Aftab *et al. (IJECI)* 2024

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2024.0801189

(IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

Research Article

Vol. 8 issue 1 Jan-Mar 2024

Digital Investigations: Navigating Challenges in Tool Selection for Operating System Forensics

Kausar Parveen and Ghulam Haider

Department of Computer Sciences, University of Engineering and Technology, Lahore
Corresponding author: kausarnawaz6@gmail.com

Received: December 31, 2023; **Accepted:** January 18, 2024; **Published:** March 15, 2024

ABSTRACT

The process of gathering, identifying, extracting, and documenting electronic evidence for use in court is known as "digital forensics." We have a lot of tools at our disposal to make this procedure quick and straightforward. Four tools have been selected for investigation and analysis in this work. For every kind of digital forensics, the top tools have been selected based on several criteria. For computer forensic tools, (Stellar and Forensic Tool Kit) have been investigated; for network forensic tools, Network Map has been selected, and OSF mount has been examined as a live forensic tool. Other forensic tool types, such as database, operating system, and mail forensic tools, are also covered in this work. The role of Artificial intelligence in Digital Forensic tools has been discussed in this paper by using both Decision Stump and Bayes net machine learning techniques. After making an investigation of the IoT device traffic dataset using these two techniques, Decision Stump gives us less accurate results compared with Bayes net.

Keywords: Forensics tool, Digital Evidence, Artificial intelligence, Forensic Analysis, Challenges.

1. INTRODUCTION

The market for electronic devices, such as laptops, PCs, and portable electronics, is growing rapidly. Since these gadgets are networked and consume a lot of data, cybercrime is thought to be mostly caused by the Internet. Comparing digital forensics (DF) to other forensic sciences, DF is still in its infancy. DF science's involvement begins after the crime has committed [1]. The process of gathering, identifying, extracting, and documenting electronic evidence from various electronic devices for use as admissible evidence in a court of law is known as digital forensics (DF). [2]. The inquiry method mostly relies on the DF tools, which will yield efficient and productive outcomes. They are different types of data to deal with these tools like the Internet of Things (IoT) devices data, computer devices, mobile devices cloud computing, etc. [3]. Most of these tools' goals are to collect and recover the original files from the devices. DF tools are used for solving problems related to computer crimes like phishing, money laundering, bank Fraud, and child exploitation. The most of shreds of evidence have been found on computers [4]. As shown in figure 1, DF tools are divided into computer forensics network forensics, live forensics, Operating System forensics, database forensics, and Mail forensics. As a part of Artificial intelligence (AI) machine learning (ML) generally and deep learning especially have an important role in DF. As we know the AI technique can work with big data in a short time with accurate results. So, AI helps the investigators in the DF analysis process. The exuberance of forensic tools will make it hard for users to choose the relevant tool for their requirements [4], [5]. So, we explored the most popular tools and collect information about others to make a comparison between them. However, the investigator can choose the appropriate one for him and for the crime that he will investigate.

The top DF tools for computer, network, and live forensic tools were identified in this study based on a number of crucial factors that are taken into account for each category. For instance, whereas port scanning and packet analysis are crucial elements for network forensic tools, imaging and hashing are significant factors in computer forensic tools. RAM dumps and live log analysis are crucial requirements for real-time forensic technologies. The use of Artificial intelligence in DF tools has been discussed in this paper by using both Decision Stump and Bayes network machine learning techniques on IoT device datasets and a comparison between them has been made. Decision Stump gives us less accurate Results were compared with Bayes net, which is less concerned about the attributes or their relationships. On the other hand, the best outcomes were obtained from Bayes Net, as it effectively represented the conditional dependencies among a set of random variables. Each node in the network signifies a variable, and each directed edge represents a conditional relationship.

