Mobile Forensic WhatsApp Services in Online Fraud Cases using Digital Forensic Research Workshop Methods

Dicky Setiawan
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
The study uses the Digital Forensic Research Workshop (DFRWS) method to apply, practice, and implement the WhatsApp application in mobile-based online fraud cases, with a record so that the perpetrators can not do the deletion as well as search for digital evidence to be used as evidence and find suspicious files that have been deleted in the form of image files. The aim of this research is to apply the Digital Forensic Research Workshop (DFRWS) methods to uncover online fraud cases and conduct a digital evidence search process. The methodology in this study uses an approach that is able to be researched and designed and formed to help a process of resolution in Digital Forensic. The results of this research use new test data using the Method of Digital Forench Research Workshop which has several stages including Identifying, Maintaining, Collecting, Examine, Analysing, and presentation. Proof obtained from the process of Mobile Forensic WhatsApp Services on Online Fraud Cases using 3 tools in this case MOBILedit forensic express, Magnet Axiom and Hash My Files, but only tools MOBILed forensics express that have a degree of accuracy in the data collection process of 67 images but the deleted image data is a total of 3 images file (image) image consisting of messages or chats asking for money, giving a bonus or a prize, and a free voucher.

General Terms
Digital Forensics

Keywords
Digital Forensics, WhatsApp, Digital Forensic Research Workshop (DFRWS), Online Fraud, MOBILedit Forensic Express.

1. INTRODUCTION
WhatsApp Messenger application uses mobile data connection as well WiFi For carry out data communications, with using WhatsApp, someone can do online chat , file sharing , exchange photos and features other interesting things its users [1]. WhatsApp is one application Instant messaging created by Facebook and is one of the popular social media applications [2]. DFRWS is a framework with standard forensic framework as well as consistent so easy used user and easy understood user Good technical and non- technical [3]. The DFRWS method helps in get goods evidence and mechanisms centralized For record information collected [4]. Digital forensics simple is the whole process of fetching, restoring, saving, checking information or document electronic, based methods and tools that can accountable in a way scientific for objective proof [5]. Digital forensics are used as investigation to devices that can storing digital data [6]. Based on the Digital Forensic Research Workshop (DFRWS) Method, there are several stages that must be carried out (Palmer, 2001) [7]. DFRWS is framework Work strong scientific for the investigation process forensics that have a number step among them namely Identification, Preservation, Collection, Examination, Analysis and Presentation. The DFRWS method helps obtain evidence and mechanisms centralized for take notes information [8]. The Digital Forensics Research Workshop (DFRWS) method is one of the methods used in digital forensic analysis to indicate a digital crime [9]. The measurement parameters are adjusted to case simulations, namely potential evidence related to cyber espionage, namely user identification, multimedia messages, text messages, timestamps, and applications [10].

WhatsApp is a free chat application that allows users to exchange text messages, photos, videos, documents and can share the latest locations available on the Android and iOS versions which was built by Brian Acton and Jan Koum [11]. But the development of the WhatsApp app was exploited by some people in committing criminal acts. One of the crimes that often occurs is online fraud [12]. Online fraud is in principle the same as conventional fraud, the only difference is in the means of action, namely using electronic systems (computers, internet, telecommunications equipment) [13]. Moment This is fraud online tend focuses on the slogans of cash advance fraud, lottery, prizes fake, online auctions, up to romance online dating [14]. MOBILedit Forensic Express Pro, Autopsy, etc [15]. Digital evidence is evidence that cannot be seen physically which is found in electronic evidence, such as user accounts, contact persons, text messages, document files, media files (audio/video images) and many more [16]. Goods the best digital evidence into 15 types, namely logical files, deleted files, encrypted audio files, video files, image files, emails, user id/password, etc. [17].

2. RELATED WORKS
Anton Yudhana, Priest of Riadi, Riski Yudhi Prasongko (2022) on “WhatsApp Forensics Using Digital Forensic Research Workshop (DFRWS)”, this research was carried out using digital forensic methods developed by the Digital forensics Investigation Workshop (DFRWS). This method provides evidence mechanisms for recording all forms of information. In this study, the digital evidence sought is a case of cybercrime with WhatsApp application that can be obtained and detected using the DFRWS method with the help of tools MOBILedit Forensic Express and Hash My Files [18].

Imam Wahyudi, Arif Muntasa, Muhammad Yusuf, Ardi Hamzah (2021) on “Developing and Testing the Authenticity of Digital Evidence on Cybercrime and Digital Forensic Research Workshop”, in this study describes an application that uses a live forensic method developed by the Digital forensics Research Workshop (DFRWS), which helps obtain evidence and a centralized mechanism to record the information collected. DFRWS also uses the FTK Imager to analyze the

data. Forensic digital analysis is so extensive that it can be grouped according to the logical and physical forms. Evidence is analyzed using various types of forensic computers, such as forensics cars, audio forenses, video forensices, forensical imagery, and cyberforensics. For this research, forensic imaging will relate to digital evidence, i.e. digital photo files [19].

