Jurnal Mandiri IT ISSN 2301-8984 (Print)
Vol. 12 No. 1, July (2023), pp. 20-28

Forensic analysis on discord application using the National Institute of Standards and Technology (NIST) Method

Fadhli Dzil Ikram[1], Muhammad Koprawi[2]
[1,2]Computer Engineering, Faculty of Computer Science, Universitas Amikom Yogyakarta, Indonesia

A R T I C L E I N F O

Article history:

Received Jul 21, 2023
Revised Jul 23, 2023
Accepted Jul 31, 2023

Keywords:

Digital Forensics
Discord
NIST
Sexual Harassment

ABSTRACT

Discord has shut down 30,000 communities due to various violations. In addressing the misuse of the Discord application, particularly in the form of sexual harassment, the problem of how to retrieve deleted messages from Discord desktop conversations using the National Institute of Standards and Technology (NIST) SP 800-86 method can be addressed. The NIST (National Institute of Standards and Technology) SP 800-86 method is employed for conducting digital evidence analysis or the process of obtaining information from digital evidence. The stages of the NIST method are Collection, Examination, Analysis, and Reporting. The accuracy level of the files obtained using the FTK Imager application is 16.67%, with the variables being evidence of image files. On the other hand, the ChromeCacheView application achieves 73.33% accuracy with variables including evidence of image files, videos, text messages, accounts, and emails. However, not all text messages are retrieved by ChromeCacheView. Autopsy, with a score of 33.33%, manages to retrieve images and emails.

Corresponding Author:

Muhammad Koprawi,
Computer Engineering,
Faculty of Computer Science,
Universitas Amikom Yogyakarta,
Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta, Indonesia.
Email: koprawi@amikom.ac.id

1. INTRODUCTION

The rapid development of digital technology in the world today is evident, and one of the main proofs of this progress is the presence of the Internet. The Internet facilitates communication and enables global interactions for people. The advancement of the Internet and various hardware devices has brought significant benefits to various aspects of our lives, such as education, business, communication, and entertainment. Discord is among the many voice chat applications that have emerged due to this technological development(Hutagaol et al., 2022).

Discord is a free chat platform similar to Slack or Skype, allowing users to communicate in real time through text, voice, or video, like other voice chat applications. This Discord application, more specifically, is popular among gamers(Geyser, n.d.).

Discord is also referred to as a digital distribution platform. The increasing number of Discord applications negatively and positively impacts its users. One of the negative impacts is that

Discord has stated to have banned over 2,000 groups suspected of having violent and extreme content. Discord has shut down 30,000 communities (servers) due to various violations committed(Saputro, n.d.). The most common violations include cybercrimes and exploitative content, encompassing explicit pornographic content, revenge materials, and sexually explicit content involving minors. The most prevalent offence is cybercrime(Layanan Pendidikan Tinggi Wilayah XII -Ambon et al., n.d.).

The rapidly advancing technology has resulted in various cybercrime cases, such as fraud, sexual harassment, pornography, cyberbullying, and hacking. Some individuals intentionally dispose of files or data related to their criminal activities to eliminate digital evidence and avoid legal consequences with the use of such digital evidence.

A Twitter user named @CrownedCollider accused the Discord admin of Phasmophobia, "Charcoal Salamender," of problematic behaviour. This is not an ordinary accusation, as the Twitter user provided screenshots of Discord containing explicit images that were shared and racist behaviour that was uncalled for(Mariza, n.d.).

According to Discord, 15% of its employees are dedicated to trust and safety, a percentage similar to other major social media companies like Facebook and Twitter. During the second half of 2020, their team deactivated around 266,000 accounts, primarily due to violations related to exploitative content, including non-consensual pornography and sexual content involving minors(Saputro, n.d.).

To address the issue of sexual harassment abuse within the Discord application can be viewed from various aspects, such as criminalization policy (formulating criminal acts) and criminal liability (including aspects of evidence presentation). Obtaining valid evidence involves conducting investigations and digital forensic examinations, using computer forensics, and referring to the investigation and acquisition of digital evidence.

The method used for the digital evidence examination on Windows devices is the NIST method. The selection of a research method, investigation, and model used systematically in digital forensics fundamentally requires the application of individuality, repetition, reliability, used performance, test capabilities, and quality standards or standards used. Previous research on Digital Forensic Acquisition and Analysis of Discord Applications has been conducted to analyze Discord and identify and organize artefact locations, such as received/sent messages, shared files, chat rooms, and user account information within the Windows application.

