CyberSecurity and Digital Forensics
Vol. 5, No. 1, May 2022, p.6-11

e-ISSN: 2615-8442

ANALYSIS OF DIGITAL EVIDENCE ON RANDOM ACCESS MEMORY ANDROID USING LIVE FORENSIC METHOD CASE OF ILLEGAL WEAPON SALES

Arjun Zakari Yahya[1], Dirman[2], Dadang Juwoto Buru[3], Bambang Sugiantoro[4]

[1,2,3,4] Program Studi Magister Teknik Informatika Universitas Islam Indonesia

Email: [1]19917001@students.uii.ac.id, [2]19917002@students.uii.ac.id, [3]17917205@students.uii.ac.id, [4]Bambang.sugiantoro@uin-suka.ac.id

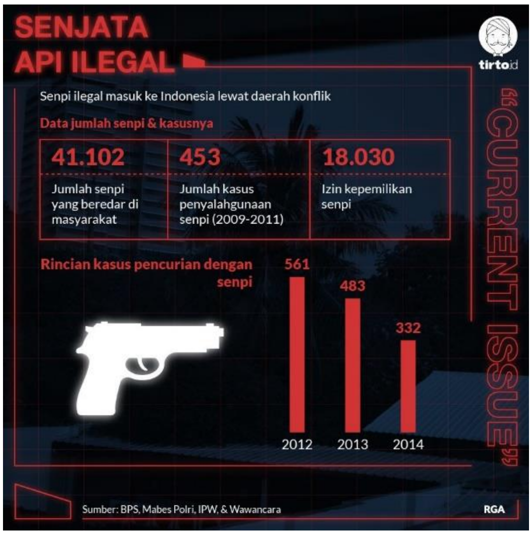
Abstract

*Live forensic method is data analysis that runs directly on the Random Access Memory section. Temporary storage places are also called Random Access Memory, the data stored in Random Access Memory is volatile or easily disappears. The purpose of this research is to obtain digital evidence through digital evidence analysis on random access memory on the perpetrators' android smartphones and victims' smartphones using the live forensic method in the case of illegal weapons sales. In the study of digital evidence seized in the form of a perpetrator's smartphone and the victim's smartphone. The victim is positioned as a student who was offered to buy illegal weapons by the perpetrator. The method of data analysis is carried out using the NIST (National Institute of Standards Technology) method which has analysis steps in the form of preservation, acquisition, examination, analysis and reporting. Data taken from random access memory in the form of log files telephone, sms, and data from whatsapp. The FTK (Forensic Tool Kit) is used to look for digital evidence of the crime of selling illegal weapons. The result is evidence of crimes that have been deleted by the perpetrators, including evidence of telephone logs, sms, WhatsApp chats, and image files with the .jpg extension. The FTK (Forensic Tool Kit) is used to look for digital evidence of the crime of selling illegal weapons. The result is evidence of crimes that have been deleted by the perpetrators, including evidence of telephone logs, sms, WhatsApp chats, and image files with the .jpg extension. The FTK (Forensic Tool Kit) is used to look for digital evidence of the crime of selling illegal weapons. The result is evidence of crimes that have been deleted by the perpetrators, including evidence of telephone logs, sms, WhatsApp chats, and image files with the .jpg extension.*Memtools are very useful for getting data from random access memory as a whole.

Keywords: Live forensics, Digital Forensics, Random Access Memory

1. INTRODUCTION

41,102 weapons have been recorded circulating in Indonesia, in terms of administration, only 18,030 have permits to own weapons. There were also 450 cases of misuse of firearms during 2009-2011. There were still a lot of cases of theft using firearms in 2012, namely 561 cases, the following two years decreased to 483 in 2013 and 332 cases in 2014. Illegal weapons can be seen in Figure 1.



Picture1. Illegal firearms

2. LITERATURE REVIEW

The illegal arms trade in Indonesia is very dangerous and detrimental to society. Throughout 2012-2014 cases of theft reached 1,373. Responding to the rise of illegal weapons that are misused by irresponsible people, a standardized digital forensic investigation method is needed that is able to uncover perpetrators of illegal firearms sales in Indonesia.

The technological revolution which is very fast developing and easy, is used by some people who are only looking for profit without regard to the losses and safety of others. Digital forensics, which combines two disciplines of law and information technology, can become an instrument for collecting evidence of illegal firearms sales.

