Jurnal Riset Sains dan Teknologi
Volume 5 No. 1 Maret 2021, 31 - 38
e-ISSN: 2549-9750
p-ISSN: 2579-9118

Forensik Router untuk Mendeteksi Flooding Attack Menggunakan Metode Live Forensic

Router Forensics to Detect Flooding Attack using Live Forensics Method

Ilman Pradhana[1], Imam Riadi[2], Yudi Prayudi[3]
[1,3] Program Studi Teknik Informatika, Fakultas Teknologi Industri
Universitas Islam Indonesia, Yogyakarta
[2] Program Studi Sistem Informasi
Universitas Ahmad Dahlan, Yogyakarta
email: [1]16917104@students.uii.ac.id, [2]imamriadi@is.uad.ac.id, [3]prayudi@uii.ac.id

DOI;
10.30595/jrst.v5i1.7662

Histori Artikel:

Diajukan:
25/06/2020

Diterima:
05/03/2021

Diterbitkan:
27/03/2021

ABSTRAK

Teknologi informasi di era saat ini menunjukkan perkembangan yang pesat khususnya dalam bidang komputer berbasis jaringan. Di sisi lain, terdapat beberapa oknum-oknum tertentu yang menyalahgunakan teknologi tersebut salah satunya dengan melakukan serangan pada jaringan komputer. *Router* merupakan perangkat jaringan yang dapat membuat jaringan lokal bisa terhubung ke jaringan public. *Router* seringkali menjadi target serangan, hal ini dikarenakan *Router* menjadi jalur lalu lintas pengiriman data. *Flooding Attack* merupakan salah satu serangan pada jaringan komputer. Serangan yang dilakukan bertujuan membanjiri lalu lintas data pada jaringan sehingga dapat menyebabkan jaringan menjadi *down* (lumpuh) diakibatkan kelebihan beban. Untuk mendeteksi *Flooding Attack* diperlukan beberapa alat seperti Winbox yang digunakan untuk mendapatkan *Log Activity, Log Traffics* dan *Ip Address* serta Wireshark sebagai alat untuk mencari informasi yang terdapat pada *Log Traffic* yang dapat digunakan sebagai bukti digital dengan menggunakan metode *Live Forensic*s. Dalam penelitian ini, informasi yang akan digali adalah *Log Activity*, *Log Traffic*s dan *IP Address*. Untuk memperoleh informasi tersebut, maka dilakukan beberapa simulasi serangan pada *Router*. Dari simulasi yang dilakukan terjadi peningkatan signifikan pada lalulintas jaringan *Router* serta penggunaan sumber daya yang juga meningkat. Adapun output dari penelitian ini yaitu menemukan dan menarik data-data penting yang merupakan bukti digital berupa *Log Activity* serta *Log Traffic*. Informasi yang diperoleh pada file log tersebut yaitu ditemukan adanya IP Address yang terdeteksi melakukan serangan yaitu IP Address 192.168.2.252. Beberapa informasi yang terdapat pada log file yang telah ditarik juga dapat dijadikan sebagai barang bukti dalam persidangan**.**

Kata Kunci: Flooding Attack, Live Forensics, Routers, Log Activity, Log Traffics

ABSTRACT

.

Information technology in the current era shows rapid development, especially in the field of network-based computers. On the other side, there are certain elements who misuse the technology,

one of which is by carrying out attacks on computer networks. A router is a network device that can make a local network connected to a public network. Routers are often the target of attacks, because Routers are the path for sending data. Flooding Attack is an attack on a computer network. The attack carried out aimed at flooding data traffic on the network so that it can cause the network to be down due to overload. To detect Flooding Attack, we need several tools such as Winbox that is used to get the Log Activity, Log Traffics and Ip Address and Wireshark as a tool to search for information contained in Traffic Logs that can be used as digital evidence using the Live Forensics method. In this study, the information that will be extracted is the Log Activity, Log Traffics and IP Address. To obtain this information, a series of attack simulations are carried out on the router. From the simulations conducted there was a significant increase in Router network traffic and resource usage which also increased. The output of this research is finding and pulling important data which is digital evidence in the form of Activity Log and Traffic Log. The information obtained in the log file is found the presence of an IP Address that was detected carrying out an attack namely IP Address 192.168.2.252. Some information contained in the log file that has been withdrawn can also be used as evidence in the court.

