
11632 ..c -/rwxrwxrwx 0 0 23011-128-4
/unzipped/csyservice/NTServiceSetup.rc
11280 ..c -/rwxrwxrwx 0 0 22988-128-4
/unzipped/csyservice/Common/SysSecurity.cpp
551 ..c -/rwxrwxrwx 0 0 23007-128-1
/unzipped/csyservice/NTServiceSetup.dsw (deleted-realloc)
3717 ..c -/rwxrwxrwx 0 0 23101-128-3
/unzipped/csyservice/ReadMe.txt
3262 ..c -/rwxrwxrwx 0 0 23104-128-3
/unzipped/csyservice/res/devil.ico
2068 ..c -/rwxrwxrwx 0 0 23005-128-4
/unzipped/csyservice/NTServiceSetup.cpp
15678 ..c -/rwxrwxrwx 0 0 23110-128-4
/unzipped/XMLPack-2.0.1/img/NTServiceSetup30.bmp

```

The names of some of these files looked suspicious. I did a search on EarthWalk Software, which yielded two potentially useful URL's, but the links were dead.

EarthWalk Software Cookies. **EarthWalk Software**. Cookies. Documentation Download Implementation Links Copyright ... **EarthWalk Software**. ... www.geocities.com/jaywheeler.geo/perl/Cookies.html - 12k

EarthWalk Software Perl for Windows. **EarthWalk Software**. Copyright © 2001. Overview. ... installation. **EarthWalk Software**. Copyright © 2001. www.geocities.com/jaywheeler.geo/perl/activeperl.html - 14k

This new evidence led me to look on the hard drive once again for files in the /unzipped directory. I found a program with the ntservicesetup. Upon investigation I did a keyword search on ntservicesetup and was led to <http://dev-www.codeguru.com/Cpp/W-P/system/ntservices/article.php/c5713> which define the program as “**CSysService** is a C++ class which wraps methods around

several of the Win32. API service functions, providing an object-oriented interface to these functions, grouping common variables and structures in a single class object. The result is an extensible base class capable of installing, enumerating, modifying, controlling and removing a service application in the Service Control Manager."

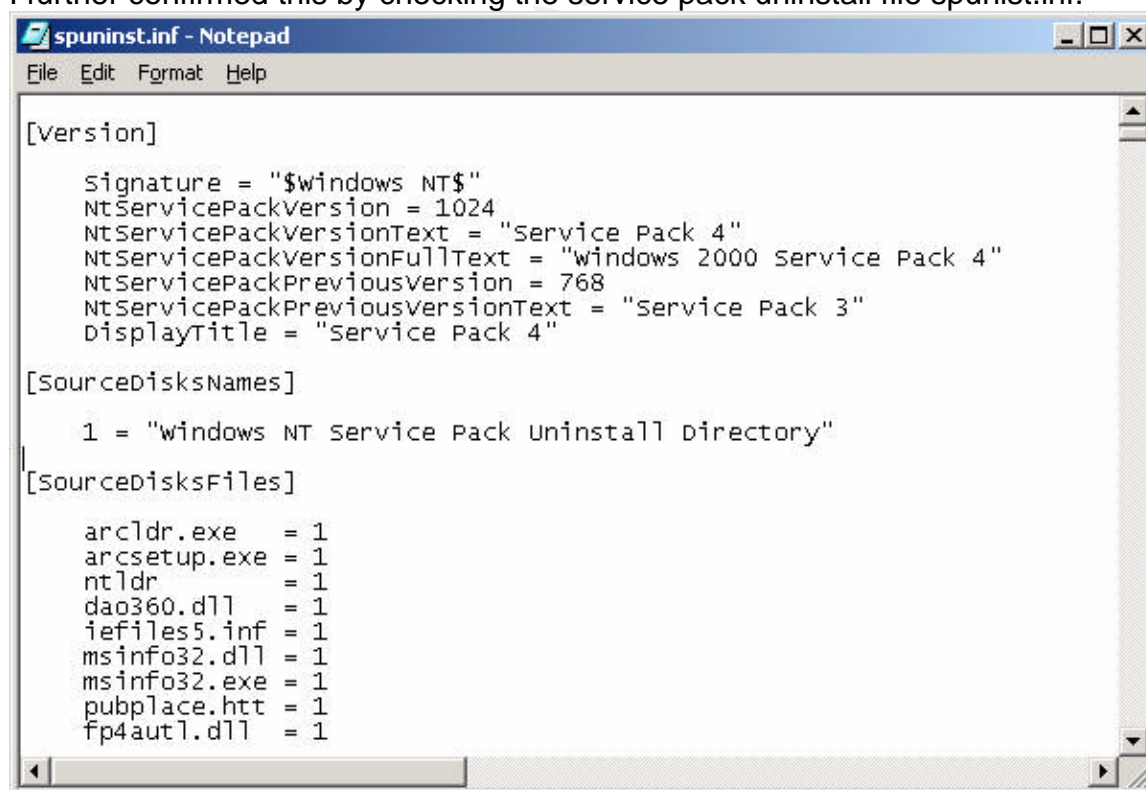
Since the computer is used for development it is most likely that the program is legitimate but it can also be used for malicious purposes. As indicated above in the sample there are some files that were deleted but there inodes were reallocated. The files deleted were gifs and could have been due to a reinstallation of the software.

My next step was to run some searches of suspect files found from my keyword search. These files included hidden32.exe, temp.mdb, klsys.exe, schd.exe which did not show up.

I also confirmed that Windows 2000 Service Pack 4 was installed on August 14th 2003

```
Thu Aug 14 2003 13:00:04  24848 .a. -/rwxrwxrwx 0      0      35301-128-3
/WINNT/system32/spdwnw2k.exe
                        600 mac d/drwxrwxrwx 0      0      35303-144-1
/WINNT/$NtServicePackUninstall$/spuninst
```

I further confirmed this by checking the service pack uninstall file spunist.inf.



```
spuninst.inf - Notepad
File Edit Format Help

[Version]

Signature = "$windows NT$"
NtServicePackVersion = 1024
NtServicePackVersionText = "Service Pack 4"
NtServicePackVersionFullText = "windows 2000 Service Pack 4"
NtServicePackPreviousVersion = 768
NtServicePackPreviousVersionText = "Service Pack 3"
DisplayTitle = "Service Pack 4"

[SourceDisksNames]

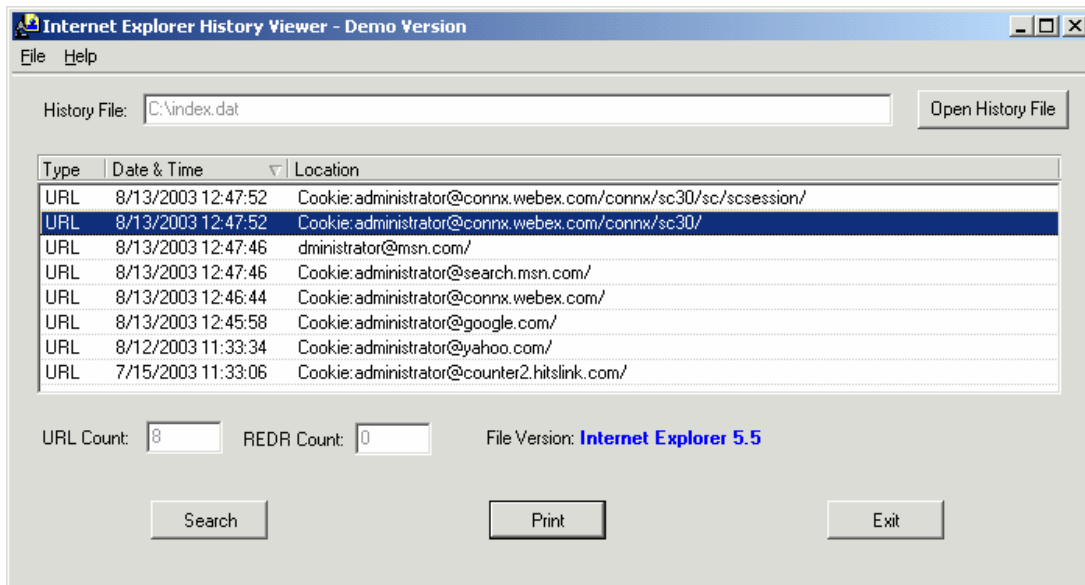
1 = "windows NT service Pack uninstall directory"

[SourceDisksFiles]

arcldr.exe = 1
arcsetup.exe = 1
ntldr = 1
dao360.dll = 1
iefiles5.inf = 1
msinfo32.dll = 1
msinfo32.exe = 1
pubplace.htt = 1
fp4aut1.dll = 1
```

Recover Deleted files

I used Autopsy to list all deleted files on the image. Many of them were files related to the data stage product. In the /document and settings/administrator/cookies directory I found a deleted index.dat file. I exported it using Autopsy and saved it in the root directory. I used the IE History Viewer to examine the contents. I found no questionable web sites.



The problem with listing deleted files in Autopsy is I found it difficult to export a list in a searchable format and due to the image size of 10gb and I had a memory limitation of 512mb and 1gb. I used the fls command to generate a list of deleted files. I used the -r -p and -d options -r = recursive -p=Display full path. The fls tool is part of the TASK and is used to collect timeline information as I demonstrated in the timeline section.

```
[Root@LinuxForensics root]# fls -rpd -f ntfs
```

```
/mnt/windows_forensic_server/odshd.img > /root/ods_deletedfiles
```

I now had a searchable and parseable list to conduct searches. I first

concentrated on the deleted files in /document and settings

Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/KGKAF6RN/top[1].vbs

I uncovered a deleted visual basic script. This file turned out to be a number conversion script. I exported the file and ran the more command on it.

```
[root@LinuxForensics root]# more images-odshd.img-
```

```
Documents.and.Settings.Administrator.Local.Settings.Temporary.Internet.Files.C  
ontent.IE5.KGKAF6RN.top.1..vbs.raw
```

```
Function vbsToLocaleDateString(sDate)
```

```
    vbsToLocaleDateString = FormatDateTime(CDate(sDate), vbLongDate)
```

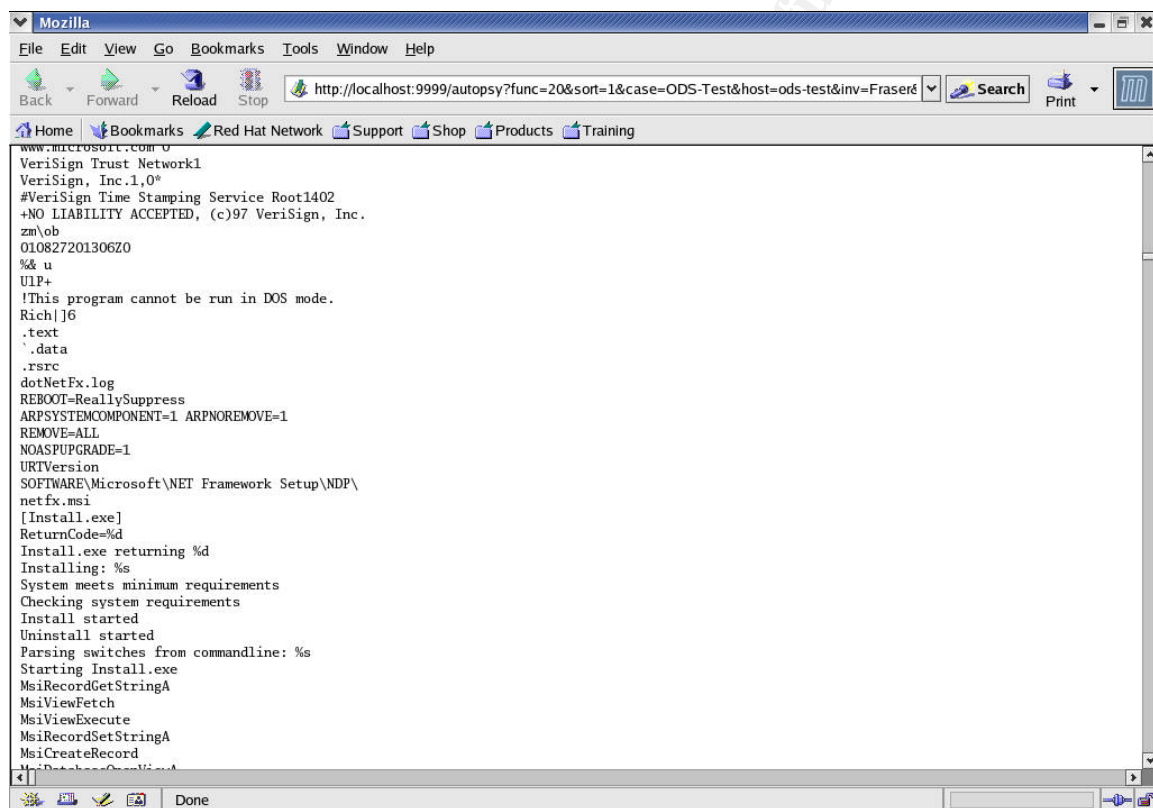
```
End Function
```

