HASIL CEK_1707048001

By Ahwan Ahmadi

WORD COUNT	3460	TIME SUBMITTED	22-JAN-2019 07:58AM
		PAPER ID	43737391

Scientific Journal of Informatics
Vol. 6, No. 1, May 2019
p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method

Anton Yudhana[1], Rusydi Umar[2], Ahwan Ahmadi[3]

[1] Department of Electrical Engineering, Universitas Ahmad Dahlan, Indonesia
[2] Department of Informatics Engineering, Universitas Ahmad Dahlan, Indonesia
[3] Department of Informatics, Universitas Ahmad Dahlan, Indonesia
Email: [1]eyudhana@ee.uad.ac.id, [2]rusydi_umar@rocketmail.com, [3]ahwanahmadi71@gmail.com

Abstract

The use of cloud storage media is very popular nowadays, especially with the Google Drive cloud storage media on smartphones. The increasing number of users of google drive storage media does not rule out the possibility of being used as a medium for storing illegal data, such as places to store negative content and so on. On a smartphone with an Android operating system that has a Google Drive application installed, digital evidence can be extracted by acquiring and analyzing the system files. This study implemented a mobile forensic method based on guidelines issued by the National Institute of Standards of Technology (NIST). The results of this study are presented in the form of data recovery in the deleted Google Drive storage media, which results in the form of headers of the data type in the form of deleting account names, deleted file types, and timestamp of deleted files. Digital evidence obtained with 59 Axiom Magnet software found in the Entry227 file, with 46 files, if the percentage is a success rate of 77%.

Keywords: Google Drive, NIST, Forensics, Mobile

1. INTRODUCTION

The use of storage media is currently very developed because more and more data is circulating and the inability of a storage medium or storage to store data, then a cloud storage storage media is created. This technology has significant potential to reduce costs and efficiency in storage (Armbrust, Fox, Griffith, Joseph, & RH, 2009). Cloud storage is one of the remote data storage techniques that are interconnected with personal computers when connected to the internet (Easwaramoorthy, Thamburasa, Samy, Bhushan, & Aravind, 2016). Storing data online using cloud storage service media is one solution for storing data (Mager, Biersack, & Michiardi, 2012), (Faheem, Le-Khac, & Kechadi, 2017).

Storage media applications offered by smartphones such as practicing bring and are supported by physical and cloud storage media (Riadi, Umar, & Firdonsyah, 2018). Cloud storage services can offer greater storage flexibility and availability, with almost unlimited storage space, as well as the ability to synchronize data between multiple devices (Mulazzani, Schrittwieser, Weippl, Leithner, & Huber, 2011), (Martini & Choo, 2013). The benefits of using cloud storage services are interesting, but security and privacy concerns are a major concern in cloud services (Subashini & Kavitha, 2011). The use of cloud storage media is increasing, it does

not rule out the possibility of abuse of cloud storage storage media as an illegal data storage medium. Illegal data, such as videos, immoral images, pirated applications, fake documents. Illegal data that has been deleted on cloud storage can be used as digital evidence of cases of violations of the ITE Law. Digital evidence is expected to be another alternative to uncover a digital crime (Yudhana, Riadi, & Anshori, 2018), (anwar & Riadi, 2017), (Putra, Fadlil, & Riadi, 2017). In uncovering cases of digital crime, computer science and technology are needed for the analysis and examination of digital evidence known as digital forensics (Riadi & Umar, n.d.), (Umar, Yudhana, & Faiz, 2016).

Digital evidence can be used as a law enforcement tool in handling digital cases obtained from cloud storage media on smartphones (Riadi & Umar, 2017). Digital forensics allows an analysis to recover a fact or event that is hidden in nature (Fadlil, Riadi, Aji, & Dahlan, 2017). Digital forensics has two models, traditional forensic and live forensic. This study applies traditional forensic methods on Google Drive on an Android smartphone. In Figure 1 shows the review rating of several types of cloud storage, storage, Google drive was ranked second with 1,044,187 reviews, and the position of the most review was Dropbox uploaded by en.softonic.com in 2016.