2. LITERATURE REVIEWS

They examined many DF analysis techniques in [4]. It claimed that the pattern recognition method is ideal for the DF's analysis step. Numerous DF tools are developed using characteristics derived from the detected patterns. Therefore, a variety of tools are crucial for finding solutions to all of the disputes that arise throughout the execution phase, in addition to being employed for the preservation and analysis of individual pieces of evidence data. Various methods for both live and dead forensic analysis were discussed in [6]. In addition to creating an understandable environment to aid a detective, it retains the crucial instructions from several DF programs, like WIRESHARK, Autopsy, O.S. forensic, TRUECRYPT, Forensic Tool Kit (FTK) Imager, and SANS SIFT. Besides, they accumulate information that can be transformed using live analysis, which sidesteps destroying the information due to the stoppage of the target node. [7] said the major process done by criminals is for destroying files by deleting, damaging, or overwriting hard disks, etc. The team only focused on how to recover the destruction data. To recover the damaged data with the help of different tools such as WIRESHARK, Autopsy, TRUECRYPT, FTK Imager, Operating system forensic, X-WAYS, and SANS SIFT. Researchers in [8] explained the attributes, constrictions, and applications of DF tools and compared them with other tools in assisting investigators or users in employing composite DF tackles for their inspection. [9] employed a machine learning technique and advising a scheme to diagnose abnormal packets and attacks. Naive Bayesian provided the best accuracy against other classifiers. [10] used NLP techniques to analyze DF shreds of evidence. [11] focused on the recent readiness and advances of DF tools in the composite atmosphere. [12] proposed a method to build a new intelligence DF model for storehouse willingness. [13] suggested an effective model for DF cloud Investigation called Cloud Forensics Investigation Model (CFIM) to pattern the crimes happening in the cloud forensically. [14] proposed a DF framework methodology for the social media network community. This system contains operative classifying digital devices, procedures, analyzing and obtaining DF pieces of evidence. [7] showed DF terms in the cyber world and informed a comparative analysis of the current stream state of forensics. [15] proposed building architecture for AI applications in the DF especially in the analysis stage. [16] described an analysis of up-to-date DF artificial intelligent schemes to raise these procedures in forensic correction. [17] said that the compression of data can disturb different DF stages. [18] analyzed different ML techniques and their usability in recognizing evidence by tracking file systems. The Machine Learning algorithms achieved good outcomes. [19] proposed a classification model for network traffic using Machine Learning techniques. The results revealed that the best outcome had been done by a random forest classifier. [20] analyzed network traffic to discover windows ransomware by spread on ML and accomplished a Total Form (TF) a percentage of 97.1% with the decision tree method. Researchers in [21] proposed a process of the text description of Natural Language Processing and spam email discovery. [22] suggested a model for the cataloging of attacks in the cloud atmosphere using ML procedures with a DF method. [23] proposed model of managing intellectual cybersecurity. The model practices AI procedures to make the analysis procedure of cybersecurity more proficient compared with old-style security instruments. Through the speedy development of technologies, it is important to select DF methods and frameworks. DF methods from 2015 to 2022 are offered in the next lines. [24] examine the environments, cruise anomaly information, and control relation report. [25] Conformist data collection process strategy, provision law of shaping the consistency of the DF pieces of evidence. [26] study the DF on IEC/ISO ethics. [27] employing Digital Forensic Readiness (DFR) mechanism in amenability through the IEC/ISO ethics. [28] proposed a model based on Online Natural Language Processing (NLP) for forensic investigation. The paper compared different DF tools in different groups such as computer Forensic Tools, Network Forensic Tools, O.S Forensic Tools, Live Forensic Tools, Database forensic tools, and Email Forensic Tools. Consequently, the investigators can choose the accurate tool used for their requirements easily.

Table 1: Analysis by using various techniques.

Ref.	Key Focus	Techniques/Tools	Findings/Contributions	Loopholes Analyzed
[4]	DF Analysis	Pattern Recognition Method	Examined various DF analysis techniques, emphasized the importance of pattern recognition in DF's analysis step.	-
[6]	Live and Dead Forensic Analysis	WIRESHARK, Autopsy, O.S. forensic, TRUECRYPT, FTK Imager, SANS SIFT	Explored methods for both live and dead forensic analysis.	-
[7]	Data Recovery	WIRESHARK, Autopsy, TRUECRYPT, FTK Imager, OS Forensic, X-WAYS, SANS SIFT	Focused on recovering data destroyed by criminals. Used different tools for data recovery.	Destruction of files by deleting, or overwriting hard disks, etc.
[8]	DF Tools Comparison	Various DF Tools	Explained attributes, constraints, and applications of DF tools. Compared DF tools with other tools for investigator assistance.	-
[9]	Machine Learning	Naive Bayesian	Used machine learning to diagnose abnormal packets and attacks. Naive Bayesian provided the best accuracy.	Abnormal packets and attacks.
[10]	NLP Techniques	NLP	Used NLP techniques to analyze DF shreds of evidence.	-
[11]	Recent Advances	-	Focused on recent readiness and advances of DF tools in a composite atmosphere.	-
[12]	Intelligence DF Model	-	Proposed a method to build a new intelligence DF model for storehouse willingness.	-

