International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Advances in Computer Applications and Information Technology
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# Role of Digital Forensics in Crime Investigation

***Prasad Pawar, Bhavesh Lende***
*G H Raisoni University Amravati*

**Abstract:** As almost every element in our lives has been embedded in the digital domain, it is the integral part of all modern criminal investigations. As the volume of computer crimes is ever-increasing along with dependency on the electronics, it is mandatory for law enforcement agencies to be equipped with the right methodologies and technology to seize, search, acquire, and preserve the electronic evidence. Digital Forensics acts as an interface between criminal investigation and the field of computer related crimes through application of scientifically methodical techniques and tools for the recovery of appropriate evidence from computers, cell phone, networks and various storage mediums [1].In this investigation the importance of Digital Forensics is described. Digital Forensics play an extremely important role in investigation by identification of digital evidence, rebuilding of crime scenes and the presenting of evidence in court to assure conviction of criminals. Investigation procedures incorporate forensic activities as acquisition, preservation, examination and analysis of evidence from various sources, and eventually presenting the data in court in an acceptable way [2]. Digital devices like smartphones, personal computers, cloud storage systems, network systems, etc contain vast amount of information to establish a relation between suspects and the crimes being investigated and to determine the time of the crime. Many invisible digital traces of crime are always helpful in the investigation process [3]. The main challenges for digital forensics come from encrypted data and anti-forensic tools [4].Digital Forensics has emerged as the scientific discipline which will lead criminal investigations by identifying, acquiring, analyzing, and presenting digital evidence collected from electronics and network devices. Since both the public and criminals are increasingly reliant on the technology of the digital age, the presence of electronic evidence can be critically important in investigations related to cyber crimes, fraud, homicides and other crimes in which digital traces have been left [5]. Digital forensic tools can be used to acquire a forensically sound image of a deleted file, recorded communication, location information and metadata which can be used as a digital evidence in the court [4].

**Keywords:** Digital Forensics [1], Crime Investigation [2], Digital Evidence [1], Evidence Acquisition [3], Evidence Preservation [3], Cyber Crime Investigation [4], Forensic Analysis [1], Incident Response [5], Chain of Custody [2] etc.

## 1. Introduction

The ubiquity of technology in modern life has lead to the existence of several digital actions, potentially involving criminal activity. To conduct such investigations effectively, a variety of systematic approaches were developed known as digital evidence: identifying it, collecting and securing evidence, analysis and the presentation of evidence. During each of these procedures the digital evidence must be kept in its pristine state throughout the whole forensic procedure; failure to do so would compromise reliability and the courts may not consider the evidence valid. Digital forensics is the application of scientific methods to discover and examine evidence of a crime in order to be applied in the courts, not only for cyber-crimes but also often for traditional crimes [1]. With most modern crimes including hacking, financial fraud, identity theft and information breach, the majority of police forces and investigators are now using digital forensics to unearth hidden digital footprints and traces that the criminal does not realize are left. When the digital evidence in an individual or a group compromises a financial system it can be retrieved and sequence reconstruction traced using digital forensic procedures where it may uncover deleted

information, connections and previous actions linking them to the criminal offense. The advent of digital forensics has therefore radically transformed criminal investigations as digital evidence is now being widely used as a core element in modern courts of law [2].

