Information Security
CS 3002

Dr. Haroon Mahmood

Assistant Professor

NUCES Lahore

Disclaimer: The contents of these slides have been taken from the book of CISSP: official study guide

Forensics

- Investigation that takes place after an incident has happened
- Try to answer questions: Who, what, when, where, why, and how
- Evidence might be required for a wide range of computer crimes and misuses
- Information collected assists in arrests, prosecution, termination of employment, and preventing future illegal activity
- Investigators must be careful to ensure that proper procedures are followed.
- Failure to abide by the correct procedures may violate the civil rights of those individual(s) being investigated and could result in a failed prosecution or even legal action against the investigator.

Investigation types

- **Administrative investigations:** internal investigations that examine either operational issues or a violation of the organization's policies. May transition to another type of investigation.

- **Root cause analysis:** determine the reason that something has occurred

- **Criminal investigations:** conducted by law enforcement agencies, related to alleged violation of criminal law. It must meet "beyond a reasonable doubt" standard which states there are no other logical conclusions.

Investigation types

- **Civil investigations:** do not involve law enforcement, but involves internal employees and outside consultants working for a legal team. Must meet the weaker "preponderance of the evidence" standard that demonstrates the outcome is more likely than not.

- **Regulatory investigations:** government agencies do these when they think there's been a violation of administrative law. Violations of industry standards!

Digital or Computer Crimes

- **An illegal activity or violation of law that involves a computer system.**

Types of Computer Crimes

- **Military and intelligence attacks: Purpose is to obtain restricted information from law enforcement or military and research sources**

- **Business attacks: focus on illegally obtaining confidential information aka corporate espionage or industrial espionage! Stealing trade secrets!**

- **Financial attacks: carried out to unlawfully obtain money or services ex: shoplifting, burglary**

Digital or Computer Crimes

- **Terrorist attacks:** to disrupt normal life and instill fear, as opposed to military or intelligence attack which is designed to extract secret information

- **Grudge attacks:** to do damage to an organization or person, usually out of resentment or to "get back at" an organization. Insider threat is big, these attacks can come from disgruntled employees.

- **Thrill attacks:** done for "the fun of it", usually by "script kiddies"

  May also be related to "hacktivism"

Digital forensics

- **Forensics process involves application of scientific methods and techniques to the investigation of a crime.**
- **Digital forensics involves the preservation, identification, extraction, documentation, and interpretation of digital media for evidentiary and/or root cause analysis.**

- **Multiple methods are required to**
  - **discover data on computer system**
  - **recover deleted, encrypted, or damaged file information**
  - **monitor live activity**
  - **detect violations of corporate policy**

SECURITY VS FORENSICS

Security	Forensics
Continuous process: Security is a service that provides defense 24 hours a day	**Time-restricted process**: after a crime is alleged to have occurred
Generalized: looks for any possible harmful behavior	**Case-centered:** reconstructs a given criminal scenario
Real-time response: implements different techniques in order to confront the threats during a live incident	**Post-mortem investigation**: identifies deficits after the incident occurred or while the system is inactive
Well-established computer science field	Young and evolving field with ever changing landscape

Media Analysis

- **Network analysis: when incidents take place over a network. Often difficult to reconstruct because networks are volatile, and depend on prior knowledge that an incident is underway or logs.**
  - **IDS and IPS system logs**
  - **Network flow data**
  - **Logs from firewall and other security devices**

- **Software analysis: reviews of applications or activity, or review of software code and log files to check for SQL injection, privilege escalation etc.**

- **Hardware/embedded device analysis: includes memory, storage systems, Smartphone, embedded computers**

Types of forensics

- **Live Forensic:** This category of forensics makes it possible to retrieve evidence from the RAM. The target location here is the primary memory which is used to extract data related to the registry, cookies etc. This procedure is specifically known as dumping of RAM.

- **Mobile Forensic:** With the rapid increase in use of mobiles, criminal cases targeting phones are getting common worldwide. Mobile forensics refers to the process of assessing, reading, extracting and recovering forensically relevant data from mobile phones.