[13]	Cloud Forensics	Cloud Forensics Investigation Model (CFIM)	Suggested an effective model for DF cloud investigation called CFIM.	Crimes happening in the cloud
[14]	Social Media DF	DF Framework Methodology	Proposed a DF framework methodology for the social media network community.	Operative classifying digital devices
[15]	AI Applications	AI in DF Analysis	Proposed building architecture for AI applications in DF, especially in the analysis stage.	-
[16]	AI Schemes	AI in Forensic Correction	Described an analysis of up-to-date DF artificial intelligent schemes to improve forensic	-
[17]	Data Compression	-	Stated that data compression can disturb different DF stages.	-
[18]	ML Techniques	Machine Learning Algorithms	Analyzed different ML techniques for recognizing evidence by tracking file systems. Achieved good outcomes.	Usability in recognizing evidence by tracking file systems.
[19]	Network Traffic	Machine Learning Techniques (Random Forest)	Proposed a classification model for network traffic using ML techniques..	-
[20]	Ransomware Detection	ML (Decision Tree)	Analyzed network traffic to discover Windows ransomware using ML.	Windows ransomware detection.
[21]	NLP and Spam Email	Natural Language Processing	Proposed a process for the text description of NLP and spam email discovery.	Spam email discovery.
[22]	Cloud Attacks	ML Procedures with DF	Suggested a model for cataloging attacks in the cloud atmosphere	Cataloging attacks in the cloud atmosphere.
[23]	Cybersecurity	AI Procedures	Proposed a model of managing intellectual AI procedures.	Analysis procedure of cyber security.

3. DIGITAL FORENSIC STAGES

In DF the first prototypical suggested has four stages: Collection, Identification, Assessment, and Admission. different prototypical is suggested to describe the stages of collecting, analyzing, preservation, and reportage of the pieces of evidence produced by many devices. Recently, a growing number of extra complicated prototypical are suggested. The goal of these models is to speed up the whole investigation procedure. The variety of sources and devices of digital shreds of evidence results in a variety of DF procedure models [29]. There is no common procedure model appropriate to use for all forms of the investigation process. [30]. Figure 2 shows the different stages of DFs. The role of each phase is discussed below:

Despite DF being a new study zone, already has completed important growth. The growth is done by the enhancement of methodologies and technology, for example, tools for gathering and analyzing DF pieces of evidence. In DF, a method to do an investigation process is called a process model which is a context with a sum of stages to do an investigation. In DF investigation a standard methodology should define the sequence of actions need in the investigation process. A perfect process model should be wide-ranging, which means it should be applied to a large number of cases. If a framework is very simple and has fewer phases, the result is not provided good guidance to the process of investigation. Otherwise, if a framework has more stages with sub-steps of each stage, the result is more limited to its usage. Many studies place special attention on outlining the whole DF investigation process; significant DF frameworks were covered in [31]. More recently, development on the DF framework has focused on addressing more specialized issues such as gathering, examining, analyzing, and preserving evidence in a single phase. For instance, the triage paradigm [4], works well in circumstances when time is a crucial factor. By using the DF pledge, investigators

may obtain information about the illegal more quickly than they would have to wait for all reports, which might take weeks, months, or even longer.

4. IDENTIFICATION STAGE

At this point, the evidence is defined, examined, and its position and source are determined. Evidence shreds need to be handled carefully and correctly. This stage's objective is to safeguard the evidence's integrity. It should be safeguarded in conjunction with a record known as the Chain of Custody (COC), which is identified by the DF connection, the paper trail, or the DF evidence's sequential certification. It shows the gathering, transfer, control sequence, and analysis.

