JOURNAL OF INFORMATION ENGINEERING AND COMPUTER TECHNOLOGY
E-ISSN: 2797-1724, DOI: 10.30811/jtrik.v8i2.7437
Vol. 8 No. 2 2025 pp. 01-13

# WHATSAPP MESSENGER DATA BACKUP AND RECOVERY ANALYSIS USING MOBILEDIT FORENSIC EXPRESS AND DR.FONE

Prasetio[1], Aswandi[1*], Ilham Safar[1]

[1]Department of Information Technology and Computer, Lhokseumawe State Polytechnic
Jln. B. Aceh Medan Km. 280 Buketrata 24301 INDONESIA

Coresponding Author : Aswandi @pnl.ac.id

**Article info:**Received 01/07/ 2025, Revised 10/07/2025, Accepted 15/08/2025



## Abstract

This research is motivated by how to backup data and recover data that has been lost due to carelessness or user error in using this WhatsApp messenger application, this research aims to Backup and Recover data on the WhatsApp messenger application that has been deleted, lost data, failure, and damage (failure). The results of the study show that the Mobiledit Forensic Express application has different levels of success in backing up and recovering data. This application cannot recover conversation data that has a percentage (50%), but is able to backup and recover various WhatsApp data such as; Links, Status, WhatsApp Animated Gifs, WhatsApp Audio, WhatsApp Documents, WhatsApp Images, WhatsApp Sticker, WhatsApp Video, WhatsApp Video Notes, and WhatsApp Voice Notes (100%) data that can be backed up and recovered by the Mobiledit Forensic Express application. While the Dr.Fone application can backup data and recover WhatsApp chat data with a percentage (80%), but data such as WhatsApp attachments (Audio, Documents, Images, Stickers, Videos, and Voice Notes) only get (50%) because it can only recover new and undamaged photos or videos from the WhatsApp application. By comparing or searching for which applications are relevant for conducting research can help the forensic team and can make it easier for those who want to backup data and recover data in the WhatsApp application using applications that support this research, Mobiledit Forensic Express and Dr.Fone.

**Keywords:**Data backup, data recovery, Mobiledit Forensic Express, Dr.Fone and Whatsapp

## 1. Introduction

The rapid growth of chat media today is a phenomenon that is deeply felt by internet users, especially those using the WhatsApp Messenger application. With the existence of instant Messenger applications, it is possible to create various types of chat content from various types of WhatsApp Messenger applications, from messages containing chats or confidential information to even criminal plans. Within this scope, WhatsApp is the most widely used instant Messenger application worldwide. According to data from wearesocial.com, WhatsApp Messenger has reached 1.5 trillion monthly users across various platforms in August 2017, exceeding 2.7 trillion social media users worldwide. With an increase in new WhatsApp Messenger users of 8 million users (wearesocial.com) across various mobile platforms from April to August[1]. In 2021, Indonesia had the third-highest number of WhatsApp users in the world. The number of WhatsApp users in the country reached 84.8 million in June 2021.

Data backup and data recovery analysis is a process that involves understanding, evaluating, and implementing methods to ensure that data related to WhatsApp, such as text messages, images, videos, and other files, can be safely backed up and recovered in the event of loss or damage, loss, or unexpected events that aim to minimize the risk of losing valuable data and maintain the integrity of user data, protect messages and personal information, and ensure that users can recover their data quickly and effectively in the event of a problem [2].

WhatsApp cybercrime is an act of intimidation, threats, harassment, or insults carried out through the WhatsApp application. Cybercrime that occurs through WhatsApp can involve sending text messages, photos, or videos that demean or emotionally harm the victim.[3]Cybercrimes committed through WhatsApp are often carried out covertly, so victims may not realize they are being targeted. This can leave victims feeling isolated and making it difficult to seek help. Both data backup and data recovery are important to ensure that data on WhatsApp Messenger or similar messaging apps remains secure and can be recovered in the event of issues such as accidental data deletion, device damage, or a smartphone device change.

In the context of Digital Forensics, Mobiledit Forensic Express is a digital forensic tool used to retrieve, analyze, and recover data from mobile devices.[4]This tool is specifically designed to assist digital forensics professionals in collecting digital evidence from various types of mobile devices, including smartphones and tablets.[5].

This study aims to This study aims to test and compare the performance of Mobiledit Forensic Express and Dr.Fone in the process of data backup and recovery of WhatsApp data. The focus is on whether these two applications can back up and recover data on WhatsApp Messenger that experiences various problems, such as data deletion, data loss, device failure, and damage. The results of this study are that using the Mobiledit Forensic Express and Dr.Fone applications works well and as it should. However, these two applications have their respective advantages and disadvantages in terms of features, speed, and reliability in analyzing each application..

## 2. Research methods

The method used is the data recovery and data backup method. This method consists of several process stages, namely retrieving, analyzing and restoring deleted data in images or chats.

