Certified Hacking Forensics Investigator

Module #01 : Computer Forensics in Today's World

Eng. Mohammad Khreesha
Twitter: @banyrock
Facebook : http://www.fb.com/khreesha

Module Objectives

➔ **After Successfully completing this module, you will be able to :**

1. Define computer forensics and understand its objectives.
2. Understand and classify different types of cybercrimes.
3. Understand different challenges cybercrimes present to investigators.
4. Understand different types of Cybercrime investigations and general rules of forensics.
5. Understand role of evidence and recognize different types of digital evidence.
6. Examine the role of computer forensics and forensics readiness in incident response plan.
7. Understand need for forensics investigators and identify their roles and responsibilities.

Understanding Computer Forensics

Computer forensics refer to a set of methodological procedures and techniques that help identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment, whereby any evidence discovered is acceptable during a legal and/or administrative proceeding.

➔ **Objectives:**

1. To track and prosecute perpetrators of a Cybercrime.
2. To gather evidence of cybercrimes in a forensically sound manner.
3. To estimate the potential impact of a malicious activity on the victim and assess the intent of the perpetrator
4. To minimize the tangible and intangible losses to the organization.
5. To protect the organization from similar incidents in future.

Types of Cybercrimes

- **Cybercrime is defined as any illegal act involving a computing device, network, its systems, or its applications.**
- **Cybercrime can be categorized into two types based on the line of attack :**

Internal Attacks

Breach of Trust by disgruntled or unsatisfied employees within the organization.

- Examples:
  1. Espionage
  2. Theft of Intellectual Property.
  3. Manipulation of the records.
  4. Trojans horse attack.

External Attacks

Attackers hired either by internal or external entities to destroy the organization's reputation.

- Examples:
  1. SQL Injection
  2. Brute Force.
  3. Identity Theft.
  4. Phishing/Spoofing.
  5. Denial of Service.

Challenges Cybercrimes Present to investigators

- **Cybercrimes pose new challenges for investigators due to their :**

1. **Speed**: Advancement in technology has boosted the speed with which cybercrimes are committed, whereas investigators require authorization and warrants before starting legal procedure.
2. **Anonymity**: Cyber criminals ca easily hide their identity by masquerading as some other or by hiding their IP addressed using proxies.
3. **Volatile nature of evidence**: Most of the digital evidence ca be easily lost as it is in the form of volatile data such as logs, records, light pulses, radio signals or other means.
4. **Evidence Size and Complexity**: Diversity and distributed nature of digital devices results in increased size of evidence data and complexity.
5. **Anti Digital Forensics**: Attackers are increasingly using encryption and data hiding techniques to hide digital evidence.
6. **Limited legal understanding**: many victims are unaware of the law violated during the incident and fail to defend their claim.
7. **Global origin and difference in laws**: The perpetrators can initiate the crime from any part of the world, whereas the authorities have jurisdiction over domestic crimes only.

Cybercrime Investigation

1. The investigation of any crime involves the painstaking collection of clues and forensic evidence with an attention to detail.
2. It is inevitable that there will be at least one electronic device found during the investigation, be it a computer, cell phone, printer, or fax machine.
3. The electronic device found may be central to the investigation as it could contain valuable evidence for solving the case.
4. Therefore, the information contained in the device must be investigated in the proper manner in the order to be relied upon in a court of law.

- Types of Cybercrime investigation cases:
  1. Civil
  2. Criminal
  3. Administrative

- Processes such as collection of data, analysis, and presentation differ based on the type of case.

Civil vs Criminal Investigation

Civil cases are brought for violation of contracts and lawsuits where a guilty outcome generally results in monetary to the plaintiff, whereas criminal cases are generally brought by law enforcement agencies in response to a suspected violation of law where a guilty outcome may result in monetary damages, imprisonment, or both.

Civil Investigation

Breach of Trust by disgruntled or unsatisfied employees within the organization.

- Examples:
  1. Espionage
  2. Theft of Intellectual Property.
  3. Manipulation of the records.
  4. Trojans horse attack.

Criminal Investigation

- Investigators must follow a set of standard forensic processes accepted by law in the respective jurisdiction.
- Investigators, under court's warrant, have the authority to seize the computing devices.
- A formal investigation report is required.
- The law enforcement agencies are responsible for collecting and analyzing evidence.
- Punishments are harsh and include fine, jail sentence or both.
- Standard of proof needs to be very high.
- Difficult to capture certain evidence, e.g., GPS device evidence

Administrative Investigation

- Administrative Cases refers to an internal investigation by an organization to discover if its employees, clients and partners are abiding by the rules or policies. Violation of company policies.
- Involves an agency or government performing inquiries to identify facts with reference to its own management and performance
- Non-criminal in nature and related to misconduct or activities of an employee that includes but are not limited to:
  1. Violation of organization's policies, rules, or protocols. Resource misuse or damage or theft
  2. Threatening or violent behavior. Sexual Exploitation, harassment and abuse
  3. Improper promotion or pay raise, corruption and bribery

Rules of Forensics Investigation

1. Limit access and examination of the original evidence
2. Record changes made to the evidence files
3. Create a chain of custody document
4. Set standards for investigating the evidence
5. Comply with the standards
6. Hire professionals for analysis of evidence
7. Evidence should be strictly related to the incident
8. The evidence should comply with the jurisdiction standards
9. Document the procedures applied on the evidence
10. Securely store the evidence
11. Use recognized tools for analysis

Enterprise Theory of Investigation (ETI)

- The Enterprise Theory of Investigation (ETI) has become the standard investigation model used by the FBI when conducting investigations against major criminal organizations.
- Rather than viewing criminal acts as isolated crimes, the ETI attempts to show that individuals commit crimes in furtherance of the criminal enterprise itself; in other words, individuals commit criminal acts solely to benefit their criminal enterprise.
- By applying the ETI with favorable state and federal legislation, law enforcement can target and dismantle entire criminal enterprises in one criminal indictment.