Ilham Algi Plianda, Rini Indrayani (2022), on "Analysis and Comparison of the Performance of Digital Forensic Tools on Android Smartphones using Instant Messaging Whatsapp", is a study that discusses a study where doing one in dealing with cases of cybercrime, forensic investigation requires the best effort in every stage. The goal is to get as much digital evidence as possible to consider the case's conclusions. Therefore, any choice of tools and methods that might be most effective should be considered. With this in mind, two forensic process tools, MOBILedit and Oxygen Forensic [20].

Rusydi Umar, Anton Yudhana, and Muhammad Noor Fadillah (2022), on "The Comparison of Forensic Tools on Digital Wallet Applications", made a method used in this study is the Digital Forensics Research Workshop (DFRWS), where this scientific method is used in digital forensics and has proven useful for obtaining digital evidence. The forensic results of the two forensical tools Autopsy and Belkasoft Evidence Center, which uses the method of Digital Forenzic Research Workshop, showed that digital evidence related to information on transaction activity carried out on four digital wallet applications was found.

Fitri Anggraini, Herman, Anton Yudhana (2022), on "Forensic Analysis of TikTok Applications on Android Smartphones Using Framework Association of Chief Police Officers" on the discussion in this study aims to be able to help in the process of MOBILedit Forensic Express used to restore data on Samsung Galaxy A8 smartphone. In this study, digital evidence such as deleted name pollution, such as hashtags from posted videos, and text messages, was returned and uploaded to the TikTok app, which was then removed from the Android smartphone. The TikTok application is installed on the Samsung Galaxy Tab A SM-P355 smartphone, and the forensic process uses the ACPO framework and Axiom Magnet tools [22].

3. METHODOLOGY

The methodology in this research uses an approach that can be researched and designed and formed to help a solution process in Digital Forensic, in solving a problem on forensic investigation.

3.1 Research Objects

The object of the research to be discussed in this study is to refer to a digital forensic on a message file where the image data of the sender of the message is obtained in a mobile phone.

3.2 Research Materials and Tools

In the process of conducting this research, using the hardware and software that serves as support in the research process, a detailed and complete description table will be drawn up so that it can be used as a reference and guide, as detailed in Table 1 and Table 2.

Table 1. Materials and Hardware Tools Used in This Research

Device Hard	Specification
LAPTOP	VivoBook_ASUS Laptop X412FLC_A412FL Intel(R) Core (TM) i5-10210U CPU @ 1.60Hz (8 CPUs), ~2.1GHz, Memory 8192MB RAM
Mobile Phone / Smartphone	Redmi 4A (Xioami Redmi 4A)

Table 2. Materials and Software Tools Used in This Research

Device Soft	Specification
MOBIledit Forensic Express	MOBILedit Forensic Express PRO Version: 7.4.0.20393 (64-bit)
Axiom Magnets	Magnet Axiom Version 5.4.026185
System Operation	Windows 11
WhatsApp Mobile	*WhatsApp Mobile Version 2.23. 13.76*
Hash My Files	HashMyFiles v2.44 Version 2.44

3.3 Research Phase

The stages of the Digital Forensic Research Workshop (DFRWS) method are implemented using a demonstrated method.

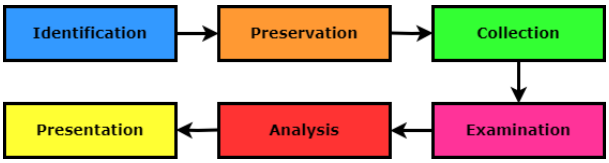


Figure 1: Scheme of the Digital Forensic Research Workshop Method

Figure 1. provides a general overview of the DFRWS Method consisting of the first phase of Identification, Maintenance, Collection, Examination, Analysis, and Presentation as the final phase, so it can be presented as follows:

3.3.1 Identification

At this stage, the process of identifying any needs that need to be prepared in conducting investigations and searching for digital evidence [23] is carried out.

3.3.2 Preservation

At this stage, a maintenance process is carried out to preserve the evidence that has been obtained and to ensure the authenticity or integrity of the evidence in order to avoid unwilling parties, so that the evidence is non-contaminated and truly valid [23].

3.3.3 Collection

At this stage, the collection process is carried out and the process of collecting and identifying the parts required to perform identification from data sources based on digital evidence [24].

3.3.4 Examination

This phase determines the filtering on one of the parts that originate from the data source, but still preserves the

authenticity of the content of the data due to the nature of the authoritative data is very important therefore the data filtering is carried out only from the side of the change of shape on the data whileining the autenticity of data [24].

3.3.5 Analysis

This stage is the process of determining where the data is made from, where it comes from, how it is made, and why the data was made [25].

3.3.6 Presentation

The presentation phase is performed to display the information obtained from the previous phase of analysis, then the submission of the data resulting from the analysis, including the reporting of the actions carried out, so that it can be understood by the public [25].

3.4 Case Scenario

In the process of research there is a scenario or simulation in the case of online fraud, which is an online investigation process in which a perpetrator of a crime on a mobile application in this case is WhastApp Mobile by sending a message file (messages) containing image data.

