Topic 3 Acquisition, examination and analysis of evidence in computers and networks Part 2

1

Learning Outcome

After successfully completing this lecture, you will be able to

- Describe and apply the techniques and technologies in acquisition and duplication of evidence data from various sources, media and devices

Road Map

- Computer Volatile and Non-volatile Data
- Computer local and remote data acquisition
- Evidence in Mobile Devices
- Mobile Devices Data Acquisition

Digital Forensics Process

- Collection
  - Collection of media/devices at the scene
  - Identification and Preservation
  - Transportation
  - Data Acquisition and Duplication
- Examination
  - Extraction and searching of data
- Analysis
  - Event and Timeline analysis
- Reporting
  - Reporting and documentation

How can you do it?

- It was reported that the police had tracked down the home address of a member of the hacker group "Anonymous" who hacked into PayPal's website.
- You are asked to accompany the police officers to collect devices and media that may contain evidence related to the website hacking case

Data Acquisition and Duplication

- Identify possible sources of data
  - Hard disks, mobile devices, network traffic, social media and memory
- Develop a plan to acquire the data
  - Likely Value
  - Volatility
  - Amount of Effort Required
- Acquire the data
- Verify the integrity of the data

Possible Data Sources

- Computers
  - Memory
  - System and data hard disks
  - Any more? (SP800-86, page 4-2)
- Mobile Devices
  - USB flash drives
  - Camera SD cards
  - Mobile phones
  - Any more?

Computers: Volatile and Non-volatile data

- For volatile data
  - Live response and Triage
    - Insert a live response CD or USB flash drive to
      - Create an image of Memory
      - Create an image of the system and data hard disks
- For non-volatile data
  - Unplug the power supply of the computer system
  - Put the computer into an evidence bag
  - Move the computer to forensic lab
  - Take photos of the computers
  - Remove all the hard disks from the computers
  - Insert the hard disks into a forensic workstation
  - Perform a physical acquisition by creating images (duplicating) of the hard disks

Computers: Local or Remote Data Acquisition

- Locally through SATA/USB/SCSI
  - Preferred
  - Write-blocker should be used to prevent modification of the original media (hard disk)
- Remotely through a network
  - When local data collection is not feasible, e.g. system-in-question and the forensic system in different rooms

Hard Disks Data Acquisition

Three (3) Approaches

1) Acquiring the image locally by removing the hard disk and connect it to a forensic workstation running of the following software
   - AccessData Imager (for Windows OS)
   - EnCase Forensic (for Windows and Linux)
2) Acquiring the image in a live system through a network using the following tools
   - dd
   - dcfldd
   - dc3dd
   - Other live response forensic disk imaging tool (EnCase linen)
3) Acquiring the image locally from boot-up forensic CD
   - CAINE forensic CD

Hard Disks Remote Data Acquisition in a Live System II

- dcfldd is an enhanced version of dd developed at the Department of Defense Computer Forensics Lab (DCFL), it has the following additional features.
  1) Hash the input data as it is being transferred, helping to ensure data integrity.
  2) Update the user of its progress in terms of the amount of data transferred and how much longer operation will take.
  3) Verify that a target drive is a bit-for-bit match of the specified input file or pattern.
  4) Output to multiple files or disks at the same time.
  5) Split output to multiple files with more configurability than the split command.
  6) Send all its log data and output to commands as well as files natively.

Hard Disks Remote Data Acquisition in a Live System II

- Steps to acquire the image of a live UNIX system using dcfldd
  1) At the target system, mount the network shared drive at the forensic system
     - mount –t nfs 10.0.0.1:/media/disk/ImageStore /mnt/forensicStore
  2) Insert a forensic Live response CD with dcfldd program
  3) Start the disk imaging process
     - dcfldd if=/dev/hda of=/mnt/forensicStore hashlog=hdaMD5.txt

