Media of Computer science (MCs)
Vol.3, No.1, Juni 2026, pp. 11~24
ISSN (print): 3063-4822, ISSN (online): 3063-4997
DOI: 10.69616/mcs. v3i1.274

Experimental Analysis of UDP Flood DDoS Attacks Using Network Forensic Methods

Mustamin[1], Muhammad Na'im Al Jum'ah*[2]
[1,2]Ilmu Komputer, Fakultas Teknologi Informasi, Universitas Sembilanbelas November Kolaka, Kolaka, Indonesia
e-mail: [1]mustamin01@gmail.com, *[2]**muhnaimaljumah@usn.ac.id**

Abstract

In the ever-evolving digital era, computer networks have become the backbone of various information and communication systems. However, increased network usage has also led to increased security threats, such as Distributed Denial of Service (DDoS) attacks, ARP Spoofing, and other attacks. To address these threats, an approach capable of detecting, analyzing, and recovering networks from cyberattacks is needed. This study aims to analyze DDoS attacks using network forensics methods with an anomaly identification and attack reconstruction approach. This process includes collection, examination, analysis, and reporting stages using tools such as Wireshark and Winbox. Attack simulations were conducted using the LOIC application on a MikroTik router. The analysis results showed that the DDoS attack caused a CPU spike of up to 100%, which made the router unresponsive. Wireshark successfully identified the attack pattern in the form of UDP packet flooding, while Winbox showed a direct impact on device performance. The anomaly identification technique proved effective in detecting traffic spikes, and the reconstruction process helped understand the chronology and methods of the attack. This research contributes to the understanding and mitigation of cyber attacks through a network forensics approach, as well as being a guide in the implementation of security systems based on anomaly identification and attack reconstruction.

Keywords— *Network Forensics, DDoS, Anomaly Detection, Attack Reconstruction, Wireshark.*

Abstrak

Di era digital, jaringan komputer menjadi infrastruktur utama dalam sistem informasi, namun juga semakin rentan terhadap serangan siber seperti Distributed Denial of Service (DDoS). Penelitian ini bertujuan menganalisis serangan DDoS menggunakan metode network forensics dengan pendekatan identifikasi anomali dan rekonstruksi serangan. Proses analisis meliputi tahapan collection, examination, analysis, dan reporting menggunakan perangkat lunak Wireshark dan Winbox. Simulasi serangan dilakukan menggunakan aplikasi Low Orbit Ion Cannon (LOIC) pada router MikroTik. Hasil penelitian menunjukkan bahwa serangan DDoS menyebabkan penggunaan CPU router meningkat hingga 100%, sehingga perangkat menjadi tidak responsif. Wireshark berhasil mengidentifikasi pola serangan berupa UDP packet flooding, sedangkan Winbox menampilkan dampak langsung terhadap kinerja router. Pendekatan identifikasi anomali efektif dalam mendeteksi lonjakan trafik jaringan, sementara rekonstruksi serangan membantu memahami kronologi dan karakteristik serangan. Penelitian ini memberikan kontribusi dalam mendukung analisis forensik jaringan serta pengembangan strategi mitigasi terhadap serangan siber berbasis DDoS.

Kata kunci—*Network Forensics, DDoS, Identifikasi Anomali, Rekonstruksi Serangan, Wireshark.*

Received May 29th,2026; Revised July 23th, 2026; Accepted July 28th, 2026

1. PENDAHULUAN

Dalam era digital yang terus berkembang, jaringan komputer menjadi tulang punggung dari sistem berbagai informasi dan komunikasi. Banyak pelanggaran data yang terjadi karenaimplementasi yang buruk atau tidak adanya kontrol keamanan baik di perusahaan swasta maupun di organisasi pemerintahan[1]. Namun, peningkatan pengunaan jaringan juga di sebabkan meningkatnya ancaman keamanan, seperti serangan *Distributed Deniel of Service* (DDoS), ARP Spoofing dan serangan lainnya[2]. Untuk menangani ancaman ini, di perlukan pendekatan yang mampu mendeteksi, mengganalisis, dan memulihkan jaringan dari serangan siber[3].

