



A Comprehensive Survey on Computer Forensics State-of-the-art, Tools, Techniques, Challenges, and Future Directions

Javed, Abdul Rehman; Ahmed, Waqas; Alazab, Mamoun; Jalil, Zunera; Kifayat, Kashif; Gadekallu, Thippa Reddy

Published in:
IEEE Access

DOI:
[10.1109/ACCESS.2022.3142508](https://doi.org/10.1109/ACCESS.2022.3142508)

Published: 01/01/2022

Document Version
Publisher's PDF, also known as Version of record

[Link to publication](#)

Citation for published version (APA):

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A Comprehensive Survey on Computer Forensics: State-of-the-art, Tools, Techniques, Challenges, and Future Directions. *IEEE Access*, 10, 11065-11089. <https://doi.org/10.1109/ACCESS.2022.3142508>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Received December 19, 2021, accepted January 8, 2022, date of publication January 12, 2022, date of current version January 31, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3142508

A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions

ABDUL REHMAN JAVED¹, (Member, IEEE), WAQAS AHMED¹,
MAMOUN ALAZAB², (Senior Member, IEEE), ZUNERA JALIL¹, (Member, IEEE),
KASHIF KIFAYAT¹, AND THIPPA REDDY GADEKALLU³, (Senior Member, IEEE)

¹Department of Cyber Security, Air University, Islamabad 44000, Pakistan

²College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT 0810, Australia

³School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India

Corresponding authors: Abdul Rehman Javed (abdulrehman.cs@au.edu.pk) and Mamoun Alazab (alazab.m@ieee.org)

This work was supported by the Higher Education Commission of Pakistan under the National Center for Cyber Security Project Grant.

ABSTRACT With the alarmingly increasing rate of cybercrimes worldwide, there is a dire need to combat cybercrimes timely and effectively. Cyberattacks on computing machines leave certain artifacts on target device storage that can reveal the identity and behavior of cyber-criminals if processed and analyzed intelligently. Forensic agencies and law enforcement departments use several digital forensic toolkits, both commercial and open-source, to examine digital evidence. The proposed research survey focuses on identifying the current state-of-the-art digital forensics concepts in existing research, sheds light on research gaps, presents a detailed introduction of different computer forensic domains and forensic toolkits used for computer forensics in the current era. The proposed survey also presents a comparative analysis based on the tool's characteristics to facilitate investigators in tool selection during the forensics process. Finally, the proposed survey identifies and derives current challenges and future research directions in computer forensics.

INDEX TERMS Survey, state-of-the-art, digital forensics, cybercrime, computer forensics, investigation, tools, cybersecurity.

I. INTRODUCTION

In this age, where everything is being digitalized, criminals are using modern technologies to attack governments, businesses, and individuals [1]–[4]. The most recent example is a cyberattack in a US state Baltimore, where attackers stole a National Security tool and caused thousands of systems to freeze. The attack lasted three weeks, disrupting emails, real estate sales, water bills, health alerts, and several other services. The annual cost of suffering is increasing rapidly; in fact, the experts have projected it to rise to \$6 trillion by 2021¹ [5]–[7]. Computer forensics techniques are used in civil, administrative, and criminal cases; however, an intelligent selection of tools is vital in

criminal investigations. Computer forensics has a close link with human behavior. Forensics can provide psychological conditions and traits of human behavior. Behavioural Evidence Analysis (BEA) within computer forensics helps to understand the psychology and behavior according to a particular case [8]. The investigators use several tools to perform forensic procedures to obtain inevitable evidence against criminals to hold them responsible in the court of law. This paper discusses computer forensic domains, available open-source and proprietary analysis tools and presents their feature-based comparison.

Computer forensic information can be extracted from applications such as software, databases, the web, and emails [9]. Since the computer is allowed to communicate and share the required information, investigations revealing network information might help [10]. Also, emerging technologies like virtualized systems, distributed computing, and cloud computing have posed challenges in the field

The associate editor coordinating the review of this manuscript and approving it for publication was Liang-Bi Chen¹.

¹<https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>

TABLE 1. Comparison of state-of-the-art papers.

Ref.	Focus	Limitation
[15]	Overview of digital forensics	Limited overview
[16]	Overview of abstraction layer for errors in toolkits	Focused on error in toolkits
[17]	Overview of digital forensics toolkits	Limited features and toolkits
[18]	Overview of digital forensics toolkits	Brief overview of features and toolkits
[19]	Comparative study between forensics application tools	Limited features, limited toolkits, no challenges and future direction
[20]	Overall forensics investigation	Limited description of digital forensics toolkits

of forensics [11], [12]. In this era of technology, the evidence is extracted from various hardware devices such as memory cards, smart cards, dongles, cameras, biometric scanners, routers, pagers, printers, answering machines, GPS systems. We present an analysis of critical characteristics for forensic examination of acquired evidence. Forensic readiness planning, evidence acquisition methods, protocols, protection of evidence integrity, and legal aspects of forensic investigations are beyond this study's scope.

From a technical perspective, the decision of choosing digital forensic tools for evidence examination is made by the investigator according to the unique nature and requirements of the case [13], [14]. However, a forensic tool would be a good choice if it has the versatility to work across multiple platforms, multiple operating systems, the ability to analyze more than one file system, the extendability of applying scripting languages to automate repetitive functions and tasks, automation of significant features and has good product support. In general, a forensic toolkit providing more features in one product/suite and multi-platform support would be more helpful. Careful and in-depth study of each tool's features can help investigators pick the most appropriate tool for investigation, thus saving investigation time and effort. Investigators can focus on other investigations such as case preparation, evidence collection, maintaining chain of custody, and report generation. This paper performed an in-depth study of tools and their features.

The surveys reported in the past are limited to facilitate forensic investigators to pick a suitable forensic tool. Some previous research works such as [15]–[19] focused more on providing an overview of digital forensics methodologies, finding errors in toolkits, and research directions but did not provide any guideline to investigators for intelligent selection of appropriate toolkit for evidence analysis. Table 1 presents the comparison of the existing research papers.

A. RESEARCH CONTRIBUTION

Several researchers presented surveys on computer forensics [20]–[23], cloud forensics [24]–[27], and mobile forensics [28]–[31], but this is the first survey that provides current state-of-the-art on computer forensics, techniques, and their

**FIGURE 1. Process flow of digital forensic model [65].**

comparison. The main contributions of this paper are as follows:

- The proposed research survey identifies the current state-of-the-art digital forensics concepts in existing research and sheds light on research gaps.
- Presents a detailed introduction of different computer forensic domains and forensic toolkits used for computer forensics in the current era.
- Provides a comparative analysis based on the tool's characteristics to facilitate forensics investigators during the digital forensics process.
- The proposed research survey also identifies challenges and provides insights and future research directions in computer forensics.

B. SURVEY STRUCTURE

The rest of the paper is organized as follows: section I-C provide a background of the proposed research work; section II reviews the computer forensic domains including operating system, file system, live memory, web, email, network, and multimedia forensics; section III includes details about powerful computer forensic toolkits such as autopsy, Redline, Belkasoft, OS, ProDiscover, XWays, Encase, and FTK; section V presents a detailed discussion of toolkits based on features in each domain; section V-A presents future research direction regarding proposed research work and section VI summarizes the survey and presents future research directions.

C. RESEARCH BACKGROUND

The focus of digital forensics is on the objects situated on different types of digital devices such as mobile phones, digital cameras, computer systems, and other digital devices. In recent years, researchers and developers have developed several forensics applications. The new applications expand digital forensics scope to volatile memory. Memory forensic techniques increase daily from a string search to deep search, structural memory analysis, and operating systems analysis. Several researchers worked on different technologies of computer forensics such as: memory forensics [32]–[36], volatile memory [35], [37]–[41], log forensics [42]–[47], operating system [48]–[53]. Table 2 presents the literature review of current research work in the areas of memory forensics, computer forensics, IoT forensics, and log forensics.

II. COMPUTER FORENSIC ANALYSIS

Digital data exists in several formats and types. Therefore, several types of analysis and examples of common digital analysis types are defined by the Digital Forensics Research Workshop (DFRWS) [65]. Authors in [17] have explained the process and the flow of a digital forensic investigation.

TABLE 2. Computer forensics literature review.

References	Forensics Area	Author Contribution
[54]	Log forensics	For efficient log displaying, storing, querying, processing, and loading, the author designed and developed a novel graphical system called GrAALF.
[55]	Computer forensics	The author analyzed data recovery and computer forensics relationships and analyzed computer forensics and anti-forensics application technology.
[56]	Computer Forensics	The author discussed computer forensics methods, including rules for data extraction, evidence management, and change of custody.
[57]	Computer forensics	For the admissibility of evidence and to overcome legal issues related to digital evidence in court author discussed the computer forensics investigation process.
[58]	IoT forensics	To protect user’s privacy and secure data sharing author proposed the digital witness technique. For IoT forensics author also applied the PRoFIT technique.
[59]	IoT forensics	By analyzing the weaknesses and strengths of IoT forensics author investigate current research work. The forensics processes, forensics data processing, forensics layers, forensics models, forensics tools, and phases author classify and categorize the literature.
[60]	Computer forensics	The author presented a detailed survey on the mitigation of privacy issues in the cloud for computer forensics. The author also presented future recommendations regarding privacy issues in cloud computing.
[61]	IoT Forensics	For the author of the smart application study, the readiness, and complexity of devices for the assistance in the investigation. The author also presented forensics methodology and smart applications related tools.
[62]	Computer forensics	The proposed paper provides the researchers and readers valuable information about forensics, the current status of forensics, and anti-forensics techniques.
[63]	Computer forensics	In this paper, the author proposed a novel technique for investigators regarding correlating evidence, analysis process with the help of numerous forensics tools.
[64]	Memory forensics	The author investigates different limitations regarding memory forensics included data change issues, data incompleteness, executable file, process inconsistencies, and data incompleteness.
[32]	Memory forensics	The author presented a survey on computer memory forensics, including future research directions in memory forensics, how technological changes influence memory forensics such as operating systems, and regarding the current generation, the author providing critical analysis of techniques used in forensics.
Proposed survey	Computer and Mobile forensics	In this survey, we perform a comparative analysis of forensics toolkits based on their characteristics, discuss computer and mobile forensics domains and cover diverse forensic toolkits used for computer and mobile forensics investigations. We also discuss forensic challenges and future research directions.

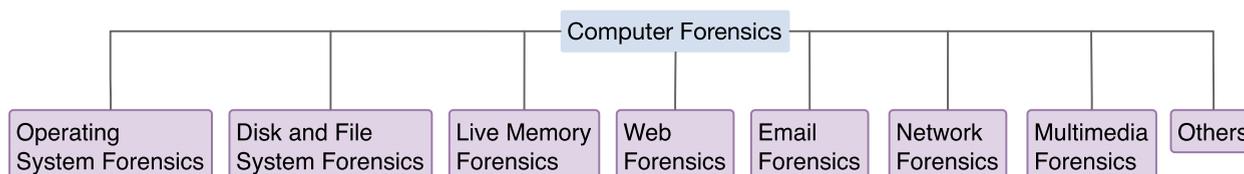


FIGURE 2. Breakdown of computer forensic domains.

The process of investigation starts right after the incident is reported or a crime is detected [66]. After the crime is detected, an investigator starts collecting evidence from the objects identified to be included in the crime. After that, the investigator follows the steps shown in Figure 1. First, The investigation identifies the suspect machine or object used in crime or violations. Next, the investigator examines the objects and generates a report on the findings. Finally, the last step is to report the findings and catch the suspect [67].

Figure 2 represents the breakdown of the computer forensic domains. In later sections, we focus on the details of each computer forensic domain.

A. OPERATING SYSTEM FORENSICS

Operating System Forensics is the process of retrieving useful information from the operating system of the computer or mobile device in question [15]. The aim of collecting this

information is to acquire empirical evidence against the perpetrator. An operating system (OS) is an application that is the first thing to execute when a computer system starts [68]. This helps to examine configuration files and output data of the OS to determine which event might have occurred. Reference [69]–[71] are some of the existing research surveys in the operating system forensics domain.

OS Forensics allows its users to identify suspicious files and activity with hash matching, drive signature comparisons, emails, memory, and binary data² [72]. It lets users extract forensic evidence from computers quickly with advanced file searching and indexing and enables this data to be managed effectively. It supports Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2000, 2003, 2008, 2012 (for 32-bit and 64-bit platforms). OSForensics is available on trial

²<https://www.osforensics.com/osforensics.html>

TABLE 3. OS with supported file system.

OS	File Type
Windows	FAT12, FAT 16, FAT 32, NTFS
Linux	GFS, Ext, Ext 2, JFS, XFS, Swap, Ext3, Ext 4, VFAT, HPFS, FreeBSD
Mac	APFS, HFX, HFS+, FAT32, exFAT
Optical media	UDF
Android	FAT32, Ext3, Ext4
iOS	APFS, HFS+

as well as the paid version. This tool's prominent features are Misnamed file searching, Drive signature comparison, Hidden disk areas.

B. FILE SYSTEM FORENSICS

The file system is highly valued in computing as all files would mess up without it. There will be no clue where data is placed, where a specific piece of data starts, and where it ends. Each file system instance has a unique size, but its underlying structure allows any computer that supports the type of file system to process it [68]. There are different types of file systems. Each one has a different structure, logic, speed, flexibility, security, size, etc. Some file systems are designed to be used for a specific application. For example, the ISO 9660 file system is designed specifically for optical discs [16]. Different storage devices use different media that support different file systems like SSDs. Another excellent example of a file system can be Random Access Memory (RAM) as a temporary file system for short-term use. Some other file system provides file access via a network protocol such as NSF and SMB [73]. The key features of file systems are filenames, directories, metadata, and space management. The analysis of the file system depends on data that exists inside of a partition or disk. This typically involves processing data to extract the contents of a file or recovering the contents of a deleted file. File system analysis examines data in a volume (i.e., a partition or disk). The file system process includes listing the files in a directory, recovering deleted content, and viewing a sector's contents [74]. Reference [75]–[77] are some of the existing research surveys in the file system forensics domain. Table 3 presents the available operating system with supported file types.

C. LIVE MEMORY FORENSICS

Live memory (RAM) is an intermediate memory between processor and storage. It enables accessing and processing information, associated Delay Locked Loops (DLLs), handles, open files, decrypted data, registry, user password and activities, connection & session details [78]. RAM allows accessing data in such a way to produce transparent information, which could not be possible otherwise [79], [80]. This can help to reveal hidden processes, malware trying to hide information, toolkits. Reference [81], [82] are some of the existing research surveys in the live memory forensics domain.

D. WEB FORENSICS

Web activities are performed on a web browser that provides an interface between the user and the Internet [83], [84]. The forensic information can be retrieved from web storage record sessions, searches, a history where complete user activity is placed [85], [86]. Every OS and Browser has its way to keep these records that can be analyzed to trace a crime [87]. Reference [76], [82], [88] are some of the existing research surveys in the web forensics domain.

