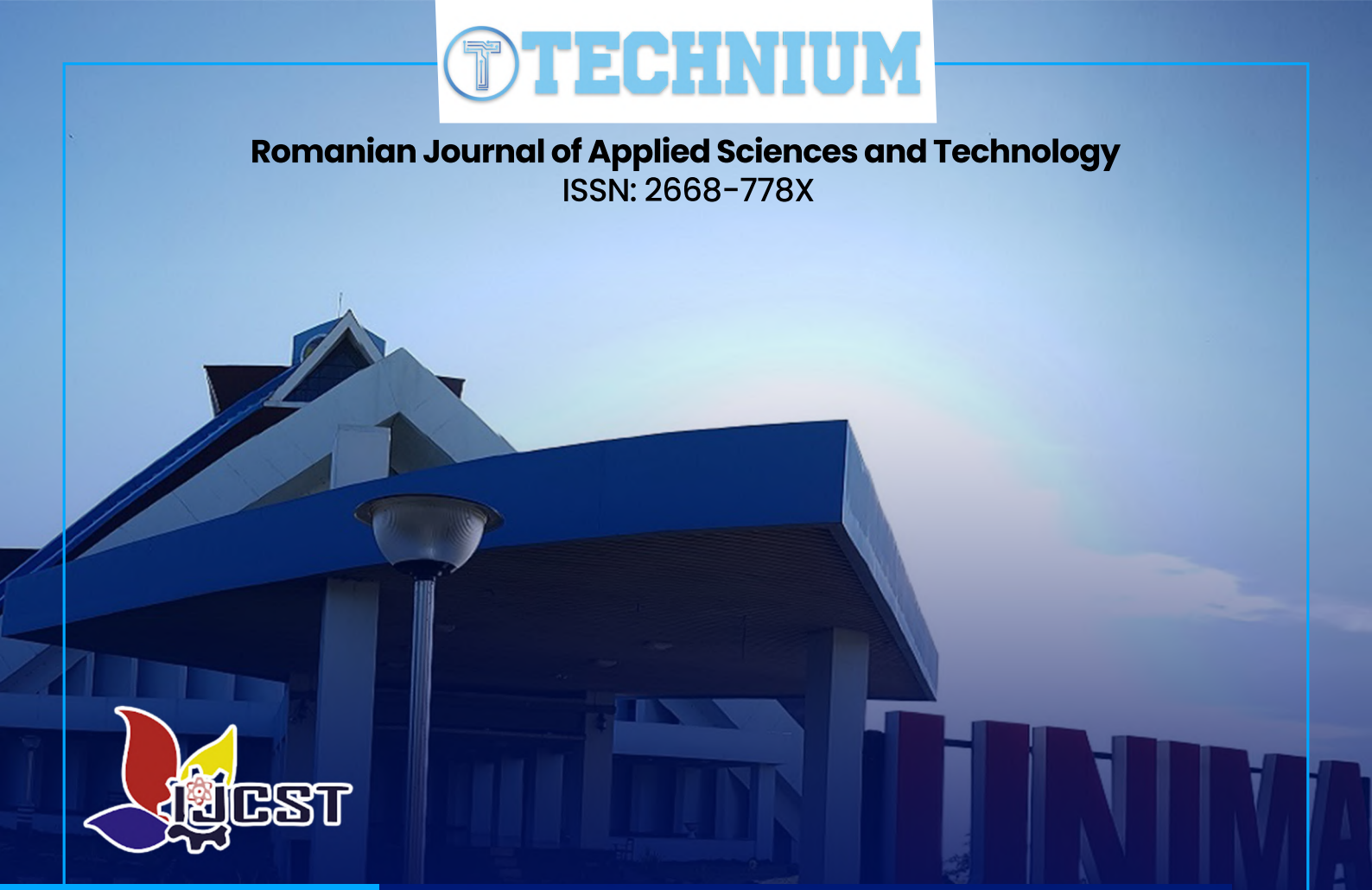
TECHNIUM

Romanian Journal of Applied Sciences and Technology
ISSN: 2668-778X



vol. 17 / 2023

The 7th International Conference on Science Technology

organized by
Faculty of Social Science and
Law Universitas Negeri Manado and
Consortium of International Conference
on Science and Technology

