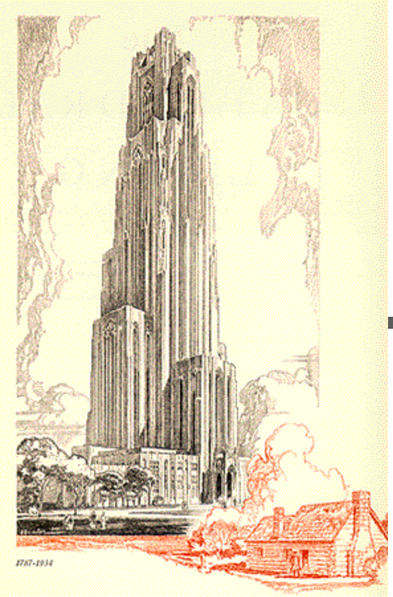
TEL2813/IS2621 Security Management



James Joshi

Associate Professor

Lecture 3

Jan 29, 2014

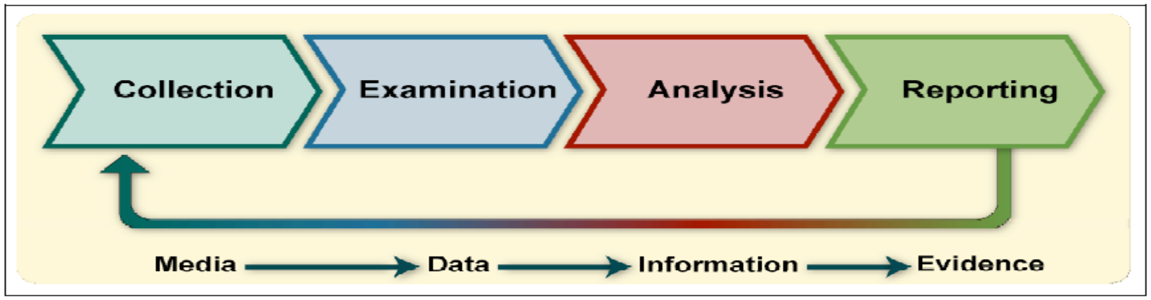
Introduction to Digital Forensics

Digital Forensics

- Also known as
  - Computer forensics or network forensics
- General definition:

  it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data

Forensic process phases



Maintain data integrity

- Collection
  - identify, label, record, and acquire data from the possible sources
- Examination
  - process large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest
- Analysis
  - use legally justifiable methods and techniques,
- Reporting
  - actions used (tools, procedures)
  - provide recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process.

Foresics in Info Systems Life Cycle

- Include Forensics considerations in Info System Life Cycle
  - Regular backups
  - Enable auditing
    - on workstations, servers, network
    - Mission critical applications
  - Centralized secure storage of audit log
  - Maintain database of file hases of Oss and deployed applications
  - Establish data retention policies
    - Support historical reviews
- Maintain guidelines and procedure for forensic activities

Forensic Capability in Organizations

- Key recommendations
  - Orgs should have good C&N forensics
    - Mainly within Incident handling
    - Many teams should participate
  - Determine which party should do it
  - Forensic considerations should be clearly addressed in policies and included in info systems life cycle
    - Roles and responsibilities (internal + external)
    - Policies, guidelines and policies should clearly explain forensic actions (normal or special situations)
  - Maintain proper guidelines and procedures for forensic tasks
    - Legal requirements, evidence preservation

Forensics Process

- Data Collection
  1. Identify possible sources
  2. Acquire data
     - Develop a plan for acquisition; prioritize based on
       - Likely value; volatility (e.g., in live systems); amount of effort required
     - Acquire data
       - Forensic tools; forensic workstations, backup devices, blank media, and evidence handling supplies (e.g., hard-bound notebooks, chain of custody forms, evidence storage bags and tags, evidence tape, digital cameras)
     - Verify the integrity of data

  Evidence preservation may be crucial
     - From legal, disciplinary/standards perspective
     - Cleary define a chain of custody
     - Detailed log of each step in the data collection

