Available online to ejournal.pnc.ac.id

Journal of Innovation Information Technology and Application

Journal Page is available to https://ejournal.pnc.ac.id/index.php/jinita

Application of the NIST 800-86 Framework to Forensic Digital Evidence for Signal and Litmatch

Nurul Puspa Hapsari[1], *Bita Parga Zen*[2*]

[1,2] *Insitut Teknologi Telkom Purwokerto, Indonesia*

[1] *18102244@ittelkom-pwt.ac.id* , [2] *bita@ittelkom-pwt.ac.id*

ARTICLE INFO

Article history:
Received 31 July 2023
Revised 29 December 2023
Accepted 29 May 2024
Available online 28 June 2024

Keywords:
Signal
Litmatch
NIST 800-86
Digital Forensic
MobilEdit Forensic

IEEE style in citing this article:
N. Puspa Hapsari and B. Parga Zen, "Application of the NIST 800-86 Framework to Forensic Digital Evidence for Signal and Litmatch," Journal of Innovation Information Technology and Application (JINITA), vol. 6, no. 1, pp. 1–11, Jun. 2024.

ABSTRACT

Exchanging messages is a routine that cannot be avoided nowadays. With the development of technology, exchanging messages has become more accessible. What makes exchanging messages easier is the instant messaging application. Examples of instant messaging applications are the Signal and Litmatch applications. Apart from the positive impact of quickly exchanging messages, there are also negative impacts, such as threats, bullying and other crimes. With so many crimes occurring, digital forensic analysis is needed to search for and obtain evidence of digital crimes. This research was conducted to search for and get proof from the Signal and Litmatch applications by running case scenarios and using the National Institute of Standards and Technology (NIST) 800-86 method. The case scenario carried out in this research is making posts on the Litmatch application and sending text messages or images on the Signal and Litmatch applications. The results found in this research using the MOBILedit Forensic and Autopsy tools are images in the Signal and Litmatch applications.

1. INTRODUCTION

Exchanging messages is very easy to do at this time because of the rapid development of technology. However, apart from the positive impact of the ease of exchanging messages, there are also negative impacts, such as threats, bullying, drug trafficking, and other criminal acts. The thing that makes it easier to exchange messages at this time is the Instant Messaging (IM) application[1]. Examples of IM apps currently available are the Signal and Litmatch apps.

Signal is an application that can be used for free to exchange messages. The Signal application uses end-to-end encryption and a modern security system. The features of the Signal application are that users can exchange text messages, voice messages, pictures, videos, and files individually or in groups. Users can also make voice and video calls.[2].

Litmatch is an app for making new friends. Litmatch application users can communicate by sending messages or calling. Users can also share moments and show them to other users via their homepage. The thing that sets Litmatch apart is the soul match feature Litmatch has, which is a feature to chat anonymously through random matches and can also add them as friends.[3].

Digital forensics is a part of forensic science used in conducting data investigation investigations to find digital evidence of a digital crime. Digital forensics is carried out to help investigators and authorities carry out these investigations.[4].

In research by Muhammad Irwan Syahib et al. entitled "Digital Forensic Analysis of Beetalk Applications for Handling Cybercrime Using the NIST Method."[5], In this study, an analysis was carried out to find

*) Corresponding Author : bita@ittelkom-pwt.ac.id

evidence of crime in the Beetalk application, which is expected to assist the authorities in resolving cybercrime cases in the Beetalk application. Research by Michelle Mawar J. Sianipar et al. entitled "Digital Forensic Analysis of OVO Applications on Android."[6], This research was carried out because OVO, a digital wallet application, is widely used by the public and is vulnerable to cyber crimes, namely data leakage and the selling of personal data. The results are activity logs carried out by cybercrime actors on the OVO application. Research by Anton Yudhana et al. entitled "Analysis of Facebook Messenger Digital Evidence Using the NIST Method."[7], This study obtained results from perpetrator accounts, conversational texts, images, and voice messages. But data from messages that have been deleted cannot be found. Imam Riadi et al. conducted research entitled "Acquisition of Digital Evidence on Android-Based Instagram Messenger Using the National Institute Of Justice (NIJ) Method."[8], This research obtains evidence through pictures/photos and conversational text messages. Research by Galih Fanani et al. entitled "Forensic Analysis of MicChat Applications Using the Digital Forensic Research Workshop Method."[9], The results obtained in this study using Mobileedit are images, voice messages, videos, and cache. DB Browser For SQLite found text messages and contacts. Oxygen Forensic Detective found text messages, contacts, pictures, voice messages, and videos. Research conducted by Dina Yuliana et al. entitled "Forensic Analysis of Cyberbullying Cases on Instagram and Whatsapp Using the National Institute Of Justice (NIJ) Method"[10], this research was conducted to find evidence of cyberbullying crimes that occurred on the Instagram and Whatsapp applications which were carried out by the cellphone is in a non-root and root condition. The results obtained in this study are in the form of images, text messages, videos, and post captions that have yet to be deleted. At the same time, the post caption that has been deleted cannot be found [11].