```
Function vbsToLocaleNumber(n)
```

```
vbsToLocaleNumber = FormatNumber(n)
End Function
```

Documents and Settings/connx/Local Settings/Temporary Internet Files/Content.IE5/ACNMAU7Z/dotnetfx_a86fd901dfe693e5d9465b4f89715da[1].exe

This file looked somewhat suspicious. I exported the file through Autopsy.
-rw----- 1 root root 24265736 Mar 14 13:04 images-odshd.img- Documents.and.Settings.connx.Local.Settings.Temporary.Internet.Files.Content.IE5.ACNMAU7Z.dotnetfx_a86fd901dfe693e5d9465b4f89715da.1..exe.raw
The file is 24 megs. I performed a strings on the file in Autopsy and ascertained that the file was actually installation files for .NET Framework.



I confirmed this by running the file on a test system.

As mentioned in the media analysis section ntdetect.com and ntldr were deleted and replaced. NTDetect was deleted and replaced on 2/25/2003 the day the system was originally loaded most like from a patch. Ntldr was deleted and replaced on 8/14/2003, which coincides with the installation of service pack4. Running a check on all deleted files. I checked the c:\winnt\system32\config for deleted files and all that was 4 userdiff.logs that were unrecoverable.

I began my examination of recycle bin. There were two recycler folders.
[root@LinuxForensics recycler]# pwd

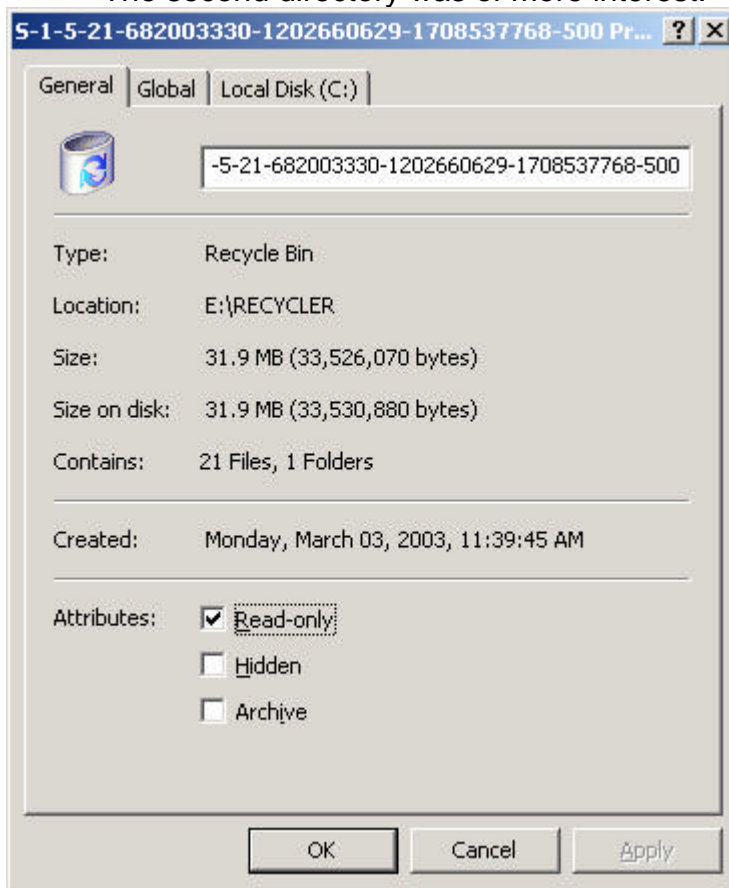

```

/mnt/windows_forensic_server/recycler
[root@LinuxForensics recycler]# ls
S-1-5-21-682003330-1202660629-1708537768-1001
S-1-5-21-682003330-1202660629-1708537768-500
[root@LinuxForensics recycler]# cd S-1-5-21-682003330-1202660629-
1708537768-1001
[root@LinuxForensics S-1-5-21-682003330-1202660629-1708537768-1001]# ls
-l
total 0
-r--r--r--  1 forensic users      65 Feb 11 10:07 desktop.ini
-r--r--r--  1 forensic users      20 Feb 11 19:07 INFO2

```

The S-1-5-21-682003330-1202660629-1708537768-1001 directory was not much interest with only desktop.ini. The directory was only 85k.

The second directory was of more interest:



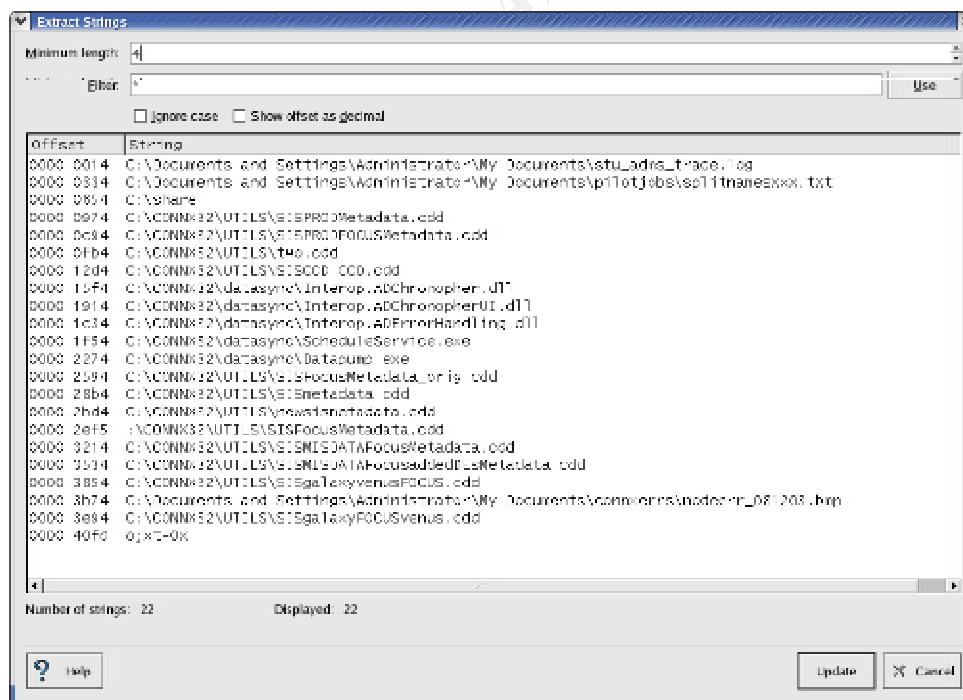
```

[root@LinuxForensics S-1-5-21-682003330-1202660629-1708537768-1001]# cd
..
[root@LinuxForensics recycler]# cd S-1-5-21-682003330-1202660629-
1708537768-500
[root@LinuxForensics S-1-5-21-682003330-1202660629-1708537768-500]# ls -l
total 0

```

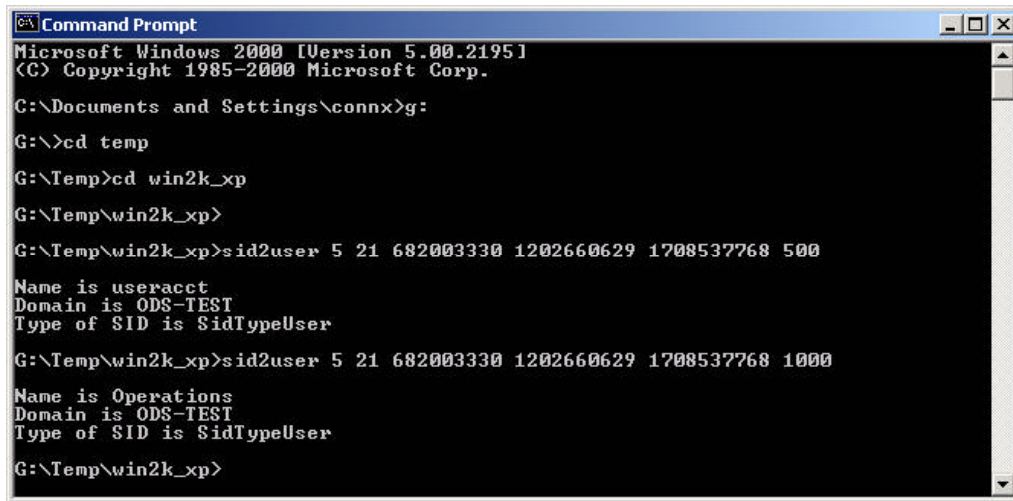

-r--r--r--	1 forensic users	13824 Jul 11 2001 Dc10.dll
-r--r--r--	1 forensic users	102400 Jun 24 2003 Dc11.exe
-r--r--r--	1 forensic users	229376 Jun 24 2003 Dc12.exe
-r--r--r--	1 forensic users	2264064 Mar 11 2003 Dc13.cdd
-r--r--r--	1 forensic users	1437696 Mar 11 2003 Dc14.cdd
-r--r--r--	1 forensic users	1417216 Mar 12 2003 Dc15.cdd
-r--r--r--	1 forensic users	2813440 Apr 4 2003 Dc16.cdd
-r--r--r--	1 forensic users	2686464 Mar 31 2003 Dc17.cdd
-r--r--r--	1 forensic users	4461568 Aug 12 2003 Dc18.cdd
-r--r--r--	1 forensic users	348454 Aug 12 2003 Dc19.bmp
-r--r--r--	1 forensic users	8183578 Mar 25 2003 Dc1.log
-r--r--r--	1 forensic users	4461568 Aug 13 2003 Dc20.cdd
-r--r--r--	1 forensic users	3841 Mar 28 2003 Dc2.txt
dr-xr-xr-x	1 forensic users	0 Mar 28 2003 Dc3
-r--r--r--	1 forensic users	480256 Apr 4 2003 Dc4.cdd
-r--r--r--	1 forensic users	864256 Apr 4 2003 Dc5.cdd
-r--r--r--	1 forensic users	2360320 Mar 12 2003 Dc6.cdd
-r--r--r--	1 forensic users	1319424 Mar 3 2003 Dc7.cdd
-r--r--r--	1 forensic users	57344 Sep 7 2001 Dc8.dll
-r--r--r--	1 forensic users	4096 Sep 6 2001 Dc9.dll
-r--r--r--	1 forensic users	65 Mar 21 2003 desktop.ini
-r--r--r--	1 forensic users	16820 Aug 14 2003 INFO2

I opened the INFO2 file with a hex editor and ran strings.



All of the deleted files coincide with the DataStage product. As indicated below the sid's of the owners of the recycle bin is operations and useracct.

Useracct is the renamed administrator account and operations is an administrator's account used for account maintenance.



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

C:\Documents and Settings\connx>g:
G:\>cd temp
G:\Temp>cd win2k_xp
G:\Temp\win2k_xp>sid2user 5 21 682003330 1202660629 1708537768 500
Name is useracct
Domain is ODS-TEST
Type of SID is SidTypeUser
G:\Temp\win2k_xp>sid2user 5 21 682003330 1202660629 1708537768 1000
Name is Operations
Domain is ODS-TEST
Type of SID is SidTypeUser
G:\Temp\win2k_xp>
```

String Searches

I found many interesting strings when I ran string searches through Autopsy the word “fuck” yielded me the best results. 114 occurrences of the word were in the image. This yielded a bounty of clues.

One of the references in my search was to [www.sponsoradulto](http://www.sponsoradulto.com) I did a search on that and found the site www.sponsoradulto.com. It was in all Spanish but I translated an FAQ page on the Google translation site http://www.google.com/language_tools?hl=en The site in question http://www.sponsoradulto.com/faq_respuesta.php?idr=23. The results are translated below. Turns out it was a sex site.

Te ofrecemos m•°s de 35 contenidos diferentes a promocionar con la idea de abarcar todas las •°reas del mercado del sexo. MilDescargas.com, DescargasMessenger.com, 10000Juegos.com, Contenidoxxx.com son solo algunos de los contenidos del dialer que te ofrecemos para promocionar. Disponemos de 3 diferentes salas de videochat en espa•±ol, c•°maras esp••a, miles de videos en l••nea, juegos animados en flash, miles y miles de fotograf••as, m•°s de 5000 relatos er••ticos, foros de contactos, pel••culas completas, y much••simo m•°s. Tambi•©n disponemos de contenidos gay y transexual con espect•°culos en directo las 24 horas del d••a.

