JURNAL MEDIA INFORMATIKA BUDIDARMA, Vol 3, No 3, Juli 2019
ISSN 2614-5278 (media cetak)
ISSN 2548-8368 (media online)
Hal 217-224 | DOI: 10.30865/mib.v3i3.1193

Simulasi Analisis Bukti Digital Pada Layanan *Cloud Computing* Menggunakan Metode NIST 800-86

Irfan Helmi, Nur Widiyasono, Rohmat Gunawan*

Fakultas Teknik, Program Studi Informatika, Universitas Siliwangi, Tasikmalaya, Indonesia
Email: [1]irfanhelmi21@gmail.com, [2]nur.widiyasono@unsil.ac.id, [3*]rohmatgunawan@unsil.ac.id

Abstrak

Kemudahan dan fleksibilitas penyimpanan data berbasis *cloud* telah mendorong peningkatan jumlah penggunaan layanan *cloud*. Bertambahnya jumlah penggunaan layanan *cloud* juga berpotensi meningkatkan jumlah tindakan kriminal berbasis digital terutama berhubungan dengan penyalahgunaan fasilitas pada layanan *cloud*. Fitur layanan *cloud* yang dirancang untuk menyimpan data guna mendukung kelancaran proses bisnis, dapat disalahdigunakan oleh pelaku kriminal untuk menyimpan data hasil kejahatan. Diperolehnya bukti digital yang akurat, merupakan salah satu cara menangkap para pelaku kejahatan digital, yang selanjutnya dapat dipergunakan sebagai bukti pendukung di persidangan. Penelitian ini bertujuan untuk melakukan simulasi analisis terhadap bukti digital dari suatu layanan *cloud*. Proses analisis menggunakan metode NIST 800-86 dilakukan pada bukti digital dari 5 skenario yang dipersiapkan sebelumnya berkaitan dengan penggunaan fitur layanan *cloud* yang berpotensi disalahgunakan. Teknik akuisisi data menggunakan metode *live acquisition* dan *physical imaging* untuk mendapatkan bukti digital. Hasil percobaan pada penelitian menunjukan bahwa, setelah dilakukan skenario 1 dan skenario 3, berhasil didapatkan informasi nama *file* dan direktori *path* yang diunduh oleh *client 1* dan *client 2* dilengkapi dengan informasi *ip address*, *mac address*, *username*, *password* dan *timestamp*. Setelah dilakukan skenario 2, berhasil didapatkan bukti digital berupa informasi nama dan lokasi *folder* di server *cloud*. Setelah dilakukan skenario 4, berhasil didapatkan informasi nama *file* dan *shared folder* dilengkapi dengan informasi *client* yang mendapatkan hak untuk mengakses *file* dan *folder* tersebut. Setelah dilakukan skenario 5, berhasil didapatkan informasi nama *file* dan direktori *path* file yang dihapus.

Kata Kunci: Akuisisi Data, Bukti Digital, *Cloud Computing*, NIST800-86.

Abstract

Ease and support for cloud-based data storage It has supported an increase in the number of cloud services. The increasing number of uses for cloud services also increases the number of digital-based criminal actions related to the addition of facilities to cloud services. The cloud service feature designed to store data to support the smooth running of business processes can be misused by criminal assistance to store crime data. Accurate digital evidence is one way to prove a digital crime, which can then be used as supporting evidence in the trial. This study discusses the analysis of digital evidence from a cloud service. The analysis process using the NIST 800-86 method is carried out on digital evidence from 5 previously prepared scenarios related to the use of cloud service features that use being misused. Data acquisition techniques use the method of direct acquisition and physical imaging to obtain digital evidence. The experimental results showed that after scenario 1 and scenario 3, information on the file name and directory of the paths downloaded by client 1 and client 2 were obtained with information on the IP address, mac address, user name, password and time stamp. After scenario 2, digital evidence has been obtained that contains information on the name and location of the folder on the cloud server. After scenario 4, information on the name of the file and the shared folder is successfully obtained, equipped with client information that has the right to access the files and folders. After scenario 5, information about the file name and directory of the file path is successfully obtained.

Keywords: Data Acquisition, Digital Evidence, Cloud Computing, NIST 800-86.

