HASIL CEK_60020397_Point-C15-IRD-850GB-Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method

by Imam Riadi 60020397

Submission date: 11-Dec-2020 09:47AM (UTC+0700)
Submission ID: 1471638733
File name: plication_using_the_National_Institute_of_Justice_NIJ_Method.pdf (913.17K)
Word count: 4112
Character count: 22129

International Journal of Computer Applications (0975 – 8887)
Volume 177 – No. 27, December 2019

Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method

Hijrah Nurhairani
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Twitter is a social media that can be used on platforms using desktop, web, android smartphones and iOS, but lost of Twitter users are currently using the Android platform. The large number of Twitter user makes Twitter inseparable from crime or cybercrime, including pornography, online gambling, Hate speech, cyberstalking, cyber-tresspass, and cyberbullying. This research uses the method of the National Institute of Justice (NIJ). NIJ is a method with five stages, namely identification, collection, examination, analysis, reporting. This study uses two smartphones with different conditions, those are the rooted smartphone and the non-rooted smartphone. Evidence that has obtained from these two conditions will be read by a database using forensic tools. This research gives a comparison between the evidence with a smartphone that has been rooted and a smartphone that has not been rooted. The conditions of the rooted smartphone are found in the form of 2 user participants, 3 chat messages and 1 image, location, and profile of the perpetrators, while on the non-rooted smartphone only get 1 APK file. Evidence in the form of a conversation that obtained from a non-rooted smartphone proves the existence of the hate speech between the perpetrator and the victim.

Keywords

Forensic, Mobile, Twitter, NIJ, Hate Speech

1. INTRODUCTION

Along with the development of the times, and technological advances that exist today, can introduce to social media, social media is a communication tool that is most often used by society today, social media can break the distance, space and time in terms of communication. The use of social media continues to grow from various circles, both from children to adults, on average already have social media, this is not immune from the development of an age that continues to progress and develop, it can be said that everyone already has a social media account. In average Indonesian spends 3 hours 23 minutes a day to access social media [1]. One of the social media that society often to use is Twitter. Twitter is a personal matter where a person shares their stories, opinions, activities, with chosen people [2]. Twitter is a social media that can be accessed using the Desktop, web, Android and iOS platforms, but now days many people are using android platform to access it. There are 120 million Indonesians use mobile devices, such as smartphones or tablets to access social media, with a 45 percent percentage. Within a week, online social media activities via smartphones reached 37 percent as in Figure 1.

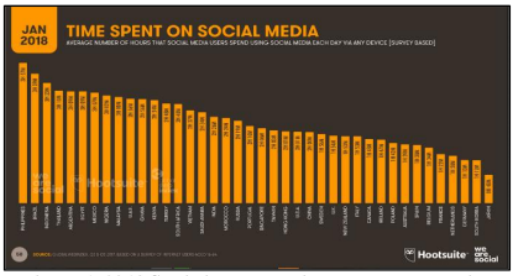

Figure 1. 2018 Statistical data using smartphone social media

Cybercriminals continue to change their strategy to move to fast-growing social media. Broadcasting social media and instant messaging in cellular services allow cybercriminals to use this service for malicious purposes [3]. Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cyber crimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some cyber crimes do both -- i.e., target computers to infect them with viruses, which are then spread to other machines and, sometimes, entire networks. [4]. The main impact of cybercrime is finance, and cybercrime can include various types of criminal activities that are driven by profits, including ransomware attacks, email fraud, internet and identity fraud, and attempts to steal financial accounts, credit card or other payment card information. Cybercriminals can target personal information, as well as company data for theft and resale. The most widespread impact of cybercrime in early 2019 was the spread of hoaxes and the spread of hate speech through on social media

This research by using the Twitter application that runs on the Android platform using the National Institute of Justice (NIJ) metode. The National Institutes of Justice (NIJ) is the research, development, and evaluation agency of the Department of Justice of the United States. The Institute's mission is to advance scientific research, development, and evaluation to enhance the administration of justice and public safety [5].