E. EMAIL FORENSICS

Communication via the Internet uses emails as mainstream for communication. An email, when transmitted, contains the source, content, actual sender and receiver information, date/time, protocols, and server information. Email forensics is a process of collecting evidence from emails since an email is an electronic communication over the Internet that carries messages to deliver files, documents, and other transaction elements [89]–[91]. Email services could either be webmail or a local mailbox [92]. Reference [20], [30], [89] are some of the existing research surveys in the email forensics domain.

F. NETWORK FORENSICS

Network forensic analysis focuses on monitoring network traffic and investigating the attack source. The objective of this analysis is to put plans in place before a security breach occurs [1], [76], [93]. The methods used for this objective are 'Catch it if you can' and 'Stop, look and listen,' which eventually covers the outline that includes identity threat, collecting evidence, examining data, analyzing and concluding data, presenting the analysis, and responding to attacks. Reference [24], [77], [94] are some of the existing research surveys in the network forensics domain. Network packets can be examined using the Open Systems Interconnection (OSI) model to interpret the raw data into an application-level stream. Figure 3 defines the OSI model layers in detail.

G. MULTIMEDIA FORENSICS

Today users enjoy smartphones, high bandwidth connection, rich media, and cheap storage. People share massive multimedia content on social sites in the form of images, audio, and video, etc. Reference [96]. Digital visual media nowadays is one of the principal means of communication. Digital image analysis is the latest digital forensics trend due to its validation of the history of an image by exploring, analyzing, and retrieving information about the image [97]. Moreover, two more essential areas in the image forensic domain are identifying the imaging device that captured the image and detecting traces of forgeries. Digital images are the target of many digital investigations because some are contraband [98], [99]. This type of analysis looks for information about where the picture was taken and who is in the picture. Image analysis also includes examining images for evidence of stenography. Video analysis can automatically

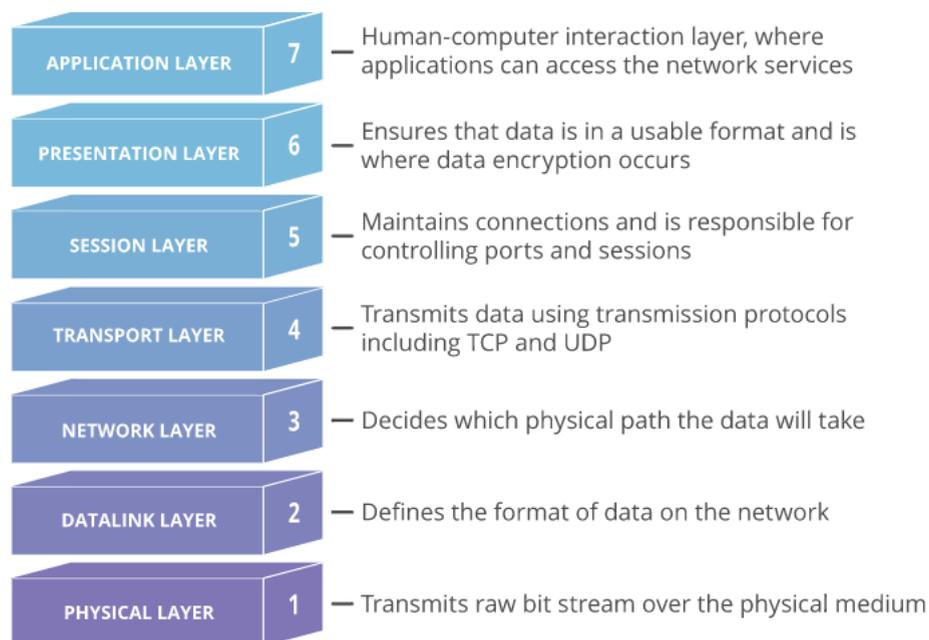


FIGURE 3. OSI model [95].

analyze video to detect and determine temporal and spatial events, while forensic video analysis compares and evaluates video in legal matters [100], [101].

Digital video is used in security cameras, personal video cameras, and webcams. Investigations of online predators can sometimes involve the examination of digital video from webcams [102]. This type of analysis examines the video for the identity of objects and the location where it was shot. Forensic video analysis and audio analysis have been used in various high-profile cases, international disagreements, and conflict zones [103]. Reference [22], [103], [104] are some of the existing research surveys in the multimedia forensics domain.

H. OTHERS

Instant messenger forensics to examine pieces of evidence collected through instant messenger applications, chat, and shared data. Media/USB/Memory card forensics helps analyze removable media investigations—Malware forensics helps identify malware objects and their behavior [46], [105]–[107]. Some other computer forensics domains, such as cloud forensic, are used to examine crimes committed using cloud platforms, and database forensics help investigate data storage and privacy-related crimes [24], [108].

III. STATE-OF-THE-ART COMPUTER FORENSIC TOOLS

With time and in the era of intelligent devices and technologies, the nature of cybercrimes has diversified. Whenever a crime is related to the virtual world, then it is called cyber crime [109], [110], and it falls in the area of digital forensic. Identify theft and espionage [55], [111]–[113], intellectual

property theft, information leakage, harassment, phishing, denial of services (DoS), and cyber defamation are some of the most common attacks nowadays [114].

Generally, digital forensics involves preservation, extraction, identification, analysis of data, and generating a report [17]. Several digital investigation tools are available nowadays to ease the job of a forensic investigator. These tools are limited to their tasks. For example, some tools are appropriate for tasks such as:

- Attribution - metadata and logs used to attribute actions to an individual. For example, personal documents on a computer drive might identify its owner.
- Alibis & statements - provided by those involved can be cross-checked with digital evidence.
- Intent – helps find objective evidence of a crime and can also be used to prove the intent.
- Evaluation of source file artifact and meta-data used to identify the origin of a particular piece of data; for example, older versions of Microsoft Word embedded a Global Unique Identifier into files which identify the computer it was created on, showing if a file was produced on the digital device being examined or obtained from elsewhere (e.g., the Internet).
- Document authentication – associated with “evaluation” metadata associated with digital documents can be easily modified (e.g., by changing the computer’s clock, you can affect the creation date of a file) and helps detect & identify “falsification”/evidence manipulation.
- Malware identification - to identify malware’s dynamic behavior by observing changes in system and network logs.

A. AUTOPSY SLEUTHKIT

The Sleuth Kit provides disk image analysis and file recovery feature.³ It allows an investigator to analyze volume and file system data. It is widely used by law enforcement agencies, military, and corporate examiners. This plug-in framework allows incorporating additional modules to analyze file contents and build automated systems [115]. In addition, the library can be incorporated into more comprehensive digital forensics tools, and the command-line tools can be directly used to find evidence. An autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools⁴ [115]. The Sleuth Kit and Autopsy are free tools and support Windows, Linux, OS X, and other Unix platforms. This kit's prominent features are collaboration, web artifact, registry analysis, email analysis, and android support.

B. REDLINE

Redline is another toolkit that provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis and develops a threat assessment profile [116]. Redline can perform an audit and collect all running processes and drivers from memory, file-system metadata, registry data, event logs, network information, services, tasks, and web history. Supported operating systems are Windows XP, Windows Vista, Windows 7, Windows 8 (32-bit and 64-bit), and Windows 10.⁵

C. BELKASOFT EVIDENCE CENTER

Belkasoft Evidence Center(BEC) is a commercial forensic tool available with the trial version. It makes it easy for an investigator to acquire, search, analyze, store, and share digital evidence found inside the computer, mobile devices, RAM, and cloud. This toolkit can quickly extract digital evidence from multiple sources by analyzing hard drives, drive images, cloud, memory dumps, IOS, Blackberry, Android backups, GrayKey, UFED, OFB, Elcomsoft, TWRP images, JTAG, and chip-off dumps. Evidence Center automatically analyzes the data source and lays out the most forensically important artifacts for the investigator to review, examine more closely, or add to the report [51].

It supports all Windows platforms, macOS, Unix-based systems (such as Linux, FreeBSD).⁶ Some critical features provided by Belkasoft are Data Carving, Live Memory Analysis, Enhanced Live RAM, Analysis, Kernel-mode RAM Capturer, JumpList Analysis.

D. PRODISCOVER BASIC

ProDiscover is designed to be a single application allowing forensics examiners to collect, analyze, manage, and report

on computer disk evidence.⁷ It simplifies computer forensics case management. When required, investigators can collect time zone, web browsing activities, and device information through a report. ProDiscover is a paid toolkit with its basic version available for free. It allows the investigators to perform live analysis. It also uses patent-pending technology and a process called Connect Collect Protect, which helps the user connect to a device, gather data, and analyze the situation during any security issue or data breach. This tool's other prominent features are inspection and search of hardware protected areas, Boolean search, Malware discovery hash sets, Automatic reports.

E. XWAYS FORENSICS

X-Ways Forensics is an advanced working environment for computer forensic examiners. Its proprietary source is available online.⁸ X-Ways Forensics runs much faster, finds deleted files and search hits that the competitors will miss, does not have any hardware requirements, does not depend on setting up a complex database. X-Ways Forensics is an integrated computer forensic software that is based on the WinHex hex, and Disk Imager [117]. It is part of an efficient workflow model where computer forensic examiners share data and collaborate with XWays Investigator investigators. Some key features of Xways are complete access to disks, RAID's, images, Carving, PhotoDNA hashing, Disk Imaging, Password Recovery.

F. ENCASE

Encase is one of the broadly utilized criminological tools in the world. Reportedly, 90% of the investigators utilize this tool. 93% of the banks, 100% of the government offices, 75% of the power wholesalers, and 80% of the Universities in the U.S. use Encase⁹ encase,encase1. The examination life cycle is nearly similar to that as portrayed in [17] beginning with an examination at that point gathering information, investigating it, and producing a report. This toolkit's key features are large-scale reports, Carving, Memory acquisition, Disk Imaging, Password Recovery.

G. FTK

Access Data Group is the creators of FTK.¹⁰ They provide training and certification of forensic tools [18]. More than 130,000 administering bodies, law offices use FTK. It can investigate PCs, networks, and mobiles, and searching is faster than other tools. Some key features of FTK are Network data, Data transfer, detection, Internal viewer, Disk Imaging, Password Recovery.

³<http://www.sleuthkit.org/sleuthkit/>

⁴<http://www.sleuthkit.org/sleuthkit/>

⁵<https://www.fireeye.com/content/dam/fireeye-www/services/freeware/ug-redline.pdf>

⁶<https://belkasoft.com/ec>

⁷<https://www.techpathways.com/pro-discover-forensics>

⁸<http://www.x-ways.net/forensics/>

⁹<https://www.guidancesoftware.com/encase-forensic>

¹⁰<https://accessdata.com/products-services/forensic-toolkit-ftk>

H. MAGNET AXIOM

Magnet Axium provides the functionality to recover digital evidence from the most sources and use robust and intuitive Analytics tools to efficiently analyze data in one case file¹¹ Furthermore, Magnet Axium has the functionality to recover data from Smartphones, Computers, and the Cloud. Magnet Axium also provides the functionality to examine evidence across all the sources in one case file. Finally, it also provides surface and shares insights with powerful analytics and reporting tools.

I. OTHERS

Increasing cybercrimes intelligently has made it necessary to develop innovative computer forensic tools to investigate intelligently. Tools are specifically designed for each computer forensic domain for a particular domain. Some of the well-known tools for data recovery are *Blade*, *Recuva*, *Recover My Files*, *CrowdStrike*, and *CrowdResponse* that are used to deal with cyber incidents such as identifying the attacker and eradicating them; Volatility framework provides the functionality of live memory analysis, ExifTool detects the image file formats, Free Hex Editor Neo is used for binary file editing, Bulk Extractor ignores all the types of the file system so that any file gets supported to run on the bulk extractor. DSI USB Write Blocker does not allow criminals to write into USB, HxD helps edit the hex files, COFFEE extracts evidence from a Windows computer, and EPRB provides encryption-decryption functionality. New tools are being developed, and existing tools are being improved to address forthcoming issues. Table 4 presents the detailed summary of the above-mentioned forensic tools.

IV. COMPARATIVE ANALYSIS

This section provides a high-level taxonomy for the computer forensic toolkit to provide the best toolkit for the investigators. We present a review of significant characteristics of computer forensic toolkits comprising of (a) license, (b) platform, (c) supported image formats, (d) domains, and (e) tool interaction as illustrated in Figure 4.

Forensic toolkits are initially compared based on available features and then domain-specific features. The toolkits discussed in the previous section are generally analyzed and compared concerning the domain.

A. GENERAL ANALYSIS

Firstly, we present the analysis of computer forensic domains based on available features such as licensing status, supported operating system, and image format.

1) LICENSING STATUS

While selecting a toolkit for forensic analysis, an important aspect is to know what kind of license it possesses. Open source forensic tools are available and modified as per the

TABLE 4. Computer forensic tools.

Tool	Summary
Autopsy Sleuthkit	The Sleuth Kit provides disk image analysis and file recovery features. The Sleuth Kit and Autopsy are free tools and support Windows, Linux, OS X, and other Unix platforms.
Redline	Help users find malicious activities through memory and file analysis and find the running processes and drivers from memory.
Belkasoft Evidence Center	This toolkit can quickly extract digital evidence from multiple sources by analyzing hard drives, drive images, cloud, memory dumps, IOS, Blackberry, Android backups, GrayKey, UFED, OFB, Elcomsoft, TWRP images, JTAG, and chip-off dumps
OS Forensics	Help users identify suspicious activities and files with hash matching techniques. It supports Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2000, 2003, 2008, 2012 (for 32-bit and 64-bit platforms).
ProDiscover Basic	using this tool, investigators can collect time zone, web browsing activities, and device information through a report when required. ProDiscover is a paid toolkit with its basic version available for free.
XWays Forensics	Much faster, finds deleted files and search hits that the competitors will miss, does not have any hardware requirements, does not depend on setting up a complex database.
Encase	This toolkit's key features are large-scale reports, Carving, Memory acquisition, Disk Imaging, Password Recovery.
FTK	It can perform an investigation on PCs, networks, and mobiles. Some key features of FTK are Network data, Data transfer, detection, Internal viewer, Disk Imaging, Password Recovery.
Magnet Axium	This toolkit's key features are data recovery, examination of evidence across all sources and reporting.

investigation requirement. Freeware tools are available, but the proprietor only defines a set of features. Commercial tools have monthly, yearly, or contracted periods of subscriptions. Some commercial tools provide trial versions with limited functionality for a short duration.

2) SUPPORTED OPERATING SYSTEM

A toolkit that supports multiple operating systems (with multiple file systems) can help investigators. Some tools are operating system-specific and cannot be used on other platforms.

