Mobile Forensic Signal Instant Messenger Services in Case of Web Phishing using National Institute of Standards and Technology Method

Trisna Irawan
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
The increasing online dependence of the entire world creates opportunities for cybercrime to occur. One of the problems with instant messaging applications that trigger phishing cybercrimes is the Signal application.Phishing is a criminal activity that uses social engineering techniques.The purpose of this study is to carry out a forensic process on an android smartphone in the form of a web phishing case using the National Institute of Standards and Technology (NIST) method to obtain digital evidence on the Signal Instant Messenger application.This study uses the NIST method with four forensic stages, namely collection, examination, analysis, and reporting. Forensic tools used to collect digital evidence are MOBILedit Forensic Express Pro and Belkasoft Evidence Center. The process in obtaining evidence is by making acquisitions of two smartphones. The acquisition results are used as digital evidence to prove the occurrence of crimes that lead to web phishing cases.The results of this study show that the MOBILedit Forensic Express Pro and Belkasoft Evidence Center tools obtained evidence from the first smartphone in the form of contacts, account phone numbers, text messages, and picture messages. Meanwhile, the second smartphone did not get the expected evidence, either using the MOBILedit Forensic Express Pro or Belkasoft Evidence Center tools, because the smartphone was not rooted and the security of the encrypted storage device system failed at the acquisition stage for digital evidence retrieval.It is hoped that further research will be able to acquire on smartphones the state of the data intentionally or accidentally deleted by the perpetrators and be able to acquire the latest android version.

Keywords
Mobile Forensic, NIST,Phishing, Signal Instant Messenger

1. INTRODUCTION
Technological developments provide the same benefits and impacts depending on the users of the technology. The benefits obtained from technology are that it makes it easier for individuals or groups to carry out their activities, while the negative impact is that development in terms of socializing becomes very slow, because they are too focused on gadgets. In addition, the negative impact is the misuse of technology by individuals or groups for criminal acts that can harm others[1].Today's increasingly sophisticated technology has become an inseparable part of society, followed by many social media users, where social media make it very easy for users to get information easily and quickly and to communicate, such as sending text messages, pictures, and videos for free[2].Social media that are often used by most people are Instagram, Line Messenger, WhatsApp, Telegram, Signal Messenger, and others[3].Signal is software that offers a messaging service whose features and functions are almost the same as other chat applications such as WhatsApp, Line, and others. Signal Messenger was launched in 2013 by Moxie Marlinspike. This app can be easily used to send chat, voice and video calls without fear of being watched by anyone. Currently, its users have penetrated more than 50 million. Currently, people are committing many crimes (Cybercrime), such as cyberbullying, extortion, trafficking in illegal goods, drug trafficking, fraud, human trafficking, and others. The increase in cyber crime in business organizations, government infrastructure, and individuals has emphasized the importance of cyber security. Therefore, cyber attack analysis is one of the things that needs to be done.The Anti-Phishing Working Group (APWG) saw 384,291 attacks in March 2022, which is the highest monthly total in APWG reporting history. In the first quarter of 2022, APWG observed 1,025,968 total phishing attacks. This is the worst quarter for phishing the APWG has observed, and the first time the quarterly total has exceeded one million. The previous record was 888,585 attacks, observed in the fourth quarter of 2021. The number of phishing attacks has more than tripled since early 2020, when the APWG observed between 68,000 and 94,000 attacks per month[4].

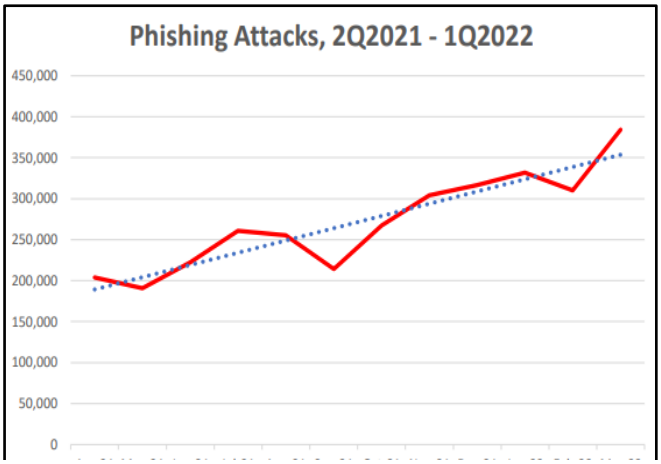

Figure 1. Phishing Attack Statistics in 2022

Figure 1 shows statistics. The number of phishing website attacks detected in January was 331,698, then in February there were 309,979 and in March 384,291 the highest in early 2022. This research will be conducted through the Signal Messenger application by applying the stages of the NIST (Collection, Examination, Analysis and Reporting) method using the forensic tools MOBILedit Forensic Express and

Belkasoft Evidence Center, which are expected to obtain digital evidence in cases of web phishing.

1.1 Literature Study

1.1.1. Previous Research

This study refers to five previous studies conducted to compare the current study with previous studies. The first research entitled "Forensic Analysis to Detect the Authenticity of Digital Images Using the NIST Method"[5].The results obtained in this study with the tools used in the forensic identification process of video files (digital image analysis).

The second research entitled "Skype Digital Evidence Recovery Analysis based on Android Smartphone Using the NIST Framework"[6].Generating digital proof recovery of Samsung J2 smartphone data with the deletion method through the Oxygen manager tool application cannot produce deleted data and the presentation of success using Belkasoft is 26%. While the results of data recovery with the manual deletion method, the success of using Oxygen is 63% and Belkasoft is 44%. The digital proof results from Andromax A in the deletion scenario through the Oxygen and Belkasoft applications cannot produce the deleted ones. While manual deletion of Oxygen is 61% and Belkasoft cannot restore data.

The third research entitled "Forensic Against Digital Evidence in Revealing Cybercrime"[1]. In this research, all simulation files as well as other files that have been stored on flash disk before reformatting can be detected or recovered. The FTK Imager and Autopsy tools are still not able to perform data acquisition and analysis with permanent deletion and encryption (password) treatment on the flash disk using Windows 10's built-in tools, namely BitLocker Drive Encryption.

The fourth study entitled "Investigation Analysis of Android Forensic Short Message Service (SMS) on Smartphones"[7].The deleted SMS has been found, from the sms evidence found in the mmssms.db file. The metadata of the mmssms.db file contains the md5 hash value, file capacity, time of creation (created), time of access (accessed), time of modification (modified), time of change (changed).

