Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Advancements in Digital Forensics: Emerging Tools and Techniques

Vidyadhari Singh[1], Aditi Nikam[2], Rohitkumar G. Singh[3], Ditixa Mehta[4]
[1]*Associate Professor, Computer Science and Engineering (Cyber Security), Thakur College of Engineering and Technology, Mumbai, India*
[2]*Student, Computer Science and Engineering (Cyber Security), Thakur College of Engineering and Technology, Mumbai, India*
[3]*Associate Professor, Engineering Sciences & Humanities, Thakur College of Engineering and Technology, Mumbai, India*
[4]*Assistant Professor, Computer Science and Engineering (Cyber Security), Thakur College of Engineering and Technology, Mumbai, India*
Email: vidyadhari.singh@tcetmumbai.in

ARTICLE INFO

Received: 30 Dec 2024

Revised: 19 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

As cybercrimes become increasingly intricate and prevalent, digital forensics has established itself as an essential field for investigating, analyzing, and presenting digital evidence. This research examines the application of various digital forensic tools and methodologies in identifying, recovering, and analyzing digital data pertinent to criminal inquiries. The tools included in this comparative study are FTK Imager, iCare Data Recovery Pro, Autopsy, Mobiledit Forensic Express, and EnCase. The research focuses on assessing these tools based on their features, efficiency, user experience, and capacity to facilitate different phases of digital forensic investigations—specifically identification, collection, preservation, analysis, and documentation. Case studies from real-world scenarios have been analyzed to illustrate how these tools aid forensic analysts in recovering deleted information, examining mobile and computer systems, and supporting legal proceedings through meticulously documented digital evidence. The results indicate that each tool possesses distinct features that render it appropriate for particular situations. For instance, FTK Imager and EnCase excel in generating forensic images and conducting comprehensive analyses, while Autopsy is recognized as a robust open-source option for general investigations. Additionally, iCare Data Recovery Pro and Mobiledit are effective for data recovery and mobile forensics. In summary, this study enhances the understanding of forensic preparedness and response in cybercrime investigations.

Keywords: Digital Forensics, Cybercrime investigation, Forensic tool comparison, Data recovery, Evidence preservation

1. INTRODUCTION

Cybercrimes and attacks have increased globally, posing significant threats to both individuals and organizations. Cybercrime refers to criminal activities carried out by cybercriminals using computers, voice messages, SMS, and surveillance to steal sensitive data and credentials. These crimes can be categorized into four types: Individual Cybercrimes, Organizational Cybercrimes, Property Cybercrimes, and Societal Cybercrimes [1]. Among the various forms of cyberattacks, phishing, ransomware, identity theft, internet fraud, and hacking of computer networks are the most common [2]. Phishing, in particular, is the most frequent cyberattack, occurring daily in large numbers. In 2025, estimated $4.88M per phishing breach, social engineers are making billions by deceiving users. [3]. During the COVID-19 pandemic, the incidence of phishing increased by up to 220% [3]. It is estimated that 3 billion spam emails are sent to users every day [3]. Ransomware is also emerging as a growing threat to individuals and organizations. In 2025, approximately $4.8 billion per month ransomware attacks are reported [5]. worldwide. Additionally, incidents of data theft, hacktivism, and denial-of-service attacks are gradually increasing [1]. In India in 2023, 880,418 cybercrime complaints were reported, out of that $12.5 billion are the losses. [7]. California led the states in reported cases, followed by Texas and Florida [7].

In today's cybersecurity and investigation procedures, digital forensics is essential. As a branch of forensic science, it plays a crucial role in investigating cybercrimes by helping to identify victims and find important digital evidence [8].

It makes it easier to recover important and frequently private data from various digital storage devices, such as USB drives, laptops, and mobile devices. This skill is crucial for detecting and preventing criminal activity and recovering lost or hidden information. Moreover, digital forensic analysts make a substantial contribution to law enforcement by helping to resolve criminal cases and protecting against possible data loss [9]. Digital forensics also plays a key role in looking into data breaches and ensuring that people's privacy is protected according to the law and moral principles [9]. This can protect the infrastructure or national security because the government can use this framework to fortify itself against cyberattacks and threats while assisting with incident response technologies, system data recovery, crime detection and prevention, and legal and regulatory compliance.

In this study, we have explored a range of tools and techniques employed in digital forensic investigations. The results have been discussed in detail, leading to identifying the most effective tools suited for ensuring robust and secure practices in the cybersecurity domain.