This can be said to apply to not only cyber-crime but also to murder and robbery investigations, which involves digital evidence acquired from mobile phones, computers, network systems and cloud services. The increase in usage and evolution of technology has shown that digital forensic will play a greater part in tackling complex crimes and that increased interconnectedness leads to a greater number of cyber-crimes. These crimes have made forensic procedures important to maintain and prevent evidence tampering while also reconstructing events and revealing hidden data for investigation purposes, such as: acquisition of data, chain of custody and forensic analysis [3]. The prevalent presence of digital devices and networks in most homes and workplaces means that the vast majority of investigations will invariably involve some form of digital evidence. These methods are scientific in their procedures of identification, collection and securing of data, analysis and finally presenting evidence at court and are primarily aimed at preserving its integrity. In cases that may range from simple crimes to sophisticated cyber crimes involving theft of personal information from computers, mobile devices, network systems, and cloud storage, digital forensics has proved invaluable in their successful resolution [4]. Through the use of digital forensics investigators are able to not only find the telltale digital footprints of criminals but also reconstruct events by tracing their virtual path and providing them with accurate timelines. Forensic tools can be used to not only locate lost or hidden data but also to reconstruct connections between the culprit and the crime using information acquired from various computer systems, mobile devices, networks, and cloud platforms. Even though digital evidence can be used for virtually all criminal investigations and crimes, even for traditional ones like murder, robbery and assault; scientific processes have been applied to digital evidence to demonstrate the connection to criminal activity and the importance in court [5]. The significance of digital forensics in crime investigation: Digital forensics assist investigator in extracting unknown information from the digital device and reconstruction of cyber event or crime. The digital evidence such as e-mails, logs, documents, browsing data, traffic data of a computer etc can assist in the investigation of cybercrime, financial crime, identity theft, terrorism etc. Using the proper forensic method, the digital evidence is kept pristine using well recorded chain of custody, vital to the success of prosecution [2]. In addition to supporting the incident response process, digital forensics helps an organization identify, analyze and even prevent cyber-attacks. However, due to proliferation of cloud computing and Internet, data volality, encryption, jurisdiction issues, and enormous amount of digital data pose new challenges to investigators Despite the difficulties, digital forensic techniques and tools have been evolving and they continue to assist law enforcement officials and forensic professionals in handling the investigation of such crimes.[3]

