ISSN No:-2456-2165

Forensic Tools in Comparison: An Assessment of Performance Across Different Parameters

Annalaxmi Valluvar[1]
Department of Computer Science
SIES Graduate School of Technology
Nerul, India

Spoorti Shetty[2]
Department of Computer Science
SIES Graduate School of Technology
Nerul, India

Subhashree Pandian[3]
Department of Computer Science
SIES Graduate School of Technology
Nerul, India

Suvarna Chaure (Professor)[4]
Department of Computer Science
SIES Graduate School of Technology
Nerul, India

Abstract:- Computer forensics is a crucial field that involves the collection, preservation, and analysis of digital evidence. Forensic tools play a vital role in this process, aiding investigators in extracting, analyzing, and interpreting data from diverse digital devices. With the increasing complexity of digital devices and the surge in digital data, selecting the appropriate forensic tool has become paramount. This study evaluates and contrasts different free forensic tools with an emphasis on network examination, data analysis, and password cracking. The evaluation considers variables such platform support, file system support, imaging capabilities, data-driven features, reporting capabilities, hash type support, attack types, resource utilization, and pattern matching capabilities. The results of this comparison research are an informative resource for forensic professionals seeking to choose the best tool for their specific requirements. Notably, the data analysis capabilities of Autopsy, FTK Imager, and ProDiscover Basic displayed unique strengths and limitations for data analysis. Due to its robust hash type support and effective administration of resources, John the Ripper and Hashcat emerged as reasonable options for password cracking. The study also recommends Wireshark for network analysis because of its intuitive user interface, substantial packet analysis tools, and flexible multi-platform compatibility with other protocols. Nevertheless, is acknowledged that the ultimate choice on a forensic tool should be tailored to the distinct requirements and constraints of each investigatory project.

Keywords:- *Computer Forensics, Digital Evidence, Forensic Tools, Network Analysis, Data Analysis, Password Cracking, Platform Support, File System Support, Imaging Capabilities, Reporting Capabilities, Hash Type Support.*

I. INTRODUCTION

Digital forensics has emerged as a critical field in today's technology-driven world, playing a pivotal role in uncovering and analyzing digital evidence during investigations.

As digital data continues to proliferate at an exponential rate, the significance of robust and reliable forensic tools has never been greater. These software applications have become indispensable tools for investigators, assisting them in collecting, preserving, and analyzing digital evidence with precision and accuracy. By aiding in data recovery, file analysis, and identification of potential cyber threats, these tools have revolutionized the landscape of digital investigations.

The selection of the right forensic tool is paramount to conducting effective and efficient investigations. With a myriad of forensic tools available, each boasting unique features and capabilities, forensic investigators face the daunting task of choosing the most suitable tool for their specific needs. Hence, a thorough comparison of forensic tools across various parameters becomes imperative to make informed decisions and maximize investigation outcomes.

This research endeavors to provide forensic practitioners with valuable insights by comparing the performance of multiple forensic tools across different categories. Specifically, the study evaluates data analysis tools, password cracking tools, and network analysis tools, all of which are crucial components of modern-day digital investigations.

Throughout the evaluation process, a diverse range of forensic tools will be scrutinized, including Autopsy, FTK Imager, ProDiscover Basic, John the Ripper, Hydra, Hashcat, CEWL, Crunch, Wireshark, Ngrep, Tcpdump, and Nsniff-ng. These tools will be put to the test in retrieving passwords from encrypted data, analyzing network traffic, and extracting and analyzing data from digital devices.

Ultimately, the outcomes of this research endeavor to empower forensic analysts with a comprehensive understanding of the strengths and limitations of various forensic tools. By assisting investigators in making informed decisions and selecting the most appropriate tool for each investigatory project, this study aims to enhance the overall efficacy and efficiency of digital investigations.

The rest of this paper is organized as follows: Firstly, Chapter 2 provides a detailed assessment of the literature. The project's proposed system and architecture including research design, data collection, and tool selection are presented Chapter 3 and 4. Chapter 5 details the implementation and results, comparing forensic tools across parameters, discussing key findings, limitations, and challenges. The conclusion summarizes findings, discusses implications for forensic science, and suggests future research directions.

Finally, the report includes a reference list citing the sources used, which provide additional details on the evaluated tools, performance assessment results, and data collection forms and worksheets.