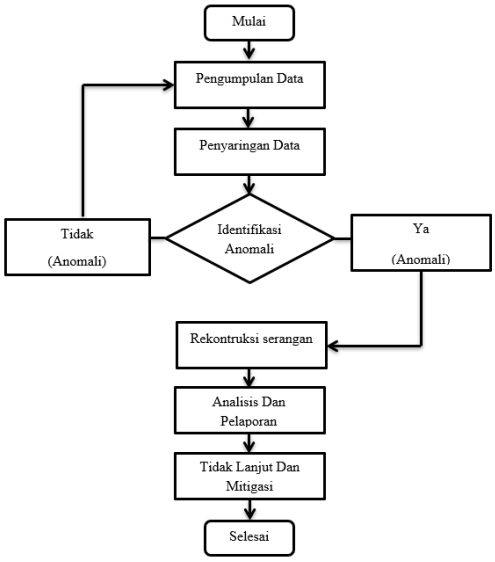
Cybercrime merupakan tindakan kejahatan pada dunia maya yang memanfaatkan perangkat computer yang terhubung dalam suatu jaringan computer dan kejatan ini merugikan pihak lain. Salah satu kejahatan pada dunia computer adalah *Distributed Daniel Of Service* (DDoS) di mana serangan ini berkerja dengan cara mengirim pesan yang bertubi-tubi sehingga membuat jaringan *down*[4][5]. Pada periode Januari 2023 hingga Juni 2024, Indonesia mendapatkan total serangan 260 miliar serangan DDos layer 7. Akamai tidak menyebut berapa persen kenaikan tersebut. Akan tetapi, hal itu membuat Indonesia menduduki posisi keempat sebagai negara teratas di kawasan asia pasifik dan jepang (APJ) yang menjadi sasaran serangan DDoS. Akamai adalah perusahaan keamanan, komputasi, dan pengiriman terkemuka. Dan membantu perusaahan global menjadi hidup lebih baik bagi miliaran orang dan perusahan di seluruh dunia[6].

Salah satu cara untuk menjaga keamanan computer yaitu melakukan Penerapan metode *network forensic*[7]. Ini dapat digunakan untuk mengganalisis serangan DoS pada perangkat router. Metode *network forensic* ini juga meliputi tahap-tahap seperti persiapan, penanganan insiden, pengumpulan data, pemeriksaan, analisis data, investigasi, dan presentasi hasil [8]. Dari proses penyerangan yang di analisa bahwa serangan DoS mengunakan aplikasi LOIC dengan cara mengirim pesan secara bertubi-tubi sehingga membuat jaringan router menjadi *down*. Metode *network forensik* dapat digunakan untuk menganalisis serangan DoS pada perangkat router dan membantu dalam mengambil tindakan untuk mencegah serangan selanjutnya[9].

Sistem deteksi intrusi berdasarkan anomali dalam sistem keamanan jaringan yang berfungsi untuk mendeteksi adanya gangguan-gangguan pada jaringan komputer dengan cara mendeteksi gangguan-gangguan tersebut berdasarkan pola-pola anomali yang ditimbulkan. Serangan *denial of services* (DoS) adalah salah satu contoh jenis serangan yang dapat mengganggu infrastruktur dari jaringan komputer, serangan jenis ini memikili suatu pola khas, dimana dalam setiap serangannya akan mengirim sejumlah paket-paket data secara terus-menerus kepada target serangannya. Dengan menggunakan metode deteksi anomali, dan serangan DoS dapat dideteksi dengan mengidentifikasi pola-pola anomali yang ditimbulkan, metode deteksi berdasarkan anomali memiliki target kesalahan deteksi yang cukup besar, namun memiliki keunggulan untuk mendeteksi jenis-jenis pola serangan baru[10].

Teknik identifikasi anomali memainkan peran penting dalam forensik jaringan. Dengan menggunakan analisis statistik, *machine learning*, atau pendekatan berbasis aturan, teknik ini dapat mendeteksi pola aktivitas yang tidak biasa yang sering kali merupakan indikasi serangan. Di sisi lain, rekonstruksi serangan membantu analis memahami urutan kejadian, teknik serangan yang digunakan, dan dampak dari insiden tersebut, sehingga memungkinkan pengembangan langkah mitigasi yang lebih efektif[11]. Anomali dapat didefinisikan sebagai suatu penyimpangan atau ketidaknormalan yang terjadi dari kondisi umum atau yang di harapkan. Dan anomali juga bersifat positif negatif[12]. Oleh karena itu berdasarkan permasalahan tersebut perlu dilakukan Analisis forensik berbasis eksperimen pada serangan DDoS di jaringan untuk deteksi anomali dengan menggunakan Metode Network Forensik. Penelitian ini bertujuan untuk menerapkan teknik identifikasi anomali dan rekonstruksi serangan dalam mendeteksi serta menganalisis serangan siber pada jaringan komputer.