The Innovation Breakthrough in Digital and Disruptive Era

PLUS COMMUNICATION

International Communication & PR

Technium: Romanian Journal of
Applied Sciences and Technology
Vol. 17, 249-254, November, 2023
ISSN: 2668-778X
www.techniumscience.com

Implementation Framework National Institute of Standards and Technology (Nist) Evidence Digital In The Forensic Process Social Media

Radika Muzdalifa Abubakar[1*], *Muhammad Sabri* Ahmad[2], *Syarifuddin* N. Kapita[3], *Ahmad* Fuad[4]

[1]Student of Informatics Engineering Department, Faculty of Engineering, Universitas Khairun, 97719 Ternate, Indonesia
[2,3,4]Informatics Engineering Department, Faculty of Engineering, Universitas Khairun, 97719 Ternate, Indonesia

Abstract. Many people carry out social media activities which are not only positive activities but also activities that have a negative impact, such as crimes in cyberspace. especially forensics mobile in assisting the resolution of crime cases through social media Instagram with media access smartphone. The biggest problem in the data retrieval process is that the perpetrator deletes or tries to eliminate digital evidence on a smartphone so this research aims to implement the framework National Institute of Standards and Technology to investigate data forensic evidence on social media Instagram accessed via smartphone Android by using tools mobile Edit forensic in data extraction on a smartphone with workflow stages collection, -reporting. This study uses a conversation scenario on the Instagram feature direct message (DM) with conditions including deleting data on the Instagram application. The method used in handling cybercrime with media evidence smartphones is the method National Institute of Standards and Technology (NIST). The results of this study are in collecting data in the form of 25 conversations (chat), 206 images, 86 videos, 5 audio, and 4 call logs on smartphones. However tools MOBILEdit Forensic in returning digital evidence are unable to recover conversations and call logs as a whole.

Keywords. Digital forensic, NIST, cybercrime, Instagram, Smartphone

* Corresponding author: muzdalifaradika@gmail.com

Technium: Romanian Journal of
Applied Sciences and Technology
Vol. 17, 249-254, November, 2023
ISSN: 2668-778X
www.techniumscience.com

1 Introduction

Currently, social media is the most commonly used communication tool by the public. Many people use social media for various activities, including both positive and negative activities, such as cyber crimes. The use of social media continues to grow among all ages, from children to adults. Almost everyone has a social media account, especially on Instagram. However, these features instagram can also have good and bad impacts on society. One of the striking negative impacts is cyberbullying or online harassment [1].

Several previous studies have been conducted in the field of mobile forensics, one of the approaches used in this study is to use the NIST framework which is focused on collecting digital evidence related to crime on the Facebook Lite application. Forensic methods are used in the process of gathering this evidence. The NIST framework has good procedures for extracting digital forensic data[2].

In another study, a forensic analysis of Android phones was performed using methods provided by NIST and assisted by MOBILedit Forensics forensic software. In the analysis process, digital evidence is obtained in the form of user profiles, contact lists, e-mails, chat conversations, and pictures. This study managed to detect around 75% of the total data on the investigated Android phones [3].

Based on the results of the research previously described, it is important to have a specific approach in the field of mobile forensics to help solve crime cases that occur through Instagram social media using an Android smartphone. When someone is involved in cybercrime and a cell phone is found as evidence showing that involvement, the biggest challenge in the data retrieval process is the perpetrator trying to hide or delete digital evidence in the cellphone to eliminate traces. To overcome this problem, an investigation of evidence is carried out by applying the National Institute of Standards and Technology (NIST) framework to obtain digital forensic copies of the evidence used and criminal activity committed via social media.

Based on the problems previously described, the authors conducted a study entitled "Implementation of the National Institute of Standards and Technology (NIST) Digital Evidence Framework in Forensic Processes on Social Media".

