Investigasi Bukti Digital pada *Platform Cloud Gaming* Menggunakan *Framework* FRED Studi Kasus pada Skyegrid *Cloud Gaming Services*

Ramansyah

17917126

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensik Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2021

Lembar Pengesahan Pembimbing

Investigasi Bukti Digital pada Platform *Cloud Gaming* Menggunakan *Framework* FRED Studi Kasus pada Skyegrid *Cloud Gaming Services*

Ramansyah

17917126

Yogyakarta, Juni, 2021

Pembimbing I	Pembimbing II
Dr. Imam Riadi, S.Pd., M.Kom.	Dr. Yudi Prayudi, S.Si., M.Kom.

Lembar Pengesahan Penguji

Lembar Pengesahan Pembimbing

Investigasi Bukti Digital pada Platform *Cloud Gaming* Menggunakan *Framework* FRED Studi Kasus pada Skyegrid *Cloud Gaming* Services

Ramansyah

17917126

Yogyakarta, Juni, 2021

Tim Penguji,

Dr. Imam Riadi, S.Pd., M.Kom

Ketua

Dr. Yudi Prayudi, S.Si., M.Kom.

Anggota I

Dr. Ir. Bambang Sugiantoro, S.Si., MT.

Anggota II

Mengetahui,

Ketua Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

Abstrak

Investigasi Bukti Digital pada Platform *Cloud Gaming* Menggunakan *Framework* FRED Studi Kasus pada Skyegrid *Cloud Gaming* Services

Layanan *cloud gaming* memberikan akses *game online* berspesifikasi tinggi dapat diakses dengan *device* minimalis. Kemudahan akses tersebut mengundang celah kejahatan baru dan memunculkan tantangan tersendiri untuk menemukan petunjuk dan bukti digital dalam mengungkap kasus kejahatan yang terjadi. Pendekatan ilmu *cloud* forensik tetap menjadi kendala dan tantangan bagi investigator dikarenakan setiap penyedia *cloud* khususnya *cloud gaming services* memiliki arsitektur yang berbeda sehingga diperlukan penelitian lebih lanjut dalam melakukan forensik *cloud gaming service*. Fokus penelitian ini melakukan investigasi bukti digital pada perangkat *client* dengan menyimulasikan tindak kejahatan pada platform Skyegrid *cloud gaming services*. Proses pembuktian menerapkan langkah kerja *Framework for Reliable Experimental Design* (FRED) dengan tahapan yaitu perencanaan, implementasi, evaluasi, ulangi, analisis, dan konfirmasi. Sementara itu metode akuisisi dan analisis menggunakan metode *live forensics* untuk mendapatkan karakteristik bukti digital dari bukti elektronik *network traffic*, RAM dan HDD. Hasil penelitian menunjukkan bahwa bukti digital pada Skyegrid diartefak HDD memiliki peranan yang penting. Karena di dalamnya terdapat *file* log.txt yang merupakan catatan informasi *user* menjalankan Skyegrid dan game online. Pada penelitian ini barang bukti digital seperti *username, password login* Steam kemudian *nickname game, id game* dan pesan *chat* tidak dapat ditemukan karena tersimpan disisi server dan adanya metode keamanan TLS pada *network traffic*. Berdasarkan hasil penerapan FRED, disimpulkan bahwa FRED merupakan *framework* yang dapat diimplementasikan pada bukti digital lainnya karena memiliki tahapan dengan cakupan yang luas.

Kata kunci

cloud gaming service, Skyegrid, FRED, *network* forensik, komputer forensik.

Abstract

Investigating Digital Evidence on Cloud Gaming Platforms Using FRED Framework Case Study on Skyegrid Cloud Gaming Services

Cloud gaming services provide access to high-spec online games that can be accessed with minimalistic devices. This ease of access invites new criminal loopholes and creates its own challenges to find clues and digital evidence in uncovering cases of crimes that occur. The cloud forensic science approach remains an obstacle and challenge for investigators because each cloud provider, especially cloud gaming services, has a different architecture, so further research is needed to conduct cloud gaming service forensics. The focus of this research is to investigate digital evidence on client devices by simulating crimes on the Skyegrid cloud gaming services platform. The proof process applies the work steps of the Framework for Reliable Experimental Design (FRED) with stages, namely planning, implementing, evaluating, repeating, analyzing, and confirming. Meanwhile, the acquisition and analysis method uses the live forensics method to obtain the characteristics of digital evidence from electronic evidence of network traffic, RAM and HDD. The results show that digital evidence on Skyegrid artifact HDD has an important role. Because it contains a log.txt file which is a record of user information running Skyegrid and online games. In this study, digital evidence such as usernames, Steam login passwords and game nicknames, game ids and chat messages could not be found because they were stored on the server side and there was a TLS security method on network traffic. Based on the results of the implementation of FRED, it is concluded that FRED is a framework that can be implemented on other digital evidence because it has stages with a wide scope.

Keywords

cloud gaming services, Skyegrid, FRED, network forensics, computer forensics.

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Juni 2021

Ramansyah, S.Kc

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dari penulisan tesis ini

Ramansyah, Prayudi, Y., & Riadi, I. (2021). Deteksi Bukti Digital Game Online Pada Platform Skyegrid Menggunakan Framework FRED. 8(2), 794–804. https://doi.org/https://doi.org/10.35957/jatisi.v8i2.793

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Ramansyah	Mendesain eksperimen (70%) Menulis *paper* (100%)
Yudi Prayudi	Memberi ide dan saran (30%) Telaah artikel
Imam Riadi	Memberi ide dan saran (30%) Telaah artikel

Halaman Kontribusi

Penelitian ini tidak terlepas dari berbagai saran maupun bimbingan dari berbagai pihak, mulai dari pra penelitian, seminar proposal, seminar progress, hingga seminar pendadaran. Pihak-pihak tersebut, antara lain, Dr. Yudi Prayudi,S.Si.,M.Kom, Dr. Imam Riadi, S.Pd., M.Kom, dan Dr. Ir. Bambang Sugiantoro, S.Si., MT.

Halaman Persembahan

Bismillahirrahmanirrahim.

Dengan mengucapkan syukur Alhamdulillah atas segala nikmat ALLAH SWT, nikmat ilmu dan segala macam hal yang telah dikaruniakan-Nya sehingga karya penelitian ini dapat terselesaikan. Untuk itu saya persembahkan kepada orang-orang yang selama ini telah mendukung, memberikan semangat dan motivasi dalam menyelesaikan pendidikan magister saya ini, secara khususnya kepada:

1. Kedua orang tua saya, yang selama ini telah memberikan dukungan tanpa henti, pengorbanan dan kasih sayang tanpa henti serta sumbangsih moril maupun materiil selama menempuh program magister ini.
2. Istri tercinta (Siti Nur Aisyah) dan sibuah hati (Masya Asy syifa). Terima kasih atas semua doa, motivasi, dan *support* yang telah diberikan kepada saya selama menempuh perkuliahan.
3. Adik-adik ku. Terima kasih atas bantuan, doa, serta selalu memberikan semangat selama proses menempuh pendidikan ini.
4. Teman-teman seperjuangan FD angkatan 16 serta keluarga besar FK UII yang telah memberikan bantuan selama menempuh pendidikan ini.

Kata Pengantar

Assalamualaikum Wr. Wb.

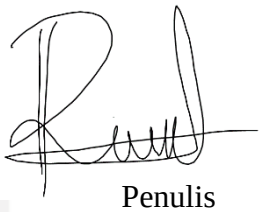
Puji syukur penulis panjatkan kepada Allah SWT atas limpahan dan karunia yang diberikan kepada penulis sehingga dapat menyelesaikan laporan penelitian tesis dengan judul "Investigasi Bukti Digital pada Platform *Cloud Gaming* Menggunakan *Framework* FRED Studi Kasus pada Skyegrid *Cloud Gaming Services*". Adapun maksud dari penulisan laporan penelitian ini adalah sebagai persyaratan dalam mencapai jenjang pendidikan Magister Teknik Informatika konsentrasi Forensik Digital di Fakultas Teknologi Industri, Universitas Islam Indonesia. Dalam proses penyelesaian tesis ini penulis tidak dapat menyelesaikannya bila tidak ada turut serta pihak lain yang juga ikut membantu baik secara langsung maupun tidak langsung dalam menyelesaikan penelitian ini, untuk itu penulis ingin menyampaikan rasa terima kasih kepada beberapa pihak yang telah mendukung dalam penyusunan tesis ini, antara lain:

1. Bapak Fathul Wahid, S.T., M.Sc., Ph.D, selaku rektor Universitas Islam Indonesia yang memberikan kesempatan kepada penulis untuk menimba ilmu di Universitas Islam Indonesia.
2. Bapak Prof. Hari Purnomo, M.T selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia yang memberikan fasilitas dan bantuan untuk belajar.
3. Ibu Izzati Muhimmah, ST., M.Sc., Ph.D, selaku Ketua Program Studi Teknik Informatika Program Magister Fakultas Teknologi Industri, Universitas Islam Indonesia, yang selalu memberikan semangat kepada setiap mahasiswa agar segera menyelesaikan tesis.
4. Bapak Dr. Imam Riadi, S.Pd., M.Kom dan Bapak Dr. Yudi Prayudi,S.SI.,M.Kom, selaku dosen pembimbing yang telah banyak meluangkan waktunya dalam memberikan berbagai saran selama proses bimbingan.
5. Seluruh Dosen, staf administrasi dan civitas Magister Teknik Informatika Universitas Islam Indonesia, baik secara langsung maupun tidak langsung telah membantu penulis selama masa studi penulis.
6. Seluruh keluarga baik Bapak, Ibu, Kakak, Adik, Istri dan Anak tercinta yang telah mencurahkan segenap cinta, kasih sayang, perhatian dan dukungan baik moril maupun materiil

7. Rekan-rekan mahasiswa MTI khususnya konsentrasi Forensik Digital angkatan XVI yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lainnya.
8. Rekan-rekan kerja di Fakultas Kedokteran UII yang selama ini memberi dukungan, dan pengertian pembagian tugas kerja, serta tempat berbagi pengalaman dan informasi terkait penyusunan penelitian ini.
9. Pihak-pihak lain yang turut membantu dalam menyelesaikan penelitian ini yang tidak dapat disebutkan satu persatu oleh penulis.

Penulis menyadari bahwa laporan penelitian ini masih memiliki kekurangan. Oleh karena itu penulis dengan senang hati menerima setiap saran atau komentar serta kritikan dari pembaca guna penyempurnaan laporan penelitian ini. Akhir kata penulis mengucapkan terima kasih, semoga penyusunan laporan penelitian ini dapat memberikan inspirasi maupun manfaat bagi pembaca, khususnya bagi mahasiswa/mahasiswi Universitas Islam Indonesia. Wassalamu'alaikum Wr. Wb.

Yogyakarta, Juni 2021



Penulis

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

FRED	- *Framework for Realiable Experimental Design*
RAM	- *Random Access Memory*
HDD	- *Hard drive*
RTS	- *Real time strategy*
FPS	- *First person shooters*
RPG	- *Role-Playing Game*
TLS	- *Transport Layer Security*

BAB 1

Pendahuluan

1.1 Latar Belakang

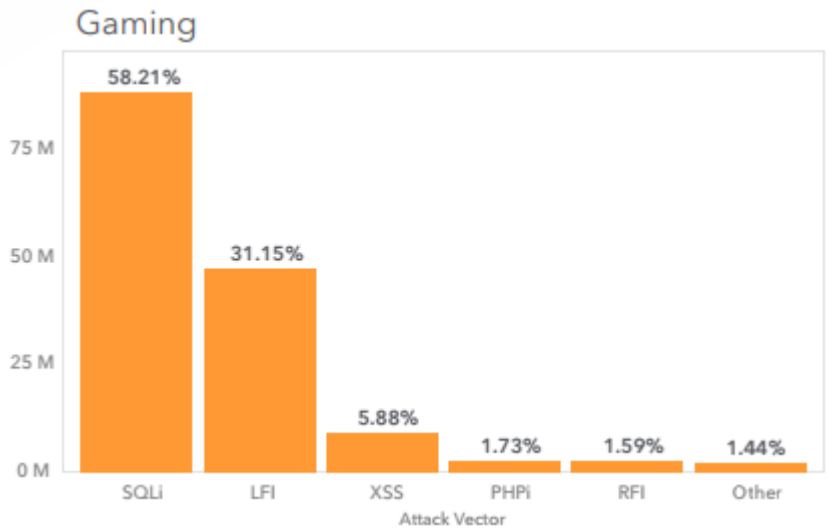
Perkembangan teknologi informasi dan komunikasi di era kini semangkin pesat seiring didorong dengan meningkatnya perekonomian. Tanpa sadar menerpa dan mempengaruhi terhadap kehidupan sosial masyarakat. Salah satu bentuk perkembangan teknologi informasi dan komunikasi yang mampu mempengaruhi kehidupan sosial adalah game online. Menurut (Padilla-Walker, Nelson, Carroll, & Jensen, 2010) game online menjadi media hiburan yang dominan digemari oleh anak muda dalam kurun waktu 20 tahun terakhir. Sementara itu merujuk data yang dipaparkan oleh Capcom *International Development Group*, menyatakan bahwa dari tahun 2011 hingga 2019 pendapatan penjualan game online di seluruh dunia mengalami peningkatan setiap tahunnya. Gambar 1.1 menjelaskan bahwa pendapatan game online dari tahun 2011 sampai 2019 mengalami pasang surut, namun dari tahun 2016 sampai tahun 2019 pendapatan game online tidak ada yang menunjukkan kerugian malah sebaliknya pendapatan game online mengalami peningkatan sebanyak satu milyar dolar pertahunya. Dengan data ini menjadi jelas bahwa setiap tahunnya peminat game online semangkin meningkat.

Gambar 1.1 Peningkatan Global Markets Game Online [1]

Beberapa alasan yang membuat game online menjadi sangat disenangi oleh kalangan anak muda masa kini adalah disebabkan pengembangan game online yang menarik, fantasi, dan disertai dengan tampilan yang memukau. sementara itu pilihan game berdasarkan *genre*

[1] https://www.wepc.com/news/video-game-statistics/#online-gaming

seperti RTS, FPS, RPG, *Life simulation game*, dan simulasi kendaraan. Beragam jenis game online menjadikan game online seperti dunia virtual yang semangkin menarik (Eskasasnanda, 2017). Sementara itu game online telah didukung dengan beragam platform seperti Xbox, PlayStation, Steam, Nintendo, Andorid, Windows dan MacOs. Namun, akhir-akhir ini isu kejahatan dunia maya (*Cybercrime*) pada game online muncul tanpa henti hingga menjadi masalah besar bagi pengembang game online. Permasalahan tersebut secara tidak langsung dapat berakibat kerugian finansial bagi perusahaan game dan para gamers (Zhao, 2018). Menurut situs penelitian Akamai dalam laporan (Can & Security, 2020) yang dilakukan di antara Juli 2018 hingga Juni 2020 ada sejumlah 152,256,924 serangan *cybercrime* pada game online dengan beragam jenis dan model serangan, persentase jenis serangan pada game online sebagaimana pada Gambar 1.2. Terlihat bahwa jenis serangan SQL *injection* dan LFI (*Local File Inclution*) menjadi serangan yang mendominasi pada game online. Hal ini menjadi pendorong tercetusnya pengembangan dan peningkatan keamanan pada platform game online yang dapat dimanajemen.



Gambar 1.2 Jenis serangan pada game online (sumber: (Can & Security, 2020))

Platform *cloud gaming* lahir semenjak (E.Ross, 2009) memperkenalkan *cloud gaming* ke dunia akademis setelah tercetusnya prototipe teknologi G-*cluster* pada layanan teknologi *cloud. Cloud gaming services* akhir-akhir ini menjadi perhatian anak-anak muda karena platform *cloud gaming services* lebih murah, mudah dan fleksibel sehingga bermain game online dapat dilakukan secara *mobile*. Menurut data dari laporan *infinity Research* memaparkan bahwa jumlah pengguna *cloud gaming* akan terus tumbuh pesat sebesar 29% mulai dari periode 2017 hingga 2021 [2]. Menurut (Harding-rolls, 2019) menjelaskan bahwa

[2] https://www.technavio.com/report/global-gaming-global-cloud-gaming-market-2017-2021

20 tahun ke depan *platfotm* game online akan berpindah menggunakan *platform cloud gaming*. Berdasarkan penjelasan (K. Chen et al., 2016) lahirnya *platfrom cloud gaming* akan menjadi solusi dari berbagai masalah keamanan yang dapat merugikan bagi *gamers*, developer dan industri game. Keuntungan bagi pengguna memilih layanan *cloud gaming* adalah, menjadi solusi bebas dari biaya *upgrade* perangkat keras yang mahal, dan masalah *storage* over kapasitas dapat diatasi karna semua game sudah terpasang di *server*. Keuntungan bagi developer game, sinkronisasi, *update patch* dan *rebuild sourcode* menjadi lebih efisien. Keuntungan bagi industri game, solusi pemasaran, penjualan, keamanan serta pembajakan game dapat teratasi. Dengan demikian *cloud gaming sevices* dapat menjadi solusi dari serangan *cybercrime*, namun menjadi permasalahan baru pada bidang forensik digital dalam menghadirkan barang bukti kejahatan.

Beragam tantangan dalam melakukan forensik digital pada ruang lingkung *cloud computing.* Hal ini menjadi tantangan baru bagi penyidik forensik digital untuk melakukan investigasi penyalahgunaan game online dengan menggunakan platform *cloud gaming services.* Tantangan utama dalam investigasi *cloud gaming services* adalah *Data Deletion*, sebagai karakteristik pada layanan *cloud* setelah masa sewa berakhir data yang tersimpan pada *storage cloud* akan terhapus atau tertimpa dengan data *users* yang baru (Narayana Samy et al., 2018). Bagi yang mengerti dengan hal ini, maka platform *cloud gaming services* memungkinkan dijadikan media untuk melakukan tindakan kejahatan tanpa risiko terdeteksi (anti forensik), karena informasi seperti data *save game* dan pesan *text* pada fitur *chat* game yang awalnya disimpan di *cloud game services* secara otomatis hilang. Oleh sebab itu, dalam penanganan bukti digital pada *cloud gaming service* perlu study digital forensik lebih lanjut untuk mengumpulkan informasi yang dapat dijadikan sebagai barang bukti digital dalam persidangan.

Dalam pembuktian di persidangan terkait kejahatan melalui game online membutuhkan para peneliti atau penyidik dalam bidang digital forensik. Penelitian forensik mengenai penyalahgunaan game online telah dilakukan oleh peneliti terdahulu. Penelitian terhadap game online Dota yang disimulasikan menggunakan platform Steam yang di *install* pada sistem operasi Windows telah dilakukan oleh (Tabuyo-benito et al., 2018). Pada penelitian tersebut dijelaskan proses investigasi mengenai artefak digital yang berpotensi dapat digunakan sebagai barang bukti digital seperti pesan *chat, id game, nickname game,* dan akun game. Keberhasilan penelitian tersebut diperoleh dari proses ekstraksi dari media penyimpanan lokal yang bersifat volatil (RAM), bukan volatil (HDD) dan *traffic* jaringan komputer. Sementara itu penelitian serupa mengenai penyalahgunaan game online pernah

dilakukan oleh (Taylor et al., 2019). Penelitian tersebut juga menjelaskan proses keberhasilan investigasi dari tiga artefak yang diekstrak dari media penyimpanan lokal bersifat volatil (RAM), bukan volatil (HDD) dan *traffic* jaringan komputer dengan simulasi game online MinerCraf menggunakan platform Linux dan Windows. Namun sejauh ini penelitian forensik pada *platform cloud gaming services* sependek pengetahuan peneliti belum ada.

Ada beberapa metode dan *framework* yang telah diteliti dan dikembangkan untuk penyelidikan forensik digital pada layanan *cloud*, salah satunya adalah FRFED. FRED (*Framework for Realiable Experimental Design)* dikembangkan oleh (Horsman, 2018). Framework FRED menyediakan kerangka kerja untuk merancang, mengembangkan, mengimplementasikan pengujian dan validasi, mendukung *output* yang andal, dapat diulang, dan dapat didokumentasikan. FRED juga mendorong transparansi dalam proses penelitian dan pengujian untuk memungkinkan *peer-review* yang efektif dan untuk penilaian menyeluruh atas keandalan setiap pekerjaan yang dilakukan. Implementasi *Framework* FRED telah diterapkan pada penelitian sebelumnya oleh (Kristiyanto et al., 2018) sebagai metode untuk menganalisis *database* pada aplikasi *website* penilaian kinerja karyawan pada PT. Campus media. penelitian ini menyimpulkan bahwa dengan penerapan *framework* FRED hasil sebuah laporan barang bukti menjadi lebih sesuai dengan rangkaian *standart operation prosedur* (SOP) forensik digital. penelitian terkait berikutnya dilakukan oleh (Don & Chen, 2018) penerapan *framework* FRED hasilnya mampu menemukan tidak hanya tempat-tempat di mana pengguna mengunjungi, tetapi juga dapat menemukan kegiatan yang dilakukan oleh pengguna Bundel Tor Browser pada perangkat Mobile.

Berdasarkan paparan di atas, maka ranah penelitian yang akan diusulkan adalah melakukan investigasi bukti digital pada *platform cloud gaming* dengan menggunakan *fremework* FRED. Skyegrid Penyedian jasa *cloud gaming service* dipilih sebagai bahan penelitian ini. Diharapkan hasil dari penelitian ini dapat mengembangkan tahapan-tahapan dalam melakukan investigasi forensik pada *platform* game online khususnya pada *platform cloud gaming* serta dapat menjadi panduan utama para penyidik dalam menghadirkan bukti digital terkait kasus-kasus penyalahgunaan pada *cloud game service* sesuai dengan prosedural hukum yang berlaku.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka yang menjadi rumusan masalah dalam penelitian ini adalah sebagai berikut:

a. Bagaimana penerapan *framework* FRED sebagai tahapan dalam penelusuran potensi bukti digital di *platform* Skyegrid *cloud gaming*?
b. Bagaimana proses analisa bukti digital untuk *cloud gaming service* sesuai degan *fremework* FRED?

1.3 Tujuan Penelitian

Adapun tujuan dilakukannya penelitian ini adalah sebagai berikut:

a. Menerapkan tahapan *framework* FRED sebagai proses pengujian dalam investigasi bukti digital pada *platform* Skyegrid *cloud gaming service* sehingga dapat dijadikan platform valid dan relevan dalam penanganan barang bukti elektronik.
b. Mencari dan menemukan jejak *data* sebagai potensi artefak digital yang dapat dihadirkan di depan persidangan.

1.4 Batasan Masalah

Adapun batasan masalah pada penelitian ini sebagai berikut:

a. Platform *Cloud gaming service* yang digunakan pada penelitian ini adalah Skyegrid
b. Proses pengumpulan barang bukti digital hanya disimulasikan pada perangkat *client*
c. Game online yang menjadi fokus penelitian ini adalah game Dota 2 dan CS:GO
d. Sistem operasi yang digunakan dalam penelitian ini adalah Windows 10 64 bit
e. *Tools* forensik yang digunakan dalam kategori *opensource.*

1.5 Manfaat Penelitian

Manfaat yang dihasilkan penelitian ini sebagai berikut:

a. Menambah informasi terbaru terhadap tahapan-tahapan dalam melakukan investigasi digital forensik pada platform c*loud gaming service*
b. Melengkapi penelitian sebelumnya terhadap penanganan barang bukti digital pada platform game online.

1.6 Literatur Review

Cloud gaming sebagai terobosan teknologi *platform* game online merupakan tantangan baru dalam digital forensik. Dalam penyelesaian kasus-kasus yang berhubungan dengan digital forensik membutuhkan sebuah eksperimen untuk membantu dan mempermudah investigasi dalam pengumpulan barang bukti digital. Sependek pengetahuan peneliti, belum ada penelitian sebelumnya yang fokus membahasa investigasi forensik pada *cloud gaming*. Penelitian terdahulu lebih fokus melakukan analisis sistematis (Cai et al., 2016), Mobile *cloud gaming* (Soliman et al., 2013) pengembangan arsitektur dan layanan *cloud gaming*

(Ojala & Tyrväinen, n.d.) , dan melakukan pengujian dan membandingkan pada layanan *cloud gaming* yang sudah rilis (K.-T. Chen et al., 2016).

Penelitian tentang investigasi bukti digital pada *platform game online* Steam telah di lakukan oleh (Tabuyo-benito et al., 2018) penelitian yang diusulkan sangat sistematis khususnya dalam memaparkan hasil temuan pada Steam. Kesamaan *platform* Steam dengan *platform cloud gaming* adalah menyediakan market *game online* yang disediakan menggunakan teknologi *cloud computing.* Konsep *cloud computing* tidak lepas dari arsitektur *client-server* yang banyak ditemui hingga merambah pada dunia *game online.* Penelitian yang diusulkan oleh (Taylor et al., 2019) adalah melakukan investigasi pada *platform clien-server* dengan sistem operasi Windows dan Ubuntu. Metode pengumpulan bukti digital yang diterapkan pada kedua peneliti sama persis, yang membedakan hanya pada *framework* yang diusulkan. Kekurangan dari *framework* yang diusulkan tidak menjelaskan tahapan verifikasi atau validasi temuan bukti digital.

