The Roadmap for Cyber Crime Investigation

Natasha Singh ¹, Sona Rani ²
¹M.Tech. Scholar, ²Asstt. Prof.
CSE Department, UIET, KUK
natasha3699@gmail.com

Abstract: As threats against digital assets have risen and there is necessitate exposing and eliminating hidden risks and threats. The ability of exposing is called “cyber forensics.” Cyber Penetrators have adopted more sophisticated tools and tactics that endanger the operations of the global phenomena. These attackers are also using anti-forensic techniques to hide evidence of a cyber crime. This paper is intended to raise awareness of the different types of computer forensics systems and to identify crucial questions for corporate planning in support of cyber forensics. Various kinds of forensic systems like Internet security system, Intrusion detection systems, Firewall security systems, Storage area network security systems, Network disaster recovery systems, Public key infrastructure security systems are explained in this paper.

Keywords: Intrusion detection systems, Network disaster recovery system, Forensics

I. Introduction to Cyber Forensics

As Internet technologies proliferate into everyday life, we come close to realizing new and existing online opportunities. One such opportunity is in Cyber forensics, unique process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally accepted. It is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. In other words, cyber forensics is the collection, preservation, analysis, and presentation.

II. Steps of Cyber Forensics

Identification

Seizure

Authentication

Acquisition

Analysis

Presentation

Preservation

Fig 1 Cyber forensic steps

1) Identification: The identification phase is the process of identifying evidence material and its probable location. This phase is unlike a traditional crime scene it processes the incident scene and documents every step of the way. Evidence should be handled properly.
The Roadmap for Cyber Crime Investigation

2) Seizure: Seizure is the process of capturing the suspect computer for purpose of evidence collection. There is a need for systematic procedure to avoid loss of digital evidence.

3) Authentication: Authentication involves the validation of the seized and acquired evidence. Hashing procedure in this method is being employed. Different hashing algorithms can be applied like SHA,MD5.

4) Acquisition: In this process possession is obtained of suspect computer physically or remotely. Bitwise copy of the digital evidence is created and stored in hard disk.
5) Analysis: Forensic analysis is the process of understanding, re-creating, and analyzing arbitrary events that have gathered from digital sources. The analysis phase collects the acquired data and examines it to find the pieces of evidences. This phase also identifies that the system was tampered or not to avoid identification.

6) Presentation: This step involves presenting the evidence in court of law in such a manner which is understood by lawyers, non-technically staff/management and is being accepted by them.

7) Preservation: The final step involves preservation of the evidence. In this step we prevent people from using the digital device or evidence and thus prevent its tampering.

III. Cyber Forensic Classifications

a) Disk Forensics: Disk forensics is science that extracts forensic information from hard disk, Removable storage devices, floppies and other storage media. It is helpful in collecting evidence from storage media.

b) Network Forensics: Network Forensics is mainly aimed at monitoring and analyzing computer network traffic for the purpose of gathering information and legal evidence from network.

c) Digital Device forensics: Digital Device forensics is a division of digital forensics that recovers digital evidences from a digital device such as a mobile phone or any device that can store and process information.

IV. Types of Forensic Systems

Forensic systems like Internet security systems, Intrusion detection systems, Firewall security systems, Storage area network security systems, Network disaster recovery systems, Public key infrastructure security systems, Wireless network security systems are used by investigators to solve cyber crimes and produce digital evidence that is acceptable in court of law. There are following types of cyber forensic systems:

- Internet security systems
- Intrusion detection systems
- Firewall security systems
- Storage area network security systems
- Biometric security systems
The Roadmap for Cyber Crime Investigation

1) **Internet security systems:** The first step in defining a corporate Internet security policy is to draft a high-level management policy statement establishing a framework and context for security within an organization. This policy needs to define the adequate and appropriate Internet security measures necessary to safeguard a company’s systems, networks, transactions, and data.

2) **Intrusion detection systems:** An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. An IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system outsourced basis.

3) **Firewall Security System:**

![Firewall security system](image)

A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network’s firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter) network, such as the Internet, that is not assumed to be secure and trusted.

4) **Network security systems:** Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

![Network Security System](image)

5) **Biometric security systems:** Biometric security (identification) systems identify a human from a measurement of a physical characteristic or behavioral trait (for example, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and handwritten signature) to determine or verify an
identity. There is typically an enrollment process in which the biological information is taken and stored in a database for future identification or verification purposes. There are several different types of biometric security technologies:

a) **Facial Recognition** technology identifies individuals by analyzing certain facial characteristics such as the distance between the eyes, the length of the nose, and the angle of the jaw. Facial recognition works for both verification and identification and is often used for surveillance purposes.

b) **Fingerprint Recognition** is the most widely used method of biometric authentication. Fingerprint recognition is based on features found in the impressions made by unique ridges and valleys on the surface of a human's fingertips.

c) **Iris Recognition** is the process of recognizing a person by analyzing the distinctly colored ring that surrounds the pupil of the eye.

d) **Voice Recognition** technology is a biometric security technology used to uniquely identify individuals based on the different characteristics in their voice such as tone, pitch, cadence, etc.

V. Conclusion

Cyber forensics uses various types of forensic technologies like intrusion detection system, firewall system and network security system in order to find digital evidences and produce them in court of law in such a manner that it is legally accepted.

References


The Roadmap for Cyber Crime Investigation
