JURNAL REKAYASA SISTEM DAN INDUSTRI
e-ISSN: 2579-9142 p-ISSN: 2356-0843
http://jrsi.sie.telkomuniversity.ac.id

Memory Volatile Forensik untuk Deteksi Malware Menggunakan Algoritma *Machine Learning*

Forensic Volatile Memory for Malware Detection Using Machine Learning Algoritm

Fikri Bahtiar*[1], Nur Widiyasono[2], Aldy Putra Aldya[3]

[1,2,3]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Siliwangi

ARTICLE INFO

Article history:
Diterima xx-xx-xx
Diperbaiki xx-xx-xx
Disetujui xx-xx-xx

Kata Kunci:
Malware Forensik, Pembelajaran Mesin, Analisis Memori Volatile, Analisis Malware, Analisis RAM Forensik

ABSTRAK

Forensik dari volatile memory memainkan peran penting dalam penyelidikan cybercrime. Akuisisi RAM Memori atau istilah lain dump RAM dapat membantu penyelidik forensik dalam mengambil banyak informasi yang berkaitan dengan kejahatan. Ada berbagai alat yang tersedia untuk analisis RAM termasuk Volatilitas, yang saat ini mendominasi alat RAM forensik open-source. Telah terjadi bahwa banyak penyelidik forensik berpikir bahwa mereka mungkin memiliki malware dalam dump RAM. Dan, jika mereka benar-benar ada, mereka masih belum mampu menganalisis Malware, jadi sulit bagi mereka untuk menganalisis kemungkinan malware dalam dump RAM. Ketersediaan alat-alat seperti Volatilitas memungkinkan penyelidik forensik untuk mengidentifikasi dan menghubungkan berbagai komponen untuk menyimpulkan apakah kejahatan itu dilakukan dengan menggunakan malware atau tidak. Namun, penggunaan volatilitas membutuhkan pengetahuan tentang perintah dasar serta analisis malware statis. Pekerjaan ini dilakukan untuk membantu penyelidik forensik dalam mendeteksi dan menganalisis kemungkinan malware dari dump RAM. Pekerjaan ini didasarkan pada kerangka kerja volatilitas dan hasilnya adalah alat Forensik untuk menganalisis dump RAM dan mendeteksi kemungkinan malware di dalamnya menggunakan algoritma pembelajaran mesin untuk mendeteksi offline (tidak terhubung ke internet).

Keywords:
Malware Forensics, Machine Learning, Volatile Memory Analysis, Malware Analysis, Forensic RAM Analysis

ABSTRACT

Forensics from volatile memory plays an important role in the investigation of cyber-crime. The acquisition of RAM Memory or other terms of RAM dump can assist forensic investigators in retrieving much of the information related to crime. There are various tools available for RAM analysis including Volatility, which currently dominates open source forensic RAM tools. It has happened that many forensic investigators are thinking that they probably have malware in the RAM dump. And, if they do exist, they're still not very capable Malware Analysts, so it's hard for them to analyze the possibilities of malware in a RAM dump. The availability of tools such as Volatility allows forensic investigators to identify and link the various components to conclude whether the crime was committed using malware or not. However, the use of volatility requires knowledge of basic commands as well as static malware analysis. This work is done to assist forensic investigators in detecting and analyzing possible malware from dump RAM. This work is based on the volatility framework and the result is a Forensic tool for analyzing RAM dumps and detecting possible malware in it using machine learning algorithms in order to detect offline (not connected to the internet).

Email: muhamad.fikri118@gmail.com (Fikri Bahtiar)
DOI: https://doi.org/10.25124/jrsi.v5i02.311

*Penulis korespondensi

1. Pendahuluan

Komputer forensik adalah investigasi dan teknik analisis komputer yang melibatkan tahapan identifikasi, persiapan, ekstraksi, dokumentasi dan interpretasi dari data yang terdapat pada komputer yang berguna sebagai bukti dari peristiwa cyber-crime [1]. Komputer forensik pada awalnya dilakukan dengan cara menganalisis media penyimpanan dari sebuah sistem yang dicurigai telah terlibat dalam sebuah tindak kejahatan, dimana biasanya sistem perlu dinonaktifkan kemudian dibuat image kloning dari media penyimpanan sistem tersebut. Image inilah yang dianalisis yang dapat digunakan sebagai barang bukti untuk keperluan investigasi lebih lanjut [2]. Data volatile khususnya pada memory fisik atau RAM sebuah system menggambarkan seluruh kegiatan yang sedang terjadi pada sistem tersebut [2]. Ketersediaan alat seperti Volatilitas memungkinkan penyelidik forensik mengidentifikasi dan menghubungkan berbagai komponen untuk menyimpulkan apakah kejahatan Cyber itu dilakukan menggunakan malware atau tidak. Namun, penggunaan volatilitas membutuhkan pengetahuan tentang alat baris perintah (Command Line) serta analisis malware statis [2]. Sebagian Alat Forensik yang berfungsi mendeteksi malware secara otomatis, tetapi harus selalu terhubung dengan internet, dan deteksi malware yang dilakukan terbatas. Pekerjaan yang disebutkan dalam makalah ini terinspirasi untuk menerapkan algoritma machine learning dan otomatisasi langkah – langkah dasar. Keuntungan terbesar dari alat ini adalah, Pengguna dapat mendeteksi semua proses yang berjalan pada memory volatile dan tidak harus terkoneksi dengan internet dan Pengguna tidak perlu mengingat perintah, sintaknya atau bahkan ketika mau menggunakan perintah mana. Ini sangat berguna bagi mereka yang tidak lebih suka bekerja pada utilitas baris perintah karena mereka menghindari mengingat perintah. Solusi yang diusulkan disebut Memory Volatile Forensik untuk deteksi malware menggunakan algoritma machine Learning, adalah solusi untuk pengguna yang ramah dan akurat untuk mengatasi masalah diatas, juga menganalisa dan memberikan laporan akhir yang akurat tentang kemungkinan penggunaan malware dalam melakukan kejahatan.