2. METHODOLOGY

The field of digital forensics is enormous, and so is its significance. It aids in the investigation, analysis, and interpretation of data by giving digital forensic analysts and examiners the tools, processes, and frameworks. The Chain of Custody (COC), states that digital evidence must be treated appropriately and without modification from the time it is gathered until it is presented in court. It is regarded as the most significant document in digital forensics [8]. The Chain of Custody form must have the following information: the officer's name, the party, the digital device's label, and the information about who handled, collected, and, if any, transferred the device to another person [4].

The entire procedure of digital forensics is carried out in the following steps:

Step-1. Identification: Locating possible proof from sources such as network records, mobile devices, cloud storage and computer systems, identifying the type of cyber security violation, and setting the investigation's objectives.

Step-2. Collection: To gather information from the sources that have been recognized and to capture metadata. Preserve the gathered evidence safely to avoid unwanted access.

Step-3. Preservation: This involves guarding against potential evidence tampering. Utilizing writes blocks to ensure data integrity and producing forensic pictures of the information.

Step-4. Analysis: Finding the trends and connecting the information to comprehend the situation and evaluate outcomes.

Step-5. Presentation: Clearly and succinctly record the results.

3. TOOLS & TECHNIQUES USED IN DIGITAL FORENSICS

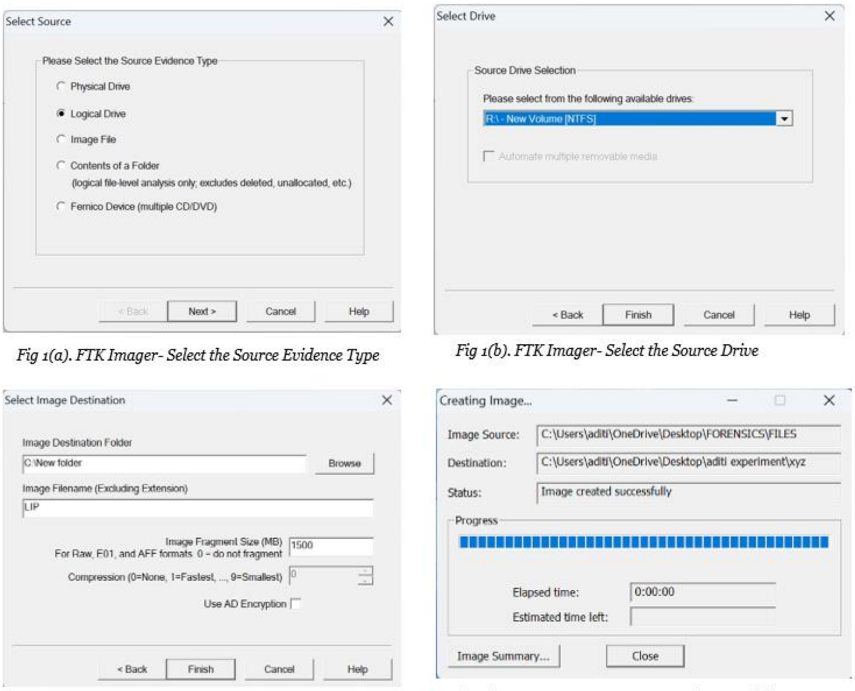
Applying specific tools and methods designed for various areas within the field is a crucial component of digital forensics. Computer forensics, mobile forensics, network forensics, and cloud forensics are some of these fields; they all deal with different kinds of digital evidence and call for different strategies.

In order to preserve and understand digital evidence, computer forensics uses programs like Volatility, FTK Imager, Autopsy, and EnCase to extract and analyze data from computers and storage media. On the other hand, data acquisition from smartphones and other portable devices is the focus of mobile forensics. Logical, physical, file system, and cloud acquisition techniques are frequently used, and programs like MOBILedit, Oxygen Forensics, Cellebrite UFED, and Belkasoft support these efforts.

Monitoring and analyzing network traffic in order to identify suspicious or malicious activity is known as network forensics. With tools like Wireshark, tcpdump, and NetFlow Analyzer frequently used in investigations, key approaches include event correlation, log analysis, packet analysis, and traffic analysis. The main goal of cloud forensics is to gather and analyze digital evidence from cloud-based settings, such as databases, storage containers, and virtual computers. In cloud platforms, tools like Google Cloud Logging and AWS CloudTrail are essential for monitoring user activities and guaranteeing data integrity.

