

Web Forensic for Hate Speech Case on Facebook Services using National Institute of Standards Technology Method

Nunung Anggriani
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

The development of information technology is increasing rapidly, has brought humans to a point where they cannot separate from the use of the internet in everyday life. The high growth of internet users is the potential for many internet users to use social media. By data compiled from databoks.katadata.co.id which shows the ranking of social media often used in Indonesia 2020, Facebook is in third place after YouTube and WhatsApp. The features offered by Facebook as a social media make many people use it as well as its ease of communication without having to incur costs such as SMS (Short Message Service). The use of Facebook through a web browser itself has often been used by many people and not a few are also used as a medium to commit crimes such as hate speech cases, so it is very important to investigate. The stages used to analyze digital evidence in this study are using the forensic method created by the National Institute of Standards Technology (NIST) which has four stages, namely Collection, Examination, Analysis, and Reporting. The percentage of results obtained from several tools used is the Facebook API 20% only managed to find account information in the form of profile photos, account names, and emails used, FTK Imager 80% successfully found posts along with deleted comments, account information, and login access, while Browser History Viewer 40% was able to find posts in the form of images and account information. From the results of this study, it was found that all the desired information was obtained using the tool, DumpIt + FTK Imager both main evidence and supporting evidence were found in tools, while Browser History Capture + Browser History Viewer only obtained information in the form of posting images, then searching for data using the Facebook API no deleted posts were found, only account information was found, because the use of the Facebook API was restricted to access permissions. By using some of these tools, this research managed to find all the posts that have been deleted.

Keywords

Digital Forensics, Facebook, Cybercrime, NIST

1. INTRODUCTION

The development of information technology which is getting faster day by day has brought people to a point where they cannot escape the use of social media in everyday life. In this era of information technology as well, the development of internet users itself has increased every year. The high growth of internet users is the potential for many internet users to use social media [1]. Through social media available on various internet applications, people can easily convey their thoughts orally and in writing. Social media is often used to spread the

news to the public to get wider coverage. However, it is often misused for criminal cases such as spreading false news, hate speech, cyberbullying, prostitution, and so on. By data compiled from databoks.katadata.co.id which shows the ranking of social media that is often used in Indonesia 2020. Facebook is in third place with a percentage of 82% below YouTube and WhatsApp [2]. The features offered by Facebook as a social media make many people use it as well as the ease of communicating without having to incur costs such as SMS (Short Message Service), Facebook can also be opened or accessed via a web browser via the link www.facebook.com. The use of Facebook through a web browser itself has often been used by many people and not a few are also used as a medium to commit crimes such as hate speech cases, so it is very important to investigate. In revealing cybercrimes that utilize computer technology, it can be done in several ways, such as extracting using the API (Application Programming Interface) provided by social media, because popular social media sites usually provide APIs to be used by software developers or used for investigations. by law enforcement officers to collect digital evidence to uncover a crime on social media [3] and take advantage of the data left on application usage activities contained in random access memory (RAM). To obtain this data and information, a technique and technique is needed, namely a technique from digital forensics and assisted by tools forensic[4].

1.1 Study Literature

1.1.1 Previous Study

In the first study, we researched laptop devices using the method live forensic to make acquisitions on Linux-based laptop memory with the tools used were Linux Memory Extractor (LiME) and volatility. This study succeeded in finding digital artifacts related to research, namely email accounts, Facebook accounts, and PayPal accounts [5].

In the second study in their research, they raised digital crime evidence on the Facebook Lite application using forensics with the tool used, namely the MOBILedit Forensic Pro forensic tools with the method used, namely the method National Institute of Standards Technology (NIST). The results obtained in the use of forensic tools are Account ID, Image, Audio, and Video [6].

Then the third research, in their research, they researched data volatile that was still recorded in Random Access Memory (RAM) with browsers analyzed, namely Google Chrome, Mozilla Firefox, and Microsoft Edge with the method used, namely the method National Institute of Justice (NIJ). with techniques live forensics and FTK Imager is used as a tool to acquire data. The results obtained are that Facebook social

media is not safe to access using Google Chrome, Mozilla Firefox, and Microsoft Edge, while Instagram social media is safer to access using Mozilla Firefox [7].

Furthermore, in their fourth study, entitled "Analysis and Comparison of Digital Forensics on Social Media Facebook and Twitter on Smartphones Android". Their research was conducted to find and compare forensic evidence on Facebook and Twitter social media applications accessed on smartphones Android. This study uses file recovery tools to restore previously deleted data to eliminate forensic evidence. And using the simulation method to get digital evidence on Facebook and Twitter, the stages of the simulation method used are Problem Simulation, Conceptual Model, Input/output data, Modeling, Simulation, Verification and Validation, Experimentation, and Output Analysis. The results of the research in the form of forensic evidence are mostly found on Facebook social media and there is no difference in the results of searching for forensic evidence using the SQLite Manager application or DB Browser for SQLite [8].

The last research, in his research, used an Acer Aspire E 14 Laptop as digital evidence of a drug transaction case using Facebook Messenger Web. Of searches of digital evidence in this study, some chats from dealers, buyers, and suppliers are still recorded in memory volatile on the Random Access Memory (RAM), at the time of taking evidence in circumstances Acer Aspire E 14 switched and used techniques Live Forensics. Data analysis and search for digital evidence were carried out using the method National Institute of Justice (NIJ) which has several steps, namely Identification, Collection, Examination, Analysis, and Reporting. The tools used are FTK Imager and managed to find digital evidence in logs the acquired and get data chat log deleted, logs image submission from dealers, account names, and delivery times chat on Facebook Messenger Web [9].

