HASIL CEK_60010313_(6)

by Sunardi 60010313

Submission date: 10-Dec-2020 09:22AM (UTC+0700)
Submission ID: 1470443294
File name: CEK6_60010313.pdf (411.59K)
Word count: 4689
Character count: 25566

Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 4, No. 4, November 2019, Pp. 305-314

Live forensics analysis of line app on proprietary operating system

Imam Riadi*[1], Sunardi[2], Muhammad Ermansyah Rauli[3]
Universitas Ahmad Dahlan, Indonesia[1,2,3]

Article Info
Keywords:
Line, Live Forensics, Digital Evidence, RamCapturer, Digital Forensic

Article history:
Received 30 June 2019
Revised 29 July 2019
Accepted 28 August 2019
Published 30 October 2019

Cite:
Riadi, I., Sunardi, S., & Rauli, M. (2019). Live Forensics Analysis of Line App on Proprietary Operating System. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 4(4). doi:http://dx.doi.org/10.22219/kinetik.v4i4.850

*Corresponding author.
Imam Riadi
E-mail address:
Imam.riadi@is.uad.ac.id

Abstract
The development of computer technology is increasing rapidly. This has positive and negative effects. One of the negative effects that occurred was the use of Line applications to conduct online shop fraud. Line is one of the instant messenger applications that can be used on computers, especially on Windows 8.1 operating system computers. Applications that run on the computer leave traces of data on Random Access Memory (RAM). Data left in RAM can be obtained using digital forensic techniques, namely live forensics which is used when the computer is running and connected to the internet. This study aims to find digital evidence regarding cases of online shop fraud using the National Institute of Standards and Technology (NIST) method. Digital evidence can be obtained using forensic tools, namely RamCapturer, FTK Imager and Winhex. RamCapturer is used to acquire data in RAM, FTK Imager is used for imaging and Winhex is used to analyze data that has been taken. The results obtained in this study were conversational recordings consisting of conversation time, conversation content and conversation status which could be digital evidence in uncovering the online shop fraud crime that occurred.

1. Introduction

The crime rate by utilizing instant messenger (IM) applications is increasing [1]. One crime that often occurs is online shop fraud. This happens because the more easily the criminals communicate with victims using IM applications [2].

The IM application is one of the messaging applications that replaces the role of Short Message Service (SMS) which is very popular today [3][4], one of which is Line. Line is an IM application that can be used on mobile devices and computers [5]. Line has many features such as text / voice chat, photo, sending video and locaton, video call, group chat and timeline. According to Statista data, active Line users around the world in 2018 are 203 million [6]. The number of users allows Line to be used as a communication medium to commit a crime. Figure 1 shows Line user statistics in 2018 [6].

Applications that run on the computer leave data and information on Random Access Memory (RAM) [7]. RAM is a temporary storage place when the computer system is running and can be accessed quickly [7][8]. Therefore handling data and information on RAM must be done quickly and carefully because the data and information will be lost if the system dies [9]. This quick and careful handling is done so that the data and information contained in RAM that has the potential to become digital evidence can be obtained [10]. Efforts made to obtain digital evidence related to criminal cases that occur are known as digital forensics [11].

Digital forensics is the science and method for obtaining valid digital evidence relating to crime cases that occur so that it can assist law enforcement officers in completing a crime [12]. The required digital evidence can be obtained using live forensics techniques. Live forensics is used to handle computer crime when a computer system is running and connected to the internet network, because it requires data and information contained in RAM [13]. The process of taking data and information on RAM must be quickly carried out after the evidence is found [8][14]. This is done to avoid losing or changing digital evidence. This technique also guarantees data integrity without losing potential digital evidence [15].

Computers can be used when having an operating system. The operating system is divided into two, namely open source operating systems and proprietary operating systems [16]. This research uses Windows 8.1 proprietary operating system. Windows 8.1 is the latest version of Windows 8 which was released on October 18, 2013 [17].

Danang Sri Yudhistira, Imam Riadi, and Yudi Prayudi [8] conducted a study to live forensics analysis on RAM. This research is based on the number of cyber crime committed using a laptop. Information that can be obtained such as e-mail, user ID and password that all information is contained in RAM. The results obtained in this study are Facebook, PayPal, internet banking and bitcoin user IDs and passwords. The tools used to acquire are the Linux Memory Extractor (LiME) and FTK Imager.

