IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Role And Implementation Of Digital Evidence Systems In Cybercrime Investigation

[1]ShashankGole,[2]Dr.DhirendraKumarTripathi

[1]ResearchScholar,[2]AssistantProfessor

[1]ComputerScienceDepartment,[2]ComputerScienceDepartment

[1]MansarovarGlobalUniversity,Bhopal,India,[2]MansarovarGlobalUniversity,Bhopal,India

Abstract:

This paper explores the critical role of digital evidence systems in cybercrimeinvestigation, emphasizing their importance in identifying, analysing, and prosecuting cybercrimes. Cybersecurity, defined as the protection of networks, devices, and data from unauthorized access and attacks, is increasingly challenged by the complexity of cybercrime, which encompasses a wide range of illegal activities facilitated by digital technologies. The paper outlines the components of digital evidence systems, including identification, collection, acquisition, preservation, analysis, and reporting, highlightingthe need for a systematic approach to handling digital evidence. Furthermore, it discusses the implementation of thesesystems, focusingon thenecessity of training law enforcement personnel, standardization of procedures, collaboration among agencies, privacyprotection, and adherence to legal standards. The findings underscore that effective digital evidence systems are essential for modern cybercrime investigations, ensuring that justiceis served while safeguarding individual rights.

Keywords: Cyber Security, Cybercrime, Digital, Digital evidence, system, e-mail spoofing, cyber-attacks, fraud.

Introduction

The term “Cyber Security” According to Digital Guardian “Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.” Cybersecurity involves securing applications by identifying, correcting, and preventing security vulnerabilities, including regular updates and protective measures. According to IT Governance “Cybersecurity is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks.” Kaspersky Says “Cybersecurity focuses on keeping software and devices free of threats, with a compromisedapplicationpotentiallyprovidingaccesstothedatait'sdesignedto protect.”Cloud security focuses on protecting cloud-based assets and services, including applications, data, and infrastructure, with a shared responsibility model between organizations and cloud service providers.

AnIntrusionDetectionSystem(IDS)isasecuritytechnologythatmonitorsanetworkor

system for malicious activity or policy violations, alerting administrators to potential threats.

Intrusion detection systems detect inappropriate, incorrect, or anomalous activity on a network or computer system. Intrusion prevention systems build on intrusion detection systems to detect attacks on a network and take action to prevent them from being successful. Security event correlation tools monitor and document actions on network devices and analyse the actions to determine if an attack is ongoing or has occurred. Computer forensic tools help us to identify, preserve, extract, and document computer- based evidence that are used in cybercrime.

The digital age has brought about a significant transformation in the way crimes are committed andinvestigated. Cybercrime, in particular, has becomeamajor concern for lawenforcementagenciesworldwide,withtherapidgrowthoftheinternetanddigital technologies providing new avenues for criminals to exploit. Digital evidence plays a crucial role in cybercrime investigation, as it provides investigators with valuable information to identify, analyze, and prosecute cybercrimes. This paper explores the concept of digital evidence systems and their implementation in cybercrime investigation. The increasing complexity ofcybercrime cases has led to the emergence ofdigital evidence systems as a vital tool in modern investigation. Digital evidence systems refer to the collection, preservation, and analysis of digital data, such as emails, chat logs, andsocial media communications, to aid in the prosecution of online crimes. This paper will examine the role and implementation of digital evidence systems in cybercrime investigation, highlighting their effectiveness and limitations.

Digital Evidence and Its Importance in Cyber crime Investigation

Digital evidence refers to any data stored or transmitted in digital form that can be used as evidence in a legal proceeding. It can include emails, text messages, social media posts, internet history, computer files, and any other digital data that can provide information relevant to a criminal investigation. The importance of digital evidence in cybercrime investigation cannot be overstated, as it provides a wealth of information that can help investigators identify suspects, establish motive, and reconstruct the sequence of events leading up to and following a crime.

