

A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements

Rusydi Umar
Department of Informatics
Engineering
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

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

Guntur Maulana Zamroni
Magister of Information Technology
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Abstract—One of the popularly used features on Android smartphone is WhatsApp. WhatsApp can be misused, such as for criminal purposes. To conduct investigation involving smartphone devices, the investigators need to use forensic tools. Nonetheless, the development of the existing forensic tool technology is not as fast as the development of mobile technology and WhatsApp. The latest version of smartphones and WhatsApp always comes up. Therefore, a research on the performance of the current forensic tools in order to handle a case involving Android smartphones and WhatsApp in particular need to be done. This research evaluated existing forensic tools for performing forensic analysis on WhatsApp using parameters from NIST and WhatsApp artifacts. The outcome shows that Belkasoft Evidence has the highest index number, WhatsApp Key/DB Extractor has superiority in terms of costs, and Oxygen Forensic has superiority in obtaining WhatsApp artifact.

Keywords—Whatsapp; acquisition; NIST parameters; artifact

I. INTRODUCTION

Smartphones with the Android operating system were introduced to the public in 2007; and it became the most popular operating system in 2011, judging from the sales [1]. In the fourth quarter of 2016 the number of smartphone sales with android operating system is 379.98 million units, as shown in Fig. 1.

Some popular smartphone features are messaging (88%), email (70%), Facebook (62%), camera (62%), and WhatsApp (51%) [2]. In [3], authors conducted a survey on instant messaging application, WhatsApp, Viber, and Telegram. From the survey results, WhatsApp tops the list at 60%. In terms of the user number, WhatsApp has increased significantly from year to year [4]. As of July 2017, the number of WhatsApp users has as many as 1.3 billion users as in Fig. 2. WhatsApp has various features, for instance sending and receiving text messages, pictures, videos, and documents. WhatsApp also comes with phone call and video call features. WhatsApp has been equipped with end-to-end encryption technology that serves to secure sent messages. With end-to-end encryption, the messages sent can only be read by senders and recipients [5].

It is impossible to separate WhatsApp from misuse. The large number of users and the end-to-end encryption technology used can be a magnet for someone with a criminal

purpose such as drug trafficking, cyber-bullying, trafficking, and so on. There are some cases involving IM or WhatsApp applications [6]. In a case involving smartphone devices, the investigator needs to do mobile forensics. Mobile forensics is one of the forensic digital branches that learn on how to perform evidence recovery from a smartphone device. The investigator will perform forensic analysis of smartphone devices using forensic tools with a forensically-tested methodology, thus the analysis results are valid before the law and can be used as means of evidence [7].

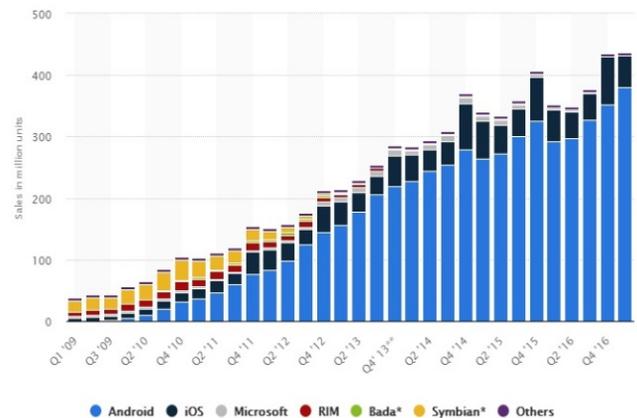


Fig. 1. Statistics of smartphone operating systems.

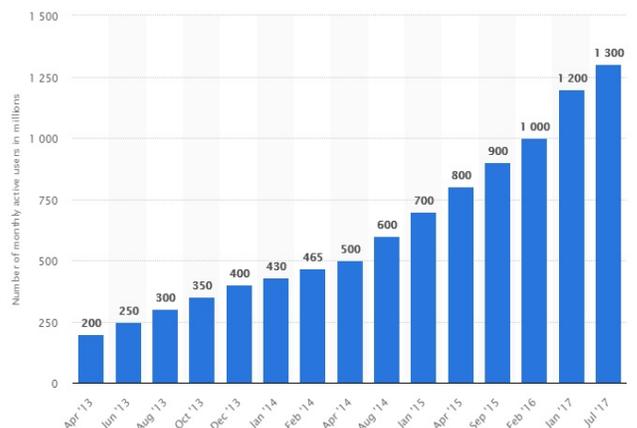


Fig. 2. Number of WhatsApp user statistics.

