A Study of Mobile Forensic Tools Evaluation on Android-Based LINE Messenger

Imam Riadi[1]
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Abdul Fadlil[2]
Department of Electrical Engineering
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Ammar Fauzan[3]
Department of Informatics Engineering
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

***Abstract*—The limitation of forensic tool and the mobile device's operating system are two problems for researchers in mobile forensics field. Nevertheless, some kinds of forensic tools testing in several devices might be helpful in an investigation. Therefore, the evaluation of forensic tool is one gate to reach the goal of a digital forensics study. Mobile forensics as one of the digital forensics branch that focusing on data recovery process on mobile devices has some problems in the analytical ability because of the different features of forensic tools. In this research, the researchers present studies and techniques on tools ability and evaluated them based on digital evidence of LINE analysis. The experiment was combined VV methods and NIST standard forensic methods to produce a model of forensic tool evaluation steps. As the result of the experiment, Oxygen Forensic has 61.90% of index number and MOBILedit Forensic has the highest index number at 76.19% in messenger application analysis. This research has successfully assessed the performance of forensic tools.**

***Keywords*—Forensic; investigation; mobile; evaluation; performance**

I. Introduction

Cybercrime is escalating and the race against cybercriminals is never ending since the internet established. The huge number of mobile phone users nowadays add the new problem of this issue. As a result of this many users, in addition to the traditional usage of mobile phones including making phone calls and texting in SMS, now mobile phones are also used for making video calls and chatting in the instant messenger.

The development of Android smartphone technology has an impact on the fast-growing number of applications developed for Android. Even though, cybercrime can happen in Android smartphone. The investigator has to be able to solve the crime case with a mobile forensic method to find a digital evidence. Digital evidence is fragile, volatile and vulnerable if it is not handled properly [1], especially in the mobile device. Mobile forensic is a science field that studies the process of digital evidence recovery using the appropriate way from a mobile device [2] which usually doing in a digital forensic investigation by the police. Digital forensic investigation is the phenomenon that solves the digitally committed crime and explores the culprit legally [3]. It is important for examiners and investigators to have the knowledge about mobile forensic methods and the tools.

National Institute of Standard Technology (NIST) considers that forensic tools might have ~~a~~ degree of error and need to be evaluated by the test against different mobile devices [4]. Experiments conducted with mobile device forensic tools can indicate the capability of the tools. The forensic tools should produce valid results based on the fact in terms of data objects that are acceptable in the court.

II. Literature Review

A. Related Work

In [5] the researchers conducted a comparative evaluation of forensic tools for WhatsApp analysis on Android-based smartphones. The author choose WhatsApp because of its easiness for expanding the user base. When installing it, one can virtually reach all contacts in his/her address book on the phone who have installed the same apps [6]. The researcher evaluating performance and ability of some forensic tools, i.e. WhatsApp DB/Key Extractor, Belkasoft Evidence, and Oxygen Forensic. The evaluation using the NIST forensic tool parameter and additional parameters from the researcher. The author did at least four steps to conduct this evaluation, i.e simulation, forensic analysis, analysis result, and conclusion.

In [7] the authors want to emphasize on the forensic investigation process and to compare mobile forensic tools used in this research by using a framework developed by National Institute of Standard and Technology (NIST). The authors used four forensic tools to examine one Android device. The performance of forensic tools was rated quantitatively. There is no strong reason in this work and the previous reference why the forensic process has to use NIST method or the specific tools.

According to [8] the researchers suggest the decision method theories trough performance and relevance parameter while doing a hypothesis testing on forensic method and tools selection. This paper is inspired by the freedom of choice necessitates theory. The freedom choice theory is a sense of responsibility that asks for separation between true and false. Sometimes the selecting process for choosing the right forensics tool is complex with major consequences. The author suggest the project to evaluate the performance of more tools against a broader set of mobile devices will help in the selection of the most appropriate forensics tool. In the previous work, the National Institute for Standards and

Technology (NIST) conducted an evaluation of the forensics tools as an independent third party.

In reference [9] the researcher doing "Validation approach" since the tools were of propitiatory nature and there was no access to their documentation and source code. This paper presents the findings with respect to the reliability of the tools only. The authors evaluate XRY and UFED forensic tool in the light of NIST Smartphone Tool Specification which consists of a number of specifications with their associated Test Assertions and Conformance Indicators.

