Mobile Forensic of Facebook Services using National Institute of Standard Technology (NIST) Method

Sri Mutmaina Dusu
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 today is increasingly rapid and also the increasing use of the internet on social media, especially on social media Facebook. Facebook has a negative impact that affects children, teenagers, and even adults such as actions taken by intentionally posting words or pictures in the form of insults or humiliating the person, not crimes like this are often called cyber harassment. This research was conducted by creating post scenarios that lead to Harassment cases in the form of insults and also humiliating someone using a mobile-based Facebook application. This study aims to restore and analyze a deleted post using the National Institute of Standards and Technology forensic stage with a Collection, Examination, Analysis, and Reporting workflow. This study uses a smartphone that has the Facebook application installed that has been rooted. The process of searching for digital evidence uses 2 forensic tools, namely MOBILedit forensics and DB Browser for SQL lite. The percentage of results obtained is based on two tools, namely the MOBILedit forensic tools 90% while the DB Browser tools 50%.The results of the study obtained evidence in the form of the perpetrator's account and posts in the form of images and text.

Keywords
Forensic, Facebook, Harassment, NIST

1. INTRODUCTION
The development of information technology today is increasingly rapid also the increasing use of the internet on social media, especially on social media Facebook, Facebook users in Indonesia there are 170.6 million in December 2020 which is 62.1% of the total population.[1]The popularity of Facebook is marked by the number of users from all walks of life and ages. The diversity of users certainly has an impact on the diversity of content on Facebook, and of course, not all of them are positive. [2]. There is negative Facebook content in the form of a case of a discovery that has happened a lot lately. Cyber harassment is an act that describes how people are constantly chasing other people online with the intent to scare or embarrass the victim. This study aims to analyze the process of investigating harassment cases and bring up evidence of posting data on the Facebook application. The research method used in this study is the National Institute of Standards and Technology method. NIST is a method that has four stages in resolving and investigating Cyber harassment cases, the first stage is Collection, Examination, Analysis, and the last is Reporting [3].

1.1. Study Literature
1.1.1 Previous Study
This research was conducted by conducting five studies. This activity is carried out to review the data that has been previously checked, among others found and relevantto this research. The first previous study with the titleentitled"Analysis of Digital Evidence on Facebook Messenger Applications using the National Institute of Justice Forensic method on Android Smartphones". From this research, several conclusions can be drawn, namely obtaining digital evidence in the form of accounts, chats, and pictures related to simulating cases of drug vape liquid circulation.[4]

The second previous study with the title "Comparison of Forensic Evidence for Facebook and Twitter Social Media Applications on Android Smartphones".This study can be concluded that the results of the scenario in the search for digital evidence that has been determined on the Facebook social media application, evidence -Forensic evidence that can be found. Forensic evidence found is account name, location data, telephone number, date of birth, profile photo, cover photo, post type text, post type image, private message type text, and private message type image. In the application Twitter, forensic evidence was obtained only in the form of account names, location data, profile photos, cover photos, tweets of text type, and tweets of image types.[5]

The third previous study with the title"Forensic Analysis of Kakaotalk Applications Using National Institute Standard Technology Methods".In this study, it was concluded that in research the work steps/procedures could be described briefly. The expected result of this research is an analysis process that can run well and get digital evidence from KakaoTalk on an android smartphone that is used as the object of further research. [6]

The fourth previous study with the title"Investigation of Cyberbullying on WhatsApp using Digital Forensics". In this study, it can be concluded that the results obtained to use a DFRWS method or stage that helps the acquisition process to reveal digital evidence against perpetrators in the group feature in the form of text. The results of actions that lead to cyberbullying are obtained with the highest result value having a cyberbullying level of 0.05 and the lowest result value having a cyberbullying level with an ISC value of 0.02 from the presentation of the value of the word cyberbullying in conversations against queries.[7]

The last previous study with the title "Identification of Skype Digital Evidence on Android Smartphones using the National Institute of Justice method".In this study, it can be concluded that the evidence found in the Skype application namely images and text that will be used as digital evidence [8].

1.1.2 Digital Forensics
Digital forensics is a science derived from computer security that discusses the discovery of digital evidence of an event that has occurred. Digital forensics is a process to identify,

maintain, analyze and also use digital evidence according to applicable law [9]. Digital forensics is also the science of finding evidence of a crime that occurred [10]. Experts say that digital forensics is a series of methodologies composed of a technique and also a procedure for collecting and seeking legal digital evidence in court [11]. Digital forensics has the first stage, namely collection, examination, analysis, and reporting, digital evidence related to criminal cases according to law [12]. Digital forensics is a branch of forensic science that includes findings during an investigation of data found on digital devices as digital evidence [13].

