

## Analisis Forensik Digital Storage pada Owncloud Drive

Dewi Estri Jayanti H<sup>\*1</sup>, Rusydi Umar<sup>2</sup>, Imam Riadi<sup>3</sup>

<sup>1, 2, 3</sup> Universitas Ahmad Dahlan

dewi1689048037@webmail.uad.ac.id<sup>\*1</sup>, rusydi.umar@tif.uad.ac.id<sup>2</sup>, imam.riadi@is.uad.ac.id<sup>3</sup>

### Abstrak

Penyimpanan data saat ini dapat menggunakan model Cloud. Cloud dapat di akses oleh beberapa user yang telah dibuatkan akun oleh admin. Semua aktivitas user terekam di history cloud. Tindak kejahatan dapat dilakukan dengan menghapus semua data penting yang ada pada Owncloud Drive yakni Nextcloud menggunakan salah satu admin dan menghapus histori pada cloud. Penelitian ini melakukan analisis investigasi untuk mengetahui siapa pelaku dan mengembalikan data yang sudah terhapus. Proses forensik digital storage pada owncloud drive (Nextcloud) dapat menggunakan metode dari National Institute of Standard and Technology (NIST) yang merupakan metode digital forensik yang digunakan secara umum oleh para peneliti di dunia. NIST dikembangkan untuk menyelesaikan simulasi kasus penyalahgunaan owncloud drive menggunakan skenario 5 akun yang terdiri dari satu admin dan user, pelaku melakukan kejahatan mengambil lalu menghapus data pada akun admin. Tahapan digital forensik NIST yakni pengumpulan data, pemeriksaan, analisis dan pelaporan. Berdasarkan proses investigasi yang dilakukan didapatkan laporan terkait pelaku kejahatan yang telah menghapus semua data penting yakni laporan keuangan, foto dokumentasi rahasia, dan beberapa data lainnya. Sebesar 75% data yang terhapus didapatkan kembali. Hasil penelitian ini juga didapatkan keterangan jejak pelaku kejahatan yang dibutuhkan sebagai barang bukti.

**Kata Kunci:** Analisis, Forensik, Owncloud, Investigasi, Nextcloud

### Abstract

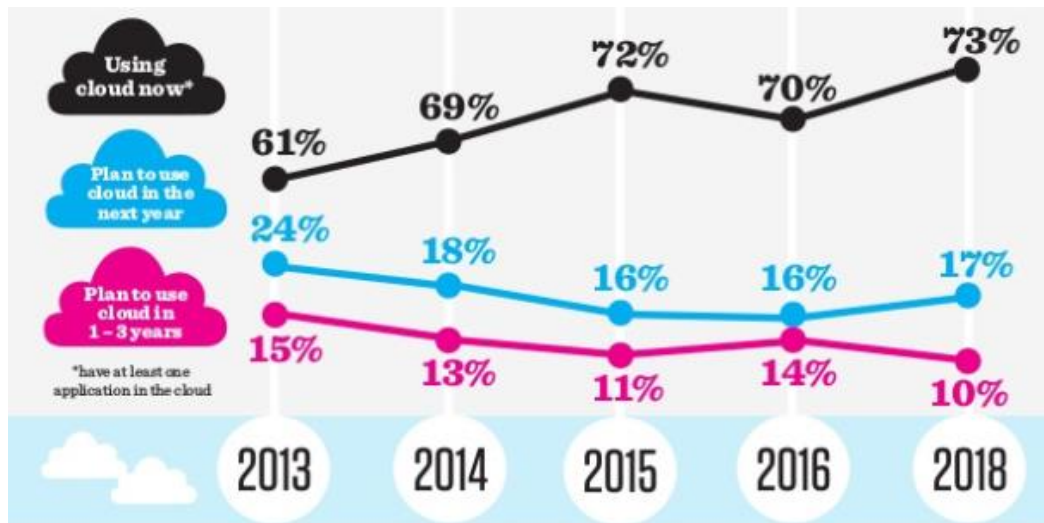
Data storage can currently use the Cloud model. Cloud can be accessed by several users who have created an account by the admin. All user activity is recorded in the cloud history. The crime can be done by deleting all important data in Owncloud Drive namely Nextcloud using one of the admins and deleting history in the cloud. This research conducts investigative analysts to find out who the perpetrators are and returns deleted data. Digital forensic storage process on owncloud drive (Nextcloud) can use methods from the National Institute of Standards and Technology (NIST) which is a digital forensic method used in general by researchers in the world. NIST was developed to solve simulations of owncloud drive abuse using 5 account scenarios consisting of two admins and users, perpetrators of the crime of taking and then deleting data on the admin account. NIST's digital forensic stages are data collection, examination, analysis and reporting. Based on the investigation process, it was obtained a report related to a criminal who had deleted all important data, namely financial statements, photos of confidential documentation, and several other data. 75% of deleted data is recovered. The results of this study also obtained traces of the perpetrators of crime needed as evidence.

