Cloud Based Drive Forensic and DDoS Analysis on Seafile as Case Study

R B Bahaweres[1], N B Santoso[2], A S Ningsih[3],

[1,2,3]Electrical Engineering Dept., Universitas Mercu Buana, Jakarta, Indonesia
[1]Informatics Dept., Faculty of Science & Tech., UIN Jakarta, Indonesia

Email: [1]rizalbroer@ieee.org, [2]benisantoso72@gmail.com, [3]sn.anggun@yahoo.com

Abstract. The rapid development of Internet due to increasing data rates through both broadband cable networks and 4G wireless mobile, make everyone easily connected to the internet. Storages as Services (StaaS) is more popular and many users want to store their data in one place so that whenever they need they can easily access anywhere, any place and anytime in the cloud. The use of the service makes it vulnerable to use by someone to commit a crime or can do Denial of Service (DoS) on cloud storage services. The criminals can use the cloud storage services to store, upload and download illegal file or document to the cloud storage. In this study, we try to implement a private cloud storage using Seafile on Raspberry Pi and perform simulations in Local Area Network and Wi-Fi environment to analyze forensically to discover or open a criminal act can be traced and proved forensically. Also, we can identify, collect and analyze the artifact of server and client, such as a registry of the desktop client, the file system, the log of seafile, the cache of the browser, and database forensic.

1. Introduction

Cloud computing is an emerging storage service in IT because with cloud computing we can increase storage capacity without the cost of buying new infrastructure, training new personnel, or licensing new software[1]. Service providers usually provide free services up to a certain capacity before required to pay[2].Although with all the convenience provided, there are still many companies are hesitant and cautious storing their data to public cloud storage services[3].

Based on Gartner [4] there are seven security issues for cloud computing. Due to the above considerations, we chose to use personal cloud storage seafile. Seafile is hosting file system software. Files are stored on a central server and can be synchronized with a personal computer and a mobile device through a client seafile. Files can also be accessed with server web interface.

Seafile function is similar to other popular services like ownCloud, Dropbox and Google Drive, but seafile is a free and open source, so users can host their own servers without limits imposed on the storage space or client connections, it only depends on the size of the storages[5]. In order for these technological advances, we chose the Raspberry Pi[6], [7] as a model of a private cloud storage infrastructure based on Seafile.

There are 5 (five) component of Seafile [16]. They consist of Seahub (django) as the web frontend, seafile server (seaf-server) as data service daemon, handles raw file upload, download and synchronization, ccnet server (ccnet-server) as RPC service daemon to enable communication among the other components, FileServer**:** handles raw file upload/download functions for Seahub,

and Controller**:** monitors ccnet and Seafile daemons.The architecture of Seafile application can be seen as the following figure 1.

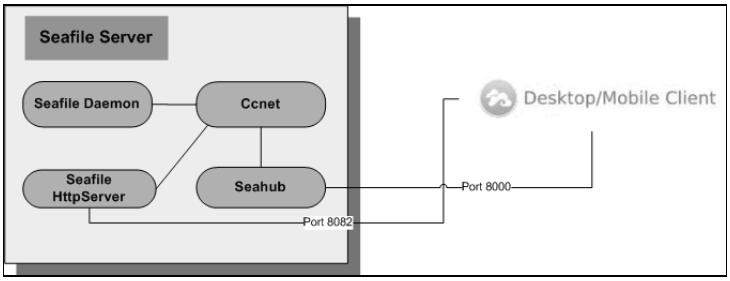

Figure 1. The Architecture of Seafile Application.

The framework of computer forensics used in this paper consists of identification and preservation, collection, examination and analysis, reporting and presentation[1], [8–10]. The diagram of framework forensics can be seen in figure 2.

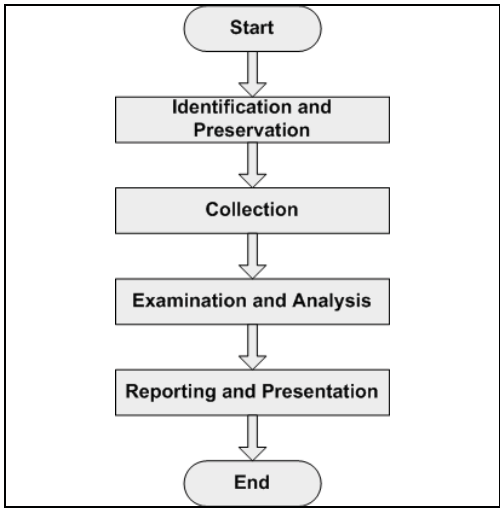

Figure 2. The Framework of Computer Forensics.

