STUDI PERBANDINGAN TEKNOLOGI *LIVE FORENSIC* UNTUK INVESTIGASI *RANDOM ACCESS MEMORY*

SKRIPSI

Diajukan untuk memenuhi salah satu syarat guna memperoleh gelar Diploma Empat (D-4/S1 Terapan) pada Politeknik Negeri Ujung Pandang

ARIE OKTARIADI AKIL
425 13 049

PROGRAM STUDI D-4 TEKNIK KOMPUTER DAN JARINGAN

JURUSAN TEKNIK ELEKTRO

POLITEKNIK NEGERI UJUNG PANDANG

MAKASSAR

2017

HALAMAN PENGESAHAN

Laporan Tugas Akhir dengan judul "**Studi Perbandingan Teknologi *Live Forensics* Untuk Investigasi *Random Access Memory***", oleh Arie Oktariadi Akil, NIM 425 13 049, telah siap diujikan sebagai salah satu syarat untuk memperoleh gelar Diploma IV (D-4/S1 Terapan) pada Program Studi Teknik Komputer dan Jaringan Jurusan Teknik Elektro Politeknik Negeri Ujung Pandang.

Makassar, 05 September 2017

Pengesahan,

Pembimbing I	Pembimbing II
Irfan Syamsuddin, S.T., M.Com. ISM. Ph.D.	Sahbuddin Abdul Kadir, S.T., M.T.
NIP.19731220 200003 1 008	NIP. 19751130 200604 1 001

Mengetahui,

Ketua Program Studi

Teknik Komputer Dan Jaringan

Rini Nur, S.T., M.T.
NIP. 19730713 200912 2 001

HALAMAN PENERIMAAN

Pada hari ini, Jumat tanggal 29 September 2017, Tim Penguji Ujian Sidang Skripsi telah menerima dengan baik skripsi oleh mahasiswa: Arie Oktariadi Akil nomor induk mahasiswa 425 13 049 dengan judul **Studi Perbandingan Teknologi *Live Forensics* Untuk Investigasi *Random Access Memory.***

Makassar, 29 September 2017

Tim Penguji Ujian Sidang Skripsi:

1. Iin Karmila Yusri, S.ST., M.Eng. Ketua (.....)
2. Ir. Dahlia Nur, M.T. Sekertaris (.....)
3. Irmawati, S.T., M.T. Anggota (.....)
4. Sulaeman, S.T., M.T. Anggota (.....)
5. Irfan Syamsuddin, ST., M.Com., ISM., Ph.D. Anggota (.....)
6. Sahbuddin Abdul Kadir, S.T., M.T. Anggota (.....)

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, karena atas segala rahmat dan hidayah-Nya yang tak henti memberikan kesehatan dan keselamatan sehingga penulis dapat menyelesaikan penyusunan skripsi dengan baik.

Skripsi ini disusun guna memenuhi salah satu syarat untuk menyelesaikan studi serta dalam rangka memperoleh gelar Sarjana Sains Terapan pada Program Studi D-IV Teknik Komputer dan Jaringan di Politeknik Negeri Ujung Pandang.

Penyusunan skripsi ini bukanlah hasil kerja penulis sendiri, melainkan juga berkat bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, melalui kesempatan ini penulis menyampaikan penghargaan dan terima kasih yang sedalam-dalamnya kepada :

1. Orang tua penulis yakni Ibunda Rosmawati serta semua Kakak Kandung Penulis yang senantiasa selalu memberikan semangat, motivasi, dukungan, bimbingan dan doa restu kepada penulis.
2. Ibu Dr. Ir. Hafsah Nirwana, M.T. selaku Ketua Jurusan Teknik Elektro Politeknik Negeri Ujung Pandang dan Ibu Rini Nur, S.T., M.T. selaku Ketua Program Studi Teknik Komputer dan Jaringan yang selalu memiliki semangat untuk memajukan program studi ini.
3. Bapak Irfan Syamsuddin S.T., M.Com. ISM. Ph.D. selaku pembimbing I dan Bapak Sahbuddin Abdul Kadir, S.T., M.T. selaku pembimbing II, yang juga telah

senantiasa dengan sabar dan selalu berusaha maksimal untuk mengarahkan dalam penyelesaian skripsi ini.

4. Teman-teman TKJ B angkatan 2013 yang memberikan banyak pembelajaran hidup tentang kebersamaan dan persaudaraan, terutama kepada Muhammad Subair yang selalu membantu dan memberikan arahan dalam penyelesaian skripsi ini.
5. Semua pihak yang telah memberikan bantuan baik moril maupun materil yang tidak dapat disebutkan satu per satu.

Penulis menyadari masih banyak kekurangan dalam penulisan skripsi ini, maka sangat diharapkan kritik dan saran dari pembaca untuk penyempurnaan karya-karya yang akan datang. Harapan dari penulis, semoga skripsi ini dapat bermanfaat bagi siapa saja yang menggunakannya.

Makassar, September 2017

Penulis

DAFTAR ISI

Hal.

DAFTAR GAMBAR

Hal.

DAFTAR TABEL

Hal.

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Arie Oktariadi Akil

NIM : 42513049

Menyatakan dengan sebenar benarnya bahwa segala pernyataan dalam skripsi

STUDI PERBANDINGAN TEKNOLOGI *LIVE FORENSIK* UNTUK INVESTIGASI *RANDOM ACCESS MEMORY*

RINGKASAN

Live forensics merupakan sebuah proses dalam upaya mendapatkan informasi dan data yang terdapat dalam *memory* pada sebuah sistem yang sedang berjalan dan akan hilang ketika sistem tersebut dimatikan. *Random Access Memory* atau biasa disingkat dengan RAM merupakan sebuah tipe penyimpanan komputer yang isinya dapat diakses dalam waktu yang tepat tidak memperdulikan letak data tersebut dalam memori. RAM juga merupakan salah satu penyimpanan yang bersifat *volatile* atau data akan hilang saat tidak terdapat aliran listrik. Sedangkan data *volatile* yang terdapat pada RAM sangat berguna untuk forensik, karena RAM pada sistem komputer menggambarkan seluruh kegiatan yang telah terjadi pada sistem tersebut. Teknologi *live forensic* dilakukan pada RAM DDR2 dan RAM DDR3, Untuk mendapatkan bukti digital pada RAM dilakukan akuisisi data pada RAM menggunakan *tools* Belkasoft RamCapture dan DumpIt yang menghasilkan *image memory*. Dalam *image memory* ini akan dilihat data apa saja yang tersimpan dalam RAM, dan melihat keakuratan data hasil dari forensik memori dengan menggunakan beberapa variasi skenario khusus yang diujikan. Ada beberapa data ditemukan dalam *random access memory* yaitu proses yang berjalan dalam sistem, proses *registry handles* yang berjalan dalam sistem, aktivitas *network* yang didapat dalam sistem, *malicious code* pada sistem, *password* dan *username* log-in pada sosial media. data proses lebih akurat saat menggunakan *tools* Belkasoft RamCapture. Data proses lebih banyak ditemukan pada RAM DDR3 dibandingkan data proses pada RAM DDR2.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Forensik merupakan kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan kejadian kriminal dan permasalahan hukum lainnya. Komputer forensik merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital (komputer, handphone, tablet, PDA, *networking devices*, *storage*, dan sejenisnya) (Rahardjo, 2013). 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. Ada beberapa teknik didalam komputer forensik salah satunya adalah *memory forensics* atau biasa disebut *live forensics* yang digunakan untuk pendekatan terhadap sistem komputer yang sedang bekerja dan terhubung pada jaringan komputer.

Live forensics merupakan sebuah proses dalam upaya mendapatkan informasi dan data yang terdapat dalam memori pada sebuah sistem yang sedang berjalan dan akan hilang ketika sistem tersebut dimatikan (Kurniawan dan Prayudi, 2014). *Live forensics* merupakan repson dari kekurangan teknik forensik tradisional yang bisa mendapatkan informasi dari data dan informasi yang hanya ada ketika sistem sedang

berjalan misalnya aktifitas *memory, network proses, swap file, running system proses,* dan informasi dari sistem dan ini menjadi kelebihan dari teknik *live forensics* (Lessing dan Solms, 2008). Dalam banyak kasus, data penting yang berkaitan dengan serangan atau ancaman hanya akan ada dalam memori sistem seperti koneksi jaringan, kredensial akun, proses yang berjalan dan riwayat internet yang tidak dapat di *chace* yang ditulis langsung ke memori fisik komputer atau biasa disebut *random access memory* (RAM).

Random Access Memory atau biasa disingkat dengan RAM merupakan sebuah tipe penyimpanan komputer yang isinya dapat diakses dalam waktu yang tepat tidak memperdulikan letak data tersebut dalam memori. RAM juga merupakan salah satu penyimpanan yang bersifat *volatile* atau data akan hilang saat tidak terdapat aliran listrik. Sedangkan data *volatile* yang terdapat pada RAM sangat berguna untuk forensic, karena RAM pada sistem komputer menggambarkan seluruh kegiatan yang telah terjadi pada sistem tersebut (Wijaya, 2016).

Berdasarkan permasalahan di atas, maka penulis melakukan mengenai *methodology digital forensic* terkhusus pada bagian *memory forensic*. Adapun hasil yang diharapkan dari penelitian ini memberikan gambaran bukti-bukti *forensic* yang bisa diperoleh dari *random access memory*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka dapat dirumuskan masalahnya sebagai berikut:

1. Bagaimana mengakuisi data pada *random access memory?*
2. Data apa saja yang tersimpan dalam *random access memory?*
3. Bagaimana keakuratan data hasil dari forensik *memory* dengan menggunakan beberapa variasi skenario kasus yang diujikan?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini adalah sebagai berikut:

1. Mampu melakukan akuisi data pada *random access memory.*
2. Mengetahui data apa yang tersimpan dalam *random access memory.*
3. Mengetahui keakuratan data hasil dari forensik *memory* dengan menggunakan beberapa variasi skenario kasus yang diujikan?

1.4 Ruang Lingkup Penelitian

Guna menghindari pembahasan yang meluas, maka penelitian ini memiliki batasan sebagai berikut:

1. Fokus penelitian pada proses identifikasi dalam *analysis methodology digital forensic.*
2. Lingkungan pengujian pada RAM DDR2 dan RAM DDR3.
3. Tidak membahas secara mendalam cara kerja *malware* dan *tools* penyerang.

4. Tidak membahas secara mendalam cara kerja dari *random access memory*.
5. Kecurigaan investigator terhadap bukti yang dicurigai bersifat tidak alami, karena pihak yang berperan sebagai penyerang dan investigator adalah orang yang sama.
6. *Tools* yang digunakan bersifat *opensource*.
7. Adapun detail lingkup penelitian terdapat pada BAB III.

1.5 Manfaat Penelitian

Adapun manfaat penelitian ini adalah sebagai berikut:

1. Menambah wawasan pengguna komputer tentang aktivitas yang bisa diungkap berdasarkan data-data yang telah diakuisisi *tools forensic.*
2. Mengungkap langkah efektif dalam mengidentifikasi *memory forensics*.

BAB II

TINJAUAN PUSTAKA

2.1 Digital Forensic

Forensik merupakan kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan kejadian kriminal dan permasalahan hukum lainnya. Forensik digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital (komputer, handphone, tablet, PDA, *networking devices*, *storage*, dan sejenisnya) (Rahardjo, 2013).

Forensik digital dapat dibagi lebih jauh menjadi forensik yang terkait dengan komputer (*host, server*), jaringan (*network*), aplikasi (termasuk database), dan perangkat (*digital devices*) (Rahardjo, 2013). Masing-masing memiliki pendalaman tersendiri. Pada forensik komputer, fokus penyidikan terkait dengan data yang berada atau terkait dengan komputer itu sendiri. Layanan yang disediakan oleh komputer atau server biasanya tercatat dalam berbagai berkas log. Sebagai contoh, pengguna yang gagal masuk karena salah memasukkan password akan tercatat. Bisa jadi ini merupakan bagian dari upaya untuk melakukan penerobosan akses dengan cara *brute force password cracking*. Di sisi desktop, pengguna memasukkan flashdisk ke port USB juga tercatat.

Forensik komputer ini bergantung kepada sistem operasi yang digunakan. Sebagai contoh, kebanyakan pengguna komputer desktop menggunakan sistem

operasi Microsoft Windows. Oleh sebab itu diperlukan kemampuan untuk melakukan forensik pada komputer yang menggunakan sistem operasi Microsoft Windows (Carvey, 2005). Sistem operasi yang lain meletakkan data di berkas yang berbeda dengan format yang berbeda. Sebagai contoh di sistem UNIX catatan tersedia pada layanan *Syslog*, sementara itu di sistem Microsoft Windows catatan dapat dilihat dengan *Event Viewer*. Berbagai *tools* forensik tersedia untuk membantu penyidik dalam mengumpulkan data yang terkait dengan sistem operasi yang digunakan.

Bukti-bukti komputer mulai masuk kedalam dokumen resmi hukum lewat *US Federal Rules of Evidence* pada tahun 1976 (Suprapto, 2012). Selanjutnya dengan berbagai perkembangan yang terjadi muncul beberapa dokumen hukum lainnya, antara lain adalah:

a. *The Electronic Communications Privacy Act* 1986, berkaitan dengan penyadapan peralatan elektronik.
b. *The Computer Security Act* 1987 (*Public Law* 100-235), berkaitan dengan keamanan sistem komputer pemerintahan.
c. *Economic Espionage Act* 1996, berhubungan dengan pencurian rahasia dagang.

Di Indonesia sendiri sebenarnya komputer forensik sudah muncul cukup lama. Hal ini ditandai dengan keluarnya undang-undang Informasi dan transaksi elektrronik (UU ITE) pada tahun 2008. Dijelaskan bahwa barang bukti digital sudah bisa

dianggap sebagai alat bukti sah di pengadilan. Secara tertulis, menurut pasal 5 UU No. 11/2008 tersebut diatas menyebutkan bahwa "informasi elektronik dan atau dokumen elektronik dan atau hasil cetaknya merupakan alat bukti hukum yang sah".

Sementara itu fokus data yang dikumpulkan dalam digital forensik dapat dikategorikan menjadi 3 domain utama, yaitu:

(i) *Active Data* yaitu informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun file yang dikendalikan oleh sistem operasi;

(ii) *Archival Data* yaitu informasi yang telah menjadi arsip sehingga telah disimpan sebagai backup dalam berbagai bentuk alat penyimpan seperti hardisk eksternal, CD ROM, *backup tape*, DVD, dan lain-lain; dan

(iii) *Latent Data* yaitu informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (*corrupted file*), dan lain sebagainya.

Menurut Wright (2001) penyelidikan sebaiknya dimulai bila sebuah rencana telah terumuskan dengan baik. Maka landasan metodologi akan memetakan kontruksi ilmiah dalam menyelesaikan sebuah pekerjaan. Demikian juga dalam komputer forensik, metodologi diharapkan akan membantu tercapainya hasil yang dituju. Walaupun tidak ada standard baku, namun terdapat sejumlah tahapan yang sebaiknya dilakukan dalam proses komputer forensik (Prayudi dan Afrianto 2007), yaitu: menentukan tujuan, memproses fakta, dan mengungkapkan bukti digital.

Tujuan diperlukan sebagai pengarah akhir dari sebuah investigasi. Dalam hal ini sebuah tujuan sebaiknya juga dideskripsikan dalam bentuk parameter-parameter kesuksesan dalam menginvestigasi kejadian. Dengan adanya parameter tersebut maka akan diketahui kapan hasil dari inverstigasi telah berakhir.

2.2 *Live Forensic*

Live forensics merupakan sebuah proses dalam upaya mendapatkan informasi dan data yang terdapat dalam memori pada sebuah sistem yang sedang berjalan dan akan hilang ketika sistem tersebut dimatikan (Kurniawan dan Prayudi, 2014). *Live Forensics* pada dasarnya memiliki kesamaan pada teknik forensik tradisonal dalam hal metode yang dipakai yaitu identifikasi, penyimpanan, analisis, dan presentasi, hanya saja *live forensics* merupakan respon dari kekurangan teknik forensik tradisonal yang tidak bisa mendapatkan informasi dari data dan informasi yang hanya ada ketika sistem sedang berjalan misalnya aktifitas *memory, network proses*, *swap file, running system proses*, dan informasi dari file sistem dan ini menjadi kelebihan dari teknik *live forensics* (Lessing dan Solms, 2008).

Teknik *live forensics* ini sangat bergantung pada keadaan komputer yang sedang menyala, karena membutuhkan data yang berjalan pada *Random Access Memory* (RAM). Data pada RAM disebut juga *data volatile* atau data sementara yaitu data yang hanya terdapat saat komputer menyala jika komputer mati maka data itu akan hilang. *Data volatile* ini berisi data penting seperti *username*, *password*, file

akses, file modifikasi, aplikasi yang digunakan, kata kunci pencarian (Faiz, 2016). Dalam analisis *live forensics*, baik proses pengumpulan bukti dan analisis itu sendiri berlangsung pada saat yang sama, jadi mungkin akan sulit untuk mengenali apakah nilai data yang diakuisisi adalah legal atau sebaliknya.

Meskipun *live forensic* mungkin tidak menghasilkan hasil yang dapat diandalkan, namun akan sangat membantu dalam banyak kasus. Misalnya, jika beberapa komputer terlibat dalam serangan dan penyidik ingin mengidentifikasi *state* masing-masing sistem maka *live forensic* adalah cara yang paling cocok (Carrier, 2006). Rahman dan Khan (2015) mengusulkan suatu model untuk analisis langsung oleh memecahnya menjadi tahapan yang berbeda seperti mengumpulkan bukti-bukti, memeriksa barang bukti, menganalisisnya dan akhirnya menghasilkan laporan. Model ini didasarkan pada memori fisik atau memori image.

Karena peningkatan pesat dalam ukuran memori, para peneliti forensik menyarankan pendekatan respon langsung untuk akuisisi bukti *volatile* (Rahman dan Khan, 2015). Melalui teknik ini penyidik dapat mengumpulkan tidak hanya informasi tentang proses berjalan tetapi juga tentang proses dihentikan dan *cache*. Analisis *volatile* menjadi bagian penting dari penyelidikan karena memori fisik bisa memiliki bukti potensial yang penyidik tidak dapat menemukan pada penyimpanan disk. Untuk mendapatkan kejadian, akuisisi data volatile adalah langkah awal dalam penyelidikan digital. Biasanya penyidik mengumpulkan data *volatile* melalui respon langsung,

sementara penyerang mungkin menggunakan perpustakaan yang berbeda untuk membuat sistem panggilan untuk terhubung ke kernel dan mengubah data volatile.