We offer to you more than 35 contents different to promote with the idea to include all the areas of the market of sex. MilDescargas.com,

DescargasMessenger.com, 10000Juegos.com, Contenidoxxx.com are single some of the contents of dialer that we offer you to promote. We have 3 different rooms of videochat in Spanish, cameras spies on, thousand of videos in line, games animated in flash, thousands and thousands of photographs, more than 5000 erotic stories, forums of contacts, complete films, and very many more. Also we have contents gay and direct transsexual with spectacles in the 24 hours of the day.

String Contents of Cluster 2097121 (4096 bytes) in images/odshd.img

```
vXJ;  
$asctime(HH:)  
$+ ?]? ?[? $+  
!web.on  
%ws.homedir  
ws.loggi  
Webserve  
(wiark32.exe  
file rtos.exe  
%b0tvers  
hidden32.exe  
$exists(dll.bat)  
(store.dll  
    DrDivXReg  
KLSYS.EXE SVCH  
%\SCHD.EXE    TARGETDIR  
g`f  
clone kill  
winnt\temp\temp.mdb  
7TBOTe2  
/n /fh mIRC  
programs\startup  
alias topicscan {  
xists(STDE9.exe)  
psyBNC  
user=virus  
Acid & W4nk-h3r  
BNC v2.6.2  
$chr($round($calc(  
$chr($calc($asc($calc(  
($exists($mircdir $+  
.EXE  
.exe /n /fh /r  
://fly.to/
```

```

fucked now %
what a life..
bl.run
ping 68.42.116
65500 -n 999
(%bot.proxy !=      $portfree
secure.exe
%botchan
bl.run
ping
-w 0 -l
65000 -n 999
!FLOOD
FUCKING OWNZ
EMAILADDR $READ
$+ @ $+
$RAND(A,Z) $+ .
      %WGETCHAN
LOOD
[MIRC]
USER=
$RAND(A,Z) $+
EMAIL=
$RAND(A,Z)
CAL=GOVSUXPENIS
ALIP=HWHWHW
@PFUCK
17 IP/HOST:
%PFUCK.PO

```

Here is another piece of code I found from doing a search on trojan.
 ASCII Contents of Cluster 365576 (4096 bytes) in images/odshd.img

```

<SoftwareResourceLocator>
<LocatorComponent Class="Computer" Name="Return of computer name failed
error 111" />
<LocatorComponent Class="SoftwareProduct" Name="DataStage" />
<LocatorComponent Class="SoftwareGroup" SubClass="Project" Name="ODS"
/>
<LocatorComponent Class="SoftwareDesign" SubClass="Job"
Name="LoadFamAwardDisbursement" />
<LocatorComponent Class="SoftwareProcess" SubClass="Stage"
Name="Transformer_2" />

```

```

<LocatorComponent Class="SoftwareFlow" SubClass="Link"
Name="FAM_AWARD_DISBURSEMENT" />
</SoftwareResourceLocator>
</Event>
</Events>
</Run>.....
.....
.....JV/Spam-
NewsAgent...Spam-Nmb...Spam-QuickFyre..
Spam-Saddamme...Spam-SE..11...Spam-UnaBomber...Spam-Uy..40..
Spam-Winam...Spark...Speed...Speedup...Splash...Spoof95...Spoof/ICQSpoof..
    Spyderweb.. SpySender..b..    SpySender...SpyTec...SQLExec..
    StartPage...StealVXS...StealVXS.dr...StitchUp...Sttray...Sunfo...SVA...Swe
et..
Swlabs.kit...Sysag..dat...Sysag...Sysfles...Sysfles.scr1...Sysfles.scr2...Sysfles.sfx
...Systry...SysWin...TapeWorm...TapwWorm.ldr...Tarrat...Taz...TCPSpeed...Tele
Commando..cli..svr...Templar...Term...Tetas...Tetris...Texron..
    Texron.dr...The-
CID...Throat..svr..cli...Thus...THW.kit...TimeGluk...Titanic...Tix...Toad..upd..upd..
    TPStrojan...TPStrojan.e...TPStrojan.f...TPStrojan.f...Tracker...Traeger...Tr
ainer...Trojan Sockets.cli...Trojan Sockets.svr..
Kit-TSWSVK...Kit-TSWSVK.hlp...Tuil.dr...Tuil...Tuil.vxd...Tuptus..
Tuptus.ini..  Tuptus.dr...TVFKill...Tweak...UBSpws..
UBSpws.dll...Udp..102..
Ultras.kit...Uploader...Uploader..
Uploader-C.. URLKiller...URLSnoop...Vbkill.worm...Virhider...VoiceSpy...Volt
Client..
WebCracker...Webmailcrack...Weird...Wel...WGetMo...Win64...Winats..
    WinNuke98..
    WinCom.dr...WinCom...WinFck...WinFold...WinFold...WS...WinInfo..
WinInfo.dr..  Win/Annoy..  Win/Cluck...Win/Conreset...WinCrash..svr..cli.a..cli.b..
Win/Desant... Winduke...WinExit...WinHawk..  WinHelper..
WinHelper.ini..
Win/Keylogger..    WinKiller...WinKiller-B...WinPanic...Winsex..a..b..c..d..e..
Win/Thrush...WinBoot...Wincheck...WishMaster.kit...Wizard...Wmd...Wmd...Wmd
...Wmd..
WormInside...WSFT-Exploit...Perl/WSFT-
Exploit...WZBot...WZBot...XalNaga...Xela...Xninja..dr...Xninja...Y2Kaos...ZAKiller.
..Zmk...Zom...Zum...MultiDropper.cfg...MultiDropper.cfg...MultiDropper...MultiDro
pper...MultiDropper...MultiDropper-J...MultiDropper.cfg..a..b...MultiDropper-
M...MultiDropper-O...MultiDropper...MultiDropper-R...MultiDropper-
S...MultiDropper.cfg...MultiDropper-T...MultiDropper-U...MultiDropper-
V...MultiDropper-W...MultiDropper-X...MultiDropper-Y...MultiDropper-
AB...MultiDropper-AD...MultiDropper-AE...MultiDropper-AF...MultiDropper-
AG...MultiDropper-AH...MultiDropper-AJ...MultiDropper-AK...MultiDropper-

```

AL...MultiDropper-AM...MultiDropper-AN...MultiDropper-AO...MultiDropper-
 AP...MultiDropper.cfg...MultiDropper.cfg...MultiDropper.cfg...MultiDropper.cfg...M
 ultiDropper.cfg...MultiDropper-AS...MultiDropper-AT...MultiDropper-
 AU...MultiDropper-AV...MultiDropper-AW...MultiDropper-AX...MultiDropper-
 AY...MultiDropper-AZ...MultiDropper-BA...MutiDropper-BB...MultiDropper-
 BC...MultiDropper-BD...MultiDropper-
 BE...MultiDropper.cfg...MultiDropper.cfg...MultiDropper.cfg...MultiDropper.cfg...
 MultiDropper.gen...Multiple.dr...APSTrojan.gen18...APSTrojan.gen18..
 APStrojan..gen1.. APStrojan..gen2.. APStrojan..gen3..
 APStrojan..gen3b.. APStrojan..gen4.. APStrojan..gen5..
 APStrojan..gen5b.. APStrojan..gen5c.. APStrojan..gen6...APStrojan.dr..
 APStrojan.sfx..gen8..
 APStrojan.sfx..gen9..
 APStrojan.sfx..cc..
 APStrojan.sfx..gen11...APStrojan.cj.. APSTrojan...APStrojan.gg..
 APStrojan.sfx..au.. APSTrojan..he...APStrojan.hy.. APStrojan..gen18..
 APStrojan..jz

APStrojan is also a trojan and I looked up the information on Network Associate's web site. NA defines the trojan as follows:

"This trojan works as a password stealer, running in Windows memory monitoring your AOL logon account information and then sends this to an email address. This trojan was written in Visual Basic and has the standard icon associated with such applications (parallelogram with turquoise header bar). This trojan has a reliance on VBRUN300.DLL and also searches for the existence of WAOL.EXE in the following directories:

C:\aol30\waol.exe
 C:\aol30a\waol.exe
 C:\aol30b\waol.exe
 C:\aol25\waol.exe
 C:\aol25a\waol.exe
 C:\aol25b\waol.exe

Without these directories, the trojan is not applicable to the system. The trojan is 49,933 bytes in size and appears as the name WINSYST.EXE and WINSYSV.EXE. Both files are identical; running either of these files will result in copying itself to the C:\WINDOWS folder and also C:\WINDOWS\SYSTEM folder."

I have not been able prove that any of this code has been executed on the system. I have searched both for undeleted and deleted files associated with the trojans and found no traces. It appears that this code was randomly placed on the hard drive when it was infected.

I ran the strings command against the dump of the memory and piped the information to a file.

```
[root@LinuxForensics disk]# strings odsmem.img >/root/odsmem.str
```

I found some interesting returns on some searches as indicated below. The code is like the code I found on the hard drive image. Like before I found no evidence of the code being executed on the system. I traced some of the links I found including <http://www.ymg.urban.ne.jp/> It was a site in Japanese I ran the site against a translator and it was a Japanese ISP.

```
pwd=%s
Legend of Mir
\RUN
WYMUMA
SMTPPASS
    dow.open(
http://69.57
pizdetz      login.htm
CHECK THIS OUT
AND FUCK OUT!
DAPHOUSE.COM
CHECK THIS OUT
AND FUCK OUT!
DAPHOUSE.COM
```

Daphouse.com is a site in russian. I ran a translator to the main page and got the following results:

It is added krjak for Alcohol 120 % 1.4.8.1222 (thanks kamora!).

It is added kejgen for Nero Burning ROM 6.3.1.6 (thanks K@iser!).

It is laid out kejgen for FlashGet 1.6 beta 1 (thanks DOLTON!).

It is added serijnik for VentaFax 5.4 (thanks Denis!).

If you use any popular program, watch for her obnovlenijami and have for it medicines can become leaders of a corresponding heading on daphouse.com

[To make comments]

[14.03.2004]

Are laid out serijniki for Nero Burning Rom 6.3.0.3 and 6.3.0.6c (thanks inpave!).

[To make comments]

[07.03.2004]

Keys for DrWeb 4.31b (thanks DOLTON, +Darknbess +, Mortimer, Andrey are added!).

It is laid out keigen for Total Commander 6.02. (thanks Mortimer!).

Also the real key for Total Commander 6.02. (again thanks Mortimer is laid out!).

[To make comments]

[28.02.2004]

The key for Outpost Firewall Pro 2.1.292 (thanks Ghost is added!).

The key for TheBat is laid out! Versions 2.04 (thanks Den Frost!).

[To make comments]

This site is either a warze site or directory for a warze site. I also found a reference to The Legend of Mir video game.

InstallKbdHook
UninstallKbdHoo
password_err <password
<phone
sion\Run
pts/WWPMsg.dll?from
half-life:
&body=
CDKEY
<http://www.163.com/>

This site is also in Japanese.

a.txt
WlxActivateUserShell
WlxIsLockOk WlxLogoff
WlxActivateUserShell
WlxIsLockOk WlxLogofft
WlxLoggedOutSAS
mslogon32.dll
MSGINA.DLL
powrprof.dll,Lo
speednet.exe
files.del
ICQTOFILE
INSTALLHOOK

SAVEDEFOICQPASS
CALLWNDPROC
GWGhost.dll
ISUNSTA.dll
ISUnstA.DLLt
DllRegisterServ
FreeLibrary
HackSoft
word
.l&a
\Scanregw.exe
\svh0st.exe
exefile\shell\ope
\Scanregw.exe
ent\Version\Run
\Inter.hks.exet
comfil
Hack
word
Version\Run
Hack
sword
Version\Run
System32
\Scanreg8w
ystem32
HackS
NOOP
QUIT
/SCRIPTS/WWPMSG.DLL
VE\HALF-LIFE\SETTINGS
ATION FLASHPOINT
dialups: password:
cached pass:
hostips:
dialups: username: password:
ZZZZ
Hearty
by HMVS
dialups:
ger\Accounts\
::[PASSWORDS
HELO %s
mail.ru rsion\Run
SsWoRd
[RAS

4U2Ct
PaSsWoRd

by GriYo/29A

00cmd.exe

...: Hax0rcit

Win32ASM Remot

wWel

=UGS

neoWar

rotokol

\Run

Mousecapture

neoWar

egatez - Protok

www.neonew.de

Hackversuch!

