Comparative Analysis of Forensic Software on Android-based Blackberry Messenger using NIJ Framework

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
imam.riadi@is.uad.ac.id

Sunardi
Department of Electrical Engineering
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
sunardi@mti.uad.ac.id

Arizona Firdonsyah
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
arizona.f@gmail.com

***Abstract*— Instant Messaging application is the most widely used application all over the world. Blackberry Messenger is a multiplatform instant messaging application with lots of features that can be a magnet for many people to use it as a tool for commiting digital crimes. In the process of investigating digital crime cases, digital evidences are required, and to obtain digital evidence, a set of forensic tools are needed to conduct forensic process on physical evidences. The topic of this research is to describe the forensic process and to compare the current forensic tools used based on acquired digital evidences by using method that refers to mobile device forensic guidelines made by the National Institute of Justice (NIJ). The forensic tools used in this research are Magnet AXIOM, Belkasoft Evidence Center, and MOBILedit Forensic Express. The outcome shows that Magnet AXIOM has the highest capability to obtain digital evidences, Belkasoft Evidence Center has superiority in terms of data text acquisition, and MOBILedit Forensic Express has superiority in physical evidence preserving and cloning.**

Keywords—Smartphone, Android, Digital Evidence, Blackberry Messenger, Digital Forensics

I. INTRODUCTION

The development of mobile operating system, especially Android is growing rapidly, this can be seen from many types of Android-based gadget with various brands and features that emerges almost every week. The rapid development of Android technology has an impact on the growing number of applications developed for the Android platform, including instant messaging applications. Developers are competing to create instant messaging applications with user friendly features.

There are many free instant messaging application available now which allow people to communicate using texts, phone calls, videos, etc, and to maintain contact with them even internationally. Recent studies have shown that the most popular instant messengers are WhatsApp, Viber, Telegram [1], and Blackberry Messenger (BBM). BBM is one of the multi-platform instant messaging applications that has many users that increase significantly each year. A survey titled "WhatsApp vs LINE vs BBM" that conducted by JakPat Mobile [2] reported that BBM is still a leading instant messaging application in Indonesia. Figure 1 shows the percentage of BBM users in Indonesia with 89,35%, followed by LINE with 77,42%, and WhatsApp ranked third with 74,19%.

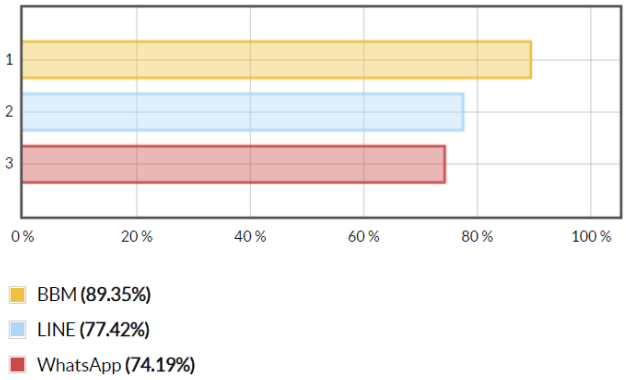

Figure 1. Graphical percentage of BBM users in Indonesia based on JakPat Mobile's Survey.

With the amount of BBM users that rapidly growing, the possibility of digital crimes that occured is also increased. Information obtained from the web site of Indonesian National Police Public Relations [3] that the crime using the Blackberry Messenger always occurred and are likely to increase, as shown in Table 1.

TABLE I. DIGITAL CRIME THAT USING BBM IN INDONESIA

No	Year	Case
1	2015	Covert prostitution transaction via BBM in Bangka Belitung
2	2016	Cyberbullying in BBM leads to massive fighting at Gorontalo
3	2016	BBM account of DPR members in Jakarta being hacked
4	2017	Online fraud and money laundering at Bangka Belitung
5	2017	Online prostitution transaction via BBM at Pekanbaru

The Increasing number of digital crimes using smartphone's messaging applications such as BBM requires law enforcement agencies to be more thorough in investigating digital crime. This investigative process requires structured analysis and a set of forensic tools to obtain digital evidence from BBM. In this research, the researchers will try to elaborate the investigative steps to obtain digital evidence and

conduct a comparative analysis on forensic tool's performance based on acquired digital evidences and features.

