LONTAR KOMPUTER VOL. 10, NO. 3 DECEMBER 2019 **p-ISSN 2088-1541**
DOI : 10.24843/LKJITI.2019.v10.i03.p06 **e-ISSN 2541-5832**
Accredited B by RISTEKDIKTI Decree No. 51/E/KPT/2017

Forensic Investigation Framework on Server Side of Private Cloud Computing

Didik Sudyana[a1], Nora Lizarti[a2], Erlin[a3]

[a]Department of Informatics Engineering, STMIK Amik Riau
Jl. Purwodadi Indah Km 10 Tampan, Indonesia
[1] didik.sudyana@stmik-amik-riau.ac.id
[2] noralizarti@stmik-amik-riau.ac.id
[3] erlin@stmik-amik-riau.ac.id

Abstract

Cloud Computing is one of the technologies that continue to develop and progress in rapid adoption rates due to the various benefits and conveniences offered. Cloud Computing has four types of adoption models, one of which is a Private model and is widely adopted by users because it is safer and customizable. The high level of cloud computing adoption is an opportunity for criminals to use cloud computing in committing their crimes and requires handling digital forensics. However, each cloud model has different characteristics, so the investigative method used is also different. Then there is no specific guidance for investigating cloud computing. So it is necessary to analyse the investigation of private cloud computing that used OwnCloud from the server-side and develop the novel investigation framework based on SNI 27037: 2014. An analysis of investigations is performed to develop the novel investigation framework and to find out what evidence can be found based on the novel framework. The results of the research conducted can be a reference for investigators to conduct forensic investigations in cloud computing on the server-side and the novel investigation framework will become a reference to be used as a guide to the investigation on private cloud computing in the server-side.

Keywords: *Cloud Computing, Investigation Framework, SNI 27037:2014*

1. Introduction

Cloud Computing is now a technology that continues to develop, and many users have adopted it. Some of the benefits of Cloud Computing are flexibility, cost reduction and scalability [1]. There are four types of Cloud Computing adoption models currently available, namely Private, Public, Community, and Hybrid. Also, there are three types of Cloud Computing service models, namely Software as a Services (SaaS), Infrastructure As a Service (IaaS) and Platform as a Service (PaaS) [2]. Based on a survey conducted by [3], 70% of respondents used the Private Cloud Computing model. Private Cloud Computing is a type of cloud adoption model whose infrastructure is built independently by an organization or company for the company's internal needs [4]. Moreover, from the three types of services, Software As a Services (SaaS) is a service that has revenue of 85.1 billion US dollars [5].

The higher level of Cloud Computing adoption has caused cybercriminals to begin improvising by using cloud computing as a tool or an intermediary for the crime [6]. When this crime occurred, digital forensics was needed to resolve this case and find digital evidence that could be used in court. [7] said that digital forensics is the use of knowledge and methods to find, collect, secure, analyse, interpret and present digital evidence related to cases that occur in the interest of the reconstruction of events and the validity of judicial processes. However, some of the differences in cloud characteristics, cloud service models, adoption models, and types of crime make the level of difficulty and method of the investigation carried out differently.

Furthermore, [8] also mentions the current digital forensic method, it is still not appropriate to be applied to the cloud computing environment. So that digital forensic experts, investigators, researchers are required to continue to expand their knowledge and capabilities to conduct investigations into Cloud Forensics [9].

Several studies have been carried out regarding the investigation method in cloud computing. [6] conducted an analysis and survey of cloud computing environments to find out the types of crimes committed in cloud computing. Next [10] analysed the investigation of DDoS attacks in cloud computing with the SaaS model that uses SeaFile to find digital evidence that can be used in court. Then [11] conducted an investigative analysis of the IAAS private cloud computing model that was used in the Ministry of Public Security to produce a framework that could be used as an investigation guide only for the ministry's environment. [12] conducted research to present a new concept for digital artefacts acquisition in cloud computing as a consolidation between digital forensics and cloud computing.

Furthermore, [13] analysed investigations on private cloud computing that uses OwnCloud in the user's computer. The results of this study are to list locations and types of evidence that can be found. The last is research from [14] which also analysed the evidence acquisition model in a private cloud computing environment using the ADAM method that focuses on the client-side and identified the evidence at layer two and three on the server.

From several studies that have been described previously, it can be seen that one investigation model cannot be applied to various cloud environments or other types of cloud adoption models due to differences in characteristics. Even though digital evidence can be found on various devices [15] so that each of these devices requires a different investigation method.

When digital forensic investigations are to be carried out, it must follow the guidelines or the stages on the framework [16]. With the use of appropriate guidelines or frameworks, the digital evidence produced can provide directions to resolve the criminal case, and digital evidence can be declared valid by the court [17]. However, from the previous study that was described before, they did not use the specific guidelines, and also there are no specific guidelines that can be accurately used to conduct investigations on cloud computing [14].

One commonly used investigation guide is SNI 27037: 2014 concerning guidelines for the identification, collection, acquisition, and preservation of digital evidence [18]. So that in this study, SNI 27037: 2014 will be expanded to propose a novel framework to investigate on the private cloud computing environment from the server-side.

