TUGAS AKHIR – KS 141501

ANALISA FORENSIK PADA APLIKASI RE-LOADER ACTIVATOR 2.6 BY R@1N MENGGUNAKAN TEKNIK WINDOWS LIVE FORENSICS DAN DYNAMIC MALWARE ANALYSIS (STUDI KASUS : MICROSOFT WINDOWS 7)

FORENSICS ANALYSIS OF RE-LOADER ACTIVATOR 2.6 BY R@1N SOFTWARE USING WINDOWS LIVE FORENSICS AND DYNAMIC MALWARE ANALYSIS (CASE STUDY : MICROSOFT WINDOWS 7)

YUSUF SHALAHUDDIN AL AYYUBI AS SOBARI
NRP 05211240000172

Dosen Pembimbing
Bekti Cahyo Hidayanto, S.Si., M.Kom.

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2018

TUGAS AKHIR – KS141501

ANALISA FORENSIK PADA APLIKASI RE-LOADER ACTIVATOR 2.6 BY R@1N MENGGUNAKAN TEKNIK WINDOWS LIVE FORENSICS DAN DYNAMIC MALWARE ANALYSIS (STUDI KASUS : MICROSOFT WINDOWS 7)

Yusuf Shalahuddin Al Ayyubi As Sobari
05211240000172

Dosen Pembimbing I
Bekti Cahyo Hidayanto, S.Si., M.Kom.

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2018

FINAL PROJECT – KS141501

FORENSICS ANALYSIS OF RE-LOADER ACTIVATOR 2.6 BY R@1N SOFTWARE USING WINDOWS LIVE FORENSICS AND DYNAMIC MALWARE ANALYSIS (CASE STUDY : MICROSOFT WINDOWS 7)

Yusuf Shalahuddin Al Ayyubi As Sobari
05211240000172

Supervisor I
Bekti Cahyo Hidayanto, S.Si., M.Kom.

INFORMATION SYSTEMS DEPARTMENT
Faculty of Information Technology and Communication
Institut Teknologi Sepuluh Nopember
Surabaya 2018

LEMBAR PENGESAHAN

ANALISA FORENSIK PADA APLIKASI RE-LOADER ACTIVATOR 2.6 BY R@1N MENGGUNAKAN TEKNIK WINDOWS LIVE FORENSICS DAN DYNAMIC MALWARE ANALYSIS (STUDI KASUS : MICROSOFT WINDOWS 7)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember

Oleh:
Yusuf Shalahuddin Al Ayyubi As Sobari
05211240000172

Surabaya, 17 Juli 2018

KEPALA
DEPARTEMEN SISTEM INFORMASI

Dr. Ir. Aris Tjahyanto, M.Kom
NIP.196503101991021001

LEMBAR PERSETUJUAN
ANALISA FORENSIK PADA APLIKASI RE-LOADER ACTIVATOR 2.6 BY R@1N MENGGUNAKAN TEKNIK WINDOWS LIVE FORENSICS DAN DYNAMIC MALWARE ANALYSIS (STUDI KASUS : MICROSOFT WINDOWS 7)

TUGAS AKHIR
Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:
Yusuf Shalahuddin Al Ayyubi As Sobari
05211240000172

Disetujui Tim Penguji: Tanggal Ujian: 23 November 2017
Periode Wisuda: September 2018

Bekti Cahyo Hidayanto, S.Si., M.Kom. (Pembimbing)

Dr. Ir. Aris Tjahyanto, M.Kom (Penguji I)

Hatma Suryotrisongko, S.Kom., M.Eng (Penguji II)

ANALISA FORENSIK PADA APLIKASI RE-LOADER ACTIVATOR 2.6 BY R@1N MENGGUNAKAN TEKNIK *WINDOWS LIVE FORENSICS* DAN *DYNAMIC MALWARE ANALYSIS* (STUDI KASUS : MICROSOFT WINDOWS 7)

Nama Mahasiswa	**:**	**Yusuf Shalahuddin Al Ayyubi As Sobari**
NRP	**:**	**05211240000172**
Departemen	**:**	**Sistem Informasi FTIF-ITS**
Pembimbing I	**:**	**Bekti Cahyo Hidayanto, S.Si., M.Kom.**

ABSTRAK

Salah satu dampak dari penggunaan software bajakan adalah ancaman terinfeksi malicious software (malware) yang sangat merugikan pengguna. Microsoft Windows menjadi software yang paling banyak dibajak dengan aplikasi Re-loader sebagai aplikasi pembajaknya. Re-loader dapat mengaktifkan Windows layaknya aplikasi resmi namun illegal.

Penelitian ini melihat dampak dari digunakannya Re-loader pada Windows 7 dengan menggunakan analisa Windows secara langsung (Live Windows Analysis) dan analisa malware dinamis (Dynamic Malware Analysis). Kemudian, Chain of Custody (CoC) digunakan untuk menangani barang bukti. Penelitian ini juga membuat Indicators of Compromise (IoC) untuk mendeteksi penggunaan Re-loader pada perangkat lain dan juga sebagai barang bukti.

Setelah dilakukan penelitian, Re-loader membawa malware yang cukup berbahaya. Re-loader juga meninggalkan 4 file prefetch yang dapat digunakan sebagai barang bukti. IoC yang dibuat berdasarkan barang bukti juga dapat mendeteksi Re-loader pada perangkat yang berbeda.

Kata Kunci : Digital Forensics, Dynamic Malware Analysis, Indicators of Compromise, Live Windows Forensics, Malware

FORENSICS ANALYSIS OF RE-LOADER ACTIVATOR 2.6 BY R@1N SOFTWARE USING WINDOWS LIVE FORENSICS AND DYNAMIC MALWARE ANALYSIS (CASE STUDY: MICROSOFT WINDOWS 7)

Student Name	**:**	**Yusuf Shalahuddin Al Ayyubi As Sobari**
Student Number	**:**	**05211240000172**
Department	**:**	**Sistem Informasi FTIF-ITS**
Supervisor I	**:**	**Bekti Cahyo Hidayanto, S.Si., M.Kom.**

ABSTRAK

One impact of the use of pirated software is the threat of infected by malicious software (malware) that is very detrimental to the user. Microsoft Windows became the most heavily hijacked software with Re-loader app as its hijacker app. Re-loaders can easily activate Windows so it can be used like an official but illegal application.

This study looks at the impact of using Re-loader on Windows 7 by using Windows Live analysis and dynamic malware analysis. Then, Chain of Custody (CoC) is used to handle the evidence. This study also makes Indicators of Compromise (IoC) to detect the use of Re-loader on other devices and also as evidence that someone has done piracy of Windows 7.

After doing research, Re-loader does carry dangerous malware. The re-loader also leaves 4 prefetch files that can be used as evidence. IoC made on the basis of evidence can also detect Re-loaders on different devices.

Keywords : Digital Forensics, Dynamic Malware Analysis, Indicators of Compromise, Live Windows Forensics, Malware

KATA PENGANTAR

Alhamdulillah, puji syukur kepada Allah SWT yang telah memberikan kekuatan, karunia-Nya dan juga masih memberikan kesempatan bagi penulis untuk menyelasaikan buku ini dengan judul :

ANALISA FORENSIK PADA APLIKASI RE-LOADER ACTIVATOR 2.6 BY R@1N MENGGUNAKAN TEKNIK WINDOWS LIVE FORENSICS DAN DYNAMIC MALWARE ANALYSIS (STUDI KASUS : MICROSOFT WINDOWS 7)

Buku ini mewakili keinginan penulis untuk melahirkan lebih banyak penelitian dan implementasi dari forensik digital. Saat buku ini ditulis, topik mengenai forensik digital masih tergolong baru dan menakutkan. Penulis sendiri memahami sulitnya mencari pekerjaan pada bidang forensik digital meskipun bidang yang menyerempet seperti keamanan informasi sudah banyak. Namun setelah lebih dari 3 tahun belajar forensik digital, bidang ini mampu membuka wawasan lebih luas terutama dari segi hukum. Sekalipun nantinya impian yang sesuai bidang ini tidak tercapai, penulis masih memiliki senjata yang tidak sembarang orang memiliki. Karena mereka yang paham forensik digital akan memahami anti forensik digital.

Semoga buku ini dapat memotivasi pembaca untuk tertarik atau bahkan menjadi ahli di bidang forensik digital. Penulis teringat pesan dari Bang Napi yang berbunyi “Ingat, kejahatan terjadi bukan hanya karena niat pelakunya, tetapi juga karena ada KESEMPATAN!! Waspadalah...! Waspadalah...!”. Siapapun yang memiliki kemampuan dalam bidang forensic digital dapat mengamankan dirinya sendiri maupun orang-orang disekitanya, termasuk mengantarkan ke penjara.

Tak lupa dalam kesempatan ini penulis mengucapkan terima kasih kepada :

- Bapak dan Ibu penulis yang memberikan dukungan penuh dan doa yang tiada henti.

- Bapak Bekti Cahyo Hidayanto selaku dosen pembimbing I yang telah memberikan waktu dan juga pikiran kepada penulis untuk mengarahkan tugas akhir ini.
- Bapak Tony Dwi S. selaku dosen wali saya yang telah mengarahkan saya dalam hal-hal akademik.
- Teman-teman di SOLA12IS yang selalu memberikan semangat, dukungan, dan ilmu selama kuliah.
- Dosen-dosen di Departemen Sistem Informasi ITS yang telah memberikan ilmu dan pengalaman berharga ketika kuliah.
- Pemerintah Kota Bontang yang telah memberikan beasiswa.
- Rekan-rekan Asosiasi Forensik Digital Indonesia (AFDI) yang telah memberikan saran dan pertimbangan dalam penulisan buku ini.
- Feti Andriani dan keluarga yang telah mendukung saya selama kuliah hingga wisuda.
- Dan tanpa mengurangi rasa hormat, saya juga berterima kasih kepada pihak-pihak yang belum saya sebutkan namanya disini

Penulis menyadari bahwa buku ini masih banyak kekurangan. Penulis memohon maaf terhadap segala kekurangan dan kekeliruan yang ada. Semoga tugas akhir ini bermanfaat bagi seluruh pembaca

Surabaya, Januari 2018

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

Pada bab ini, akan dijelaskan tentang Latar Belakang Masalah, Perumusan Masalah, Batasan Masalah, Tujuan Tugas Akhir, Manfaat Kegiatan Tugas Akhir ini.

1.1 Latar Belakang Masalah

Berdasarkan data dari Microsoft *Malware* Protection Center (MMPC) dan Microsoft Security Intelligence Report (SIRv20), Indonesia termasuk dalam peringkat 2 negara di Asia Pasifik dengan ancaman *malware* terbesar [1]. *Malware* ini masuk ke Indonesia dengan berbagai macam cara, diantaranya melalui komputer desktop, smartphone, website, dan masih banyak lagi. Dari berbagai macam varian sistem operasi, Windows 7 menempati urutan pertama (47,34%) sebagai sistem operasi desktop terbanyak digunakan di Indonesia [2]. Disusul oleh Windows XP (12,04%) diposisi kedua dan Windows 10 (11,8%) diposisi ketiga [2]. Windows 7 juga menguasai pasar internasional dengan market share sebesar (20,64%) [3].

Tingginya penggunaan Microsoft Windows tidak diimbangi dengan kesadaran menggunakan produk asli. Berdasarkan data Statista pada tahun 2015, Indonesia menempati urutan ke 10 negara pengguna *software* bajakan tertinggi dengan kontribusi nilai komersial *software* bajakan seniali USD 1,1 miliar atau sekitar Rp. 14 triliun dan tingkat peredaran sebesar 84% [4]. Sistem Operasi Windows merupakan salah satu dari sekian banyak *software* yang dibajak. Salah satu aplikasi yang sering digunakan untuk membajak Windows adalah aplikasi Re-loader yang dikembangkan oleh R@in. Meskipun aplikasi Re-loader banyak digunakan, masih banyak pengguna yang tidak memahami bahaya dari aplikasi ini. Penelitian ini bertujuan untuk mengetahui perilaku dan dampak dari aplikasi Re-loader menggunakan analisa forensik digital. Analisa ini meliputi analisa Windows secara langsung (*Live Windows Forensics*) dan analisa *malware* secara dinamis (*Dynamic Malware Analysis*) dengan menjalankan pada lingkungan terkontrol

kemudian mengamati perilakunya. Diharapkan dengan adanya penelitian ini masyarakat dapat berhati-hati dalam menjalankan sebuah program dan mengurangi tingkat pembajakan *software*.

1.2 Perumusan Masalah

Permasalahan yang dihadapi dalam penelitian ini adalah sebagai berikut:

a. Apa saja barang bukti/artefak yang ditinggalkan oleh aplikasi Re-loader ?
b. Bagaimana melakukan analisa forensik menggunakan teknik *Windows Live Forensics* dan *Dynamic Malware Analysis* pada aplikasi Re-loader ?
c. Apa saja dampak penerapan aplikasi Re-loader ?

1.3 Batasan Masalah

Batasan pemasalahan dalam tugas akhir ini adalah:

a. Tugas Akhir ini menggunakan Microsoft Windows 7 Professional 32 Bit asli dan aplikasi Re-loader versi 2.6 By R@1n dengan hash terlampir pada **Lampiran A**.
b. Analisa yang digunakan hanya sebatas analisa *malware* dinamis, tidak mencakup analisa statis dan *hybrid*.
c. Analisa tidak termasuk aktivitas internet yang dilakukan oleh aplikasi Re-loader.
d. Fitur update Windows, firewall, dan antivirus akan dimatikan untuk mempermudah menjalankan Re-loader sebagai administrator.
e. Barang bukti tidak pernah diubah atau dilakukan teknik anti forensik.
f. Penulis melakukan aktivitas pembajakan pada penelitian ini hanya untuk kepentingan pendidikan. Penulis tidak dapat dikenai sanksi hukuman pidana, perdata mapun administrasi/administratif karena aktivitas tersebut.

1.4 Tujuan Tugas Akhir

Tujuan dari pengerjaan tugas akhir ini adalah:

1. Mengetahui barang bukti/artefak yang ditinggalkan oleh aplikasi Re-loader.
2. Mengetahui cara melakukan analisa forensik menggunakan teknik *Windows Live Forensics* dan *Dynamic Malware Analysis* pada aplikasi Re-loader.
3. Mengetahui dampak penerapan aplikasi Re-loader.

1.5 Manfaat Tugas Akhir

Manfaat yang diberikan dengan adanya tugas akhir ini adalah sebagai berikut:

1. Membantu penyidik menemukan bukti penggunaan aplikasi Re-loader dalam aktifitas pembajakan Windows.
2. Memberikan panduan dalam melakukan analisa *Windows Live Forensics* dan *Dynamic Malware Analysis* pada sebuah aplikasi yang dicurigai.
3. Menjadi dasar untuk penelitian selanjutnya dalam hal *malware* analysis menggunakan teknik statis dan *hybrid*.
4. Memberikan edukasi dampak penggunaan aplikasi Re-loader pada masyarakat.

1.6 Relevansi

Tugas akhir ini berkaitan dengan mata kuliah Forensika Digital, Keamanan Aset Informasi, dan Sistem Operasi. Tugas akhir ini masuk ke dalam bidang keilmuan laboratorium Infrastruktur dan Keamanan Teknologi Informasi serta mendukung salah satu profil lulusan JSI-ITS yaitu Konsultan dan Integrator Sistem.

Halaman ini sengaja dikosongkan

BAB 2
TINJAUAN PUSTAKA

Pada bagian tinjauan pustaka ini, akan dijelaskan mengenai referensi-referensi yang terkait dalam penyususan tugas akhir ini.

2.1 Penelitian Sebelumnya

Dalam merancang penelitian ini, penulis mengambil beberapa penelitian terkait *Dynamic Malware Analysis* dan *Live Windows Forensics*. Ada berbagai macam penelitian mengenai *malware* di dunia. Salah satunya adalah penelitian dari Navroop Kaur tentang menganalisa *malware* secara dinamis menggunakan cuckoo sandbox dan berhasil menemukan fitur baru pada sampel *malware* yang tidak diketahui sebelumnya [5]. Ada pula penelitian dari Fenu Gianni yang melakukan *Live Windows forensics* dan menemukan bahwa tidak ada perbedaan antara Windows XP dan Windows 7 [6]. Mandiant [7] melalui white papernya menjelaskan dengan detail mengenai IoC dan framework OpenIOC. Hun-Ya [8] juga menjelaskan bagaimana menggabungkan analisa *malware* dengan OpenIOC secara mendalam dalam papernya. Selain itu, penelitian ini juga terinspirasi dari video dengan judul "TWC: Malware Hunting with Mark Russinovich and the Sysinternals Tools" [9] yang menjelaskan penggunaan Sysinternals. **Tabel 2.1** adalah tabel mengenai perbandingan penelitian yang sudah ada.

Tabel 2.1 Penelitian sebelumnya

Penulis	Judul	Metode	Hasil
Navroop Kaur dan Amit Kumar Bindal, PhD [5]	A Complete Dynamic *Malware* Analysis	Dynamic Analysis menggunakan Cuckoo Sandbox	Menemukan fitur baru pada sampel *malware* yang tidak diketahui
Fenu Gianni	Live Digital Forensics:	Live Digital Forensics,	Tidak ditemukan

dan Fabrizio Solinas [6]	Windows XP vs Windows 7	Ram Forensics Analysis	perbedaan antara Windows XP dan Windows 7
Mandiant [7]	White Paper : An Introduction to OpenIOC	Framework OpenIOC	Menjelaskan Indicators of Compromise (IOCs) dan Framework OpenIOC
ISSA [10]	Working with Indicators of Compromise	Menggunakan tools yang tersedia untuk membuat dan menerapkan IOC	IOC dapat dibuat, dirubah dan diterapkan menggunakan berbagai macam tools
Hun-Ya Lock [8]	Using IoC (Indicators of Compromise) in *Malware* Forensics	Menggunakan analisa *malware* dinamis dan statis untuk menyusun IOC	*Malware* dapat teridentifikasi dan IoC dapat mendeteksi *malware* tersebut

2.2 Windows 7

Sejarah Microsoft dimulai ketika IBM memperkenalkan produk *Personal Computer* (PC) dan membutuhkan sebuah Operating Sistem (OS) yang dapat berjalan pada PC. IBM kemudian menghubungi Microsoft untuk menyiapkan OS tersebut. Microsoft yang pada saat itu belum memiliki pengalaman dalam membuat OS pergi ke Seattle Komputer Product untuk membeli sebuah OS bernama 86-DOS. Microsoft kemudian merubah nama 86-DOS menjadi MS-DOS dan menyerahkannya pada IBM untuk disertakan dalam produk PCnya. Saat itu ketika kita memesan PC dari IBM, kita akan mendapatkan DOS yang bernama PC-DOS

bukan MS-DOS. **Tabel 2.2** adalah daftar rilis Microsoft Windows [11] :

Tabel 2.2 Daftar rilis Microsoft Windows

Version	Marketing name	Editions	Release date	Build number
3.1	Windows NT 3.1	Workstation (named just *Windows NT*), Advanced Server	July 27, 1993	528
3.5	Windows NT 3.5	Workstation, Server	September 21, 1994	807
3.51	Windows NT 3.51	Workstation, Server	May 30, 1995	1057
4.0	Windows NT 4.0	Workstation, Server, Server Enterprise Edition, Terminal Server, Embedded	July 29, 1996	1381
5.0	Windows 2000	Professional, Server, Advanced Server	February 17, 2000	2195
		Datacenter Server	September 26, 2000	
5.1	Windows XP	Home, Professional, Media Center (original, 2004 & 2005), Tablet PC (original and 2005), Starter, Embedded,	October 25, 2001	2600

Version	Marketing name	Editions	Release date	Build number
		Home N, Professional N		
	Windows Fundamentals for Legacy PCs	N/A	July 8, 2006	
5.2	Windows XP	64-bit Edition Version 2003	March 28, 2003	3790
	Windows Server 2003	Standard, Enterprise, Datacenter, Web, Storage, Small Business Server, Compute Cluster	April 24, 2003	
	Windows XP	Professional x64 Edition	April 25, 2005	
	Windows Server 2003 R2	Standard, Enterprise, Datacenter, Web, Storage, Small Business Server, Compute Cluster	December 6, 2005	
	Windows Home Server	N/A	July 16, 2007	
6.0	Windows Vista	Starter, Home Basic, Home Premium,	Business: Novemb	6000 (RTM)

Version	Marketing name	Editions	Release date	Build number
		Business, Enterprise, Ultimate, Home Basic N, Business N	er 30, 2006	
			Consumer: January 30, 2007	6001 (SP1)
				6002 (SP2)
	Windows Server 2008	Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server, Itanium-Based Sistems	February 27, 2008	6001 (RTM)
				6002 (SP2)
6.1	Windows 7	Starter, Home Basic, Home Premium, Professional, Enterprise, Ultimate	October 22, 2009	7600 (RTM)
				7601 (SP1)
	Windows Server 2008 R2	Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server, Itanium-Based Sistems	October 22, 2009	7600 (RTM)
				7601 (SP1)
	Windows Home Server 2011	N/A	April 6, 2011	7600 (RTM)
6.2	Windows 8	Windows 8, Windows 8 Pro, Windows 8 Enterprise, Windows RT	October 26, 2012	9200

Version	Marketing name	Editions	Release date	Build number
	Windows Server 2012	Foundation, Essentials, Standard, Datacenter	September 4, 2012	9200
6.3	Windows 8.1	Windows 8.1, Windows 8.1 Pro, Windows 8.1 Enterprise, Windows RT 8.1	October 18, 2013	9600
	Windows Server 2012 R2	Foundation, Essentials, Standard, Datacenter	October 18, 2013	9600
10.0	Windows 10	Home, Pro, Pro Education, Enterprise, Education, IoT Core, Mobile, Mobile Enterprise	July 29, 2015	10240 (TH1)
				10586 (TH2)
				14393 (RS1)
	Windows Server 2016	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server	September 26, 2016	14393 (RS1)

Secara umum, hanya Windows NT 3.1, NT 4.0, XP, Vista dan Windows 10 yang merupakan perubahan besar dalam versi windows. Windows XP termasuk rilis yang sukses dimana hingga saat ini masih banyak ATM (*Automated Teller Machine*) di Indonesia masih menggunakan Windows XP. Setelah sukses dengan XP, Microsoft mencoba keberuntungannya dengan merilis Windows Vista.

Windows Vista tidak dapat menggapai sukses yang sama dengan Windows XP dikarenakan banyaknya masalah kompatibilitas dan batasan dari dalam sistem yang membuat pengguna lebih memilih untuk tetap menggunakan Windows XP. Disini Windows 7 hadir untuk memperbaiki kesalahan pada Windows Vista. Hal ini dibuktikan pada nomor versi dimana Windows Vista memiliki nomor versi 6.0 dan Windows 7 memiliki nomor versi 6.1.

Windows 7 tersedia dalam enam edisi berbeda yaitu Home Premium, Professional, dan Ultimate yang tersedia secara retail sementara Starter, dan Home Basic tersedia secara OEM serta Enterprise yang tersedia melalui Microsoft Volume Licensing. Pada dasarnya setiap edisi memiliki semua fungsi edisi sebelumnya dengan beberapa fungsi tambahan yang hanya tersedia untuk edisi tersebut. Berikut adalah daftar kebutuhan hardware minimal [12] **Tabel 2.3** dan batasan memory [13] **Tabel 2.4** pada Windows 7 :

Tabel 2.3 Kebutuhan hardware minimal Windows 7

Component	**Operating sistem architecture**	
	32-bit	**64-bit**
Processor	1 GHz IA-32 processor	1 GHz x86-64 processor
Memory (RAM)	1 GB	2 GB
Graphics card	DirectX 9 graphics processor with WDDM driver model 1.0	
Free hard drive space	16 GB	20 GB
Optical drive	DVD-ROM drive (Only to install from DVD-ROM media)	

Tabel 2.4 Batasan memory Windows 7

Edition	Processor architecture	
	IA-32 (32-bit)	x64 (64-bit)
Ultimate	4 GB	192 GB
Enterprise		
Professional		
Home Premium		16 GB
Home Basic		8 GB
Starter	2 GB	N/A

Windows mendukung berbagai macam file sistem seperti DOS, File Allocation Table (FAT), New Technology File Sistem (NTFS), dan Resilient File Sistem (ReFS). Semua file sistem ini pada dasarnya adalah pengembangan dari DOS yang dibuat pada tahun 1970. Setiap perubahan sistem akan mendukung file yang lebih besar pada sistem yang lebih besar, namun desain dasar fungsionalitas dari sistem file tetap sama seperti DOS. NTFS adalah sistem file yang paling umum pada windows namun baik itu NTFS maupun ReFS terdaftar sebagai milik Microsoft sehingga tidak banyak dokumentasi tersedia untuk detail yang lebih teknis [14].

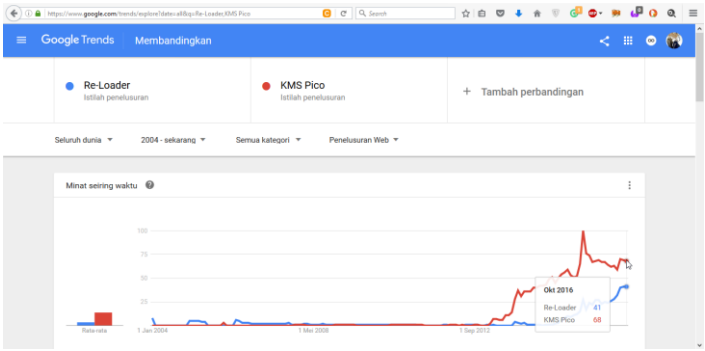
Windows juga menjaga sebuah database berupa registry berisi keseluruhan pengaturan dan perubahan. Pengaturan ini dibagi menjadi dua yaitu sistem dan pengguna sehingga setiap pengguna akan mendapatkan pengaturannya sendiri. Selain itu, Windows juga membuat log kejadian untuk digunakan oleh OS dan aplikasi. Terdapat tiga jenis log yang disimpan oleh Windows yaitu log aplikasi, Sistem dan kemanan [14].

2.3 Teknik Membajak Windows dan Re-loader

Pada dasarnya setiap aplikasi yang dirilis ke pasar sudah mengandung semua fungsionalitas yang ditawarkan dengan lengkap. Apabila sebuah aplikasi memiliki beberapa edisi seperti trial, basic dan pro, hanya proses aktivasi yang

menentukan fungsi apa saja berdasar edisi dari aktivasi yang diterima yang dapat diberikan. Sehingga fungsi yang dapat dijalankan tergantung pada proses ativasi meskipun pada saat melakukan instalasi aplikasi semua fungsionalitas penuh aplikasi sudah terpasang.

Dalam dunia aplikasi ada beberapa cara yang bisa digunakan untuk mengaktifkan aplikasi berbayar layaknya kita membeli secara sah. Beberapa diantaranya menggunakan serial number (SN), Crack, Keygen, dan Loader. Apalikasi yang sudah lama biasanya dapat diaktifkan hanya dengan memasukkan SN yang disertakan bersama aplikasi saat didownload atau bisa dicari di Google. Beberapa aplikasi bajakan juga disertai Crack yaitu beberapa file yang apabila ditempatkan pada direktori yang tepat dapat mengaktifkan aplikasi seperti aslinya. Adapun Keygen adalah aplikasi yang digunakan untuk menghasilkan beberapa SN beserta Activation Key. Beberapa Keygen juga menyertakan fungsi patch yaitu fungsi yang mirip dengan crack namun dilakukan secara otomatis. Apabila tidak dapat diaktivasi secara permanen, biasanya akan dipilih opsi terakhir yaitu menggunakan Loader. Loader memanfaatkan batas waktu untuk menggunakan aplikasi secara gratis atau trial. Loader akan membuat aplikasi terus berjalan meskipun telah melewati masa trial dengan memodifikasi aplikasi dan OS.



Gambar 2.1 Hasil Google Trend untuk Re-loader dan KMS Pico [15]

Berdasarkan data dari Google Trend diatas, KMS Pico dan Re-loader cukup dikenal dengan KMS Pico mendapatkan 68 poin sementara Re-loader mendapatkan 41 poin.

Pada saat Windows 8 dirilis pada tahun 2012 muncul sebuah aktivator baru yaitu KMS Micro yang dibuat oleh programmer di Rusia bernama Ratiborus. KMS Micro merupakan aktivator pertama yang mampu mengaktivasi Windows 8. Seiring berjalannya waktu KMS Micro dikembangkan kembali oleh Heldgard menjadi KMS Nano atau yang lebih dikenal dengan KMS Pico. KMS Pico dapat digunakan untuk mengaktivasi Windows Vista, 7, 8, 8.1 serta Office 2010 / 2013. KMS Pico berkerja layaknya Loader dengan mengaktivasi Windows selama 180 hari. KMS Pico berkerja secara otomatis pada saat Windows melakukan *booting*, sehingga KMS Pico bisa dianggap sebagai aktivator permanen [16].

Program kedua yang dapat digunakan untuk mengaktivasi Windows adalah aplikasi Re-loader. Re-loader merupakan pengembangan lanjutan dari Windows Loader yang dikembangkan oleh seorang programmer bermana Daz. Windows Loader ini berkerja dengan menginjeksi SLIC (*Sistem Licensed Internal Code*) kedalam windwos sebelum windows melalui proses booting [16]. Dengan cara ini Windows yang sudah terinstal Windows Loader akan

mampu menipu Microsoft WAT (*Windows Activation Technologies*) dan menganggap Windows tersebut asli. Adapun Re-loader menambahkan dukungan untuk mengaktivasi dari yang sebelumnya hanya Windows Vista dan 7 menjadi Windows 8, 8.1, dan 10. Re-loader juga menambahkan kemampuan untuk mengaktivasi aplikasi Office dari yang sebelumnya hanya Office 2010 menjadi Office 2013 dan 2016. Aktivasi yang dilakukan oleh Re-loader berlaku permanen kecuali pengguna melakukan update atau terdeteksi oleh Microsoft sebagai bajakan. Sebagian besar Re-loader yang ada di Google memiliki versi 2.6 dan 3.0 . Sebagian besar artikel yang memuat aplikasi Re-loader hanya salinan dari konten aslinya tanpa merubah file instalasi Re-loader. Hal ini dibuktikan dengan nilai hash yang sama dari file Re-loader meskipun didapatkan dari berbagai tempat.

2.4 Forensik Digital

Forensik digital termasuk cabang dari ilmu forensik yang fokus pada pemulihan dan investigasi dari bahan yang ditemukan dalam perangkat digital dan seringkali berkaitan dengan kejahatan komputer. Dengan kata lain, forensik digital adalah praktek mengumpulkan, menganalisis dan melaporkan data digital dengan cara yang sah dan diterima di pengadilan [17]. Forensik Digital menggunakan metodologi dan SOP yang telah teruji secara internasional untuk mendapatkan data yang otentik. Forensik digital juga dapat digunakan di berbagai bidang baik pemerintah maupun sektor privat seperti perusahaan.

Berikut adalah beberapa keuntungan yang dapat diberikan oleh forensik digital pada organisasi [18] :

- Memastikan integritas dan keberlangsungan dari sistem dan infrastruktur orgnisasi.
- Membantu organisasi mendapatkan informasi penting jika sistem atau jaringan organisasi tersebut mendapat serangan. Hal ini akan membantu organisasi menangkap pelaku kejahatan tersebut.

- Membantu organisasi dalam membuktikan kejahatan pelaku dengan mengekstrak, proses, dan menterjemahkan barang bukti sesuai dengan standar yang berlaku.
- Dapat melacak pelaku kriminal dunia maya dan teroris dimanapun berada secara efektif.
- Membantu menghemat waktu dan keuangan organisasi.
- Membantu melacak kasus sulit seperti pornografi anak dan spam email.

