FORENSIK DIGITAL RANDOM ACCESS MEMORY PADA SISTEM OPERASI LINUX MENGGUNAKAN METODE DUMPMEMORY

DIGITAL FORENSIC RANDOM ACCESS MEMORY ON LINUX OPERATING SYSTEM USING DUMPMEMORY METHOD

Rivan Hikmawan[1], Periyadi,S.T., M.T.[2], Giva Andriana Mutiara,S.T., M.T.[3]
[1,2,3]Prodi D3 Teknik Komputer, Fakultas Ilmu Terapan, Universitas Telkom
[1]rivanhikmawan@gmail.com, [2]periyadi2k9@gmail.com, [3]giva.andriana@tass.telkomuniversity.ac.id

Abstrak

Kemajuan teknologi saat ini bisa dimanfaatkan untuk melacak sebuah aktifitas pelaku kejahatan dalam melakukan aksi kejahatan internet, seperti: pencurian, penggelapan, pencucian uangan dan lain sebagainya. Bukti digital dari komputer sulit dibedakan antara asli mupun salinan, karena berdasarkan sifat alaminya, data yang ada dalam komputer sangat mudah dimodifikasi. Sebuah proses transaksi elektronik akan disimpan pada media penyimpanan yang digunakan komputer dengan salah satu media penyimpanan pada *Random Access Memory* (RAM).
Forensik digital adalah penggunaan metode ilmiah yang berasal dan terbukti menuju pelestarian, koleksi, validasi, identifikasi, analisis, interpretasi, dokumentasi dan presentasi bukti digital yang berasal dari sumber-sumber digital untuk tujuan memfasilitasi atau melanjutkan rekonstruksi peristiwa ditemukan pidana, atau membantu untuk mengantisipasi tindakan yang tidak sah terbukti mengganggu operasi yang direncanakan.
Forensik memory merupakan salah satu teknik forensik yang digunakan untuk mendapatkan sebuah data atas inseden penyerangan terhadap suatu pengguna. Dalam digital forensik memiliki dua teknik forensik yang digunakan untuk keperluan investigasi, yaitu: Teknik forensik tradisional dan Teknik live forensik.
Proses *dumpmemory* dilakukan dengan bantuan perangkat lunak tambahan untuk *capture memory* pada sistem operasi linux menggunakan LiME dan melakukan analilis memory menggunakan *volatility*. Hasil dari *capture memory* berupa informasi jenis file backdoor, script dan waktu penyerangan dalam file image dari beberapa skenario pengujian yang menghasilkan bukti secara sah dan bisa dipertanggung jawabkan.
Kata Kunci : RAM, forensik digital, forensik memory, dumpmemory, analisis memory

Abstract

Current technological advances can be used to track a criminal activity in Internet crime, such as theft, embezzlement, money laundering and so on. Digital evidence from computers is difficult to distinguish between original and copy, because based on their nature, the data in the computer is very easy to modify. An electronic transaction process will be stored on storage media used by a computer with one of the storage media in Random Access Memory (RAM).
Digital forensics is the use of scientific methods originating and proven towards conservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence originating from digital sources for the purpose of facilitating or continuing reconstruction of criminal incidents, or assisting in anticipating action The unauthorized proved to disrupt the planned operation.
Forensic memory is one of the forensic techniques used to obtain a data on the attack incidents against a user. In digital forensics has two forensic techniques used for investigation purposes, namely: traditional forensic techniques and forensic live techniques.
The dumpmemory process is done with the help of additional software for capture memory on linux operating system using LiME and performs memory analytics using volatility. The results of capture memory in the form of backdoor file type information, script and time of attack in the image file of some test scenarios that produce the evidence legally and can be accounted for.
Keyword : Blackbox, Flight Data Recorder (FDR), Data Compression.

