JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 07 Issue 02
2024

Research Article
https://doi.org/10.56979/702/2024

# A Comparative Study of CAINE Linux: A Digital Forensics Distribution

**Talha Saleem[1*], Zata Ul Nataqain[2], Mueed Saleem[1], and Gohar Mumtaz[1]**

[1]Faculty of Computer Science and Information Technology, Superior University, Lahore, 54000, Pakistan.
[2]Virtual University of Pakistan, Lahore, 54000, Pakistan.
[*]Corresponding Author: Talha Saleem. Email: talha.itp@gmail.com

**Received:** April 11, 2024 **Accepted:** August 19, 2024 **Published:** September 01, 2024

**Abstract:** Global crimes have necessitated digital forensics to be a more important factor in solving criminal incidences hence effectively needs some measures. Some of the best-known distributions of digital forensics are CAINE (Computer Aided Investigative Environment) Linux one of the distributions contain tools developed to assist investigators to recover, analyze and preserve Data & Digital Evidence. This review article's purpose is to describe major characteristics of CAINE Linux as the tool used for digital forensics and its performance mainly usefulness. This work also contrasts CAINE Linux with other distributions in digital forensics to show how CAINE works and the limitations when used in various forensic scenarios. As part of the analysis, the writer will attempt to understand how effective CAINE Linux is as a forensic tool based on factors such as the software's operational capability, integration of tools and how it is supplemented with new threats. It is admired that the findings of this study will enable practitioners to select the right forensic distribution that meets the need of an investigation, hence enhancing efficiency and efficacy in cybercrime investigation.

**Keywords:** CAINE Linux; Digital Forensics Distribution; Cybercrime Investigation; Forensic Analysis Tools; Cyber Security

## 1. Introduction

The CAINE (Computer Aided Investigative Environment) Linux is a free of charge, Linux based tool developed as a digital forensics ready operating environment to help investigators in the processing of digital material. CAINE was developed by Nanni Bassetti and offers enhanced flexibility and adaptability, a subject-friendly interface and powerful tools for the purposes of forensic investigation as well as for managing and responding to computer security incidents. In essence, CAINE focuses on the requirements of digital investigators providing them with a range of tools integrated and tested in the environment in order to cover all aspects of digital forensic investigation. From data capture and data retrieval, file system analysis and reporting, CAINE guarantees that the investigator has access to reliable tools which maintain the continuity of digital evidence. The important aspect of CAINE Linux distribution is the concern of its developers for the data integrity during the investigation. It means that CAINE can be used for the absolute legal investigations as it provides live forensic techniques and the information generalization does not affect the data. Using CAINE Linux some important fields in global community is Law enforcement, Cyber security, corporate investigations, and academic institutions. It has a lot of functionality and is quite flexible, which is why any specialists dealing with DFIR should consider it mandatory.

As mentioned before, CAINE Linux distribution has many tools integrated right out of the box such as disk imaging, file carving, data recovery, network, and memory forensic tools [1]. All these tools are packaged in a graphical user interface to enhance efficient working of forensic procedures. The distribution provides its own graphical front-end that even a typical user not familiar with Linux in CAINE forensic environment is straightforward to work with. This means that the interface itself is constructed to host and then facilitate the usage of tools and completion of aims in the forensic pipeline. As a live distort CAINE Linux can be executed from a USB or a DVD, the potential of this approach is that the conditions on the

analyzed system remain unchanged because the data on the host computer are not altered. This capability helps in preserving the evidential information during investigations as explained.

Some of the tools of CAINE are Caine Report which gives fully formatted forensic report as soon as the analysis is done. This feature assists in capturing the process of investigation and guarantee that all the processes are well captured for legal or procedural reasons [2]. In accord with this, the distribution comes equipped with powerful tools for data recovery which allow recovering deleted files, lost partitions and damaged data. These tools are useful in case you need to recover information which could have been deleted, by intention or by accident. CAINE Linux again, is equipped for a profound analysis of the memory, which helps detect such mutable information as launched processes, open connections, keys for the encryption, etc. This is especially valuable when dealing with complicated malware, or threats that reside in memory, such as viruses. The tools present in CAINE work well in dealing with different file systems and operating systems such as Windows, macOS and Linux and that makes it flexible when handling different digital ecosystems. CAINE Linux has many applications in a particular field of work, especially among law enforcement departments for investigating hacking, frauds and data breaches. Due to reliability of maintaining the originality of the digital evidence, it is widely used in law related proceedings [3].