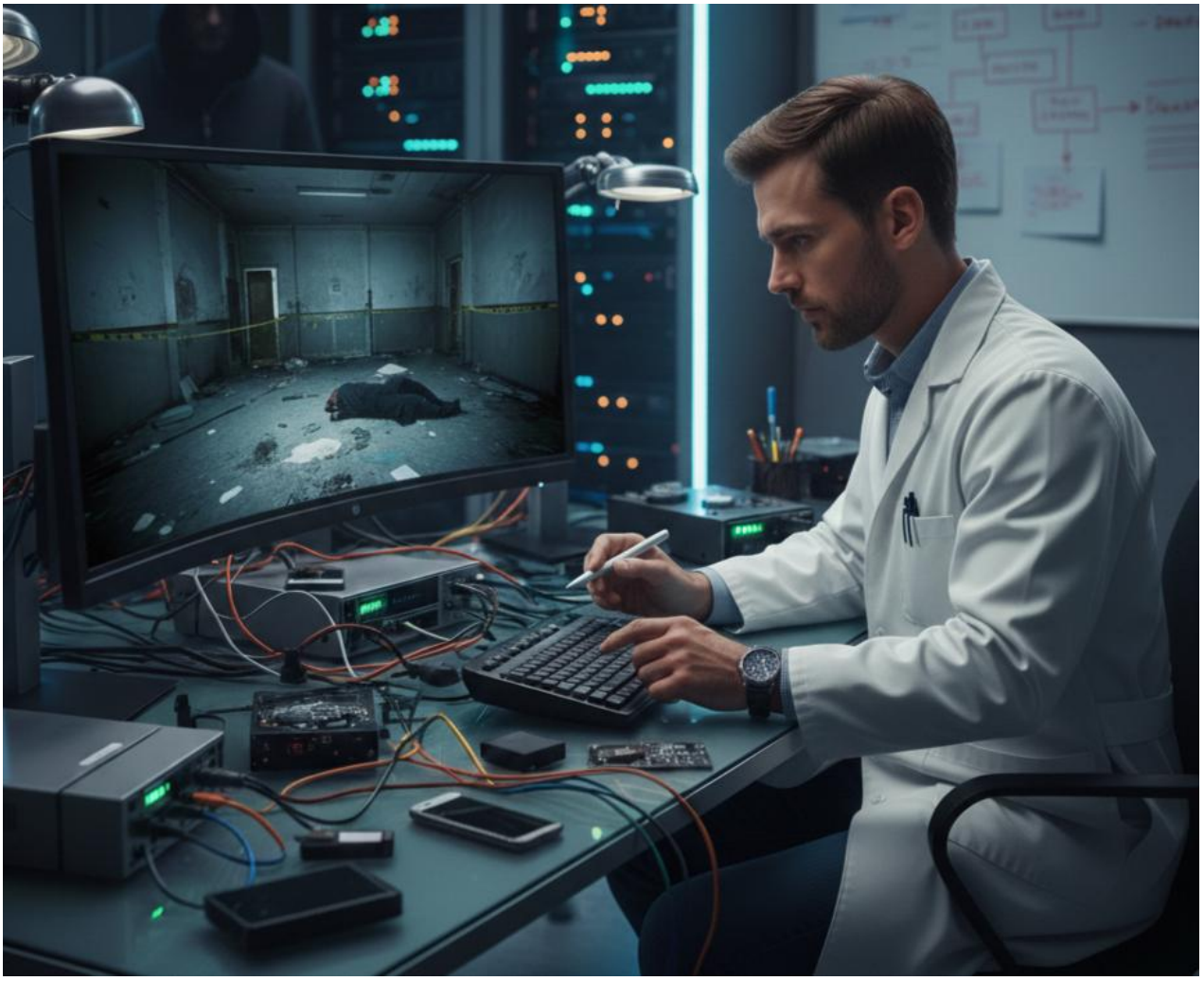

Fig 1. Analyzing Crime Scene Evidence Using Computer-Based Investigation Tools

## 2. Literature Review

Many studies have considered the use of digital forensics in modern crimes, especially the scientific approach applied in legal framework with regards to the law enforcement and the judicial process. The general term used for Digital Forensics is an investigative science focusing on the collection, retention, analysis and presentation of digital evidence from computer and network to be used in court [1]. Digital forensics is of significant value since digital evidence that has been extracted from computer hard drives, memory cards, and any storage devices contain very significant information that will assist in criminal cases, such as deleted files, usage history of computers, browsing history, network log that assist to recreate the event and tie the criminals to the scene of the crime. However, as technology continues to progress, a very vast amount of digital evidence becomes available and the methods of analyzing it become even more important [2].

With regards to how AI may be useful in the analysis of digital evidence there are quite a lot of papers looking at the integration of AI in Digital Forensics investigations. AI can be considered very useful as it helps with pattern recognition, automatic classification of digital evidence and huge data processing. However it is pointed out that there are many papers describing the use of weak AI techniques that is currently used in Digital Forensics, and the further research needed for the use of strong AI in Digital Forensics investigations [3]. Privacy issues have been discussed in several review papers concerning the privacy implications of forensic investigations in the legal context and it seems it will continue to be a critical factor to consider. Literature structured around AI in digital forensics emphasizes potential and limitations [4]. Significant attention has been given by researchers to the issue of cross-border digital forensics from legal and practical standpoints, in relation to admissibility of digital evidence, and

protection of data privacy rights. It has been suggested that the effectiveness of digital forensics needs legal and technical improvements [5].It is pointed out by several papers that digital forensics is an emerging scientific discipline, which enhances the traditional law enforcement investigative processes by laying down a systematic methodology for the identification, collection, preservation, examination and presentation of digital evidence obtained from computer networks and storage media. It plays an essential part due to the pervasive use of computer and digital technology in virtually all crimes, cyber crime, or traditional crimes which include computer forensics [6].

2.1 Beginning of literature on digital forensics

Digital Forensics was at first considered as a sub-domain of forensic science which was used for criminal investigation related to computer crimes and retrieval of data from the digital storage devices. It was later demonstrated that computer systems and digital storage devices could hold incriminating evidence (like deleted files, network data, meta data etc).

2.2 Complementarity with traditional investigation

A recent work highlights the role of traditional and digital forensic investigation. It emphasizes that combining traditional and digital forensic investigation leads to better understanding of the crime scenes and behavior of the criminals from the evidence [7].

2.3 Sub-domains and methodology

Digital Forensics can be further divided into different sub-domains like memory forensics, network forensics, mobile forensics, disk forensics and cloud forensics, etc. In addition to the existing forensic tools and techniques available for each of these sub-domains, new ones are still being developed. Integration of AI for data processing and classification purposes is being studied , [8].

