Mobile Forensic on Social Media for the Spread of Covid-19 Hoaxs using National Institute of Justice Method

Lalu Hendri Bagus Wira Setiawan
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Technological advances are currently also very progressive, one of which is marked by the development of information dissemination facilities. Besides being used as a medium for communicating, social media is also often used to disseminate information about the surrounding environment. Social media commonly used by people include Twitter and Instagram. Both of these social media are easily accessible from your smartphone. The progress of the information media is not spared by irresponsible people who use social media to spread false information (hoax), especially in the current situation where the issue of covid-19 is rampant. This is the reason for researching the Twitter, and Instagram applications. It is hoped that this research can find digital evidence in cases of spreading fake news or hoaxes of COVID-19. This study uses forensic tools such as MOBILedit forensic, Magnet Axiom, and Autopsy using the National Institute of Justice (NIJ) method. That is by identification, collection, testing, analysis, and reporting. The results of digital evidence obtained using MOBILedit forensics, namely, accounts, deleted posts, messages, pictures, audio, videos, and documents, Magnet Axiom tools managed to get accounts, pictures, while autopsy tools got pictures, audio, video, and documents.

Keywords

Forensics,Mobile, Hoax,Instagram,Twitter, NIJ

1. INTRODUCTION

Today's technological advances are also very progressive, one of which is marked by the development of information dissemination facilities. Technological developments not only have a positive impact but also have a negative impact[1]. Besides being used as a medium for communicating, social media is also often used to disseminate information about the surrounding environment. Social media commonly used by people include Twitter and Instagram. Both of these social media are easily accessible from your smartphone.

In today's era of digital information, the use of mobile devices, especially smartphones, has become a daily necessity[2]. The bad impact that results from the use of this technology is the misuse in committing crimes[3]. The progress of the information media cannot be separated from irresponsible people who use social media to spread false information (hoax), especially in the current situation where the issue of covid-19 is rampant.

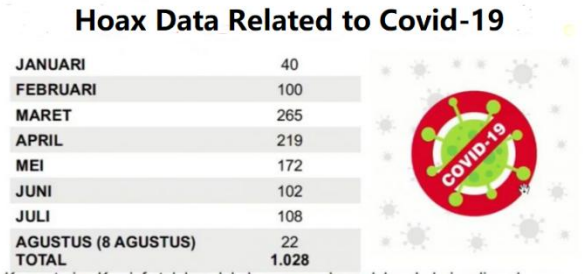

Figure 1. Data on the Spread of Hoaxeson Social Media

Figure 1,is a hoax data related to covid-19 from January to August 2020, the Ministry of Communication and Information (Kominfo) obtained 1028 cases of hoaxes rife on various social media platforms linked to the disinformation of the corona virus (COVID19). From this data, knowledge of Mobile forensics is needed which will later be needed to investigate evidence of cases of spreading false information or hoaxes, because hoaxes are spread on social media which are usually accessed via smartphones.Due to a large number of cases the spread of this fake news or hoax through social media that can be accessed by the public via their smartphone then Mobile knowledge is needed Forensic to investigate evidence of hoax spreaders[4].The disclosure of this evidence uses the National Institute of Justice method with 5 stages, namely identification, collection, examination, analysis, and report.

1.1 Study Literature

1.1.1 Previous Study

This study refers to five previous studies conducted as a comparison with the current research with the previous one. The first research entitled "Analysis of Digital Evidence for Facebook Messenger Applications on, android Smartphones Using the NIJ Method". The results obtained in this study in the form of the contents of Facebook Messenger conversations were obtained in the form of accounts, chats, and images related to the simulation of drug vape liquid trafficking cases[5].

The second research entitled "Forensic Analysis of, Android-based Instant Messaging Applications". This study uses forensic measures that have proven successful to extract conversational artifacts from an android-based WA application even though the chat archive has been deleted from the device[6].

The third research entitled "Acquisition of Digital Evidence on, Android-based Instagram Messenger Using the National Institute of Justice (NIJ) Method". The results of this research are in accordance with what is desired, namely digital evidence in the form of pictures/photos, and conversations/chats from Instagram social media installed on the smartphone[7].

