IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Bytes By Bytes: Unmasking Digital Shadows In Forensic Investigations

Kadam Vijay[1], Mr. Parth Lakhalani[2,] Kiranbhai R Dodiya[3]

1 Student, Department of Forensic Science, PIAS, Parul University, Vadodara, Gujarat, India.
2* Mr Parth Lakhalani is a Research Scholar and Student at IU International University of Applied Sciences in Berlin, Germany.
3 Research scholar, Department of Biochemistry & Forensic Science, Gujarat University, Ahmedabad, Gujarat, India.

Abstract: -Cyber-attacks represent a pervasive threat in the digital age, with perpetrators leaving behind digital artefacts that can potentially unveil their identities and behaviours. In response, forensic agencies and law enforcement departments leverage an array of digital forensic toolkits, both commercial and open-source, to examine digital evidence comprehensively. This research survey, a comprehensive and in-depth study, is a comprehensive overview of the current state-of-the-art digital forensics concepts, identifying research gaps, introducing different computer forensic domains and toolkits, and offering a comparative analysis to aid investigators in tool selection during forensic processes. It also pinpoints current challenges and suggests future research directions in computer forensics. The field of digital forensics is multidimensional, encompassing various domains such as network forensics, memory forensics, and mobile forensics. Each domain presents unique challenges and requires specialised toolkits tailored to effectively extract and analyse digital evidence. The survey, designed to provide a nuanced understanding of the forensic landscape, aims to equip investigators with a comprehensive view of these domains and the corresponding toolkits. Commercial and open-source digital forensic toolkits are pivotal in evidence acquisition, analysis, and presentation. While commercial solutions often offer comprehensive features and user-friendly interfaces, open-source toolkits provide flexibility and customisation options. Through a detailed examination of these toolkits, the survey aims to empower investigators with insights into their capabilities and limitations, enabling informed decision-making during the forensic process. Moreover, the survey includes a comparative analysis of toolkit characteristics, such as scalability, reliability, and compatibility with operating and file systems. This comparative framework, a comprehensive guide, facilitates the selection of appropriate toolkits based on the specific requirements of each forensic investigation, thereby enhancing efficiency and efficacy. In addition to providing an overview of existing

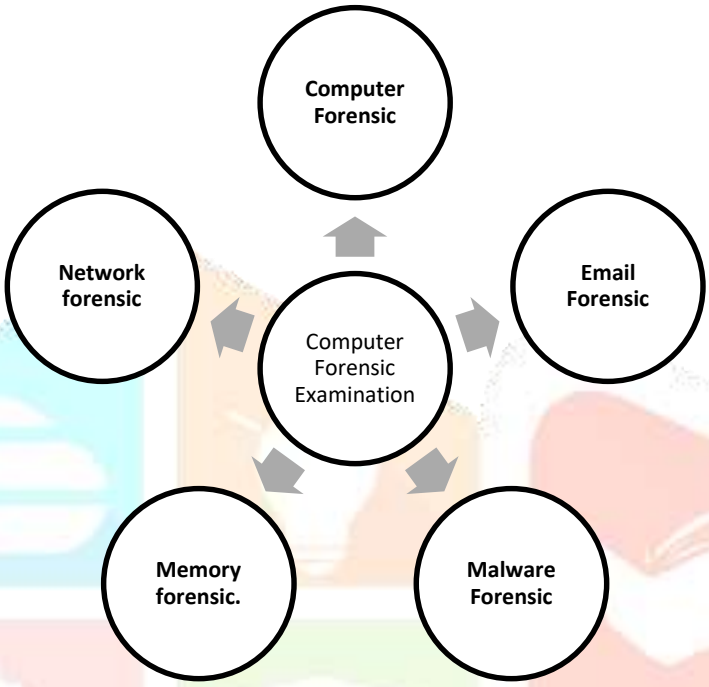
digital forensic practices, the survey identifies research gaps and challenges in the field. These challenges encompass technological limitations, legal and ethical considerations, and the evolving nature of cyber threats. By acknowledging these challenges, the survey encourages further research and innovation to address emerging issues and enhance the effectiveness of digital forensic investigations. Furthermore, the survey delineates future research directions, emphasising areas such as the integration of artificial intelligence and machine learning techniques into digital forensic processes, the development of standardised procedures and protocols, and the enhancement of forensic readiness in emerging technologies such as Internet of Things (IoT) and cloud computing. In conclusion, the proposed research survey is a comprehensive tool that aims to provide a comprehensive overview of digital forensics, identifying current practices, research gaps, and challenges. By offering insights into different forensic domains, toolkits, and comparative analysis, the survey empowers investigators to navigate the complex landscape of digital evidence examination effectively. Moreover, by identifying future research directions, the survey contributes to advancing the field and developing innovative solutions to combat cybercrime.

