International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(4): 292-297
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-0011

Forensic Analysis in Cloud Storage with Live Forensics in Windows (Adrive Case Study)

Tri Rochmadi and Dadang Heksaputra
Department of Information System, Universitas Alma Ata, Yogyakarta, Indonesia
Street Brawijaya 99, Yogyakarta 55183
trirochmadi@almaata.ac.id, dadang@almaata.ac.id

ABSTRACT

Digital era such as now, cloud technology can not be released in our lives. Cloud computing has also become one of the fastest-growing and transformative technologies. In addition to some convenience and comfort in using the cloud, it turns out to cause new problems, namely cybercrime. Cybercrime will be increasingly diverse and allow criminals to innovate with the cloud. Cloud forensics remains an obstacle and challenge for investigators because each cloud provider has a different architecture so different investigations are needed in conducting cloud forensics. In this research, forensic cloud storage research was carried out from ADrive services. Some ADrive features that make it possible for cybercriminals are data can be synchronized with a client application, encrypted and given a password on a file that is on the cloud. This research applies the NIST framework in the investigation process and from the results of the analysis of digital evidence can be detected and found on 3 digital evidence namely RAM, logical drive and Google Chrome Database. Of the three pieces of evidence, the most potential as digital evidence is in RAM and logical drives because of the digital evidence found files uploaded to adrive.

KEYWORDS

digital forensics, cloud forensics, cloud storage applications forensics, live forensics, memory forensics.

1 INTRODUCTION

Internet of things technology currently dominates in human life, this is evident from the many devices between one device and another connected to the internet [1]. Examples of the many uses of the internet of things are smart home, smart village, smart city and so on which all of these examples cannot be separated from cloud computing.

Cloud computing has become one of the fastest-growing and transformative technologies [2], according to its type there are four types of cloud computing namely infrastructure as a service, platform as a service, software as a service and storage as a service. Of the four types of cloud computing services, the main reason for using cloud computing, including cloud storage, is because of its convenience and can be accessed anywhere, anytime [3] besides that according to Shariati also saves the budget if using infrastructure on a large scale [4].

However, from the advantages of using cloud computing, there are still many risks in the case of cybercrime [5], for example when the cloud used by the Sony PlayStation Network suffers from paralysis due to hacker attacks [6] or another example of cloud storage is used as a medium for sharing illegal files or a means in planning major cases such as the exploitation of children, selling drugs or even terrorism.

Based on these problems, cloud forensics is a challenge for an investigator because it is still a hot topic and a variety of architectures developed by vendors either managed by companies or personally in making cloud computing.

2 LITERATUR REVIEW

This research focuses on cloud types of services on the storage side. Research forensic digital analysts on cloud storage already exist with various cloud storage objects and operating systems both desktop and smartphone computers.

In 2015 study by Martini that proposed a step to remotely collect digital evidence in the case of vCloud objects [7]. According to Daryabar in 2016, in his research with OneDrive, Box, GoogleDrive and Dropbox objects on Android 4 and iOS 7 smartphones, he found digital evidence on the smartphone's internal memory,

including its IP, timestamp, and history [8]. Teing research in 2018 exploring CloudMe on the Ubuntu 14 and Mac OS X operating systems focuses on the analysis side of a database, web and log file [9].

2.1 Digital Forensics

Digital forensics is part of the application of computer science and technology to examine and analyze electronic evidence and digital evidence to see the relationship between one evidence and another so that cybercrime can be investigated and accounted for [10].

2.2 Live Forensics

Live forensics is the development of traditional forensics that is done when the system is still alive [11]. The purpose of live forensics is to do forensics on memory, swap files, network, and running system processes to get more detailed information.

2.3 Cloud Forensics

Cloud computing is a new technology that provides services over the network so that it can be accessed everywhere, convenient and scalable as needed [12]. Cloud computing according to the National Institute of Standards and Technology (NIST) is divided into 3 namely cloud with software, platforms, and infrastructure as a service. But because there are many cloud services as storage then it is also called STaaS / Storage as a Service [13].
In his research [12], Hemdan said cloud forensics is digital forensics that is done in a cloud environment. In particular, cloud forensics is related to the internet of things because it is virtual, remote, networked, client-server and also related to big data because it is inseparable from the interconnected data and the process of sending data between clients to the server.

