Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 22, No. 3, July 2023, pp. 615∼626
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v22i3.3033

Digital Forensic Analysis of WhatsApp Business Applications on Android Smartphones Using NIST

William Barkem , Jeckson Sidabutar
Politeknik Siber dan Sandi Negara, Bogor, Indonesia

Article Info

Article history:

Received June 01, 2023
Revised July 23, 2023
Accepted July 29, 2023

Keywords:

Android
Digital Evidence
Digital Forensics
MOBILedit
National Institute of Standards and Technology
WhatsApp Business

ABSTRACT

WhatsApp Business is an Android application that can be downloaded on Playstore to serve small business owners. This provides an opportunity for criminals to take advantage of the app's features. These crimes can take the form of fraud, misdirection, and misuse of applications, so digital forensics is necessary because there has never been any research that has done this. This study aims to obtain digital evidence and is carried out on Android smartphones with the WhatsApp Business application installed with four scenarios tested. This study uses the NIST SP 800-101 Rev 1 guidelines with four stages: preservation, acquisition, inspection & analysis, and reporting. The forensic method used is static forensics using the MOBILedit forensic express forensic tools and SysTools SQLite Viewer. The results of this study in scenario 1, by not deleting, get a 100% percentage. Then, scenario 2, namely direct write-off, gets a percentage of 71%. Furthermore, scenario 3, namely uninstalling the application, does not get digital evidence, and scenario 4, namely deleting data through the application manager, also does not get any evidence. The contribution of this research is expected to be a reference in uncovering cases in the WhatsApp Business application with digital forensics.

Corresponding Author:

William Barkem, +6281317923171,
Department of Cyber Security Engineering,
Politeknik Siber dan Sandi Negara, Bogor, Indonesia,
Email: william.barkem@gmail.com

How to Cite:
W. Barkem and J. Sidabutar, "Digital Forensic Analysis of WhatsApp Business Applications on Android-Based Smartphones Using NIST", MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 22, no. 3, pp. 615-626, Jul. 2023.

1. INTRODUCTION

Android is one of the most popular operating systems actively used in many fields, such as banking, payments, transactions, and social networks [1]. Data on Android users support this claim as the most popular operating system in the world, which continues to grow every year. More than 2.5 billion active users are currently in more than 190 countries. WhatsApp Business is an Android application that can be downloaded for free on PlayStore for the needs of small business owners. The WhatsApp business application can send free images, videos, audio, files, and calls provided it is connected to the internet [2]. This application is used to communicate with the business world because communication with buyers is very important [2]. The WhatsApp Business application was first launched in 2018, and in 2021 global users recorded around 220.5 million downloads of the application. This data is supported by the number of countries using the WhatsApp Business application in June 2022, and Indonesia is in second place with around 73.12 million downloads. However, this WhatsApp business app is not protected from offenses such as fraudulent business activities, misdirection, and abuse of circumstances in entering into or performing business contracts, which are still very likely to occur. For every crime committed, he must show evidence, including digital evidence. The evidence that is usually stored and transmitted on electronic devices is digital evidence. Criminals often try to hide or remove traces of digital evidence from electronic devices resulting from crimes. Therefore, digital forensics is becoming an important part of almost every criminal investigation conducted, given the amount of information available and the opportunities that electronic data offers to be able to prove a crime [3]. Digital forensics is a branch of forensic science that plays an important role in obtaining digital evidence from digital devices to be brought to the courtroom [4]. In digital forensics, there is a section that conducts inspections, namely mobile forensics, which examines digital evidence stored on mobile devices such as call logs, short message service (SMS), emails, photos, videos, and others to determine communication between criminals or map factors related to the crime. Digital evidence is any information processed by electronic media to support or refute hypotheses about the state of digital artifacts or digital events that have potential relevance and evidentiary value for criminal investigations [5]. Implementing forensic investigation or analysis must apply appropriate digital forensic standards to obtain valid digital evidence to be presented in court [6].