Some of the organizations are using CAINE Linux in incident response with a special focus on analyzing infected systems and the level of intrusion. It also has the live boot functionality that enables responders evaluate the impacted machines without endangering their data. CAINE Linux is also very extensively used within the academic community as an educational platform in the learning and teaching of digital forensics or an environment in which new techniques or tools are tested. It is open source hence use can be experimented on hence developed. Some organizations deploy CAINE for internal operations, for examples when there are suspected instances of piracy, embezzlement or those required by law that check compliance. It offers extensive features that will enable proper and efficient analysis to be conducted. CAINE Linux can be used by security professionals during penetration testing and security audit to determine the effectiveness of existing security measures and possibly, probe for weak links in systems.

1.1. Objectives

1. This review article therefore sets out to present analysis of CAINE Linux as a digital forensics' distribution.
2. The purpose of this work is to assess the major characteristics, efficiency, and usefulness of CAINE Linux within the framework of digital forensics.
3. The general purpose is to give a reader an overall impression of CAINE Linux and to help choosing the most appropriate digital forensics distribution in specific cases.

## 2. Literature Review

2.1. Core Features of CAIN Linux

*2.1.1. Live Forensic Environment*

The CAINE Linux (Computer Aided Investigative Environment) offers exactly all necessary tools for live forensics allowing digital investigators to investigate a system while that system is live. CAINE can further be run in live USB device or live DVD. This mode lets the operating system to run directly from the bootable media without writing anything on the host machine's hard drive. When booting in the live mode, CAINE can guarantee that no changes will be made to the system's data and thus remove the chances of making a change inadvertently. The live environment of CAINE comes with features for the tools for automatically setting disks to read-only mode [4]. This is very important so that no changes are made to the evidence that is on the system.

*2.1.2. Built-in Forensic Tools*

The CAINE was found to be packaged with several integrated tools for forensic investigations right from disk imaging and remote data acquisition to memory analysis and network traffic analysis. Due to its Graphical user interfaces and complex Command Line interfaces it can be used by both the new generation forensic investigators as well as the old ones, and provides both ease of use and inclusiveness in handling virtually all the forensics chores.

***Autopsy:*** Autopsy is the Sleuth Kit's GUI since it is one of the popular digital forensic tools. It provides an easy way to work with the file system and to analyze it as well as to recover files and get brief information about them. Can facilitate timeline analysis, keyword search and modules addition for virtually any type of investigations such as email investigation, web artifacts and Windows registry analysis [5].

***Sleuth Kit:*** The Sleuth Kit, abbreviated as TSK, is a set of commands which can be used to analyze disk images. TSK parses disk partitions, files and metadata to gain desired information. Eg., fls – a tool, used at a very basic 'low level' of 'forensic investigation,' along with other tools like, icat, istat and mmls [6].

Wireshark: Wireshark is a network protocol analyzer that captures and analyze network. Wireshark is useful in network forensics since it can filter out suspicious activities, dissect the communication profiles, and recreate the packet streams.

***Volatility Frame Work:*** Volatility is a powerful memory analysis tool that aims at identifying and extracting digital information from RAM dump. It can assist in detecting the presence of malware, rootkits, hidden processes and other potential violations [7]. They support plugins for different purposes, such as process listing, DLL injection detection, and connection scanning.

***Bulk Extractor:*** Utility that possibly looks for disk images, files, or directories to obtain specific information such as email addresses, URLs, credit card numbers, without comprehending the file system hierarchy. It is helpful for identifying potential data leaks or PII compromise.

***RegRipper:*** RegRipper, a tool developed for the analysis of Windows Registry files, contains several plugins that can be used to extract such information as user activities, malware activity, and system settings from Windows registry hive files.

***Xplico:*** A network forensics analysis tool (NFAT) capable of reconstructing network activity from PCAP files. Xplico can parse HTTP, VoIP, email (IMAP, POP3, SMTP), and FTP to identify malicious or suspicious traffic [8]. They help investigators in detecting files that may be concealed or dangerous to the security of a system.