An overview of the primary tools used in the various digital forensics fields is given in this section.

3.1. FTK Imager Tool: With this tool, digital evidence may be precisely and bit-by-bit copied from digital devices to create a forensic image. In order to prevent tampering or alteration, original digital evidence is maintained and kept in a secure environment. Tools like AD1 (Access Data Forensic ToolKit Image), AFF (Advanced Forensic Format), E01 (Encase Image File Format), and Raw Image File are used to create various kinds of forensic photos. As a result, the image is correctly made, hash values are produced, and we are able to verify the accuracy of digital evidence [6]. The figure, Fig 1(a) shows how to select the source evidence type, Fig 1(b) shows how to select the source drive, Fig 1(c) shows how to select image destination folder, Fig 1(d) shows how to create image successfully.



Select Source

Please Select the Source Evidence Type
○ Physical Drive
● Logical Drive
○ Image File
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
○ Fernico Device (multiple CD/DVD)

Fig 1(a). FTK Imager- Select the Source Evidence Type

Select Drive

Source Drive Selection
Please select from the following available drives:
R:\ - New Volume [NTFS]
□ Automate multiple removable media

Fig 1(b). FTK Imager- Select the Source Drive

Select Image Destination

Image Destination Folder: C:\New folder
Image Filename (Excluding Extension): LIP
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500
Compression (0=None, 1=Fastest, ..., 9=Smallest): 0
Use AD Encryption □

Fig 1(c). FTK Imager- Select Image Destination Folder

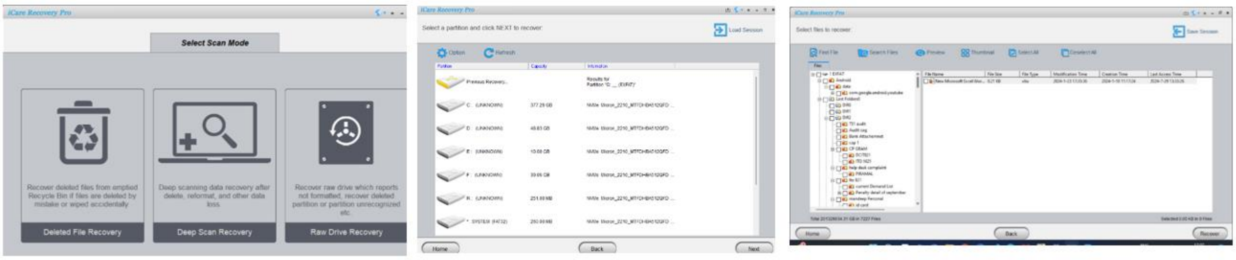
Creating Image...

Image Source: C:\Users\aditi\OneDrive\Desktop\FORENSICS\FILES
Destination: C:\Users\aditi\OneDrive\Desktop\aditi experiment\xyz
Status: Image created successfully
Progress
Elapsed time: 0:00:00
Estimated time left:

Fig 1(d). FTK Imager- Image Created Successfully

Fig 1.FTK Imager Tool

3.2. iCare Data Recovery Pro: This tool can be used to recover data from erased files, pen drives, formatted hard drives, USB drives, and inaccessible drives. This tool offers a number of scans that aid in the recovery of deleted data. The use of scans like Raw Drive Recovery, Deep Scan Recovery, and Deleted File Recovery. It examines each and every FAT folder layer by layer. The deleted data is later displayed on the tool, allowing us to preview it. By selecting "Recover the files," we can retrieve the desired data, which will be saved in the designated folder. As a result, we have access to the removed data files. The figure no. Fig 2(a) shows Pro-Scan Mode, Fig 2(b) shows Pro-Select Partition Dosk and Fig 2(c) shows Pro-Recover Deleted Files of the iCare Data Recovery Pro Tool.



iCare Recovery Pro

Select Scan Mode

Recover deleted files from emptied Recycle Bin if files are deleted by mistake or wiped accidentally — Deleted File Recovery
Deep scanning data recovery after delete, reformat, and other data loss. — Deep Scan Recovery
Recover raw drive which reports not formatted, recover deleted partition or partition unrecognized etc. — Raw Drive Recovery

Fig 2(a). iCare Data Recovery Pro- Scan Mode

Select a partition and click NEXT to recover:

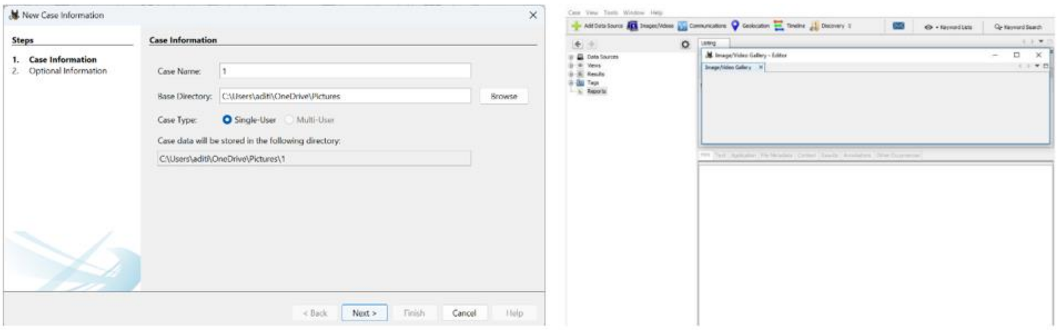
Fig 2(b). iCare Data Recovery Pro- Select Partition Disk

Select files to recover

Fig 2(c). iCare Data Recovery Pro- Recover Deleted Files

Fig2. iCare Data Recovery Pro Tool

3.3. Autopsy: This open-source program is used to examine and evaluate digital evidence. Law enforcement agencies like it because of its user-friendly graphical user interface. Numerous file system formats, including NTFS, FAT, EXT, and others, can be examined using Autopsy. User files, deleted files, file system metadata, and many other things are included. Email and chat logs can be extracted with this tool. The comprehensive reports that Autopsy produced regarding the files that were recovered may also be exported in a variety of file formats, including PDF, HTML, and Excel, making sharing them simple. It is employed in the incident response process to locate the data breach and ascertain its primary cause. All things considered; this is a useful tool with a wide range of applications [6]. The figure, Fig 3(a) shows the case information and Fig 3(b) shows the generated reports.



New Case Information

Steps
1. Case Information
2. Optional Information

Case Information

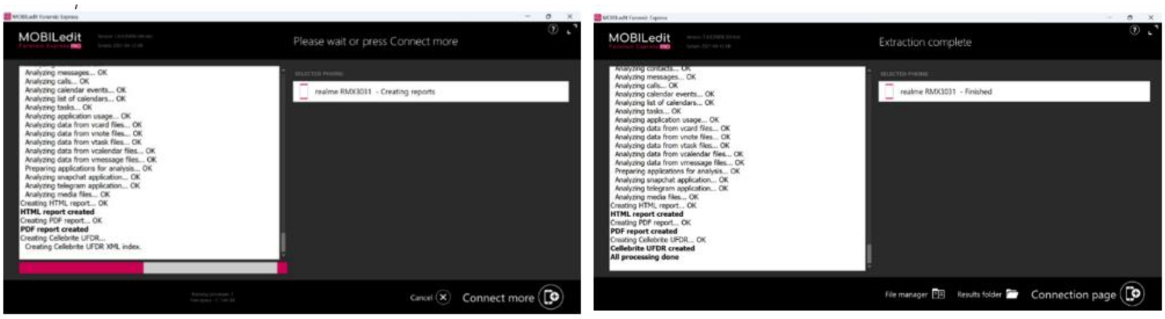
Case Name: 1
Base Directory: C:\Users\aditi\OneDrive\Pictures
Case Type: ● Single-User ○ Multi-User
Case data will be stored in the following directory:
C:\Users\aditi\OneDrive\Pictures\1

Fig 3(a). Autopsy- Case Information

Fig 3(b). Autopsy- Generated Reports

Fig 3. Autopsy Tool

3.4. Mobiledit Forensic Express Pro- It is a tool for mobile forensics. Law enforcement and digital forensic experts utilize it extensively to retrieve and analyze mobile data. It contains contacts, phone numbers, call logs, images, videos, and data that can be extracted that have been erased. With this tool, you can extract app data and get around passwords, patterns, and PINs. Because this tool provides reports, more data may be retrieved and examined. A forensic connector is installed on the mobile device after it is connected to a computer via USB cable; as a result, the data is retrieved and the extraction process begins. The figure, Fig 4(a) shows how the data is analyzed and Fig 4(b) shows the generated reports.