Performance can be measured from historical data or from the results of carefully designed experiments. Historical data included performance evaluation results by both the vendors and a trusted third party. The problems, however, were that: (i) vendor evaluation lacked trust and (ii) trusted third party's evaluation used different mobile devices to evaluate the forensic tools. The tools were not evaluated on equal grounds and thus the results cannot be generalized for comparing their performance.

Every digital forensic method has different stages in each handling of the digital evidence found, so in the handling of various evidence, it requires different digital forensic models [10]. In many references, digital forensics process at least can be divided into four steps as in Fig. 1**,** collection, preservation, analysis, and presentation [11]. The naming four stage of digital forensic model is very flexible to be changed as needed for investigation. Sometimes at the end of the process called "reporting" instead of presentation and at the beginning begins with the identification process before collection/preservation.

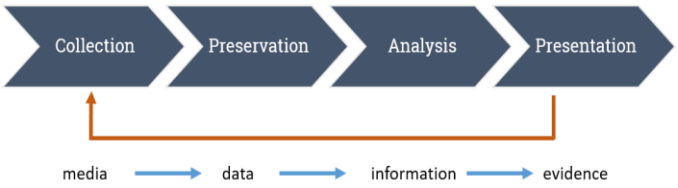

Fig. 1. Digital Forensic Process.

Having knowledge of the digital forensic process is important, same as forensic tools that have a vital role in the whole forensic process. Examiners must understand the capabilities of a forensic tool with insights from good references of tool testing. But, most of the mobile forensic tool testing and evaluations are done by the vendors. Mobile forensic tools developed in the forensic world are rarely validated independently and scientifically. Moreover, forensic tools are used almost in all the stage of mobile forensics process.

B. Digital Forensics Problem

There are many proprietary forensic tools have been developed. As a result, a wide variety of tools exist to extract evidence from mobile devices, no one tool or method can acquire all the evidence from all devices [12]. The software applications for mobile forensics available today are not 100% forensically sound [13]. The complexity formally representing all the science need to start with a literature and discussions with industry leaders from diverse backgrounds [14]. Experiment in the past concentrated on the trustworthiness of digital evidence that is the product of the process and not the validity of the tools. Recently, there is an attempt to formalize the theory of digital forensics and dissertation about definitive research that focuses on the model the process has already started to appear. There is also research on validation of the investigation results forensic (that is the reliability of the evidence), only a few on the reliability of tools that produces the evidence. The researcher have to consider that when the examiner/investigator want to conduct an analysis, they need to use a method along with forensically tested tools [15]. Each tools can be validated and verified on its merits and the examiner can focus on the results required rather than the domain of all possible functions and all possible specifications.

C. Mobile Device Forensic Tools Evaluation

Mobile device forensic tools evaluation is consist of the validation and verification process. Validation is the confirmation by examination and the provision of objective evidence that a tool, technique or procedure functions correctly and as intended, while verification is the confirmation of a validation with laboratories tools, techniques, and procedures [14]. It is important for a forensic examiner to know how reliable and accurate a tool is before being used. The researcher have used the evaluation to gauge and verify the reliability and accuracy of two most prominent mobile forensic tools such as MOBILedit Forensic and Oxygen Forensics based on the Smart Phone Tools Specifications by NIST [16]. The parameters for tool evaluation are depend on the needs of researchers, but they are not far from the issue background.

III. Research Methodology

A. Evaluation Method

This article is inspired by many previous works of forensic tool evaluation, one of them is validation verification (VV) methodology that was proposed by Guo, Slay, and Beckett [17]. The first step in evaluation is listing the forensic tools function. From the documentation of both tools; Oxygen Forensic and MOBILedit Forensic, their function as seen as in Table 1.

TABLE I. Forensic Tools Functions

Oxygen Forensic	**MOBILedit Forensic**
Device Identification	Device identification
Data Extraction	Application data extraction for Android and iOS
Messenger Application Analysis	Application Analysis
Data Report	Data Report
Case Management	-
-	Deleted data retrieval

- Device Identification : The ability of a forensic tool in device recognition
- Data Extraction : The ability in data extraction from the device
- Messenger Application Analysis : The Ability to show the content of messenger application
- Data Report: The ability of tools evidence documentation in form of report file (.xml, .pdf, .xsl, etc.)
- Case Management : Management of cases during the analysis process
- Deleted data retrieval : The capability of a forensic tool to retrieve any deleted data from the device

Six aspects above need for validation and verification for evaluating the tools. Validation technique used quantitative calculation so that assessment more objective, but to verify, the researcher simply apply quantitative assessment. Among the aspects that can be considered qualitatively are device identification, data extraction, case management and deleted data retrieval. While to messenger application analysis and data report can be assessed quantitatively in the term of the performance in producing the evidence.

