Logical Acquisition in the Forensic Investigation Process of Android Smartphones based on Agent using Open Source Software

Mukhli Prasetyo Aji¹, Dedy Hariyadi², Tri Rochmadi³
¹Department of Informatics Engineering, Universitas Muhammadiyah Purwokerto
²Department of Informatics Engineering, Universitas Achmad Yani Yogyakarta
³Department of Information System, Universitas Alma Ata

¹prasetyo-aji@ump.ac.id, ²milisdad@gmail.com, ³trirochmadi@almaata.ac.id

Abstract. Smartphones have an architecture with integrated components. Maintain the process of procuring digital goods on smartphones when asking for special assistance. According to the National Institute of Standards and Technology the process of procuring digital evidence on mobile devices There are 5 levels of acquisition: Manual Extraction, Logical Extraction, Hex Dumping / JTAG, Chip-Off and Micro Read. Which means buying digital evidence using logical acquisition methods or logical extraction still approved in SNI ISO 27037: 2014 also supports the process of procuring logistical permits in Special requirements, limited space. Dengen uses the live procurement method for logical acquisition on smartphones using ALogical OSE can be obtained digital proof in the form of Contact List, Call Log, SMS and MMS. The use of digital proof Larons can be obtained through basic data from the application installed on the smartphone.

1. Introduction
Smartphones have an architecture with integrated components. For example, a smartphone with an Android operating system has components including: applications, application framework, libraries, runtime, and Linux kernel [1], see Figure 1. Based on this architecture, the process of acquiring digital evidence on smartphones generally requires special handling. According to David Ashfield, the acquisition process on smartphones is divided into four: logical acquisition, file system acquisition, physical acquisition, and manual acquisition [2].

![Android Operating System Architecture](image)

**Figure 1.** Android Operating System Architecture
According to the National Institute of Standards and Technology, U.S. The Department of Commerce for the acquisition of digital evidence on mobile devices has been translated back into 5 acquisition levels that are illustrated in the form of a pyramid [3]. The lowest level, **Level 1** is Manual Extraction, extracting digital evidence from electronic evidence by looking directly at it. **Level 2**, Logical extraction, extracts digital evidence from electronic evidence utilizing electronic evidence connectivity with computer forensic analysis using wired or wireless media. **Level 3**, Hex Dumping / JTAG, Hex Dumping / JTAG requires tools in the form of Flasher Boxes on the market to support digital evidence extraction by changing the boot loader. **Level 4**, Chip-Off, the acquisition process focuses on flash memory on the device. **Level 5**, Micro Read, conducts acquisitions on NAND or NOR gates that require an electron microscope, see Figure 2.

This means that the acquisition of digital evidence using logical acquisition or logical extraction methods is still allowed. SNI ISO 27037:2014 also supports the acquisition process logically in certain conditions, such as limited scope [4]. The logical acquisition process on mobile devices can indeed save time, because the process of copying data that is relevant to the crime, for example, mobile numbers on contacts, Short Message Service (SMS), or Multimedia Messaging Service (MMS). This is as in Figure 3, about the standard diagram of the acquisition of electronic evidence in a lit condition.

Background the logical acquisition process does not violate the rules of digital forensics, so in this study proposed the implementation of the logical acquisition on smartphones with agent-based
Android operating systems. This agent will be embedded or installed on a smartphone with an Android operating system. Test this logical acquisition-based agent, using an agent that has an open-source license.

2. Related Works
The handling of crimes involving digital devices following the principle should minimize interaction with electronic evidence and digital evidence. However, this is different from electronic evidence in the form of smartphones that sometimes require further interaction [5]. In this study, the acquisition process of digital evidence on smartphones with intelligent operating systems uses agent-based systems. The principle is an ecosystem that implements an agent-based system, adding special applications that are embedded in a target to execute certain commands [6]. So that the smartphone will be installed by an agent whose function is to collect digital evidence, while the additional applications are AFLogical OSE and Laron.

2.1. AFLogical OSE
AFLogical OSE1 is a forensic application that is open-source licensed so that it can be used easily by non-law enforcement personnel [7]. The AFLogical OSE function is to collect or extract information on a smartphone with an Android operating system such as Contacts Phones, CallLog Calls, SMS, MMS messages, and MMSParts. AFLogical OSE there are two models available, the AFLogical OSE application is available in the form of an Android application and bundling with the Santoku Linux operating system in the form of a virtual machine sponsored by the company NowSecure2[8].

