Scientific Journal of Informatics
Vol. 5, No. 2, Nov 2018
p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method

Imam Riadi[1], Anton Yudhana[2], Muhamad Caesar Febriansyah Putra[3]

[1] Department of Information System, Universitas Ahmad Dahlan, Indonesia
[2] Department of Electrical Engineering, Universitas Ahmad Dahlan, Indonesia
[3] Department of Informatics, Universitas Ahmad Dahlan, Indonesia
Email: [1]imam.riadi@is.uad.ac.id, [2]eyudhana@ee.uad.ac.id, [3]muhamadcaesar16@yahoo.co.id

Abstract

The growth of Android-based smartphone users to access media in communicating using Instagram social media is very fast. Activities are carried out when using Instagram social media in communicating to share information such as sending chat texts and pictures. A large number of Instagram users make this application vulnerable to abuse of Instagram such as pornography crimes from Instagram users. This case can be forensic to get digital evidence in the form of chat text and pictures from Instagram messenger is a feature of Instagram. The investigation in this study uses the National Institute of Standards and Technology (NIST) method which provides several stages of collecting, examining, analyzing, reporting while forensic tools use forensic oxygen and axiom magnets. The results of the recovery and comparison of data result using Oxygen forensics and Axiom Magnets obtained digital evidence in the form of data in the form of images and chat. The data obtained by Magnet Axiom is 100% while forensic oxygen is 84%. These data are the results of the performance of both forensic applications in obtaining digital evidence that has been deleted from the Instagram messenger.

Keywords: Digital, Evidance**,** Instagram, NIST, Smartphone

1. INTRODUCTION

Smartphone technology is growing rapidly. Smartphones are slowly starting to replace the role of computers by increasing the number of features and applications available on mobile devices [1], Android-based smartphones are the most popular with more and more users every year [2]. Smartphones are equipped with various applications for chat, email, telephone, social media, and other applications [3]. The number of Instagram users in the world has experienced rapid growth in 2018. The growth in the number of Instagram social media users in January reached 100 million active users. The United States is the country that has the most active Instagram users, namely 100 million active users while for Indonesia is ranked third for the number of active users with a total of 60 million active users [4]. Instagram growth statistics for active users can be seen in Figure 1.

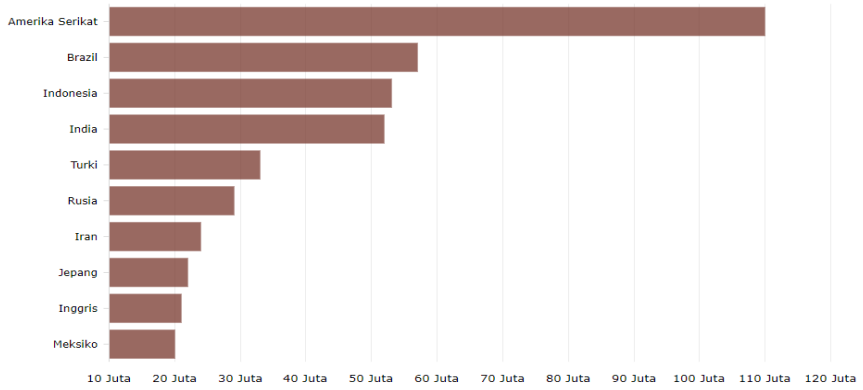

Figure 1. The growth of instagram users in January 2018

Activities carried out by active users to access social media Instagram mostly use smartphones with Android operating systems. The smartphone was introduced to the public in 2007, and became the most popular operating system in 2011, judging by sales in the fourth quarter of 2016 the number of smartphone sales with the Android operating system was 379.98 million unit [5], as shown in Figure 2.

