Navigating the cyber forensics landscape a review of recent innovations

Gyana Ranjana Panigrahi[1], Nalini Kanta Barpanda[2], Prabira Kumar Sethy[3]
[1]Department of Electronics, Ph.D. Scholar, Sambalpur University, Odisha, India
[2]Department of Electronics, Faculty of Engineering, Sambalpur University, Odisha, India
[3]Department of Electronics and Communication Engineering, Guru Ghasidas Vishwavidyalaya, Bilaspur, India

Article Info

Article history:

Received Jul 7, 2023
Revised Oct 14, 2023
Accepted Nov 5, 2023

Keywords:

Cybercrimes
Digital forensics
Digital investigations
Oxygen forensic suite
Prodiscover

ABSTRACT

The extensive relevance of digital forensics in today's data-driven environment has been emphasized in this article. The free software and the commercial software community are debatable, despite users and developers often differing views on important topics like software safety and usability. This article primarily uses pre-defined criteria and a platform-oriented approach to examine promising freeware (Magnet Forensics and Sleuth Kit) vs. profitable (ProDiscover and Oxygen Forensic Suite) mobile forensics tools. Under diverse settings, the tools' capacity to develop and analyze forensically sound digital forensic media sources is validated. After erasing data, each media type was tested again after formatting. The study concludes with a comparison matrix that may aid in determining the best-fit option for the investigation's requirements among the tools. The findings indicate the potential for freeware to supplant numerous proprietary applications, as users can opt for freeware instead of incurring costs associated with proprietary software. Furthermore, this perception can be put into practice.

Corresponding Author:

Prabira Kumar Sethy
Department of Electronics and Communication Engineering
Guru Ghasidas Vishwavidyalaya, Bilaspur, C.G., 495009, India
Email: prabirsethy.05@gmail.com

1. INTRODUCTION

Smartphone forensics is an emerging discipline for digital forensics that dates back to the early 2000s. Digital evidence or data from a mobile device are analyzed and stored forensically. In today's data-driven world, digital forensics plays a pivotal role in ensuring the safety and security of our digital assets. While there may be differing opinions among users and developers regarding software safety and usability, the debate between free and commercial software communities continues to persist. In order to shed light on this complex issue, our review takes a closer look at some of the most promising freeware tools available, such as Magnet Forensics and Sleuth Kit, as well as profitable mobile forensics solutions like ProDiscover and Oxygen Forensic Suite. Our approach is based on a range of pre-defined criteria and takes a platform-oriented perspective, in order to provide a comprehensive and insightful overview of these crucial tools and their capabilities. By doing so, we hope to contribute to the ongoing discussion surrounding digital forensics and its importance in our modern, technology-driven world. In a variety of research, these tools have been verified for their capacity to produce and evaluate digital media sources for forensic purposes, with a mere focus on maintaining forensic integrity. Following the removal of data, each media format was tested again after being reformatted. The investigation culminates in a comparative chart that aids in selecting the most suitable tool for the inquiry. This suggests that freeware can serve as a substitute for numerous proprietary applications, affording us the opportunity to utilize it without incurring software costs. Additionally, this notion is pragmatic and can be readily put into practice. Cybercrime activities in mobile telephones have expanded exponentially as they are utilized in many daily tasks, such as personal and business data storage and transfer, and in Internet-based communications [1]–[3]. With an alarming 188% increase in Windows Phone vulnerabilities and a 262% increase in iOS vulnerabilities, mobile devices have become one of the most prevalent weaknesses, increasing more than three times faster than other threats [4], [5]. Forensic investigation of mobile devices is especially difficult owing to the considerable evidence and technological levels. Without the necessary knowledge, serious mistakes can occur during a forensic examination, causing key data to be removed and jeopardizing lawsuit results. Therefore, when a series of software programs were selected for the study, four were chosen: Oxygen Forensic Suite, Discover, Sleuth Kit, and Magnet Forensic Suite [6]–[8].