2.4 Challenges in digital forensics

Challenges faced by digital forensic investigators, as illustrated through different works, are mainly the increasing rate of technology, advanced encryption and anti-forensics techniques that create difficulties to the available forensic tools and human investigator, coupled with the huge volume of digital evidence available [5], [9]. Privacy issues related to the collection and storage of data used for forensic investigations remain a critical challenge and need to be managed legally [4], As a result of new technologies, today digital forensics also manages large and complicated data such as cloud computing, Internet of Things and mobile system. According to researches, increasing volumes and variations of digital data lead to problems in the acquisition and examination of the evidences. It is necessary for investigators to be equipped with new methods and to employ automation for efficiently processing large datasets and extracting significant information [4].In recent publications, researchers have presented and discussed using artificial intelligence and machine learning in digital forensics domain. AI and ML techniques help investigators to detect the pattern, classification of digital evidences and accelerate the forensic examination. For instance, machine learning has been used in multimedia forensics, malware detection and anomaly detection successfully [5].

## 3. Research Methodology

A methodologically organized digital forensic investigation methodology is introduced, used for analysis of the contribution of digital forensics in criminal investigations. Digital forensic investigation constitutes obtaining, securing, analyzing, and presenting digital evidence in a court-admissible format for court and investigation purposes. This research aims to present an efficient method using existing forensic process models and investigation stages accepted by digital forensics professionals and practitioners [1].

3.1 Research Design

The research employed a descriptive and analytical approach to explore standard techniques, equipment and phases in digital forensic investigation. The research utilizes existing forensic process models and investigation phases to a degree for systematic analysis of the role digital forensics in criminal

investigation. The technique employed is based on established scientific techniques described in forensic research and industry standards [2].

3.2 Data Sources and Analysis

To present a proposed methodology, data was acquired from research papers, survey studies and published articles about digital forensic investigation and processes models. Analysis of documents from scientific articles, standards and forensic guidance resulted in organizing the phases of the investigation and creating a consistent method that conforms to how a law enforcement agency investigates crime [3].

3.3 Digital Forensic Process Model

A six-phase model for digital forensic investigation is proposed in this study. The stages involved are as follows:

3.4 Identification

This is the recognition that digital evidence is present and identifying the extent of digital evidence. Investigators identify what devices to acquire evidence from to ensure it is being obtained legally and handle devices until seizure [4].

3.5 Preservation

Preservation is the act of protecting digital evidence from loss, damage or alteration, this entails the creation of forensically acquired copies of digital evidence. It involves maintaining proper evidence control, or 'chain of custody', so the integrity of the digital evidence cannot be compromised throughout the investigation [1].The approach taken in the methodology of digital forensics in a criminal investigation follows an orderly, legal procedure, in order to make sure digital evidence is authentic, reliable, and usable in a court of law. Initially, the identification process involves an investigator locating potential digital evidence (such as computer systems, networks, mobile phones, storage devices) used during the commission of the crime. The next step, the preservation of digital evidence, protects digital evidence against modification or loss and upholds the integrity of the chain of custody. Next, is acquisition of the digital evidence where the information stored in devices is duplicated bit-by-bit to make a forensic image of the data (original data is not touched in this stage), this is accomplished using imaging tools. The next step is the examination stage where deleted files are recovered, encrypted files are recovered and hidden data is found, along with filtering data for relevant pieces of information. The fourth stage of digital forensics is the analysis stage where recovered data is examined to piece together how events took place, form a timeline, identify perpetrators of a crime and link digital evidence to a particular crime. The final stage is the presentation stage, the investigator composes a digital forensic report detailing all evidence, and presents the evidence in court. This logical methodology used to deal with digital evidence is key in criminal investigations and the legal system [3].

The method involved in digital forensics to investigate a crime scene is an organized, scientifically based, step by step method that ensure the integrity of the digital evidence, its genuineness and admissibility in the court. The first step involved is 'Identification' stage where investigators determine and search for potential sources of digital evidence such as computer, mobile devices, storage, IoT, network devices and cloud where logs might be found. Identifying the sources of digital evidence makes sure that no piece of digital evidence is left unattended. The second step involved is 'Preservation' stage that consists of preserving the digital evidence found so that it is not destroyed, modified or lost during the process of the investigation. Investigators keep away the device or collect digital data on a portable storage device at the crime scene and maintain a tight chain of custody of digital evidence. The use of tools such as write blockers and forensic imaging tool used to prevent the changes to the digital data. This methodical process ensures that the digital evidence is scientifically and legally examined before it is submitted as evidence in court. With the increase of data and technologies it requires newer methods to cope with this challenge of data and investigation [6]. This shows how evidence should be collected, managed and submitted for investigation. Evidence Identification; potential digital evidence are identified on computer, laptop,