This data backup and data recovery method candescribes digital artifacts stored in hardware or software devices. These digital artifacts can include computer systems, storage media (such as hard disks or CD-ROMs), electronic documents (e.g., PDF messages or JPEG images). The following are the stages in the data backup and data recovery methods below;

**A. Data Backup and Recovery Methods**

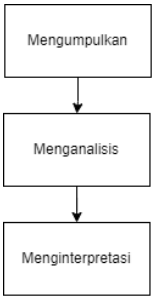



Figure 1. Data backup and data recovery methods

Explanation of the stages of the data backup and data recovery methods:

1. Taking: This stage is the stage of collecting data which is directly obtained from the source and given to the data collector or researcher (Simulation).
2. Analyze: At this stage, researchers analyze the data obtained by conducting a simulation system, then extract it, then use the features provided by the Mobiledit Forensic Express and Dr.Fone applications. Researchers can search for data consisting of WhatsApp images, WhatsApp videos, WhatsApp stickers, WhatsApp voice notes, WhatsApp documents, WhatsApp audio, and WhatsApp GIFs related to digital forensic methods.
3. Recovering: After performing data retrieval or data collection and analysis, researchers can continue with more in-depth analysis to identify differences between data before and after the backup process, as well as recover data related to deleted chats, images and videos.

**B. *Architecture*Network**

The design or implementation of the network topology that will be analyzed and simulated is as shown in the image below:

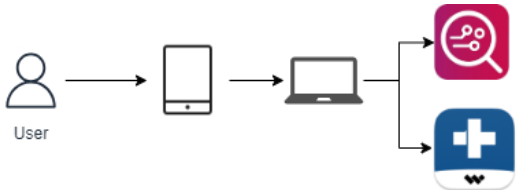



Figure 2. Network Architecture

In the network architecture design in Figure 2, the user tries to perform analysis in carrying out the data

recovery process and restoring data using Mobiledit Forensic Express and Dr.Fone.

As for the Block Diagram

This block diagram will illustrate or explain the system design that will be analyzed, including how Mobiledit Forensic Express and Dr.Fone work and how they are implemented. The explanation will be presented through a block diagram as shown below:

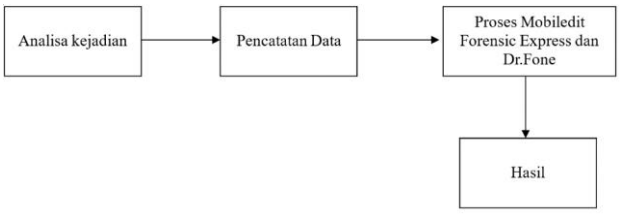



Figure 3. Block Diagram

Explanation of the stages of the Block Diagram

Based on the block diagram above, it explains the system design with various stages that will explain or produce the results being worked on in the block diagram above.

1. Conducting Incident Analysis: When analyzing the incident, the perpetrator committed his crime (Cybercrime) via personal chat and removed traces when he had carried out the attack or sent a message or chat.
2. Data Recording: After the data has been successfully collected, the next step is the information search process where the user wants to see the chat and then searches for the day, date and month the user was affected by the chat.
3. Data Backup and Data Recovery Process: This process uses the Mobiledit Forensic Express and Dr.Fone applications or software, after obtaining all the simulated data, it is then processed to perform data backup and data recovery.
4. Results: After that, the researchers conducted an analysis on the successful backup and recovery process and viewed the data before and after backup by the Mobiledit Forensic Express and Dr.Fone applications. After that, all researchers recovered data in the form of documents. Network Forensic Analysis at this stage, forensic analysis was carried out to identify digital traces or other evidence of suspicious or illegal activity on the network.

## 3. Results and Discussion

The results of the WhatsApp Messenger Data Recovery analysis process using the Mobiledit Forensic Express and Dr.Fone applications or Backing Up Data on WhatsApp;

A. Mobiledit Forenic Express

Mobiledit Forensics Express is a digital forensics software used to collect, analyze and assemble digital evidence from mobile devices.

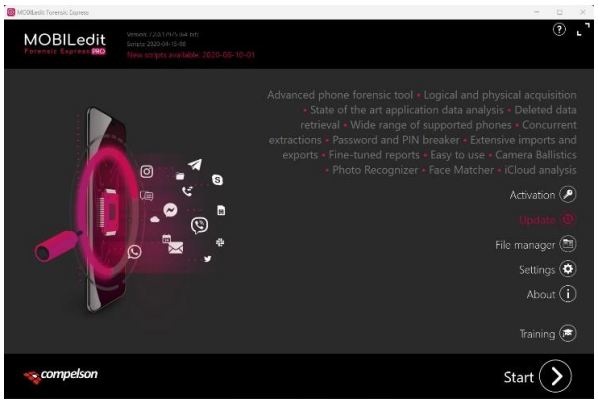



Figure 4. Mobiledit Forensic Express Application Display

Using Mobiledit Forensic Express, users can access, extract, and analyze data contained within mobile devices, including text messages, calls, contacts, images, videos, audio files, notes, calendars, and more. The software can

also recover deleted data, track device activity, and provide detailed forensic reports.

