ANALISIS KINERJA METODE LIVE FORENSICS UNTUK INVESTIGASI RANDOM ACCESS MEMORY PADA SISTEM PROPRIETARY

Rusydi Umar, Anton Yudhana, M. Nur Faiz
Magister Teknik Informatika
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
Email: rusydi@mti.uad.ac.id

Abstrak - Berkembangnya teknologi mengubah dunia nyata menjadi dunia maya dalam segala bidang termasuk informasi. Informasi berkaitan erat dengan keamanan, kapasitas dan enkripsi. Kapasistas penyimpanan informasi yang besar dan teknik enkripsi informasi yang semakin kuat menyebabkan penggunaan teknik* forensic *secara tradisional tidak memadai lagi. Oleh karena itu sebagai pengganti maka digunakan teknik* live forensics *untuk melakukan investigasi. Investigasi menggunakan teknik* live forensics *memerlukan kecermatan dan ketelitian sebab data* volatile *pada RAM yang dapat hilang jika sistem mati, serta memungkinkan tertimpanya data penting yang ada pada RAM oleh aplikasi yang lainnya. Karena itu diperlukan metode live forensics yang dapat menjamin integritas dan keaslian data* volatile *tanpa menghilangkan data yang berpotensial menjadi barang bukti. Banyak* tools *untuk digunakan* live forensics *untuk analisis data.* Tools *yang dibandingan pada metode* live forensics *yaitu dari kemampuan pengunaan* memory, *waktu, jumlah langkah dan akurasi paling baik dalam melakukan* live forensics. *Hasil* file *investigasi tersebut akan menjadi acuan dalam menentukan* tools *metode* live forensics *terbaik, selain dari faktor pendukung yang lainnya.

Kata Kunci :* live forensic, tools, *RAM

I. 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]. Tindak kejahatan pada komputer berdasarkan penggunaanya dapat diketahui dari analisis *data volatile* yang terdapat pada RAM (*Random Access Memory*). Metode *Live forensics* bertujuan untuk penanganan insiden lebih cepat, integritas data lebih terjamin, teknik enkripsi lebih memungkinkan bisa dibuka dan kapasitas memori yang lebih rendah bila dibandingkan dengan metode tradisional yang membutuhkan memori besar, waktu yang lama dan memungkinkan data hilang. *Data volatile* khususnya pada RAM merupakan sistem yang menggambarkan semua kegiatan yang sedang terjadi pada sistem tersebut [2]. Penanganan *data volatile* pada RAM harus ditangani secara khusus dan hati-hati karena selain datanya dapat hilang jika sistem dimatikan, penggunaan *tools* akan meninggalkan *footprint* yang kemungkinan dapat menimpa bukti berharga yang ada ada pada memori. Penggunaan *chat* pada facebook, *username* dan *password* juga hanya tersimpan pada saat sistem berjalan. Oleh karena itu diperlukan metode *live forensics* yang dapat menjamin integritas *data volatile* tanpa menghilangkan data yang berpotensi menjadi barang bukti.

Metode forensik merupakan faktor penting yang mendukung untuk investigasi tindak kejahatan yang lebih efektif dan efisien dalam menangani sebuah kasus. Model forensik yang sering digunakan yaitu investigasi bertahap untuk menelusuri penggunaan komputer, atau dalam bahasa Inggris disebut sebagai *Phased Investigation Methodology* (PIM), berfokus pada pemilihan target investigasi dan menelusuri penggunaan sistem target. Dengan membagi investigasi forensik menjadi beberapa langkah dan menerapkannya secara bertahap, memungkinkan PIM untuk memberi reaksi yang cepat terhadap kasus [3].

Selain model PIM, terdapat model respon insiden dan forensik komputer, yang merupakan model proses baru yang diajukan untuk menginvestigasi insiden keamanan komputer. Model proses ini menggabungkan konsep respon insiden dan forensik komputer untuk meningkatkan keseluruhan proses investigasi. Model proses ini terdiri atas tiga tahap utama, yaitu praanalisis, analisis, dan pascaanalisis.

Model Proses Umum Respon Insiden dan Forensik Komputer/*Generic Computer Forensic Investigation Model* (GCFIM), merupakan model yang didapatkan dengan membandingkan beberapa model proses forensik. Model ini terdiri atas lima tahap, yaitu [4] :

- Praproses
- Akuisisi dan preservasi
- Analisis

ISBN: 978-602-19568-1-6

• Presentasi
• Pascaproses

Tahapan dalam model ini tidak harus dilakukan secara berurutan. Investigator dapat kembali ke tahap yang telah dilakukan sebelumnya untuk memperbaiki kekurangan atau memperoleh informasi baru.