The fifth research is entitled “Digital Forensic Analysis of CCTV Camera Recordings Using the NIST (National Institute of Standards Technology) Method”[8].In this study, the results of CCTV video recordings about the characteristics of digital evidence and metadata information are produced.

1.1.2. Digital Forensics

Digital forensics is a scientific study method that results from the identification, preservation, collection, validation, analysis, interpretation, documentation and presentation of digital evidence. The evidence comes from electronic devices such as computers, laptops, smartwatches, and smartphones[6].Digital forensics is a scientific method that studies the maintenance of the collection, validation, analysis, interpretation, documentation and presentation of digital evidence originating from digital sources for the purpose of facilitating the reconstruction of criminal events or helping to anticipate actions that are proven to violate prescribed procedures[9].To carry out proper and appropriate investigations, not only use computer forensics but also develop forensics for mobile or mobile phones that need to be carried out to obtain digital evidence[10].

1.1.3. Mobile Forensics

Forensics is related to the types of electronic evidence in the form of cellphones and smartphones. Mobile Forensics is a branch of digital forensics which is carried out to find and analyze evidence related to cybercrime cases so that it can be legally accounted for[6].Mobile forensics is a branch or derivative of digital forensics. Mobile forensics aims to recover data from mobile devices[11].There are a number of pieces of evidence that can be extracted from cell phones. Types of evidence that can be extracted from cell phones include: other contact numbers, call logs, sms messages, audio files, emails and internet history. These artifacts can be extracted by logical or physical methods. Logically, it extracts data from system files by interacting directly with the device using special tools or software for forensic mobile devices[12].

1.1.4. Digital Evidence

Digital evidence is data collected from any type of digital storage that is the subject of a computer forensic examination. So anything that carries digital information can be the subject of research, and any carrier of information targeted for examination should be treated as evidence[13].There are two similar terms for digital evidence, namely electronic evidence and digital evidence. Electronic evidence is physical and can be identified visually, such as computers, mobile phones, cameras, CDs, hard disks, and others. While digital evidence is in the form of evidence extracted or recovered from electronic evidence, the evidence can be in the form of evidence in the form of files, emails, messages, pictures, videos, logs or text.[8].There are many challenges and difficulties encountered in processing digital evidence on mobile devices. Some of them are differences in mobile phone hardware, security features, lack of resources, such as USB cables, batteries, and chargers for different mobile devices, anti-forensic techniques, dynamic or volatile evidence, accidental reset processes, device changes , passcode recovery and malicious programs[14].

1.1.5. Instant Messaging

Instant messaging is a facility for internet users to communicate via chat. Instant Messaging can communicate by sending text messages with other users. In addition, Instant Messaging also serves to exchange files. Instant messaging, better known as Online Chat, is a long-distance communication tool that has a fast transmission speed[15].

1.1.6. Signal Messenger

Signal is a cross-platform and centralized encrypted messaging service developed by the Signal Technology Foundation and Signal Messenger LLC. Users can send one-to-one and group messages, which can include files, voice notes, pictures, and videos. The app can also be used to make voice, one-to-one and group video calls, and the Android version can optionally function as a texting app.

1.1.7. Cybercrime

Cybercrime is a form of crime that arises because of the use of internet technology[3].Cybercrime is a consequence of the over-availability and ability of users of computer systems in unethical hands[16]. Cybercrime is any kind of use of computer networks for criminal purposes by abusing the convenience of digital technology[17].Cybercrime has several types, such as unauthorized access, illegal content, hacking and cracking, data falsification, and many others. This is the use of information technology to bully people to send or post texts that are intimidating or threatening to others[3].

1.1.8. Phishing

Phishing is a cybercrime activity that uses social engineering and technical fraud to steal identity data and financial credentials. The social engineering scheme is carried out using fake emails claiming to be from legitimate business institutions and designed to direct victims to deceptive fake websites, so that victims leak financial data such as names and passwords[18].Phishing can also be defined as a form of eavesdropping on websites so that customers' personal data can be stolen[19].Web Phishing is the most widely used method for perpetrators because it has a similar appearance to the original website. Therefore, it is very likely that the victim could be trapped in a phishing web[20].

1.1.9. Android

Android is an operating system that was originally created for mobile devices, such as smartphones and tablets, but has now become popular and popular on other smart devices, such as cars, televisions, and watches. The kernel is based on Linux, but also includes components not normally found in the Linux kernel[3].Android provides an open platform for developer users to create their own applications that will be used by various mobile devices[21].

1.1.10. Smartphone

The smartphone is a communication tool that continues to grow every year. Smartphones are not only used as a communication tool, smartphones can also be used for other purposes, such as online shopping, money transfers, playing games, and social media. Smartphones are not only for making voice calls but can also take pictures and can install many applications that ordinary mobile devices cannot do, such as chatting, sharing videos, photos and documents[22].Android smartphone technology provides an opportunity for application developers to expand the use of applications, especially Signal social media on the Android operating system[23]

1.1.11. Forensic Tools

Hardware and software are digital forensic tools that are used to facilitate the digital forensic process[24]. Forensic tools are available to assist investigators in collecting data related to the case under investigation. Appropriate forensic tools are needed to collect evidence and ensure the authenticity of digital evidence so that it can be accepted and needs to be ensured through mechanisms such as hashing or implementing write protection to maintain data integrity and prevent changes to data or files that make digital evidence unacceptable. Differences in the use of forensic tools will also affect the digital evidence obtained.

1.1.12. NIST

The National Institute of Standards and Technology (NIST) is a method that is often used to analyze digital evidence artifacts or forensic stages in order to obtain information from digital evidence. This method refers to the basic stages in forensic analysis, namely collection, examination, analysis, and reporting, as presented in Figure 2[25].

