

## **BAB IV**

### **Hasil Dan Pembahasan**

Pada bab ini akan membahas terkait proses penelitian, analisis serta hasil yang ditemukan dalam penelitian ini. Pembahasan dalam bab ini meliputi observasi router dalam setiap simulasi serangan, analisis serangan, akuisisi data pada router dalam simulasi serangan *flooding* pada router. Tahap analisis digunakan untuk mencari barang bukti dari hasil traffic file log serta file log activity pada perangkat router.

#### **4.1 Implementasi Serangan *Flooding***

Dalam tahapan ini akan dilakukan dua simulasi serangan yang kemudian akan dilanjutkan dengan analisis serta observasi pada router, monitoring traffic, akuisisi file log, analisis forensik dan hasil analisis tiap simulasi. Simulasi serangan pertama akan dilakukan dimana suatu jaringan menggunakan satu buah router yang kemudian akan diserang. Sedangkan simulasi serangan kedua akan dilakukan dalam jaringan yang menggunakan dua buah router untuk kemudian router yang terhubung langsung ke internet yang akan diserang.

Serangan *flooding* merupakan suatu serangan yang membanjiri suatu jaringan sehingga menyebabkan padatnya lalu lintas data dalam suatu jaringan. Hal ini dapat membuat konsumsi daya pada server meningkat sehingga dapat membuat server menjadi down. Salah satu tipe serangan *flooding* yaitu *Syn Flood* yang merupakan salah satu bentuk serangan dimana penyerang akan mengirimkan *Syn request* kepada target sehingga membuat lalu lintas data menjadi ramai.

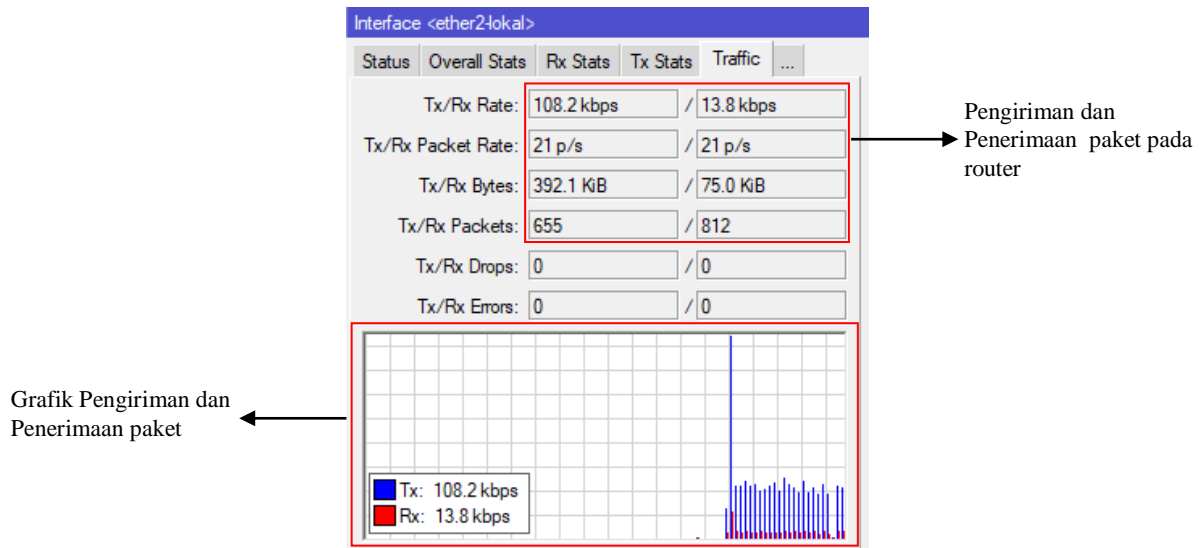
Dalam keadaan normal, client akan mengirimkan paket TCP SYN untuk melakukan sinkronisasi paket ke penerima. Penerima akan mengirimkan *respond* atau jawaban berupa acknowledgement paket TCP SYN ACK. Setelah paket TCP SYN ACK di terima oleh client, maka client akan mengirimkan paket ACK sebagai tanda proses pengiriman atau penerimaan data akan dimulai.

##### **4.1.1 Simulasi Serangan Pertama**

Dalam tahapan ini, berdasarkan gambaran scenario simulasi yang ditunjukkan sebelumnya pada gambar 3.3, akan dilakukan serangan SYN Flood pada router. 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.

#### 4.1.1.1 Analisis dan Observasi Router

Dalam mengawali proses simulasi serangan terhadap Router, perlu dilakukan analisis dan observasi terhadap Router untuk mengetahui apakah Router dalam keadaan normal atau sementara diserang. Untuk melakukan pengecekan dapat melalui menu yang terdapat pada aplikasi Winbox, yaitu pada menu interface kemudian tab traffic. Dalam proses pengecekan akan terlihat bahwa router belum mengalami serangan, hal ini terlihat dari grafik traffic Tx dan Rx.



Gambar 4.1 Tampilan traffic sebelum ada serangan pada router.

Berdasarkan gambar 4.1, dapat diketahui bahwa belum ada serangan terhadap router pertama serta aktivitas lalu lintas jaringan pada Router berjalan normal. Hal ini berdasarkan informasi pada Tx/Rx Rate yang masih dalam keadaan normal dan belum terlihat padat.

Selanjutnya dilakukan observasi terhadap Address Resource Protocol (ARP) List yang terdapat pada router. Dalam hal ini untuk mengetahui informasi terkait IP Address yang terhubung pada router dan juga MAC Address yang setiap IP Address seperti pada gambar 4.2.

	IP Address	MAC Address	Interface
D	192.168.2.252	08:00:27:EB:F5:30	ether2-lokal
D	192.168.2.253	10:7B:44:D7:39:F5	ether2-lokal

↓

IP Address yang terhubung pada router

2 items

Gambar 4.2 ARP List.

Dalam gambar 4.2 terdapat 2 perangkat yang terhubung pada jaringan router. Setiap perangkat yang terhubung memiliki IP Address dan MAC Address yang berbeda namun terhubung pada interface yang sama. Pada langkah berikutnya akan dimulai simulasi serangan *flooding* pada router menggunakan aplikasi Metasploit untuk mengetahui bahwa serangan yang dilakukan berhasil atau gagal. Dalam kondisi yang sama akan dilakukan juga analisis terhadap lalu lintas jaringan menggunakan aplikasi *Wireshark* yang kemudian akan dilakukan penarikan data sebagai barang bukti digital melalui metode *Live Forensic*.

#### 4.1.1.2 Simulasi Serangan

Pada tahap ini, simulasi serangan akan dilakukan menggunakan aplikasi metasploit. Metasploit merupakan salah satu tools pengujian penetrasi terkemuka saat ini dan juga salah satu proyek open-source terbesar dalam hal keamanan informasi serta pengujian penetrasi. Adapun tools ini dapat digunakan hampir disemua sistem operasi. Dalam simulasi serangan ini, attacker akan menyerang router yang terhubung ke internet seperti pada gambar 4.3 berikut

```
msf auxiliary(dos/tcp/synflood) > set rhost 192.168.2.1
rhost => 192.168.2.1
msf auxiliary(dos/tcp/synflood) > exploit
[*] SYN flooding 192.168.2.1:80...
```

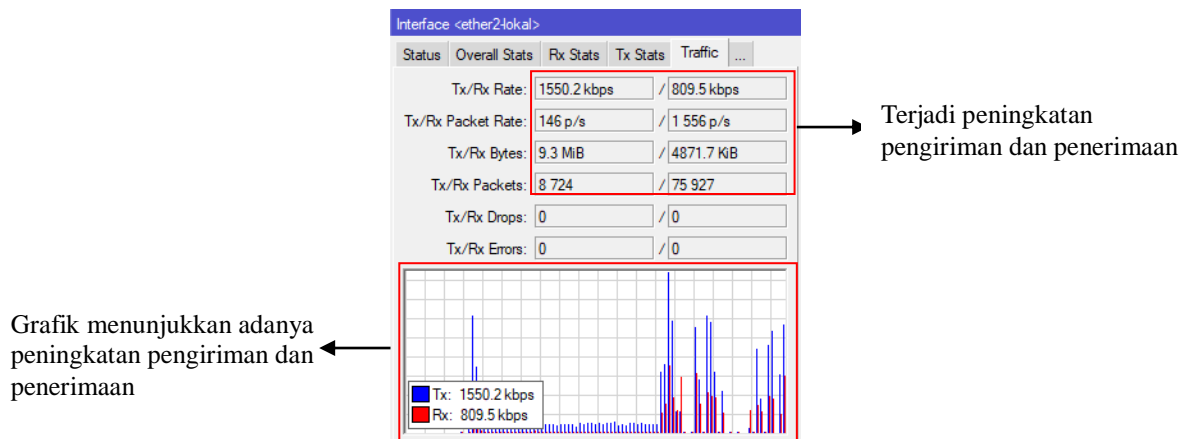
Gambar 4.3 Simulasi Serangan Syn Flood.

Dalam gambar 4.3 dijelaskan **rhost 192.168.2.1** yang artinya bahwa alamat IP Address target yaitu 192.168.2.1. Adapun **exploit** memiliki arti eksploitasi atau dapat diartikan serangan dijalankan. Dari perintah diatas menunjukkan bahwa serangan Syn

Flood telah dilaksanakan, untuk tahapan selanjutnya akan dilakukan monitoring trafik dan akuisisi.

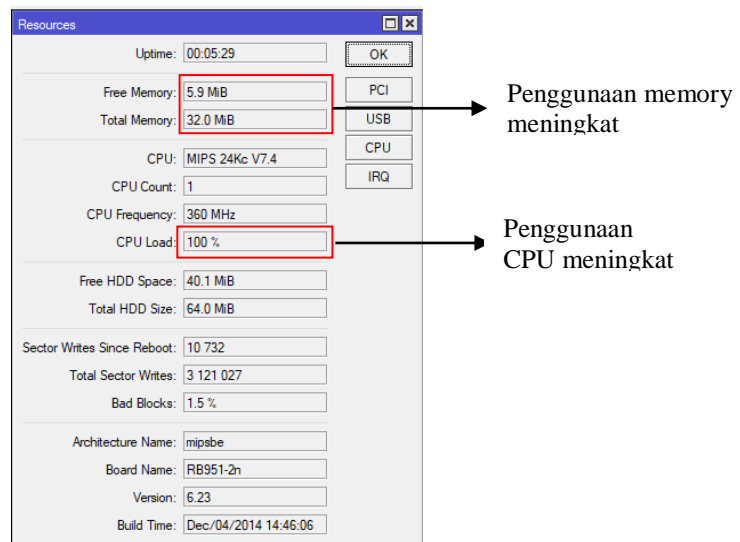
#### 4.1.1.3 Monitoring Trafik dan Akuisisi

Setelah dilakukan observasi dan simulasi serangan yang dilakukan berhasil masuk, maka selanjutnya dilakukan monitoring serangan pada router. Dalam proses ini, langkah yang akan dilakukan yaitu dengan cara men-capture lalu lintas jaringan untuk kemudian dilakukan analisis menggunakan wireshark serta memantau keadaan router melalui aplikasi winbox.



Gambar 4.4 Pemantauan traffic pada router.

Setelah serangan berhasil dilakukan, pada gambar 4.4 terjadi peningkatan traffik pengiriman dan penerimaan pada router. Hal ini mengindikasikan bahwa serangan yang dilakukan telah berhasil dijalankan. Peningkatan traffik ini diatas dapat membuat jaringan menjadi lambat disebabkan oleh hal tersebut.



Gambar 4.5 Pemantauan Resource Router.

Meningkatnya trafik pada router menyebabkan konsumsi daya pada router ikut meningkat. Hal tersebut terlihat dimana resource pada router ikut meningkat terutama pada penggunaan CPU naik secara signifikan seperti yang ditunjukkan pada gambar 4.5. Peningkatan aktivitas router dalam simulasi pertama ini menunjukkan bahwa simulasi serangan yang dilancarkan telah berjalan.

Untuk bisa melakukan proses metode *Live Forensic* kondisi yang harus dipenuhi yaitu dimana system sedang dalam keadaan hidup, hal ini dikarenakan beberapa informasi yang tersimpan pada router akan hilang jika system tersebut dimatikan atau melakukan reboot. Oleh sebab itu sebagai investigator harus masuk kedalam jaringan sebagai client untuk melakukan pengambilan data pada router. Tujuan dalam melakukan proses akuisisi data yaitu untuk menemukan bukti digital sebagai laporan pemeriksaan forensik. Proses pemeriksaan forensik ini dengan melakukan analisis terhadap data yang telah di akuisisi untuk mendapatkan informasi dari data Log Activity, Log Traffic dan ARP list dalam menemukan pelaku penyerangan pada router menggunakan metode *Live Forensics*.

12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:17140->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:61908->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:25374->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:45652->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:24671->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:38624->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:60290->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:34969->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:41203->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:41323->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:34262->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:33496->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:27731->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:37567->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:1472->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:1920->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:2702->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:56787->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:28327->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:38660->192.168.2.1:80, len 40
12:13:17	firewall,info input: in:ether2-lokal out:(none), src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 100.153.158.165:47430->192.168.2.1:80, len 40

Gambar 4.6 Hasil Akuisisi Data Log Activity Router.

Pada gambar 4.6 menampilkan informasi data log activity yang telah diakuisisi oleh penyidik. Informasi yang tercatat pada data log tersebut berupa timestamp, interface, mac address, protocol serta IP Address. Hasil akuisisi ini kemudian akan dianalisis sehingga dapat diketahui aktivitas apa saja yang terjadi pada router, termasuk serangan yang telah dilakukan.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	100.153.158.165	192.168.2.1	TCP	60	31789 → 80 [SYN] Seq=0 Win=267 Len=0
2	0.002864	100.153.158.165	192.168.2.1	TCP	60	9169 → 80 [SYN] Seq=0 Win=594 Len=0
3	0.017088	100.153.158.165	192.168.2.1	TCP	60	10435 → 80 [SYN] Seq=0 Win=728 Len=0
4	0.018783	100.153.158.165	192.168.2.1	TCP	60	23731 → 80 [SYN] Seq=0 Win=1221 Len=0
5	0.025965	100.153.158.165	192.168.2.1	TCP	60	30567 → 80 [SYN] Seq=0 Win=3750 Len=0
6	0.026972	100.153.158.165	192.168.2.1	TCP	60	6189 → 80 [SYN] Seq=0 Win=2051 Len=0
7	0.028012	100.153.158.165	192.168.2.1	TCP	60	50597 → 80 [SYN] Seq=0 Win=2123 Len=0
8	0.029195	100.153.158.165	192.168.2.1	TCP	60	45326 → 80 [SYN] Seq=0 Win=265 Len=0
9	0.030280	100.153.158.165	192.168.2.1	TCP	60	47928 → 80 [SYN] Seq=0 Win=2099 Len=0
10	0.031136	100.153.158.165	192.168.2.1	TCP	60	31802 → 80 [SYN] Seq=0 Win=2803 Len=0
11	0.032262	100.153.158.165	192.168.2.1	TCP	60	36151 → 80 [SYN] Seq=0 Win=1931 Len=0
12	0.033569	100.153.158.165	192.168.2.1	TCP	60	49855 → 80 [SYN] Seq=0 Win=2949 Len=0
13	0.0341					Seq=0 Win=1667 Len=0
14	0.0353					Seq=0 Win=2655 Len=0
15	0.0364					Seq=0 Win=2823 Len=0
16	0.0371					Seq=0 Win=3383 Len=0
17	0.038014	100.153.158.165	192.168.2.1	TCP	60	19875 → 80 [SYN] Seq=0 Win=1750 Len=0
18	0.039685	100.153.158.165	192.168.2.1	TCP	60	31020 → 80 [SYN] Seq=0 Win=3646 Len=0
19	0.040808	100.153.158.165	192.168.2.1	TCP	60	22194 → 80 [SYN] Seq=0 Win=29 Len=0
20	0.041837	100.153.158.165	192.168.2.1	TCP	60	41562 → 80 [SYN] Seq=0 Win=3165 Len=0

Gambar 4.7 Hasil Akuisisi Log Traffic Router.

Gambar 4.7 merupakan hasil akuisisi berupa file log traffic. Data hasil akuisisi ini kemudian akan analisis untuk mencari informasi yang diperlukan dalam proses penyelidikan. Didalam router, log activity dan log traffic sangat penting sebab data log ini dapat hilang apabila system dimatikan atau mengalami reboot.

#### 4.1.1.4 Analisis Forensik

Analisis forensik merupakan salah satu tahapan penting dalam mencari informasi yang terdapat pada data yang telah diakuisisi. Dalam tahapan ini, setelah melakukan akuisisi dilanjutkan dengan menganalisis data hasil akuisisi tersebut. Analisis forensik akan dilakukan pada log activity dan log traffic.

Salah satu bukti digital yang paling penting dalam setiap aktifitas yang terjadi pada router adalah Log Activity. Aktifitas yang terjadi didalam router akan dicatat berdasarkan Time, Topic dan Message. Komponen tersebut memberikan informasi yang sangat penting untuk keperluan penyelidikan yang dilakukan oleh investigator dalam menemukan pelaku penyerangan.

Gambar 4.6 merupakan hasil penarikan Log Activity yang menunjukkan bahwa ada kegiatan serangan syn flood pada router. Hal ini dapat diketahui dari komponen diatas yaitu Time, Topic dan Message dimana IP Address 100.153.158.165 melakukan pengiriman paket syn secara terus menerus ke port 80 dengan MAC Address 08:00:27:eb:f5:30 dan menggunakan port yang berbeda-beda. Aktivitas ini mengindikasikan adanya pengiriman paket syn pada router pertama secara terus menerus pada Router.

Log traffic merupakan salah satu komponen penting dalam mengungkapkan aktivitas serangan yang terjadi pada router. Hal ini dikarenakan, log traffic merupakan hasil capture terhadap aktivitas yang terjadi dalam lalu lintas jaringan. Informasi yang ditampilkan dalam log traffic sangat penting dalam memperkuat apa yang telah ditemukan

dalam log activity. Dalam log traffic, informasi yang disampaikan dapat berupa time, source, destination, protocol, length dan info. Untuk dapat melihat informasi yang terdapat dalam log traffic ini, dapat dilihat melalui aplikasi Wireshark seperti pada gambar 4.7.

Informasi yang didapatkan dari log traffic berdasarkan gambar 4.7 hampir sama dengan yang ditemukan dalam log activity. Tampilan diatas menunjukkan bahwa adanya aktivitas serangan pada router. Hal tersebut diketahui melalui Time, Source, Destination, Protocol, Length dan Info dimana IP Address 100.153.158.165 melakukan pengiriman paket SYN secara terus menerus kepada IP Address 192.168.2.1. Adapun Port yang digunakan oleh penyerang selalu berubah-ubah tiap pengiriman paket. Hal ini dicurigai sebagai sebuah aktivitas yang tidak wajar pada jaringan router.

Berdasarkan analisis yang dilakukan, informasi yang diperoleh dari Log Activity dan juga Log Traffic yang kemudian dikomparasikan dengan observasi pada router yaitu informasi IP Address yang tercatat pada router. Dalam Log Activity dan Log Traffic, IP Address 100.153.158.165 merupakan IP Address yang tidak terdaftar pada router. Namun pada IP Address 192.168.2.252 memiliki MAC Address yang sama dengan IP Address 100.153.158.168 yaitu 08:00:27:eb:f5:30. Berdasarkan temuan tersebut diindikasikan bahwa pelaku penyerangan berusaha menyembunyikan IP Address asli milik dirinya agar tidak ditemukan.

#### **4.1.1.5 Hasil Analisis**

Berdasarkan hasil analisis serangan yang dilakukan diatas maka diperoleh alamat IP Address 192.168.2.252 berusaha menyembunyikan IP Address yang asli dengan mengubahnya menjadi 100.153.158.168 namun tidak dapat menyembunyikan MAC Address yaitu 08:00:27:eb:f5:30. IP Address tersebut melakukan serangan dengan mengirimkan paket SYN secara terus menerus dengan menggunakan Port yang berubah secara acak/random. Hal ini menjadi temuan dalam scenario penelitian dalam mendeteksi serangan *Flooding* pada router menggunakan metode *Live Forensics*.

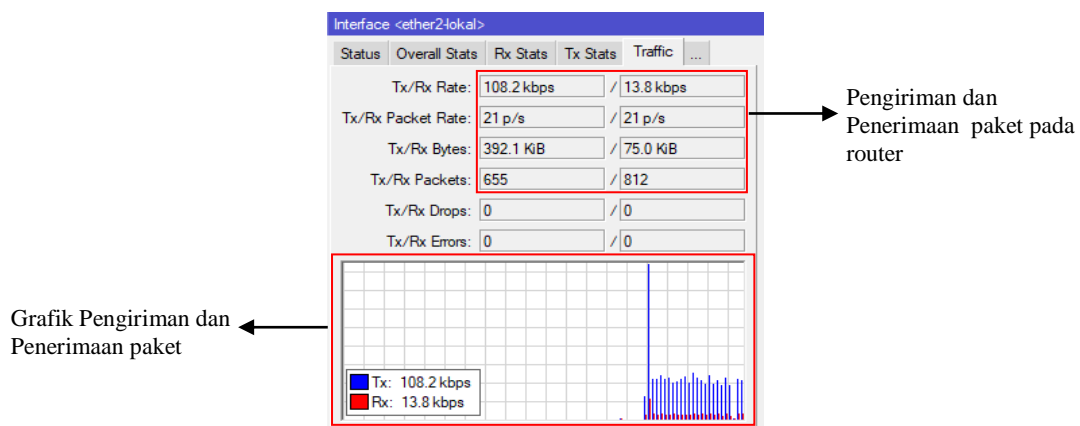
#### **4.1.2 Simulasi Serangan Kedua**

Dalam simulasi kedua ini, berdasarkan gambaran scenario simulasi yang ditunjukkan sebelumnya pada gambar 3.4, akan dilakukan serangan SYN Flood pada router. Namun serangan kali ini menggunakan 2 buah router yaitu router local dan router internet. Serangan yang akan dilakukan akan ditujukan pada router internet namun dalam prosesnya akan melewati router local terlebih dahulu. 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.

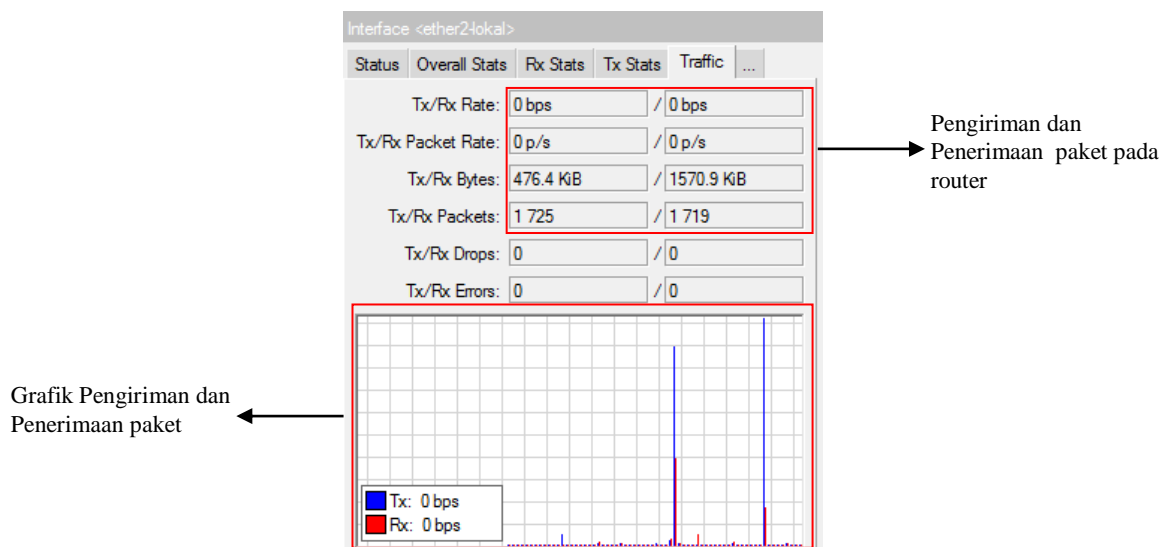
#### 4.1.2.1 Analisis dan Observasi Router

Seperti halnya pada serangan pertama, proses ini diawali dengan melakukan analisis dan observasi terhadap Router untuk mengetahui apakah Router dalam keadaan normal atau sementara diserang. Untuk melakukan pengecekan dapat melalui menu yang terdapat pada aplikasi Winbox, yaitu pada menu interface kemudian tab traffic. Dalam proses pengecekan akan terlihat bahwa router belum mengalami serangan, hal ini terlihat dari grafik traffic Tx dan Rx.



Gambar 4.8 Tampilan traffic sebelum ada serangan pada router local.

Pada gambar 4.8 menunjukkan traffic pada router local berjalan dengan normal. Hal ini terlihat dari pengiriman dan penerimaan paket yang tidak terlalu besar serta tidak terlalu padat.

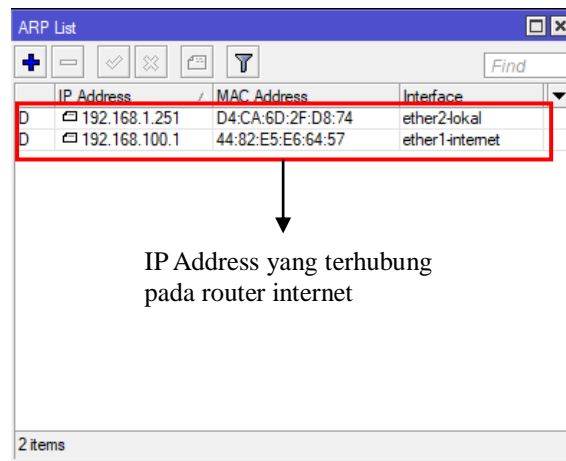


Gambar 4.9 Tampilan traffic sebelum ada serangan pada router internet.



Berdasarkan gambar 4.9, dapat diketahui bahwa belum ada serangan terhadap router local dan router internet serta aktivitas lalu lintas jaringan pada kedua Router berjalan normal. Hal ini berdasarkan informasi pada Tx/Rx Rate yang masih dalam keadaan normal dan belum terlihat padat.

Selanjutnya dilakukan observasi terhadap Address Resource Protocol (ARP) List yang terdapat pada router. Dalam hal ini untuk mengetahui informasi terkait IP Address yang terhubung pada router dan juga MAC Address yang setiap IP Address.

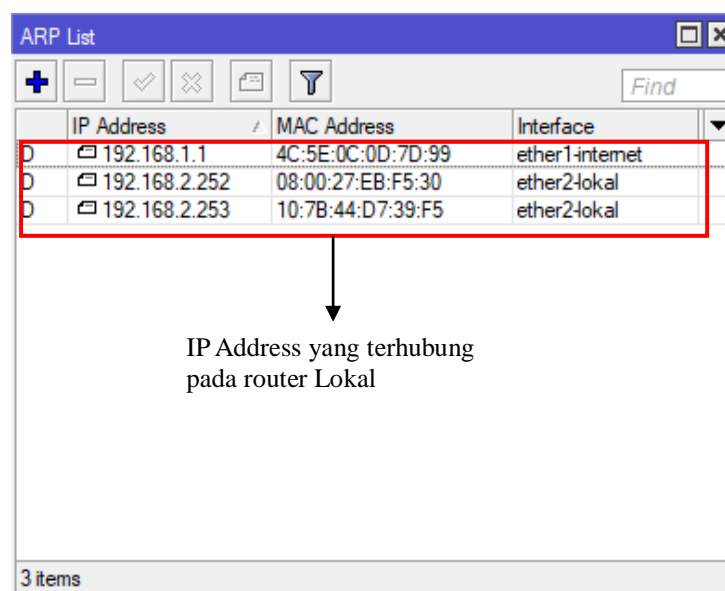


IP Address	MAC Address	Interface
192.168.1.251	D4:CA:6D:2F:D8:74	ether2-lokal
192.168.100.1	44:82:E5:E6:64:57	ether1-internet

IP Address yang terhubung pada router internet

Gambar 4.10 ARP List Pada Router Internet.

Pada gambar 4.10 menunjukkan ada 2 IP Address yang terhubung pada router internet. IP 192.168.100.1 merupakan IP yang terhubung langsung dengan internet, sedangkan IP 192.168.100.251 merupakan IP dari router local. Setiap IP memiliki MAC Address yang berbeda sehingga dapat dimanfaatkan sebagai informasi.



IP Address	MAC Address	Interface
192.168.1.1	4C:5E:0C:0D:7D:99	ether1-internet
192.168.2.252	08:00:27:EB:F5:30	ether2-lokal
192.168.2.253	10:7B:44:D7:39:F5	ether2-lokal

IP Address yang terhubung pada router Lokal

Gambar 4.11 ARP List Pada Router Lokal.

Pada langkah berikutnya akan dimulai simulasi serangan *flooding* pada router menggunakan aplikasi Metasploit untuk mengetahui bahwa serangan yang dilakukan berhasil atau gagal. Dalam kondisi yang sama akan dilakukan juga analisis terhadap lalu lintas jaringan menggunakan aplikasi *Wireshark* yang kemudian akan dilakukan penarikan data sebagai barang bukti digital melalui metode *Live Forensic*.

#### 4.1.2.2 Simulasi Serangan

Pada tahap ini, simulasi serangan akan dilakukan menggunakan aplikasi metasploit. Metasploit merupakan salah satu tools pengujian penetrasi terkemuka saat ini dan juga salah satu proyek open-source terbesar dalam hal keamanan informasi serta pengujian penetrasi. Adapun tools ini dapat digunakan hampir disemua sistem operasi. Dalam simulasi serangan ini, attacker akan menyerang router yang terhubung ke internet seperti pada gambar 4.12

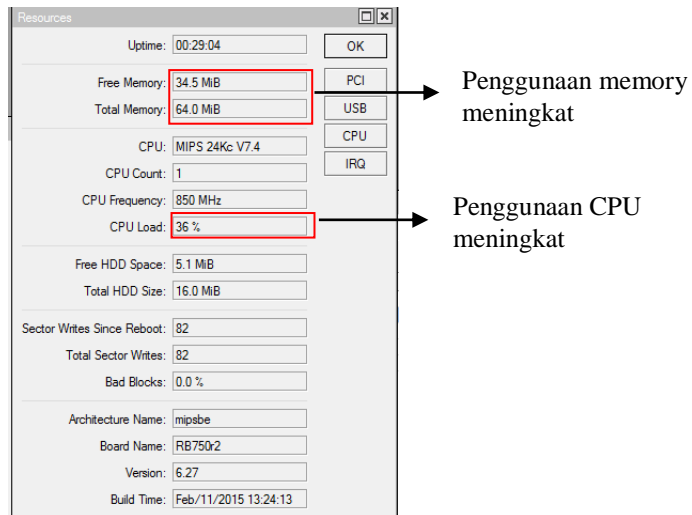
```
msf auxiliary(dos/tcp/synflood) > set rhost 192.168.1.1
rhost => 192.168.1.1
msf auxiliary(dos/tcp/synflood) > exploit
[*] SYN flooding 192.168.1.1:80...
```

Gambar 4.12 Simulasi Serangan Syn Flood.

Dalam gambar 4.12 dijelaskan **rhost 192.168.1.1** yang artinya bahwa alamat IP Address target yaitu 192.168.1.1. Adapun **exploit** memiliki arti eksploitasi atau dapat diartikan serangan dijalankan. Dari perintah diatas menunjukkan bahwa serangan Syn Flood telah dilaksanakan, untuk tahapan selanjutnya akan dilakukan monitoring trafik dan akuisisi.

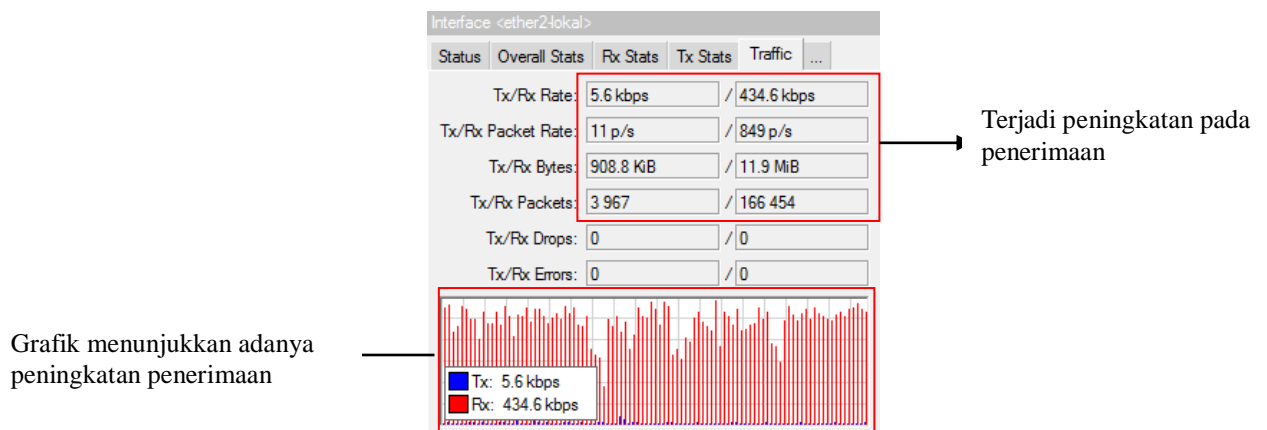
#### 4.1.2.3 Monitoring Trafik dan Akuisisi

Setelah dilakukan observasi dan simulasi serangan yang dilakukan berhasil masuk, maka selanjutnya dilakukan monitoring serangan pada router. Dalam proses ini, akan dilakukan proses men-capture terhadap traffic lalu lintas pada router internet dan juga router lokal untuk kemudian akan dianalisis menggunakan aplikasi Wireshark serta memantau aktivitas yang terdapat pada kedua router melalui aplikasi winbox.



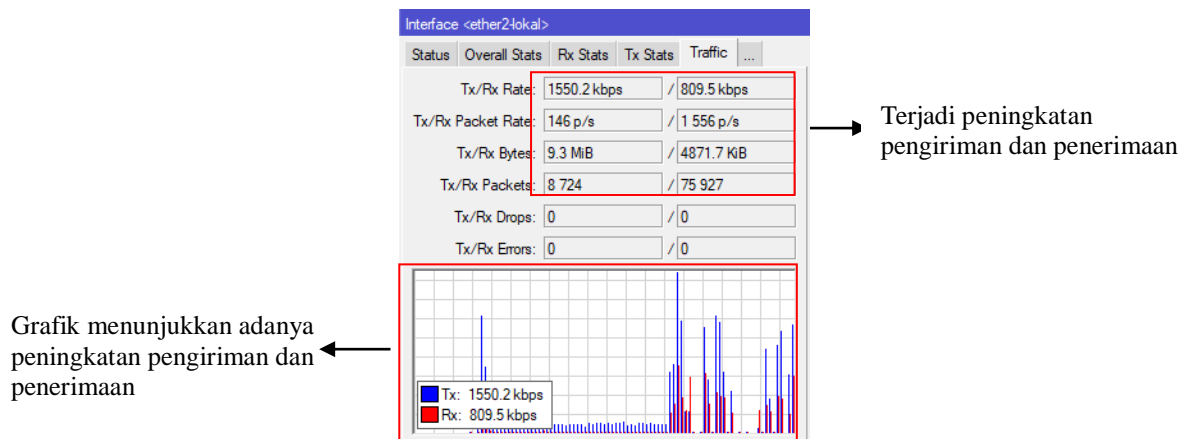
Gambar 4.13 Pemantauan Resource Router Internet.

Dalam gambar 4.13 terjadi peningkatan penggunaan memory dan juga CPU. Hal ini terjadi karena meningkatnya aktivitas lalu lintas data pada router yang diakibatkan serangan yang dilakukan. Aktivitas tersebut dapat menyebabkan router mengalami kelebihan beban dan akan melakukan reboot pada system.



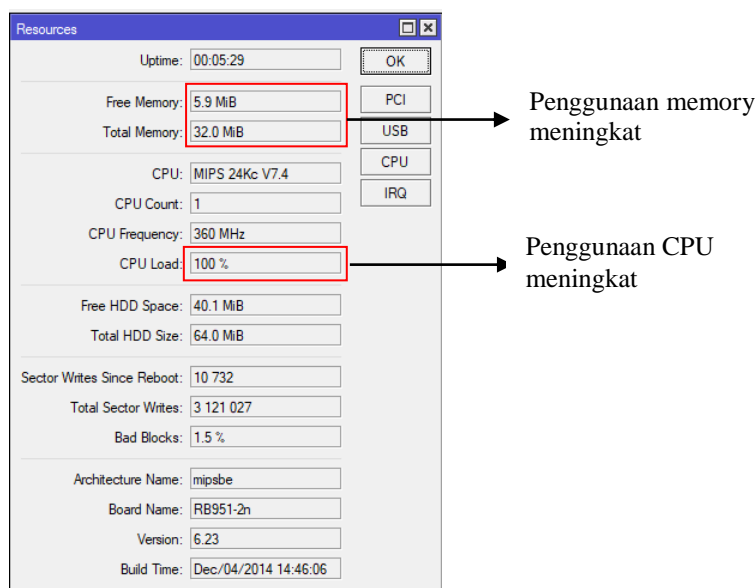
Gambar 4.14 Pemantauan Traffic Router Internet.

Selain adanya peningkatan resource pada router internet baik penggunaan memory maupun penggunaan CPU meskipun belum terlalu tinggi penggunaannya. Namun dalam traffic router internet terlihat mengalami peningkatan penerimaan paket (Rx) yang begitu signifikan seperti yang ditunjukkan pada gambar 4.14.



Gambar 4.15 Pemantauan traffic pada router lokal.

Ketika router internet mengalami peningkatan traffic dalam pengiriman paket. Hal sebaliknya terjadi pada router local, berdasarkan gambar 4.15 menunjukkan bahwa terjadi peningkatan traffic tidak hanya penerimaan paket namun juga pengiriman paket. Peningkatan ini terjadi ketika serangan dilakukan pada router internet.



Gambar 4.16 Pemantauan Resource Router lokal.

Selain lalu lintas jaringan ikut meningkat, penggunaan sumber daya pada router lokal mengalami peningkatan yang signifikan. Hal ini terlihat pada gambar 4.16 yang menunjukkan penggunaan CPU Load mencapai 100% dan memori yang bebas tersisa 5,9MB dari total memory sebesar 32 MB.

Apabila serangan pada router tersebut dilakukan terus-menerus maka dapat mengakibatkan Router akan melakukan Restart sendiri dikarenakan kelebihan beban. Sebelum hal tersebut terjadi, peneliti akan menarik data untuk memperkuat hasil analisis.

Untuk bisa melakukan proses metode *Live Forensic* kondisi yang harus dipenuhi yaitu dimana system sedang dalam keadaan hidup, hal ini dikarenakan beberapa informasi

yang tersimpan pada router akan hilang jika system tersebut dimatikan atau melakukan reboot. Oleh sebab itu sebagai investigator harus masuk kedalam jaringan sebagai client untuk melakukan pengambilan data pada router. Tujuan dalam melakukan proses akuisisi data yaitu untuk menemukan bukti digital sebagai laporan pemeriksaan forensik. Proses pemeriksaan forensik ini dengan melakukan analisis terhadap data yang telah di akuisisi untuk mendapatkan informasi dari data Log Activity, Log Traffic dan ARP list dalam menemukan pelaku penyerangan pada router menggunakan metode *Live Forensics*.

```

23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:49594->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:37302->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:4251->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:11125->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:22875->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:50123->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:60152->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:18585->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:23044->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:44839->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:62126->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:25380->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:25193->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:43800->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:58455->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:40054->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:12319->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:63619->192.168.1.1:80, len 40
23:59:20 firewall,info input: in:ether2-lokal out:(none), src-mac d4:ca:6d:2f:d8:74, proto TCP (SYN), 192.168.1.254:53077->192.168.1.1:80, len 40

```

Informasi yang diperoleh berupa timestamp, interface, mac address, protocol, ip address

Gambar 4.17 Hasil Akuisisi Data Log Activity Router Internet.

Gambar 4.17 merupakan hasil akuisisi log activity pada router internet. Informasi yang terdapat dalam log tersebut berupa timestamp, interface, mac address, protocol serta ip address. File log tersebut akan dianalisis lebih dalam sehingga dapat memberikan informasi terkait aktivitas pada router.

```

23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:45644->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:26094->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:26547->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:33346->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:19921->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:60497->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:11200->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:14537->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:45795->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:8361->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:11337->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:34232->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:18520->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:30889->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:7583->192.168.1.1:80, len 40
23:59:20 firewall,info srcnat: in:(none) out:ether1-internet, src-mac 08:00:27:eb:f5:30, proto TCP (SYN), 29.169.243.34:8688->192.168.1.1:80, len 40

```

Informasi yang diperoleh berupa timestamp, interface, mac address, protocol, ip address

Gambar 4.18 Hasil Akuisisi Data Log Activity Router Lokal.

Pada gambar 4.18 menunjukkan hasil akuisisi data log activity pada router local. Informasi yang ditampilkan dari log tersebut berupa timestamp, interface, mac address, protocol dan ip address.

No.	Time	Source	Destination	Protocol	Length	Info
34	0.068433	192.168.1.254	192.168.1.1	TCP	60	55984 → 80 [SYN] Seq=0 Win=3645 Len=0
35	0.068482	192.168.1.254	192.168.1.1	TCP	60	31838 → 80 [SYN] Seq=0 Win=667 Len=0
36	0.068532	192.168.1.254	192.168.1.1	TCP	60	39359 → 80 [SYN] Seq=0 Win=3051 Len=0
37	0.072397	192.168.1.254	192.168.1.1	TCP	60	30988 → 80 [SYN] Seq=0 Win=3497 Len=0
38	0.072545	192.168.1.254	192.168.1.1	TCP	60	22010 → 80 [SYN] Seq=0 Win=1942 Len=0
39	0.072599	192.168.1.254	192.168.1.1	TCP	60	29311 → 80 [SYN] Seq=0 Win=2642 Len=0
40	0.072652	192.168.1.254	192.168.1.1	TCP	60	60952 → 80 [SYN] Seq=0 Win=2145 Len=0
41	0.072700	192.168.1.254	192.168.1.1	TCP	60	57557 → 80 [SYN] Seq=0 Win=578 Len=0
42	0.072750	192.168.1.254	192.168.1.1	TCP	60	44603 → 80 [SYN] Seq=0 Win=2154 Len=0
43	0.072799	192.168.1.254	192.168.1.1	TCP	60	35583 → 80 [SYN] Seq=0 Win=3516 Len=0
44	0.072849	192.168.1.254	192.168.1.1	TCP	60	25045 → 80 [SYN] Seq=0 Win=5305 Len=0
45	0.072898	192.168.1.254	192.168.1.1	TCP	60	1239 → 80 [SYN] Seq=0 Win=290 Len=0
46	0.072948	192.168.1.254	192.168.1.1	TCP	60	21153 → 80 [SYN] Seq=0 Win=1869 Len=0
47	0.073000	192.168.1.254	192.168.1.1	TCP	60	39514 → 80 [SYN] Seq=0 Win=1126 Len=0
48	0.073051	192.168.1.254	192.168.1.1	TCP	60	39514 → 80 [SYN] Seq=0 Win=3960 Len=0
49	0.073100	192.168.1.254	192.168.1.1	TCP	60	39514 → 80 [SYN] Seq=0 Win=2150 Len=0
50	0.073150	192.168.1.254	192.168.1.1	TCP	60	39514 → 80 [SYN] Seq=0 Win=3059 Len=0
51	0.073201	192.168.1.254	192.168.1.1	TCP	60	39514 → 80 [SYN] Seq=0 Win=727 Len=0
52	0.073250	192.168.1.254	192.168.1.1	TCP	60	43193 → 80 [SYN] Seq=0 Win=887 Len=0
53	0.073301	192.168.1.254	192.168.1.1	TCP	60	9045 → 80 [SYN] Seq=0 Win=1441 Len=0

Gambar 4.19 Hasil Akuisisi Data Log Traffic Router Internet.

Log traffic merupakan salah satu komponen penting dalam memperoleh informasi terkait aktivitas lalu lintas data pada jaringan. Informasi yang terdapat pada log traffic dapat berupa time, source, destination, protocol, length dan info seperti yang ditunjukkan pada gambar 4.19.

No.	Time	Source	Destination	Protocol	Length	Info
24	0.020270	29.169.243.34	192.168.1.1	TCP	60	22479 → 80 [SYN] Seq=0 Win=2039 Len=0
26	0.020379	29.169.243.34	192.168.1.1	TCP	60	48234 → 80 [SYN] Seq=0 Win=2649 Len=0
28	0.020477	29.169.243.34	192.168.1.1	TCP	60	17926 → 80 [SYN] Seq=0 Win=2061 Len=0
30	0.020574	29.169.243.34	192.168.1.1	TCP	60	14945 → 80 [SYN] Seq=0 Win=3547 Len=0
32	0.020632	29.169.243.34	192.168.1.1	TCP	60	8827 → 80 [SYN] Seq=0 Win=3822 Len=0
34	0.020724	29.169.243.34	192.168.1.1	TCP	60	5799 → 80 [SYN] Seq=0 Win=2604 Len=0
36	0.020821	29.169.243.34	192.168.1.1	TCP	60	16189 → 80 [SYN] Seq=0 Win=3471 Len=0
38	0.020923	29.169.243.34	192.168.1.1	TCP	60	60124 → 80 [SYN] Seq=0 Win=798 Len=0
40	0.021022	29.169.243.34	192.168.1.1	TCP	60	50846 → 80 [SYN] Seq=0 Win=401 Len=0
42	0.021121	29.169.243.34	192.168.1.1	TCP	60	41213 → 80 [SYN] Seq=0 Win=4020 Len=0
44	0.021218	29.169.243.34	192.168.1.1	TCP	60	41455 → 80 [SYN] Seq=0 Win=964 Len=0
46	0.021318	29.169.243.34	192.168.1.1	TCP	60	26368 → 80 [SYN] Seq=0 Win=1481 Len=0
48	0.021419	29.169.243.34	192.168.1.1	TCP	60	19111 → 80 [SYN] Seq=0 Win=368 Len=0
50	0.021517	29.169.243.34	192.168.1.1	TCP	60	32840 → 80 [SYN] Seq=0 Win=2847 Len=0
52	0.021614	29.169.243.34	192.168.1.1	TCP	60	32840 → 80 [SYN] Seq=0 Win=2372 Len=0
54	0.021743	29.169.243.34	192.168.1.1	TCP	60	32840 → 80 [SYN] Seq=0 Win=876 Len=0
56	0.021842	29.169.243.34	192.168.1.1	TCP	60	32840 → 80 [SYN] Seq=0 Win=240 Len=0
58	0.021938	29.169.243.34	192.168.1.1	TCP	60	32840 → 80 [SYN] Seq=0 Win=2432 Len=0
60	0.022671	29.169.243.34	192.168.1.1	TCP	60	44591 → 80 [SYN] Seq=0 Win=2232 Len=0
62	0.023777	29.169.243.34	192.168.1.1	TCP	60	28033 → 80 [SYN] Seq=0 Win=3565 Len=0

Gambar 4.20 Hasil Akuisisi Data Log Traffic Router Lokal.

Pada gambar 4.20 merupakan hasil akuisisi berupa file log traffic. Data hasil akuisisi ini kemudian akan analisis untuk mencari informasi yang diperlukan dalam proses penyelidikan. Didalam router, log activity dan log traffic sangat penting sebab data log ini dapat hilang apabila system dimatikan atau mengalami reboot.

#### 4.1.2.4 Analisis Forensik

Analisis forensik merupakan salah satu tahapan penting dalam mencari informasi yang terdapat pada data yang telah diakuisisi. Dalam tahapan ini, setelah melakukan akuisisi

dilanjutkan dengan menganalisis data hasil akuisisi tersebut. Analisis forensik akan dilakukan pada log activity dan log traffic.

Salah satu bukti digital yang paling penting dalam setiap aktifitas yang terjadi pada router adalah Log Activity. Aktifitas yang terjadi didalam router akan dicatat berdasarkan Time, Topic dan Message. Komponen tersebut memberikan informasi yang sangat penting untuk keperluan penyelidikan yang dilakukan oleh investigator dalam menemukan pelaku penyerangan.

Dalam simulasi kedua dilakukan penarikan log activity pada router internet dan router lokal. Gambaran hasil akuisisi data log activity yang telah diambil ditunjukkan pada gambar 4.17 dan gambar 4.18.

Gambar 4.17 menunjukkan adanya aktivitas tidak wajar dimana terjadi pengiriman paket SYN secara terus menerus kepada IP Router 192.168.1.1 dan menggunakan Port yang berbeda-beda. Adapun IP 192.168.1.251 merupakan IP dari router lokal. Sedangkan pada gambar 4.18 yang merupakan log activity dari router lokal menunjukkan adanya pengiriman paket syn kepada IP Router kedua yaitu 192.168.1.1 serta menggunakan port yang berbeda-beda. Adapun IP 29.169.243.34 memiliki MAC Address yaitu 08:00:27:eb:f5:30. Aktivitas yang terjadi pada router lokal mengindikasikan adanya aktivitas tidak wajar pada router tersebut.

Log traffic merupakan salah satu komponen penting dalam mengungkapkan aktivitas serangan yang terjadi pada router. Hal ini dikarenakan, log traffic merupakan hasil capture terhadap aktivitas yang terjadi dalam lalu lintas jaringan. Informasi yang ditampilkan dalam log traffic sangat penting dalam memperkuat apa yang telah ditemukan dalam log activity. Dalam log traffic, informasi yang disampaikan dapat berupa time, source, destination, protocol, length dan info.

Seperti halnya pada simulasi pertama, dalam simulasi kedua yang telah dilakukan menunjukkan informasi bahwa IP Address 192.168.1.251 melakukan pengiriman paket SYN secara terus menerus seperti pada gambar 4.19 kepada IP Address 192.168.1.1 yang mana IP tersebut merupakan IP Address Router internet.

Pada log traffic yang ditunjukkan router internet dalam simulasi kedua menampilkan informasi adanya IP Address yang melakukan pengiriman paket SYN kepada IP Address 192.168.1.1 yang merupakan IP dari router lokal. Adapun IP Address yang mengirimkan paket SYN secara terus menerus yaitu 29.169.243.34 seperti yang ditampilkan pada gambar 4.20.

Berdasarkan analisis yang dilakukan, informasi yang diperoleh dari Log Activity dan juga Log Traffic yang kemudian dikomparasikan dengan observasi pada router yaitu informasi IP Address yang tercatat pada router. Dalam Log Activity dan Log Traffic, IP Address 29.169.243.34 merupakan IP Address yang tidak terdaftar pada router. Namun pada IP Address 192.168.2.252 memiliki MAC Address yang sama dengan IP Address 29.169.243.34 yaitu 08:00:27:eb:f5:30. Berdasarkan temuan tersebut diindikasikan bahwa pelaku penyerangan berusaha menyembunyikan IP Address asli milik dirinya agar tidak ditemukan.

#### 4.1.2.5 Hasil Analisis

Berdasarkan hasil analisis serangan yang dilakukan diatas maka diperoleh alamat IP Address 192.168.2.252 berusaha menyembunyikan IP Address yang asli dengan mengubahnya menjadi 29.169.243.34 namun tidak dapat menyembunyikan MAC Address yaitu 08:00:27:eb:f5:30. IP Address tersebut melakukan serangan dengan mengirimkan paket SYN secara terus menerus dengan menggunakan Port yang berubah secara acak/random. Hal ini menjadi temuan dalam scenario penelitian dalam mendeteksi serangan *Flooding* pada router menggunakan metode *Live Forensics*.

#### 4.2 Hasil Analisis Serangan

Berdasarkan hasil analisis serangan yang dilakukan pada simulasi diatas, maka hasil tersebut dapat disajikan sebagai laporan forensik berdasarkan proses analisis yang telah dilakukan oleh peneliti. Adapun hasil analisis serangan secara keseluruhan akan dijelaskan pada tabel 4.1.

Tabel 4.1 Hasil Analisis Serangan

No	Analisis Temuan	Keterangan
1.	Traffik mengalami peningkatan drastis	Terjadi peningkatan traffic pada jaringan setelah serangan dilakukan baik pengiriman maupun penerimaan, hal ini dapat menyebabkan jaringan down.
2.	Terjadi peningkatan request pada protocol TCP SYN	Berdasarkan informasi yang tercatat pada log activity dan log traffic, telah terjadi peningkatan request pada protocol TCP SYN sehingga menyebabkan kepadatan pada router
3.	Port yang digunakan berubah-ubah atau acak	Dalam informasi yang tersimpan pada log activity dan log traffic, tercatat serangan yang dilakukan menggunakan port secara acak atau random



4.	Memiliki besaran paket yang sama pada setiap request	Besaran paket yang dikirim untuk melakukan serangan adalah 40 bytes pada log activity dan 60 bytes pada log traffic
5.	Terjadi peningkatan penggunaan resource pada router	Pada router yang diserang terjadi peningkatan penggunaan resource baik CPU maupun memory mengalami peningkatan penggunaan hingga 100%
6.	IP Address pelaku adalah 192.168.2.252	Pelaku serangan mengubah IP Addressnya menjadi 100.153.158.168 pada simulasi pertama dan 29.169.243.34 pada simulasi kedua. Pada akhirnya ditemukan bahwa IP Address sebenarnya adalah 192.168.2.252 setelah mencocokkan MAC Address yang tercatat pada ARP list dengan MAC Address pada log activity
7.	Tipe serangan flooding yang berhasil terdeteksi adalah SYN Flood	Serangan yang dilakukan tertuju pada protocol TCP SYN dengan cara membanjiri router dengan melakukan request paket SYN secara terus menerus

Proses investigasi yang telah dilakukan dengan menggunakan metode live forensic diketahui mampu mendeteksi adanya serangan flooding pada router. Hal ini berdasarkan informasi yang diperoleh dengan cara melakukan akuisisi atau penarikan log activity serta *men-capture* lalu lintas jaringan menggunakan paket sniffing yang terdapat pada aplikasi winbox. Hasil yang diperoleh menunjukkan bahwa ditemukannya paket SYN yang dikirim secara terus menerus oleh IP Address yang tidak terdaftar pada router. Penggunaan metode live forensic ini dipandang perlu dalam mendeteksi adanya aktifitas ilegal yang terjadi pada router, hal ini dikarenakan informasi yang terdapat pada router bersifat volatile sehingga ketika router melakukan restart atau mati maka informasi yang terdapat pada router tersebut akan hilang.

Hasil dari akuisisi atau penarikan data serta *capture* yang telah dilakukan pada router berupa log activity dan log traffic dapat dijadikan sebagai barang bukti digital. Hal ini dikarenakan didalam file log tersebut terdapat informasi yang dapat mengungkapkan aktivitas yang terjadi pada router seperti perubahan konfigurasi secara ilegal, pengiriman paket-paket serangan hingga usaha untuk menjebol router. Selain itu, file log juga terdapat informasi mengenai timestamp, interface, mac address, protocol, ip address, port dan lain sebagainya sehingga dapat menjadi bukti yang legal didalam persidangan.