07/06/24

Mobile and Forensics
Vol. 1, No. 1, March 2019, pp. XX-XX
ISSN: 2714-6685 (online), 2656-6257 (print)
DOI: http://dx.doi.org/10.12928/mf.v1i1.XXX

Digital Forensic Analysis of Gojek Conversations using the NIJ Method and Tools Comparison

[1]Suprayogi Budhi Purwanto, [2,*]Guntur Maulana Zamroni
[1,2]Program Studi Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan
[1,]Suprayogi1900018049@webmail.uad.ac.id, [2*]guntur.zamroni[at]tif.uad.ac.id
*correspondence email

Abstract

Gojek has an instant messaging feature that can be used to communicate. The instant messaging feature of the Gojek application has the potential to be used as a medium for infidelity or other misuse. For handling and proving cases involving digital devices, it is necessary to use digital forensic methods. However, there is no research that explores digital forensics on these features. This research applies mobile forensics to the Gojek instant messaging feature by adopting the NIJ method. The research stages consist of 8 stages, namely case scenarios, identification, collection, examination, analysis, comparison of tools, validation and conclusions. This research uses 6 digital forensic tools including Oxygen Forensics, Belkasoft, Mobiledit, Magnet Axiom, Autopsy, and FTK Imager. This research uses two smartphones as electronic evidence, namely M6 and SM-G530H. This research succeeded in finding evidence artifacts from the implementation process of mobile digital forensics. On the M6 only Oxygen Forensics managed to get text message and contact artifacts. While on SM-G530H all tools managed to get complete artifacts both text message artifacts, images, and contacts. The validation process is carried out on digital evidence artifacts with the result that all artifacts meet the validation aspects of repeatability, and reproducibility. The digital forensic tool with consistent performance is Oxygen Forensics version 12 by successfully obtaining 100% artifacts on the M6 and 86% artifacts on the SM-G530H.

Keywords: Analysis; Instant Messaging; Forensics; Gojek; NIJ

INTRODUCTION

Gojek application is an application-based public transportation service platform for both motorbikes and cars that can be ordered online. Gojek is equipped with an instant messaging feature that can be used to communicate, Gojek application users often use the messaging feature to fellow Gojek users to communicate with Gojek drivers, friends and their families [1]. This instant messaging feature facilitates users to be able to communicate both directly and quickly with people in their social network, which can help strengthen relationships between parties. In addition, users also often interact with Gojek drivers during the trip, which can be an opportunity to exchange information and experiences[1]. The availability of instant messaging features on the Gojek application is not impossible to potentially be used as a medium for infidelity and has the potential to appear other abuses such as spam messages, fraud, phishing, and so on. Handling cases of crimes that occur in Cyberspace certainly involves digital evidence which in its handling involves activities including identifying, storing, analyzing, and presenting digital evidence [2].

Research conducted by Achmad Syauqi in 2020 entitled Analysis of Recovery of Instant Messenger Evidence on Android Smartphones using the NIST Method. This study aims to obtain evidence of digital infidelity crimes using an android smartphone, in this study the tools used are Oxygen Forensics software using the NIST method to obtain SMS artifacts [3]. Research conducted by Aldian et al in 2021 entitled Digital Forensic Analysis of the Gopay Application on android. The research aims to conduct digital forensics in solving cybercrime cases against digital wallets [19]. Research conducted by Arif et al in 2023 conducted research entitled Analysis of Direct Message Digital Evidence on Twitter Using the National Institute of Justice (NIJ) Method. Aiming to obtain digital evidence of pornography services using NIJ and forensic tools, where

***Article History:** Received December 9, 2018; Revised January 3, 2019; Accepted February 17, 2019*

digital evidence can be used as support in handling crimes [4]. Research conducted by Saputri et al in 2022 entitled Forensic Data Analysis of Investigations of Narcotics and Drug Distribution Cases on Android-Based Smartphones. The study used the NIJ method, the purpose of the study was to reveal forensic evidence of narcotics and drug distribution cases on smartphones using the Whatsapp application based on the android operating system. The tools used are Magnet Axiom and MobilEdit Forensic [5]. Research conducted by Mahendra et al in 2021 entitled Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases. This research uses the NIJ approach as a method that serves to explain the research steps carried out as a guide in solving problems, the research aims to reveal evidence of online prostitution cases. The tools used in this research are Mobiledit Forensic Express and SysToolsSQLite Viewer [6]. Research conducted by Mailangkay et al in 2022 entitled Comparative Analysis of Tiktok Lite Digital Evidence Using the NIJ Method. This study aims to obtain digital evidence in the form of conversation messages and account data on the Tiktok Lite application in crimes, especially cyberbullying using the National Institute of Justice method or abbreviated as NIJ and the percentage of digital evidence obtained by forensic tools, the tools used in this study include MOBILedit Forensics Express, Belkasoft Evidence Center, and Magnet Axiom [7]. However, of the previous studies, there is no research that analyzes mobile digital forensics and compares the performance of tools in the digital forensics process on the instant messaging feature to fellow Gojek application users.

The process of retrieving digital evidence can be done using several methods, such as Integrated Digital Forensics Identification Framework (IDFIF)[8], National Institute of Standards and Technology (NIST)[9], Digital Forensics Research Workshop (DFRWS)[10], Association of Chief Police Officers (ACPO)[11], General Computer Forensic Investigation Model (GCFIM)[12], National Institute of Justice (NIJ)[13]. NIJ has better steps compared to other methods. The NIJ method is one of the forensic frameworks that has advantages in the forensic process, ease of use, guidelines for respondents who are still very lay [14], [15], [16]. The NIJ method also has a systematic flow, and is a method that is often used [17], [18]. This research conducts forensic analysis using the NIJ method and compares the performance of mobile forensic tools. This research looks for digital evidence of infidelity cases in the instant messaging feature of fellow users in the Gojek application.

