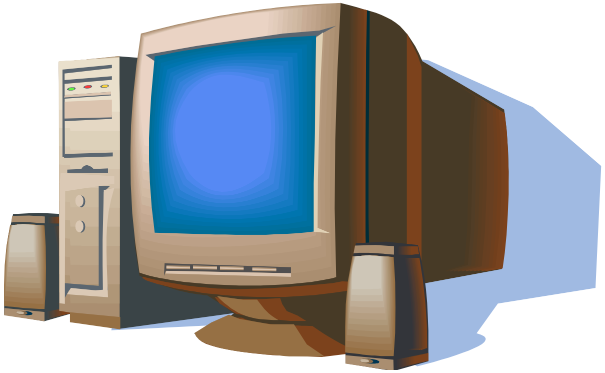
IT GOVERNANCE AND CYBERCRIME

19/04/10

Open Source Forensic Tools

Agenda

- What is Open Source
- Features Open Source
- Relevance to Digital Forensics
- Windows Based
- Unix Based
- Caveats of Open Source
- Open Source vs. Closed Source
- Future



What is Open Source?

- □ **NOT** free
- □ License – GNU/GPL/GNU 2.0
- □ Collaboration
- □ Many Iterations
- □ Successful

Features of Open Source?

- Cost Effective
- **RAD** – Rapid Application Development
- “Great minds think alike”
- Standards Compliant
- Constantly updated
- Can be cross platform

Relevance to Digital Forensic

- Many areas – Network, Computer and Environmental for example

- Work in the same principal and approach:
  - Acquisition
  - Extraction
  - Analysis
  - Report

- Environment Independent
  - Windows 32/64 bit
  - Unix/Linux – 32/64bit

Windows Based Software

Microsoft®

Forensic Acquisition Utilities 32/64 bit

- Open License – Allows for use in commercial and non-commercial environments
- Collection of software
- 4MB download
- Allows collection of data from a running computer

http://www.gmgsystemsinc.com/fau/

FAU – Includes

- □ DD – creates byte-level images of source input
- □ FMData – displays details of file and directory attributes
- □ NC – remake of netcat – read and write data across networks
- □ Volume Dump – shows information about all drives in computer
- □ Wipe – wipes the data from hard drive

