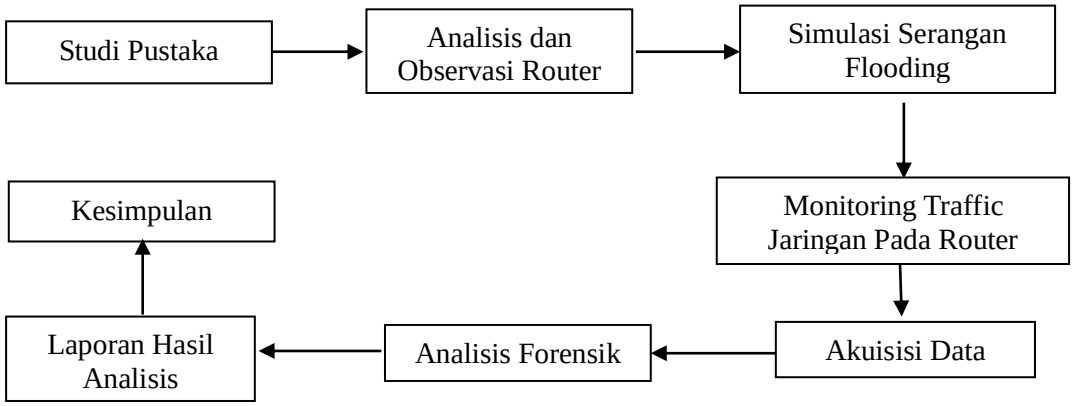
BAB III
Metodologi Penelitian

3.1 Studi Pustaka

Studi pustaka merupakan kegiatan untuk mempelajari, mengkaji berbagai sumber literature-literatur dan teori yang mendukung dalam melakukan penelitian ini. Studi literature melalui paper, jurnal, artikel, buku, website yang terkait dengan teori *Network Forensics, Live Forensics,* Router, Flooding Attack, Metasploit dan Wireshark.

Adapun tahapan pelaksanaan dalam penelitian ini seperti pada gambar 3.1



Gambar 3.1 Alur Penelitian.

Gambar 3.1 menerangkan tahapan penelitian yang akan dilaksanakan dalam penelitian yang akan dilakukan. Dalam alur penelitian tersebut peneliti akan melakukan studi pustaka untuk melakukan kajian terkait penelitian yang akan dilaksanakan. Selain itu, dalam penelitian ini akan dilakukan analisis dan observasi router sebagai tahapan berikutnya penelitian ini. Simulasi serangan dan monitoring traffic jaringan juga termasuk dalam tahapan penelitian ini. Pada tahapan akuisisi data, analisis forensik serta laporan hasil analisis akan menjadi tahapan akhir dalam penelitian ini.

3.2 Alat dan Persiapan Penelitian

Untuk mendukung implementasi dalam pelaksanaan penelitian diperlukan perangkat keras dan perangkat lunak sebagai alat dan bahan penelitian, adapun alat dan bahan yang akan digunakan yaitu :

a. *Hardware* (Perangkat Keras)

Perangkat keras yang dibutuhkan dalam penelitian ini merupakan perangkat keras yang pada umum digunakan dalam jaringan computer. Adapun perangkat tersebut seperti yang tertera pada tabel 3.1.

Tabel 3.1 Kebutuhan Perangkat Keras

No	Hardware	Spesifikasi
1.	Router Mikrotik RB750r2	CPU : QCA9531-BL3A-R 850MHz Main Storage/NAND : 16MB RAM : 64MB LAN Ports : 5 RouterOS License : Level 4
2.	Router Mikrotik RB951-2n	CPU : AR9331 300MHz Main Storage/NAND : 64MB RAM : 32MB LAN Ports : 5 Wireless Standarts : 802.11 b/g/n RouterOS License : Level 4
3.	Laptop Asus X555Q	Processor : AMD Quad Core A12-9720P Memory : 8GB Graphic : AMD Radeon™ R7 Dual Graphics Storage : SATA 1TB Optical Drive : Super-Multi DVD Network : Integrated 802.11 b/g/n Battery : 2 Cells
4.	Laptop HP 14-bw015AU	Processor : AMD Dual Core A9-9420 Memory : 4GB Graphic : AMD Radeon™ R5 Graphics Storage : SATA 500GB Optical Drive : Super-Multi DVD Network : Integrated 802.11 b/g/n Battery : 2 Cells

b. *Software* (Perangkat Lunak)

Perangkat lunak yang akan digunakan pada penelitian ini umumnya sering dikaitkan dengan jaringan pada computer. Adapun perangkat lunak yang akan digunakan pada penelitian ini seperti yang tertera pada tabel 3.2

