Published *online* on the journal's web page : http://innovatics.unsil.ac.id

Innovation in Research of Informatics (INNOVATICS)

| ISSN (Online) 2656-8993 |

Data Integrity Testing of Digital Evidence Data Capture Results on Private Cloud Computing Services

*Arif Maulana Komarudin[1], Nur Widiyasono[2], Aldy Putra Aldya[3], Randi Rizal[4]**

[1,2,3,4]*Department of Informatics, Siliwangi University, Jl. Pembela Tanah Air (PETA) No. 177, Kota Tasikmalaya 46115, Indonesia*
[1]*arifmaulana@gmail.com,* [2]*nur.widiyasono@unsil.ac.id,* [3]*aldy@unsil.ac.id,* [4]*randirizal@unsil.ac.id*

ARTICLE INFORMATION

Article History:
Received: August 22, 2023
Last Revision: October 11, 2023
Published *Online*: November 5, 2023

KEYWORDS

Acquisition,
Digital Evidence,
Digital Forensics,
Investigations,
Private Cloud,
Data Integrity

CORRESPONDENCE

Phone: +6285320132014

E-mail: randirizal@unsil.ac.id

ABSTRACT

Private Cloud has better advantages than other cloud services because private cloud is managed and run by the company itself so that cloud needs can be tailored to the company's needs, but allows abuse from within the company itself, as in the case study simulation of a Gojek startup company. This case occurred because of a security weakness in the system so that internal people took advantage of these weaknesses for their own benefit by leaking confidential data, acquisitions were carried out to prove and find evidence of crime, acquisitions used live acquisition techniques, namely acquisitions on an ongoing system, namely monitoring network traffic using Wireshark tools , the method in this case uses the Digital Forensics Investigating Framework (DFIF), data integrity must be properly maintained when acquiring digital evidence because to maintain the authenticity of the digital evidence obtained, then data integrity is tested on the digital evidence obtained, testing is carried out on digital evidence before and after the acquisition to see if there is a change in data integrity, the research results show that there is no change in data integrity.

1. INTRODUCTION

Data integrity is an aspect of information security (CIA Triad) [1], so data integrity must be maintained properly to maintain data authenticity and ensure information is not changed. Digital evidence is a digital trace that is found in a crime in the form of information, data, or the activity of the perpetrator obtained by the process of forensic investigation by investigators [2].

Based on this, data integrity is very important in digital evidence to maintain the authenticity of digital evidence so that this evidence can be used in court and is legally valid because the integrity of the data is maintained and is valid evidence [3]. One of the algorithms used to check data integrity is MD5, SHA-1, RIPEMD-160, SHA-2, and SHA-3. This algorithm is used to check the hash value of the data [4], this algorithm can maintain data integrity very well because if there is even a slight change in the data, the hash value will also change. Also, the algorithm described in the text provides a robust mechanism for maintaining data integrity through hash value verification. Its ability to detect even the slightest changes in data content makes it a valuable tool in various fields that rely on trustworthy data, ensuring the accuracy, reliability, and security of information in a world driven by digital data and technology.

Private cloud is created with the aim of functioning as a data processing server that is used to store and manage programs on the internet [5]. One of the advantages of private cloud is that cloud management is carried out independently by the company so that it can adjust to its needs, but there are drawbacks, namely integrity, where there are irresponsible persons such as leaking confidential data [6]. Acquisition and integrity testing is carried out to obtain activity, digital evidence, and data integrity either before acquisition or after acquisition by checking the hash value [7]. It involves the careful collection of digital evidence, maintaining the integrity of that evidence, and verifying its authenticity through the comparison of hash values. These processes are essential for ensuring the credibility of digital evidence in investigations, legal proceedings, and various analytical tasks.

In this research, the method used is the Digital Forensics Investigation Framework (DFIF) [8]. This framework is used as a guideline for analyzing in investigations and testing the integrity of digital evidence data captured data on private clouds. The use of this method is because only a few use this method , as well as the use of the DFIF method in the acquisition and testing of data integrity is the latest in this research.

2. RELATED WORK

Several studies regarding the acquisition of digital evidence in private clouds using various methods, such as those carried out [9], discuss the analysis of the PC desktop investigation process connected to private cloud services. The research uses the End-to-End Digital Investigation (EEDI) method. The EEDI stages consist of Collecting Evidence, Analysis of Individual Events, Preliminary Correlation, Event Normalizing, Event Deconfliction, Second Level Correlation, Timeline Analysis, Chain of Evidence Construction, and Corroboration. Investigation of data capture in private clouds, such as Firefox browser cache and cookies, activities carried out by perpetrators such as traces of sending emails and sending files, as well as carrying out crime reconstruction.

