JTIIK ID 1516

by 1516 Jtiik

Submission date: 02-Jan-2019 07:21AM (UTC+0700)
Submission ID: 1061092606
File name: 1516-5001-1-RV.docx (1.66M)
Word count: 4014
Character count: 26591

Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)
Vol. x, No. x, April 2014, hlm. x-x
Akreditasi KEMENRISTEKDIKTI, No. 30/E/KPT/2018

DOI: 10.25126/jtiik...
p-ISSN: 2355-7699
e-ISSN: 2528-6579

ANALISIS FORENSIK SOLID STATE DRIVE (SSD) MENGGUNAKAN FRAMEWORK *GRR RAPID RESPONSE*

(Naskah masuk:, diterima untuk diterbitkan:)

Abstrak

Teknologi komputer mengalami perkembangan dapat menyamai kemampuan manusia dalam berpikir *(Artificial Intelligence)* dan mengalami kemajuan dalam hal integrasi dengan perangkat lain *Internet of Things (IoT)*. Namun bersamaan dengan itu, pemakaian komputer juga berdampak negatif. Dampak negatif komputer salah satunya adalah berupa kejahatan komputer. Kejahatan komputer meninggalkan jejak aktivitas kejahatannya yang perlu dilakukan analisa dengan ilmu dan metode forensik. Bagaimana jika terjadi kejahatan komputer pada media penyimpanan komputer berjenis *non-volatile memory* dan dilakukan secara *live forensics*. Pada penelitian ini dilakukan proses forensik pada *Solid State Drive (SSD)* dengan framework *Grr Rapid Response* pada kasus kehilangan *data (lost data)* suatu organisasi. Langkah kerja forensik mengimplementasikan dari *National Institute of Standards Technology (NIST)*. Framework *Grr Rapid Response* digunakan untuk memberikan tanggapan terhadap insiden forensik digital yang difokuskan pada lingkungan forensik jarak jauh, *framework* ini berbasis arsitektur *client server*. Hasil penelitian ini menunjukkan langkah kerja forensik *NIST* dapat diimplementasikan pada proses pengambilan bukti digital dengan metode akuisisi secara *live forensik*, kemampuan *tool* forensik pada proses eksaminasi *Grr Rapid Response* pada *Workstation (Client Grr)* dengan media simpan *SSD*, artefak digital dapat ditemukan dan dikembalikan. Bukti digital yang dapat dikembalikan berupa *file* dokumen dengan nama $IU8CR9P.docx memiliki ukuran *file* 136 *byte* dan memiliki nilai *hash* yang sama yaitu dengan nilai *hash* MD5 e3b73544af0686081d9b72e481450af2 dan nilai *hash* SHA1 3e66678e5a30d2731b100e1cf646c206a583e808, maka dapat dikatakan bukti digital tersebut identik.

Kata kunci: *Analisis, Forensik, SSD, Grr Rapid Response*

FORENSIC ANALYSIS OF SOLID STATE DRIVES (SSD) USING THE GRR RAPID RESPONSE FRAMEWORK

Abstract

Computer technology has evolved to be able to match human capabilities in thinking (Artificial Intelligence) and progress in terms of integration with other devices Internet of Things (IoT). But along with that the use of computers also had a negative impact. One of the negative effects of computers is computer crime. Computer crime leaves a trail of criminal activity that needs to be analyzed with forensic science and methods. What if there is a computer crime on a computer storage medium of a type of non-volatile memory and carried out live forensics. In this study a forensic process on Solid State Drive (SSD) was carried out in the Grr Rapid Response framework for lost data in an organization. The forensic work step is implemented from the National Institute of Standards Technology (NIST). The Grr Rapid Response Framework is used to provide responses to incidents of digital forensics focused on remote forensic environments, this framework is based on a client server architecture. The results of this study indicate that NIST's forensic work steps can be implemented in the process of taking digital evidence with live forensic acquisition methods, the ability of forensic tools in the Grr Rapid Response examination process on Workstations (Client Grr) with SSD storage media, digital artifacts can be found and returned. Digital evidence that can be returned in the form of a document file with the name $IU8CR9P.docx has a file size of 136 bytes and has the same hash value with MD5 hash value e3b73544af0686081d9b72e481450af2 and SHA1 hash value 3e66678e5a30d2731b100e1cf646c206a583e808, digital evidence is identical.

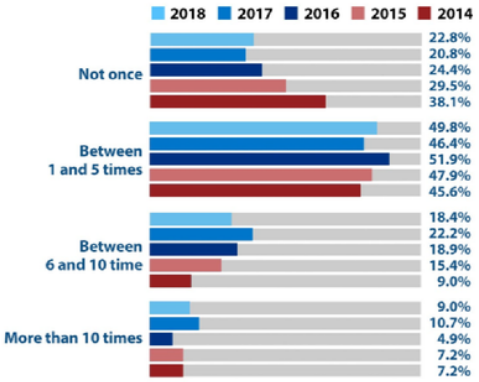
Keywords: *Analysis, Forensics, SSD, Grr Rapid Response*

1. PENDAHULUAN

Komputer telah berkembang selama lebih dari 5 dekade, di era teknologi komputasi sekarang ini aktivitas penggunaan teknologi komputer, perangkat keras, dan perangkat lunak komputer berkembang sangat pesat. Pada awalnya perkembangannya komputer memberikan dampak yang signifikan terutama pada industri perbankan, asuransi, dan industri manufaktur terutama dari segi efisiensi operasional. Namun saat ini teknologi komputer mengalami perkembangan dimana teknologi ini dapat menyamai kemampuan manusia dalam berpikir atau disebut dengan kecerdasan buatan *(Artificial Intelligence)*, dan saat ini sistem komputer juga mengalami kemajuan dalam hal integrasi dengan perangkat lain. Komputer semakin banyak terhubung dengan berbagai perangkat di berbagai tempat dengan teknologi yang berkembang bersama yaitu *Internet of Things (IoT)*.