The document is divided into six sections. The first section provides an overview of the digital developments and the purpose of this study. The following is a summary of the field research: in the third section, we address various forensic malware open-source and commercial tools used in this study [9], [10]. The area above discusses the different parts of a forensic study and the most important things to consider when judging how well an instrument class works. Next, the research infrastructure, which includes many computers and mobile devices, is characterized. The main deliverables of this study are the comparison matrix and the inferences drawn from it [11]–[13]. Numerous cyber forensic publications have demonstrated the importance and efficacy of commercial or open-source digital forensic equipment in solving crimes [14], [15]. Mobile forensics, which covers tools, trends, and law enforcement challenges, highlights the need for improvements and research gaps in the process of mobile law enforcement. An analysis of open source and proprietary digital forensic tools in which a brief introduction of such forensic examination is presented, followed by a similar evaluation of Forensic Toolkit (FTK), Autopsy, Sans Investigative Forensic Toolkit (SIFT), and OS Forensics, is conducted [16]–[21]. Finally, different features of mobile forensics are compared to the cost, MD5 hashing algorithm, general ease of use, and platform support survey. The technique for mobile forensic tools is laid up in a series of phases, including data gathering, sleuthing, processing, and storage [18], [22]. The tools may be recovered from smartphones and produce reports relying on excellent forensic procedures. These reports contain all information about a person's cash transactions and trips.

Software tools possess the capability to analyze a wide range of expertise levels, ranging from basic to extraordinary and sophisticated, in effectively addressing novel challenges. The process of comparing software options for specific tasks facilitates a comprehensive understanding of their respective advantages and limitations. In this discussion, we will examine a pair of open-source tools as well as a duo of commercially available solutions [23], [24]. The Oxygen Forensic Suite represents a pioneering smartphone forensic software that empowers investigators to comprehensively examine essential data within a unified and centralized framework.

ProDiscover Forensic is an all-in-one digital forensic solution that enables analysts to extract crucial evidence from various computing devices. The Passwords tab stores the credentials retrieved from the system's keychain or default secure storage. ProDiscover manages all facets of an in-depth forensic investigation, including collecting, preserving, filtering, and analyzing evidence. A magnet-encrypted disk detector is a wide integrated platform for digital forensics. The only outlets for the PC, smartphone, and cloud in a single scenario gather and process the data. Autopsy (Sleuth Kit) is a digital forensic software platform that also serves as a portal for other technologies. Computer forensics are widely employed by federal, local, state, military forces, and computer investigators in the business world. Autopsy is the best-in-class digital forensic platform. Based on basic forensic technology and customer demands, autopsy is a rapid, comprehensive, and competent digital forensic solution that stays ahead of the curve. The following are some of the important contributions of this review:

- The evaluation of tool performance was conducted utilizing digital media in both Windows and Linux formats. A series of experiments were undertaken to assess the comparative effectiveness of open-source computer forensic capabilities in relation to commercial computer forensic tools, as well as to explore potential synergies between these tools in terms of different standards and characteristics.
- The evaluation of the tools was conducted with a focus on their forensic reliability, specifically their ability to develop and examine mobile forensic applications. Two trials were conducted for each medium type: one after the data had been erased and another after formatting.
- The conducted experiments provided evidence that computer forensic tools, both commercial and open-source, exhibited varying levels of effectiveness in different scenarios, thereby highlighting their potential for mutual validation and supplementation.
- These findings suggest that researchers have the opportunity to conduct digital media investigations and verify their results with minimal expenses, ease of use, and a sense of responsibility.

- By cross-checking investigations using our attributes and norms, experts can look at the data differently and double-check the stated results. They also have perfect and modular control over the processing and display of the data.
- Forensic labs may benefit greatly from employing open-source software in many ways, including cross-platform solutions, ingest/case management, mobile collection and analysis, virtual platforms, and other tools of interest.

2. METHOD

During the various phases of forensic examination, the authors engaged in the formulation of pertinent criteria for the purpose of comparing different tools. This was achieved through the utilization of brainstorming techniques. These metrics would assess the viability of the instrument as an inclusive tool that can be utilized for research purposes across various scales. As an illustration, a conventional forensic tool examines the collected information in order to produce conclusive evidence during the analysis phase.

