PAPER NAME	AUTHOR
10. MTI-60181103-Syfa3.pdf	Syifa Riski Ardiningtias

WORD COUNT	CHARACTER COUNT
4119 Words	23441 Characters

PAGE COUNT	FILE SIZE
18 Pages	755.5KB

SUBMISSION DATE	REPORT DATE
Apr 4, 2023 12:41 PM GMT+7	Apr 4, 2023 12:42 PM GMT+7

● **23% Overall Similarity**

The combined total of all matches, including overlapping sources, for each database.

- 21% Internet database
- Crossref database
- 0% Submitted Works database

- 10% Publications database
- Crossref Posted Content database

● **Excluded from Similarity Report**

- Bibliographic material
- Cited material

- Quoted material
- Manually excluded sources

A Comparative Analysis of Digital Forensic Investigation Tools on Facebook Messenger Applications

Sunardi[1], Herman[2] and Syifa Riski Ardiningtias[2,*]

[1]*Department of Electrical Engineering, Ahmad Dahlan University, Yogyakarta-55166, Indonesia*
[2]*Master in Informatics, Ahmad Dahlan University, Yogyakarta-55164, Indonesia*
E-mail: Sunardi@mti.uad.ac.id; Hermankaha@mti.uad.ac.id; Srqa.riski@gmail.com
Corresponding Author

Abstract

Technological developments make it easier for people to communicate and share information. Facebook Messenger is an instant messenger that contains multi-platform for sending text, image, sound, and video messages. Besides being used for positive purposes, this technology can also be used to carry out harmful activities. This study conducts a forensic investigation on a crime simulation in pornographic content distribution using Facebook Messenger as a communication medium on Android smartphones. Perpetrators communicate and send pornographic content in the shape of conversations, audio, and video, then delete them to eliminate traces. Every crime can leave evidence therefore after erasing the track, it can be revealed through digital forensic investigations on the smartphone devices that are used as objects to find digital evidence. The collection of evidence in this study is used four forensic tools with the research stages the National Institute of Justice (NIJ) framework. The study result can be used as evidence by

investigators on handling criminal cases with the results obtained in the shape of application versions, accounts, emails, conversation, time of occurrence, pictures, audio, and video. MOBILedit Forensic Express has an accuracy of 84.85%, Wondershare Dr. Fone 36.36%, Magnet Axiom 75.76%, and Belkasoft Evidence Center 69.70%.

Keywords: National Institute of Justice, media social, Facebook Messenger, fraud.

1 Introduction

Facebook, the popular online social network, has changed our lives. Users can create a customized profile to share information with others that have agreed to be their friend [1]. Twitter, Facebook, Instagram etc. rank both in top ten downloaded apps or frequently visited sites. Simplicity, with no cost account creation and usage, has attracted masses in huge numbers towards these sites [2].

In the information era, society actively uses information and communication, automating various branches of production, creating integrative communication systems, increasing sources and carriers of information leading to transformation [3]. Technological advances allow the interaction process between humans to reach all levels of society in any part of the world. Internet, one of most the technological developments, can be used to find out the culture of society [4]. Besides their benefits advances in technology advances also have negative effects in the form of criminal cases along with the use of social media. Figure 1 shows the number of smartphone user 2016-2023 in worldwide.

Every year, the number of criminal cases in cyberspace was growths. The internet has influenced social lifestyle, education, and even community activities. One of the negative consequences of technology is a crime. The term cybercrime refers to the misuse of the internet and social media. In 2015, cybercrime cost is $3 trillion globally [5].