3 METHODOLOGY

The methodology in this study can be seen in Figure 1. A literature review is a technique to collect reviews from relevant research both from books, reports, and papers.

Figure 1. The Methodology

From the developing literature and identified the needs are as follows:

1. Windows
2. FTK Imager
3. Autopsy
4. SQLite Browser
5. Adrive Application
6. Web Browser

4 EXPERIMENT SETUP

The study is carried out with a case simulation from an experiment or case scenario determined to help the research. This research uses a cloud from Adrive that is installed to the device which is initialized as a victim. Victims upload documents through synchronization of the adrive client installed on the device, which then logs into the web adrive to get a link that can be shared. Then the victim deletes the uploaded document file and uninstalls the adrive application installed on the device, this scenario can be seen in Figure 2.

Figure 2. Case Scenario

5 FRAMEWORK INVESTIGATION

This research refers to the investigation process used by the National Institute of Standards and Technology (NIST). This investigation process can be seen in Figure 3.

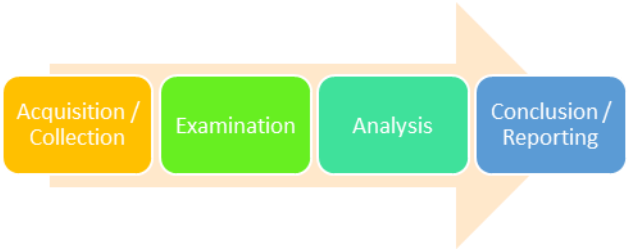

Figure 3. Investigation Process

- Acquisitions: Acquisition of devices from the target laptop by taking data directly into RAM, Storage and Database Browser. This step done when the laptop is still alive called the Live Forensic Technique to get more information at the time of analysis later.
- Examination: Examination of acquired digital evidence including duplication of digital evidence following applicable operational standards.
- Analysis: Analyze the results of the examination of each forensic tool according to the justified technical method.
- Conclusion: Classify the ability of each forensic tool to produce a forensic investigation report that will be used in litigation.

6 RESULTS AND DISCUSSION

The examination and analysis process begins with the acquisition process first as the NIST method presented earlier and adopting the NIST method is the forensic investigation stage as shown in Figure 4.

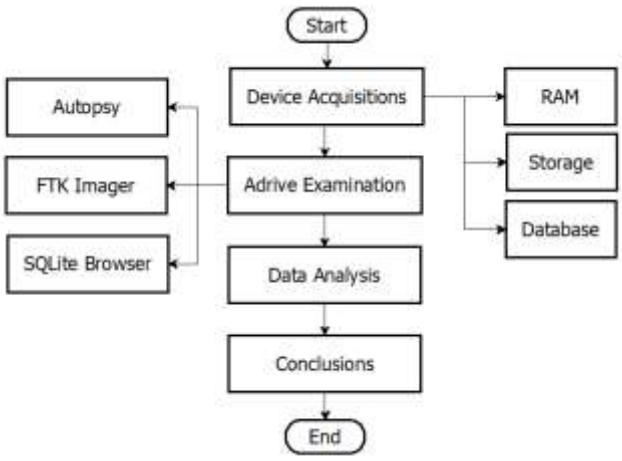

Figure 4. Forensic Investigation Stage

The above stages use the tools as in table 1.

Table 1. Tool Investigation

Tool	Function
FTK Imager 3.1.1.8	Acquisition of digital files from RAM memory and digital files from the Drive Adrive installation location on the suspect's computer.
Autopsy 4.11.0	Tool for analyzing image files from the acquisition of digital evidence of RAM and Storage.
SQLite Browser 3.11.2	Tool for analyzing digital files that are possible can be digital proof from the google chrome database used.