Pendekatan *memory image analysis* juga digunakan untuk menyelidiki data volatile dari sistem target. Pendekatan ini bisa berfungsi sebagai alternatif untuk *live response*. Menggunakan *tool - tool* administrasi, pemeriksa dapat memperoleh semua informasi yang stabil dalam memori termasuk informasi proses dihentikan. Teknik virtualisasi juga digunakan dalam forensik digital (Mrdovic dkk, 2009). Dalam pendekatan virtualisasi, setelah mendapat *memory image* dan urutan *imaging* hardisk boot / mekanisme sistem target, duplikat copy target hardisk dipasang pada mesin virtual.

2.3 Forensik Memori

Forensik memori adalah arah penelitian yang baru namun berkembang dengan cepat, dan menjanjikan satu dibidang *forensic*. Sedangkan forensik tradisional melibatkan studi penyimpanan data persisten seperti hardisk dan penyimpanan USB, yang juga dikenal sebagai *dead-box-analysis* (Amari, 2009). Forensik memori melibatkan pengambilan dan analisis memori *volatile* seperti RAM.

Data dianggap tidak stabil dan kemungkinan akan hilang ketika mesin di-reboot atau data akan ditimpa selama penggunaan mesin normal. Karena data tidak stabil, seringkali data tidak terstruktur dengan cara yang sama seperti file sistem, dan bisa juga lebih sulit diprediksi dan diurai menjadi data yang berarti sebagai hasilnya.

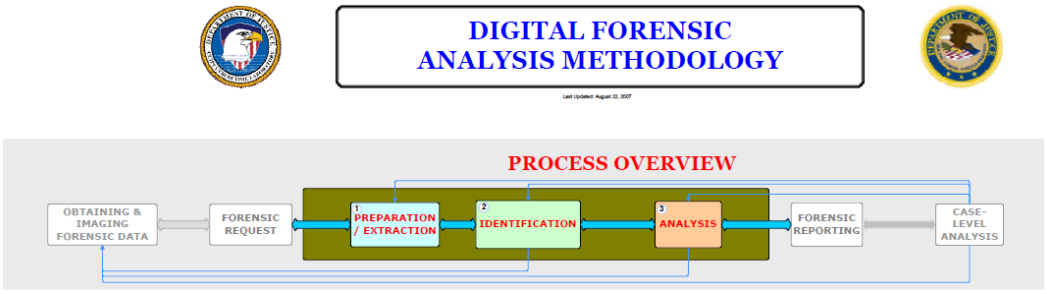
Seringkali, barang bukti dapat dipulihkan dari data yang mudah hilang yang sangat berharga dalam membantu penyelidikan dalam semua bidang, dan banyak barang bukti hanya dapat dipulihkan dari memori.

Analisis dari setiap memori *volatile* yang ditangkap oleh responden kejadian saat ini adalah cara yang kurang tepat dari pada analisis hardisk. Hardisk memiliki struktur yang telah ditetapkan secara ketat, dan analisis mengetahui di mana harus mencari struktur dan tipe data tertentu pada jenis file sistem tertentu (misalnya FAT32). Di sisi lain, memori dapat dialokasikan dan dialokasikan ulang ke berbagai area tergantung pada memori yang digunakan, untuk semua maksud dan tujuan tidak mungkin untuk memprediksi apa yang akan ditemukan dalam memori yang mudah hilang atau di tempat mana file itu akan disimpan (Amari, 2009).

Dengan mudah terlihat bahwa memperoleh dan menganalisis jenis data ini lebih menantang dan berbahaya dari pada *dead-box-analysis*. Karena pendekatan yang kurang terstruktur terhadap penyimpanan dan kecepatan di mana memori *volatile* dimodifikasi analisi harus lebih berhati-hati saat *capture* data dan menguraikannya. Hampir setiap tindakan yang dilakukan pengguna di komputer mengubah memori pada mesin, yang menyebabkan hasil tidak terduga dalam *capture* yang dihasilkan (Amari, 2009).

Belum ada format atau standar khusus yang mengikat dalam proses penyelidikan dengan metode *live forensics*. Namun demikian, tahapan penyelidikan

yang digunakan kurang lebih sama dengan investigasi digital yang telah diterapkan di *United States Department Of Justice Executive Office For United States Attorneys*.



Gambar 2.1 *Digital Forensic Analysis Methodology*

Terdapat 3 hal utama dalam metodologi digital forensik (Carollet dan Basten, 2008), yaitu:

1. *Preparation / Extraction*

Hal yang perlu diperhatikan ialah validasi perangkat.Semua perangkat baik berupa perangkat keras dan perangkat lunak, harus dipastikan bahwa mereka bekerja dengan baik.Masih terdapat perdebatan mengenai seberapa sering perangkat lunak ataupun peralatan harus diuji.Namun, validasi sebaiknya dilakukan setelah pembelian perangkat dan sebelum perangkat tersebut digunakan. Kemudian, perangkat harus divalidasi lagi setelah mengalami *update* atau konfigurasi ulang.Ketika perangkat siap maka masuk ke proses akuisisi data. Barang bukti yang telah disita akan di akuisisi dengan mengunakan teknik *forensic imaging* atau yang sering disebut dengan metode kloning, di mana mengkopi data sama persis dengan aslinya. Cara tersebut dilakukan untuk menghindari perubahan bukti asli pada saat proses analisis. Dengan

kloning, barang bukti hasil duplikasi ini akan 100 persen identik dengan barang bukti yang asli.

2. *Identification*

Pada tahap ini, akan dilakukan identifikasi data yang telah diakuisisi. Hal yang perlu diperhatikan pertama ialah memastikan bahwa data yang telah diperoleh mempunyai korelasi dengan laporan yang terima. Apabila data yang telah diperoleh ternyata informasi di dalamnya tidak mempunyai korelasi dengan laporan yang diterima maka seluruh aktivitas harus segera dihentikan. Kemudian melakukan komunikasi dengan pelapor dan menunggu instruksi lebih lanjut. Misalnya, penegak hukum melakukan penyitaan komputer untuk membuktikan penipuan pajak, tetapi pemeriksa menemukan gambar pornografi anak. Yang paling bijaksana dilakukan adalah menghentikan pencarian atau memperluas cangkupan penyelidikan pada surat perintah. Pemeriksa juga berkawajiban untuk meminta surat perintah baru. Misalnya, setelah dilakukan identifikasi ternyata terdapat indikasi penyalinan data oleh orang tertentu yang sebenarnya tidak mempunyai hak mengakses secara langsung komputer tersebut, maka pemeriksa berkeinginan untuk memeriksa data rekaman video di gedung tersebut.

3. *Analisis*

Pada tahap analisis, pemeriksa menghubungkan semua titik-titik dan melukiskan gambaran yang lengkap untuk pelapor. Untuk setiap *item* pada data yang

relevan, penguji menjawab pertanyaan seperti siapa, apa, kapan, di mana, dan bagaimana. Pemeriksa harus bisa menjelaskan apa yang telah dilakukan mulai dari awal hingga akhir oleh pelaku. Sehingga pada tahap ini, pemeriksa mengamati dan menjelaskan urutan peristiwa dan catatan yang peristiwa yang terjadi bahkan dalam waktu yang sama. Penguji juga menjelaskan di mana mereka menemukannya. Yang paling penting, mereka menjelaskan mengapa semua informasi ini penting dan apa artinya untuk kasus ini. Pemeriksa juga harus mendokumentasikan semua analisis mereka, dan informasi lain yang relevan dengan permintaan pelapor, dan menambahkan itu semua ke dalam sebuah daftar untuk di laporkan.

2.4 Data Yang Ditemukan Forensik Memori

Ada banyak data yang tersedia dalam memori volatile seperti Proses, informasi tentang *registry handle*, *password*, informasi jaringan dan kunci kriptografi, dan *malicious code* (Amari, 2009). Berikut akan dibahas secara terperincih tentang jenis informasi apa yang dapat dipulihkan melalui forensik memori.

2.4.1 Proses

Ada beberapa jenis proses yang berbeda yang mungkin ditemukan pada memori *volatile*. Semua proses yang masih berjalan disimpan di memori dan dapat dipulihkan dari struktur data tempat data tersebut disimpan (Amari, 2009). Selain itu, proses yang telah dihentikan mungkin masih berada di memori karena mesin belum

di reboot sejak diakhiri dan ruang yang berada di dalamnya belum direalokasi. Ini juga bisa diuraikan dan dianalisis.

2.4.2 *Registry Handle*

File yang prosesnya terbuka serta *registry handle* yang diakses oleh sebuah proses, juga tersimpan dalam memori, informasi tentang file yang digunakan oleh sebuah proses dapat sangat berharga. Jika prosesnya adalah virus malware, *registry handle* dapat menyebabkan penyidik menemukan tempat penyimpanan virus malware dimana virus tersebut menulis ouputnya, atau file yang sebelumnya bersih yang mungkin berubah karena virus malware untuk menjalankan tujuan virus itu sendiri (Amari, 2009).

2.4.3 *Network Information*

Informasi tentang koneksi jaringan, termasuk *listening ports*, koneksi yang *estabilished*, informasi IP *address local*, dan IP *address remote access* dapat dipulihkan dari memori (Amari, 2009). Hal ini berguna karena *tool* yang dijalankan pada mesin itu sendiri sebagai netstat, penyusup dapat berbahaya pada pengguna untuk memberikan informasi palsu. Ketika mengambil informasi langsung dari memori dump menggunakan data struktur sendiri, itu jauh lebih sulit bagi penyerang untuk menyembunyikan backdoor penyusup, atau koneksi ke alamat server penyusup yang mana penyusup mentransfer malware dan file berbahaya atau file illegal lainnya (Amari, 2009). Informasi koneksi jaringan merupakan salah satu bagian yang paling

penting dari informasi yang bisa dipetik dari komputer yang sedang diselidiki, dan lebih dapat diandalkan ketika berasal dari analisis statis memori dump.

2.4.4 *Password dan Cryptographic Keys*

Salah satu keuntungan besar dari forensik memori adalah potensi pemulihan kata sandi pengguna dan kunci kriptografi yang dapat digunakan untuk mendekripsi file yang diminati dan mengakses akun pengguna. Aturan umum kata sandi dan kunci kriptografi adalah *password* tidak pernah tersimpan pada hardisk tanpa beberapa jenis pengamanan (Amari, 2009). Ketika *password* digunakan, entah bagaimana, *password* harus disimpan pada memori *volatile* dan ini terjadi sekali, maka *password* akan tetap berada dalam memori sampai *password* ditimpa oleh data lain atau mesin di reboot.

2.4.5 *Malicious Code*

Baru-baru ini semakin popular bagi penyerang untuk menjalankan eksploitasi dengan memori dari pada menyimpan kode berbahaya pada hardisk itu sendiri. Hal ini dilakukan untuk menghindari deteksi dari anti-virus dan alat pendeteksi malware atau virus lainnya. Hal ini terutama untuk menghindari deteksi, karena perangkat lunak anti-virus dan *tool* deteksi malware saat ini tidak sebaik menganalisis memori *volatile* untuk kode berbahaya karena yang dianalisis adalah hardisk, dan beberapa di antaranya sama sekali tidak memiliki kemampuan ini (Amari, 2009).

2.5 *Random Access Memory*

RAM adalah komponen penyimpanan utama atau sekunder yang ada pada komputer, ram mampu menyimpan data dari proses yang sedang berlangsung. Jadi sifat penyimpanan memori ram hanya bersifat sementara, ini sangat berbeda dengan memori penyimpanan hardisk (Rajif, 2006).

RAM juga menjadi penentu kelangsungan kinerja komputer, karena setiap proses dalam sistem komputer akan selalu melibatkan memori Utama sebagai Hardware yang melayani CPU.

2.5.1 RAM DDR2

RAM DDR2 adalah memory yang paling banyak beredar saat ini di pasaran, terbukti komputer ber-pentium 4 ke atas banyak menggunakan jenis memory ini. Penggunaan ini banyak di pergunakan karena memory jenis ini hanya membutuhkan daya listrik sebesar 1,8Volt sehingga dapat menghemat performa listrik/ tegangan yang masuk ke komputer, RAM jenis ini di kembangkan pada tahun 2005 (Rajif, 2006). Adapun spesifikasi dari RAM DDR2 yaitu sebagai berikut:

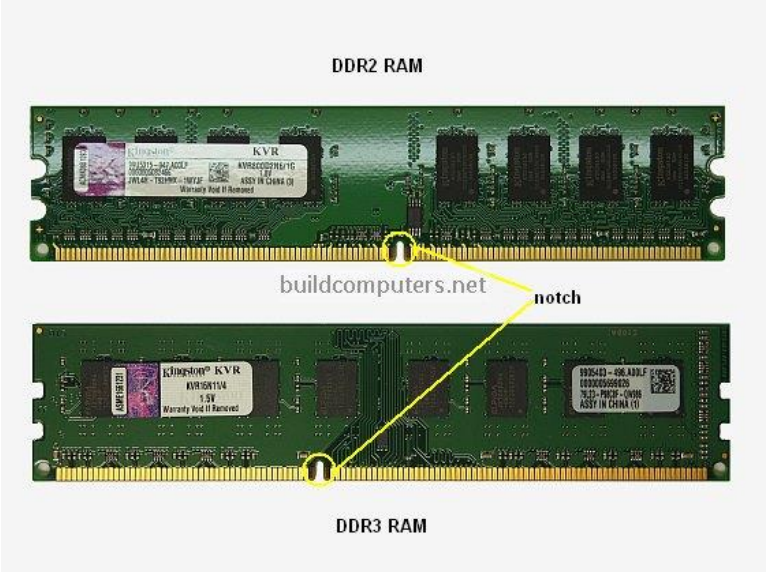
a. Memerlukan Voltase 1.8V
b. Frekuensi transfer 400MHz sampai 1066MHz
c. Nama standar DDR2-400, DDR2-533, DDR2-677, DDR2-800, dan DDR2-1066

2.5.2 RAM DDR3

Pada tahun 2007 akhir Intel mengembangkan memory dengan label DDR3, dengan pengunaan daya listrik 1,5Volt membuat memory jenis ini lebih memukau karena kecepatan membacanya sangat cepat dibanding beberapa memory hasil evolusi RAM sebelumnya (Rajif, 2006). Adapun spesifikasi dari RAM DDR3 yaitu sebagai berikut:

a. Memerlukan Voltase 1.5V
b. Frekuensi transfer hingga 2133 MHz
c. Lebih hemat
d. Harga lebih mahal daripada DDR2
e. Latensi yang lebih unggul
f. Kemampuan untuk mentransfer I / O data di delapan kali data tingkat memori berisi sel

Selain perbedaan RAM DDR2 dan RAM DDR3 dari segi spesifikasi, pada bagian hardware atau bentuk juga berbeda. Terlihat pada bagian notch. notch adalah bagian ram yang terdapat celah pada pin.



Gambar 2.2 Perbedaan RAM DDR2 dan RAM DDR3

a. DDR2 bagian notch terletak sedikit ke arah sisi kanan.
b. DDR3 bagian notch terletak sedikit lebih ke tengah board modul memori.
c. DDR3 yang terbaru saat ini notchnya terletak sedikit kearah kiri berlawanan dengan letak notch DDR pertama.
d. DDR2 dan DDR 3 memiliki pin yang lebih kecil dan padat Jumlahnya 240 buah (120-pin di setiap sisi).

Karena DDR2 dan DDR3 mempunyai bentuk yang berbeda maka jika komputer Anda menggunakan DDR2 sudah dipastikan tidak bisa digunakan DDR3 begitu juga sebaliknya. Kecuali motherboard komputer Anda support DDR2 dan DDR3.

Keuntungan Utama RAM DDR3 adalah kemampuan untuk mentransfer I / O data didelapan kali data tingkat memori berisi sel, sehingga memungkinkan bus lebih

tinggi dan harga lebih tinggi pula dari harga sebelumnya puncak teknologi memori. Selain itu, standar RAM DDR3 memungkinkan chip kapasitas 512 megabits hingga 8 gigabits, efektif memungkinkan maksimum ukuran modul memori 16 gigabyte. Keuntungan lainnya, memori RAM DDR3 memberikan pengurangan konsumsi daya lebih dari 30% dibandingkan RAM DDR2 dan RAM DDR1 modul karena RAM DDR 3 kurang dari 1,5 V pasokan tegangan, dibandingkan dengan RAM DDR2 dan DDR 1 dari 1,8 V atau 2,5 V. Pasokan tegangan bekerja dengan baik dengan 90 nanometer pembuatan teknologi yang digunakan dalam RAM DDR3.

2.6 *Live forensic tools*

Pada saat ini ada beberapa *tools* yang tersedia untuk analisa forensik memori yang dijelaskan dan dianalisis. Analisis ini berfokus pada *tools* yang tersedia secara gratis yang dapat diperoleh dan digunakan untuk analisa.

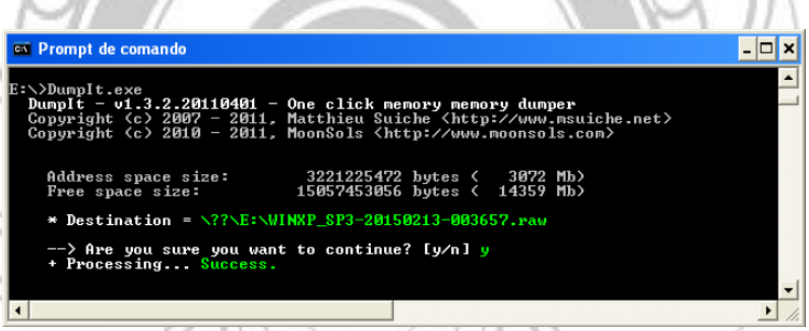
Cara lain untuk menguji *tool* baru adalah dengan menggunakan *tool* serupa yang telah terbukti bekerja dengan benar sebagai dasar perbandingan sehingga analis dapat mengetahui apakah *tool* tersebut kehilangan informasi penting atau memberikan bukti digital yang positif.