According to Dogan and Akbal [4] that conducted a comparative study using Oxygen Forensic Suite 2014 and MOBILedit Forensics, it can be explained that every forensic tool has its own advantages and disadvantages. This research's result shows that MOBILedit Forensics has advantages in terms of run time, while Oxygen Forensic Suite 2014 has an advantage in terms of artifact analysis.

Other comparative analysis research is conducted by Maurya, Awasthy, Singh, and Vaish [5] by using 2 proprietary forensic tools and 3 open source forensic tools, The conclusion is that many of the features that are present in proprietary forensic tools are also present in open source tools. Even there are certain features that provided by open source tool but proprietary tool does not, for example: SHA-1 hashing is not provided in EnCase but available in open source tools.

Comparison and analysis of proprietary and open source forensic tools also conducted by Padmanabhan, Lobo, Ghelani, Sujan, and Shirole [6] with the tools put into comparison are The Sleuth Kit (TSK) Autopsy, SANS SIFT, MOBILedit Forensics, and Cellebrite UFED. The results of this research are: open source forensic tools have advantages in the number of users, flexibility in terms of use with console commands or GUI- based applications, logging capability, and good in tolerating errors, and proprietary forensic tools are superior in terms of processing speed, the accuracy of data extraction, analytical features, and data restoring ability.

Another comparative research counducted by Salem, Popov and Kubi [7] using Cellebrite UFED and XRY shows that XRY is better than Cellebrite UFED for acquiring most of the artifact types, while Cellebrite UFED is better on preserving the integrity of digital evidence.

II. Research Methodology and Tools

The objective of this research was to describe the forensic process and evaluate forensic tools. Magnet AXIOM, Belkasoft Evidence Center, and MOBILedit Forensics Express will be used and evaluated based on parameters from from researchers in terms of the ability to perform BBM's forensic analysis on Android.

A. Research Methodology

The U.S. National Institute of Justice (NIJ) has published a process model in the Electronic Crime Scene Investigation Guide, the process model consists of the following steps [8]:

1. Preparation: Prepare the equipment and tools to perform the tasks required during an investigation.
2. Collection: Search for, document, and collect or make copies of the physical objects that contain electronic evidence.
3. Examination: Make the electronic evidence visible and document contents of the system. Data reduction is performed to identify the evidence.
4. Analysis: Analyze the evidence from the Examination phase to determine the significance and probative value.
5. Reporting: Create examination notes after each case.

And the diagram is shown at Figure 2

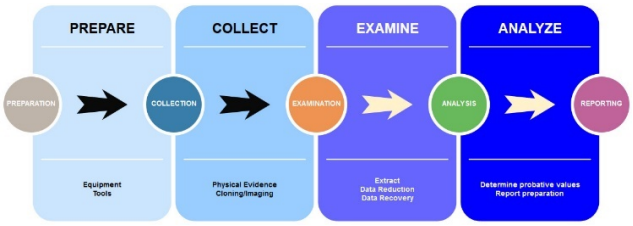

Figure 2. NIJ Forensics Method Diagram.

Based on the framework, the steps of the research are divided into five: software installation, evidence preservation/cloning, extraction experiment, result evaluation and analysis, and the last step is reporting as shown on Figure 3

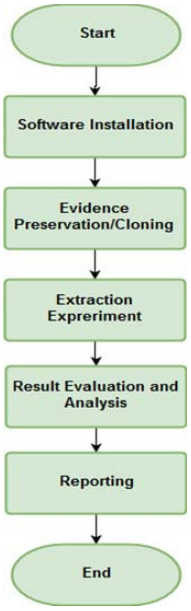

Figure 3. Flowchart of research's steps.

The flowchart can be described as follows:

• Software Installation: The researchers will install forensic tools that will be compared on the notebook.

• Evidence Preservation/Cloning: The researchers will perform the cloning process on smartphone devices to preserve and maintain data integrity.

• Extraction Experiment: The researchers will perform Extraction process on smartphone devices using Magnet AXIOM, Belkasoft Evidence, and MOBILedit Forensic Express.