2.4.1 Metodologi Forensik Digital

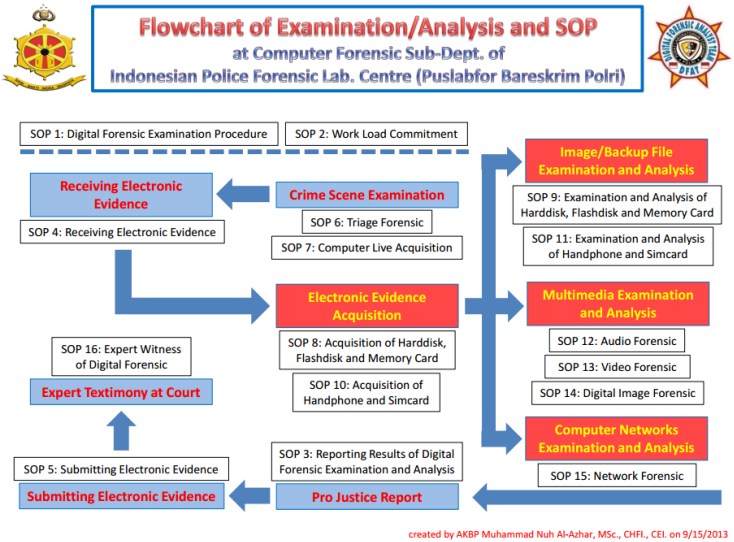
Terdapat beberapa metodologi dalam melakukan forensik digital. Menurut EC-Council [19] metode yang dapat digunakan untuk melakukan forensik digital adalah :

- Mendapatkan surat penyidikan.
- Mengamankan Tempat Kejadian Perkara (TKP).
- Mengumpulkan barang bukti.
- Mengamankan barang bukti.
- Mengambil data.
- Menganalisis data.
- Memberikan penilaian kasus dan barang bukti.
- Menyiapkan laporan final.
- Memberikan keterangan pada peradilan.

Sedangkan David Watson [20] merumuskan tahapan-tahapan forensik digital sebagai berikut :

- Menyiapkan barang bukti.
- Mengidentifikasi barang bukti.
- Mengekstrak barang bukti.
- Mendokumentasikan barang bukti.
- Menginterpretasikan barang bukti.
- Melakukan presentasi barang bukti, ke klien maupun pengadilan.

Berikut adalah contoh Standart Operating Procedure (SOP) yang digunakan di Puslapfor Bareskrim Polri :



Gambar 2.2 SOP Puslabfor Bareskrim Polri [21]

2.4.2 Incident Response dan Chain of Custody

Incident Response atau Respon Insiden adalah pendekatan yang terorganisir untuk menangani dan mengelola kejadian seperti pelanggaran keamanan atau serangan. Tujuannya adalah untuk menangani situasi dengan cara membatasi kerusakan, mengurangi waktu pemulihan dan biaya. Rencana tanggap insiden termasuk kebijakan yang mendefinisikan, dalam hal tertentu, apa yang merupakan insiden dan memberikan proses langkah-demi-langkah yang harus diikuti ketika insiden terjadi.

Chain of Custody adalah dokumen yang mendokumentasi penyitaan barang bukti, mengontrol, menganalisa, dan perpindahan dari barang bukti fisik maupun digital [22]. Setiap barang bukti harus dapat dilacak dari tempat kejadian perkara hingga ke ruang sidang. Jika terdapat kesalahan pada *Chain of Custody*, maka barang bukti yang sudah didapatkan dan di analisa bisa tidak berlaku lagi karena tidak dapat dipertanggungjawabkan kebenaran dan keasliannya.

2.4.3 Digital Forensics Workstation

Pada penelitian ini penulis menggunakan banyak aplikasi dan sistem operasi diantaranya Sysinternals Suite, FTK Imager, IoC Editor, IoC Finder, Ubuntu Studio, SANS SIFT, dan REMnux. Sysinternals adalah kumpulan aplikasi yang dibuat oleh Mark Russinovich dan biasa digunakan dalam melakukan forensik Windows [23]. FTK Imager adalah salah satu produk dari AccessData yang dapat melakukan duplikasi RAM dan hardisk dengan mudah [24]. IoC Editor adalah aplikasi buatan FireEye yang digunakan untuk membantu penyidik dalam membuat IoC dengan tapilan yang mudah dipahami [25]. IoC Finder adalah aplikasi buatan FireEye yang dapat mengumpulkan data sistem pada komputer serta melaporkan kehadiran dari IoC yang sudah dibuat sebelumnya [26]. Ubuntu Studio adalah sistem operasi yang gratis dan opensource serta ditunjukkan kepada para pembuat konten multimedia [27]. SANS Incident Forensics Toolkit (SIFT) adalah workstation yang dibuat khusus untuk menangani respon kejadian dan forensik digital dan dijalankan diatas sistem operasi Ubuntu [28]. REMnux adalah kumpulan aplikasi yang dibuat untuk membantu dalam menganalisa *malware* dan mengakomodasi berbagai macam analisa serta proses *reverse-engineering malware* atau mengembalikan *malware* menjadi kode untuk dianalisa secara statis [29].

2.4.4 Windows Live Forensics

Pada sebuah komputer umumnya terdapat dua jenis data yaitu *volatile* dan *nonvolatile*. Data yang bersifat *volatile* adalah data yang akan hilang ketika tidak ada arus listrik atau komputer dalam keadaan mati, contohnya adalah (*Random Access Memory*) RAM. Sementara data yang bersifat *nonvolatile* adalah data yang tetap ada meskipun tidak ada arus listrik, contohnya adalah hardisk dan flashdisk.

Windows Live Forensics atau analisa forensik Windows secara langsung merupakan metodologi yang mengekstrak

sistem yang masih berjalan untuk menghindari hilangnya data yang bersifat *volatile* atau mudah hilang ketika komputer mati [30]. Data yang termasuk dalam kategori *volatile* adalah *memory*, *swap file*, proses sistem, informasi file sistem, dan *registry*.

Metode ini akan memudahkan penyidik dalam memindahkan barang bukti namun tetap menjaga keaslian dari barang bukti tersebut. Pada kasus khusus bisa ditemukan sebuah hardisk yang hanya bisa dibuka oleh aplikasi tertentu yang berjalan di RAM. Karena tidak mungkin memindahkan komputer yang menyala tanpa memutus listrik, penyidik harus melakukan akusisi RAM menggunakan tools yang ada dan didapatkan kunci untuk membuka data pada hardisk. Umumnya metode ini akan menghasilkan barang bukti utama yang nantinya akan dianalisa beserta dengan komputer asli.

Salah satu dampak yang ditimbulkan apabila tidak melakukan analisa ini adalah penyidik akan kehilangan kesempatan untuk melakukan analisa secara *live*. Apabila penyidik menemui kasus seperti diatas tanpa melakukan analisa secara langsung maka semua analisanya akan sia-sia. Tidak ada data yang dapat dibaca karena hardisk telah terkunci, RAM sudah bersih karena tidak dialiri listrik dan kode pembuka hardisk hanya bisa dibuka oleh pelaku dimana hal ini akan memudahkan pelaku dalam menghapus barang bukti.

2.4.5 Malware Forensics Analysis

Malicious Software atau *Malware* adalah aplikasi yang bertujuan untuk merusak atau mengganggu operasi dari komputer dan sistem komputer seperti *virus*, *worms*, *trojan*, *ransomware*, *spyware*, *adware*, *scareware* dan lain lain [8]. Dalam analisa ini file yang diindikasi mengandung *malware* dianalisa menggunakan metode forensik yang dapat memastikan keaslian dari barang bukti disertai dengan proses analisa yang dapat dipercaya dan dilakukan kembali. Terdapat tiga jenis analisa *malware* diantaranya :

2.4.5.1 Dynamic Malware Analysis

Dynamic Malware Analysis atau analisa *malware* dinamis adalah prosses mengekstrak informasi dari *malware* pada saat *malware* tersebut berjalan. Teknik ini memungkinkan peneliti melihat lebih dalam pada fungsi yang dilakukan *malware* karena setiap kali *malware* berjalan dan menjalankan fungsi tertentu peneliti sudah mendapatkan datanya [31].

Untuk melakukan analisa malware secara dinamis dibutuhkan dua hal yaitu :

1. *Malware Test Environment.*
   Malware Test Environment adalah sebuah sistem dimana *malware* akan dijalankan untuk dianalisa. Sistem ini didesain untuk memenuhi semua kebutuhan bagi *malware* untuk berjalan secara sempurna dan terpisah dari sistem yang digunakan untuk membuat laporan atau analisa lainnya.
2. *Dynamic Analysis Tools*.
   Dynamic Analysis Tools adalah aplikasi yang digunakan untuk memonitor aktivitas dari *malware* pada sistem percobaan. Beberapa hal yang dimonitor adalah perubahan pada file sistem, *configuration file*, dan perubahan lain yang dibuat oleh *malware*.

Teknik ini termasuk yang paling beresiko namun paling efektif untuk dilakukan. Resiko yang tinggi dihasilkan dari malware yang benar-benar berjalan sehingga benar-benar bisa menginfeksi sistem lain apabila terdapat kesalahan.

Dalam buku Incident Response Computer Forensics menyarankan apasaja yang harus dilakukan agar aman dalam menganalisa malware sebagai berikut [32]:

1. Gunakan lingkungan virtual untuk menganalisa malware dan jangan pernah membuka file yang terinfeksi diluar lingkungan virtual.

2. Mesin virtual dapat menggunakan system operasi apapun. Tambahkan semua software analisa yang dibutuhkan, kemudian simpan sebagai snapshot.
3. Jaga agar software pada lingkungan virtual tetap update.
4. Matikan fitur drag and drop dan clipboard sharing.
5. Pastikan lingkungan virtual telah terisolasi.

Setelah analisa selesai kembalikan pada kondisi semula menggunakan fitur snapshot.

2.4.5.2 Static Malware Analysis

Static Malware Analysis atau analisa *malware* statis adalah teknik analisa *malware* dimana peneliti melakukan penyelidikan pada kode sumber *malware* dengan melakukan *reverse engineering* untuk mengembalikan aplikasi menjadi kode sumber tanpa menjalankan *malware* [33]. Analisa ini tergolong lambat dan membutuhkan pengetahuan teknikal mendalam. Masalah utama pada analisa ini adalah keterbatasan waktu yang dimiliki peneliti dimana *malware* bisa memiliki ribuan baris kode yang belum tentu benar.

2.4.5.3 Hybrid Malware Analysis

Hybrid Malware Analysis atau analisa *malware* secara gabungan adalah analisa *malware* yang menggabungkan teknik statis dan dinamis [33]. Saat menemukan suatu petunjuk pada kode assembly yang didapat dari analisa statis peneliti memastikannya dengan menjalankan *malware* seperti pada analisa dinamis dan mengambil kesimpulan.

2.4.5.4 Indicators of Compromise dan OpenIOC

Indicators of Compromise (IOCs) adalah artefak forensik yang didapatkan dari kejadian atau gangguan yang menimpa komputer atau jaringan [7]. OpenIOC adalah standar berbagi informasi ancaman TI yang memungkinkan peneliti untuk secara logika menggolongkan artefak forensik dan mengkomunikasikan informasi yang ada menjadi dapat dibaca oleh mesin atau komputer. OpenIOC ditulis menggunakan Extensible Markup Language (XML) yang

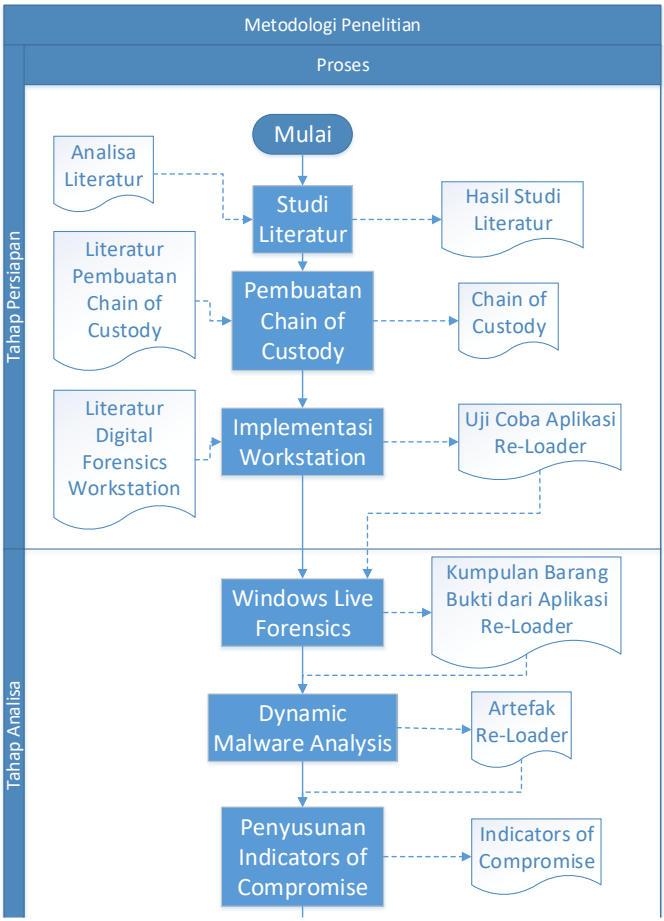
menyediakan standar format terorganisir dalam melakukan encoding data menjadi data yang dapat dibaca oleh mesin.

BAB 3
METODOLOGI PENELITIAN

Bagian ini menjelaskan bagaimana runtutan pengerjaan tugas akhir yang akan dilakukan beserta detail penjelasan untuk masing-masing tahapan.

3.1 Diagram Metodologi Pengerjaan Tugas Akhir

Diagram metode pada Tugas Akhir ini ditampilkan pada Gambar 3.1.



Gambar 3.1 Diagram alur metodologi tugas akhir

3.2 Studi Literatur dan Verifikasi Metode Dengan SOP

Tahapan ini dilakukan untuk menggali lebih banyak informasi dan *best practice* dalam melakukan teknik forensik digital. Penulis juga dapat memastikan serta memverifikasi metode, konsep-konsep dasar dan perkembangan dari setiap teknik yang digunakan pada tugas akhir ini. Pada tahapan ini diharapkan mampu menjadi dasar dari setiap aktivitas yang dilakukan.

3.3 Pembuatan Chain of Custody

Pada umumnya *Chain of Custody* digunakan untuk melacak perpindahan dari barang bukti dengan lebih dari satu orang analis. Pada tugas akhir ini penulis menggunakan *Chain of Custody* untuk memudahkan dalam mendukumentasikan perpindahan barang bukti antara Virtualbox, workstation dan komputer lain bila dibutuhkan. Adapun apabila penulis membutuhkan bantuan orang lain, *Chain of Custody* akan siap untuk mendokumentasikan sesuai standar. *Chain of Custody* juga akan mencatat analisa apa saja yang dilakukan beserta waktunya sehingga dapat mempermudah pembuatan laporan.

3.4 Implementasi Workstation

Penulis akan menggunakan workstation gabungan dari Ubuntu Studio 14.04, SANS SIFT, dan REMnux. Ubuntu Studio akan menangani kompabilitas untuk setiap file Windows di Linux, SANS SIFT akan menangani barang

bukti hasil duplikasi RAM dan hardisk, dan REMnux akan menangani analisa *malware* secara komprehensif. Aplikasi Virtualbox juga akan ditambahkan pada workstation untuk menjalankan Windows 7 secara virtual. Penulis juga menggunakan aplikasi dari Sysinternals yang disimpan dalam flashdisk dan dijalankan pada Windows virtual.

3.5 Windows Live Forensics

Pada tahap ini akan dilakukan pengumpulan barang bukti. Pada umumnya barang bukti yang dihasilkan dari forensik komputer adalah hasil duplikasi dari RAM dan hardisk menggunakan aplikasi FTK Imager. Implementasi aplikasi Re-loader membutuhkan Windows untuk melakukan restart, sehingga pada penelitian ini penulis melakukan tiga kali pengumpulan barang bukti. Pertama, saat selesai menginstall Windows 7 untuk mendapatkan file dalam kondisi bersih. Kedua, saat setelah selesai menginstall Re-loader dan tepat sebelum restart. Ketiga, saat Windows kembali hidup dari restat untuk mengumpulkan bukti dalam keadaan normal. Analisa Windows secara langsung juga mengumpulkan imformasi melalui Command Prompt dengan cara memasukkan perintah dasar maupun lanjutan untuk melengkapi data yang tidak terdapat pada hardisk dan RAM.

3.6 Dynamic Malware Analysis

Analisa *malware* dinamis dilakukan menggunakan aplikasi dari Sysinternals yang telah disimpan pada flashdisk. Aplikasi ini bersifat portable sehingga dapat langsung dijalankan tanpa harus menginstall dan merubah barang bukti. Aplikasi yang digunakan meliputi Process Explorer, Autoruns, Process Monitor, dan Systems Monitor. Analisa ini akan melihat aktivitas *malware* pada proses, registry, dan autorun di Windows 7. Process Explorer akan memeriksa proses yang berjalan terverifikasi dan bebas virus saat di bandingkan dengan database VirusTotal secara online. Autoruns akan memeriksa program yang berjalan secara otomatis saat komputer dinyalakan dan membandingkannya

dengan database VirusTotal secara online. Process Monitor akan memantau aplikasi yang telah ditentukan dan mencatat semua perubahan yang dihasilkan. Systems Monitor akan memantau system mulai dari awal berjalan hingga selesai digunakan dan mencatat semuanya dalam log file. Analisa ini juga akan menganalisa hasil duplikasi RAM dan hardisk untuk memastikan kebenaran dari hasil analisa Windows langsung. SANS SIFT dan REMnux akan menyediakan semua kebutuhan aplikasi dan keamanan yang dibutuhkan dalam penelitian ini dan telah terpasang pada Ubuntu Studio. Penulis berharap dari analisa ini akan menghasilkan komponen penyusun *Indicators of Compromise* yang akan digunakan pada tahap berikutnya.

3.7 Penyusunan Indicators of Compromise

Indicators of Compromise akan disusun menggunakan komponen tahap sebelumnya. Komponen ini dapat berupa nama file, hash, path, string, registry, dan berbagai macam file atau petunjuk lain yang dihasilkan selama aplikasi Re-loader berjalan. Komponen ini akan dituliskan kedalam IoC menggunakan aplikasi IoC Editor sehingga dapat menghasilkan IoC sesuai dengan framework OpenIOC. Pada setiap tahapan pengumpulan barang bukti juga dilakukan audit data yang dibutuhkan untuk IoC menggunakan IoC Finder. IoC yang telah dibuat dengan IoC Editor akan di gunakan pada IoC Finder sebagai acuan keberadaan malware. IoC Finder juga akan menghasilkan laporan kesesuaian IoC dengan barang bukti yang didapatkan saat audit IoC dan dapat digunakan sebagai bukti pembajakan Windows.

3.8 Penarikan Hasil dan Kesimpulan

Tahap ini adalah tahap terakhir dari penelitian ini dimana penulis merangkum dan mendokumentasikan hasil serta kesimpulan yang didapat. Hasil ini akan dibuat menjadi laporan penelitian yang diwujudkan menjadi buku tugas akhir mahasiswa. Buku tugas akhir ini akan berisi seluruh dokumentasi penting terkait pelaksanaan penelitian.

BAB 4
PERANCANGAN

Pada bab ini, akan dijelaskan mengenai data yang akan diolah beserta rancangan proses pengolahannya, serta mempersiapkan sistem yang akan digunakan untuk mengolah data.

4.1 Skenario

Untuk mendapatkan data yang berkualitas dibutuhkan skenario yang sesuai dengan kondisi dilapangan. Kondisi ini kemudian di sesuaikan dengan lingkungan penelitian yang dalam hal ini adalah lingkungan VirtualBox. Meskipun lingkungannya berbeda hasilnya tidak akan berbeda jauh.

Setelah mempelajari dari internet dan pengalaman memasang Windows bajakan, ternyata ada banyak cara berbeda yang dapat dilakukan untuk memasang Windows bajakan. Umumnya untuk memasang Windows bajakan pada komputer atau laptop yang memiliki slot pembaca DVD dibutuhkan DVD-R atau DVD-RW yang telah diisi ISO Windows. Cara ini sudah mulai ditinggalkan karena terlalu rumit karena harus mendownload ISO dari Windows yang akan dipasang dan menyiapkan DVD-R atau DVD-RW untuk kemudian di *burn* menggunakan *software* tertentu. Perlu diingat bahwa DVD-R hanya bisa digunakan untuk *write* sebanyak satu kali sehingga apabila proses *burn* gagal harus menyiapkan DVD-R baru. Setelah DVD siap, DVD tersebut dimasukkan kedalam slot pembaca DVD dan komputer dinyalakan untuk *booting* melalui DVD.

Saat ini ada cara yang lebih praktis daripada menggunakan DVD-R atau DVD-RW yaitu dengan menggunakan *Flashdisk*. Pada umumnya tidak semua komputer atau laptop memiliki pembaca DVD namun dapat dipastikan semua memiliki slot USB yang dapat digunakan untuk membaca *Flashdisk*. *Flashdisk* ini akan diisi dengan ISO Windows dan dibuat *bootable* agar bisa *booting* menggunakan *flashdisk.*

Dari kedua cara diatas, penggunaan *flashdisk* dapat diimitasi pada lingkungan VirtualBox. Pada VirtualBox dapat diatur agar *booting* melalui *file* ISO dan melakukan instalasi seperti biasa. Adapun proses selanjutnya adalah memasang .NET *framework* 4 dan Re-loader. Pemasangan ini tidak terlalu sulit karena pengguna hanya perlu memilih tombol "Next" layaknya memasang aplikasi biasa.

4.2 Pengumpulan Data

Penelitian ini mengambil data dari implementasi Re-loader pada Windows 7 didalam lingkungan VirtualBox. Proses pengambilan data telah mengikuti prosedur forensik digital dengan melakukan duplikasi pada RAM dan Hardisk menggunakan FTK Imager. Proses duplikasi dilakukan sebanyak tiga kali yaitu :

1. Tahap Clean
   Pada tahap ini, Windows 7 berada pada clean state atau fresh install dimana tidak ada aplikasi dan malware yang berjalan selain aplikasi bawaan Windows 7.
2. Face Infected 1
   Pada tahap ini, aplikasi Re-loader telah dijalankan dan dilakukan duplikasi sesaat sebelum Restart.
3. Tahap Infected 2
   Pada tahap ini, Windows 7 telah selesai Restart dan Re-loader telah terpasang dengan sempurna.

4.3 Chain of Custody (CoC)

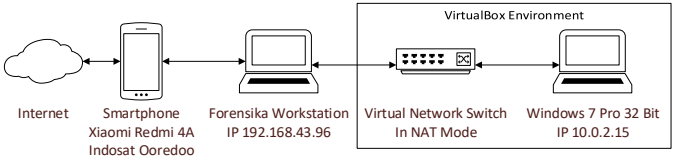
Penelitian ini akan didokumentasikan melalui media CoC agar peneliti berikutnya dapat melakukan penelitian yang sama dan mendapatkan hasil yang sama juga. CoC juga akan memudahkan transparansi apa saja yang dilakukan oleh peneliti dan mempertanggung jawabkan penelitiannya. Adapun form CoC penelitian ini terdapat pada lampiran dibagian akhir buku ini.

4.4 Perancangan Infrastruktur

Salah satu keuntungan menggunakan Virtual Box adalah fleksibilitas dalam mengatur jaringan dan Guest OS yang digunakan. Untuk menjaga Host OS agar tidak terinfeksi dibutuhkan pengaturan jaringan dan OS terbaik.

4.4.1 Pengaturan Jaringan

Instalasi Windows 7 pada VirtualBox tidak membutuhkan koneksi internet, namun untuk mendapatkan keadaan yang mendekati kenyataan VirtualBox dibuat tetap dapat terhubung dengan internet menggunakan pengaturan NAT pada jaringan VirtualBox sebagaimana pada **Gambar 4.1**.



Gambar 4.1.1 Pengaturan Jaringan

4.4.2 Spesifikasi Hardware

Forensika (Host OS)

Processor : Intel® Celeron® N2840

RAM : 4 GB

HDD : 500 GB

OS : GMacOS

Windows 7 (Guest OS)

Processor : Intel® Celeron® N2840

RAM : 2 GB

HDD : 20 GB

OS : Windows 7 Professional 32 Bit

4.4.3 Spesifikasi Software

Daftar aplikasi yang terpasang pada workstation

a. SANS Investigative Forensic Toolkit (SIFT) Workstation Version 3

b. Reverse Engineering Malware Linux (REMNux) v4

4.5 Instalasi Software

Tahap ini menjelaskan instalasi yang dilakukan pada workstation untuk memasang SANS SIFT dan REMnux. Dalam proses instalasi terdapat perbedaan mendasar pada tampilan atau Dekstop Environment (DE) workstation apabila urutan pemasangannya berbeda. Apabila memasang SANS SIFT terlebih dahulu kemudian REMnux, maka tampilan pada Ubuntu akan mengikuti DE standar Ubuntu yaitu Unity. Namun apabila memasang REMnux kemudia SANS SIFT maka DE pada Ubuntu akan berubah mengikuti DE bawaan dari REMnux yaitu LXDE. Dalam penelitian ini disarankan untuk memasang SANS SIFT terlebih dahulu kemudian memasang REMnux agar lebih mudah melakukan navigasi sesuai DE bawaan Ubuntu sebagai dasar workstation.

Setelah Ubuntu terpasang, gunakan script berikut untuk memasang SANS SIFT :

wget --quiet -O - https://raw.github.com/sans-dfir/sift-bootstrap/master/bootstrap.sh | sudo bash -s -- -i -s -y

Setelah SANS SIFT terpasang, gunakan script berikut untuk memasang REMNux :

wget --quiet -O - https://remnux.org/get-remnux.sh | sudo bash

Setelah selesai, gunakan script berikut untuk melakukan update SIFT dan REMNux :

update-sift && update-remnux

BAB 5
IMPLEMENTASI

Pada bab ini akan dijelaskan proses pengolahan barang bukti yang didapatkan dari tahap sebelumnya dan juga langkah-langkah analisa secara live, analisa memory, analisa hardisk dan mendapatkan indicator untuk IOC.

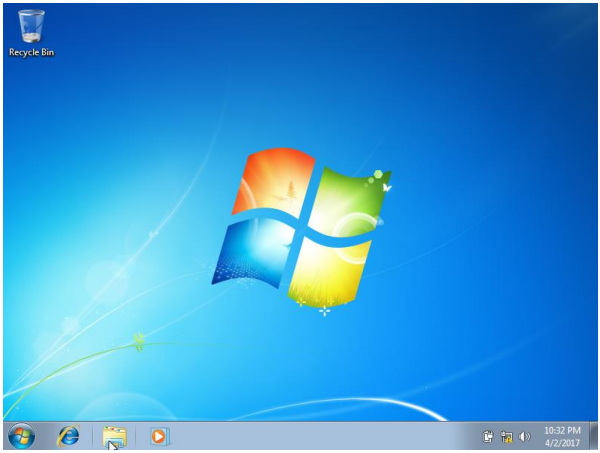
5.1 Menjalankan Skenario

Penelitian ini menggunakan skenario umum yang biasa digunakan untuk membajak windows. Skenario tersebut adalah :

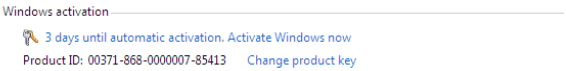
1. Pertama kali yang harus dilakukan adalah memulai instalasi dengan booting melalui DVD atau flashdisk yang bootable. Booting yang berhasil akan memiliki tampilan seperti pada **Gambar 5.1**.

Gambar 5.1 Proses booting awal

2. Instalasi Windows tergolong mudah. Hanya dengan mengikuti perintah yang ada, Windows telah terpasang memiliki tampilan seperti pada **Gambar 5.2**. Karena belum dilakukan aktivasi, Windows masih berada pada versi trial seperti pada **Gambar 5.3**.

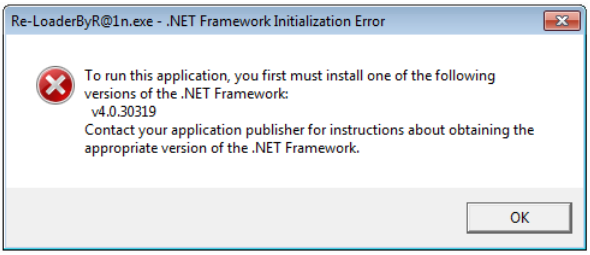


Gambar 5.2 Windows telah terpasang

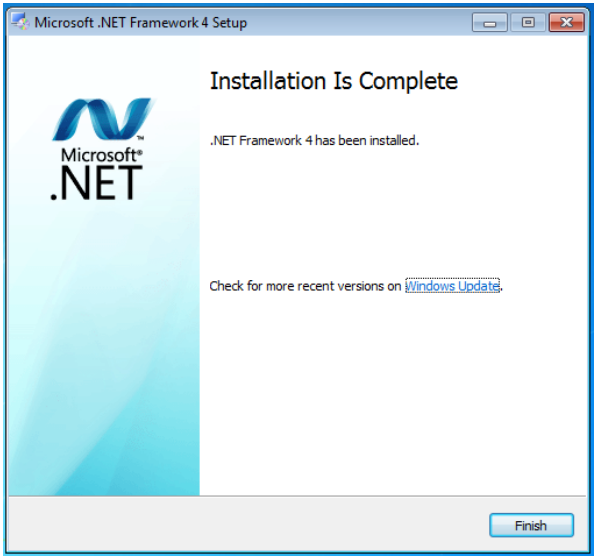


Gambar 5.3 Bukti Windows berada pada versi trial

3. Pada **Gambar 5.4** terlihat bahwa aplikasi Re-loader membutuhkan Framework .NET versi 4. Untuk itu dilakukan instalasi .Net Framework 4 seperti pada **Gambar 5.5**.

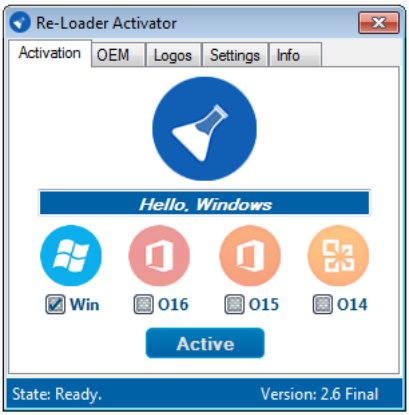


Gambar 5.4 Re-loader membutuhkan .Net Framework 4



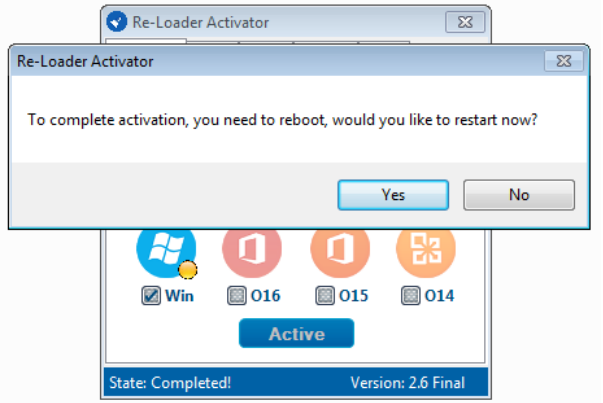
Gambar 5.5 Instalasi .Net Framework 4 selesai

4. Jalankan aplikasi ReLoader sebagai Run as Admin hingga muncul tampilan seperti pada **Gambar 5.6**.



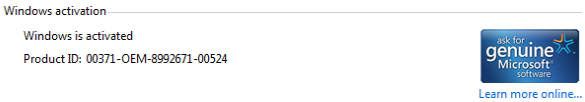
Gambar 5.6 Tampilan awal Re-loader

5. Re-loader akan meampilkan permintaan reboot seperti pada **Gambar 5.7**. Klik Yes untuk melakukan reboot.



Gambar 5.7 Re-loader membutuhkan reboot

6. Setelah komputer menyala kembali terlihat Windows telah aktif layaknya windows asli sebagaimana ditampilkan pada **Gambar 5.8**.