Namun bersamaan dengan itu, pemakaian komputer juga memiliki manfaat positif maupun dampak negatif. Dampak negatif tersebut yang perlu perhatian dan perlu penanganan dari semua *stakeholder*. Dampak negatif komputer salah satunya adalah berupa kejahatan komputer, kejahatan tersebut yang sering terjadi antara lain, 1) *Illegal Access*, kejahatan ini terkait dengan pencurian data penting dengan cara mengakses komputer secara tidak sah, dengan tujuan untuk mengambil data atau dokumen yang ada di komputer. 2) *Data Forgery*, kejahatan ini terkait dengan pemalsuan data atau dokumen. 3) *Data Theft*, kejahatan terkait pencurian data untuk digunakan sendiri atau diberikan pada pihak lain. 4) *Data Leakage*, kejahatan yang terkait kebocoran data keluar organisasi. 5) *Data Diddling*, suatu kejahatan dengan mengubah data valid atau sah dengan cara yang tidak sah. 6) *Misuse of Devices*, kejahatan dengan menyalahgunakan peralatan komputer secara seluruh atau sebagian sistem komputer dengan tujuan digunakan untuk melakukan akses tidak sah, intersepsi tidak sah, mengganggu data atau sistem komputer, atau melakukan perbuatan-perbuatan melawan hukum lain (Jahankhani, 2014).

Terdapat beberapa kategori kejahatan *cybercrime* berdasarkan hubungan komputer dengan kejahatan, yaitu; 1) Komputer sebagai target; 2) Komputer sebagai instrumen kejahatan; 3) Komputer atas kejadian kejahatan lain; 4) Kejahatan terkait dengan prevalensi komputer (Jahankhani et al., 2014). Menurut hasil riset CyberEdge Group yang dipublikasikan dalam laporannya *"2018 Cyberthreat Defense Report"* frekuensi serangan komputer yang berhasil dalam 12 bulan terakhir, seperti pada Gambar 1. (CyberEdge, 2018)



Gambar 1. Frekuensi Serangan Komputer 12 Bulan Terakhir

Kejahatan komputer memiliki bukti elektronik dan digital dari tindak kejahatan berupa jejak aktivitas kejahatannya dan perlu dilakukan analisa terhadap bukti digital yang didapatkan dengan ilmu dan metode forensik. Pada bidang teknologi, analisa forensik terhadap barang bukti digital atau elektronik disebut dengan sebutan komputer forensik atau *digital forensics* (Ridho, Yudhana, & Riadi, 2016). Digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum *(pro justice)*, yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi atau komputer *crime* secara ilmiah hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan (Firdonsyah, Riadi, & Sunardi, 2016). Sehingga digital forensik itu sendiri merupakan tindakan memperoleh, mengambil, melestarikan, dan menyajikan data sesuai dengan metode, langkah kerja forensik, dan tool forensik.

Akuisisi bukti digital secara langsung pada sistem yang sedang berjalan dikenal dengan istilah *live forensic* (Faiz, Umar, & Yudhana, 2017), *live forensics* bertujuan untuk mendapatkan informasi dari data yang hanya ada ketika sistem sedang berjalan misalnya aktivitas *RAM Memory*, *Network Process*, *Swap File*, *Running System Process*, dan *Log System* (Ahmad, Riadi, & Prayudi, 2017). Sedangkan akuisisi pada perangkat yang tidak aktif atau dalam kondisi tidak berjalan *(off)*, dikenal dengan istilah *static forensic* (Imam Riadi, Umar, & Nasrulloh, 2018a), pada umumnya digunakan untuk akuisisi media penyimpanan komputer berjenis *non-volatile memory* misalnya *Harddisk, Solid State Drive (SSD), Flashdisk, Memory Card, Zip Drive, Optical Drive, dan Nand Flash* (Riadi & Nasrulloh, 2018b).

Penelitian yang pernah dilakukan dalam proses forensik dengan menggunakan metode *live* dilakukan oleh (Umar, Yudhana, & Faiz, 2018) dengan mengakuisisi proses *RAM* untuk melihat keamanan *Web Browser*. Penelitian dengan metode serupa juga dilakukan oleh (Mazdadi, Riadi, & Luthfi, 2017)

melakukan akuisisi pada sistem operasi pada *router* yang sedang berjalan dengan menggunakan metode *live forensic*. Pada forensik dengan menggunakan metode *static* dilakukan (Riadi, Umar & Nasrulloh, 2018) melakukan akuisisi pada *SSD* yang dilakukan pembekuan *(frozen SSD)* dan (Prayogo, Riadi, & Luthfi, 2017) menggunakan metode *static* untuk forensik pada perangkat *mobile*.

Bagaimana jika terjadi kejahatan komputer dan proses analisis forensik pada media penyimpanan komputer berjenis *non-volatile memory* dilakukan secara *live forensik*, pada penelitian ini dilakukan analisis forensik pada *Solid State Drive* dengan menggunakan *framework Grr Rapid Response*. *Framework* tersebut merupakan kerangka kerja dalam memberikan tanggapan terhadap insiden yang difokuskan pada forensik jarak jauh dan dilakukan secara langsung (Umar, Riadi, & Sugandi, 2017).

