Monitoring Log Aplikasi *Mobile Native* Menggunakan *Framework* Grr Rapid Response

Imam Riadi[1], Sunardi[2], Ahmad Azhar Kadim[3]

[1]Program Studi Sistem Informasi, Fakultas Matematika dan Ilmu Pengetahuan Alam
[2]Program Studi Teknik Elektro, Fakultas Teknologi Industri
[3]Program Studi Teknik Informatika, Fakultas Teknologi Industri
Universitas Ahmad Dahlan, Yogyakarta, Indonesia
Jln. Prof. Dr. Soepomo S.H, Warungboto, Umbulharjo, Kota Yogyakarta, Indonesia
Email: [1] imam.riadi@is.uad.ac.id, [2]sunardi@mti.uad.ac.id,
[3]ahmad1707048007@webmail.uad.ac.id

Masuk: 17 Januari 2019; Direvisi: 22 Februari 2019; Diterima: 23 Februari 2019

Abstract.
In order to acquire the data in the security investigation process comprehensively, respondents need to take general information that uses logs, configured services, cron tasks, patch statuses, and user accounts. This information are known as forensic artifacts. The location and format are varied by system. One manifestation of forensic artifacts that is frequently investigated is files. A Quick Response Grr Framework has been created to describe forensic artifacts that allow data collected and conditioned to quickly use forensics directly on the original mobile application log using Laravel. Retrieving forensic evidence uses the NIST method which has steps such as acquisition, examination, analysis and report. This research produces log files from the laravel framework and detailed activity information from users when accessing the server. The results for which the log is obtained will become evident to be the material of the report.
Keywords: *Grr, Forensic, Framework, Laravel*

Abstrak. *Agar akuisisi data pada proses investigasi keamanan dapat dilakukan secara komprehensif, responden perlu mengambil informasi umum yang mencakup log, layanan terkonfigurasi, tugas cron, status patch, dan akun pengguna. Informasi-informasi ini dikenal sebagai artefak forensik. Lokasi dan formatnya bervariasi di setiap sistem. Salah satu manifestasi dari artefak forensik yang sering diinvestigasi oleh para praktisi adalah file. Framework Grr Rapid Response telah membangun kerangka kerja untuk mendeskripsikan artefak forensik yang memungkinkan data yang diperlukan dapat dikumpulkan dan dikondisikan dengan cepat menggunakan live forensics pada log aplikasi mobile native menggunakan laravel. Pengambilan barang bukti forensik menggunakan metode NIST memiliki langkah-langkah seperti akuisisi, eksaminasi, analisis, dan pelaporan. Penelitian ini menghasilkan log file dari framework laravel dan informasi aktifitas detail dari user saat mengakses server. Hasil log yang diperoleh akan menjadi barang bukti untuk untuk menjadi bahan laporan.*
Kata Kunci: *Grr, Forensik, Framework, Laravel*

1. Pendahuluan

Kejahatan komputer merupakan tindak kejahatan yang jejak aktivitas kejahatannya perlu dianalisa untuk menjadi barang bukti. Pada bidang teknologi, analisa forensik terhadap barang bukti digital atau elektronik disebut dengan sebutan komputer forensik atau digital forensik. 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 kejahatan komputer hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan. Digital forensik itu sendiri

merupakan tindakan memperoleh, mengambil, melestarikan, dan menyajikan data sesuai dengan metode, langkah kerja forensik, dan *tool forensics* [1].

Forensika digital merupakan salah satu bidang yang sering dilakukan dalam penyelidikan perdata dan kriminal baik kebutuhan teknikal maupun operasional [2]. Penyelidikan digital dalam perusahaan sering kali dikaitkan dengan deteksi masalah pada sistem yang berhasil diterobos oleh pihak ketiga dan berawal dari serangan yang sudah ditargetkan sebelumnya. Penyerang memanfaatkan kelemaham pada *web server* untuk mendapatkan keuntungan pada suatu organisasi atau institusi baik milik pemerintah maupun swasta [3]. Untuk itu penyelidikan biasanya berfokus pada penilaian tanggapan dan ketepatan waktu, selain mempertahankan standar pembuktian.

