IOP Conference Series: Materials Science and Engineering

PAPER • **OPEN ACCESS**

A Prototype of Portable Digital Forensics Imaging Tools using Raspberry Device

To cite this article: F Yudha *et al* 2021 *IOP Conf. Ser.: Mater. Sci. Eng.* **1077** 012064

A Prototype of Portable Digital Forensics Imaging Tools using Raspberry Device

F Yudha[1], E Ramadhani, R M Komaryan

Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia

E-mail: [1]yudha@uii.ac.id

Abstract. One of the digital forensics activities has the goal to prove a cybercrime. There are several stages in digital forensics when doing an investigation. Each stage has its suitable hardware and software that is used while investigating a case. Standalone forensics hardware is a suitable media in the process of investigation. It can do an acquisition and imaging process at the same time as the investigation process. Nowadays, standalone forensics hardware for imaging devices has a very high price. This paper gives a solution to develop low budget portable imaging forensics devices using a raspberry device. The device enables us to do an acquisition to a hard disk or flash drive. The output has a raw format file type i.e .dd. This device includes a logging file consisting of detailed information related to the digital evidence also hashing to provide file integrity. The result of this paper describes how to construct a prototype low budget portable device for digital forensics acquisition using a raspberry device and how to operate it in GUI. The prototype was successfully created and tested in several scenarios. The performance test of this device has a result of that transfer rate of 1,85 MB/s.

1. Introduction

Digital forensics arose as the implication of computer-related crime. It is the branch of forensics science that deals with the examination and analysis of digital evidence stored on physical(electronic) evidence in the form of personal computers (personal computers-PCs), laptops/notebooks, netbooks, and tablets. These methods needed to prove the crime that happened and connect it with the perpetrators. Based on data from the Internet Crime Complaint Center (IC3), in 2019 there were 467361 complaints in the United States[1]. The development of technology and its applications enforce digital forensics science practice harmonizing the application. The digital forensics investigation becomes complex due to the rapid growth of technology[2].

Process and procedure are the core component of a digital forensics investigation. The common investigation process contains preservation, acquisition, examination, analysis, and reporting. The acquisition process takes an important part in the digital forensics investigation process. It is a process of collecting evidence that correlates with the crime. A mistake in the acquisition process can have an impact on all of the investigation process. One of the techniques used in the acquisition process is imaging. It is the process of creating identical duplicate copies of electronic evidence.

To acquire and analyze digital evidence from cybercrime cases special treatment is required, due to minor errors in the handling of digital evidence that can make digital evidence not legally recognized and automatically cannot serve as valid evidence in court. According to The Indonesian act number 19 of 2016 regarding Information and Electronic Transactions (UU ITE) article 43 paragraph 5 alphabet (J) reads, "Requesting expert assistance needed in investigating criminal acts in the field Information

Technology and Electronic Transactions"[3]. One way to secure digital evidence by copying data from the storage media bitstream image and place it in a safe place. The technique takes bit by bit bits of data from a physical storage medium called imaging, and the result of such cloning is called a disk image.

To perform the disk imaging process, an investigator certainly needs devices and applications which can help the work. Today there are many applications of forensics imaging that can be used, ranging from paid to free. The outline of devices for computer forensics is differentiated by hardware and software, but both in terms of hardware and computer forensics software it is expected to fulfill 5 functions, that are acquisition, validation and discrimination, extraction, reconstruction, and reporting. Reporting from the site forensicswiki.com, here are some applications that can be used for forensics imaging including guymager, ewfacquire, Adepto, aimage, AIR, dcfldd, dd, and many more.

Traditionally, forensics analysis is accomplished by standalone several means to acquire hard drives and external media such as hardware write-blocker, dock attached to a laptop, computer, workstation with the preinstalled operating system. A standalone forensics acquisition and imaging device are very expensive. In this paper, we propose an acquisition system using a raspberry device as an imaging device in the digital forensics investigation. The raspberry device will consist of an operating system and tool. The tool that will be used is a graphical user interface (GUI) based tool. We use raspberry pi because of its low cost and its portability, popularity, and convenience of use.

