An-Najah University Journal for Research – A
Natural Sciences

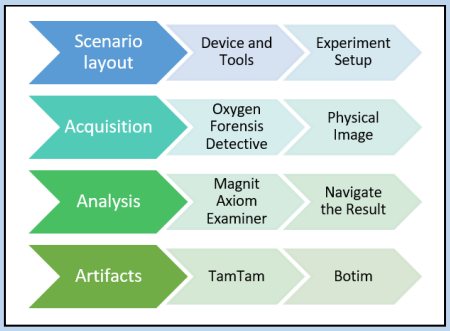
Mobile Forensics Analysis for Instant Messaging Applications Namely TamTam and Botim

Alsharif H. Aburbeian [1,*], Majdi Owda[2] & Amani Y. Owda[1,3]

Received: 17th Sep. 2023, Accepted: 4th Oct. 2024, Published: ××××, DOI: https://doi.org/10.xxxx

Accepted Manuscript, In press

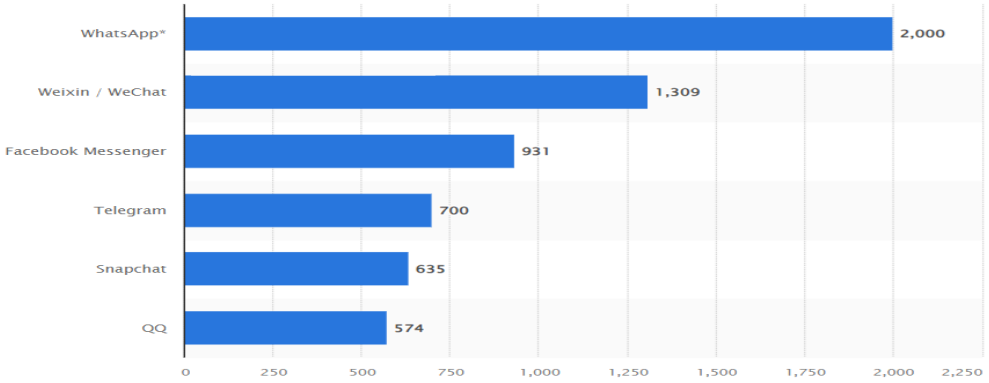
Abstract: Cybercrimes are rapidly increasing in parallel with the usage of digital tools. Criminals can use many methods to carry out their crimes such as mobile phones and instant messaging applications. Because of that, it is important to investigate the ability to retrieve evidence from mobiles that may be involved in cybercrime. This research aims to perform a mobile forensic analysis to retrieve evidence from specific instant messaging applications. To this end, an experiment was conducted to mimic the scene of illegal messages, delete them, and investigate the ability to retrieve deleted files. According to the result, this research successfully obtained text messages, multimedia data, and contact lists. The research's novelty can be derived from its ability to retrieve deleted data, demonstrating the feasibility of retrieving evidence from instant messaging applications that have not been investigated before. In future work, analyzing these applications under other operating system platforms may offer valuable artifacts for investigators.



Keywords: Cybercrime, digital forensics, mobile forensics, physical acquisition, artifacts.

Introduction

Criminals are increasingly turning to technology to carry out their nefarious activities. From cyberattacks on businesses and governments to online harassment of individuals, digital crime is a growing problem that requires sophisticated solutions [1]. Many solutions are offered by researchers to fight against digital crimes such as using machine learning [2], and digital forensics [3]. The process of gathering, analyzing, and preserving digital evidence for use in court cases is known as "digital forensics." [4]. Young users are encouraged to use new technologies [5], which may lead to misuse. Instant messaging (IM) applications are widely used for communication on mobile devices; see Figure (**1**. Such applications have completely changed the way we interact. Users may now participate in real-time, multimedia-rich conversations anywhere in the world utilizing these tools, which go beyond the limitations of traditional text messages and voice calls. In a time when information is shared quickly, apps like TamTam and Botim have become essential resources for millions of users, they perfectly capture the ever-changing world of instant messaging, where users prioritize simplicity, privacy, and the smooth integration of different media formats. These applications contain valuable data that can be relevant to criminal investigations. For example, IM apps may store chat logs, multimedia files, geolocation data, and other information that can be used to build a case against a suspect [6].



1 Department of Natural, Engineering and Technology Sciences, Arab American University, Ramallah, Palestine
*Corresponding author: a.aburbeian@student.aaup.edu
2 Faculty of Artificial Intelligence and Data Science, UNESCO Chair in Data Science for Sustainable Development, Arab American University, Ramallah, Palestine. majdi.owda@aaup.edu
3 E-mail: amani.owda@aaup.edu

Figure (1): Based on monthly active users (in millions), the most widely used mobile chat apps worldwide [57]

This research focuses on two specific IM applications (TamTam and Botim) and explores the digital artifacts that can be retrieved from these applications on the Android operating system. As mentioned before, IM applications have become a critical source of evidence in cybercrime investigations, and forensic investigators require reliable and effective methods to retrieve artifacts from these applications. Because of that, this study aims to perform digital forensics analysis for TamTam and Botim instant messaging applications and investigate the ability to retrieve artifacts under the Android operating system.

