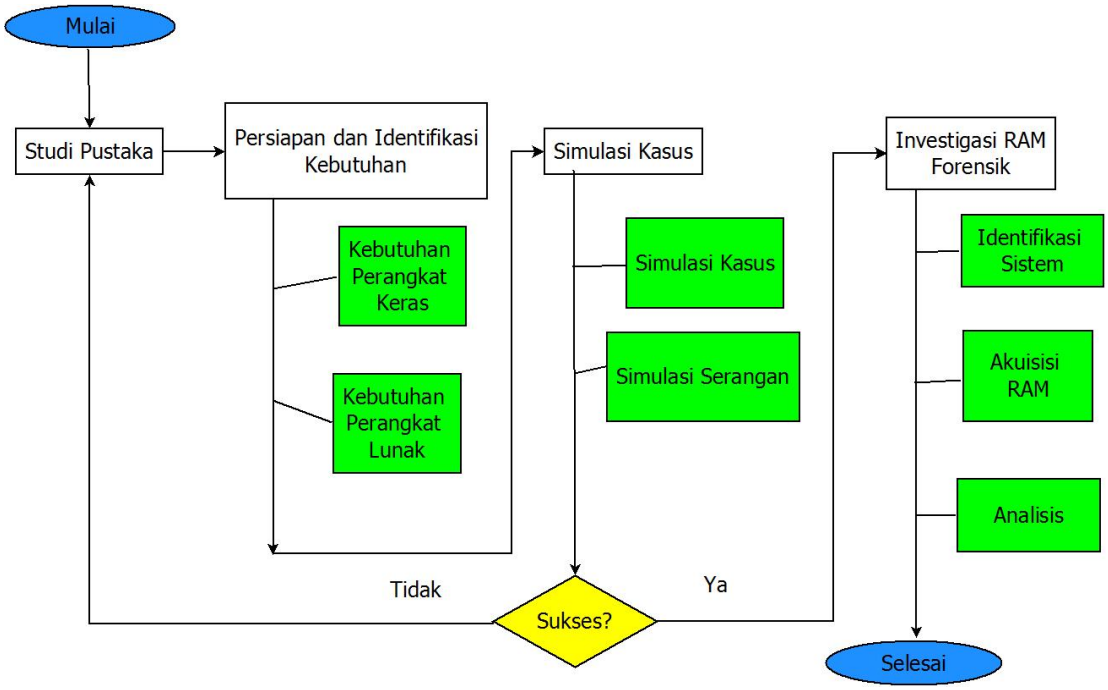
BAB 3
Metodologi Penelitian

Berdasarkan latar belakang dan rumusan masalah yang sudah dijelaskan pada Bab 1 maka untuk menyelesaikan penelitian, berikut uraian dari sejumlah tahapan yang akan dilakukan pada penelitian ini dijelaskan dalam bagan Gambar 3.1.



Gambar 3.1 Alur Metodologi Penelitian

3.1 Studi Pustaka

Tahapan studi pustaka adalah langkah awal yang dilakukan dalam penelitian ini, studi pustaka dilakukan dengan cara mengumpulkan dan mendapatkan berbagai data dan informasi, baik berupa jurnal, paper, artikel, buku, dokumen, informasi dari internet dan lain-lain yang berkaitan dan relevan dengan penelitian yang sedang dilakukan kemudian dari berbagai informasi dan data yang didapat bisa dijadikan sebagai acuan dalam penelitian ini.

3.2 Persiapan Sistem dan Identifikasi Kebutuhan

Pada tahapan ini dilakukan identifikasi tentang bagaimana melakukan persiapan dalam membangun sebuah lingkungan kerja yang dibutuhkan dalam penelitian seperti, mempersiapkan perangkat keras yang dibutuhkan, menyiapkan perangkat lunak yang diperlukan serta membangun jaringan komputer untuk keperluan simulasi dan analisis.

3.2.1 Kebutuhan Perangkat Keras

Dalam penelitian ini digunakan dua buah perangkat yaitu 3 laptop, Router Mifi dan USB drive dengan uraian spesifikasi sebagai berikut

Tabel 3.1 Laptop 1

Prosesor	Intel® Core™ i3-380M
Memory	3 GB
Harddisk	500 GB
Grafis	Intel® HD Graphics

Tabel 3.2 Laptop 2

Prosesor	AMD E2 Vision
Memory	4 GB
Harddisk	500 GB
Grafis	AMD Radeon

Tabel 3.3 Laptop 3

Prosesor	AMD
Memory	2 GB
Harddisk	500 GB
Grafis	AMD

Tabel 3.4 Router MiFi

Merk	Andro Max
Type	M3z
Chipset	Qualcomm 9307
Wifi	2.4 Ghz

Tabel 3.5 USB drive

Merk	**Kapasitas**	**Jumlah**
Toshiba	4 GB	1
Sandisk	8 GB dan 32 GB	Masing-masing 1
Adata	8 GB	4

3.2.2 Kebutuhan Perangkat Lunak

Untuk keperluan simulasi penelitian diperlukan perangkat lunak, pada PC desktop yang digunakan sebagai target serangan dalam simulasi ini menggunakan sistem operasi Windows 8 dan Windows 10 sedangkan pada perangkat Laptop digunakan sebagai penyerang menggunakan sistem operasi Kali Linux versi 2018.2.