2. METODOLOGI PENELITIAN

Langkah kerja forensik pada penelitian ini mengimplementasikan langkah kerja forensik dari *National Institute of Standards Technology (NIST)* (Riadi, Sunardi, & Firdonsyah, 2017). Langkah kerja ini untuk menjelaskan bagaimana tahapan-tahapan forensik yang akan dilakukan sehingga dapat diketahui alur penelitian secara sistematis, sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada. Menurut (Putra, Fadlil, & Riadi, 2017) disebutkan melakukan teknik forensik dan analisa forensik berdasarkan metode yang benar akan memiliki keberhasilan hampir seluruhnya dalam mengumpulkan data forensik. Langkah forensik pada penelitian ini dapat digambarkan seperti pada Gambar 2.

Gambar 2. *National Institute of Standards Technology (NIST)*

1) Tahap Collection

Tahap pengumpulan merupakan serangkaian kegiatan mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan untuk menjaga integritas barang bukti dari perubahan.

2) Tahap Examination

Tahap pemeriksaan ini merupakan tahap pemeriksaan data yang dikumpulkan secara forensik baik secara otomatis atau manual, serta memastikan bahwa data yang didapat berupa file tersebut asli sesuai dengan yang didapat pada tempat kejadian kejahatan komputer, untuk itu pada file digital perlu dilakukan identifikasi.

3) Tahap Analysis

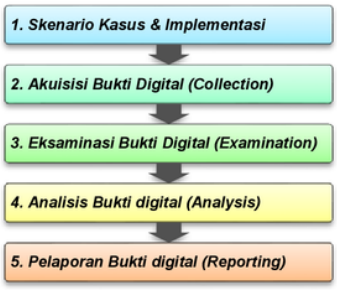
Tahap meneliti ini dilakukan setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail dan komprehensif dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut. Hasil analisis terhadap data digital selanjutnya disebut digunakan sebagai barang bukti digital serta dapat dipertanggungjawabkan secara ilmiah dan secara hukum.

4) Tahap Reporting

Tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai tool, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan aspek pendukung lainnya pada proses tindakan digital forensik.

Metode akuisisi yang digunakan pada akuisisi forensik menggunakan metode *live forensics*, dengan mengimplementasikan *framework Grr Rapid Response*. *Framework* tersebut untuk memberikan tanggapan terhadap insiden forensik digital yang difokuskan pada lingkungan forensik jarak jauh. *Framework* ini berbasis arsitektur *client server*, ada agen yang terpasang pada sistem target dan sebuah infrastruktur server Python yang bisa mengatur dan berkomunikasi dengan agen (Cruz, Moser, & Cohen, 2015).

Bukti digital yang didapatkan tidak pada lingkungan yang sebenarnya atau barang bukti tidak didapatkan dari hasil tindak kejahatan komputer yang sebenarnya, melainkan bukti digital dibuat dan peroleh dari hasil skenario pada tahap skenario kasus dan implementasi. Adapun tahapan forensik yang dilalui pada penelitian ini mengacu pada 4 (empat) tahap dari *NIST*. Dari metode dan langkah kerja tersebut pada penelitian ini dibagi menjadi 5 (lima) tahapan penelitian, seperti pada Gambar 3.



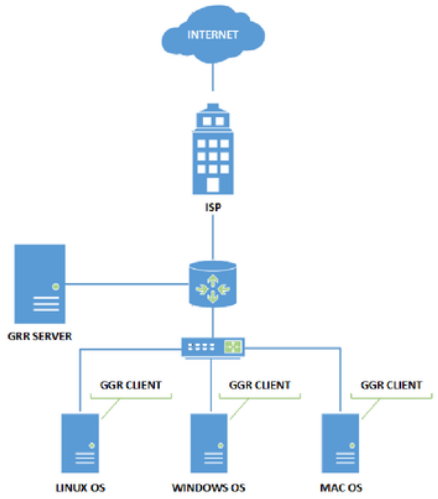
Gambar 2. Tahapan Penelitian

3. HASIL DAN PEMBAHASAN

Penelitian ini mengimplementasikan metode *live forensics* dan langkah kerja forensik dari *NIST*, dengan mensimulasikan kasus, untuk didapatkannya barang bukti digital dari media penyimpanan *Solid State Drive (SSD)* secara *live forensics* menggunakan *framework Grr Rapid Response*.

3.1. Skenario Kasus dan Implementasi

Kasus kejahatan pada penelitian ini dilakukan dengan berdasarkan skenario kasus, dengan tujuan untuk mensimulasikan kasus kejahatan komputer yang sebenarnya dan didapatkan barang bukti seperti pada kasus yang sebenarnya. Kasus yang diskenariokan pada penelitian ini adalah kasus kehilangan data *(lost data)* pada suatu organisasi, maka perlu adanya penanganan forensik. Penanganan forensik dilakukan dengan penanganan jarak jauh. Data atau file yang diujicobakan pada penelitian ini berupa *file* dokumen.