2. Landasan Teori

2.1 Digital Forensik

Digital Forensik merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital. Penguasaan ilmu ini tidak hanya ditunjukan kepada kemampuan teknis semata tetapi juga terkait dengan bidang lain, seperti bidang hokum [3].

2.2 Ilmu Forensik

Forensik adalah ilmu apapun yang digunakan untuk tujuan hokum dengan tidak memihak bukti ilmiah untuk digunakan dalam pengadilan hukum, dan dalam penyelidikan dan pengadilan pidana [4].

2.3 Forensik Jaringan

Forensik Jaringan Merupakan ilmu keamanan computer berkaitan dengan investigasi untuk menemukan sumber serangan pada jaringan berdasarkan bukti log, mengidentifikasi, menganalisis, serta merekonstruksi ulang kejadian tersebut. Istilah *Network Forensik* memang di ambil dari terminologi yang berhubungan dengan kriminologi [5].

2.4 Cybercrime

Cyber Crime adalah segala macam penggunaan jaringan computer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital [6].

2.5 Barang Bukti

Barang Bukti (*Evidance*) yang diartikan pada forensic tidak lain ialah informasi dan data dari apa yang didapatkan pada suatu kasus. Barang bukti bagian terpenting dalam sebuah kasus kejahatan untuk memecahkan kasus tersebut [7]

1) Barang bukti elektronik: Barang bukti ini bersifat fisik dan dapat di kenali secara visual, sehingga investigator dan analis forensic harus sudah memahami serta menegnali masing-masing barang bukti elektronik ini ketika sedang melakukan proses pencarian (*searching*) barang bukti di TKP. Jenis barang bukti elektronik ini antara lain:

- PC
- *Notebook*
- *Tablet*
- *Handphone*
- *Flashdisk*
- *Harddisk*
- *CD/DVD*
- *Router,Switch*
- *Kamera*
- *CCTV*

2) Barang bukti digital: Barang bukti digital sangat rentan terhadap perubahan informasi didalamnya, perlu penanganan untuk menjaga keutuhan barang bukti.

- *Logical Drive*
- *Deleted File / Unallocated Custer*
- *Lost File*
- *Slack File*
- *Log File*
- *Encrypted File*
- *Steganography File*
- *Office File*
- *Audio File*
- *Image File*
- *Video File*
- *Email / Electronic Mail*
- *User ID and Password*
- *SMS / Short Message Service*
- *Call Log*

2.6 Memory Volatile

Memori volatile adalah penyimpanan komputer yang hanya menyimpan datanya saat perangkat diaktifkan.
Sebagian besar RAM (*Random Access Memory*) yang digunakan untuk penyimpanan primer di komputer adalah

Email: muhamad.fikri118@gmail.com (Fikri Bahtiar)
DOI: https://doi.org/10.25124/jrsi.v5i02.311

*Penulis korespondensi

memori yang mudah menguap. RAM jauh lebih cepat untuk dibaca dan ditulis dibandingkan dengan jenis penyimpanan lain di komputer, seperti hard disk atau media yang dapat dipindahkan. Namun, data dalam RAM tetap ada ketika komputer sedang berjalan, akan tetapi sebaliknya ketika komputer dimatikan, RAM kehilangan datanya. [8]

2.7 Machine Learning

Machine learning (Pembelajaran Mesin) merupakan kemampuan komputer untuk melakukan pembelajaran tanpa harus menjelaskan (programmed) secara eksplisit kepada komputer, atau menurut Tom Mitchel suatu komputer dikatakan melakukan pembelajaran dari pengalaman E terhadap tugas T dan mengukur peningkatan kinerja P, jika kinerja Tugas T diukur oleh kinerja P, meningkatkan pengalaman E [18].

