JURNAL TIMES
TECHNOLOGY INFORMATICS & COMPUTER SYSTEM

Volume VI No 2, Desember 2017
*p*ISSN : 2337 – 3601
*e*ISSN : 2549 – 015X

Tersedia *online* di http://ejournal.stmik-time.ac.id

Implementasi Log Dalam Forensik Router Terhadap Serangan Distributed Denial of Service(DDoS)

Faizin Ridho [1)] Anton Yudhana [2)] Imam Riadi[3)]
Magister Teknik Informatika [1,2,3)]
Universitas Ahmad Dahlan[1,2,3)]
Yogyakarta, Indonesia[1,2,3)]
e-mail : faizin1607048009@webmail.uad.ac.id[1], eyudhana@mti.uad.ac.id[2] , imam.riadi@mti.uad.ac.id[3]

Abstrak
Serangan *Distributed Denial of Service* (DDoS) merupakan ancaman serius terhadap keamanan jaringan khusus di *router* yang mengakibatkan penghentian koneksi, konfigurasi yang hilang yang mempengaruhi semua komunikasi dan transaksi menjadi terhambat dengan kerugian banyak pihak dan memungkinkan untuk masuk pada sistem. Langkah pertama yang harus dilakukan adalah merancang dan membangun sistem deteksi yang melibatkan sistem deteksi intrusi seperti mendengus. Pemanfaatan *snort* sangat berguna untuk merekam serangan DDoS serta data lalu lintas yang ada di *router* yang tersimpan di *log*. Analisis forensik dilakukan dengan menggunakan *log* untuk penyelidikan dengan metode forensik untuk menemukan bukti adanya serangan. Hasil penelitian menunjukkan bahwa dengan memanfaatkan *Basic Analysis and Security Engine* dan *wireshark* yang mampu mendeteksi serangan dengan menggunakan *rule* yang ada pada snort yang menjadi dasar bukti adanya serangan.
Kata Kunci : *Network Forensics, Router, Intruction Detection System (IDS), DDoS.*.

1. Pendahuluan

Perkembangan teknologi yang telah terbuka bebas, hacker telah berevolusi dengan teknik menurunkan kinerja server Anda dengan membanjiri lalu lintas jaringan. Terlepas dari upgrade perangkat keras yang telah Anda lakukan untuk meningkatkan kinerja server Anda, peretas masih dapat mensimulasikan lebih banyak pengguna dari pada yang dapat ditangani oleh server.

Data IDSIRTI yang dikutip Aidil menyatakan jumlah total serangan kedalam jaringan 135,6 juta serangan (2016) kenaikan 50% dibandingkan dengan 2015. Port 53, DNS yang paling banyak mendapatkan serangan dengan sumber serangan majoritas dari AS, China dll. jenis serangan yang berbahaya DDOS dan Serangan paling banyak terjadi bulan April 45.5 juta. Insiden yang paling banyak adalah dari Malware[1].

Peningkatan ancaman dan serangan terhadap keamanan sistem meningkat karena didukung oleh kemudahan akses dan ketersediaan sumber daya yang lebih mudah di dapatkan. pengetahuan mengenai hacking yang terbuka luas di *internet*, *tools* yang dapat diakses secara bebas menjadikan pelaku mudah untuk melakukan tindakan untuk mendapatkan informasi untuk di jadikan sebagai target kejahatan.

Banyak tahapan yang di lakukan seorang pelaku kejahatan *cyber* untuk memuluskan langkahnya mendapatkan informasi sebanyak mungkin pada target salah satunya adalah DDoS. Untuk memuluskan langkahnya biasanya seorang pelaku kejahatan *cyber* yaitu dengan menggunakan metode untuk membanjiri *source* pada perangkat jaringan.

Router merupakan bagian dari perangkat vital dalam sebuah jaringan yang mampu bekerja sebagai lapisan keamanan. Salah satu keamanan yang sering digunakan adalah *filtering* dengan *Mac Address* yang menyebabkan *device mac address* nya bisa terkoneksi. Hal ini menyebabkan hanya *device* yang didaftarkan *Mac Address* nya lah yang bisa mengakses jaringan. *Mac Addess filtering* sangat berguna untuk menyulitkan hacker untuk menyusup pada jaringan. Dalam hal ini, Teknik DDoS lah yang sering digunakan untuk menurunkan kinerja *router* hingga *hacker* dapat melakukan penyadapan dengan merubah *Mac Address* pelaku dengan *Mac Address* yang terdaftar pada tabel router dengan teknik scaning menggunakan beberapa *tools* yang tersedia bebas di internet.

