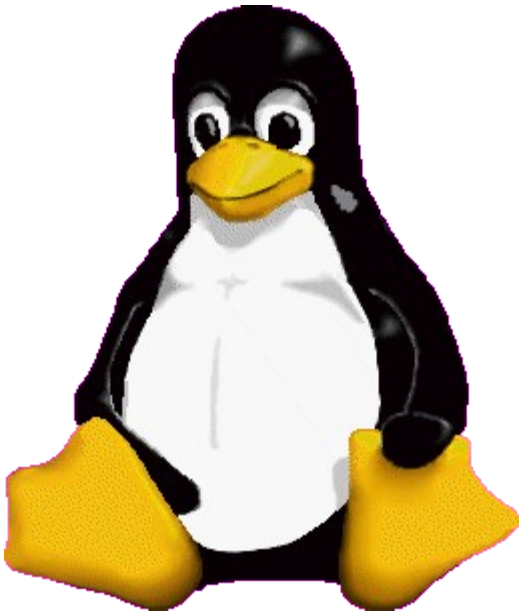
Linux in Law Enforcement



It's all about CONTROL

Barry J. Grundy
CPOSC
October 2010

!! Disclaimer !!

- **This presentation is not sponsored by any organization of the US Government**
- **I am here representing only myself**
- **The opinions stated in this presentation are my own and do NOT represent any official position of the US Government or any Government agency**

Linux in Law Enforcement

Agenda

- Who is this guy?
- What is a computer crime?
- What is computer forensics?
- Why use Linux and Open Source?
  - Technical Arguments
  - Legal Arguments
- What Linux and Open Source tools are available?
- Okay…so how is it done under Linux?

Linux Credentials

Author - *Law Enforcement and Forensic Examiner's Introduction to Linux, A Beginner's Guide*

- FLETC, NSLETC, Interpol, Multiple Universities in the US and Overseas.
- http://www.LinuxLEO.com

Linux LEO

The Law Enforcement and Forensic Examiner's Introduction to Linux

News

-Version 3.21 released: 12 Dec 2007
-Version 3.20 released: 22 Oct 2007
-Linux LEO Goes Live: 22 Oct 2007

Documents

The Beginner's Guide v3.21 (PDF)
Readme File (txt)
Change log (txt)
ToDo List (txt)

Supplemental Files

Floppy Practice Image (practical.floppy.dd)
"Able2" Ext2 Disk Image (able2.tar.gz)
Practice Log Archive (logs.v3.tar.gz)
Raw Carving Practice (image_carve.raw)

Welcome to Linux LEO

You have reached the home of the Law Enforcement and Forensic Examiner's Introduction to Linux. The guide has been around for a long time now, without any sort of permanent home. This Web site hopefully takes care of that.

The Purpose of this Site

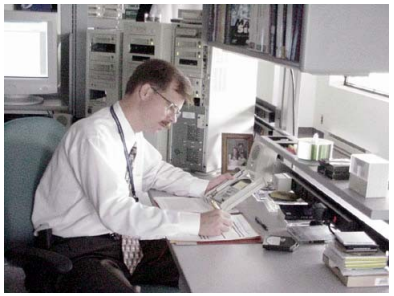
This site is intended to be a simple on line repository for documents (the guide and upcoming additions) that I've written to assist members of the computer forensic community learn more about Linux and its potential as a forensic tool. This is NOT meant to be another "community portal" with forums and articles, etc. There's already plenty of those around (see "Resources" on the left). I've been asked plenty of times to open a forum or mail list for those with questions about the guide, but I don't have the time to administer such an undertaking, and I really feel more can be learned by visiting some of the already established resources. Having said that...feel free to e-mail me at any time with any questions, comments or flames. Feedback is exceedingly important to me. Positive or negative...

What is "Computer Crime"

When is a Crime a Computer Crime?

- When...
  - A computer (computer services or intellectual property) is the *TARGET* of a crime.
  - A computer is a principal *INSTRUMENTALITY* of a crime.
- Or...
  - A computer is *INCIDENTAL* to a crime.

