International Journal of Life Sciences, Biotechnology and Pharma Research Vol. 13, No. 6, June 2024 Online ISSN: 2250-3137
Print ISSN: 2977-0122

DOI: 10.69605/ijlbpr_13.6.2024.80

REVIEW ARTICLE

The Role and Importance of Digital Forensics and Digital Evidence in Cyber Crime Detection

Jaydevsinh B. Vala[1], Vipul M. Vekariya[2]

[1]Research Scholar, Gujarat Technological University, Ahmedabad, Gujarat, India
[2]Dean and Principal, FET, Parul University, Vadodara, Gujarat, India

Corresponding Author
Vipul M. Vekariya
Dean and Principal, FET, Parul University, Vadodara, Gujarat, India
Email: vekariya.vipul@gmail.com

Received: 04 May, 2024 Accepted: 10 June, 2024

ABSTRACT
Digital forensics has emerged as a critical field in the modern criminal justice system, evolving from its early focus on standalone and networked computers to encompass a wide array of digital devices. This paper explores the multifaceted role of digital forensics in investigating both cyber and traditional crimes. As technology has advanced, the scope of digital forensics has expanded, enabling the recovery and analysis of evidence from devices such as mobile phones, GPS systems, and car engine management systems. These advancements have allowed investigators to uncover detailed insights into suspects' movements and activities, which were previously inaccessible.This paper provides a comprehensive overview of the various branches of digital forensics, including network forensics, disk forensics, mobile device forensics, database forensics, printer forensics, digital music device forensics, scanner forensics, multimedia forensics, and memory forensics. Each branch focuses on a specific type of digital evidence, employing specialized techniques to collect, preserve, and analyze data.The literature review highlights the evolution of digital forensic practices, noting significant studies and advancements in the field. It underscores the growing recognition of the importance of digital evidence in criminal investigations and the ongoing need for updated tools and techniques to address the expanding range of digital devices.The paper also discusses the reasons for conducting digital forensic investigations, emphasizing their critical role in incident response, remediation activities, and tracking advanced persistent threats. The discussion extends to the emerging challenges in digital forensics, including the proliferation of digital devices and the increasing complexity of digital environments.By examining the standard operating procedures (SOP) for digital forensic investigations, this paper outlines the systematic approach required to ensure the integrity and reliability of digital evidence. It concludes with an exploration of the significant role digital forensics will continue to play in the criminal justice system, advocating for continuous advancements in forensic techniques and tools to keep pace with technological developments.

Keywords: Digital Forensics, Digital Evidence, Cyber Crime Detection

INTRODUCTION

In its infancy, digital forensics primarily targeted standalone and networked computer systems. However, as technology has progressed, the scope of digital forensics has broadened to encompass the extraction of evidence from any device equipped with a digital processor or storage capacity. This has led to the evolution of digital forensics from solely focusing on computer-based crimes, such as hacking, to investigating a wide array of criminal activities.

Technological advancements have significantly expanded the types of evidence that can be recovered. Investigators can now extract data from various sources, including car engine management systems, satellite navigation systems, and mobile phones. This data includes not only documents, images, and records of network activity but also detailed information about an individual's movements and behaviours.

Investigators of traditional crimes, such as murder, theft, extortion, and drug trafficking, are increasingly relying on digital evidence to track suspects' activities. Historically, many investigators did not fully appreciate the potential value of digital evidence and often overlooked it. However, this perspective is shifting. There is a growing acknowledgment of the importance of digital evidence in traditional crime investigations, prompting efforts to allocate the necessary resources to address this need.This paper provides an overview of the various branches of cybercrime scene investigation, the techniques used,

DOI: 10.69605/ijlbpr_13.6.2024.80

and the types of evidence encountered. Digital forensics, which involves the detection, extraction, and analysis of evidence from digital media, is a crucial component in cyberspace investigations. One of the primary goals of digital forensics is to produce reports that are admissible in court. Key aspects of digital forensics include hard disk, memory, and network forensics, each playing a crucial role in recording and analyzing the activities of cybercriminals.