Dalam rangka mengurangi ancaman keamanan pada jaringan, administrator harus menggunakan berbagai strategi keamanan yang jitu dengan audit sistem secara berkala dengan mengelola *log*. Umumnya pada setiap sistem memiliki log untuk mencatat peristiwa pada setiap perangkat. Data log mengambil peran penting dalam mengungkap suatu tindak kriminal yang terjadi di dunia *cyber*.

Di era teknologi informasi, terdapat bidang forensik jaringan (network Forensics) yang mampu membuktikan tindak kejahatan berdasarkan serangkaian tahapan seperti mengidentifikasi, menguji, menganalisis, serta dapat mendokumentasikan bukti yang terdapat pada sumber serta hasil Analisa yang dilakukan. Forensik jeringan dirasa perlu dilakukan dengan tujuan membantu administrator jaringan untuk mempermudah dalam menemukan serangan yang biasanya di lakukan secara manual. Pada sistem keamanan jaringan *Intrusion Detection System* di rancang untuk mencatat segala kejadian yang ada pada sistem. Desain dan implementasi forensik log perlu dilakukan dengan tujuan untuk menemukan bukti berdasarkan sumber serangan, waktu kejadian, serta dampak dari serangan distributed denial of service pada router.

2. Landasan Teori

A. Kajian Peneliti Terdahulu

Penelitian yang pernah dilakukan[2] dengan judul *Network Forensics For Detecting Flooding Attack On Web Server* yaitu melakukan Analisa forensik yang terjadi pada web server universitas muhammadiyah magelang yang sebagian besar terejadi serangan flooding.

Imam Riadi[3] dengan judul "*Log Analysis Techniques using Clustering in Network Forensics*" yaitu Proses dari mengidentifikasi serangan yang terjadi juga membutuhkan dukungan dari kedua hardware dan software juga. Serangan itu terjadi di jaringan internet secara umum dapat disimpan dalam file log yang memiliki format data yang spesifik. Teknik Clustering merupakan salah satu metode yang dapat digunakan untuk mempermudah proses identifikasi. Memiliki dikelompokkan file data log menggunakan metode K-Means dengan teknik klastering, kemudian data tersebut dikelompokkan menjadi tiga kategori serangan, dan akan dilanjutkan dengan proses forensik yang nantinya dapat diketahui sumber dan target serangan yang ada dalam jaringan. Ini menyimpulkan bahwa kerangka yang diusulkan dapat membantu penyidik dalam proses persidangan.

S.T.Shenbagavalli telah melakukan penelitian dengan judul "*Router Interface Based Ip Traceback Method For DDoS Attack In Ipv6 Networks"*. Pada penelitian ini, penulis menggunakan metode *IP Traceback* untuk menemukan pelaku serangan DDoS yang mampu menyembunyikan identitasnya menggunakan teknik *Spoofing* pada perangkat router dengan IPv6[4].

B. Network Forensics

Forensik jaringan adalah kegiatan untuk merekam dan menganalisa peristiwa yang terjadi dalam jaringan untuk menemukan sumber serangan dan peristiwa lainnya[5]. Dengan kata lain, tahapan forensik dilakukan dengan merekam dan menganalisa lalu lintas data yang tercatat pada *intrusion detection system.* Jaringan data berasal dari peralatan jaringan seperti *router, firewall, snort*, dilakukan proses analisa pada *log* untuk menemukan karakteristik serangan serta melacak pelaku serangan.

C. Router

Router merupakan perangkat jaringan komputer yang bertujuan sebagai penghubung antara jaringan luar (public) dengan jaringan dalam (local) dan dapat di jadikan sebagai gerbang (gateway) untuk meneruskan paket data antara dua atau lebih jaringan yang berbeda agar keduanya dapat saling berkomunikasi[6]. Semisal menghubungkan dua jaringan komputer yang berbeda kelas pada IP Address.