Facebook is one of the mainstream social networking sites. Millions of users publish daily billions of posts through them, as they are freely accessible and provide low publication barriers for both posting and viewing information [6]. Facebook Messenger is an instant messaging application with a third-party application. In Figure 2, it can be seen from the growth in the immense number of users in the world, which also opens up opportunities for communication media for harmful purposes.
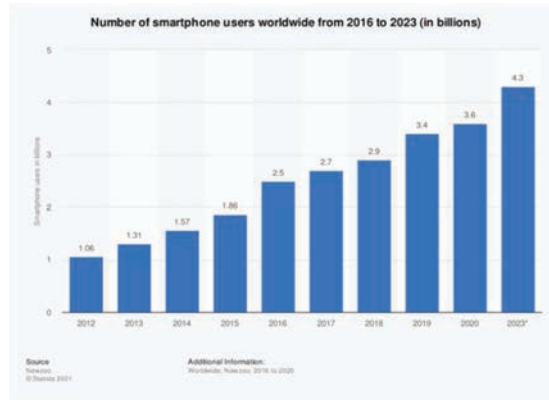
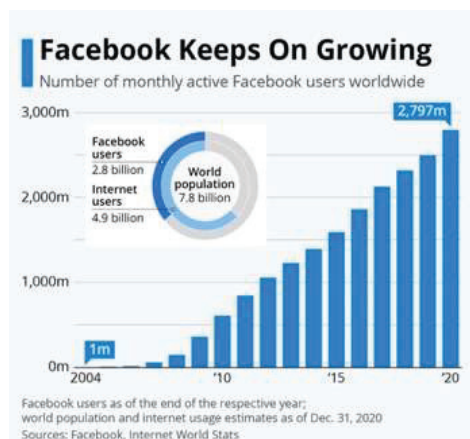**Figure 1** Number of Smartphone user worldwide.

Figure 2 Number of Smartphone user worldwide.

Rapid technological growth was accompanied by the increase of social media starting in 2014. Then, instant messaging applications have launched cybercrimes and crucial harmful effect activities. Facebook Messenger is an instant messaging application widely used with 2.13 billion monthly active users [7] easy to use and create an account, especially in spreading pornography, defamation, and fraud.

Previous research conducted digital forensic on Facebook Messenger using the National Institute of Justice (NIST) framework. The Galaxy V+ SMG31HZ android mobile phone carried out the rooting method, installed Facebook Messenger, created messages, and do an investigation using a

forensic software tool called Oxygen Forensics. The analysis results are reported as evidence. The NIST framework is used to analyze for digital track or steps in obtaining information from evidence [8].

This study conducted a digital investigation by comparing four forensic tools, these are MOBILedit Forensic, Wondershare Dr. Fone, Magnet Axiom, and Belkasoft Evidence Center, to extract evidence from the instant messaging application Facebook Messenger. Forensic simulations were implemented in cases of pornography spread using the Facebook Messenger application as a communication medium on Android-based smartphones. Criminals wipe in-app data to eliminate traces. The evidence sought are pictures, videos, accounts, conversations, emails, time of occurrence, and voice messages.

2 Material and Method

This study employs the National Institute of Justice (NIJ) digital forensic framework to obtain digital evidence and record the available information, then collected by implementing a centralized data mechanism. Forensic investigations are designed to obtain evidence using various forensic tools to collect complete results.

Maintaining evidence and competences of cyber perpetrators so that they are used for evidence in court is the goal of digital forensics. Forensic investigations with the NIJ framework have several stages, as shown in Figure 3.

The stages of NIJ are described as shown in Figure 3:

(1) Preservation, making efforts to maintain the authenticity and security of discovered evidence so it would not be changed or lost.
(2) Collection, carrying out data collection activities to assist all the investigation process, to find evidence.
(3) Examination, investigating the available data by automatic or manual forensic processes and determining whether the files obtained are authentic.
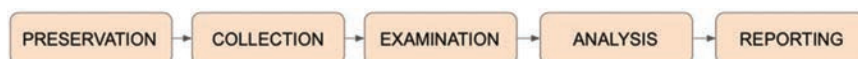(4) Analysis, document extraction that aims to ensure significant and valuable evidence in the verification.

