Digital Forensics using Linux and Open Source Tools

Sept 26, 2005

Bruce Nikkel

Overview/Goals of Seminar

Provide a high level overview of forensic and investigative tools available for Linux

Present advantages and disadvantages

- Show advantages for teaching, learning and research
- Show advantages for Corporate and Law Enforcement forensic labs
- Outline the disadvantages of Linux & OSS

Target audience both forensics techies and forensics managers

Unix, Linux and Open Source Software

OSS Licensing and Freedoms

- designed to protect the user, not the vendor
- freedom to modify, use, distribute
- freedom to learn, understand, and improve
- [GPL, LGPL, BSD License, GNU, FSF]

Unix Philosophy

- book: "The UNIX Philosophy"
- many small tools which do one job very well
- piping, redirecting
- scripting, automating
- [shell, tee, >> | << & > <]

The Linux Environment

What exactly is Linux?

- "Linux" is just an OS kernel
- the rest is additional Open Source Software
- together they are a "Linux Distribution"
- [Knoppix, Ubuntu, Redhat, Novell/SuSe]

Large choice of GUI and/or commandline environments

- most popular are KDE and Gnome
- Unix-like, Mac-like, MSWindows-like, NeXT-like
- advanced shell environments
- web front-ends, GUI front-ends
- [KDE, Gnome, Windowmaker, bash, zsh, emacs, mc]

The Linux Environment (cont.)

Forensic boot CDs

- fully installed Linux environment on bootable CD or DVD
- non-mount booting
- large pre-installed forensic toolset
- Knoppix based

Most up to date (at the moment)

- FCCU GNU/Linux Forensic Boot CD (Belgian Federal Computer Crime Unit)
- Helix (US e-fense Inc.)

Full installation:

- learning Linux -> Ubuntu, doing forensics -> Debian
- must strip down automount services

Imaging and Evidence Acquisition

Wide range of supported technologies and media

- ATA, SATA, SCSI, USB, Firewire
- cd, dvd, USB sticks, tapes, floppies, etc

Forensically sound acquisition

- typically any sector-based storage medium accessible as a device can be safely imaged
- can acquire an image without mounting drive
- hardware write-blocker not needed for unmounted devices
- support for handling errors, bad blocks
- [dd, dcfldd, dd_rescue, sdd, AIR, sleuthkit, adepto, grab]

Imaging and Evidence Acquisition (cont.)

Image handling (with piping, redirection, file desc.)

- compression - possible to acquire devices which are larger than the size of the investigator workstation
- splitting - possible to acquire an image in usable chunks
- secure imaging - possible to encrypt, sign, and hash while imaging
- [gzip, openssl, dcfldd, gnupgp, split, md5sum]

Embedded and other small devices

- toolkits for accessing many embedded devices (but often not in the same way as disks)
- PDAs, iPods, digital cameras, cellphones, smartcards
- [pilot-link, gnupod, gnokii, opensc]

Imaging and Evidence Acquisition (cont.)

Evidence file formats

- currently raw images such as dd are the open standard
- Simpson Garfinkel has recently developed the Advanced Forensic Format (AFF), as an open source equivalent of the Encase .E0* files.
- [dd,afflib]

Managing Acquired Data/Evidence

Preservation

- cryptographic hashing (MD5, SHA-1)
- investigator signing (pgp/gpg, smime)
- timestamping/TSA (RFC 3161)
- [md5sum, openssl, dcfldd, gnupg, openTSA]

Packaging

- archive multiple files/directories
- vendor-independent format
- compressed, possibly encrypted
- [tar, zip, gzip, bzip, openssl, gnupg]

Managing Acquired Data/Evidence (cont.)

Storage

- long-term storage of evidence data
- different storage media supported (CD, DVD, Tape)
- backup systems
- [dump, tar, amanda, cdrecord]

Transfer

- secure transfer of data/evidence
- inter-divisional, inter-organizational
- encrypted and authenticated
- [scp, apache-ssl, smime, pgp]

Recovery/Normalization

Partitions

- deleted partition detection, restoration
- [gpart, disktype, testdisk, hexedit --sector]

Files/filesystems

- deleted file recovery (many fs supported)
- slackspace recovery
- data carving
- [gpart, sleuthkit, formost, fatback, e2salvage, formost, disktype, testdisk, scrounge-ntfs, scapel, magicrescue]

Recovery/Normalization (cont.)

Cryptographically protected/hidden data

- password recovery
- steganography detection
- [fcrackzip, crack, lcrack, nasty, john the ripper, stegdetect,stegbreak, cmospwd, pwl, madussa]

Analysis

- Searching/filtering
  - known-good, contraband files, NSRL/Hash databases
  - support for powerful regular-expressions
  - antivirus and rootkit searches
  - [clamAV, F-PROT, chkrootkit, grep, autopsy, find, swish-e, glimpse, ftimes, md5deep, hashdig]
- International language support, Unicode
- Timelining/correlation/sorting
  - Sleuthkit produces excellent filesystem timelines
  - [pyflag, autopsy, zeitline, sleuthkit]

Analysis (cont.)