Another study was conducted by [10] with the title Application of the ADAM Method in the Investigation Process of Private Cloud Computing Services, research using The Advance Data Acquisition Model (ADAM) method, the ADAM stages consist of Initial Planning, Planning on location (The On-Site Planning), Digital Data Acquisition (Acquisition Digital Data) case studies in this study are carried out in a simulation manner, the research focuses on private cloud investigations using the ADAM method, namely making acquisitions using live acquisition techniques and write block data acquisition, namely monitoring network traffic is then saved in .pcap format found mac-addresses, hosts, frames, files, images, messages, credentials, sessions, DNS(s), parameters, keywords, cleartext, anomalies and searches for digital evidence on the device.

Subsequent research was carried out by [11] research entitled Forensic Investigation Framework on Server Side of Private Cloud Computing using the SNI 27037:2014 method using the SNI 27037:2014. Method the research was carried out on case study simulations, this study managed to find evidence of digital files and folders from the user, also find web server logs that contain user activity on the server, and a timeline that is a case reconstruction.

Based on research related to each method having advantages and disadvantages in private cloud investigations, therefore, this research was conducted using the Digital Forensics Investigation Framework (DFIF) on private clouds as well as testing the integrity of data captured by the data, the process was carried out by simulating case studies as well as acquisition with DFIF with the stages of collection, examination, analysis, reporting and documentation and at the end of the research data integrity testing is carried out, namely checking whether there is a change in the hash value in the file before the acquisition is carried out and after the acquisition is carried out.

3. METHODOLOGY

This research has flow stages, as shown in Figure 1 below.

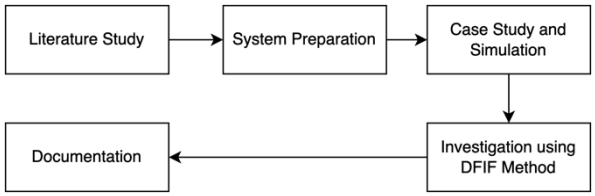


Figure 1. Methodology

3.1 Literature Study

The literature study was carried out with the aim of collecting data and sources related to digital evidence acquisition research on private clouds using the DFIF method so that it supports the research process, and literature is carried out in journals, e-proceeding, and via the internet.

3.2 System Preparation

This research was carried out in a case study simulation so that system preparation had to be carried out before the case study simulation was carried out. System preparation included building a network topology, namely using a proxy, and access point, installing the owncloud-5.0.5 server using Windows advanced server 2008, as well as client preparation used by the actor. The following is the network topology used in Figure 2 below.

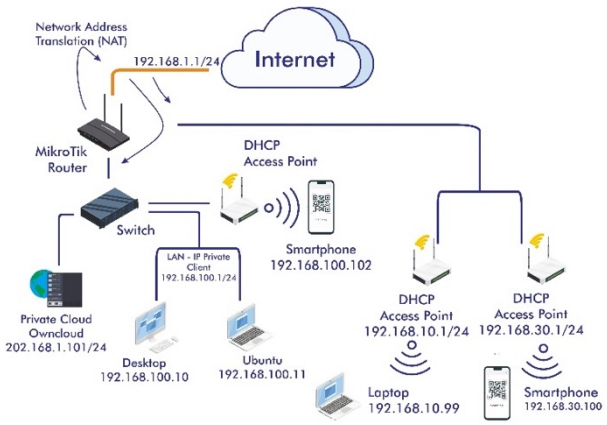


Figure 2. Network Topology

Investigation of a case study simulation using a private cloud: the investigation begins on the own cloud private cloud server side, then on the network side by monitoring network traffic at layer 5 using the wiresharsk tool then on the device of each actor used, the purpose of this investigation is to find evidence digital devices located on each device, whether on the server side, network, or perpetrator's device, then finds logs or activity from the perpetrators on the network side, namely at layer 5. The devices used in this study are listed in Table I below.