The fourth research entitled "Forensic Analysis of Recovery on, android Smartphones Using the National Institute of Justice (NIJ) Method". The test results of the forensic tool used by the researcher showed that the forensic tool MOBILedit could not recover the deleted data, Wondersharedr. dr. fone for, android has successfully recovered deleted contact data, call logs, and messages. while the Belkasoft Evidence Center tool can only restore contact data ,and call logs that have been deleted[1].

The fifth research entitled "Mobile Forensics on LinkedIn Social Media Services". This research has other results found in the investigation are 17 WiFi passwords, 117 download histories, 263 phone calls, 1 deleted file, 1 hidden file, and 1 displayed file, the research has achieved the expected target[8].

1.1.2 Digital Forensics

Digital Forensics is the application of science,and computer technology in pro-justice[9]. In this case, it is to scientifically demonstrate high-tech crimes or computer crimes to obtain digital evidence that can be used to fight criminals[7]. Digital forensics is the act of obtaining, retrieving, preserving, and presenting data following forensic methods, and tools[10]. Digital forensics has many branches, one of which is mobile forensics[11]. Digital forensics is the process of obtaining digital evidence that can be stored on temporary computer storage, permanent storage, USB, CD, Network Crossing, etc[12].

1.1.3 Mobile Forensics

Mobile forensics is a branch of digital forensics concerned with the recovery of digital evidence or data from mobile devices under sound forensic conditions. A mobile device is usually the phrase referring to a cell phone, but it can also be associated with a digital device that has internal memory and communication capabilities[13]. Mobile device forensics is forensics where data is taken from mobile phones, which by itself can be used as evidence. This evidence can be used as a basis when investigating a case by law enforcement agencies[14]. A mobile device can be associated with a digital device that has internal memory, and communication capabilities, or commonly called a smartphone. Much of the information is retrieved from mobile devices used for crimes and is useful in a variety of administrative, legal, and investigative matters[15].

1.1.4 Digital Evidence

Digital evidence is information stored or transmitted in binary form that can be relied upon in Courts. Especially for digital evidence related to mobile such as smartphones, it can be found in call history, phonebooks, SMS,and MMS, Photo, Audio, Video, and others.[7]. Digital evidence is data sent or stored using a mobile device or computer that denies or supports a particular crime, or provides clues that point to important elements related to a violation[15]. Digital evidence is fragile, volatile,and vulnerable if not handled properly. Any kind of alteration that contains digital evidence will lead to wrong conclusions, or the evidence will be useless[13]. Digital evidence in mobile devices is prone to be overwritten by new data or even being deleted[16].

1.1.5 Hate Speech

Hate speech is speech, behavior, writing, or performance that is prohibited because it can trigger acts of violence,and commotion in social life[17]. Hate speech is an act that harms other people and can be said to be a crime because it has understood the meaning,and elements of a criminal act[18].

1.1.6 Hoax

Hoax is information that is engineered to cover up actual information, in other words, hoax is defined as an attempt to distort facts using information that is convincing but cannot be verified, it can also be interpreted as an act of obscuring the actual information, by flooding the media with the wrong message to cover up the correct information[19]. Fake news or known as a hoax or also called hate speed itself is untrue information or fake news that has no certainty and is deliberately disseminated to create situations and circumstances in the community into panic or anxiety[20].

1.1.7 Social media

Instagram is a combination of the words Instant-Telegram. From the use of the word, it can be interpreted as an application to send information quickly, namely in the form of photos in the form of managing photos, editing photos ,and sharing (Share) to other social networks. This application is one of the most widely used applications in Indonesia[21]. Twitter is one of the social media that is widely used by its users. Crimes such as fraud, insults, hate speech,and other crimes have recently been using social media applications, especially Twitter[3].

1.1.8 Smartphones andandroid

Android smartphone itself is a hybrid device that can work as a cellphone, and can also work almost like a computer but in a simpler portable form[22],andandroid is one of the most widely used operating systems on smartphones today[23]. Android is an open-source operating system released by Google under the Apache license. The open-source nature of the Android operating system allows this operating system to be freely modified and distributed by smartphone developers, wireless operators, and application developers[24].

1.1.9 Forensic Tools

Mobile forensics is a relatively new field in the digital forensics area, so the software and tools that can be used to retrieve data from mobile phones are still relatively new. The extraction tool can be hardware or software, depending on how the data was extracted from the mobile device. There are many extraction tools available in the market today, and some new tools bring some innovative ideas. Most of the existing tools are commercial tools, some are open source tools. However, the procurement of these tools is quite difficult to obtain due to privacy and security issues and the costs involved[25].