Based on the fact and brief problem above, this research will propose a prototype portable tool for digital forensics imaging using Raspberry Pi. Raspberry Pi was chosen because of the capability to run it by using micro USB power through any power source with 5V voltage and easy to connect to the network using Wi-Fi. The objective of this paper is to describe how to make a prototype of a forensics acquisition device using a raspberry pi with the GUI interface. We build the system using raspberry pi and python programming language. The result of this paper is the performance of the imaging device. This paper is organized into several sections. Section I is the introduction to explaining the research background. In section II explaining the literature review of the paper. Section III explains the methodology of the paper. Finally, section IV has explained the result of the paper and we conclude the paper in the last section in section V.

2. Literature Review

Digital forensics research that utilizes the Raspberry Pi device has been done before. This research performs digital forensics analysis on the raspberry pi devices in connection with cybersecurity investigation was studied by [4]. They used Raspberry Pi to act as an attacker also as a target. A forensics investigation was performed by acquiring a Raspberry Pi sdcard using Encase Acquisition. This process showed that the researcher uses a traditional forensics method instead of a live forensics method. This research has some information that produces by this research which is the use of Raspberry Pi as an attack platform and Raspberry Pi as a target.

Research conduct by [5] addresses software that was used for digital forensics analysis and examination. Based on that research they found that open source tools might be used for supporting digital forensics investigation processes. The tools produced clear and comprehensive results as closed source tools (paid tools). This research suggests several suggestions that are the development of the comprehensive test, tool publication, creation of a standard, publication of specific procedures for the tool.

Research in the development of open-source digital forensics devices was started by [6] which is called FIREBrick. They used a mini-ITX motherboard and customized operating system to build a digital forensics workstation and used dcfldd as the imaging platform. The result of this research shows that FIREBrick performed acquisition on the SSD devices on 5 GB/min but they were not compared with other storage media devices. This result makes sense because they used full pc features in this device, so they will get better results.

[7] Conducted research to test different ARM processor-based single board computers. ARM-based computer board is used to demonstrate an effective, low cost, and low energy forensics imaging device. They used Raspberry Pi 2 and Odroid XU4 and 3 storage media to perform acquisition tests on the

testbed using a command-line application (DC3DD). This research found that Odroid XU4 takes 2 times faster in acquisition time than Raspberry Pi. Researchers do not create any application to perform forensics imaging easily.

Storage Evaluator and Knowledge Extraction Reader were developed by [8]. It was a triage device that performed data extraction on the storage media setups on Raspberry Pi devices and used a web interface for running the scripts. SEAKER collect data from storage media that was mounted to this device and analyzed the collected data. The result of this research shows that the researcher creates a device and application that perform logical data collection. They do not provide any imaging process in this research.

Based on the research gap in this section, this research will utilize Raspberry Pi devices to create a prototype open-source forensics imaging devices and develop an application interface to make the forensics imaging process better.