1. INTRODUCTION

Computer forensics is the branch of digital forensics, which generally includes digital forensics, which involves preservation, extraction, identification, analysis of data, and generating a report. Whenever a crime is related to cyberspace, then it is called cybercrime. Acquiring, protecting, retrieving, and presenting material that has been processed electronically and saved on computer media" isone definition of computer forensicsThe most recent instance is a hack in Baltimore, Maryland, where attackers stole a National Security tool and affectedthousands of freezing of systems the three-week attack caused disruptions because emails, property transactions, utility bills, health warnings, and many additional services. The annual price of pain is increasing quickly; scientists have forecasted that it will escalate to $6 trillion by 2021**.** It is possible to retrieve computer forensic evidence from programmers, databases, websites, and emails. In the current technological era, evidence is gathered via various hardware components, including memory cards, smart cards, dongles, cameras, and biometric devices—printers, pagers, scanners, answering machines, routers, a n d GPS systems. We examine crucial traits in our investigation for the forensic analysis of gathered evidence. Forensic planning for preparation, collecting evidence, following protocols, safeguarding the integrity of the evidence and forensic law Investigations are outside the purview of this study. However, a forensic tool would be an excellent option if it is adaptable enough to function with many platforms and operating systems and can examine many file systems, the extensibility to using scripting languages to automate tedious automation of essential processes and features, and offers adequate product support. Typically, a forensic toolbox would be more beneficial in providing more features in a single product or suite and support for several platforms. Investigators can benefit from carefully and in-depth studying each tool's features. Select the investigational instrument that will save you the most time and effort in the investigation. Since everything is digital today, criminals use contemporary technology to attack governments, businesses, and people. The ever-popular smartphone today has storage space comparable to a laptop and is frequently used as a mobile workplace, social network, and entertainment hub in one simple, handy gadget. A

smartphone is a mobile device with more connectivity possibilities than a cellular phone, sophisticated computational capabilities, and the capacity to run mobile applications. Mobile device technology and storage capacity have increased dramatically. Due to their capabilities and features, mobile devices have evolved over the past ten years into data repositories that can hold much data[9].

1.1 Recent advancement in computer forensic Investigating tools and techniques: -



FFigure 1 Types of computer Forensic Examination

There are various types of computer forensics

The types of computer forensic examinations include the following types

1. Computer Forensic-Computer forensics is the branch of digital forensics that legally deals with the evidence associated with the computer system. This mainly includes data recovery from a crime scene or a live system in a forensically sound manner, making the evidence admissible in legal proceedings[8].

2. Email Forensic-E-mail forensics refers to the investigation of the source and content of an email message, including verification of the actual sender and receiver, the time and date the message was transmitted, and other related information. A forensic investigation of an email communication aims to discover all affected parties and the history of the message[7].

3. malware forensics- Malware forensics identifies, studies, and investigates various malware characteristics to identify the attackers and the reason for the assault. The method also entails steps like inspecting the malicious code, figuring out how it entered the system, how it spread, what effect it has on the system, what ports it tries to utilise, etc. Using a range of tools and techniques, investigators conduct forensic analysis

3.1 Types of Malware Forensic (Malware Analysis)

1. Static analysis
2. Dynamic analysis (Behavioral Analysis)
3. Code analysis
4. Memory analysis (Memory forensics)

4. Memory forensics involves collecting information stored in the device's random access memory (RAM) and dealing with catch data, hard disk, and pen derive. It also consists of investigating mobile devices to retrieve and examine the data they hold, including contacts, outgoing and incoming text messages, image and video files, and other data.[6]

Forensic Importance of the Memory Forensic

1. A device's persistent functioning
2. Dump data analysis
3. Device attached to the particular system
4. Executable code, open port IP address,
5. file access, network details, and user login data.[15]

5. Network forensics. The scientific field of network forensics collects, retrieves, and examines network events to pinpoint the source of security breaches. This phenomenon functions as a tool for investigations when it occurs and helps identify unauthorised access to computer network systems[1].