The research aimed to achieve the following goals: -

1. Analyze application integration for forensic analysis: examine how well the Galaxy J7 Prime's TamTam and Botim applications integrate and function to decide whether or not they are appropriate for retrieving forensic evidence.
2. Perform device acquisition for evidence retrieval: in the context of a forensic investigation, carry out a thorough physical acquisition of the mobile phone to gather all relevant information, including system files, application data, and user-generated content.
3. Extract and examine forensic artifacts: from the obtained device data, locate, extract, and examine digital artifacts associated with the IM applications, placing special emphasis on the recovery of text messages, multimedia files, and logs that could be used as forensic evidence.
4. Examine the Possibility of Data Recovery: Determine if it is possible to retrieve data that has been destroyed, particularly from the TamTam and Botim applications. This assessment should consider the consequences of forensic inquiries and the retrieval of data that has been purposefully deleted.

The remainder of the paper is structured as follows: Section 2 describes the present related studies' results. Section 3 describes the methodology and development for conducting the forensics analysis. Section 4 draws the paper's overall conclusions.

Literature Review

This section presents an overview of TamTam and Botim applications, a definition of mobile forensics, a general overview of the mobile devices' data acquisition techniques and challenges utilized by digital forensic investigators, and lastly, a discussion about related studies in the field will be provided.

TamTam and Botim Applications

TamTam is a free messenger that can be used on both mobiles and PCs. TamTam offers different capabilities such: as channels, video calls, voice calls, and geolocation services. Botim is another free messenger application working on both mobiles and PCs, using Botim will make you able to send and receive images, and text messages. Perform video, audio calls, and group chats [7–9].

Mobile Forensics

Retrieval of electronic evidence from mobiles under regulated and appropriate investigative scientific circumstances is known as mobile forensics. [10]. This branch has become essential as a result of the expanding need for mobile-based services, an increase in users, and sporadic improvements in mobile technologies like accessibility and widespread as well as the quickly developing Internet of Things (IoT) technology, which requires device connectivity. [11].

Challenges of Acquiring Mobile Phones

Because of the rising variability of mobile operating systems and their supporting features, mobile forensics is inherently interdisciplinary and challenging. In addition to legacy phones with core features and smartphones, Information obtained from a variety of digital electronic devices, including personal digital assistants (PDAs), tablets, and navigation systems is included in mobile forensics. The development of mobile forensics is being influenced by complex systems, the appearance of new types of devices, and the mounting pressure on device manufacturers to build more sophisticated safety features for their products, making the gathering of evidence more challenging [12].

Mobile Devices Data Acquisition Techniques

Acquiring data from mobile devices can be achieved using one of two main ways, logical acquisition, and physical acquisition [13]. It may be possible to obtain a logical copy of the device without having to root it, and this method can deliver virtual files of the data that is kept in the memory., whereas the physical version may require rooting the device which may cause problems [14]. The investigator must be aware of forensics tools to choose the most appropriate instrument for each case. In certain circumstances, investigators just need specific and significant data. In some cases, however, complete extraction of the mobile device's physical memory and internal storage files is necessary to recover erased data and conduct a thorough forensic examination [15].

Used Forensic Analysis Tools

Magnet AXIOM and Oxygen Forensic Detective were used to perform the analysis in this research. Both tools are considered essential tools in the field of digital forensic analysis, each of which provides a wide range of potent features designed to satisfy the complicated needs of forensic investigations. Call logs, text messages, multimedia material, and geolocation data are just a few of the many types of digital data that Oxygen Forensic Detective may collect, decode, and analyze. Its ability to adapt to a variety of platforms and devices, which lets investigators follow a complete digital trail, is what makes it so strong [16]. Similarly, Magnet AXIOM is excellent at recovering artifacts and obtaining data from cloud accounts, mobile phones, and PCs. It is distinguished by the smooth integration and correlation of data it offers, giving investigators a thorough picture of a subject's digital activity. These technologies' simple graphical user interfaces, sophisticated search features, and effective reporting tools make the normally difficult work of gathering and analyzing information easier. It makes sense to use Oxygen Forensic Detective and Magnet AXIOM because they may speed the examination of digital evidence, and improve the effectiveness of investigations [17,18].

Related Work

Many studies in the literature performed a forensic analysis for instant messaging (IM) applications. Some of these studies investigated the ability to retrieve artifacts from different applications under the IOS operating system [19–22], windows platform [23–30], and Android operating system. As soon as this study performs the forensic analysis under the Android operating system, we will discuss some studies in the Android environment.

The study of [31], analyzed WhatsApp, WeChat, Viber, and Telegram applications. The study aimed to locate where the user data is stored in the mobile file system and show how these applications store data in the Android OS. In the end, they were able to retrieve some text messages only. The WeChat application's database file location is examined by [32]. The database files are recovered with the use of reverse engineering methods. However, with the latest version of the WeChat app, the methods employed and discussed in this research are no longer relevant. The Telegram artifacts are addressed in [33], however, the writers were unable to find the location of the conversation database storage. They just talk about the various conversation modes offered by Telegram and its level of security. The author of [34] goes into great depth about the forensically significant artifacts that Telegram Messenger stores. Their methods for reconstructing contact lists, text and non-textural communications, and voice call log files are also covered in the study. This paper was able to acquire the metadata information about the message details only, and the actual text communications could not be obtained.