1.1.3 Mobile Forensics

Mobile forensics is a type of data collection - electronic data with the intent or purpose of legal evidence. Forensic itself is a tool used for investigations with the method of collecting criminal evidence from traces of digital data, which is very difficult to delete. Extraction of files on deleted phones will be used as evidence, this is the main job of mobile forensic investigators techopedia. Mobile forensics can be used on various smartphones based on a method and the type of software used[15]. Mobile Forensics can also apply science that can recover evidence from mobile devices with a method that is acceptable in law. Mobile forensics has the aim of meeting the needs of digital evidence in court, but it can also be used as a non-literacy process [16].

1.1.4 Digital Evidence

In the digital book Evidence and Computer Crime Edition (2011), digital evidence is a type or type of data stored or data sent using a computer, with the onset of a crime. Violations or crimes can be interpreted with intent or alibis. The definition of data in accordance with this is a combination of numbers that represent information from the type of media text, images, audio, documents, or video. By considering the available data and also how the benefits can be provided in an investigation [17]. There is also a traditional forensic where an investigator can work using physical evidence but after conducting an analysis the investigator uses the results of the duplication of evidence for example storage on media, or computing devices [14].

1.1.5 Cyber Harassment

Cyber harassment is one type of cybercrime that is busy being discussed among people who use social media. Based on data from women's commission regarding internet abuse in 2017 there were 14 cases of cyber violence, 1 case of cyber grooming for women as victims, 20 cases of cyber harassment for threatening and disturbing, 16 cases of illegal content, and 19 cases of malicious distribution such as distribution personal photos or videos. In Indonesia, there are several cases of cyber harassment, one of which is the case of Via Vallen receiving nasty messages from strangers on her social media and the case of Shandy Aulia receiving body shamming comments on her social media. Apart from Indonesia, other countries such as South Korea and Australia also face many cases of cyber harassment, one of which is Choi Jin-RI or also known as Sulli from girl group F(X), and police officer MP Jenny Leong from Sydney who received harsh comments that contain racism in their social media[18].

1.1.6 Facebook

Social media itself is a program or application that is widely used by the community, its development is also very popular in Indonesia. One of the most popular social media applications is Facebook[19]. Facebook refers to a site that allows users to post photos, videos, notes, and status updates to share with other users in their network, called 'Friends' [20]. Facebook was created in 2004 by Mark Zuckerberg[21] and is currently the most popular platform used worldwide [22].

1.1.7 Android

Android is a mobile device that includes a Linux-based operating system. Android is also an operating system for a cellular phone, android provides a platform for developers to create their applications [23]. Android can also be interpreted as an open-source mobile device platform developed by the Linux 2.6 kernel and maintained by the OpenHandset Alliance, the OpenHandset Alliance is a group of operators, manufacturers, mobile devices, and components, and is a software vendor. Android has a history as a platform that started in 2008 [24].

1.1.8 National Institute of Standards Technology Stages

The National Institute of Standards and Technology is a unit of the United States Department of Commerce, often known as the National Bureau of Standards -NBS, the name was known from 1901 to 1988. NIST has provided a standardized and usable method as a problem solver and analyzes digital evidence or the stages in obtaining information from the digital evidence[25].NIST stages can be seen in Figure 1.

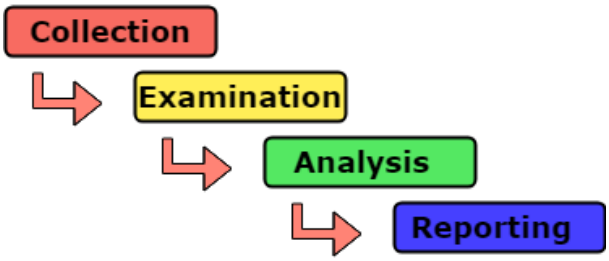

Figure 1.The Stages of NIST Method

Figure 1 shows the stages of NIST mobile forensics, there are several stages as follows[24]:

a. Collection, this stage is the initial stage which is often referred to as the stage of collecting or identifying the evidence used in the form of a hardware device from which data will be taken to be used as digital evidence of a digital crime case. This stage is carried out by following all data integrity security steps.
b. Examination This stage is the stage of returning data on digital evidence such as a smartphone, the return of the data can be done using trusted forensic tools so that the data obtained has high integrity.
c. Analysis This stage is a process to analyze the data that has been returned, the data that is analyzed such as data of database type, to perform the analysis can use trusted forensic tools.
d. Reporting This stage is the final stage of the investigation process, this stage is the stage of reporting the results of the analysis process which can include data information that has been successfully returned and which can be used as the final report of the forensic process, this stage can be presented in a comparison table of digital evidence found.