1.1.2 Digital Forensics

Is a method used in the investigation process of electronic or digital evidence to reconstruct crimes cyber or assisting in the process of analyzing crime cases [10], which includes the discovery and investigation of material (data) found on digital devices. (computers, mobile phones, tablets, PDAs, networking devices, storage, and the like) [11]. Another definition of digital forensics is a branch of science that aims to obtain information and investigate digital evidence so that it can be accounted for in court as legal evidence [7].

1.1.3 Digital Evidence

Evidence is defined as data stored or transmitted or distributed using a computer which will later be used as evidence to support or disprove theories about how the violation occurred. The data referred to here is in the form of a basic combination of numbers that represent various types of information such as video, audio, images, and text [12]. By Article 1 of the Law of the Republic of Indonesia Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, digital evidence has been legally used as evidence in court. In its original form, social media can be considered as a form of evidence, but unlike traditional criminal evidence, social media is very unique. Digital evidence from social media tends to be more extensive, more difficult to destroy, easy to modify, easy to duplicate, potentially more expressive, and easily available when compared to other traditional criminal evidence [13].

1.1.4 Cybercrime

Cybercrime is a criminal activity carried out in cyberspace that uses information technology as a crime target which includes all unauthorized access to data and damage to electronic devices and security, privacy, PINs, passwords, and others [14]. Criminal activities carried out in cyberspace such as fraud online, virus attacks, gambling online, pornography, email spam, call spam, SMS spam, cyber phishing, cyberbullying, data destruction, hate speech, and others.

1.1.5 Random Access Memory

Random-access memory (RAM) is a form of computer data storage that allows information to be stored and retrieved on a computer. Because information is accessed randomly and not sequentially like on a hard drive, computers can access data more quickly [15]. The downside of RAM is that it requires power to remain accessible. As soon as the power is turned off, all information stored in RAM will be permanently lost [16]

1.1.6 Hate Speech

The term hate speech itself means an expression that advocates incitement to harm based on targets identified with certain social or demographic groups [17]. Hatred or utterances of hate speech can be spread easily through a variety of media, both print, and social media. In general, hate speech itself often appears on social media timelines, one of which is on social media Facebook [18], whether it is done openly through a personal site, leaving it in the post comment column, or delivered privately via private message.

1.1.7 National Institute of Standards Technology

National Institute of Standards Technology (NIST) is one of the forensic stages used to obtain information from digital evidence [19]. The stages of the National Institute of Standards Technology (NIST) can be seen in Figure 1:

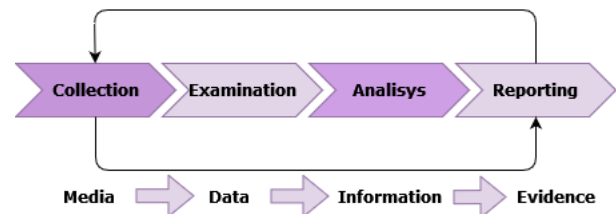


Figure 1. Stages of NIST Method

Based on Figure 1 the stages of digital forensics The National Institute of Standards Technology (NIST) has four stages, namely Collection, Examination, Analysis, and Reports. 19):

1. **Collection**, is the stage of collecting, identifying, labeling, retrieving data from relevant data sources while maintaining data integrity.
2. **Examination**, is the stage of examining data processing that has been obtained forensically, both automatically and manually according to the needs of digital forensics while maintaining data integrity.
3. **Analysis**, is the stage of analyzing the results of the examination by using methods that are legally correct and obtain useful information for the interest of investigators and can be accounted for.
4. **Reporting**, is the reporting stage on the results that have been obtained in the analysis which includes a description of the actions taken.

1.1.8 Facebook

Facebook is a Social Network Service (SNS) or social networking site that was created to provide technical facilities with the intention that users can socialize or interact in cyberspace [20]. On Facebook users can make comments, share photos, videos, and links to news or other interesting content on other sites, play games, live chat, and even do live video streaming. Content shared by Facebook users is publicly accessible, or can only be shared among a selected group of friends or family members, or shared with one person. Users must register to be able to use this site. After that, users can create private profiles and add other users as friends, including automatic notifications when profiles are updated. In addition, users can join groups of users with similar interests [21]. Facebook services provide a platform that can be used by developers to access or retrieve data contained in Facebook according to their needs. The platform is the Facebook Graph API or the which is an API for accessing objects and connections in the Facebook social graph. API stands for (Application Programming Interface).

2. METHODOLOGY

2.1 Research Scenario

Making of this scenario is made to explain the stages of the forensic process web browser that will be carried out to obtain the evidence sought. This research scenario uses a laptop that is used by the perpetrator to post content that contains hate speech.

The scenario begins with the perpetrator posting hate speech content on the Facebook service aimed at the victim via the Chrome web browser. The victim who feels the post is intended for him then interacts by commenting on the post. Victims who feel aggrieved and slandered report it to the authorities by bringing screenshots of the perpetrator's post. Perpetrators who feel panicked then delete the posts with the assumption that the data is deleted to eliminate traces of the crime. The case simulation can be seen in Figure 2.

