

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 Hapsari¹, Bita Parga Zen^{2*}

^{1,2} Insitut Teknologi Telkom Purwokerto, Indonesia

¹18102244@ittelkom-pwt.ac.id, ²bita@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.

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.

ABSTRACT

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 outto help investigators and authorities carry out these investigations.[4].

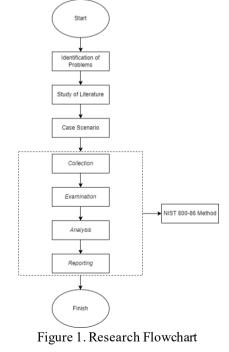
In research by Muhammad Irwan Syahib et al. entitled "Digital Forensic Analysis of Beetalk Applications for Handling Cybercrime Using the NIST Method." [5], In this study, an analysis was carried out to find

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 Litmatch application analysis.

2. METHOD

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



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.

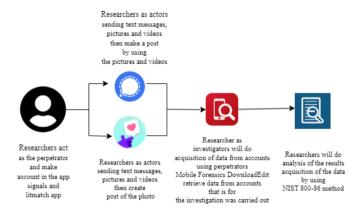


Figure 2. Case Scenario Diagram

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.

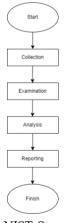


Figure 3. NIST Stages 800-86

3. RESULT AND DISCUSSION

3.1. Collection

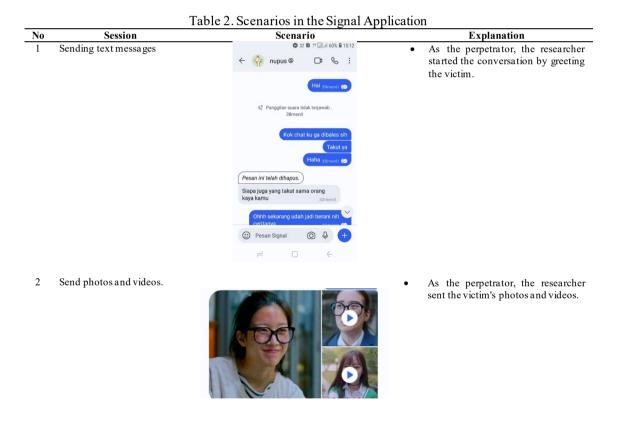
Prepare the tools and scenarios that will be carried out in the research. The tools that will be used are as follows.

		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.



5

No	Session	Scenario	Explanation
3	Making threats	Kalo itu di share gimana ya kira-kira 27menit <table-cell> Panggilan video tidak terjawab . 27menit</table-cell>	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.	Mau kamu apa? _{26menit} ✓	 The researcher, as the perpetrator, distributed photos and videos belonging to the victim.
	belonging to the victum.	Cerita Saya \widehat{O} penonton Sekarang \widehat{O} penonton \widehat{I} menit \widehat{U} :	belonging to the victim.
5	The victim replied to the perpetrator's story.	Trie De Mala 160% en 15:12	• The researcher, as the victim, replies to the perpetrator's story.
		Image: Object of the state	

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.

1				
	Sending text messages	⊂ © 7 ← S red 2 ment yang		As the perpetrator, the researcher started a cha on the Litmatch application by greeting the victim. The researcher, as the perpetrator, claimed to b
			haii red	an old friend of the victim.
		siapa ya?		
		w mas	men lama	
		temen lama?		
		yang mana ya?		
		Panggilan ditolak ole Q ketik pesan	n pengguna 🔛	
2	Create a post	⊑ &¥⊞	জালী নানা 86% 🗎 12:41 🕂 📌 🙆 ⊚	Researchers as perpetrators make posts on th Litmatch application.
		2022-11-07 12:37		
		what?		
		18 dilhat		
		Public >		
3	Send photos and videos.	≅ ●≋ ← ∱rec	■ #	As the perpetrator, the researcher sent th
		2 ment yer		victim's photos and videos. The perpetrator threatened to distribute th victim's photos and videos.
		kalo itu pasti in		
		ketik pesan		
4	The perpetrator distributed	•	•	As the perpetrator, the researcher distributed th
	photos belonging to the victim.		🛙 🕼 🕼 15:13	victim's photo on the perpetrator's Litmate homepage.
	victim.		♂ 📌 ① ⊙	nomepage.
			:	
		keep dreaming to be a pri	ncess BESTIE 🤫	
		58 dilihat Publik >		

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.
		Verify and the set of	
		maksudnya apa ya	
		maksudnya apa ya	
		🧋 ga ada	
		cuma ga suka aja sama kamu hihi	
		Q ketik pesan 😳 🛱 🛨	

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

	Select a phone or da	ta and press Next	() '
	samsung SM-J260G		~
(i)	Searching for devices		
samsung SM-J260G IMEI - 352051103256167 IMSI - 510019268063606			
	ᅙ Wi-Fi connection	Bluetocth connection	
	🗁 Import data	Connect iCloud	
	Hack phone		
			\sim



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.

