Penerapan *Metode ADAM* Pada Proses Investigasi Layanan *Private Cloud Computing*

Nur Widiyasono[#1], Imam Riadi[*2], Ahmad Luthfi[#3]

[#] *Magster Teknik Informatika, Universitas Islam Indonesia*
Jl. Kaliurang KM 14,5 Yogyakarta 55584

[1]nur.widiyasono@unsil.ac.id

[3]ahmad.luthfi@uii.ac.id

[*] *Teknologi Industri, Universitas Ahmad Dahlan*
Jl. Prof. Dr. Soepomo, S.H. Janturan Yogyakarta 55164

[2]imam.riadi@is.uad.ac.id

***Abstrak*— Layanan *Private Cloud Computing* memiliki potensi terjadinya penyalahgunaan yang dilakukan oleh internal di dalam perusahaan, sebagai contoh kasus yang yang terjadi di RSIA XYZ. Penyalahgunaan tersebut terjadi dikarenakan adanya kelemahan sistem yang digunakan ,ataupun sebab lain. Proses akuisisi data pada layanan *cloud computing* penanganannya tidaklah sama dikarenakan jenis dan karakteristik layanan *cloud computing* tersebut. Isu mengenai masalah realibilitas data atau bagaimana proses data digital evidence didapatkan, pada persidangan akan menjadi perhatian khusus bagi majelis hakim, sehingga untuk menangani masalah tersebut digunakanlah metode *ADAM* (*The Advance Data Acquisition Model*), sayangnya metode tersebut belum pernah dilakukan evaluasi secara independen. Penelitian ini menggunakan metode *ADAM* di dalam melakukan investigasi kasus pada layanan *private cloud computing* dan telah berhasil 100% menerapkannya, kemudian kontribusi pada penelitian ini telah menemukan penyebab potensi terjadinya penyalahgunaan layanan aplikasi *owncloud* tersebut.**

Kata kunci*— *Akusisi, ADAM, Cloud, Forensik, Investigasi

I. PENDAHULUAN

Layanan *cloud computing* merupakan teknologi yang banyak ditawarkan oleh *Cloud Service Provider (CSP)* antara lain jenis yang ditawarkan adalah *platform as a service (PaaS), infrastructure as a service (IaaS)* dan *software as a services (SaaS)*. Layanan tersebut memberikan berbagai kemudahan dan keuntungan bagi konsumen antara lain adalah *self-service provisioning, Elasticity*, dan *pay per use*. Layanan *cloud* terbagi menjadi 4 bagian yaitu *private clouds, community cloud, public cloud dan hybrid cloud* [1].

Private cloud dibangun untuk kebutuhan organisasi yang mencakup seluruh *cloud infrastructure* termasuk sumber daya *hardware* yang dimiliki organisasi tersebut. *Community cloud* adalah *cloud* yang digunakan secara bersama oleh organisasi yang memiliki jenis bisnis yang sama. *Public Cloud* adalah *cloud* yang dibangun dan digunakan oleh organisasi secara publik untuk kepentingan bisnisnya. *Hybrid Cloud* merupakan kombinasi dari *private, community* dan *public cloud.*

Layanan *cloud* yang ditawarkan diantaranya adalah *hosted desktop* yang merupakan mesin *virtual* pada *cloud*. Layanan ini memiliki aplikasi dan data-data yang berada pada *remote data center*. Pemilik layanan ini dapat melakukan akses aplikasi dan data melalui *computer desktop*. Layanan *hosted desktop* ini dapat disalahgunakan untuk melakukan kejahatan *cyber* [2]. Penyalahgunaan layanan ini dapat terjadi juga dikarenakan adanya kelemahan *(bugs)* dari sisi keamanan sistem tersebut. Menurut *NIST*, tahapan pada *cloud computing forensics* adalah *identification, collection, preservation, examination, interpretation* and *reporting of digital evidence.*

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*. Proses akusisi data secara *live system* maksudnya adalah proses untuk mendapatkan bukti digital dilakukan ketika sistem dalam keadaan hidup sedangkan *write block system* adalah proses akuisisi data yang dilakukan ketika sistem dalam keadaan mati misalnya proses akuisisi data pada *harddisk*.

Proses akuisisi data pada layanan *cloud computing* tidak dapat diperlakukan sama dikarenakan karakteristik layanan tersebut tidak sama [4].

Solusi yang diberikan pada masalah *cloud forensics* yaitu dengan memanfaatkan *logging framework* hal tersebut digunakan untuk memastikan bahwa *data log* yang berhasil dikumpulkan dapat digunakan untuk proses investigasi *forensic* [5]. Ada beberapa metode yang ditawarkan antara lain dengan metode *ADAM (The Advance Data Acquisitions Model)*. Metode ini dikembangkan dalam kerangka untuk mengatasi masalah reabilitas data yaitu bagaimana *data digital evidence* didapatkan dan hal ini akan menjadi perhatian khusus di persidangan namun sayangnya metode *ADAM* belum pernah dilakukan evaluasi secara independent [6].