1. PENDAHULUAN

Layanan *cloud computing* merupakan kolaborasi pemanfaatan teknologi komputasi dan pengembangan sistem berbasis internet yang menawarkan fasilitas sumber daya tanpa perangkat tambahan, biaya yang lebih terjangkau dan penyimpanan data yang tidak terbatas. Secara umum terdapat tiga jenis layanan pada *cloud computing* yaitu: *Cloud Software as a service (SaaS)*, *Cloud Platform as a Service (PaaS)* dan *Cloud Infrastructure a Service (IaaS)*. Sedangkan *cloud computing* menurut NIST berdasarkan sifat jangakauannya terdapat empat model, yaitu: *Private Cloud*, *Public Cloud*, *Community Cloud* dan *Hybrid Cloud* [1]. Organisasi maupun perusahaan sudah banyak yang menggunakan layanan ini untuk mendukung kelancaran proses bisnis dan efisiensi penyimpanan arsip digital [2]. *Private cloud* mencakup seluruh *cloud infrastructure* termasuk sumber daya *hardware* yang dimiliki organisasi maupun perusahaan tersebut [2]. Namun, selain memiliki banyak manfaat *cloud* juga membawa dampak negatif diantaranya penyalahgunaan *cloud* untuk menyimpan data hasil kejahatan.

Merujuk masalah tersebut, maka diperlukan metode untuk menangani kasus kejahatan *cyber*, yaitu dengan menggunakan teknik akuisisi data untuk menganalisa dan mengumpulkan bukti-bukti digital dari tindak kejahatan. Penanganan kejahatan *cyber* tersebut diperlukan teknik akuisisi data, dimana teknik akusisi data dapat dilakukan secara *live system* ataupun *write-block system* [3]. Kedua teknik akuisisi data tersebut tidak hanya dilakukan pada layanan *cloud computing*, melainkan dapat dilakukan juga pada *computer client*, *server*, *laptop atau notebook* dan *smartphone* [3].

JURNAL MEDIA INFORMATIKA BUDIDARMA, Vol 3, No 3, Juli 2019
ISSN 2614-5278 (media cetak)
ISSN 2548-8368 (media online)
Hal 217-224 | DOI: 10.30865/mib.v3i3.1193

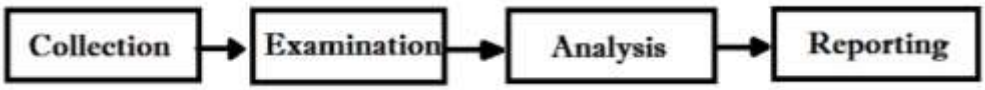
Berbagai analisis forensik digital untuk menemukan bukti dari suatu aktivitas kriminal berbasis layanan *cloud computing* pernah dilakukan dalam penelitian sebelumnya, diantaranya: menggunakan metode *The Advance Data Acquisition Model* (ADAM) [4], metode *End to End Digital Investigation* (EEDI) [5], *National Institute of Standard and Technology* (NIST) [6], *National Institute of Justice* (NIJ) [7]. Penelitian [4] berhasil menemukan lokasi *files folder data digital evidences*, *username* dan *password*, *timestamps*, *ip address* dan *mac-address*, dan kesesuaian *file-file data digital evidence* yang didapatkan pada perangkat *smartphone*, komputer *desktop* dan pada komputer *private cloud computing*. Penelitian [5] berhasil mendapatkan aktivitas yang tersimpan pada *cache browser*, *username password*, *logs chatting mIRC*, *e-mail*, *file* dalam *MS Word*. Penelitian [6] berhasil mengungkap bukti kejahatan dari lalu lintas jaringan pada layanan *ownCloud.* Penelitian [7] berhasil menerjemahkan kode-kode *hexsa* hasil akuisisi untuk menghasilkan barang bukti yang yang bisa di mengerti oleh hakim.

Penelitian ini bertujuan untuk melakukan akuisisi data bukti digital menggunakan metode NIST melalui simulasi dari beberapa skenario yang mencakup fitur *cloud* yang sering digunakan, serta skenario yang dapat menghilangkan bukti digital. Bukti digital dan perubahan yang disebabkan oleh aktivitas yang dilakukan pada skenario tersebut dianalisis dan ditampilkan ke dalam bentuk tabel. Proses analisa dilakukan untuk menyimpulkan karakteristik bukti digital dari layanan *cloud computing* yang diteliti.

2. METODE PENELITIAN

2.1 Proses Akuisisi Data

Proses akuisisi data untuk mendapatkan informasi dari bukti digital mengikuti tahapan dari metode *National Institute of Standards Technology* (NIST) [8].