Forensics Process

- Data Collection

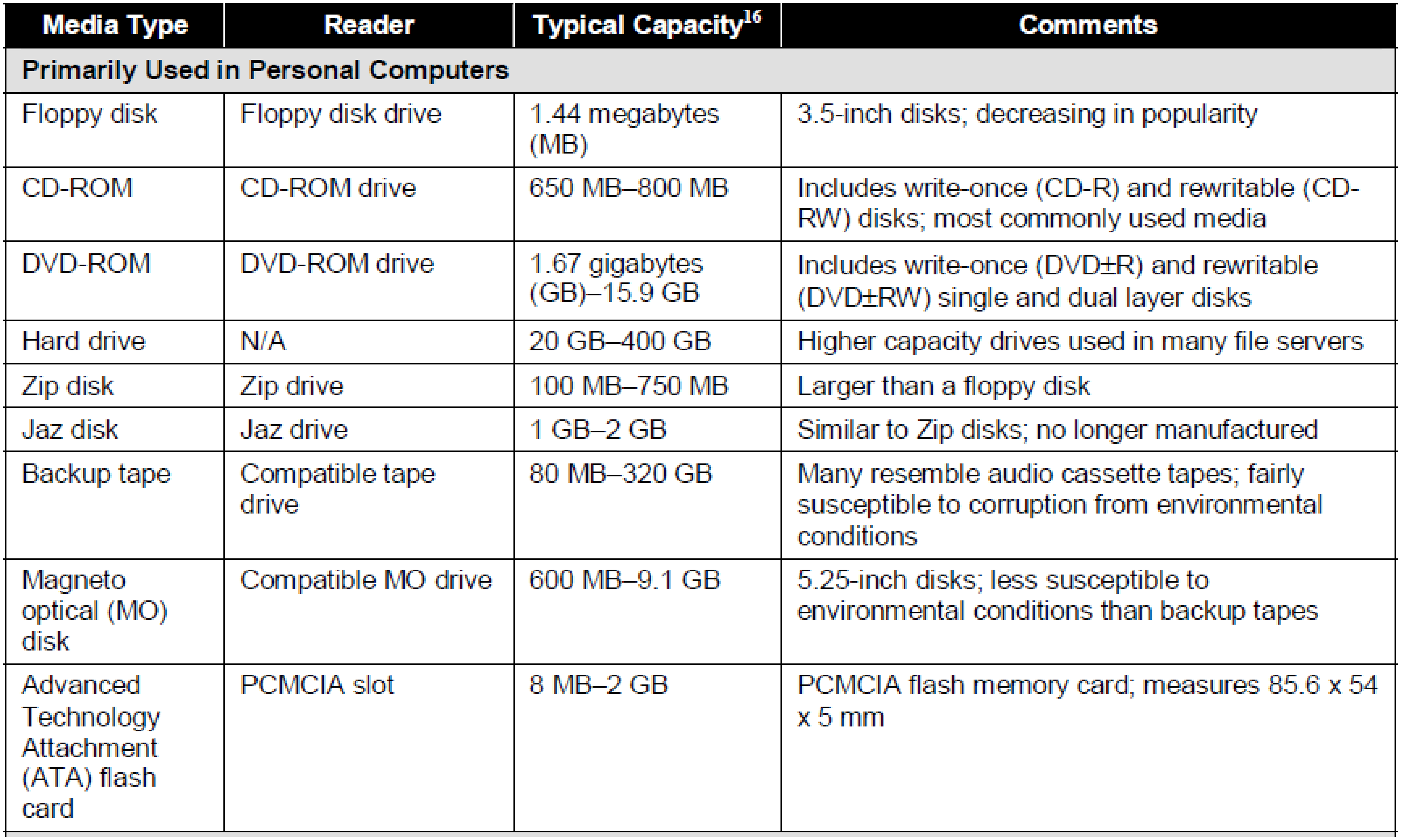
  3. Incident Response Considerations

  - When and how to contain the incident
  - Consider in advance the impact of containment strategies
- Examination
  - Assess and extract relevant information
  - Bypass or mitigate OS or application features
    - Compression, encryption, access control etc.
    - Use tools to search