According to [8], there are three forensic acquisition techniques: manual, physical, and logical. In the manual acquisition, the investigator will manually create the acquisition by directly looking at the contents of the smartphone device to find evidence. The advantage of manual acquisition is that investigators do not require forensic tools to create acquisitions. Manual acquisition has constraints in terms of the integrity of the evidence as investigators will directly examine the evidence which may result in the possibility of data changes. In physical acquisition, the investigator will clone a smartphone device. The cloning results will then be analyzed using forensic tools. In logical acquisition, the investigator will perform the data acquisition found in the smartphone device to be subsequently analyzed.

In [9], authors performed forensic analyzes using Oxygen Forensic and MOBILedit. The researchers argue that every forensic tool has its own advantages and disadvantages. It can be handled using several forensic tools that have different capabilities in addressing cases related to smartphone devices. MOBILedit has advantages in terms of run time, while Oxygen Forensic has an advantage in terms of artifact analysis. In other research conducted by [10] using Oxygen Forensic tools managed to find artifacts of call logs, text messages, media files (photos, video, audio), internet data, geolocation, applications, and social media data. In [10], authors also explained that mobile forensic has several challenges, such as: malicious programs, lack of availability of tools, password recovery, accidental reset, and anti-forensic technique.

In [11], authors performed comparisons and analysis of commercial forensic and open source tools. The tools put into comparison are TSK Autopsy, SIFT, MOBILedit, and Cellebrite UFED. The researcher believes that No. 1 forensic tool is perfect for performing all processes. 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. Meanwhile, commercial forensic tools are superior in terms of process speed, data extraction accuracy, and analytical skills. Commercial forensic tools also have the ability to restore deleted data. In [12], authors also conducted mobile forensic analysis using Celebrite UFED in order to determine the extent of forensic tool performance. In [12], authors obtained information on IMSI and ICCID. The artifacts, such as call logs, social media chat, contact list, email, SMS, and media files (audio, documents, image, video) also retrieved. In [12], authors added that each of the forensic tools has the possibility to produce different outputs. Therefore, an investigator should know what forensic tool he should use for a case.

The development of mobile technology and the large number of smartphone devices on the market become a challenge for investigators. One of the challenges of mobile forensics is the lack of resources in the sense that the rapid development of mobile technology and the growing number of smartphone devices are not put in a balance by the development of forensic mobile technology and the existing forensic tools [13].

NIST released a test plan to measure the performance of a forensic tool in a publication entitled “Mobile Device Tool

Test Assertions and Test Plan ver. 2” and “Mobile Device Tool Specification ver. 2” [14], [15]. NIST argues that increasing the number of smartphone devices each year gives problems in forensics cases. Therefore, a method is needed to measure the ability of forensic tools on the market. NIST provides 42 measurement parameters and methods to measure the performance of forensic tools based on the results of each test plan.

Judging from the development of mobile technology and WhatsApp technology, WhatsApp’s popularity, the possibility of cases involving WhatsApp, and previous research, the researcher conducted a comparative evaluation of forensic tools for WhatsApp analysis on Android-based smartphones. The forensic tools used are WhatsApp DB/Key Extractor, Belkasoft Evidence, and Oxygen Forensic. The performance and ability to perform WhatsApp forensic analysis from each forensic tool will be evaluated using the NIST forensic tool parameter and additional parameters from the researcher. The research’ results will be used as a recommendation for investigators when handling cases related to WhatsApp.

II. METHODOLOGY AND TOOLS

The objective of this study was to evaluate forensic tools. WhatsApp DB/Key Extractor, Belkasoft Evidence and Oxygen Forensic will be evaluated based on parameters from NIST and additional parameters from researchers in terms of the ability to perform WhatsApp’s forensic analysis on Android.

A. Research Methodology

The research used the steps as in Fig. 3. The steps of the research are divided into four: experiment simulation, forensic analysis, analysis result, and conclusion.