(Horsman, 2018) mengusulkan sebuah *framework* baru, yang mampu mengatasi terkait validasi temuan bukti digital yang disebut *Framework for Reliable Experimental Design* (FRED). FRED terdiri dari enam tahapan yaitu *plan, implement, evaluate, repeat, analysis* dan *confirm.* FRED telah diterapkan pada penelitian sebelumnya oleh (Kristiyanto et al., 2018) untuk melakukan analisis *datatbase* Mariadb pada aplikasi penilai kinerja karyawan PT. Campus Media, dan (Don & Chen, 2018) untuk menganalisis fitur anonim pada aplikasi browser Tor Bundle pada Android. Hasil kedua penelitian yang telah dilakukan memperlihatkan temuan bukti digital yang relevan dan aktual, dalam proses validasi temuan bukti digital, kedua peneliti melakukan beberapa kali pengujian dengan berbeda metode pengumpulan (akuisisi) bukti digital, kemudian hasil analisis dibandingkan untuk melihat kesamaan dan perbedaan bukti yang didapat.

Tabel 1.1 Rangkuman *Review* Penelitian

No	Paper Utama	Isu	Tahapan Framework	Metode Akuisisi	Target
1	(Ojala & Tyrväinen, n.d.)	Pengembangan *cloud gaming* sebagai bisnis model	-	-	Bukan penelitian eksperimental
2	(Soliman et al., 2013)	Membahas isu dan tantangan pada *mobile cloud gaming*	-	-	Bukan penelitian eksperimental
3	(Cai et al., 2016)	Melakukan survei pada perkembangan c*loud gaming*	-	-	*Cloud gaming services*
4	(K.-T. Chen et al., 2016)	*Cloud gaming*	-	-	Bukan penelitian eksperimental
5	(Kristiyanto et al., 2018)	Visualisasi dan interpretasi *database engine*	FRED	*live* forensik	Database engine, MariaDB, log database
6	(Don & Chen, 2018)	Analisis browser anonim Tor Bundle Pada Android	FRED	*Logical* forensik	Samsung Galaxy Note 5, Browser.db, Log cache Tor Bundle
7	(Tabuyo-benito et al., 2018)	Investigasi MMOG pada platform Steam	McKammish	*Network* forensik, *live* forensik, *Post-mortem* forensik, dan Windows forensik	Log game, Network traffic, data volatil, teks dan audio chat
8	(Taylor et al., 2019)	Investigasi MMOG pada *cross* platform *client-server*	Cloud Computing	Network forensik, dan live forensik	Log game, pada client-server, network traffic
9	Usulan Penelitian	Investigasi Bukti digital pada platform *cloud gaming*: Studi kasus pada Skyegrid *cloud gaming services*	FRED	Network Forensik, dan *live* forensik	
		Penelitian yang akan diusulkan adalah melakukan penelitian terkait investigasi bukti digital pada platform *cloud gaming services* dengan menggunakan tahapan framework FRED. Studi kasus penelitian ini pada Skyegrid cloud gaming service. untuk pengumpulan bukti digital menerapkan metode live forensik, Network forensik dan post-mortem forensik untuk akuisisi Skyegrid. Harapan penelitian ini menjadi solusi dan acuan investigator dalam mengakuisisi cloud gaming service sesuai dengan permasalahan yang ada.			

1.7 Metode Penelitian

Langkah-langkah dalam proses penelitian ini adalah sebagai berikut:

Gambar 1.3 Alur Metode Penelitian

1.8 Sistematika Penelitian

Untuk memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka dibuat sistematika penulisan sebagai berikut:

BAB I Pendahuluan

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Di dalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian serta sistematika penulisan.

BAB II Tinjauan Pustaka

Pada Bab ini menjelaskan tentang teori-teori dasar yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori menyangkut penelitian yang sedang diteliti.

BAB III Metodologi Penelitian

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat lunak, perangkat keras dan bahan penelitian yang digunakan serta perancangan antar muka aplikasi yang akan dibuat.

BAB IV Pembahasan

Pada Bab ini membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis dan evaluasi dari penelitian yang diangkat.

BAB V Penutup

Pada bab ini memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan karena keterbatasan dalam mendapatkan materi yang dibuat selama melakukan penelitian dan rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.

BAB 2

Kajian Pustaka

2.1 Digital Forensik

Komputer forensik menurut (Sulianta, 2016) bidang ilmu yang mengkaji terkait pengumpulan dan analisis informasi dari berbagai sumber daya komputer sebagai media tindak kejahatan yang pernah digunakan sehingga layak untuk diajukan di saat sidang pengadilan. Komputer forensik mencakup sumber daya sebagai berikut:

a. Sistem komputer
b. Jaringan komputer
c. Media komunikasi (mencakup secara fisik menggunakan media kabel dan *wireless*/nirkabel)
d. Berbagai media *storage/*penyimpanan komputer

Komputer forensik atau sering disebut digital forensik, sebagian memahami bahwa bidang ilmu digital forensik hanya berkaitan dengan kasus-kasus kriminal yang melibatkan hukum, namun seutuhnya digital forensik selain berkaitan kasus-kasus kriminal dapat berguna untuk kebutuhan tertentu yang berkaitan dengan perkerjaan yang melibatkan teknologi informasi. Sementara itu mengutif dari (Nuh Al-Azhar, 2012) digital forensik merupakan "*aplikasi bidang ilmu pengetahuan dan teknologi komputer yang digunakan dalam kepentingan pembuktian hukum (pro justice), untuk melakukan pembuktian kejahatan dengan menggunakan teknologi atau komputer secara ilmiah hingga mendapatkan bukti digital yang digunakan untuk menjerat pelaku kejahatan*". Digital forensik menjadi salah satu pengembangan bidang ilmu teknologi informasi dan ilmu hukum hingga kini menjadi bentuk spesialisasi untuk melakukan investigasi yang berhubungan dengan kejahatan komputer (*computer related crime*). Para penyidik/investigasi digital forensik disebut akan melakukan pemeriksaan setiap barang bukti elektronik dalam rangka mencari data digital yang berkaitan dengan kasus kejahatan dan pelakunya.

Tabel 2.1 barang bukti elektronik dan barang bukti digital

NO	Barang Bukti Elektronik	Barang Bukti Digital
1	Komputer PC	Logical file
2	Laptop/notebook, netbook, tablet	Deleted file
3	Handphone, smartphone	Lost file
4	Flashdisk/thumb drive	File slack
5	Floppydisk	Log file
6	Harddisk	Encrypted file
7	CD/DVD	Steganography file

8	Router, switch, hub	Office file
9	Kamera video, cctv	Audio file
10	Kamera digital	Video file
11	Digital recorder	Image file
12	Music/video player, dan lain-lain	Email
13		User ID dan password
14		Short message service
15		Call logs

Dari hasil investigasi forensik pada perangkat digital dapat ditemukan barang bukti bersifat digital yang dapat membantu mengungkap fakta dari sebuah kejadian. Barang bukti digital membutuhkan penanganan secara khusus mulai dari pelestarian, pengumpulan, validasi, identifikasi, analisa, interpretasi, dokumentasi, dan penyajian agar dapat dijadikan landasan kuat pada proses persidangan. Penanganan khusus tersebut yaitu dengan memperhatikan *standart operation procedure* (SOP) yang ada serta menggunakan metode ilmiah yang memang dibuat dalam penanganan bukti digital.

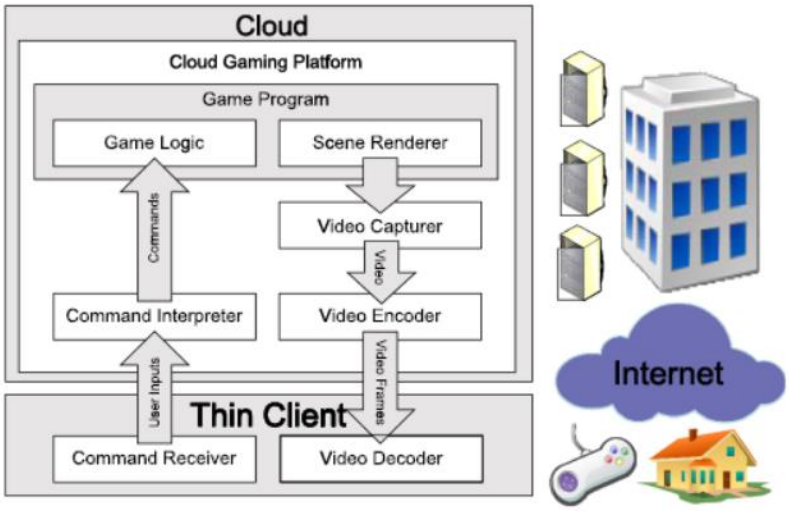
2.2 Cloud Gaming

Cloud gaming atau *gaming on-demand* terobosan yang lahir dari layanan *Game as a Service* (GaaS) dari infrastruktur teknologi *cloud computing*. *cloud gaming* hadir sebagai solusi bagi pecinta game namun terbatas pada *hardware* game yang mahal. *cloud gaming* menjadikan relatif lebih murah dan efisien, sebab *gamer's* dapat bermain game di berbagai macam perangkat di mana-pun dan kapan-pun melalui internet, dengan catatan koneksi internet wajib stabil dan cepat (Soliman et al., 2013). Sedangkan definisi menurut (Cai et al., 2016) semua sumber daya *hardware game* dan proses *rendering* di eksekusi di *cloud* server yang andal, kemudian setiap *output* hasil *rendering* di transmisikan kepada *gamer's* melalui internet serta proses *input/control*.

Secara eksplisit gambar proses kerja dari kedua komponen utama *cloud gaming* dapat dilihat pada Gambar 2.1 , ketika menjalankan sebuah games:

1) *Command receiver* program game menerima *input* perintah gamer menjadi interaksi dalam game

2) *Cloud gaming* memproses dan melakuan *renderer* yang menghasilkan interaksi game secara *real-time*. *Command* gamer berasal dari interpreter perintah, dan adegan permainan ditangkap oleh penangkap video ke video, yang kemudian dikompres oleh video *encoder*.



Gambar 2.1 Tipikal Cloud Gaming Service

Cloud gaming services akhir-akhir ini menjadi perhatian para pecinta game online yang keterbatasan perangkat komputer. Perusahaan besar seperti Google, Nvdia dan perusahaan game lainya turut mengembangkan layanan *cloud gaming*. sebagai contoh, Google telah merilis Google Stadia pada pertengahan bulan November 2019, namun Google Stadin belum seutuhnya dapat dinikmati karena dalam tahap pengembangan.

Popularitas yang luar biasa dari *game cloud* disebabkan keuntungan yang dapat dirasakan oleh *gamer'*s, developer game, dan penyedia jasa/ *service provide*r (Cai et al., 2016). Berikut beberapa keuntungan *cloud gaming* bagi para pecinta game dengan keterbatasan *hardware game* :

a. memiliki akses ke permainan mereka di mana saja dan kapan saja,
b. membeli atau menyewakan game sesuai permintaan,
c. hindari secara berkala meningkatkan perangkat keras mereka, dan
d. menikmati fitur unik seperti migrasi di komputer klien selama game sesi, mengamati turnamen yang sedang berlangsung, dan berbagi permainan ulangan dengan teman.

Berikut beberapa keuntungan *cloud gaming* bagi pengembang game :

a. berkonsentrasi pada satu platform, yang di gilirannya mengurangi biaya porting dan pengujian,
b. memotong pengecer untuk margin keuntungan yang lebih tinggi,

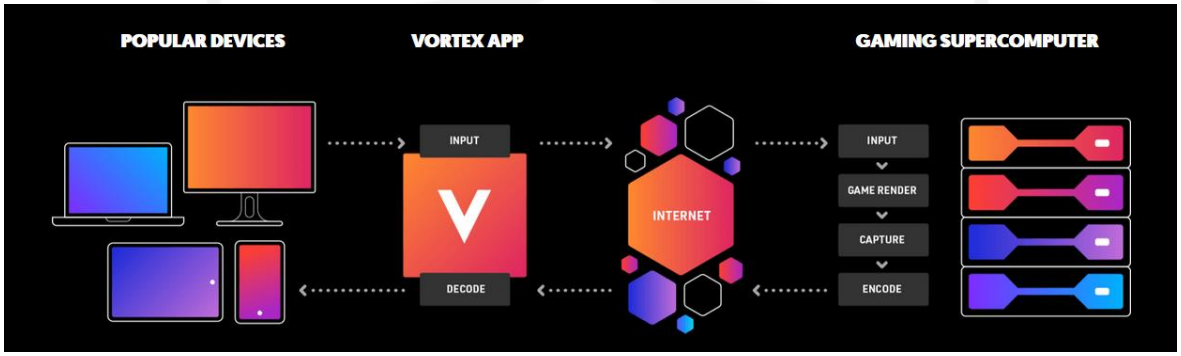
c. menjangkau lebih banyak *gamer*, dan
d. menghindari pembajakan karena perangkat lunak game tidak pernah diunduh ke komputer konsumen.

Berikut beberapa keuntungan cloud gaming bagi *service provider*:

a. mengarah pada model bisnis baru,
b. menciptakan lebih banyak tuntutan sumber daya *cloud* yang sudah dikerahkan,
c. menunjukkan potensi aplikasi eksekusi jarak jauh lainnya / baru, sejak cloud gaming memberikan batasan paling ketat pada berbagai hal sumber daya komputasi dan jaringan.

2.3 Skyegrid sebagai Cloud gaming service

Skyegrid merupakan cloud gaming service yang menawarkan layanan *streaming game*, yang andal mampu untuk mentransmisikan antarmuka game ke berbagai perangkat sepeti ponsel, laptop, dan smart TV selama komputer tersambung dengan internet, maka tugas perangkat komputer hanya menampilkan video *gameplay* serta command input *control* saat proses bermain game. Model teknologi didukung dengan infrastruktur *Processor* Intel Xeon, mencapai 512GB RAM dan NVIDIA GPU memungkinkan untuk bermain dari jarak jauh namun kualitas tertinggi dengan 60 frame per detik. Skyegrid memiliki 100 lebih koleksi game yang dapat dipilih dan dimainkan sesuai keinginan *gamer*. dengan adanya fitur algoritma adaptasi *bitrate* memungkinkan pengendali kontrol kualitas game yang ditransmisikan berdasarkan kecepatan internet saat sedang bermain game. selain itu Vortek dilengkapi dengan metode penyandian utuh yang di *encoder* menggunakan *hardware* khusus, sehingga mesin grafis dan CPU bebas untuk mendukung operasi lain.



Gambar 2.2 Teknologi Skyegrid Cloud Gaming (sumber: vortex.gg/technology)

2.4 *Framework for Reliable Experimental Design* (FRED)

Dalam proses menghadirkan bukti digital terkait penyelesaian kasus sangat penting adanya sebuah model/tahapan investigasi sesuai prosedur yang memiliki standarisasi yang diakui

oleh hukum, sehingga bukti digital yang diperoleh dapat diterima dalam proses pengadilan. Menganalisis data sembari mempertahankan integritas atau validitas data merupakan hal penting, karena hasil yang baik menambah keyakinan hakim dalam memutuskan perkara.

Framework for Realiable Experimental Design (FRED) difungsikan untuk menyederhanakan proses desain eksperimental, implementasi dan pengujian pada bukti digital, tanpa mengurangi nilai validasi secara forensik digital. FRED berfokus pada prosedur pendukung yang terlibat dalam melakukan rekayasa balik struktur data digital dan proses mengekstraksi dan menafsirkan konten digital dengan cara yang andal. Struktur FRED terdiri dari enam tahapan yaitu plan, *implement, evaluate, repeat, analysis* dan *confirm. Framework* yang diusulkan dirancang untuk menjadi sumber daya dalam bidang forensik digital, baik di industri dan akademisi, untuk mendukung dan mengembangkan praktik penelitian terbaik dalam disiplin ilmu.

2.4.1 Plan

Tahap perencanaan penelitian apa pun memberikan dasar yang kuat untuk memperoleh serangkaian hasil yang andal. Dalam beberapa kasus, menentukan rencana yang sesuai dapat dilakukan secara langsung dan yang lain harus beragam, tergantung pada kompleksitas struktur data digital yang sedang diselidiki. Sebagai bagian dari tahap perencanaan, harus jelas apa yang sedang diteliti oleh penelitian mana pun, oleh karena itu perlu untuk menentukan tujuan penelitian sejak awal.

a. Apa tujuan peneliti

   Apa yang kelihatannya merupakan pertanyaan yang jelas dapat dengan mudah dilewatkan, melakukan penelitian DF harus jelas tentang apa yang diharapkan akan dicapai oleh penelitian / tes yang direncanakan. Kegagalan untuk menentukan tujuan tertentu dapat menghasilkan temuan yang tidak spesifik dan tidak dapat diterapkan dari tes yang diberikan. Untuk memberikan contoh, penetapan tujuan dapat sesederhana menetapkan di mana sejarah Internet disimpan oleh aplikasi penelusuran Internet tertentu atau serumit rekayasa balik. struktur metadata internal dari setiap data riwayat Internet.

b. Kondisi dan lingkungan pengujian

   Pertimbangan lingkungan pengujian adalah kunci untuk memastikan validitas *output*. Hasil pengujian harus akurat, dapat diulang, dan dapat diterapkan, di mana ketiga variabel tunduk pada platform tempat pengujian dilakukan.

2.4.2 Implement

Mengikuti rencana yang dirancang dengan tepat, tahap kedua FRED melibatkan implementasinya. Implementasi mengharuskan pengguna untuk melakukan serangkaian tindakan untuk menyimulasikan perilaku pengguna sesuai dengan metodologi yang direncanakan. Tindakan ini merupakan "kumpulan data" yang digunakan selama pengujian.

Penggunaan kumpulan data merupakan faktor utama untuk dipertimbangkan dan bisa dibilang, elemen ini juga harus dipertimbangkan selama perencanaan metodologi. Menentukan set data uji yang akan digunakan selama penelitian apa pun (untuk menstimulasikan perilaku pengguna standar, yang kemudian dapat dievaluasi) melibatkan pembuatan set konten pengujian yang sesuai yang dapat digunakan untuk memperoleh hasil yang andal dari tes yang direncanakan, memastikan bahwa semua hasil memiliki telah habis. Data pengujian dapat mencakup serangkaian tindakan (seperti menyimpan atau mengedit file, atau memanfaatkan fungsi aplikasi) atau serangkaian input (seperti mencari istilah tertentu atau membuat konten tertentu). Konten pengujian yang efektif harus cukup beragam untuk mengimplementasikan pengujian pada kedalaman yang cukup untuk menghabiskan semua hasil potensial dan untuk memastikan fungsionalitas aplikasi atau objek yang diberikan dapat dipahami sepenuhnya. Juga, pada tahap-tahap FRED selanjutnya, satu set data yang cukup berbeda dan ekstensif memungkinkan reposisi pengujian untuk membangun perilaku yang konsisten selama tahap-tahap terakhir dari FRED.

2.4.3 Evaluate

Setelah implementasi tes yang sukses, hasilnya harus dievaluasi. Untuk melakukan ini, efek dari tes yang dilaksanakan pada sistem atau serangkaian artefak harus diidentifikasi dan dikumpulkan.

a. Mengidentifikasi dan menangkap perubahan yang ditimbulkan oleh pengujian. Setelah fase uji coba dilaksanakan, perubahan data digital harus diidentifikasi. Perubahan-perubahan ini mewakili bagaimana artefak / aplikasi tertentu berperilaku mengikuti penggunaan sistem, dan data yang disimpan mendokumentasikan tindakan ini. Proses mengidentifikasi perubahan tidak mudah, karena jumlah modifikasi yang terjadi pada sistem operasi setiap detik dan kedua perubahan pada file aplikasi spesifik dan struktur sistem operasi generik dan data log harus diselidiki dan dikumpulkan secara keseluruhan.

   Mengidentifikasi di mana perubahan terjadi setelah pengujian mungkin tidak membuktikan masalah karena data dapat dibatasi hanya dalam artefak itu. Namun, ketika mencoba mengidentifikasi perubahan yang ditimbulkan oleh pengujian

aplikasi yang berpotensi memicu peristiwa sistem yang luas, tugas tersebut menimbulkan tantangan yang lebih besar. Teknik pencarian kata kunci dapat membantu mendukung identifikasi perubahan atau penyimpanan kriteria pengujian yang digunakan, menghubungkan kembali ke tahap implementasi FRED dan kebutuhan untuk menggunakan data uji yang unik seperti yang dibahas sebelumnya.

b. Apakah hasil dalam batas-batas hipotesis awal

Penting juga pada tahap evaluasi untuk mempertimbangkan apakah hasil dari tes yang dilaksanakan berada dalam batas-batas apa yang diharapkan dari pengujian. Sebagai contoh, penelitian yang ada mungkin telah menginformasikan desain tes yang direncanakan, tetapi perubahan yang terjadi kemudian dalam suatu sistem mungkin berbeda dengan yang sebelumnya didokumentasikan atau apa yang awalnya diharapkan. Selain itu, mungkin tidak mungkin untuk mengidentifikasi perubahan sistem setelah pengujian yang dilaksanakan. Jika salah satu situasi hadir, opsi berikut tersedia.

i. Desain ulang tes: Peneliti harus mempertimbangkan apakah penelitian telah direncanakan secara memadai. Jika kelemahan dalam metodologi hadir pada tahap ini, maka perlu untuk kembali ke tahap perencanaan FRED dan desain ulang rencana berdasarkan pengalaman yang diperoleh dari putaran pengujian ini.

ii. Jalankan kembali tes: Semakin sering tes diulang, semakin besar peluang untuk membangun konsistensi dalam perilaku. Meskipun perubahan mungkin tidak berada dalam batas harapan awal, itu tidak berarti bahwa hasilnya tidak sesuai. Membangun perilaku konsisten berarti membangun perilaku faktual..

iii. Masalah kumpulan data uji: Pertimbangan juga harus diberikan pada data uji yang digunakan selama fase implementasi. Jika data uji adalah tipe yang salah atau kurang keragaman yang diperlukan untuk menyederhanakan penggunaan aplikasi di dunia nyata, mungkin gagal memicu peristiwa yang relevan pada suatu sistem.

iv. Jika perubahan tidak dapat dideteksi: Jika tidak mungkin mendeteksi perubahan dalam artefak target OS, ini bisa disebabkan oleh alasan berikut:

- Data yang diubah dapat dikompresi atau dienkripsi. Akibatnya pencarian kata kunci dapat menghasilkan klik terbatas (tergantung pada proses dekompresi / dekripsi sebelumnya dijalankan).

- Data uji mungkin tidak komprehensif / dari jenis yang salah, untuk memicu peristiwa yang cukup oleh aplikasi yang sedang diselidiki.
- Kesalahpahaman artefak / aplikasi yang sedang diselidiki berarti bahwa fungsinya secara fundamental berbeda dengan apa yang semula direncanakan untuk, memerlukan perencanaan ulang metode pengujian.
- Perubahan bukti dapat terjadi eksternal untuk penyimpanan lokal apa pun. Pertimbangkan bahwa informasi dapat disimpan di sisi cloud / server bahkan dalam memori fisik (terutama yang relevan untuk aplikasi peningkatan privasi).
- Kesalahan pengguna. Peneliti melakukan sesuatu yang secara fundamental salah dan akibatnya, gagal mendeteksi perubahan yang ada.

2.4.4 Repeat

Tujuan dari setiap pengujian adalah untuk mengembangkan struktur berulang yang menawarkan konsistensi dalam aplikasi dan kesehatan pengambilan keputusan. Rencana yang dirancang dengan tepat harus mempertimbangkan pengulangan untuk membedakan antara hasil yang dapat diandalkan dan yang telah dihasilkan oleh anomali, kejadian sekali pakai atau hanya kebetulan.

Pengulangan dan konsistensi hasil juga merupakan persyaratan bagi mereka yang berusaha mengembangkan algoritma parsing yang akurat untuk mengotomatiskan prosedur pemulihan dan interpretasi bukti yang dirancang. Di sini, konsistensi (dan penyimpangan) dalam struktur metadata harus diidentifikasi dengan benar untuk memastikan proses otomatis tidak mengabaikan konten yang berpotensi relevan. Pengembangan dan penggunaan pseudo-code (deskripsi yang disederhanakan dari suatu program dan strukturnya) untuk menguji setiap metadata yang teridentifikasi, *offset file* dan struktur internal akan mendukung proses ini.

Jika konsistensi dalam output dapat ditetapkan melalui pengulangan pengujian, hasilnya kemudian dapat dianalisis.