The difference between this research and previous studies is that this research uses a case study of the Signal application and the Litmatch application using a case scenario. The method used is NIST 800-86. The tools used in this research are Mobileedit Forensic, Autopsy, and FTK Imager. The number of cases in instant messaging applications is a problem for this research. The reason for conducting this research is to find out how digital forensics obtains evidence using the NIST 800-86 method and what digital evidence is obtained in the analysis of Signal and Litmatch applications. This study aims to apply the NIST 800-86 method for Signal and Litmatch application analysis and find digital evidence of Signal and Litmach application analysis.

2. METHOD

The stages of forensic evidence analysis research on the Signal and Litmatch applications are as follows:

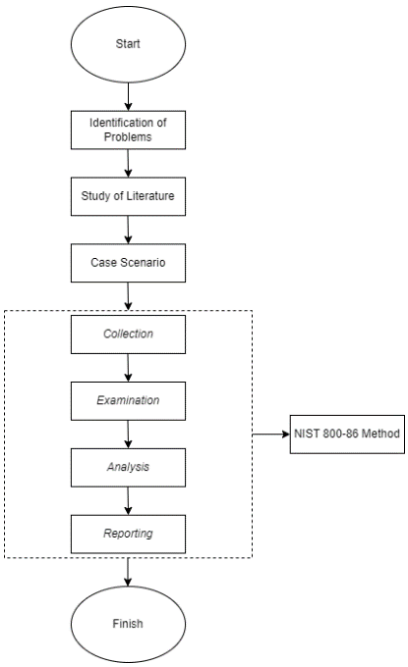


Figure 1. Research Flowchart

2.1 Problem Identification and Literature Study

At this stage, identifying existing problems is carried out, namely, the rampant crimes that occur through instant messaging applications using the Signal and Litmatch case studies. Crimes can occur through bullying, threats, planning to kill, and others. After identifying the problem, conduct a literature study from various available sources such as journals, books, websites, or other relevant sources.

2.2 Case Scenario

This research uses case scenarios to explain the steps needed to collect the data needed in the research. Scenarios are carried out by creating Signal, and Litmatch accounts with researchers acting as perpetrators. Then send text, image, and video messages on the Signal and Litmatch applications, make text and image posts on the Litmatch application, and make text, image, and video posts on the Signal application. Then perform data acquisition using Mobileedit and then implement the NIST 800-86 method to analyze the data that has been acquired.

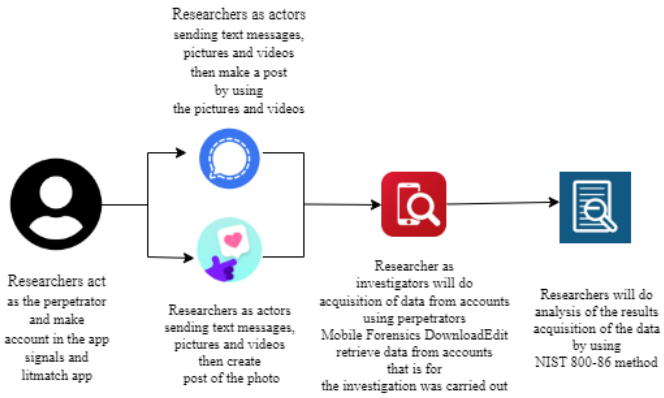


Figure 2. Case Scenario Diagram

2.3 Analysis Using the NIST 800-86 Method

The National Institute of Standards and Technology (NIST) 800-86 method consists of 4 stages[12], as follows:

a. Collection, This stage begins with creating an account on the Signal and Litmatch applications and preparing the tools. Then carry out case scenarios and collect identification evidence.
b. Examination, Perform data acquisition using Mobileedit to search for data as evidence of digital crimes on the Signal and Litmatch applications.
c. Analysis, analyzing the evidence that has been obtained using autopsy tools and FTK Imager
d. Reporting, At this stage, reporting is carried out regarding the results of the digital evidence analysis that has been carried out. Explain what results are obtained after searching for evidence and analyzing the evidence.

