Analisis Proses Investigasi *Dekstop PC* Yang Terhubung *Layanan Private Cloud*

Irfan Febrian Editia Kurdiat[#1], Nur Widiyasono[*2], Husni Mubarok[#3]

[#]*Teknik Informatika,Universitas Siliwangi*
Jl. Siliwangi No. 24, Kota Tasikmalaya
[1]irfan.febrian@student.unsil.ac.id
[2]nur.widiyasono@unsil.ac.id
[3]Husni.mubarok@unsil.ac.id

Abstract — **Private Cloud Computing Services is one of current technology advances that can meet the needs of companies and organizations, many cloud service providers to offer facilities at affordable costs. However, in addition to bringing the benefits, cloud services can be misused by insiders in the company to commit cyber crimes that hurt companies such as leakage of confidential data, take advantage of the company itself, data manipulation etc. Handling process in such cases it is necessary to use a digital forensic investigation to obtain information from the digital evidence. This research used EEDI (End to End Digital Investigation) in the process of investigation on the desktop side by getting the files and folders associated with crimes. The results of an investigation carried out in the form of information proving that the offender is committing a crime, The information then presented in the form of a forensic report which will be used during the trial.**

Keywords— **Acquisition, Digital evidence, Digital forensic, investigation**

I. PENDAHULUAN

Layanan *cloud computing* merupakan penggabungan pemanfaatan teknologi komputasi dan pengembangan berbasis internet yang menawarkan fasilitas sumber daya tanpa perangkat tambahan, biaya yang lebih terjangkau dan penyimpanan data yang tidak terbatas. *Cloud computing* dibagi tiga yaitu *Cloud Software as a service* (SaaS), *Cloud Platform as a Service* (PaaS) dan *Cloud Infrastructure a Service* (IaaS) .Model *cloud computing* menurut *NIST* empat model, yaitu *Private Cloud, Public Cloud, Community Cloud, Hybrid Cloud* [11]. Perusahaan atau organisasi pun sudah banyak yang menggunakan layanan ini untuk kebutuhan kerja. Private *cloud* mencakup seluruh *cloud* infrastructure termasuk sumber daya *hardware* yang dimiliki organisasi atau perusahaan tersebut.

Namun, selain mendatangkan manfaat, layanan ini juga dapat memberikan dampak negatif jika disalahgunakan untuk melakukan kejahatan siber. Kejahatan *cyber* dapat terjadi diiringi dengan berkembangnya teknologi, berdasarkan laporan dari Pusat Informasi Kriminal Nasional POLRI, kejahatan dunia maya atau *Cyber Crime* yang ada di indonesia paling banyak terjadi pada tahun 2015-2016, yaitu berjumlah 587 kasus. Jumlah tersebut merupakan jumlah terbanyak dibandingkan tahun-tahun sebelumnya, hal ini menunjuk sejalan dengan berkembangnya teknologi maka kejahatan siber pun akan terus bertambah.

Merujuk masalah tersebut, maka diperlukan metode untuk menangani kasus kejahatan *cyber*, yaitu dengan menggunakan teknik digital forensik untuk menganalisa dan menelusuri bukti-bukti digital dari tindak kejahatan. Penelitian ini meggunkan model *EEDI* (*End to End Digital Investigation*) untuk mencari, mendapatkan serta menganalisisa bukti digital dari perangkat yang digunakan dalam melakukan kejahatan *cyber.*

Manfaat dari penelitian ini adalah mengetahui bagaimana proses melakukan investigasi kejahatan *cyber* pada sisi desktop yang terhubung *layanan private cloud*, sehingga hasil investigasi tersebut dapat digunakan dalam persidangan .

II. KAJIAN PUSTAKA

A. Digital Forensik

Menurut Digital Forensics Research Workshop "Penggunaan ilmu ilmiah yang diambil dan mengacu pada hasil preservation, collection, validation, identification, analysis, interpretation, documentation and presentation bukti digital yang diambil dari sumber digital untuk tujuan memfasilitasi atau melanjutkan rekonstruksi atau membantu untuk mengantisipasi tindakan tidak sah yang terbukti menganggu operasi yang direncanakan." [7]

Tahapan Digital Forensik anatara lain:

1. Identifikasi Bukti Digital
   Tahap ini segala bukti-bukti yang mendukung penyelidikan dikumpulkan, penyelidikan dimulai dari idetifikasi di mana bukti itu berada, dimana bukti itu disimpan dan bagaimana penyimpanannya untuk mempermudah penyelidikan.
2. Penyimpanan Bukti Digital

Tahapan ini mencakup penyimpanan dan penyiapan bukti-bukti ang ada termasuk melindungi bukti-bukti dari kerusakan, perubahan dan pengilangan oleh pihak-pihak tertentu.

3. Analisa Bukti Digital
   Tahapan ini melakukan analisa terhadap bukti-bukti yang ada, bukti yang telah didapatkan perlu ditelusuri kembali kedalam sejumlah skenario yang berhubungan dengan tindak pengusutan. Penelusuran bisa dilakukan pada data-data sebagai berikut: alamat *URL* yang telah dikunjungi, pesan *e-mail* atau kumpulan alamat *e-mail* yang terdaftar, *program word processing* atau format ekstensi yang dipakai, dokumen *spreedsheat* yang dipakai, format gambar yang dipakai apabila ditemukan, *file*s yang dihapus maupun diformat, *password, registry windows, hidden files, log event viewers*, dan *log application*, termasuk juga pengecekan pada *metadata.*
4. Presentasi
   Presentasi dilakukan dengan menyajikan dan menguraikan secara detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa secara mendalam dan dapat dipertanggung jawabkan secara hukum di pengadilan.

B. Komputer Forensik

Komputer forensik merupakan salah satu cabang ilmu forensik yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpaan secara digital [20]. Bidang ilmu yang dimanfaatkan dan dilibatkan pada suatu kasus kejahatan atau kriminal ada banyak yang bisa dimanfaatkan untuk suatu kepentingan hukum dan keadilan, di mana ilmu pengetahuan tersebut dikenal dengan ilmu forensik.