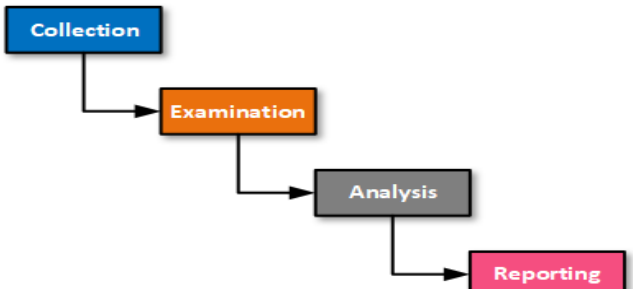

Figure 2. Stage of National Institute of Standards and Technology

The following is an explanation of the stages contained in the National Institute of Standards and Technology (NIST) in the digital evidence analysis process:

1. Collection
   The collection stage or stage in data collection with the aim of identifying various sensitive information that is considered very important in the analysis process and how all the data can be collected properly.
2. Examination
   The examination stage is carried out through the process of processing the data collected forensically by using various combinations of scenarios, both automatic and manual, calculating and sorting the appropriate information in the case study from the original data that has been collected while protecting the integrity of the data.
3. Analysis
   Data analysis can be done with various approaches or algorithms. The task of this analysis includes various activities, such as identifying users who are indirectly involved in cases, analyzing examination results using other methods or approaches that are technically and legally justified in order to obtain useful information and can respond to questions-questions that can drive the audit data collection process.
4. Reporting
   The reporting stage is reporting the results of the forensic analysis stage, which includes a description of the perpetrator's activities taken, a description of the selected forensic tools and procedures, determining other actions that need prevention and carried out with other aspects of the forensic process. There are several factors that can affect the results of documentation and reports, including the following:
   a. Alternative Explanations, namely an analyst who basically must be able to use an approach or method to approve or reject any explanation of a case or case being carried out.
   b. Owner Consideration (Audience Consideration) is to provide data or various information to the audience which is very useful and necessary in the forensic process. Cases involved with a number of rules are urgently needed in specific reports relating to the data that has been collected. Besides that, a copy of data is very much needed.
   c. Actionable Information is a process of recording and reporting documentation that includes how to identify actionable information that can be obtained from a set of data generated from previous data and then, with the help of this data, we can draw conclusions and take the latest information from the results of the sorting.

2. METHODOLOGY

2.1 Research Scenario

This research does not use real scenarios, but uses engineered scenarios, including smartphones, phone numbers, usernames, and other identities. This scenario started with an actor named Dila who spread promotions about sweepstakes or prizes in the form of tens of millions of money.Among these promotions, the perpetrator fills in a URL to trap the victim so that later the victim can be easily fooled by the URL. Then the victim accesses the URL and inputs personal data that has been provided on the website.Perpetrators get sensitive data such as email, ID numbers, and other data. After the perpetrator obtains the identity of the victim, the perpetrator deletes messages related to the spread of promotions regarding sweepstakes or prizes to remove traces so that other people do not know about their actions.This scenario uses 11 numbers for the simulation of the incident, where 10 numbers are the destination numbers in the phishing spread and 1 number is the perpetrator himself on behalf of Dila.One of these numbers is a victim of the perpetrator who will carry out a forensic process to verify data from the perpetrator. Then the perpetrator's smartphone will be carried out a forensic process according to a cyber crime case study in the form of phishing or visual-based fraud. The details of the scenario are shown in Figure 3.

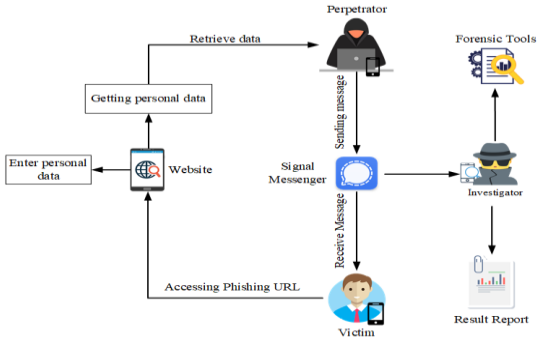

Figure 3. Web Phishing Case Scenario

Figure 3 indicates that a case of web phishing occurred in the Signal application. Initially, the perpetrator sent a broadcast message to several telephone numbers in the form of phishing via a signal application, then the victim opened the message and accessed the website URL sent by the perpetrator. Then the victim sees the information on the website and then the victim is interested and fills in his personal data on the website. The victim's personal data can be accessed by the perpetrator through the database on the website. Messages in the Signal application will be examined by investigators from the perpetrator's device using the MOBILedit Forensic Express Pro and Belkasoft Evidence Center tools. After carrying out the examination process using forensic tools, the investigator then makes a report of the results of the examination of the web phishing case that occurred in the Signal application.Reports resulting from forensic acquisitions by investigators can be used later for court proceedings according to studies analyzing cases. Reports can be in the form of brief explanations of artifact analysis or case study analysis of digital evidence.This scenario will use two android smartphones. Two Smartphones with the Signal application installed, which will then be examined by investigators. The tools used in this study can be seen in Table 1.

Table 1. Research Tools

No	Tools Name	Description	Information
1	Laptop	HP 14-cm0066au, 8GB DDR 4, Memori 1 TB	Hardware
2	Windows 10	Windowsn10 Pro	Operating system
3	*Smartphone* 1	Samsung Galaxy J3 Pro	Hardware
4	*Smartphone* 2	Samsung Galaxy J6	Hardware
5	Signal	Versi 5.46.6	Android Application
6	MOBILedit Forensic Express Pro	Versi7.2.0.17975	Forensic Tools
7	Belkasoft Evidence Center	Versi 1.13.10673	Forensic Tools

In Table 1, it is a forensic tool needed to examine evidence on a smartphone. The examination will use the MOBILedit Forensic Express Pro and Belkasoft Evidence Center applications.The application will be used to collect supporting data from smartphones associated with messages in the form of phishing. Then the existing evidence will be analyzed and reported. The implementation of the case scenarios mentioned earlier was carried out on two smartphones with the status of evidence. This study simulates the evidence in the form of the Samsung Galaxy J3 Pro smartphone as smartphone 1 and the Samsung Galaxy J6 as smartphone 2.

Figure 4. Smartphone as Digital Evidence

The Figure 4 shows smartphone devices used in this study were 2 units, smartphone 1 using the Samsung Galaxy J3 Pro brand cellphone and smartphone 2 using the Samsung Galaxy J6 brand cellphone, each of which has different specifications. The specifications of the two smartphones can be seen in Table 2.

Table 2. Specifications of Smartphone Evidence

Specification	Smartphone 1	Smartphone 2
Brands	Samsung	Samsung
Seri	Galaxy J3 Pro	Galaxy J6
IMEI	358067081384445	358471092069732
OS	Android	Android
OS Version	5.1 (Lollipop)	10 (Quince Tart)

Table 2 is evidence of smartphones that have different specifications. For smartphone 1, the condition of the cellphone is rooted, while smartphone 2 is not in a root condition. The difference between the first and second smartphones can be seen from the IMEI. The IMEI of each smartphone has different values as a differentiator between one smartphone and another. For example, if a smartphone with the Samsung J3 Pro brand and Samsung J6 has a different IMEI as a differentiator.

2.2 Research Stages

2.2.1. Mobile Forensics Stage Diagram

Forensic stages are carried out in obtaining digital evidence. So that the search process is very easy to follow by following the existing steps. The stages of mobile forensics in obtaining digital evidence can be presented as shown in Figure 5.

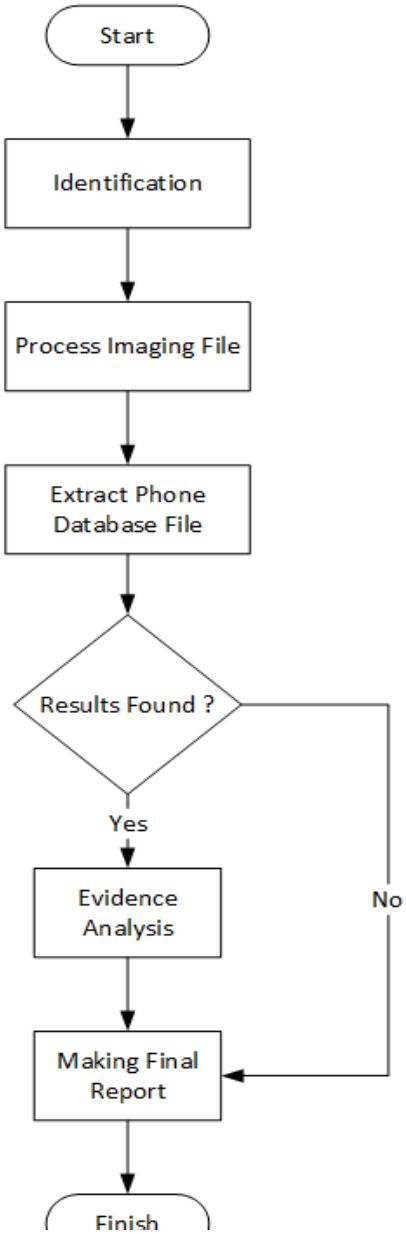

Figure 5. Diagram Stage of Mobile Forensics

Based on Figure 5 the investigation process begins with the identification of evidence related to the case being handled.The next process is Imaging File or Data Backup.This process will minimize changes to the smartphone. Extraction of data on evidence in the form of smartphones using the MOBILedit Forensic Express and Belkasoft applications. After the results are found, an analysis of the evidence is carried out. After obtaining all the necessary data, then making a report related to the results found to help strengthen the evidence in court.

2.2.2. Collection

This stage is the initial stage of the NIST method in which they search and collect data. In the case scenario, it is explained that the smartphone is a tool used by the perpetrator to send messages, the smartphone becomes evidence of a crime.The evidence obtained from this study is 1 cellphone with the Samsung Galaxy J3 Pro brand belonging to the perpetrator and 1 cellphone brande Samsung Galaxy J6 brand, to the victim. In addition, other evidence was found, namely 1 data cable used to charge the brand's cellphone Samsung

Galaxy J3 Pro and 1 power cable are used to charge the Samsung Galaxy J6 brand cellphone. The two smartphones that have become evidence have the Signal application installed.The evidence that has been collected can be seen in table 2.To keep the evidence original and undamaged, data integrity can be maintained by isolating physical evidence and making backups in the form of clones or evidence image files. This stage of taking digital evidence has a very high risk. If a fatal error occurs, data and digital evidence on the smartphone can be lost or damaged (problematic) so that it cannot be read. Therefore, it is necessary to preserve it in the form of a physical image. The process of data obtained through extraction from smartphone 1 is shown in Figure 6 using the MOBILedit Forensic Express application for the process of taking evidence. This stage determines what evidence is needed to determine whether the evidence processed is in accordance with the case study or not.

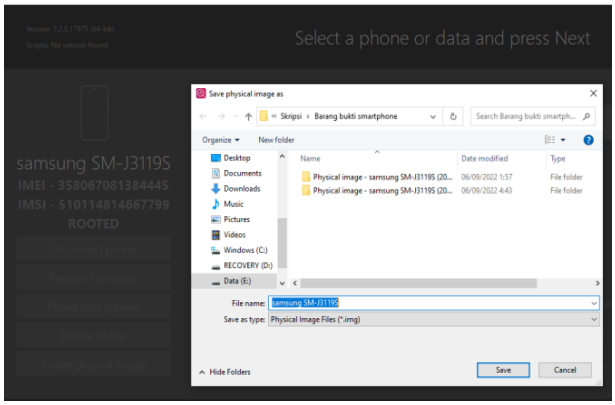

Figure 6. Backup Process for Smartphone Evidence

Figure 6 shows the smartphone proof backup process using the MOBILedit Forensic Express application. MOBILedit Forensic Express is capable of making smartphone backups with the extension AB (Android Backup), img, zip, and several other types of extensions so that they can be opened in various forensic applications. The results of this backup process are image documents from each Android smartphone with the img extension with varying document sizes depending on the amount of data on the smartphone. The results of smartphone backups can be seen in Figure 7.

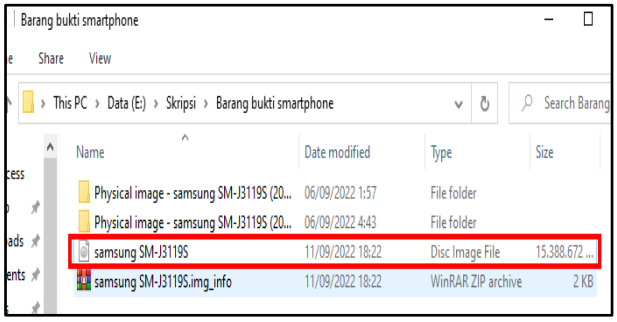

Figure 7. Backup Process Results

Figure 7 is an imaging result from the perpetrator's smartphone with the information that the imaging file is internal to the perpetrator's smartphone, so the file size of the imaging results depends on the size of the internal storage on the smartphone.

2.2.3. Examination

Two forensic applications were used as acquisition tools at this stage of the examination, namely MOBILedit Forensic Express and Belkasoft. Checking with MOBILedit Forensic Express has 2 ways. The first way is that the evidence must be connected to the computer or laptop where MOBILedit Forensic Express is installed. The second way is to create an image file from a smartphone that has been imaged previously. In this examination process, the second method is done by opening an image file from a smartphone that has been imaged previously.The initial process is to open the physical image data, which can be done by selecting imported data, then clicking on the physical image, then selecting the image file from the smartphone that has been done with the previous physical image. The type of file is Disc Image File (img).The acquisition process did not run long enough, wait a few minutes and then the acquisition process was complete. Acquisition generates overall application target data and acquisition results reports. The acquisition process is presented in Figure 8.

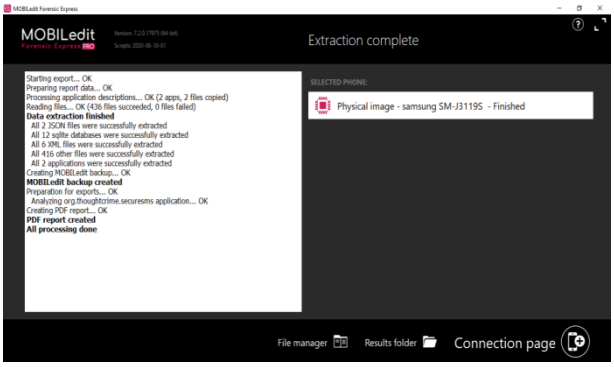

Figure 8. MOBILedit Acquisition Process on Smartphone

Figure 8 is the acquisition process from a smartphone, this process will take a few minutes and then after the acquisition process is complete it will displayresults.To see the results after exporting the data, see the selected storage destination. The results of the smartphones that have been acquired are shown in Figure 9.

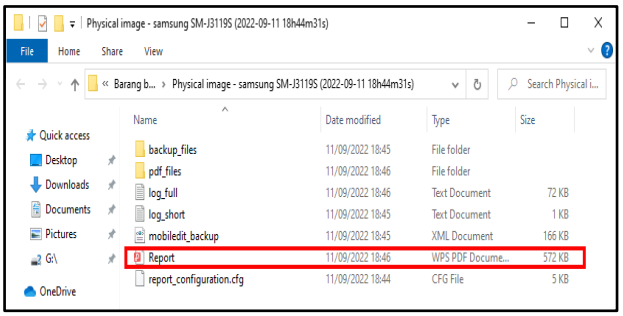

Figure 9. Smartphone Acquisition Results using MOBILedit

Figure 9 shows the results of the smartphone acquisitionsamsung galaxy j3 pro using the MOBILedit application. The export results are stored in the folder E:\Thesis\Smartphone Evidence\Physical image - samsung SM-J3119S (2022-09-11 18h53m24s). The export results are backup_file, pdf_files, tmp_files, log_full, log_short, mobileedit_backup, Report.pdf, and report_configuration.cfg. The selected full report is in PDF format. In the Report.pdf file you can see the results of previous acquisitions of the Samsung Galaxy J6 smartphone.The extraction results that have been carried out with MOBILedit Forensic Express will be displayed in a full report. In this study, the selected full report is in PDF format. Full report display of smartphone evidence as presented in Figure 10.

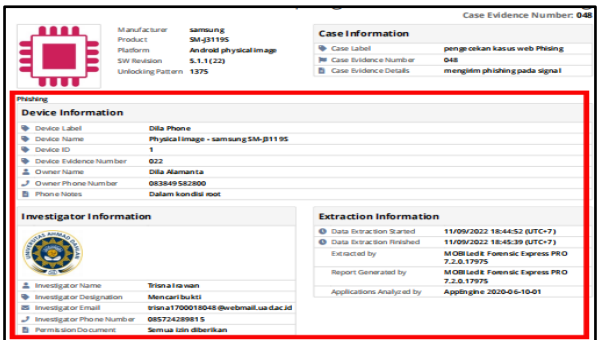

Figure 10. Full Report of MOBILedit Smartphone

Figure 10 is a display of the full report. The full report contains information on device information, investigator information, and extraction information. Examination with Belkasoft can perform direct extraction and extraction through physical images. Examination with Belkasoft is done by extracting the physical image that has been created using the previous MOBILedit Forensic Express. Extraction results are obtained in the form of files such as contacts, text messages (chat), and image files. Each of these files has a different size and number of files according to the number of chats contained in the signal application on each smartphone.

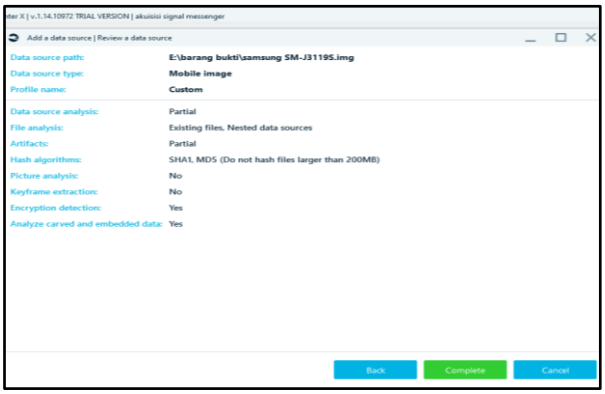

Figure 11. Belkasoft Acquisition Process on Smartphone

Figure 11 is a view of the reviewsource of data to be acquired.There is information about the data source path, which is a file taken from storage. The file is a samsung SM-J31195.img.The file is contained from the results of processing the physical image on MOBILedit Forensic Express Pro.

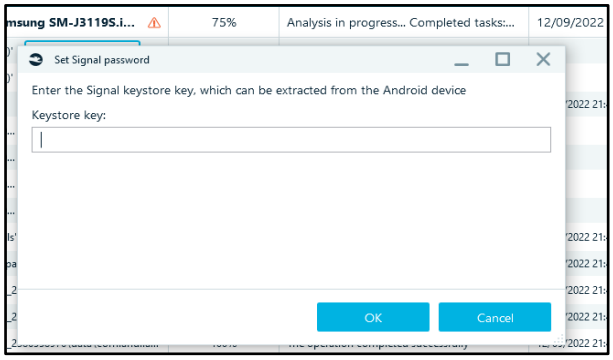

Figure 12. Input Keystore key Signal

In Figure 12 is a display of information about the input of the keystore key signal. So that the acquisition process can run well on the signal application, it is necessary to fill in a keystore key to make it easier to get data on the application. The data stored in the signal application regarding phishing cases carried out by the perpetrators. The keystore key is found in the org.thoughtcrime.securesms_preferences.xml file. The keystore key can be seen in Figure 13.

Figure 13. Keystore key data on Signal

Figure 13 shows information about the keystore data for the keys in the signal application, in the form of a code that is "92e3f5817375f9e4bed2cd57308102b0651949a0e08773d6a7 238508e7abce2c". Then there is a backup password code, namely "06259 09098 65423 13823 80469 32203". The data is used to make it easier to open files in the signal application during the acquisition process.The data is used to make it easier to open files in the signal application during the acquisition process.After the acquisition process is complete then generate report data. The full report displays evidence of one of the smartphones extracted by Belkasoft as can be seen in Figure 14.

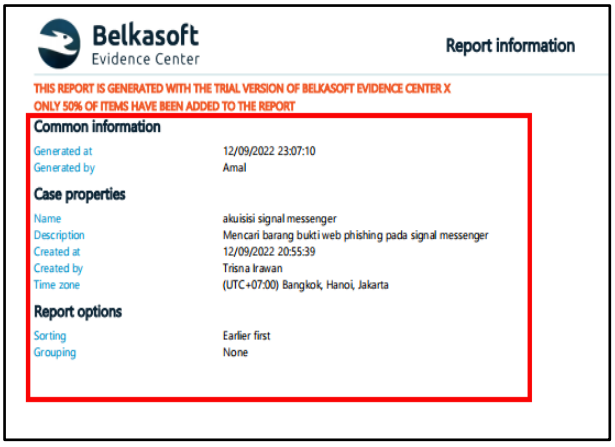

Figure 14. Results of Acquisition of Belkasoft Smartphone

Figure 14 is a display of the report results from Belkasofton the Samsung Galaxy J3 Pro smartphone. The report contains the date of the resulting acquisition process, case properties including case name, case description, case creation date, case maker or investigator name, and time, as well as report options.The acquisition result from the Belkasoft application uses an image file resulting from a physical image from MOBILedit Forensic Express Pro. Belkasoft forensic application has successfully acquired a smartphone.

2.2.4. Analysis

The Analysis stage is the analysis stage or the stage to see the results of the previous Examination stage in detail to obtain digital evidence on forensic evidence. This study limits the search for digital evidence to the results obtained from the Signal application in the form of accounts, contacts, text messages (chat), and pictures. The extraction results obtained

from the Examination process that has been carried out on two smartphones using the MOBILedit Forensic Express application get results in the form of mobile phone numbers, contact lists, text messages, and images.

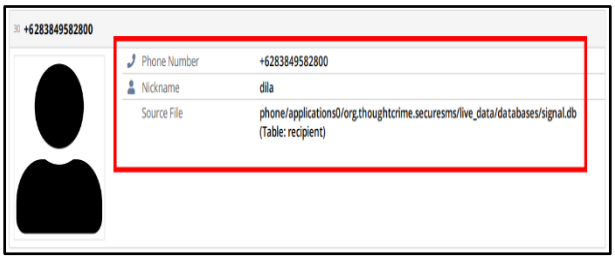

Figure 15. Information on the Perpetrator's Cellphone Number on Smartphone Evidence

In Figure 15 the mobile number of the perpetrator whoused on the signal application account in committing crimes in the form of phishing. The number is 083849582800 with the nickname "dila`".The perpetrator uses the number for the signal account as an action in spreading phishing messages. The message is spread by the perpetrators to several signal accounts in a broadcast manner, which later on the victim will be provoked to access the URL contained in the message.

Figure 16. Contact Information on Smartphone Evidence

Figure 16 shows that there are 48 contacts obtained on the evidence. The contact is a mobile number stored on the smartphone in the signal application. These numbers are used for the distribution of phishing messages by the perpetrators.

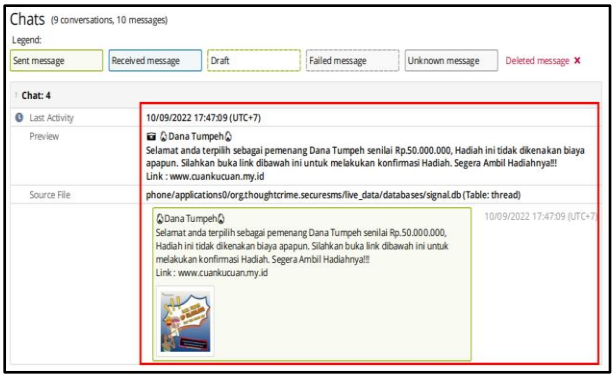

Figure 17. Proof of Text Messages on Smartphone Evidence

In Figure 17 there is evidence of text messages (chat) obtained on smartphones. The message indicates that there is a phishing message or tricking the victim by sending a promotional or gift message and a URL for the victim to then access.The URL shown in the message is "cuankucuan.my.id", which can be seen in Figure 18.

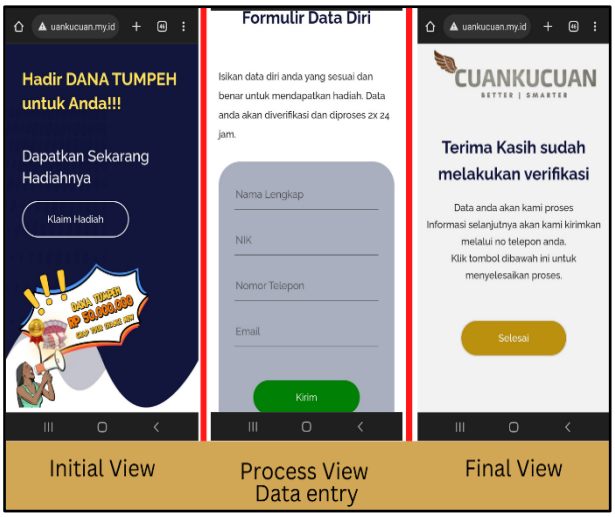

Figure 18. Phishing Web Display

Figure 18 is a phishing web display accessed from the URL found in the perpetrator's message. This URL is distributed by the perpetrator to trick the victim into accessing the web and filling in their personal data.The data entered includes the full name, nick, phone number and email, the data is sensitive data owned by the victim. The data that has been inputted will later be accessed by the actors on the web database.

Figure 19. Image Evidence on Smartphone Perpetrator's

Figure 19 shows evidence of images obtained on a smartphone. The image contains promotional words or cash prizes and includes a phishing web URL on the image.

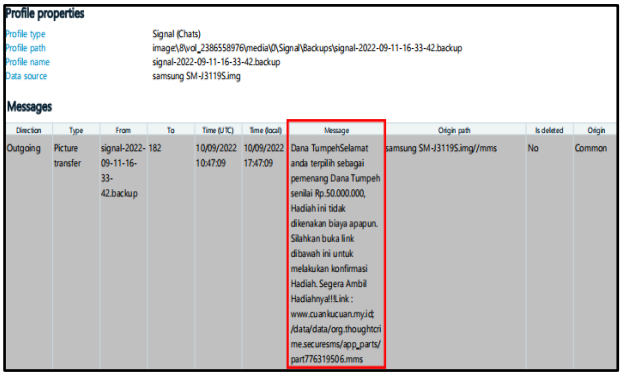

Figure 20. Smartphone Text Message Proof on Belkasoft

Figure 20 shows the messages found on thesmartphone samsung galaxy j3 pro, the message contains information about the phishing message sent by the perpetrator to the victim. There is information about the image sent by the perpetrator to the victim in the form of a promotional image,

but the image cannot be read in the results of the report provided by the Belkasoft application.This is because the Belkasoft application that investigators use is the free Belkasoft application or trial, so the Belkasoft application only provides information about the results of reports from evidence.Smartphones that are carried out in the acquisition process only get 50% of the data provided, so there is data that has not been found or read on the smartphone. However, in the Belkasoft application on the artifacts menu, an image was found which was presented in Figure 21.

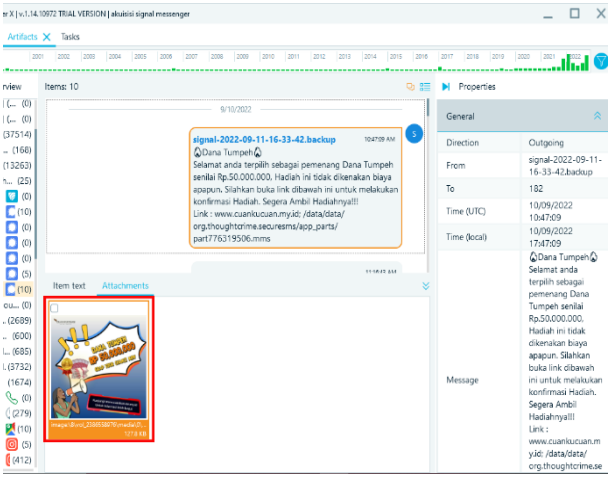

Figure 21. Smartphone Image Evidence on the Artifacts Menu Belkasoft

In Figure 21 found a message and an image that was sent by the perpetrator to the victim in the form of phishing information, namely a message about a promotion or gift to trick the victim and there is a website URL created by the perpetrator which will later be accessed by the victim, the URL is "cuankucuan.my.id".

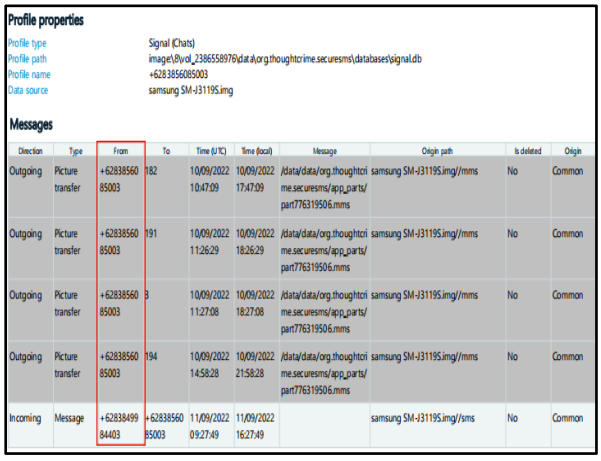

Figure 22. Smartphone Account Contact Information on Belkasoft

Figure 22 shows that it managed to get the signal account contact number used on the Samsung Galaxy J3 Pro smartphone, but for the other contact numbers or the victim it could not be found.There is only information about the intended purpose of the perpetrator in sending a message.

2.2.5. Reporting

The Reporting stage is the stage of making a report in the form of data from the analysis in the previous stage, which includes a description of what evidence has been obtained and the presentation of the success of forensic tools in carrying out extractions in obtaining evidence. proof. The results obtained from the acquisition process of 2 smartphones can be seen in table 3 and table 4.

Table 3. Digital Evidence Obtained on a Smartphones 1

No	Proof Digital	Forensic Tools	
		MOBILedit	Belkasoft
1	Account	1	1
2	Contact	48	0
3	Chat	9	5
4	Picture	9	1

Based on table 3, the extraction results from MOBILedit Forensic Express Pro get 1 mobile account number, 48 contacts, 9 chats and 9 pictures.While the extraction results from Belkasoft get 1 mobile account number, 5 chats and 1 picture. For contact can't be found on Belkasoft.The results of the acquisition of smartphone 2 can be seen in table 4.

Table 4. Digital Evidence Obtained on a Smartphone 2

No	Proof Digital	Forensic Tools	
		MOBILedit	Belkasoft
1	Account	0	0
2	Contact	0	0
3	Chat	0	0
4	Picture	0	0

Based on table 4, the extraction results from MOBILedit Forensic Express Pro and Belkasoft could not be found.As explained in the analysis stage, this is because the device storage is still encrypted and the smartphone condition is not rooted, so extraction using the MOBILedit Forensic Express Pro and Belkasoft applications does not give the expected results or gives zero results (zero result)and prove that technology security is more secure and prove that Signal data cannot be opened by just anyone.

3. CONCLUSION

Based on the discussion and results of research and testing using the National Institute of Standards and Technology (NIST) method and the stages of mobile forensic procedures on smartphones, it can be concluded that the NIST forensic method can be obtained as evidence in the form of information used by perpetrators to commit crimes on instant messenger signal applications with web phishing case.The results obtained from the acquisition of 2 pieces of evidence using 2 forensic applications can be concluded that the analysis process using MOBILedit Forensic Express Pro on a smartphone obtains smartphone account numbers, contacts, text messages, and images as well as for deleted text messages that have not been found.As for the smartphone 2 did not get any results from the acquisition stage. In the analysis process using the Belkasoft Evidence Center on smartphone 1, get a smartphone account number, text messages and pictures. Smartphone 2 does not give the expected results. In other words, smartphone 2 gives zero results. This is because the acquisition process at Belkasoft failed, thus making the acquisition of smartphone 2 not produce the desired results. This study only uses a smartphone with an old android version, it is recommended to use a different model or type of smartphone and use the latest android version. It is hoped that in the next research, development will be carried out using forensic applications and supporting software with the latest versions, both paid and unpaid in testing a case to get maximum evidence, because the era of security levels on smartphones and social media applications is getting more and more advanced.

4. REFERENCES

[1] M. Riskiyadi, "Forensic Investigation of Digital Evidence in Exposing Cybercrime," *CyberSecurity and Digit Forensics.*, vol. 3, no. 2, hal. 12–21, 2020, [Daring]. Available on: http://202.0.92.5/saintek/cybersecurity/article/view/2144.

[2] Imam Riadi, Rusydi Umar, dan M. I. Syahib, "Digital Evidence Acquisition of Viber Messenger Android Using National Institute of Standards and Technology (NIST) Method," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, hal. 45–54, 2021, doi: 10.29207/resti.v5i1.2626.

[3] I. Riadi, Sunardi, dan P. Widiandana, "Investigating Cyberbullying on WhatsApp Using Digital Forensics," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, hal. 730–735, 2020, [Daring]. Available on: https://jurnal.iaii.or.id/index.php/RESTI/article/view/2161/285.

[4] P. E. Reports, P. S. Trends, B. P. Measurement, E. P. Attacks, M. Targeted, dan I. Sectors, "Uni fying the Global Response To Cybercrime," no. June, hal. 1–13, 2022.

[5] K. Khairunnisak, H. Ashari, dan A. P. Kuncoro, "Forensic Analysis To Detect Authenticity Of Digital Image Using The Nist Method," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 3, no. 2, hal. 72–81, 2020, doi: 10.31598/jurnalresistor.v3i2.634.

[6] A. Yudhana, A. Fadlil, dan M. R. Setyawan, "Analysis of Skype Digital Evidence Recovery based on Android Smartphone Using NIST Framework," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, hal. 682–690, 2020, [Daring]. Available on: http://jurnal.iaii.or.id/index.php/RESTI/article/view/2093/278.

[7] M. Unik, V. G. Larenda, dan H. Mukhtar, "Android Forensic Short Message Service (SMS) Investigation Analysis On Smartphone," *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 3, no. 1, hal. 10–15, 2019, [Daring]. Available on: http://www.ejournal.pelitaindonesia.ac.id/ojs32/index.php/JOISIE/article/download/414/374.

[8] D. Mualfah dan R. A. Ramadhan, "Digital Forensic Analysis of CCTV Camera Recordings Using the NIST (National Institute of Standards Technology) Method," *IT J. Res. Dev.*, vol. 5, no. 2, hal. 171–182, 2020, doi: 10.25299/itjrd.2021.vol5(2).5731.

[9] N. Nasirudin, S. Sunardi, dan I. Riadi, "Forensic Analysis of Android Smartphones Using the NIST Method and the MOBILedit Forensic Express Tool," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, hal. 89, 2020, doi: 10.32493/informatika.v5i1.4578.

[10] A.- Ahmadi, "Google Drive Forensic Data Acquisition On Android With The National Institute of Justice (NIJ) Method," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 4, no. 1, hal. 8, 2018, doi: 10.24014/coreit.v4i1.5803.

[11] M. Fitriana, K. A. AR, dan J. M. Marsya, "Application of the National Institute of Standards and Technology (NIST) Method in Digital Forensic Analysis for Handling Cyber Crime," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, hal. 29, 2020, doi: 10.22373/cj.v4i1.7241.

[12] S. Madiyanto, H. Mubarok, dan N. Widiyasono, "Mobile Forensics Investigation Mobile Forensics Investigation Process on IOS-Based Smartphones," *J. Rekayasa Sist. Ind.*, vol. 4, no. 01, 2017, doi: 10.25124/jrsi.v4i01.149.

[13] I. Riadi, A. Yudhana, dan M. Al Barra, "Mobile Forensics on LinkedIn Social Media Services," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 6, no. 1, hal. 9–20, 2021, doi: 10.14421/jiska.2021.61-02.

[14] A. Wirara, B. Hardiawan, dan M. Salman, "Identification of Digital Evidence on Mobile Device Acquisition of Instant Messaging Application 'WhatsApp,'" *Teknoin*, vol. 26, no. 1, hal. 66–74, 2020, doi: 10.20885/teknoin.vol26.iss1.art7.

[15] E. Zuliarso dan H. Februariyant, "Utilization of Instant Messaging for Academic Service Applications," *Jurna; Teknol. Inf. Din.*, vol. 18, no. 2, hal. 112–121, 2013.

[16] N. Iman, A. Susanto, dan R. Inggi, "Analysis of Digital Forensics Development in Cybercrime Investigation in Indonesia (Systematic Review)," *J. Telekomun. dan Komput.*, vol. 9, no. 3, hal. 186, 2020, doi: 10.22441/incomtech.v9i3.7210.

[17] F. Natsir, "Content Forensic Analysis and Timestamp on Tiktok App," *STRING (Satuan Tulisan Ris. dan Inov. Teknol.*, vol. 6, no. 2, hal. 203, 2021, doi: 10.30998/string.v6i2.11454.

[18] Z. Efendy, I. E. Putra, dan R. Saputra, "Phishing Web Attack Analysis on E-commerce Services with Network Forensic Process Method," *J. Terap. Teknol. Inf.*, vol. 2, no. 2, hal. 135–146, 2019, doi: 10.21460/jutei.2018.22.103.

[19] J. Ju *dkk.*, "Cyberfraud Criminal Witness In Law Number 11 Year 2008 Regarding Information and Electronic Transactions Reviewed According to Islamic Criminal Law," *J. Chem. Inf. Model.*, vol. 43, no. 1, hal. 7728, 2020, [Daring]. Available on: https://online210.psych.wisc.edu/wp-content/uploads/PSY-210_Unit_Materials/PSY-210_Unit01_Materials/Frost_Blog_2020.pdf%0Ahttps://www.economist.com/special-report/2020/02/06/china-is-making-substantial-investment-in-ports-and-pipelines-worldwide%0Ahttp://.

[20] A. Nofiyan dan M. Mushlihudin, "Forensic Analysis on Web Phishing Using the National Institute Of Standards And Technology (NIST) Method," *JSTIE (Jurnal Sarj. Tek. Inform.*, vol. 8, no. 2, hal. 53, 2020, doi: 10.12928/jstie.v8i2.16697.

[21] Y. N. K. Yadi, Ilman Zuhri, "Forensic Analysis On Android Platform," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, hal. 87–95, 2019.

[22] H. M. Al Fawareh dan S. Jusoh, "The Use and Effects of Smartphones in Higher Education," *Int. J. Interact. Mob. Technol.*, vol. 11, no. 6, hal. 103–111, 2017, doi: 10.3991/ijim.v11i6.7453.

[23] I. Riadi, A. Yudhana, M. Caesar, dan F. Putra, "Digital Evidence Acquisition on Android-Based Instagram Messenger Using the National Institute Of Justice (NIJ) Method," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, hal. 219–

227, 2018.

[24] A. Yudhana, I. Riadi, dan I. Anshori, "Facebook Messenger Digital Evidence Analysis Using the Nist Method," *It J. Res. Dev.*, vol. 3, no. 1, hal. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[25] Mustafa, I. Riadi, dan R. Umar, "E-mail Forensic Investigation Design with the National Institute of Standards and Technology (NIST) Method," *Snst Ke-9*, vol. 9, hal. 121–124, 2018, [Daring]. Available on: https://publikasiilmiah.unwahas.ac.id/index.php/PROSIDING_SNST_FT/article/download/2385/2371.