Analisis Forensik Solid State Drive (SSD) Menggunakan Framework Rapid Response

By Sunardi Sunardi

WORD COUNT 5302
TIME SUBMITTED 19-OCT-2019 11:06AM
PAPER ID 51319086

Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)
Vol. 6, No. 5, Oktober 2019, hlm. 509-518
Akreditasi KEMENRISTEKDIKTI, No. 30/E/KPT/2018

DOI: 10.25126/jtiik.201961516
p-ISSN: 2355-7699
e-ISSN: 2528-6579

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

Sunardi[1], Imam Riadi[2], Imam Mahfudl Nasrulloh[3]

[1]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, [2]Program Studi Sistem Informasi, Universitas Ahmad Dahlan , [3]Program Studi Magister Teknik Informatika Universitas Ahmad Dahlan
Email: [1]sunardi@mti.uad.ac.id, [2]imam.riadi@si.uad.ac.id [3]imam1707048016@webmail.uad.ac.id

(Naskah masuk: 31 Desember 2018, diterima untuk diterbitkan: 02 Oktober 2019)

Abstrak

Teknologi komputer pada empat tahun terahir ini mengalami perkembangan yang pesat. Bersamaan dengan itu juga berdampak negatif salah satunya adalah berupa kejahatan komputer. Kejahatan komputer akan meninggalkan jejak aktivitas kejahatan, maka perlu dilakukan analisa dengan ilmu dan metode forensik untuk mendapatkan barang bukti. Bagaimana jika terjadi kejahatan komputer pada media penyimpanan komputer berjenis *non-volatile memory* dan dilakukan secara *live* forensik. 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,* bukti digital dapat ditemukan dan dikembalikan. Bukti digital yang dapat dikembalikan berupa *file* dokumen, dan hasil validasi pada bukti digital tersebut memiliki nilai *hash* yang sama dari dua algoritma validasi bukti digital yang diimplementasikan, MD5 dan SHA-1. Sehingga hasil integritas dari dokumen tersebut menunjukkan bahwa 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 in the last four years has experienced rapid development. At the same time, it also has a negative impact, one of which is a computer crime. Computer crime will leave traces of criminal activity, so it is necessary to analyze with forensic science and methods to obtain evidence. 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 with 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 evidence can be found and returned. Digital evidence that can be returned is a document file, and the results of the validation of digital evidence have the same hash value from the two digital proof validation algorithms implemented, MD5 and SHA-1. So the results of the integrity of the document so that the digital evidence is identical.

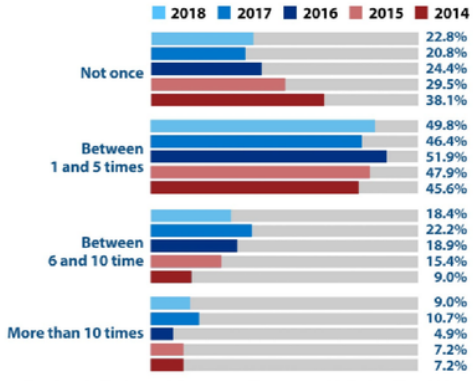
Keywords: *Analysis, Forensics, SSD, Grr Rapid Response*

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).



Gambar 1. Frekuensi Serangan Komputer 12 Bulan Terakhir

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).

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 Forensik (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, Ria & 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* forensik (Faiz, Umar, & Yudhana, 2017), *live* forensik 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* forensik 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, Umar, & Nasrulloh, 2018).

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* forensik. 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. Analisis forensik secara *live* forensik dapat 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).

Solid State Drive (SSD) merupakan salah satu media penyimpanan komputer selain *Harddisk*. Teknologi *SSD* menggunakan *solid state memory* berbasis *NAND memory* untuk penyimpanan datanya, *SSD* menggunakan teknologi yang hampir mirip seperti *Random Access Memory (RAM)*. Pada media penyimpanan *SSD* sistem penamannya menggunakan teknologi semikonduktor, sedangkan pada *Harddisk* menggunakan *platter* magnetis yang berputar (Silberschatz, Galvin, & Gagne, 2013). Pada *SSD* hanya terdapat komponen elektronik seperti *Intergrated Circuit (IC), Micro Chip* dan komponen elektronik pendukung lainnya seperti kapasitor. Semua proses pembacaan dan penulisan data dilakukan secara elektrik sama seperti proses yang terjadi pada *Flashdisk* dan *RAM* (Geier, 2015). Pada *SSD juga* tidak terjadi fragmentasi seperti pada *Harddisk* karena data tersimpan pada *chip flash*, maka pemrosesan data pada *SSD* jauh lebih cepat dan lebih hemat energi dibanding *Harddisk*.