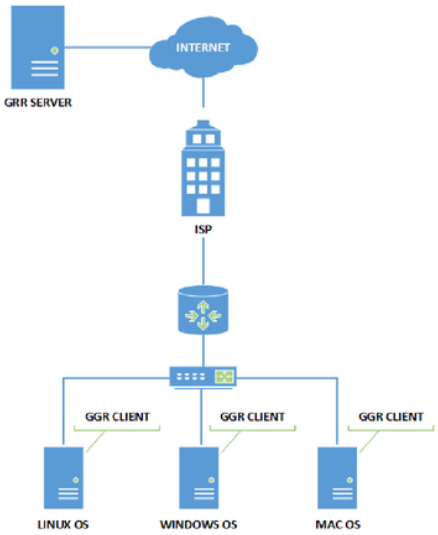
Gambar 3. Topologi *Grr Rapid Response* Didalam Organisasi

Perangkat implementasi *Grr Rapid Response* berupa alat dan bahan yang diperlukan dalam penelitian diantaranya:

Tabel 1. Alat dan Bahan Implementasi *Grr Rapid Response*

No	Alat dan Bahan	Keterangan
1	SSD 256 SSD	Samsung 850 PRO
2	Intel i7, Ram 32 GB, 256 SSD	Komputer Server
3	Intel i3, Ram 8 GB, 256 SDD	Komputer Client
4	openSUSE Leap 15.0	OS Server
5	Windows 10 Pro	OS Client
6	Ubuntu 18.04	OS Client
7	Mikrotik CCR 1016-12S	Router
8	Mikrotik CRS CAS125-24G	Switch Manageble
9	Cisco Catalyst 2960	Switch

Arsitektur *Grr Rapid Response* bersifat *client server* sehingga untuk menjalankannya diperlukan komponen jaringan minimal ada *server* dan *client*. Pada sisi server digunakan untuk menempatkan *Worker, Frontend,* dan *Admin UI,* pada sisi *client* untuk menjalankan *Service Grr Rapid Response* (Reichert, Richards, & Yoshigoe, 2015). Pada sebuah organisasi *Grr Rapid Response* dapat terapkan pada berbagi topologi jaringan, baik secara *Interior* maupun *Exterior*. Pada *Interior Gateway Protokol* berjalan di dalam *Autonomous System*, sedangkan *Exterior Gateway Protokol* berjalan diantara *Autonomous System* (Muliandri, & Trisnawan, 2019). Pada sebuah organisai dapat diilustrasikan seperti pada Gambar 3 dan Gambar 4.



Gambar 4. Topologi *Grr Rapid Response* Diluar Organisasi

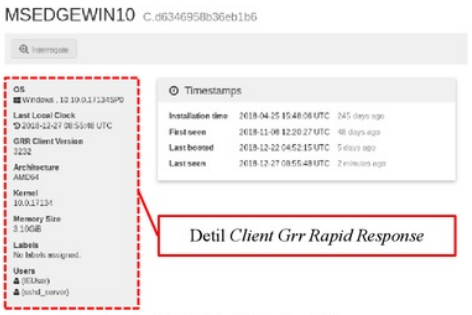
3.2. Akuisisi Bukti Digital *(Collection)*

Tahap awal untuk mendapatkan barang bukti dilakukan dengan mengkoneksikan *Client Grr Rapid Response* dengan *Grr Rapid Response Server* melalui perangkat lunak agen *(client)* ditempatkan. Untuk menghubungkan keduanya dapat melalui *IP Address, Domain Name,* atau *MAC Address*. Pada *server Grr Rapid Response* akan terdeteksi *host* yang terhubung. *Client* dapat berupa *Workstation* atau *Server*. Host yang aktif dan terdeteksi pada *server Grr Rapid Response* ditandai dengan status *online* warna hijau, seperti pada Gambar 5. Pada bagian tersebut jika dibuka akan menampilkan profil secara detil *client* dari *Grr Rapid Response* seperti ditampilkan pada Gambar 6.

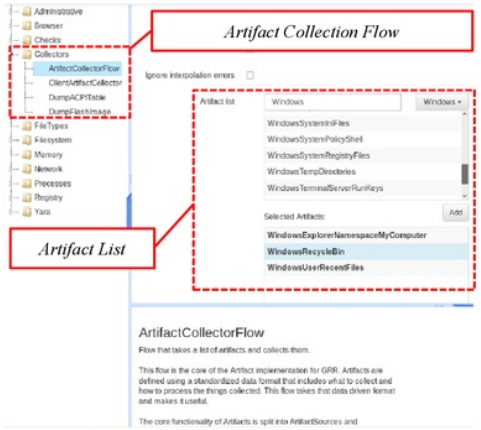
Setelah *server* dan *client Grr Rapid Response* saling terhubung, tahap selanjutnya yaitu proses pengumpulan atau koleksi barang bukti. Pada *Grr Rapid Response* dikenal istilah *Flows* yaitu mengirimkan *request* dan *response* pada agen atau *client*, dan istilah *Result* yaitu tanggapan *client* atau

agen *Grr Rapid Response* atas *Flows* dari *server Grr Rapid Response*. Pengumpulan barang bukti dilakukan dengan cara mengakuisisi dengan metode *live forensics* melalui *Grr Rapid Response.* Akuisisi dilakukan dengan menggunakan fitur *Collection* pada *Grr Rapid Response.* Proses ini seorang administrator *(system administrator)* membuat *Artifact list. Artifact list* merupakan pesan yang akan dikirim ke *client*. Pesan tersebut berisi instruksi untuk *client* agar menjalankan aksi tertentu dan memberikan hasilnya ke *server*. Aksi *client* ini merupakan sejumlah kode program komputer yang dapat dimengerti oleh agen sehingga dapat menjalankan aksi yang diinginkan, contohnya seperti mendapatkan daftar *file* di dalam sebuah direktori atau membaca *buffer* sebuah *file*.