3. Penelitian Terkait

Investigator Forensik, Analis Malware, dan Perusahaan sedang bekerja dari bertahun-tahun dalam mengotomatisasi proses analisis untuk memudahkan pekerjaan mereka. Kecuali aspek forensik seperti yang dibahas dalam hal ini, ada banyak Tools sandBoxes tersedia yang gratis seperti cuckoo [9] yang menyediakan otomatisasi dalam proses analisis malware. Juga Michael Bailey, et. Al. mengusulkan otomatisasi klasifikasi dan analisis cara kerja Malware Internet [10]. Manuel Egele, et. Al. dalam survei mereka mendiskusikan berbagai Tools sanBoxes dan alat analisis malware otomatis [11]. Akan tetapi hasil otomatisasi memory forensik sangat sedikit dalam proses pengerjaanya sampai selesai Tomer Teller, et. Al. mengusulkan solusi berdasarkan cuckoo, Volatility dan IDA [12] dalam jurnal mereka di Blackhat [13], tetapi, itu sangat tergantung pada tool Cuckoo. Penelitian yang lain seperti Logen, Höfken dan Schuba menyediakan solusi berbasis GUI sebagai Perkembangan Volatilitas dalam jurnal mereka [14], meskipun pekerjaan yang diajukan oleh mereka melakukan beberapa tugas dasar secara otomatis, Sementara alat lain eVOLe yang dikembangkan oleh James Habben [15] adalah alat berbasis web, AJEAT Vol.6 No.2 Juli-Desember 2017 akan tetapi alat itu hanya menanyakan profil Image pada saat eksekusi, yang menunjukkan bahwa pengguna diminta untuk menjalankan Volatilitas secara terpisah untuk mendapatkan profil dan pekerjaan menjadi membosankan. GUI eVOLe yang lebih lanjut tidak menyediakan Analisis Malware yang lengkap. Rughani Vimal, et. al. mengusulkan solusi GUI untuk proses deteksi malware secara otomatis, akan tetapi dalam pendekteksian malware dengan jumlah yang terbatas dan harus terhubung dengan internet [16]. Untuk mengatasi semua masalah seperti itu, Memory Volatile Forensik Untuk deteksi malware menggunakan Algoritma Machine Learning [17] diusulkan di bagian berikutnya.

4. Alat yang Diusulkan

Penelitian ini dilakukan untuk membantu Digital Forensic Investigator, diasumsikan yang tidak ahli dalam menganalis malware tetapi diperlukan untuk memiliki beberapa mekanisme yang dapat dengan mudah mereka identifikasi Kehadiran malware apa pun dalam dump memory RAM (Random Access Memory). Alat yang diusulkan yaitu Memory Volatile Forensik menggunakan Algoritma Machine Learning adalah GUI berbasis Desktop untuk melakukan Memori Forensik secara Otomatis terkait pekerjaan yang rumit dan membosankan. GUI dari alat ini dikembangkan dalam bahasa pemrograman Java [18], berbasis desktop, untuk melakukan Forensik Memori. Investigator Forensik harus melakukan langkah-langkah yang sangat minimal dalam menganalisis laporan dari Memory Forensic. Alat yang dibuat ini hanya membutuhkan satu file image dump RAM yang akan dianalisis. Alat ini menyediakan peramban file untuk mengunggah image dump RAM. Setelah file image akan diunggah dan mulai mengeksekusi secara komplek proses yang berbeda secara otomatis di latar belakang, pengguna juga akan mendapatkan tampilan secara langsung status pada proses yang sedang dieksekusi. Proses Otomatis pertama yang dilakukan oleh alat ini adalah mengekstrak file dump dan menempatkan file dump yang valid di tempat yang tepat untuk dieksekusi lebih lanjut. Langkah selanjutnya adalah mengidentifikasi informasi file image dump RAM yang akan memberikan rincian tentang Sistem Operasi. Alat ini akan mengidentifikasi informasi seperti Profil (Volatilitas) untuk melihat arsitektur Sistem Operasi). Semua informasi file image dump RAM ini akan digunakan saat melakukan semua perintah lainnya. Setelah merberikan informasi file image dan profil, alat ini mulai menjelajahi dan menganalisis dump proses pada memory volatile, Proses ini berperan penting dalam mengidentifikasi serangan malware. Sebagian besar malware termasuk ransomware berbasis jaringan dan berfungsi sebagai botnet. Sbagian besar malware ini harus terhubung ke pusat kontrol untuk mengeksekusi perintah selanjutnya atau mengirim informasi penting atau rahasia. Untuk menyelesaikan komunikasi semacam itu, malware menggunakan IP dengan port yang terbuka. Liming Cai, dkk. menyatakan “Kita harus mengakses memori fisik komputer sistem untuk menemukan informasi yang lebih penting, seperti alamat IP penyusup, informasi tentang program jahat yang sedang berjalan, proses, worm, Trojan dan sebagainya di jurnal mereka [19]. Untuk mengidentifikasi IP dengan Port yang terbuka seperti itu, Alat ini akan menganalisis Koneksi Jaringan dari file dump RAM yang diberikan. Ini akan memberikan semua informasi yang mungkin dan perlu secara detail kepada Anda untuk mengidentifikasi IP atau port yang terbuka. Jadi jika ada IP atau port yang ditemukan, kita dapat dengan mudah menghubungkan dengan proses yang terkait. Penting untuk dicatat bahwa yang sebutkan di atas proses mungkin menjadi sulit bagi peneliti Forensik yang awam, jika mereka melakukan pemeriksaan malware secara manual untuk setiap IP, port dan proses. Alat ini yang berperan sangat penting dalam melakukan proses yang disebutkan di atas secara otomatis. Setelah mengidentifikasi Proses yang dicurigai malware, tugas penting berikutnya adalah untuk menggali lebih banyak tentang proses itu dan mengidentifikasi executable, DLL, dan file yang digunakan oleh Proses itu [27],[28]. Alat ini menyediakan fitur pengunduhan untuk diproses, jadi Forensic Investigators bisa bereksperimen dengan mencurigai file executable atau Proses di lingkungan yang terisolasi atau mereka bisa mengirim file tersebut untuk diajukan ke pusat penelitian malware untuk penyelidikan lebih lanjut. Selain itu untuk sistem windows, Registry adalah sumber untuk forensic artefak yang dapat digunakan selama investigasi, insiden penanganan respons, dan analisis