Gambar 1. Tahapan Metode NIST 800-86

Berdasarkan gambar 1 hal ini dapat dijelaskan tahap akuisisi data sebagai berikut:

a. *Collection:* proses akuisisi data dilakukan dengan teknik *live acquisition* dan *imaging* pada *database server* layanan *ownCloud.*
b. *Examination*: proses pemeriksaan terhadap data barang bukti menggunakan *tool HashCalc* dan diberi *Hash Message Digest* 5 (MD5) untuk menjaga integritas data.
c. *Analysis:* Data bukti digital yang ditemukan pada tahap *examination* dianalisis untuk membuat kesimpulan dari bukti digital. File hasil *live acquisition* dan *database ownCloud* yang relevan akan dibuka dan dianalisis menggunakan *tools Wireshark*, *Network Miner* dan *Magic ISO Maker*.
d. *Reporting*: Investigator melaporkan hasil investigasi beserta bukti digital yang ditemukan. Pelaporan dalam penelitian meliputi penyajian artefak digital yang telah disimpulkan dari tahap analisis.

2.2 *Hardware* dan *Software* Yang Digunakan

Perangkat keras dan perangkat lunak yang digunakan dalam penelitian ini ditampilkan pada Tabel 1 dan Tabel 2.

Tabel 1. *Hardware* Yang Digunakan

No	Hardware	Spesifikasi	Keterangan
1	PC *Server*	Asus A455L, Windows 10 64-bit	Komputer *server*
2	PC *Client*	Toshiba Tecra Z40t, Windows 10 64-bit	Komputer *Client 1*
3	*Smartphone*	Samsung Galaxy S5 G900H	*Smartphone Client 2*

Tabel 2. *Software* Yang Digunakan

No	Software	Keterangan
1	*OwnCloud*	Layanan *Cloud* yang akan dianalisa.
2	*Apache Server*	*Server local ownCloud.*
3	*MySQL*	*Database server ownCloud.*
4	*Wireshark*	*Tool live acquisition* lalu lintas data pada layanan *ownCloud.*
5	*Network miner*	*Tool* untuk menganalisia file hasil *live acquisistion.*
6	*Magic ISO Maker*	*Tool imaging* bukti digital server *ownCloud.*
7	*HashCalc*	*Tool* untuk memeriksan nilai *hash* file bukti digital.
8	*Chrome Browser*	Browser yang digunakan *server.*

JURNAL MEDIA INFORMATIKA BUDIDARMA, Vol 3, No 3, Juli 2019
ISSN 2614-5278 (media cetak)
ISSN 2548-8368 (media online)
Hal 217-224 | DOI: 10.30865/mib.v3i3.1193

2.3 Perancangan Skenario Kasus

Skenario dibuat untuk merekontruksi aksi relevan yang mungkin pengguna lakukan dalam tindakan kejahatan *cyber* dan menyembunyikan jejaknya[2]. Pembuatan skenario dilakukan berdasarkan hasil analisa fungsionalitas layanan *cloud*. Skenario mencakup fitur-fitur layanan *cloud* yang berpotensi disalahgunakan untuk tindakan kejahatan, serta skenario yang dapat menghilangkan bukti digital.

a. Skenario 1 : *Client* Mengunduh File dari Server.
b. Skenario 2 : *Client* Membuat Folder Baru.
c. Skenario 3 : *Client* Mengunggah File.
d. Skenario 4 : *Client* Membagikan Folder/File Ke Sesama Pengguna *Cloud*.
e. Skenario 5 : *Client* Menghapus File

Skenario simulasi yang telah dibuat selanjutnya akan diterapkan pada layanan *ownCloud* yang telah disiapkan. Saat setiap skenario dijalankan, akan diteliti fitur-fitur pada aplikasi yang terkait dengan skenario, sehingga diketahui bukti digital yang masih ditinggalkan dari penggunaan fitur tersebut serta karakteristiknya. Beberapa dari skenario merupakan aktivitas yang dapat merubah dan menghilangkan bukti digital.

3. ANALISA DAN PEMBAHASAN

3.1 *Collection*

OwnCloud menyimpan berbagai data yang digunakan ketika dijalankan. Data-data tersebut tersimpan dalam *folder* khusus seperti terlihat pada tabel 3.