II. LITERATURE SURVEY

This section gives an overview of the approaches used in the literature for forensic assessments. In the recent decade, several strategies have been proposed, but each has significant differences. Below is a summary of the many methodologies and categorization strategies used in recent years.

In "Cyber Forensics Tools: A Review on Mechanism and Emerging Challenges [1]," the authors emphasize the importance of cyber forensic tools in investigating cybercrimes. They emphasize the need for suitable, accurate, affordable, and reliable tools to support investigators in their work across different branches of cyber forensics. However, they acknowledge limitations in existing tools such as data acquisition, examination challenges, and compatibility issues, which can impact investigation effectiveness and evidence accuracy.

"The State-of-the-art tools and techniques for remote digital forensic investigations [2]" emphasizes the importance of remote forensic techniques in digital investigations to eliminate cost and time delays. The paper analyzes various tools and methodologies, providing a comparative assessment. However, the study may not have covered all possible techniques, and effectiveness can vary depending on specific circumstances.

"Comparative Analysis of Network Forensic Tools and Network Forensics Processes [3]" focuses on Network Forensics (NFs) and compares four popular Network Forensic Tools (NFTs). The paper acknowledges limitations in terms of the limited number of tools assessed and the specific functionalities considered. Factors such as cost, usability, and compatibility with different network environments may not have been fully considered. Further research is needed to determine the most suitable NFT for comprehensive network forensic investigations.

"Emerging trends in Digital Forensic and Cyber security- An Overview [4]" provides an overview of digital forensics and its various domains, including network forensics, server forensics, and computer forensics. The paper discusses challenges related to technical, legal, and resource issues. It emphasizes the importance of exploring new dimensions of digital forensics, such as internet forensics, social media forensics, and IoT forensics, to keep up with evolving technologies. The paper also highlights the need for ethical practices, privacy concerns, and further research to develop compatible methods and preserve evidence in emerging fields like social media, IoT, and cloud forensics.

"A Study on Digital Forensic Tools [5]" addresses the growing risk of data misuse and emphasizes the significance of digital forensic tools in investigating cyberattacks and gathering evidence. The paper provides a comprehensive examination of various tools used by corporations, government agencies, and individuals, comparing them based on different criteria. However, limitations exist, including a limited number of tools compared and the potential exclusion of other available tools. The chosen attributes for comparison may not provide a comprehensive evaluation, and the results may be subjective and dependent on specific investigation scenarios.

"An Insight into Digital Forensics Branches and Tools [6]" addresses the challenges posed by cybercrime in the era of Ubiquitous Computing. The paper explores various digital forensic branches and compares available forensic tools based on their features, efficiency, and effectiveness. It serves as a valuable resource for security practitioners, forensic researchers etc. seeking to understand and utilize the capabilities of different forensic tools. However, limitations may arise from factors such as limited access to evidence, incomplete or corrupted data, technical constraints of the tools used, and limitations in time and resources allocated for investigations.

"Qualitative Assessment of Digital Forensic Tools [7]" highlights the significance of digital forensics in investigating cybercrimes and addresses the challenges of digital investigations. The paper categorizes different forensic domains and provides a list of digital forensic tools, comparing them based on defined parameters. However, possible limitations include the lack of discussion on newer or advanced tools, limited scope in the covered forensic categories, and the need for empirical data to support the tool comparisons.