Gambar 5. Host yang Terhubung pada *Grr Rapid Response*

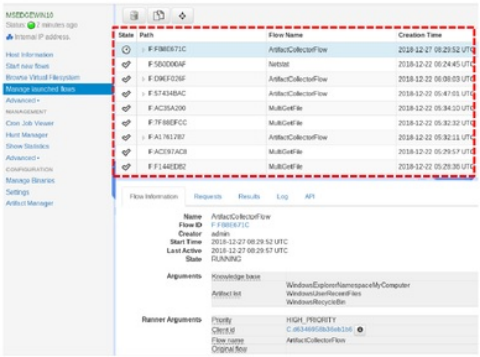


Gambar 6. Detail Client *Grr Rapid Response*



Gambar 7. *Artifact list Grr Rapid Response*

Penelitian ini sesuai dengan rancangan awal skenario kasus yaitu data yang hilang *(lost data)*, kemudian membaca *file* yang pernah ada dan mengembalikan *file* tersebut dari media simpan *Solid Sate Drive (SSD)* pada sistem operasi Windows 10 Pro. *Artifact list* yang digunakan adalah *Windows ExplorerNamespaceMyComputer, WindowsRecycleBin,* dan *WindowsUserRecentFiles.* Melalui *WindowsExplorerNamespaceMyComputer* artefak yang akan dikumpulkan berupa daftar *file* yang ada pada direktori *My Computer*, melalui *WindowsRecycleBin* artefak yang akan dikumpulkan berupa daftar *file* yang ada dan pernah dihapus dari direktori *RecycleBin,* dan *WindowsUserRecentFiles* artefak yang akan dikumpulkan berupa daftar *file* yang terakhir dibuka oleh *user,* seperti pada Gambar 7. Proses selanjutnya menjalankan *Artifact list*, proses yang berjalan seperti pada Gambar 8.



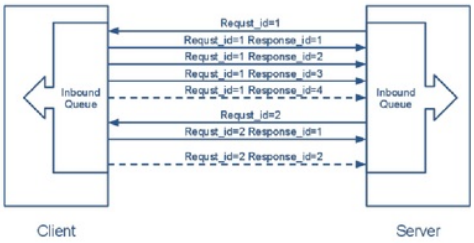
Gambar 8. *Artifact Collection Flow* sedang Berjalan

Akuisisi dilakukan dari sisi *server* melalui apa yang disebut sebuah *flow*. *Flow* merupakan bagian dari kode di sisi *server* yang memberikan instruksi ke sistem *Grr Rapid Response* untuk menjalankan dan menjadwalkan panggilan jarak jauh ke *client* dan memiliki beberapa logika tambahan sehingga dapat memutuskan apa yang dilakukan berdasarkan hasil panggilan dari kode tersebut.

Pada media komunikasi data pesan yang dikirim dan diterima di antara *client* dan server *Grr Rapid Response*, pesan yang dikirim dari server ke *client*

disebut dengan *request* dan pesan yang dikirim dari *client* ke *server* disebut dengan *response*. *Request* yang dikirim ke *client* berisi instruksi ke *client* untuk melakukan beberapa aksi. Aksi seperti ini disebut dengan aksi *client*. Sebuah *request* tunggal bisa jadi menghasilkan banyak *response*, diilustrasikan pada Gambar 8.

Saat *server* mengirim pesan ke *client* pesan akan ditandai pada penyimpanan data dengan waktu sewa tertentu *(lease time)*. Jika *client* tidak membalas permintaan dalam rentang waktu tertentu, *request* tersebut akan dimunculkan kembali bersama dengan waktu sewanya. Skenario *Grr Rapid Response* ini dirancang untuk kasus *client* yang dilakukan *reboot* atau *restart*, dan kehilangan konektivitas jaringan komputer saat proses pengiriman *request* berlangsung, maka *request* akan dikirim kembali dan aksi *client* ke *server* dijalankan kembali (Cruz et al., 2015).

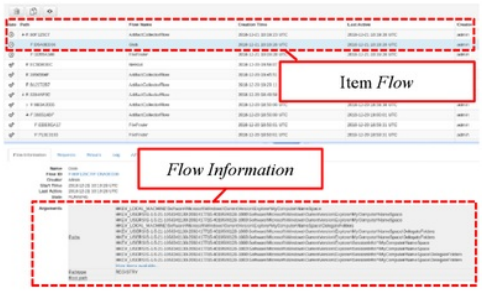


Gambar 8. *Request* dan *Response Grr Rapid Response*

3.3. Eksaminasi Bukti Digital *(Examination)*

Setelah dilakukan akuisisi maka tahap berikutnya yaitu proses eksaminasi. Proses pengujian ini untuk mengetahui sebesar mana *Grr Rapid Response* dapat bekerja dengan optimal terhadap *request* yang diminta atau *flows* yang dijalankan, sehingga didapatkan hasil yang optimal dalam menemukan artefak digital yang dibutuhkan. Dari akuisisi yang dikirim *client Grr Rapid Response* ke *server* melalui komponen *FrontEnd*, maka selanjutnya komponen *Worker* menjalankan tugas analisis forensik yaitu dengan menyimpan hasil akusisi ke dalam *data storage* atau penyimpanan *Grr Rapid Response* dan menampilkan kembali ke halaman *AdminUI*.