2. METHODOLOGY

2.1 Research Scenario

In this scenario, the perpetrators have installed Instagram and Twitter applications on their smartphones. Then the perpetrator used the two social media to spread false news about covid-19, and a few hours later the post was deleted

because a user saw the post,and reported it to the authorities.Then an investigation will be carried out by the authorities to handle the case of spreading the hoax.

Figure 2. Evidance Research Scenario

Figure 2,is a simulation of the case of uploading fake news on social media Instagram, and Twitter, where the perpetrator posted information about COVID-19 in the form of an image on the Instagram application, and in the form of a tweet (text) on the Twitter application.

This study uses a Xiaomi MI 4 smartphone that has been rooted to make it easier for investigators to access data from smartphones. Then the investigator analyzed the smartphone using forensic tools such as MOBILedit forensic express, Magnet Axiom, and Autopsy. The smartphone is first carried out by the imaging process so that there are no changes to the data, and maintain data security.

2.2 Research Stage

This study adopts the investigation process of the NIJ forensic analysis method. This method is used to describe how the description of the research process that is being carried out so that the stages of this research can be known more systematically so that it can be used as a reference for further research[26].

Figure 3. Stages National Institute of Justice method

Figure 3,is a stage in the National Institute of Justice method which is one of the methods in digital forensics where the forensic process will be carried out sequentially starting from identification, collection, examination, analysis, and finally reporting.

2.2.1 Identification

The identification stage is an activity that assists the investigation stage in the context of taking digital criminal evidence by selecting digital criminal evidence and sorting the data. At this stage, the researcher succeeded in collecting evidence, and tools that would later be used in the process of finding evidence.After the evidence is collected, the researcher will identify what tools and tools will be used to search for evidence from the case being studied.

Table 1. Research Tools ,and Materials

No	ToolsandMaterials	Information
1	Laptop	Acer Aspire A315-41 with AMD Ryzen 5 2500U with
2	Smartphone	Xiamo MI4 is already rooted
3	USB Cable	To connect a laptop with a smartphone
4	MOBILedit Forensic Express	Forensic tools
5	Magnet Axiom	Forensic tools
6	Autopsy	Forensic tools
7	*Instagram*	Social media apps
8	*twitter*	Social media apps

Table 1,Is a description of the tools, and materials that will be used in research or forensic processes, the tools,and materials are divided into two, namely tools, and materials used to carry out the investigation process such as MOBILedit software, Magnet Xxiom, Autopsy used to process materials into digital evidence, following forensic procedures.

2.2.2 Collection

The collection stage or the stage of collecting a series of data collection activities that assist the investigation process to find evidence of digital crimes.

Figure 4. Smartphones as Evidencefor the case of the spread of hoaxes

Figure 4,is evidence in the form of a smartphone that is used to spread information about the covid-19 hoax in which the Instagram and Twitter applications have been installed and this is the electronic evidence obtained. then later the smartphone will be rooted to gain access to the smartphone where later the data on the smartphone will be analyzed.

2.2.3 Examine

The examination stage is the stage for testing the search for evidence on the Instagram,and Twitter applications using three tools, namely MOILEdit Forensic Express, Magnet Axiom, and Autopsy.

2.2.3.1 MOBILedit Forensic

The first test uses the MOBILedit Forensic Express tool where the smartphone will be connected to a laptop using a data cable or using a wifi device, after connecting to the MOBILedit tools, data extraction will then be carried out to obtain evidence or you can also use these tools to create imaging files.

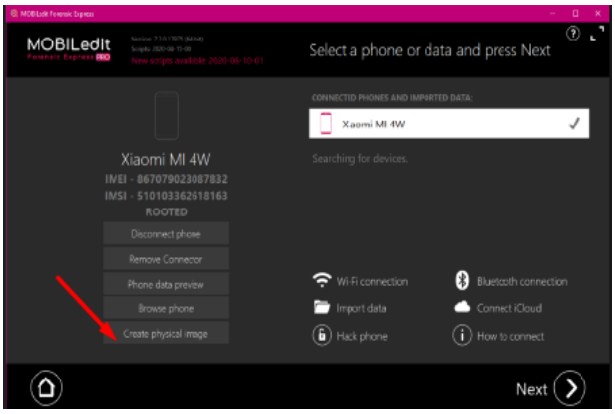

Figure 5. Smartphone Display Connected with MOBILedit Tools Tools

Figure 5, This is the smartphone display after connecting to the MOBILedit tool, after the smartphone is connected to the tools, a physical image file will then be created so that data changes do not occur. Then the file will be extracted to look for items in the form of posts or tweets containing hoax elements which will later be used as evidence.