LITERATURE REVIEW

Early evaluations of crimes involving digital evidence did not always specifically target digital crime investigations. Instead, they often considered the broader role of digital forensics in general criminal investigations.

With technological progress, the use of digital devices in government, business, academia, and personal lives has transformed. The potential value of these advanced devices has been recognized and adopted by both criminals and investigators. There has been a continuous demand for updated tools, methods, and techniques for digital forensic investigations to address the growing variety of devices with digital processors or storage media, as well as to manage the complex environments in which they are used.

A significant study by Rahul Bhaskar (2006), conducted between 2004 and 2010, examined the response to the devastation caused by Hurricane Katrina. Bhaskar compared the inadequate federal, state, and local government response to the potential impact of a digital disaster of similar magnitude. The study found that only a small number of law enforcement personnel had a basic understanding of computer forensics. Additionally, individual organizations struggled to respond to incidents due to the limited knowledge of computer forensics among law enforcement and legal personnel, such as prosecuting attorneys (Bhaskar, 2006). Bhaskar identified the key elements of computer forensics as identification, preservation, analysis, and presentation. He noted that the inconsistent execution of these tasks across agencies created uncertainty about the ability to ensure that digital evidence would withstand legal scrutiny (Bhaskar, 2006).

Research from 2014 to 2019 has explored various aspects of digital forensics, including the different types of digital devices, the evidence they contain, and the methods for collecting and analyzing digital evidence. This body of work has also examined the tools and technologies used in digital forensics, contributing to the ongoing development and refinement of forensic practices in the digital realm.

REASONS FOR CONDUCTING A DIGITAL FORENSIC INVESTIGATION

Over the past decade, technological advancements have significantly benefited both individuals and businesses. However, these advancements have also equipped fraudsters and cybercriminals with sophisticated tools and methods to steal money and sensitive data while avoiding detection.

Hackers exploit advanced technologies to hide their illegal activities and transfer assets across multiple jurisdictions and globally. Their operations are intricate and well-resourced, making them difficult to detect using traditional investigative methods. Consequently, professionals responsible for investigating cybercrimes must continually update their skills and knowledge to stay abreast of these evolving threats. This has led to the emergence of specialized digital forensic professionals.

Digital forensic experts utilize a variety of tools and techniques to investigate and analyze cybercrimes. These tools offer deep insights into attack patterns, the operational methods of criminal groups, their motivations, and the new tactics and tools they employ. For instance, digital forensics enables investigators to understand how cybercriminals exploit software vulnerabilities, deploy malware, or execute phishing attacks. The evidence gathered through digital forensics is critical for building comprehensive knowledge bases, best practice resources, and threat intelligence databases, which are essential for predicting and preventing future attacks.

Moreover, the evidence collected from digital forensic analysis is crucial for incident response (IR) and remediation efforts once a breach is detected. Digital forensics enables organizations to gather data on new attack vectors, sophisticated types of malware, and other emerging threats that may not have been previously encountered. This information is vital for developing effective strategies to mitigate these threats and enhance the organization's cybersecurity defenses.

Digital forensics is particularly valuable in tracking advanced persistent threats (APTs), which are long-term, targeted cyberattacks aimed at stealing information or disrupting operations. APTs employ a range of tactics and tools to achieve their objectives, often remaining undetected on a victim's network for extended periods while conducting surveillance and data exfiltration. Digital forensic investigations help trace these attacks, identify the perpetrators, uncover their methods, and understand their motivations. This information is essential for developing targeted defenses and effectively responding to such threats.

Security professionals frequently use digital forensic tools to analyze network intrusions. The primary goal is not necessarily to convict the attacker but to understand how the breach occurred, identify vulnerabilities in the system, and implement measures to prevent future breaches. This proactive approach is vital for maintaining the integrity and security of information systems. Similarly, data recovery firms use forensic tools to retrieve files from drives that have been accidentally reformatted, corrupted, or damaged. These tools can recover valuable data that

DOI: 10.69605/ijlbpr_13.6.2024.80

would otherwise be lost, assisting organizations in recovering from data loss incidents.