Some studies conducted digital forensics of the WhatsApp application on Android smartphones using the NIST Special Publication (SP) 800-101 Rev 1 standard. The first is Shadi Zakarneh [7]. This study conducted a forensic investigation of WhatsApp application crimes to determine digital evidence using the NIST method. This research results in finding forensic artifacts of the WhatsApp application in the form of contacts, messages, deleted messages, calls, photos, audio files, video files, and documents. Second is Gede Agus Surya Atmaja and I Komang Ario Mogi [8]. In this study, they also conducted forensics of the WhatsApp application using the NIST method. Based on this research, digital evidence was obtained through chat content found on the perpetrator's smartphone by looking through the application database. Meanwhile, in this study, a digital forensic analysis of the WhatsApp business application using NIST will be carried out, where this application focuses on small and medium-sized businesses that are widely used to communicate business [2]. This Mulia Fitriana, Khairan AR, and Jiwa Malem Marsya [9] conducted a forensic analysis of the WhatsApp application using the NIST method. This research produces forensic procedures in conducting WhatsApp application investigations to obtain previously deleted evidence in the form of conversation sessions, lists of contact numbers, victim profile photos, and others. Fourth is Sang Putu Febri Wira Pratama, I Gusti Ngurah Anom Cahyadi Putra, Muhammad Akbar Hamid, Calvin Christian, I Ketut Kusuma Merdana [10] conducted a digital photographic analysis of Twitter applications on Android using the National Institute of Justice (NIJ) method. The relationship between this research and the research conducted by the author is the tools used, namely MOBILedit Forensic Express and SysTools SQLite Viewer. This research found conversations related to online prostitution, which were then used as digital evidence.

The difference between this research and previous research is that no one has ever done digital forensics of the WhatsApp Business application. Even though the application is a place of crime for business, by utilizing the features in the application that are not owned by the regular WhatsApp application, therefore, this research will analyze the digital forensics of WhatsApp business applications on Android-based smartphones using NIST SP 800-101 Rev 1 to obtain digital evidence. The forensic investigation process in this study uses the NIST SP 800-101 Rev 1 standard as a guide in conducting digital forensics. NIST SP 800-101 Rev 1, entitled "Guidelines on Mobile Device Forensics," aims to assist organizations in developing appropriate policies and procedures for handling mobile devices and preparing forensic specialists for conducting proper smartphone examinations [11]. The NIST SP 800-101 Rev 1 standard has four stages in conducting mobile forensics: preservation, acquisition, examination, analysis, and reporting [11]. In this research, testing will be carried out by simulating crimes and four test scenarios that utilize the features of the WhatsApp business. The results of each test scenario will be analyzed by comparing crime simulation data using WhatsApp business to obtain digital evidence.

Based on the research conducted, it is compiled into a paper that begins with an explanation of the research method used, namely NIST SP 800-101 Rev 1. This method will be tested based on four scenarios that have been made, namely, 1) No data deletion is performed. 2) Data deletion is carried out directly in the WhatsApp business application. 3) Uninstall the WhatsApp business application via the Google Play Store. 4) Data deletion using Application Manager. To support testing, forensic tools are used in the form of MOBILedit Forensic Express and SysTools SQLite Viewer. When testing NIST SP 800-101, Rev 1 is the main reference source in carrying out testing, consisting of four stages: Preservation, Acquisition, Examination & Analysis, and reporting. In preservation, the process of maintaining the integrity of potential digital evidence is carried out during the testing process, which is then continued with the stage of obtaining information from a mobile device called acquisition. Furthermore, conducting an examination of the information or digital evidence obtained previously and conducting an analysis by looking at the examination results for direct significance and evidentiary value. After all the sequences are complete, the last one is reporting by writing down every detail of the digital forensics process carried out and drawing conclusions from this research's results.

2. RESEARCH METHOD

The main objective of this research is to obtain digital evidence from the WhatsApp Business application on Android-based Smartphones using NIST SP 800-101 Rev 1 with forensic tools MOBILedit Forensic Express and SysTools SQLite Viewer in the analysis process. The approach taken in this research uses qualitative and quantitative approaches. Data collection and processing methods use a qualitative approach. In contrast, this research uses a quantitative approach to examine the results of digital forensic data, which in this case is digital evidence from the WhatsApp business application. The data sources obtained in this study are based on scenarios created using the WhatsApp Business application.

2.1. NIST

NIST SP 800-101 Rev 1, entitled "Guidelines on Mobile Device Forensics," is one of the standards used in mobile forensics. This guide aims to help organizations develop appropriate policies and procedures for handling mobile devices and prepare forensic specialists for proper examination of mobile forensics in Figure 1 [11].