Data Target Investigasi merupakan hal yang sangat penting dalam proses forensik. *Image* forensik yang telah diperoleh kemudian dianalisis untuk mengetahui data yang berpotensi menjadi barang bukti. Data-data penting tersebut digolongkan ke dalam lima kategori, yaitu: metadata sistem berkas, berkas prefetch, registry, berkas peramban web dan berkas dokumen spesifik [3].

Tabel 1. Jenis data target [3]

Jenis Data	Deskripsi
Metadata Sistem Berkas	Semua daftar berkas dalam folder
Prefetch	Jumlah penggunaan aplikasi dan waktu terakhir aplikasi berjalan
Registry	Daftar dari perintah yang dieksekusi, kata kunci pencarian, folder yang terakhir diakses, berkas yang baru dieksekusi, penggunaan aplikasi terkini
Berkas Peramban Web	URL yang dikunjungi beserta waktunya, berkas yang diunduh, kata kunci pencarian diunduh, kata kunci pencarian
Berkas dokumen spesifik	Berkas yang dienkripsi, nama berkas, dan berkas dengan ekstensi yang telah dimodifikasi.

a. Metadata Sistem Berkas

Metadata sistem berkas merupakan informasi yang terdapat pada *harddisk* dan mengandung informasi dari semua berkas [5]. Informasi yang terdapat dalam metadata diantaranya: nama berkas dan direktori, ekstensi berkas, waktu pembuatan berkas, waktu modifikasi berkas, waktu berkas diakses, ukuran berkas, lokasi berkas, dan lain-lain. Metadata dapat digunakan secara efektif dalam memilih sistem target dengan melakukan pencarian berkas atau kata kunci. Cara ini lebih efisien dibandingkan dengan menelusuri seluruh isi *disk image*.

b. Prefetch

Berkas *prefetch* isinya berkas *cache* tentang waktu *running* suatu aplikasi [6]. Berkas data dapat dibuka sebelum aplikasi berjalan. Informasi yang dapat dibaca dari berkas prefetch antara lain: nama berkas, jumlah program yang berjalan, waktu *running* terakhir, daftar berkas referensi yang dibutuhkan untuk meluncurkan program, dan lain-lain. Informasi ini memberitahu program apa saja yang dijalankan tersangka baru-baru ini dan program apa yang sering ia jalankan [7].

c. Registry

Registry berisi informasi paling banyak mengenai penggunaan komputer dan konfigurasi pengguna, aplikasi dan perangkat keras pada sistem operasi Windows. Informasi dikategorikan berdasarkan perintah yang telah dieksekusi, kata kunci pencarian, folder yang terakhir kali diakses, log aplikasi, dan lain-lain [7]. Perintah yang telah dieksekusi merupakan daftar perintah yang digunakan dengan menekan "Start + Run(R)" pada Windows. Hal ini dilakukan untuk proses investigasi penelusuran dan tujuan dari penggunaan sistem. Kata kunci pencarian menunjukkan daftar kata kunci yang digunakan pada fitur pencarian Windows. Folder yang terakhir kali diakses mengandung berkas yang diakses dengan "Open" dari tiap aplikasi. Berkas yang dieksekusi baru-baru ini menunjukkan berkas dan folder apa saja yang telah dibuka pengguna baru-baru ini. Log aplikasi memberikan *running path*, waktu eksekusi terakhir, dan jumlah *running* suatu aplikasi [7].

d. Riwayat Internet

Riwayat internet yaitu merekam jejak penggunaan internet dalam berkas log peramban web. Berkas log dari Internet Explorer adalah berkas index.dat, berkas log Firefox2 adalah history.dat, berkas log Firefox3 adalah places.sqlite, sedangkan berkas log Google Chrome terdapat pada basis data sqlite bernama "History". Peramban web tersebut memberikan informasi mengenai alamat situs yang dikunjungi beserta waktu kunjungannya. Informasi kata kunci dapat diekstrak dari URL. Dengan mengekstrak daftar pencarian, riwayat penggunaan web dapat membantu menelusuri riwayat penggunaan komputer [7].

e. Berkas Dokumen Spesifik

Berkas dokumen spesifik yaitu mengacu pada berkas-berkas dengan nama file dan ekstensinya yang telah dimodifikasi. Jika file tertentu telah dienkripsi maka akan menjadi suatu permasalahan karena investigator harus bisa memecahkan enkripsi dengan bantuan software dan analisis yang tepat karena berkas ini dapat menjadi bukti yang sangat penting [7].