Types of Network Forensic

1. Network Traffic.
2. System that detects intrusions.
3. Risk Management.

2. Tools used in computer Forensic Investigation

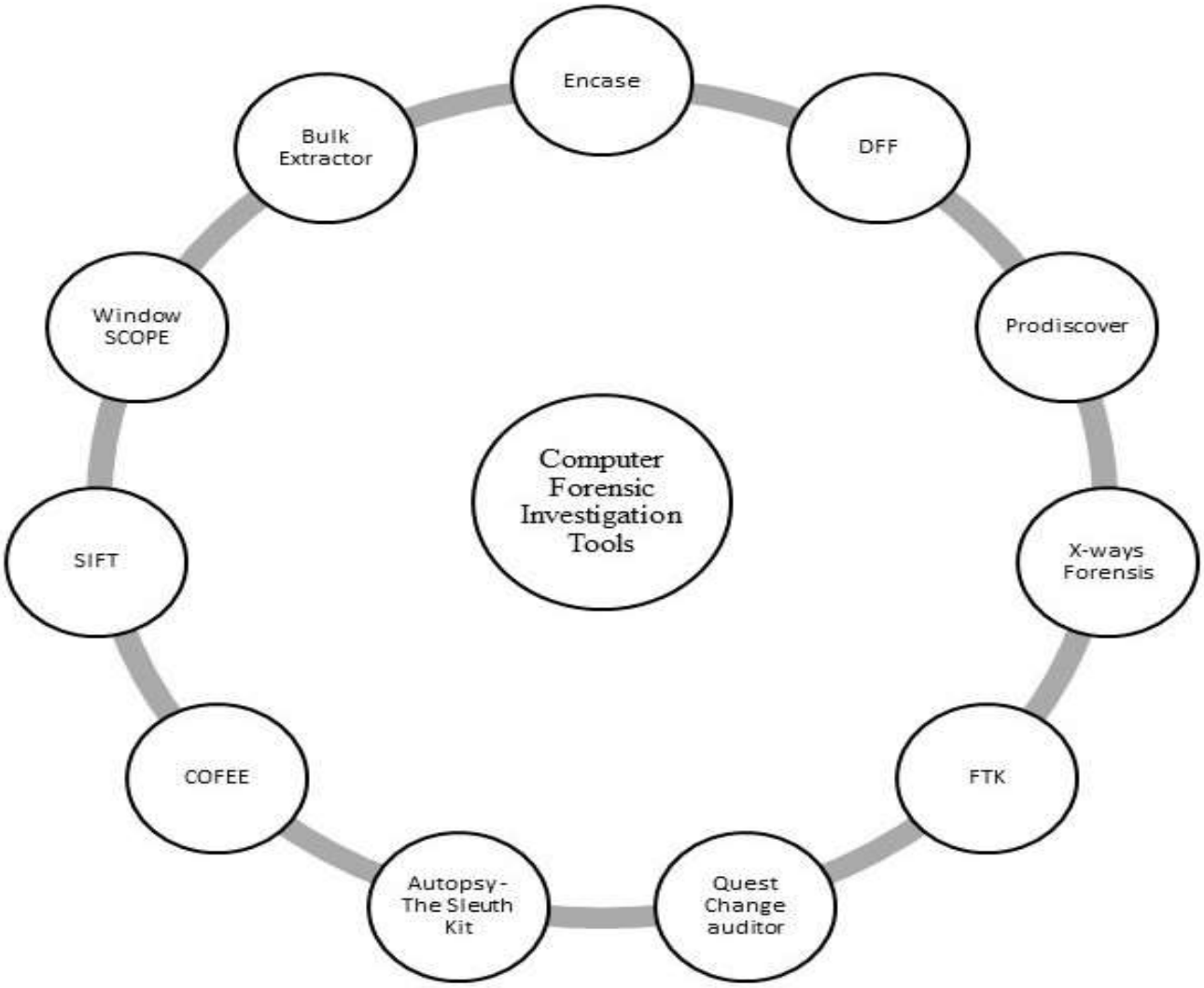


Figure 1 computer Forensic Investigation Tools

A) ENCASE: This Encase software is created using the guidelines software. It is commonly used by the commercial sector and law enforcement organisations as one of their most vital instruments. This software program is used by all law enforcement organisations (100%) and by consumer goods corporations (90%), banks (93%), and colleges (75%). This program is capable of research, data collection, analysis, and report generation. It can collect data from mobile devices, networks, and the cloud, among other sources[5].

