Buletin Ilmiah Sarjana Teknik Elektro
Vol. 2, No. 2, Agustus 2020, pp. 70~74
ISSN: 2685-9572, DOI: 10.12928/biste.v2i2.1065

Analysis of Digital Evidence on Denial of Service (DoS) Attack Log Based

Analisis Bukti Digital tentang Serangan Denial of Service (DoS) Berdasarkan Log

Galih Pramuja Inngam Fanani [1], Imam Riadi [2]

[1] Mahasiswa Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Indonesia
[2] Dosen Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Indonesia

INFORMASI ARTIKEL

Riwayat Artikel:

Dikirimkan 20xx,
Direvisi 20xx,
Diterima 20xx.

Kata Kunci:

DoS (Denial of Service),
IDS *Snort*,
Loic,
Log,
Wireshark.

Penulis yang Berkaitan:

Galih Pramuja Inngam F.
Dr. Imam Riadi
Kampus 4 UAD, Jln. Ring Road Selatan, Tamanan, Banguntapan, D.I. Yogyakarta

Surel:
gpramuja05@gmail.com
imam.riadi@is.uad.ac.id

ABSTRAK

This research is carried out an analysis and investigation of digital log file data retrieval from DoS (Denial of Service) attacks, on internet networks that have been detected by IDS (Intrusion Detection System) and using Wireshark as Tools Analysis Network. The research phase begins with the design of an experimental scenario which is often carried out daily where users access the internet network. The next stage is an attack in the form of ping flood on the target computer connected to the internet network, the final stage of data retrieval which will be analyzed later. Testing research using UAT (User Acceptance Test), to prove that the analysis has been received by the user. The results of research conducted to obtain data in the form of an attacker's IP (Internet Protocol), target IP, protocol type, the port used and the time of the attack. In the UAT test results, the obtained value of 18% of students disagrees, 58% of students agree, and 24% of students strongly agree. This research has conducted an analysis of random data attacks using Wireshark applications received by users.

Penelitian ini dilakukan analisis dan investigasi pengambilan data file log digital dari serangan DoS (Denial of Service), pada jaringan internet yang telah terdeteksi oleh IDS (Intrusion Detection System) dan menggunakan Wireshark sebagai Tools Analysis Network. Fase penelitian dimulai dengan desain skenario eksperimental yang sering dilakukan setiap hari di mana pengguna mengakses jaringan internet. Tahap selanjutnya adalah serangan berupa banjir ping pada komputer target yang terhubung ke jaringan internet, tahap akhir pengambilan data yang akan dianalisis nanti. Pengujian penelitian menggunakan UAT (User Acceptance Test), untuk membuktikan bahwa analisis telah diterima oleh pengguna. Hasil penelitian dilakukan untuk memperoleh data dalam bentuk IP penyerang (Internet Protocol), IP target, tipe protokol, port yang digunakan dan waktu serangan. Dalam hasil tes UAT, nilai yang diperoleh dari 18% siswa tidak setuju, 58% siswa setuju, dan 24% siswa sangat setuju. Penelitian ini telah melakukan analisis serangan data acak menggunakan aplikasi Wireshark yang diterima oleh pengguna.

Sitasi Dokumen ini:

G. P. I. Fanani and I. Riadi, "Analysis of Digital Evidence on Denial of Service (DoS) Attack Log Based," *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 2, no. 2, pp. 70–74, 2020. DOI: 10.12928/biste.v2i2.1065

1. PENDAHULUAN

Jaringan internet pada era saat ini sudah menjadi kebutuhan utama dalam aktivitas sehari-hari. Sehingga keamanan suatu jaringan komputer yang terhubung dengan layanan internet sangat penting. Sehingga apabila terjadi ancaman dari tindak *hacker* dapat mencuri informasi data dan serangan tersebut dapat merusak jaringan komputer [1]. Jenis serangan yang sering digunakan oleh *hacker* adalah (*Denial of Services*) DoS yang bersifat mengirimkan sejumlah paket melalui internet *protocol* (IP) secara terus menerus yang dapat mengganggu organisasi dari jaringan komputer dengan tujuan melumpuhkan server [2] [3].

Pada sebuah sistem jaringan internet diperlukan sebuah sistem pendeteksi dengan metode (*Intrusion Detection System*) IDS, yang berguna untuk menjaga validitas dan integritas layanan bagi semua pengguna jaringan internet [4][5]. Keseluruhan aktivitas yang dilakukan oleh pengguna layanan internet dapat di amati berdasarkan *Log file* yang sudah tersimpan pada sistem IDS yang digunakan. *File log* tersebut berisi informasi penyebab terjadinya kegagalan sistem yang dilakukan *hacker* pada jaringan internet [6][7].