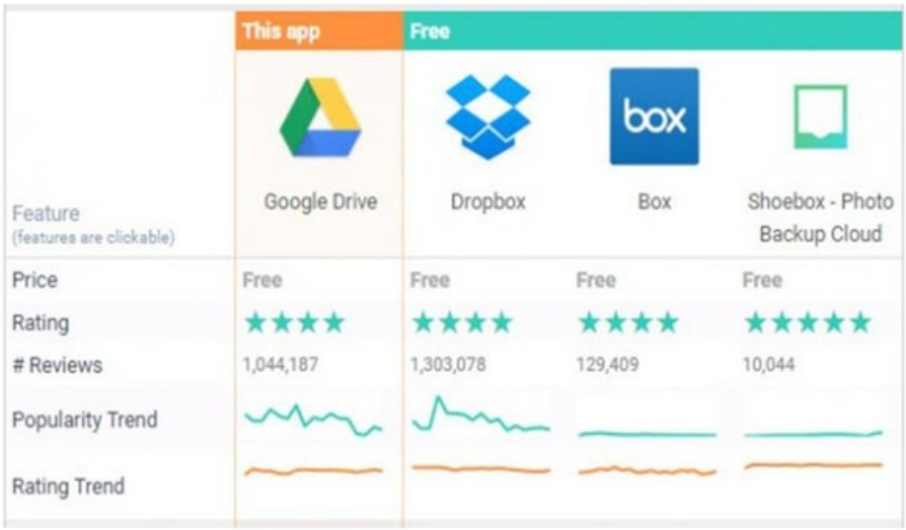

Figure 1 Cloud storage media user data

The services provided by users get 15GB of free storage space, including word processing, spreadsheet applications, and presentations, even program files with exe extensions. The 15GB of storage space must be shared with a Gmail account, photos uploaded to Google+, and every document created on Google Drive (Juliandi, 2014). Google's view of the android application can be seen in Figure 2.

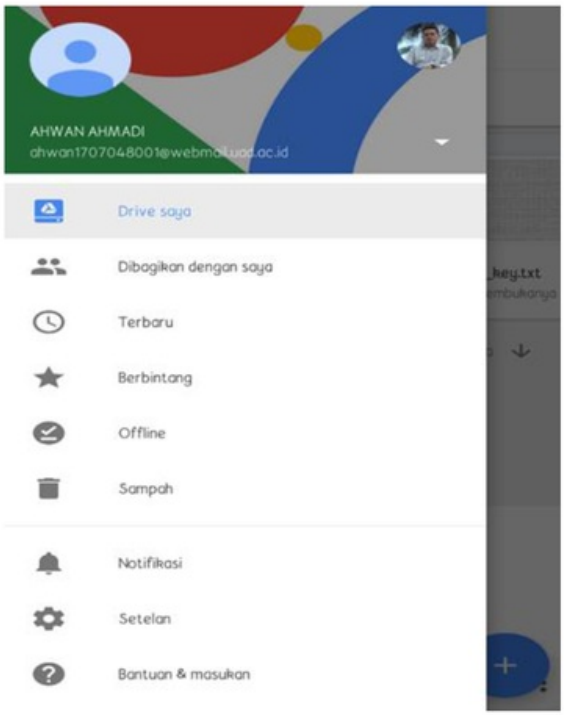

Figure 2 Display Google Drive on an Android Smartphone

2. METHODS

Digital forensic aims to analyze and reconstruct an event related to a computer or digital artifact (Forensics, 2009). Digital forensic methods and processes have been developed by forensic investigators and practitioners (Faiz, Prabowo, & Sidiq, 2018). This study applies a method for the National Institute of Standards and Technology (NIST) which is a forensic method for analyzing digital evidence on a smartphone media (Kent, Chevalier, Grance, & Dang, 2006). The flow of the NIST method as shown in Figure 3.

Figure 3: The NIST method for mobile forensic stages

The flow must be done in a mobile forensic process, these stages include:

1. Collection/Preservation

This stage is also called the preservation stage. This stage is the process of collecting, identifying, labeling, recording, and retrieving evidence in the form of

hardware which data will be taken to be used as digital evidence of a digital crime case. This process is carried out by following data integrity safeguard procedures. Data integrity can be maintained by isolating physical evidence and making backups in the form of cloning or image files from physical evidence. Figure 4 shows the flow of the Collection stage.