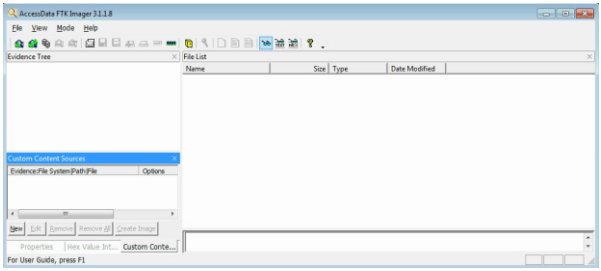


Gambar 5.8 Windows sudah aktif

5.2 Windows Live Forensics

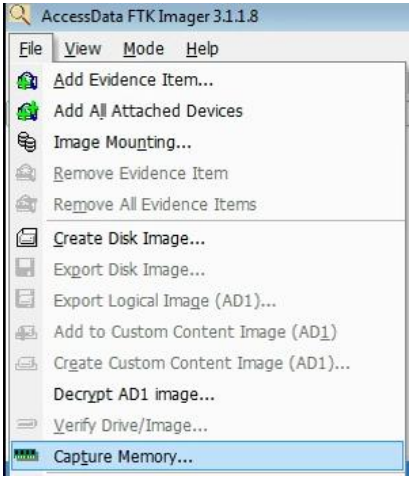
Windows Live Forensics menggunakan aplikasi FTK Imager untuk mendapatkan barang bukti berupa duplikasi hardisk dan RAM. Adapun cara menggunakan FTK Imager untuk menduplikasi RAM adalah sebagai berikut :

1. Buka aplikasi FTK Imager Lite melalui Command Prompt hingga tampil seperti pada **Gambar 5.9**.



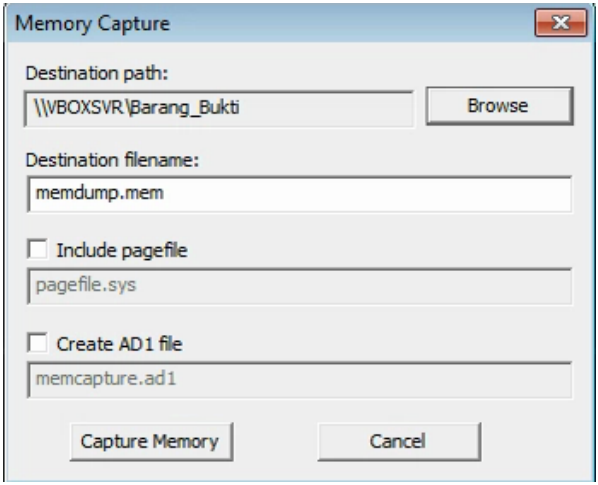
Gambar 5.9 Tampilan awal FTK Imager

2. Untuk menduplikat RAM, klik pada File pilih Capture Memory seperti pada **Gambar 5.10**.



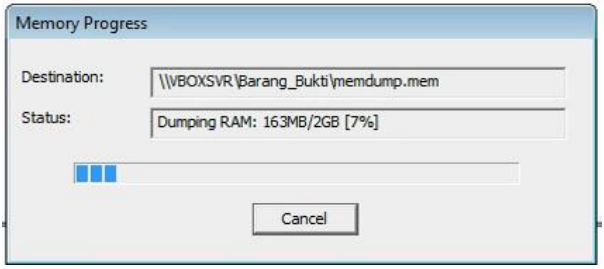
Gambar 5.10 Pilihan Capture Memory

3. Pada tampilan berikutnya sesuai **Gambar 5.11**, Pilih tempat penyimpanan dengan klik Browse dan sesuaikan nama file yang diinginkan pada bagian yang kosong.



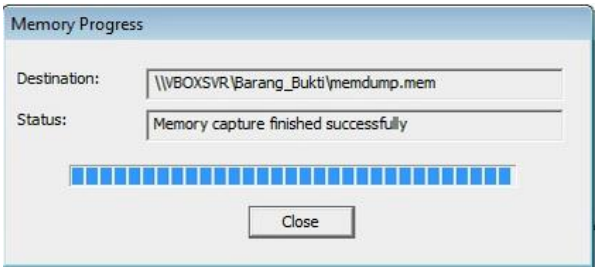
Gambar 5.11 Pilihan penyimpanan hasil Memory Capture

4. Proses duplikasi RAM akan berjalan seperti pada **Gambar 5.12**.



Gambar 5.12 Proses Imaging berjalan

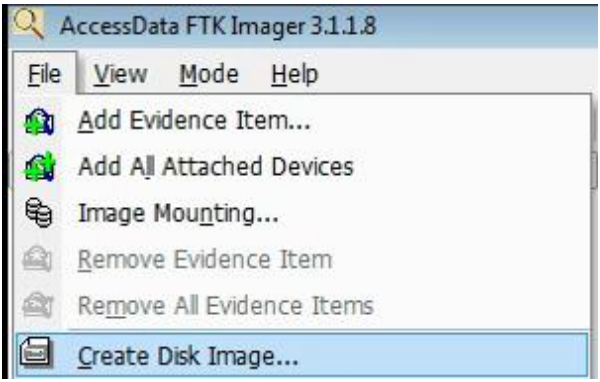
5. Proses yang selesai akan memiliki tampilan seperti pada **Gambar 5.13**.



Gambar 5.13 Tampilan proses imaging yang telah selesai

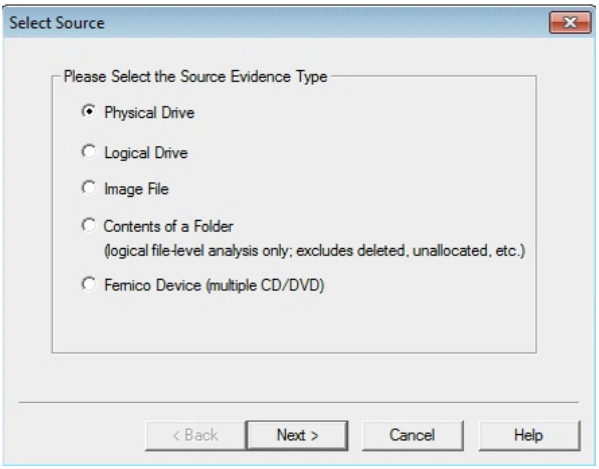
Setelah berhasil menduplikasi RAM langkah berikutnya adalah menduplikasi hardisk dengan cara sebagai berikut :

1. Untuk melakukan imaging pada Hardisk, klik pada menu File pilih Create Disk Image… seperti pada **Gambar 5.14**.



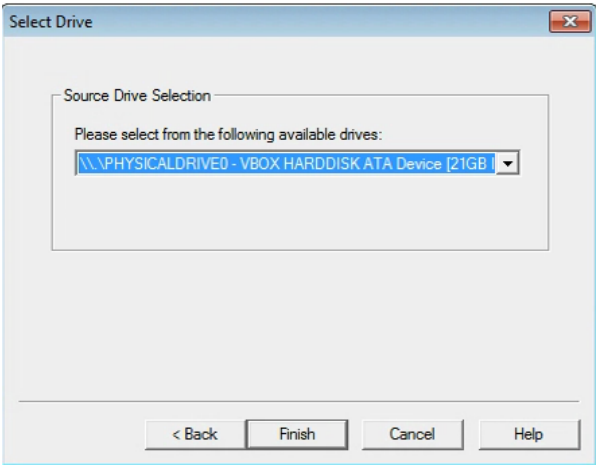
Gambar 5.14 Pilihan untuk duplikasi Hardisk

2. Pada tampilan **Gambar 5.15** disarankan untuk memilih Physical Drive untuk melakukan imaging pada keseluruhan hardisk.



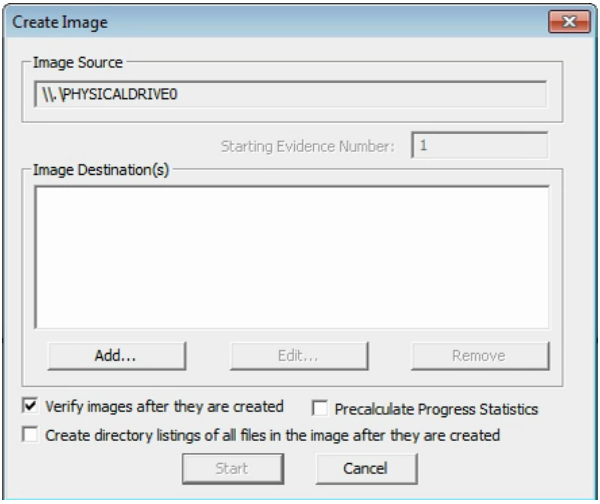
Gambar 5.15 Pilihan sumber barang bukti

3. Pada menu dropdown seperti pada **Gambar 5.16** pilih drive yang akan di imaging.



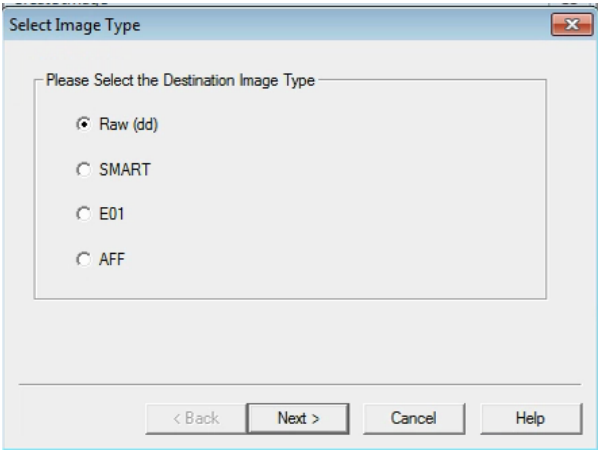
Gambar 5.16 Pemilihan drive barang bukti

4. Pada tampilan Create Image seprti pada **Gambar 5.17** Pilih Add untuk memilih lokasi penyimpanan file.



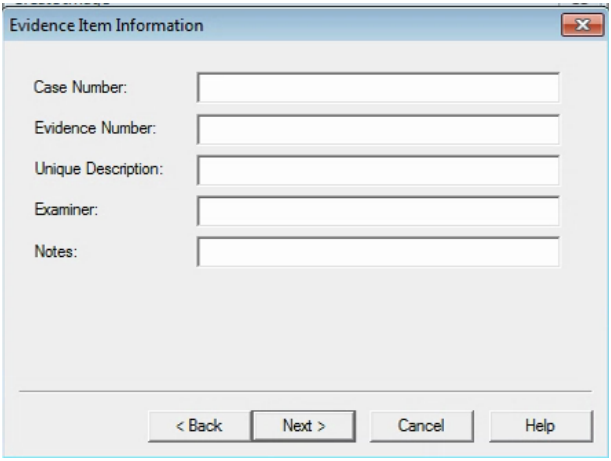
Gambar 5.17 Pemilihan tempat penyimpanan hasil imaging

5. Pada tampilan berikutnya, pilih format Raw (dd) karena format ini yang paling umum dan dapat dibaca pada aplikasi forensik berbayar maupun gratis sebagaimana terlihat pada **Gambar 5.18**.



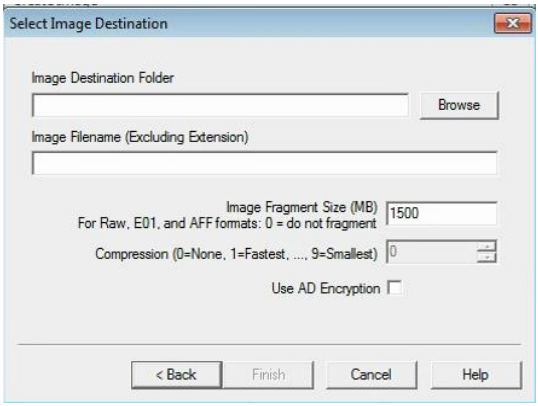
Gambar 5.18 Format yang tersedia pada FTK Imager

6. Tampilan seperti pada **Gambar 5.19** memungkinan peneliti untuk menambahkan informasi terkait barang bukti.



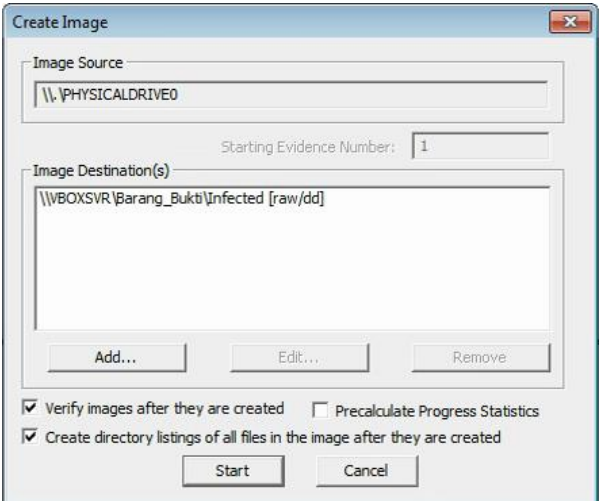
Gambar 5.19 Tempat mengisi informasi barang bukti

7. Pada tampilan berikutnya sesuai dengan **Gambar 5.20** Pilih lokasi penyimpanan file dan nama file. Untuk Image Fragment Size disarankan 0 agar file barang bukti tidak terpisah-pisah.



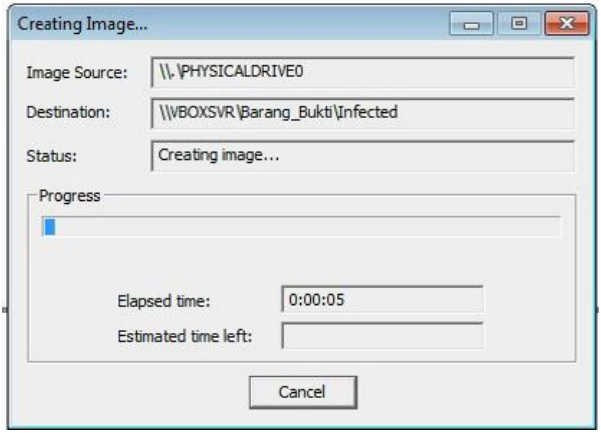
Gambar 5.20 Pengaturan akhir tempat menyimpan hasil imaging

8. Centang pada pilihan Create directory listings of all files in the image after they are created untuk memudahkan menganalisa direktori file seperti pada **Gambar 5.21**.



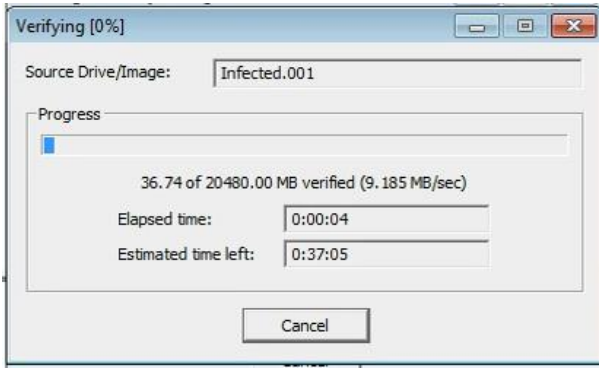
Gambar 5.21 Komfirmasi akhir sebelum imaging

9. Proses imaging akan berjalan seperti pada **Gambar 5.22**.



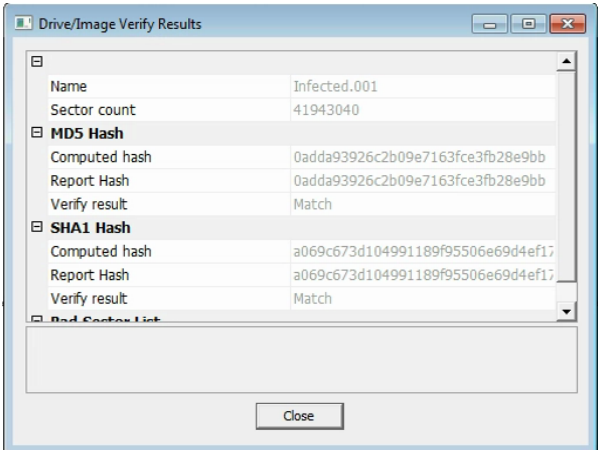
Gambar 5.22 Proses imaging

10. Setelah imaging selesai akan dilanjutkan dengan proses verifikasi seperti pada **Gambar 5.23**.



Gambar 5.23 Proses verifikasi file

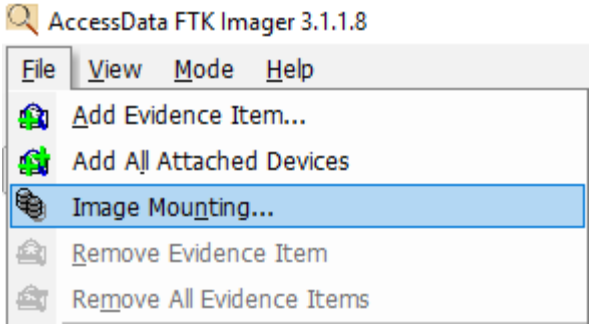
11. Setelah semua selesai, FTK imager akan menghasilkan hash untuk mejaga integritas file seperti pada **Gambar 5.24**.



Gambar 5.24 Hasil hash file

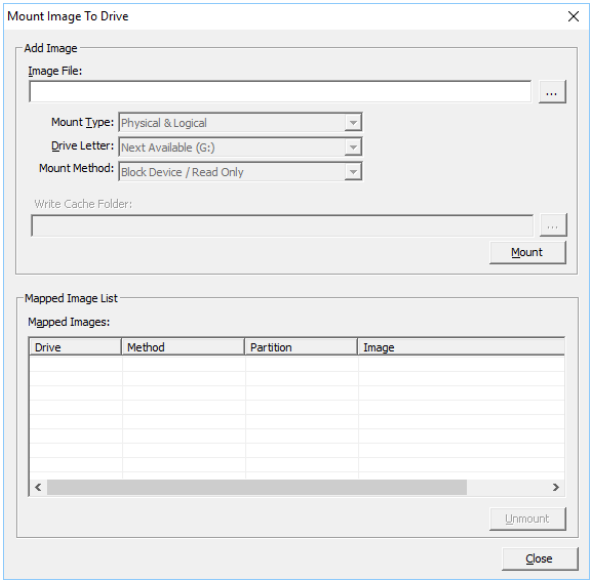
Image yang telah dihasilkan dapat dilihat dengan cara berikut :

1. Pilih File pilih Image Mounting untuk melakukan mounting pada image seperti pada **Gambar 5.25**.



Gambar 5.25 Pilihan Image Mounting

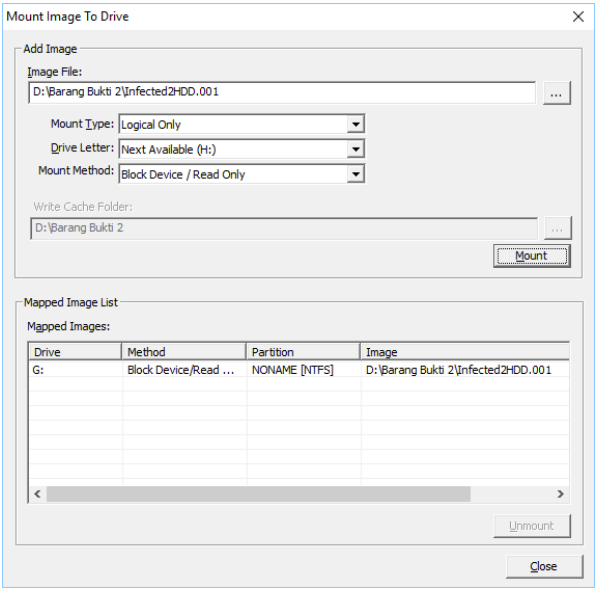
2. Pilih image file yang diinginkan pada tampilan **Gambar 5.26**.



Gambar 5.26 Tampilan Image Mounting

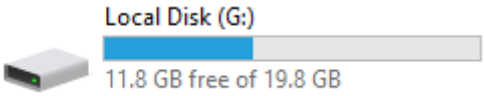
3. Mount type dapat disesuaikan dengan imaging awal baik logical maupun physical. Sangat disarankan

untuk memilih Block Device /Read Only pada Mount Method agar tidak mencemari barang bukti seperti pada **Gambar 5.27**.



Gambar 5.27 Pengaturan Image Mounting

4. Sebuah partisi baru akan muncul dan dapat dianalisa lebih lanjut seperti pada **Gambar 5.28**.



Gambar 5.28 Partisi baru hasil mounting

5.3 Dynamic Malware Analysis

Dynamic Malware Analysis menggunakan beberapa aplikasi campuran dari keluarga Sysinternals (Sysmon, Procexp, Procmon, dan Autoruns), Regshot, dan Volatility. Penggunaan banyak aplikasi akan menjaga objektifitas dari penelitian dengan meminimalkan bias dari hasil yang

didapatkan. Setiap aplikasi akan mengkonfirmasi hasil yang didapatkan dari aplikasi lainnya dan juga melengkapi beberapa bagian yang tidak bisa dijangkau oleh aplikasi itu sendiri. Untuk meminimalisir jejak yang tidak diperlukan, setiap aplikasi dijalankan melalui commandprompt (cmd). Apabila komputer target dapat menerima flashsik, dapat langsung mengakses drive letter yang diberikan oleh komputer. Namun apabila aplikasi forensik disimpan menggunakan folder yang dishare melalui jaringan, peneliti dapat menggunakan perintah *net use* seperti :

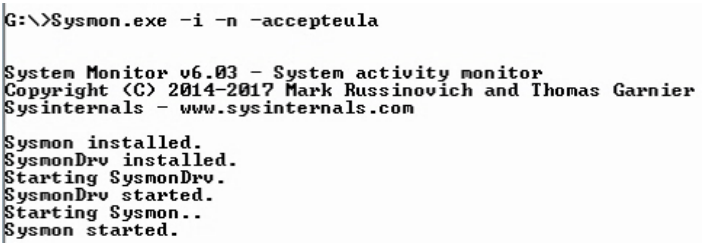
net use F: \\VBOXSRV\Forensika_Tool /Persistent:No.

5.3.1 Analisa System Monitor (Sysmon)

Sysmon sangat handal dalam mengawasi aktifitas yang terjadi pada sistem. Untuk mengoptimalkan kinerja, Sysmon di pasang pada saat sistem masih baru dan bersih. Untuk menggunakan Sysmon masukkan perintah :

Sysmon.exe –I –n –accepteula

Aplikasi Sysmon akan berjalan dan menghasilkan output seperti pada **Gambar 5.29**.



Gambar 5.29 Perintah dalam menjalankan Sysmon

Log hasil Sysmon akan disimpan pada Event Viewer pada bagian Applications and Services Logs pilih Microsoft pilih Windows pilih Sysmon pilih Operational. File log ini dapat disimpan sebagai Event Viewer (*.evtx), Xml (*.xml), Text (*.txt), dan Comma Separated Value (*.CSV).

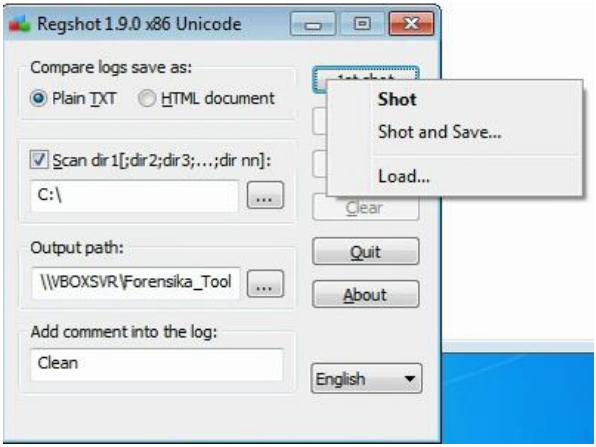
5.3.2 Analisa Regshot

Regshot memiliki kemampuan dalam merekam perubahan pada registry dan file pada direktori yang telah ditentukan. Regshot memiliki 2 jenis metode perekaman yaitu Unicode dan ANSI. ANSI dapat digunakan pada semua sistem operasi baik yang baru seperti Windows 10 maupun yang lama seperti Windows ME. Unicode hanya dapat digunakan untuk sistem operasi Windows XP sampai dengan Windows 10. Dalam penggunaannya apabila komputer yang akan dianalisa lebih lama dari windows XP disarankan menggunakan ANSI dan apabila diatas Windows XP disarankan menggunakan Unicode. **Gambar 5.30** menampilkan isi direktori Regshot pada umumnya

```
G:\Regshot-1.9.0>dir
 Volume in drive G is VBOX_Forensika_Tool
 Volume Serial Number is 0000-0807

 Directory of G:\Regshot-1.9.0

02/03/2013  03:40 AM           136,704 Regshot-x64-Unicode.exe
02/03/2013  03:32 AM            27,032 License.txt
02/03/2013  03:33 AM             7,498 History.txt
02/03/2013  03:41 AM           122,880 Regshot-x86-Unicode.exe
02/03/2013  03:41 AM           132,096 Regshot-x64-ANSI.exe
02/03/2013  03:34 AM             6,368 ReadMe.txt
02/03/2013  03:41 AM           118,784 Regshot-x86-ANSI.exe
08/27/2017  08:26 AM               151 regshot.ini
02/03/2013  03:32 AM            27,749 language.ini
               9 File(s)        579,262 bytes
               0 Dir(s)   8,586,010,624 bytes free

G:\Regshot-1.9.0>Regshot-x86-Unicode.exe
```

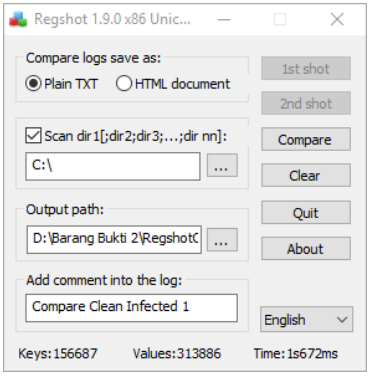
Gambar 5.30 Perintah dalam menjalankan Regshot

Pada **Gambar 5.31** berikut dapat ditentukan direktori yang akan dipantau dan format laporan perbandingan yang dapat dipilih antara Plain Text (.txt) atau HTML Document (.html). Hasil Regshot disimpan dalam sebuah file dengan ekstensi .hivu yang dapat digunakan kembali bila dibutuhkan.



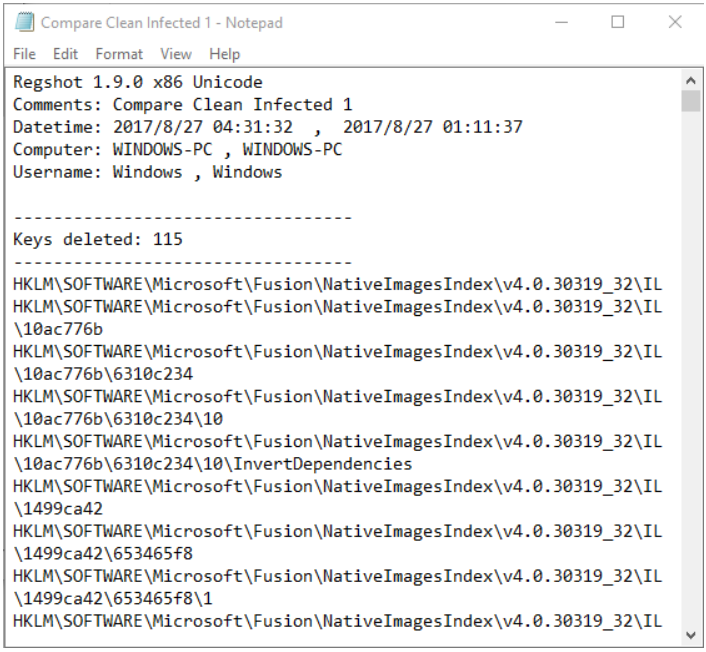
Gambar 5.31 Pengaturan untuk Shot pada Regshot

Secara konsep, Regshot dibuat untuk membandingkan antara 2 keadaan yakni sebelum dan sesudah. Dalam penelitian ini terdapat 3 keadaan yaitu Clean, Infected 1 dan Infected 2 sehingga setiap keadaan dilakukan Shot and Save untuk mendapatkan 3 file hivu. Untuk menganalisa file hivu klik 1st shot pilih Load dan pilih file hivu pertama. Klik 2nd shot pilih Load dan pilih file hivu yang ingin di bandingkan dengan hivu pertama seperti pada **Gambar 5.32**.



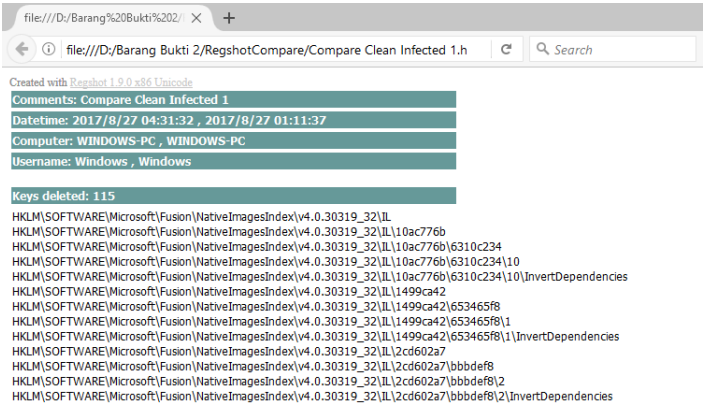
Gambar 5.32 Pengaturan untuk Compare Regshot

Gambar 5.33 adalah hasil perbandingan dalam bentuk Plain TXT (.txt)



Gambar 5.33 Hasil Regshot dalam bentuk text

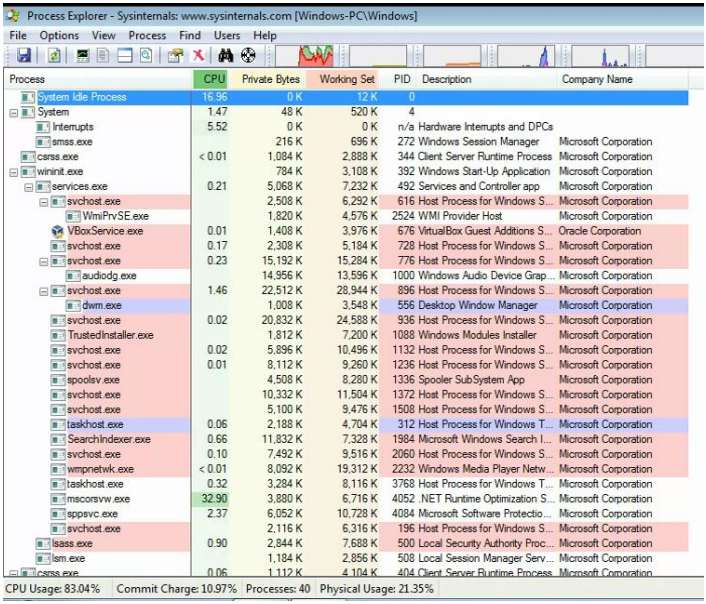
Gambar 5.34 adalah hasil perbandingan dalam bentuk HTML document (.html)



Gambar 5.34 Hasil Regshot dalam bentuk html

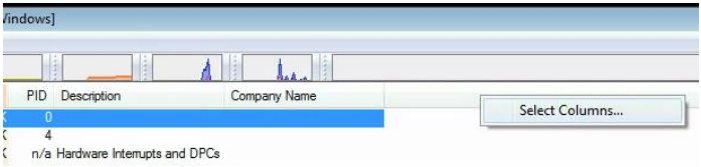
5.3.3 Analisa Process Explorer (Procexp)

Procexp memiliki fungsi yang sama dengan Task Manager namun memiliki fitur yang lebih lengkap. Procexp sudah terintegrasi dengan VirusTotal sehingga bisa menguji proses secara online apakah mengandung virus atau malware. **Gambar 5.35** adalah tampilan awal Process Explorer.



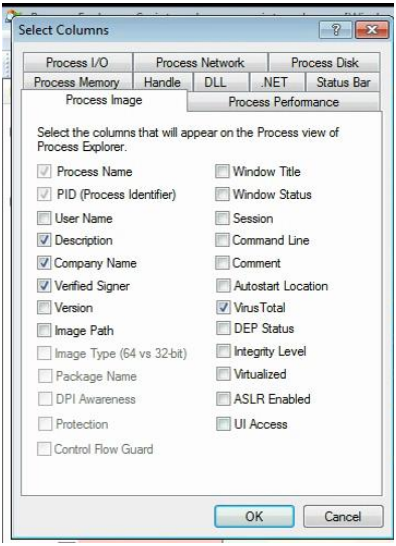
Gambar 5.35 Tampilan Procexp

Untuk menampilkan kolom VirusTotal klik kanan pada kolom yang kosong dan pilih Select Colomns seperti pada **Gambar 5.36**.



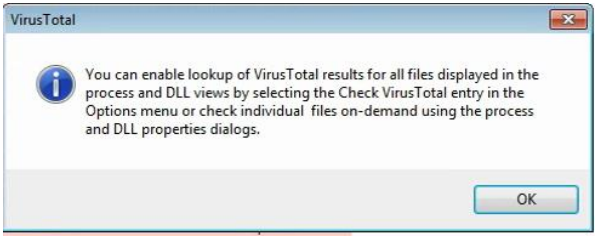
Gambar 5.36 Menampilkan Select Columns

Pada Process Image pilih Verivied Signer dan Virus Total seperti pada **Gambar 5.37**.



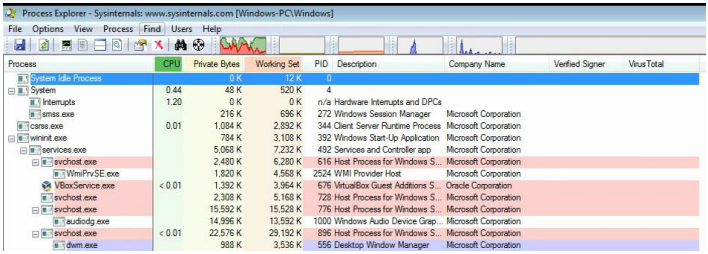
Gambar 5.37 Pilihan kolom yang bisa ditampilkan

Pada popup yang muncul klik pada bagian OK untuk melanjutkan seperti pada **Gambar 5.38**.