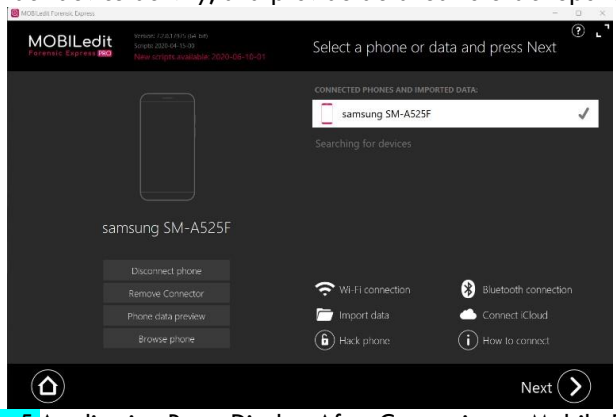



Figure 5.Application Page Display After Connecting to Mobile Phone

In the image above, this is the display after connecting from the mobile forensic express application to the cellphone. The process when connecting to this application goes through several stages that have been set in the application which is written "About".

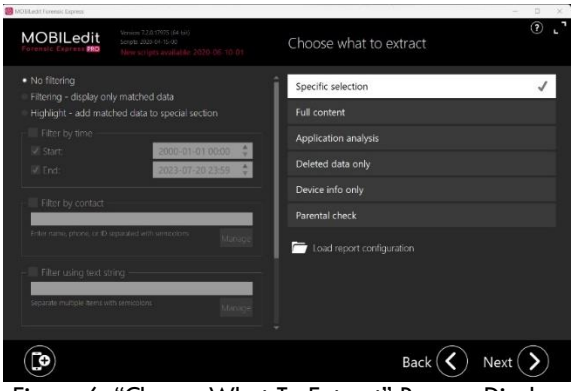



Figure 6. “Choose What To Extract” Process Display

“Choose what to extract” With this feature, forensic investigators or those who want to backup and recover data can determine what data they want to extract from mobile devices and investigate more carefully and specifically.

As well aslnvestigators can select the specific types of data they want to extract from the mobile device under investigation. This feature allows them to focus on data that is relevant and critical to their investigation, saving time and streamlining the analysis process.

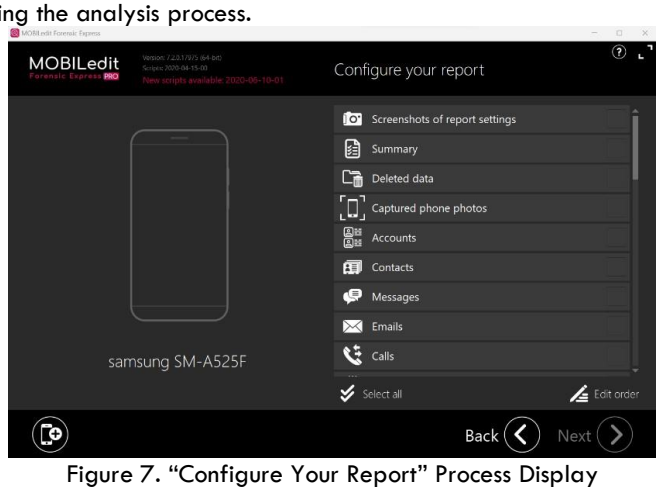



Figure 7. “Configure Your Report” Process Display

"Configure your report" is a feature in Mobiledit Forensic Express that allows users to customize the analysis and investigation reports generated by the software. Once the analysis is complete, users can configure the report by selecting what information and data to include, as well as adjusting its appearance and formatting as needed.

Here are some important points related to the "configure your report" feature in Mobiledit Forensic Express:

1. Data Selection

Users can choose the type of data they want to include in the report. For example, they can choose to include information about text messages, calls, contacts, apps, social media, or other data relevant to the investigation.

2. Filter and sorting

Users can use filters and sorting settings to refine the data entered into reports. This feature helps users select relevant and significant data and clarify analysis results.

3. Export and Distribution

Once a report is configured to your liking, users can export it in various formats, such as PDF, Excel, or other formats. Additionally, the report can be distributed to relevant parties who need the information.

The "configure your report" feature allows those who want to back up data, recover data, forensic teams, investigators to create reports that are neat, structured, and contain relevant information for investigation purposes.

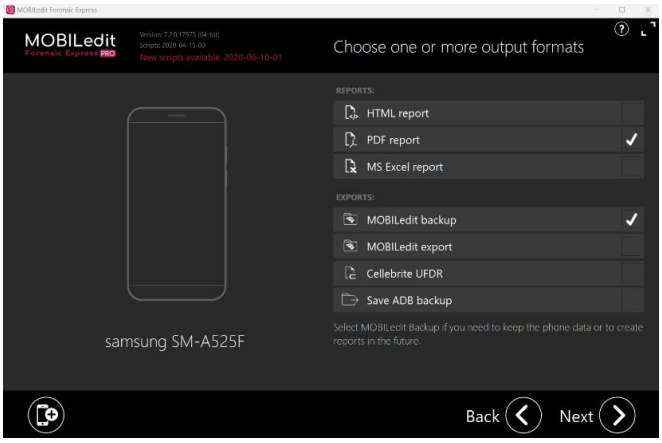



Figure 8. “Choose One Or More Output Formats” Process Display

"Choose one or more output formats" is a feature in Mobiledit Forensic Express that allows users to select one or more output formats when exporting or saving analysis and investigation reports generated by the software. This feature provides users with the flexibility to save and share analysis results in various formats according to their needs and preferences. Here, the researcher selects or checks several formats used for research, namely "PDF report" and "MOBILedit backup."