Forensic terminology is often referred to in crime, especially digital forensics, which is a human effort to convey justice with scientific principles, namely preparation, search, collection, analysis and reporting in the legal field. The scope of digital forensics covers everything related to computer technology (Sulianta, 2016).

3. RESEARCH METHODOLOGY

This study uses a qualitative method

3.A Researched Variables

The variables studied in Random Access Memory include:

1. SMS : Proof of Chat
2. Telephone : Proof of incoming and outgoing calls
3. Whatsapp: Evidence of chat and image files

3.B Data collection

The data collection that we obtained refers to Donnie & Tindall (2015) by taking the PID (process ID) of the application that is running on random access memory using memtools. What is obtained from random access memory is in the form of telephone log files, SMS transcripts, Whatsapp data.

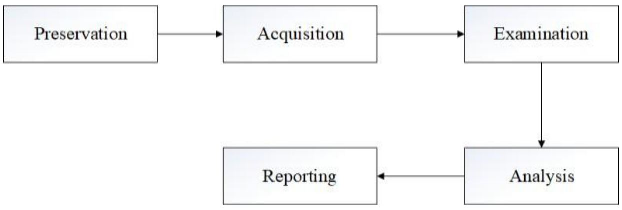
3.C Data source

The source of the data comes from evidence, namely the perpetrator's smartphone and the victim's android smartphone which will be acquired on RAM. In the scenario the victim plays as a student who is offered an illegal weapon by the perpetrator.

The perpetrator communicated via smartphone with the victim (student) via telephone call after which the perpetrator sent an SMS message to the victim and sent photos of illegal weapons being sold via Whatsapp messages. The perpetrator deleted logs in the form of telephone call logs, SMS messages and Whatsapp.

3.D Data analysis

The analysis in this study refers to the NIST (National Institute of Standards Technology) method, a technology administration body from the United States Department of Commerce (Ayers, et al. 2014) as shown in Figure 2.

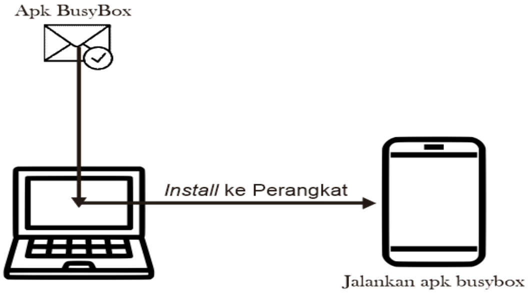


Picture2. NIST method

The steps in conducting data analysis using NIST are:

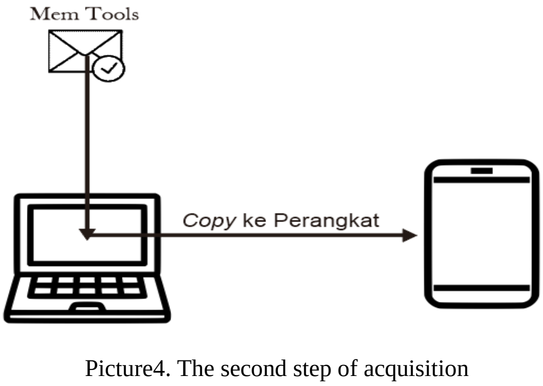
a. *preservation*This step is to identify the perpetrator's and victim's smartphone devices, as well as view the IMEI codes of the two smartphones by pressing the button via the keypad *#06#.

b. *Acquisition*(acquisition) is the step of finding and getting data files that are in random access memory using memtools. Following is the flow of acquisition of random access memory files:



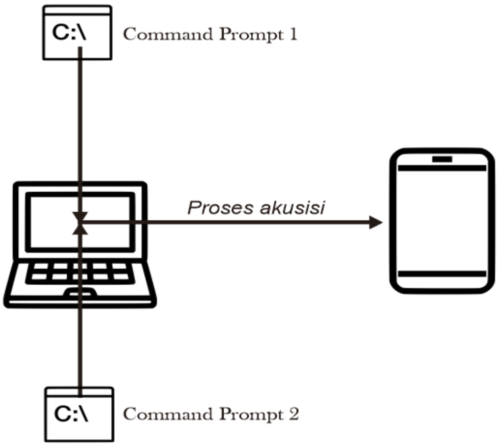
Picture3. The first step of acquisition

The first step is to install the busybox.apk application from the computer to the Android smartphone by executing the "adb -d install busybox.apk" command on the smartphone, then establishing a connection between the computer and smartphone via the "adb forward TCP TCP" command.