1. Pendahuluan

Kemajuan teknologi saat ini bisa dimanfaatkan untuk melacak sebuah aktifitas pelaku kejahatan dalam melakukan aksi kejahatan internet, seperti: pencurian, penggelapan, pencucian uangan dan lain sebagainya. Bukti

digital dari komputer sulit dibedakan antara asli mupun salinan, karena berdasarkan sifat alaminya, data yang ada dalam komputer sangat mudah dimodifikasi[1]. Seiring berjalannya waktu proses penindak lanjutan kejahatan digital sebagai barang bukti secara sah dalam sebuah pengadilan umum, maka diterbirkan UU ITE untuk mengatur transfer informasi elektronik sesuai dengan etika transaksi informasi elektronik. Sehingga UU No. 11 tahun 2008 diharapkan tidak ada pihak yang merasa dirugikan atas transaksi informasi elektronik. Sebuah proses transaksi elektronik akan disimpan pada media penyimpanan yang digunakan komputer dengan salah satu media penyimpanan pada *Random Access Memory* (RAM).

Random Access Memory (RAM) ialah komponen yang penting dalam sistem komputer, berperan sebagai ruang penyimpanan yang bersifat volatile. Kapasitas *main memory* ini sangat berguna untuk proses forensik, karena *Random Access Memory* ini menyimpan seluruh aktifitas yang terjadi saat komputer sedang digunakan oleh pengguna[2].

Forensik memori merupakan proses investigasi untuk menganalisa data-data *volatile* yang terdapat pada *Random Access Memory* sebuah komputer sebagai bukti digital yang akurat dan dapat dipertanggung jawabkan. Cara kerja digital forensik ialah mengembalikan, mengumpulkan, memeriksa dan menyimpan bukti informasi yang secara magnetis tersimpan pada komputer[3][4].

Penangan forensik main memory pada *Random Access Memory* harus sangat berhati-hati dan bersabar karena jika sistem yang sedang berjalan mati maka data yang terdapat di dalam *main memory* akan hilang. Oleh karena itu hasil dari forensik memori berupa beberapa log aktifitas dan riwayat penyerang dalam sistem operasi yang diretas untuk mengambil data-data[7].

2. Dasar Teori

2.1 FORENSIK DIGITAL

Forensik digital adalah penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti informasi yang secara magnetis tersimpan pada komputer atau media penyimpanan digital sebagai alat bukti dalam mengungkap kasus kejahatan yang bisa dipertanggung jawabkan secara hukum[1][3][4][8][10].

2.2 *RANDOM ACCESS MEMORY* (RAM)

Random Access Memory (RAM) adalah memori utama sebuah komputer yang bersifat *volatile* untuk media penyimpanan sementara pada saat komputer dijalankan dan dapat diakses secara acak atau randomRAM digunakan untuk penyimpanan data sementara dan mengeluarkan data yang diminta oleh processor serta alur data yang tersimpan serta keluarkan secara dinamis serta sebuah tipe penyimpanan komputer yang isinya dapat diakses dalam waktu yang tetap tidak memperdulikan letak data tersebut dalam memori. Ini berlawanan dengan *alat memori urut*, seperti tape magnetik, disk dan drum. Gerakan mekanikal dari media penyimpanan memaksa komputer untuk mengakses data secara berurutan.

Dalam memproses sebuah data yang masuk dalam inputan user, beberapa bagian RAM saling membantu proses pengolahan data tersebut. Berikut bagian utama RAM yang mengelola data dari inputan hinga output:

1. Input storage, digunakan untuk menampung input yang dimasukkan melalui alat input.
2. Penyimpanan program, digunakan untuk menyimpan semua instruksi-instruksi program yang akan diakses.
3. *Working storage*, digunakan untuk menyimpan data yang akan diolah dan hasil pengolahan.
4. *Output storage*, digunakan untuk menampung hasil akhir dari pengolahan data yang akan ditampilkan ke alat *output*.

2.3 SISTEM OPERASI

Sistem Operasi (*Operating System* : *OS*) adalah komponen pengolah peranti lunak dasar (*essential component*) tersistem sebagai pengelola sumber daya perangkat keras komputer, dan menyediakan layanan umum untuk aplikasi perangkat lunak. Sistem operasi adalah jenis yang paling penting dari perangkat lunak sistem dalam sistem komputer. Tanpa sistem operasi, pengguna tidak dapat menjalankan program aplikasi pada komputer mereka, kecuali program booting[2][5].