😸 MOBLeát Formic Express				- 0 ×
MOBILedit			Select applications to	extract
			signal	ର
			D Signal (org.thoughtcrii	ne securesms) 🗸
	samsung SM			
	IMEI - 35205110 IMSI - 51001926			Set Deselect shown
				Back 🔇 Next 📎
	·	7 C1	1 0'	1.4

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.

	Tab	ole 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

Applications	1
Litmatch	1
Other Media Files	2
Images	2
Signal	3

Figure 7. Table of Contents Non Root

	me.everything.badger.permission.BADGE_COUNT_WRITE
First Installed	2022-06-02 12:16:49 (UTC+7)
Last Updated	2023-01-15 02:25:27 (UTC+7)
Application a	nalysis is empty
Application a	harysis is empty

Figure 8. Mobiledit Signal Result

5b1347049c16d421bd0f4c21	906d21f0	
CONCEPTION OF	Filename	5b1347049c16d421bd0f4c21906d21f0
- 2	Path	phone/applications0/com.litatom.app/live_external/files/compress/ 5b1347049c16d421bd0f4c21906d21f0
Contraction of the local distance of the loc	Size	10.1 KB
	Modified	2022-09-02 22:06:33 (UTC+7)
A particular of	D Accessed	2022-09-02 22:06:33 (UTC+7)
A Dares	+ Width	225 px
The state of the s	I Height	225 px
	Format	ipeg

Figure 9. Mobiledit Litmatch Result(1)

		Filename	95560dab86aa733ac382893068d4e605
		Path	phone/applications0/com.litatom.app/live_external/files/compress/ 95560dab86aa733ac382893068d4e605
A DOM		Size	20.9 KB
	0	Modified	2023-02-08 22:16:05 (UTC+7)
	0	Accessed	2023-02-08 22:16:05 (UTC+7)
	••	Width	500 px
6.	1	Height	500 px

Figure 10. Mobiledit Litmatch Result(2)

-	Filename	a76c3faea2cc6959406db716924cf847
222	Path	phone/applications0/com.litatom.app/live_external/files/compress/ a76c3faea2cc6959406db716924cf847
	Size	22.6 KB
	Modified	2022-11-07 12:37:38 (UTC+7)
	Accessed	2022-11-07 12:37:38 (UTC+7)
	↔ Width	700 px
-	1 Height	677 px
	Format	ipeg

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.

JINITA Vol. 6, No. 1, June 2024 **DOI:** doi.org/10.35970/jinita.v6i1.2025

MOBLedit Forenic Express MOBILedit Forenice Express (200	Retson 7.4.1.21502 (94-brt) Scripte 2021-11-30-42	Select a phone or data a	- ه × ۲ است Ind press Next
	samsung SM-J260G IMEI - 332051103256187 IMSI - 5109329782164	COMMECTED PHONES AND IMPORTED DAT samsung SM-J260G Searching for devices	us. √
	Discennect phone Rémove Connector	_	
		 WI-Fi connection Import data Hack phone 	Bluetooth connection Connect iCloud How to connect
	<u>e e a 1 8 0</u>		Next >

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

Table of Contents	
Applications	1
Litmatch	1
Other Media Files	2
Images	2
Audio	73
Video	73
Documents	118
Signal	126
Other Media Files	127
Images	127

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.