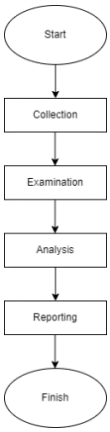


Figure 3. NIST Stages 800-86

3. RESULT AND DISCUSSION

3.1. Collection

Prepare the tools and scenarios that will be carried out in the research. The tools that will be used are as follows.

Table 1. Tools Used

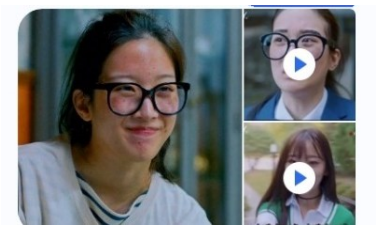
No	Alat dan Bahan	Spesifikasi	Keterangan
1	Toshiba Laptops	Intel Core™ i3	Investigation Tools
2	HP Samsung J2Core	Android 8.1.0	Hardware
3	Mobiledit Forensic	Version 8.0.1	Software
4	Autopsy	Version 4.19.1	Software
5	FTK Imager	AccessData FTK Imager 4.5.0.3	Software
6	Signal	0881*****7	The application to be analyzed
7	Litmatch	Soul lit ID : 3644706823	The application to be analyzed

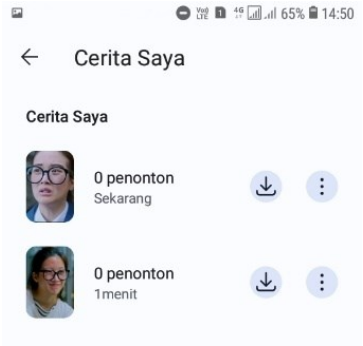
After preparing the tools used in this research, carry out case scenarios in the Signal and Litmatch applications. The scenario in the case involved threats with the threat of distributing private photos and videos belonging to the victim. The case scenario used is as follows:

3.1.1 Signal

As the perpetrator, the researcher started the chat by greeting the victim and sending the victim text messages, photos, and videos on the Signal application. The researcher, as a victim, answered with no interest. The researcher, as the perpetrator, felt annoyed and threatened the victim to distribute the victim's photos and videos. The following scenario is carried out in this research with the Signal application.Signal.

Table 2. Scenarios in the Signal Application

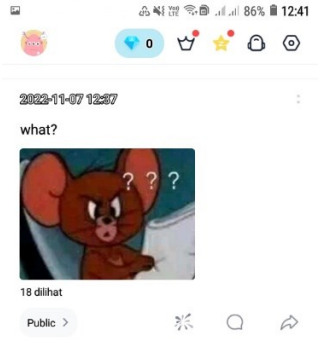
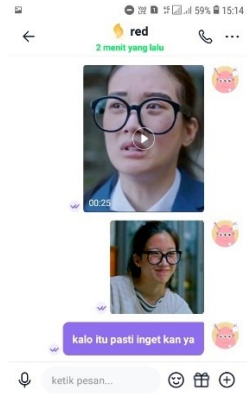
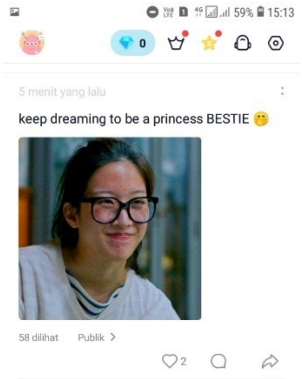
No	Session	Scenario	Explanation
1	Sending text messages		• As the perpetrator, the researcher started the conversation by greeting the victim.
2	Send photos and videos.		• As the perpetrator, the researcher sent the victim's photos and videos.

No	Session	Scenario	Explanation
3	Making threats		• The researcher, as the perpetrator, threatened the victim to share the victim's photos and videos.
4	The perpetrator distributed photos and videos belonging to the victim.		• The researcher, as the perpetrator, distributed photos and videos belonging to the victim.
5	The victim replied to the perpetrator's story.		• The researcher, as the victim, replies to the perpetrator's story.

3.1.2 Litmatch

As the perpetrator, the researcher started the chat by greeting by sending text messages, photos and videos to the victim on the Litmatch application. The researcher, as a victim, answered with no interest. The researcher, as the perpetrator, felt annoyed and threatened the victim to distribute the victim's photos and videos. The following scenario is carried out in this research with the Litmatch application.

