The Comparison National Institute of Standards and Technology and Digital Forensics Research Workshop Method in Instant Messenger Services

Vendratama Catur Prasetya
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
There have been many crimes committed through the internet (cybercrime). Especially for the problem of cybercrime, digital forensics is needed, where the handling is the same as in other forensic fields, only in the handling of digital forensics, the media used to obtain evidence is through mobile devices and other digital devices. This researchaims to compare the results of the tools used, namely MOBILedit Forensic, Magnet AXIOM, and FTK Imager. As well as knowing the differences in digital forensic methods between the methods of the National Institute of Standards and Technology and Digital Forensics Research Workshop. In this research, it is necessary to carry out research stages including case simulation used to obtain data to be investigated next is a comparison of tools used to determine the application that has the best extraction results, the next stage is to analyze NIST method in which there are four stages including Collection, Examination, Analysis and Reporting and DFRWS method that consists of six stages, including Identification, Preservation,Collection,Examination, Analysis, and Presentation, then an analysis of the differences between two methods is carried out. The results showed the use of tool MOBILedit Forensic WhatsApp with the extraction percentage in the form of group chat and picture by 50% and tool Magnet AXIOM by 50%, and tool FTK Imager by 25%, while the use of tool Magnet AXIOM WhatsApp Business, the extraction percentage in the form of group chat and picture 50% and a tool MOBILedit Forensic is 0% and tool FTK Imager 25%. This researchcan determine the strengths and weaknesses of the forensic method between NIST and DFRWS methods in handling cyberbullying and online shop fraud, with NIST method is more inclined to reporting evidence and for handling cases that are not too complex, while DFRWS method is more directed to handling by investigators and for handling more complex cases.

Keywords
Cybercrime, DFRWS, NIST,WhatsApp, WhatsApp Business

1. INTRODUCTION
Human needs in the use of information technology have now turned into a major need, different from previous years, especially for the millennial generation who cannot be separated from information technology. Along with the rapid development of information technology, it has many positive impacts, especially in supporting daily life. On the other hand, it has a negative impact that cannot be avoided. With the sophistication of digital devices at this time, crime is also advancing, with various new modes of crime that have never existed before. Crimes in the field of information technology are commonly referred to as cybercrime. Referring to the katadata.co.id website, statistics on reports of cybercrime cases in Indonesia that occurred in 2021 [1].Statistics on cybercrime cases can be seen in Figure 1.

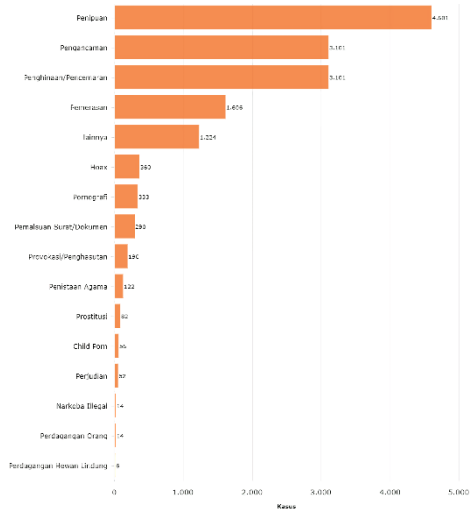

Figure 1. Cybercrime Statistics

Figure 1 is a statistical report on cybercrime cases where fraudulent content occupies the top rank with a total of 4,601 cases, followed by threats and insults or slander content with the same number of cases, namely 3,101, and for the last rank, there is the trade-in protected animals, with a total of 6 case reports. According to research conducted by Ana Irawati, regarding the role of cyber law and how it is applied in Indonesia. The results of the research showed that the role of cyber law in strengthening national information system security is very strategic[2]. According to the report obtained on wearesocial.com, in October 2020 the number of social media users in the world was at 4.14 billion users or 53% of the total world population, while at the beginning of the year In 2021, there were 4.20 billion social media users or 53.6% of the total world population [3]. One of the most popular social media that is widely used by the world community is WhatsApp and WhatsApp Business. In 2021, there were approximately 1250 case reports out of a total of 1885 cybercrime[4]. To handle the crime cases described above, expertise in the field of digital forensics is required. As for making it easier to handle cybercrime cases, a method in digital forensic investigations is needed. There are several kinds of digital forensic methods that can be used, including NIJ [5], NIST[6], DFRWS[7], IDFIF[8], GCFIM [9], SRDFIM. In this research, the researcher used 2 methods. Namely the National Institute of Standards and Technology

method and the Digital Forensics Research Workshop method, which aims to find out the differences in the application between the two methods.