METHODS

This research adopts the NIJ method to obtain digital evidence in infidelity case studies in the form of conversation text, image and contact media and compares the performance of the tools used. The forensic process uses several tools, namely Oxygen Forensics, Belkasoft X (Belkasoft Evidence Center X), Mobiledit Forensics, Magnet Axiom, Autopsy, and FTK Imager.

Research Method

This research implements the investigation process adopting the National Institute of Justice (NIJ) method. It consists of eight stages, namely identification, collection, examination, analysis, comparison tools, validation and conclusion. The stages of the NIJ method can be seen in Figure 1.

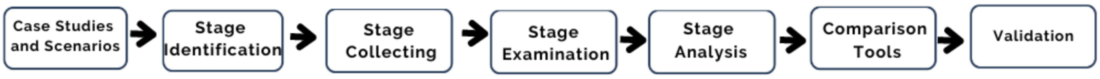


Fig. 1. The Stage of NIJ mobile forensic method.

a. **Case Study and Scenario**

The simulation scenario of this research uses a case scenario of infidelity on the Gojek instant messaging feature. Involving the perpetrators A and B and the victim, the scenario can be seen in Figure 2 below.

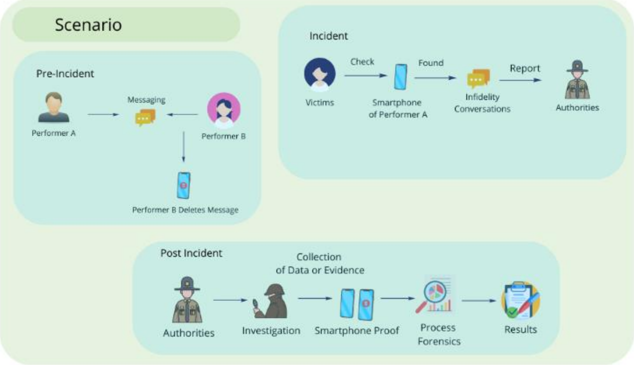


Fig. 2. Case Study and Scenario.

b. Identification Stage

It is the process of classifying digital crime evidence and sorting data to strengthen investigation steps in an effort to uncover digital crime evidence. In the identification stage, there is a process of identification, labeling, and recording carried out to ensure the integrity of the evidence [19]. Furthermore, preparing the tools and materials used, namely computers / PCs, Oxygen Forensics, Belkasoft X (Belkasoft Evidence Center X), Mobiledit Forensics, Axiom Magnets, Autopsy, and FTK Imager.**Abbreviations and Acronyms**

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

c. Collection Stage

Is a series of data collection activities aimed at supporting the investigation stage related to the search for digital crime evidence. In this phase, data collection and retrieval are carried out from relevant sources and maintain the integrity of evidence against possible changes [19]. The tools used in this stage to perform data acquisition on the perpetrator's smartphone are Oxygen Forensics, Belkasoft, Mobiledit, and Magnet Axiom.

d. Examination Stage

This stage includes forensically examining the data that has been obtained, both through manual and automated processes. At this stage, verification is carried out to ensure that the data obtained in file format remains authentic and in accordance with its original state [19]. The data inspection and checking process is carried out using Oxygen Forensics, Belkasoft, Magnet Axiom, Autopsy, FTK Imager, and Hash my file. The hashing used is CRC-32

e. Analysis Stage

Analysis is carried out after successfully obtaining the desired data or digital files from the previous examination stage. The data is analyzed in detail and completely using a technically and legally valid approach to be able to prove the data [19].

f. Tools Comparison

Comparing the performance of digital forensic tools used in this research. The comparison was carried out to get recommendations for good tools for handling infidelity case studies using the Gojek instant messaging feature. The comparison is done by looking at the ability of forensic tools to obtain artifacts and their numbers from the case studies in this study, namely messages in the form of text, images, and contacts.

g. Validation

The results of the forensic process will be repeated using the same tools, and repeated using different tools. At this stage, we will also discuss the comparison of the hashing value of the conversation database artifacts to validate the results of the findings of messages in the form of text that have been successfully obtained from smartphones that have been carried out anti-forensics.

RESULT AND DISCUSSIONS

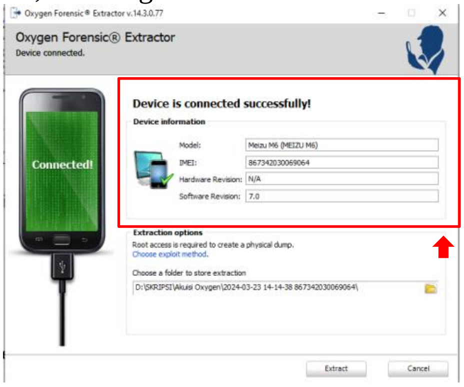
Mobile digital forensics process and comparison of forensic tools by adopting the National Institute of Justice method. The object of this research is the instant messaging feature of the Gojek application version 4.77.1 which runs on the Android operating system.

Identification

In this case the devices that are electronic evidence are two android smartphones so that the forensic tools used include Oxygen Forensics, Belkasoft, Mobiledit Forensics, Axiom Magnet, Autopsy, and FTK Imager. The condition of the electronic evidence obtained is connected to the internet, without a password, there is no SD Card / internal memory only and has been rooted.

Collection

Collect data from related sources and look for relevant data to become evidence, and maintain the authenticity of the evidence from changes. After the smartphone evidence is secured, it is necessary to activate airplane mode to anticipate contamination of the evidence, and perform charging to maintain the condition of the smartphone. The data acquisition process on this smartphone uses a data cable that is connected to a PC / computer in the Digital Forensics Laboratory. The condition of the smartphones of Perpetrator A and Perpetrator B is not locked in any password or encryption so as to facilitate the process of performing data acquisition. The acquisition process is carried out to retrieve digital data from the internal memory of the smartphone because there is no SD Card found. Data copying or imaging is done using Oxygen Forensics, Belkasoft, Mobiledit, and Magnet Axiom tools as shown in Figure 3.