TABLE 1. HARDWARE USED

No	Hardware	Information
1.	Server	*Server-PC H61H2-M6 Intel(R) Core(TM) i3-3220 CPU @ 3.30Ghz (4 CPUs), ~ 3.3GHz*
2.	Laptop	*Acer E5-476G Intel(R) Core(TM) i5-8250U CPU @ 1.60Ghz (8 CPUs), ~ 1.8GHz*
3.	Desktop	*Presario V3500 Intel(R) Core(TM)2 Duo T7100 @ 1.80Ghz (2 CPUs), ~ 1.8GHz*
4.	Switch	T7100 @ 1.80Ghz (2 CPUs), ~ 1.8GHz
5.	Mikrotik	Mikrotik RB941-2nD-TC hAP Lite

6.	Smartphone	Xiaomi POCO X3 GT MediaTek MT6891 Dimensity 1100 (6 nm), Octa-core (4x2 GHz Cortex-A78 & 4x2.0 GHz Corte A55), Mali-G77 MC9
7.	Access Point	TP-LINK TL-WA701ND
8.	UTP+RJ45 cable	To connect local network devices.
9.	USB cable	To transfer digital evidence on a smartphon
10	Smartphone 2	*Xiaomi POCO M3 Pro MediaTek MT6833 Dimensity 700 (7 nm Octa-core (2x2.2 GHz Cortex-A76 & 6x2. GHz Cortex-A55), Mali-G57 MC2*
11	Laptop 2	*Samsung NP355e4x AMD Dual Core E. 1200*

This study uses several supporting software, as listed in Table 2 below.

TABLE 2. SOFTWARE USED

No	Hardware	Information
1.	Windows Server 2008	The operating system used for the own cloud server.
2.	OwnCloud	*A Cloud storage application, as research objects.*
3.	XAMPP v3.2.1	Supporting applications in building own cloud servers.
4.	Wireshark Network Miner	Network analyzer for monitoring and analyzing network traffic
5.	MailServer	AP Lite The application is used as an email server on the Windows operating system.
6.	*Mozilla Thunderbird*	Email client for case scenarios sending emails by perpetrators.
7.	*Folder2Iso IsoCraft*	Application used for cloning digital evidence.
8.	*HashMyFile HashChecker*	The application used to check digital proof hash value.
9.	*Winbox*	The tools used to configure the proxy.
10	*Windows 7*	The operating system is used by a third actor
11	*Linux Ubuntu 20.04*	The operating system used by the second perpetrator
12	*Android 12*	The operating system used by the first offender

3.3 Case study simulation

The case study in this research was carried out in a simulation in a lab, so it does not use actual cases, the case study occurred at a Gojek Startup company in the city of Tasikmalaya, this case occurred because there were employees who misused private cloud storage to leak company confidential data to competitors , the investigator is tasked with carrying out investigations on the server side, network traffic, and devices used by the suspect, it is known that the private cloud used is a shared cloud because it is a building facility and allows abuse by leaking confidential data. The following scenario is carried out.

3.3.1 First Actor:

a. Opening Google Chrome on the POCO X3 GT smartphone, then accessing the company's own cloud site.
b. Login using the operator staff account on the owncloud site.
c. Uploading a secret file from the smartphone storage that the perpetrator is using then sharing access to the uploaded file to the second actor, namely market sales staff.

3.3.2 Second Actor

a. Open the browser from the Acer Aspire E5-476G laptop with the Linux operating system.
b. Login to the own cloud site, download the file that was shared by the first actor and then save it on the laptop's internal storage.
c. Log out of the owncloud site.
d. Sending confidential files to third actors using Mozilla Thunderbird.

3.3.3 Third actor

a. Opened Mozilla Thunderbird from desktop, i.e., Presario V3500.
b. Opened the email and downloaded the file shared by the second perpetrator.
c. Sending back secret files to the next perpetrator using Mozilla Thunderbird.

3.3.4 Fourth Actor

a. Received the third perpetrator's email and stored it on internal storage.
b. Login to the own cloud site
c. Upload files and share access to these files with colleagues, namely the next perpetrator.

3.3.5 Fifth Actor

a. Login to own cloud.
b. Downloading files shared by the fourth perpetrator, then storing them on a smartphone device.

3.4 Investigative using the DFIF Method

The method used in this study refers to the stages of the DFIF (Digital Forensics Investigation Framework) process and performs data integrity testing by comparing hash values, the steps taken are shown in Figure 2 below.

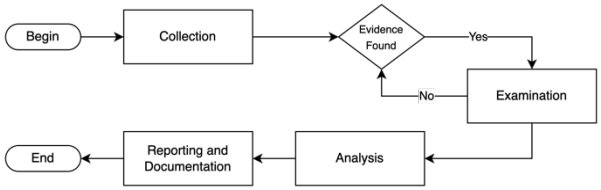


FIGURE 3. STAGES OF THE DFIF METHOD

3.4.1 Collection

Collecting digital evidence, namely monitoring the owncloud server network traffic, then the results of monitoring network traffic are stored in the .pcap format which will be analyzed further at the examination stage.