The study of [35], performed a forensics analysis for Yahoo Messenger, and Google Talk, on iPhone devices, and they were able to retrieve the conversation log and passwords [36]. Analyzed WhatsApp, Viber, and Tango applications on Android mobiles and retrieved chat logs and history, sent and received multimedia files. The study of [37], conducted a forensics analysis for Telegram, Line, and Kakao talk messenger on Android OS, and they were able to retrieve private chat, secret chat, and hidden chat from them. [38], were able to retrieve account information and messages from the Instagram application on Android OS.

The mentioned studies were able to retrieve some artifacts from different applications but they do not illustrate what kind of data acquisition they performed for the analysis, and this is an important point when performing such an analysis. The normal thing for a cybercriminal is to delete files related to his crime. For example, in the case of electronic blackmail, the criminal deletes the conversation between him and the victim to erase any evidence proving his guilt. In this case, the forensic analysis will not make sense if not recover deleted files.

Some of the studies were able to retrieve metadata information about the message details only. Others were able to retrieve text messages. This research was able to retrieve text messages, contact lists, and multimedia messages successfully.

This will contribute to the body of knowledge by:

1. Offering a methodology to perform a forensics investigation for TamTam and Botim applications that may be used in cybercrimes.
2. Highlight the importance of performing the physical acquisition to retrieve deleted files.
3. A better understanding for forensic practitioners, law enforcement agencies, and policymakers about the tools involved in the investigation process.
4. Demonstrating the feasibility of retrieving evidence from TamTam and Botim applications.
5. Clarifies the significance of data safety and privacy due to the prevailing belief that deleting data from mobile phones will erase it forever and it can't be retrieved.

Materials and Methods

The general framework for conducting this study is illustrated in Figure (**2**.

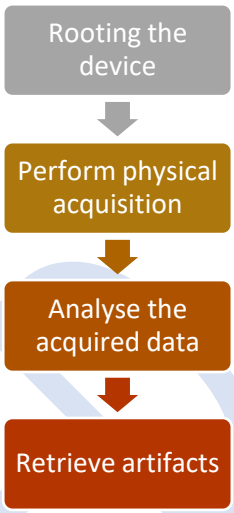


Figure (2): The general framework used in the study

As shown in Figure (**2**, the first step in the framework was rooting the device to gain elevated access to it. This gives the user full access to the internal functions of the device by allowing them to change system files and configurations. Then a physical acquisition was performed to gain all data including deleted ones. Then we analyze the acquired data and navigate the result to retrieve artifacts from the mentioned applications.

The methodology used in this paper consists of four phases which are: 1. The Experiment setup phase. 2. Acquisition phase. 3. Analysis phase. 4. Artifacts phase. In this section, we will discuss each phase separately. See Figure (**3**, which illustrates the methodology used to conduct this study.

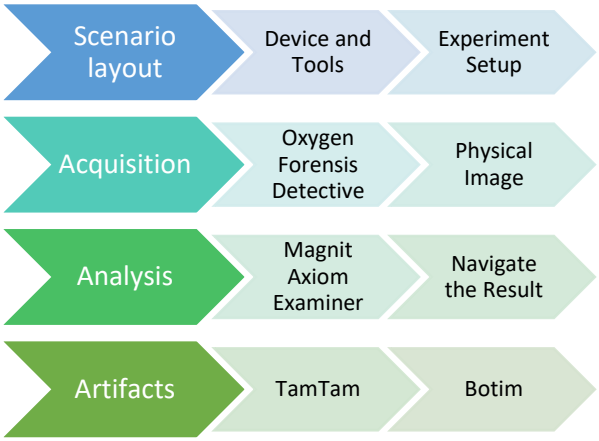


Figure (3). Methodology

As shown in Figure (**3**, our methodology consists of four steps which we will discuss in a separate section.

Scenario layout

In this phase, we perform an experiment to simulate a crime scenario in which the criminal uses an IM application for illegal purposes and then deletes the messages to dispose of the evidence. So, we install the mentioned applications on two mobile devices, sending and receiving messages and finally, we delete the messages and the applications.

Devices and Tools

To perform the forensics analysis, this paper uses different types of devices and software illustrated in

Table **1**.

Table 1. Tools and Devices used to perform forensics investigation

	Devices & Tools	Description
1	HP laptop Intel(R) Core (TM) i5	Perform the forensics analysis
2	USB cable	USB connector to connect mobile device and PC
3	Samsung Galaxy J7 Prime OS: Android version 8.1.0 Storage: 16 GB internal storage	Smart mobile to be analyzed
4	Samsung Galaxy A52s OS: Android version 12	Smart mobile For experiment setup
5	TamTam v2.29.1	Application
6	Botim v2.7.9	Application
7	Magnet axiom	Analysis tool
8	Oxygen forensic detective	Analysis tool

As shown in

Table **1**, this paper uses Galaxy J7 Prime and Galaxy A52s mobile phones to conduct experiments. Two different forensics tools were used; Oxygen forensics for acquisition and Magnet axiom for analysis, both tools were installed on an HP Core I5 laptop.