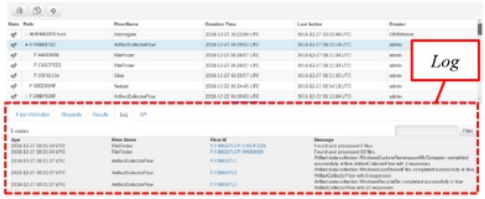
Pada bagian *Manage Launched Flows* menampilkan hasil kerja dari *flows* atau kode yang dijalankan, untuk melihat hasil ditampilkan dalam bentuk *Flow Information*, didalamnya memuat informasi *Request* yang dikirim oleh *server*, informasi *Log*, dan informasi lainnya. Pada tahap ini didapatkan berupa informasi terhadap *path* atau direktori yang dapat diakses oleh *Grr Rapid Response*. Pada penelitian ini *request* dari ketiga *flows* yaitu *WindowsExplorerNamespaceMy Computer, WindowsRecycleBin,* dan *WindowsUser RecentFiles* dapat diakses oleh *Grr Rapid Response*, seperti pada Gambar 9.



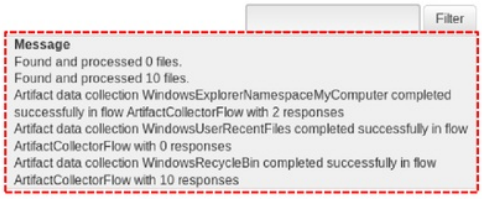
Gambar 9. *Path* atau Direktori yang Berhasil Diakses

3.4. Analisis Bukti Digital *(Analysis)*

Tahap ini menampilan analisis terhadap hasil akuisisi berkas pada *WindowsExplorerNamespace MyComputer, WindowsRecycleBin,* dan *Windows UserRecentFiles*. Pada bagian *log* dan *results* semua informasi akuisisi yang dijalankan pada *client Grr Rapid Response* ditampilkan secara rinci diantaranya *TimeStamp*, *Payload*, *Path*, *Flow Id,* dan identitas artefak digital yang ditemukan yang digunakan untuk mendapatkan bukti digital yang diharapkan. Hasil pada *log Grr Rapid Response* yang ditampilkan memberikan informasi didapatkan 10 Artefak Digital dari hasil kode perintah *WindowsRecycleBin* seperti pada Gambar 10 dan Gambar 11.

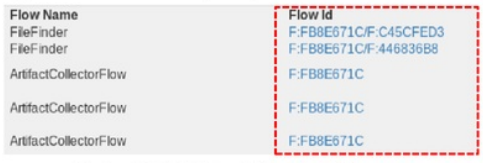


Gambar 10. *Log Grr Rapid Response*



Gambar 11. Detil *Log Grr Rapid Response*

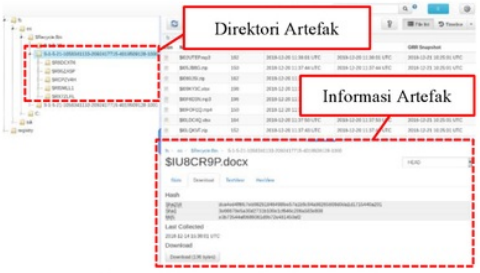
Hasil informasi tersebut tersebut didapatkan juga *Flow Id. Flow Id* merupakan kode unik yang diberikan *Grr Rapid Response* ketika perintah *flow* dijalankan. *Flow Id* seperti pada Gambar 12.



Flow Name	Flow Id
FileFinder	F:FB8E671C/F:C45CFED3
FileFinder	F:FB8E671C/F:446836B8
ArtifactCollectorFlow	F:FB8E671C
ArtifactCollectorFlow	F:FB8E671C
ArtifactCollectorFlow	F:FB8E671C

Gambar 12. Detil *Flow Id Grr Rapid Response*

Melalui *Flow Id* yang didapatkan maka dapat dilakukan penelusuran artefak melalui *Flow Id* tersebut. *Flow Id* pada *Grr Rapid Response* akan merujuk pada *path* atau direktori *data storage* pada *Grr Rapid Response* yang dibuat dan menyimpan secara otomatis hasil akuisisi pada *client*. *Flow Id* dengan kode unik F:FB8E671C ketika dibuka maka akan merujuk pada direktori *VirtualFileSystem* pada *Grr Rapid Response* seperti pada Gambar 13.

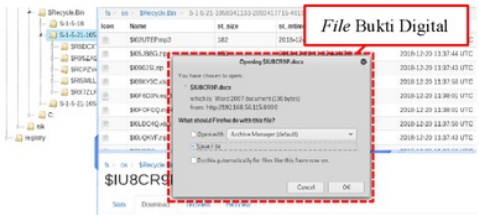


Gambar 13. *Path* atau Direktori Artefak

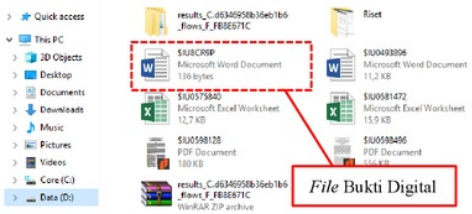
dari *Flow Id* dan informasi log maka didapatkan artefak digital $IU8CR9P.docx dengan informasi ukuran file artefak tersebut 136 *byte* yang diperoleh dari *VirtualFileSystem* pada direktori *$Recycle Bin*. Artefak digital yang didapatkan seperti pada Gambar 14 dan didapatkan pula informasi nilai *hash* pada *file* tersebut.