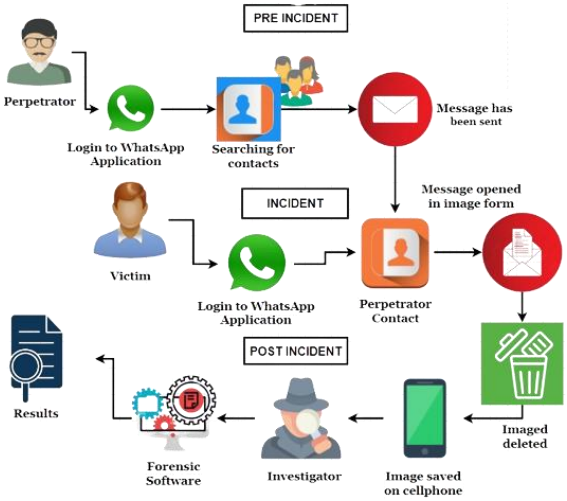


Figure 2: Case Scenario

Figure 2. shows a picture of the scenario or simulation that has been displayed and described in the evaluation above then draw a simulation illustration there are 3 stages in the illustration of the simulation case made in this case consists of Pre-incident, Incident, and Post-incidence, and post-incidents, as follows:

3.4.1 Pre-Incident

The case scenario begins with an offender who wants to commit bad intentions or negative intentions where he finds a victim's contact randomly on the WhatsApp mobile app and then sends a message to the victim with the aim of making a fraud victim so that it can harm the victims both materially and financially, and also has a purpose on the offender's side where he will get a profit from what he gets from victims either money, or other things.

3.4.2 Incident

At the time of the online fraud message has been sent by the perpetrator, the victim entered the WhatsApp mobile application and saw the performer's contact where it was sent a message of a dangerous nature or in a negative sense that the message is in the form of a conversation and then sent a picture of the fraud online, which consists of 3 different messages but the perjury has done a deletion of the message in the shape of the image so that there are no traces of online form of fraud but the data of the messages that have been sent previously has been stored in a mobile phone in the WhatsApp application.

3.4.3 Post-Incident

After that digital evidence in the form of messages that have been previously deleted has been automatically in the cell phone, then the victim reports the online fraud case to the responsible party which will then be carried out a process and data processing and analyzed by experts in such a case is the investigators, after which the forensic process will run using a Forensic Software aimed at helping and obtaining the data that has been removed earlier, and finally the data results have been obtained in form of 3 images.

3.5 Research Process Flow

Research process flow is stages in the investigation process Frequent digital forensics known with forensic imaging. This stage is an initial stage in the data identification process where the data is identified in order to obtain several data consisting of 3 types of online fraud, consisting of asking for money, giving bonuses, and free vouchers from someone, this stage is a data processing process which functions to obtain complete data from files in the form of messages or chats that have been sent by the perpetrator, as well as other supporting data, namely smartphones/cellphones. Then after the data has been collected, it is continued to the data examination. Therefore, the process and how the MOBILedit Forensic Express and Magnet Axiom tools work will be explained. In the data maintenance stage here is a form of process of checking the completeness of the data which will later be collected into one data unit, with the intention that the data can be processed for data collection using the MOBILedit Forensic Express application. Based on the research process then on stage This data collection then make it Illustration Acquisition.

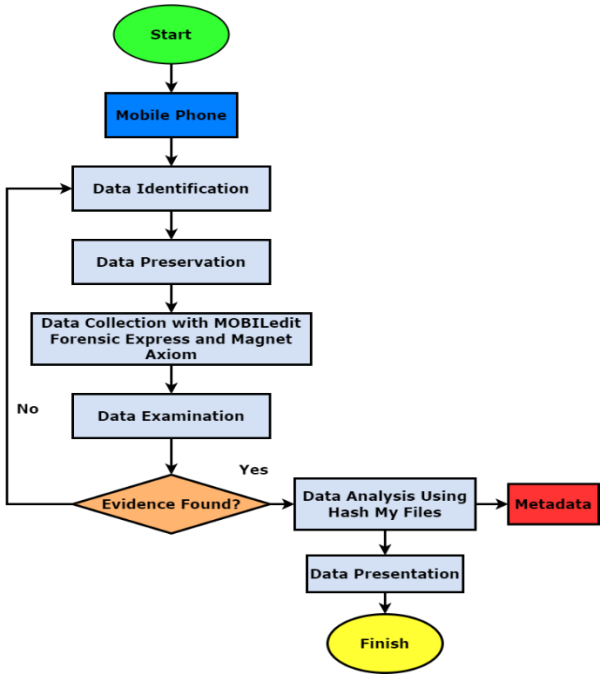


Figure 3: Research Process Flow

Figure 3. provides description general from the flow of the research process that begins with start after That will enter the mobile phone then will next to data identification, data maintenance, data collection with MOBILedit Forensic Express and Magnet Axiom, data inspection, data analysis

using Hash My Files, data presentation, and finally with finished.

4. RESULTS AND DISCUSSION

This research uses method scientific with base for maintenance, collection, validation, identification, analysis, interpretation, documentation, and presentation originating digital evidence from digital sources, with A analysis digital forensics ie use method *Digital Forensics Research Workshop* (DFRWS).

