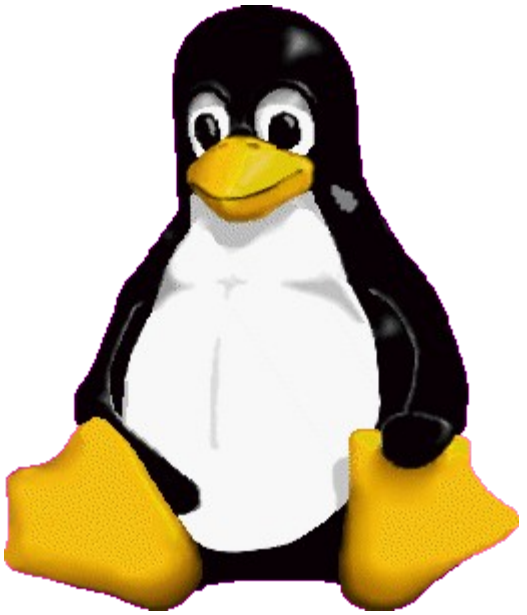
Open Source Data Recovery



Options and Techniques

Barry J. Grundy
CALUG MEETING
October 2008

!! 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**

Open Source Data Recovery

Agenda

- What do we mean by “data recovery”?
- How does it differ from computer forensics?
- Types of recovery:
  - Damaged or dying disks
  - Damaged file systems or partition tables
  - Deleted and lost files
- What Linux and Open Source tools are available?
- Okay...so how is it done under Linux?

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 "DATA RECOVERY"?

Data recovery is the process of **salvaging data** from **damaged, failed, corrupted, or inaccessible secondary storage media** when it cannot be accessed normally. Often the data are being salvaged from storage media formats such as hard disk drives, storage tapes, CDs, DVDs, RAID, and other electronics. Recovery may be required due to **physical damage to the storage device or logical damage to the file system** that prevents it from being mounted by the host operating system..

Wikipedia

Data Recovery != Forensics

Computer Forensics: Recovery of EVIDENCE

- Meta data
- Attribution
- Lead Generation
- Temporal Analysis
- Simple Data Recovery without Forensic Analysis
  maybe *harmful* to a case

Data Recovery: Recovery of INFORMATION

-regardless of meta data (but not always)

-Attribution is often meaningless

Data Recovery Strategy

The #1 guaranteed strategy for proper data recovery:

Data Recovery Strategy

Proper Backups!

***but y'all knew that, right?**

Barry J. Grundy

Data Recovery Strategy

Given the time limits of this presentation, I will concentrate on the specifics of a limited number of Open Source Tools.

- Media Errors: *ddrescue*
- Partition and FS recovery: *testdisk*
- File recovery (Logical): *Sleuthkit*
- File recovery (Physical): *photorec / scalpel*

I would be remiss in not mentioning R-Studio suite of tools:

http://www.r-tt.com/

Data Recovery Strategy

Every data recovery effort has a common step:

PRESERVE THE ORIGINAL MEDIA

- Whenever possible, create an image of the data container.
  - Provides redundancy
  - Guards against user error
  - Guards against further loss resulting from mis-diagnosed cause
- This starts with *ddrescue*
- Continued "physical recovery" can proceed using */dev/loop*

Data Recovery Strategy – Media Errors

Disk Drive Failure

User Recoverable:

- disk must be kernel accessible
- bad sectors (constantly remapping)
- some magnetic defects

Clean Room:

- platter and mechanical failure
- “head crash”

You may only get one shot at this, so choose wisely!

Data Recovery Strategy – Media Errors

Disk Drive Failure

http://www.myharddrivedied.com/

- Go to the “presentations” section
- Good source for advice

You may only get one shot at this, so choose wisely!

Data Recovery Strategy – Media Errors

ddrescue

Viable tools:

- dd
- dc3dd/dcfldd – forensic variants
- ddrescue (gnu ddrescue, not dd_rescue)

Be careful of buffering issues with dd and related programs – use direct i/o (flag).

Data Recovery Strategy – Media Errors

ddrescue

Benefits:

- Non-linear acquisition
- Interruptions can be continued
- Robust logging
- Specifically designed to deal with bad sectors, not just “skip over them”.

General Usage:

ddrescue input output log

ddrescue /dev/sdx outputfile.ddr ddrlog.txt

Data Recovery Strategy – Media Errors

ddrescue

ddrescue recovery strategy (bad disk):

- Keep a log for multiple runs
- Start by skipping bad areas – get the good first
- Keep the drive cool

Recovery Usage – 2 (or more) Runs:

ddrescue -n /dev/sdx outputfile.ddr ddrlog.txt

ddrescue -d -r3 /dev/sdx outputfile.ddr ddrlog.txt

Data Recovery Strategy – Deleted Partitions

Disk Drive Failure

Partition table deletion can be recovered using ***testdisk*** - http://www.cgsecurity.org/wiki/TestDisk

- Deleted partitions
- Recover boot sectors
- MFT/ FAT recovery
- EXT Backup Superblocks
- “testdisk” – “mkfs.ext2 -n” “e2fsck -b”

DEMO

Data Recovery Strategy – Deleted Files

Deleted Files

Two Basic Approaches:

1) Logical Recovery
   - use the file system meta data to locate and recovery

2) Physical Recovery
   - Use file "magic" (headers and footers) to "carve" files from physical blocks on the file system.

Data Recovery Strategy – Deleted Files

Deleted Files

Logical Recovery

- File system dependent meta data:
  - NTFS = MFT
  - FAT = File Allocation Table
  - EXT = Inode Table / Superblock
- We use directory entries for file names

Data Recovery Strategy – Deleted Files

Deleted Files

Logical Recovery

- The Sleuthkit
  - www.sleuthkit.org
- Tool Organization (Layers)
  - File system layer (**fs**)
  - File name layer (**f**)
  - Data layer (**d**)
  - Inode layer (**i**)

Data Recovery Strategy – Deleted Files

Deleted Files

The SleuthKit (TSK)

- Disk: *disk_stat, disk_sreset*
- Media Mgmt: *mmls, mmstat*
- File System:
  - *fsstat, ffind, fls*
  - *istat, ifind, ils, icat*
  - *dstat, dls, dcat, dcalc*
  - *jls, jcat*
- Other tools: *hfind, sorter, mactime*

Data Recovery Strategy – Deleted Files

Deleted Files

Physical Recovery

- Use file “magic” to recover files
- file header and footer
- known types, or build your own
- subject to fragmentation
- can be targeted through block groups, etc.

- scalpel, foremost, Photorec.

Data Recovery Strategy – Deleted Files

Deleted Files

Scalpel:

http://www.digitalforensicssolutions.com/Scalpel/

- edit the config file (looks like a magic file)
- output is to empty or non-existing dir
- use cluster size (for boundry)
- consider using unallocated only (dls).

DEMO

"Rescue" Linux Boot Disks

Bootable CD's for Forensics:

- Helix:
  - http://www.e-fense.com/helix/
  - Based on Knoppix
  - Forensic adjustments
  - Forensic software, including TSK
  - Has a real nice Windows side for live acquisitions
  - Free, and a good starting point for forensic exploration.

“Rescue” Linux Boot Disks

Bootable CD's for Forensics:

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

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

Questions?

For example:

- **Can I recover deleted ext3 files?**
- **What's the difference between deleted ext2 and ext3?**

It's all about Control

Barry J. Grundy