- Experiment Simulation: Fig. 4 shows the experimental simulations performed. User A’s smartphone device will be used to communicate with User B and simulates the daily use of WhatsApp, such as sending messages, making calls, receiving pictures. User A’s Smartphone then will be used for forensic analysis in the next step. User A’s smartphone used in the research is Samsung Galaxy S4 GT-I9500 with Android Lollipop 5.0.1 operating system and it has been rooted. WhatsApp version used in this research is version 2.17.351.
- Forensic Analysis: The researches will perform forensic analysis on smartphone devices using the WhatsApp DB/Key Extractor, Belkasoft Evidence, and Oxygen Forensic. The forensic analysis will be conducted under closed conditions in the sense that smartphone devices will be converted into Airplane Mode to maintain data integrity.
- Result Analysis: The performance of each forensic tool will then be analyzed using NIST parameters and additional parameters from the researcher. The parameters used are adjusted to the objective of the research, namely, WhatsApp analysis.

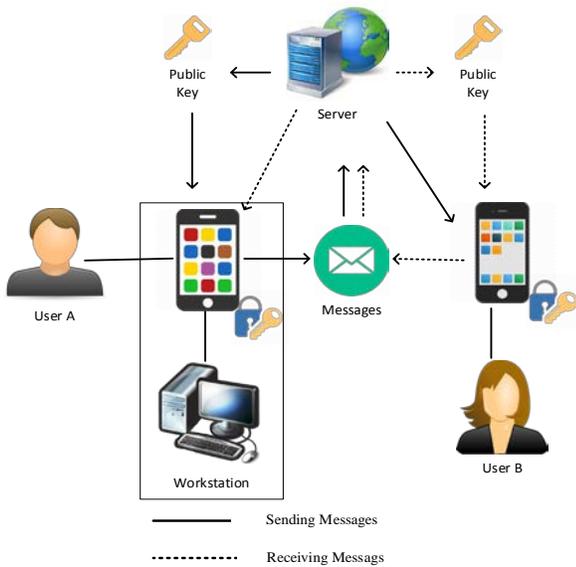


Fig. 3. Experiment simulation.

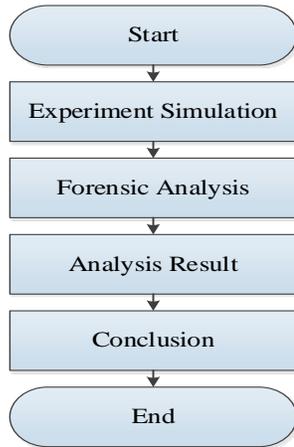


Fig. 4. Research methodology.

- Conclusion: The evaluation of forensic tools using NIST parameters and additional parameters are presented.

B. Research Tools

The research tools used in this research are divided into two: Experimental tools and forensic tools. Table I describes the experimental tools used in the research. Table II describes the forensic tools used in the research.

TABLE I. EXPERIMENT TOOLS

No	Experiment Tool	Description
1	Samsung Galaxy S4 GT-I9500	Android Lollipop 5.0.1, Rooted
2	WhatsApp	Instant Messaging application, Ver. 2.17.351
3	Workstation	Windows 7 64 Bit, Intel i5-4440, 4.00 GB RAM
4	USB Cable	Connecting smartphone to workstation

TABLE II. FORENSIC TOOLS

No.	Forensic Tool	Version	Description
1	WhatsApp DB/Key Extractor	4.7	Open source
2	Belkasoft Evidence (Trial ver)	8.4	Proprietary
3	Oxygen Forensic	6.4.0.67	Proprietary

TABLE III. NIST FORENSIC TOOL PARAMETERS

Core Assertions	Optional Assertions	Core Features Requirements	Optional Features Requirement
MDT-CA-01	MDT-AO-01	MDT-CR-01 A	MDT-RO-01 A
MDT-CA-02	MDT-AO-02	MDT-CR-02 A	MDT-RO-02 A
MDT-CA-03	MDT-AO-03	MDT-CR-03 A	MDT-RO-03 A
MDT-CA-04	MDT-AO-04		
MDT-CA-05	MDT-AO-05		
MDT-CA-06	MDT-AO-06		
MDT-CA-07	MDT-AO-07		
MDT-CA-08			
MDT-CA-09			

Here, the researcher used parameters from NIST as on Table III. NIST lists the measurement parameters of forensic tools on two written reports entitled “Mobile Device Tool Specification” and “Mobile Device Tool Test Assertions and Test Plan”. The measurement parameters are divided into cores and optional. The division is done based on the type of acquisition made. Core leads to logical acquisition features and capabilities. Meanwhile, optional leads more to physical acquisition features and capabilities. In this research, the researcher does not include the parameters of MDT-CA-10 and the parameters on Universal Integrated Circuit Card (UICC) because the data on WhatsApp application are in the internal memory, not on UICC.