**3. Integrated Workflow**

There many processes that occur in CAINE Linux and there are more specific tools that are used to ensure the whole process of forensic investigation is made to flow in the correct manner. Here's a breakdown of how CAINE does this:

***Unified Interface with Case Management:*** A CAINE has the application tools compartmentalized in one place making the shifting between tools easier as one practices on the GUI environment. The main working platform of CAINE contains a case management, where an investigator is able to create process and organize cases within the environment. This makes a record on all activities to be done on the case highly effective and documented and there are no way misconceptions or forgery gets into docketing of the case [9].

***Automated Evidence Collection and Documentation:*** Another method that makes the proof assortment method easier is the CAINEs Automation Software. Automation helps the investigator create scripts for performing various actions such as imaging, hashing, among others by just clicking the mouse. It also records every step made or taken and therefore it prepares comprehensive reports that may be used to keep proper records such as the chain of custody or to present results during a court session.

***Integrated Imaging and Acquisition Tools:*** A few of its applications include Multimodal Image Fusion and Acquisition. A number of applications kept in the CAINE suite includes program for disk imaging is: Guymager, dcfldd, and AIR (Automated Image & Restore). They are designed so that they can be connected in a smooth manner to allow the investigators to carry out disk imaging with integrated verification and hashing to confirm the accurateness of the duplicated data [10]. Every time a picture is once captured, it is already normalized and input directly to the case management system together with its hash values, among other pertinent data. The connection also helps to minimize the time for the manual handling of the data as well as the possibility of making errors in entry.

***Evidence Preservation and Write Protection:*** With this, there is a safeguard of the evidence and recommendation of disable of write protection. CAINE, everything is reopened in 'read-only' further disc operations on the source media do not inadvertently make changes. This is very important in maintaining the credibility of an evidence as it was at the time of collection. The ability to mount and unmount drives

is also included in the CAINE Mounter tool and there is an incorporated feature of write-blocking and also the feature that helps to maintain and preserve the evidence.

***Data Analysis and Correlation:*** Autopsy/Sleuth Kit Integration: Another thing is that CAINE perfectly complements Autopsy, which is The Sleuth Kit's shell, or a graphical interface, in other worlds. When it comes to disk images, they may be opened for the purpose of viewing the file system, to conduct a data carving in an attempt to recover lost files or may be opened for a timeline analysis all within the confines of Autopsy.

Volatility and Memory Analysis: through the integration with the Volatility Framework dumping analysis of memory can be done. Another advantage that the investigators have is that they transition from disk forensic analysis to memory forensic analysis easily.

***Cross-Tool Data Sharing:*** The idea is that with the help of CAINE it will be easier to exchange and exploit information in the technologies of the surroundings. For instance, result of an autopsy can be shared in file format and subjects to further examination using programs such as RegRipper to analyze the windows Registry or Bulk Extractor if keen focus is on specific type of data. This interface would eliminate the process in which investigators have to export data they have analyzed in one tool, and then import them in another tool manually, thus making their work easier and more accurate [11].

***Reports and Documentation:*** One can also mention that CAINE combines tools for automatic preparation of reports at the same time. The case management system provides reports that comprise details relating to all stages of the investigation from acquisition. Such important information may be documented in the reports in the form of the PDF as well as HTML in conjunction with the proofs such as screenshots and log files which in their turn may act as the evidential material.

## 4. Other Digital Forensics Distributions

### 4.1. Ubuntu-based distributions

Such Ubuntu distributions include DEFT, Helix, REMnux, Kali Linux which is an Ubuntu variant, CAINE, BackBox, and Tsurugi Linux – that come with an entire toolkit for the digital forensic and cyber security roles. Both distribution concerning add certain characteristics pertinent to specific components of the forensic processes, and for this reason, useful to the digital forensic experts and cyber security professionals. The distributions leverage on stability, security, and RPMs and DEB packages of Ubuntu to present advanced and accurate forensic tools and utility for investigators and anti-hacker.

***DEFT Linux (Digital Evidence & Forensics Toolkit):*** The operational system DEFT Linux offers investigators an effective toolkit for the analysis of digital evidence integrated into a live CD/DVD distribution. The tool comes with a complete package of tools for data acquisition, file system inspection, artifact extraction, network traffic analysis, and mobile device investigation. DEFT Linux also has a reputation of being friendly, easy to use and convenient to integrate with other forensic tools which make this a preferred choice by the investigators. The ability to allow investigators perform forensic actions while not influencing the system's evidence [12].