Regardless of the motivation behind an investigation, the process of assessing, understanding, or reconstructing digital evidence involves identifying, collecting, examining, and reporting information found on computers, mobile devices, and networks. Proper handling of digital evidence is crucial to ensure its integrity and reliability, which are essential for legal proceedings.In addition to cybercrime, digital evidence is increasingly found in cases of traditional crimes such as assault, murder, human trafficking, fraud, and drug trafficking. Digital devices used by either the perpetrator or the victim, such as mobile phones, can contain text messages, call logs, and location data that provide critical evidence in investigations. Similarly, computers and tablets can hold documents, emails, and internet browsing histories that reveal important information about a suspect's activities and intentions.Digital forensics is not only vital for law enforcement and investigations but also for commercial, private, and institutional organizations. Every activity conducted on an individual's computer systems or a company network leaves digital traces. These traces can include web browser history, caches, cookies, document metadata, deleted file fragments, email headers, process logs, and backup files. By analyzing these traces, digital forensic professionals can reconstruct events, understand the sequence of actions taken, and identify the individuals involved.In commercial settings, digital forensics can investigate intellectual property theft, corporate espionage, fraud, and breaches of company policies. In private and institutional organizations, digital forensics can help uncover misconduct, ensure compliance with regulations, and protect sensitive information. The ability to conduct thorough and effective digital forensic investigations is crucial for maintaining trust, ensuring accountability, and safeguarding the integrity of information systems.

VARIOUS BRANCHES OF DIGITAL FORENSICS

Digital forensics is a broad field encompassing various sub-disciplines, each focusing on a specific aspect of digital evidence collection and analysis. Here are the main branches of digital forensics:

1. Network Forensics
2. Disk Forensics
3. Mobile Device Forensics
4. Database Forensics
5. Printer Forensics
6. Digital Music Device Forensics
7. Scanner Forensics
8. Multimedia Forensics
9. Memory Forensics

Figure1: Branches of Digital Forensics

Network Forensics: Network forensics is a crucial sub-branch of digital forensics that focuses on monitoring and analyzing computer network traffic to gather information, collect legal evidence, or detect intrusions. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information since network traffic is transmitted and then lost. Consequently, network forensics often involves proactive investigations.

Traffic interception typically occurs at the packet level, where data is either stored for later analysis or filtered in real-time. Security professionals routinely use network forensic tools not only to convict attackers but also to understand how they gained access and to secure the vulnerabilities exploited. Network forensics assists in post-event investigations to determine how offenses occurred and identify the responsible parties. A digital forensic investigator gathers network-based evidence from specific devices within the network to present it in court, ensuring a thorough investigation and a documented chain of evidence.

Disk Forensics: Disk forensics involves extracting data from storage media such as hard disks, USB devices, FireWire devices, CDs, DVDs, flash drives, and floppy disks. The process involves searching for deleted files, active and unallocated spaces, and slack spaces. Here are the key steps involved in disk forensics:

- **Identification**: Identifying storage devices at the crime scene, which may include various types of disks (e.g., IDE/SCSI hard disks, CDs, DVDs, floppy disks), mobiles, PDAs, and other storage media such as flashcards, SIM cards, USB/FireWire disks, magnetic tapes, Zip drives, and Jazz drives.
- **Acquisition**: Using forensic imaging tools to acquire data by creating bit-stream images. This process should maintain disk geometry and ensure data integrity by write-protecting the source media.
- **Authentication**: Verifying the forensic image against the original data using hashing mechanisms to ensure the copy is exact and unaltered.

DOI: 10.69605/ijlbpr_13.6.2024.80

- **Preservation**: Storing original evidence in secure storage and creating additional copies on reliable mass storage media, such as optical media, which offer reliability, speed, longer lifespan, and reusability.
- **Analysis**: Conducting a thorough analysis of digital evidence, searching for relevant information across files, folders, databases, cookies, temporary files, swap files, internet history, registries, pictures, passwords, and ambient data areas such as deleted, formatted, slack, and unallocated spaces.
- **Finding**: Generating reports that present technical evidence in a simple and precise manner, ensuring comprehensibility for non-technical audiences.