Adapun perangkat lunak berupa *tools* untuk mendukung simulasi adalah sebagai berikut:

1. Metasploit untuk melakukan serangan terhadap target
2. FTK Imager untuk melakukan akuisisi pada RAM komputer target berbasis Windows
3. Magnet Forensics RAM Capturer untuk melakukan akuisisi pada RAM komputer target berbasis Windows
4. Dumpit untuk melakukan akuisisi pada RAM komputer target berbasis Windows
5. Volatility untuk analisis file image hasil akuisisi pada RAM komputer target

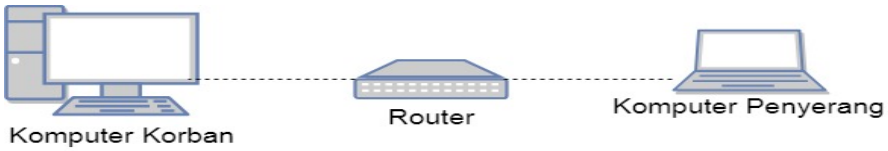
3.3 Skenario dan Simulasi Kasus

Pada penelitian ini dibuatkan sebuah skenario simulasi serangan pada perangkat PC desktop dengan berbagai jenis sistem operasi diantaranya Windows 8 dan Windows 10 yang kemudian akan dianalisis menggunakan metode live forensik khususnya pada RAM komputernya.

3.3.1 Simulasi Kasus

Adapun skenario kasusnya adalah sebagai berikut:

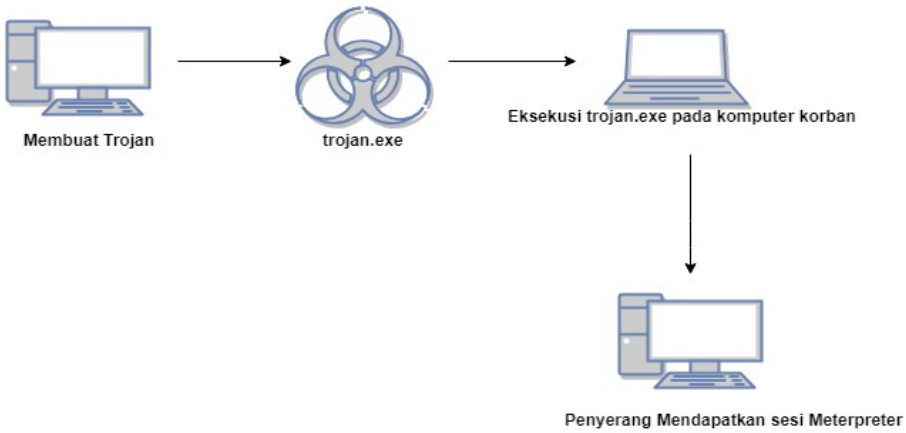
Terdapat PC desktop pada sebuah kantor yang menyimpan file penting kantor terhubung secara LAN pada sebuah jaringan kantor, PC desktop (Komputer Korban) tersebut memiliki hak akses terbatas di mana hanya sekretaris dan jajaran petinggi kantor saja yang boleh mengaksesnya, namun muncul dugaan ada pencurian file rahasia yang bocor yang diduga dilakukan oleh karyawan lain (Komputer Penyerang) dalam satu jaringan, untuk itu pihak kantor melakukan investigasi terhadap komputer tersebut.



