

Deteksi Bukti Digital *Game Online* Pada Platform Skyegrid Menggunakan *Framework FRED*

Ramansyah ^{*1}, Yudi Prayudi², Imam Riadi³

^{1,2}Program Studi Teknik Informatika, Universitas Islam Indonesia, Jl. Kaliurang KM.14,5 Sleman, Yogyakarta, 55584

³Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Jl. Prof. Dr. Soepomo, Janturan, Yogyakarta 55164

e-mail: ^{*1}17917126@students.uui.ac.id, ²prayudi@uui.ac.id, ³imam.riadi@is.uad.ac.id

Abstrak

Layanan cloud gaming memberikan akses game online berspesifikasi tinggi, namun 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. Berbagai kerangka kerja telah diusulkan oleh para peneliti terdahulu salah satunya adalah kerangka kerja Framework for Reliable Experimental Design (FRED). Fokus penelitian ini adalah melakukan identifikasi bukti digital dari tindak kejahatan yang terjadi pada platform Skyegrid cloud gaming services dengan menerapkan langkah kerja FRED. Hasil temuan penting dari penelitian ini berupa username, password login di Skyegrid, dan file log.txt yang mendeskripsikan adanya riwayat akses Skyegrid dan game online.

Kata kunci—cloud gaming service, Skyegrid, FRED, network forensik, komputer forensik.

Abstract

Cloud gaming services provide access to high-specification online games, but can be accessed with a minimalist device. The ease of access invites new crimes and challenges violations that are found to find digital clues and evidence in uncovering cases of crimes that occur. The cloud forensic science approach remains a challenge for investigators because each cloud provider, especially cloud gaming services, has a different architecture so that further research is needed in carrying out cloud gaming forensics services. Various frameworks have been proposed by previous researchers, one of which is the Framework for Reliable Experimental Design (FRED) framework. The focus of this research is to show digital evidence of crime on the Skyegrid cloud gaming services platform by implementing FRED work steps. The important findings of this research are username, password login on Skyegrid, and log.txt file which describes the history of access to Skyegrid and online game.

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

1. PENDAHULUAN

Perkembangan teknologi jaringan informasi dan teknologi komunikasi semakin meningkat. Hal ini juga menerpa pada perkembangan *game online* khususnya pada platform *game online*. *Game online* sebagai media hiburan mampu mengubah berbagai sektor seperti sektor ekonomi, teknologi, dan sosial. *Game online* pada umumnya membutuhkan platform komputer

yang mahal untuk mendukung komputasi dan grafis. Namun hal tersebut menjadi permasalahan bagi pengguna *game* yang hanya memiliki komputer spesifikasi minim.

Cloud gaming services merupakan pengembangan dari metode *cloud computing* [1], teretus setelah diperkenalkan prototipe teknologi *G-cluster* [2]. *Cloud gaming service* akan menjadi teknologi yang berkembang 20 tahun ke depan dalam platform *game online* [3], seiring perkembangan teknologi jaringan komunikasi. *Cloud gaming service* seperti layanan *cloud hosted desktop* [4], seluruh *file game* sudah terpasang di komputer server *cloud gaming service* sehingga *game online* berspesifikasi grafis tinggi dapat dinikmati melalui perangkat mini. Selain itu platform *cloud gaming* akan menjadi solusi yang menguntungkan bagi kalangan pengguna, developer dan industri *game*. Bagi pengguna keuntungan menggunakan *cloud gaming services* adalah tidak membutuhkan perangkat keras yang mahal, tidak perlu *download, install, dan update game* dikarenakan semua utilitas *game* sudah terpasang di server *cloud gaming services*. Kemudian keuntungan bagi *developer game* yaitu sinkronisasi, *update patch* dan *rebuild sourcecode* menjadi lebih efisien. Pada industri *game*, keuntungan yang didapatkan yaitu mempermudah dalam pemasaran, penjualan, dan minimalnya dari pembajakan *game* [1].

Skyegrid merupakan vendor asal Indonesia yang menyediakan jasa sewa *cloud gaming services*. Pengguna dapat menggunakan layanan Skyegrid dengan berlangganan mingguan atau bulanan. Keunggulan dari layanan Skyegrid dari platform *game online* lainnya seperti Xbox dan PlayStation yaitu pengguna tidak perlu melakukan pengunduhan dan pemasangan *game*. Pada Skyegrid ratusan *game* telah dipasang dan *update* secara berkala, pengguna hanya tinggal bermain *game* yang diminati. Bermain *game online* pada Skyegrid dapat digambarkan seperti mengoperasikan *game online* secara *remote desktop*, sehingga seluruh aktivitas *game online* tersimpan pada komputer server Skyegrid. Hal ini menjadikan Skyegrid dapat dimanfaatkan oleh individu ataupun kelompok untuk melakukan kejahatan dunia maya seperti *cyber bully, child grooming, cyber terrorism*, dan perdagangan narkoba [5][6].