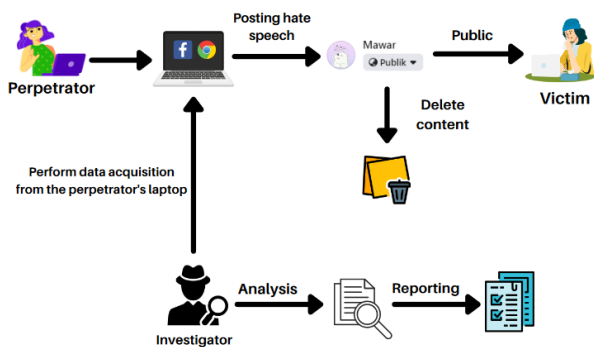


Figure 2. Research Case Scenario

Figure 2 shows that after the arrest, the evidence that was secured was a laptop and charger. It's used by the perpetrator and is alive and still accessing Chrome. After the investigators received the digital evidence, the process was captured carried out and, imaging namely copying (cloning/duplicate) correctly with the help of a flash drive to install the tool ram capturer on the perpetrator's laptop and also collecting data using the Facebook API. Then from the results of the copy and data search with the Facebook API, an analysis was carried out. The analysis is carried out mainly on the contents of the data that has been deleted as well as analyzing the results of data retrieval from the Facebook API. The final stage is reporting or reporting the results of the analysis of

digital evidence that is already valid and explaining the stages that have been used to obtain digital evidence that is proven to be genuine and valid.

2.2 Research Stages

Stages based on theory and literature study, the stages used to analyze digital evidence or stages to obtain information from digital evidence in this study, namely using the forensic method created by the National Institute of Standards Technology (NIST) because it has work guidelines, both policies, and standards to ensure that each investigator follows the same workflow so that work can be documented and results can be repeated and defended [22]. NIST has four stages which include Collection, Examination, Analysis, and Reporting.

These four stages are used as the implementation flow carried out by investigators to obtain digital evidence. This stage is necessary to maintain the integrity of the digital evidence obtained [23]. The following explains the steps used.

2.2.1 Collection

The Collection stage is the initial stage carried out by investigators to collect evidence. At this stage, it will be done sorting the evidence found to support the investigation process, which includes identification, labeling, recording, maintaining the authenticity of the evidence obtained.

The physical evidence used in this scenario is a laptop with a Windows operating system complete with a charger, which has the Chrome web browser installed which has previously been used as a means of hate speech. The data contained in the laptop RAM will be acquired using several forensic tools to avoid changing the data that will become digital evidence. The evidence used in this study can be seen in Table 1:

Table 1. Physical Evidence Found



No.	Name of Evidence	Picture	Description
1.	Laptop		Laptop with the Windows operating system that is alive and connected to the internet.
2.	The Charging		Laptop Charger

Table 1 is physical evidence that has been collected which will then be acquired using several tools forensic and Facebook APIs to search for and retrieve data that can be used as legal evidence.

2.2.2 Examination

This stage is the main stage in the investigation process to obtain data from electronic evidence obtained, namely the perpetrator's laptop. At the time of acquisition, it is ensured that the integrity of digital evidence is protected from contamination by things that can invalidate its status as digital evidence in court. The acquisition process is carried out using live forensics because it is adjusted to the scenario that has

been made, namely the acquisition process is carried out on a laptop that is turned on. This acquisition process uses several methods, namely searching data using the Facebook API and also using the help of several forensic tools which is carried out by acquiring RAM from the device used by the perpetrator.

The acquisition process in this study uses two tools, namely BrowserHistory Capturer to get data in Chrome browser and DumpIt for RAM data acquisition. The goal is to get additional information regarding the characteristics of the resulting data.

2.2.2.1 Data Search Using the Facebook API

The data search process using the Facebook API is accessed via Facebook Developers to get access tokens through devices used by the perpetrator. This access token is very much needed later used for the API function call to get data from Facebook. However, the access token needed to retrieve the data from Facebook will be updated every hour. Stages of data collection on offender account use Python and Facebook API to get JSON containing account data from the Facebook account used based on the parameters called and extracted into CSV format [24]. Figure 3 is a Python code used for the data collection and extraction process, which will then be analyzed at the analysis stage.

```
import facebook
import json
import pandas as pd

def main():
    token = "EAALS1sWqQkkBAEZACXKioO8FHd8ORexDKrMeZBk
    graph = facebook.GraphAPI(token)
    #menentukan parameter yg dipanggil
    profile = graph.get_object('me', fields='name, email, posts, picture')
    #memudahkan pembacaan hasil
    print(json.dumps(profile, indent=4))
    #simpan dlm format json
    with open('data.json', 'w', encoding='utf-8') as f:
        json.dump(profile, f, ensure_ascii=False, indent=4)

if __name__ == '__main__':
    main()

df = pd.read_json('data.json')
df.to_csv('hasil pencarian data.csv')
```

Figure 3. Python Code for Crawling Data Facebook

The extracted JSON to CSV file using python is stored in a folder that is the same as the code file. The CSV file that was successfully retrieved is shown in Figure 4.