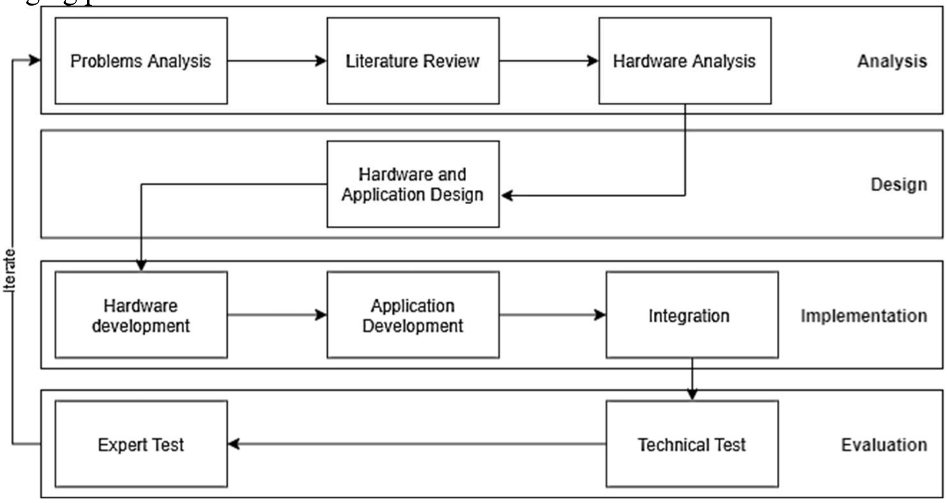


Figure 1. Methodology

3. Method

There are several phases in this paper i.e. analysis, design, implementation, and evaluation. It is divided into 9 stages that are problem analysis, literature review, hardware analysis, hardware and application design, hardware development, application development, integration technical test, and expert test.

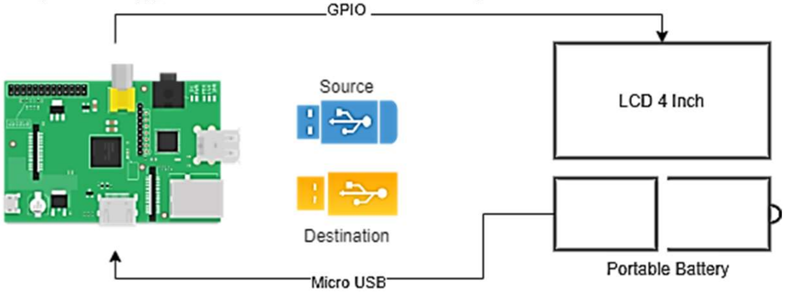


Figure 2. Prototype Architecture

In the analysis phase, preliminary analysis of this research was conducted and the hardware that will be used was chosen based on hardware analysis. It stages to analyze the best hardware for this research by comparing the technical specifications of every single board computer. Design phase we organized the hardware and software that were used to build the system. Then in the design system, a display of the user interface and created pseudo code were made. The implementation section is the process to implement the system related to the design system. The last process was an evaluation phase. It was a process to evaluate the prototype by performing technical and expert testing. Technical testing was evaluated by testing the devices by several scenarios of acquisition and digital forensics experts performed expert testing by evaluating survey instruments.

The prototype used Raspberry Pi 3 Model B+ as a portable device powered by a portable battery and attached an LCD 4 Inch to controlling the devices and application status as shown in **Figure 2**. It consisted of a Raspbian operating system, python shell, python library/module, and GUI based application[9]. Qt Designer was used to making a GUI application for forensics imaging that will be ported into the Raspberry Pi.

