e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021

Penerapan *Memory Forensic* Menggunakan Metode *Live Forensic* untuk Investigasi *Random Access Memory*

Mochammad Nauval Rifkiansyah [1], Rizky Satria Wibowo [2], Rifky Priambudi [3], Kartika Ananda Putri [4], Henki Bayu Seta, S.Kom., MTI. [5]

Informatika / Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. RS. Fatmawati Raya, Pd. Labu, Kec. Cilandak, Kota Depok, Jawa Barat 12450
mnauvalr27@gmail.com

Abstrak. *Memory forensic* (terkadang disebut sebagai analisis memori) mengacu pada analisis data volatile dalam dump sebuah memori komputer, *memory forensic* dibutuhkan untuk menyelidiki dan mengidentifikasi serangan atau perilaku jahat yang tidak meninggalkan jejak yang dapat dideteksi dengan mudah pada data hard drive. Investigasi menggunakan Teknologi live forensic membutuhkan ketelitian dan akurasi, karena jika sistem dimatikan, data volatile dalam RAM dapat hilang dan data penting dalam RAM dapat ditimpa oleh aplikasi lain. Karena itu membutuhkan metode live forensik yang dapat menjamin keutuhan dan keaslian data yang mudah menguap tanpa kehilangan data yang dapat menjadi bukti.. Hasil investigasi ini akan menjadi acuan untuk seberapa canggih penerapan *memory forensic* menggunakan metode *live forensic* pada RAM.

Kata Kunci: *Memory Forensic, Live Forensic*, RAM

1 Pendahuluan

Forensik komputer merupakan teknik investigasi dan analisis komputer yang melibatkan tahapan dalam mengidentifikasi, menyiapkan, mengekstraksi, merekam, dan menginterpretasikan data yang terdapat pada komputer, tahapan tersebut dapat digunakan sebagai bukti adanya kejadian kejahatan dunia maya *cybercrime* [1]. Komputer forensik pada awalnya dilakukan dengan cara menganalisis media penyimpanan dari sebuah sistem yang dicurigai telah terlibat dalam sebuah tindak kejahatan, dimana biasanya sistem perlu dinonaktifkan kemudian dibuat *image* kloning dari media penyimpanan sistem tersebut. *Image* inilah yang dianalisis yang dapat digunakan sebagai barang bukti untuk keperluan investigasi lebih lanjut [2].

Dengan menganalisis data volatile yang terdapat dalam RAM (Random Access Memory), dapat diketahui perilaku kriminal berdasarkan penggunaan komputer [3]. Komputer forensik pada awalnya dilakukan dengan cara menganalisis media penyimpanan dari sebuah sistem yang dicurigai telah terlibat dalam sebuah tindak kejahatan, dimana biasanya sistem perlu dinonaktifkan kemudian dibuat *image* kloning dari media penyimpanan sistem tersebut. *Image* inilah yang dianalisis yang dapat digunakan sebagai barang bukti untuk keperluan investigasi lebih lanjut [2].

Metode live forensik dirancang untuk memproses kejadian lebih cepat, memastikan integritas data, teknologi enkripsi yang lebih mudah dibuka, dan memiliki kapasitas memori yang lebih rendah daripada metode tradisional yang membutuhkan memori dalam jumlah besar, membutuhkan waktu lebih lama, dan memungkinkan kehilangan data [3] . Data volatile, khususnya RAM, merupakan sistem yang mendeskripsikan semua aktivitas yang sedang terjadi pada sistem [2]. Data volatile dalam RAM harus ditangani dengan hati-hati, karena jika sistem dimatikan, selain kehilangan data, penggunaan alat juga akan menyisakan ruang yang dapat menimpa bukti berharga dalam memori. Oleh karena itu, diperlukan metode live forensik yang dapat menjamin integritas data volatile tanpa menghilangkan data yang mungkin menjadi bukti [3].

e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021

Ketersediaan alat seperti Volatilitas memungkinkan penyelidik forensik mengidentifikasi dan menghubungkan berbagai komponen untuk menyimpulkan apakah kejahatan *cyber* itu dilakukan menggunakan *malware* atau tidak. Namun, penggunaan volatilitas membutuhkan pengetahuan tentang alat baris perintah (*Command Line*) serta analisis *malware* statis [2]. Sebagian tools forensik yang berfungsi mendeteksi malware secara otomatis, hal ini men haruskan kita untuk terhubung dengan internet, dan deteksi malware yang dilakukan terbatas. Pekerjaan yang disebutkan dalam jurnal ini terinspirasi untuk menerapkan algoritma machine learning dan otomatisasi langkah-langkah dasar. Keuntungan terbesar dari tools ini adalah, Pengguna dapat mendeteksi semua proses yang berjalan pada RAM dan tidak harus terkoneksi dengan internet [4]. Penerapan *memory forensic* dengan metode *live forensic* diusulkan untuk berbagai macam keperluan dalam identifikasi proses yang berjalan pada RAM dan juga menganalisis dan memberikan laporan akhir yang akurat.