1) Comprehensive reporting on results that preserve the authenticity of the data

2) Hash values, keywords, and metadata are used.[1]

3) Memory acquisition

4) It performs Disk Imaging

5) Encase Forensic Imager can be run through a USB drive and acquire live system data.

6) Data Carving can be performed with the help of Encase software.

7) Password Recovery

8) Data collection and processing

B) DFF- Digital Forensic Framework -A free-to-download computer forensics system called Digital Forensics Framework was developed on top of a particular API. Users may use it to investigate computers, restore deleted files, look for classified information, and more**.** A GUI programmer called Digital Forensics Framework provides a conventional tree view in addition to various functions such as recursive viewing and live search. This enables you to perform digital investigations from the remote. Furthermore, it is a command-line tool with many widely used shell features, including completion, task management, globing, and keyboard shortcuts. DFF may be used straight from a Python interpreter by advanced users and developers to script their study.[4]

C) PRODISCOVER BASIC: Discover is a premium program, but the basic edition is free. It can collect information and evaluate the circumstances surrounding any security breach or data leak. It consists of Boolean search, malware-finding hash sets, automatic reporting, and the inspection and scanning of hardware-protected locations. It may be constructed for analytical purposes by combining several applications into a single application. Prodiscove Forensic was founded by the ARC Group of New York[1].

D) XWAYS FORENSICS: Xway Forensic is a commercially available proprietary tool. Features like Win Hex and Disk Imager are included in this integrated program. The characteristics of this tool are given below.

1) Recovery of passwords.

2) Imaging of disks.

3) The original compressed file may be decompressed for examination.

4) Files may also be carved within other files[1].

5) It also provides tools to recognise known photographs, such as photo DNA hashing.

6) Multiple hash values may be computed concurrently[1].

7) It can access the entire disk, RAIDs, and images [1].

E) FTK (Forensic Tool kit) - It also integrates software made by the access data group. It can collect and store information from 3,500 mobile devices throughout the network. It can quickly identify missing information, vindictive behaviour, and data theft. Let's say data is kept in a location other than the FTK, which can determine who created the original and how it got there. Has moved, and even mention any changes if the original has undergone modifications. If any data has been transmitted from the system or mobile device, it can quickly identify it. Even when performing static analysis, it can collect data. FTK can be launched from a USB disc. [3]It offers the choice of expert review, which involves reviewing and shall be carried out and assessed against the witness on the final data evaluation. Password restoration FTK Imager is used to perform disc imaging. Boolean operations and Hashing techniques are used to search results. The forensic officer might also utilise the FTK Internal viewer in Word, PowerPoint, and Excel. It is capable of examination of emails. It is multilingual. When exporting the proof, the customer can use the PDF or TIFF format[1].

F) Quest change auditor: This tool's primary goal is to provide complete visibility while tracking real-time analysis. It generates a report and can detect insider threats quickly. It can detect whether an item has changed; it displays the evolving and prior values and allows you to return to them with previous clicks.

[1]. Paths for the investigation are dynamic. Can perform a comprehensive text search, saving time spent determining which files have been altered[14]

G) Autopsy (sleuth kit): The Sleuth Kit offers disk image analysis and file recovery features. The investigator can analyse data from the volume and file systems. Law enforcement, the military and corporate examiners all frequently employ it. This plug-in architecture enables adding other modules to develop automated systems and evaluate file contents. The command-line tools can be used directly to look for evidence, and the library can be included in more thorough digital forensics programs. The Sleuth Kit and other digital forensics tools can be accessed through an autopsy, a platform for digital forensics. The Sleuth Kit and Autopsy are free utilities with Windows, Linux, OS X, and other UNIX platforms. Collaboration, online artefact analysis, email analysis, registry analysis, and support for Android are some of this kit's standout features[2]

