Digital Forensic Signal Instant Messages Services in Case of Cyberbullying using Digital Forensic Research Workshop Method

Aji Gelar Prayogo
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Advances in information technology have a negative impact, including the public can freely act in cybercrimes. One of the popular instant messaging services is Signal Instant Messenger, which can trigger cyber crimes such as cyberbullying, pornography, gambling, fraud, and phishing. Cyberbullying crimes can occur as long as the application used provides features to send text messages, pictures, or videos. This study aims to analyze digital evidence so that it can be identified as a case of cyberbullying on the Signal Instant Messenger application.The investigation process uses one of the methods of the Digital Forensic Research Workshop (DFRWS) framework, with stages including identification, preservation, collection, examination, analysis, and presentation in the digital evidence search process. The digital forensic tools used to collect evidence are MOBILedit Forensic Express Pro, Belkasoft Evidence Center, and SQLite DB Browser. The process of identifying digital evidence uses a repetition of words that contain ridicule or insult to the victim so that the perpetrator is identified as committing cyberbullying.The results of this study are in the form of digital evidence in the form of reports to be analyzed and used to support cyberbullying investigations in court. This study obtained the results that the actions or conversations that led to cyberbullying were as many as 4 people, 2 as victims, and 1 as witness in accordance with the expected research objectives, even though they had not been able to read deleted or accidentally deleted chats.

Keywords

Cyberbullying, Digital Forensic; DFRWS; Signal Messenger; Smartphone

1. INTRODUCTION

The development of technology and information capabilities is growing rapidly, followed by the use of social media to convey messages and information and to obtain actual information. Social media is an online-based media where users can easily participate, share, and interact[1]. Social media is used as a medium for interacting, exchanging information and/or communicating.The increase in social media users makes other users worry about defending themselves from cybercrimes. Every criminal case has been stipulated by law according to the existing case. For example, the case of bullying is included in Article 45 paragraph (1). The article has a different sound, and the determination of the provisions of the article is determined by the MPR.

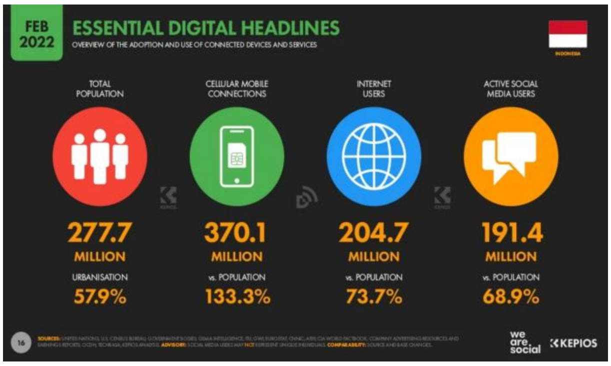


Figure1. Indonesia's State Social Media Usage Data

Figure 1shows statistics on social media users in Indonesia, with a total population of around 277.7 million people, the source of research conducted by we are social and hootsuite with an update in February 2022. Based on statistical data we are social Hootsuite in January 2022, active internet users in Indonesia reached 204.7 billion people, followed by active social media users by as many as 191.4 billion, and then Indonesia's population itself reached 277.1 billion people, an increase of 12.6% compared to the previous year[2]. The increasing number of social media users currently occurs because during the pandemic, activities require to be transferred online. One of the social media applications that attracts users today is Signal Instant Messenger. Signal Instant Messenger has become a popular application in Indonesia and throughout the world because of user concerns about maintaining their privacy and personal information [3].

The development of information technology has both positive and negative impacts. The positive impact of information technology, one of which is being able to communicate with other people through chat directly, even through the internet network[4]. The negative impact of information technology is the existence of crime (cybercrime). Cybercrime is a term that refers to all activities involving computers and/or computer networks as tools, targets, or the occurrence of crimes, including cybercrimes [5]. Technological facilities that include mobile phones, smartphones, and others that can be done through a global electronic network[6]. Cybercrime can take the form of cyberbullying, cyber fraud, cyber human trafficking, cyber extortion, and others that can have fatal consequences, such as suicide or murder.

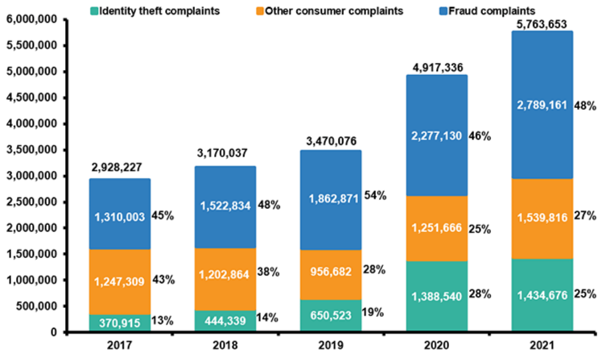


Figure2. Cybercrime Statistics on A Global Scale

Figure 2shows some percentage of cybercrime statistics on a global scale based on a statistical survey from the Insurance Information Institute from 2017 to 2021[7].

Based on data from the Directorate of Cyber Crime (Dittipidsiber), the National Police Criminal Investigation Unit handled 4656 cybercrime cases during the January to November 2020 period[8]. The criminal cases of the 4 thousand are divided into 15 types of crimes. Most cases handled by the police are defamation cases. One of the causes of this case is the use of social media by providing the Signal service feature to send text messages and emojis as an expression of feelings. The high number of bullying cases on social media encourages the investigation of cyberbullying cases through forensic analysis using the Digital Forensic Research Workshop (DFRWS) method.

1.1 Study Literature

1.1.1 *Previously Study*

This research is based on five previous studies that conducted as a reference while comparing the current research with previous research.

The first research conducted by Imam Riadi, Sunardi, and Panggah Widiandana (2020) is a research entitled "Investigating Cyberbullying on Whatsapp Using Digital Forensics Research Workshop". This study was shown to look for evidence on the WhatsApp Messaging application related to cyberbullying by comparing different values from the various results. Digital evidence is disclosed to the suspect with the group feature in the form of text. DFRWS can raise evidence digitally in groups and use the Improved Sqrt-Cosine method. Cosine Similarity is one of the algorithms in text mining that serves to classify a document or text [9].

