Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 7, No. 3, December 2021, pp. 512-521
ISSN: 2338-3070, DOI: 10.26555/jiteki.v7i3.22381

The Comparison Performance of Digital Forensic Tools Using Additional Root Access Options

Aljo Leonardo, Rini Indrayani
Faculty of Computer Science, Universitas AMIKOM Yogyakarta, Yogyakarta, 55283, Indonesia

ARTICLE INFO

Article history:

Received December 06, 2021
Revised December 27, 2021
Accepted January 19, 2022

Keywords:

Mobile Phone;
Forensic;
MiChat;
SayHi Chat;
Root;
Digital Evidence

ABSTRACT

This research used MiChat and SayHi as materials for forensic investigations using three different tools, namely MOBILedit, Magnet Axiom, and Belkasoft. These three tools will show each performance in the forensic process. We also added a rooting process as an option if data cannot be extracted optimally even when using these three applications. The result of this study shows that the cases studied with processes without root access and with root access have the aim of complementing each other in obtaining evidence. So that these two processes complement each other's shortcomings. The main contribution of this research is a recommendation of a tool based on the best performance shown during the forensic process with rooting access and without rooting access. Based on the comparison, Magnet Axiom is superior with a total of 34 items of data found without root access, while MOBILedit is 30 items and 30 items for Belkasoft. While comparison using root access, Magnet Axiom and MOBILedit are superiors with a total of 36 items found in Magnet Axiom without root access, while MOBILedit is 36 items and 33 items for Belkasoft. Based on the test results, it can be concluded that the recommended tool according to the used scenario is Magnet Axiom.

Corresponding Author:

Rini Indrayani, Universitas AMIKOM Yogyakarta, Yogyakarta, Indonesia
Email: rini.i@amikom.ac.id

1. INTRODUCTION

The rapid development of technology affects almost all aspects of human life [1][2]. The application of technology with the latest updates is widely used in daily life [3]. One of the applications of technology that is frequently used in human life is communication technology, especially mobile phones [4][5]. Humans in communicating with each other are now very dependent on technology ranging from daily conversations to exchanging data and documents via mobile phones [6][7]. Mobile phones are now one of the most important variables in future technology infrastructure [8]. Mobile phones now contain applications that are usually run on desktop-based devices, thus increasing human dependence on mobile phones [9]. This dependence makes communication technology application manufacturers busy in producing applications. One type of product that is widely developed is a chat service application [10][11].

Chat service applications can meet human communication needs from the most basic communication needs to communication needs at a higher level [12][13]. Basic communication needs such as voice telephone conversations and messaging [14]. Meanwhile, communication needs at a higher level, such as sending documents that are integrated with other services and supported by security technologies such as cryptographic functions [15]. Various communication technology companies issue chat service application products, including Telegram, Whatsapp, Line, SayHi Chat, MiChat, and various other chat service products. Each product comes with the advantages of each feature [16]. However, along with the convenience and completeness of the services provided, these various chat service products are often used as a medium for criminal acts [17].

Various criminal transactions such as child sexual abuse material often occur using chat application services [18][19]. Also, an application that is often in the spotlight is MiChat, which is often being a medium

for prostitution transactions [20]. Dating apps are also one of the digital platforms that are often the object of police investigations [21], one application that is often in the spotlight is SayHi Chat, which is often being a medium for online prostitution [22]. Disclosure of prostitution cases by involving chat application media usually utilizes the digital forensic investigation process because sometimes perpetrators delete data to eliminate digital evidence [20].

The digital forensics investigation process can help the competent authorities to collect case evidence that would normally have been removed from the data history [23][24][25][26][27]. All forensic procedures are carried out with prudence and documented [28][29][30]. Various studies regarding the digital forensic investigation process on chat application services have been carried out before. One of them is research on law enforcement investigations with a forensic approach on the WhatsApp instant messaging application [15]. The forensic approach carried out is related to wiretapping, database decryption, and analysis of WhatsApp application communication. This study also uses a test scenario for objective verification of the results. The result of this research is a recommendation of wiretapping methods that can be used by the authorities for the needs of law enforcement investigations.

A study about the forensic investigation of conversations in an Instagram application has also been carried out by [31]. This study compares the performance of Oxygen Forensics tools with Magnet Axiom in data extraction performance using the National Institute of Standards and Technology (NIST) method. The results of this study indicate that the performance of Magnet Axiom is superior with a performance percentage of 100% and axiom magnets by 84%.

Forensic analysis of telegram and BBM instant messenger applications has also been carried out by [32]. Encrypted data contained in the telegram and BBM applications is extracted and then analyzed for investigative purposes. The encryption method found in the investigation process is SQL encryption. After successful data extraction, the data is decrypted with a certain protocol for being analyzed as digital evidence [33]. Forensic analysis of IM application's encrypted data was also carried out by [34]. This research uses the Wickr and Private Text Messaging forensic object. The result of this research is a protocol for decrypting the extracted data from the forensic process on Wickr and Private Text Messaging platforms.