Researcher adds several additional measurement parameters as shown in Table IV. The additional parameters are more focused on the abilities of forensic tools to extract artifacts from WhatsApp for logical acquisition and physical acquisition. Additional parameters listed are essential for investigator during investigation related to WhatsApp.

TABLE IV. WhatsApp ARTIFACT

Artifact
Contact lists WhatsApp
Call Log WhatsApp
Text
Images
Video
Documents

be acquired individually or as a whole, as shown in Fig. 10 in accordance to the parameters of MDT-CA-01, MDT-CA-02, and MDT-CA-03. Investigators can choose what data needed for acquisition and will reduce acquisition run time. Fig. 11 shows the notification when there is a disruption to the acquisition process using Belkasoft Evidence. Notification feature during connection interruption is in accordance with MDT-CA-04 NIST parameter.

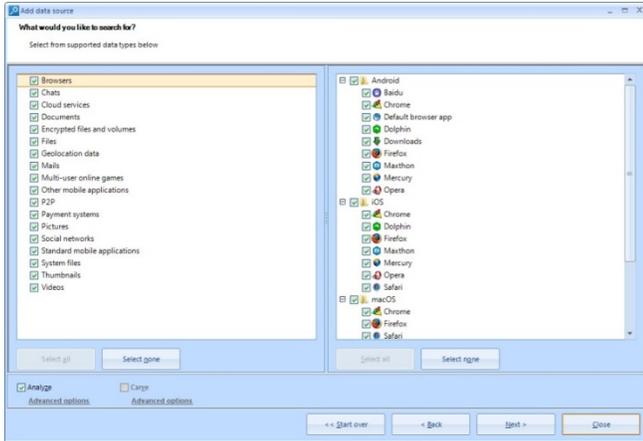


Fig. 10. Belkasoft evidence acquisition options menu.

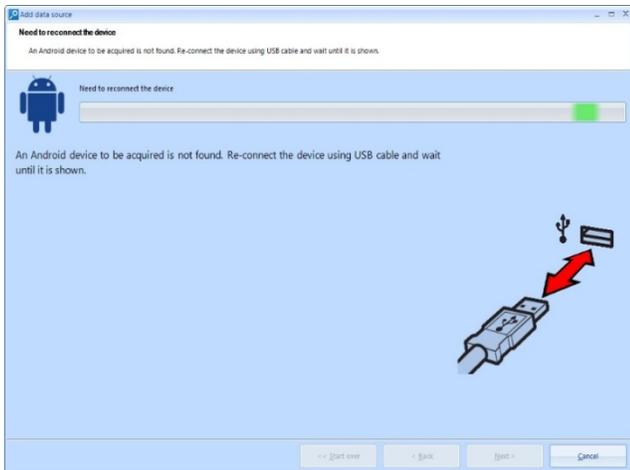


Fig. 11. Belkasoft evidence error notification.

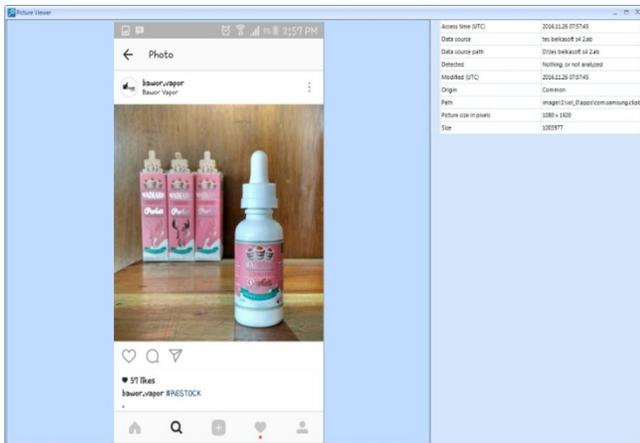


Fig. 12. Belkasoft evidence image artifact.