The second research conducted by Afif Nur Ichsan and Imam Riadi (2021) has a research entitled "Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method". This research is aimed at acquiring and obtaining digital evidence in the IMO chat application and comparing different forensic tools. The increasing number of IM application users on mobile devices has become a source of forensic investigations on mobile [10]. This study uses the Belkasoft Evidence Center forensic tools, MOBILEdit Forensic, and AccessData FTK Imager then compares the acquisition results.

The third research conducted by Imam Riadi, Herman, and Nur hamida Siregar (2021) has a research entitled "Mobile Forensics in Cyber Fraud Cases of Signal Messenger Services Using the NIST Method". Fraud is a crime that uses abusive methods to take valuables from other people[11].This research is shown for the acquisition steps using forensic equipment in accordance with NIST procedures, with a percentage result of 57.14%, and has an inability that is unable to recover lost data.

The fourth research conducted by Imam Riadi, Sunardi, and Panggah Widiandana (2022) has a research entitled "Cyberbullying Detection on Instant Messaging Services Using Rocchio and Digital Forensics Research Workshop Framework". This study uses the Rocchio approach. The Rocchio algorithm is an algorithm to obtain the minimum relevance of feedback in a document so that users ideally get information according to their needs[12].This study aims to examine how to detect cases of cyberbullying with the Digital Forensics Research Workshop (DFRWS) approach.

The fifth research conducted by Galih Fanani, Imam Riadi, and Anton Yudhana (2022) has a research entitled "Forensic Analysis of Michat Applications Using Digital Forensics Research Workshop Methods". This study uses the DFRWS forensic method with various tools as a comparison in the retrieval of data artifacts. Data artifacts can be used as digital evidence [13].The files that successfully retrieved include conversational text files, images, sounds, videos, and web caches. The Oxygen forensic tool has the highest data artifact retrieval capability, with a percentage of 83.3%.

1.1.2 *Digital Evidence*

Digital evidence is information stored or transmitted in binary form that can be used in court. This digital evidence can be found on a computer drive, a cellphone, or other storage device[14].

Figure3 Digital Evidence

Figure 3shows some examples of digital evidence, including: flashdisk, Hard Disk Drive (HDD), handphone, external microSD, Random Access Memory (RAM). A flashdisk is a hardware device that is capable of sending and receiving data from one computer to another offline and requires USB connectivity. A HDD is a computer storage device like the internal storage of a mobile phone that stores sensitive data such as cache.Mobile phones are sophisticated communication devices with facilities that can send and receive various types of information and are able to interact remotely. Mobile phones have data storage in which various sensitive user data, such as passwords or caches, are stored.An external Micro SD is an additional storage medium on cellphones that people usually use to increase storage capacity if the internal storage is not enough. Users sometimes store collections of camera photos that store EXIF datafor digital evidence purposes, such as details of the device used, time, data type, and gps location. RAM is the memory of various processes carried out by the computer able to help the investigation.

1.1.3 Digital Forensic

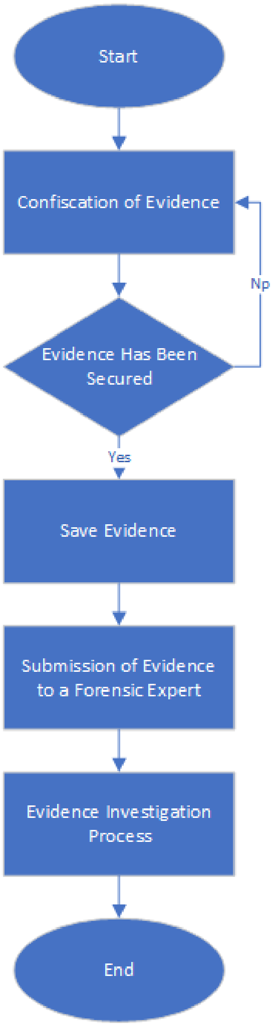

Start
Confiscation of Evidence
Np
Evidence Has Been Secured
Yes
Save Evidence
Submission of Evidence to a Forensic Expert
Evidence Investigation Process
End

Figure4 Forensics Process

Figure4are the stages or forensic processes according to existing investigation procedures.

Forensic is a part of forensic science that covers the discovery and investigation of material (data) found on digital devices (computers, mobile phones, tablets, PDAs, networking devices, storage, and the like)[15].Digital forensics is an investigative method by applying science and technology with the aim of examining and analyzing evidence digitally[16].

1.1.4 Signal Instant Messaging

Signal Instant Messenger, or better known as Signal, is an instant messaging application developed by the Signal Foundation and Signal Messenger LLC. Signal offers advanced end-to-end encryption (an offering of the open source Signal protocol), thus maintaining conversation privacy[17].Users can send messages to each other or through a group conversation.

1.1.5 Cybercrime

Cybercrime is an unlawful act carried out by using a computer network as a means/tool or a computer as an object, either to gain profit or not, to the detriment of other parties[18].Types of cybercrime, including cracking, carding, illegal content, data forgery, and others[19].

1.1.6 Android

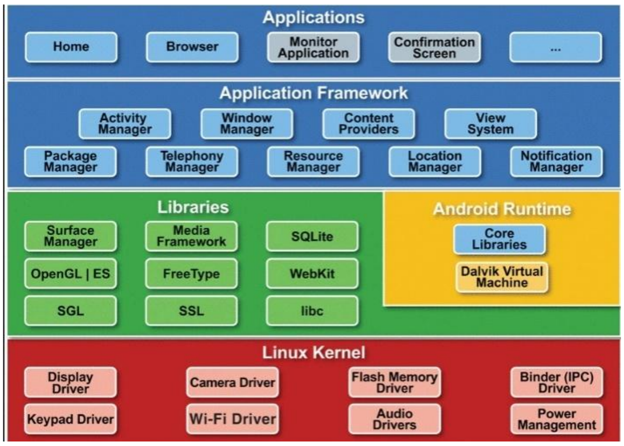


Figure5. Android Components

Figure5shows the Android components consist of the Linux Kernel, Libraries & Runtime, Framework, and Application . Android is a set of software on mobile devices that includes an operating system, middleware, and application lock[20].This study uses the Android operating system, provided that it has been rooted and the Android version is version 5 (Lollipop). Subsequent testing shows that on Android version 6 or above, the data will be well encrypted and not easy to decrypt.