Rumusan masalah pada penelitian ini:

1. Apa hasil yang didapat ketika kita melakukan proses *memory forensic* menggunakan metode *live forensic*?

2. Bagaimana metode *live forensic* diterapkan dalam penanganan investigasi *memory forensic* pada *Random Access Memory*?

2 Studi Literatur

2.1 Digital Forensik

Forensik digital merupakan bagian dari ilmu forensik, termasuk dalam penemuan dan investigasi material (data) yang terdapat dalam perangkat digital [4]. Dalam mencari bukti digital yang dapat disimpan di penyimpanan sementara komputer, penyimpanan permanen, USB, CD, lalu lintas jaringan, dll, forensik digital telah banyak digunakan di bidang hukum. Secara umum terdapat dua jenis analisis forensik digital, yaitu forensik valid dan forensik real-time [3]. Tujuan utama dari *forensics digital* menurut Prof. Richardus Eko Indrajit adalah sebagai berikut [8]:

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat bukti yang sah di pengadilan.
2. Untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivasi tindakan, tersebut sambil mencari pihak-pihak terkait yang terlihat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan.

2.2 *Cybercrime*

Cybercrime adalah berbagai bentuk penggunaan jaringan komputer untuk tujuan kriminal dan / atau penjahat berteknologi tinggi melalui penyalahgunaan kemudahan teknologi digital [4]. Kejahatan *cybercrime* dapat diinvestigasi dengan melakukan komputer forensik, yaitu analisis data volatile.

2.4 Memory

Memory atau juga biasa disebut *Random Access Memory* (RAM) merupakan *memory* yang berfungsi sebagai penyimpanan sementara untuk perintah dan data pada saat program dijalankan. Perintah dan data tersebut mencakup data yang akan dibaca dari harddisk, data-data yang dimasukkan melalui alat input komputer dan data-

e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021

data hasil pemrosesan sebuah program. Pada saat daya listrik tidak ada atau *power off* data-data yang ada pada memory akan segera hilang secara permanen [8].

2.4 Data Volatile

Data dalam RAM (*random access memory*) terdapat data volatile atau bisa disebut juga data sementara. Dengan data volatile dapat dilakukan analisis tindakan kejahatan pengguna komputer. Karena dengan data volatile dapat mengetahui log dari aktivitas kegiatan penggunanya [3].

2.5 Memory Forensic

Dalam melakukan investigasi cyber crime dilakukan memory forensic. *Memory forensic* merupakan teknologi forensik yang digunakan untuk memperoleh data (yaitu data volatile) tentang tindakan kejahatan atau kejadian serangan.

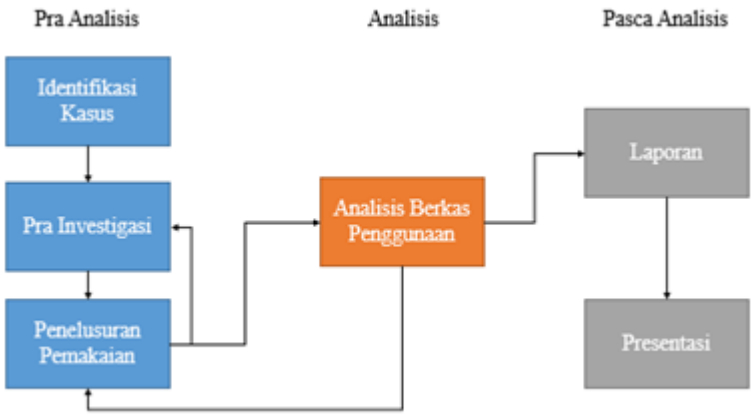
2.6 Metode *Live Forensic*

Menurut (Rusyadi Umar, dkk [3]) metode live forensic dapat memastikan keutuhan data volatile tanpa kehilangan data yang dapat menjadi bukti. Sementara itu menurut (Faiz, dkk [5]) metode *live forensic* bergantung pada keadaan komputer yang sedang berjalan, karena membutuhkan data yang berjalan pada random access memory (RAM). Berdasarkan uraian tersebut, dapat disimpulkan dengan metode live forensic dapat memproses peristiwa lebih cepat, memastikan integritas data, dan lebih mungkin untuk mengaktifkan teknologi enkripsi dan memiliki kapasitas memori yang lebih rendah. *Live forensics* pada dasarnya memiliki kesamaan pada teknik tradisional dalam hal metode yang dipakai yaitu identifikasi, penyimpanan, analisis, dan presentasi, hanya saja *live forensics* merupakan respon dari kekurangan teknik forensics tradisional yang tidak bisa mendapatkan informasi dari data dan informasi yang hanya ada ketika sistem sedang berjalan misalnya aktivitas *memory, network process, swap file, running system proses,* dan informasi dari file sistem. pada metode *live forensics* bertujuan penanganan insiden lebih cepat, integritas data lebih terjamin, teknik enkripsi lebih memungkinkan bisa dibuka dan kapasitas *memory* yang rendah dibandingkan dengan metode *forensics* tradisional. Banyak *tools* yang dapat digunakan untuk *live forensics* untuk analisa data [8].