• Result Evaluation and Analysis: The performance of each forensic tool will then be analyzed based on software features and digital evidence obtained from each device.. The

Universitas Ahmad Dahlan

parameters used are adjusted to the objective of the research, namely, Blackberry Messenger analysis.

• Reporting: The evaluation and analysis of forensic tools are presented..

B. Research Tools

The research tools used in this research are divided into two parts: Experimental tools and Forensic tools. Experimental tools related to hardware and experimental objects, while Forensic tools are the tools that will be used to acquire digital evidences. Table II describes both tools.

TABLE II. EXPERIMENTAL AND FORENSIC TOOLS

Experimental Tools		
No	***Tools***	***Description***
1	Notebook	Asus SonicMaster X450J, OS Windows 10 64bit
2	Data Cable	A data cable that can be used to connect laptop with smartphone
3	Smartphone 1	Sony Xperia SL, OS Android Jellybean
4	Smartphone 2	Samsung Galaxy A5 2015, OS Android Marshmallow
5	Blackberry Messenger	A multiplatform instant messaging application
Forensic Tools		
No	***Tools***	***Description***
1	Magnet AXIOM	Windows-Based Applications that can be used to acquire digital evidence on a smartphone
2	Belkasoft Evidence Center	Windows-Based Applications that can be used to acquire digital evidence on a smartphone
3	MOBILedit Forensic Express	Windows-Based Applications that can be used to acquire digital evidence and make smartphone's system copy

III. RESULTS AND DISCUSSION

A. Preparation

Preparation stage is a process of preparing physical evidence that will be used to conduct forensic investigation process as shown on Figure 4, and to determine what kind of digital evidences that will be extracted from physical evidence as shown on Table III.

Figure 4. Smartphones as Physical Evidence.

TABLE III. BBM'S DIGITAL EVIDENCE

No	***Digital Evidence***	***Description***
1	BBM Profile	Digital Evidence/Artifact related to the owner of BBM Account
2	BBM Contact	A list of BBM Contact, including BBM PIN
3	BBM Chat	Digital Evidence/Artifact related to BBM user's conversation data
4	BBM Transferred Picture/File	Pictures/Files transferred among BBM users
5	BBM Invitation	An invitation to communicate using BBM for other BBM users

B. Collection

At this stage, physical evidence collection, documentation, and preservation will be conducted. The process at this stage is conducted by checking the type of evidence, specifications, operating system, IMEI, android versions, and other related data. The content of physical evidences may vary depends on the evidence's condition. Table IV shows the results.

TABLE IV. PHYSICAL EVIDENCE SPECIFIATION

Physical Evidence 1		
	Brand	Sony
	Serial	Xperia
	Model	SL
	Model #	LT26ii
	IMEI	353617051988xxx
	OS	Android
	Version	4.1.4 (Jellybean)
	Processor	Dual core
Physical Evidence 2		
	Brand	Samsung
	Serial	Galaxy
	Model	A
	Model #	SM-A500F
	IMEI	-
	OS	Android
	Version	6.0.1 (Marshmallow)
	Processor	Quad core 1.2 GHz Cortex-A53

To maintain the integrity of physical evidence so as not to change, the cloning process of this android smartphone is also conducted by using MOBILedit Forensic Express since this tool is the only tool that have this feature, other tools might do the cloning process while running data extraction. The cloning process and result is as shown on Figure 5.

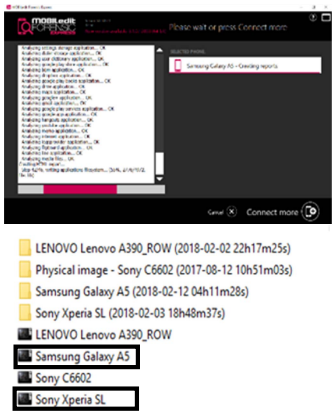

Figure 5. Cloning Process and Results.

C. *Examination and Analysis*

Examination and Analysis is the process of retrieving, searching, and analyzing data from physical evidence. In this stage, The examination process is conducted by reducing the search data only on BBM applications. Figure 6 and Figure 7 shows the results of the examination result using Magnet AXIOM for both physical evidences.