Figure 4 Collection process

2. Examination

Processing data collected digitally forensics using a combination of various scenarios, both automatically and manually, as well as assessing and issuing data according to needs while maintaining data integrity. Figure 5 describes the stages of the Examination process.

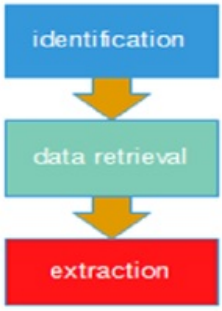

Figure 5 Examination process

3. Analysis

The process of analysis is carried on the results of the examination with methods that have been justified technically and legally to obtain useful information and answer questions that are a reference or as a driver in conducting

collection and examination. Figure 6 describes the flow of the analysis phase. Figure 6 describes the stages of the Analysis process.

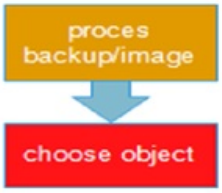

Figure 6 Process analysis

4. Reporting

The final result of an analysis process is a report. Reports from an analysis can be in the form of written reports needed as reports for documentation or oral reports in the form of presentations. The reporting process is explained in a groove like Figure 7.

Figure 7 Reporting Process

2. 1 Research tools and materials

There are 2 types of tools used in this study, namely tools in the form of hardware and software devices. The hardware used in this study is in the form of one smartphone device that is used as a test material, a computer as a workstation for forensic analysis and a USB Connector as a connecting medium between smartphone and workstation devices.

Table 1. Hardware requirements

No	Device name	Specification	Description
1	Notebook	AMD A10-9600P RADEON R5 HP, Windows 10 64 Bit.	Workstation
2	Smartphone	Samsung Galaxy V Plus, OS Android 4.4 KitKat	Hardware (test material)
3	USB Connector	-	Media is connecting smartphone with workstations

Table 2. Software requirements

Number	Device name	Description
1	MOBILedit Forensic Express	Forensic tool for imaging
2	Magnet Axiom	Forensic tool for image file analysis
3	Forensic Connector	Media is connecting forensics tool
4	Google Drive Smartphone Android	Object of research

3. RESULT AND DISCUSSION

This research is an effort in analyzing evidence by applying the mobile forensic method on an Android smartphone by utilizing a forensic tool that will be tested for its performance, on a smartphone also already installed a google drive application. To analyze the evidence, a crime scenario is created in which a smartphone user saves a drug photo that will be circulated. The photo is saved on the smartphone Google drive. From the example of this scenario, it is assumed that the smartphone has been secured by the officer. Then the Investigation Team followed up on the smartphone found by making a copy of the system from the device so that the authenticity was maintained, and analyzed the evidence contained in the google drive application.

3.1 Collection/Preservation

The preservation stage is the first stage to secure evidence found by investigators or investigators. In this case, the investigator collected evidence from the owner, the evidence obtained in the form of 1 cellphone Samsung Galaxy V Plus with specifications OS, Android 4.4 KitKat, 6GB RAM, and inside it installed the Google Drive application. To avoid changing data on the smartphone the isolation process is needed by activating the Airplane mode feature. This feature is enabled to stop all data connectivity that can change the data integrity in the smartphone. Retrieval of evidence is shown in Figure 5.

Figure 5 Collecting evidence

This process is carried out with the aim of maintaining data integrity. Data integrity safeguards are carried out by physical evidence isolation techniques and data backup by cloning technique or image files from the smartphone physical evidence. Figure 6 describes the collection process of evidence by using the MOBILedit FORENSIC EXPRESS tool.