Barang bukti merupakan bagian yang paling dibutuhkan dalam sebuah kasus tindak kejahatan [8]. Barang bukti dikelompokkan menjadi 2 bagian yaitu barang bukti ini bersifat fisik dan dapat dikenali secara visual, antara lain contohnya yakni komputer, laptop, *fashdisk/hardisk*, kamera, *router, handphone* dan barang bukti yang direcovery dan diesktrak dari barang bukti elektronik, antara lain contohnya *lost file*, *log file*, *email*, *image file*, *video file*, *delete file* [9]. *Log* merupakan riwayat aktivitas yang terjadi dalam sebuah sistem organisasi jaringan komputer. Awalnya *Log* digunakan untuk memulihkan kegagalan dalam suatu sistem. Namun untuk saat ini *Log* memiliki fungsi yang lebih luas, seperti untuk merekam informasi tindak kejadian dalam penggunaan layanan internet, bahkan *Log* digunakan sebagai barang bukti atas tindakan kejahatan di dunia internet. Pada era saat ini *Log* sudah menjadi bagian penting untuk para penyelidik dalam bidang Digital forensik [10]. Proses yang digunakan untuk melakukan analisa serangan yaitu dengan menggunakan pendekatan model proses forensik.

Proses forensik mempunyai 4 tahapan yang digunakan dalam proses forensik antara lain, 1. *Collecting*: Pada tahap ini meliputi pencarian, pengumpulan, dan dokumentasi alat bukti dengan menggunakan *tools* yang dibutuhkan. 2. *Examination:* Proses pemeriksaan informasi dengan menganalisis *file log* yang di tangkap oleh IDS. 3. *Snort.Analysis*: Proses mempelajari dan mengidentifikasi kasus, hasilnya untuk dijadikan barang bukti digital. 4. *Reporting*: Menulis laporan mengenai informasi yang di dapat dari seluruh penyelidikan. Laporan ini digunakan untuk bukti dari hasil penyelidikan [10].

Loic (*Low Orbit Ion Cannon*) merupakan sebuah *tool* atau aplikasi peretas jaringan atau *open source stress testing*, *Loic* sering digunakan untuk serangan DDoS [11]. Loic begitu mudah digunakan dengan memasukkan dan mengunci URL atau IP target, pilih metode penyerangan, *attack*, dan tinggal menunggu hasil, maka target tersebut akan *down*, tidak bisa diakses, dan menyebabkan kerusakan pada *serve*r tersebut.

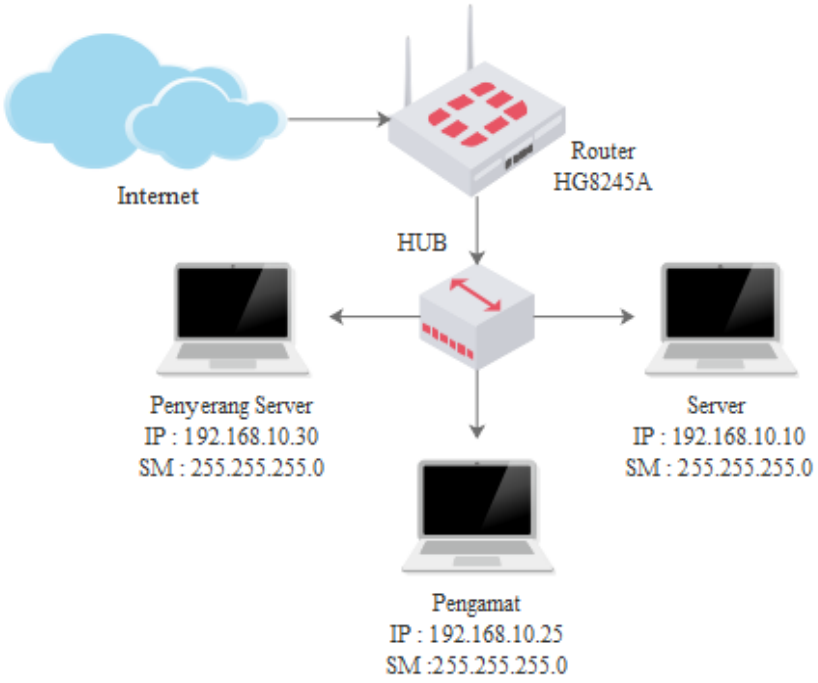
IDS (*Intrution Detection System*) adalah sebuah sistem aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan [12]. *Snort* merupakan salah satu contoh program *Network-based Intrusion Detection System*, yaitu sebuah program yang dapat mendeteksi suatu usaha penyusupan pada suatu sistem jaringan computer dan *Snort* bersifat *open source* [13].