This research follows some basic forensic concepts that are also used by several previous studies, but we use different platforms for the forensic process. We used MiChat and SayHi as materials for forensic investigations using 3 different tools, namely MOBILedit, Magnet Axiom, and Belkasoft. These three tools will show each performance in the forensic process. We also added a rooting process as an option if data cannot be extracted optimally even when using these three applications. The main contribution of this research is a recommendation of a tool based on the best performance shown during the forensic process with rooting access and without rooting access.

2. METHOD

This study obtains information and analyzes the evidence by using the NIJ (National Institute of Justice) method. The stages of the method include the preparation stage, collection, examination, analysis, and reporting [20].

1. Preparation – Gathering information or issues to be raised, as well as preparing tools and materials to be analyzed for investigation purposes [35].
2. Collection – Collection of physical evidence (smartphone).
3. Examination – The process of extracting or acquiring data [36].
4. Analysis – The process of analyzing the extracted or acquired data [37].
5. Reporting – The final stage is to make a report on the final results of the investigation and analysis that has been carried out [38].

The data extraction process at the examination stage utilizes the live forensic method where researchers try to carry out the extraction or acquisition process of digital evidence [39][40][41]. It is stored on smartphones that have the MiChat and SayHi Chat applications installed. Extraction using MOBILedit Forensic Express PRO, Belkasoft Evidence Center, and Magnet Axiom tools. The extracted data is used as material for the analysis process. Data extraction is divided into three types based on the character of the data that can be collected. They are logical, file system, and physical. Logical data extraction is the fastest and most supported data extraction by any mobile phone [42]. Logical extraction can load data such as SMS & MMS, Call Logs, Contacts, Media, and application data. Data file system extraction is a data extraction that can be done by examiners to thoroughly examine the file system on the smartphone, not only data snippets but system files as well [43][44]. This file system extraction can contain SMS & MMS, call logs, contacts, media, application data, and all files (including hidden data, database, system, and logs). Physical data extraction is the most detailed and extensive method. Physical extraction can contain SMS & MMS, call logs, contacts, media, application data, all files (including hidden data, database, system, and logs), temporal data, and deleted data.

2.1. Preparation (Identification)

The preparation stage was the stage where the researchers prepared some materials and tools for forensic process purposes [45]. The prepared items are mentioned as

1) Laptop Acer Aspire E 14 E5-475G-70XV
2) Smartphone Samsung Galaxy GT-19060
3) MOBILedit Forensics Express Pro Version 7.3.1.19798 (64-bit)
4) Belkasoft Evidence Center version 9.9800.4928
5) Magnet Axiom version 4.10.0.23663
6) Oxygen Forensic Detective version 12.0.0.151
7) MiChat App version 1.3.149
8) SayHi Chat Application Version 8.33
9) Forensic Connector App
10) iRoot for PC version 1.8.9.21144
11) USB Cable

2.2. Collection

The collection stage is the stage where the researcher investigates to collect the form of physical evidence and documentation [46]. This study used the Samsung Galaxy Duos GT-19060 version of Android 4.2.2 as the physical evidence, shown in Fig. 1. Physical device basic information of used physical evidence are explained in Table 1.

Fig. 1. Physical Evidence

Table 1. Physical Device Basic Information

No.	Information Item	Description
1	Manufacturer	Samsung
2	Product	GT-19060
3	HW Revision	JDQ39
4	Platform	Android
5	SW Revision	4.2.2 (17)
6	Serial Number	RF1F61SQQKB
7	Unlocking Pattern	0124678
8	IMEI	352700062003099
9	Rooted	Yes/No*
10	SIM Card	Yes/No*
11	Operator	MCC:510, MNC:10

We use a scenario as a reference for the investigation process. A scenario in general investigative research is used to parameterize a unique individual pattern [47][48]. This scenario was carried out on the Samsung Galaxy GT-1960 Smartphone as the property of the perpetrators of online prostitution transactions. This research scenario positions the perpetrators to try to eliminate evidence of transactions by deleting conversation history and data from the MiChat and SayHi applications as online transaction media. The investigative process of this research seeks to uncover digital evidence that has been deleted using digital forensic protocols.

2.3. Examination

The examination stage is the stage where the researchers carried out several investigative processes to find and retrieve the database from the MiChat application and SayHi Chat application. The examination stage

has an imaging process that occurs where the original data of the android phone is copied for being analyzed in the next process [49][50]. The imaging process is very important to maintain data integrity [51][52][53]. The results of the examination process were analyzed to find the digital evidence [54][55][56]. Researchers use two options in the examination process, namely the process without rooting and the process with rooting [57]. If the process without root access cannot find data from MiChat and SayHi Chat, then the device is rooted. Several stages of the process are carried out using three tools, namely MOBILedit, Magnet Axiom, and Belkasoft Evidence Center. The extraction process or data acquisition is divided into two, namely, without rooting and using root access, shown in Fig. 2, Fig. 3, Fig. 4, and Fig. 5.