PRESERVATION → COLLECTION → EXAMINATION → ANALYSIS → REPORTING

Figure 3   Stages of NIJ method.

(5) Reporting, making reports from digital evidence obtained through the inspection and analysis process.

The next inspection stage broke down into several parts, such as identification. Identification is to find data or artifacts to be retrieved and possibly produce evidence to assist the investigation. After determining the data or artifacts to be recovered, proceed to the data retrieval process [8].

2.1 Case Scenario

The study was carried out by simulating pornographic crime cases, as illustrated in Figure 4. The simulation process is required to determine the chronological sequence of circumstances indicated by the spread of pornography.

Based on the case simulation, two users use Facebook Messenger to communicate. User A is the sender and considered as attacker while user B is the message recipient and victim of the crime.

In this simulation, User A uses a Samsung J2 Prime smartphone, while user B uses a Samsung J7 Prime smartphone. They have Facebook's accounts to communicate each other such as sending chats and photos through the Facebook Messenger feature. User A sends messages exposing pictures of women wearing revealing clothes to user B. Then, user A immediately deletes everything to eliminate evidence. User B, as a victim, reports to the authorities for the incident experienced.
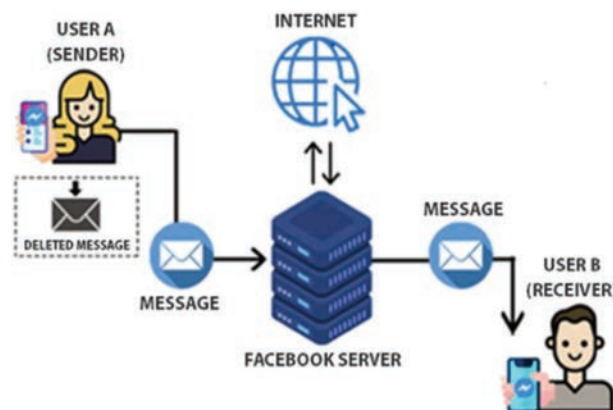

Figure 4   The chronology of Facebook Messenger communication activities.

Table 1   Research data variable

No.	Variables	Quantity
1	Application version	1
2	Account	9
3	Email	1
4	Conversation	1
5	Time of occurrence	1
6	Picture	3
7	Video	1
8	Audio	1
9	Url	1
10	IP Address	1
11	Location	1

In response to user B's report, the authorities issued a search warrant to user A to secure the smartphone managed to access Facebook Messenger and communicate with user B as electronic evidence. For the procedure afterward, an investigation of user A's smartphone is conducted. The return of digital proof is verified on the smartphone of user B (victim) to ensure that the evidence on the smartphone of user A (perpetrator) exists and is the same as that received by user B.

Hereafter, the case showing the crime of spreading pornography continues in court. Based on the chronological simulation of the circumstance indicated by the pornography crime, the NIJ method can be applied using the following step. The variable of investigation of evidence and its amount, as shown in Table 1, is the focus of inspection of evidence.

Based on the data variables researched, a forensic investigation is conducted to obtain the desired digital evidence.

2.2 Digital Forensic

The use of scientifically proven methods for the preservation, collection, validation, identification, analysis, and interpretation of evidence derived from digital sources is known as digital forensics. Digital forensic investigations have evolved with the passage of time and it's impacted by many externalities [9].

Digital forensics, a field of technology and knowledge discipline, is beneficial for proving the law on criminal acts with negative technology or cybercrime according to scientific rules so that digital evidence is essential to winning the court in having the strong ones [10].

2.3 Facebook Messenger

Facebook recently changed its name after almost two decades and is now referred to as Meta [11]. The changes do not apply to its platforms, such as Facebook, Instagram, and WhatsApp, but only the parent company owns them [12].