Keywords: Flooding Attack, Live Forensics, Routers, Log Activity, Log Traffics

1. PENDAHULUAN

Pesatnya perkembangan teknologi informasi dan komunikasi di era saat ini terutama dalam bidang komputer berbasis jaringan. Bidang ini memberi kemudahan bagi para pengguna dalam proses penyampaian maupun memperoleh informasi. Namun, di balik semua itu masih terdapat pihak-pihak tertentu yang menyalahgunakan teknologi untuk mengambil data tanpa izin ataupun merusaknya dengan cara melakukan serangan pada jaringan komputer.

Serangan pada jaringan komputer atau yang biasa disebut *Network Attack* ini, dapat dilakukan oleh pihak dalam maupun pihak luar. Tujuannya pun berbeda-beda, beberapa di antaranya melakukan serangan hanya sekedar untuk mencoba tools yang ditemukan di internet namun ada beberapa juga yang melakukan serangan dengan tujuan saling menjatuhkan satu sama lain dalam konteks persaingan bisnis. Teknik serangan yang dilakukan pun bermacam-macam, beberapa diantaranya seperti *DoS (Denial of Service), Server Message Block, Browser, Brute Force, Web, DNS, Scan* dan *SSL.*

Teknologi informasi dan komunikasi di bagian jaringan komputer masih rentan terhadap serangan. Serangan dilakukan dengan memanfaatkan celah yang ada pada perangkat jaringan yang digunakan. Dari serangan yang dilakukan dapat mengakibatkan akses pada website menjadi lambat, terjadinya flooding data serta pencurian informasi dan data melalui jaringan internet. Salah satu akibat yang ditimbulkan dapat membuat perangkat jaringan yang digunakan menjadi down.

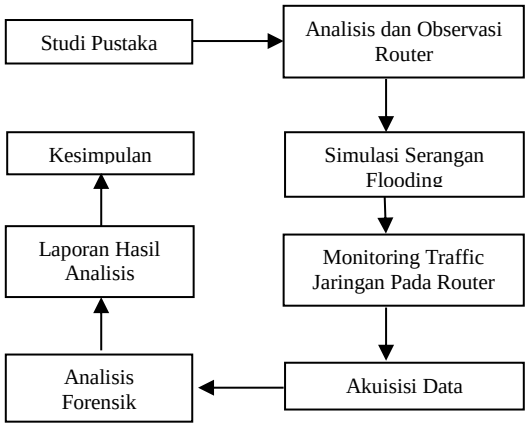
Serang *DoS (Denial of Service)* tipe *Syn* atau yang biasa disebut *Syn Flood* merupakan yang paling sering dilakukan. *Router* merupakan perangkat jaringan yang sering diserang. Hal ini dikarenakan *Router* merupakan perangkat yang mengatur lalu lintas pengiriman paket data ke perangkat lain melalui jaringan internet. Beberapa *Router* menggunakan system operasi berbasis linux yang dapat digunakan sebagai pengatur jaringan. *Router* memiliki hak akses penuh dalam mengatur pengendalian lalu lintas pada jaringan. Hal ini dikarenakan *Router* memiliki banyak fungsi di dalamnya sehingga menjadikan *Router* sebagai target utama karena perannya yang sangat penting dalam jaringan.

