International Journal of Information System & Technology
Akreditasi No. 36/E/KPT/2019 | Vol. 5, No. 3, (2021), pp. 331-338

Forensic Whatsapp Investigation Analysis on Bluestack Simulator Device Using Live Forensic Method With ACPO Standard

Kurniadin Abd. Latif[1], Rifqi Hammad[2], Tomi Tri Sujaka[3], Khairan Marzuki[4], Andi Sofyan Anas[5]

[1,2] Software Engineering Study Program, Universitas Bumigora
[3,4] Computer Science Study Program, Universitas Bumigora
[5]Application Software Engineering Study Program, Universitas Bumigora

e-mail: [1]kurniadin@universitasbumigora.ac.id, [2]rifqi.hammad@universitasbumigora.ac.id, [3]tomi_tri@universitasbumigora.ac.id, [4]khairan.marzuki@universitasbumigora.ac.id, [5]andi.sofyan@universitasbumigora.ac.id

Abstract

This study aims to conduct a forensic analysis of the WhatsApp application on the Bluestacks android simulator device. BlueStacks App Player is designed to allow Android apps to run on PCs running Microsoft Windows and Apple's macOS. In this study, the scenario was carried out using two devices as Whatsapp communication media. The first device is a laptop device that uses the Bluestacks android simulator with the SM-G955F device type, and the second is a smartphone device as opposed to communication. This study uses the ACPO standard which consists of several stages such as Plan, Capture, Analysis, Present. Pada tahap Capture, teknik yang digunakan dalam melakukan pencarian bukti pada aplikasi BlueStacks adalah live forensik. Hasil penelitian ini menunjukan bahwa analisis forensik pada perangkat android simulator Bluestacks dapat dilakukan sesuai prosedur ACPO. From the procedure carried out, information related to communication on the WhatsApp application was obtained. The source of this information is obtained from the WhatsApp database file msgstore.db.crypt12 which has been decrypted using the SQLite Browser application with a combination of the WhatsApp Key file contained in the cloned digital evidence. From the results of the decryption that has been carried out, then an explanation is carried out through the WhatsApp viewer application to make it easier to understand from the display side.

Keywords*: Analysis, Forensics, Whatsapp, Bluestacks, ACPO*

1. Introduction

Based on data compiled by GWI, more than half of the population in Indonesia, or 56.2% have used smartphones in 2018. A year later, as many as 63.3% of people use smartphones. Until 2025, at least 89.2% of the population in Indonesia has used smartphones. In the six years since 2019, smartphone penetration in the country has grown by 25.9% [1]. Almost 94 percent of the population aged 16-64 years use social media such as YouTube, WhatsApp, Instagram, and others [2]. Social media is online media that is used as a social tool that allows humans to interact with each other without any limitations of space and time.. Social media consists of various types such as content, social networks, microblogs, instant messages, and others. WhatsApp is an instant messaging application that operates over the internet. Based on data compiled by GWI, the use of the WhatsApp application is ranked second after YouTube in 2020 and 2021 [2]. The use of this WhatsApp application is very effective as a communication tool or medium. But on the other hand, this utilization also has a negative impact that we cannot just ignore. With the sophistication of today's digital devices, crime is also getting more

ISSN : 2580-7250

sophisticated in various ways that have never existed before. There are several cases related to the misuse of WhatsApp such as fraud, pornography, insults, and others. On the other hand, WhatsApp can be used as a guide for other cases outside the ITE law such as murder, corruption, and others. The WhatsApp app is a smartphone app, but there are also web and desktop versions. The web and desktop versions must be integrated with the smartphone. Besides smartphones and the web, the WhatsApp application can also be run on simulated devices such as the BlueStacks App Player. This method in the future can be used as an opportunity to commit crimes because this is an application that runs on a computer that can be deleted at any time with the aim of eliminating evidence of a crime.

Based on Locard's Exchange Principle developed by Dr. Edmond Locard (1877-1966) stated that there is no activity without a trace. As a consequence of these activities, this is a section that has a high value in disclosing criminal investigation cases, because it can show the relationship between the things involved in the case. Several studies related to forensic analysis of the use of applications as a tool to commit crimes such as those carried out by [3] which was to analyze and investigate mobile forensics on the WhatsApp application. This study performs recovery of the WhatsApp database to get WhatsApp data that has been deleted through attacks via remote access using the Sypnote application. Based on the research carried out starting from the preservation stage to reporting the results of digital artifacts obtained from the WhatsApp database and other WhatsApp data, 100% can be recovered and extracted depending on the length of time for deletion using the CWM application. This research was conducted on android smartphone devices.

Another study was conducted by [4] which was to analyze the web-based WhatsApp messenger forensic investigation. The purpose of this study was to find evidence of WhatsApp conversations through the Mozilla Firefox and Chrome web browsers. The results of this study are SQLite data found in a sub-directory containing a WhatsApp Web conversation database that must be extracted, conversations found following WhatsApp evidence on the main smartphone.

Another research by [5] is to conduct network forensic analysis on WhatsApp. In his research describes how to decrypt network traffic and get forensic artifacts related to the features of text messages, group messages, audio/video calls. The purpose of this research is to find out hidden communications that use encryption to protect the integrity of the messages exchanged by knowing them through forensic and sniffing techniques. The result of his research is that whatsapp network forensics contains hidden artifacts and we get a lot of information that can be of evidence value. In particular, how do we analyze network traffic to describe the data contained in the network.

Another research by [6] is to conduct a live forensic analysis on WhatsApp web to prove cases of electronic transaction fraud. The purpose of this study is to prove cases of fraudulent electronic transactions on the Whatsapp web using the Live forensics method. The NIST (National Institute of Standards and Technology) methodology with the stages of collection, examination, analysis, and reporting is used in this study. The search for digital evidence was carried out on the perpetrator's laptop, while the victim's smartphone was used as a comparison. Digital evidence is analyzed in the form of conversational texts, images, and videos. Live forensics is performed with RAM imaging as well as the acquisition of log files, cache, and browser history using the FTK Imager and Browser History Viewer. The results of the study are the conversation text, image filename, video filename, timestamp, history, the perpetrator's account number, and the victim's cellphone number which is digital evidence to prove the case. Digital evidence from the Live Forensic process is legal evidence based on UU Number 11 of 2008 concerning Information and Electronic Transactions.

Based on the problem above, the researcher wants to discuss the WhatsApp analysis on the bluestack simulation application. In this discussion, we discuss how to do the bluestack rooting process, get a key from WhatsApp to open WhatsApp databases, and extract the WhatsApp database using the live forensic method. The analysis was carried out to find evidence in the form of chat content that had been carried out.

2. Research Methodology

2.1. Live Forensik

Live forensics techniques have evolved in the last decade, such as analysis of memory content to get a better picture of applications and running processes [7]. Live forensics methods have similarities to traditional forensic techniques, namely storage identification, analysis, and presentation, Live forensics methods are a response to the shortcomings of traditional forensic techniques that cannot get information from data and information that only exists when the system is running, for example, Memory activity, Network processes, Swap files, running system processes, and information from system files and these are the advantages of Live forensic techniques.

2.2. ACPO

This study uses the ACPO standard with the live forensics method in searching for evidence of WhatsApp chat on the BlueStacks application. The ACPO standard is a Procedure or SOP that refers to the Association of Chief Police Officers (ACPO). ACPO has been adopted by Police Forces in England, Wales, and Northern Ireland. ACPO procedures generally consist of Plan, Capture, Analysis, Present [8].

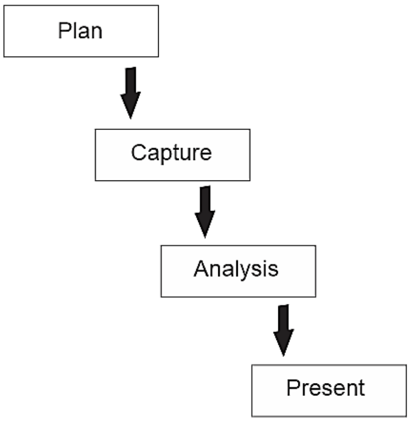


Figure 1. ACPO stage

The explanation of the standard steps of the ACPO procedure, among others:

a) Plan
This stage is the stage in determining what types of evidence may have a connection with the crime committed. At this stage, strategies are also determined in handling evidence so that evidence and digital data can be well preserved.

b) Capture
This stage is where the process of recording, capturing, and seizing everything related or relevant to the crime committed is carried out. This stage is also related to the process of acquiring or cloning digital evidence. Every process or activity carried out must be recorded or documented. People attending a scene should be acutely aware that a powered-on (running) system needs to be handled with care, as there is the potential to make unintended changes to the evidence if this is not handled properly.

c) Analyze.
At this stage, where the equipment that has been confiscated and has been acquired will be analyzed as part of the search for evidence and information. Due to the volume and complexity of data stored on digital devices, it is not possible or desirable to extract all data stored on devices for review by investigators.

Instead, a forensic strategy needs to be formulated to allow the examination to be focused on the relevant data.

d) Present

This stage is the stage where digital evidence is described and presented in the form of presentations or reports that are easy to understand. This stage is very important because the nature of digital forensic evidence is not always immediately understood by the layman.

2.3. Scenario

This study conducted a scenario using two devices as Whatsapp communication media. The first device is a laptop device that uses the Android Bluestacks simulator with the SM-G955F device type and the second is a smartphone device. BlueStacks is an American technology company known for its BlueStacks App Player and other cloud-based cross-platform products. BlueStacks App Player is designed to allow Android apps to run on PCs running Microsoft Windows and Apple's macOS. The communication carried out is in the form of sending ordinary messages. The scenario scheme carried out is shown in Figure 2.

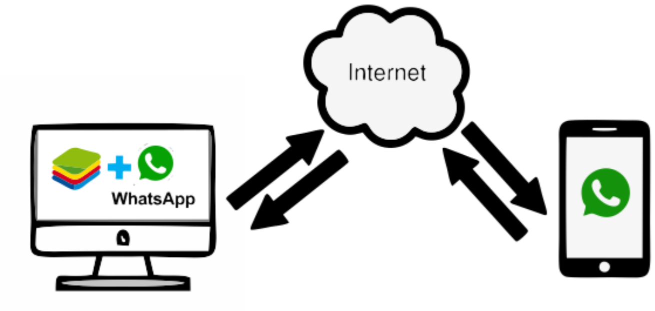


Figure 2. Scenario

Figure 2 is an illustration of the scenario carried out, namely WhatsApp communication between 2 devices. The results of the communication will be used as digital evidence which is carried out according to the standard for the acquisition of digital evidence.

3. Result and Discussion

3.1. Plan

At this stage, the determination of what types of evidence may have a connection with the crime committed. Based on the scenario, the crime was committed through the WhatsApp application. Generally, applications can be run via a smartphone as the master, besides that WhatsApp can also be run via a browser and laptop by linking the device or synchronizing with the master. In addition, the master can also be run via a PC or laptop by installing the android simulator or IoS Simulator. At this stage, a strategy is also designed for handling evidence. In the scenario, communication is carried out with Whatsapp on the "Bluestack" android emulator. Handling evidence between real devices and emulator devices, of course, there are differences in the implementation. In this scenario, the method used is live forensic techniques. Live forensic are techniques that are carried out by means of the condition of the device in live or on the state.

3.2. Capture

At this stage, it is the process of taking digital evidence from a device suspected of being a tool to commit a crime or violation. Every process or activity carried out must be recorded or documented. This process is carried out using the live forensic method. The flow that is carried out includes:

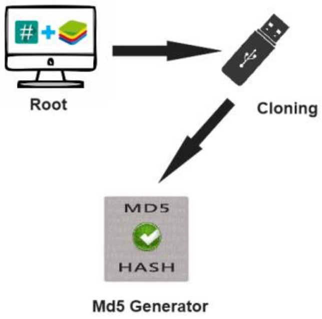
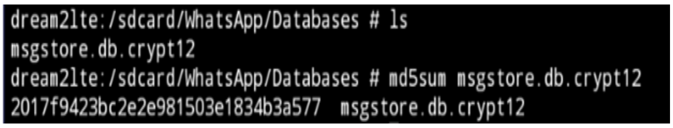


Figure 3. Cloning Process Flow

Figure 3 is the flow of the capture stage in the form of an acquisition or cloning process carried out to obtain evidence from the bluestacks application. This process is carried out directly while the computer is on and carried out carefully, in order to maintain the integrity of the evidence to be analyzed further and can be accounted for. The explanation of each stage includes:

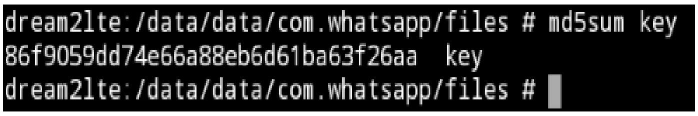
a) Root Bluestacks by using Bluestacks tweaker. The purpose of this root is to get root access to retrieve or clone the WhatsApp key. After rooting, search for the WhatsApp database and WhatsApp key then check the hash before cloning to another device (flash disk).

   1) Root Bluestacks by using Bluestacks tweaker. The purpose of this root is to get root access to retrieve or clone the WhatsApp key. After rooting, search for the WhatsApp database and WhatsApp key then check the hash before cloning to another device (flash disk).



```
dream2lte:/sdcard/WhatsApp/Databases # ls
msgstore.db.crypt12
dream2lte:/sdcard/WhatsApp/Databases # md5sum msgstore.db.crypt12
2017f9423bc2e2e981503e1834b3a577  msgstore.db.crypt12
```

Figure 4. Screenshot of database file location and hash check results

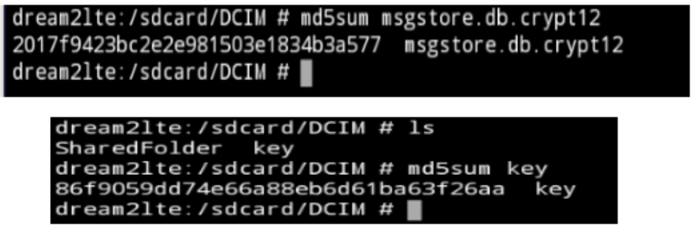


```
dream2lte:/data/data/com.whatsapp/files # md5sum key
86f9059dd74e66a88eb6d61ba63f26aa  key
dream2lte:/data/data/com.whatsapp/files # █
```

Figure 5. Screenshot of the Whatsapp Key file location and hash check results

b) Cloning using FTK Imager. This process aims to duplicate the evidence for further analysis. This duplication is done to avoid direct access against the original digital evidence, which may cause the digital evidence to be damaged.

c) Check Hash using Md5 on digital evidence that has been cloned. This process aims to check and re-assure that the digital evidence has not changed after cloning. If there is a change, then the digital evidence is invalid and cannot be further analyzed. The following is the result of the hash check.



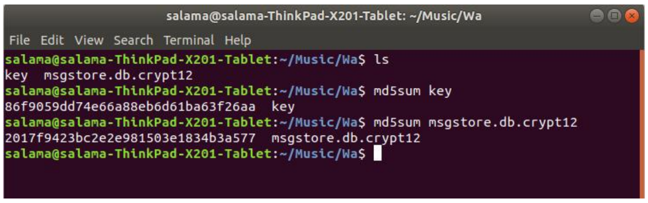
```
dream2lte:/sdcard/DCIM # md5sum msgstore.db.crypt12
2017f9423bc2e2e981503e1834b3a577  msgstore.db.crypt12
dream2lte:/sdcard/DCIM # █
```

```
dream2lte:/sdcard/DCIM # ls
SharedFolder  key
dream2lte:/sdcard/DCIM # md5sum key
86f9059dd74e66a88eb6d61ba63f26aa   key
dream2lte:/sdcard/DCIM # █
```

Figure 6. Check Hash results after being cloned or acquired

3.3. Analysis

At this stage, an analysis of digital evidence that has been cloned or acquired is carried out. Before further analysis is carried out, it is necessary to re-check the hash of the digital evidence to ensure that the digital evidence to be analyzed is the same digital evidence as to the digital evidence that has been cloned or previously acquired. The hash check results are done using Md5.


salama@salama-ThinkPad-X201-Tablet: ~/Music/Wa
File Edit View Search Terminal Help

```
salama@salama-ThinkPad-X201-Tablet:~/Music/Wa$ ls
key  msgstore.db.crypt12
salama@salama-ThinkPad-X201-Tablet:~/Music/Wa$ md5sum key
86f9059dd74e66a88eb6d61ba63f26aa  key
salama@salama-ThinkPad-X201-Tablet:~/Music/Wa$ md5sum msgstore.db.crypt12
2017f9423bc2e2e981503e1834b3a577  msgstore.db.crypt12
salama@salama-ThinkPad-X201-Tablet:~/Music/Wa$ 
```

Figure 7. Checksum results using Md5 before being analyzed

After doing the checksum, then the decryption process is carried out on the digital evidence of the WhatsApp database that has been cloned using SQLite Browser. This decrypt process requires a key to open all WhatsApp conversations from the digital evidence database. The results of the decryption can be seen in Figure 8.

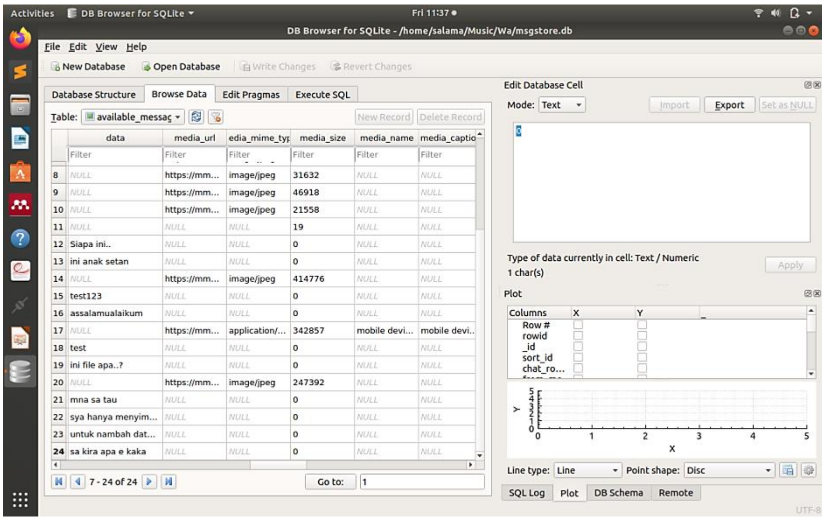


Table: available_messag

	data	media_url	edia_mime_typ	media_size	media_name	media_captio
	Filter	Filter	Filter	Filter	Filter	Filter
8	NULL	https://mm...	image/jpeg	31632	NULL	NULL
9	NULL	https://mm...	image/jpeg	46918	NULL	NULL
10	NULL	https://mm...	image/jpeg	21558	NULL	NULL
11	NULL	NULL	NULL	19	NULL	NULL
12	Siapa ini..	NULL	NULL	0	NULL	NULL
13	ini anak setan	NULL	NULL	0	NULL	NULL
14	NULL	https://mm...	image/jpeg	414776	NULL	NULL
15	test123	NULL	NULL	0	NULL	NULL
16	assalamualaikum	NULL	NULL	0	NULL	NULL
17	NULL	https://mm...	application/...	342857	mobile devi...	mobile devi...
18	test	NULL	NULL	0	NULL	NULL
19	ini file apa..?	NULL	NULL	0	NULL	NULL
20	NULL	https://mm...	image/jpeg	247392	NULL	NULL
21	mna sa tau	NULL	NULL	0	NULL	NULL
22	sya hanya menyim...	NULL	NULL	0	NULL	NULL
23	untuk nambah dat...	NULL	NULL	0	NULL	NULL
24	sa kira apa e kaka	NULL	NULL	0	NULL	NULL

7 - 24 of 24 Go to: 1

Mode: Text

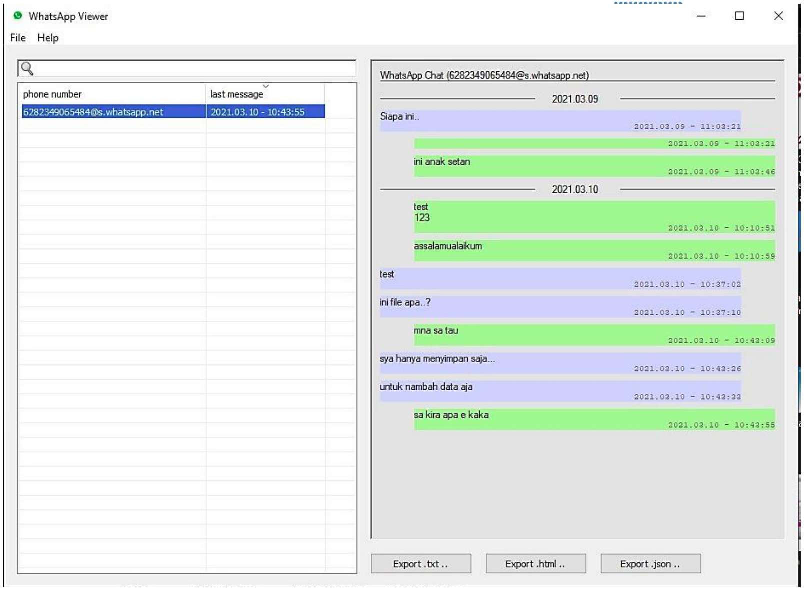
Type of data currently in cell: Text / Numeric
1 char(s)

Line type: Line Point shape: Disc

Figure 8. Database Decrypt Results

3.4. Present

This stage is the stage where the results of the investigation are presented in the form of reports and presentations. This stage aims to make it easier for judges to understand information from communications or conversations made through the WhatsApp application. From the results of the decryption that has been done, it will produce a database with open access status, then the database is presented using the WhatsApp viewer application for easier understanding. The results of the exposure carried out using the WhatsApp viewer are in the image.



phone number	last message
6282349065484@s.whatsapp.net	2021.03.10 - 10:43:55

WhatsApp Chat (6282349065484@s.whatsapp.net)

2021.03.09

Siapa ini.. 2021.03.09 - 11:03:21

2021.03.09 - 11:03:21

ini anak setan 2021.03.09 - 11:03:46

2021.03.10

test
123 2021.03.10 - 10:10:51

assalamualaikum 2021.03.10 - 10:10:59

test 2021.03.10 - 10:37:02

ini file apa..? 2021.03.10 - 10:37:10

mna sa tau 2021.03.10 - 10:43:09

sya hanya menyimpan saja... 2021.03.10 - 10:43:26

untuk nambah data aja 2021.03.10 - 10:43:33

sa kira apa e kaka 2021.03.10 - 10:43:55

Figure 9. Presentation of Communication Information on Whatsapp via Whatsapp Viewer

4. Conclusion

Based on the results and discussions carried out, it is concluded that the forensic analysis of WhatsApp on the Bluestacks simulator android device can be carried out according to the procedure. The method used in this Bluestack WhatsApp forensic analysis is the ACPO standard procedure which consists of several stages, namely Plan, Capture, Analysis, and Present. At the Capture stage, live forensic techniques are used to obtain specific digital evidence. From the procedure carried out, information related to communication on the WhatsApp application was obtained. The source of this information is obtained from the WhatsApp database file msgstore. db.crypt12 which has been decrypted using the SQLite Browser application with a combination of the WhatsApp key file contained in the cloned digital evidence. From the results of the decryption that has been carried out, then an explanation is carried out through the WhatsApp viewer application to make it easier to understand from the display side.

References

[1] Y. Pusparisa, “Pengguna Smartphone diperkirakan Mencapai 89% Populasi pada 2025,” *katadata.co.id*, 2020. [Daring]. Tersedia pada: https://databoks.katadata.co.id/datapublish/2020/09/15/pengguna-smartphone-diperkirakan-mencapai-89-populasi-pada-2025. [Diakses: 15-Jul-2021].

[2] Yudo dahono, “Data: Ini Media Sosial Paling Populer di Indonesia 2020-2021,” *beritasatu.com*, 2021. [Daring]. Tersedia pada: https://www.beritasatu.com/digital/733355/data-ini-media-sosial-paling-populer-di-indonesia-20202021. [Diakses: 13-Jul-2021].

[3] E. Palallo, “Analisis dan Investigasi Mobile Forensik pada Aplikasi WhatsApp Artikel Ilmiah,” *Artik. Ilm.*, 2017.

[4] N. Anwar dan I. Riadi, “Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web,” *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, hal. 1, 2017.

[5] Ubaidillah dan D. Stiawan, “Analisis Forensik Jaringan pada WhatsApp,” *Annu. Res. Semin.*, vol. 3, no. 1, hal. 1–4, 2017.

[6] S. D. Utami, C. Carudin, dan A. A. Ridha, “Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik,” *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, hal. 24–32, 2021.

[7] Syngress, *Scene of the Cybercrime: Computer Forensics Handbook*. Rockland: Syngress Publishing, Inc, 2002.

[8] DAC Janet Williams QPM, *ACPO Good Practice Guide for Digital Evidence*, 5 ed. Wales, 2012.