3 Metodologi Penelitian

3.1 Flowchart Penelitian

Metode yang diusulkan dalam penelitian ini adalah integrasi model proses umum dari respon insiden dan forensik komputer, model umum investigasi forensik komputer, dan metode investigasi langkah demi langkah untuk melacak penggunaan komputer. Model proses bertujuan untuk memilih sistem dan menganalisis bukti secara efektif. Model tersebut meliputi tiga tahap utama yang ditunjukan pada gambar 1 yaitu tahap pra analisis, tahap analisis dan tahap pasca analisis.



Gambar. 1. Ide Model Forensik yang diajukan

3.1.1 Tahap Pra Analisis

Tahap pertama dari model proses forensik memori adalah tahap pra-analisis. Tahapan ini meliputi tiga tahap, yaitu menentukan kasus, melakukan penyelidikan dan penelusuran penggunaan.

3.1.1.1 Identifikasi Kasus

Langkah pertama dalam tahap pra-analisis adalah mengidentifikasi kasus / insiden. Penyelidik harus dapat mengidentifikasi kasus dan meminimalkan kemungkinan kejadian atau risiko. Penyidik harus mengetahui dan memastikan waktu kejadian, lokasi kasus, dan sistem mana yang harus diselidiki berdasarkan jenis kasusnya. Tahapan ini dapat memberikan metode yang efektif untuk merespon insiden / kasus dengan mempersingkat total waktu investigasi.

3.1.1.2 Pra Investigasi

Selain itu, data waktu nyata dan metadata sistem file diperoleh dan dianalisis. Data real-time diperoleh dalam random access memory (RAM). Untuk mengumpulkan informasi data waktu nyata, sistem target tentunya harus aktif. Data waktu nyata memberikan informasi kunci dari sistem target pada waktu respons insiden awal, seperti "penangkapan". Dengan menggunakan informasi tentang penggunaan sistem dalam data waktu nyata, Anda juga dapat mengidentifikasi informasi tentang sistem dasar, seperti nama komputer, pengguna yang baru masuk, waktu mulai, dan waktu aktif. Penyidik dapat menyelidiki keberadaan file yang terkait dengan kasus tersebut melalui pencarian atau pemfilteran kata kunci. Dengan menggunakan metadata sistem file, penyelidikan menggunakan teknik ini tentu lebih cepat daripada menyelidiki seluruh citra disk.

3.1.1.3 Penelusuran Pemakaian

Data target yang diperoleh pada tahap ini adalah registry prefetching dan aktivitas internet, seperti file web history, penggunaan Messenger, dan arsip email. Analisis diperlukan untuk mendapatkan informasi yang diperlukan. Registry dapat memberikan informasi, seperti perintah yang dijalankan, kata kunci pencarian, folder yang terakhir diakses, file yang terakhir dieksekusi, log aplikasi, dan informasi lainnya. Peneliti dapat menjalankan analisis registry untuk mengekstrak file dan data yang relevan. File prefetch dapat digunakan untuk menentukan aplikasi mana yang sering digunakan akhir-akhir ini. File browser adalah alat yang ampuh untuk melacak penggunaan internet pengguna.Berkas temporary bahkan dapat menampilkan isi dari surel yang ditemukan di random access memory (RAM) pada suatu komputer.

e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021

3.1.2 Tahap Analisis

Pada tahap analisis ini dilakukan setelah tahapan pra analisis selesai dijalankan, tahapan analisis pada memory forensik ini dilakukan dalam dua macam tahapan yaitu analisis pola pemakaian komputer dan analisis berkas pemakaian.

3.1.2.1 Analisis Pola Pemakaian Komputer

Tahapan awal analisis adalah pola pemakaian komputer. Berdasarkan data yang didapat dari hasil pra analisis penyidik dapat melakukan analisis dan menyimpulkan pola dari pemakaian komputer tersangka. Analisis pola pemakaian komputer dapat memberikan informasi berupa kapan waktu tersangka biasanya menggunakan komputer dan jenis data serta aplikasi apa saja yang tersangka gunakan. Log pemakaian data dan aplikasi juga dapat digunakan kapan data dan aplikasi tersebut digunakan. Secara signifikan juga, MAC *time* dapat dipakai dalam memperkirakan pola pemakaian aplikasi. Data peramban web juga dapat dijadikan dalam proses investigasi kapan waktu tersangka melakukan akses terhadap situs web tersebut.