Experiment Setup

In this research, experimental work was performed as follows:

- Install the TamTam, and Botim applications from the Google Play Store on both devices Samsung Galaxy J7 Prime, and Samsung Galaxy A52s.
- Start using the application within both devices (adding numbers, contact list…etc.).
- Sending and receiving data between both devices (J7 Prime and A52s).
- Take a logical image of the Samsung Galaxy J7 Prime device (using the Magnet axiom process).
- Delete the conversation.
- Take a logical image of the Samsung Galaxy J7 Prime device again (using the Magnet axiom process).
- Take a physical image of the Samsung Galaxy J7 Prime device (using Oxygen Forensic Detective).
- Navigate the image to retrieve artifacts (using the Magnet axiom examine).

Acquisition

This research performed a physical acquisition technique using the Oxygen forensic detective tool. Oxygen Forensic Detective is a robust mobile forensic tool that combines powerful data extraction, analysis, and reporting capabilities. The tool supports both logical and physical extractions from a wide range of mobile phones, including smartphones and tablets running on different operating systems such as iOS, Android, and others. It can acquire data through various methods, including cable connections, wireless connections, and even through cloud backups. It assists investigators in uncovering and analyzing mobile data to analyze it and aid in the successful conclusion of crime investigations.

Analysis

The analysis was performed using the Magnet axiom tool. Magnet AXIOM is a preferred choice in mobile forensics due to its comprehensive device support, powerful analysis features, recovery tools, and collaborative functionalities. It empowers investigators to efficiently collect and analyze digital evidence, aiding in the successful resolution of cybercrime cases and facilitating efficient reporting and collaboration among investigators. It enables the creation of detailed reports with customizable templates, annotations, and bookmarks, making it easier to present findings and collaborate with other forensic professionals.

Results and Discussion

The experiment conducted in this research yielded significant findings in the domain of mobile forensic analysis. Through an examination of the TamTam and Botim applications on the Galaxy J7 Prime, various data artifacts were successfully retrieved. These artifacts included text messages, multimedia files, and contact lists, demonstrating the applications' potential as sources of forensic evidence. Notably, the research also explored the feasibility of recovering deleted data, and the results indicated a promising ability to retrieve information that had been intentionally erased by the user.

Because the aim of the study, research is concerned with searching for TamTam, and Botim artifacts in the internal storage of the device, we will highlight the artifacts related to them only.

TamTam Application Artifacts

The forensic analysis of the TamTam application revealed critical data storage locations within the device. Messages and contacts associated with the TamTam application were identified and recovered from the file path userdata.bin - Entire Disk (EXT-family, 11.24 GB)\data\ru.ok.messages\databases\cache.db (see Figure 4). This discovery is significant as it demonstrates that even after users attempt to delete their communication history, residual data can still be retrieved from the device.