Please wait or press Connect more

```
  Analyzing messages... OK
  Analyzing calls... OK
  Analyzing calendar events... OK
  Analyzing list of calendars... OK
  Analyzing tasks... OK
  Analyzing application usage... OK
  Analyzing data from vcard files... OK
  Analyzing data from vnote files... OK
  Analyzing data from vtask files... OK
  Analyzing data from vcalendar files... OK
  Analyzing data from vmessage files... OK
  Preparing applications for analysis... OK
  Analyzing snapchat application... OK
  Analyzing telegram application... OK
  Analyzing media files... OK
Creating HTML report... OK
HTML report created
Creating PDF report... OK
PDF report created
Creating Cellebrite UFDR...
  Creating Cellebrite UFDR XML index.
```

realme RMX3031 - Creating reports

Extraction complete

```
  Analyzing contacts... OK
  Analyzing messages... OK
  Analyzing calls... OK
  Analyzing calendar events... OK
  Analyzing list of calendars... OK
  Analyzing tasks... OK
  Analyzing application usage... OK
  Analyzing data from vcard files... OK
  Analyzing data from vnote files... OK
  Analyzing data from vtask files... OK
  Analyzing data from vcalendar files... OK
  Analyzing data from vmessage files... OK
  Preparing applications for analysis... OK
  Analyzing snapchat application... OK
  Analyzing telegram application... OK
  Analyzing media files... OK
Creating HTML report... OK
HTML report created
Creating PDF report... OK
PDF report created
Creating Cellebrite UFDR... OK
Cellebrite UFDR created
All processing done
```

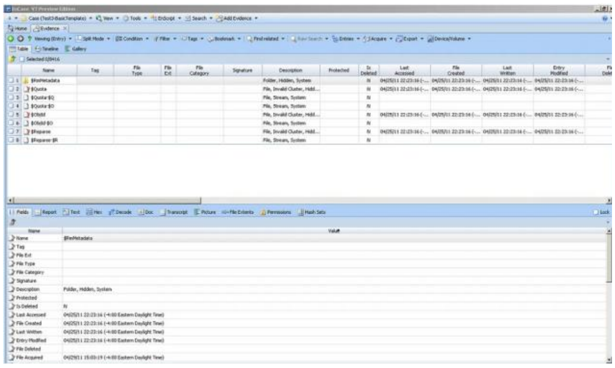
realme RMX3031 - Finished

Fig 4(a). Mobiledit Forensic Express Pro- Analyzing Data

Fig 4(b). Mobiledit Forensic Express Pro- Reports

Fig 4. Mobiledit Forensic Express Pro Tool

3.5. Encase: OpenText is the developer of this utility. It's one of the digital forensics tools that's employed the most frequently. Governmental entities, forensic analysts, cybersecurity experts, and law enforcement agencies all use it. It is employed in the gathering, storing, processing, and display of digital evidence. It is capable of extracting metadata from files and analyzing various file systems. It is employed in file carving techniques, which involve looking for file signatures in unallocated space in order to retrieve erased data. Therefore, by utilizing these technologies, cyber dangers can be reduced and the crime case can be solved.



	Name	Tag	File Type	File Ext	File Category	Signature	Description	Protected	Is Deleted	Last Accessed	File Created	Last Written	Entry Modified
1	$FileMetadata						Folder, Hidden, System		N	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...
2	$Quota						File, Invalid Cluster, Hidd...		N	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...
3	$Quota·$Q						File, Stream, System		N				
4	$Quota·$O						File, Stream, System		N				
5	$ObjId						File, Invalid Cluster, Hidd...		N	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...
6	$ObjId·$O						File, Stream, System		N				
7	$Reparse						File, Invalid Cluster, Hidd...		N	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...	04/25/11 22:23:16 (-...
8	$Reparse·$R						File, Stream, System		N				

Name	Value
Name	$FileMetadata
Tag	
File Ext	
File Type	
File Category	
Signature	
Description	Folder, Hidden, System
Protected	
Is Deleted	N
Last Accessed	04/25/11 22:23:16 (-4:00 Eastern Daylight Time)
File Created	04/25/11 22:23:16 (-4:00 Eastern Daylight Time)
Last Written	04/25/11 22:23:16 (-4:00 Eastern Daylight Time)
Entry Modified	04/25/11 22:23:16 (-4:00 Eastern Daylight Time)
File Deleted	
File Acquired	04/29/11 15:03:19 (-4:00 Eastern Daylight Time)

Fig 5. Encase Tool

Fundamental ethical and legal factors ensure that investigations are carried out appropriately, protecting people's privacy, abiding by the law, and preserving the forensic process's integrity. Robust security protocols are additionally instituted to ensure that the digital evidence remains inaccessible to unauthorized parties. The chain of custody is upheld and isn't altered. By using the hash value for authentication, data integrity and authenticity must be maintained. The figure, Fig 5 shows one of the screens of the Encase Tool.