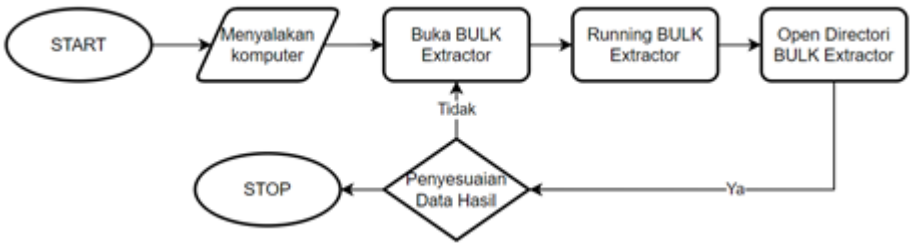
3.1.2.2 Analisis Data Pemakai

Selanjutnya pada tahap ini, data-data yang dianggap relevan dapat digunakan dan diambil. Kemudian data-data bukti dilakukan proses investigasi berdasarkan hasil dari analisis data serta pemahaman kasus secara menyeluruh. Tahapan ini juga berfokus pada apabila tersangka melakukan hapus data, enkripsi ataupun memodifikasi data tersebut untuk merusak bukti yang ada.

3.1.3 Tahap Pasca Analisis

Pada tahapan terakhir dari model yang telah dibuat prosesnya adalah tahap pasca analisis. Tahapan ini terdiri atas dua tahapan, yaitu dimana pembuatan laporan atas segala hal yang didapatkan serta juga proses proses pemaparan atau persentasi. Laporan itu biasanya berisi atas rincian dokumentasi serta insiden dari semua langkah yang sebelumnya telah dilakukan pada tahapan analisis. Presentasi dan pemaparan mengenai apa saja yang telah diperoleh pada hasil investigasi juga memperkuat untuk bukti di pengadilan.

3.2 Flowchart Program



Gambar. 2. Flowchart Bulk Extractor

3.3. Studi Literatur

Untuk mengetahui bagaimana kinerja *memory forensic* menggunakan metode live forensic akan digunakan metode studi literatur sebagai salah satu metode penelitiannya. Pencarian literatur dengan topik *memory forensic* serta metode live forensic guna mendapatkan informasi terkait dengan analisis *memory forensic* menggunakan metode *live forensic*. Dari hasil pencarian tersebut kemudian dipilih artikel serta pembahasan yang memiliki korelasi yang kuat dengan topik yang akan dibahas.

4 Hasil dan Pembahasan

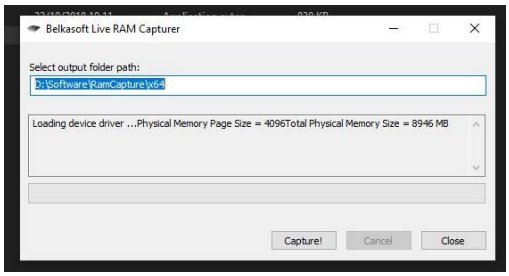
4.1. Pengujian Bulk Extractor

Berdasarkan hasil dan penelitian yang sudah dilakukan maka dapat ditarik bahwa penelitian terkait analisis tentang penerapan memory forensic pada live forensic memperoleh hasil yang berupa berkas yang kedepannya bisa digunakan sebagai barang bukti atau bahan penyelidikan lebih lanjut. Investigasi pada data volatile yang sedang berjalan RAM dapat mengetahui berbagai aktivitas yang terekam di dalam komputer tersebut atau *log* dari aktivitas pengguna. Data yang terekam ini bisa menjadi salah satu barang bukti yang berguna dalam proses penyidikan. Selain barang bukti dengan memory forensic kita juga mendapatkan metadata sistem berkas, berkas prefetch, registry, serta berkas peramban dan dokumen spesifik. Penelitian ini diharapkan dapat merekomendasikan tools yang sesuai dengan kasusnya dan berjalan pada sistem operasi. Selain itu juga penelitian ini diharapkan akan mempermudah para investigator untuk melakukan investigasi terkait dengan forensic digital yang dimana bisa dikatakan bahwa dengan metode forensic ini cukup efektif digunakan dalam proses forensik digital.

Dalam penelitian ini telah dicapai beberapa penemuan bukti-bukti informasi yang terdapat pada *Random Access Memory* dalam bentuk digital, seperti penelusuran website yang dilakukan, akun email yang berkaitan, serta file-file apa saja yang bersangkutan dengan RAM. Informasi yang didapat direkap oleh *tools* dari sistem operasi Linux yaitu Bulk Extractor dengan mengolah data dengan ekstensi .mem yang didapat dari proses perekaman RAM menggunakan *tools* Belkasoft dari sistem operasi Windows.