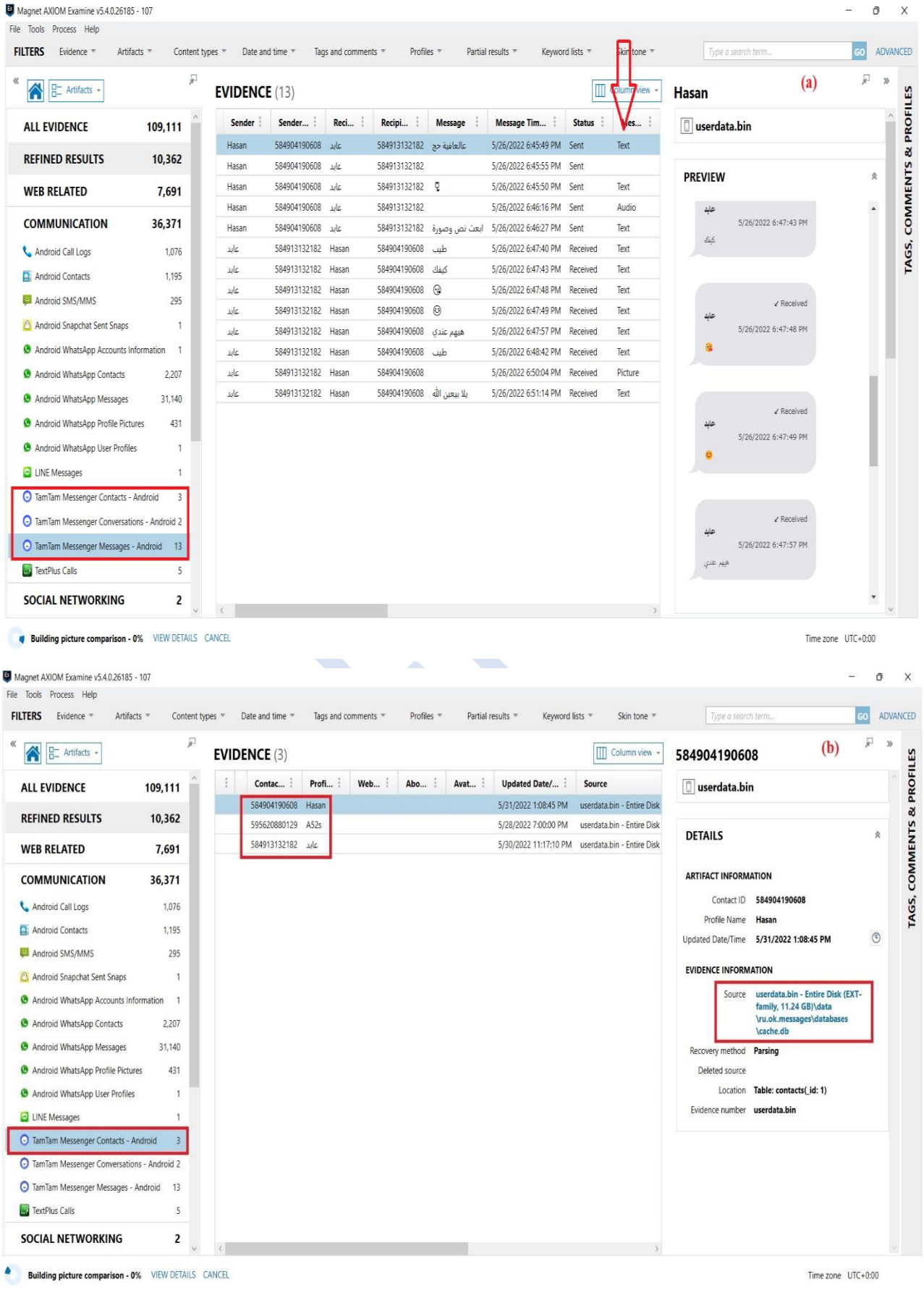


Figure (4): TamTam Artifacts; **a)** TamTam messages. **b)** TamTam contact list.

As illustrated in (Figure 4, a), the messages that were sent using the TamTam application were successfully retrieved post-deletion. This finding is crucial for forensic investigations, as it indicates that vital communication evidence can be preserved despite deliberate erasure by users. Furthermore, (Figure 4, b) displays the recovered contact list from the application, which, in this experiment, contained the three contacts that were saved during the setup phase. This reinforces the capability of forensic tools to recover essential user data even in scenarios where the application has been partially or fully uninstalled.

Botim Application Artifacts

Similarly, the analysis of the Botim application revealed key storage paths and data structures within the device's internal storage. The data relating to the Botim application was found in the directory "media\0\Android\data\im.thebot.messenger\files", as shown in Figure 5. This directory contained various artifacts, including log files, media files, and hex files, all of which are of potential interest in a forensic investigation.

Particularly noteworthy is the recovery of photo messages, which were retrieved after the user had deleted them. These images were stored in the path "userdata.bin - Entire Disk (EXT-family,11.24GB)\media\0\Android\data\im.thebot.messenger \files\Media\BOT\Images\8363ec9e88141127b8241ec1883ff96 b.jpg". The ability to recover such media files is particularly important in cases where visual evidence plays a critical role in the investigation.

Because forensic tools are sensitive and security-related, Oxygen Forensic Detective and Magnet AXIOM use proprietary techniques and approaches that they do not publicly publish. To recover erased data, digital forensics programs frequently combine different methodologies, which can differ throughout solutions. However, these are the popular methods for recovering erased data in the field of digital forensics: -

1. File Carving: File carving is a technique used to recover files based on their headers, footers, and internal data structures. Even if a file has been deleted, remnants of its data may still exist on the storage medium. Forensic tools can identify these remnants and reconstruct deleted files.

2. Journaling and Logging: Many file systems maintain a journal or log that records changes made to the file system, including file creations, modifications, and deletions. Forensic tools can analyze these logs to reconstruct the history of file operations and recover deleted files.

3. Unused Space Analysis: When a file is deleted, the space it occupies on the storage medium is marked as "free" or "unused." Forensic tools can scan the unused space to identify and recover fragments of deleted files.

4. Metadata Analysis: File metadata, such as timestamps and file attributes, can provide valuable information about the existence and characteristics of deleted files. Forensic tools often analyze metadata to reconstruct the timeline of file activities [39,40].

Overall, the results of this study underscore the importance of thorough forensic analysis in mobile investigations. The successful recovery of deleted data from both TamTam and Botim applications highlights the potential for obtaining crucial evidence from instant messaging platforms that have not been widely studied before. These findings contribute to the growing body of knowledge in mobile forensics, offering new insights and methodologies for future investigation.