Other research conducted by Tri Rochmadi, Imam Riadi and Yudi Prayudi [9] who used anti-forensics to complicate investigators in the investigation process. The anti-forensics process is carried out such as using a portable web browser that provides private mode features and deletes the registry. This study aims to obtain digital evidence using live forensics techniques related to the portable use of the Private Mode web browser and anti forensics by perpetrators. The results of this study are getting 3 digital evidence contained on the computer.

According to research conducted by Rushita Dave, Nilay R. Mistry and Dr. M. S. Dahiya [18] uses live forensics tools to get data and information on a system that is running on RAM. RAM is volatile memory that will disappear when the system turns off or restarts. Therefore, a quick handling is needed so that the digital evidence contained in the current system can be obtained.

In this study the author will conduct research using the desktop-based Line application on the Windows 8.1 proprietary operating system using live forensics to obtain digital evidence of online shop crime cases.

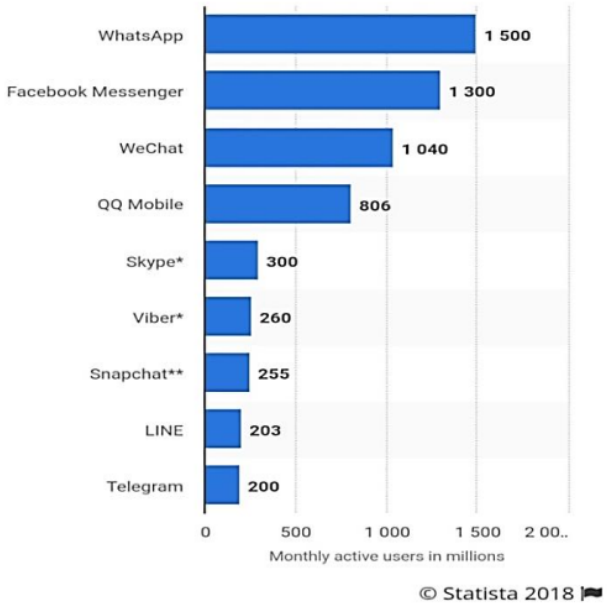

Figure 1. Line Users Statistic [6]

2. Research Method

2.1 Method

The method in this study refers to the forensic work steps developed by the National Institute of Standards and Technology (NIST). The agency is one of the bodies that develops standards, guidelines and requirements in information technology security. Its scope of work includes government agencies in the fields of law, law enforcement, forensics specialists and forensics examiners. The forensic work step of the National Institute of Standards Technology (NIST) is used to carry out the analysis stage of digital evidence or the stage to obtain information from digital evidence [19]. The NIST method consists of several steps, as shown in Figure 2 [19].

Figure 2. NIST Stages

1. Collection

   A series of activities to collect data to support the investigation process in search of evidence. The stage of digital data retrieval is a process undertaken to make the acquisition of conversation data. This process is carried out using acquisition tools that support live forensics techniques. Then the acquisition results obtained will be carried out the imaging process (doubling).

2. Examination

The stage of examining digital evidence that is collected forensically by scenario, either done manually or automatically. This is done to identify relevant information from the data collected while maintaining its integrity. The process of forensic examination of digital evidence is carried out after the process of collecting evidence.

3. Analysis

Analyze the results of the examination process that has been carried out, so that it can identify content or data that can be used as digital evidence related to online shop fraud cases.

4. Reporting

Report or document the results of the analysis that has been carried out.

The tools and materials needed in this study to obtain digital evidence are the ASUS X453S type laptop with the Windows 8.1 operating system that has 1.2.45 version of desktop based Line IM applications and the Redmi Note 5 Xiaomi smartphone installed on the IM Line application. Forensic tools used for acquisition are RamCapturer, imaging is FTK Imager and digital evidence analysis using Winhex tools.