Picture4. The second step of acquisition

The second step is to copy memtools to the Android smartphone device by running the "adb push mem sdcard" command. The second step is to configure the system. The second step is to configure the Android system via the "adb shell" command, and enter root mode with the "su" command. Then create a folder in the dev directory, then move memtools to the dev directory. Change the permissions of the memtools file with the chmod (change mood) command, then type the command "dumpsys meminfo | grep activities" to see which applications are currently active in random access memory.

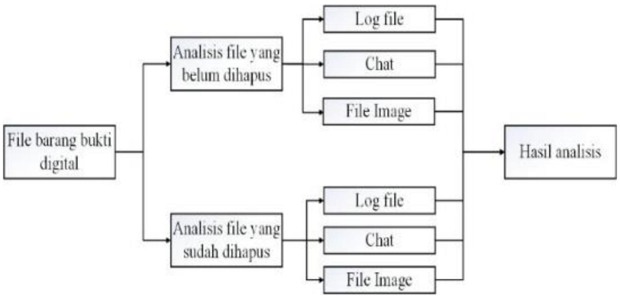


Picture5. The third step is acquisition

The third step is to look for Contact, SMS and Whatsapp PID (Process ID) with the ps command but the resulting data is too much so it's simplified to "ps | grep (PID name)", grep function for matching character search. If the PID has been found, do the acquisition process with the command "./mem PID | busybox nc -l -p TCP", tcp must be the same as adb forward, while the acquisition process is running open a second terminal command prompt and type the command "ncat 127.0.0.1 tcp > filename" with the aim of sending data from smartphone to computer via tcp port.

c. *examination*(Examination) is to check the hash value of each imaging file in random access memory obtained using the FTK tool, which aims to find out the hash value, so that when checked again it has the same value to avoid changing files.

d. *Analysis*Is a step to search for evidence of crime using FTK (Forensic Tool Kit) tools. The following data analysis flowchart is presented in Figure 3.


File barang bukti digital
Analisis file yang belum dihapus
Log file
Chat
File Image
Analisis file yang sudah dihapus
Log file
Chat
File Image
Hasil analisis

Picture6.Evidence Analysis Flow

Explanation of Fig. digital evidence in the form of random access memory files as input, the process of searching for data that has not been deleted comes from the victim's smartphone and searching for data that has been deleted from the perpetrator's smartphone, in the form of log files (incoming calls and outgoing calls), chat between the perpetrator and the victim via SMS and WhatsApp, image files sent or received are in the form of photos. The output of digital evidence includes evidence of crimes in the form of telephone call logs, SMS chats and Whatsapp chats in the form of text and images.

e. *reporting*Is a step to test the comparison of the results of digital evidence analysis between perpetrators and victims to find that they are carrying out illegal arms sales.

3.E Research Tools

The tools used in research to carry out simulations and scenarios are as follows:

a. Hardware
1. Laptop Asus Intel Core i5
2. Asus ZenFone
3. Xiaomi redmi 6

b. Software
1. Windows 10 64 Bit.
2. Busybox
3. ADB (Android Debug Bridge)
4. Memtools
5. FTK (Forensic Tool Kit)
6. NETCAT (ncat)s

4. RESULTS AND DISCUSSION

4.A preservation

The first stage is to identify the evidence of the two rooted smartphones, by accessing the system with the command cat system/build.prop and accessing the IMEI (International Mobile Enquipment Identity) code with the command *#06#

table1. Identify the Victim's Smartphone

Smartphone name	Asus Zenfone Max
Smartphone Models	ASUS_Z010D
Android version	Lollipop 5.0.2
SDK version	21
IMEI number	3533810751xxxxx 3533810751xxxxx

From the identification of the victim's smartphone, the Asus model ASUS_Z010D, Android Lollipop version 5.0.2, SDK 21 version with IMEI codes 3533810751xxxxx and 3533810751xxxxx were used.

Table 2. Identification of the Perpetrator's Smartphone

Smartphone name	Samsung
Smartphone Models	SM-J210F
Android version	Lollipop 5.1.1
SDK version	22
IMEI number	3570040788xxxxx 3570040788xxxxx

From the results of Table 2 the identification obtained from the perpetrator's smartphone, using a Samsung type Android smartphone with the SM-J210F model, Android Lollipop version 5.1.1, SDK version 22, with IMEI 3570040788xxxxx and 3570050788xxxxx.