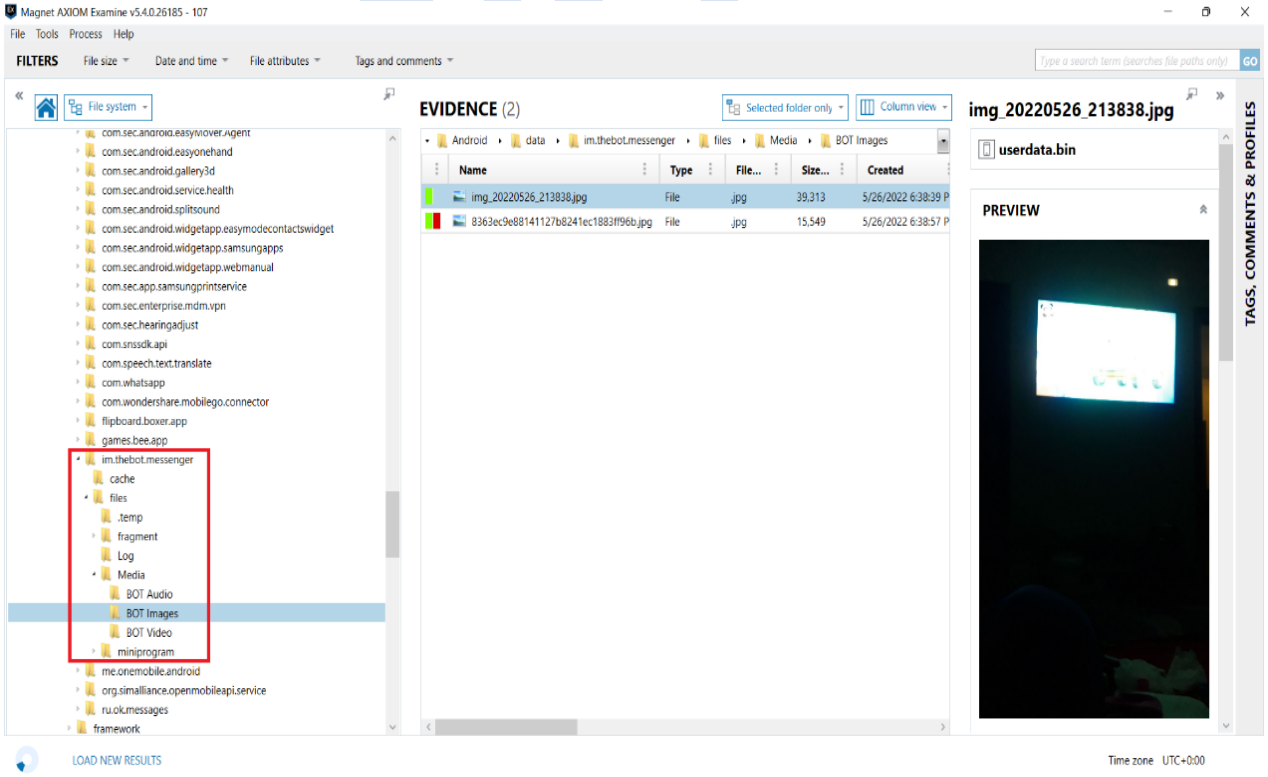


Figure (5): Botim Application Artifacts.

Conclusion

This study performed a forensics analysis for instant messaging applications that have not been discussed before in the literature namely; TamTam, and Botim applications. This study was investigated using the Oxygen Forensic Detective tool. A physical analysis was employed to retrieve artifacts related to the mentioned applications from an Android mobile phone (J7 Prime). The findings of the study were: - First, the authors were able to retrieve text messages, photos, voice messages, and contact lists from the TamTam application. Second, the multimedia files within the Botim application were retrieved. The results of the present study do not conflict with the general framework of the instant messaging forensics studies in the field [41–47]; [48–56] The limitations of the study were as follows: First, finding a suitable forensics tool was hard, because of the varied number of mobile types, software, and applications of anti-forensics techniques. Second, time limitations. In future work, the analysis of mentioned applications on PCs (Windows or MAC operating systems) may offer additional information for investigators in the forensics field.

Ethics approval and consent to participate

Not applicable

Consent for publication

Not applicable

Availability of data and materials

The study team gathered the information utilized in this article, and it will be provided to additional researchers upon request.

Author's contribution

The authors confirm their contribution to the paper as follows: study conception and design: Aburbeian, A.H, Owda, M and Owda, A; theoretical calculations and modeling: Aburbeian, A.H and Owda, M; data analysis and validation, Aburbeian, A.H, Owda, M and Owda, A; draft manuscript preparation: Aburbeian, A.H, Owda, M and Owda, A. All authors reviewed the results and approved the final version of the manuscript.

Funding

This research received no external funding.

Conflicts of interest

The authors declare no conflict of interest.

References

1] Iqbal F, Ahmed W, Shahzad F, Javed AR, Ali L. Whatsapp network forensics: Discovering the ip addresses of suspects. ieeexplore.ieee.orgW Ahmed, F Shahzad, AR Javed, F Iqbal, L Ali11 2021th IFIP International Conference on New Technologies, 2021•ieeexplore.ieee.org. 2021.

2] Aburbeian AM, Ashqar HI. Credit Card Fraud Detection Using Enhanced Random Forest Classifier for Imbalanced Data. In: Lecture Notes in Networks and Systems In the Proceedings of the 2023 International Conference on Advances in Computing Research (ACR'23) Springer, Cham. Orlando, USA: Springer, Cham; 2023; p. 605–16.

3] Aburbeian AM, Owda M, Owda AY. Digital Forensic Analysis of Hologram Projection Fans. 2023 International Conference on Information Technology (ICIT). 2023 Aug 9; 7–12.

4] Das P, Sarkar P. The Importance of Digital Forensics in the Admissibility of Digital Evidence. NUJS Journal of Regulatory Studies. 2022.

5] Aburbeian AM, Owda AY, Owda M. A Technology Acceptance Model Survey of the Metaverse Prospects. AI 2022, Vol 3, Pages 285-302. 2022 Apr 11.

6] Bawankar L, Bongirwar M, Sharma P, Bhojane S, Mangrulkar N. Android Forensic Tool. In: Lecture Notes in Electrical Engineering. Springer Science and Business Media Deutschland GmbH; 2022. p. 709–16.