Table 3. Scenarios on the Litmatch Application

No	Session	Scenario	Explanation
1	Sending text messages		• As the perpetrator, the researcher started a chat on the Litmatch application by greeting the victim. • The researcher, as the perpetrator, claimed to be an old friend of the victim.
2	Create a post		• Researchers as perpetrators make posts on the Litmatch application.
3	Send photos and videos.		• As the perpetrator, the researcher sent the victim's photos and videos. • The perpetrator threatened to distribute the victim's photos and videos.
4	The perpetrator distributed photos belonging to the victim.		• As the perpetrator, the researcher distributed the victim's photo on the perpetrator's Litmatch homepage.

No	Session	Scenario	Explanation
5	The victim replied to the perpetrator's post.		• As the victim, the researcher responded to the perpetrator's homepage post, which shared his photo.

3.2 Examination

At this stage, a data search will be carried out. Data search will be carried out in two ways: with a smartphone in a non-rooted condition and with a smartphone in a rooted condition.

1. Non Root

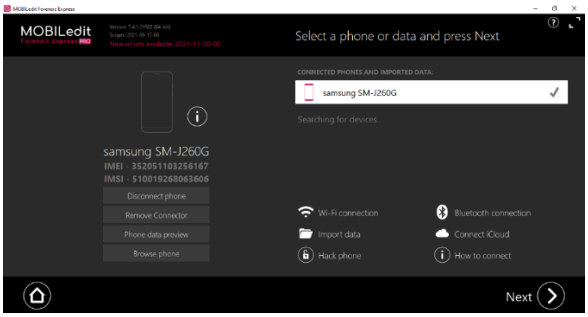


Figure 4. Display Mobiledit Non-Root

The Mobileedit display in a non-root smartphone condition only displays the smartphone name, IMEI number, and IMSI. The data acquisition will be done with Mobileedit by selecting which application you want.

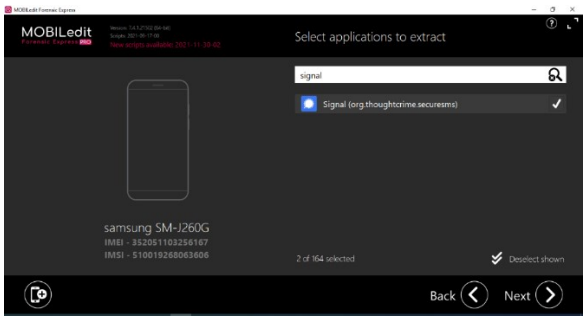


Figure 5. Choose the Signal App

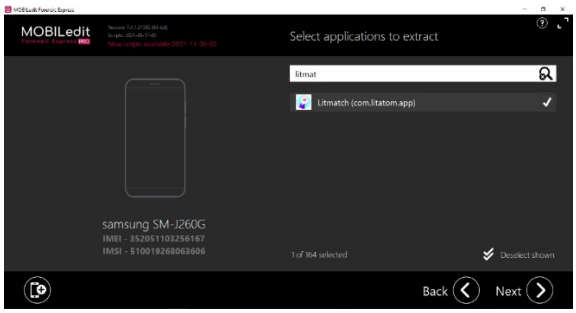


Figure 6. Choose the Litmatch App

The data results found using Mobileedit with a smartphone in a non-root condition are as follows.

Table 4. Mobiledit non root result

No	Hasil	Signal	Litmatch
1	Text	Not Found	Not Found
2	Picture	Not Found	Found
3	Video	Not Found	Not Found

Figure 7. Table of Contents Non Root

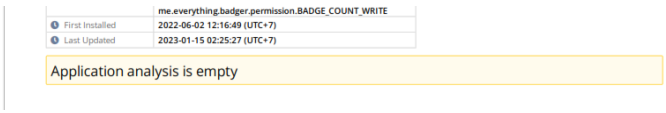


Figure 8. Mobiledit Signal Result

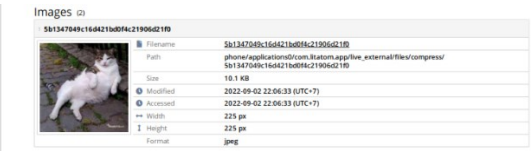


Figure 9. Mobiledit Litmatch Result(1)