Oxygen Forensic® Extractor v.14.3.0.77

Oxygen Forensic® Extractor
Device connected.

Device is connected successfully!

Device information

Model: Meizu M6 (MEIZU M6)
IMEI: 867342030069064
Hardware Revision: N/A
Software Revision: 7.0

Extraction options
Root access is required to create a physical dump.
Choose exploit method.

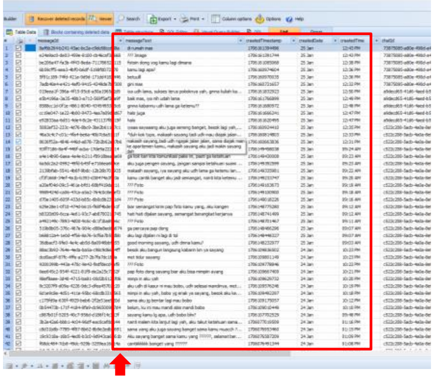
Choose a folder to store extraction
D:\SKRIPSI\Akuisi Oxygen\2024-03-23 14-14-38 867342030069064\

Fig. 3. Smartphone Data Acquisition.

Oxygen successfully performed data acquisition using physical imaging on the M6 and SM-G530H smartphones while Belkasoft, Mobiledit and Magnet Axiom used logical acquisition on the M6 smartphone because the tools did not successfully detect root status. But for SM-G530H using physical imaging.

Examination

Examination is carried out on the acquired data to read the data that has been obtained. At this stage forensic tools are used including Oxygen Forensics, Belkasoft X (Belkasoft Evidence Center X), Mobiledit Forensics, Magnet Axiom, Autopsy, and FTK Imager. Oxygen Forensics succeeded in obtaining data artifacts in the form of text messages, contacts and images on the M6 smartphone, totaling 63 text message artifacts, 9 image artifacts, and 10 contacts and SM-G530H totaling 18 text messages, 7 deleted images stored in the cache and 27 contacts. The results are shown in Figure 4.

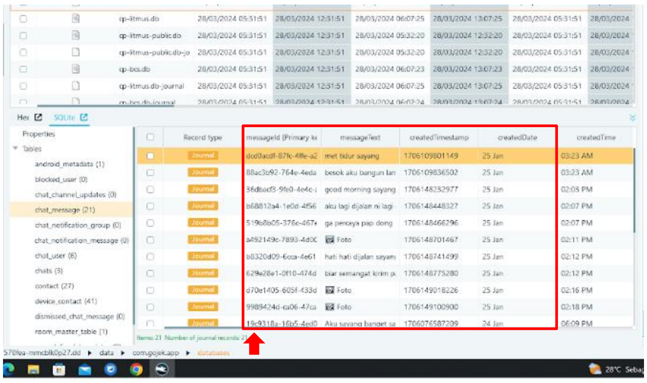


Recover deleted records · Viewer · Search · Export · Print · Column options · Options · Help

#	messageText	createdDate	createdTime
1	di rumah mas	25 Jan	12:43 PM
2	??? Image	25 Jan	12:43 PM
3	fotoin dong yng kamu lagi dimana	25 Jan	12:38 PM
4	kamu lagi apa?	25 Jan	12:36 PM
5	betuull	25 Jan	12:36 PM
6	gini mas	25 Jan	12:32 PM
7	iya udh lama, sukses terus pokoknya yah, gmna kabah ka...	25 Jan	12:50 PM
8	baik mas, iya nih udah lama	25 Jan	12:49 PM
9	gmna kabarnu udh lama ga ketemu??	25 Jan	12:48 PM
10	halo juga	25 Jan	12:47 PM
11	halo	25 Jan	12:47 PM
12	iyaaa sayaaang aku juga seneng banget, besok lagi yah,...	25 Jan	12:35 PM
13	*duh kok tapa, makasih sayang tadi udh mau diajak jalan...	25 Jan	12:33 PM
14	makasih sayang tadi udh ngajak jalan jalan, sama diajak main ke apartemen kamu, makasih sayang aku jadi makin sayang deh	25 Jan	12:31 PM
15	[illegible]	25 Jan	09:24 AM
16	ga kok kan kita komunikasi pake ini, paan ga ketahuan	25 Jan	09:23 AM
17	aku juga pengen sayang, jangan sampai ketahuan suami ...	25 Jan	09:23 AM
18	makasih sayang, iya sayang aku udh lama ga ketemu lan...	25 Jan	09:22 AM
19	kamu cantik banget aku jadi semangat, nanti kita ketemu ...	25 Jan	09:20 AM
20	??? Foto	25 Jan	09:19 AM
21	??? Foto	25 Jan	09:18 AM
22	??? Foto	25 Jan	09:16 AM
23	biar semangat kirim pap foto kamu yang, aku kangen	25 Jan	09:12 AM
24	hati hati dijalan sayang, semangat berangkat kerjanya	25 Jan	09:12 AM
25	??? Foto	25 Jan	09:11 AM
26	ga percaya pap dong	25 Jan	09:07 AM
27	aku lagi dijalan ni lagi di tol	25 Jan	09:07 AM
28	good morning sayang, udh dena kamu?	25 Jan	09:03 AM
29	besok aku bangun langsung kabarin kn ya sayang	24 Jan	10:23 PM
30	met tidur sayang	24 Jan	10:23 PM
31	??? Foto	24 Jan	10:22 PM
32	pap foto dong sayang biar aku bisa mimpiin ayang	24 Jan	10:21 PM
33	mimpi in aku yah	24 Jan	10:20 PM
34	aku udh di kasur ni mau bobo, udh selesai mandinya, met...	24 Jan	10:19 PM
35	mimpi in aku yah, bobo yg enak ya sayang, besok aku ka...	24 Jan	10:18 PM
36	sama aku jg bentar lagi mau bobo	24 Jan	10:12 PM
37	belum, ku ini mau mandi abis mandi bobo	24 Jan	10:10 PM
38	sayang kamu lg apa, udh bobo blm?	24 Jan	09:48 PM
39	nanti malem kita lanjut lagi yah, aku takut ketahuan sama...	24 Jan	01:16 PM
40	sama yang aku juga sayang banget sama kamu muacch ?...	24 Jan	01:15 PM
41	Aku sayang banget sama kamu yang ??????, selamat ber...	24 Jan	01:09 PM
42	cantiiiiiik banget yang ??????	24 Jan	01:08 PM