2. RESEARCH METHOD

The method used for analyzing digital evidence or the stages to obtain information from digital evidence is the NIST (National Institute of Standards and Technology) method. This method describes the step-by-step and systematic process to address existing problems. The stages of the NIST method are Collection, Examination, Analysis, and Reporting(Nasirudin et al., 2020).

Forensic data can be obtained using external storage devices such as USB flash drives, hard disks, CDs, DVDs, or Imaging. The investigator will then bring this data to the forensic lab to undergo various methods for analyzing it as forensic evidence(Kent et al., n.d.; Rafique & Khan, 2013). NIST SP 800-86 is a guide for conducting digital forensics with the flow of Collection, Examination, Analysis, and Reporting(Hariyadi et al., 2021; Indriyanto et al., 2020; Kent et al., n.d.; Ramadhan et al., 2022).

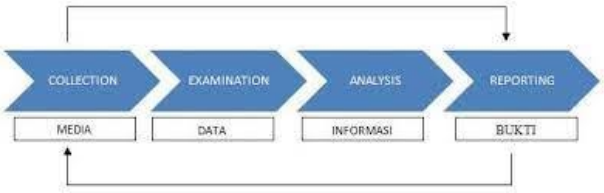


Figure 1. The process of the NIST method

a. The collection is the stage where researchers prepare the materials for the study. These materials are obtained from hardware belonging to the perpetrator, which has been secured, and then the acquisition process or making a copy of the digital evidence is conducted to preserve its authenticity.
b. In the Examination stage, the process of identifying data that can be used as evidence occurs. Once the data is determined, it will be analyzed using tools in the subsequent stage.
c. The Analysis stage is performed after receiving the desired files or digital data from the previous process. The data is then analyzed in detail to obtain digital evidence.
d. In the Reporting stage, the researcher carries out the reporting process. The reporting in this study involves the digital evidence obtained and the conclusions drawn from the analysis stage.

Table 1. Research Variable

No.	Variable	Amount of data
1	Conversation Text	34
2	Image	3
3	Video	1

In the research variable table above, by attaching the variables that have been studied in previous studies (Afdal et al., 2022), in this study, the parameters studied included conversational text, images, and videos, as in Table 1. In this study, researchers added three additional variables to maximize digital evidence to maximize the results obtained while investigating digital evidence on the Discord application. Additional evidence is explained in Table 2 below.

In the research variable table above, by attaching the variables that have been studied in previous studies (Afdal et al., 2022), in this study, the parameters studied included conversational text, images, and videos, as in Table 1. In this study, researchers added three additional variables to maximize digital evidence to maximize the results obtained while investigating digital evidence on the Discord application. Additional evidence is explained in Table 2 below.

Table 2. Additional Variable

No.	Variable	Amount of data
1	Email	1
2	Account	1
3	Time	1

To calculate the level of accuracy of evidence from the variables that have been set, then do the calculations for each application using the formula(Riadi et al., 2018):

$$\frac{dy}{dx} \times 100\% \quad (1)$$

The formula above explains that to get accuracy on all the variables examined from each application that is used with a *dy* count, namely, the total number of variables obtained, divided (÷) by *dx*; the number of variables that are set, and multiplied by (×) 100, will get the results of the accuracy in each application in collecting evidence from each variable that has been set.

Tools and materials

Table 3. Hardware

No.	Type	specification
1	Processor	AMD Ryzen 5 3400G
2	RAM	V-GeN RESCUE 16GB (8x2)
3	Storage	V-GeN 256GB SATA 3 SSD
4	Motherboard	ASRock B450M
5	Graphics Card	GeForce GTX 1650S OC 4GB
6	Power Supply	FSP HV PRO 550W 80+ Bronze
7	Display	LG 24" Monitor TV

Table 4. Software

No.	Type	specification
1	Discord	-
2	AccessData FTK Imager	4.5.0.3
3	ChromeCacheViewer	2.41
4	Autopsy	4.19.3
5	Mozilla Firefox	-