Figure 1. NIST SP 800-101 Rev 1 Stage

Figure 1 shows the following stages of handling mobile devices in the NIST SP 800-101 Rev 1 standard [11]. First, preservation is the process of maintaining safe custody of property without changing the content or data residing on the device and removable media. Preservation involves searching, recognizing, documenting, and collecting electronic-based evidence. It needs to be preserved to successfully use evidence, whether in court or in less formal processes. Failure to preserve evidence in its original state can jeopardize the entire investigation and potentially lose valuable case-related information. Then, acquisition is the process of obtaining information from mobile devices and their associated media. Conducting this process at the scene has the advantage of minimal loss of information due to battery exhaustion, damage, and others. Unlike a laboratory setting, this process off-site may be challenging in finding a controlled setting to work with appropriate equipment while meeting additional prerequisites. Examination & analysis is an examination that reveals digital evidence, including that which may be hidden or disguised. Results are obtained from the application of established scientifically based methods and should describe the content and state of the data, including source and potential significance. Data reduction separates relevant from irrelevant information after the data has been exposed. The analysis process differs from the examination that looks at the results for their immediate significance and evidentiary value to the case. Examination is a technical process that falls under the authority of forensic specialists, whereas analysis can be performed by roles other than specialists, such as investigators or forensic examiners. The last thing is reporting to process a detailed summary of all the steps taken and conclusions reached in the investigation of a case. Reporting depends on maintaining careful records of all actions and observations, describing the results of tests and examinations, and explaining the conclusions drawn from the data. Good reporting depends on solid documentation, notes, photos, and tool-generated content.

Using NIST in finding valid digital evidence so that it can be used as legally valid evidence and provide understanding for investigators [12]. The digital forensic results of each scenario will be displayed in an easy-to-understand table and analyzed in relation to the digital evidence that has been obtained. The results of this research will be compared with the actions that have been simulated in each scenario with an index number. The index number calculation formula used is an unweighted index equation 1. In the calculation formula, Pon is the expected percentage result, Pn is the amount of evidence obtained from the results of the forensic stage, and P_o is the amount of initial evidence [13].

$$P_{on} = \frac{\Sigma P_n}{\Sigma P_n} \times 100\% \quad (1)$$

The digital evidence index can be obtained from each scenario run based on the calculation formula. Thus, it will be seen what digital evidence is found and not found and how much data is found and lost in each scenario. The digital evidence found will be displayed, complete with the storage path of the evidence.

2.2. Research Scenario

Before testing the scenario, a crime simulation is carried out by utilizing the features in the WhatsApp business application using the perpetrator's smartphone. Some crime simulations that will be carried out on WhatsApp business are group conversations, sending and receiving personalized messages, sending and receiving picture messages, sending and receiving voice note messages, sending and receiving location messages via Google Maps, sending video messages, sending doc messages, receive pdf document messages, send greeting feature messages, sending catalog feature messages, sending a quick reply feature messages, messaging the out-of-hours messaging feature, making voice calls and making video calls.

Scenario creation is done to obtain digital evidence with no specific time limit on the WhatsApp application, as shown in Table 1.

Table 1. Research Scenario Testing

Scenario	Tests Performed
Scenario 1	No data deletion is performed
Scenario 2	Data deletion is done directly on the WhatsApp business application
Scenario 3	Uninstall the WhatsApp business application via Google Play Store
Scenario 4	Data deletion using Application Manager.

Each scenario is performed in Table 1 and an Android-based smartphone with the WhatsApp Business application installed on it.

2.3. Research Tools

In this research, research tools are needed to support this research. This research device consists of hardware and software. This research requires root access on Android devices to support further analysis. An explanation of the devices used can be seen in Table 2 should be placed at the center of the line and provided consecutively with equation numbers in parentheses flushed to the right margin, as in (1). The use of Microsoft Equation Editor or Math Type is preferred.

Table 2. Research Tools Used

No	Tools	Version
1	WhatsApp Business Application	Versi 2.23.6.76
2	Smartphone Xiaomi Redmi 8	Android 10
3	Laptop Legion 5 Pro 16ITH6	Windows 11 Pro 64bit 11th Gen Intel(R) Core (TM) i7-11800H with NVIDIA GeForce RTX 3050
4	USB Cable Type C	Type C 3A
5	MOBILedit Forensic Express	Versi 7.4.0.20393 (64-bit)
6	SysTools SQLite Viewer	Versi 3.0

Based on Table 2, the main research object is the WhatsApp business application. One of the devices used is Xiaomi Redmi 8 with the Android 10 operating system because it can run business communication activities on the WhatsApp business application. Legion 5 pro 16ith6 laptop devices are used to run predetermined forensic tools. Forensic tools used in this research are MOBILedit Forensic Express and SysTools SQLit Viewer. MOBILedit Forensic Express is one of the forensic tools used to view, and extract data from mobile contact lists, call history, messages, multimedia SMS, files, notes, reminders, calendars, raw data applications, IMEI, device OS, SIM card details, ICCID, and location. This tool is also used to retrieve data from cell phone memory with the ability to bypass cell phone backup security pins and passcodes and support the physical consumption of Android devices and SD cards [14]. Calculation of the percentage number of evidence obtained on mobile devices with root conditions using MOBILedit forensic tools forensic express is 100% [14]. In other studies, MOBILedit Forensic Express is superior to other forensic tools, such as Magnet AXIOM, with a percentage of 22.22% [15]. SysTools SQLite Viewer is one of the forensic tools used to view and open the contents of SQLite-compatible database files [16]. This forensic tool also examines the Android-based mobile device database in the form of tables and graphs, and full records. The tool also checks table records with hexadecimal codes and displays information about unfilled, deleted, active, and securely deleted records. Deleted databases can be traced based on the deleted records of a particular table.