The digital artifact reference as the term is widely used in computer forensics. Content types of digital artifact include text, audio, video, image, animation or a combination. The digital artifact result from hardware malfunction, software malfunction, compression, aliasing, rolling shutter and error diffusion.[17]

Denial of Service is one type of attack on Server or Computer that makes the target crash or hangs so that the resources of the server cannot be accessed by the end user. The Distributed Denial of Services (DDoS) is a coordinated attack on the availability of services of a given target system that is launched indirectly through many compromised computing systems.

The goal of the DoS/DDoS attack : bandwidth depletion, cut off the connection between servers, prevent the victim using the services of system or resources depletion and devastate the system[11], [12]. From the security approach, the internal user can do DoS attack from internal local area network or Wi-Fi Environment. The schema of DDoS as following figure 3.

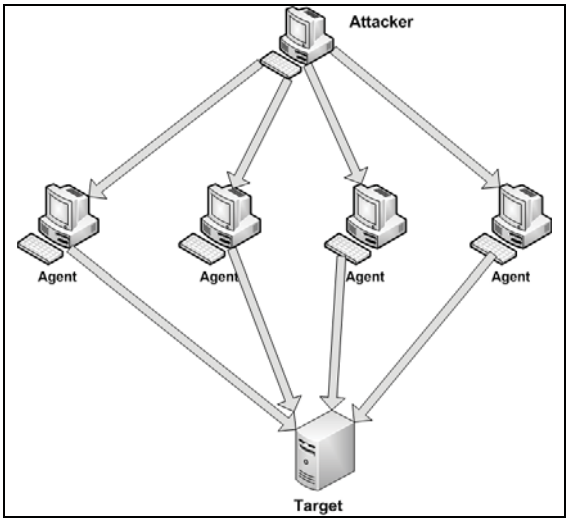

Figure 3. The Schema of DDoS Attack.

2. Related Works

Ben Martini, et. al focus on upon client and server artifacts on ownCloud cloud storage[1]. Darren Quick, et. al, discuss data remnant on end user devices using Dropbox in Windows 7 and Apple iPhone[9] and Google Drive Analysis[8]. Chen Long and Zhang Qing proposes a method to investigate and analyze the artifacts for reconstructing the event of user's activities on 360 Cloud service and Baidu Cloud service[13]. Kayvan Atefi, et. al, try to find a number of artifacts and make some measurements of CPU load on Seafile cloud storage[5]. Rizal BroerBahaweres, et. al, focus on denial of service on ownCloud personal storage[12]. Our research focuses on client and server artifact and DoS analysis on Seafile cloud storage.

Table 1. Matrix Related Research.

No	Journal Title	Author	Server Artifact	Client Artifact	Cloud Storage	DoS
1	Forensic Analysis to China's Cloud Storage Services	Chen Long, et.al		√	√	
2	Cloud storage forensics: ownCloud as a case study	Ben Martini, et.al	√	√	√	
3	Dropbox analysis: Data remnants on user machines	Darren Quick, et.al		√	√	
4	Google Drive: Forensic Analysis of Cloud Storage Data Remnants	Darren Quick, et.al		√	√	
5	Building a Private Cloud Computing and the analysis against DoS (Denial of Service) attacks: a Case study at SMKN 6 Jakarta	R.B. Bahaweres, et.al		√	√	√
6	Cloud Based Drive Forensic & DOS Analysis on Seafile as a Case Study	N. B. Santoso, et.al	√	√	√	√

3. Methodology

This study tries to install and implement a personal cloud-based storage based on Seafile. Installation and configuration Seafile on Raspberry Pi[14]. After the system is built, we install Seafile client on a computer running windows 7 and Android mobile phone.[15] The framework of research methodology as seen the following picture:

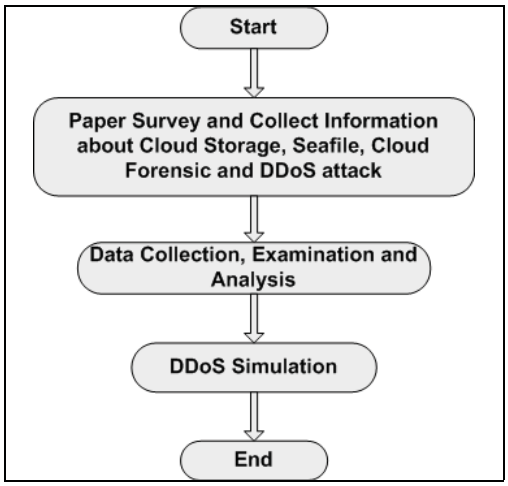

Figure 4. The Framework of Research Methodology.

The identification, preservation, and collection were performed as follow:

- The artifact in a browser at windows client.
- The artifact in seafile windows client apps and seafile android client's apps.
- Collectlog on Seafile Personal Cloud Storage such as access log, Syslog, etc.
- Collect database and registry artifact at Seafile and Windows 7 desktop client.
- Throughput with DDoS and without DDoS simulation on seafile cloud storage with 5PC sending packets simultaneously.

The cloud storage specification:

- Raspberry Pi 2, 900MHz quad-core ARM Cortex-A7 CPU
- Memory 1GB
- External SanDisk 64GB
- Network 10/100 Mbps
- Operating System : Raspbian

The cloud storage system consists of 1 (one) Seafile app and 1 (one) external disk attach to Raspberry Pi. And the simulation of DoS and client artifact analysis, we use 2 (two) notebook, 2 (two) server and 2 Android Smartphone. The architecture of Seafile cloud storage can be seen at following figure 5:

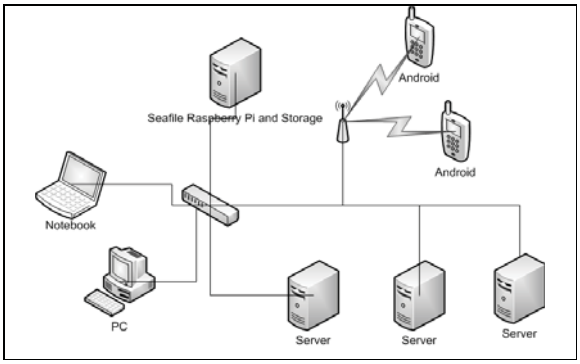

Figure 5. The Architecture of Private Seafile Cloud Storage.

4. Result and analysis

We try to present the overview of Seafile filesystem and configuration. To know depth forensic of Seafile, we must know all about Seafile architecture, from the filesystem, log file, database and configuration file. Here the overview about file system of seafile application [16]:

a. File system of Seafile server: /home/pi, seafile-server-6.0.3, seafile-data (seafile configuration and data), seahub-data (seahub data), ccnet (ccnet configuration and data), seahub.db (sqlite3 database used by seahub), seahub_settings.py (optional config file for seahub).
b. Configuration file of seafile server: ccnet.conf, seafile.conf, seafdav.conf, seahub_settings.py, and seafevents.conf (professional edition only).
c. Log files of seafile server: seafile.log (logs of Seafile server), controller.log (logs of Controller), seahub_django_request.log (logs of Seahub), seahub.log (logs from Django framework and emails sending), and ccnet log: logs/ccnet.log (logs for internal RPC, not useful).
d. Firewall setting:
   By default, open 2 ports, 8000 and 8082, in the firewall settings.
   If run Seafile behind Nginx/Apache with HTTPS, only need to open ports 443.
e. Security of seafile server:
   Seafile provides a feature called the encrypted library to protect the privacy. The file encryption/decryption is performed on client-side when using the desktop client for file synchronization. The password of an encrypted library is not stored on the server. Even the system admin of the server can't view the file contents, however they can view the metadata which is currently not encrypted. The metadata includes the complete list of directory and file names, every files size, the history of editors, when, and what byte ranges were altered.
   After we know filesystem and architecture of Seafile, we can separate forensic into some of forensic methods, as follow:
f. File system and Registry Forensic
   In Seafile desktop client, we can find the file system and registry artifact in a certain folder. We can see the following figure.