Name	Date modified	Type	Size
idea	07/10/2021 22:13	File folder	
cobalagi	10/09/2021 10:54	Python File	1 KB
data.json	07/10/2021 23:21	JSON File	3 KB
First	06/10/2021 17:43	Python File	1 KB
hasil pencarian data	06/10/2021 17:57	XLS Worksheet	3 KB
sample	07/10/2021 22:46	Microsoft Edge P...	0 KB
Second	10/09/2021 16:40	Python File	1 KB

Figure 4. Results of the CSV File

Figure 4 shows data collection through the Facebook API using the help of PyCharm Community software to read a file containing Python code and managed to get data in CSV format with the name "data search results".

2.2.2.2 Data Acquisition from Chrome Browser

The data acquisition process from Chrome is carried out using the data tool forensic Browser History Capturer which is a tool for capturing web browser history from a Windows computer. Figure 5 below shows the results of the capture with a predetermined file location.

Name	Date modified	Type
Cache	31/08/2021 23:54	File folder
History	31/08/2021 23:54	File folder

Figure 5. Result Data Browser History Capturer

Figure 5 shows the captured file stored under the name Capture folder and in that folder, there are two more folders, namely the Cache and History folders. Inside the folder, several files will be read using the tool Browser History Viewer.

2.2.2.3 RAM Data Acquisition

The next data search is done by acquiring RAM on the laptop used by the perpetrator. In the activity of using an application, there must be data and information contained in Random Access Memory (RAM). Memory is a very important source of evidence in an investigative process. All activities that occur on a system are usually reflected in memory at that time. The acquisition process was carried out using the DumpIt forensic tool. Data retrieval using the DumpIt tool is carried out on applications that are running or capture all RAM activity when the laptop is used, then the results of the RAM dump file will be analyzed using the FTK Imager tool. The results of the acquisition can be seen in Figure 6.

Name	Date modified	Type	Size
DESKTOP-N02MALM-20210831-164443	31/08/2021 23:46	RAW File	6.291,456 KB
DumpIt	14/08/2021 22:03	Application	203 KB
README	14/08/2021 22:03	Text Document	1 KB

Figure 6. RAM Acquisition Results

Figure 6 is the result of the acquisition of RAM on the perpetrator's laptop which is then hashed using the FTK Imager tool to maintain the authenticity of the data.

2.2.3 Analysis

At this stage, an analysis is carried out on the results of data collection or acquisition of evidence obtained at the stage examination previous. In this research, the tools used are: to open and analyze the results of the acquisition of RAM using the FTK Imager and Browser History Viewer is used to analyze the data acquired by Chrome while to analyze or read the files extracted from the Facebook API using a simple program, namely CSV Viewer.

2.2.3.1 Facebook API

The data search results using the Facebook API have previously been successful got the CSV file. Then the CSV file will be analyzed using a simple program to make it easier to read the contents of the file. The CSV file cannot be changed at all or in the sense of a file that will be displayed is the original file generated from the extraction using Python. Because if the CSV file data is changed, then the program cannot display the contents of the CSV file.

Pilih menu > 1

name	email	posts
Mawar	nununganggriani90@gmail.com	[{"created_time": "2021-08-30T16:23:58+0000", "message": "Akun ini sedang digunakan untuk penelitiann!!", "id": "162093162734210_162164482727078"}, {"created_time": "2021-07-15T09:32:40+0000", "id": "162093162734210_130573345886192"}, {"created_time": "2021-06-21T10:37:55+0000", "id": "162093162734210_123528169924043"}, {"created_time": "2021-06-20T15:26:53+0000", "message": "Test lagi.", "id": "162093162734210_123254559951404"}, {"created_time": "2021-05-15T13:33:02+0000", "id": "162093162734210_103858148557712"}, {"created_time": "2021-05-15T13:26:02+0000", "message": "Haili, aku mawar.", "id": "162093162734210_103852641891596"}, {"created_time": "2021-05-15T13:25:23+0000", "id": "162093162734210_103852315224962"}, {"created_time": "1994-12-11T08:00:00+0000", "id": "162093162734210_103849075225286"}]

Figure 7. Data Display Results

Figure 7 above shows that the deleted post could not be found due to limited access permissions from Facebook. Therefore, the search for digital evidence on the Facebook API is not prioritized because in the simulation case this study explains that the perpetrator posted hate speech which then intentionally deletes the content. But found other supporting data in the form of account names and emails. The Post view cannot be tidied up because it must use the original file without having to be changed.

2.2.3.2 Browser History Viewer

The results of data acquisition using the tool Browser History Capturer will previously be analyzed or read using the tool Browser History Viewer to be able to view the access history of the Chrome browser.

Date Visited	Title	URI	Visit C.	Calc.	Web Browser
31/08/2021 16:42:14	Mawar Facebook	https://www.facebook.com/profile.php?id=100068005809954	10	14	Chrome (De
31/08/2021 16:42:06	Facebook	https://www.facebook.com/	11	19	Chrome (De
31/08/2021 16:41:59	Facebook	https://www.facebook.com/permalink.php?story_fbid=1629481	1	1	Chrome (De
31/08/2021 16:41:54	Facebook	https://www.facebook.com/permalink.php?story_fbid=1629501	1	1	Chrome (De
31/08/2021 16:38:28	Mawar Facebook	https://www.facebook.com/profile.php?id=100068005809954	10	14	Chrome (De
31/08/2021 16:34:44	Mawar Facebook	https://www.facebook.com/profile.php?id=100068005809954	10	14	Chrome (De
31/08/2021 16:32:39	Mawar Facebook	https://www.facebook.com/profile.php?id=100068005809954	10	14	Chrome (De
31/08/2021 16:28:49	Mawar Facebook	https://www.facebook.com/profile.php?id=100068005809954	10	14	Chrome (De
31/08/2021 16:28:21	Facebook	https://www.facebook.com/	11	19	Chrome (De
31/08/2021 16:28:19	Facebook	https://www.facebook.com/	11	19	Chrome (De
31/08/2021 16:28:19	Facebook	https://www.facebook.com/	11	11	Chrome (De
31/08/2021 16:27:49	Facebook	https://www.facebook.com/	11	11	Chrome (De
31/08/2021 16:27:48	Facebook	https://www.facebook.com/	11	11	Chrome (De