1.1 Literature Review

1.1.1 Previous Studies

This research was conducted by conducting several previous studies. This activity is carried out to review the data that has been checked before, among others were found and relevant to this research. Ammar Fauzan, Imam Riadi & Abdul Fadlil (2016) conducted research related to "Digital Forensic

Analysis on Line Messenger for Handling Cybercrime" which makes a good investigation and elevation process to prove digital on Line Messenger on Android smartphone devices. [6].

Nuril Anwar & Imam Riadi (2017) conducting research related to "WhatsApp Messenger Smartphone Forensic Investigation Analysis of WhatsApp Web-Based" that produced this research has shown that a person can get complete access to all information on WhatsApp, both WhatsApp smartphone and WhatsApp We [7]. Imam Riadi, Anton Yudhana & Muhamad Caesar Febriansyah Putra (2018) conduct research related to "The acquisition of digital evidence on Android-based Instagram Messenger using the National Institute of Justice (NIJ)" method that results in the acquisition of digital evidence that was successfully obtained on Instagram on smartphones in the root condition [8]. Rauhulloh Ayatulloh Khomeini Noor Bintang, Rusydi Umar & Anton Yudhana (2018) conduct research related to "The Design of Comparison of Live Forensics on Social Media Security Instagram, Facebook and Twitter on Windows 10" that produce data on social media in the form of original data that has been valid [9]. Wisnu Ari Mukti, Siti Ummi Masruroh, Dewi Khairani (2019) conduct research related to "Analysis and Comparison of Forensic Evidence Facebook and Twitter Social Media Applications on Android Smartphones" which found all the evidence from the Facebook application while the Twitter application is only partially [10].

1.1.2 Digital Forensic

Digital forensics, the art of recovering and analyzing content found on digital devices such as desktops, notebooks / netbooks, tablets, smartphones, etc., was little known a few years ago. However, with the increasing of incidence of cybercrime, and the increasing of adoption of digital devices, this branch of forensics has gained significance in the past, adding to what is conventionally limited to the recovery and analysis of biological and chemical evidence during criminal investigations [11]. Digital Forensics is the application of computer science and technology for the purposes of provi law, which in this case is proving high technology or computer crimes scientifically to be able to obtain digital evidence that can be used against violators. Digital forensics has many fields, one of it which is Mobile Forensics [12]. Digital forensics is, in essence, able to find digital evidence that can be stored on temporary computer storage, permanent storage, USB, CDs, network traffic, etc. [13].

1.1.3 Mobile Forensic

Mobile Forensics is the science that carries out the process of recovering digital evidence from cellular devices using methods that are in accordance with forensic conditions [14]. The use of mobile devices such as smartphones with various types and operating systems for crime has increased in number, but the presence of forensics for mobile devices can help to deal with criminal cases relating to mobile devices, especially smartphones [15].

1.1.4 Digital evidence

Digital evidence related to digital crime such as those that help social media the place to commit crime, so digital evidence is used to assist in prosecuting all types of digital crimes [16]. Digital evidence is ver vulnerable to change so that it can affect its authenticity if not handled properly. All types of changes that contain digital evidence will lead to wrong conclusions, or evidence will not be useful [17].

1.1.5 Hate Speech

Hate speech or hate speech is an utterance that is done by a person or group of people to a certain person or group that can indirectly hurt someone's heart or lead to cases of bullying.

a circular issued by the National Police Chief stated that hate speech can be in the form of criminal acts regulated in the Criminal Code (KUHP) and other criminal provisions outside the Criminal Code, which take the form , among others, insults, defamation, misconduct pleasing, provoking, inciting, and spreading false news, and all of these actions have a purpose or can have an impact on acts of discrimination, violence, loss of life, and / or social conflict [18]

2. METHODOLOGY

1.2 Research Scenario

The research scenario aims to explain the mobile forensic stages that occur on Twitter social media. In this research scenario, there are two people who act as perpetrator and victims who are communicating via smartphone and have previously installed the android twitter application and have conversations using the Direct Messenger feature or secret chats that cannot be seen by other users. The conditions on the smartphone of the offender and the victim are different, namely the perpetrator has been rooted while the victim is not rooted, the conversation between the perpetrator and the victim is indicative of cybercrime acts, which contain hate speech, as shown in **Figure 2.**