1.1.7 DFRWS

The Digital Forensics Research Workshop (DFRWS) method is one of the methods used in digital forensic analysis to indicate a digital crime[21].The DFRWS method is complex because it incorporates other forensic methods, such as the NIST (National Institute of Standards and Technology) method and the NIJ (National Institute of Justice) method. NIST covers collection, examination, analysis, and reporting. NIJ covers collection, preservation, analysis, and presentation.

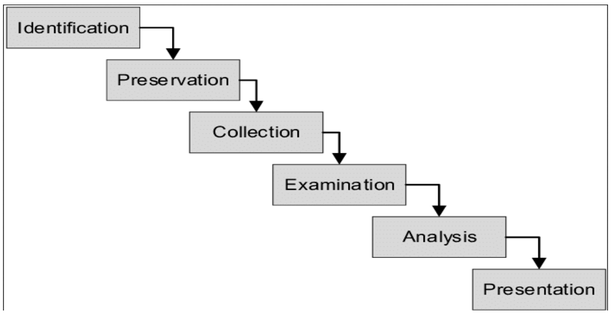


Figure6. DFRWS Forensic Method Stages

The forensic stages in Figure 6 are in accordance with the provisions of the DFRWS, with a total of 6 forensic stages. Other forensic methods may be different.

1.1.7.1 Identification

This process aims to identify and determine what data needs are needed in the investigation and search for digital evidence. Investigators need information in the form of complete details of the cases that occurred so that the analysis process does not save the existing cases.

1.1.7.2 Preservation

This process aims to maintain data to maintain digital evidence, then ensure the authenticity of the evidence and deny claims that the evidence has changed data or there is sabotage.

1.1.7.3 Collection

This data collection process is used to specifically identify digital evidence and identify various data sources.

1.1.7.4 Examination

The stages in which data-containing cases are determined and specific parts of data from various data sources are filtered. This filtering is carried out to check for changes in the data, but changes in the contents of the data are not identified because there is validation of the authenticity of the data.

1.1.7.5 Analysis

The process by which the data was created, by whom the data was created, how the data was created, and why the data was created. Analysis is the core of the forensic process, in which part of the data indicates the case and is presented in the form of a report.

1.1.7.6 Presentation

This process is carried out to display information on the results of the analysis process at the previous stage. This stage is the reporting stage of the analysis results, including the description (scenario) of the suspect actions, an explanation of the tools and methods used, determination of supporting actions taken, and providing recommendations for improvement of policies, methods, tools, or other supporting aspects in the digital forensics action process.

1.1.8 Bullying

Bullying is a deliberate attempt to hurt or humiliate another person[22].The purpose of this bullying is to injure or weaken the victim and is carried out continuously[23].

1.1.9 Cyberbullying

Cyberbullying is the act of sending or posting malicious, violent text or images over the internet (for example, via instant messaging, email, group chat rooms, and social networking).[24].

2. METHODOLOGY

2.1 Research Scenario

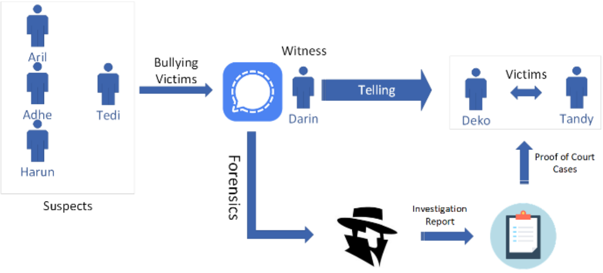


Figure7. Event Scenarios of Cyberbullying

Scenarios at Figure7started with the suspect name is Tedi Mariono was disappointed because Tedi didn't win in the judging results at BKS (Burung Kicau Sakti) in a group chat application called Signal. Then the suspect started an act of insulting his good name followed by disrespectful words in the form of insulting the victim to the two winners, namely Deko Miki Aprilianto and Tandy Sudanto. The first provocateur, Tedi Mariono, caused other people to join in the argument but as other defendants, including Aril Nujianto, Adhe Jariadi, and Harun Perwirantoro.

Meanwhile, Darin Asep, the witness who was in contact with Deko Miki and Tandy Sudanto then showed the conversation in the Signal application. The victims, Deko Miki and Tandy Sudanto, because they felt their good names insulted and polluted, then reported the conversation as evidence, namely from the suspect smartphone, and handed over the conversation to the authorities Investigator on the Signal application for analysis by further investigators so that the defendant could be processed in this case.

Other suspects, namely Aril Nujianto, Adhe Jariadi, and Harun Perwirantoro, became suspects but only questioned by the law, while Tedi Mariono was sanctioned as a provocateur in Harassment of Good Name and Threats of Fighting. The proof that Tedi Mariono is bullying with the criteria of being a provocateur to heat up the victim. The victim did nothing but save the screenshots and report the incident to the police. Darin Asep, as a Witness Explained the incident to the local police along with the two victims, namely Deko Miki and Tandy Sudanto. Tedi Mariono and with other suspects including Aril Nujianto, Adhe Jariadi, and Harun PerwirantoroSanctioned Based on Article 310 of the Criminal Code Regarding Harassment of Good Names and Article 368 Paragraph (1) of the Criminal Code.

2.2 Result and Discussion

The research step is the process by which investigators apply forensics to find evidence according to the procedures that have been applied.There are six stages in the forensic process as shown in Figure 8.