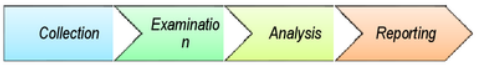
Grr Rapid Response merupakan *framework respons insiden* yang fokus pada forensik secara langsung dan jarak jauh. *Framework* tersebut untuk memberikan tanggapan terhadap insiden forensik digital yang difokuskan pada lingkungan forensik jarak jauh. *Framework* ini berbasis arsitektur *client server*, ada agen yang terpasang pada sistem target dan sebuah infrastruktur server Python yang bisa mengatur dan berkomunikasi dengan agen (Cruz & Moser, 2015). Tujuan dari *Grr Rapid Response* adalah untuk mendukung aktivitas forensik dan investigasi dalam waktu yang cepat, berskala, sehingga dapat dilakukan analisis dan triase terhadap serangan yang ada dan menganalisisnya dari jarak jauh (Acharya, Glenn, & Carr, 2015). *Grr Rapid Response* terdiri dari 2 bagian *Client Grr* sebagai agen dan *Server Grr*.

Client Grr ditempatkan pada sistem-sistem yang ingin diinvestigasi. Pada sistem tersebut perangkat lunak agen *Grr* ditempatkan. *Client GRR* secara periodik akan melakukan *request* pada server *frontend Grr* untuk menjalankan sebuah aksi tertentu berupa *flows*. Server *Grr* merupakan infrastruktur yang terdiri dari komponen *Frontend, Worker, Server UI* dengan antarmuka berbasis *Web,* dan sebuah *endpoint Application Programming Interface (API)* yang memungkinkan investigator forensik untuk dapat menjadwalkan aksi-aksi yang ingin dijalankan oleh *client Grr* untuk menampilkan dan melakukan pemrosesan terhadap artefak digital yang dikumpulkan (Rasheed, Hadi, & Khader, 2017). *Grr* dapat bekerja secara berskala sehingga investigator forensik dapat secara efektif melakukan akuisisi dan pemrosesan data yang berasal dari banyak komputer atau *client Grr*.

Penelitian ini dilakukan pengambilan bukti digital dengan skenario kasus dan implementasi pada sebuah organisasi jaringan komputer, bukti digital yang dicari dan dikembalikan berupa *file* dokumen pada media penyimpanan komputer *non-volatile memory* yaitu *Solid State Drive (SSD)*, pengambilan bukti digital atau akuisisi dilakukan dengan metode *live* forensik, dengan cara forensik jarak jauh menggunakan *framework Grr Rapid Response,* dan menerapkan standar langkah kerja forensik untuk penanganan bukti digital dari *National Institute of Standards Technology (NIST)* untuk mendapatkan bukti-bukti digital yang valid dan dapat dipertanggungjawabkan.

2. METODOLOGI PENELITIAN

Obyek forensik, *tool* forensik, dan langkah kerja forensik merupakan bagian penting dari proses investigasi forensik. Dalam pemilihan model, metode, atau langkah kerja forensik diantaranya harus memenuhi *individuality, repeatability, reliability, performance, testability, scalability*, dan *quality standards* (Agarwal, Gupta, & Gupta, 2011). 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, dan dapat dijadikan acuan 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 *(collection)* merupakan proses identifikasi, pelabelan, pendokumentasian, dan pengambilan data dan informasi dari sumber data yang relevan. Selain pengumpulan barang bukti juga untuk menjaga validitas dan integritas data, sehingga dilakukan proses pengamanan barang bukti *(isolation)* dan membuat salinan dari barang bukti atau akuisisi *(acquisition)*.

2) Tahap *Examination*

Tahap *examination* (pemeriksaan) yaitu tahap pemilahan dan pemeriksaan artefak digital yang didapatkan dengan proses secara manual atau otomatis, serta memastikan bahwa artefak tersebut benar. Pada artefak digital misalnya dilakukan identifikasi dan validasi berdasarkan

nama *file,* jenis *file*, nilai *hash* yang sesuai dengan bukti digital yang akan dicari.