2.4.5 Analysis

Tahap analisis melibatkan interpretasi hasil yang dihasilkan dari pengujian yang dilakukan dan dikumpulkan selama tahap "mengevaluasi" dan "mengulang" FRED. Pada titik ini, seorang peneliti harus memiliki setidaknya dua set (kemungkinan lebih) hasil yang dihasilkan dari tes yang sama atau proses pengujian yang terkait. Fokus tahap analisis adalah untuk dapat menjelaskan secara pasti bagaimana artefak / aplikasi berfungsi dan apa yang

hasil tindakan pengguna tertentu. Sebagai gantinya, sebagian besar penelitian DF dilakukan menggunakan pengujian fungsional (juga disebut sebagai pengujian perilaku atau kotak hitam) (Khan dan Khan, 2012), di mana tindakan uji dipilih dengan cermat untuk memeriksa hasil yang diharapkan.

Tujuan dari fase analisis adalah untuk menentukan secara andal apakah sebagai hasil pengujian, temuan memungkinkan peneliti untuk mengkonfirmasi fakta yang terkait dengan pengujian. Jika hasil faktual tidak dapat ditetapkan, maka dua opsi menyajikan sendiri, revisi rencana pengujian dan strukturnya atau melakukan pengujian lebih lanjut (dengan peninjauan data uji yang digunakan) untuk mengidentifikasi mengapa ada kurangnya konsistensi dalam hasil.

2.4.6 Comfirm

Tahap akhir FRED adalah kemampuan untuk menegaskan sebagai fakta, hasil dan interpretasi pengujian yang telah terjadi dan untuk mendokumentasikan proses tersebut. Peneliti harus pada tahap ini dapat secara faktual menetapkan bahwa ketika menyelidiki suatu aplikasi / artefak , katakan “X”, menggunakan FRED, tindakan pengguna “Y” menghasilkan hasil “Z”. Pada titik mana, prosedur pengujian dapat didokumentasikan dan metodologi diformalkan untuk tinjauan sejawat, menunjukkan pengujian dasar yang ketat. Pertimbangan juga harus diberikan pada fakta bahwa hasil yang dihasilkan dari pengujian harus dapat dipertahankan, oleh karena itu persyaratan inti pada konfirmasi adalah untuk sepenuhnya mendokumentasikan semua prosedur sesuai dengan tahapan FRED.

Transparansi dalam pengujian yang dilakukan memungkinkan keandalan penelitian apa pun untuk dinilai secara obyektif dan potensi kelemahan dalam validitas hasil yang akan disorot sebelum mereka salah dimasukkan ke dalam penyelidikan. Sallavaci dan George (2013) menyatakan bahwa persyaratan peraturan baru untuk para ahli, terutama di Inggris dan Wales kemungkinan akan menempatkan saksi ahli DF dalam "mode pertahanan", mencoba untuk membenarkan setiap langkah evaluatif, ketika menulis laporan mereka '. Memanfaatkan FRED mendukung praktisi untuk menunjukkan penggunaan perencanaan menyeluruh, pengujian yang ketat dan interpretasi yang valid, yang dapat diandalkan di pengadilan hukum.

Dengan kecepatan perkembangan teknologi, praktisi DF akan sering menemukan aplikasi dan artefak selama investigasi mempertahankan fungsi yang tidak sepenuhnya dipahami. Dalam situasi ini, kepercayaan ditempatkan baik pada yang ada atau pengembangan penelitian yang valid ke dalam bidang-bidang ini. Ketergantungan pada penelitian DF oleh para praktisi sangat penting, di mana seringkali hal tersebut menjadi dasar

dari temuan investigasi. Konsekuensi dari temuan-temuan penelitian yang tidak valid dapat menjadi berat bagi semua yang terlibat, khususnya dalam proses pidana.

2.5 Dota

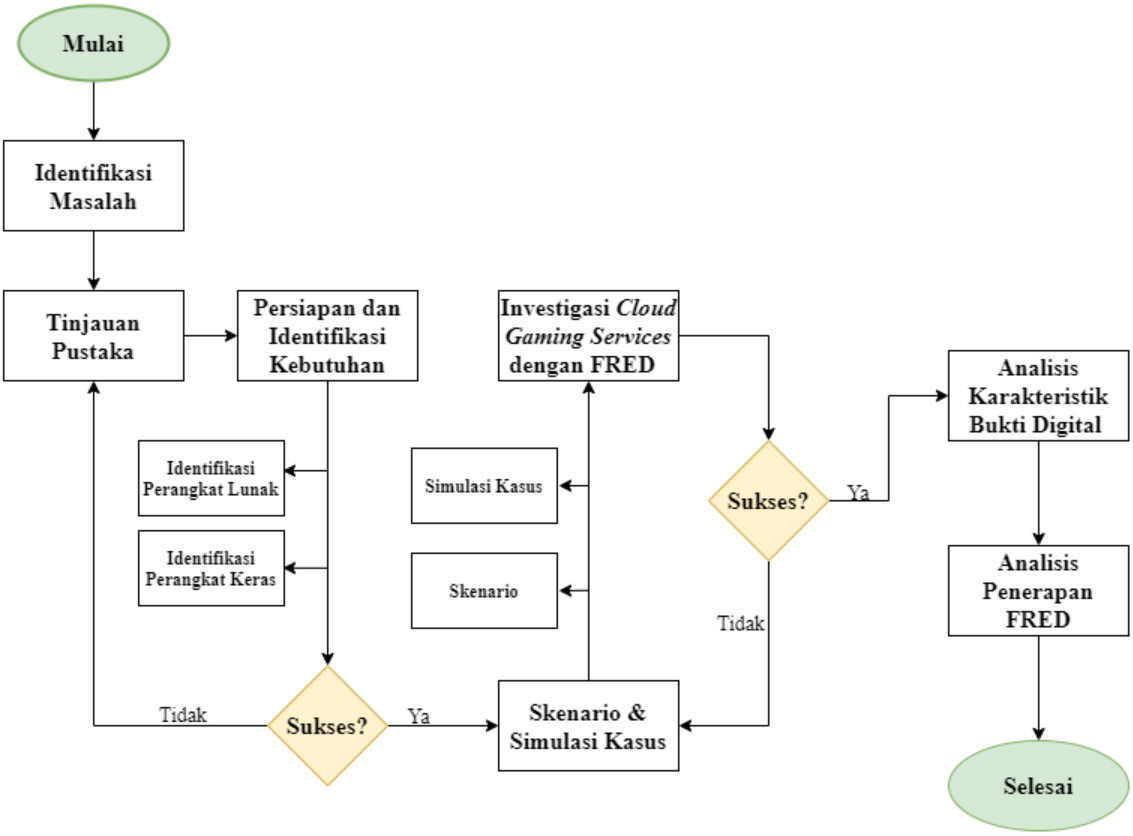
Dota 2 salah satu video game yang di rilis oleh Valve pada 9 Juli 2013 versi Windows. Dota 2 video game ber-*genre* MOBA (*Multiplayer Online Battle Arena)* merupakan lanjutan dari video game *Defense of the Ancients* (DotA). Skema model permainan pada Dota 2 hanya ada dua tim dalam pertandingan yang terdiri dari lima pemain. Masing-masing tim akan menempati dan mempertahankan altar mereka yang disebut *acient*, Agar para pemain dapat mempertahankan *acient* mereka, dan menyerang *acient* milik lawan para pemain akan mengendalikan dan mengontrol karakter *Hero* yang memiliki *skill,* atau *ability* unik yang berbeda-beda. Pada permainan ini, bertujuan menghancurkan *acient* lawan, dan mengumpulkan *point*, serta item *skill* untuk meningkatkan kekuatan serangan dan pertahanan *hero*. Selama permainan para pemain dapat saling berinteraksi dengan tim sendiri maupun tim lawan. Dota 2 dilengkapi dengan fitur pesan *chat* dan *voice,* sebagai media komunikasi tim untuk mengatur strategi bertahan dan menyerang tim lawan[3].

[3] https://en.wikipedia.org/wiki/Dota_2

BAB 3

Metode penelitian

Bab ini menjelaskan tentang bagaimana penelitian ini dilakukan, sehingga dapat diketahui tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan, membuat analisis terhadap hasil penelitian, serta kesulitan-kesulitan yang dihadapi. Adapun langkah-langkah atau tahapan-tahapan pada penelitian ini dapat dilihat pada Gambar 3.1.



Gambar 3.1 Metode Penelitian

3.1 Identifikasi Masalah

Identifikasi Masalah merupakan tahap awal dalam penelitian ini, hal ini dilakukan untuk memperoleh dan menemukan topik penelitian yang akan diteliti lebih lanjut. Proses identifikasi melalui berbagai macam fenomena, kejadian dan informasi yang di dapatkan dengan berbagai macam cara yang berhubungan dengan penelitian yang dilakukan. Dalam penelitian ini yang akan dilakukan adalah melakukan investigasi bukti digital pada Skyegrid sebagai *platform Cloud gaming* dengan penerapan *framework* FRED, sehingga dapat dijadikan sebagai gambaran atau perluasan studi forensik dalam penanganan bukti digital pada penyalahgunaan game online dengan menggunakan platform Skyegrid. Sementara itu

menilai dari pemanfaatan dan kegunaan dari framework FRED. agar penelitian lebih mengerucut Studi kasus penelitian mengarah pada layanan Skyegrid *cloud gaming* sehingga *Output* dari penelitian ini dapat dijadikan sebagai rekomendasi oleh penyidik dalam melakukan investigator pada game online dengan penggunaan *platform cloud gaming*.

3.2 Tinjauan Pustaka

Tinjauan pustaka dilakukan untuk mengumpulkan bahan-bahan informasi mengenai topik penelitian yang dapat bersumber dari buku, artikel, paper, jurnal, makalah, yang berupa teori, laporan penelitian, atau penemuan sebelumnya dan mengunjungi beberapa situs yang terdapat pada internet terkait dengan teori-teori tentang digital forensik, barang bukti, *cloud gaming*, *framework* FRED, Skyegrid *Cloud gaming service*, sehingga dapat menunjang tujuan akhir dilakukannya penelitian ini.

3.3 Persiapan dan Identifikasi Kebutuhan

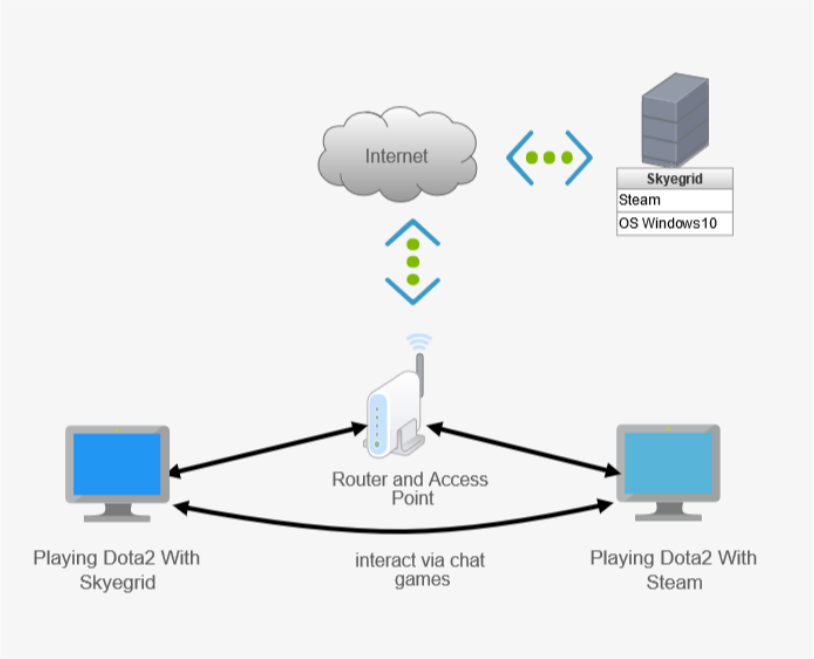
Merupakan tahapan identifikasi tentang kebutuhan yang akan digunakan dalam penelitian, sehingga terbangun sebuah lingkungan kerja sesuai dengan tujuan penelitian. Pada tahap ini akan dilakukan pengelompokan dimulai dari kebutuhan perangkat keras (*hardware*), dan menyiapkan perangkat lunak (*software*) yang diperlukan, serta membangun jaringan komputer untuk keperluan simulasi kasus saat penelitian.

3.4 Skenario dan Simulasi Kasus

Pada penelitian ini sebuah skenario simulasi penyalahgunaan game online Dota 2 berjalan pada platform Skyegrid yang dioperasikan pada sistem operasi Windows 10. Selanjutnya dilakukan analisis menggunakan *framework* FRED.

3.4.1 Persiapan Skenario

Tahapan skenario merupakan sebuah gambaran sederhana yang dapat ditangkap dari sebuah peristiwa kejadian yang telah berlangsung. Berikut Gambar 3.2 merupakan ilustrasi sederhana yang menggambarkan interaksi korban dengan pelaku kejahatan terhubung dengan *platform cloud gaming.* dengan demikian dapat mudah dipahami dalam pengumpulan informasi dan berjalan sesuai yang diharapkan dan dapat memenuhi target yang diinginkan. Berikut ini merupakan *topologi* yang diterapkan pada penelitian ini yang digambarkan pada Gambar 3.2



Gambar 3.2 Skenario Kasus Penelitian

3.4.2 Simulasi Kasus

Tahap pembuatan simulasi untuk mendukung proses pengambilan data agar penelitian yang dirancang mendapatkan hasil yang sesuai dengan rumusan yang sudah dibuat. Simulasi bertujuan untuk melakukan kegiatan uji coba dari skenario yang telah dibuat untuk menghasilkan pembuktian terhadap hipotesis yang dibuat. Simulasi dilakukan karena tidak memungkinkan untuk melakukan investigasi pada kasus sebenarnya. Tahap ini akan diperjelas dengan alur kerja simulasi dalam proses dilakukan pada yang selanjutnya akan dicari sebagai temuan dalam proses investigasi forensik.

3.5 Investigasi *Framework* FRED

Pada tahap ini dilakukan proses investigasi terhadap barang bukti elektronik berupa laptop yang digunakan pelaku penyalahgunaan terhadap game online. Seluruh Proses investigasi mengacu pada tahapan *framework* FRED yang memiliki beberapa aktivitas sebagai berikut:

3.5.1 Perencanaan (*Plan*)

Tahap Perencanaan sebagai fondasi awal investigasi yaitu dengan melakukan identifikasi rencana penelitian yang didasarkan dari tujuan penelitian. Tujuan penelitian bekerja pada lingkungan *cloud* sehingga investigasi dalam menghadirkan potensi bukti digital hanya dapat dilakukan pada perangkat PC desktop yang berjalan pada sistem operasi Windows. Selanjutnya merencanakan penggunaan metode forensik serta *tools* forensik sesuai tujuan penelitian, menggambarkan tahapan pengumpulan bukti digital.

3.5.2 Implementasi *(Implement*)

Tahap implementasi bertujuan untuk mengumpulkan barang bukti digital (*digital evidance*) yang dihasilkan melalui penerapan prosedur kerja dari tahap perencanaan yang telah diusulkan. Hasil dari tahap implementasi adalah barang bukti digital dari berbagai media penyimpanan komputer atau lalu lintas jaringan internet. Proses implementasi investigasi dilakukan secara bertahap dan sejalan dengan simulasi studi kasus dimulai hingga selesai sehingga barang bukti digital yang diperoleh utuh dan valid.

3.5.3 Evaluasi (*Evaluasi)*

Tahap evaluasi merupakan serangkaian proses pengamatan dan deteksi potensi bukti digital dengan menggunakan *tools* forensik yang telah direncanakan. Pemeriksaan dilakukan pada sistem atau artefak barang bukti digital yang telah dikumpulkan ditahap implementasi.

3.5.4 Ulangi (*Repeat)*

Tujuan dari tahap ini untuk menciptakan hasil pengujian bernilai konsistensi oleh karena itu pada tahap ini tahap implementasi dan evaluasi diuji kembali dengan menggunakan perangkat atau studi kasus yang berbeda, namun hasil yang didapat memiliki nilai konten yang konsisten dengan hasil temuan pada tahap implementasi. Dengan demikian rencana yang dirancang dinyatakan tepat dan dapat diandalkan dalam penanganan studi kasus yang dihadapi.

3.5.5 Analisis (*Analysis)*

Tahap analisis bertujuan untuk menentukan secara andal apakah sebagai hasil pengujian, temuan memungkinkan peneliti untuk mengkonfirmasi fakta yang terkait dengan pengujian. Analisis melibatkan interpretasi hasil yang diperoleh dari pengujian melalui proses pengumpulan pada tahap "*evaluate*" dan "*repeat*". Analisa dilakukan dengan cara: mengidentifikasi akun *login* user, menelusuri rangkaian kejadian berdasarkan catatan waktu aplikasi, dan *log* komunikasi teks dan audio, sehingga peneliti mampu mendapatkan kesimpulan.

3.5.6 Konfirmasi (*Confirmation)*

Tahapan ini berbicara mengenai temuan yang terdapat pada langkah-langkah sebelumnya dalam bentuk laporan yang memuat temuan faktual dari hasil analisis serta prosedur pengujian. Semua hasil dan metodologi yang diimplementasikan didokumentasi untuk tinjauan penanganan kasus yang sama dikemudian hari.

3.6 Analisis Karakteristik Bukti Digital

Merupakan tahapan penyajian dan pemaparan dari hasil temuan barang bukti digital yang diperoleh melalui tahapan investigasi dengan penerapan *framework* FRED. Temuan disajikan berdasarkan artefak yang dianalisis untuk melihat karakteristik bukti digital. Berdasarkan studi kasus pada lingkup *cloud* maka sajian karakteristik melalui proses investigasi pada tiga potensi barang bukti digital yaitu pada *network traffic*, RAM Volatil, dan HHD sehingga dapat di gambarkan pada tabel berikut:

Tabel 3.1 Karakteristik bukti digital yang ditemukan

No.	Informasi Bukti Digital	Artefak Bukti Digital		
		Network *Traffic*	*Voletile Memory* (RAM DUMP)	Non *Voletile Memory Image* harddsik
1	Metode Akuisisi			
2	Jenis *image*			
3	Format *image*			
4	*Tools* Akuisisi			
5	*Tools* Analisis			
6	Ukuran Artefak			
7	Jenis temuan penting			
8	Lokasi file temuan penting			

3.7 Analisis Penerapan FRED

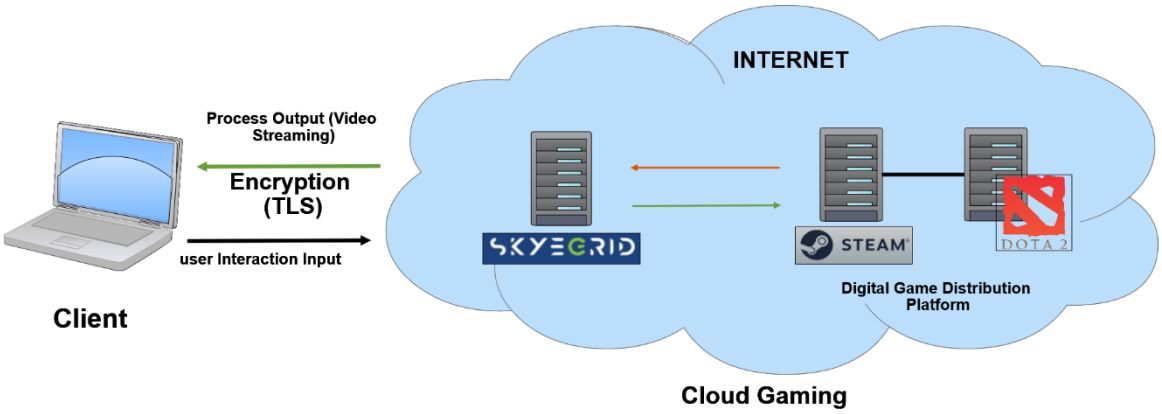
Pada tahap ini merupakan penjelasan kritis terkait penerapan *framework* FRED pada studi kasus Skyegrid *game online services* yang telah dilakukan. Analisis dipaparkan berdasarkan aktivitas yang sudah dilakukan dan menyimpulkan dengan memberikan evaluasi terhadap *fremework* FRED yang telah digunakan. Evaluasi *framework* digunakan untuk melihat keunggulan, kekurangan dan keberhasilan dalam menghadirkan bukti digital pada Skyegrid *platform cloud gaming*.

BAB 4

Hasil dan Pembahasan

4.1 Identifikasi Masalah

Platform Skyegrid termasuk dalam katagori *cloud gaming* berbasis *file streaming*, sebagaimana terlihat pada Gambar 4.1. Konsep dasar proses kerja dari layanan Skyegrid seperti *remote* komputer pada umumnya, *Client* wajib menjalankan aplikasi Skyegrid terlebih dahulu baru kemudian tampilan layar *Client* langsung mengarah pada *console game* setelah *Client* menjalankan *game* yang tersedia pada *dashboard* Skygrid. Selanjutnya *Client* akan diarahkan ke *lobby* game setelah *login* Steam (*Digital Game Distribution platform*). Semua interaksi *user* berupa *input keyboard* dan *mouse* serta *output* dari server Skyegrid berupa video *streaming* ditransmisikan melalui jaringan internet yang ter-*encryption*.



Gambar 4.1 Mekanisme Skyegrid Cloud gaming

Pada Gambar 4.1 menjelaskan dari proses kerja layanan Skyegrid secara umum dalam pengoperasian game online di platform Skyegrid. Interaksi *client* seperti *input* dari *mouse* dan *keyboard* dapat diteruskan ke *cloud gaming* setelah terjadi sebuah hubungan koneksi jaringan internet dengan lalu lintas yang terenkripsi. Dalam penanganan barang bukti digital dengan konsep gambar di atas akan sangat sulit, karena adanya metode *encryption* dari metode keamanan TLS (*Transport Layer Security*). Sementara itu sesuai dengan karakteristik investigasi pada *cloud computing* dalam penanganan bukti digital tidak memungkinkan dilakukan investigasi pada sisi server.

Pada literatur (Taylor et al., 2019) telah mengimplementasikan dan menjelaskan proses investigasi game online dengan menyimulasikan model *client server*. Hasil investigasi dapat menemukan beragam bukti digital baik dari sisi *client* maupun server. Namun penelitian yang telah dilakukan tersebut tidak dapat diadopsi ke dalam penelitian ini,

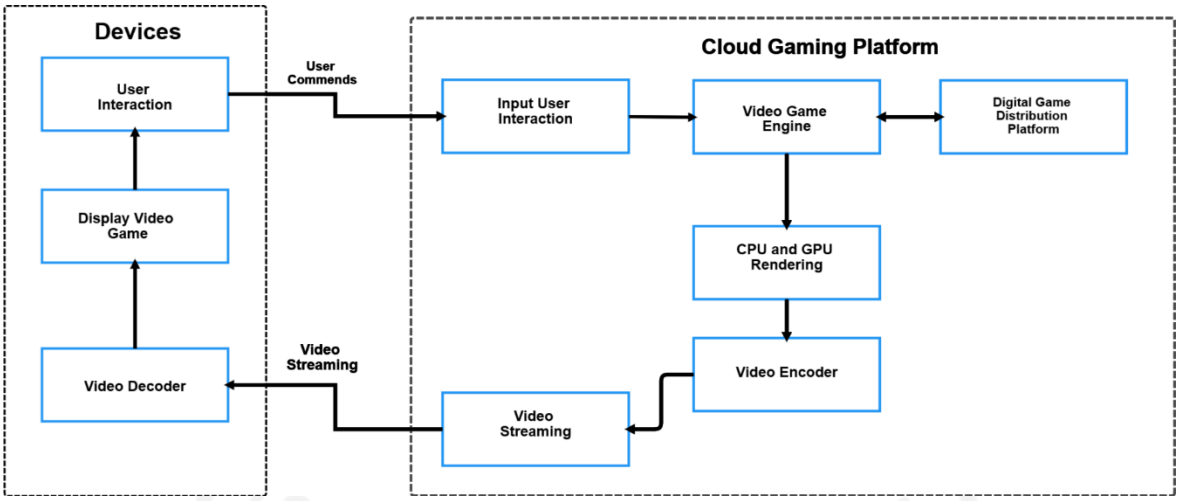
dengan membuat skema *client* server atau mengembangkan laboratorium riset, dikarenakan *resource*, literatur, dan infrastruktur Skyegird *cloud gaming* tidak bersifat terbuka (*opensource*). Oleh karena itu proses investigasi pada sisi *cloud gaming services* juga tidak mungkinkan untuk dilakukan investigasi sehingga pada penelitian ini fokus pencarian bukti digital pada perangkat *client*.

Dalam penanganan barang bukti digital pada platform *cloud gaming* yang perlu diperhatikan adalah pada mekanisme *data deletion*, secara otomatis akan menghapus atau menimpa data yang disimpan pada *storage cloud gaming*, hal ini dapat menyebabkan hilang data selamanya, untuk itu penanganan barang bukti digital harus dilakukan segera setelah menemukan *username* dan *password* login pada game.

