Digital Forensics
Week 2

The Forensics Case

Nelson - Chapter 1

Readings – Week 2

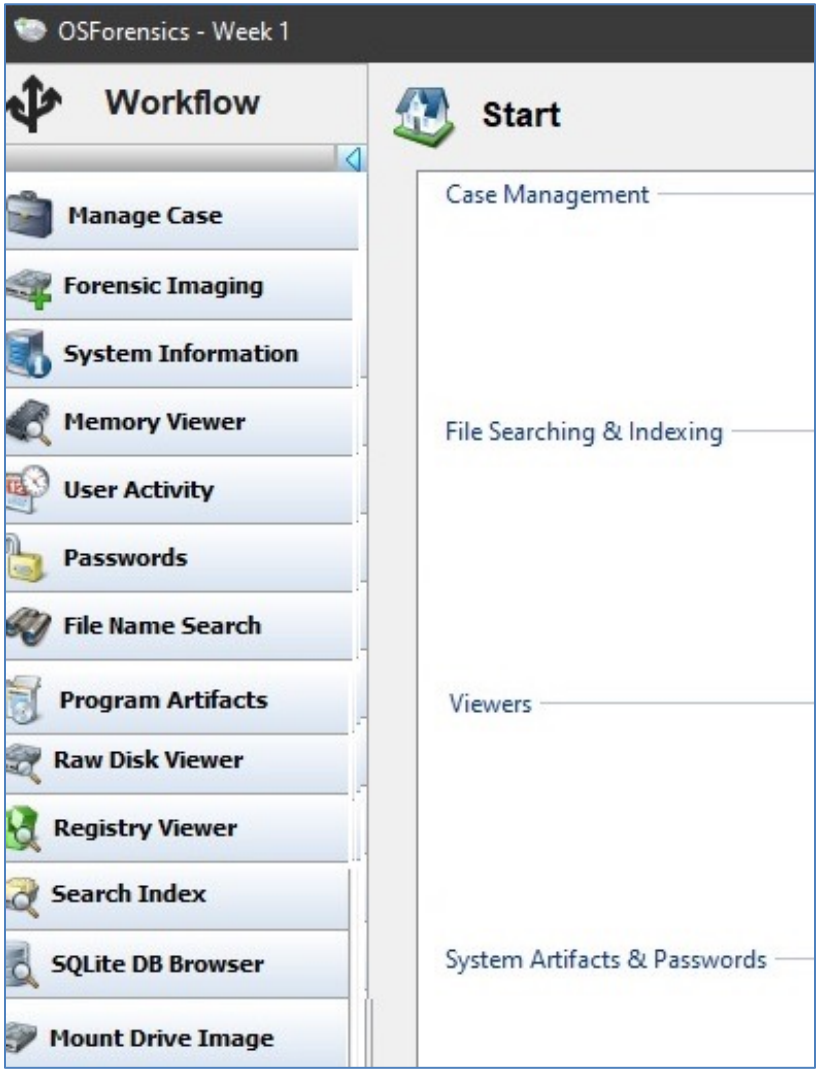
Objectives

- To understand the field of Digital Forensics
- To learn the principles of Digital Forensics

Digital Forensics

- Digital Forensics is the action of applying scientific tests or techniques on a device used in the investigation of a crime.
- Digital Forensics Investigators recover Evidence to support a hypothesis before a criminal court

The Digital Forensics Case



Causes of Forensic Incidents

- Threats and extortion
- Accidents and negligence
- Stalking and harassment
- Commercial disputes
- Disagreements, deceptions, and malpractice
- Property rights infringement
- Economic crime e.g. fraud, money laundering
- Distributing illegal Pornography
- Content abuse
- Privacy invasion and identity theft

The Forensic Process

- A suspicious item is found

- What is the item?
- How did it get there?
- When was it placed there?
- Who put it there?
- Why was it placed there?

- Is it forensic evidence?