Forensics Process

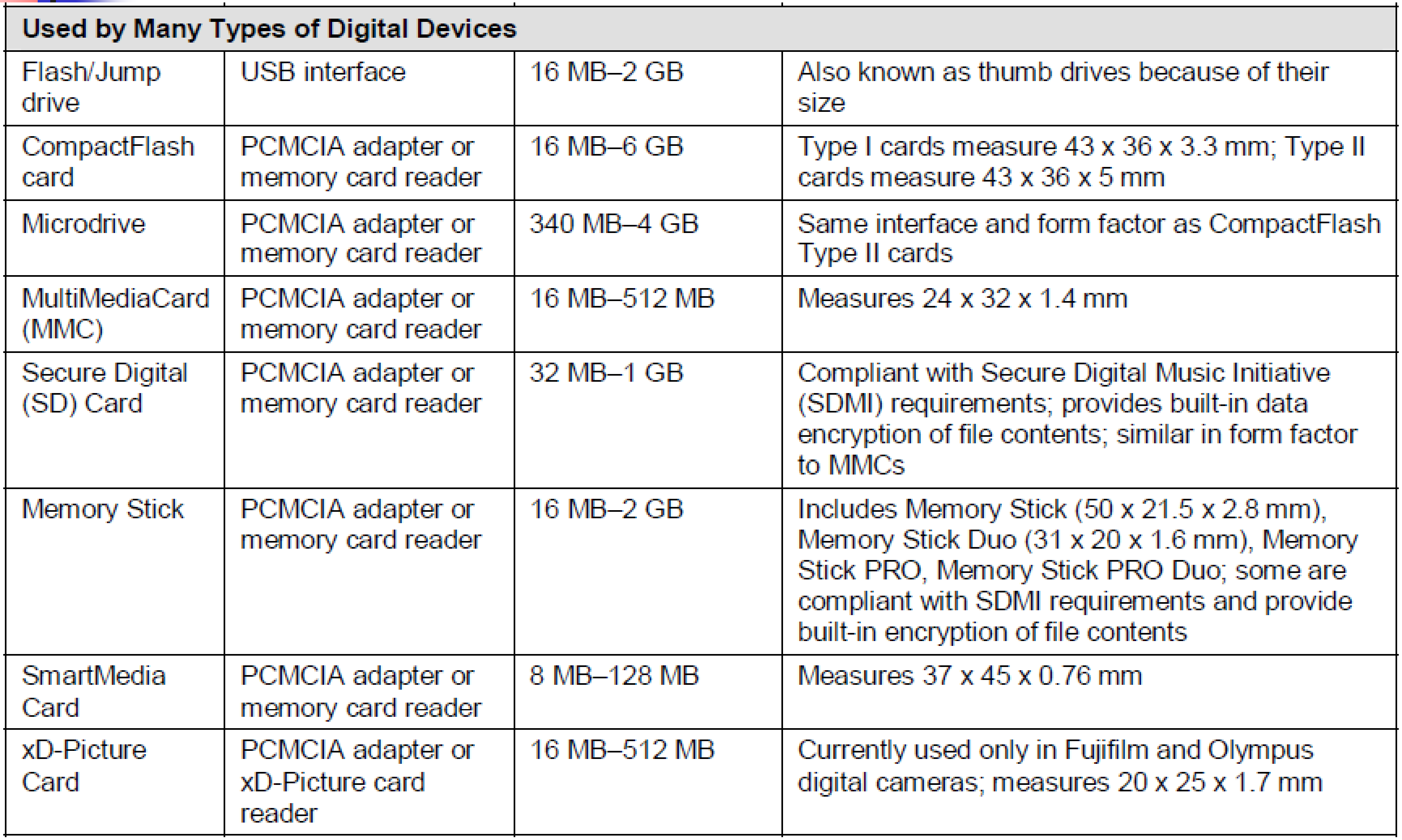
- Analysis
  - Foundation of forensics – use a methodological approach to reach appropriate conclusions
  - identify people, places, items, and events, and determe how these elements are related so that a conclusion can be reached
    - correlate data among multiple sources
- Reporting
  - Prepare and present information from analysis phase
    - Alternative explanations
    - Audience consideration (legal journal, visualization and charts)
    - Actionable information
  - Identify other issues
    - Policy remedy, procedural errors; formal review

Common Media



Media Type	Reader	Typical Capacity[16]	Comments
Primarily Used in Personal Computers			
Floppy disk	Floppy disk drive	1.44 megabytes (MB)	3.5-inch disks; decreasing in popularity
CD-ROM	CD-ROM drive	650 MB–800 MB	Includes write-once (CD-R) and rewritable (CD-RW) disks; most commonly used media
DVD-ROM	DVD-ROM drive	1.67 gigabytes (GB)–15.9 GB	Includes write-once (DVD±R) and rewritable (DVD±RW) single and dual layer disks
Hard drive	N/A	20 GB–400 GB	Higher capacity drives used in many file servers
Zip disk	Zip drive	100 MB–750 MB	Larger than a floppy disk
Jaz disk	Jaz drive	1 GB–2 GB	Similar to Zip disks; no longer manufactured
Backup tape	Compatible tape drive	80 MB–320 GB	Many resemble audio cassette tapes; fairly susceptible to corruption from environmental conditions
Magneto optical (MO) disk	Compatible MO drive	600 MB–9.1 GB	5.25-inch disks; less susceptible to environmental conditions than backup tapes
Advanced Technology Attachment (ATA) flash card	PCMCIA slot	8 MB–2 GB	PCMCIA flash memory card; measures 85.6 x 54 x 5 mm