Facebook released an instant messaging application for mobile, Facebook Messenger, with nearly 1.2 billion active users in 2008–2020 [13]. The fast-growing market for instant messaging applications has resulted in the decline of traditional cellular operators' revenues. Facebook Messenger is an instant messaging application that can send text, images, video, and audio. This application is compatible with Android, Blackberry, and Windows smartphones. The Facebook Messenger application allows its users to send messages to other users effortlessly.

2.4 Digital Evidence

Digital evidence related to mobile, such as smartphones, can be found in call history, phonebooks, SMS, MMS, photo, audio, video, and others [14]. In general, digital evidence is related to social media as a place to commit crimes so that it is used to aid in the prosecution of cybercrime. Digital evidence is prone to changes that create doubts about its authenticity if not handled appropriately. Any form of alteration of evidence can lead to wrong conclusions and unacceptable evidence. Therefore, it is essential to maintain the validity of digital evidence [15].

2.5 MOBILedit Forensic

MOBILedit Forensic Express is a mobile device forensics tool that can recover deleted data, contact details, chats, graphic files, call information, IMEI, multimedia messages, calendar items, data files, and passwords [16]. MOBILedit can extract application cache history and web browser data from various installed applications such as Skype, Dropbox, Facebook, WhatsApp, etc. [17].

2.6 Wondershare Dr. Fone

Wondershare Dr. Fone for Android is a computer application to restore accidentally deleted or formatted data on Android smartphone devices. Wondershare is an application to restore deleted data in the shape of messages, contacts, call logs, photos, videos, audios, and documents.

Wondershare installation is very easy because users can directly install it on a PC or laptop. Wondershare application is compatible with all operating systems and Windows 10 [18].

2.7 Magnet Axiom

AXIOM Magnet is a forensic software produced by Magnet Forensic that can process and prepare digital evidence on smartphones and computers into a report document. AXIOM Magnet is an examination tool that helps forensic professionals. Professionals in the digital forensics field used AXIOM Magnets to search for evidence that other forensic applications cannot find, verify data, and integrate images obtained by other tools into a report document for the examination process.

AXIOM Magnet is the production investigation platform of Magnet Forensics, one of the global leaders in digital forensic software development that receives, examines, and allocates information from computers, smartphones, and tablets [19].

2.8 Belkasoft Evidence Center

Belkasoft Evidence Center can obtain, search, analyze, and store various evidence found on a smartphone or computer. This forensic tool extract digital evidence from different sources and then examine hard drive storage, BlackBerry, and android backup afterward by automatically analyzing the data source and then storing it in a report [20].

2.9 Tools and Material

The process to obtain evidence on smartphones is carried out using the forensic tools of MOBILedit Forensic, Wondershare Dr. Fone, Magnet Axiom, and Belkasoft Evidence Center, as shown in Table 2 While Table 3 is list of the tools needed in this study.

Table 2   Forensic tools

No	Forensic Tools	Version
1	MOBILedit Forensic	7.2
2	Wondershare Dr. Fone	10.7.2
3	Magnet Axiom	3.1.1
4	Belkasoft Evidence Center	V.1.8

Table 3 Hardware material

No	Hardware	Description
1	Samsung J2 Prime	Android Lolipop, Experiment Device
2	Xiaomi 5 Plus	Android Oreo, Experiment Device
3	Vivo 1718	Android Oreo, Experiment Device
4	Laptop Intel 5-7210 200 GB RAM	Windows 10 64 bit, Workstation
5	USB Connector	Media Connecting smartphone with workstation

Figure 5   Evidence isolation.

3 Result and Discussion

3.1 Preservation Stage

The preservation is the stage of maintaining the authenticity and maintenance of evidence. The steps are conducted by isolating the device to prevent outgoing and incoming data. Isolation techniques are implemented to prevent any damage on digital evidence. The isolation is also important to maintain authenticity of the documents on the device. The preservation stage is done by changing the device condition into airplane mode, as shown in Figure 5.

The isolation process is critical in determining the possibilities for changes to data on the device that could affect the authenticity of digital evidence.