2.2.3.2 Magnets Axiom

The second test uses the magnet axiom tool, this tool is not much different from the forensic MOBILedit tool where the smartphone will be connected to the magnet axiom tools process for. Once connected, data extraction will be carried out on the Instagram and Twitter applications to look for evidence that is suspected to be false information.

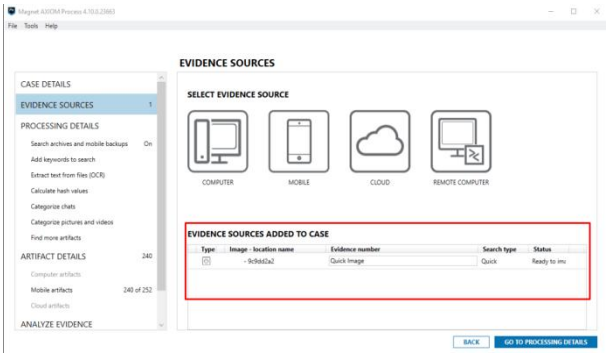

Figure 6. Smartphone Connected with Magnet Axiom Process Tools

Figure 6, This is a display on the evidence source menu where a smartphone will be detected that will be connected to the tools, in this menu we will choose what evidence to use, whether using a smartphone or using an imaging file that has been created. After that, the analysis process will be carried out to search for the desired evidence.

2.2.3.3 Autopsy

The third test uses Autopsy tools, these tools are quite different from the previous two tools, namely MOBILedit forensics,and Magnet Axiom. Because this tool simply utilizes the image file that has been created, and then the file analysis process will be carried out to find evidence.

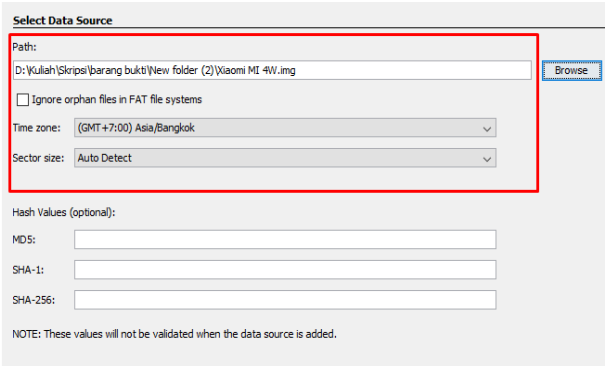

Figure 7. Display Selecting Image File

Figure 7, is a display where the data source selection process will be carried out where the image file will be used for the acquisition process, then researchers can choose the time zone used for the investigation time.

2.2.4 Analysis

The analysis stage is the stage where the researcher checks the results of the examination stages in detail to obtain evidence.The results of the analysis obtained are then made a comparison table of each software to obtain the recommended software combination for solving a digital crime case on certain devices and applications.

2.2.4.1 MOBILeditForensic Analysis

The MOBILedit tool obtains evidence in the form of post information uploaded by the perpetratorand deleted tweets. Not only that, using this tool you can get other evidence such as accounts, ids, messages, pictures, videos, audio,and documents.

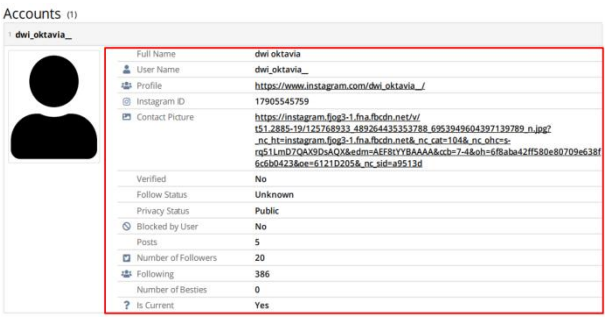

Figure 8. Information Account Instagram use Mobiledit

Figure 8, is the information obtained by the researcher from the Instagram account, where the researcher gets the name, username, id, profile, number of followers, number of followers, number of posts, and others. This is important information and can be used as evidence.