Sistem operasi *proprietary* lebih dikenal dengan sistem operasi yang berbayar. Sistem operasi ini hanya dikembangkan oleh pengembang yang mengetahui source code, hal ini menjadikan tindak kejahatan semakin besar karena banyak perusahaan menggunakan sistem operasi ini. Salah satu produsennya yaitu Microsoft. Pada April 2015, Microsoft resmi memperkenalkan produk

ISBN: 978-602-19568-1-6

terbarunya yaitu windows 10, sebagai pembaharuan dari windows 8.1. Microsoft sendiri telah merilis 17 sistem operasi berbasis desktop dan 19 sistem operasi untuk bisnis dan fokus pada NT kernel [8].

Penelitian [9] membandingkan dari segi forensik antara windows 7 dan windows 8 dengan tools FTK dan EnCase Microsoft account. Hasilnya windows 7 lebih rentan dari dari windows 8 karena windows 8 sudah lebih baik teknik enkripsi dan lebih aman. Untuk kemananan account, windows 7 menggunakan kunci sebanyak 8 sedangkan windows 8 menggunakan kunci sebanyak 30 dengan menggunakan tools FTK.

Penelitian [10] membandingkan tools metode *live forensics* yang memiliki kemampuan terbaik dalam segi penggunaan memory pada windows XP, akurasinya, waktunya dan jumlah langkah yang dilakukan dalam menganalisis melakukan *live forensics*. Hasil yang diperoleh yaitu metode eksternal dengan ManTech sebagai tools akuisisi memory serta Volatility sebagai tools analisis dengan penggunaan virtual memory sebesar 24,492 KB, working sets 1,388 KB, melakukan penulisan pada registry sebanyak 8 key dengan akurasi 75% lalu waktu total yang digunakan 311 dan total langkah yang digunakan 22

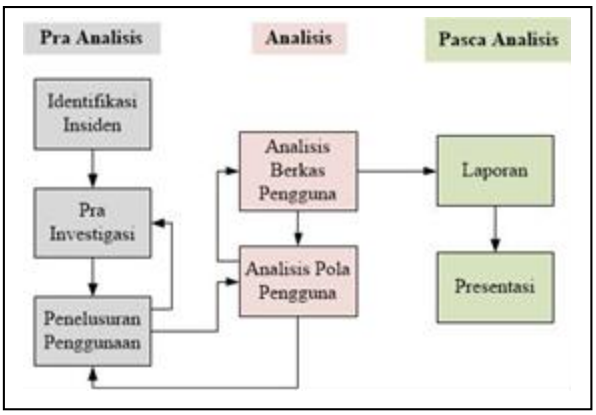
Penelitian [11] menghasilkan identifikasi yang dilakukan untuk menganalisa tools forensics, tekniknya dan cakupan serta paltformnya. Setiap tools harus disesuaikan dengan kasusnya. Dibutuhkan metodologi serta algoritma yang efektif dan efisien.

Penelitian [12] menyebutkan Banyak tools untuk forensik yang tersedia, untuk *hardware* dibutuhkan untuk hati-hati membuka kunci pokoknya, untuk tools *softwar*enya lebih akurat jika *live* dari sistem. Sangat penting untuk menemukan informasi berdasarkan aktivitas yang berjalan pada sistem dan menganalisisnya. Pada penelitian ini analisis memory RAM pada *time system*, *logged on user*, *open filesNetwork information*, *process information, process-to-port mapping, process memory, service/driver information, command history*. Penelitian ini menggunakan 6 tools yaitu Tribble, firewire untuk hardware dan FTK manager, DumpIt, Redline, Microsoft crash dump pada softwarenya.

Penelitian [13] menyimpulkan bahwa analisis tingkat keefektifan tools untuk forensik data pada *static* dan *live* membutuhkan isi memori yang konsisten secara spesifik *tools* yang digunakan untuk forensik dari nama *tools*, sistem operasinya, deskripsinya dan *static* atau *live*. Hasil penelitian melibatkan 38 *tools* yang dibandingkan dengan fungsinya serta menyesuaikan *tools* dan kasusnya. *Tools* yang berjalan pada *live* dan *static* memungkinkan struktur data akan tertimpa dan menjadi inkonsistan.