Wireshark merupakan salah satu dari sekian banyak *tool network analyser* yang banyak digunakan oleh *network administrator* untuk menganalisis dan melacak kinerja jaringannya termasuk *protocol* di dalamnya [14]. *Wireshark* mampu menangkap paket-paket data atau informasi yang melewati jaringan. Semua jenis paket informasi dalam berbagai format *protocol* pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang *tool* ini juga dapat dipakai untuk *sniffing* (memperoleh informasi penting seperti *password email* atau *account* lain) dengan menangkap paket-paket yang melewati jaringan dan menganalisisnya [15].

2. METODE PENELITIAN

2.1. Skenario Penelitian

Skenario yang dilakukan yaitu skenario dengan sistem *internet connecting sharing* di laboratorium teknik elektro UAD. Skenario eksperimen. Cara kerjanya adalah komputer pengamat, komputer penyerang *server* dan komputer *server* yang terhubung pada satu jaringan menggunakan perangkat HUB di laboratorium teknik elektro UAD. Penyerang *server* akan melakukan serangan targetnya yaitu komputer *server* dan komputer pengamat akan mendeteksi dan melacak serangan tersebut. Riwayat serangan yang akan tersimpan dalam bentuk *Log file*. Sebagai gambaran saat proses eksperimen dilakukan Gambar 1.



Gambar 1. Skenario eksperimen

2.2. Diagram Alir Deteksi Serangan

Diagram alir sistem deteksi merupakan alur berjalannya sistem (*Intrusion Detection system*) IDS untuk mendeteksi sebuah serangan (*Denial of Services*) DoS yang dikirim oleh penyerang menggunakan aplikasi *Loic*. Hasil dari serangan yang terdeteksi akan langsung tersimpan dalam bentuk *file Log Snort*. Gambar 2. Merupakan diagram alir sistem dengan *metode Intrusion Detection system* (IDS) *Snort* dengan sistem operasi *Windows*. Cara kerja Gambar 2. sebagai berikut:

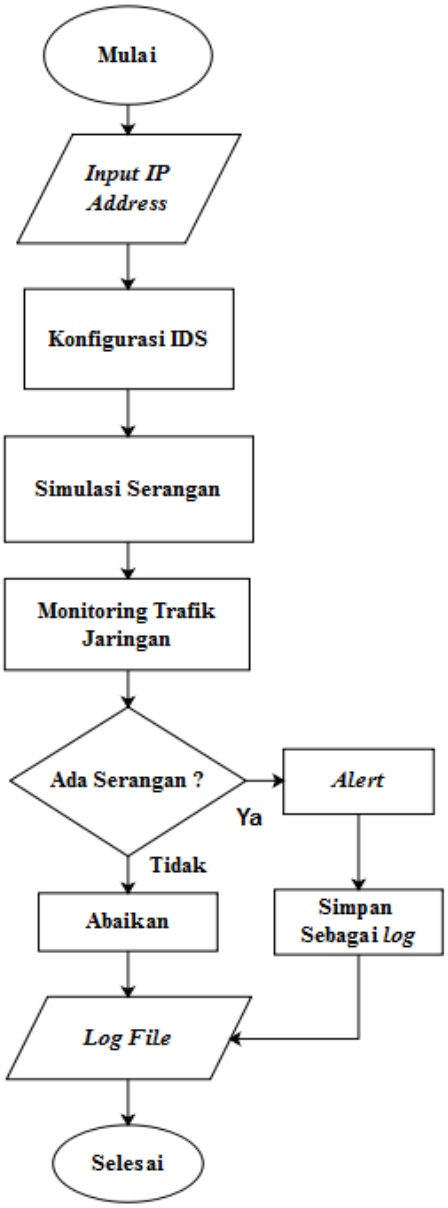
1. Mulai membuka modul yang digunakan.
2. Input IP *address* adalah proses memasukkan IP *destination* pada *software Loic*.
3. Konfigurasi IDS merupakan proses pengaktifan *Snort* (IDS) sebagai pendeteksi terjadinya serangan.
4. Simulasi serangan merupakan proses melakukan serangan. Serangan yang dilakukan serangan *(Denial of service)* DoS menggunakan aplikasi *Loic*.
5. Monitoring jaringan dengan IDS proses memantau pergerakan trafik *packet* secara *real time*. Apabila terjadi serangan DoS maka trafik *packet* akan berjalan sangat cepat, dan akan ada *alert* dari IDS. Jika tidak ada *packet* serangan maka akan diabaikan.
6. Simpan *Log* merupakan proses penyimpanan *alert* deteksi dalam bentuk *output Log file Snort* yang berisi riwayat serangan yang dilakukan penyerang.
7. Selesai, berakhirnya semua proses sudah dilakukan.