***Helix3:*** Helix3 is another platform that offers a number of instruments for the identification of digital evidence is digital forensics. It provides functionalities of; Data Gathering, File System Analysis and Recovery, Artifacts Recovery, Net traffic analysis and Mobile Device Analysis. The Helix3 solution is disguised as a processing tool and it is user-friendly with strong emphasis on managing and preserving the electronic evidence. It is common among the police, IT specialists dealing with cybercrimes, and the members of the digital forensics team. It has easy to use GUI interface with well-organized set of menus to run the tools/scripts with ease [13].

***Kali Linux:*** TheKali Linux is a Debian Linux based distribution which is specifically designed for penetration testing and ethical hacking. It is loaded with hundreds of tools and programs related to Security of Networks, like network port scanners, password auditors, vulnerability prober and exploit databases. The reasons as to why this tool is deemed as a suitable tool for security researchers, penetration testers and forensic Analysts include; It is similar in functionality with the basic Ubuntu and can access Ubuntu repositories while providing the same level of forensic and security possibilities [14].

### 4.2. Fedora-based distributions

Fedora distribution is the type of Linux operating system that is created using Fedora kernel for some specific purposes like forensic, security and incident handling. This distribution is unique for its highly

developed technologies, carefully thought security features, and complete compliance with the principles of free and open source software, the virtues that make Fedora the base for several specialized distributions.

***SIFT Workstation:*** IFT Workstation is a complex software in the field of digital forensics developed particularly for investigating officers to handle digital evidence. SIFT represents the toolkit of SANS Institute which provides rich opportunities and various tools for data collection, work with file systems, traffic investigation, and mobile device investigation. Program's clear and simple interface, as well as detailed documentation, and the well-developed community around SIFT, make it loved by both experienced and newcomers in the field of digital forensics [15].

***Fedora Security Lab:*** Fedora Security Lab is a project whose main aim is to enhance security of the Fedora Linux distribution. The primary goals of the lab include the task of identifying and fixing the security holes, developing the security tools and procedures and introducing security enhancements to Fedora. The work of the lab in research and development of Fedora makes it possible to achieve general security and stability in the Fedora system [16].

***Qubes OS:*** Qubes OS is designed to be secure operating system and it utilizes microkernel approach where programs and virtual machines are isolated from each other. This way it is easier to contain any virus or other forms of malignant software which may wish to penetrate the system. Qubes OS provides the best way of running risky applications such as browsers and email clients, but also protects the systems that are most necessary for a user, for example, file managers or operating systems [17]. However, it is most loved by security specialist and anyone who requires enhanced protection from hackers' attacks.

4.3. Proprietary Distributions

EnCase, Cellebrite, Magnet AXIOM, FTK, X1 Social Discovery, BlackLight, and Oxygen Forensic Detective are proprietary distribution that contain entire, and standard tool kits for a digital forensic examination, mobile forensics, and incident response. Because of these qualities of reliability, capability of supporting extensive features and legal, including court-admissible reporting, these technologies are trusted by professionals, involved in law enforcement, corporate security, and private inquiry.

***EnCase Forensic:*** EnCase Forensic is a commercial digital investigation tool which has all tools to analyze the digital evidence. These are data gathering, file system analysis, artifact extraction, network traffic analysis and mobile device forensic. This compact, yet powerful software is particularly popular among law enforcement agencies, cyber security experts and a business investigator due to its enhanced functions and easily navigable interface as well as prolonged functionality [18].

***FTK (Forensic Toolkit):*** FTK is one of the powerful digital forensics solutions in current days where it contains number of tools for investigation and analysis of the hard disk data. It helps in data gathering, file system scans, artifact capturing and also in the preparation of the report. FTK is designed to be easy to use and cost effective and that is why it is widely adopted by law enforcement, business investigators and digital forensic professionals [19].