3.4.2 Examination

Examination is carried out on the packets that were carried out in the collection process earlier, namely checking network traffic on the server, namely examining criminal activity. After being found, an acquisition is carried out, namely on the server side, layer 5, as well as the perpetrator's device, namely imaging the digital evidence found.

3.4.3 Analysis

After obtaining digital evidence, the next step is to test the digital evidence obtained, namely by checking the hash value before the acquisition is carried out and checking the hash value after the acquisition is carried out.

3.4.4 Reporting and Documentation

This stage reports and documents what happened during the investigation, such as activity on network traffic, and tests the integrity of the evidence, namely the hash value, namely digital evidence before the acquisition and digital evidence after the acquisition, whether there is

a change in the integrity of the hash value of the file. The digital evidence. After completing the investigative stages using the DFIF method, the research continued with the documentation stage, namely reporting on the research process, such as the tools used, and the methods used, and providing recommendations for improvement for further research.

4. RESULT AND DISCUSSION

The research implementation tests data integrity and investigates digital evidence of data capture on private cloud services using the DFIF method, several IP addresses of devices connected to the network:

TABLE 3. IP ADDRESS DEVICE

No	Device	IP Address	Status
1.	Server 1	202.168.1.101/24	Connected
2.	Laptop	192.168.100.11/24	Connected
3.	Desktop	192.168.100.10/24	Connected
4.	Mikrotik	192.168.100.1/24	Connected
5.	Access Point1	192.168.100.101/24	Connected
6.	*Smartphone*	192.168.100.102/24	Connected
7.	*Laptop 2*	192.168.10.99/24	Connected
8.	*Smartphone 2*	192.168.30.100/24	Connected

The steps taken in the investigation of the private cloud are as follows:

4.1 Collection

This stage collects digital evidence, carried out by monitoring network traffic using Wireshark. The monitoring process is shown in Figure 4 below.

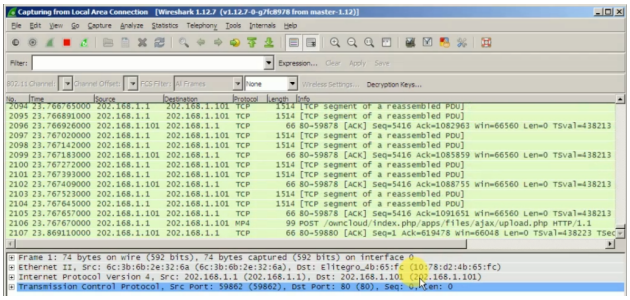


FIGURE 4. MONITORING NETWORK TRAFFIC

The monitoring process gets some suspicious activity from the actors, where there are uploading, downloading, and sending activities to each device, and then the captures are stored with the name Network Traffic Server. pcap, then stored on the server device in the C:\Users\Administator\Pictures directory.

4.2 Examination

The examination process found several perpetrators' activities on Wireshark. The first activity was obtained by the first perpetrator logging in to OwnCloud using an Android 12 operating system smartphone using Google Chrome with the username udin and the password udin, shown in Figure 5 below.

```
Host: 202.168.1.101
Connection: keep-alive
Content-Length: 61
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://202.168.1.101
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Linux; Android 12; 21061110AG) AppleWebKit/537.36 (KHTML, like
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
signed-exchange;v=b3;q=0.9
Referer: http://202.168.1.101/owncloud/
Accept-Encoding: gzip, deflate
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: 5628b95ebbba2=kodt98jire6jldsp4spdrc02c1

user=udin&password=udin&password-clone=udin&timezone-offset=7HTTP/1.1 302 Found
```