Tabel 3. Lokasi Bukti Digital Layanan *OwnCloud*

Bukti Digital	Lokasi
Database ownCloud	\owncloud\data
Database Server	\mysql\data\owncloud
Unggah File	\owncloud\data**user***\files
Hapus File	\owncloud\data**user***\files-trashbin\files
Data Folder	\owncloud\data**user***\files

Keterangan : user* = nama folder sesuai dengan nama pengguna

3.2 *Examination*

Proses *examination* merupakan aktivitas pemeriksaan barang bukti hasil akuisisi data sebelum barang bukti diperiksa oleh investigator. Akuisisi barang bukti dilakukan dengan melakukan pemeriksaan nilai *hash* pada *file* tersebut. Pemeriksaan nilai *hash* MD5 dilakukan dengan menggunakan *tool HashCalc*.Hasil pemeriksaan nilai Hash disajikan pada tabel 4.

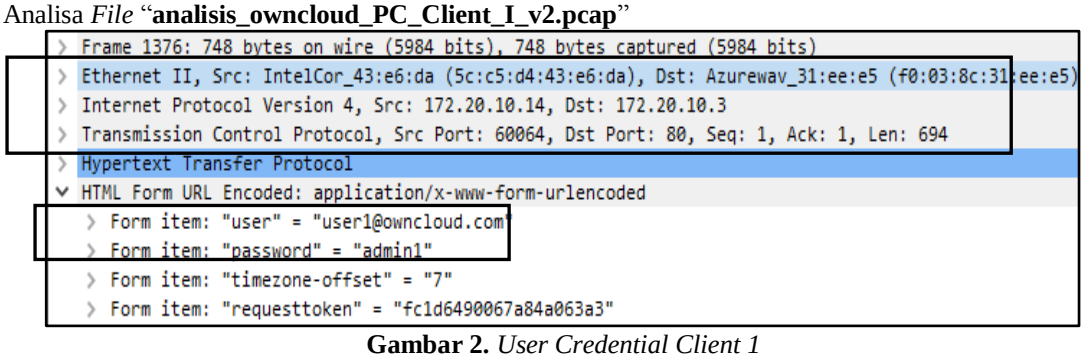
Tabel 4. Nilai *Hash* MD5 Barang Bukti

Nama File	MD5
akuisisi_dari_server_cloud.iso	e6b674731f63ea75f8ac5b 7444ae2308
analisis_owncloud_PC_Client_I_v2.pcap	50be296230d006217604bf5dca9987c8
analisis_owncloud_android_II.pcap	f4afe2ecb6d2cdaa82a79e29f76a7ad8
digital_evidence_browser_client1.iso	783169194ec60c2b1ee5c2f3f7 abd16e
browser_artefact_client2.zip	3fcf3dc8607d357b00cee3536df9f9ff

3.3 *Analysis*

Pada tahap awal, proses analisis dilakukan pada file **.pcap* hasil *live acquisistion client 1* dan *client 2* serta *file imaging database ownCloud*.

a. Analisa *File* "**analisis_owncloud_PC_Client_I_v2.pcap**"

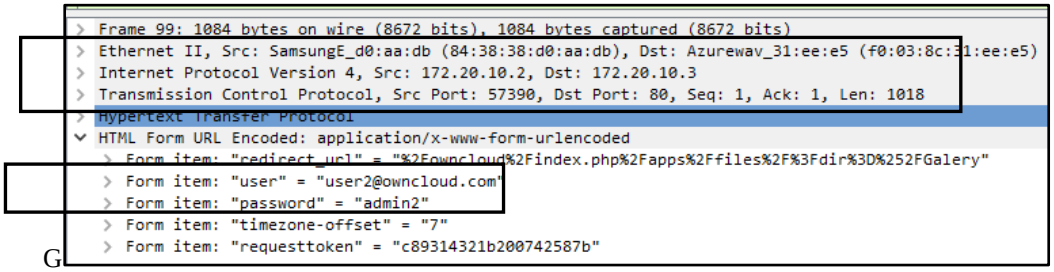


Gambar 2. *User Credential Client 1*

JURNAL MEDIA INFORMATIKA BUDIDARMA, Vol 3, No 3, Juli 2019
ISSN 2614-5278 (media cetak)
ISSN 2548-8368 (media online)
Hal 217-224 | DOI: 10.30865/mib.v3i3.1193

Gambar 2 menunjukan *client 1* melakukan login ke layanan *ownCloud* dengan menggunakan *username* "user1@owncloud.com" dan *password* "admin1". *Client 1* mengakses layanan owncloud melalui *host* dengan *ip address* 172.20.10.14 dan *mac addrees* "5c:c5:d4:43:e6:da" dengan *port* 60064.