Gambar 5.38 Pemberitahuan untuk mengaktifkan VirusTotal

Kolom Verivied Signer dan Virus Total akan muncul seperti **Gambar 5.39**.

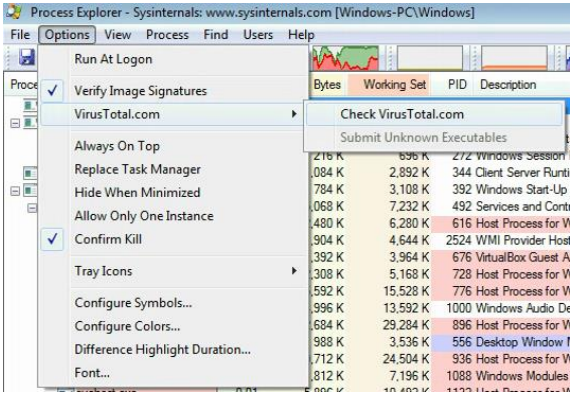


Gambar 5.39 Tampilan kolom baru

Untuk menguji Verivied Signer klik Options pilih Verify Image Signatures seperti pada **Gambar 5.40**.

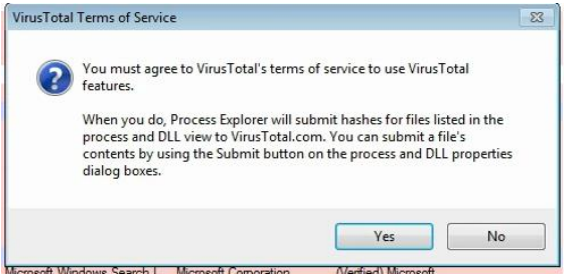
Gambar 5.40 Pilihan untuk Verify Image Signatures

Untuk melihat hasil analisa Virus Total, klik Options pilih VirusTotal.com dan pilih Check VirusTotal.com seperti pada **Gambar 5.41**.



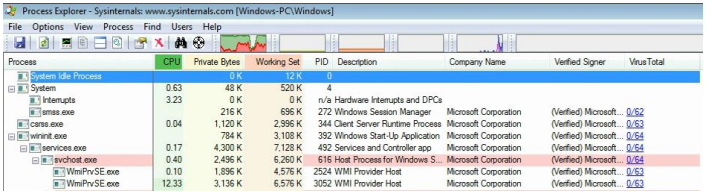
Gambar 5.41 Pilihan untuk Check VirusTotal.com

Untuk menggunakan VirusTotal harus setuju dengan Terms of Service pada **Gambar 5.42**.



Gambar 5.42 Pernyataan ToS VirusTotal

Setelah selesai Process Explorer dapat memperlihatkan proses yang tidak terverifikasi dan mengandung virus maupun malware menurut VirusTotal seperti pada **Gambar 5.43**.



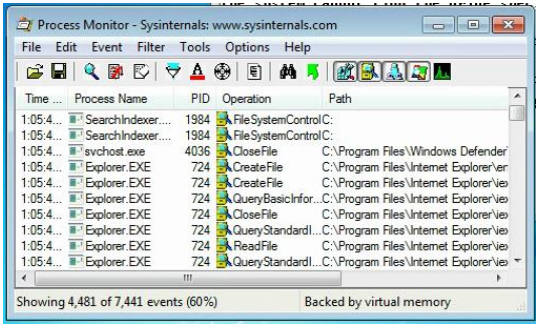
Gambar 5.43 Tampilan keseluruhan kolom yang dibutuhkan

5.3.4 Analisa Process Monitor (Procmon)

Procmon memiliki pendekatan yang berbeda dengan Procexp dimana Procmon akan dapat difokuskan untuk memonitor satu program atau proses. Untuk dapat menjalankan Procmon harus menyetujui License Agreement seperti pada **Gambar 5.44**.

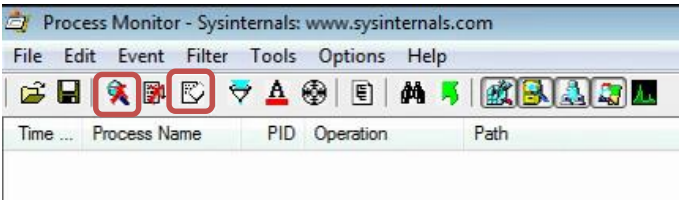
Gambar 5.44 Pernyataan License Agreement SysInternals

Gambar 5.45 adalah tampilan awal dari Procmon.



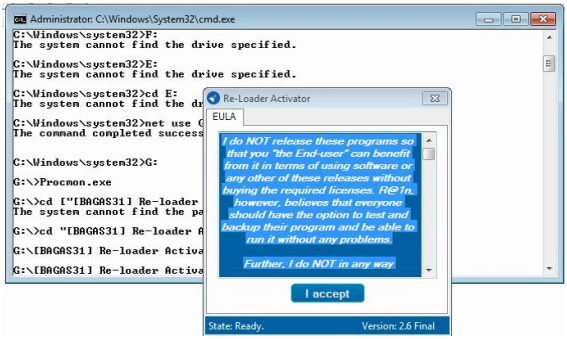
Gambar 5.45 Tampilan awal procmon

Sebelum memulai menganalisa, klik ikon ke 3 dari kiri untuk menghentikan pencarian event dan klik ikon ke 5 dari kiri untuk membersihkan tampilan seperti pada **Gambar 5.46**.



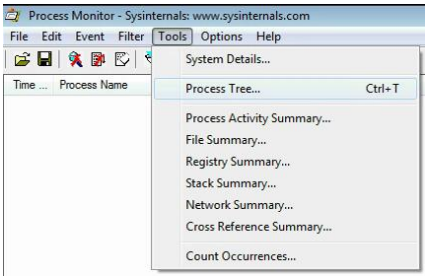
Gambar 5.46 Tampilan procmon yang bersih

Untuk bisa memonitor aplikasi, aplikasi tersebut harus juga berjalan saat Procmon berjalan seperti pada **Gambar 5.47**.



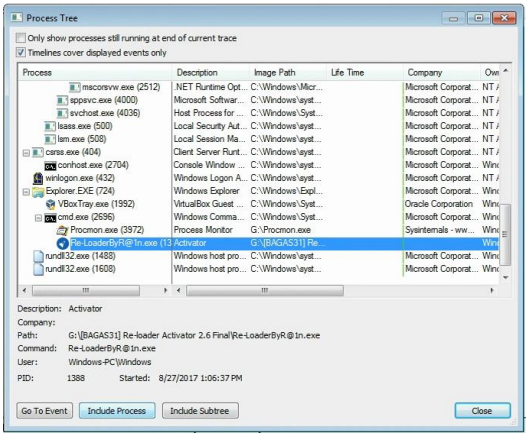
Gambar 5.47 Menjalankan Re-loader dari CMD

Untuk mulai memonitor klik pada Tools pilih Process Tree seperti pada **Gambar 5.48**.



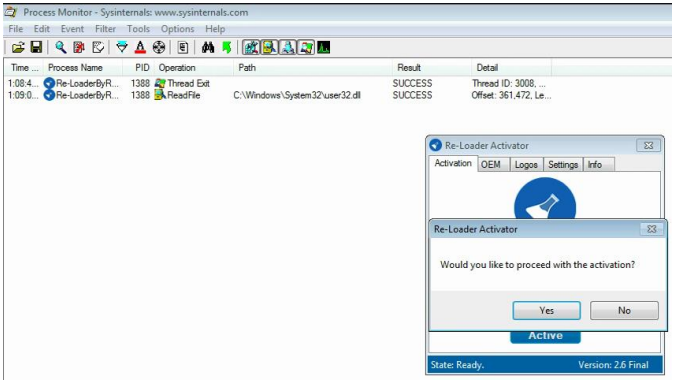
Gambar 5.48 Pilihan Procss Tree

Pada **Gambar 5.49** terlihat bahwa aplikasi Re-loader telah berjalan dan dapat dimasukkan dalam daftar monitor dengan mengklik Include Process



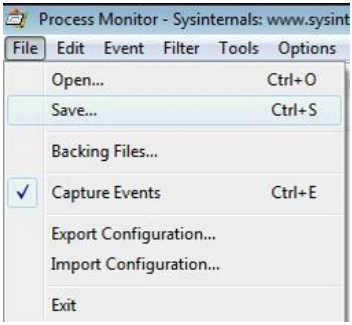
Gambar 5.49 Pilih proses Re-loader

Setelah Re-loader masuk dalam daftar monitor, apapun yang dilakukan oleh Re-loader akan terekam dalam Procmon seperti pada **Gambar 5.50**.



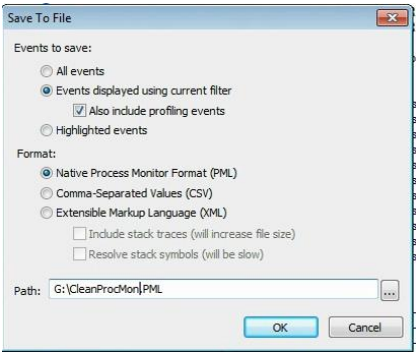
Gambar 5.50 Jalankan Re-loader untuk merekam aktifitas program

Hasil monitor dari Procmon dapat disimpan dengan mengklik File pilih Save seperti pada **Gambar 5.51**.



Gambar 5.51 Pilihan untuk menyimpan hasil procmon

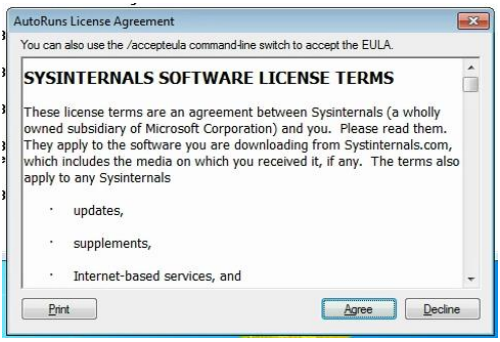
File hasil monitor Procmon dapat disimpan dalam 3 format yaitu PML, CSV, dan XML seperti pada **Gambar 5.52**.



Gambar 5.52 Pengaturan penyimpanan procmon

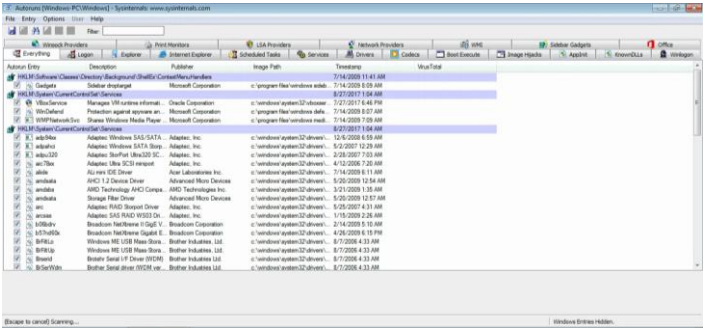
5.3.5 Analisa Autoruns

Autoruns berfungsi untuk memonitor fungsi autorun (Menjalankan sebuah program atau aplikasi secara otomatis saat komputer dinyalakan atau media penyimpanan diaktifkan) yang memiliki kemungkinan menjalankan virus atau malware. Autoruns juga akan menguji apakah fungsi autorun yang ada berasal dari Microsoft sendiri atau ditambahkan oleh aplikasi lain. Untuk menjalankan AutoRuns harus menyetujui License Agreement seperti pada **Gambar 5.53**.



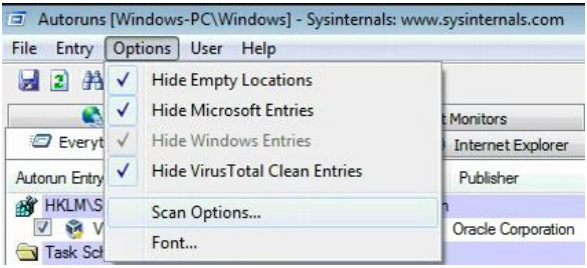
Gambar 5.53 pernyataan License Agreement SysInternals

Gambar 5.54 adalah tampilan awal AutoRuns dimana banyak fungsi autorun yang tersimpan dalam registry dan menjalankan berbagai program sekaligus.



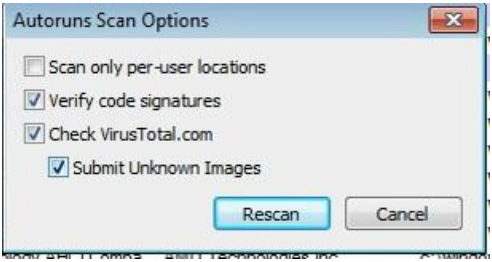
Gambar 5.54 Tampilan awal autoruns

Setelah Autoruns siap dan pencarian autorun berhenti, analisa lanjutan dilakukan dengan meminimalisir hasil yang tidak diperlukan. Autorun yang resmi dan tidak berbahaya dapat disembunyikan dengan klik Options pilih Hide Empty Locations pilih Hide Microsoft Entries pilih Hide Windows Entries pilih Hide VirusTotal Clean Entries. Selanjutnya klik Options pilih Scan Options untuk menampilkan pilihan lanjutan seperti pada **Gambar 5.55**.



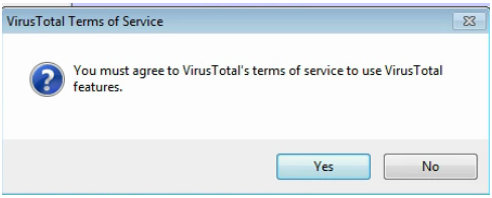
Gambar 5.55 Pilihan filter autorun

Gambar 5.56 adalah tampilan Autoruns Scan Options. Pada tampilan ini beritanda centang pada Verify code signatures, Check VirusTotal.com, Submit Unknown Images



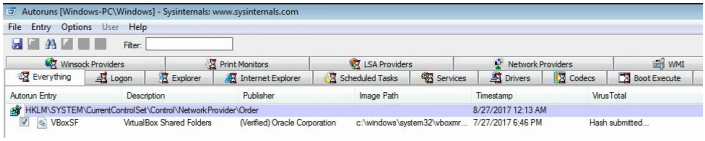
Gambar 5.56 Pilihan scan autorun

Untuk dapat menggunakan VirusTotal harus menyetujui VirusTotal Terms of Service pada **Gambar 5.57**.



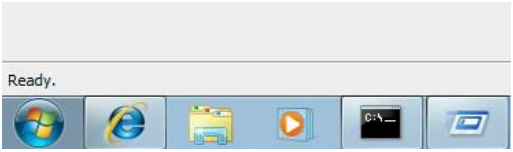
Gambar 5.57 Pernyataan ToS VirusTotal

Autoruns akan mulai mencari autorun yang tidak sesuai dengan kriteria hide diawal sebagaimana ditampilkan dalam **Gambar 5.58**.



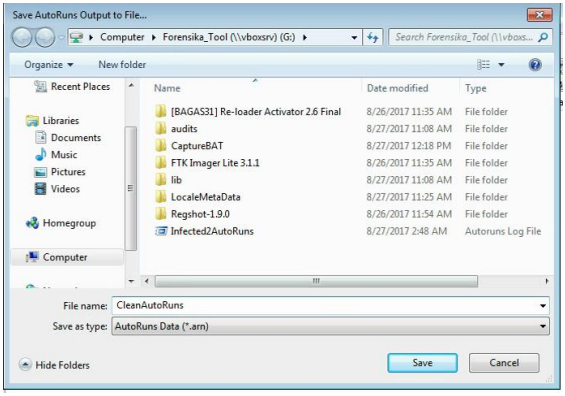
Gambar 5.58 Tampilan proses pencarian autorun

Pencarian akan selesai apabila status pada bagian kiri bawah aplikasi menjadi Ready seperti pada **Gambar 5.59**.



Gambar 5.59 Pemberitahuan pencarian selesai

Autorun yang telah didapatkan dapa disimpan dalam bentuk AutoRuns Data (.am) untuk dianalisa lebih lanjut seperti pada **Gambar 5.60**.



Gambar 5.60 Penyimpanan hasil autorun

5.3.6 Analisa Volatility

Anlisa pada memory memiliki pendekatan yang berbeda dengan analisa pada *removable media* seperti Hardisk dan Flashdisk dimana hasil duplikasi dari RAM hanya bisa di baca dan di ekstrak. Aplikasi Volatility akan menganalisa

barang bukti dengan menjelaskan apa saja isi dari RAM yang telah di bekukan baik itu program maupun berkas pendukungnya. Analisa menggunakan Volatility ini akan di lakukan dalam setiap tahap barang bukti. Volatility dapat berjalan pada sistem operasi Windows maupun Linux. Dalam penelitian ini digunakan Volatility dengan sistem operasi Windows yang mendukung implementasi OpenPyxl. OpenPyxl dapat menyimpan hasil analisa Volatility dalam bentuk Excel .xlsx. Adapun analisanya adalah sebagai berikut :

1. Buka terminal pada Windows seperti Gambar dibawah dan masuk kedalam folder tempat menyimpan barang bukti
2. Untuk memeriksa jenis OS yang digunakan masukkan perintah berikut dengan hasil seperti **Gambar 5.61**.

   volatility2.6.exe -f CleanRAM.mem imageinfo

```
D:\Barang Bukti 2>volatility2.6.exe -f CleanRAM.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\Barang Bukti 2\CleanRAM.mem)
                      PAE type : No PAE
                           DTB : 0x185000L
                          KDBG : 0x82958be8L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x82959c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2017-08-27 04:14:20 UTC+0000
     Image local date and time : 2017-08-27 11:14:20 +0700
```

Gambar 5.61 Hasil imageinfo

Untuk lebih meyakinkan dapat juga memasukkan perintah berikut dengan hasil seperti **Gambar 5.62**.

volatility2.6.exe -f CleanRAM.mem kdbgscan

```
D:\Barang Bukti 2>volatility2.6.exe -f CleanRAM.mem kdbgscan
Volatility Foundation Volatility Framework 2.6
**************************************************
Instantiating KDBG using: D:\Barang Bukti 2\CleanRAM.mem WinXPSP2x86 (5.1.0 32bit)
Offset (P)                    : 0x2958be8
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x86_23418
Version64                     : 0x2958bc0 (Major: 15, Minor: 7600)
PsActiveProcessHead           : 0x82970658
PsLoadedModuleList            : 0x82977570
KernelBase                    : 0x82838000

**************************************************
Instantiating KDBG using: D:\Barang Bukti 2\CleanRAM.mem WinXPSP2x86 (5.1.0 32bit)
Offset (P)                    : 0x2958be8
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x86
Version64                     : 0x2958bc0 (Major: 15, Minor: 7600)
PsActiveProcessHead           : 0x82970658
PsLoadedModuleList            : 0x82977570
KernelBase                    : 0x82838000

**************************************************
Instantiating KDBG using: D:\Barang Bukti 2\CleanRAM.mem WinXPSP2x86 (5.1.0 32bit)
Offset (P)                    : 0x2958be8
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP0x86
Version64                     : 0x2958bc0 (Major: 15, Minor: 7600)
PsActiveProcessHead           : 0x82970658
PsLoadedModuleList            : 0x82977570
KernelBase                    : 0x82838000
```

Gambar 5.62 Hasil kdbgscan

Kedua perintah diatas menghasilkan 2 buah profil yaitu Win7SP0x86 dan Wind7SP0x86. Hal ini menandakan bahwa penggunaan kedua profil tersebut tidak akan menghasilkan perbedaan sehingga profil manapun yang dipilih akan menghasilkan analisa yang sama.

3. Untuk memeriksa proses yang berjalan dapat dilakukan dengan 3 cara yaitu pslist, pstree dan psscan. Untuk menggunakan pslist masukkan perintah berikut dengan hasil seperti **Gambar 5.63**.

   volatility2.6.exe -f CleanRAM.mem --profile=Win7SP1x86 pslist --output=xlsx --output-file=CleanPslist.xlsx

```
D:\Barang Bukti 2>volatility2.6.exe -f CleanRAM.mem --profile Win7SP1x86 pslist --o
utput=xlsx --output-file=CleanPslist.xlsx
Volatility Foundation Volatility Framework 2.6
Outputting to: CleanPslist.xlsx
```

Gambar 5.63 Hasil pslist

Untuk menggunakan pstree masukkan perintah berikut dengan hasil seperti **Gambar 5.64**.

volatility2.6.exe -f CleanRAM.mem --profile=Win7SP1x86 pstree --output=xlsx --output-file=CleanPstree.xlsx

```
D:\Barang Bukti 2>volatility2.6.exe -f CleanRAM.mem --profile Win7SP1x86 pstree --o
utput=xlsx --output-file=CleanPstree.xlsx
Volatility Foundation Volatility Framework 2.6
Outputting to: CleanPstree.xlsx
```

Gambar 5.64 Hasil pstree

Untuk menggunakan psscan masukkan perintah berikut dengan hasil seperti **Gambar 5.65**.

volatility2.6.exe -f CleanRAM.mem --profile=Win7SP1x86 psscan --output=xlsx --output-file=CleanPsscan.xlsx

```
D:\Barang Bukti 2>volatility2.6.exe -f CleanRAM.mem --profile Win7SP1x86 psscan --o
utput=xlsx --output-file=CleanPsscan.xlsx
Volatility Foundation Volatility Framework 2.6
Outputting to: CleanPsscan.xlsx
```

Gambar 5.65 Hasil psscan

4. Program yang berjalan dapat di ekstrak menggunakan perintah berikut dengan hasil seperti **Gambar 5.66**.

   volatility2.6.exe -f CleanRAM.mem --profile=Win7SP1x86 procdump -D CleanProc/ --output=xlsx --output-file=CleanProcDump.xlsx

```
D:\Barang Bukti 2>volatility2.6.exe -f CleanRAM.mem --profile Win7SP1x86 procdump -
D CleanProc/ --output=xlsx --output-file=CleanProcDump.xlsx
Volatility Foundation Volatility Framework 2.6
Outputting to: CleanProcDump.xlsx
```

Gambar 5.66 Hasil procdump

5. Selain program, Volatility juga dapat mengenali DLL yang ada dengan memasukkan perintah berikut dengan hasil seperti **Gambar 5.67**.

   volatility2.6.exe -f CleanRAM.mem --profile=Win7SP1x86 dlllist --output=xlsx --output-file=CleanDllList.xlsx

```
D:\Barang Bukti 2>volatility2.6.exe -f CleanRAM.mem --profile Win7SP1x86 dlllist --
output=xlsx --output-file=CleanDllList.xlsx
Volatility Foundation Volatility Framework 2.6
Outputting to: CleanDllList.xlsx
```

Gambar 5.67 Hasil dlllist

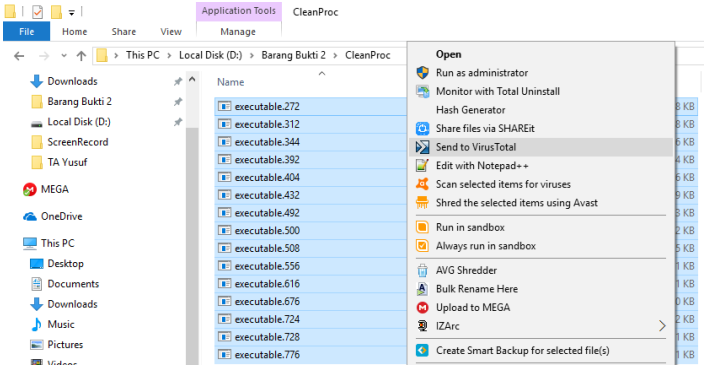
6. Untuk mengekstrak DLL yang ada masukkan perintah berikut dengan hasil seperti **Gambar 5.68**.

   volatility2.6.exe -f CleanRAM.mem --profile=Win7SP1x86 dlldump -D CleanDll/ --output=xlsx --output-file=CleanDllDump.xlsx

```
D:\Barang Bukti 2>volatility2.6.exe -f CleanRAM.mem --profile Win7SP1x86 dlldump -D
 CleanDLL/ --output=xlsx --output-file=CleanDllDump.xlsx
Volatility Foundation Volatility Framework 2.6
Outputting to: CleanDllDump.xlsx
```

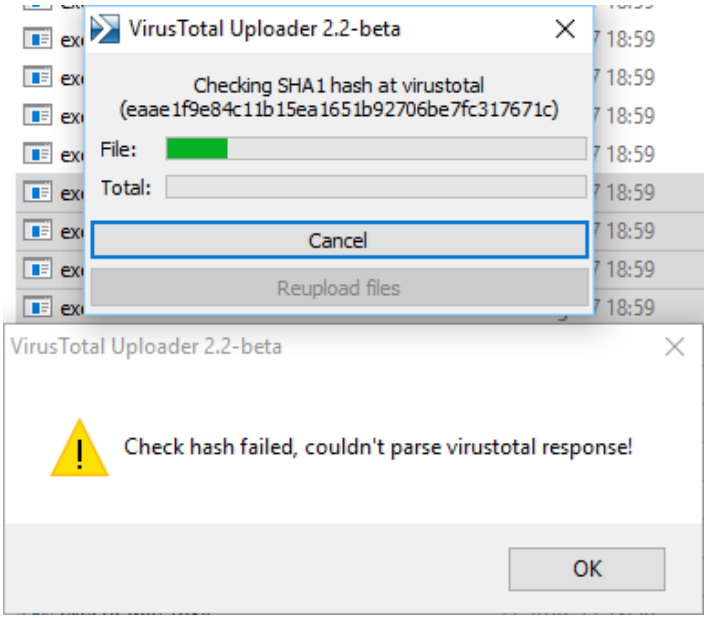
Gambar 5.68 Hasil dlldump

Program yang telah di ekstrak sebelumnya akan dikirim ke VirusTotal untuk diuji apakah mengandung virus atau malware. Pada dasarnya VirusTotal hanya menerima 1 file namun dengan menggunakan VirusTotal Uploader dapat mengirim file sampai dengan 15 file. Untuk mengupload file secara bersamaan klik kanan pada file yang akan diupload dan klik Send to VirusTotal seperti pada **Gambar 5.69**.



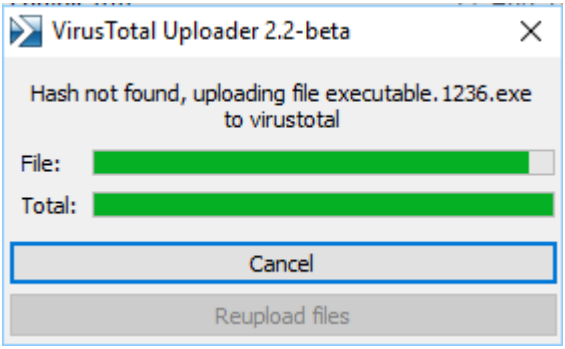
Gambar 5.69 Pilihan upload VirusTotal

VirusTotal Uploader akan mengecek hash dari file yang diupload. Apabila hash tersebut tidak ada dalam database VirusTotal, VirusTotal akan memunculkan popup seperti pada **Gambar 5.70**.



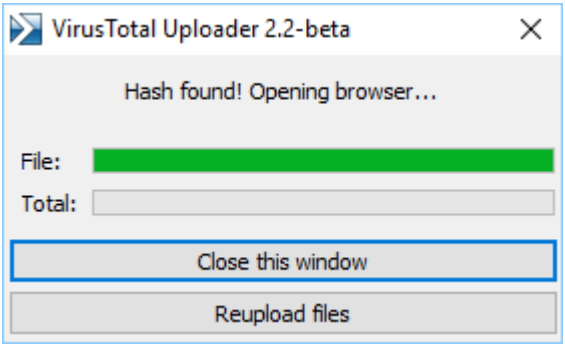
Gambar 5.70 Pengecekan hash pada VirusTotal

Klik OK dan VirusTotal Uploader akan mengupload file untuk diperiksa seperti pada **Gambar 5.71**.



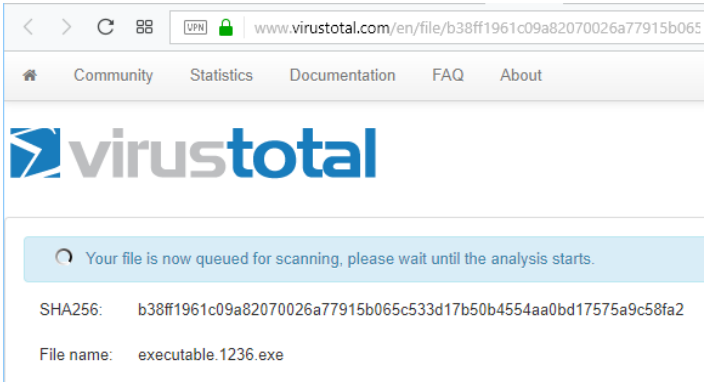
Gambar 5.71 Upload file karena hash tidak ditemukan

Apabila hash ditemukan VirusTotal Uploader akan langsung membuka browser dengan link yang sesuai dengan hash file tersebut seperti pada **Gambar 5.72**.



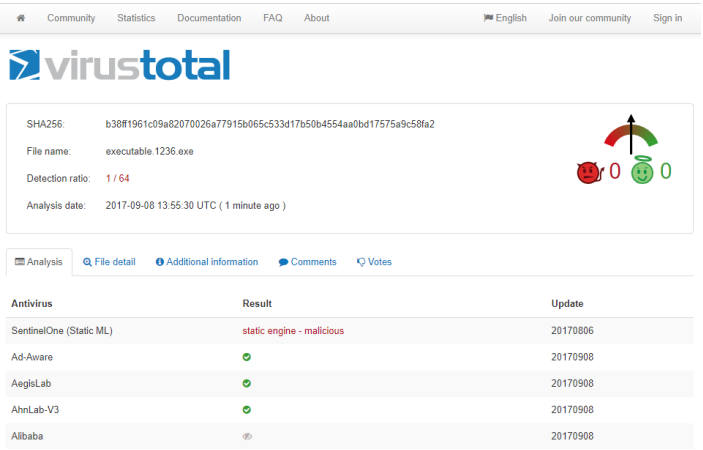
Gambar 5.72 Membuka browser karena hash telah ditemukan

Untuk file yang hashnya belum ada dalam database VirusTotal, VirusTotal akan melakukan scanning secara menyeluruh pada file tersebut seperti pada **Gambar 5.73**.



Gambar 5.73 Scan awal VirusTotal

Setelah selesai, VirusTotal akan menampilkan hasil analisa dari setiap AntiVirus yang terintegrasi dalam VirusTotal sebagimana ditampilkan pada **Gambar 5.74**.



Gambar 5.74 Hasil scan VirusTotal

5.4 Membuat dan Menguji IOC

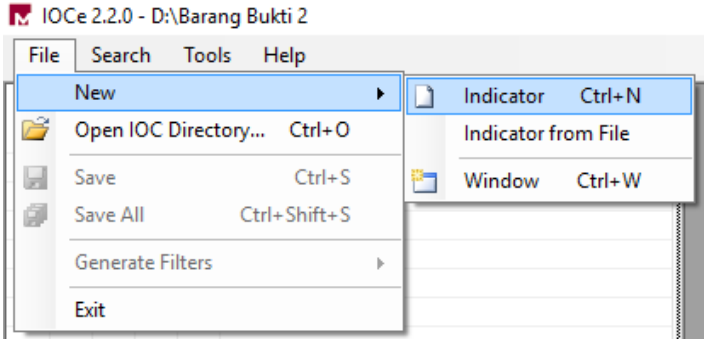
Untuk dapat berkerja dengan IoC dibutuhkan dua aplikasi yatu Mandiant IoC Editor dan Mandiant IoC Finder.

5.4.1 Membuat IoC dengan IoC Editor

Untuk membuat IoC buka aplikasi IOCe dan akan tampil IoC Editor sesuai dengan **Gambar 5.75**.

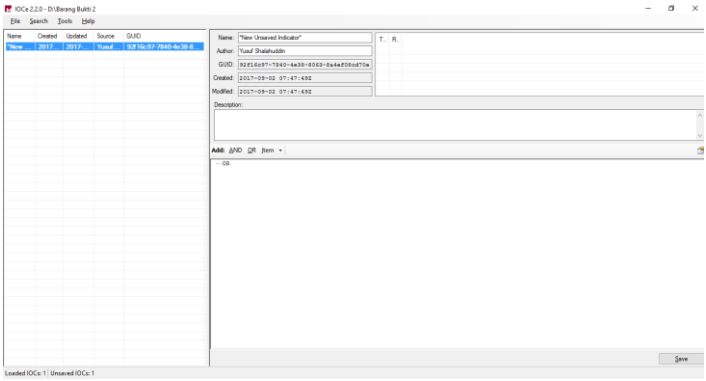
Gambar 5.75 Tampilan awal IoC Editor

Klik pada bagian File pilih New pilih Indicator seperti pada **Gambar 5.76**.