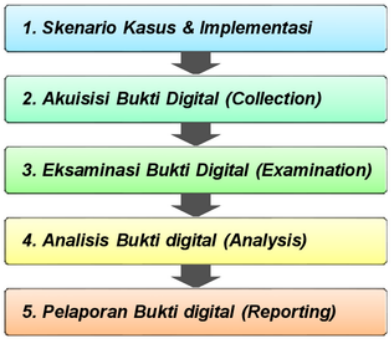
3) Tahap *Analysis*

Tahap *analysis* (meneliti) ini dilakukan setelah mendapatkan artefak digital dari proses pemeriksaan sebelumnya. Artefak digital tersebut selanjutnya dilakukan analisis secara mendalam dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan artefak digital tersebut. Hasil analisis terhadap artefak digital selanjutnya disebut sebagai barang bukti digital yang dapat dipertanggungjawabkan secara ilmiah dan hukum.

4) Tahap *Reporting*

Tahap *reporting* (pelaporan) dilakukan setelah barang bukti digital diperoleh dari proses pemeriksaan dan analisis artefak digital. Pada tahap ini meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai *tool*, metode yang digunakan, penentuan tindakan pendukung yang dilakukan atau aspek lainnya yang mendukung pada proses tindakan digital forensik (Riadi, Umar, & Firdonsyah, 2017).

Metode akuisisi yang digunakan pada akuisisi forensik menggunakan metode *live* forensik, dengan mengimplementasikan *framework Grr Rapid Response*. Bukti digital yang didapatkan tidak pada kasus yang sebenarnya dan barang bukti tidak didapatkan dari hasil kejahatan komputer yang sebenarnya, bukti digital dibuat dan peroleh dari hasil skenario pada tahap skenario kasus dan implementasi. Adapun tahapan forensik pada penelitian ini mengacu pada 4 (empat) tahap standar langkah kerja forensik dari *NIST*. Dari metode dan langkah kerja tersebut pada penelitian ini dibagi menjadi 5 (lima) tahapan penelitian, seperti pada Gambar 3.



Gambar 3. Tahapan Penelitian

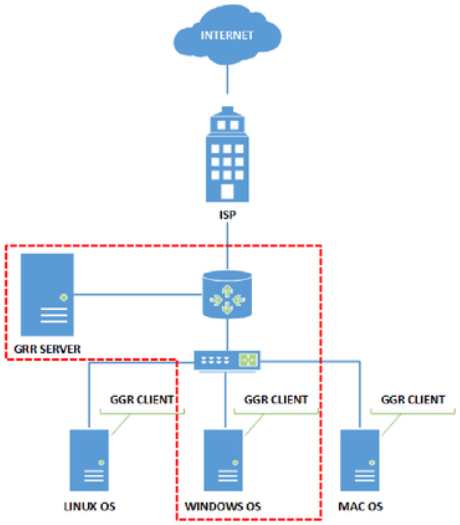
3. HASIL DAN PEMBAHASAN

Penelitian ini mengimplementasikan metode *live* forensik jarak jauh dan langkah kerja forensik dari *NIST,* dengan mensimulasikan kasus, untuk didapatkannya barang bukti digital dari media penyimpanan *Solid State Drive (SSD)* secara *live* forensik dengan menggunakan *framework Grr Rapid Response*. Adapun hasil dan pembahasan pada setiap tahapan sebagai berikut:

3.1. Skenario Kasus dan Implementasi

Kasus kejahatan pada penelitian ini dilakukan dengan berdasarkan skenario kasus, dengan tujuan untuk mensimulasikan kasus kejahatan komputer dan didapatkan bukti digital seperti pada kasus yang sebenarnya. Kasus yang diskenariokan pada penelitian ini adalah kasus kehilangan data *(lost data)* yang dihapus oleh oknum pada suatu *Workstation* di organisasi tersebut. Maka untuk mengetahui, mencari, dan mengembalikannya perlu adanya penanganan forensik digital. Penanganan forensik dilakukan dengan penanganan jarak jauh, dengan kata lain dilakukan terpisah dari komputer *(server)* yang berbeda. Data atau *file* yang diujicobakan pada penelitian ini berupa *file* dokumen.

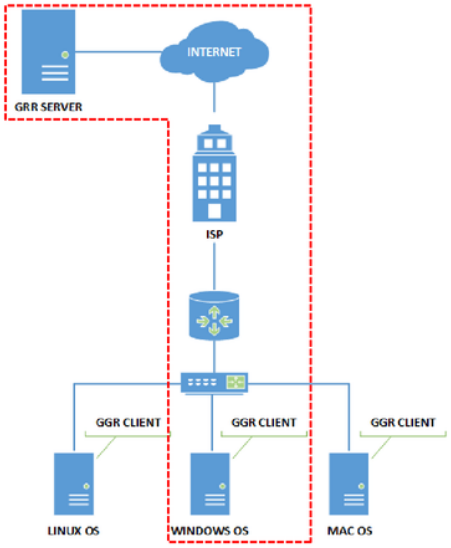
Pada sebuah organisasi *Grr Rapid Response* dapat terapkan pada berbagi topologi jaringan, baik secara *Interior* maupun *Exterior*. Pada *Interior Gateway Protokol* berjalan di dalam *Autonomous System*, sedangkan *Exterior Gateway Protokol* berjalan diantara *Autonomous System* (Muliandri, & Trisnawan, 2019). Pada sebuah organisai topologi jaringan dapat diilustrasikan seperti pada Gambar 4 dan Gambar 5.