stubs\Serv

lorerKlasse

svchost

sion\Run

\svchost.exe

.mirabil

neoW

\Active

svaccs

RCPT TO

ion\run

http://

.php

%s?s=%d

PRIVMSG

KILLTHREAD

INFO

READIRCLOG

SOCKS4

WIN32SERV.EXE

WIN33SERV.EX OWS\CURRE

KILLPROC

fuckmycpu

Kodikos

Kyrg

v2.5

.naro

ost:

ktwrm@

ResultOfWrmF
newkt98.zip
{[ZH}
command.
fx.sve
E\Numega
.l&A]\$
tallServ
dllInst
viceMain
ActiveS
svcho
BackD
EggDr
Spawn A
BackD
eggdrop
Disconne
EggD
ROd_
DevilFol
svchost
NT\Curr
DevilFol
KWind
WinSoc
{Ns{t
rosoft\Active Setup\Inst
RunServices
StubPath
#PORT
#SRVDELETE
user,disableoemla
cad_off
\getpwd.htm
[INJECT]
[LOGONINFO]
SimulateCtrlAltDel
SimulateMouseEv
forbidCtrlAltDel
HTTPSAPP
update,%d,%s
QUOTE PONG
:kill
allof%d
copy iis

ms3sprt.dll
inetsrv\met
amateur
babes
bondage
\shellexpi.exe
orer\Shell Folder
hw 2
ntlworld.com
I've been infect
FILE*
FILE*
BEGIN Event
EventType="End"
Message="Finished Job LoadCourseInformationUnrot2."
OccurredAt="2004-02-17 12:54:21"
CreationModel="DataStage6"
StatusCode="0"
BEGIN SoftwareResourceLocator
Computer="ods-test"
SoftwareProduct="DataStage"
SoftwareGroup(Project)="ODS"
SoftwareExecutable(Job)="LoadCourseInformationUnrot2"
END SoftwareResourceLocator
END Event
FILE*
FILE*
RCRD(
j,hP
h}h]

left by KoTuK
Hacker I.S.S.
SuperWork \$
5555-
boot
shell
+username+:+
Activ14_alf_
RasEnumEntri
EnableAutodial
http://wwp.
ipts/WWPMsg
y=l+am+
ghtSe
mail.ho

Default Archive File Cache Overridden With The Value %d
MCSCNAFC.TXT

API version (%s - %s) %s

Driver version %ld (%d.%d)

MCSCAN32.DLL

RELEASE

rwabs32.dll

4.3.20

EXTRA.DRV

REPAIR.DRV

NAMES.DRV

FIND.DRV

..... GFS Disabled

*

mcscan.log

mcscan.vlt

,could be a new

,found

,is like

application

killed

wannabee

test NOT a virus

joke

compressed using

trojan

virus

,not scanned (code %d)

,delete on reboot.

,symbolic link.

,corrupt compressed file.

,no repair info.

,rename denied.

,delete denied.

,corrupt file.

,zero length.

,caller denied.

,object incorrect.

,BCS file.

,circular link.

,access denied.

,load failure.

,component failure.

,driver failure.

,out of memory.

,encrypted.
,locked.
,not scanned (not executable).
%s, %u, %u, %u,
%s, %lu
seqnum_%ld_
seqnum_%ld_thread_%s_
.md5
%s %s, %s
%s, %u
%s, %u, %u, %u
%s, %s
%02X
%s %lu
%s%lu
,macros deleted
,contains macros
,re-checking
,repair failed.
,moved.
,renamed.
,deleted.
,repared.
,not repaired (code %d)
,no repair - out of memory.
,no repair - access denied.
,is ok.
, normal hit "%s"
, negative hit "%s"
%s %s
%s entering subdirectory.
"%s"
, "%s"
EXT[%s]MASK[%.8x] &
'%lu'
Scan started at: %s
NoFileName
LDCdnerekram_
Scan completed at: %s
%s: '%s'
tid=%s
tid=
%s%d
Timer, %u, 1/100ms,
Component failed
Engine fhbin

#{8c07dd50-7a8d-11d2-8f8c-00c04fbf8fef}&dmusic
{f18a0e88-c30c-11d0-8815-00a0c906bed8}
{fbf6f530-07b9-11d2-a71e-0000f8004788}
##?#SW#{a7c7a5b0-5af3-11d1-9ced-00a024bf0407}#{9B365890-165F-11D0-
A195-0020AFD156E4}#{fbf6f530-07b9-11d2-a71e-0000f8004788}
##?#
#SAD3
SymbolicLink
Devi
Device Parameters
CLSID
FriendlyName
DriverDate

Some code I found as indicated above was part of the McAfee AntiVirus program either from a live update or memory resident. The ISS is also mentioned ISS is Internet Security Systems Inc. a security consulting company which most notably reported a coordinated hacker attack on July 6th 2003. Finding the malicious code in memory is very dis-concerning. None of the executables or strings can be tied to any files.

Conclusions

Based on my findings there is more than sufficient evidence to recommend taking this system out of service, formatting it and reinstalling with very stringent security policies (A side note the new equipment replacing this system has just arrived.). Based on the sensitive nature of this system there are more risks than benefits in leaving the system running as is. I found a many security risks on the system. The most glaring was that everyone has full control on the NTFS file system. Basically any user guest or otherwise has full access to the system files. This is a major security risk especially with an FTP process being run with the Connx product.

The Networking department was not able to help me with any logs of any use showing any suspicious behavior. Once the system comes off-line further investigation will be warranted. The suspect system is blocked from the internet and all but a few subnets at my institution. Most likely the malicious data was transferred via other windows machine which have been infected. I am also recommending that a policy be implemented that any sensitive department process workstations or systems be place on a highly secured network accessible only via VPN.

I found no evidence of malice by any staffers at my institution. There were no mp3, pictures or other questionable material on the system. My examination of Internet Explorer data uncovered no adverse evidence other than remnants of trojans and the one registry entry IPROCESSDESTROY. There were many human procedural and security errors in the setting up and operation of this

system. My recommendations to management will include a VPN between the Administrative system this system and the SQL server, and security training for all personnel who configure desktop and server systems. Further, my recommendation will include an implementation of security policies on at the very least systems which handle sensitive data. Most of the malware I found on the system looked to be viral and attempts at accessing the system case in point the malicious code found in the page file. It is possible that the code is from memory and is randomly written to the disk if the system was powered off or rebooted in an unstable manner.

Hopefully this investigation will serve as a wakeup call to management that a major overhaul of the institutions security procedures and policies. The first step would be a risk assessment followed by an implementation plan. The liability is great if any information could be siphoned from this system. This system certainly is an accident waiting to happen.

Part III – Legal Issues of Incident Handling

- A. The following Federal laws would apply to the suspect if he was distributing copyrighted material.
U.S. Copyright Law {Title 17 U.S.C. Section 101 et seq., Title 18 U.S.C. Section 2319} The law prohibits the distribution of copyrighted material recorded after 1972. Also **17 U.S.C. 506**. Would apply if the offender was distributing the material for profit. I have cited the full text of 17 USC. 506 below. Depending on the value of the material seized is what penalties will be assessed. Fines and penalties can range from \$1000-\$2500 and 1-10 years in jail per convicted offense.

17 U.S.C. 506.

§ 506. Criminal offenses

(a) Criminal Infringement.--Any person who infringes a copyright willfully either--

(1) for purposes of commercial advantage or private financial gain, or

(2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than \$1,000, shall be punished as provided under section 2319 of title 18, United States Code. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.

(b) Forfeiture and Destruction.--When any person is convicted of any violation of subsection (a), the court in its judgment of conviction shall, in addition to the penalty therein prescribed, order the forfeiture and destruction or other disposition of all infringing copies or phonorecords and all implements, devices, or equipment used in the manufacture of such infringing copies or phonorecords.

(c) Fraudulent Copyright Notice.--Any person who, with fraudulent intent, places on any article a notice of copyright or words of the same purport that such person knows to be false, or who, with fraudulent intent, publicly distributes or imports for public distribution any article bearing such notice or words that such person knows to be false, shall be fined not more than \$2,500.

(d) Fraudulent Removal of Copyright Notice.--Any person who, with fraudulent intent, removes or alters any notice of copyright appearing on a copy of a copyrighted work shall be fined not more than \$2,500.

(e) False Representation.--Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 409, or in any written statement filed in connection with the application, shall be fined not more than \$2,500.

(f) Rights of Attribution and Integrity.--Nothing in this section applies to infringement of the rights conferred by section 106A(a)

18 U.S.C. 2319.

Criminal Infringement of a Copyright

§ 2319. Criminal Infringement of a Copyright

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b) and (c) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.

(b) Any person who commits an offense under section 506(a)(1) of title 17--

(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than \$2,500;

(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.

(c) Any person who commits an offense under section 506(a)(2) of title 17, United States Code--

(1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of \$2,500 or more;

(2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than \$1,000.

(d)

(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim.

(2) Persons permitted to submit victim impact statements shall include--

(A) producers and sellers of legitimate works affected by conduct involved in the offense;

(B) holders of intellectual property rights in such works; and

(C) the legal representatives of such producers, sellers, and holders.

(e) As used in this section--

(1) the terms "phonorecord" and "copies" have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17; and

(2) the terms "reproduction" and "distribution" refer to the exclusive rights of a copyright owner under clauses (1) and (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 120, of title 17.

- B. The appropriate steps to take if I were to find the information on my systems would be to follow incident handling procedures. I would first verify the incident then perform a minimal check of the system and its contents then a full forensic analysis. I would get the logs from our IDS, Firewalls, Routers, Mail and File servers. Under 18 USC 2511 (2) (a) i) it states "Authorized employees or agents of communication service providers may intercept and disclose communications in self-defense to protect the providers' rights and property." Since the computers are owned by my organization and all of the information is its property I would not need to obtain a warrant or permission from the users to investigate the system. At my institution as directed by the NJ Attorney General's office all information on a computer owned by the state of NJ is the property of the State.
- C. If my corporate counsel decided not to pursue this infraction I would tag all evidence seized and log it. I would place all of the evidence in sealed envelopes with the date, time and a brief description on the envelope. I would either lock the evidence in my safe or turn the evidence over to our counsel to be stored obtaining the proper signatures and receipts to preserve the custody and chain of the evidence.
- D. If John Price were distributing child pornography general procedure would be to contact the local field office of the FBI. However, at my institution we have an in house commissioned police department and institutional policy is to report all suspected crimes there and they would involve other law enforcement agencies. Our local agency would lead the investigation. Under the U. S. C [TITLE 18](#) > [PART I](#) > [CHAPTER 110](#) > Sec. 2252A. If it can be proven that Mr. Price received, emailed or distributed the child pornography he would be guilty. The law does not allow for much room it is a crime just to be in possession of the material. I would then turn over all of my notes and tagged evidence over to the law enforcement agency investigating the crime and make myself available to answer questions or act as a witness.

Appendix I Useful Links

Useful Links Section 1

<http://www.forinsect.de/forensics/forensics-tools.php>
http://www.its.bldrdoc.gov/projects/devglossary/_mp3.html
http://www.linuxsecurity.com/feature_stories/data-hiding-forensics.html
<http://build.lnx-bbc.org/packages/fs/bmap.html>
<http://www.e-evidence.info/other.html>
<http://www.phrack.org/show.php?p=59&a=6>

Legal Resources Section 1

<http://www.riaa.com/issues/copyright/laws.asp#uscopyright>
<http://www.cybergov.gov>

Useful Links Section 2

<http://users.erols.com/gmgarner/forensics/>
<http://www.sleuthkit.org/>
<http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/tips/setuplog.msp>
<http://www.tripwire.com>
<http://www.nai.com>
<http://www.legendofmir.net>
<http://www.iss.net>
<http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,82730,00.html>
<http://dev-www.codeguru.com/Cpp/W-P/system/ntservices/article.php/c5713>
http://vil.nai.com/vil/content/v_10477.htm

Useful Links Section 3

<http://www4.law.cornell.edu/uscode/18/2252A.html>
<http://trac.syr.edu/laws/18USC2251.html>
<http://www.riaa.com/issues/copyright/laws.asp>

Software Vendors of software running on the suspect system.

<http://www.connx.com/products/connx.html>
<http://www.sct.com>
<http://www.ascential.com>

Appendix II Excerpt of NJ Criminal Code

2C:20-8. Theft of Services.

a. A person is guilty of theft if he purposely obtains services which he knows are available only for compensation, by deception or threat, or by false token, slug, or other means, including but not limited to mechanical or electronic devices or

through fraudulent statements, to avoid payment for the service. "Services" include labor or professional service; transportation, telephone, telecommunications, electric, water, gas, cable television, or other public service; accommodation in hotels, restaurants or elsewhere; entertainment; admission to exhibitions; use of vehicles or other movable property. Where compensation for service is ordinarily paid immediately upon the rendering of such service, as in the case of hotels and restaurants, absconding without payment or offer to pay gives rise to a presumption that the service was obtained by deception as to intention to pay.

b. A person commits theft if, having control over the disposition of services of another, to which he is not entitled, he knowingly diverts such services to his own benefit or to the benefit of another not entitled thereto.

c. Any person who, without permission and for the purpose of obtaining electric current, gas or water with intent to defraud any vendor of electricity, gas or water or a person who is furnished by a vendor with electric current, gas or water:

(1) Connects or causes to be connected by wire or any other device with the wires, cables or conductors of any such vendor or any other person; or

(2) Connects or disconnects the meters, pipes or conduits of such vendor or any other person or in any other manner tampers or interferes with such meters, pipes or conduits, or connects with such meters, pipes or conduits by pipes, conduits or other instruments--is guilty of a disorderly persons offense.