2.2 Scenario

This research requires scenarios to obtain digital evidence. The scenario made includes all activities that are run on the Line application. The purpose of this scenario is to be a guideline for information to be analyzed as a fraud crime. The scenario is as follows:

1. Make a suspect Line account.
2. Make a Line victim account.
3. Victims chat to suspects for negotiations.
4. Victims send pictures and voice chat to suspects.
5. Suspects commit fraud against victims.
6. Suspects delete all conversation messages.

This study uses conditions that usually occur in everyday life in carrying out online shop fraud crimes, such as sending and receiving conversation texts, sending and receiving image files or voice messages on the Line. The case simulation that will be carried out in this study is a simulation of conversations between the suspect and the victim. The suspect will use a computer or laptop while the victim uses a smartphone. Conversation messages that have been deleted by the suspect will be revealed from the suspect's laptop using forensic tools. Figure 3 shows the scenario that will be run.

Figure 3. Online Shop Fraud Case Scenario

3. Results and Discussion

This research was conducted using a computer that has a Windows 8.1 64 Bit Operating System that has been installed on the desktop based IM Line application version 5.10.0.1789. Based on the scenario that has been made, the investigator finds evidence of a computer in the living conditions used by the suspect. The laptop is left on and it is not refreshed. This is done to avoid losing potential digital evidence. At this stage, the process of finding digital evidence is carried out based on the stages of the NIST method until digital evidence is found.

3.1 Collection

At this stage, the acquisition of digital evidence contained in RAM is carried out using tools that support live forensics techniques. The use of live forensics techniques is done to obtain evidence of digital line conversations contained in RAM. The live forensics tool used in this study is RamCapturer. RamCapturer is one of the tools that supports live forensics techniques. RamCapturer can retrieve data and information contained in RAM, including records of Line conversations that have been deleted. Figure 4 shows the acquisition process in RAM using RamCapturer tools.

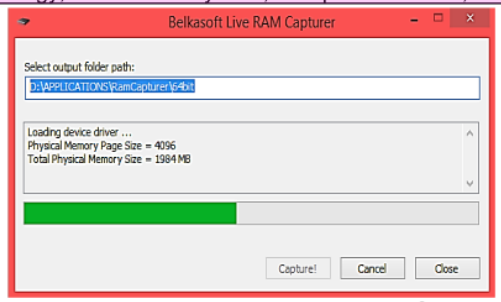

Figure 4. Acquisition Process using RamCapturer

The results obtained in the digital evidence retrieval process will be stored in D: \ APPLICATIONS \ RamCapturer \ 64bit and extension to the .mem file. The size of the file results from taking digital evidence with RamCapturer depends on the amount of RAM capacity of the acquired computer. The capacity of RAM size also affects the speed of the acquisition of digital evidence. The bigger the RAM size, the longer the acquisition process and the smaller the RAM size, the faster the acquisition process will be. Figure 5 shows the results of the digital evidence acquisition process with RamCapturer.

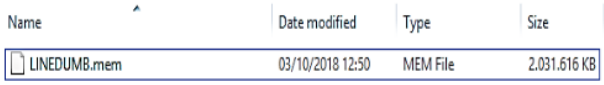

Figure 5. Line Acquisition Results

After the acquisition process is complete, the next process is imaging. The imaging process aims to avoid damage to the original digital evidence when the analysis process is carried out. The digital evidence of the imaging process must be the same as the original digital evidence, because a little difference will have an impact on the results of the analysis. In this study the imaging process was carried out using FTK Imager tools. FTK Imager can duplicate the acquisition results that have .mem extension file, as shown in Figure 6.

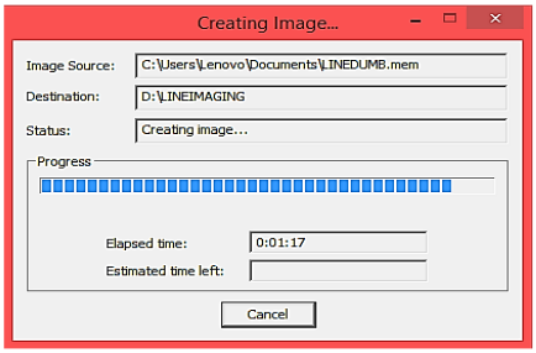

Figure 6. Imaging Process using FTK Imager

The analysis process carried out at the next stage uses digital imaging results. The original digital evidence will be stored to anticipate errors that will occur when the analysis process is carried out.