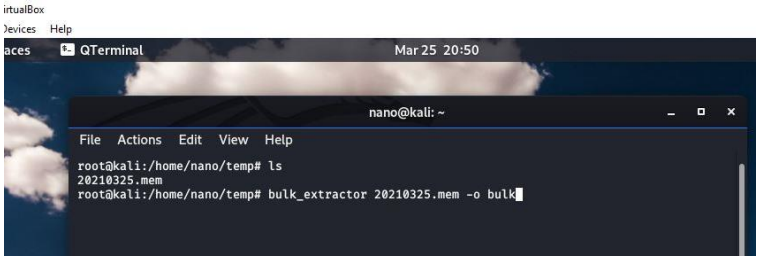
4.2. Tahapan Pengujian

a). Pra Investigasi

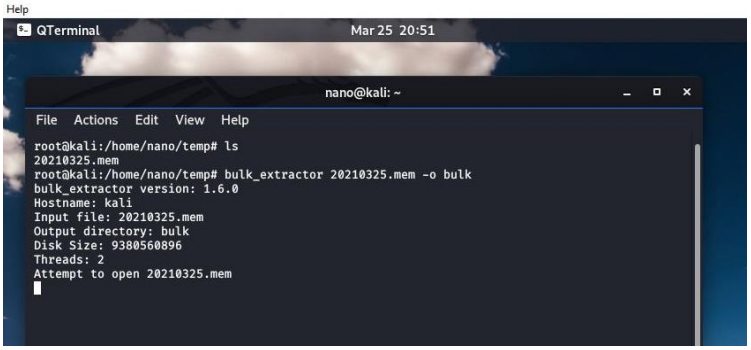


Gambar. 3. Capture terhadap RAM. Langkah pertama dalam tahapan pengujian ini adalah melakukan *capture* terhadap RAM dengan sistem operasi windows dimana *software* yang digunakan yaitu RAM Capturer dari Belkasoft**.** Proses ini memakan waktu kurang lebih 20-30 menit, tergantung kapasitas RAM, semakin besar RAM maka semakin lama.

b.) Analisis Berkas

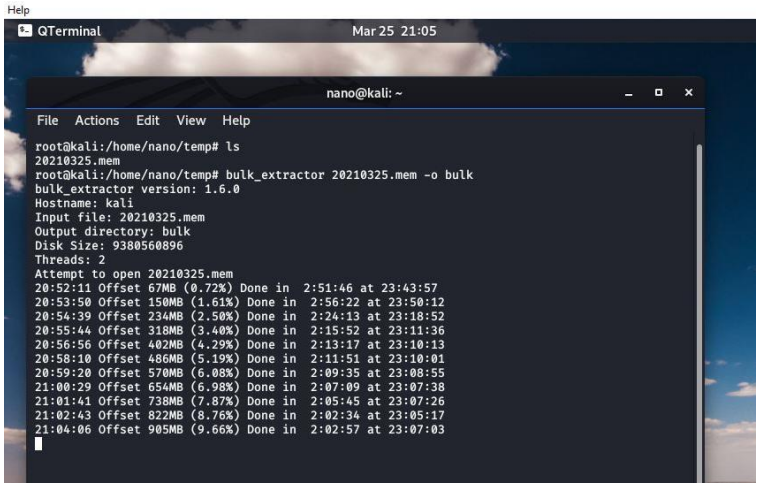


Gambar. 4. Hasil dari *capture* RAM. Capture terhadap RAM menghasilkan file dengan ekstensi ****.mem***, dari hasil file tersebut dipindahkan ke sistem operasi Kali Linux dikarenakan penggunaan *tools* hanya bisa dilakukan pada sistem operasi Kali Linux. Didalam sistem operasi Kali Linux terdapat *tools* bernama Bulk Extractor, percobaan dilakukan dengan membuka atau menjalankannya dengan cara menuliskan sintaks **bulk_extractor *tanggal/waktu*.mem –o bulk.**



Gambar. 5. Step Bulk Extractor. Bulk Extractor ini jika berhasil dijalankan akan menampilkan versi dari Bulk Extractor yang dijalankan, kemudian akan menampilkan informasi berupa hostname, kemudian input file yang akan dilakukan forensik pada waktu tertentu, output menggunakan bulk, kemudian ukuran dari disk yang dilakukan forensik, dan jumlah threads yang ada.