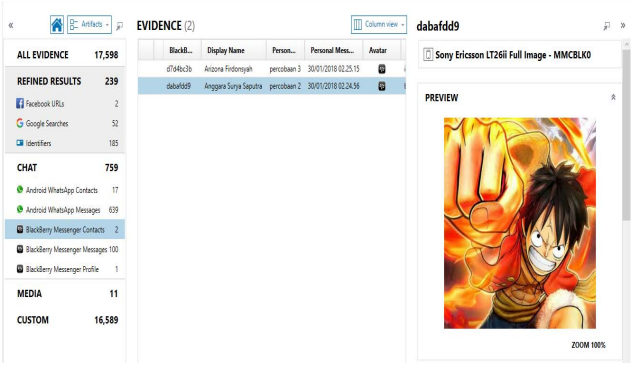

Figure 6. Physical Evidence 1 Examination Result using Magnet AXIOM.

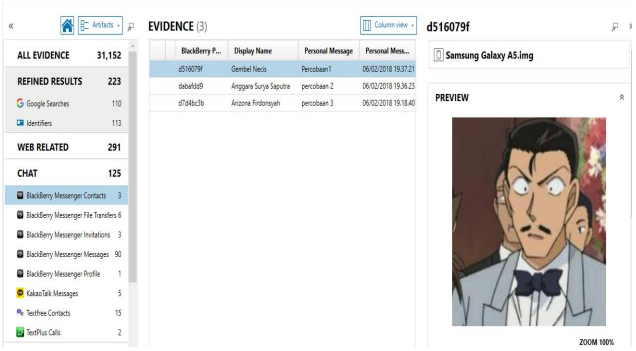

Figure 7. Physical Evidence 2 Examination Result using Magnet AXIOM.

Examination result that acquired using Magnet AXIOM provide a set of Contact List, BBM Invitation, BBM File Transfer, BBM Chat, and BBM Account Owner's Profile. Magnet AXIOM has the ability to conduct physical and logical extraction, so in this research, the researchers did physical extraction on Physical Evidence 1, and logical extraction on Physical Evidence 2.

As shown on Figure 8 and 9, examination process using Belkasoft Evidence Center resulted in BBM Chat and Pictures.

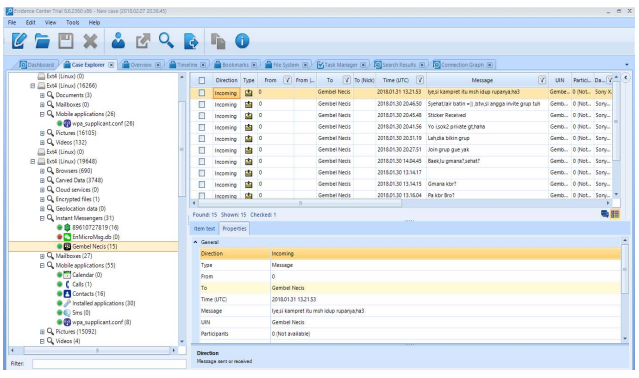

Figure 8. Physical Evidence 1 Examination Result using Belkasoft.

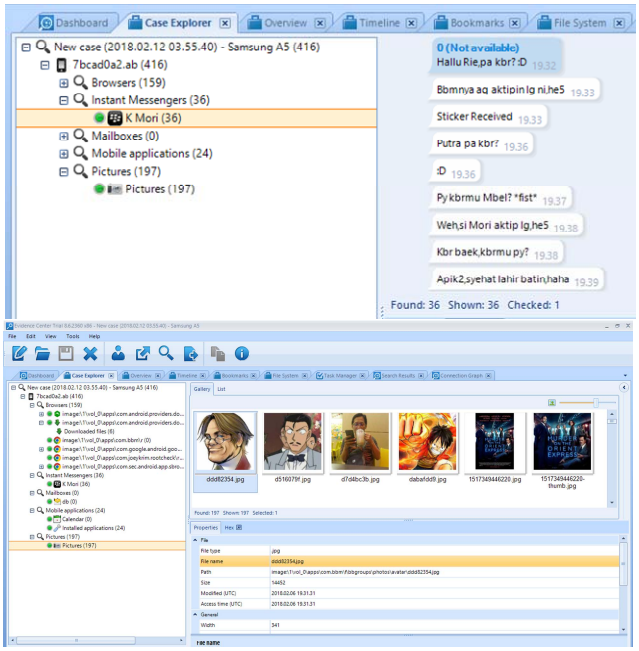

Figure 9. Physical Evidence 2 Examination Result using Belkasoft.