3) SUPPORTED IMAGE FILE FORMAT

According to the investigator's acquisition tool or preferences, the acquired image can be in different file formats for the forensic investigation. However, the investigator must know which image formats are analyzable with the selected toolkit for the analysis phase. Although an investigator's perspective requires choosing the toolkit according to evi-

¹¹<https://www.magnetforensics.com/products/magnet-axiom/>

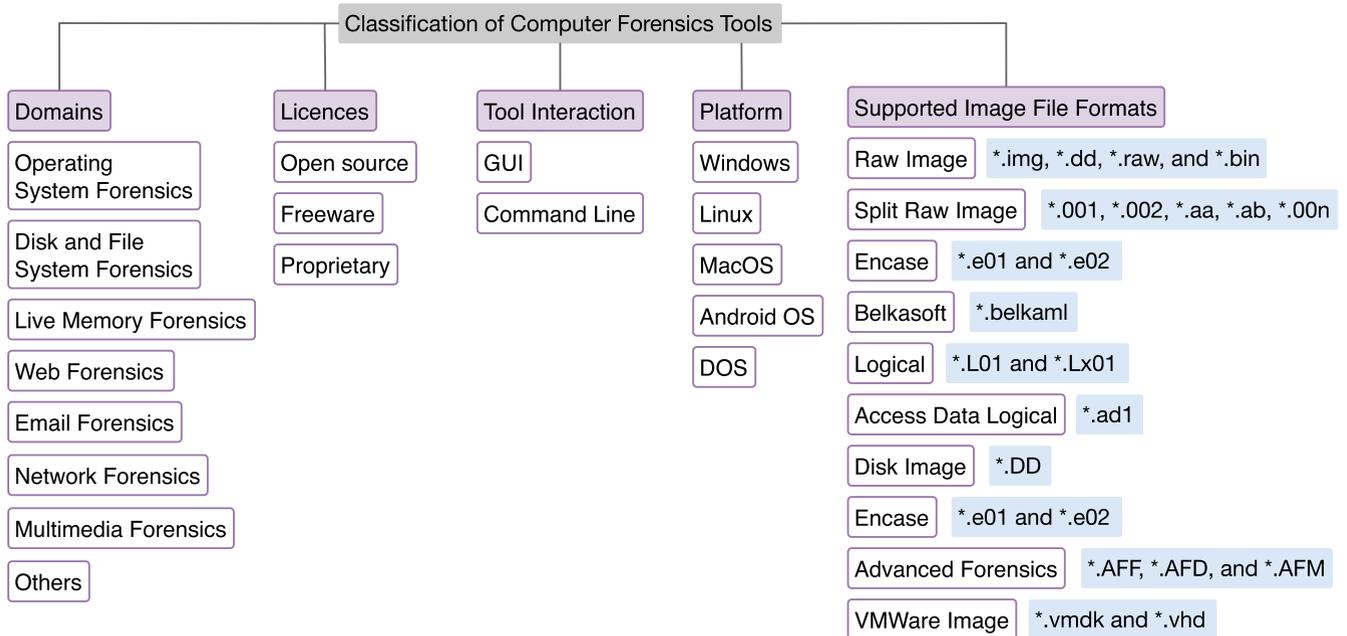


FIGURE 4. Taxonomy of computer forensic investigation tools.

TABLE 5. Comparison of general features of computer forensic tools.

	Autopsy	Redline	BEC	OSF	PD	XWays	Encase	FTK	MA
									
License	Open	Freeware	Proprietary	Proprietary	Open	Proprietary	Proprietary	Open	Proprietary
Platform	Window, Linux, OS X	Window (XP- 2008)	Window (all), Android Mac OS, Linux	Window Vista, 7, 8, 10 Server (2000, 2003, 2008, 2012)	Window 2000/ 2003/ 2008/XP/ Vista/ Window7, Linux.	Window (all) DOS	Window, MAC, Linux, DOS, Machine	Windows, XP/Vista /7/8/10	Computer, Mobile, Cloud
Supported Image File Formats	Raw Single, Raw Split EnCase	Raw, .mans file	Atola, Raw , DMG, EnCase, FTK, AFF X-Ways CTR, SMART	Raw, Split, A. F. S, Virtual, EnCase, SMART (.S01), VHD (.VHD)	Raw, EnCase, A. F. S	Raw Encase V. I	Raw, VMware, Encase, Safeback.	Raw, SMART, EnCase, Snapback, Safe back	Raw

BEC-Belkasoft Evidence Center; OSF-OSForensics; PD-ProDiscover Basic, MA-Magnet Axiom.

dence format, a multi-faceted toolkit that supports multiple formats would be more worthy. Therefore, the following image formats are used:

- Raw Single Image: supports multiple extensions such as *.img, *.dd, *.raw and *.bin.
- Raw Split Image: supports multiple extensions such as *.001 and *.002, *.aa, *.ab.
- Encase Image: supports multiple extensions such as *.e01 and *.e02.
- Virtual Image (VI): supports multiple extensions such as *.vmdk and *.vhd.
- Advanced Forensics Format (AFS): supports .AFF, .AFD, .AFM, VMWare.

- Belkasoft image file: supports extension such (*.belkaml)
- Logical Image: supports .L01, .Lx01.
- AccessData logical image (ALI): supports (*.ad1).
- Disk iMaGe: DD.

Table 5 shows a general comparison of toolkits discussed in Section 5 based on their licensing statement, supported OS, and supported image file system.

Autopsy, ProDiscover Basic, and FTK are toolkits with an open license and support raw and encase image formats. These toolkits also support almost all versions of the Windows Operating system, and ProDiscover Basic supports Linux OS. Belkasoft Evidence Center (BEC) and

TABLE 6. Comparison of operating system related features in forensic tools.

Features \ Tools	Autopsy	Redline	BEC	OSF	PD	XWays	Encase	FTK
								
LNK files	✓	✗	✓	✓	✓	✓	✓	✓
Prefetch Files	✓	✓	✓	✓	✓	✓	✗	✓
Services Analysis	✗	✓	✗	✗	✗	✗	✗	✓
Event Log	✓	✓	✓	✓	✓	✓	✓	✓
Registry	✓	✓	✓	✓	✓	✓	✓	✓
Installed program	✓	✗	✓	✓	✗	✗	✗	✓
User Activity	✓	✓	✓	✓	✗	✓	✓	✓
Passwords	✗	✗	✓	✓	✓	✗	✓	✓
Recycle Bin	✗	✗	✓	✓	✗	✓	✓	✓

BEC, Belkasoft Evidence Center; OSF-OSForensics; PD-ProDiscover Basic.

OSForensics support diverse image formats and can be used where multiple evidence images of different storage devices are available in diverse formats. BEC can perform quick extraction from sources such as hard drives, memory dumps, UFED, JTAG, and chip-off dumps.

B. DOMAIN WISE ANALYSIS

Forensic investigations are performed to investigate for different purposes. The nature of the investigation required is determined based on the nature of the committed crime. For one case, evidence found in Instant Messenger (IM) application may be of more value, and for another, audio files may be more worthy of observing. This section presents a detailed analysis of the computer forensic domains in which an investigator can be interested. We identified significant features provided by forensic tools in each domain and compared tools with others. We have picked domain-specific tools and analyzed their features for comparison. For example, we have observed Network Miner, Volatility, and other tools.

1) OPERATING SYSTEM FORENSICS

The operating systems produce many valuable operating system artifacts that can be further used as pieces of digital evidence [118]. In the case of Windows OS, the most common sources of such artifacts are the Recycle Bin, Windows event logs, LNK files, and prefetch files are shown in Table 6.

- **LNK files:** The link file is windows shortcut files that contain metadata. It usually provides timelines, target size, serial number, network volume share name, file attributes.
- **Prefetch files:** These files are designed to speed up the application startup process. They contain valuable information about applications used, including their run count, last run date, time, executable name, and size.
- **Event Log:** It is a logging system that maintains application systems, security logs, and server-based logs. These logs are stored in pre-defined formats to record all necessary information regarding an event.

Event Log records contain a “magic number” or unique identifier [119].

- **Recycle Bin:** It covers the functionality to recover deleted files. If a user simply deletes some files, its copy is retained in the recycle bin and can be restored if required; this is known as soft delete.
- **Services Analysis:** It covers the analysis of components of windows services from the acquired image.
- **Registry:** Registry viewer displays the content of registry hive files, shows value names, data, and can export registry keys and their subkeys to a text file.
- **Installed Program:** Scanning for programs installed on the operating system.
- **User Activity:** The User Activity module scans the system for evidence of user activity, such as accessed websites, USB drives, wireless networks, and recent downloads. This is especially useful for identifying the user’s trends and patterns and any material accessed recently.
- **Passwords:** Retrieve passwords and product keys that have been stored by various applications and web browsers on the system.
- **AmCache:** A registry file called *Amcache.hve* is used to store information associated with running programs in the Windows operating system. Several important artifacts are stored in Amcache.hve files related to different actions performed by the user, such as running portable applications, installation of applications, or running host-based applications from an attached external portable device.
- **Timeline:** For each unallocated and existing metadata structure, timeline analysis took the metadata values from the file system and arranged them accordingly, from the recent to the earliest, and interpreted and viewed by the forensic analyst for investigation purposes.
- **Telemetry:** Telemetry is an automated communication process; this data is used to improve application health, customer experiences, monitor security, quality, and process performance.

TABLE 7. Comparison of file system and disk forensic features.

Tools \ Features	Autopsy	Redline	BEC	OSF	PD	XWays	Encase	FTK	MA
									
File System Explorer	✓	✓	✓	✓	✓	✓	✓	✓	✓
HEX Viewer	✓	✗	✓	✓	✗	✓	✓	✓	✓
Carving	✓	✓	✓	✓	✓	✓	✓	✓	✓
VSC Service	✓	✗	✓	✓	✓	✓	✗	✓	✓
Slack Space	✓	✗	✓	✓	✓	✓	✓	✓	✓
Registry	✓	✓	✓	✓	✓	✓	✓	✓	✓
Malware analysis	✓	✓	✓	✓	✗	✓	✓	✓	✓
Hiber/Page/swap files	✓	✗	✓	✓	✓	✗	✗	✓	✓
RAID reconstruction	✗	✗	✓	✗	✗	✓	✓	✓	✗

VSC, Volume Shadow Copy; BEC, Belkasoft Evidence Center; OSF-OSForensics; PD-ProDiscover Basic.

- **SRUM:** Forensic analysts use data collected using SRUM to correlate user activities and even paint a picture of user activity with processes, data transfer, network-related events, and more.

We performed a study on Autopsy, Redline, BEC, OSForensics, ProDiscover Basic, XWays, Encase, and FTK analyzer and identified the features mentioned above by these toolkits. Table 6 summarizes our findings where it can be seen that Belkasoft Evidence Center and OSForensics are promising tools in this domain. FTK also provides most of the features except for the analysis of Windows service.

2) FILE SYSTEM AND DISK FORENSICS

Storage disks have defined mechanisms, structures, and RAID configurations to store and retrieve data. The disk is divided into small units such as tracks and sectors to manage its operations efficiently [49], [120]. The operating system manages files, and each OS has a specific file system. The file system structure contains information to keep data in files secure, precise, and easily accessible when needed. File system forensic analysis examines data in a volume (i.e., a partition or disk) and interprets it as per the file system. There are many results from this process, but examples include listing the files in a directory, recovering deleted content, and viewing the contents of a sector [16], [73]. In addition, files such as paging, hidden, configuration, swapped, encrypted, misnamed, and deleted can be helpful. The following features of a forensics toolkit broadly cover the requirements for file system and disk forensics:

- **File system explorer:** The user maintains files and folders in a hierarchical structure to keep data separated and easy to access. A forensic tool that provides the ability to analyze a file format must present this hierarchical view so that it is as easy for an investigator to view as it would have been for the suspect.
- **Deleted file search & retrieval:** Deleted file entries get removed from the file system, but the deleted content of files can still be found through carving. Recovery of such data/files is critical for the investigator; hence it is an essential forensic feature. It is supported by all toolkits shown in Table 7.

- **Slack space:** Slack space is the portion of the disk occupied by the file but has not been thoroughly utilized. It may contain the residue of a file that previously existed in this portion and may contain a clue to find evidence. A forensic tool capable of retrieving such portions can be a handful for the investigator. This feature is available in each tool listed in Table 7.
- **HEX viewer:** At the lowest level, files exist in the form of bits. Usually, hex values are analyzed by the investigator to have a clear picture of events, especially the metadata that can be obtained and analyzed in hex form.
- **Carving:** In cases where the metadata about the files has been deleted, file carving is employed to recover the data within the files.
- **Volume Shadow Copy Service:** Volume Shadow copies are backup copies of windows files taken during the ordinary course of using a machine. The shadow copy search modules aid in the forensic analysis of these files.
- **Registry:** Windows Operating system maintains a registry to manage its task and record user activities and programs. Windows Registry is one of the richest sources of digital evidence. Computer configurations recently visited web pages and opened documents, connected USB devices, and many other artifacts that can all be acquired by examining registry hives and keys.
- **Malware analysis:** As malicious software can damage a system, the researchers have detected the patterns to avoid these damages. Malware analysis includes various methodologies, like timeline reconstruction and comparison of malware hashes. A tool differentiating these files would be a preference for the investigators.
- **Hibernation/Paging/Swap Files:** Identification, extraction, and analysis of hibernation/paging/memory dump files are vital for file system forensics. If an investigator receives a turned-off system, hibernation, swap, and paging files would be pretty helpful. The system's current state and most recent RAM content are dumped to disk if a system is hibernated. Page and swap files are maintained on disk to utilize the RAM effectively.

- **RAID reconstruction:** An essential part of File System analysis is reconstructing a RAID map when given a set of disk images [118]. The information must be stored on disk in different RAID configurations based on the required balance between reliability, availability, performance, and capacity.

Table 7 depicts our analysis and findings using the features mentioned above, where Belkasoft Evidence Center and FTK prove to be promising tools in this domain. Redline is the most immature tool in this domain. XWays support all necessary features, but it would be a wrong choice if the system received for investigation is powered off. Magnet Axiom provides all features except RAID reconstruction.

3) LIVE MEMORY FORENSICS

A few years back, digital forensics procedures were mainly based on Static analysis of the system. The typical step to perform static analysis was “pulling the plug” so that information on the disk does not change [80], [121]. With the advancement of technology (i.e., the increased storage capacity of the disk, etc.) and techniques (i.e., Data Encryption, password protection, memory-resident malware, etc.), the importance of volatile data existing on Memory (RAM) is realized. RAM is an intermediate memory between processor and secondary storage. It enables access to running process information, associated DLLs, handles, open files, decrypted data, registry, user password and activities, connection & session details. RAM analysis allows accessing data in ways that produce transparent information, which otherwise could not have been possible [79]. This can help reveal hidden processes, malware hiding information, decrypted data/passwords, and many other interesting pieces [122].

Operating systems manage their activities through kernels residing in RAM by defining kernel and user spaces. The kernel performs memory, resource, and device management by maintaining complex data structures. Several tools are designed to perform memory forensics using specialized techniques to access memory structure. In this part of the paper, we have compared some memory forensic tools based on attributes or features required to perform analysis [78]. Volatility, Rekall, F-response, and Windows Scope are specific tools to support live memory forensic analysis. Some of the prominent features which are provided by live memory tools are as follows:

- **Command Line/Graphical User Interface (CLI/GUI):** Some tools provide a user-friendly GUI, while others provide only a command-line interface, and some provide both.
- **Remote access:** An investigator may want to capture the memory remotely to be analyzed. Tools can load agents to the victim machine and perform required operations remotely.
- **Acquisition:** As the acquisition is the initial phase of digital forensics, this attribute shows if the tool can dump the memory by itself or not. Several challenges

are associated with memory acquisition, i.e., Volatility of data, loading new processes, and modifying memory. Since analysis is performed on a separate system, some tools only support analysis, not acquisition.

