Current Computer Forensics Tools

Evaluating Computer Forensics Tool Needs

- Look for versatility, flexibility, and robustness
  - OS, File system(s), Script capabilities, Automated features, Vendor's reputation for support
- **Hardware forensic tools**
  - single-purpose components to complete computer systems and servers
- **Software forensic tools**
  - Specialized to perform one task to many different tasks
  - Types- Command-line applications, GUI applications

Tasks Performed by Computer Forensics Tools

- Five major categories:
  - Acquisition
  - Validation and discrimination
  - Extraction
  - Reconstruction
  - Reporting

Acquisition

- Making a copy of the original drive
- Acquisition subfunctions:
  - Physical data copy
  - Logical data copy
  - Data acquisition format
  - Command-line acquisition
  - GUI acquisition
  - Remote acquisition
  - Verification

Validation and discrimination

- **Validation**
  - Ensuring the integrity of data being copied
- **Discrimination** of data
  - Involves sorting and searching through all investigation data

- Subfunctions
  - Hashing
  - Filtering
  - Analyzing file headers

Extraction

- Recovery task
- Subfunctions
  - Data viewing
  - Keyword searching
  - Decompressing
  - Carving (reconstructing file fragments)
  - Decrypting
  - Bookmarking

Reconstruction

- Re-create a suspect drive to show what happened during a crime or an incident
- Subfunctions
  - Disk-to-disk copy (dd command, H/W & S/W tools)
  - Image-to-disk copy
  - Partition-to-partition copy
  - Image-to-partition copy
- Some tools that perform an image-to-disk copy:
  - SafeBack, SnapBack, EnCase, FTK Imager, ProDiscover
- Shadowing technique

Reporting

- Earlier - Manual examination, paper report
- Subfunctions
  - Log reports (tools records activities the investigator performed)
  - Report generator (EnCase, ProDiscovery,FTK)

Computer Forensics Software Tools

- Command-line tools
- GUI tools

Command-line Forensic Tools

- **MS-DOS tools for IBM PC file systems**
  - Norton DiskEdit

UNIX/Linux Forensic Tools

- *nix tools for forensics analysis
    - SMART, Helix, BackTrack , Autopsy with Sleuth Kit, Knoppix-STD

Computer Forensics Hardware Tools

- Forensic Workstation
- Write Blocker

Forensic Workstations

- Carefully consider and balance what we need
- Get from - Computer vendors OR tailor to meet needs
- Categories
  - **Stationary**
  - **Portable**
  - **Lightweight**

Using a Write-Blocker

- **Write-blocker**
  - Prevents data writes to a hard disk
  - Software write-blockers
  - Hardware blockers write-blockers

Validating and Testing Forensic Software

- Make sure the evidence we recover and analyze can be admitted in court
- Test and validate the software to prevent damaging the evidence
- **Computer Forensics Tool Testing (CFTT)** program- NIST sponsors project
- Always verify your results
- Use at least two tools
  - Retrieving and examination
  - Verification