Gambar 4. Topologi *Grr Rapid Response* Didalam Organisasi

Arsitektur *Grr Rapid Response* bersifat *client server* sehingga untuk menjalankannya diperlukan komponen jaringan minimal terdapat *server* dan *client,* serta dapat dilakukan pada jaringan luas. Pada sisi server digunakan untuk menempatkan *Worker, Frontend,* dan *Admin UI,* pada sisi *client* untuk menjalankan perangkat lunak agen yaitu *Service Grr*

Rapid Response (Reichert, Richards, & Yoshigoe, 2015).



Gambar 5. Topologi *Grr Rapid Response* Diluar Organisasi

Gambar 4 menunjukkan *framework Grr Rapid Response* bekerja pada lingkungan jaringan *Local Area Network (LAN)* atau didalam organisasi dalam skenario tersebut melibatkan *Client Grr* berupa *Workstation* dengan media penyimpanan komputer *Solid State Drive (SSD)* yang berjalan pada sistem operasi *Windows 10 Pro* dan *Server Grr* yang berjalan pada sistem operasi *openSUSE Leap 15.0*. Pada proses forensik jarak jauh dengan metode *live* forensik untuk mendapatkan barang bukti dilakukan dengan mengkoneksikan *Grr Rapid Response Client* dengan *Grr Rapid Response Server* melalui perangkat lunak agen *(client)* yang ditempatkan dan keduanya dihubungkan melalui *IP Address Local Area*, *Domain Name,* atau *MAC Address*. Implementasi *framework Grr Rapid Response* juga dapat diimplementasikan diluar organisasi atau pada lingkungan jaringan *Wide Area Network (WAN)* dan *Internet* seperti Gambar 5, untuk menghubungkan *Grr client* dengan *Grr server* dapat melalui *IP Public* atau *Domain*.

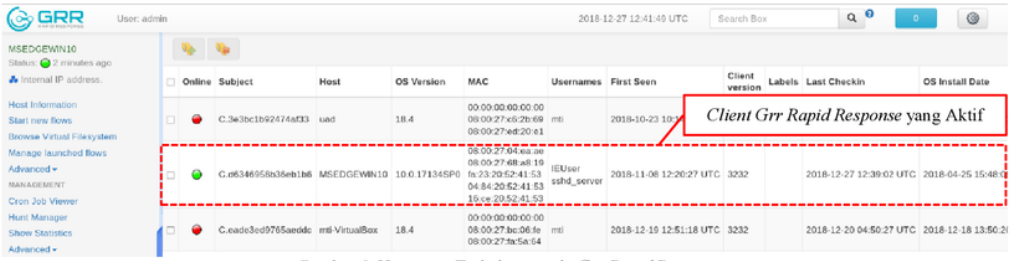
Perangkat implementasi *Grr Rapid Response* berupa alat dan bahan yang diperlukan dalam penelitian ini diantaranya seperti pada Tabel 1.

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

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

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*. Pada server *Grr Rapid Response* akan terdeteksi *host* yang terhubung. *Client* dapat berupa *Workstation* atau *Server*. Host yang aktif akan terdeteksi pada *server Grr Rapid Response* ditandai dengan status *online* warna hijau, seperti pada Gambar 6.

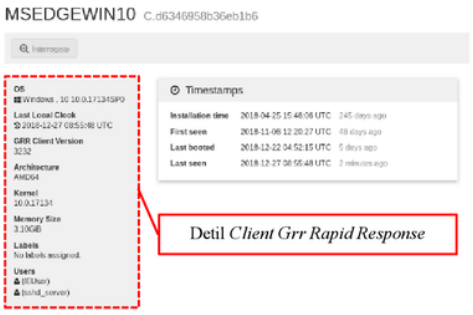


Gambar 6. Host yang Terhubung pada *Grr Rapid Response*

Pada bagian tersebut secara lengkap menampilkan profil *client* dari *Grr Rapid Response* seperti pada Gambar 7. 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*.