4.2 Tinjauan Pustaka

Layanan *Cloud gaming* disebut *gaming on demand*, merupakan platform game daring dari penggabungan teknologi komputasi awan yang menyediakan fasilitas sumber daya penyimpanan data tidak terbatas, dipadukan dengan teknologi komputasi grafis tingkat tinggi sehingga memungkinkan pemain mengontrol dan menjalankan game yang diinginkan melalui internet dari beragam perangkat gawai secara daring. Layanan *cloud gaming* menawarkan sumber daya *hardware* grafis dan penyimpanan tidak terbatas sebagai kebutuhan utama menjalankan sebuah game. Secara mendasar konsep platform *cloud gaming* terlihat sebagaimana pada Gambar 4.2. Alur proses dimulai dari *user* mengirimkan aksi *commands* seperti gerakan *mouse* atau aksi perintah melalui *keyboard*. Dalam hitungan mili detik aksi *commands* tersebut diterima server dan mentransmisikan kembali setiap pergerakan gambar ke *display* monitor *user* melalui jaringan internet. Pada proses lainnya yang terjadi pada server adalah interaksi dengan digital distribusi video game (Steam) sebagai proses perizinan dan hak akses ke dalam video game, yang sudah diunduh dan tersimpan pada server *cloud gaming* (Wu, 2014).

Skyegrid merupakan salah satu layanan *cloud gaming* yang menawarkan akses ratusan video game yang telah tersedia pada server-server *cloud* Skyegrid. Skyegrid terkategori pada *cloud gaming* berbasis *file straming*, sebelum bermain menggunakan Skyegrid, gawai terlebih dahulu di-*install* aplikasi Skyegrid. Game dialirkan langsung dari server-server Skyegrid kemudian langsung dialirkan ke *display* gawai *user* melalui jaringan internet. Game berjalan tanpa di emulasi atau di-*install* pada gawai, hal ini membuat *user* tidak melakukan pengunduhan, pemasangan dan pembaharuan game, memilih layanan Skyegrid sebagai platform *game online* merupakan solusi para gamer dari pada membeli gawai yang mahal, serta lebih fleksibel untuk bepergian.



Gambar 4.2 Gambaran Platform Cloud Gaming Services

Dota 2 salah satu video game yang di rilis oleh Valve pada 9 Juli 2013 versi Windows. Dota 2 video game ber-*genre* MOBA (*Multiplayer Online Battle Arena)* merupakan lanjutan dari video game *Defense of the Ancients* (DotA). Skema model permainan pada Dota 2 hanya ada dua tim dalam pertandingan yang terdiri dari lima pemain. Masing-masing tim akan menempati dan mempertahankan altar mereka yang disebut *acient*, Agar para pemain dapat mempertahankan *acient* mereka, dan menyerang *acient* milik lawan para pemain akan mengendalikan dan mengontrol karakter *Hero* yang memiliki *skill*, atau *ability* unik yang berbeda-beda. Pada permainan ini, bertujuan menghancurkan *acient* lawan, dan mengumpulkan *point*, serta item *skill* untuk meningkatkan kekuatan serangan dan pertahanan *hero*. Selama permainan para pemain dapat saling berinteraksi dengan tim sendiri maupun tim lawan. Dota 2 dilengkapi dengan fitur pesan *chat* dan *voice,* sebagai media komunikasi tim untuk mengatur strategi bertahan dan menyerang tim lawan[4].

4.3 Persiapan Sistem

Persiapan sistem mencakup kebutuhan perangkat lunak dan perangkat keras, sebagai pendukung kelancaran penelitian ini. Kebutuhan perangkat lunak yang digunakan mencakup kebutuhan sistem aplikasi Skyegrid dan *tools* digital forensik, dan perangkat keras mencakup komputer/laptop, maupun pendukungnya. Persiapan sistem pendukung penelitian ini antara lain:

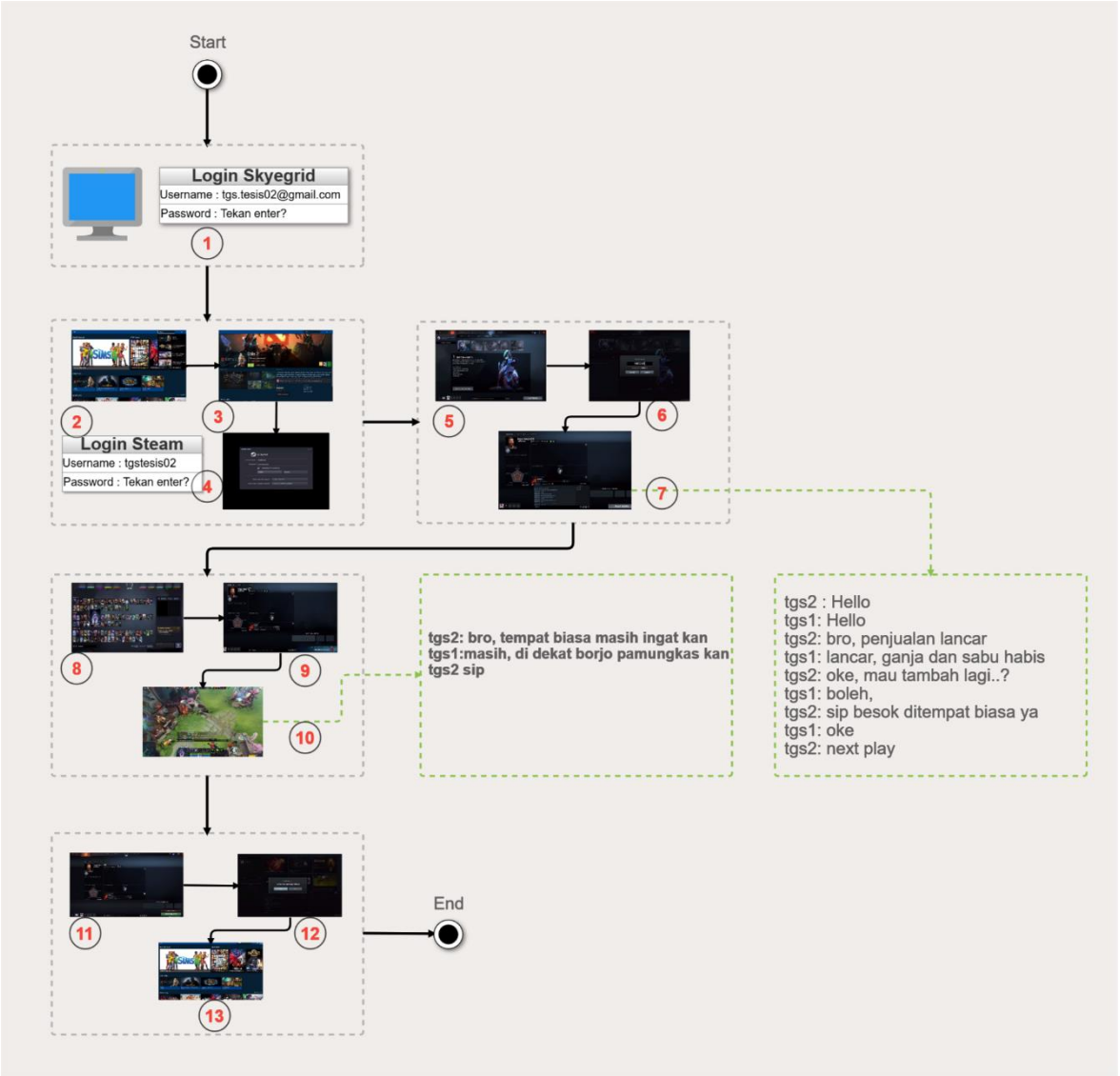
[4] https://en.wikipedia.org/wiki/Dota_2

Tabel 4.1 Persiapan perangkat keras dan perangkat lunak.

No.	Hardware/ Software	Keterangan
1	Laptop DELL Inspiron 14, Core i5, SSD 128 GB (Laptop Pelaku)	Hardware
2	Laptop Asus VIvoBook Flip 14, Corei7, SSD 128, HDD 1 TB (Laptop Investigator)	Hardware
3	SATA 3.0 HDD Docking Station	Hardware
4	HDD 3.0 TB WD30PURX	Hardware
5	Sistem Operasi Windows 10 Profesional dengan arsitektur 64bit	Sistem Operasi (Komputer pertama)
6	Sistem Operasi Windows 10 Profesional dengan arsitektur 64bit	Sistem Operasi (Komputer kedua)
7	FTK Imager 4.2.0.13	Forensic Tools
8	Sleuth Kit Autopsy Forensics 4.15.0	Forensic Tools
9	Network Miner 2.5 Windows	Forensic Tools
10	Wireshark Version 3.2.1 Windows	Forensic Tools
11	WinHex 18.7 Windows	Forensic Tools
12	Volatility Windows	Forensic Tools
13	Hashmyfile	Tools Hashing

4.4 Skenario dan Simulasi Kasus

Tahapan ini memiliki peranan penting untuk memperoleh hasil yang diinginkan dalam penelitian nantinya. Mendesain sebuah skenario berupa gambaran dari peristiwa nyata kemudian diilustrasikan sederhana menjadi sebuah topologi jaringan dan dilanjutkan dengan melakukan simulasi tindak kejahatan penyebaran obat-obatan terlarang (narkoba) dengan memanfaatkan layanan *cloud gaming* Skyegrid. Skenario penyebaran narkoba dilakukan melalui fitur *chating* game online, salah satu *player* dengan menggunakan akun tgsatesis02 sebagai penyalur narkoba, selebihnya sebagai pendistribusi menggunakan akun game tgstesis01. Skenario investigasi dalam pengumpulan barang bukti digital pada perangkat laptop sebagai barang bukti elektronik dilakukan dalam keadaan menyala dan dikerjakan bersamaan dengan simulasi penyalahgunaan game online dilakukan. Pada penelitian ini, simulasi dilakukan dua kali dengan studi kasus game online yang berbeda pertama menggunakan game Dota 2, dan kedua menggunakan game CS:GO. Secara umum untuk gambaran dari skenario komunikasi para pelaku diperjelas melalui ilustrasi Gambar 4.3.



Gambar 4.3 Tahap simulasi studi kasus

Tahapan pada gambar diatas dapat dijelaskan sebagai berikut:

1. Tersangka *login* pada aplikasi Skyegrid dengan menggunakan *username* : tgs.tesis02@gmail.com, password: Tekan enter?
2. Selah berada di *dashboard* Skygrid tersangka menjalankan game Dota 2 kemudian *user* tgs.tesis02 melakukan *login* menggunakan akun Steam dengan *username*: tgstesis02, *password* : Tekan enter?
3. Setalah berada di *lobby* game Dota 2, tersangka mengundang teman dengan ID *user* : 1092245, untuk main bersama (mabar).
4. Setelah undangan pertemanan diterima, mereka melakukan komunikasi menggunakan fitur *chat*, adapun isi *chat* sebagai berikut:

Tabel 4.2 List Chatting di Lobby Game

User	Isi chat
tgs.tesis02	Hello
tgs.tesis01	Hello
tgs.tesis02	bro, penjualan lancar
tgs.tesis01	lancar, ganja dan sabu habis
tgs.tesis02	oke, mau tambah lagi..?
tgs.tesis01	boleh,
tgs.tesis02	sip besok ditempat biasa ya
tgs.tesis01	Oke
tgs.tesis02	next play

5. Selanjutnya memilih *hero* / karakter pemain untuk memulai bertanding game Dota2, disaat game berjalan, mereka kembali melakukan komunikasi menggunakan fitur *chat*. Adapun isi percakapan sebagai berikut:

   Tabel 4.3 List *chatting* didalam geme

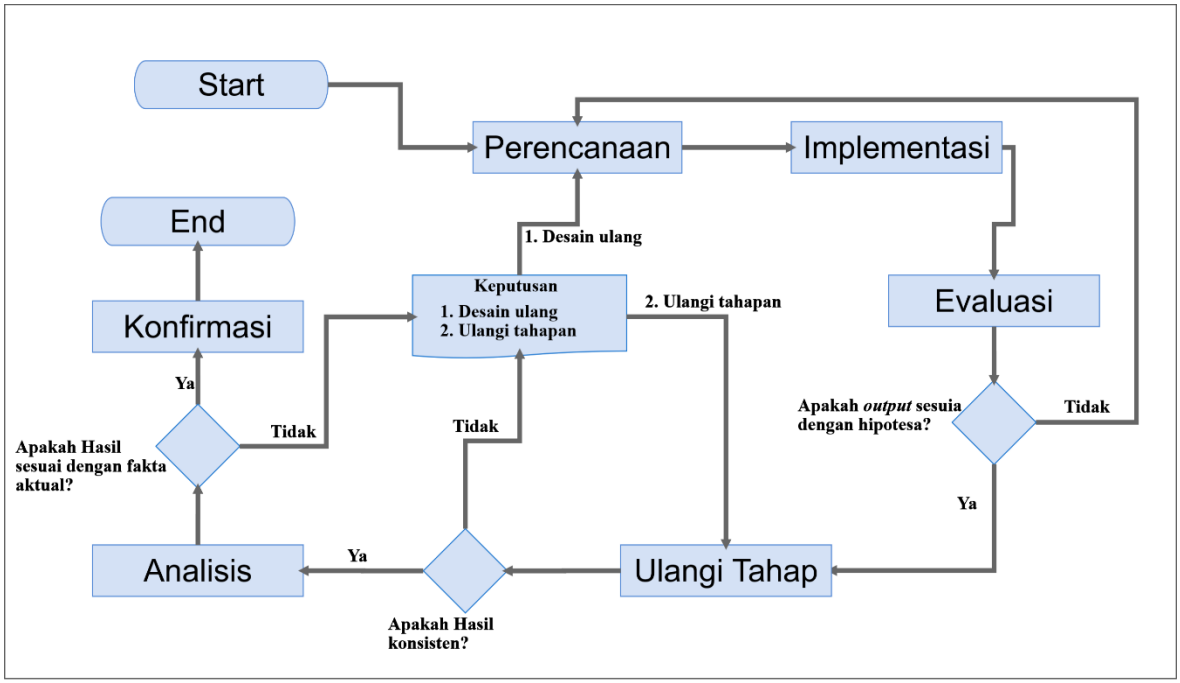
User	Isi chat
tgs.tesis02	bro, tempat biasa masih ingat kan
tgs.tesis01	masih, di dekat borjo pamungkas kan
tgs.tesis02	Sip

6. Terakhir yaitu kedua *user logout* dari permainan, Steam dan Skyegrid.

4.5 Investigasi FRED Framework

Sebagaimana yang dipaparkan pada poin **4.1 identifikasi masalah**, bahwasanya dalam investigasi pada platform Skyegrid hanya dapat dilakukan pada perangkat *client*. Adapun metodologi tahapan forensik akan mengacu pada *framework* FRED (*Framework for Reliable Experimental Design*) yang di desain oleh (Horsman, 2018). Menurutnya, FRED dikembangkan sebagai upaya untuk menyederhanakan tahapan desain, implementasi dan pengujian pada *framework* SWGDE dan NIST. Selain itu, FRED didesain dengan keutamaan dalam menyediakan langkah-langkah kerja secara formal untuk mengembangkan prosedur pengujian yang baik secara keilmuan digital forensik. Adapun FRED terdiri dari enam langkah kerja di antaranya adalah perencanaan, implementasi, evaluasi, proses pengulangan, analisis dan konfirmasi.

Penerapan langkah kerja FRED sebagai prosedur investigasi bukti digital pada ruang lingkung Skyegrid *cloud gaming services.* Berikut alur proses investigasi pada platform Skyegrid yang diusulkan pada penelitian ini.



Gambar 4.4 Alur investigasi *framework* FRED (Horsman, 2018)

4.5.1 *Plan* (Perencanaan)

Tahap perencanaan merupakan langkah pertama yang akan disusun pada setiap penelitian, guna untuk memfokuskan arah penelitian sehingga hasil dari sebuah penelitian menghasilkan nilai yang diharapkan. Pada ruang lingkup studi kasus dirancang beberapa kebutuhan penelitian berdasarkan dokumen standar SNI ISO/IEC 27037:2014 terkait prosedur pengolahan barang bukti elektronik, ada beberapa aktivitas perencanaan yang diterapkan pada tahapan ini, yaitu:

1) Identifikasi

Proses identifikasi meliputi pencarian, mengenali, dan mendokumentasikan semua barang elektronik yang berpotensi menjadi barang bukti digital. Pada studi kasus penelitian ini telah teridentifikasi perangkat desktop berupa laptop DELL Inspiron dengan sistem operasi Windows 10, kapasitas RAM 4 GB, harddisk 120 GB, serta menggunakan jaringan internet berupa Wi-Fi. Di dalam sistem operasi Windows 10 terpasang aplikasi Skyegrid desktop.

2) Pengumpulan

Proses perencanaan dalam penanganan barang bukti digital, termasuk metodologi pengumpulan bukti digital dengan menggunakan *tools* yang paling sesuai berdasarkan situasi, biaya, dan waktu. Pada studi kasus ini, pengumpulan barang bukti digital pada penelitian ini mengikuti penelitian terdahulu yang telah dilakukan oleh (Tabuyo-Benito et

al., 2019; Taylor et al., 2019) yang telah menjelaskan bahwa dalam penelitian tersebut pengumpulan bukti digital dilakukan dari tiga sumber barang bukti digital yaitu pada *traffic* jaringan internet, data volatil (RAM), dan data non volatil (HDD). Sehingga pada penelitian ini dalam pengumpulan bukti digital akan dilakukan pada ketiga sumber data tersebut dengan menggunakan *tools open source* sebagai mana telah dipaparkan pada Tabel 4.1 Persiapan perangkat keras dan perangkat lunak.

3) Akuisisi

Dalam dokumen SNI ISO/IEC 27037:2014, akuisisi merupakan sebuah proses untuk membuat salinan barang bukti digital dan mendokumentasikan metodologi yang digunakan serta aktivitas yang diterapkan. Dalam melakukan akuisisi pada studi kasus ini memilih metode *live acquisition data* karena dinilai yang paling sesuai dengan studi kasus. Metode *live acquisition data* pada penelitian ini mengacu pada penelitian (Tabuyo-Benito et al., 2019), yaitu dengan melakukan proses akuisisi secara langsung melalui beberapa perangkat laptop seperti jaringan komputer (Wi-Fi), *valotile memory* (RAM), dan non *volatile memory* (HDD). Perencanaan akuisisi di jelaskan sebagai berikut:

i) Network *traffic capture*, melakukan penangkapan lalu lintas data yang ditransmisikan melalui NIC (*network interface card*) yang disebut Wi-Fi. Menggunakan *tool* Wireshark, *start capture* dilakukan di awal sebelum simulasi studi kasus penyalahgunaan pada platform Skyegrid dilakukan. Kemudian proses *capture* dihentikan setelah seluruh rangkaian simulasi telah selesai, dan terakhir melakukan validitas dengan cara *hashing* MD5 agar hasil *network capture* yang di dapatkan otentik dan terjaga keasliannya.

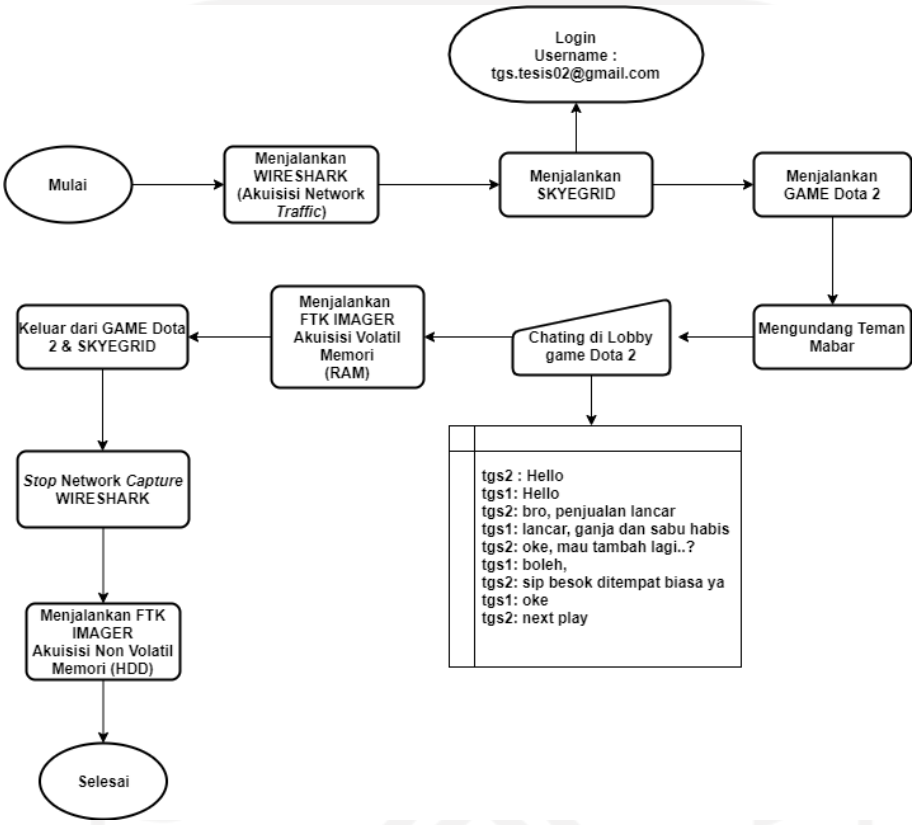
ii) *Volatile memory* (RAM), melakukan pengumpulan data volatil pada RAM dengan cara *dumping* memori menggunakan *tool* FTK Imager. Proses akuisisi memori di lakukan saat simulasi game sedang berlangsung (*in match*) dikarenakan sifat dari data volatil yang dapat menguap. Untuk analisis data *volatile memory* menggunakan *tool* FTK Imager dan WinHex.

iii) *Non volatile memory* (HDD), melakukan akuisisi pada *harddisk* dengan menerapkan metode *physical acquisition,* yaitu melakukan *imaging copy* bit per bit keseluruhan pada *harddisk* menggunakan *tool* FTK Imager yang ditransfer pada HHD *externeal* menggunakan *docking station*.

4.5.2 Implementasi

Pada tahap implementasi bertujuan untuk mengumpulkan barang bukti digital pada platform Skyegrid sesuai dengan tahap perencanaan. Pengumpulan barang bukti digital dilakukan

pada perangkat *client* dalam keadaan masih menyala dan proses pengumpulan barang bukti digital pada penelitian ini diskenariokan sebagaimana pada Gambar 4.5 yaitu berjalanya proses simulasi kejahatan juga diiringi dengan proses pengumpulan barang bukti digital dengan tujuan potensi bukti digital yang diperoleh lebih banyak dan beragam. Kemudian agar proses pengumpulan dapat terdokumentasi berikut tahapan pengumpulan barang bukti yang diusulkan sebagai berikut:

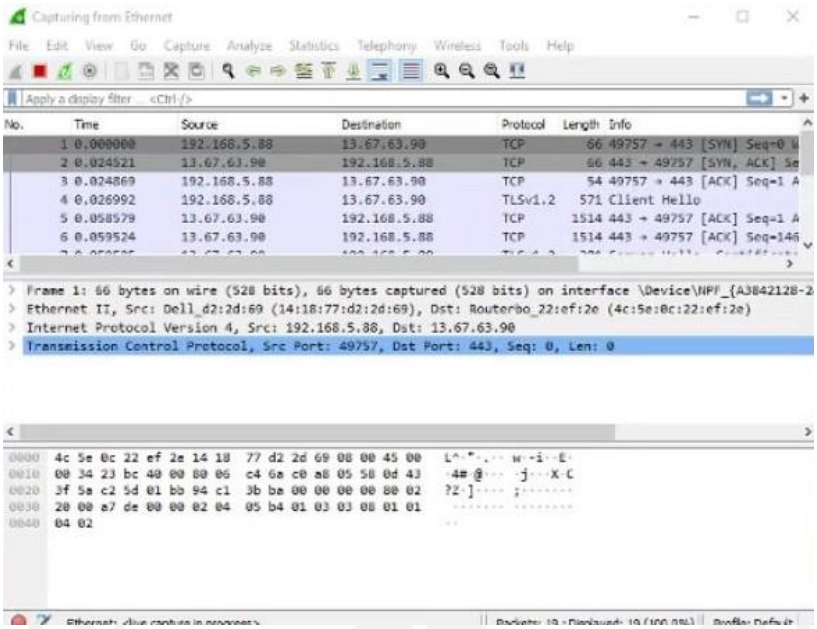


Gambar 4.5 Mekanisme akuisisi barang bukti digital

Akuisisi sebagai proses pengumpulan barang bukti digital dilakukan bersamaan dengan melakukan proses simulasi tindakan kejahatan, sesuai dengan alur pada Gambar 4.5 yang diperjelas sebagai berikut:

1) Network *traffic capture*

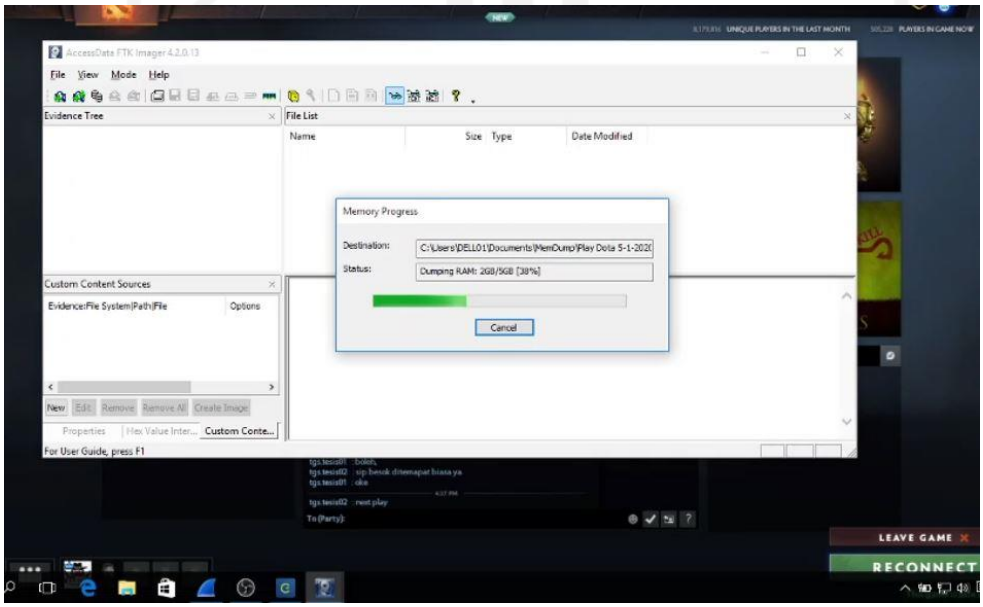
Proses pertama dalam pengumpulan barang bukti pada lalu lintas jaringan internet, dengan menggunakan aplikasi Wireshark dengan cara menangkap seluruh *traffic* jaringan Wifi pada laptop Dell. Proses *capturing traffic* dijalankan di awal sebelum proses simulasi *login* pada Skyegrid dan bermain game, kemudian proses *capture traffic* dihentikan ketika proses simulasi bermain game telah selesai.