3. RESULT AND ANALYSIS

The research successfully obtained the desired digital evidence, where the evidence was obtained from the results of data extraction or databases containing group or personal conversations on the WhatsApp Business application.

3.1. Preservation

After carrying out the scenario on the Android device, all connected connections were disconnected by activating airplane mode on the device, turning off Wi-Fi, and turning off Bluetooth to maintain data integrity. Documentation and labeling of the device are also carried out at this stage. The identification results carried out by researchers are shown in Table 3 as follows:

Table 3. Identification of Electronic Evidence

Electronic Evidence	Identification Results
 	1. Evidence found in a lit state 2. Evidence is a Xiaomi Redmi 8 smartphone 3. The Android version of the evidence is Android 10 4. Android ID of evidence is 37165cb8d2ac8f57 5. The serial number of the proof is 13dbecbd0606 6. The first IMEI of the proof is 860417040768728 7. The second IMEI of evidence is 860417040768736 8. The evidence was found in a rooted condition 9. The IMSI of the evidence is 510115015865226 10. The SIM card of the evidence is from Indonesia 11. ICCID of the evidence is 8962115350158652267 12. The operator used is XL 13. ROM of the evidence is 64 GB 14. 4 GB evidence RAM

3.2. Acquisition

The acquisition stage is the stage of data collection on the device that the scenario has carried out. Data retrieval using the static forensic method is carried out by retrieving data on the internal memory of the Xiaomi Redmi 8 Android device that has been rooted. In carrying out the acquisition stage, it is carried out using forensic tools MOBILedit Forensic Express 7.4.0.203.93 (64-bit). The acquisition stage will be carried out as many of the test scenarios carried out so that as many as four image files will be generated. This stage is carried out every time after carrying out one test by implementing one of the specified test scenarios. The following are the image files resulting from the acquisition carried out in Table 4.

Table 4. Acquisition Results

Image File	Size File	Hash Value (MD5)
skenario1.img	61,071,360 KB	711103c83066c2aa550904dc3f523163
skenario2.img	61,071,360 KB	53194dc97fde9b9aa2cebc89347020ae
skenario3.img	61,071,360 KB	f8f8352c2dc3b55007fc714373b986e9
skenario4.img	61,071,360 KB	869dec5cdb5c3ea2af7d7e80c6ae422c

3.3. Examination & Analysis

After carrying out the acquisition stage of the evidence, the next step is to examine & analyze the results of the acquisition. Application data related to the scenario results on the WhatsApp Business application will be collected so that analysis can be carried out. The examination & analysis stage with static forensics is carried out to find digital evidence of the scenarios that are run using the forensic tools MOBILedit Forensic Express 7.4.0.203.93 (64-bit) and SysTools SQLite Viewer to view the database of the WhatsApp Business application. It should be placed at the center of the line and provided consecutively with equation numbers in parentheses flushed to the right margin, as in (1). The use of Microsoft Equation Editor or Math Type is preferred.

Scenario 1 Based on the results at the acquisition stage, an image file is obtained that draws the events in scenario 1. In the image file, various kinds of information about the electronic evidence smartphone will be analyzed. The following is the digital evidence found in the electronic evidence smartphone after running the first scenario in Figure 2.

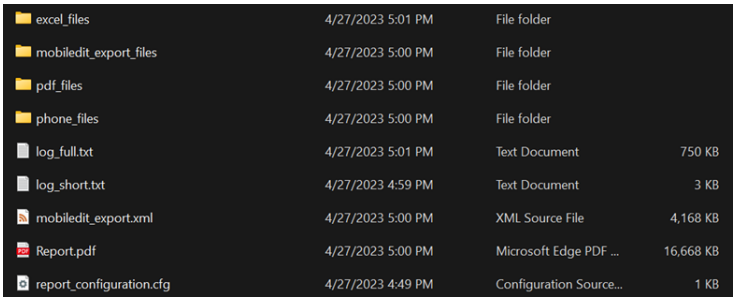

Figure 2. Acquisition results in scenario 1

Figure 2 shows the report.pdf document presented directly by the MOBILedit Forensic Express forensic tools. Various kinds of smartphone information become electronic evidence in this study. The contents of the report.pdf are shown in Figure 3.

