HSPI Inc. The Open Access Publisher

JFSR ISSN 2575-0186 JOURNAL OF FORENSIC SCIENCE AND RESEARCH

Research Article

Analysis and Comparison of Social Media Applications Using Forensic Software on Mobile Devices

Hüseyin Çakır[1]* and Merve Hatice Karataş[2]

[1]Computer Education and Instructional Technologies, Gazi University, Türkiye
[2]Turkish Standards Institute, Türkiye

More Information

*Address for correspondence: Hüseyin Çakır, Computer Education and Instructional Technologies, Gazi University, Ankara, Türkiye, Email: hcakir@gazi.edu.tr

Submitted: October 15, 2024
Approved: October 21, 2024
Published: October 22, 2024

How to cite this article: Çakır H, Karataş MH. Analysis and Comparison of Social Media Applications Using Forensic Software on Mobile Devices. J Forensic Sci Res. 2024; 8(1): 058-063. Available from: https://dx.doi.org/10.29328/journal.jfsr.1001065

Keywords: Social media; Mobile devices; Forensic software

Check for updates

OPEN ACCESS

Abstract

With the integration of mobile systems into daily life, social media applications used especially on Android and iOS platforms contain a significant amount of sensitive information. Social media applications on mobile systems have huge personal and sensitive content. Therefore, it is important to design effective techniques for forensic analysis of social media applications and to detect personal data. In this research, three different paid mobile forensic software and 4 different brands and models of smartphones with different operating systems were used and analyzed. The study shows that private messages, e-mails, time information, shared data, location and time information, and other personal data can be obtained by a forensic expert who performs an examination, and it is seen that one software can access the deleted data, but another software cannot access it. In proportion to the technology used in today's world, mobile forensics incidents are increasing day by day, and a competitive environment is created among the software used to illuminate these incidents. With this competition, software companies dealing with forensic informatics are trying to obtain different data to illuminate forensic events that may occur due to the active use of social media accounts with the developing technology, and software that does not meet the needs in the face of this situation remains in the background. The criminal elements in the investigation areas of mobile forensics differ daily, and the scope of crimes in the virtual environment is expanding with the developing technology. Therefore, mobile forensic analysis applications should be successful in social media applications other than standard data.

Introduction

Today, with the development of information technologies, especially with the widespread use of the internet in mobile systems, personal and corporate data and information have become easily accessible and portable in electronic media. Smartphone usage in the world is increasing day by day. According to research, the number of smartphone users is projected to be more than 2.6 billion by 2019 [1]. Users use their smartphone devices not only for making voice calls and exchanging SMS but also for mobile banking, social media applications, and location-based services. This communication environment, called social media, is a form of communication independent of time and space, where people share and interact with each other. It provides an environment for people to present their thoughts or pictures, videos, locations, and artefacts they want to share. Social media has become a tool where people spend their free time, have fun, chat, access information, and follow the agenda. The increase in the commission of cybercrimes through smartphones has led to the necessity of examining cybercrimes in this field and many analysis software/methods have been produced. In the field of forensic informatics crimes, the sub-heading of examining smartphones and mobile phones has emerged, and specialization areas that examine only this subject have emerged.

This research aims to identify the data of social media applications on mobile devices and operating systems on different platforms that can be presented as evidence and to analyze their effectiveness and advantages/disadvantages by analyzing them with different forensic software.

Mobile device investigation in forensic informatics

Crimes committed in the virtual environment are increasing rapidly and individuals should be aware of possible damages when using this technology. Forensic informatics reports should be clear and understandable to protect both individuals and institutions, contain all the information that will identify the case, and bear the signature of the responsible person [2]. Smartphones are a common source of evidence in both criminal investigations and civil cases. The continuous development of mobile devices and mobile applications makes forensic investigations complex [3]. Evidence obtained as a result of forensic informatics investigations is used by courts and government agencies to clarify cases. Investigators should not leave the results open to interpretation. Smart device users may be trapped through social media, e-mail, SMS, and fake calls and may face violations of private life and financial damages. For this reason, individuals should know their legal rights and the ways they can apply for possible victimization [2].