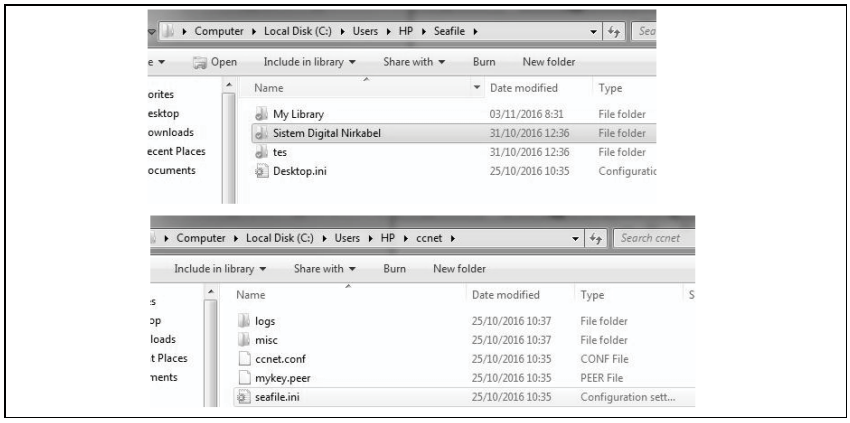

Figure 6. The Artifact of Seafile Desktop Client.

Figure 7. The Artifact of Seafile Android Client.

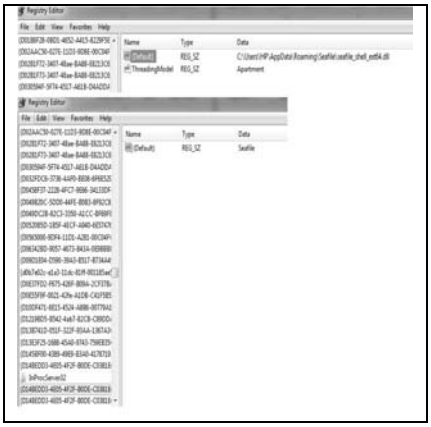

Figure 8. Registry Artifact of Seafile Desktop Client.

g. Database Forensic
With DB Browser for SQLite, we can view and display artifact of user data, like a platform that used by the user, device name, last accessed, the last login, created by, etc

Figure 9. DB Browser for SQLite.

h. Browser Forensics
With Chrome Forensic tools, we can capture and analyze data that store the following SQLite Files in google chrome browser:

- History

- Cookies
- Web Logins
- Archived History (Web History and search terms)
- Bookmarks
- File locations : C:\Users\USERNAME\AppData\Local\Google\Chrome\User Data\Default

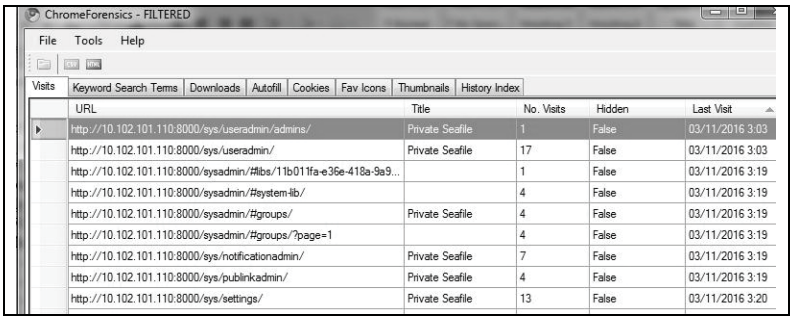

Figure 10. Chrome Forensics Tools.

i. Throughput calculation with or without DDoS attack Simulation
The researchers use Wireshark tool to see throughput when uploading files to Seafile Cloud Storage. The researchers used three scenarios to analyze throughput. The uploaded size file has 60.9MB, we make 3 scenarios of DDoS simulation, the first scenario, the file is uploaded without DDoS attack and throughput is captured with Wireshark tool. The second scenario, the file is uploaded simultaneously with DDoS attack by 5 computers with 30000 bytes, the third scenario, the file is uploaded simultaneously with DDoS attackby 5 computers with 50000 bytes.The result of throughput rate as seen by the following table 2.