Opsi penanganan kejahatan tersebut dapat menggunakan metode forensik yang telah diusulkan oleh peneliti sebelumnya, seperti metode *network*, dan *computer forensik* dengan teknik akuisisi *live system* dan *post-mortem* [7]. Perlu menjadi perhatian meskipun opsi penanganan telah dikemukakan, tentunya setiap proses identifikasi jejak digital pada layanan cloud tidak dapat ditangani dengan perlakuan yang sama, disebabkan standar dan karakteristik layanan cloud yang beredar tidak identik [8]. Selain itu, sejauh ini belum ada peneliti yang membahas investigasi pada layanan cloud gaming. Sehingga perlu dilakukan penelitian bagaimana penanganan kasus kejahatan pada layanan cloud gaming sebagai platform *game online* yang *reliable* dan terdokumentasi.

Ada beberapa *framework* yang telah ditawarkan untuk penyelesaian masalah pada layanan cloud, antara lain adalah *Framework for Reliable Experimental Design (FRED)* [9]. FRED dikembangkan dalam kerangka kerja untuk mengatasi permasalahan reliabilitas data, pengujian, validasi, mendukung output yang andal, dapat diulang, dan dapat didokumentasikan [9].

Berdasarkan paparan di atas, perlu dilakukan investigasi bukti digital pada layanan cloud gaming dengan pendekatan *framework* FRED. Studi kasus menggunakan Skyegrid sebagai vendor layanan cloud gaming services, dan *game online* yang digunakan adalah Dota 2 dan Counter Strike GO (CS:GO).

2. METODE PENELITIAN

2.1 Tinjauan Pustaka

2.1.1 Penelitian Terdahulu

Sependek pengetahuan peneliti, belum ada penelitian sebelumnya yang fokus membahas investigasi forensik pada *cloud gaming*. Penelitian terdahulu lebih fokus pada pendekatan

melakukan analisis sistematis dan usulan pengembangan pada teknologi dan infrastruktur *cloud gaming*. Penelitian oleh [10], berjudul *A Survey on Cloud Gaming: Future of Computer Games*, mengkaji beberapa penelitian *cloud gaming* dari berbagai aspek yang mencakup pengoptimalan arsitektur, dan layanan *cloud gaming* yang direntalkan. Penelitian selanjutnya berjudul *Toward Multiplayer Cooperative Cloud Gaming* secara sistematis membahas tren dan perkembangan arsitektur jaringan pendukung untuk game *multiplayer* pada platform *cloud gaming services* [11], dengan fokus pembahasan pada modalitas optimalisasi *cloud gaming services* yang mengadopsi *game multiplayer*. Berikutnya penelitian pada *cloud gaming* yang berjudul *Cost-Efficient and Quality of Experience-Aware Provisioning of Virtual Machines for Multiplayer Cloud Gaming in Geographically Distributed*, mengusulkan algoritma yang disebut *grey wolf* untuk pengoptimalan pada masalah *delay* pada *interface player* yang diintegrasikan dengan arsitektur jaringan *virtual mesin multiplayer cloud gaming* [12].

Pada lingkup platform *game online*, beberapa peneliti telah melakukan analisis forensik digital terhadap platform *game online* yang telah beredar, seperti pada platform Steam yang berjudul *Forensic Analysis Of A Steam Based Online Game*, dengan fokus penelitian pada *game online Counter Strike Nexon Zombies (CSNZ)* [7]. Penelitian yang diusulkan sangat sistematis khususnya dalam memaparkan hasil temuan dan analisis yang bersumber dari tiga barang bukti digital, yaitu *network capture*, memori volatil dan harddisk, dengan penerapan *framework forensik McKemish*. Peneliti juga dapat memaparkan adanya celah keamanan pada *session_id* dari Steam yang dapat diduplikasi. Penelitian selanjutnya yaitu terkait platform Windows dan Linux yang berjudul *Forensic investigation of cross platform massively multiplayer online games: Minecraft as a case study* [13], peneliti memaparkan hasil investigasi dari platform Windows dan Ubuntu yang dibentuk menjadi arsitektur *client server*, dengan studi kasus pada *game online Minergraf*. Metode pengumpulan bukti digital yang diterapkan juga bersumber dari *network traffic*, memori volatil dan harddisk, dengan penerapan *framework integrated conceptual digital forensic* yang dibuat oleh [14]. Hasil analisis peneliti berhasil memaparkan bukti digital pada *client* dan server.