**Table 1.** Comparing CAINE Linux with other distribution tools

| Tool | Base | Purpose | Target Market | Cost |
|---|---|---|---|---|
| Caine Linux | Ubuntu Based | Digital forensic and incident response | Digital forensic investigators and cyber security professionals | Open source |
| DEFT Linux | Ubuntu Based | Digital forensics and incident response | Cybersecurity professionals, and law enforcement agencies. | Open source |
| Helix3 | Originally Ubuntu | Digital forensics and incident response | Corporate investigator and | Open source |

| | | | | |
|---|---|---|---|---|
| | Later: Lubuntu | | cybersecurity teams. | |
| Kali Linux | Debian Based | Penetration testing and ethical hacking | Security professionals, ethical hackers, and IT administrators | Open source |
| SIFT Workstation | Originally by Ubuntu Other: Fedora | Digital forensics and incident response | Cybersecurity professionals, ethical hackers, and penetration testers | Open source |
| Fedora Security Lab | Fedora | Security testing, forensics, and system auditing. | Penetration testers, digital forensic analysts and system administrators | Open source |
| Qubes OS | Primarily Fedora-based | Security through compartmentalization. | Security-conscious users, privacy advocates, and digital forensic professionals | Open source |
| EnCase Forensics | Proprietary based | Disk imaging, data recovery, and investigation | Government institutions, corporate security teams, and digital forensic professionals | Proprietary |
| FTK (Forensic Toolkit) | Proprietary based | Process and interpret all of your digital evidence. | Enterprise security teams and digital forensics experts | Proprietary |

4.4. Portability and Flexibility of Digital Forensics Tools

It can now be readily seen that portability and flexibility are indeed important considerations in the selection of a digital forensics tool or distribution. They define the extent to which the tool can be implemented in various contexts, its compatibility with different hardware and software configurations, and how it can meet the peculiarities of selected cases.

CAINE Linux, DEFT Linux, and Helix3 these kinds of distributions are generally portable and flexible because they are open sourced and built by a community that allows for easy modification. similar to the previously mentioned distributions Kali Linux, SIFT Workstation, and Fedora Security Lab, here also there might be certain limitations or flexibility on what these distributions are used for and they offer good portability. As a virtualization-based OS, Qubes OS provides a high security and isolation level, and may seem restricted when it comes to portability and compatibility with other tools. EnCase Forensics and FTK (Forensic Toolkit) are Proprietary tools also have certain disadvantages due to the fact that being specific

software, they are restricted in many ways compared to its open source counterparts. However, they can provide specific functionalities and modes not present in other free software.