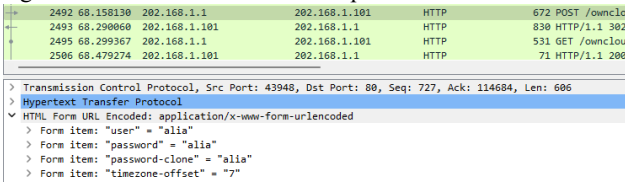
FIGURE 5. FIRST OFFENDER LOGGED IN

After that, the first actor uploaded three files, namely New Service Innovation.docx, Advertising Pamphlets.jpg, and New Services.mp4 on the owncloud server 202.168.1.101, after which they distributed the files to the next actor with user aliases. It is shown in Figure 6 below.

```
[{"status":"success","mime":"application\/msword","size":618229,"id":1205,"name":"Inovasi Pelayanan
Terbaru.docx","uploadMaxFilesize":536870912,"maxHumanFilesize":"512 MB"}]GET /owncloud/index.php/apps/files/ajax/

[{"status":"success","mime":"image\/jpeg","size":60511,"id":1204,"name":"Pamflete iklan.jpg","uploadMaxFilesize":
536870912,"maxHumanFilesize":"512 MB"}]GET /owncloud/index.php/apps/files/ajax/mimeicon.php?mime=image%2Fjpeg HTTP/1.1
Host: 202.168.1.101

[{"status":"success","mime":"video\/mp4","size":1089856,"id":1206,"name":"Inovasi Pelayanan Baru.mp4","uploadMaxFilesize":
536870912,"maxHumanFilesize":"512 MB"}]

action=share&itemType=file&itemSource=1204&shareType=0&shareWith=alia&permissions=17HTTP/1.1 200 OK
```

FIGURE 6. UPLOAD AND SHARE FILE

The next process is that there is an activity from the second perpetrator, the perpetrator uses an Acer E5-476g laptop with the Linux Ubuntu 20.04 operating system, namely logging in to the owncloud site that is the same as the first perpetrator, shown in Figure 7 with the username alia and password alia.



```
2492 68.158130  202.168.1.1      202.168.1.101    HTTP    672 POST /owncl
2493 68.290060  202.168.1.101    202.168.1.1      HTTP    830 HTTP/1.1 302
2495 68.299367  202.168.1.1      202.168.1.101    HTTP    531 GET /ownclou
2506 68.479274  202.168.1.101    202.168.1.1      HTTP     71 HTTP/1.1 200

> Transmission Control Protocol, Src Port: 43948, Dst Port: 80, Seq: 727, Ack: 114684, Len: 606
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "user" = "alia"
  > Form item: "password" = "alia"
  > Form item: "password-clone" = "alia"
  > Form item: "timezone-offset" = "7"
```

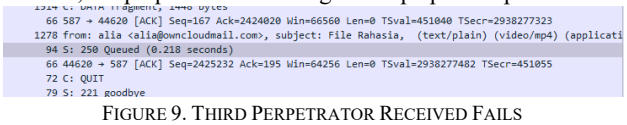
FIGURE 7. THIRD PERPETRATOR LOGIN

After logging in, the perpetrator then downloaded the file shared by the first perpetrator and immediately sent it via email Thunderbird, the activity is shown in Figure 8. The contents of the email are with the subject "secret files" and the contents of the email are "Sorry, new contact again, along with a confidential file that I promised regarding innovation from our company" was sent to komar@owncloudmail.com, and the email came from alia@owncloudmail.com in that email included three files shared by the second actor.

```
318 POST /order.php HTTP/1.1
633 GET /owncloud/index.php/apps/files/ajax/download.php?files=Inovasi%20Pelayanan%20Baru.mp4&dir=%2
 60 HTTP/1.1 200 OK
314 POST /diff.php HTTP/1.1
386
210 HTTP/1.1 200 OK
637 GET /owncloud/index.php/apps/files/ajax/download.php?files=Inovasi%20Pelayanan%20Terbaru.docx&di
3895 HTTP/1.1 200 OK  (application/msword)
623 GET /owncloud/index.php/apps/files/ajax/download.php?files=Pamflete%20iklan.jpg&dir=%2FShared Ht
3233 HTTP/1.1 200 OK  (JPEG JFIF image)

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
 Thunderbird/91.11.0
Content-Language: en-US
To: komar@owncloudmail.com
From: alia <alia@owncloudmail.com>
Subject: File Rahasia

This is a multi-part message in MIME format.
--------------NQ9iJ4MVS1kbE2mebiWJwfKD
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit

Mohon maaf baru menghubungi lagi, berikut file rahasia yang saya
janjikan mengenai inovasi dari perusahaan kami

--------------NQ9iJ4MVS1kbE2mebiWJwfKD
Content-Type: video/mp4; name="Inovasi Pelayanan Baru.mp4"
Content-Disposition: attachment; filename="Inovasi Pelayanan Baru.mp4"
Content-Transfer-Encoding: base64
```