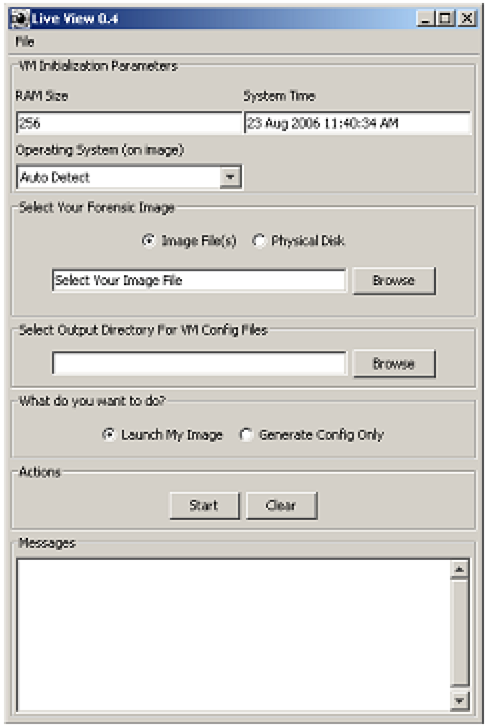
http://www.gmgsystemsinc.com/fau/

LiveView

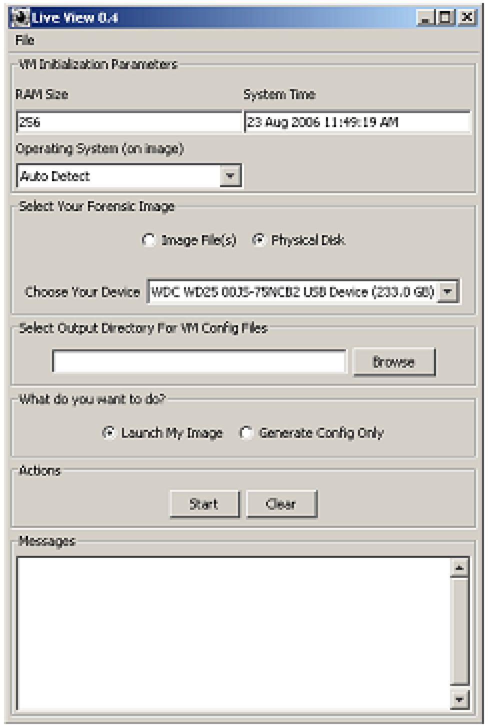
- Written in Java
- Boots DD-style Hard disk images into the operating system
- Requires other free software to run
- Auto generation of MBR (if not present)

http://liveview.sourceforge.net/

Screenshots of LiveView

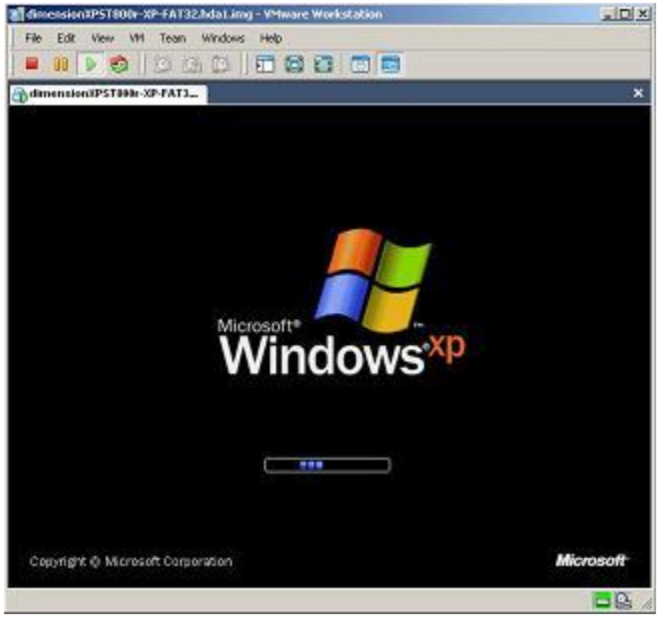

Live View 0.4
File
VM Initialization Parameters
Select Your Forensic Image
Browse
Select Output Directory For VM Config Files
Browse
What do you want to do?
Actions
Start
Clear
Messages

RAM Size: 256
System Time: 23 Aug 2006 11:40:34 AM
Operating System (on image): Auto Detect
● Image File(s) ○ Physical Disk
Select Your Image File
● Launch My Image ○ Generate Config Only


Live View 0.4
File
VM Initialization Parameters
Select Your Forensic Image
Select Output Directory For VM Config Files
Browse
What do you want to do?
Actions
Start
Clear
Messages

RAM Size: 256
System Time: 23 Aug 2006 11:49:19 AM
Operating System (on image): Auto Detect
○ Image File(s) ● Physical Disk
Choose Your Device: WDC WD25 00JS-75NCB2 USB Device (233.0 GB)
● Launch My Image ○ Generate Config Only