Web server merupakan suatu hal yang penting dalam pengembangan sistem. Saat ini penerapan *web server* pada aplikasi *mobile* sangat dibutuhkan untuk menyimpan data atau memberikan pelayanan kepada pengguna aplikasi agar *request* yang diinginkan sesuai. Tentunya penggunaan *web server* biasanya menjadi sasaran penyerangan terutama pada aplikasi dan *server* perusahaan yang menyimpan data penting atau perbankan. Adanya digital forensik dapat membantu admin *server* untuk melakukan *monitoring* atau mendapatkan bukti kejahatan yang dilakukan.

Akuisisi bukti digital secara langsung pada sistem yang sedang berjalan dikenal dengan istilah *live forensics* [4]. *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* [5]. Sedangkan akuisisi pada perangkat yang tidak aktif atau dalam kondisi tidak berjalan *(off)*, dikenal dengan istilah *static forensic* [6]. 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* [7].

Framework yang ditawarkan untuk melakukan forensika digital secara *live* adalah Grr Rapid Response yang merupakan *framework* berbasis arsitektur *client server* dan sebuah infrastruktur *server* Phyton yang bisa mengatur dan berkomunikasi dengan agen [8]. Keunggulan dari *framework* ini adalah bisa melakukan *monitoring log* jarak jauh dengan cara *remote* sehingga dapat membantu admin untuk mengetahui aktifitas yang dilakukan oleh penyerang. Berdasarkan latar belakang yang diuraikan penelitian ini bertujuan menganalisa jejak digital yang ada pada *server* suatu aplikasi *mobile*.

2. Tinjauan Pustaka

2.1. Digital Forensik

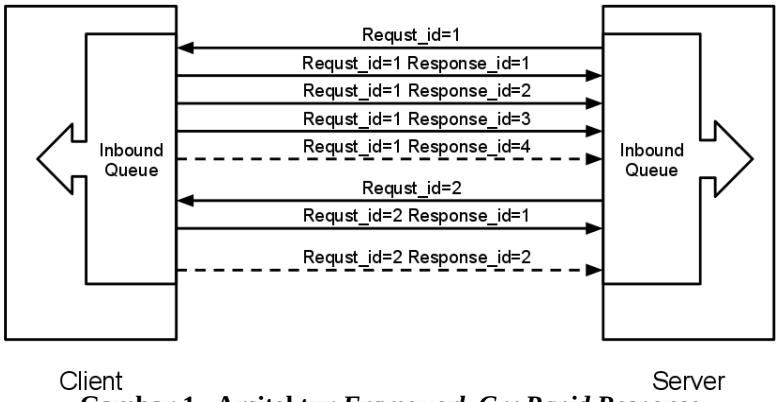
Digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (*pro justice*), yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi atau kejahatan komputer secara ilmiah hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan [2].

2.2. *Cloud Computing*

Cloud Computing merupakan suatu metode komputasi dengan memanfaatkan internet sebagai gerbang utamanya untuk mengelola piranti lunak, media penyimpanan, sampai dengan infrastruktur sebagai bentuk layanan. Penggunaan sumber daya komputasi baik *hardware* atau *software* yang disajikan sebagai layanan melalui jaringan (internet). Istilah "*cloud*" berasal karena penggunaan simbol berbentuk awan sebagai abstraksi untuk jaringan internet yang sangat luas. *Cloud computing* (komputasi awan) merupakan gabungan antara pemanfaatan teknologi komputer dengan teknologi internet. Dengan *cloud computing*, perangkat lunak yang digunakan tersimpan pada *server-server* yang diakses melalui internet sehingga seluruh *cloud services* dan *storage* dapat diakses darimana saja selama terdapat koneksi internet. Dengan kata lain perangkat lunak tersebut tidak berada pada komputer pengguna [9].