**Keywords:** Analysis, Forensics, Owncloud, Investigation, Nextcloud

### 1. Pendahuluan

Komputasi awan atau *cloud computing* merupakan salah satu contoh perkembangan teknologi informasi. Komputasi awan adalah transformasi teknologi informasi dan komunikasi dari komputer berbasis klien atau server. *Cloud computing* memungkinkan pengguna untuk menggunakan layanan *software*, media penyimpanan (*Storage*), platform infrastruktur dan aplikasi layanan teknologi melalui jaringan internet [1]. *Cloud Computing* adalah teknologi yang menjadikan internet sebagai pusat pengolahan data dan aplikasi, di mana pengguna komputer diberikan hak akses atau *login* [2]. Penerapan komputasi awan saat ini sudah dilakukan oleh sejumlah perusahaan IT terkemuka di dunia. Perusahaan yang telah menggunakan komputasi awan adalah Google (*Google Drive*) dan IBM (*Blue Cord Initiative*) [3]. Perusahaan Indonesia yang telah menerapkan komputasi awan adalah Telkom [4]. Gambar 1. Menunjukkan grafik

pertumbuhan pengguna layanan *cloud computing*, banyak perusahaan besar menggunakan layanan tersebut untuk keperluan penting perusahaan (IDG's Enterprises, 2016).



Gambar 1. Grafik Perkembangan Penggunaan Cloud

Penelitian terdahulu mengemukakan bahwa *Owncloud* sebagai *open source* dapat menyesuaikan kebutuhan ketika digunakan, fleksibel dan *adaptable solution* dan tersedia module sistem dan keamanan data yang sesuai [5]. Keamanan data yang dikemukakan ternyata memungkinkan untuk adanya tindak kejahatan [6]. Pengambilan data secara ilegal atau melanggar hukum adalah salah satu usaha tindak kejahatan yang dapat dilakukan, yakni masuk ke dalam *Nextcloud* tanpa mempunyai ID dan *Password* terverifikasi sehingga mencoba masuk secara paksa dengan *Tools Forensics* seperti aktivitas *hacking* serta menghapus semua data penting perusahaan yang sebelumnya sudah di ambil alih oleh si pelaku. Proses penanganan dalam kasus seperti itu diperlukan untuk menggunakan penyelidikan forensik digital untuk mendapatkan informasi dari bukti *digital* [7]. Proses investigasi untuk mengembalikan data yang sudah dihilangkan atau dihapus oleh pelaku serta menemukan jejak pelaku kejahatan tersebut agar bisa dijadikan barang bukti dalam persidangan maka proses Analisa Forensik *Digital Storage* Pada *Owncloud Drive* dilakukan.

## 2. Metode Penelitian

Proses Investigasi dilakukan dengan menggunakan metode dari *National Institute of Standard Technology* (NIST) [8]. Skenario kasus yang dilakukan adalah kasus penyalahgunaan *Owncloud Drive* untuk melakukan kejahatan pencurian data pada *Owncloud Drive* yakni *Nextcloud*. Pelaku masuk menggunakan *user ID* salah satu pengguna dan melakukan proses *hacking* untuk mengetahui *Password* dan ID yang digunakan tersebut. Setelah mendapatkan *Password* secara *illegal* pelaku *login* menggunakan akun tersebut. Pelaku berhasil masuk dan melakukan tindak kejahatan berupa pencurian data penting yang mengakibatkan data tersebut hilang dan menghapus semua histori pada *nextcloud* agar tidak dapat diketahui. Skenario diterapkan, berikutnya adalah melakukan proses investigasi berdasarkan metode dari NIST seperti pada Gambar 2.



Gambar 2. Tahapan Digital Forensik dari NIST

Tahapan dari metode NIST [9] ada 4 yakni: 1. *Collection* yang merupakan langkah pertama dalam proses forensik adalah untuk mengidentifikasi sumber data potensial dan memperoleh data dari sebuah kasus yang berkaitan dengan tindak kejahatan, memperoleh data dengan mengembangkan rencana data dari nilai volatilitas dan jumlah usaha yang diperlukan serta memverifikasi integritas data, 2. *Examination* dilakukan setelah data terkumpul dan tahap selanjutnya adalah memeriksa data yang melibatkan penilaian serta mengekstraksi bagian informasi yang relevan dari data yang dikumpulkan, 3. *Analysis* dilakukan setelah informasi yang relevan telah diekstraksi, analisis harus mempelajari dan menganalisis data yang diambil dan kesimpulan dari proses *examination*, 4. *Reporting* adalah tahapan terakhir yaitu proses mempersiapkan dan menyajikan informasi yang dihasilkan dari tahapan analisis. Penelitian ini dalam prosesnya membutuhkan alat atau *tools* yang digunakan untuk memperoleh bukti digital. Alat atau *tools* yang digunakan dalam penelitian ini dibagi menjadi dua jenis yakni *Hardware* dan *Software*. Tabel 1 menjelaskan tentang *hardware* yang digunakan dalam penelitian. Tabel 2 menunjukkan *software* forensik yang digunakan dalam penelitian.