- First stage: data sources and integration of existing data

The initial stage entails the physical and logical acquisition of data that is stored in diverse formats across a range of mobile devices. In this particular scenario, it may be imperative to bypass the phone's security measures in order to access and retrieve encrypted data. It is imperative to ascertain the level of compatibility between frequently utilized devices. Subsequently, the computer consolidates all the fragmented data into a comprehensive report, which can serve as evidentiary support.

- Second stage: information execution

During this phase, a series of ingestion modules were executed in order to analyze the data that was obtained. The efficacy of a tool is contingent upon two prominent factors: speed and accuracy. Nevertheless, unforeseen events such as power failures or system crashes have the potential to disrupt the standard operating procedure. Furthermore, it is worth noting that damage may occasionally be inflicted upon the devices under investigation with the intention of impeding the utilization of information.

- Third stage: integrity authentication

This form of testing has the potential to ascertain the presence of illegal activities, thereby serving as a tool for identifying instances of corruption. Criminal investigation involves the systematic collection and analysis of data derived from real-world cases, with a focus on identifying recurring errors or patterns. Initially, the process involves the generation of fingerprints, which are subsequently compared to authenticate the acquired data. Consistency in the total amount of data is expected when the software is applied to an identical number of items and across various devices. The comprehensive system assesses the findings in order to ascertain their replicability and establish their validity as evidence.

- Fourth stage: exhibition

Each reporting tool has several modules for generating reports. In addition, these devices can be linked to external applications to enhance reporting. The level at which such partnerships can be formed differs. Ultimately, one of the most important aspects to consider is how reliant the supplier’s reliability and effectiveness in these phases is tracked using the right criteria. The settings were selected to be simple and sophisticated. There was no bias in the selection procedure.

The research parameter and assessment criteria for each metric are mentioned herewith: a single tool data integration using Multiple Smart Devices/Sources, examining the tool's source coverage; data formats may be held together using Data Support, allowing the organization to derive coherent and standardized results from several sources with varying degrees of validity and integrity. For example, outpacing cryptography and account logins can overcome user-enabled credentials and their level locks, analyze the detectability of concealed files, and detect and extract data using file-level encryption and obfuscation techniques.

Data manipulation detection could be an application that detects the manipulation of digital photos, audio, and video files (resized, transformed, and observed). Controlling how users sign in more securely means that the integrity of the data can be verified in all the goods after the files have been moved, which demonstrates the multiple file levels of file integrity. If there are any difficulties, it looks for differences in the file extensions.

Data extraction confidentiality with extraction methods would help in deciding whether the user's identity may be exposed by applying logic as well as usefulness. In this case, a recovery feature may be included to ensure that no form of the device or files is lost. When crashes occur, it is important to consider the error tolerance of forensic tools, the amount of data gathered before and after the collision during extraction or analysis, and the backup efficiency calculation if applicable. The evaluation of forensic tool alliance characteristics pertains to assessing the internal collaborative capacity of forensic instruments. This evaluation is based on factors such as the quantity and functionality of plug-ins, as well as the instrument's ability to collaborate with external applications.

Therefore, it is necessary to assess the frequency and efficacy of vendor updates. The assessment of vendor dependability in relation to the security and multi-user functionality of data storage systems is contingent upon the acquisition of an in-depth capacity to detect these aspects. One of the key factors in this assessment is the number of reliable users. The acceptance of evidence, whether admissible or acceptable, is contingent upon its verification through a court of law. The stages of digital forensic investigation can be correlated with the plotting attributes enumerated in Table 1.

Table 1. Plotting attributes

Sources	Attributes
Integration of source information	- Data integration with a single tool from several mobile devices/sources. - Capability to bypass user authentication. - Extracted data privacy and extraction methods.
Data interpretation	- Data extraction speed and data accuracy. - Forensic instrument fault tolerance.
Error detection and correction, authentication	- Detection of data handling. - Management of data integration.
Exhibition	- Forensic instrument integration functionality.
Additional factors	- Seller details (updates, security data storage, integrity, evidence admissible).