4.1 Data Collection Results

In study This is the data collected and obtained with use questionnaire has spread to respondents who have experience or knowledge related with case online fraud that uses WhatsApp service around 107 respondents' data. Incoming data the many excel in type online fraud, namely Banks, Lottery / Prizes, Vacancies Jobs, as well Still There is a number of others too, but that has been recorded and created material for researched there are 3 namely method ask for money, give bonuses/ gifts, and vouchers for free.

4.2 Implementation

DFRWS method is abbreviation from *Digital Forensics Research Workshop*, which has function in give proof mechanism for record all required information. Based on rule digital forensics and safeguarding integrity authenticity digital evidence, forensic processes follow procedure method forensics *Digital Forensics Research Workshop* (DFRWS) which has a number of Forensic stages include: *Identification, Preservation, Collection, Examination, Analysis,* and *Presentation,* as following:

4.2.1 Identification

Stage This is A stage beginning in carry out the process of identifying the data where the data is succeed identified with obtained some data in form *image* (image) *online* fraud. The cellphone used in identify all data from 3 types of fraud data *online* ie using a Redmi 4A cellphone (Xioami Redmi 4A).

Figure 4: Redmi 4A smartphone (Xioami Redmi 4A)

Figure 4. shows a detailed diagram of the Redmi 4A cellphone specification. The Redmi 4A cellphone, or Xiaomi Redmi 4A, has system important specifications for forensic processing Because used as goods proof. Therefore That will Explained specification from the Redmi 4A cellphone (Xioami Redmi 4A) so can seen in Table 3.

Table 3. Specifications of Mobile Phone

No	Specification Type 1 Brand	Evidence Specifications
1	Device Name	Xiaomi
2	Series	Redmi 4A
3	IMEI	865592037675329
4	System Operation	Android
5	Version System Operation	7.1.2 N2G47H

4.2.2 Preservation

In stages data preservation here is A form of checking process completeness of the data later will collected become One data unity, with the purpose of that data Can The data collection process was carried out using use *tools* MOBILedit Forensic Express.

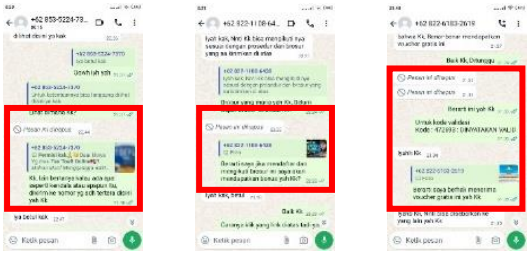


Figure 5: Screenshot Results of 3 Types of Messages from the Perpetrator

Figure 5. shows screenshot from appearance results picture chat or messages asking for money, offering bonuses or prizes, and also free vouchers from someone, who is one case online fraud Once rooting is complete, the approval process access via the Options menu Developers are very important. With access this menu, user can access various options that don't available by default in normal cellphone settings, such as enable USB debugging, control application background processes, and setup arrangement more network advanced.

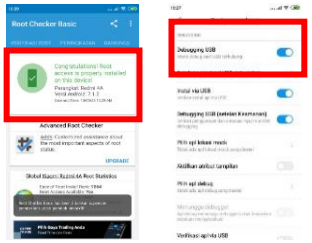


Figure 6: Root Checker Results and Developer Options

Figure 6. shows the rooting process finished carried out and also the activation process Option Developer as well as USB Debuggin Menu settings, Install via USB, and USB Debugging (settings security).

4.2.3 Collection

At stage This is A stage important in digital forensics, where the data has been identified and implemented maintenance will collected and processed in the application MOBILedit Forensic Express. Stage This is a data processing process with use application MOBILedit Forensic Express and Magnet Axiom with order collection, search, and processing of data.

4.2.3.1 MOBILedit Forensic Express

Based on matter the so will is displayed a process of using MOBILedit Forensic Express tools in the collection process search, and data processing.

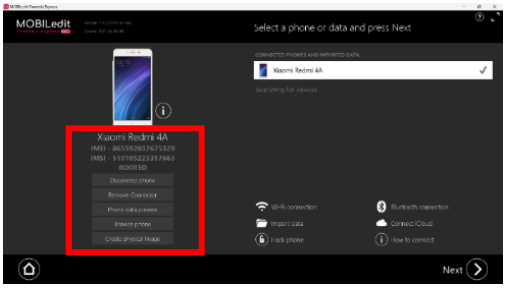


Figure 7: Display of the mobile phone connected to the MOBILedit Forensic Express application

Figure 7. shows appearance beginning moment user open application MOBILedit Forensic Express. Display, and also an appearance the process of connecting a cellphone, especially the Redmi 4A cellphone (Xiaomi Redmi 4A). In step this, user connect device mobile and running computer application forensics in a way physique or wireless.