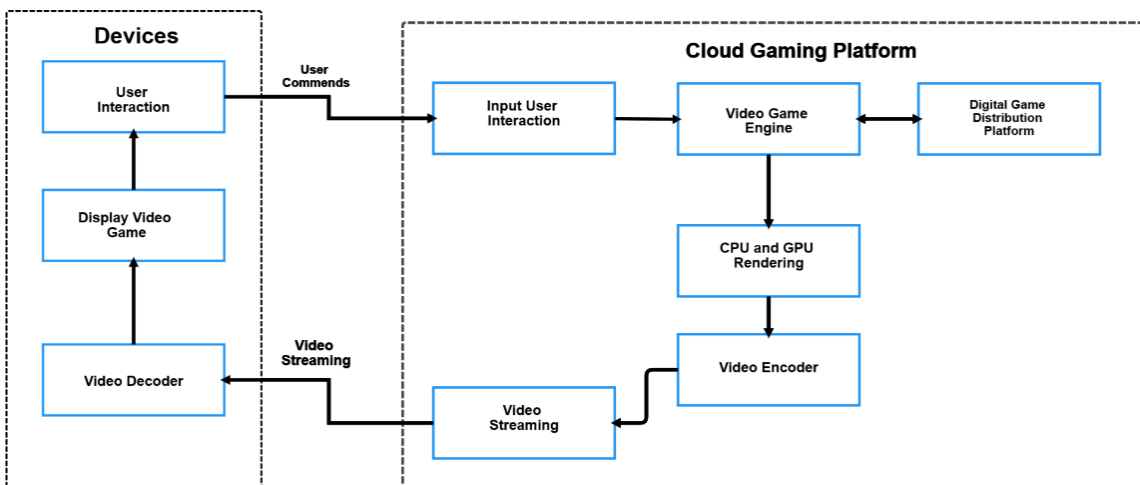
Framework for Reliable Experimental Design (FRED) terdiri dari enam tahapan yaitu *plan, implement, evaluate, repeat, analysis, dan confirm*. Desain FRED sebagai *framework* yang diunggulkan yaitu pada nilai validasi dari temuan bukti digital. Sejauh ini FRED telah diadopsi pada beberapa penelitian diantaranya oleh [14] yang berjudul *Visualisasi dan Interpretasi Database Engine Website Penilai Kinerja Karyawan Berbasis Online Transaction Processing (OLTP)* peneliti melakukan analisis pada *log*, dan *database Mariadb* pada aplikasi penilai kinerja karyawan PT. Campus Media dengan menggunakan teknik akuisisi *perfect copy*, dengan menggunakan FRED peneliti dapat memaparkan hasil temuan bukti digital dari tindakan kecurangan catatan digital dari beberapa *data* seperti pada *file type, file path, file logical size, file physical size, hash (checksum) created date, modified date, accessed date, sector, cluster*, dan lainnya pada website penilai kinerja karyawan pada PT. Campus Media. Penelitian selanjutnya oleh [15] berjudul *Issues in Information Systems Exposing The Tor Failures On Mobile Devices Using Paraben's E3:DS Issues in Information Systems*. Penelitian ini berupaya menguji hipotesis dari fungsi *privasi* yang ditawarkan oleh *browser Tor Bundle* di Android. Namun hasil analisa yang dipaparkan menjelaskan bahwa fitur *privasi* tersebut tetap berhasil diekstrak sehingga situs-situs yang pernah diakses dapat diketahui, selain itu peneliti juga memaparkan adanya celah atau kelemahan di *Tor Bundle* yaitu data aktivitas pengguna tidak seutuhnya terlindungi sehingga tidak terpenuhi konsep anonim.

2.1.2 Skyegrid Cloud Gaming Services

Layanan *cloud gaming* disebut *gaming on demand*, yaitu platform *game* daring dari penggabungan teknologi komputasi awan yang menyediakan fasilitas sumber daya penyimpanan data tidak terbatas, dipadukan dengan teknologi komputasi grafis tingkat tinggi.

Layanan *cloud gaming* memungkinkan pemain mengontrol dan menjalankan game yang diinginkan melalui internet dari beragam perangkat gawai secara daring. Secara mendasar konsep platform *cloud gaming* sebagaimana tersebut pada Gambar 1. 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 ditransmisikan kembali setiap pergerakan gambar ke *display* monitor *user* melalui jaringan internet [16].