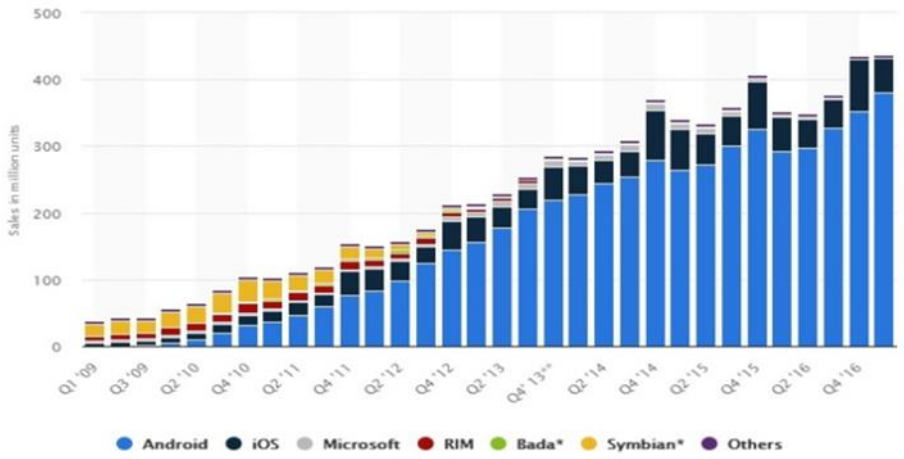

Figure 2. Smartphone sales statistics with various operating systems

Smartphone devices have the same function as computers [6]. This makes more and more active social media Instagram users using smartphones as their access media can provide many benefits in communicating among fellow Instagram users such as sharing photos or chatting. With various features that Instagram has like Instagram Messenger. This feature is more personal in sending messages in the

form of photos or chatting to fellow Instagram users who are sent alone, Instagram Messenger almost has in common with Instant Messaging like Whatsapp, LINE, and others. This helps Instagram users to communicate using this feature which is more personal. But more and more activities in using the Instagram Messenger feature will potentially be exploited by users who are not responsible for cybercrime crime. This crime has many types, but the most potential for pornography crime is a person who uses the Instagram messenger feature by sending messages in the form of photos-chat that contains pornography so that it can cause harm to the recipient of the message. This can be a criminal case that can be a case in court.

Based on the problems described above, the need for forensic handling, especially forensic mobile in helping to solve Pornography crime cases through social media Instagram with Smartphone as media access. From the research that will be carried out is the development of previous studies such as research with the title "Analysis of Digital Evidence on Android-based Instagram Messenger using the National Institute of Justice (NIJ) method" In this study retrieving data on Instagram messenger from cyberbullying cases using OXYGEN Forensic tool with the stages of the NIJ method [4]. Whereas the author develops the research using a different method namely NIST and performs testing using two tools namely OXYGEN Forensic and AXIOM Forensic MAGNET to get a stronger comparison of results from the data on Instagram messengers that are pornographic in the form of photos or chat can become digital evidence under the court.

Digital Forensic is the application of computer science and technology for the sake of legal proof (pro-justice), which in this case is proving high-tech crime or computer scientifically to be able to obtain digital evidence that can be used against violators. Digital forensics has many fields, one of which is mobile forensic. Digital forensics is part of science involves returning to the initial condition and investigation of items found in digital [7]. Digital forensics is a process that assists in the disclosure of a specific digital crime event [8]. Mobile Forensic is the science that performs the process of recovering digital evidence from mobile devices using methods that are appropriate for forensic conditions [9]. mobile forensics retrieves data from the Instagram database installed on the smartphone [10]

Instagram is a photo sharing service application that allows users to take pictures and provide filters and then disseminate them on social networks. Instagram is one of the social media that is being used by smartphone users today. The features Instagram has become a factor for many Instagram users that aims to communicate through social media, one of the newest features is an Instagram messenger, this feature can help in the process of sending photos or chats of privacy that are done along with Instagram users [11].

The Smartphone is the device as the most popular product in the form of mobile phones with an operating system in it that allows users to run various applications, such as the Android operating system [12]. The open-source Android platform

gives developers the freedom to contribute to the rapid growth of the Android market. Android smartphone technology provides an opportunity for application developers to expand the use of applications, especially social media, Instagram on the Android operating system [13]. A smartphone has an Instant Messaging (IM) application, this application can send messages and images quickly to receive messages, Instagram is one of the instant messaging applications [14].

Cybercrime is against the law that uses computer technology based on the sophistication of Internet technology development. Cybercrime is a term that refers to criminal activity with a computer or computer network to become a tool, target, or crime scene. cybercrime is divided into various types of crimes namely online auction fraud, counterfeiting checks, credit/card fraud, trust fraud, identity fraud, pornography [3]. Cybercrime can occur in all electronic devices, such as Android smartphones [15].