2.3. Diagram Alir Analisis Data Log

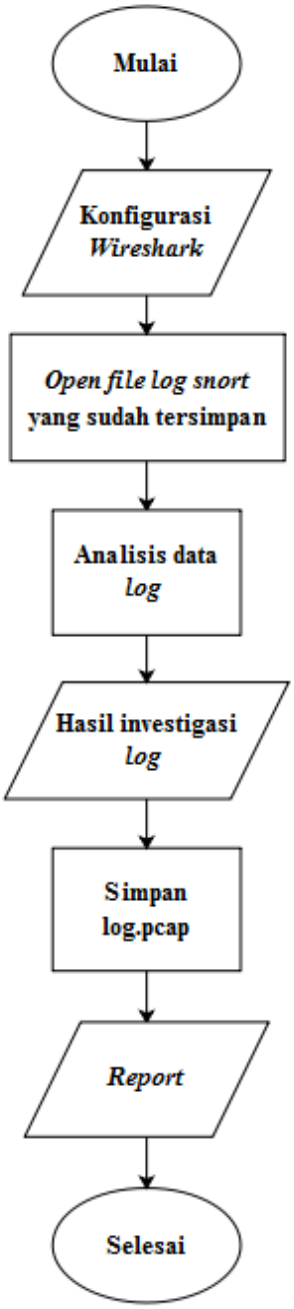
Diagram alir analisa *Log file* merupakan alur identifikasi informasi data yang sudah dikumpulkan, proses ini menggunakan *software Wireshark*. Hasil akhir dari proses analisis data *Log file* dalam bentuk *report* dan akan dijadikan sebagai barang bukti digital. barang bukti digital. Cara kerja Gambar 3. Merupakan diagram alir analisa dari *Log file Snort* untuk dijadikan barang bukti digital, dengan menggunakan *tools Wireshark.* Berikut penjelasan Gambar 4. Diagram alir analisa *Log file*.

1. Mulai membuka modul yang digunakan.
2. Konfigurasi *Wireshark* merupakan proses untuk melakukan konektivitas terhadap jaringan yang aktif.
3. *Open file Log Snort*, melakukan *open file yang sudah tersimpan* dari *folder Log Snort*.
4. Analisa data *Log*, proses idetifikasi *Log file*, untuk memperoleh informasi yang dibutuhkan.
5. Hasil investigasi *log*, berupa data informasi IP penyerang, IP target, waktu serangan, protocol dan *port*
6. Simpan log. pcap, *Log* yang sudah dianalisis akan disimpan dengan format pcap yang selanjutnya akan di *export* ke dalam format .csv.

7. *Output* data dari simulasi ini dalam bentuk *report*.