Types of forensics

- **Desktop Forensic:** Desktop forensics deals with the acquisition of forensically significant data from secondary memory. It contributes in recovering the files that have been deleted.

- **Device forensics:** The focus of the device forensics is mainly collection of evidences from smart devices. Those devices may be home appliances, tag readers, smart phones, computer systems, smart watches or any other IoT devices. The digital evidence residing in these devices can be in the form of text, audio files, video or graphics retrieved from a CCTV camera.

Types of forensics

- **Network forensics:** The goal of network forensics is to analyse the networks through which the devices dispatch and collect data. These networks can be local area networks, personal networks, wide area networks and home networks.

- **Cloud forensics:** Often the devices are connected to the internet. The data and resources are stored in cloud. It can be accessed via cloud which is susceptible to great attacks. In a cloud infrastructure, data is available from various locations and sources. This makes the task of evidence acquisition difficult for the investigators.

Technical Issues

- **Data transfer or recovery**
- **Level of rights required for tasks**
- **Additional hardware/software familiarisation**
- **New skills for archives staff**
- **Redaction (**obscuring information for legal purposes**)**
- **Finding new software for particular tasks**

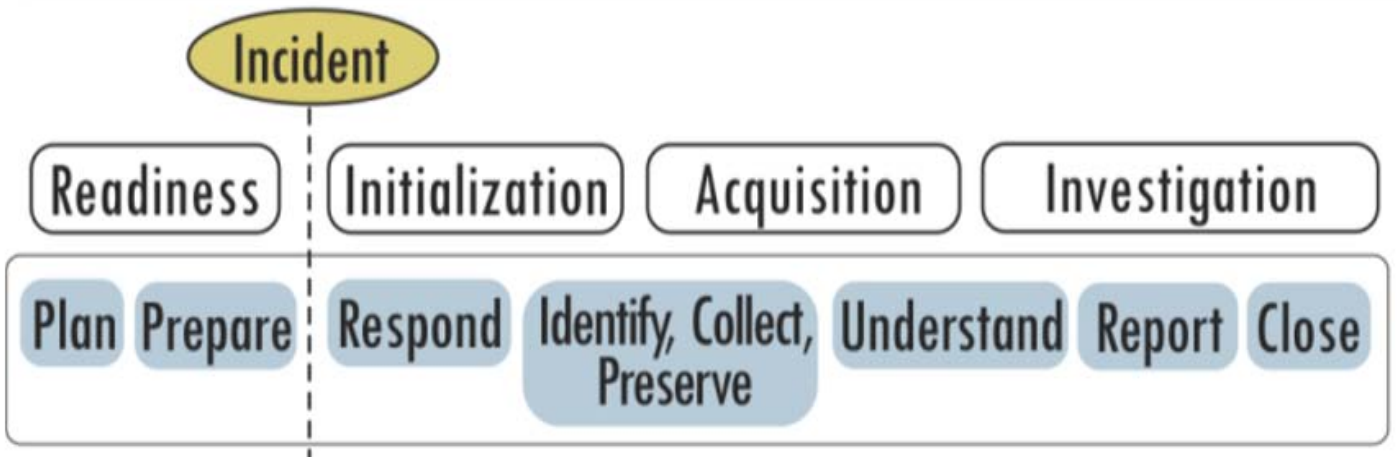
Process of digital forensics

- **Acquisition: Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices**
- **Identification: locates the information**
- **Preservation: protected against alteration or deletion**
- **Collection: gathers the responsive information centrally**
- **Processing: screens the collected information to exclude irrelevant information**
- **Review: determine what information is relevant to event**
- **Analysis: deeper inspection of the content**
- **Production: place info in a format that it may be shared**
- **Presentation: show info to witnesses, the court, other parties**

Evidence Collection and Forensic Procedures

- When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
- Actions taken to collect information should not change evidence.
- Person should be trained to access original digital evidence.
- All activity related to seizure, access, storage or transfer of digital evidence should be fully documented, preserved, and available for review.
- Individuals are responsible for all actions taken while the evidence is in their possession.