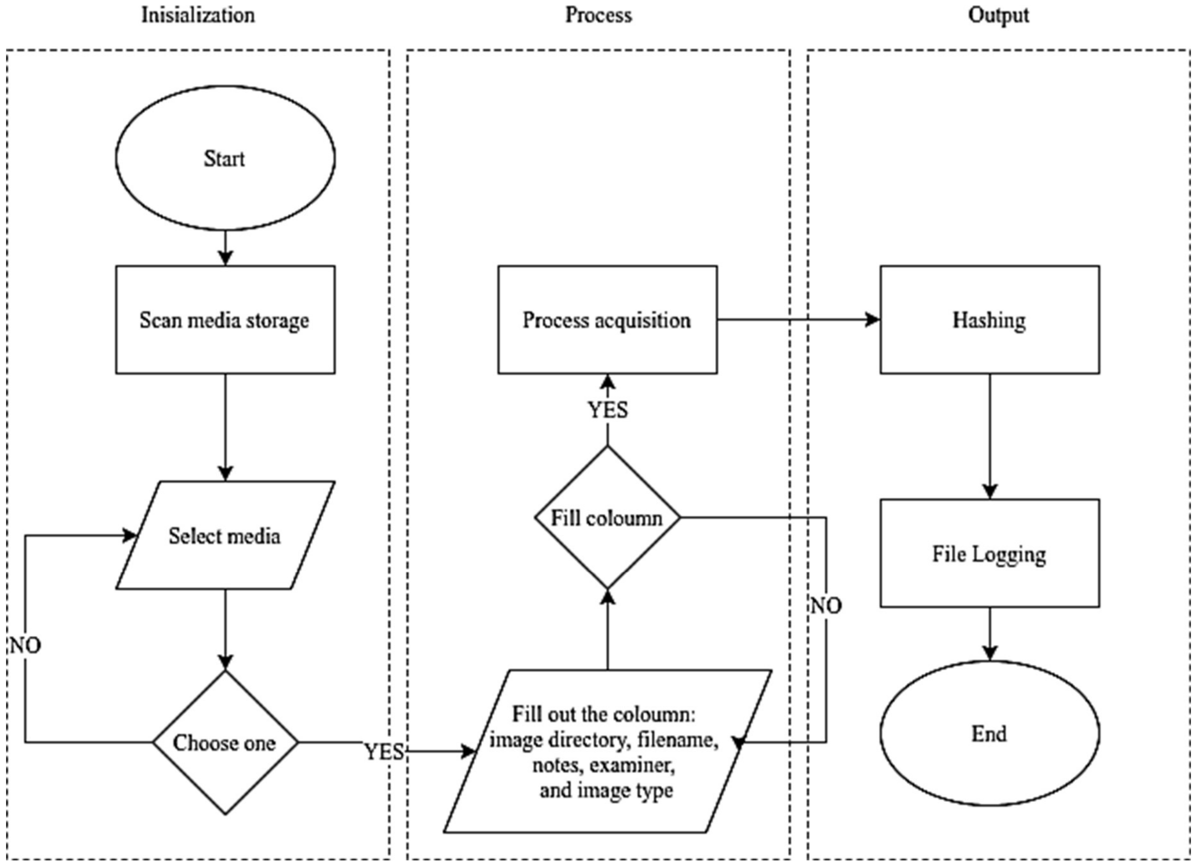


Figure 3. Application Flowchart

This system is divided into three stages i.e. initialization, process, and output. In the initialization stage, the system was able to detect the storage media that was to be acquired. The user chooses which media to process and selects the features in the application such as image directory, filename, notes, examiner, and image type. The main process is scanning, acquisition process, hashing, and generating a log as shown in **Figure 3**. The result of the acquisition process was raw file type. We use MD5 and SHA512 hash to ensure the integrity of the result.

The designing process also designed an application using Qt Designer. The first scenario is the system will present the available storage media in the list form and after choosing the devices that will be acquired the window will be redirected to the pre-process window. Pseudocode is designed by two scenarios i.e. initialization and pre-process. In the first initialization process, three libraries are used such as PyQt5, sys, and os, and the pre-process used libraries such as PyQt5, sys, hashlib, subprocess, logging, time, datetime, and os.

4. Result and Discussion

The prototype was developed with two stages: the first stages was the application development process that develops applications based on Python and Qt5 that port into Raspberry Pi. The second stage was the performance test of the tools, after the application was ported to the device, the performance of the application tested and monitored. The Tool was tested using 6 scenarios and it was monitored using Cacti. **Figure 4** showed the prototype of a forensics imaging device using Raspberry Pi and was powered by a portable power source.

Application interfaces were designed using the Qt5 library in Python. The application developed following the flowchart in Figure 3. The applications consist of 2 pages that are storage list and acquisition information form with 480 x250 resolution to comply with the display used in this device. Because these devices used 4 inch Raspberry Pi LCD. The device that will be acquired is attached to the devices on the USB port and the application will scan the attached devices.

