Autopsy

St. Louis Security Group
1/26/2004
University of Missouri at St. Louis
West County Computer Center
Clarence Johnson
Clarence@johnsonct.net

Autopsy is a front end to sluethkit 1.66 which has a series of software programs used to analyze computer hard drives.

The following is an example used as an introduction to computer forensics.

Software used: Knoppix STD
Computer system: Gateway PII using windows 2000 Server
Network connections: 12 computer connected together through a hub.
IP Address configurations: 192.168.1.X
Other: There is no access to the internet.

1) Load Knoppix STD
2) Verify IP address
3) If no IP Address then set one
4) Determine hard disk slices/partitions
5) Determine pertinent information
6) Start Autopsy
7) Copy the URL link from the autopsy server
8) Start mozilla browser
9) Create a new case
10) Enter case information
11) Enter case directory information
12) Enter case category information
13) Add the host
14) Enter host information
15) Add image
16) Enter image information
17) Perform file analysis
18) Investigate Data

1-3

Place Knoppix STD CDROM into bootable PC
Start a root terminal by right clicking on the desktop and choosing shells then root shell
Within the root terminal type the following

```
        /sbin/ifconfig eth0
```

If you have an IP Address go to next steps else set your IP Address.

```
        /sbin/ifconfig eth0 192.168.1.1 netmask 255.255.255.0
```

Verify IP Address

```
        /sbin/ifconfig eth0
```

An IP address is not needed for autopsy to run but could be helpful in sending data to a different computer through FTP.

4-6
Determine hard disk partitions or slices
Right click on the desktop and select x shells and then root aterm, then type in the following.

```
        fdisk –l /dev/hda
```

You should see at least one partition please note if it is NTFS or LINUX and write down the Partition to diagnose.

Partitions of interest ____________________ and __________________

Company name of computer _________________________

Reason for forensic study _________________________

Your Name _______________________________________

This computers name ______________________________

Time Zone ___________CST ________________

Hard drive partition _________/dev/hda1_____________

Start autopsy
Right click on the desk top, select forensics, select autopsy service. Do not close the window.

7-9
After you started the Autopsy server there will be an URL listed. Copy this URL it will be pasted into the mozilla browser later.

To copy the URL left click at the beginning of the URL line then highlight the entire line.

Start mozilla→ Right click on the desktop, select Internet, select mozilla firebird.

Remove the original data from the URL line.

Click both buttons on the mouse at the same time while you are in the URL line and the previously copied data will be pasted into the URL. Press enter.

At the bottom of the web page click on New case.

10-12
Case information
1 Enter case name. I have been using the company name like Safeway.
2 Description: Quickbook data is an example
3 Your name: Clarence (remember no spaces)

Click on new case

Case directory information
After you click on new case you should see the directory information

Click on OK

You should now be in the case category section. Your case should appear.
Click on OK

13-14
Add the host
Click on add a host

Host name: I normally use the computer name such as cmptr1
Description: quickbooks
Time Zone: CST
Leave the rest as is.

Click on Add Host
Click OK
Your host should be listed (cmptr1) and the investigator should be listed.
Click OK

15-16

Add IMAGE for forensics

Click on ADD IMAGE

Location : /dev/hda1 (or whatever hard drive you are concerned with)

Import Method: Chose symlink

File system Type: Chose NTFS (for our example)

Original Mount point: c:\

Integrity check: choose ignore (otherwise the process will take all day)

Click on ADD IMAGE.

Click on OK

17-18
Now Case Gallery, Host Gallery and Host Manage should all be bold.
Your image should be listed.
Click on OK

Click on File Analysis

Investigate your files and directories

If you select a file there are multiple ways of looking at it.
Ascii (Display or Report) Strings (Display or Report) Export or Add notes

Also note you may select all deleted files on the left.

You may also select file type to get a numeric count for all of the different files.

The rest is left for you to investigate.

Other computer forensic tools.

- **autopsy 1.75** : Web front-end to TASK. Evidence Locker defaults to /mnt/evidence
- **biew** : binary viewer
- **bsed** : binary stream editor
- **consh** : logged shell (from F.I.R.E.)
- **coreography** : analyze core files
- **dcfldd** : US DoD Computer Forensics Lab version of dd
- **fenris :** code debugging, tracing, decompiling, reverse engineering tool
- **fatback** : Undelete FAT files
- **foremost** : recover specific file types from disk images (like all JPG files)
- **ftimes** : system baseline tool (be proactive)
- **galleta** : recover Internet Explorer cookies
- **hashdig** : dig through hash databases
- **hdb** : java decompiler
- **mac-robber** : TCT's graverobber written in C
- **md5deep** : run md5 against multiple files/directories
- **memfetch** : force a memory dump
- **pasco** : browse IE index.dat
- **photorec** : grab files from digital cameras
- **readdbx** : convert Outlook Express .dbx files to mbox format
- **readoe** : convert entire Outlook Express .directory to mbox format
- **rifiuti** : browse Windows Recycle Bin INFO2 files
- **secure_delete** : securely delete files, swap, memory....
- **testdisk** : test and recover lost partitions
- **wipe** : wipe a partition securely. good for prep'ing a partition for dd

  and other typical system tools used for forensics (dd, lsof, strings, grep, etc.)