Topic 3 Acquisition, examination and analysis of evidence in computers and networks Part 1

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

- Digital Forensics Vs Data Recovery
- Needs for Digital Forensics
- Data Acquisition and Duplication
- Physical, Logical and Manual Data Acquisition
- Write Blockers
- Integrity Hashes

Digital Forensics vs Data Recovery

- Data recovery involves recovering information from a computer that was deleted by mistake or loss due to unforeseen circumstances
  - Typically you know what you are looking for
- Digital Forensics recovers data that are deleted or hidden, with the goal to ensure the recovered data is valid and can be used as evidence
  - Investigator often does not know if a computer contains evidence

Digital Forensics for Incident Response

- Information security incidents
  - Malicious code
  - Unauthorized access
  - Inappropriate usage
  - Denial of services
  - Multiple Component incidents

- Digital forensics help to collect evidence on
  - Date/time of the incident
  - Source of the attack
  - The damages and other potential damages

Digital Forensics for Incident Response

- The primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings.
- In such cases, evidence should be collected according to procedures that meet all applicable laws and regulations.
- Evidence gathering and handling is not typically performed for every incident that occurs; for example, incidents with low impact do not merit evidence acquisition. (Why?)

Computer Security Incident Handling Guide SP800-61 NIST (csrc.nist.gov)

Digital Forensics for Judiciary Courts

- As more crimes are committed using computers, data network and mobile devices, digital forensics are needed to collect the required evidence related to the crimes.

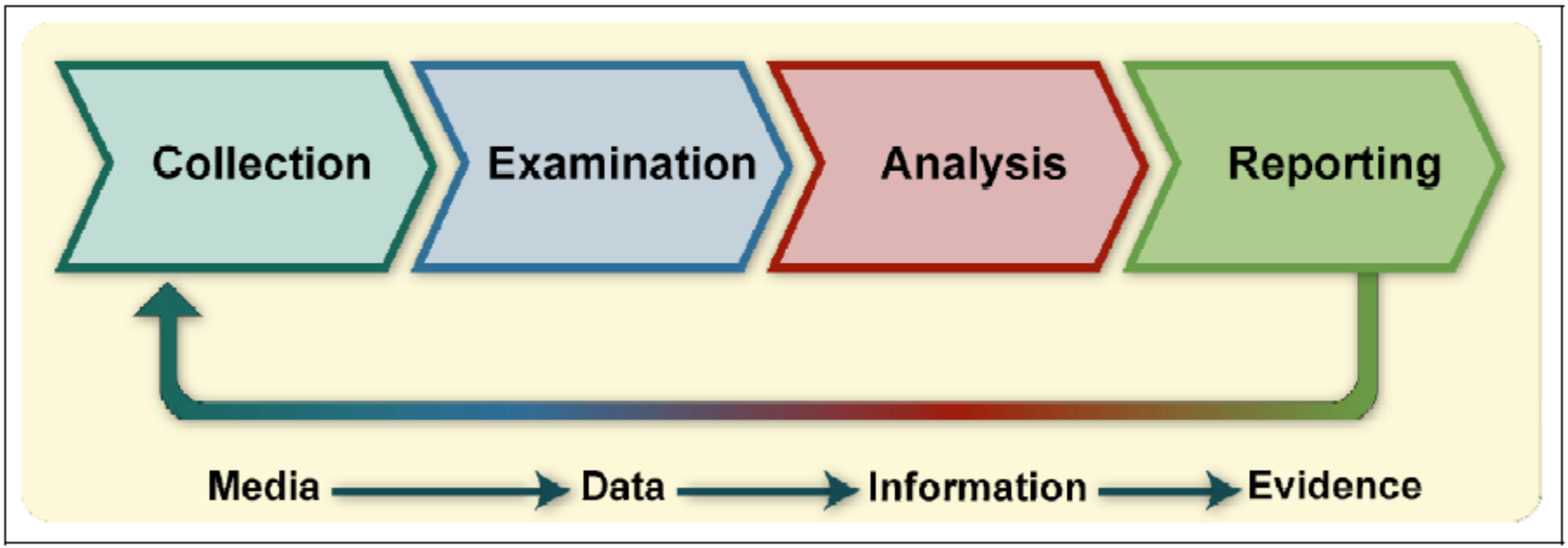
- The objective of the evidence is to prove that a subject (suspected person)
  1. performed some actions (for prosecution use) or
  2. did not perform some actions (for defence use)