5. ACQUIRING STAGE

For more analysis, this stage helps to save the state of the pieces of evidence. In this stage, hard disk imaging is done as a copy of the data on the hard disk. Three kinds of acquisition are accepted according to law enforcement forensic duplication, mirror image, and live acquisition. A mirror image makes a forensics duplication which saves the backup of the device's hard disk as a bit-for-bit cloning copy.

6. ANALYSIS STAGE

Three types of analysis can be performed at the analysis stage: restricted, partial, or complete analysis. The narrow study only considers a small portion of the available data. While full inquiry aids in determining the initial cause of the crime, partial analysis works with cookies, log papers, email files, etc. [4] Several tools made for the analysis step, such as Encase and FTK, which can handle a lot of scripts to extract information from the data that has to be examined.

7. REPORTING STAGE

The reporting stage helps to deduce, in a documented report form based on pieces of evidence. This is done with the help of digital crime laws represent the information for further investigation.

8. DIGITAL FORENSIC TOOLS

The software programs created for the DF investigation process in digital crimes are known as digital forensic tools. There are several DF tools available on the market. They also come in generic or commercially licensed versions. In this paragraph, we shall discuss DF tools in several groups and conduct a proportionate analysis of different tools within each group. A variety of factors, including technological considerations, general concerns, disk imaging, string searching, and legal difficulties, have been taken into account while choosing DF tools.

8.1. Computer forensic tools

Computer DF tools are intended to certify that the pieces of evidence taken out from computers are correct and dependable. There are different types of computer DF tools like Data and Disk seizure DF tools. A comparative investigation of five Computer forensic tools based on feature parameters questions have been made. For example, hashing, imaging, and data recovery. In this paper, the Stellar tool and Forensic Tool Kit (FTK) have been explored in this review for computer forensic analysis. Stellar: Stellar tool helps the investigator to find all files they want from the computer disk. Stellar is designed to be a comprehensive recovery tool to help its users to deal with all types of data loss scenarios, without needing any expert knowledge. Digital investigators can do normal or deep scanning. Figure 5 show the deep scanning mode. It does a whole signature-based file search which is useful for recovering the files that normal scanning could not found it.

Access Data's Forensic Toolkit, or FTK, is a computer forensics tool that searches a hard disk for various types of data. For instance, it can look for text strings on a disk or in deleted emails in order to decrypt encryption by utilizing them as a dictionary of passwords. Forensic Tool Kit Imager is a disk imaging application that is also connected to FTK. This program creates an image clone of a hard drive, generates hash values (such as Secure Hash Algorithms (SHA1) or Message-digest Algorithms (MD5)), and verifies the integrity of the result by comparing it to the original. Using the FTK tool throughout the file analysis process, the forensic data picture may be stored and examined in a variety of formats, including E01, DD/raw, and AD1.

Table 1 has the comparison of key parameters like imaging which is a technique of copying physical storage for making investigations and gathering shreds of evidence. The copy does not only include files, but every bit, sector, partition, files, deleted files, folder, and also unallocated spaces. The copy image is identical to all the device or drives architecture and contents. The second key parameter is hashing, the professionals in Digital forensics should use hashing algorithms, like MD5 and SHA1, to produce hash values of the original files which they use in an investigation to ensure that the pieces of evidence are not changed or modified during the investigation, pieces of evidence collection and analysis so they protect their integrity. Another reason for using hash values is that electronic pieces of evidence are shared with various parties during the investigation process like legal professionals, law enforcement, etc. So, we need to ensure that everybody has the same copies of the pieces of evidence. Stellar forensics that we chose to explore in this study calculates hash values automatically.

8.2. Network Forensic Tools

Network forensics works through interpreting and controlling networks to make an intrusion detection and find unknown malicious and abnormal threats through networks and their associated devices. The Nmap DF tool has been discovered in network investigation in this paper as shown in Figure 8. Network Map: This program examines the replies to packets sent in order to identify hosts and services on a computer network. We may probe networks using Nmap's many services, which include sophisticated services like vulnerability detection, host finding, and O.S. detection. Nmap may also work in varied situations of the network such congestion, latency, and high traffic during the scan process.