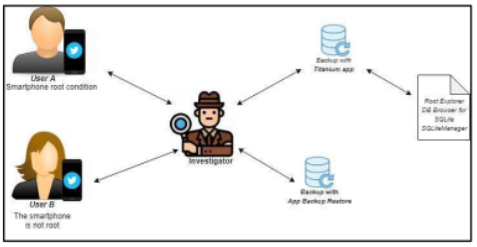

Figure 2. Research Scenario

The scenario in the illustration above that User A with the condition of the smartphone is rooted as the perpetrator communicates with User B with the condition that the smartphone is not rooted as a victim using a smartphone with the Twitter application installed on it, all the conversations that they have traced on their respective device accounts. The backup process on User A's smartphone uses the Titanium application and User B's smartphone uses the App Backup Restore application, and the database reading uses the DB Broswer for SQLite application which can help restore the data that the perpetrator tries to remove but still following standard forensic steps and does not change the content from the device being analyzed.

The initial step in conducting this investigation is to run the Titanium Application to backup data on a rooted smartphone, run the App backup & restore application on a rooted smartphone and read the database using the DB Browser for SQLite, SQLiteManager, and Root Explorer applications to obtain the goods proof.

1.3 Analysis Research

Analysis of rainy research to make a simulation of the design of the search for evidence that occurred on social media Twitter which in this case occurred when the perpetrators sent

hate speech to the victim through Direct Messenger and the way the investigator revealed the evidence as shown in Figure 3.

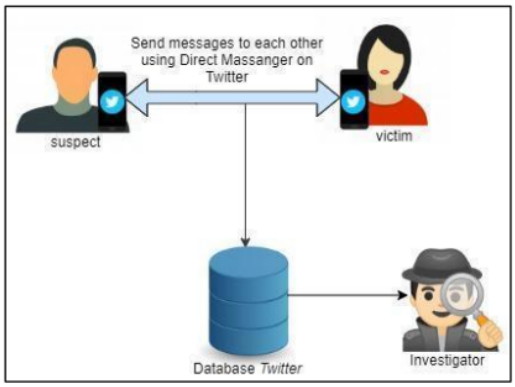

Figure 3. Simulation scheme of evidence search

1.4 Research Stages

The research phase seeks to simulate a case and become a reference for conducting an investigation. The following figure 4 is the National of Justice (NIJ)

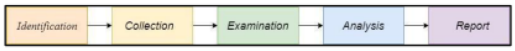

Figure 4. Method National of Justice (NIJ)

The stages in the National of Justice (NIJ) method are carried out sequentially in accordance with established procedures, in order to obtain the evidence that appeared, while the stages of the National Institute of Justice (NIJ) method consist of identification, collection, examination, analysis and reporting. But this research starts from the stages of Examination, analysis and reporting.

1.4.1 Identification

Identification is the process of preparing the equipment used in the investigation stage by the investigator, which at this stage all evidence such as a smartphone along with the data cable from the victim and perpetrator is secured, in order to protect the authenticity of the evidence.

In facilitating the stages of identifying problems that have occurred between the victim and the perpetrator, the investigator makes an investigation flow in order to obtain evidence that has removed by the perpetrator. The investigation flow is conducted as in Figure 5.

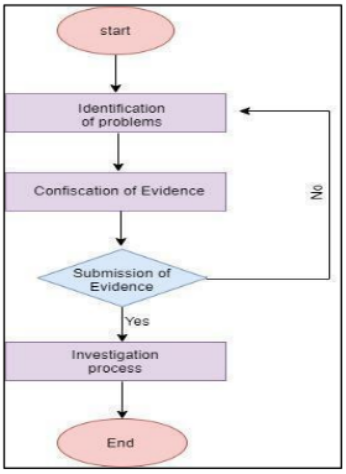

Figure 5. Flowchart Investigation flow

The following is an explanation of the investigation flow to reveal evidence, as shown in Figure 5. Flowchart Investigation flow

a) Identification of the problem, it is done by the authorities in order to know the details of the problem that occurs with victims and perpetrators

b) Confiscation of evidence, it is done to secure the evidence that the offender will try to keep on trial and keep it in its original state

c) Investigation process, it is done when the authorities submit evidence to the investigator to carry outcome an investigation in order to obtain evidence.