Choose boot type – image or physical drive

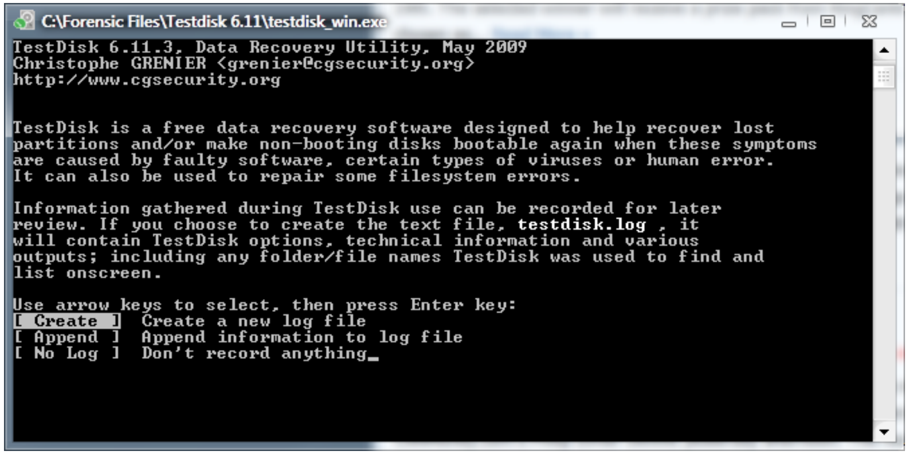

dimensionXPST800r-XP-FAT32.hda1.img - VMware Workstation
File
Edit
View
VM
Team
Windows
Help
dimensionXPST800r-XP-FAT3...
Microsoft®
Windows xp
Copyright © Microsoft Corporation
Microsoft

Booting operating system in virtual environment

TestDisk 6.11

- Open source
- Recovery of files and partitions
- Command line Interface

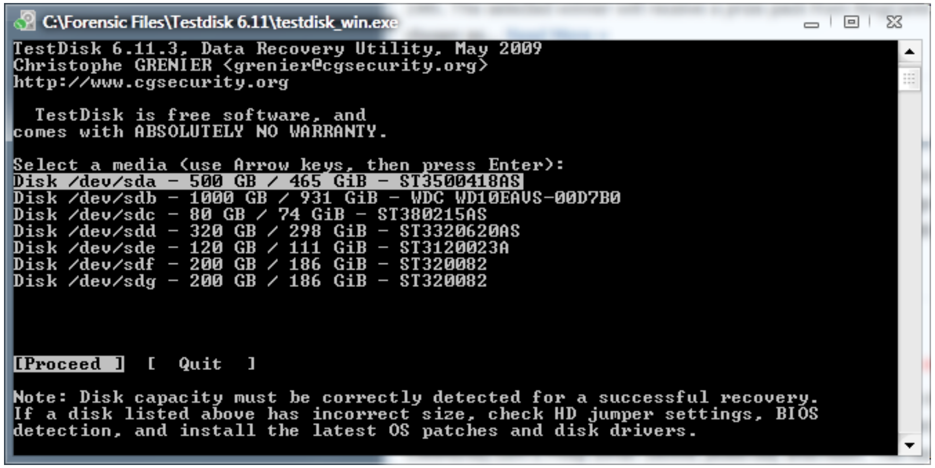
Screenshots of TestDisk 6.11



```
TestDisk 6.11.3, Data Recovery Utility, May 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org


TestDisk is a free data recovery software designed to help recover lost
partitions and/or make non-booting disks bootable again when these symptoms
are caused by faulty software, certain types of viruses or human error.
It can also be used to repair some filesystem errors.

Information gathered during TestDisk use can be recorded for later
review. If you choose to create the text file, testdisk.log , it
will contain TestDisk options, technical information and various
outputs; including any folder/file names TestDisk was used to find and
list onscreen.

Use arrow keys to select, then press Enter key:
[ Create ]  Create a new log file
[ Append ]  Append information to log file
[ No Log ]  Don't record anything_
```

TestDisk can create logs and work off the logs. This can easily help with long file recovery processes. Or even additional – saving time and time.

