BAB 2
Kajian Pustaka

2.1 Penelitian Terdahulu

Menurut (Hausknecht et al., 2015) ada data dan informasi yang bisa ditemukan dalam RAM diantaranya ialah proses, file yang terbuka dan "*penanganan registry*", file umum, informasi dalam lalu lintas jaringan, data internet, password dan kunci kriptografi, konten terdekripsi, dan lainnya. Penelitian yang selanjutnya mengenai RAM menggunakan metode *live forensics* dilakukan oleh (Yudhistira, 2018), menurutnya analisis terhadap RAM komputer pada perangkat laptop dalam penelitian tersebut dibuat sebuah simulasi dengan barang bukti beberapa laptop dengan berbagai macam sistem operasi dan dengan beberapa kondisi seperti *hibernate,* normal dan ada aktivitas. Dari hasil analisis dalam penelitian tersebut disimpulkan terdapat informasi sensitif password dan username masih tersimpan di dalam RAM dan menjadi salah satu celah terjadinya kejahatan pencurian informasi selanjutnya untuk meminimalisir kejahatan tersebut dalam penelitian tersebut memberikan saran untuk segera melakukan *shut down* pada komputernya agar jejak digital pada RAM hilang.

Selanjutnya penelitian menggunakan metode *live forensics* pada RAM dilakukan untuk analisis anti forensik di portable web browser mode private, dalam penelitian tersebut dilakukan pencarian bukti digital yang masih tersimpan pada RAM dan mencari karakteristik bukti digital seperti apa jika ditemukan sebuah kasus di mana pengguna menggunakan portable web browser mode private penelitian dilakukan oleh (Rochmadi, 2017).

Sedangkan penelitian mengenai ekstraksi pada image RAM windows 7 pernah dilakukan (Thomas et al., 2013) menurutnya pada penelitian tersebut dijelaskan mengenai metodologi untuk melakukan *listing* proses yang berjalan, Pemuatan DLL dan ekstraksi proses memori dari proses yang berjalan dan menggunakan pendekatan analisis pada KPCR (*Kernel Processor Control Region*) .

Sementara itu penelitian untuk mengetahui RAM untuk mengetahui bukti digital sosial media pada Windows 10 dilakukan oleh (Thantilage & Jeyamohan, 2017) pada penelitian itu fokus pada pengembangan *framework* untuk memori *volatility* untuk barang bukti digital pada sosial media berbasis Windows 10 *workstation.*

Di lain sisi penelitian mengenai RAM forensik dilakukan untuk deteksi serangan malware, dilakukan oleh (Podile, Gottumukkala, & Sastry Pendyala, 2015) analisis

dilakukan dengan memanfaatkan analisis pada memori komputer dengan serangan *Man In The Browser* Trojan yang dikembangkan dengan tujuan melakukan serangan ke bank dan industri finansial.

Penelitian memanfaatkan memory forensic dilakukan oleh (Wadner, 2014) melakukan penelitian terhadap analisis serangan menggunakan shell Meterpreter pada sistem Windows 7 menggunakan Metasploit *Framework*. Menganalisis mengenai karakteristik bukti digital Meterpreter dalam memori dan modul-modul setelah eksploitasi.

Tabel 2.1 Literature Review

No	Paper Utama	Fokus Bukti Digital yang dianalisis	Sistem Operasi	Teknik Serangan	Keterangan
1	Hausknecht et al., (2015)	Proses, File terbuka dan penanganan registry, file umum, informasi pada lalu lintas jaringan, data internet, password dan kunci kriptografi, konter terdekripsi, dll.	Windows	Tidak ditemukan simulasi atau skenario serangan	-
2	Yudhistira (2018)	Password, user_id, Link URL	Windows dan Linux	Tidak ditemukan simulaisi atau skenario serangan	
3	Rochmadi (2017)	Artefak anti forensik di portal web browser mode private	Windows	Tidak ditemukan simulasi atau skenario serangan	
4	Thomas, et al., (2013)	Mencari informasi dan data pada RAM melalui pendekatan	Windows	Tidak ditemukan simulasi atau	