2.3.2. Collection

Electronic evidence in the form of a smartphone with an Android operating system that has been installed with the Twitter application which is a communication tool used to indicate cybercrime crime. Then in addition to that found evidence of the data cable used by the perpetrator to charge his cellphone, this data cable evidence can help connect the smartphone to the PC, which is used in proving evidence. The following the following are the evidences that have collected, can be seen in Table 1

Table 1. Evidence

No	Name of evidence	Image	Information
1.	Smartphone 1	 **Figure 5.** Smartphone 1 with root condition	Smartphone 1, Brand Xiomi 4i is alive, connected to the network and is already rooted.

2	smartphone data cable 1	 **Figure 6.** smartphone data cable 1	Data cable that is still connected to the smartphone
2.	Smartphone 2	 **Figure 7. Smartphone 1 with not root condition**	Smartphone 2, Merk Vivo 1902
3.	smartphone data cable 2	 **Figure 8.** smartphone data cable 2	Data cable that is still connected to the smartphone

After successfully collecting evidence used by the perpetrators, then the evidence is given to the investigator for an investigation.

2.3.3 Examination

The data checking stage on the electronic evidence of cybercrime crime can be carried out by performing the data backup process that exists on the smartphone. This process performs data backups using Titanium Backup tools for root smartphones and Apps Backup & Restore for non-rooted smartphones.

2.3.4 Analysis

This stage is the stage to write the results of the investigation process and the data obtained from all investigations. The report contains the results of the identification of the extracted image file from the evidence of smartphones are rooted and smartphones are not rooted. This reporting process will also be brought to the trial process and must include all evidence found in the physical form and obtained from the forensic process.

2.3.5 Reporting

The results of the analysis have been obtained using the DB Browser fo SQLite application, SQLiteManager, Root Explorer. The data that was successfully obtained became digital evidence from a smartphone attached to Twitter.

3. RESULT AND DISCUSSION

Rainy research to make a design simulation of the finding evidence that occurred on social media Twitter which in this case occurred when the perpetrator sent hate speech or Hate speech to the victim through Direct Messenger and the way the investigator revealed the evidence. The tools and materials needed in this study can be seen in Table 2.

Table 2. Tools & materials needed

Tools & Materials	Information
Laptop	Merk Lenovo AMD E1-6010 APU with AMD Radeon R2 Graphics, OS Windows, 64-bit.
Smartphone 1	Xiaomi 4i brand, Android OS, in root condition.
Smartphone 2	Vivo 1907 brand, in a condition not rooted.
Kabel Data	Connecting Smartphone and Laptop
Titanium Pro	Backup root application.
DB Browser for SQLite **SQLiteManager** **Root Explorer**	Application for reading databases in applications
App Backup & Restore	Data Backup application is not root.

3.1 Examination

This stage is the data backup stage that is on the smartphone of the perpetrator and the victim of crime

3.1.1 Backup process on the root smartphone.

The backup process is done using the Titanium application, the backup process runs successfully using this application as shown in Figure 9

Figure 9. Successful backup process with Titanium

The backup process can be seen by using the Twitter 8.30. version

3.1.2 The backup process on the not rooted smartphone

Perform backups on smartphones that are not rooted, using the App Backup Restore application. App Backup & Restore is an application that can be used to backup and restore the installed apps, results of the backup are shown in Figure 10.

Figur 10. Successful backup process with app backup & restore

3.2 Analysis

3.2.1 Search for evidence on root smartphones

This process is carried out in order to obtain evidence in the form of a conversation between

the perpetrators and victims as well as other important evidence that can be identified, while the flowchart description for conducting the database reading process can be seen in Figure 11.