b. Analisis File "**analisis_owncloud_android_II.pcap**"



G

Gambar 3. *User Credential Client 2*

Gambar 3 menunjukan informasi *Client 2* melalui IP address 172.20.10.2 mengakses layanan *ownCloud* menggunakan *username* "user2@owncloud.com" dan password "admin2". *Client 2* menggunakan *mac addrees* "84:38:38:d0:aa:db" dengan port 57390.

c. Analisa *Device* yang mengakses layanan *OwnCloud*

Analisa yang dilakukan juga berhasil mendapatkan informasi nama sistem operasi yang digunakan oleh setiap device yang mengakses layanan owncloud. Informasi nama sistem operasi beserta parameter lainnya yang berhasil diperoleh seletah dilakukan analisa ditampilkan pada Tabel 5.

Tabel 5. Data *Device* Yang Mengakses Layanan *ownCloud*

Data	*Server*	*Client 1*	*Client 2*
Sistem Operasi	Windows	Windows	Android
IP Address	172.20.10.3	172.20.10.14	172.20.10.2
Mac Address	F0:03:8C:31:EE:E5	5C:C5:D4:43:E6:DA	84:38:38:D0:AA:DB
Paket Dikirim	15391 paket	5762 paket	6824 paket
Paket Diterima	12397 paket	10345 paket	4463 paket

d. Analisa *Database OwnCloud*

Gambar 4. Struktur Direktori database *OwnCloud*

Lokasi database *ownCloud* dapat ditemukan pada direktori "\owncloud\data" seperti ditampilkan pada gambar 4. Direktori tersebut menyimpan *database* pengguna *ownCloud*. Berkas media yang diunggah ke - *ownCloud* seperti: dokumen, gambar, dan video disimpan pada direktori "\owncloud\data**user**\files". *File* yang dihapus berada pada direktori"\owncoud\data**user**\files-trashbin\files".

3.4 *Reporting*

Berikut laporan bukti digital yang berhasil disusun berdasarkan skenario yang telah dirancang sebelumnya dalam penggunaan fungsional layanan *owncloud*.

a. **Skenario 1** : *Client* Mengunduh File dari *Server*.

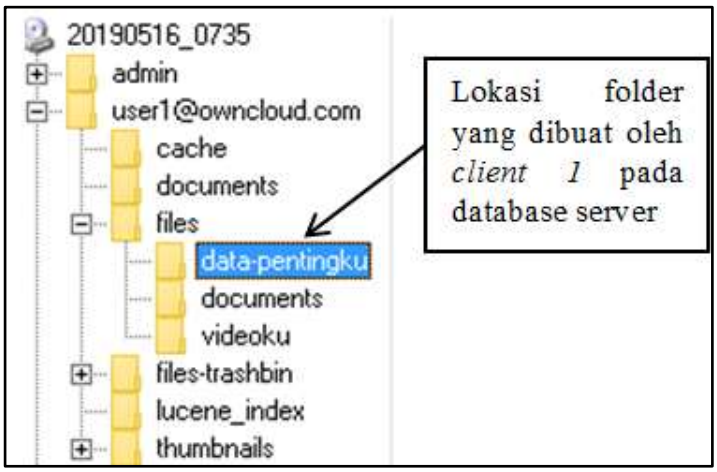
Gambar 5. Bukti Digital *File* yang diunduh

JURNAL MEDIA INFORMATIKA BUDIDARMA, Vol 3, No 3, Juli 2019
ISSN 2614-5278 (media cetak)
ISSN 2548-8368 (media online)
Hal 217-224 | DOI: 10.30865/mib.v3i3.1193

Aktivitas mengunduh *file* dari layanan *ownCloud* berhasil ditemukan file *path*-nya secara utuh menggunakan teknik *live acquisiton* pada direktori "C:\Program Files\NetworkMiner2 \AssembledFiles\172.20.10.3\TCP-80\owncloud\index.php\apps\files\ajax" seperti ditampilkan pada gambar 5. *File* yang diunduh *client 1* yaitu "BAB V HASIL DAN PEMBAHSAN.docx, magang (5).JPG, BAB IV PROFIL LOKASI MAGANG, magang (2).JPG dan DAFTAR PELAKU P.docx". *Client 2* mengunduh file magang (10).JPG, magang (9).JPG dan ANALISIS KASUS.docx. Teknik *imaging* pada *database ownCloud* tidak menemukan *log* dari skanario tersebut.

b. **Skenario 2** : *Client* Membuat Folder Baru.