Belkasoft Evidence Center also has the ability to do physical and logical extraction, so as well as Magnet AXIOM, the researchers did physical extraction on Physical Evidence 1 and logical extraction on Physical Evidence 2.

MOBILedit Forensic Express is a tool with backup and cloning features, by using this feature, forensic examiners are able to maintain the integrity of physical and digital evidences. Examination process that using MOBILedit Forensic Express resulted in a set of HTML report that can be accessed via browser. The examination result for both physical evidences is shown on Figure 10.

Based on the results of this analysis, a full forensic report contained a summary of acquired digital evidences and performance comparison of forensic tools can be presented.

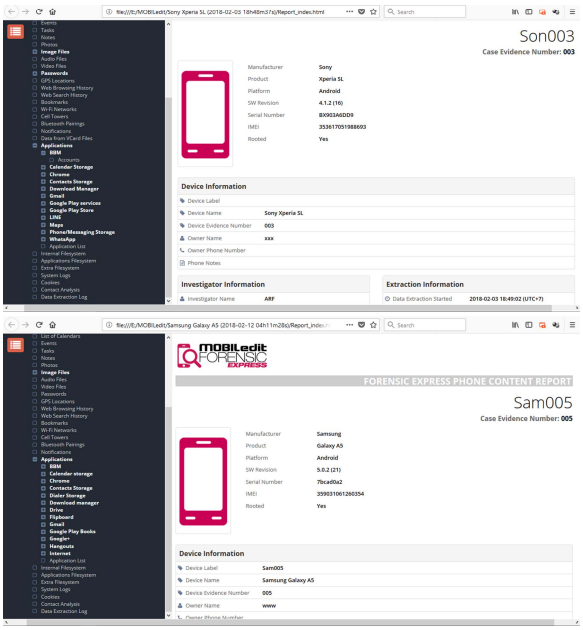

Figure 10. Physical Evidence 1 and 2 Examination Result using MOBILedit Forensic Express.

D. Reporting

Reporting [9] is the last stage on NIJ framework. Here, the report will be presented in 2 comparison tables based on software features and based on digital evidence obtained by each device. Feature-based comparison result is as shown in Table V.

TABLE V. FEATURE-BASED EVALUATION RESULT

Measurement Parameters	Forensic Tools		
	Magnet AXIOM	Belkasoft Evidence Center	MOBILedit Foresic Express
Physical Extraction Capability	√	√	√
Logical Extraction Capability	√	√	√
Physical Evidence Preserving and Cloning Capability	-	-	√
Report Generation	√	√	√

The researchers used calculations with index numbers to determine the performance of each forensic tool in accordance with the experiment results. The calculation of index number used is unweighted index as shown in equation 1 [10].

$$Par = \frac{\sum ar0}{\sum arT} x\ 100\% \quad (1)$$

Where:

Par = Percentage of index number
ar0 = Digital Evidence/Artifact gained by Forensic Tool
arT = Total Digital Evidence/Artifact

MOBILedit Forensic Express has superiority in preserving and cloning capability because this tool has the ability to create cloning file that can be read by other tool. By using equation 1 to calculate the index number from each forensic tool, MOBILedit Forensic Express has the highest index number of 100%. Belkasoft Evidence Center and Magnet AXIOM each has an index number of 75%.

TABLE VI. DIGITAL EVIDENCE-BASED EVALUATION RESULT

No.	BBM's Digital Evidence	Forensic Tools		
		Magnet AXIOM	Belkasoft Evidence Center	MOBILedit Foresic Express
1	BBM Profile	√	√	√
2	BBM Contact	√	√	-
3	BBM Chat	√	√	-
4	BBM Transferred Picture/File	√	√	-
5	BBM Invitation	√	-	-

Table VI shows the results of performance analysis conducted on each forensic tool related to the acquired digital evidences. By using the same equation, MOBILedit Forensic Express got 20% performance index score by only managed to acquire 1 type of BBM Digital Evidence, Belkasoft Evidence Center got 80% performance index score, and Magnet AXIOM got the highest index performance score of 100% because it successfully acquired all 5 types of BBM Digital Evidences.