2. METHODOLOGY

2.1 Research Scenario

This scenario is shown to be able to explain how the steps or methods of the forensic stage on Android are to look for digital evidence that will be investigated by the investigative team. This research scenario uses a laptop and smartphone, where the smartphone will be used by the suspect to create a

fake email and fake Facebook account using fake personal data, the perpetrator uses the account to post pictures and also words that lead to cyber harassment using an account. After that, the post was widely discussed, therefore the perpetrator deleted the post of the image and words on purpose to be able to remove digital traces, the perpetrator's account and email of the perpetrator were also deleted to remove traces, and a laptop would be used by investigators to identify the post based on forensic stage. The flow of the case simulation can be seen in Figure 2.

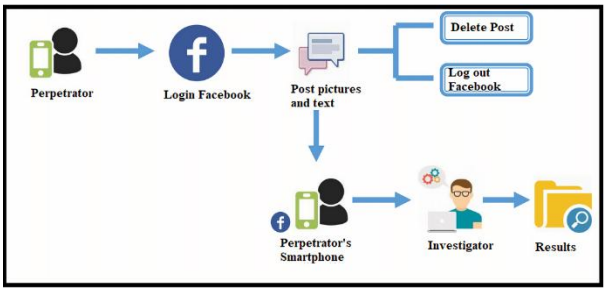

Figure 2.Research Scenario on Facebook

The perpetrator created a new Facebook account on his smartphone and then uploaded a post in the form of text and images, the post was deleted after a lot of discussion on Facebook, the perpetrator deleted his account from the smartphone. The investigator will take over or digital evidence belonging to the perpetrator, namely a smartphone, the investigator will carry out several processes to carry out the investigation, namely rooting the smartphone perpetrator and will also create an imaging file using the MobileEdit Forensic tool, then an analysis will be carried out using the tool to obtain the goods. evidence in the form of posts that have been deleted by the perpetrator. The results of the evidence displayed will be carried out with a comparative analysis table of digital evidence using forensic tools, which can later be delegated to the court if needed.

2.2 Research Stages

This research requires several methods to prepare the necessary reports to complete the research process. The method used to analyze a case is the NIST forensic stage. This stage has 4 steps, namely Collection, at this stage the investigation party will collect evidence, then the smartphone will be rooted using Odin then it will be Backup data on the smartphone using MOBILedit Forensic, the next stage is the Examination stage, at this stage data acquisition is carried out Facebook uses the MOBILedit Forensic tools, the results of the acquisition are in the form of pdf, Excel and CSV data, then the next stage is the analysis stage at this stage analysis is carried out using a PDF file from the Facebook data acquisition at the examination stage, then using the DB Browser for SQL lite tool to analyze the database contained in the smartphone backup results, then the final stage is the reporting stage, at this stage comparison of the evidence found will be carried out.

2.2.1 *Collection*

The collection stage is the initial preparation process in the form of tools and materials used by investigators to conduct investigations. At this stage, the initial evidence that has been obtained will be secured to maintain the authenticity of the evidence. The evidence that becomes the object of this research is an Android-based smartphone that has Facebook services installed. Other supporting media in the form of a data cable that is used as a connecting medium between a smartphone and a laptop that will be used as a tool for conducting investigations, and other tools, namely a laptop, there is an Odin application for smartphone rooting, the MOBILedit forensic tool for creating imaging files and obtaining data. Facebook as the social media application to be used, SQL lite tool is used to open the database file, and lastly, the Hash tool is used to match the code on the evidence found to find out whether the evidence is genuine or has been altered. The tools and materials in this study can be seen in Table 1.

Table 1. Tools and materials used for research

Tools and materials	Description
Smartphone	Samsung Galaxy J5
Laptop	Acer Apire Z3-451 OS Windows 10, AMD A10-5757M APU with Radeon ™ AMD Radeon HD 8650G + AMD Radeon Graphics Processor SDI (0x990B)
Data Cable	Smartphone link with laptop
Odin V3.14.4	Support application to root smartphone
MobileEdit Forensic Express Pro V 7.2.0.17975 (64-bit)	File imaging application for digital evidence search
Db Browser for SQLite	Smartphone database file analysis application
Hash Tool	Application for hashing image and text files
Facebook Mobile	Social Media Apps

Evidence in the form of a smartphone that is not rooted and will be rooted by the investigator team, and a data cable that will be used to connect a smartphone device to a laptop when creating imaging files using the forensic tools MobileEdit Forensic Express Pro. The evidence that has been secured by the police and submitted to the investigator team for investigation can be seen in Table 2.