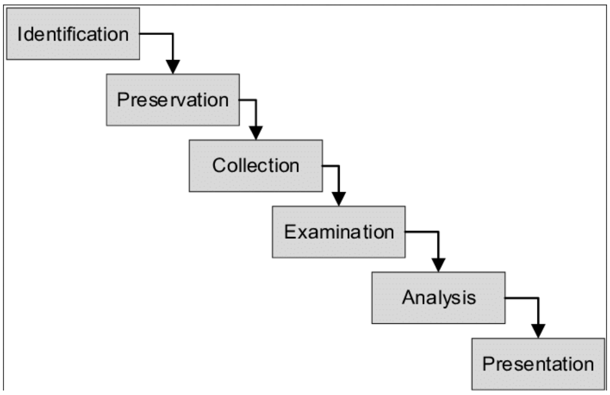


Figure8. Research Step

The Figure 8 is explanation of research step for evidence obtaining and based on DFRWS forensic measures.The following is an explanation of the forensic stages and tables for more complete details

2.2.1 Identification

The identification stage begins with Before the start of the forensic process, the investigator or investigator first identifies or prepares what data is needed that relates to the case under investigation then preparing forensic tools that will be used by the investigators in taking digital evidence. Digital evidence is used by investigators to maintain its integrity and guarantee its authenticity. Some of the software and hardware needed by investigators during the process of searching for digital evidence can be seen in Table 1

Table 1Forensic Equipment Investigators Need

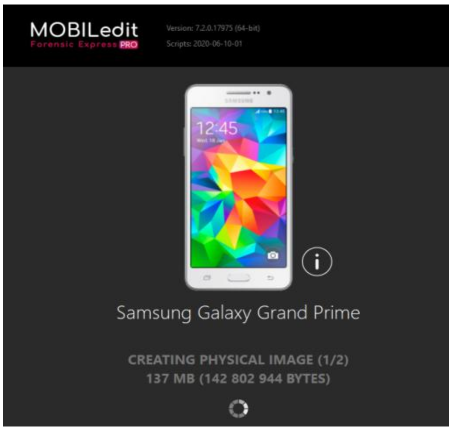
Equipment and materials	Description	Category
Laptop	Lenovo I 320 14AST, AMD A9-9420, AMD R3 M430, Windows 10 Pro	Hardware
Smartphone	Samsung Galaxy Grand Prime, Rooted condition, OS Android, V.5.1.1 (Lollipop)	Hardware
MOBILedit Forensic Express Pro	Tools forensic	Software
Belkasoft Evidence Center	Tools forensic	Software
DB Browser SQLite	Tools forensic	Software
Signal Instant Messenger	Instant messages application target (Version 5.38.5)	Software

Table 1 shows the various forensic tools and equipment needed to assist in the process of investigating digital evidence.

The data in table 1 shows that software is mostly used to help analyze the digital evidence retrieval process. Meanwhile, hardware is used for media against investigators in obtaining digital evidence.

2.2.2 Preservation

Preservation, or the maintenance process, starts with a smartphone (Samsung) already rooted so that it can be fully accessed by investigators. The next step is to create an image file on a rooted smartphone for analysis and verify its authenticity. The image files are stored and quarantined to prevent third parties from accessing or modifying the data.



MOBILedit Forensic Express PRO

Version: 7.2.0.17975 (64-bit)

Scripts: 2020-06-10-01

Samsung Galaxy Grand Prime

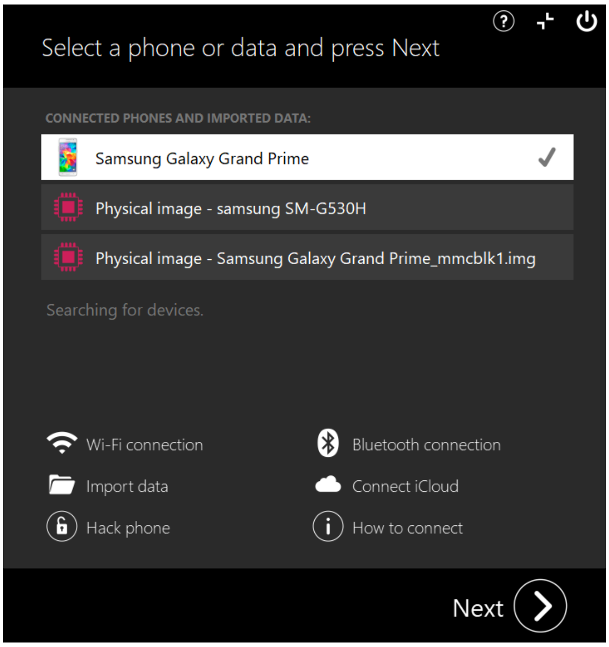
CREATING PHYSICAL IMAGE (1/2)
137 MB (142 802 944 BYTES)

Figure9.Imaging Process Using MOBILEdit Forensic

Figure9shows the imaging process so that the imaging results file is used as a reference if the data that has been acquired at the next forensic stage does not change during the hash validation process. The imaging provisions are that the first file is the internal storage of the smartphone, followed by the second file, which is the extSDCard or external memory of the smartphone.This image file can be accessed by a computer and various data can be browsed from the entire internal storage of the smartphone or just copy folder of Signal app which location at /data/data/com.thoughtcrimes.securesms/.

2.2.3 Collection

The collection stage is the stage of the acquisition process and validates the data on the suspect smartphone to obtain evidence as well as validate the authenticity of the evidence that has been collected. This collection stage needs to be considered regarding the data taken because during the acquisition process there is a risk of corrupt (problematic) data, such as the state of the computer suddenly turning blue during the collection process. The process of data collection, obtained through extraction from a smartphone, is shown in the image with the help of the MOBILedit Forensic application for collecting evidence. At this stage, it is determined which evidence is needed to determine whether the evidence is in accordance with the case study or not.This collection stage generates various data from the target application, complete with reports as well as imaging data files from both target smartphone storages.The first collection stage is retrieving imaging data files on both storage devices and ensuring the imaging file size matches the storage capacity followed next step is aqcuisition.



Select a phone or data and press Next

CONNECTED PHONES AND IMPORTED DATA:

Samsung Galaxy Grand Prime ✓

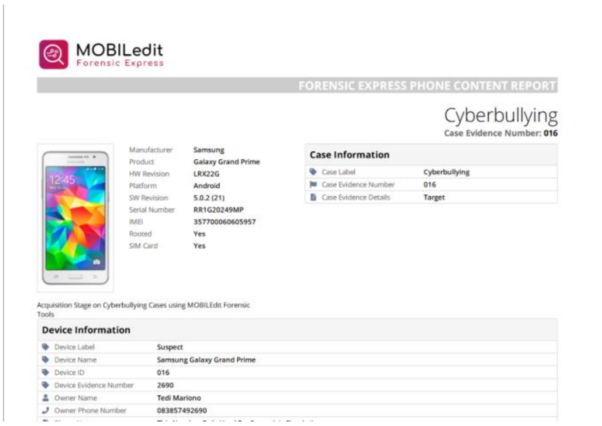
Physical image - samsung SM-G530H

Physical image - Samsung Galaxy Grand Prime_mmcblk1.img

Searching for devices.