II. METODE PENELITIAN

Metode yang diajukan dalam penelitian ini merupakan integrasi dari model proses umum respon insiden dan komputer forensik, model umum investigasi forensik komputer dan metodologi investigasi bertahap untuk menelusuri penggunaan komputer. Model proses ini bertujuan untuk memilih sistem dan menganalisis bukti-buktinya secara efisien. Model ini terdiri atas tiga tahapan utama yaitu tahap pra Analisis, tahap Analisis, dan tahap pasca Analisis, seperti terlihat pada gambar 1.



Gambar 1. Ide Model Forensik yang diajukan

A. Tahap Pra Analisis

Tahap pertama dari model proses forensik yang diusulkan adalah tahap pra analisis. Tahap ini terdiri atas tiga langkah, yaitu identifikasi insiden, pra investigasi, dan penelusuran penggunaan.

a) Identifikasi Insiden

Langkah pertama pada tahap pra analisis adalah mengidentifikasi insiden/kasus. Penyidik harus dapat mengidentifikasi kasus dan meminimalisir hal-hal yang memungkinkan terjadi atau resikonya. Penyidik harus mengetahui dan memastikan waktu insiden terjadi, lokasi kasus, sistem apa yang harus diinvestigasi berdasarkan jenis kasus. Tahap ini dapat memberikan cara yang efektif dalam menanggapi suatu insiden/kasus dengan mempersingkat waktu keseluruhan investigasi.

b) Pra investigasi

Pada langkah ini, *live data* dan metadata sistem berkas diperoleh dan dianalisis. *Live data* terdapat di dalam *Random Access Memory* (RAM). Untuk mengumpulkan informasi *live data*, sistem target tentunya masih aktif. *Live data* memberikan informasi penting dari sistem target seperti "*Snap shot*" pada waktu respon insiden awal. Dengan adanya informasi penggunaan sistem dalam *live data*, informasi mengenai sistem dasar seperti nama komputer, pengguna yang baru *log-on*, waktu *booting*

ISBN: 978-602-19568-1-6

dan *uptime* pun dapat diidentifikasi. Penyidik dapat menginvestigasi keberadaan berkas-berkas yang berhubungan dengan kasus melalui pencarian atau *filtering* kata kunci. Dengan menggunakan metadata sistem berkas, investigasi dengan teknik ini tentu lebih cepat daripada investigasi keseluruhan *disk image*.

c) Penelusuran Penggunaan Komputer

Data target yang diperoleh pada tahap ini adalah *registry*, *prefetch* dan aktivitas internet seperti berkas riwayat web, penggunaan *messenger*, dan arsip surel. Semua data tersebut dianalisis untuk menentukan apakah tersangka melakukan suatu kasus atau tidak. *Registry* dapat memberikan informasi seperti perintah-perintah yang telah dieksekusi, kata kunci pencarian, folder yang terakhir diakses, berkas yang terakhir dieksekusi, log aplikasi, dan lain-lain. Penyidik dapat melakukan analisis *registry* untuk mengekstrak berkas dan data yang berkaitan. Berkas *prefetch* dapat digunakan untuk menentukan aplikasi mana yang sering digunakan akhir-akhir ini. Berkas peramban web merupakan alat bantu yang ampuh untuk menelusuri penggunaan internet tersangka. Berkas dari temporary bahkan dapat menunjukkan isi dari surel.

B. Tahap Analisis

Setelah semua langkah pada tahap pra analisis selesai dilakukan, tahap selanjutnya tahap analisis. Pada tahap ini dilakukan dua macam analisis, yaitu analisis pola penggunaan komputer dan analisis berkas pengguna.

a) Analisis Pola Penggunaan Komputer

Langkah pertama pada tahap analisis adalah menganalisis pola penggunaan komputer. Dari hasil analisis data yang telah dilakukan pada tahap praanalisis, penyidik dapat menganalisis pola penggunaan komputer tersangka. Analisis pola penggunaan komputer dapat memberikan petunjuk tentang kapan tersangka sering menggunakan komputer dan jenis berkas atau aplikasi apa saja yang digunakan. Log penggunaan berkas dan aplikasi dapat digunakan untuk menelusuri kapan berkas dan aplikasi tersebut digunakan. Secara khusus, MAC *time* dapat digunakan untuk memperkirakan pola penggunaan aplikasi. Berkas peramban web dapat digunakan untuk menginvestigasi kapan tersangka mengakses suatu situs web.

b) Analisis Berkas Pengguna

Pada tahap ini, berkas-berkas dan data yang relevan diambil. Selain itu, berkas-berkas bukti diinvestigasi berdasarkan hasil analisis data dan pemahaman kasus secara keseluruhan. Pada tahap ini secara khusus lebih berfokus pada investigasi mengenai apakah tersangka menghapus, mengenkripsi, atau memodifikasi nama/ekstensi berkas untuk merusak bukti.