- **Multi-user:** Multiple investigators working on the same case may require a tool that allows multiple users to maintain their activities separately. So memory forensics tools are also analyzed on this basis.
- **Supported formats:** The growth of technology has introduced new techniques to acquire memory dumps. For example, Windows allows hibernation, which creates hiberfile.sys on disk, so system states and processes can be restored on power-up. Similarly, VMware produces a .vmem file that can be analyzed, and this file can be extracted and analyzed in some tools. A list of memory dump formats supported by the tool is given in Table 4.
- **Source OS:** Every operating system has its specific structure to manage operations in memory. To analyze a memory dump, it is necessary to know which forensic tools support OS versions.
- **Carving:** Memory dump contains several data structures that may yield forensic information, known extraction techniques for memory are traversing, pool tag scanning, or pattern-based extraction. In traversing, information is extracted through doubly link lists (i.e., Process list, DLLs list, etc.). A search for pool tags can help reveal unlinked objects or the ones that try to hide. It is also possible to scan dumps for specific patterns to reveal something. This feature is available with every toolkit mentioned in Table 9.
- **Data recovery:** A tool can recover data that has been deleted, corrupted, or hidden in memory. Since deleting objects generally deletes object entry, it leaves associated content and some relevant information. It is recoverable as long as not overwritten. This feature is supported by every tool mentioned in Table 9.
- **Slack space:** If a tool can look in space reserved for a data structure where part of it is not currently in use and contains the left-overs of previously existing data, it may lead to evidence [123]. This feature is available in every tool shown in Table 9.
- **Static or live analysis:** The live analysis is performed on critical systems that should not be powered off, or a longer time is required to image RAM of large size [35]. It is inherently inconsistent but somehow useful against anti-forensic techniques, affecting the static analysis [124]. The live analysis feature is also supported by all tools shown in Table 9.
- **Swap space:** Memory creates swap space to allow optimal access to the current application. This space holds information of processes not yet active, yet recoverable [124] and may contain forensic evidence as discussed by Savoldi [123].
- **Graphical access view:** A tool may provide an output that can be presented graphically to better view how

TABLE 8. General comparison of live memory forensic toolkits.

Tools	Volatility Framework	Rekall	F-Response	Redline	Encase	BEC	WS
Features							
License	Open	Open	Propriety	Open	Propriety	Propriety	Propriety
Platform	Window, Linux, OSX	Window, Linux, OSX	Window, Linux, MAC, Android	Window	Window, Linux	Window	Window
CLI/ GUI	CLI	CLI	CLI/GUI	GUI	CLI	GUI	GUI
Supported Formats	Raw Image, EWF, Crash Dumps, Hiberfil.sys, V. I, MacOS HPAK FireWire	Raw Image, AFF4, EWF, Hyberfil	Raw Image, SMART, E01, AFF	Raw Image	Raw Image, Crash Dump, E01, EWF,	Raw Image, EWF, AFF, DMG, Hyberfil.sys,	Raw Image
Source OS	Window, Linux MAC OSX	Window, Linux MAC OSX	Window	Window	Window, Linux OS X	Window, Linux OS X	Window

BEC, Belkasoft Evidence Center; OSF-OSForensics; PD-ProDiscover Basic.

TABLE 9. Comparison of live memory forensic tools based on specific features.

Tools	Volatility Framework	Rekall	F-Response	Redline	Encase	BEC	WS
Features							
Remote access	×	✓	✓	×	✓	✓	✓
Acquisition	✓	✓	✓	✓	✓	✓	✓
Multi-user	×	×	✓	×	✓	✓	×
Format conversion	✓	✓	×	×	×	×	×
Swap space	✓	✓	✓	×	✓	✓	×
Graphical Access View	✓	✓	×	×	×	✓	✓
Password Recovery	✓	✓	×	×	✓	✓	×

BEC, Belkasoft Evidence Center; OSF-OSForensics; PD-ProDiscover Basic.

objects are related/linked to each other, either through its embedded viewer or a third-party viewer.

Volatility, Rekall, F-Response, Redline, Encase, Belkasoft Evidence Center, and Windows Scope have prominently used memory forensics tools. Table 8 presents the analysis and findings of these tools based on generic features such as licensing status, supported platforms, interface information (CLI/GUI), supported memory formats, and source operating system. Volatility seems a better choice with multi-OS and multi-format support and open licensing status but with a command-line interface.

In Table 9, we present an extensive feature-wise analysis of memory forensic tools. Malware detection, rootkit identification, timeline analysis are the core features of all these tools. Rekall and Volatility are appropriate choices with an open license. Belkasoft is the most promising propriety tool but does not support the operating system other than windows.

4) WEB FORENSICS

These activities can critically represent human behavior. Most of the web activities are performed using a web browser and web application linked with the browsers [125]. Complete user activity is placed in web storage records, and many artifacts related to emails, visited web pages, chats, search queries can be retrieved. Every OS and browser

manages these artifacts differently, and a careful OS and browser-specific analysis can help trace a crime [87], [126]. Authors in [127] presented a forensic model to investigate web activity, where the disk and live memory images are acquired to access web activity and search engine records. Later, a sort match or statistical analysis is performed to establish a correlation with a specific crime as discussed in [128]–[130]. The worth observing features of web forensic tools presented in Table 10 are as follows:

- **Supported browsers:** Each browser application has its structures to manage data, and it is necessary to know which browser’s support is provided by a forensic tool. A generic forensic tool supporting multiple browsers would be a better choice for an investigator in general [127].
- **Bookmarks:** Since a user can bookmark important links (URLs) that they have to use frequently, a correlation can be established by obtaining important links a criminal might be using.
- **History:** A browser maintains a record of each website visited and kept it for a specific time duration. Some useful information like when and how frequently a website has been visited, by whom, and the activity performed on that website is information that can be processed intelligently.

TABLE 10. Generic comparison of toolkits for web forensic features.

Features \ Tools	Autopsy	Redline	OSF	PD	XWays	Encase	FTK
							
Supported Browsers	Firefox, Chrome, Internet Explorer	All	Chrome, IE, Firefox, Safari, Opera	Index.dat files containing Internet Explorer Web history and populate the Internet History Viewer	IE, Firefox, Chrome Safari	IE, Firefox, Chrome Safari Opera Mac IE	IE, Firefox, Chrome
Supported database	Ingest modules: Parse SQLite Databases, Parse, SQLite, Deleted Records	✓	SQLite analysis: Freelists, Journal/WAL, carving, SQLite Viewer	×	SQLite databases	SQLite	SQLite

OSF-OSForensics; PD-ProDiscover Basic.

TABLE 11. Feature wise comparison of toolkits for web forensics.

Features \ Tools	Autopsy	Redline	OSF	PD	XWays	Encase	FTK
							
Bookmarks	✓	✓	✓	×	✓	×	✓
Cookies	✓	✓	✓	×	✓	✓	✓
History	✓	✓	✓	×	✓	✓	✓
Downloads	✓	✓	✓	×	×	✓	✓
Search queries	✓	✓	✓	×	×	✓	✓
Cache	×	×	×	×	✓	✓	✓

OSF-OSForensics; PD-ProDiscover Basic.

- **Cookies:** Cookies are used by browsers to keep user browsing information, manage necessary web functionalities (Add-ons, items on display, etc.), and are helpful in traffic analysis. Getting access to these can reveal name, domain, content, path, creation, and expiry times.
- **Downloads:** The browser keeps the information and files downloaded from websites. Some cases may require investigation by observing downloaded files.
- **Search queries:** Browsers log every searched keyword. An investigator might be interested in determining a suspect is searching profile concerning a particular crime, such as which search engine is used, which keywords have been searched, and when.
- **Cache:** To have faster access to data and to maintain some information about previous sessions, websites keep requested data in cache files. URL, content type, file size, accessed date and time, server time, expiry time, server response, eTag, cache-control can be extracted through the cache.

General and feature-specific comparison of well-known toolkits in the forensic web domain can be observed in Table 10 and 11 respectively. For example, encase, and Redline has maximum multi-browser support and supports most web forensics, while ProDiscover basic does not support database queries.

5) EMAIL FORENSICS

Email is an electronic communication over the Internet that carries messages to deliver files, documents, and other transaction elements. An email, when transmitted, contains the source, content, actual sender and receiver information, date/time, protocols, and server information. Email services used could either be webmail or a local mailbox. A criminal can misuse email to send viruses, worms, or trojan and may transmit phishing emails, spam, or perform other illegitimate activities. Email forensics uses header analysis, sender fingerprints, server-side, and network device-based investigation or software embedded identifier. For analysis of forensic tools for email analysis, we have chosen the following features:

- **Header:** According to [131], a thorough investigation of email headers should include: examining the sender’s email address, examining message initiation protocol (HTTP vs. SMTP), examining message ID, and examining the sender’s IP address. In addition, the investigation includes system files analysis (pagefile.sys, swapfile.sys, and hiberfil.sys) in webmail [118]. This also includes investigation supporting artifacts such as protocols used (SMTP or HTTP) metadata, keyword searching, port scanning, etc. [132]. The renowned ones include OST and PST files (MS Outlook), and NSF (Lotus Notes) files, mbox, and Maildir (which are the two primary local mail storage

TABLE 12. Comparison of email forensic toolkits.

Tools	Autopsy	BEC	OSF	PD	XWays	Encase	FTK
Features							
Email Type	Offline	Online Offline	Offline	Offline	Online Offline	Offline	Offline
Module	Email Parser	×	×	×	×	×	×
Search Option	×	Searching, connection graph & attachments	Index searching, attachments	searching	×	Keyword Searching	✓
Mailbox	Identifies Thunderbird MBOX files and PST format files based on file signatures, extracting the e-mails	Outlook, Outlook Express, Gmail offline, Mozilla Thunderbird, Window Live Mail, The Bat, Apple Mail Parsing carving such as EML, Mbox, MSG, and MIME	Email search	PST/OST /DBX	MBOX	DBX, EDB, PST/NSF, EMLX, AOL, MBOX,	DBX, MBX, PST/OST, Saved, Sent Mail, Trash,
System Artifact Analysis	×	Live memory, System file analysis	✓	×	Searches signature at byte level within pagefile.sys files, to find e-mail fragments	✓	✓
Visualization Support	✓	✓	✓	×	✓	✓	✓

BEC, Belkasoft Evidence Center; OSF-OSForensics; PD-ProDiscover Basic.

formats used by Linux email clients), and Apple Mailbox [97].

- **Email type:** This entry describes if the tool has support to perform analysis in online or offline mode.
- **Modules:** Describes which modules are used by the tool to view emails
- **Search option:** A tool can perform routine searches, indexed searches, attachment, and connection graph searches.
- **Mailbox:** lists the mailboxes and email formats that can be identified & have support provided in the forensic tool.
- **System artifacts analysis:** Since email, artifacts can be recovered from system files or RAM. The table entry describes what level of extraction, i.e., memory analysis, swap analysis, system files, etc., are performed to recover artifacts.
- **Visualization support:** This module investigates if the email can be visualized in an interface or not.

Table 12 presents a comparative analysis of features provided for email forensics in chosen toolkits. Belkasoft Evidence center seems the most powerful toolkit with offline and online email analysis features and supports multiple mailboxes.

6) NETWORK FORENSICS

Most of the cyber-attacks are also performed using networks [133]. A network is a collection of devices

connected to communication. The network can be classified based on nature (LAN/MAN/WAN), accessibility (public/private/hybrid), and medium (wired or Wireless) [99]. User accountability while communicating on the network is essential. Forensic analysis of networks is critical. Reference [134] presented taxonomy to carry out network forensic processes.

Network forensics refers to determining the source of the attack and collecting evidence by proactive monitoring and analyzing network traffic that is highly dynamic and volatile. A network comprises several essential components like a switch, router, firewall, Intrusion detection system, IoT devices. Reference [135]–[139]. Information is distributed and can be collected and analyzed based on several features. There are specialized tools used for network forensics: Network Miner, LogRhythm, PLIXER, NIKSUN, Nmap, and XPLiCO are some of the well-known network forensic tools [140]. The following features have been identified for comparison:

- **NetFlow:** A tool capturing packet can reveal the source and destination addresses, protocols used to communicate among nodes, summarize conversation/session period, and several packets captured. In addition, the tool may present protocol-specific statistics such as RTP Stats, Response time, TCP re-transmissions, VoIP calls, etc. This necessary feature is available with all the tools mentioned above.

TABLE 13. Generic comparison of network forensic toolkits.

Tools	Network Miner	LogRhythm	PLIXER	NIKSUN	Nmap	XPLiCO
Features						
License	Open Source	Open Source	Commercial	Open Source	Open Source	Open Source
Supported OS	Window, Linux, MAC OS X, FreeBSD)	×	×	×	Window, Linux, Solaris, MAC OS, HP-UX	Linux
Report	✓	✓	✓	✓	✓	✓

TABLE 14. Feature wise comparison of network forensic toolkits.

Tools	Network Miner	LogRhythm	PLIXER	NIKSUN	Nmap	XPLiCO
Features						
OS Fingerprints	✓	✓	×	✓	✓	×
Port Scanner	✓	✓	✓	✓	✓	×
Banner grabber	×	×	×	×	✓	×
Threat analysis	✓	✓	✓	✓	✓	×
Recover data	✓	✓	✓	×	✓	✓
Extract user credentials	✓	✓	✓	×	×	×
Log collection	✓	✓	✓	✓	✓	×
Remote Analysis	✓	✓	✓	✓	✓	×

- **OS fingerprints:** Operating systems are an essential consideration to design and implement security control on either the network or the local machine. Therefore, a tool must determine the OS fingerprint to narrow down the problem.
- **Port scanner:** It allows probing a system for open ports, which could help establish if the system was exposed to a particular kind of attack.
- **Banner grabber:** In support of port scanning, it allows determining what services and which of their versions were running on the system’s open ports.
- **Threat analysis:** Some tools may detect intrusion patterns using IDS/IPS capabilities and determine threat impact levels by heuristic methods.
- **Recover Data:** Several vital contents such as files, emails, and VoIP data are regular communication over the Internet. Therefore, a tool recovering these from network traffic can be helpful for forensic investigation. Besides, a tool can reassemble raw PDUs from multiple TCP segments and reveal import contents.
- **Extract user credentials:** Since network packets contain passwords and other sessions, critical information to authenticate users over the internet/network, a forensic tool can detect and extract such critical information to serve the investigator’s purpose.
- **Encrypted traffic:** Traffic encryption is an increasing trend, as experts recommend to make your conversation secure. Although encryption on network traffic prevents deep packet inspection, there are tools to detect and prevent attacks. This is provided by all the tools shown in Table 14.