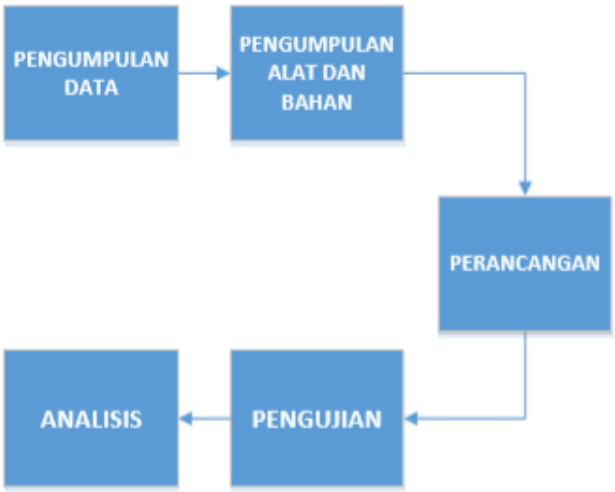
malware. Selain fitur yang disebutkan di atas, Alat ini menyediakan fitur pemindaian file proses individual untuk virus, worm, Trojans dan segala macam malwares. Alat ini menggunakan algoritma Machine Learning sebagai proses pendeteksian malware untuk dapat mendeteksi malware secara offline dan tidak terbatas selama proses memory berjalan. Alat ini adalah wadah untuk menutupi dan mengotomatiskan semua langkah yang diperlukan oleh proses Memori Forensik dalam membantu Digital Forensic Investigator. Pengguna akan mendapatkan hasil yang akurat tanpa mengetahui baris perintah yang diberikan tools volatility. Alat ini tersedia hanya untuk Windows 7, 8.1 dan 10 dan mendukung file image dump memori dari Windows, Linux dan Mac.

5. Metodologi Penelitian

5.1 Tahapan Penelitian

Merupakan langkah-langkah dalam melakukan penelitian, berikut tahapan penelitian yang dilakukan sebagai berikut :

1) *Pengumpulan data:* Pengumpulan informasi dari sumber yang berkaitan dengan penelitian, studi literatur yaitu sumber-sumber dari jurnal, buku, internet, artikel dan lain-lain.
2) *Pengumpulan Alat dan Bahan:* Pengumpulan kebutuhan-kebutuhan yang digunakan pada penelitian, baik berupa perangkat keras, dan perangkat lunak yang mendukung dalam pembuatan alat forensik ini.
3) *Perancangan:* Membuat rancangan dan interface untuk menghubungkan framework volatilitas dengan algoritma machine learning.
4) *Pengujian:* Pengujian hasil analisis dump memory, dan proses deteksi malware menggunakan algoritma machine learning.
5) *Analisis:* yaitu ntuk menganalisis terhadap proses yang terinfeksi malware pada memory volatile.



Gambar 1. Tahapan Penelitian

5.2 Kebutuhan Bahan

1) *Perangkat Keras*

Beberapa perangkat keras yang dibutuhkan dalam pembuatan *tool forensic* ini, berikut dijelaskan pada Tabel I.

TABEL I
PERANGKAT KERAS YANG DIBUTUHKAN

NO	NAMA	JUMLAH
1	Laptop *HP* Intel Core i3 Ram 4GB	1 Unit
2	Flashdisk	1 Unit

2) *Perangkat Lunak*

Beberapa perangkat lunak yang dibutuhkan untuk membuat *tools forensic* ini, berikut dijelaskan pada Tabel II.

TABEL II
PERANGKAT LUNAK YANG DIBUTUHKAN

NO	NAMA	Fungsi
1	Windows 7, 8,1, 10	Sistem Operasi
2	Framework Volatility	Analisis memory
3	Scikit-learn	Library python untuk algoritma machine learning
4	pefile	Library python untuk membaca PE-Header
4	Java Netbeans	Program GUI yang menghubungkan framework volatility dengan algoritma machine learning.