Table 2. Perpetrator's Evidence

No	Name	Image	Description
1	Smartphone		Samsung Galaxy J5, connected in a network condition not rooted
2	Data Cable		Cableis used to connect the smartphone with the laptop

Table 2 contains evidence found by investigators and will be used to search for data in the form of a Samsung Galaxy J5 smartphone and a data cable that will be used to connect the smartphone to a computer.

2.2.2 *Examination*

Examination Stage At this stage, an examination or data acquisition is carried out on the imaging files that have been collected at the Collection stage, then data acquisition will be carried out using the MOBILedit Forensic tool. The first step in the acquisition is to select application analysis in MOBILedit, then look for the application you want to analyze, namely the Facebook application, then choose the format to be used, there are PDF, Excel, Html formats and also enter investigator information in the form of investigator's name, email, and phone number. Then extract it. The location of the data acquisition analysis file on the Facebook application can be seen in Figure 3.

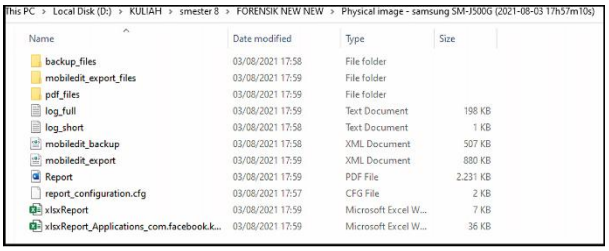

Figure 3.Facebook Application Analysis File

Figure 3 shows the results of the acquisition from Facebook in the form of PDF and Excel data files, there are also backup folders and also the original folders resulting from data acquisition, in that folder there are several files including Newsfeed files, database files, caches, etc. The files obtained will be analyzed using the MOBILedit Forensic forensic tool and also DB Browser for SQLite. In the PDF file, information on the perpetrators, digital evidence in the form of images, and also text evidence was found.

2.2.3 *Analysis*

This stage discusses the PDF file resulting from Facebook's data acquisition on the MOBILedit tools that have been backed up at the inspection stage, in the PDF file there is digital evidence in the form of images and digital evidence in the form of text, then to analyze the database file using the Db Browser for SQLite tool. The file to be analyzed in the DB Browser tool is located at D:\COLLEGE\smester 8\FORENSIK NEW NEW\Physical image - Samsung SM-J500G (2021-08-03 17h57m10s) \backup_files, the file is a backup file on the MOBILedit Forensic tool, and then the CSV file analysis will be carried out using a simple program, the program can only display CSV files and search for CSV files.

2.2.3.1 MOBILedit Forensic Express

The results of data acquisition in a PDF file obtained with the forensic tool MOBILedit express, showing an account with the name Bakalele used by perpetrators to commit cybercrimes of harassment, and there is also information about perpetrators who posted posts mixed with harassment, namely gender: female, birthday: 2000-07-08, telephone number: +6287736562310, and email address Bakalele0@gmail.com also found the perpetrator's profile photo in the form of a URL link stored in a PDF file. The view of the perpetrator's account can be seen in Figure 4.

Figure 4. Facebook Account Information

The process of searching for digital evidence that has been deleted by the perpetrator in the form of a post in the form of an image and also a post in the form of text, the post in the form of an image has been successfully returned by the MOBILedit forensic tools while the post in the form of text cannot be returned using the MOBILedit tools so that database analysis will be carried out using DB Browser for SQLiteThe display of evidence in the form of posted images can be seen in Figure 5.

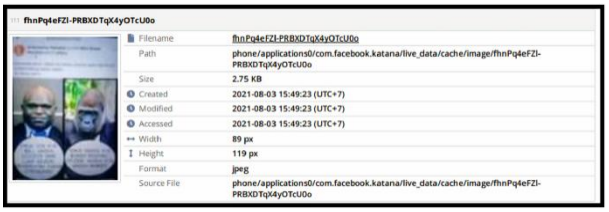

Figure 5. Information on posting pictures on MOBILedit

Figure 5 is an analysis of the pdf file in the post in the form of an image that was successfully returned, the location of the post is located on phone/applications0/com.facebook.katana/live_data/cache/image/fhnPq4eFZlPRBXDTqX4yOTcU0o,when you open the file in the folder, you will get an image post that has been uploaded. deleted. The information contained in the image is in the form of file name information, file location, file size, date edited and also the date on which the file was accessed, the height and width of the file, and also the file format.