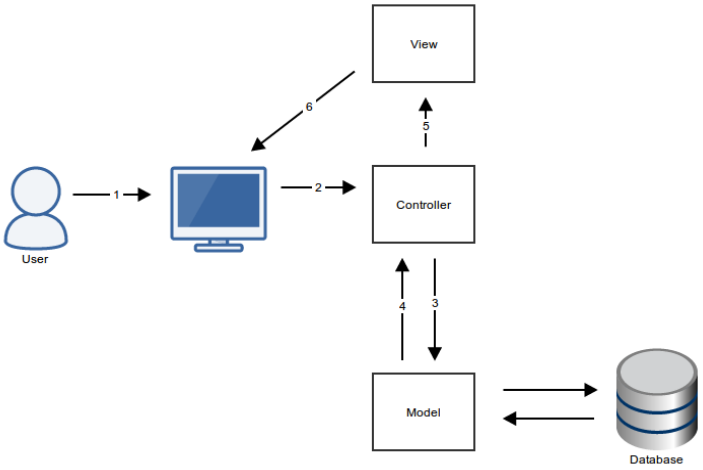
2.3. Grr *Rapid Response*

Grr Rapid Response merupakan sebuah *framework* 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 [10],. Ilustrasi *framework* dapat dilihat pada Gambar 1.



Gambar 1. Arsitektur *Framework Grr Rapid Response*

2.4. Laravel



Gambar 2. Proses Kerja Laravel (MVC)

Laravel adalah *framework open source* PHP yang ditujukan untuk pengembangan aplikasi *web* mengikuti *model-view-controller* (MVC). *View* pada laravel digunakan untuk tampilan *(interface)* dari web yang berinteraksi langsung dengan *user*, *controller* merupakan bagian yang memproses *request* dari *user*, dan *model* merupakan fungsi untuk mengakses *database* [11]. Ilustrasi seperti pada Gambar 2. Beberapa fitur dari Laravel adalah pengembangan sistem modul-modul yang dapat dimanajemen, mengenalkan cara yang berbeda untuk mengakses *database* relasional, utilitas yang membantu dalam penyebaran aplikasi, dan pemeliharaan yang mudah.

3. Metodologi Penelitian

Metode yang digunakan untuk mengumpulkan barang bukti digital adalah dengan menggunakan metode *National Institute of Standards Technology* (NIST). Berikut mekanisme yang digunakan untuk mengumpulkan barang bukti [9] seperti yang ditunjukkan oleh gambar 3.

Gambar 3. Metode Pengumpulan Barang Bukti

3.1. *Collection (Acquisition)*

Tahap ini merupakan proses koleksi, identifikasi, pelabelan, perekaman, dan pengambilan barang bukti berupa perangkat keras yang akan diambil datanya untuk digunakan sebagai bukti digital dari suatu kasus tindak kejahatan digital. Proses ini dilakukan dengan mengikuti prosedur penjagaan integritas data. Penjagaan integritas data dapat dilakukan dengan teknik isolasi barang bukti fisik dan pembuatan *backup* berupa *cloning* atau *image file* dari barang bukti fisik tersebut. Gambar 3 menunjukkan alur dari tahapan *Collection* [12].

3.2. *Examination*

Tahap ini merupakan proses pengujian dimana alur ini diharapkan dapat menguji sebesar mana Grr Rapid Response dapat bekerja dengan optimal terhadap *server* yang ada, sehingga diperoleh hasil yang optimal dalam pencarian barang bukti forensik yang dibutuhkan [13].

3.3. *Analysis*

Pada tahap ini Grr Rapid Response harus dapat mengumpulkan data aplikasi dari berbagai sumber. *Framework* Grr Rapid Response harus dapat meninjau hasil pemeriksaan sumber data aplikasi komputer target dan menentukan bagaimana informasi diperoleh, untuk melakukan analisis peristiwa secara rinci terkait aplikasi dan rekonstruksi kejadian. *Framework* Grr Rapid Response harus dapat menangani banyak situasi paling efektif dengan menganalisis sumber data objek, kemudian menghubungkan kejadian di antara objek-objek tersebut. Teknik dan proses untuk memperoleh dan memeriksa berbagai jenis sumber data secara fundamental berbeda. Banyak aplikasi memiliki data yang diambil dalam *file* data, sistem operasi, dan lalu lintas jaringan komputer [14].