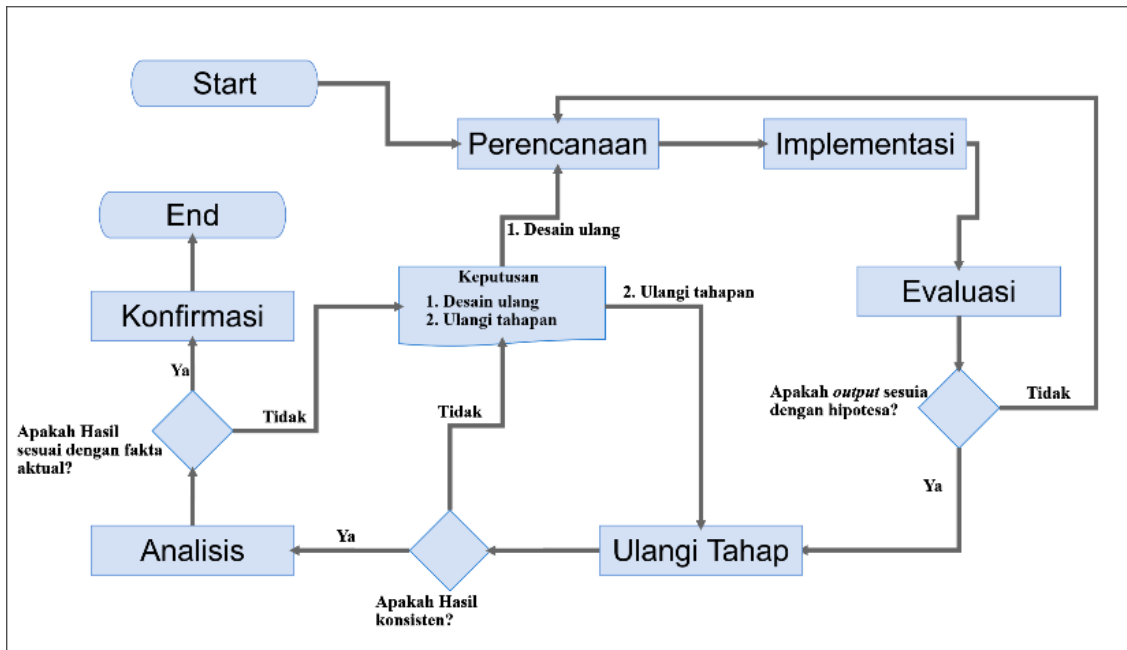
Skyegrid merupakan salah satu layanan *cloud gaming* yang menawarkan akses ratusan game *online* yang siap untuk dimainkan. Harga sewa Skyegrid terbilang murah dibandingkan dengan layanan *cloud gaming* lainnya. Game online yang tersedia di beranda Skyegrid berjalan tanpa di emulasi pada perangkat lokal, cukup *install* Skyegrid pada perangkat yang akan digunakan sehingga *user* tidak perlu melakukan pengunduhan, pemasangan dan pembaharuan game.



Gambar 1. Alur Proses Kerja *Cloud Gaming Service*

2.1.3 Framework for Reliable Experimental Design (FRED)

Framework for Reliable Experimental Design FRED terdiri dari enam tahapan yakni: perencanaan, implementasi, evaluasi, pengulangan, analisis, dan konfirmasi. Tahap perencanaan merupakan proses merumuskan tujuan dan bagaimana cara untuk mendeteksi bukti digital pada platform Skyegrid dengan pendekatan metode analisis forensik. Selanjutnya perencanaan harus diimplementasikan sesuai rumusan yang telah direncanakan. Selanjutnya setelah tahap implementasi sukses, hasilnya dilakukan evaluasi dengan cara melakukan identifikasi dan mendeteksi potensi bukti digital dengan metode forensik yang telah direncanakan. Tahap pengulangan adalah serangkaian proses pengujian kembali dimulai dari tahap implementasi dan evaluasi. Hasil deteksi bukti digital harus konsisten sehingga dapat disebut reliabel. Tahap analisis menginterpretasikan hasil yang diperoleh dari pengujian, pengumpulan, dan identifikasi pada tahap evaluasi dan pengulangan. Tahap konfirmasi sebagai tahap terakhir berisi rangkuman dari serangkaian proses yang telah dilakukan sebagai proses dokumentasi pengujian Berikut adalah alur *framework* FRED yang dapat dipresentasikan sebagaimana tersebut pada gambar 2.



Gambar 2. Diagram Tahapan FRED

2.2 Metode Penelitian

Pada penelitian ini dalam penyelidikan potensi bukti digital pada Skyegrid *cloud gaming services* akan mengadopsi *framework* FRED. Berikut adalah alur tahapan penelitian yang dapat dipresentasikan sebagaimana tersebut pada Gambar 3:



Gambar 3. Metode Penelitian

Metodologi yang diusulkan menjelaskan bagaimana tahapan penelitian dilakukan sehingga dapat diketahui tahapan proses dan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan khususnya pada ruang lingkup *cloud gaming services*.