← -> -> ↑ ↑ ↓ This FC > MASTER(D) > DATA D > Kampus > Tuges Abhir > cobe > unnected					
		Name	Date modified	3.5**	Size
🖈 Quick access		errorted	13/07/2023 8-07	WeiR6R archive	1,535,000 Ю
Desinep	10	arrested 001	13/07/2023 9:54	Microsoft Excel C.,	225.10
🕹 Downloads	1	II argentiat 001	18/07/2023 9:30	Text Decortant	10
Documents	*	unrecoted 002	13/07/2023 0-48	002 File	1.535-000 K
Fictures		worepared 003	13/07/2023 8-49	003 File	1.525,000 Ю
Tanan Akhir		unreceived 004	13/07/2023 8:50	004 File	1.535.000 Ю
-		unwooted 005	13/07/2023 8:51	005 File	1.535.000 Ю
CneDrike - Person	el.	unworked 000	13/07/2023 0.52	005 File	1.535.000 K
This PC		unreated 007	13/07/2023 0:53	007 file	1.535.000 Ю
3D Objects		enrooted 008	13/07/2023 8:54	003 File	1.535.000 K
Deckterp		unrooted 009	13/07/2023 8:55	009 File	1.535.000 Ki
Documents		www.uted.010	13/07/2023 0.55	010 File	1.535.000 K
		unrooted 011	13/07/2023 0:56	011 Mile	1.535/000 10
Downloads		unrooted 012	13/07/2023 0:57	012 File	1.535.000 Ю
👌 Music		unvooted-013	13/07/2023-8:58	013 File	1.535.000 Ki
E Pictures		unrooted.014	13/07/2023 8:59	014 File	1.535.000 K
Wideos		areosted 015	13/07/2023 9:00	015 File	1.535/000 K
55D (C.)		unroated 016	13/07/2023 9/01	016 File	1.535.000 Ю
- MASTER (D-)		unreated.017	13/07/2023 9:02	017 File	1535/000 Ю
- 0556 (2)		are stated 418		018 File	1.535.000 Ю

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		Application Non-root Proof			
	Name	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.

	TisFC >	MASTER (D) > DAIA D > Kare	← → × ↑ 📙 > This PC > MASTER (D) > 0484 D > Kanyous > Tugas Akhir > celus > root Rk					
		Name	Data readified	Type	See			
Quéck access		🖬 x0042	25/05/2323 21 09	WellaR active	1,510,000 (
Desktop		enet2.00	29/29/2022 21/25	Microsoft Local C.	2221			
👃 Downicads	*	F root2.001	29/05/2023 21:31	Text Document	31			
Documents	*	root2.002	29/05/2023 21/10	002 File	1,536,000			
Piktunis	*	most2.003	29/05/2023 21:11	008 F/w	1,556,000			
Tases Akhir		apot2.004	25/05/2323 21:12	004 File	1,535,000			
		root2.005	29/05/2023 21:13	005 File	1.596.000			
OneDrive - Person	el	root2.005	25/05/2023 21:13	006 File	1.536.000			
This PC		root2.007	29/05/2023 21:14	007 File	1.536.000			
23 Objects		F0047.005	29/05/2023 21:15	000 71#	1.556.000			
Desition		root2.009	29/05/2028 21:16	000 F7k	1,536,000			
R Decements		K0062.010	25/03/2823 21:17	013 File	1,558,000			
		rpot2.011	29/05/2023 21:13	011 File	1,536,000			
Downloads		5 M0.5toos	29/05/2023 21:19	012 FTe	1.536.000			
Musik		root2.013	29/05/2023 21/20	013 File	1,536,000			
Ridures		root2.014	29/05/2028 21:20	014 File:	1,536,000			
Webes		0 #2012.015	25/05/2323 21 21	013 File	1,536,990			
🏪 550 (Ci)		00052.016	29/05/2023 21:22	015 File	1.536.000			
MASTER (D.)		voot2.017	25/05/2023 21 23	017 File	1.536.000			
- DATA (E)	_	root2.018	26/05/2023 21:24	013 File	1.536.000			
		Foot2.019	29/05/2825 21:25	011 77#	1,556,5901			
Intervenk		root2.020	29/05/2828 21-25	023 File	860.760			

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		Bukti Root		
	Name	Text Messaging	Picture	Video	
1	Signal	Not Found	Found	Not Found	
2	Litmatch	Not Found	Found	Not Found	

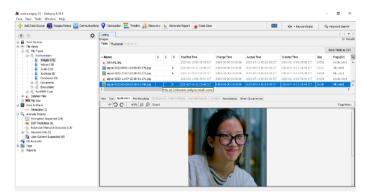


Figure 15. Search results on Autopsy Root

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.

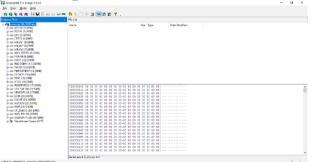


Figure 16. FTK Imager Result

4. CONCLUSION

Based on existing research, it can be concluded that the results obtained on smartphones in nonroot 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.

JINITA Vol. 6, No. 1, June 2024 **DOI:** doi.org/10.35970/jinita.v6i1.2025 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)."
- "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 NationalInstitute 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".