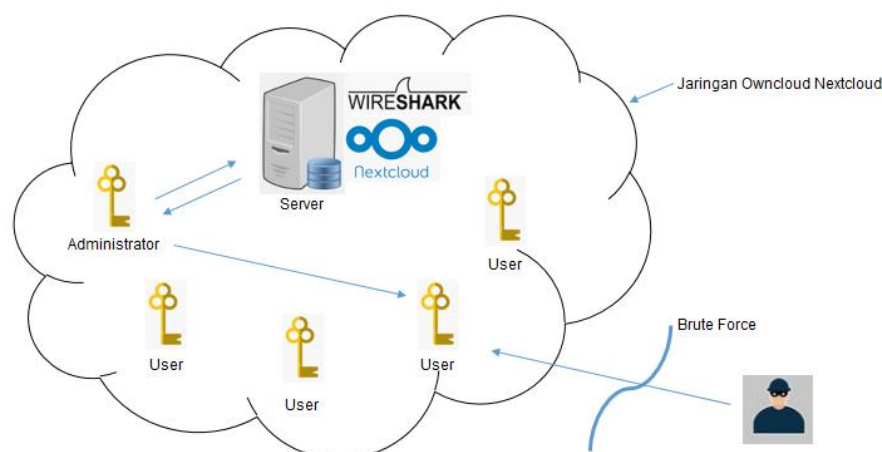
Tabel 1. Hardware (Perangkat Keras)

Hardware	Keterangan
PC Server	Processor core 2 duo, 1GB RAM, 80GB HDD, NIC, OS Debian 8.7 dan BIND9
Modem Router	TPLINK ADSL 2+
Client	Processor dual core, 512MB, 80GB HDD, NIC, Win 10
PC Penyerang	Windows 7
Laptop Acer	Windows 7 32 bit

Tabel 2. Software (Perangkat Lunak)

Software	Version	Keterangan
Owncloud Drive		
Nextcloud	12.0	Open Source
Wireshark	3.0.1	Open Source
GetDataBack	3.62	Propietary
Encase Acquisition	Evaluation Trial	Open Source

Penelitian ini menggunakan simulasi tindak kejahatan digital pada *Owncloud Drive Nextcloud*, simulasi tersebut melibatkan 5 akun pada jaringan *cloud*. Detail akun yang dibuat yakni satu administrator dan 4 *user*. Satu *user* diketahui telah di *hack* oleh orang luar, sehingga mengakibatkan semua data hilang. Peneliti melakukan proses investigasi *digital* forensik untuk mencari tahu pelaku. Proses *hacking* oleh pelaku dilakukan menggunakan teknik *Brute Force* ke server pribadi. Gambar 3 menunjukkan simulasi kejahatan *digital* pada *owncloud drive nextcloud*.



Gambar 3. Skema Simulasi Kejahatan Digital

Gambar 3 merupakan skema simulasi kejahatan digital pada jaringan Owncloud Drive Nextcloud, simulasi ini di mulai dengan menggunakan proses *brute force* yang dilakukan oleh pelaku untuk mendapatkan ID dan *Password* targetnya. Proses brute force berhasil, password diketahui sehingga pelaku langsung menargetkan untuk mencari semua data penting yang dibutuhkan. Pelaku adalah orang yang mengetahui tentang semua data penting tersebut dari orang dalam perusahaan, sehingga dengan mudah pelaku mengambil data-data yang diketahui penting bagi perusahaan. Pelaku menghapus seluruh jejak yang ada pada histori dan menghapus seluruh file. Proses investigasi dilakukan mulai dengan menelusuri jejak lalu lintas yang terjadi dan melihat nya pada wireshark yang telah ada pada server. Proses selanjutnya menggunakan IP *Tracer* karena sebelumnya telah diketahui ada jejak lalu lintas berupa IP yang tidak biasa, sehingga dilakukan pencarian melalui IP *Tracer*. Setelah jejak pelaku diketahui maka selanjutnya proses pengembalian data yang telah terhapus agar bisa dikembalikan atau di *restore*. Proses pengembalian data menggunakan *GetDataBack*. Selanjutnya proses menunggu hasil *restore* dari *GetDataBack*.

### 3. Hasil Penelitian dan Pembahasan

Pada bagian ini, hasil dari proses penelitian menggunakan metode dari NIST adalah sebagai berikut:

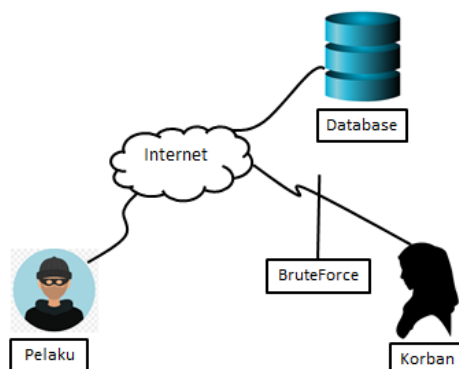
#### 3.1 Collection

Langkah pertama dalam proses forensik adalah untuk mengidentifikasi sumber data potensial dan memperoleh data dari sebuah kasus yang berkaitan dengan tindak kejahatan, memperoleh data dengan mengembangkan rencana data dari nilai volatilitas dan jumlah usaha yang diperlukan serta memverifikasi integritas data. Pada proses collection menggunakan laptop acer dengan spesifikasi berikut.



Gambar 4. Laptop Acer yang digunakan

Gambar 4 Merupakan laptop yang digunakan untuk proses collection dalam penelitian ini dengan spesifikasi laptop processor: Intel Core i3-380M, VGA: Intel GMA HD, Memory RAM: 2GB, HDD: 320GB, Layar: LCD 14.0 Inchi LED, Fitur Lainnya: DVDRW, LAN, WiFi, USB. Skema pada proses pengumpulan informasi dari sumber yang berkaitan dengan penelitian seperti Gambar 5.