Dalam perkembangan teknologi saat ini, terdapat studi ilmu yang mempelajari hal tersebut. *Network forensic* merupakan salah satu cabang ilmu yang mempelajari keamanan jaringan termasuk menyelidiki serangan yang terjadi pada sebuah jaringan berdasarkan bukti digital yang ditemukan di lokasi kejadian. Bukti digital yang ditemukan kemudian akan di identifikasi untuk mengetahui serangan yang dilakukan oleh penyerang. Salah satu metode yang bisa dilakukan untuk melakukan identifikasi yaitu metode *Live Forensic*s.

Bukti digital dapat ditemukan dalam file *Log Activity, Log Traffic* dan *IP Address.* Informasi yang terdapat di dalam file tersebut dapat digunakan sebagai barang bukti untuk di gunakan dalam persidangan.

2. METODE PENELITIAN

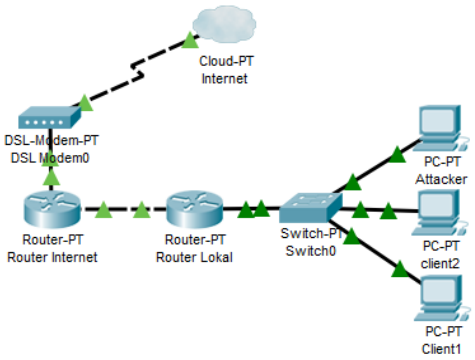
Adapun tahapan pelaksanaan dalam penelitian ini seperti pada Gambar 1



Gambar 1. Alur Penelitian.

A. 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. 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 2

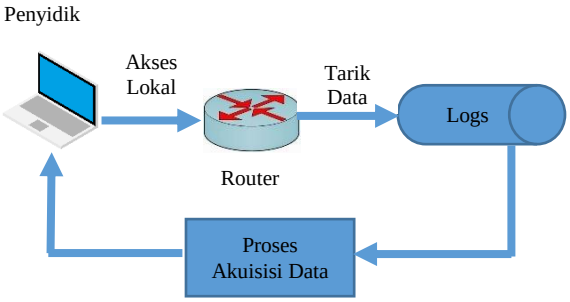


Gambar 2. Simulasi Serangan

Simulasi serangan akan dilakukan dalam jaringan yang menggunakan dua buah *Router* untuk kemudian *Router* yang terhubung langsung ke internet yang akan di serang. 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* diterima oleh clien, maka client akan mengirimkan paket *ACK* sebagai tanda proses pengiriman atau penerimaan data akan dimulai.

B. Tahapan Akuisisi

Adapun tahapan akuisisi yang akan dilakukan dalam penelitian ini akan dijelaskan pada Gambar 3



Gambar 3. Tahapan Akuisisi Secara *Live Forensics*.

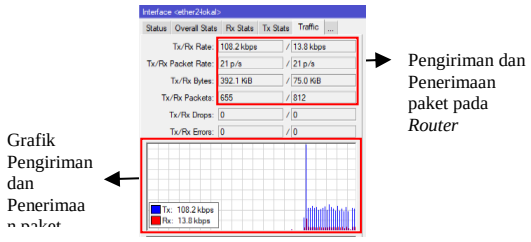
Dalam tahapan ini kondisi utama yang harus terpenuhi dalam menggunakan metode *Live Forensics* yaitu di mana system sedang dalam keadaan beroperasi/running. Hal ini dikarenakan beberapa informasi serangan yang ada pada jaringan *Router* akan hilang jika system tersebut dimatikan ataupun dilakukan reboot,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

3. HASIL DAN PEMBAHASAN

Dalam tahapan ini akan dilakukan simulasi serangan yang kemudian akan dilanjutkan dengan analisis serta observasi pada *Router*, *monitoring traffic*, akuisisi file *log*, analisis forensik dan hasil analisis. Berdasarkan gambaran scenario simulasi yang ditunjukkan sebelumnya pada Gambar 2, maka akan dilakukan serangan *Syn Flood* pada *Router*.