5.3 Perancangan

1) *Proses Permodelan Algortima Klasifikasi*

Algoritma Klasifikasi yang digunakan adalah dengan cara mengevaluasi 5 algoritma yaitu :

A. *Algoritma Naive Bayes*

Naïve Bayes adalah salah satu model paling praktis dalam algoritma machine learning. Mitchell memperkenalkan metode naive bayes secara rinci dalam buku nya [20]. Michie, Spiegelhalter, dkk meneliti dan mendalami model naive bayes [21], dan mereka membandingkan algoritma model klasifikai Naive bayes dengan algoritma pembelajaran lainnya, seperti pohon keputusan (Decision Tree). Hasil studi mereka menunjukkan bahwa di Indonesia kebanyakan kasus kinerja Naive Bayes sama baiknya dengan model lainnya.

B. *Algoritma Decision Tree / Pohon Keputusan*

Metode pohon keputusan mencapai popularitasnya karena kesederhanaannya. Bisa mengoptimalkan dengan baik dengan dataset yang besar dan dapat menangani ketidakakuratan di dataset dengan sangat baik. Keuntungan lainnya adalah tidak seperti algoritme lain, seperti SVM atau KNN, pohon keputusan beroperasi dalam "White Box", yang berarti bahwa kita dapat melihat dengan jelas bagaimana hasil yang diperoleh dan keputusan mana yang paling akurat. Fakta-fakta ini menjadikannya solusi untuk diagnosis medis, filtering spam,filtering keamanan, dan bidang lain [18].

C. *Algoritma Random forest*

Aloritma Random Forest merupakan algoritma yang dapat dipakai pada klasifikasi dan regresi. Diperkenalkan oleh Leo Breinan [22] dimana teknik ini dapat menghasilkan banyak pohon klasifikasi. Bagaimana Random Forest dapat menghasilkan

klasifikasi berawal mula dari input vector yang bergerak menuruni masing masing pohon. Masing-masing pohon merupakan klasifikasi berdasarkan mekanisme suara terbanyak atau vote untuk menandai class tersebut. Sehingga pepohonan (forest) dapat menentukan klasifikasi berdasarkan hasil voting tersebut.

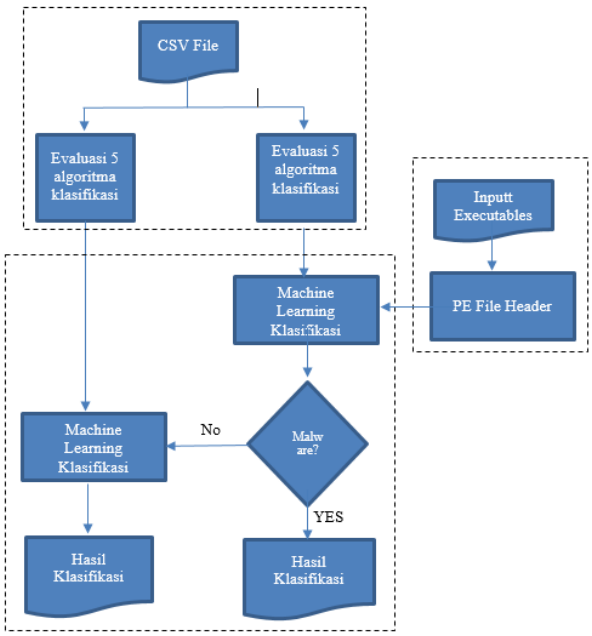
D. Algoritma AdaBoost

Algoritma AdaBoost adalah algoritma klasifikasi yang dapat meningkatkan algoritma machine learning yang lemah dengan akurasi sedikit lebih baik dari pada menebak secara acak menjadi algoritma machine learning yang kuat. [23].

E. Gradient bossting

Algoritma Gradient boosting seperti halnya keluarga algoritma Boosted lainnya memiliki kemampuan untuk meningkatkan akurasi prediktif model. Beberapa algoritma boosting lainnya seperti: XGBoost, AdaBoost dan GentleBoost memiliki formula matematika tersendiri dan bervariasi. Konsep Gradient Boosting terletak pada pengengembangannya yang mana memiliki ekspansi tambahan terhadap fitting criterion [24].

Sehingga dapat efektif dalam mengklasifikasi file PE Header pada dataset dengan hasil ektraksi file PE yang diinput dari modul python yaitu "pefile". Berikut adalah proses permodelan algoritma klasifikasi :