Figure 8. Website History Page

Figure 8 shows the activity of Mawar's account with id "100068005809954" visiting Facebook on 31/08/2021 in the above timeframe and Time zone UTC.

Last Fetched	Filename	URL	Fetch Count	File Size (Bytes)	Web Browser
31/08/2021 16:42:06	440xIMV7ce.png	https://static.xx.fbcdn.net/rs		13077	Chrome (De
31/08/2021 16:42:19	196405127_123528153257378_6864838792227023309_n.jpg	https://scontent.fjog3-1.fna		12476	Chrome (De
31/08/2021 16:38:30	zleVfcqexHq.png	https://www.facebook.com/		11774	Chrome (De
31/08/2021 16:42:12	zleVfcqexHq.png	https://static.xx.fbcdn.net/rs		11774	Chrome (De
31/08/2021 16:42:06	240471603_162951665981693_667529780960317802_2_n.jpg	https://scontent.fjog3-1.fna		11047	Chrome (De
31/08/2021 08:18:45	Gear_128x128.png	https://app.diagrams.net/m		10678	Chrome (De
31/08/2021 16:38:29	F8jSULCiaha.png	https://www.facebook.com/		10387	Chrome (De
31/08/2021 16:38:55	F8jSULCiaha.png	https://static.xx.fbcdn.net/rs		10387	Chrome (De
31/08/2021 08:07:57	android-chrome-512x512.png	https://app.diagrams.net/m		9291	Chrome (De
31/08/2021 16:42:19	217404240_13057332528	https://scontent.fjog3-1.fna		8724	Chrome (De
31/08/2021 16:28:27	An-V1eo7VQ3O9lqK29nfo3	https://scontent.tir2-1.xx.fb		8724	Chrome (De
31/08/2021 16:34:48	An-V1eo7VQ3O9lqK29nfo3	https://scontent.fdac69-1.fna		8724	Chrome (De

Figure 9. Display Cached Images

Figure 9 shows the image that was found, namely the profile photo of the perpetrator found with the file name "196405127_123528153257378_6864838792227023309_n.jpg" which has been matched with the perpetrator's profile photo from the previous victim's screenshots.

Last Fetched	Filename	URL	Fetch Count	File Size (Bytes)	Web Browser
31/08/2021 16:42:48	fAZrRM8pGA.png	https://static.xx.fbcdn.net/rs		6935	Chrome (Default)
31/08/2021 16:28:27	An8KSKhoMKUjVSZ4NVh8ln	https://scontent.fhjl1-1.fna		6756	Chrome (Default)
31/08/2021 16:34:48	An8KSKhoMKUjVSZ4NVh8ln	https://scontent.fhjl1-1.fna		6756	Chrome (Default)
31/08/2021 16:38:32	An8KSKhoMKUjVSZ4NVh8ln	https://scontent.fhjl1-1.fna		6756	Chrome (Default)
31/08/2021 08:08:43	data_flow_3.png	https://app.diagrams.net/m		8555	Chrome (Default)
31/08/2021 16:42:15	240471603_162948749315318_1557997128582372145_n.jpg	https://scontent.fjog3-1.fna		8532	Chrome (Default)
31/08/2021 16:42:15	240270169_162948749315318_1557997128582372145_n.jpg	https://scontent.fjog3-1.fna		8168	Chrome (Default)
31/08/2021 16:29:48	240471603_1629516659816	https://scontent.fjog3-1.fna		5848	Chrome (Default)
31/08/2021 16:42:15	151895214_63855302980991	https://scontent.fjog3-1.fna		3773	Chrome (Default)
31/08/2021 16:28:35	shared-story-right.png	https://www.facebook.com/		5646	Chrome (Default)
31/08/2021 16:28:30	o4Z7Vlc-5C-bico	https://static.xx.fbcdn.net/rs		5430	Chrome (Default)
31/08/2021 16:42:06	o4Z7Vlc-5C-bico	https://www.facebook.com/		5430	Chrome (Default)

Figure 10. Posted by the perpetrator

In Figure 10 above, we also managed to get an image that matches the scenario of the evidence created which is the result of posting a picture of the perpetrator with the file name "240270169_162948749315318_1557997128582372145_n.jpg".