Gambar 2. Diagram alir deteksi serangan

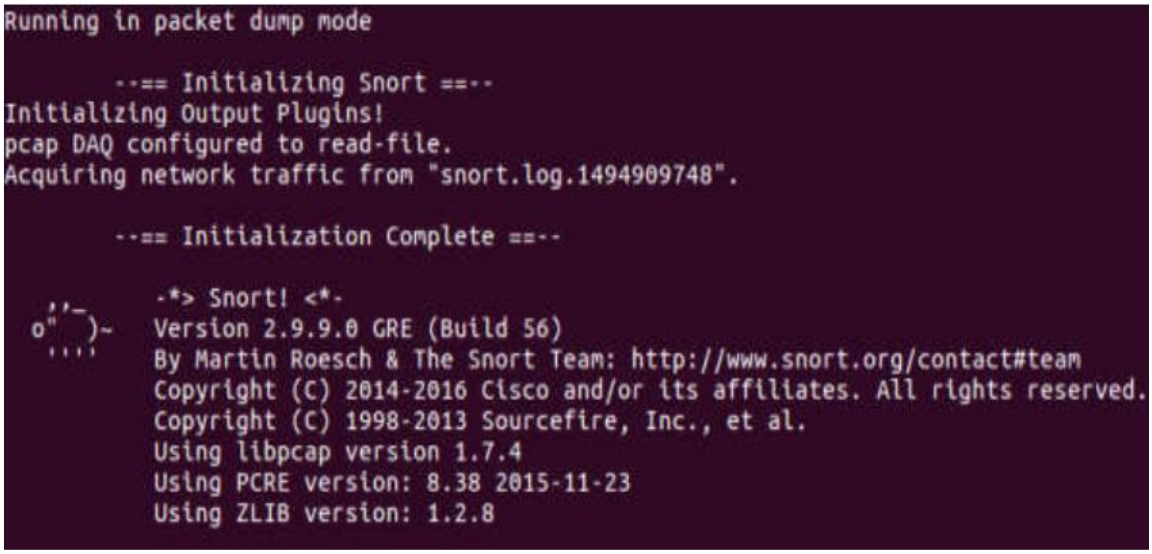


Gambar 3. Diagram alir analisis *Log file.*

3. HASIL DAN PEMBAHASAN

3.1. Implementasi

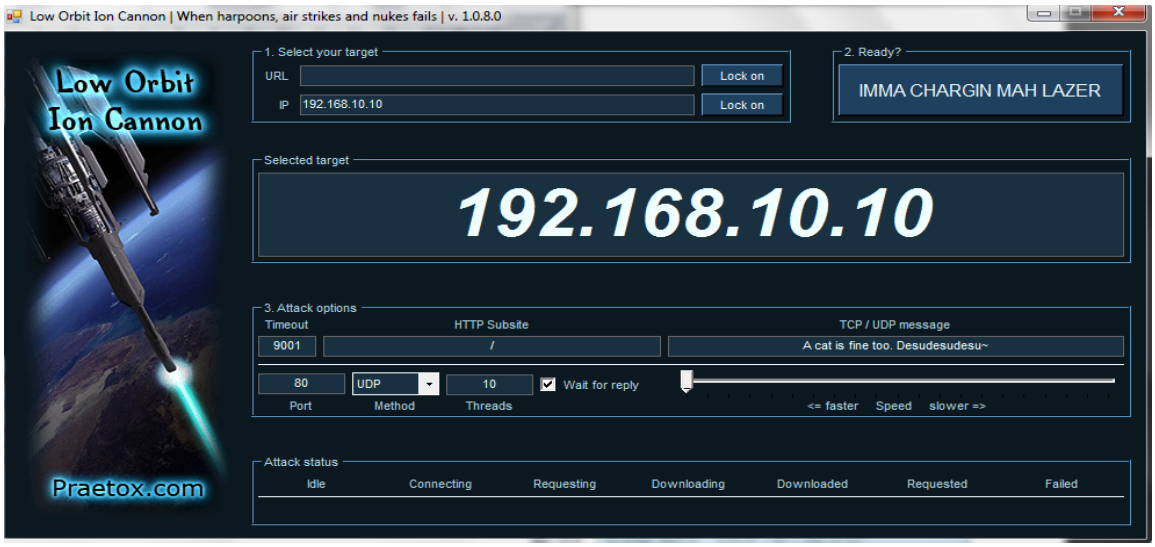
Implementasi dilakukan pemasangan *(Intrusion Detection System)* IDS sebagai pendeteksi paket yang dicurigai sebagai serangan keamanan jaringan. IDS yang digunakan adalah *Snort* versi *windows*. Sofware *Wireshark* digunakan sebagai monitoring lalu-lintas jaringan internet. Selain untuk memonitoring jaringan *Wireshark* juga akan digunakan sebagai *tools* untuk analisis *Log fil*e. Serangan data acak (*Denial of Service*) DoS menggunakan software *Loic* [14]. Gambar 4. Merupakan implementasi IDS *Snort* yang digunakan pada eksperimen.



Gambar 4. Implementasi *Snort*

3.2. Penyerangan UDP dan TCP menggunakan aplikasi *LOIC*

Pada pengujian dilakukan penyerangan data acak DoS dengan melalui protocol UDP dengan menggunakan aplikasi *Loic*, untuk mengirimkan banyak *packet* kepada (*internet protocol address*) IP komputer target 192.168.10.10 dan IP pada penyerang 192.168.10.25. Setelah melakukan penyerang pada komputer target, maka IDS *Snort* akan mendeteksi serangan tersebut. Selanjutnya *alert* yang terdeteksi akan disimpan sebagai *Log file*, yang akan diidentifikasi menggunakan *software Wireshark.* Seperti gambar 5. berikut ini

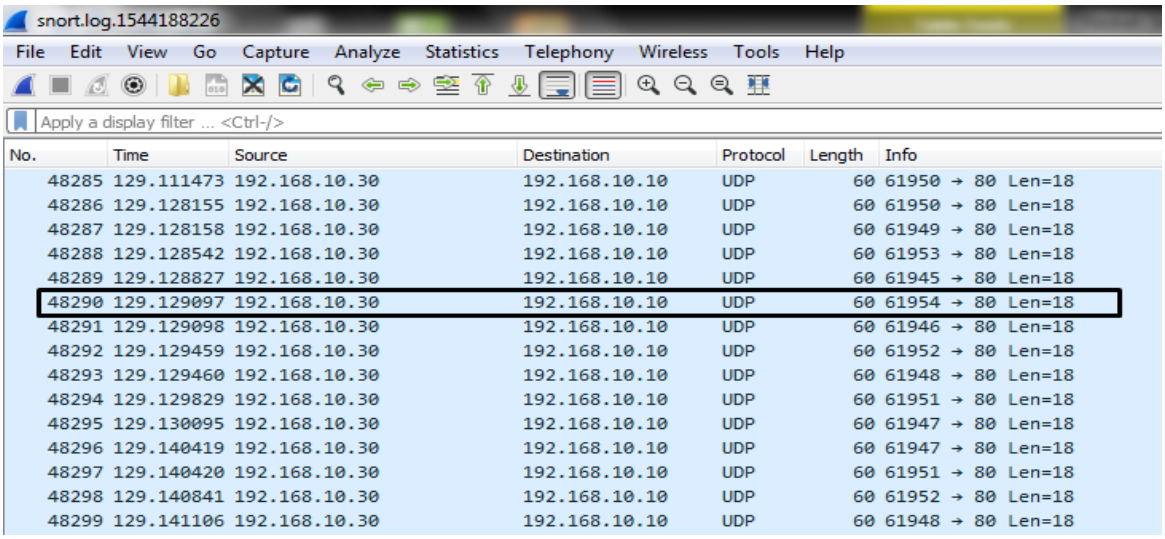


Gambar 5. Tampilan serangan UDP menggunkan *LOIC*

.