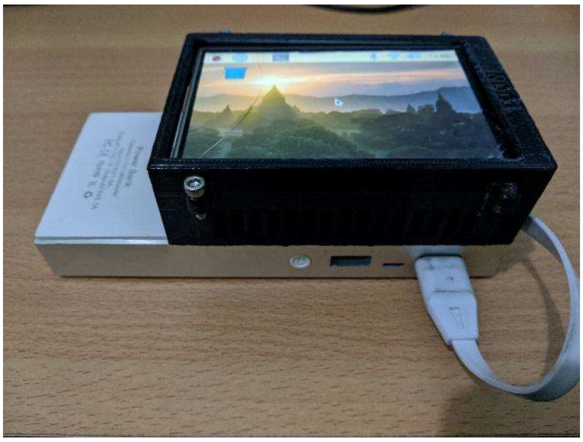
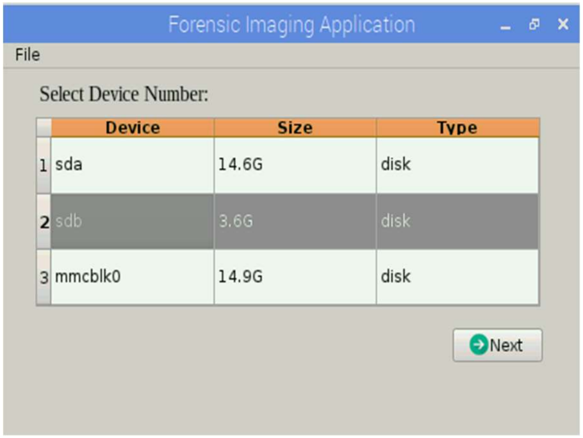


Figure 4. Prototype Forensics Imaging Device



Select Device Number:

	Device	Size	Type
1	sda	14.6G	disk
2	sdb	3.6G	disk
3	mmcblk0	14.9G	disk

Figure 5. Application Interface – Disk List

Figure 5 depicted the user interface of the GUI application for forensics imaging. The first page shows the list of physical devices that were attached to the device. This is an automated process to detect the disk which is attached to this prototype forensics acquisition device. The device that was selected from the list would be acquired by the highlighted row. Mmcblk0 was a default device that always appeared on the list, which is the primary partition of Raspberry OS.

After the acquisition process was finished, the application will generate a log file that contains information relevant to the investigation process as shown in **Figure 7**. Information's that are generated by the application are as follow:

a. Media information

Media information showed base information about the device. This information is generated automatically by the application based on physical device information on the fdisk –l command. The information that is generated in this process is Physical source, label, size, number of sectors. and UUID.

b. Acquisition Information

Acquisition information contains base information about the acquisition process such as result file name, destination directory, note, and examiner name. This information is captured before the acquisition process is started as indicated in **Figure 6**.

c. Time

This section shows the start time and end time of the acquisition process of the physical device and is displayed in a long time format. It is generated by the system based on the time when the acquisition was launched and finished.

d. Hash Checksum

After the acquisition process has been finished, the application will generate a hash checksum. There were 2 types of hash checksum which are md5 and sha512. The checksum was generated in 2 forms: source checksum and cloning checksum. The Source was the checksum from the physical device (/dev/sdx) and the cloning checksum is generated from the result of the acquisition process.