FIGURE 8. DOWNLOAD AND SEND E-MAIL

After the second actor managed to send files to the third actor, in the packet it was found that the third actor had managed to receive files from Thunderbird, the activity is shown in Figure 9 below, the perpetrator was using a Compaq desktop.



```
 66 587 → 44620 [ACK] Seq=167 Ack=2424020 Win=66560 Len=0 TSval=451040 TSecr=2938277323
1278 from: alia <alia@owncloudmail.com>, subject: File Rahasia,  (text/plain) (video/mp4) (applicati
 94 S: 250 Queued (0.218 seconds)
 66 44620 → 587 [ACK] Seq=2425232 Ack=195 Win=64256 Len=0 TSval=2938277482 TSecr=451055
 72 C: QUIT
 79 S: 221 goodbye
```

FIGURE 9. THIRD PERPETRATOR RECEIVED FAILS

then next is that the file is sent back using Mozilla Thunderbird to the fourth actor with the contents of the email with the subject "Confidential File" and the contents of the email "The following is a secret file that the Gojek company will come, the recipient of the email is aay@kita.com and the sender of the email is komar @owncloudmail.com, the same as the perpetrator's previous email including the same three file attachments as the previous perpetrator.

```
To: aay@kita.com
From: komar <komar@owncloudmail.com>
Subject: File Rahasia
Message-ID: <63648601.9020605@owncloudmail.com>
Date: Fri, 4 Nov 2022 10:24:49 +0700
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:38.0) Gecko/20100101
 Thunderbird/38.5.0
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="------------080108020208030606050202"

This is a multi-part message in MIME format.
--------------080108020208030606050202
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 7bit

Berikut file rahasia yang perusaan jojek akan datang

--------------080108020208030606050202
Content-Type: video/mp4;
 name="Inovasi Pelayanan Baru.mp4"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="Inovasi Pelayanan Baru.mp4"
```

FIGURE 10. EMAIL EVIDENCE THIRD PERPETRATOR

The next activity found was that the fourth perpetrator managed to get the email and then downloaded it. After that the perpetrator then logged in to owncloud with user away and password aay and uploaded the three files to share them with the fifth perpetrator, then after that the perpetrator shared the file that was uploaded to the next actor with user Malik, evidence of this activity is in Figure 11 below. The perpetrator was using a Samsung laptop device.

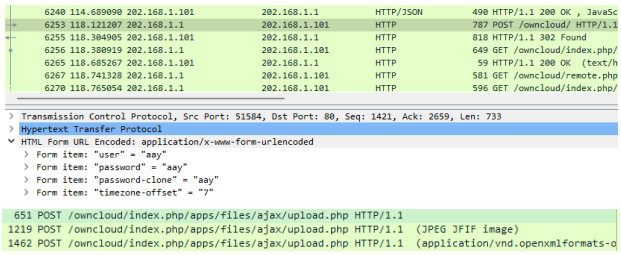


FIGURE 11. FOURTH PERPETRATOR ACTIVITY

After that there was activity from the fifth perpetrator where the perpetrator was caught logging in to their own cloud and then downloading the files shared by the fourth perpetrator. This activity is shown in Figure 12 below. The perpetrator uses a smartphone with the Poco M3 Pro type.

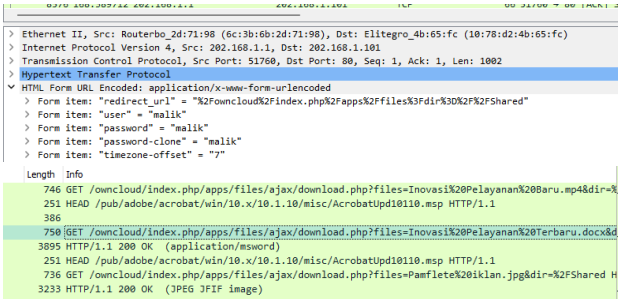


FIGURE 12. FIFTH PERPETRATOR ACTIVITY

After finding several activities from the perpetrators through Wireshark tools, the next step was to conduct a search regarding digital evidence on each device. Digital evidence was found in Table IV.

TABLE 4. DIGITAL EVIDENCE FOUND

Device	Directory
First offender	*Internal\Movies\Anime]Secret*
Second offender	*Home/Download*
Third offender	*C:\Users\Compaq\Pictures*
Fourth offender	*C:\Users\Komar\Pictures*
Five offender	*Internal\download*
Server offender 1	*C:\xampp\htdocs\owncloud\data\udin\files*
Server offender 3	*C:\xampp\htdocs\owncloud\data\aay\files*
Network (Layer 5)	*E:\Penelitian Skripsi\Tools Penelitian\NetworkMiner_2-7-3\AssembledFiles\202.168.1.101\TCP-143*

Acquisition is carried out on each device by imaging/cloning on the Windows and Ubuntu operating systems. The imaging process is carried out using folder2iso, while on the Android operating system using Isocraft, the process for one of the acquisitions is shown in Figures 13 and 14 below.