3.2 Collection Stage

At the collection stage, evidence on smartphones is prone to damage, documents and other digital evidence in the device can be lost or corrupted so that the data is illegible. Figure 6 is the process of collecting data with forensic tools.

Belkasoft Evidence Center can perform system backups and data collection on smartphone devices and then extract them as shown in Figure 6.
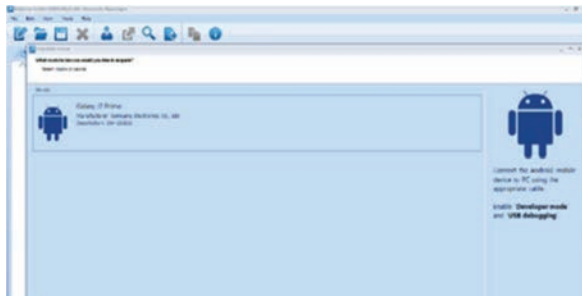
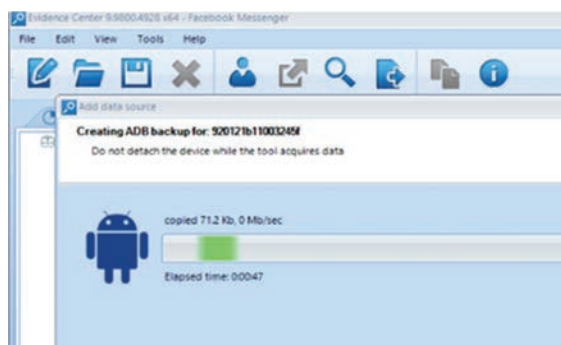**Figure 6**   Collection process on Belkasoft evidence center.

Figure 7   Backup data information.

Figure 8   Collection data information.

The results of the process backup are obtained in the form of document files sourced from within the smartphone with the .mfdb extension. The results of the backup and collection process are as shown in Figure 8.

3.3 Examination Stage

The examination stage in this study uses forensic tools. This test checks and generates data that includes files and directories stored on the smartphone.

Figure 9 Examination result with forensic tools.

Figure 10 Smartphone Samsung information report.

The data contains files in the mobile device memory associated with the instant messaging application Facebook Messenger.

In order to get digital evidence on Android specifically related to artifacts in the Facebook Messenger application, the main thing that is needed is to know the location where Facebook Messenger is placed. The data extraction result using MOBILedit Forensic, Wondershare Dr. Fone, Magnet Axiom, and Belkasoft Evidence Center obtained data on smartphone storage. Figure 9 show the results of data extraction.

3.4 Analysis Stage

The next step is to look for evidence, pictures, videos, and other supporting evidence. Based on the obtained extraction results that have been obtained, which contain the application version, time of occurrence, account, email, location, IP Address, conversation, image, video, and audio on Facebook Messenger. In addition to the specifications, other information such as time zone, IMEI, Storage, and others, is also obtained, as shown in Figures 10, 11, and 12.

Evidence of deleted chat data or conversations can also be known and displayed again, making it easier to locate previously deleted evidence. Figure 13 shows evidence of a deleted chat conversation.

Figure 11   Smartphone Xiaomi information report.

Figure 12   Smartphone Vivo information report.

Figure 13   Smartphone information report.

The digital evidence extraction process results show one of the Facebook Messenger accounts used. It contains three selfies, a video of a woman with pornographic elements, and a conversation. This proves that there are elements that lead to cases of pornography. In addition to conversation evidence, photo evidence deleted from Facebook Messenger can also be obtained, as shown in Figures 14, 15, 16 and video evidence is shown in Figure 17.

Digital investigations were carried out to recover deleted criminal activity data. The evidence will be obtained using Forensic tools. Finally, each tool is used to measure the accuracy of each tool used in the ability to obtain digital evidence.

Figure 14 Evidence in photo.