		KPCR		skenario serangan	
5	Thantilage & Jeyamohan, (2017)	Pengembangan tools untuk mencari bukti digital media sosial berbasis windows 10 *workstation*	Windows	Tidak ditemukan simulasi atau skenario serangan	
6	Podile, Gottumukkala, & Sastry Pendyala, (2015)	Sistem logs dan registry yang dikumpulkan dari nasabah bank yang terinfeksi trojan	Windows	Man In The Browser Malware Trojan	
7	Wadner (2014)	Mencari Meterpreter pada serangan Metasploit	Windows	Metasploit Meterpreter	

Berdasarkan hasil studi pustaka dan menemukan literatur-literatur terdahulu seperti sudah diuraikan di atas maka dapat disimpulkan bahwa penelitian mengenai RAM forensik untuk investigasi serangan eksploitasi menggunakan Metasploit *Framework* masih sedikit dilakukan, meskipun ada penelitian mengenai RAM forensik untuk investigasi serangan menggunakan Metasploit *Framework* namun masih terbatas dilakukan pada sistem operasi Windows itupun masih terbatas pada Windows 7, selain itu dalam tulisan-tulisan dalam literature review tersebut masih belum ditemukan tentang studi komparatif tentang tool yang dipakai dalam proses akuisisi RAM komputer yang terkena serangan menggunakan Metasploit

Untuk itu pada penelitian ini akan dilakukan penelitian mengenai RAM forensik untuk investigasi serangan menggunakan Metasploit *Framework* pada sistem operasi Windows 8 dan Windows 10 dan untuk menambah pengetahuan juga dilakukan studi komparatif terhadap tool yang digunakan untuk akuisisi RAM komputer, dalam penelitian kali digunakan tiga tool akuisisi RAM yaitu FTK Imager, Dumpit dan Magnet Forensics

2.2 Landasan Teori

2.2.1 Sistem Komputer

Dalam bukunya yang berjudul *Komputer Forensik: Melacak Kejahatan Digital* (Sulianta, 2016) menyebutkan bahwa sistem komputer adalah sekumpulan komponen-komponen pada komputer yang saling berkaitan dan bekerja sama untuk suatu tujuan. Komponen inti dari sistem komputer umumnya mempunyai hal-hal sebagai berikut: CPU, media penyimpanan, serta perangkat tambahan lain yang berguna untuk mempermudah kemampuan komputer seperti monitor, keyboard dan mouse.

2.2.2 Sistem Operasi

Sistem operasi adalah perangkat lunak yang memiliki tugas untuk mengontrol atau manajemen perangkat keras yang bertujuan untuk memberikan fasilitas kemudahan dalam menggunakan komputer, sistem operasi memiliki kode-kode tertentu yang menyediakan layanan atau fasilitas untuk akses ke disk, pengaturan memory, antarmuka user dan lain-lain dimana kode-kode tersebut dikenal dengan sebutan kernel. Umumnya terdapat tiga sistem operasi besar yang dikenal oleh masyarakat yaitu: Keluarga Microsoft Windows, Keluarga Unix, Keluarga Mac OS. (Munif, 2013)

2.2.3 RAM (Random Access Memory)

RAM atau Random Access Memory adalah bagian dari sebuah komputer yang mempunyai peranan penting di mana dalam RAM terdapat informasi dan data selama komputer dihidupkan dan sifatnya volatile karena data atau informasi akan hilang jika listrik mati (Sulianta, 2016).