e. FTK Imager is a forensic software developed by AccessData. FTK Imager collects digital evidence from computers or other devices in digital forensic investigations.
f. ChromeCacheView is a software NirSoft developed to access and extract cache files from the Google Chrome browser(nirsoft, n.d.). ChromeCacheView can be used by digital forensic experts and general users to examine data stored in cache files, such as images, videos, audio, and other files that may have been accessed or downloaded from specific websites. This can assist in investigating user activity on the internet and gathering digital evidence that can be used in criminal investigations or legal cases.
g. Forensic Autopsy is a software application developed by Basis Technology Corp. This application is one of the tools used by digital forensic experts to carry out analysis and investigations on digital evidence related to computer crime and digital forensics.
h. Discord is a free service accessed via a computer, tablet, mobile app, or browser. Originally intended to allow gamers to voice chat while playing online games, it was later adopted by many other communities to facilitate discussion, share ideas, and share resources. The service now allows video chatting, screen sharing and direct messaging between users(Wiles & Simmons, 2022).
i. The Mozilla Firefox browser, formerly Phoenix, is now known as Mozilla. Mozilla Firefox is a web browser (web browser) developed by the Mozilla Foundation and a community of volunteers(Noviantoro et al., 2022).

Scenario Development

It begins with the suspect conversing using the Discord application with a woman (victim) he just recognized from an online game. The conversation started by getting to know each other and just discussing the game they were playing. However, the conversation was increasingly heading in a negative direction because the suspect commented on the profile photo of this friend's discord account. Then the suspect finally sent photos and videos containing pornographic content showing his genitals to persuade his friend to do the opposite.

However, the victim felt harassed by his friend's behavior and immediately sent a reply message warning that the behavior carried out by his friend was inhumane. Responding to this message from his friend, the suspect, instead of apologizing, sent another photo of his genitals. With such a message, the victim immediately took a screenshot and informed the suspect that his actions in the conversation had been secured as a digital image and would be reported to the authorities. The suspect was frightened and immediately deleted all conversations sent, including videos and photos, to destroy evidence.

In short, the authorities received the victim's report, and the perpetrators' arrest was carried out immediately. The evidence found was in the form of an Android smartphone used by the perpetrator to send messages using the Discord application. Furthermore, the authorities submitted the evidence to the forensic team due to a lack of evidence to ensure that the reports from the victims were accurate. Because of that, a digital forensic process was carried out to find digital evidence that the perpetrator deleted.

3. RESULTS AND DISCUSSIONS

Collection

This stage is the process of retrieving evidence on the perpetrator's computer with evidence stored in the C:\Users\Vtrl\AppData\Roaming\discord directory and evidence from the victim's computer C:\Users\iamzy\AppData\Roaming\discord.

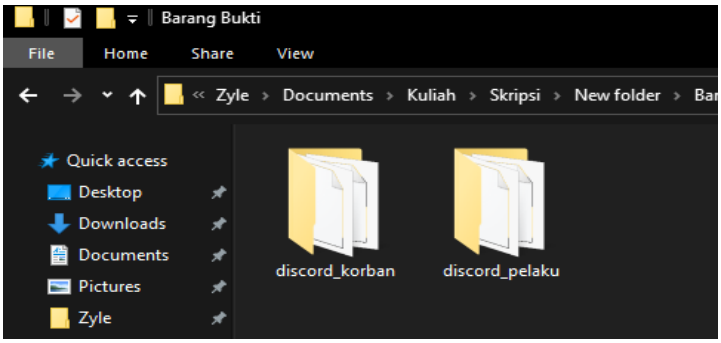


Figure 2. The process of taking evidence in the form of cache files

Examination

Examination of digital evidence is carried out manually or automatically from the data obtained at the previous stage, namely collection. The evidence referred to in the form of files from the Discord file directory will be included in each application and will be analyzed one by one.

Analysis

The initial steps of the analysis are carried out alternately from each application, starting with analyzing the cache files in the FTK Imager application. For the FTK Imager application, the analysis is carried out slowly by checking the cache files one by one on the two cache files, namely the cache files from the perpetrator's discord and the cache files from the victim's discord.

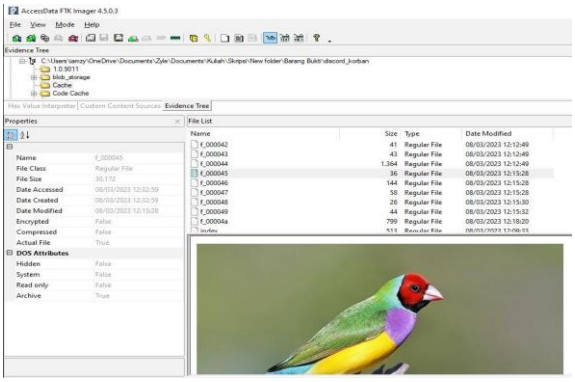


Figure 3. Image finding in cache file f_000045

The next stage is to analyze digital evidence in the ChromeCacheView application; the analysis process begins by checking the victim's cache files. A file with the name tegang.mp4 was found in the victim's cache file.