Sistem operasi mempunyai penjadwalan yang sistematis mencakup perhitungan penggunaan memori, pemrosesan data, penyimpanan data, dan sumber daya lainnya. Secara umum sistem operasi dibagi menjadi beberapa bagian, antara lain:

1. Booting, meletakan karnel kedalam memori.
2. Kernel, bagian inti dari sebuah sistem operasi.
3. Command Interpreter atau shell, membaca input dari pengguna.

4. Pustaka-pustaka, menyediakan kumpulan fungsi dasar dan standar yang dapat dipanggil oleh perangkat lunak lain

Untuk fungsi-fungsi perangkat keras seperti sebagai masukan dan keluaran dan alokasi memori, sistem operasi bertindak sebagai perantara antara program aplikasi dan perangkat keras computer, meskipun kode aplikasi biasanya dieksekusi langsung oleh perangkat keras dan seringkali akan menghubungi system operasi atau terputus oleh itu. Sistem operasi yang ditemukan pada hampir semua perangkat yang berisi computer dari ponsel dan konsol permainan video untuk superkomputer dan server web[2][5].

2.4 DUMPMEMORY

Forensik memory merupakan salah satu teknik forensik yang digunakan untuk mendapatkan sebuah data penyerangan terhadap suatu pengguna. Dalam digital forensik memiliki dua teknik forensik yang digunakan untuk keperluan investigasi, yaitu: Teknik forensik tradisional dan Teknik live forensik[6][7].

Proses dumpmemory pada sebuah sistem operasi target pengguna haruslah sistem yang sudah terindikasi diserang oleh penyerang dengan menyisipkan sebuah file backdoor untuk mengakses segala sistem, direktori dan dokumen dalam sistem operasi pengguna. Setelah sistem operasi pengguna yang telah diserang dan penyerang meninggalkan sebuah file backdoor yang disisipkan, lakukan proses dumpmemory pada RAM korban untuk melihat aktifitas yang dilakukan oleh penyerang.

Tenik forensik tradisional atau teknik offline merupakan teknik yang sering digunakan untuk investigasi dengan mengharuskan investigator mematikan sistem korban, hal ini bertujuan untuk antisipasi adanya proses berbahaya yang dapat beresiko menghapus data untuk keperluan investigasi.

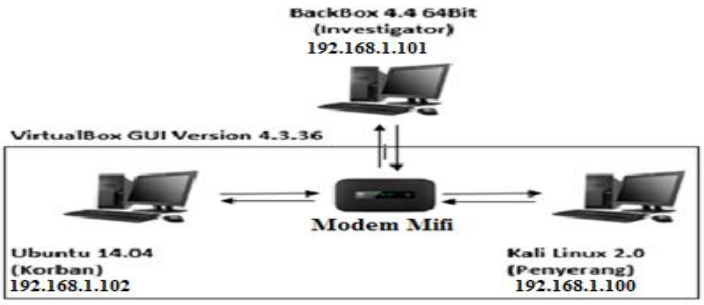
Teknik live forensik ialah teknik forensik yang mengharuskan sistem komputer target tidak boleh mati (*shutdown*) untuk proses investigasi penyerangan, dengan melakukan teknik live forensik pada sebuah data volatile yang ada dalam sebuah sistem komputer[10][14].

3. Pembahasan

Pada penelitian ini, akan membahas mengenai gambaran umum pengujian sistem yang telah dibuat. Dengan menggunakan dua buah komputer yang telah dipasang sistem operasi sebagai penyerang dan investigator, modem Mi-Fi sebagai trasmisi internet, perancangan alur penyerangan untuk proses menyerang target, perancangan alur investigasi untuk proses investigasi, serta membahas parameter yang digunakan untuk melakukan dumpmemory.

3.1 Gambaran Umum Sistem

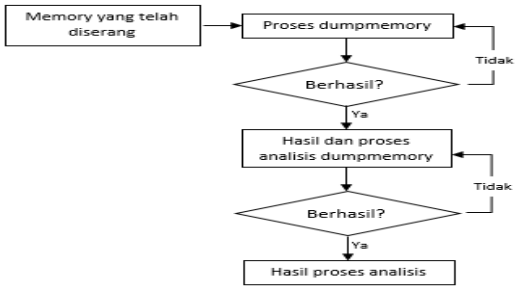
Untuk sistem yang dirancang memiliki gambaran fisik seperti Gambar 3-1.