Forensic analysis of social media applications

Today, cell phones, especially smartphones, are used extensively for data communication. The reasons for keeping this type of forensic informatics separate are the use of GSM architecture and SIM card technology and the availability of a wider range of standards than computers [4]. However, with the widespread use of smartphones, free communication software (skype, WhatsApp, tango, viber, etc.) that can be downloaded and used from virtual markets have emerged in addition to the call and sms communication of portable devices, thus phone applications and related data have also become a part of forensic informatics [5].

Today, hundreds of social networks store personal information. Information that used to be kept private is now shared on public websites. Searching and gathering intelligence on these sites has gained importance. The rapid growth of social media and instant messaging applications has facilitated cybercrime and malicious activities [6]. Many social media and instant messaging providers have expanded the services of mobile platforms [7]. Which further exacerbates the situation [8]. With users in danger of losing more personal information [7]. Such as the spread of malicious code, and the acquisition and dissemination of confidential information. Copyright infringement, cyber-stalking, cyber-bullying, slander spreading and sexual harassment are becoming serious threats for social media and IM mobile users [9]. Therefore, it has become common to encounter various mobile devices during various forensic investigations [10]. Mobile devices are now an important source of forensic remains related to users' social media and instant messaging activities [11]. However, the difference between mobile devices makes it imperative for forensic investigators to develop specialized methods and techniques for investigating different phones [12]. Beyond evidence acquisition, many investigators have shown great interest in investigating social media and instant messaging services on different mobile platforms.

Analyzed eight social media apps on Apple iOS, e.g. Cyworld, Me2Day, Daum Yozm, Twitter, Facebook, NateOn UC, KakaoTalk, and MyPeople, and were able to detect user information, friend list, message, contact, and media information [13]. Observed the diversification of backup files for Facebook, Whatsapp Messenger, Skype, Windows Live Messenger, and Viber on Apple iOS [14]. Analyzed the remnants of the Whatsapp Messenger application on an Android smartphone and reconstructed the chronology of communicated messages and the contacts list [15]. Successfully decoded Whatsapp Messenger's network traffic and obtained forensic artifacts related to call features and visual messages exchanged between users [16]. Analyzed 20 popular instant messaging apps on an Android platform and reconstructed some or all message content of 16 apps [17]. Conducted a comparative study with Facebook and Twitter data on Apple iOS, Windows Mobile, and RIM BlackBerry, and analyzed Facebook and Twitter applications on Apple iOS [18]. Compared the artifacts of Samsung's ChatON application between a Samsung Galaxy Note running Android 4.1 and an Apple iPhone running iOS 6 and was able to detect sent and received messages by timestamp and the location of the files sent on both platforms [19]. Investigated Facebook, Twitter, LinkedIn, and Google+ on Android and Apple iOS platforms and managed to recover many artifacts including username, contact information, location, friends list, social media messages, messages, comments, and IP addresses of selected social media apps [8].

Several studies have explored the forensic analysis of social networking applications on mobile devices, focusing on various platforms, devices, and forensic techniques. These studies provide valuable insights into the recoverability of user data from social networking apps and the challenges faced during forensic investigations. Some notable research in this area includes:

Several studies have examined the forensic analysis of social networking applications on smartphones, highlighting various approaches and findings. One study focused on forensic analysis of Facebook, Twitter, and MySpace on BlackBerry, iPhone, and Android devices, determining whether app activities were stored in internal memory. The results showed that no data could be recovered from BlackBerry devices, while iPhones and Android phones stored significant recoverable data useful for forensic investigations [20].

Another study analyzed four popular social networking platforms—Facebook, Twitter, LinkedIn, and Google+—on Android and iOS devices to detect user activity traces. Researchers attempted to uncover artefacts such as usernames, passwords, logins, personal information, uploaded posts, messages, and comments that could facilitate criminal investigations [21].