Mobile Device Forensics: Mobile device forensics involves recovering digital evidence from mobile phones under forensically sound conditions using accepted methods. Mobile phones, especially those with advanced capabilities, are relatively new and not typically covered in classical computer forensics. Mobile devices vary in design and continually evolve as technologies improve and new ones are introduced. Understanding the components and organization of cell phones is essential for effectively dealing with them forensically.
Mobile device forensics includes analyzing both SIM cards and phone memory, each requiring different procedures. Unlike computer forensics, mobile forensics deals with inbuilt communication systems (e.g., GSM) and proprietary storage mechanisms. Investigations often focus on simple data such as call logs and communications (SMS/Email) rather than in-depth recovery of deleted data.

Database Forensics: Database forensics is a sub-discipline of digital forensics focused on applying investigative techniques to databases and their related metadata. Forensic examination of a database may involve analyzing timestamps associated with the update times of rows in relational tables to verify the actions of database users. Alternatively, the examination may focus on identifying transactions within a database system or application that indicate evidence of wrongdoing, such as fraud.
Database forensics involves scrutinizing the integrity and authenticity of database records, ensuring that any detected anomalies or suspicious activities are thoroughly investigated. This branch of forensics is essential for uncovering fraudulent activities and ensuring the accountability of database users.

Printer Forensics: Printer forensics is crucial for identifying the devices used to print materials related to criminal or terrorist activities. Forgers often use digital scanners and printers to create counterfeit currency and documents. By analyzing printed documents, forensic experts can identify unique characteristics of printers and even differentiate between devices of the same model. This helps law enforcement agencies trace counterfeit materials back to specific printers.

Digital Music Device Forensics: Digital music devices, with their large storage capacities and multifunctional capabilities, have become relevant to digital forensics. These devices can store various types of files, making them potential tools for criminal activities. Forensic experts must determine whether current cyber forensics frameworks apply to these devices and adapt guidelines accordingly. Investigations may focus on identifying sensitive information or evidence stored on these devices.

Scanner Forensics: Scanner forensics involves identifying the brand and model of scanners used to create digital images. Scanners, like digital cameras, capture images of printed materials and are used in controlled environments. Forensic techniques analyze scanning noise and other statistical features to identify the source of scanned images. This approach can also be extended to other imaging devices, highlighting the need for standardized analytical procedures and protocols.

Multimedia Forensics: Multimedia forensics encompasses techniques for analyzing audio, video, and image files to recover evidence. This branch aims to reveal the history of digital content, including creation, modification, and transmission details. By analyzing multimedia signals, forensic experts can retrieve critical information, aiding in criminal investigations and legal proceedings.

Memory Forensics: Memory forensics, or memory analysis, involves examining volatile data in a computer's memory dump. This branch is essential for investigating and identifying attacks or malicious behaviors that do not leave detectable tracks on hard drive data. Memory forensics provides insights into activities occurring in the system's RAM, helping investigators uncover hidden or transient evidence crucial for understanding cyber threats.

IMPORTANT SOURCES OF DIGITAL EVIDENCE

Digital evidence can originate from a variety of sources, each providing crucial information that can aid in investigations and prosecutions. Here are the primary sources of digital evidence:

A. Computer System: A computer system and its components can be valuable evidence in an investigation. The following elements are potential sources of digital evidence:

- **Computer Hardware**: Physical components of the computer, such as the central processing unit (CPU), memory (RAM), and hard drives.

DOI: 10.69605/ijlbpr_13.6.2024.80

- **Software**: Applications installed on the computer, including operating systems and software applications.
- **E-mails and Attachments**: Communication records and associated files.
- **Databases**: Structured collections of data, such as financial information and customer records.
- **Internet Browsing History**: Records of websites visited, which can provide insights into user activities.
- **Documents and Photos**: Files created or stored on the computer.
- **Image Files**: Digital photographs and graphics.
- **Chat Logs and Event Logs**: Records of online conversations and system events.
- **Data Stored on External Devices**: Information on connected storage devices like USB drives and external hard drives.
- **Identifying Information**: Metadata and system identifiers associated with the computer and its components.