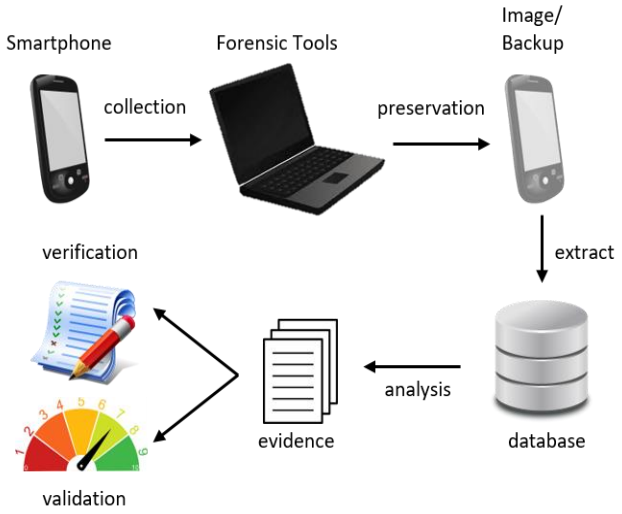

Fig. 2. A Brief Process of Forensic Tools Evaluation.

This experiment was conducted using simulations on a smartphone and two forensic tools. The brief process of this experiment is described in Fig. 2. The explanation of the tool verification and validation will be described in the next section.

B. Tool Verification

In the verification process, the researcher compare the function of the forensic tools with the experiment they did. Some functions that need to be verified are device identification, data extraction, case management in Oxygen Forensics, and deleted data retrieval in MOBILedit forensic. Verification is done manually by comparing one by one function then assessed by its performance.

C. Tool Validation

Forensic tools validation can be done accurately by judging the performance index number as shown in equation (1). Performance is measured in terms of probability of successful (Ps) extraction of a particular type of digital evidence by a specific forensics tool using the equations below:

$$P_s = \frac{x}{n} \quad (1)$$

The number of objects extracted by two forensic tools, Oxygen Forensic and MOBILedit Forensic. Objects that populated in this experiment is from LINE messenger by manual acquisition. Equation (1) used to calculate the index number of the messenger application analysis and the data report from each forensic tool. This equation also can be used in validating the data report for each forensic tools. The equipment that used in this research can be seen in Table 2 as follows:

The whole research processes can be drawn as in Fig. 3. This research model is an adoption of NIST method with alteration with VV methodology as needed for the research purposes.

TABLE II. EVALUTION RESULT FROM OXYGEN FORENSIC AND MOBILEDIT FORENSIC

No.	Equipment	Description
1	SONY Xperia Z	Android Smartphone
2	ASUS A455L	Workstation, OS Win.10
3	Oxygen Forensics	Suite 2014
4	MOBILedit Forensic Express	Ver. 4.0
5	USB Cable	Ver. 2.0

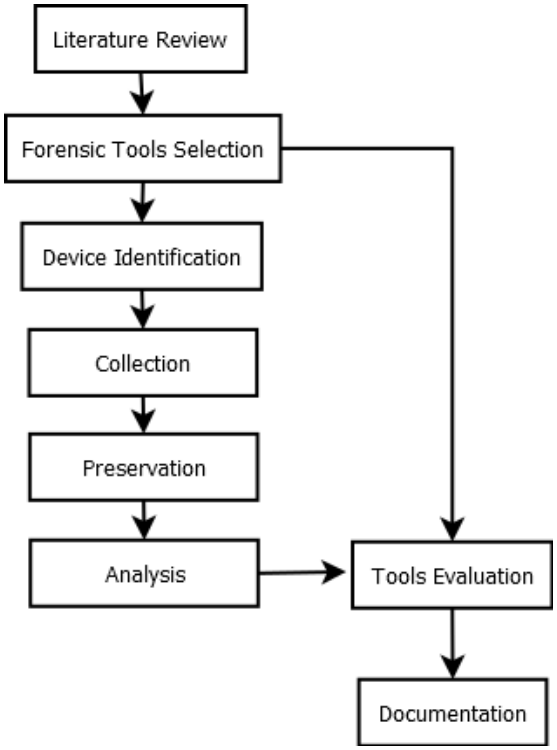

Fig. 3. Tools Evaluation Methodology.

The evaluation methodology can be modified according to the needs and the expected results. The method above is one method that can be applied in evaluation tool research.