The existence of any of the conditions with reference to meters, pipes, conduits or attachments, described in this subsection, is presumptive evidence that the person to whom gas, electricity or water is at the time being furnished by or through such meters, pipes, conduits or attachments has, with intent to defraud, created or caused to be created with reference to such meters, pipes, conduits or attachments, the condition so existing; provided, however, that the presumption shall not apply to any person so furnished with gas, electricity or water for less than 31 days or until there has been at least one meter reading.

A violation of this subsection shall be deemed to be a continuing offense as long as the conditions described in this subsection exist.

d. Any person who, without permission or authority, connects or causes to be connected by wires or other devices, any meter erected or set up for the purpose of registering or recording the amount of electric current supplied to any customer by any vendor of electricity within this State, or changes or shunts the wiring leading to or from any such meter, or by any device, appliance or means whatsoever tampers with any such meter so that the meter will not measure or record the full amount of electric current supplied to such customer, is guilty of a disorderly persons offense.

The existence of any of the conditions with reference to meters or attachments described in this subsection is presumptive evidence that the person to whom electricity is at the time being furnished by or through such meters or attachments has, with intent to defraud, created or caused to be created with reference to such meters or attachments, the condition so existing; provided, however, that the presumption shall not apply to any person so furnished with electricity for less than 31 days or until there has been at least one meter reading.

A violation of this subsection shall be deemed to be a continuing offense as long as the conditions described in this subsection exist.

e. Any person who, with intent to obtain cable television service without payment, in whole or in part, of the lawful charges therefor, or with intent to deprive another of the lawful receipt of such service, damages, cuts, tampers with, installs, taps or makes any connection with, or who displaces, removes, injures or destroys any wire, cable, conduit, apparatus or equipment of a cable television company operating a CATV system; or who, without authority of a cable television company, intentionally prevents, obstructs or delays, by any means or contrivance, the sending, transmission, conveyance, distribution or receipt of programming material carried by equipment of the cable television company operating a CATV system, is a disorderly person.

The existence of any of the conditions with reference to wires, cables, conduits, apparatus or equipment described in this subsection is presumptive evidence that the person to whom cable television service is at the time being furnished has, with intent to obtain cable television service without authorization or compensation or to otherwise defraud, created or caused to be created the condition so existing.

f. Any person who purposely or knowingly manufactures, constructs, sells, offers for sale, distributes or installs any equipment, device or instrument designed or intended to facilitate the interception, decoding or receipt of any cable television service with intent to obtain such service and avoid the lawful payment of the charges therefor to the provider, in whole or in part, is a disorderly person.

Any communications paraphernalia prohibited under this subsection shall be subject to forfeiture and may be seized by the State or any law enforcement officer in accordance with the provisions of N.J.S.2C:64-1 et seq.

g. Any person who purposely or knowingly maintains or possesses any equipment, device or instrument of the type described in subsection f. of this section or maintains or possesses any equipment, device or instrument actually used to facilitate the interception, decoding or receipt of any cable television

service with intent to obtain such service and avoid the lawful payment, in whole or in part, of the charges therefor to the provider, is a disorderly person.

Any communications paraphernalia prohibited under this subsection shall be subject to forfeiture and may be seized by the State or any law enforcement officer in accordance with the provisions of N.J.S.2C:64-1 et seq.

h. Any person who, with the intent of depriving a telephone company of its lawful charges therefor, purposely or knowingly makes use of any telecommunications service by means of the unauthorized use of any electronic or mechanical device or connection, or by the unauthorized use of billing information, or by the use of a computer, computer equipment or computer software, or by the use of misidentifying or misleading information given to a representative of the telephone company is guilty of a crime of the third degree.

The existence of any of the conditions with reference to electronic or mechanical devices, computers, computer equipment or computer software described in this subsection is presumptive evidence that the person to whom telecommunications service is at the time being furnished has, with intent to obtain telecommunications service without authorization or compensation or to otherwise defraud, created or caused to be created the condition so existing.

i. Any person who purposely or knowingly manufactures, constructs, sells, offers for sale, distributes, installs, or otherwise provides any service, equipment, device, computer, computer equipment, computer software or instrument designed or intended to facilitate the receipt of any telecommunications service and avoid the lawful payment of the charges therefor to the provider, in whole or in part, is guilty of a crime of the third degree.

Any communications paraphernalia, computer, computer equipment or computer software prohibited under this subsection shall be subject to forfeiture and may be seized by the State or any law enforcement officer in accordance with the provisions of N.J.S.2C:64-1 et seq.

j. Any person who purposely or knowingly maintains or possesses any equipment, device, computer, computer equipment, computer software or instrument of the type described in subsection i. of this section, or maintains or possesses any equipment, device, computer, computer equipment, computer software or instrument actually used to facilitate the receipt of any telecommunications service with intent to obtain such service and avoid the lawful payment, in whole or in part, of the charges therefor to the provider, is guilty of a crime of the third degree.

Any communications paraphernalia, computer, computer equipment or computer software prohibited under this subsection shall be subject to forfeiture and may

be seized by the State or any law enforcement officer in accordance with the provisions of N.J.S.2C:64-1 et seq.

k. In addition to any other disposition authorized by law, and notwithstanding the provisions of N.J.S.2C:43-3, every person who violates this section shall be sentenced to make restitution to the vendor and to pay a minimum fine of \$500.00 for each offense. In determining the amount of restitution, the court shall consider the costs expended by the vendor, including but not limited to the repair and replacement of damaged equipment, the cost of the services unlawfully obtained, investigation expenses, and attorney fees.

l. The presumptions of evidence applicable to offenses defined in subsections c., d., e. and h. of this section shall also apply in any prosecution for theft of services brought pursuant to the provisions of subsection a. or b. of this section.

Amended 1983, c.15, s.1; 1985, c.10; 1989, c.112; 1997, c.6, s.4.

2C:20-23 Definitions - Computer-related Crimes

2.As used in this act:

a."Access" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer storage medium, computer system, or computer network.

b."Computer" means an electronic, magnetic, optical, electrochemical or other high speed data processing device or another similar device capable of executing a computer program, including arithmetic, logic, memory, data storage or input-output operations and includes all computer equipment connected to such a device, computer system or computer network, but shall not include an automated typewriter or typesetter or a portable, hand-held calculator.

c."Computer equipment" means any equipment or devices, including all input, output, processing, storage, software, or communications facilities, intended to interface with the computer.

d."Computer network" means the interconnection of communication lines, including microwave or other means of electronic communications, with a computer through remote terminals, or a complex consisting of two or more interconnected computers, and shall include the Internet.

e."Computer program" means a series of instructions or statements executable on a computer, which directs the computer system in a manner to produce a desired result.

f. "Computer software" means a set of computer programs, data, procedures, and associated documentation concerned with the operation of a computer system.

g. "Computer system" means a set of interconnected computer equipment intended to operate as a cohesive system.

h. "Data" means information, facts, concepts, or instructions contained in a computer, computer storage medium, computer system, or computer network. It shall also include, but not be limited to, any alphanumeric, hexadecimal, octal or binary code.

i. "Data base" means a collection of data.

j. "Financial instrument" includes but is not limited to a check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security and any computer representation of these items.

k. "Services" includes but is not limited to the use of a computer system, computer network, computer programs, data prepared for computer use and data contained within a computer system or computer network.

l. "Personal identifying information" shall have the meaning set forth in subsection a. of N.J.S.2C:21-17, and shall also include passwords and other codes that permit access to any data, data base, computer, computer storage medium, computer program, computer software, computer equipment, computer system or computer network, where access is intended to be secure, restricted or limited.

m. "Internet" means the international computer network of both federal and non-federal interoperable packet switched data networks.

n. "Alter," "damage" or "destroy" shall include, but not be limited to, any change or impairment to the integrity or availability of any data or other information, data base, computer program, computer software, computer equipment, computer, computer storage medium, computer system, or computer network by any means including introduction of a computer contaminant.

o. "User of computer services" shall include, but not be limited to, any person, business, computer, computer network, computer system, computer equipment or any other device which makes use of any resources of a computer, computer network, computer system, computer storage medium, computer equipment, data or data base.

p. "Computer contaminant" means any set of computer instructions that are designed to alter, damage, destroy, record or transmit information within a computer, computer system or computer network without the authorization of the

owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, alter, damage, destroy, record or transmit data or in some other fashion usurp the normal operation of the computer, computer program, computer operations, computer services or computer network.

q."Authorization" means permission, authority or consent given by a person who possesses lawful authority to grant such permission, authority or consent to another person to access, operate, use, obtain, take, copy, alter, damage or destroy a computer, computer network, computer system, computer equipment, computer software, computer program, computer storage medium, or data. An actor has authorization if a reasonable person would believe that the act was authorized.

L.1984,c.184,s.2; amended 2003, c.39, s.1.

2C:20-24 Value of property or services; additional measures.

3.For the purposes of this act, the value of any property or services, including the use of computer time, shall be their fair market value, if it is determined that a willing buyer and willing seller exist. Value shall include the cost of repair or remediation of any damage caused by an unlawful act and the gross revenue from any lost business opportunity caused by the unlawful act. The value of any lost business opportunity may be determined by comparison to gross revenue generated before the unlawful act that resulted in the lost business opportunity. Value shall include, but not be limited to, the cost of generating or obtaining data and storing it within a computer or computer system.

L.1984,c.184,s.3; amended 2003, c.39, s.2.

2C:20-25 Computer criminal activity; degree of crime; sentencing.

4.A person is guilty of computer criminal activity if the person purposely or knowingly and without authorization, or in excess of authorization:

a.Accesses any data, data base, computer storage medium, computer program, computer software, computer equipment, computer, computer system or computer network;

b.Alters, damages or destroys any data, data base, computer, computer storage medium, computer program, computer software, computer system or computer network, or denies, disrupts or impairs computer services, including access to any part of the Internet, that are available to any other user of the computer services;

c. Accesses or attempts to access any data, data base, computer, computer storage medium, computer program, computer software, computer equipment, computer system or computer network for the purpose of executing a scheme to defraud, or to obtain services, property, personal identifying information, or money, from the owner of a computer or any third party;

d. (Deleted by amendment, P.L.2003, c.39).

e. Obtains, takes, copies or uses any data, data base, computer program, computer software, personal identifying information, or other information stored in a computer, computer network, computer system, computer equipment or computer storage medium; or

f. Accesses and recklessly alters, damages or destroys any data, data base, computer, computer storage medium, computer program, computer software, computer equipment, computer system or computer network.

g. A violation of subsection a. of this section is a crime of the third degree. A violation of subsection b. is a crime of the second degree. A violation of subsection c. is a crime of the third degree, except that it is a crime of the second degree if the value of the services, property, personal identifying information, or money obtained or sought to be obtained exceeds \$5,000. A violation of subsection e. is a crime of the third degree, except that it is a crime of the second degree if the data, data base, computer program, computer software, or information:

(1) is or contains personal identifying information, medical diagnoses, treatments or other medical information concerning an identifiable person;

(2) is or contains governmental records or other information that is protected from disclosure by law, court order or rule of court; or

(3) has a value exceeding \$5,000.

A violation of subsection f. is a crime of the fourth degree, except that it is a crime of the third degree if the value of the damage exceeds \$5,000.

A violation of any subsection of this section is a crime of the first degree if the offense results in:

(1) a substantial interruption or impairment of public communication, transportation, supply of water, gas or power, or other public service. The term "substantial interruption or impairment" shall mean such interruption or impairment that:

- (a)affects 10 or more structures or habitations;
- (b)lasts for two or more hours; or
- (c)creates a risk of death or significant bodily injury to any person;
- (2)damages or loss in excess of \$250,000; or
- (3)significant bodily injury to any person.

Every sentence of imprisonment for a crime of the first degree committed in violation of this section shall include a minimum term of one-third to one-half of the sentence imposed, during which term the defendant shall not be eligible for parole.

h. Every sentence imposed upon a conviction pursuant to this section shall, if the victim is a government agency, include a period of imprisonment. The period of imprisonment shall include a minimum term of one-third to one-half of the sentence imposed, during which term the defendant shall not be eligible for parole. The victim shall be deemed to be a government agency if a computer, computer network, computer storage medium, computer system, computer equipment, computer program, computer software, computer data or data base that is a subject of the crime is owned, operated or maintained by or on behalf of a governmental agency or unit of State or local government or a public authority. The defendant shall be strictly liable under this subsection and it shall not be a defense that the defendant did not know or intend that the victim was a government agency, or that the defendant intended that there be other victims of the crime.