2. METHODS

This study refers to the investigation process used by the National Institute of Standard and Technology (NIST) method. This method recommends a basic stage in the forensic process, namely collection, examination, analysis, reporting. The author describes the forensic stages in Figure 3.

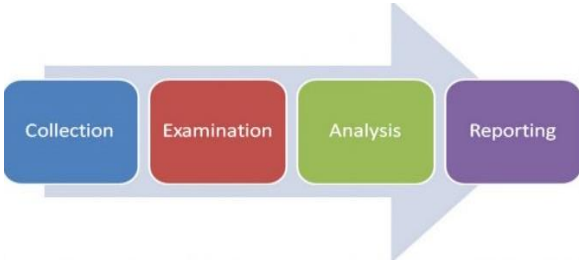

Figure 3. Forensic mobile stages from NIST

Explanation from the National Institute of Standards and Technology (NIST), namely collection, examination, analysis, and reporting as follows.

1. The Collection is a stage that collects, identifies, labels, records, and retrieves data from data sources namely hardware by maintaining the integrity of the original data, maintaining data integrity by isolating physical evidence and backing up data by cloning or image files from items physical evidence.
2. Examination Phase processing data collected forensically using a combination of various scenarios, both automatic and manual, assessing and releasing data as needed while maintaining data integrity.
3. Analysis Phase Analysis performs an analysis of the results of the examination using a method that is technically and legally justified by law to obtain useful information and answer questions that encourage collection and inspection.

4. Reporting The reporting phase is to report the results of an analysis that includes a description of the actions taken, an explanation of the tools and procedures selected, the determination of other actions that need to be carried out (for example forensic checks from additional data sources, security identified gaps or increased security controls), and provide recommendations to improve policies, procedures, equipment, and other aspects of the forensic process [7].

2.1. Case Scenario Process

The research was carried out with a simulated case of Pornography crime. The simulation process is needed to assist the researcher in determining the chronology of the process of the occurrence of indicated cases of pornography crime, while the scenario can be seen as in Figure 4.

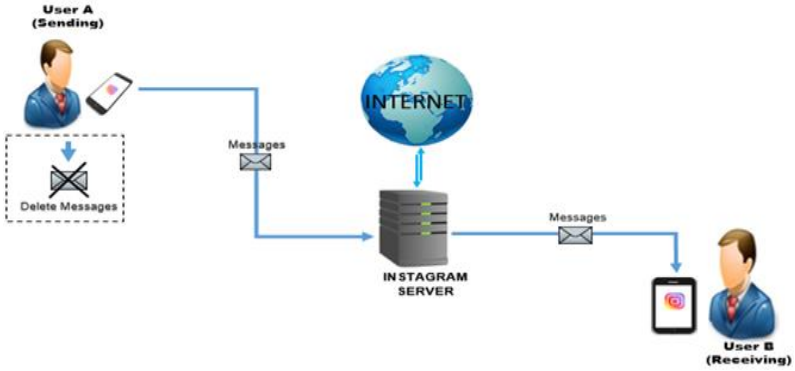

Figure 4. Chronology of using a communication activity and user B using A smartphone with instagram messenger installed

Based on the above case simulation, there are two users using the Instagram application to communicate, namely user a (Message Sender) and user b (Message Recipient). Both users have a smartphone, the user has a smartphone with Samsung Galaxy Star GT-S5282, while the user has a smartphone with Samsung Galaxy GT-S7580. Both have Instagram social media accounts, from the account owned by the user is used to communicate with each other ie sending chat and photos via Instagram messenger feature, user a sends chat and pictures that indicate pornography to the user b, after sending chat and pictures, the user an immediately delete everything to remove evidence. User b reports directly to the authorities for the incident they experienced. Authorities respond directly to user reports b. The next action the authorities issue a search letter to the user to secure the smartphone belonging to the user a that is used as Instagram access media to communicate with the user b. This user a smartphone will be made into electronic evidence. For the next procedure, inspection of the smartphone belonging to the user a will be carried out. In order to be able to identify and return digital evidence in the form of chat and pictures deleted by user b from the smartphone. After that a case that indicates pornography crime can continue in court. Based on the simulation of the

chronology of the cases indicated by pornography crimes described above, then the following stages can be applied to the NIST method, namely Collection, Examination, Analysis, and Report.