- **Log collection:** As the network devices maintain logs for security and audit purposes, a tool can collect these logs and produce information regarding the particular event that led to a cyber-attack.
- **Remote analysis:** A network forensic tool can perform forensic analysis by connecting remotely and may present an analysis report to maintain a record.

The authors in [141] presented critical research areas like social networks and cloud computing forensics. A general comparison of tools specific for network forensic based on licensing status and supported OS can be found in Table 13 and a comparison concerning specific features can be found in Table 14. It can be observed that except PLIXER, all the network forensic tools are open source tools, and Nmap supports most of the operating systems. However, the banner grabber feature is provided by Nmap only, and XPLiCO can perform data recovery only.

7) MULTIMEDIA FORENSICS

In this technology era, users enjoy intelligent devices, high bandwidth connections, and bulks of diverse storage space. Using different software platforms, people share massive multimedia content on social sites in images, texts, audio, software, and videos [142]. This rise has also caused an increase in cybercrimes, including harassment, content forgery, intellectual property theft, and repudiation. Governments need continuous monitoring to combat such crimes. However, it is a complex task for the investigator to go through all the records for a particular event. Automating

TABLE 15. Comparison of multimedia forensic toolkits.

Tools Features	IntaForensics	Amped	Cognitech	FMDES	AMR	avdetective
						
Authentication	✓	✗	✗	✗	✓	✓
Clarification and Speed Correction	✓	✓	✓	✓	✓	✓
Compilation	✓	✗	✓	✗	✗	✓
Highlighting or Pixelation	✓	✓	✓	✓	✗	✗
Restoration of Distorted Video and Audio	✓	✓	✓	✓	✗	✗
Interlacing and De-interlacing	✗	✓	✓	✓	✗	✓
Object Detection	✓	✓	✓	✓	✓	✓

FMDES, Forensic Clarification and Analysis Solutions; AMR, Advanced Micro Resource.

the investigation process and using the multimedia forensic tool can be a solution discussed in¹² and [143].

Digital visual media represents one of the principal means of communication nowadays. Digital images are the target of many digital investigations because some are contraband. This type of analysis looks for information about where the picture was taken and who is in the picture. Image analysis also includes examining images for evidence of stenography.

Video analysis can automatically analyze video to detect and determine temporal and spatial events, while forensic video analysis compares and evaluates video in legal matters [100]. Digital video is used in security cameras, personal video cameras, and webcams. Investigations of online predators can sometimes involve digital video from webcams. This type of analysis examines the video for the identity of objects and the location where it was shot. Forensic video analysis has been used in various high-profile cases, international disagreements, and conflict zones. The following features should be available with any multimedia forensics tool:

- **Image authentication:** Image ballistics is used to match metadata & file structure for available device features (i.e., Digital Camera, Make & Model, etc.). Active authentication can be performed by obtaining the embedded watermark or digital signature while recording or sending, usually performed to keep copyrights. At the same time, images without embedded code can passively access themselves for integrity.
- **Clarification:** Classifying video footage means removing noise, interlacing lines, and video graininess. Transient items like rain and snow are removed, revealing hidden details. Blurring caused by interlacing, lens blur, and camera/subject motion is reduced, and images are significantly improved with multi-frame and velocity reconstruction processing technologies for the best enhancement job available.
- **Image sequence compilation:** It converts a set of images into a video for analysis or courtroom presentation.

- **Highlighting or Pixelation:** This focuses the viewer on a user-defined area of interest to provide insight into the case.
- **Reconstruction of Distorted Video/ Image:** An image that is only partially visible at any one time as a complete image. For example, a car passes by, but only part of the car is visible as it passes by. We create a mosaic image that stitches the whole car and renders it still.
- **Interlacing and de-interlacing:** This functionality allows for loss-less conversion between interlaced and progressive video.
- **Object Detection:** This module is used to detect any object in an image or video, as a human, car, or weapon.

InstaForensics, Amped, Cognitech, FMDES, AMR, and detective are essential specialized tools for multimedia forensics. The detailed comparison of these tools based on the features mentioned above is presented in Table 15: IntaForensics and Cognitech and promising tools providing various features.

In this section, we analyzed eight computer forensic toolkits in general, and then we had a detailed study on features provided by these toolkits in different computer forensic domains.

According to its unique requirements, a forensic investigator handles each case, maintaining set protocols for evidence collection, acquisition, examination, and reporting while maintaining a chain of custody and preserving evidence’s integrity. The choice of a forensic tool depends on case requirements. However, in some cases, he needs to make choices based on features supported by that tool. This work’s primary goal is to help the investigator select forensic toolkits. This section proposes a mathematical scoring model to compare the forensic toolkits in general and then their strength in each forensic domain. A feature supported by a forensic toolkit is given 2 points, and in case of no support, it is given 0 points. We have assigned equal weights to all features since one feature may be necessary in one forensic investigation case while another may not be important. Therefore, all features are treated equally in the proposed model. Total points of supported features are summed up, and the score is normalized between 0 and 100.

¹²<https://www.nist.gov/topics/forensic-science/reference-materials-standards-and-guidelines>

TABLE 16. FSM-based comparison of operating system forensic toolkits.

Tools \ Features	Autopsy	Redline	BEC	OSF	PD	XWays	Encase	FTK
								
Total Score	12	10	16	16	10	12	12	18
Percent Score	66	55	88	88	55	66	66	100

Key: BEC, Belkasoft Evidence Center; PD-ProDiscover Basic; OSF-OSForensics

TABLE 17. FSM-based comparison of file system and disk forensic toolkits.

Tools \ Features	Autopsy	Redline	BEC	OSF	PD	XWays	Encase	FTK
								
Total Score	16	8	18	16	12	16	14	18
Percent Score	88	44	100	88	66	88	77	100

BEC, Belkasoft Evidence Center; PD-ProDiscover Basic; OSF-OSForensics

TABLE 18. FSM-based comparison of live memory forensic toolkits.

Tools \ Features	Volatility Framework	Rekall	FR	Redline	Encase	BEC	WS
							
Total Score	10	12	8	2	10	12	6
Average Score	71	85	57	14	71	85	42

BEC, Belkasoft Evidence Center; WS, Window Scope; FR, F-Response.

The scores of toolkits are calculated using Equation (1) to rank the best toolkit. Scores are ranked between 0 and 100 where 100 is maximum score indicating best toolkit.

$$S(t) = \sum_{i=1}^n \sum_{f_i=1}^F f_i \tag{1}$$

where S represents the overall score of the tool t , n denotes the total number of tools, f is the score of a particular feature that a tool supports, and F is the total number of features in the tool.

Table 16 shows the scores obtained by various forensic toolkits for 9 features to rank tools for operating system analysis. For example, the table depicts that for investigation of operating system artifacts using open source tools FTK, Autopsy, Redline, and Pro-Discover Basic version scored 100, 60, 55, and 55 respectively. In contrast, proprietary toolkits such as Encase, Belkasoft, OSForensics, and XWays scored points with the percentage of 66, 88, 88, 66, respectively, out of 100. Thus, our study suggests using FTK or OSForensics from propriety toolkits to investigate the operating system.

Table 17 includes a total score and percent score in the file system and disk forensics domain for 9 features. FTK and Autopsy scored 100 and 88 percent among open-source toolkits, and among proprietary toolkits, Belkasoft scored the highest percentage of 100, OSForensics, and XWays scored 88 Encase scored 77 out of 100. Belkasoft provides the unique functionality of RAID Reconstruction not provided by

any other toolkit. Our study suggests using FTK and Autopsy as a freeware tool and Belkasoft as a paid tool to investigate the file system and disk.

The comparative score for the investigation of live memory artifacts based on FSM using seven features is shown in Table 18. Open-source toolkits such as Volatility Framework, Rekall, and Redline scored 71, 85, and 14, respectively, while proprietary toolkits such as F-Response, Encase, Belkasoft, and Window Scope scored 57, 71, 85, and 42, respectively, out of 100. Therefore, our study suggests using Rekall as an open-source tool or Belkasoft, a commercially paid tool to investigate memory artifacts.

Table 19 presents FSM scores of web forensics toolkits based on six features. FTK scored 100, whereas Encase, OSForensics, Autopsy, and Redline scored 83 percent. Our study suggests using FTK or Autopsy as a freeware tool first, or an investigator can use OSForensic and Encase commercial tools.

For email analysis, Table 20 depicts that using open source toolkits such as FTK, Autopsy, and Pro-Discover Basic scored 83, 66, and 50 percent respectively proprietary toolkits such as Belkasoft, OSForensics, and XWays scored a similar percentage. Therefore, to investigate email artifacts, our study suggests using FTK, which supports maximum features.

FSM-based scoring of network forensics tools is shown in Table 21. Results show that Network Miner and LogRythm are the most appropriate choices among open-source toolkits. Plixer is a proprietary tool that scored 66 percent out of 100 and can be used.

TABLE 19. FSM-based comparison of web forensics toolkits.

Features \ Tools	Autopsy	Redline	OSF	PD	XWays	Encase	FTK
							
Total Score	10	10	10	0	8	10	12
Average Score	83	83	83	0	66	83	100

PD-ProDiscover Basic; OSF-OSForensics

TABLE 20. FSM-based comparison of email forensic toolkits.

Features \ Tools	Autopsy	BEC	OSF	PD	XWays	Encase	FTK
							
Total Score	8	10	10	6	8	10	10
Percent Score	66	83	83	50	66	83	83

BEC, Belkasoft Evidence Center; PD-ProDiscover Basic; OSF-OSForensics.

TABLE 21. FSM-based comparison of network forensics tools.

Features \ Tools	Network Miner	LogRhythm	Plixer	NIKSUN	Nmap	Xplico
						
Total Score	14	14	12	10	14	22
Percent Score	77	77	66	55	77	11

TABLE 22. FSM-based comparison of multimedia forensic tools.

Features \ Tools	IntaForensics	Amped	Cognitech	FMDES	AMR	avdetective
						
Total Score	12	10	12	10	6	10
Percent Score	85	71	85	71	41	71

FMDES, Forensic Clarification and Analysis Solutions; AMR, Advanced Micro Resource.

Six investigation tools for multimedia forensics were also analyzed using FSM, and scores are shown in Table 22. Our study suggests using instaforensic or cognitive as their FSM-based score is highest along all tools used in this study to investigate multimedia artifacts.

Figure 5 summarizes our findings based on our proposed Feature Scoring Model (FSM). Initial feature-based analysis in each computer forensic domain and then scored-based analysis of toolkits revealed that FTK is the most appropriate toolkit for investigating operating system artifacts as it enables the user to perform services analysis. FTK is the best choice for file system and disk forensic and outclasses all other forensic toolkits for email-related investigation.

For live memory analysis as shown in Figure 6, Belkasoft Evidence Center and Rekall are the most promising choices. Belkasoft Evidence Center supports Windows operating system only whereas Rekall supports Windows, Linux as well as OS X. Multimedia artifacts can be examined using instaforensics or Cognitech toolkits effectively, as shown in Figure 8. Network Miner, LogRythm, and Nmap are

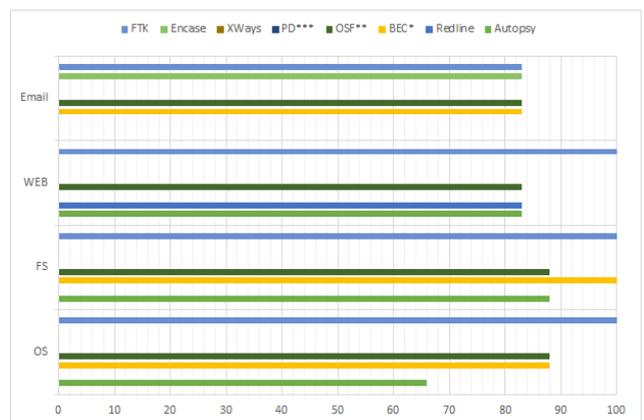


FIGURE 5. Overall FSM-based comparison of toolkits in operating system, file system, web forensics and email forensics domains.

good choices for network forensics investigations, as shown in Figure 7. However, Nmap supports multiple operating systems and provides most of the required features.

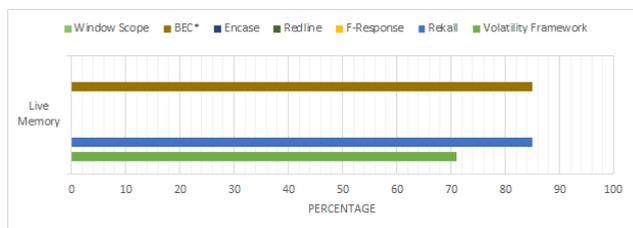


FIGURE 6. Overall FSM-based comparison of live memory forensic domain.

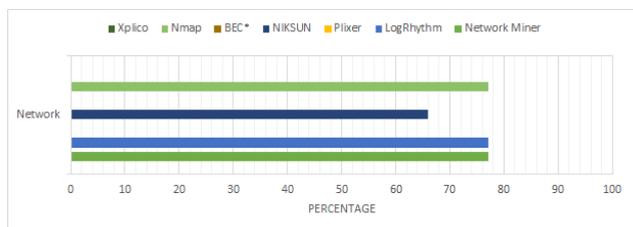


FIGURE 7. Overall FSM-based comparison of network forensic domain.

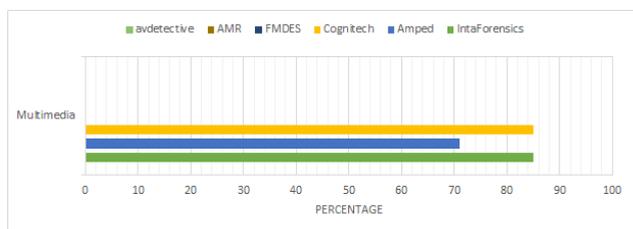


FIGURE 8. Overall FSM-based comparison of multimedia forensic domain.

V. DISCUSSION

Cybersecurity attacks continue to grow in number and sophistication, and the costs of these incidents are more substantial than ever before [144]. With the increasing rate of cybercrimes worldwide of diverse nature and complexity, ranging from content forgery, financial data frauds to cyber terrorism with large groups and government involvement, the need for computer forensic algorithms, solutions, and tools have arisen [145]–[148]. As a result, governments and organizations have started taking this up seriously and developing and applying laws and standards related to cybercrimes, digital evidence, search and seizure methods, evidence recovery, investigation, and reporting processes.

Cybercriminals are growing more sophisticated in their use of technologies that allow them to hide their conduct better than ever. Financial losses caused to large organizations on an ongoing basis have compelled them to either employ a computer forensic agency or hire computer forensic investigators to protect them from attacks and solve cases by performing competent and thorough investigations in a reduced time frame. The investigators must follow the investigation process abiding by the local laws and established standards, ensuring evidence’s integrity and proving a case in a court of law.

In this study, our findings based on FSM show that FTK forensic toolkit outperformed other toolkits in four major fields of computer forensic (i.e., operating system forensics, file system forensics, web forensics, email forensics) while Belkasoft Evidence Center outperformed other toolkits in live memory forensics domain. Network miners outperformed other toolkits in the network forensics domain. Magnet axiom only covers the artifacts collected from data recovery, which is why its low scores. An excellent forensic tool helps investigators sort and analyze the large volumes of data obtained through different sources. An intelligent selection of tools based on supported features using our proposed Feature Scoring Model would reduce investigation time and effort. We observed in this study that several features provided by video and audio forensic tools are limited and time taking, and real-time forensic solutions for video/audio/network stream data are missing.