Gambar 3.2 Gambaran Umum Topologi Skenario Kasus

3.3.2 Simulasi Serangan

Pada penelitian ini menggunakan tiga sistem operasi berbeda yaitu Windows 8 dan Windows 10 untuk dijadikan target, serangan yang dilakukan memanfaatkan backdoor Trojan yang dibuat memanfaatkan *framework* Metasploit, yaitu msfvenom. Setelah berhasil membuat Trojan dengan ekstensi .exe tersebut kemudian di simpan dalam USB *drive* diasumsikan serangan ini menggunakan teknik *social engineering* sehingga korban bisa mengeksekusi Trojan tersebut. Setelah korban mengekseskusi Trojan tersebut penyerang yang telah melakukan *listening* akan mendapatkan meterpreter session dan komputer korban akan bisa diambil alih secara jarak jauh



Gambar 3.3 Gambaran umum simulasi serangan

3.4 Investigasi RAM Forensik

Investigasi RAM forensik adalah tahapan yang penting dalam penelitian ini di mana tahapan ini dimulai dengan Identifikasi Sistem kemudian Akuisisi RAM dan yang terakhir adalah tahapan Analisis, berikut uraian singkatnya menurut (Rochmadi, 2017):

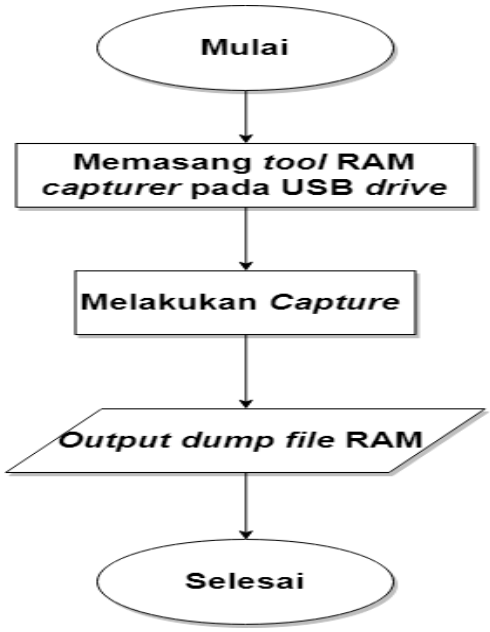
A. Identifikasi Sistem

   Adalah proses awal untuk melakukan pengumpulan informasi dan identifikasi sistem yang berjalan pada komputer yang akan dilakukan investigasi.

B. Akuisisi RAM

Melakukan *capture* data pada memori komputer yang dilakukan pada saat komputer sedang menyala. Pada penelitian ini menggunakan metode Live Forensik dalam melakukan akuisisi di mana komputer harus dalam keadaan menyala, untuk mendapatkan data analisis yang lebih baik pada penelitian kali ini melakukan analisis pada dua sistem operasi yang berbeda yaitu Windows 8 dan Windows 10, selain itu dalam penelitian ini juga akan menggunakan *tool* RAM *capturer* lebih dari satu yaitu Magnet Forensik RAM *capturer,* FTK *Inager* dan Dumpit hal ini berbtujuan untuk mendapatkan pengetahuan tambahan tentang karakteristik data yang dihasilkan dari tiap-tiap *tool*

Untuk itu berikut uraian singkat untuk melakukan akuisisi RAM pada Windows dapat dilihat pada Gambar 3.4



Gambar 3.4 Diagram Alur Proses Akuisisi RAM Komputer Windows

C. Analisis

Merupakan tahap penting untuk melakukan investigasi forensik yaitu menggunakan analisis hasil *capture* RAM menggunakan *volatility tools,*

Dengan *volatility tools* akan terlihat proses apa saja yang sedang berjalan pada RAM komputer, mencari dan melakukan *dump* terhadap file *malicious* yang berjalan sebagai *backdoor.* Dengan analisis perbandingan proses yang berjalan antara komputer normal dan komputer dalam keadaan *under attack* bisa diketahui *running process* yang mencurigakan, selain itu juga akan dicari koneksi kemana saja yang terhubung dalam komputer korban.

Pada tabel 3.1 akan dilakukan *listing* proses yang sedang berjalan pada komputer normal dan komputer yang sedang terkena serangan.

Tabel 3.6 Proses yang berjalan

No	Sistem Operasi	RAM *capturer tool*	*Malicious* Proses yang Berjalan	PID
1				
2				

Tabel 3.2 akan menyajikan bukti digital apa saja seperti telah ditentukan dalam penelitian ini yang berhasil ditemukan pada tiap-tiap sistem operasi dan RAM Capturer Tool dalam melakukan analisis pencarian bukti digital ini menggunakan *tool* volatility. Apabila bukti digital ditemukan akan diberikan tanda *checklist*

Tabel 3.7 Barang bukti digital yang ditemukan

No.	Barang bukti yang dicari	OS	RAM Capturer Tool	Ditemukan/tidak
1	IP Penyerang			
2	Exploit/trojan			
3	Proses berjalan			
4	Profile OS			
5	Lokasi exploit/trojan			

3.5 Pembuatan Laporan

Setelah dilakukan serangkaian simulasi serangan dan analisis terhadap file akuisisi RAM Komputer korban maka dibuatkan laporan mengenai segala aktivitas yang sudah dilakukan terkait penelitian.