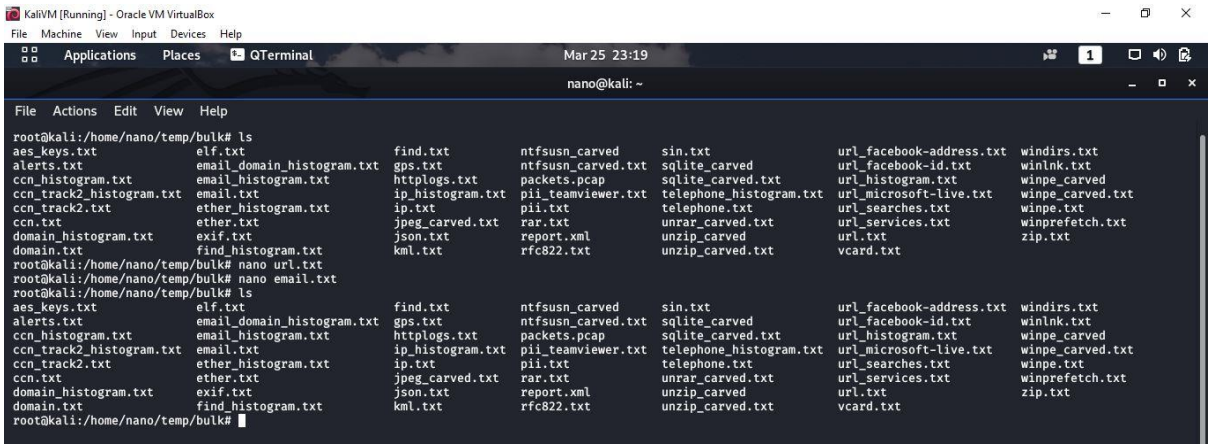
c). Proses Analisis



Gambar. 6. Eksekusi Bulk Extractor. Bulk Extractror melakukan running *scanning* terhadap RAM target dimana semakin besar RAM dan semakin banyak pemakaiannya maka akan semakin lama waktu yang diperlukan dalam proses *scanning*, kemudian memory yang sudah dilakukan proses forensik akan ditampung ke dalam file dari Bulk Extractor.

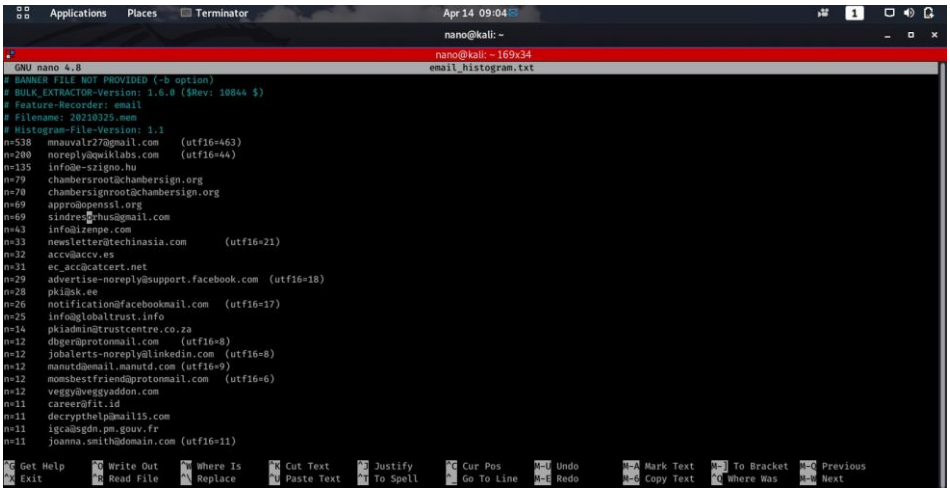
e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021

d). Laporan



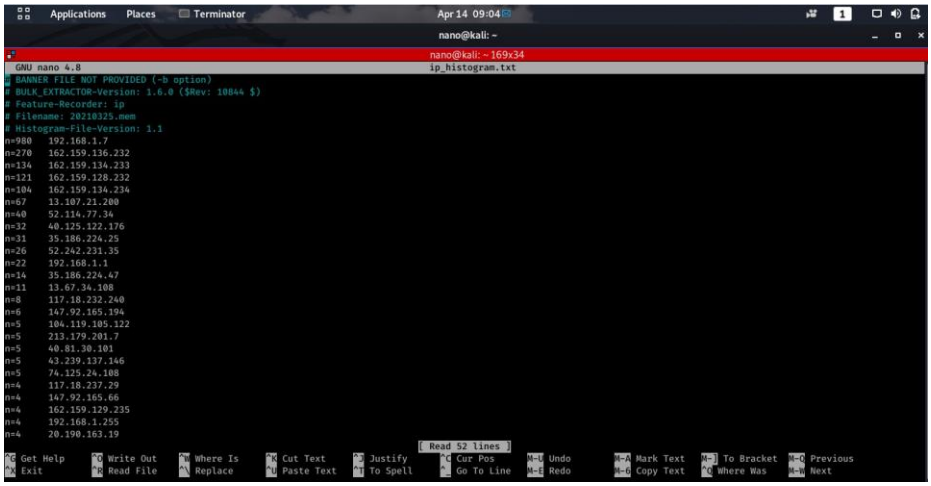
Gambar. 6. Laporan. Hasil laporan dari proses ekstraksi menggunakan *tools* Bulk Extractor seperti terlihat pada dimana pada file dengan ekstensi ****.mem*** bahwa Bulk Extractor menyimpan hasil dari forensik yang dilakukan dalam folder bulk, kemudian ketika folder tersebut dibuka terdapat beberapa informasi tentang rekan hasil forensik yang dilakukan dimana hasil ini berekstensi .txt dan berisikan keseluruhan yang dijalankan pada RAM atau memory yang dijalankan.

Berikut adalah hasil pembacaan beberapa informasi digital yang terekam pada RAM.