During the implementation phase, the efficacy of the chosen forensic instruments was assessed by testing their compatibility with various computers and mobile devices, as part of the evaluation of the training dataset. In future scenarios involving identical systems, it may not be necessary to rely on the same calculation gadgets or smartphones. The utilization of personal computers is essential in the context of Sleuth Kits, as they are necessary for the analysis of data, examination of findings, and preparation of reports. Both Oxygen and Prodiscover are commercially available forensic tools. Simultaneously, the utilization of Magnet Forensics and Sleuth Kit, both of which rely on system investigation and detection, as well as being freeware, facilitated the processing and uncovering of relevant information. The Sleuth Kit is exclusively compatible with Linux operating systems. Consequently, if your Linux machine restricts the use of the command line interface (CLI), it becomes necessary to utilize the Sleuth graphical user interface (GUI) version.

The oxygen forensic and discovery products, which could be utilized with Windows 10 workstations, were installed on the workstations. The list of modern smartphone PDAs used in this research is Apple 11 Pro Max/11 Pro. iPhone XR, iPhone 12 Pro Max, Galaxy A12, Galaxy A72, Samsung Galaxy A31, BlackBerry Evolve X, and BlackBerry Key2. In order to ensure the authenticity and applicability of the research findings, the mobile devices utilized in this study underwent extensive usage by real-world users prior to their inclusion in the research. The experiments were carried out on multiple operating systems, as well as different versions of those operating systems. As a result, only more recent models of phones were chosen. This is a purposeful attempt to compare previous versions of the analytic tools. Wire-based connecting mechanisms and an SCSI-based micro-type USB cable were necessary for Android, BlackBerry, and Windows Phones, but the iOS phones required a sync-type 8-pin in the USB cable. Radiocommunication: The mobile device may be linked through Wi-Fi or near-frequency communication for products such as oxygen or forensics.

3. RESULTS AND DISCUSSION

The authors of this study have presented the difference measure in Table 2, following a thorough examination of freeware versus commercially viable tools. The table presented illustrates the diverse landscapes associated with each device, as categorized by their respective roles. The essential components of freeware tools include a multiuser setting, a CLI or GUI, the ability to log activities, and enhanced failure tolerance. The popularity of this product can be attributed to its convenient purchasing options and the strong support it receives from the community.

Nevertheless, it is worth noting that superior tools exhibit superior performance compared to their freeware counterparts in terms of accuracy and efficiency in the domains of data mining and analysis. These domains are crucial for conducting forensic investigations, making them the paramount attributes of such work. Effective tools can also assist in file slicing, data recovery, breaking user-level encryption through physical removal, conducting efficient dead-and-live analysis, and revealing identity information. Upon careful consideration of potential adjustments, a notable inclination towards the adoption of freeware technologies becomes apparent.