In a similar investigation, Facebook, WhatsApp Messenger, Instagram, and Twitter were installed on an Android device to perform basic user behaviour analysis. Forensic tools like Oxygen Forensic, Paraben E3: DS, and Magnet Axiom were employed for manual data extraction and mobile forensic information retrieval. The comparative analysis showed that some important forensic data could only be obtained through manual extraction methods [22].

A comprehensive digital forensic analysis of social media platforms, such as YouTube, Instagram, and TikTok, was conducted on two Android devices (OnePlus 7 Pro and Motorola X4). This study emphasized the differences and similarities in user interactions and the impact of varying devices and access methods [23].

Additionally, a study on Facebook, Twitter, and LinkedIn examined whether these applications stored user activity data on Apple iPhones, Android, Windows, and BlackBerry devices. The findings revealed that while BlackBerry smartphones yielded no extractable data, significant information was recoverable from Android, Windows, and iPhone devices [24].

Finally, another research explored the challenges in smartphone forensics by testing various operating systems (OSs), including Android, iOS, and Windows, to extract forensic artefacts. The results from both logical and physical acquisitions were presented [25].

Materials and methods

The objective of this research is to identify data that can be used as evidence in social media applications on different mobile devices and operating systems. In addition, by analyzing these data using various forensic software, the effectiveness, advantages, and disadvantages of the software were investigated. In this context, it is aimed at raising awareness through these investigations.

This study aims to analyze social media applications using four different mobile devices and three different paid forensic software. The devices used include the iPhone SE, Samsung A800I, Samsung J710FQ, and Venus V3 5010. Analyses were performed on these devices, especially on intentionally deleted data. Cellebrite, XRY, and Oxygen Suite software were used for analysis. Logical and physical image retrieval was performed using the graphical interfaces and SQLite editors of this software. Models with different operating systems among the devices were analyzed, and the capacities of each software to support data retrieval, social media applications, and GPS data were compared.

The current smartphone operating systems in the market are Google Android 86%, Apple iOS 13%, and others less than 1%, but Google Android has a large share of the total market share [3]. Therefore, this paper covers forensic analysis of social networking applications such as Facebook, Instagram, Twitter, and WhatsApp, which are commonly used on this platform due to the intensive use of Google Android and Apple iOS operating systems.

In this research, "XRY, Celebrite and Oxygen Suite" software and "iPhone SE and Samsung A800I, Venus V3_5010, Samsung J710FQ" devices and "Android and iOS" operating systems were used. Also used hardware and software: Windows 8.1 Enterprise 64-bit operating system 64 GB RAM, iPhone SE iOS 11.2.1 operating system 2 GB RAM 16 GB internal memory, Samsung Galaxy SM A800I 6.0.1 Android operating system 2 GB Ram 32 GB internal memory, Venus V3_5010 6.0. 1 Android operating system 1 GB Ram 8 GB internal memory, Samsung J710FQ 6.0.1 Android operating system 2 GB Ram 16 GB internal memory, Cellebrite 6.3.11.36, XRY 7.4.0, Oxygen 2016 8.2.0.273, Micro USB cable, iPhone USB Cable, Instagram version:27.0, Facebook version: 153.0, Whatsapp version: 2.17.82, Twitter version:7.14

There should be many forensic software and hardware on a computer where a forensic forensic evidence examination and analysis will be performed. In this research, logical images were taken using paid forensic software "Cellebrite 6.3.1.477, XRY 7.4.0 and Oxygen Suite 2016" installed on the Windows 10 Professional operating system, and these operations were performed directly through the Graphical (GUI) interfaces of the software, Hexa Decimal Editors and SQLite editors. The logical and physical images were analyzed with XRY Reader for XRY images, UFED within Cellebrite, and SQLite editor software on Oxygen Suite itself. Previously used devices and the data on these devices were deliberately deleted for analysis. Only the Venus V3 5010 model was rooted on the analyzed devices. In addition, the devices were previously shared via social media by leaving the location open.