4.B Acquisition

Retrieving data contained in random access memory uses ADB (Android Debug Bridge) tools to enter the Android system, while memtools is used to retrieve data in random access memory.

Table 3. Acquisition results

Evidence	Model	tools	*Files*RAM
Asus	ASUS_Z010D	mem	Logasus. raw
Asus	ASUS_Z010D	mem	Smsasus. raw
Asus	ASUS_Z010D	mem	Waasus. raw
Samsung	SM-J210F	mem	Logsamsung. raw
Samsung	SM-J210F	mem	Smssamsung. raw
Samsung	SM-J210F	mem	Wasamsung. raw

Based on Table 3, the results of the acquisition are getting files from each smartphone as digital evidence, on the victim's smartphone getting logasus.raw, smsasus.raw, waasus.raw while the perpetrator's smartphone is logsamsung.raw, smssamsung.raw, wasamsung. raw.

4.C examination

Here we check the hash value as digital evidence by using the FTK (Forensic Tool Kit) tool which aims to verify digital evidence files if checked again the file is still original and there have been no changes or modifications.

Table 4. Hash value of the file from the victim's smartphone

File name	MD5	SHA1
Logasus. raw	8F16AAE09A67AA3F56F28904009747F5	2EE395FC345769A5BF1FAB23972A6D724B47B44F
Smsasus. raw	26E3DBD91CF924B41E141E9CE3DC8208	206D799371375254603BC600044F05C2CBD59667
Waasus. raw	DD0ABD93A926456D61D4D702AFD92D42	6E9F662A618A9F4F2731F63C1C99C64AA4D74CF4

Based on Tabel 4, nilai hash dari random access memory yang diperiksa ada dua kategori yaitu MD5 dan SHA1, untuk file logasus.raw memiliki nilai hash 8F16AAE09A67AA3F56F28904009747F5 MD5, 2EE395FC345769A5BF1FAB23972A6D724B47B44F SHA1, file Smsasus.raw memiliki nilai hash 26E3DBD91CF924B41E141E9CE3DC8208 MD5, 206D799371375254603BC600044F05C2CBD59667 SHA1, file waasus. raw has hash value DD0ABD93A926456D61D4D702AFD92D42 MD5, 6E9F662A618A9F4F2731F63C1C99C64AA4D74CF4 SHA1.

Table 5. File hash value from the offender's smartphone

File name	MD5	SHA1
Logsamsung. raw	2AF4DBFAEA80C9F2B38AD11E02442279	B500F84FD32CEEDD6B8C65153ECAA478811F1B3E
Smssamsung. raw	59D230AAD78CF01C21F52DC79EBD5275	903A3281AAB6D9613629F755A840FC08AC0156FD
Wasamsung. raw	FAEAF6B2815026E9B86587393F99BC56	5033D7E58E98B9995D4DA85F61FF61FB02350C5A

Based on Table 5, the hash values of the random access memory examined are in two categories, namely MD5 and SHA1, for the logsamsung.raw file it has a hash value of 2AF4DBFAEA80C9F2B38AD11E02442279 MD5, B500F84FD32CEEDD6B8C65153ECAA478811F1B3E SHA1, the Smssamsung.raw file has a hash value of 59D230AAD MD5,903A3281AAB6D9613629F755A840FC08AC0156FD SHA1, file wasamsung.raw has hash value FAEAF6B2815026E9B86587393F99BC56 MD5,5033D7E58E98B9995D4DA85F61FF61FB02350C5A SHA1.

4.D Analysis

Looking for evidence of crimes that have not been deleted from the victim's smartphone and looking for evidence of crimes that have been deleted from the perpetrator's smartphone based on digital evidence files obtained from random access memory through FTK (Forensic Tool Kit) tools.

Table 6. Results of analysis of crime evidence findings

Bukti Digital	**Hasil analisis *Smartphone* korban**	**Hasil analisis *Smartphone* pelaku**
Log *file* Chat SMS	+628122987**** Siang mas ini saya agung dari	+628132742**** Siang mas ini saya agung dari