Forensic readiness



- **Forensic Readiness refers to the extent a device is ready for capturing and detecting any unwanted events**

- **It is a measure to maximize the forensic value of the potential evidence and minimize the amount of resources spent on the investigation**

Evidence Processing Guidelines

- New Technologies Inc. recommends following 16 steps in processing evidence
- Step 1: Shut down the computer
  - Considerations must be given to volatile information
  - Prevents remote access to machine and destruction of evidence (manual or ant-forensic software)
- Step 2: Document the Hardware Configuration of The System
  - Note everything about the computer configuration prior to re-locating

Evidence Processing Guidelines (cont)

- **Step 3: Transport the Computer System to A Secure Location**
  - **Do not leave the computer unattended unless it is locked in a secure location**
- **Step 4: Make Bit Stream Backups of Hard Disks**
- **Step 5: Mathematically Authenticate Data on All Storage Devices**
  - **Must be able to prove that you did not alter any of the evidence after the computer came into your possession**
- **Step 6: Document the System Date and Time**
- **Step 7: Make a List of Key Search Words**
- **Step 8: Evaluate the Windows Swap File**

Evidence Processing Guidelines (cont)

- **Step 9: Evaluate File Slack**
  - **File slack is a data storage area of which most computer users are unaware; a source of significant security leakage.**
- **Step 10: Evaluate Unallocated Space (Erased Files)**
- **Step 11: Search Files, File Slack and Unallocated Space for Key Words**
- **Step 12: Document File Names, Dates and Times**
- **Step 13: Identify File, Program and Storage Anomalies**
- **Step 14: Evaluate Program Functionality**
- **Step 15: Document Your Findings**
- **Step 16: Retain Copies of Software Used**

Tools utilized for forensics

- **ProDiscover Basic: The main service provided by ProDiscover is the evaluation of the hard disk data. It is widely used for creating legal procedural reports in court.**
- **Encase: Encase is one of the traditional tools for data analysis and recovery. It assists in reformation and assessment of evidences which have been attained from the forensic procedure.**
- **Autopsy: Autopsy is free to use software that works as the graphical interface for another set of tools termed as Sleuth Kit [53] [58]. Examination and recovery of evidential information from hard drive or mobile phone contents is possible using Autopsy [54]. It accepts data in the form of virtual machine images, disk images or raw images. Autopsy formulates reports from analyzed sets of data and files.**

Tools utilized for forensics

- **Magnet RAM:** Magnet RAM is capable of analyzing and extracting live traces from RAM. It provides compatibility with various versions of Windows [54]. It also enables recovery of data and significant files. It can sense and notify about presence of malware in memory.

- **X-ways Forensics:** It comes blended with some other beneficial forensic tools like Disk Imager, WinHex etc. [55]. It can recover passwords and perform decompression of files. It allows users to create their own hash sets.

Tools utilized for forensics

- **Forensic Toolkit:** Forensic Toolkit (FTK) is amongst the most widely used tools in the world. It is being used in court of law for various purposes. It is competent enough to analyze data in smart phones, computers, network channels and laptops [55]. It is faster than other forensic tools known. FTK is capable of identifying leaks, unusual activities and missing information. It can recover passwords and analyze emails as well. Users can execute its setup even through a USB drive.

Network forensics tools

- **Wireshark:** Wireshark is widely used in industries for assessing network traffic. It is regarded as the best tool for network analysis [54]. It helps in identifying the packets that pass through the network. It can also read and overwrite contents of a packet.

- **Nmap:** The basic service provided by Nmap is sensing ports in a network. Identifying the host source and enhancing security are some of its additional features. It captures host information and scans its details by traversing a parcel to the source.

Network forensics tools

- **Nessus:** This is one useful tool for scanning the network. It can detect any unusual activity taking place in a computer by scanning it. It is capable of entering any system which is linked with the network.

- **Snort:** It is an open source tool. It performs packet logging in a network along with detection of traffic.