2.6.1 DumpIt

DumpIt adalah perpaduan dua *tool* terpercaya, win32dd dan win64dd digabungkan menjadi satu executable. Pengguna hanya perlu mengklik dua kali DumpIt yang dapat dieksekusi dan membiarkan *tool* itu berjalan. DumpIt kemudian

akan mengambil snapshot dari memori fisik dan menyimpannya difolder tempat eksekusi DumpIt berada (Borges, 2015).

DumpIt menyediakan cara mudah untuk mendapatkan *image memory* dari sistem Windows bahkan jika penyidik tidak secara fisik duduk didepan komputer target. Ini sangat mudah digunakan bahkan pengguna awampun bisa melakukannya. Ini tidak sesuai semua skenario, tapi pasti akan membuat perolehan memori lebih mudah dalam banyak situasi (Borges, 2015). Adapun contoh tampilan DumpIt seperti pada Gambar 2.3.



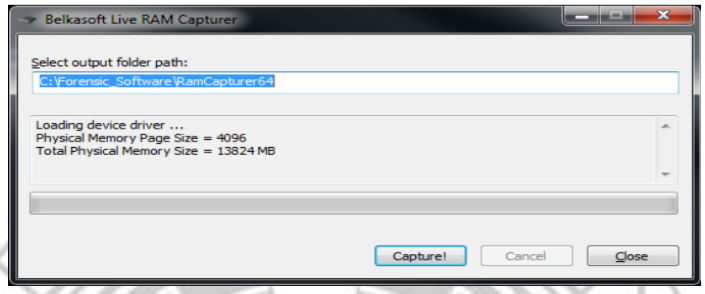
Gambar 2.3 Proses Dumpit

2.6.2 Belkasoft RamCapture

Live RamCapture adalah tool kecil dan sangat kuat untuk memperoleh memori pada sstem seperti windows XP, windows 7, windows 8, windows 2003, windows 2008 dan sebagainya (Borges, 2015).

Live RamCapture adalah fitur yang sangat baik serta mampu mengelolah memori dari sistem dengan anti-debugging dan anti-memori dumping. *Image* yang diakuisis oleh *tool* Belkasoft RamCapture dan dapat dianalisis dengan Volatility

(Borges, 2015). Live RAM capturer 64-bit disusun oleh dua file (RamCapture64.exe dan RamCaptureDriver64.sys) dan untuk memperoleh memori dengan cara seperti pada Gambar 2.4.



Gambar 2.4 Memperoleh Memori Pada RamCapture

BAB III

METODE PENELITIAN

3.1 Waktu dan Tempat Penelitian

Tempat penelitian ini adalah Lab. CAIR, Politeknik Negeri Ujung Pandang, KM.10, Jalan Perintis Kemerdekaan, Tamalanrea, Makassar. Sedangkan waktu pengerjaan penelitian ini adalah semester ganjil tahun ajaran 2016/2017 yaitu dimulai dari bulan Januari 2017.

3.2 Kebutuhan Perangkat Penelitian

Kebutuhan sistem yang digunakan untuk penelitian ini terbagi menjadi dua yaitu perangkat keras dan perangkat lunak sebagai berikut.

1. Kebutuhan perangkat keras (Hardware)
    a. Lenovo G40-45, Memori RAM DDR3
    b. Acer Aspire 4736 Series, Memori RAM DDR2
2. Kebutuhan perangkat lunak (software)
    a. Sistem Operasi Windows 7 Ultimate
    b. volatility-2.4.standalone
    c. Belkasoft RamCapture versi 32bit
    d. DumpIt v1.3.2
    e. Winhex v19.3 SR-4 32bit
    f. VMware v10.0.7

3.2 Tahapan Penelitian

Tahapan penelitian diperlukan agar penelitian yang dilakukan dapat terstruktur sehingga hasil yang diperoleh sesuai dengan tujuan penelitian. Adapun prosedur penelitian yang akan dilakukan untuk mencapai hasil yang diinginkan seperti pada Gambar 3.1.

Gambar 3.1 Diagram Tahapan Penilitian

Diagram alur digunakan agar lebih memudahkan dan memberikan gambaran jelas mengenai tahapan yang akan dilakukan. Berikut ini adalah penjelasan dari tahapan penelitian yang akan dilakukan.

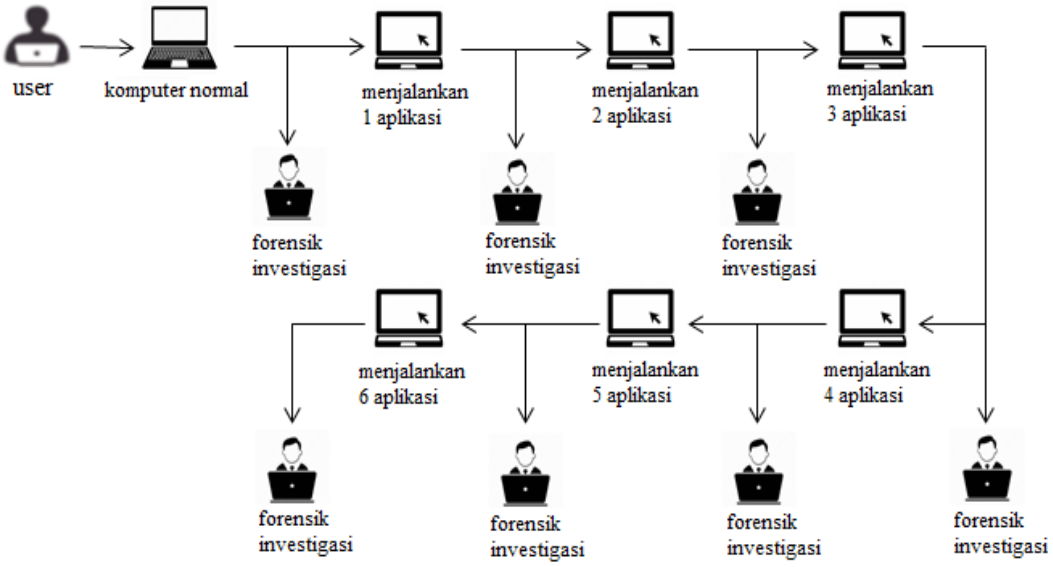
1. Studi Literatur

Tahapan awal yakni studi literatur dan pemahaman dasar teori melalui pengumpulan referensi dimana data-data dapat diperoleh dari hasil membaca buku, jurnal penelitian serta referensi-referensi yang dianggap relevan dan berhubungan dengan judul yang diangkat. Studi literatur dilakukan untuk lebih memahami metode live forensic pada random access memory. Sebagian besar informasi yang diperoleh pada tahapan ini akan menjadi bahan evaluasi pada akhir penelitian.

2. Desain Skenario

Pada tahap ini, langkah yang dilakukan adalah mendesain skenario uji coba yang didesain sedemikian rupa agar menyerupai kondisi yang mungkin terjadi di lapangan. Skenario tersebut kemudian dipaparkan terhadap *Random Access Memory* untuk kemudian dilakukan uji coba ekstraksi data pada kondisi tersebut. Adapun skenario tersebut adalah sebagai berikut :

a) Pemeriksaan RAM saat aplikasi dijalankan



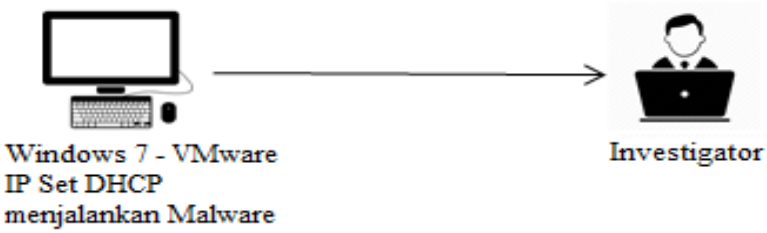
Gambar 3.2 Skenario Pemeriksaan RAM Saat Aplikasi Dijalankan

Pada skenario ini komputer yang telah disiapkan tersebut dengan menggunakan RAM DDR2 dan RAM DDR3 akan diperiksa berapa jumlah proses yang berjalan, berapa jumlah proses *registry handles* yang terlihat, dan jumlah informasi jaringan yang tercatat. Adapun beberapa prosedur yang dilakukan pada komputer yaitu:

1) Komputer normal yaitu komputer dalam keadaan baru sudah diinstall dan tidak menjalankan aplikasi kemudian RAM akan diakuisisi dengan cara *image memory* menggunakan *tools* Dumpit dan Belkasoft RamCapture.
2) Menjalankan 1 aplikasi yaitu komputer dalam keadaan baru dinyalakan kemudian menjalankan aplikasi Winrar. Selanjutnya RAM diakuisisi dengan melakukan *image memory* menggunakan *tools* Dumpit dan Belkasoft RamCapture.
3) Menjalankan 2 aplikasi yaitu komputer dalam keadaan baru dinyalakan kemudian menjalankan aplikasi Winrar dan menjalankan Media Player Classic. Selanjutnya RAM diakuisisi dengan melakukan *image memory* menggunakan *tools* Dumpit dan Belkasoft RamCapture.
4) Menjalankan 3 aplikasi yaitu komputer dalam keadaan baru dinyalakan kemudian menjalankan aplikasi Winrar, menjalankan Media Player Classic, dan menjalankan AIMP Player. Selanjutnya RAM diakuisisi dengan melakukan *image memory* menggunakan *tools* Dumpit dan Belkasoft RamCapture.

5) Menjalankan 4 aplikasi yaitu komputer dalam keadaan baru dinyalakan kemudian menjalankan aplikasi Winrar, menjalankan Media Player Classic, menjalankan AIMP Player, dan membuka Foxit Reader. Selanjutnya RAM diakuisisi dengan melakukan *image memory* menggunakan *tools* Dumpit dan Belkasoft RamCapture.
6) Menjalankan 5 aplikasi yaitu komputer dalam keadaan baru dinyalakan kemudian menjalankan aplikasi Winrar, menjalankan Media Player Classic, menjalankan AIMP Player, membuka Foxit Reader, dan menjalankan Google Chrome dengan penelusuran *digital forensic* dan *plugin volatility*. Selanjutnya RAM diakuisisi dengan melakukan *image memory* menggunakan *tools* Dumpit dan Belkasoft RamCapture.
7) Menjalankan 6 aplikasi yaitu komputer dalam keadaan baru dinyalakan kemudian menjalankan aplikasi Winrar, menjalankan Media Player Classic, menjalankan AIMP Player, membuka Foxit Reader, menjalankan Google Chrome dengan penelusuran *digital forensic* dan *plugin volatility* dan menjalankan Mozilla Firefox dengan penelusuran *digital forensic* dan *plugin volatility*. Selanjutnya RAM diakuisisi dengan melakukan *image memory* menggunakan *tools* Dumpit dan Belkasoft RamCapture.

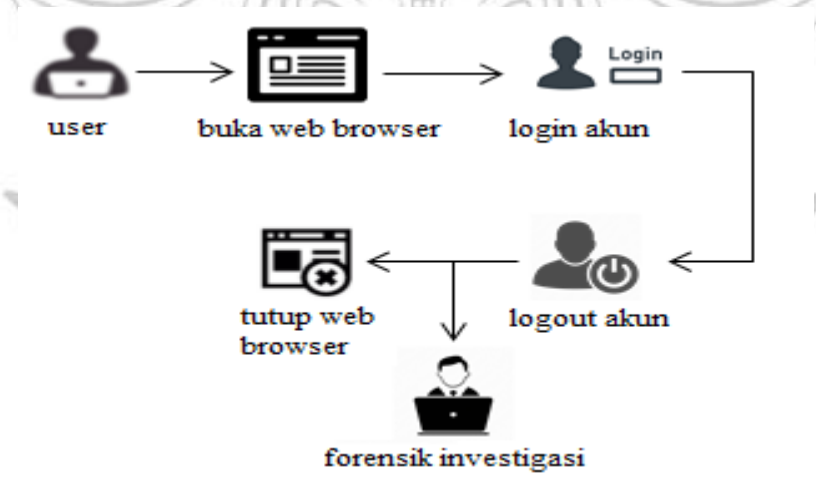
b) *Malicious code*



Gambar 3.3 Skenario *Malicious Code*

Pada pengujian *malicious code* pada RAM DDR2 dan RAM DDR3 dilakukan pada VMware untuk menjaga kejadian hal-hal yang tidak di inginkan. Pada pengujian ini dilakukan dengan menjalankan *malware* yang sudah ditentukan kemudian mengakuisisi RAM dengan melakukan *image memory* menggunakan *tools* Belkasoft RamCapture.

c) *Password* Log-in Pada Beberapa *Social Media*



Gambar 3.4 Skenario *Password*

Pencarian bukti digital dilakukan dengan menggunakan browser *Google Chrome* dengan log-in ke akun *social media* selanjutnya log-out dari akun *social media* kemudian mengakuisisi RAM dengan menggunakan *tools* Belkasoft RamCapture.

3. Implementasi

Pada tahapan ini dilakukan untuk pengujian skenario yang telah ditentukan dengan mencari informasi dan barang bukti dalam sebuah RAM. Dalam hal ini menghadapi keadaan dimana komputer atau alat bukti yang ditemui ditempat kejadian perkara terhubung pada sebuah jaringan komputer dan dalam keadaan power on. Mengaplikasikan skenario yang telah ditentukan sebelumnya kemudian melakukan *collection & acquisition* yaitu mengumpulkan barang bukti yang di dapat termasuk melakukan *imaging* pada RAM.

4. Analisis Data

Pada tahap ini peneliti melakukan analisa dari pengujian yang sudah dilakukan untuk memperoleh data maupun informasi yang dibutuhkan sesuai dengan tujuan penelitian. Selain itu, data atau informasi hasil pengujian yang dievaluasi akan dijadikan sebagai bahan dalam pembuatan dokumen sebagai produk akhir dalam penelitian. Masalah yang ditemukan dalam proses penelitian ini turut dijadikan sebagai data hasil penelitian agar memudahkan pembaca untuk pengembangan penelitian ini berikutnya.

Adapun analisis yang dapat dilakukan terdapat pada tahapan verifikasi extraksi data *random access memory* yaitu :

1. Membandingkan data diekstraksi dari 2 tipe RAM yang berbeda, akan dilakukan pemeriksaan apakah setiap data yang diambil pada RAM DDR 2 dan RAM DDR 3 akan sama dengan jumlah data yang di dapatkan oleh setiap tools dan membandingkan hasil yang di dapat dan memastikan akurasinya.
2. Identifikasi bukti digital, tahapan selanjutnya adalah melakukan pengecekan dan indentifikasi terhadap bukti digital untuk mendapatkan informasi antara lain mengenai proses yang di dapat, analisis terhadap aktivitas *network* yang terjadi saat sistem bekerja, dan menganalisis hasil data yang di dapat.

5. Hasil

Pada tahap terakhir ini, peneliti menyusun hasil penelitian dengan data-data yang sudah diperoleh dengan menarik sebuah kesimpulan dari semua kegiatan penelitian.

BAB IV

HASIL DAN PEMBAHASAN

Pada penelitian ini difokuskan untuk mengakuisisi bukti digital pada *random access memory* (RAM) dalam 3 skenario pengujian. 3 skenario pengujian tersebut meliputi pemeriksaan RAM saat aplikasi dijalankan, deteksi *malicious code,* dan menemukan *password* log-in pada beberapa sosial media. Pengujian 3 skenario tersebut dilakukan pada RAM DDR2 dan RAM DDR3.

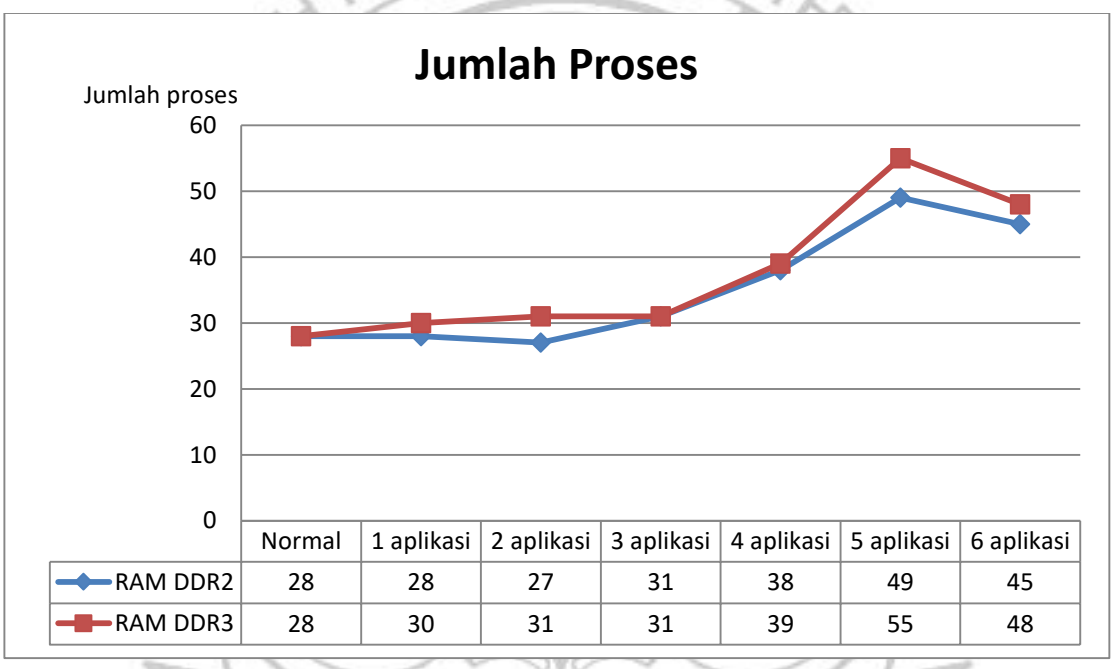
4.1 Hasil Pengujian 3 Skenario

4.1.1 Pemeriksaan RAM Saat Aplikasi Dijalankan

Pada skenario ini komputer yang telah disiapkan tersebut dengan menggunakan RAM DDR2 dan RAM DDR3 akan diperiksa berapa jumlah proses yang berjalan, berapa jumlah proses handle yang terlihat, dan jumlah information jaringan yang tercatat. Adapun beberapa proses yang dijalankan pada komputer yang meliputi menjalankan Winrar, memutar video menggunakan Media Player Classic, memutar lagu menggunakan aplikasi AIMP Player, membuka Foxit Reader, menjalankan Google Chrome dengan penelusuran *digital forensic* dan *plugin volatility,* kemudian menjalankan Mozilla Firefox dengan penelusuran *digital forensic* dan *plugin volatility*. Dalam penelitian digunakan 2 *tools* untuk mengakuisisi RAM dengan melakukan *image memory* yang meliputi Dumpit, dan Belkasoft Ramcapture.