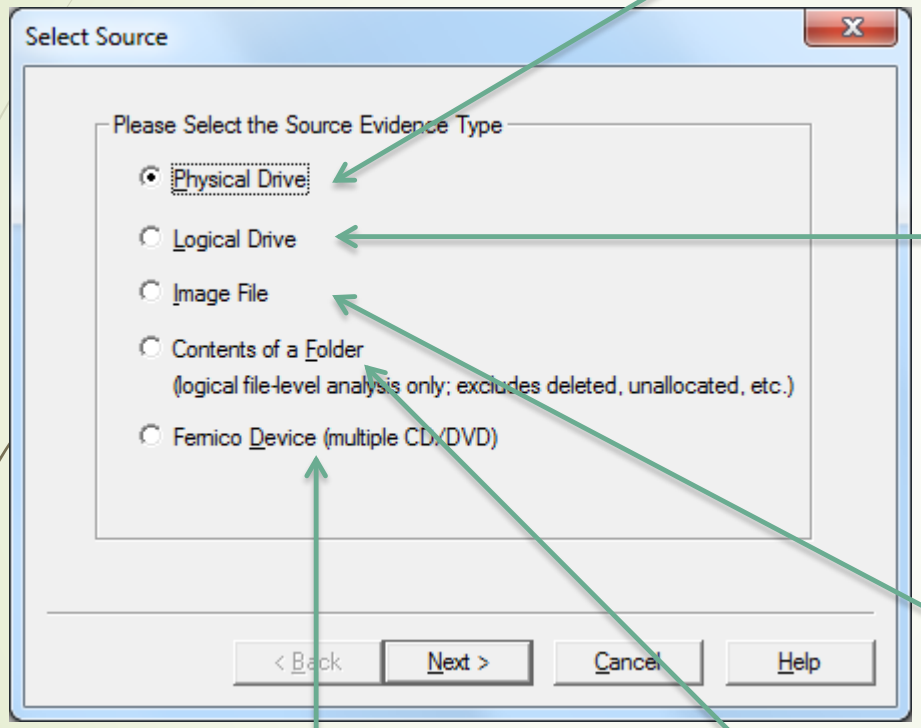
dcfldd and dc3dd used in Linux

- Limitations of dcfldd
  - Fails to create image file for hard drive with bad sectors
- dc3dd is developed by DoD Cyber Crime Center and works for hard drive with bad sectors
- Limitations of dc3dd
  - Support lesser hash algorithms compared to dcfldd
- References
  - http://forensicswiki.org/wiki/Dcfldd
  - http://forensicswiki.org/wiki/Dc3dd

Hard Disk Data Acquisition via Write Blocker

FTK Imager

The usual choice. It will image everything including unallocated space, partition information.



There are scenarios where acquiring the logical drive is more desirable.

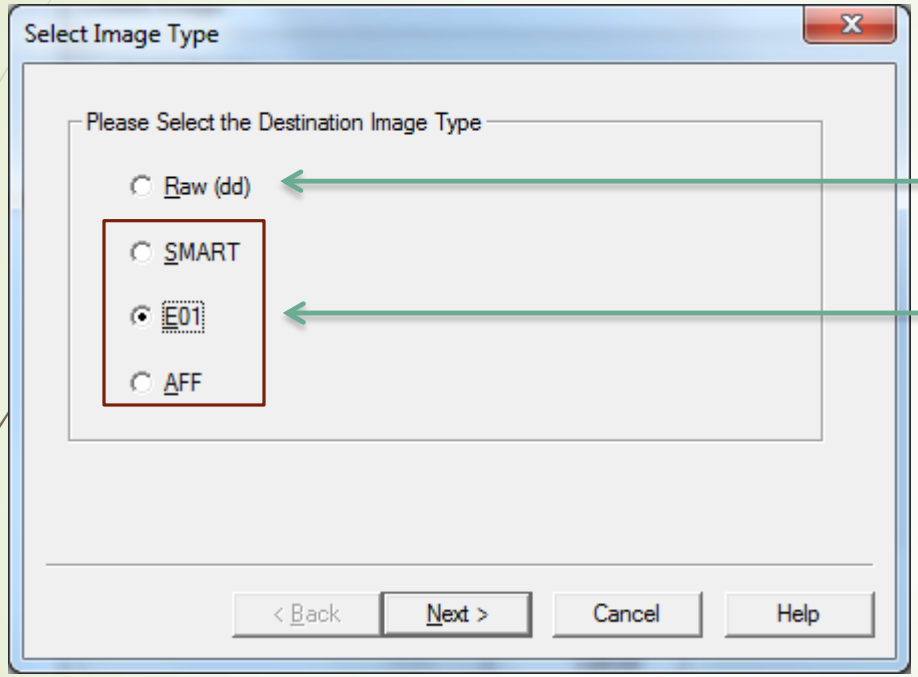
- Multi-disk RAID system
- Encrypted disk

Reimaging an image file comes in handy if there's a need to convert the image format, e.g. E01 to DD

For creating images for multiple CD/DVD with same parameters

Sometimes it's not practical or you are not authorised to acquire the whole drive, e.g. a specific user folder at a corporate server