2.2.3.2 DB Browser ForSQLLite

At this stage the post to be analyzed is in the form of text contained in the newsfeed_db database, to open the database file on the DB browser tools, you can select the open database menu on the DB browser then select the newsfeed_db file stored in the reporting file located at \applications0 \com.facebook katana\live_data\ databases. The display of the top stories file on the DB Browser for SQL Lite tool can be seen in Figure 6.

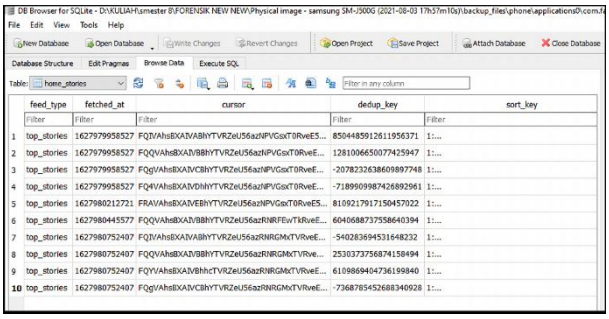

Figure 6. Location of text posts in Db Browser

Figure 6 shows the location of the post file in the form of text, the top_stories file 1627980752407 stored in the perpetrator's smartphone database, the location of the file is at /data/user/0/com.facebook.katana/files/NewsFeed/A0/f3cb52fa-dcd5-4a43-ac46 -60bf275a6e5d. The file is a post in the form of text posted by the perpetrator and the post was intentionally deleted from the Facebook account, the file can only be opened using the Notepad application on the laptop, but the file cannot be read clearly. The text post is in the form of "you are ugly, items are rich in charcoal, dirty, you don't deserve to be in this world, just die there".

2.2.3.3 Search Program

This search program is a simple program that is used to open and search for data in CSV format files where the file is

obtained at the examination stage. This simple program can display CSV formatted files in tabular and regular form so that they are easy to read, and also this searching program can search for data using ID, in the CSV format file, this searching program can make it easier to read CSV files that were originally irregular to be neater with tables, and also makes it easier to find data in CSV files. The initial appearance of the searching program can be seen in Figure 7.

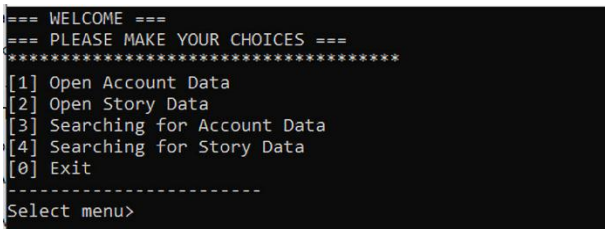

Figure 7. The search programstart screen

Figure 7 is the initial view of the searching program, there are menu options that can be selected by entering numbers according to the menu you want to display. The first menu is opening account data, on the menu when displayed it will open a CSV file containing the perpetrator's Facebook account in the form of id, label, gender,birthday, phone number, email, account picture, and also path. The menu display opening the account data can be seen in Figure 8.

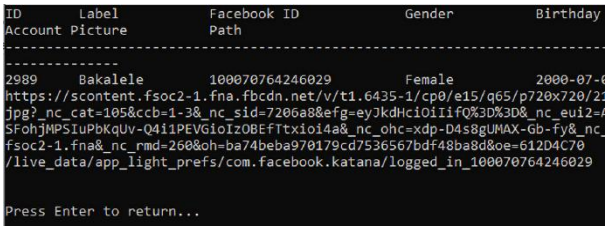

Figure8. Menu display opens onaccount data

The menu display opens the account data in Figure 8, it can be seen that the account picture data is very long so that the data path is not in the right place. At the end of the program there is a command to return to the menu display by pressing the enter key. The second menu is opening the data story, by entering command 2 then the data story menu display will be opened. The data contained in the menu is in the form of post data in the form of text and also images that have been posted by the perpetrator, the data in the form of id, label, paths, as well as tables. The data story menu display can be seen in Figure 9.