Meskipun paling sering dikaitkan dengan penyelidikan dari berbagai kejahatan komputer, komputer forensik juga dapat digunakan dalam proses sipil dengan menggunakan teknik yang mirip dan prinsip untuk memulihkan data, tapi dengan pedoman tambahan dan praktek yang dirancang untuk membuat jejak audit hukum. Bukti dari invertigasi komputer forensik biasanya dikenakan dengan pedoman yang sama dan praktek bukti digital.

Terdapat 4 fase dalam komputer forensik (NIST, 2006) antara lain yaitu:

1. Pengumpulan Data
   Pengumpulan data yang tujuannya mengidentifikasi berbagai sumber daya yang dianggap penting dan bagaimana seluruh data dapat terhimpun dengan baik.
2. Pengujian
   Pengujian mencakup suatu proses penilaian dan memilah berbagai informasi yang sesuai dari semua data yang telah dikumpulkan, juga *bypassing* proses atau meminimalisasi berbagai fitur dalam sistem operasi dan aplikasi yang bsa menghlangkan data seperti enkripsi, kompresi, akses mekanisme kontrol, mengalokasi *file*, pemeriksanan pemetaan metadata, mengekstrak *file* dan lain-lain.
3. Analisis,
   Analisis dapat dilakukan dengan berbagai pendekatan metode, tugas dari analisis ini mencakup banyak kegiatan, seperti mengidentifikasi *user* (pengguna) yang terlibat secara tak langsung, lokasi, kejadian, perangkat dan mempertimbangkan bagaimana caranya agar semua komponen itu saling terhubung sampai mendapatkan kesimpulan akhir.
4. Dokumentasi dan Laporan. Beberapa faktor yang dapat mempengauhi hasil dokumentasi dan laporan, antara lain sebagai berikut:
   a. Penjelasan Alternatif (*Alternative Explanations*) - Seorang analis pada dasarnya harus mampu menggunakan pendekatan yang berupa metode untuk menyetujui ataupun menolak setiap penjelasan dari sebuah kasus atau perkara yang diajukan.
   b. Pertimbangan Penilik (*Audience Consideration*) - Yaitu menyediakan data ataupun informasi kepada *audience* yang sangat berguna dan diperlukan. Kasus yang melibatkan sejumlah aturan sangat dibutuhkan laporan yang spesifik berkaitan dengan informasi data yang dikumpulkan, selain itu juga sangat dibutuhkan- kopian dari setiap fakta yang diperoleh.
   c. *Actionable Information* - Merupakan sebuah proses dokumentasi dan laporan yang mencakup tentang identifikasi *actionable information* yang diperoleh dari sekumpulan- jumlah data terdahulu lalu dengan bantuan sejumlah data tersebut maka kita dapat memperoleh dan mengambil informasi terbaru.

C. Digital Forensics Investigation Framework (DFIF)

Kerangka kerja digital forensik merupakan proses yang harus dilakukan yang mencakup [7]:

1. Identifikasi (*Identification*). Mengenali insiden dari indikator dan menentukan jenisnya
2. Persiapan (*Preparation*). Persiapan mencakup dari persiapan alat, teknik, surat penggeledahan, wewenang pengawasan dan dukungan manajemen.
3. Strategi Pendekatan (*Approach Strategy*). Mengembangkan prosedur yang digunakan

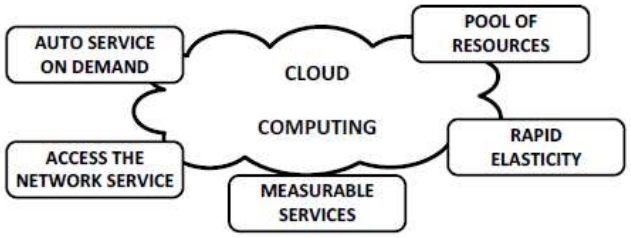
untuk memaksimalkan pengumpulan bukti dan menimimalkan dampak kepada korban.

4. Pengawetan (*Preservation*). Pemeliharaan yang melibatkan pemisahan, mengamankan dan pemeliharaan bukti fisik dan digital.
5. Koleksi (*Collection*). Mencakup rekaman adegan fisik dan duplikat bukti digital menggunakan standar prosedur yang berlaku.
6. Pemeriksaan (*Examination*). Melibatkan pencarian sistematis mendalam dari bukti yang berkaitan dengan kejahatan.
7. Analisa (*Analysis*). Menentukan makna, merekonstruksi potongan data dan menarik kesimpulan berdasarkan bukti yang ditemukan.
8. Persentasi (*Presetation*). Rangkuman dan penjelasan mengenai kesimpulan yang didapat.
9. Pengembalian Barang Bukti (*Returning Evidence*). Memastikan hak milik dan fisik dari bukti digital dikembalikan kepada pemilik aslinya.

D. Cloud Computing

NIST mendefinisikan cloud computing sebagai "sebuah model untuk kenyamanan, akses jaringan on-demand untuk menyatukan pengaturan sumber daya komputasi yang dapat dengan cepat ditetapka dan dirilis dengan usaha manajemen yang minimal atau interaksi denga penyedia layanan"[11]

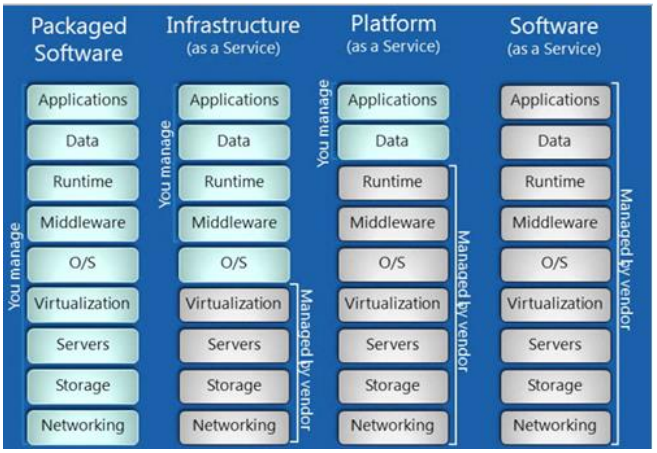
Karakteristik cloud computing yaitu:



Gambar 1. Karakteristik *cloud computing*

1. *On-demand self-service*
   Konsumen dapat menentukan kemampuan komputasi secara sepihak, seperti *server time* dan *network storage*, secara otomatis sesuai kebutuhan tanpa memerlukan interaksi manusia dengan masing-masing penyedia layanan.
2. *Broad network access*
   Kemampuan yang tersedia melalui jaringan dan diakses melalui mekanisme standar yang mengenalkan penggunaan berbagai *platform* (misalnya, telepon selular, tablet, laptop, dan *workstations*).
3. *Resourcer Pooling*
   Penyatuan sumberdaya komputasi yang dimiliki penyedia untuk melayani beberapa konsumen *virtual* yang berbeda, ditetapkan secara dinamis dan ditugaskan sesuai dengan permintaan konsumen. Pelanggan pada umumnya tidak memiliki kontrol atau pengetahuan atas keberadaan lokasi sumberdaya yang disediakan, tetapi ada kemungkinan dapat menentukan lokasi di tingkat yang lebih tinggi (misalnya, negara, negara bagian, atau *data center*). Contoh sumber daya termasuk penyimpanan, pemrosesan, memori, *bandwidth* jaringan, dan mesin *virtual*.
4. *Rapid elasticity*
   Kemampuan dapat ditetapkan dan dirilis secara elastis, dalam beberapa kasus dilakukan secara otomatis untuk menghitung keluar dan masuk dengan cepat sesuai dengan permintaan. Kemampuan yang tersedia yang sering kali tidak terbatas dan kuantitasnya dapat disesuaikan setiap saat.
5. *Measured Service*
   Sistem *cloud computing* secara otomatis mengawasi dan mengoptimalkan penggunaan sumber daya dengan memanfaatkan kemampuan pengukuran (*metering*) pada beberapa tingkat yang sesuai dengan jenis layanan (misalnya, penyimpanan, pemrosesan, *bandwidth*, dan *account* pengguna aktif). Penggunaan sumber daya dapat dipantau, dikendalikan, dan dilaporkan sebagai upaya memberikan transparansi bagi penyedia dan konsumen dari layanan yang digunakan.

Jenis Layanan Cloud Computing



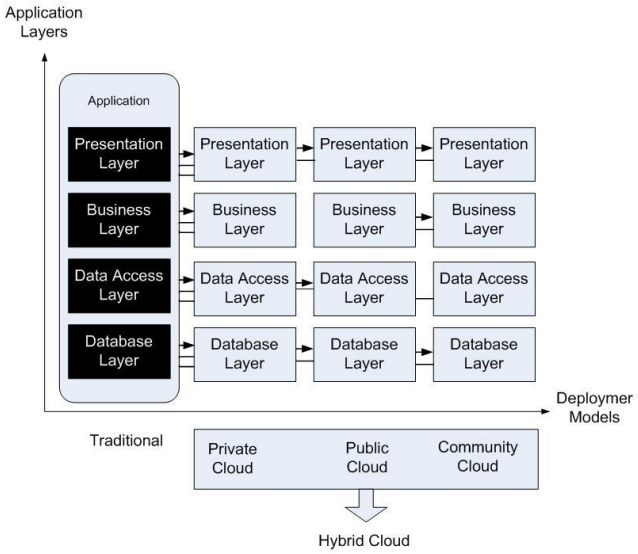
Gambar 2.Stack Layanan *cloud computing*

1. *Cloud software as a service (SaaS)*
   Kemampuan yang diberikan kepada konsumen untuk menggunakan aplikasi penyedia dapat beroperasi pada infrastruktur *cloud*. Aplikasi dapat diakses dari berbagai perangkat klien melalui antarmuka seperti *web browser* (misalnya, *email* berbasis *web*). Konsumen tidak mengelola atau mengendalikan

infrastruktur *cloud* yang mendasar termasuk jaringan, server, sistem operasi, penyimpanan, atau bahkan kemampuan aplikasi individu, dengan kemungkinan pengecualian terbatas terhadap pengaturan konfigurasi aplikasi pengguna tertentu. Contohnya adalah *Google Apps, SalesForce.com* dan aplikasi jejaring sosial seperti *Facebook.*

2. *Cloud Plaform as a service (PaaS)*
   Kemampuan yang diberikan kepada konsumen untuk menyebarkan aplikasi yang dibuat konsumen atau diperoleh ke infrastruktur *cloud computing* menggunakan bahasa pemrograman dan peralatan yang didukung oleh *provider*. Konsumen tidak mengelola atau mengendalikan infrastruktur *cloud* yang mendasar termasuk jaringan, server, sistem operasi, atau penyimpanan, namun memiliki kontrol atas aplikasi yang disebarkan dan memungkinkan aplikasi melakukan hosting konfigurasi. Contohnya yang sudah mengimplementasikan ini adalah *Force.com* dan *Microsoft Azure investment*.
3. *Cloud Infrastructure as a service (IaaS)*
   Kemampuan yang diberikan kepada konsumen untuk memproses, menyimpan, berjaringan, dan sumber komputasi penting yang lain, dimana konsumen dapat menyebarkan dan menjalankan perangkat lunak secara bebas, yang dapat mencakup sistem operasian aplikasi. Konsumen tidak mengelola atau mengendalikan infrastruktur *cloud* yang mendasar tetapi memiliki kontrol atas sistem operasi, penyimpanan, aplikasi yang disebarkan, dan mungkin kontrol terbatas komponen jaringan yang pilih (misalnya, *firewall host*). Contohnya seperti *Amazon Elastic Compute Cloud* dan *Simple Storage Service.*

Penyebaran cloud computing



Gambar 3. Model Penyebaran *Cloud Computing*

(microsoft.com)

Empat model penyebaran *cloud computing* [11]