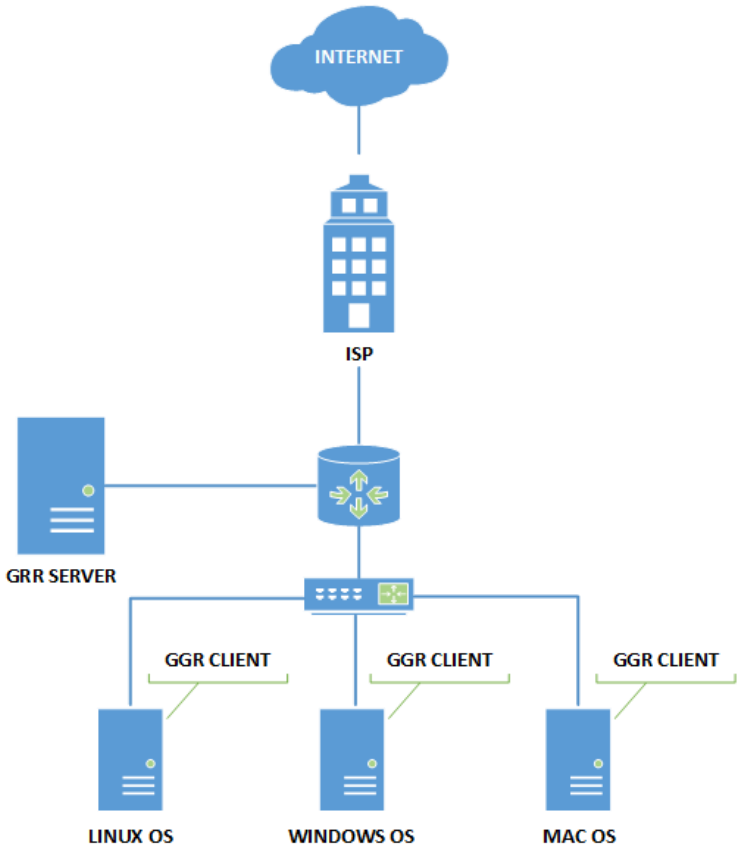
3.4. *Reporting*

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*, metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan aspek pendukung lainnya pada proses tindakan digital forensik [15].

4. Hasil dan Diskusi

4.1 Skenario Kasus dan Implementasi

Pada penelitian ini mengimplementasikan *live forensic* pada suatu *server* dari aplikasi *mobile*. Adapun skenario yang diterapkan pada penelitian ini adalah dalam bentuk simulasi kasus kejahatan perubahan data yang bisa terjadi pada *server* lengkap dengan *log* yang didapatkan sehingga menyerupai kasus sebenarnya. Kasus yang diskenariokan pada penelitian ini adalah kasus untuk mengetahui aktifitas yang mencurigakan dan perubahan data pada *server* oleh *user* yang tidak memiliki hak akses. *Framework* Grr Rapid Response digunakan untuk penanganan jarak jauh dengan tujuan mendapatkan *log* dari *server*. Ilustrasi proses Grr Rapid Response seperti pada Gambar 4.