Fig. 4. Result Examination Oxygen.

Belkasoft on the M6 smartphone found artifacts including images and contacts sent to the Gojek application, the number of image artifacts found was 9 images. While the SM-G530H smartphone managed to get data artifacts in the form of text messages, contacts and images, totaling 21 conversations, 27 contacts and 13 image caches. The results are shown in Figure 5 below.



□	cp-litmus.db	28/03/2024 05:31:51	28/03/2024 12:31:51	28/03/2024 06:07:25	28/03/2024 13:07:25	28/03/2024 05:31:51	28/03/2024
□	cp-litmus-public.db	28/03/2024 05:31:51	28/03/2024 12:31:51	28/03/2024 05:32:20	28/03/2024 12:32:20	28/03/2024 05:31:51	28/03/2024
□	cp-litmus-public.db-jo	28/03/2024 05:31:51	28/03/2024 12:31:51	28/03/2024 05:32:20	28/03/2024 12:32:20	28/03/2024 05:31:51	28/03/2024
□	cp-bcs.db	28/03/2024 05:31:51	28/03/2024 12:31:51	28/03/2024 06:07:23	28/03/2024 13:07:23	28/03/2024 05:31:51	28/03/2024
□	cp-litmus.db-journal	28/03/2024 05:31:51	28/03/2024 12:31:51	28/03/2024 06:07:25	28/03/2024 13:07:25	28/03/2024 05:31:51	28/03/2024
□	cp-bcs.db-journal	28/03/2024 05:31:51	28/03/2024 12:31:51	28/03/2024 06:07:24	28/03/2024 13:07:24	28/03/2024 05:31:51	28/03/2024

Hex SQLite

Properties
Tables
- android_metadata (1)
- blocked_user (0)
- chat_channel_updates (0)
- chat_message (21)
- chat_notification_group (0)
- chat_notification_message (0)
- chat_user (6)
- chats (3)
- contact (27)
- device_contact (41)
- dismissed_chat_message (0)
- room_master_table (1)

□	Record type	messageId (Primary k	messageText	createdTimestamp	createdDate	createdTime
□	Journal	dcd0acdf-87fc-4ffe-a2	met tidur sayang	1706109801149	25 Jan	03:23 AM
□	Journal	88ac3b92-764e-4eda	besok aku bangun lan	1706109836502	25 Jan	03:23 AM
□	Journal	36dbacf3-9fe0-4e4c-a	good morning sayang	1706148232977	25 Jan	02:03 PM
□	Journal	b68812a4-1e0d-4f56	aku lagi dijalan ni lagi	1706148448327	25 Jan	02:07 PM
□	Journal	519b8b05-376c-467e	ga percaya pap dong	1706148466296	25 Jan	02:07 PM
□	Journal	a492149c-7893-4d0C	🖼 Foto	1706148701467	25 Jan	02:11 PM
□	Journal	b8320d09-6cca-4e61	hati hati dijalan sayan	1706148741499	25 Jan	02:12 PM
□	Journal	629e28e1-0f10-474d	biar semangat krim p	1706148775280	25 Jan	02:12 PM
□	Journal	d70e1405-605f-433d	🖼 Foto	1706149018226	25 Jan	02:16 PM
□	Journal	9989424d-ca06-47ca	🖼 Foto	1706149100900	25 Jan	02:18 PM
□	Journal	19c9318a-16b5-4ed0	Aku sayang banget sa	1706076587209	24 Jan	06:09 PM

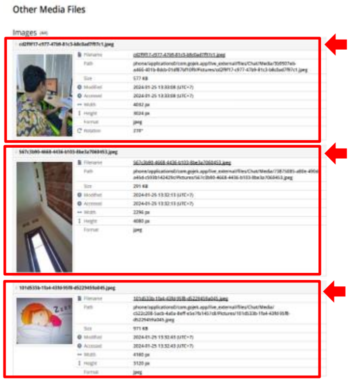
Items: 21 Number of journal records: 21

570fea-mmcblk0p27.dd ▸ data ▸ com.gojek.app ▸ databases

28°C Seba

Fig. 5. Result Examination Belkasoft.

Mobiledit on the M6 smartphone found image and contact artifacts, namely 9 images. On the SM-G530H smartphone, artifacts in the form of text messages, images and contacts were found, totaling 7 images, 13 conversations, and contact data totaling 44 contacts. The results are shown in Figure 6.