4. RESULTS & DISCUSSION

This research assessed five prominent digital forensic tools for their efficacy in practical investigative contexts. FTK Imager proved effective in generating forensic images of storage devices while maintaining data integrity through hash verification, making it particularly suitable for initial evidence acquisition. iCare Data Recovery Pro excelled in retrieving deleted or lost files from both formatted and corrupted drives, featuring a user-friendly interface that facilitates rapid data recovery. Autopsy, an open-source forensic platform, offers a comprehensive analysis of digital evidence through functionalities such as timeline analysis, keyword searches, and tracking of recent activities, rendering it invaluable for thorough investigations. Mobiledit Forensic Express extracted detailed information from mobile devices, including messages, call logs, and application data, and produced court-admissible reports beneficial for mobile-related cybercrime cases. Finally, EnCase provided extensive forensic capabilities for large-scale investigations, encompassing memory analysis, email tracing, and detailed reporting, making it a favored choice in professional and legal settings despite its complexity. Collectively, these tools exhibit a range of strengths and applications across various forms of digital forensic investigations. The table 1 provides a comparative analysis of the various tools and techniques examined in this research.

Table 1. Comparative Analysis of tools and techniques used for performing digital forensics

Tools	Best Use Area	Strengths	Limitations
FTK Imager	Evidence Imaging [6]	Speed, Integrity Check	No in-depth analysis
iCare Data Recovery Pro	File Recovery [6]	Simplicity, Quick Recovery	Limited Forensic logging
Autopsy	General Investigations [8]	Open-Source, Extensible	Steeper learning curve
Mobiledit Forensic Express	Mobile Data Analysis [6]	Detailed Extraction, Report Generation	Limited access to encrypted data
EnCase	Comprehensive Investigation [9]	Detailed, Court- Admissible Reports	High cost, requires training

The results indicate that there is no one tool that stands out as the best; rather, their effectiveness is contingent upon the specifics of each case. Utilizing a combination of these tools can greatly improve the precision, comprehensiveness, and legal validity of digital forensic investigations.

5. REAL-WORLD USE CASES OF DIGITAL FORENSICS

Digital forensics is crucial in revealing evidence, identifying victims or offenders, and supporting legal processes. Forensic analysts employ specialized tools and methodologies designed for the specific circumstances of each case, guaranteeing precision and pertinence in the analysis of evidence. Although it is relatively recent, digital forensics is advancing swiftly, with new technologies improving its practical effectiveness. Two significant examples that illustrate both present applications and future trends in this domain are:

5.1. BTK (Bind, Torture, Kill) Case: Dennis Rader, a psychotic serial murderer, killed ten people. He was also referred to as the BTK murderer. His method of operation involved killing, torturing, and binding his victims—often leaving little to no trace for the authorities. Rader used to provide the local police with a variety of cryptic letters that described his crimes. The cops were essentially kept guessing by the codes and hints that were used in these exchanges. After a prolonged period of silence, Rader resumed communication with police in 2005. He attempted to conceal his identity by sending them a Microsoft Word document on a floppy disk that included a local newspaper, but he was unsuccessful. Rader asked the police if they could track down the disk, but they made a major error and Rader was apprehended. The role of the forensic team was significant. They discovered a floppy disk to be digital evidence, and it may contain important information that would identify the BTK's murderer. The floppy disk was meticulously maintained to prevent tampering. They began analyzing the floppy disk after creating a bit-by-bit replica of it. They employed "Encase," a specific program or tool, which successfully recorded all the pertinent information. Additionally, erased data was restored without compromising digital evidence. They were able to solve the case because to the information found in the Microsoft Word document. The Christ Lutheran Church in Wichita developed the document on the floppy disk. They also noticed that Dennis had updated the paper most recently. Thus, this was a significant hint that assisted the authorities in identifying the sender of the communications. Ultimately, a written report was created and given to law enforcement representatives. Thus, the case taught us the following lessons: digital footprints may be tracked, technical expertise is crucial and hence digital forensics is powerful. [10]