2.2.4 Komputer Forensik

Istilah forensik sering kita dengar dalam berbagai berita kriminal, forensik memang lekat hubungannya dengan dunia kejahatan, namun menurut artinya kata forensik sendiri memiliki arti menyajikan ke pengadilan, forensik adalah suatu upaya yang berdasarkan ilmu pengetahuan dan bersifat ilmiah untuk melakukan pencarian, pengumpulan, analisis dan melakukan pelaporan segala hasilnya ke suatu pengadilan sesuai hukum yang berlaku. (Sulianta, 2016)

Komputer forensik memiliki perbedaan yang cukup mendasar dari cabang keilmuan forensik pada umumnya seperti pada cabang keilmuan kedokteran forensik yang selama ini lebih dikenal oleh masyarakat pada umumnya, objek dari komputer forensik adalah segala sesuatu yang bersumber dari suatu teknologi komputer seperti: sitem komputer, jaringan komputer, media komunikasi serta media penyimpanan pada komputer. Komputer forensik tidak hanya berguna untuk melakukan pengungkapan suatu perkara kriminal atau pelanggaran hukum namun lebih dari itu komputer forensik bisa dimanfaatkan antara lain sebagai: proses pencarian rekonstruksi penanganan insiden keamanan sistem komputer, masalah *troubleshooting* pada suatu sistem komputer, memahami perilaku *malware* dan lainnya (Sulianta, 2016).

Seiring dengan berkembangnya jaman komputer forensik lebih sering dikenal dengan istilah *digital forensik.* Menurut (Kurniawan & Prayudi, 2014) dalam papernya menyebutkan hal ini terjadi karena perkembangan teknologi informasi yang kian berkembang, dimana pesatnya teknologi komputer tidak terbatas pada komputer konvensional saja namun juga mencakup segala teknologi digital yang konsep kerjanya menggunakan konsep dasar komputer di dalamnya.

2.2.5 Live Forensik

(Mazdadi, Riadi, & Luthfi, 2017) menerangakan bahwa live forensik adalah sebuah cara dalam sebuah proses forensik di mana sistem masih dalam keadaan berjalan, hal ini dilakukan dikarenakan jika sistem mati maka akan ada data atau informasi yang hilang. Metode live forensik biasanya digunakan untuk kasus yang terdapat data yang sifatnya *volatile* di mana data akan hilang jika sumber listrik mati, *volatile* data biasanya tersimpan dalam media sementara seperti RAM. Sedangkan menurut (Hermaduanti & Riadi, 2016) dalam papernya menyebutkan bahwa live forensik digunakan untuk mengumpulkan data ketika sistem yang terkena serangan masih hidup.

Menurut (Yudhistira, 2018) secara umum teknik live forensik sama dengan forensik tradisional dalam hal metode yaitu identifikasi, penyimpanan, analisis dan presentasi namun bedanya live forensik mampu mengambil data dan informasi yang hanya ada ketika sistem sedang berjalan.

2.2.6 Bukti Digital

Dalam suatu upaya hukum dalam hal ini lebih spesifik menggunakan proses komputer forensik tentu diperlukan bukti digital yang bisa diajukan dalam proses pengadilan. Bukti digital menjadi kompleks dalam pengertian cara pandangnya, menurut (Sulianta, 2016) terdapat katagori umum diantaranya adalah arsip (archieval files), file aktif dan residual data yang sering disebut juga dengan data sisa atau data sampingan (Sulianta, 2016).

2.2.7 Metasploit

Metasploit adalah sebuah *framework* untuk keperluan *penetration testing* di dalam dunia keamanan, Metasploit adalah proyek yang dikembangkan untuk memberikan informasi tentang suatu kerentanan terhadap suatu sistem, Metasploit *framework* adalah *tools* bersifat *open source* dikembangkan oleh H D Moore seorang ahli dalam bidang keamanan jaringan pada tahun 2003, tujuan dikembangkannya Metasploit adalah menyediakan sumber daya untuk pengembangan dan riset kode *exploit.* Dalam awal pengembangannya Metasploit dikembangkan menggunakan dalam bahasa Perl namun pada akhir tahun 2007 semua *source code*nya ditulis ulang menggunakan bahasa Ruby, kemudian pada tahun 2009 diakuisisi oleh perusahaan yang bergerak di bidang keamanan teknologi informasi Rapid7 (Timalsina & Gurung, 2017).

Menurut (Timalsina & Gurung, 2017) di Metasploit terdapat lebih dari satu pilihan antarmuka diantaranya adalah:

A. Msfconsole

   Msfconsole menyediakan antarmuka yang lengkap dengan ini seorang penyerang bisa melakukan banyak hal, seperti meeluncurkan *exploit,* memuat *auxiliary module,* membuat *listener* dan lainnya, untuk menjalankan antarmuka ini ketikan *msfconsole* pada *command line interface* (CLI) pada terminal Kali Linux

B. Msfcli

   Msfcli berbeda dengan Msfconsole di mana Msfcli lebih mengarah pada *scripting* dan *interpretability* dengan *tools* berbasis konsol. Msfcli dijalankan langsung dengan *command line.*

C. Armitage

   Armitage adalah salah satu bagaian dari Metasploit dan mempunyai grafis antarmuka pengguna yang interaktifu untuk menjalankan armitage, masukan *armitage* CLI pada terminal Kali Linux.

Metasploit adalah sebuah *open source framework* yang dikembangkan untuk melakukan serangan ke dalam sebuah sistem, menguji kerentanan sebuah sistem untuk di*exploit*. Ada beberapa langkah dasar yang digunakan untuk melakukan serangan menggunakan Metasploit adalah (Choudhary & Khurana, 2017):

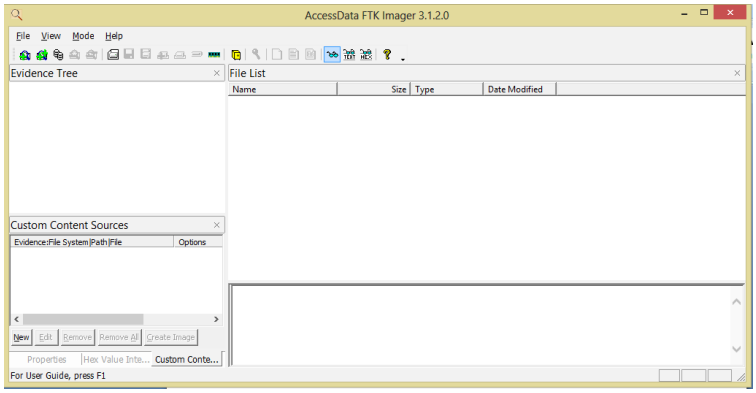
A. Menyesuaikan *exploit* yang akan digunakan dengan *vulnerable system* target
B. Mencari Informasi tentang *exploit*
C. Melakukan *set up payload*
D. Mengatur Opsi
E. Menjalankan *Exploit*

2.2.8 Exploit

Exploit dimanfaatkan oleh penyerang atau pentester untuk melakuan eksploitasi ke dalam suatu mesin yang mempunyai kerentanan baik kerentanan sistem, aplikasi atau layanannya (Timalsina & Gurung, 2017).

2.2.9 FTK Imager

Adalah salah satu *tools* untuk melakukan akuisisi, salah satu fiturnya bisa melakukan akuisisi terhadap RAM komputer, FTK Imager adalah salah satu *tools* yang dikembangkan oleh Access Data, perusahaan pengembangan aplikasi untuk keperluan digital forensik (Yudhistira, 2018)



Gambar 2.1 Gambar Tampilan AccessData FTK Imager

2.2.10 Payload

Payload adalah kode yang dimanfaatkan penyerang atau pentester untuk dieksekusi oleh mesin. Payload dapat dapat dipilih dan dikirim menggunakan Metasploit
(Timalsina & Gurung, 2017).

2.2.11 Volatility Memory Forensics Tools

Volatility adalah sebuah *tool* yang bisa dimanfaatkan untuk melakukan analisis forensik untuk RAM forensik sifatnya *open source* dan dipublikasikan dibawah lisensi GNU. Volatility berjalan secara *command line interface*, *tool* ini bisa melakukan ekstraksi terhadap *file dump* pada momori untuk mengetahui proses yang sedang berjalan, Modul Kernel OS, Koneksi yang berjalan pada komputer dan lainnya (Logen, Höfken, & Schuba, 2012) .

.