3. HASIL DAN PEMBAHASAN

3.1 Persiapan Sistem

Persiapan sistem merupakan tahapan menyediakan kebutuhan *software* dan *hardware* mencakup berlangganan Skyegrid, membuat akun *game online* dan memasang Skyegrid pada laptop DELL Inspiron 14 dengan menggunakan platform sistem operasi Windows 10 Pro. Kemudian menyiapkan *tools* digital forensik, dan perangkat tambahan HDD eksternal beserta *Docking Station*. Sebagaimana terlampir pada Tabel 1:

Tabel 1. Spesifikasi *Tools* yang Digunakan

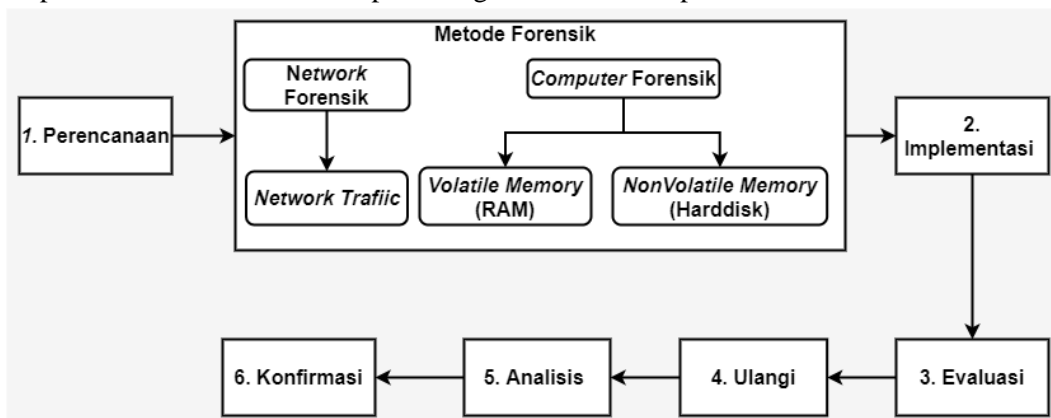
No	Hardware/ Software	Keterangan
1	Laptop DELL Inspiron 14, Core i5, SSD 128 GB	Hardware
2	SATA 3.0 HDD Docking Station	
3	HDD 3.0 TB WD30PURX	
4	Sistem Operasi Windows 10 Profesional dengan arsitektur 64bit	Sistem Operasi
5	FTK Imager 4.2.0.13	Forensic <i>Tools</i>
6	Sleuth Kit Autopsy Forensics 4.15.0	
7	Network Miner 2.5 Windows	
8	Wireshark Version 3.2.1 Windows	
9	WinHex 18.7 Windows	
10	Volatility Windows	
11	Hashmyfile	<i>Tools Hashing</i>

3.2 Skenario Kasus

Pada tahapan ini membuat simulasi penyalahgunaan game online pada game Dota 2 menggunakan Skygrid, dengan cara mengirim pesan *chat* saat berada dalam *lobby* game Dota 2, dan disaat permainan berlangsung. Akun yang digunakan di Skygrid adalah *username*: tgs.thesis02@gmail.com, dan *password*: Tekan enter?, kemudian untuk akun game Dota 2 adalah *username*: tgs.thesis02, dan *password*: Tekan enter?. Selanjutnya melakukan akuisisi, eksaminasi, dan analisis apakah komunikasi menggunakan fitur *chat* dapat ditemukan.

3.3 Penerapan FRED

Setelah tahapan simulasi berhasil dilakukan, proses selanjutnya adalah melakukan identifikasi dan analisis potensi bukti digital dengan penerapan Framework FRED. Sehingga dalam penelitian ini diusulkan tahapan sebagaimana tersebut pada Gambar 4:



Gambar 4. FRED pada Skygrid Cloud Gaming Services

3.3.1 Perencanaan

Perencanaan deteksi bukti digital pada penelitian ini dilakukan dengan menggunakan dua pendekatan metode forensik digital yaitu *network* dan *computer forensics*. Metode *network*

forensik digunakan untuk pengumpulan, identifikasi, dan analisis pada artefak *network capture* dengan cara melakukan penangkapan lalu lintas data pada NIC (*network interface card*) menggunakan *tool* Wireshark saat proses simulasi kasus berjalan. Sedangkan pendekatan *computer forensik* digunakan untuk pengumpulan, identifikasi, dan analisis pada artefak memori volatil (RAM), dan memori non-volatil (HDD) dengan cara *dumping* memori menggunakan *tool* FTK Imager. Proses akuisisi memori RAM dilakukan saat simulasi *game* sedang berlangsung. Kemudian akuisisi pada HDD menggunakan *tool* FTK Imager secara *physical acquisition imaging copy bit to bit* keseluruhan pada HDD yang ditransfer ke HDD *external docking station*.