<input type="checkbox"/>	Time (UTC)	Type	Message	Recipient Id
<input type="checkbox"/>	2017.10.29 23:20:51	1	Baik2	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.29 09:00:06	0	いまわどこですか	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.29 08:59:47	0	こんいちわ	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.29 05:52:24	0	DD	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.22 09:54:01	0	call_screen_presented	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.22 09:53:21	1	call_screen_presented	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.14 06:18:52	0	yuhu	62823 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.14 04:49:50	1	Ra	62823 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.14 04:48:12	1	Masuk bos	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.14 04:47:51	0	Masuk gak?	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.08 10:29:02	0	Tes diterima	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.08 10:29:02	0	Tes diterima	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.08 10:29:02	0	Tes diterima	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.08 10:29:02	0	Tes diterima	62813 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.08 10:28:42	1		62823 [REDACTED]@s.whatsapp.net
<input type="checkbox"/>	2017.10.08 10:28:42	1		62823 [REDACTED]@s.whatsapp.net

Fig. 13. Belkasoft evidence message artifact.

In logical acquisition, Belkasoft Evidence failed to retrieve contact list artifact of WhatsApp, WhatsApp call log, and text messages. The researcher only managed to find images, video, and document artifacts. Video and document artifact files can be opened, simplifying the analysis process. Fig. 12 shows image artifact obtained using Belkasoft Evidence. The image artifact obtained comes with considerably large pixel resolution, so that it not blurred when being zoomed in.

Text message artifact is successfully obtained using the physical acquisition Belkasoft Evidence as in Fig. 13. The timestamp information, the contact number of the sender and the recipient of the message can be found. Japanese letter used for experiment and successfully read by Belkasoft Evidence in accordance with NIST MDT-AO-06 parameter.

C. Oxygen Forensic

Just like Belkasoft Evidence, Oxygen Forensic has the ability to perform logical acquisition and physical acquisition. Oxygen Forensic successfully obtains smartphone device information as shown in Fig. 14. Information regarding IMEI and IMSI is able to obtain according to NIST MDT-CA-06 parameter. Oxygen Forensic only has one feature to choose entire data acquisition according to NIST parameter MDT-CA-01, and does not have feature to individually select the data to be acquired.

Samsung Galaxy S IV (GT-I9500)

	Alias	Samsung Galaxy S IV (GT-I9500)
	Retail Name	Samsung Galaxy S IV (GT-I9500)
	Internal Name	GT-I9500
	Platform	Android OS
	IMEI	357 [REDACTED]
	Software Revision	5.0.1
	Rooted	Yes
	IMSI	35719 [REDACTED]
	S/N	4d005016bef2b099
	Extracted by version	6.4.0.67
	Extraction started	15-Oct-17 7:54:27 AM
	Extraction finished	15-Oct-17 10:24:16 AM

Fig. 14. Oxygen forensic smartphone information.

TABLE V. EVALUATION RESULTS

Measurement Parameter		Forensic Tools		
		WhatsApp DB/Key Extractor	Belkasoft Evidence (Trial ver)	Oxygen Forensic
Core Assertions	MDT-CA-01	-	√	√
	MDT-CA-02	-	√	-
	MDT-CA-03	-	√	-
	MDT-CA-04	-	√	-
	MDT-CA-05	-	√	√
	MDT-CA-06	-	√	√
	MDT-CA-07	√	√	√
	MDT-CA-08	√	-	√
	MDT-CA-09	-	√	√
Optional Assertions	MDT-AO-01	-	√	√
	MDT-AO-02	-	√	-
	MDT-AO-03	-	√	√
	MDT-AO-04	-	√	√
	MDT-AO-05	-	√	√
	MDT-AO-06	-	√	√
	MDT-AO-07	-	√	√
Core Features Requirements	MDT-CR-01 A	√	√	√
	MDT-CR-02 A	-	√	-
	MDT-CR-03 A	√	√	√
Optional Features Requirements	MDT-RO-01 A	-	√	√
	MDT-RO-02 A	-	√	-
	MDT-RO-03 A	-	√	√
Logical Acquisition Artifact	WhatsApp Contact List	√	-	√
	WhatsApp Call Log	√	-	√
	Text	√	-	√
	Image	√	√	√
	Video	-	√	√
	Document	-	√	√
Physical Acquisition Artifact	WhatsApp Contact list	-	√	√
	WhatsApp Call Log	-	√	√
	Text	-	√	√
	Image	-	√	√
	Video	-	√	√
	Document	-	√	√