mobile phones, portable media storage, server, cloud platform. Relevant digital data include emails, chat history, web surfing history, etc. [4]. Evidence Collection; digital evidence are collected by digital forensic tool in a safe and security place. Forensic imaging is performed to keep original copies of evidence, while ensuring to maintain a proper chain of evidence [5]. Evidence Preservation; the collection evidence should not be lost, damaged or altered. This involves use of techniques such as encryption and write-blocker to maintain secure data [1]. Evidence Examination; evidence collected are inspected and examined for hidden or deleted evidence, signs of malicious attacks or abnormal signs [6]. Evidence Analysis; findings are correlated and analyzed using specific tools in order to establish facts and evidence that support and are related to the cause of the crime. Example of techniques to establish facts include timeline analysis and keyword search [3]. Reporting and Presentation; reports are produced to highlight relevant findings including methods and tools used in the investigation. Reports are written for law enforcement and judiciary so they can be able to understand it well and the evidence obtained can be legally submitted to court [2]The methodology used in this research is based on a well-defined systematic digital forensic investigation process in the context of crime investigation. This procedure is a set of several sequential phases including identification, preservation, acquisition, examination, analysis and reporting of digital evidence which ensures the integrity of evidence during the legal proceeding [1]. The identification phase is to find out possible digital evidence such as computers, mobile phones, storage media and network log files carefully and describe them to keep chain of custody of evidence [1]. During preservation stage the evidence is kept intact by preventing from any modification by using write blockers, secure storage and by using cryptographic hash function such as MD5 and SHA which ensure the integrity of data [2]. Acquisition phase is used to get exact replica of storage media by taking bit-to-bit copy image of evidence using forensic imaging tool to be able to recover the deleted, hidden or encrypted data by applying forensic tool like EnCase and FTK [3]. In examination stage filtering, extracting the required information out of a very large data set and recovered deleted file, key word search and metadata analysis were done. While in the analysis phase the investigator reproduces the events, identify malicious activity and correlation between digital evidence and the incident to produce relevant outcomes [4]. Finally in presentation stage the extracted results are presented in a formal manner and well defined forensic report so that the evidence are easily interpretable and admissible to be supported for judicial purposes [5]. It is clear from the description of the above mentioned procedure that how much important role digital forensics plays in the present crime investigation that allows to deal with data properly, reconstructing cyber crime and support to law enforcement agencies.

The goal of the preservation phase is to prevent loss, modification, destruction or tampering with the digital evidence. Devices are removed from networks and locked write-blockers used; evidence is stored in controlled forensic surroundings and cryptographic hash functions such as MD5 or SHA-256 applied to detect any alterations, ensuring data integrity throughout the lifecycle of an investigation [2]. The acquisition stage involves a bit-by-bit forensic image of a storage device without alterations and aims at recovering deleted, hidden or encrypted files in a forensically sound manner, using commonly found software such as EnCase, FTK and Autopsy [3].


Fig 2 : Crime Investigation Process

## 4. Result


Fig 3:: Result Synopsis – Forensic Efficacy in Conviction Integrity

## 5. Conclusion

In this technology-driven age, digital devices are inseparable from our lives and their growing use in cyber-criminal activities has become an important issue to be tackled. This paper addresses the impact of digital forensics in modern crime investigation and its contribution to the criminal justice system. The scope of digital forensic involves identification, acquisition, preservation, examination, analysis, and reporting of digital evidence, in a manner acceptable to courts. These processes are helpful for investigators to unearth information and reconstruct scenes and links between suspects and crimes using digital evidence obtained from digital sources [1]. From the results, digital forensics has contributed positively in criminal investigation. Electronic data like emails, chat messages, browser history, GPS data,

system logs and multimedia data play a significant role in solving both cyber and physical crimes. Advanced tools used can recover lost, deleted and encrypted data, making it impossible for the culprits to completely destroy or remove any digital trace they left behind. The proper collection and maintenance of chain of custody ensure its legal admissibility in court [2]. A further significant role that digital forensics can play is in documentation and reporting. The structure and content of a forensic report can help explain the intricate findings of a technically-oriented investigation into a form that judges, lawyers and investigators can easily understand. In the courtroom, digital forensics experts can present technical evidence to the judge, attorney and investigator so that it can be used effectively to secure the conviction of the guilty and prevent the persecution of the innocent [3].