Last Fetched	Filename	URL	Fetch Count	File Size (Bytes)	Web Browser
31/08/2021 16:42:08	440xIMV7ce.png	https://static.xx.fbcdn.net/rs		13077	Chrome (Default)
31/08/2021 16:42:19	196405127_123528153257378_6864838792227023309_n.jpg	https://scontent.fjog3-1.fna		12426	Chrome (Default)
31/08/2021 16:38:30	zleVfcqexHq.png	https://www.facebook.com/		11774	Chrome (Default)
31/08/2021 16:42:15	zleVfcqexHq.png	https://static.xx.fbcdn.net/rs		11774	Chrome (Default)
31/08/2021 16:42:06	240471603_162951665981693_667529780960317802_2_n.jpg	https://scontent.fjog3-1.fna		11047	Chrome (Default)
31/08/2021 08:18:45	Gear_128x128.png	https://app.diagrams.net/m		10678	Chrome (Default)
31/08/2021 16:38:29	F8jSULCiaha.png	https://www.facebook.com/		10387	Chrome (Default)
31/08/2021 16:38:55	F8jSULCiaha.png	https://static.xx.fbcdn.net/rs		10387	Chrome (Default)
31/08/2021 08:07:57	android-chrome-512x512.png	https://app.diagrams.net/m		9291	Chrome (Default)
31/08/2021 16:42:19	217404240_13057332528	https://scontent.fjog3-1.fna		9289	Chrome (Default)
31/08/2021 16:28:27	An-V1eo7VQ3O9lqK29nfo3	https://scontent.tir2-1.xx.fb		8724	Chrome (Default)
31/08/2021 16:34:48	An-V1eo7VQ3O9lqK29nfo3	https://scontent.fdac69-1.fna		8724	Chrome (Default)

Figure 11. Posts of Image 2 of Actors

Figure 11, shows the post managed to find a second and identical image to the image in the victim's screenshot, found in the Cached Image menu. With the file name "240471603_162951665981693_667529780960317802_2_n.jpg". The post is a post that has been deleted by the perpetrator and found.

2.2.3.3 FTK Imager

Files resulting from the acquisition of RAM using the DumpIt tool at the examination stage previously then an analysis will be carried out using the FTK imager. The file has been imaged and the hash value of the file has been verified is the same as the original file hash value, meaning no change data in the file.

Drive/Image Verify Results	
Sector count	12582912
MD5 Hash	
Computed hash	836907ba3b845a984393ff771b51a295
Report Hash	836907ba3b845a984393ff771b51a295
Verify result	Match
SHA1 Hash	
Computed hash	0bf6f96c6415abe4190d3b4a4b38ee2e6c1
Report Hash	0bf6f96c6415abe4190d3b4a4b38ee2e6c1
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 12. Hashing Value of DumpIt File

Figure 12 shows the hashing results showing the MD5 value with SHA1 Match, meaning that the data integrity is maintained. After hashing has been done, then enter the hashed results into the "Evidence Tree".

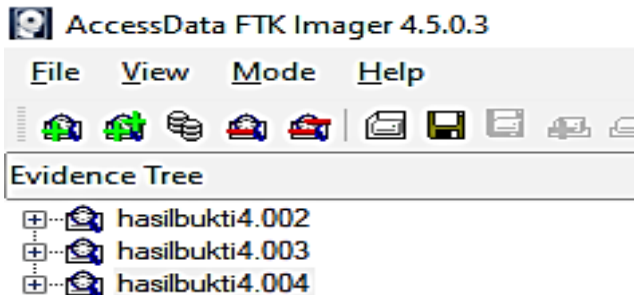


Figure 13. File Analysis with FTK Imager

Figure 13 shows the imaging results ready for analysis. The analysis process using FTK Imager can include one main file with the RAR extension which is a combination of the three files and can also include one file at a time as shown above. To facilitate the analysis process, use the "Find" or CTRL+F feature or you can also right-click. In this analysis using the FTK Imager, managed to find the desired digital evidence, namely in the form of posts that have been deleted by the perpetrators. The posts found were posts in the form of text and comments from the victim. While the post in the form of an image was not found. The post results found can be seen in Figure 14, Figure 15, and Figure 16.

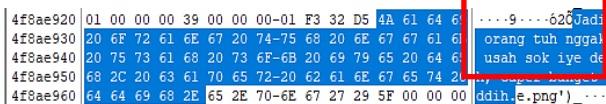


Figure 14. First Results of Text Post

Figure 15 above shows the results of the perpetrator's first text posting that contained "Jadi orang tuhnggakusahsokiyedeh, caper bangetddih ". The results obtained are identical to the results of the victim's screenshot, a second post was also found which can be seen in Figure 15.

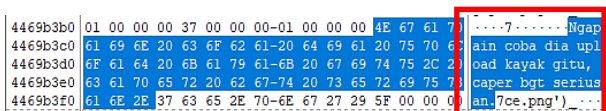


Figure 15. Second Text Post

Next Figure 15 shows the second text post that was also found which contained "Ngapaincobadia upload kayak gitu, caper bgtseriusan.". This post was also obtained by searching using the word parameter in the victim's screenshots.

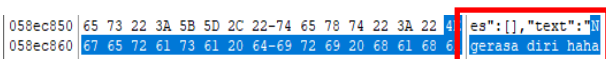


Figure 16. Third Text Post

Figure 16 shows the third text post that was found which was also obtained by searching using the word parameter which contained the results of the victim's screenshots which contained "Ngerasadirihaha".

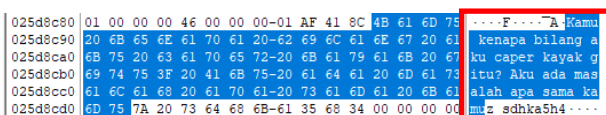


Figure 17. Victim's First Comment

Figure 17 is the result of the search for evidence of the comments being sought using the word parameter in the victim's screenshots where the comment is a comment from the perpetrator's post on the second text post with the victim's comment containing "Kamu kenapa bilang aku caper kayak gitu? Aku ada salah apa sama kamu". In addition, further comments were also found.