Digital Forensics

- There are several branches of digital forensics
- computer forensics
  - examining computer memory and computer disks
- network forensics
  - examining network devices and network packets
- database forensics
  - examining database records
- mobile device forensics
  - examining mobile devices

The three Security Teams

- Vulnerability, threat assessment and Risk Management
  - Penetration Testing
- Network Intrusion detection and incident response
  - Automatic monitoring of Firewall and IDS logs
- Digital Investigations
  - Forensic analysis of systems suspected of containing evidence
  - Initiate the legal process as follows:
  - Allegation or complaint, investigation, case building, trial

Digital Evidence examples

- Was the device used to commit a crime?
  - Sexual exploitation of minors
  - communication of drug deals and their financial records
- Was it simple trespass? (Just looking inside another PC using ssh)
- Or was it theft or vandalism?
- Were a person's rights infringed?
  - cyberstalking or social media harassment

Civil Cases

- Examples include email harassment, falsification of data, discrimination, embezzlement, sabotage and espionage.
- The business needs to continue operating while the investigation proceeds.
- The primary aim is to stop any intrusion and minimise further losses and possible litigation.

Policies

- The best way to reduce the risk of a civil case is to setup and enforce strong policies that are easy to read and follow
- The main policy is for the Acceptable Use of the company's devices and networks
- Published policies provide a line of authority for conducting an internal investigation
- They state who has the right to initiate an investigation, take possession of evidence and access such evidence

Live and Disk Forensics

- You suspect a device is involved in an attack
- How can you confirm this?
- Live Forensics
  - The device is live and the attack is current or very recent
  - You want to capture live evidence before you power it down
- Disk Forensics (post mortem)
  - The device is powered down, or the attack is over
  - You want to examine permanent disk or usb storage for traces of the attack

Order of Volatility

- (Starting with the most volatile)
- CPU Registers, CPU Cache
- Routing table, Process table, Memory allocation
- Temporary File Systems, Swap Space
- Disks
- Remote logging (such as syslog)
- Network Topology, Device Hardware
- Archived data

Life Span of Data

Registers, peripheral memory, caches, etc.	nanoseconds
Main Memory	nanoseconds
Network state	milliseconds
Running processes	seconds
Disk	minutes
USBs, backup media, etc.	years
CD-ROMs, printouts, etc.	tens of years