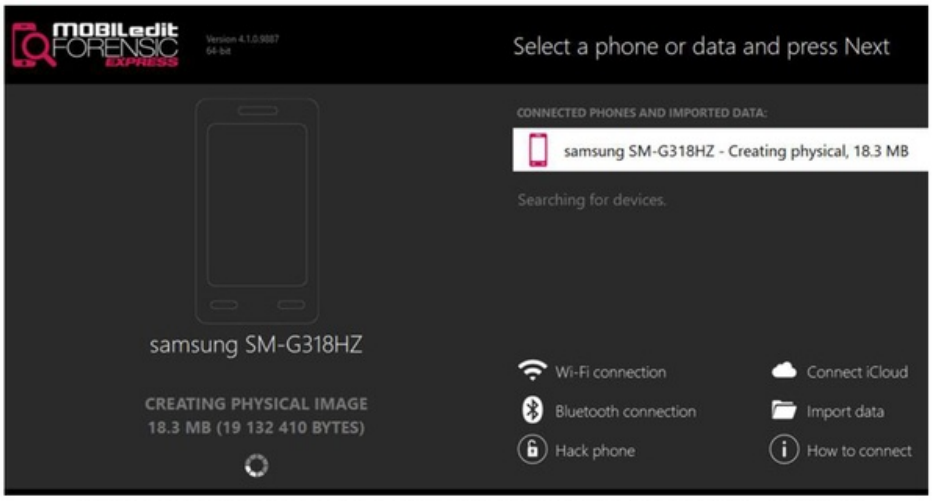

Figure 6 image processing using MOBILedit FORENSIC EXPRESS

Examination of the google drive application that has been installed on the smartphone is done by acquiring data when the smartphone is on. To obtain digital evidence that you want to identify in the outlined case scenario, which is contained in the google drive application. The application used in this study is Magnet Axiom, which is one of the forensic tools that can be implemented for smartphones supported by data cables as a link between smartphones and Forensic Magnet

software and then acquisitions. The Axiom magnet when extracting data from physical evidence when the smartphone is connected to the internet network is shown in Figure 6.

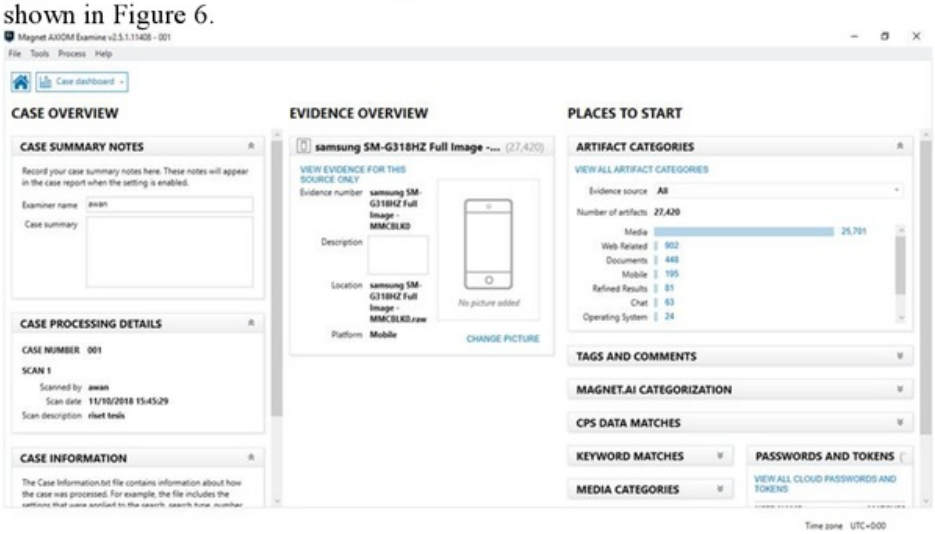

Figure 6 smartphone data extraction process from physical evidence

3.2 Examination

The next stage is the process of retrieving data from the results of the MOBILedit FORENSIC EXPRESS image tool, then the image file data is extracted with the Axiom Magnet tool. Figure 7 is the image processor extension file.