4.1.1.1 Hasil Jumlah Proses

Pada pengujian ini mengimplementasikan skenario pertama pada RAM DDR2 dan RAM DDR3 yang telah ditentukan kemudian akan diperiksa jumlah proses yang sedang berjalan pada sistem. RAM di akuisisi dengan melakukan *image memory* menggunakan 2 *tools* yakni Dumpit dan Belkasoft RamCapture. Adapun hasil pengujian dapat dilihat pada Gambar 4.1 dan Gambar 4.2



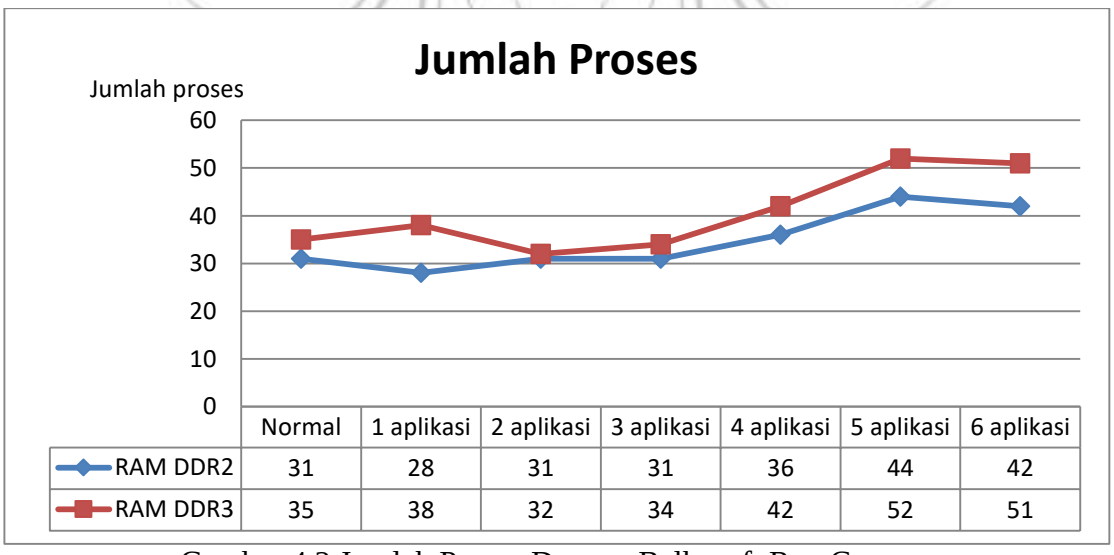
	Normal	1 aplikasi	2 aplikasi	3 aplikasi	4 aplikasi	5 aplikasi	6 aplikasi
RAM DDR2	28	28	27	31	38	49	45
RAM DDR3	28	30	31	31	39	55	48

Gambar 4.1 Jumlah Proses Dengan Dumpit

Pada Gambar 4.1 memperlihatkan setiap menambahkan jumlah aplikasi yang dijalankan jumlah proses yang didapatkan akan semakin bertambah. Pada saat 2 aplikasi yang dijalankan jumlah proses RAM DDR2 mengalami penurunan dari jumlah proses sebelumnya. Pada saat menjalankan 3 aplikasi jumlah RAM DDR3 tidak memiliki perubahan pada jumlah proses sebelumnya. Namun pada saat 6

aplikasi dijalankan pada RAM DDR2 dan RAM DDR3 jumlah proses yang didapat mengalami penurunan dari jumlah proses sebelumnya.

Dari data yang didapat pada RAM DDR2, saat menjalankan 5 aplikasi pada chrome.exe terdapat 6 kali proses, WmiPrvSE.exe 3 kali proses dan ada Msiexec.exe yang sedang berjalan. Sedangkan saat menjalankan 6 aplikasi pada chrome.exe hanya menjalankan 5 kali proses dan WmiPrvSE.exe hanya 1 kali proses dan Msiexec.exe tidak melakukan proses. Pada RAM DDR3 saat menjalankan 5 aplikasi pada chrome.exe terdapat 6 kali proses, taskhost.exe 2 kali proses, conhost.exe 2 kali proses, DumpIt.exe 2 kali proses, dan ada proses Msiexec.exe, sdclt.exe, dan proses schtasks.exe yang berjalan. Sedangkan saat 6 aplikasi yang berjalan pada chrome.ex hanya melakukan 5 kali proses, taskhost.exe 1 kali proses, conhost.exe 1 kali proses, DumpIt.exe 1 kali proses, dan proses Msiexec.exe, proses sdclt.exe, dan proses schtasks.exe tidak melakukan proses.



	Normal	1 aplikasi	2 aplikasi	3 aplikasi	4 aplikasi	5 aplikasi	6 aplikasi
RAM DDR2	31	28	31	31	36	44	42
RAM DDR3	35	38	32	34	42	52	51

Gambar 4.2 Jumlah Proses Dengan Belkasoft RamCapture

Pada Gambar 4.2 menunjukkan bahwa setiap melakukan penambahan aplikasi yang dijalankan jumlah proses yang didapat mengalami peningkatan. Pada saat 2 aplikasi yang dijalankan jumlah proses yang didapat pada RAM DDR3 mengalami penurunan dari jumlah proses sebelumnya. Pada saat 3 aplikasi yang dijalankan pada RAM DDR2 tidak mengalami peningkatan dari jumlah proses sebelumnya. Namun pada saat 6 aplikasi yang dijalankan RAM DDR2 mengalami penurunan dari jumlah proses sebelumnya.

Ketika membandingkan jumlah proses di Gambar 4.1 dan Gambar 4.2 terkhusus pada bagian 6 aplikasi yang dijalankan terlihat bahwa *tools* Belkasoft RamCapture bisa mendapatkan proses yang lebih banyak dibandingkan *tools* Dumpit pada RAM DDR3. Hal ini mengindikasikan bahwa hasil yang diperoleh setiap *tools* bisa berbeda ketika mengambil data proses yang terdapat di RAM. Adapun contoh proses yang berjalan didalam sistem ketika menjalankan semua aplikasi yang telah ditentukan dapat dilihat pada gambar 4.3.

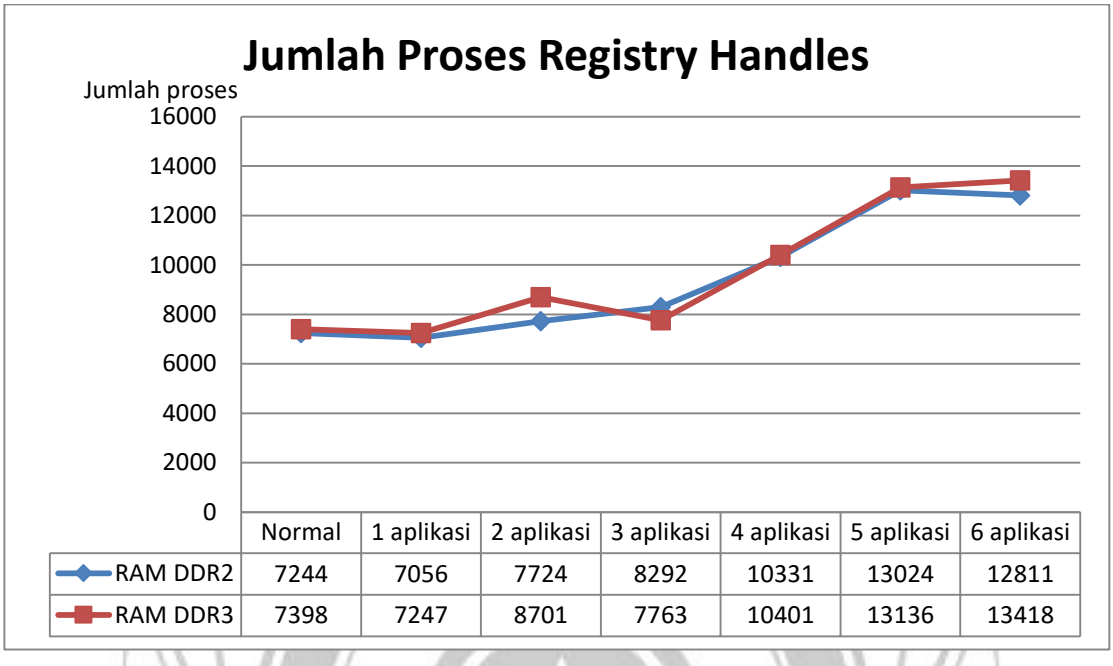
Pada Gambar 4.3 menunjukkan bahwa semua aplikasi yang sudah dijalankan dapat ditemukan dalam RAM. Pada Gambar 4.3 terdapat proses ID (PID) dari proses yang berjalan, sub-proses (PPID) dari proses ID, dan tanggal dan waktu proses tersebut mulai berjalan.

Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
0x00000000039d98c0	System	4	0	0x00185000	2017-09-04 14:45:22 UTC+0000	
0x00000000048646a0	csrss.exe	404	384	0x6d75f040	2017-09-04 14:45:26 UTC+0000	
0x0000000069be5030	conhost.exe	3060	404	0x6d75f520	2017-09-04 14:50:32 UTC+0000	
0x000000006ce5cbf8	SearchIndexer.	1792	440	0x6d75f240	2017-09-04 14:45:46 UTC+0000	
0x000000006ce71030	WmiPrvSE.exe	1660	632	0x6d75f5a0	2017-09-04 14:48:33 UTC+0000	2017-09-04 14:51:11 UTC+0000
0x000000006cf7bd40	FoxitReader.ex	2960	1336	0x6d75f400	2017-09-04 14:47:16 UTC+0000	
0x000000006d028030	firefox.exe	2836	1336	0x6d75f5e0	2017-09-04 14:49:05 UTC+0000	
0x000000006d02c1f0	svchost.exe	632	440	0x6d75f080	2017-09-04 14:45:36 UTC+0000	
0x000000006d040958	svchost.exe	360	440	0x6d75f3a0	2017-09-04 14:45:41 UTC+0000	
0x000000006d05f030	svchost.exe	832	440	0x6d75f1a0	2017-09-04 14:45:36 UTC+0000	
0x000000006d069030	svchost.exe	772	440	0x6d75f160	2017-09-04 14:45:36 UTC+0000	
0x000000006d07f558	svchost.exe	892	440	0x6d75f1c0	2017-09-04 14:45:36 UTC+0000	
0x000000006d0af570	audiodg.exe	972	772	0x6d75f1e0	2017-09-04 14:45:37 UTC+0000	
0x000000006d0d28e8	svchost.exe	1032	440	0	2017-09-04 14:45:37 UTC+0000	
0x000000006d132a40	chrome.exe	3272	1336	0	2017-09-04 14:47:25 UTC+0000	
0x000000006d13cd40	explorer.exe	1336	1276	0	2017-09-04 14:45:39 UTC+0000	
0x000000006d1475a0	dwm.exe	1288	832	0	2017-09-04 14:45:39 UTC+0000	
0x000000006d17ea98	spoolsv.exe	1432	440	0	2017-09-04 14:45:39 UTC+0000	
0x000000006d1c7808	taskhost.exe	1640	440	0	2017-09-04 14:45:39 UTC+0000	
0x000000006d1c9540	FCUpdateServic	1620	440	0	2017-09-04 14:45:39 UTC+0000	
0x000000006d1ff030	mpc-hc.exe	2380	1336	0	2017-09-04 14:46:50 UTC+0000	
0x000000006d2a4c48	lsass.exe	456	392	0	2017-09-04 14:45:26 UTC+0000	
0x000000006d2a7d40	lsm.exe	464	392	0	2017-09-04 14:45:26 UTC+0000	
0x000000006d2d1d40	winlogon.exe	500	384	0	2017-09-04 14:45:26 UTC+0000	
0x000000006d367528	svchost.exe	1480	440	0	2017-09-04 14:45:39 UTC+0000	
0x000000006d3daa88	svchost.exe	708	440	0	2017-09-04 14:45:36 UTC+0000	
0x000000006d424d00	svchost.exe	1312	440	0	2017-09-04 14:45:39 UTC+0000	
0x000000006d52e030	AIMP3.exe	2700	632	0	2017-09-04 14:47:03 UTC+0000	
0x000000006d546428	services.exe	440	392	0	2017-09-04 14:45:26 UTC+0000	
0x000000006d667c70	csrss.exe	344	324	0	2017-09-04 14:45:26 UTC+0000	
0x000000006d69dd40	wininit.exe	392	324	0	2017-09-04 14:45:26 UTC+0000	
0x000000006d759608	smss.exe	264	4	0	2017-09-04 14:45:22 UTC+0000	
0x000000006d9293b8	svchost.exe	1700	440	0	2017-09-04 14:45:39 UTC+0000	
0x000000006e21fcc8	RamCapture.exe	2840	1336	0	2017-09-04 14:50:40 UTC+0000	
0x000000006e2b6cc8	RamCapture.exe	2840	1336	0	2017-09-04 14:50:40 UTC+0000	
0x000000006e34dcc8	RamCapture.exe	2840	1336	0	2017-09-04 14:50:40 UTC+0000	
0x000000006e40f030	chrome.exe	2056	3272	0	2017-09-04 14:47:38 UTC+0000	
0x000000006e4acd40	mscorsvw.exe	2136	440	0	2017-09-04 14:47:41 UTC+0000	
0x000000006e4ec030	sppsvc.exe	2296	440	0	2017-09-04 14:47:44 UTC+0000	
0x000000006e4f7ab8	svchost.exe	2332	440	0	2017-09-04 14:47:44 UTC+0000	
0x000000006e501030	chrome.exe	1580	3272	0	2017-09-04 14:48:12 UTC+0000	
0x000000006e55c600	DumpIt.exe	296	1336	0	2017-09-04 14:50:32 UTC+0000	
0x000000006e566610	conhost.exe	1984	404	0	2017-09-04 14:50:40 UTC+0000	
0x000000006e6019a0	WmiPrvSE.exe	2800	632	0	2017-09-04 14:47:08 UTC+0000	
0x000000006e611d40	svchost.exe	3328	440	0	2017-09-04 14:47:26 UTC+0000	
0x000000006e61f9e0	FTK Imager.exe	3880	1336	0	2017-09-04 14:50:14 UTC+0000	
0x000000006e656b60	plugin-contain	2348	2836	0	2017-09-04 14:49:42 UTC+0000	2017-09-04 14:50:48 UTC+0000
0x000000006e66b7c8	chrome.exe	3280	3272	0	2017-09-04 14:47:25 UTC+0000	
0x000000006e67a6f8	chrome.exe	3312	3272	0	2017-09-04 14:47:26 UTC+0000	

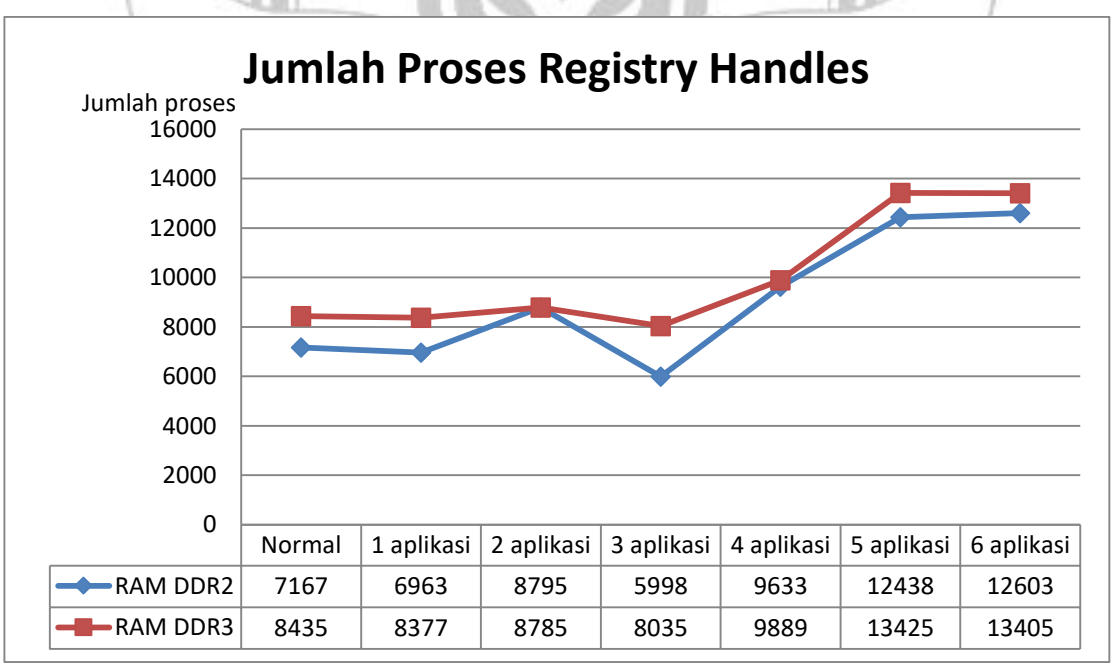
Gambar 4.3 Proses Yang Berjalan Didalam Sistem

4.1.1.2 Hasil Jumlah Proses Registry Handles

Pada pengujian ini mengimplementasikan skenario pertama pada RAM DDR2 dan RAM DDR3 yang telah ditentukan kemudian akan diperiksa jumlah proses Regstry handles yang terlihat pada sistem. RAM di akuisisi dengan melakukan *image memory* menggunakan 2 *tools* yakni Dumpit dan Belkasoft RamCapture. Adapun hasil pengujian dapat dilihat pada Gambar 4.4 dan Gambar 4.5.