The Forensic Method #1

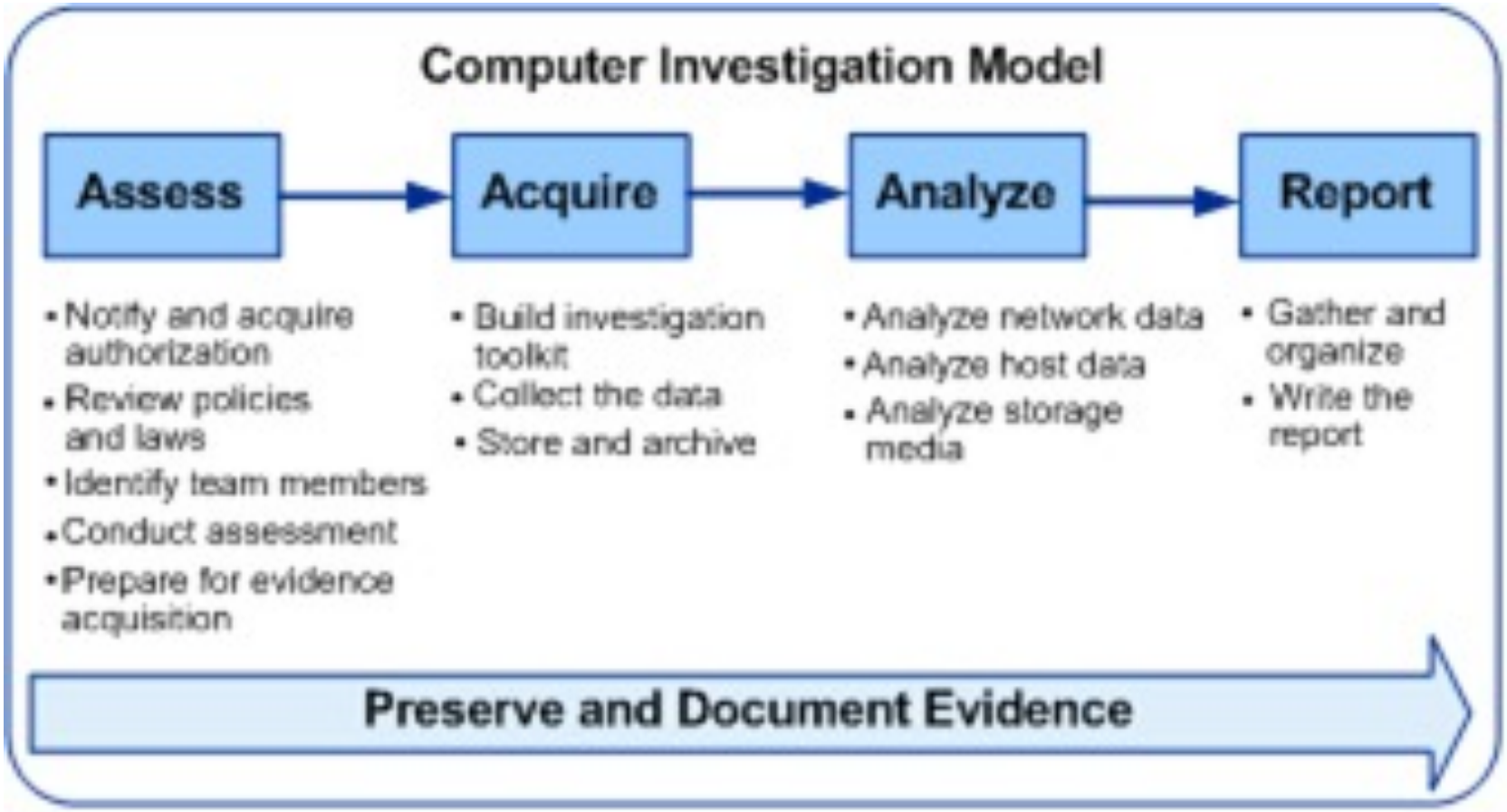
- Obtain Authority to search
  - this may be a Search Warrant
- Secure and isolate
  - locate removable media
  - secure mobile devices (Faraday Bag)
- Record the scene
  - document and photograph
- Conduct a systematic search for evidence
  - order of volatility

The Forensic Method #2

- Assess the risk of the suspect having the ability to hide or destroy evidence.
- Collect and package evidence
  - Maintain a chain of custody
- Analyse the evidence in a forensic lab
- Prepare a forensic report
- Submit the evidence as an expert witness
  - an expert is allowed to give an opinion to the court
- Be prepared to have your methods challenged

The Forensic Method

- Assess, Acquire, Analyse and Report



Incident Response

ACTION	EXPERTISE REQUIRED	TIME CONSUMED
Ignore the Incident	None	Almost none
Minimal effort	Installing system software	1/2 - 1 day
Minimum Recommended	Jr. System Administrator	1-2 days+
Serious effort	Senior Sys Admin	2+ days - weeks
Fanaticism	Expert Sys Admin	days - months+

An example Forensics Case

- The company suspects a policy violation has occurred.
- The suspect is suspected of conducting a private business using company resources while at work.
- The business involves setting up and maintaining special purpose websites for clients.
- The suspect's USB drive has been confiscated.
- Your task is to examine the USB to confirm or deny this allegation.

Objective

- To understand the field of Digital Forensics
- To learn the Principles of Digital Forensics

Forensics Principles

- The next few slides list some Forensic Principles
- Understanding these principles will help you perform a sound forensic investigation

Aims of Forensics

- To gather admissible evidence legally and without interfering with business processes;
- To gather evidence targeting the potential crimes and disputes that may adversely impact an organisation;
- To allow an investigation to proceed at a cost in proportion to the incident;
- To minimise interruption to the business from any investigation;
- To ensure that evidence makes a positive impact on the outcome of any legal action.