Figure10.Imaging Results of MOBILEdit Forensic

Figure10shows imaging results that can be used to explore various data before filtering.Imaging process generates data files in IMG format. IMG file can easily be browsed includes the internal storage of the perpetrator's smartphone and IMG file can be saved by investigators for forensic application at the prevention stage, which can later be known if there is a change in data before and after acquisition.Then, the investigator compares the acquisition results between the results of the imaging process and the direct acquisition process by the perpetrator's smartphone.



MOBILedit Forensic Express

FORENSIC EXPRESS PHONE CONTENT REPORT

Cyberbullying
Case Evidence Number: 016

Manufacturer	Samsung
Product	Galaxy Grand Prime
HW Revision	LRX22G
Platform	Android
SW Revision	5.0.2 (21)
Serial Number	RR1G20249MP
IMEI	357700060605957
Rooted	Yes
SIM Card	Yes

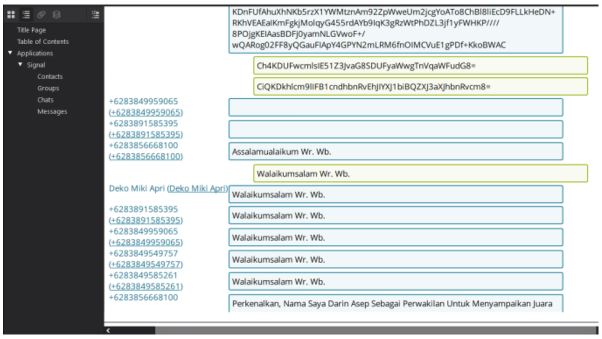
Case Information	
Case Label	Cyberbullying
Case Evidence Number	016
Case Evidence Details	Target

Acquisition Stage on Cyberbullying Cases using MOBILEdit Forensic Tools

Device Information	
Device Label	Suspect
Device Name	Samsung Galaxy Grand Prime
Device ID	016
Device Evidence Number	2690
Owner Name	Tedi Mariono
Owner Phone Number	083857492690

Figure 11.The Result of the Acquisition Report From MOBILEdit Forensic Tools

Figure 11 shows the results of the acquisition of MOBILEdit Forensic tools with a description, namely the details of the smartphone used by the suspect.This report only shows the main interface of the reports that have been successfully created by MOBILEdit Forensic.



KDnFUfAhuXhNKb5rzX1YWMtznAm92ZpWweUm2jcgYoATo8ChBl8liEcD9FLLkHeDN+RKhVEAEaIKmFgkjMolqyG455rdAYb9IqK3gRzWtPhDZL3jf1yFWHKP////8POjgKEIAasBDFj0yamNLGVwoF+/wQARog02FF8yQGauFIApY4GPYN2mLRM6fnOIMCVuE1gPDf+KkoBWAC

Ch4KDUFwcmlsIE51Z3JvaG8SDUFyaWwgTnVqaWFudG8=

CiQKDkhlcm9lIFB1cndhbnRvEhJlYXJ1biBQZXJ3aXJhbnRvcm8=

+6283849959065 (+6283849959065)

+6283891585395 (+6283891585395)

+6283856668100 (+6283856668100)
Assalamualaikum Wr. Wb.

Walaikumsalam Wr. Wb.

Deko Miki Apri (Deko Miki Apri)
Walaikumsalam Wr. Wb.

+6283891585395 (+6283891585395)
Walaikumsalam Wr. Wb.

+6283849959065 (+6283849959065)
Walaikumsalam Wr. Wb.

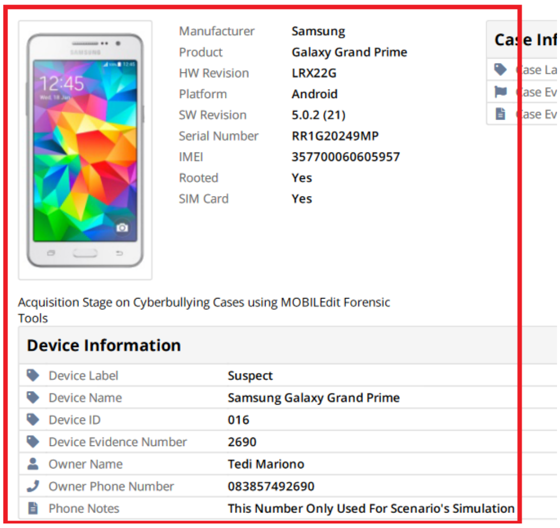
+6283849549757 (+6283849549757)
Walaikumsalam Wr. Wb.

+6283849585261 (+6283849585261)
Walaikumsalam Wr. Wb.

+6283856668100
Perkenalkan, Nama Saya Darin Asep Sebagai Perwakilan Untuk Menyampaikan Juara

Figure 12.Other Acquisition Reportson Conversations using MOBILEdit Forensic Tools.

Figure 12 shows the MOBILEdit Forensic report in the form of conversations carried out by various users who were successfully acquired.



Manufacturer	Samsung
Product	Galaxy Grand Prime
HW Revision	LRX22G
Platform	Android
SW Revision	5.0.2 (21)
Serial Number	RR1G20249MP
IMEI	357700060605957
Rooted	Yes
SIM Card	Yes

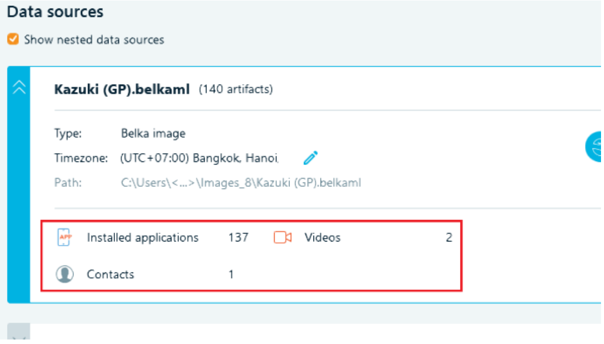
Case Inf
ase La
ase Ev
ase Ev

Acquisition Stage on Cyberbullying Cases using MOBILEdit Forensic Tools

Device Information	
Device Label	Suspect
Device Name	Samsung Galaxy Grand Prime
Device ID	016
Device Evidence Number	2690
Owner Name	Tedi Mariono
Owner Phone Number	083857492690
Phone Notes	This Number Only Used For Scenario's Simulation

Figure13.Details of the Suspect Tedi Mariono

Figure 13 shows the acquisition results of suspect by Tedi Mariono. The red color indicates that the details of the suspect especially on Tedi Mariono smartphone, such as the smartphone used, imei, phone number, and other details of the suspect.