Table 2. Comparison matrix

Norms	Freeware application		Profitable application	
	Magnet forensics	Sleuth kit (Autopsy)	ProDiscover	Oxygen forensic suite
Correctness	Less accurate	More accurate	Less accurate	More accurate
Support for graphics and videos	Existing	Existing	Existing	Existing
Availability of community assistance	Massive	Massive	Limited	Limited
Are the findings stable in several imaging?	Regularly	Constantly	Regularly	Constantly
Accessibility and readiness	Certainly	Certainly	Certainly	Certainly
Software	Accessible	Accessible	Accessible	Accessible
Cloud forensics	Partial Support	No	Yes	Yes
Geolocation capability	No	Yes	No	Yes
Recovery rate in %	65	78	68	82
Password breeching ability	File, user level	Application, user and file level	Application, user and file level	Application, user and file level
Owner tracing back capability	It can	No	It can	It can
Unallocated data carving support	Yes	No	No	Yes
Multilingual capabilities for full-text search	Contemporary	Contemporary	Contemporary	Contemporary
Extensive automation and scripting	Not so thorough	Very thorough	Comprehensive	Comprehensive
Price	No	No	Costlier	Very Costlier
Integrated AI/ML tools for image and video analytics	Not integrated	Not integrated	Integrated	Integrated
Add on plug-in support	Not support	Partial support	Yes support	Yes support
Dead case efficacy	79%	81%	97%	100%
Explicit smartphone Compatibility	No	Yes	Yes	Yes
Failure resistance	Fewer	More	Fewer	Very Less
Hybrid filtering ability	Better	Best	Excellent	Excellent
Social media artifacts	Plug-in to installed	NA	Integrated	Integrated
Hashing mechanisms	MD-4, 5, SHA-1, 256	MD5, SHA – 1/256/512, MD-2, CRC32	MD 4,5, SHA – 1/256/384/512, MD-2, CRC32	MD 4,5, SHA – 1/256/384/512, MD-2, CRC32, RIPEMD 160
Core competencies	Satisfactory	Sufficient	Outstanding	Outstanding
Automatic report generation	Manual	Manual	Automatic	Automatic
Is it official?	Yes	Yes	Yes	Yes
Can transcripts be customized?	No	Yes	No	No
Is the evidence acceptable in the judiciary?	Absolutely	Absolutely	Absolutely	Absolutely
License required	No	No	Yes	Yes
Multiuser support	Exist	Exist	No	No
CDR analysis	Not possible	Not possible	Not possible	Possible
Weekly downloads	3890	5291	788	1267
Update patches	Presented	Seldom	Presented	Presented
Acquisition ability status	Encountered and acquired	Encountered only	Encountered and acquired	Encountered and acquired
CLI console support	Yes	Yes	No	No
GNOME support	Yes	Yes	No	Yes
Protection capability	Stable and highly matured	Stable and highly matured	Stable and highly matured	Stable and highly matured
Cataloging ability	No	No	Exist	Exist
Scanning speed	Moderate	High	Higher	Highest
Graph and timeline analysis	Yes	Yes	Yes	Yes
Location visualization	Exist	No	No	Exist
SQLite viewer	Exist	No	No	Exist
Merchant support	Upright	Upright	Better	Best
Web activity detection	Exist	Exist	Exist	Exist

4. CONCLUSION

The utilization of a universal approach in selecting forensic instruments is not feasible. Previous studies have indicated that open-source tools can be utilized to verify the outcomes produced by proprietary tools. Furthermore, it has been observed that open-source tools have the capability to surpass the performance of proprietary tools. It is imperative to give careful consideration to the identification of certain subjective factors, including the availability of resources, the skills possessed by researchers, the probable need for instrument interoperability, and the application of these factors. A variety of additional freely available and commercially viable tools have become readily available in the market, catering to a broader set of criteria. These tools have been developed by various authors with the aim of expanding and applying the findings of this research in a more comprehensive manner. In this study, the verification of subsequent answers can be conducted to examine the concurrent evolution and development of mobile telephone technology, as new forensic instruments are introduced and existing versions are updated. Through the process of cross-referencing inquiries utilizing established attributes and norms, professionals possess the ability to approach the data from alternative perspectives and verify the accuracy of the reported outcomes. Additionally, they possess precise and adaptable management of the processing and presentation of the data. The utilization of open-source software in forensic laboratories can yield significant advantages across various aspects, such as the adoption of cross-platform solutions, the implementation of ingest/case management systems, the utilization of mobile collection and analysis tools, the integration of virtual platforms, and the exploration of other relevant tools. The proliferation of cybercrime has led to the emergence of highly advanced and sophisticated bots in contemporary society. The implementation of specific metrics that directly target emerging risks can contribute to the assessment of the effectiveness of freely available digital forensic tools. The significance of investigating the efficacy of the tool in identifying and retrieving these artifacts has grown in importance due to the escalating ubiquity of mobile devices and the wide range of models and operating systems available.

ACKNOWLEDGEMENTS

We are very thankful to the editor and reviewers for their positive suggestions for the improvement of the article.

REFERENCES

[1] G. Horsman, "That tool is rubbish!…or is it?," *Science & Justice*, vol. 62, no. 5, pp. 515–519, Sep. 2022, doi: 10.1016/j.scijus.2022.07.006.

[2] A. Zhang, B. Bradford, R. M. Morgan, and S. Nakhaeizadeh, "Investigating the uses of mobile phone evidence in China criminal proceedings," *Science & Justice*, vol. 62, no. 3, pp. 385–398, May 2022, doi: 10.1016/j.scijus.2022.03.011.