Tabel 2. Throughput Calculation without DDoS and with DDoS Simulation.

No	Trial	Throughput without DDoS (MBit/s)	Throughput DDoS 30000 bytes (Mbit/s)	Throughput DDoS 50000 bytes(Mbit/s)
1	N1	9.784	7.472	4.615
2	N2	5.486	4.344	2.634
3	N3	10.842	8.425	8.084
4	N4	6.355	8.249	9.166
5	N5	8.455	9.024	9.188
6	N6	8.487	6.602	6.225
7	N7	11.202	8.618	8.013
8	N8	7.486	6.137	5.967
9	N9	11.174	6.014	6.027
10	N10	8.972	7.151	7.229
Average		8.8243	7.2036	6.7148

With DoS attacks influence the reduction in throughput rate, though the cloud services still able to running well, but this should be a concern so it does not become an obstacle later.The throughput rate has reduced to 81.63% with DDoS (30000 bytes), and 76.09% with DDoS (50000 bytes).

5. Conclusion and Future Works

This research demonstrated that private cloud Seafile provides a significant number of useful artifacts for forensic investigators. And provides a discussion on private cloud forensics from both client and server artifact, database forensics, and simulation of DDoS attack against private cloud services itself. The Seafile has a default security feature such as the encrypted library.

For future works, we need to protecting and securing the Seafile cloud storage from DDoS with making clustering Seafile applications, both in the application, database, Memcached enabled and storage clustering. And protect the cloud storage with firewall and bandwidth management.

Acknowledgment

Many thanks to all colleagues and family to support us to finish this paper completely.

References

[1] Martini B and Choo K K R 2013 Cloud storage forensics: ownCloud as a case study *Digital Investigation* vol **10** no 4 pp 287–299
[2] Drago I, Bocchi E, Mellia M, Slatman H and Pras A 2013 Benchmarking personal cloud storage *in Proceedings of the 2013 conference on Internet measurement conference* pp 205–212
[3] So K 2011 Cloud computing security issues and challenges *International Journal of Computer Networks* vol **3** no 5
[4] Singh V 2014 Well-known Gartner's Seven Security Issues Which Cloud Clients Should Advert
[5] Atefi K, Yahya S and Atefi A 2014 A survey on digital forensics investigation of Seafile as a cloud storage *International Journal of Engineering Research And Management (IJERM)* vol **1**
[6] Maksimovi M, Vujovi V, Davidovi N, Milosevi V and Perisi B 2014 Raspberry Pi as Internet of things hardware: performances and constraints *Design issues* vol **3** p 8
[7] Severance C 2013 Eben upton: Raspberry pi Computer vol **46** no 10 pp 14–16
[8] Quick D and Choo K K R 2014 Google drive: forensic analysis of data remnants *Journal of Network and Computer Application*s vol **40** pp 179–193
[9] Quick D and Choo K K R 2013 Dropbox analysis: Data remnants on user machines *Digital Investigation* vol **10** no 1 pp 3–18
[10] Roussev V, Barreto A and Ahmed I 2016 Forensic acquisition of cloud drives *arXiv preprint arXiv:1603.06542*
[11] Chauhan K and Prasad V 2015 Distributed Denial of Service (DDoS) Attack Techniques and Prevention on Cloud Environment *International Journal of Innovations & Advancement in Computer Science* pp 210–215
[12] Bahaweres R B, Syarif J and Alaydrus M 2016 Building a Private Cloud Computing and the analysis against DoS (Denial of Service) attacks: Case study at SMKN 6 Jakarta The 4th International Conference on Information Technology for Cyber and IT Service Management
[13] Long C and Qing Z 2015 Forensic Analysis to China's Cloud Storage Services *International Journal of Machine Learning and Computing* vol **5** no 6 p 467
[14] Chung H, Park J, Lee S and Kang C 2012 Digital forensic investigation of cloud storage services *Digital investigation* vol **9** no 2 pp 81–95
[15] Gracia-Tinedo R, Artigas M S, Moreno-Martinez A, Cotes C and Lopez P G 2013 Actively measuring personal cloud storage *Proceedings of the Cloud* pp 301–308
[16] https://manual.seafile.com
[17] https://en.wikipedia.org/wiki/Digital_artifact