1. *Private cloud*
   Infrastruktur *cloud* yang semata-mata dioperasikan bagi suatu organisasi. Ini mungkin dimiliki, dikelola dan dijalankan oleh suatu organisasi, pihak ketiga atau kombinasi dari beberapa pihak dan mungkin ada pada *on premis* atau *off premis.*
2. *Community cloud*
   Infrastruktur *cloud* digunakan secara bersama oleh beberapa organisasi dan mendukung komunitas tertentu yang telah berbagi *concerns* (misalnya; misi, persyaratan keamanan, kebijakan, dan pertimbangan kepatuhan). Model mungkin dikelola oleh organisasi atau pihak ketiga dan mungkin ada pada *on premis* atau *off premis.*
3. *Public cloud*
   Infrastuktur *cloud* yang disediakan untuk umum atau kelompok industri besar dan dimiliki oleh sebuah organisasi yang menjual layanan *cloud.*
4. *Hybrid cloud*
   Infrastruktur *cloud* merupakan komposisi dari dua atau lebih *cloud* (swasta, komunitas, atau publik) yang masih entitas unik namun terikat bersama oleh standar atau kepemilikan teknologi yang menggunakan data dan portabilitas aplikasi (e.g., *cloud bursting for load-balancing between clouds*).

E. Tools

Tools yang digunakan dalam melakukan investigasi digital forensik ada yang khusus dan ada yang digunakan

untuk keperluan umum lain di luar digital forensik. Tools digital forensik sebagian ada yang bisa digunakan secara gratis dengan batas waktu tertentu dan ada yang berbayar dengan fitur lebih lengkap, penelitian ini menggunakan tools sebagai berikut:

1. Belkasoft Evidence Center
   Merupakan salah *tools* yang digunakan dalam proses digital forensik. *Software* forensik *all-in-one* ini dapat menemukan lebih dari 700 jenis artefak, termasuk lebih dari 100 aplikasi *mobile,* semua format utama dokumen, *browser, email client,* sejumlah format foto dan *video*, *instant messenger, social network, file* sistem dan *registry, P2P* dan *tools transfer file*, dll. *Toolkit* ini akan cepat mengekstrak bukti digital dari berbagai sumber dengan menganalisis *hard drive, image drive , memory dumpt, iOS, Blackberry* dan *backup Android, UFED, JTAG* dan *chip-off dumpt*. Ekstraksi data dari berbagai operating sistem utama. Baik komputer maupun *mobile: Windows, Linux, MacOS X, iOS, Android, Windows Phone, Blackberry.*
2. *DumpIt*
   DumpIt merupakan perpaduan dari dua *tools* yaitu *win32dd* dan *win64dd*, digabungkan menjadi satu *executable* yang digunakan untuk melakukan akusisi *physical memory*. DumpIt dirancang untuk diberikan kepada pengguna non-teknis menggunakan *removable drive USB*. *DumpIt* akan mengambil *snapshot* dari phsycal memory dan menyimpan ke *folder* di mana eksekusi DumpIt berada.
3. *Folder2Iso*
   Folder 2Iso merupakan *tools* untuk membuat *file* dengan ekstensi *.iso* dari suatu *folder*. *Tools* ini bersifat *portable* sehingga bisa digunakan melalui *USB.*
4. *Passwordfox*
   PasswordFox adalah *password recovery tools* yang dapat meilhat *username* dan *password* yang disimpan pada *browser Mozilla Firefox*
5. *MD5 & SHA-1 Checksum Utility*
   MD5 & SHA-1 Checksum Utility adalah *portable tool* yang menghasilkan dan memverifikasi *hash kriptografi MD5 dan SHA-1*. Fungsi *hash* biasanya digunakan untuk menjadga terhadap perubahan berbahaya untuk data yang dilingungi dalam berbagai macam aplikasi perangkat lunak, internet dan keamanan termasuk *digital signature*s dan bentuk lain dari otentifikasi.

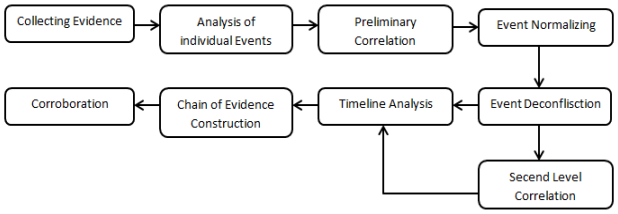
III. METODOLOGI PENELITIAN

Metode yang digunakan dalam penelitin ini mengacu pada tahapan proses EEDI [9], metode ini dilakukan dengan menganalisa semua barang bukti yang ditemukan, namun untuk penelitian ini investigasi hanya dilakukan pada sisi desktop. Skenario kasus yang dijalankan pada simulasi di laboratorium jaringan komputer adalah kasus penyalahgunaan private cloud computing oleh karyawan yang melakukan kejahatan pengiriman barang ilegal dengan memanfaatkan jasa kirim milik perusahaan. Karyawan tersebut mengganti file daftar pengiriman barang yang seharusnya dikirim oleh perusahaan dengan daftar barang illegal pada private cloud milik perusahaan. Digital investigator memiliki peran untuk mendapatkan bukti-bukti digital yang menunjukkan kejahatan yang dilakukan oleh terduga pelaku. Setelah skenario dijalankan, tahap selanjutnya adalah melakukan investigasi menggunakan metode EEDI:

1. *Collecting Evidence* yaitu mengumpulkan barang bukti desktop atau laptop di TKP yang diketahui dan diidentifikasi sebagai perangkat yang terlibat pada aktivitas kejahatan *cyber.* Barang bukti laptop tersebut kemudian dicari *file folder* yang dapat dijadikan bukti digital terkait kasus kejahatan. Proses selanjutnya melakukan imaging terhadpat bukti digital untuk mendapatkan duplikat asli dari bukti digital
2. *Analysis of Individual Events* yaitu menganalisis masing-masing peristiwa yang terdapat pada bukti digital untuk mendapatkan informasi yang menunjukkan tindak kejahatan. Analisa dilakukan terhadap *image* artefak *browser*, *logs miRC*, *file* yang terdapat pada folder own*cloud* client dan *virtual memory.*
3. *Preliminary Correlation* yaitu mencari keterkaitan informasi yang terdapat pada bukti digital dengan kejahatan yang terjadi. Informasi yang saling berkaitan ini kemudian akan disimpan dan akan dibentuk menjadi rantai bukti yang nantinya dapat menjelaskan apa yang sebenarnya terjadi pada kasus kejahatan ini.
4. *Event Normalizing* yaitu melakukan normalisasi informasi yang didapat dari bukti digital, sehingga yang digunakan hanya dari satu sumber bukti digital, seperti keterangan waktu yang terdapat pada bukti digital tersebut berbeda (waktu lokal dan *UTC*) jika ditemukan keadaan seperti ini maka perlu dilakukan *event normalizing*. Tahap ini dilakukan untuk menormalisasikan peristiwa tersebut dengan menyamakan waktu, tujuannya agar tidak membingungkan saat investigasi ataupun saat pembuatan laporan investigasi.
5. *Event Deconfliction* Tahapan ini melakukan penggabungan peristiwa-peristiwa sama yang muncul beberapa kali, ketika menemukan kejadian ini maka perlu dilakukan *deconfliction*, yaitu menggabungkan peristiwa-peristiwa yang sama tersebut menjadi satu, tujuannya adalah agar tidak perlu memasukkan peristiwa sama yang terjadi berulangkali.
   Contohnya ketika terdapat peristiwa akses web, akses yang terlihat dilakukan berulang kali dengan waktu yang sama, maka hal yang harus dilakukan adalah cukup

mengambil satu persitiwa saja, tidak perlu semua peristiwa tersebut diambil dan dicatat ke dalam laporan investigasi.

6. *Second Level Correlation* yaitu melakukan keterkaitan tahap kedua, jika berdasarkan korelasi pertama cukup maka korelasi tahap kedua ini tidak perlu dilakukan.
7. *Timeline Analysis* yaitu Proses ini membuat timeline garis waktu bukti digital, bukti digital yang telah melawati tahapan-tahapan sebelumnya, kemudian diurutkan berdasarkan timestamp pada bukti digital itu sendiri. Proses ini akan berguna pada tahapan *Chain of Evidence* atau pembuatan rantai bukti
8. *Chain of Evidence Construction* yaitu membuat rantai bukti atau kejadian sesuai berdasarkan tahapa sebelumnya, Peristiwa-peristiwa yang telah melalui tahap-tahap sebelumnya lalu dibentuk berdasarkan informasi yang didapat dari masing-masing peristiwa sehingga membentuk sebuah rantai bukti yang menjelaskan rentetan kejadian yang dilakukan pelaku dalam kejahatan.
9. *Corroboration* yaitu Tahap ini dilakukan untuk menguatkan hasil investigasi dan meyakinkan bahwa pelaku tersebut benar-benar melakukan kejahatan, penguatan dapat berupa data tentang kegiatan pelaku di perusahaan seperti data absensi, prilaku pelaku saat bekerja di perusahaan. Setelah penguatan diyakini cukup maka tahap selanjutnya adalah pembuatan laporan akhir investigasi yang nantinya akan digunakan dalam persidangan.

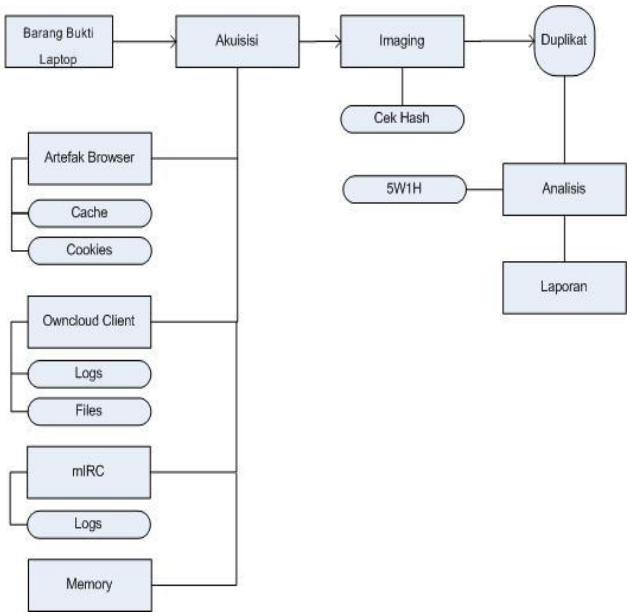


Gambar 4. Tahapan *End to End Digital Investigation*

(Peter Stephenson 2003)

IV. HASIL PENELITIAN

Berdasarkan skenario kasus kejahatan, Hasil dari penelitan ini sebagai berikut:



Gambar 5. Alur Investigasi

Gambar 5 merupakan alur yang dilakukan pada penelitian ini untuk melakukan investigasi pada sisi *desktop* (laptop).

Proses Akuisisi

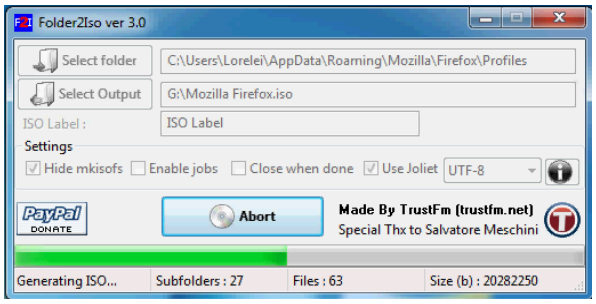
Merujuk pada gambar 5 telah ditentukan *file* dan *folder* yang akan diakusisi, berikut ini adalah strukturnya:

TABEL I

STRUKTUR *FILE* DAN FOLDER BUKTI DIGITAL PADA LAPTOP

No	Bukti Digital	Direktori
1	*Cache Mozilla Firefox*	C:\Users\Lorelei\AppData\Local\Mozilla\Firefox\Pro*files*\8kqzk9a1.default
2	*Cookies Mozilla Firefox*	C:\Users\Lorelei\AppData\Roaming\Mozilla\Firefox\Pro*files*\8kqzk9a1.default.
3	*Logs mIRC*	C:\Users\Lorelei\AppData\Roaming\mIRC*logs*
4	*File folder Owncloud Client*	C:\Users\Lorelei\own*Cloud*
5	*Virtual Memory*	C:\page*file*s.sys

Setelah menentukan bukti digital yang akan diakusisi, proses selanjutnya adalah melakukan *imaging* untuk menggandakan barang bukti. *Tools* yang digunakan untuk melakukan *imaging* menggunakan *folder2iso*. Proses *imaging* perlu dilakukan karena investigasi digital forensik dilakukan dengan menganalisis hasil *imaging* bukti digital tersebut untuk menghindari terjadinya perubahan data pada bukti digital asli.