Gambar 4.6 Akuisisi dengan *capture traffic* jaringan wifi

2) *Volatile* Memori

Proses kedua adalah pengumpulan barang bukti digital pada memori volatil (RAM) dengan cara melakukan dump memori menggunakan tools FTK Imager. Informasi yang tersimpan di memori RAM bersifat volatil atau mudah menguap, oleh sebab itu pada proses dump memori dilakukan saat simulasi bermain game sedang berlangsung atau dapat disebut live akuisisi setelah user tgs.tesis02 selesai melakukan chating kepada user tgs.tesis01 di dalam permainan.



Gambar 4.7 Proses akuisisi *volatile* memori *dump*

Proses selanjutnya adalah melakukan verifikasi nilai *hash*, sebelum hasil *dump* memori di pindah atau di *copy* ke laptop penyidik.

3) Non *Volatile Memory* (HDD)

Proses terakhir mengumpulkan bukti digital dari *harddisk* laptop Dell. Proses akuisisi menggunakan metode *Physical Acquisition* harddisk dengan tipe *bit-stream disk-to-image file. Tool* yang digunakan adalah FTK Imager. Ketika melakukan *create image file*, lokasi penyimpanan diarahkan di harddisk *external* berkapasitas 3.0 TB dengan menggunakan Docking station.

Gambar 4.8 Proses *imaging* harddisk

Setelah seluruh proses akuisisi selesai, maka dapat dipaparkan hasil akuisisi dengan nilai *hash* MD5. Barang bukti digital dari *network traffic* dan RAM memori volatil dilakukan *hashing* MD5 menggunakan *tool* Winmd5free untuk melihat nilai *hash* MD5. Berikut tabel dari hasil akuisisi dan nilai *hashing* MD5 pada platform Skyegrid.

Tabel 4.4 Hasil Akuisisi dan nilai hash MD5

No.	Barang Bukti	Nilai Hash	Hasil dari
1	play dota 5-1-2020.pcap	f22cb11bb805536747d74e3098e0ba72	Capture traffic jaringan
2	Play Dota 5-1-2020.mem	9f4c07b1caf5449257d54298c99043e6	RAM Memori *dump*
3	Steam-chat-dota	fdbca6f70ff0b6d615eb06ae2b331a6f	*Imaging hard disk*

4.5.3 Evaluasi

Pada tahap ini akan melakukan evaluasi pada *image* yang diperoleh dari proses sebelumnya. Evaluasi bertujuan untuk menghadirkan informasi data yang *realiable* dan relevan berkaitan dengan kasus. Proses evaluasi dilakukan dengan melakukan duplikasi terhadap hasil akuisisi yang diperoleh, selanjutnya agar integritas dari hasil akuisisi tetap terjaga keasliannya, maka

perlu di identifikasi keasliannya dengan melakukan pengecekan *hash* MD5 pada duplikasi hasil akuisisi tersebut menggunakan tool Winmd5free. Adapun hasil validasi dapat dilihat pada tabel berikut ini .

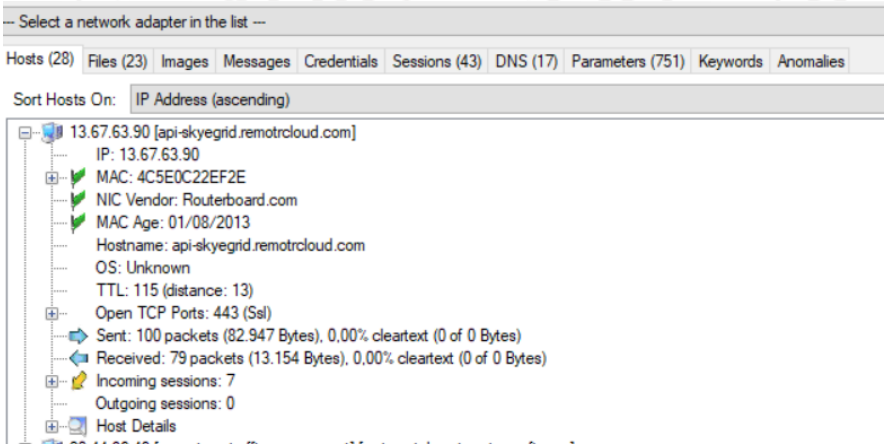
Tabel 4.5 Hasil verifikasi Hash MD5 dari Barang bukti game Dota 2

No.	Barang Bukti	Nilai Hash	Hasil dari	Keterangan
1	play dota 5-1-2020.pcap	f22cb11bb805536747d74e3098e0ba72	Capture traffic jaringan	*Verified*
2	Play Dota 5-1-2020.mem	9f4c07b1caf5449257d54298c99043e6	Memori *dump*	*Verified*
3	Steam-chat-dota	fdbca6f70ff0b6d615eb06ae2b331a6f	*Imaging hard disk*	*Verified*

Setelah hasil duplikasi dari *imaging* otentik, proses selanjutnya adalah melakukan penelusuran potensi bukti digital untuk menguak kejahatan pada platform Skyegrid. Berikut pemaparan penyelidikan berdasarkan klasifikasi artefak digital yang diperoleh:

1) Analisis barang bukti Network *traffic capture*

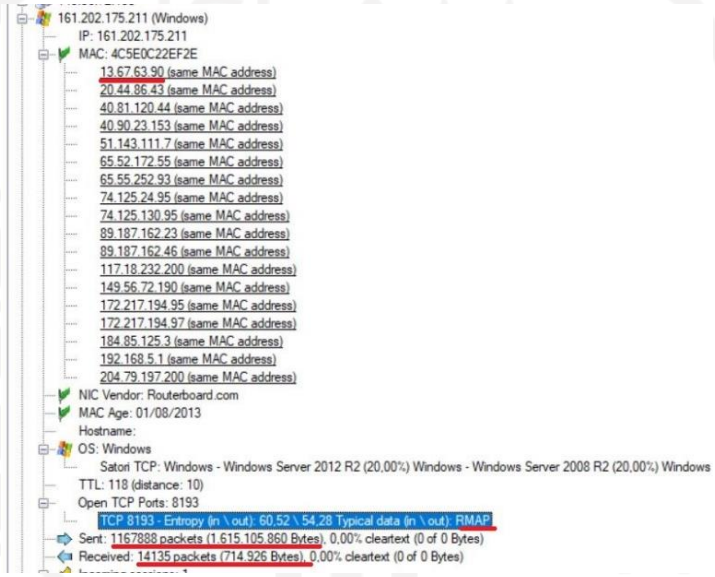
Eksplorasi pada artefak jaringan menggunakan *tools* Wireshark dan Network Miner. Diawali dengan menggunakan Network Miner supaya visualisasi IP dan DNS lebih mudah di amati. Fokus awal adalah mengamati pada *keyword* "Skyegrid" untuk mempermudah penemuan potensi bukti digital. Pada tab *Hosts* ditemukan dengan IP *Address* 13.67.63.90 dan MAC *address* 4C5E0C22EF2E dengan DNS "api-skyegrid.remotrcloud.com". Setelah menekan tombol + untuk melihat detail isi dari paket data, tampak komunikasi data melalui protokol TCP, komunikasi menggunakan keamanan dengan *port* 443 ssl, namun transaksi data *sent* dan *receive* sangat kecil ukuran data yaitu yang dikirim sekitar 100 dengan besar *size* data sekitar 83 *bytes* dan paket data yang diterima sekitar 75 dengan ukuran



Gambar 4.9 IP dan DNS dari Skyegrid

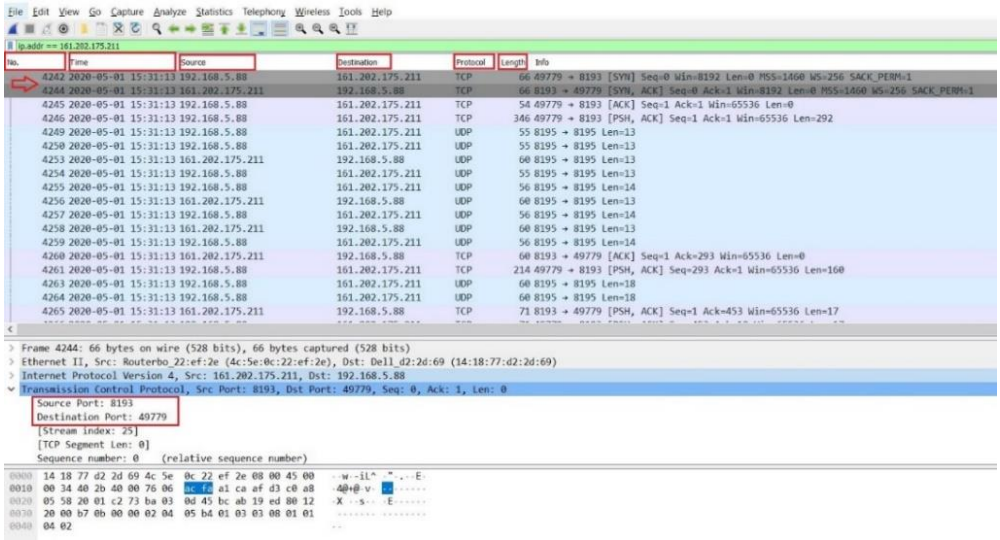
13 bytes. Jumlah paket data yang sangat sedikit, padahal *size* dari artefak *network capture* sangat besar.

Oleh karena itu eksplorasi dilanjutkan pada IP 161.202.175.211, karena MAC *address* identik dengan IP 13.67.63.90. Pada IP 161.202.175.211 jumlah paket data yang diterima dan dikirim sangat besar, 1167888 paket *sent*, dan 14135 paket *receive* data. Dengan jumlah data yang cukup besar akan tetapi tidak banyak informasi yang dapat di temukan pada *tools* NetworkMiner. Langkah selanjutnya beralih menggunakan *tool* Wireshark.



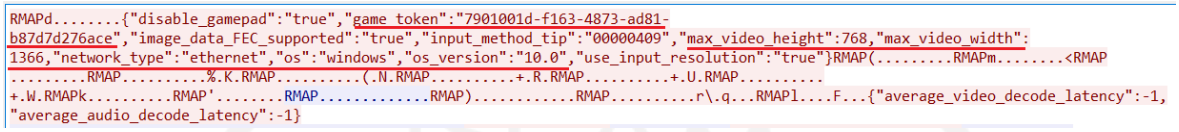
Gambar 4.10 IP Address Skyegrid

Menggunakan filter pada Wireshark guna mempersingkat proses penyelidikan dengan menggunakan *keyword* “ip.addr == 161.202.175.211”, hasilnya menunjukkan adanya paket data yang ditransmisikan dari ip 192.168.5.88 ke ip 161.202.175.211 dan sebaliknya dengan menggunakan protokol TCP dan UDP.



Gambar 4.11 Informasi Filter IP 161.202.175.211

Pada protokol TCP terlihat *source port*: 8193 dan *destination port*: 49779, untuk melihat isi dari informasi paket data yang ditransmisikan digunakan perintah Follow TCP Stream pada paket data nomor 4244. Hasil yang diperoleh berupa informasi dari konfigurasi *client-server* Skyegrid, selain itu informasi penting lainnya adalah *Game token* 7901001d-f163-4873-ad81-b87d7d276ace merupakan kunci untuk melakukan penyelidikan lebih lanjut pada artefak *volatile memory dump*.



Gambar 4.12 Informasi *file config*

2) Analisis barang bukti Memori *Dump* RAM

Eksplorasi pada artefak memori menggunakan *tools* FTK Imager dikombinasi dengan Winhex untuk memverifikasi temuan. Proses eksplorasi pada *image* memori *dump* menggunakan beberapa *keyword* untuk mempercepat proses penemuan potensi bukti digital. *Keyword* pertama yang digunakan adalah *game token: "*7901001d-f163-4873-ad81-b87d7d276ace" yang sebelumnya diperoleh dari artefak *network capture*.

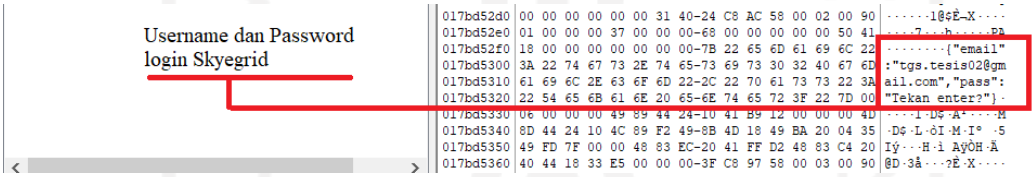
Gambar 4.13 *Search Keyword*

Proses pencarian menggunakan *keyword* tersebut menghasilkan beberapa temuan yang layak dijadikan sebagai informasi barang bukti seperti:

a. Informasi *timestamp* Skyegrid dijalankan
b. Informasi *manufacture*, model, dan CPU dari laptop DELL
c. Informasi *timestamp* game Dota 2 dijalankan
d. Informasi dari *game token*

Gambar 4.14 Hasil *search* dengan *game token*

Investigasi selanjutnya ditujukan untuk menemukan informasi kredensial seperti *username* dan *password login* dari Skyegrid. Untuk menemukan informasi tersebut, *keyword* yang digunakan berupa alamat e-*mail*: tgs.tesis02@gmail.com, sebagai proses pencarian informasi *username* dan *password* dari Skyegrid.



Gambar 4.15 Informasi *Username* dan *password* Skyegrid

Hasil pencarian secara spesifik menghasilkan temuan yang baik, pada temuan ini adanya alamat e-*mail* dan *password* yang digunakan untuk *login* ke Skyegrid. Proses selanjut melakukan analisis pada artefak harddisk yang telah di akuisisi dengan metode *copy bit-to-bit* data.

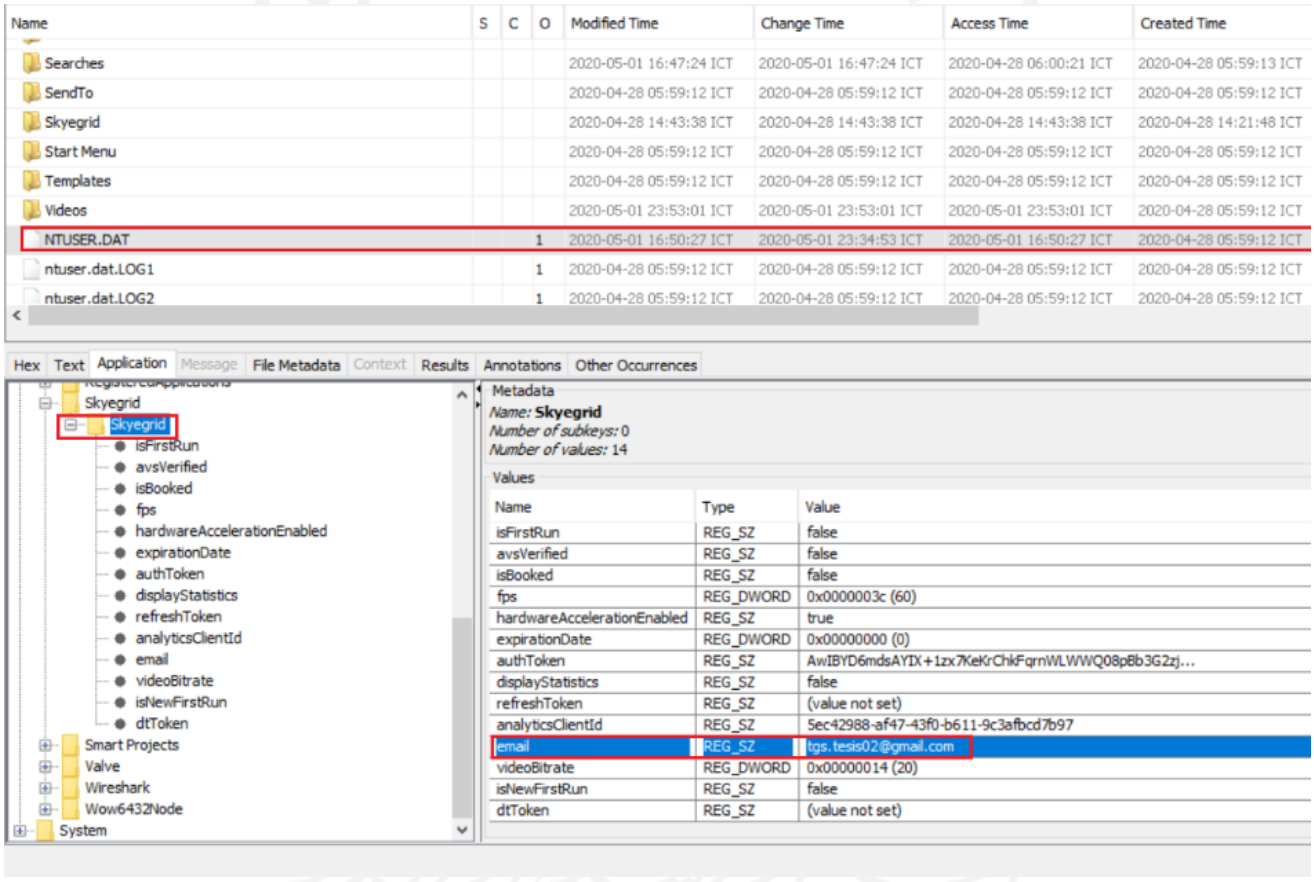
3) Analisis barang bukti image HDD

Jumlah ukuran *file* yang cukup besar, sehingga proses eksplorasi pada *image harddisk* dilakukan secara portabel dengan menggunakan *harddisk* eksternal yang dihubungkan *docking station*. *Imaging* disimpan berformat E01, kemudian karna alasan *size* yang cukup besar maka dilakukan klaster hingga 77 bagian sehingga menjadi penamaan Steam-chat-dota.001 - Steam-chat-dota.077. Pemeriksaan dan ekstraksi bukti digital

menggunakan *tools* Autopsy dan FTK Imager. Sesuai dengan tahap perencanaan di atas, maka pemaparan analisa *harddisk* dapat dipresentasikan sebagai berikut:

i. NTUSER.DAT

NTUSER.DAT merupakan fasilitas dari sistem operasi Windows yang memiliki peranan peting sebagai *database* yang berisi informasi terkait konfigurasi registri seperti *user* profil, aktivitas *user*, dan menyimpan konfigurasi *software* secara berkala di saat *software* dijalankan, pada studi kasus ini NTUSER.DAT tersimpan pada *directory* c:\users\DELL01\NTUSER.DAT. Pada eksplorasi NTUSER.DAT ditemukan informasi berupa konfigurasi e-*mail* "tgs.tesis02@gmail.com" sebagai *username* dari Skyegrid. Letak *File* konfigurasi berada pada *directory* NTUSER.DAT*Software**Skyegrid*.

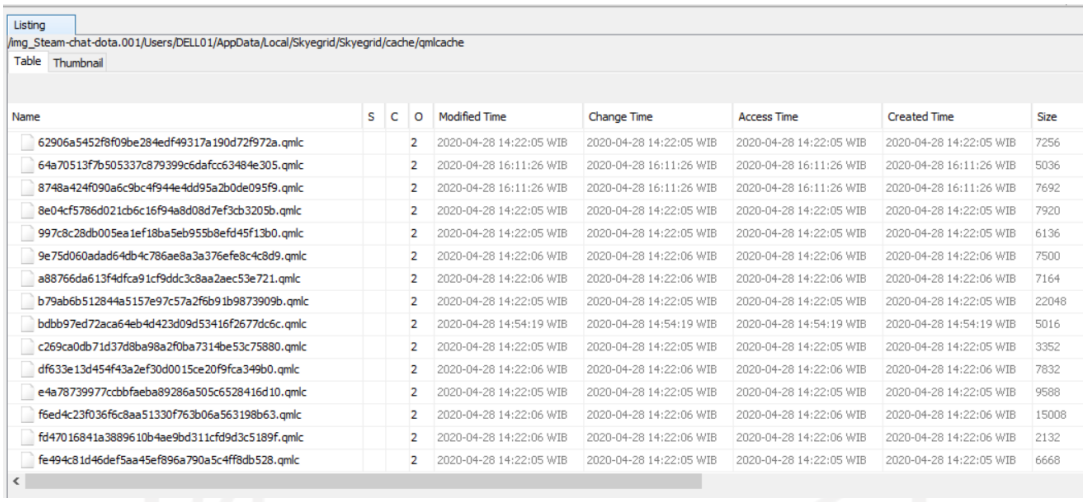


Gambar 4.16 NTUSER.DAT dan *registri* Skyegrid

Pada gambar 4.17 mendeskripsikan bahwa NTUSER.DAT telah terjadi modifikasi waktu, jika diamati perubahan waktu menjadi sesuai saat simulasi kejahatan pada Skygerid.

ii. AppData Skyegird

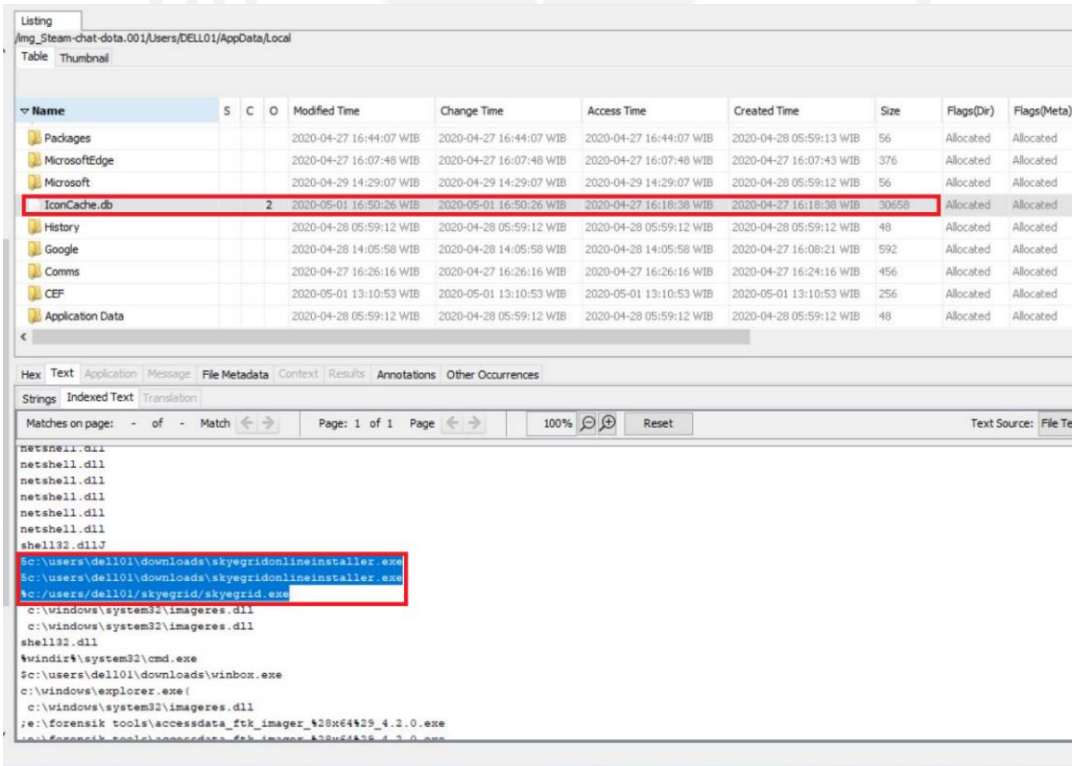
Folder *Temp/temporary* Skyegrid ditemukan terletak pada *directory c:\users\DELL01\AppData\Local\Skyegrid* didalam folder ini berisi *cache* dari *file* konfigurasi *qmlcache* Skyegrid saat dijalankan oleh *user*.