Figure 15 Evidence in photo.

Figure 16 Evidence in photo.

3.5 Reporting

After analyzing the evidence on the perpetrator's smartphone and cross-referencing it with the proof on the victim's smartphone, it is possible to conclude that related digital artifacts as evidence were obtained using
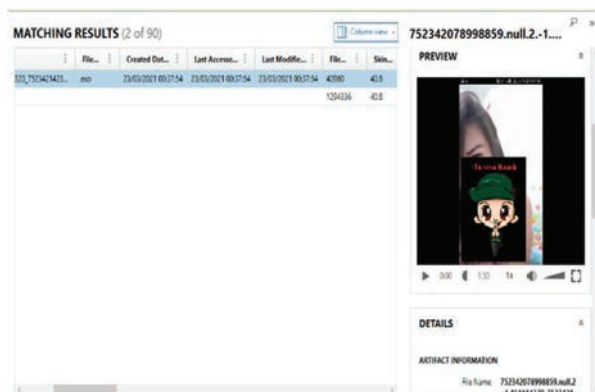
Figure 17   Evidence in video.

Android forensics. Digital artifacts, evidence of the spread and upload of images and videos carried out by suspects and users of pornography services, were obtained based on the scenarios and simulations carried out.

Table 4 provides an overview of some data after the testing and analysis process on three different smartphones, especially on the Facebook Messenger application. Collecting data process with mobile forensic tools, namely MOBILedit Forensics, Wondershare Dr. Fone, AXIOM Magnet, and Belkasoft Evidence Center. Table 4 shows that the four forensic tools used have different features. For example, data extraction accuracy as in Table 4, mobile forensic tool MOBILedit Forensics Express has a value of 90.9%, Wondershare Dr. Fone is 27.27%, AXIOM Magnet is 81.81%, and Belkasoft Evidence Center is 72.72%.

Table 4   Extraction result with forensic tools

Phone Type	Artefact Type	MOBILedit Forensic	Wondershare Dr. Fone	AXIOM Magnet	Belkasoft Evidence C.
Samsung	App. Ver.	304.2.0.17.118	304.2.0.17.118	304.2.0.17.118	304.2.0.17.118
J2 Prime	Account	100062123935886	Unavailable	100062123935886	Unavailable
	Email	Available	Unavailable	Available	Unavailable
	Conver.	Available	Unavailable	Unavailable	Available
	Times	Available	Unavailable	Available	Unavailable
	Doc.	Available	Unavailable	Available	Available
	Picture	Available	Available	Available	Available
	Video	Available	Available	Available	Available
	Audio	Unavailable	Unavailable	Unavailable	Available
	Location	Available	Unavailable	Available	Available

(*Continued*)

Table 4   Continued

Phone Type	Artefact Type	MOBILedit Forensic	Wondershare Dr. Fone	AXIOM Magnet	Belkasoft Evidence C.
	IP Addr.	Available	Unavailable	Available	Available
	Total	10	3	9	8
Xiaomi Redmi 5 Plus	App. Ver.	350.0.0.9.89	350.0.0.9.89	350.0.0.9.89	350.0.0.9.89
	Account	100062123935886	Unavailable	100062123935886	100062123935886
	Email	Available	Unavailable	Available	Unavailable
	Conver.	Available	Unavailable	Unavailable	Available
	Times	Available	Unavailable	Available	Unavailable
	Doc.	Available	Unavailable	Unavailable	Available
	Picture	Available	Available	Available	Available
	Video	Available	Available	Available	Available
	Audio	Unavailable	Unavailable	Unavailable	Available
	Location	Unavailable	Unavailable	Available	Unavailable
	IP Addr.	Available	Available	Available	Available
	Total	9	4	8	8
Vivo 1718	App. Ver.	350.0.0.9.89	350.0.0.9.89	350.0.0.9.89	350.0.0.9.89
	Account	100062123935886	100062123935886	100062123935886	Unavailable
	Email	Available	Unavailable	Available	Unavailable
	Conver.	Available	Unavailable	Unavailable	Available
	Times	Available	Unavailable	Available	Unavailable
	Doc.	Available	Available	Available	Available
	Picture	Available	Available	Unavailable	Available
	Video	Available	Available	Available	Unavailable
	Audio	Unavailable	Unavailable	Unavailable	Available
	Location	Available	Unavailable	Available	Available
	IP Addr.	Unavailable	Unavailable	Available	Available
	Total	9	5	8	7
	Accuracy (%)	84.85	36.36	75.76	69.70