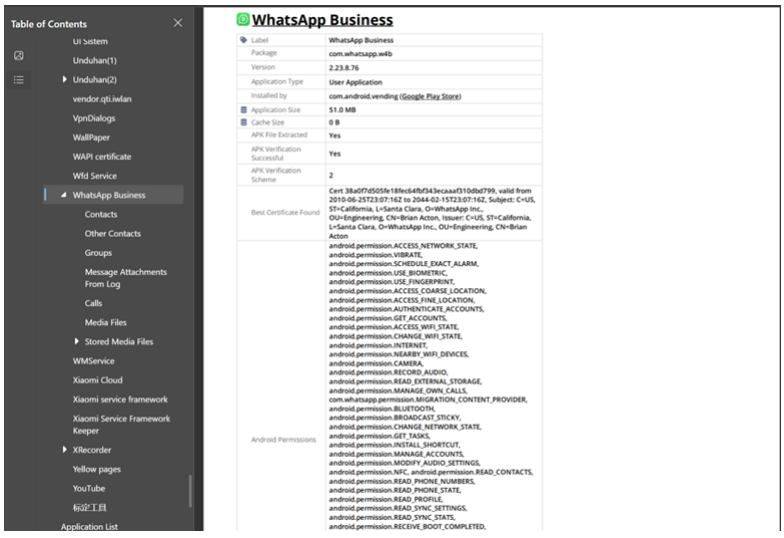

Figure 3. Examination Results Scenario 1

Based on the report.pdf document produced by scenario 1, we can continue the research into the analysis stage to find what digital evidence can be obtained. After conducting the analysis, various kinds of information are obtained that are needed to be related to the case study of the use of crime in the WhatsApp Business application. The following are the findings obtained from the analysis results in Table 5.

Table 5. Digital Evidence Found in Scenario 1

No	Evidence	Scenario	Found
1	Group conversations	9	9
2	Send and receive personalized messages	28	28
3	Send and receive picture messages	7	7
4	Send and receive voice note messages	10	10
5	Send and receive location messages via Google Maps	2	2*
6	Send video messages	5	5
7	Send doc messages	5	5
8	Receive pdf document messages	5	5
9	Send greeting feature messages	1	1
10	Sending catalog feature messages	5	5*
11	Sending a quick reply feature messages	1	1
12	Messaging the out-of-hours messaging feature	1	1
13	Making voice calls	5	5
14	Making video calls	5	5

Notes:
*: log message found, but file not found

Scenario 2 Based on the results at the acquisition stage, an image file is obtained that draws the events in scenario 2. In the image file, various kinds of information about the electronic evidence smartphone will be analyzed. The following is digital evidence found in the electronic evidence smartphone after running the first scenario in Figure 4.

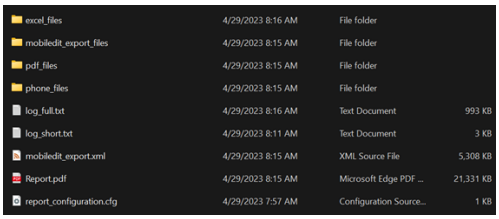

Figure 4. Acquisition results in scenario 2

Figure 4 shows the report.pdf document, presented directly by the MOBILedit Forensic Express forensic tools. Various kinds of smartphone information become electronic evidence in this study. The contents of the report.pdf are shown in Figure 5.

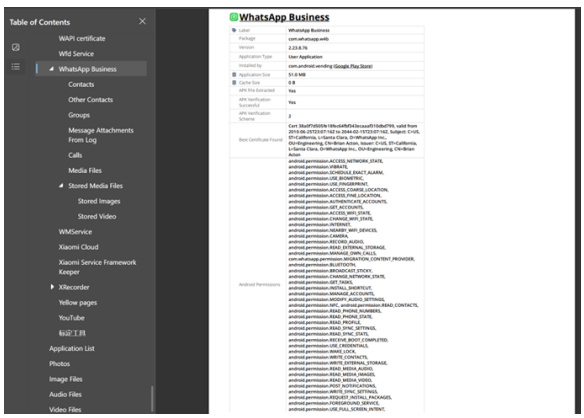

Figure 5. Examination results scenario 2

Based on the report.pdf document produced by scenario 2, we can continue the research into the analysis stage to find what digital evidence can be obtained. After conducting the analysis, various kinds of information are obtained that are needed related to the case study of the use of crime in the WhatsApp Business application. The following are the findings obtained from the analysis results in Table 6.