3.3.2 Implementasi

Untuk memperoleh artefak digital yang menginterpretasikan hasil yang diinginkan, proses akuisisi dilakukan secara bertahap dan bersamaan saat simulasi bermain game Dota 2 berjalan. Pertama, proses *network capture* yang dilakukan sebelum menjalankan Skyegrid. Kedua, proses *dump* pada memori volatil dilakukan setelah melakukan proses *login* di Skyegrid, *login* di Steam, mengirim pesan *chat*, dan main game. Ketiga, proses akuisisi pada HDD dilakukan setelah seluruh proses simulasi main game selesai. Namun sebelum melakukan proses akuisisi pada HDD dilakukan, terlebih dahulu menghubungkan HDD eksternal berupa *docking station* ke perangkat yang diuji coba. Selanjutnya ketiga artefak dilakukan *hashsing* MD5 untuk menjaga keaslian artefak digital. Kemudian ketiga artefak disimpan di HDD eksternal untuk proses selanjutnya. Adapun hasil hashing MD5 dari ketiga artefak terlampir pada Tabel 2.

Tabel 2. Nilai *Hash* MD5

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

3.3.3 Evaluasi

Setelah proses pengumpulan selesai, selanjutnya dilakukan identifikasi dan eksplorasi terhadap artefak digital yang sudah terkumpul. Setelah beberapa saat melakukan identifikasi pada seluruh artefak digital yang telah dikumpulkan, peneliti menemukan letak *file* dan *directory* sebagai informasi penting yang bisa dijadikan bukti digital sebagaimana tercantum pada Tabel 3.

Tabel 3. Hasil Temuan dari Tahap Evaluasi

Network Capture	Dump Memori RAM	Image Harddisk
1. Pada <i>tcp.stream eq 25</i> di <i>source IP address</i> 161.202.172.211	1. Informasi di temukan pada <i>offset</i> 0134F38B0	1. log.txt (c:\\Users\DELL01\SKYEGRID\LOG.TXT)
	2. Informasi di temukan pada <i>offset</i> 07b51cee0	2. IconCache.db (C:\users\DELL01\AppData\Local\Skyegrid\)
	3. Informasi di temukan pada <i>offset</i> 0134f36d0	3. qmlcache (c:\users\DELL01\AppData\Local\Skyegrid\cache\qmlcache)
	4. Informasi di temukan pada <i>offset</i> 0134f2ff0	4. NTUSER.DAT (c:\users\DELL01\NTUSER.D

		AT\Software\Skyegrid)
		5. Windows Prefetch (c:\Windows\Prefetch)
		6. Web Browsing Histori (C:\users\DELL01\AppData\Local\Google\Chrome\User Data\Default\History)

Tabel 4. Hasil Temuan dari Tahap Ulang

Network Capture	Dump Memori RAM	Image Harddisk
Pada tcp.stream eq 37 dengan source IP address 161.202.175.213	1. Informasi di temukan pada offset 01f7258c0	1. log.txt (c:\Users\DELL01\SKYEGRID\LOG.TXT)
	2. Informasi di temukan pada offset 025a81a40	2. IconCache.db (C:\Users\DELL01\AppData\Local\Skyegrid)
	3. Informasi di temukan pada offset 01f7256e0	3. qmlcache (c:\Users\DELL01\AppData\Local\Skyegrid\cache\qmlcache)
	4. Informasi di temukan pada offset 01f725000	4. NTUSER.DAT (c:\Users\DELL01\NTUSER.DAT\Software\Skyegrid) 5. Windows Prefetch (c:\Windows\Prefetch) 6. Web Browsing Histori (C:\Users\DELL01\AppData\Local\Google\Chrome\User Data\Default\History)

3.3.4 Ulangi

Agar hasil temuan dapat disebut reliabel maka pada tahap ini, akan dilakukan kembali dimulai dari proses simulasi, pengumpulan dan identifikasi artefak digital dengan game CS:GO yang dijalankan pada Skyegrid. Hasilnya informasi yang ditemukan baik letak *file* dan *directory* masih identik serupa dari hasil temuan pada tahap evaluasi. Adapun temuan informasi bukti digital dari proses ini, dapat dilihat pada Tabel 5.