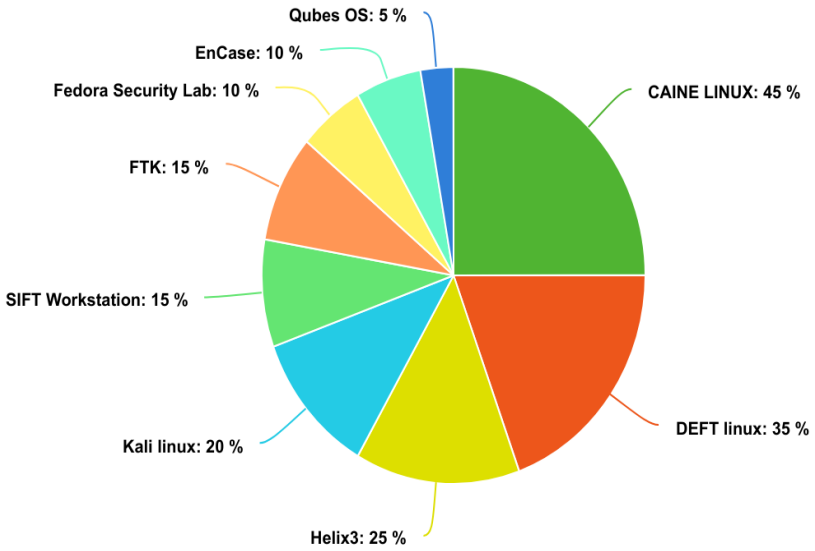


**Figure 1.** Portability and Flexibility comparison.

4.5. Usage-based Comparison of CAINE Linux Tools

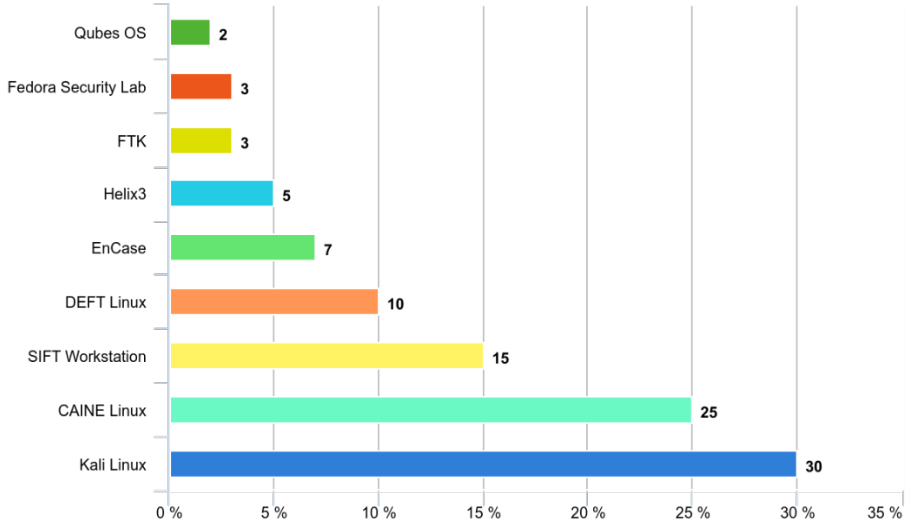


**Figure 2.** Usage-based comparison of CAIN Linux Tools

From all the tools, Kali Linux is the most used (30%) while CAINE Linux comes second at a 25% usage. A 15% usage ratio is also observed in SIFT Workstation. While DEFT Linux and EnCase Forensics are used at a lower rate of 10 and 7 per cent, respectively. There are other tools which are used by a few people including Helix3, FTK (Forensic Toolkit), Fedora Security Lab, and Qubes OS with usage ratios ranging from 2% to 5%.

## 5. Limitations and Challenges ion

When CAINE Linux is employed together with other digital forensic distribution, problems of libraries, dependencies, or kernel modules can occur. Although it may be convenient to run multiple distributions on the same system, there are compatibility issues which may arise especially from other tools that may not be compatible to such systems. This means that, in reference to other distributions, CAINE may not always be compatible with the particular set up or update hence interrupting its operations. Like nearly all the Linux distributions, CAINE Linux depends on certain compatibility in hardware. There could be hardware that are either old, or are of specialized use, which would not be compatible with the operating system or may not be supported as far as drivers are concerned. When using the hardware with unsupported drivers or with specific proprietary drivers, CAINE does not work optimally. Moreover, CAINE devoted tools are created specifically for certain file systems along with the data storage formats;

so, it has restricted capacity to deal with less widespread or custom developed programs. Being an open-source distribution, CAINE is updated and has its toolsets updated and the vulnerabilities fixed constantly thanks to contributors. Reviewing its usefulness time by time as well as need of updates and patches for protection against new threats and improved techniques can be a demerit for the users. While consolidating up-to-date systems, it is obligatory to monitor often, and this may not always be possible.

**6. Future Directions**

- Learn how to work with CAINE Linux, and how this can be extended notably with newer tech innovations like AI Machine Learning and Block chain. These technologies are capable of improving the features of the official digital forensics instruments for efficient investigation.
- Analyze the feasibility of CAINE Linux on clouds. This could offer advantage such as scalability, access and collaboration for the digital forensics team.
- Discuss the ethical issues of employing digital forensics instruments such as privacy and data protection as well as International cooperation. Define the principles for the proper and acceptable way to conduct the digital forensics investigations.

**7. Conclusions**

Therefore, this comparative analysis aims at defining CAINE Linux as an efficient and effective digital forensics distribution. It has been primarily criticized for the following reasons: it is an open source tool which has been extensively used for creating built-in forensic tools and its features that allow it to work in the live system mode while maintaining the evidential value of the material. With high flexibility, CAINE Linux provides convenience and ease for investigating various areas such as data acquirement, data examine, and compiling various reports as well as case management. It is highly flexible and can be run as a live USB or DVD environment so forensic investigators are able to perform tests and tasks in the real operating environment without its affecting the host system hence preserving the data integrity. But it does have its drawbacks: there are possible conflicts with other distributions besides, CAINE Linux is oriented on definite hard and software environment, and, finally, new users can experience some difficulties with it. Also, it can be stressed that the use of CAINE should be accompanied by its constant updates due to newly emerged threats and emerging issues in the field of digital forensics.

When compared to other tools like DEFT Linux, Helix3, Kali Linux, SIFT Workstation and the commercial ones like EnCase Forensics and FTK, CAINE Linux is a very light, flexible and comparatively cheaper tool. However, it would not perform very well on environments that need specific support and, or while handling lesser known file systems and extensions. Lastly, this research contributes to the knowledge on the strengths and weaknesses of CAINE Linux and would enable practitioners to make right decisions on the recommendation of the right digital forensics distribution required for an investigation.