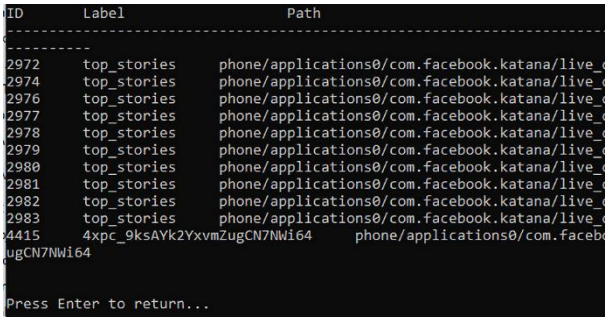

Figure 9. Story data in menu display

Figure 9 is a menu display that opens the story data on the second menu, there is an image or text post id, label, and path. The path is the location where the top_stories data and images are stored and there is also a table. On the label that says top_stories is a post in the form of text while the label that says "4xpc_9ksAYk2YxvmZugCN7NWi64" is a post in the form of an image, the label on the pictorial post has no data according to the CSV file. At the end of the data, story menu displays there is a command to return to the main menu by pressing the enter key. Next, look at the searching view in Figure 10.

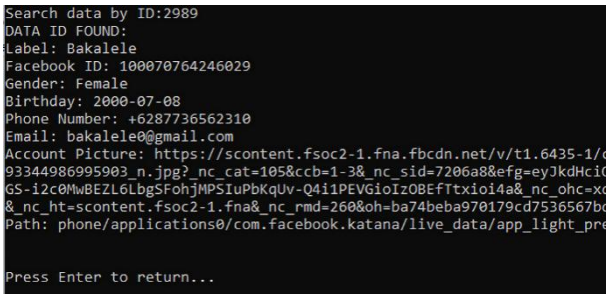

Figure 10. Display looking for account data using id

The menu display searching for account data on the third menu, namely searching for data using an id contained in the CSV file, the first display of this search menu is a command to search for data using an id, by entering the appropriate id it will display search results in the form of a label, Facebook id, gender, birthday, phone number, email, account picture, and path according to the id you are looking for, whereas if you enter an id that does not match the CSV file, what will be displayed is the data-id not found. The display of the search data story menu can be seen in Figure 11.

Figure 11. Display menu search for account data using id

The fourth menu is the display of the searching data menu contained in the CSV file, when entering the command to open this menu it will display a commanding display to enter the id contained in the CSV file, if the id entered is correct it will display the data label, path and also tables. Furthermore, if the input id does not match it will display the data-id not found. At the end of the display, there is a command to return by pressing the enter key, and you can select command 0 (exit) in the start menu to exit the program.

2.2.3.4 Hashing

Hashing in this study aims to investigate the integrity of the data on the digital evidence found so that the evidence is original and no modifications or changes are made. The initial hashing results can be matched with the final hashing results with a CSV Hashing file to ensure the authenticity of the data from the evidence found. The FileHashing data display can be seen in Figure 12.

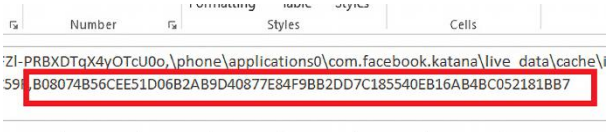

Figure 12. CSV FileHashes ofView

In this hashing process using the hash tool, the digital evidence found is stored in a PDF file resulting from the acquisition in the Inspection process using the MOBILedit Forensic Express tool. which will be checked for authenticity is proven to be in the form of pictures and writings, it can be

seen the results of hashing evidence in the form of images in Figure 13.

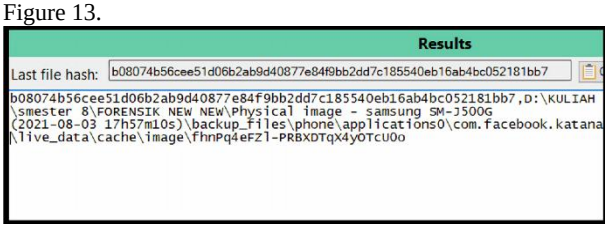

Figure 13. Hashing Results on Image Files

Figure 13 explains that the results of hashing using hash tools, the results of digital evidence images found have similarities with the CSV file hashes file, meaning that the file is original and has not been modified. The algorithm code obtained is"B08074B56CEE51D06B2AB9D40877E84F9BB2DD7C185540EB16AB4BC052181BB7". Furthermore, the results of the text file can be seen in Figure 14.