Choose the disk from which you want to recover the partitions



```
TestDisk 6.11.3, Data Recovery Utility, May 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

  TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk /dev/sda - 500 GB / 465 GiB - ST3500418AS
Disk /dev/sdb - 1000 GB / 931 GiB - WDC WD10EAVS-00D7B0
Disk /dev/sdc - 80 GB / 74 GiB - ST380215AS
Disk /dev/sdd - 320 GB / 298 GiB - ST3320620AS
Disk /dev/sde - 120 GB / 111 GiB - ST3120023A
Disk /dev/sdf - 200 GB / 186 GiB - ST320082
Disk /dev/sdg - 200 GB / 186 GiB - ST320082



[Proceed ]  [  Quit  ]

Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

Microsoft Coffee

- Used specifically by law enforcement (FBI)
- Not open source; ***free***
- Easy training – can be trained in 10 minutes
- Supported by INTERPOL and NW3C (USA)

http://www.microsoft.com/industry/government/solutions/cofee/default.aspx

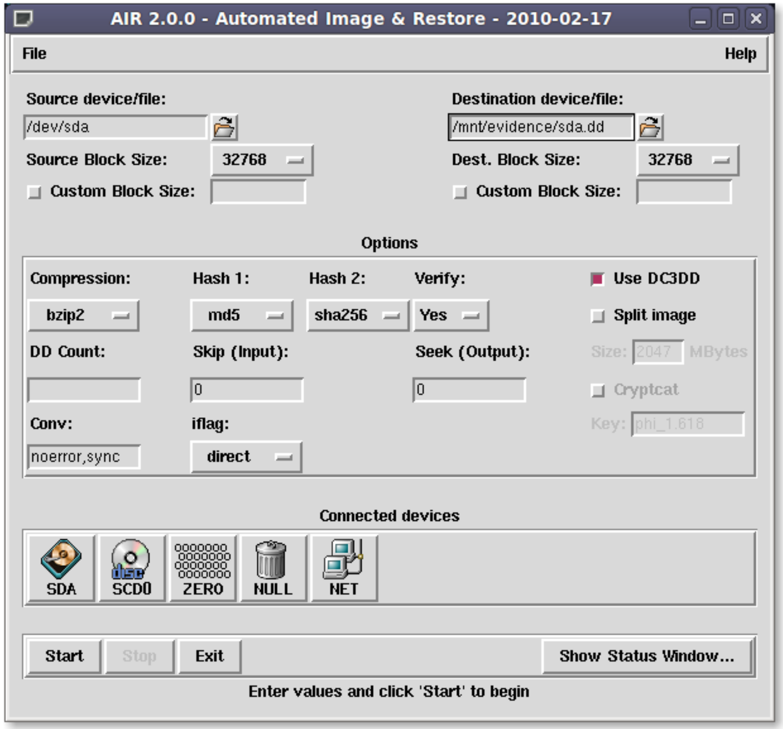
Unix/Linux Based

AIR – Automated Image Restore

- Open source
- Provides GUI for DD/DC3DD imaging CLI
- User friendly
- Does not require knowledge of DD-CLI

http://air-imager.sourceforge.net/

Screenshots of AIR



AIR 2.0.0 - Automated Image & Restore - 2010-02-17

Source device/file: /dev/sda

Source Block Size: 32768

□ Custom Block Size:

Destination device/file: /mnt/evidence/sda.dd

Dest. Block Size: 32768

□ Custom Block Size:

Options

Compression: bzip2

Hash 1: md5

Hash 2: sha256

Verify: Yes

☒ Use DC3DD

□ Split image

Size: 2047 MBytes

DD Count:

Skip (Input): 0

Seek (Output): 0

□ Cryptcat

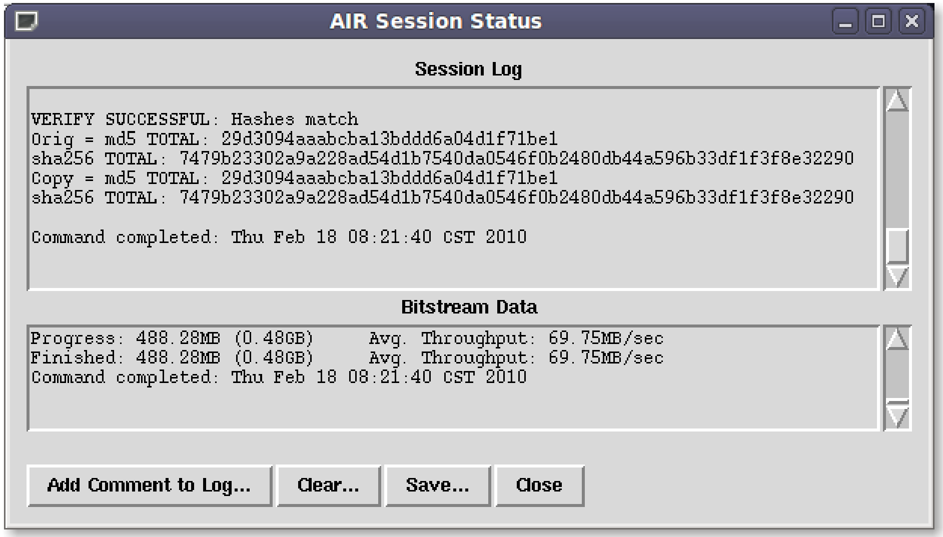
Key: phi_1.618

Conv: noerror,sync

iflag: direct

Connected devices

Enter values and click 'Start' to begin



AIR Session Status

Session Log