8.3. Live Forensic Tools

Active systems are the focus of live forensic. It concentrates on RAM attribute extraction and does a forensic analysis for it. Therefore, live forensics offer reliable and accurate data for investigations, which is far superior than the insufficient data from previous DF processes. We investigated the OSF mount tool as a live forensic tool in this article. Because it mounts image files produced by disk cloning programs such as OSF Clone, it is known as OSF mount. With OS Forensics, which is mounted as a virtual disk on Windows, the picture file may be examined. You may also use the OSF Mount Forensic program to mount CD-ROMs and DVDs as RAM drives.

Four live DF tools are chosen grounded on key parameters like dealing with Search, Logs analysis, memory dumping, and Live logs analysis which is the process of taking all the content in RAM and writing it to a storage device.

8.4. Other Forensic Tools

There are sub-branches of forensic tools like Database Forensic tools, O.S Forensic tools, and Email Forensic tools. These three types of tools have been explored in this section. Critical data is warehoused in various Database Management System (DBMS) i.e., Oracle as a Relational Database Management System store commercial data, MySQL work with web stores as a back-end packing, while SQLite stores personal data like SMS and browser bookmarks. So, databases need their special set of forensic tools. DF investigators still need the necessary DF tools to investigate Database Management Systems forensic objects. Also, we require to establish a special standard for artifact storage and its mechanisms to develop advanced analysis tools for Database. Operating System Forensics tools are used for recovering and gathering important information from the Operating System of the device. The goal is to find practical proof against the criminal. Four methods are used for Operating system forensics: disk-to-disk clone, disk-to-image file, disk-to-data file, and the backup of a file. This tool identifies abnormal files and makes a hash-matching signature. In a live manner, the data has been loaded and exported with all key parameters like module, run count, title, file size, category, last run time, date, time, etc. then, the report is generated and presented to the investigator includes I/O read-write, threads, total CPU, etc. Emails played an important role in communication through the internet like business communications and transmitting information between different devices. Unfortunately, there are a lot of encounters in email DF, for example, spoofing, forged emails, and Unsigned Re-emailing. Investigator has to collect the proof, identify the criminal, and show up the judgments. It can work with various Email formats, for example, .msg, emlx, .pdf, .mht, xps, etc. by examining header information, message body content, and other key parameters like time. In addition, it has a filtering option, exporting, saving, and analysis.

8.5. Digital Forensics Tools Evaluation Metrics

To enable the community of investigators to independently assess different tools, it is crucial to verify DF technologies using a variety of criteria. Additionally, developers will identify the areas of a tool that need improvement. Metrics should encompass all of the DF Tools' properties in order to achieve exceptional accuracy and meet all criteria. There hasn't been much study on the metrics of DF Tools in this subject, despite the proposal of a few techniques up until recently. A solution was put out by [32] who defined metrics to count the number of files generated by the list of files (referred to as the precision rate) and the number of pieces of evidence correctly created from the list of pieces of evidence (referred to as the accuracy rate).

The publication proposed a mechanism for assessing the tool's performance. The outcome is accurate if the evidence that has been replicated is identical to the original. An MD5 hashing technique can be used for this. Unfortunately, there are drawbacks to this approach as well. For instance, since the signatures will be altered, it is ineffective if a single bit is lost or altered during the collecting phase. Additionally, while the tool is not the source of issues like disk damage, the collection step may not retrieve the exact pieces of evidence.