Understanding Digital Evidence

- Digital evidence includes all such information that is either stored or transmitted in digital form and has probative value.
- Investigators should take utmost care while gathering digital evidence as it is fragile in nature.
- According to Locard's Exchange Principle, “anyone or anything, entering a crime scene takes something of the scene, and leaves something of themselves behind.”

Types of Digital Evidence

- **Volatile Data** - Volatile data refers to the temporary information on a digital device that requires a constant power supply and is deleted if the power supply is interrupted. Important volatile data includes system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, command history, etc.
- **Non-volatile Data** - Non-volatile data refers to the permanent data stored on secondary storage devices, such as hard disks and memory cards. Information stored in non-volatile form includes hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, registry settings, and event logs.

Characteristics of Evidence

- **Admissible Evidence** - Evidence is relevant to the case, act in support of the client presenting it, and be well communicated and non-prejudiced.
- **Authentic Evidence** - The investigators must provide supporting documents regarding the authenticity, accuracy, and integrity of the evidence with details such as source and its relevance to the case. If necessary, they must also furnish details such as author of the evidence or path of transmission.
- **Complete Evidence** - The evidence must either prove or disprove the consensual fact in the litigation
- **Reliable Evidence** – The evidence must be proven to be dependable by maintaining a record of the tasks performed while the evidence was extracted and handled. Forensic investigation is conducted only on the copies of evidence.
- **Believable Evidence** – The evidence must be presented in a clear manner and expert opinions must be obtained where necessary

Rules of Evidence

- Evidence that is to be presented to the court must comply with the established rules of evidence.
- Prior to the investigation process, it is important that the investigator understands the rules of evidence.

Best Evidence rule is established to prevent any alteration of digital evidence either intentionally or unintentionally.

- It states that the court only allows the original evidence of a document, photograph or recording at the trial rather than a copy, but duplicate will be allowed as an evidence under the following conditions:
  - Original evidence destroyed due to fire/flood.
  - Original evidence destroyed in the normal course of business.
  - original evidence is possession of third party.

Scientific Working Group on Digital Evidence (SWGDE)

Principle - To ensure that digital evidence is collected, preserved, examined, or transferred in a manner that safeguards the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective system for quality control.

- **Standards and Criteria :**

1. All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document.
2. Agency management. must review SOPs on an annual basis to ensure their continued suitability and effectiveness.
3. SOPs must be generally accepted or supported by data gathered and recorded in a scientific manner.
4. The agency must maintain written copies of the appropriate technical procedures.
5. The agency must use hardware and software that is appropriate and effective for the seizure/examination procedure.
6. All activities related to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing and be available for review and testimony.

Forensics Readiness

Forensic Readiness refers to an organization's ability to make optimal use of digital evidence in a limited period and with minimal investigation costs. It includes technical and nontechnical actions that maximize an organization's competence to use digital evidence.

- **Benefits:**

1. Fast and efficient investigation with minimal disruption to the business.
2. Provides security from cybercrimes such as intellectual property theft, fraud, or extortion.
3. Offers structured storage of evidence that reduces expense and time of an investigation.
4. Improves law enforcement interface.
5. Easy identification of evidence related to the potential crimes.
6. Helps organization use the digital evidence in its own defense
7. Blocks the attackers from covering their tracks.
8. Averts similar attacks in the future.

Forensics Readiness Planning

Forensics readiness planning refers to a set of processes required to achieve and maintain forensics readiness.

- Identify the potential evidence required for an incident.
- Determine the source of the evidence.
- Define a policy that determines the pathway to legally extract electronic evidence with minimal disruption
- Establish a policy for securely handling and storing the collected evidence.
- Identify if the incident requires full or formal investigation.
- Train the staff to handle the incident and preserve the evidence.
- Create a special process for documenting the procedure.
- Establish a legal advisory board to guide the investigation process.

Need for Forensics Investigator

- **A forensic investigator performs the following tasks:**
  - Evaluates the damages of a security breach
  - Identifies and recovers data required for investigation
  - Extracts the evidence in a forensically sound manner
  - Ensures proper handling of the evidence
  - Acts as a guide to the investigation team
  - Creates reports and documents about the investigation required to present in a court of law
  - Reconstructs the damaged storage devices and uncovers the information hidden on the computer
  - Updates the organization about various methods of attack and data recovery techniques, and maintains a record of them (following a variant of methods to document) regularly
  - Addresses the issue in a court of law and attempts to win the case by testifying in court
  - Fourth Amendment states that government agents may not search or seize areas or things in which a person has a reasonable expectation of privacy, without a search warrant.
  - Note: Private intrusions not acting in the color of governmental authority do not come under the Fourth Amendment.

Follow us :

- https://www.fb.com/technawidotcom
- https://www.twitter.com/technawidotnet
- http://www.technawi.net

تكناوي
technawi.net