2. STUDY LITERATURE

2.1 Previous Study

In the research conducted by Muhammad Nur Faiz, Wahyu Adi Prabowo, Muhammad Fajar Sidiq, they only researched forensic methods without implementing them in forensic cases[10], while in the research conducted by Imam Riadi, Herman, Nur Hamida Siregar, only conducted research on one messenger application and only used one forensic method[11], and in research conducted by Imam Riadi, Sunardi, Panggah Widiandana, only conducted research on the WhatsApp application with one method focused on only one forensic case[12],then in further research conducted by Amer Shakir, Muhammad Hammad, Muhammad Kamran focused on researching tool comparisons using several devices without comparing forensic methods[13], and in the latest research conducted by Ikhsan Zuhriyanto, Anton Yudhana, Imam Riadi only researched one messenger application with one forensic method and several forensic tools[14]. Therefore, it could be concluded that the difference between this research and previous research is in the objects, tools, and methods used, namely with WhatsApp and WhatsApp Business objects and 3 forensic tools including MOBIL edit Forensic, Magnet AXOIM, and FTK Imager, and consists of 2 methods including the NIST and DFRWS methods.

2.2 Digital Forensic

Digital forensics is a part of forensic science which includes the discovery and investigation of data found on digital devices such as computers, cell phones, tablets, storage media, and the like[15]. Digital forensics is divided into several sub-branches including computer forensics, mobile forensics, forensics network, database forensics [16]. In digital forensics there are 4 stages to process digital evidence including identification, maintenance, analysis, presentation [17].

2.3 Mobile Forensic

Mobile Forensics is a sub-branch of digital forensics, which in the process of managing digital evidencecomes from mobile devices, cellphones, tablets, and various terms and other similar variants. In principle, mobile forensics has similarities with existing digital forensics, only the point of view is changed from the target of digital evidence which is usually found on desktop computer devices, then transferred to mobile devices.

2.4 Digital Evidence

Digital evidence is evidence in digital form obtained from electronic evidence that has been processed so that it can be used to clarify a case and direct the evidence to other elements or even to criminals. The forms of electronic evidence include logical files, data, audio, web browsers, email addresses, and others [18]. Digital evidence must have the following criteria: valid, original, complete, trustworthy, reliable [19].

2.5 WhatsApp

WhatsApp is an instant messaging service application for smartphones that can run across operating systems such as iOS, Android, BlackBerry, Symbian Series 40 and Windows Phone. WhatsApp uses internet data packages in its use, just like other instant messengers. By using WhatsApp, one can have online chats, share files, exchange photos, video calls, share voice messages and other features that attract users [20]. WhatsApp is able to reach more than 1 million users every day. In addition, more than 70% of the total WhatsApp users are daily active users, and by 2020 it is known that monthly active users have reached 2 billion users.

2.6 WhatsApp Business

WhatsApp released the WhatsApp Business API, to fulfil the needs of business people in communicating with consumers. With the WhatsApp Business API, businesses can send automated notifications, such as payment and delivery information, to consumers directly [21]. According to sensortower.com WhatsApp Business has been downloaded 21 million times on Google Play & App Store in December 2021. [22].

2.7 National Institute of Standards andTechnology (NIST)

NIST is one of the oldest Physical Science Laboratories in the country. Congress created the agency to remove a major challenge to the competitiveness of United States industry at that time [23]. The vision and mission of the agency is to promote innovation and competitiveness of United States industry with advanced science, standards, and measurement technology in ways that enhance economic security and enhance our quality of life [24].

2.8 Digital Forensics ResearchWorkshop (DFRWS)

DFRWS is a non-profit volunteer organization dedicated to bringing together everyone with a legitimate interest in digital forensics. The goal of DFRWS is to cultivate transdisciplinary knowledge that stimulates healthy growth in this fast-growing field [25].

3. METHOD

3.1 Research Scenario

In this research, two scenarios are needed to obtain digital evidence. The researcher made two scenarios, namely the cyberbullying case and the online shop fraud case, where cyberbullying activities were carried out on the WhatsApp application while buying and selling transactions were carried out through the WhatsApp Business application. The purpose of this scenario is to simplify the process of investigating evidence until the final report. This study used an account created as an account of criminals.

a. Cyber bullying case scenario
   The cyber bullying case scenario can be seen in Figure 2.