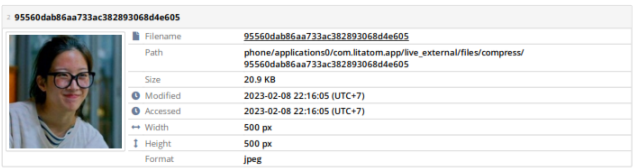


Figure 10. Mobiledit Litmatch Result(2)

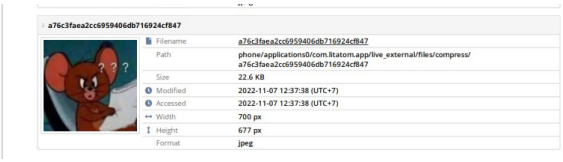


Figure 3. 1 Mobiledit Litmatch Result(3)

2. Root

Next, data acquisition will be done on a smartphone in a root condition. The following is the Mobileedit display if the smartphone is detected in a root condition.

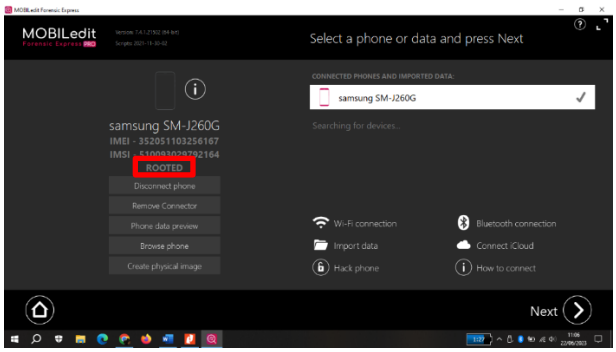


Figure 11. Mobiledit Root Display

The steps taken are the same as before: choosing which application you want to acquire data from. The following is a table of smartphone data results in root conditions using the Mobiledit tool.

Table 5. Mobiledit root Result

No	Hasil	Signal	Litmatch
1	Text	Not Found	Not Found
2	Picture	Not Found	Found
3	Video	Not Found	Not Found

Figure 12. Table of Contents Root

3.3 Analysis

The next stage is analysis. This stage will be carried out using an autopsy and FTK imager. Data on a non-rooted smartphone is cloned using a flash disk, then a disk image will be created using the FTK Imager and analyzed using Autopsy.

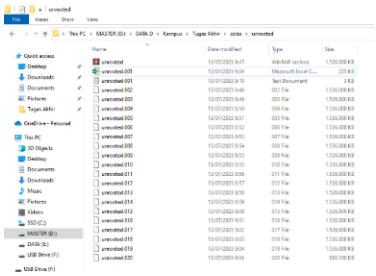


Figure 13. Result of Creating Disk Image on FTK Imager

After creating the disk image, the data will be read using the Autopsy tool. The following data was obtained using the Autopsy tool.

Table 6. Autopsy Non Root Result

No	Application Name	Non-root Proof		
		Text Messaging	Picture	Video
1	Signal	Not Found	Found	Not Found
2	Litmatch	Not Found	Found	Not Found

The analysis results using Autopsy tools on smartphones in non-root conditions on the Signal and Litmatch applications only found evidence in images. An analysis will be carried out on a smartphone in a root condition to get better results.

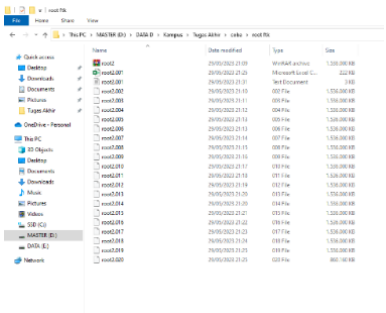


Figure 14. Result of Creating Disk Image on FTK Imager (Root)

The disk image file will be read using the Autopsy tool. The results obtained using the Autopsy tool on a smartphone in root conditions are as follows.

Table 7. Autopsy Root Result

No	Application Name	Bukti *Root*		
		Text Messaging	Picture	Video
1	Signal	Not Found	Found	Not Found
2	Litmatch	Not Found	Found	Not Found

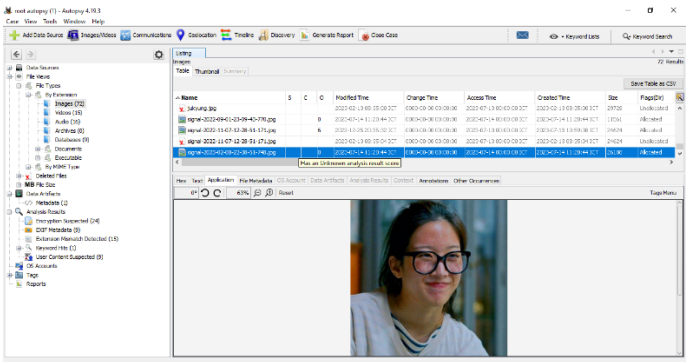


Figure 15. Search results on Autopsy Root

Furthermore, an analysis was carried out using the FTK Imager tool, but no files were obtained that could be used using the FTK Imager tool.