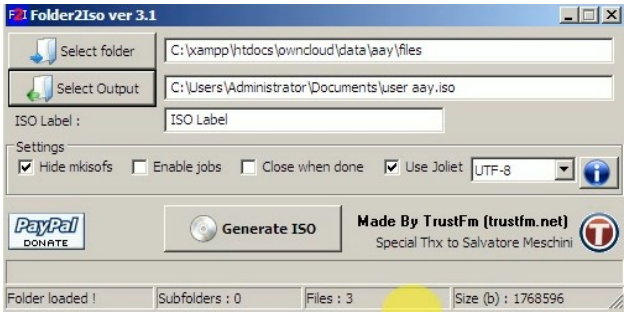


FIGURE 13. IMAGING ON WINDOWS AND UBUNTU

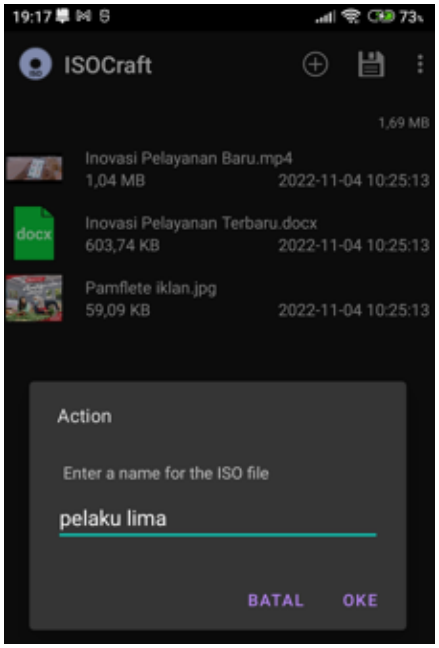


FIGURE 14. IMAGING PROCESSING ON ANDROID

Imaging was carried out on the five perpetrator devices, on the server side, as well as on the network (layer 5). The iso results obtained from each device are shown in Table V below.

TABLE 5. DIRECTORY OF DIGITAL EVIDENCE

Device	Directory	Iso Name
First offender	*Internal\Movies\Anime]Secret*	*Secret.iso*
Second offender	*Home/Download*	*Download.iso*
Third offender	*C:\Users\Compaq\Pictures*	*Pictures.iso*
Fourth offender	*C:\Users\Komar\Pictures*	*Offender4.iso*
Five offender	*Internal\download*	*Offender5.iso*
Server offender 1	*C:\xampp\htdocs\owncloud\data\udin\files*	*User udin.iso*
Server offender 3	*C:\xampp\htdocs\owncloud\data\aay\files*	*User aay.iso*
Network (Layer 5)	*E:\Penelitian Skripsi\Tools Penelitian\NetworkMiner_2-7-3\AssembledFiles\202.168.1.101\TCP-143*	*Owncloud files.iso*

4.3 Analysis

Next is to carry out an analysis of the digital evidence after obtaining the following, the results of the data integrity obtained are in the table below VI below, checking the hash value on the Windows and Ubuntu operating systems using existing open-source tools, namely hashmyfile while checking on the Android operating system using hash checker.

TABLE 6. ANALYSIS OF DATA INTEGRITY

Device	Hash Result Before Acquisition	Hash Result After Acquisition	Inf.
Smartphone POCO X3 GT	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90 AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	Same
Laptop Acer E5-476G Linux Ubuntu 20.04	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	Same
Desktop Compaq Presario V3500	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	Sama
Server H61H2-M6	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	Sama
Laptop Samsung NP355e4x	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	Sama
Smartphone POCO M3 PRO	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	sama
Layer 5	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	File : Inovasi Pelayanan Baru.mp4 CAA4CB92BF35D1CFDA786C09401D63E1(MD5)C872E7AE6C4301060D0D 7E4D8721C2270CF3A0C90AA512EA194CBFBF50760FC2(SHA256) File : Inovasi Pelayanan Terbaru.docx 7586B4610341328097F452B7D1DAFD34(MD5)8EF91F2087B827FB35F697 E2715OA8E9C686A00EFE3340DDD5D952E4172772E7(SHA256) File : Pamflete iklan.jpg F4F82FDB682E225D018DD87710338533(MD5)E2EA44DFD0C46EE6F79E5 E9413967099C3AE3D3523041BD5EE4CF8AD70B49E69(SHA256)	sama

Based on Table 6, data integrity was obtained from the three digital evidence files for each device, both before and after the acquisition.