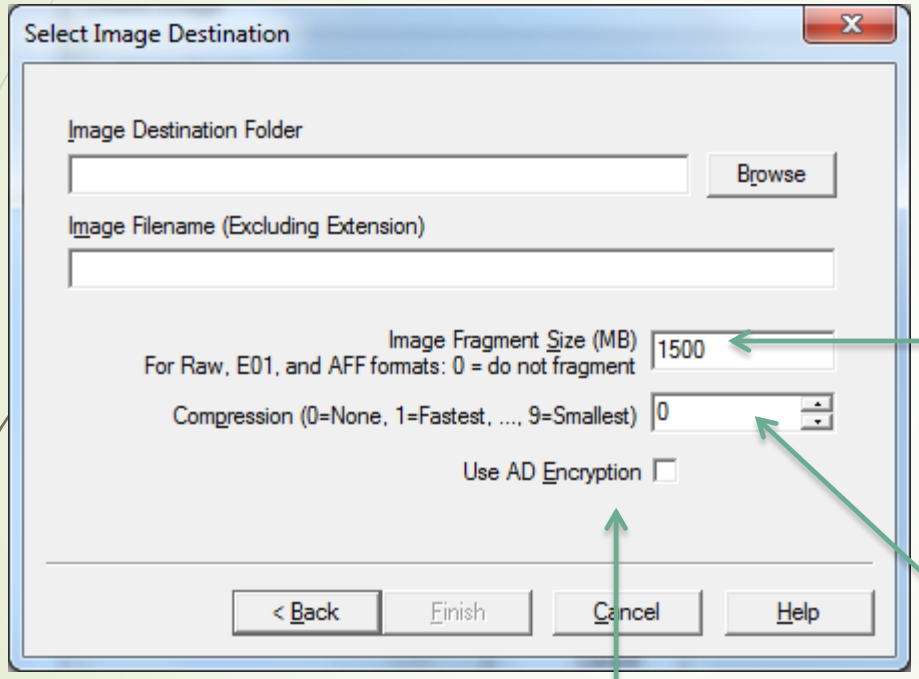
FTK Imager



Data dump

Different formats created by different product manufacturers.
E01 – Encase evidence file format is widely used. It contains acquisition metadata and can compress data.

FTK Imager



Set to 0 to avoid fragmenting the image file, if possible. Modern file systems should be able to handle large files.

Compression is not available for RAW image. Adjusting the compression level may cause compatibility issues across different forensic products.

Good feature if the seized data contains sensitive information. But it requires FTK to decrypt the image during analysis.

Types of Evidence in Computers

- Windows
  - Registry (NTUSER, SAM, SOFTWARE, HARDWARE, SECURITY)
  - Event Logs (Application, System, Security, Custom…)
  - User profile folders (Recently accessed files, downloads…)
  - Jump list (Recently/frequently used files by the applications)
  - Prefetch (Executed programmes)
  - Recycle bin (Deleted files)
  - Thumbnails (Images)
  - Office document metadata
  - Browser (Internet activities: history, cache, cookies, downloads, bookmarks…)

Mobile Devices Data Acquisition

- Mobile Storage Devices
  - USB flash drives
  - Camera SD cards
  - Use Hard Disk Data Acquisition Tools
- Mobile Devices with Operating Systems
  - Personal Digital Assistance (PDA)
  - Mobile phones
  - Tablets
  - Use Special Data Acquisition Tools
- Special Considerations
  - Handling passcode
  - Network isolation
  - Device time difference

Types of Mobile Phones

- Basic mobile phones (2G)
  - Text-based
  - Phone call and maybe SMS

- Advanced mobile phones (2.5G)
  - Multimedia-based: MMS, Email
  - Web-ready

- Smartphones (3G)
  - Multi-applications, multi-processing
  - Touchscreen
  - Soft key
  - GPS