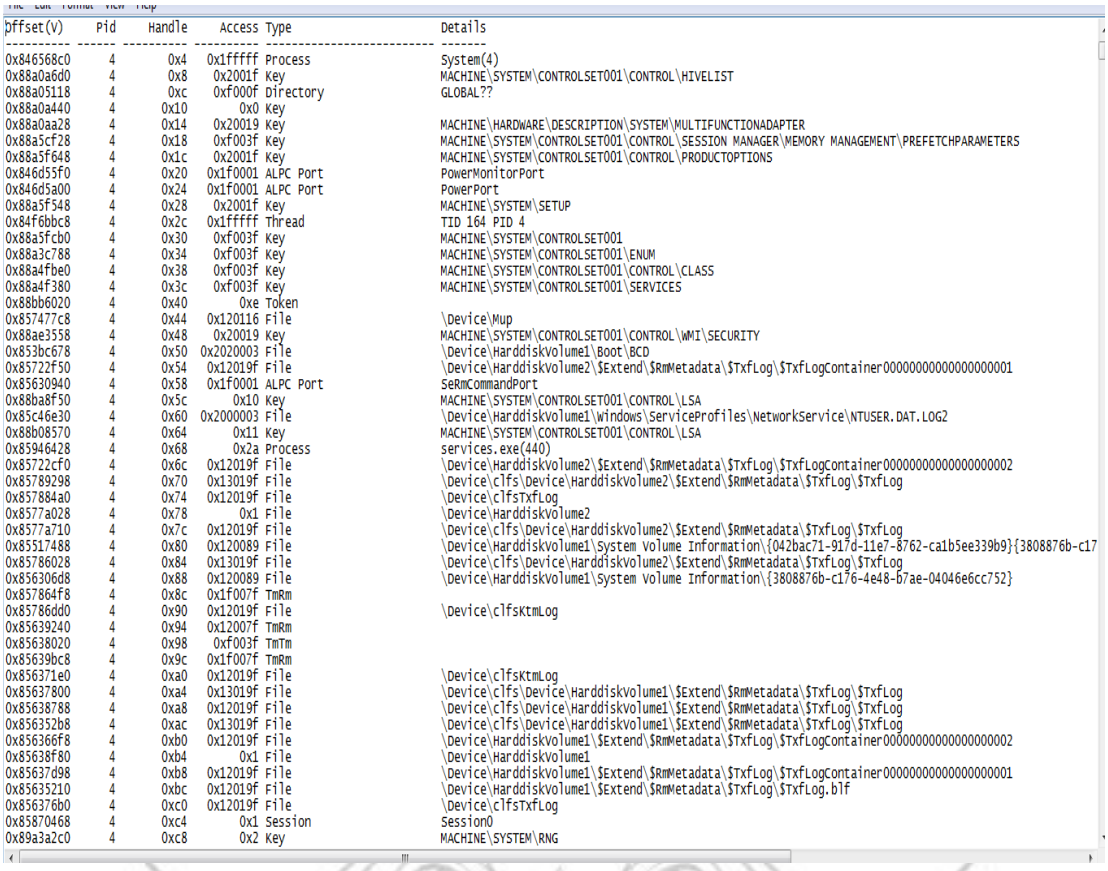
Gambar 4.4 Jumlah Proses Registry Handles Dengan Dumpit



Gambar 4.5 Jumlah Proses Registry Handles Dengan Belkasoft RamCapture

Pada Gambar 4.4 terlihat bahwa pada RAM DDR3 memiliki jumlah *Handles* lebih banyak dari RAM DDR2 kecuali pada saat 3 aplikasi dijalankan. Pada Gambar 4.5 dapat dilihat bahwa jumlah *Handles* pada RAM DDR3 lebih banyak dari jumlah *Handles* pada RAM DDR2 kecuali pada saat 2 aplikasi yang dijalankan. Pada Gambar 4.4 saat 1 aplikasi dijalankan RAM DDR2 dan RAM DDR3 mengalami penurunan jumlah *Handles* dari jumlah sebelumnya pada saat normal. Saat 3 aplikasi dijalankan RAM DDR3 mengalami penurunan dari jumlah *Handles* sebelumnya sedangkan pada saat 6 aplikasi dijalankan RAM DDR2 mengalami penurunan dari jumlah *Handles* yang sebelumnya. Pada Gambar 4.5 saat menjalankan 1 aplikasi jumlah *Handles* pada RAM DDR2 dan RAM DDR3 mengalami penurunan dari jumlah sebelumnya. Saat 3 aplikasi yang berjalan pada RAM DDR2 dan RAM DDR3 jumlah *Handles* mengalami penurunan dari jumlah saat 2 aplikasi yang berjalan sedangkan pada saat 6 aplikasi yang berjalan RAM DDR3 mengalami penurunan dari jumlah *Handles* sebelumnya.

Ketika membandingkan jumlah proses *Handles* dari Gambar 4.4 dan Gambar 4.5 terkhusus pada bagian 3 aplikasi yang berjalan terlihat bahwa *tools* Dumpit bisa mendapatkan proses yang lebih banyak dibandingkan *tools* Belkasoft RamCapture pada RAM DDR2. Hal ini mengindikasikan bahwa hasil yang diperoleh setiap *tools* bisa berbeda ketika mengambil data proses yang terdapat di RAM. Adapun contoh proses handles yang berjalan pada sistem dapat dilihat pada gambar 4.6.



```
Offset(V)     Pid     Handle     Access Type                    Details
---------- ------ ---------- ---------- ----------------------- -------
0x846568c0      4        0x4   0x1fffff Process                 System(4)
0x88a0a6d0      4        0x8    0x2001f Key                     MACHINE\SYSTEM\CONTROLSET001\CONTROL\HIVELIST
0x88a05118      4        0xc    0xf000f Directory               GLOBAL??
0x88a0a440      4       0x10        0x0 Key
0x88a0aa28      4       0x14    0x20019 Key                     MACHINE\HARDWARE\DESCRIPTION\SYSTEM\MULTIFUNCTIONADAPTER
0x88a5cf28      4       0x18    0xf003f Key                     MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER\MEMORY MANAGEMENT\PREFETCHPARAMETERS
0x88a5f648      4       0x1c    0x2001f Key                     MACHINE\SYSTEM\CONTROLSET001\CONTROL\PRODUCTOPTIONS
0x846d55f0      4       0x20   0x1f0001 ALPC Port               PowerMonitorPort
0x846d5a00      4       0x24   0x1f0001 ALPC Port               PowerPort
0x88a5f548      4       0x28    0x2001f Key                     MACHINE\SYSTEM\SETUP
0x84f6bbc8      4       0x2c   0x1fffff Thread                  TID 164 PID 4
0x88a5fcb0      4       0x30    0xf003f Key                     MACHINE\SYSTEM\CONTROLSET001
0x88a3c788      4       0x34    0xf003f Key                     MACHINE\SYSTEM\CONTROLSET001\ENUM
0x88a4fbe0      4       0x38    0xf003f Key                     MACHINE\SYSTEM\CONTROLSET001\CONTROL\CLASS
0x88a4f380      4       0x3c    0xf003f Key                     MACHINE\SYSTEM\CONTROLSET001\SERVICES
0x88bb6020      4       0x40        0xe Token
0x857477c8      4       0x44   0x120116 File                    \Device\Mup
0x88ae3558      4       0x48    0x20019 Key                     MACHINE\SYSTEM\CONTROLSET001\CONTROL\WMI\SECURITY
0x853bc678      4       0x50  0x2020003 File                    \Device\HarddiskVolume1\Boot\BCD
0x85722f50      4       0x54   0x12019f File                    \Device\HarddiskVolume2\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000001
0x85630940      4       0x58   0x1f0001 ALPC Port               SeRmCommandPort
0x88ba8f50      4       0x5c       0x10 Key                     MACHINE\SYSTEM\CONTROLSET001\CONTROL\LSA
0x85c46e30      4       0x60  0x2000003 File                    \Device\HarddiskVolume1\Windows\ServiceProfiles\NetworkService\NTUSER.DAT.LOG2
0x88b08570      4       0x64       0x11 Key                     MACHINE\SYSTEM\CONTROLSET001\CONTROL\LSA
0x85946428      4       0x68       0x2a Process                 services.exe(440)
0x85722cf0      4       0x6c   0x12019f File                    \Device\HarddiskVolume2\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000002
0x85789298      4       0x70   0x13019f File                    \Device\clfs\Device\HarddiskVolume2\$Extend\$RmMetadata\$TxfLog\$TxfLog
0x857884a0      4       0x74   0x12019f File                    \Device\clfsTxfLog
0x8577a028      4       0x78        0x1 File                    \Device\HarddiskVolume2
0x8577a710      4       0x7c   0x12019f File                    \Device\clfs\Device\HarddiskVolume2\$Extend\$RmMetadata\$TxfLog\$TxfLog
0x85517488      4       0x80   0x120089 File                    \Device\HarddiskVolume1\System Volume Information\{042bac71-917d-11e7-8762-ca1b5ee339b9}{3808876b-c17
0x85786028      4       0x84   0x13019f File                    \Device\clfs\Device\HarddiskVolume2\$Extend\$RmMetadata\$TxfLog\$TxfLog
0x856306d8      4       0x88   0x120089 File                    \Device\HarddiskVolume1\System Volume Information\{3808876b-c176-4e48-b7ae-04046e6cc752}
0x857864f8      4       0x8c   0x1f007f TmRm
0x85786dd0      4       0x90   0x12019f File                    \Device\clfsKtmLog
0x85639240      4       0x94   0x12007f TmRm
0x85638020      4       0x98    0xf003f TmTm
0x85639bc8      4       0x9c   0x1f007f TmRm
0x856371e0      4       0xa0   0x12019f File                    \Device\clfsKtmLog
0x85637800      4       0xa4   0x13019f File                    \Device\clfs\Device\HarddiskVolume1\$Extend\$RmMetadata\$TxfLog\$TxfLog
0x85638788      4       0xa8   0x12019f File                    \Device\clfs\Device\HarddiskVolume1\$Extend\$RmMetadata\$TxfLog\$TxfLog
0x856352b8      4       0xac   0x13019f File                    \Device\clfs\Device\HarddiskVolume1\$Extend\$RmMetadata\$TxfLog\$TxfLog
0x856366f8      4       0xb0   0x12019f File                    \Device\HarddiskVolume1\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000002
0x85638f80      4       0xb4        0x1 File                    \Device\HarddiskVolume1
0x85637d98      4       0xb8   0x12019f File                    \Device\HarddiskVolume1\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000001
0x85635210      4       0xbc   0x12019f File                    \Device\HarddiskVolume1\$Extend\$RmMetadata\$TxfLog\$TxfLog.blf
0x856376b0      4       0xc0   0x12019f File                    \Device\clfsTxfLog
0x85870468      4       0xc4        0x1 Session                 Session0
0x89a3a2c0      4       0xc8        0x2 Key                     MACHINE\SYSTEM\RNG
```

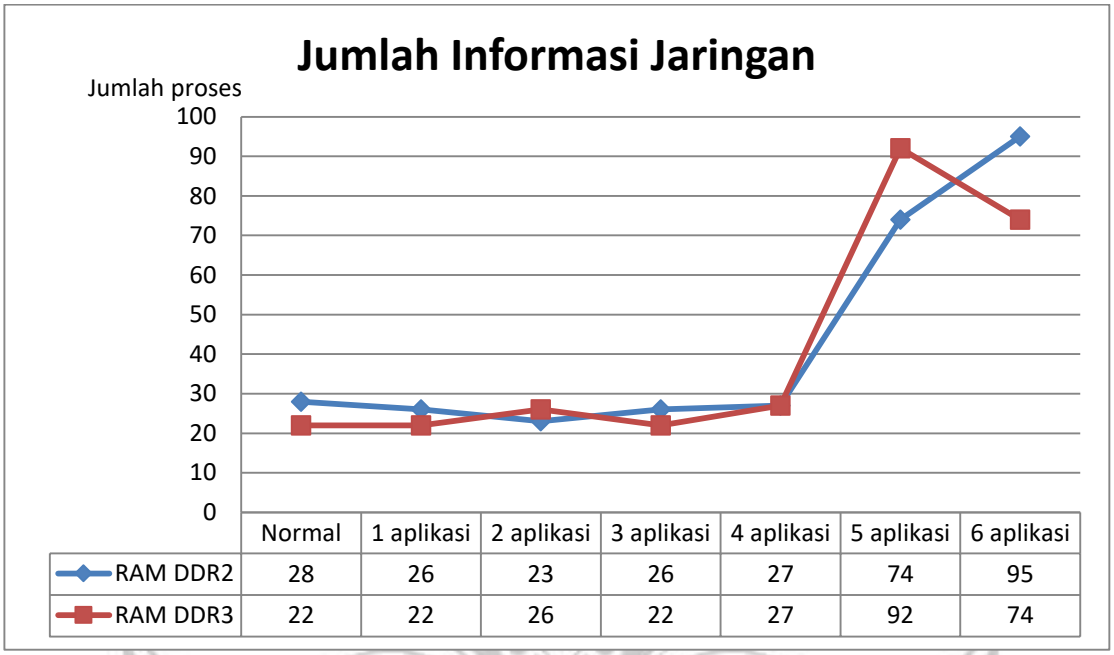
Gambar 4.6 Proses Registry Handles Yang Berjalan Didalam Sistem

Pada Gambar 4.6 dapat dilihat bahwa di dalam proses handles terdapat beberapa proses yang memiliki *type* proses yang berbeda yang berjalan pada proses ID (PID) 4 dan memiliki detail proses yang dijalankan.

4.1.1.3 Hasil Jumlah Informasi Jaringan

Pada pengujian ini mengimplementasikan skenario pertama pada RAM DDR2 dan RAM DDR3 yang telah ditentukan kemudian akan diperiksa jumlah informasi jaringan yang didapat pada sistem. RAM di akuisisi dengan melakukan *image*

memory menggunakan 2 *tools* yakni Dumpit dan Belkasoft RamCapture. Adapun hasil pengujian dapat dilihat pada Gambar 4.7 dan Gambar 4.8.

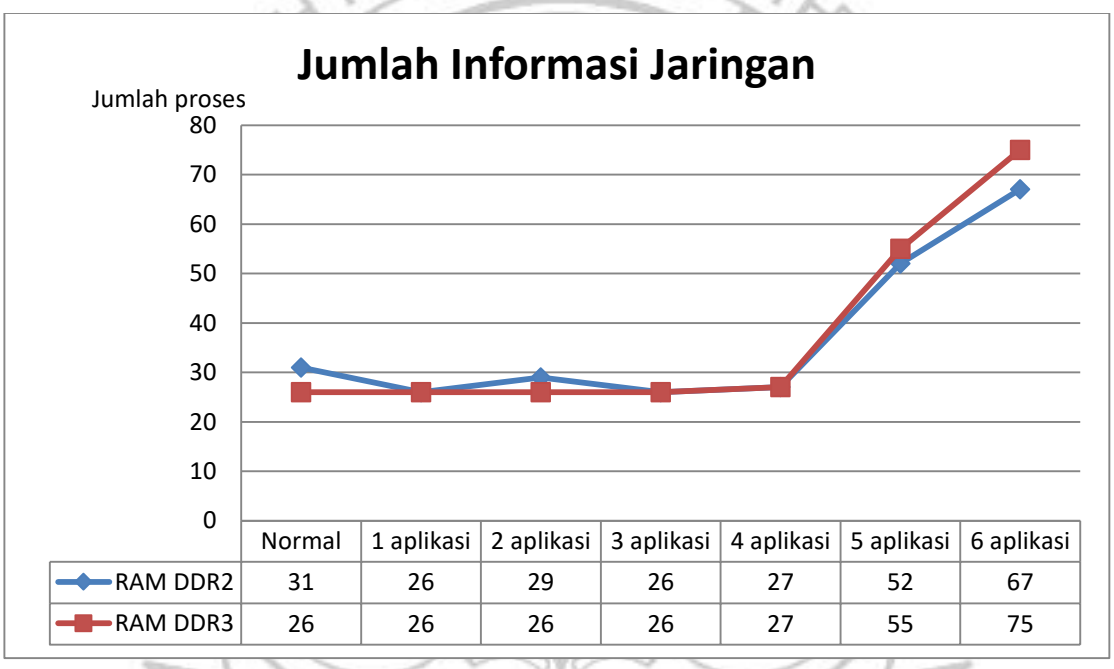


	Normal	1 aplikasi	2 aplikasi	3 aplikasi	4 aplikasi	5 aplikasi	6 aplikasi
RAM DDR2	28	26	23	26	27	74	95
RAM DDR3	22	22	26	22	27	92	74

Gambar 4.7 Grafik Hasil Jumlah Informasi Jaringan Dengan Dumpit

Pada Gambar 4.7 dapat dilihat bahwa pada saat 5 aplikasi dan 6 aplikasi yang berjalan memiliki jumlah informasi jaringan lebih banyak dari yang sebelumnya karena aplikasi yang dijalankan memang aplikasi yang mengakses jaringan. Pada saat menjalankan 1 aplikasi RAM DDR2 mengalami penurunan dari hasil saat normal dan pada RAM DDR3 tidak ada perubahan dari hasil normal. Pada saat menjalankan 2 aplikasi jumlah data yang dihasilkan berkurang dari hasil pada saat menjalankan 1 aplikasi namun pada RAM DDR3 memiliki peningkatan dari hasil data pada saat 1 aplikasi yang berjalan. Pada saat aplikasi menjalankan 3 aplikasi RAM DDR2 mengalami peningkatan yang memiliki jumlah data yang sama pada saat menjalankan

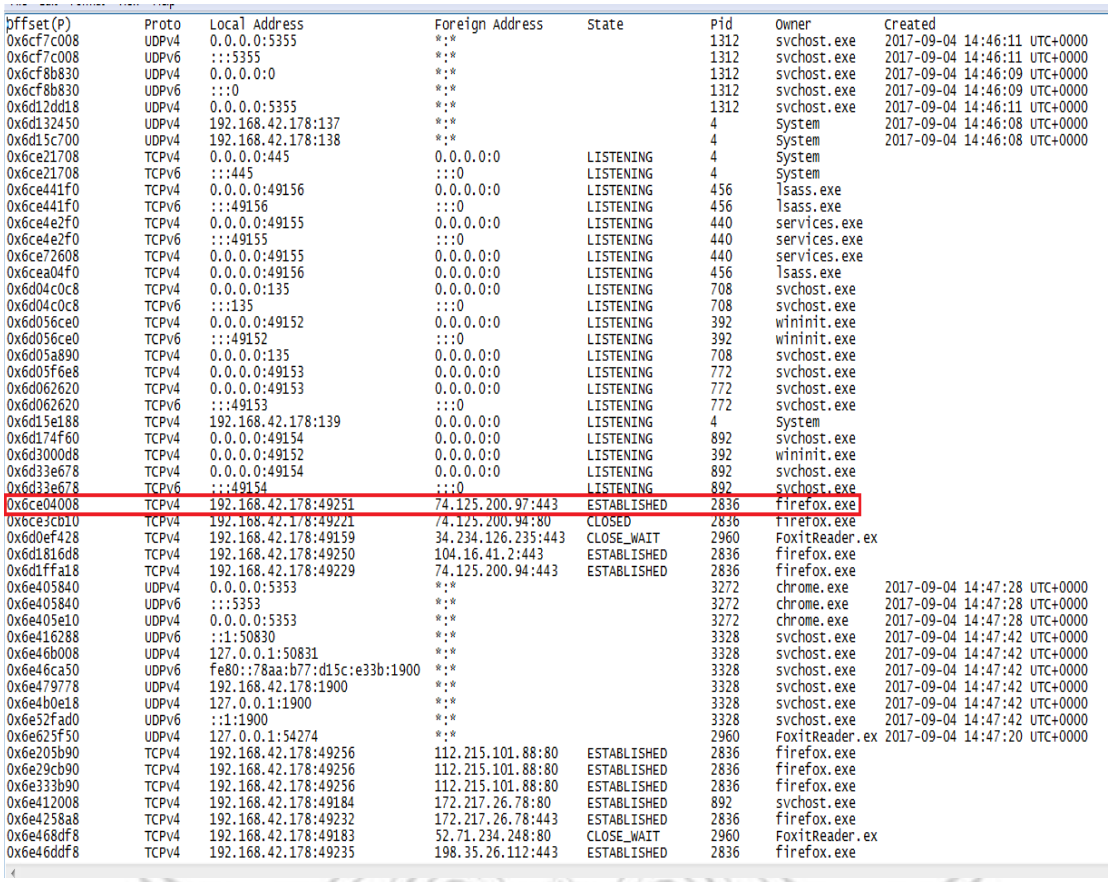
1 aplikasi dan pada RAM DDR3 jumlah data yang dihasilkan berkurang dan memiliki jumlah data yang sama pada saat 1 aplikasi yang berjalan. Pada saat 6 aplikasi yang berjalan jumlah data pada RAM DDR3 mengalami penurunan dari jumlah data yang sebelumnya sedangkan saat melihat Tabel 4.8 jumlah data pada RAM DDR3 mengalami peningkatan, hal ini mengindikasi bahwa hasil yang diperoleh setiap *tools* bisa berbeda ketika ketika mengambil data informasi jaringan yang terdapat di RAM.