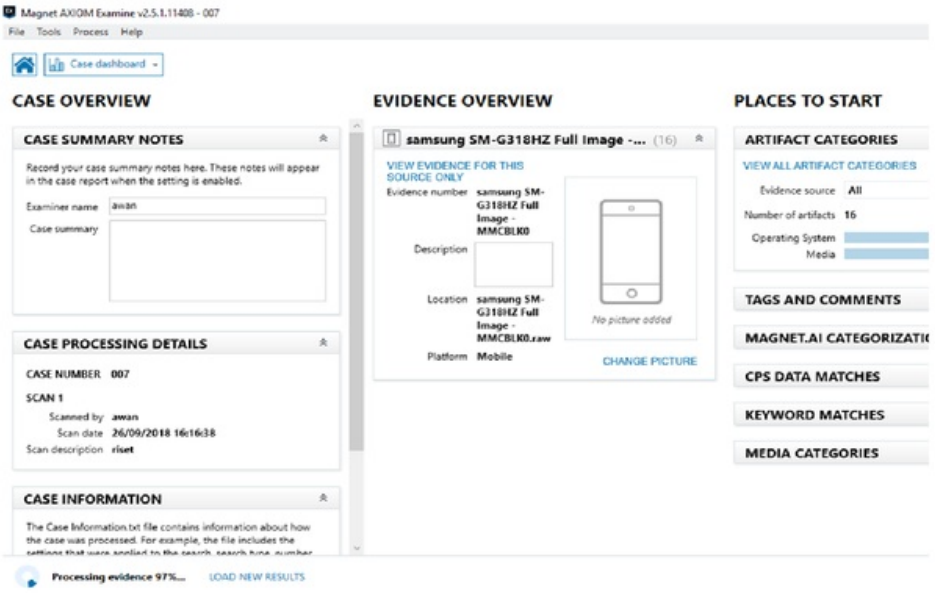

Figure 7 image file extraction process

After carrying out the extraction process, the inspection of the location of the evidence was located. Based on the results of the examination of the extraction results obtained 24 file partitions, where one of the partition files contained the location of the google drive file sought. The location of the partition and google drive data are shown in figure 8.

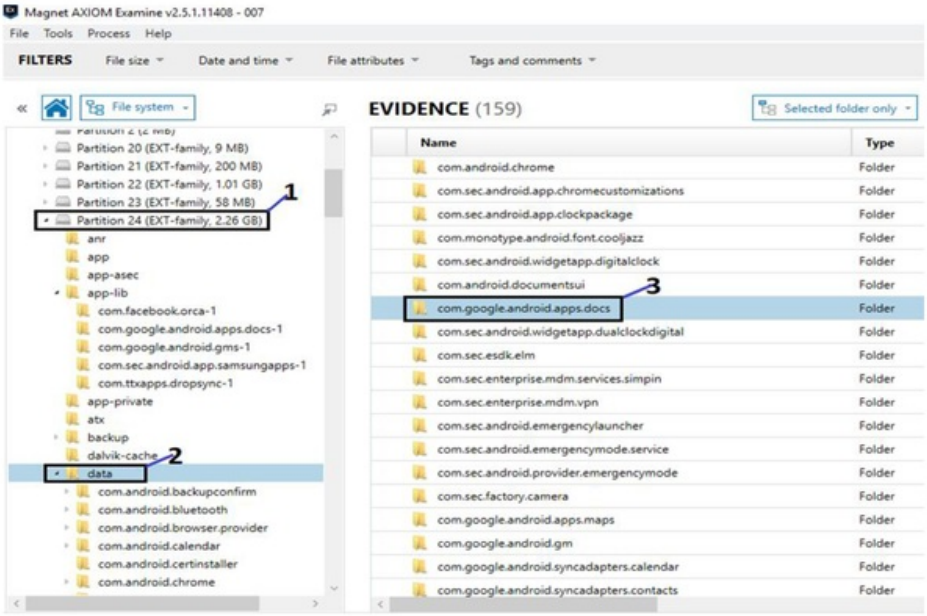

Figure 8 location of the google drive data partition

Information from the partition location and google drive data is explained in table 3.

Table 3 detailed information about the location of the google drive data partition

No	Information
1	Shows the number of system partitions on the smartphone
2	Shows file system data in partition 24 (EXT-Family)
3	Shows the location of the google drive folder from data partition 24 (EXT-Family)

3.3 Analysis

The Google drive system is in the can. google. android. apps. docs folder in the file that allows the data the investigation team is looking for. Figure 9 shows the locations indicated for evidence.