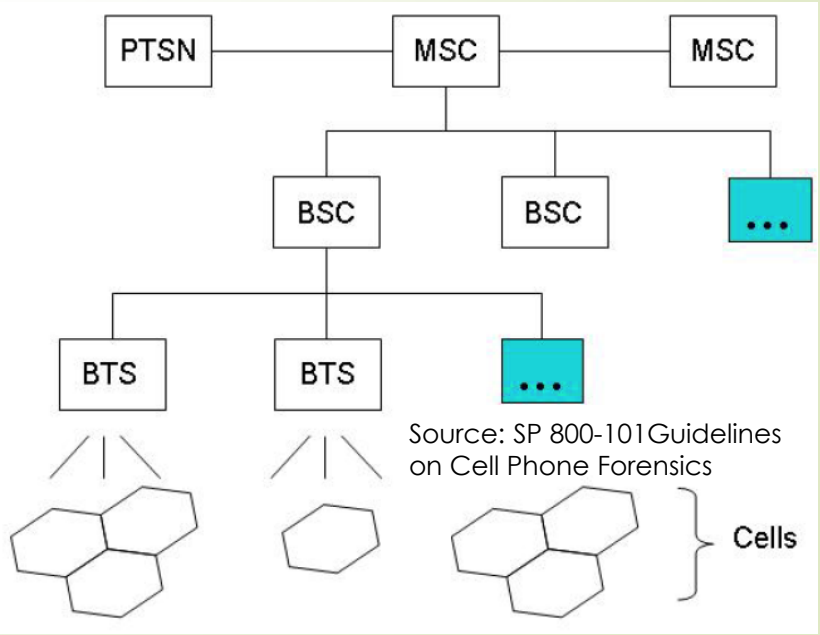
Cellular Network Overview

- GSM (Global System for Mobile Communications)
  - Standards for cellular network serving 80% of the world's population
- GPRS (General Packet Radio Services)
  - Enables packet data transport – 2.5G
- W-CDMA (Wideband Code Division Multiple Access
  - Air interface standard found in 3G mobile telecommunications networks

Cellular Network Overview

- PTSN (Public Telephone Switched Network)
  - MSC (Mobile Switching Centers)
    - BSC (Base Station Controllers)
      - BTC (Base Transceiver Stations)

Mobile phones and smartphones connect to BTC through radio signals



Source: SP 800-101Guidelines on Cell Phone Forensics

Types of Evidence in Mobile Phones

- Call history: details of previous phone calls, voice mails
- Phone book with information of people related to the case
- SMS texts and MMS images/video
- Calendar
- Emails messages
- Photos
- Videos
- GPS location history: where the suspects visited and when
- Internet browsing history and cache
- Passwords to other systems/applications (Yes! Yes!)
- Social relationship (Facebook, twitter etc)

Mobile Phone File System

- SIM Card
  - Subscriber Identity Module, a detachable smart card containing the user's subscription information and phone book
- File System
  - MF (the root of the file system)
    - DF (directory file) GSM
      - EF (elementary data file 1)
        - Service-related information such as IMEI
      - EF (elementary data file 2)
        - Phonebook
      - EF (elementary data file 2)
        - Call information such as last number dialed
      - EF (elementary data file 2)
        - SMS (Short Message Service) messages

Android Phone Data Acquisition

- Physical acquisition
  - Root the Android device
  - Run mobile forensic tool to create an image of the Android physical internal storage, byte-by-byte, sector-by-sector
  - Use "Chip-Off" techniques to read data directly from the internal storage IC chips on the motherboard of the device.
- Logical acquisition
  - Run backup program in Android Studio to create a logical backup copy of the internal storage
- Manual acquisition
  - If the device is not protected by a passcode, do a manual acquisition of the data through the GUI and a camera
- Challenges
  - After rooting an Android phone, the phone may NOT be recovered back to the state before rooting.

Apple iPhone Data Acquisition

- Physical acquisition
  - Bypass passcode protection
  - Install basic kernel into RAM disk
  - Boot up the basic kernel
  - Install and execute live recovery agent
  - Transfer bit-by-bit of the user data partition to a forensic workstation
- Logical acquisition
  - If the iPhone is not protected by a passcode, use the iPhone-iTune synchronization software to backup (image) the data from the iPhone
- Manual acquisition
  - If the iPhone is not protected by a passcode, do a manual acquisition of the data through the GUI and a camera
- Challenges
  - Technical limitation in performing physical acquisition on iPhone 4S and above.
  - Jail-breaking the phone may discredit the evidence's admissibility to court

Cellebrite

Source: Cellebrite http://www.cellebrite.com/mobile-forensics/products/standalone/ufed-touch-ultimate

Other Mobile Forensic Tools

- Autopsy
- Oxygen (oxygen video)
- XRY

Summary

- Computer volatile and non-volatile Data Acquisition
- Computer local and remote data acquisition
- Mobile Devices Data Acquisition

References

1. File System Forensic Analysis, Brian Carrier, 2005, Addison Wesley
2. Guide to Integrating Forensic Techniques into Incident Response SP800-86 NIST, csrc.nist.org
3. http://en.wikipedia.org/wiki/Mobile_device_forensics