Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 23 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Digital Forensics: Techniques and Tools for Cybercrime Investigations

By Madhav Vedpathak & Aarti Kashid

Abstract- Digital forensics is a crucial aspect of modern-day investigations, particularly those involving cyber crimes. With the increasing prevalence of digital devices, the amount of electronic evidence available for investigation has also grown significantly. Therefore, it is essential to have the necessary techniques and tools to extract and analyse digital evidence accurately and efficiently. This paper aims to provide an overview of digital forensics and highlight some of the most popular techniques and tools used in the field.

Keywords: *digital evidence, cybercrime, computer crimes, electronic fraud, recovery and preservation of electronic data, analysis of electronic data, disk imaging, file carving, network forensics, memory analysis, mobile forensics, digital forensics tools, en case, forensic toolkit (FTK), sleuth kit, encryption, anti-forensic techniques, cloud-based storage.*

GJCST-E Classification: *LCC Code: HV8079.2-8109.5*

Strictly as per the compliance and regulations of:

Digital Forensics: Techniques and Tools for Cybercrime Investigations

Madhav Vedpathak [α] & Aarti Kashid [σ]

Abstract- **Digital forensics is a crucial aspect of modern-day investigations, particularly those involving cyber crimes. With the increasing prevalence of digital devices, the amount of electronic evidence available for investigation has also grown significantly. Therefore, it is essential to have the necessary techniques and tools to extract and analyse digital evidence accurately and efficiently. This paper aims to provide an overview of digital forensics and highlight some of the most popular techniques and tools used in the field.**

Keywords: digital evidence, cybercrime, computer crimes, electronic fraud, recovery and preservation of electronic data, analysis of electronic data, disk imaging, file carving, network forensics, memory analysis, mobile forensics, digital forensics tools, en case, forensic toolkit (FTK), sleuth kit, encryption, anti-forensic techniques, cloud-based storage.

I. Introduction

Digital forensics is a branch of forensic science that involves the recovery, preservation, and analysis of electronic data. Digital forensics is essential in investigating cybercrimes, computer crimes, and electronic fraud. With the widespread use of digital devices in everyday life, digital forensics has become an essential tool for law enforcement agencies, corporations, and government agencies. The objective of this paper is to provide a comprehensive overview of digital forensics, including its history, techniques, tools, and challenges.

II. History of Digital Forensics

The history of digital forensics can be traced back to the 1970s when computer forensics began. In the early days of computer forensics, the focus was on recovering data from computer hard drives. However, with the advent of the internet and the proliferation of digital devices, digital forensics has expanded to include the recovery and analysis of data from a wide range of devices, including smartphones, tablets, and cloud-based storage.

III. Digital Forensics Objectives

The primary objective of digital forensics is the identification, preservation, extraction, interpretation, and documentation of electronic evidence. Digital forensics is typically used to support criminal investigations, litigation, and other legal proceedings. However, digital forensics is also used in non-criminal cases, such as data breach investigations, corporate investigations, and employee misconduct investigations.

IV. Digital Forensics Techniques

Digital forensics employs a wide range of techniques to extract and analyze electronic evidence. The Disk Imaging: Disk imaging is the process of creating a bit-by-bit copy of a digital device's hard drive. The purpose of disk imaging is to preserve the integrity of the data and prevent any changes to the original data. Disk imaging is essential in any digital forensic investigation, as it provides a reliable and accurate copy of the original data.

1. *File Carving:* File carving is the process of extracting deleted files from a digital device. This technique involves searching for deleted files based on specific file signatures and recovering them. File carving is essential in cases where files have been intentionally or unintentionally deleted, as it allows investigators to recover valuable evidence.
2. *Network Forensics:* Network forensics involves the analysis of network traffic to identify and gather evidence related to cybercrime the capture and analysis of network packets to identify the source and destination of data, the type of data transmitted, and any anomalies in the traffic. Network forensics is used in cases such as data breaches, network intrusions, and malware attacks.
3. *Memory Analysis:* Memory analysis is the process of analyzing a digital device's volatile memory to identify and gather evidence related to cybercrime. Volatile memory includes data stored in RAM, which is lost when a device is turned off or restarted. Memory analysis involves capturing the memory image of a running system and analyzing it to identify running processes, network connections, and any malicious code present in the memory.
4. *Mobile Forensics:* Mobile forensics involves the recovery and analysis of data from mobile devices, such as smartphones and tablets. Mobile forensics includes techniques such as logical and physical extraction, file carving, and analysis of app data, call logs, and messaging data. Mobile forensics is

Author α σ: Guide: Prof. Salunkhe A. A (HOD of Computer Department) Rajgad Dnyanpeeth Technical Campus Polytechnic, Gat No. 237, Pune Bangalore Highway, Dhangawadi, Tal. Bhor, Dist - Pune.
e-mail: themadhavvedpathak@gmail.com

such as smartphones and tablets. Mobile forensics includes techniques such as logical and physical extraction, file carving, and analysis of app data, call logs, and messaging data. Mobile forensics is essential in cases where mobile devices are involved in criminal activities, such as drug trafficking, terrorism, and child exploitation.

V. Digital Forensics Tools

Digital forensics tools are software applications that are used to assist in digital forensic investigations. Digital forensics tools are designed to assist in disk imaging, file carving, network analysis, and memory analysis. Some of the commonly used digital forensics tools include:

1. *EnCase:* EnCase is a commercial digital forensic tool that is used for disk imaging, file carving, and memory analysis. EnCase has a user-friendly interface and provides a wide range of features for digital forensic investigations.
2. *Forensic Toolkit (FTK):* FTK is a commercial digital forensic tool that is used for disk imaging, file carving, and mobile forensics. FTK provides advanced search and analysis capabilities and is widely used in law enforcement agencies and government agencies.
3. *Sleuth Kit:* Sleuth Kit is an open-source digital forensic tool that is used for disk imaging and file carving. Sleuth Kit provides a command-line interface and can be used on a wide range of operating systems.

VI. Challenges in Digital Forensics

Digital forensics faces several challenges, including the following:

1. *Encryption:* Encryption makes it challenging to extract and analyze electronic evidence. Encryption is commonly used to protect data, and without the proper decryption keys, investigators cannot access the data.
2. *Anti-Forensic Techniques:* Anti-forensic techniques are used to hide or destroy electronic evidence. Anti-forensic techniques include file wiping, encryption, and data hiding.
3. *Complexity:* Digital devices are becoming increasingly complex, making it challenging to extract and analyze electronic evidence. The use of cloud-based storage, virtual machines, and encrypted communication channels makes it difficult for investigators to gather electronic evidence.

VII. Conclusion

Digital forensics is an essential tool for investigating cybercrime, computer crimes, and electronic fraud. Digital forensics techniques, tools, and challenges are constantly evolving, and investigators need to stay up to date with the latest developments to conduct effective digital forensic investigations. Digital forensics is critical in maintaining the integrity of digital data and ensuring that justice is served in criminal and civil cases. digital data and ensuring that justice is served in criminal and civil cases.

References Références Referencias

1. Casey, E., & Carrier, B. (Eds.). (2014). Handbook of digital forensics and investigation. Academic Press.
2. Nelson, B., Phillips, A., & Steuart, C. (2018). Guide to computer forensics and investigations. Cengage Learning.
3. "Computer Forensics: Investigating Data and Image Files" by EC-Council.
4. "Challenges in Digital Forensic Investigations of Cybercrime in India" by Geeta Sharma and B. B. Gupta.