IV. Result and Analysis

The evaluation is ended with the documentation process. This documentation can be either a report or a presentation file to show to the examiner and investigator. The results of the evaluation process that is conducted by applying VV methods are as follows:

A. Device Identification

The device identification is the first step that must be done by any forensic tool. The collection of information about the device is very useful in the report on the final process. Oxygen forensic is able to identify the device that the researcher use, Sony C6602 or known as Sony Xperia Z, as can be seen in Fig. 4. But, Oxygen forensics is not able to recognize the IMEI number or the serial number of this device.

While in MOBILedit forensic the device identification result is as expected. Metadata from the device like serial number, IMEI, IMSI, ICCID, Root status. All of the important metadata can be revealed and documented as in Fig. 5. MOBILedit forensic is quite successful in identification mobiledit mobile device.

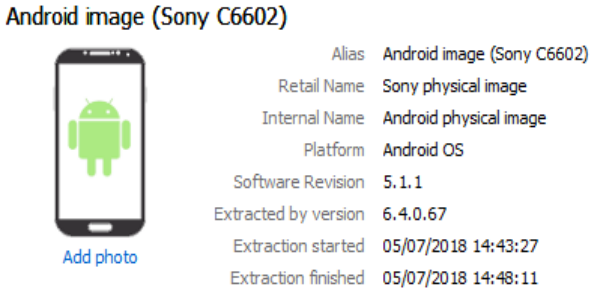

Fig. 4. Device Identification by Oxygen Forensic.

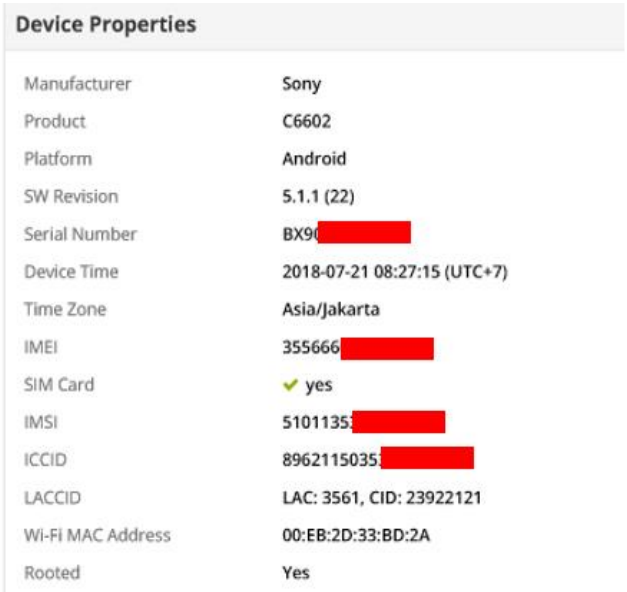

Fig. 5. Device Identification by MOBILedit.

Both devices are quite good in the device identification function. Although Oxygen forensics has its lack, at least it can recognize the device's manufacturer name. These results may be different on the other devices.

B. Data Extraction

Data extraction on both devices is desirable, as this is much needed in a long-period investigation. Data extraction on Oxygen Forensics is quite successful because it is able to create backup files from data acquisition devices, as shown in Fig. 6.

While in MOBILedit, as seen in Fig. 7, data extraction to generate backup data is not as good as expected, because the data extraction data that we get was corupted and error.

Both forensic tools have different ways of extracting data. MOBILedit is not success in performing its functions. However, Oxygen can be used in investigations over a long period of time, so the examiner can analyze the digital evidence more deeply. The difference of the forensic tools result can be aspect that can be considered by the examiner.

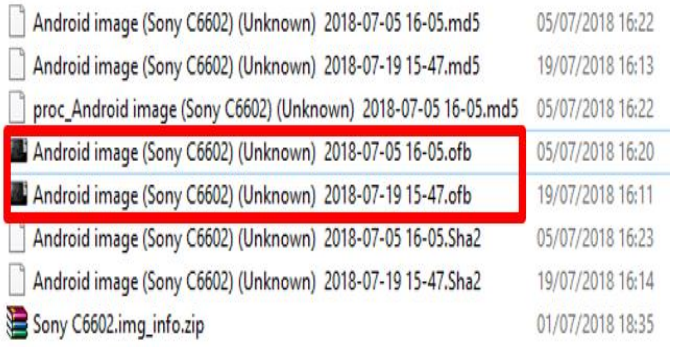

Fig. 6. Data Extraction by Oxygen Forensic.