Gambar 4. Topologi *Grr Rapid Response*

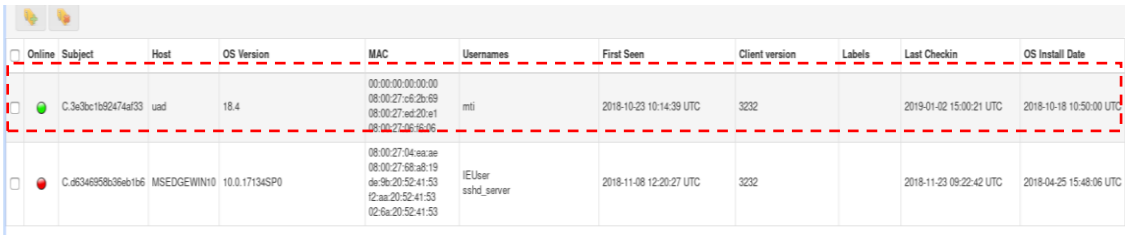
Perangkat implementasi Grr Rapid Response berupa alat dan bahan yang diperlukan dalam penelitian seperti terlihat pada Tabel 1.

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 i5, Ram 8 GB	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 Manageable*
9	Cisco Catalyst 2960	*Switch*

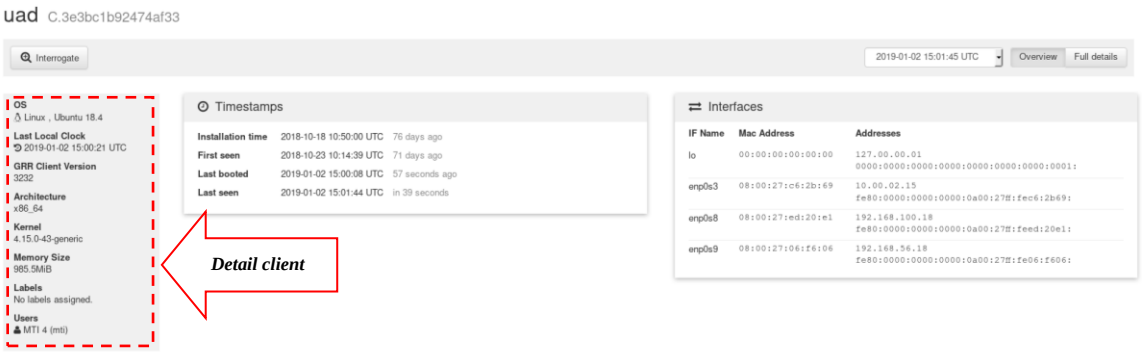
Arsitektur Grr Rapid Response bersifat *client server* sehingga untuk menjalankannya diperlukan komponen jaringan minimal ada *server* dan *client*. Pada sisi *server* digunakan untuk menempatkan *Worker*, *Frontend*, dan *Admin UI*. Pada sisi *client* untuk menjalankan *Service* Grr Rapid Response. Pada sebuah organisasi Grr Rapid Response dapat diterapkan pada berbagai topologi jaringan, baik secara *interior* maupun *exterior*. Pada *Interior Gateway Protokol* berjalan di dalam *Autonomous System*, sedangkan *Exterior Gateway Protokol* berjalan di antara *Autonomous System* [15].

4.2 Akuisisi Bukti Digital *(Collection)*



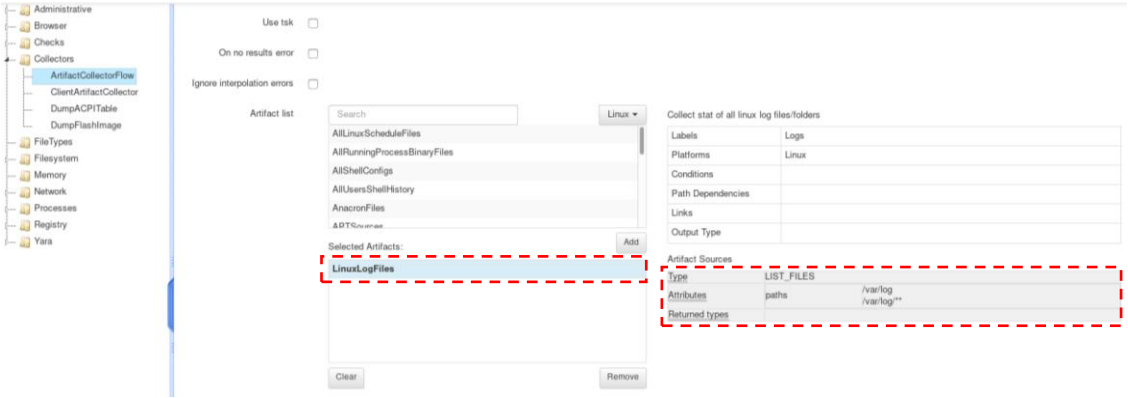
Gambar 5. *Host* yang Terhubung pada Grr Rapid Response