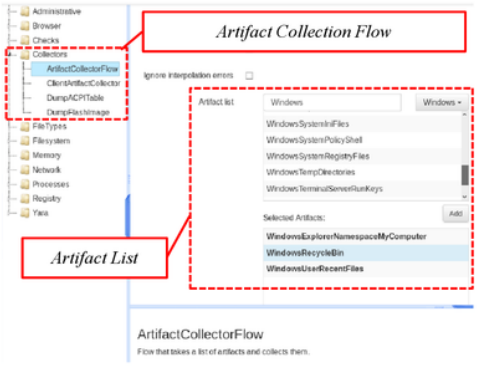
Pengumpulan barang bukti dilakukan dengan cara mengakuisisi dengan metode *live* forensik melalui *Grr Rapid Response*. Akuisisi dilakukan dengan menggunakan fitur *Collection* pada *Grr Rapid Response*. Proses ini seorang administrator *(system administrator)* membuat *Artifact list*. *Artifact list* 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*.



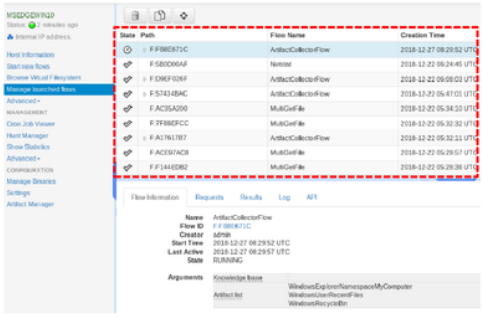
Gambar 7. Detail Client *Grr Rapid Response*

Penelitian ini sesuai dengan rancangan awal skenario kasus yaitu adanya data yang hilang *(lost data)*, kemudian dilakukan pengumpulan informasi terkait *file* yang pernah ada dan kemudian mengembalikan *file* tersebut dari *Client Grr* berupa *Workstation* dengan media penyimpanan komputer *SSD* yang berjalan pada sistem operasi *Windows 10 Pro*. *Artifact list* yang digunakan pada *framework Grr Rapid Response* diantaranya *Windows Explorer Namespace MyComputer, Windows RecycleBin,* dan *Windows User Recent Files.* Melalui *Windows Explorer Namespace My Computer* artefak yang akan dikumpulkan berupa daftar *file* yang ada pada direktori *MyComputer*, melalui *Windows RecycleBin* artefak yang akan dikumpulkan berupa daftar *file* yang ada dan pernah dihapus dari direktori *RecycleBin,* dan melalui *WindowsUserRecentFiles* artefak yang akan dikumpulkan berupa daftar *file* yang terakhir dibuka oleh *user,* seperti Gambar 8.



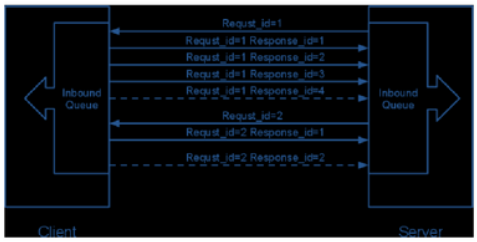
Gambar 8. *Artifact list Grr Rapid Response*

Akuisisi dilakukan dari sisi *server* melalui proses yang disebut *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. Proses selanjutnya menjalankan *Artifact list* berupa perintah *flow*, proses yang berjalan seperti pada Gambar 9.



Gambar 9. *Artifact Collection Flow* sedang Berjalan

Pada proses 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 10.



Gambar 10. *Request* dan *Response Grr Rapid Response*

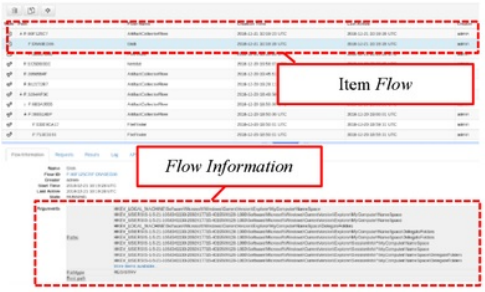
Saat *server* mengirim pesan ke *client* pesan akan ditandai pada penyimpanan data dengan waktu sewa tertentu *(lease time)*. Jika *client* tidak membalas permintaan dalam rentang waktu tertentu, *request* tersebut akan dimunculkan kembali bersama dengan waktu sewanya. Skenario *Grr Rapid Response* ini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

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* 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*.