Therefore this study will focus on analysing digital forensic investigations on the server-side of the private cloud computing adoption model that uses OwnCloud using the novel framework to verify the compatibility of this framework and find out what digital evidence can be found. So this study will fill the gap research in the field of server-side from private cloud computing using the novel framework that has been proposed based on the guidelines standard.

The acquisition techniques that be used in this research is Static Forensic. Traditionally, there are two digital forensic categories, namely, “static forensic" and "live forensic" [19]. Static forensics involves the analysis of static data such as hard drives that are obtained using traditional formal acquisition procedures. The consideration to use Static Forensic Model is because this research only focuses on non-volatile data.

2. Research Methods

This study will be started by preparing the cloud computing system and environment. Then make case study and simulation based on cloud computing, and next analysed the critical components on SNI 27037:2014 that has four essential stages namely identification, collection, acquisition, and preservation of digital evidence to be carried out in the investigation process. After that, the digital evidence will be analysed to gather the information that can be used to solve the case. The hypothesis is that there are two potential forms of evidence, namely user folders and server logs.

The research methodology that will be carried out to complete this research are as follows :

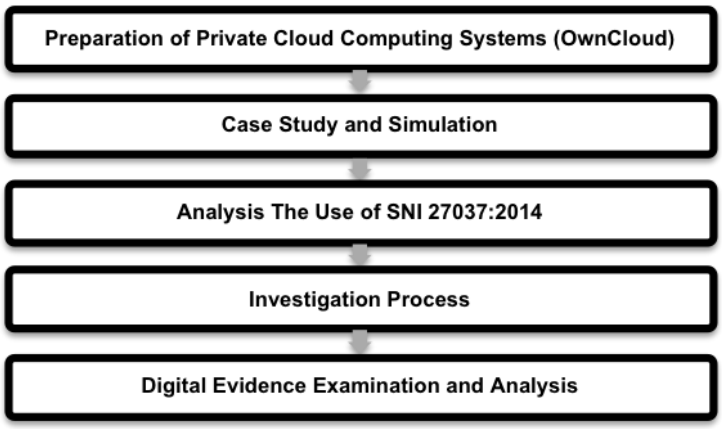


Figure 1. Research Methodology

2.1. Preparation of Private Cloud Computing Systems (OwnCloud)

It is the stage in preparing hardware and software specifications used in the research that is designing and implementing SaaS private cloud computing, such as installing, configuring and testing OwnCloud servers.

2.2. Case Study and Simulation

It is the stage of making a case simulation on the OwnCloud Private Cloud Computing SaaS. Case simulations will be carried out related to abuse of data authority on OwnCloud, and an investigation will be conducted to find evidence of abuse of authority against the data on the server-side.

2.3. Analysis The Use of SNI 27037:2014

This stage will analyse the application of SNI 27037: 2014 in the private cloud computing investigation environment. In SNI 27037: 2014, there are four essential stages in the investigation process, namely identification, collection, acquisition, and preservation of digital evidence. At this stage, the four investigation processes will be mapped, and the investigation planning will be prepared. From this mapping, the novel investigation framework will be proposed to be used in the cloud computing environment.

2.4. Investigation Process

At this stage, the investigation process will begin to be carried out based on the planned investigation activities and the novel investigation framework. The investigation process will be divided into four main stages, namely, identification, collection, acquisition, and preservation of digital evidence.

2.5. Digital Evidence Examination and Analysis

It is the stage of checking digital evidence that has been acquired by extracting digital evidence. After extracting the evidence, the next is to analyse digital evidence.

The analysis is carried out by carefully examining the structure of files and folders and then conducting a process of searching for digital evidence that can be used as a guide to the case of an investigation conducted.

3. Result and Discussion

3.1. Preparation of Private Cloud Computing Systems (OwnCloud)

The first stage in this research is to prepare the system to simulate the Private Cloud Computing environment using OwnCloud by installing and configuring the server. Some requirements related to hardware, software, and computer specifications are shown in Table 1.

Table 1. List of Hardware and Software Specifications

No	Hardware / *Software*	Notes
1	PC *Server*, Processor Intel Core i3-2100 CPU@3.10*Ghz*, Hard Disk 10 GB, RAM 6 GB	Hardware
2	Operating System Linux Ubuntu Server 18.04	*Software*
3	OwnCloud Server 10.0.3	Software

The Cloud Computing Server is installed using Ubuntu Server 18.04 and has the IP Address 172.10.6.69. Then, the OwnCloud can be accessed on address http://172.10.6.69/OwnCloud.

3.2. Case Study and Simulation

This stage creates a case simulation in the Cloud Computing Private environment. The case used as a simulation in this study is a case of leakage of internal company information with the suspect initials "A." The secret company file is suspected to be stored by the suspect in the company's cloud storage, but the suspect denied this. So a digital forensic procedure must be performed on the server-side to find digital evidence as proof that the suspect has committed the crime. Figure 2 shows the flow of the case simulation.

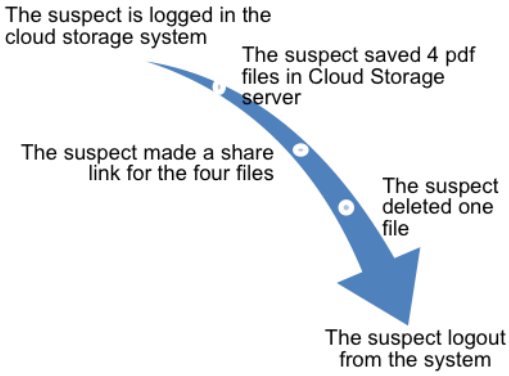


Figure 2. Case simulation process flow

There are four pdf extension files prepared in this case simulation. The hash code values of the four files can be seen in Table 2. *Hash Values* below.