Gambar 14. Artefak Digital dan Nilai Hash

Hasil eksaminasi dan analisis yang dilakukan maka didapatkan artefak digital yang kemudian artefak tersebut dilakukan restorasi menggunakan fitur unduhan pada *Grr Rapid Response* dari *VirtualFileSystem*, didapatkan bukti digital berupa *file* dokumen dengan ekstensi *docx* dengan ukuran *file* 136 *byte*, bukti digital hasil restorasi seperti pada Gambar 15 dan Gambar 16.



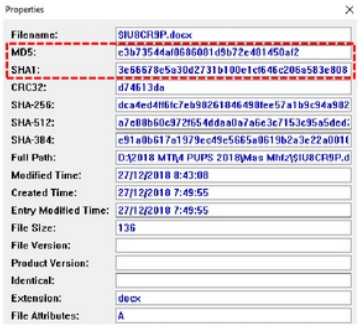
Gambar 15. Bukti Digital yang Didapatkan



Gambar 16. Bukti Digital yang Dikembalikan

Bukti digital pada proses forensik perlu dilakukan proses verifikasi dan validasi untuk mendapatkan bukti digital yang valid. Verifikasi dan validasi dilakukan berdasarkan nilai *hash* yang didapatkan pada *log* artefak digital pada *Grr Rapid Response* dengan bukti digital yang berhasil dikembalikan.

Gambar 17. Nilai *Hash* Artefak Digital



Gambar 18. Nilai *Hash* Bukti Digital

Bukti digital dilakukan verifikasi dan validasi dengan menggunakan perangkat lunak hashing HashMyFile, hasil yang didapatkan artefak dan bukti digital memiliki nilai *hash* yang sama, pada Gambar 17 menunjukkan nilai *hash* dari artefak yang didapatkan melalui *Grr Rapid Response* dan Gambar 18 menunjukkan nilai *hash* dari bukti digital yang dilakukan proses *hashing*.

3.5. Pelaporan Bukti Digital *(Reporting)*

Tahap pelaporan *(reporting)* merupakan tahap ke-4 pada langkah kerja forensik *NIST*, tahap ini merupakan tahap akhir dari langkah kerja forensik. Tahap pelaporan berisi tentang deskripsi kasus yang sedang dilakukan proses forensik, tindakan terhadap barang bukti yang didapatkan, metode dan langkah kerja forensik yang digunakan, *tool* forensik yang digunakan, teknik verifikasi dan validasi yang

dilakukan, serta aspek penunjang lainnya yang diperlukan pada proses forensik digital. Pada bagian pelaporan meliputi deskripsi barang bukti, langkah kerja forensik yang dilakukan, tool forensik yang digunakan, dan hasil bukti digital yang didapatkan.

Informasi bukti fisik yang akan dilaporkan. berupa barang bukti elektronik *Workstation* pada sebuah perusahaan, dengan spesifikasi Processor Intel i3 3 Ghz, 8 GB *RAM*, 256 *SSD* terkoneksi sebagai *client Grr Rapid Response*. Kasus yang sedang ditangani dalam proses forensik adalah kasus kehilangan data *(lost data)* pada suatu organisasi, data atau file yang dilakukan pencarian berupa *file* dokumen. Maka perlu adanya penanganan forensik. Tool yang digunakn *Grr Rapid Response*, penanganan forensik dilakukan dengan penanganan jarak jauh dengan metode *live forensik*.

Bukti digital yang didapatkan berdasarkan eksaminasi, restorasi, dan validasi berhasil menjawab tujuan dari proses forensik yang dilakukan, hasil pemeriksaan sebagai berikut:

1) Ditemukan informasi terkait artefak bukti digital.
2) Hasil analisis dari proses eksaminasi terdapat artefak *file* dokumen.
3) Hasil analisis dari proses eksaminasi adanya indikasi file tersebut dihapus dan kemudian masuk pada direktori *Recycle Bin* dan kemudian dikosongkan.
4) Hasil restorasi menunjukan adanya bukti digital yang dikembalikan berupa *file* dokumen dengan ekstensi *docx*.
5) Hasil validasi pada bukti digital menunjukan nilai *hash* yang sama pada artefak digital.

4. KESIMPULAN

Berdasarkan hasil analisis forensik *Solid State Drive (SSD)* menggunakan *framework Grr Rapid Response* yang telah dilakukan memberikan kesimpulan sebagai berikut;

1) Langkah kerja forensik dari *National Institute of Standars Technology (NIST)* dapat diimplementasikan pada proses pengambilan bukti digital dengan metode *live forensik* dan dilakukan secara jarak jauh dengan menggunakan *framework Grr Rapid Response.*
2) Kemampuan tool forensik pada proses eksaminasi, restorasi, dan analisis menggunakan *framework Grr Rapid Response* yang dilakukan pada *Solid State Drive (SSD)* pada *Workstation (client Grr)* berhasil mengembalikan bukti digital.
3) Artefak digital dan bukti digital yang dapat dikembalikan berupa *file* dokumen dengan nama $IU8CR9P.docx memiliki ukuran file 136 *byte*.
4) Hasil validasi menunjukan artefak bukti digital yang didapatkan dengan bukti digital hasil restorasi memiliki nilai *hash* yang sama, dengan nilai *hash* MD5 e3b73544af0686081d9b72e481450af2 dan nilai *hash* SHA1 3e66678e5a30d2731b100e1cf646c206a583e808, maka dapat dikatakan bukti digital tersebut identik atau sama.