A violation of any subsection of this section shall be a distinct offense from a violation of any other subsection of this section, and a conviction for a violation of any subsection of this section shall not merge with a conviction for a violation of any other subsection of this section or section 10 of P.L.1984, c.184 (C.2C:20-31), or for conspiring or attempting to violate any subsection of this section or section 10 of P.L.1984, c.184 (C.2C:20-31), and a separate sentence shall be imposed for each such conviction.

When a violation of any subsection of this section involves an offense committed against a person under 18 years of age, the violation shall constitute an aggravating circumstance to be considered by the court when determining the appropriate sentence to be imposed.

Appendix 3 – US Child Pornography Laws

18USC2251

CITE

18 USC Sec. 2251 -- 01/05/99

EXPCITE

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 110 - SEXUAL EXPLOITATION AND OTHER ABUSE OF
CHILDREN

HEAD

Sec. 2251. Sexual exploitation of children

STATUTE

(a) Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, shall be punished as provided under subsection (d), if such person knows or has reason to know that such visual depiction will be transported in interstate or foreign commerce or mailed, if that visual depiction was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported in interstate or foreign commerce or mailed.

(b) Any parent, legal guardian, or person having custody or control of a minor who knowingly permits such minor to engage in, or to assist any other person to engage in, sexually explicit conduct for the purpose of producing any visual depiction of such conduct shall be punished as provided under subsection (d) of this section, if such parent, legal guardian, or person knows or has reason to know that such visual depiction will be transported in interstate or foreign commerce or mailed, if that visual depiction was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported in interstate or foreign commerce or mailed.

(c)(1) Any person who, in a circumstance described in paragraph (2), knowingly makes, prints, or publishes, or causes to be made, printed, or published, any notice or advertisement seeking or offering -

(A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; or

(B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;
shall be punished as provided under subsection (d).

(2) The circumstance referred to in paragraph (1) is that -

(A) such person knows or has reason to know that such notice or advertisement will be transported in interstate or foreign commerce by any means including by computer or mailed; or

(B) such notice or advertisement is transported in interstate or foreign commerce by any means including by computer or mailed.

(d) Any individual who violates, or attempts or conspires to violate, this section shall be fined under this title or imprisoned not less than 10 years nor more than 20 years, and (FOOTNOTE 1) both, but if such person has one prior conviction under this chapter, chapter 109A, or chapter 117, or under the laws of any State relating to the sexual exploitation of children, such person shall be fined under this title and imprisoned for not less than 15 years nor more than 30 years, but if such person has 2 or more prior convictions under this chapter, chapter 109A, or chapter 117, or under the laws of any State relating to the sexual exploitation of children, such person shall be fined under this title and imprisoned not less than 30 years nor more than life. Any organization that violates, or attempts or conspires to violate, this section shall be fined under this title. Whoever, in the course of an offense under this section, engages in conduct that results in the death of a person, shall be punished by death or imprisoned for any term of years or for life.

(FOOTNOTE 1) So in original. Probably should be "or".

SOURCE

(Added Pub. L. 95-225, Sec. 2(a), Feb. 6, 1978, 92 Stat. 7; amended Pub. L. 98-292, Sec. 3, May 21, 1984, 98 Stat. 204; Pub. L. 99-500, Sec. 101(b) (title VII, Sec. 704(a)), Oct. 18, 1986, 100 Stat. 1783-39, 1783-75, and Pub. L. 99-591, Sec. 101(b) (title VII, Sec. 704(a)), Oct. 30, 1986, 100 Stat. 3341-39, 3341-75; Pub. L. 99-628, Sec. 2, 3, Nov. 7, 1986, 100 Stat. 3510; Pub. L. 100-690, title VII, Sec. 7511(a), Nov. 18, 1988, 102 Stat. 4485; Pub. L. 101-647, title XXXV, Sec. 3563, Nov. 29, 1990, 104 Stat. 4928; Pub. L. 103-322, title VI, Sec. 60011, title

XVI, Sec. 160001(b)(2), (c), (e), title XXXIII, Sec. 330016(1)(S)-(U), Sept. 13, 1994, 108 Stat. 1973, 2037, 2148; Pub. L. 104-208, div. A, title I, Sec. 101(a) (title I, Sec. 121(4)), Sept. 30, 1996, 110 Stat. 3009, 3009-26, 3009-30; Pub. L. 105-314, title II, Sec. 201, Oct. 30, 1998, 112 Stat. 2977.)

COD

CODIFICATION

Pub. L. 99-591 is a corrected version of Pub. L. 99-500.

MISC3

AMENDMENTS

1998 - Subsec. (a). Pub. L. 105-314, Sec. 201(a), inserted "if that visual depiction was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer," before "or if".

Subsec. (b). Pub. L. 105-314, Sec. 201(b), inserted ", if that visual depiction was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer," before "or if".

Subsec. (d). Pub. L. 105-314, Sec. 201(c), substituted ", chapter 109A, or chapter 117" for "or chapter 109A" in two places.

1996 - Subsec. (d). Pub. L. 104-208 amended subsec. (d) generally. Prior to amendment, subsec. (d) read as follows: "Any individual who violates, or attempts or conspires to violate, this section shall be fined under this title, imprisoned not more than 10 years, or both, but, if such individual has a prior conviction under this chapter or chapter 109A, such individual shall be fined under this title, imprisoned not less than five years nor more than 15 years, or both. Any organization which violates, or attempts or conspires to violate, this section shall be fined under this title. Whoever, in the course of an offense under this section, engages in conduct that results in the death of a person, shall be punished by death or imprisoned for any term of years or for life."

1994 - Pub. L. 103-322, Sec. 330016(1)(S)-(U), which directed the amendment of this section by substituting "under this title" for "not more than \$100,000", "not more than \$200,000", and "not more than \$250,000", could not be executed because those phrases did not appear in text subsequent to amendment of subsec. (d) by Pub. L. 103-322, Sec. 160001(b)(2). See below.

Subsec. (d). Pub. L. 103-322, Sec. 160001(e), inserted ", or attempts or conspires to violate," after "violates" in two places.

Pub. L. 103-322, Sec. 160001(c), substituted "conviction under this chapter or chapter 109A" for "conviction under this section".

Pub. L. 103-322, Sec. 160001(b)(2)(C), substituted "fined under this title" for "fined not more than \$250,000" in penultimate sentence.

Pub. L. 103-322, Sec. 160001(b)(2)(B), substituted "fined under this title," for "fined not more than \$200,000, or" before "imprisoned not less than five years".

Pub. L. 103-322, Sec. 160001(b)(2)(A), substituted "fined under this title," for "fined not more than \$100,000, or" before "imprisoned not more than 10 years".
Pub. L. 103-322, Sec. 60011, inserted at end "Whoever, in the course of an offense under this section, engages in conduct that results in the death of a person, shall be punished by death or imprisoned for any term of years or for life."

1990 - Subsec. (a). Pub. L. 101-647 substituted "person to engage in," for "person to engage in,,".

1988 - Subsec. (c)(2)(A), (B). Pub. L. 100-690 inserted "by any means including by computer" after "commerce".

1986 - Subsec. (a). Pub. L. 99-628, Sec. 2(1), (3), inserted ", or who transports any minor in interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in," after "assist any other person to engage in," and substituted "subsection (d)" for "subsection (c)".
Subsec. (b). Pub. L. 99-628, Sec. 2(2), substituted "subsection (d)" for "subsection (c)".

Subsecs. (c), (d). Pub. L. 99-628, Sec. 2(3), (4), added subsec. (c) and redesignated former subsec. (c) as (d).

Pub. L. 99-500 and Pub. L. 99-591 substituted "five years" for "two years" in subsec. (c).

1984 - Subsecs. (a), (b). Pub. L. 98-292, Sec. 3(1), (2), substituted "visual depiction" for "visual or print medium" in three places and substituted "of" for "depicting" before "such conduct".

Subsec. (c). Pub. L. 98-292, Sec. 3(3)-(6), substituted "individual" for "person" in three places, "\$100,000" for "\$10,000", and "\$200,000" for "\$15,000", and inserted "Any organization which violates this section shall be fined not more than \$250,000."

SHORT TITLE OF 1996 AMENDMENT

Section 101(a) (title I, Sec. 121) of div. A of Pub. L. 104-208 provided in part that: "This section (enacting section 2252A of this title, amending this section, sections 2241, 2243, 2252, and 2256 of this title, and section 2000aa of Title 42, The Public Health and Welfare, and enacting provisions set out as notes under this section and section 2241 of this title) may be cited as the 'Child Pornography Prevention Act of 1996'."

SHORT TITLE OF 1990 AMENDMENT

Section 301(a) of title III of Pub. L. 101-647 provided that: "This title (amending sections 1460, 2243, 2252, and 2257 of this title and enacting provisions set out as notes under section 2257 of this title and section 994 of Title 28, Judiciary and Judicial Procedure) may be cited as the 'Child Protection Restoration and Penalties Enhancement Act of 1990'."

SHORT TITLE OF 1988 AMENDMENT

Section 7501 of title VII of Pub. L. 100-690 provided that: "This subtitle (subtitle N (Sec. 7501-7526) of title VII of Pub. L. 100-690, enacting sections 1460, 1466 to 1469, 2251A, and 2257 of this title, amending this section, sections 1465, 1961, 2252 to 2254, 2256, and 2516 of this title, section 1305 of Title 19, Customs Duties, and section 223 of Title 47, Telegraphs, Telephones, and

Radiotelegraphs, and enacting provisions set out as a note under section 2257 of this title) may be cited as the 'Child Protection and Obscenity Enforcement Act of 1988'."

SHORT TITLE OF 1986 AMENDMENTS

Section 1 of Pub. L. 99-628 provided that: "This Act (enacting sections 2421 to 2423 of this title, amending this section and sections 2255 and 2424 of this title, and repealing former sections 2421 to 2423 of this title) may be cited as the 'Child Sexual Abuse and Pornography Act of 1986'."

Section 101(b) (title VII, Sec. 701) of Pub. L. 99-500 and Pub. L. 99-591 provided that: "This title (enacting section 2255 of this title, amending this section and section 2252 of this title, redesignating former section 2255 of this title as 2256, and enacting provisions set out as notes under this section) may be cited as the 'Child Abuse Victims' Rights Act of 1986'."

SHORT TITLE OF 1984 AMENDMENT

Section 1 of Pub. L. 98-292 provided: "That this Act (enacting sections 2253 and 2254 of this title, amending this section and sections 2252, 2255, and 2516 of this title, and enacting provisions set out as notes under this section and section 522 of Title 28, Judiciary and Judicial Procedure) may be cited as the 'Child Protection Act of 1984'."

SHORT TITLE

Section 1 of Pub. L. 95-225 provided: "That this Act (enacting this chapter and amending section 2423 of this title) may be cited as the 'Protection of Children Against Sexual Exploitation Act of 1977'."

SEVERABILITY

Section 101(a) (title I, Sec. 121(8)) of Pub. L. 104-208 provided that: "If any provision of this Act (probably means section 121 of Pub. L. 104-208, div. A, title I, Sec. 101(a), see Short Title of 1996 Amendment note above), including any provision or section of the definition of the term child pornography, an amendment made by this Act, or the application of such provision or amendment to any person or circumstance is held to be unconstitutional, the remainder of this Act, including any other provision or section of the definition of the term child pornography, the amendments made by this Act, and the application of such to any other person or circumstance shall not be affected thereby."

Section 4 of Pub. L. 95-225 provided that: "If any provision of this Act (see Short Title note set out above) or the application thereof to any person or circumstances is held invalid, the remainder of the Act and the application of the provision to other persons not similarly situated or to other circumstances shall not be affected thereby."