H) Computer Online Forensic Evidence Extractor (COFEE): Microsoft developed a computer forensic toolkit to extract evidence from the windows. It can deal with live system analysis. It is not available to everyone. It is only available to law enforcement agencies. Microsoft now collaborates with the National White-Collar Crime Center and Interpol[1]. The device's command line software, which may collect evidence, supports over 150 commands and removes the need to remove the computer from the scene. Passwords may be cracked, and computer data and Internet activity can be examined using the instructions. This method has the advantage that data may be examined while the laptop is still connected to the Internet or a network, which is not feasible if the laptop is taken into custody[1].

I) SANS Investigative Forensic Toolkit (SIFT): It was created by an international group of specialists. One Of the most popular open-source forensic tools is this one. It was found to be an incident response workstation and subsequently made accessible to everyone. SIFT have the following characteristics: it can do real-time analysis. It is capable of swift report and analysis. It can recognise malware. It is capable of disk imaging. Reference Framework NTFS, fat12/16/32, ext2, 3, 4, UFS, and HFS are supported, and also VMware Appliance; it even promotes expert witness format[1].

(J) Windows Scope - Windows scope comes in useful while collecting data from electronic gadgets. The only tool that can reverse engineer is this one. This utility is GUI-based [1]. A bulk extractor is a useful tool that may retrieve important data, such as credit card numbers, web addresses, network connections, email addresses, phone numbers, and URLs, from evidentiary hard drives or files found during forensics investigations. It also helps with data theft and cyber-investigation, as well as assessing pictures or viruses. The Windows Scope software offers the following functions. a disk image, a file, or a directory containing files are examined without scanning in order to retrieve pertinent data.Bulk extractor is superior to other forensic tools in terms of speed and completeness.

(K) Bulk ExtractorForensic instruments appropriate for Windows, Linux, and macOS are bulk extractors. (Extractor Bulk.)] It is capable of doing disk imaging, email analysis, live analysis on any platform, data recovery, data carving, and password recovery with the use of a bulk extractor[1].

3. COMPARATIVE STUDY OF THE SOFTWARE

NO	Categoryo	EnCase	FTK	Autopsy
1.	Cost	commercial	Free	Free
2.	License	Proprietary	Open	Open
3.	Uses MD5 Hash	Runs a search first then yes	Yes	Yes
4.	Uses SHA1 Hash	No	Yes	Yes
5.	Shows hash for individual file	Runs a search first then yes	Yes	Yes
6.	Can verify image integrity	Yes	Yes	Yes
7.	Find deleted files	Yes	Yes	Yes
8.	Identify deleted files clearly	Yes	Yes	Yes
9.	Recover deleted files	If not overwritten , Yes	If not overwritten Yes	If not overwritten Yes
10.	Find encrypted files	Yes	Yes	Yes
11.	Identify encrypted files clearly	No	Yes	No
12.	Identify file extension mismatches	Yes , after search or selection of “conditions Renamed extensions “	Yes	Run a “Sort By File Type “then Yes
13.	Can search for strings (ASCII and Unicode)	Yes	Yes	Yes
14.	Include HEX level viewer	Yes	Yes	Yes