2 Research Method

The method used to obtain digital evidence information is the National Institute of Standards and Technology (NIST) method

2.1 National Institute of Standards and Technology (NIST)

Captions should be typed in 9-point Times. They should be centred above the tables and flush left beneath the figures. The National Institute of Standards and Technology (NIST) Framework is an institution tasked with developing standards, guidelines and minimum requirements needed to maintain information security in the field of digital forensics. Although initially used by central government agencies in America, this framework can also be adopted by other organizations such as academia, private investigative agencies, and the like [4].

NIST provides a comprehensive framework for conducting digital forensic investigations with trusted and trusted standards. This framework provides clear guidelines and a structured methodology for conducting analysis, gathering digital evidence, and recovering lost data. Using the NIST approach, organizations and individuals with competence in digital forensics can adopt internationally recognized best practices in investigating digital crimes and ensure the integrity and reliability of digital evidence obtained.

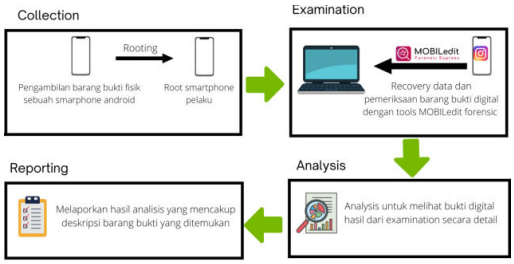


Fig. 1. The Stages of the NIST method

Based on the stages in Figure 1, it is explained:

1. Collection This stage involves collecting physical evidence by identifying and recording the evidence found.
2. Examination At this stage, the data that has been collected from the evidence will be tested and checked with the aim of maintaining the integrity of the information and preventing changes to the evidence.
3. Analysis at this stage, evidence will be analyzed in depth to obtain information relevant to the case being investigated.
4. Reporting This stage involves preparing a report containing the results of the analysis of the evidence that has been investigated. The report will contribute to the investigation process to identify suspects and help develop further cases [5].

2.2 Digital Forensic

Digital forensics is the application of computer knowledge and technology in a legal or judicial context [6]. This field uses the scientific method to prove cases through a series of steps, including the maintenance, validation, collection, analysis, identification, documentation, interpretation, and presentation of digital evidence obtained from digital sources [7].

2.3 Mobile Forensics

Mobile Forensics is a branch of science that originates from the discipline of digital forensics, also known as computer forensics [8]. Digital forensics on mobile devices plays an important role. Forensic experts can use specific methods and tools to collect, analyze and recover digital evidence present on smartphones with logical and physical extraction methods [3].

Technium: Romanian Journal of
Applied Sciences and Technology
Vol. 17, 249-254, November, 2023
ISSN: 2668-778X
www.techniumscience.com

2.4 Smartphone Android

An Android smartphone is a device that has the dual function of being a mobile phone and also a practical portable computer [9]. This device has a large storage capacity, and is not only limited to call logs or SMS messages. Smartphones can also store various other information related to user usage, behavior or activities. In smartphones, users can store various types of data, such as contacts, text messages, multimedia files, applications, internet browsing history, and other application data[3].

2.5 MOBILEdit Forensic Express

MOBILedit Forensic is a software that has a function to carry out investigations and retrieve data from smartphones. The software has the ability to read messages, record calls, access SIM cards, and other functions. Mobile phones can be connected via a direct cable or using a wireless connection [10]. This software then combines the data found, removes duplicates, and presents them in a complete and easy-to-read report [11].

2.6 Social Media

Social media is an online platform that can be used as a means of remote communication, building relationships with other people, and getting news through special applications connected to the internet[12]. By simply opening social media, users can connect with other people, share daily activities, and carry out various other activities [13].

2.7 Instagram

Instagram is an application designed for sharing photos and videos. Users can take photos or record videos, use digital filters to edit them, and share them through various social networking platforms, including the Instagram platform itself [14]. The following is the percentage of internet users who use each social media platform (based on a survey), Instagram is in second place in the use of social media in Indonesia, shown in Figure 2 [15].