Results and discussion

In this research, 4 different brand model smartphones with three different paid software and different operating systems were used and analyzed. The SIM card of the devices can be shown as an example of "Call recording, contact list, picture, video, audio, location information, data belonging to installed applications, and data belonging to social media tools" that may be in internal memory and external memory. Most of this data is personal data belonging to the user that mobile devices contain. These data can be encrypted or unencrypted and can be accessed through the software on the devices without damaging these data in the forensic analysis process. The table below shows which software and which devices are used.

As can be seen in Table 1, three different paid software and 4 different brand models of smartphones with different operating systems were used, and it is indicated whether the software used supports mobile devices with different hardware and software to be analyzed.

As can be seen in Table 2, the general features and analysis levels of the software to be used in the research are specified. The features of three successful software, which are the

https://doi.org/10.29328/journal.jfsr.1001065

leading paid software used in the field of mobile forensics, are given in Table 2.

In Table 3, XRY reports the data analyzed both logically, physically, and as a file system on devices with iOS and Android operating systems. XRY did not support only one device (Venus V3 5010) among the analyzed devices.

In Table 4, Cellebrite was found to be more successful in retrieving deleted data. Cellebrite analyzed both logical, physical, and file system data on devices with iOS and Android operating systems and reported the data by making sense of it. Cellebrite did not support only one device (Samsung J710FQ) among the analyzed devices.

In Table 5, Cellebrite Analysis results 5, Oxygen suite was able to retrieve many data within the scope of logical data retrieval on the iPhone SE model device with the iOS operating system. However, as a result of the logical image study on the Samsung A800I model device with the Android operating system, it could not make sense of social media applications and location information. Oxygen suite did not support the other two devices (Venus V3 5010 and Samsung J710FQ).

The operating systems of the devices used during the analysis, "iOS and Android," required different mobile forensics platforms, different hardware and software settings, and many different settings and methods even according to the devices.

Another problem is the differences in the hardware structure of the devices and the installed applications. It was observed that the paid software used did not support many newly released devices, and some devices had version differences.

In one study, it was stated that more experimental cases are needed to examine a wider variety of social networking applications and different mobile phone platforms [26].

In addition, the software used is paid and very high cost. In the technical settings and software installations made to change the connection methods of the mobile devices to be analyzed, problems were experienced in the operating systems and these devices were reinstalled.

On all smart devices, the user is not an authorized user on the device and is not authorized to access many system files.

The Android operating system provides access to the file system on the device and the process of becoming an authorized user is called rooting. Jailbreaking, on the other hand, is generally used as a method to get rid of the restrictions imposed by Apple on devices with iOS operating systems (such as iPhone, iPad, iPod Touch, and Apple TV) [2].

Table 1: Devices and software analyzed.

Mobile Software	iPhone SE	Samsung A800I	Venus V3_5010	Samsung J710FQ
XRY 7.4.0	Examined	Examined	There is no support available	Examined
Cellebrite 6.3.11.36	Examined	Examined	Examined	There is no support available
Oxygen 8.2.0.273	Examined	Examined	There is no support available	There is no support available

Table 2: Features of the software.

Mobile Software	Network Type	Forensics Tools	Investigation	Analysis	Report
XRY 7.4.0	GSM	+	+	+	+
Cellebrite 6.3.11.36	GSM	+	+	+	+
Oxygen 8.2.0.273	GSM	+	+	+	+

Table 3: XRY analysis results.

	Device Brand / Model	Level of Analysis	Facebook (Messenger)	Instagram	Whatsapp	Other Applications	GPS (Location Information)
XRY	iPhone SE	Logical	7	-	462	9	2
	Samsung A800I	Logical	10	-	17952	6	188
	Venus V3 5010	No support available	-	-	-	-	-
	Samsung J710FQ	Physical	37 data 1 deleted	-	39	213	41

Table 4: Cellebrite analysis results.