	Normal	1 aplikasi	2 aplikasi	3 aplikasi	4 aplikasi	5 aplikasi	6 aplikasi
RAM DDR2	31	26	29	26	27	52	67
RAM DDR3	26	26	26	26	27	55	75

Gambar 4.8 Jumlah Informasi Dengan Belkasoft RamCapture

Pada Gambar 4.8 menunjukkan bahwa pada saat 5 aplikasi dan 6 aplikasi yang berjalan terjadi peningkatan lebih banyak jumlah informasi jaringan dari jumlah sebelumnya karena aplikasi yang dijalankan memang aplikasi yang mengakses jaringan. Adapun contoh aktivitas *network* yang terjadi saat sistem bekerja dapat dilihat pada Gambar 4.9.



Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0x6cf7c008	UDPv4	0.0.0.0:5355	*:*		1312	svchost.exe	2017-09-04 14:46:11 UTC+0000
0x6cf7c008	UDPv6	:::5355	*:*		1312	svchost.exe	2017-09-04 14:46:11 UTC+0000
0x6cf8b830	UDPv4	0.0.0.0:0	*:*		1312	svchost.exe	2017-09-04 14:46:09 UTC+0000
0x6cf8b830	UDPv6	:::0	*:*		1312	svchost.exe	2017-09-04 14:46:09 UTC+0000
0x6d12dd18	UDPv4	0.0.0.0:5355	*:*		1312	svchost.exe	2017-09-04 14:46:11 UTC+0000
0x6d132450	UDPv4	192.168.42.178:137	*:*		4	System	2017-09-04 14:46:08 UTC+0000
0x6d15c700	UDPv4	192.168.42.178:138	*:*		4	System	2017-09-04 14:46:08 UTC+0000
0x6ce21708	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System	
0x6ce21708	TCPv6	:::445	:::0	LISTENING	4	System	
0x6ce441f0	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	456	lsass.exe	
0x6ce441f0	TCPv6	:::49156	:::0	LISTENING	456	lsass.exe	
0x6ce4e2f0	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	440	services.exe	
0x6ce4e2f0	TCPv6	:::49155	:::0	LISTENING	440	services.exe	
0x6ce72608	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	440	services.exe	
0x6cea04f0	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	456	lsass.exe	
0x6d04c0c8	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	708	svchost.exe	
0x6d04c0c8	TCPv6	:::135	:::0	LISTENING	708	svchost.exe	
0x6d056ce0	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	392	wininit.exe	
0x6d056ce0	TCPv6	:::49152	:::0	LISTENING	392	wininit.exe	
0x6d05a890	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	708	svchost.exe	
0x6d05f6e8	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	772	svchost.exe	
0x6d062620	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	772	svchost.exe	
0x6d062620	TCPv6	:::49153	:::0	LISTENING	772	svchost.exe	
0x6d15e188	TCPv4	192.168.42.178:139	0.0.0.0:0	LISTENING	4	System	
0x6d174f60	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	892	svchost.exe	
0x6d3000d8	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	392	wininit.exe	
0x6d33e678	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	892	svchost.exe	
0x6d33e678	TCPv6	:::49154	:::0	LISTENING	892	svchost.exe	
0x6ce04008	TCPv4	192.168.42.178:49251	74.125.200.97:443	ESTABLISHED	2836	firefox.exe	
0x6ce3cd10	TCPv4	192.168.42.178:49221	74.125.200.94:80	CLOSED	2836	firefox.exe	
0x6d0ef428	TCPv4	192.168.42.178:49159	34.234.126.235:443	CLOSE_WAIT	2960	FoxitReader.ex	
0x6d1816d8	TCPv4	192.168.42.178:49250	104.16.41.2:443	ESTABLISHED	2836	firefox.exe	
0x6d1ffa18	TCPv4	192.168.42.178:49229	74.125.200.94:443	ESTABLISHED	2836	firefox.exe	
0x6e405840	UDPv4	0.0.0.0:5353	*:*		3272	chrome.exe	2017-09-04 14:47:28 UTC+0000
0x6e405840	UDPv6	:::5353	*:*		3272	chrome.exe	2017-09-04 14:47:28 UTC+0000
0x6e405e10	UDPv4	0.0.0.0:5353	*:*		3272	chrome.exe	2017-09-04 14:47:28 UTC+0000
0x6e416288	UDPv6	::1:50830	*:*		3328	svchost.exe	2017-09-04 14:47:42 UTC+0000
0x6e46b008	UDPv4	127.0.0.1:50831	*:*		3328	svchost.exe	2017-09-04 14:47:42 UTC+0000
0x6e46ca50	UDPv6	fe80::78aa:b77:d15c:e33b:1900	*:*		3328	svchost.exe	2017-09-04 14:47:42 UTC+0000
0x6e479778	UDPv4	192.168.42.178:1900	*:*		3328	svchost.exe	2017-09-04 14:47:42 UTC+0000
0x6e4b0e18	UDPv4	127.0.0.1:1900	*:*		3328	svchost.exe	2017-09-04 14:47:42 UTC+0000
0x6e52fad0	UDPv6	::1:1900	*:*		3328	svchost.exe	2017-09-04 14:47:42 UTC+0000
0x6e625f50	UDPv4	127.0.0.1:54274	*:*		2960	FoxitReader.ex	2017-09-04 14:47:20 UTC+0000
0x6e205b90	TCPv4	192.168.42.178:49256	112.215.101.88:80	ESTABLISHED	2836	firefox.exe	
0x6e29cb90	TCPv4	192.168.42.178:49256	112.215.101.88:80	ESTABLISHED	2836	firefox.exe	
0x6e333b90	TCPv4	192.168.42.178:49256	112.215.101.88:80	ESTABLISHED	2836	firefox.exe	
0x6e412008	TCPv4	192.168.42.178:49184	172.217.26.78:80	ESTABLISHED	892	svchost.exe	
0x6e4258a8	TCPv4	192.168.42.178:49232	172.217.26.78:443	ESTABLISHED	2836	firefox.exe	
0x6e468df8	TCPv4	192.168.42.178:49183	52.71.234.248:80	CLOSE_WAIT	2960	FoxitReader.ex	
0x6e46ddf8	TCPv4	192.168.42.178:49235	198.35.26.112:443	ESTABLISHED	2836	firefox.exe	

Gambar 4.9 Aktivitas *Network*

Pada Gambar 4.9 dapat dilihat bahwa ada beberapa *network* yang berjalan pada sistem saat bekerja. Yang ada dalam kotak merah dapat dilihat bahwa pada *owner* firefox.exe yang berjalan pada proses ID (PID) 2836 memiliki status *estabilished* yang sedang mengakses IP *address* (*foreign address*) 74.125.200.97 melalui port 443. Pada kotak merah firefox.exe memiliki IP *address local* 192.168.42.178 melalui port 49251 yang berjalan pada *protocol* TCPv4.

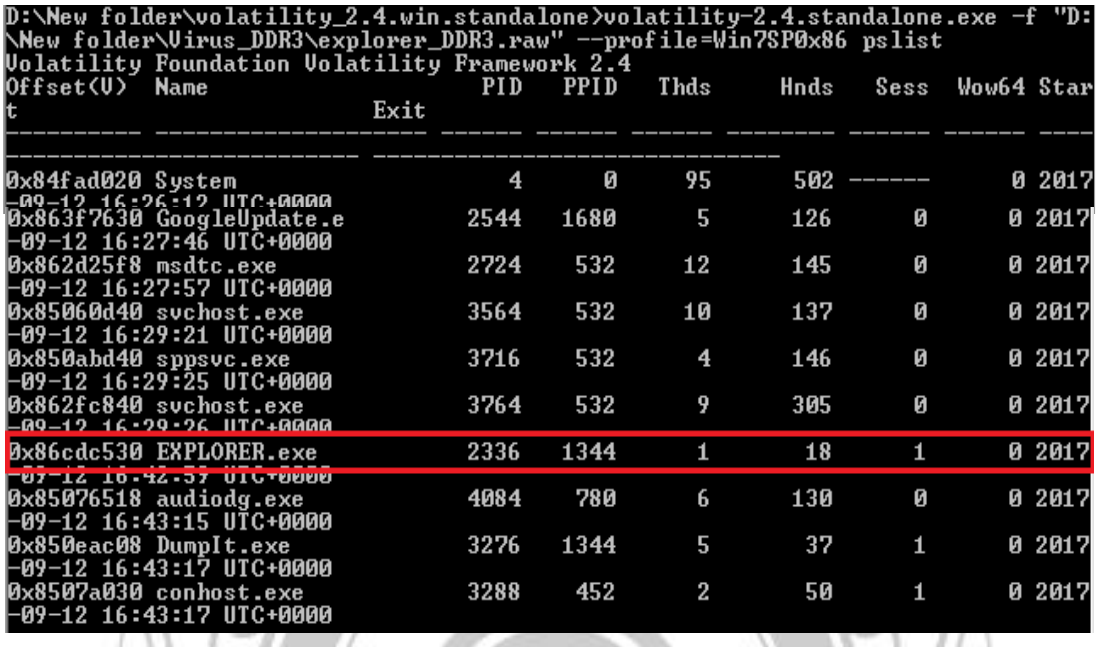
4.1.2 Malicious *Code*

Pada pengujian *malicious code* pada RAM DDR2 dan RAM DDR3 dilakukan pada VMware untuk menjaga kejadian hal-hal yang tidak di inginkan. Pada pengujian ini dilakukan dengan menjalankan *malware* yang sudah ditentukan kemudian mengakuisisi RAM dengan melakukan *image memory* menggunakan *tools* Belkasoft RamCapture. Dari hasil akuisisi diperoleh ekstensi file .raw selanjutnya menganalisis menggunakan *tools* Volatility. Adapun hasil pengujian pada tahapan ini dapat dilihat pada Tabel 4.1

Tabel 4.1 Hasil Pengujian Malicious Code

	Autorun Malware	**Explorer Malware**	**Sality Malware**	**Zeus Malware**
RAM DDR2	-	✓	-	✓
RAM DDR3	-	✓	-	✓

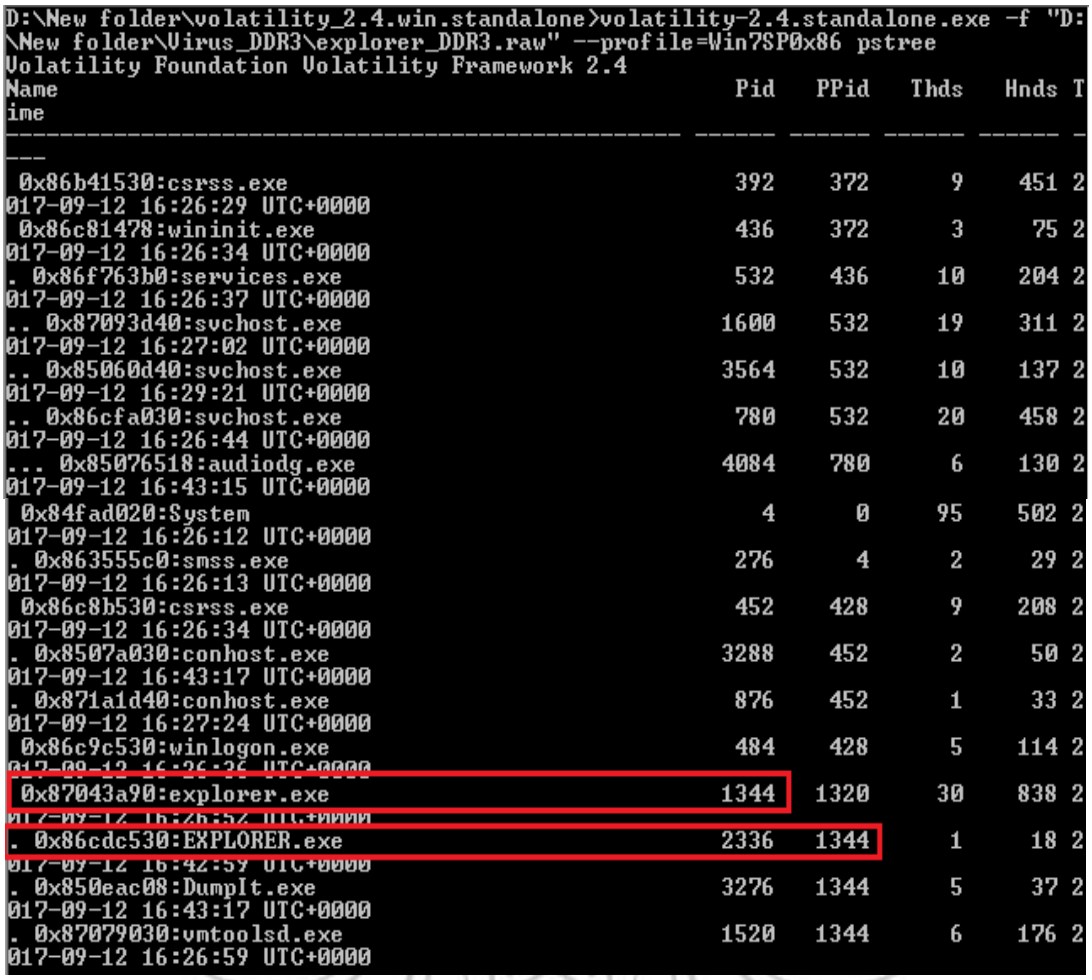
Pada Tabel 4.1 menunjukkan bahwa *malware* yang dapat ditemukan pada RAM DDR2 sama dengan apa yang di temukan pada RAM DDR3. Adapun *malware* yang dapat ditemukan yaitu *explorer malware* dan *zeus malware*. Saat dilakukan pemeriksaan proses yang berjalan di RAM, *explorer malware* terdeteksi pada proses ID (PID 2336) seperti pada gambar 4.10.



```
D:\New folder\volatility_2.4.win.standalone>volatility-2.4.standalone.exe -f "D:
\New folder\Virus_DDR3\explorer_DDR3.raw" --profile=Win7SP0x86 pslist
Volatility Foundation Volatility Framework 2.4
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Star
t                            Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ----
------------------------- ------------------------------
0x84fad020 System                    4      0     95      502 ------      0 2017
-09-12 16:26:12 UTC+0000
0x863f7630 GoogleUpdate.e         2544   1680      5      126      0      0 2017
-09-12 16:27:46 UTC+0000
0x862d25f8 msdtc.exe              2724    532     12      145      0      0 2017
-09-12 16:27:57 UTC+0000
0x85060d40 svchost.exe            3564    532     10      137      0      0 2017
-09-12 16:29:21 UTC+0000
0x850abd40 sppsvc.exe             3716    532      4      146      0      0 2017
-09-12 16:29:25 UTC+0000
0x862fc840 svchost.exe            3764    532      9      305      0      0 2017
-09-12 16:29:26 UTC+0000
0x86cdc530 EXPLORER.exe           2336   1344      1       18      1      0 2017
-09-12 16:42:57 UTC+0000
0x85076518 audiodg.exe            4084    780      6      130      0      0 2017
-09-12 16:43:15 UTC+0000
0x850eac08 DumpIt.exe             3276   1344      5       37      1      0 2017
-09-12 16:43:17 UTC+0000
0x8507a030 conhost.exe            3288    452      2       50      1      0 2017
-09-12 16:43:17 UTC+0000
```