D. Elemen Ancaman Keamanan

Serangan terhadap kemanan sistem informasi dapat dilihat dari sudut peranan komputer yang fungsinya adalah sebagai penyedia informasi[7]. Ada beberapa kemungkinan serangan yaitu:

1. Interruption
   Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan pada ketersediaan dari sistem sehingga informasi dan data yang ada dalam sistem komputer dirusak dan dihapus, hal ini berdampak saat informasi dan data dibutuhkan maka data dan informasi tersebut tidak ada lagi. Contoh serangan adalah " Distributed Denial of Service Attack".
2. Interception
   Merupakan ancaman terhadap kerahsiaan. Pihak yang tidak berwenang berhasil mengakses aset dan informasi dimana informasi tersebut disimpan. Contoh dari serangan ini adalah penyadapan (wiretapping).
3. Modification
   Merupakan ancaman terhadap integritas. Pihak yang tidak berwenang tidak saja berhasil mengakses, tetapi dapat juga mengubah data. Contoh dari serangan ini adalah mengubah pesan dari website dengan pesan yang merugikan pemilik website
4. Fabrication
   Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil memalsukan suatu informasi yang ada sehingga orang lain yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh penerima pesan tersebut.

E. Intrusion Detection System (IDS)

Intrusion Detection System atau disingkat IDS[9] adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).Terdapat dua jenis IDS, yaitu :

1. Host-Based Intrusion Detection System (HIDS)

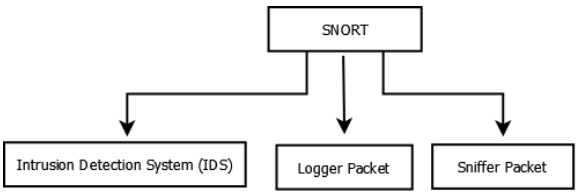
Host-Based IDS memperoleh informasi dari data yang dihasilkan oleh system pada sebuah komputer yang diamati. Data Host-Based IDS biasanya berupa log yang dihasilkan dengan memonitor system file, event, dan keamanan pada Windows NT dan syslog pada lingkungan system operasi UNIX. Saat terjadi perubahan pada log tersebut, dilakukan analisis untuk mengetahui apakah sama dengan pola yang ada pada database IDS.

2. Network-Based Intrusion Detection System (NIDS)
   Network IDS menempati jaringan secara langsung dan melihat semua aliran yang melewati jaringan. Network-Based IDS merupakan strategi yang efektif untuk melihat traffic masuk / keluar maupun traffic diantara host ataupun diantara segmen jaringan lokal.

F. Snort

Snort adalah software open source yang berguna untuk mendeteksi intruksi pada sistem, mampu menganalisa lalu lintas data secara real-time pada IP Address. Mampu mendeteksi serangan berdasarkan anomaly detection maupun misuse detection untuk menemukan segala ancaman serangan. Cara kerja Snort dibedakan berdasarkan berdasarkan Gambar 1. ada tiga mode paket Yaitu :

1. Sniffer Packet
   Mode ini bertugas untuk memonitoring atau melihat lalu lintas data yang ada pada jaringan komputer.
2. Logger Packet
   untuk mencatat semua paket yang lewat di jaringan untuk di Analisa untuk menemukan bukti dalam proses forensic jaringan.
3. Intrusion Detection Mode
   pada mode ini snort akan berfungsi untuk mendeteksiserangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini di perlukan setup dari berbagai rules / aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.



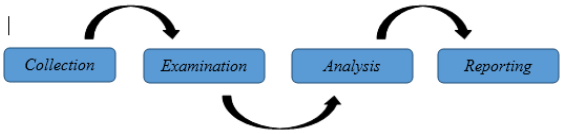
Gambar 1. Snort Mode

3. Metode Penelitian

Metode penelitian dilakukan dengan beberapa bagian diantaranya :

A. Tahap Penelitian

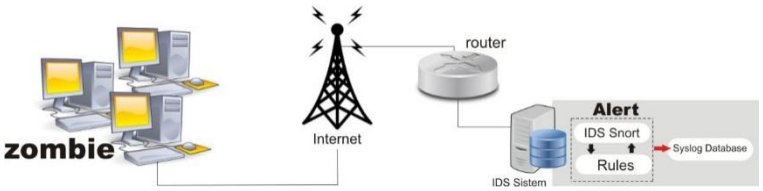
Serangan DDoS dapat dianalisa dengan memanfaatkan system deteksi serangan yaitu *Intrusion Detection System* (IDS) Snort. Konfigurasi dilakukan untuk mendeteksi serangan pada *router* menggunakan IDS Snort, tahap selanjudnya adalah menguji apakah IDS telah berhasil terinstal. Alart pada snort bekerja untuk mendeteksi serangan berdasarkan anomaly yang terdapat pada Snort. File Log pada snort dapat disimpan dalam format p.cap yang menjadi dasar untuk di analaisa agar memperoleh hasil dari bukti forensik terhadap serangan yang di lakukan pada router. Proses Analisa di lakukan berdasarkan metode forensik yaitu *Collection, Examination, Analysis, Reporting* seperti pada gambar 2. berikut :