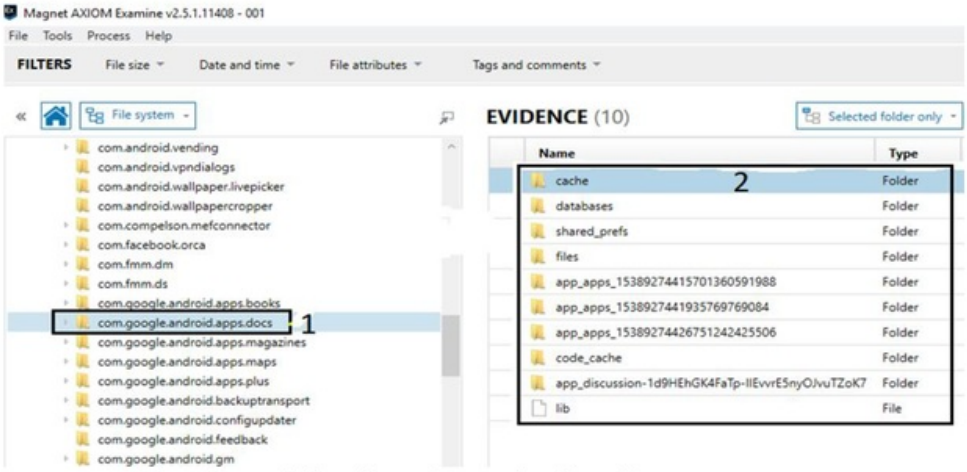

Figure 9 data from the google drive file system

The google drive file system can be explained in table 4

Table 4 description of figure 9.

No	Information
1	Location of the Google Drive data system
2	Fill in the data on the Google Drive system folder

From the process of analyzing Partition 24 system files (EXT-Family, 2.26 GB) that refers to the com. google. android. apps. docs folder, there is a database system, where the database contains information about what files are on Google actor's drive. Indication of evidence is shown in figure 10.

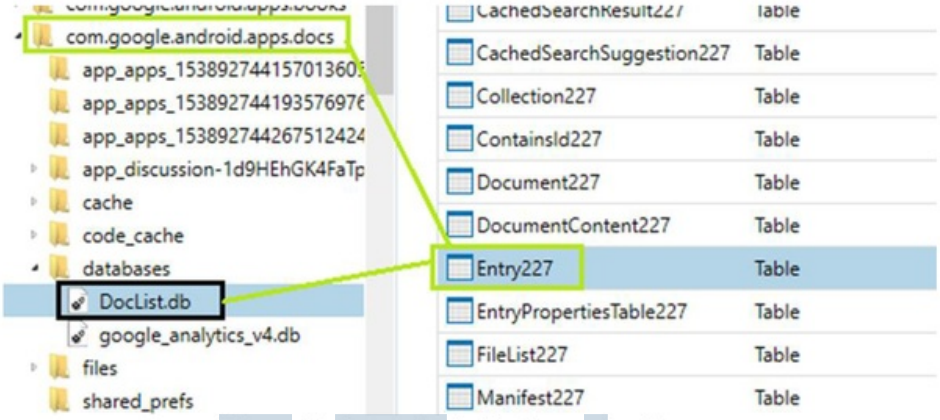

Figure 10 shows the indications of evidence

Table 5 shows the analysis of the Partition 24 system files (EXT-Family, 2.26 GB).

Table 5 description of figure 10.

No	Name	Information
1	Com.google.android.apps.docs	Location of Google Drive data
2	DocList.db	Google Drive data base system
3	Entry2227	Location of all types of files on Google Drive

The process analysis of the Entry227 data is shown in Figure 11 by analyzing erased data.

Entry227

Entry_id	title	owner	ownerPictureUrl	creationTime	lastModifiedTime	lastModifierAccountName	lastOpenedTime
59	heroin.jpg	ahwanahmadi71@gmail.com	https://lh6.googleus...	1539103369317	1539103369317	A Ahwan Ahmadi	1540105745667

recencyTime		modifiedByMeTime	mimeType	trashed
15401057456...	0	1539103369317	image/jpeg	3

Figure 11 results of data analysis are deleted

Table 6 shows the results of the data analysis deleted from the google drive application which is in the Entry 227 data.

Table 6 description of picture 11

No	Nama	Keterangan
1	Entry_id	Number of files on Google Drive
2	Title	file name
3	Owner	File owner
4	OwnerPictureUrl	Image of owner from Url
5	creationTime	When the file was created
6	lastModifiedTime	The last time was modified the file
7	lastModifierAccountName	The last account name that changed the file
8	lastOpennedTime	The last time the file was opened
9	recencyTime	The time period for opening the file
10	modifiedByMeTime	When the file is changed
11	mimeType	File type
12	trashed	Deleted

3.4 Reporting

At this stage the results of digital evidence that has been acquired and has undergone an analysis process carried out by the investigation team are then reported as the results of the findings of the analysis process. Table of process results Analysis of the Axiom Magnet tool is shown in table 7.