There are many challenges encountered in digital forensic investigation, for example the rate of technological growth and wide use of encryption, the sheer volume of digital evidence generated, lack of skilled forensic professionals etc. There are also a lot of issues regarding the legal and ethical nature, for instance protecting the privacy of the data. The field has to be developed constantly both in terms of tools, knowledge and the legal and regulatory framework to keep up with these challenges [4]. In essence, digital forensics have revolutionized crime detection by providing an entirely new perspective. As the world gets connected through internet, smart phones, social networking and cloud computing, virtually every act committed leaves behind a digital footprint. This digital evidence is increasingly becoming one of the most valuable evidence sources in many criminal proceedings. It not only aids investigation but also crime prevention, by being able to identify trends and indicators of behavior from the digital environment. [5]. Modern tools for digital forensic have allowed rapid processing of enormous amount of digital data and has provided useful assistance in case of crimes like cyber fraud, hacking, identity theft, financial crimes and also organized cyber-attacks, among others. It can support financial forensics and network security by presenting technical knowledge and findings [1, 5]. Mobile and cloud forensic are two areas which fall under digital forensics that have become critically important as almost all modern crime scenarios are based on smartphones, chat applications or data on the cloud. Digital evidence is extracted from these media, for instance from smart phones data includes call records, chat logs, photos and activity logs whereas the cloud data are extracted through cloud forensics methods. This becomes very useful to obtain the deleted and hidden data in remote storage [2]. It has also been recognized that digital forensic experts are key individuals, since cyber-crimes are developing with the evolution of technology. The professionals engaged in digital forensics must continuously update their knowledge of forensic tools, techniques and strategies, the application of encryption technologies and the legal processes. The authorities must invest in state-of-the-art labs, provide necessary training and conduct relevant research to enhance our digital forensics capabilities [3].

Ethical and legal considerations are at the forefront of digital forensic investigations. To ensure that no rights of a person are infringed, the investigators should adhere strictly to all legal procedures and laws governing the handling and processing of digital evidence. Unauthorized access or mistreatment of digital evidence can compromise investigations and could potentially jeopardize the legal standing of a case. Adherence to ethical standards and laws relating to the processing and handling of data is crucial [4]. In addition to the investigative process, digital forensics also has a vital role in public safety and national security. Authorities can monitor cyber threats, control cyber terrorism and identify and prevent large scale organized cyber-crimes. The findings derived from digital forensic analysis can be used to strengthen the criminal justice system and enhance organizational security [5]. Digital forensics is now an important part of crime investigation as digital technologies and cyber crimes are growing exponentially. This paper had the opportunity to identify the crucial need for a well structured digital forensic investigation methodology to find, preserve, acquire, examine, analysis, and report digital evidence properly. Using scientifically approved forensic procedures in a digital forensic investigation will enable integrity, authenticity and credibility of digital evidence to be maintained thus making it admissible to court [1]. From the above it was seen how the field of digital forensics assist the police, investigative agencies to re-establish the nature and timeline of the cyber incident and to pinpoint the offenders who have committed crimes through cyber technology. Forensic imaging, recovery, log analysis, and timeline

construction were all techniques in digital forensics used to search and find deleted data and establish facts relation to the criminal activities [2]. Appropriate documentation and chain of custody is crucial to transparency of findings for any court proceedings [3].