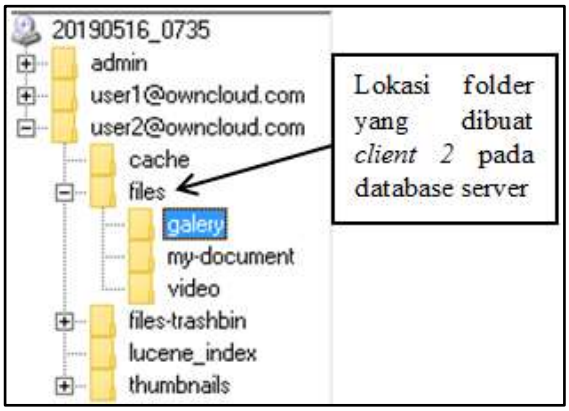
1. *Client 1* Membuat Folder Baru



Gambar 6. Folder *Client 1*

Aktivitas *client 1* membuat folder baru tersimpan pada direktori "\owncloud\data\user1 @owncloud.com\files" pada database *ownCloud* seperti terlihat pada gambar 6. *Folder* yang dibuat oleh *cient 1* pada layanan *ownCloud* yaitu folder "data pentingku, documents dan videoku".

2. *Client 2* Membuat Folder Baru

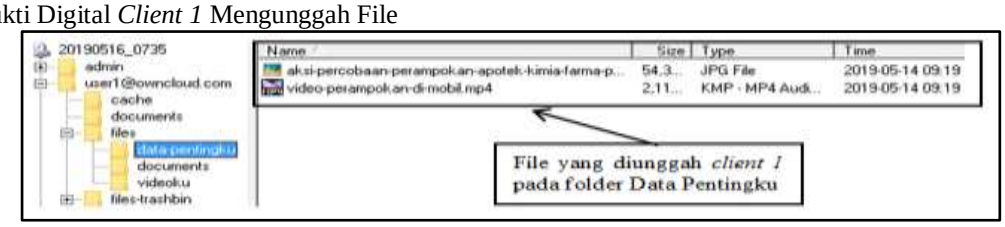


Gambar 7 Folder *Client 2*

Aktivitas *client 2* membuat folder baru tersimpan pada direktori "\owncloud\data\user2 @owncloud.com\files" pada database *ownCloud* seperti terlihat pada gambar 7. *Folder* yang dibuat oleh *cient 2* pada layanan *ownCloud* yaitu folder "galery, my-document dan video".

c. **Skenario 3 :** *Client* Mengunggah File.

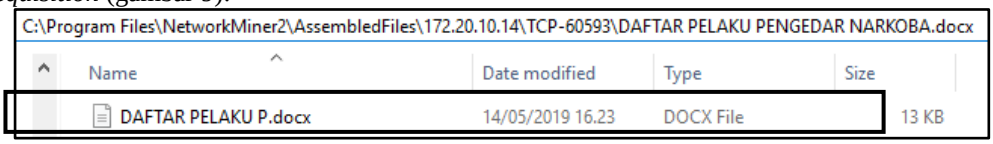
1. Bukti Digital *Client 1* Mengunggah File



Gambar 8. Bukti Digital File Yang Diunggah *Client 1*

JURNAL MEDIA INFORMATIKA BUDIDARMA, Vol 3, No 3, Juli 2019
ISSN 2614-5278 (media cetak)
ISSN 2548-8368 (media online)
Hal 217-224 | DOI: 10.30865/mib.v3i3.1193