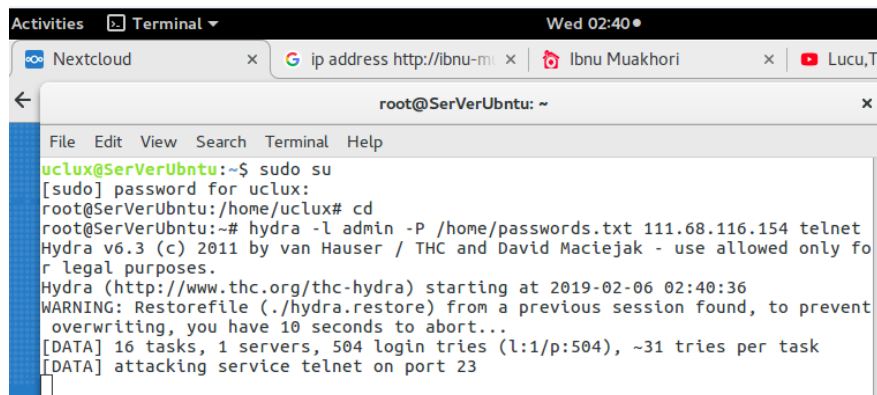


Gambar 5. Skema Pengumpulan Barang Bukti

Gambar 5 Merupakan skema pengumpulan bukti digital yang dilakukan menggunakan teknik *Brute Force* dengan *Tools Hydra*. Pelaku melakukan teknik brute force untuk mengetahui Password dan ID korban yakni user admin di jaringan *Nextcloud*.

### 3.2 Examination

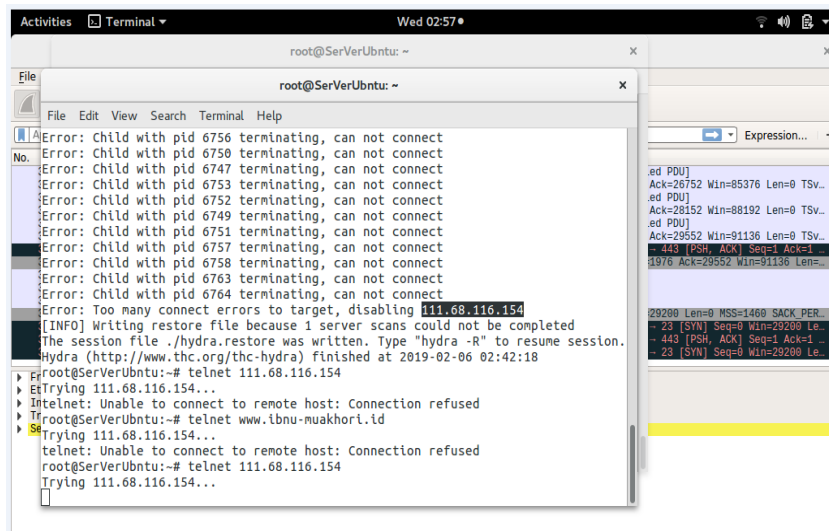
Examination dilakukan dengan pengujian pada server pribadi yang telah diinstall software Wireshark dan dilakukan serangan berupa seseorang masuk secara ilegal ke jaringan *Nextcloud* yang ada pada server pribadi tersebut menggunakan teknik *Brute Force* dengan *Tools Hydra*. Teknik *Brute Force* adalah metode untuk meretas Password (*Password Cracking*) dengan mencoba semua kemungkinan kombinasi yang ada pada "Word List" [10]. Teknik *Brute Force* dilakukan mulai dari tanggal 17 Februari 2019 pukul, 10.20wib. Berikut ini adalah perintah *Hydra* ke telnet server pribadi seperti pada Gambar 6.



```
root@SerVerUbuntu: ~  
File Edit View Search Terminal Help  
uclux@SerVerUbuntu:~$ sudo su  
[sudo] password for uclux:  
root@SerVerUbuntu:/home/uclux# cd  
root@SerVerUbuntu:~# hydra -l admin -P /home/passwords.txt 111.68.116.154 telnet  
Hydra v6.3 (c) 2011 by van Hauser / THC and David Maciejak - use allowed only fo  
r legal purposes.  
Hydra (http://www.thc.org/thc-hydra) starting at 2019-02-06 02:40:36  
WARNING: Restorefile (./hydra.restore) from a previous session found, to prevent  
overwriting, you have 10 seconds to abort...  
[DATA] 16 tasks, 1 servers, 504 login tries (l:1/p:504), ~31 tries per task  
[DATA] attacking service telnet on port 23
```