As cyber threats continually develop, new and emerging technologies such as the cloud, IoT and AI have introduced new complexities and challenges for the digital forensics investigators. These issues require ongoing research, better forensic tools and updated methodologies for a better digital forensics investigation practice. Digital forensics is the powerful and accurate technique in modern crime investigation that helps to fight cyber crime, manage digital evidence and contributes greatly to the judicial process [4]. With the rapid growth of technology and its use in all areas of life, digital forensics has developed into an essential branch of crime detection in the 21 st century. This research has highlighted the need for a coherent and scientific digital forensic investigation methodology which has all elements in place for dealing with digital evidence from the moment it is identified right through to being presented in court. From identification to preservation, acquisition, examination, analysis, and reporting, it ensures that the evidence is legitimate and defensible [1]. When forensic models and chain of custody is kept and followed, illegal manipulation of digital evidence will be avoided [2].It has shown how digital forensics is fundamental to the recovery of cyber incidents, finding suspect and building facts and relationships between digital evidence and a crime [3]. It helps by recovering hidden, deleted or encrypted data by using methods such as forensic imaging, deleted file recovery, searching using keywords, analyzing metadata or even building a timeline of activity, allowing this data to be used as evidence against the offender [3]. The police can utilize digital forensics as a way to investigate any form of computer crime such as hacking, fraud, identity theft, cyber stalking anddata breaches [4]. Besides its applications to investigative work, digital forensics is important in managing evidence, incident response and cybercrime investigation. Clearly defined documentations and detailed forensic reporting can make technical data easy to understand by legal agencies and court system. The utilization of modern forensic tools, such as the automation of the analysis process, makes the digital investigation process much more accurate and time effective [5]. Despite its helpfulness, rapidly advancing technology also raises some challenges for the digital forensic investigators. Widespread of cloud computing, Internet of Things, encrypting and artificial intelligence bring larger and more complicated amount of data and, thus more sophisticated forensic tools and methodologies are required to cope with those challenges. It requires more research, training and advanced forensic frameworks in this field [6].

**Reference**

1. Beebe, Nicole Lang, and Jan Guynes Clark. 2005. "A Hierarchical, Objectives-Based Framework for the Digital Forensics Process." Digital Investigation Journal.
2. Pollitt, Mark. 1995. "Computer Forensics: An Approach to Evidence in Cyberspace." National Institute of Justice Journal.
3. Kohn, Michael, Morris Olivier, and Jan Eloff. 2006. "Framework for a Digital Forensic Investigation." Information Security South Africa Conference.
4. Reith, M., C. Carr, and G. Gunsch. 2002. "An Examination of Digital Forensic Models." International Journal of Digital Evidence, vol. 1, no. 3, pp. 1–12.
5. Pollitt, M. 2006. "A History of Digital Forensics." In Advances in Digital Forensics, vol. 2. Springer, pp. 3–15.
6. Rosenblatt, K. 2012. "Digital Forensics and Incident Response." SANS Institute InfoSec Reading Room.
7. Van Baar, R. B., W. Alink, and A. R. Van Ballegooij. 2008. "Forensic Data Recovery from Flash Memory." Small Scale Digital Device Forensics Journal, vol. 2, no. 1, pp. 1–17.
8. Casey, Eoghan. 2011. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.

9. Carrier, Brian. 2005. File System Forensic Analysis. Addison-Wesley Professional.
10. Nelson, Bill, Amelia Phillips, and Christopher Steuart. 2018. Guide to Computer Forensics and Investigations. Cengage Learning.
11. Rogers, Marcus. 2004. Cyber Forensics: Understanding Information Security Investigations. Springer.
12. Volonino, Linda, and Reynaldo Anzaldua. 2008. Computer Forensics for Dummies. Wiley Publishing.
13. Palmer, Gary. 2001. "A Road Map for Digital Forensic Research." Digital Forensic Research Workshop (DFRWS).
14. Casey, E. 2011. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd ed. Burlington, MA, USA: Academic Press.
15. Carrier, B. 2005. File System Forensic Analysis. Boston, MA, USA: Addison-Wesley.
16. Behl, N., and K. Behl. 2017. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford, U.K.: Oxford University Press.
17. Garfinkel, S. L. 2010. "Digital Forensics Research: The Next 10 Years." Digital Investigation, vol. 7, pp. S64–S73.
18. Jain, A. K., and B. B. Gupta. 2017. "Digital Forensics: An Overview." International Journal of Advanced Research in Computer Science, vol. 8, no. 5, pp. 1–6.
19. Sammons, J. 2012. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Boston, MA, USA: Syngress.
20. Carvey, H. 2011. Digital Forensics with Open Source Tools. Burlington, MA, USA: Syngress.
21. Van Baar, R. B., W. Alink, and A. R. Van Ballegooij. 2008. "Forensic Data Recovery from Flash Memory." Small Scale Digital Device Forensics Journal, vol. 2, no. 1, pp. 1–17.
22. Palmer, G. 2001. "A Road Map for Digital Forensic Research." DFRWS Digital Forensic Research Workshop.