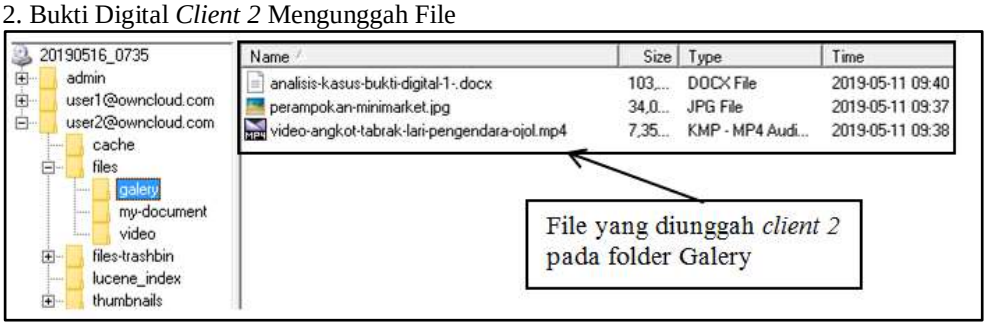
Bukti digital dari Skenario 3 berhasil diakuisisi pada direktori "\owncloud\data\user1 @owncloud.com\files\data-pentingku" seperti terlihat pada gambar 8. *File* yang diunggah *client 1* adalah "aksi-percobaan-perampokan-apotek-kimia-farma-pelaku-pakai-pistol-mainan.jpg dan video-perampokan-di-mobil.mp4" sedangkan file dokumen yang diunggah kemudian dihapus tidak ditemukan pada *database ownCloud*. Bukti digital file yang dihapus oleh *client 1* berhasil diakuisisi dengan teknik *live acquisition* (gambar 9).



Gambar 9. Bukti Digital File Yang Diunggah Kemudian Dihapus

Barang bukti file yang dihapus oleh *client 1* berhasil diakuisisi menggunakan teknik *live acquisistion* pada direktori "C:Program Files\NetworkMiner2\AssembledFiles \172.20.10.14\TCP-60593\" dengan nama file "DAFTAR PELAKU PENGEDAR NARKOBA.docx.

2. Bukti Digital *Client 2* Mengunggah File



Gambar 10. Bukti Digital File Yang Diunggah *Client 2*

Bukti digital aktivitas *client 2* menggunggah file berhasil diakuisisi pada direktori "\owncloud\data\user2@owncloud.com\files\galery", file yang diunggah *client 2* adalah "analisis-kasus-bukti-digital-1.docx, perampokan minimarket.jpg dan video-angkot-tabrak-lari-pengendara-ojol.mp4".

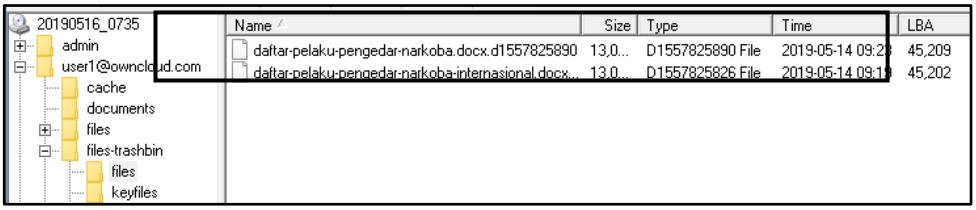
d. Skenario 4 : *Client* Men-*share* Folder/File Ke Sesama Pengguna *Cloud*.

Gambar 11. Bukti Digital Share Folder/File

Skenario 4 yaitu client men-*share* file/folder ke pengguna lain. Bukti digital dari Client 2 yang men-*share* folder "Galery" berhasil diakuisisi pada database server *ownCloud* "oc_share" pada *phpmyadmin*, sedangkan data *client 1* yang men-*share* file dokumen lalu menghapus file dokumen yang telah dibagikan ke *client 2* tidak ada di database server.

e. **Skenario 5** : *Client* Menghapus File

Skenario 5 hanya dilakukan oleh *client 1* sebagai pengguna PC karena *client 2* yang mengakses layanan *ownCloud* menggunakan *smartphone* tidak memiliki fitur menghapus file maupun folder pada layanan *ownCloud*.



Gambar 12. Bukti Digital Client 1 Menghapus File

Aktivitas *client 1* menghapus file berhasil diakuisisi pada direktori "owncloud\data\user1 @owncloud.com\files-trashbin\files", file yang dihapus tersebut adalah "daftar-pelaku-pengedar-narkoba.docx dan daftar-pelaku-pengedar-narkoba-internasional.docx".

4. IMPLEMENTASI

4.1 Hasil Akuisisi Data Secara *Live Acquisition* dan *Imaging*

Hasil analisis akuisisi data secara *live acquisiton* dan *imaging* bukti digital dari simulasi fungsional layanan *ownCloud* pada penelitian ini disusun dalam tabel bukti digital yang ditemukan seperti pada Tabel 6 dan Tabel 7.