Table 2. Hash Values

No	File Name	File Size	MD5 Value
1	Draft Annual Report (SECRET).pdf	11.73 MB	E084E4F46B782178C32EE5CF748566C8
2	Director Statement about The Responsibility (SECRET).pdf	1.34 MB	BEA17D8CCFFFF56B750BCEBBA8982F68
3	Financial Report (SECRET).pdf	32.46 MB	DCB0A8DC2660A8611F546DD356BC4659
4	Draft Organization Structure (SECRET).pdf	471.96 KB	618F75868CD5321A6FDC7A0F37C64F99

3.3. Analysis The Use of SNI 27037:2014

The four main stages of SNI 27037:2014 will be developed and adjusted to the needs contained in the cloud computing environment so that the investigation process will follow the basis of this standard. [20] have mapped in detail the sequence and essential stages of each investigation process and in this study will use the mapping as the primary basis for planning the investigation process.

Based on the results of the mapping, the next step is to propose a framework in the private cloud computing environment that will be tested to complete a predetermined case simulation. After the acquisition process is completed, the next stage is the examination and analysis of digital evidence focused on two stages. The first stage is looking for the location of folders and user files related to the case, and the second stage is searching for logs of activities carried out

by suspects in cloud computing to be used as a timeline for reconstructing events that have occurred.

The proposed novel investigation framework on private cloud computing based on SNI 27037: 2014 named The Private Cloud Computing Investigation Framework (PCCIF) can be seen in Figure 3.

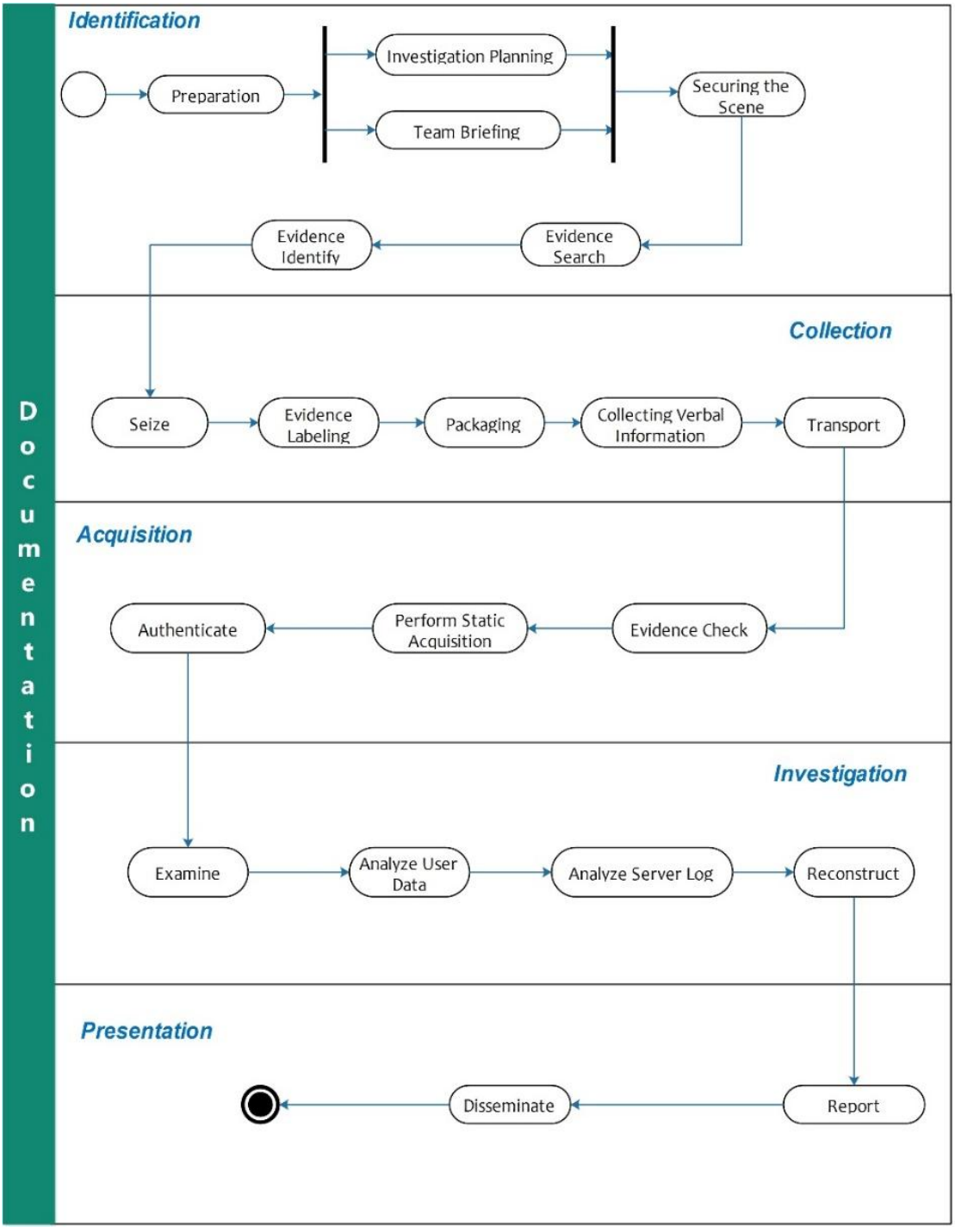


Figure 3. The Private Cloud Investigation Framework

3.4. Investigation Process

The investigation process will be divided into four main stages, namely, identification, collection, acquisition, and preservation of digital evidence. The investigation process carried out based on the framework that has been proposed previously is:

A. Identification

1. Preparation
   - Investigation Planning
     The planning tools used are prepared and must be ready to use.
   - Team Briefing
     In this case, the entire investigation team was reminded that the main focus of the evidence was the cloud computing server.
2. Securing the scene

   The process of securing a crime scene is carried out by investigators by placing a dividing line so that the crime scene cannot be entered by people who do not have access.
3. Evidence Search

   Based on the team's direction, it has been determined that the primary evidence is the cloud server. The server has been found in powered-on.
4. Evidence Identify

   The Cloud Computing server found at the crime scene has the following specifications:

Table 3. Evidence Specification

No	Hardware	Notes
1	PC *Server*, Processor Intel Core i3-2100 CPU@3.10*Ghz*, Hardisk 10 GB, RAM 6 GB	Black colour, Casing PowerLogic

B. Collection

1. Determine evidence seized or acquired at the crime scene

   In the case of this cloud investigation, it was determined from the beginning that the evidence would be seized first, and then the acquisition procedure would be carried out in the forensic laboratory.
2. Seize the evidence

   Based on the related procedures, the adjustments are made to the case of an investigation on the cloud server to be performed. On the server, no volatile or live data is needed because it will focus on non-volatile data. Moreover, the data on the server is unstable, and then a standard system shutdown procedure is performed on the server.
3. Evidence Labelling

   The server that has been shut down is then given an evidence label. The label provided contains the identity of the server computer, specifications, the time and date the seizure of evidence was carried out.
4. Evidence Packing

   The server as evidence must put into the evidence wrapping such as server computer box.
5. Gathering verbal statements from witnesses

   The verbal information collected is the server's computer password as an internal requirement of the investigator.

C. Acquisition

1. Security inspection of evidence

Activities at this stage are to ensure the use of write blockers as protection against evidence that the acquisition process does not contaminate the evidence.

2. Selection of the acquisition model

   Based on the needs of this research, the acquisition model used is the acquisition model on the powered-off devices in point (b) due to the state of the server that has been turned off in the previous procedure. The acquisition procedure is carried out following the procedure set out in sub-clause 7.1.3.2.

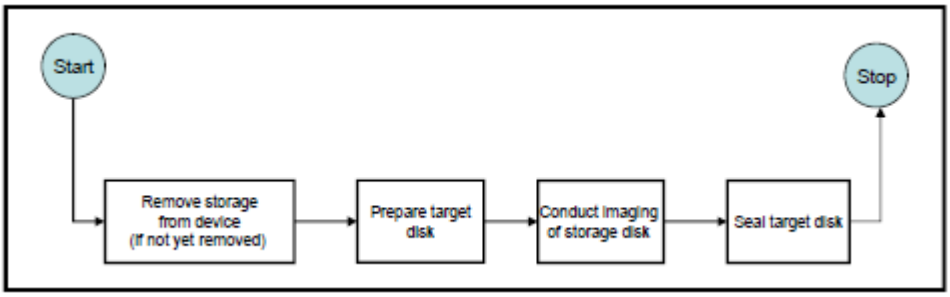


Figure 4. Acquisition Procedures

Based on this procedure, the hard disk on the server computer is removed first. In the target disk seal process, the type of seal used is hashing with md5, which degenerates automatically by the AccessData FTK Imager software used for acquisition.

3. Implementation of the acquisition

   The acquisition procedure is carried out using the AccessData FTK Imager tool. The 10 GB disk capacity takes 70 minutes from the acquisition to verification, and the acquisition file is named Evidence001-OwnCloudServer. The acquisition procedure starts on July 15, 2019, at 11:35, ICT, and finishes at 13.05.

4. Verification of acquisition

   Verification is done using a hash function. Figure 5 is the result of hashing the file of the acquisition result, and the result of proof files whose hash results are verified.