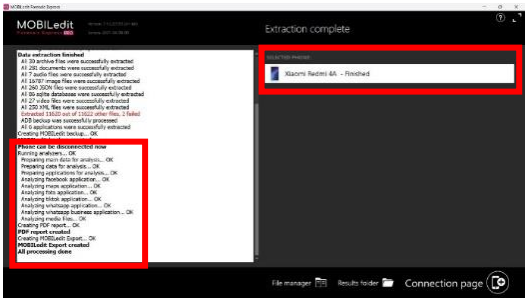


Figure 8: Extraction Complete display

Figure 8. illustrates about data export process starts. User requested for wait while the export process taking place or choose option for connected with more Lots device on the display “Wait or press for connected more Lots ".

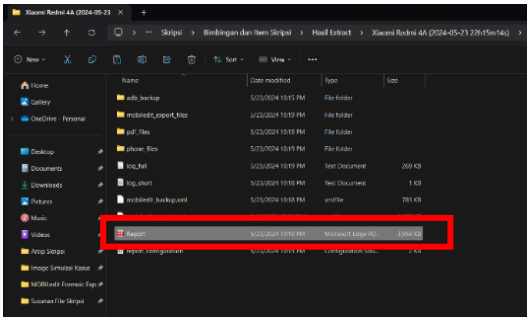


Figure 9: Storage Layout Display

Figure 9. is place its storage is in folder E:/ Xiaomi Redmi 4A Extract Results on April 25 2020 at 12:10 Export produces a PDF file with report forensics. Application MOBILedit Forensic Express, a ordinary tools used For analyze device data mobile, used For produce report This. in PDF format and image data files. Information about request for money, bonus or gifts, and free vouchers.

4.2.3.2 Axiom Magnets

Based on matter the so will is displayed a process of using Magnet Axiom tools in the collection process search, and data processing.

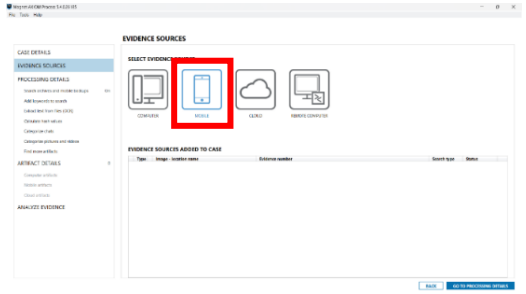


Figure 10: Evidence display by selecting Mobile in Magnet Axiom

Figure 10. shows the process of connecting a cellphone with the Magnet Axiom tool in the *"Evidence Sources" menu display*, followed by selecting the *"Mobile" option*. At this stage, the user begins the process to direct to stage furthermore.

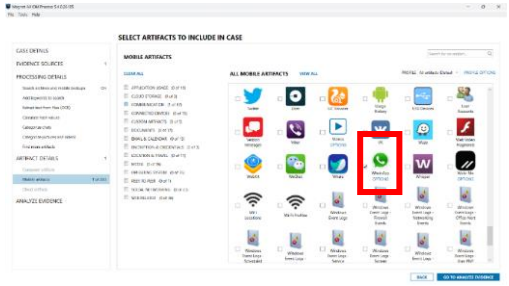


Figure 11: Display of data extraction selection

Figure 11. displays the *"Select Artifacts to Include in Case" display* which has various type applications For An internal data extraction process was carried out matter This is WhatsApp *Mobile* application.

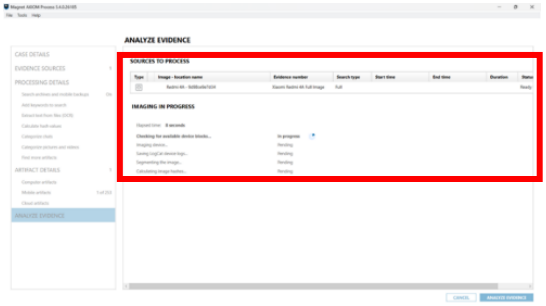


Figure 12: Display of the extraction process on a mobile phone

Figure 12. shows the extraction process from election application on in matter it's WhatsApp, then will directed to appearance furthermore that is *Analyze Evidence.*

4.2.4 Examination

Stage this is a process of examining the data obtained from stages previously Where obtained form results *(image)* picture that has been sent by the perpetrator.

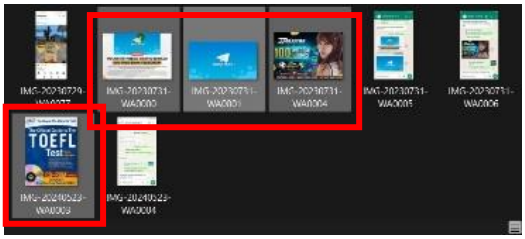


Figure 13: Display of deleted image files

Figure 13. shows stage end Where will Found image file (image) from case online fraud consisting from ask for money, give bonuses / gifts, and free vouchers from someone, where is the storage folder is located in the \Sent folder, so the image file has been deleted succeed obtained.