Gambar 6. Proses Imaging

Bukti digital yang telah menjadi *image* kemudian dilakukan pemeriksaan nilai *hash* menggunakan *tools MD5 and SHA Checksum Utility*. Fungsi *hash* adalah fungsi yang menerima masukan string atau pesan yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap atau *fixed*. *Hash* memang umumnya digunakan untuk mengecek integritas dari sebuah pesan atau *file*.

Tujuan pemeriksaan nilai *hash* terhadap barang bukti serta *file* adalah untuk memastikan keaslian *file* terhadap barang bukti. Seandainya nilai *hash file* tidak sama dengan nilai *hash* dari barang bukti asli, maka telah terjadi modifikasi terhadap *file*. Berikut hasil pemeriksaan nilai *hash*

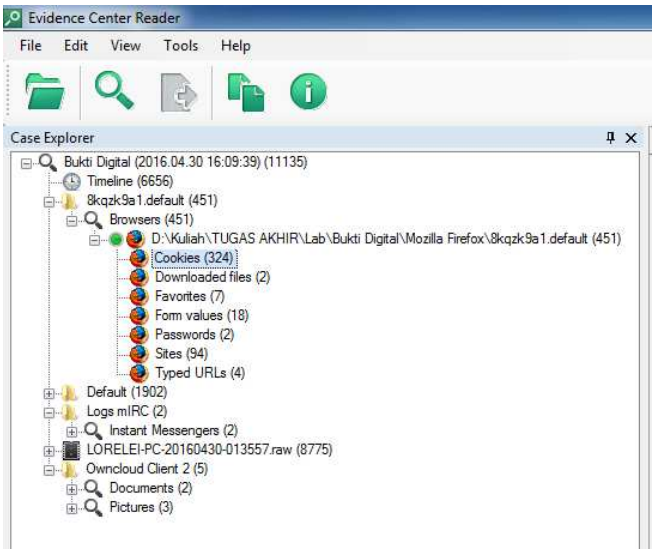
TABEL II

NILAH *HASH* BUKTI DIGITAL

No	Nama *File*	Nilai *Hash* MD5
1	Mozilla Firefox	4A4F8C132225E766D84750 35417DC340
2	Mozilla Firefox 2	C71326D7188B492B2A7D74 8B7EE676AA
3	Logs mIRC	FDA7B235ED373DC1627C2 9BF73D6B8A3
4	Owncloud Client 2	7337ABCF29853754B9CC83 7EC42B4629
5	Virtual Memory	9EF5619E37B87B1AA926A 18D5762422B

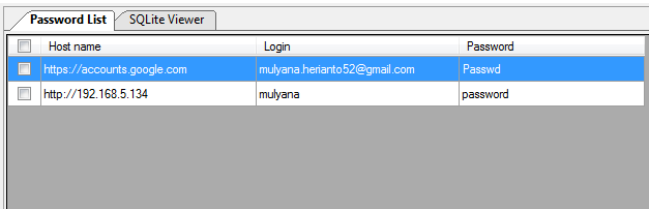
Proses Analisis

Proses analisis yang dilakukan menggunakan aplikasi *Belkasoft Evidence Center*, *file image* yang telah didapatkan dari barang bukti kemudian diekstrak lalu dibuka menggunakan *Belkasoft*. Proses analisis dilakukan secara mendalam dengan melihat informasi yang ada pada bukti digital.



Gambar 7. Artfeak *Browser Mozilla Firefox*

File image yang periksa pertama adalah artefak browser mozilla firefox. Merujuk gambar di atas terdapat 7 kategori yang terekstrak dari *mozilla firefox.iso, yaitu Cookies, Download Files, Favorites, Form Values, Passwords, Sites, Typed URLs,* masing-masing mempunyai informasi dengan jumlah yang berbeda.



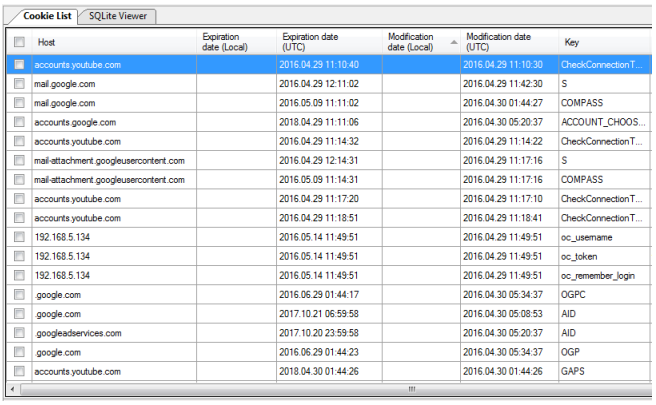
Gambar 8. U*sername* dan P*assword*

Gambar 8 merupakan hasil investigasi yang menunjukkan *username* dan *password email* milik pelaku yang tersimpan pada artefak *Mozilla firefox*, namun *password* yang tersimpan telah terenkripsi, maka perlu dilakukan dekripsi *password* menggunakan *decrypt tool.*

Gambar 9. *Decrypted Password*

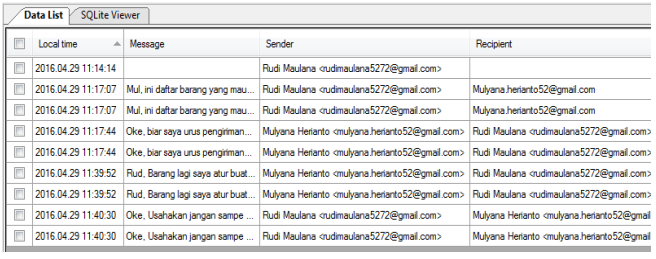
e-ISSN : 2443-2229

Gambar 9 Merupakan password yang telah didekrip, *Username* dan *password* tersebut jika perlu dapat digunakan pihak investigator untuk melakukan *login* pada *email* pelaku untuk mendapatkan bukti digital lebih lanjut.