Here are some points related to the "choose one or more output formats" feature in Mobiledit Forensic Express:

1. Available Export Formats: Mobiledit Forensic Express typically offers several commonly used export formats, such as PDF, Excel, CSV (Comma-Separated Values), HTML, XML, and others. Users can select one or more of these formats to save their analysis reports.
2. Specific Requirements: Users can choose the output format that best suits their needs. For example, if a report is needed for presentations or printing, PDF format may be more appropriate. If the data needs to be imported into another application, CSV or Excel format may be more suitable.
3. Customization and Compatibility: This feature allows users to save reports in a format that is compatible with other applications or devices that will be used to open or process the report.
4. Multiple Output Formats: Users can select more than one output format if they need to save the report in different formats for different purposes or to share with different parties.

With the "choose one or more output formats" feature in Mobiledit Forensic Express, forensic teams or investigators have the flexibility to save and share analysis results in a way that best suits their needs.

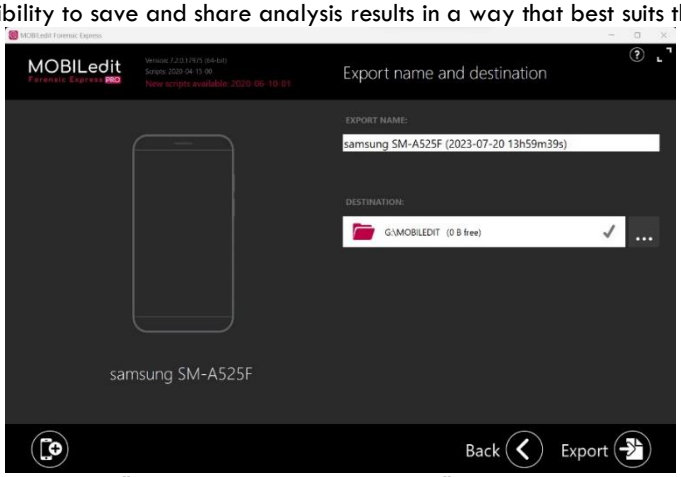



Figure 9. "Export Name and Destination" Process Display

"Export name and destination" is a feature that allows users to specify a file name and destination location

when exporting or saving analysis results and reports from Mobiledit Forensic Express. This feature gives users control over how analysis reports will be stored and identified.

Here are some points related to the "export name and destination" feature in Mobiledit Forensic Express:

1. Determining File Name and Storage Location: Users can specify the file name for the analysis results report to be exported and this feature allows users to select the storage location or destination folder to save the analysis results report.
2. Export Format: In addition to specifying the file name and destination location, users can also choose the desired export format for the report. Commonly used formats include PDF, Excel, CSV, HTML, XML, and others.
3. Ease of Identification: Specifying a descriptive file name and a precise destination location will make it easier for users to identify saved reports and access them again when needed.

With the "export name and destination" feature in Mobiledit Forensic Express, forensic teams or investigators have complete flexibility and control over how analysis reports are stored. This feature ensures reports are neatly stored and easily accessible.

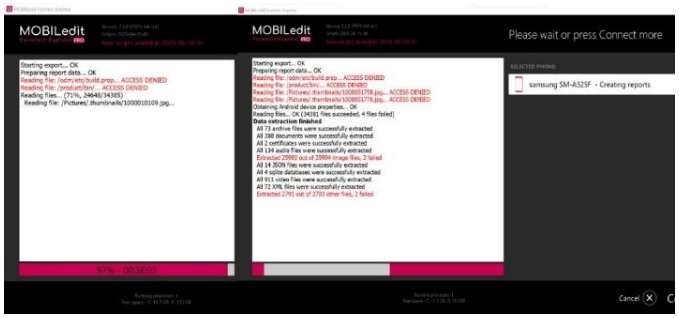



Figure 10. Process Result Display

During this process, several files, including image files, and other files, received "access denied" during reading. The reason for this is the failure to root the phone at the initial page. However, there were a few unreadable files: 4 in the read file, 2 in the image file, and 2 in the other file. Many were readable and could be backed up by Mobiledit Forensic Express.

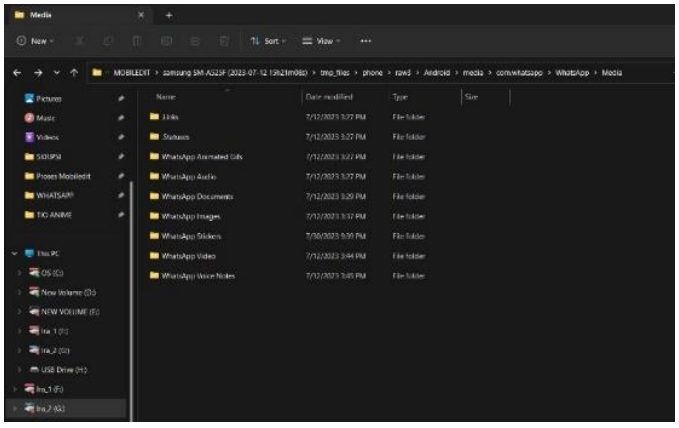


Figure 11. Saved View of Mobiledit Forensic Express Results Folder

The image above shows where the results folder for Mobiledit Forensic Express files, or the results extracted from the Mobiledit Forensic Express application, are stored. Some files were successfully extracted by Mobiledit Forensic Express, while others were not.