2.2. Comparison Method

Comparison of tools is based on the data expected from each tool. Quantitative comparison using percentage formula (1).

$$Pon = \frac{\sum Pn}{\sum Po} \times 100\% \quad (1)$$

Information :
ΣPo = The Result of Data Acquisition Tools
ΣPn = Original Data from Smartphone
Pon = Percentage results are expected [5].

3. RESULTS AND DISCUSSION

3.1. Collection

The Collection Phase collects physical evidence, ie electronic evidence needed to assist in conducting research to gather expected digital evidence. The research was carried out using electronic evidence, namely one smartphone with the Samsung brand with the type Samsung Galaxy Star GT-S5282 can be seen in Figure 5.

Figure 5. Smartphones that become electronic evidence

Electronic evidence in the form of a smartphone with an Android operating system that has an Instagram application installed which is a communication tool that is used to indicate a pornographic crime. Data contained on both Android smartphones will be taken by cloning to avoid changes in data or data deletion that will become digital evidence later to do data acquisition using Forensic Oxygen and Forensic Axiom tools.

3.2. Examination

This stage checks the physical evidence, namely electronic evidence in the form of a smartphone. Data - data that is on this smartphone will be checked using the forensic tool to get the expected digital evidence. The first rare process of this stage is to back up all data by means of Image Data from a smartphone to protect data integrity so that there are no changes from the original data when conducting checks. This process uses the Mobile Edit Express forensic tool can be seen in Figure 6.

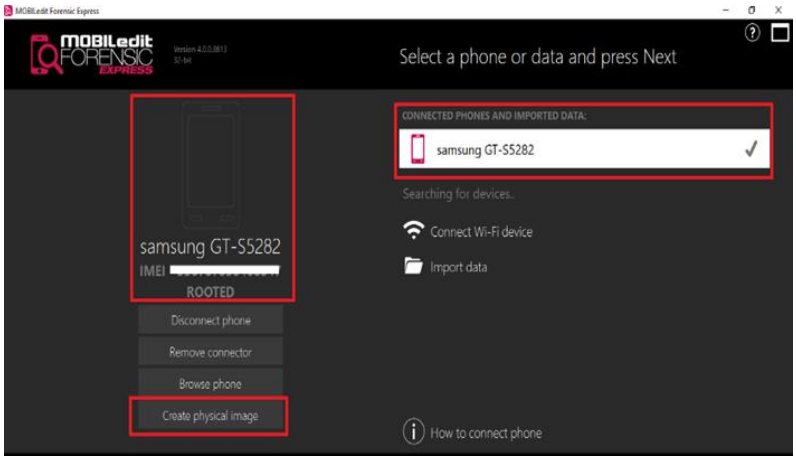

Figure 6. The smartphone is connected to the mobile edit express tool

Image Process Data can be done when electronic evidence in the form of a smartphone has been connected to a computer using a data cable. The Edit Express Mobile Tool installed on the computer can be run automatically and will search for the smartphone device as shown above. Next, to start the imaging process the data uses these tools to produce format data (.img) as shown in Figure 7.

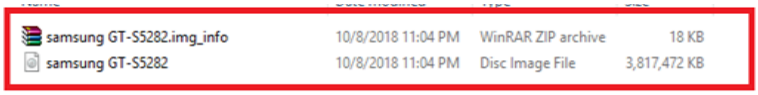

Figure 7. Data image results using the mobile edit express tool

Image Process This data is used to back up data from a smartphone by cloning data by per byte so that it can resemble the original data, the results of image data processing cannot be changed or added and subtracted but can only be opened using other forensic tools for examination purposes.

The results of the data backup process by means of Image data will be stored in the form of ISO with the data type (img). This process can also recover data that has been erased, this depends on the ability of the Car Edit Express tool that is used to restore all data or part of it. For finding out this need for other forensic tools to be

used in the process of checking and analyzing the results of the Image data that has been obtained. Then check the Image data results using Axiom Magnet and Oxygen Forensic tools like Figure 8 and 9.

Figure 8. Smartphones connected with axiom magnet tools

Oxygen Forensic tools connected to a smartphone can be seen in Figure 9.