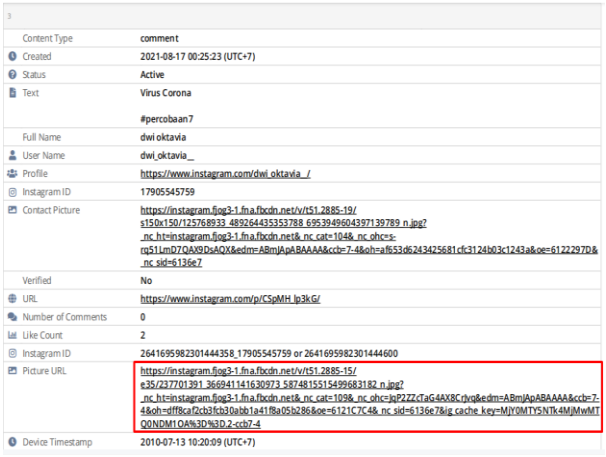

Figure 9. Display of Deleted Hoax Post Information on the Instagram Application

Figure 9,This is the information on the hoax post that has been deleted, the post obtained a lot of important information that can be used as evidence, such as the date of creation/upload, caption, username, id, number of likes, and picture URL.and when you click on the URL on the picture URL it will display the image of the deleted post.

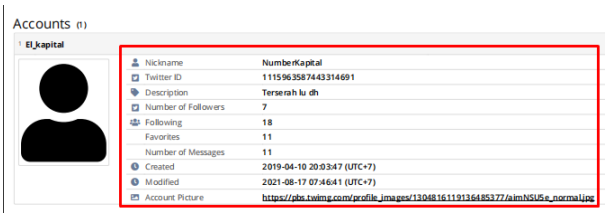

Figure 10. Information Account Twitter use Mobiledit

Figure 10, is the information obtained on the twitter account, the researcher managed to get a username, nickname, id, account description, number of followers, number of followers, profile photo.

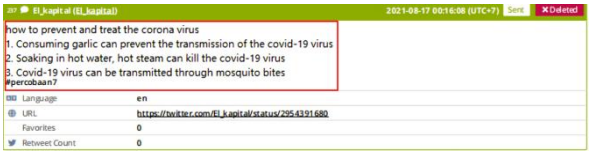

Figure 11. Display of Deleted Tweets

Figure 11,Is a tweet that has been deleted on the Twitter application. In the post, there is information about how to treat and prevent the coronavirus which is false or hoax information.

2.2.4.2 Magnet Axiom Analysis

The second analysis stage uses the magnet axiom examine tools. In the previous stage were using the magnetic axiom process was for data extraction was, then used the magnetic axiom examine to analyze the data from the extraction process was. Unlike the forensic MOBILedit tool, using this tool you can get accounts, messages, pictures of posts that have been deleted on the Instagram application, and do not find deleted tweets on the Twitter application.

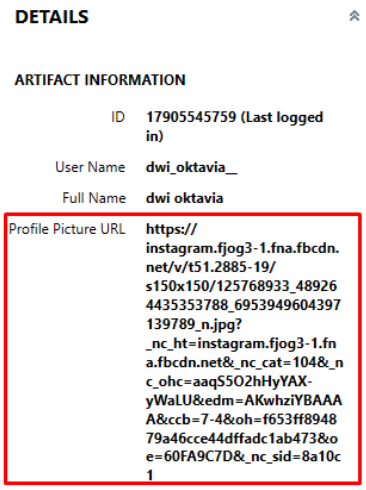

Figure 12. Information Account Instagram use Magnet Axiom

Figure 12, is the information obtained on the Instagram account, the researcher managed to get an id, username, full name, and profile photo.

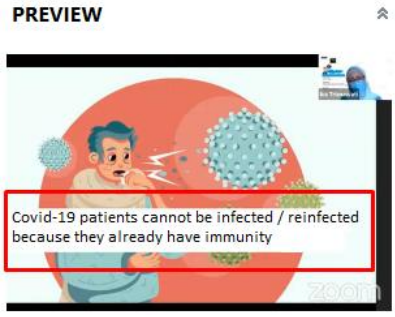

Figure 13. Display of Hoax Posts to 1

Figure 13, This is one of the hoax posts that was uploaded and then deleted by the perpetrator on the Instagram application, where the image contains incorrect information about COVID-19.