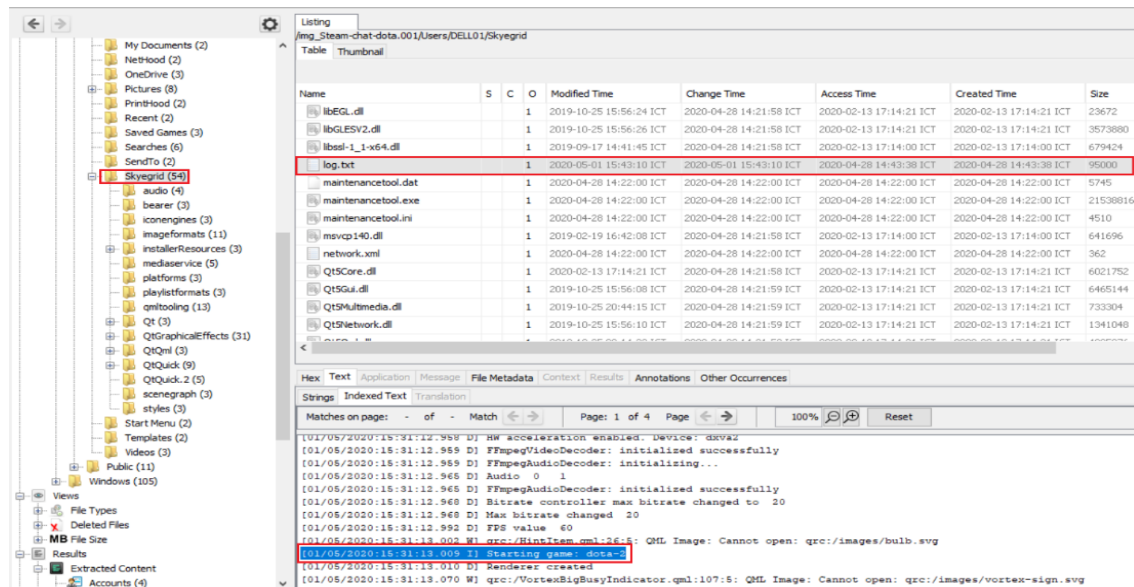
Tabel 5. Karakteristik Temuan Bukti Digital pada Platform Skyegrid

Network Capture	Dump Memori RAM	Image Harddisk
1. Game token dan informasi perangkat yang digunakan saat menjalankan aplikasi Skyegrid “7901001d-f163-4873-ad81-b87d7d276ace”	1. Game token dan informasi perangkat yang digunakan saat menjalankan aplikasi Skyegrid	1. File Log.txt aplikasi Skyegrid
	2. Username dan password akun Skyegrid	2. informasi File IconCache.db
	3. Game Dota 2 nama dari game yang digunakan	3. Folder qmlcache berisi informasi konfigurasi session Skyegrid

4. <i>Timestamp</i> menjalankan Skyegrid [01/05/2020:15:30:33]	4. NTUSER.DAT
	5. Windows <i>Perfecth</i>
	6. Web <i>browsing</i> histori

3.3.5 Analisis

Interpretasi hasil analisis dari proses evaluasi, dan pengulangan dapat dikemukakan sebagai mana terlihat pada Tabel 5. Analisis dari artefak *network capture* terhambat dikarenakan adanya metode keamanan TLSv1.2 yang membuat beberapa komunikasi data menjadi terenkripsi, sehingga hanya satu informasi yang dapat ditemukan pada artefak *network capture*. Selain itu informasi otentik yang dapat dijadikan bukti digital adalah *log.txt* dari aplikasi Skyegrid. Di dalam *log.txt* ada informasi terkait waktu aplikasi Skyegrid dijalankan, waktu dijalankan game Dota 2, dan informasi *token* game serta dilengkapi informasi perangkat yang digunakan saat menjalankan Skyegrid. Sebagai terlihat pada Gambar 5.



Gambar 5. File Log.txt

3.3.6 Konfirmasi

Karakteristik bukti digital yang ditemukan meskipun tidak dapat menunjukkan secara gamblang siapa pelaku dan bukti percakapan *chatting* 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. *Timestamp* pada ketiga artefak dikorelasikan dan hasilnya sesuai dengan waktu simulasi penyalahgunaan game pada platform Skyegrid. 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 di dalam komputer server Skyegrid.

4. KESIMPULAN

Berdasarkan hasil yang diperoleh setelah melakukan berbagai proses, maka dapat disimpulkan bahwa dalam penelitian ini dengan penerapan FRED pada penyalahgunaan *game online* di platform Skyegrid *cloud gaming services*, bukti digital dapat dideteksi dari akuisisi dan analisis pada artefak *network capture*, memori volatil RAM, dan HDD. Dari hasil analisis bentuk karakteristik bukti digital berupa *token game*, akun *login* di Skyegrid, nama *game* yang digunakan, waktu menjalankan Skyegrid dan *game*, *file log.txt* Skyegrid, dan informasi lokasi pemasangan (*install*) aplikasi Skyegrid. Namun hasil pemeriksaan pada artefak *network traffic* jejak digital yang ditemukan sangat sulit dan sedikit disebabkan protokol komunikasi TCP/UDP menggunakan keamanan TLSv1.2 sehingga seluruh paket data yang ditransmisikan menjadi terenkripsi. Selain itu, informasi berupa akun *login* Steam, percakapan melalui fitur *chat* tidak dapat ditemukan di tiga artefak digital, hal ini menandakan informasi tersebut tersimpan di server Skyegrid.