Data sources
☑ Show nested data sources

Kazuki (GP).belkaml (140 artifacts)

Type: Belka image
Timezone: (UTC+07:00) Bangkok, Hanoi
Path: C:\Users\<...>\Images_8\Kazuki (GP).belkaml

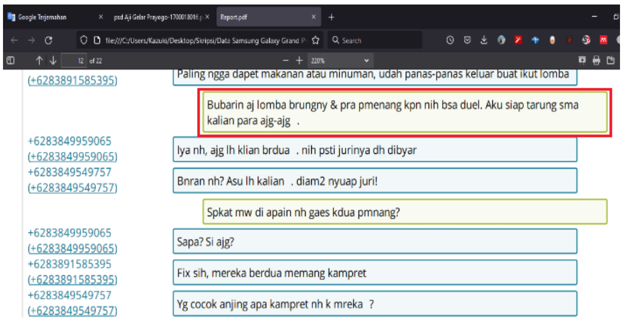
Installed applications	137	Videos	2
Contacts	1		

Figure14.Results Acquisition of Belkasoft Evidence Center

Figure 14 shows Belkasoft Tools did not live up to expectations in the artifact retrieval acquisition process. Belkasoft is only able to retrieve a list of installed applications and a list of contacts with 1 data and2data videos.

2.2.4 Examination

The examination or screening stage is the stage of the examination process on the collected data, both from the imaging process and direct backup. The stages of selecting data for evidence according to case studies are very important considering that there are so many types of data taken. The first step in the filtering process is to disable cellular data or wifi so that there is no sending or receiving data from the cloud. Then the smartphone is connected to the laptop. Data files that have been extracted, such as chat files, emojis, hashes files, contacts, and web caches, each have data authenticity and are validated using hashing tools so that the data can be claimed that the file has not changed. Details of participants and group chat can be seen in Figure 13.



Google Terjemahan
psd Aji Gelar Prayogo-1700018016.p
Report.pdf
file:///C:/Users/Kazuki/Desktop/Skripsi/Data Samsung Galaxy Grand P
Search
12
of 22
220%

(+6283891585395)
Paling ngga dapet makanan atau minuman, udah panas-panas keluar buat ikut lomba

Bubarin aj lomba brungny & pra pmenang kpn nih bsa duel. Aku siap tarung sma kalian para ajg-ajg .

+6283849959065 (+6283849959065)
Iya nh, ajg lh klian brdua . nih psti jurinya dh dibyar

+6283849549757 (+6283849549757)
Bnran nh? Asu lh kalian . diam2 nyuap juri!

Spkat mw di apain nh gaes kdua pmnang?

+6283849959065 (+6283849959065)
Sapa? Si ajg?

+6283891585395 (+6283891585395)
Fix sih, mereka berdua memang kampret

+6283849549757 (+6283849549757)
Yg cocok anjing apa kampret nh k mreka ?

Figure15.The Screening Process According to Bullying Criteria

Figure 15 shows the suspect, Tedi Mariono, starting the bullying by badmouthing the victim so that other suspects also badmouth the victims to chat in groups of various users and it’s stored in a report on the acquisition of forensic tools MOBILEdit Forensic, followed by a report and the marks area is the proof cyberbullying happen with green color mean the area marker is an indication where the cyberbullying occurred and the green color proves that it was carried out by the suspect's smartphone.

2.2.5 Analysis

Analysis of the results of the data retrieval process from the MOBILedit Forensic Express application and exporting them in the form of a pdf file report then filtered as needed and adjusted for the identification process of cyberbullying cases so that the identification process is easier and can see the rapid details, both message content, message recipients and recipient information numbers, and message sender. Belkasoft is the second forensic tool to compare whether it is more effective in retrieving smartphone data artifacts, but Belkasoft does not meet expectations because it cannot retrieve appropriate artifacts.Belkasoft managed to retrieve the smartphone artifact with a description of only showing a list of applications with as many as 158 items installed and retrieving contacts but only one contact.Based on the results of the acquisition between tools forensic MOBILEdit and Belkasoft, it can be seen that MOBILEdit is more effective in taking evidence.A possible problem with Belkasoft forensic tools is that the version of the application or the agent is not compatible with Belkasoft's analytical reference and for now, the MOBILEdit forensic tool is the most powerful compared to Belkasoft.

Table 2Group Conversations of Suspects

Tedi Mariono	Bubarin aj lomba brungny & pra pmenang kpn nih bsa duel. Aku siap tarung sma kalian para **ajg-ajg**￼￼ .
Aril Nujianto	Iya nh, ajg lh klian brdua ￼￼ . nih psti jurinya dh **dibyar**
Adhe Jariadi	Bnran nh? **Asu** lh kalian ￼￼ . diam2 **nyuap** juri!
Tedi Mariono	Spkat mw di apain nh gaes kdua pmnang?
Aril Nujianto	Sapa? Si **ajg**?
Harun Perwirantoro	Fix sih, mereka berdua memang **kampret**
Adhe Jariadi	Yg cocok **anjing** apa **kampret** nh k mreka ￼￼ ?
Tedi Mariono	Lbih cocok **ajg** sh, **jlekdekil** + tkang **suap**.
Aril Nujianto	Woy pra **anjing**, mna klian brdua ￼￼ ?!