	Device Brand / Model	Level of Analysis	Facebook (Messenger)	Instagram	Whatsapp	Other Applications	GPS (Location Information)
Cellebrite 6.3.11.36	iPhone SE	File System	5	-	273 data 3 deleted	431	24
	Samsung A800I	Logical	-	-	-	1091	62
	Venus V3 5010	Physical	-	9	8 data 1 deleted	1913 data 66 deleted	79
	Samsung J710FQ	No support available	-	-	-	-	-

https://doi.org/10.29328/journal.jfsr.1001065

Table 5: Cellebrite analysis results 5, oxygen suite analysis results.

	Device Brand / Model	Level of Analysis	Facebook (Messenger)	Instagram	Whatsapp	Other Applications	GPS (Location Information)
Oxygen 8.2.0.273	iPhone SE	Logical	112 - 692	193	1254	545	3
	Samsung A800I	Logical	It finds data on the device but cannot make sense of social media apps.				
	Venus V3 5010	No support available	-	-	-	-	-
	Samsung J710FQ	No support available	-	-	-	-	-

Another study proposes future enhancements to improve the effectiveness of Andriller in Android forensic investigations. Andriller is a software application that consists of a set of forensic tools designed for Android devices. It collects forensically sound, non-destructive, and read-only data from these devices. The proposed enhancements include improvements to data extraction techniques, compatibility with new Android versions, support for additional data types, integration with advanced analysis methods, and addressing existing limitations [27].

In another study, the reason for rooting Android phones is that a lot of data on these smartphones cannot be accessed or saved to the host computer via backup without rooting the device. Rooted Android devices give the user full rights or root privileges on the operating system. It is emphasized that the restrictions imposed by the factory can be overcome through root Access [24].

For this reason, due to the intensive use of Google Android and Apple iOS operating systems, it covers the forensic analysis of social networking applications such as Location information, Facebook, Instagram, Twitter WhatsApp, etc., which are commonly used on his platform.

In another study, it was stated that these applications may be significant in digital forensics research due to their popularity. It was also emphasized that a large amount of information can be extracted from these applications and that it is essential to investigate and identify important artifacts [28].

Even if this data is encrypted, even if it cannot be found by mobile device forensics software, it can be obtained by advanced forensics data recovery processes.

In another study, when the contents of application files extracted from the file system were manually examined, it was found that more information was obtained than what was retrieved from the tools, and some deleted data was also discovered depending on user behavior. Compared to the methods used in the analysis, manual data acquisition methods and Oxygen Forensics were found to be more successful than other methods in terms of physical image acquisition [22].

Traces and detection methods of the same applications installed on these systems may show various features according to device brand models. In addition, as a single software may not be able to access the desired data, the analysis results using different software should be compared, and always performing a verification process will add certainty to the analysis process.

Conclusion

In the analysis phase, the logical and file system image of the iPhone SE with the iOS operating system could be taken and its direct content could be viewed in “XRY, Celebrite, and Oxygen Suite” software. Although Android systems have a more flexible structure than iOS, data can be accessed as a result of the analysis in the logical image of iOS devices, while data was obtained in the logical image analysis on Android, but the data could not make sense due to the study on social media applications. Rooting is required to obtain a physical image on Android devices.

There are big differences between the number of data in the logical image of Android devices and the number of data in the physical image, and it has been observed that the data on the physical image is more. The process of taking the physical image of devices with the iOS operating system could not be performed because it was seen that the “XRY, Celebrite, and Oxygen Suite” applications did not open this service to users. Except for the iPhone 4 device with the iOS operating system, it does not authorize users to take physical images. In the iOS analysis, only the image folders on the device could be seen because the device connected to the computer to start the analysis process with its software was a closed system. This is a concrete feature that shows that the iOS system is more secure than other systems. Another issue was the connection method of the devices used and the software used. A micro USB cable from a different brand model device was used to connect and analyze the data.

Considering the software used and the number of data found, it was determined that there was a big difference in the number of data found between the software. It has been determined that Cellebrite software has wider technical possibilities and capabilities in terms of mobile forensic software features. The XRY application, on the other hand, is more successful on mobile devices with older versions.