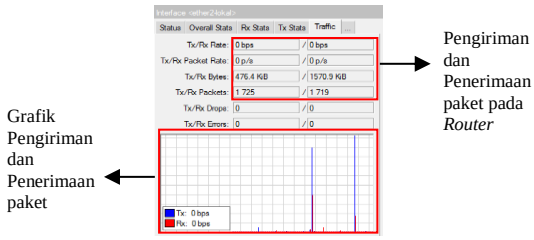
A. Analisis dan Observasi Router

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



Gambar 4. Tampilan traffic sebelum ada serangan pada *Router* local.

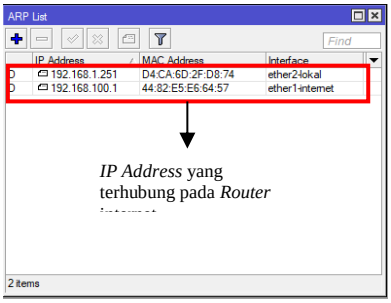
Gambar 4 menunjukkan traffic pada *Router* lokal berjalan dengan normal. Hal ini terlihat dari pengiriman dan penerimaan paket yang tidak terlalu besar serta tidak terlalu padat.



Gambar 5. Tampilan traffic sebelum ada serangan pada *Router* internet.

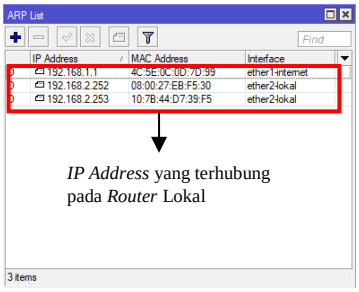
Berdasarkan Gambar 5, dapat diketahui bahwa belum ada serangan terhadap *Router* lokal dan *Router* internet serta aktivitas lalulintas jaringan pada kedua *Router* berjalan normal. Hal ini berdasarkan informasi pada Tx/Rx Rate yang masih dalam keadaan normal dan belum terlihat padat.

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



Gambar 6. ARP List Pada *Router* Internet.

Pada Gambar 6 ditunjukkan 2 *IP Address* yang terhubung pada *Router* internet. IP 192.168.100.1 merupakan *IP Address* yang terhubung langsung dengan internet, sedangkan *IP Address* 192.168.100.251 merupakan IP dari *Router* lokal. Setiap IP memiliki *MAC Address* yang berbeda sehingga dapat dimanfaatkan sebagai informasi.



Gambar 7. 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.*

B. Simulasi Serangan

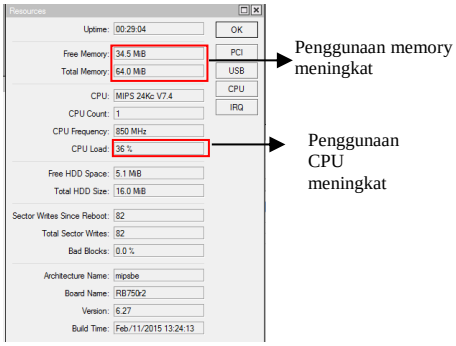
Pada tahap ini, simulasi serangan akan dilakukan menggunakan aplikasi metasploit. Metasplot merupakan salah satu tools pengujian penetrasi terkemuka saat ini dan juga salah satu proyek open-source terbesar dalam hal keamanan informasi serta pengujian penetrasi. Adapun tools ini dapat digunakan hampir disemua sistem operasi. Dalam simulasi serangan ini, attacker akan menyerang *Router* yang terhubung ke internet dengan cara seperti pada gambar 8.

Gambar 8. Simulasi Serangan *Syn Flood*.

Dalam gambar 8 dijelaskan rhost 192.168.1.1 yang memiliki arti bahwa alamat *IP Address* target yaitu 192.168.1.1. Adapun exploit memiliki arti exploitasi atau dapat diartikan serangan dijalankan. Dari perintah diatas menunjukkan bahwa serangan *Syn Flood* telah dilaksanakan, untuk tahapan selanjutnya akan dilakukan monitoring trafik dan akuisisi.