ISSN No:- 2456-2165

III. PROPOSED SYSTEM

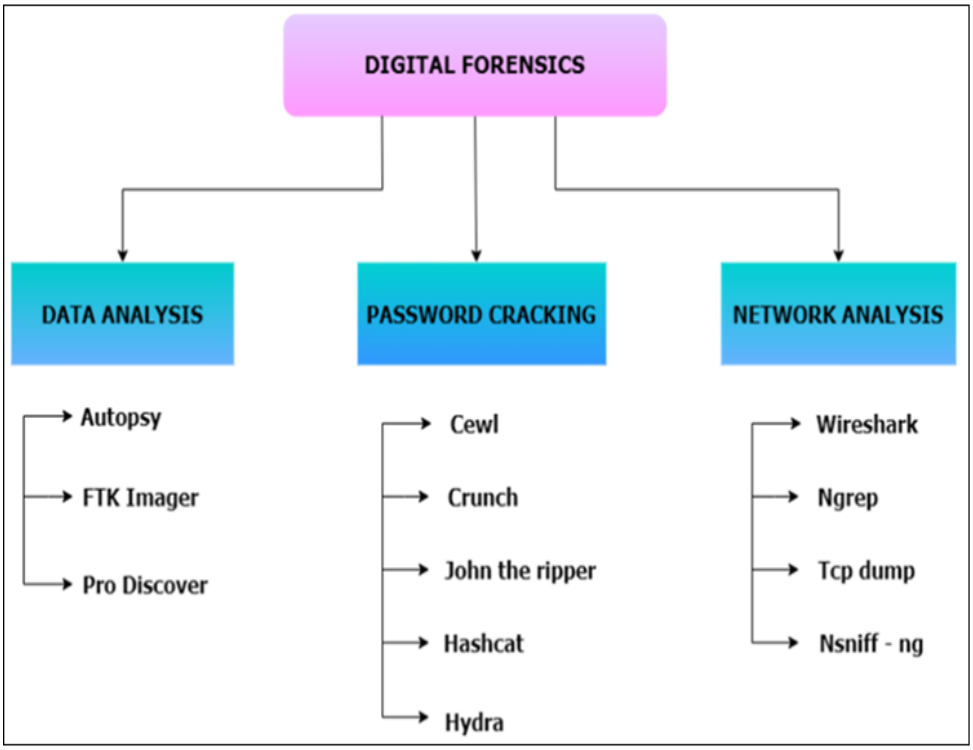

Fig 1 Forensic Tools Proposed System

The proposed project has a clear objective: to assess and compare the performance of digital forensic tools in three critical categories - data analysis, password cracking, and network analysis. This comparison aims to guide investigators in selecting the most suitable tools for their investigations, enhancing the overall efficiency and effectiveness of digital forensics.

To accomplish this, a range of well-established tools has been chosen, considering their popularity and capabilities in their respective domains. These tools will be rigorously evaluated across multiple parameters. The tools will be used to extract and analyze data from digital devices, recover passwords from encrypted data, and analyze network traffic.

The project's outcomes will provide valuable insights into the strengths and weaknesses of these tools, facilitating informed decision-making for forensic investigators. Additionally, this research will contribute to the continuous advancement of forensic tools by identifying areas that require further development and by providing guidance on the selection and use of forensic tools.

IV. ARCHITECTURE

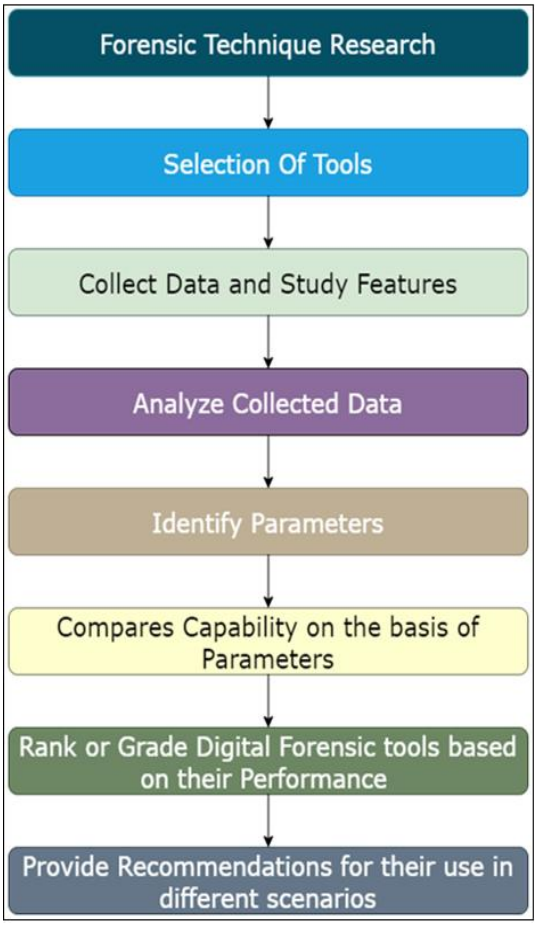

Fig 2 Architecture

ISSN No:- 2456-2165

The architecture of the proposed project involves several steps that are essential for evaluating and comparing the performance of digital forensic tools. The project will follow a systematic approach, starting with forensic technique research and concluding with recommendations for the use of digital forensic tools.