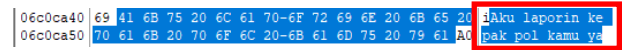


Figure 18. Victims Second Comments

Figure 18 shows evidence of comments from the victim that is identical to the contents of the comments on the victim's screenshots which contain "Aku laporin ke pak pol kamu ya ". The comment is a victim's comment on the perpetrator's post in the form of an image.

In the analysis using the FTK Imager tool, other supporting evidence was also found, namely the username and password, as well as the perpetrator's account id. The search for digital evidence is found in analysis using the FTK Imager tool.

2.2.4 Reporting

After going through the previous three stages, this stage is the final stage of research where all evidence, both physical evidence and digital evidence that has been obtained relating to the case under study, will be reported or presented to reveal a criminal case that has been previously scripted, namely a report on the results of the analysis carried out. on the perpetrator's laptop related to the case of hate speech carried out on the Facebook service which was accessed via the Chrome web browser. Techniques and tools used in the data search process will also be included to see the comparison results from several search processes used [25].

Information about the device used in this study is a Windows 10-based laptop with details in Table 2:

Table 2. Specification of Hardware

Brands	ASUS X441M
Processor	Intel (R) Celeron (R) CPU @ 1.10GHz N40001:10 GHz
Graphics	Intel (R) UHD Graphics 600
Memory	4 GB 2133MHz SDRAM
Hard disk	1 TB

Table 2 is information on the devices used by the perpetrators as a means of hate speech. While the software for which the forensic process is carried out or analyzed is the Facebook service that runs on the Chrome web browser. By following several stages of examination, the evidence is analyzed using several forensic tools with different functions and features to obtain additional information regarding the characteristics of the resulting data. So the main focus of this search is some things related to the perpetrators and social media use, especially on posts that have been deleted.

Table 3. Evidence of Screenshots and Findings


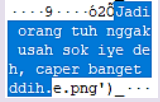

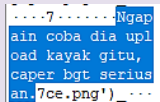


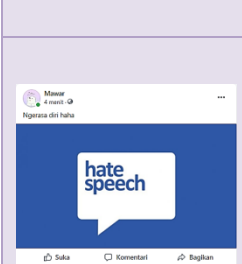
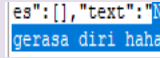
Evidence of Screenshots of Victims	Findings	Description
	 ...9...620 orang tuh nggak usah sok iye deh, caper banget ddih. (e.png) _....	Post: " Jadi orang tuh nggak usah sok iye deh, caper banget ddih." Comment: "Kamu kenapa bilang aku caper kayak gitu? Aku ada masalah apa sama kamu "
	 ...7...7...Ngapain coba dia upload kayak gitu, caper bgt seriusan. (7ce.png) _....	Post: " Ngapain coba dia upload kayak gitu, caper bgt seriusan."
	 ...240270169_162948749315318_1557997128582372145_n.jpg	Posts: "240270169_162948749315318_1557997128582372145_n.jpg" Comments: "Aku laporin ke pak pol kamu ya"
	 es": [], "text": "Ngerasadirihaha"	Posts: "Ngerasadirihaha" "240471603_162951665981693_6675297809603178022_n.jpg"

Table 3 is the digital evidence that was found from the acquisition of random access memory (RAM) on the perpetrator's laptop in the web browser forensic process. The digital evidence found is the main evidence that is desired because it is a post that has been deleted by the perpetrator who was found with the help of several forensic tools. The digital evidence is by the previous scenario, namely posts in the form of text, posts in the form of images along with comments, and other supporting evidence, namely username and password, profile photo, and the user id of the Facebook account used.

2.2.5 Results

Digital evidence that was obtained after going through an analysis process using the Facebook API and several forensic tools, namely DumpIt, FTK Imager, Browser History Capturer, and Browser History Viewer, was found deleted posts, both images, and text, as well as account information,

comments, and login access.

Table 4. Digital Evidence Search Results

Information	Tools		
	DumpIt + FTK Imager	Browser History Capture + Browser History Viewer	API Facebook + CSV Viewer
Text Posts	✓	-	-
Image Posts	-	✓	-
Account Information	✓	✓	✓
Comments	✓	-	-
Login Access	✓	-	-

In Table 4 of all the results Reporting above, it is concluded that all the desired information was obtained using the tool, DumpIt + FTK Imager both main evidence and supporting evidence were found in tools, while Browser History Capture + Browser History Viewer only obtained information in the form of image postings, then searching the data using the Facebook API only found account information, because the use of the Facebook API was restricted to access permissions.

3. CONCLUSION

After conducting several series of studies conducted using the National Institute of Standards and Technology (NIST) stages, all the desired digital evidence related to hate speech carried out on Facebook services was found which was accessed via a web browser based on a pre-determined evidence search scenario. The results of digital evidence are found in the form of text posts and pictures that have been deleted, comments, and supporting evidence such as account id, username, and password from the Facebook account used. The percentage of results obtained from several tools used is the Facebook API 20% only managed to find account information in the form of profile photos, account names, and emails used, 80% FTK Imager found posts along with deleted comments, account information, and login access, while Browser History Viewer 40% was able to find posts in the form of images and account information. From the results of this research, it was found that all the desired information was obtained using the DumpIt + FTK Imager tool, both main evidence and supporting evidence were found in these tools, while Browser History Capture + Browser History Viewer only obtained information in the form of posting images, then searching for data. using the Facebook API no deleted posts were found, only account information was found because the use of the Facebook API was restricted to access permissions. By using some of these tools, this research managed to find all the posts that have been deleted.