Table 6. Digital Evidence Found In Scenario 2

No	Evidence	Scenario	Found
1	Group conversations	9	9
2	Send and receive personalized messages	28	0
3	Send and receive picture messages	7	7
4	Send and receive voice note messages	10	0
5	Send and receive location messages via Google Maps	2	2*
6	Send video messages	5	5
7	Send doc messages	5	5
8	Receive pdf document messages	5	5
9	Send greeting feature messages	1	1
10	Sending catalog feature messages	5	5*
11	Sending a quick reply feature messages	1	1
12	Messaging the out-of-hours messaging feature	1	1
13	Making voice calls	5	0
14	Making video calls	5	0

Notes:
*: log message found, but file not found

Scenario 3 Based on the results at the acquisition stage, an image file is obtained that draws the events in scenario 3. In the image file, various kinds of information about the electronic evidence smartphone will be analyzed. The following are digital evidence found in the electronic evidence smartphone after running the first scenario in Figure 6.

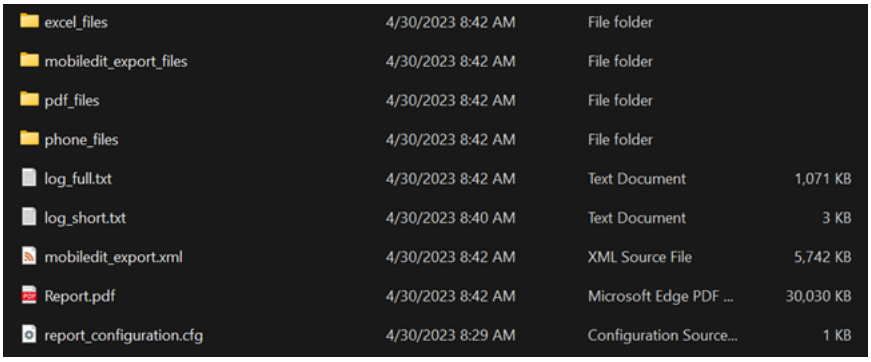

Figure 6. Acquisition results scenario 3

Figure 6 shows the report.pdf document, presented directly by the MOBILedit Forensic Express forensic tools. Various kinds of smartphone information become electronic evidence in this study. The contents of the report.pdf can continue the research into the analysis stage to find any digital evidence that can be obtained. After analyzing, we cannot find any evidence related to the WhatsApp Business application. Instead, only evidence of uninstalling the WhatsApp Business application through the Google Play store is obtained, as shown in Figure 7.

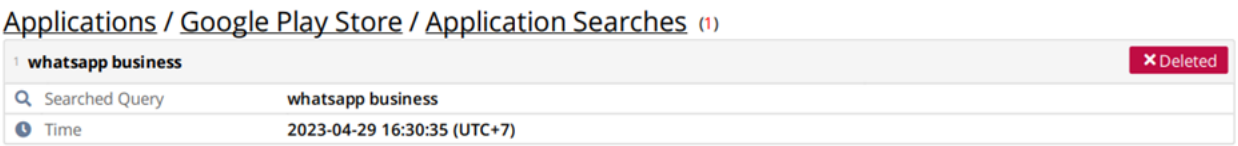

Figure 7. Evidence uninstalling the whatsApp business application via Google Play Store scenario 3

Scenario 4 Based on the results at the acquisition stage, an image file is obtained that draws the events in scenario 4. In the image file, various kinds of information about the electronic evidence smartphone will be analyzed. The following are digital evidence found in the electronic evidence smartphone after running the first scenario in Figure 8.

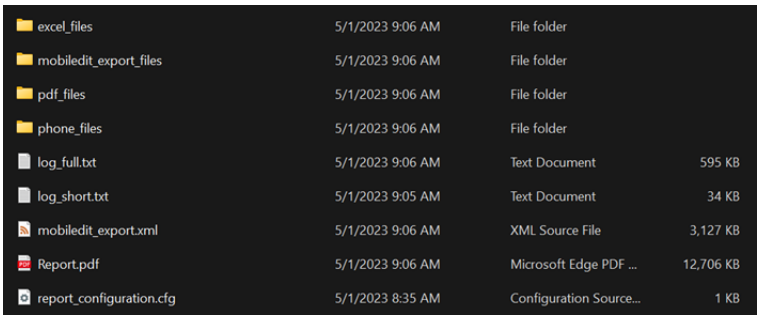

Figure 8. Acquisition results scenario 4

Figure 8 shows the report.pdf document, presented directly by the MOBILedit Forensic Express forensic tools. Various kinds of smartphone information become electronic evidence in this study. The contents of the report.pdf are shown in Figure 9.