Gambar 6. Perintah Script Hydra pada Cloud Server Pribadi

Gambar 6 merupakan *script* perintah *Hydra* ke *Cloud Telnet* IBNU (Server Pribadi). *Script* tersebut mencoba untuk meretas *Password* salah satu akun user pada jaringan *Cloud Server* pribadi di *Nextcloud*. Hasil perintah telnet ke *cloud server* pribadi menggunakan *Hydra* seperti Gambar 7.



```
root@SerVerUbuntu: ~  
File Edit View Search Terminal Help  
Error: Child with pid 6756 terminating, can not connect  
Error: Child with pid 6750 terminating, can not connect  
Error: Child with pid 6747 terminating, can not connect  
Error: Child with pid 6753 terminating, can not connect  
Error: Child with pid 6752 terminating, can not connect  
Error: Child with pid 6749 terminating, can not connect  
Error: Child with pid 6751 terminating, can not connect  
Error: Child with pid 6757 terminating, can not connect  
Error: Child with pid 6758 terminating, can not connect  
Error: Child with pid 6763 terminating, can not connect  
Error: Child with pid 6764 terminating, can not connect  
Error: Too many connect errors to target, disabling 111.68.116.154  
[INFO] Writing restore file because 1 server scans could not be completed  
The session file ./hydra.restore was written. Type "hydra -R" to resume sesstion.  
Hydra (http://www.thc.org/thc-hydra) finished at 2019-02-06 02:42:18  
root@SerVerUbuntu:~# telnet 111.68.116.154  
Trying 111.68.116.154...  
telnet: Unable to connect to remote host: Connection refused  
root@SerVerUbuntu:~# telnet www.ibnu-muakhori.id  
Trying 111.68.116.154...  
telnet: Unable to connect to remote host: Connection refused  
root@SerVerUbuntu:~# telnet 111.68.116.154  
Trying 111.68.116.154...
```

Gambar 7. Hasil Perintah Telnet ke Cloud Server Pribadi Menggunakan Hydra

Gambar 7 merupakan hasil dari perintah telnet ke *cloud server* pribadi pada *hydra*. Perintah tersebut merupakan perintah menggunakan IP Address yang memungkinkan untuk dapat mengetahui lalu lintas mencurigakan yang ter-record pada proses *Brute Force Hydra* [11]. Percobaan teknik *Brute Force* juga dilakukan untuk perintah *Snort Sniffing* ke *Cloud Server* seperti pada Gambar 8.

```

root@SerVerUbuntu: ~
[sudo] password for uclux:
uclux@SerVer: /home/uclux# cd
[sudo] password for root:
root@SerVerUbuntu:~# snort -v -d -e
Running in packet dump mode

--- Initializing Snort ---
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "wlp2s0".
Decoding Ethernet

--- Initialization Complete ---

--> Snort! <*-
o'-'-~
  ''''
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.41 2017-07-05
Using ZLIB version: 1.2.8

Commencing packet processing (pid=6457)

```

Gambar 8. Perintah Snort Sniffing ke Cloud Server

Gambar 8 merupakan perintah *Snort Sniffing* yang sudah selesai inialisasi untuk dapat mengetahui *Password user* yang diretas. Proses *Dump* dilakukan memerlukan proses inialisasi terlebih dahulu agar dapat berjalan dengan baik [12]. Penelusuran jejak pelaku menggunakan *Software Wireshark* hanya dapat memperlihatkan gerak lalu lintas jaringan data yang aneh atau tidak biasanya berupa *IP Address*. Proses pencarian pelaku dilanjutkan menggunakan proses pencarian alamat IP tersebut. Selain menggunakan *software* pencarian pelaku juga dilakukan interogasi mendalam terhadap semua *user* yang menggunakan akun *Nextcloud*. Interogasi dilakukan untuk mendapatkan informasi terkait waktu dan tempat kejadian masing-masing user, beserta semua aktifitas yang mereka lakukan saat terjadi tindakan kejahatan tersebut.

### 3.3 Analysis

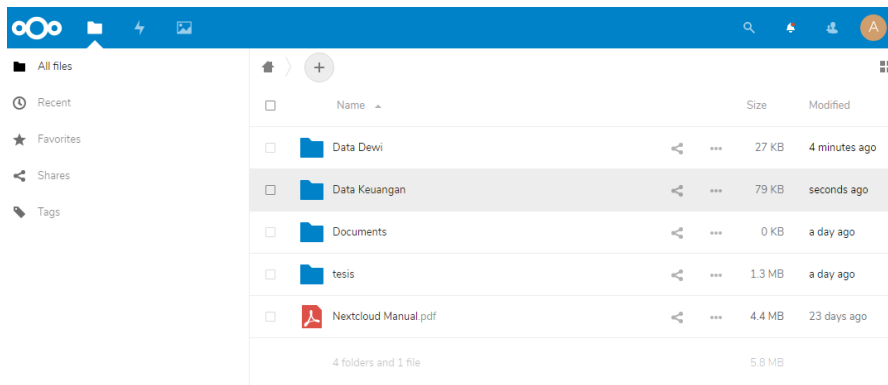
Tahap analisis adalah fase dimana semua barang bukti yang telah ditemukan diperiksa menggunakan metode yang diperbolehkan untuk digunakan dan dapat menjawab pertanyaan yang mengacu pada rumusan masalah yang dikemukakan sebelumnya. Hal pertama yang dilakukan adalah membangun *Owncloud Drive* yakni *Nextcloud* pada server pribadi [13]. Proses instalasi pada server ini sudah dilakukan sebelumnya dengan membuat akun admin, lalu membuat 4 akun *user* sesuai simulasi dengan ID dan Password berbeda seperti Gambar 9.