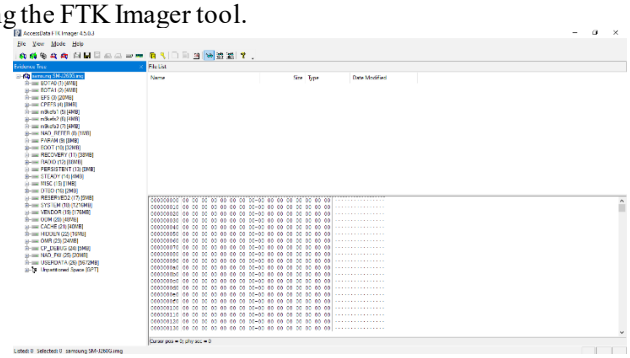


Figure 16. FTK Imager Result

4. CONCLUSION

Based on existing research, it can be concluded that the results obtained on smartphones in non-root conditions using mobiledit tools and the Signal application did not obtain any evidence. In contrast, the Litmatch application obtained evidence from 3 images. By using autopsy tools in the Signal application, the results are 1 image and 1 image that has been deleted. In contrast, in the Litmatch application, the results are 3 images and 2 images that have been deleted.

Furthermore, with the smartphone in root condition, the results using the mobiledit tools on the Signal application did not get any results. On the Litmatch application, the results were in the form of 3 images. Then the results using the Autopsy tool in the Litmatch application found 3 images. In comparison, in the Signal application, the results were obtained in the form of 3 images and 1 image that had been deleted. Meanwhile, using the FTK Imager, no results were found. In this result, the text of the conversation on the Signal and Litmatch applications cannot be found.

The limitations of this research are using tools that are not paid, can be further developed using paid tools or other tools, and use other applications and methods to get different results.

REFERENCES

[1] A. Wirara, B. Hardiawan, and M. Salman, "Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan 'WhatsApp,'" *Teknoin*, vol. 26, no. 1, pp. 66–74, 2020, doi: 10.20885/teknoin.vol26.iss1.art7.

[2] "Signal >> Beranda." Accessed: Apr. 03, 2022.

[3] "Litmatch." Accessed: Feb. 09, 2022.

[4] S. RACHMIE, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website," *Litigasi*, vol. 21, no. 21, pp. 104–127, 2020, doi: 10.23969/litigasi.v21i1.2388.

[5] "Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan Cybercrime Menggunakan Metode Nist | Syahib | Seminar Nasional Informatika (SEMNASIF)."

[6] "Analisis Digital Forensik Aplikasi Ovo Pada Android | Sianipar | eProceedings of Applied Science." Accessed: Jun. 03, 2022.

[7] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *IT Journal Research and Development*, vol. 3, no. 1, pp. 13–21, Aug. 2018, doi: 10.25299/ITJRD.2018.VOL3(1).1658.

[8] "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ) | Jurnal Teknik Informatika dan Sistem Informasi." Accessed: Jun. 05, 2022. [Online]. Available: https://journal.maranatha.edu/index.php/jutisi/article/view/1490

[9] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 2, pp. 1263–1271, Apr. 2022, doi: 10.30865/MIB.V6I2.3946.

[10] D. Yuliana, T. Yuniati, and B. Parga Zen, "Analisis Forensik Terhadap Kasus Cyberbullying Pada Instagram Dan Whatsapp Menggunakan Metode National Institute of Justice (Nij)," *Cyber Security dan Forensik Digital*, vol. 5, no. 2, pp. 52–59, 2023, doi: 10.14421/csecurity.2022.5.2.3734.

[11] F. Al Rasyid and B. Parg Zen, "Dead Forensic Analysis of Qutebrowser and Librewolf Browsers Using The Nist 800-86 Method," vol. 4, no. 5, pp. 1009–1019, 2023, doi: 10.52436/1.jutif.2023.4.5.688.

[12] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology".