Building a Basic Computer Forensics Laboratory

SSA J. P. McDonald
Laboratory Director - PHRCFL
FBI Philadelphia
jpmcdonald@rcfl.gov
Topics

• Lab Space
• Equipment Needs
• Software Needs
• Supply needs
• Training
• Procedures
Lab Space

- Secure
- Adequate electricity for equipment
- Adequate cooling, low humidity for equipment
- Desks/benches for forensic analysis and administrative work
- Locking rooms, or containers for evidence, both original and Derivative
- Internet connection
Equipment – Write Blockers

- Hardware write blockers
  - Support all types of hard drives
  - www.wiebetech.com
Equipment – Exam Computers

• Want fastest computers you can afford with:
  – Ram – As much as it will take and you can afford
  – CPU – Quad, or at least duel core CPUs
  – Good Graphics card, Sound Card, Speakers
  – Fire wire 800, 400
  – USB 2
  – DVD/CD-RW and DVD/CD-R drives
  – Large Monitor
  – Printers
Exam Computers

- Currently evaluating Apple GS5 and Apple Raid
- Can Tri Boot and run Apple, windows and Linux from same box
Exam Computers - Storage

- 1 Terabyte drives are here. How much is that?
  - 1 million photos
  - 16 days of DVD quality video
  - 1 million minutes of music
Exam Computers - Storage

• Need to base storage on what is being used by subjects.
• With 1 TB drives now being sold, would get at least 10 – 20 TB, or as much as you can afford.
• If more than 1 examiner, would recommend buying some type of network storage (NAS, SAN) note, could also use hard drives
  – Possible vendors (many others are out there)
    • Apple xraid
    • Raid Inc. falcon
    • Compellent SAN
Network Equipment

- Network switch, cabling, network cards for forensic work
- Another complete set for Internet and a firewall, can be combined firewall/router/switch
Equipment – Cell Phones/PDAs

• Each phone and PDA use different data connectors and power connectors.
• May consider itips for power needs.
• Sustain cables for phone data cables.
• Also will need some type of signal blocking enclosure for cell phone exams, Faraday Bag.
Equipment – Tape Dives

- Tapes come in all types and sizes
  - DLT/SDLT
  - DDS/DAT
  - LTO
- Used for reading subject’s tapes and archiving work product
Forensic Software

- Virus protection
  - Symantec
  - McAfee
- Forensic Suites
  - Encase
  - FTK
    - FTK
    - PRTK
    - Registry Viewer
  - Ilook
  - Black Bag – Apple
- Cell Phones
  - Data pilot
  - Mobil edit – forensic
  - Simmus
  - bkforensics
  - Software from phone manufacturer
- System Ghosting software
  - Symantec – Ghost
- Free Forensic tools www.acesle.org
Supplies

• Administrative – paper, pens etc..
• Forensic
  – Cables for devices
  – CD-Rs, DVD-Rs, and clamshells for them
  – Tapes
  – Hard Drives
  – Tool Kit
  – Flash light
  – Plastic static bags and bubble wrap
  – Labels – CD/DVD and regular
  – Printers cartridges
Training - Minimum

- Computer hardware / Networking
  - A+; Net+
- Basic Computer forensics knowledge
  - International Association of Computer Investigative Specialists (IACIS)
  - NW3C – BDRA, ADRA (Basic/Advanced Data Recovery)
- Tool Specific Training
  - Encase
  - FTK
  - Ilook
- Legal training – Search Warrants, testifying, computer crime laws and issues for your country.

 NOTES:
 - The field of computer forensics requires daily learning, technology changes everyday
 - Testing – Each Examiner should take and pass a competency test, to show they understand both forensic principals as well as tool use.
Laboratory Policies

- A Laboratory should establish and then follow a set of policies and procedures to run the lab and for doing exams in general.
- Basics
  - Chain of custody and protection of evidence
    - Original Evidence
    - Derivative Evidence
    - All evidence handled by examiner should be initialed, dated and case number written with indelible marker on the item
    - Chain of Custody (Who, What, When, Where, Why)
  - Examination Notes
  - Examination Reports
  - Review of work done in Lab
    - Technical review of examiner’s notes
    - Administrative review of Examination Report
Laboratory Guidance

• Scientific Working Group on Digital Evidence (SWGDE)  
http://ncfs.org/swgde

• American Society of Crime Laboratory Directors / Laboratory Accreditation Board – International  
http://www.asclld-lab.org/
Laboratory Procedures - Exams

- Exams should not be done on original evidence, a write blocker should be attached to the hard drive and a verified (MD5; SHA1) image made (DD, E01, etc..) with archiving software (Encase, FTK imager, DD, etc...)
- The examination computer used for the exam should be reloaded (Symantec Ghost) between exams with a base load and up to date virus software (Symantec, McAfee)
- Findings (files of interest) should be burned to CD-R, or DVD-R, and finalized (nothing else can be burned to disk)
- After exam, image file used for the exam should re validated to show exam did not corrupt
- All of the examiner’s actions should be in their notes. The notes should be initialed on each page, pages numbered 1 of __, and have case #.
Questions

SSA J.P. McDonald
jpmcdonald@rcfl.gov

www.rcfl.gov
www.phrcfl.org