C. Tahap Pasca analisis

Tahap terakhir dari model proses yang diajukan adalah tahap pasca analisis. Tahap ini terdiri atas dua langkah, yaitu pembuatan laporan dan presentasi. Laporan tersebut berisi rincian insiden dan dokumentasi dari semua langkah yang dilakukan pada tahap pra analisis dan tahap analisis. Presentasi mengenai apa saja yang diperoleh selama hasil investigasi dan menjelaskannya untuk bukti di pengadilan.

III. HASIL DAN PEMBAHASAN

Berdasarkan peneltian yang telah dilakukan pada pendahuluan maka dapat disimpulkan belum ada penelitian tentang *live forensics* pada system operasi *proprietary* terutama pada sistem operasi terbaru. Investigasi pada *data volatile* pada sistem yang berjalan RAM dapat mengetahui log dari aktivitas pengguna. Data yang memungkinkan menjadi barang bukti bisa didapat dari metadata sistem berkas, berkas *prefetch*, *registry*, berkas peramban web dan berkas dokumen spesifik. Penelitian ini diharapkan dapat merekomendasikan *tools* yang sesuai dengan kasusnya dan berjalan pada sistem operasi *proprietary*. Kasus diskenario dengan kejahatan yang sering muncul dan memanfaatkan *tools freeware*. Kinerja dari *tools* akan dihitung akurasi, waktu, penggunaan memori serta jumlah langkahnya dan merekomendasikan kepada investigator tools yang sesuai dengan kasus yang terjadi.

IV. KESIMPULAN

Berdasarkan penelitian terdahulu yang telah dipaparkan, maka penelitian akan dilaksanakan dengan metode pendekatan baru. Harapan dari penelitian ini yaitu merekomendasikan kepada investigator tools terbaik pada sistem operasi *proprietary*. Memanfaatkan tools *freeware* dan skenario kasus yang sering terjadi. Membandingkan kinerja tools *live forensics* dari segi akurasi, waktu, penggunaan memori serta jumlah langkahnya.

DAFTAR PUSTAKA

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

[2] Frank Adestein. (2006). "Live Forensics – Diagnosing Your System Without Killing It First ". Communication of The ACM February, Vol 49, Hal 63-66.

[3]. Seungbong Lee, Jewan Bang, Kyungsoo Lim, Jongsung Kim, Sangijin Lee. (2009). "A Stepwise Forensic Methodology for Tracing Computer Usage". The Fifth International Joint Conference on INC, IMS and IDC Vol 246, Hal 1852-1857.

[4] Yusoff. Yunus., Ismail. Roslan., Hassan. Zainuddin. (2011). "Common Phases of Computer Forensics Investigation Models".

ISBN: 978-602-19568-1-6

International Journal of Computer Science & Information Technology (IJCSIT), Volume 3, Hal 17-31.

[5] Brian Carrier. (2005) "File System Forensic Analysis". Indiana : Addison Wesly Professional.

[6] Harlan Carvey. (2005). "Windows Forensic and Incident Recovery". Burlington: Addison Wesley.

[7] Microsoft Corporation "Windows Registry, Information for Advanced User", 2008

[8]. Mike Hasley. (2015). "Windows 10 Primer: What to Expect from Microsoft's New Operating System". New York : Apress.

[9].Peter Wilson. (2013). "A Forensic Comparison : Windows 7 and Windows 8". New York: Rochester Institute of Technology

[10].Haryo Bintoro, Niken Dwi Cahyani, Niken, Endro Ariyanto. (2012). "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory pada Sistem Operasi Microsoft Windows XP". Bandung : Universitas Telkom

[11]. Bashir. Muhammad Shamraiz Bashir, M.N.A. Khan. (2013). "Triage in Live Digital Forensic Analysis". The International Journal of Forensic Computer Science, Volume 1, Halaman 35-44.

[12]. Jyoti Belsare, Aditya Sinha. (2015). "Live Memory Forensics Analysis". International Journal on Recent and Innovation Trends in Computing and Communication, Volume 3, Halaman 2775-2778.

[13] Mamoona Rafique, M.N.A.Khan. (2013). "Exploring Static and Live Digital Forensics : Methods, Practices and Tools" International Journal of Scientific & Engineering Research, Volume 4, Halaman 1048-1056.

ISBN: 978-602-19568-1-6