Literature Review

Cybercrime is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognized by the Information TechnologyAct in different countries. There are number of illegal activities which are committed over the internet by technically skilled criminals. Taking a wider interpretation, it can be said that, Cybercrime includes any illegal activity where computeror internet is eithera toolor target orboth. Cybercrime is anuncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber-defamation etc.Some conventional crimes may also come under the category of cybercrimes if they are committed through the medium of computer or Internet.

Cybercrime can be categorised as crimes exclusive to internet and use of computer and traditional crimes. Crimes such as stalking, harassing, fraud orscam committed using social media such as Facebook, Instagram, Twittercan be regardedas traditional crimes which are committed entirely in new ways. Criminal acts done by using electronic communicationsand information systems are generally considered as cybercrime which consists of a variety of criminal acts. It can be individual acts as well as state sponsored cybercrime. There is no definition of cybercrime which has been accepted globally. However, the term cybercrime has been used to describe a range of crimes excluding traditional crimes but crimes committed using the computer network system. Because of the complexity of the nature of crime, a single act of cybercrime can cause overly high damages. Cybercrime currently contributestothe highest percentage of all crime. Historically,legislationhas been used asa way to combat the challenges posed by cybercrime. For instance, the United States and European Union have legislation in an effort to deal with cybercrime.

Cybercrime is growing and current technical models to tackle cybercrime are inefficient in stemming the increase in cybercrime. This serves to indicate that further preventive strategiesarerequiredinordertoreducecybercrime.Justasitisimportanttounderstand the characteristics of the criminals in order to understand the motivations behind the crime and subsequently develop and deploy crime prevention strategies, it is also important to understand victims, i.e., the characteristics of the users of computer systems in order to understand the way theseusers fall victim tocybercrime. Current erais toofast to utilize thetime factorto improve theperformance factor. It isonly possible due the useof Internet. The term Internet can be defined as the collection of millions of computers that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone appreciates the use of Internet but there is another side of the coin that is Cyber Crime by the use of Internet.

Particularly noteworthy were the highest occurrences of fraud observed in the loanportfolios of Indian banks over the past two years (RBI, 2023). The financial repercussions were significant, with banks reporting substantial loan-related fraud totalling Rs 28,792crore in the fiscal year 2022–23. Simultaneously, the increase in white-collar crimes within thedigitalrealm,asevidencedbyactivitiessuchasmoneylaundering, mortgage fraud, financialinstitution fraud,andsecuritiesandcommodities fraud, presents a substantial threat. Recent legal proceedings in India during 2023, specifically cases such as Enforcement Directorate v. Aditya Tripathi (Rajasekaran and Korada, 2024), underscore the gravity of this issue. Such fraudulent activities contribute to substantialfinanciallossesfor victims and underminepublic trust in institutionssuch as law enforcement agencies and the associated online banking services.

Components of Digital Evidence System

Identification

In the identification phase, preliminary information is obtained about the cybercrime case prior to collecting digital evidence. This preliminary information is similar to that which is sought during a traditional criminal investigation. The investigator seeks to answer the following questions:

- Whowasinvolved?
- Whathappened?
- Whendidthecybercrimeoccur?
- Wheredidthecybercrimeoccur?
- Howdidthecybercrimeoccur?

The answers to these questions will provide investigators with guidance on how to proceed with the case.

Collection

With respect to cybercrime, the crimescene isnot limited to thephysical location of digital devices used in the commissions of the cybercrime and/or that were the target of the cybercrime. The cybercrime crime scene also includes the digital devices that potentially hold digital evidence, and spans multiple digital devices, systems, and servers. The crime scene is secured when a cybercrime is observed, reported, and/or suspected.

SlNo	DigitalDevice	PotentialEvidence
1	ADesktopComputer	The device contains all the files andfolders stored including deleted files and information which may not be seen normally. Analysis of key document files like word documents, excel files, email‘s tallydatamayhelpinunearthingpotential evidences. Retrieval of deleted files using Cyber Forensics can help get keyevidences that have been destroyed.
2	PenDrives	The device stores many files and may be hidden easily. In many cases the parallel books of accounts maintained as tally data orexcelsheetsarekeptinPenDrivesthat canbeeasilyhidden
3	HardDrives	The device stores many files and may be hiddeneasily. Backup of earlier years may be kept and may be easily hidden.