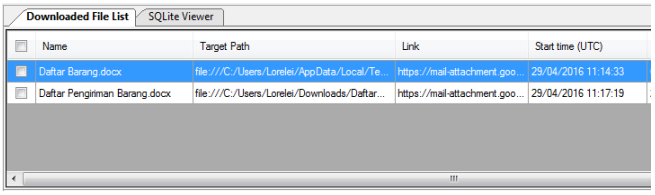
Gambar 10 Cookies Mozilla firefox

Investigasi dilanjutkan dengan melihat data *cookies* pada *mozilla firefox*, merujuk gambar 10, pada tanggal 29-04-2016 pukul 11:11:02 pelaku sedang membuka *email* miliknya, meilhat pada kolom *host* dapat diketahui bahwa pelaku sedang membuka *email* yang memiliki *attachment* sebuah *file.* Melihat data tersebut, diduga pelaku telah berkirim *email* dengan seseorang dan pada salah satu *email* tersebut terdapat *file attachment* yang dikirim. Maka untuk lebih memastikan, perlu dilihat apa isi dari *email* tersebut. *Email* tersebut dapat dilihat. *Browser* selain *mozilla firefox* pun memiliki letak *file* dan *folder* yang bisa dijadikan bukti digital, namun letak direktorinya berbeda sesuai browser masing-masing, ketika bukti digital dari *browser* lain (*cache, cookies, password* dll.) dibuka menggunakan *belkasoft*, data yang dihasilkan kurang lebih akan sama. Penelitian yang dilakukan hanya menggunakan *browser Firefox* saja.



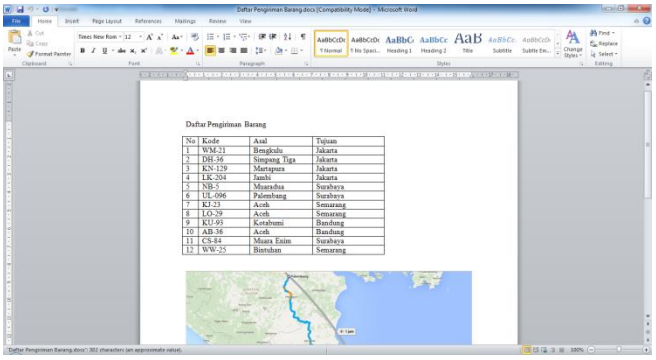
Gambar 11.Komunikasi berupa *e-mail*

Gambar 11 merupakan hasil investigasi yang didapat dari *virtual memory*, hasilnya didapatkan komunikasi *email* antara pelaku dan seseorang dengan alamat *email* rudimaulana5272@gmail.com yang isinya rencana kejahatan yang dilakukan serta terdapat *attachment file* dokumen *.docx* yang diterima oleh pelaku.



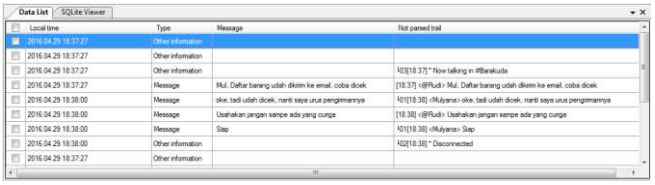
Gambar 12. File Download

Gambar 12 Merupakan *file* yang didownload oleh pelaku, terlihat *url download file* tersebut berasal dari *attachment gmail*. *File* dokumen tersebut dapat dilihat dengan cara melakukan *eksport file* dari *image folder owncloud client*



Gambar 13.*File* dokumen Daftar Pengiriman Barang.docx

Gambar 13 Merupakan isi dari *file* dengan nama Daftar Pengirima Barang.*docx*



Gambar 14. *Logs mIRC*

Merujuk pada gambat di atas, interaksi yang dilakukan pelaku adalah dengan seseorang bernama rudi melalui aplikasi *chatting mIRC*, lalu pada informasi yang didapat dari *gmail* orang yang berinteraksi dengan pelaku muncul kembali dengan nama rudi maulana dan alamat *email*nya rudimaulana5272@gmail.com. Berdasarkan isi dari *chatting mIRC* dan pesan *email* dapat disimpulkan bahwa pelaku berinteraksi dengan sesorang bernama lengkap Rudi Maulana yang memiliki alamat mail rudimaulana5272@gmail.com, maka data yang diambil adalah data dari *Gmail Live Ram* yang tersimpan pada *virtual memory.*

Setelah proses analisis terhadap image bukti digital selesai, proses selajutnya membuat *timeline* bukti digital. *Timeline* dibuat berdasarkan waktu (*timestamp*) yang terdapat pada bukti digital artefak *browser, virtual memory, logs mirc.*

TABEL III
TIMELINE BUKTI DIGITAL

No	Waktu	Peristiwa
1	11:10:29 29-04-2016	*Login email*
2	11:17:07 29-04-2016	Menerima *email* berisi *attachment file*
3	11:17:19 29-04-2016	Mengunduh *attachment file* dokumen dari email masuk dengan nama "Daftar Pengiriman Barang.docx"
4	11:49:51 29-04-2016	*Login Owncloud*
5	12:06:15 29-04-2016	Mengunggah *file* "Daftar Pengiriman barang.docx"
6	18:37:27 29-04-2016	*Chatting* melalui *mIRC* (awal mulai chatting)
7	18:38:00 29-04-2016	*Chatting* melalui *mIRC* (akhir *chatting*)

Proses selanjutnya adalah membuat *Chain of Evidence Construction* atau rekonstruksi bukti digital untuk menjelaskan seperti apa kejahatan yang dilakukan oleh pelaku. Pembuatan tahapan ini berdasarkan timeline yang telah dibuat sebelumnya. Berikut ini adalah rekonstruksi bukti digital