Grr Rapid Response bisa mendapatkan barang bukti jika antara Grr Rapid Response *client* dengan Grr Rapid Response *server* saling terhubung melalui *IP address*, *IP server* dan *IP client*. Pada Grr Rapid Response *server* akan terdeteksi *list host* yang terhubung. *Client* dapat berupa *workstation* atau *server* ditandai dengan warna hijau seperti pada Gambar 5. Detail dari *client* dapat dilihat ketika *host* yang aktif dipilih seperti pada Gambar 6.



Gambar 6. Detail *Host* Grr Rapid Response *Client*

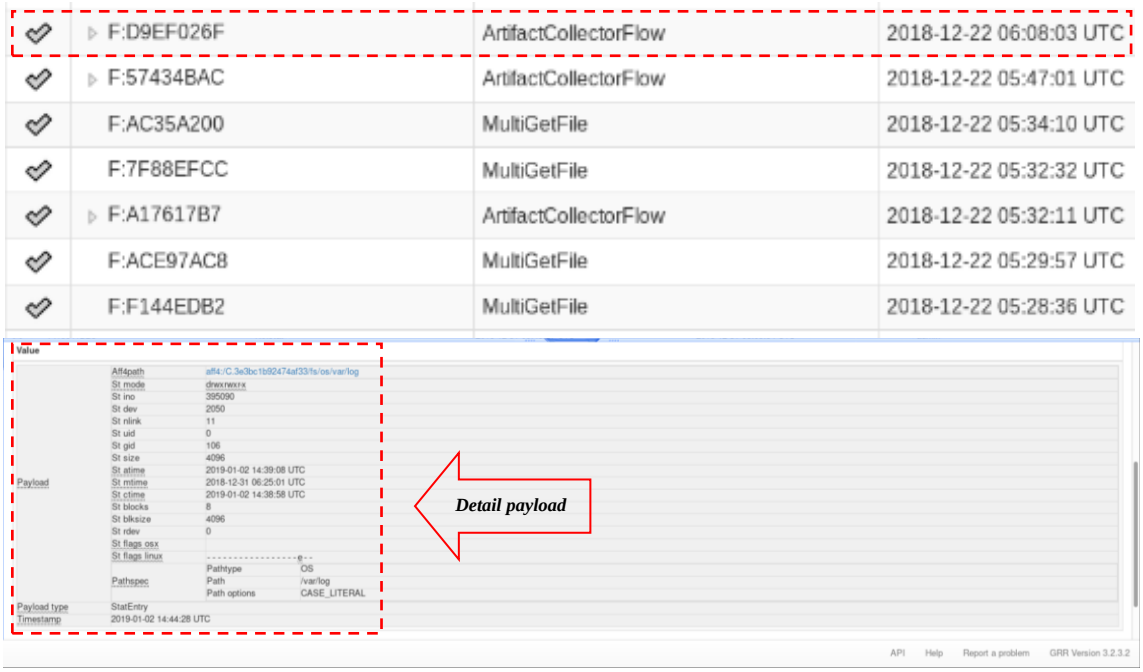
Gambar 7 merupakan proses pengumpulan atau koleksi barang bukti. Pada Grr Rapid Response dikenal istilah *flows* yaitu mengirimkan *request* dan *response* pada agen atau *client*, dan istilah *result* yaitu tanggapan *client* atau agen Grr Rapid Response atas *flows* dari *server* Grr Rapid Response. 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)* mebuat *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.