4	Handheld Devices like Mobile Phones (Smart Phones), Electronic Organizer, IPAD, Personal Digital Assistantetc	Much information can be obtained fromthe devices like Address Book, Appointment calendars/information, documents, emails, phone book, messages (text and voices), video recording, email passwords etc. Many applications like CHAT, WhatsApp application can store many crucial conversations important for the investigations. Remittances and transactions are done by fund transfer through mobile phone service providers utilizing money deposited with the latter bypassing banking channels. Apersonmaydoallhisbusinessthrough a mobile phone without any computer or laptop or warehouse for his inventory – as example, online business platform www.amazon.com maintains huge warehouseatseveralplaces in India where online traders can store their merchandise. In such cases the trader may make all transactions through mobile phone and storeinsmallexternalmicrochips makingdetectiondifficult.
5	Smart cards, Dongles and Biometric Scanners	Thedeviceitselfenablestounderstandthe userlevelaccesstovariousinformation and places.

6	Display Monitor (CRT/LCD/TFT etc), Screens of Mobile Phones if switched on	Allthegraphics andfiles thatareopenand visible on the screen in the switched-on systems can be noted as electronic evidence. This evidence can be captured only in video, photographs and through description in seizure memos
7	AnsweringMachines	The device can store voice messages and sometimes, the time and date information about when the message was left. It may have details such as last number called, memos, phone numbers and names, caller identificationinformationandalsodeleted messages.
8	LocalArea Networks (LAN) Card or Network Interface Cards	The device itself is a digital evidence and may contain crucial evidences
9	Modems, Routers, Hubs and Switches	ThedevicemaycontaindetailsofIP addresses where the actual data is stored.
10	Servers	Contains crucial data on business related applications like SAP, ERP, CRM, Mail Servers.The device is a potential evidence for pulling out audit logs using forensic analysis.Analysisofemails of keypersons fromMailServerscanhelpinfinding crucialevidencesrequiredforthecase.
11	Removable storage devices like SD Cards in Mobile phones	All new generation phones use these and store filesinwhichevidence canbe found.

12	ScannersandCopiers	The device itself, having the capability to scan may help prove illegal activity like making bogus bills etc. Copiers may also contain stored data which can be crucial evidences.
13	DigitalCameras	The device can be looked for images, videos, sounds, removable cartridges, time and date stamps
14	Pagers	The device can be looked for address information, Text message and phone numbers
15	CD/DVDs/	The devicestoresmany files whichmay contain the evidence
16	FacsimileMachines	The device stores some documents, phone numbers, send/receive logs that cancontain the evidence.
17	Global Positioning Systems (GPS)	The device may provide travel logs, home location,previousdestinationsetcwhich maybecrucialinfindingplaceswhere evidences may be stored.
18	CloudDataServers	Thedevice isavailableonallsmartphones and tablets. The Cloud may be used to store hidden data where crucial evidences may be stored. Some enterprises offer service for storage of commercial data in servers located in foreign countries and business data are stored there through internet–

		whichcanbeaccessedasper termsandconditions.

Table4.2.1–TypesofDigitalEvidenceDevices

From the digital devices, two types of evidences are possible, one is persistent evidence and other is volatile evidence:

- Persistent evidence: the data that is stored on a local hard drive and is preserved when the computer is turned off. For example, Documents (word, slide, sheet, pdf), Images, Chat log, Browser history, Registry, Audio/ Video, Application, Email, SMS/ MMS, Phonebook, Call log.

- Volatile evidence: any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. For example, Memory, Network status and connection, Process running, Time information it is to be noted that in certain cases, where volatile evidence is crucial, switching off a switched-on system may result in destruction of volatile evidence.

Acquisition

Different approaches to performing acquisition exist. The approach taken depends on thetype of digital device. For example, the procedure for acquiring evidence from a computer hard drive is different from the procedure required to obtain digital evidence from mobile devices, such as smartphones.