3.2 Examination

At this stage an examination of digital evidence is available after the process of taking digital evidence that has been done. This process aims to find out the digital evidence obtained based on the results of the scenarios that have been made. The process of checking digital evidence can be done using Winhex tools. Winhex has a feature to look for digital evidence from the acquisition results that have been done in the previous stage. Figure 7 shows evidence of digital Line conversations found.

Figure 7. Examination Results of Line Conversation Text

Based on the scenarios that have been made, the Line conversation data besides the conversation text contains an image file. During the inspection process, the image file was found, as shown in Figure 8.

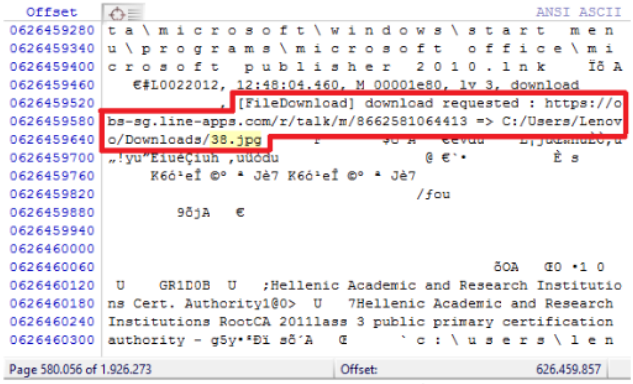

Figure 8. Examination Results of Image File

After checking the image file. Voice chat that are on the conversation data that have been screened have been found, as shown in Figure 9.

Figure 9. Examination Results of Voice Chat

Cite: Riadi, I., Sunardi, S., & Rauli, M. (2019). Live Forensics Analysis of Line App on Proprietary Operating System. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 4(4). doi:http://dx.doi.org/10.22219/kinetik.v4i4.850

Based on the examination results of Line digital evidence that have been done using Winhex tools, conversation text, image files and sound files have been found. The results of the examination of digital evidence will be analyzed at a later stage to find out the type of data and information contained in the conversation text, image files and voice chat that have been found. Table 1 shows the results of the inspection process that has been carried out.

Table 1. Availability of Digital Evidence on Line

Conversation data	Information
Conversation text	Found
Picture	Found
Voice chat	Found

3.3 Analysis

At this stage, analysis of the results of the acquisition is carried out using Winhex tools. Based on the results of the RAM data acquisition that has been done, it is found a record of conversations that have occurred on the Line. The conversation data is in the form of conversation text that has several data types. The analysis process is done by looking at the data displayed on the WinHex tools. In these data there are types of data and information needed, as shown in Figure 10.

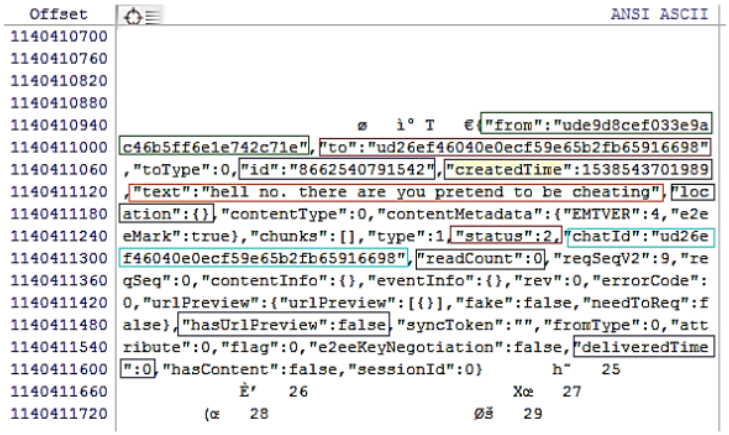

Figure 10. Line Conversation Text

Based on Figure 10 above, conversation data that has been simulated has several data types. These data types can be summarized to find out more clearly the functions of each of these data types, as shown in Table 2.