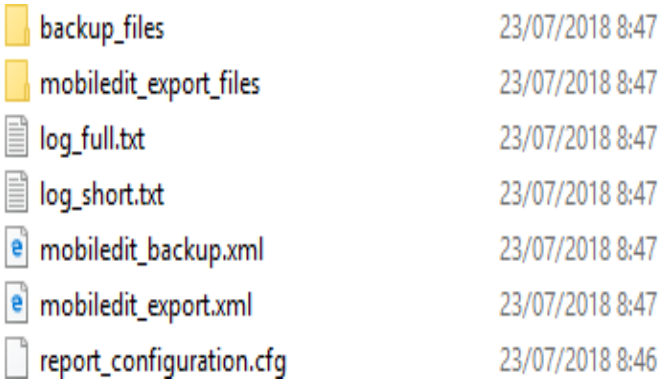

Fig. 7. Data Extraction by MOBILedit Forensic.

C. Messenger Application Analysis

Analysis of messenger apps in this experiment will see the ability of forensic tools on LINE messenger analysis. LINE messenger that was tested is the latest version, with simulated conversations that have been done in it. In Oxygen forensic, messenger analysis result is presented in table form by displaying ID, the direction of the message, remote party, text, and the timestamp. In the Fig. 8 there are no any images nor videos that can be displayed.

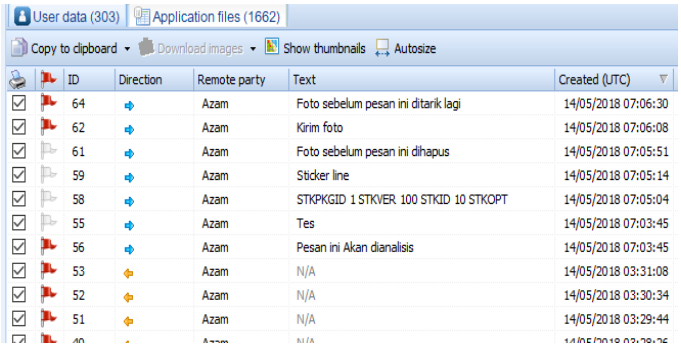

Fig. 8. LINE Messenger Analysis in Oxygen Forensic.

While in MOBILedit forensic, analysis of messenger is presented in the report file with a colored block display like a message application look, as shown in Fig. 9.

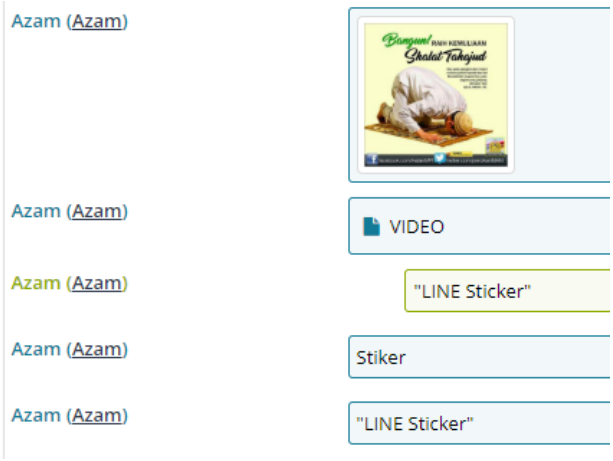

Fig. 9. LINE Messenger Analysis in MOBILedit Forensic.

Both of forensic tools have the ability to analyze the data, but in different way. In this experiment, MOBILedit is perform better than Oxygen Forensics.

D. Data Report

Oxygen forensic has the ability to create reports in the form of pdf, rtf, xls, xml, csv, tsv, and html. While MOBILedit has the ability to create reports in html, pdf, and excel formats. In oxygen forensic, only pdf files that unable work properly while others are pretty good. In MOBILedit report is very complete and works entirely.

E. Case Management

Case management in Oxygen Forensics is reliable for deeper analysis. While on MOBILedit, there is no case management like in Oxygen forensic. For this feature, MOBILedit has to consider for completed their tools.

F. Deleted Data Retrieval

The function for deleted data recovery was found on the MOBILedit forensic express. While on Oxygen this function the researcher did not find it. This function is helpful in criminal cases where the perpetrator removes some data from digital devices.