Digital forensics for daily operations

- Operational Troubleshooting
- Log Monitoring
- Data Recovery
- Data Acquisition
- Due Diligence/Regulatory Compliance

Computer Security Incident Handling Guide SP800-61 NIST (csrc.nist.gov)

Digital Forensics Process



Guide to Integrating Forensic Techniques into Incident Response
SP800-86 NIST (csrc.nist.gov)

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

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 with required tools
- Verify the integrity of the data (by its hash value)

Data Acquisition and Duplication

- Non-volatile data
  - Permanent storage such as hard disk data does not change after a power shutdown but it may be modified or contaminated during examination and analysis. Creating duplicated images of the original hard disk data for examination and analysis purpose is needed
- Volatile data
  - Evidence in computer memory and network traffic will be lost due to power shutdown or passage of time. Creating a snapshot of the memory or network traffic is needed to preserve this volatile data

Manual Acquisition

Manual Acquisition

- The user interface can be utilized to investigate the content of the system. Therefore the device is used as normal and pictures are taken from the screen.
- Advantages:
  - The operating system makes the transformation of raw data into human interpretable information.
  - Only cameras are needed, specific forensic tools for specific media is not required

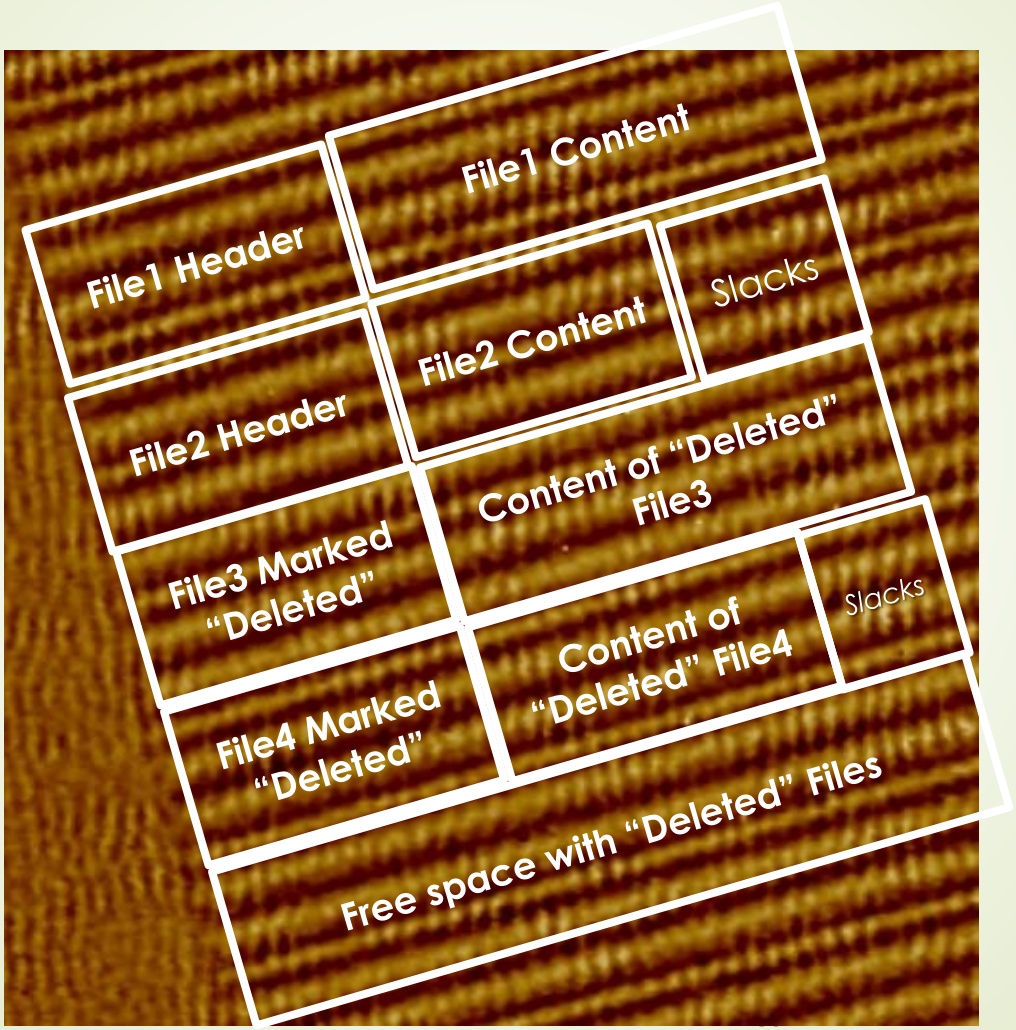
Logical Acquisition

- Logical acquisition implies a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition).
- Advantages
  - Easier for a tool to extract and organise system data structures
  - For example, use the smartphone-PC synchronizing software provided by the manufacturers (e.g. Google, Apple iTune) to extract the required information