The results of digital forensic tools must be repeatable and reproducible to assess “trueness and precision.” Repeatability ensures that independent test results are obtained with the same method, identical test items, in the same laboratory, by the same operator, using the same equipment within short intervals. Reproducibility ensures that the test results are obtained with the same method on identical test items in different laboratories with different operators using different equipment. The investigator must follow a repeatable and well-documented set of steps such that every iteration of analysis gives the same findings. In this study, we relied on the information provided by vendors and users of forensics toolkits; therefore, the repeatability and reproducibility of results produced by these toolkits are not assessed.

A. FUTURE RESEARCH DIRECTIONS

Cybercriminals wreak havoc in many ways: identity theft, money laundering, personal security, ensuring against blackmailing, unauthorized access to private data, averting sexual provocation, corruption, and other such cybercrimes where advanced information and delicate data are included. Current digital forensics presents a variety of unique challenges. There exist some technological challenges, legal challenges, and resource challenges during the investigation.

1) GENERATION OF STRUCTURED DATA

One of the significant future research challenges is generating structured data from hybrid data efficiently and automatically. Future researchers should consider the operating system for the generation of structured data and the standard for the semistructured formats used for different data types.

2) DOMAIN CASE STUDY

In the future, a case-specific study can be conducted for each domain to assess the repeatability and reproducibility of results generated by each forensic toolkit.

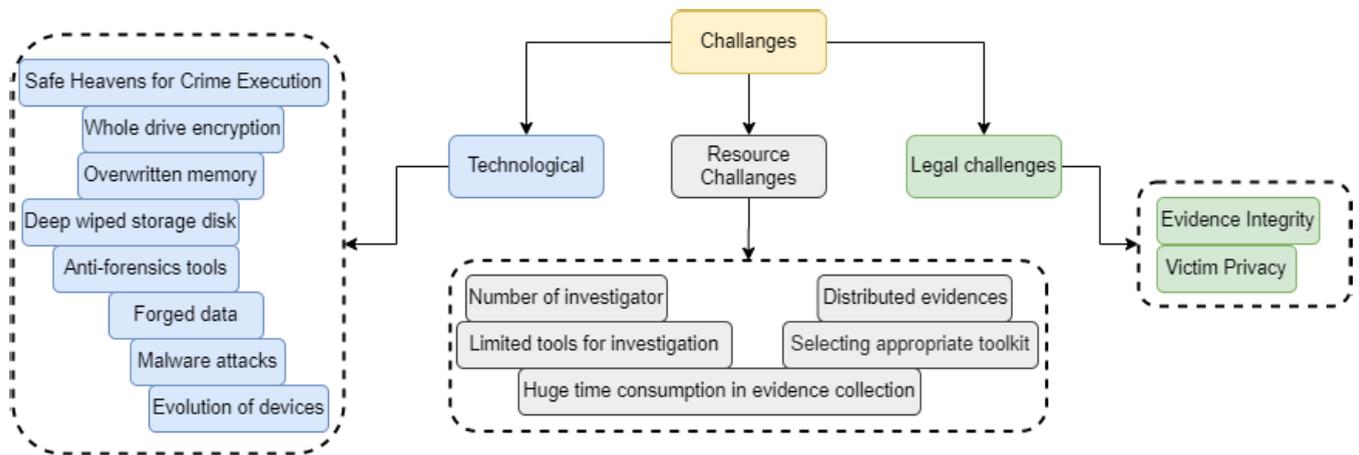


FIGURE 9. Overview of the digital forensics challenges.

3) ADVANCE FORENSIC TOOLS

The future work incorporates the mapping of advanced digital forensic tools and improvement of information precision, high-speed evidence collection, reduction of evidence complexity, consistent and up-to-date quality of tools and investigation techniques, evidence security, use of blockchain in evidence handling, and other protection measures by carrying out a comparative investigation on available forensic tools.

4) MACHINE LEARNING AND DEEP LEARNING FOR FORENSIC

In this era of fast technologies, automated forensic tools using machine learning and deep learning algorithms are required to learn from the usage behaviors of users by observing system logs and generating an alarm or taking actions for all anomalous behaviors of users beforehand [149]. These behaviors may likely be reported and analyzed on a dedicated machine separately.

5) PROACTIVE FORENSIC APPROACH

A proactive forensic approach can be a good solution for crime prevention. Automated post-breach software forensic tools collecting evidence proactively without compromising user privacy are required.

6) ANTI-FORENSIC TOOLS

Having anti-forensic tools aligned with operating systems can be a solution for large organizations to combat internal cyber-attacks. Speaker identification solutions from large volumes of audio data and objection detection and identification solutions from bulks of image and video data need to be designed and improved. For example, an investigator might be interested in observing videos containing a specific type of weapon or in observing people of a particular age group or gender [150].

7) DIGITAL FORENSIC ONTOLOGIES

The standardization of digital forensic ontologies is another significant future research challenge in this field because most of the frameworks and techniques used in the existing research literature apply custom applications and domains. The use of proprietary implementations avoids the ultimate use and global deployment of digital forensic tools.

8) AI AND DIGITAL FORENSIC

AI is the future of digital forensic from the perspective of automation. The researchers should identify AI's role in the "Evidence Analysis" phase. In the future, digital forensic AI will process data, develop hypotheses that can be presented in the court of law.

9) BLOCKCHAIN FOR FORENSICS

Blockchain can offer several applications for a digital forensics investigation, including evidence collection, preservation, evidence validation, evidence analysis. Researchers can use blockchain for digital forensics, as with blockchain, traceability can be achieved, and also the records will be immutable.

B. CHALLENGES

1) TECHNOLOGICAL CHALLENGES

Technological challenges include whole drive encryption, overwritten memory data, deep wiped storage disk, forged data, anti-forensics tools, scale and cloud resources, the fast evolution of devices, shift towards IoT, malware attacks, execution of crime from safe places, and Botnet attacks [4], [151]–[153].

2) LEGAL CHALLENGES

In case of legal challenge, investigators have to keep the integrity of evidence, and the investigator has to investigate without damaging the accused or the organization's privacy.

3) RESOURCE CHALLENGES

Researchers' challenge in the digital forensics domain is the nonavailability of benchmarks and standard data sets to facilitate comparisons on research findings. In addition, resource challenges include massive time consumption in evidence collection, limited tools for investigation, number of investigators, and distributed pieces of evidence; These are some challenges that need to be addressed. Figure 9 provides an overview of Digital Forensics Challenges.

VI. CONCLUSION

This paper presented the current state-of-the-art research on computer forensics and sheds light on research gaps. The core findings of this extensive research are to provide a detailed analysis of computer forensic domains and toolkits used for each computer forensic domain investigation. We presented a detailed comparative analysis of computer forensic domains and proposed a scoring model for paid and unpaid toolkits based on different features to help investigators choose a potential toolkit for a particular situation depending on the subtleties. The investigator can likewise focus on a potential toolkit for forensic investigations, provide proof of compliance, and ensure a reduction in investigation time. Each tool has its qualities and shortcomings that require attention while using them in a particular situation. The investigators can utilize our exploration as a manual to contrast their toolkits under use with other toolkits and possibly invoke improvements in forensic tools.

A. FUTURE WORK

In the future, we intend to cover more studies on digital forensics tools and techniques included live forensics, registry forensics, and adversary machine learning, and deep learning forensics techniques.

B. LIMITATIONS

Most of the forensics tools used in the survey are available for free or trial versions because the paid tools are too expensive and challenging for students, practitioners, and researchers to purchase for experiments purposes.

REFERENCES

- [1] W. Ahmed, F. Shahzad, A. R. Javed, F. Iqbal, and L. Ali, "WhatsApp network forensics: Discovering the IP addresses of suspects," in *Proc. 11th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Apr. 2021, pp. 1–7.
- [2] C. Iwendi, Z. Jalil, A. R. Javed, T. Reddy G., R. Kaluri, G. Srivastava, and O. Jo, "KeySplitWatermark: Zero watermarking algorithm for software protection against cyber-attacks," *IEEE Access*, vol. 8, pp. 72650–72660, 2020.
- [3] A. R. Javed, M. O. Beg, M. Asim, T. Baker, and A. H. Al-Bayatti, "AlphaLogger: Detecting motion-based side-channel attack using smartphone keystrokes," *J. Ambient Intell. Hum. Comput.*, pp. 1–14, Feb. 2020.
- [4] A. R. Javed, Z. Jalil, S. A. Moqurrab, S. Abbas, and X. Liu, "Ensemble AdaBoost classifier for accurate and fast detection of botnet attacks in connected vehicles," *Trans. Emerg. Telecommun. Technol.*, Aug. 2020, Art. no. e4088.
- [5] N. Serketzis, V. Katos, C. Ilioudis, D. Baltatzis, and G. Pangalos, "Improving forensic triage efficiency through cyber threat intelligence," *Future Internet*, vol. 11, no. 7, p. 162, Jul. 2019.
- [6] M. Keshavarzi and H. R. Ghaffary, "I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion," *Comput. Sci. Rev.*, vol. 36, May 2020, Art. no. 100233.
- [7] S. Niksefat, P. Kaghazgaran, and B. Sadeghiyan, "Privacy issues in intrusion detection systems: A taxonomy, survey and future directions," *Comput. Sci. Rev.*, vol. 25, pp. 69–78, Aug. 2017.
- [8] N. A. Mutawa, J. Bryce, V. N. L. Franqueira, A. Marrington, and J. C. Read, "Behavioural digital forensics model: Embedding behavioural evidence analysis into the investigation of digital crimes," *Digit. Invest.*, vol. 28, pp. 70–82, Mar. 2019.
- [9] M. Hina, M. Ali, A. R. Javed, F. Ghabban, L. A. Khan, and Z. Jalil, "SeFACED: Semantic-based forensic analysis and classification of e-mail data using deep learning," *IEEE Access*, vol. 9, pp. 98398–98411, 2021.
- [10] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan, and M. S. Haghghi, "Anomaly detection in automated vehicles using multistage attention-based convolutional neural network," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4291–4300, Jul. 2021.
- [11] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Comput. Sci. Rev.*, vol. 33, pp. 1–48, Aug. 2019.
- [12] T. Wang, Y. Quan, X. S. Shen, T. R. Gadekallu, W. Wang, and K. Dev, "A privacy-enhanced retrieval technology for the cloud-assisted Internet of Things," *IEEE Trans. Ind. Informat.*, early access, Aug. 10, 2021, doi: 10.1109/TII.2021.3103547.
- [13] S. Sachdeva, B. Raina, and A. Sharma, "Analysis of digital forensic tools," *J. Comput. Theor. Nanosci.*, vol. 17, no. 6, pp. 2459–2467, 2020.
- [14] A. R. Javed, Z. Jalil, W. Zehra, T. R. Gadekallu, D. Y. Suh, and M. J. Piran, "A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions," *Eng. Appl. Artif. Intell.*, vol. 106, Nov. 2021, Art. no. 104456.
- [15] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digit. Invest.*, vol. 7, pp. S64–S73, Aug. 2010.
- [16] B. Carrier, *File System Forensic Analysis*. Reading, MA, USA: Addison-Wesley, 2005.
- [17] V. R. Ambhire and B. Meshram, "Digital forensic tools," *IOSR J. Eng.*, vol. 2, no. 3, pp. 392–398, 2012.
- [18] J. Dykstra and A. T. Sherman, "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform," *Digit. Invest.*, vol. 10, pp. S87–S95, Aug. 2013.
- [19] M. Lovanshi and P. Bansal, "Comparative study of digital forensic tools," in *Data, Engineering and Applications*. Springer, 2019, pp. 195–204.
- [20] S. Mohammed and R. Sridevi, "A survey on digital forensics phases, tools and challenges," in *Proc. ICCII*, 2020, p. 237.
- [21] M. A. Alsmirat, R. A. Al-Hussien, W. T. Al-Sarayrah, Y. Jararweh, and M. Etier, "Digital video forensics: A comprehensive survey," *Int. J. Adv. Intell. Paradigms*, vol. 15, no. 4, pp. 437–456, 2020.
- [22] H. Kaur and N. Jindal, "Image and video forensics: A critical survey," *Wireless Pers. Commun.*, vol. 112, pp. 1281–1302, Jan. 2020.
- [23] B. Salazar, "Survey on real time security mechanisms in network forensics," *Int. J. Comput. Appl.*, vol. 151, no. 2, pp. 1–4, 2016.
- [24] P. Purnaye and V. Kulkarni, "A comprehensive study of cloud forensics," *Arch. Comput. Methods Eng.*, vol. 29, pp. 33–46, Jan. 2022.
- [25] S. N. Joshi and G. R. Chillarge, "Secure log scheme for cloud forensics," in *Proc. 4th Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Oct. 2020, pp. 188–193.
- [26] S. Schleppehorst, K.-K. R. Choo, and N.-A. Le-Khac, "Digital forensic approaches for cloud service models: A survey," in *Cyber and Digital Forensic Investigations*. Springer, 2020, pp. 175–199.
- [27] A. Sawant, A. Vanjari, S. Sahare, and S. Wasade, "A survey on cyber forensics for securing cloud logs," *Int. J. Sci. Res. Eng. Develop.*, vol. 3, no. 1, pp. 1–4, 2020.
- [28] U. Shukla, B. Mandal, and K. Kiran, "Perustration on mobile forensics tools," in *Computer Networks and Inventive Communication Technologies*. Springer, 2021, pp. 1225–1231.
- [29] M. Indhumathi, "Survey collection mobile hacking app and detection method," *IEICE Trans. Inf. Syst.*, vol. 7, no. 1, pp. 1–5, 2020.
- [30] S. Pawar, C. Bhusari, and S. Vaz, "Survey on digital forensics investigation and their evidences," *Int. J. Adv. Res. Sci., Commun. Technol.*, vol. 10, no. 1, pp. 1–7, 2020.
- [31] R. V. Mante and R. Khan, "A survey on video-based evidence analysis and digital forensic," in *Proc. 4th Int. Conf. Comput. Methodol. Commun. (ICCMC)*, Mar. 2020, pp. 118–121.