II. KAJIAN PUSTAKA

Cloud Computing Forensic adalah aplikasi ilmu forensika *digital* yang berada lingkungan *cloud computing*, dan secara teknis yang dilakukan terdiri dari pendekatan *forensic hybrid* seperti *remote, virtual, network, live, thin-client* terhadap bukti digital dan secara organisasi melibatkan interaksi antara *actor cloud computing* untuk penyelidikan internal dan

eksternal, serta secara hukum menyiratkan multi-yuridiksi dan situasi multi-penyewa [7].

Laporan dari *National Institute of Standards and Technology* mencatat bahwa panduan untuk memperoleh dan melakukan forensik pada layanan *cloud computing* dan menyarankan bahwa pedoman terbaik yang ada dan masih berlaku untuk melakukan forensik *digital* di lingkungan *cloud computing*[8]. Metode forensik *digital* yang ada, sudah tidak cocok untuk lingkungan *cloud computing* [9].

Pedoman dan panduan pada pengumpulan bukti digital sudah langka dan ketinggalan jaman. Tidak ada pedoman khusus untuk mengumpulkan bukti digital di *Cloud Computing* [10]. Penelitian yang ditemukan pada *cloud computing* ini sedikit, misalnya bagaimana untuk mengambil data dari layanan *cloud* secara forensik suara [11].

Pengamatan serupa digaungkan oleh sejumlah praktisi forensik digital, termasuk Direktur US Departemen Pertahanan Laboratorium Komputer Forensik dan Kepala Ilmuwan di *US Air Force Research Laboratory Information Directorat* yang mengemukakan bahwa " penelitian diperlukan dalam domain *cyber*, terutama dalam *cloud computing*, untuk melakukan identifikasi dan melakukan klasifikasi aspek unik di mana dan bagaimana bukti digital dapat ditemukan. Titik akhir seperti perangkat mobile juga berperan meningkatkan kompleksitas domain ini. Bukti jejak dapat ditemukan di *server*, *switch*, *router*, ponsel, dan lain-lain[12].

Sudut pandang hukum, sistem *cloud computing* memiliki potensi tingkat kesulitan yang tinggi untuk melakukan proses analisis *forensic computer* seperti halnya untuk mendapatkan dan melakukan analisis bukti digital dengan standar yang sama seperti pada sistem server tradisional [13]. Hal tersebut disebabkan adanya kesulitan dalam membangun data-data yang disimpan atau diproses oleh *software* khusus. Penelitian pada tahap "*collection*" menjadi proses yang jauh lebih rumit di lingkungan *cloud computing* karena lokasi fisik data, distribusi data di beberapa *server* atau perangkat penyimpanan dan yurisdiksi, dan lain-lain[10][14].

Pembahasan pada framework NIST tentang identifikasi (*identification*) dan pelestarian (*preservation*) sebagai bagian dari fase koleksi (*collection*) sehingga hal ini menunjukkan bahwa fase identifikasi pada *cloud computing* lebih penting, sedangkan fase pelestarian harus bekerja sama dengan *cloud service provider* , kedua langkah tersebut penting di dalam penyelidikan pada *cloud computing*. Fase identifikasi dan fase pelestarian merupakan sumber bukti yang harus secara serentak dan secepat mungkin [17][15]. Contoh jika sumber data sudah teridentifikasi, maka harus segera menghubungi *cloud service provider* untuk memulai pelestarian.

Peran artefak (misalnya metadata) dalam analisis forensik dan (calon) hilangnya artefak ini ketika data dikumpulkan dari lingkungan *cloud computing*. Jika metadata (misalnya pembuatan / modifikasi tanggal *file*, dan *log* kepemilikan (pengguna) yang hilang selama proses pengumpulan, ini sangat berdampak kemampuan peneliti forensik untuk melakukan investigasi dengan standar yang dibutuhkan oleh pengadilan [16].

Proses forensika digital dapat dibagi menjadi empat fase yang berbeda :

- Koleksi artefak (baik bukti digital dan bahan pembantu) yang dianggap memiliki nilai potensial untuk dikumpulkan.
- Pelestarian artefak asli dengan cara yang handal, lengkap, akurat, dan dapat diverifikasi.
- Analisis penyaringan artefak untuk menghilangkan atau masuknya barang-barang yang dianggap berharga.
- Presentasi di mana bukti disajikan untuk mendukung penyelidikan

Secara tradisional, ada dua kategori forensika digital yaitu, *static digital* atau "*write block"* dan "*live forensic*", Zimmerman dan Glavach berpendapat bahwa ada dua kategori sebagai hasil dari *evolusi forensic* untuk menciptakan dan mendokumentasikan insiden secara canggih [17].