Physical Acquisition

- Physical acquisition implies a bit-by-bit copy of an entire physical store such as every sector in a disk drive and every byte in computer memory chips.
- Physical extraction acquires information from a smartphone by direct access to the flash memory, or direct access to every sector in a disk drive through SATA/USB/SCSI instructions.
- Advantages:
  - Allows deleted files and data in unallocated sections to be examined.

Physical Acquisition



By T.J. McMaster *et al.*
Source from University of Britol www.phy.bris.ac.uk

Requirements of Data Acquisition Tools

1. Obtain an exact copy of the original media to be investigated, without altering the original in any way.
   - See how a tool is tested for obtaining exact copy without altering the original copy at http://www.ncjrs.gov/pdffiles1/nij/196352.pdf
2. Ensure that the processes and procedures used can stand up to scrutiny by the opposition's legal team.

See how the available tools are tested at www.cftt.nist.gov

Image duplication Tools

Caution: **All programs that make a duplicate image of a drive must be validated before using.** Validation is independently verifying that the duplicate image program works the way it claims to.

Product	Company	Drive-to-Drive?	Drive-to-Image?	Segmented?	Website
Byte Back[2]	Tech Assist, Inc.	Yes	Yes	Yes	www.toolsthatwork.com
EnCase	Guidance Software	No	Yes	Yes	www.encase.com
Forensic Toolkit	AccessData	No	Yes	Yes	www.accessdata.com
Ghost[3]	Symantec	No	Yes	Yes	www.symantec.com
ILook	Law enforcement only	No	Yes	Yes	www.ilook-forensics.org/
Linux DD		No	Yes	Yes	www.cftt.nist.gov/disk_imaging.htm
ProDiscover	Technology Pathways	No	Yes	Yes	www.techpathways.com
SafeBack[4]	New Technologies, Inc.	Yes	Yes	Yes	www.forensics-intl.com
SMART	ASR Data	No	Yes	Yes	www.asrdata.com

Write-blocker in Data Acquisition

- Create a disk image through write-blockers
  - Devices that allow acquisition (reading) of information on media without accidentally writing or modifying the evidence in the media
  - Hardware write-blockers
    - Drop(block) SATA/USB/SCSI write instructions and data sent from forensic workstation to media contain evidence
  - Software write-blockers
    - Run on a forensic workstation which modifies the interrupt table so that CPU calls write blocker code without writing action instead of normal BIOS write routines