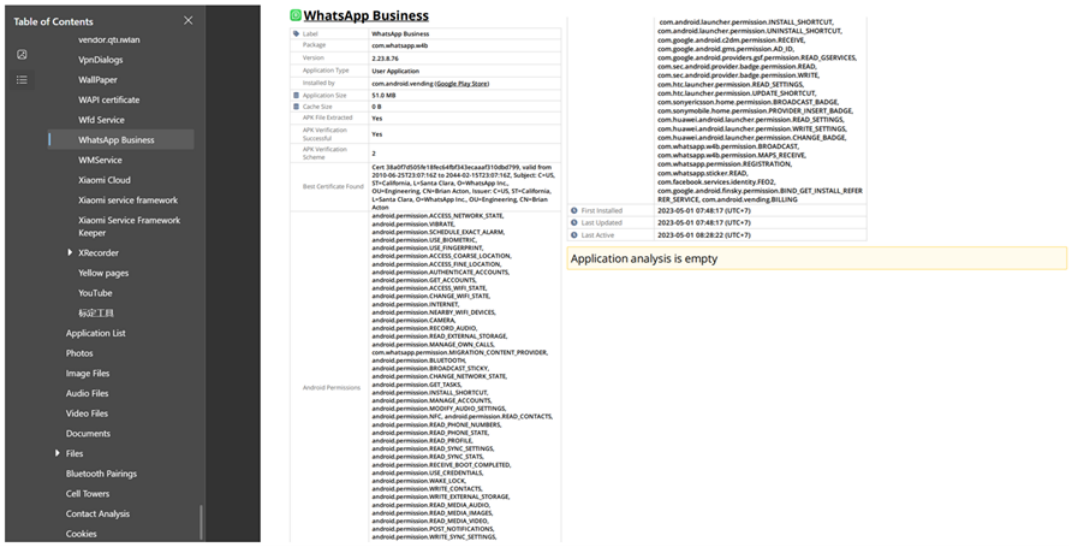

Figure 9. Acquisition results scenario 4

Based on the report.pdf document produced by scenario 4, we can continue the research into the analysis stage to find any digital evidence that can be obtained. After the analysis, no evidence was found related to the WhatsApp Business application but only artifacts from applications previously installed in Figure 10.

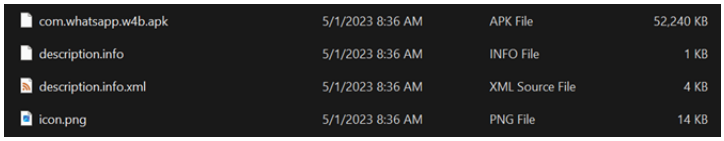

Figure 10. WhatsApp business application artifacts in Scenario 4

3.4. Reporting

In this research, the reporting stage is carried out at each forensic stage, documented, explained, and processed in such a way and adjusted using NIST SP 800-101 Rev 1. The digital evidence found in each scenario will be arranged and sorted in order to form a sequence of events that can be drawn conclusions for each case. The following are the results of digital evidence found from each scenario run compiled in Table 7.

Table 7. Reporting Results

No	Evidence	Scenario 1	Scenario 2	Scenario 3	Scenario 4
1	Group conversations	9	9	0	0
2	Send and receive personalized messages	28	0	0	0
3	Send and receive picture messages	7	7	0	0
4	Send and receive voice note messages	10	0	0	0
5	Send and receive location messages via Google Maps	2	2	0	0
6	Send video messages	5	5	0	0
7	Send doc messages	5	5	0	0
8	Receive pdf document messages	5	5	0	0
9	Send greeting feature messages	1	1	0	0
10	Sending catalog feature messages	5	5	0	0
11	Sending a quick reply feature messages	1	1	0	0
12	Messaging the out-of-hours messaging feature	1	1	0	0
13	Making voice calls	5	0	0	0
14	Making video calls	5	0	0	0
	Total	100 %	71 %	0 %	0%

Based on the results of the research, it is found that there are differences with digital forensic research on ordinary WhatsApp applications conducted by previous studies like contacts, messages, deleted messages, calls, photos, audio files, video files, dan documents [7–9] with forensic tools MOBILedit Forensic Express and SysTools SQLite [10], specifically on the features of the WhatsApp business application. Where in the catalog feature can only be found in the message log. Other features, such as greeting feature messages, quick reply feature messages, and out-of-hours messages, can still be found even though direct data deletion is carried out.

4. CONCLUSION

After the researcher analyzes digital evidence through various stages and experimental scenarios, the researcher can draw conclusions where the results of digital forensic research on the WhatsApp Business application can be seen using NIST SP 800-101 Rev 1 through four scenarios. The first scenario was with no changes or concealment of data, getting 100% digital evidence from 14 evidence of the test results carried out. In addition, the second scenario with file deletion and chat directly on the application gets 10 out of 14 proofs of test results or 71% of the evidence obtained. Meanwhile, the third scenario does not get any digital evidence and only gets evidence of deleting the application through the Google Play Store. Likewise, the fourth scenario does not get any digital evidence and only gets artifacts of previously installed applications. This research shows the effect of forensics on digital evidence focused on the WhatsApp business application where the catalog feature only gets the message log while greeting feature messages, quick reply feature messages, and out-of-hours messages can be found even though direct data deletion is carried out. For further research, researchers suggest using other forensic methods or other forensic tools with the latest version so that it is expected to provide more accurate results. Another suggestion that can be made is to make comparisons with other operating systems, such as Android with IOS.