IV. CONCLUSION

Related to Digital Evidence extraction capability, Magnet AXIOM has the highest index number at 100%, followed by Belkasoft Evidence Center with index number at 80%, and MOBILedit Forensic Express with index number at 20%. MOBILedit Forensic Express has weakness in extracting BBM's Digital Evidences. However, related to physical evidence's backup and data preservation, MOBILedit Forensic Express has the highest index number at 100% and manages to make physical evidence backup that can be used by another tool, while Magnet AXIOM and Belkasoft Evidence Center has index number at 75%. The outcome shows that Magnet AXIOM has the highest capability to obtain digital evidences, Belkasoft Evidence Center has superiority in terms of data text acquisition, and MOBILedit Forensic Express has superiority in physical evidence preserving and cloning.

V. FUTURE WORK

For future work, there are many comparative study using many forensic tools such as Oxygen Forensic Suite [11], Andriller [12], Cellebrite UFED Physical Pro and XRY [13] that can be conducted. to get an overview on what forensic tool that best for digital forensic investigations. The comparison also can be conducted on forensic frameworks and parameters such as National Institute of Standard Technology (NIST) [14] [15], and Integrated Digital Forensic Investigation Framework (IDFIF) [16].

ACKNOWLEDGMENT

This research was supported by Lembaga Penelitian dan Pengembangan Universitas Ahmad Dahlan. We also thank our colleagues from Universitas Ahmad Dahlan who provided insight and expertise that greatly assisted the research.

REFERENCES

[1] 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.*, vol. 6, no. 3, pp. 909–914, 2016.

[2] Jakpat Mobile, "WhatsApp vs LINE vs BBM," pp. 1–21, 2016.

[3] I. Riadi, Sunardi, and A. Firdonsyah, "Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework," *Int. J. Cyber-Security Digit. Forensics*, vol. 16, no. 4, pp. 198–205, 2017.

[4] S. Dogan and E. Akbal, "Analysis of mobile phones in digital forensics," *2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron.*, no. October, pp. 1241–1244, 2017.

[5] N. Maurya and J. Awasthi, "Analysis of Open Source and Proprietary Source Digital Forensic Tools," *Int. J. Adv. Eng. Glob. Technol.*, vol. 3, no. 7, pp. 916–922, 2015.

[6] R. Padmanabhan, K. Lobo, M. Ghelani, D. Sujan, and M. Shirole, "Comparative analysis of commercial and open source mobile device forensic tools," *2016 9th Int. Conf. Contemp. Comput. IC3 2016*, 2017.

[7] S. Saleem, O. Popov, and O. K. Appiah-Kubi, "Evaluating and Comparing Tools for Mobile Device Forensics Using Quantitative Analysis," *Stock. Univ.*, pp. 264–282, 2013.

[8] M. Nur Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," *JISKa*, vol. 1, no. 3, pp. 108–114, 2017.

[9] 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. 15, no. 5, pp. 156–160, 2017.

[10] R. Umar, I. Riadi, and G. M. Zamroni, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017.

[11] O. Osho and S. O. Ohida, "Comparative Evaluation of Mobile Forensic Tools," *Int. J. Inf. Technol. Comput. Sci.*, vol. 8, no. 1, pp. 74–83, 2016.

[12] Andriller, "Andriler – Android Forensic Tools," 2017. [Online]. Available: https://www.andriller.com/. [Accessed: 15-Aug-2017].

[13] A. K. Kubi, S. Saleem, and O. Popov, "Evaluation of some tools for extracting e-evidence from mobile devices," in *2011 5th International Conference on Application of Information and Communication Technologies, AICT 2011*, 2011, no. January 2011.

[14] W. C. Barker, "Digital Forensics NIST Information Technology Laboratory," 2012.

[15] National Institute of Standards and Technology, "Mobile Device Tool Test Assertions and Test Plan Version 2.0," 2016.

[16] 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.*, vol. 7, no. 5, pp. 2806–2817, 2017.