The results of this evaluation will provide valuable insights into the strengths and weaknesses of each tool, and help forensic investigators choose the most appropriate tool for their specific needs.

- *Forensic Technique Research*

This initial phase of the project is dedicated to a comprehensive exploration of the diverse techniques employed in digital forensics investigations. The objective here is to gain a deep understanding of the various methodologies and approaches used in this field. By conducting thorough research, we can discern the precise categories and domains of digital forensic tools that will be indispensable for the forthcoming investigation. Once this research phase concludes, we will be well-equipped to proceed to the crucial task of tool selection.

- *Selection of Tools*

The process of tool selection is a critical juncture in our project, necessitating a meticulous evaluation of various essential parameters. These parameters encompass a spectrum of factors ranging from features and compatibility to user interface and performance. Each tool's ability to align with these factors will determine its efficiency and effectiveness in the investigation. Once we have identified the tools that align best with our parameters, we will proceed to the next pivotal phase: data collection and an in-depth study of the selected tools' features.

- *Collect Data and Study Features*

During this phase, the selected tools will be used to extract and analyze data from digital devices, recover passwords from encrypted data, and analyze network traffic. The collected data will be studied to identify the different parameters that are important for the investigation. These parameters may include accuracy, speed, and other factors that can impact the effectiveness and efficiency of the investigation.

- *Comparing the Capability of Each Tool and Grade Them on Performance*

With the critical parameters in focus, the subsequent phase involves a comprehensive comparison of each tool's capability in alignment with these factors. This evaluative process delves into a thorough performance assessment of each tool. Based on their performance, we will assign grades to these tools, creating a ranked list.

This graded list will serve as the foundation for our recommendations, which will guide the selection of tools for specific scenarios and investigative needs.

- *Recommendation of Tools*

In the concluding phase of the project, our objective is to offer clear and informed recommendations regarding the utilization of digital forensic tools within various investigative scenarios. These recommendations will be meticulously grounded in the performance data gathered across a spectrum of parameters. Forensic practitioners will find these insights invaluable for making the precise selection of tools that align with their unique investigative requirements.

V. EXPERIMENTS AND RESULTS

In this project, a series of experiments are conducted to rigorously assess the performance of various digital forensic tools across a range of critical parameters.

The objective was to provide a comprehensive evaluation of these tools, shedding light on their individual strengths and limitations. The outcomes of the experiments have clearly demonstrated that each forensic tool possesses unique attributes that excel in specific areas while potentially falling short in others.

Consequently, the selection of an appropriate tool should be a meticulously considered decision, contingent upon the precise requisites of the investigation at hand.

In summary, the experiments have yielded invaluable insights into the nuanced performance characteristics of digital forensic tools. By leveraging the right tool for the job, investigators can substantially enhance the efficiency and efficacy of their digital investigations, ultimately yielding superior outcomes and bolstering the strength of their cases.

A. Data Analysis

Autopsy, ProDiscover Basic, and FTK Imager stand as crucial players in the realm of digital forensic tools, specializing in data analysis.

- *Autopsy shines as an open-source solution with cross-platform compatibility, offering an intuitive user interface that facilitates accessibility.*
- *ProDiscover Basic, on the other hand, is proprietary software exclusive to Windows, distinguished by its remarkable processing speed, ensuring rapid results.*
- *FTK Imager, also proprietary but available across multiple platforms, excels in expeditious data acquisition and analysis.*

ISSN No:- 2456-2165

Table 1 Data Analysis Tools Comparison

Parameters	Autopsy	FTK Imager	ProDiscover Basic
Open source	Yes	No	No
File system support	FAT, NTFS, ext2/3/4, HFS+	FAT, NTFS, ext2/3/4, HFS+, RAW, DD	FAT, NTFS, ext2/3/4, HFS+, RAW
Image creation	Yes	Yes	Yes
File carving	Yes	Yes	Yes
Keyword search	Yes	Yes	Yes
Timeline analysis	Yes	No	Activity Viewer
Hash calculation	Yes	Yes	Yes
Metadata analysis	Yes	Yes	Yes
Email analysis	Yes	No	No
Registry analysis	Yes	Yes	Yes

In conclusion, the comparison of digital forensic tools highlights their varying capabilities and complexity levels. Autopsy emerges as a powerful open-source tool with extensive features for in-depth investigations, making it suitable for experienced users. FTK Imager offers simplicity and broad file system support, catering to beginners and straightforward cases. ProDiscover Basic, while user-friendly, lacks some advanced features found in Autopsy.