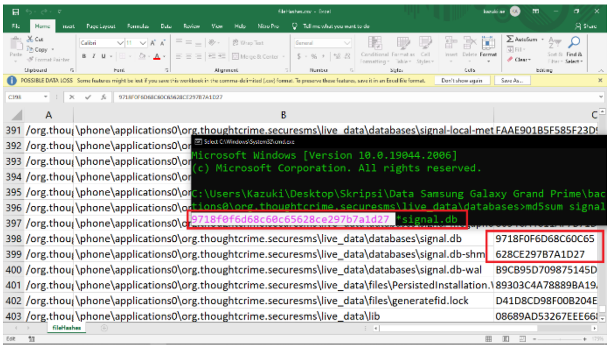
The data that has been obtained from the process of taking evidence is then grouped according to the conversation and preprocessing is carried out before being identified as a cyberbullying case by counting bad words so that the final result is the chat identified as cases of cyberbullying and with the counted bad words, the person who makes the bad words with the highest count is automatically identified as the defendant. Other results prove that numbers with low weights are aslo identified as cyberbullying.The victim was included in the bullying case because of the analysis of whether the victim felt his name was tainted and it was confirmed that the calculation of the number of words was rude.

The next stage is the process of drawing conclusions, namely counting the perpetrators who have said harsh words and ridiculed the victim repeatedly as if the perpetrators felt the highest authority. It was identified that the perpetrators included Tedi Mariono, Aril Nujianto, Adhe Jariadi, and Harun Perwirantoro.The perpetrators are then sanctioned in accordance with national law, with each country having its own set of penalties.The victims also mentioned that the perpetrators bribed the jury and that the victims were considered to have paid the jury so that they could win easily in the competition.

Table 3

Tedi Mariono	3 words that include "anjing" and other insults like "jelek" and "dekil"
Aril Nujianto	3 words "anjing" and 1 word "suap"
Adhe Jariadi	2 words “anjing”and 1 word “suap”
Harun Perwirantoro	1 word “kampret”

From table 3, various conversations that have been analyzed contain harsh words and slander mentioned by the perpetrators towards the two victims. It is known that the first perpetrator was Tedi Mariono, who said 3 harsh words "anjing" and then 1 harsh word in the form of body shaming, namely "jelek" and "dekil", which means the victim's perspective is very dirty. The second perpetrator is Aril Nujianto, with 3 mentions of the word "anjing" and 1 slanderous word, "suap". The third perpetrator, Adhe Jariadi, mentioned two words: "anjing" and "suap". The last or fourth perpetrator, Harun Perwirantoro, mentioned the word "kampret" which means damn.


fileHashes.csv - Excel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Help
Nitro Pro
Tell me what you want to do
Share
POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format.
Don't show again
Save As...
C398
fileHashes
Select C:\Windows\System32\cmd.exe

```
9718F0F6D68C60C65628CE297B7A1D27
```

```
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kazuki\Desktop\Skripsi\Data Samsung Galaxy Grand Prime\bac
tions0\org.thoughtcrime.securesms\live_data\databases>md5sum signal
9718f0f6d68c60c65628ce297b7a1d27 *signal.db
```

```
    A                 B                                                                          C
391 /org.thou \phone\applications0\org.thoughtcrime.securesms\live_data\databases\signal-local-met FAAE901B5F585F23D
392 /org.thou \phone\applications0\or
393 /org.thou \phone\applications0\or
394 /org.thou \phone\applications0\or
395 /org.thou \phone\applications0\or
396 /org.thou \phone\applications0\or
397 /org.thou \phone\applications0\o
398 /org.thou \phone\applications0\org.thoughtcrime.securesms\live_data\databases\signal.db       9718F0F6D68C60C65
399 /org.thou \phone\applications0\org.thoughtcrime.securesms\live_data\databases\signal.db-shm   628CE297B7A1D27
400 /org.thou \phone\applications0\org.thoughtcrime.securesms\live_data\databases\signal.db-wal   B9CB95D709875145D
401 /org.thou \phone\applications0\org.thoughtcrime.securesms\live_data\files\PersistedInstallation.\ 89303C4A78889BA19
402 /org.thou \phone\applications0\org.thoughtcrime.securesms\live_data\files\generatefid.lock    D41D8CD98F00B204E
403 /org.thou \phone\applications0\org.thoughtcrime.securesms\live_data\lib                       08689AD53267EEE66
```

Figure16.Hash Validation on Signal Databases

Figure 16 explains that the acquired Signal database is then validated with md5sum. The file from the acquisition of MOBILEdit Forensic shows that the hash value in the form of Excel shows 9718F0F6D68C60C65628CE297B7A1D27, then the hash result with the help of the bash command prompt shows the hash value is the same as the data in Excel, namely 9718f0f6d68c60c65628ce297b7a1d27. The data authenticity statement has proven that there is no change in the Signal database during the acquisition with the original Signal database files.

2.2.6 Presentation

The data that has been obtained from this research is in the form of complete evidence with reports of results from the MOBILedit Forensic Express application in the form of conversations, user numbers, hash values of data authenticity, and calculating word suspect whoever words counted carry out cyberbullying in groups conversation. Forensic tools from Belkasoft have not obtained artifacts from smartphones, so they cannot be used as benchmarks in digital evidence.

3. CONCLUSIONS

Based on this research, it can be concluded that forensics on the MOBILEdit Forensics Pro tool can retrieve Compared to Belkasoft, which only takes a few data artifacts on smartphoneand analyze digital evidence targeting the Signal Instant Messenger application and prove the authenticity of the data. The data proves that the DFRWS forensic method can retrieve evidence in the form of text in a group conversation, identify cyberbullying on a person and prove that there is no change in the data from the retrieval of evidence.Identified perpetrators who carried out bullying of as many as 4 people, with 2 victims and 1 witness.Further research is expected to be able to obtain deleted data and be able to implement methods to calculate the word weight of the perpetrators that lead to cyberbullying with a lot of data.

4. REFERENCES

[1] A. Sugeng Cahyono, “The Influence of Social Media on Social Changes in Indonesian,” *Asy Syar’Iyyah J. Shari’ah Sci. Islam. Bank.*, vol. 5, no. 2, pp. 202–225, 2020, doi: 10.32923/asy.v5i2.1586.

[2] G. Fanani, I. Riadi, and A. Yudhana, “Michat Application Forensic Analysis Using Digital Forensics Research Workshop Method,” vol. 6, no. April, pp. 1263–1271, 2022, doi: 10.30865/mib.v6i2.3946.