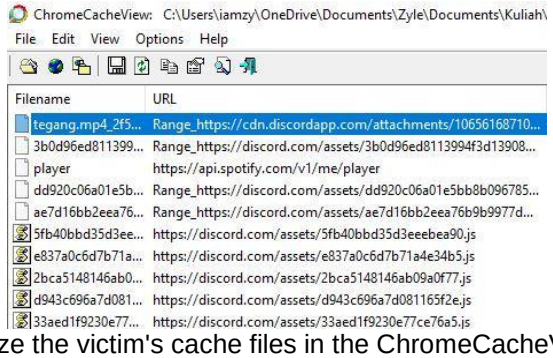


Figure 4. Analyze the victim's cache files in the ChromeCacheView application

When the file is opened, it displays a video sent by the perpetrator, with the discovery of a video cache; further analysis is carried out to look for other findings.

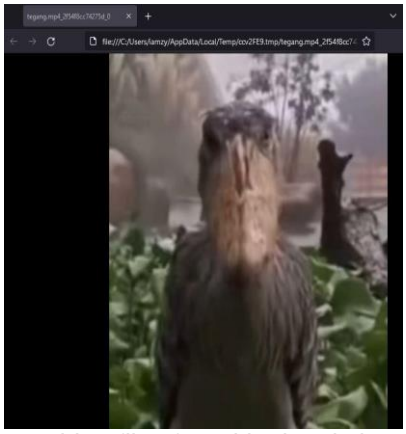
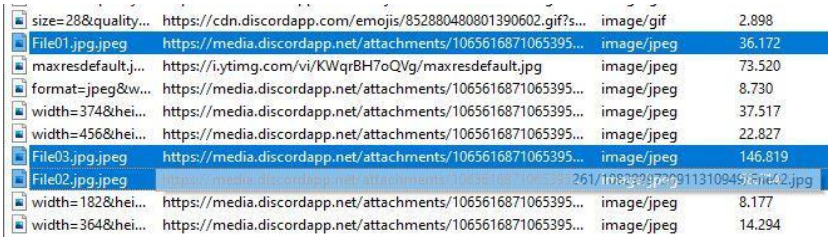


Figure 5. Video files found in the victim's cache

Another finding in the perpetrator's cache file is an image file; the image found is the same as the other images. After getting the image file, the following analysis focuses on finding cache files from text messages in the perpetrator's cache.



size=28&quality...	https://cdn.discordapp.com/emojis/852880480801390602.gif?s...	image/gif	2.898
File01.jpg.jpeg	https://media.discordapp.net/attachments/1065616871065395...	image/jpeg	36.172
maxresdefault.j...	https://i.ytimg.com/vi/KWqrBH7oQVg/maxresdefault.jpg	image/jpeg	73.520
format=jpeg&w...	https://media.discordapp.net/attachments/1065616871065395...	image/jpeg	8.730
width=374&hei...	https://media.discordapp.net/attachments/1065616871065395...	image/jpeg	37.517
width=456&hei...	https://media.discordapp.net/attachments/1065616871065395...	image/jpeg	22.827
File03.jpg.jpeg	https://media.discordapp.net/attachments/1065616871065395...	image/jpeg	146.819
File02.jpg.jpeg	https://media.discordapp.net/attachments/1065616871065395...	image/jpeg	261,108
width=182&hei...	https://media.discordapp.net/attachments/1065616871065395...	image/jpeg	8.177
width=364&hei...	https://media.discordapp.net/attachments/1065616871065395...	image/jpeg	14.294

Figure 6. Image files found in the perpetrator's cache

The finding of a file named 50. json was opened using the Mozilla Firefox browser application for further analysis regarding text messages stored in the perpetrator's cache. The text messages found were as many as 16 lines; the victim sent these messages to the perpetrator, so all messages totalling 16 lines were from the victim to the perpetrator.

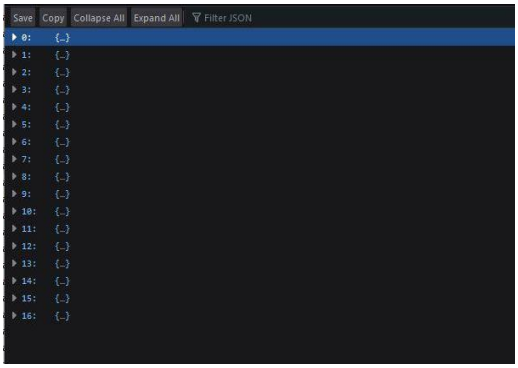


Figure 7. The number of messages found in the perpetrator's cache files

Further analysis using the Autopsy application in this application no chats and videos were found. The files found were only image files and artefacts in the form of e-mails used by the perpetrators.