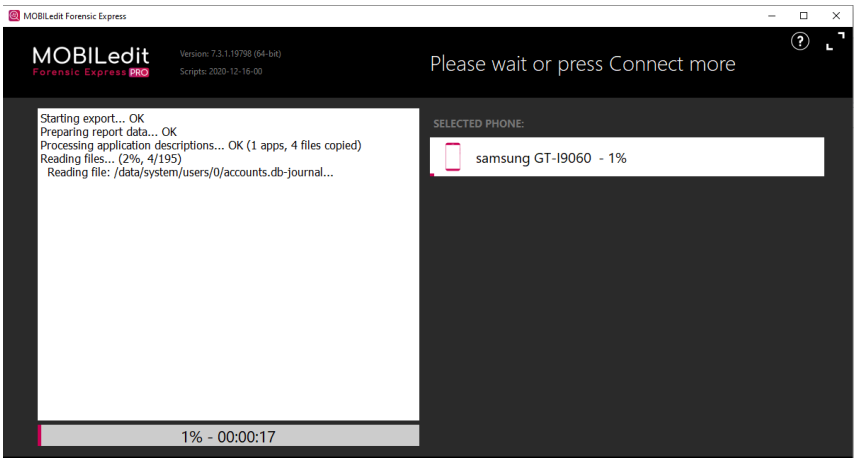

Fig. 2. Examination process using MOBILedit without rooting

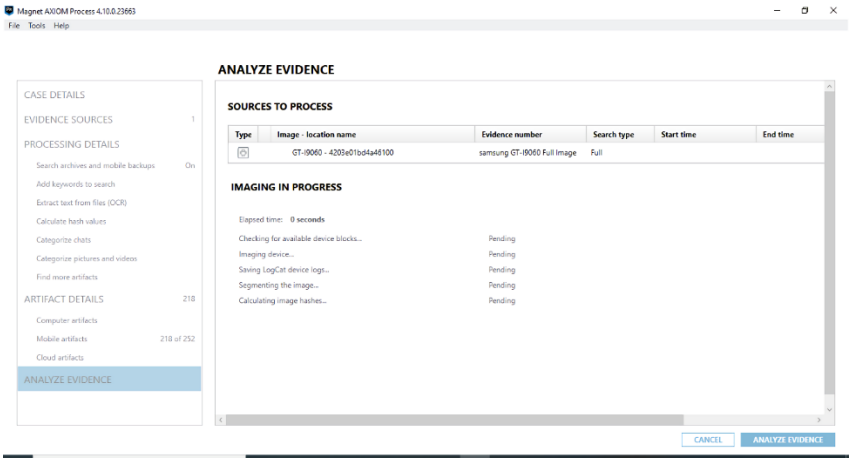

Fig. 3. Examination process using Magnet Axiom without rooting

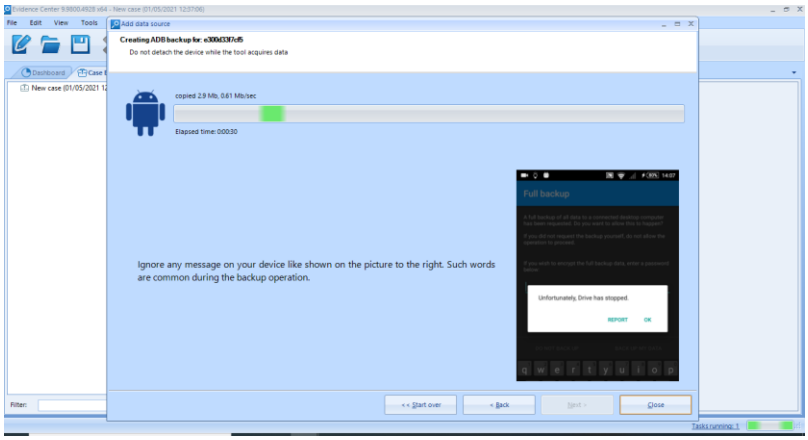

Fig. 4. Examination process using Belkasoft without rooting

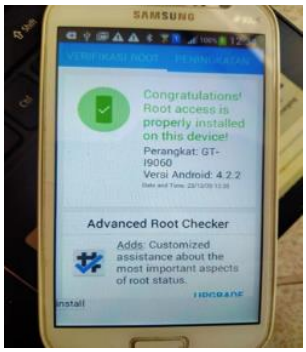

Fig. 5. Examination process with root access

2.4. Analysis

The Analysis stage has the goal to carry out analytical actions and reveal the results of the examination stage [58][59]. In this stage, the researcher tried to analyze all the data that has been successfully acquired previously, which has a connection with the MiChat and SayHi Chat applications. All data found are connected. Completeness between contact data, avatars, conversation activities, multimedia files, and other data are associated with each other. If the results of the analysis show that there are indications of data deletion and it is not revealed using a process without root, then proceed with the analysis process using the root process. The analysis process is carried out by matching metadata, shown in Fig. 6.