Tabel 3.2 Kebutuhan Perangkat Lunak

No	Software	Fungsionalitas
1.	Winbox	Aplikasi untuk akses mikrotik
2.	Kali Linux	Sistem Operasi
3.	Metasploit	Tool untuk melakukan penyerangan
4.	Wireshark	Aplikasi untuk menganalisa trafik lalu lintas pada jaringan

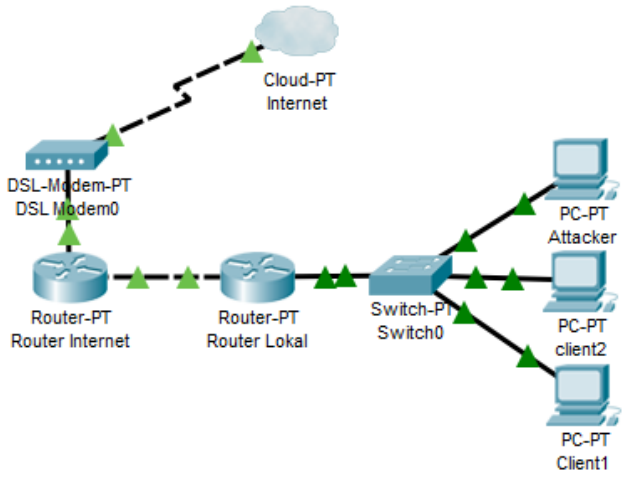
3.3 Simulasi Serangan

Simulasi serangan dilakukan dengan tujuan untuk meninggalkan jejak digital dalam serangan pada router yang kemudian akan dicari sebagai temuan dalam proses investigasi

forensik. Dalam Flooding Attack memiliki beberapa cara dalam penyerangannya, di antaranya sebagai berikut :

a. *Traffic flooding*, merupakan suatu teknik dimana penyerang membanjiri lalu lintas jaringan dengan data yang banyak sehingga menyebabkan lalu lintas menuju korban tidak dapat direspon.
b. *Request flooding*, merupakan teknik membanjiri lalu lintas jaringan oleh penyerang dengan memanfaatkan layanan yang disediakan oleh korban sehingga ketika pengguna ingin melakukan request terhadap suatu layanan, maka layanan tersebut tidak dapat dilayani.
c. Menggunakan banyak cara untuk mengganggu proses komunikasi dalam jaringan seperti ARP Poisoning, Spoofing dan juga termasuk mengubah konfigurasi pada system atau bahkan dapat merusak komponen serta server.

Adapun jenis simulasi serangan yang akan diterapkan pada simulasi ini adalah Flooding Attack dengan menyerang protocol *Transmission Control Protocol* (TCP) pada router menggunakan tools Metasploit seperti pada Gambar 3.2



Gambar 3.2 Simulasi Serangan.

Terkait simulasi serangan diatas berikut penjelasan terkait perancangan serangan pada router yang akan diterapkan dalam penelitian ini.

a. Internet, digunakan untuk terhubungan dengan jaringan luar melalui indihome.
b. Router, digunakan untuk membagi jaringan internet dan local ke client dan juga penyerang.
c. Attacker, digunakan untuk melakukan simulasi serangan flooding pada router.

3.4 Teknik Serangan

Dalam simulasi ini peran attacker/penyerang sangat penting dalam melakukan serangan untuk membanjiri trafik jaringan pada router. Hal ini dilakukan dengan tujuan agar router bisa kelebihan beban dan akses yang dilakukan pengguna lain menjadi sulit. Pada keadaan normal, client akan mengirimkan paket TCP SYN untuk melakukan sinkronisasi paket ke penerima. Penerima akan mengirimkan respond atau jawaban berupa acknowledgement paket TCP SYN ACK. Setelah paket TCP SYN ACK di terima oleh clien, maka client akan mengirimkan paket ACK sebagai tanda proses pengiriman atau penerimaan data akan dimulai.