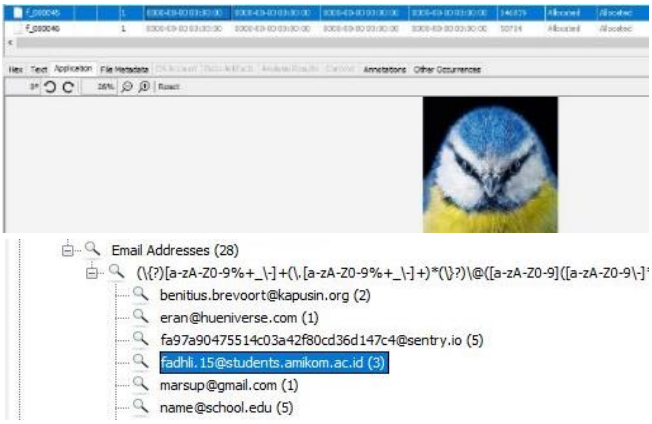


Figure 8. Images and emails found on the Autopsy application

Reporting

Furthermore, the results of the analysis that has been carried out must be drawn appropriate and objective conclusions. Digital forensic experts must make clear and easy-to-understand reports of the findings and conclusions that have been found. This report can later be used as evidence in court to prove the existence of a crime committed by the perpetrator—proof of cases of sexual harassment in the Windows-based Discord application with digital evidence that has been found.

Table 5. Obtained Digital Evidence

No	Digital Evidence	Initial Data Amount of Digital Evidence	FTK Imager	Chrome CacheView	Autopsy
1	Conversation Text	34	-	20	-
2	Image	3	3	3	3
3	Video	1	-	1	-
4	Email	1	-	1	1
5	Account	1	-	1	-
6	Time	1	-	-	-

Researchers use calculations with index numbers to determine the performance of each forensic tool according to the experimental results. The index number calculation is an unweighted index, as in the formula before(Riadi et al., 2018).

Table 6 below shows the results of the performance of each application in conducting the analysis. FTK Imager gets a score of 16.67%, which only gets images, ChromeCacheView gets a score of 76.33% because it gets almost all of the variables that have been determined, and Autopsy with a score of 33.33% can get two variables, namely images and artefacts in the form of email.

Table 6. App Performance

No	Digital Evidence	FTK Imager	Chrome CacheView	Autopsy
1	Conversation Text	-	√	-
2	Image	√	√	√
3	Video	-	√	-
4	Email	-	√	√
5	Account	-	√	-
6	Time	-	-	-
	accuracy	**16,67%**	**73,33%**	**33,33%**

4. CONCLUSION

The conclusion of this study is to find out the messages that the perpetrator has deleted according to the scenarios prepared beforehand in the form of text messages, photos, and videos, as well as securing digital evidence. The level of accuracy of the files obtained in the FTK Imager application is 16.67%, with the variable obtained as evidence of image files. In comparison, the ChromeCacheView application gets 73.33%, with the variables obtained as evidence of image files, videos, text messages, accounts, and emails. However, not all text messages obtained by ChromeCacheView, and Autopsy, with a score of 33.33%, manage to get images and emails. With this result, it can be concluded that to perform forensic analysis on cache files such as browser cache and applications such as Discord, it is more recommended to use ChromeCacheView to support the success rate of digital evidence analysis so that the results obtained from research can be used by investigators or investigators in handling crime cases. Moreover, references for investigators in searching for evidence in cases of sexual harassment or distribution of pornography on the Discord application. For further research, use live forensic techniques that are used on the discord web so that researchers can see comparisons using methods that have been done before. Then for further testing, using different platforms such as mobile Discord and different tools as well as paid ones such as Magnet Axiom, EnCase, ProDiscover Forensic, and Caine.