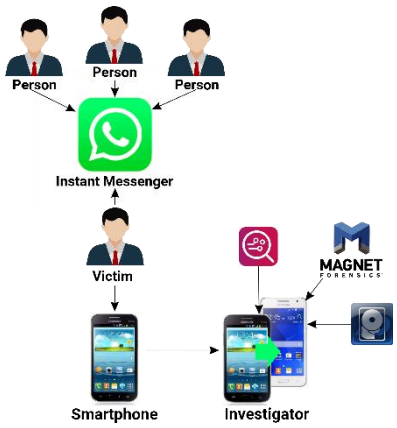

Figure 2. Cyberbullying Case Scenario

Figure 2 four people who are having a conversation through the WhatsApp application.In this scenario, the perpetrator commits a crime in the form of cyberbullying which is carried out in a WhatsApp group chat. The conversation was started by one of the actors who received a report from the teacher who knew about the damage to the glass ceiling based on a report from the security guard, then the perpetrator continued the report to the class group chat. The digital evidence provided by the victim was a smartphone that was focused on being investigated in a group chat. The next step is to determine the tools to retrieve data from the WhatsApp account.

b. Online Shop Fraud Case Scenario
Theonline shop fraud case scenario can be seen in Figure 3.

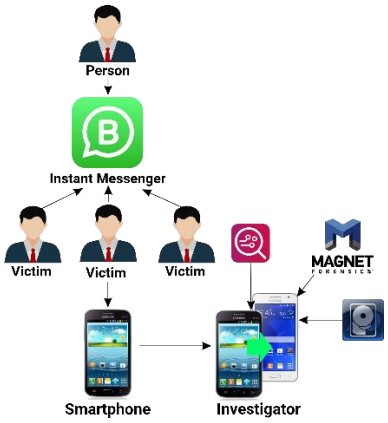

Figure 3. Online Shop Fraud Case Scenario

Figure 3 four people are having a conversation through the WhatsApp Business application. In this scenario, the perpetrator commits a crime in the form of online shop fraud which is carried out on WhatsApp Business group chats. The transaction was initially carried out through the buying and selling community on Facebook social media, but to place an order the transaction was continued through the WhatsApp Business application. The digital evidence provided by the victim was a smartphone that was focused on being investigated in a group chat. The next stage is to determine the tools to retrieve data from the WhatsApp Business account.

3.2 Research Stages

In this study, 2 methods of Mobile forensics are used including NIST and DFRWS. The stages of the NIST method are divided into 4 stages including in Figure 4.

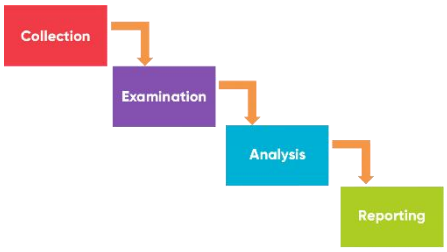

Figure 4. Stages of the National Institute of Standards and Technology

Figure 4 is the stages of NIST method there were Collection, Examination, Analysis, and Reporting. For the DFRWS method, the stages are divided into 6 stages including in Figure 5.

Figure 5.Stages of the Digital Forensics Research Workshop

Figure 5 is the stages of the DFRWS method including Identification, Preservation, Collection, Examination, Analysis, and Presentation. In this research, it is necessary to have this research stages aimed at conducting simulations and as a reference for conducting investigations. The stages of research can be seen in Figure 6.

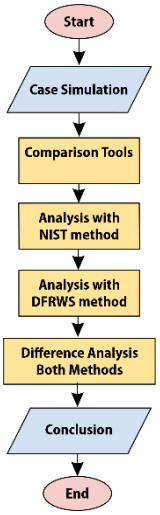

Figure 6. Research Flowchart

Figure 6 is the stages of research that has been carried out in this study, which began with simulating cyberbullying cases through application mediaWhatsApp and cases of online shop fraud through the WhatsApp Business application. Furthermore, a comparison of digital forensic tools is carried out using three tools, namely MOBILedit Forensic, Magnet AXIOM, and FTK Imager in each scenario.After knowing the results of the tools used, an investigation step is carried out with two forensic methods between the National Institute of Standards and Technology and Digital Forensics Research Workshop, then the results of the comparison of the two methods are concluded.