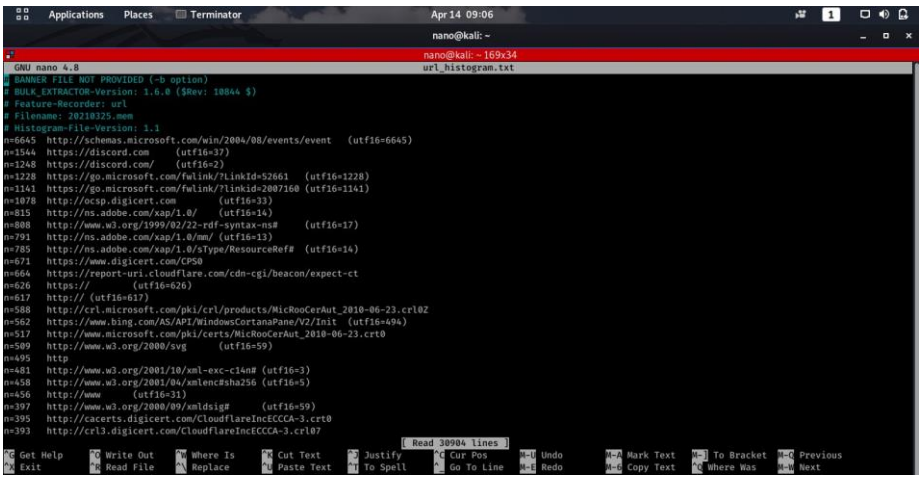


Gambar. 7. Histogram aktivitas email yang sering diakses oleh user pada RAM.

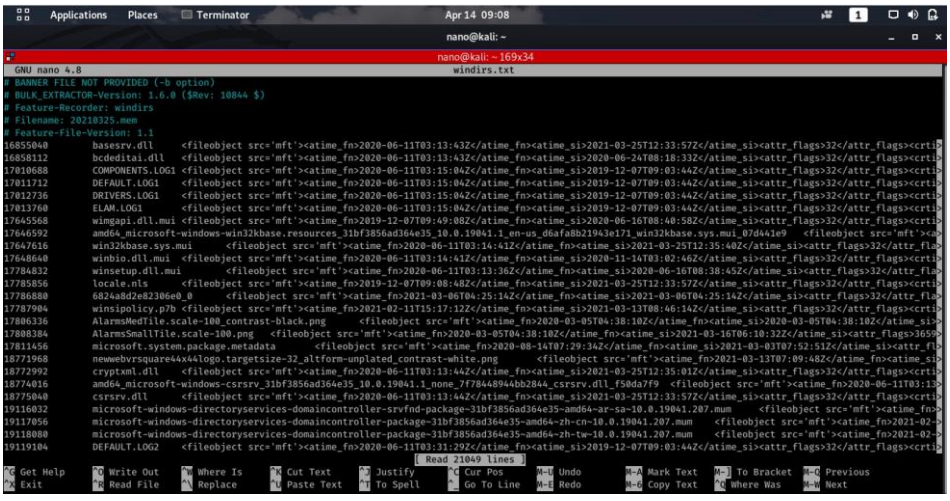
e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021



Gambar. 8. Frekuensi IP Address yang berjalan pada RAM.

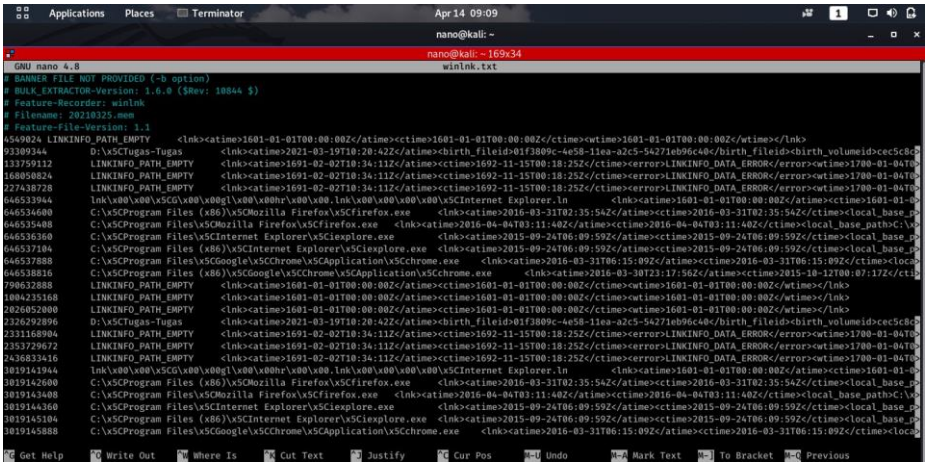


Gambar. 9. Aktivitas URL yang diakses pada *memori* perangkat.



Gambar. 10. Direktori yang terekam pada windows yang diakses pada saat komputer berjalan.

e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021



Gambar. 11. Informasi rekaman *path* direktori yang diakses pada saat komputer hidup.