[3] I. Riadi, Herman, and N. H. Siregar, “Mobile Forensics in Cyber Fraud Cases on Signal Messenger Service Using the NIST Method,” vol. 3, no. 28, pp. 137–144, 2021.

[4] A. Widiastuti, “Positive And Negative Impacts of Technology,” *Http://Staffnew.Uny.Ac.Id,* 2012, [Online]. Available: http://dheanda478.blogspot.co.id/2012/11/dampak-positif-dan-negatif-teknologi.html

[5] R. Hughes, “Chapter II. Cyber Crime,” *J. Chem. Inf. Model.*, vol. 53, no. 9, p. 287, 2008.

[6] A. P. Utama Siahaan, “Cybercrime Violations and the Power of Jurisdiction in Indonesian,” *J. Eng. Informatics*, vol. 5, no. 1, pp. 6–9, 2018.

[7] “Facts + Statistics: Identity theft and cybercrime | III.” https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (accessed Aug. 21, 2022).

[8] “Indonesian Police handle 4,656 cyber cases, with defamation being the most common.” https://www.cnnindonesia.com/nasional/20201229094838-12-587280/polri-tangani-4656-kasus-siber-pencemaran-nama-baik-dominan (accessed Aug. 25, 2022).

[9] M. Yusuf and A. Cherid, “Implementation of the Cosine Similarity Algorithm and PHP-Based TF-IDF Method to Generate Seminar Recommendations,” *Sci. J. Fac. Comput. Sci.*, vol. 9, no. 1, pp. 8–16, 2020.

[10] A. Ababneh, M. A. Awwad, and M. I. Al-Saleh, “IMO forensics in Android and windows systems,” *2017 8th Int. Conf. Information, Intell. Syst. Appl. IISA 2017*, vol. 2018-Janua, pp. 1–6, Mar. 2018, doi: 10.1109/IISA.2017.8316377.

[11] M. Button and C. Cross, “Cyber Frauds.,” p. 232, 2017, [Online]. Available: https://books.google.co.uk/books?hl=en&lr=&id=GggqDwAAQBAJ&oi=fnd&pg=PP1&dq=ransomware+targeting+charities&ots=yWNs5vQOHj&sig=-lzDnFxe0e0kfYMHkJ0VGSHPZx0#v=onepage&q&f=false

[12] M. Van Uden, “Rocchio : Relevance Feedback in Learning Classification Algorithms,” *Proc. ACM SIGIR Conf.*, 1998, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.53.3960&amp;rep=rep1&amp;type=pdf

[13] W. Sanjaya, B. Sugiantoro, and Y. Prayudi, “An Offline Forensic Method For Digital Artifact Analysis In The TOR Browser On Linux Operating System,” *JITU J. Inform. Technol. Commun.*, vol. 4, no. 2, pp. 41–51, 2020, doi: 10.36596/jitu.v4i2.345.

[14] “Digital Evidence and Forensics | National Institute of Justice.” https://nij.ojp.gov/digital-evidence-and-forensics (accessed May 22, 2022).

[15] B. Rahardjo, “Digital Forensics at a Glance,” *Sociotechnology*, vol. 29, pp. 384–387, 2013.

[16] A. Satria S and D. M. A. Mansyur, “Chapter I Application of Digital Forensics,” *Inf. Technol.*, pp. 1–19, 2005, [Online]. Available: https://repository.unair.ac.id/97887/9/BAB I.pdf

[17] “Signal >> Home Page.” https://signal.org/id/ (accessed Aug. 24, 2022).

[18] D. A. Arifah, “Indonesia’s Cybercrime Case,” *J. Bus. Econ.*, vol. 18, no. 2, pp. 185–195, 2011, [Online]. Available: https://media.neliti.com/media/publications/24189-ID-kasus-cybercrime-di-indonesia.pdf

[19] F. G. Becker *et al.*, “AN EXAMPLE OF CYBER CRIME CASES AND ITS RESOLUTION,” *Syria Stud.*, vol. 7, no. 1, pp. 37–72, 2015, [Online]. Available: https://www.researchgate.net/publication/269107473_What_is_governance/link/548173090cf22525dcb61443/download%0Ahttp://www.econ.upf.edu/~reynal/Civil wars_12December2010.pdf%0Ahttps://think-asia.org/handle/11540/8282%0Ahttps://www.jstor.org/stable/41857625

[20] A. Kharisma, “What is Android?,” *Linux You*, vol. 15, no. 1, pp. 137–138, 140, 2008, [Online]. Available: https://www.academia.edu/2537177/What_is_Android

[21] A. Yudhana, I. Riadi, and I. Zuhriyanto, “Live Forensics Analysis of Social Media Applications on Browsers Using the Digital Forensics Research Workshop (DFRWS) Method,” *Techno*, vol. 20, no. 2, pp. 125–130, 2019, [Online]. Available: https://core.ac.uk/download/pdf/270178608.pdf

[22] "Office of Children and Young People ' s Services Anti-Bullying Strategy," no. November, 2007, [Online]. Available: https://web.archive.org/web/20120118183631/http://www.cambridgeshire.gov.uk/NR/rdonlyres/470E5F18-2397-416C-B265-087B18DD8E30/0/AntiBullyingStrategyNovember07.pdf

[23] N. Yuliani, "The phenomenon of bullying at school," *J. Chem. Inf. Model.*, vol. 53, no. 1, pp. 1689–1699, 2013, [Online]. Available: https://www.kemenpppa.go.id/lib/uploads/list/8e022-januari-ratas-bullying-kpp-pa.pdf

[24] T. Feinberg and R. Nicole, *Cyberbullying*. [Online]. Available: https://www.proquest.com/openview/df7b85db5268ac4d18d07478e8fe197f/1.pdf

[25] P. Studi, T. Informatika, F. Sains, D. A. N. Teknologi, U. Islam, and N. Syarif, "Application of Sentence Tokenization and TF(Term Frequency) Method in Automatic Text Summarizer," 2014, [Online]. Available: https://repository.uinjkt.ac.id/dspace/bitstream/123456789/57344/1/SALAMAH-FST.pdf