4. Challenges and issues in computer forensics with tools and techniques.

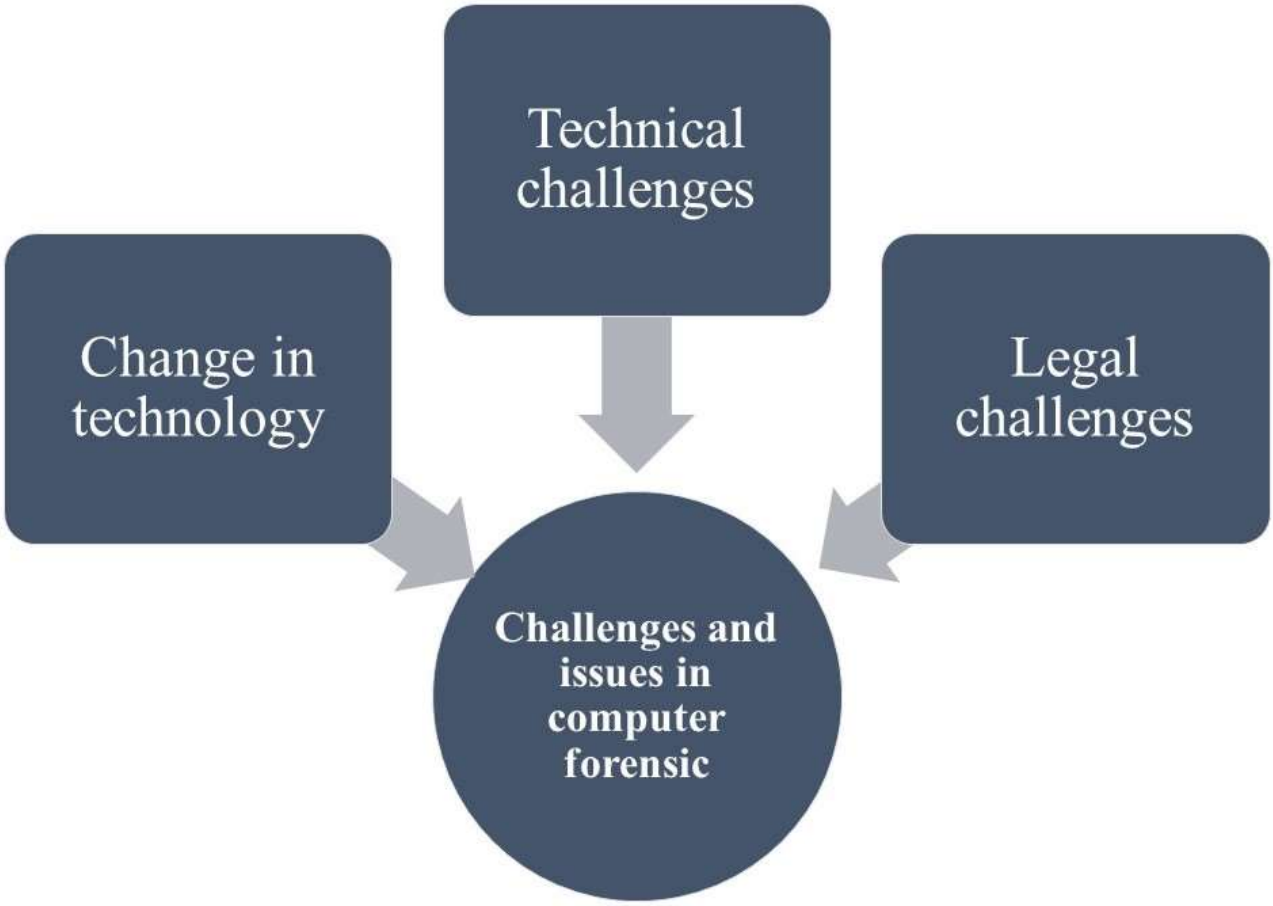


Figure 3 challenges and issue in computer forensic

Many important computer forensics programs, including EnCase, FTK, look, Sleuth Kit, and Win Hex, have been successfully attacked. Aside from programs that write to file slack, change file signatures, and flip bits to avoid hash set detection, programsthat tinker with FAT directories, NTFS master file tables, and ext. Have been aroundfor years. Forensic software developers do not produce goods that are adequately guarded against defects such as stack overflows, poor memory page management, and unsafe exception handling leakage. Users of forensic software do not evaluate the products they buy using rigorous enough standards. In truth, most computer forensics labs buy the software that "everyone else" uses without independently testing dependability, completeness, and authenticity, especially as new software becomes available. Releases of the software versions occur[10].

change in technology- Nowadays, digital evidence is becoming more challenging due to the rapid change in technology, including operating systems, application software, and hardware, because newer versions of software do not support older versions, and software development companies do not provide any backward compatibles. This has legal ramifications. Electronic document integrity, secrecy, and accessibility can all be easily compromised. Wide-area networks and the internet create a vast network that enables data to move beyond physical boundaries. Due to the ease of communication and accessibility of electronic documents, there is a surge

in the volume of data, making it more challenging to find the original and pertinent material[11].