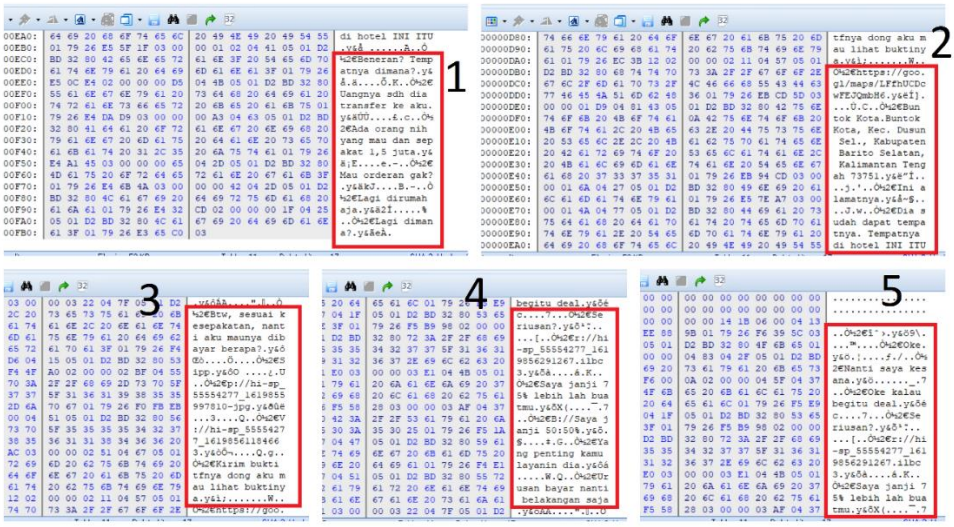

Fig. 6. Metadata Matching Process from Data

2.5. Reporting

The reporting stage is the result of the previous analysis that has been carried out on the MiChat and SayHi Chat analysis investigation process. All stages of the analysis were carried out reported at the reporting stage. The researcher explained in detail all the result sets and compared all the results of the analysis that has been carried out starting from the analysis without rooting access to the analysis using rooting access.

3. RESULTS AND DISCUSSION

The forensic process is an attempt to uncover digital evidence as much as possible [60]. Therefore, the various processes needed are expected to support each other. If one process cannot solve a problem, then another additional process is needed as long as it gets permission from the competent authority and is under applicable regulations [61]. Usually, one process that is an additional option is the rooting process. In the process of investigating criminal cases, the forensic process as much as possible avoids the use of root access, but if rooting is needed to complete the investigation process, the rooting process can be carried out by the competent authorities. The rooting process is the last option because the rooting process can open new security holes on the device [24].

Table 2 shows a comparison of the results of the analysis without rooting using MOBILedit. The data in the table shows that almost all data in the SayHi Chat application can be extracted without having to use the rooting process. At the same time, the data on the MiChat application cannot be extracted optimally by the

process without rooting. Table 3 shows a comparison of the results of the analysis without rooting using Magnet Axiom. The data in the table shows that almost all data in the SayHi Chat application can be extracted without having to use the rooting process. In contrast, the data on the MiChat application cannot be extracted optimally by the process without rooting. Table 4 shows a comparison of the results of the analysis without rooting using Belkasoft. The data in the table shows that almost all data in the SayHi Chat application can be extracted without having to use the rooting process. In comparison, the data on the MiChat application cannot be extracted optimally by the process without rooting. Based on the comparison of Table 2, Table 3, and Table 4, Magnet Axiom is superior with a total of 34 items of data found without root access, while MOBILedit is 30 items, and 30 items for Belkasoft.

Table 2. Comparison of Analysis Without Root Access in MOBILedit

Revealed Data	Amount of Revealed Data in MiChat	Amount of Revealed Data in SayHi Chat
Database File	0	2
Account Name	0	2
Contact List	0	6
Contact Number	0	0
Chat Logs	0	18
Location	0	1
Deleted Message	0	1
Suspect Avatar	0	0
Client Avatar	0	0
Image File	0	0
Video File	0	0

Table 3. Comparison of Analysis Without Root Access in Magnet Axiom

Revealed Data	Amount of Revealed Data in MiChat	Amount of Revealed Data in SayHi Chat
Database File	0	4
Account Name	0	2
Contact List	0	6
Contact Number	0	0
Chat Logs	0	18
Location	0	1
Deleted Message	0	1
Suspect Avatar	1	0
Client Avatar	1	0
Image File	0	1
Video File	0	1

Table 4. Comparison of Analysis Without Root Access in Belkasoft

Revealed Data	Amount of Revealed Data in MiChat	Amount of Revealed Data in SayHi Chat
Database File	0	2
Account Name	0	2
Contact List	0	6
Contact Number	0	0
Chat Logs	0	18
Location	0	1
Deleted Message	0	1
Suspect Avatar	0	0
Client Avatar	0	0
Image File	0	0
Video File	0	0

Table 5 shows that using MOBILedit with root access. Data extraction can be more optimal in both the SayHi application and the Mi chat application. Table 6 shows that using Magnet Axiom with root access. Data extraction can be more optimal in both the SayHi application and the Mi chat application. Table 7 shows that using Belkasoft with root access. Data extraction can be more optimal in both the SayHi application and the MiChat application. Based on the comparison of Table 5, Table 6, and Table 7, Magnet Axiom and MOBILedit are superiors with a total of 36 items found in Magnet Axiom without root access, while MOBILedit is 36 items and 33 items for Belkasoft.