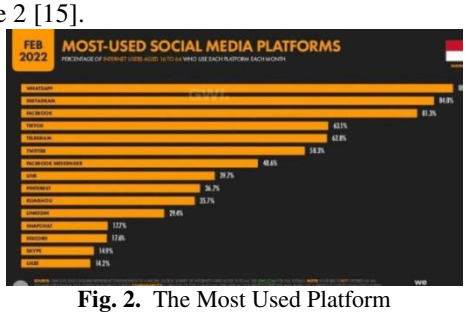


Fig. 2. The Most Used Platform

2.8 Cyberbullying

Cyberbullying can be considered a form of verbal bullying. Cyberbullying, also known as online bullying, refers to actions carried out in cyberspace that aim to humiliate, ridicule, humiliate, denounce, or even threaten victims or other social media users [16].

2.9 Digital Evidence

In cases of crimes in the field of computer technology, there are often traces of activity related to the crime. Evidence of computer crimes can be in the form of physical evidence or digital evidence [17]. Electronic evidence is the electronic device itself or related storage media, while digital evidence includes document files, history, or log files containing related data [18].

Electronic and digital evidence is very important in the computer crime investigation process because they provide information that supports decision-making [19]. Through analysis and interpretation of this evidence, investigators and forensic experts can gain important insights to reveal crimes, identify perpetrators, and strengthen legal cases in court [20].

2.10 Case Skenario

Case scenarios are needed to assist researchers in determining the chronology of the occurrence of cases of indicated crime. Researchers create a scenario where there is a conversation that includes threatening actions or bullying behavior [21]. Then, the evidence of the conversation was deliberately deleted. In the case scenario of this research, there are two Instagram accounts that interact with each other via the Direct Message (DM) feature on an Android-based smartphone. In this interaction, there is one account that acts as a cyberbullying actor and one account as a cyberbullying victim. In the case scenario, the researcher created two Instagram accounts namely Account A (as the perpetrator) and Account B (as the victim). Account A chats with me B by sending messages (normal conditions).

Account A send chating berupa pesan ancaman dan bullying kepada akun B yang menjadi korban.

1. Akun Account A sends chat messages in the form of threats and bullying to account B who is the victim.
2. Account A sends an image to account B.
3. Account A deletes all chat data from account A's device in an effort to destroy evidence.
4. User B reports directly to the authorities for what happened to him. Authorities responded directly to reports of user B.

The next step is for the authorities to issue a search warrant to secure the smartphone belonging to user A, which is used as an access medium for Instagram to communicate with user B. The next stage will involve examining the smartphone owned by user A as physical evidence. The purpose of this check is to identify and retrieve digital evidence in the form of text messages that have been deleted by user A from the smartphone.

Fig. 3. Case Scenario

3 Result and Discussion

TECHNIUM

Technium: Romanian Journal of Applied Sciences and Technology
Vol. 17, 249-254, November, 2023
ISSN: 2668-778X
www.techniumscience.com

3.1 Collection

At this stage, the investigator carried out the acquisition process or taking physical evidence involving an Android smartphone with the type version of SAMSUNG SM-J105F. The device will be used as an object of research.

Smartphone evidence must be rooted first to back up the data on the smartphone. The rooting process is carried out as the first step in mobile digital forensics so that investigators get smartphone access rights as a whole on the Android operating system.

The collection process also records the technical details of the physical evidence used during the research. The following are smartphone specifications in Table 1.

Table 1. Information of Smartphone Specifications

Smartphone Information	
Owner	Arifandi Jibran
Smartphone Name	SAMSUNG
Model Number	SM-J105F
Operating System	Android 5.1.1 (Lolipop)
IMEI	3583100****8014
IMSI	510105639091615
Password	No
External Memory	Yes
SIM Card	Yes
Rooted	Yes

3.2 Examination

At the Examination stage, the process of examining and retrieving data from the cellphone is carried out with the aim of getting data that has been deleted by the perpetrator from the device. The initial step before carrying out data collection is to connect the cellphone to the laptop and install the forensic connector on the smartphone. After that, the MOBILedit Forensic forensic tool will be able to read data from the smartphone if the rooting process has been carried out previously.

It can be seen that the smartphone has been connected to the MOBILEdit Forensic tools used. Furthermore, the data extraction process that has been deleted is carried out concerning the digital data recovery process or information backup.