- [32] A. Case and G. G. Richard, III, "Memory forensics: The path forward," *Digit. Invest.*, vol. 20, pp. 23–33, Mar. 2017.
- [33] V. L. L. Thing, K.-Y. Ng, and E.-C. Chang, "Live memory forensics of mobile phones," *Digit. Invest.*, vol. 7, pp. S74–S82, Aug. 2010.
- [34] N. Ruff, "Windows memory forensics," *J. Comput. Virol.*, vol. 4, no. 2, pp. 83–100, May 2008.
- [35] A. Aljaedi, D. Lindskog, P. Zavarovsky, R. Ruhl, and F. Almari, "Comparative analysis of volatile memory forensics: Live response vs. memory imaging," in *Proc. IEEE 3rd Int. Conf. Privacy, Secur., Risk Trust IEEE 3rd Int. Conf. Social Comput.*, Oct. 2011, pp. 1253–1258.
- [36] J. Stüttgen, S. Vömel, and M. Denzel, "Acquisition and analysis of compromised firmware using memory forensics," *Digit. Invest.*, vol. 12, pp. S50–S60, Mar. 2015.
- [37] J. Sylve, A. Case, L. Marziale, and G. G. Richard, "Acquisition and analysis of volatile memory from Android devices," *Digit. Invest.*, vol. 8, nos. 3–4, pp. 175–184, 2012.
- [38] P. Feng, Q. Li, P. Zhang, and Z. Chen, "Private data acquisition method based on system-level data migration and volatile memory forensics for Android applications," *IEEE Access*, vol. 7, pp. 16695–16703, 2019.
- [39] R. P. Iyer, P. K. Atrey, G. Varshney, and M. Misra, "Email spoofing detection using volatile memory forensics," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2017, pp. 619–625.
- [40] N. R. Mistry and M. S. Dahiya, "Signature based volatile memory forensics: A detection based approach for analyzing sophisticated cyber attacks," *Int. J. Inf. Technol.*, vol. 11, no. 3, pp. 583–589, Sep. 2019.
- [41] J. Taylor, B. Turnbull, and G. Creech, "Volatile memory forensics acquisition efficacy: A comparative study towards analysing firmware-based rootkits," in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, pp. 1–11.
- [42] S. Rane and A. Dixit, "BlockSLaaS: Blockchain assisted secure logging-as-a-service for cloud forensics," in *Proc. Int. Conf. Secur. Privacy*. Springer, 2019, pp. 77–88.
- [43] J. Lian, "Implementation of computer network user behavior forensic analysis system based on speech data system log," *Int. J. Speech Technol.*, vol. 23, no. 3, pp. 559–567, Sep. 2020.
- [44] H. N. Noura, O. Salman, A. Chehab, and R. Couturier, "DistLog: A distributed logging scheme for IoT forensics," *Ad Hoc Netw.*, vol. 98, Mar. 2020, Art. no. 102061.
- [45] P. Chauhan and P. Bansal, "Assessment of forensics investigation methods," in *Intelligent Manufacturing and Energy Sustainability: Proceedings of ICIMES 2020*, vol. 213. Sparks, NV, USA: IEEE, 2021, p. 317.
- [46] K. Moffitt, U. Karabiyik, S. Hutchinson, and Y. H. Yoon, "Discord forensics: The logs keep growing," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2021, pp. 993–999.
- [47] T. R. Sree and S. M. S. Bhanu, "Data collection techniques for forensic investigation in cloud," in *Digital Forensic Science*. London, U.K.: IntechOpen, 2020.
- [48] O. F. Yakut and F. Ertam, "A digital forensics analysis for detection of the modified COVID-19 mobile application," in *Proc. 5th Int. Conf. Comput. Sci. Eng. (UBMK)*, Sep. 2020, pp. 1–5.
- [49] M. A. Wani, A. AlZahrani, and W. A. Bhat, "File system anti-forensics—Types, techniques and tools," *Comput. Fraud Secur.*, vol. 2020, no. 3, pp. 14–19, Jan. 2020.
- [50] T. Rochmadi, Y. Wicaksono, and N. D. Nisa, "Digital evidence identification of Android device using live forensics acquisition on cloud storage (iDrive)," *Int. J. Comput. Appl.*, vol. 175, no. 26, pp. 40–43, Oct. 2020.
- [51] H. H. Lwin, W. P. Aung, and K. K. Lin, "Comparative analysis of Android mobile forensics tools," in *Proc. IEEE Conf. Comput. Appl. (ICCA)*, Feb. 2020, pp. 1–6.
- [52] J. A. Mathews, G. P. George, and M. Dhanalakshmi, "Analysis of virtual machine in digital forensics," *Int. Res. J. Eng. Technol.*, vol. 7, no. 3, pp. 1–6, 2020.
- [53] D. Aju, A. K. Kakelli, A. S. Varma, and K. Rajendiran, "A comprehensive perspective on mobile forensics: Process, tools, and future trends," in *Confluence of AI, Machine, and Deep Learning in Cyber Forensics*. Hershey, PA, USA: IGI Global, 2021, pp. 1–28.
- [54] O. Setayeshfar, C. Adkins, M. Jones, K. H. Lee, and P. Doshi, "GrAALF: Supporting graphical analysis of audit logs for forensics," *Softw. Impacts*, vol. 8, May 2021, Art. no. 100068.
- [55] R. Duan and X. Zhang, "Research on computer forensics technology based on data recovery," *J. Phys., Conf. Ser.*, vol. 1648, no. 3, Oct. 2020, Art. no. 032025.
- [56] Y. V. Akay, "Computer forensics and cyber crime handling," *Jurnal Teknik Informatika*, vol. 15, no. 4, pp. 291–296, 2020.
- [57] G. R. Otieno and L. Dinga, "Legal issues in computer forensics and digital evidence admissibility," *Int. J. Comput. Sci. Mobile Comput.*, 2020.
- [58] A. Nieto, R. Rios, and J. Lopez, "IoT-forensics meets privacy: Towards cooperative digital investigations," *Sensors*, vol. 18, no. 2, p. 492, Feb. 2018.
- [59] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, "Internet of Things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Gener. Comput. Syst.*, vol. 92, pp. 265–275, Mar. 2019.
- [60] R. A. Kumar, M. V. Kumar, and R. Sreejith, "Privacy issues in cloud computing for computer forensics: An analysis," *Netw. Commun. Eng.*, vol. 10, no. 8, pp. 152–154, 2018.
- [61] A. Shalaginov, A. Iqbal, and J. Olegård, "IoT digital forensics readiness in the edge: A roadmap for acquiring digital evidences from intelligent smart applications," in *Proc. Int. Conf. Edge Comput.* Springer, 2020, pp. 1–17.
- [62] D. P. Joseph and J. Norman, "An analysis of digital forensics in cyber security," in *First International Conference on Artificial Intelligence and Cognitive Computing*. Springer, 2019, pp. 701–708.
- [63] F. Amato, A. Castiglione, G. Cozzolino, and F. Narducci, "A semantic-based methodology for digital forensics analysis," *J. Parallel Distrib. Comput.*, vol. 138, pp. 172–177, Apr. 2020.
- [64] D. Uroz and R. J. Rodríguez, "On challenges in verifying trusted executable files in memory forensics," *Forensic Sci. Int., Digit. Invest.*, vol. 32, Apr. 2020, Art. no. 300917.
- [65] B. Carrier and E. Spafford, "An event-based digital forensic investigation framework," *Digit. Invest.*, 2004.
- [66] L. Englbrecht and G. Pernul, "A privacy-aware digital forensics investigation in enterprises," in *Proc. 15th Int. Conf. Availability, Rel. Secur.*, Aug. 2020, pp. 1–10.
- [67] A. R. Javed and Z. Jalil, "Byte-level object identification for forensic investigation of digital images," in *Proc. Int. Conf. Cyber Warfare Secur. (ICCSWS)*, Oct. 2020, pp. 1–4.
- [68] C. M. da Silveira, R. T. de Sousa, Jr., R. de Oliveira Albuquerque, G. D. A. Nze, G. A. de Oliveira Júnior, A. L. S. Orozco, and L. J. G. Villalba, "Methodology for forensics data reconstruction on mobile devices with Android operating system applying in-system programming and combination firmware," *Appl. Sci.*, vol. 10, no. 12, p. 4231, Jun. 2020.
- [69] R. Komatwar and M. Kokare, "A survey on malware detection and classification," *J. Appl. Secur. Res.*, vol. 16, no. 3, pp. 390–420, Jul. 2021.
- [70] R. Kumars, M. Alazab, and W. Wang, "A survey of intelligent techniques for Android malware detection," in *Malware Analysis Using Artificial Intelligence and Deep Learning*. Springer, 2021, pp. 121–162.
- [71] M. A. Omer, S. R. M. Zeebaree, M. A. M. Sadeeq, B. W. Salim, S. X. Mohsin, Z. N. Rashid, and L. M. Haji, "Efficiency of malware detection in Android system: A survey," *Asian J. Res. Comput. Sci.*, vol. 7, pp. 59–69, Apr. 2021.
- [72] G. R. Panigrahi, N. K. Barpanda, and S. Mishra, "A review on: The rise in cyber forensics & innovations," EasyChair, Tech. Rep., 2021.
- [73] C. S. Şentürk, T. Apaydın, and H. Yaşar, "Image and file system support framework for a digital mobile forensics software," in *Proc. Turkish Nat. Softw. Eng. Symp. (UYMS)*, Oct. 2020, pp. 1–3.
- [74] F. Faust, A. Thierry, T. Müller, and F. Freiling, "Technical report: Selective imaging of file system data on live systems," 2020, *arXiv:2012.02573*.
- [75] Sudhakar and S. Kumar, "An emerging threat fileless malware: A survey and research challenges," *Cybersecurity*, vol. 3, no. 1, pp. 1–12, Dec. 2020.
- [76] L. F. Sikos, "Packet analysis for network forensics: A comprehensive survey," *Forensic Sci. Int., Digit. Invest.*, vol. 32, Mar. 2020, Art. no. 200892.
- [77] E. Nowroozi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, "A survey of machine learning techniques in adversarial image forensics," *Comput. Secur.*, vol. 100, Jan. 2021, Art. no. 102092.
- [78] R. Palutke, F. Block, P. Reichenberger, and D. Stripeika, "Hiding process memory via anti-forensic techniques," *Forensic Sci. Int., Digit. Invest.*, vol. 33, Jul. 2020, Art. no. 301012.
- [79] K. Hausknecht, D. Foit, and J. Burić, "RAM data significance in digital forensics," in *Proc. 38th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2015, pp. 1372–1375.

- [80] G. Varshney, P. Iyer, P. Atrey, and M. Misra, "Evading DoH via live memory forensics for phishing detection and content filtering," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2021, pp. 1–4.
- [81] G. B. Satrya and F. Kurniawan, "A novel Android memory forensics for discovering remnant data," *Int. J. Adv. Sci., Eng. Inf. Technol.*, vol. 10, no. 3, p. 6, 2020.
- [82] S. Talukder and Z. Talukder, "A survey on malware detection and analysis tools," *Int. J. Netw. Secur. Appl.*, vol. 12, no. 2, pp. 37–57, Mar. 2020.
- [83] R. Chiramdasu, G. Srivastava, S. Bhattacharya, P. K. Reddy, and T. R. Gadekallu, "Malicious URL detection using logistic regression," in *Proc. IEEE Int. Conf. Omni-Layer Intell. Syst. (COINS)*, Aug. 2021, pp. 1–6.
- [84] C. Rupa, G. Srivastava, S. Bhattacharya, P. Reddy, and T. R. Gadekallu, "A machine learning driven threat intelligence system for malicious URL detection," in *Proc. 16th Int. Conf. Availability, Rel. Secur.*, Aug. 2021, pp. 1–7.
- [85] R. Nelson, A. Shukla, and C. Smith, "Web browser forensics in Google Chrome, Mozilla Firefox, and the TOR browser bundle," in *Digital Forensic Education*. Springer, 2020, pp. 219–241.
- [86] R. U. Rahman and D. S. Tomar, "A new web forensic framework for bot crime investigation," *Forensic Sci. Int., Digit. Invest.*, vol. 33, Jun. 2020, Art. no. 300943.
- [87] N. Shafiq, "Forensic investigation of user's web activity on Google Chrome using various forensic tools," *Int. J. Comput. Sci. Netw. Secur.*, vol. 16, no. 9, pp. 123–132, 2016.
- [88] H. Adamu, A. A. Ahmad, A. Hassan, and S. B. Gambasha, "Web browser forensic tools: Autopsy, BHE and net analysis," *Int. J. Res. Innov. Appl. Sci.*, vol. 6, no. 5, pp. 103–107, 2021.
- [89] A. Ghafarian, "An empirical analysis of email forensics tools," Tech. Rep., 2020.
- [90] M. Alazab and R. Broadhurst, "Spam and criminal activity," in *Trends and Issues in Crime and Criminal Justice*, no. 526. Hershey, PA, USA: IGI Global, 2016, pp. 1–20.
- [91] M. Alazab and M. Tang, *Deep Learning Applications for Cyber Security*. Springer, 2019.
- [92] M. Z. Khan, M. S. Husain, and M. Shoaib, "Introduction to email, web, and message forensics," in *Critical Concepts, Standards, and Techniques in Cyber Forensics*. Hershey, PA, USA: IGI Global, 2020, pp. 174–186.
- [93] A. R. Javed, S. U. Rehman, M. U. Khan, M. Alazab, and G. T. Reddy, "CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1456–1466, Apr. 2021.
- [94] A. Mangino and E. Bou-Harb, "A multidimensional network forensics investigation of a state-sanctioned internet outage," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2021, pp. 813–818.
- [95] M. M. Alani, "OSI model," in *Guide to OSI and TCP/IP Models*. Springer, 2014, pp. 5–17.
- [96] C. Zeng, D. Zhu, Z. Wang, Z. Wang, N. Zhao, and L. He, "An end-to-end deep source recording device identification system for web media forensics," *Int. J. Web Inf. Syst.*, vol. 16, no. 4, pp. 413–425, Aug. 2020.
- [97] J. A. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: A booklet for beginners," *Multimedia Tools Appl.*, vol. 51, no. 1, pp. 133–162, Jan. 2011.
- [98] Y. Quan, C.-T. Li, Y. Zhou, and L. Li, "Warwick image forensics dataset for device fingerprinting in multimedia forensics," in *Proc. IEEE Int. Conf. Multimedia Expo (ICME)*, Jul. 2020, pp. 1–6.
- [99] H. Arshad, A. Jantan, G. K. Hoon, and I. O. Abiodun, "Formal knowledge model for online social network forensics," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101675.
- [100] K. Sitara and B. M. Mehtre, "Digital video tampering detection: An overview of passive techniques," *Digit. Invest.*, vol. 18, pp. 8–22, Sep. 2016.
- [101] L. Verdoliva, "Media forensics and DeepFakes: An overview," *IEEE J. Sel. Topics Signal Process.*, vol. 14, no. 5, pp. 910–932, Aug. 2020.
- [102] P. Mullan, "Digital cues in multimedia forensics," M.S. thesis, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Erlangen, Germany, 2021.
- [103] C. Pasquini, I. Amerini, and G. Boato, "Media forensics on social media platforms: A survey," *EURASIP J. Inf. Secur.*, vol. 2021, no. 1, pp. 1–19, Dec. 2021.
- [104] S. Kumar, B. K. Singh, and M. Yadav, "A recent survey on multimedia and database watermarking," *Multimedia Tools Appl.*, vol. 79, no. 27, pp. 20149–20197, 2020.
- [105] T. Thomas, M. Piscitelli, B. A. Nahar, and I. Baggili, "Duck hunt: Memory forensics of USB attack platforms," *Forensic Sci. Int., Digit. Invest.*, vol. 37, Jul. 2021, Art. no. 301190.
- [106] H. Alatawi, K. Alenazi, S. Alshehri, S. Alshamakh, M. Mustafa, and A. Aljaedi, "Mobile forensics: A review," in *Proc. Int. Conf. Comput. Inf. Technol. (ICCIT)*, Sep. 2020, pp. 1–6.
- [107] S. I. Imtiaz, S. U. Rehman, A. R. Javed, Z. Jalil, X. Liu, and W. S. Alnumay, "DeepAMD: Detection and identification of Android malware using high-efficient deep artificial neural network," *Future Gener. Comput. Syst.*, vol. 115, pp. 844–856, Feb. 2021.
- [108] C. Karagiannis and K. Vergidis, "Digital evidence and cloud forensics: Contemporary legal challenges and the power of disposal," *Information*, vol. 12, no. 5, p. 181, Apr. 2021.
- [109] V. K. Sanap and V. Mane, "Comparative study and simulation of digital forensic tools," *Int. J. Comput. Appl.*, vol. 975, p. 8887, 2015.
- [110] R. Ch. T. R. Gadekallu, M. H. Abidi, and A. Al-Ahmari, "Computational system to classify cyber crime offenses using machine learning," *Sustainability*, vol. 12, no. 10, p. 4087, May 2020.
- [111] W. A. Bhat, A. AlZahrani, and M. A. Wani, "Can computer forensic tools be trusted in digital investigations?" *Sci. Justice*, vol. 61, no. 2, pp. 198–203, Mar. 2021.
- [112] V. Fernando, "Cyber forensics tools: A review on mechanism and emerging challenges," in *Proc. 11th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Apr. 2021, pp. 1–7.
- [113] K.-N. Tran et al., "Towards a feature rich model for predicting spam emails containing malicious attachments and URLs," Austral. Comput. Soc., Darlinghurst, NSW, Australia, Tech. Rep., 2014.
- [114] S. U. Rehman, M. Khaliq, S. I. Imtiaz, A. Rasool, M. Shafiq, A. R. Javed, Z. Jalil, and A. K. Bashir, "DIDDOS: An approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU)," *Future Gener. Comput. Syst.*, vol. 118, pp. 453–466, May 2021.
- [115] A. Ghosh, K. Majumder, and D. De, "Android forensics using sleuth kit autopsy," in *Proceedings of the Sixth International Conference on Mathematics and Computing*. Springer, 2021, pp. 297–308.
- [116] J. Kävrestad, "Memory analysis tools," in *Fundamentals of Digital Forensics*. Springer, 2020, pp. 217–224.
- [117] 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, Apr. 2020, Art. no. 012034.
- [118] O. Skulkin and S. De Courcier, *Windows Forensics Cookbook*. Birmingham, U.K.: Packt, 2017.
- [119] C. Altheide and H. Carvey, *Digital Forensics With Open Source Tools*. Amsterdam, The Netherlands: Elsevier, 2011.
- [120] E. T. Harshany, "Distributed file system digital forensic triage integration," M.S. thesis, Univ. South Alabama, Mobile, AL, USA, 2020.
- [121] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *Int. J. Digit. Evidence*, vol. 1, no. 3, pp. 1–12, 2002.
- [122] P. Bajpai and R. Enbody, "Memory forensics against ransomware," in *Proc. Int. Conf. Cyber Secur. Protection Digit. Services (Cyber Security)*, Jun. 2020, pp. 1–8.
- [123] H. Kaur and G. Singh, "Volatile memory forensics: A legal perspective," *Int. J. Comput. Appl.*, vol. 155, no. 3, pp. 11–15, Dec. 2016.
- [124] S. Rahman and M. N. A. Khan, "Review of live forensic analysis techniques," *Int. J. Hybrid Inf. Technol.*, vol. 8, no. 2, pp. 379–388, 2015.
- [125] F. Shahzad, W. Iqbal, and F. S. Bokhari, "On the use of CryptDB for securing electronic health data in the cloud: A performance study," in *Proc. 17th Int. Conf. E-Health Netw., Appl. Services (HealthCom)*, Oct. 2015, pp. 120–125.
- [126] D. Muallfah and I. Riadi, "Network forensics for detecting flooding attack on web server," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 2, p. 326, 2017.
- [127] A. Varol and Y. Ü. Sönmez, "The importance of web activities for computer forensics," in *Proc. Int. Conf. Comput. Sci. Eng. (UBMK)*, Oct. 2017, pp. 66–71.
- [128] J. Luo and W. Xu, "The application research of electronic evidence system based on analysis of user correlative behavior," in *Proc. IEEE Workshop Adv. Res. Technol. Ind. Appl. (WARTIA)*, Sep. 2014, pp. 718–720.
- [129] D. Wu, "Empirical study of knowledge withholding in cyberspace: Integrating protection motivation theory and theory of reasoned behavior," *Comput. Hum. Behav.*, vol. 105, Apr. 2020, Art. no. 106229.
- [130] M. Babiker, E. Karaarslan, and Y. Hoscán, "Web application attack detection and forensics: A survey," in *Proc. 6th Int. Symp. Digit. Forensic Secur. (ISDFS)*, Mar. 2018, pp. 1–6.