III. METODOLOGI PENELITIAN

Alur proses tahapan penelitian dapat digambarkan seperti Gambar 1 dibawah ini:

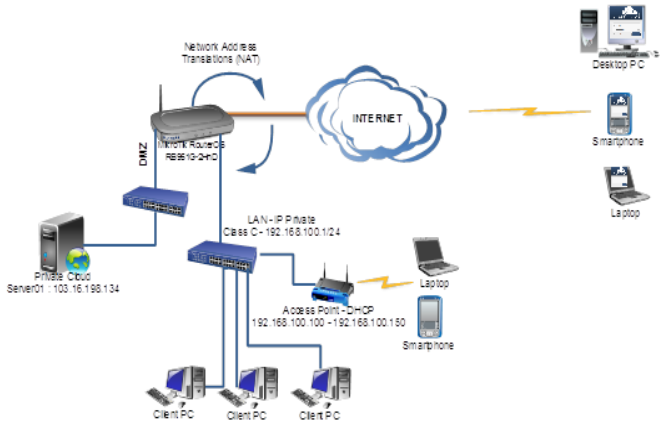
Gambar 1 Metode Penelitian

Kajian Penelitian terdahulu dilakukan untuk mengetahui masalah-masalah yang ada pada proses investigasi layanan *cloud computing* terutama yang terkait dengan proses akusisi data layanan *cloud computing*, metoda-metoda yang digunakan untuk melakukan proses akuisisi data, serta yang melatar belakangi isu dibalik metoda *ADAM*, sehingga dapat menunjang pada tujuan akhir dilakukannya penelitian ini.

Persiapan sistem merupakan tahapan dibangunnya layanan *private cloud computing* dengan menggunakan platform sistem operasi *Microsoft Windows 2008 Advances server, VirtualMachine (VMware), OwnCloud-5.0.5 Server* dengan memberikan *ip public* maka layanan *private cloud* ini dapat diakses melalui jaringan internet, maupun jaringan local dan hotspot. Layanan ini juga dapat diakses dengan menggunakan *pc-desktop, notebook* ataupun *smartphone*.

Studi kasus yang digunakan pada simulasi dilaboratorium jaringan komputer adalah kasus RSIA di kota Tasikmalaya yang namanya disamarkan menjadi RSIA XYZ. Kasus ini merupakan contoh terjadinya penyalahgunaan oleh seorang karyawan yang membocorkan rahasia perusahaan tersebut kepada pihak *competitor*. *Private Digital Investigator* memiliki tugas untuk mendapatkan bukti-bukti digital yang sangat potensial yang terdapat pada sisi layanan *private cloud* , *pc desktop* ataupun *smartphone* yang digunakan tersangka. Diketahui setiap karyawan pada perusahaan RSIA XYZ dapat menggunakan fasilitas layanan *private cloud* ini sehingga dimungkinkan terjadi penyalahgunaan fasilitas tersebut untuk membocorkan rahasia perusahaan kepada kompetitornya.

Adapun topologi jaringan seperti pada gambar 2 dibawah ini:



Gambar 2 Konseptual Akses layanan *private cloud*

Investigasi terhadap simulasi kasus yang menggunakan layanan *private cloud computing*. Investigasi yang dilakukan diawali pada layanan *private cloud computing* atau dari sisi *server*, kemudian dari sisi *network* yaitu melakukan monitoring terhadap *traffic data* yang keluar atau masuk ke dalam *server* layanan *private cloud computing* dan mendapatkan *digital evidence* pada *layer sessions* (*layer 5* pada *7 OSI layers*) dengan menggunakan *tool Wiresharks*, kemudian melakukan investigasi terhadap *desktop* atau *laptop* serta *smartphone* yang terhubung ke layanan tersebut. Tolak ukur kesuksesan didalam melakukan investigasi adalah dapat diketahuinya lokasi atau posisi bukti digital baik yang berada di sisi *private cloud server*, *pc desktop*, *laptop* ataupun *smartphone*, disamping itu parameter lainnya adalah *ip source*, *mac-address*, *username* dan *password*, *data log sistem* , dapat membuka *file enkripsi*, sumberdaya *(resources)* lainnya yang dapat dijadikan bukti digital tambahan, kemudian bukti digital tersebut dapat dilakukan verifikasi dan kesesuaian antara bukti digital yang terdapat pada sisi *private cloud server*, *pc desktop*, *laptop* dan *smartphone.* Investigasi pada contoh kasus ini menggunakan metode *ADAM* (*The Advance Data Acquisitions Model*) yang memiliki 3 tahap yaitu:

(1) Perencanaan Awal *(Initial Planning)*: Seorang *senior investigator* dan tim harus memahami tugas atau kasus akan dihadapi yaitu harus memiliki kemampuan detil tentang sistem *computer / cloud system* , jumlah dan lokasi data, jenis harddisk dan sistem operasi yang digunakan, disamping itu harus mampu menentukan gambaran secara menyeluruh tentang kasus yang dihadapi, menentukan hasil akhir yang diinginkan pada kasus yang dihadapi, menentukan parameter. Kemudian ada beberapa yang harus dipertimbangkan yakni adanya kendala-kendala seperti otorisasi secara *internal*, *eksternal* dan *legal* , kendala phisik terkait akses terhadap *property* yang lokasinya banyak, kendala waktu terkait perintah pengadilan terhadap *property pribadi* maupun *komersial*, kendala data yaitu jenis dan jumlah lokasi yang diidentifikasi, sehingga hal tersebut harus dibuat perencanaan dan persiapan serta *logistic* yang diperlukan. Simulasi kasus pada kajian penelitian ini, seorang senior investigator dan tim harus memahami kasus yang terjadi pada layanan *private cloud computing* dengan membuat perencanaan termasuk membentuk tim yang memiliki keahlian seperti yang telah disebutkan diatas. Beberapa lembar formulir yang telah disiapkan ditanda tangani oleh *senior investigator* dan selanjutnya dilakukan perencanaan yang akan dilakukan ditempat kejadian perkara.

(2) Perencanaan di Lokasi *(The On Site Planning)*: Tahapan kedua dari proses *metode ADAM*, yaitu ketika berada dilokasi kejadian perkara maka *senior investigator* dan tim membuat rencana akuisisi utama, karena hal ini berkaitan dengan lokasi data, ukuran dan format data. Masalah keselamatan pada saat di tempat kejadian perkara, personil tim dan data-data akan memerlukan *equipment* yang dapat melakukan isolasi, disertai dengan melakukan update atau maintain terhadap dokumentasi atas seluruh aktifitas yang berlangsung (catatan kontemporer dari semua kegiatan), melakukan survey pendahuluan untuk memastikan lokasi data, menentukan identitas teknis, dan menentukan akuisisi campuran pada lokasi kejadian perkara atau dibawa ke laboratorium *digital forensic*. Kemudian melakukan update terhadap perencanaan yang akan digunakan pada tahapan proses *metode ADAM* selanjutnya.

(3) Akuisisi Data Digital *(Acquisition Digital Data)*: Tahapan ketiga dari *metode ADAM* adalah akuisisi data digital yang dilakukan per perangkat dalam hal ini perangkat yang akan dilakukan akuisisi data pada sisi server layanan *private cloud computing*, dari sisi *laptop/desktop* maupun dari sisi *smartphone* atau perangkat yang digunakan oleh tersangka. Proses akuisisi data yang dilakukan oleh praktisi forensik *digital* harus mempertimbangkan beberapa hal, seperti *data digital evidence* sangatlah rapuh karena sifatnya yang mudah rusak (terkait dengan perangkat keras yang menyertainya), integritasnya sangatlah rentan terhadap perubahan (sangat mungkin dimodifikasi), bahkan kerusakan bisa saja terjadi karena kesalahan teknis atau *human error*. Penanganan yang sangat hati-hati perlu dilakukan, kesalahan dan kegagalan akan menyimpangkan hasil akhir bahkan menghilangkannya, sehingga dibutuhkan proteksi dan penanganan yang seksama akan otentisitas *digital evidence*.

Analisa merupakan tahapan untuk melakukan evaluasi terhadap proses investigasi kasus yang terjadi dengan memanfaatkan metode ADAM (*The Advance Data Acquisition Model*) atau Implementasi *metode ADAM* pada proses investigasi layanan *private cloud computing* dapat menghasilkan *data digital evidence* yang sesuai dan merupakan isu kritikal di dalam proses akusisi data sehingga dapat menjawab masalah realibilitas data atau proses untuk mendapatkan *data digital evidence* yang menjadi perhatian majelis hakim dipersidangan .

Dokumentasi merupakan tahapan dimana setiap tahapan dalam proses investigasi dilakukan pengarsipan atau dokumentasi, setiap perubahan ataupun didapatkannya *data digital evidence* pendukung dilakukan pencatatan / pembaruan dokumentasi.

IV. HASIL DAN PEMBAHASAN

Persiapan sistem yang dilakukan adalah dengan menguji masing-masing perangkat baik dari sisi client (*smartphone, laptop* ataupun *pc desktop*) melalui *internet* ataupun *local area network (LAN)* dapat terhubung ke layanan *private cloud* sehingga hasil yang didapatkan seperti pada Tabel 1 dibawah ini *:*

TABEL I
HASIL VERIFIKASI CLIENT ACCESS MENUJU LAYANAN PRIVATE CLOUD COMPUTING

No	Sumber	Status	Keterangan
1	*IP LAN* 192.168.2.0/24 192.168.3.0/24 192.168.4.0/24 192.168.5.0/24 HotSpot 192.168.100.0/24	 Terhubung Terhubung Terhubung Terhubung Terhubung	 *Pc desktop , Laptop /notebook , smartphone*
2	*Ip Publics Router AT&T*	Terhubung	*International Exchanges (IX)*
3	*Ip Publics Router iix.jk2.cyber*	Terhubung	*Indonesian Internet Exchange (IIX)*
4	*Smartphone – Lenovo 780*	Terhubung	Via *HotSpot / Access Point*atau *Internet*

Pemanfaatan aplikasi *client oCloud.de* ini dapat dilakukan melalui *pc desktop* maupun *smartphone*, sedangkan pada *smartphone* koneksi ke layanan *private cloud* dapat dilakukan melalui akses *internet* maupun akses melalui *access point / hotspot* jaringan lokal.

Hasil proses investigasi yang dilakukan dengan *metode ADAM* adalah sebagai berikut:

(1) Perencanaan Awal :

- Membuat perencanaan awal terkait kasus RSIA "*XYZ Hospital*" pembocoran Informasi rahasia perusahaan yang dilakukan oleh seorang karyawati kepada pihak lain, dimana Informasi tersebut didapatkan dengan memanfaatkan kelemahan dan kesalahan tata kelola layanan *private cloud computing.*
- Menentukan Tim yang akan terlibat di dalam proses investigasi kasus tersebut mencakup pemenuhan kompetensi IT yang diperlukan.
- Menentukan *Software* Aplikasi dan *Tools* yang diperlukan dalam investigasi tersebut.
- Membuat surat tugas/surat perintah yang diperlukan oleh petugas yang kemudian akan diteruskan kepada pihak Manajemen *RSIA "XYZ Hospital"*.
- Membuat dan melakukan pembaharuan terhadap setiap aktifitas yang dilakukan

(2) Perencanaan di lokasi:

- Menentukan sumber-sumber yang menjadi potensi *data digital evidences* seperti layanan *private cloud server, layer 2 datalink , layer 3 network, layer 5 Session, dan layer 7 applications.*
- Membuat rencana proses akusisi data dengan metode *Live Acquisitions* atau *Write Block Acquisitions.*
- Menentukan Aplikasi Software yang digunakan seperti *WireSharks, Network Minner, WinISO atau UltraISO*

(3) Akuisisi Data:

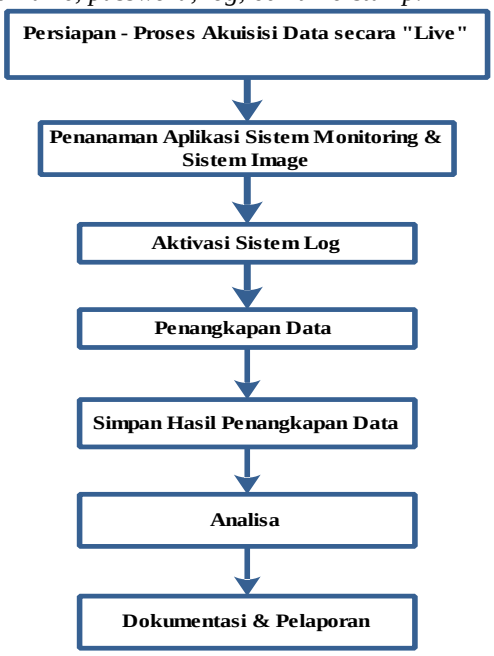
- Mendapatkan *data digital evidences* yang terdapat pada layanan *private cloud system*, *pc desktop* atau *smartphone*, dan perangkat *network* seperti *switch* dan *router.*
- Membuat laporan hasil investigasi

Tahapan Perencanaan Awal (*Initial Planning*) untuk menentukan tim *digital forensic analyst investigator* / terdiri dari ketua tim dan 2-3 anggota yang memiliki kompetensi keahlian dibidang IT secara umum , memiliki pengetahuan tentang teknologi *virtualisasi* / *cloud computing*, memahami berbagai sistem operasi seperti berbasis *linux base* , *windows base*, memahami struktur *folder* dan *files*, memahami tentang keamanan jaringan dan sistem seperti perangkat jaringan *switch, router* dan *access-point*, memahami tentang teknologi layanan berbasis *mobile* seperti *smartphone*. Selain itu tim *investigator* juga harus dapat menentukan jenis dan alat bantu yang akan digunakan untuk melakukan proses investigasi di lapangan seperti halnya menyiapkan perangkat lunak *Wiresharks, Network Minner, UltraISO* atau *WinISO*. Kemudian tim juga harus menyiapkan dokumen surat perintah atau surat tugas untuk melakukan proses investigasi penanganan kasus dan senantiasa melakukan *update* Informasi setiap aktifitas yang dilakukan.

Tahapan perencanaan di lokasi (*the on site planning*) tim investigasi menentukan sumber-sumber potensial *data digital evidences* yang terdapat pada layanan *private cloud computing* dan membuat rencana untuk menentukan proses akuisisi data secara *live acquisitions* atau *write-block acquisitions*. Proses akuisisi data yang dimaksud seperti pada gambar 4 dan gambar 5 kemudian setelah ditentukan proses yang akan dilakukan adalah menggunakan *tools* atau aplikasi piranti lunak yang dapat digunakan untuk melakukan proses akuisisi data. Sejauh ini tidak ada *consensus* khusus mengenai *software* aplikasi yang digunakan untuk melakukan proses akuisisi data pada layanan *cloud computing.* Penelitian ini menggunakan beberapa *software* aplikasi penunjang untuk melakukan proses akuisisi data baik secara *live acquisitions* ataupun *write block acquisitions*.

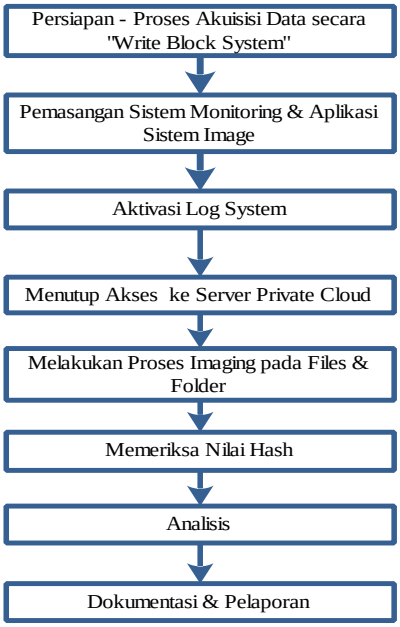
Gambar 4 merupakan alur proses untuk melakukan *data live acquisitions* dimana *software* aplikasi atau *tools* yang digunakan ditanam pada mesin layanan *private cloud*. Kemudian aktivasi sistem *log* yang berada pada layanan *private cloud, router mikrotik* dengan membuat *rule* (*IP-Firewall-Chain (Forward/Input/Output) – action log)*. Penangkapan data secara *live acquisitions* dilakukan pada layer 5 (*session layer*) dengan memanfaatkan perangkat lunak seperti *wiresharks atau network minner. File* yang dihasilkan dari proses penangkapan data pada *layer 5 (session layer)* adalah **.pcap* (*packet captures*) atau **. Cscpkt (colasoft capsa*

packet) kemudian file tersebut dianalisa untuk ditemukan beberapa data bukti *digital* seperti *jenis files, mac-address, username, password, log,* dan *time-stamp.*



Gambar 4 Proses *Data Live Acquisitions*

Gambar 5 merupakan proses yang akusisi data secara *write-block*, dimana seluruh akses yang mengarah ke layanan *private cloud* dilakukan *blocking access* sehingga data yang akan diakuisisi tidak mengalami perubahan atau dihilangkan oleh tersangka. Proses *blocking access* dapat dilakukan melalui perangkat *mikrotik router os* dengan membuat rules pada *IP-Firewall-IP Destinations action drop*.



Gambar 5 Proses *Write Block Data Acquisitions*

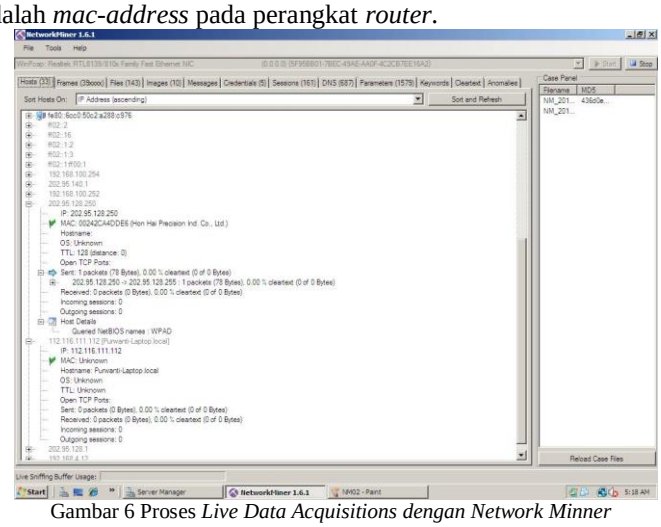
Sistem layanan *private cloud* ditanam aplikasi yang memiliki kemampuan untuk melakukan *proses imaging file (*.iso atau *.dd)* atau proses akusisi data dapat dilakukan secara remote ke mesin layanan *private cloud* meski melalui *local area network (LAN).* Simulasi kasus yang dilakukan menggunakan aplikasi *UltraISO* atau *WinISO,* setelah diketahui posisi *folder* dan *files* yang berada disisi mesin layanan *private cloud computing* kemudian dilakukan proses *imaging files* dan dilakukan pemeriksaan nilai *hash* pada *files* tersebut. Selanjutnya *file image* tersebut dilakukan analisa dan temukan files yang menjadi objek penyalahgunaan atau beberapa *files* yang dibocorkan kepada pihak ketiga pada simulasi kasus ini dan langkah selanjutnya adalah membuat laporan proses akuisisi data secara *write-block*. Proses akuisisi data dengan *metode ADAM* dapat dilakukan per perangkat yang memiliki potensi sumber-sumber *data digital evidences* seperti *server, pc desktop, smartphone*, perangkat *network* seperti *router mikrotik* sehingga pada simulasi kasus dalam penelitian dapat disusun tabel *data digital evidence* yang ditemukan seperti pada tabel 2 sebagai berikut:

TABEL II
AKUISISI DATA PER DEVICE MENURUT METODE ADAM

No	*Parameter*	*PCS*	*PC*	*Sp*	*R*
1	*IP Source*	√	√	√	√
2	*Mac Address Source*	√	√	√	√
3	*IP Destinations*	√	-	-	√
4	*Mac Address Destination*	√	-	-	√
5	*Struktur Folder dan Files*	√	√	√	-
6	*Log Activity - System*	√	√	-	√
7	*Username dan Password*	√	√	√	-
8	*Time Stamp*	√	√	√	√
9	*Data Locations*	√	√	√	-
10	*Protocol & Port Access*	√	√	√	√
11	*Browser – artefact*	√	√	√	-

Keterangan: PCS: *Private Cloud Server*, PC: *Personal Computer*
Sp: *Smartphone*, R: *Router*

Tabel 2 diatas untuk mendapatkan *mac-address* asli dari sumbernya sulit untuk diketahui disebabkan ketika perangkat *pc desktop* ataupun *smartphone* ketika terhubung ke perangkat *network* seperti *router* maka *mac-address* yang digunakan adalah *mac-address* pada perangkat *router.*

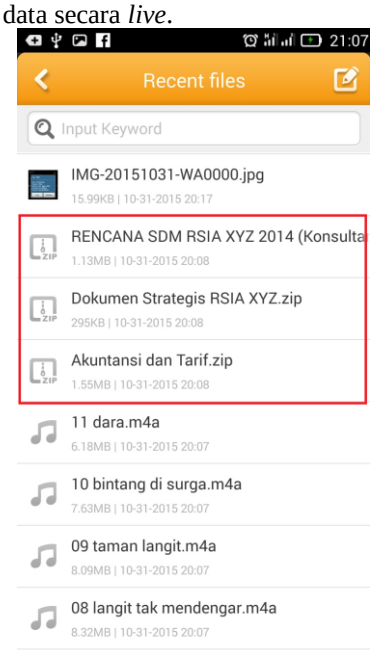


Gambar 6 Proses *Live Data Acquisitions dengan Network Minner*

Gambar 6 merupakan hasil penangkapan data trafik menuju ke mesin *private cloud* dengan menggunakan *Network Minner*

di dapatkan bahwa *client access* dengan *ip public* (*202.95.128.xxx*) yang melewati perangkat *router* akan menggunakan *mac-address router* (*D4CA6D688907*) tersebut demikian halnya dengan perangkat (*pc desktop/smartphone*) yang melalui *access-point / hotspot* ketika melakukan akses ke layanan *private cloud* dan melalui perangkat *router* maka akan didapati menggunakan *mac-address router*.

Menggunakan *network minner* akan didapatkan *host, frames, files, image, message, credentials, sessions, DNS(s), parameters, keyword, cleartext, anomalies*, hasil penangkapan data akan disimpan pada *file* berekstensikan *.pcap (packet captures).*Memanfaatkan fitur-fitur yang dimiliki oleh *network minner* dapat memberikan hasil yang diperlukan di dalam proses akuisisi data secara *live*.



Gambar 7 Data Digital Evidence pada Smartphone

Gambar 7 diatas merupakan hasil investigasi pada perangkat *smartphone*, investigator dapat menemukan 3 *files* yang di duga berkaitan dengan kasus pada RSIA XYZ.

Merujuk pada hasil investigasi dengan menggunakan metode *ADAM*, maka di dapatkan hasil bahwa penyebab terjadinya penyalahgunaan layanan *private cloud* pada RSIA XYZ adalah manajemen *user* pada aplikasi *OwnCloud versi 5.0.5 server* memiliki kelemahan sehingga antara *user* satu dengan lainnya dalam kelompok group yang sama dapat merubah *password*. Verifikasi temuan *data digital evidence* pada komputer *desktop*, perangkat *smartphone* dan sisi *server private cloud computing* , maupun proses akusisi data secara *live* ataupun *write-block acquisition* dapat dilakukan sehingga capaian keberhasilan metode *ADAM* dalam proses investigasi layanan *private cloud computing* adalah 100%. Keberhasilan investigasi dalam kasus RSIA XYZ adalah dapat ditemukannya lokasi *files folder data digital evidences, username* dan *password, time stamps, 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*.

Peningkatan keamanan untuk meminimalisir terjadinya penyalahgunaan dapat memanfaatkan teknologi layanan *virtual private network* , menggunakan produk yang memiliki fasilitas manajemen *user* lebih baik, dan kebijakan manajemen perusahaan di dalam menggunakan layanan *private cloud computing* agar lebih diperketat dan dibatasi pada pengguna tertentu saja

V. KESIMPULAN DAN SARAN

Penggunaan *metode ADAM (The Advance Data Acquisition Model)* pada proses investigasi layanan *private cloud computing* telah berhasil dilakukan dan proses akuisisi data pada layanan tersebut dapat dilakukan baik secara *live* ataupun *write-block acquisition* per perangkat sehingga masalah *realibilitas data digital evidence* tersebut dapat dipertanggungjawabkan di persidangan. Merujuk kasus yang terjadi pada RSIA XYZ potensi penyalahgunaan terhadap tersebarnya informasi data yang bersifat rahasia dapat terjadi disebabkan oleh kelemahan sistem yang digunakan, ataupun telah terjadi kesalahan konfigurasi dan tidak digunakannya kebijakan *access policy* terhadap layanan *private cloud computing*.

Penelitian yang dapat dilakukan selanjutnya adalah melakukan analisa atau *asessment* terhadap piranti lunak atau piranti keras yang digunakan untuk melakukan proses akuisisi data pada layanan *cloud computing*, karena sampai dengan saat ini masih belum ada konsensus mengenai standarisasi penggunaannya.

REFERENSI

[1] Emma Webb Hobson. (2010). "Digital Investigations in the Cloud." Farnborough, UK:QinetiQ Digital Investigations Service

[2] Hogan Lovell, Winston Maxwell, Christopher Wolf, (2012) DCA Global Reality: Governmental Access to Data in the Cloud A comparative analysis of ten international jurisdictions, Hogan Lovell White papers.13.

[3] Marthie Lessing, Basie von Solms (2011), "Live Forensic Acquisition as Alternative to Traditional Forensic Processes", Council for Scientific and Industrial Research Meiring Naudé Road, Scientia Pretoria, South Africa, 2011.

[4] Bodenheimer, D. Z. (2012), Cloud Computing Acquisitions & Cyber security. Briefing Papers, No. 12-11, 20.

[5] Raffael Marty (2011), "Cloud application logging for forensics," in proceedings of the 2011 ACM Symposium on Applied Computing. ACM, 2011, pp. 178–184, 2011.

[6] Richard Adams, V. H. (2013), The Advanced Data Acquisition Model (ADAM): A Process Model For Digital Forensic Practice. Journal of Digital Forensics, Security and Law, Vol. 8(4), 24.

[7] Keyun Ruan, P. J. (2011). Cloud forensics: An overview. *IBM Ireland Ltd*, 16.

[8] National Institute of Standard and Technology (NIST) 2011,Challenging security requirements for US government Cloud Computing adoption, U.S. Department of Commerce, National Institute of Standards and Technology, Gaitherbug

[9] Barrett, D & Kipper, G (2010), Virtualization and Forensics: a digital forensic investigator's guide to virtual environments, Syngress.

[10] Birk, D & Wegener, C (2011), Technical Issues of forensics IInvestigations in cloud computing environments, Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), IEEE.

[11] Huber M, Mulazzani M, Leithner M, Schrittwieser S, Wondracek G,Weippl, E, (2011). Social snapshots: digital forensics for online social networks, In: Annual Computer Security Applications

Conference – ACSAC 2011, Orlando, Florida, USA; 2011, pp. 113–122.

[12] Zatyko, K & Bay, J .(2011), The Digital forensics cyber exchange principle, Forensics Magazine, pp.5-13.

[13] Taylor M, Haggerty J, Gresty D, Lamb D, (2011). Forensic investigation of cloud computing systems. Network Security, (3):4–10.

[14] McKemmish R, (1999). What is forensic computing? Trends & Issues in Crime and Criminal Justice;118:1–6

[15] Kent, K., Chevalier, S., Grance, T., & Dang, H.(2006). Guide to Integrating Forensic Techniques into Incident Response. In National Institute of Standards and Technology (Ed.) (Vol. 800-86): U.S. Department of Commerce.

[16] Reilly, D, Wren, C & Berry, T (2010), Cloud Computing: Forensics Challenges for Low enforcement, International Conference for Internet Technology and Secured Transactions (ICITST), IEEE.

[17] S. Zimmerman and D. Glavach (2011), "Cyber Forensics in the Cloud," *IA Newsletter*, vol. 14, no. 1, pp. 4-7; http://iac.dtic.mil/iatac/download/Vol14_No1.pdf.