4.4 Reporting and Documentation

The final stage of the investigation using the DFIF method is reporting and documentation. Based on the investigation, there are several suspicious activities from several company staff and from other users, which include uploading, sharing, and downloading confidential files that should not be shared. The digital evidence that has been obtained is checked for the integrity of the data, along with the results of the test.

Based on Table 6, the conclusion of testing the integrity of digital evidence on owncloud service data capture on three digital evidence that has been found on each perpetrator's device according to the stages that have been carried out, data integrity both before acquisition and after acquisition hash value displayed is the same value.

5. CONCLUSIONS

The process of acquiring one's own cloud computing uses the stages of the DFIF (Digital Forensics Investigation Framework) framework, and these stages consist of collection, examination, analysis, reporting, and documentation, which should not be shared. The process

of testing the integrity of the data captured on this private cloud service has the result that there are no changes either before the acquisition or after the acquisition is carried out. The test is carried out using existing tools, and the tools are HashMyFile on windows and on Android using HashChechker. Testing is carried out by comparing the hash value of each digital evidence.

REFERENCES

[1] Q. Covert, D. Steinhagen, M. Francis, and K. Streff, "Towards a Triad for Data Privacy," in *Hawaii International Conference on System Sciences*, 2020. DOI: 10.24251/HICSS.2020.535

[2] M. F. Panende, I. Riadi, and Y. Prayudi, "Konsep Attribute Based Access Control (ABAC) Pada Lemari Penyimpanan Bukti Digital (LPBD)," *JURNAL TEKNIK INFORMATIKA*, vol. 11, no. 1, pp. 85–94, May 2018. DOI: 10.15408/jti.v11i1.7220

[3] Amin Aenurahman Ali and Niken Dwi Wahyu Cahyani, "Digital Forensic Analysis on iDevice: Jailbreak iOS 12.1.1 as a Case Study," Telkom Univesity, Bandung, 2019.

[4] L. Singh and N. Dutta, "Routing Protocols for CRAHN: A Comparative Evaluation," 2020, pp. 3–11. DOI: 10.1007/978-981-15-1624-5_1

[5] M. A. Adam, N. Widiyasono, and H. Mubarok, "Analisis Data Digital Evidence pada Layanan Voice Over Internet Protocol (VoIP)," *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, vol. 2, no. 2, Nov. 2016. DOI: 10.26418/jp.v2i2.17578

[6] E. Chintia, R. Nadiah, H. N. Ramadhani, Z. F. Haedar, A. Febriansyah, and M. Sc. E. N. A. Rakhmawati S.Kom., "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya," *Journal of Information Engineering and Educational Technology*, vol. 2, no. 2, p. 65, Feb. 2019. DOI: 10.26740/jieet.v2n2.p65-69

[7] Y. | Setya and A. Suganda, "Design of Digital Evidence Collection Framework in Social Media Using SNI 27037:2014," 2022.

[8] S. Madiyanto, H. Mubarok, and N. Widiyasono, "Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS," *Jurnal Rekayasa Sistem & Industri (JRSI)*, vol. 4, no. 01, Sep. 2017. DOI: 10.25124/jrsi.v4i01.149

[9] I. F. Editia Kurdiat, N. Widiyasono, and H. Mubarok, "Analisis Proses Investigasi Dekstop PC Yang Terhubung Layanan Private Cloud," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 2, no. 2, Aug. 2016. DOI: 10.28932/jutisi.v2i2.463

[10] N. Widiyasono, I. Riadi, and A. Luthfi, "Penerapan Metode ADAM Pada Proses Investigasi Layanan Private Cloud Computing," *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, vol. 2, no. 1, Jun. 2016. DOI: 10.26418/jp.v2i1.15501

[11] D. Sudyana, N. Lizarti, and E. Erlin, "Forensic Investigation Framework on Server Side of Private Cloud Computing," *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, p. 181, Dec. 2019. DOI: 10.24843/lkjiti.2019.v10.i03.p06

AUTHORS

Arif Maulana Komarudin
Graduated from the Department of Informatics, Faculty of Engineering, Siliwangi University, Indonesia.

Nur Widiyasono
Lecturer in Department of Informatics, Faculty of Engineering, Siliwangi University, Indonesia.

Aldy Putra Aldya
Lecturer in Department of Informatics, Faculty of Engineering, Siliwangi University, Indonesia.

Randi Rizal
Lecturer in Department of Informatics, Faculty of Engineering, Siliwangi University, Indonesia.