2.2. Laron
Laron is a forensic application that acquires logically digital evidence in the form of information installed on an Android system smartphone with an MIT license. The acquisition process using Laron must meet several requirements, namely: the cellphone is on, the cellphone is unlocked, Debugging mode is activated, the busy box is installed, and the cellphone is rooted. Laron development has been adjusted accordingly SNI ISO/IEC 27037:2014, see Figure 3 [9].

2.3. Android Debug Android (ADB)
Android Debug Bridge (ADB) is a tool or application part of Android Software Developers Kit (SDK) which connects between Android devices and computers so that it can be used to control and access files on Android-based smartphone devices [10]. The use of the Android Debug Bridge (ADB) can acquire digital evidence stored on smartphones but cannot return digital evidence that has been deleted. The requirements for implementing ADB on an Android-powered smartphone are the USB Debugging Mode must be active [11].

3. Acquisition Methods
The complexity of smart cellphone architecture requires adjustments in the process of acquiring digital evidence. So the approach to the acquisition process is not like the acquisition of digital evidence from a computer [12]. In this study, it was proposed to obtain digital evidence with various considerations that need to be installed on additional applications or agents on smartphones. Figure 4 shows the flow of agent-based acquisition processes on smartphones.
The acquisition process is divided into two parts, namely computer parts, and smartphones. In the computer agent section has been prepared in advance, namely AFLogical OSE and Laron in the form of files with extension .apk. The agent installation process can be installed via a smartphone or from a computer. If through a computer, the agent is uploaded to the smartphone first. The acquisition of agent-based digital evidence, the investigator will run the process on a smartphone. From the agent selected objects indicated as related to crime. Objects that are indicated as related to crime are copied on the external or internal memory. The selection of objects must be adjusted to the facts and the title of the case from a crime. After the acquisition process is complete, returning to the computer section uses ADB to copy the object. The final process, investigators carry out extraction and analysis of digital evidence obtained from the agent-based acquisition process. Software for extraction and analysis is adjusted to cases of crime that occur. The investigator is allowed to delete the agent installed on the smartphone, but this is optional.

4. Result and Discussion
The Agent used is AFLogical OSE and Laron has a license under the auspices Open Source Initiative [13]. AFLogical has a license GNU Public License, while Laron has a license MIT License. The agent is downloaded from the respective repository code available on the developer Github34.

The main requirement for the implementation of the acquisition of agent-based digital evidence is that the smartphone is on, the screen is not locked, and ADB must be activated manually by the investigator. Optional requirements that can be done is to install the busy box and the cell phone is rooted, see Table 1. If these requirements have been met, the first step that must be prepared for acquisition is downloading AFLogical OSE and Laron.

| Agent     | Smartphone ON | Unlock Screen | ADB Active | BusyBox | Rooted |
|-----------|---------------|---------------|------------|---------|--------|
| AFLogical OSE | √             | √             | √          | X       | X      |
| Laron     | √             | √             | √          | √       | √      |

Install agent AFLogical and Laron uses command ADB, namely ADB install AFLogical-OSE_1.5.2.apk to install agent AFLogical OSE and ADB install Laron-app-release.apk to install agent Laron. The installation process is done on the computer by typing the command it. To get digital evidence on a smartphone agent AFLogical OSE and Laron must be run from a smartphone. Digital evidence that can be obtained on smartphones using agent AFLogical OSE is Contact List, Call Log, SMS, and MMS, see Figure 5. Different from agent AFLogical OSE, evidence obtained or found
using agent Laron is database file from the application installed on the smartphone, see Figure 6. For example, smartphone users who have installed Whatsapp then database files in the form of *.db can be acquired.