Username	Display name	Password
admin	admin	New password
dewi	dewi	New password
ibnu	ibnu	New password
nina	nina	New password
Riase	Raisa	New password

Gambar 9. Detail 5 Akun User yang telah dibuat

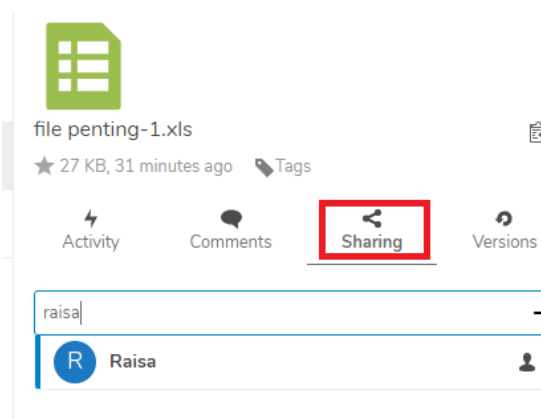
Gambar 9 merupakan daftar list kelima akun yang telah dibuat yakni Admin sebagai administrator, lalu dewi, ibnu, nina dan raisa sebagai *user*. Masing- masing user memiliki password yang berbeda sehingga untuk masuk bukan sebagai pemilik tidak bisa. Setelah dibuat

akun maka simulasi berikutnya adalah *sharing* data ke salah satu user. Proses *sharing* data dilakukan dengan terlebih dahulu dilakukan proses *uploading file* atau sinkronisasi data ke *nextcloud* seperti pada Gambar 10.



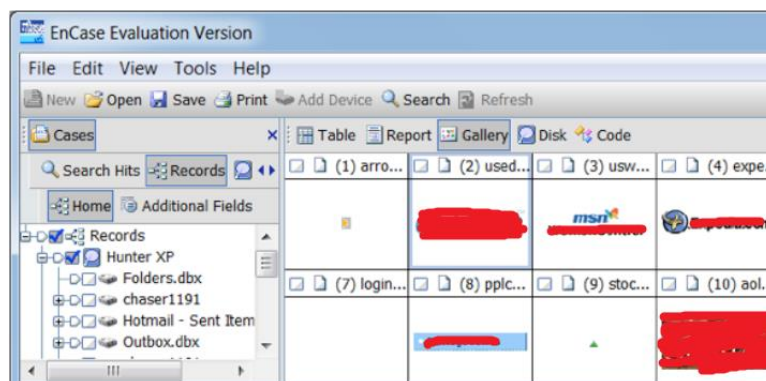
Gambar 10. Upload File dan Membuat New Folder di Nextcloud

Gambar 10 merupakan hasil dari proses *uploading file* ke *folder nextcloud* yang berupa data keuangan. Proses *upload file* berhasil dilakukan sehingga dapat dilakukan proses selanjutnya yakni *sharing file* ke salah satu *user* bernama *raisa* seperti pada Gambar 11.



Gambar 11. Proses Sharing File oleh Admin ke User Raisa

Gambar 11 merupakan proses *sharing* data ke *user* *raisa* untuk dapat dipergunakan sebagaimana mestinya. Tahap selanjutnya dalam menganalisis menggunakan beberapa *tools* forensik pertama yakni *Encase V6 Demo* yang merupakan *tools* tidak berbayar. Proses investigasi menggunakan *tools* *encase V6 demo* pada modul *encase evaluation version* seperti pada Gambar 12.



Gambar 12. Hasil Evaluation Version Encase pada Email

Gambar 12 merupakan hasil evaluasi versi encase V6 Demo trial dibuat sebuah *folder Cases* untuk mencari tahu apakah ada jejak pelaku melalui percakapan via email. Hasil percakapan dapat dilihat pada gallery. Pada proses investigasi ini ditemukan sebuah chat dari seseorang yang tidak dikenal yang menunjukkan bahwa ternyata pelaku dibantu oleh user dalam jaringan *nextcloud*. Membuktikan kebenaran adanya orang dalam yang membantu maka proses investigasi dilakukan kembali dengan menginterogasi *user* terkait yang membantu pelaku secara lebih detail. Tahap selanjutnya adalah menganalisa IP *address* yang ditemukan pada lalu lintas aneh yang sebelumnya terdeteksi oleh *wireshark*. IP tersebut dilakukan proses pencarian menggunakan IP Tracer agar lokasi pelaku dapat diketahui seperti pada Gambar 13.

Geolocation data from IP2Location (Product: DB6, updated on 2019-5-1)

IP Address	Country	Region	City
114.125.76.201	Indonesia 🇮🇩	Jawa Timur	Batu
ISP	Organization	Latitude	Longitude
PT Telekomunikasi Selular Indonesia	Not Available	-7.8700	112.5283

Geolocation data from ipinfo.io (Product: API, real-time)

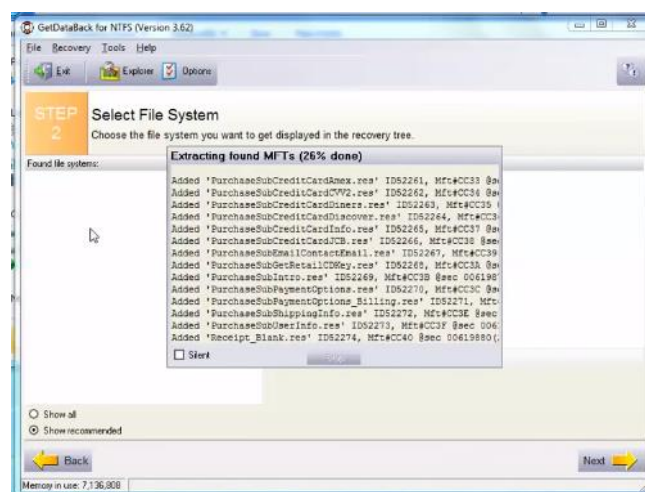
IP Address	Country	Region	City
114.125.76.201	Indonesia 🇮🇩	East Java	Surabaya
ISP	Organization	Latitude	Longitude
PT. Telekomunikasi Selular Indonesia (telkomsel.co.id)	PT. Telekomunikasi Selular (Telkomsel) Indonesia	-7.2484	112.7420