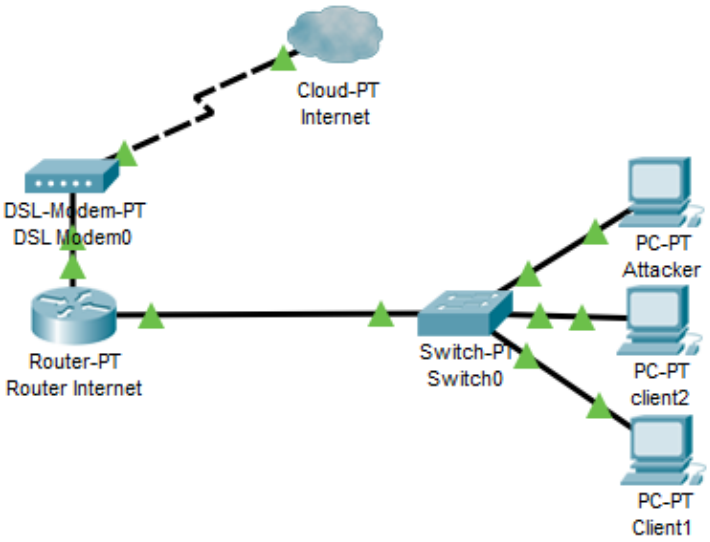
Dalam teknik serangan ini, client (attacker) akan membanjiri server (penerima) dengan paket TCP SYN. Paket yang dikirim akan dijawab oleh penerima dengan paket TCP SYN ACK. Penerima akan terus menunggu respon TCP ACK dari client yang mengirimkan paket. Dan di dalam serangan ini *attacker* akan mengirim data SYN dalam jumlah yang banyak serta di kirim ke port-port pada server (penerima) yang ada dengan alamat atau isi data SYN yang tidak sesuai. Hal ini menyebabkan server (penerima) yang menerima paket data tersebut menjadi bingung dan mengirim paket data SYN ACK yang tidak ada tujuannya sehingga mengakibatkan *lost* data SYN yang sangat banyak di dalam router dan menyebabkan router menjadi *crash* karena menunggu balasan dari komputer yang berada di dalam alamat SYN pertama kali.

3.5 Tahap Implementasi Simulasi

Pada tahapan ini akan dilakukan simulasi serangan berdasarkan desain simulasi yang telah dibuat. Simulasi ini akan menjadi perbandingan sekaligus menguji apakah simulasi yang dilakukan berjalan sesuai dengan yang diharapkan. Adapun simulasi yang akan dilakukan adalah sebagai berikut

3.5.1 Simulasi Serangan Pertama

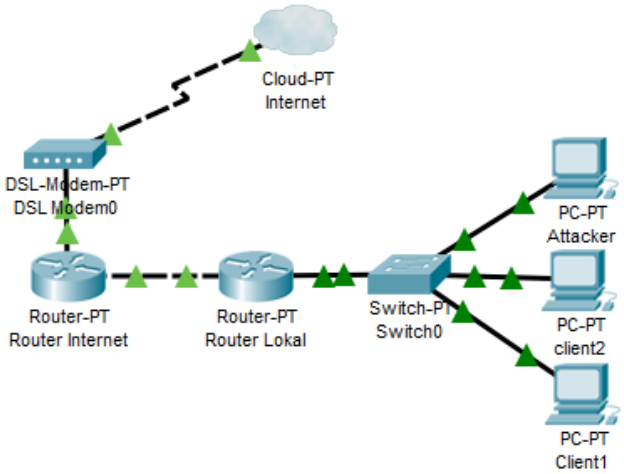
Pada simulasi ini serangan flooding akan dilakukan pada jaringan yang menggunakan satu router untuk pembagian jaringannya. Dalam serangan tersebut, perangkat yang akan diserang adalah router seperti pada gambar 3.3



Gambar 3.3 Simulasi Serangan Pertama.

3.5.2 Simulasi Serangan Kedua

Dalam simulasi berikut ini serangan flooding akan dilakukan pada jaringan yang menggunakan 2 buah router. Pada simulasi ini, serangan akan ditujukan pada router terakhir dimana router tersebut berfungsi sebagai pembagi jaringan ke internet seperti pada gambar 3.4.