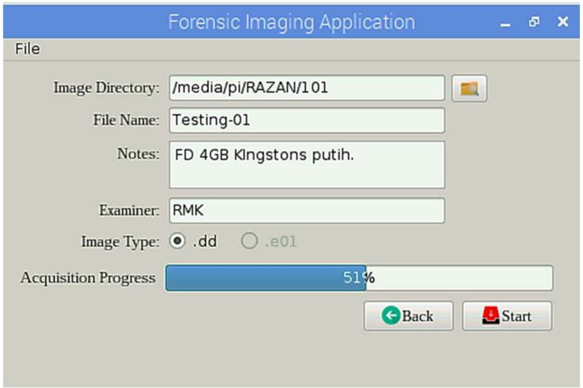


Image Directory: /media/pi/RAZAN/101

File Name: Testing-01

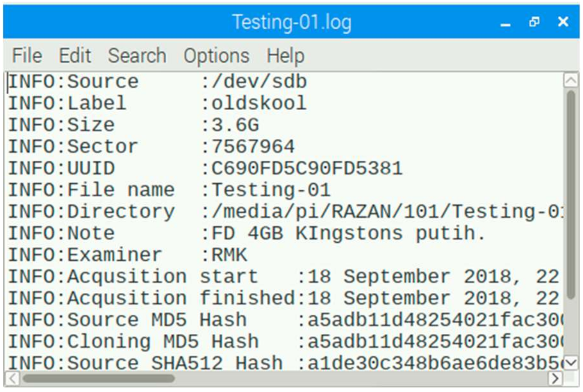
Notes: FD 4GB Kingstons putih.

Examiner: RMK

Image Type: ● .dd ○ .e01

Acquisition Progress 51%

Figure 6. Application Interface – Imaging Information Form



```
INFO:Source         :/dev/sdb
INFO:Label          :oldskool
INFO:Size           :3.6G
INFO:Sector         :7567964
INFO:UUID           :C690FD5C90FD5381
INFO:File name      :Testing-01
INFO:Directory      :/media/pi/RAZAN/101/Testing-0
INFO:Note           :FD 4GB KIngstons putih.
INFO:Examiner       :RMK
INFO:Acqusition start    :18 September 2018, 22
INFO:Acqusition finished:18 September 2018, 22
INFO:Source MD5 Hash     :a5adb11d48254021fac30
INFO:Cloning MD5 Hash    :a5adb11d48254021fac30
INFO:Source SHA512 Hash :a1de30c348b6ae6de83b5
```

Figure 7. Example of Log File

The prototype was tested using 6 scenarios and 6 samples of various storage devices. There were 3 categories of the sample based on the sample size that are 4 GB, 8 GB, and 16 GB. Table 1 describes the performance of the system from different samples. The objective of this evaluation is to find out if the system opens with several types of samples.

As mentioned before the system was monitored using Cacti to get the memory usage and CPU load in the device. **Figure 8** showed the memory usage of sample 1. Based on the result of Cacti average memory usage for every sample was recorded in Table 1. The data showed that the size of the sample affects the acquisition time. The size of the disk does not affect the transfer speed of the acquisition process. The transfer speed is one of the challenges that must be solved in this research. Transfer speed was calculated by using the formula (1).

$$Transfer\ Speed = \left(\frac{Total\ Bytes\ Acquired}{Total\ Time\ in\ Second}\right) \Big/ 10^{20} \tag{1}$$

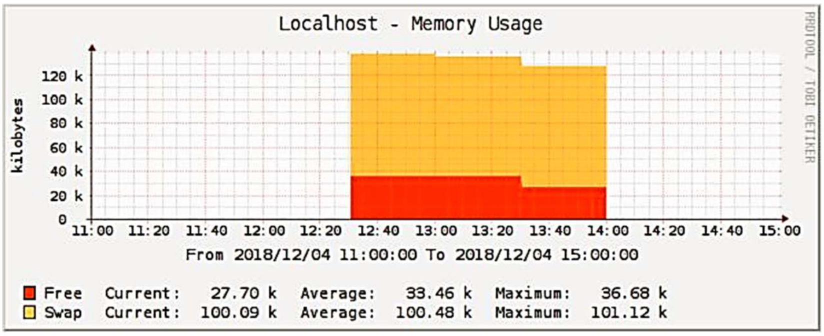


Figure 8 Memory Usage Monitored on Cacti

The transfer speed was spread between 1.69 MB/s to 1.93 MB/s and the average transfer speed was 1.85 MB/s. It is good speed for low-cost digital forensics imaging hardware using Single Board PC. The average total memory used in this prototype tends to be the same in all samples. It took 1048543.65 Kilobytes average of total memory use when the total memory of Raspberry Pi was 1,048,576 Kilobytes. Total memory used means that include memory used by the operating system because in this test Cacti cannot display the individual memory usage of the developed application.