5. SARAN

Perkembangan *game online* akhir dekade ini semakin pesat, hal ini terjadi disebabkan meningkatnya peminat *game online* sehingga penyalahgunaan pada *game online* dapat terjadi. Saran untuk pengembangan penelitian selanjutnya dapat melakukan analisis yang memfokuskan pada artefak *network traffic* dengan metode dan *tools* forensik yang beragam untuk memperluas temuan bukti digital khususnya percakapan pada fitur *chat game*.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa karena atas penyertaan-Nya sehingga penulis dapat menyelesaikan jurnal ini. Penulis juga mengucapkan terima kasih kepada keluarga, guru, teman-teman terdekat yang sudah memberikan dukungan kepada penulis untuk menyelesaikan jurnal ini.

DAFTAR PUSTAKA

- [1] K. Chen, C. Huang, C. Hsu, and G. Integration. 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.*”
- [2] P. E.Ross. 2009, “*Cloud Computing ’ s Killer App: Gaming,*” *EEE Spectr.*
- [3] P. Harding-rolls. 2019, “*Next-Generation Cloud Gaming Market Report - 2019.*”
- [4] N. Widiyasono, I. Riadi, and A. Luthfi. 2016, “*Penerapan Metode ADAM pada Proses Investigasi Layanan Private Cloud Computing,*” *J. Edukasi dan Penelit. Inform., Vol. 2, No. 1, doi: 10.26418/jp.v2i1.15501.*

-
- [5] K. R. Choo. 2009, "Online Child Grooming: A Literature Review On The Misuse of Social Networking Sites For Grooming Children For Sexual Offences," *Aust. Inst. Criminol.*, p. 132, doi: 10.1037/e582922012-001.
- [6] I. Riadi, R. Umar, and M. A. Aziz. 2019, "Forensik Web Layanan Instant Messaging Menggunakan Metode Association of Chief Police Officers (ACPO)," *Mob. Forensics*, Vol. 1, No. 1, p. 30, doi: 10.12928/mf.v1i1.705.
- [7] R. Tabuyo-Benito, H. Bahsi, and P. Peris-Lopez. 2019, "Forensics Analysis of An Online Game Over Steam Platform," in *Lecture Notes of The Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, Vol. 259, pp. 106–127, doi: 10.1007/978-3-030-05487-8_6.
- [8] D. Birk and C. Wegener. 2011, "Technical Challenges of Forensic Investigations in Cloud Computing Environments," doi: 10.1109/SADFE.2011.17.
- [9] W. Yassin, M. Faizal Abdollah, R. Ahmad, Z. Yunus, and A. Ariffin. 2020, "Cloud Forensic Challenges and Recommendations: A Review," *J. Cyber Secur.*, Vol. 2, No. 1, pp. 19–29, [Online]. Available: <https://www.oic-cert.org/en/journal/vol-2-issue-1/cloud-forensic-challenges-and-recommenda.html>.
- [10] W. E. I. Cai *et al.* 2016, "A Survey on Cloud Gaming: Future of Computer Games," *IEEE Access*, Vol. 4, pp. 7605–7620, doi: 10.1109/ACCESS.2016.2590500.
- [11] W. Cai, F. Chi, X. Wang, and V. C. M. Leung. 2018, "Toward Multiplayer Cooperative Cloud Gaming," *IEEE Cloud Comput.*, Vol. 5, No. 5, pp. 70–80, doi: 10.1109/MCC.2018.326105129.
- [12] Y. Gao, L. Wang, and J. Zhou. 2019, "Cost-Efficient and Quality of Experience-Aware Provisioning of Virtual Machines for Multiplayer Cloud Gaming in Geographically Distributed Data Centers," *IEEE Access*, Vol. 7, pp. 142574–142585, doi: 10.1109/ACCESS.2019.2944405.
- [13] D. C. P. J. Taylor *et al.*, "Forensic Investigation of Cross Platform Massively Multiplayer Online Games: Minecraft As a Case Study," *Sci. Justice*, Vol. 59, No. 3, pp. 337–348, 2019, doi: 10.1016/j.scijus.2019.01.005.
- [14] D. Y. Kristiyanto, A. Iriani, S. Yulianto, and J. Prasetyo, 2018, "Visualisasi dan Interpretasi Database Engine Website Penilai Kinerja Karyawan Berbasis Online Transaction Processing (OLTP)," *Pros. SINTAK 2018*, No. Mvc, pp. 325–332.
- [15] T. Don and L. Chen. 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/>, Vol. 19, No. 1, pp. 58–67, [Online]. Available: http://www.iacis.org/iis/2018/1_iis_2018_58-67.pdf.
- [16] Z. Wu. 2014, "Gaming in The Cloud: One of The Future Entertainment," *Interact. Multimed. Conf.*