CONGRESSIONAL FINDINGS

Section 101(a) (title I, Sec. 121(1)) of Pub. L. 104-208 provided that: "Congress finds that -

"(1) the use of children in the production of sexually explicit material, including photographs, films, videos, computer images, and other visual depictions, is a form of sexual abuse which can result in physical or psychological harm, or both, to the children involved;

"(2) where children are used in its production, child pornography permanently records the victim's abuse, and its continued existence causes the child victims of sexual abuse continuing harm by haunting those children in future years;

"(3) child pornography is often used as part of a method of seducing other children into sexual activity; a child who is reluctant to engage in sexual activity with an adult, or to pose for sexually explicit photographs, can sometimes be convinced by viewing depictions of other children 'having fun' participating in such activity;

"(4) child pornography is often used by pedophiles and child sexual abusers to stimulate and whet their own sexual appetites, and as a model for sexual acting out with children; such use of child pornography can desensitize the viewer to the pathology of sexual abuse or exploitation of children, so that it can become acceptable to and even preferred by the viewer;

"(5) new photographic and computer imaging (sic) technologies make it possible to produce by electronic, mechanical, or other means, visual depictions of what appear to be children engaging in sexually explicit conduct that are virtually indistinguishable to the unsuspecting viewer from unretouched photographic images of actual children engaging in sexually explicit conduct;

"(6) computers and computer imaging technology can be used to -

"(A) alter sexually explicit photographs, films, and videos in such a way as to make it virtually impossible for unsuspecting viewers to identify individuals, or to determine if the offending material was produced using children;

"(B) produce visual depictions of child sexual activity designed to satisfy the preferences of individual child molesters, pedophiles, and pornography collectors; and

"(C) alter innocent pictures of children to create visual depictions of those children engaging in sexual conduct;

"(7) the creation or distribution of child pornography which includes an image of a recognizable minor invades the child's privacy and reputational interests, since images that are created showing a child's face or other identifiable feature on a body engaging in sexually explicit conduct can haunt the minor for years to come;

"(8) the effect of visual depictions of child sexual activity on a child molester or pedophile using that material to stimulate or whet his own sexual appetites, or on a child where the material is being used as a means of seducing or breaking down the child's inhibitions to sexual abuse or exploitation, is the same whether the child pornography consists of photographic depictions of actual children or visual depictions produced wholly or in part by electronic, mechanical, or other means, including by computer, which are virtually indistinguishable to the unsuspecting viewer from photographic images of actual children;

"(9) the danger to children who are seduced and molested with the aid of child sex pictures is just as great when the child pornographer or child molester uses visual depictions of child sexual activity produced wholly or in part by electronic,

mechanical, or other means, including by computer, as when the material consists of unretouched photographic images of actual children engaging in sexually explicit conduct;

"(10)(A) the existence of and traffic in child pornographic images creates the potential for many types of harm in the community and presents a clear and present danger to all children; and

"(B) it inflames the desires of child molesters, pedophiles, and child pornographers who prey on children, thereby increasing the creation and distribution of child pornography and the sexual abuse and exploitation of actual children who are victimized as a result of the existence and use of these materials;

"(11)(A) the sexualization and eroticization of minors through any form of child pornographic images has a deleterious effect on all children by encouraging a societal perception of children as sexual objects and leading to further sexual abuse and exploitation of them; and

"(B) this sexualization of minors creates an unwholesome environment which affects the psychological, mental and emotional development of children and undermines the efforts of parents and families to encourage the sound mental, moral and emotional development of children;

"(12) prohibiting the possession and viewing of child pornography will encourage the possessors of such material to rid themselves of or destroy the material, thereby helping to protect the victims of child pornography and to eliminate the market for the sexual exploitative use of children; and

"(13) the elimination of child pornography and the protection of children from sexual exploitation provide a compelling governmental interest for prohibiting the production, distribution, possession, sale, or viewing of visual depictions of children engaging in sexually explicit conduct, including both photographic images of actual children engaging in such conduct and depictions produced by computer or other means which are virtually indistinguishable to the unsuspecting viewer from photographic images of actual children engaging in such conduct."

Section 101(b) (title VII, Sec. 702) of Pub. L. 99-500 and Pub. L. 99-591 provided that: "The Congress finds that -

"(1) child exploitation has become a multi-million dollar industry, infiltrated and operated by elements of organized crime, and by a nationwide network of individuals openly advertising their desire to exploit children;

"(2) Congress has recognized the physiological, psychological, and emotional harm caused by the production, distribution, and display of child pornography by strengthening laws prescribing such activity;

"(3) the Federal Government lacks sufficient enforcement tools to combat concerted efforts to exploit children prescribed by Federal law, and exploitation victims lack effective remedies under Federal law; and

"(4) current rules of evidence, criminal procedure, and civil procedure and other courtroom and investigative procedures inhibit the participation of child victims as

witnesses and damage their credibility when they do testify, impairing the prosecution of child exploitation offenses."

Section 2 of Pub. L. 98-292 provided that: "The Congress finds that -

"(1) child pornography has developed into a highly organized, multi-million-dollar industry which operates on a nationwide scale;

"(2) thousands of children including large numbers of runaway and homeless youth are exploited in the production and distribution of pornographic materials; and

"(3) the use of children as subjects of pornographic materials is harmful to the physiological, emotional, and mental health of the individual child and to society."

REPORT BY ATTORNEY GENERAL

Section 101(b) (title VII, Sec. 705) of Pub. L. 99-500 and Pub. L. 99-591 required Attorney General, within one year after Oct. 18, 1986, to submit a report to Congress detailing possible changes in Federal Rules of Evidence, Federal Rules of Criminal Procedure, Federal Rules of Civil Procedure, and other Federal courtroom, prosecutorial, and investigative procedures which would facilitate the participation of child witnesses in cases involving child abuse and sexual exploitation.

ANNUAL REPORT TO CONGRESS

Attorney General to report annually to Congress on prosecutions, convictions, and forfeitures under this chapter, see section 9 of Pub. L. 98-292, set out as a note under section 522 of Title 28, Judiciary and Judicial Procedure.

SECREf

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 1961, 2253, 2254, 2255, 2516, 3486A, 3559 of this title; title 8 section 1101; title 42 sections 2000aa, 13032.

Appendix 4 Text File Listing From part 2

Listing of text files from forensic investigation.

```
/mnt/windows_forensic_server/comcheck/Streams/BuildGuess.TXT
/mnt/windows_forensic_server/comcheck/Streams/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/OutputData/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/NT4.0 -
2.50.3719.14/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/InputData/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7
SP1(WinXP)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7 SP1
(2.71.9030.9)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7 RTM
Refresh (2.70.9001.0)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7 RTM
(2.70.7713.4)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP2
Refresh (2.62.7400.1)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP2
(2.62.7926.1)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP1
(2.61.7326.6)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 RTM
(2.60.6526.3)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.518D/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.518/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP3
(2.53.6200.2)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP2
(2.52.6019.2)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP1
(2.51.5303.5)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 RTM
(2.50.4403.12)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5
(4403.3)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.1 SP2
(2.1.2.4202.3) GA/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.1
SP1/CompFile.TXT
```

/mnt/windows_forensic_server/comcheck/Streams/2.1
RTM/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.1
GA/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP2/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0 SP1
(OLAP)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP1/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0/CompFile.
TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5d (IE4.0
SP1)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5C/CompFile
.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5b/CompFile
.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5a/CompFile
.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5
PDC97/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5
(IE4.0)/CompFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/GetData.TXT
/mnt/windows_forensic_server/unzipped/csyservice/GPL.TXT
/mnt/windows_forensic_server/comcheck/Streams/InputData/Jus
tFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP2
Refresh (2.62.7400.1)/JustFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.518D/JustFi
le.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.518/JustFil
e.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP1
(2.51.5303.5)/JustFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP2/JustFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP1/JustFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0/JustFile.
TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5C/JustFile
.TXT
/mnt/windows_forensic_server/Program
Files/EuroTool/LEESMIJ.TXT

/mnt/windows_forensic_server/Program
Files/EuroTool/LEGGIMI.TXT
/mnt/windows_forensic_server/Program
Files/EuroTool/LEIAME.TXT
/mnt/windows_forensic_server/Program
Files/WinZip/LICENSE.TXT
/mnt/windows_forensic_server/comcheck/Streams/ODBCFile.TXT
/mnt/windows_forensic_server/comcheck/Streams/OLEDBFile.TXT
/mnt/windows_forensic_server/Program Files/WinZip/ORDER.TXT
/mnt/windows_forensic_server/comcheck/ReadMe.TXT
/mnt/windows_forensic_server/Program
Files/WinZip/README.TXT
/mnt/windows_forensic_server/Program Files/Adobe/Acrobat
5.0/Reader/Optional/README.TXT
/mnt/windows_forensic_server/Documents and
Settings/connx/Local
Settings/Temp/pft22D~tmp/Reader/Optional/README.TXT
/mnt/windows_forensic_server/comcheck/Streams/NT4.0 -
2.50.3719.14/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/InputData/REG
ISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7
SP1 (WinXP)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7 SP1
(2.71.9030.9)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7 RTM
Refresh (2.70.9001.0)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7 RTM
(2.70.7713.4)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP2
Refresh (2.62.7400.1)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP2
(2.62.7926.1)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP1
(2.61.7326.6)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 RTM
(2.60.6526.3)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.518D/REGIST
RYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.518/REGISTR
YKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP3
(2.53.6200.2)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP2
(2.52.6019.2)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP1
(2.51.5303.5)/REGISTRYKEYVALUE.TXT

/mnt/windows_forensic_server/comcheck/Streams/2.5 RTM
(2.50.4403.12)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5
(4403.3)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.1 SP2
(2.1.2.4202.3) GA/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.1
SP1/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.1
RTM/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.1
GA/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP2/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0 SP1
(OLAP)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP1/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0/REGISTRYK
EYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5d (IE4.0
SP1)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5C/REGISTRY
KEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5b/REGISTRY
KEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5a/REGISTRY
KEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5
PDC97/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5
(IE4.0)/REGISTRYKEYVALUE.TXT
/mnt/windows_forensic_server/comcheck/Streams/InputData/Reg
KeysNewFileName.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP2
Refresh (2.62.7400.1)/RegKeysNewFileName.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.518D/RegKey
sNewFileName.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.518/RegKeys
NewFileName.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP1
(2.51.5303.5)/RegKeysNewFileName.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP2/RegKeysNewFileName.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP1/RegKeysNewFileName.TXT

/mnt/windows_forensic_server/comcheck/Streams/2.0/RegKeysNewFileName.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5C/RegKeysNewFileName.TXT
/mnt/windows_forensic_server/comcheck/Streams/NT4.0 -
2.50.3719.14/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7
SP1 (WinXP) /RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7 SP1
(2.71.9030.9)/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7 RTM
Refresh (2.70.9001.0)/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.7 RTM
(2.70.7713.4)/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP2
(2.62.7926.1)/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP1
(2.61.7326.6)/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 RTM
(2.60.6526.3)/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP3
(2.53.6200.2)/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP2
(2.52.6019.2)/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 RTM
(2.50.4403.12)/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5
(4403.3)/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.1 SP2
(2.1.2.4202.3) GA/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.1
SP1/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.1
RTM/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.1
GA/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0 SP1
(OLAP) /RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5d (IE4.0
SP1) /RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5b/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5a/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5
PDC97/RegKeysNew.TXT

```

/mnt/windows_forensic_server/comcheck/Streams/1.5
(IE4.0)/RegKeysNew.TXT
/mnt/windows_forensic_server/comcheck/Streams/InputData/REG
KEYSNEW.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP2
Refresh (2.62.7400.1)/REGKEYSNEW.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.518D/REGKEY
SNEW.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.518/REGKEYS
NEW.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP1
(2.51.5303.5)/REGKEYSNEW.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP2/REGKEYSNEW.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP1/REGKEYSNEW.TXT
/mnt/windows_forensic_server/comcheck/Streams/2.0/REGKEYSNE
W.TXT
/mnt/windows_forensic_server/comcheck/Streams/1.5C/REGKEYSN
EW.TXT
/mnt/windows_forensic_server/ODSBACKUPS/Projects1/Pilot/STU
_FED_DATA_ERRORS_NEW.TXT
/mnt/windows_forensic_server/Ascential/DataStage/Projects/P
ilot/STU_FED_DATA_ERRORS_NEW.TXT
/mnt/windows_forensic_server/Ascential/DataStage/Projects/O
DS/STU_FED_DATA_ERRORS_NEW.TXT
/mnt/windows_forensic_server/comcheck/Streams/TakeSnapshot.
TXT
/mnt/windows_forensic_server/Program
Files/WinZip/VENDOR.TXT
/mnt/windows_forensic_server/comcheck/Streams/VerAnalysis.T
XT

/mnt/windows_forensic_server/WINNT/Active Setup Log.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Cookies/administrator@connx.webex[2]
.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Cookies/administrator@counter2.hitsl
ink[2].txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Cookies/administrator@google[1].txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Cookies/administrator@msn[2].txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Cookies/administrator@sc30[1].txt