```
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 29d3094aaabcba13bddd6a04d1f71be1
sha256 TOTAL: 7479b23302a9a228ad54d1b7540da0546f0b2480db44a596b33df1f3f8e32290
Copy = md5 TOTAL: 29d3094aaabcba13bddd6a04d1f71be1
sha256 TOTAL: 7479b23302a9a228ad54d1b7540da0546f0b2480db44a596b33df1f3f8e32290

Command completed: Thu Feb 18 08:21:40 CST 2010
```

Bitstream Data

```
Progress: 488.28MB (0.48GB)      Avg. Throughput: 69.75MB/sec
Finished: 488.28MB (0.48GB)      Avg. Throughput: 69.75MB/sec
Command completed: Thu Feb 18 08:21:40 CST 2010
```

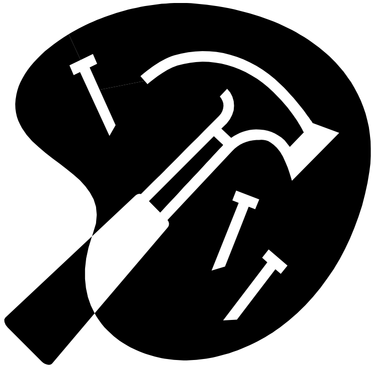
http://air-imager.sourceforge.net/

The Sleuth Kit (TSK) 3.0.1

- Open source
- Comes with a GUI “Autopsy Forensic Browser”
- Command line analysis tool
- Works similar to encase.
- Digital Evidence Bag

Caveats of Open Source

- □ Integrity – not validated in the court of Law
- □ Easily reverse-engineered
- □ Can be exploited
- □ No financial backing



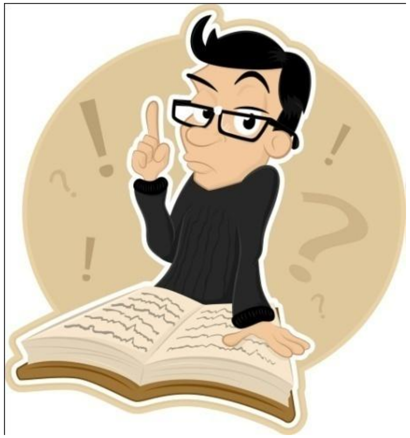
Open Source vs. Closed Source

- Open source tools are better tested – more time ensuring it meets the standards

- Closed source provides manuals and guidelines on usability of application

- Support is often phone based – additional charges vs. Online forum based

- Direct developer interaction



Future

- Demand
- Forensic Laboratory
- Subject Matter Experts
- Validity/Integrity

Thanks…Any Questions?