Geolocation data from DB-IP (Product: Full, 2019-5-1)

IP Address	Country	Region	City
114.125.76.201	Indonesia 🇮🇩	Jakarta	Jakarta
ISP	Organization	Latitude	Longitude
PT Telekomunikasi Selular Indonesia	Not Available	-6.17511	106.865

Gambar 13. Detail IP Location Pelaku

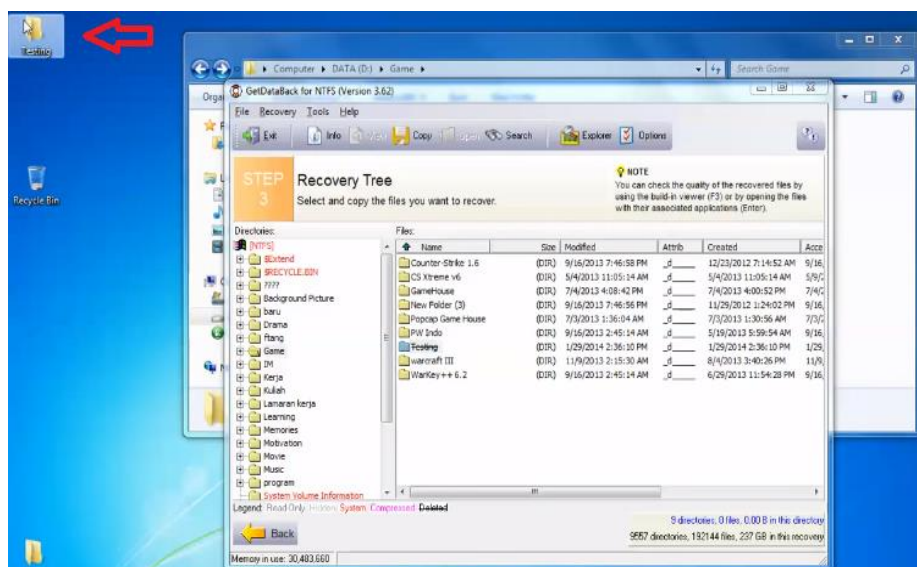
Gambar 13 menurut *Geolocation* data dari IP2 *Location* berada di negara Indonesia, propinsi jawa timur, kota batu dan *Geolocation* data dari ipinfo.io pelaku berada di negara indonesia, propinsi jawa timur kota surabaya. Sedangkan *Geolocation* DB-IP nya berada di Indonesia, jakarta. Tahap selanjutnya adalah recovery data menggunakan software getdataback seperti pada Gambar 14.



Gambar 14. Proses Extracting File GetDataBack



Gambar 14 merupakan proses *Extracting file* yang dihapus oleh pelaku. Proses *extracting* ini memerlukan waktu cukup lama dan tunggu hingga proses *Extracting Completed*. Hasil dari *Extracting file* tersebut dapat dilihat pada *Recovery Tree* seperti Gambar 15.



Gambar 15. Hasil *Extracting* Tampilan *Recovery Tree*

Gambar 15 merupakan hasil dari *extracting* dan dapat dilihat pada *recovery tree*. Folder “*Testing*” adalah yang diskenario kan sebagai *folder* yang telah dihapus pelaku. Folder *testing* akan dicek secara keseluruhan untuk mengetahui apakah semua data bisa dikembalikan seperti file sebelumnya atau ada sebagian data yang hilang atau tidak dapat dikembalikan.

**3.4 Reporting**

Proses Reporting dilakukan agar mudah dimengerti tentang rincian sebuah kasus. Tahap Reporting dapat dilihat pada Tabel 3.

Tabel 3. Rangkuman Proses Investigasi Beserta Hasil

No.	Tahapan Proses Investigasi	Hasil yang ditemukan	Keterangan
1	Collection data menggunakan software <i>wireshark</i>	IP 192.168.1.147 <i>not identified (security alert setting software wireshark)</i>	Ada alamat IP yang tidak teridentifikasi oleh software <i>wireshark</i> yang sebelumnya sudah setting alert jika IP masuk selain 5 IP yang telah diidentifikasi <i>confirmed login</i> .
2	Examination - <i>Wireshark</i>  - Encase  - IP Tracer	Terdeteksi adanya lalu lintas IP yang aneh dan diketahui alamat IP tersebut bukan alamat yang boleh <i>login</i> ke <i>nextcloud</i> . Pencarian <i>chatting</i> via email yang telah dihapus terlihat namun tidak ada percakapan yang dapat dijadikan barang bukti. IP Address 192.168.1.147 berada di propinsi Jawa timur kota batu.	Alamat IP yang dapat akses <i>login</i> yakni: 192.18.1.7, 192.18.1.9, 192.18.1.121, 192.168.1.120 dan 192.168.1.2. Email menggunakan <i>outlook</i> tidak dapat digunakan  Menggunakan <i>Geolocation Data</i> .