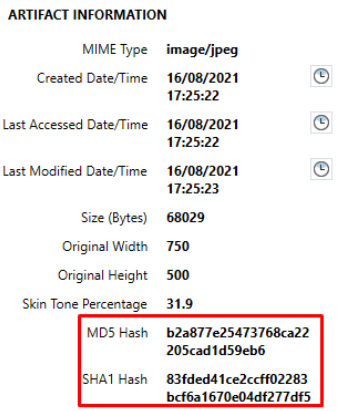

Figure 14. *Hoax Post Information Display*

Figure 14,This is the information displayed in Figure 10. It contains information such as file type, date, size, md5, and SHA1 in the image file.

2.2.4.3 Autopsy Analysis

The third analysis uses autopsy tools, in these tools researchers get evidence in the form of pictures, videos, audio, and dokument.

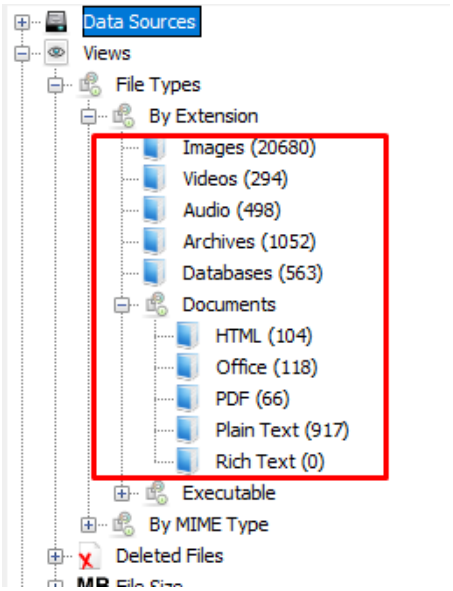

Figure 15. Data Extraction Results from Image File

Figure 15, is the result of data extraction on imaging files, where researchers get data or files such as images, videos, documents, audio, databases,and others that can be used as digital evidence to uncover cases of spreading false information related to the coronavirus.

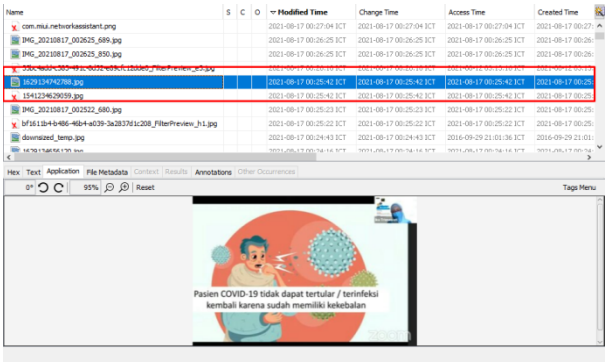

Figure 16. Hoax Image Information

Figure 16, is a display of information obtained on a hoax image that has been deleted, where there is information on where the image is stored, file type, date, size, and md5. where the information is sufficient to be used as digital evidence in cases of spreading fake news related to the corona virus or covid-19.

2.2.5 Report

Reporting in this study includes a summary of the smartphone used, and the forensic procedures carried out as well as a comparison of the forensic tools used.The reporting stage is reporting the results of the analysis which includes a description of the actions taken[27]. After the comparison will be made the percentage of success of these tools

Table 2. Comparison of Three Forensic Tools on Instagram

Tools / Data	MOBILedit Forensic	Magnet Axiom	Autopsy
Instagram account	1	1	0
Instagram ID	1	1	0
Profile Photo	1	1	0
Post	5	0	0
Post delete	2	0	0
Message	35	398	2797
Picture	848	572	20680
Audio	2	0	294
Videos	42	0	498
Document	79	0	1205

Table 2, is a comparison of the results of 3 forensic tools for searching digital evidence on the Instagram application. Evidence obtained using the MOBILedit tool includes account, id, profile photo, number of posts, number of deleted posts, picture messages, audio, video, and documents. then the axiom magnet tool obtained evidence in the form of accounts, ids, profile photos, messages, pictures. while the autopsy tools get picture, audio, video, and document messages.