8.6. Use Of Artificial Intelligence in Digital Forensic Tools

Digital investigators have a difficult time finding pieces of evidence in digital information. It has become difficult to specify an investigation and its source of proof. The various technology, specific procedures, and processes used in the DF investigation are not keeping up with the development of criminals. So, criminals use these weaknesses to do their crimes. Artificial intelligence (AI) is very important in identifying crime in DF investigations. An algorithm based on AI is very effective and highly recommended in detecting and preventing risks and criminal activity. Also, it is important in forecasting illegal activity. Researchers have used the available evidence data in court to condemn a person. The pattern recognition techniques are the best for the Analysis stage of the DF. Recognition of the Pattern has two procedures. The first is an examination and the other one is recognition. The features are taken out from the patterns to be recognized in the analysis step. Then, applying different methods of pattern recognition to these features are practical for DF investigation. These techniques are projected to improve diverse DF tools to identify and gather pieces of evidence that would be cooperative to deal with explicit kinds of digital criminalities. For example, the Jaro Winkler algorithm [33]and Cosine similarity function [34] are considered advanced pattern recognition algorithms for identity resolution in DF they are typically based on making similarity metrics for more complex strings. The increasing popularity of IoT devices and their privacy concerns encourage us to choose an IoT device traffic to analyze and make some investigations. We chose an IOT Fridge device traffic dataset from the University of New South Wales (UNSW) Canberra at Australian Defense Force Academy (ADFA). It contains six attributes (Time, date, temperature, condition, label, type) with full training set classifier. We examine this dataset using two different machine-learning techniques. We chose these techniques because they are two separate concepts. The first one is the decision stump tree which is the ML technique of a single-level of decision tree. Decision stumps frequently work with apparatuses named base learners or weak learners in ML. For nominal attributes, it builds a stump that has a sprig for every probable attribute rate or a stump has a double of leaves, the first one matches a specific class, and the second one has matched all the other classes. The second machine learning technique we used is the Bayesian network, it is ideal for predicting the probability of several possible known causes the occurrence of an event was the contributing factor. As we see in Table 6, compared with Bayes Net, Decision Stump gives us less accurate results because it does not care that much about the attributes or their relationships. It focuses only on how these attributes affect the target.

On another hand, the best results, we got from Bayes Net were because it represents a conditional dependency of a set of random variables. Each node in the network represents a variable, and each directed edge in the network represents a conditional relationship the Confusion Matrix of Bayes net.

These findings highlight the need for a digital inquiry and resolution in order to safeguard an IoT device owner's privacy. It also shows how important artificial intelligence methods are in this industry, particularly machine learning methods, and how continuing legislative discussions around ISP data collecting and utilization need to take IoT-specific issues into account.

9. CHALLENGES

The limits of the DF tools are highlighted in this section. In [35], four DF issues have been highlighted. The first is the difficulties with law enforcement and the legal system, which include issues with jurisdiction, privacy, legal procedure, inadequate provisions for criminal cases, standards, and the paucity of research on DF Tools. Second, technological difficulties with huge data, cloud computing, encryption, instability, and overuse of bandwidth. Thirdly, a lack of defined procedures, skilled specialists in DF, and a lack of unified formal representation and forensic understanding. Fourth, the difficulties in determining the incidence response, the reliability of audit trails, and the preparedness of DF. The globule in the hard drive with the computer storage capacity was the main focus of the researchers in [17]. The development of cameras, computers, and portable electronics is another. [36] highlights the massive data of DF challenge, especially in the Internet of Things (IoT), and suggested a data modification process in DF by distinguishing the imaging in a massive amount of forensic data. [37] emphasized DF process limitations with cloud atmosphere like volatility, namely records, data integrity, and creation of the forensic image. [38] presented DF process difficulties with the smartwatches.

10. CONCLUSION

An adequate investigation and incident response strategy must be employed to complete the inspection in the event of any digital crime or assault. The steps of DF inspection were discussed before along with a comparison of several DF Tools. The sort of crime or attack will determine which instruments are used for the investigation. Artificial Intelligence (AI) is playing a significant role in analysis and prediction. To determine which is better, many machine learning techniques are used, and they are validated using various metrics. The paper analyzed various tools like Computers, Networks, Databases, O.S, Live, and Mail DF Tools. In computer forensics, the Stellar tool has been chosen relatively to a comparison with other tools according to some features like imaging, hashing, recovery data, reparation capability, seizure, acquisition, and availability. In network forensic Nmap tool has been chosen according to some features like Port scanning, Packet analyzing & spoofing topology and protocol analyzing, and availability. OSF mount for the live forensic tool has been chosen according to some features in this study according to Live log analysis, RAM dumping, search, and availability. It likewise introduced the tender of AI in the DF framework. Additionally, some challenges are emphasized through supplementary the DF examination procedure. The future road of DF research should focus on the main challenges in this field like IoT forensics, Cloud DF as a service, big data, and new tools of DF. For example, determining specific data in IoT is stimulating the investigator to identify where to locate or straight the examination. Accordingly, the above challenges can consider as a research opportunity to continue in this field. As we mention before, the main problem in DF is the big forensic data, especially in network forensics and IOT forensics. Therefore, handling huge data in a trustworthy forensic manner is a major difficulty in DF, and this is seen to be an excellent chance for the researchers to develop new methods and tools to handle this large data. With DF, researchers may also employ artificial intelligence approaches. For instance, they can use natural language processing (NLP) to analyze DF data and Artificial Neural Networks (ANN) to recognize complex patterns in a variety of DF branches. In order to provide us with the ideal inquiry outcomes, future study should also concentrate on creating cutting-edge methods and instruments to examine more complex settings, such as clouds and networks that resemble cyberspace.

REFERENCES

[1] K. K. Sindhu and B. B. Meshram, "Digital Forensics and Cyber Crime Datamining" Journal of Information Security, vol. 3, no. 3, pp. 196-201, 2012.

[2] J. K. Alhassan, R. T. Oguntoye, S. Misra, A. Adewumi, R. Maskeliunas, and R. Damasevicius, "Comparative evaluation of mobile forensic tools", Advances in Intelligent Systems and Computing, vol. 721, pp. 105-114. 2018.

[3] O. Osho, U. L. Mohammed, N. N. Nimzing, A. A. Uduimoh, and S. Misra, "Forensic Analysis of Mobile Banking Apps", Computational Science and Its Applications, 2019, pp. 613-626, 2019.

[4] S. Sachdeva, B. L. Raina, and A. Sharma, "Analysis of Digital Forensic Tools", Journal of Computer Theoratical Nanoscience, vol. 17, no. 6, pp. 2459-2467, 2020.

[5] H. Hibshi, T. Vidas, and L. Cranor, "Usability of forensics tools: A user study", 6th International Conference on IT Security Incident Management and IT Forensics, pp. 81-91, 2011.

[6] C. H. Yang and P. H. Yen, "Fast Deployment of Computer Forensics with USBs", Journal of Computer Theoratical Nanoscience, vol. 10, no.6, pp. 114-123. 2010.

[7] D. Joseph and K. Singh, "Review of Digital Forensic Models and A Proposal For Operating System Level Enhancements", International Journal of Computer Science and Information Security, vol. 14, pp. 797-806, 2016.

[8] J. U. Lee and W. Y. Soh, "Comparative analysis on integrated digital forensic tools for digital forensic investigation", IOP Conf Ser Mater Sci Eng, vol. 834, no. 1, p. 12-34, 2020.

[9] A. Abirami and Palanikumar, "Proactive Network Packet Classification Using Artificial Intelligence", Computational Science, pp. 169-187, 2021.

[10] F. Amato, G. Cozzolino, V. Moscato, and F. Moscato, "Analyse digital forensic evidences through a semantic-based methodology and NLP techniques", Computer Systems, vol. 98, pp. 297-307, 2019.

[11] T. Wu, F. Breitinger, and S. O'Shaughnessy, "Digital forensic tools: Recent advances and enhancing the status quo", Digital Investigation, vol. 34, p. 30-39, 2020.

[12] J. Cosic, C. Schlehuber, and D. Morog, "Digital Forensic Investigation Process in Railway Environment", International Conference on New Technologies, Mobility and Security, pp. 1-6. 2021.

[13] E. E. D. Hemdan and D. H. Manjaiah, "An Efficient Digital Forensic Model for Cybercrimes Investigation in Cloud Computing", Multimedia Tools Applications, vol. 80, no. 9, pp.

14255-14282, 2021.

[14] Y. J. Jang and J. Kwak, “Digital forensics investigation methodology applicable for social network services”, Multimedia Tools Applications, vol. 74, no. 14, pp. 5029-5040, 2015.

[15] S. Costantini, G. D. Gasperis, and R. Olivieri, “Digital forensics and investigations meet artificial intelligence”, Ann Math Artif Intell, vol. 86, no. 1, pp. 193-229, 2019.

[16] A. Krivchenkov, B. Misnevs, and D. Pavlyuk, “Intelligent Methods in Digital Forensics: State of the Art”, Networks and Systems, pp. 274-284. 2019.

[17] D. Quick and K.-K. R. Choo, “Impacts of increasing volume of digital forensic data: A survey and future research challenges”, Digit Investigation, vol. 11, no. 4, pp. 273-294, 2014.

[18] R. Mohammad and M. Alq, “A comparison of machine learning techniques for file system forensics analysis”, Journal of Information Security and Applications, vol. 46, pp. 53-56, 2019.

[19] J. Pluskal, O. Lichtner, and O. Rysavy, “Traffic Classification and Application Identification in Network Forensics”, Advances in Digital Forensics, pp. 161-181. 2018.

[20] O. M. K. Alhawi, J. Baldwin, and A. Dehghantanha, “Leveraging machine learning techniques for windows ransomware network traffic detection”, Advances in Information Security, vol. 70, pp. 93-106, 2018.

[21] S. Srinivasan, V. Ravi, M. Alazab, S. Ketha, A. Al Zoubi, and S. Padannayil, “Spam Emails Detection Based on Distributed Word Embedding with Deep Learning”, Digital Investigation, pp. 161-189, 2018.

[22] S. Sachdeva and A. Ali, “Machine learning with digital forensics for attack classification in cloud network environment”, International Journal of System Assurance Engineering and Management, vol. 13, no. 1, pp. 156-165, 2022.

[23] I. Sarker, “Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects”, Annals of Data Science, pp. 1-26, 2022.

[24] A. R. Jadhao and A. J. Agrawal, “A Digital Forensics Investigation Model for Social Networking Site,” Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, 2016.

[25] R. Montasari, “A standardised data acquisition process model for digital forensic investigations”, pp. 23-28, 2017.

[26] I. Kigwana, V. R. Kebande, and H. S. Venter, “A proposed digital forensic investigation framework for an eGovernment structure for Uganda”, IST-Africa Week Conference

(IST-Africa), pp. 1-8. 2017.

[27] A. Singh, I. Adeyemi, and H. Venter, "Digital Forensic Readiness Framework for Ransomware Investigation", 10th International EAI Conference, ICDF2C 2018, New Orleans, LA, USA, pp. 91-105, 2019.

[28] D. Sun, X. Zhang, K.-K. R. Choo, L. Hu, and F. Wang, "NLP-based digital forensic investigation platform for online communications", Computer Security, vol. 104, pp. 10-22, 2021.

[29] X. Du, N.-A. Le-Khac, and M. Scanlon, "Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service", Multimedia Tools Applications, vol. 14, no. 4, pp. 50-54, 2017.

[30] M. Scanlon, "Battling the digital forensic backlog through data deduplication", Sixth International Conference on Innovative Computing Technology, pp. 10-14, 2016.

[31] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, "Integrated Digital Forensic Process Model", Computer Security, vol. 38, pp. 103-115, 2013.

[32] B. Hitchcock, N.-A. Le-Khac, and M. Scanlon, "Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists", Digital Investigation, vol. 16, pp. 75-85, 2016.

[33] C. Dietzel, T. U. Berlin, D. Cix, M. Wichtlhuber, G. Smaragdakis, and A. Feldmann, "Stellar: Network Attack Mitigation using Advanced Blackholing", pp. 3-9, 2019.

[34] DHS, "Access Data Forensic Toolkit (FTK) Version, Test Results for String Search Tool", Computer, pp. 19-23, 2016.

[35] K. M. A. Kamal, M. Alfadel, and M. S. Munia, "Memory forensics tools: Comparing processing time and left artifacts on volatile memory", International Workshop on Computational Intelligence, pp. 84-90, 2016.

[36] A. Dizdarević, S. Baraković, and J. Baraković Husić, "Examination of Digital Forensics Software Tools Performance: Open or Not?", International Symposium on Innovative and Interdisciplinary Applications of Advanced Technologies, pp. 442-451, 2020.

[37] D. Quick and K. K. R. Choo, "Digital Forensic Data Reduction by Selective Imaging", Computer, pp. 69-92, 2018.

[38] A. Shaaban and N. Abdelbaki, "Comparison study of digital forensics analysis techniques", Procedia Computer Science, vol. 141, pp. 545-551, 2018.