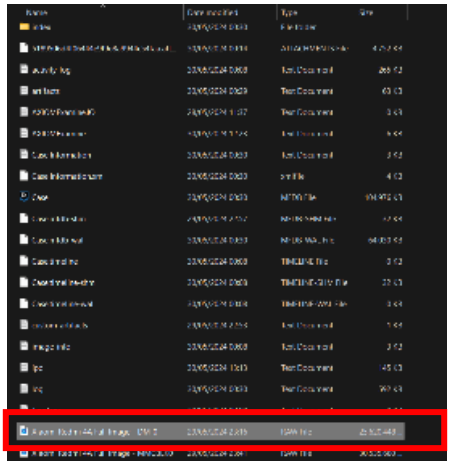


Figure 14: Display of the results from the Magnet Axiom extraction tools

Figure 14. shows A data check with using Magnet Axiom tools, where the process of collecting, searching and processing data has been carried out done, but the image data files (images) from case online fraud is not obtained some folders, so results extraction from the Magnet Axiom tools have displayed.

4.2.5 Analysis

In stages this, that is A form of data analysis process that has been done collection, and processing with use application MOBILedit Forensic Express and previous data examination processes has succeed do and get appropriate and valid results. Based on from matter the so data analysis will done with use Hash My Files application, where application This aim for show MD5, and SHA-256 codes of the files that have been processed Previously, the analysis process done with insert file *(image)* picture to Hash My files application with clicking on file then select Add Files, next select file *(image)* picture the.

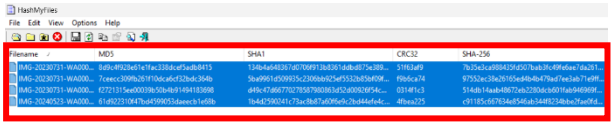


Figure 15: Display of Hash My Files Results

Figure 15. shows all over information MD5 and SHA-256 codes as well codes other from image files *(image)* message from third case fraud *on line* Where has entered.

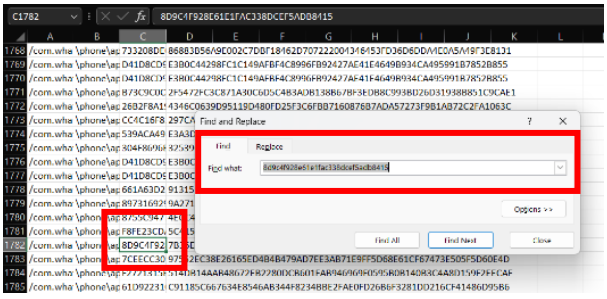


Figure 16: Display of the Results of Matching MD5 and SHA-256 Codes

Figure 16. loading MD5 and SHA-256 codes from data files *(image)* picture fraud *online*, which has obtained so will analysis process is carried out furthermore Where match MD5 and SHA-256 codes are the results obtained use Hash My Files application with excel folder from *extraction* use MOBILedit Forensic Express where the name of the folder that is file_hashes_backup, p the done with copies MD5 and SHA-256.

4.2.6 Presentation

This phase is a final phase in which all the results of the data that has been done are both data identification, data maintenance, data collection using MOBILedit Forensic Express and Magnet Axiom, data inspection, data analysis using Hash My files, and last is the final presentation result. Based on this, a comparison table of the data collection process will be drawn first using two different tools in this case: MOBILedit Forensic Express and Magnet Axiom, so that it can be seen on a Table 4.

Table 4. Results of the Comparison of Data Collection Tools

No	Digital Evidence	WhatsApp	
		MOBILedit Forensic Express	Axiom Magnets
1	Conversation / Chat	95	95
2	Image/Image	67	-
3	Videos	-	-
Amount		162	95

Based on table comparison on so can outlined results from invention goods digital evidence through a collection process *(Collection)* data with use two different *tools* in matter is MOBILedit Forensic Express and Magnet Axiom. Therefore That so Can make it A percentage data collection for 2 *tools* in matter This MOBILedit Forensic Express and Magnet Axiom in form *"pie charts"*.

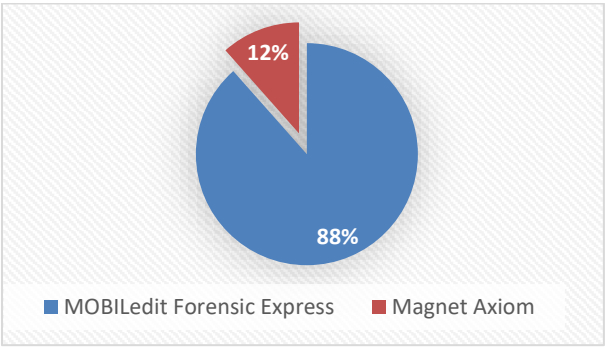


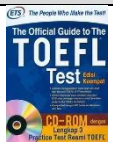
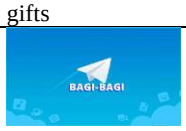
Figure 17: Percentage of Comparison Results of Data Collection Tools

Figure 17. shows about presentation from results comparison second *tools* collection *(Collection)* data is very significant Where *tools* MOBILedit Forensic has amount highest percentage with total 88% in carry out the collection process *(Collection)* data is good form message conversations, images, videos, contacts, files and so on. Whereas different with Axiom Magnet *tools* only own amount very small percentage with amount only 12 % in the collection process *(Collection)* data.