**References**


1. Satish, S., Phadke, G., &Rawtani, D. (2023). Future aspects of modern forensic tools and devices. Modern Forensic Tools and Devices: Trends in Criminal Investigation, 393-413.
2. Alexander, B. Evaluation of Open-Source & Proprietary Forensic Software Tools.
3. Cardoso, S., Jean, H., Cherrier, M., Dubettier, A., Gernot, T., Giguet, E., & Rosenberger, C. (2023, October). Towards an Open-source Digital Investigation Platform. In 2023 International Conference on Cyberworlds (CW) (pp. 472-479). IEEE.
4. Khairunnisak, K., & Widodo, W. (2023). Digital Forensic Tools and Techniques For Handling Digital Evidence. Jurnal RESISTOR (RekayasaSistemKomputer), 6(1), 1-11.
5. Tretyak, M., Cherckesova, L., Korochentsev, D., Revyakina, E., & Popov, A. (2023). Internet platform for analyzing computer memory of Windows operating systems for conducting information security investigations. In E3S Web of Conferences (Vol. 402, p. 03027). EDP Sciences.
6. Suvarna, D., Mahesh, K. M., Gupta, M., Gabburi, S., Honnavalli, P., & Sapna, V. M. (2024, April). The Development of a Digital Forensic Framework for Ease of Forensic Analysis. In 2024 12th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.
7. Rawtani, D., & Hussain, C. M. (Eds.). (2023). Modern forensic tools and devices: Trends in criminal investigation. John Wiley & Sons.
8. Becker, E., Gupta, M., &Awaysheh, F. M. (2023, November). Analyzing Edge IoT Digital Forensics Tools: Cyber Attacks Reconstruction and Anti-Forensics Enhancements. In 2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 0991-0998). IEEE.
9. Menendez, D. (2021). Cyber forensic tools and utilities. In Cyber Forensics (pp. 335-358). CRC Press.
10. Moric, Z., Redzepagic, J., & Gatti, F. (2021). ENTERPRISE TOOLS FOR DATA FORENSICS. Annals of DAAAM & Proceedings.
11. Reedy, P. (2020). Interpol review of digital evidence 2016-2019. Forensic Science International: Synergy, 2, 489-520.
12. Patil, D. N., & Meshram, B. B. An Evidence Collection and Analysis of Ubuntu File System.
13. Zhang, J., Simisky, J., Tsai, F. T., & Geller, D. S. (2005). A critical role of helix 3–helix 5 interaction in steroid hormone receptor function. Proceedings of the National Academy of Sciences, 102(8), 2707-2712.
14. Cisar, P., & Pinter, R. (2019). Some ethical hacking possibilities in Kali Linux environment. Journal of Applied Technical and Educational Sciences, 9(4), 129-149.
15. Tyagi, S., & Yadav, D. (2023). ForensicNet: Modern convolutional neural network-based image forgery detection network. Journal of Forensic Sciences, 68(2), 461-469.
16. Du, J., Zhu, J., Liu, H., Chen, W., Xu, L., Liu, J., & Chen, Z. (2023). A Case Study of Dependency Network for Building Packages: The Fedora Linux Distribution. In SEKE (pp. 158-161).
17. Vepsäläinen, K. (2024). Cyber intelligence for anti-money laundering, counter-terrorism financing and know your customer.
18. Wangchuk, T., Tshering, Y., Mandela, N., &Rughani, P. (2024). Forensic analysis of Scientific Linux image using commercial and opensource forensic tools. Journal of Applied Engineering, Technology and Management, 4(1), 68-82.
19. Alshammari, A. (2023). Detection and Investigation Model for the Hard Disk Drive Attacks using FTK Imager. International Journal of Advanced Computer Science and Applications, 14(7).
20. Khan, M. I., Khan, Z. A., Imran, A., Khan, A. H., & Ahmed, S. (2022). Student performance prediction in secondary school education using machine learning. In 2022 8th International Conference on Information Technology Trends (ITT) (pp. 94-101). IEEE.
21. Hafeez, M. A., Imran, A., Khan, M. I., Khan, A. H., Nawaz, A., & Ahmed, S. (2022). Diagnosis of liver disease induced by hepatitis virus using machine learning methods. In 2022 8th International Conference on Information Technology Trends (ITT) (pp. 154-159). IEEE.