Table 3. Comparison of Three Forensic Tools on Twitter

Tools / Data	MOBILedit Forensic	Magnet Axiom	Autopsy
Twitter account	1	1	0
Twitter ID	1	1	0
Profile Photo	1	1	0
Tweet	383	226	0
Tweet deleted	157	0	0
Message	128	6	2797
Picture	110	0	20680
Audio	0	0	294
Videos	0	0	498
Document	4	0	1205

Table 3,is a comparison of the results of 3 forensic tools for searching digital evidence on the twitter application. Evidence obtained using the MOBILedit tool includes account, id, profile photo, number of posts, number of deleted posts, picture messages, and documents. then the axiom magnet tool obtained evidence in the form of accounts, ids, profile photos, tweet, messages. while the autopsy tools get picture, audio, video, and document messages.

3. CONCLUSION

Test results using the National Institute of Justice method succeeded in obtaining evidence in cases of spreading COVID-19 news or false information (hoaxes). The acquisition process uses three forensic tools, namely MOBILedit Forensic Express, Magnet Axiom, and Autopsy. the results of the acquisition on the Instagram application

usingThe forensics MOBILedit tool managed to find 10 of the total 10 pieces of evidence to be obtained with a 100% success rate, including hoax posts and tweets that had been deleted on the Instagram and Twitter applications. not only that, but the researcher also got accounts, ID, messages, pictures, audio, videos, and documents, whilethe results of the acquisition on the Instagram application using the Magnet axion tools found 5 out of a total of 10 pieces of evidence that were wanted with a presentation of 50% and an autopsy found 5 out of a total of 10 pieces of evidence with a presentation of 50 %. the results of the acquisition on the Twitter application usingusingThe forensics MOBILedit tool managed to find of the total 10 pieces of evidence to be obtained with a 66.6% success rate, including hoax posts and tweets that had been deleted on the Instagram and Twitter applications. not only that, but the researcher also got accounts, ID, messages, pictures, audio and documents. and for the acquisition results on the Twitter application in magnet axiom and autopsy tools, the results are the same as those on Instagram with 50% gain for magnet axiom and 50% for autopsy.The Magnet Axiom and Autopsy tools did not find deleted posts but found pictures of deleted posts and other evidence.when doing forensics after the evidence or post is deleted. Suggestions for further research are to look for evidence of cases of spreading hoaxes or other crimes on social media Facebook, TikTok, and others using oxygen tools, belkasoft, and using other forensic methods to uncover crime cases.

4. REFERENCES

[1] I. Riadi, S. Sunardi, and S. Sahiruddin, "Forensic Analysis of Recovery on Android Smartphones Using the National Institute Of Justice (NIJ) Method," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, p. 87, 2019, doi: 10.30872/jurti.v3i1.2292.

[2] M. S. Hartawan, A. Damuri, and A. S. Putra, "Data Processing To Find Evidence On Mobile Forensics," 2020.

[3] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Comparative Analysis of Forensic Tools on Twitter Applications Using the Digital Forensics Research Workshop Method," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 829–836, 2020.

[4] R. Rahmansyah, "Comparison of Investigation Results of Digital Evidence on Facebook and Instagram Applications With the Nist . Method," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 49–57, 2021, doi: 10.14421/csecurity.2021.4.1.2421.

[5] I. Anshori, K. E. Setya Putri, and U. Ghoni, "Analysis of Digital Evidence for Facebook Messenger Applications on Android Smartphones Using the NIJ Method," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 118–134, 2020, doi: 10.25299/itjrd.2021.vol5(2).4664.

[6] G. M. Zamroni, R. Umar, and I. Riadi, "AForensic Analysis Android Based Instant Messaging Application," vol. 2, no. 1. pp. 102–105, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id.

[7] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "1490-Article Text-2859-1-10-20190413," Digital Evidence Acquisition on Android-Based Instagram Messenger Using the National Institute Of Justice (NIJ) Method, vol. 4. pp. 219–227, 2018.

[8] I. Riadi, A. Yudhana, and M. Al Barra, "Mobile Forensics on LinkedIn Social Media Services," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 6, no. 1, pp. 9–20, 2021, doi: 10.14421/jiska.2021.61-02.

[9] I. Riadi, A. Fadlil, and M. I. Aulia, "Review of the Optical Drive Forensic Process Using the National Institute of Justice (NIJ) Method," *J. Tek. Inform. dan Sist. Inf.*, vol. 8, no. 3, pp. 107–118, 2019.