The choice of tool should align with the investigator's expertise and the complexity of the case. Autopsy stands out for comprehensive investigations, FTK Imager for simplicity, and ProDiscover Basic for basic needs.

B. Password Cracking

Password cracking tools are indispensable in digital forensic investigations, as they enable forensic experts and security professionals to recover lost, forgotten, or stolen passwords. These tools use various techniques to decipher passwords, ranging from simple dictionary attacks to more complex brute-force methods.

- *Cewl:*

An open-source tool used to generate custom wordlists by scraping words from websites. This tool is helpful for creating wordlists that may contain relevant words or phrases for password cracking.

- *Crunch:*

Another open-source tool used for generating custom wordlists. Crunch allows users to create wordlists with specific criteria, such as character sets, lengths, and patterns.

- *John the Ripper:*

A widely used open-source password cracking tool that supports various cracking techniques, including dictionary attacks, brute-force attacks, and more. It is known for its flexibility and ability to crack a variety of password hashes.

- *Hashcat:*

An open-source password cracking tool that is highly efficient and supports multiple hashing algorithms. Hashcat is known for its speed and ability to leverage GPU acceleration for faster cracking.

- *Hydra:*

A proprietary password cracking tool that supports brute-force and dictionary attacks. Hydra is known for its versatility and the ability to attack various network protocols and services.

ISSN No:- 2456-2165

Table 2 Password Cracking Tools Comparison

Parameters	Cewl	Crunch	John the Ripper	Hashcat	Hydra
Password Complexity	Medium	High	High	High	Medium
Brute-Force Capabilities	No	Yes	Yes	Yes	Yes
Wordlist Generation	Yes	Yes	Yes	Yes	No
Multi-Hash Support	No	No	Yes	Yes	No
Distributed Computing	No	No (does not support directly but can be integrated externally)	Yes (with community versions)	Yes	Yes
Rainbow Tables	No	No	Yes	Yes	No
GPU Acceleration	No	No	Yes	Yes	No
Attack Modes	Wordlist	Wordlist	Wordlist, Brute Force, Mask, Rule-based, Hybrid	Dictionary, Brute-force, Combination, Mask, Hybrid	Brute-force, Dictionary, Combination
Output Formats	Text	Text, XML, CSV	Text, XML, JSON	Text, CSV, JSON	Text, XML
CPU Usage	Low	Low	High	Very High	High
Memory Usage	Low	Low	Medium	Very High	High
Error Handling	Limited	Limited	Good	Good	Good

In summary, the discussed tools serve distinct purposes in digital forensics and password cracking. Cewl and Crunch are valuable for generating wordlists, with Cewl focusing on web content extraction and Crunch offering customization options. John the Ripper stands out as a versatile password cracking tool with support for various attack methods and advanced features, making it suitable for complex tasks. Hashcat excels in speed and hash type compatibility, making it a powerful choice for password cracking, especially when coupled with GPU acceleration. Hydra, while limited in some aspects, shines in brute-forcing login credentials for various services.

The selection among these tools should align with specific investigation requirements and expertise levels.

C. Network Analysis

➢ *Packet Analyzer Tools*

Packet analyser tools, also known as network packet sniffers or packet capture tools, are indeed crucial for network analysis and digital forensic investigations.

- *Wireshark:*

Wireshark is one of the most widely used and powerful packet analyzers available. It allows users to capture and analyse the data traveling back and forth on a network in real-time.

Wireshark supports a wide range of network protocols and provides detailed packet-level information. Its user-friendly graphical interface makes it accessible to both beginners and experienced network analysts.

- *Tcpdump:*

Tcpdump is a command-line packet analyzer that operates in a terminal window. It is highly efficient for capturing and displaying packet data but lacks the graphical interface of Wireshark.

Tcpdump is known for its speed and flexibility, making it a favorite among experienced network administrators and security professionals.