Gambar 7. *Artifact list Grr Rapid Response*

Sesuai dengan skenario kasus yang telah dibuat sebelumnya untuk melihat aktifitas *log* yang dilakukan pada *server*. *Artifact list* yang digunakan pada penelitian ini menggunakan artifak *LinuxLogFiles* yang dapat menampilkan *log file* yang dilakukan pada *server* lengkap dengan aktifitas yang dilakukan.

4.3 Eksaminasi Bukti Digital *(Examination)*

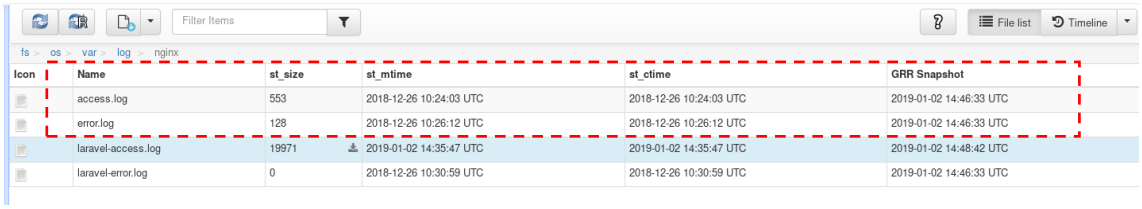


Gambar 8. Proses *Artifact list Grr Rapid Response*

Setelah dilakukan akuisisi maka tahap berikutnya yaitu proses eksaminasi. Proses pengujian ini untuk mengetahui seberapa besar 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. 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 detail *payload* dari *ArtifactCollectorFlow* yang dapat diakses oleh Grr Rapid Response seperti pada Gambar 8.

4.4 Analisis Bukti Digital *(Analysis)*

Pada tahap ini analisis digital dilakukan pada saat *server* terhubung dengan internet guna mendapatkan *log* aktifitas yang dilakukan. Pada penelitian ini *log framework laravel* dapat ditemukan oleh Grr Rapid Response setelah pengiriman *artifact list* berupa *LinuxLogFiles* seperti pada Gambar 9.



Gambar 9. *Log file* dari *Server*

Pada proses ini didapatkan hasil *filter* dari aktifitas yang pernah dilakukan pada *server*. Adapun hasil yang diperoleh meliputi IP *address*, *browser* yang digunakan ketika mengakses *server*, *file* yang diakses dan aktifitas dari *client* ketika *login* dan *update* data, diilustrasikan pada Gambar 10.

Gambar 10. Detail *Log* Aktifitas di *Server*

Pada tahap ini hasil yang diharapkan sesuai dengan skenario yang dibuat sebelumnya bahwa terdapat aktifitas perubahan pada *server* yang dilakukan oleh *user* yang mencurigakan dan tidak memiliki hak akses yaitu diperoleh bukti digital dari *user* yang memiliki IP *address* 192.168.56.1 telah melakukan aktifitas perubahan data beberapa kali pada tanggal yang sama yaitu 26 Desember 2018. Bukti yang diperoleh dengan Grr Rapid Response kemudian akan menjadi bukti digital dan sebagai acuan pada tahap selanjutnya yaitu tahap pelaporan bukti digital.

4.5 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 bukti yang didapatkan pada tahap analisis seperti deskripsi kasus yang sedang dilakukan, 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.

Hasil analisis bukti digital yang didapatkan berdasarkan metode forensika digital yang digunakan berhasil menjawab tujuan dari proses forensika yang dilakukan, hasil pemeriksaan diperoleh berupa *IP address user* 192.168.56.1 yang telah melakukan aktifitas perubahan data pada tanggal 26 Desember 2018 melalui *browser* Mozilla. Dengan didapatkan hasil ini proses forensika selesai maka tahap selanjutnya bukti digital ini akan diteruskan kepada pihak penegak hukum sebagai tambahan laporan di berita acara pemeriksaan (BAP) untuk ditindaklanjuti.