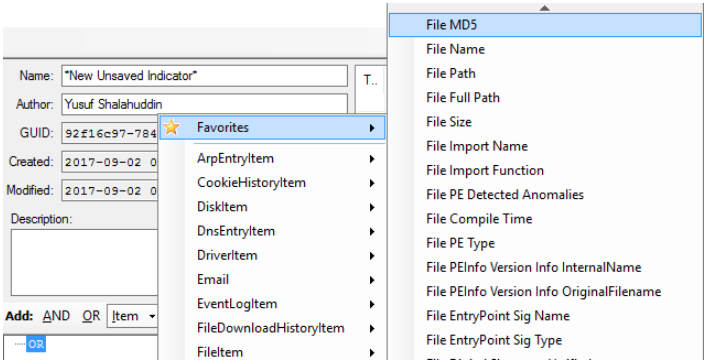
Gambar 5.76 Pilihan membuat indikator baru

IOC baru akan dibuat lengkap dengan TimeStamp dan GUID yang membedakan satu IoC dengan IoC yang lain seperti pada **Gambar 5.77**.



Gambar 5.77 Indikator siap untuk diisi

Untuk mengisi IoC dapat menggunakan AND, OR atau langsung pada Item dan pilih indikator yang sesuai seperti pada **Gambar 5.78**.



Gambar 5.78 Pilihan isi dari indikator

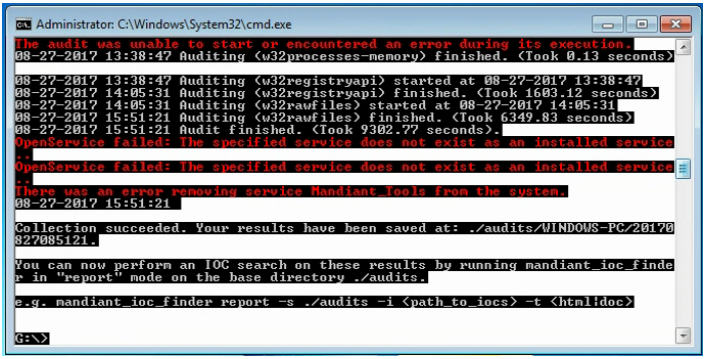
5.4.2 Menguji IoC dengan IoC Finder

IOC Finder berkerja dengan cara mengumpulkan hasil audit sistem dan membandingkannya dengan IoC yang telah dibuat. Audit ini dapat berlangsung selama 3 sampai 4 jam. Untuk melakukan audit system masukkan perintah seperti pada **Gambar 5.79**.

```
G:\>mandiant_ioc_finder.exe collect
08-27-2017 13:16:15 Setting up dependencies...
08-27-2017 13:16:15 Starting collection...
```

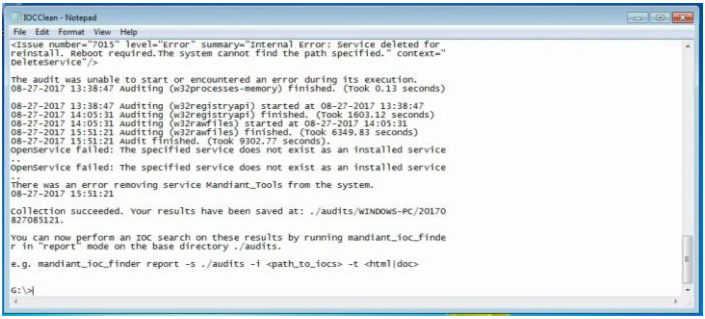
Gambar 5.79 Perintah audit dengan IoC Finder

Gambar 5.80 adalah tampilan IoC Finder saat selesai melakukan audit sistem. Hasil audit disimpan pada direktori ./audits yang nantinya dapat digunakan kembali untuk menguji IOC.



Gambar 5.80 Hasil perintah IoC Finder collect

Hasil perintah IoC Finder pada cmd dapat disimpan pada Notepad untuk lebih mudah melihat audit yang gagal seperti pada **Gambar 5.81**.



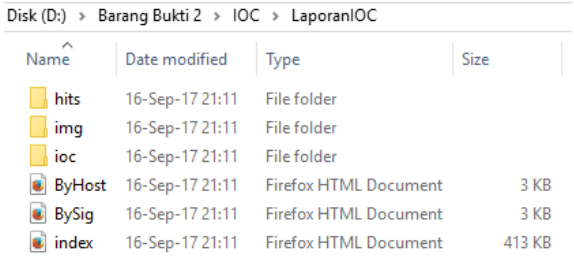
Gambar 5.81 Hasil dari CMD dipindah ke Notepad

Untuk menguji IoC yang telah dibuat masukkan perintah seperti pada **Gambar 5.82**.

```
D:\Barang Bukti 2\IOC>mandiant_ioc_finder.exe report -i 6630471
9-5aa4-4040-a740-efafd8c64549.ioc -t html -o LaporanIOC
09-16-2017 21:06:55 1 iocs were loaded.
09-16-2017 21:06:55 No source folder provided, using './Audits'
.
09-16-2017 21:06:55 Beginning search of audit bundle at path=./
Audits\WINDOWS-PC\20170826222839 (1 of 1).  Total size=492.55 M
B.
09-16-2017 21:07:10 Searched 5% of audit bundle #1...
09-16-2017 21:07:27 Searched 10% of audit bundle #1...
09-16-2017 21:07:49 Searched 15% of audit bundle #1...
09-16-2017 21:08:07 Searched 20% of audit bundle #1...
09-16-2017 21:08:20 Searched 25% of audit bundle #1...
09-16-2017 21:08:34 Searched 30% of audit bundle #1...
09-16-2017 21:08:50 Searched 35% of audit bundle #1...
09-16-2017 21:09:06 Searched 40% of audit bundle #1...
09-16-2017 21:09:23 Searched 45% of audit bundle #1...
09-16-2017 21:09:33 Searched 50% of audit bundle #1...
09-16-2017 21:09:43 Searched 55% of audit bundle #1...
09-16-2017 21:09:55 Searched 60% of audit bundle #1...
09-16-2017 21:10:04 Searched 65% of audit bundle #1...
09-16-2017 21:10:14 Searched 70% of audit bundle #1...
09-16-2017 21:10:25 Searched 75% of audit bundle #1...
09-16-2017 21:10:34 Searched 80% of audit bundle #1...
09-16-2017 21:10:44 Searched 85% of audit bundle #1...
09-16-2017 21:10:55 Searched 90% of audit bundle #1...
09-16-2017 21:11:05 Searched 95% of audit bundle #1...
09-16-2017 21:11:17 Searched 100% of audit bundle #1...
20170826222839,WINDOWS-PC,66304719-5aa4-4040-a740-efafd8c64549.
ioc,6
09-16-2017 21:11:23 Generating HTML report at LaporanIOC...
09-16-2017 21:11:24 Report generation completed.
09-16-2017 21:11:24 Search complete.
```

Gambar 5.82 Hasil IoC Finder report

Gambar 5.83 adalah hasil dari pengujian IoC terhadap Audit.



Gambar 5.83 File yang dihasilkan dari IoC Finder report

Halaman ini sengaja dikosongkan

BAB 6
HASIL DAN PEMBAHASAN

Bab ini menjelaskan tentang hasil dari pengambilan barang bukti beserta analisa yang dilakukan meliputi analisa live, Memory, Hardisk, dan pembuatan IOC.

6.1 Hasil Windows Live Forensics

Setelah dilakukan imaging, FTK Imager menghasilkan 4 file dalam 1 tahap dengan total keseluruhan terdapat 12 file. File tersebut adalah

1. RAM.mem yang merupakan hasil imaging RAM dan disimpan dalam format .mem
2. HDD.001 yang merupakan hasil imaging Physical Harddisk dengan format RAW .001
3. HDD.001.txt yang merupakan laporan hash dan waktu pelaksanaan aplikasi dalam format text .txt
4. HDD.001.csv yang merupakah hasil listing direktori yang terdapat pada Physical Harddisk dalam format excel .csv

Informasi lengkap mengenai barang bukti terdapat dalam lampiran pada bagian akhir penelitian ini.

6.2 Hasil Dynamic Malware Analysis

Hasil dari analisa masing-masing program pada bagian ini akan saling mendukung satu sama lain meskipun terlihat berdiri sendiri.

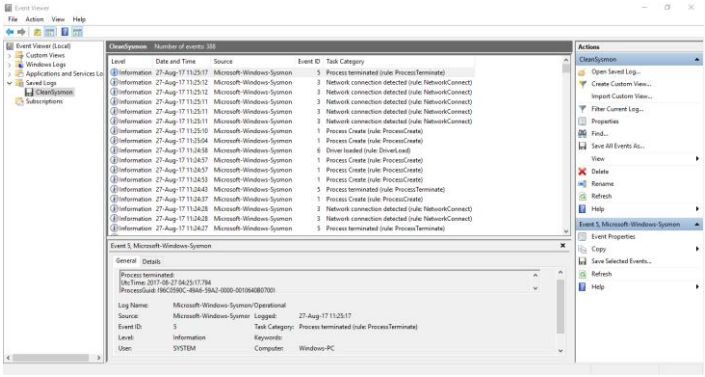
6.2.1 Hasil Analisa Sysmon

Dalam mencatat event, sysmon memiliki 16 klaisifikasi Event ID [34] yaitu :

1. Event ID 1:Process creation
2. Event ID 2: A process changed a file creation time
3. Event ID 3: Network connection
4. Event ID 4: Sysmon service state changed
5. Event ID 5: Process terminated
6. Event ID 6: Driver loaded

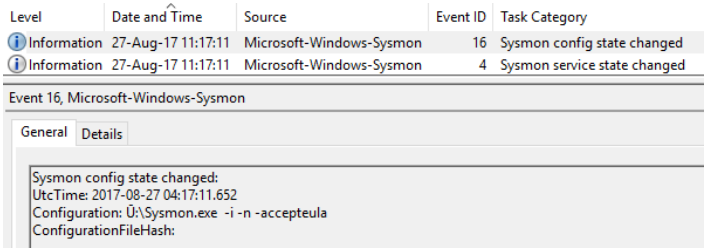
7. Event ID 7: Image loaded
8. Event ID 8: CreateRemoteThread
9. Event ID 9: RawAccessRead
10. Event ID 10: ProcessAccess
11. Event ID 11: FileCreate
12. Event ID 12: RegistryEvent (Object create and delete)
13. Event ID 13: RegistryEvent (Value Set)
14. Event ID 14: RegistryEvent (Key and Value Rename)
15. Event ID 15: FileCreateStreamHash
16. Event ID 255: ErrorA

Sysmon mendapatkan 388 event dari menjalankan aplikasi Re-loader sebagaimana ditampilkan pada **Gambar 6.1**.



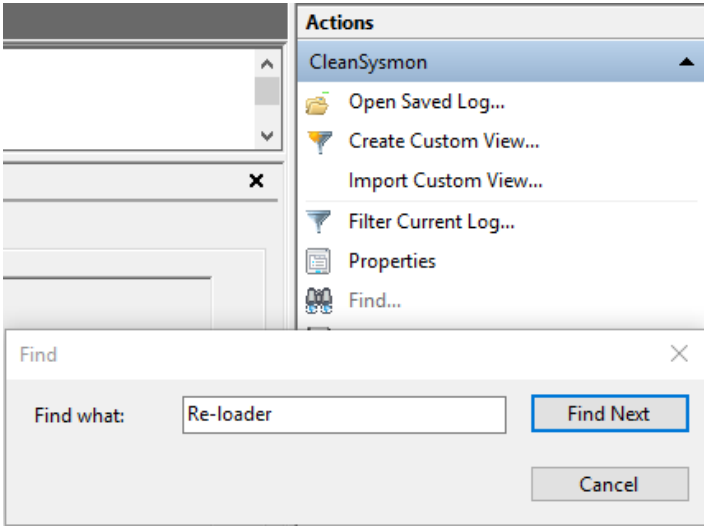
Gambar 6.1 Tampilan awal anlsia log sysmon

Pada log pertama terlihat aktivasi program sysmon seperti pada **Gambar 6.2**.



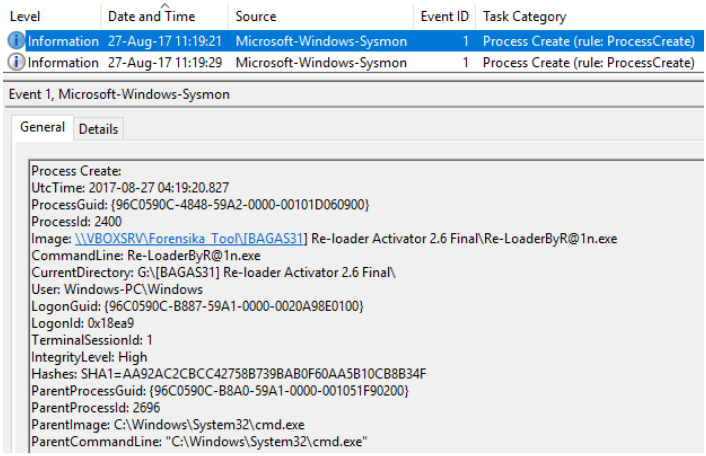
Gambar 6.2 Sysmon terekam dalam log

Untuk mempermudah pencarian gunakan fitur find pada bagian kanan Event Viewer dan masukkan "Re-loader" seperti pada **Gambar 6.3**.



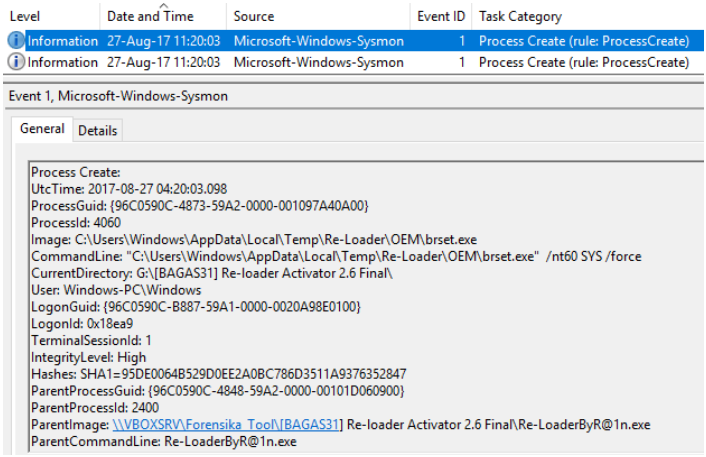
Gambar 6.3 Pencarian Re-loader dalam log

Event Viewer akan menampilkan log yang berisi aplikasi Re-loader seperti pada **Gambar 6.4**.



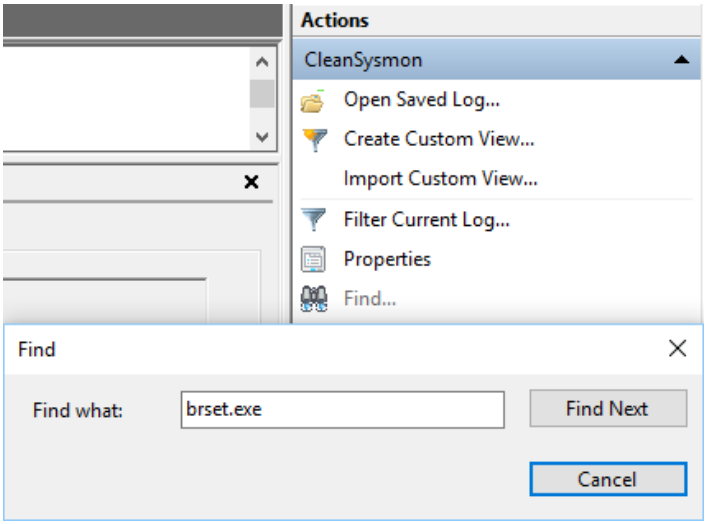
Gambar 6.4 Ditemukan Re-loader yang dijalankan dari CMD

Pada **Gambar 6.4** diatas terlihat aplikasi Re-loader mendapatkan ParentImage berupa cmd.exe. Hal ini disebabkan karena program Re-loader dijalankan melalui cmd untuk meminimalkan jejak. Selanjutnya dilakukan pencarian kembali dan didapatkan proses pada **Gambar 6.5**.



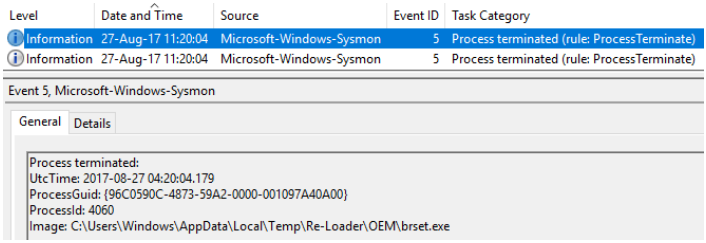
Gambar 6.5 Re-loader menjalankan brset.exe

Pada **Gambar 6.5** terlihat aplikasi Re-loader menjalankan program brset.exe yang dijalankan dari direktori C:\Users\Windows\AppData\Local\Temp\Re-loader\OEM\brset.exe. Hal ini membuktikan bahwa Re-loader telah menempatkan duplikat pada folder temporer tersebut. Ketik brset.exe pada fungsi Find untuk memfokuskan pencarian seperti pada **Gambar 6.6**.



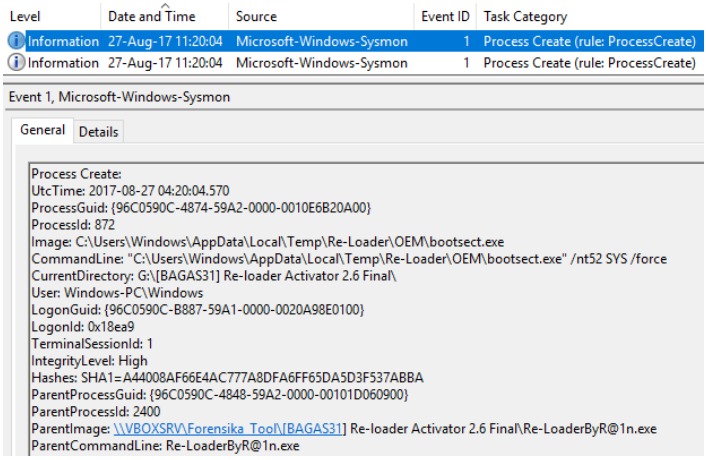
Gambar 6.6 Mencari brset.exe pada log

Log berikutnya menunjukkan proses brset.exe dimatikan seperti pada **Gambar 6.7**.



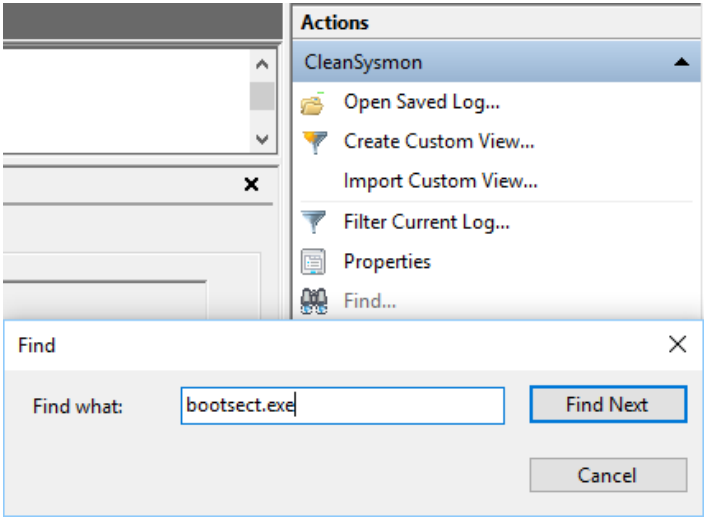
Gambar 6.7 Proses brset.exe ditutup

Pencarian Re-loader berikutnya menampilkan log aplikasi Re-loader menjalankan bootsec.exe dari direktori yang sama dengan brset.exe seperti pada **Gambar 6.8**.



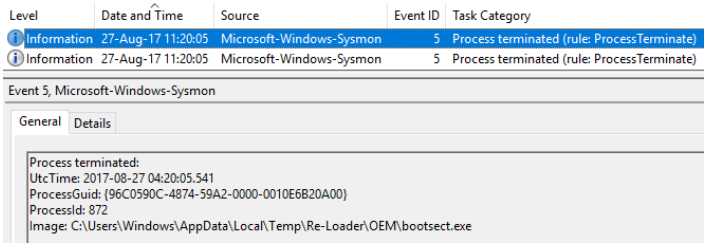
Gambar 6.8 Re-loader menjalankan bootsect.exe

Untuk memusatkan pencarian, masukkan bootsect.exe pada fitur find seperti pada **Gambar 6.9**.



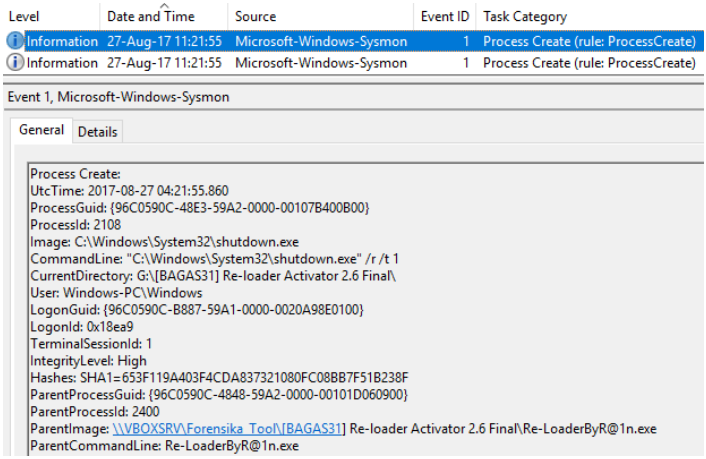
Gambar 6.9 Mencari bootsect.exe pada log

Log yang muncul menunnjukkan aplikasi bootsect.exe dimatikan seperti pada **Gambar 6.10**.



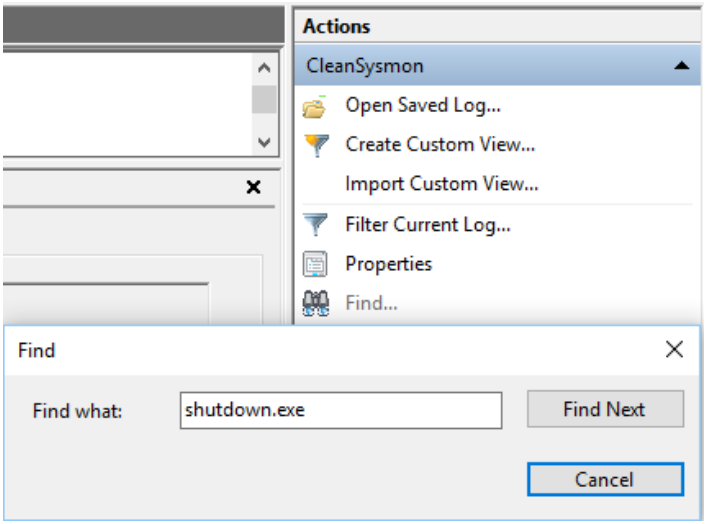
Gambar 6.10 Proses bootsect.exe ditutup

Pencarian Re-loader berikutnya menampilkan aplikasi shutdown.exe yang dijalankan dari direktori C:Windows\System32\shutdown.exe seperti pada **Gambar 6.11**.



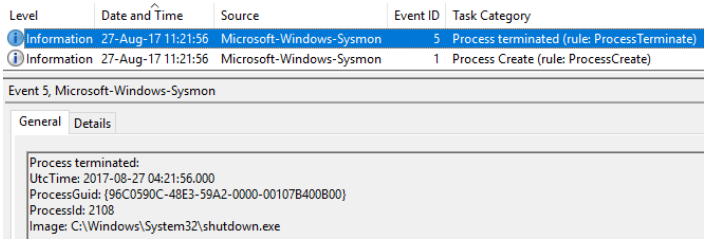
Gambar 6.11 Re-loader menjalankan shutdown.exe

Untuk memusatkan pencarian masukkan shutdown.exe pada fungsi find seperti pada **Gambar 6.12**.



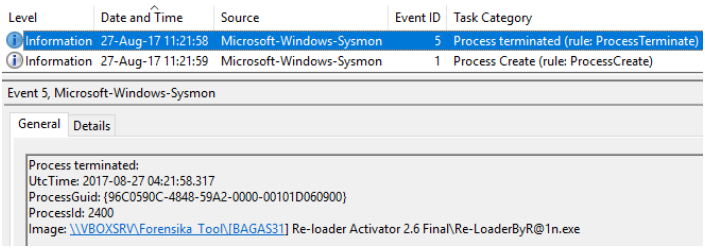
Gambar 6.12 Mencari shutdown.exe pada log

Log menunjukkan shutdown.exe dimatikan seperti pada **Gambar 6.13**.



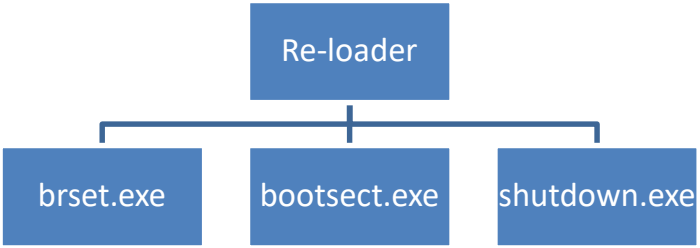
Gambar 6.13 Proses shutdown.exe ditutup

Karena komputer dimatikan log mencatat aplikasi Re-loader dan aplikasi lainnya yang berajalan ikut dimatikan seperti pada **Gambar 6.14**.



Gambar 6.14 Proses Re-loader ditutup

Dengan dimatikannya aplikasi Re-loader sebelum komputer dimatikan, sysmon tidak lagi mencatat aplikasi yang berhubungan dengan Re-loader dijalankan bahkan setelah komputer menyala kembali. Dengan demikian dapat disimpulkan bahwa aplikasi Re-loader menjalankan 2 aplikasi anak yaitu brset.exe dan bootsect.exe dan juga 1 aplikasi bawaan windows yaitu shutdown.exe sebagaimana pada **Gambar 6.15**.



Gambar 6.15 Gambaran umum aplikasi yang dijalankan oleh Re-loader

6.2.2 Hasil Analisa Regshot

Gambar 6.16, **Gambar 6.17**, dan **Gambar 6.18** adalah perbandingan Regshot dari semua tahapan yang ada.

```
Regshot 1.9.0 x86 Unicode
Comments: Compare Clean Infected 1
Datetime: 2017/8/27 04:31:32  ,  2017/8/27 01:11:37
Computer: WINDOWS-PC , WINDOWS-PC
Username: Windows , Windows

----------------------------------
Keys deleted: 115
----------------------------------
Keys added: 1
----------------------------------
Values deleted: 635
----------------------------------
Values added: 16
----------------------------------
Values modified: 99
----------------------------------
Files added: 7
----------------------------------
Files deleted: 20
----------------------------------
Files [attributes?] modified: 88
----------------------------------
Folders added: 1
----------------------------------
Folders deleted: 16
----------------------------------
Total changes: 998
----------------------------------
```

Gambar 6.16 Hasil perbandingan Regshot Clean dengan Infected 1

```
Regshot 1.9.0 x86 Unicode
Comments: Compare Infected 1 Infected 2
Datetime: 2017/8/27 01:11:37  ,  2017/8/26 19:29:32
Computer: WINDOWS-PC , WINDOWS-PC
Username: Windows , Windows

----------------------------------
Keys deleted: 18
----------------------------------
Keys added: 49750
----------------------------------
Values deleted: 92
----------------------------------
Values added: 118740
----------------------------------
Values modified: 200
----------------------------------
Files added: 9
----------------------------------
Files deleted: 33
----------------------------------
Files [attributes?] modified: 155
----------------------------------
Folders added: 1
----------------------------------
Folders deleted: 5
----------------------------------
Total changes: 169003
----------------------------------
```

Gambar 6.17 Hasil perbandingan Regshot Infected 1 dan Infected 2

```
Regshot 1.9.0 x86 Unicode
Comments: Compare Clean Infected 2
Datetime: 2017/8/27 04:31:32  ,  2017/8/26 19:29:32
Computer: WINDOWS-PC , WINDOWS-PC
Username: Windows , Windows

----------------------------------
Keys deleted: 97
----------------------------------
Keys added: 49715
----------------------------------
Values deleted: 282
----------------------------------
Values added: 118311
----------------------------------
Values modified: 244
----------------------------------
Files added: 10
----------------------------------
Files deleted: 47
----------------------------------
Files [attributes?] modified: 171
----------------------------------
Folders added: 1
----------------------------------
Folders deleted: 20
----------------------------------
Total changes: 168898
----------------------------------
```

Gambar 6.18 Hasil perbandingan Regshot Clean dan Infected 2

Gambar 6.19 dan **Gambar 6.20** adalah rangkuman dari perbandingan sebelumnya.

Regshot 1.9.0 x86 Unicode	Regshot 1.9.0 x86 Unicode
Comments: Compare Clean Infected 1	Comments: Compare Infected 1 Infected 2
Datetime: 2017/8/27 04:31:32 , 2017/8/27 01:11:37	Datetime: 2017/8/27 01:11:37 , 2017/8/26 19:29:32
Computer: WINDOWS-PC , WINDOWS-PC	Computer: WINDOWS-PC , WINDOWS-PC
Username: Windows , Windows	Username: Windows , Windows
Keys deleted: 115	Keys deleted: 18
Keys added: 1	Keys added: 49750
Values deleted: 635	Values deleted: 92
Values added: 16	Values added: 118740
Values modified: 99	Values modified: 200
Files added: 7	Files added: 9
Files deleted: 20	Files deleted: 33
Files [attributes?] modified: 88	Files [attributes?] modified: 155
Folders added: 1	Folders added: 1
Folders deleted: 16	Folders deleted: 5
Total changes: 998	Total changes: 169003

Gambar 6.19 Hasil perbandingan 1 dan 2

Regshot 1.9.0 x86 Unicode	Regshot 1.9.0 x86 Unicode
Comments: Compare Clean Infected 1	Comments: Compare Clean Infected 2
Datetime: 2017/8/27 04:31:32 , 2017/8/27 01:11:37	Datetime: 2017/8/27 04:31:32 , 2017/8/26 19:29:32
Computer: WINDOWS-PC , WINDOWS-PC	Computer: WINDOWS-PC , WINDOWS-PC
Username: Windows , Windows	Username: Windows , Windows
Keys deleted: 115	Keys deleted: 97
Keys added: 1	Keys added: 49715
Values deleted: 635	Values deleted: 282
Values added: 16	Values added: 118311
Values modified: 99	Values modified: 244
Files added: 7	Files added: 10
Files deleted: 20	Files deleted: 47
Files [attributes?] modified: 88	Files [attributes?] modified: 171
Folders added: 1	Folders added: 1
Folders deleted: 16	Folders deleted: 20
Total changes: 998	Total changes: 168898

Gambar 6.20 Hasil perbandingan 1 dan 3

Pada perbandingan diatas terlihat bahwa tidak banyak perubahan pada saat implementasi Infected 1, namun setelah implementasi Infected 2 banyak sekali Keys dan Values yang ditambahkan. Penambahan ini terjadi saat komputer mengalami restart dimana saat selesai implementasi Infected 1, komputer harus melakukan restart untuk bisa lanjut ke Infected 2. Keys dan Values merupakan bagian dari Registry yang akan terus berubah setelah restart. Menurut jurnal dengan judul “A Forensic Analysis Of The Windows Registry” [35] Registry bertindak sebagai catatan perubahan mulai dari autorun, aplikasi yang sering digunakan, koneksi internet, perangkat yang terhubung, serta riwayat Internet Explorer. Sebagian besar analisa Registry berfokus pada aktivitas hacking dan pencurian data. Dalam penelitian ini sebagian besar Registry yang ditambahkan adalah Registry terkait mekanisme aktivasi Windows. Mekanisme ini akan memastikan pengaturan Windows biasa sesuai dengan Windows teraktivasi. Analisa Registry pada penelitian ini hanya melihat Registry terkait Autorun dibahas pada bagian analisa Autoruns.

