IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DIGITAL FORENSIC

[1] Dr Balaji K, [2]Rahul P,[3]Naveen Kumar, [4]Sharath U, [5]Nandeep

[1]Professor, Department of MCA, Cambridge Institute of Technology CITech, Bengaluru, India, [2,3,4] Student, Department of MCA, CITech, Bengaluru, India.

ABSTRACTION

Crimes committed in electronic or digital spaces, particularly within cyberspace, have become widespread. Criminals utilize technology to carry out their unlawful activities, presenting novel challenges for law enforcement agents, legal practitioners, military personnel, and security specialists. Digital forensics has assumed a critical role in detecting and resolving crimes involving computers and digital assistance. This paper presents a brief overview of digital forensics, offering an introduction to its importance in tackling modern criminal activities.

1.INTRODUCTION

The ubiquity of digital devices like cell phones, tablets, gaming consoles, laptops, and desktop computers has made them integral to modern society. As these devices proliferate in everyday life, there's a growing trend of using information from them for criminal activities. Crimes such as fraud, drug trafficking, homicide, hacking, forgery, and terrorism frequently involve computers.

In response to these challenges, digital forensics (DF) emerged within law enforcement, computer security, and national defense sectors. Entities such as law enforcement agencies, financial institutions, and investment firms are integrating digital forensics into their operations.

Digital forensics aids in investigating cybercrime and identifying direct evidence of computer- assisted crimes. The concept originated in the late 1990s and early 2000s under the term "computer forensics." Various sectors including the legal profession, law enforcement, policymakers, businesses, education, and government have a stake in digital forensics. While it's commonly associated with criminal law, digital forensics is also utilized in private investigations, demanding strict standards to withstand cross-examination in court

CHARACTERISTICS OF DF

Digital forensics is often linked with the detection and prevention of cybercrime, closely related to digital security as both address digital occurrences.

While digital security emphasizes proactive measures, digital forensics concentrates on reactive actions. The realm of digital forensics comprises five main branches: computer forensics, network forensics, mobile device forensics, memory forensics, and email forensics.

Perpetrators frequently exploit vulnerable areas like peer-to-peer file sharing. Mobile device forensics, an evolving field, concerns the extraction of digital evidence from mobile devices. The digital domain has increasingly become a primary target for email hacking incidents.

PRINCIPLES OF DF

DF, initially synonymous with computer forensics, has evolved to encompass the forensic examination of all digital technologies. A digital forensic inquiry typically comprises three main phases: evidence preservation, analysis, and presentation/reporting.

Digital evidence spans across open computer systems, communication systems, and embedded computer systems. Notably, digital evidence can be precisely duplicated and is resistant to destruction. It can be sourced from various devices such as hard drives, flash drives, phones, mobile devices, routers, tablets, and GPS devices. For evidence to be deemed admissible in court, it must beboth relevant and reliable. Thus far, there have been relatively few legal challenges to digital evidence.

Forensic analysis involves piecing together the elements necessary to solve the computer-related crime, necessitating the use of effective tools. Numerous software tools are now available to trained forensic investigators. These analysts employ various techniques in line with the principles of forensic science during their investigations.

The presentation of evidence entails preparing a comprehensive report to communicate the findings to all relevant parties, including the judge, jury, defendant, attorneys, and prosecutors. The report must be meticulously crafted to meet the standards of admissibility in a court of law.

CHALLENGES

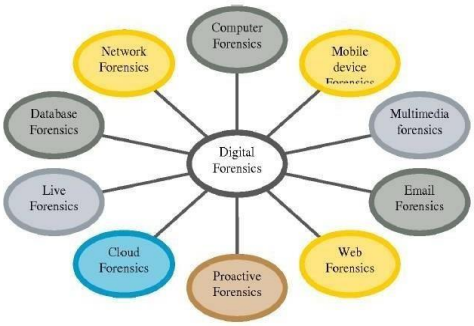
The rapid growth and advancements in computing and network technologies have rendered existing digital forensics tools and techniques ineffective.

The swift evolution of digital forensics has led to a lack of standardization and training. Due to the unique nature of each investigation, creating standardized procedures for forensic analysis is challenging. However, to address the need for standardization, various organizations like the National Institute of Standards and Technology (NIST) have issued guidelines for digital forensics. In responseto the demand for training, some companies have initiated certification programs.

Analyzing evidence stored on digital computers poses one of the foremost forensic challenges for law enforcement. Legal constraints may limit analysts' investigative capabilities, as national and international laws can restrict the amount of information that can be seized.

Another significant challenge in digital forensics is the escalating volume of data requiring analysis. With the advent of big data, the approach to digital forensics investigations must evolve. Big data encompasses datasets that are excessively large, characterized by the volume, velocity, variety, and variability of data.

Key future challenges include cloud computing, metadata analysis, anti-forensics (methods to impede forensic analysis), encryption, social networking, the Internet of Things, and wirelessnetworks.