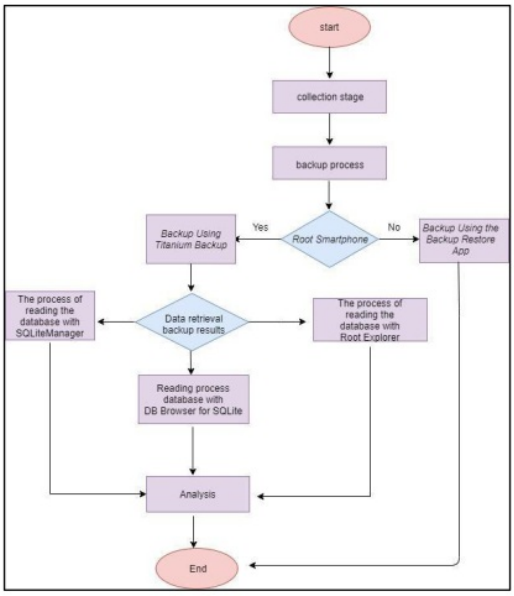

Figure 11. Database Reading Flowchart

Figure 11. Shows the flowchart for making evidence to find evidence

3.2.1.1. The process of searching for evidence with DB Browser for SQLite

The following is the evidence obtained using the DB Browser for SQLite application, shown in Figure 12

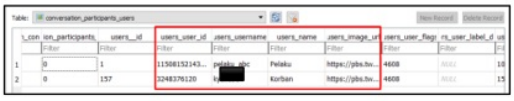

Figure 12. Evidence that was successfully obtained

In this application also managed to get evidence of conversation between the perpetrator and the victim, proof of conversation can be seen in Figure 13 and Figure 14

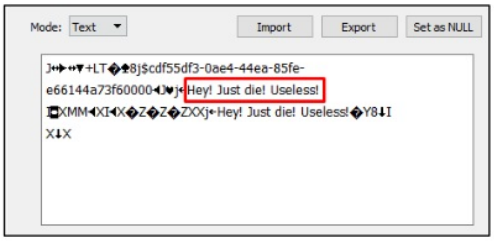

Figure 13. Evidence of the offender sending hate speech

Figure 13 shows the utterance of hatred that the perpetrator sent to the victim. This hate speech was successfully obtained from the conversation between the perpetrator and the suspect, the conversation sent by the perpetrator to the victim was not the only evidence but there was the other evidence where the perpetrator sent the hate speech to the victim, as shown in figure 14.

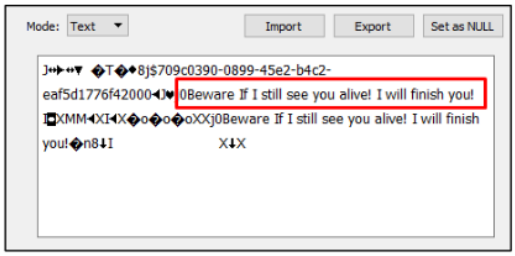

Figure 14. Evidence of the offender sending hate speech

Figure 14 shows evidence of hate speech sent by the perpetrator to the victim after the hate speech

3.2.1.2. The process of searching for evidence with SQLiteManager

In this application managed to get evidence in the form of a conversation with a profile of the perpetrators that can be seen as Figure 15, Figure 16 and Figure 17.

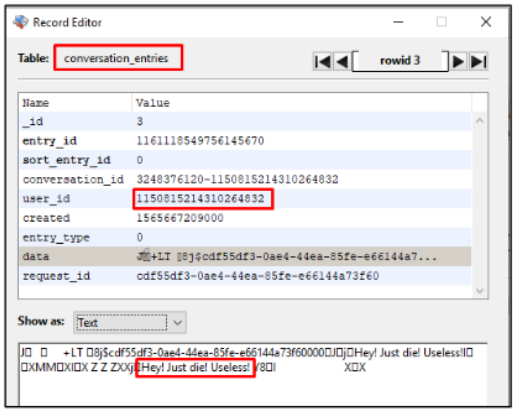

Figure 15. Evidence of hate speech conversations

Figure 15 explains the evidence that has been obtained.

The evidence is obtained from conversations between the victim and the suspect, when the suspect sends hate speech to the victim. The conversation in the form of hate speech that sent by the suspect is the very important evidence, which can prove the crime that occurred, hate speech that obtained as evidence can strengthen the existence of a crime in the form of hate speech committed by the suspect to the victim, evidence in the form of conversation can be seen in figure 16 and the evidence of the suspect's profile can be seen in figure 17.