Gambar 4.10 Proses Yang Berjalan

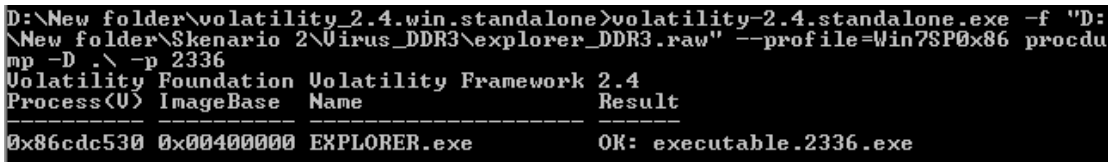
Pada gambar 4.10 Ada beberapa proses yang berjalan pada sistem. Namun, proses yang ditimbulkan EXPLORER.exe (PID 2336) sangat mencurigakan karena *malware* yang di jalankan memang bernamakan EXPLORER.exe. Setelah melihat ID proses orang tua (PPID 1344) dari EXPLORER.exe, proses EXPLORER.exe ini berjalan di sub-proses explorer.exe yang memiliki proses ID (PID 1344) dapat dilihat pada gambar 4.11.



```
D:\New folder\volatility_2.4.win.standalone>volatility-2.4.standalone.exe -f "D:
\New folder\Virus_DDR3\explorer_DDR3.raw" --profile=Win7SP0x86 pstree
Volatility Foundation Volatility Framework 2.4
Name                                                  Pid   PPid   Thds   Hnds T
ime
-------------------------------------------------- ------ ------ ------ ------ -
---
 0x86b41530:csrss.exe                                 392    372      9    451 2
017-09-12 16:26:29 UTC+0000
 0x86c81478:wininit.exe                               436    372      3     75 2
017-09-12 16:26:34 UTC+0000
. 0x86f763b0:services.exe                             532    436     10    204 2
017-09-12 16:26:37 UTC+0000
.. 0x87093d40:svchost.exe                            1600    532     19    311 2
017-09-12 16:27:02 UTC+0000
.. 0x85060d40:svchost.exe                            3564    532     10    137 2
017-09-12 16:29:21 UTC+0000
.. 0x86cfa030:svchost.exe                             780    532     20    458 2
017-09-12 16:26:44 UTC+0000
... 0x85076518:audiodg.exe                           4084    780      6    130 2
017-09-12 16:43:15 UTC+0000
 0x84fad020:System                                      4      0     95    502 2
017-09-12 16:26:12 UTC+0000
. 0x863555c0:smss.exe                                 276      4      2     29 2
017-09-12 16:26:13 UTC+0000
 0x86c8b530:csrss.exe                                 452    428      9    208 2
017-09-12 16:26:34 UTC+0000
. 0x8507a030:conhost.exe                             3288    452      2     50 2
017-09-12 16:43:17 UTC+0000
. 0x871a1d40:conhost.exe                              876    452      1     33 2
017-09-12 16:27:24 UTC+0000
 0x86c9c530:winlogon.exe                              484    428      5    114 2
[illegible]
 0x87043a90:explorer.exe                             1344   1320     30    838 2
[illegible]
. 0x86cdc530:EXPLORER.exe                            2336   1344      1     18 2
[illegible]
. 0x850eac08:DumpIt.exe                              3276   1344      5     37 2
017-09-12 16:43:17 UTC+0000
. 0x87079030:vmtoolsd.exe                            1520   1344      6    176 2
017-09-12 16:26:59 UTC+0000
```

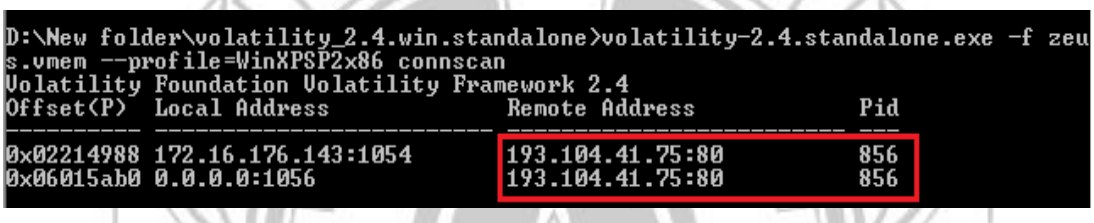
Gambar 4.11 Proses dan Sub-proses Yang Berjalan

Pada Gambar 4.11 Menunjukkan bahwa explorer.exe memiliki PID 1344 dan EXPLORER.exe memiliki PPID 1344. untuk mengetahui proses EXPLORER.exe bersifat virus, maka akan mendapatkan proses dump dari EXPLORER.exe seperti pada gambar 4.12 Kemudian dilakukan live scanning virus menggunakan website virus total untuk mengetahui kandungan virus yang terdapat di dalamnya.



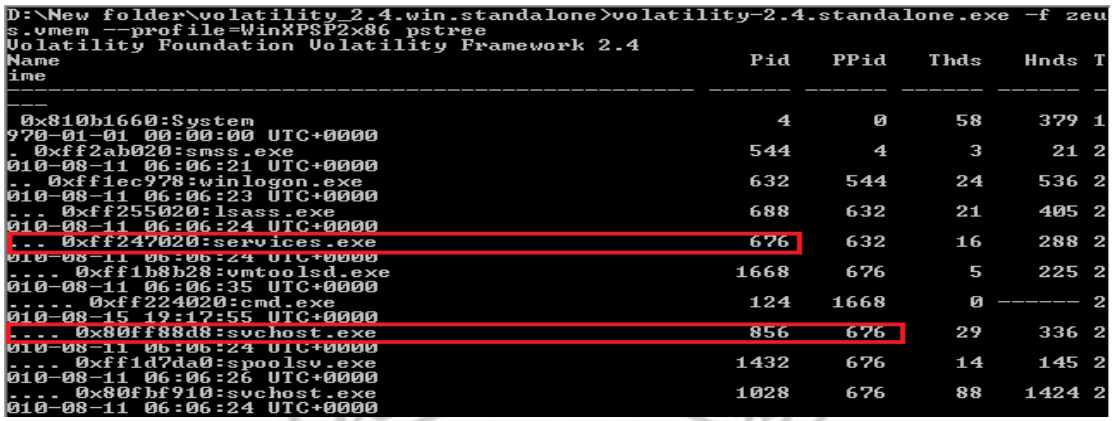
Gambar 4.12 Hasil Proses Dump EXPLORER.exe

Jika explorer malware ditemukan di proses yang berjalan, beda halnya dengan zeus malware yang dapat diketahui melalui informasi jaringan seperti pada gambar 4.13.



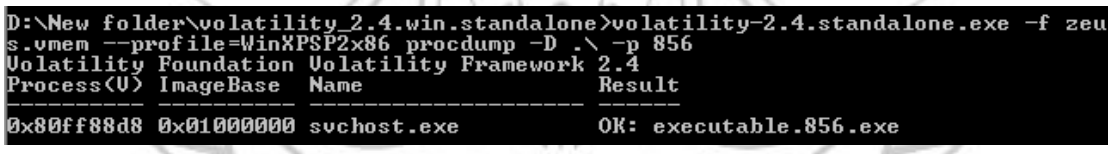
Gambar 4.13 Aktivitas Jaringan Yang Dilakukan Oleh Sistem

Pada Gambar 4.13 Menunjukkan bahwa ada aktivitas jaringan yang melakukan *remote access* menggunakan IP *address* 193.104.41.75 pada port 80 yang berjalan pada proses ID (PID 856). Setelah melihat proses ID-nya, IP *address* ini berjalan pada proses svchost.exe pada proses ID (PID 856) dapat dilihat pada gambar 4.14.



Gambar 4.14 Proses dan Sub-proses yang berjalan

Dari gambar 4.14 Dapat dilihat bahwa PID 856 berjalan pada proses svchost.exe dan berjalan pada sub-proses service.exe yang memiliki proses ID (PID 676). untuk mengetahui proses svchost.exe bersifat virus, maka akan mendapatkan proses dump dari svchost.exe seperti pada gambar 4.15 Kemudian dilakukan live scanning virus menggunakan website virus total untuk mengetahui kandungan virus yang terdapat di dalamnya.



Gambar 4.15 Hasil Proses Dump Svchost.exe

4.1.3 *Password* Log-in Pada Beberapa *Social Media*

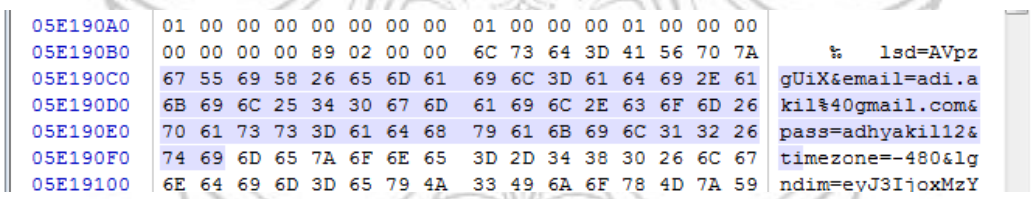
Pencarian bukti digital dilakukan dengan menggunakan browser Google Chrome dengan log-in ke akun *social media* selanjutnya log-out dari akun *social media* kemudian mengakuisisi RAM dengan *image memory* menggunakan *tools*

Belkasoft RamCapture. Dari hasil akuisisi diperoleh ekstensi file .raw selanjutnya menganalisis menggunakan WinHex. Setelah melakukan beberapa tahap analisis, hasil analisis dalam penelitian ini dapat dilihat pada table 4.2.

Tabel 4.2 Hasil Pengujian *Password* Pada Beberapa *Social Media*

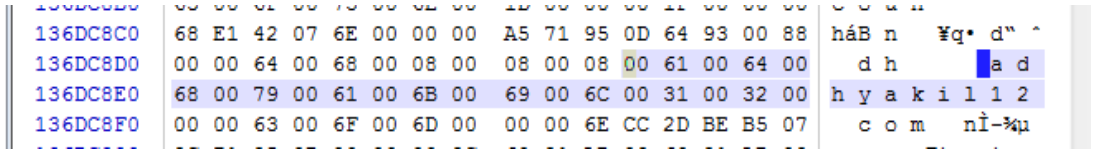
	Akun Gmail	**Akun Facebook**	**Akun Twitter**
RAM DDR2	✓	✓	✓
RAM DDR3	✓	✓	✓

Pada Tabel 4.2 dapat dilihat bahwa akun *password* yang biasa digunakan login ke *social media* dapat ditemukan pada dalam RAM DDR2 dan RAM DDR3, namun password yang digunakan untuk login hanya bisa ditemukan apabila browser yang digunakan belum di tutup dan *registry* belum di hapus. Bukti *password* yang ditemukan pada Facebook dapat dilihat pada gambar 4.16



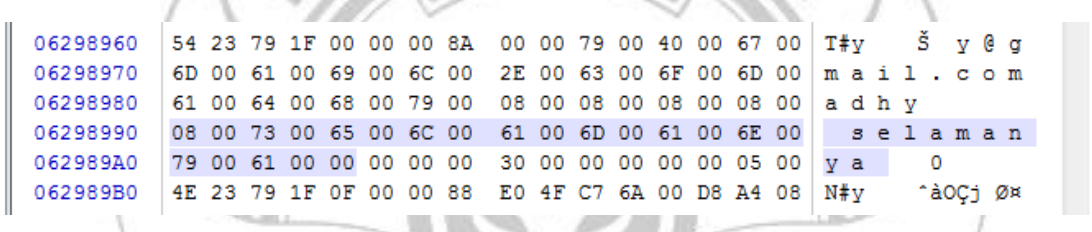
Gambar 4.16 *Password* dan Email Facebook

Gambar 4.16 Menunjukkan bahwa *password* dan *Email* yang digunakan dengan *password* "adhyakil12" dan email "adi.akil04@gmail.com. Bukti *password* yang ditemukan pada akun *Gmail* dapat dilihat pada gambar 4.17



Gambar 4.17 *Password* Gmail

Gambar 4.17 Menunjukkan bahwa password yang digunakan yaitu “adhyakil12”, namun tidak ada yang memberikan tanda bahwa itu adalah password tidak seperti password Facebook yang memberikan tanda “pass=” seperti pada gambar 4.16. Bukti password yang ditemukan pada akun Twitter dapat dilihat pada gambar 4.18.



Gambar 4.18 *Password* Twitter

Gambar 4.18 menunjukkan bahwa password yang digunakan log-in di twitter yaitu “selamanya”. Namun sama halnya dengan password Gmail yang tidak ada tanda bahwa itu password. Jadi untuk mencarinya yaitu dengan menuliskan password yang digunakan untuk log-in pada pencarian WinHex.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisa dan pengujian akuisisi bukti pada *random access memory* dapat ditarik kesimpulan sebagai berikut:

1. Akuisisi data pada *random access memory* bisa dilakukan menggunakan metode *image memory*.
2. Data yang berhasil ditemukan dalam *random access memory* yaitu proses yang berjalan dalam sistem, proses registry handles yang berjalan dalam sistem, aktivitas *network* yang didapat dalam sistem, *malicious code* pada sistem, password dan username log-in pada sosial media.
3. Keakuratan data yang dihasilkan dari forensik *memory* dari data proses yang ditemukan pengambilan data proses lebih akurat saat menggunakan *tools* Belkasoft RamCapture. Lebih banyak data proses yang ditemukan pada RAM DDR3 dibandingkan data proses pada RAM DDR2.

5.2 Saran

Pada penelitian ini terdapat beberapa hal yang dapat dikembangkan lebih lanjut dinataranya adalah :

1. Melakukan penelitian akuisisi bukti digital pada *random access memory* yang berbeda misalnya RAM DDR4.

2. Pada penelitian selanjutnya diharapkan mampu mengembangkan jangkauan akuisisi bukti digital dengan menemukan password pada sosial media lain seperti instagram desktop, dan pinterest.
3. Penelitian ini menggunakan perangkat lunak *open source*, diharapkan penelitian selanjutnya dapat menggunakan lab khusus digital forensik.

DAFTAR PUSTAKA

Amari, Kristine. 2009. Techniques and Tools for Recovering and Analyzing Data from Volatile Memory. :Sans Institut.

Borges, Alexandre. 2015. "*memory acquisition".* Versi 1.1, (http://alexandreborges.org) Diunduh tanggal 20 Juni 2017.

Carollet, Ovie Louis dan Samuel Basten. 2008. *Digital Forensic Analysis Methodology*. Computer Forensics, Vol. 56, No. 1. Washington: United States Department of Justice. (https://www.justice.gov/sites/default/files/usao/legacy/2008/02/04/usab5601.pdf) Diunduh 01 Desember 2016.

Carrier, Bryan Domani. 2006. "Risks of live digital forensic analysis," Communications of the ACM, vol. 49, no. 2, (2006), pp. 56-61.

Carvey, Harlan. 2005. "*windows forensics and incident recovery*", Addison Wesley, (Online), (https://media.neliti.com>publications) Diunduh tanggal 20 juni 2017.

Faiz, Muhammad. 2016. *"analisis live forensics untuk perbandingan keamanan email pada system operasi proprietary"*. (online), (https://www.researchgate.net/publication/316274589_ANALISIS_LIVE_FORENSICS_UNTUK_PERBANDINGAN_KEMANANAN_EMAIL_PADA_SISTEM_OPERASI_PROPRIETARY) Diunduh tanggal 20 juli 2017.

Kurniawan, Aan dan Yudi, Prayudi. 2014. "*teknik live forensics pada aktivitas zeus malware untuk mendukung malware forensics*". (https://www.researchgate.net/publication/263847986_Teknik_Live_Forensics_Pada_Aktivitas_Zeus_Malware_Untuk_Mendukung_Investigasi_Malware_Forensics) Diunduh pada tanggal 20 juni 2017.

Lessing, Marthie dan Vonbasie, Solms. 2008, "*Live Forensic Acquisition as Alternative to Traditional Forensic Processes*". Tersedia di (http://researchspace.csir.co.za/) Diunduh pada tanggal 12 Desember 2016.

Prayudi dan Afrianto. 2007. *Antisipasi Cybercrime Menggunakan Teknik. Komputer Forensik*. Seminar Nasional Aplikasi Teknologi Informasi.

Rahardjo, Budi. 2013. "*sekilas mengenai forensic digital".* jurnal sosioteknologi, Edisi 29. FSRD-ITB.

(budi.rahardjo.id/files/digital%20forensik%20fsrd%20journal.pdf) Diunduh pada tanggal 9 Maret 2017.

Rahman, Shuaibur dan Manuel Khan. 2015."*review of live forensic analysis techniques"*. Vol.8, No.2. (online), (http://dx.doi.org/10.14257/ijhit.2015.8.2.35) Diunduh pada tanggal 30 Oktober 2017.

Rajif, Maulana. 2006. "*pengamatan RAM di DDR1, DDR2, dan DDR3"*. Jurnal informatika. UII.

Mrdovic, Stjepan, Andrej, Huseinovic, dan Emanuel, Zajko. 2009."*Combining static and live digital forensic analysis in virtual environment*," In IEEE Information, Communication and Automation Technologies, 2009. ICAT 2009. XXII International Symposium on

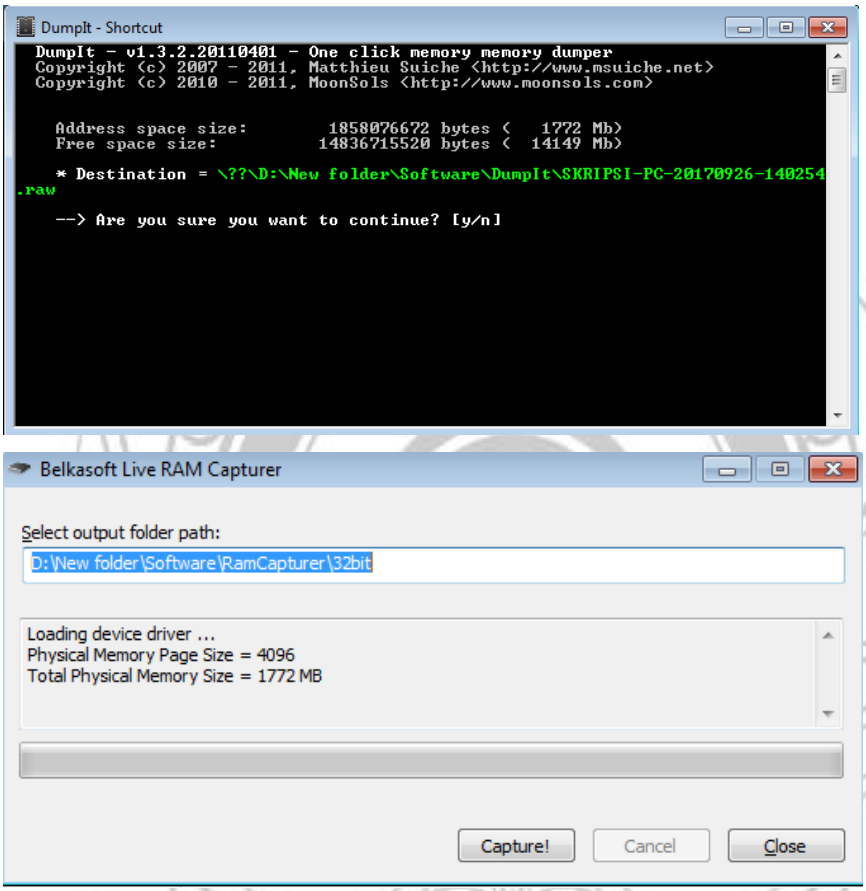
Suprapto, Eko. 2012. *Peran Komputer Forensik dalam Penegakan Hukum untuk Pembuktian Kasus Cyber Crime.*Jurnal Ilmiah Universitas Batanghari Jambi, Vol. 12.

