Cyber Forensics in the New Age of Cyber Security

Soham Das

MAKAUT

14th September 2023

Profile

Hi , Friends I am Soham , i am Cyber Security Researcher. My qualification MS Information Technology in Cyber Security from Maulana Abul Kalam Azad University of Technology, West Bengal.

Disclaimer

Warning: This lecture will not make you a certified digital forensics technician. This lexture is designed to provide an introduction to this field from both a theoretical and practical perspective.Digital forensics is a maturing scientific field with many sub-disciplines.

Introduction

Cyber Forensics is the systematic collection, analysis, and preservation of digital evidence for legal purposes. In the new age of cyber security, it plays a crucial role in uncovering cybercrimes and strengthening cybersecurity measures. With the increasing complexity of cyber threats, cyber forensics is more essential than ever. For instance, consider a case where a company's sensitive customer data is breached. Cyber forensics can help trace the attack, identify the culprits, and prevent future incidents.

The Evolution of Cybersecurity

Cybersecurity has evolved significantly, from basic antivirus software to advanced threat detection systems. For example, early antivirus programs only scanned for known malware, whereas modern systems use machine learning algorithms to identify new threats in real-time.

The Need for Cyber Forensics

In the modern age, the need for cyber forensics is paramount due to the surge in cybercrime. Consider the rise of ransomware attacks, where cybercriminals encrypt victim's data and demand a ransom. Cyber forensics can help victims recover their data and track down the perpetrators.

Key Components of Cyber Forensics

Cyber forensics consists of digital evidence, forensic tools, and forensic procedures. Digital evidence can include logs, network traffic, and emails, all of which are vital for investigations. Forensic tools like EnCase and Autopsy aid in analyzing this evidence, while forensic procedures ensure proper handling and documentation.

Digital Evidence

Digital evidence, such as metadata in files or timestamps in logs, can provide critical clues in investigations. For instance, analyzing the metadata of a document can reveal who created it and when.

Forensic Tools - Slide 1

Tools like Wireshark, which captures network traffic, or FTK (Forensic Toolkit), which assists in analyzing hard drives, are instrumental in cyber forensic investigations.

Forensic Tools - Slide 2

1. **EnCase**: EnCase is a widely used commercial forensic tool known for its robust capabilities in acquiring, analyzing, and reporting on digital evidence. It is favored by law enforcement and cybersecurity professionals.
2. **AccessData Forensic Toolkit (FTK)**: FTK is a comprehensive digital forensics platform used for analyzing and processing digital evidence, including hard drives, mobile devices, and network data.
3. **Autopsy**: An open-source digital forensics platform that offers a range of features for analyzing disk images, smartphones, and other sources of digital evidence. It has a user-friendly interface and is commonly used in both law enforcement and corporate investigations.

Forensic Tools - Slide 3

4. **Sleuth Kit**: Also open-source, Sleuth Kit is a collection of command-line-based forensic tools for analyzing disk images and file systems. It is often used in conjunction with Autopsy.
5. **X-Ways Forensics**: A comprehensive commercial forensic tool used for data carving, analysis, and reporting. It offers advanced features for examining file systems and artifacts.
6. **Volatility**: An open-source memory forensics framework used for analyzing volatile memory (RAM). It helps in the identification of running processes, network connections, and other artifacts that can be crucial in cyber investigations.

Forensic Tools - Slide 4

7. **Wireshark**: Although primarily a network protocol analyzer, Wireshark is valuable for capturing and analyzing network traffic, making it a useful tool for cyber forensics when investigating network-related incidents.
8. **Cellebrite UFED**: This tool is focused on mobile device forensics, supporting the extraction and analysis of data from a wide range of smartphones and tablets.
9. **OpenVAS**: Open Vulnerability Assessment System (OpenVAS) is an open-source vulnerability scanner used to identify and assess security vulnerabilities in networks and systems, which is crucial in forensic analysis.

Forensic Tools - Slide 5

10. **RegRipper**: An open-source tool for parsing and analyzing Windows Registry data. It helps investigators gather information about system configuration, user activity, and more.
11. **OSForensics**: OSForensics is a commercial forensic tool that covers a wide range of digital forensic tasks, from data recovery to password cracking.
12. **FTimes**: FTimes is a lightweight open-source tool used for gathering and comparing file attributes across different points in time, helping to detect file tampering or unusual changes.

Forensic Tools - Slide 6

13. **Bulk Extractor**: This open-source tool specializes in extracting and analyzing digital artifacts from various data sources, such as disk images and memory dumps.
14. **Log2Timeline**: An open-source tool for timeline analysis of system events, helping investigators create a chronological view of system activity.
15. **Paladin Forensic Suite**: A live forensic system that provides a comprehensive set of tools and utilities for conducting digital investigations.

Forensic Procedures

Following proper forensic procedures, like maintaining the chain of custody, ensures that evidence is admissible in court. For instance, if evidence is mishandled, it may be deemed unreliable in legal proceedings.

Challenges in Cyber Forensics

Challenges include encryption, where data is scrambled and inaccessible without decryption keys. A notable example is the FBI's battle with Apple to unlock the iPhone of a suspect involved in the San Bernardino terrorist attack.

Cybercrime Trends

Ransomware attacks, like the Colonial Pipeline attack in 2021, highlight current trends. These attacks demand large ransoms to decrypt systems, making them lucrative for cybercriminals.

Legal and Ethical Considerations

Adhering to legal and ethical standards is crucial. An example is the General Data Protection Regulation (GDPR) in Europe, which mandates strict data protection and privacy regulations.

Case Study 1: Financial Data Breach

The Equifax data breach in 2017 exposed the personal information of 147 million people. Cyber forensics helped trace the breach to a software vulnerability, leading to legal action against the responsible parties.

Case Study 2: Insider Threat Investigation

In the case of Edward Snowden, a former NSA contractor, cyber forensics was used to investigate the theft and disclosure of classified documents.

Emerging Technologies

Emerging technologies like quantum computing pose new challenges. Quantum computers could potentially break encryption algorithms, requiring the development of quantum-resistant encryption methods.

Future Trends

Future trends include the growth of IoT and its impact on cyber forensics. For instance, IoT forensics will be necessary to investigate crimes involving connected devices.

Best Practices

Best practices involve continuous training, certification, and staying updated with the latest forensic techniques to ensure the effectiveness of cyber forensics in an ever-changing landscape.

Autopsy (Practical)

AUTOPSY
DIGITAL FORENSICS

Conclusion

In conclusion, cyber forensics is the linchpin of modern cybersecurity. Its ability to investigate cybercrimes, recover data, and prevent future attacks makes it indispensable in the new age of cyber security.

Contact Information

Soham Das,BCA,MS in Cyber Security(MAKAUT)
Ph/Whatsapp- (+91) 6289071973
E-mail- juhinsohamdas@gamil.com
Linkedin- https://www.linkedin.com/in/soham-das-2ab73212b
Github-https://github.com/sohamjuhin
Website:-https://sohamjuhin.github.io/SohamJuhinDas.github.io/

QA and Thank You

QA and Thank You