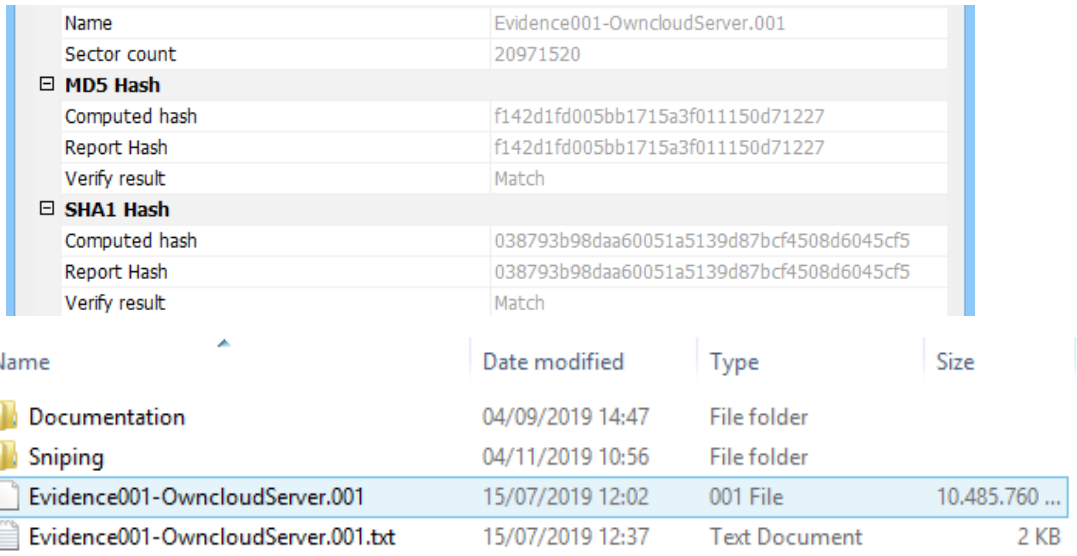


Figure 5. Verification Acquisition

D. Preservation

1. Provide evidence seals

   The sealing is carried out on the packaging of evidence that has been packaged starting from the evidence to be moved to the laboratory until it reaches the laboratory, the seal is opened for analysis and examination of the evidence.

2. The security check of evidence transport

   The security aspect check is carried out by ensuring the position of the evidence in the transport vehicle is in an excellent position to keep the evidence from collision during the trip to the laboratory.

3. Evidence Transport

   The transport of evidence is carried out with care and caution. The officer always updates the chain of custody documents when there is an event outside the plan that occurs.

4. Evidence Storage

   The analysed evidence must remain in the laboratory or be stored in the police evidence storage room until the court judge will decide whether the evidence is returned to the owner or destroyed for court purposes.

3.5 Digital Evidence Examination and Analysis

Based on the results of the examination carried out on digital evidence, the results obtained that the evidence can be read well by forensic software and the overall structure of files and folders can be read correctly.

Four partitions have been successfully read by autopsy forensic software. The four partitions are vol1, vol4, vol5, and vol6. The results of the examination of the four partitions are summarised in Table 4.

Table 4. Examination results

No	Type of Findings	Function	Result
1	Vol1	Unallocated Space	Can be examined
2	Vol4	Swap Partition	Can be Examined
3	Vol5	Data Partition	Can be Examined
4	Vol6	Unallocated Space	Can be Examined

Vol1 and vol6 partitions are unallocated space partitions, then vol4 is a swap partition, there is only one file, so the three partitions are not analysed. The analysis process is carried out only on partition vol5.

There are two focuses of analysis conducted on vol5 partitions, namely the first focus is to find the location of the company's secret files and files stored by the suspect in the Cloud, the second focus is to search for logs that record the activities carried out by suspects in the Cloud.

3.5.1 The First Focus of Analysis

Based on the results of the analysis conducted, it is known that the location of the user's data storage folder on the OwnCloud system depends on the choices made by the administrator when first configuring OwnCloud. So that the location of this folder cannot be a global provision because each server admin can make changes to the folder location as needed. However, by default, according to the installation guide released by OwnCloud, the folder location is in the directory */var/www/html/owncloud/data*. In this directory, all files are belonging to users grouped by folders based on the username registered on the OwnCloud system.

The configuration of the OwnCloud directory in this research is standard, so the directory location is found in */var/www/html/owncloud/data*. There are two users in this cloud system based on the folder found, namely “admin” and “aliandoputra”.

Aliandoputra folder is a directory that is suspected as the location of evidence. So that further checks are carried out on the folder. From the results of the inspection, it is known that in the folder, there are four folders, namely cache, files, files_trashbin, and uploads. The cache folder

is the default folder that the OwnCloud system creates as a cache, then files_trashbin is a folder that contains files deleted by the user from the OwnCloud system, the uploads folder is a folder that contains user data uploaded from the web system.

The primary location of evidence is in the "files" folder because it is a folder that contains all user data stored in the cloud. Based on the examination of the folder, there are four confidential company files which become evidence, as shown in Figure 6 below.

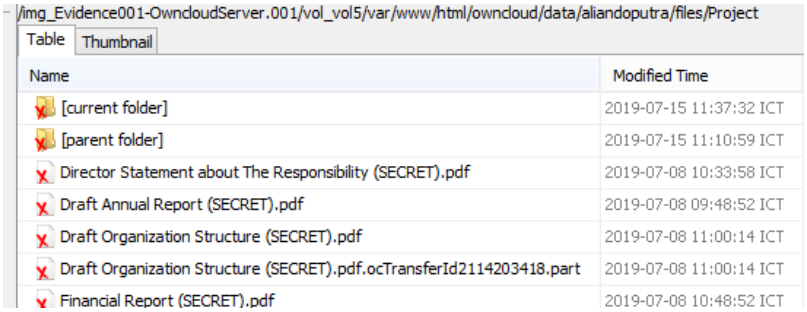


Figure 6. User Directory

Based on an examination of the four files, it is known that the four files are original and identical files with the original files prepared in this study. This can be seen from the match of the hash code between the four files found with the original file that has been prepared.