REFERENCES

Afdal, A. M., Salim, Y., & Rachman Manga', A. (2022). Analisis Bukti Digital Forensik pada Discord menggunakan Metode National Institute of Standards Technology. *Buletin Sistem Informasi Dan Teknologi Islam (BUSITI)*, *3*(4), 293–300. https://doi.org/10.33096/BUSITI.V3I4.1425

nirsoft. (n.d.). *ChromeCacheView - Cache viewer for Google Chrome Web browser*. Retrieved April 6, 2023, from https://www.nirsoft.net/utils/chrome_cache_view.html

Geyser, W. (n.d.). *The Latest Discord Statistics: Servers, Revenue, Data, and More*. Retrieved June 6, 2023, from https://influencermarketinghub.com/discord-stats/

Hariyadi, D., Kusuma, M., Sholeh, A., & Fazlurrahman. (2021). Digital Forensics Investigation on Xiaomi Smart Router Using SNI ISO/IEC 27037:2014 and NIST SP 800-86 Framework. *Proceedings of the International Conference on Science and Engineering (ICSE-UIN-SUKA 2021)*, *211*, 143–147. https://doi.org/10.2991/AER.K.211222.023

Hutagaol, A.-, Waleleng, G. J., & Harillama, S. H. (2022). PEMANFAATAN APLIKASI DISCORD SEBAGAI MEDIA KOMUNIKASI OLEH MAHASISWA MAGANG DIMASA PANDEMI COVID-19 DI SKILVUL. *ACTA DIURNA KOMUNIKASI*, *4*(3). https://ejournal.unsrat.ac.id/v3/index.php/actadiurnakomunikasi/article/view/42967

Indriyanto, M. W., Hariyadi, D., Habibi, M., Achmad, U. J., & Yogyakarta, Y. (2020). INVESTIGASI DAN ANALISIS FORENSIK DIGITAL PADA PERCAKAPAN GRUP WHATSAPP MENGGUNAKAN NIST SP 800-86 dan SUPPORT VECTOR MACHINE. *Cyber Security Dan Forensik Digital*, *3*(2), 34–38. https://doi.org/10.14421/CSECURITY.2020.3.2.2193

Kent, K., Chevalier, S., Grance, T., & Dang, H. (n.d.). *Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology*.

Layanan Pendidikan Tinggi Wilayah XII -Ambon, L., Rachmad Dwi Miarsa, F., & Heru Romadhon, A. (n.d.). *Jurnal Ilmu Sosial dan Humaniora Pelanggaran Hukum dalam Tindakan Vandalisme di Ruang Cyberspace*.

Mariza, B. (n.d.). *Berita : Berbagi Gambar Dewasa di Chat, Seorang Admin Discord Game Phasmophobia Ditendang | KotakGame*. Retrieved June 6, 2023, from https://www.kotakgame.com/berita/detail/96378/Berbagi-Gambar-Dewasa-di-Chat-Seorang-Admin-Discord-Game-Phasmophobia-Ditendang

Nasirudin, N., Sunardi, S., & Riadi, I. (2020). Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, *5*(1), 89–94. https://doi.org/10.32493/INFORMATIKA.V5I1.4578

Noviantoro, A., Silviana, A. B., Fitriani, R. R., & Permatasari, H. P. (2022). RANCANGAN DAN IMPLEMENTASI APLIKASI SEWA LAPANGAN BADMINTON WILAYAH DEPOK BERBASIS WEB. *Jurnal Teknik Dan Science*, *1*(2), 88–103. https://doi.org/10.56127/JTS.V1I2.108

Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools. *International Journal of Scientific & Engineering Research*, *4*(10). http://www.ijser.org

Ramadhan, R. A., Rachmat Setiawan, P., Hariyadi, D., Riau, I., & Yogyakarta, A. Y. (2022). Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework. *IT Journal Research and Development*, *6*(2), 162–168. https://doi.org/10.25299/ITJRD.2022.8968

Riadi, I., Umar, R., & Firdonsyah, A. (2018). Forensic Tools Performance Analysis on Android-based Blackberry Messenger using NIST Measurements. *International Journal of Electrical and Computer Engineering (IJECE)*, *8*(5), 3991–4003. https://doi.org/10.11591/IJECE.V8I5.PP3991-4003

Saputro, P. (n.d.). *Discord Cekal 2.000 Grup Chat Karena Konten Kekerasan*. Retrieved June 6, 2023, from https://inet.detik.com/cyberlife/d-5528681/discord-cekal-2000-grup-chat-karena-konten-kekerasan

Wiles, A. M., & Simmons, S. L. (2022). Establishment of an Engaged and Active Learning Community in the Biology Classroom and Lab with Discord. *Journal of Microbiology & Biology Education*, *23*(1). https://doi.org/10.1128/JMBE.00334-21/SUPPL_FILE/JMBE00334-21_SUPP_1_SEQ4.PDF