Table 5. Comparison of Analysis Using Root Access in MOBILedit

Revealed Data	Amount of Revealed Data in MiChat	Amount of Revealed Data in SayHi Chat
Database File	14	5
Account Name	2	2
Contact List	18	6
Contact Number	2	0
Chat Logs	17	18
Location	1	1
Deleted Message	0	1
Suspect Avatar	0	1
Client Avatar	0	1
Image File	0	1
Video File	0	0

Table 6. Comparison of Analysis Using Root Access in Magnet Axiom

Revealed Data	Amount of Revealed Data in MiChat	Amount of Revealed Data in SayHi Chat
Database File	13	6
Account Name	2	2
Contact List	18	6
Contact Number	2	0
Chat Logs	18	18
Location	1	1
Deleted Message	1	1
Suspect Avatar	1	0
Client Avatar	1	0
Image File	0	1
Video File	0	1

Table 7. Comparison of Analysis Using Root Access in Belkasoft

Revealed Data	Amount of Revealed Data in MiChat	Amount of Revealed Data in SayHi Chat
Database File	13	5
Account Name	2	2
Contact List	18	6
Contact Number	2	0
Chat Logs	18	18
Location	1	1
Deleted Message	1	1
Suspect Avatar	0	0
Client Avatar	0	0
Image File	0	0
Video File	0	0

4. CONCLUSION

Based on the results without root access, MiChat managed to find evidence in the form of 2 avatars and can only be found using the Magnet Axiom tool. While the results for SayHi Chat on MOBILedit, Magnet Axiom, and Belkasoft managed to findings in the form of evidence of database files, conversation activities, and other evidence information. Meanwhile, specifically for Axiom Magnet tools, authentic evidence was found in the form of 1 picture (proof of transaction) and one video (proof of transaction).

Based on the results through rooting access, MiChat managed to find evidence in the form of 2 avatars, and this can only be found using the Magnet Axiom tool. Other pieces of evidence were found in the form of database files conversation activities accompanied by other supporting evidence. While the results for SayHi Chat on MOBILedit, Magnet Axiom, and Belkasoft managed to get findings in the form of evidence of database files, conversation activities, and other evidence. Especially for Magnet Axiom tools, authentic evidence was found in the form of an image file (proof of transaction) and one video file (proof of transaction). Especially for MOBILedit, you can find authentic evidence in the form of 1 image file and two avatars of suspect and client accounts.

The SayHi Chat evidence obtained through root access is more complete, and in more detail regarding the evidence obtained, it is different when without root access. While more evidence of MiChat was found when it was done with the smartphone rooting process. This is because the cases studied with processes without root access and root access have the aim of complementing each other in obtaining evidence. So that these two processes complement each other's shortcomings, based on the test results, it can be concluded that the recommended tool according to the used scenario is Magnet Axiom.