Backup_File > phone > raw3 > Android > Media > com.whatsapp > Whatsapp

Table 1. Display of Backed Up WhatsApp Files

| Mobiledit Forensic Express | |
|---|---|
| backup_files 7/12/2023 4:39 PM File folder | |
| WHATSAPP | |
| .Shared | Found |
| Backups | Found |
| Databases | Found |
| Media | Found |

The table above displays the "backup_files" files that were successfully backed up by the Mobiledit Forensic Express application. These files are important files or core files of WhatsApp data files. "Backup_files" or "File security" (Backup_Files) refers to the process of making copies of important data or information from a device or system and storing them in a secure location. The goal is to ensure that valuable data is not lost due to device failure, malware attacks, or human error.

Table2. Contents View “File .Shared”.Shared

| .Shared | | | |
|---|---|---|---|
| No | File | Type | Information |
| 1 | u4lGjF5URPXN52urtm-HTsEV5c6u9033VDNtT20klqc=.tmp.chck | CHCK | Found |
| 2 | tHNAx51jaoWg5BAA595vKqlWMHQmwL0o73Mb6TDWu3k=.tmp.chck | CHCK | Found |
| 3 | imikmw0TcomjDpbhZLw0L7dES1e9h2RtBnHlboLzD38=.tmp.chck | CHCK | Found |
| 4 | K5or8gYhMCrG40inwYkCLk3Wq63osyz3CxbjMd4Qcjc=.chk.tmp | TMP | Found |
| 5 | K5or8gYhMCrG40inwYkCLk3Wq63osyz3CxbjMd4Qcjc=.tmp | TMP | Found |

The table above displays the contents of the ".shared" files that can be backed up by the Mobiledit Forensic Express application. ".shared" refers to the act of sending or sharing content, such as text messages, images, videos, links, or documents, to contacts or groups on WhatsApp. When a user shares something on WhatsApp, they choose to send it to one or more people, either privately or in a group.

Table 3. Display of the Contents of the "Backups" File

| Backups | | | |
|---|---|---|---|
| o | File | Type | Information |
| | backup_settings.json.crypt14 | Crypt14 | Found |
| | chatsettingsbackup.db.crypt14 | Crypt14 | Found |
| | commerce_backup.db.crypt14 | Crypt14 | Found |
| | stickers.db.crypt14 | Crypt14 | Found |
| | wa.db.crypt14 | Crypt14 | Found |
| | wallpaper.bkup.crypt14 | Crypt14 | Found |
| | wallpapers.backup.crypt14 | Crypt14 | Found |

The table above displays the contents of important WhatsApp folders, and the files mentioned above are among the core WhatsApp files. "Backup files" refer to copies or duplicates of data stored for security or recovery purposes. Backup files are created to prevent the loss of valuable data in situations where the primary data becomes corrupted, lost, or inaccessible.

The primary purpose of creating backup files is to ensure that important and sensitive data remains secure and can be recovered in an emergency. Backup files can include various types of data, such as documents, images, videos, system configurations, application data, and more.

| Databases | | | |
|---|---|---|---|
| o | File | Type | Information |
| | msgstore.db.crypt15 | Crypt15 | Found |

Table1.View "Database" File Contents

| | | | |
|---|---|---|---|
| | msgstore-2023-08-10.1.db.crypt15 | Crypt15 | Found |
| | msgstore-2023-08-09.1.db.crypt15 | Crypt15 | Found |
| | msgstore-2023-08-08.1.db.crypt15 | Crypt15 | Found |
| | msgstore-2023-08-07.1.db.crypt15 | Crypt15 | Found |

The table above displays the contents of important WhatsApp folders, and the files above represent the core WhatsApp files. A "database" is a data storage structure used by the WhatsApp application to store information such as text messages, calls, contacts, images, videos, and other data related to the user and conversations between other users. This database allows WhatsApp to manage and provide quick access to all the information a user needs.

Table2. Display the contents of the "Media" file

| Media | | | |
|---|---|---|---|
| o | File | Type | Information |
| | Links | File Folder | Found |
| | Statuses | File Folder | Found |
| | Whatsapp Animated Gifs | File Folder | Found |
| | Whatsapp Audio | File Folder | Found |
| | Whatsapp Documents | File Folder | Found |
| | Whatsapp Images | File Folder | Found |
| | Whatsapp Stickers | File Folder | Found |
| | Whatsapp Video | File Folder | Found |
| | Whatsapp Video Notes | File Folder | Found |
| 0 | Whatsapp Voice Notes | File Folder | Found |

The table above displays the contents of important WhatsApp folders or supporting files. "Media" refers to the various types of multimedia content that can be shared and received through the application. WhatsApp media includes files or data such as links, statuses, WhatsApp animated GIFs, WhatsApp audio, WhatsApp documents, WhatsApp images, WhatsApp stickers, WhatsApp videos, WhatsApp video notes, and WhatsApp voice notes.

B. Dr.Fone App

Dr.Fone is a suite of software developed by Wondershare. It's designed to help users manage, secure, and recover data from mobile devices, particularly Android and iOS devices.