With this software and other forensic tools on it, it is evaluated that there is no need for a separate analysis software in the first stage. However, no matter how precise and accurate the result seems to be, it is considered that the analyses should be performed with different software using both classical computer forensics and mobile forensics tools, the results should be compared and the final report to be submitted to the relevant legal authority should be presented in this way. This will ensure that the analysis is more consistent and that the legal process continues or ends healthily. Although data recovery in each software is easy for Android, it is not possible to say the same for iOS. What needs to be done is to analyze a device with several softwares and, if possible, by different experts, compare the results and check the accuracy.

References

1. Hornyak T. Android grabs record 85 percent smartphone share. 2014. Available from: http://www.pcworld.com/article/2460020/android-grabs-record-85-percent-smartphone-share.html

2. Ukşal M. Mobile forensics. Istanbul Bilgi University Institute of Social Sciences; 2015.

3. Ashraf RA. Performance analysis of video call application on tablet using 3G network. Melaka: UTEM; 2013.

4. Emekci A, Kuğu E. Computer forensics and agent-based systems. In: Proceedings of the 7th International Information Security and Cryptology Conference; 2014; 17-18.

5. Özen M, Özocak G. Legal regime of search and seizure measures in computer forensics, electronic evidence and computers (CMK Art. 134). Ankara Bar Association Magazine. 2015;1.

6. Mohtasebi S, Dehghantanha A. Defusing the hazards of social network services. Int J Digit Inf Wirel Commun. 2011;1:504–516.

7. Taylor M, Hughes G, Haggerty J, Gresty D, Almond P. Digital evidence from mobile telephone applications. Comput Law Secur Rev. 2012;28:335–339. Available from: http://dx.doi.org/10.1016/j.clsr.2012.03.006

8. Dezfouli FN, Dehghantanha A, Eterovic-Soric B, Choo KR. Investigating social networking applications on smartphones: detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. Aust J Forensic Sci. 2016;46(4):469–488. Available from: http://dx.doi.org/10.1080/00450618.2015.1066854

9. Dezfouli FN, Dehghantanha A, Mahmod R, Mohd Sani NF, Shamsuddin S. A data-centric model for smartphone security. Int J Adv Comput Technol. 2013;5:9–17. Available from: http://dx.doi.org/10.4156/ijact.vol5.issue9.2

10. Damshenas M, Dehghantanha A, Mahmoud R. A survey on digital forensics trends. Int J Cyber-Security Digit Forensics. 2014;3(4):209–235. https://www.semanticscholar.org/paper/A-Survey-on-Digital-Forensics-Trends-Dehghantanha-Damshenas/d3dcb45bbdbb440186a926b7541870d6c3844c72

11. Mohtasebi S, Dehghantanha A. Towards a unified forensic investigation framework of smartphones. Int J Comput Theory Eng. 2013;5:351–355. Available from: http://dx.doi.org/10.7763/IJCTE.2013.V5.708

12. Mohtasebi S, Dehghantanha A, Broujerdi HG. Smartphone forensics: a case study with Nokia E5-00 mobile phone. Int J Digit Inf Wirel Commun. 2012;1:651–655. http://www.ijcte.org/index.php?m=content&c=index&a=show&catid=48&id=821

13. Jung J, Jeong C, Byun K, Lee S. Sensitive privacy data acquisition in the iPhone for digital forensic analysis. In: Park JJ, Lopez J, Yeo SS, Shon T, Taniar D, editors. Secure and trust computing, data management and applications. Communications in Computer and Information Science. 2011;186: Springer; 172-186. Available from: http://dx.doi.org/10.1007/978-3-642-22339-6_21

14. Tso YC, Wang SJ, Huang CT, Wang WJ. iPhone social networking for evidence investigations: using iTunes forensics. In: Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication - ICUIMC'12. New York, NY: ACM Press; 2012; 1. Available from: http://dx.doi.org/10.1145/2184751.2184827