REFERENCES

[1] A. Okutan and Y. Çebi, "A Framework for Cyber Crime Investigation," *Procedia Comput. Sci.*, vol. 158, pp. 287–294, Jan. 2019. https://doi.org/10.1016/j.procs.2019.09.054
[2] Q. Do, B. Martini, and K. K. R. Choo, "The role of the adversary model in applied security research," *Comput. Secur.*, vol. 81, pp. 156–181, Mar. 2019. https://doi.org/10.1016/j.cose.2018.12.002
[3] M. M. Singh and A. A. Bakar, "A Systemic Cybercrime Stakeholders Architectural Model," *Procedia Comput. Sci.*, vol. 161, pp. 1147–1155, Jan. 2019. https://doi.org/10.1016/J.PROCS.2019.11.227
[4] U. Hur, M. Park, G. Kim, Y. Park, I. Lee, and J. Kim, "Data acquisition methods using backup data decryption of Sony smartphones," *Digit. Investig.*, vol. 31, p. 200890, Dec. 2019. https://doi.org/10.1016/j.fsidi.2019.200890
[5] X. Lin, T. Chen, T. Zhu, K. Yang, and F. Wei, "Automated forensic analysis of mobile applications on Android devices," *Digit. Investig.*, vol. 26, pp. S59–S66, 2018. https://doi.org/10.1016/j.diin.2018.04.012
[6] M. Rath, B. Pati, and B. K. Pattanayak, "An Overview on Social Networking: Design, Issues, Emerging Trends, and Security," *Soc. Netw. Anal.*, pp. 21–47, Jan. 2019. https://doi.org/10.1016/B978-0-12-815458-8.00002-5
[7] M. Bas Seyyar and Z. J. M. H. Geradts, "Privacy impact assessment in large-scale digital forensic investigations," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 200906, Jun. 2020. https://doi.org/10.1016/j.fsidi.2020.200906
[8] M. de Gruijter and C. J. de Poot, "Cognitive challenges at the crime scene: The importance of social science research when introducing mobile technologies at the crime scene," *Forensic Sci. Int.*, vol. 297, pp. e16–e18, Apr. 2019. https://doi.org/10.1016/J.FORSCIINT.2019.01.026
[9] W. J. Buchanan, S. Chiale, and R. Macfarlane, "A methodology for the security evaluation within third-party Android Marketplaces," *Digit. Investig.*, vol. 23, pp. 88–98, 2017. https://doi.org/10.1016/j.diin.2017.10.002
[10] C. Hargreaves and A. Marshall, "SyncTriage: Using synchronisation artefacts to optimise acquisition order," *Digit. Investig.*, vol. 28, pp. S134–S140, Apr. 2019. https://doi.org/10.1016/j.diin.2017.10.002
[11] C. M. S. Steel, E. Newman, S. O. Rourke, and E. Quayle, "Forensic Science International : Digital Investigation An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 300971, 2020. https://doi.org/10.1016/j.fsidi.2020.300971
[12] J. Choi, J. Yu, S. Hyun, and H. Kim, "Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger," *Digit. Investig.*, vol. 28, pp. S50–S59, Apr. 2019. https://doi.org/10.1016/j.diin.2019.01.011
[13] G. Cornelis, R. Seelt, and N. Le-khac, "Forensic Science International : Digital Investigation Forensic analysis of Matrix protocol and Riot . im application," *Forensic Sci. Int. Digit. Investig.*, vol. 36, p. 301118, 2021. https://doi.org/10.1016/j.fsidi.2021.301118
[14] M. Nicoletti and M. Bernaschi, "Forensic analysis of Microsoft Skype for Business," *Digit. Investig.*, vol. 29, pp. 159–179, Jun. 2019. https://doi.org/10.1016/j.diin.2019.03.012
[15] D. Wijnberg and N. Le-khac, "Forensic Science International : Digital Investigation Identifying interception possibilities for WhatsApp communication," *Forensic Sci. Int. Digit. Investig.*, vol. 38, p. 301132, 2021. https://doi.org/10.1016/j.fsidi.2021.301132
[16] Y. C. Tok, C. Wang, and S. Chattopadhyay, "Stitcher: Correlating digital forensic evidence on internet-of-things devices," *Forensic Sci. Int. Digit. Investig.*, vol. 35, p. 301071, Dec. 2020. https://doi.org/10.1016/j.fsidi.2020.301071
[17] J. Park, Y. H. Jang, and Y. Park, "New flash memory acquisition methods based on firmware update protocols for LG Android smartphones," *Digit. Investig.*, vol. 25, pp. 42–54, 2018. https://doi.org/10.1016/j.diin.2018.04.002