The prototype was also tested on the digital forensics community in the special region of Yogyakarta with 56 respondents who have expertise in the fields of digital forensics. The test was performed by creating a demo video related to the process of acquiring flash drives using these prototypes. There were

3 aspects of the question in the questionnaire that were functionality, user interface, and benefit. It breaks into 14 instruments. The instrument of this test can be shown in **Table 2**. The result was calculated using the Likert formula and the average score of the test was 4.04 in all aspects.

Table 1. Test Result of Samples

No	Sample	Time Taken (Minutes)	Transfer Speed (MB/s)	Average Memory Usage (Kilobytes)
1	Sample 1 - 4 GB	35	1.75	1048543.32
2	Sample 2 - 4 GB	34	1.91	1048543.61
3	Sample 3 - 8 GB	73	1.69	1048542.13
4	Sample 4 - 8 GB	64	1.92	1048545.56
5	Sample 5 - 16 GB	129	1.93	1048543.63
6	Sample 6 - 16 GB	131	1.88	1048543.63
		Average Transfer Speed	**1.85**	**1048543.65**

Table 2. Survey Instruments

No	Aspect	Instrument
1	Benefit	Have the prototype advantages for digital forensics investigator
2		The use of a single-board computer (SBC) specifically Raspberry Pi can decrease the cost of the prototype against the real digital forensics hardware
3		The prototype is easy to carry because it is a small device
4		Will the investigator use this prototype for creating a digital forensic image
5		The imaging result of the prototype has been met with digital forensic investigation methodology
6		The prototype has prospects to used later
7	User Interface	The application interface is interesting to use
8		The application interface is easy to recognize
9		The displayed menu is easy to understand
10		The placement of all the features and application buttons is appropriate
11	Functionality	The autorun feature of the application runs well
12		Auto-scan feature to detect what storage is available is running well
13		All buttons and menus work normally
14		All error handling run well

5. Conclusion

In this paper, this research proposed a prototype portable device for performing digital forensics acquisition by utilizing Raspberry Pi devices with an application developed for this purpose. These tools can be used for supporting digital forensics investigation processes especially in the process of acquisition. The prototype was successfully created and tested, Not only in a scenario-based test but also tested by the digital forensics community. Based on the test result of the scenario-based test, the prototype forensics imaging device can perform the acquisition process on the sample flash drive with 1,85 MB/s speed. Also, responses from the digital forensics community have a good result.

For future work, some improvements are needed, not only in the scope of application development but also in the operating system and hardware development. The application must be improved to cover another disk format such as E01 and AFF4. Besides, Transfer speed needs to be improved for a better and faster acquisition process such as perform acquisition in Raspberry Pi Cluster.

References

[1] FBI 2019 *2019 Internet Crime Report* Retrieved from https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[2] Reedy P 2020 Digital evidence review 2016–2019 *Forensics Sci. Int. Synerg.* **2** pp 489–520

[3] Goverment of Republik Indonesia 2016 *Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik* Retrieved from https://jdih.kominfo.go.id/produk_hukum/view/id/555/t/undangundang+nomor+19+tahun+2016+tanggal+25+november+2016

[4] Feng X, Babatunde O and Liu E 2015 Cyber security investigation for raspberry Pi devices *Int. Ref. J. Eng. Sci.* pp 1–14

[5] Carrier B 2002 *Open Source Digital Forensics Tools: The Legal Argument* Retrieved from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.581.6818&rep=rep1&type=pdf

[6] Tobin L and Gladyshev P 2015 Open forensics devices *J. Digit. Forensics, Secur. Law* **10** 1–5

[7] Olson E and Shashidhar N 2016 Low budget forensics drive imaging using arm based single board computers *J. Digit. Forensics, Secur. Law* **11** pp 53–76

[8] Gentry E and Soltys M 2019 SEAKER: A mobile digital forensics triage device *Procedia Computer Sci.* vol **159** pp 1652–61

[9] RASPBERRY PI FOUNDATION 2018 Raspberry Pi 3 Model B+ *Raspberry Pi*