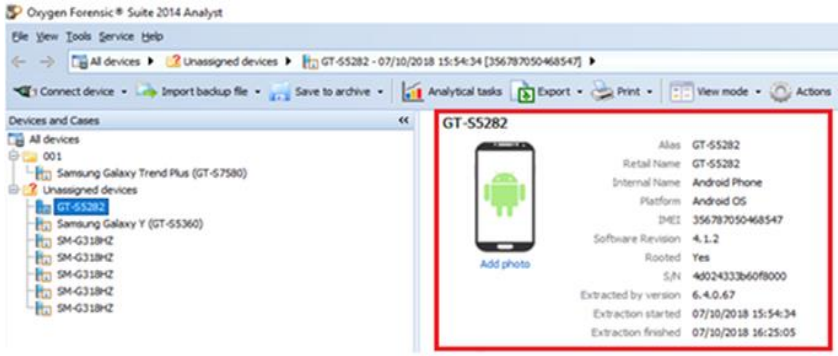

Figure 9. Smartphone connected with oxygen forensic tool

The process of checking the results made using forensic Axiom Magnetics and Oxygen forensic tools has in common that the smartphone must be connected with forensic tools. Image data processing data can be directly generated through the features that are available both of these tools are Load Evidence that can read the results of Image data. Inspection of Smartphone GT-S5282 is electronic evidence belonging to the user b aimed at obtaining digital evidence, namely chat and pictures from the smartphone. The use of Axiom Magnet and forensic Oxygen tools. Both of these tools can acquire data - data that is on the smartphone and check the results of the Image Data which can then be analyzed to become a digital evidence report. The inspection process is carried out in an offline condition the smartphone is connected to the computer using a USB cable to be connected to both of these tools.

3.3. Analysis

The results of the Image Data examination using Magnet Axiom and Oxygen forensic tools obtained some data from the Image data that was successfully recovered using the Mobile Edit Express tool. The results of the examination in the form of data - data will be analyzed as shown in Figure 10.

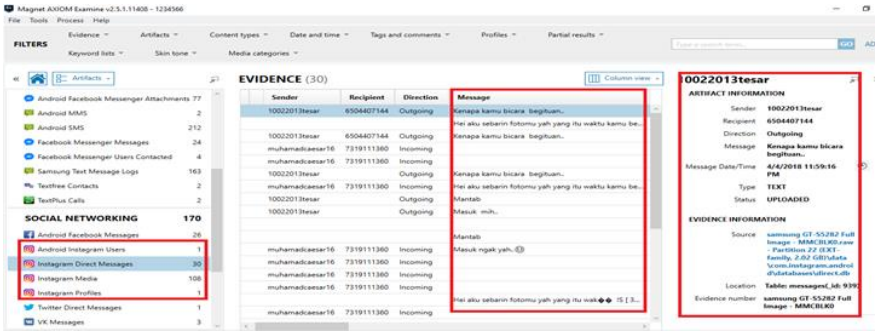

Figure 10. Results of data checking in the form of chatting with the axiom magnet tool

The results of the analysis obtained from the text conversation data in the form of a chat can be known the message content, message status, message type, timestamp, and Instagram owner account. This will be digital evidence while the results of data in the form of images/photos can be seen in Figure 11.

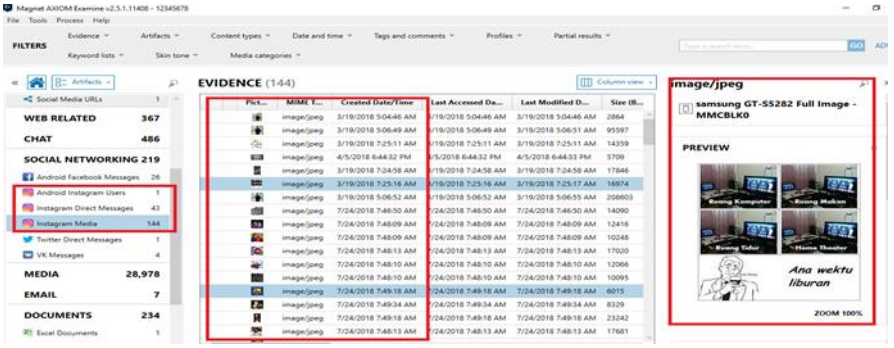

Figure 11. Results of analyzing data in the form of image with axiom magnet

The results of the analysis obtained from the data in the form of images/photos that get everything from Instagram are known, namely the image content, image type, timestamp, and Instagram owner account. Data that is successfully analyzed will be used as digital evidence. Then analyze the results of the Oxygen Forensic in Figure 12.