Other Media Files

Images (44)

cd2f9f17-c977-47b9-81c3-b8c0ad7f97c1.jpeg

Filename	cd2f9f17-c977-47b9-81c3-b8c0ad7f97c1.jpeg
Path	phone/applications0/com.gojek.app/live_external/files/Chat/Media/5fd507eb-a466-401b-8deb-01df87bf10f6/Pictures/cd2f9f17-c977-47b9-81c3-b8c0ad7f97c1.jpeg
Size	577 KB
Modified	2024-01-25 13:33:08 (UTC+7)
Accessed	2024-01-25 13:33:08 (UTC+7)
Width	4032 px
Height	3024 px
Format	jpeg
Rotation	270°

567c3b90-4668-4436-b103-8be3a7068453.jpeg

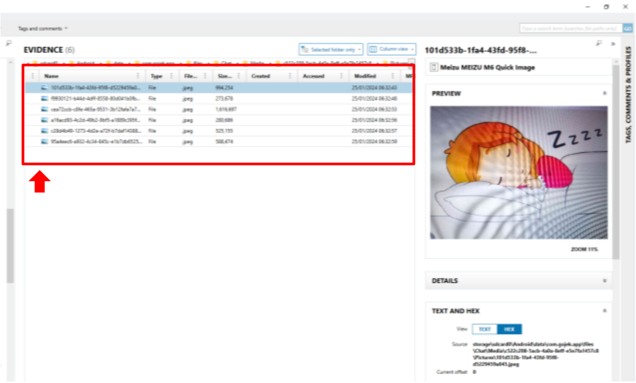
Filename	567c3b90-4668-4436-b103-8be3a7068453.jpeg
Path	phone/applications0/com.gojek.app/live_external/files/Chat/Media/73875085-a80e-490d-a45d-c593b142429c/Pictures/567c3b90-4668-4436-b103-8be3a7068453.jpeg
Size	291 KB
Modified	2024-01-25 13:32:13 (UTC+7)
Accessed	2024-01-25 13:32:13 (UTC+7)
Width	2296 px
Height	4080 px
Format	jpeg

101d533b-1fa4-43fd-95f8-d5229458a045.jpeg

Filename	101d533b-1fa4-43fd-95f8-d5229458a045.jpeg
Path	phone/applications0/com.gojek.app/live_external/files/Chat/Media/c522c208-5acb-4a0a-8eff-e5e7fa1457c8/Pictures/101d533b-1fa4-43fd-95f8-d5229458a045.jpeg
Size	971 KB
Modified	2024-01-25 13:32:43 (UTC+7)
Accessed	2024-01-25 13:32:43 (UTC+7)
Width	4160 px
Height	3120 px
Format	jpeg

Fig. 6. Result Examination Mobiledit.

The examination results on the M6 smartphone using Magnet Axiom managed to get image artifacts and contacts, namely 9 images. On the SM-G530H smartphone, artifacts of text messages, image caches, deletion traces and contacts were found, totaling 10 text messages, 6 traces, and 7 images. The examination results can be seen in Figure 7.



Name	Type	File...	Size...	Created	Accessed	Modified
101d533b-1fa4-43fd-95f8-d5229459a0...	File	.jpeg	994,254			25/01/2024 06:32:43
f9930121-b44d-4df9-8558-80d041b0fb...	File	.jpeg	273,678			25/01/2024 06:32:48
cea72ccb-c8fe-465a-9531-3b12fafa7a7...	File	.jpeg	1,616,697			25/01/2024 06:32:53
a1facd93-4c2d-49b2-9bf5-a1889c3956...	File	.jpeg	280,689			25/01/2024 06:32:56
c28d4b49-1273-4d2a-a72f-b7daf14088...	File	.jpeg	525,155			25/01/2024 06:32:57
f95a4eec6-a832-4c34-845c-e1b7db6525...	File	.jpeg	588,474			25/01/2024 06:32:59

Source storage\sdcard0\Android\data\com.gojek.app\files\Chat\Media\c522c208-5acb-4a0a-8eff-e5e7fa1457c8\Pictures\101d533b-1fa4-43fd-95f8-d5229459a845.jpeg
Current offset 0

Fig. 7. Result Examination Magnet Axiom.

The examination results using Autopsy on the acquisition results from Oxygen Forensics, Belkasoft, Mobiledit, and Magnet Axiom successfully obtained artifacts similar to the original tools. However, there is a difference in the number of artifacts found. Autopsy managed to obtain artifacts of 63 text messages, 9 images and 10 contacts on the M6 smartphone and 11 text messages, 9 image traces, and 41 contacts from the SM-G530H smartphone acquired by Oxygen Forensics. Successfully obtained 9 image artifacts from the M6 smartphone acquired by Belkasoft, Mobiledit, and Magnet Axiom. Obtained 11 text messages, 8 images and 41 contacts from SM-G530H smartphone acquired by Belkasoft, 13 text messages, 8 images and 41 contacts from Mobiledit, and 10 text messages, 8 images and 41 contacts from Magnet Axiom. The results can be seen in Figure 8.

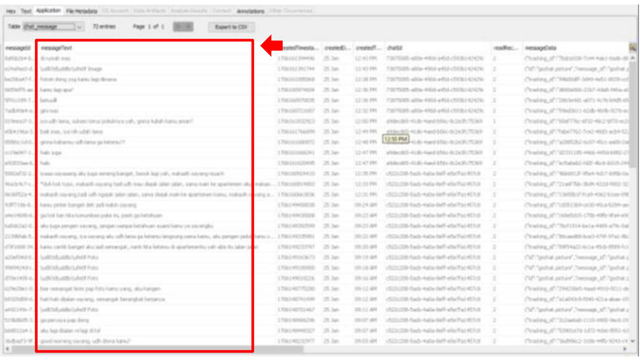
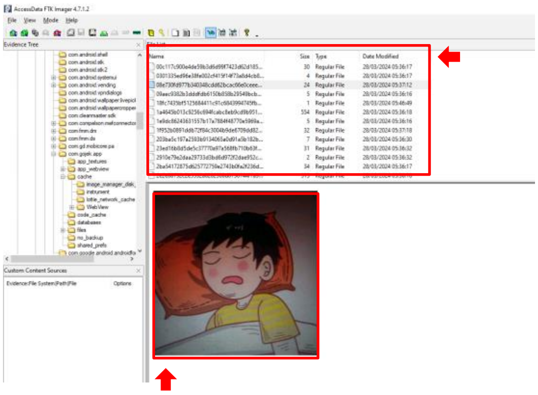


Fig. 8. Result Examination Autopsy.