Table 2. Line Conversation Structure

Data Type	Information
"from":"ude9d8cef033e9ac46b5ff6e1e742c71e"	Sender Id
"to":"ud26ef46040e0ecf59e65b2fb65916698"	Recipient Id
"Id" : "8662540791542"	Line conversation Id
"createdTime":1538543701989	Coversation time
"text":"hell no. there are you pretend to be cheating"	Conversation contents
“location” : { }	Location
“status” : 2	Status of message. 1 to send and 2 to read
"chatId":"ud26ef46040e0ecf59e65b2fb65916698"	Conversation ID. If the conversation is unicast (conversation that occurs between 2 people), then the identity of the conversation is the same from the other person.
“readCount” : 0	The number of users who have read the message. If the conversation is multicast (group), it will show the number of people who read the message.
“hasUrlPreview” : false	Indicates the message has a url or not
“deliveredTime” : 0	The time when the message was sent

The results obtained from the Line analysis process using Winhex tools have several data types such as "from": "ude9d8cef033e9ac46b5ff6e1e742c71e", "to": "ud26ef46040e 0ecf59e65b2fb65916698", "Id":" 8662540791542 "," created Time": 1547433132908", "text": "hell no. there are you pretend to be cheating ", " location ": {}, "status": 2, "chatId": "ud26ef460 40e0ecf59e65b2fb65916698", "readCount": 0," hasUrlPreview": false and "deliveredTime": 0. The data type that contains the code ude9d8cef033e9ac46 b5ff6e1e742c71e which is the identity of the sender of the message cannot be translated into text. The code is the result of conversion from hexadecimal numbers to text form so that it cannot be translated into text so that the name or ID of the sender can be known. This is the same as the data type to (identity of the recipient of the message), id (Line message identity) and chatId (conversation identity) whose code cannot be translated into text form because the code is the result of converting hexadecimal numbers to text. Then for the deliveredTime data type and location it is not known when the message is sent and its location because the contents of the data type are empty, so there is no information regarding the time of sending the message and its location. Data types that can be translated are only createdTime (conversation time) and Text (contents of conversation messages). The createdTime code can be translated into datetime using the EpochConverter application [20]. Based on the code obtained on createdTime data type, which is 1538543701989, it can be converted to Wednesday, 3 October 2018 at 12:15:01, as shown in Figure 11. The time of the conversion results is the conversation time during the simulation. Next the Text data type that contains "hell no. there are you pretend to be cheating "is the content of the conversation that occurs when the scenario is done. Then for the readCount data type there is no information obtained because the simulation is unicast (conversation between 2 people). If the simulation is multicast (the conversation is group), the readCount data type will display the number of people who have read the message.

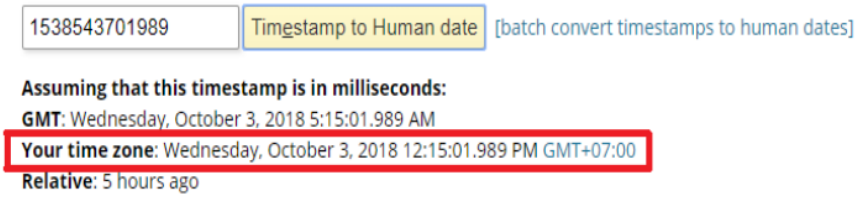

Figure 11. Line Conversation Time

Based on the results of the acquisition that has been done, the image file was found. The image file obtained is only a file name, 38 is the file name and jpg is extension files and the image file cannot be displayed. Before being deleted by the suspect the image file is stored in C: / Users / Lenovo / Downloads /, as shown in Figure 12.