DAFTAR PUSTAKA

Ahma M. S., Riadi, I., & Prayudi, Y. (2017). Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Serangan Man in the Middle Attack Berbasis Evil Twin. *ILKOM nal Ilmiah*, *9*(April), 1–8. Retrieved from http://jurnal.fikom.umi.ac.id/index.php/ILKOM/article/view/103/60

Cruz, F., Moser, A., & Cohen, M. (2015). A scalable file based data store for forensic analysis. *ital Investigation*, *12*(S1), S90–S101. https://doi.org/10.1016/j.diin.2015.01.016

CyberEdge. (2018). *2018 Cyberthreat Defense Report. CyberEdge Group*. Retrieved from https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf

Faiz, M. N., Umar, R., & Yudhana, A. (2017). Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email. *JISKa*, *1*(February), 108–114. https://doi.org/10.14421/jiska.2017.13-02

Firdonsyah, A., Riadi, I., & Sunardi. (2016). Analisis Forensik Bukti Digital Blackberry Messenger Pada Android. *Seminar Nasional Click Karawang*, 25–29.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). *Cybercrime classification and characteristics. Cyber Crime and yber Terrorism Investigator's Handbook*. Elsevier Inc. https://doi.org/10.1016/B978-0-12-800743-3.00012-8

Mazdadi, M. I., Riadi, I., & Luthfi, A. (2017). Live Forensics on RouterOS using API Services to Investigate Network Attacks. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(2), 406–410.

Mulia i, E., Trisnawan, P. H., & Amron, K. (2019). Analisis Perbandingan Kinerja Routing Protokol IS-IS dengan Routing Protokol EIGRP dalam Dynamic Routing, *3*(2), 9221–9228.

Prayogo, A., Riadi, I., & Luthfi, A. (2017). Mobile Forensics Development of Mobile Banking Application using Static Forensic. *International Journal of Computer Applications*, *160*(1), 5–10. https://doi.org/10.5120/ijca2017912925

Putra, R. A., Fadlil, A., & Riadi, I. (2017). Forensik Mobile Pada Smartwach Berbasis Android. *Jurti*, *1*(1), 41–47. https://doi.org/25798790

Reichert, Z., Richards, K., & Yoshigoe, K. (2015). Automated forensic data acquisition in the cloud. *Proceedings - 11th IEEE International Conference on Mobile Ad Hoc and sor Systems, MASS 2014*, 725–730. https://doi.org/10.1109/MASS.2014.135

Riadi, I., Sunardi;, & Firdonsyah, A. (2017). Forensic Investigation Technique on Androids Blackberry Messenger using NIST Framework. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *16*(4), 198–205. https://doi.org/10.17781/P002306

Riadi, I., Umar, R., & Nasrulloh, I. (2018a). Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods, *9*(3), 169–181.

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018b). Analisis Forensik Digital Pada Frozen Slod State Drive Dengan Metode National Institute of Justice (Nij), *3*(May), 70–82. https://doi.org/10.21831/elinvo.v3i1.19308

Ridho, F., Yudhana, A., & Riadi, I. (2016). Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time, *2*(1), 111–116. Retrieved from http://ars.ilkom.unsri.ac.id

Umar, R., Riadi, I., & Sugandi, A. (2017). Investigasi Bukti Digital Pada File Dokumen menggunakan framework GRR Rapid Response. *Semantikom 2017 UNIRA*, 1–6.

Umar, R., Yudhana, A., & Faiz, M. N. (2018). Experimental Analysis of Web Browser Sessions using Live Forensics Method. *International Journal of Electrical and Computer Engineering (IJECE)*, *8*(5), 2951–2958. https://doi.org/10.11591/ijece.v8i5.pp.2951-2958

JTIIK ID 1516

ORIGINALITY REPORT

21%	21%	4%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	10%
2	www.scribd.com Internet Source	2%
3	kemajuanteknolo.blogspot.com Internet Source	1%
4	eprints.umm.ac.id Internet Source	1%
5	jutisi.maranatha.edu Internet Source	1%
6	scholar.uad.ac.id Internet Source	1%
7	bimarioeza.blogspot.com Internet Source	1%
8	"Proceedings of Sixth International Conference on Soft Computing for Problem Solving", Springer Nature, 2017 Publication	1%

9	journals.aserspublishing.eu Internet Source	<1%
10	www.jatit.org Internet Source	<1%
11	www.vaadata.com Internet Source	<1%
12	www.iaescore.com Internet Source	<1%
13	"Digital Forensics and Cyber Crime", Springer Nature, 2018 Publication	<1%
14	doaj.org Internet Source	<1%
15	j-ptiik.ub.ac.id Internet Source	<1%
16	tel.archives-ouvertes.fr Internet Source	<1%
17	ariefhari.wordpress.com Internet Source	<1%
18	waesearch.kobv.de Internet Source	<1%
19	dblp.dagstuhl.de Internet Source	<1%

20	sentrin.filkom.ub.ac.id Internet Source	<1%
21	digilib.uin-suka.ac.id Internet Source	<1%
22	docobook.com Internet Source	<1%
23	jurnal.umk.ac.id Internet Source	<1%
24	rezkijurunk.blogspot.com Internet Source	<1%
25	www.cased.de Internet Source	<1%
26	"The GENI Book", Springer Nature, 2016 Publication	<1%
27	Jason Farina, Mark Scanlon, Nhien-An Le-Khac, M-Tahar Kechadi. "Overview of the Forensic Investigation of Cloud Services", 2015 10th International Conference on Availability, Reliability and Security, 2015 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		