4. REFERENCES

[1] Y. Fitriani and R. Pakpahan, "Analysis of the Abuse of Social Media for the Spread of Cybercrime in Cyberspace," *CAKRAWALA J. Hum. Bina Sarana Inform.*, vol. 20, no. 1, 2020.
 [2] D. H. Jayani, "10 Most Used Social Media in Indonesia," 2020. <https://databoks.katadata.co.id/datapublish/2020/02/26/10-media-sosial-yang-paling-sering-digunakan-di>

indonesia.

- [3] H. Arshad, A. Jantan, and E. Omolara, "Evidence collection and forensics on social networks: Research challenges and directions," *Digit. Investig.*, vol. 28, pp. 126–138, 2019, doi: 10.1016/j.diin.2019.02.001.
- [4] T. D. Larasati, "Live Forensics Perbandingan Aplikasi Instant Messenger Live Forensics Analysis for Comparing Instant Messenger Applications (Line, Facebook, and Telegram) on Windows 10 Operating System," 2017.
- [5] M. A. Yaqin, "Live Forensics Method Analysis on Laptop Memory Devices for Linux-Based Digital Artifact Search," 2019, [Online]. Available: <http://repository.unmuhjember.ac.id/id/eprint/3386>.
- [6] R. A. Bintang, R. Umar, and A. Yudhana, "Facebook Lite Social Media Analysis with Forensic tools using the NIST Method," *Techno (Jurnal Fak. Tek. Univ. Muhammadiyah Purwokerto)*, vol. 21, no. 2, p. 125, 2020, doi: 10.30595/techno.v21i2.8494.
- [7] R. A. Kinasih, A. W. Muhammad, and W. A. Prabowo, "Browser Security Analysis Using the National Institute of Justice Method (Case Study: Facebook and Instagram)," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. x, pp. 174–184, 2020.
- [8] W. A. Mukti, S. U. Masrurroh, and D. Khairani, "Analysis and Comparison of Forensic Evidence Facebook and Twitter Social Media Applications on Android Smartphones," *J. Tek. Inform.*, vol. 10, no. 1, pp. 73–84, 2018, doi: 10.15408/jti.v10i1.6820.
- [9] Setie Ruhdi Koara, "Digital Forensic Analysis On Facebook Messenger Web For Cybercrime Case Handling," 2019.
- [10] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," no. June 2018, doi: 10.18517/ijaseit.8.3.3591.
- [11] B. Rahardjo, "Digital Forensics at a Glance," *J. Siosioteknologi*, 2013.
- [12] E. Casey, *Digital evidence and computer crime: Forensic science, computers, and the internet*, Third. Academic Press, 2011.
- [13] S. Pomalingo, "Social Media Investigation Using Data Visualization With Directed Graph Method," 2019, [Online]. Available: dspace.uui.ac.id.
- [14] D. Z. Abidin, "Crimes in Information and Communication Technology," *J. Ilm. Media Process.*, vol. 10, no. 2, pp. 1–8, 2015, [Online]. Available: <http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107/105>.
- [15] A. Josi, *Operation System*. Yayasan Kita Menulis, 2019.
- [16] L. F. Al Hakim, "Design and build an automatic salted fish packaging device based on a programable logic controller (plc) zelio," *Dr. Diss. Univ. Muhammadiyah Surabaya*, 2021.
- [17] S. Mawarti, "Hate Speech Phenomenon The Impact of Hate Speech," *Toler. Media Ilm. Komun. Umat Beragama*, vol. 10, no. 1, p. 83, 2018, doi: 10.24014/trs.v10i1.5722.
- [18] Y. Pramadi, "Indonesia in the Middle of the Digital Wilderness," 2020. <https://jmb.lipi.go.id/jmb/article/view/1117>.
- [19] D. Hariyadi and I. Y. Pasa, "Identification of Digital Evidence in Mi Video Application Using Live Forensics Method," vol. 2018, no. November, pp. 166–172, 2018.
- [20] Madcoms, *Hang out Friends via Facebook*. Yogyakarta: C.V Andi Offset, 2009.
- [21] D. Nations, "What is social media? Explaining the big trend," vol. 30.05, 2017.
- [22] A. P. Heriyanto, *Mobile Phone Forensics: Theory: Mobile Phone Forensics dan Security Series*, 1st ed. Yogyakarta: ANDI, 2016.
- [23] A. N. Ichsan, "Mobile Forensics on Android-Based IMO Messenger Services Using Digital Forensic Research Workshop Methods Mobile Forensics on Android-Based IMO Messenger Services Using Digital Forensic Research Workshop Methods," 2020.
- [24] Guntur Kondang Prakoso, "Design and build an application for post-classification on local government social media in Indonesia using a Support Vector Machine (SVM)," (*Doctoral Diss. Inst. Teknol. Sepuluh Nopember*), vol. 10, no. 1, pp. 279–288, 2018.
- [25] T. Pandela, "Browser Forensics on Web-Based TikTok Applications," 2020.