"Computer Forensics"?

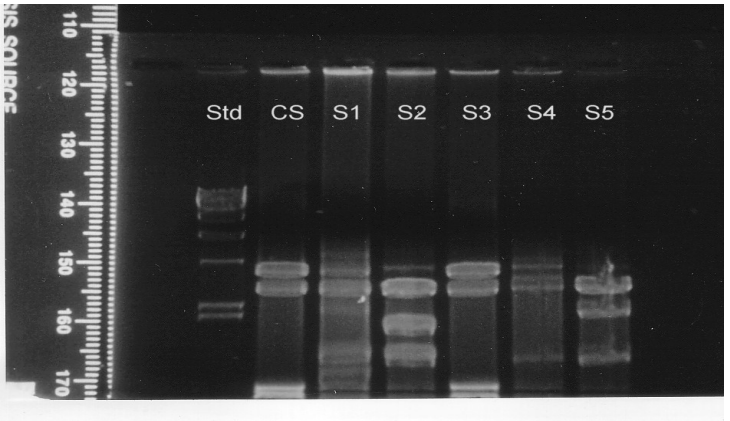


What is "Computer Forensics"?

Forensics **(Webster's Abridged)**

The application of scientific knowledge and procedures to legal problems;

Especially**:**
scientific analysis of evidence (as from a crime scene)



What is "Computer Forensics"?

Computer Forensics has "branched":

- Classic Computer Forensics
  - Data Recovery
  - "Pull the plug"
- Computer Intrusion analysis
  - Lots of Correlation
  - Volatile data (no plug pulling!)
- Electronic Discovery ("E-Discovery")
  - Civil Litigation (IP, etc.)
  - Drives the industry

What is "Computer Forensics"?

At its Core – regardless of case:

- Acquisition – collection of evidence.
  - Drive imaging…
  - Volatile data recovery, log recovery, etc.
  - **Acquisition is the "heart" of computer forensics.**
  - A plausible case derives from this step.

What is "Computer Forensics"?

At its Core – regardless of case:

- Analysis
  - Multiple "layers"
    - Physical through Application
  - Looking for:
    - Inculpatory Evidence
    - Exculpatory Evidence
    - Tampering
  - Data recovery, temporal analysis, etc.

What is "Computer Forensics"?

At its Core – regardless of case:

- Reporting and Testimony
  - Driven largely by jurisdiction.
  - Can be automated by the forensic tools used.
  - Level of detail and format depends on the audience or customer.
  - This is DIFFERENT than "Documentation".

Why Linux for Forensic Examinations?

It's Free!

(Which is why I started using it...)

Why Linux for Forensic Examinations?

But really it's because of...

Total Control

Why Linux for Forensic Examinations?

- Direct control of all attached hardware.
- Control of all device (and FS) permissions.
  - Read/Write/Execute (mount options)
  - HAL has complicated this
- Built in disk image and *basic* analysis capabilities
- Many ported and native forensic utilities available.

Why Linux for Forensic Examinations?

Support for multiple file systems

- Ext3 / Ext4, etc. (Linux Native)
- Fat 16 (msdos)
- Fat 32 (vfat)
- NTFS (ntfs-3g)
- XFS
- UFS
- HFS
- Many more… (most are native to kernel)

Why Linux for Forensic Examinations?

- Maximum Flexibility.
  - Vmware/VirtualBox
  - Wine/Cygwin
  - Legacy hardware support.
- Endless support base.
  - Web forums
  - LUGS
  - IRC

Why Linux for Forensic Examinations?

Provides an *alternative platform* for cross-verification and validation

- Open source tools (legal argument)
- Different set of “issues” than Windows
  - Notice the word “different”
- Testing environment for hardware and software.

Why Linux for Forensic Examinations?

How about:

Just Plain Powerful?

Power of CLI!

- Speed (vs. GUI…really!)
  - Log parsing
  - (grep/sed/awk vs. Notepad…)
- Granular command control
- More intuitive scripting
  - it's just BASH.