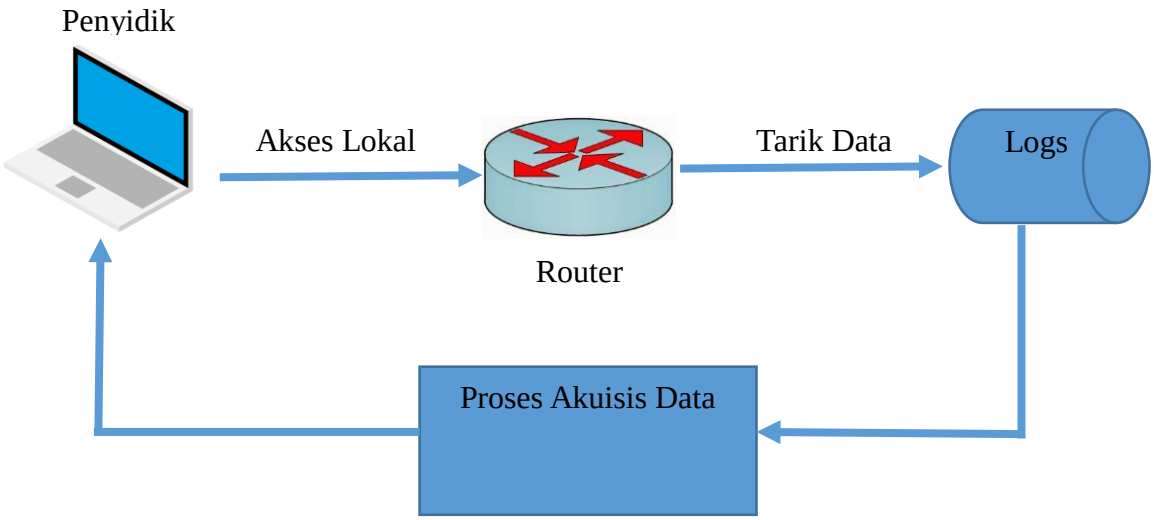


Gambar 3.4 Simulasi Serangan Kedua.

Untuk pengujian apakah simulasi berjalan sesuai yang diharapkan maka dilakukan monitoring lalu lintas pada jaringan router menggunakan aplikasi Wireshark. Adapun hasil dari kedua simulasi tersebut kemudian akan dianalisis untuk kemudian dibuat perbandingan terkait hasil analisis yang dilakukan.

3.6 Tahap Akuisisi

Adapun tahapan akuisisi yang akan dilakukan dalam penelitian ini akan dijelaskan pada Gambar 3.5



Gambar 3.5 Tahapan Akuisisi Secara Live Forensics.

Dalam tahapan ini kondisi utama yang harus terpenuhi dalam menggunakan metode *Live Forensics* yaitu dimana system sedang dalam keadaan beroperasi/*running*. Hal ini dikarenakan beberapa informasi serangan yang ada pada jaringan Router akan hilang jika system tersebut dimatikan ataupun dilakukan *reboot*, sehingga untuk pengambilan data pada Router, Komputer *investigator* perlu untuk bergabung dengan jaringan sebagai *client*, (Casey, 2010).

Untuk dapat membaca informasi secara keseluruhan terkait serangan flooding pada Router maka perlu *login* sebagai admin pada router untuk mendapatkan hak akses keseluruhan. Tahapan selanjutnya dilakukan proses penarikan data dan melakukan analisis untuk mendapatkan laporan serangan flooding sebagai tahapan akhir dari investigasi penyidik forensik.

3.7 Analisis Forensik

Focus utama proses analisis forensik dalam penelitian ini tertuju pada analisis serangan flooding pada router dengan menggunakan fitur aplikasi yang terdapat dalam router untuk penarikan data atau informasi terkait Log Activity, Log Traffic serta IP Address List yang digunakan penyerang. Langkah selanjutnya setelah informasi yang diperlukan telah dipenuhi yaitu melakukan analisis lalu lintas pada system Router menggunakan aplikasi *Wireshark*. Adapun hasil pelaporan yang akan disampaikan adalah penjelasan terkait

kondisi Router sebelum dan setelah diserang sebagai tahapan analisis serangan flooding pada Router serta informasi dari log activity dan log traffic seperti pada table 3.3.

Tabel 3.3 Informasi dalam Log

No	**Timestamp**	**Source Address**	**Dest. Address**	**Protocol**	**Source Port**	**Desr. Port**	**Length**

Komponen-komponen Router yang berpotensi dan dapat digunakan sebagai bukti digital meliputi Log Akses, Log Aktivitas, Daftar Pengguna, DNS Cache, IP *Address*, Hostname, Mac *Address,* dan versi Router, (Fiebig, 2013).

Munculnya perubahan data atau penambahan data pada barang bukti dalam proses *Live Forensics* merupakan konsekuensi atas aktivitas yang dilakukan dalam proses tersebut. Hal ini dikarenakan terhubungnya computer investigator dalam jaringan serta aktivitas permintaan data yang dilakukan melalui aplikasi WinBox pada Router.

Reporting atau pelaporan merupakan tahapan akhir dari proses Forensik. Segala data serta temuan dalam proses analisis serangan flooding pada Router disajikan dalam tahapan ini. Dalam pelaporan hasil analisis akan dilampirkan terkait data-data temuan beserta hasil analisis penelitian.