	jawabarat, ingin menawarkan senjata api rakitan untuk pegangan menjaga diri, jika minat balas pesan ini mas. Kami menawarkan harga yang sangat terjangkau	jawabarat, ingin menawarkan senjata api rakitan untuk pegangan menjaga diri, jika minat balas pesan ini mas. Kami menawarkan harga yang sangat terjangkau
Chat Whatsapp	Ini senjata illegal atau legal ya mas? Bisa lihat foto senjatanya Ini illegal mas tapi dijamin keamanannya dan ini kami beri dengan harga yang terjangkau. Seperti ini mas senjata rakitan yang kami jual. Wah, ini illegal berarti tidak ada ijin mas dari pihak yang berwajib, dan kegiatan anda ini bisa saya laporkan kepada pihak berwajib karena melanggar undang-undang dengan menjual senjata illegal yang tidak memiliki ijin. Saya akan laporkan mas Kalau anda berani lapor polisi saya akan cari dan tembak anda.	Ini senjata illegal atau legal ya mas? Bisa lihat foto senjatanya Ini illegal mas tapi dijamin keamanannya dan ini kami beri dengan harga yang terjangkau. Seperti ini mas senjata rakitan yang kami jual. Wah, ini illegal berarti tidak ada ijin mas dari pihak yang berwajib, dan kegiatan anda ini bisa saya laporkan kepada pihak berwajib karena melanggar undang-undang dengan menjual senjata illegal yang tidak memiliki ijin. Saya akan laporkan mas Kalau anda berani lapor polisi saya akan cari dan tembak anda.
File Image	IMG-20191206-WA0000.jpg	IMG-20191206-WA0004.jpg

From the results of the analysis, there is a log file of outgoing calls from the perpetrator's smartphone with the number +628132742**** and incoming call logs from the victim's smartphone with the number +628122987****, and SMS chat and whatsapp chat look the same as well as image files received on the smartphone the victim, namely IMG-20191206-WA0004.jpg and the image file sent from the perpetrator's smartphone, namely IMG-20191206-WA0000.jpg.

4.E reporting

Conduct a comparative test by matching the results of the analysis of the two smartphones, to get the conclusion that the perpetrator committed the crime.

Table 7. Digital evidence comparison test

Analysis results	log files	SMS chat	Chat Whatsapp	Image files	Information
Smartphones Victim	✓	✓	✓	✓	The same
Smartphones Perpetrator	✓	✓	✓	✓	The same

Based on Table 7, a comparative test of the results of the analysis of the two Android smartphones found the same evidence, and the conclusion has been successful in carrying out an analysis of digital RAM evidence on smartphones in cases of illegal arms sales using the live forensic method. And the perpetrators were proven to be trading illegal weapons, offering and selling them to civilians who did not have the right to own weapons, and the perpetrators were trying to erase digital track records by deleting telephone call logs, SMS chats, and Whatsapp.

5. CONCLUSION

Based on the research conducted, it can be concluded that by using memtools to capture data on the Random Access Memory as a whole using the FTK (Forensic Tool Kit) researchers can search for evidence of crimes that have been deleted or not from the perpetrator's smartphone. The results obtained were in the form of a log of incoming calls on the victim's smartphone, namely the perpetrator's telephone number +628132742****, while on the perpetrator's smartphone there was a log file of outgoing calls, namely the victim's telephone number +628122987****. Then in the SMS there is a conversation between the perpetrator and the victim, in which the perpetrator offers the victim an illegal weapon. In the Whatsapp message from the perpetrator's smartphone, there is an image file sent, namely IMG-20191206-WA0004.jpg and an image file received on the victim's smartphone, namely IMG-20191206-WA0000.jpg

BIBLIOGRAPHY

Al-Azhar, M. N (2013). Digital Forensic Panduan Praktis Investigasi Komputer.Jakarta: Salemba Infotek.

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on Mobile Device Forensics. 800-101.USA: CreateSpace Independent Publishing Platfrom.

Donnie, R. T., & Tindall, D. (2015). Learning Android Forensic. Birmingham:Packt Publishing Ltd.

Ermadi, S. W., & Teguh, S. Analisis Bukti Digital Pada *Random Access Memory* Android Menggunakan Metode *Live forensic* Kasus Penculikan Anak.

Suhariyanto. (2017). Statistik Kriminal 2018. (S. S. P. dan Keamanan, Ed.),04330.1802.Jakarta: Badan Pusat Statistik.

Yudhana, A., Riadi, L., & Ashori, I. (2018). Analisis Bukti Digital Facebook Messanger Menggunakan Metode Nist. IT Journal Research and Development, 3(1), 13-21.

Yudhistira, D. S., Riadi, I., & Prayudi, Y. (2018). *Live forensic* Analysis Method For *Random Access Memory* On Laptop Devices. International Journal of Computer Science and Information Security, 16(4), 188-192.