B. Portable Devices

Handheld devices can also be significant sources of digital evidence. These include:

- **Mobile Phones and Smartphones**: Devices that store a wide range of data including call logs, text messages, and app data.
- **PDAs (Personal Digital Assistants)**: Early forms of handheld computers with various functionalities.
- **Digital Multimedia Devices**: Devices such as MP3 players and portable video players.
- **GPS Receivers**: Devices that record location data.
- **Pagers**: Communication devices used to receive messages.
- **Digital Cameras**: Devices used to capture and store photographs and videos.

These devices can contain software applications, documents, e-mail messages, Internet browsing history, chat logs, buddy lists, photographs, image files, databases, and financial records, all of which are valuable evidence in an investigation.

C. Storage Devices

Storage devices store vast amounts of information that can be critical for investigations. Examples include:

- **Hard Drives and External Hard Drives**: Primary storage units in computers and as standalone devices.
- **Removable Media**: CDs, DVDs, and Blu-ray discs.
- **Thumb Drives and Memory Cards**: Portable storage solutions often used in cameras and smartphones.

These devices may contain e-mail messages, Internet browsing history, chat logs, buddy lists, photographs, image files, databases, financial records, and event logs.

D. Peripheral Devices

Peripheral devices enhance the functionality of computers and can also provide valuable evidence. These include:

- **Printers and Scanners**: Devices that can store information about printed, scanned, or faxed documents.
- **Fax Machines**: Devices that transmit documents electronically.
- **External Drives and Storage**: Additional storage devices connected to a computer.
- **Keyboards and Mice**: Input devices that can contain user data and provide fingerprints or other physical evidence.

Information stored on these devices regarding their use, such as incoming and outgoing phone and fax numbers, printed documents, and scanned images, can be crucial. Additionally, these devices can provide forensic evidence like fingerprints, DNA, and other identifiers.

E. Computer Networks

A computer network links multiple computers and devices, sharing resources and data. Elements of a computer network that can serve as evidence include:

- **Networked Computers**: Systems connected to the network, each potentially holding valuable data.
- **Peripheral Devices**: Printers, scanners, and other devices connected to the network.
- **Data Routing Devices**: Routers, switches, and hubs that manage network traffic.
- **Network Information**: Data such as software, documents, photos, image files, e-mail messages, attachments, databases, financial information, Internet browsing history, log files, event logs, chat logs, and buddy lists.
- **Device Functions and Capabilities**: Information on how network devices are used and their specific functionalities.
- **Identifying Information**: IP addresses, LAN addresses, MAC addresses, and NIC addresses associated with networked devices.

STANDARD OPERATING PROCEDURES (SOP) OF DIGITAL FORENSICS INVESTIGATION

The Standard Operating Procedures (SOP) for digital forensics investigations are divided into several key steps, typically defined by different standard organizations into four to five stages. These procedures ensure that digital forensic investigations are conducted systematically and in compliance with legal and technical standards.

The National Institute of Standards and Technology (NIST) divides any forensics investigation into four phases, which are briefly summarized below:

A. Collection: The collection phase involves identifying, labeling, recording, and acquiring data from potential sources while preserving the integrity of the data. This step is crucial as it

DOI: 10.69605/ijlbpr_13.6.2024.80

ensures that the evidence is gathered in a manner that maintains its original state and prevents contamination or alteration. The collection process includes:

- **Identification**: Locating relevant data sources such as computers, mobile devices, storage media, and network logs.
- **Labelling**: Clearly marking each piece of evidence to maintain a chain of custody.
- **Recording**: Documenting the condition and location of each piece of evidence.
- **Acquisition**: Using forensic tools to create exact copies of data without altering the original evidence.

B. Examination

The examination phase uses manual and automated methods to assess and extract data of particular interest while preserving the data's integrity. This phase focuses on:

- **Data Assessment**: Evaluating the collected data to determine its relevance to the investigation.
- **Data Extraction**: Extracting pertinent information using forensic software tools.
- **Data Preservation**: Ensuring that the extracted data remains unchanged and is securely stored.