Gambar 3-1: Gambaran Umum Sistem

Pada Gambar 3-1 menunjukan gambaran umum sebuah proses yang berlangsung dengan menggunakan dua buah laptop/komputer menggunakan media transmisi internet modem Mi-Fi. Dua buah laptop sudah terpasang sistem operasi Kali linux sebagai penyerang dan BackBox linux sebagai investigator serta Ubuntu linux yang terpasang secara virtual dalam sistem operasi investigator. Teknik yang digunakan dalam pengujian ini menggunakan metode *FTP Attack, ilegal access* dan *session hijacking*. Kali linux dipasang untuk menyerang sistem korban yang terpasang dalam virtual komputer investigator dan investigator menganalisa hasil serangan yang dilakukan oleh penyerang dengan menemukan sebuah file backdoor dan jenis script yang digunakan untuk penyerangan.

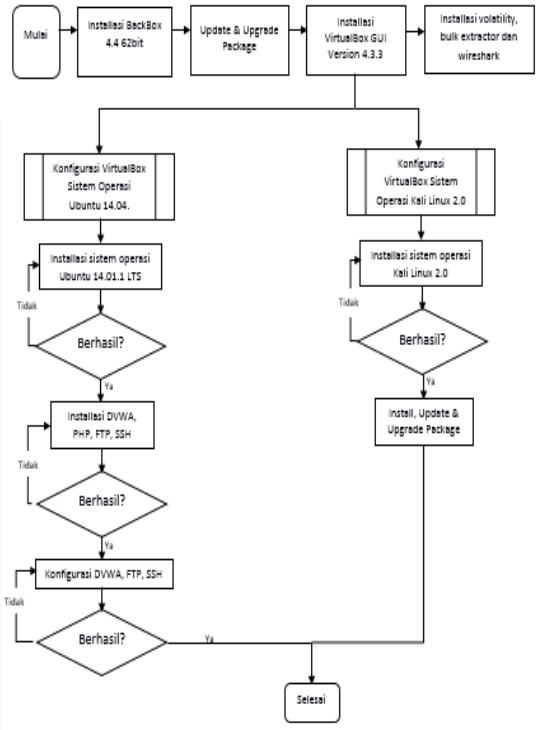
3.2. Diagram Alur Dumpmemory



Gambar 3-2: Diagram Alur Dumpmemory

Pada Gambar 3-2 menunjukkan proses alur dumpmemory yang dilakukan dalam sebuah *Random Access Memory* pada sistem operasi yang telah diserang. Proses dumpmemory ini dilakukan dalam kondisi komputer user yang diserang keadaan aktif (on). Hasil dari dumpmemory akan dianalisis untuk mendapatkan informasi tentang penyerangan.