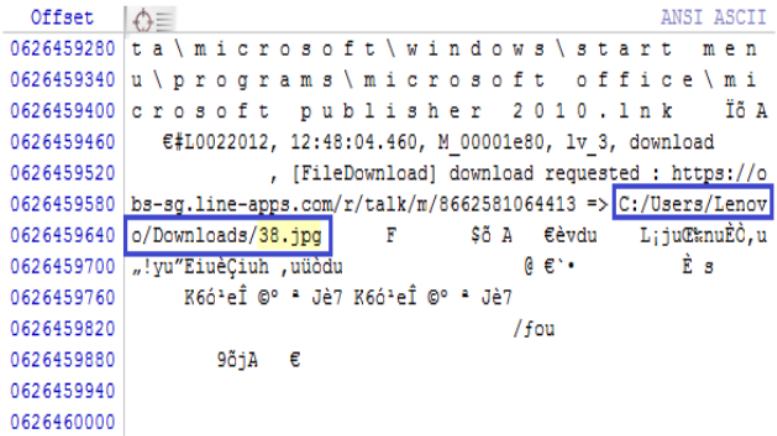

Figure 12. Image File in Conversation

Based on the scenarios that have been made, it is found a voice message found in the conversation that occurred. Voice messages obtained are only in the form of voicemail names, namely voice_37 and have .m4a file extension and the voicemail cannot be played or heard, as shown in Figure 13.

Figure 13. Voice Chat in Conversation

3.4 Reporting

This stage is the stage of reporting the results of the analysis process that has been carried out in the previous stage. At this stage digital evidence is reported based on information obtained. Table 3 shows the results that have been found.

Table 3. Evaluation Results

Conversation Data	Data Type	Data Information	Results (Information)
Conversation Text	From	Sender Id	Not found
	To	Recipient Id	Not found
	Id	Line conversation Id	Not found
	CreatedTime	Conversation time	Found
	Text	Conversation contents	Found
	Location	Location	Not found
	Status	Status	Found
	ChatId	Conversation Id	Not found
	ReadCount	The number of users who have read the message	Not found
	HasURLPreview	Indicates the message has a url or not	Not found
	DeliveredTime	The time when the message was sent	Not found
Picture	-	-	Just name
Voice chat	Name	Image file name	Just name
	Extension	Image file extension	

This research managed to get digital evidence related to online shop fraud crime cases. Digital evidence obtained in the form of Line conversations data between suspects and victims. The conversation data is in the form of conversation text that has several data types, namely from (sending id), to (recipient id), id (Line message id), createdTime (conversation time), text (conversation content), location (location), chatId (conversation id), readCount (number of message readers), hasUrlPreview (URL contained in the message), delivered Time (time of message sent) and information obtained in the form of conversation time, conversation text and conversation status. Image files and voice messages in the conversation data are found to be incomplete, only in the form of file names. The incompleteness of acquired digital evidence is likely due to the tools used during the process of acquisition and analysis of digital evidence. The compatibility of the live forensics tools with the IM application used greatly influences the completeness of the digital evidence obtained. The more complete the digital evidence, the faster the investigator reveals an online shop fraud crime case. Another thing that causes this incompleteness is the use of trial tools or not paid. The use of paid tools allows the digital evidence obtained to be more complete, while this study only uses trial or free tools.

This research can also be done in other crime case scenarios that support live forensics techniques. The complexity of finding, obtaining and analyzing digital evidence that exists when an application is running on a computer requires a lot of knowledge, ability and experience. This also really requires forensics tools that support getting quality digital evidence. This research can be the first step to address complicated crime cases and can help further research, especially in the scope of digital forensics.

4. Conclusion

Based on the results of the research, live forensics techniques can be applied to the acquisition of digital evidence from desktop-based IM Line applications on the Windows 8.1 operating system using RamCapturer, FTK Imager and Winhex forensic tools. Conversationa data that is used as digital evidence has several data types, but only 3 data types have information, namely conversation time, conversation content and status. These information can be used as digital evidence related to cases of online shop fraud crimes that occur.

Some suggestions for further research are several types of digital forensic methods, desktop-based IM applications and computer operating systems that can be combined into research topics that are likely to support live forensics techniques and obtain different and more accurate research results. The use of live forensics tools in the process of acquisition and analysis of digital evidence can also be combined with other tools and using paid tools to obtain quality digital evidence so that it can assist investigators in uncovering a crime that has occurred.

References

[1] M. S. Chang and C. Y. Chang, "Forensic Analysis of LINE Messenger on Android," *Journal of Computer*, Vol. 29, No. 1, Pp. 11–20, 2018. http://dx.doi.org/10.3966/199115992018012901002

[2] R. Umar, I. Riadi, and G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements, " *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 8, No. 12, Pp. 69–75, 2017. https://dx.doi.org/10.14569/IJACSA.2017.081210

[3] A. T. Kabakus and R. Kara, "Survey of Instant Messaging Applications Encryption Methods," *European Journal of Science and Technology*, Vol. 2, Pp. 112–117, 2015.