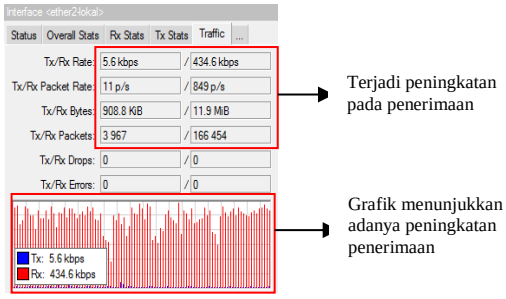
C. Monitoring Trafik dan Akuisisi

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 lalulintas pada *Router* internet dan juga *Router* lokal menggunakan fitur *Packet Sniffer* yang terdapat pada tool Winbox untuk kemudian akan dianalisis menggunakan aplikasi Wireshark serta memantau aktivitas yang terdapat pada kedua *Router* melalui aplikasi winbox.



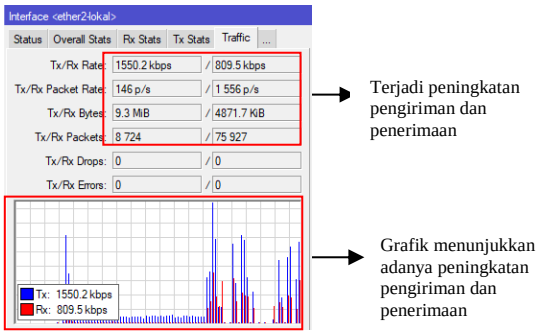
Gambar 9. Pemantauan Resource *Router* Internet.

Dalam Gambar 9 menunjukkan terjadi peningkatan penggunaan memory dan juga CPU. Hal ini terjadi karena meningkatnya aktivitas lalulintas data pada *Router* yang diakibatkan serangan yang dilakukan. Aktivitas tersebut dapat menyebabkan *Router* mengalami kelebihan beban dan akan melakukan reboot pada system.



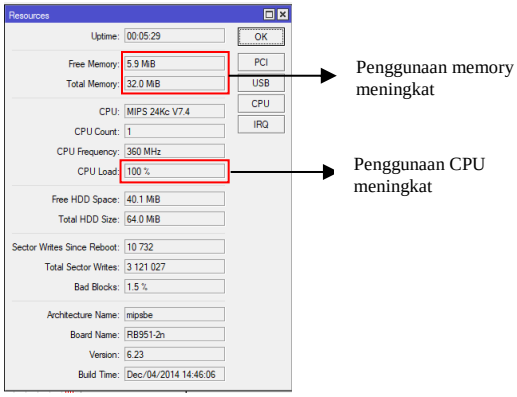
Gambar 10. Pemantauan Traffic *Router* Internet.

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 10.



Gambar 11. Pemantauan traffic pada *Router* lokal.

Ketika *Router* internet mengalami peningkatan traffic dalam pengiriman paket. Hal sebaliknya terjadi pada *Router* local, berdasarkan gambar 11 menunjukkan bahwa terjadi peningkatan traffic tidak hanya penerimaan paket namun juga pengiriman paket. Peningkatan ini terjadi ketika serangan dilakukan pada *Router* internet.



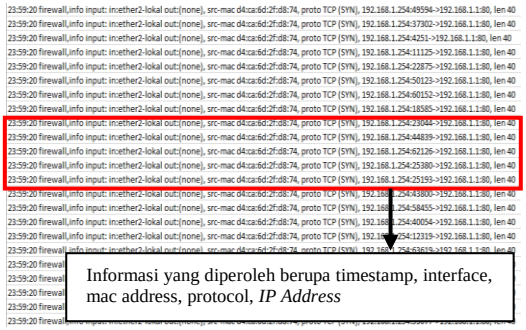
Gambar 12. Pemantauan Resource *Router* lokal.

Selain lalulintas jaringan ikut meningkat, penggunaan sumber daya pada *Router* lokal mengalami peningkatan yang signifikan. Hal ini terlihat pada gambar 12 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.