Comparison of data collection tools from MOBILedit Forensic Express and Magnet Axiom was made, then data such as Message/Text, Images, and Video were sometimes found but there were also not found. The data focused to be displayed in the final presentation is data Images where from the results of comparison data collection tools obtained files Images of 67 images, of some of these images there are 3 pictures of online

fraud cases used as final presentation material, in this case images asking for money, giving a bonus / gift, as well as a free voucher from someone. Based on the interpretation of the comparison results of the tools that have been displayed previously then this final presentation results are described as the completion stage or completion of the whole of all the stages described previously, where the result of the 3 data about online cheating i.e. money request messages, giving bonuses, and free vouchers with MD5 and SHA-256, so can be seen in Table 5.

Table 5. Final Presentation Results

No	Data Results	MD5 code	SHA-256 code
1	 *(image)* image : Orderor Chatan Ask for money	61d922310f47bd4599053daeecb1e68b	c91185c6676348546ab344f824bbe2fae0fd266f3281dd216cf41486d95b6
2	 *(image)* image : Giving bonuses/ gifts	f2721315ee00039b50b4b91494183698	514db14aab48672eb2280dcb601fab946969f0595b0b140b3c4a8d159f2eecaf
3	 *(image)* Gambar : Voucher Gratis  *(image)* Gambar : Voucher Gratis	7ceecc309fb261f10dca6cf32bdc364b 8d9c4f928e61e1fac338dcef5adb8415	97552ec38e26165ed4b4b479ad7ee3ab71e9ff5d68e61cf67473e505f5d60e4d 7b35e3ca988435fd507bab3fc49fe6ae7da261d6258bff8475c0e6c8aebe34e3

5. CONCLUSION

This research uses new test data using the Digital Forensic Research Workshop Method which has several stages including Identification, Maintenance, Collection, Examination, Analysis and Presentation. The test results using this method provide significant accuracy results and produce valid and correct data as well as appropriate and correct image file (image) similarities. Evidence obtained from the WhatsApp Service Mobile Forensic process in Cases Online Fraud with using 3 *tools* in matter This MOBILedit Forensic Express, Magnet Axiom and Hash My Files, however only MOBILedit Forensic Express *tools* only have it level accuracy in the data collection process there were 67 images will but the image data is deleted totaling 3 pictures in the form of a file (image) consisting of images from Message or Chatan Asking for Money, Giving Bonuses/ Gifts , and Free Vouchers. Evidence found on the device through a forensic process own similarity MD5 and SHA-256 codes of image files with file_hashes_backup which goes through the extraction process.

6. REFERENCES

[1] V. Arista Yuliani and I. Riadi, "Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standards and Technology (NIST) Framework," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 3, p. 223–231, 2019, doi: 10.17781/P002615.

[2] Safrizal, S., Gustina, D., Aisyah, N., Putra, A., Valentino, V., & Prasetyo, B. (2022). Analysis of Tapping on the WhatsApp Application Using Data Synchronization. *Infocom Essence Journal: Journal of the Essence of Information Systems and Computer Systems*, *6* (1), 28-34. https://doi.org/10.55886/infokom.v6i1.453

[3] M. Wibowo, MR Firmansyah, and RS Efendi, "Analysis of Digital Evidence in the Discord Desktop Application Using the Dfrws Framework," 2024, [Online]. Available at: http://ejurnal.provisi.ac.id/index.php/JTIKP page98

[4] A. Yudhana, I. Riadi, I. Zuhriyanto, and A. Dahlan, "Live Forensics Analysis of Social Media Applications in Browsers Using the Digital Forensics Research Workshop (DFRWS) Method," vol. 20, no. 2, p. 125–130, 2019.

[5] AN Ichsan and I. Riadi, "Mobile Forensics on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method," *Int J Comput Appl* , vol. 174, no. 18, p. 34–40, Feb 2021, doi: 10.5120/ijca2021921076.

[6] M. I. Ramadhan and I. Riadi, "Forensic WhatsApp based Android using National Institute of Standard Technology (NIST) Method," *International Journal of Computer Applications*, vol. 177, no. 8, hlm. 8887, Okt. 2019, doi: 10.5120/ijca2019919443.

[7] MN Fadillah, R. Umar, A. Yudhana, A. Dahlan, Y. Jalan, and SH Soepomo, "Forensic Analysis of Digital Wallet Applications on Android Smartphones Using the Dfrws Method , " *Journal Knowledge Computers* , vol.9, no. 2, 2022, doi : http://dx.doi.org/10.20527/klik.v9i2.327

[8] Sunardi, Riadi Imam, Umar Rusydi, and Gustafi4y Muhammad Fauzan, "Audio Forensics on Smartphones with Digital Forensic Research Workshop (DFRWS)" method 6739-Article Text-39474-1-10-20210527," p. 41-47, March 2021, doi:10.21512/commit.v15i1.6739.

[9] AG Prayogo , UA Dahlan, and I. Riadi , "Digital Forensic Signal Instant Messages Services in Case of Cyberbullying using Digital Forensic Research Workshop Method," *International Journal of Computer Applications* , vol. 184, no. 32, p . 8887, Oct 2022, doi: 10.5120/ijca2022922393.