5. ACKNOWLEDGEMENTS

The authors would like to thank all those who have helped this paper to complete and published, especially editors from Matrik: Journal of Management, Informatics Engineering, and Computer Engineering also Politeknik Siber dan Sandi Negara, which has provided infrastructure support during the research and helped fund the publication of this research.

6. DECLARATIONS

AUTHOR CONTIBUTION

The research was prepared by two authors and divided into their respective tasks. William Barkem conceived and designed the research, collected, analyzed, interpreted the data, and prepared the article. Meanwhile, Jeckson Sidabutar was the supervisor in conducting the research.

FUNDING STATEMENT

This research is supported by the Politeknik Siber dan Sandi Negara, especially the Center for Research and Community Service, in the form of the cost of publishing an accredited national journal.

COMPETING INTEREST

This research has no financial, public, or institutional competing interests.

REFERENCES

[1] D. Özdemir and H. Ç. Zaim, "Investigation of Attack Types in Android Operating System," *Journal of Scientific Reports-A*, no. 046, pp. 34–58, jun 2021.

[2] D. Astria, M. Santi, and S. Muhammadiyah Tulungagung, "Pemanfaatan Aplikasi Whatsapp Bisnis dalam Strategi Pemasaran Online untuk Meningkatkan Jumlah Penjualan," pp. 246–270, dec 2021.

[3] H. Arshad, A. B. Jantan, and O. I. Abiodun, "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence." *Journal of Information Processing Systems*, vol. 14, no. 2, 2018.

[4] X. Zhang and K.-K. R. Choo, *Forensic Education an Experiential Learning Approach*. Springer Cham, 2019.

[5] R. Stoykova, "Digital evidence: Unaddressed threats to fairness and the presumption of innocence," *Computer Law & Security Review*, vol. 42, sep 2021.

[6] M. S. Jafri, S. Raharjo, and M. R. Arief, "Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones," *CCIT Journal*, vol. 15, no. 1, pp. 82–105, 2022.

[7] S. Zakarneh, "Forensic Investigation of WhatsApp on Android Smartphone's," *International Journal of Science, Engineering and Technology*, 2021.

[8] G. A. S. Atmaja and I. K. A. Mogi, "Acquisition of Digital Evidence in Online Scam Cases (CyberCrime) on WhatsApp Chat Application Using NIST Method," *Jurnal Elektronik Ilmu Komputer Udayana*, vol. 9, no. 4, pp. 511–518, 2021.

[9] M. Fitriana, K. Ar, J. M. Marsya, P. T. Informasi, F. Tarbiyah, and D. Keguruan, "Penerapan Metode National Institute of Standars and Technology (NIST) dalam Analisis Forensik Digital untuk Penanganan Cyber Crime," *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, vol. 4, no. 1, pp. 29–39, jul 2020.

[10] S. P. F. W. Pratama, I. G. N. A. C. Putra, M. Akbar, H. Hamid, C. Christian, and I. K. K. Merdana, "Analisis Forensik Digital pada Aplikasi Twitter di Android sebagai Bukti Digital dalam Penanganan Kasus Prostitusi Online," *Jurnal Elektronik Ilmu Komputer Udayana*, vol. 10, no. 3, pp. 271–278, 2022.

[11] W. Jansen, R. Ayers, and S. Brothers, "Guidelines on mobile device forensics," *NIST Special Publication*, pp. 101–800, 2014.

[12] S. Sarjimin, H. Herman, and A. Yudhana, "Perbandingan Tool Forensik pada Mozilla Firefox Private Mode Menggunakan Metode NIST," *Jurnal Algoritma*, vol. 18, no. 1, pp. 283–291, 2021.

[13] I. Riadi, S. Sunardi, and S. Sahiruddin, "Perbandingan Tool Forensik Data Recovery Berbasis Android menggunakan Metode NIST," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 7, no. 1, pp. 197–204, 2020.

[14] A. N. Ichsan and I. Riadi, "Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method," *International Journal of Computer Applications*, vol. 174, no. 18, pp. 34–40, feb 2021.

[15] I. Riadi, H. Herman, and N. H. Siregar, "Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 3, pp. 489–502, jul 2022.

[16] K. D. O. Mahendraa and I. K. A. Mogia, "Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases," *Jurnal Elektronik Ilmu Komputer Udayana p-ISSN*, vol. 9, no. 3, pp. 381–390, 2021.