C. Analysis

The analysis phase involves using legally justifiable methods and techniques to derive useful information from the extracted data. This step includes:

- **Data Analysis**: Interpreting the extracted data to uncover relevant information related to the investigation.
- **Pattern Recognition**: Identifying patterns, anomalies, and correlations in the data.
- **Hypothesis Testing**: Formulating and testing hypotheses based on the evidence.

D. Reporting

The reporting phase involves documenting the findings and describing the actions taken during the investigation. The report should explain the tools and procedures used, determine what additional actions are needed, and recommend improvements. This phase includes:

- **Documentation**: Creating a detailed report of the investigation process and findings.
- **Explanation**: Clarifying how specific tools and methods were chosen and used.
- **Recommendations**: Suggesting further forensic examinations, securing vulnerabilities, and improving security controls.
- **Policy Improvements**: Proposing enhancements to policies, guidelines, procedures, and tools used in the forensic process.

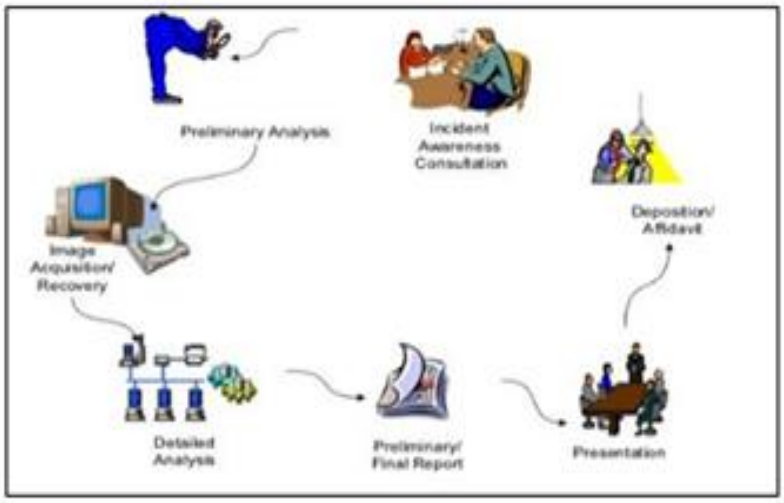

Figure 2: Stages of Digital Forensics Process

This figure visually represents the stages involved in a digital forensics process, outlining the flow from preliminary analysis to detailed reporting and presentation.

The SOPs ensure a structured and systematic approach to digital forensic investigations, maintaining the integrity and reliability of the evidence throughout the process.

COMPUTERS IN BUSINESS ENVIRONMENT

In business environments, computer systems often have complex configurations involving multiple computers networked together, connected to a common server, or integrated with various network devices. Securing a scene and collecting digital evidence in such settings can pose significant challenges for first responders. Improperly shutting down a system can lead to data loss, destruction of evidence, and potential civil liabilities.

First responders might encounter similar scenarios in private residences, especially when businesses operate from home. In these cases, responders may face unfamiliar operating systems or unique hardware and software configurations requiring specific shutdown procedures, which are beyond the scope of this guide.

DOI: 10.69605/ijlbpr_13.6.2024.80

EMERGING PROBLEMS

Despite the challenges that digital forensics has faced to date, more intriguing problems are emerging on the horizon. Computers are becoming increasingly pervasive in modern society, changing in size, shape, speed, and function as their numbers grow. While digital evidence was once gathered from monolithic, stand-alone mainframes, today we have a diverse array of devices including PCs, laptops, palmtops, PDAs, supercomputers, and distributed client-server networks, all of which can provide digital evidence.

Networks now use a variety of transmission media such as twisted pairs, coaxial cables, fiber optic cables, radio, and infrared radiation to convey information. We have local area networks (LANs) and wide area networks (WANs). Digital evidence stored on one computer can be accessed by a perpetrator using another computer located halfway across the world, spanning several legal jurisdictions.

As computers become smaller, faster, and more affordable, they are increasingly embedded within larger systems in ways that are not always obvious. This allows data to be created, stored, processed, and transmitted in unique ways. Consequently, digital evidence can appear in unexpected places and forms. The instrumentation of spaces for various purposes, from environmental monitoring to interactive control of heart rhythms, means that collecting and analyzing digital evidence will become even more challenging. Presenting this evidence in a comprehensible and useful manner for legal proceedings will also become more difficult.