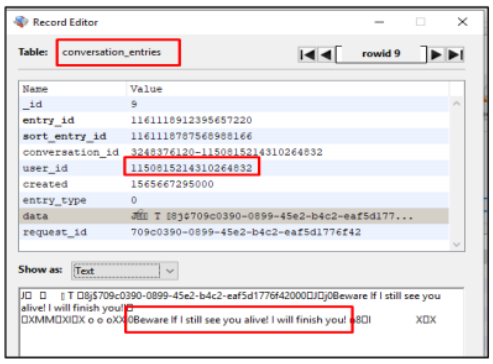

Figure 16. Evidence of hate speech conversations

Figure 16 shows evidence in the form of a conversation sent by the perpetrator to the victim

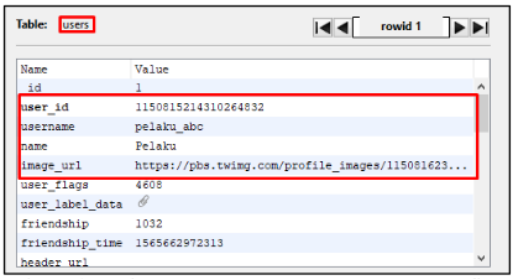

Figure 17. Evidence username, name and suspect profile

3.2.1.3. The process of searching for evidence with Root Explorer

In this application successfully obtained evidence in the form of user._id, username, image url and location of the suspect as shown in Table 3

Table 3. evidence the root explorer application

Type Data	Information
Pelaku_abc	**Id_user_name belongs to the suspect**
Pelaku	Usernames suspect
https://pbs.twimg.com/profile_images/1150816235157741568/2hQ_wgL1_normal.jpg	suspect photo url
Yogyakarta, Indonesia	suspect location

3.2.2. The non-rooted smartphone

3.2.2.1 Process of Finding Evidence

No evidence was found in the form of a conversation on a smartphone in a non-rooted condition. It is because when backing up backups are only in the form of applications, not databases. As shown in Figure 18.

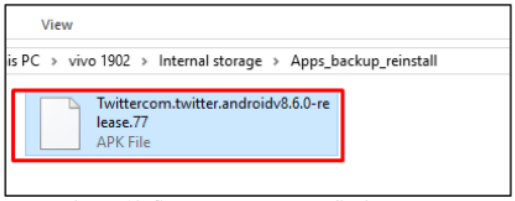

Figure 18. Smartphone backup file is not root

Describes evidence that has found on a non-rooted smartphone only in the form of an APK file.

3.3 Reporting

The results / information that were successfully obtained on the two smartphones that have been analyzed can be seen in Table 4. in table 4. The results of the report have been collected from the results obtained, using the DB Browser for SQLite, SQLiteManager and Root Explorer applications.

Table 4. Comparison of the results of evidence on the Rooted and Non-Rooted smartphone

Condition on smartphone	Tools	Suspect's username	Suspect's Id	Suspect's location	Suspect's Image	Conversation
Root	DB Browser for SQLite	✓	✓	–	✓	✓
	SQLiteManager	✓	✓	–	✓	✓
	Root Explorer	✓	✓	✓	✓	–
Non-Rooted	–	–	–	–	–	–

Based on the comparison of the results of evidence that has found as shown in table 4, the condition of the rooted smartphone shown the evidence in the form of the perpetrator's username, victim's username, id of the perpetrator, id of the victim, profile photo of the perpetrator, location and victim as well as the contents of the conversation between the two.the Proof on a non-rooted gets an APK file

4. CONCLUSION AND FUTURE WORK

Based on the results of the research on forensic evidence obtained from the results of the National Institute for Justice (NIJ) method stages, with the stages of identification, collection, examination, analysis, report using a smartphone rooted with DB Browser for SQLite, SQLiteManager, Root Explorer, goods evidence that can be found 2 user participants, 3 chat messages and 1 image, location, and profile of the perpetrators while the smartphone with non-root condition only gets 1 APK file. The Suggestions from this research can develop the finding evidence in the same case but using different methods or platforms

5. REFERENCES

[1] We Are Social., Digital in 2018. (2018) found on 13 October2018,fromhttps://wearesocial.com/blog/2018/01/global-digital-report-2018.