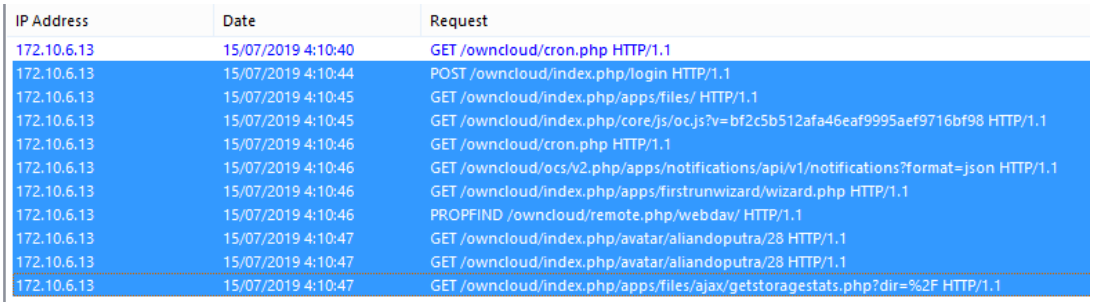
In the user's folder, there is also a folder with the name files_trashbin. This folder is used by OwnCloud as a location for files deleted by the user from the data folder. Then an examination of the folder was carried out, and it was found that there was one file that was deleted with the file name "Director Statement about The Responsibility (SECRET).pdf". The file was last accessed at 11:37:32.

3.5.2 The Second Focus of Analysis

The second focus of the analysis is carried out on the OwnCloud server log to find out the suspect's activity record. The first analysis log file is the log contained on the webserver. It is performed because the apache webserver will record all requests that come to the server. So the request for access the OwnCloud will be recorded in the log. On a server with a Linux operating system and using apache2 as a webserver service, logs are generally located in /var/ www/apache2/.

In this research, the webserver log is still in the default position. After finding the log, the file \ is extracted, and then it will be analysed using the Apache Log Viewers software. This additional software is used to simplify and speed up the analysis process because the software will improve the log structure and can sort it by time.

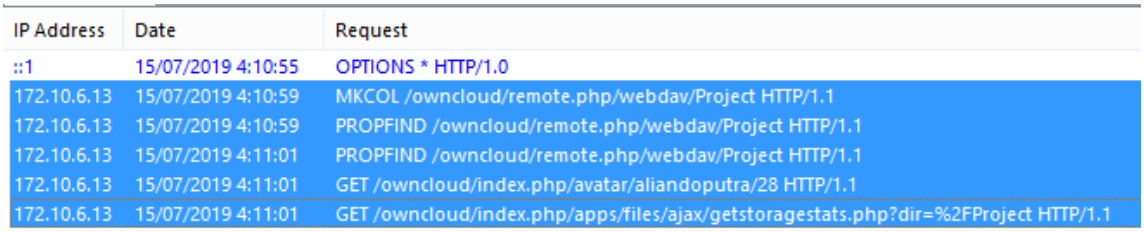
Based on the results of the analysis conducted on the file access.log, it can be found that on July 15, 2019, at 4:10:44 there is login access to OwnCloud from IP 172.10.6.13 using the username "aliandoputra" as shown Figure 7. The time difference on analysis of autopsy software with Apache Log Viewer because autopsy has been configured to display the time in the ICT zone (IndoChina Time +7) while the Apache Log Viewer uses the default time zone of the OwnCloud server, which is GMT 0.



IP Address	Date	Request
172.10.6.13	15/07/2019 4:10:40	GET /owncloud/cron.php HTTP/1.1
172.10.6.13	15/07/2019 4:10:44	POST /owncloud/index.php/login HTTP/1.1
172.10.6.13	15/07/2019 4:10:45	GET /owncloud/index.php/apps/files/ HTTP/1.1
172.10.6.13	15/07/2019 4:10:45	GET /owncloud/index.php/core/js/oc.js?v=bf2c5b512afa46eaf9995aef9716bf98 HTTP/1.1
172.10.6.13	15/07/2019 4:10:46	GET /owncloud/cron.php HTTP/1.1
172.10.6.13	15/07/2019 4:10:46	GET /owncloud/ocs/v2.php/apps/notifications/api/v1/notifications?format=json HTTP/1.1
172.10.6.13	15/07/2019 4:10:46	GET /owncloud/index.php/apps/firstrunwizard/wizard.php HTTP/1.1
172.10.6.13	15/07/2019 4:10:46	PROPFIND /owncloud/remote.php/webdav/ HTTP/1.1
172.10.6.13	15/07/2019 4:10:47	GET /owncloud/index.php/avatar/aliandoputra/28 HTTP/1.1
172.10.6.13	15/07/2019 4:10:47	GET /owncloud/index.php/avatar/aliandoputra/28 HTTP/1.1
172.10.6.13	15/07/2019 4:10:47	GET /owncloud/index.php/apps/files/ajax/getstoragestats.php?dir=%2F HTTP/1.1

Figure 7. Login Access

Then at 4:10:59, there is access to the server to create a new directory with the directory name "Project" as shown in Figure 8. It was previously known that the "Project" directory contained all of the company's confidential files.