From the acquisition process obtained digital evidence with the extension .mem, .ad1 which is the result of the acquisition of RAM, while for the acquisition of the logical drive extension. Digital evidence from the google chrome database is stored in the directory C:\Users\%USERNAME%\AppData\Local\ Google\Chrome\User Data\Default\databases so the acquisition is done traditionally.

6.1 RAM Analysis

From RAM analysis using the Autopsy 4.11.0 tool, it was detected that the suspect installed the Adrive application located in the C: \\ Program Files \ Adrive directory as shown in Figure 5.

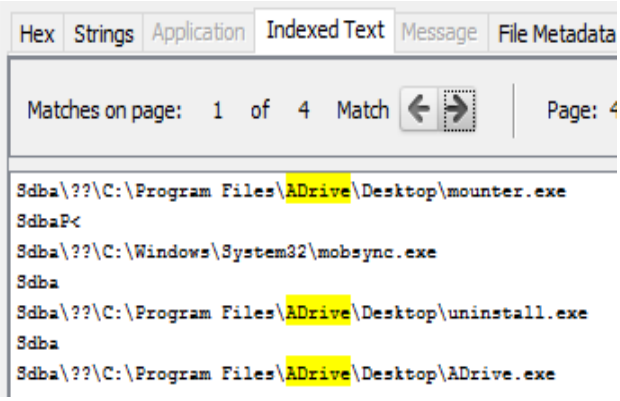

Figure 5. Adrive Application Located

Detection results are then analyzed and found a document file with the extension .doc with the link on http://www31.adrive.com/filemanager/ downloadfile/326830777/LAPORAN_PERTANGGUNGJAWABAN_PENERIMAAN_DA.doct as in Figure 6.

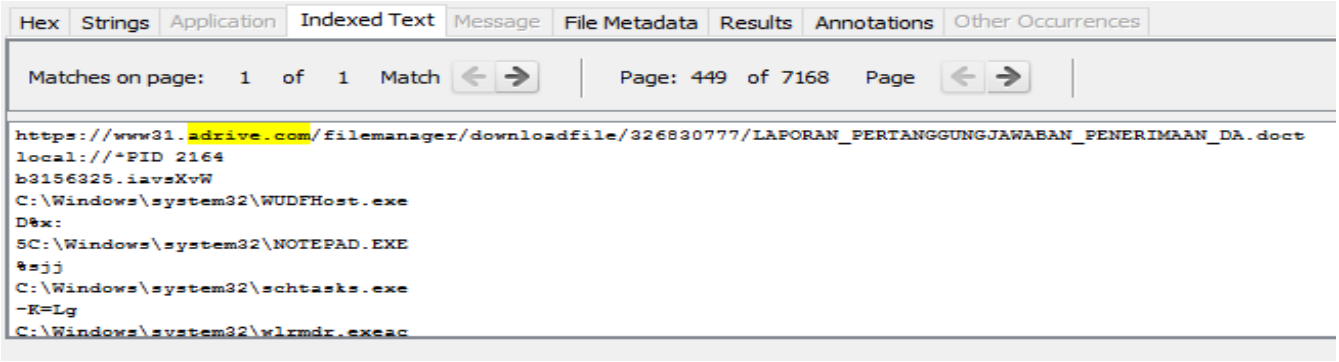

Figure 6. Link Detection Results from RAM

6.2 Analysis of Windows Logical System

Logical analysis using the Autopsy 4.11.0 tool on the evidence of the acquisition file ie admit.001 shows the same as RAM analysis that can detect the installation of the Adrive application in the Program Files - Adrive directory as shown, where the default Program Files folder is the folder which is in the System directory on the Windows operating system as in Figure 7.