Gambar 2. Metode Forensik

B. Simulasi Serangan

Simulasi serangan dilakukan berdasarkan skerion dengan mengirimkan paket ICMP *syn flooding* guna menguji apakah konfigurasi Intrusion Detection System (IDS) pada router sudah berjalan sesuai dengan yang diharapkan. Simulasi serangan dilakukan dengan menggunakan tools *Nmap* untuk mengguji melalui *Syn flooding* serta hping3 guna mengirim paket yang banyak terhadap router.



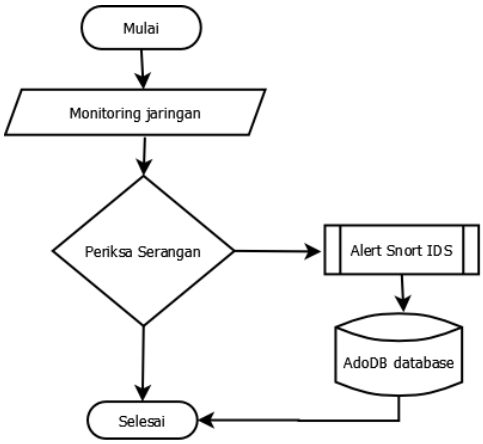
Gambar 3. Skenario Serangan Pada Router

Pada gambar 3. Dilakukan skenario dengan mengirimkan paket syn kepada router melalui komputer yang terhubung dengan internet dengan menggunakan alat *hping3* dan *nmap*. Pengujian menggunakan skenario tersebut bertujuan untuk mengetahui alert pada IDS yang telah di pasang pada router.

4. Hasil Penelitian

A. Mekanisme Deteksi Serangan

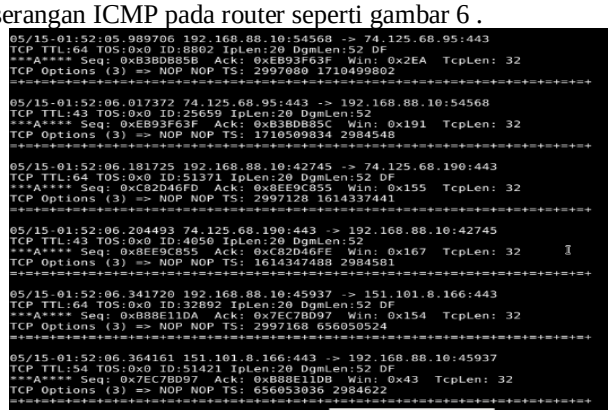
Snort pada *Intrusion Detection System* (IDS) dimanfaatkan untuk mendeteksi serangan guna penyelidikan forensik dengan memeriksa file *log* maupun *database* yang tersimpan. Menerjemahkan aturan *snort* ke dalam *iptables* dan menghasilkan *shell script* yang dapat digunakan untuk penerapan hasil *monitoring* pada *router*. Mekanisme deteksi akan dilakukan berdasarkan tahapan pada gambar 4.



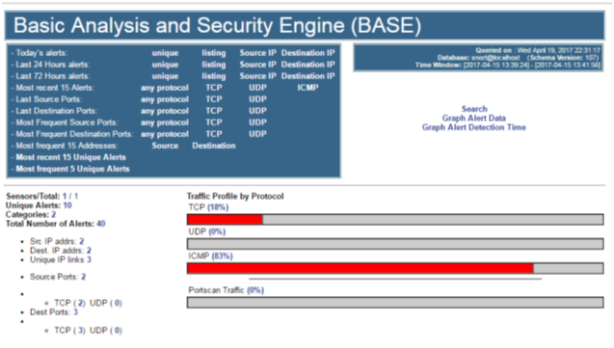
Gambar 4. Tahapan Penelitian

B. Implementasi IDS Sistem

Pada bagian ini administrator melakukan simulasi serangan dengan mencoba melakukan serangan pada target kemudian IDS bertugas mendetesi serangan dengan mencocokan *rule* yang telah tersedia pada pada *snort*. dengan melihat catatan lalu lintas jaringan pada snort pada router seperti terlihat pada gambar 5. Kemudian rule snort akan bertugas mendeteksi apabila terjadi serangan, selanjudnya data serangan di simpan melalui *Basic Analysis and Security Engine* (BASE) pada IDS. Berdasarkan simulasi yang dilakukan BASE mencatat bahwa terjadi serangan ICMP pada router seperti gambar 6 .