Superman?

Linux will NOT solve all your forensic woes…

- Steep learning curve (for new users).
- Mainstream software availability.
- Linux assumes you know what you are doing. (Age old danger of “root”).
- Starting to lose some control with Desktop orientation…see Fedora/Ubuntu.

Open Source Legal Argument

http://www.digital-evidence.org/papers/opensrc_legal.pdf

Admissibility of Evidence:

- Previously based on “Frye Test”
  - Peer review and Journal published
- Now based on “Daubert Test”
  - Not every forensic discipline had access to a peer reviewed scientific journal
  - Offered additional quality tests

Open Source Legal Argument

- Daubert Test addresses:
  - Testing (false negatives/positives)
  - Error Rate
  - Publication
  - Acceptance
    - generally accepted
    - *relevant* scientific community?
  - Digital evidence can also be seen as “testimony” under the Federal Rules of Evidence

Open Source Legal Argument

Open source programs address these issues:

- Access to code improves testing – in code review
- Error rates can be reported through open “bug tracking” or code “diffs” in releases.
- Bug tracking is not driven by revenue.
  - Bugs are not “features”.
- Published “abstraction” techniques allow the analyst to decide on the veracity of findings
  - NTFS file name analysis, for example.
  - What is this tool doing?

Linux for Forensic Examinations

How is it done?

"Forensic" Utilities Included in Linux

Acquisition Tools:

- *dd* – disk imaging, carving, splicing
- *md5sum* and *sha1sum* – hashing tools

Analysis Tools:

- *fdisk* and *sfdisk* – disk geometry
- *find* and *grep* - search tools
- *xxd* – hex editor
- *file* – magic!

- Tons of other stuff…

"Forensic" Utilities available for Linux

Acquisition Tools:

- *dcfldd/dc3dd* – DoD version of *dd* with logging and hash window functions.
- *ddrescue/dd_rescue* – error handling *dd*.
- *ewfacquire* – libewf project to work with EWF images (EnCase).
- *aimage* – Advanced Forensic Format (afflib).
- *Air/Adepto/GRAB* – GUI frontends to dd/dcfldd
- md5deep – recursive hashing tool.
- *SMART* – not open source, but important for Linux...

“Forensic” Utilities available for Linux

Analysis Tools:

- The SleuthKit (TSK) – the big daddy of open source computer forensics.
  - Provides a suite of CLI tools for all layers of analysis (short of application).
- Carving Tools:
    - Scalpel / Foremost / Photorec
- More at : http://www.opensourceforensics.org
- *SMART* – not open source, but important for Linux…

"Forensic" Utilities available for Linux

Analysis Tools:

- The SleuthKit (TSK)
  - Media Mgmt: *mmls, mmstat, mmcat*
  - File System:
    - *fsstat, ffind, fls*
    - *istat, ifind, ils, icat*
    - *blkstat, blkls, blkcat, blkcalc, blkid*
    - *jls, jcat*
  - Other tools: *hfind, sorter, mactime, sigfind*
  - Recent *beta* updates

“Forensic” Linux Boot Disks

Bootable CD's for Forensics:

- Helix:
  - http://www.e-fense.com/helix/
  - Bootable Mac/Linux/Win
  - Forensic adjustments
  - Forensic software, including TSK
  - Excellent for live acquisitions
  - No longer free, used to be a good starting point for forensic exploration.

“Forensic” Linux Boot Disks

Bootable CD's for Forensics:

- SMART for Linux
  - http://www.asrdata2.com/
  - Based on Ubuntu
  - Forensically optimized
  - Forensic software, including TSK
  - Evaluation version SMART
  - Free CD, But SMART app is $$

  - Also see the FBCD: http://www.forensicbootcd.com/

What next? Your Choice!

Demo of Forensics?

- Image recovery from NTFS (TSK)
- Physical File Recovery from String Search
- Anything else?

or just Questions?

It's all about Control