[2] Nurhadi, Z. F. (2017). Models of Youth Social Communication Through Twitter Media. ASPIKOM Journal. 3(3), (h 539).

[3] Arizona, Y., (2016). Live Forensic Analysis For Comparison of Email Security in Proprietary Operating Systems. ILKOM Scientific Journal, p (242).

[4] Rouse. M., (2018) Cybercrime. Identified 13 October 2018, from https://searchsecurity.techtarget.com/definition/cybercrime

[5] United Nations Office on Drugs and Crime Identified 10 Septembe2019,fromhttps://www.unodc.org/unodc/en/commissions/CCPCJ/PNI/institutes-NIJ.html

[6] Fauzan, A., Riadi, I., & Fadlil, A. (2017). Digital Forensic Analysis of Messenger Line for Handling Cybercrime. Annual Research Seminar (ARS), 2(1), 159-163.http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752

[7] Anwar, N., & Riadi, I. (2017). WhatsApp Messanger Smartphone Forensic Investigation Analysis of WhatsApp Web Based. Scientific Journal of Electrical Computer Engineering and Information Technology, 3(1), 1-10. https://doi.org/10.26555/jiteki.v3i1.6643

[8] Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2018). Acquisition of Digital Evidence on Android-Based Instagram Messenger Using the National Institute of Justice (NIJ) Method, 4, 219-227. https://doi.org/10.11591/ijece.v7i5.pp2806-2817

[9] Arizona, Y. (2018). Prosiding SNST ke-9 years 2018 Fakultas Teknik Universitas Wahid Hasyim 121, 121-124.

[10] Mukti, W. A., Masruroh, S.U., & Khairani, D. (2017). Analysis and Comparison of Forensic Evidence of Facebook and Twitter Social Media Applications on Android Smartphones. Journal of Informatics Engineering. 10(1), 73-84.

[11] Prasad, A., & Studies, E. (2016). Digital Forensics, (h. 182).

[12] Riadi, I., Rusydi, U., Firdonsyah, A., (2017). Idetification of Digital Evidance On Android's Blackberry Messenger Using NIST Mobile Forensic method. International Journal of Computer Science and Information Security, 15 (5), 3-8.

[13] Arizona, Y., (2016). Live Forensics Analysis For Comparison of Email Security in Proprietary Operating Systems. ILKOM Scientific Journal, p (242).

[14] Riadi, I., Rusydi, U., Firdonsyah, A., (2017). Idetification of Digital Evidance On Android's Blackberry Messenger Using NIST Mobile Forensic method. International Journal of Computer Science and Information Security, 15 (5), 3-8.

[15] Faiz, Muhammad Nur Umar, Rusydi Yudhana, Anton (2016). Live Forensics Analysis For Comparison of Email Security in Proprietary Operating Systems. ILKOM Scientific Journal, p (242).

[16] Riadi, I., Rusydi, U., Firdonsyah, A., (2017). Idetification of Digital Evidance On Android's Blackberry Messenger Using NIST Mobile Forensic method. International Journal of Computer Science and Information Security, 15 (5), 3-8.

[17] Albanna, F,. & Riadi, I,. (2017). Forensic Analysis of Frozen Hard Drive Using Static Forensics Method. International Journal of Computer Science and Information Security (IJCSIS), 15(1), 173-178.

[18] National Police of the Republic of Indonesia Headquarters., (2015) Circular of the National Police Chief Number SE / 6 / X / 2015 concerning Handling (Hate Speech) Hate Speech. Determined September 9, 2018,from http://surat-edaran-kapolri-tentang-penanganan-ujaran-kebencian-hate-speech/

HASIL CEK_60020397_Point-C15-IRD-850GB-Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method

ORIGINALITY REPORT

9%	9%	2%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.ijcaonline.org Internet Source	2%
2	Submitted to Canterbury Christ Church University Student Paper	2%
3	mafiadoc.com Internet Source	2%
4	www.unodc.org Internet Source	1%
5	karyailmiah.unisba.ac.id Internet Source	1%
6	Submitted to School of Business and Management ITB Student Paper	1%
7	Submitted to Binus University International Student Paper	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		