Gambar 2. Proses Permodelan algortima klasifikasi

2) Pengambilan sampel DataSet

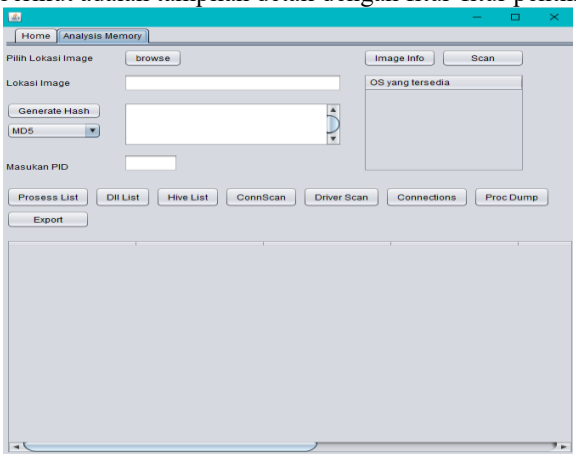
DataSet yang dikumpulkan yaitu sebanyak 41,323 file sampel dari hasil ekstraksi folder system32 di Windows 7,8.1 dan 10, File-file dalam folder system32 diekstrak setelah instalasi OS dengan update terbaru. Sampel malware yang dapat dieksekusi diunduh dari situs web VXheaven [25]. Jumlah total sampel malware adalah 96.724 yang mengandung PE-header. "pefile" yang merupakan salah satu dari modul python dipilih untuk mendeteksi PE-header pada suatu file dan mengekstraksi informasi header-PE dari file PE tersebut [26].

6. Hasil dan Pembahasan

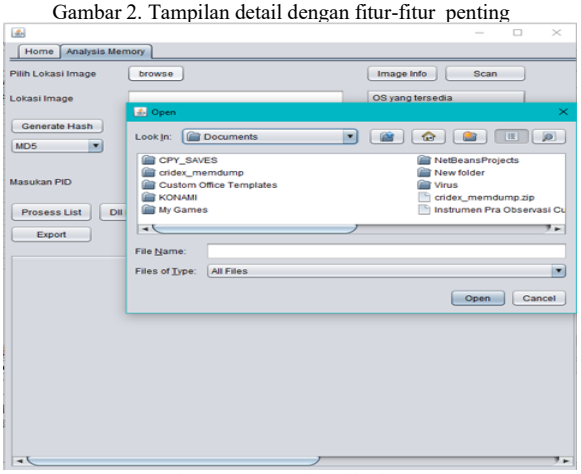
Setelah mendapatkan file, Seseorang dapat menginstal alat ini setelah terinstall software pendukung yaitu :

a. JDK & JRE versi 1.8.0
b. Python 2.7
c. Pandas
d. Numpy
e. Pickle
f. Scipy
g. Scikit-learn
h. Pefile

Setelah terinstal semua, alat ini bisa dijalankan. Gambar 2-3 berikut adalah tampilan detail dengan fitur-fitur penting..

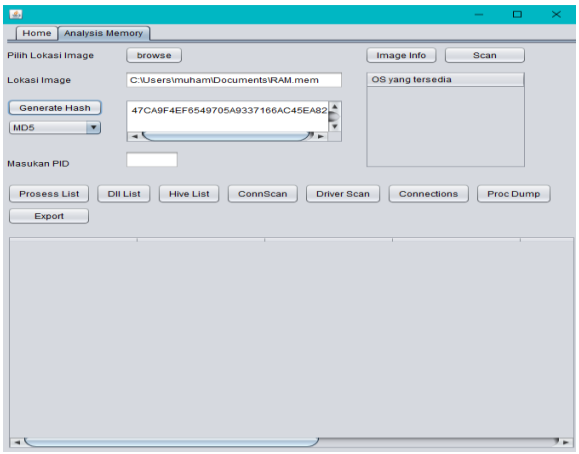


Gambar 2. Tampilan detail dengan fitur-fitur penting



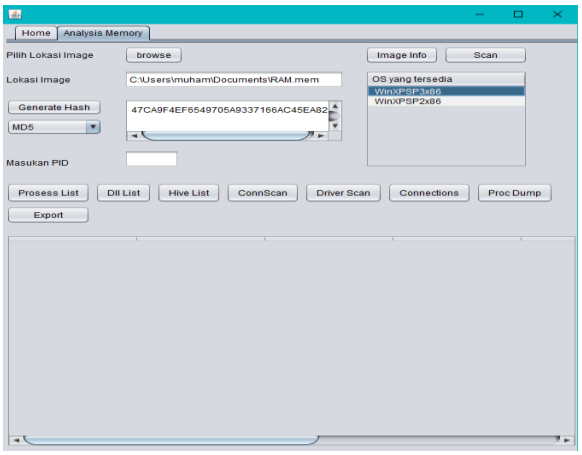
Gambar 3. Memasukan file dump RAM

Pengguna dapat mengunggah file image dump memory menggunakan tombol browse yang ditampilkan pada gambar berikut. Karena ukuran dump memory mungkin dalam GB atau MB sesuai ukuran memory fisik yang diakusisi, pengguna diminta untuk mengklik tombol Analyze Dump, Alat ini akan mulai Menganalisa file dump tersebut dan akan memperbarui menampilkan hasil dari forensic memory berupa profil, proses yang sedang berjalan.