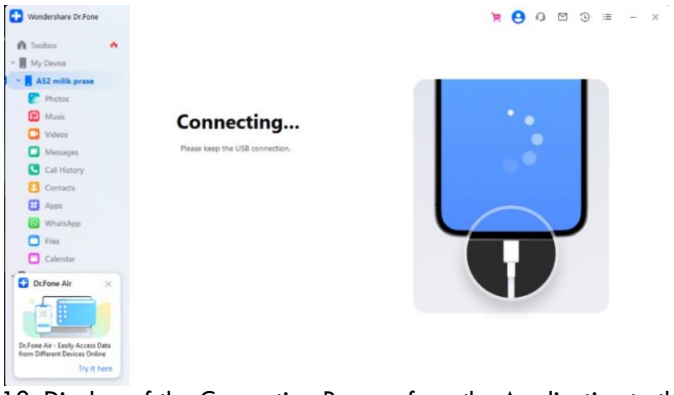



Figure 12. Display of the Connecting Process from the Application to the Mobile Phone

In this process, the application tries to connect from the Dr.Fone application to the researcher's cellphone so that it can enter the researcher's WhatsApp data to carry out the thesis research process.

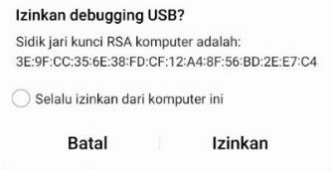
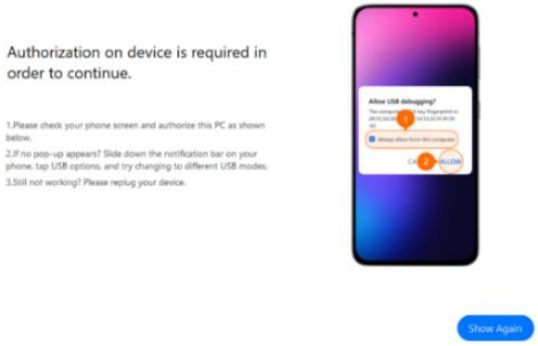



Figure 13. USB Debugging Permission View

Once detected, the application asks for debug permission and requests access to the phone data so that the Dr.Fone application can carry out the next process.




*Picture14. Display of the Whatsapp Connecting Command Process*

After that, there are several commands so that the Dr.fone application and cellphone can be connected to the cellphone and WhatsApp.

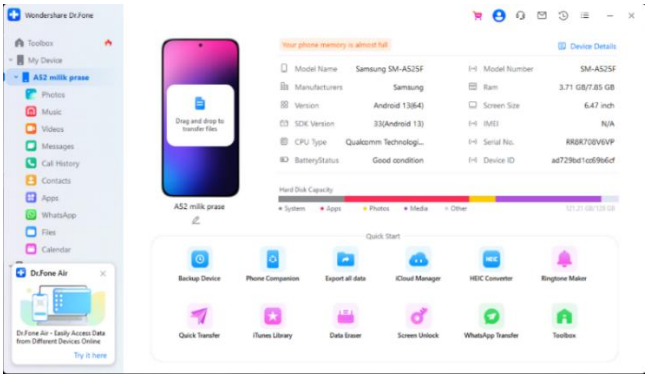


Figure 15. Page Display After Connecting to Mobile Phone

The display after the cellphone is connected to the Dr.fone application, Dr.Fone can read the specifications of the owner's cellphone or cellphone connected to the application and can see the memory, etc.

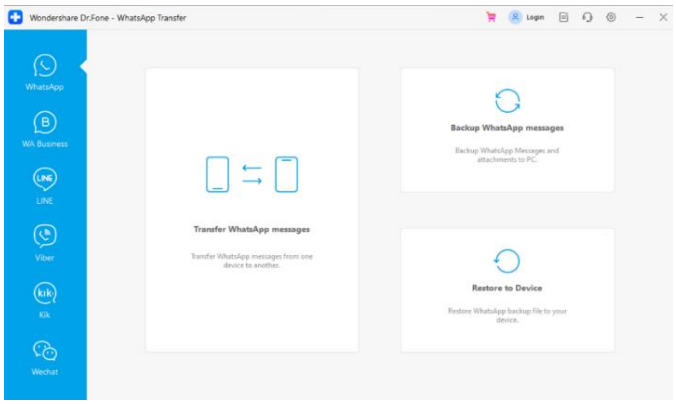



*Figure 16. Display of Applications That Can Be Backed Up and Restored*

WhatsApp transfer display that can read several applications that can be backed up or restored to this application.