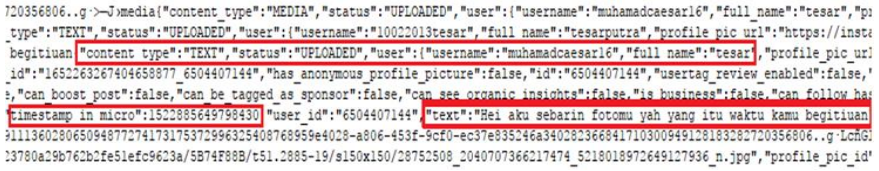

Figure 12. Results of data analysis in the form of chat with oxygen forensic tools

The results of the analysis obtained from the text conversation data in the form of chat can know the message content, message status, message type, timestamp, and Instagram account owner but there are differences in the chat result display from the Oxygen forensic tool that is the results in the form of metadata analyzed in the database (DB) Instagram as in the picture above. This will be digital evidence while the results of data in the form of images/photos can be seen in Figure 13.

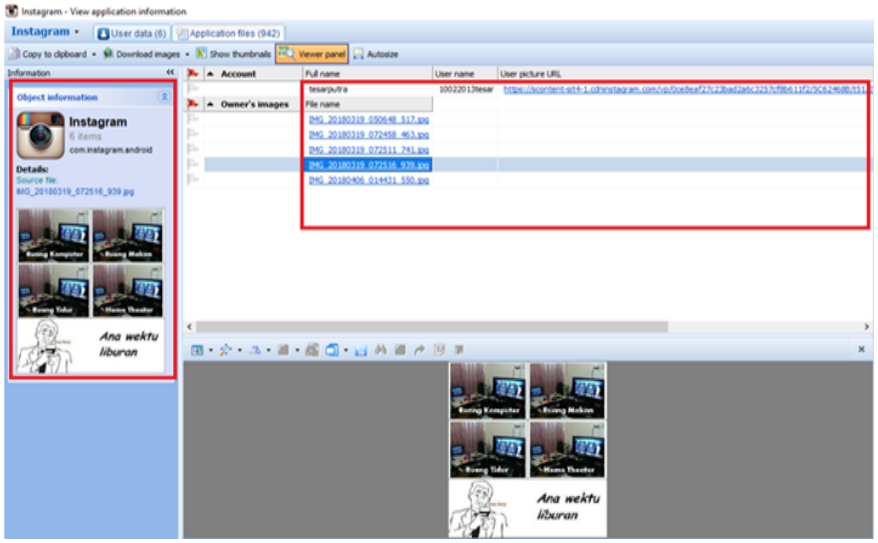

Figure 13. Results of data analysis in the form of images with oxygen forensic

3.4. Reporting

The results of the analysis obtained from the data in the form of images/photos that get everything from Instagram are known, namely image content, type of image, timestamp, and Instagram owner account. The amount of image data analyzed was not as much as that obtained by the Axiom Magnet tool but the images were obtained directly from the Instagram messenger feature. Successful data obtained from both forensic tools can be seen in the Table 1.

Table 1. Results of data recovery from 2 forensic tools

No	Forensic Tools	Digital Evidence	Data recovered from forensic tools	Original Data Smartphone
1	Magnet Axiom	Image	5	5
		Chat	8	8
2	Oxygen Forensik	Image	4	5
		Chat	7	8

Data from the table compared above is obtained from the analysis of the amount of special data from the Instagram Messenger feature which is a place for communication activities carried out by User B for indications of pornographic crime, forensic tool data recovery results compared to the original Instagram messenger data on smartphones. Then the comparison results obtained for the Axiom Magnet tool are 100% while the Oxygen Forensic tool is 84% of the overall data available.

Based on the results of digital evidence obtained by using the tools of Axiom Magnet and Oxygen Forensic namely image and chat. The results of the analysis of the digital evidence obtained specifications compared to the results obtained using 2 forensic tools as in Table 2.