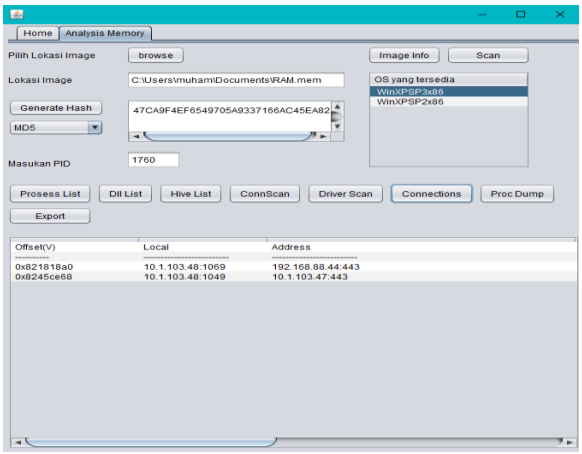
Gambar 4. Menampilkan Nilai Hash pada file image yang diinputkan

Setelah memasukan file image, pengguna juga dapat melihat nilai hash suatu file, dengan cara memilih tombol *generate hash*. Nilai hash ini berfungsi sebagai keaslian suatu data, jika file image tersebut sudah ada yang memodifikasi , dapat diketahui pada bagian hash nya akan berubah, tidak akan sama dengan yang original.



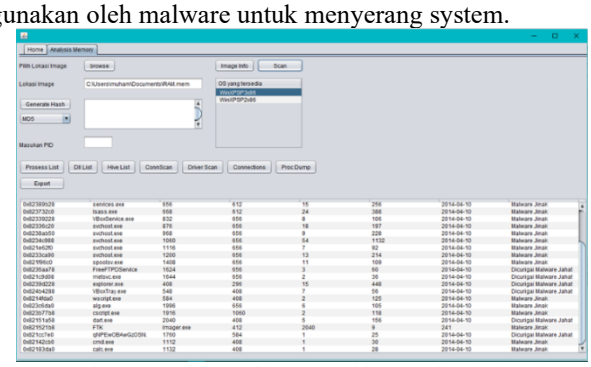
Gambar 4. Informasi dan proses keseluruhan dari memory volatile

Setelah analisis yang berhasil, alat ini mengalihkan pengguna ke tombol yang lain di interface awal untuk menampilkan daftar proses dengan detail yang relevan seperti thred, handle, dan dll terkait dengan setiap proses.



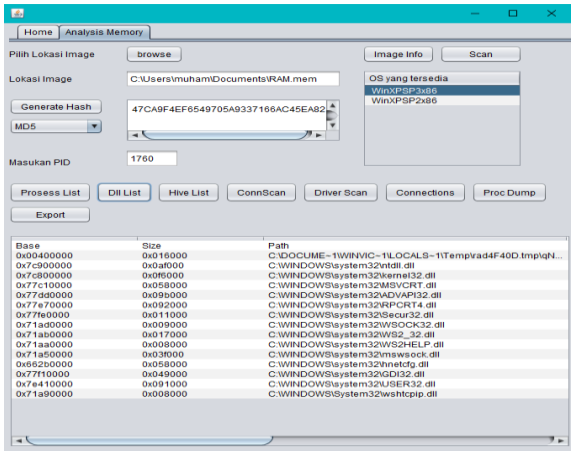
Gambar 5. Tampilan *Connection* pada jaringan

Pengguna dapat mengetahui IP dan port yang terhubung pada komputer, sehingga dapat diketahui port mana yang digunakan oleh malware untuk menyerang system.



Gambar 5. Proses scan file Executable yang dicurigai malware

Dari perspektif analisis malware, proses yang mencurigakan dapat dianalisis dengan mengklik tombol scan. Itu akan memindai proses individu untuk virus, worm, Trojan. Ketika Anda mengklik tombol scan, itu akan menjalankan algorima machine learning untuk mendeteksi malware pada proses tersebut.



Pada proses ini pengguna dapat mengetahui file-file terinfeksi yang digunakan oleh malware dalam menyerang system operasi, dan dapat ekstrak melalui tombol *procdump*.

7. Kesimpulan

Hasil dari pekerjaan ini akan memberikan manfaat dan bantuan untuk penyelidik forensik dalam menganalisis memori volatile dan mendeteksi malware secara offline (tidak terhubung ke internet) yang mungkin ada pada memory volatile. Alat ini telah diuji dengan 4 berbagai sampel dan memberikan hasil yang akurat untuk semua sampel. Akurasi dan keramahan pengguna alat ini akan membantu penyidik forensic investigator. Alat ini juga dapat mengurangi biaya pelatihan penyelidik forensik untuk menganalisis malware.

8. Ruang Lingkup Pengembangan

Padahal, alat ini memenuhi semua persyaratan dalam menganalisis malware dengan algoritma klasifikasi, masih ada ruang lingkup untuk pengembangan. Alat ini dapat diperluas dalam menganalisis malware secara detail. Alat yang dikerjakan saat ini hanya mendukung proses yang mengandung/terinfeksi malware, sehingga tidak dapat

memberikan informasi yang lebih detail dari malware tersebut. Terakhir, dibuatkan sebuah GUI untuk proses otomatis ini dapat operasikan pada system operasi yang lain seperti Linux dan Mac untuk lebih bervariasi.