[10] J. Triyanto and I. Riadi, "Analysis of Cyber Espionage Investigations on Facebook Using the Digital Forensics Research Workshop (DFRWS)," vol. 23, no. 1, p. 39–46, 2022, doi: 10.30595/techno.v23i1.9064

[11] R. Adijisman, UA Dahlan, and I. Riadi, "Mobile Forensics on WhatsAppServices using National Institute of Standards and Technology Method," *International Journal of Computer Applications*, vol. 183, no. 29, Oct 2021, doi: 10.5120/ijca2021921680 .

[12] Putra Ikhwan Wiratama, Suharso Aries, and Rozikin Chaerur, "Digital Evidence Acquisition and Image Authenticity Detection on WhatsApp Using the NIST and ELA 370-747-1-SM Methods," vol. 5, p. 1–15, Sep 2021, doi : http://dx.doi.org/10.30645/j-sakti.v5i2.370.

[13] S. Sunardi, A. Fadlil, and NMP Kusuma, "Implementation of Data Mining with the Naïve Bayes Algorithm for Profiling Online Fraud Victims in Indonesia,"

Budidarma Media Informatics Journal, vol. 6, no. 3, p. 1562, July 2022, doi: 10.30865/mib.v6i3.3999.

[14] Wahyuddin, Lutfiah Firdausiah Ersa, Gusti Aningsih, Taufik Hidayat, & Alem Febri Sonni. (2024). Analysis of Online Fraud Communication Networks Through Social Media Whatsapp Messenger. *Journal of Communication Netnography*, 2(2), 73–90. doi: https://doi.org/10.59408/Jnk.V2i2.27.

[15] I. Faisal, A. Budiman, and EI Fitiria, "Application of Digital Forensics Research Workshop in the Acquisition of Forensic Evidence for Snack Video Applications , " Vol. 2 No. 2 (2023) , September 2023 doi : https://doi.org/10.62712/juktisi.v2i2.108 .

[16] M. Rizki Setyawan and M. Fadli Hasa, "Digital Forensic Analysis on Skype Based on Windows 10 Using the Acpo Framework," *Journal Scientific Betrik* , vol. 13, no. 02, p. 111-119, Aug 2022, doi : https://doi.org/10.36050/betrik.v13i2.469 .

[17] D. A. Putri and I. Riadi, "Forensic Mobile against Threat WhatsApp Services using National Institute of Standards Technology Method," *International Journal of Computer Applications*, vol. 183, no. 32, Okt 2021, doi : 10.5120/ijca2021921681.

[18] Yudhana Anton, Riadi Imam, dan Prasongko Riski Yudhi, *"Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)" Hardcore twenty-four : a Stephanie Plum novel*, vol. 7. Yogyakarta, 2022.

[19] Wahyudi, I., Muntasa, A., Yusuf, M., & Hamzah, A. (2021). Revealing and Testing the Authenticity of Digital Evidence in Cybercrime Using the Digital Forensic Research Workshop Method. *Journal of Information Technology and Management Applications (JATIM)*, vol. 2, no. (2), p. 120-127. doi : https://doi.org/10.31102/jatim.v2i2.1068 .

[20] IA Plianda and R. Indrayani, "Analysis and Comparison of the Performance of Digital Forensic Tools on Android Smartphones using WhatsApp Instant Messaging," *Budidarma Media Informatics Journal*, vol. 6, no. 1, p. 500, Jan 2022, doi: 10.30865/mib.v6i1.3487.

[21] R. Umar, A. Yudhana, and Muhammad Noor Fadillah, P. Master of Informatics Studies, and U. Ahmad Dahlan, "Comparison of Forensic Tools in Digital Wallet Applications," *Journal of Informatics and Computers)* , vol. 6, no. 2, p. 242–250, 2022.

[22] F. Anggraini, H. Herman, and A. Yudhana, "Forensic Analysis of the TikTok Application on Android Smartphones Using the Association of Chief Police Officers Framework," *JURIKOM (Journal of Computer Research)* , vol. 9, no. 4, p. 1117, Aug 2022, doi: 10.30865/jurikom.v9i4.4738.

[23] S. Sunardi, I. Riadi, and MH Akbar, "Steganalysis of Digital Evidence on Storage Media Using Static Forensics Methods," *National Journal of Information Technology and Systems*, vol. 6, no. 1, p. 1–8, May 2020, doi: 10.25077/teknosi.v6i1.2020.1-8.

[24] RM Gegang *et al.*, Analysis of Digital Forensic Evidence in the Threads Application Using the Digital Forensic Research Workshop Method. (2024). *FAHMA: Journal of Computer Informatics, Business and Management*, vol. 22 no. (2), pp. 1-10, May 2024. doi: https://doi.org/10.61805/fahma.v22i2.118.

[25] G. Fanani, I. Riadi, and A. Yudhana, "Forensic Analysis of the Michat Application Using Digital Forensics Research Workshop Methods," *Budidarma Media Informatics Journal* , vol. 6, no. 2, p. 1263, Apr. 2022, doi: 10.30865/mib.v6i2.3946.