3	<p><i>Analysis</i></p> <p>- Berdasarkan keterangan dari saksi <i>user</i> akun <i>nextcloud</i>.</p>	Ada kejanggalan dalam proses interogasi dan informasi alibi masing-masing <i>user</i> .	Tidak dijelaskan seara detail pertanyaan proses interogasi namun interogasi dilakukan untuk mengetahui apakah ada orang dalam yang terkait tindak kejahatan dengan pelaku.
	<p>- Berdasarkan waktu terakhir <i>login</i> menggunakan ID dan <i>password</i> masing-masing</p>	Ada ketidaksesuaian antars data <i>time stamp</i> yang ditemukan dengan pengakuan salah satu <i>user</i> .	Hal tersebut mengakibatkan adanya kecurigaan terhadap pemilik akun, kemungkinan pemilik akun mengetahui siapa pelaku.

Tabel 3 merupakan rangkuman proses investigasi beserta hasil yang didapatkan dari Proses *Collection*, *Examination*, dan *Analysis* semua dapat terlihat pada tabel tersebut secara terperinci. Klasifikasi *recovery* data yang dilakukan menggunakan *Software GetDataBack* dapat dilihat pada Tabel 4.

Tabel 4. Klasifikasi *Recovery GetDataBack*

Klasifikasi Data	Size	Ada	Tidak	Persentase (%)	Keterangan
format.docx	1224 KB	V		75%	Ada perubahan
format.jpeg	164 KB		V	100%	Tidak ada perubahan
format.mp4	209447 KB		V	100%	Tidak ada perubahan
format.xlsx	1442 KB	V		98%	Ada perubahan
format.ppt	1921 KB		V	100%	Tidak ada perubahan
format.pdf	595 KB		V	100%	Tidak ada perubahan
Total	214793 KB				

Tabel 4 merupakan hasil dari *recovery* data menggunakan *software GetDataBack*. Perubahan file dan *persentase recovery* data yang dimaksud "Ada" karena beberapa data mengalami perubahan dan tidak semua data dapat di *recovery* secara full sedangkan maksud dari kata "Tidak" berarti bahwa *recovery* data berhasil dan tidak ada perubahan dalam hal isi maupun *subject*.

#### 4. Kesimpulan

Kesimpulan dari hasil penelitian ini adalah proses investigasi pada *Owncloud Drive* yang bernama *Nextcloud* telah berhasil dilakukan dengan baik karena semua rangkaian proses investigasi berdasarkan metode dari NIST seperti *Collection*, *Examination*, *Analysis* dan *Reporting* dapat dilakukan *step by step* serta mendapatkan hasil tindak kejahatan pelaku. Berdasarkan hasil proses investigasi menggunakan beberapa *Tools Forensics* bukti kejahatan pelaku dapat diketahui dan untuk data yang hilang 75% dapat di kembalikan.

#### Referensi

- [1] W. Ono Purbo. Membuat Sendiri Cloud Computing Server Menggunakan Open Sourcem. Yogyakarta : Penerbit Andi. 2012.
- [2] Affiyanto, Dedy Setyo. 2016. "The Power of Owncloud". Penerbit Leutikaprio, Yogyakarta.
- [3] I. S. Bianchi and R. D. Sousa. IT Governance mechanisms in higher education, *Procedia - Procedia Comput. Sci*, vol. 100, pp. 941-946, 2016.
- [4] Budiyanto, Alex. 2012. "Pengantar Cloud Computing". Komunitas Cloud Computing Indonesia.
- [5] Karovic, V and Gregus, M. Practical Implementation of Private Cloud Based on Open Source Owncloud for Small Teams - Case Study, *International Conference Business, Computer Science*, 2015.

- [6] DFRWS, "Digital Forensics Research Conference a Road Map for Digital Forensics Research",2001.
- [7] E. Akbal and S. Dogan, Forensics Image Acquisition Process of Digital Evidence, International Journal of Computer Network and Information Security, vol. 10, no. 5, pp.1-8, 2018.
- [8] E. Information and S. Techincal, "A Comprehensive Approach to Digital Incident Investigation," pp.1-13,2003.
- [9] S. Vidwarshi and N. Chandra, Analysis of Development pHases in Digital Forensics, International Journal of Advanced Computational Engineering and Networking, vol. 2, no. 8, pp. 90-95, 2015..
- [10] Faiz, M. N., Umar, R., & Yudhana, A. (2017). Implementasi Live Forensics untuk Perbadningan Browser pada Keamanan Email. JISKa, 1(February), 108-114. <https://doi.org/10.14421/jiska.2017.13-02>.
- [11] M. Patankar and D. Bhandari, Forensics Tools used in Digital Crime investigation, Indian Journal of Applied Research, vol. 4, no. 5, pp. 278-283,2014.
- [12] JAMIL, Mohamad. 2016. "Buku Ajar Cloud Computing". Penerbit Deepublish, Yogyakarta.
- [13] Actoriano, B., & Riadi, I. (2018). Forensics Investigation on Whatsapp Web Using Framework Integrated Digital Forensics Investigation Framework Version 2, (September)