4. RESULT AND DISCUSSION

4.1 Initiation

The researcher was carried out the data using computer equipment and smartphones, in the form of hardware, and some software, includingin Table1.

Table 1. Research Tools and Materials

No	Name	Components	Specifications
1.	Laptop	Processor	IntelCore i7-7700HQ 2.80GHZ
		Memory	8 GB
		SSD	128 GB
2.	Smart phone	Operating System	4.4.2 (KitKat)
		RAM	700MB
		Mode	Root
3.	Soft ware	Operating System	Windows 10 64-bit
		MOBILedit Forensic	7.0.2.16723
		Magnet AXIOM	5.4.0.26185
		AccessData FTK Imager	4.5.0.3

4.2 Research

4.2.1 Simulation Cases of Cyberbullying

The conversation scenario can be seen in Figure 7.

Figure 7. Evidence of Group Chat on WhatsApp

Figure 7 is a conversation between the perpetrators and the victim taken from the victim's smartphone. In the conversation, it was seen that the perpetrator took actions that led to cyberbullying behavior. Perpetrators intentionally used harsh words and insults such as stupid (goblok), stupid (tolol), and so on to victims of.

4.2.2 Simulation Cases of Online Shop Fraud

The conversation scenario can be seen in Figure 8.

Figure 8. Evidence of Group Chat on WhatsApp Business

Figure 8 is a conversation between the perpetrators and victim taken from one of the victim's smartphones. In the conversation, it was seen that the perpetrator and the victim made a sale and purchase transaction, but after the goods were received by the victim, it was found that the goods did not match what was in the product details. Therefore, the victims made a complaint to the perpetrator but the perpetrator only responded once to the complaints of the victims and then disappear.

4.3 WhatsApp Analysis

4.3.1 Comparison of Digital Forensic Tools

The conclusion from the comparison of tools on the WhatsApp application proves that the MOBILedit Forensic Exspress tool is better at extracting than the Magnet AXIOM and FTK Imager tools, the results ofthe comparison can be seen in Table 2.

Table 2. Results of the Comparison of Tools on WhatsApp

Data Evidence	MOBILedit Forensic Express 7.0.2.16723	AXIOM Magnet 5.4.0.26185	AccessData® FTK® Imager 4.5.0.3
Chats Not Deleted	Yes	Yes	Yes
Chats Deleted	No	No	No
Pictures With Download	Yes	Yes	No
Pictures Without Downloading	No	No	No
	$\frac{2}{4} \times 100\% = 50\%$	$\frac{2}{4} \times 100\% = 50\%$	$\frac{1}{4} \times 100\% = 25\%$

Table 2 is the result of a comparison of three tools, namely MOBILedit Forensic, Magnet AXIOM, and FTK Imager, the first column is the evidence data obtained which contains the types of data can be extracted. The second column to the fourth column was a description of whether the application can acquire of each type of data, "Yes" means it can be extracted, while "No" means it cannot be extracted. To obtain data from four parameters, it can be concluded that MOBILedit Forensic can extract 50%, Magnet AXIOM tool 50% and FTK Imager can extract 25%.

4.3.2 Analysis of National Institute of Standards and Technology (NIST)

4.3.2.1 Collection

At this stage, the identification process is carried out in the form of a smartphone that has been rooted, then the evidence is secured from interference by irresponsible parties, as well as making preparations and planning before investigating the evidence. The results of the collection stage can be seen in Figure 9.

Figure 9. Smartphone Victims of the National Institute of Standards and Technology

Figure 9 is the identification stage where the victim's smartphone is in airplane mode and the rooting process has been carried out. Next, back up data on the MOBILedit

Forensic tool, the process of backing up data on the MOBILedit Forensic tool can be seen in Figure 10.

4.3.2.2 Examination

This stages is carried out by the investigator's acquisition process on the evidences. The evidences has been obtained by using the MOBILedit Forensics tool.In this stage, the imaging process and data captured on smartphone memory are carried out.The results of the examination stage can be seen in Figure 10.

Figure 10. Process of Imaging Data in MOBILedit Forensic

Figure 10showed theexaminationform of imaging process which used by MOBILEdit Forensic. At this stages, the smartphone is backed up the data to secure the internal data that have been investigated. Therefore, all of the data are protected from irresonsible parties. The length of the imaging depends on the size ofsmartphone internal data. Before the imaging data process is carried out, some information from the victim's smartphone can be known include the brand and model of device, IMEI number, and the condition of the smartphone that is already rooted.

4.3.2.3 Analysis

The results of the analysis stage can be seen in Figure 11.

Figure 11. WhatsApp Application Information

Figure 11 is information from the WhatsApp application installed on the victim's smartphone in the form of application size and data, application version, and so on. Furthermore, an analysis of the group chat is carried out. The results of the analysis on group chats can be seen in Figure 12.

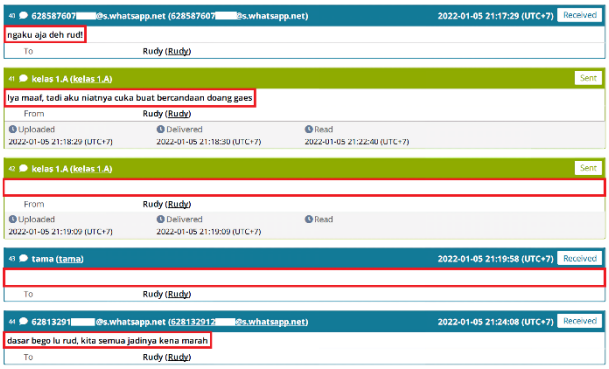

Figure 12. Group Chat Conversations on WhatsApp

Figure 12 is the result of the analysis stage in which there were Group Chat information with analysis results in the form of time sent and received, sender's contact, and deleted chat information either from both the sender and the recipient in an empty field but has not been successfully returned or extracted by the MOBILedit Forensic tool.

4.3.2.4 Reporting

This process is carried out after all the steps above have been completed. Investigators must provide a report as a result. Reporting is done by collecting each result from the analysis and arranged in a coherent manner and can explain clearly.After a simulation based on a cyberbullying case scenario was carried out and an analysis stage was carried out according to the stages of the NIST method with the MOBILedit Forensic tool on the WhatsApp application, it can be concluded that the investigation process was going well enough to be able to raise digital evidence. Based on the results of the investigation of the data that has been analyzed, the original group chats data and the results of the evidence in the form of group chat conversations, but with the inability of the MOBILedit Forensic tool to restore lost data on the WhatsApp application, is the main reason for the lack of the MOBILedit Forensic tool, so it cannot read chat data that has been deleted from both the victim and the perpetrator.

4.3.3 Analysis of Digital Forensics Research Workshop (DFRWS)

4.3.3.1 Identification

The results of the identification stage can be seen in Figure 13.

Figure 13. Smartphone Victim of the Digital Forensics Research Workshop

Figure 13 is the identification stage where the victim's smartphone is in airplane mode and the rooting process has been carried out. Next, prepare the MOBILedit Forensic tool, then prepare tool that have been used, namely MOBILedit Forensic, the initial view of the MOBILedit Forensic tool can be seen in Figure 14.

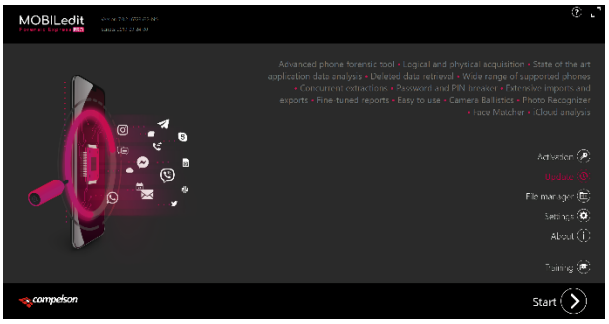

Figure 14. Initial View of MOBILedit Forensic

Figure 14 is the initial view when using the forensic MOBILedit application.

4.3.3.2 Preservation

The results of the preservation stage can be seen in Figure 15.

Figure 15. Process of Creating a Physical Image in MOBILedit Forensic

Figure 15 is the result of the preservation stage, at the preservation stage of the victim's smartphone, a data backup process is carried out which aimed to secure evidence and maintain the authenticity of the evidence, the length of the physical image process itself depends on the size internal memory of the investigated smartphone.

4.3.3.3 Collection

The results of the collection stage can be seen in Figure 16.

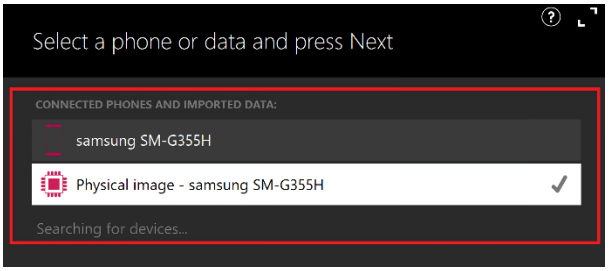

Figure 16. Data Collection Process

Figure 16 is the result of the collection stage in the form of an image file which is still in the form of data from the victim's internal smartphone, later the data have been selected according to the needs to be investigated.

4.3.3.4 Examination

The results of the examination stage can be seen in Figure 17.

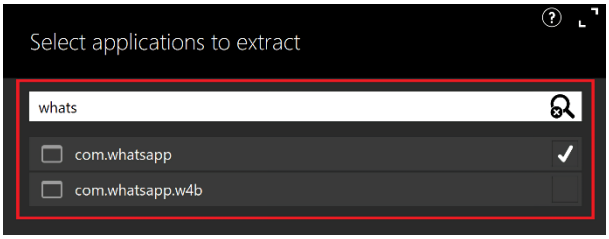

Figure 17. Data Filtering Process

Figure 17 is the result of the examination stage in which there are many choices of data from the victim's internal smartphone, the data is then filtered or selected according to the needs of the investigation, filtering can be done by writing the name of the application in the search box or scroll in alphabetical order, then check the list on the WhatsApp application as shown in the image above.

4.3.3.5 Analysis

The results of the analysis stage can be seen in Figure 18.

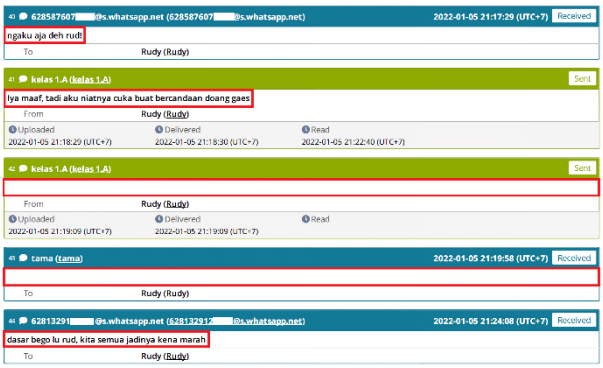

Figure 18. Group Chat Conversations on WhatsApp

Figure 18 is the result of the analysis stage in which there is Group Chat information with analysis results in the form of time sent and received, the sender's contact, and chat information that was deleted from both the sender and recipient in an empty column but was not returned successfully or extracted by the MOBILedit Forensic tool.

4.3.3.6 Presentation

It was concluded that the investigation process was going well enough to be able to raise digital evidence. Based on the results of the investigation of the data that has been analyzed, the original group chats data and the results of the evidence in the form of group chat conversations, but with the inability of the MOBILedit Forensic tool in restoring lost data on the WhatsApp application, is the main reason for the lack of the MOBILedit Forensic tool.Therefore, it cannot read chat data that has been deleted from both the victim and the perpetrator. It is hoped that other researchers can use several different tools from the tools that have been tested in this research, and try to use methods other than the Digital Forensics Research Workshop.

4.4 Comparison ofMethod

Research Methods on WhatsApp Business is carried out exactly according to the steps taken on the WhatsApp application, the results in the comparison of tools on WhatsApp Business can be seen in Table 3.

Table 3. Results of the Comparison of Tools on WhatsApp Business

Data Evidence	MOBILedit Forensic	Magnet AXIOM	FTK Imager
Chats Not Deleted	No	Yes	Yes
Chats Deleted	No	No	No
Pictures With Download	No	Yes	No
Pictures Without Downloading	No	Yes	No
	$\frac{0}{4} \times 100\% = 0\%$	$\frac{2}{4} \times 100\% = 50\%$	$\frac{1}{4} \times 100\% = 25\%$

Table 3is the result of a comparison of three tools, namely MOBILedit Forensic, Magnet AXIOM, and FTK Imager. With the result that MOBILedit Forensic can extract 0% or fail to extract, the Magnet AXIOM tool 50% with extraction results in the form of chats that are not deleted and downloaded images and FTK Imager can extract 25% with the extraction results in the form of chats that are not deleted. The results of the comparison of the National Institute of Standards and Technology method and the Digital Forensics Research Workshop method can be seen in Table 4.

Table 4. Comparison of the Results of the National Institute of Standards and Technology and Digital Forensics Research WorkshopMethods

No	Name	Advantages	Disadvantages
1.	NIST	1. NIST has simpler stages because NIST has 4 stages while DFRWS there are 6 stages. 2. NIST is quite effective in handling cases that are simple to use because the documentation in each stage is not too much. 3. Has a relatively faster time because the documentation of the stages is not so much.	1. NIST method does not document the results of identification, preservation, collection, and examination separately so the mapping will experience difficulties. 2. For complex cases, NIST method is not recommended to be used because the framework still incorporates stages. 3. NIST method is more suitable for conducting investigations that are software because in conducting pre-investigation there is not too much. 4. NIST method does not have stages for filtering evidence such asDFRWS examination stage. 5. NIST method does not explain how to maintain digital evidence, but only tests different digital evidence at the preservation stage inDFRWS method so that the application of chain of custody is so weak in NIST method.
2.	DFRWS	1. The method separates the stages for identification, preservation, collection, and examination separately so that it is easy to map. 2. DFRWS method is very suitable for handling complex cases because the framework is worked out separately in DFRWS stages. 3. DFRWS method is more suitable for conducting hardware investigations because pre-investigation requires a lot of preparation. 4. DFRWS method has stages for filtering evidence at the examination stage, so that it can fulfill Article 43 paragraph (2) which explains to pay attention to the protection of privacy, confidentiality, smoothness, public services and maintain the integration and integrity of evidence. According to DFI (Digital Forensic Investigator) does not disclose confidential information obtained without proper authorization or an order from a competent court.	1. DFRWS method is more numerous than NIST method because the acquisition and authenticity grouping of DFRWS method has 3 stages. 2. DFRWS method is not recommended for handling light or uncomplicated cases because DFRWS method requires many stages and documentation at each stage. 3. Has a relatively long time because of the many stages of documentation.

Table 4showed the advantages and disadvantages of each forensic method in dealing with cases of cyberbullying and online store fraud. From the comparison of the two methods that have been tested, it can be concluded that the National Institute of Standards and Technology method is more inclined to report and handle cases that are not too complex, while theDigital Forensics Research Workshop method is more directed to investigators and for handling more complex cases.

5. CONCLUSION

Basedon the result, it couldbe carried out forensic processes on WhatsApp using forensic tools with a 50% MOBILedit Forensic extraction presentation, 50% Magnet AXIOM, and 25% FTK Imager. Meanwhile, WhatsApp Business can carry out the forensic process with presentations on MOBILedit

Forensic extraction at 0%, Magnet AXIOM at 50%, and FTK Imager at 25%.Research could find out the advantages and disadvantages of forensic methods between the National Institute of Standards and Technology and Digital Forensics Research Workshop methods in handling cases of cyberbullying and online shop blowing, with the National Institute of Standards and Technology method being more inclined to reporting evidence and for handling cases involving not too complex, while the Digital Forensics Research Workshop method is more directed towards handling by investigators and for handling more complex cases.

6. REFERENCES

[1] Azkiya Dihni, V. (2021). Losses Due to Cybercrime Reaches IDR 3.88 Trillion, What are the Forms? Databoks.Katadata.Co.Id.https://databoks.katadata.co.id /datapublish/2021/10/07/loss-of-cyber-crime-achieved-rp-388-trillion-what-is-form (accessed Dec. 19, 2021).

[2] Irawati, A., Fadholi, HB, Alamsyah, AN, & Dwipayana, DP (2021). The Urgency of Cyber Law in the Life of Indonesian Society in the Digital Age. Proceedings of Conference on Law and Social Studies, 0(0).

[3] Social, W. are. (2021). Social Media Users Pass the 4.5 Billion Mark. Wearesocial.Com. https://wearesocial.com/uk/blog/2021/10/social-media-users-pass-the -4-5-billion-mark/ (accessed Dec. 19, 2021).

[4] Cyber, P. (2021). Statistics on the Number of Police Reports Made by the Community. Patrolisiber.Id. https://patrolisiber.id/statistics (accessed Dec. 19, 2021).