[18] H. Lee, T. Ermakova, V. Ververis, and B. Fabian, "Forensic Science International : Digital Investigation Detecting child sexual abuse material : A comprehensive survey," *Forensic Sci. Int. Digit. Investig.*, vol. 34, p. 301022, 2020. https://doi.org/10.1016/j.fsidi.2020.301022
[19] C. H. Ngejane, J. H. P. Eloff, T. J. Sefara, and V. N. Marivate, "Forensic Science International : Digital Investigation Digital forensics supported by machine learning for the detection of online sexual predatory chats," *Forensic Sci. Int. Digit. Investig.*, vol. 36, p. 301109, 2021. https://doi.org/10.1016/j.fsidi.2021.301109
[20] K. Dwi, O. Mahendra, and I. K. Ari, "Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases," vol. 9, no. 3, pp. 381–390, 2021. https://doi.org/10.24843/JLK.2021.v09.i03.p09
[21] N. Dwi, W. Cahyani, D. Ph, K. R. Choo, and D. Ph, "DIGITAL & MULTIMEDIA SCIENCES An Evidence-based Forensic Taxonomy of Windows Phone Dating Apps," no. 7, 2018. https://doi.org/10.1111/1556-4029.13820
[22] A. Phan, K. Seigfried-Spellar, and K.-K. R. Choo, "Threaten me softly: A review of potential dating app risks," *Comput. Hum. Behav. Reports*, vol. 3, p. 100055, Jan. 2021. ttps://doi.org/10.1016/j.chbr.2021.100055
[23] E. Casey, "Maturation of digital forensics," *Digit. Investig.*, vol. 29, pp. A1–A2, Jun. 2019. https://doi.org/10.1016/j.diin.2019.05.002
[24] D. Kim and S. Lee, "Forensic Science International : Digital Investigation Study of identifying and managing the potential evidence for effective Android forensics," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 200897, 2019. https://doi.org/10.1016/j.fsidi.2019.200897
[25] P. Mullan, C. Riess, and F. Freiling, "Forensic source identification using JPEG image headers: The case of smartphones," *Digit. Investig.*, vol. 28, pp. S68–S76, Apr. 2019. https://doi.org/10.1016/j.diin.2019.01.016
[26] G. Horsman, "Digital Evidence Certainty Descriptors (DECDs)," *Forensic Sci. Int. Digit. Investig.*, vol. 32, p. 200896, Mar. 2020. https://doi.org/10.1016/j.fsidi.2019.200896
[27] E. Casey, "Strengthening trust: Integration of digital investigation and forensic science," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 301000, Jun. 2020. https://doi.org/10.1016/j.fsidi.2020.301000
[28] E. Gentry and M. Soltys, "SEAKER: A mobile digital forensics triage device," *Procedia Comput. Sci.*, vol. 159, pp. 1652–1661, 2019. https://doi.org/10.1016/j.procs.2019.09.335
[29] R. O. Andrade and S. G. Yoo, "Cognitive security: A comprehensive study of cognitive science in cybersecurity," *J. Inf. Secur. Appl.*, vol. 48, p. 102352, Oct. 2019. https://doi.org/10.1016/j.jisa.2019.06.008
[30] N. Akatyev and J. I. James, "Evidence identification in IoT networks based on threat assessment," *Futur. Gener. Comput. Syst.*, vol. 93, pp. 814–821, Apr. 2019. https://doi.org/10.1016/j.future.2017.10.012
[31] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," vol. 5, no. 2, pp. 235–247, 2018. https://doi.org/10.15294/sji.v5i2.16545
[32] G. Kim, M. Park, S. Lee, Y. Park, I. Lee, and J. Kim, "Forensic Science International : Digital Investigation A study on the decryption methods of telegram X and BBM-Enterprise databases in mobile and PC," *Forensic Sci. Int. Digit. Investig.*, vol. 35, p. 300998, 2020. https://doi.org/10.1016/j.fsidi.2020.300998
[33] G. Horsman, "Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework," *Digit. Investig.*, vol. 28, pp. 146–151, Mar. 2019. https://doi.org/10.1016/j.diin.2019.01.007
[34] G. Kim, S. Kim, M. Park, Y. Park, I. Lee, and J. Kim, "Forensic Science International : Digital Investigation Forensic analysis of instant messaging apps : Decrypting Wickr and private text messaging data," *Forensic Sci. Int. Digit. Investig.*, vol. 37, p. 301138, 2021. https://doi.org/10.1016/j.fsidi.2021.301138
[35] T. Wu, F. Breitinger, and S. O'Shaughnessy, "Digital forensic tools: Recent advances and enhancing the status quo," *Forensic Sci. Int. Digit. Investig.*, vol. 34, p. 300999, Sep. 2020. https://doi.org/10.1016/j.fsidi.2020.300999
[36] E. OliveiraJr, A. F. Zorzo, and C. V. Neu, "Towards a conceptual model for promoting digital forensics experiments," *Forensic Sci. Int. Digit. Investig.*, vol. 35, p. 301014, Dec. 2020. https://doi.org/10.1016/j.fsidi.2020.301014
[37] G. Tully, N. Cohen, D. Compton, G. Davies, R. Isbell, and T. Watson, "Quality standards for digital forensics: Learning from experience in England & Wales," *Forensic Sci. Int. Digit. Investig.*, vol. 32, p. 200905, Mar. 2020. https://doi.org/10.1016/j.fsidi.2020.200905
[38] R. Yokota, Y. Hawai, K. Tsuchiya, D. Imoto, M. Hirabayashi, N. Akiba, H. Kakuda, K. Tanabe, M. Honma, and K. Kurosawa, "A revisited visual-based geolocalization framework for forensic investigation support tools," *Forensic Sci. Int. Digit. Investig.*, vol. 35, p. 301088, Dec. 2020. https://doi.org/10.1016/j.fsidi.2020.301088
[39] M. Guido, J. Buttner, and J. Grover, "Rapid differential forensic imaging of mobile devices," *DFRWS 2016 USA - Proc. 16th Annu. USA Digit. Forensics Res. Conf.*, vol. 18, pp. S46–S54, 2016. https://doi.org/10.1016/j.diin.2016.04.012
[40] C. Jin, R. Wang, and D. Yan, "Source smartphone identification by exploiting encoding characteristics of recorded speech," *Digit. Investig.*, vol. 29, pp. 129–146, Jun. 2019. https://doi.org/10.1016/j.diin.2019.03.003
[41] M. Park, O. Yi, and J. Kim, "A methodology for the decryption of encrypted smartphone backup data on android platform: A case study on the latest samsung smartphone backup system," *Forensic Sci. Int. Digit. Investig.*, vol. 35, p. 301026, Dec. 2020. https://doi.org/10.1016/j.fsidi.2020.301026
[42] P. Feng, Q. Li, P. Zhang, and Z. Chen, "Logical acquisition method based on data migration for Android mobile devices," *Digit. Investig.*, vol. 26, pp. 55–62, 2018. https://doi.org/10.1016/j.diin.2018.05.003
[43] J. Wagner, A. Rasin, K. Heart, R. Jacob, and J. Grier, "DB3F & DF-Toolkit: The Database Forensic File Format and the Database Forensic Toolkit," *Digit. Investig.*, vol. 29, pp. S42–S50, Jul. 2019.