```

```

/mnt/windows_forensic_server/Documents and
Settings/Administrator/Cookies/administrator@scsession[1].t
xt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Cookies/administrator@search.msn[2].
txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Cookies/administrator@yahoo[1].txt
/mnt/windows_forensic_server/Program
Files/Tripwire/TFS/Bin/agentcfg.txt
/mnt/windows_forensic_server/comcheck/Streams/NT4.0 -
2.50.3719.14/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/InputData/All
Files.txt
/mnt/windows_forensic_server/comcheck/Streams/2.7
SP1(WinXP)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.7 SP1
(2.71.9030.9)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.7 RTM
Refresh (2.70.9001.0)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.7 RTM
(2.70.7713.4)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP2
Refresh (2.62.7400.1)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP2
(2.62.7926.1)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP1
(2.61.7326.6)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.6 RTM
(2.60.6526.3)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.518D/AllFil
es.txt
/mnt/windows_forensic_server/comcheck/Streams/2.518/AllFile
s.txt
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP3
(2.53.6200.2)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP2
(2.52.6019.2)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP1
(2.51.5303.5)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.5 RTM
(2.50.4403.12)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.5
(4403.3)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.1 SP2
(2.1.2.4202.3) GA/AllFiles.txt

```

/mnt/windows_forensic_server/comcheck/Streams/2.1
SP1/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.1
RTM/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.1
GA/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP2/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.0 SP1
(OLAP)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP1/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/2.0/AllFiles.
txt
/mnt/windows_forensic_server/comcheck/Streams/1.5d (IE4.0
SP1)/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/1.5C/AllFiles
.txt
/mnt/windows_forensic_server/comcheck/Streams/1.5b/AllFiles
.txt
/mnt/windows_forensic_server/comcheck/Streams/1.5a/AllFiles
.txt
/mnt/windows_forensic_server/comcheck/Streams/1.5
PDC97/AllFiles.txt
/mnt/windows_forensic_server/comcheck/Streams/1.5
(IE4.0)/AllFiles.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My
Documents/pilotjobs/ArathiPivotTest1.csv.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install1/ClickPack/Artistic.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install/ClickPack/Artistic.txt
/mnt/windows_forensic_server/WINNT/Microsoft.NET/Framework/
v1.0.3705/assemblylistLoc.txt
/mnt/windows_forensic_server/Program
Files/Ascential/MetaStage/Documents/Templates/BasicModelTem
plate.txt
/mnt/windows_forensic_server/Program
Files/Ascential/MetaStage/Documents/Templates/BasicObjectTe
mplate.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install1/Samples/BCP Demo/bcpdemo.txt

/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install/Samples/BCP Demo/bcpdemo.txt
/mnt/windows_forensic_server/Documents and
Settings/Operations/Application Data/Microsoft/Internet
Explorer/brndlog.txt
/mnt/windows_forensic_server/Documents and Settings/Default
User/Application Data/Microsoft/Internet
Explorer/brndlog.txt
/mnt/windows_forensic_server/Documents and
Settings/connx/Application Data/Microsoft/Internet
Explorer/brndlog.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Application Data/Microsoft/Internet
Explorer/brndlog.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/CLUF.txt
/mnt/windows_forensic_server/CONN32/InfoNaut/connections.t
xt
/mnt/windows_forensic_server/Documents and
Settings/connx/Cookies/connx@connx.webex[2].txt
/mnt/windows_forensic_server/Documents and
Settings/connx/Cookies/connx@doubleclick[1].txt
/mnt/windows_forensic_server/Documents and
Settings/connx/Cookies/connx@microsoft[2].txt
/mnt/windows_forensic_server/Documents and
Settings/connx/Cookies/connx@msn[1].txt
/mnt/windows_forensic_server/Documents and
Settings/connx/Cookies/connx@sc30[1].txt
/mnt/windows_forensic_server/Documents and
Settings/connx/Cookies/connx@scsession[1].txt
/mnt/windows_forensic_server/Documents and
Settings/connx/Cookies/connx@search.msn[2].txt
/mnt/windows_forensic_server/RECYCLER/S-1-5-21-682003330-
1202660629-1708537768-500/Dc2.txt
/mnt/windows_forensic_server/ODSBACKUPS/Projects1/VERSION/d
ssendmail_template.txt
/mnt/windows_forensic_server/ODSBACKUPS/Projects1/PROD/dsse
ndmail_template.txt
/mnt/windows_forensic_server/ODSBACKUPS/Projects1/Pilot/dss
endmail_template.txt
/mnt/windows_forensic_server/Ascential/DataStage/Template/d
ssendmail_template.txt
/mnt/windows_forensic_server/Ascential/DataStage/Projects/V
ERSION/dssendmail_template.txt
/mnt/windows_forensic_server/Ascential/DataStage/Projects/P
ROD/dssendmail_template.txt

/mnt/windows_forensic_server/Ascential/DataStage/Projects/P
ilot/dssendmail_template.txt
/mnt/windows_forensic_server/Ascential/DataStage/Projects/O
DS/dssendmail_template.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install1/XMLPack/ENUReadMe.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install/XMLPack/ENUReadMe.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/eula_de.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/eula_du.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/eula_EL.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/eula_fi.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/eula_fr.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/eula_it.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/eula_pt.txt
/mnt/windows_forensic_server/WINNT/system32/eula.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/eula.txt
/mnt/windows_forensic_server/Ascential/DataStage/Projects/O
DS/XMLORDERDIR/Ex1-INPUT.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My
Documents/PRODRUNERRS/FAM_STU_BUDGET_ERRS.txt
/mnt/windows_forensic_server/ODS/XMLFILES/FSAXMLFMT1.xsd.tx
t
/mnt/windows_forensic_server/WINNT/system32/drivers/gmreadm
e.txt
/mnt/windows_forensic_server/WINNT/system32/iisperf.txt
/mnt/windows_forensic_server/comcheck/Streams/InputData/Inp
RegFile.txt
/mnt/windows_forensic_server/comcheck/Streams/2.6 SP2
Refresh (2.62.7400.1)/InpRegFile.txt
/mnt/windows_forensic_server/comcheck/Streams/2.518D/InpReg
File.txt
/mnt/windows_forensic_server/comcheck/Streams/2.518/InpRegF
ile.txt
/mnt/windows_forensic_server/comcheck/Streams/2.5 SP1
(2.51.5303.5)/InpRegFile.txt

/mnt/windows_forensic_server/comcheck/Streams/2.0
SP2/InpRegFile.txt
/mnt/windows_forensic_server/comcheck/Streams/2.0
SP1/InpRegFile.txt
/mnt/windows_forensic_server/comcheck/Streams/2.0/InpRegFi
le.txt
/mnt/windows_forensic_server/comcheck/Streams/1.5C/InpRegFi
le.txt
/mnt/windows_forensic_server/Program
Files/WindowsUpdate/V4/iuident.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/Leame.txt
/mnt/windows_forensic_server/unzipped/csyzservice/lesser.tx
t
/mnt/windows_forensic_server/unzipped/XMLPack-
2.0.1/license.txt
/mnt/windows_forensic_server/Program
Files/Tripwire/TFS/License.txt
/mnt/windows_forensic_server/Program Files/timbuktu
pro/License.txt
/mnt/windows_forensic_server/Program Files/Adobe/Acrobat
5.0/Reader/Legal/License.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/lisezmoi.txt
/mnt/windows_forensic_server/Program
Files/Ascential/MetaStage/Listener/listener.cfg.092303.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/LUEMINUT.txt
/mnt/windows_forensic_server/WINNT/ModemDet.txt
/mnt/windows_forensic_server/WINNT/ServicePackFiles/i386/ms
oe.txt
/mnt/windows_forensic_server/Program Files/Outlook
Express/msoe.txt
/mnt/windows_forensic_server/WINNT/OEWABLog.txt
/mnt/windows_forensic_server/Documents and Settings/All
Users/Application Data/Network
Associates/VirusScan/OnAccessScanLog.txt
/mnt/windows_forensic_server/Documents and Settings/All
Users/Application Data/Network
Associates/VirusScan/OnDemandScanLog.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My
Documents/DSERRORS/packaging_cursorreposerr.txt
/mnt/windows_forensic_server/Program
Files/Ascential/DataStage/perrorENU.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My Documents/pinglog.txt

/mnt/windows_forensic_server/Documents and
Settings/Administrator/My
Documents/pilotjobs/Pivot_Input_File_1New.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My
Documents/pilotjobs/Pivot_Input_File_1.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My
Documents/pilotjobs/Pivot_Input_File_2.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My
Documents/pilotjobs/Pivot_Output_1latest.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My
Documents/pilotjobs/Pivot_Output_1New.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My
Documents/pilotjobs/Pivot_Output_File_1.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local Settings/Temporary Internet
Files/Content.IE5/KGKAF6RN/plain[1].txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local Settings/Temporary Internet
Files/Content.IE5/FR7382PE/plain[1].txt
/mnt/windows_forensic_server/CONN32/InfoNaut/queries.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/readm_DE.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local Settings/Temp/install1/IBM DWC
Interface/readmeENU.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local Settings/Temp/install/IBM DWC
Interface/readmeENU.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/readm_el.txt
/mnt/windows_forensic_server/Program Files/Network
Associates/VirusScan/readme.txt
/mnt/windows_forensic_server/Program Files/Internet
Explorer/readme.txt
/mnt/windows_forensic_server/Program
Files/EuroTool/readme.txt
/mnt/windows_forensic_server/Program
Files/Ascential/MetaStage/readme.txt
/mnt/windows_forensic_server/Program
Files/Ascential/DataStage/readme.txt

/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local Settings/Temp/install1/Version
Control/readme.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install1/Readme/ENU/readme.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local Settings/Temp/install1/GCI
64bit/readme.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install1/ClickPack/readme.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local Settings/Temp/install/Version
Control/readme.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install/Readme/ENU/readme.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local Settings/Temp/install/GCI
64bit/readme.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install/ClickPack/readme.txt
/mnt/windows_forensic_server/Ascential/DataStage/readme.txt
/mnt/windows_forensic_server/Ascential/DataStage/Dsdk/Plugi
n Samples/Jobs/readme.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install1/Mainframe Components/Readme.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/Local
Settings/Temp/install/Mainframe Components/Readme.txt
/mnt/windows_forensic_server/unzipped/csysservice/ReadMe.tx
t
/mnt/windows_forensic_server/Program
Files/Ascential/MetaStage/unsupported/Samples/NT/readresour
ce.txt
/mnt/windows_forensic_server/Program
Files/Ascential/MetaStage/RunImport/runimport.cfg_092303.tx
t
/mnt/windows_forensic_server/WINNT/Microsoft.NET/Framework/
v1.1.4322/1033/SetupENU1.txt
/mnt/windows_forensic_server/WINNT/Microsoft.NET/Framework/
v1.1.4322/1033/SetupENU2.txt
/mnt/windows_forensic_server/WINNT/setuplog.txt

/mnt/windows_forensic_server/Ascential/DataStage/Setuplog.txt
/mnt/windows_forensic_server/Program Files/Common
Files/Network Associates/Engine/signlic.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My
Documents/pilotjobs/splitnames1.txt
/mnt/windows_forensic_server/WINNT/\$NtUninstallKB828749\$/sp
uninst/spuninst.txt
/mnt/windows_forensic_server/WINNT/\$NtUninstallKB828035\$/sp
uninst/spuninst.txt
/mnt/windows_forensic_server/WINNT/\$NtUninstallKB828028\$/sp
uninst/spuninst.txt
/mnt/windows_forensic_server/WINNT/\$NtUninstallKB826232\$/sp
uninst/spuninst.txt
/mnt/windows_forensic_server/WINNT/\$NtUninstallQ828026\$/spu
ninst/spuninst.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My
Documents/DSERRORS/STUBIODEMOINFOERRORS.txt
/mnt/windows_forensic_server/Program Files/Internet
Explorer/support.txt
/mnt/windows_forensic_server/WINNT/system32/Adobe/SVG
Viewer/SVG Viewer License.txt
/mnt/windows_forensic_server/Documents and
Settings/connx/Local Settings/Temp/pft22D~tmp/SVG Files/SVG
Viewer License.txt
/mnt/windows_forensic_server/Documents and
Settings/Administrator/My Documents/swfileSQL.txt
/mnt/windows_forensic_server/Program
Files/Ascential/MetaStage/unsupported/Samples/NT/swresource
.txt
/mnt/windows_forensic_server/WINNT/Windows Update Setup
Files/This folder is safe to delete.txt
/mnt/windows_forensic_server/Program
Files/Tripwire/TFS/Bin/twcfg.txt
/mnt/windows_forensic_server/Program
Files/Tripwire/TFS/Policy/twpol.txt
/mnt/windows_forensic_server/Documents and
Settings/connx/Local Settings/Temp/{7DE65376-28D7-4CDD-
82E2-C38D53BE6132}/UnformattedLicense.txt
/mnt/windows_forensic_server/Documents and Settings/All
Users/Application Data/Network
Associates/VirusScan/UpdateLog.txt
/mnt/windows_forensic_server/Program
Files/Ascential/MetaStage/unsupported/Samples/NT/writeresou
rce.txt

© SANS Institute 2004, Author retains full rights.