15. Anglano C. Forensic analysis of WhatsApp Messenger on Android smartphones. Digit Investig. 2014;11:1–13. Available from: http://dx.doi.org/10.1016/j.diin.2014.04.003

16. Karpisek F, Baggili I, Breitinger F. WhatsApp network forensics: decrypting and understanding the WhatsApp call signaling messages. Digit Investig. 2015;11:1–9. Available from: http://dx.doi.org/10.1016/j.diin.2015.09.002

17. Walnycky D, Baggili I, Marrington A, Moore J, Breitinger F. Network and device forensic analysis of Android social-messaging applications. Digit Investig. 2015;14–S84. Available from: http://dx.doi.org/10.1016/j.diin.2015.05.009

18. Said H, Yousif A, Humaid H. iPhone forensics techniques and crime investigation. In: Proceedings of the International Conference and Workshop on Current Trends in Information Technology (CTIT 11). IEEE; 2011; 120–125. Available from: http://dx.doi.org/10.1109/CTIT.2011.6107946

19. Iqbal A, Marrington A, Baggili I. Forensic artifacts of the ChatON instant messaging application. In: Proceedings of the International Workshop on Systematic Approaches to Digital Forensic Engineering; 2014. Available from: http://dx.doi.org/10.1109/SADFE.2013.6911538

20. Al Mutawa N, Baggili I, Marrington A. Forensic analysis of social networking applications on mobile devices. Digit Investig. 2012;9–S33. Available from: https://doi.org/10.1016/j.diin.2012.05.007

21. Norouzi F, Dehghantanha A, Eterovic-Soric B, Choo KR. Investigating social networking applications on smartphones: detecting Facebook, Twitter, LinkedIn, and Google+ artifacts on Android and iOS platforms. Aust J Forensic Sci. 2015;48(4):469–488. Available from: http://dx.doi.org/10.1080/00450618.2015.1066854

22. Eriş FG, Akbal E. Forensic analysis of popular social media applications on Android smartphones. Balkan J Electr Comput Eng. 2021;9(4):386–397. Available from: https://doi.org/10.17694/bajece.761271

23. Millatina D, Gunawan EH, Sugiantoro B. Forensic analysis of WhatsApp, Instagram, and Telegram on virtual Android device. In: Proceedings of the 12th International Symposium on Digital Forensics and Security (ISDFS); 2024; 1–4. IEEE. Available from: http://dx.doi.org/10.1109/ISDFS60797.2024.10527308

24. Awan FA. Forensic examination of social networking applications on smartphones. In: Proceedings of the 2015 Conference on Information Assurance and Cyber Security (CIACS); 2015; 36–43. IEEE. Available from: https://doi.org/10.1109/CIACS.2015.7395564

25. Alblooshi A, Aljneibi N, Iqbal F, Ikuesan R, Badra M, Khalid Z. Smartphone forensics: a comparative study of common mobile phone models. In: Proceedings of the 12th International Symposium on Digital Forensics and Security (ISDFS); 2024; 1–6. IEEE. Available from: http://dx.doi.org/10.1109/ISDFS60797.2024.10527262

26. Al Mushcab R, Gladyshev P. The significance of different backup applications in retrieving social networking forensic artifacts from Android-based mobile devices. In: Proceedings of the 2nd International Conference on Information Security and Cyber Forensics (InfoSec); 2015; 66–71. IEEE. Available from: http://dx.doi.org/10.1155/2021/5567592

27. Almuqren A, Alsuwaelim H, Rahman MH, Ibrahim AA. A systematic literature review on digital forensic investigation on Android devices. Procedia Comput Sci. 2024;235:1332–1352. Available from: http://irep.iium.edu.my/112663/1/112663_A%20systematic%20literature%20review%20on%20digital%20forensic%20investigation.pdf

28. Johnson H, Volk K, Serafin R, Grajeda C, Baggili I. Alt-tech social forensics: forensic analysis of alternative social networking applications. Forensic Sci Int Digit Investig. 2022;42:301406. Available from: http://dx.doi.org/10.1016/j.fsidi.2022.301406