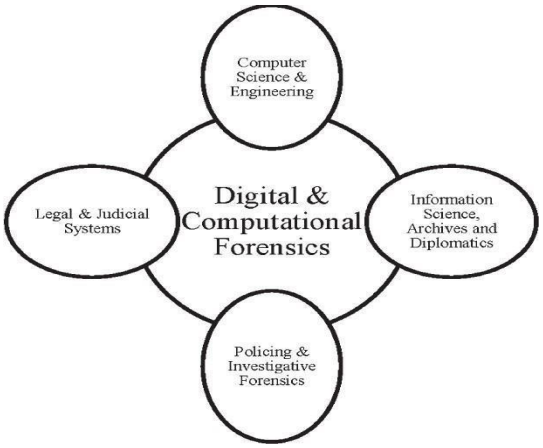
PERSONNEL-RELATED CHALLENGES

Personnel-related challenges pose a significant threat to the integrity of digital evidence. Among these challenges, the shortage of well-trained forensic staff stands out prominently. Despite the critical importance of digital forensics in combating cybercrimes, the scarcity of qualified forensic officers jeopardizes the entire process. This shortage stems from intense competition in law enforcement and the high technical proficiency required for digital forensics, including certification and scientific training.

Moreover, the field of digital forensics has garnered substantial attention from forensic practitioners, law enforcement agencies, and computer professionals. However, its advancement has also led to differences in terminology, creating an environment fraught with challenges.

Another key personnel-related challenge is maintaining the chain of custody in digital forensic analysis. This entails documenting the evidence's collection point, a task complicated by the lack of physical control in a digital environment. Managing the chain of custody is further hindered by proprietary technology, diverse procedures, and cross-jurisdictional laws.

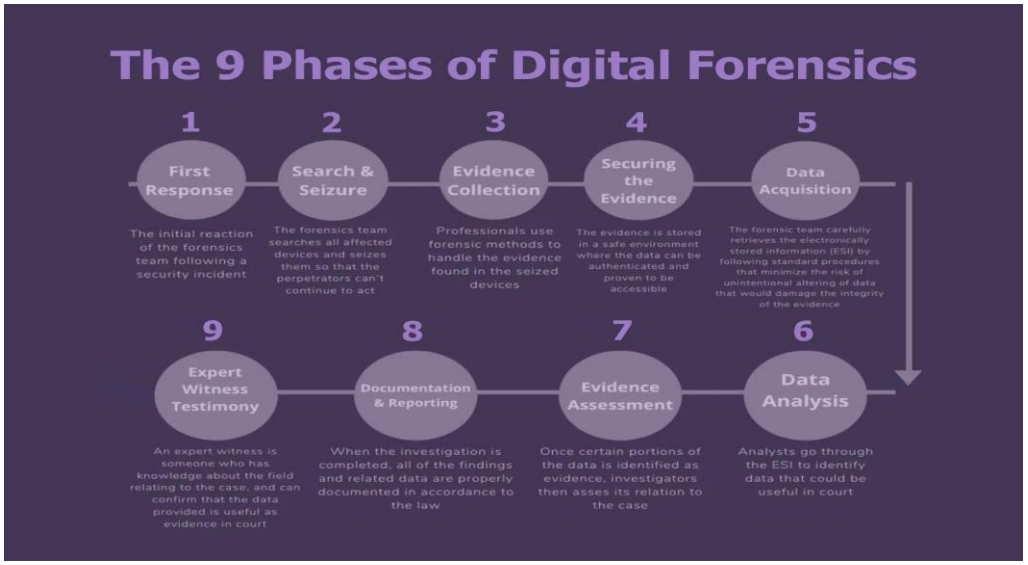
Beyond these challenges, digital forensics lacks a unified, formal representation of standardized procedures and knowledge for analyzing and gathering digital artifacts. This results in compatibilityissues and conflicts among various forensic tools. Errors in interpretation and analysis arise when standardized procedures are absent, leading to inconsistencies.
Furthermore, forensic experts often overlook documenting their work, hindering training and externalreviews. Leveraging past knowledge and experience is essential for training new digital forensic personnel and promoting knowledge sharing among investigative communities. Failure to adhere to legal practices exacerbates the threats to digital forensic investigations.



CONCLUSION

Digital forensics emerges as a multi-disciplinary and inter-disciplinary field, bridging diverse disciplines such as criminology, law, ethics, computer engineering, ICT, computer science, and forensic science. Its essence lies in uncovering and interpreting electronic data to preserve evidence in its original form. While still in its nascent stage, increased awareness has propelled digital forensics into a developing field undergoing a transition from an obscure tradecraft to a scientific discipline held to stringent standards. With the advent of next-generation forensic analysis systems and the integration of digital forensics courses in academic curricula worldwide, the field is poised for further advancement. Notably, organizations like the Digital Forensic Research Workshop (DFRWS) have played a pivotal role in driving research and

development in digital forensics, hosting annual workshops dedicated to its progression since 2001.



REFERENCE

[1] I. Resendez, P. Martinez, and J. Abraham, "An Introduction to Digital Forensics," June 2014, https://www.researchgate.net/publication/228864187_An_Introduction_to_Digital_Forensics

[2] N. Kumari and A. K. Mohapatra, "An insight into digital forensics branches and tools," *Proceedings of the International Conference on Computational Techniques inInformation and Communication Technologies*, 2016.

[3] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *International Journal of DigitalEvidence*, vol. 1, no. 3, Fall 2002.

[4] *Computer Crime: Forensic Science, Computers and the Internet*. San Diego,CA:Academic Press, 3rd edition, 2011, chapter 1.

[5] "Digital forensics," *Wikipedia*, the free encyclopedia,https://en.wikipedia.org/wiki/Digital_forensics