5.2. Bengaluru Cryptocurrency Scam 2021: It is a large-scale fraud in which con artists tricked people into believing they were investing in cryptocurrency schemes in exchange for 300 crore rupees before going missing. In essence, the con artists built phony websites for investing in cryptocurrency and advertised and marketed these kinds of schemes. With the use of equipment, the forensics analysts began to locate and examine the website. They looked into it for a while in order to gather some information. The identification and collection of scam victims' data aided in the case-building process. The website logs were stored in a secure location because there is no ongoing manipulation. Computer systems and servers that were utilized in scams were backed up and kept in a secure location. After the logs were gathered, they were later examined with the aid of tools, which also helped to spot any patterns of fraudulent activity. A thorough investigation was conducted to identify the victims, figure out how to trick them, and siphon off their money. Strong preventive measures were implemented to stop such scams in the future, and a forensic report was later created and provided with the law enforcement agencies for the next step in the process. Lessons from this case included early detection, data preservation, future planning, collaborating with law enforcement to apprehend perpetrators, and educating the public about fraudulent schemes. These applications highlight the increasing significance of digital forensics in law enforcement and organizational security, emphasizing its critical function in addressing the challenges posed by cybercrime in the real world. [11]

6. CONCLUSION

This study emphasizes the essential function of digital forensics in tackling the increasing intricacies of cybercrimes by facilitating the identification, recovery, and analysis of digital evidence. By conducting a comparative assessment of five prominent forensic tools—FTK Imager, iCare Data Recovery Pro, Autopsy, Mobiledit Forensic Express, and EnCase—the research illustrates how each tool contributes to various phases of the forensic investigation process, including identification, collection, preservation, analysis, and documentation. FTK Imager and EnCase were particularly effective for forensic imaging and thorough analysis, while Autopsy provided a dependable open-source option for general investigations. iCare Data Recovery Pro excelled in retrieving lost or deleted files, and Mobiledit Forensic Express offered significant insights from mobile device data. The results highlight that the choice of forensic tools should be tailored to the specific needs of each case, as no single tool is universally suitable. By recognizing the advantages and limitations of these tools, forensic analysts can make well-informed decisions to improve investigation results. Furthermore, compliance with legal standards such as chain of custody and accurate documentation is crucial for ensuring the admissibility of digital evidence in court. In summary, the study reinforces the necessity of continually enhancing digital forensic tools and methodologies to bolster security measures.

REFERENCES

[1] Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 491–497.

[2] Mahmoud, N., & Rezvanian, A. (2022). Ransomware and Phishing Cyberattacks: Detection Techniques and Mitigation. *Uppsala University*.

[3] Hoxhunt. (2025). Phishing Trends Report: Insights and Key Statistics 2025.

[4] Pollitt, Mark. "A History of Digital Forensics." In *Digital Forensics and Cyber Crime*, edited by Joshua I. James and Pavel Gladyshev, 3-15. IFIP Advances in Information and Communication Technology, Vol. 337. Springer, 2010.

[5] Morgan, S. (2024). Global Ransomware Damage Costs Predicted to Exceed $275 Billion by 2031. *Cybersecurity Ventures*.

[6] Rafique, Mamoona, and M. N. A. Khan. *Exploring Static and Live Digital Forensics: Methods, Practices and Tools*. PDF. Accessed August 31, 2024.

[7] Federal Bureau of Investigation (FBI) - Internet Crime Complaint Center. (2024). 2023 Internet Crime Report.

[8] Garfinkel, S. L. (2010). Digital Forensic Research: The Next 10 Years. *Digital Investigation*, 7(Supplement), S64–S73.

[9] Kessler, G. C. (2024). The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Physical World. *Forensic Science International: Digital Investigation*, 38, 301497.

[10] S. Jones, H. C. (O. Chan), W. C. Myers, and K. Heide, “Case 09—The Kansas B.T.K. Strangler: The Case of Dennis Lynn Rader (1974–1991; U.S.A.),” *International Journal of Offender Therapy and Comparative Criminology*, vol. 63, no. 9, pp. 1573–1591, 2019.

[11] G. Shelke, “Legal Challenges to Cryptocurrency and its Guardian-Less Victims in India: A Critical Victimological Analysis,” *International Annals of Criminology*, vol. 58, no. 1, pp. 1–15, 2020.