Hardware Write-Blocker

USB Flash Drive Collected from Crime Scene

SD Memory Cards Collected from Crime Scene

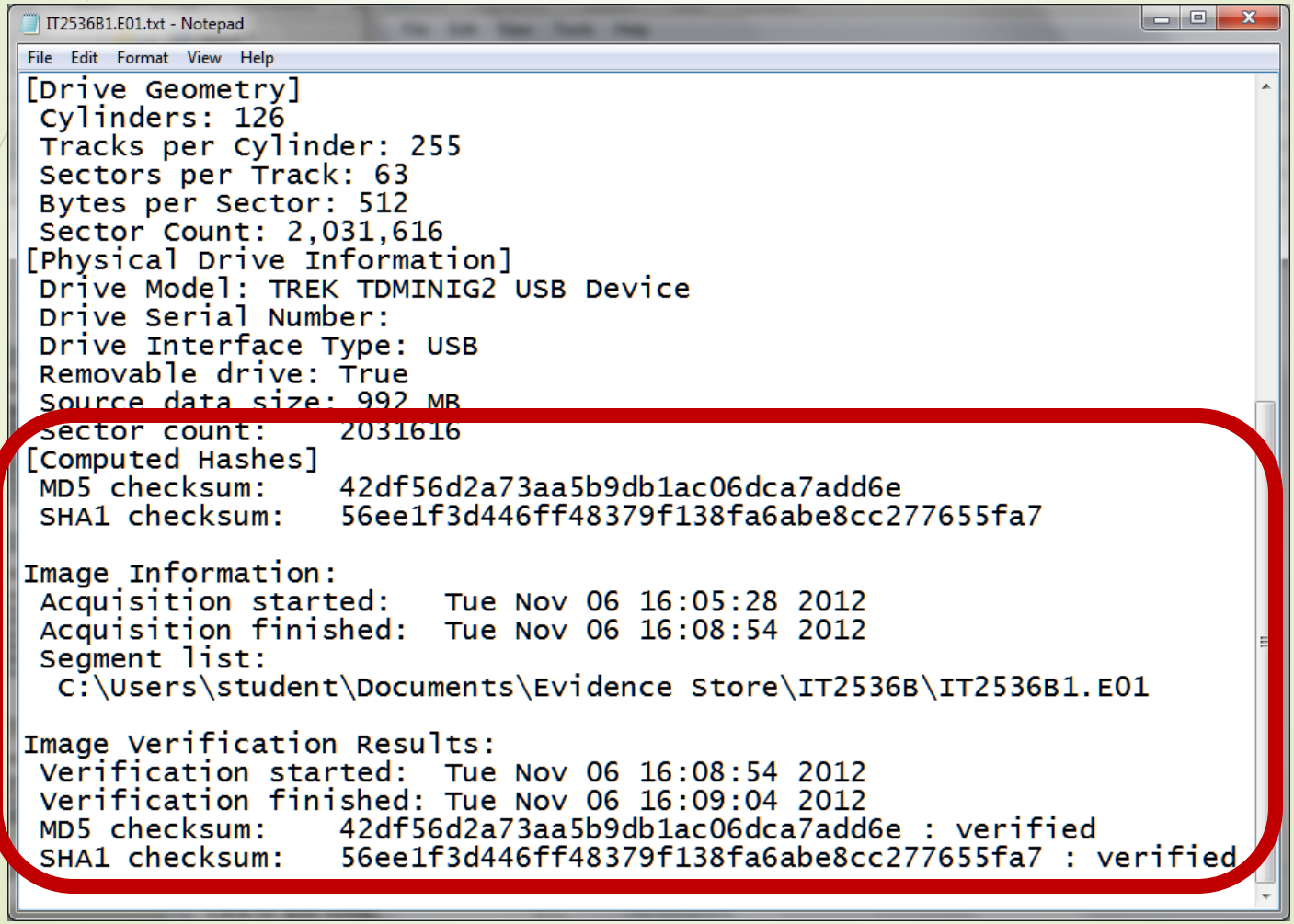
Forensic Bridges / Write Blockers

Forensic Workstation

Integrity Hashes

- The integrity and accuracy can be assured by calculating hash values for the evidence where examiners can later verify the integrity of the data
- Data acquisition tools calculate a hash while the data are being copied.
- Some tools such as Linux dd require a separate tool md5sum to calculate the hash values after the data acquisition

Integrity Hashes



Systems Maintenance Policies that Support Data Acquisition

- Perform regular backups of systems and maintaining previous backups for a specific period of time
- Forward audit records to secure centralized log servers
- Configuring mission-critical applications to perform auditing, including recording all authentication attempts
- Maintain records of system and network configurations
- Comply to data retention policy

FCIV
Microsoft File Checksum Integrity Verifier

- This Microsoft File Checksum Integrity Verifier tool is an unsupported command line utility that computes MD5 or SHA1 cryptographic hashes for files.

```
C:\Users\sinkh\Documents\tools>.\fciv -md5 -sha1 ReadMe.txt
//
// File Checksum Integrity Verifier version 2.05.
//
                MD5                                 SHA-1
------------------------------------------------------------------------
79ac8d043dc8739f661c45cc33fc07ac 2fe398f1ebced1660873626262241b95efeaab407 readme.txt
```

Summary

- Needs for Digital Forensics
- Needs for Data Acquisition and Duplication
- Physical, Logical and Manual Data Acquisition
- Write Blockers
- Integrity Hashes

References

1. Guide to Integrating Forensic Techniques into Incident Response SP800-86 NIST, csrc.nist.org
2. http://en.wikipedia.org/wiki/Write_blocker