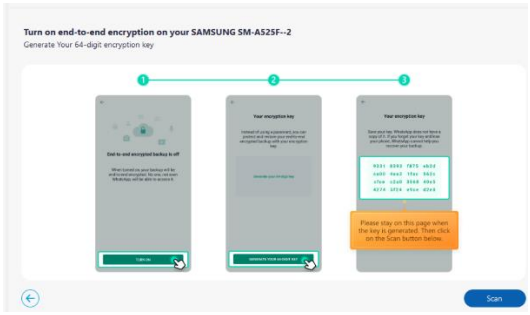



*Figure 17. Display 1 Connect WhatsApp Mobile to WhatsApp Laptop*

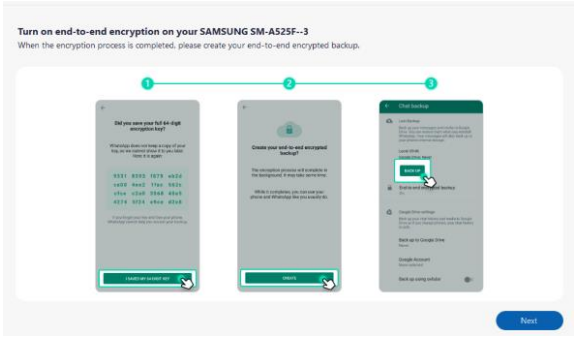



*Figure 18. Display 2 Connecting WhatsApp from Mobile Phone to WhatsApp from Laptop*

At this stage, the phone used for the research must follow the instructions in the application to first encrypt WhatsApp. Encryption is the process of securing data by converting it into a secret code to prevent unauthorized access. In this context, Dr.Fone may offer an encryption feature to protect the user's personal data on the phone. If this feature is available, the user can enable encryption on their phone through the device's security settings.

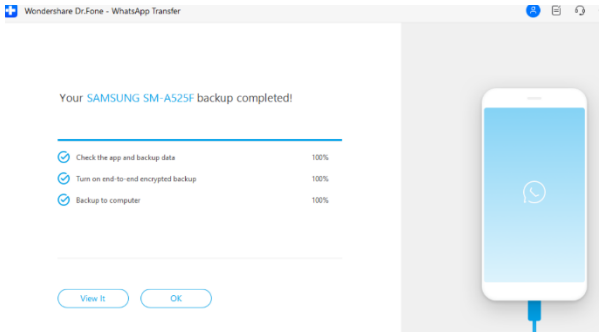



*Figure 19. Display of 2 WhatsApp Processes and Data Scans on a Mobile Phone*

During this process, the application processes and scans WhatsApp data on the phone and backs up the data from the researcher's phone. This process, transferring or retrieving the backup data, takes a considerable amount

of time, depending on the data used in the research.

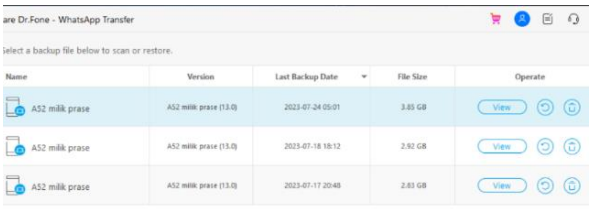



*Figure 20. Display of Backed-Up WhatsApp Data*

The display above is a display of some WhatsApp data that has been backed up by the Dr.Fone application. You can read the file size, last backup data, cellphone version and cellphone owner name.

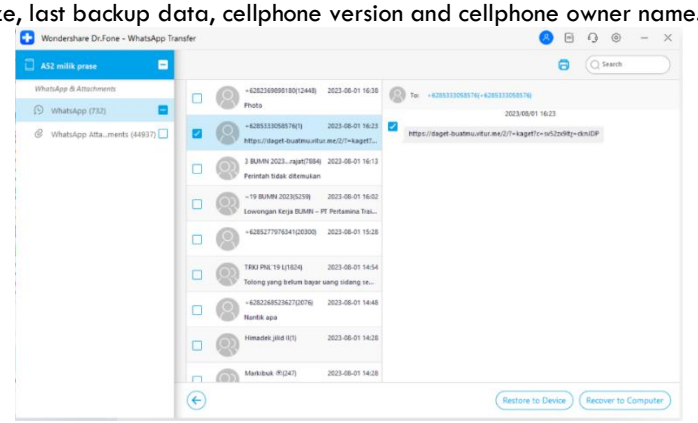



*Figure 21. Phishing Chat Process Display*

In this process, Dr.Fone can view several chats that have been backed up by the Dr.Fone application and can view phishing links sent by the attacker.

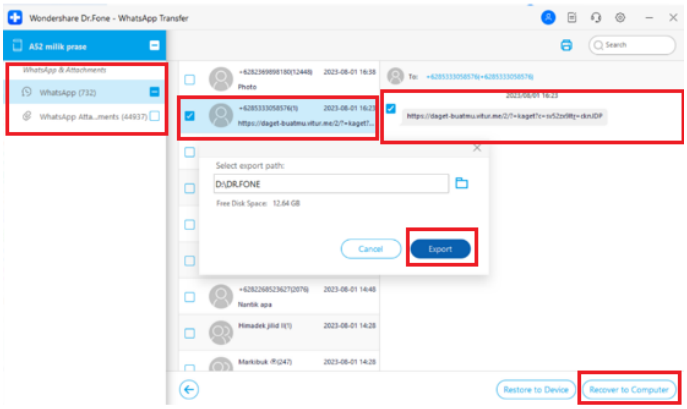



*Figure 22. Process 1 Recovery To Computer Display*

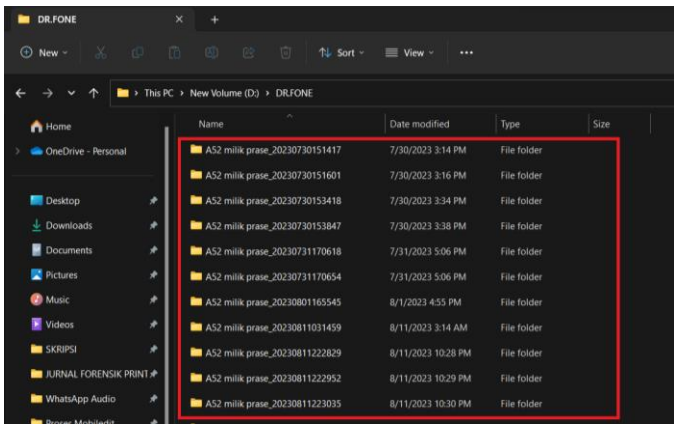



Figure 23. Display of Process 2 Recovery To Computer

Above is the process of saving chats that you want to back up to your computer and the results are in PDF format and some that have been recovered are in a predetermined folder.

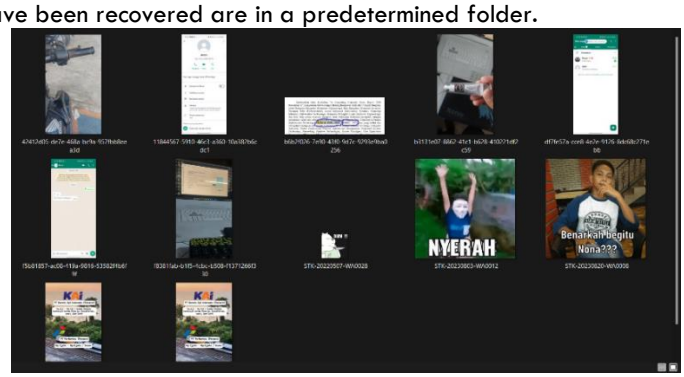



Figure 24. PDF Result Display

Above are the results of research on recovering sticker, video, and image data to a computer that can be backed up and can be seen in WhatsApp attachment files.

*Table3. Dr.Fone Data View*

| Dr.Fone | | | |
|---|---|---|---|
| Device | Document | Backup | Information |
| A52 | Whatsapp Attachment | Chat | Found |
| | | Picture | Found |
| | | Video | Found |
| | | Sticker | Found |
| | | World | Found |
| | | Contact | Damaged |
| | | Maps | Damaged |
| | | Voice note | Damaged |
| | | Audio | Damaged |
| | | Pdf | Damaged |

The table above shows the WhatsApp data that was found and not found (corrupted). Some files from Dr.Fone were visible, but when transferred or restored to a computer, they were corrupted or unreadable, and there was no file content in the restored WhatsApp attachment folder.

## 4. Conclusion

The conclusion of this study is that using the Mobiledit Forensic Express and Dr.Fone applications, both applications performed well. However, each has its own advantages and disadvantages in terms of features, speed, and analysis reliability.

1. Using MobileEdit Forensic Express and Dr.Fone, it can be concluded that both applications have significant capabilities in collecting, analyzing, and recovering WhatsApp Messenger related data.
2. MobileEdit Forensic Express offers extensive coverage in data extraction from the target device, including text messages, Links, Status, Whatsapp Animated Gifs, Whatsapp Audio, Whatsapp Documents, Whatsapp Images, Whatsapp Stickers, Whatsapp Videos, Whatsapp Video Notes, and Whatsapp Voice Notes, and related metadata.
3. Dr.Fone boasts outstanding capabilities in recovering lost or deleted data. This app can help restore deleted messages and media, specifically WhatsApp.
4. Dr.Fone's advantages in data recovery have limitations, such as the possibility of not being able to recover all data, and the length of time that data is lost
5. MOBILedit Forensic Express and Dr.Fone can help in recovering lost WhatsApp data, but the results may vary depending on the specific situation and condition of the lost data as well as on the specific needs and objectives of the investigation or analysis.

## REFERENCE

[1] N. Anggraini, S. U. Masruroh, and H. Tiaraningtias, "Analisa Forensik Whatsapp Messanger Pada Smartphone Android," J. Ilm. FIFO, vol. 12, no. 1, p. 83, 2020, doi: 10.22441/fifo.2020.v12i1.008.

[2] M. S. Simanjuntak and J. Panjaitan, "Analisa Recovery Data Menggunakan Software," J. Tek. Inform. Komput. Univers., vol. 1, no. 1, pp. 26–32, 2021.

[3] F. A. Maulana, I. Ernawati, P. Labu, and J. Selatan, "Analisa sentimen cyberbullying di jejaring sosial twitter dengan algoritma naïve bayes," Semin. Nas. Mhs. Ilmu Komput. dan Apl. (SENAMIKA, pp. 529–538, 2020, [Online]. Available: https://conference.upnvj.ac.id/index.php/senamika/article/view/619

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

[5] M. R. D. Qibriya, A. Ambarwati, and K. E. Susilo, "Analisis Forensik Digital Pada Aplikasi Instant Messaging Di Smartphone Berbasis Android Untuk Bukti Digital," J. Teknol. Inf., vol. 5, no. 2, pp. 114–121, 2021, doi: 10.36294/jurti.v5i2.2200.