Tabel 6. Data Bukti Digital Yang Berhasil Ditemukan

No	Skenario	*Client 1*	*Client 2*
1	Unduh File	√	√
2	Membuat Folder Baru	√	√
3	Unggah File	√	√
4	*Share* File / Folder	√	√
5	Menghapus File	√	-

Keterangan :
√ : Ditemukan, × : Tidak ditemukan, - : Skenario tidak dilakukan

Tabel 7. Parameter Pendukung Bukti Digital

No	Parameter	*Client 1*	*Client 2*
1	*IP Source*	√	√
2	*Mac Address Source*	√	√
3	*IP Destination*	√	√
4	*Mac Address Destination*	√	√
5	*Struktur Folder dan File*	√	√
6	*Log Activity*	√	√
7	*Username and Password*	√	√
8	*Time Stamp*	√	√
9	*Data Locations*	√	√
10	*Protocol and Port Access*	√	√

5. KESIMPULAN

Berdasarkan peneletian ini, maka dapat disimpulkan bahwa bukti digital hasil akuisisi data secara *live acquisition* dan *imaging* berdasarkan skenario yang dilakukan adalah sebagai berikut. Bukti digital skenario 1 dan skenario 3 berhasil mendapatkan detail nama file dan direktori *path* file yang diunduh oleh *client 1* dan *client 2* dilengkapi dengan data *ip address*, *mac address*, *username* dan *password*, *timestamp* dan data lainnya yang mendukung bukti digital skenario tersebut. Skenario 2 berhasil mendapatkan bukti digital berupa nama dan lokasi folder di *cloud*. Skenario 4 berhasil mendapatkan nama file dan folder yang di-*share* dilengkapi dengan data *client* yang mendapatkan hak akses file dan folder tersebut. Hasil skenario 5 berhasil mendapatkan detail nama file dan direktori *path* file yang dihapus oleh *client 1*. *Client 2* tidak melakukan skenario 5 karena layanan *ownCloud* pada *smartphone* tidak memiliki fitur hapus file maupun folder.

REFERENCES

[1] NIST (National Institute of Standards and Technology), "The attached DRAFT document (provided here for HISTORICAL purposes) has been superseded by the following publication", 2012.
[2] M. S. Asyaky, "Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android," vol. 3, pp. 220-231, 2019.
[3] M. Lessing and Van, S. B., "Live forensic acquisition as alternative to traditional forensic processes", 2016.
[4] N. Widiyasono, I. Riadi, and A. Luthfi, "Investigasi, Penerapan Metode ADAM Pada Proses Computing, Layanan Private Cloud," 2016.
[5] I. Febrian, E. Kurdiat, N. Widiyasono, and H. Mubarok, "Analisis Proses Investigasi Dekstop PC Yang Terhubung Layanan Private Cloud," vol. 2, pp. 221–230, 2016.
[6] P. Yakub, "Network Forensic Pada Jaringan Berbasis Awan," Mei 2017.
[7] A. Yudhana, R. Umar, and A. Ahmadi, "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ)," vol. X, no. X, pp. 8–13.
[8] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," vol. 8, no. 3, pp. 949–955, 2018.
[9] A. Aziz, Muhammad, "Analisis Forensik Line Messenger Berbasis Web Menggunakan Framework National Institute Of Justice (NIJ)," *in Seminar Nasional Informatika*. Yogyakarta, 2018.

[10] Furht, Borko and Armando Escalante, "Handbook of Cloud Computing," New York : Springer, 2010.
[11] Hendri, "Analisis Resiko Implementasi Teknologi Cloud Computing Pada Infrastruktur Saas (Software As A Service)," vol. 8, pp. 32-40, 2013
[12] H. Lovell, W. Maxwell and C. Wolf, "DCA Global Reality: Governmental Access to Data in the Cloud A comparative analysis of ten international jurisdictions," Hogan Lovell White papers.13, 2012.
[13] Howard, John D, "An Analysis Of Security Incidents On The Internet 1989 – 1995," PhD thesis, Engineering and Public Policy, Carnegie Mellon University. 1997
[14] I. Riadi and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode NIST," vol. 3, pp. 13-21, 2018.
[15] R. Imam, "Analisis Forensik Bukti Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Standards And Technology (NIST) ",Vol. 2, pp. 33-40, 2017.
[16] R. Tri, "Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar," vol. 1, pp. 32-38, 2018.
[17] Wardhana, Indrawata. "Membangun Owncloud Cloud Storage," IAIN, 2016.
[18] Yudhana, Anton. 2018. "Analisis Bukti Digital Facebook Messenger Menggunakan Metode NIST," Vol. 3, pp. 13-21, 2018.