TABLE III. EVALUATION RESULT FROM OXYGEN FORENSIC AND MOBILEDIT FORENSIC

Function	Oxygen Forensic	MOBILedit Forensic Express
Device Identification	As expected	As expected
Data Extraction	As expected	Not As expected
Case Management	As expected	N/A
Deleted Data Retrieval	N/A	As expected
Messenger Application Analysis	61,90%	76,19%
Data Report	90%	100%

Table 3 shows a summary of the results from tools evaluation that we have been done. It can be seen that MOBILedit looks better than Oxygen. However, for some functions, such as data extraction and case management, MOBILedit needs to consider installing it on the tool.

V. CONCLUSION

Analytical ability of MOBILedit Forensic has the highest index number as much as 76.19% while Oxygen Forensic has 61.90% of index number. In this case LINE messenger analysis. Oxygen Forensic can be better in data report than MOBILedit forensic. MOBILedit has a limit in extracting video in LINE messenger. However, MOBILedit Forensic is don't have case management function to as in Oxygen Forensic, but MOBILedit is very efficient in term of data report and data extraction.

VI. FUTURE WORK

Considering the growing number of smartphones and forensic methods emerging, research on forensic evaluation has to be done. In Future work, the researchers suggest the evaluation of forensic methods and forensic tools more detailed, so that the reference to this issue more complete. Some suggestions about the evaluation parameter can be discuss in the further research as well as additional variations of forensic tools that can be evaluated.

REFERENCES

[1] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," Int. J. Comput. Sci. Inf. Secur., vol. 3, no. 5, pp. 29–36, 2017.

[2] I. Riadi, A. Fadlil, and A. Fauzan, "Evidence Gathering and Identification of LINE Messenger on Android Device," Int. J. Comput. Sci. Inf. Secur. (IJCSIS), vol. 16, no. June, pp. 201–205, 2018.

[3] U. Kumar Singh, C. Joshi, U. Neha Gaud, and U. Chanchala Joshi, "A Framework for Digital Forensic Investigation using Authentication Technique to maintain Evidence Integrity," Int. J. Comput. Appl., vol. 154, no. 6, pp. 975–8887, 2016.

[4] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on mobile device forensics," NIST Spec. Publ., vol. 1, no. 1, p. 85, 2014.

[5] R. Umar, I. Riadi, and G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," Int. J. Adv. Comput. Sci. Appl., 2017.

[6] T. Sutikno, L. Handayani, D. Stiawan, M. A. Riyadi, and I. M. I. Subroto, "WhatsApp, viber, and telegram: Which is the best for instant messaging?," Int. J. Electr. Comput. Eng., 2016.

[7] I. Riadi and A. Firdonsyah, "Forensic Investigation Technique on Android ' s Blackberry Messenger using NIST Framework," Int. J. Cyber - Secur. Digit. Forensics (IJCSDF) Soc. Digit. Inf. Wirel. Commun., vol. 6, no. 4, pp. 198–205.

[8] S. Saleem, O. Popov, and I. Baggili, "A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis," Digit. Investig., 2016.

[9] A. K. Kubi, S. Saleem, and O. Popov, "Evaluation of some tools for extracting e-evidence from mobile devices," 2011 5th Int. Conf. Appl. Inf. Commun. Technol. AICT 2011, no. 10, 2011.

[10] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Evaluation of integrated digital forensics investigation framework for the investigation of smartphones using soft system methodology," Int. J. Electr. Comput. Eng., 2017.

[11] N. Widiyasono, I. Riadi, and A. Luthfi, "Investigation on the services of private cloud computing by using ADAM Method," Int. J. Electr. Comput. Eng., vol. 6, no. 5, pp. 2387–2395, 2016.

[12] E. Benkhelifa, B. E. Thomas, L. Tawalbeh, and Y. Jararweh, "Framework for Mobile Devices Analysis," Procedia Comput. Sci., vol. 83, pp. 1188–1193, 2016.

[13] K. Curran, A. Robinson, S. Peacocke, and S. Cassidy, "Mobile Phone Forensic Analysis," Int. J. Digit. Crime Forensics, vol. 2, no. 2, pp. 1941–6210, 2010.

[14] J. Beckett and J. Slay, "Digital forensics: Validation and verification in a dynamic work environment," Proc. Annu. Hawaii Int. Conf. Syst. Sci., no. February 2014, 2007.

[15] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. June, pp. 949–955, 2018.

[16] National Institute of Standards and Technology, "Mobile Device Tool Specification Version 2.0," 2016.

[17] Y. Guo, J. Slay, and J. Beckett, "Validation and verification of computer forensic software tools-Searching Function," Digit. Investig., vol. 6, no. SUPPL., 2009.