Gambar 4.17 Isi *temporary* Skyegrid

iii. IconCache.db

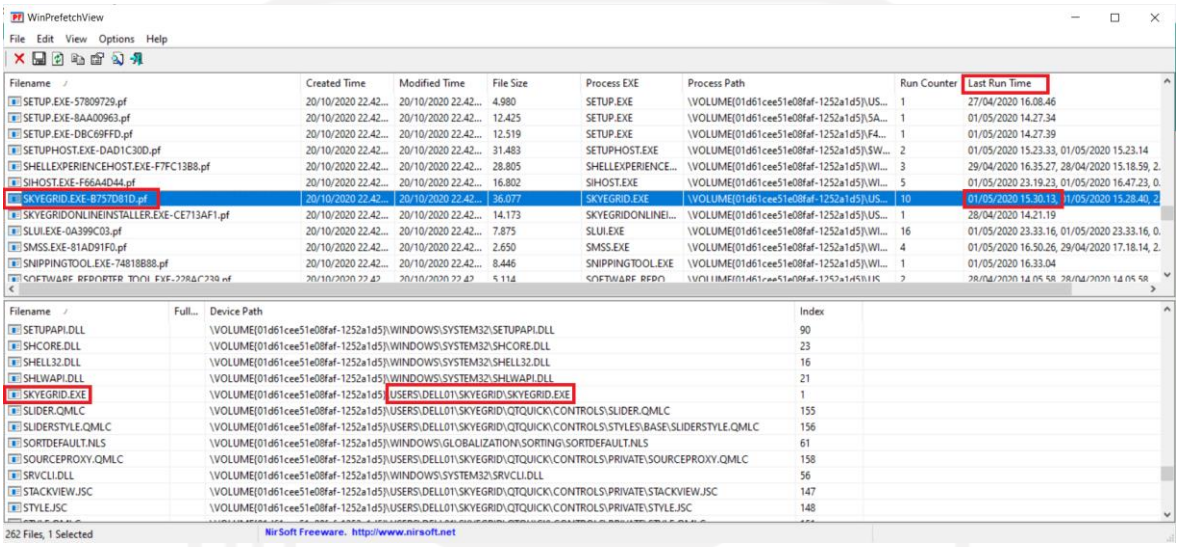
Pada IconCache.db informasi yang disimpan berupa informasi *file executable* yang pernah diakses/dijalankan pada sistem operasi Windows, setelah melakukan pengamatan lebih lanjut, ditemukan berupa *executable installer* dan skygerid menandakan Skyegrid pernah dijalankan. IconCeche.db tersimpan pada *directory* C:\Users\DELL01\AppData\Local\IconCache.db



Gambar 2.18 *File* IconCache.db

iv. Prefetch Windows

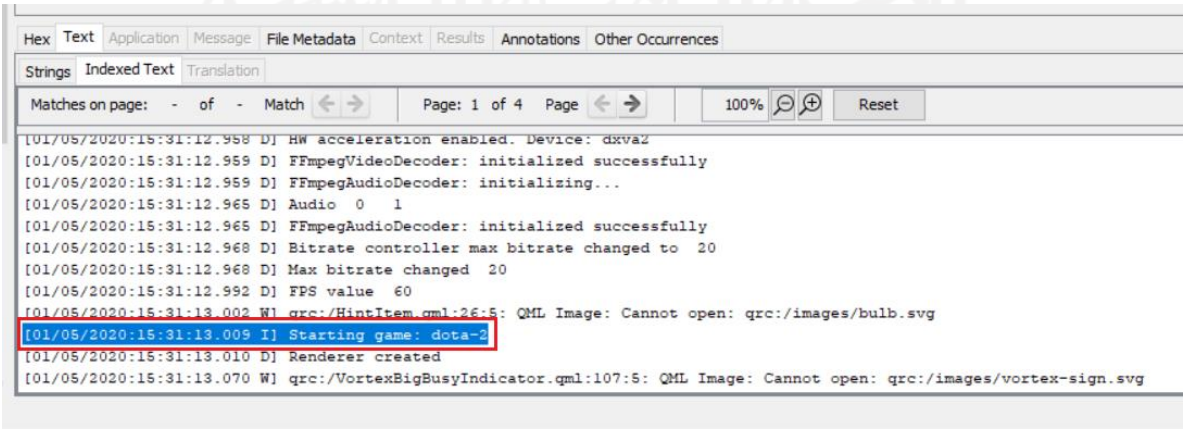
Untuk melakukan analisis pada folder Prefetch, sebelumnya diekstrak terlebih dahulu menggunakan *tool* Autopsy yang tersimpan di \Windows\Prefetch kemudian dilakukan eksplorasi menggunakan *tool* WinPrefetchView. Hasil temuan berupa informasi yang menunjukkan bahwa *Last Run Time* Skyegrid pada tanggal dan jam yang sama saat simulasi kasus dilakukan. Petunjuk lainnya adalah letak SKYEGRID.EXE yang merupakan *file executable* tersimpan pada *directory* \Users\DELL01\SKYEGRID\SKYEGRID.EXE.



Gambar 4.19 Skyegrid Prefetch

v. Log Skyegrid

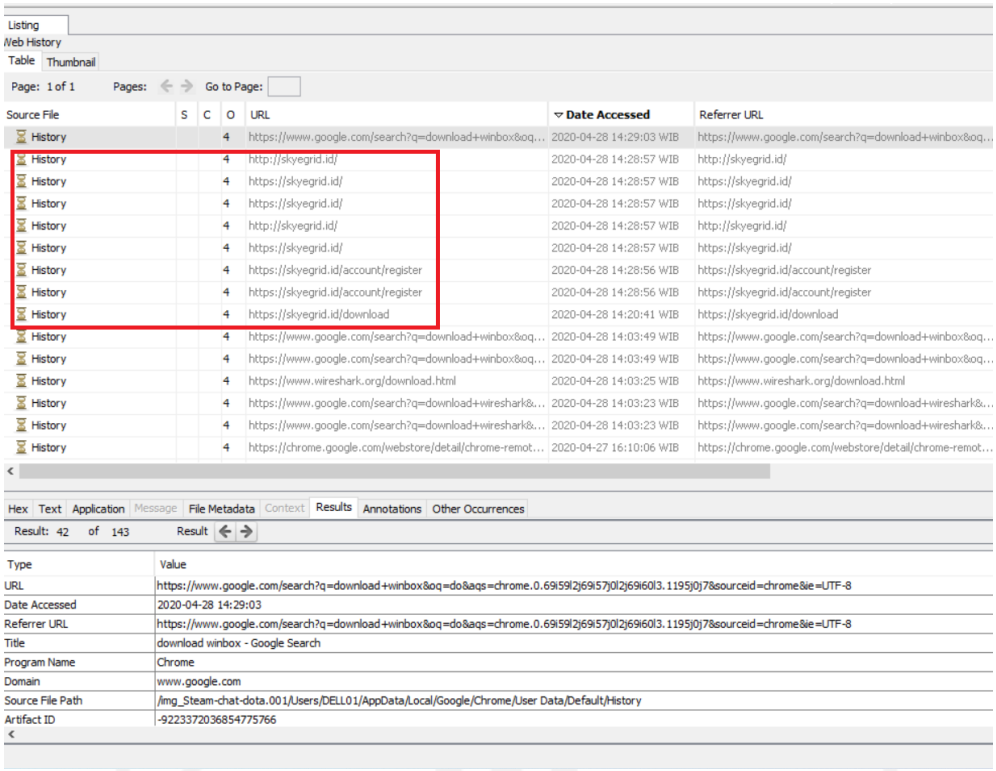
File SKYEGRID.EXE tersimpan pada *directory installer*, maka langkah selanjutnya melakukan eksplorasi pada *directory installer* Skyegrid dengan menggunakan *tool* Autopsy. Hasil temuan berupa *file* log.txt Skyegrid, yang di dalamnya terdapat informasi terkait Game yang dijalankan/mainkan yaitu game Dota 2, Selain itu pada log ini berisi informasi *timestamp* yang relevan keitka simulasi studi kasus dilakukan.



Gambar 4.20 Log Skyegrid

vi. *History* Web *Browsing*

Pencarian informasi selanjutnya pada *history* web *browsing* dengan menggunakan *tool* Autopsy. Hasil temuan yang diperoleh adanya *history* diaksesnya laman web, register dan melakukan *download* aplikasi Skyegrid. Tanggal akses dilakukan *browsing* dilakukan sebelum tindak simulasi dilakukan, hal ini dianggap sebagai persiapan sebelum melakukan penyalahgunaan pada platform Skyegrid.

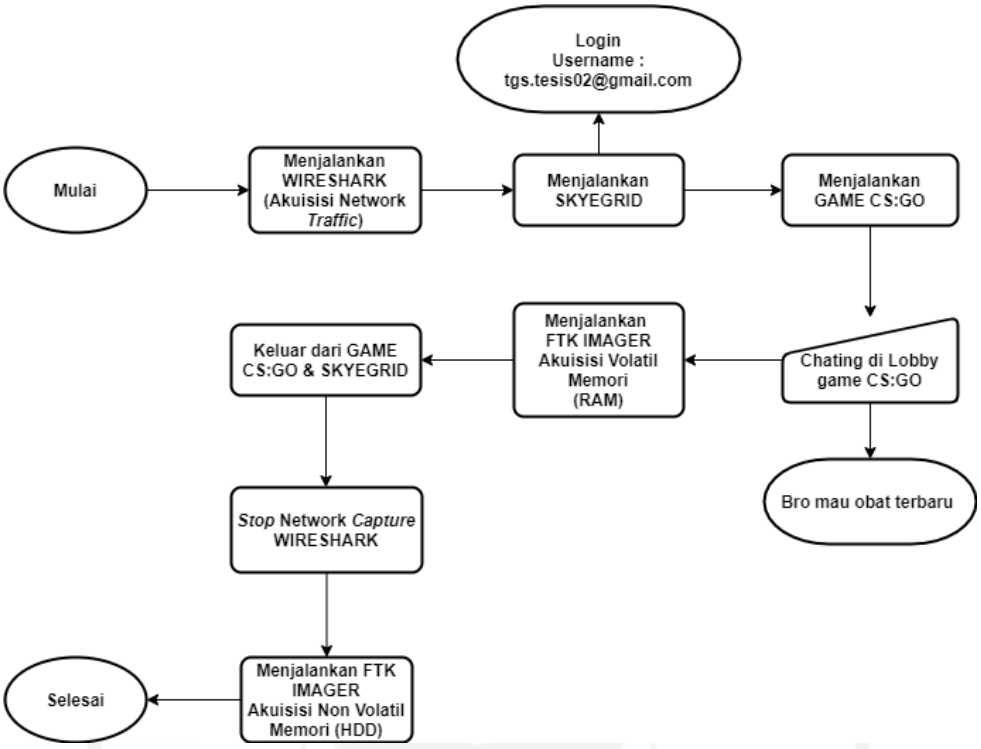


Gambar 4.21 History web browser

4.5.4 *Repeat Process* (Ulangi tahap)

Pada tahap ini, melakukan tindakan akuisisi dan analisis ulang, namun obyek game yang dijadikan studi kasus adalah CS:GO (*Counter - Strike*: Global Offensive). Semua proses akan disamakan, dimulai dari langkah-langkah simulasi game dan akuisisi, sehingga alur dari proses melakukan simulasi dan pengumpulan barang bukti digital dapat dipaparkan sebagai berikut.

Proses akuisisi dimulai dari artefak *network capture*, proses akuisisi menggunakan *tools* Wireshark. Kemudian dari artefak memori volatil, diakuisisi dengan menggunakan *tool* FTK Imager hasil *output* berupa *Memory dump,* dan selanjutnya barang bukti dari *harddisk* diakuisisi menggunakan *tool* FTK Imager dengan metode *Physical Acquisition* tipe *bit-stream disk-to-image file* dengan format *file* E01. Semua barang bukti dihasilkan dari laptop DELL, sebagai catatan laptop DELL terlebih dahulu di bersihkan dengan cara *install* ulang Windows dan partisi ulang *harddisk,* agar barang bukti tidak tumpang tindih.



Gambar 4.22 Alur Akuisisi barang bukti studi kasus game CS:GO

Sebelum melakukan evaluasi atau melakukan analisis terlebih dahulu dilakukan verifikasi keaslian dari barang bukti digital yang di gandakan, agar tidak ada perubahan pada barang bukti yang akan dianalisis. Berikut tabel hash MD5 yang didapat dari *tool* Winmd5free.

Tabel 4.6 Hasil verifikasi Hash MD5 dari Barang bukti game CS:GO

No.	Barang Bukti	Nilai Hash	Hasil dari	Keterangan
1	CS-GO-Network-Capture.pcap	3532948c0bb0456387347f5fd66aa894	*Capture traffic* jaringan	*Verified*
2	memdumo-cs-go.mem	623 5c49e33581a628a9c479934481272	*Memori dump*	*Verified*
3	Disk-Imaging-CS-GO.E01	a237d00ee9d4e9537104fd5e91d60cf4	*Imaging hard disk*	*Verified*

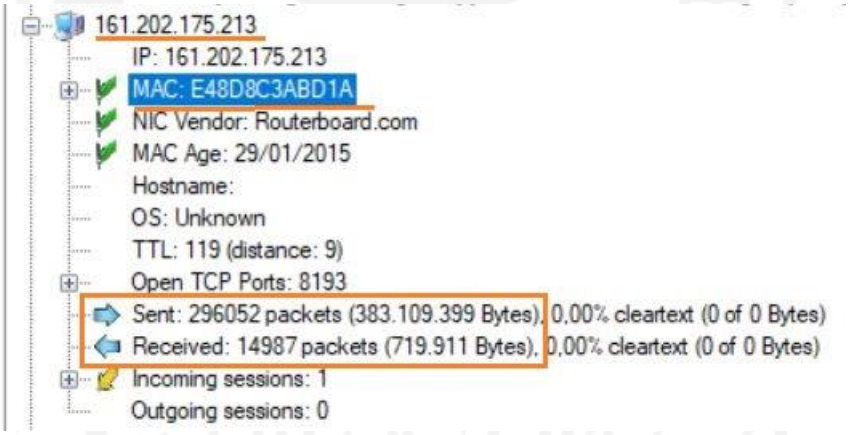
Verifikasi untuk menjaga keaslian telah dilakukan dan semua *image* yang digandakan memiliki integritas sama dengan yang asli. Selanjutnya adalah melakukan investigasi penelusuran barang bukti yang dipresentasikan sebagai berikut:

1. *Network Capture*

Pertama-tama Investigasi pada *image network capture* ini menggunakan *tools* Network Miner sebagai visualisasi IP dan DNS dari platform Skyegrid, hasil temuan dapat dilihat sebagai berikut.

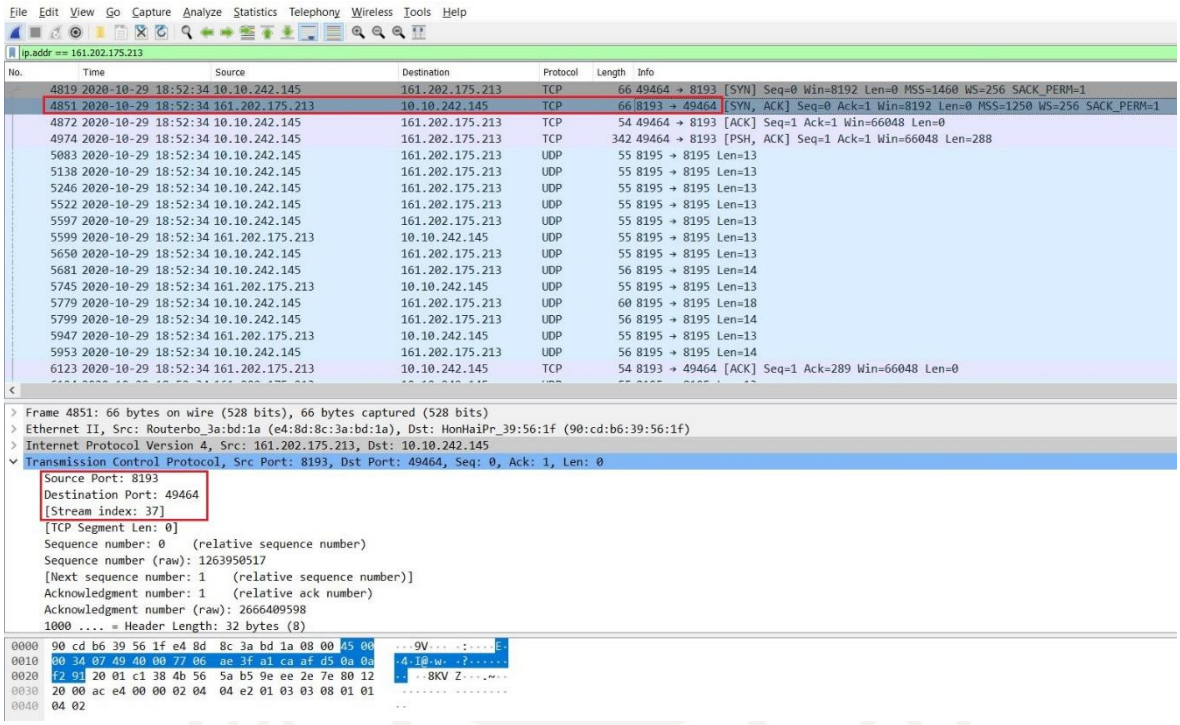
Gambar 4.23 IP dan DNS Skyegrid CS:GO

IP dan DNS dari api-skyegrid.remotcloud.com yang digunakan masih sama seperti temuan sebelumnya yaitu,13.67.63.90. Kemudian pada alamat *address* ini jumlah paket yang di kirim dan diterima juga masih relatif kecil yaitu sekitar 112 paket kirim sebesar 89 Bytes, dan 98 paket data yang di terima berukuran 14 Bytes, serta TCP dan port 443 juga sama sebagai protokol yang digunakan. Proses selanjutnya melakukan investigasi terhadap IP *address* yang memiliki jumlah paket data *sent* dan *receive* yang besar yaitu pada IP 161.202.175.213 dengan jumlah *sent* paket data 296052 dan *receive* paket data 14987. Hal ini merupakan jumlah paket data *sent* dan *receive* paling banyak pada artefak *network traffic*.



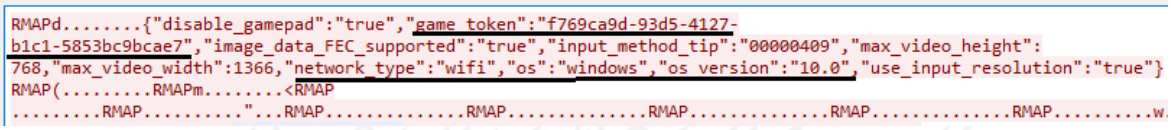
Gambar 4.24 Informasi IP 161.202.175.213

Selanjutnya untuk melihat informasi data apa saja yang ditransmisikan melalui IP 161.202.175.213, investigasi menggunakan *tools* Wireshark. Kemudian menggunakan fitur filter dengan *keyword* ip.addr == 161.202.175.213.



Gambar 4.25 Filter ip.addr == 161.202.175.213

Proses ini menghasilkan informasi relatif sama dari hasil sebelumnya, sekilas dapat diperhatikan masih adanya komunikasi menggunakan protokol TCP dan UDP. Pada paket nomor 4851 merupakan komunikasi server ke *client* menggunakan protokol TCP dengan *source port* 8193 masih sama dengan temuan sebelumnya, dan *destination port* 49464. Pada paket ini dilakukan pemeriksaan isi informasi yang ditransmisikan dengan cara *follow TCP stream*.



Gambar 4.26 Informasi Konfigurasi Skyegrid pada CS:GO

Hasil dari *keyword* tersebut ditemukan *Game token*: f769ca9d-93d5-4127-b1c1-5853bc9bcae7 yang merupakan informasi dari adanya proses koneksi *user* dengan Skyegrid. *Game token* ini akan digunakan sebagai *keyword* pada investigasi selanjutnya.

2. *Volatile Memory* (RAM)

Proses investigasi memori *dump* menggunakan *tool* FTK Imager dan dikombinasi Winhex. *Keyword* yang digunakan pertama adalah *game token*: f769ca9d-93d5-4127-b1c1-5853bc9bcae7 untuk mempercepat proses penyelidikan. Dari *keyword game token* tersebut menghasilkan beberapa temuan yang sangat berpotensi sebagai barang bukti digital yaitu:

a. informasi *timestamp* saat Skyegrid dijalankan

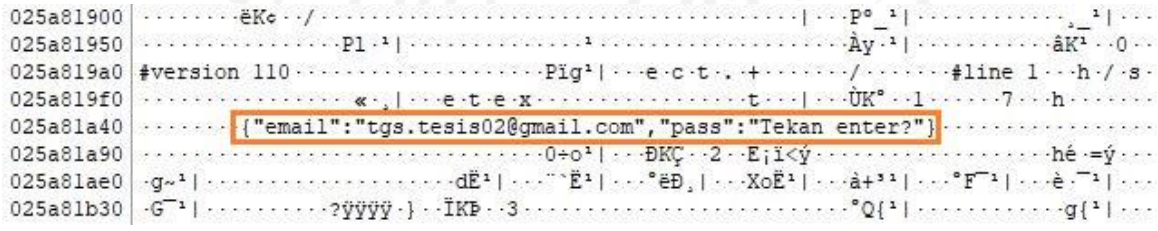
b. Informasi *manufacture*, model, dan CPU dari laptop DELL

c. Informasi *timestamp* game CS:GO dijalankan

d. Informasi *game token*: “f769ca9d-93d5-4127-b1c1-5853bc9bcae7”

Gambar 4.27 Potensi bukti digital pada memory dump

Masih melanjutkan investigasi pada artefak memori *dump*, diproses ini akan digunakan kata kunci akun dari Skyegrid “tgs.tesis02@gmail.com”. Pada FTK Imager ditemukan hasil berupa e-*mail*: tgs.tesis02@gmail.com dan pass: Tekan enter? Sebagaimana terlihat pada gambar 4.28.