Modernized control systems manage banks, factories, retail inventories, air traffic control, hospitals, schools, corporations, and government organizations. Computers and software programs are embedded in our vehicles, boats, trains, and planes, as well as in tools, equipment, telecommunications systems, and public switched networks. Digital devices are even found within our bodies. Each of these is a potential source of digital evidence. The collection, storage, analysis, and presentation of this evidence will be constrained by evolving legal standards and requirements that we must understand and comply with to avoid significant risks.

CONCLUSION

As discussed above, digital forensics plays a significant role in the criminal justice system, especially as we integrate a wide range of technologies into our daily lives. Evidence of almost all types of crimes is increasingly found in digital devices used by either the perpetrator or the victim. Because of this potential for evidence that did not exist before, investigators of traditional crimes must increasingly consider any digital evidence that may be available.

Moreover, security professionals routinely use digital forensic tools to analyze network intrusions not necessarily to convict the attacker but to understand how the perpetrator gained access and to secure the vulnerabilities. Data recovery firms rely on similar tools to recover files from drives that have been accidentally reformatted or damaged.

In the future, digital forensics will play an increasingly significant role in the criminal justice system as we continue to incorporate a range of technologies into our everyday lives. As the digital forensic discipline continues to mature, those in the criminal justice system will more readily understand and accept the contributions it can make to the discovery and production of evidence. This acceptance will enhance the ability to solve crimes and secure convictions based on reliable and verifiable digital evidence.

Furthermore, as technology evolves, digital forensics must also adapt and develop new methods and tools to keep pace with emerging threats and complex digital environments. Continuous advancements in forensic techniques and tools will ensure that digital evidence remains a robust and integral part of the investigative process, supporting the pursuit of justice in an increasingly digital world.

REFERENCES

1. Joseph Peterson, Ira Sommers, Deborah Baskin, and Donald Johnson. The Role and Impact of Forensic Evidence in the Criminal Justice Process.National Institute Of Justice 2010. (Peterson, 2010).
2. Teri A. Cummins Flory (Purdue University). Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies. Journal of Digital Forensics, Security and Law 2016; 11(1): article 4,7-38.
3. Digital Forensics Department, Cyber Security Malaysia. Standard Operating Procedure Of Digital Evidence Collection. 2013. (Talib, 2013).
4. John Ashcroft, Deborah J. Daniels, Sarah V. Hart. Forensic Examination of Digital Evidence: A Guide for Law Enforcement," 1994.U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.
5. ISO/IEC JTC 1/SC 27 Information Security. "ISO/IEC 27037:2013, Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence," International Standard Organization, 2012.
6. SWGDE. "SWGDE Best Practices for Computer Forensics Version 2.1," 2006.
7. ASCLD/LAB-International. "Supplemental Requirements for the Accreditation of Forensic Science Testing Laboratories," 2011 edition, 2010. (Laboratories, 2010).
8. ISO/IEC JTC 1/SC 27 Information Security. "ISO/IEC 17025:2005, General Requirements for the Competence of Testing and Calibration Laboratories," 1st Revision, 2005.
9. Morgan. "2019 Official Annual Cybercrime Report," Cybersecurity Ventures, 2019.
10. Marshall. "Digital Forensics: Digital Evidence in Criminal Investigations," 2013.
11. Henry Gladney. "Long-Term Preservation of Digital Records: Trustworthy Digital Objects," The American Archivist, vol. 72, 2009. (Gladney, 2009).

DOI: 10.69605/ijlbpr_13.6.2024.80

12. Ankit Agarwal. "Systematic Digital Forensic Investigation Model," ResearchGate, 2011. (Agarwal, 2011).
13. Daniel. "Digital Forensics for Legal Professionals: Understanding Digital Evidence From the Warrant to the Courtroom," 2011.
14. National Institute of Science and Technology, Information Technology Library. "NIST Computer Forensics Tool Testing Program," http://www.cftt.nist.gov, 2019. (NIST, 2019).
15. Henry. "Best Practices In Digital Evidence," 2009.