IP Address	Date	Request
::1	15/07/2019 4:10:55	OPTIONS * HTTP/1.0
172.10.6.13	15/07/2019 4:10:59	MKCOL /owncloud/remote.php/webdav/Project HTTP/1.1
172.10.6.13	15/07/2019 4:10:59	PROPFIND /owncloud/remote.php/webdav/Project HTTP/1.1
172.10.6.13	15/07/2019 4:11:01	PROPFIND /owncloud/remote.php/webdav/Project HTTP/1.1
172.10.6.13	15/07/2019 4:11:01	GET /owncloud/index.php/avatar/aliandoputra/28 HTTP/1.1
172.10.6.13	15/07/2019 4:11:01	GET /owncloud/index.php/apps/files/ajax/getstoragestats.php?dir=%2FProject HTTP/1.1

Figure 8. Create a New Directory Process

Then starting at 4:12:35 until 4:21:39, the suspect carried out the process of uploading four company files into the folder "Project." The details of the process of uploading the four files are based on the results of an analysis of the access log summarised in Table 5 below.

Table 5. Detail Process of Upload Four Files

Date	Request	Note
15/07/2019 4:12:35	PUT /OwnCloud/remote.php/dav/uploads/aliandoputra/web-file-upload-a793a34d850b1788da191dc244bee16b-1563163954604/0 HTTP/1.1	Upload process the first file
15/07/2019 4:12:47	PROPFIND /OwnCloud/remote.php/webdav/Project/Draft%20Annual%20Report%20(SECRET).pdf HTTP/1.1	Get properties process the first file.
15/07/2019 4:14:30	PUT /OwnCloud/remote.php/webdav/Project/Director%20Statement%20about%20The%20Responsibility%20(SECRET).pdf HTTP/1.1	Upload process the second file
15/07/2019 4:14:35	PROPFIND /OwnCloud/remote.php/webdav/Project/Director%20Statement%20about%20The%20Responsibility%20(SECRET).pdf HTTP/1.1	Get properties process the second file.
15/07/2019 4:20:03	PUT /OwnCloud/remote.php/dav/uploads/aliandoputra/web-file-upload-2e42075a3cf116c597f24b66073888da-1563164402672/0 HTTP/1.1	Upload process the third file
15/07/2019 4:20:59	PROPFIND /OwnCloud/remote.php/webdav/Project/Financial%20Report%20(SECRET).pdf HTTP/1.1	Get properties process the thir file.
15/07/2019 4:21:34	PUT /OwnCloud/remote.php/webdav/Project/Draft%20Organization%20Structure%20(SECRET).pdf HTTP/1.1	Upload process the fourth file
15/07/2019 4:21:39	PROPFIND /OwnCloud/remote.php/webdav/Project/Draft%20Organization%20Structure%20(SECRET).pdf HTTP/1.1	Get properties process the fourth file.

Furthermore, at 4:37:32, evidence was obtained from the log that the suspect deleted one file with the file name "Director Statement about The Responsibility (SECRET) .pdf." The log details can be seen in Table 6 below.

Table 6. Deleted File Process

Date	Request	Note
15/07/2019 4:37:32	DELETE /OwnCloud/remote.php/webdav/Project/Director%20Statement%20about%20The%20Responsibility%20(SECRET).pdf HTTP/1.1	Process delete file

From the analysis of evidence obtained on the web server log, the timeline chronology is obtained, which is one of the essential things in digital forensic analysis. Based on the timeline, step by step, how a case occurs can be clearly described. The timeline chronology details of the cases that occurred in this research are:

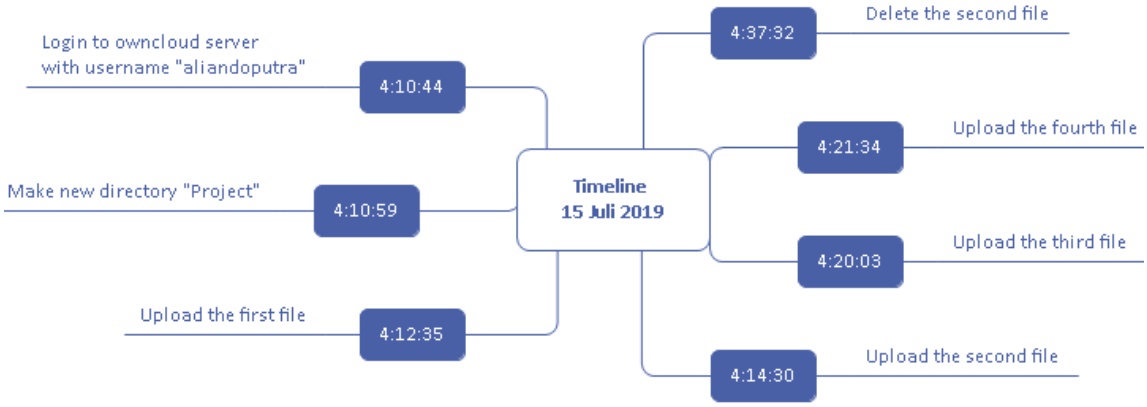


Figure 9. Timeline Chronology

Based on the entire investigation process, it can be concluded that the investigative analysis carried out on a cloud computing private server, can find two digital evidence items that can be used for the trial. First is digital evidence that has been obtained in the OwnCloud data directory that contains user data stored in cloud computing and user data that has been deleted. The second is digital evidence obtained from a web server log that contains the chronology of the chase sequence.