Table 2. Comparison of digital evidence results from 2 forensic tools

Digital Evidance recovered	Specification Digital Evidence	Tools Forensic	
		Magnet Axiom	Oxygen Forensic
Image	1. Image Content	✓	✓
	2. Image Type	✓	✓
	3. Timestamp	✓	X
	4. Account Profile	✓	✓
Chat	1. Chat Content	✓	✓
	2. Chat Status	✓	✓
	3. Chat Type	✓	✓
	4. Timestamp	✓	✓
	5. Account Profile	✓	✓

The label above is digital evidence in the form of image and chat that is obtained using 2 forensic tools. From the digital evidence, there are specifications that become parameters for digital evidence. Each parameter can be compared with the results of each tool used, namely Axiom and Oxygen Forensic Magnets. Based on the results of comparisons of digital evidence is known tools Axiom Magnet more complete the digital proof specifications than Oxygen Forensic. Forensic Oxygen Tools there are deficiencies in the results of digital evidence, namely the timestamp image, while for the results of the amount of image and chat data that is successfully obtained not all are only 84% for the Axiom Magnet tools the overall results of digital evidence data obtained 100%.

4. CONCLUSION

This research was conducted to compare the results of the performance of tools to find digital and chat and pictures from Instagram Messenger installed on Samsung Galaxy Star GT-S5282 smartphones. The forensic process uses the stages recommended by NIST, namely Collection, Examination, Analysis, Reporting. The data obtained is that the Axiom Magnet tool reaches 100% while Forensic Oxygen is 84%. For development, it is recommended to add a tool to get more valid data as digital evidence.

5. REFERENCES

[1] Umar, R., Riadi, I., & Zamroni, G. M. (2018). Mobile forensic tools evaluation for digital crime investigation. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(3): 949-955.

[2] Riadi, I., Umar, R., & Firdonsyah, A. (2018). Forensic Tools Performance Analysis on Android-based Blackberry Messenger using NIST Measurements. *International Journal of Electrical and Computer Engineering*, *8*(5): 3991–4003.

[3] Kohar, A., Riadi, I., & Lutfi, A. (2015). Analysis of Smartphone Users Awareness Activities Cybercrime. *International Journal of Computer Applications*, *129*(2): 1–6.

[4] Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2018). Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ). *Jurnal Teknik Informatika dan Sistem Informasi*, *4*(3): 219–227.

[5] Umar, R., Riadi, I., & Zamroni, G. M. (2017). A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements. *International Journal Of Advanced Computer Science And Applications*, *8*(12): 69–75.

[6] Ruuhwan, R., Riadi, I., & Prayudi, Y. (2017). Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of Smartphones Using Soft System Methodology. *International Journal of Electrical and Computer Engineering (IJECE)*, *7*(5), 2806-2817.

[7] Rizal, R., Riadi, I., & Prayudi, Y. (2018). Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device. *International Journal of Cyber-Security and Digital Forensics*, *7*(4): 382–390.

[8] Kukuh, M., Riadi, I., & Prayudi, Y. (2018). Forensics Acquisition and Analysis Method of IMO Messenger. *International Journal of Computer Applications 179*(47): 9-14.

[9] Riadi, I., Umar, R., & Firdonsyah, A. (2017). Identification of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. *International Journal of Computer Science and Information Security*, *15*(5): 3–8, .

[10] Marfianto, A., & Riadi, I. (2018). WhatsApp Messenger Forensic Analysis Based on Android Using Text Mining Method. *International Journal of Cyber-Security and Digital Forensics*, *7*(3): 319–327.

[11] Remaja. E. S. (2017). Eksistensi Sosial Remaja dalam Instagram. *Visi Komun.*, *16*(1) 151–160.
[12] Faiz, M. N., Umar, R., & Yudhana, A. (2016). Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary. *Jurnal Ilmiah ILKOM*, *8*(3) 242–247.
[13] Putra, R. A., Fadlil, A., & Riadi, I. (2017). Forensik Mobile Pada Smartwach Berbasis Android, J*urnal Rekayasa Teknologi Informasi*, *1*(1), 41-47.
[14] Riadi, I., Fadlil, A., & Fauzan, A. (2018). Evidence Gathering and Identification of LINE Messenger on Android Device. *International Journal of Computer Science and Information Security*, *16*(5): 201–205.
[15] Riadi, I., Sunardi, S., & Fauzan, A. (2018). Examination of Digital Evidence on Android-based LINE Messenger. *International Journal of Cyber-Security and Digital Forensics*, *7*(3): 337–343.