- Converters, editors, data dumping
  - wide variety of hexeditors
  - email analysis, attachments
  - many data and log file analysis tools (cookie files, browser cache, history, etc.)
  - [ghex, khex, hexedit, openssl, uuencode, mimedecode, hexdump, od, strings, antiword]
- Document/Image viewers and multimedia players
  - wide range of tools for current and obsolete documents
  - scriptable thumbnail, image manipulation support
  - configurable video playback, variety of formats
  - [openoffice, gv, xv, imagemagic, mplayer, vlc]

Mounting and Booting Suspect Images

- Loopback mounting acquired images
  - in a read-only manner
  - useful for browsing/searching
  - Wide range of filesystem support (apple, microsoft, various unix)
  - [mount, losetup]
- Virtually booting an image on a Linux PC
  - booting a Macintosh image (MacOS9, OSX)
  - booting Windows images
  - Any other X86 OS image (Linux)
  - [pearpc, VMWare*]

Simulators for Running Programs

- Dos/Windows simulation
- Mac simulation
- Palm simulation
- HP48
- Various unix binary support
- [dosemu, wine, VMWare*, pose, x48, linux-abi]

Support for Analyzing Legacy Technologies

- Home computers from the 80s and early 90s
  - Sinclair ZX Spectrum, ZX81 [xzx, fuse, x81]
  - Apple IIGS, early Mac [xgs,prodosemu, vMac, basiliskII]
  - Commodore C64, C128, VIC20, PET, and CBM-II [vice,frodo]
  - Amiga [uae, hatari, e-uae]
  - AtartiST, Atari 800 [stonx, atari800]
- Mainframes and minis
  - IBM System/370, ESA/390 [hercules]
  - Dec PDP- series, Nova, and IBM 1401 [sim, klh10]
- Other legacy operating system support
  - MS-DOS [doscmd, dosbox, dosemu]
  - CPM [cpmemu]

Case Management, Bookmarking, Reporting

- Auto generated pdf reports possible to a certain degree
- Integrated bookmarking support is difficult, too many separate tools
- Integrated reporting is also difficult when using multiple tools.
- Case management is often rudimentary (file/directory based)
- [pyFlag, autopsy, sleuthkit, Latex, pdf tools]

Microsoft Specific Tools

MS System tools
- Tools for viewing the registry
- Tools for the event viewer
- Analysis of INFO2 and Recycle bin
- cab files, OLE properties
- [ntreg, kregedit, regviewer, grokevt, rifiuti, orange,fccu-docprop,]

Outlook and IE tools
- converting MS Outlook .pst files to plain text
- analyzing cache files and cookies
- [libpst, readpst, pasco, galleta]

Other Forensic Areas (very brief)

Network Forensics
- packet capturing tools
- [tcpdump, etherreal, tcpflow, ssldump, tcptrace, ngrep, driftnet]
- basic tools for Internet investigations
- [nslookup, dig, whois, traceroute]
- various other troubleshooting tools

Other Forensic Areas (very brief)

Live system Forensics
- memory examination
- state of system and configuration
- logs
- host-based intrusion detection systems
- [ps, netstat, ifconfig, lsof, memdump, tripwire]

Other Forensic Areas (very brief)

Software Forensics
- emulators/simulators
- debuggers
- dissassemblers
- reverse-engineering tools
- [gdb, strace, coreography, fenris, truss and dtrace (Solaris)]

Non-forensic Tools for Forensics

Non-forensic tools are often useful
- trouble shooting and debugging tools
- conversion and data migration tools
- repair tools
- log processing, statistics/trend tools

Getting additional data from existing tools
- many programs have additional verbose or debugging flags
- can be configured to do additional logging

Resources for Linux tools

e-evidence.info
opensourceforensics.org
linux-forensics.com
freshmeat.net
sourceforge.net

Disadvantages of Linux in Forensics Labs

- Requires some retraining
  - it takes time and effort to learn Unix/Linux
  - command line is not as intuitive as an all-GUI environment
- Support model is different
  - often no formal support organization (however, the informal support is sometimes superior)
  - support queries are often direct to the community at large, and the quality of the answers varies greatly

Disadvantages of Linux in forensics labs (cont.)

- Interoperating with proprietary technology is hard
  - proprietary technologies are reverse engineered, not licensed
  - sometimes this takes time to implement
  - maybe not be a complete implementation
- Volunteer development effort
  - software maybe in perpetual state of development
  - maybe abandoned, dead projects
  - "rough around the edges"
  - in some cases poorly documented (the source code might be the only documentation)

Advantages of Linux/OSS in forensics labs

- Software availability and accessibility
  - software is freely available on the Internet
  - source code is provided
  - tools can be closely scrutinized for correctness
- Efficiency
  - allows for much automation and scripting
  - helpful in labs with high volumes of casework
- Optimizing and Customizing
  - since the source can be freely modified, software can be modified to fit the requirements of a particular lab

Advantages of Linux in Forensics Labs (cont.)

- Support
  - ad-hoc community support can be excellent
  - mailing lists can answer calls for help within minutes
  - often quick implementation of patch and feature requests.
- Linux/OSS is ideal for an academic/lab settings
  - it uses open, published standards, not closed or proprietary
  - vendor-neutral
  - strives to work together with competing groups, not against them
  - building on previous work is encouraged
  - interoperable/compatible across technologies, organizations, and over time

Summary

Over 100 open source tools have been listed here which can be used to perform forensic and investigative work. This list is not exhaustive and many more exist, or are in development.

Using Linux for corporate or law enforcement labs is viable. A complete range of functionality exists to deal with typical laboratory casework.

The open, published, and free nature of open source tools lends itself well to the academic community. They are an excellent teaching/learning aid, and are well suited for open research environments.

Concluding Remarks

Thanks for listening

If you have comments or want to contact me:

nikkel@digitalforensics.ch

Slides will be available at:

www.digitalforensics.ch

Any questions?