The examination using FTK Imager of the acquisitions from Oxygen Forensics, Belkasoft and Magnet Axiom resulted in artifacts similar to the original tools. However, there is a difference in the number of artifacts found. FTK Imager managed to obtain 63 text messages, 9 images and 10 contacts on the M6 smartphone and 9 text messages, 7 images and 44 contacts on the SM-G530H smartphone from the Oxygen Forensics acquisition. Successfully obtained 9 images from the M6 smartphone from the acquisition of Belkasoft, Mobiledit and Magnet Axiom and 11 text messages, 7 images and 44 contacts on the SM-G530H smartphone from the acquisition of Belkasoft and Magnet Axiom. As well as getting 10 text messages, 7 pictures and 44 contacts on the SM-G530H smartphone as a result of Mobiledit acquisition. The results can be seen in Figure 9.



Name	Size	Type	Date Modified
00c117c900e4de59b3d6d99f7423d62d185...	30	Regular File	28/03/2024 05:36:17
0301335ed96e38fe002cf415f14f73a8d4cb8...	4	Regular File	28/03/2024 05:36:17
08e730fd977b340348cdd62bcac66e0ceee...	24	Regular File	28/03/2024 05:37:12
09aec9382b3dddfdb6150b858b29540bcb...	5	Regular File	28/03/2024 05:36:16
18fc7435bf5125684411c91c6843994745fb...	1	Regular File	28/03/2024 05:46:49
1a4645b013c9256c694fcabc8eb9cd9b951...	554	Regular File	28/03/2024 05:36:18
1a9dc86243631557b17a7884f48770e5969a...	5	Regular File	28/03/2024 05:36:16
1f952b0891ddb72f84c3004b9de6709dd82...	32	Regular File	28/03/2024 05:37:18
203ba5c197a2593b9134065a0d91a5b182b...	7	Regular File	28/03/2024 05:36:30
23ed16b8d5de5c37770a97a568fb710b63f...	31	Regular File	28/03/2024 05:36:32
2910e79e2daa29733d3bd6d972f2dae952c...	2	Regular File	28/03/2024 05:36:32
2ba54172875d625772756e2743b0fa2f236d...	34	Regular File	28/03/2024 05:36:17

Fig. 9. Result Examination FTK Imager.

Analysis

Oxygen managed to get 9 image files, 63 text messages, and 10 contacts and 18 text messages, 7 deleted images stored in the cache and 27 contacts. However, the evidence relevant to the case scenario from the findings on the M6 smartphone is 37 text messages, 6 images and found the perpetrator number A. While on the SM-G530H smartphone is 18 text messages and 6 images and found the perpetrator number B. The findings obtained are in accordance with the scenario that has been applied.

Belkasoft, and Magnet Axiom in the previous stage managed to get 9 images on the M6 smartphone. However, the digital evidence relevant to the scenario is 6 images. On the SM-G530H smartphone using Belkasoft managed to get 21 text messages, 13 images and 41 contacts. However, the relevant ones are 21 text messages, 6 images, and found contacts belonging to perpetrator B. While using Magnet Axiom managed to get 10 text messages, 7 images and 41 contacts. However, the relevant ones are 10 text messages, 6 images and found contacts belonging to perpetrator B.

In the previous stage, Mobiledit managed to get 9 images from the M6 smartphone and on the SM-G530H smartphone 13 text messages, 7 images and 41 contacts. However, the relevant digital evidence of artifact findings from the M6 smartphone is 6 images. while the relevant digital evidence from the SM-G530H smartphone is 13 text messages, 6 images and the finding of contacts belonging to the perpetrator B. The overall analysis results can be seen in Appendix 1 in the appendix.

Tools Comparison

A comparison of tools used in uncovering digital evidence is carried out to produce recommendations for mobile digital forensic tools. Tool recommendations are determined based on the acquisition of artifacts. The results of the comparison of tools used in uncovering digital evidence on the first and second smartphones can be seen in Table 3. Calculation of the percentage of digital evidence artifacts is done using the following formula can be seen in Equation 1 and the overall percentage formula can be seen in Equation 2.

$$PA = \frac{\mathrm{T}}{\mathrm{K}} \text{ x } 100\% \qquad (1)$$

Description:
PA = Percentage of Digital Evidence Artifacts
T = Artifact Findings

K = Grand Total of Artifacts in the Scenario

$$KP = \frac{(PP + PG + PK)}{3} \quad (2)$$

Description:
KP = Overall Percentage
PP = Percentage of text messages
PG = Image percentage
PK = Contact percentage

Table 3. Forensic Tools Performance Comparison Table.

No	*Tools*	Percentage of Total Performance M6 Smartphone Artifact Findings	Percentage of Total Performance SM-G530H Smartphone Artifact Findings
1	Oxygen Forensik	100%	86%
2	Belkasoft	33%	89%
3	Mobiledit	33%	80%
4	Magnet	33%	77%
5	Autopsy (Oxygen)	100%	78%
6	Autopsy (Belkasoft)	33%	78%
7	Autopsy (Mobiledit)	33%	80%
8	Autopsy (Magnet)	33%	77%
9	FTK Imager (Oxygen)	100%	76%
10	FTK Imager (Belkasoft)	33%	78%
11	FTK Imager (Mobiledit)	33%	77%
12	FTK Imager (Magnet)	33%	78%

Based on the overall data comparison of tools performance on smartphones M6 and SM-G530H. It is concluded that the forensic tool whose performance is very good as evidenced by consistency in all conditions is Oxygen Forensics which managed to get 100% artifacts on the M6 Smartphone and 86% artifacts on the SM-G530H smartphone. So that the optimal tools recommendation based on this is Oxygen Forensics version 12.