[10] I. Riadi, R. Umar, and I. M. Nasrulloh, "Digital Forensic Analysis on Frozen Solid State Drive With National Institute of Justice (Nij) Method," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[11] M. R. Setyawan, A. Yudhana, and A. Fadlil, "Identification of Skype Digital Evidence On Android Smartphones With the National Institute Of Justice (NIJ) Method," *Semnastek*, pp. 565–570, 2019.

[12] A.- Ahmadi, "Google Drive Forensic Data Acquisition On Android With The National Institute of Justice (NIJ) Method," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 4, no. 1, p. 8, 2018, doi: 10.24014/coreit.v4i1.5803.

[13] A. Yudhana, I. Riadi, and I. Anshori, "Facebook Messenger Digital Evidence Analysis Using the Nist . Method," *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[14] S. Madiyanto, H. Mubarok, and N. Widiyasono, "Mobile Forensics Investigation Mobile Forensics Investigation Process on IOS Based Smartphone," *J. Rekayasa Sist. Ind.*, vol. 4, no. 01, 2017, doi: 10.25124/jrsi.v4i01.149.

[15] R. Umar and Sahiruddin, "Nist Method For Forensic Analysis Of Digital Evidence On Android Devices," *Pros. SENDU_U_2019*, pp. 978–979, 2019.

[16] N. Anwar and I. Riadi, "WhatsApp Messenger Smartphone Forensic Investigation Analysis Against Web-Based WhatsApp," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, vol. 3, no. 1. p. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.

[17] S. Hendrawati, "Criminal responsibility for the crime of hate speech through social media," *J. Res Justitia J. Ilmu Huk.*, vol. 1, pp. 246–255, 2021.

[18] I. M. Kardiyasa, A. A. S. L. Dewi, and N. M. S. Karma, "Criminal Sanctions Against Hate Speech," *J. Analog. Huk.*, vol. 2, no. 1, pp. 78–82, 2020, doi: 10.22225/ah.2.1.1627.78-82.

[19] H. Septanto, "The Effect of Hoax and Hate Speech A Cyber Crime with Simple Technology in People's Social Life," *J. Sains dan Teknol.*, vol. 5, no. 2, pp. 157–162, 2018.

[20] J. E. Latupeirissa, J. D. Pasalbessy, E. Z. Leasa, and C. Tuhumury, "Dissemination of Fake News (HOAX) During the Covid-19 Pandemic and its Countermeasures in Maluku Province," *J. Belo*, vol. 6, no. 2, pp. 179–194, 2021, doi: 10.30598/belovol6issue2page179-194.

[21] I. Riadi, A. Yudhana, and M. C. F. Putra, "Instagram Messenger Digital Evidence Recovery Analysis Using the National Institute of Standards and Technology (NIST) Method," *Semin. Nas. Teknol. Inf. dan Komun. - Semant.*, pp. 161–166, 2017.

[22] N. Nasirudin, S. Sunardi, and I. Riadi, "Android Smartphone Forensic Analysis Using the NIST Method

and the MOBILedit Forensic Express Tool," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.

[23] N. Anggraini *et al.*, "Forensic Analysis of Whatsapp Messenger on Android Smartphone," vol. XII, no. 1, pp. 83–100, 2020.

[24] M. S. Asyaky, "Digital Evidence Analysis and Comparison of Instant Messenger Applications On Android," *J. Penelit. Tek. Inform.*, vol. Vol. 3 No, no. 1, pp. 220–231, 2019.

[25] I. Z. Yadi and Y. N. Kunang, "National Conference on Computer Science (KONIK) 2014 Forensic Analysis on Android Platform," *Konf. Nas. Ilmu Komput.*, p. 142, 2014, [Online]. Available: http://eprints.binadarma.ac.id/2191/.

[26] M. A. Aziz, I. Riadi, and R. Umar, "WEB-Based Line Messenger Forensic Analysis Using National Institute of Justice (NIJ) Framework," *Seminar Nasional Informatika 2018 (semnasIF 2018)*, vol. 2018, no. November. pp. 51–57, 2018.

[27] R. Adijisman and I. Riadi, "Mobile Forensic on WhatsAppServices using National Institute of Standards and Technology Method," vol. 183, no. 29, pp. 41–48, 2021.