Gambar 4.28 E-*mail* dan pass akun Skyegrid

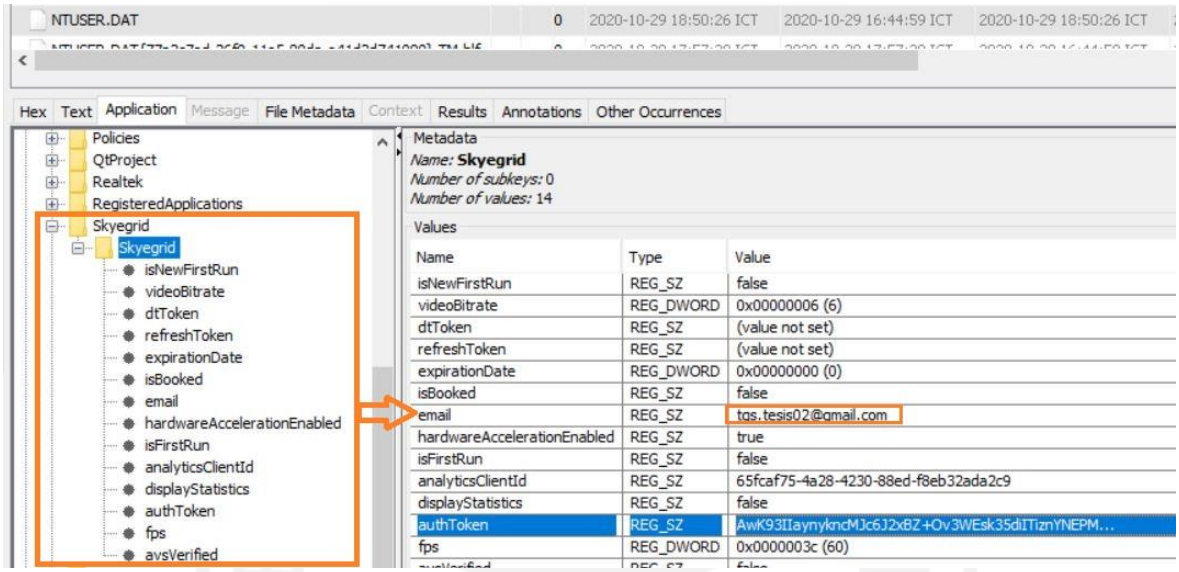
3. Analisis Non *Volatile Memory* (HDD)

Proses analisis pada *file image* HDD dilakukan sesuai dengan langkah-langkah analisis *file image* HDD sebelumnya. *Tools* yang digunakan untuk proses penyelidikan

menggunakan Autopsy dan FTK Imager. Berikut pemaparan analisis temuan dari barang bukti *file image* HDD:

a. NTUSER.DAT

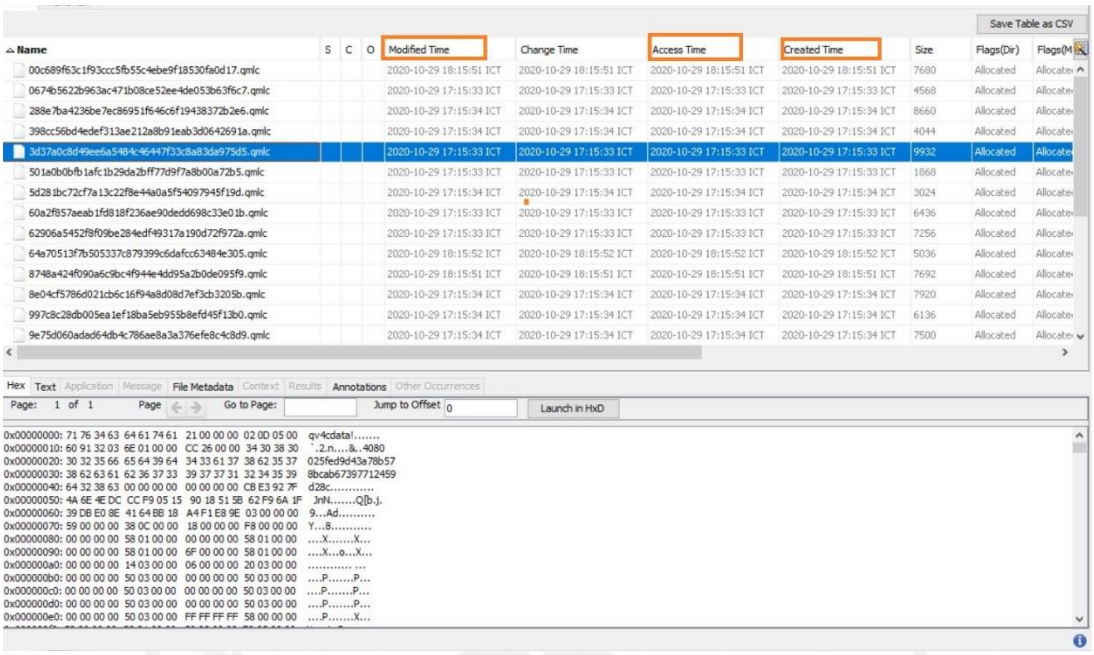
Letak NTUSER.DAT tersimpan masih pada *directory* yang sama yaitu pada *directory* c:\users\DELL01\NTUSER.DAT. Informasi yang ditemukan adalah informasi e-*mail* tgs.tesis02@gmail.com yang merupakan *username* dari Skyegrid yang digunakan oleh *user*. Informasi ini tersimpan pada *directory* NTUSER.DATA\Software\Skyegrid.



Gambar 4.29 Informasi e-mail dari NTUSER.DAT

b. AppData Skyegrid

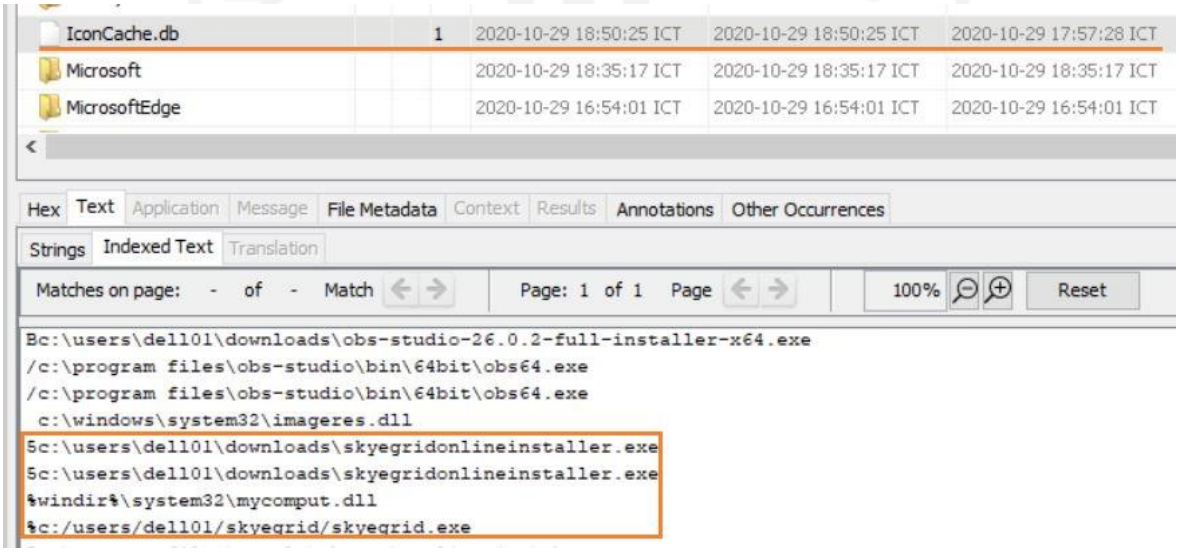
Pada *directory* c:\users\DELL01\AppData\Local\Skyegrid\ informasi yang tersimpan berupa *file* konfigurasi dari *qlmcache*. Informasi yang didapat masih sesuai dengan temuan sebelumnya dengan game Dota 2. *Timestamp modified*, *access*, dan *created* semua identik sama dengan waktu simulasi kejahatan pada platform Skyegrid.



Gambar 4.30 Qlmcache AppData Skyegrid

c. IconCache.db

Informasi IconCache.db menyimpan beberapa *executable* Windows yang pernah dijalankan *user* maupun berjalan secara otomatis oleh sistem. Letak IconCache.db tersimpan pada directory C:\Users\DELL01\AppData\Local\IconCache.db. Pada penyelidikan ini ditemukan *executable* Skyegrid, dengan demikian menandakan aplikasi Skyegrid pernah di jalankan oleh *user*. *Timestamp modified*, *access*, dan *created* semua identik sama dengan waktu simulasi kejahatan.

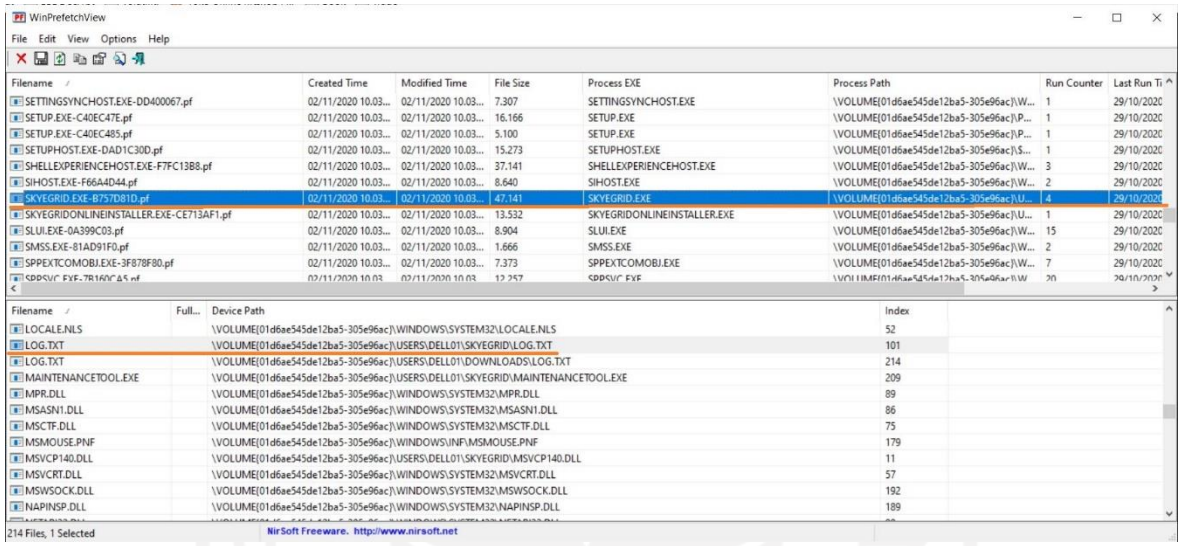


Gambar 4.31 Informasi IconCache.db

d. *Prefetch* Windows

Informasi *prefetch* Windows terletak pada *directory* \Windows\Prefetch, untuk analisis *prefetch* Windows perlu dilakukan ekstrak terlebih dahulu menggunakan *tool*

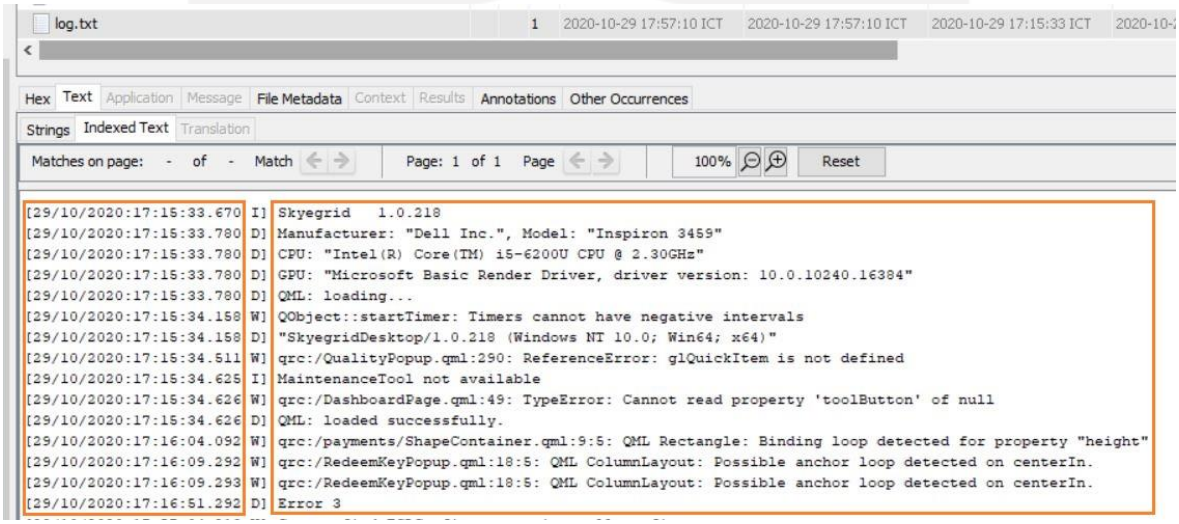
Autopsy, kemudian untuk memvisualisasikan *task* program yang pernah berjalan dapat menggunakan *tool* WinPrefetchView. Hasil penyelidikan menemukan informasi tentang adanya program Skyegrid yang dijalankan pada waktu yang sama dengan simulasi kejahatan. Selain itu ditemukan informasi terkait *file* LOG dari program Skyegrid yang tersimpan pada *directory* \Users\DELL01\SKYEGRID\LOG.TXT, maka proses penyelidikan selanjutnya mengarah pada *file* LOG.TXT.



Gambar 4.32 *Prefetch* Windows

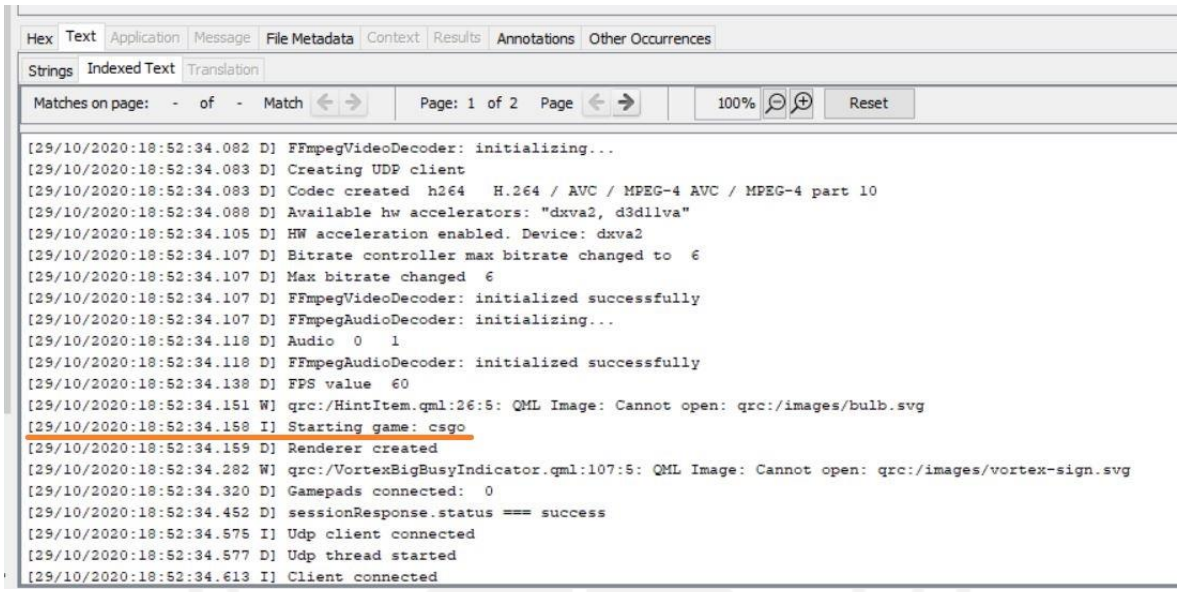
e. *Log file* Skyegrid

Sebagaimana penjelasan sebelumnya *file* log Skyegrid tersimpan pada *directory* \Users\DELL01\SKYEGRID\LOG.TXT, dengan menggunakan *tool* Autopsy diperoleh informasi yang sangat akurat dan relevan. *File* log.txt menyimpan informasi *history* dari setiap proses yang berjalan pada program Skyegrid, serta dilengkapi dengan *timestamp* yang akurat. Namun informasi terkait pesan *chat* tidak terekam pada *file* log.txt.



Gambar 4.33 *File* Log.txt Skyegrid

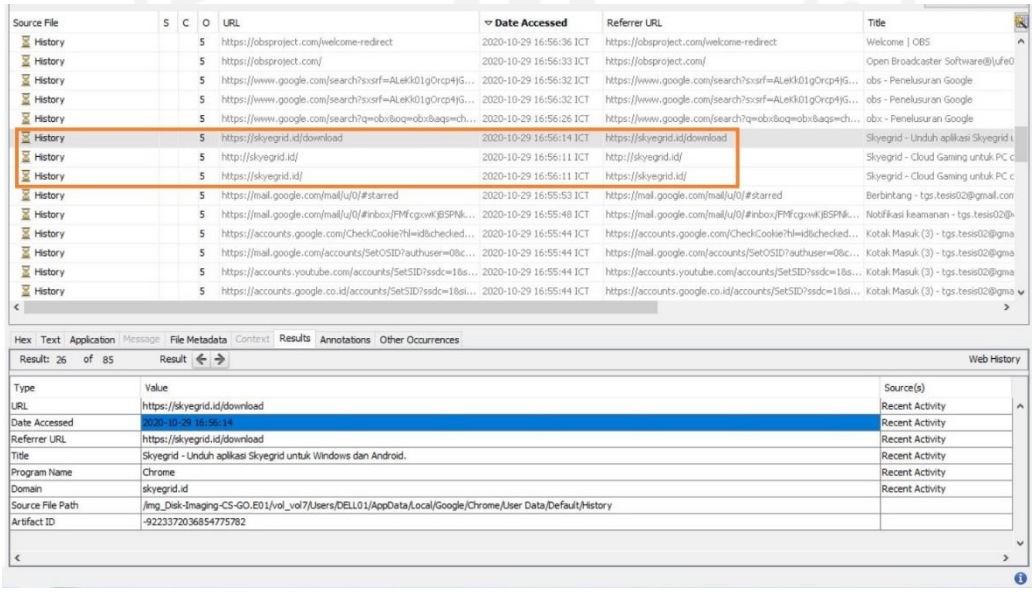
Pada *file* log.txt ditemukan game CS:GO dan catatan *timestamp* saat dijalankan oleh *user* pada platform Skyegrid, terlihat oleh gambar berikut.



Gambar 4.34 *File* log.txt, game CS:GO

f. *History* Web *Browsing*

Informasi histori web *browsing* dapat ditemukan menggunakan *tool* Autopsy. Informasi yang diperoleh yaitu adanya catatan histori *user* melakukan akses ke laman web Skyegrid dan melakukan *download* aplikasi desktop Skyegrid sebagaimana terlihat pada gambar berikut.

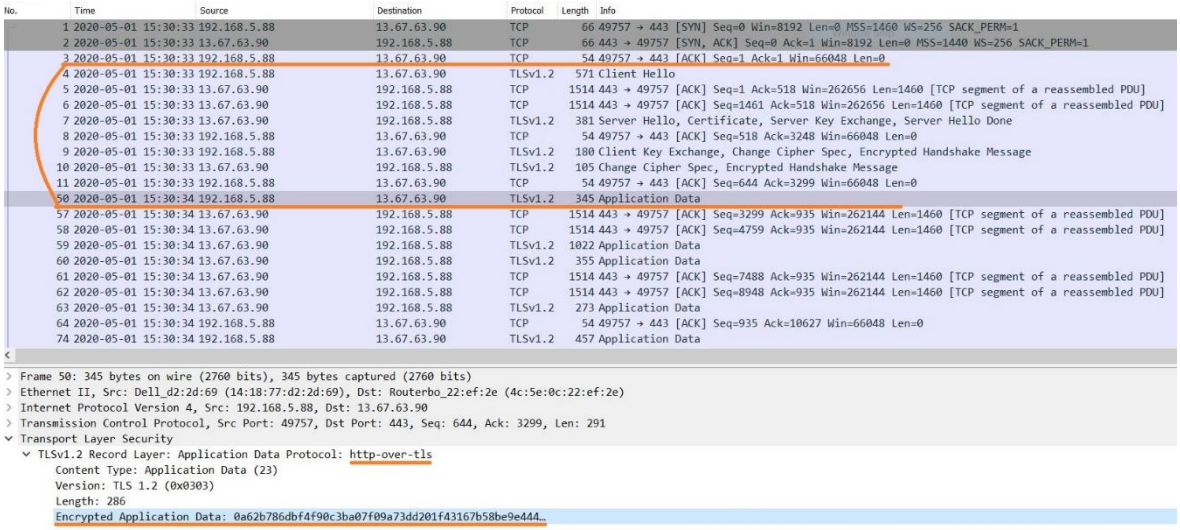


Gambar 4.35 Histori akses web Skyegrid

4.5.5 *Analyse* (Analisis)

Dari serangkaian tindakan berdasarkan runtutan tahapan yang sudah dilakukan maka dapat disimpulkan secara garis besar artefak digital pada penyalahgunaan layanan *cloud gaming*

Skyegrid tidak dapat diperoleh seutuhnya, seperti artefak komunikasi *chating*, *user* ID, *user* ID teman, dan Akun Steam. Penyebabnya seperti pada barang bukti *network capture*, paket data yang ditransmisikan oleh *user* ke server Skyegrid maupun sebaliknya pada paket data yang mengandung informasi penting ditransmisikan melalui protokol TLSv1.2, sehingga untuk melihat informasi paket data (*decrypt*) sangat sulit karena diperlukan *key exchange* dari komputer *user* dan server Skyegrid, sebagaimana terlihat pada gambar berikut:



Gambar 4.36 Proses *handshake* TLSv1.2 pada artefak *network traffic*

Dengan demikian informasi yang dapat dipaparkan dari hasil analisis forensik dari barang bukti *network traffic* pada tahap evaluasi dan *repeat* dapat dijelaskan melalui tabel berikut:

Tabel 4.7 Artefak digital yang ditemukan pada *network traffic*

Bukti digital: Skyegrid dan Game Dota 2						
Timestamp	**Source Address**	**Dest.Address**	**Protokol**	**Source Port**	**Dest. Port**	**Informasi artefak digital**
01/05/2020 - 15:31:13	161.202.175.211	192.168.5.88	TCP	8193	49779	*Game token* 7901001d-f163-4873-ad81-b87d7d276ace
Bukti digital: Skyegrid dan Game CS:GO						
29/10/2020 - 18:52:34	161.202.175.213	10.10.242.145	TCP	8193	49464	*Game token* f769ca9d-93d5-4127-b1c1-5853bc9bcae7

Berdasarkan dari tabel 4.7 korelasi kedua artefak *network traffic* dari tahap evaluasi dan tahap *repeat* yang dapat ditentukan sebagai potensi bukti digital yaitu pada *source*

address, *source port* dan *token game*. Pada studi kasus ini hasil temuan dari artefak *network traffic* relatif sama. Dengan demikian metode *network* forensik yang diaplikasikan pada tahapan *fremework* FRED dapat dikategorikan berhasil.

Selanjutnya dengan ditemukan *token game*, maka penelusuran artefak digital pada barang bukti *memory dump* dan *image harddisk* menjadi lebih mudah dan cepat, pasalnya *token game* dapat dijadikan kunci penelusuran atau *keyword* pencarian pada menu *search* pada *tools* FTK Imager dan WinHex. Hasil pencarian kursor langsung mengarah pada *offset token game* dilanjut dengan informasi lainnya yang berpotensi sebagai bukti digital. Pada artefak *image harddisk*, *token game* tersimpan di dalam *file log* aplikasi Skyegrid. Dengan demikian temuan pada artefak *memory dump* dan *image* harddisk dapat ditampilkan menjadi tabel berikut:

Tabel 4.8 Artefak digital yang ditemukan pada RAM dan HDD

Bukti digital: Skyegrid dan Game Dota 2		
Potensi Artefak	Volatil Memori (RAM)	Non Volatil Memori (HDD)
Username	tgs.tesis02@gmail.com	tgs.tesis02@gmail.com
Password	Tekanenter?	N/A*
Pesan *Chating*	N/A*	N/A*
Game token	7901001d-f163-4873-ad81-b87d7d276ace	7901001d-f163-4873-ad81-b87d7d276ace
Timestamp mulai akses Skyegrid	01/05/2020:15:30:33	01/05/2020:15:30:33
Timestamp mulai akses game Dota 2	01/05/2020:15:31:13	01/05/2020:15:31:13
Bukti digital: Skyegrid dan Game CS:GO		
Username	tgs.tesis02@gmail.com	tgs.tesis02@gmail.com
Password	Tekanenter?	N/A*
Pesan *Chating*	N/A*	N/A*
Game token	f769ca9d-93d5-4127-b1c1-5853bc9bcae7	f769ca9d-93d5-4127-b1c1-5853bc9bcae7
Timestamp mulai akses Skyegrid	01/05/2020:15:30:33	01/05/2020:15:30:33
Timestamp mulai akses game CS:GO	01/05/2020:15:31:13	01/05/2020:15:31:13

Keterangan : * bukti digital tidak dapat ditemukan.

Dari pemaparan pada tabel 4.7 dan 4.8 dapat diketahui bahwa informasi yang berpotensi digunakan sebagai bukti digital banyak ditemukan pada artefak *memory volatile*, seperti akun *username* dan *password* Skyegrid. Dengan temuan tersebut penyidik dapat menelusuri lebih lanjut ke dalam aplikasi Skyegrid. Akan tetapi untuk penelusuran lebih lanjut ke dalam *game* untuk melihat *history* penggunaan, penyidik membutuhkan *username*

dan *password* dari Steam. Namun pada studi kasus ini, akun *username* dan *password* tidak dapat ditemukan dikarenakan jejak digital tersimpan disisi server Skyegrid. Hal ini juga yang membuat informasi komunikasi *chating* tidak dapat ditemukan.

4.5.6 *Comfirm* (Konfirmasi)

Dengan melakukan serangkaian simulasi dan analisis forensik terhadap penyalahgunaan platform Skyegrid sebagai salah satu layanan *cloud gaming* yang berkembang di tanah air. Dalam proses pembuktian studi kasus ini menggunakan *framework* FRED dengan simulasi menggunakan game Dota 2 pada tahap evaluasi, dan CS:GO pada tahap *repeat*. Dengan karakteristik *cloud computing* pada Skyegrid, maka dalam perencanaan identifikasi, pengumpulan dan analisis artefak digital mengikuti metode dari terapan ilmu *network* forensik dan *computer* forensik. Dengan penerapan *framework*, metode dan *tools* forensik tersebut menghasilkan karakteristik bukti digital yang dipaparkan pada Tabel 4.9 dan 4.10:

4.6 Analisa Karakteristik Hasil

Melihat dari informasi yang telah dikumpulkan melalui proses analisis spasial kepada tiga barang bukti digital, dapat dilihat detail perbandingan informasi yang didapat dari barang bukti *network capture*, memori RAM, dan HDD pada Tabel 4.9. Karakteristik bukti digital pada *network capture* sangat sedikit yang dapat diidentifikasi karena protokol keamanan TLS, sementara itu ukuran *file* hasil *capture* sangat besar, apabila dapat dilakukan deskripsi kode-kode yang tersimpan maka banyak informasi yang dapat dijabarkan. Namun itu sangat sulit dan membutuhkan jumlah sumber daya dan waktu yang cukup banyak (Faisal & Zulkernine, 2020). Menemukan potongan informasi dalam bentuk kode digital yang ter-*generete* menjadi sebuah *token* game dapat membantu pencarian pada barang bukti lainnya.