Table 7 Results of analysis of the Axiom Magnet tool

No	Type File	Number of File types	Deleted type of file type
1	Image	8	✓
2	Video	3	✓
3	Zip	2	
4	Rar	4	
5	PDF	20	
6	Docx	4	✓
7	Pptx	2	
8	Aplication	1	✓
9	Data Base	2	

The stages that have been carried out in the sample case scenario can also be applied in other cybercrime cases. Complexity in finding and obtaining digital evidence for cybercrime cases using smartphone media such as those mentioned in the report mentioned by RSA in 2013The stages that have been carried out in the sample case scenario can also be applied in other cybercrime cases. Complexity in finding and obtaining digital evidence for cybercrime cases using smartphone media such as those mentioned in the report mentioned by RSA in 2013(EMC, 2014). the availability of forensic tools is also very supportive to overcome the complexity that may be faced by digital investigation teams in dealing with digital crime. This research is at least a reference in conducting further studies with the latest cases such as social media and cloud storage media on smartphones.

4. CONCLUSION

The results of the analysis and discussion that have been made and explained in this study, there are a number of things that can be concluded including: the NIST method in digital forensic processes can be applied to cloud storage media case studies using the help of Axiom Magnet software. From the data obtained with the Axiom Magnet software, 59 files were found in the Entry227 file, with 46 files, 8 image files, video 3, zip 2, rar 4, pdf, 20, docx 4, pptx 2, Application 1, Database 2 and 15 files are only folder names that do not have data. Based on the scenario made by the investigator to find the image file sought, it is in the image type file where of the 8 image files found 2 of them have been deleted, including the files searched for, 3 video files deleted there are 2 files, application files also deleted

and files docs whose number 4 is found 1 deleted file that is known to be based on its trashed value. From the results of testing with the Magnet Axiom software the file was found, but the researcher could not open the file, the researcher could only find out the file name and type. From the description of the results of the above research, the researchers also suggested the further development by using more detailed and complete forensic methods and trying out mobile forensic tools that could be used to find evidence on cloud storage media. The use of methods and supported by other forensic tools will provide more satisfying results by staying referral to mobile forensic standards and with more in-depth analysis also included with more complete report results..

5. REFERENCES

[1] Anwar, nuril, & Riadi, I. (2017). Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web. Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika, 3(1), 1–10. Retrieved from http://journal.uad.ac.id/index.php/JITEKI/article/view/6643/3530

[2] Armbrust, M., Fox, A., Griffith, R., Joseph, A., & RH. (2009). Above the clouds: A Berkeley view of cloud computing. University of California, Berkeley, Tech. Rep. UCB, 07–013. https://doi.org/10.1145/1721654.1721672

[3] Easwaramoorthy, S., Thamburasa, S., Samy, G., Bhushan, S. B., & Aravind, K. (2016). Digital Forensic Evidence Collection of Cloud Storage Data for Investigation.

[4] EMC. (2014). The Current Trend in Cybercrime 2014 - An Inside Look at the Changing Threat Landscape (pp. 1–9). Retrieved from http://www.emc.com/collateral/white-paper/rsa-cyber-crime-report-0414.pdf

[5] Fadlil, A., Riadi, I., Aji, S., & Dahlan, U. A. (2017). Pengembangan sistem pengaman jaringan komputer berdasarkan analisis forensik jaringan. Jurnal Ilmu Teknik Elektro Komputer Dan Informatika (JITEKI), 3(1), 11.

[6] Faheem, M., Le-Khac, N. A., & Kechadi, T. (2017). Toward a new mobile cloud forensic framework. 2016 6th International Conference on Innovative Computing Technology, INTECH 2016, (November), 736–742. https://doi.org/10.1109/INTECH.2016.7845142

[7] Faiz, M. N., Prabowo, W. A., & Sidiq, M. F. (2018). Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal. Journal of Informatics, Information System, Software Engineering and Applications (INISTA), 1(1), 63–70. https://doi.org/10.20895/INISTA.V1I1

[8] Forensics, D. (2009). Hashing and Data Fingerprinting in Digital Forensics, (April), 49–55.