3.3. Analisa dan Indentifikasi *Log File*

Serangan (*Denial of Service*) DoS yang memanfaatkan *protocol* UDP dengan cara *connectionless* (mengurangi sambungan) untuk menyerang target. Pada pengujian ini *Log file* yang diidentifikasi menggunakan *tools Wireshark* adalah *snort.log*.1544188226.Tujuan identifikasi adalah untuk memperoleh informasi yang dibutuhkan. Pada kolom *source* dan *destination* terdapat IP (*Internet Protocol*) dari masing-masing komputer dalam melakukan komunikasi antara satu dengan lainnya. IP *source* adalah 192.168.10.30 dan IP *destination* adalah 192.168.10.10. IP yang digunakan merupakan jenis IP lokal. Jenis *protocol* yang digunakan adalah UDP (*User Datagram Protocol*). Port yang digunakan 80. Dapat dilihat pada gambar 6. Merupakan aliran lalu lintas data serangan yang terdeteksi dan di monitoring *Wireshark.*

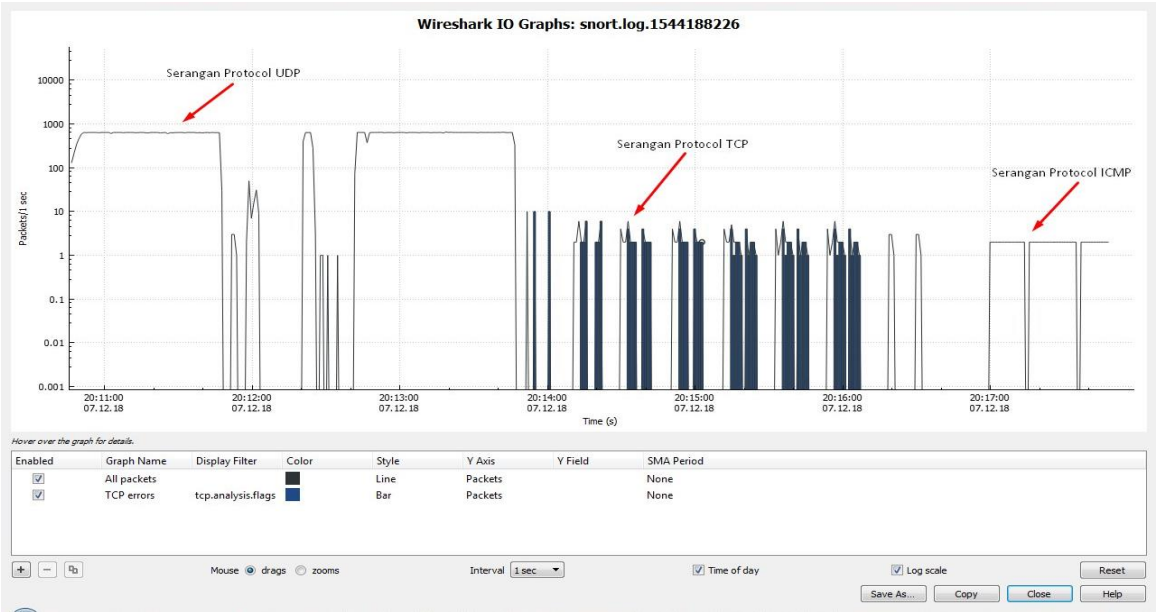


No.	Time	Source	Destination	Protocol	Length	Info
48285	129.111473	192.168.10.30	192.168.10.10	UDP	60	61950 → 80 Len=18
48286	129.128155	192.168.10.30	192.168.10.10	UDP	60	61950 → 80 Len=18
48287	129.128158	192.168.10.30	192.168.10.10	UDP	60	61949 → 80 Len=18
48288	129.128542	192.168.10.30	192.168.10.10	UDP	60	61953 → 80 Len=18
48289	129.128827	192.168.10.30	192.168.10.10	UDP	60	61945 → 80 Len=18
48290	129.129097	192.168.10.30	192.168.10.10	UDP	60	61954 → 80 Len=18
48291	129.129098	192.168.10.30	192.168.10.10	UDP	60	61946 → 80 Len=18
48292	129.129459	192.168.10.30	192.168.10.10	UDP	60	61952 → 80 Len=18
48293	129.129460	192.168.10.30	192.168.10.10	UDP	60	61948 → 80 Len=18
48294	129.129829	192.168.10.30	192.168.10.10	UDP	60	61951 → 80 Len=18
48295	129.130095	192.168.10.30	192.168.10.10	UDP	60	61947 → 80 Len=18
48296	129.140419	192.168.10.30	192.168.10.10	UDP	60	61947 → 80 Len=18
48297	129.140420	192.168.10.30	192.168.10.10	UDP	60	61951 → 80 Len=18
48298	129.140841	192.168.10.30	192.168.10.10	UDP	60	61952 → 80 Len=18
48299	129.141106	192.168.10.30	192.168.10.10	UDP	60	61948 → 80 Len=18