Referensi

[1] Michael Solomon, Diane Barrett, Neil Broom. (2005), "Computer Forensics Jumpstart", Alameda, SYBEX Inc.

[2] Adestein. Frank, 2006, "Live Forensics – Diagnosing Your System Without Killing It First ", Communication of The ACM February 2006/Vol 49.

[3] B. Raharjo, "SEKILAS MENGENAI FORENSIK DIGITAL," Jurnal Sosioteknologi, 2013

[4] E. S. Wijaya and Y. P. , "Integrasi Metode Steganografi DCS pada Image dengan Kriptografi Blowfish sebagai Model Anti Forensik untuk Keamanan Ganda Konten Digital," 2015.

[5] R. U. Putri and J. E. Istiyanto, "Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada," 2012.

[6] M. N. Al-Azhar, Digital Forensic : Panduan Praktis Investigasi Komputer, Jakarta: Salemba Infotek, 2012.

[7] K. E. Pramudita, "Brute Force Attack dan Penerapannya pada Password Cracking," p. 1, 2010.

[8] Rouse Margaret, "Home/Topic/Data Center/Storage Hardware/volatile memory," https://whatis.techtarget.com/definition/volatile-memory,2014 accessed May 31, 2018.

[9] Cuckoo Sandbox – A malware Analysis system https://www.cuckoosandbox.org

[10] Kim Dong-Hee, Woo Sang-Uk, Lee Dong-Kyu, Chung Tai-Myoung, " Static Detection of Malware and Benign Executable Using Machine Learning Algorithm" in The Eighth International Conference on Envolving Internet", 2016.

[11] Manuel Egele, Theodoor Scholte, Engin Kirda and Christopher Kruegel, "A Survey on Automated Dynamic Malware Analysis Techniques and Tools" in the ACM Computing Surveys, Vol.44 ,Issue 2, Article No. 6, pp. 1–49, 2012.

[12] IDA - Multi-processor disassembler and debugger, https://www.hex-rays.com/products/ida/

[13] Tomer Teller, Adi Hayon, "Enhancing Automated Malware Analysis Machines with Memory Analysis" , Blackhat Arsenal , pp. 1-5, 2014.

[14] Rughani Vimal, Rughani Parag H, "AUMFOR : Automated Memory Forensics for Malware Analysis" in Asian Journal of Engineering And Applied Technology, Vol.6, No.2, pp.36-39, 2017.

[15] eVOLve by JamesHabben, https://github.com/ James Habben/evolve

[16] Rughani Vimal, Rughani Parag H, "AUMFOR : Automated Memory Forensics for Malware Analysis" in Asian Journal of Engineering And Applied Technology, Vol.6, No.2, pp.36-39, 2017

[17] Kim Dong-Hee, Woo Sang-Uk, Lee Dong-Kyu, Chung Tai-Myoung, " Static Detection of Malware and Benign Executable Using Machine Learning Algorithm" in The Eighth International Conference on Envolving Internet", 2016.

[18] "Oracle, "http://www.oracle.com/technetwork/articles/java/index-137868.html, accessed May 30, 2018

[19] Liming Cai, Jing Sha ,Wei Qian, "Study on Forensic Analysis of Physical Memory" in the proceedings of 2nd International Symposium on Computer, Communication, Control and Automation (3CA 2013), pp. 221-224, 2013.

[20] [18] Tom Michael Mitchell, "Machine Learning 1 Edition", McGraw Hill. New York, March, 1997: 112-143.

[21] Donald Michie, David J. Spiegelhalter, Charles C. Taylor,. "Machine Learning, Neural and Statistical Classification", Ellis Horwood, NJ, USA, 1994.

[22] L. Breiman, —RANDOM FORESTS, ‖ pp. 1 – 35, 1999.

[23] Ying CAO, Qi-Guang MIAO, Jia-Chen LIU, Lin GAO,. "Advance and Prospects of AdaBoost Algorithm", Acta Automatika Sinica, Vol 39, No 6 June, 2013.

[24] J. H. Friedman, —Greedy Function Approximation: A Gradient Boosting Machine, ‖ Ann. Stat., vol. 29, p. 5, 2001.

[25] "Vxheaven," http://vxheaven.org/vl.php, 2016, accessed November 2, 2016.

[26] E. Carrera, "erocarrera/pefile," https://github.com/erocarrera/pefile,2016, accessed November 2, 2016.

[27] O. T. Suryati and A. Budiono, "Impact Analysis of Malware Based on Call Network API With Heuristic Detection Method," *Int. J. Adv. Data Inf. Syst.*, vol. 1, no. 1, pp. 1–8, Apr. 2020.

[28] A. F. Muhtadi and A. Almaarif, "Analysis of Malware Impact on Network Traffic using Behavior-based Detection Technique," *Int. J. Adv. Data Inf. Syst.*, vol. 1, no. 1, pp. 17–25, Apr. 2020.