[5] Agarwal, A., Gupta, M., & Saurabh, G. (2011). Systematic Digital Forensic Investigation Model. In Saurabh Gupta & Prof. (Dr.) SC Gupta International Journal of Computer Science and Security (IJCSS) (Issue 5).

[6] Riadi, I., Yudhana, A., Caesar Febriansyah Putra, M., & Soepomo, J. (2017). Instagram Messenger Digital Evidence Recovery Analysis Using the National Institute of Standards and Technology (NIST) Method. In the National Seminar on Information and Communication Technology-SEMANTIKOM.

[7] Suryana, AL, Akbar, R. El, & Widiyasono, N. (2016). Email Spoofing Investigation Using Digital Forensics Research Workshop (DFRWS) Method. Journal of Informatics Education and Research (JEPIN), 2(2).

[8] Dwi Rahayu, Y. (2014). Building an Integrated Digital Forensics Investigation Framework (IDFIF) Using the Sequential Logic Method. National Seminar on Information and Communication Technology 2014 (SENTIKA2014).

[9] Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models. International Journal of Computer Science and Information Technology, 3(3), 17–31.

[10] Nur Faiz, M., Adi Prabowo, W., & Fajar Sidiq, M. (2018). Journal of Informatics, Information Systems, Software Engineering and Applications Comparative Studies of Digital Forensics Investigations on Crime. Institute for Community Service (LPPM) Telkom Institute of Technology Purwokerto, 1(1), 63–70.

[11] Riadi, I., & Hamida Siregar, N. (2021). Mobile Forensics in Cyber Fraud Cases Signal Messenger Service Using the NIST Method. JOINTECS (Journal of Information Technology and Computer Science), 6(3), 137–144.

[12] Riadi, I., Sunardi, & Widiandana, P. (2020). Investigating Cyberbullying on WhatsApp Using Digital Forensics Research Workshop. RESTI Journal (Systems Engineering and Information Technology), 4(4), 730–735.

[13] Shakir, A., Hammad, M., & Kamran, M. (2021). Comparative Analysis & Study of Android/iOS Mobile Forensics Tools. Digitala Vetenskapliga Arkivet.

[14] Zuhriyanto, I., Yudhana, A., & Riadi, I. (2020). Comparative Analysis of Forensic Tools on Twitter Applications Using the Digital Forensics Research Workshop Method. RESTI Journal (Systems Engineering and Information Technology), 1(3), 829–836.

[15] Raharjo, B. (2013). Overview of Digital Forensics. Journal of Sociotechnology, 12(29), 384–387, Aug. 2013, doi: 10.5614/SOSTEK.ITBJ.2013.12.29.3.

[16] Technology, B. (2020). Digital Forensics. Bagitechnology.Com.https://www.bagitechnology.com/ 2020/04/digital-forensic.html (accessed Dec. 19, 2021).

[17] Carrier, BD (2006). Digital Investigation and Digital Forensic Basics. Digital-Evidence.Org.https://digital-evidence.org/di_basics.html (accessed Dec. 19, 2021).

[18] Ma'ruf, F. (2014). Definition and Explanation of Digital Evidence. Academia.Edu, 1–11.

[19] Wulandari, WA (2015). Paper Forensics About the Characteristics of Digital Evidence. Academia.Edu, 14917163.

[20] Anwar, N., & Riadi, I. (2017). WhatsApp Messenger Smartphone Forensic Investigation Analysis Against Web-Based WhatsApp. Scientific Journal of Computer Electrical Engineering and Informatics, 3(1), 1.

[21] Qiscus. (2020). Get to know the History of WhatsApp Business API. Qiscus.Com https://www.qiscus.com/id/blog/menenal-sejarah-whatsapp-api/ (accessed Dec. 19, 2021).

[22] Sensor Tower. (2022). Sensor Tower - Mobile App Store MarketingIntelligence.Sensortower.Com/.https://sensortower.com/ (accessed Jan. 03, 2022).

[23] NIST. (2017). About NIST | NIST. Nist.Gov.https://www.nist.gov/about-nist (accessed Jan. 03, 2022).

[24] NIST. (2021). NIST Mission, Vision, Core Competencies, and Core Values | NIST. Nist.Gov.https://www.nist.gov/about-nist/our organization/mission-vision-values (accessed Jan. 03, 2022).

[25] DFRWS. (2021). About Us - DFRWS. Dfrws.Org.https://dfrws.org/about-us/ (accessed Dec. 19, 2021).