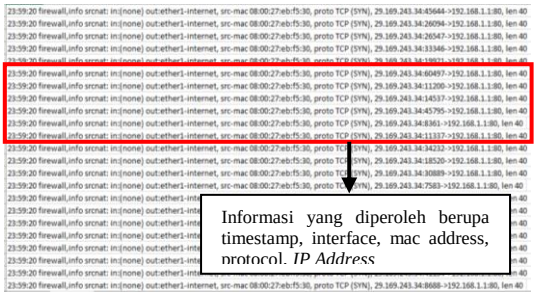
Untuk bisa melakukan proses metode *Live Forensic* kondisi yang harus dipenuhi yaitu dimana system sedang dalam keadaan hidup, hal

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*.



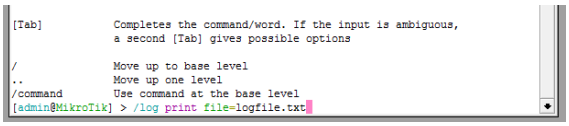
Gambar 13. Hasil Akuisis Data *Log Activity Router* Internet.

Gambar 13 menunjukkan hasil akusisi *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*.



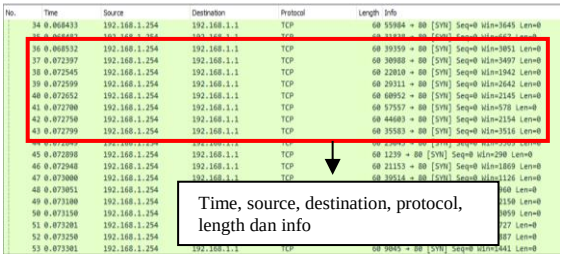
Gambar 14. Hasil Akuisisi Data *Log Activity Router* Lokal.

Pada Gambar 14 menunjukkan hasil akuisisi data *Log Activity* pada *Router* local. Informasi yang ditampilkan dari log tersebut berupa *timestamp, interface, mac address, protocol* dan *IP Address*. Proses penarikkan *Log Activity* dilakukan menggunakan tool Winbox dengan cara memasukkan perintah pada terminal seperti yang ditunjukkan pada Gambar 15



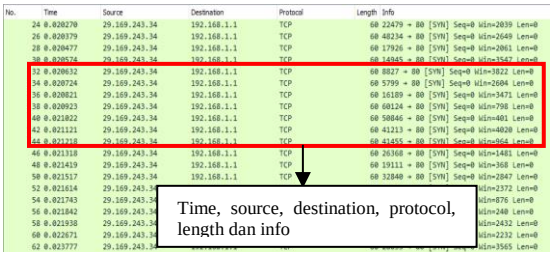
Gambar 15. Hasil Akuisisi Data Log Traffic Router Internet.

Gambar 15 menunjukkan bagaimana mengakuisisi file *Log Activity* dengan menggunakan perintah *print* pada terminal. Hal ini bertujuan agar segala aktivitas yang terjadi pada *router* dapat segera di simpan. Di sisi lain, aktivitas yang tercatat pada *router* akan terhapus secara otomatis ketika *router* dalam keadaan mati atau melakukan *reboot.*



Gambar 16. Hasil Akuisisi Data *Log Traffic Router* Internet.

Log Traffic merupakan salah satu komponen penting dalam memperoleh informasi terkait aktivitas lalulintas data pada jaringan. Informasi yang terdapat pada *Log Traffic* dapat berupa *time, source, destination, protocol, length* dan info seperti yang ditunjukkan pada Gambar 16.



Gambar 17. Hasil Akuisisi Data *Log Traffic Router* Lokal.

Pada Gambar 17 menunjukkan hasil akuisisi berupa file *Log Traffic*. Data hasil akuisisi ini di peroleh setelah melakukan *capture* menggunakan *Packet Sniffer* yang terdapat pada tool Winbox kemudian akan dilakukan analisis

untuk mencari informasi yang diperlukan dalam proses penyelidikan menggunakan aplikasi Wireshark. Di dalam *Router*, *Log Activity* dan *Log Traffic* sangat penting sebab data log ini dapat hilang apabila system dimatikan atau mengalami reboot.

D. 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 tersebut dilakukan penarikan *Log Activity* pada *Router* internet dan *Router* lokal. Gambaran hasil akuisisi data *Log Activity* yang telah diambil ditunjukkan pada Gambar 13 dan Gambar 14.

Gambar 13 menunjukkan adanya aktivitas tidak wajar di mana 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 14 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 lalulintas 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.

Pada simulasi ini ditemukan informasi bahwa *IP Address* 192.168.1.251 melakukan pengiriman paket *SYN* secara terus menerus seperti pada Gambar 16 kepada *IP Address* 192.168.1.1 yang mana IP tersebut merupakan *IP Address Router* internet.

Pada *Log Traffic* yang ditunjukkan *Router* internet 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 17.

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. KESIMPULAN

Selama proses penelitian serta melakukan simulasi serangan *Flooding* pada *Router*, menganalisis serta menarik data forensik, maka dapat disimpulkan dari penelitian ini yaitu :

- Penerapan metode *Live Forensic* mampu mendeteksi adanya serangan pada router berdasarkan informasi yang di peroleh dari hasil akuisisi file *log activity* dan juga hasil *capture* terhadap lalu lintas jaringan menggunakan *paket sniffing* yang terdapat pada aplikasi winbox.
- Dalam proses akuisisi data pada *Router* menggunakan metode *Live Forensics*, ditemukan adanya aktivitas yang tidak wajar pada *Router* melalui protocol TCP dengan *IP Address* 29.169.243.34 dan setelah diidentifikasi melalui ARP List tidak ditemukan *IP Address* tersebut namun terdapat *IP Address* yang memiliki MAC Address yang sama yaitu IP 192.168.2.252

- yang mana *IP Address* tersebut merupakan IP asli penyerang. Hal ini berdasarkan informasi yang didapatkan melalui *Log Activity*, *Log Traffic* dan *ARP List* sehingga informasi ini dapat digunakan sebagai bukti digital.

DAFTAR PUSTAKA

Al-Azhar, M. N. (2012). Digital Forensic: Panduan Praktis Investigasi Komputer. Jakarta: Penerbit Salemba Infotek.

Fadlil, A., Riadi, I., & Aji, S. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *J. Ilmu Tek. Elektro Komput dan Inform.,* vol. 3, no. 1, pp. 12-19.

Mazdadi, M. I., Riadi, I., & Luthfi, A. (2017). *Live Forensic*s on *Router*OS using API Services to Investigate Network Attacks. *International Journal of* Komputer *Science and Information Security (IJCSIS)*, *15*(2), 406–410.

Ahmad, M. S., Riadi, I., & Prayudi, Y. (2017). Investigasi Live Forensik dari Sisi Pengguna untuk Menganalisa Serangan Man In The Middle Attack Berbasis Evil Twin. *ILKOM Jurnal Ilmiah, 9(1), 1-8.*

Zulkifli. M. A., Riadi, I., & Prayudi, Y. (2018). *Live Forensic*s Method for Analysis Denial of Service (DoS) Attack on *Router*board. *International Journal of* Komputer *Applications (IJCA), 180(35), 23-30.*

Hildayanti, N., & Riadi, I. (2019). Forensics Analysis of *Router* on Komputer Network Using *Live Forensic*s Method. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 8(1), 74-81.*

Widodo, S. (2012). Pemantauan Jaringan Komputer dengan DNS Server berbasis Routing Statis Menggunakan Wireshark. *Jurnal Teknik Elektro Terapan (JTET), 1(2), 1-7.*

Casey, E. (2010). *Handbook of Digital Forensics and Investigation.* London: Elsevier Inc

.