IV. CONCLUSION

Belkasoft has the highest index number at 88.23%, followed by Oxygen Forensic with index number at 82.35%, and WhatsApp DB/ Key Extractor with index number at 23.52%. WhatsApp Key/DB Extractor has weakness in keeping up with the NIST parameter criteria. However, WhatsApp Key/DB Extractor manages to get text message artifacts, WhatsApp contact lists, and WhatsApp call logs using logical acquisition. WhatsApp Key/DB Extractor also has superiority in terms of cost because it is an open source forensic tool. Belkasoft Evidence has the highest index number among the three forensic tools used. Belkasoft Evidence almost

meets all the NIST parameters. Belkasoft Evidence has an obstacle in obtaining WhatsApp artifacts using logical acquisition. With logical acquisition, Belkasoft Evidence is unable to get WhatsApp contact list artifacts, WhatsApp call logs, and text messages. Oxygen Forensic has weakness in terms of options to select data for acquisition and notification if there is a connection disruption during the acquisition process. Oxygen Forensic successfully fulfills all WhatsApp artifact parameters with logical acquisition and physical acquisition. Despite Belkasoft Evidence having the highest index number and WhatsApp Key/DB Extractor superiority in terms of cost, Oxygen Forensic is more superior in obtaining WhatsApp artifacts, either through logical acquisition or physical acquisition.

REFERENCES

- Statista, "Global smartphone sales to end users from 1st quarter 2009 to 1st quarter 2017, by operating system (in million units)," 2017. [Online]. Available: <https://www.statista.com/statistics/266219/global-smartphone-sales-since-1st-quarter-2009-by-operating-system/>. [Accessed: 10-Nov-2017].
- "REVEALED: Top uses of our smartphones - and calling doesn't even make the list," 2017. [Online]. Available: revealed: Top uses of our smartphones - and calling doesn't even make the list%0A%0A. [Accessed: 10-Nov-2017].
- 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.
- Statista, "Number of monthly active WhatsApp users worldwide from April 2013 to July 2017 (in millions)," 2017. [Online]. Available: <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/>. [Accessed: 10-Nov-2017].
- J. Koum and B. Acton, "End-to-end encryption," 2016. [Online]. Available: <https://blog.whatsapp.com/10000618/end-to-end-encryption>. [Accessed: 10-Nov-2017].
- B. Bennet, "With Islamic State using instant messaging apps, FBI seeks access to data," Los Angeles Times, 2015. [Online]. Available: <http://www.latimes.com/world/middleeast/la-fg-terror-messaging-20150608-story.html>. [Accessed: 17-Nov-2017].
- R. Ayers, W. Jansen, and S. Brothers, "Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)," NIST Spec. Publ., vol. 1, no. 1, p. 85, 2014.
- N. R. Roy, A. K. Khanna, and L. Aneja, "Android phone forensic: Tools and techniques," Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2016, pp. 605-610, 2017.
- S. Dogan and E. Akbal, "Analysis of Mobile Phones in Digital Forensics," MIPRO 2017, pp. 1241-1244, 2017.
- G. M. Jones and S. G. Winster, "Forensics Analysis On Smart Phones Using Mobile Forensics Tools," Int. J. Comput. Intell. Res., vol. 13, no. 8, pp. 1859-1869, 2017.
- I. Technology, R. Padmanabhan, K. Lobo, M. Ghelani, D. Sujana, and M. Shirole, "Comparative Analysis of Commercial and Open Source Mobile Device Forensic Tools," 2016.
- T. B. Tajuddin and A. A. Manaf, "Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone," 2015 World Congr. Internet Secur. WorldCIS 2015, pp. 132-138, 2015.
- D. M. Sai, N. R. G. K. Prasad, and S. Dekka, "The Forensic Process Analysis of Mobile Device," Int. J. Comput. Sci. Inf. Technol., vol. 6, no. 5, pp. 4847-4850, 2015.
- National Institute of Standards and Technology, "Mobile Device Tool Test Assertions and Test Plan Version 2.0," 2016.
- National Institute of Standards and Technology, "Mobile Device Tool Specification Version 2.0," 2016.