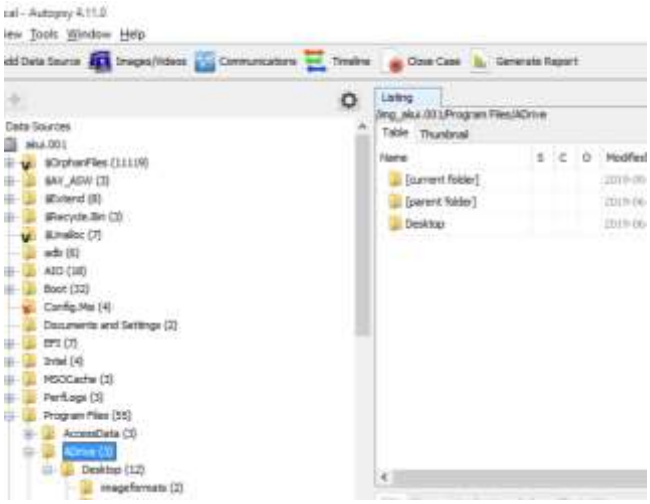

Figure 7. Detection Application Adrive on Directory

The next analysis results also found a document file with the file name LAPORAN_PERTANGGUNGJAWABAN_PENERIMAAN_DA.doc as in Figure 8.
From this file we can know the timestamp that the file is accessed on 27-06-2019 10:02:39, the modified file at the time 27-06-2019 10:02:41, file changes occur on 27-06-2019 11:07:00 and the file was first created on 27-06-2019 10:02:39 as in Figure 9.

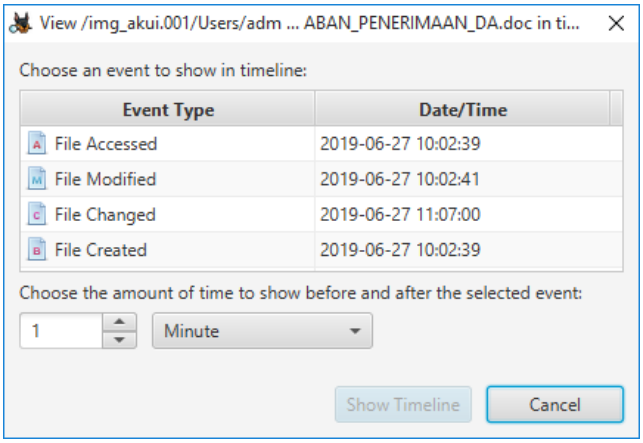

Figure 9. Timestamp

6.3 Google Chrome Database Analysis

In the analysis of the Google Chrome database, the acquisition is done traditionally by copying the source database file for the Google Chrome software stored in C: \ Users \ <username> \ AppData \ Local \ Google \ Chrome \ User Data \ Default \ Databases. From this analysis, only a link to adrive.com was obtained.

This research succeeded in getting digital evidence related to the use of cloud storage from Adrive in the form of detection applications that are installed on the client in this case on the computer. Other evidence is also able to find a link that is used to share with friends so that digital evidence can be found in the form of uploaded document files and shared via adrive as shown in table 2. This research can be the first step to deal with similar crime cases in Adrive and other cloud storage by implementing forensic tools that support to obtain higher quality digital evidence.