Gambar 6. Lalu lintas serangan UDP pada *Wireshark*.

3.4. Statistik *Log*

Statistik *log* merupakan grafik dari jumlah *packet* yang dikirim dalam waktu 1 *second*, pada penelitian ini berdasarkan Gambar 9. *packet* yang dikirim IP 192.168.10.30 melalui *protocol* UDP sebanyak 940 *packet/second*, melalui *protocol* TCP sebanyak 9 *packet/second*, dan melalui *protocol* ICMP sebanyak 2 *packet/second*. Banyaknya *packet* yang dikirim bisa berubah-ubah sesuai dengan kondisi jaringan internet. Berikut gambar 7. Merupakan statistik *log*.



Gambar 7. Statistik *log packet*

Semua hasil lalu-lintas jaringan yang sudah di capture dan diidentifikasi, selanjutnya disimpan dengan format *packet capture* (pcap) untuk dijadikan sebagai barang bukti. *Log file* pcap juga bisa disimpan dengan format *Comma Separated Values* (CSV) untuk diolah sebagai data tertulis atau lampiran. Dari serangkaian hasil analisa untuk memudahkan dalam membaca hasil serangan, maka disajikan dalam bentuk tabel. Tabel 1. Merupakan hasil invertigasi serangan yang menggunakan *protocol* termasuk berbahaya dikarenakan dalam waktu 1 detik penyerang mengirimkan *packet* sebanyak 940 *packet*, dalam 1 jam, *packet* yang dikirimkan ke target sebanyak 338.400 *packet*. Dengan hasil analisa dan investigasi diatas yang sudah dalam bentuk tabel akan memudahkan investigator untuk presentasi, dilengkapi dengan data *Log* terlampir yang sudah dicetak

Tabel 1. Hasil analisa dan invertigasi

No	Waktu (WIB)	IP Penyerang	IP Target	Port	Protocol	Jumlah *Packet*/second	Bahaya Iya/Tidak
1.	Desember 7 20:17:43	192.168.10.30	192.168.10.10	-	ICMP	2	Tidak
2.	Desember 7 20:14:15	192.168.10.30	192.168.10.10	80	TCP	9	Tidak
3.	Desember 14 20:10:46	192.168.10.25	192.168.10.10	80	UDP	940	Iya

3.5. Validasi data digital (*Log*)

Setelah dilakukan pengujian analisa *Log* menggunakan *Wireshark* untuk menemukan informasi data digital, Validasi *Log file* dapat dilakukan dengan cara membandingkan *Log file* yang asli dengan *Log file* yang sudah di analisis dengan *tools Wireshark*. Dari perbandingan validasi ini dapat diketahui bahwa pengamatan barang bukti digital bisa dikatakan asli. Waktu simpan merupakan waktu saat *Log* disimpan. Selanjutnya, dengan *Wireshark Log file* diekstraksi untuk di analisa, hasil analisa berisi informasi IP 192.168.10.30 sebagai penyerang dan IP 192.168.10.10 sebagai target. Dari validasi ini *Log file* asli hanya berubah format menjadi pcap dan akan dikonversi ke format csv, karena hasil ekstrasi *Log file* akan dijadikan *report* pada penelitian ini. Tabel 2. Merupakan validasi data *Log file*.

Tabel 2. Validasi *Log file*

No.	*File Log* Asli	Waktu Simpan	*File Log* Ekstraksi	Waktu Baca	Keterangan
1.	*Snort*.log.1544188226	12/7/2018 8:17 PM	log 1.pcap	2/1/2019 12:01 AM	Sesuai Skenario
2.	*Snort*.log.1544187285	12/7/2018 7:59 PM	log 2.pcap	2/1/2019 12:09 AM	Sesuai Skenario
3.	*Snort*.log.1544188899	12/7/2018 8:25 PM	log 3.pcap	2/1/2019 12:10 AM	Sesuai Skenario
4.	*Snort*.log.1544190249	12/7/2018 8:52 PM	log 4.pcap	2/1/2019 12:10 AM	Sesuai Skenario

3. KESIMPULAN

Berdasarkan dari hasil pengujian dengan menggunakan *software Loic*, untuk mengirim serangan *packet* data acak, *Snort* sebagai (*Intrusion Detection System*) IDS, mampu untuk mendeteksi dan mengenali serangan tersebut secaara cepat. *Tools Wireshark* mampu membaca *Log file* yang berisi informasi riwayat penyerang data acak (*Denial of Services*) DoS. *Log file* tersebut dapat dijadikan barang bukti digital jaringan.