4 Conclusion

Based on the research conducted following the NIJ framework using MOBILedit Forensic tools, Wondershare Dr. Fone, Magnet Axiom, and Belkasoft Evidence Center was able to conduct forensic investigations toward Facebook Messenger, an Android instant messenger application. The results obtained from the research can be used for evidence by investigators in handling criminal cases and as a reference for investigators in looking for evidence in the spreading of pornographic content cases on the Facebook Messenger application. MOBILedit Forensic Express has the highest accuracy of 84.85%, while Wondershare Dr. Fone is 36.36%, Magnet Axiom is 75.76%, and Belkasoft Evidence Center is 69.70%. Further research can be carried out using forensic tools and other possible methods to complement each other and get the best results.

References

[1] M. Albayati. and A. Altamimi, "Identifying Fake Facebook Profiles Using Data Mining Techniques," *Journal of ICT Research and Applications*, vol. 13, no. 2, pp. 107–117, 2019.

[2] N. Shetty, B. Muniyal and A. Anand, "An Enhanced Sybil Guard to Detect Bots in Online Social Networks," *Journal of Cyber Security and Mobility*, vol. 9, no. 2, pp. 203–236. 2018.

[3] N. Isachenko, "The Role of Information and Informational and Communication Technologies in Modern Society," *Utopía y Praxis Latinoamericana*, vol. 11, no. 1, pp. 105–126. 2021.

[4] D. Setiawan, "Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Budaya," *Journal SIMBOLIKA*, vol. 4, no. 1, pp. 62–72, 2018.

[5] M. Hsieh and S. Wang, "Routine Activities in a Virtual Space: A Taiwanese Case of an ATM Hacking Spree," *International Journal of Cyber Criminology*, vol. 12, no. 1, pp. 333–352, 2018.

[6] A. Tundish, L. Bock and V. Stanescu, "Experiencing the Detection of Radicalized Criminals on Facebook Social Network and Data-related Issues," *Journal of Cyber Security and Mobility*, vol. 9, no. 2, pp. 203–236. 2018.

[7] A. Pourkhani, K. Andipour, and B. Baher, "The impact of Social Media in Business Growth and Performance," *A Scientometrics Analysis. International Journal of Data and Network Science*, vol. 24, no. 1, pp. 223–244. 2019.

[8] D. Nieborg and A. Helmond, "The Political Economy of Facebook's Platformization in the Mobile Ecosystem: Facebook Messenger as a Platform Instance," *Sage Journal*, vol. 41, no. 2, pp. 196–218, 2018.

[9] E. Boateng, E. Bonsu, "Digital Forensic Investigations: Issues of Intangibility, Complications and Inconsistencies in Cyber Crime," *Journal of Cyber Security and Mobility*, vol. 4, pp. 87–104. 2016.

[10] R. Umar, I. Riadi, and G. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *International Journal on Advanced Science Engineering Information Technology*, vol. 8, no. 3, pp. 949–955. 2018.

[11] G. Palmer, "A Road Map for Digital Forensic Research. 1st Digital Forensic Research Workshop", Utica, New York, pp. 27–30.

[12] Al-Azhar, M., "Digital Forensic, Panduan Praktis investigasi Komputer. Jakarta," Salemba Infotek, 2012.