Validation

Validation is needed to check whether the results of the digital forensic process that have been obtained are correct, accurate, credible, and maintain data integrity so that they can be recognized in the eyes of the law. The validation process includes aspects of repeatability, reproducibility and hashing. Based on Table 2, the artifacts that have been found meet the validation aspects of repeatability, reproducibility in accordance with ISO / IEC 27037: 2012 [20].

The conversation database hashing process is carried out by comparing the results of the database findings on the SM-G530H smartphone to validate the findings of the conversation messages in the form of text that have been successfully obtained. The results of the comparison of the hash value of the conversation database artifacts that have been carried out by anti-forensics produce the same hash value, so that the conversation message artifacts in the form of text that have been found on the SM-G530H smartphone in the conversation-database file are valid. The results can be seen in Table 4.

Table 4. Hashing Comparison Table.

Nilai *Hashing* CRC32			
No	***Hash Value***	***Tools***	**Validation**
1	145d223a(*database*)	Oxygen Forensik	✓
2	145d223a(*database*)	Belkasoft	✓
3	145d223a(*database*)	Mobiledit	✓
4	145d223a(*database*)	Magnet Axiom	✓

CONCLUSIONS

The process of implementing mobile digital forensics adopting the NIJ method was successfully carried out by obtaining digital evidence on the M6 smartphone, namely text messages, images and contacts but not all tools got text message artifacts, only Oxygen Forensics managed to get these artifacts and for the second smartphone, the SM-G530H, which has been carried out anti-forensics, managed to get evidence of recovery of text messages, contacts, and image caches.

The results of the comparison of the tools obtained resulted in a recommendation on the Oxygen Forensics version 12 tool. Oxygen managed to carry out the forensic process equally well on the M6 and SM-G530H smartphones. The M6 smartphone managed to get a total of 100% artifacts, namely getting 63 text messages in text form, 9 images and 10 contacts. Meanwhile, the SM-G530H smartphone received a total of 86% artifacts, namely 87 text messages in the form of text, 7 images and 41 contacts.

REFERENCES

[1] R. Azhar Ramdhani, M. Nafis Rojabi, M. Chusni Mubarok, and D. Azman Refah Fuadi, "APLIKASI GOJEK SEBAGAI MEDIA PENINGKATAN INTERASI INTRA DAN ANTAR MASYARAKAT," *Jurnal Scholary Jurnal Of Elementary School*, vol. 3, 2023.

[2] S. Mirfandaresky, A. Kaimuddin, and P. P. Paramita, "DIGITAL FORENSIK DALAM PENYIDIKAN TINDAK PIDANA PENIPUAN ONLINE (Studi Kasus di Wilayah Hukum Kepolisian Resor Ponorogo)," 2022.

[3] R. A. Cahyadri, *Apa Yang Harus Ditanyakan Kepada Ahli Digital Forensics?(Panduan Bagi Praktisi Hukum)*. Sleman: Penerbit Deepublish (Grup Penerbitan CV Budi Utama, 2021.

[4] I. Anshori, K. E. Setya Putri, and U. Ghoni, "Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ," *IT Journal Research and Development*, vol. 5, no. 2, pp. 118–134, Aug. 2020, doi: 10.25299/itjrd.2021.vol5(2).4664.

[5] N. Saputri and R. Indrayani, "ANALISIS DATA FORENSIK INVESTIGASI KASUS PEREDARAN NARKOBA PADA SMARTPHONE BERBASIS ANDROID," 2022.

[6] K. D. O. Mahendra and I. K. A. Mogi, "Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases," 2021.

[7] I. G. R. Mailangkay, E. Zakharia, and A. Hadi, "Komparasi Analisis Bukti Digital Tiktok Lite Menggunakan Metode National Institute of Justice," 2022.

[8] F. F. Febrian and J. Sidabutar, "Comparative Analysis of Forensic for Whatsapp Desktop on Mac OS and Windows Using IDFIF V2," *IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, 2023.

[9] R. Muzdalifa Abubakar, M. Sabri Ahmad, S. N. Kapita, and A. Fuad, "Implementation Framework National Institute of Standards and Technology (Nist) Evidence Digital In The Forensic Process Social Media," 2023. [Online]. Available: www.techniumscience.com

[10] A. G. Prayogo and I. Riadi, "Digital Forensic Signal Instant Messages Services in Case of Cyberbullying using Digital Forensic Research Workshop Method," 2022.

[11] M. Iqbal and B. Soewito, "Digital Forensics on Solid State Drive (SSD) with TRIM Feature Enabled and Deep Freeze Configuration Using Static Forensic Methods and ACPO Framework", doi: 10.5281/zenodo.4428140.

[12] N. Hamad and M. Jazzar, "An Improved GCFIM Framework for Analyzing Digital Evidence Steganography," 2024. [Online]. Available: www.ijeais.org/ijeais

[13] Sunardi, Herman, and S. R. Ardiningtias, "A Comparative Analysis of Digital Forensic Investigation Tools on Facebook Messenger Applications," *Journal of Cyber Security and Mobility*, vol. 11, no. 5, pp. 655–672, 2022, doi: 10.13052/jcsm2245-1439.1151.

[14] Sunardi, I. Riadi, and J. Triyanto, "Analisis Forensik Layanan Signal Private Messenger pada Smartwatch Menggunakan Metode National Institute of Justice," *Jurnal Edukasi dan Penelitian Informatika*, 2021.

[15] S. Mohammad and R. Sudesh, "DIGITAL FORENSIC MODELS: A COMPARATIVE ANALYSIS," 2018. [Online]. Available: http://www.ijmra.us,

[16] K. Mushtaque, "Digital Forensic Investigation Models, an Evolution study," *Journal of Information Systems and Technology Management*, vol. 12, no. 2, May 2015, doi: 10.4301/s1807-17752015000200003.

[17] Sunardi, I. Riadi, and J. Triyanto, "Forensics Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice," *Journal of Information Technology and Computer Science*, vol. 3, no. 1, pp. 63–70, 2021.

[18] F. M. Kaffah, S. Nur, A. Fitrianto, and U. Syaripudin, "ANALISIS LIVE FORENSICS PADA SSD SATA FUNGSI TRIM MENGGUNAKAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ) TEKNOLOGI NUSANTARA," *Jurnal Penelitian Fakultas Teknik UNINUS*, vol. 4, no. 2, 2022, [Online]. Available: http://ojs.uninus.ac.id/index.php/teknologinusantara

[19] I. Riadi and B. F. Muthohirin, *Forensik Email*. Depok Sleman: Diandra Kreatif (Kelompo Penerbit Diandra), 2022.

[20] BSN, *Teknologi Informasi - Teknik keamanan - Pedoman identifikasi, pengumpulan, akuisisi dan preservasi bukti digital (ISO/IEC 27037:2012, IDT)*. 2014.

AUTHORS BIBLIOGRAPHY

Suprayogi Budhi Purwanto was born in Yogyakarta, on February 19, 2001, currently pursuing a Bachelor of Informatics degree at Ahmad Dahlan University Yogyakarta. Research fields related to digital forensics. Email: Suprayogi1900018049@webmail.uad.ac.id.

Guntur Maulana Zamroni obtained a Bachelor of computer science (B.Sc.), S1 Informatics Study Program Staffordshire University UK, graduated in 2012. Obtained a Master of Computer (M.Kom) degree, Ahmad Dahlan University Informatics Postgraduate Program, graduated in 2018. Currently a Lecturer at Ahmad Dahlan University Yogyakarta in the S1 Informatics Study Program. Research fields related to Mobile Forensic, Software Engineering. Email: guntur.zamroni@tif.uad.ac.id.

Appendix

Appendix 1. Analysis Result.

No	Tools	Acquisition	Text message	Image	Contact	Compatibility		
						Text message	Image	Contact
1	Oxygen (M6)	1	63	9	10	63	6	1
2	Oxygen (M6)	2	63	9	10	63	6	1
3	Oxygen(SM-G530H)	1	18	7	41	18	6	1
4	Oxygen(SM-G530H)	2	18	7	41	18	6	1
5	Belka(M6)	1	-	9	-	-	6	-
6	Belka(M6)	2	-	9	-	-	6	-
7	Belka (SM-G530H)	1	21	13	41	21	6	1
8	Belka (SM-G530H)	2	21	13	41	21	6	1
9	Mobiledit(M6)	1	-	9	-	-	6	-
10	Mobiledit(M6)	2	-	9	-	-	6	-
11	Mobiledit (SM-G530H)	1	13	7	44	13	6	1
12	Mobiledit (SM-G530H)	2	13	7	44	13	6	1
13	Magnet (M6)	1	-	9	-	-	6	-
14	Magnet (M6)	2	-	9	-	-	6	-
15	Magnet(SM-G530H)	1	10	7	41	10	6	1
16	Magnet(SM-G530H)	2	10	7	41	10	6	1
17	Autopsy (Oxygen M6)	1	63	9	10	63	6	1
18	Autopsy (Oxygen M6)	2	63	9	10	63	6	1
19	Autopsy (Belka M6)	1	-	9	-	-	6	-
20	Autopsy (Belka M6)	2	-	9	-	-	6	-

21	Autopsy (Mobiledit M6)	1	-	9	-	-	6	-
22	Autopsy (Mobiledit M6)	2	-	9	-	-	6	-
23	Autopsy (Belka M6)	1	-	9	-	-	6	-
24	Autopsy (Belka 6)	2	-	9	-	-	6	-
25	FTK Imager (Oxygen M6)	1	63	9	10	63	6	1
26	FTK Imager (Oxygen M6)	2	63	9	10	63	6	1
27	FTK Imager (Belka M6)	1	-	9	-	-	6	-
28	FTK Imager (Belka M6)	2	-	9	-	-	6	-
29	FTK Imager (Mobiledit M6)	1	-	9	-	-	6	-
30	FTK Imager (Mobiledit M6)	2	-	9	-	-	6	-
31	FTK Imager (Magnet M6)	1	-	9	-	-	6	-
32	FTK Imager (Magnet M6)	2	-	9	-	-	6	-
33	Autopsy (Oxygen SM-G530H)	1	11	8	41	18	6	1
34	Autopsy (Oxygen SM-G530H)	2	11	8	41	18	6	1
35	Autopsy (Belkasoft SM-G530H)	1	11	8	41	21	6	1
36	Autopsy (Belkasoft SM-G530H)	2	11	8	41	21	6	1
37	Autopsy (Mobiledit SM-G530H)	1	13	8	41	13	6	1
38	Autopsy (Mobiledit SM-G530H)	2	13	8	41	13	6	1

39	Autopsy (Magnet SM-G530H)	1	10	8	41	10	6	1
40	Autopsy (Magnet SM-G530H)	2	10	8	41	10	6	1
41	FTK Imager (Oxygen SM-G530H)	1	9	7	44	9	6	1
42	FTK Imager (Oxygen SM-G530H)	2	9	7	44	9	6	1
43	FTK Imager (Belkasoft SM-G530H)	1	11	7	44	11	6	1
44	FTK Imager (Belkasoft SM-G530H)	2	11	7	44	11	6	1
45	FTK Imager (Mobiledit SM-G530H)	1	10	7	44	10	6	1
46	FTK Imager (Mobiledit SM-G530H)	2	10	7	44	10	6	1
47	FTK Imager (Magnet SM-G530H)	1	11	7	44	10	6	1