Registry yang tercantum pada hasil dapat dikelompokkan menjadi :

1. HKLM\COMPONENTS
    a. 118.280 Value ditambahkan
    b. 49.704 Key ditambahkan
2. HKLM\SOFTWARE
    a. 29 Value ditambahkan
    b. 86 Value dirubah
    c. 10 Key ditambahkan
3. HKLM\SYSTEM
    a. 427 Value ditambahkan
    b. 278 Value dirubah
    c. 31 Key ditambahkan
4. HKLM\HARDWARE
    a. 6 Value dirubah
    b. 3 Key ditambahkan

Berdasarkan data diatas terlihat seluruh registry yang terkait dengan aplikasi Re-loader berada pada HKEY_LOCAL_MACHINE (HKLM). HKLM tidak menyimpan key dan value pada media penyimpanan sehingga akan hilang setelah komputer mengalami restart. Hal ini akan menyulitkan implementasi barang bukti pada komputer yang sudah sering mengalami restart sehingga hasil analisa registry dapat diabaikan.

Selain registry, perubahan pada file juga dianalisa. Setelah didapatkan perubahan yang terjadi, semua file yang ditambahkan kedalam system dikumpulkan dan dianalisa. Kemudian dilakukan pengecekan pada barang bukti dan didapatkan hasil keberadaan barang bukti yang dijabarkan dalam **Tabel 6.1** dan **Tabel 6.2** sebagai berikut :

Tabel 6.1 Pengujian keberadaan file dengan daftar file dtambahkan

File ditambahkan	Ket	Status
C:\ProgramData\Microsoft\RAC\ Temp\sql2D39.tmp	Tidak ada	
C:\ProgramData\Microsoft\RAC\ Temp\sql2FA7.tmp	Tidak ada	
C:\ProgramData\Microsoft\RAC\ Temp\sql3594.tmp	Tidak ada	
C:\ProgramData\Microsoft\RAC\ Temp\sql3DB8.tmp	Tidak ada	
C:\Users\All Users\Microsoft\RAC\ Temp\sql2D39.tmp	Tidak ada	
C:\Users\All Users\Microsoft\RAC\ Temp\sql2FA7.tmp	Tidak ada	
C:\Users\All Users\Microsoft\RAC\ Temp\sql3594.tmp	Tidak ada	
C:\Users\All Users\Microsoft\RAC\ Temp\sql3DB8.tmp	Tidak ada	
C:\Windows\assembly\ NativeImages_v4.0.30319_32\ index5.dat	Tidak ada	
C:\Windows\ServiceProfiles\ NetworkService\AppData\Local\ Microsoft\Windows Media Player NSS\ 3.0\Icon Files\e0191160-02e3-4826-90d3-133d3e32d2cb.png	Tidak ada	
C:\Windows\SoftwareDistribution\ PostRebootEventCache\ {8AF5A929-7CC6-44C8-8A9A-CEA4E9763361}.bin	Ada	Dihapus

File ditambahkan	Ket	Status
C:\Windows\System32\config\ COMPONENTS{fc378261-8a81-11e7-a1e5-0800270bb186}.TxR.0.regtrans-ms	Ada	Dihapus
C:\Windows\System32\config\ COMPONENTS{fc378261-8a81-11e7-a1e5-0800270bb186}.TxR.1.regtrans-ms	Ada	Dihapus
C:\Windows\System32\config\ COMPONENTS{fc378261-8a81-11e7-a1e5-0800270bb186}.TxR.2.regtrans-ms	Ada	Dihapus
C:\Windows\System32\config\ COMPONENTS{fc378261-8a81-11e7-a1e5-0800270bb186}.TxR.blf	Ada	Dihapus
C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\ {644550d4-87fb-4d37-81a1-e7b7da9d9153}\snapshot.etl	Tidak ada	

Tabel 6.2 Pengujian keberaaan file dengan daftar file dihapus

File dihapus	Ket	Status
C:\ProgramData\Microsoft\Crypto\ RSA\MachineKeys\dfea9a60a88a18 de05161d5ff20e6381_96c0590c-f01d-4c4d-ad14-0f455af7ec07	Ada	Ada
C:\ProgramData\Microsoft\RAC\ Temp\sql2D39.tmp	Tidak ada	
C:\ProgramData\Microsoft\RAC\ Temp\sql2FA7.tmp	Tidak ada	
C:\ProgramData\Microsoft\RAC\ Temp\sqlB4D6.tmp	Tidak ada	

File dihapus	Ket	Status
C:\ProgramData\Microsoft\RAC\ Temp\sqlB71C.tmp	Tidak ada	
C:\ProgramData\Microsoft\Search\ Data\Applications\Windows\Projects\ SystemIndex\Indexer\CiFiles\00010004.ci	Ada	Dihapus
C:\ProgramData\Microsoft\Search\ Data\Applications\Windows\Projects\ SystemIndex\Indexer\CiFiles\00010004.dir	Ada	Dihapus
C:\ProgramData\Microsoft\Search\ Data\Applications\Windows\Projects\ SystemIndex\Indexer\CiFiles\00010004.wid	Ada	Dihapus
C:\ProgramData\Microsoft\Search\ Data\Applications\Windows\Projects\ SystemIndex\Indexer\CiFiles\00010005.ci	Ada	Dihapus
C:\ProgramData\Microsoft\Search\ Data\Applications\Windows\Projects\ SystemIndex\Indexer\CiFiles\00010005.wid	Ada	Dihapus
C:\ProgramData\Microsoft\Search\ Data\Applications\Windows\Projects\ SystemIndex\Indexer\CiFiles\00010005.wsb	Ada	Dihapus
C:\ProgramData\Microsoft\Search\ Data\Applications\Windows\Projects\ SystemIndex\Indexer\CiFiles\CiMG0005.000	Ada	Dihapus
C:\ProgramData\Microsoft\Search\ Data\Applications\Windows\Projects\ SystemIndex\Indexer\CiFiles\CiMG0005.001	Ada	Dihapus
C:\ProgramData\Microsoft\Search\ Data\Applications\Windows\Projects\ SystemIndex\Indexer\CiFiles\CiMG0005.002	Ada	Dihapus
C:\Users\AllUsers\Microsoft\Crypto\ RSA\MachineKeys\dfea9a60a88a18de0	Tidak ada	

File dihapus	Ket	Status
5161d5ff20e6381_96c0590c-f01d-4c4d-ad14-0f455af7ec07		
C:\Users\All Users\Microsoft\RAC\Temp\sql2D39.tmp	Tidak ada	
C:\Users\All Users\Microsoft\RAC\Temp\sql2FA7.tmp	Tidak ada	
C:\Users\All Users\Microsoft\RAC\Temp\sqlB4D6.tmp	Tidak ada	
C:\Users\All Users\Microsoft\RAC\Temp\sqlB71C.tmp	Tidak ada	
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010004.ci	Tidak ada	
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010004.dir	Tidak ada	
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010004.wid	Tidak ada	
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010005.ci	Tidak ada	
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010005.wid	Tidak ada	
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010005.wsb	Tidak ada	
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\Projects\	Tidak ada	

File dihapus	Ket	Status
SystemIndex\Indexer\CiFiles\CiMG0005.000		
C:\Users\All Users\Microsoft\Search\ Data\Applications\Windows\Projects\ SystemIndex\Indexer\CiFiles\CiMG0005.001	Tidak ada	
C:\Users\All Users\Microsoft\Search\ Data\Applications\Windows\Projects\ SystemIndex\Indexer\CiFiles\CiMG0005.002	Tidak ada	
C:\Users\Public\Desktop\R@1n.txt	Ada	Ada
C:\Users\Windows\AppData\Local\ GDIPFONTCACHEV1.DAT	Ada	Ada
C:\Windows\assembly\ NativeImages_v4.0.30319_32\index5.dat	Tidak ada	
C:\Windows\assembly\ NativeImages_v4.0.30319_32\index6.dat	Tidak ada	
C:\Windows\assembly\ NativeImages_v4.0.30319_32\index7.dat	Tidak ada	
C:\Windows\assembly\ NativeImages_v4.0.30319_32\ Microsoft.CSharp\ 05503f37aef5261d80ccca19f8078679\ Microsoft.CSharp.ni.dll	Ada	Ada
C:\Windows\assembly\ NativeImages_v4.0.30319_32\ mscorlib\246f1a5abb686b9dcd f22d3505b08cea\mscorlib.ni.dll	Ada	Ada
C:\Windows\assembly\ NativeImages_v4.0.30319_32\ System.Configuration\ ac18c2dcd06bd2a0589bac94ccae5716\ System.Configuration.ni.dll	Ada	Ada

File dihapus	Ket	Status
C:\Windows\assembly\ NativeImages_v4.0.30319_32\ System.Core\ 713647b987b140a17e3c4ffe4c721f85\ System.Core.ni.dll	Ada	Ada
C:\Windows\assembly\ NativeImages_v4.0.30319_32\ System.Data.SqlXml\ 1fdd0961d8d07ef4d1fcaf30f0050c0a\ System.Data.SqlXml.ni.dll	Ada	Ada
C:\Windows\assembly\ NativeImages_v4.0.30319_32\System.Xml\ e997d0200c25f7db6bd32313d50b729d\ System.Xml.ni.dll	Ada	Ada
C:\Windows\assembly\ NativeImages_v4.0.30319_32\System\ 964da027ebca3b263a05cadb8eaa20a3\ System.ni.dll	Ada	Ada
C:\Windows\Prefetch\BOOTSECT.EXE-C171AF2B.pf	Ada	Ada
C:\Windows\Prefetch\BRSET.EXE-CFAE891C.pf	Ada	Ada
C:\Windows\Prefetch\DLLHOST.EXE-B2EB1806.pf	Ada	Ada
C:\Windows\Prefetch\ RE-LOADERBYR@1N.EXE -82D80485.pf	Ada	Ada
C:\Windows\Prefetch\ReadyBoot\Trace4.fx	Ada	Ada
C:\Windows\Prefetch\RUNDLL32.EXE-6C3B79A1.pf	Ada	Ada

File dihapus	Ket	Status
C:\Windows\Prefetch\SHUTDOWN.EXE-E7D5C9CC.pf	Ada	Ada
C:\Windows\Prefetch\WLRMDR.EXE-C2B47318.pf	Ada	Ada
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player NSS\3.0\Icon Files\e0191160-02e3-4826-90d3-133d3e32d2cb.png	Tidak ada	
C:\Windows\System32\LogFiles\HTTPERR\httperr1.log	Ada	Ada
C:\Windows\System32\LogFiles\SQM\SQMLogger.etl.007	Tidak ada	
C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\{28615cb3-76c0-43d3-9b4d-759d3e4273c3}\snapshot.etl	Tidak ada	
C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\{9ef18d48-f1c5-42f2-8473-865af1c00a4c}\snapshot.etl	Ada	Ada

Pada table diatas terlihat bahwa aplikasi Re-loader.exe, brset.exe, bootsect.exe, dan shutdown.exe meninggalkan jejak berupa file prefetch yang akan menjadi bahan penyusun IoC pada folder C:\Windows\Prefetch dengan detail sebagai berikut :

- C:\Windows\Prefetch\BOOTSECT.EXE-C171AF2B.pf
- C:\Windows\Prefetch\BRSET.EXE-CFAE891C.pf
- C:\Windows\Prefetch\RE-LOADERBYR@1N.EXE-82D80485.pf

- C:\Windows\Prefetch\SHUTDOWN.EXE-E7D5C9CC.pf

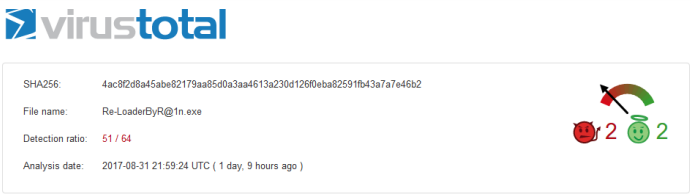
6.2.3 Hasil Analisa Procexp

Lampiran C adalah hasil analisa Procexp dimana tidak ditemukan virus sesuai dengan analisa VirusTotal dan semua program yang berjalan memiliki Verivied Signer yang berarti semua program tersebut adalah asli.

Secara mengejutkan hanya aplikasi Re-loader yang dianggap sebagai Virus dengan jumlah deteksi sebanyak 49 dari 65 antivirus yang terintegrasi dalam VirusTotal sebagaimana ditunjukkan dalam **Gambar 6.21** dan **Gambar 6.22**. Hasil analisa VirusTotal yang lebih lengkap juga dapat dilihat pada **Tabel 6.3**.

Process	CPU	Private Bytes	Working Set	PID
Re-LoaderByR@1n.exe	< 0.01	52,048 K	71,504 K	3432
Description	Company Name	Verified Signer	VirusTotal	
Activator		(No signature was present in the subject)	49/65	

Gambar 6.21 Detail hasil procmon untuk Re-loader



Gambar 6.22 Hasil scan VirusTotal terhadap Re-loader

Tabel 6.3 Daftar virus dan malware yang ditemukan oleh VirusTotal

Antivirus	Result	Update
Ad-Aware	Application.Hacktool.UV	20170831
AegisLab	Troj.Spy.Msil.Keylogger!c	20170831
AhnLab-V3	Unwanted/Win32.AutoKMS.C1638205	20170831
ALYac	Misc.HackTool.WinActivator	20170831

Antivirus	Result	Update
Antiy-AVL	Trojan/Win32.BTSGeneric	20170831
Arcabit	Application.Hacktool.UV	20170831
Avast	FileRepMalware [PUP]	20170831
AVG	FileRepMalware [PUP]	20170831
AVware	Trojan.Win32.Generic!BT	20170831
BitDefender	Application.Hacktool.UV	20170831
CAT-QuickHeal	HackTool.Wpakill	20170831
Comodo	TrojWare.Win32.Spyware.sbdxn	20170831
CrowdStrike Falcon (ML)	malicious_confidence_70% (D)	20170804
Cylance	Unsafe	20170831
Cyren	W32/Trojan.ETRK-6518	20170831
DrWeb	Tool.Wpakill.12	20170831
Emsisoft	Riskware.WinAct (A)	20170831
Endgame	malicious (high confidence)	20170821
ESET-NOD32	a variant of MSIL/HackTool.WinActivator.J potentially unsafe	20170831
F-Secure	Application.Hacktool.UV	20170831
Fortinet	W32/Keylogger.CGBC!tr	20170831
GData	MSIL.Riskware.Hacktool.B	20170831
Ikarus	HackTool.Win32.Wpakill	20170831
Sophos ML	Heuristic	20170822
Jiangmin	Trojan/Jorik.htdp	20170831
K7AntiVirus	Unwanted-Program (004f09ab1)	20170831
K7GW	Unwanted-Program (004f09ab1)	20170831

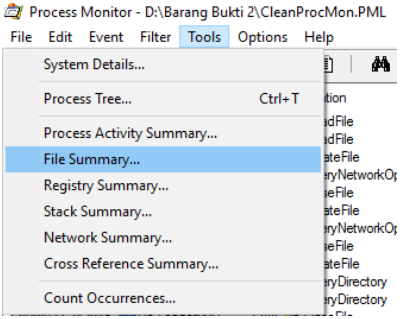
Antivirus	Result	Update
Kaspersky	Trojan-Spy.MSIL.Keylogger.cgbc	20170831
Malwarebytes	PUP.Optional.WpaKill	20170831
McAfee	Artemis!686A5620C3DA	20170831
McAfee-GW-Edition	BehavesLike.Win32.Generic.tc	20170831
Microsoft	Trojan:Win32/Skeeyah.A!rfn	20170831
eScan	Application.Hacktool.UV	20170831
NANO-Antivirus	Trojan.Win32.Keylogger.egihod	20170831
nProtect	Trojan-Dropper/W32.Keylogger.1584122	20170831
Palo Alto Networks (Known Signatures)	generic.ml	20170831
Panda	PUP/Crack	20170831
Rising	Spyware.Keylogger!8.12F (cloud:9BC62Dn4D4J)	20170831
SentinelOne (Static ML)	static engine – malicious	20170806
Sophos AV	Mal/Generic-S	20170831
SUPERAnti Spyware	Trojan.Agent/Gen-Kazy	20170831
Symantec	Hacktool	20170831
Tencent	Msil.Trojan-spy.Keylogger.Wozy	20170831
TrendMicro	TROJ_GEN.R021C0EHI16	20170831
TrendMicro-HouseCall	TROJ_GEN.R021C0EHI16	20170831
VBA32	TrojanSpy.MSIL.Keylogger	20170831

Antivirus	Result	Update
VIPRE	Trojan.Win32.Generic!BT	20170831
Webroot	W32.Hack.Tool	20170831
Yandex	TrojanSpy.Keylogger!dlmQ0fE/Qxk	20170831
Zillya	Tool.WinActivator.Win32.328	20170831
ZoneAlarm by Check Point	Trojan-Spy.MSIL.Keylogger.cgbc	20170831
Alibaba		20170831
Avira (no cloud)		20170831
Baidu		20170831
Bkav		20170831
ClamAV		20170831
CMC		20170828
F-Prot		20170831
Kingsoft		20170831
MAX		20170831
Qihoo-360		20170831
Symantec Mobile Insight		20170831
TheHacker		20170828
Trustlook		20170831
ViRobot		20170831
WhiteArmor		20170829
Zoner		20170831

6.2.4 Hasil Analisa Procmon

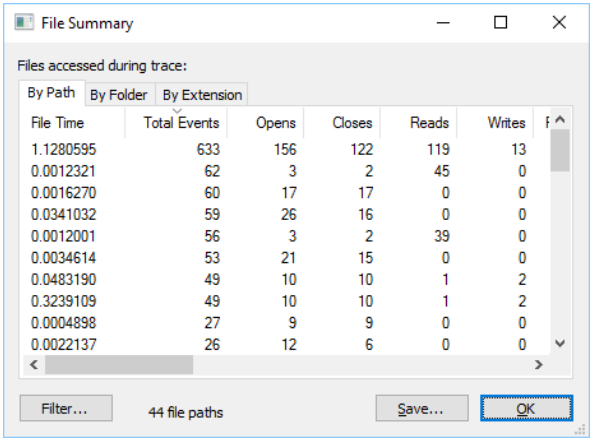
Process Monitor dapat digunakan untuk memberikan Gambaran pergerakan aplikasi pada file dan folder. Untuk

melihat rangkuman file pilih Tools pilih File Summary… seperti pada **Gambar 6.23**.



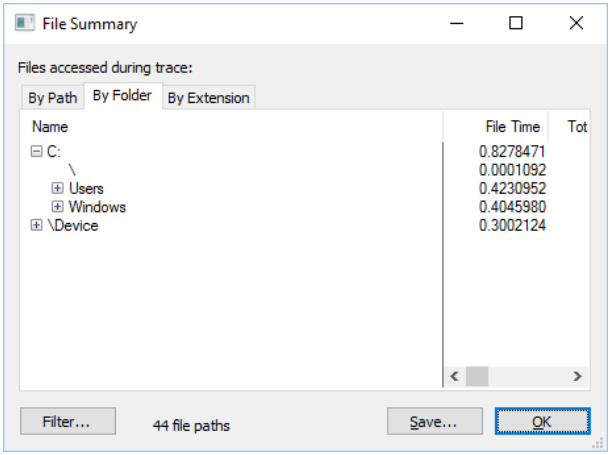
Gambar 6.23 Pilihan File Summary procmon

File Summary dapat dilihat berdasarkan Path, Folder, maupun Extension seperti pada **Gambar 6.24**.



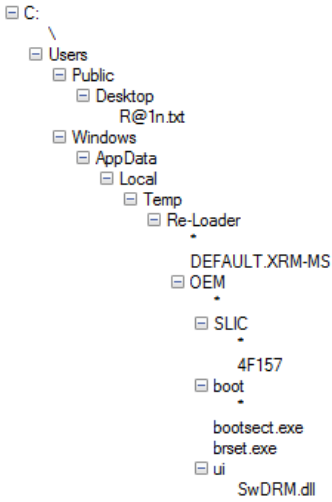
Gambar 6.24 Tampilan awal File Summary

Penelitian ini menggunakan File Summary By Folder seperti pada **Gambar 6.25**.

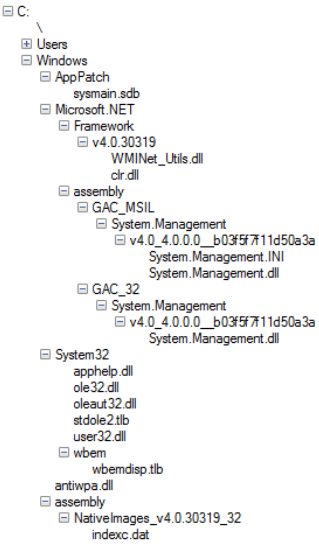


Gambar 6.25 File Summary berdasarkan folder

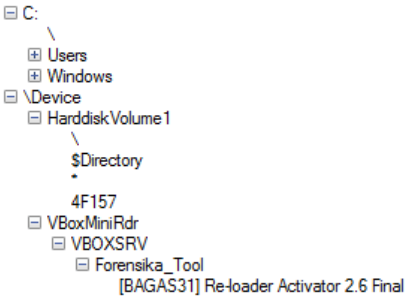
Berikut adalah folder yang diakses oleh aplikasi Re-loader.



Gambar 6.26 Daftar folder yang diakses Re-loader pada C:\users

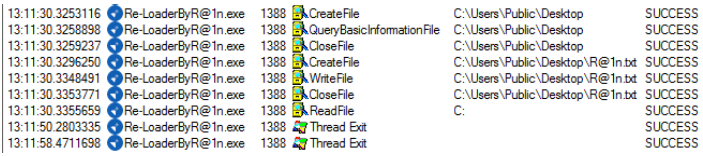


Gambar 6.27 Daftar folder yang diakses Re-loader pada C:\Windows



Gambar 6.28 Daftar folder yang diakses oleh Re-loader pada :\Device

Berdasarkan **Gambar 6.26**, **Gambar 6.27** dan **Gambar 6.28** diatas terlihat bahwa Re-loader hanya menjalankan brset.exe dan bootsect.exe dalam merubah banyak file bawaan dari Windows untuk diaktivasi. Sebelum seluruh implementasi Re-loader berakhir, Re-loader membuat file baru di C:\Users\Public\Desktop dengan nama R@in.txt yang terekam pada **Gambar 6.29**.

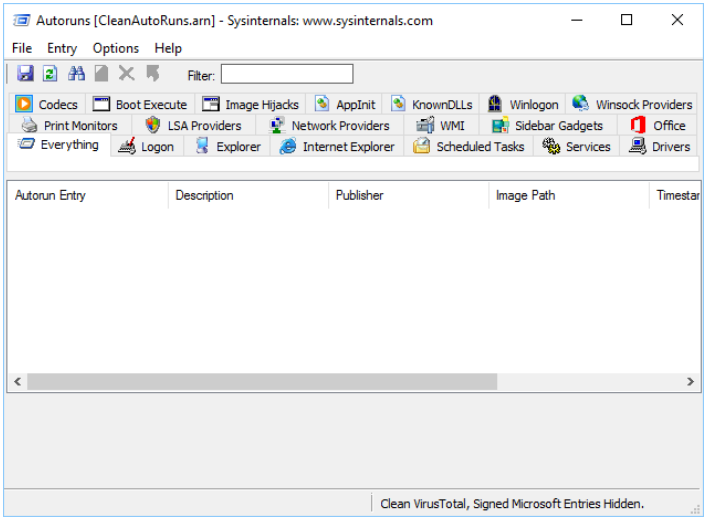


13:11:30.3253116	Re-LoaderByR@1n.exe	1388	CreateFile	C:\Users\Public\Desktop	SUCCESS
13:11:30.3258898	Re-LoaderByR@1n.exe	1388	QueryBasicInfomationFile	C:\Users\Public\Desktop	SUCCESS
13:11:30.3259237	Re-LoaderByR@1n.exe	1388	CloseFile	C:\Users\Public\Desktop	SUCCESS
13:11:30.3296250	Re-LoaderByR@1n.exe	1388	CreateFile	C:\Users\Public\Desktop\R@1n.txt	SUCCESS
13:11:30.3348491	Re-LoaderByR@1n.exe	1388	WriteFile	C:\Users\Public\Desktop\R@1n.txt	SUCCESS
13:11:30.3353771	Re-LoaderByR@1n.exe	1388	CloseFile	C:\Users\Public\Desktop\R@1n.txt	SUCCESS
13:11:30.3355659	Re-LoaderByR@1n.exe	1388	ReadFile	C:	SUCCESS
13:11:50.2803335	Re-LoaderByR@1n.exe	1388	Thread Exit		SUCCESS
13:11:58.4711698	Re-LoaderByR@1n.exe	1388	Thread Exit		SUCCESS

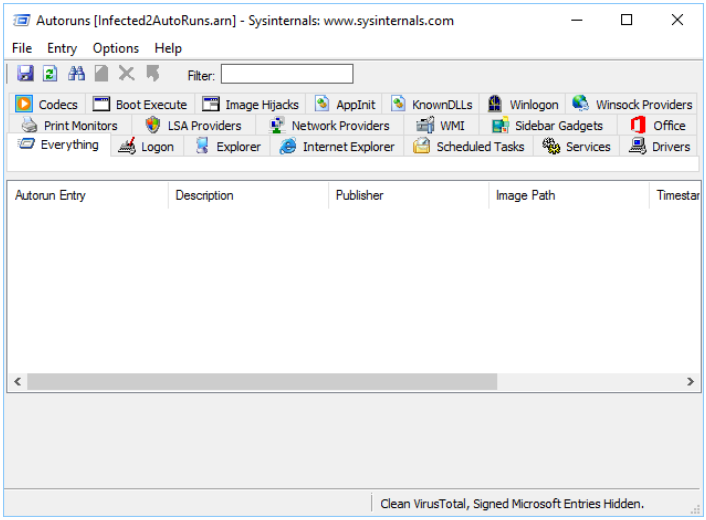
Gambar 6.29 Rekaman penambahan file R@1n.txt pada desktop

6.2.5 Hasil Analisa Autoruns

Autoruns tidak mendeteksi adanya kelainan pada autorun baik pada tahap Clean maupun Infected 2 seperti pada **Gambar 6.30** dan **Gambar 6.31**.



Gambar 6.30 Hasil autoruns pada tahap Clean



Gambar 6.31 Hasil autoruns pada tahap Infected 2

6.2.6 Hasil Analisa Volatility

Hasil scan VirusTotal untuk setiap tahap akan dijabarkan dalam **Tabel 6.4**, **Tabel 6.5** dan **Tabel 6.6**.

Tabel 6.4 Hasil scan program pada tahap Clean

Name	Detection ratio	Antivirus	Result
smss.exe	1/65	Qihoo-360	HEUR/QVM00.1.B583.Malware.Gen
csrss.exe	1/65	SentinelOne (Static ML)	static engine - malicious
wininit.exe	3/64	Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9511
		CrowdStrike Falcon (ML)	malicious_confidence_90% (D)
		SentinelOne (Static ML)	static engine - malicious
csrss.exe	1/65	SentinelOne (Static ML)	static engine - malicious
winlogon.exe	1/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
services.exe	1/65	SentinelOne (Static ML)	static engine - malicious

Name	Detection ratio	Antivirus	Result
lsass.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_60% (D)
		SentinelOne (Static ML)	static engine - malicious
lsm.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
VBoxService.ex	2/65	Ikarus	Virus.Win32.Cryptor
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious

Name	Detection ratio	Antivirus	Result
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
audiodg.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		SentinelOne (Static ML)	static engine - malicious
TrustedInstall	2/65	Cylance	Unsafe
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
spoolsv.exe	3/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne	static engine - malicious

Name	Detection ratio	Antivirus	Result
		(Static ML)	
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
taskhost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
dwm.exe	4/65	Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9807
		CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		Cylance	Unsafe
		SentinelOne (Static ML)	static engine - malicious
explorer.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		SentinelOne (Static ML)	static engine - malicious

Name	Detection ratio	Antivirus	Result
rundll32.exe	1/65	SentinelOne (Static ML)	static engine - malicious
rundll32.exe	1/65	SentinelOne (Static ML)	static engine - malicious
VBoxTray.exe	2/65	Ikarus	Virus.Win32.Cryptor
		SentinelOne (Static ML)	static engine - malicious
SearchIndexer.	3/65	CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
wmpnetwk.exe	3/65	CrowdStrike Falcon (ML)	malicious_confidence_60% (D)
		Cylance	Unsafe

Name	Detection ratio	Antivirus	Result
		SentinelOne (Static ML)	static engine - malicious
WmiPrvSE.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		SentinelOne (Static ML)	static engine - malicious
cmd.exe	1/65	SentinelOne (Static ML)	static engine - malicious
conhost.exe	4/65	Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9971
		CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious
FTK Imager.exe	0/65		
mscorsvw.exe	2/65	CrowdStrike	malicious_confidence_60% (D)

Name	Detection ratio	Antivirus	Result
		Falcon (ML)	
		SentinelOne (Static ML)	static engine - malicious
sppsvc.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
WmiPrvSE.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		SentinelOne (Static ML)	static engine - malicious
SearchProtocol	2/65	CrowdStrike Falcon (ML)	malicious_confidence_90% (D)
		SentinelOne (Static ML)	static engine - malicious

Name	Detection ratio	Antivirus	Result
SearchFilterHo	3/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		Cylance	Unsafe
		SentinelOne (Static ML)	static engine - malicious

Tabel 6.5 Hasil scan program pada tahap Infected 1

Name	Detection ratio	Antivirus	Result
csrss.exe	1/65	SentinelOne (Static ML)	static engine - malicious
csrss.exe	1/65	SentinelOne (Static ML)	static engine - malicious
winlogon.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		SentinelOne (Static ML)	static engine - malicious
services.exe	2/65	CrowdStrike	malicious_confidence_60% (D)

Name	Detection ratio	Antivirus	Result
		Falcon (ML)	
		SentinelOne (Static ML)	static engine - malicious
lsass.exe	3/65	CrowdStrike Falcon (ML)	malicious_confidence_90% (D)
		Qihoo-360	HEUR/QVM20.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious
lsm.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_90% (D)
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
VBoxService.ex	3/65	Ikarus	Virus.Win32.Cryptor
		McAfee-GW-Edition	BehavesLike.Win32.Dropper.tz
		SentinelOne	static engine - malicious

Name	Detection ratio	Antivirus	Result
		(Static ML)	
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
audiodg.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		SentinelOne (Static ML)	static engine - malicious
TrustedInstall	2/65	CrowdStrike Falcon (ML)	malicious_confidence_60% (D)
		SentinelOne (Static ML)	static engine - malicious

Name	Detection ratio	Antivirus	Result
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
spoolsv.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
taskhost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
dwm.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		SentinelOne	static engine - malicious

Name	Detection ratio	Antivirus	Result
		(Static ML)	
explorer.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		SentinelOne (Static ML)	static engine - malicious
rundll32.exe	1/65	SentinelOne (Static ML)	static engine - malicious
rundll32.exe	1/65	SentinelOne (Static ML)	static engine - malicious
VBoxTray.exe	2/65	Ikarus	Virus.Win32.Cryptor
		SentinelOne (Static ML)	static engine - malicious
SearchIndexer.	3/65	CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious

Name	Detection ratio	Antivirus	Result
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
WmiPrvSE.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_90% (D)
		SentinelOne (Static ML)	static engine - malicious
cmd.exe	1/65	SentinelOne (Static ML)	static engine - malicious
conhost.exe	4/65	Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9971
		CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious
ReloaderByR@1	10/65	AhnLab-V3	HackTool/Win32.Activator.C1908685
		Comodo	Heur.Corrupt.PE
		CrowdStrike	malicious_confidence_80% (D)

Name	Detection ratio	Antivirus	Result
		Falcon (ML)	
		Cylance	Unsafe
		Emsisoft	Riskware.WinAct (A)
		GData	MSIL.Riskware.Hacktool.B
		Sophos ML	heuristic
		Jiangmin	Trojan/Jorik.htdp
		Qihoo-360	HEUR/QVM20.1.B583.Malware.Gen
		TheHacker	W32/Behav-Heuristic-CorruptFile-EP
mscorsvw.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_60% (D)
		SentinelOne (Static ML)	static engine - malicious
sppsvc.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne	static engine - malicious

Name	Detection ratio	Antivirus	Result
		(Static ML)	
WmiPrvSE.exe	3/65	CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		NANO-Antivirus	Virus.Win32.Gen.ccmw
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
SearchProtocol	2/65	CrowdStrike Falcon (ML)	malicious_confidence_90% (D)
		SentinelOne (Static ML)	static engine - malicious
FTK Imager.exe	0/65		
SearchFilterHo	3/65	CrowdStrike Falcon (ML)	malicious_confidence_100% (D)

Name	Detection ratio	Antivirus	Result
		Cylance	Unsafe
		SentinelOne (Static ML)	static engine - malicious
mscorsvw.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_60% (D)
		SentinelOne (Static ML)	static engine - malicious

Tabel 6.6 Hasil scan program pada tahap Infected 2

Name	Detection ratio	Antivirus	Result
smss.exe	1/65	Qihoo-360	HEUR/QVM00.1.B583.Malware.Gen
csrss.exe	1/65	SentinelOne (Static ML)	static engine - malicious
wininit.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		SentinelOne (Static ML)	static engine - malicious

Name	Detection ratio	Antivirus	Result
csrss.exe	1/65	SentinelOne (Static ML)	static engine - malicious
winlogon.exe	1/65	SentinelOne (Static ML)	static engine - malicious
services.exe	2/65	Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9919
		SentinelOne (Static ML)	static engine - malicious
lsass.exe	1/65	SentinelOne (Static ML)	static engine - malicious
lsm.exe	2/65	Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
VBoxService.ex	3/65	AegisLab	Troj.Dropper.W32.Agent.mcSg
		Ikarus	Virus.Win32.Cryptor
		SentinelOne	static engine - malicious

Name	Detection ratio	Antivirus	Result
		(Static ML)	
svchost.exe	2/65	Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	2/65	Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
audiodg.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_60% (D)
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious

Name	Detection ratio	Antivirus	Result
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
spoolsv.exe	3/65	CrowdStrike Falcon (ML)	malicious_confidence_70% (D)
		Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
svchost.exe	2/65	Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious
taskhost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
dwm.exe	3/65	Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9649
		CrowdStrike Falcon (ML)	malicious_confidence_80% (D)

Name	Detection ratio	Antivirus	Result
		SentinelOne (Static ML)	static engine - malicious
explorer.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		SentinelOne (Static ML)	static engine - malicious
VBoxTray.exe	2/65	Ikarus	Virus.Win32.Cryptor
		SentinelOne (Static ML)	static engine - malicious
SearchIndexer.	3/65	CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious
wmpnetwk.exe	3/65	CrowdStrike Falcon (ML)	malicious_confidence_60% (D)
		Cylance	Unsafe

Name	Detection ratio	Antivirus	Result
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
WmiPrvSE.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		SentinelOne (Static ML)	static engine - malicious
SearchProtocol	2/65	CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
		SentinelOne (Static ML)	static engine - malicious
cmd.exe	1/65	SentinelOne (Static ML)	static engine - malicious
conhost.exe	4/65	Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9980
		CrowdStrike Falcon (ML)	malicious_confidence_100% (D)

Name	Detection ratio	Antivirus	Result
		Qihoo-360	HEUR/QVM10.1.B583.Malware.Gen
		SentinelOne (Static ML)	static engine - malicious
taskhost.exe	1/65	SentinelOne (Static ML)	static engine - malicious
FTK Imager.exe	0/65		
mscorsvw.exe	1/65	SentinelOne (Static ML)	static engine - malicious
sppsvc.exe	2/65	CrowdStrike Falcon (ML)	malicious_confidence_80% (D)
		SentinelOne (Static ML)	static engine - malicious
svchost.exe	1/65	SentinelOne (Static ML)	static engine - malicious

Setelah mendapatkan data VirusTotal, dilakukan filterisasi program yang benar-benar bermasalah dengan mengabaikan hasil dari SentinelOne dan CrowdStrike. Hal lain yang diabaikan adalah apabila jumlah deteksi maupun hasil pada tahap clean sama dengan tahap infected 2 maka program

tersebut juga ikut diabaikan. Dengan demikian didapatkan hasil yang dijabarkan pada **Tabel 6.7**.