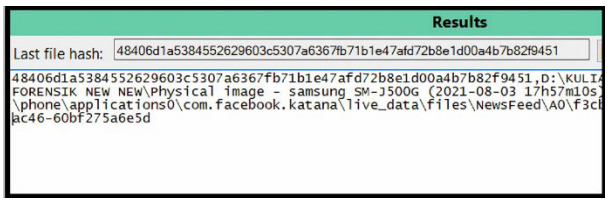

Figure 14. Hashing Results on Text Files

In Figure 14, it can be concluded that the results of hashing using hash tools, the results of the digital evidence text found have similarities with the CSV file hashes file, meaning that the file is original and has not been modified. The algorithm code obtained is"48406D1A5384552629603C5307A6367FB71B1E47AFD72B8E1D00A4B7B82F9451".

2.2.4 *Reporting*

The reporting stage or the reporting stage is the final stage of this research after obtaining evidence and also analyzing the evidence found using forensic tools. At this stage, reporting and comparison of the evidence obtained are carried out based on the MOBILedit Forensic tools, and Db Browser for SQL Lite. Reports and comparisons can be seen in Table 3.

Table 3.Comparison of digital evidence with tools

Comparison of Evidence found		
Information	**MOBILedit Forensic**	**SQLite DB Browser**
Recover Facebook account	✓	✖
Show Facebook account data	✓	✖
Showing the location of the text post	✓	✓
Show image location	✓	✖
Open image post	✓	✓

Based on Table 3, it can be seen a comparison of two forensic tools and one simple program, with the first information on the forensic MOBILedit tool being able to recover a Facebook account while DB Browser cannot recover a Facebook account, the second information for the MOBILedit forensic tool can display account data while DB Browser cannot display data account information, information on the three MOBILedit forensic tools, and the DB Browser can display the location of the post in the form of text, information on the three MOBILedit Forensic tools can display the location of the post in the form of an image, while the DB Browser cannot display the location of the post in the form of an image and the latest information, namely the MOBILedit Forensic tools and DB Browser can open a post in the form of an image with a URL.In this explanation, it can be concluded that the MOBILedit Forensic tool can display forensic evidence that has been deleted.It is hoped that in the future someone will develop this research with other social media services or other forensic methods or develop this research using different tools.The evidence obtained from the two tools can be charted as shown in Figure 15.

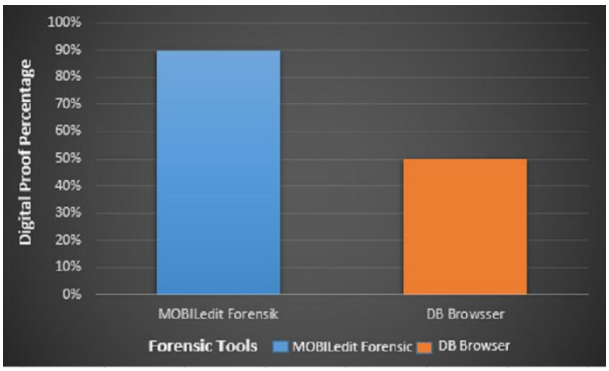

Figure 15. Chart of Digital Evidence

Figure 15 shows a comparison graph between the results of digital evidence found in the MOBILedit forensic tools and DB Browser for SQL lite. The picture shows that the blue chart is a forensic MOBILedit tool and the orange chart is a DB Browser tool.

3. CONCLUSION

The forensic process carried out with harassment cases on mobile-based Facebook services has succeeded in obtaining digital evidence in the form of the perpetrator's account, and postings in the form of images using the MOBILedit forensic tools while the posts in the form of text cannot be opened but the DB Browser for SQL lite tool can display the stored location post file in the form of the text. The percentage of results obtained is based on two tools, namely the MOBILedit forensic tools 90% while the DB Browser tools 50%. The search for digital evidence refers to the stages of the National Institute of Standards and Technology with four stages used, namely collection, examination, analysis, and reporting. It is hoped that in the future someone will develop this research with other social media services or other forensic methods or develop this research using different tools.

4. REFERENCES

[1] DailySocial.id (August 1, 2012) Facebook user data from SocialBakers Updated, Indonesian Facebook users Up 1.27%.

[2] Waedhani FOK, Sarwosri S, Esti RN. Status Filtering Application and Comments on Facebook. J Tek ITS.2016;5(2):6-8. Doi:10.12962/j23373539.v5i2.19605

[3] M. Fitriana, K. A. AR, and J. M. Marsya, "Application of the National Institute of Standards and Technology (Nist) Methods in Digital Forensic Analysis for Handling Cyber Crime," Cybersp. J. Educator. Technol. Inf., vol. 4, no. 1, p. 29, 2020, doi:10.22373/cj.v4i1.7241.