Gambar 5. Monitoring Jaringan Menggunakan Snort

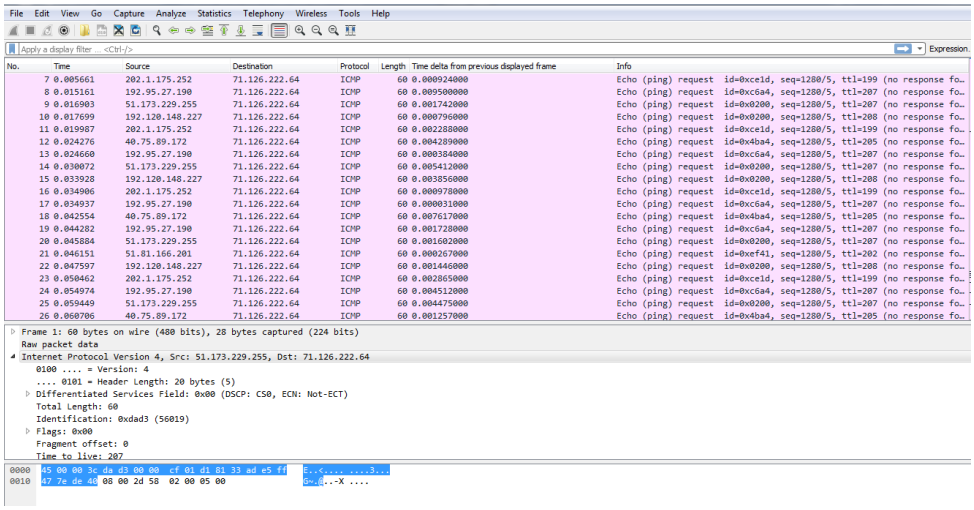


Gambar 6. Deteksi Menggunakan BASE

Hasil simulasi menunjukan bahwa IDS bekerja dengan baik. Paket yang dikirim kepada router di deteksi oleh alert IDS berdasarkan anomaly yang terdapat pada rule alert. Rule tersebut bekerja untuk menentukan apakah paket dianggap sebagai serangan atau bukan. Selama simulasi pemanfaatan *Basic Analysis and Security Engine* (BASE) bekerja untuk menangkap serangan pada lalu lintas data yang tercatat pada file *log* serta disimpan melalui database snort.

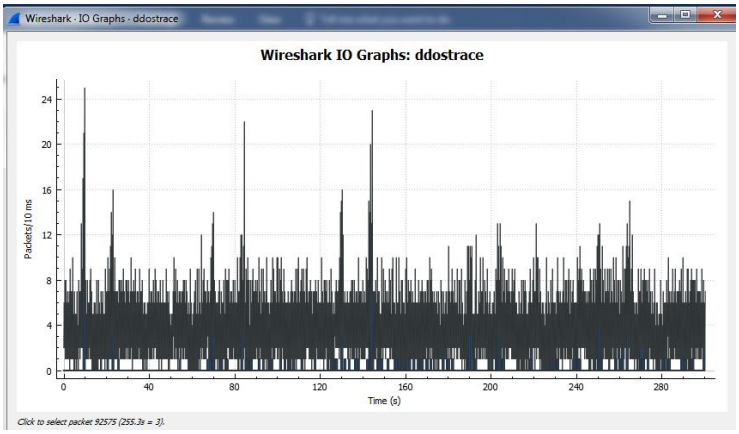
C. Tahap Analisa Menggunakan Mekanisme Forensik

Tahapan ini peneliti menggunakan data *log* yang tersimpan pada *snort router* dengan format .pcap, kemudian file *log* akan dianalisa untuk mencari bukti forensik dengan menggunakan aplikasi wireshark untuk memaparkan karekteristik file *log* yang terdapat pada *snort* seperti pada gambar 7.



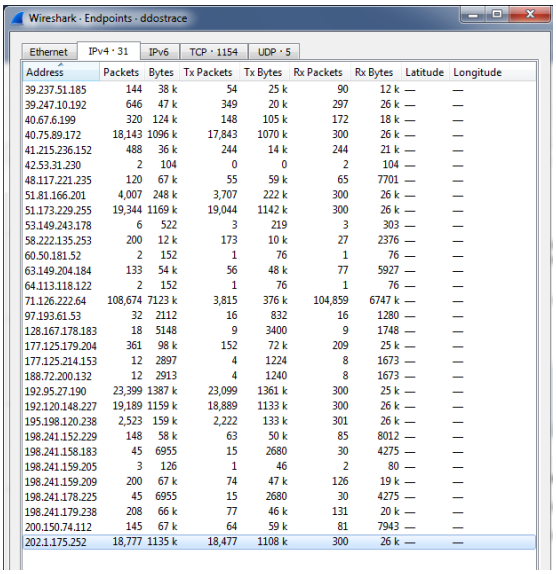
Gambar 7. Analisa Log Menggunakan Wireshark

File *log* akan diperiksa satu per satu utnuk menentukan perubahan yang terjadi dalam jaringan dengan melihat *timestamp*. *Wireshark* mencatat terjadi peningkatan aktivitas lalu lintas jaringan yang terdapat pada gambar 8.



Gambar 8. Grafik Peningkatan Aktivitas Jaringan

Tahapan Analisa dilakukan dengan mekanisme *filtering* menggunakan perintah ip.src== kemudian dianalisa satu per satu pada paket ICMP pada wireshark. Hasil pada gambar7. Menunjukkan bahwa terjadi serangan yang memiliki panjang 60 byte. Pada IPv4 dengan sumber alamat 51.173.229.255 dengan tujuan 71.127.222.64 memiliki panjang *header* 20 *byte* serta panjang total 60 *byte*. Pada tahap ini peneliti juga memanfaatkan endpoint ada wireshark untuk mengumpulkan data-data paket serangan yang tersimpan pada log snort intrusion detection system (IDS) guna memberikan informasi setiap paket yang terdeteksi oleh IDS pada kecepatan yang berbeda setiap byte nya yang terdapat pada gambar 9.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
39.237.51.185	144	38 k	54	25 k	90	12 k	—	—
39.247.10.192	646	47 k	349	20 k	297	26 k	—	—
40.67.6.199	320	124 k	148	105 k	172	18 k	—	—
40.75.89.172	18,143	1096 k	17,843	1070 k	300	26 k	—	—
41.215.236.152	488	36 k	244	14 k	244	21 k	—	—
42.53.31.230	2	104	0	0	2	104	—	—
48.117.221.235	120	67 k	55	59 k	65	7701	—	—
51.81.166.201	4,007	248 k	3,707	222 k	300	26 k	—	—
51.173.229.255	19,344	1169 k	19,044	1142 k	300	26 k	—	—
53.149.243.178	6	522	3	219	3	303	—	—
58.222.135.253	200	12 k	173	10 k	27	2376	—	—
60.50.181.52	2	152	1	76	1	76	—	—
63.149.204.184	133	54 k	56	48 k	77	5927	—	—
64.113.118.122	2	152	1	76	1	76	—	—
71.126.222.64	108,674	7123 k	3,815	376 k	104,859	6747 k	—	—
97.193.61.53	32	2112	16	832	16	1280	—	—
128.167.178.183	18	5148	9	3400	9	1748	—	—
177.125.179.204	361	98 k	152	72 k	209	25 k	—	—
177.125.214.153	12	2897	4	1224	8	1673	—	—
188.72.200.132	12	2913	4	1240	8	1673	—	—
192.95.27.190	23,399	1387 k	23,099	1361 k	300	25 k	—	—
192.120.148.227	19,189	1159 k	18,889	1133 k	300	26 k	—	—
195.198.120.238	2,523	159 k	2,222	133 k	301	26 k	—	—
198.241.152.229	148	58 k	63	50 k	85	8012	—	—
198.241.158.183	45	6955	15	2680	30	4275	—	—
198.241.159.205	3	126	1	46	2	80	—	—
198.241.159.209	200	67 k	74	47 k	126	19 k	—	—
198.241.178.225	45	6955	15	2680	30	4275	—	—
198.241.179.238	208	66 k	77	46 k	131	20 k	—	—
200.150.74.112	145	67 k	64	59 k	81	7943	—	—
202.1.175.252	18,777	1135 k	18,477	1108 k	300	26 k	—	—

Gambar 9. Endpoint Wireshark

5. Kesimpulan

Berdasarkan Analisa yang telah dilakukan menunjukkan bahwa terjadi peningkatan lalu lintas data yang menunjukkan bahwa telah terjadi serangan ddos melalui ICMP berdasarkan analisa log yang di lakukan. IDS dapat dimanfaatkan untuk mendeteksi, merekam lalu lintas data yang ada pada router kemudian di simpan pada log dengan format .pcap. Hasil Analisa dapat membantu administrator dan pihak terkait dalam menemukan bukti serangan untuk keperluan persidangan.