One of the main difference between the result of this research and other research that has been described previously is these results can produce the detail of timeline chronology based on the evidence that is gathered from the analysis process. This timeline is useful for the investigator to analyse the case. Then, the investigation process is performed using the novel framework based on SNI 27037:2014. While the previous research, not used the standard to perform the investigation. So the digital evidence can be declared as a piece of valid evidence at a court.

4. Conclusion

Based on the results and analysis process carried out in this research, it can be concluded that the novel investigation framework based on SNI 27037: 2014 can be used to investigate a cloud computing environment. The whole process in the latest framework can be carried out, and evidence can be examined and analysed using forensic software.

From the results of the examination and analysis carried out, it can be found digital evidence in the form of files and folders from user data sorted by user name. Then also in the form of a web server log that contains historical data activities carried out by the user on the server. Based on the webserver log, an event timeline can be generated to reconstruct the case.

Based on the limitations of the research, the suggestions for further research development is to do acquiring volatile data, because there may also be evidence stored in volatile data and also analyse a database server that has the potential to become evidence.

References

[1] C. T. S. Xue and F. T. W. Xin, "Benefits and Challenges of the Adoption of Cloud Computing in Business," *International Journal on Cloud Computing: Services and Architecture*, vol. 6, no. 6, pp. 01–15, 2017.

[2] E. Erturk, "An incremental model for cloud adoption: Based on a study of regional organizations," *TEM Journal*, vol. 6, no. 4, pp. 868–876, 2017.

[3] RightScale, "RightScale 2018 : State of the Cloud Report," 2018.

[4] S. Goyal, "Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review," *International Journal of Computer Network and Information Security*, vol. 6, no. 3, pp. 20–29, 2014.

[5] L. Columbus, "Roundup Of Cloud Computing Forecasts And Market Estimates, 2018," *Forbes*, 23-Sep-2018.

[6] D. Kolthof, "Crime in the Cloud : An Analysis of the Use of Cloud Services for Cybercrime," in *23rd Twente Student Conference on IT*, 2015.

[7] S. Hraiz, "Challenges of digital forensic investigation in cloud computing," *ICIT 2017 - 8th International Conference on Information Technology, Proceedings*, pp. 568–571, 2017.

[8] S. Simou, C. Kalloniatis, S. Gritzalis, and H. Mouratidis, "A survey on cloud forensics challenges and solutions," *Security and Communication Networks*, vol. 9, no. 18, pp. 6285–6314, 2016.

[9] S. Almulla, Y. Iraqi, and A. Jones, "A State-Of-The-Art Review Of Cloud," *Journal of Digital Forensics, Security and Law*, vol. V9N4, pp. 7–28, 2014.

[10] R. B. Bahaweres, B. Santoso, and A. Ningsih, "Cloud Based Drive Forensic and DDoS Analysis on Seafile as Case Study," in *International Conference on Computing and Applied Informatics*, 2017, vol. 755, no. 1.

[11] G. Zeng, "Research on Digital Forensics Based on Private Cloud Computing," *IPASJ International Journal of Information Technology*, vol. 2, no. 9, pp. 24–29, 2014.

[12] M. M. Nasreldin, M. El-hennawy, H. K. Aslan, and A. El-hennawy, "Digital Forensics Evidence Acquisition and Chain of Custody in Cloud Computing," *IJCSI International Journal of Computer Science Issues*, vol. 12, no. 1, pp. 153–160, 2015.

[13] G. Al Sadi, "Extracting Potential Forensic Evidences from Cloud Client Device using own Cloud as a Case Study," *International Journal of Computer Applications*, vol. 132, no. 7, pp. 15–21, 2015.

[14] N. Widiyasono, I. Riadi, and A. Luthfi, "Investigation on the Services of Private Cloud Computing by Using ADAM Method," *International Journal of Electrical and Computing Engineering (IJECE)*, vol. 6, no. 5, pp. 2387–2395, 2016.

[15] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," in *CDFSL Proceedings*, 2016, pp. 9–20.

[16] Y. D. Rahayu and Y. Prayudi, "Membangun Integrated Digital Forensics Investigation Frameworks (IDFIF) Menggunakan Metode Sequential Logic," *Seminar Nasional SENTIKA*, vol. 2014, no. Sentika, 2014.

[17] D. Sudyana, Y. Prayudi, and B. Sugiantoro, "Analysis and Evaluation Digital Forensic Investigation Framework Using ISO 27037 : 2012," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 8, no. 1, pp. 1–14, 2019.

[18] Badan Standarisasi Nasional, *SNI 27037:2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, pengumpulan, Akuisisi, dan Preservasi Bukti Digital*. Jakarta, 2014.

[19] R. Montasari, "A standardised data acquisition process model for digital forensic investigations," *International Journal of Information and Computer Security*, vol. 9, no. 3, pp. 229–249, 2017.

[20] D. Sudyana, B. Sugiantoro, and A. Luthfi, "Instrumen Evaluasi Framework Investigasi Forensika Digital Menggunakan SNI 27037:2014," *Jurnal Informatika Sunan Kalijaga*, vol. 1, no. 2, pp. 75–83, 2016.