4.2 Technical challenges: As we know, technological advancement can be achieved day by day. As Technology develops, crime and criminals also develop. Digital forensic experts use forensic tools to collect shreds of evidence against criminals. Criminals use such tools to hide, alter, or remove their crimes' traces. Anti-forensics techniques are considered a significant challenge in the digital forensics world. Some Technical challenges are given below. Technical challenges include Data hiding in storage space, Encryption, and Covert Channels. Other technical challenges include Operating in the cloud, skill gaps, steganography, and Time to archive data[12].

Main technological challenges

a)Multiple media types

b)Encrypted communications

c)Anti-forensics

d)Obfuscation techniques.

e)Real-time gathering and analysis

4.3. Legal challenges: No guidelines or standards exist for working with or analysing digital evidence. The Indian Evidence Act of 1872 contains limitations or loopholes. Concerns about privacy while dealing with Admissibility in Courts, the Power to gather digital evidence, the preservation of electronic evidence analysed with a live computer system, and limited resources also exist[13].

4.5 Legal challenges: Issues with jurisdictional.

1. The absence of standard regulations causes legal problems.

2. Status as evidence in research.

3. Explain the method's known or potential error rate and whether the scientific community has generally accepted the concept or methodology Nilu Singh

Conclusion

Law enforcement agencies widely use the above-discussed forensic tools to analyse digital evidence to discover cyber threats or criminals. Advanced technology has become a challenging task for law and enforcement agencies. Also, lacking resources can be a significant problem when dealing with digital evidence. This review work will be helpful in the investigation agency to choosing the best tools for the investigation, and this work also gives the comparison of the different types of digital forensic software so that for the investigation purpose, it will become easy for the digital forensic expert to identify the best tools and techniques.

References

[1] A. W. a. B. Premchand Ambhore, *International Journal of Current Engineering and Technology*, 2018.

[2] [Online]. Available: https://www.brainbell.com/tutors/A+/Hardware/_Geometry.htm.

[3] [Online]. Available: http://www.cleardata-forensics.com/importance.html.

[4] [Online]. Available: https://www.boot-disk.com/manual/zdelete/Authoring/wipe-concepts.html.

[5] T. S. a. W. G. Joe Buchanan-Wollaston, "COMPARISON OF THE DATA RECOVERY FUNCTION OF FORENSIC
TOOLS," *IFIP International Federation for Information Processing*, 2013.

[6] A. T. S. Josiah Dykstra, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques," *J. Dykstra, A.T. Sherman / Digital Investigation 9 (2012) S90–S98.*

[7] D. M. V. K. C. K. R. S. Kambiz Ghazinour, "A Study on Digital Forensic Tools," *978-1-5386-0814-2/17/$31.00 ©2017 IEEE.*

[8] J. G. C. ,. G. B. D. M. S. K. D. K. Nicole Lang Beebe, "Post-retrieval search hit clustering to improve information retrieval effectiveness: Two digital forensics case studies," *N.L. Beebe et al. / Decision Support Systems 51* , pp. 732-744, 2011.

[9] V. K. S. a. V. Mane, "Comparative Study and Simulation of Digital Forensic Tools," *International Conference on Advances in Science and Technology*, 2015.

[10] T. A. S. P. Ioannis Lazaridis, "Evaluation of Digital Forensics Tools on Data Recovery and Analysis," *Proceedings of the Third International Conference on Computer Science, Computer Engineering, and Social Media*, 2016.

[11] S. R. a. S. V. Raghavan, "A Study of Forensic & Analysis Tools," *IEEE Louisville Chapter. 978-1-4799-4061-5/13.*

[12] P. A. a. Premchand Ambhore, "Disk based Forensics Analysis," *International Journal of Current Engineering and Technology* , 2018.

[13] Y. P. B. S. a. D. J. Manish Hirwani, "Forensic Acquisition and Analysis of VMware Virtual Hard Disks".

[14] D. R. K. a. N. Jain, "DIGITAL FORENSIC TOOLS: A COMPARATIVE APPROACH," *International Journal of Advance Research In Science And Engineering* .

[15] D. D. R. K. Nilakshi Jain, "A Comparative Study based Digital Forensic Tool:Complete Automated Tool," *The International Journal of FORENSIC COMPUTER SCIENCE.*