7] Li J, Cheng G, Chen Z, Zhao P. Protocol clustering of unknown traffic based on embedding of protocol specification. Comput Secur. 2024 Jan 1; 136:103575.

8] Weimann G, Pack A. TamTam: The Online Drums of Hate. Studies in Conflict & Terrorism. 2023. [Available from: https://www.tandfonline.com/doi/abs/10.1080/1057610X.2023.2225275]

9] Botim T. Botim. 2023. BOTIM - Free, Secure & Reliable Messages and Calls. [Available from: https://botim.me/home/]

10] Riadi I, Firdonsyah A. Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. Article in International Journal of Computer Science and Information Security. 2017.

11] Al-Dhaqm A, Razak SA, Ikuesan RA, Kebande VR, Siddique K. A review of mobile forensic investigation process models. IEEE Access. 2020; 8:173359–75.

12] Alatawi H, Alenazi K, Alshehri S, Alshamakhi S, Mustafa M, Aljaedi A. Mobile Forensics: A Review. 2020 International Conference on Computing and Information Technology, ICCIT 2020.

13] Lee LH, Zhu Y, Yau YP, Braud T, Su X, Hui P. One-thumb Text Acquisition on Force-assisted Miniature Interfaces for Mobile Headsets. 18th Annual IEEE International Conference on Pervasive Computing and Communications, PerCom 2020.

14] Martinelli L, Foti F, Perotti F, Cucchi M. Floor vibrations from data acquisition with android phones. J Phys Conf Ser. 2024 Jun 1;2647(13):132006.

15] Xue L, Qian C, Zhou H, Luo X, Zhou Y, Shao Y, et al. NDroid: Toward tracking information flows across multiple android contexts. IEEE Transactions on Information Forensics and Security. 2019 Mar 1;14(3):814–28.

16] Muhammed Mahdi Salih K, Badi Ibrahim N. Digital Forensic Tools: A Literature Review. Journal of Education and Science. 2023;32(01):202–5.

17] Cristina Barrilari C, Greco Filho V, Ricardo Marcondes Ramos J, Guilherme Müller Kurban Brunno Ruschel de Lia Pires P, Ferreira de Albuquerque Costa R, Antonio Borri Rafael Junior Soares L, et al. DIGITAL FORENSICS TOOLS: DEVELOPMENT AND CONCERNS IN THE CONTEXT OF LAW ENFORCEMENT. ibccrim.org.brJRM RamosBoletim•ibccrim.org.br. 2022.

18] Strandberg K, Nowdehi N, Olovsson T. A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection. IEEE Transactions on Intelligent Vehicles. 2023 Feb 1;8(2):1350–67.

19] Sgaras C, Kechadi MT, Le-Khac NA. Forensics acquisition and analysis of instant messaging and VoIP applications. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2015; 8915:188–99.

20] Ovens KM, Morison G. Forensic analysis of Kik messenger on iOS devices. Digit Investig. 2016 Jun 1; 17:40–52.

21] Salamh FE, Mirza MM, Hutchinson S, Yoon YH, Karabiyik U. What's on the horizon? An in-depth forensic analysis of android and iOS applications. IEEE Access. 2021; 9:99421–54.

22] Jadhav Bhatt A, Gupta C, Mittal S. Network Forensics Analysis of iOS Social Networking and Messaging Apps. 2018 11th International Conference on Contemporary Computing, IC3 2018. 2018 Nov 9;

23] Salem Y, Owda M, Owda AY. An experimental approach for locating WhatsApp digital forensics artefacts on Windows 10 and the cloud. International Journal of Electronic Security and Digital Forensics. 2023;15(3):281–300.

24] Febrian FF, Sidabutar J. Comparative Analysis of Forensic for Whatsapp Desktop on Mac OS and Windows Using IDFIF V2. 2023

IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs). 2023 Aug 22; 327–31.
25] Bowling H, Seigfried-Spellar K, Karabiyik U, Rogers M. We are meeting on Microsoft Teams: Forensic analysis in Windows, Android, and iOS operating systems. J Forensic Sci. 2023 Mar 1; 68(2):434–60.
26] Fernández-Álvarez P, Rodríguez RJ. Extraction and analysis of retrievable memory artifacts from Windows Telegram Desktop application. Forensic Science International: Digital Investigation. 2022 Apr 1; 40:301342.
27] Bowling H, Seigfried-Spellar K, Karabiyik U, Rogers M. We are meeting on Microsoft Teams: Forensic analysis in Windows, Android, and iOS operating systems. J Forensic Sci. 2023 Mar 1; 68(2):434–60.
28] Ababneh A, Awwad MA, Al-Saleh MI. IMO forensics in Android and windows systems. 2017 8th International Conference on Information, Intelligence, Systems and Applications, IISA 2017. 2018 Jul 2;2018-January:1–6.
29] Yang TY, Dehghantanha A, Choo KKR, Muda Z. Windows Instant Messaging App Forensics: Facebook and Skype as Case Studies. PLoS One. 2016 Mar 1;11(3):e0150300.
30] Usman A. WINDOWS 10 INSTANT MESSAGING APPLICATION FORENSICS In Fulfilment of the Requirements for the Degree of Master of Information Security. MSc thesis, University Putra Malaysia. 2018;
31] Rathi K, Karabiyik U, Aderibigbe T, Chi H. Forensic analysis of encrypted instant messaging applications on Android. 6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding. 2018 May 4;2018-January:1–6.
32] Wu S, Zhang Y, Wang X, Xiong X, Du L. Forensic analysis of WeChat on Android smartphones. Digit Investig. 2017 Jun 1; 21:3–10.
33] Satrya GB, Daely PT, Nugroho MA. Digital forensic analysis of Telegram Messenger on Android devices. Proceedings of 2016 International Conference on Information and Communication Technology and Systems, ICTS 2016. 2017 Apr 24;1–7.
34] Anglano C, Canonico M, Guazzone M. Forensic analysis of Telegram Messenger on Android smartphones. Digit Investig. 2017 Dec 1; 23:31–49.
35] Husain MI, Sridhar R. iForensics: Forensic analysis of instant messaging on smart phones. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering. 2010; 31 LNICST:9–18.
36] Mahajan A, Dahiya MS, Sanghvi HP. Forensic Analysis of Instant Messenger Applications on Android Devices. Int J Comput Appl. 2013 Apr 17;68(8):38–44.
37] Satrya GB, Daely PT, Shin SY. Android forensics analysis: Private chat on social messenger. International Conference on Ubiquitous and Future Networks, ICUFN. 2016 Aug 9;2016-August:430–5.
38] Alisabeth C, Pramadi YR. Forensic Analysis of Instagram on Android. IOP Conf Ser Mater Sci Eng. 2020 Dec 1; 1007(1):012116.
39] Casey E. Computer Basics for Digital Investigators. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 2011;(April):437–63.
40] Carrier B, Spafford EH. Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence Fall. 2003; 2(2).
41] Pirzada S, Hidayah N, Rahman A, Dwi N, Cahyani W, Othman MF. A Survey of Forensic Analysis and Information Visualization Approach for Instant Messaging Applications. IJACSA) International Journal of Advanced Computer Science and Applications. 2023;14(2).
42] Abu Hweidi RF, Jazzar M, Eleyan A, Bejaoui T. Forensics Investigation on Social Media Apps and Web Apps Messaging in Android Smartphone. 2023 International Conference on Smart Applications, Communications and Networking, SmartNets 2023.
43] Sharma YK, Noval SS, Jain A, Sabitha B, Ramya T. Forensics-as-a-service: A Review of Mobile Forensics. Proceedings of 5th International Conference on Contemporary Computing and Informatics, IC3I 2022. 2022;486–91.
44] Moreb M, Salah S. A Novel Framework for Mobile Forensics Investigation Process. Res Sq. 2023 Mar 8.
45] Ramadhan MI, Riadi I. Forensic WhatsApp based Android using National Institute of Standard Technology (NIST) Method. Int J Comput Appl. 2019;177(8):975–8887.
46] Paligu F, Varol C. Browser Forensic Investigations of WhatsApp Web Utilizing IndexedDB Persistent Storage. Future Internet 2020, Vol 12, Page 184. 2020 Oct 28;12(11):184.
47] Son J, Kim YW, Oh D Bin, Kim K. Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema. Forensic Science International: Digital Investigation. 2022 Mar 1; 40:301347.
48] Malik AW, Bhatti DS, Park TJ, Ishtiaq HU, Ryou JC, Kim K Il. Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. Sensors 2024, Vol 24, Page 433. 2024 Jan 10;24(2):433.
49] Aburbeian AM, Fernández-Veiga M. Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. AI 2024, Vol 5, Pages 177-194. 2024 Jan 10 ;5(1):177–94.
50] Alblooshi A, Aljneibi N, Iqbal F, Ikuesan R, Badra M, Khalid Z. Smartphone Forensics: A Comparative Study of Common Mobile Phone Models. 12th International Symposium on Digital Forensics and Security, ISDFS 2024. 2024;
51] Ogundiran A, Chi H, Yan J, Miller J. Forensic Analysis of Social Media Android Apps via Timelines. Lecture Notes in Networks and Systems. 2024;921 LNNS:544–59.
52] Almuqren A, Alsuwaelim H, Hafizur Rahman MM, Ibrahim AA. A Systematic Literature Review on Digital Forensic Investigation on Android Devices. Procedia Comput Sci. 2024 Jan 1; 235:1332–52.
53] Hyder MF, Arshad S, Fatima T. Toward social media forensics through development of iOS analyzers for evidence collection and analysis. Concurr Comput. 2024 Jun 10;36(13):e8074.
54] Sarhan SAE, Youness HA, Bahaa-Eldin AM, Taha AE. VoIP Network Forensics of Instant Messaging Calls. IEEE Access. 2024; 12:9012–24.
55] Soni N. Forensic Analysis of WhatsApp: A Review of Techniques, Challenges, and Future Directions. forensicscijournal.com. 2024;19–24.
56] Sudiana D, Nuruddin CH, Rizkinia M, Husna D. Forensic Analysis of WhatsApp Disappearing Message on Unrooted Android Using Mobile Device Forensics Methodology NIST SP 800-101r1. Evergreen.
57] Dixon SJ. Statica. 2023. Most popular messaging apps 2023 | Statista. [Available from: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/].