In the process of acquisition between agents AFLogical OSE and Laron, there are fundamental differences regarding checksums, agent AFLogical OSE does not provide checksum result information after the acquisition process, while the Laron agent hash values included as evidence of maintaining the integrity of the acquired evidence, see Table 2. Therefore, Laron agents have BusyBox installation requirements and rooted conditions to produce sha1 hash values.

| Agent          | Contact | Call Log | SMS | MMS | DB Apps | Hash |
|----------------|---------|----------|-----|-----|---------|------|
| AFLogical OSE  | ✓       | ✓        | ✓   | ✓   | X       | X    |
| Laron          | X       | X        | X   | X   | ✓       | ✓    |

The extraction results from the AFLogical OSE Agent are files *.csv dan *.xml, see Figure 7. Meanwhile, the extraction result from Laron Agent is a compressed database in the format tar.bz2 to avoid contamination and the text file contains sha1 hash values from the tar.bz2 file, see Figure 8. Since the extraction from the AFLogical OSE agent is a *.csv file, the analysis uses spreadsheet software while the Laron agent uses SQL viewer because digital evidence is an SQLite database.

5. Conclusion
The acquisition of electronic evidence in the form of smartphones is different from computers, although it still pays attention to the prevailing digital forensic rules, namely minimizing interactions
with electronic and/or digital evidence. The stages of logical acquisition are still allowed to speed up the process of investigating a crime. Installation of acquisition agents on smartphones can still be considered to obtain digital evidence because the acquisition process is following the applicable digital forensic rules and is right on target. According to the results of this study, the AFLogical agent OSE can acquire digital evidence in the form of Contact List, Call Log, SMS, and MMS, while the Laron agent can acquire proof of database applications installed on the smartphone. The two acquisition agents can be used by non-law enforcement personnel because they are freely available in the code repository and licensed under the auspices of the Open Source Initiative. So the two agents have their respective advantages and functions depending on the case faced and adjusted to the case title. Besides AFLogical OSE and Laron, there is still proprietary digital-based agent-based digital forensic software. It is hoped that further research can analyze the implementation of agent-based digital forensic software both proprietary and licensed under the Open Source Initiative.

References
[1] L. Vogel, “Getting started with Android development - Tutorial.” [Online]. Available: https://www.vogella.com/tutorials/Android/article.html. [Accessed: 08-Jul-2019].
[2] D. Ashfield, “MOBILE DEVICE FORENSICS: DATA ACQUISITION TYPES,” CCL Solutions Group Ltd. 2014. [Online]. Available: https://web.archive.org/web/20150319193302/http://www.cclgroupltd.com/mobile-device-forensics-data-acquisition-types/.
[3] R. Ayers, S. Brothers, and W. Jansen, “Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1),” NIST Spec. Publ., vol. 1, no. 1, p. 85, 2014.
[4] B. S. Nasional, SNI 27037:2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital. Jakarta, 2014.
[5] R. Fasra and A. R. Nagoor Meeran, “Performing digital autopsy on an android device: An ‘open source’ approach,” Int. J. Control Theory Appl., vol. 9, no. 15, pp. 7111–7117, 2016.
[6] W. Buchanan, J. Graves, L. Saliou, H. Al Sebea, and N. Migas, “Agent-based forensic investigations with an integrated framework,” 4th Eur. Conf. Inf. Warf. Secur. 2005, ECIW 2005, no. May 2014, pp. 47–52, 2005.
[7] Z. R. Mair and A. Ashari, “Aplikasi untuk Identifikasi Short Message Service (SMS) Spam Berbasis Android,” J. Math. Nat. Sci., vol. 24, no. 3, pp. 257–262, 2014.
[8] N. Y. P. Lukito, F. A. Yulianto, and E. Jadied, “Comparison of data acquisition technique using logical extraction method on Unrooted Android Device,” 2016 4th Int. Conf. Inf. Commun. Technol. ICoICT 2016, vol. 4, no. c, 2016.
[9] D. Harihadi and A. A. Huda, “Laron: Aplikasi Akuisisi Berbasis SNI 27037:2014 pada Ponsel Android,” Indones. Secure. Conf. 2015, no. September, pp. 1–10, 2015.
[10] S. J. Yang, J. H. Choi, K. B. Kim, and T. Chang, “New acquisition method based on firmware update protocols for Android smartphones,” Digit. Investig., vol. 14, no. S1, pp. S68–S76, 2015.
[11] D. Quick and M. Alzaabi, “Forensic analysis of the Android file system Yaffs2,” Proc. 9th Aust. Digit. Forensics Conf., no. December, 2011.
[12] M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, “Forensic investigation of cloud computing systems,” Netw. Secur., vol. 2011, no. 3, pp. 4–10, 2011.
[13] “The Open Source Definition (Annotated).” [Online]. Available: https://opensource.org/osd-annotated.