[4] I. Anshori, K. E. Setya Putri, and U. Ghoni, "Analysis of Digital Evidence for Facebook Messenger Applications on Android Smartphones Using the NIJ

Method," IT J. Res. Dev., vol. 5, no. 2, pp. 118–134, 2020, doi:10.25299/itjrd.2021.vol5(2).4664.

[5] W. A. Mukti, S. U. Masruroh, and D. Khairani, "Analysis and Comparison of Forensic Evidence for 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.

[6] R. Y. Prasongko, A. Yudhana, and A. Fadil, "Forensic analysis of the KakaoTalk application using the National Institute Standard Technology method," Semin. Nas. information. 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 Novemb. 2018 ISSN 1979-2328, vol. 2018, no. November, pp. 129–133, 2018.

[7] P. W,I. Riadi, Sunardi, "Investigating Cyberbullying on WhatsApp Using Digital Forensics," Engineering Sist. and Technol. Inf., vol. 4, no. 4, pp. 730–735, 2020.

[8] M. R. Setyawan, A. Yudhana, and A. Fadlil, "Identification of Skype Digital Evidence on Android Smartphones Using the National Institute Of Justice (NIJ) Method," Semnastek, pp. 565–570, 2019.

[9] Asrizal. 2019. Digital Forensics. Ministry of Religion E-Documents.

[10] MN Faiz, R. Umar, A. Yudhana, and UA Dahlan, "Analysis of Live Forensics for Comparison of Email Security in Proprietary Operating Systems," J. Ilm. Ilk., vol. 8, no. 3, pp. 242–247, 2016.

[11] Rachmie S. Digital Website.2020;21(1):104-127.

[12] V. Rosalina, A. Suhendarsah, and M. Natsir, "Data Recovery Analysis Using Forensic Software: Winhex and X-Ways Forensic," PROSISKO: Journal of Research Development and Computer System Observation, vol. 3, no. 1, pp. 51-55, 2016.

[13] Warsito A, A "Analysis of Autopsy Performance on Android-Based Smartphones Using NIST Measurements". 2020.

[14] A. Yudhana, R. Umar, and A. Ahmadi, "Google Drive Forensic Data Acquisition on Android Using the National Institute of Justice (NIJ) Method," vol. X, no. X, pp. 8–13.

[15] S. Madiyanto, H. Mubarok, N. Widiyasono, T. Informatika, F. Teknik, and U. Siliwangi, "MOBILE FORENSIC INVESTIGATION PROCESS ON SMARTPHONE BASED ON IOS INVESTIGATION PROCESS," vol. 4, pp. 93–98, 2017.Negara,

[16] R. Firmansyah, M. Akbar, and S.E, "mobile forensics data recovery in instant messaging," *J. Geol. soc. Japan*, vol. 61, no. 718, pp. 324–325, 2017.

[17] Casey, E. "Digital Evidence and Computer Crime: Forensic Science, Computer and Internet (3rd edition)".California: Elsevier Inc.2011

[18] Ashiq, S., Majeed, S., & Malik, F. (2016). Psychological predictors of cyber bullying in early adulthood. Health Science Journal, 10(3), 1.

[19] Murphy, J., Link, MW, Childs, JH, Tesfaye, CL, Dean, E., Stern, M., et al. (2019). Social media in public opinion research: Report of the AAPOR task force on emerging technologies in public opinion research. American Association for Public Opinion Research.

[20] Abhyankar, A. (2019). Social networking sites. SAMVAD, 2, 18-21.

[21] Sagrista, M., &Matbob, P. (2016). The digital divide in PNG: Implications for journalism education. Pacific Journalism Review.

[22] Safaat H, Nazruddin 2011. Programming Mobile Smartphone and Tablet PC Applications Based on Android. Informatics Bandung: Bandung.

[23] Umar R, Sahiruddin. NIST Methods for Forensic Analysis of Digital Evidence on Android Devices. Proceedings of SENDI_U 2019 ISBN: 978-979-3649-99-3.

[24] A. Nofiyan, "Forensic Analysis on Web Phishing Using National Institute of Standards and Technology Methods," vol. 4, no. 02, 2020.

[25] A. Ahmadi *et al.*, "Comparation Of Forensic Tool Results On File Image Smartphone Comparison Of Forensic Tool Results On Android Smartphone," vol. 4, no. 2, pp. 92–97, 2021, doi:10.33387/jiko.