Data Acquisition

Prof. Zaheed Shaikh

Overview

- Digital Storage formats
- Validating Data acquisition
- Remote Network acquisition tools

Data Acquisition

- Live acquisition
- Static Acquisition

Digital Evidence Storage formats

- Open Source
  - RAW
  - Advanced Forensic Format
- Proprietary Formats

Raw Format

- Bit by Bit copy
- Sequential Flat file is made of suspect drive/data set

Raw Format Advantages/Disadvantage

- Fast data transfer
- Requires similar space
- Not collect marginal bad sectors on disk drive

AFF

- Create compressed or uncompressed files
- No size restriction
- Open source for multiple platforms
- Internal consistency checks for self authentication

Best Acquisition Method

- Static acquisition limitations that encrypted drives readable only when powered on
- Computers accessible only through network

Acquisition Methods

- Disk to image
- Disk to disk
- Logical disk to disk
- Disk to data file
- Sparse copy of folder or file

Disk to image

- Bit for bit replication
  - Pro Discover
  - Encase
  - FTK
  - Smart
- Not possible for cases where software incompatibilities exist

Disk to Disk

- Older incompatible systems
  - Encase
  - Safeback

Logical or Sparse

- Logical
  - Capture only specific files of interest
  - Email investigation
- Sparse
  - Also collects fragments of unallocated data

Encrypted data

- Key is with suspect
- Free and slack space are nor altered

Validating Data Acquisition

- Byte by byte comparisons
  - X Ways Forensics
  - X ways Win Hex
- CRC-32, MD5, SHA-1-SHA-512
- Linux
  - dd
  - dcfldd

RAID Acquisition

- RAID Random Array of Independent Disks
- RAID 0 Two or more disks seen as one
  - Speed
- RAID 1 making data to be written on two disks simultaneously- mainly for recovery purposes
- RAID 2- similar but uses error correcting codes for validation

RAID Acquisition

- RAID 3 atleast three disks one is used for parity checking
- RAID 4 only difference from raid 3 is data written in blocks not as bytes
- RAID 5 does striping and parity on each disk
- RAID 6, RAID 10, RAID 15- Best speed and data recovery capabilities

RAID Recovery Tools

- Pro Discover
- X Ways Forensics
- Runtime Software

Remote Network Acquisition Tools

- Pro Discover
  - View remote drive when powered on
  - Live acquisition- Smear
  - Encrypt connection
  - Copy Suspects RAM while powered on
  - Use stealth mode to hide remote connection