4.3 Hasil Eksekusi

Berdasarkan eksekusi pada hasil investigasi *memory* pada RAM dengan menggunakan metode *live forensics*, bahwa aktivitas pada RAM yang telah di-*capture* menggunakan *software* Belkasoft merekap beberapa informasi digital dengan berbagai aktivitas. Itu terbukti dari hasil analisis menggunakan *tool* Bulk Extractor berikut sistem operasi Linux dengan dipaparkan beberapa hasil yang bisa ditangkap bisa dilihat

Tabel. 1. Hasil Eksekusi

Tools	IP Addres	URL	Direktori	Path
Bulk Extractor	✓	✓	✓	✓

Dari semua hasil analisis dapat diketahui bahwa dari tools ini sangat lengkap dan dapat digunakan untuk proses investigasi dan kebutuhan penyelidikan di lapangan terkait perkara.

4.4. Pengujian Kecepatan dan Respon

Dalam pengujian ini dilakukan percobaan sebanyak tiga kali *scanning* pada RAM menggunakan metode *live forensic.* Tools yang digunakan disini adalah Bulk Extractor yang terdapat didalam sistem operasi Linux. Waktu yang diperoleh dalam skema pengujian ini didapatkan langsung dari program eksekusi yang memperlihatkan proses waktu dalam *scanning* yang sedang berjalan.

Gambar. 12. Hasil Percobaan *Scanning*. Berdasarkan hasil dari percobaan selama tiga kali terhadap *scanning*

dengan menggunakan perangkat yang sama serta data yang sama diperoleh peningkatan atas waktu kinerja (*running execute*). Hal ini disebabkan oleh beberapa faktor dimana salah satu faktor yang mempengaruhi hal tersebut adalah peningkatan suhu terhadap komputer yang sedang dilakukan proses *scanning*.

Gambar. 13. Peningkatan Suhu Perangkat. Dapat dilihat peningkatan suhu ini terjadi ketika dilakukan proses *scanning* yang dilakukan lebih dari satu kali. Hal ini yang menyebabkan proses *scanning* cenderung meningkat dari waktu ke waktu yang disebabkan kenaikan suhu pada perangkat.

5 Kesimpulan

Berdasarkan penelitian yang telah dipaparkan, maka *memory forensic* dengan metode *live forensic* ini dapat mempermudah para investigator untuk memperoleh *log data* pada data volatile serta berbagai hal lainnya untuk digunakan sebagai proses investigasi dan juga sebagai barang bukti yang kedepannya bisa digunakan untuk proses penyidikan atau persidangan dimana efektifitas serta apa yang dibutuhkan guna proses penyidikan dan hal lainya bisa didapatkan dengan metode ini.

Analisis forensik pada dasarnya untuk menjawab pertanyaan penyelidikan dengan menganalisis data yang ditemukan pada data forensik yang dibuat pada tahapan “Analisis Berkas Penggunaan”. Proses analisis yang sebenarnya dapat bervariasi antara investigasi, tetapi metodologi yang digunakan bisa berbeda, bukti yang telah diperoleh dianalisis untuk merekonstruksi peristiwa atau tindakan dan untuk mencapai kesimpulan dan juga pelaporan.

Penelitian ini berhasil menggunakan alat dari sistem operasi Linux (yaitu ekstraktor massal) untuk meringkas laporan dalam bentuk memori akses acak. Untuk penelitian selanjutnya diharapkan dapat dibandingkan dengan berbagai alat bantu penanganan forensik memori lainnya, agar diperoleh hasil terbaik pada kasus yang sering terjadi.

Referensi

[1] Bahtiar, F., Widiyasono, N., & Aldya, A. P. (2018). Memory Volatile Forensik Untuk Deteksi Malware Menggunakan Algoritma Machine Learning. *Jurnal Teknik Informatika dan Sistem Informasi* , 242-253.

[2] Belsare, J., & Sinha, A. (International Journal on Recent and Innovation Trends in Computing and Communication). 2015. *Live Memory Forensic Analysis*, 2775-2778.

[3] Frank, A. (2006). Live Forensic - Diagnosing Your System Without Killing It First. *Communication of The ACM*, 63-66.

[4] Solomon, M., Barett, D., & Broom, N. (2005). *Computer Forensics Jumpstart.* Alameda: SYBEX Inc.

[5] Umar, R., Yudhana, A., & Faiz, M. N. (-). Analisis Kinerja Live Forensics Untuk Investigasi RAM Pada Sistem Propierty. *Prosiding Konferensi Nasional Ke- 4*, 207-211.

[6] Yaqin, M. A., & Cahyanto, T. A. (-). *Analisis Metode Live Forensic Pada Perangkat Memory Laptop Untuk Pencarian Artefak Digital Berbasis Linux.* Jember: Universitas Muhammadiyah.

[7] Yudhistira, D. S., & Prayudi, Y. (2018). Live Forensics Analysis Method For Random Access Memory On Laptop Devices. . *International Journal of Computer Science and Information Security*, 188-192.