5. Kesimpulan

Berdasarkan hasil analisis *log* pada *framework laravel* pada *server* yang digunakan oleh aplikasi *mobile* dapat diambil kesimpulan bahwa: proses akuisisi dilakukan dengan *framework* Grr Rapid Response secara *live* forensik jarak jauh dan ditemukan informasi terkait artefak bukti. Langkah kerja forensik dari *National Institute of Standars Technology (NIST)* dapat diimplementasikan pada proses pengambilan bukti digital dengan metode *live forensics* dan dilakukan secara jarak jauh dengan menggunakan *framework* Grr Rapid Response. Kemampuan *tool* forensik pada proses eksaminasi, restorasi, dan analisis menggunakan *framework* Grr Rapid Response yang dilakukan pada *server* berhasil mendapatkan detail *log* dari *server*. Grr Rapid Response mendapatkan hasil *netstat* berupa *IP address, timestamp* dan *port* yang digunakan oleh *server*.

Referensi

[1] R. F. Cassidy, A. Chavez, J. Trent, and J. Urrea, "Remote Forensic Analysis of Process Control Systems," *IFIP International Federation for Information Processing Critical Infrastructure Protection*, pp. 223–235, 2008.

[2] Rosmiati, and I. Riadi, "Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal Dan Operasional Mengkombinasikan Standar Iso 27001:2005 Dengan Maturity Level (Studi Kasus Kantor Biro Teknologi Informasi PT. XYZ)," *Semin. Nas. Teknol. Inf. Dan Multimed*, vol. 6, no. 6, pp. 6–7, 2016.

[3] A. Yudhana, W. Yunanri, I. and Riadi, "Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing," *Annual Research Seminar (ARS)*, vol. 2, no. 1, pp. 300–304, 2016.

[4] M. N. Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," *JISKA (jurnal informatika sunan kalijaga)*, vol. 1, no. 3, pp. 108–114, 2017.

[5] M. S. Ahmad, I. Riadi, and Y. Prayudi, "Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Serangan Man in the Middle Attack Berbasis Evil Twin," *ILKOM Jurnal Ilmiah*, vol. 9, no. 1, pp. 1–8, 2017.

[6] I. Riadi, R. Umar, and I. Nasrulloh, "Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods," *Lontar*, vol. 9, no. 3, pp. 169–181, 2018.

[7] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ)," *Elinvo (Electronics, Informatics, and Vocational Education)*, vol. 3, no. 1, pp. 70–82, 2018.

[8] F. Cruz, A. Moser, and M. Cohen, "A scalable file based data store for forensic analysis," *Digital Investigation*, vol. 12, pp. S90–S101, 2015.

[9] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *IT JOURNAL RESEARCH AND DEVELOPMENT*, vol. 3, no. 1, pp. 13–21, 2018.

[10] A. A. Mohallel, J. M. Bass, and A. Dehghantaha, "Experimenting with docker: Linux container and base OS attack surfaces," *2016 International Conference on Information Society (i-Society)*, pp. 17-21, 2016.

[11] F. Sahrul, M. A. Safi'ie, and W. A. O. Decroly, "Implementasi Sistem Informasi Akademik Berbasis Web Menggunakan Framework Laravel", *Jurnal Transformasi*, vol. 12, no. 1, pp. 1–4, 2016.

[12] R. Imam, A. Yudhana, and M. Caesar F.P, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," *Scientific Journal of Informatics*, vol. 5, no. 2, pp. 235–247, 2018.

[13] G. M. Zamroni, "Analisis Forensik Aplikasi Instant Messaging Berbasis Android," *Annual Research Seminar (ARS)*, vol. 2, no. 1, pp. 102–105, 2017.

[14] U. Rusydi, R. Imam, and M. B. Fauzan, "Acquisition Of Email Service Based Android," *Kinetik*, vol. 3, no. 4, pp. 1–9, 2018.

[15] R. Umar and P.H. Prabowo, "Pencarian Dan Pemesanan Travel Berbasis Mobile dengan Google Maps API," *Annual Research Seminar (ARS)*, vol. 2, no. 1, pp. 369–373, 2017.

(Halaman ini sengaja dikosongkan.)