Wijaya, Roni. 2016. *forensic digital random access memory pada sistem operasi komputer menggunakan metode dumpmemory*. Jurnal Ilmu Pedidikan, (online), (https://openlibrary.telkomuniversity.ac.id/pustaka/122597/forensik-digital-random-access-memory-pada-sistem-operasi-komputer-menggunakan-metode-dumpmemory.html) diakses 24 september 2017.

Wright, Mal. 2001. *Investigating an Internal Case of Internet Abuse*, SANS Institute.

LAMPIRAN

1. *Imaging memory* menggunakan Dumpit dan Belkasoft RamCapture

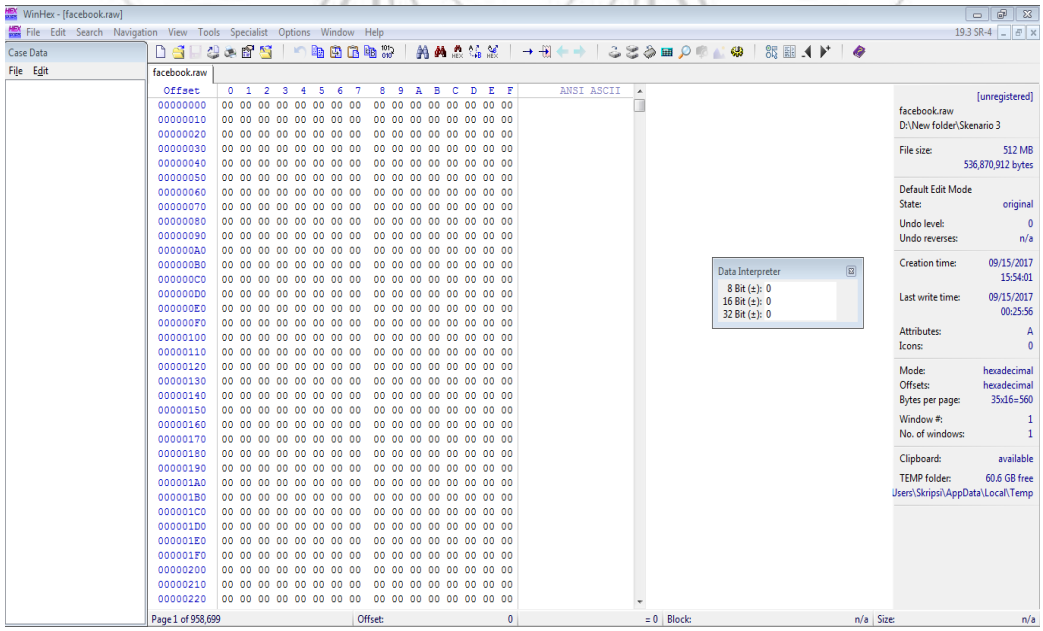


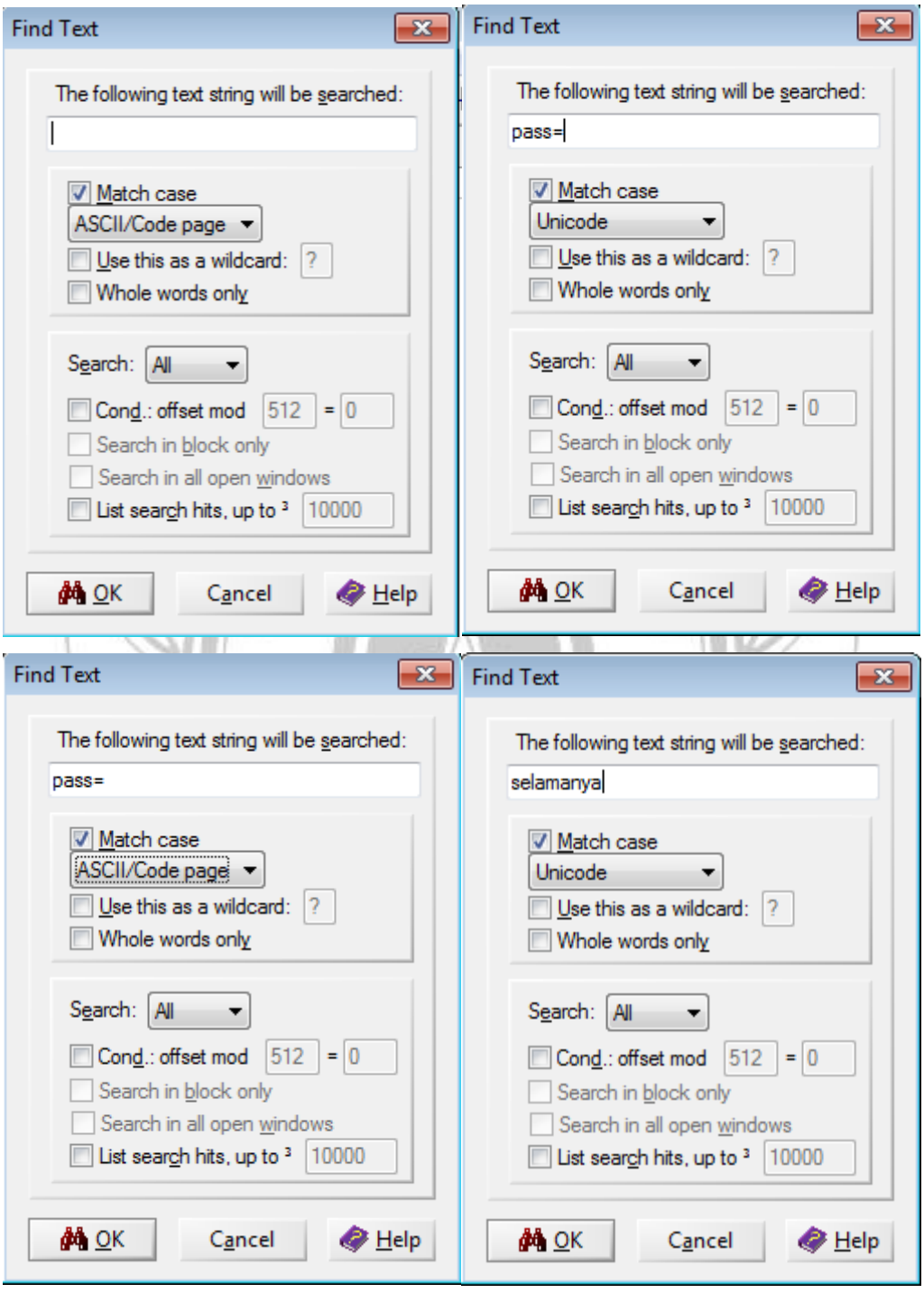
2. Akuisisi Data dengan Volatality dan Winhex

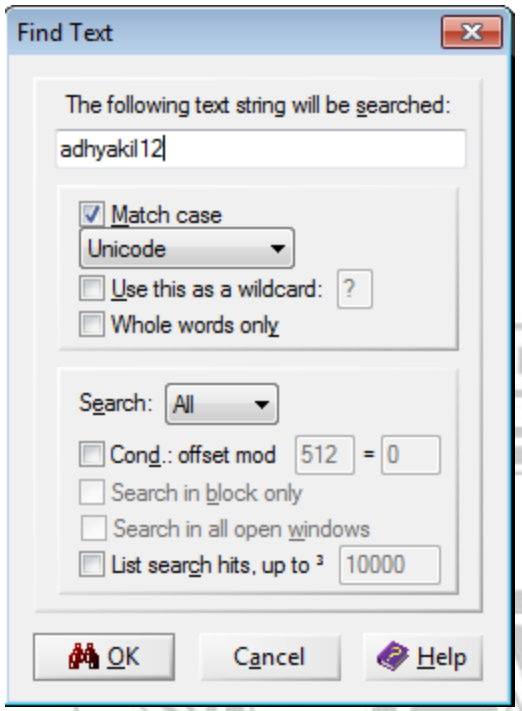
```
D:\New folder\volatility_2.4.win.standalone>volatility-2.4.standalone.exe -f "D:
\New folder\RAM DDR2\SKRIPSI-PC-20170815-105348.raw" imageinfo
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\New folder\RAM DDR2\SKRIPS
I-PC-20170815-105348.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82b68c28L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82b69c00L
                KPCR for CPU 1 : 0x807c6000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2017-08-15 10:59:54 UTC+0000
     Image local date and time : 2017-08-15 18:59:54 +0800
```

```
D:\New folder\volatility_2.4.win.standalone>volatility-2.4.standalone.exe -f "D:
\New folder\RAM DDR2\SKRIPSI-PC-20170815-105348.raw" --profile=Win7SP0x86 psscan

Volatility Foundation Volatility Framework 2.4
Offset(P)          Name                PID   PPID PDB        Time created
           Time exited
------------------ ---------------- ------ ------ ---------- ------------------
------------ ----------------------------
0x000000000002e4b20 IEMonitor.exe      1468    548 0x7a6ab420 2017-08-15 10:43:58
 UTC+0000
0x0000000000f09238 chrome.exe          2772   2768 0x7a6ab860 2017-08-15 10:47:34
 UTC+0000
0x0000000003148030 taskhost.exe        1976    708 0x7a6ab340 2017-08-15 10:43:37
 UTC+0000
0x0000000000669dd40 wermgr.exe         5832    708 0x7a6ab7c0 2017-08-15 10:56:38
 UTC+0000   2017-08-15 10:56:49 UTC+0000
0x0000000009123d40 taskeng.exe          884   1092 0x7a6ab160 2017-08-15 10:43:40
 UTC+0000
0x0000000000cff75d8 FCUpdateServic      560    708 0x7a6ab3e0 2017-08-15 10:43:38
 UTC+0000
0x0000000000101314a8 RamCapture.exe    2356   1564 0x7a6ab640 2017-08-15 10:54:03
 UTC+0000
0x000000000104a7550 avp.exe            1908    708 0x7a6ab320 2017-08-15 10:43:35
 UTC+0000
0x0000000001203bd40 WmiPrvSE.exe       4892    820 0x7a6abc00 2017-08-15 10:48:02
 UTC+0000
0x0000000014a0f6c8 PWRISOVM.EXE        2008   1564 0x7a6ab360 2017-08-15 10:43:37
 UTC+0000
0x000000000176c85a8 SearchIndexer.     2608    708 0x7a6ab380 2017-08-15 10:44:09
 UTC+0000
0x0000000001b8de940 chrome.exe         4956   2768 0x7a6ab620 2017-08-15 10:48:05
 UTC+0000
0x0000000001fc89938 AIMP3.exe          2840    820 0x7a6ab760 2017-08-15 10:46:16
 UTC+0000
0x0000000021e56d40 wininit.exe          588    524 0x7a6ab080 2017-08-15 10:43:14
 UTC+0000
0x0000000023338318 OSPPSVC.EXE         2644    708 0x7a6ab440 2017-08-15 10:44:10
 UTC+0000
0x0000000027189d40 chrome.exe          4496   2768 0x7a6abae0 2017-08-15 10:47:47
 UTC+0000
0x000000000276a7868 chrome.exe         5372   2768 0x7a6ab5a0 2017-08-15 10:49:01
 UTC+0000
0x0000000028a057e8 svchost.exe         2704    708 0x7a6ab460 2017-08-15 10:44:10
 UTC+0000
0x0000000029890890 csrss.exe            616    596 0x7a6ab040 2017-08-15 10:43:14
 UTC+0000
0x000000002a7a4c78 System                 4      0 0x00185000 2017-08-15 10:43:10
 UTC+0000
0x000000002e488728 svchost.exe         1092    708 0x7a6ab1c0 2017-08-15 10:43:23
 UTC+0000
0x000000002e7c6ad0 svchost.exe          996    708 0x7a6ab180 2017-08-15 10:43:21
 UTC+0000
0x000000002eafc928 svchost.exe         2388    708 0x7a6ab720 2017-08-15 10:46:03
 UTC+0000
0x000000002f414b38 svchost.exe         1064    708 0x7a6ab1a0 2017-08-15 10:43:23
 UTC+0000
0x000000002f8e0d40 svchost.exe          900    708 0x7a6ab140 2017-08-15 10:43:21
```

```
D:\New folder\volatility_2.4.win.standalone>volatility-2.4.standalone.exe -f "D:
\New folder\RAM DDR2\20170815.mem" --profile=Win7SP0x86 netscan
Volatility Foundation Volatility Framework 2.4
Offset(P)          Proto    Local Address                  Foreign Address
State            Pid      Owner          Created
0x17945150       TCPv4    0.0.0.0:1110                   0.0.0.0:0
LISTENING        1908     avp.exe
0x23c11150       TCPv4    0.0.0.0:1110                   0.0.0.0:0
LISTENING        1908     avp.exe
0x397905e8       UDPv4    192.168.43.36:1900             *:*
                 4056     svchost.exe    2017-08-15 10:46:02 UTC+0000
0x3ef20d70       TCPv4    127.0.0.1:49198                127.0.0.1:1110
CLOSED           1328     SM?RTP.exe
0x51272e20       UDPv4    127.0.0.1:1900                 *:*
                 4056     svchost.exe    2017-08-15 10:46:02 UTC+0000
0x520b7008       TCPv4    -:49918                        151.101.8.133:443
CLOSED           1908     avp.exe
0x53681e48       UDPv4    127.0.0.1:51082                *:*
                 4056     svchost.exe    2017-08-15 10:46:02 UTC+0000
0x543429d0       TCPv4    127.0.0.1:49200                127.0.0.1:1110
CLOSED           1328     SM?RTP.exe
0x543d77e0       TCPv4    192.168.43.36:49950            74.125.200.102:80
ESTABLISHED      1908     avp.exe
0x55416140       UDPv4    0.0.0.0:5355                   *:*
                 1356     svchost.exe    2017-08-15 10:44:24 UTC+0000
0x55416140       UDPv6    :::5355                        *:*
                 1356     svchost.exe    2017-08-15 10:44:24 UTC+0000
0x57323688       UDPv4    0.0.0.0:2560                   *:*
                 1244     svchost.exe    2017-08-15 10:54:06 UTC+0000
0x57323688       UDPv6    :::2560                        *:*
                 1244     svchost.exe    2017-08-15 10:54:06 UTC+0000
0x59ef7cf8       TCPv4    0.0.0.0:1110                   0.0.0.0:0
LISTENING        1908     avp.exe
0x59ef7cf8       TCPv6    :::1110                        :::0
LISTENING        1908     avp.exe
0x5a3274b0       TCPv4    0.0.0.0:1111                   0.0.0.0:0
LISTENING        1908     avp.exe
0x5d687a00       TCPv4    0.0.0.0:49157                  0.0.0.0:0
LISTENING        708      services.exe
0x5d687a00       TCPv6    :::49157                       :::0
LISTENING        708      services.exe
0x61c178f8       TCPv4    127.0.0.1:1001                 0.0.0.0:0
LISTENING        4        System
0x61f94008       TCPv4    192.168.43.36:49670            202.70.57.153:80
ESTABLISHED      1908     avp.exe
0x62c21e20       UDPv4    127.0.0.1:1900                 *:*
                 4056     svchost.exe    2017-08-15 10:46:02 UTC+0000
0x69a88140       UDPv4    0.0.0.0:5355                   *:*
                 1356     svchost.exe    2017-08-15 10:44:24 UTC+0000
0x69a88140       UDPv6    :::5355                        *:*
                 1356     svchost.exe    2017-08-15 10:44:24 UTC+0000
0x6a88f688       UDPv4    0.0.0.0:2560                   *:*
                 1244     svchost.exe    2017-08-15 10:54:06 UTC+0000
0x6a88f688       UDPv6    :::2560                        *:*
                 1244     svchost.exe    2017-08-15 10:54:06 UTC+0000
0x6ab50008       TCPv4    192.168.43.36:49670            202.70.57.153:80
ESTABLISHED      1908     avp.exe
```




Find Text
The following text string will be searched:
Match case
ASCII/Code page
Use this as a wildcard: ?
Whole words only
Search: All
Cond.: offset mod 512 = 0
Search in block only
Search in all open windows
List search hits, up to ³ 10000
OK
Cancel
Help
Find Text
The following text string will be searched:
pass=
Match case
Unicode
Use this as a wildcard: ?
Whole words only
Search: All
Cond.: offset mod 512 = 0
Search in block only
Search in all open windows
List search hits, up to ³ 10000
OK
Cancel
Help
Find Text
The following text string will be searched:
pass=
Match case
ASCII/Code page
Use this as a wildcard: ?
Whole words only
Search: All
Cond.: offset mod 512 = 0
Search in block only
Search in all open windows
List search hits, up to ³ 10000
OK
Cancel
Help
Find Text
The following text string will be searched:
selamanya
Match case
Unicode
Use this as a wildcard: ?
Whole words only
Search: All
Cond.: offset mod 512 = 0
Search in block only
Search in all open windows
List search hits, up to ³ 10000
OK
Cancel
Help



DAFTAR ISTILAH

Proses ID (PID) : Nomor identitas setiap proses atau program yang aktif berjalan.

Sub-Proses (PPID) : Sub-proses atau bagian dari proses ID

Thread : Unit terkecil dalam suatu proses yang bisa dijadwalkan oleh sistem operasi.

Registry Handle : Handle registry key (HKEY) merupakan sistem komputer terdistribusi untuk menetapkan pengidentifikasi, pegangan, sumber informasi, dan penyelesaiannya secara terus-menerus, dan untuk menyelesaikan "yang menangani informasi yang diperlukan untuk menemukan, mengakses, dan menggunakan sumber daya lainnya.

Cache : Tempat penyimpanan data sementara.

Volatile : memory yang datanya dapat ditulis serta dihapus,tetapi akan hilang saat kehilangan power (kondisi off) serta membutuhkan satu daya dalam mempertahankan memory.

Dead-box-analysis : Analisis memori hardisk.

Image memory : Proses pembuatan sallinan memori sedikit demi sedikit.

Snapshot : Pengambilan image memory pada RAM yang diambil secara spontan dan cepat.

Port : mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan.

Swap file : Memori cadangan berfungsi untuk membackup memori RAM. Ketika memori RAM anda kehabisan space/ruang, maka sebagian proses file disimpan sementara kedalam Swap File.

Malware : Suatu program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer.