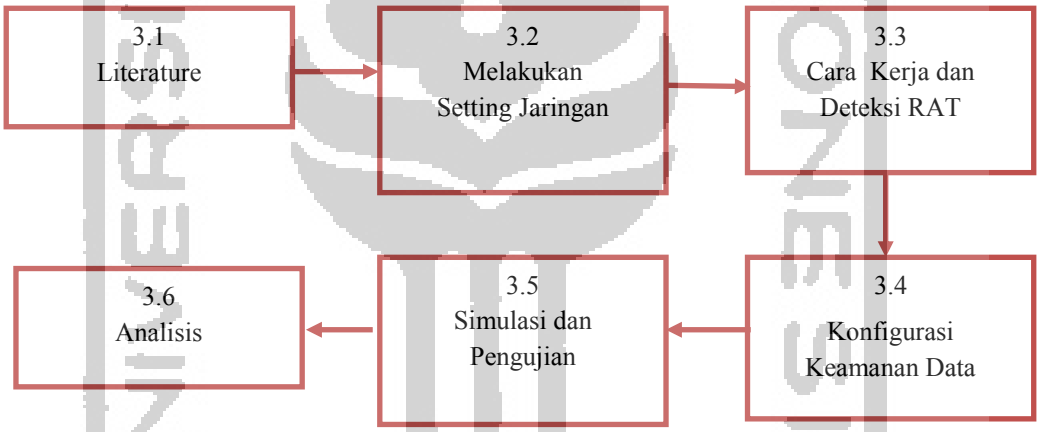
BAB 3

Metode Penelitian

Studi pustaka merupakan kegiatan untuk mengkaji dan mempelajari berbagai sumber literatur dan teori-teori yang mendukung tentang penelitian yang dilakukan. Sumber pembelajaran pada studi pustaka dapat bersumber dari jurnal, paper, artikel, buku-buku, website, dan sumber pembelajaran lainnya yang membahas berkaitan tentang Network Forensics, Malware, *Remote Access Trojan (RAT)*, Router Forensik, MikroTik, dan Router. Pada tahap ini akan dilakukan pula pembuatan proposal penelitian. Berikut tahapan-tahapan yang akan dilakukan dalam penelitian ini :



Gambar 3. 1 Flowchart Alur Penelitian

Metode yang digunakan dalam penelitian ini adalah metode *Dynamic Analysis*, dimana metode ini melakukan analisa *malware* pada suatu sistem dan melihat aktivitas atau proses yang diaktifkan oleh *malware* tersebut.

3.1 Literature

Untuk mendukung impementasi dalam penelitian ini diperlukan adanya perangkat keras dan perangkat lunak sebagai alat dan bahan penelitian.

3.1.1 Hardware

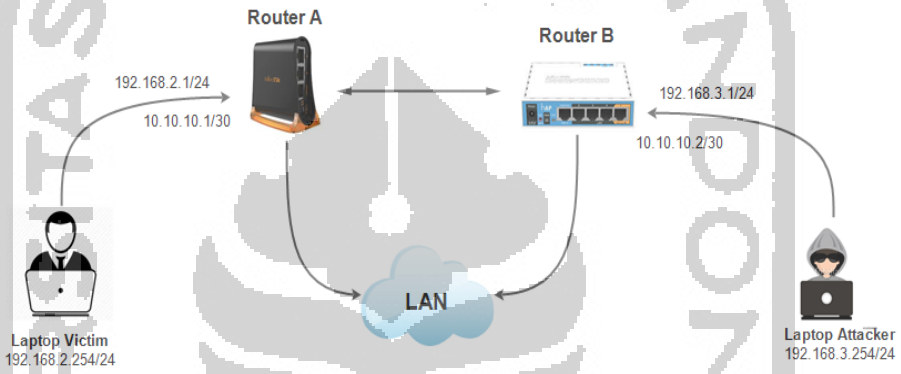
a. Mikrotik RouterOS tipe Router RB951Ui versi 6 dan Router RB931-2nD
b. Laptop Core i3, RAM 2GB sebagai komputer untuk melakukan penarikan data dan analisa
c. Laptop sebagai client jaringan server dan Laptop sebagai client korban

3.1.2 Software

a. Winbox v3.18
b. Wireshark, Disk Investigator dan Virus Total
c. Jenis file *Remote Access Trojan* (RAT)
d. Microsoft Windows 8.1

3.2 Melakukan Setting Jaringan

Dalam penerapan simulasi kondisi jaringan untuk pada penelitian ini maka perlu dilakukan perancangan topologi jaringan, Adapun topologi yang diterapkan pada penelitian ini.

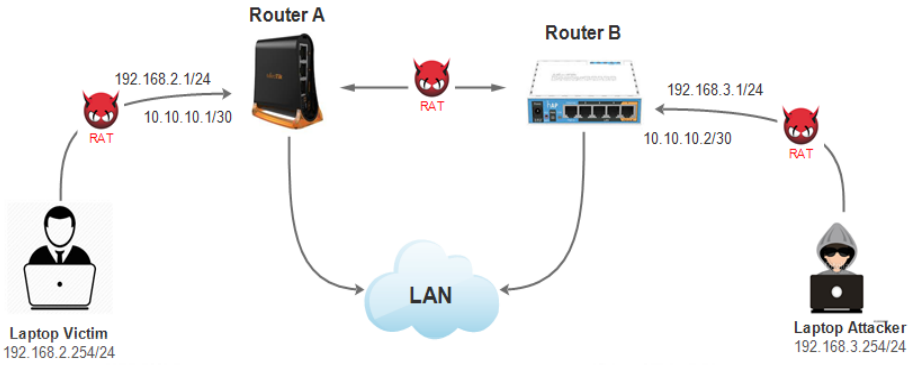


Gambar 3. 2 Topologi Jaringan

Topologi ini adalah topologi jaringan menggunakan router RB951Ui versi 6 yang mana ada seorang *attacher* yang menyerang beberapa client mengunakan *Trojan* RAT melalui akses internet ke beberapa client dan terhubung dengan router RB951Ui ke server jaringan dalam simulasi ini. Hasil simulasi nantinya bisa mencegah masuknya serangan *malware Trojan* RAT ke komputer/laptop client yang terinfeksi *malware Trojan* dengan menggunakan jaringan MikroTik router ini.

3.3 Cara Kerja dan Deteksi Serangan *Remote Access Trojan* (RAT)

Cara kerja serangan RAT dibahas dalam rangkaian topologi serangan *Remote Access Trojan* (RAT) yang digambarkan dibawah ini :



Gambar 3. 3 Topologi Serangan RAT

Berdasarkan topologi penelitian ini bagaimana serangan program *malware* jenis RAT terjadi diawali dari tindakan pelaku *attacker* yang melakukan penyerangan melalui jaringan LAN *(Local Area Network)* dengan mengirimkan program *malware* jenis RAT melalui via email, bisa lewat *file sharing,* atau media sosial dengan cara menanamkan program *malware* tersebut ke Laptop korban yang terhubung dengan jaringan router tipe RB951Ui ke server admin. Laptop korban akhirnya terjangkit yang mengakibatkan Laptop korban bisa diakses dalam jaringan LAN, program *malware* jenis ini bisa mengendalikan program dalam *file manager, run file, remote desktop, remote cam, microphone, remote shell, process manager, registry, keylogger, open chat, get passwords, server,* dan *open folder.*

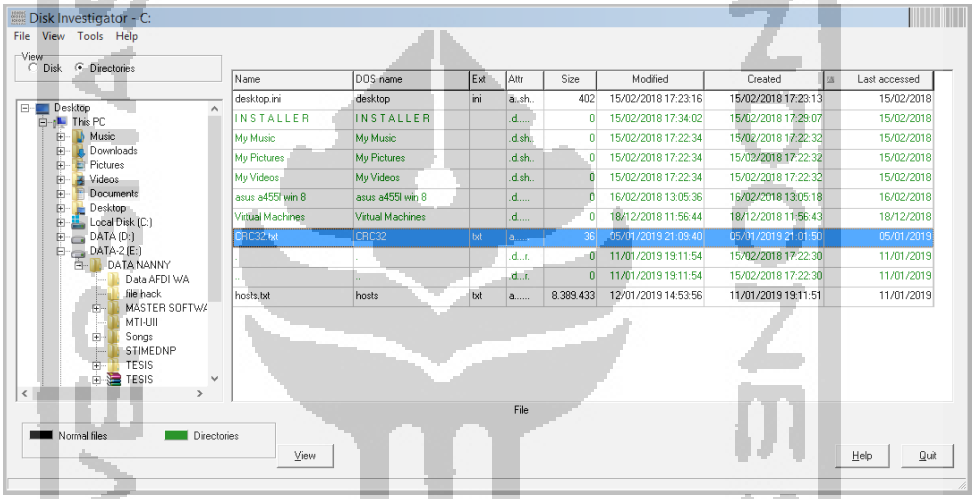
Cara deteksi adanya serangan *Remote Access Trojan* (RAT) ini bisa diketahui melalui aplikasi *forensics* dan beberapa tools diantaranya menggunakan tools Wireshark dan disk inverstigator, seperti terlihat berikut :

Gambar 3. 4 Packet Data Berjalan

Dalam tools Wireshark terdapat informasi packet data yang berjalan dalam jaringan LAN secara detail dalam keterangan akses Ethernet, informasi detail

packet data dan informasi Raw data yang didefenisikan dalam bentuk simbol *hash.* Jaringan packet data apa saja dalam packet capture yang tampil dalam bentuk alamat IP-*Address* yang berjalan yang dilihat dari port-port jaringan.

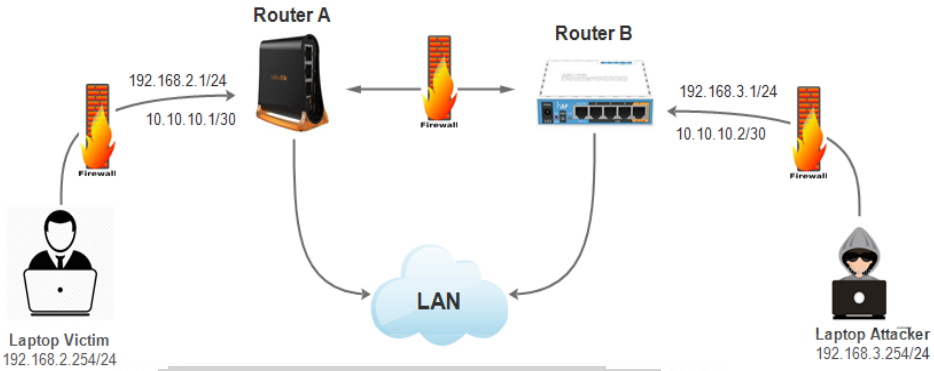
Selanjutnya dalam tools Disk Investigator memberikan informasi adanya program yang mencurigakan terdapat dalam drive yang diketahui melalui *file extension* dan timestamp, kapan file tersebut dimodifikasi, dibuat dan kapan terakhir di akses, juga memberikan informasi apakah adanya program *malware* dalam drive tersebut. Disk investigator juga memberikan informasi pada data *raw file* berupa *text, hexadecimal, decimal,* dan juga memberikan informasi *cluster disk* pada *sector* ke *sector* berikutnya serta informasi *hash* dalam *disk.*



Gambar 3. 5 Disk Investigator

3.4 Konfigurasi Keamanan Data

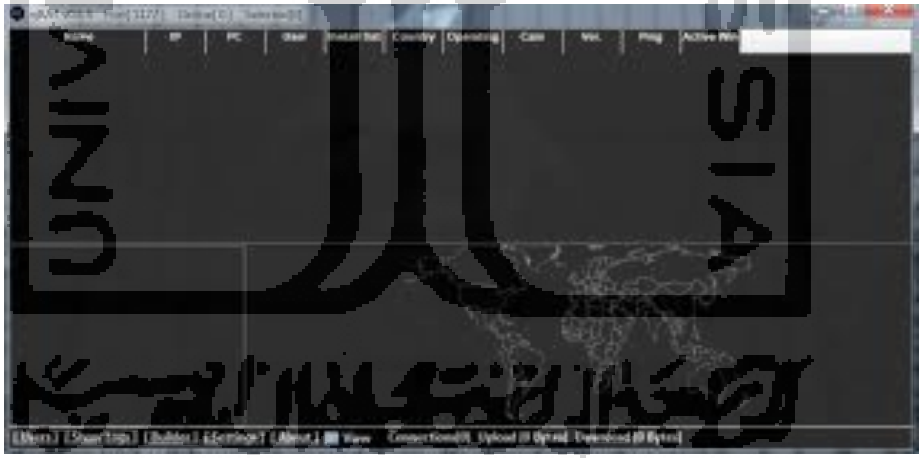
Dalam penelitian ini dilakukan konfigurasi keamanan data dalam settingan jaringan dengan memasang firewall di port sedang berjalan yang menghubungkan dengan port Laptop *attacker*. Memasang firewall merupakan cara untuk memfilter paket yang dilakukan untuk meningkatkan keamanan jaringan dan mengatur flow data dari ke client ataupun router. Pembacaan rule dilakukan dari atas kebawah secara berurutan. Jika melewati rule yang kriterianya sesuai akan dilakukan action yang ditentukan, jika tidak sesuai maka akan dianalisa ke rule berikutnya. Kemudian memasang *Firewall traffic* di jaringan lokal dan menentukan port yang terhubung dengan Laptop korban yang digunakan secara dinamik mendistribusikan konfigurasi dalam jaringan, seperti IP *address* dan *Netmask,* IP address default gateway, konfigurasi DNS yang bisa support.



Gambar 3. 6 Topologi Serangan RAT setelah dipasang Firewall

3.5 Simulasi dan Pengujian

Dalam simulasi ini yang digunakan berupa perangkat MikroTik RouterOS RB951Ui Versi 6, file RAT jenis *trojan* njRAT sebagai contoh program *malware* untuk mengetahui cara kerja daripada RAT dan mengetahui bagaimana mendeteksi *malware* RAT pada Laptop korban. Hasil simulasi nantinya bisa mencegah masuknya serangan program *malware Trojan* RAT ke komputer/laptop korban yang terinfeksi *malware Trojan* dengan menggunakan jaringan MikroTik router ini.



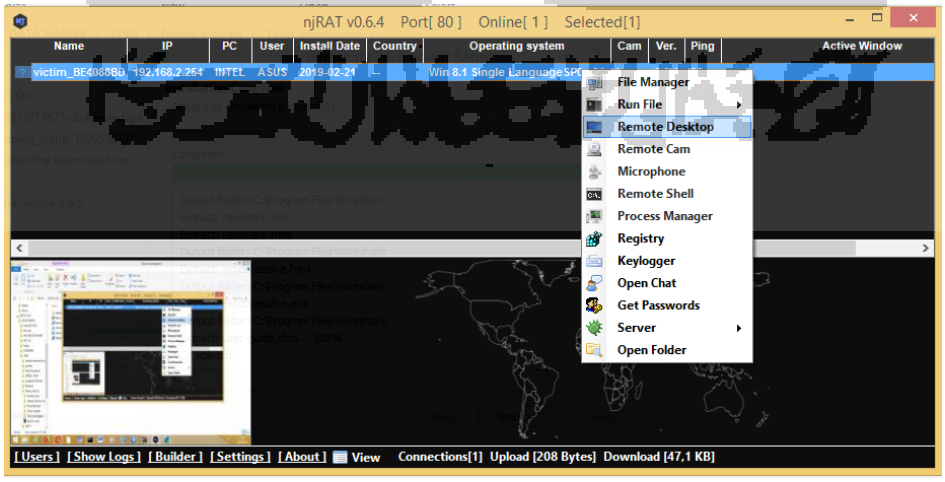
Gambar 3. 7 Tools jenis njRAT

Gambar 3. 8 Builder jenis njRAT

3.6 Analisis

Proses analisis pada metode *malware analysis* ini akan memeriksa Laptop dengan secara keseluruhan seperti proses yang berjalan di Laptop, perubahan *registry*, komunikasi internet dan peristiwa janggal lainnya yang memungkinkan terjadi ketika sebuah Laptop telah terinfeksi oleh *malware jenis* RAT. Beberapa bukti digital yang akan didapatkan setelah program *malware* jenis *trojan* ini terbuka. Bukti digital yang berhasil didapatkan pada menu *malware* jenis RAT diantaranya *manager, run file, remote desktop, remote cam, microphone, remote shell, process manager, registry, keylogger, open chat, get passwords, server,* dan *open folder*.

Analisis dalam penelitian ini menggunakan Winbox sebagai aplikasi MikroTik RouterOS manajemen. Selanjutnya dalam proses analisis juga menggunakan beberapa aplikasi forensik dan beberapa tools forensik, berikut ini hasil analisis njRAT :



Gambar 3. 9 Analisis njRAT