- *Ngrep:*

Ngrep is another command-line packet capture tool. It stands out for its ability to search packet payloads using regular expressions, allowing users to filter packets based on specific content within the packets. This is particularly useful for finding specific network patterns or identifying potential security threats.

- *Nsniff-ng:*

Nsniff-ng is an open-source network sniffer that provides real-time packet statistics and analysis. It is designed for simplicity and ease of use, making it suitable for both beginners and experienced users. Nsniff-ng offers various filtering options to narrow down captured packets based on specific criteria.

Table 3 Packet Analyzer Tools Comparison Table

Parameters	Wireshark	tcpdump	ngrep	nsniff-ng
Live Capture	Yes	Yes	Yes	Yes
Capture Filter	Yes	Yes	Yes	Yes
Display Filter	Yes	Yes	Yes	No
Supported Platforms	Windows, macOS, Linux	Linux, macOS, FreeBSD, OpenBSD, NetBSD	Linux	Linux
Packet Capturing	Yes	Yes	Yes	Yes
Packet Filtering	Yes	Yes	Yes	Yes
Packet Reconstruction	Yes	Yes	No	Yes
Flow Analysis	Yes	Limited	No	Yes
Performance	High	High	Moderate	Moderate
Memory Usage	High	Low	Low	Moderate
CPU Usage	Moderate to High	Low	Low	High

In conclusion, the choice of the best packet capture tool among Wireshark, tcpdump, ngrep, and nsniff-ng depends on your specific needs and priorities. Wireshark offers the most comprehensive feature set but is memory-intensive. tcpdump is a simpler option for live capture. ngrep is suitable for capturing traffic based on regular expressions. Lastly, nsniff-ng is geared toward security threat analysis.

VI. CONCLUSION

In conclusion, forensic tools play a crucial role in digital investigations, and choosing the right tool is essential for effective and efficient investigations. By comparing forensic tools across different parameters, investigators can identify the strengths and weaknesses of each tool and select the one that best suits their needs. The project discussed in this paper aims to evaluate the performance of various forensic tools across several parameters, including data analysis, password cracking, and network analysis. The results of this project will help forensic investigators choose the most appropriate tool for their specific needs and contribute to the ongoing development and improvement of forensic tools and techniques.

FUTURE SCOPE

There is a lot of scope for further research and development in the field of forensic tools. Integrating Artificial Intelligence (AI) and Machine Learning (ML) into digital forensics tools can enhance data analysis, pattern recognition, and anomaly detection. These technologies offer the ability to identify subtle patterns and anomalies in vast datasets, improving investigative efficiency. Furthermore, the field of mobile device forensics is poised for growth, given the rising prevalence of smartphones and tablets. Tools that can overcome encryption and locked bootloaders to extract data from these devices will be crucial for investigators facing evolving security challenges in the mobile realm.

REFERENCES

[1]. Fernando, V. (2021, April). Cyber forensics tools: A review on mechanism and emerging challenges. In 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-7). IEEE.

[2]. Shobana, G. (2021, May). The State-of-the-art tools and techniques for remote digital forensic investigations. In 2021 3rd International Conference on Signal Processing and Communication (ICPSC) (pp. 464-468). IEEE.

[3]. Ghabban, F. M., Alfadli, I. M., Ameerbakhsh, O., AbuAli, A. N., Al-Dhaqm, A., & Al-Khasawneh, M. A. (2021, June). Comparative analysis of network forensic tools and network forensics processes. In 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 78-83). IEEE.

[4]. Sharma, B. K., Joseph, M. A., Jacob, B., & Miranda, B. (2019). Emerging trends in digital forensic and cyber security-an overview. 2019 Sixth HCT Information Technology Trends (ITT), 309-313.

[5]. Ghazinour, K., Vakharia, D. M., Kannaji, K. C., & Satyakumar, R. (2017, September). A study on digital forensic tools. In 2017 IEEE international conference on power, control, signals, and instrumentation engineering (ICPCSI) (pp. 3136-3142). IEEE.

[6]. Kumari, N., & Mohapatra, A. K. (2016, March). An insight into digital forensics branches and tools. In 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT) (pp. 243-250). IEEE.

[7]. Singh, S., & Kumar, S. (2020). Qualitative Assessment of Digital Forensic Tools. Asian Journal of Electrical Sciences, 9(1), 25-32.