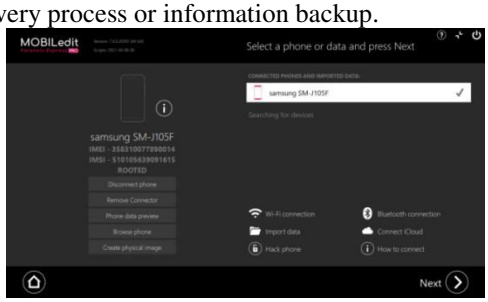


Fig. 4. Examination Process

The first step is to activate airplane mode on the smartphone and require the condition of the smartphone to be in USB debugging enabled mode, then MOBILEdit forensic will install a small application on the cellphone to back up data, you can see the backup process in Figure 5.

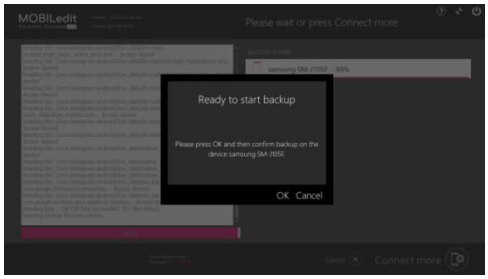


Fig. 5. Process Backup

3.3 Analysis

At the Analysis stage, a search for relevant information is carried out from various data that has been obtained at the examination stage. The data files that are the focus of evidence are text messages (chats) that contain cyberbullying content.

Fig. 6. Conversation Evidence

Figure 6 shows digital evidence in the form of the conversation the suspect sent with the victim. The text message acquisition results that were successfully returned contain the date, month, time, and contents of the message from the suspect. The conversation contains cyberbullying messages directed at the victim.

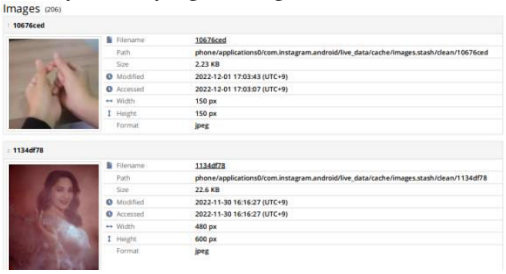


Fig. 7. Image Evidence

Figure 7 shows digital evidence with image file types with a total of 206 images that were successfully extracted and returned. The results of the analysis of the digital image evidence obtained are the digital traces of the suspect in searching and liking photos or images from posts by several other users accounts on Instagram.

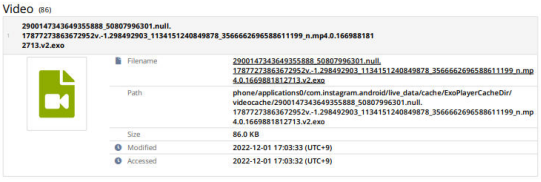


Fig 8. Video Evidence

Figure 8 shows the digital video evidence extracted from the physical evidence of the smartphone that was successfully returned with a total of 86 video digital evidence. The video is a digital trail of the suspect

TECHNIUM

Technium: Romanian Journal of Applied Sciences and Technology
Vol. 17, 249-254, November, 2023
ISSN: 2668-778X
www.techniumscience.com

visiting other Instagram user accounts and then liking the video post or watching the video post.

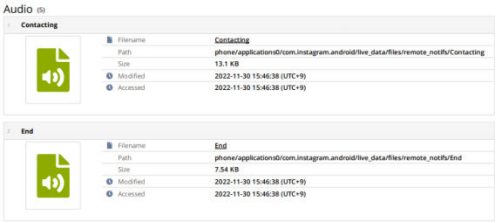


Fig. 9. Audio Evidence

Figure 9 shows the digital audio evidence that was extracted and returned with a total of 5 digital audio evidence that was successfully returned. The audio is an audio notification from the suspect's Instagram account.

Fig. 10. Video Call Log Evidence

Figure 10 shows digital evidence in the form of a video call message made by the suspect to the victim which was successfully acquired by investigators.

The following are digital evidence of conversation messages that were successfully backed up and returned by the investigator in Table 2.