"*Tanggal 29.04.2016 pukul 11:10:29 pelaku menerima email dari seseorang bernama Rudi maulana, isi email tersebut berisi attachment file dokumen. Pelaku kemudian mengunduh file tersebut dengan nama "Daftar Pengiriman Barang", setelah file tersebut diunduh, pelaku kemudian mengunggah file tersebut ke owncloud milik perusahaan. Setelah selesai mengunggah file tersebut, pelaku mengirim email pada rudi untuk memberitahu bahwa file yang tersebut telah diunggah dan pengiriam barang sedang diatur oleh pelaku. Selain menggunakan email pelaku dan rudi melakukan chatting menggunakan mIRC, isi dari chatting tersebut masih mengenai rencana yang akan mereka lakukan.*"

Pembuatan Laporan Forensik

Berdasarkan investigasi terhadap bukti digital pada laptop pelaku, didapatkan informasi yang menunjukkan bahwa pelaku telah melakukan kejahatan dengan memanfaatkan perusahaan tempat pelaku bekerja. Hasil investigasi tersebut kemudian dibuat menjadi laporan forensik dan akan diberikan kepada pihak majelis hakim untuk digunakan sebagai dasar untuk mengambil keputusan dalam persidangan nanti. Pengadilan akan merima laporan tersebut sebagai alat bukti karena minimal tiga bukti digital telah ditemukan, yaitu struktur file dan folder bukti digital telah diketahui, timestamp, , email yang berisi rencana kejahatan, file dokumen kejahatan, chatting logs mIRC [21].

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian, maka dapat diambil kesimpulan Investigasi terhadap *desktop PC* yang terhubung pada layanan *private cloud computing* dilakukan dengan mencari bukti digital yang terkait langsung dengan kasus kejahatan, yaitu *browser*, aplikasi *chatting mIRC*, aplikasi *owncloud client* dan *virtual memory*. Bukti digital yang didapatkan diantaranya adalah aktivitas yang tersimpan pada *cache browser, username password, logs chatting mIRC*, *e-mail*, *file* dalam *MS Word*.

Investigasi digital forensik menggunakan metode EEDI memiliki potensi kelemahan pada masalah waktu investigasi jika diterapkan pada kasus nyata dengan barang bukti yang banyak, meski telah diketahui mana barang bukti yang terkait langsung dengan kejahatan namun berdasarkan tahapan *collecting evidence* maka semua benda elektronik yang ditemukan di TKP harus dikumpulkan, koneskuensinya proses investigasi akan berlangsung lama, namun akan bermanfaat ketika menangani kasus dengan ditemukan banyaknya barang bukti dan belum diketahui sama sekali barang bukti mana yang terkait kasus kejahatan.

B. Saran

Saran-saran yang dapat diberikan sebagai bahan penelitian lanjut adalah sebagai berikut:

1. Penelitian ini menggunakan Belkasoft untuk melakukan proses analisis, Belkasoft merupakan tool berbayar dan dapat digunakan secara gratis selama 1 bulan. Saran untuk penelitian selanjutnya diharapkan dapat menggunaka tool lain, seperti EnCase yang merupakan tools berbayar untuk proses investigasi digital forensik dengan fitur lebih lengkap untuk mendapatkan hasil akusisi dan ekstraksi yang lebih maksimal dalam penyelidikan.

DAFTAR PUSTAKA

[1] M. Ahmed and M. A. Hossain, "*Cloud Computing* And Security Issues In The *Cloud*," vol. 6, no. 1, pp. 25–36, 2014.
[2] Asrizal, "Digital Forensik," pp. 1–15.
[3] S. and L. Association of Digital Forensics, "Journal of Digital Forensics, Security and Law," vol. 7, no. 1, 2012.
[4] B. D. Carrier, "Hypothesis-Based Approach To Digital Forensic Investiga Ations," p. 190, 2006.
[5] B. D. Carrier and E. H. Spafford, "An Event-Based Digital Forensic Investigation Framework ∗," pp. 1–12, 2004.
[6] S. Coty, "Computer Forensics and Incident Response in the *Cloud*."
[7] DFRWS, "DIGITAL FORENSIC RESEARCH CONFERENCE A Road Map for Digital Forensic Research A Road Map for Digital Forensic Research," 2001.
[8] G. Grispos and W. B. Glisson, "Calm Before the Storm : The Challenges of *Cloud Computing* in Digital Forensics," vol. 4, no. 2, pp. 28–48, 2012.
[9] E. Information and S. Technical, "A Comprehensive Approach To Digital Incident Investigation," pp. 1–13, 2003.
[10] M. Kohn, "Framework for a Digital Forensic Investigation 1."

[11] NIST (National Institute of Standards and Technology), "The attached DRAFT document (provided here for HISTORICAL purposes) has been superseded by the following publication :," 2012.
[12] D. J. Ohana, "Do Private and Portable Web Browsers Leave Incriminating Evidence ? A Forensic Analysis of Residual Artifacts from Private and Portable Web Browsing Sessions," pp. 135–142, 2013.
[13] Z. Ramadhan, "Digital forensik dan penanganan pasca insiden," 2008.
[14] D. Reilly, C. Wren, T. Berry, L. John, D. Reilly, C. Wren, and T. Berry, "*Cloud Computing* : Pros and Cons for Computer Forensic Investigations," vol. 1, no. 1, pp. 26–34, 2011.
[15] P. A. Rt, "Digital Evidence and Computer Crime, Third Edition," 2011.
[16] S. R. Selamat, R. Yusof, and S. Sahib, "Mapping Process of Digital Forensic Investigation Framework," vol. 8, no. 10, pp. 163–169, 2008.
[17] L. Slusky, "*Cloud computing* and computer forensics for business applications," pp. 1–10.
[18] S. Universitas, G. Mada, and G. Mada, "Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada," vol. 6, no. 2, 2012.
[19] Y. Yusoff, R. Ismail, and Z. Hassan, "Common Phases Of Computer Forensics Investigation Models," vol. 3, no. 3, pp. 17–31, 2011.
[20] Feri Sulianta, Komputer Forensik: Elex Media Komputindo, 2008.
[21] Purwanti, Indah TRI "Digital forensik sebagai alat bukti tindak pidana 1," pp. 1–19, 2008.