Tabel 6.7 Hasil scan program keseluruhan

Program	Keterangan
Audiodg.exe	Aman
Cmd.exe	Aman
Conhost.exe	Aman
Csrss.exe	Aman
Dwm.exe	Aman
Explorer.exe	Aman
FTK Imager.exe	Aman
Lsass.exe	Aman
Lsm.exe	Malware HEUR/QVM10.1.B583.Malware.Gen terdeteksi oleh Qihoo-360 pada tahap Infected 2
Mscorsvw.exe	Aman
Rundll32.exe	Aman
SearchFilterHo	Aman
SearchProtocol	Aman
Services.exe	Trojan Win32.Trojan.WisdomEyes.16070401.9500.9919 terdeteksi oleh Baidu pada tahap Infected 2
Smss.exe	Aman
Spoolsv.exe	Aman
Sppsvc.exe	Aman
Svchost.exe	Malware HEUR/QVM10.1.B583.Malware.Gen

Program	Keterangan
	terdeteksi oleh Qihoo-360 pada tahap Infected 2
Taskhost.exe	Aman
TrustedInstall	Aman
VBoxService.ex	Trojan Troj.Dropper.W32.Agent.mcSg terdeteksi oleh AegisLab pada tahap Infected 2
VBoxTray.exe	Aman
Wininit.exe	Aman
Winlogon.exe	Aman
WmiPrvSE.exe	Aman
Wmpnetwk.exe	Aman

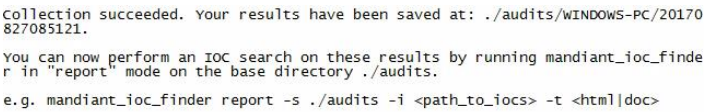
Berdasarkan hasil analisa VirusTotal diatas, Re-loader terlihat tidak terlalu berbahaya karena hanya sebagian kecil yang terindentifikasi sebagai malware. Ancaman sebenarnya dari malware pada Re-loader terletak pada jenis malwarenya. Malware yang terdeteksi adalah Trojan Dropper dan HEUR dimana malware ini berfungsi untuk mendatangkan malware lain serta mengirimkan data-data sensitive seperti password dan email tanpa disadari. Hal ini juga memungkinkan suatu saat pengendali utama Re-loader dapat menyisipkan malware yang lebih berbahaya tanpa disadari pengguna.

6.3 Hasil Indicator IOC

6.3.1 Hasil audit awal

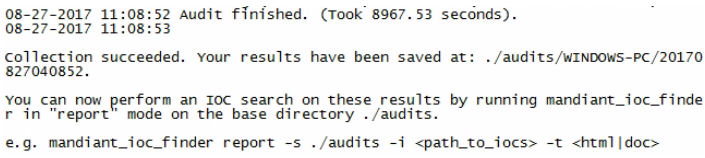
Terdapat beberapa error dalam melakukan audit pada tahap Clean sehingga total waktu tidak bisa ditampilkan. Namun hal ini bukan masalah karena IoC yang diuji nantinya adalah IoC pada tahap Infected 2. Hasil audit tahap Clean disimpan

pada folder ./audits/WINDOWS-PC/20170827085121 sebagaimana tercantum dalam **Gambar 6.32**.



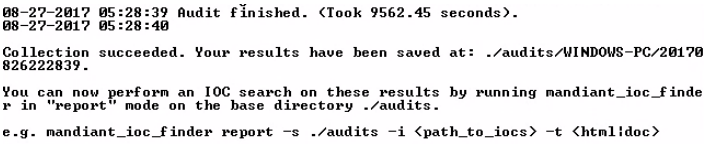
Gambar 6.32 Hasil audit tahap Clean

Audit pada tahap Infected 1 selesai dalam waktu 8.967,57 detik atau sekitar 2 jam 30 menit. Hasil audit tahap Infected 1 disimpan pada folder ./audits/WINDOWS-PC/20170827040852 sebagaimana tercantum dalam **Gambar 6.33**.



Gambar 6.33 Hasil audit tahap Infected 1

Audit pada tahap Infected 2 selesai dalam waktu 9.562,45 detik atau 2 jam 40 menit. Hasil audit tahap Infected 2 disimpan pada folder ./audits/WINDOWS-PC/20170826222839 sebagaimana tercantum dalam **Gambar 6.34**.



Gambar 6.34 Hasil audit tahap Infected 2

6.3.2 Komponen penyusun IOC

Berdasarkan hasil analisa didapatkan barang bukti berupa file sebagai berikut :

1. C:\Users\Public\Desktop\R@1n.txt
2. C:\Windows\Prefetch\RE-LOADERBYR@1N.EXE-82D80485.pf

3. C:\Windows\Prefetch\BRSET.EXE-CFAE891C.pf
4. C:\Windows\Prefetch\BOOTSECT.EXE-C171AF2B.pf
5. C:\Windows\Prefetch\SHUTDOWN.EXE-E7D5C9CC.pf

Dari file diatas didapatkan hash file pada **Tabel 6.8** berikut

Tabel 6.8 Hasil prefetch pada percobaan pertama

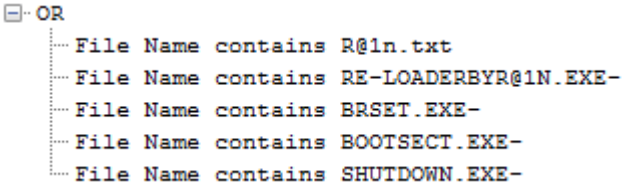
File	R@1n.txt
Path	C:\Users\Public\Desktop\
MD5	14ab52e1ac9a0733ad0b33e79b220a48
SHA1	9b7a9aa627528a24546de7d3584c5d95817efcd1
File	RE-LOADERBYR@1N.EXE-82D80485.pf
Path	C:\Windows\Prefetch\
MD5	fd9200533aa82405e66b2637217ee5f3
SHA1	1e81b802fe75f47f1a8fe8aca0da615f15e9aa3c
File	BRSET.EXE-CFAE891C.pf
Path	C:\Windows\Prefetch\
MD5	ff1f05100eb0a1b9bebbb419ee45fbe5
SHA1	187da21e9c0aa717f73f656f19f503c47dce159e
File	BOOTSECT.EXE-C171AF2B.pf
Path	C:\Windows\Prefetch\
MD5	d94f29faf0fa1aa446c9f4cd134595f7
SHA1	43c9910bf336eddefcdccd5c0118823035bbb9fd
File	SHUTDOWN.EXE-E7D5C9CC.pf
Path	C:\Windows\Prefetch\
MD5	7cfb6a240ac6b4ffd03977bbae0ad509
SHA1	c8c0b70c7c5f9ebfa4e4c8c0535e98dc177be873

Untuk membuat IoC dapat digunakan secara umum, peneliti melakukan kembali instalasi ulang dan didapatkan hasil **Tabel 6.9** berikut

Tabel 6.9 Hasil prefetch pada percobaan kedua

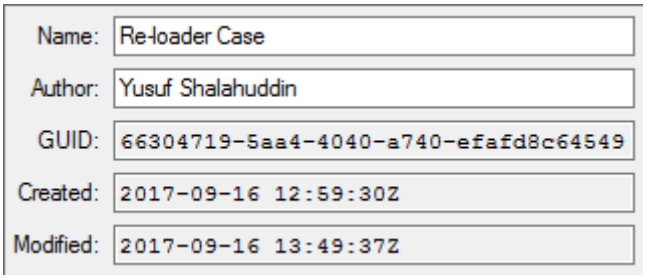
File	R@1n.txt
Path	C:\Users\Public\Desktop\
MD5	14ab52e1ac9a0733ad0b33e79b220a48
SHA1	9b7a9aa627528a24546de7d3584c5d95817efcd1
File	RE-LOADERBYR@1N.EXE-7204F358.pf
Path	C:\Windows\Prefetch\
MD5	5bff0807d969d1acf30f1a87d16ee75b
SHA1	8632f95ea3e944d4e547479c74e6acf81a442989
File	BRSET.EXE-CFAE891C.pf
Path	C:\Windows\Prefetch\
MD5	d8e2d438cc0203e54b547837f4169485
SHA1	6d51dc82a2a7bd8a1848b026474d9f6c982a18ae
File	BOOTSECT.EXE-C171AF2B.pf
Path	C:\Windows\Prefetch\
MD5	a6e4d7156cdf1dc41ee54ddd3d91a905
SHA1	886680e92b44acb582314718840e9e05eda5cc85
File	SHUTDOWN.EXE-E7D5C9CC.pf
Path	C:\Windows\Prefetch\
MD5	3eb7879030745affd78069099e9a4188
SHA1	f10af91607ba3546c1de89696389376c892463f8

Berdasarkan kedua tabel diatas diketahui bahwa barang bukti bisa saja memiliki nama posisi yang sama namun dapat dipastikan memiliki hash yang berbeda. Dengan demikian penulisan IoC yang dapat digunakan secara umum seperti pada **Gambar 6.35**.



Gambar 6.35 Isi indikator pada IOC

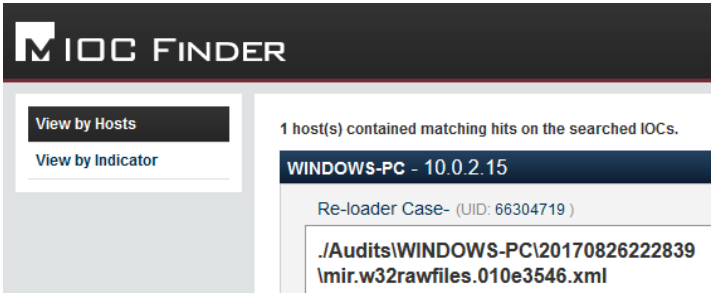
IOC yang telah dibuat mendapatkan GUID tercantum pada **Gambar 6.36**.



Gambar 6.36 Indentifkasi IOC

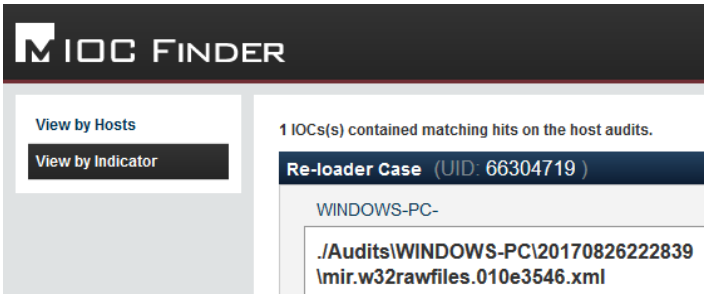
6.3.3 Hasil pengujian IOC

IOC yang telah dibuat berhasil membuktikan penggunaan Re-loader untuk membajak windows. Tampilan IoC Finder lebih mendukung untuk pengujian banyak IoC dengan banyak audit. Apabila dalam satu Host ditemukan indikator dari IoC yang berbeda, maka setiap penemuan akan dituliskan pada halaman View by Host. Halaman ini akan menampilkan IoC berdasarkan Host atau Audit dari perangkat yang berbeda sebagaimana terlihat pada **Gambar 6.37**.



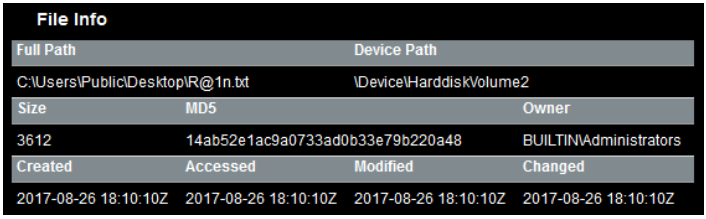
Gambar 6.37 Hasil pengujian IoC berdasarkan host

Apabila penelitian menggunakan satu IoC yang diuji pada banyak audit Host maka tampilan View by Indicator adalah yang terbaik. Halaman ini akan menampilkan Host mana saja yang terkena indicator IoC sebagaimana ditampilkan pada **Gambar 6.38**.

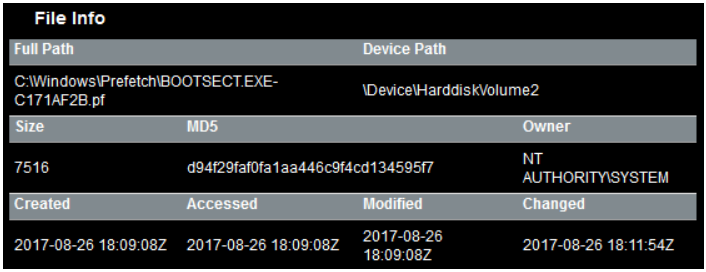


Gambar 6.38 Hasil pengujian IoC berdasarkan indikator

Berikut adalah penjelasan dari masing-masing file yang tercantum pada **Gambar 6.39**, **Gambar 6.40**, **Gambar 6.41**, **Gambar 6.42**, **Gambar 6.43** dan **Gambar 6.44**.



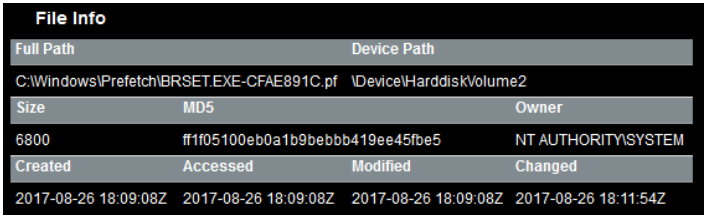
Gambar 6.39 Penjelasan dari file R@1n.txt



File Info

Full Path		Device Path	
C:\Windows\Prefetch\BOOTSECT.EXE-C171AF2B.pf		\Device\HarddiskVolume2	
Size	**MD5**		**Owner**
7516	d94f29faf0fa1aa446c9f4cd134595f7		NT AUTHORITY\SYSTEM
Created	**Accessed**	**Modified**	**Changed**
2017-08-26 18:09:08Z	2017-08-26 18:09:08Z	2017-08-26 18:09:08Z	2017-08-26 18:11:54Z

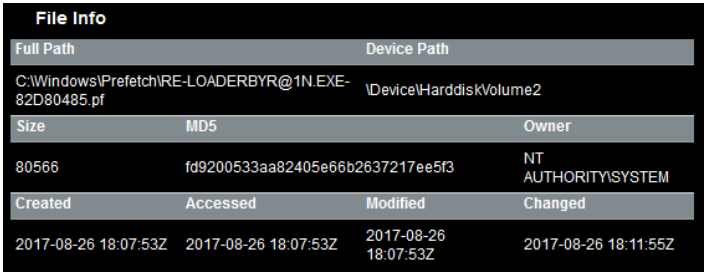
Gambar 6.40 Penjelasan dari file BOOTSECT.EXE-C171AF2B.pf



File Info

Full Path			Device Path
C:\Windows\Prefetch\BRSET.EXE-CFAE891C.pf			\Device\HarddiskVolume2
Size	**MD5**		**Owner**
6800	ff1f05100eb0a1b9bebbb419ee45fbe5		NT AUTHORITY\SYSTEM
Created	**Accessed**	**Modified**	**Changed**
2017-08-26 18:09:08Z	2017-08-26 18:09:08Z	2017-08-26 18:09:08Z	2017-08-26 18:11:54Z

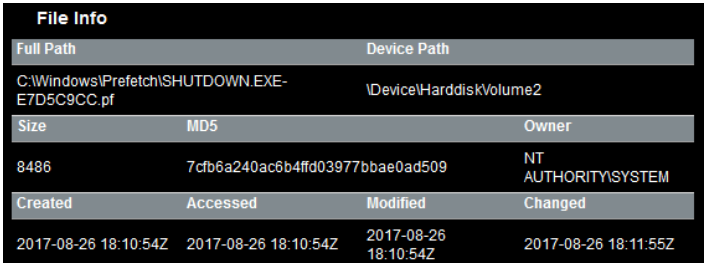
Gambar 6.41 Penjelasan dari file BRSET.EXE-CFAE891C.pf



File Info

Full Path		Device Path	
C:\Windows\Prefetch\RE-LOADERBYR@1N.EXE-82D80485.pf		\Device\HarddiskVolume2	
Size	**MD5**		**Owner**
80566	fd9200533aa82405e66b2637217ee5f3		NT AUTHORITY\SYSTEM
Created	**Accessed**	**Modified**	**Changed**
2017-08-26 18:07:53Z	2017-08-26 18:07:53Z	2017-08-26 18:07:53Z	2017-08-26 18:11:55Z

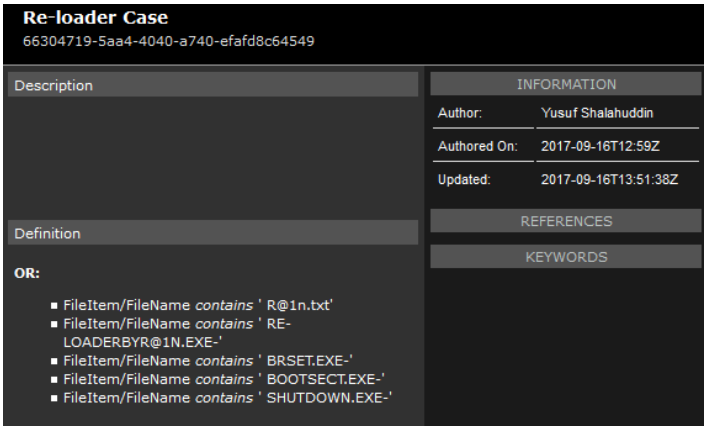
Gambar 6.42 Penjelasan dari file RE-LOADERBYR@1N.EXE-82D80485.pf



File Info

Full Path		Device Path	
C:\Windows\Prefetch\SHUTDOWN.EXE-E7D5C9CC.pf		\Device\HarddiskVolume2	
Size	**MD5**		**Owner**
8486	7cfb6a240ac6b4ffd03977bbae0ad509		NT AUTHORITY\SYSTEM
Created	**Accessed**	**Modified**	**Changed**
2017-08-26 18:10:54Z	2017-08-26 18:10:54Z	2017-08-26 18:10:54Z	2017-08-26 18:11:55Z

Gambar 6.43 Penjelasan dari file SHUTDOWN.EXE-E7D5C9CC.pf



Re-loader Case

66304719-5aa4-4040-a740-efafd8c64549

Description

Definition

OR:

- FileItem/FileName *contains* ' R@1n.txt'
- FileItem/FileName *contains* ' RE-LOADERBYR@1N.EXE-'
- FileItem/FileName *contains* ' BRSET.EXE-'
- FileItem/FileName *contains* ' BOOTSECT.EXE-'
- FileItem/FileName *contains* ' SHUTDOWN.EXE-'

INFORMATION

Author:	Yusuf Shalahuddin
Authored On:	2017-09-16T12:59Z
Updated:	2017-09-16T13:51:38Z

REFERENCES

KEYWORDS

Gambar 6.44 Penjelasan indikator yang digunakan

6.4 Hasil Pengujian pada Windows Asli

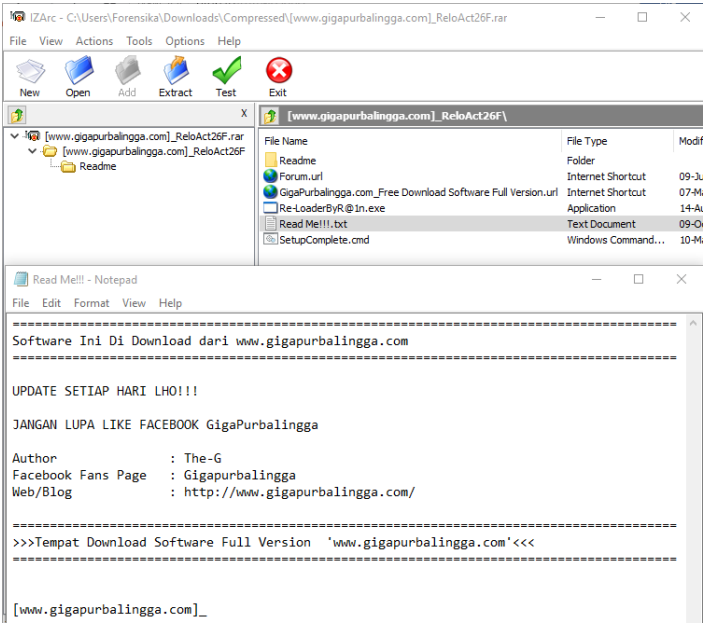
Sebagian besar barang bukti yang didapatkan berupa file prefetch. Hal ini memiliki kelebihan dan kekurangan. File prefetch akan tetap ada setelah computer restart namun hanya menyimpan 128 file prefetch terbaru sesuai dengan pernyataan MSDN terkait prefetch [36]. Setelah diuji, Windows 7 yang baru keluar dari toko komputer maupun yang diaktivasi manual tidak memiliki 5 barang bukti yang dicurigai.

Berikut beberapa alasan barang bukti tidak ditemukan :

1. R@1n.txt
   File ini dapat dihapus dengan mudah dan tergantikan dengan file lain di Desktop.
2. RE-LOADERBYR@1N.EXE- .pf
   File ini dapat memiliki nama yang berbeda-beda sehingga nama file prefetch juga berbeda.
3. BRSET.EXE- .pf
   Windows asli tidak menjalankan Brset.exe atau prefetch tertimpa dengan prefetch yang lebih baru.
4. BOOTSECT.EXE- .pf
   Windows asli tidak menjalankan Bootsect.exe atau prefetch tertimpa dengan prefetch yang lebih baru.
5. SHUTDOWN.EXE- .pf
   Windows asli tidak menjalankan Shutdown.exe kecuali pengguna pernah mematikan komputer melalui cmd.

6.5 Hasil Pengujian Varian Re-loader

Sebagian besar persebaran Re-loader yang umum didapatkan dari Google. Setelah menggunakan pencarian Google, sebagian besar website yang menyediakan aplikasi Re-loader hanya mengupload ulang aplikasi dan beberapa disertai dengan catatan dari mana aplikasi tersebut di dapatkan sebagaimana terlihat pada **Gambar 6.45**.



Gambar 6.45 Re-loader dari www.gigapurbalingga.com

Sebagian besar varian versi Re-loader yang muncul pada halaman awal Google hanya versi 2.6 yang telah diteliti dan versi 3.0 update dari versi sebelumnya. Versi yang lebih lama dapat ditemukan pada halaman Google berikutnya yang kemungkinan besar jarang dikunjungi karena hasil halaman awal Google sudah memenuhi kebutuhan pengguna. Setelah mencoba mengunduh aplikasi Re-loader khusus versi 2.6, semua file memiliki hash yang sama dengan yang digunakan pada penelitian ini. Nilai yang sama ini membuktikan file tersebut benar-benar sama tanpa perubahan.

BAB 7
KESIMPULAN

7.1 Kesimpulan

Berdasarkan hasil dari analisa diatas didapatkan kesimpulan sebagai berikut :

- Re-loader meninggalkan 5 file yang dapat digunakan sebagai bukti penggunaan aplikasi Re-loader yaitu R@1n.txt, RE-LOADERBYR@1N.EXE-82D80485.pf, BRSET.EXE-CFAE891C.pf, BOOTSECT.EXE-C171AF2B.pf, dan SHUTDOWN.EXE-E7D5C9CC.pf. File prefetch dengan ekstensi .pf dapat memiliki 8 karakter unik setelah nama aplikasi dan sebelum .pf. Karakter ini dapat berubah sesuai dengan media penyimpanannya, namun tetap dapat digunakan sebagai barang bukti.
- Dari sekian banyak analisa yang telah dilakukan, Re-loader dapat menginfeksi aplikasi lain menjadi Trojan Dropper dan HEUR yang akan mengirimkan data sensitif pngguna dan mengunduh lebih banyak malware dikemudian hari. Analisa Sysmon membuktikan aplikasi Re-loader menjalankan tiga aplikasi lain yaitu brset.exe, bootsect.exe, dan shutdown.exe. Analisa Regshot membuktikan bahwa ketiga aplikasi tersebut meninggalkan jejak berupa file prefetch untuk setiap aplikasi yang dijalankan. Analisa procexp hanya mendeteksi Re-loader sebagai proses yang mengandung virus sementara proses lain bersih. Analisa procmon menemukan satu file tambahan yang sengaja ditempatkan pada dekstop dengan nama R@1n.txt. Analisa autoruns tidak menemukan adanya autorun yang berbahaya atau mencurigakan. Analisa RAM menggunakan Volatility memang menemukan beberapa proses teridentifikasi mengandung malware.

- Aplikasi Re-loader 2.6 By R@1n yang diteliti menyimpan bahaya yang mengancam dimasa depan. Hal ini terlihat dari malware yang teridentifikasi merupakan malware yang mengundang malware lain untuk mencuri data dan kejahatan lainnya. Penegak hukum juga dapat mendeteksi adanya penggunaan aplikasi Re-loader menggunakan IoC seperti yang dilakukan dalam penelitian ini dan dapat menjerat pengguna dengan undang-undang hak cipta ataupun ITE.

7.2 Saran

Berdasarkan penelitian yang telah dilakukan, peneliti memiliki beberapa saran sebagai berikut :

- Dari sekian banyak aplikasi yang digunakan, hanya sysmon dan procmon yang mampu merekam secara akurat meskipun komputer mengalami restart.
- Hasil dari penelitian ini bisa berbeda apabila dilakukan kembali dalam jangka waktu yang lama. Hal ini dapat terjadi karena VirusTotal terus mengupdate database yang dimiliki dan para pembuat AntiVirus juga terus berkerja mendeteksi varian baru dari virus maupun malware.
- Apabila dalam penggunaanya di lapangan dilakukan anti forensik dengan menghapus secara permanen barang bukti yang telah disebutkan dalam penelitian ini, maka satu-satunya jalan untuk menemukan barang bukti lainnya adalah dengan menganalisa Registry yang tentu saja lebih sulit.
- Penggunaan IoC tidak hanya terbatas pada pencarian malware. IoC juga bisa digunakan untuk hal yang lain sesuai dengan kreatifitas pembuat IoC seperti mencari pencuri file, mendeteksi file porno, mendeteksi ancaman internal dan masih banyak lagi.
- Dalam penelitian ini CoC (Chain of Custody) tidak memiliki pengaruh yang besar, namun akan sangat

membantu apabila sebuah penelitian forensik digital menggunakan banyak peneliti.

- Penelitian ini hanyalah dasar pemahaman dari alur forensik digital yang lebih besar. Setiap pembahasan dalam penelitian ini dapat menjadi penelitian tersendiri dengan kasus yang berbeda namun memiliki penjelasan yang lebih mendalam. Adapun topik yang tidak dibahas secara mendalam dalam penelitian ini adalah Evidence Imaging, Standard Operating Procedure, Static Malware Analysis, SANS SIFT, REMnux, SysInternals, Nirsoft Package, Volatility, Chain of Custody, dan Indicators of Compromise.

Halaman ini sengaja dikosongkan

DAFTAR PUSTAKA

[1] M. A. N. Center, "Malware Infection Index 2016 highlights key threats undermining cybersecurity in Asia Pacific: Microsoft Report," Microsoft, 7 Juni 2016. [Online]. Available: https://news.microsoft.com/apac/2016/06/07/malware-infection-index-2016-highlights-key-threats-undermining-cybersecurity-in-asia-pacific-microsoft-report/#sm.000885kpv18yif7cpgd1881cw6iql. [Diakses 23 September 2016].

[2] StatCounter, "Top 7 Dekstop OSs in Indonesia on July 2016," [Online]. Available: http://gs.statcounter.com/#desktop-os-ID-monthly-201607-201607-bar. [Diakses 23 September 2016].

[3] W3Counter, "Browser & Platform Market Share Agustus 2016," W3Counter, [Online]. Available: http://www.w3counter.com/globalstats.php?year=2016&month=8. [Diakses 23 September 2016].

[4] B. Sadewo, "Indonesia Masuk 10 Besar Pengguna Software Bajakan," Telset, 23 Juli 2016. [Online]. Available: https://telset.id/141170/indonesia-masuk-10-besar-pengguna-software-bajakan/. [Diakses 23 September 2016].

[5] N. Kaur dan P. Amit Kumar Bindal, "A Complete Dynamic Malware Analysis," *International Journal of Computer Applications*, vol. 135, no. 4, pp. 20-25, 2016.

[6] F. Gianni dan F. Solinas, "Live DIgital Forensics: Windows XP vs WIndows 7," *IEEE*, no. 13, pp. 1-6, 2013.

[7] Mandiant, "WHITE PAPER: An Introduction to OpenIOC".

[8] H.-Y. Lock, "Using IoC (Indicators of Compromise) in Malware Forensics," *SANS Institute InfoSec Reading Room*, pp. 1-56, 2015.

[9] D. J. Andress, "Working with Indicators of Compromise," *ISSA Journal*, pp. 14-20, 2015.

[10] "Operating System Versioning," Microsoft, [Online]. Available: https://msdn.microsoft.com/en-gb/library/dd371754(VS.85).aspx. [Diakses 17 Oktober 2016].

[11] "Windows 7 system requirements," Microsoft, 1 September 2016. [Online]. Available:

https://support.microsoft.com/en-us/help/10737/windows-7-system-requirements. [Diakses 17 Oktober 2016].

[12] "Memory Limits for Windows and Windows Server Releases," Microsoft, [Online]. Available: https://msdn.microsoft.com/en-us/library/aa366778(VS.85).aspx#physical_memory_limits_windows_7. [Diakses 17 Oktober 2016].

[13] R. Messier, Operating System Forensics, Massachusetts: Syngress, 2016.