[3] N. H. Nik Zulkipli and G. B. Wills, "An exploratory study on readiness framework in iot forensics," *Procedia Computer Science*, vol. 179, pp. 966–973, 2021, doi: 10.1016/j.procs.2021.01.086.

[4] R. Shree, A. Kant Shukla, R. Prakash Pandey, V. Shukla, and D. Bajpai, "Memory forensic: acquisition and analysis mechanism for operating systems," *Materials Today: Proceedings*, vol. 51, pp. 254–260, 2022, doi: 10.1016/j.matpr.2021.05.270.

[5] M. Alrammal, M. Naveed, S. Sallam, and G. Tsaramirsis, "Malware analysis: Reverse engineering tools using santuko linux," *Materials Today: Proceedings*, vol. 60, pp. 1367–1378, 2022, doi: 10.1016/j.matpr.2021.10.243.

[6] A. H. Saragih, Q. Reyhani, M. S. Setyowati, and A. Hendrawan, "The potential of an artificial intelligence (AI) application for the tax administration system's modernization: the case of Indonesia," *Artificial Intelligence and Law*, vol. 31, no. 3, pp. 491–514, Sep. 2023, doi: 10.1007/s10506-022-09321-y.

[7] K. A. Alissa *et al.*, "Appling tracking game system to measure user behavior toward cybersecurity policies," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 5, Oct. 2022, doi: 10.11591/ijece.v12i5.pp5164-5175.

[8] M. Al-Shabi and A. Al-Qarafi, "Improving blockchain security for the internet of things: challenges and solutions," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 5, pp. 1–11, Oct. 2022, doi: 10.11591/ijece.v12i5.pp5619-5629.

[9] X. Huang, P. Craig, H. Lin, and Z. Yan, "SecIoT: a security framework for the Internet of Things," *Security and Communication Networks*, vol. 9, no. 16, pp. 3083–3094, 2016, doi: 10.1002/sec.1259.

[10] M. A. Naagas and A. P. Gamilla, "Denial of service attack: an analysis to IPv6 extension headers security nightmares," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 3, pp. 1–9, Jun. 2022, doi: 10.11591/ijece.v12i3.pp2922-2930.

[11] T. Rocha, E. Souto, and K. El-Khatib, "Functionality-based mobile application recommendation system with security and privacy awareness," *Computers & Security*, vol. 97, pp. 1–18, Oct. 2020, doi: 10.1016/j.cose.2020.101972.

[12] M. Mukhtar *et al.*, "Hybrid model in machine learning–robust regression applied for sustainability agriculture and food security," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, pp. 1–19, Aug. 2022, doi: 10.11591/ijece.v12i4.pp4457-4468.

[13] J. Schneider, M. Eichhorn, and F. Freiling, "Ambiguous file system partitions," *Forensic Science International: Digital Investigation*, vol. 42, pp. 1–10, Jul. 2022, doi: 10.1016/j.fsidi.2022.301399.

[14] A. Akinbi, Á. MacDermott, and A. M. Ismael, "A systematic literature review of blockchain-based internet of things (IoT) forensic investigation process models," *Forensic Science International: Digital Investigation*, vol. 42–43, pp. 1–11, Oct. 2022, doi: 10.1016/j.fsidi.2022.301470.

[15] S. Park and S. Lee, "DiagAnalyzer: User behavior analysis and visualization using Windows Diagnostics logs," *Forensic Science International: Digital Investigation*, vol. 43, pp. 1–7, Sep. 2022, doi: 10.1016/j.fsidi.2022.301450.

[16] G. Thornton and P. Bagheri Zadeh, "An investigation into unmanned aerial system (UAS) forensics: Data extraction and analysis," *Forensic Science International: Digital Investigation*, vol. 41, pp. 1–22, Jun. 2022, doi: 10.1016/j.fsidi.2022.301379.

[17] A. Vasilaras, D. Dosis, M. Kotsis, and P. Rizomiliotis, "Retrieving deleted records from Telegram," *Forensic Science International: Digital Investigation*, vol. 43, pp. 1–15, Sep. 2022, doi: 10.1016/j.fsidi.2022.301447.

[18] P. Gonçalves, K. Dološ, M. Stebner, A. Attenberger, and H. Baier, "Revisiting the dataset gap problem – On availability, assessment and perspective of mobile forensic corpora," *Forensic Science International: Digital Investigation*, vol. 43, pp. 1–9, Sep. 2022, doi: 10.1016/j.fsidi.2022.301439.

[19] J. Yang, J. Kim, J. Bang, S. Lee, and J. Park, "CATCH: cloud data acquisition through comprehensive and hybrid approaches," *Forensic Science International: Digital Investigation*, vol. 43, pp. 1–10, Sep. 2022, doi: 10.1016/j.fsidi.2022.301442.

[20] J. R. Del Mar-Raave, H. Bahşi, L. Mršić, and K. Hausknecht, "A machine learning-based forensic tool for image classification - a design science approach," *Forensic Science International: Digital Investigation*, vol. 38, pp. 1–13, Sep. 2021, doi: 10.1016/j.fsidi.2021.301265.

[21] H. Johnson, K. Volk, R. Serafin, C. Grajeda, and I. Baggili, "Alt-tech social forensics: forensic analysis of alternative social networking applications," *Forensic Science International: Digital Investigation*, vol. 42, pp. 1–13, Jul. 2022, doi: 10.1016/j.fsidi.2022.301406.

[22] R. Sharma, Diksha, A. R. Bhute, and B. K. Bastia, "Application of artificial intelligence and machine learning technology for the prediction of postmortem interval: a systematic review of preclinical and clinical studies," *Forensic Science International*, vol. 340, Nov. 2022, doi: 10.1016/j.forsciint.2022.111473.

[23] I. Kara and M. Aydos, "The rise of ransomware: Forensic analysis for windows based ransomware attacks," *Expert Systems with Applications*, vol. 190, Mar. 2022, doi: 10.1016/j.eswa.2021.116198.

[24] Z. Shah, A. Kyaw, H. P. Truong, I. Ullah, and A. Levula, "Forensic investigation of remnant data on USB storage devices sold in New Zealand," *Applied Sciences*, vol. 12, no. 12, pp. 1–29, Jun. 2022, doi: 10.3390/app12125928.

BIOGRAPHIES OF AUTHORS

Gyana Ranjana Panigrahi (Member of Microsoft, EC-Council, and IEEE) is a Ph.D. scholar currently pursuing a Ph.D. from Sambalpur University in the department of Electronics, Sambalpur, Odisha, India. My research area includes cyber security, digital forensics, physical cyber systems, communication, wireless communication, data communication and networking, iot, and storage area networks (SAN). He can be contacted at email: gyana.ranjana.panigrahi@suiit.ac.in.

Dr. Nalini Kanta Barpanda received his Ph.D. in Engineering from the Sambalpur University. He is working as Reader in Electronics, at Sambalpur University, Odisha. He has published over 62 research articles in various areas of performance analysis of communication interconnection N/W, wireless sensor N/W, image processing, and the internet of things. He can be contacted at email: nkbarpanda@suniv.ac.in.

Dr. Prabira Kumar Sethy (Senior Member IEEE) currently working as an Associate Professor in the Department of Electronics and Communication Engineering at Guru Ghasidas Vishwavidyalaya, Bilaspur. He has ten years of teaching, research & administrative experience and four years of Industry experience. Previously he worked as Engineer in Doordarshan, Prashar Bharati, from 2009 to 2013. He has received his Ph.D. and M. Tech degrees from Sambalpur University and IIT (ISM) Dhanbad, respectively. His research area is image processing, machine learning, and deep learning. He has published 80 research papers in different reputed journals and conferences. In addition, he has two patents. He is an editorial board member of the International Journal of Electrical and Computer Engineering. He is also Editorial Board Member in Ingénierie des Systèmes d'Information. IIETA. He received the "InSc Young Achiever Award" for the research paper "Detection of coronavirus (COVID-19) based on Deep Features and Support Vector Machine, organized by the Institute of Scholars, Ministry of MSME, Government of India in the year 2020. He is a Senior Member of IEEE. He is a frequent reviewer of many journals and session chair of international conferences. He can be contacted at email: prabirsethy.05@gmail.com.