

Free Forensics With Linux

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: forensic_with_linux.pdf*
- ❖ *GNU Free Documentation License*
- ❖ *Version 1.00, 2005-05-27*
- ❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*
- ❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Limitation

- Linux cannot see the last sector on hard drives with an odd number of sectors
- If you come across an odd-sized drive, use a BSD variant to image

❖ General information about the case

- -Your name and organization
- -Case number or other identifier for this job
- -Date
- -General information about the case
- Information about medias
 - -Your name and organization
 - -Case number or other identifier for this job
 - -Evidence number assigned to this HD
 - -Date and time image will be made
 - -Make, model, and serial number of computer
 - -IP and hostname of computer
 - -Make, model, and serial number of HD
 - -Where HD came from and why you are looking at it

❖ The F.I.R.E. Boot CD

- Prepare the drives
 - **note size and total number of sectors of the suspect drive**
 - **Wipe and format a very large drive (Inspector drive)**
 - `dcflddd if=/dev/zero of=/dev/hda bs=8k conv=noerror,sync`
 - Create a partition with `fdisk /dev/hda`
 - Reboot
 - Format with `mkfs -t ext3 /dev/hda1`
 - **Mount evidence drive read-write (mount /dev/hda1 /mnt/hda1)**
 - **Create directory on the evidence drive for this case `mkdir /mnt/hda1/case_no`**
 - **Create a subdirectory under that for this piece of evidence `mkdir /mnt/hda1/case_no/evidence_no`**
- Connect evidence
 - **Connect Evidence Drive and Image Drive to imaging System**
 - **Ensure that Master/Slave/Cable Select jumper(s) are correct**
 - **Ensure BIOS is set to boot from CD only**
- Starting Imaging Process
 - **Change to another VT (Ctrl-Alt-F2)**
 - **Change to emacs style by typing `set -o emacs`**

- Log in as root - the root password is “firefire”
- Figure out which hard drive is which `dmesg | grep hd`
- Mount the image hard drive read-write mount `/dev/hdc1 /mnt/hdc1`
- Change to your directory for this piece of evidence `cd /mnt/hdc1/case_no/evidence_no`
- `dmesg | tee case_no_dmesg.txt`
- `hdparm -gil /dev/hda | tee case_no_hdparm.txt`
- List partitions with `sfdisk sfdisk -luS /dev/hda | tee sfdisk.txt`
- Hashing
 - hash text files - `md5sum *.txt | tee case_no_txt_hashes.txt`
 - hash drive - `md5sum /dev/hda | tee serial_no.original.md5.txt`
- Imaging
 - `dcfldd if=/dev/hda of=/mnt/hdc1/case_no/evidence_no/serial_no.dd conv=noerror,sync hashwindow=0 hashlog=serial_no.md5.txt`
 - shutdown with `shutdown -h now`
 - Disconnect and store evidence

❖ Preparing the analysis system

- **Install Red hat on Forensic Analysis box**
 - Install NASA Enhanced Loopback Drivers
 - ftp://ftp.hq.nasa.gov/pub/ig/ccd/enhanced_loopback/
 - Run `./createdev start`
 - Install loop-utils `rpm rpm --force -ivh loop-utils-0.0.1-1.i386.rpm`
 - Untar kernel to /
 - `cd /; tar xvfz vmlinuz-2.4.xx-xfsenhanced_loop.x.tar.gz`
 - Edit grub.conf
 - ♦ `gedit /boot/grub/grub.conf`
 - title Red Hat Linux (2.4.18-14)
 - root (hd0,4)
 - kernel /boot/vmlinuz-2.4.18-14 ro root=LABEL=
 - initrd /boot/initrd-2.4.18-14.img
 - title Red Hat Linux with NASA Loopback (2.4.21-pre4-xfs-enhanced_loop)
 - root (hd0,4)
 - kernel /boot/vmlinuz-2.4.21-pre4-xfs-enhanced_loop ro root=LABEL=
 - initrd /boot/initrd-2.4.21-pre4-xfs-enhanced_loop.img
-
- **Install NSRL**
 - Download from ftp://ftp.nist.gov/pub/itl/div897/nsrl/ver_2_0/nsrl_2_0.iso
 - Unzip NSRL before you install Autopsy
- **Install Sleuthkit**
 - Download sleuthkit www.sleuthkit.org and autopsy source files to `/usr/local/src`.
 - Decompress: `tar zxvf sleuthkit-1.62.tar.gz`
 - Change Dir: `cd sleuthkit-1.62`
 - Compile: `make`
- **Install Autopsy**
 - Decompress: `tar zxvf autopsy-1.73.tar.gz`
 - Change Dir: `cd autopsy-1.73`
 - Install: `make`
 - Give location of sleuthkit and NSRL

- Give location of “evidence locker” where all case data is kept
- **Install Foremost**
 - Download from foremost.sourceforge.net
 - Decompress: `tar xzvf foremost-0.64.tar.gz`
 - Change Dir: `cd foremost-0.64`
 - Compile: `make`
 - Install: `make install`
- ❖ **Conducting analysis**
 - Make image file read-only `chmod a-w serial_no.dd`
 - Hash complete image and compare to hash of drive and hash result from `dcfldd md5sum serial_no.dd`
 - To backup to CDs - Compress and Split `gzip -c serial_no.dd | split -b 699m - serial_no.dd.gz`
 - Hash all chunks : `md5sum serial_no.dd* >> serial_no_chunks.md5.txt`
 - Burn image chunks, text files, and hashes
 - Reconstruct with `cat serial_no.dd.gz* | gunzip - > serial_no_out.dd`
 - As root, mount loopback device with `losetup /dev/loopa serial_no.dd`
 - List the partition table from the image `sfdisk -luS /dev/loopa`
 - Leave the loopback device mounted to run Autopsy
 - When done unmount with `losetup -d /dev/loopa`
 - **mounting image loopback**
 - `losetup /dev/loopa wd40gb.dd`
 - `sfdisk -luS /dev/loopa`
 - **Mount Filesystems if desired**
 - For example mount `-o ro /dev/loopa2 /mnt/evidence_a2`
 - When you are done with the files, you unmount with `umount /mnt/evidence_a2`
 - `mkdir /mnt/image2`
 - `mount -o ro /dev/loopa2 /mnt/image2`
 - `ls -la /mnt/image2`
 - `umount /mnt/image2`
 - **Searching**
 - **ACSII** - `strings -t d case_no.dd > case_no.strings`
 - **UNICODE** - `strings -t d -e l case_no.dd > case_no.strings-el`
 - **Run Foremost**
 - Copy `foremost.conf` from install directory to current directory
 - Edit `foremost.conf` to search for file types you want
 - Run Foremost `foremost -o serial_no_fm -v serial_no.dd`
 - This will create the `serial_no_fm` directory if it does not exist If `serial_no_fm` directory exists, it **MUST** be empty
 - Can run on disk image or on loopback devices `foremost -o loopa3_fm -v /dev/loopa3`