[14] "Google Trends," Google, [Online]. Available: https://www.google.com/trends/explore?date=all&q=Re-loader,KMS%20Pico. [Diakses 17 Oktober 2016].

[15] S. 182, "4 Aktivator Windows yang Paling Terkenal Sepanjang Masa," September 2014. [Online]. Available: http://www.software182.com/2014/09/aktivator-windows-dan-office-terkenal-sepanjang-masa.html#axzz4MzTlkems. [Diakses 14 Oktober 2016].

[16] E. Ozkaya, "Microsoft Virtual Academy," 14 Desember 2015. [Online]. Available: https://mva.microsoft.com/en-US/training-courses/windows-security-forensics-14383?l=YCKufUQsB_5105244527. [Diakses 4 Oktober 2016].

[17] EC-Council, Computer Forensics Evidence Collection & Preservation, Clifton Park: Cengage Learning, 2010.

[18] E. Council, Computer Hacking Forensics Investigators, EC-Council, 2013.

[19] D. Watson, Digital Forensics Processing and Procedures, Waltham: Elsevier, 2013.

[20] M. N. Al-Azhar, "The Essentials of Digital Forensic," 2016.

[21] K. Ryder, "Computer Forensics – We've had an incident, who do we get to investigate?," *SANS Institute InfoSec Readig Room*, pp. 1-12, 2002.

[22] M. Russinovich, "Windows Sysinternals," Microsoft, 29 Agustus 2016. [Online]. Available: https://technet.microsoft.com/en-us/sysinternals. [Diakses 5 Oktober 2016].

[23] ACCESSDATA, “FTK Imager,” ACCESSDATA, 23 Februari 2016. [Online]. Available: http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.2. [Diakses 5 Oktober 2016].

[24] “IOC EDITOR,” FireEye, 4 Desember 2012. [Online]. Available: https://www.fireeye.com/services/freeware/IoC-editor.html. [Diakses 5 Oktober 2016].

[25] “IOC FINDER,” FireEye, 31 Oktober 2011. [Online]. Available: https://www.fireeye.com/services/freeware/IoC-finder.html. [Diakses 5 Oktober 2016].

[26] “About,” Ubuntu Studio, [Online]. Available: https://ubuntustudio.org/about-ubuntustudio/. [Diakses 5 Oktober 2016].

[27] “SANS Investigative Forensic Toolkit (SIFT) Workstation Version 3,” SANS DFIR, [Online]. Available: http://digital-forensics.sans.org/community/downloads. [Diakses 5 Oktober 2016].

[28] L. Zeltser, “REMnux: A Linux Toolkit for Reverse-Engineering and Analyzing Malware,” REMnux, [Online]. Available: https://remnux.org/. [Diakses 5 Oktober 2016].

[29] M. McDougal, “Live Forensics on a Windows System: Using Windows Forensic Toolchest (WFT),” *Live Forensics on a Windows System,* pp. 1-23, 2006.

[30] C. C. Elisan, Advance Malware Analysis, Mc Graw Hill Education, 2015.

[31] M. P. a. K. M. Jason T. Luttgens, “Chapter 15 Malware Triage,” dalam *Incident Response & Computer Forensics, Third Edition*, New York, Mc Graw Hill Education, 2014, pp. 542-543.

[32] S. Pierce, “Cybrary Malware Analysis and Reverse Engineering,” 19 Januari 2015. [Online]. Available: https://www.cybrary.it/course/malware-analysis/comment-page-1/#comments. [Diakses 5 Oktober 2016].

[33] H. Bai, C.-z. Hui, X.-c. Jing, N. Li dan X.-y. Wang, “Approach for malware identification using dynamix behaviour and outcome triggeing,” *IET Information Security,* vol. 8, no. 2, pp. 140-151, 2014.

[34] H. C. Cory Altheide, Digital Forensics With Open Source Tools, Syngress, 2011.

[35] "A. Road Map for Digital Forensic Research," dalam *Digital Forensics Research Workshop*, 2001.

BIODATA PENULIS

Penulis dilahirkan di Bontang, Kalimantan Timur pada tanggal 4 Februari 1994. Penulis merupakan anak dari 2 bersaudara. Penulis telah menempuh pendidikan formal, yaitu TKIT YABIS Bontang, SDIT YABIS Bontang, SMPN 1 Bontang dan SMAN 1 Bontang. Setelah tamat SMA, penulis melanjutkan studi di Institut Teknologi Sepuluh Nopember Surabaya dan diterima di Departemen Sistem Informasi dengan NRP 05211240000172.

Penulis pernah melakukan kerja praktik di Departemen TI&Telkom, PT. Pupuk Kalimantan Timur. Selain itu, penulis juga pernah berkerja sebagai Asisten Praktikum Mata Kuliah Forensika Digital selama dua semester. Penulis juga memiliki sertifikasi Certified Secure Computer User v2 (CSCUv2) dari EC-Council dan Forensic Investigator dari Asosiasi Keamanan Siber Indonesia (AKSI). Selain itu penulis juga menjadi anggota Asosiasi Forensik Digital Indonesia (AFDI) dan Indonesia Honeynet Project (IHP)

Pada pengerjaan tugas akhir di Departemen Sistem Informasi ITS, penulis mengambil bidang minat Infrastruktur dan Keamanan Teknologi Informasi dengan topik Forensika Digital. Jika ada pertanyaan mengenai tugas akhir ini, penulis dapat dihubungi melalui email yusuf.shalahuddin@live.com.

Halaman ini sengaja dikosongkan

LAMPIRAN A - Chain of Custody

Case No.	1
Date/Time Collected	27 Agustus 2017 dan 13 September 2017
Collected by	Yusuf Shalahuddin
Site Address	Laboratorium Infrastuktur dan Keamanan Teknologi Informasi
Evidence No.	1
File Name	Re-LoaderByR@1n.exe
Storage Location	D:\Barang Bukti 2\[BAGAS31] Re-loader Activator 2.6 Final
File Size	1.51 MB (1,585,152 bytes)
MD5 Hash	686a5620c3da7834205c14d95d2a2d10
SHA1 Hash	aa92ac2cbcc42758b739bab0f60aa5b10cb8b34f
Note	Aplikasi untuk membajak Windows
Evidence No.	2
File Name	CleanRAM.mem
Storage Location	D:\Barang Bukti 2
File Size	1.99 GB (2,147,418,112 bytes)
MD5 Hash	ed4491a0b2ba4911b2b490fb84db6dbf
SHA1 Hash	40bc81d5ddbb9b6138eaccb0801d6adbc0ff9899
Note	Hasil imaging RAM tahap Clean
Evidence No.	3
File Name	Infected1RAM.mem
Storage Location	D:\Barang Bukti 2
File Size	1.99 GB (2,147,418,112 bytes)
MD5 Hash	9ef4fd024852bdc09ae03ea250770fd3
SHA1 Hash	d40bf8faa7adbcfb1e4573c160202435a5f577f1
Note	Hasil imaging RAM tahap Infected 1
Evidence No.	4
File Name	Infected2RAM.mem
Storage Location	D:\Barang Bukti 2
File Size	1.99 GB (2,147,418,112 bytes)
MD5 Hash	765f85e870104e9e6aebb66194bc7230
SHA1 Hash	e6eef14b029819c9031826509e92508ff40a7b0b
Note	Hasil imaging RAM tahap Infected 2
Evidence No.	5
File Name	Infected2HDD.001
Storage Location	D:\Barang Bukti 2

A-2

File Size	19.9 GB (21,367,881,728 bytes)
MD5 Hash	a93f389a37c3bff948be0040a742ccc6
SHA1 Hash	779ff0f6f3ecba28a90ec2eb76687fffef714034
Note	Hasil imaging HDD tahap Infected 2
Evidence No.	6
File Name	SW_DVD5_Win_Pro_7_32BIT_English _Full_MLF_X15-71033
Storage Location	D:\Barang Bukti 2
File Size	2.23 GB (2,400,239,616 bytes)
MD5 Hash	ea29222a152a3090d586f80d948fc0aa
SHA1 Hash	304817e859a5b27e828f46aac54cb46a576a34cc
Note	ISO Windows 7 Pro 32 bit asli
Evidence No.	7
File Name	66304719-5aa4-4040-a740-efafd8c64549.ioc
Storage Location	D:\Barang Bukti 2
File Size	4.00 KB (4,096 bytes)
MD5 Hash	d83ccfcaf48dacbd48231bc3c2955c57
SHA1 Hash	7a4f7ad1a60c501c0d2bd1b2570d8e3e47e09419
Note	IOC yang dapat digunakan secara umum

LAMPIRAN B - Forensic Analysis Log

Case No	1
Stage	1
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Menyiapkan Windows pada Virtualbox
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox
Time	Work
00:00-00:45	Instalasi Windows 7 Pro
00:45-00:55	Memasang VirtualBox Guest Additions
00:55-01:00	Mengatur Net Use pada CMD
01:00-01:05	Memasang .Net Framework 4
01:05-01:07	Memasang Snapshot 1 “Ready” Sebagai penanda tahapan Clean
01:07-01:09	Memasang Re-loader
01:09-01:10	Memasang Snapshot 2 “Infected 1” Sebagai penanda tahapan Infected 1
01:10-01:12	Melanjutkan pemasangan Re-loader
01:12-01:13	Memasang Snapshot 3 “Infected 2” Sebagai penanda tahapan Infected 2

Case No	1
Stage	2
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Akusisi RAM pada tahap Infected 2
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox FTK Imager
Time	Work
02:24-02:25	Menjalankan VirtualBox dengan Snapshot 3
02:25-02:26	Menjalankan FTK Imager melalui CMD

02:26-02:28	Melakukan Imaging RAM

Case No	1
Stage	3
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Regshot pada tahap Infected 2
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox Regshot
Time	Work
02:26-02:28	Menjalankan VirtualBox dengan Snapshot 3
02:28-02:29	Menjalankan Regshot melalui CMD
02:29-02:40	Melakukan 1st Shot and Save pada Regshot

Case No	1
Stage	4
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Process Explorer pada tahap Infected 2
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox Process Explorer
Time	Work
02:42	Menjalankan VirtualBox dengan Snapshot 3
02:42	Menjalankan Process Explorer melalui CMD
02:42-02:44	Mengatur kolom Verified Signer dan VirusTotal
02:44-02:45	Menyimpan hasil yang didapat

Case No	1
Stage	5
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017

Work	Autoruns pada tahap Infected 2
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox Autoruns
Time	Work
02:45	Menjalankan VirtualBox dengan Snapshot 3
02:45	Menjalankan Autoruns melalui CMD
02:45-02:47	Mengatur filter pada Autoruns
02:47-02:48	Menyimpan hasil yang didapat

Case No	1
Stage	6
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Audit IOC pada tahap Infected 2
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox IOC Finder
Time	Work
02:48	Menjalankan VirtualBox dengan Snapshot 3
02:49-05:28	Menjalankan IOC Finder melalui CMD

Case No	1
Stage	7
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Akusisi RAM pada tahap Infected 1
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox FTK Imager
Time	Work
08:06	Menjalankan VirtualBox dengan Snapshot 2
08:07	Menjalankan FTK Imager melalui CMD
08:07-08:09	Melakukan Imaging RAM

Case No	1
Stage	8
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Regshot pada tahap Infected 1
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox Regshot
Time	Work
08:10	Menjalankan VirtualBox dengan Snapshot 2
08:11	Menjalankan Regshot melalui CMD
08:11-08:26	Melakukan 1st Shot and Save pada Regshot

Case No	1
Stage	9
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Process Explorer pada tahap Infected 1
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox Process Explorer
Time	Work
08:27	Menjalankan VirtualBox dengan Snapshot 2
08:27	Menjalankan Process Explorer melalui CMD
08:27-08:29	Mengatur kolom Verified Signer dan VirusTotal
08:29-08:30	Menyimpan hasil yang didapat

Case No	1
Stage	10
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Autoruns pada tahap Infected 1

Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox Autoruns
Time	Work
08:33	Menjalankan VirtualBox dengan Snapshot 2
08:33	Menjalankan Autoruns melalui CMD
08:33-08:34	Mengatur filter pada Autoruns
08:34-08:35	Menyimpan hasil yang didapat

Case No	1
Stage	11
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Audit IOC pada tahap Infected 1
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox IOC Finder
Time	Work
08:38	Menjalankan VirtualBox dengan Snapshot 2
08:38-11:05	Menjalankan IOC Finder melalui CMD

Case No	1
Stage	12
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Akusisi RAM pada tahap Clean
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox FTK Imager
Time	Work
11:07	Menjalankan VirtualBox dengan Snapshot 1
11:08	Menjalankan FTK Imager melalui CMD
11:13-13:16	Melakukan Imaging RAM

B-6

Case No	1
Stage	13
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Sysmon pada tahap Clean
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox Sysmon
Time	Work
11:16	Menjalankan VirtualBox dengan Snapshot 1
11:17	Menjalankan Sysmon melalui CMD
11:17-11:29	Menjalankan Re-loader
11;29	Menyimpan Log file

Case No	1
Stage	14
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Regshot pada tahap Clean
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox Regshot
Time	Work
11:31	Menjalankan VirtualBox dengan Snapshot 1
11:31	Menjalankan Regshot melalui CMD
11:32-11:48	Melakukan 1st Shot and Save pada Regshot

Case No	1
Stage	15
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Process Explorer pada tahap Clean
Related Evidence	Evidence Number 1 Evidence Number 6

Related Software	VirtualBox Process Explorer
Time	Work
12:59	Menjalankan VirtualBox dengan Snapshot 1
12:59	Menjalankan Process Explorer melalui CMD
13:00-13:01	Mengatur kolom Verified Signer dan VirusTotal
13:01	Menyimpan hasil yang didapat

Case No	1
Stage	16
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Autoruns pada tahap Clean
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox Autoruns
Time	Work
13:02	Menjalankan VirtualBox dengan Snapshot 1
13:02	Menjalankan Autoruns melalui CMD
13:02-13:03	Mengatur filter pada Autoruns
13:03-13:04	Menyimpan hasil yang didapat

Case No	1
Stage	17
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Process Monitor pada tahap Clean
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox Process Monitor
Time	Work
13:05	Menjalankan VirtualBox dengan Snapshot 1
13:05	Menjalankan dan mengatur Process Monitor melalui CMD

13:06-13:12	Menjalankan Re-loader
13:12	Menyimpan hasil yang didapat

Case No	1
Stage	18
Investigator Name	Yusuf Shalahuddin
Date	27 Agustus 2017
Work	Audit IOC pada tahap Clean
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox IOC Finder
Time	Work
13:17	Menjalankan VirtualBox dengan Snapshot 1
13:17-15:51	Menjalankan IOC Finder melalui CMD

Case No	1
Stage	17
Investigator Name	Yusuf Shalahuddin
Date	13 September 2017
Work	Akusisi HDD pada tahap Infected 2
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox FTK Imager
Time	Work
12:37	Menjalankan VirtualBox dengan Snapshot 3
12:39	Menjalankan FTK Imager melalui CMD
12:39-13:04	Melakukan Imaging HDD

Case No	1
Stage	18
Investigator Name	Yusuf Shalahuddin
Date	28 Agustus 2017
Work	Ekstraksi proses pada RAM

Related Evidence	Evidence Number 2 Evidence Number 3 Evidence Number 4
Related Software	Volatility
Time	Work
01:46-02:02	Ekstraksi CleanRAM.mem
02:47-03:50	Ekstraksi Infected1RAM.mem
04:29-05:05	Ekstraksi Infected2RAM.mem

Case No	1
Stage	19
Investigator Name	Yusuf Shalahuddin
Date	13 September 2017
Work	Akusisi HDD pada tahap Infected 2
Related Evidence	Evidence Number 1 Evidence Number 6
Related Software	VirtualBox FTK Imager
Time	Work
12:37	Menjalankan VirtualBox dengan Snapshot 3
12:39	Menjalankan FTK Imager melalui CMD
12:39-13:04	Melakukan Imaging HDD

Case No	1
Stage	20
Investigator Name	Yusuf Shalahuddin
Date	16 September 2017
Work	Membuat IOC
Related Evidence	Evidence Number 7
Related Software	IOC Editor IOC Finder
Time	Work
09:53-20:51	Mencoba dan Menulis ulang IOC

LAMPIRAN C – Hasil Analisa Procexp

Hasil procexp pada tahap Clean

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
System Idle Process	0.24	0 K	12 K	0				
System	1.01	48 K	520 K	4				
Interrupts	2.17	0 K	0 K	n/a	Hardware Interrupts and DPCs			
smss.exe		216 K	696 K	272	Windows Session Manager	Microsoft Corporation	(Verified) Microsoft Windows	0/62
csrss.exe	< 0.01	1,120 K	3,000 K	344	Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft Windows	0/63
wininit.exe		784 K	3,104 K	392	Windows Start-Up Application	Microsoft Corporation	(Verified) Microsoft Windows	0/64
services.exe		4,300 K	7,124 K	492	Services and Controller app	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe		2,496 K	6,256 K	616	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
WmiPrvSE.exe		1,896 K	4,576 K	2524	WMI Provider Host	Microsoft Corporation	(Verified) Microsoft Windows	0/63
WmiPrvSE.exe		3,136 K	6,540 K	3052	WMI Provider Host	Microsoft Corporation	(Verified) Microsoft Windows	0/63
VBoxService.exe	0.61	1,408 K	3,976 K	676	VirtualBox Guest Additions Service	Oracle Corporation	(Verified) Oracle Corporation	0/63
svchost.exe		2,300 K	5,164 K	728	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	0.03	15,692 K	15,740 K	776	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
audiodg.exe	0.04	14,948 K	13,344 K	1000	Windows Audio Device Graph Isolation	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	0.22	23,232 K	29,724 K	896	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
dwm.exe		988 K	3,536 K	556	Desktop Window Manager	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	0.02	21,868 K	25,380 K	936	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
TrustedInstaller.exe		2,424 K	8,040 K	1088	Windows Modules Installer	Microsoft Corporation	(Verified) Microsoft Windows	0/65
svchost.exe	0.02	5,592 K	10,516 K	1132	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	< 0.01	10,468 K	10,196 K	1236	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
spoolsv.exe		4,460 K	8,224 K	1336	Spooler SubSystem App	Microsoft Corporation	(Verified) Microsoft Windows	0/64

C-2

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
svchost.exe		10,212 K	11,408 K	1372	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	0.03	4,828 K	9,296 K	1508	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
taskhost.exe		6,780 K	5,704 K	312	Host Process for Windows Tasks	Microsoft Corporation	(Verified) Microsoft Windows	0/65
SearchIndexer.exe	0.06	15,760 K	10,000 K	1984	Microsoft Windows Search Indexer	Microsoft Corporation	(Verified) Microsoft Windows	0/63
SearchProtocolHost.exe	< 0.01	1,516 K	4,964 K	3508	Microsoft Windows Search Protocol Host	Microsoft Corporation	(Verified) Microsoft Windows	0/64
SearchFilterHost.exe		916 K	3,248 K	2760	Microsoft Windows Search Filter Host	Microsoft Corporation	(Verified) Microsoft Windows	0/65
SearchProtocolHost.exe	0.25	1,100 K	3,396 K	3636	Microsoft Windows Search Protocol Host	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe		7,672 K	9,544 K	2060	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
wmpnetwk.exe	0.01	8,072 K	19,156 K	2232	Windows Media Player Network Sharing Service	Microsoft Corporation	(Verified) Microsoft Windows	0/65
taskhost.exe		3,284 K	8,112 K	3768	Host Process for Windows Tasks	Microsoft Corporation	(Verified) Microsoft Windows	0/65
mscorsvw.exe	0.05	4,160 K	7,724 K	4052	.NET Runtime Optimization Service	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
mscorsvw.exe	70.90	13,332 K	19,084 K	3364	.NET Runtime Optimization Service	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
sppsvc.exe		5,436 K	10,140 K	4084	Microsoft Software Protection Platform Service	Microsoft Corporation	(Verified) Microsoft Windows	0/65
svchost.exe		1,992 K	6,252 K	196	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
lsass.exe	0.63	2,764 K	7,800 K	500	Local Security Authority Process	Microsoft Corporation	(Verified) Microsoft Windows	0/64

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
lsm.exe	0.09	1,184 K	2,836 K	508	Local Session Manager Service	Microsoft Corporation	(Verified) Microsoft Windows	0/63
csrss.exe	1.30	1,112 K	4,452 K	404	Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft Windows	0/63
conhost.exe		888 K	3,940 K	2704	Console Window Host	Microsoft Corporation	(Verified) Microsoft Windows	0/64
winlogon.exe		1,844 K	5,596 K	432	Windows Logon Application	Microsoft Corporation	(Verified) Microsoft Windows	0/65
explorer.exe	0.39	23,168 K	32,292 K	724	Windows Explorer	Microsoft Corporation	(Verified) Microsoft Windows	0/64
VBoxTray.exe	0.07	1,484 K	5,172 K	1992	VirtualBox Guest Additions Tray Application	Oracle Corporation	(Verified) Oracle Corporation	0/65
cmd.exe		2,540 K	2,328 K	2696	Windows Command Processor	Microsoft Corporation	(Verified) Microsoft Windows	0/65
procexp.exe	20.82	17,688 K	30,344 K	3488	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com	(Verified) Microsoft Corporation	0/65
iexplore.exe		10,244 K	21,068 K	444	Internet Explorer	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
iexplore.exe	0.02	13,116 K	25,356 K	1348	Internet Explorer	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
rundll32.exe	0.72	1,600 K	3,916 K	1488	Windows host process (Rundll32)	Microsoft Corporation	(Verified) Microsoft Windows	0/64
rundll32.exe	0.29	1,536 K	3,856 K	1608	Windows host process (Rundll32)	Microsoft Corporation	(Verified) Microsoft Windows	0/64

C-4

Hasil procexp pada tahap Infected 1

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
System Idle Process	0.93	0 K	12 K	0				
System	2.05	48 K	1,220 K	4				
Interrupts	1.89	0 K	0 K	n/a	Hardware Interrupts and DPCs			
smss.exe		216 K	632 K	272	Windows Session Manager	Microsoft Corporation	(Verified) Microsoft Windows	0/62
csrss.exe	0.04	1,116 K	2,776 K	344	Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft Windows	0/63
wininit.exe		784 K	2,768 K	392	Windows Start-Up Application	Microsoft Corporation	(Verified) Microsoft Windows	0/64
services.exe	0.05	4,660 K	6,132 K	492	Services and Controller app	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe		2,472 K	5,556 K	616	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
WmiPrvSE.exe		1,776 K	4,396 K	2524	WMI Provider Host	Microsoft Corporation	(Verified) Microsoft Windows	0/63
WmiPrvSE.exe		4,308 K	8,808 K	3656	WMI Provider Host	Microsoft Corporation	(Verified) Microsoft Windows	0/63
VBoxService.exe		1,440 K	3,496 K	676	VirtualBox Guest Additions Service	Oracle Corporation	(Verified) Oracle Corporation	0/63
svchost.exe	0.04	2,592 K	5,256 K	728	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	0.03	14,876 K	12,532 K	776	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
audiodg.exe		14,948 K	8,556 K	1000	Windows Audio Device Graph Isolation	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	< 0.01	26,384 K	32,340 K	896	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
dwm.exe		1,144 K	3,964 K	556	Desktop Window Manager	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	0.01	14,908 K	23,068 K	936	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
TrustedInstaller.exe		2,128 K	6,576 K	1088	Windows Modules Installer	Microsoft Corporation	(Verified) Microsoft Windows	0/65
svchost.exe	0.01	5,952 K	10,536 K	1132	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	0.01	14,932 K	15,728 K	1236	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
spoolsv.exe		4,412 K	6,384 K	1336	Spooler SubSystem App	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe		10,432 K	9,812 K	1372	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe		5,260 K	9,452 K	1508	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
taskhost.exe		6,696 K	5,492 K	312	Host Process for Windows Tasks	Microsoft Corporation	(Verified) Microsoft Windows	0/65
SearchIndexer.exe	1.65	19,404 K	14,832 K	1984	Microsoft Windows Search Indexer	Microsoft Corporation	(Verified) Microsoft Windows	0/63
SearchProtocolHost.exe	0.12	4,508 K	7,960 K	1104	Microsoft Windows Search Protocol Host	Microsoft Corporation	(Verified) Microsoft Windows	0/64
SearchFilterHost.exe	0.09	1,876 K	5,596 K	2836	Microsoft Windows Search Filter Host	Microsoft Corporation	(Verified) Microsoft Windows	0/65
svchost.exe	< 0.01	7,516 K	9,132 K	2060	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
wmpnetwk.exe	< 0.01	8,052 K	3,820 K	2232	Windows Media Player Network Sharing Service	Microsoft Corporation	(Verified) Microsoft Windows	0/65
mscorsvw.exe	1.74	4,392 K	7,928 K	3472	.NET Runtime Optimization Service	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
mscorsvw.exe	64.20	10,568 K	14,220 K	1100	.NET Runtime Optimization Service	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
sppsvc.exe		7,628 K	12,184 K	3560	Microsoft Software Protection Platform Service	Microsoft Corporation	(Verified) Microsoft Windows	0/65
svchost.exe		2,032 K	5,272 K	3600	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe		1,044 K	3,712 K	4016	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe		460 K	1,756 K	340	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/64
lsass.exe	0.10	2,900 K	6,776 K	500	Local Security Authority Process	Microsoft Corporation	(Verified) Microsoft Windows	0/64
lsm.exe		1,192 K	2,548 K	508	Local Session Manager Service	Microsoft Corporation	(Verified) Microsoft Windows	0/63

C-6

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
csrss.exe	0.80	1,180 K	5,972 K	404	Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft Windows	0/63
conhost.exe		864 K	3,788 K	2704	Console Window Host	Microsoft Corporation	(Verified) Microsoft Windows	0/64
winlogon.exe		1,808 K	4,720 K	432	Windows Logon Application	Microsoft Corporation	(Verified) Microsoft Windows	0/65
explorer.exe	0.09	23,404 K	25,896 K	724	Windows Explorer	Microsoft Corporation	(Verified) Microsoft Windows	0/64
VBoxTray.exe	0.01	1,468 K	4,476 K	1992	VirtualBox Guest Additions Tray Application	Oracle Corporation	(Verified) Oracle Corporation	0/65
cmd.exe		2,540 K	2,252 K	2696	Windows Command Processor	Microsoft Corporation	(Verified) Microsoft Windows	0/65
Re-LoaderByR@1n.exe	< 0.01	52,048 K	71,504 K	3432	Activator		(No signature was present in the subject)	49/65
procexp.exe	23.07	21,532 K	35,472 K	4072	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com	(Verified) Microsoft Corporation	0/65
iexplore.exe	0.01	10,276 K	21,524 K	3312	Internet Explorer	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
iexplore.exe		13,356 K	25,392 K	3592	Internet Explorer	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
iexplore.exe	0.09	21,756 K	33,484 K	3332	Internet Explorer	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
rundll32.exe		1,536 K	3,540 K	1488	Windows host process (Rundll32)	Microsoft Corporation	(Verified) Microsoft Windows	0/64
rundll32.exe		1,492 K	3,492 K	1608	Windows host process (Rundll32)	Microsoft Corporation	(Verified) Microsoft Windows	0/64

Hasil Procexp pada tahap Infected 2

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
System Idle Process		0 K	12 K	0				
System	0.20	44 K	508 K	4				
Interrupts	3.13	0 K	0 K	n/a	Hardware Interrupts and DPCs			
smss.exe		212 K	692 K	272	Windows Session Manager	Microsoft Corporation	(Verified) Microsoft Windows	0/62
csrss.exe	0.12	1,100 K	2,920 K	348	Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft Windows	0/63
wininit.exe		780 K	3,088 K	396	Windows Start-Up Application	Microsoft Corporation	(Verified) Microsoft Windows	0/64
services.exe		4,056 K	7,276 K	480	Services and Controller app	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe		2,592 K	6,404 K	616	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/65
WmiPrvSE.exe	0.61	1,864 K	4,604 K	2352	WMI Provider Host	Microsoft Corporation	(Verified) Microsoft Windows	0/63
WmiPrvSE.exe		2,680 K	6,168 K	1928	WMI Provider Host	Microsoft Corporation	(Verified) Microsoft Windows	0/63
VBoxService.exe		1,396 K	3,960 K	676	VirtualBox Guest Additions Service	Oracle Corporation	(Verified) Oracle Corporation	0/63
svchost.exe	0.39	2,316 K	5,200 K	740	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/65
svchost.exe		15,604 K	15,780 K	828	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/65
audiodg.exe		14,892 K	13,548 K	988	Windows Audio Device Graph Isolation	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	< 0.01	22,904 K	30,296 K	884	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/65

C-8

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
dwm.exe		972 K	3,624 K	392	Desktop Window Manager	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	14.94	21,452 K	25,428 K	912	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/65
WMIADAP.exe	11.54	1,336 K	3,620 K	2452	WMI Reverse Performance Adapter Maintenance Utility	Microsoft Corporation	(Verified) Microsoft Windows	Hash subm...
svchost.exe	0.01	5,552 K	10,440 K	1060	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/65
svchost.exe	< 0.01	10,012 K	10,132 K	1204	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/65
spoolsv.exe		4,332 K	8,280 K	1340	Spooler SubSystem App	Microsoft Corporation	(Verified) Microsoft Windows	0/64
svchost.exe	0.02	9,360 K	10,604 K	1376	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/65
svchost.exe	0.02	4,796 K	9,524 K	1476	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/65
taskhost.exe		6,628 K	5,868 K	2020	Host Process for Windows Tasks	Microsoft Corporation	(Verified) Microsoft Windows	0/65
SearchIndexer.exe	0.02	18,820 K	12,532 K	356	Microsoft Windows Search Indexer	Microsoft Corporation	(Verified) Microsoft Windows	0/63
SearchProtocolHost.exe		1,684 K	4,740 K	2504	Microsoft Windows Search Protocol Host	Microsoft Corporation	(Verified) Microsoft Windows	0/64
SearchProtocolHost.exe		1,516 K	4,984 K	476	Microsoft Windows Search Protocol Host	Microsoft Corporation	(Verified) Microsoft Windows	0/64

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
SearchFilterHost.exe		916 K	3,252 K	3904	Microsoft Windows Search Filter Host	Microsoft Corporation	(Verified) Microsoft Windows	0/65
wmpnetwk.exe	0.02	7,568 K	19,160 K	1716	Windows Media Player Network Sharing Service	Microsoft Corporation	(Verified) Microsoft Windows	0/65
svchost.exe	0.02	7,544 K	9,708 K	2272	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/65
mscorsvw.exe	0.05	3,860 K	7,480 K	3980	.NET Runtime Optimization Service	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
mscorsvw.exe	59.04	21,684 K	29,280 K	2972	.NET Runtime Optimization Service	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
sppsvc.exe		5,768 K	10,524 K	4016	Microsoft Software Protection Platform Service	Microsoft Corporation	(Verified) Microsoft Windows	0/65
svchost.exe		1,948 K	6,304 K	4052	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft Windows	0/65
lsass.exe	1.00	2,748 K	7,912 K	504	Local Security Authority Process	Microsoft Corporation	(Verified) Microsoft Windows	0/64
lsm.exe		1,196 K	2,840 K	512	Local Session Manager Service	Microsoft Corporation	(Verified) Microsoft Windows	0/63
csrss.exe	1.30	1,124 K	4,472 K	404	Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft Windows	0/63
conhost.exe		860 K	3,916 K	2636	Console Window Host	Microsoft Corporation	(Verified) Microsoft Windows	0/64
winlogon.exe		1,820 K	5,716 K	444	Windows Logon Application	Microsoft Corporation	(Verified) Microsoft Windows	0/65
explorer.exe	0.07	21,184 K	32,916 K	308	Windows Explorer	Microsoft Corporation	(Verified) Microsoft Windows	0/64

C-10

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
VBoxTray.exe	0.03	1,436 K	5,216 K	1528	VirtualBox Guest Additions Tray Application	Oracle Corporation	(Verified) Oracle Corporation	0/65
cmd.exe		2,536 K	2,388 K	2628	Windows Command Processor	Microsoft Corporation	(Verified) Microsoft Windows	0/65
procexp.exe	7.45	16,432 K	30,556 K	3636	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com	(Verified) Microsoft Corporation	0/65
iexplore.exe	0.01	8,212 K	20,808 K	2940	Internet Explorer	Microsoft Corporation	(Verified) Microsoft Corporation	0/65
iexplore.exe	< 0.01	11,656 K	25,108 K	3092	Internet Explorer	Microsoft Corporation	(Verified) Microsoft Corporation	0/65