Karakteristik bukti digital pada data volatil RAM berpotensi sebagai bukti digital yang dapat digunakan, informasi *username* dan *password login* pada Skyegrid dapat ditemukan di data volatil RAM, kemudian informasi game online yang dioperasikan disertai adanya *timestamp*. Sementara itu karakteristik pada barang bukti *imaging* HDD berpotensi juga, namun hanya sebatas pada temuan pada *file* log.txt dari aplikasi Skyegrid. Selebihnya informasi yang ditemukan hanya dapat menggambarkan adanya aplikasi Skyegrid terpasang pada sistem. Pada penelitian ini karakteristik bukti digital yang menggambarkan pelaku dari *game online* seperti *id user*, *nickname*, *id user* dan *nickname* teman yang diundang, serta informasi pesan tidak dapat ditemukan. Oleh sebab itu hasil temuan bukti digital pada studi kasus ini hanya dapat dijadikan pendukung untuk memberi gambaran adanya aktivitas penggunaan aplikasi Skyegrid dan game online.

Tabel 4.9 Detail karakteristik bukti digital dari tahap Evaluasi

No.	Informasi Bukti Digital	Jenis Bukti Digital		
		Network *Traffic*	*Voletile Memory* (RAM DUMP)	Non *Voletile Memory Image* harddsik
1	Metode Akuisisi	Live	Live	Static
2	Jenis *image*	Logical	Logical	Logical
3	Format *image*	.pcap	.mem	.E01
4	*Tool* Akuisisi	Wireshark	FTK Imager	FTK Imager
5	*Tool* Analisis	Network Miner dan Wireshark	FTK Imager dan WinHex	Autopsy, FTK Imager, dan WinPrefetchView
6	Ukuran Artefak	1,54 GB	5,49 GB	111,8 GB
7	Jenis temuan penting	*Game token* dan informasi perangkat yang digunakan saat menjalankan aplikasi Skyegrid	1. *Game token* dan informasi perangkat yang digunakan saat menjalankan aplikasi Skyegrid 2. *Usename* dan *password* akun Skyegrid 3. Game Dota 2 nama dari game yang digunakan 4. *Timestamp* menjalankan Skyegrid [01/05/2020:15:30:33]	1. *File* Log.txt aplikasi Skyegrid 2. *File* IconCache.db informasi 3. Folder *qmlcache* berisi informasi konfigurasi *session* Skyegrid 4. NTUSER.DAT 5. Windows *Perfecth* 6. Web *browsing* histori

No.	Informasi Bukti Digital	Jenis Bukti Digital		
		Network *Traffic*	*Voletile Memory* (RAM DUMP)	Non *Voletile Memory Image* harddsik
8	Lokasi file temuan penting	Pada tcp.stream eq 25 dengan *source* IP *address* 161.202.172.211	1. Pada *tools* FKT Imager dan WinHex Informasi di temukan pada *offset 0134F38B0* 2. Pada tools FKT Imager dan WinHex Informasi di temukan pada offset 07b51cee0 3. Pada tools FKT Imager dan WinHex Informasi di temukan pada offset 0134f36d0 4. Pada tools FKT Imager dan WinHex Informasi di temukan pada offset 0134f2ff0	1. log.txt (c:\\Users\DELL01\SKYEGRID\LOG.TXT) 2. IconCache.db (C:\users\DELL01\AppData\Local\Skyegrid\ ) 3. qmlcache (c:\users\DELL01\AppData\Local\Skyegrid\cache\qmlcache) 4. NTUSER.DAT (c:\users\DELL01\NTUSER.DAT\Software\Skyegrid) 5. Windows Prefecth (c:\Windows\Prefetch) 6. Web Browsing Histori (C:\users\DELL01\AppData\Local\Google\Chrome\User Data\Default\History)

Tabel 4.10 Detail karakteristik hasil temuan dari tahap ulangi/*Repeat*

No.	Informasi Bukti Digital	Jenis Bukti Digital		
		Network Traffic	*Voletile Memory* (RAM DUMP)	Non *Voletile Memory Image* harddsik
1	Metode Akuisisi	Live	Live	Static
2	Jenis *image*	Logical	Logical	Logical
3	Format *image*	.pcap	.mem	.E01
4	*Tools* Akuisisi	Wireshark	FTK Imager	FTK Imager
5	*Tools* Analisis	Network Miner dan Wireshark	FTK Imager dan WinHex	Autopsy, FTK Imager, dan WinPrefetchView
6	Ukuran Artefak	383 MB	5,49 GB	111,8 GB

No.	Informasi Bukti Digital	Jenis Bukti Digital		
		Network Traffic	*Voletile Memory* (RAM DUMP)	Non *Voletile Memory Image* harddsik
7	Jenis temuan penting	*Game token* dan informasi device yang digunakan saat menjalankan aplikasi Skyegrid	1. Game token dan informasi device yang digunakan saat menjalankan aplikasi Skyegrid 2. Usename dan password akun Skyegrid 3. Game CS:GO nama dari game yang digunakan 4. Timestamp menjalankan Skyegrid [29/10/2020:18:52:04]	1. file Log.txt aplikasi Skyegrid 2. File IconCache.db informasi 3. Folder *qmlcache* berisi informasi konfigurasi *session* Skyegrid 4. NTUSER.DAT 5. Windows Perfecth 6. Web browsing histori
8	Lokasi file temuan penting	Pada tcp.stream eq 37 dengan source IP address 161.202.175.213	1. Pada *tools* FKT Imager dan WinHex Informasi di temukan pada *offset 01f7258c0* 2. Pada tools FKT Imager dan WinHex Informasi di temukan pada offset 025a81a40 3. Pada tools FKT Imager dan WinHex Informasi di temukan pada offset 01f7256e0 4. Pada tools FKT Imager dan WinHex Informasi di temukan pada offset 01f725000	1. log.txt (c:\Users\DELL01\SKYEGRID\LOG.TXT) 2. IconCache.db (C:\Users\DELL01\AppData\Local\Skyegrid\ ) 3. qmlcache (c:\Users\DELL01\AppData\Local\Skyegrid\cache\qmlcache) 4. NTUSER.DAT (c:\Users\DELL01\NTUSER.DAT\Software\Skyegrid) 5. Windows Prefecth (c:\Windows\Prefetch) 6. Web Browsing Histori (C:\Users\DELL01\AppData\Local\Google\Chrome\User Data\Default\History)

Berdasarkan hasil pemaparan Tabel 4.9 dan 4.10 dapat diamati bahwa potensi bukti digital yang didapatkan sangat beragam dan sudah dapat digunakan dalam pembuktian sesuai fakta yang ada, namun pembuktian tersebut masih kurang jelas dalam menggambarkan identitas *client* secara eksplisit meskipun telah ditemukan *username* dan *password* untuk *login* Skyegrid. Hasil temuan bukti digital pada penelitian ini dengan hasil temuan dari literatur (Tabuyo-Benito et al., 2019), dan (Taylor et al., 2019) sudah identik sama, namun karena investigasi bukti digital hanya pada perangkat *client* sehingga ada beberapa potensi bukti digital lain yang tidak dapat ditemukan sebagaimana yang telah dipaparkan pada literatur yang dirujuk. Berikut pemaparan potensi bukti digital yang tidak dapat ditemukan karena artefak tersimpan pada server Skyegrid:

Tabel 4.11 Bukti digital pada *client* dan server Skyegrid

No	Bukti digital pada c*lient* (Ditemukan)	Bukti digital pada server Skyrgid (Tidak ditemukan)
1	1. Game token dan informasi perangkat yang digunakan saat menjalankan aplikasi Skyegrid 2. *Usename* dan *password* akun Skyegrid 3. Game Dota 2 nama dari game yang digunakan 4. *Timestamp* menjalankan Skyegrid [01/05/2020:15:30:33] 5. *File* Log.txt aplikasi Skyegrid 6. *File* IconCache.db informasi 7. Folder *qmlcache* berisi informasi konfigurasi *session* Skyegrid 8. NTUSER.DAT 9. Windows *Perfecth* 10. Web *browsing* histori	1. *Username* dan *password* Steam 2. Id_game (*Player*) 3. *Nick Name* game (*Player*) 4. Id_game (*Player* teman) 5. *Nick Name* game (*Player* teman) 6. Pesan *chatting* antar *player*

Karakteristik bukti digital yang ditemukan meskipun tidak dapat menunjukkan secara gamblang siapa pelaku dan bukti percakapan *chating* yang berindikasi penjualan narkoba. Namun dengan adanya temuan log.txt dari aplikasi Skyegrid dan dilengkapi *timestamp* dapat menunjukkan adanya aktivitas menjalankan aplikasi Skyegrid, game Dota 2, dan CS:GO. Kemudian temuan *timestamp* saat dikorelasikan dengan ketiga artefak hasilnya identik sama dengan waktu simulasi penyalahgunaan game. Dengan demikian penggunaan *framework* FRED pada penelitian ini berhasil menemukan potensi dan karakteristik bukti elektronik yang tersimpan pada laptop DELL. Dengan catatan minus informasi *user* yang detail seperti User ID game, *Nickname Game*, dan pesan *chat* percakapan tidak dapat ditemukan baik pada *image* bukti digital *network traffic*, *volatile memory* (RAM), dan *non volatile memory* (HDD) karena bukti-bukti tersebut tersimpan atau tertinggal pada server Skyegrid.

4.7 Analisis Penerapan FRED

Setelah seluruh rangkai proses telah tercapai maka dapat ditarik kesimpulan bahwa, secara umum penerapan *framework* FRED pada penelitian ini terhadap keenam tahapan dapat dijelaskan sebagai berikut:

1. Tahap *plan*/perencanaan: peneliti dapat menentukan metode forensik apa saja yang akan digunakan sesuai karakteristik dari kasus bukti elektronik yang dihadapi atau peneliti hanya merencanakan pada lokasi tersimpan bukti digital dan menentukan *tools* yang akan digunakan. Pada penelitian ini peneliti menggunakan metode keilmuan *network* forensik dan *computer* forensik untuk mengidentifikasi potensi bukti digital yang tersimpan pada laptop pelaku penyalahgunaan game online menggunakan platform *cloud gaming* Skyegrid, *tools* forensik yang digunakan berupa Wireshark dan NetworkMiner untuk pengumpulan dan penyelidikan pada artefak *network traffic, tools* FTK Imager dan Winhex pada artefak *memory dump,* dan *tools* FTK Imager, Autopsy, dan Winprefetchview pada artefak image harddisk. Dengan diawali tahap *plan* peneliti/penyelidik dapat merencanakan secara detail sebelum melakukan penelitian. Sehingga penelitian dapat tercapai sesuai dengan harapan dan bernilai saat digunakan sebagai alat bantu dalam pembuktian kasus kejahatan elektronik.
2. Tahap implementasi: merupakan serangkaian tindakan penerapan dari tahap *plan/*perencanaan. Penerapan dapat berupa melakukan simulasi pengumpulan bukti digital dengan metode dan *tools* forensik yang telah direncanakan. Setelah artefak

dikumpulkan dilanjut dengan melakukan verifikasi *hash* md5 agar tetap otentik dan tidak terjadi modifikasi terhadap bukti digital.

3. Tahap evaluasi: melanjutkan serangkaian proses implementasi, yaitu identifikasi dan pengumpulan informasi yang nantinya dapat menggambarkan fakta aktual tentang kejahatan yang pernah terjadi melalui artefak networ *traffic*, memori volatil dan harddrisk dengan *tools* yang telah direncanakan sebelumnya.
4. Tahap *Repeat*: merupakan tahap pengulangan yang bertujuan untuk menguji atau mengkaji ulang dari tahap *plan, implementation,* dan *evaluation* dengan objek studi kasus sebelumnya. *Repeat* adalah kunci keberhasilan dari penerapan *framework* FRED, ketika seluruh rangkaian proses pada tahap sebelum *repeat* dapat diulang kembali dengan studi kasus yang baru, dan menghasilkan temuan yang sama, maka peneliti tersebut dapat disebut *reliable* dengan konsep FRED.
5. Tahap Analisis: merupakan interpretasi hasil yang diperoleh dari serangkaian proses pada empat tahap sebelumnya. Pada penelitian ini, dari hasil analisis dapat dijelaskan bahwa temuan informasi yang banyak ditemukan tersimpan pada artefak memori volatil. Namun pada artefak lainnya informasi yang ditemukan termasuk informasi yang dapat menggambarkan adanya tindakan mengoperasikan Skyegrid dan menjalankan game.
6. Tahap Konfirmasi: merupakan tahap yang menegaskan kembali fakta yang diperoleh dari hasil dan interpretasi seluruh proses yang telah diuji, serta mempresentasikan lokasi temuan bukti digital agar terdokumentasi, dengan tujuan agar penelitian ini dapat dijadikan sebagai rujukan penyidik dalam menangani tindak kejahatan *game online* yang menggunakan layanan platform *cloud gaming*.

Sebagai laporan tambahan dalam analisa penerapan FRED yaitu dilakukan perbandingan antara *framework* FRED dengan *framework cloud computing* yang telah diterapkan oleh peneliti Taylor dkk, dalam investigasi *game online* MineCraft. Adapun *framework* yang digunakan adalah *framework An integrated conceptual digital forensic framework for cloud computing* yang dikembangkan oleh (Martini & Choo, 2012). Perbandingan atau komparasi *framework* dapat dilihat pada tabel berikut:

Tabel 4.12 Perbandingan *framework*

No	Kategori	*Framework for Reliable Experimental Design* (FRED)	*An integrated conceptual digital forensic framework for cloud computing* ((Martini & Choo, 2012)
1	Tahapan	1. *Plan* 2. *Implement* 3. *Evaluate* 4. *Repeat* 5. *Analyse* 6. *Confirm*	1. *Evidence source identification and preservation* 2. *Collection* 3. *Examination and analysis* 4. *Reporting and presentation*
2	Aktivitas	1. Merencanakan atau merumuskan secara dinamis kebutuhan berdasarkan tujuan penelitian yang akan diimplementasikan 2. Aplikasi dari tahap perencanaan, dapat berupa identifikasi, pengumpulan, akuisisi, dan pengamanan barang bukti 3. Analisis hasil pengkajian atau pengumpulan informasi yang menjadi tujuan penelitian 4. Melakukan proses ulang dimulai dari tahapan 2 dan 3, namun dengan studi kasus yang berbeda 5. Interpretasi dan klarifikasi hasil yang didapat dari tahap *evaluate* dan *repeat*. Kecocokan hasil merupakan keberhasilan pada tahap perencanaan 6. Penjelasan dan presentasi hasil	1. Identifikasi dan pelestarian sumber bukti digital berkaitan dengan layanan *cloud*. 2. Penangkapan data aktual dengan menggunakan metode pengumpulan yang sesuai dengan jenis layanan *cloud* 3. Melakukan pemeriksaan dan analisis barang bukti digital yang telah dikumpulkan. 4. Penjelasan dan presentasi fakta aktual secara hukum berdasarkan barang bukti yang ditemukan.
3	Kelebihan	Memiliki tahapan yang dinamis dengan cakupan ruang lingkup yang luas sehingga dapat digunakan dalam proses investigasi di segala cabang digital forensik. Serta dapat digunakan dalam pengembangan atau pengujian metode/*framework* sistem informasi. Hasil akhir dengan nilai reliabel, hal ini dapat meningkatkan pengambilan keputusan analisis. Serta dapat dikolaborasikan dengan metode	Memiliki Tahapan lengkap dan bersifat *logic* sesuai dengan penanganan barang bukti digital pada layanan *cloud computing*

No	Kategori	*Framework for Reliable Experimental Design* (FRED)	*An integrated conceptual digital forensic framework for cloud computing* ((Martini & Choo, 2012)
		lain yang memiliki terminologi sama.	
4	Kekurangan	Memiliki tahapan yang kompleks, membutuhkan pendefinisian yang andal dan terarah sesuai dengan tujuan penelitian. Dengan adanya tahap pengulangan hal ini akan membuat *cost atau* sumber daya menjadi mahal dan membutuhkan waktu lebih lama.	Tidak dapat digunakan dalam proses investigasi pada cabang bidang ilmu digital forensik lain. Tidak ada proses verifikasi temuan barang bukti digital.

Berdasarkan pemaparan pada Tabel 4.12 *framework* FRED memiliki tahapan dengan cakupan yang luas sehingga dapat digunakan untuk proses investigasi pada penanganan bukti elektronik maupun barang bukti digital seperti *smartphone*, IoT, multimedia, *cloud computing* dan sebagainya. FRED sebenarnya memberikan alur tahapan yang mudah untuk di implementasi, namun perlu pemahaman dan pengalaman yang cukup pada bidang digital forensik apabila akan diaplikasikan sebagai *framework* investigasi bukti digital. Tahapan plan/perencanaan merupakan kunci sukses dari penerapan FRED, untuk itu perlu pendefinisian yang baik sebagai proses identifikasi tujuan penelitian maka hasil yang diperoleh akan sesuai dengan yang diharapkan.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Setelah melakukan berbagai proses percobaan dan pengujian maka dapat ditarik sebuah kesimpulan bahwa penerapan framework FRED (*Framework for Reliable Experimental Design*) pada studi kasus penyalahgunaan game online menggunakan platform *cloud gaming* Skyegrid adalah sebagai berikut:

1. Pengumpulan barang bukti digital pada platform Skyegrid *cloud gaming services* dapat dilakukan menggunakan *framework* FRED. Tahapan FRED memiliki cakupan yang luas sehingga dapat diterapkan untuk melakukan investigasi digital forensik pada media digital lain selain pada layanan *cloud gaming*. Tahapan FRED sangat fleksibel dan mendukung verifikasi hasil. Hal ini sesuai dengan tujuan integritas penyajian informasi saat di muka hukum. Namun tahapan FRED memiliki keterbatasan yaitu perlunya pemahaman dalam tujuan perencanaan analisis yang kompleks dan besarnya *cost* sumber daya dan waktu dalam penerapan FRED saat diimplementasikan dengan studi kasus menggunakan perangkat bernilai tinggi.
2. Pada hasil pemeriksaan pada artefak *network traffic*, karakteristik jejak digital yang dapat ditemukan hanya berupa *token game* dari Skyegrid. Hal ini disebabkan metode keamanan TLS. Sementara itu temuan informasi *file* log.txt dari aplikasi Skyegrid menyimpan informasi jejak digital yang dapat menggambarkan adanya aktivitas *user* dalam mengoperasikan game. Selain itu catatan aktivitas tersebut diperkuat dengan adanya *timestamp* dari setiap aktivitas yang berjalan, dan berkorelasi dengan waktu saat melakukan simulasi game.
3. Pada penelitian ini penelusuran bukti digital disimulasikan di perangkat *client* sehingga jejak digital seperti *userID*, dan *password* Steam, *Nickname* game dan yang terpenting adalah bukti percakapan *players* melalui fitur *chating* baik saat berada di *lobby* maupun saat permainan game berlangsung tidak dapat ditemukan. Selain bukti-bukti tersebut tersimpan pada server Skyegrid, metode keamanan TLS juga menjadi penghambat pencarian pada barang bukti *network traffic* karena data *flow* menjadi terenkripsi.

5.2 Saran

Adapun saran untuk penelitian selanjutnya adalah sebagai berikut:

1. FRED merupakan *framework* yang dikembangkan dengan tujuan dapat diimplementasikan dalam segala kondisi dan jenis barag bukti digital. Sejauh ini penelitian yang menerapkan FRED masih terbatas sehingga untuk peneliti selanjutnya dapat melakukan pengujian FRED dibidang cabang digital forensik lainnya seperti forensik *smartphone*, email, IoT dan lain-lainnya.
2. Pada penelitian ini dalam proses pengumpulan bukti digital, bukti digital yang dominan ditemukan pada penyimpanan komputer (volatil memori dan harddisk), sedangkan pada artefak *network traffic* sangat sulit ditemukan karena adanya keamanan TLS. Sehingga saran untuk penelitian selanjutnya memfokuskan penelitian pada *network traffic* dengan *tools* bervariasi .
3. Sejauh pemahaman peneliti secara keilmuan digital forensik belum ada *framework* yang dikhususkan untuk menangani kejahatan pada platform game online khususnya pada platform *cloud gaming*. Untuk itu bagi peneliti selanjutnya dapat mengembangkan *framework* yang dapat mengumpulkan data digital pada game online.

Daftar Pustaka

Cai, W. E. I., Shea, R., Huang, C.-Y., Chen, K.-T., Liu, J., Leung, V. C. M., & Hsu, C.-H. (2016). A Survey on Cloud Gaming : Future of Computer Games. *IEEE Access*, *4*, 7605–7620. https://doi.org/10.1109/ACCESS.2016.2590500

Can, Y., & Security, S. (2020). *GAMING _*. *6*(2).

Chen, K.-T., Cai, W., Shea, R., Huang, C.-Y., Liu, J., Leung, V. C. M., & Hsu, H.-H. (2016). *Cloud Gaming*.

Chen, K., Huang, C., Hsu, C., & Integration, G. (2016). *CLOUD GAMING ONWARD : RESEARCH OPPORTUNITIES AND OUTLOOK Institute of Information Science , Academia Sinica Department of Computer Science and Engineering , National Taiwan Ocean University Department of Computer Science , National Tsing Hua University*.

Don, T., & Chen, L. (2018). Issues in Information Systems EXPOSING THE TOR FAILURES ON MOBILE DEVICES USING PARABEN ' S E3 : DS Issues in Information Systems. *Http://Www.Iacis.Org/Iis/*, *19*(1), 58–67. http://www.iacis.org/iis/2018/1_iis_2018_58-67.pdf

E.Ross, P. (2009). Cloud Computing ' s Killer App : Gaming. *EEE SpEctruM*.

Eskasasnanda, I. D. P. (2017). Causes and Effects of Online Video Game Playing among Junior-Senior High School Students in Malang East Java. *KOMUNITAS: International Journal of Indonesian Society and Culture*, *9*(2), 191–202. https://doi.org/10.15294/komunitas.v9i2.9565

Faisal, A., & Zulkernine, M. (2020). A secure architecture for TCP/UDP-based cloud communications. *International Journal of Information Security*, *1*. https://doi.org/10.1007/s10207-020-00511-w

Harding-rolls, P. (2019). *Next-Generation Cloud Gaming Market Report - 2019*.

Horsman, G. (2018). Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. *Computers & Security*, *73*, 294–306. https://doi.org/10.1016/j.cose.2017.11.009

Kristiyanto, D. Y., Iriani, A., Yulianto, S., & Prasetyo, J. (2018). Visualisasi dan Intepretasi Database Engine Website Penilai Kinerja Karyawan Berbasis Online Transaction Processing (OLTP). *Prosiding SINTAK 2018*, *Mvc*, 325–332.

Martini, B., & Choo, K. K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, *9*(2), 71–80.

https://doi.org/10.1016/j.diin.2012.07.001

Narayana Samy, G., Shanmugam, B., Maarop, N., Magalingam, P., Perumal, S., & Albakri, S. H. (2018). Digital forensic challenges in the cloud computing environment. *Lecture Notes on Data Engineering and Communications Technologies*, *5*, 669–676. https://doi.org/10.1007/978-3-319-59427-9_69

Nuh Al-Azhar, M. (2012). *digital forensik.* 302.

Ojala, A., & Tyrväinen, P. (n.d.). *Developing Cloud Business Models : A Case Study*. 42–47.

Soliman, O., Rezgui, A., Soliman, H., & Manea, N. (2013). *Mobile Cloud Gaming : Issues and Challenges*. 121–128.

Sulianta, F. (2016). *Komputer Forensik: Melacak Kejahatan Digital* (Ignas (ed.); Ed. I.). ANDI Yogyakarta.

Tabuyo-benito, R., Bahsi, H., & Peris-lopez, P. (2018). *Digital Forensics and Cyber Crime* (Vol. 88). Springer International Publishing. https://doi.org/10.1007/978-3-642-35515-8

Tabuyo-Benito, R., Bahsi, H., & Peris-Lopez, P. (2019). Forensics Analysis of an On-line Game over Steam Platform. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *259*, 106–127. https://doi.org/10.1007/978-3-030-05487-8_6

Taylor, D. C. P. J., Mwiki, H., Dehghantanha, A., Akibini, A., Choo, K. K. R., Hammoudeh, M., & Parizi, R. (2019). Forensic investigation of cross platform massively multiplayer online games: Minecraft as a case study. *Science and Justice*, *59*(3), 337–348. https://doi.org/10.1016/j.scijus.2019.01.005

Wu, Z. (2014). Gaming in the cloud : one of the future entertainment. *Interactive Multimedia Conference*.

Zhao, C. (2018). Cyber security issues in online games. *AIP Conference Proceedings*, *1955*(April). https://doi.org/10.1063/1.5033679

LAMPIRAN A