[4] I. Riadi, Sunardi, and A. Firdonsyah,"Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework," *International Journal of Cyber-Security and Digital Forensics (IJCSDF) and The Society of Digital Information and Wireless Communications (SDIWC)*, Vol. 6, No. 4, Pp. 198–205, 2017.

[5] I. Riadi, A. Fadlil, and A. Fauzan, "A Study of Mobile Forensic Tools Evaluation on Android-Based LINE Messenger," *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 9, No. 10, Pp. 201–206, 2018. https://dx.doi.org/10.14569/IJACSA.2018.091024

[6] "Statista," *https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/*. .

[7] H. K. Mann and G. S. Chhabra, "Volatile Memory Forensics: A Legal Perspective," *International Journal of Computer Applications*, Vol. 155, Pp. 975–8887, 2016. https://dx.doi.org/10.5120/ijca2016912276

[8] D. S. Yudhistira, I. Riadi, and Y. Prayudi, "Live Forensics Analysis Method For Random Access Memory On Laptop Devices," *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 16, Pp. 188–192, 2018.

[9] T. Rochmadi, I. Riadi, and Y. Prayudi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," *International Journal of Computer Applications*, Vol. 164, Pp. 31–37, 2017.

[10] K. Sreelakshmi and P. Sugathan, "Significance of Residual Artifacts from Random Access Memory," *International Journal of Science and Research*, Vol. 5, Pp. 2013–2016, 2016.

[11] M. P. Aji, I. Riadi, and A. Lutfhi, "The Digital Forensic Analysis of Snapchat Application Using XML Records," *Journal of Theoretical and Applied Information Technology*, Vol. 95, Pp. 4992–5002, 2017.

[12] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Evaluation of Integrated Digital Forensics Investigation Framework for The Investigation of Smartphones Using Soft System Methodology," *International Journal of Electrical and Computer Engineering*, Vol. 7, Pp. 2806–2817, 2017. http://doi.org/10.11591/ijece.v7i5.pp2806-2817

[13] M. I. Mazdadi, I. Riadi, and A. Luthfi, "Live Forensics on RouterOS using API Services to Investigate Network Attacks," *International Journal of Computer Science and Information Security*, Vol. 15, Pp. 406–410, 2017.

[14] I. Riadi, A. Yudhana, and M. C. F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," *Scientific Journal of Informatics*, Vol. 5, No. 2, Pp. 235–247, 2018. https://doi.org/10.15294/sji.v5i2.16545

[15] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *International. Journal on Advanced Science Engineering Information Technology*, Vol. 8, No. 3, Pp. 949, 2018. http://dx.doi.org/10.18517/ijaseit.8.3.3591

[16] A. Kurniawan, I. Riadi, and A. Luthfi, "Forensic Analysis and Prevent of Cross Site Scripting in Single Victim Attack Using Open Web Application Security Project (OWASP) Framework," *Journal of Theoretical and Appied. Information Technology*, Vol. 95, No. 6, Pp. 1363–1371, 2017.

[17] A. Majeed, H. Zia, R. Imran, and S. Saleem, "Forensic Analysis Social Media Apps in Windows 10," *2015 12th International Conference High-Capacity Opt. Networks Enabling/Emerging Technol. HONET-ICT 2015*, Vol. 10, Pp. 37–45, 2016. http://dx.doi.org/10.24949%2Fnjes.v10i1.321

[18] R. Dave, N. R. Mistry, and M. S. Dahiya, "Volatile Memory Based Forensic Artifacts & Analysis," *International Journal for Research in Applied Science and Engineering Technology*, Vol. 2, Pp. 120–124, 2014.

[19] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensics Method," *International Journal of Computer Science and Information Security*, Vol. 15, Pp. 3–8, 2017.

[20] "EpochConverter," *https://www.epochconverter.com/*.

HASIL CEK_60010313_(6)

ORIGINALITY REPORT

4%	2%	2%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Central Queensland University Student Paper	2%
2	Submitted to University of Nottingham Student Paper	2%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		