[9] Juliandi, A. (2014). Personal Storage, 0–14. https://doi.org/10.5281/zenodo.1067932

[10] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. https://doi.org/10.6028/NIST.SP.800-86

[11] Mager, T., Biersack, E., & Michiardi, P. (2012). A measurement study of the Wuala on-line storage service. 2012 IEEE 12th International Conference on

Peer-to-Peer Computing, P2P 2012, 237–248. https://doi.org/10.1109/P2P.2012.6335804
[12] Martini, B., & Choo, K. K. R. (2013). Cloud storage forensics: OwnCloud as a case study. Digital Investigation, 10(4), 287–299. https://doi.org/10.1016/j.diin.2013.08.005
[13] Mulazzani, M., Schrittwieser, S., Weippl, E., Leithner, M., & Huber, M. (2011). Dark Clouds on the Horizon : Using Cloud Storage as Attack Vector and Online Slack Space. USENIX Security, 8, 11. Retrieved from http://research.securityresearch.at/wp-content/uploads/publications/dropboxUSENIX2011.pdf
[14] Putra, R. A., Fadlil, A., & Riadi, I. (2017). Forensik Mobile Pada Smartwach Berbasis Android. Jurti.
[15] Riadi, I., & Umar, R. (n.d.). Analisis Forensik Serangan Sql Injection Menggunakan Metode Statis Forensik. In Prosiding Interdisciplinary Postgraduate Student Conference 1st Program Pascasarjana Universitas Muhammadiyah Yogyakarta (PPs UMY) (pp. 102–103).
[16] Riadi, I., & Umar, R. (2017). Identification Of Digital Evidence On Android ' s. International Journal of Computer Science and Information Security, 15(5), 3–8.
[17] 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 (IJECE), 8(5), 3991–4003. https://doi.org/10.11591/ijece.v8i5.pp3991-4003
[18] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11. https://doi.org/10.1016/j.jnca.2010.07.006
[19] Umar, R., Yudhana, A., & Faiz, M. N. (2016). Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory pada Sistem Proprietary. In Prosiding Konferensi Nasional Ke- 4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM) (pp. 207–211).
[20] Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. IT JOURNAL RESEARCH AND DEVELOPMENT, 3(1), 13–21.

HASIL CEK_1707048001

ORIGINALITY REPORT

9%

SIMILARITY INDEX

PRIMARY SOURCES

1	docplayer.info Internet	94 words — 3%
2	George Grispos, William Bradley Glisson, Tim Storer. "Recovering residual forensic data from smartphone interactions with cloud storage providers", Elsevier BV, 2015 Crossref	43 words — 2%
3	www.researchgate.net Internet	28 words — 1%
4	T Setiadi, A Tarmuji, B Suhendra, F Noviyanto, S L Khasbullah. "Planting time determination for food crops using decision tree", IOP Conference Series: Materials Science and Engineering, 2018 Crossref	15 words — 1%
5	telsoc.org Internet	11 words — < 1%
6	journal.unnes.ac.id Internet	9 words — < 1%
7	unsri.portalgaruda.org Internet	8 words — < 1%
8	Lecture Notes in Computer Science, 2010. Crossref	8 words — < 1%
9	www.sans.org Internet	8 words — < 1%
10	Sunardi, S A Akbar, F Noviyanto, E Wibowo, R Naufal. "Irigation distribution automatization based on scheduling system", IOP Conference Series: Materials	8 words — < 1%

Science and Engineering, 2018
Crossref

11 Mark Pollitt. "The key to forensic success: examination planning is a key determinant of efficient and effective digital forensics", Elsevier BV, 2016 — 8 words — < 1%
Crossref

12 Tutut Herawan. "Soft Set Theoretic Approach for Discovering Attributes Dependency in Information Systems", Lecture Notes in Computer Science, 2010 — 8 words — < 1%
Crossref

13 D Napitupulu, R Rahim, D Abdullah, MI Setiawan, LA Abdillah, AS Ahmar, J Simarmata, R Hidayat, H Nurdiyanto, A Pranolo. "Analysis of Student Satisfaction Toward Quality of Service Facility", Journal of Physics: Conference Series, 2018 — 7 words — < 1%
Crossref

EXCLUDE QUOTES ON
EXCLUDE BIBLIOGRAPHY ON
EXCLUDE MATCHES OFF