Corroboration

- While one example of class evidence is not compelling, several independent class examples together can build a compelling case.
- For example the threatening letter may have also been printed by an Epson printer and the suspect has an Epson printer

Forensic Soundness

- The methods used to obtain evidence must not alter the evidence
- For example the act of reading a disk file will alter the time of last access stored with the file
- Similarly the act of accessing memory will alter that memory
- Some minor alterations are inevitable and can be accepted by precedent
- The processes used to obtain evidence must be well documented to identify possible changes

Authentication

- Identifying the source of evidence
  - Human and digital device
  - One does not imply the other
- This can involve
  - Oral evidence (a suspect identifies his laptop)
  - Circumstantial evidence
  - Digital evidence (a private encryption key is compelling)

Attribution

- Liability is extended to a defendant who did not actually commit the criminal act.
- Asserting that the evidence found on a device can be attributed to one and only one person.
- Examples:
  - a web history file may contain web searches for axe murderer.
  - A wireshark packet capture may indicate visits to a child pornography website
  - A web server apache2 log may indicate visits from the suspect

Attribution 2

- We need to assert only the suspect did the deed.
- We rely on:
  - Authentication (logon passwords)
  - Dhcp logs for linking MAC addresses to ip addresses
  - Gateway router logs for linking public ip addresses to private ip addresses
  - Phone GPS tracking (google maps)
  - Syslog remote logging (and auth.log on Linux)
  - net user commands to find login timestamps
  - Linux last command for logon details

Objectivity

- Investigators should be free from bias when investigating
- Use of judgemental language may harm your soundness and your reputation

Repeatability

- The scientific method requires evidence to be able to be independently verified
- The second investigator will need to be able to follow your documentation
- In particular, the name and version of all tools used must be documented

Evidence Exchange

- Locard's Exchange Principle:
  - Contact between two items will result in an exchange
  - Between the suspect and the victim
  - Between the investigator and the crime scene
  - The exchange can be physical (fingerprints)
  - The exchange can be digital (an email)
  - In a computer intrusion, the attacker may leave evidence in disk space, log files and the Windows Registry
  - The act of sending an email may leave traces on the sender's hard disk, complete with time stamps

Evidence Integrity

- We need to confirm that the evidence has not been altered after collection
- Most evidence is kept as disk files so this is usually done by hashing the files to get a digital fingerprint when the evidence is collected
- Any copy of the evidence file used for forensics can be hashed again
- The hash of the copy should match the hash of the original

Forensic Acquisition

- Working on a disk may require minor alterations to its contents.
- You need to prove these alterations are minor.
- Best to work on a copy of the disk.
- The copy can be to another, similar disk
- Or the copy can be to an image file
- The image file can be raw or in a forensic container
- You can also acquire the contents of the device's RAM

Evidence Characteristics

- Evidence traces can have class characteristics or individual characteristics
- Class characteristics apply to many cases
  - For example a threatening letter was written in MS Word version 2007. A copy of Word 2007 was found on the suspect's laptop.
- Individual characteristics apply to one case
  - For example each copy of Photoshop embeds its serial number in every image produced.

Chain of Custody

- We need to ensure continuity of possession of evidence
- Each person handling evidence may be asked to testify that the evidence has not been altered while in their possession
- A Chain of Custody form is used to log when, where and why evidence was transferred
- The technique helps to minimise loss or contamination of evidence

Levels of Certainty

- C0- Evidence contradicts the known facts
  - Incorrect
- C1 - Evidence is highly questionable
  - Highly uncertain
- C2 - Only one source of evidence which is not protected against tampering
  - Somewhat uncertain
- C3 - Some tamper protection, some inconsistencies
  - Possible

Levels of Certainty #2

- C4 - Evidence is tamperproof or there are multiple independent sources of evidence that agree
  - Probable
- C5 - Tamperproof evidence from several independent sources that agree, some minor uncertainties (loss of data, timing uncertainties)
  - Almost certain
- C6 - Tamperproof evidence with a high statistical probability
  - Certain

Fin