https://doi.org/10.1016/j.diin.2019.04.010
[44] A. Fukami, R. Stoykova, and Z. Geradts, "A new model for forensic data extraction from encrypted mobile devices," *Forensic Sci. Int. Digit. Investig.*, vol. 38, p. 301169, 2021. https://doi.org/10.1016/j.fsidi.2021.301169
[45] L. F. Sikos, "Packet analysis for network forensics: A comprehensive survey," *Forensic Sci. Int. Digit. Investig.*, vol. 32, p. 200892, Mar. 2020. https://doi.org/10.1016/j.fsidi.2019.200892
[46] G. Horsman and N. Sunde, "Part 1: The need for peer review in digital forensics," *Forensic Sci. Int. Digit. Investig.*, vol. 35, p. 301062, Dec. 2020. https://doi.org/10.1016/j.fsidi.2020.301062
[47] T. Holt and D. S. Dolliver, "Forensic Science International : Digital Investigation Exploring digital evidence recognition among front-line law enforcement of fi cers at fatal crash scenes," *Forensic Sci. Int. Digit. Investig.*, vol. 37, p. 301167, 2021. https://doi.org/10.1016/j.fsidi.2021.301167
[48] K. Opasiak and W. Mazurczyk, "(In)Secure Android Debugging: Security analysis and lessons learned," *Comput. Secur.*, vol. 82, pp. 80–98, May 2019. https://doi.org/10.1016/j.cose.2018.12.010
[49] E. Casey, "Interrelations between digital investigation and forensic science," *Digit. Investig.*, vol. 28, pp. A1–A2, Mar. 2019. https://doi.org/10.1016/j.diin.2019.03.008
[50] D. Mothi, H. Janicke, and I. Wagner, "A novel principle to validate digital forensic models," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 200904, Jun. 2020. https://doi.org/10.1016/j.fsidi.2020.200904
[51] R. M. Carew and D. Errickson, "Imaging in forensic science: Five years on," *J. Forensic Radiol. Imaging*, vol. 16, pp. 24–33, Mar. 2019. https://doi.org/10.1016/j.jofri.2019.01.002
[52] T. Latzo, R. Palutke, and F. Freiling, "A universal taxonomy and survey of forensic memory acquisition techniques," *Digit. Investig.*, vol. 28, pp. 56–69, Mar. 2019. https://doi.org/10.1016/j.diin.2019.01.001
[53] G. Singh and K. Singh, "Digital image forensic approach based on the second-order statistical analysis of CFA artifacts," *Forensic Sci. Int. Digit. Investig.*, vol. 32, p. 200899, Mar. 2020. https://doi.org/10.1016/j.fsidi.2019.200899
[54] R. M. A. Mohammad, "An Enhanced Multiclass Support Vector Machine Model and its Application to Classifying File Systems Affected by a Digital Crime," *J. King Saud Univ. - Comput. Inf. Sci.*, Oct. 2019. https://doi.org/10.1016/j.jksuci.2019.10.010
[55] W. Jo, Y. Shin, H. Kim, D. Yoo, D. Kim, C. Kang, J. Jin, J. Oh, B. Na, and T. Shon, "Digital Forensic Practices and Methodologies for AI Speaker Ecosystems," *Digit. Investig.*, vol. 29, pp. S80–S93, Jul. 2019. https://doi.org/10.1016/j.diin.2019.04.013
[56] P. Sharma, D. Arora, and T. Sakthivel, "Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 907–917, 2020. https://doi.org/10.1016/j.procs.2020.03.390
[57] S. J. Yang, J. H. Choi, K. B. Kim, R. Bhatia, B. Saltaformaggio, and D. Xu, "Live acquisition of main memory data from Android smartphones and smartwatches," *Digit. Investig.*, vol. 23, pp. 50–62, 2017. https://doi.org/10.1016/j.diin.2017.09.003
[58] G. S. Morrison and F. Kelly, "A statistical procedure to adjust for time-interval mismatch in forensic voice comparison," *Speech Commun.*, vol. 112, pp. 15–21, Sep. 2019. https://doi.org/10.1016/j.specom.2019.07.001
[59] G. Horsman, "Opinion: Does the field of digital forensics have a consistency problem?," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 300970, Jun. 2020. https://doi.org/10.1016/j.fsidi.2020.300970
[60] A. Fukami and K. Nishimura, "Forensic analysis of water damaged mobile devices," *Digit. Investig.*, vol. 29, pp. S71–S79, 2019. https://doi.org/10.1016/j.diin.2019.04.009
[61] G. Humphries, R. Nordvik, H. Manifavas, P. Cobley, and M. Sorell, "Law Enforcement educational challenges for mobile forensics," *Digit. Investig.*, vol. 38, p. 301129, 2021. https://doi.org/10.1016/j.fsidi.2021.301129