Daftar Pustaka

[1] ICION 2017. Teknologi Keamanan Fokus Konferensi Indonesia CIO Network di bali. Diakses 15 April 2017, dengan alamat https://komite.id/category/cyber/

[2] Muamalah D. dan Riadi I., (2017). " Network Forensics For Detecting Flooding Attack On Web Server", International Journal of Computer Science and Information Security, Vol.15, No. 2

[3] Riadi imam (2012), "*Log Analysis Techniques using Clustering in Network Forensics*", International Journal of Computer Science and Information Security (IJCSIS) , Vol. 10, No.7

[4] Shenbagavalli. (2015). " Router Interface Based IP Traceback Method for DDoS Attack in IPv6 Network". Journal of Resent Research in Engineering and Technology, Vol 2 Issue 3 ISSN : 2349-2252

[5] Iswardani A, Riadi I, (2016). "Danial of Service Log Analysis Using Density K-Means Method", Journal of Theoretical & Applied Information Technology, Vol. 83 Issue 2, ISSN: 1992-8645.

[6] Cartealy I. (2013). "Linux Networking", Jasakom, ISBN : 978-979-1090-73-5

[7] Fadhila Nisya Tanjung, Muhammad Irwan Padli Nasution, (2012) *Implementasi Pemrograman Java Untuk Alert Intrusion Detection System*, pematang siantar, 31 agustus – 2 september 2012, ISBN 978-602-18749-0-5, https://www.researchgate.net/publication/307973619 di akses 29 September 2016

[8] Sahid Aris Budiman, Catur Iswahyudi, Muhammad Sholeh, (2014), *Implementasi Intrusion Detection System (Ids) Menggunakan Jejaring Sosial Sebagai Media Notifikasi*, Yogyakarta, 15 November 2014, ISSN: 1979-911X

[9] I Wayan Bevin Waranugraha, Ary Mazharuddin S. , dan Baskoro Adi Pratomo (2012), *Aplikasi Forensik Jaringan Terdistribusi Menggunakan JADE*, Jurnal Teknik Pomits Vol. 1, No. 1, (2012) 1-6.

[10] Ariyus Doni, 2006, *Computer Security*, Andi, Yogyakarta

[11] Faisal Riyadi, (2014), *Forensik Jaringan Pada Lalu Lintas Data Dalam Jaringan Honeynet Di Indonesia Security Incident Respone Team On Internet Infrastructure/Coordination Center*, Jurnal ICT Penelitian dan

Penerapan Teknologi. Diakses 15 September 2016 dengan alamat URL : https://simonline.akademitelkom.ac.id/slims/index.php?p=show_detail&id=1130

[12] Azikin Askari, 2011, Debian GNU/Linux, Informatika, Bandung ISBN : 978-602-8758-28-24

[13] Yogi Surya Nugroho, 2015, Investigasi Forensik Jaringan Dari serangan DDoS menggunakan metode Naïve Bayes, *skripsi*, Fakultas Sains dan Teknologi, UIN Sunan kalijaga, Yogyakarta.

[14] Valentina dan Mirjana, (2014). "Applcation of Forensic Analisys for Intrusion Detection against DDoS Attacks in Mobile Ad Hoc Networks". Latest Trends in Information Technology, ISBN : 978-1-61804-134-0

[15] Jeong, E. dan Lee, B., (2014). "An IP TraceBack Protocol using a Copressed Hash Table, a Sinkhole Router and Data Mining based on Network Forensics against", Future Generation Computer Systems 33 (2014) 42-2, Diakses 15 Januari 2017 dengan alamat URL: ttp://elsevier.com/locate/fgcs

[16] Kemmish, R. M, 2015, What is forensic computer. Australian institute of Criminology, Canberra. http://www.aic.gov.au/publications/tandi/ti118.pdf