Preservation

Evidence preservation seeks to protect digital evidence from modification. The integrity of digital evidence should be maintained in each phase of the handling of digital evidence (ISO/IEC 27037). First responders, investigators, crime scene technicians, and/or digital forensics experts must demonstrate, wherever possible, that digital evidence was not modified during the identification, collection, and acquisition phase; the ability to do so, of course, depends on the digital device (e.g., computer and mobile phones) and circumstances encountered by them (e.g., need to quickly preserve data).

AnalysisandReporting

In addition to the handling of digital evidence, the digital forensics process also involves the examination and interpretation of digital evidence (analysis phase), and the communicationof the findings of the analysis (reporting phase). During the *analysis* phase, digital evidenceis extracted from the device, data is analysed, and events are reconstructed. Before the analysis of the digital evidence, the digital forensics analyst in the laboratory must be informed of the objectives of the search, and provided with some background knowledge of the case and any other information that was obtained during the investigation that can assist the forensics analyst in this phase (e.g., IP address or MAC addresses). Various forms of analyses are performed depending on the type of digital evidence sought, such as network, file system, application, video, image, and media analysis (i.e., analysis of data on storage device).

Implementation of Digital Evidence Systems

In Cybercrime Investigation The implementation of digital evidence systems in cybercrime investigationrequiresacoordinatedeffortbetweenlawenforcementagencies,forensicexperts, and other stakeholders. The following are some of the key considerations for implementing digital evidence systems.

Training

Law enforcement agencies must provide training to their personnel on digital evidence collection, analysis, and presentation. This training should be ongoing and updated regularly to keep up with the latest technologies and techniques.

Standardization

Digitalevidence systems must bestandardizedto ensure thatevidence is collected,analysed, and presentedin aconsistentandreliablemanner.Thisincludestheuse ofstandardizedtools, procedures, and reporting formats.

Collaboration

Cybercrime investigation often requires collaboration between multiple agencies andexperts. Digital evidence systems must be designed to facilitate collaboration andinformation sharing.

Privacy

Digitalevidence systems must be designed toprotect individualprivacyrights.This includes ensuring that only relevant data is collected and that data is handled and stored securely.

5.4LegalConsiderations

Digitalevidence systems must be designed tocomplywith legal requirements and standards. This includes ensuring that evidence is collected and analysed in a forensically soundmanner and that proper chain of custody is maintained.

Conclusion

Digital evidence systems play a critical role in cybercrime investigation, providing investigators with valuable information to identify, analyse, and prosecute cybercrimes. The implementation of digital evidence systems requires a coordinated effort between law enforcement agencies, forensic experts, and other stakeholders. By providing training, standardization, collaboration, privacy, and legal considerations, digital evidence systemscan help ensure that cybercrime is investigated effectively and efficiently, while protecting individual privacy rights and maintaining the integrity of the legal system.

2. References

[1] Goni, O.,Ali, M. H., Showrov, M. M.A., &Shameem,M.A. (2022). The basic concept of cyber crime. Journal of Technology Innovations and Energy, 1(2), 16-24.

[2] Khan, S., Saleh, T., Dorasamy, M., Khan, N., Tan Swee Leng, O., & Gale Vergara, R. (2022). A systematic literature review on cybercrime legislation. F1000Research, 11, 971. https://doi.org/10.12688/f1000research.123098.1

[3] Goni, O. (2022). Cyber crime and its classification. Int. J. of Electronics Engineeringand Applications, 10(1), 17.

[4] Sarkar,G.,&Shukla,S.K.(2024).Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. Journal of Economic Criminology, 4, 100063.

[5] Chougule, H., Dhadiwal, S., Lokhande, M., Naikade, R., & Patil, R. (2022). Digital Evidence Management System for Cybercrime Investigation using Proxy Re-Encryption and Blockchain. Procedia Computer Science, 215, 71–77. https://doi.org/10.1016/j.procs.2022.12.008