3.3. Diagram Alur Implementasi Sistem

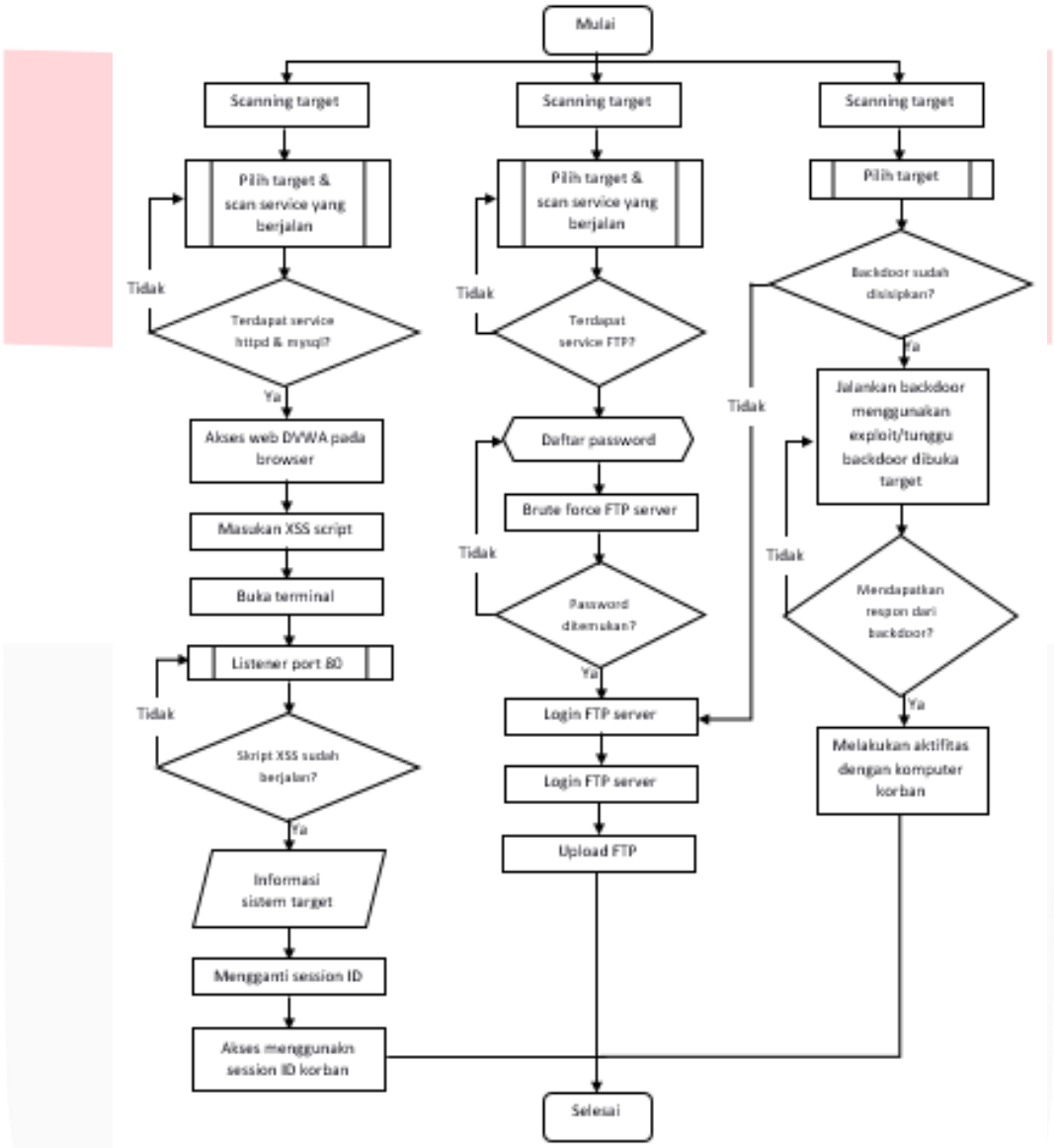


Gambar 3-3: Diagram Alur Implementasi Sistem

Pada Gambar 3-2 menunjukkan proses implementasi yang dilakukan dalam mengerjakan proyek dengan menggunakan sistem operasi BackBox linux sebagai investigator dan Ubuntu linux sebagai target yang dipasang dalam mesin virtual. Mesin virtual dijalankan dalam sistem operasi investigator untuk mendungkung proses pemasangan sistem operasi target, dalam pemasangan sistem operasi target terdapat fitur-fitur yang dipasang, seperti: DVWA, PHP, SSH, FTP dan LiME. Fitur ini dipasang dalam sistem operasi target untuk membuka celah keamanan dalam target dan menjadi jalan untuk penyerang dapat eksploitasi sistem korban.

Selain dipasang sistem operasi target dalam virtual, investigator juga memasang fitung pendukung untuk analisis hasil dumpmemory, seperti: Volatility, Bulk_extraktor dan wireshark. Volatility berfungsi untuk mencari image dari hasil dumpmemory dengan menampilkan beberapa image hasil dumpmemory. Bulk_extraktor berfungsi sebagai esktraktor dari hasil dumpmemory untuk mendapatkan file data base aktifitas log jaringan penyerangan. Wireshark berfungsi untuk analisis jaringan dari file data base yang telah diekstrak oleh bulk_extraktor.