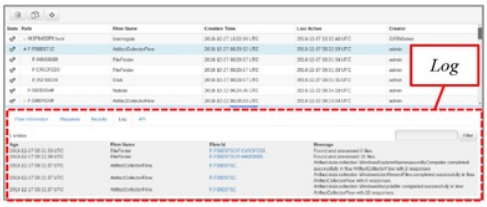
Pada bagian *Manage Launched Flows* menampilkan hasil kerja dari *flows* atau kode yang dijalankan, untuk melihat hasil ditampilkan dalam bentuk *Flow Information*, didalamnya memuat informasi *Request* yang dikirim oleh *server*, informasi *Log*, dan informasi lainnya. Pada tahap ini didapatkan berupa 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 11.



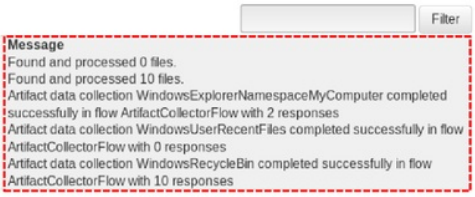
Gambar 11. *Path* atau Direktori yang Berhasil Diakses

3.4. Analisis Bukti Digital *(Analysis)*

Tahap ini menampilan analisis terhadap hasil akuisisi berkas pada *Windows Explorer Namespace MyComputer, Windows Recycle Bin,* dan *Windows User Recent Files*. Pada bagian *log* dan *results* semua informasi akuisisi yang dijalankan pada *client Grr Rapid Response* ditampilkan secara rinci diantaranya *Time Stamp*, *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 *Windows Recycle Bin* seperti pada Gambar 11 dan Gambar 12. 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 13.



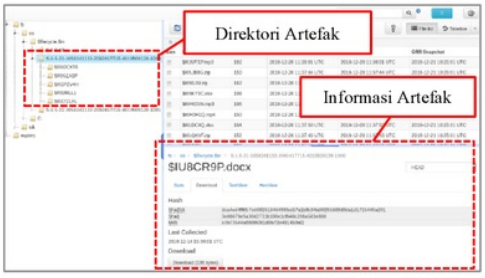
Gambar 11. *Log Grr Rapid Response*



Gambar 12. Detil *Log Grr Rapid Response*

Gambar 13. *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 *Virtual File System* pada *Grr Rapid Response* seperti pada Gambar 14.

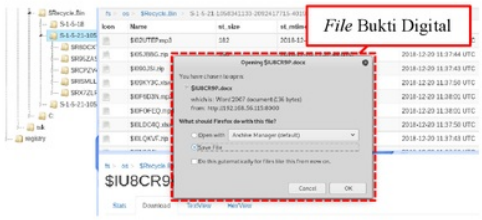


Gambar 14. *Path* atau Direktori Artefak

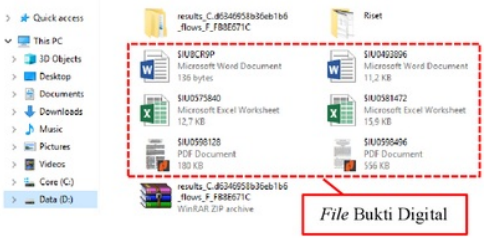
Pada direktori *Virtual File System* didapatkan beberapa artefak digital dengan ukuran file artefak bervariasi, dan didapatkan informasi bahwa artefak tersebut berasal dari direktori aslinya yaitu *Recycle Bin* yang sudah dikosongkan. Artefak digital yang didapatkan secara detil dapat dilihat melalui *Admin UI Grr*, dan pada *log* artefak juga didapatkan informasi nilai *hash* pada artefak tersebut seperti pada Gambar 15.

Gambar 15. Artefak Digital dan Nilai Hash

Hasil dari proses eksaminasi dan analisis yang dilakukan maka didapatkan artefak digital yang kemudian artefak tersebut dilakukan pengambilan bukti digital dengan menggunakan fitur unduhan pada *Admin UI Grr Rapid Response*. Bukti digital didapatkan dari *Flow Id* F:FB8E671C pada direktori *VirtualFile System*, hasil unduhan berupa beberapa *file* dokumen. Proses pengambilan bukti digital seperti pada Gambar 16 dan Gambar 17.



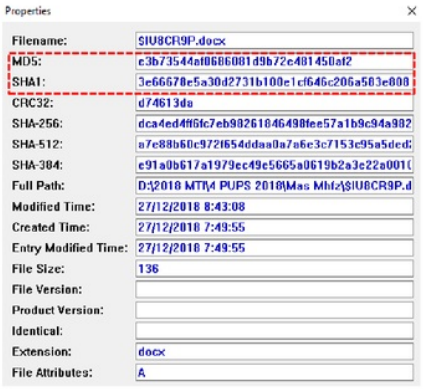
Gambar 16. Bukti Digital yang Didapatkan



Gambar 17. 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. Bukti digital dilakukan verifikasi dan validasi dengan menggunakan perangkat lunak *hashing HashMyFile*.