Common Media



Used by Many Types of Digital Devices			
Flash/Jump drive	USB interface	16 MB–2 GB	Also known as thumb drives because of their size
CompactFlash card	PCMCIA adapter or memory card reader	16 MB–6 GB	Type I cards measure 43 x 36 x 3.3 mm; Type II cards measure 43 x 36 x 5 mm
Microdrive	PCMCIA adapter or memory card reader	340 MB–4 GB	Same interface and form factor as CompactFlash Type II cards
MultiMediaCard (MMC)	PCMCIA adapter or memory card reader	16 MB–512 MB	Measures 24 x 32 x 1.4 mm
Secure Digital (SD) Card	PCMCIA adapter or memory card reader	32 MB–1 GB	Compliant with Secure Digital Music Initiative (SDMI) requirements; provides built-in data encryption of file contents; similar in form factor to MMCs
Memory Stick	PCMCIA adapter or memory card reader	16 MB–2 GB	Includes Memory Stick (50 x 21.5 x 2.8 mm), Memory Stick Duo (31 x 20 x 1.6 mm), Memory Stick PRO, Memory Stick PRO Duo; some are compliant with SDMI requirements and provide built-in encryption of file contents
SmartMedia Card	PCMCIA adapter or memory card reader	8 MB–128 MB	Measures 37 x 45 x 0.76 mm
xD-Picture Card	PCMCIA adapter or xD-Picture card reader	16 MB–512 MB	Currently used only in Fujifilm and Olympus digital cameras; measures 20 x 25 x 1.7 mm

File Systems

File Systems	
FAT12	in floppy disks and FAT volumes smaller than 16 MB
FAT16	MS-DOS, Win 95/98/T/200/XP, etc. Multimedia devises (Camera, audio players); 2 GB in MS/Win
FAT32	Win 95 OEM, Win 98/2000/XP, Win 2003, multimedia devices; volume size is 2 TB
NTFS	(New Technology FS) Win NT/2000/XP/2003 etc; *recoverable*: recover consistency; support data compression/encryption; 2TB
HPFS	(High Performance FS) OS/2; 64 GB
ext2fs	(Second Extended FS) Linus (Unix File types); 4TB – improvement in ext3fs
Others	HFS (Mac OS), CDFS, ISO 9660 & Joliet (for CD); UDF (DVD); Unix File System

Deleted Files

Slack Space

Free Space

Alternate Data Streams (in NTFS)

Data may still be available in store

Copying files from Media

- Logical backup –
  - copies directories & files; it does not capture other data (e.g., deleted files, residual data in slack space)
  - preferable not to copy files from a live system
- Bit Stream Imaging (aka: disk imaging)
  - Bit-by-bit copy of the media including free and slack space

  disk-to-disk copy -- copies the contents of the media directly to another media (requires a second media similar to the original media)

  disk-to-file copy -- copies the contents of the media to a single logical data file

Copying files from Media

- Live systems
  - BSI should not be used as cannot be validated
  - Bit-by-bit copy of logical areas of live system can be completed and validated
  - For logical backups analysts can use standard system backup software

- policy, guidelines, and procedures should indicate the circumstances under which bit stream images and logical backups are to be used

Data File Integrity

- Backed up/Imaged files – integrity!!
  - Write-blocker (hardware or software tool)
  - Hardware write blocker
    - physically connected to the computer and the storage media being processed
  - Software write blocker
    - installed on the analyst's forensic system and currently are available only for MS-DOS and Windows systems
  - Message digest
    - To verify copied data is an exact duplicate
      - MD5, SHA-1, CRC32

Some issues in data collection

- Several approaches to thwart
  - Wiping
    - Tools to remove data (overwrite)
  - Demagnetizing hard drive (degaussing)
  - Physically damaging/destrying
  - Hidden data (not displayed in directories)
  - Striping in RAIDs
    - a striped volume consists of equal-sized partitions that reside on separate disk drives

Examining Data Files

- Locate files – use tools (slack space, etc.)
- Extract the Data
  - Different file types – need to know them from *file header*
    - *Challenges;* when encrypted; use of steganography
  - Use forensic toolkits
    - File viewer
    - Uncompressing files
    - Graphically display directory structures
    - Indentify know files
    - Perform string search/pattern matches
    - Access File Metadata

Analysis

- Recommendations
  - Examine only copies/images
    - BSI for evidence preservation
  - Preserve and verify file integrity (e.g., write blocker)
  - Reply on file header not extensions
  - Use forensic toolkits for examination/analysis