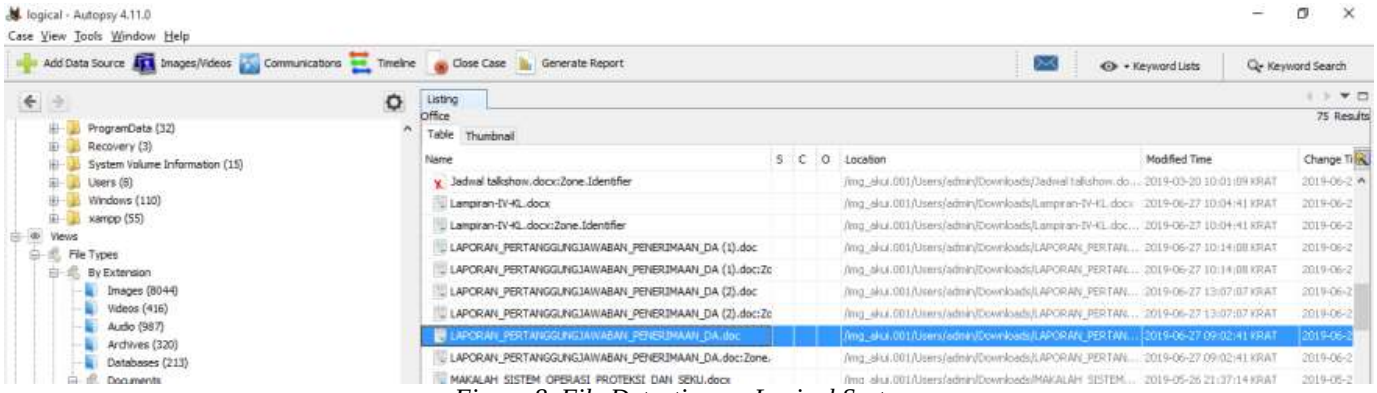

Figure 8. File Detection on Logical System

Table 2. Digital Evidence Analysis

	RAM	Logical	DB Chrome
Application Detection	√	√	
Link Detection	√	√	√
File Recovery	√	√	

7 CONCLUSION AND FUTURE WORK

Based on the analysis of digital evidence, the most potent evidence found when analyzing RAM and Storage is being able to find the distributed link and also an account to login to the adrive.com cloud.

The results of the analysis are able and sufficient to represent valid evidence because the link used was active when it was found and is a document file used by the suspect.

Future research can incorporate data mining in the analysis process because the use of cloud that will impact the impact of data in a larger amount and varied or commonly referred to as big data. The use of other digital forensic methods is also a consideration to obtain quality and accurate digital evidence so that it can assist in the criminal process.

REFERENCES

[1] R. Rizal, I. Riadi, and Y. Prayudi, "Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 7, no. 4, pp. 382–390, 2018.

[2] A. Alenezi, R. K. Hussein, R. J. Walters, and G. B. Wills, "A Framework for Cloud Forensic Readiness in Organizations," *Proceedings - 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2017*, pp. 199–204, 2017.

[3] Yee Say Keat, B. B. Rad, and M. Ahmadi, "Cloud Computing Security and Forensics Issues and Awareness of Cloud Storage Users in Malaysia," *International Journal of Cyber-Security and Digital Forensics*, vol. 6, no. 1, pp. 1–13, 2017.

[4] M. Shariati, A. Dehghantanha, and K. K. R. Choo, "SugarSync forensic analysis," *Australian Journal of Forensic Sciences*, vol. 48, no. 1, pp. 95–117, 2016.

[5] A. Naser, M. F. Zolkipli, S. Anwar, and M. S. Al-Hawawreh, "Present status and challenges in cloud monitoring framework: A survey," *Proceedings - 2016 European Intelligence and Security Informatics Conference, EISIC 2016*, p. 201, 2017.

[6] J. Galante, O. Kharif, and P. Alpeyev, "Sony Network Breach Shows Amazon Cloud's Appeal for Hackers," *Bloomberg*, 2011. .

[7] B. Martini and K. K. R. Choo, "Remote programmatic vCloud forensics: A six-step collection process and a proof of concept," *Proceedings - 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014*, pp. 935–942, 2015.

[8] F. Daryabar, A. Dehghantanha, B. Eterovic-Soric, and K. K. R. Choo, "Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices," *Australian Journal of Forensic Sciences*, vol. 48, no. 6, pp. 615–642, 2016.

[9] Y. Y. Teing, A. Dehghantanha, and K. K. R. Choo, "CloudMe forensics: A case of big data forensic investigation," *Concurrency Computation* , vol. 30, no. 5, pp. 1–12, 2018.

[10] M. N. Al-Azhar, *Digital Forensic: A Practical Guide of Computer-based Investigation*. Salemba Infotek, 2012.

[11] T. Rochmadi, I. Riadi, and Y. Prayudi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," *International Journal of Computer Applications*, Apr. 2017.

[12] E. E. D. Hemdan and D. H. Manjaiah, "A cloud forensic strategy for investigation of cybercrime," *Proceedings of IEEE International Conference on Emerging Technological Trends in Computing, Communications and Electrical Engineering,*

ICETT 2016, 2017.

[13] S. H. Mohtasebi, A. Dehghantanha, and K. K. R. Choo, *Cloud Storage Forensics: Analysis of Data Remnants on SpiderOak, JustCloud, and pCloud*. 2016.