Gambar 18. Contoh Nilai *Hash* pada Artefak Digital



Gambar 19. Contoh Nilai *Hash* pada Bukti Digital

Pada Gambar 18 menunjukkan nilai *hash* dari artefak yang didapatkan melalui *Grr Rapid Response*. Gambar 19 menunjukkan nilai *hash* dari bukti digital yang dilakukan proses *hashing*. Setelah dilakukan komparasi didapatkan nilai *hash* keduannya memiliki nilai *hash* yang sama.

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 barang bukti fisik yang 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 untuk mengembalikan bukti digital tersebut. Tindakan forensik dilakukan dengan penanganan forensik jarak jauh menggunakan *framework Grr Rapid Response* dengan metode *live* forensik.

Bukti digital yang didapatkan pada proses eksaminasi dan validasi berhasil menjawab tujuan dari proses forensik yang dilakukan, dengan hasil sebagai berikut:

1) Proses akuisisi dilakukan dengan *framework Grr Rapid Response* secara *live* forensik jarak jauh dan ditemukan informasi terkait artefak bukti digital.

2) Hasil proses eksaminasi ditemukan artefak *file* dokumen yang hilang *(lost data)* berdasarkan informasi artefak digital pada *Admin UI* dan *Log Grr Rapid Response*.
3) Hasil analisis terdapat adanya dugaan file tersebut dihapus dan kemudian masuk pada direktori *Recycle Bin* dan kemudian dikosongkan, berdasarkan informasi pada *Log Grr Rapid Response*.
4) Hasil pengembalian bukti digital menunjukan adanya bukti digital berupa *file* dokumen, seperti pada Tabel 2.
5) Validasi dilakukan pada bukti digital dengan perangkat lunak hashing *HashMyFile*, proses ditunjukkan pada Gambar 18 dan Gambar 19.
6) Hasil validasi menunjukan nilai *hash* yang sama pada artefak digital dan bukti digital, seperti pada Tabel 2.

Tabel 2. Bukti Digital yang Didapatkan dan Valid

No	*File* Bukti Digital	Ukuran *File (byte)*	Nilai *Hash*	
			MD5	SHA-1
1	$IU8CR9P.docx	136	e3b73544af0686081d9b72e481450af2	3e66678e5a30d2731b100e1cf646c206a583e808
2	$IU0493896.docx	11.555	534379bc93d7ec318890355c45e18f2a	05667b66186740433f5ad791771ebec769ae1b0c
3	$IU0575840.xlsx	13.101	71c6f8181fcb01ea752fc8ffcb11a5b6	68788db2a42d669dd90f25398bd61cccb1c8a2e1
4	$IU0581472.xlsx	16.353	31514f08b4ccf357fc0c1c855060a03f	303277d22fbfc80509bc331c9f8f1dff8f589187
5	$IU0598128.pdf	184.728	4d1518c91c53da625ae800cfdd06ff90	b3cb1fcd91ec3f2d92a5db6e4cd880c22e1ac5e0
6	$IU0598496.pdf	569.810	b4791406338db847ae817c5e1bf3e58e	a59578a3f80d6fc0dec3fa3392f19851123e8255

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 penanganan forensik secara jarak jauh dengan menggunakan *framework Grr Rapid Response*.
2) Kemampuan *framework Grr Rapid Response* pada proses eksaminasi, analisis, dan pengembalian bukti digital yang dilakukan pada media penyimpanan komputer *Solid State Drive (SSD)* pada *Workstation (client Grr)* berhasil mengembalikan bukti digital.
3) Bukti digital yang dapat dikembalikan berupa *file* dokumen
4) Hasil validasi pada bukti digital tersebut memiliki nilai *hash* yang sama dari dua algoritma validasi bukti digital yang diimplementasikan, MD5 dan SHA-1. Sehingga hasil integritas dari dokumen tersebut menunjukkan bahwa bukti digital tersebut identik.

Pada penelitian selanjutnya dapat menggunakan langkah kerja forensik yang berbeda pada penelitian ini. Langkah kerja lain yang dapat digunakan *National Institute of Justice (NIJ), Digital Forensic Research Work Shop (DFRWS)*, *Association of Chief Police Officers (ACPO)*, atau langkah forensik terstandar lainnya. Dan penelitian lebih lanjut dapat dilakukan analisa forensik menggunakan *framework Grr Rapid Response* pada obyek forensik lainnya seperti *Random Access Memory (RAM), Server Log,* atau dengan segmentasi yang lebih besar yaitu pada *Cloud Computing* dan *Data Center*.