3.4. Diagram Alur Pengujian Sistem

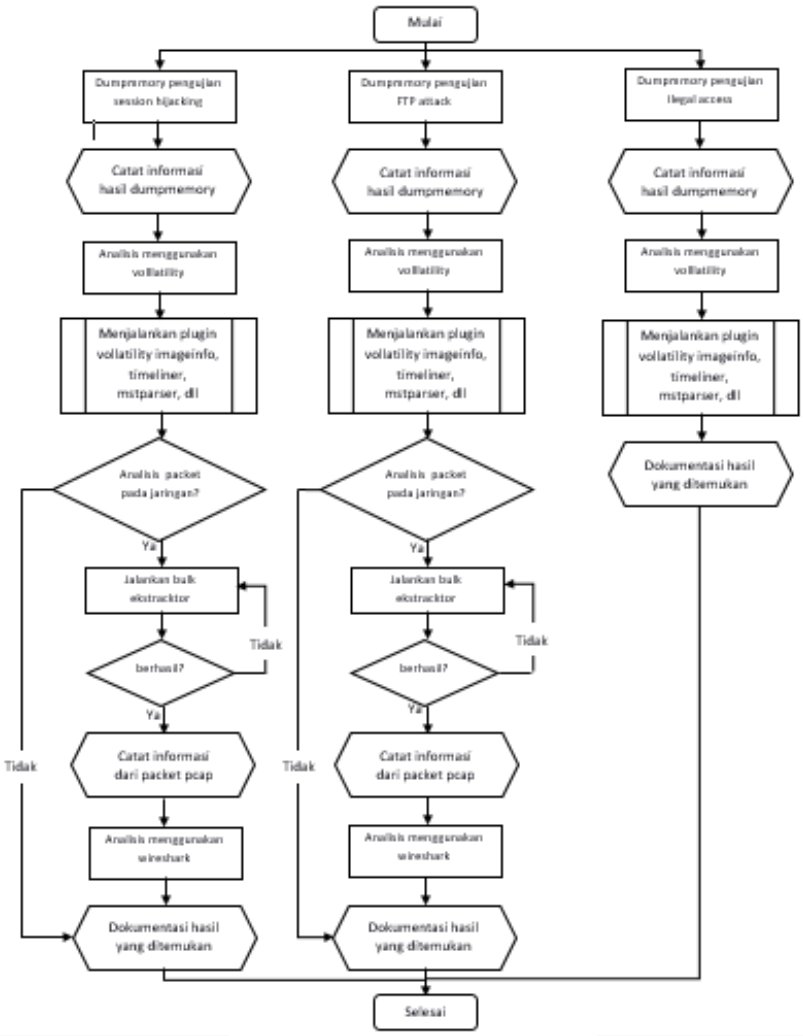


Gambar 3-4: Diagram Alur Pengujian Sistem

Pada Gambar 3-4 menunjukkan proses alur pengujian dengan menggunakan 3 cara pengujian, yaitu FTP Attack, Session Hijacking dan Illegall Access. Tahap alur pengerjaan dari pengujian ialah:

1. Pengujian FTP Attack: scan port jaringan yang aktif dengan memilih target port yang terbuka, cari informasi *password* target list *password* yang telah dibuat, siapkan backdoor yang telah dibuat, masuk dengan port yang terbuka, login *username* dan *password* yang telah didapatkan, sisipkan backdoor kepada target dan buat file akses untuk remote target.
2. Pengujian Session Hijacking: buka browser untuk akses dvwa, login *username* dan *password* secara default, masukan nama dan jenis script pada XSS Script, reload ulang browser, dan salin SSID yang telah didapatkan.
3. Pengujian Illegall Access: Pastikan file backdoor telah disisipkan, jalankan backdoor untuk mendapatkan hak ases target, buat folder pada direktori target dan buat hak ases untuk mengendalikan target.

3.5. Diagram Alur Investigasi Sistem



Gambar 3-5: Diagram Alur Investigasi Sistem

Pada Gambar 3-5 menunjukkan proses alur investigasi dengan pengujian FTP Attack, Session Hijacking dan Illegall Access. Tahap alur investigasi dari pengujian ialah:

1. Investigasi FTP Attack: catat hasil dari dumpmemory, analisis menggunakan volatility, jalankan plugin volatility (timeliner, image info dan msfarser), catat hasil image, jalankan bulk_extractor, jalankan wireshark dan catat hasil log jaringan.
2. Investigasi Session Hijacking: catat hasil dari dumpmemory, analisis menggunakan volatility, jalankan plugin volatility (timeliner, image info dan msfarser), catat hasil image, jalankan bulk_extractor, jalankan wireshark dan catat hasil script jaringan .
3. Pengujian Illegall Access: catat hasil dari dumpmemory, analisis menggunakan volatility, jalankan plugin volatility (timeliner, image info dan msfarser), dan catat hasil image.

4. Pengujian

Pada tahap ini, target yang diserang adalah komputer yang telah dimasukan sebuah backdoor melalui teknik ftp attack dan script yang dimasukan melalui teknik session hijacking. Sebagai contoh, format file backdoor shell(.sh) akan didump dengan menggunakan LiME menjadi format memory (.mem), dan mendapatkan jumlah size memory yang telah didump serta menemukan md5 dari hasil dumpmemory. Data hasil dumpmemory tersebut memiliki ukuran data sebesar 5,12MB. Pengujian dilakukan dengan menggunakan teknik penyerangan FTP Attack, Session Hijacking dan Illegal Access.

4.1 Pengujian Dumpmemory FTP Attack

Tabel 4-1: Hasil Dumpmemory FTP Attack

File Name	Mencoba.mem
File Size	512,3 MB
File Address	/home/target/ mencoba.mem
Format	Lime
MD5 sum	40f2e9a39972a9fcbbc83ade83744842
SHA1	2ee41c0158792f71e2964adaa9a1816f3ce16284

Pada Tabel 4-1 menunjukkan hasil dumpmemory target yang telah terindikasi diserang oleh penyerang dengan menggunakan teknik FTP Attack. Ketika memory yang telah diserang dan proses dumpmemory sudah dilakukan, ukuran data, format, file address dan md5 sum.

4.2 Pengujian Dumpmeory Illegal Access

Tabel 4-2: Hasil Dumpmemory Illegal Access

File Name	Mencoba.mem
File Size	512,3 MB
File Address	/home/target/ mencoba.mem
Format	Lime
MD5 sum	40f2e9a39972a9fcbbc83ade83744842
SHA1	2ee41c0158792f71e2964adaa9a1816f3ce16284

Pada Tabel 4-2 menunjukkan hasil dumpmemory target yang telah terindikasi diserang oleh penyerang dengan menggunakan teknik illegal access. Ketika memory yang telah diserang dan proses dumpmemory sudah dilakukan, ukuran data, format, file address dan md5 sama dengan teknik sebelumnya.

4.3 Pengujian Dumpmemory Session Hijacking

Tabel 4-3: Hasil Dumpmemory Session Hijacking

File Name	Mencoba.mem
File Size	512,3 MB
File Address	/home/target/ mencoba.mem
Format	Lime
MD5 sum	40f2e9a39972a9fcbbc83ade83744842
SHA1	2ee41c0158792f71e2964adaa9a1816f3ce16284

Pada Tabel 4-3 menunjukkan hasil dumpmemory target yang telah terindikasi diserang oleh penyerang dengan menggunakan teknik session hijacking. Ketika memory yang telah diserang dan proses dumpmemory sudah dilakukan, ukuran data, format, file address dan md5 sama dengan teknik sebelumnya.

4.5 Analisa Hasil Pengujian

4.5.1 Hasil Analisa FTP Attack

Tabel 4-4: Hasil Analisa FTP Attack

IP Address	192.168.1.102
Celah Keamanan	FTP Server
Port	21
Jenis file	ReadMe.sh
Metode	Brute Force

Sistem Operasi	-
Waktu	-

Pada Tabel 4-4 dapat diketahui informasi hasil analisis pada dumpmemory dengan pengujian FTP Attack. Dilihat informasi tentang Ip Address, celah keamanan, port, jesnis file, dan metode yang digunakan penyerang untuk menyerang korban. Untuk mendapatkan jenis sistem operasi dan waktu penyerangan belum dapat diketahui dari hasil dempmory ini pada pengujian FTP Attack.

4.5.2 Hasil Analisa Session Hijacking

Tabel 4-5: Hasil Analisa Session Hijacking

IP Address	192.168.1.102
Jenis Script	<script>alert(document.cookie)</script>
Metode	DVWA, Security = Low
Sistem Operasi	-
Waktu	-

Pada Tabel 4-5 dapat diketahui informasi hasil analisis pada dumpmemory dengan pengujian Session Hijacking. Dilihat informasi tentang Ip Address, jenis script, dan metode yang digunakan penyerang untuk menyerang korban. Untuk mendapatkan jenis sistem operasi dan waktu penyerangan belum dapat diketahui dari hasil dempmory ini pada pengujian Session Hijacking.

4.5.3 Hasil Analisa Illegall Access

Tabel 4-6: Hasil Analisa Illegall Access

IP Address	192.168.1.102
Jenis Script	<script>alert(document.cookie)</script>
Metode	DVWA, Security = Low
Sistem Operasi	-
Waktu	-

Pada Tabel 4-6 dapat diketahui informasi hasil analisis pada dumpmemory dengan pengujian Illegall Access. Dilihat informasi tentang Ip Address, jenis script, dan metode yang digunakan penyerang untuk menyerang korban. Untuk mendapatkan jenis sistem operasi dan waktu penyerangan belum dapat diketahui dari hasil dempmory ini pada pengujian Illegal Access.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil pengujian yang telah dilakukan dapat disimpulkan bahwa:

1. Menggunakan cara forensik memory dengan menggunakan metode dumpmemory dengan akusisi pada RAM dari hasil memory yang telah diserang oleh penyerang.
2. Hasil belum mendapatkan jenis sistem operasi yang digunakan oleh penyerang, hanya diperoleh berupa informasi MD5SUM, jenis file, celah keamanan, jenis script. IP Address dan file size dokumen backdoor dari hasil dumpmemory.

5.2 Saran

Adapun beberapa saran untuk pengembangan selanjutnya adalah :

1. Sistem operasi korban dapat menggunakan sistem operasi Android dan Mac OS.
2. Analisis dapat dilakukan dengan tools lain untuk dapat mengetahui image dari penyerang.
3. Dapat dilanjutkan dengan menggunakan file hasil dumpmemory dengan perangkat ekstraktor Android
4. Dapat menggunakan jenis file exstension backdoor lain untuk penyerangan dalam sistem operasi base linux, seperti: .sh, .deb, .py, .php, .elf.

DAFTAR PUSTAKA

[1] Q. Darren and R. C. Kim-Kwang, "Big forensic data reducation : digital forensic images and electronic evidence," in *Cluster Computing*, Volume 19, Springer Science, 2016, pp. 723-740.

[2] Mutiara. G. A and Periyadi, Sistem Komputer, Yogyakarta: Deepublish, 2013.

[3] Al-Azhar, Muhammad Nuh. Digital Forensic – Panduan Praktis Investigasi Komputer. Depok: Salemba Infotek, 2012.

[4] Sudyana, Didik. Belajar Mengenali Forensika Digital. Yogyakarta: Diandra, 2015.

[5] E. V. Haryanto and U. P. Utama, Sistem Operasi Konsep dan Teori, Yogyakarta: Andi, 2012.

[6] Seo. Jungtaek, Lee. Seokjun and Shon. Taeshik, "A Study memory dump analysis based on digital forensic tools," in *Peer-to-Peer Networking and Aplication*, Volume 8, Springer Science, pp. 694-703, 2015.

[7] Wijaya, Roni. Forensik Digital Random Access Memory Pada Sistem Operasi Komputer Menggunakan Metode Dumpmemory. Bandung: Telkom University, 2016.

[8] Jo. WooYeon, Chang. Hyunsoo and Shon. Taeshik, "Digital forensic approach for file recovery in Unix systems: Research of data recovery on Unix file system," in *Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2016.

[9] Janarthanan. Tharmini and Dr. Shahrzuad Zargari, "The Evidentiary Value of Link Files in Linux File System to Digital Forensic Investigation," in IEEE *International Conference on Computer and Information Technology (ICCIT)*, 2015.

[10] Periyadi, Mutiara. G. A and Wijaya. Roni,"Digital Forensic Random Access Memory Using Live Forensic Technique Based on Network Attacked," in *International Confrence on Information and Comunication Technology (ICoICT)*, 2017.

[11] Sofana, Iwan. Mudah Belajar Linux. Bandung: Informatika, 2010.

[12] Lessing. Marthie and Solms. Basie von," Live Forensic Acquisition as Alternative to Traditional Forensic Process," in *4th International Conference on IT Incident Management & IT Forensics(IMF)*, 2008.