UCAPAN TERIMA KASIH

Terima kasih kepada editor dan *reviewer* atas segala saran, masukan dan telah membantu dalam proses penerbitan naskah. Ucapan terima kasih juga ditunjukkan kepada pembimbing tugas akhir dan pihak-pihak yang telah mendukung.

REFERENSI

[1] A. Fadlil, I. Riadi, and S. Aji, "Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, vol. 3, no. 1, pp. 11–19, 2017.

[2] O. Wijaya, Jusak, and A. Sukmaaji, "Pemodelan Karakteristik Denial of Service Attack Melalui Analisis Data Trafik," *JCONES: Journal of Control and Network*, vol. 3, no. 1, pp. 105–111, Jul. 2014.

[3] A. Fadlil and S. Aji, "DDoS Attacks Classification using Numeric Attribute-based Gaussian Naive Bayes," *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 8, no. 8, 2017.

[4] E. K. Dewi and P. Kasih, "Analisis Log Snort Menggunakan Network Forensic," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 2, no. 2, pp. 72–79, Dec. 2017.

[5] Christos Douligeris and Dimitrios N. Serpanos, *Network Security: Current Status and Future Directions*. Wiley-IEEE Press, 2007.

[6] T. A. Cahyanto and Y. Prayudi, "Investigasi Forensika Pada Log Web Server untuk Menemukan Bukti Digital Terkait dengan Serangan Menggunakan Metode Hidden Markov Models," *Seminar Nasional Aplikasi Teknologi Informasi (SNATI) Yogyakarta*, vol. 1, no. 1, pp. 21–2014, Jun. 2014.

[7] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis," *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, vol. 2, no. 1, pp. 19–30, 2017.
[8] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital pada Frozen Solid State Drive dengan Metode National Institute of Justice (NIJ)," *Elinvo (Electronics, Informatics, and Vocational Education)*, vol. 3, no. 1, pp. 70–82, Jul. 2018.
[9] M. F. Sandwinata, "Analisis DNA dalam Kasus Forensik," *TEKNOSAINS: MEDIA INFORMASI SAINS DAN TEKNOLOGI*, vol. 12, no. 1, pp. 1–10, Feb. 2018.
[10] F. Ridho, A. Yudhana, and I. Riadi, "Implementasi Log Dalam Forensik Router Terhadap Serangan Distributed Denial of Service (DDoS)," *JTM (JURNAL TIMES: Technology Informatics & Computer System)*, vol. 6, no. 2, 2017.
[11] A. Iswardani and I. Riadi, "Denial of Service log Analysis Using Density K-Means Method," *Journal of Theoretical and Applied Information Technology*, vol. 20, no. 2, pp. 299–302, 2016.
[12] Faizin Ridho, "Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time," in *Annual Research Seminar (ARS)*, 2016.
[13] J. Fahana, R. Umar, and F. Ridho, "Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan," *Query: Journal of Information Systems*, vol. 1, no. 2, Oct. 2017.
[14] M. A. Zulkifli, I. Riadi, and Y. Prayudi, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," *International Journal of Computer Applications*, vol. 180, no. 35, pp. 23–30, 2018.
[15] M. Aziz, M. Aziz, R. Umar, and F. Ridho, "Implemetasi Jaringan Saraf Tiruan Untuk Mendeteksi Serangan DDoS Pada Forensik Jaringan," *Query: Journal of Information Systems*, vol. 3, no. 1, Apr. 2019.

BIOGRAFI PENULIS

Galih Pramuja Inngam Fanani
Lahir di Blitar 18 Desember 1993. Menyelesaikan pendidikan S1 Program Studi Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta. Bidang peminatan adalah telematika.

Dr. Imam Riadi., S.Pd., M. Kom
Lahir di Kudus, 10 Agustus 1980. Menyelesaikan pendidikan S1 Pendidikan Teknik Komputer/ Teknik Elektro di Universitas Negeri Yogyakarta, S2 Ilmu Komputer di Universitas Gajah Mada Yogyakarta, dan S3 Ilmu Komputer di Universitas Gajah Mada Yogyakarta. Bidang keahlian : Jaringan Komputer, Sekuritas Komputer, Administrasi Sistem dan Jaringan, Organisasi dan Arsitektur Komputer, dan Forensik Digital. Saat ini beliau adalah Dosen di Universitas Ahmad Dahlan.