Table 2. Real Conversation Data

Digital Evidence Conversation	Activity Logs	
	Sending	*Delete*
You are arrogant, just read my message	10/11/22 16:12:42	14/12/2022 06:47:39
Pretend to forget or be arrogant	10/11/22 20:49:02	14/12/2022 06:47:39
Yes, you are very cute	10/11/22 20:52:17	14/12/2022 06:47:39
You, who did not pass the test yesterday, are you sorry	10/11/22 20:54:10	14/12/2022 06:47:39
That's why you don't have to take the test if you're stupid	10/11/22 20:54:11	14/12/2022 06:47:39
You're really fat when you take a photo, it's better not to upload more photos	10/11/22 21:02:02	14/12/2022 06:47:39
I'm your friend	10/11/22 21:05:12	14/12/2022 06:47:39
If you don't use a filter, your face will be dirty	11/11/22 13:03:20	14/12/2022 06:47:39
So pretty stupid face	15/11/22 08:42:07	14/12/2022 06:47:39
Try it if you dare	15/11/22 09:12:24	14/12/2022 06:47:39
Before I unfollow and block, I want to say	15/11/22 09:13:24	14/12/2022 06:47:39
NAJISssssss		
Report it, you think I don't know your house, I'll kill you	15/11/22 09:16:11	14/12/2022 06:47:39
Report lives lost	15/11/22 09:16:49	14/12/2022 06:47:39
Want to die brutally	15/11/22 09:17:15	14/12/2022 06:47:39
heh	17/11/22 15:34:14	14/12/2022 06:47:39
Is there a mirror at home?	28/11/22 22:51:10	14/12/2022 06:47:39
ugly so why confident	28/11/22 22:51:28	14/12/2022 06:47:39

3.4 Reporting

The report includes a detailed description of the evidence found as well as a presentation of the forensic tools used in the process of backing up and acquiring evidence.

Table 3. Reporting on Digital Evidence

Information	On Evidence
Smartphone	Samsung SM-J105F
Name Of The Owner	Arifandi Jibran
Username akun	arifandijbrn__
IMEI	358310*****8014

Table 3 shows the information on the digital evidence report on the suspect's smartphone specifications and the username of the suspect's Instagram account that was successfully obtained.

Table 4. Mobiledit Forensic Results

Evidence	Information
Image	206
Conversation	21
Audio	5
Video	86
Call Log	4

The digital evidence found in the forensic analysis of the cellphones seized for investigation, found evidence of image files, audio files, video files, call log files and conversation (chat) files. The final result of the reporting of this research case is chat messages with an analysis of 14 conversational messages from suspects containing cyberbullying aimed at victims according to the evidence found and 7 messages that do not contain cyberbullying, because this digital evidence is accurate and relevant and can be properly understood after going through the analysis phase by looking at the system activity log analysis which shows the time the message was sent and efforts to delete digital evidence by the suspect to remove traces of cybercrime that has been committed.

4 Conclusion

Based on the research conducted, several conclusions were obtained as follows:

1. In this study, a case scenario involving the use of the Samsung SM-J105F smartphone was carried out. The scenario includes the process of rooting the device, installing the Instagram application,

creating a text message, and carrying out an investigation using the MOBILEdit forensic tool. After that, an analysis was performed using three different forensic software.

2. The final result of reporting from this research case is digital evidence of conversational messages (chat) because this digital evidence is accurate and relevant which can be properly understood after going through the stages of analyzing the metadata information in the files found to provide clues about the time of creation, change, location of origin of the evidence file when it was acquired.

References

[1] A. S. Hutagalung, A. B. P. Negara, and E. E. Pratama, "Aplikasi Pendeteksi Cyberbullying Terhadap Komentar Postingan Media Sosial Instagram dengan Metode Naïve Bayes Classifier Berbasis Website," *J. Sist. dan Teknol. Inf.*, vol. 9, no. 3, p. 364, 2021, doi: 10.26418/justin.v9i3.44843.

[2] R. A. Bintang, R. Umar, and A. Yudhana, "Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST," *Techno (Jurnal Fak. Tek. Univ. Muhammadiyah Purwokerto)*, vol. 21, no. 2, p. 125, 2020, doi: 10.30595/techno.v21i2.8494.

[3] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.

[4] J. S. Komputer, F. L. Nafila, I. Fakultas, T. Industri, and U. I. Indonesia, "Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android dengan metode NIST," vol. 6, pp. 532–543, 2022, doi:http://dx.doi.org/10.30645/j-sakti.v6i1.466

[5] A. Nofiyan, "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST)," vol. 8, no. 2, pp. 11–23, 2020, doi: http://dx.doi.org/10.29406/cbn.v4i02.2287

[6] I. Riadi, A. Fadlil, and M. I. Aulia, "Review Proses Forensik Optical Drive Menggunakan Metode National Institute of Justice (NIJ)," *Jutisi J. Ilm. Tek. Inform. dan Sist. Inf.*, vol. 8, pp. 107–118, 2019, doi: 10.35889/jutisi.v8i3.384

[7] 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.

[8] T. N. Manoppo, "Penggunaan Perangkat Mobile Terhadap Suatu Tindak Kejahatan (Studi Kasus Pada Temuan Bukti Digital Short Message Service (Sms) Di Unallocated Data)," *Cyber Secur. dan Forensik Digit.*, vol. 2, no. 1, pp. 30–37, 2019, doi: 10.14421/csecurity.2019.2.1.1419.

[9] A. Galih Pradana and S. Nita, "Rancang Bangun Game Edukasi 'AMUDRA' Alat Musik Daerah Berbasis Android," *J. Semin. Nas. Teknol. Inf. dan Komun. 2019*, vol. 2, no. 1, pp. 49–53, 2019.

[10] S. K. Dirjen *et al.*, "Terakreditasi SINTA Peringkat 2 Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop," *Masa Berlaku Mulai*, vol. 1, no. 3, pp. 829–836, 2017, doi: https://doi.org/10.29207/resti.v4i5.2152.

[11] Y. N. K. Yadi, Ilman Zuhri, "Analisis Forensik Pada Platform Android," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, pp. 87–95, 2019.

[12] C. Sya, D. Misnawati, J. Jend, And A. Y. No, "Penggunaan Media Sosial Instagram Pada Akun @ Yhoophii _ Official Sebagai Media Komunikasi Dengan Pelanggan," vol. 14, no. 1, pp. 32–41, 2020.

[13] J. Jordan, N. Listia, and K. Daniel, "Perancangan Desain Konten Sosial Media tentang Sepak Bola melalui Instagram dengan berbasis Microblog," *J. DKV Adiwarna*, vol. 1, no. 18, p. 10, 2021.

[14] M. S. I. Lubis, "DAMPAK KOMUNIKASI DAN PERUBAHAN SOSIAL BAGI PENGGUNA INSTAGRAM," *J. War. Ed.*, 2018, doi: https://doi.org/10.46576/wdw.v0i55.209.

[15] Simon Kemp, "DIGITAL 2022: ANOTHER YEAR OF BUMPER GROWTH," *Wearesocial.com*, 2022. https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/ (accessed Jun. 12, 2022).

[16] N. L. A. M. Dwipayana, S. Setiyono, and H. Pakpahan, "Cyberbullying Di Media Sosial," *Bhirawa Law J.*, vol. 1, no. 2, pp. 63–70, 2020, doi: 10.26905/blj.v1i2.5483.

[17] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. Media Inform. Budidarma*, vol. 6, no. 2, p. 1263, 2022, doi: 10.30865/mib.v6i2.3946.

[18] R. Sistem *et al.*, "Jurnal resti," vol. 1, no. 10, pp. 45–54, 2021.

[19] D. Mualfah and R. A. Ramadhan, "Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 2, pp. 257–267, 2020, doi: 10.31849/digitalzone.v11i2.5174.

[20] M. A. Aziz, I. Riadi, and R. Umar, "2616-6260-1-Sm," *Semin. Nas. Inform. UPN "Veteran" Yogyakarta*, vol. 2018, no. November, pp. 51–57, 2018.

[21] R. N. Dasmen and F. Kurniawan, "Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial," *Techno.Com*, vol. 20, no. 4, pp. 527–539, 2021, doi: 10.33633/tc.v20i4.5170.