[13] J. Clement, *Facebook: Number of Monthly Active Users Worldwide 2008–2020*, 2020.

[14] I. Riadi, A. Yudhana and M. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," *Scientific Journal of Informatics*, vol. 5, no. 2, pp. 235–247. 2018.

[15] H. Douglas and R. Fitzgerald, "Proving Non-Fatal Strangulation in Family Violence Cases: A Case Study Criminalisation of Family Violence," *The International Journal of Evidence & Proof*, vol. 25, no. 4, pp. 350–370, 2018.

[16] K. Gajjar and P. Sharma, "Android Based Mobile Forensic and Comparison Using Various Tools," *International Research Journal of Engineering and Technology (IRJET)*, vol. 7, no. 4, pp. 1399–1404, 2020.

[17] O. Osho and S. Ohida, "Comparative Evaluation of Mobile Forensic Tools. I.J. Information Technology and Computer Science," vol. 1, no. 1, pp. 74–83, 2016.

[18] Sunardi, I. Riadi and J. Triyanto, "Forensics Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice," *Journal of Information Technology and Computer Science (JOINTECS)*, vol. 3, no. 1, pp. 63–70, 2019.

[19] A. Doshi and P. Sharma, "Digital Forensics Analysis for Network Related Data," *International Research Journal of Engineering and Technology (IRJET)*, vol. 7, no. 4, pp. 1390–1398, 2020.

[20] I. Riadi, Sunardi and A. Firdonsyah, "Comparative Analysis of Forensic Software on Android-based Blackberry Messenger using NIJ Framework," *Proceeding of EECSI*, Malang – Indonesia, 2018.

Biographies

Sunardi graduated bachelor and master degree in Electrical Engineering from Universitas Gadjah Mada (Yogyakarta, Indonesia) and Institut Teknologi Bandung (Bandung, Indonesia) in 1999 and 2003 respectively.

Ph.D. degree received in Electrical Engineering from the Universiti Teknologi Malaysia (Johor Bahru, Malaysia) in 2011. Currently as lecturer at Univesitas Ahmad Dahlan (Yogyakarta, Indonesia). His expert on Data, Information, and Communication.

Herman graduated bachelor degree in Informatics from Perbanas (Jakarta, Indonesia). Master and Ph.D. degree received in Computer Science from Universiti Teknologi Malaysia (Johor Bahru, Malaysia). Currently as lecturer at Univesitas Ahmad Dahlan, (Yogyakarta, Indonesia). His expert on Mobile and Multimedia Technologies.

Syifa Riski Ardiningtias graduated bachelor degree in Computer Science from Universitas Muhammadiyah Purwokerto (Purwokerto, Indonesia) in 2019. Currently doing master in Informatics at Universitas Ahmad Dahlan (Yogyakarta, Indonesia). His research interest on Digital Forensic and Network Forensics.

● **23% Overall Similarity**

Top sources found in the following databases:

- 21% Internet database
- Crossref database
- 0% Submitted Works database

- 10% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	**journals.riverpublishers.com** Internet	**10%**
2	**knepublishing.com** Internet	**2%**
3	**ijcaonline.org** Internet	**2%**
4	**journal.universitasbumigora.ac.id** Internet	**1%**
5	**insightsociety.org** Internet	**<1%**
6	**Dongliang Bian, Jun Pan, Yanhui Wang. "Study of Encrypted Transmiss...** Crossref	**<1%**
7	**Imam Riadi, Herman, Nur Hamida Siregar. "Mobile Forensic Analysis o...** Crossref	**<1%**
8	**doaj.org** Internet	**<1%**

● **Excluded from Similarity Report**

- Bibliographic material
- Cited material

- Quoted material
- Manually excluded sources

EXCLUDED SOURCES

researchgate.net
Internet

95%

Sunardi, Herman, Syifa Riski Ardiningtias. "A Comparative Analysis of Digital ...
Crossref

95%