- [131] M. Al-Zarouni, "Tracing e-mail headers," in *Proc. Austral. Comput., Netw. Inf. Forensics Conf.* Princeton, NJ, USA: Citeseer, 2004, pp. 16–30.
- [132] M. T. Bandy, "Techniques and tools for forensic investigation of e-mail," *Int. J. Netw. Secur. Appl.*, vol. 3, no. 6, p. 227, 2011.
- [133] A. Naem, A. R. Javed, M. Rizwan, S. Abbas, J. C.-W. Lin, and T. R. Gadekallu, "DARE-SEP: A hybrid approach of distance aware residual energy-efficient SEP for WSN," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 2, pp. 611–621, Jun. 2021.
- [134] S. Khan, A. Gani, A. W. A. Wahab, M. Shiraz, and I. Ahmad, "Network forensics: Review, taxonomy, and open challenges," *J. Netw. Comput. Appl.*, vol. 66, pp. 214–235, May 2016.
- [135] C. Easttom and M. Adda, "Application of the spectra of graphs in network forensics," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2021, pp. 846–852.
- [136] M. Mittal, C. Iwendi, S. Khan, and A. Rehman Javed, "Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg–Marquardt neural network and gated recurrent unit for intrusion detection system," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, Jun. 2021, Art. no. e3997.
- [137] S. Bhattacharya, S. S. R. Krishnan, P. K. R. Maddikunta, R. Kaluri, S. Singh, T. R. Gadekallu, M. Alazab, and U. Tariq, "A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU," *Electronics*, vol. 9, no. 2, p. 219, Jan. 2020.
- [138] R. M. S. Priya, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, and M. Alazab, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Comput. Commun.*, vol. 160, pp. 139–149, Jul. 2020.
- [139] G. Srivastava, G. T. Reddy, N. Deepa, B. Prabadevi, and M. P. K. Reddy, "An ensemble model for intrusion detection in the internet of softwareized things," in *Proc. Adjunct Proc. Int. Conf. Distrib. Comput. Netw.*, Jan. 2021, pp. 25–30.
- [140] H. N. F. Cantanhede and S. B. Vale, "Computer network forensics assistance methodology focused on denial of service attacks," *Int. J. Comput. Appl.*, vol. 177, no. 33, pp. 1–11, 2020.
- [141] G. Shrivastava, K. Sharma, and R. Kumari, "Network forensics: Today and tomorrow," in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, 2016, pp. 2234–2238.
- [142] A. Abbasi, A. R. Javed, C. Chakraborty, J. Nebhen, W. Zehra, and Z. Jalil, "ElStream: An ensemble learning approach for concept drift detection in dynamic social big data stream learning," *IEEE Access*, vol. 9, pp. 66408–66419, 2021.
- [143] S. Mashhadani, H. Al-kawaz, N. Clarke, S. Furnell, and F. Li, "A novel multimedia-forensic analysis tool (M-FAT)," in *Proc. 12th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2017, pp. 388–395.
- [144] C. Iwendi, S. U. Rehman, A. R. Javed, S. Khan, and G. Srivastava, "Sustainable security for the Internet of Things using artificial intelligence architectures," *ACM Trans. Internet Technol.*, vol. 21, no. 3, pp. 1–22, Jun. 2021.
- [145] A. R. Javed, S. U. Rehman, M. U. Khan, M. Alazab, and H. U. Khan, "Betalogger: Smartphone sensor-based side-channel attack detection and text inference using language modeling and dense multilayer neural network," *ACM Trans. Asian Low-Resour. Lang. Inf. Process.*, vol. 20, no. 5, pp. 1–17, Sep. 2021.
- [146] S. Afzal, M. Asim, A. R. Javed, M. O. Beg, and T. Baker, "URLdeep-Detect: A deep learning approach for detecting malicious URLs using semantic vector models," *J. Netw. Syst. Manage.*, vol. 29, no. 3, pp. 1–27, Mar. 2021.
- [147] F. Iqbal, R. Batool, B. C. M. Fung, S. Aleem, A. Abbasi, and A. R. Javed, "Toward tweet-mining framework for extracting terrorist attack-related information and reporting," *IEEE Access*, vol. 9, pp. 115535–115547, 2021.
- [148] W. Ahmed, A. Rasool, A. R. Javed, N. Kumar, T. R. Gadekallu, Z. Jalil, and N. Kryvinska, "Security in next generation mobile payment systems: A comprehensive survey," *IEEE Access*, vol. 9, pp. 115932–115950, 2021.
- [149] S. Iqbal and S. A. Alharbi, "Advancing automation in digital forensic investigations using machine learning forensics," in *Digital Forensic Science*. London, U.K.: IntechOpen, 2019.
- [150] M. M. Karakoç and A. Varol, "Visual and auditory analysis methods for speaker recognition in digital forensic," in *Proc. Int. Conf. Comput. Sci. Eng. (UBMK)*, Oct. 2017, pp. 1113–1116.
- [151] M. Shabbir, A. Shabbir, C. Iwendi, A. R. Javed, M. Rizwan, N. Herencsar, and J. C.-W. Lin, "Enhancing security of health information using modular encryption standard in mobile cloud computing," *IEEE Access*, vol. 9, pp. 8820–8834, 2021.
- [152] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, Jan. 2021.
- [153] A. Muhammad, M. Asad, and A. R. Javed, "Robust early stage botnet detection using machine learning," in *Proc. Int. Conf. Cyber Warfare Secur. (ICWS)*, Oct. 2020, pp. 1–6.



ABDUL REHMAN JAVED (Member, IEEE)

received the master's degree in computer science from the FAST National University of Computer and Emerging Sciences, Islamabad, Pakistan. He has worked with the National Cybercrimes and Forensics Laboratory, Air University, Islamabad, where he is a Lecturer at the Department of Cyber Security. He is a cybersecurity researcher and practitioner with industry and academic experience. He has reviewed over 150 scientific research

articles for various well-known journals including, *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, *Computer and Electrical Engineering* (Elsevier), *Sustainable Cities and Society* (Elsevier), *Journal of Information Security and Applications* (Elsevier), *IEEE Internet of Things Magazine*, *IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING*, *Transactions on Internet Technology* (ACM), *Telecommunication Systems* (Springer), *IEEE ACCESS*, and *International Journal of Ad Hoc and Ubiquitous Computing* (Inderscience). He has authored over 50 peer-reviewed research articles. He is supervising/co-supervising several graduate (B.S. and M.S.) students on topics related to health informatics, cybersecurity, mobile computing, and digital forensics. His current research interests include but are not limited to mobile and ubiquitous computing, data analysis, knowledge discovery, data mining, natural language processing, smart homes, and their applications in human activity analysis, human motion analysis, and e-health. He aims to contribute to interdisciplinary research of computer science and human-related disciplines. He is an ACM Member. He is a TPC Member of CID2021 (Fourth International Workshop on Cybercrime Investigation and Digital forensics—CID2021) and the 44th International Conference on Telecommunications and Signal Processing. He has served as a Moderator for the 1st IEEE International Conference on Cyber Warfare and Security (ICWS).



WAQAS AHMED is currently pursuing the Ph.D.

degree with the Department of Cyber Security, Air University, Islamabad, Pakistan. His research interests include machine learning, wireless sensor networks, mobile computing, and security issues in mobile cloud computing.



MAMOUN ALAZAB (Senior Member, IEEE) received the Ph.D. degree in computer science from the School of Science, Information Technology and Engineering, Federation University Australia. He is an Associate Professor at the College of Engineering, IT, and Environment, Charles Darwin University, Australia. He is a cyber security researcher and practitioner with industry and academic experience. His research is multidisciplinary and focuses on cyber security and digital forensics of computer systems, including current and emerging issues in the cyber environment like cyber-physical systems and the Internet of Things, by considering the unique challenges present in these environments a focus on cybercrime detection and prevention. His look into the intersection use of artificial intelligence and machine learning as essential tools for cybersecurity, for example, detecting attacks, analyzing malicious code, or uncovering vulnerabilities in software and hardware.



KASHIF KIFAYAT received the Ph.D. degree in cyber security from Liverpool John Moores University, Liverpool, U.K., in 2008. He is currently a Professor and the Chair of the Cyber Security Department, Air University, Islamabad, Pakistan. Prior to this, he worked as a reader in cyber security at Liverpool John Moores University. He has published over 90 articles in international conference proceedings and journals and served in several conferences, IPCs, and journal editorial boards. His research interests include network security, security of complex systems, risk analysis, intrusion detection systems, digital forensics, secure service composition, privacy-preserving data aggregation, cryptography, computer forensics, and the IoT security. He has also played a key role in many funded research and development projects related to his research topics.



ZUNERA JALIL (Member, IEEE) received the master's degree in computer science, in 2007, with a scholarship from the Higher Education Commission of Pakistan, and the Ph.D. degree in computer science from the FAST National University of Computer and Emerging Sciences, Islamabad, Pakistan, in 2010, with specialization in information security. She is an Assistant Professor at the Department of Cyber Security, Faculty of Computing and Artificial Intelligence, Air University, Islamabad, and a Senior Researcher at the National Cybercrimes and Forensics Laboratory, National Center for Cyber Security, Islamabad. She has served as a full-time Faculty Member at the International Islamic University, Islamabad; Iqra University, Islamabad; and Saudi Electronic University, Riyadh, Saudi Arabia. Her research interests include but are not limited to computer forensics, machine learning, criminal profiling, software watermarking, intelligent systems, and data privacy protection.



THIPPA REDDY GADEKALLU (Senior Member, IEEE) received the B.Tech. degree in CSE from Acharya Nagarjuna University, India, the M.Tech. degree in CSE from Anna University, Chennai, Tamil Nadu, India, and the Ph.D. degree from the Vellore Institute of Technology (VIT), Vellore, Tamil Nadu. He has more than 14 years of experience in teaching. He is currently working as an Associate Professor with the School of Information Technology and Engineering, VIT. He has published more than 50 international/national publications. His research interests include machine learning, the Internet of Things, deep neural networks, blockchain, and computer vision.

• • •