DAFTAR PUSTAKA

ACHARYA, S., GLENN, W., & CARR, M. (2015). A GRReat framework for incident response in healthcare. *Proceedings - 2015 IEEE International Conference on Bioinformatics and Biomedicine, BIBM 2015*, 776–778. Tersedia melalui: https://ieeexplore.ieee.org/document/7359784

AGARWAL, A., GUPTA, M., & GUPTA, S. (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118–131.

AHMAD, 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 Jurnal Ilmiah*, *9*(4), 1–8. Tersedia melalui: http://jurnal.fikom.umi.ac.id/index.php/ILKOM/article/view/103/60 [Diakses 15 Oktober 2018]

CRUZ, F., MOSER, A., & COHEN, M. (2015). A scalable file based data store for forensic analysis. *Digital Investigation*, *12*(1), 90–101.

CYBEREDGE. (2018). *2018 Cyberthreat Defense Report*. *CyberEdge Group*. Tersedia melalui: https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf [Diakses 23 Desember 2018]

FAIZ, M. N., UMAR, R., & YUDHANA, A. (2017). Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email. *JISKa*, *1*(2), 108–114.

FIRDONSYAH, A., RIADI, I., & SUNARDI. (2016). Analisis Forensik Bukti Digital Blackberry Messenger Pada Android. *CLICK 2016, STMIK Pamitran*, *1*(1), 25–29.

GEIER, F. (2015). *The Differences Between SSD and HDD Technology Regarding Forensic Investigations*. Linnaeus University Sweden. Tersedia melalui: http://lnu.diva-portal.org/smash/get/diva2:824922/FULLTEXT01.pdf [Diakses 24 November 2018]

JAHANKHANI, H., AL-NEMRAT, A., & HOSSEINIAN-FAR, A. (2014). *Cybercrime classification and characteristics*. *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Elsevier Inc.

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.

MULIANDRI, E., TRISNAWAN, P. H., & AMRON, K. (2019). Analisis Perbandingan Kinerja Routing Protokol IS-IS dengan Routing Protokol EIGRP dalam Dynamic Routing. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer (JPTIIK)*, *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.

PUTRA, R. A., FADLIL, A., & RIADI, I. (2017). Forensik Mobile Pada Smartwach Berbasis Android. *Jurnal Rekayasa Teknologi Informasi (JURTI)*, *1*(1), 41–47.

RASHEED, H., HADI, A., & KHADER, M. (2017). Threat Hunting Using GRR Rapid Response. In *2017 International Conference on New Trends in Computing Sciences (ICTCS), IEEE* 2018, 155–160 Tersedia melalui: https://ieeexplore.ieee.org/document/8250281

REICHERT, Z., RICHARDS, K., & YOSHIGOE, K. (2015). Automated forensic data acquisition in the cloud. *Proceedings - 11th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2014*, 725–730.

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.

RIADI, I., UMAR, R., & FIRDONSYAH, A. (2017). Identification of Digital Evidence on Android's Blackberry Messenger Using NIST Mobile Forensic Method. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(5), 155–160.

RIADI, I., UMAR, R., & NASRULLOH, I. M. (2018). Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods. *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, *9*(3), 169-181.

RIDHO, F., YUDHANA, A., & RIADI, I. (2016). Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time, *Prosiding - Annual Research Seminar, ARS 2016 UNSRI*, *2*(1), 111–116. Tersedia melalui: http://ars.ilkom.unsri.ac.id [Diakses 7 September 2018]

SILBERSCHATZ, A., GALVIN, P. B., & GAGNE, G. (2013). *Operating System Concepts*. (Beth Lang Golub, Ed.) (9th ed.). United States of America: John Wiley & Sons, Inc.

UMAR, R., RIADI, I., & SUGANDI, A. (2017). Investigasi Bukti Digital Pada File Dokumen menggunakan framework GRR Rapid Response. *Prosiding - Seminar Nasional Teknologi Informasi dan Komunikasi, SEMANTIKOM 2017 UNIRA*, 1–6. Tersedia melalui: https://semantikom.unira.ac.id/2017/ [Diakses 27 Oktober 2018]

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.

Analisis Forensik Solid State Drive (SSD) Menggunakan Framework Rapid Response

ORIGINALITY REPORT

21%

SIMILARITY INDEX

MATCHED SOURCE

1	www.researchgate.net Internet	317 words — 6%

★www.researchgate.net
Internet
6%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	ON		