2. METODE PENELITIAN



Gambar 1 Alur Penelitian

2.1 Pengumpulan Data

Tahap pengumpulan data merupakan proses awal dalam penelitian yang bertujuan untuk memperoleh berbagai data yang berkaitan dengan objek penelitian. Data yang dikumpulkan dapat berupa log jaringan, aktivitas sistem, trafik data, file digital, maupun bukti digital lainnya. Tahapan ini sangat penting karena kualitas data yang diperoleh akan mempengaruhi hasil analisis pada tahap berikutnya. Semakin lengkap dan relevan data yang dikumpulkan, maka proses identifikasi anomali dapat dilakukan dengan lebih akurat.

2.2 Penyaringan Data

Setelah data berhasil dikumpulkan, tahap selanjutnya adalah penyaringan data. Pada tahap ini dilakukan proses seleksi dan pembersihan data untuk memisahkan data yang relevan dari data yang tidak diperlukan. Dengan adanya penyaringan data, proses identifikasi anomali dapat berjalan lebih efektif dan efisien.

2.3 Identifikasi Anomali

Tahap identifikasi anomali merupakan proses utama dalam penelitian untuk mendeteksi adanya aktivitas yang tidak normal atau mencurigakan. Pada tahap ini sistem akan menentukan apakah data yang dianalisis termasuk kondisi normal atau mengandung indikasi serangan maupun penyimpangan.

2.4 Rekonstruksi Serangan

Tahap rekonstruksi serangan bertujuan untuk menelusuri dan memahami bagaimana serangan terjadi. Pada tahap ini dilakukan analisis terhadap jejak digital, urutan kejadian, sumber serangan, serta metode yang digunakan oleh pelaku. Rekonstruksi serangan membantu peneliti dalam menyusun kronologi kejadian secara sistematis sehingga penyebab dan dampak serangan dapat dipahami dengan jelas.

2.5 Analisis dan Pelaporan

Hasil dari rekonstruksi serangan kemudian dianalisis lebih lanjut dan disusun dalam bentuk laporan penelitian atau laporan investigasi. Laporan tersebut biasanya berisi jenis serangan, metode analisis yang digunakan, bukti digital yang ditemukan, dampak serangan, serta

hasil identifikasi anomali. Tahapan ini bertujuan untuk mendokumentasikan seluruh hasil penelitian secara sistematis dan ilmiah.

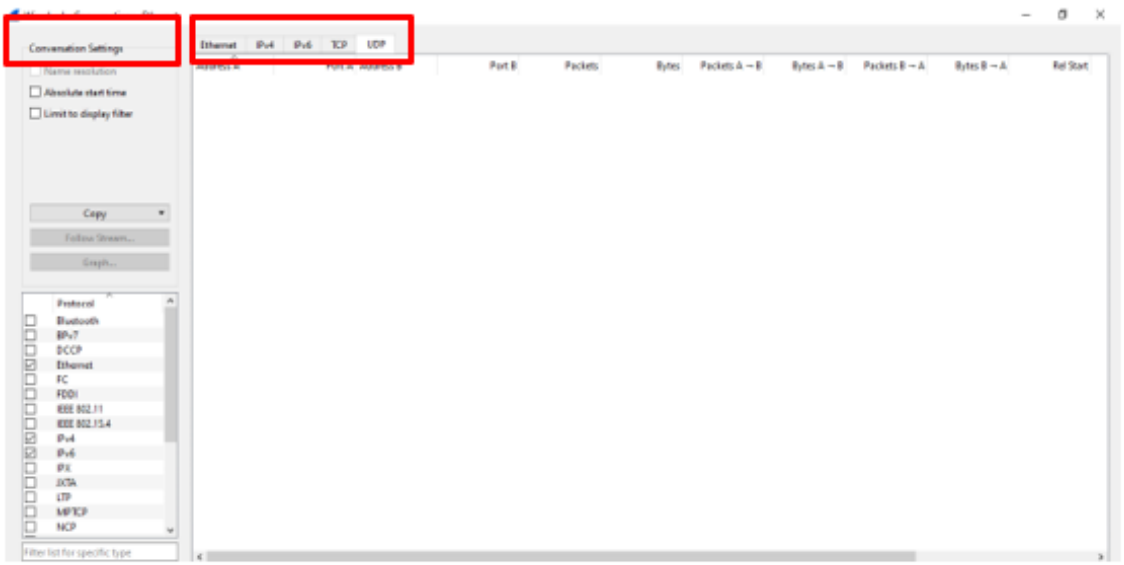
2.6 Tindak Lanjut dan Mitigasi

Tahap tindak lanjut dan mitigasi dilakukan sebagai upaya penanganan terhadap ancaman atau serangan yang ditemukan. Kegiatan mitigasi dapat berupa penutupan celah keamanan, perbaikan konfigurasi sistem, pemblokiran akses berbahaya, serta peningkatan sistem keamanan. Tujuan utama tahap ini adalah untuk mencegah terjadinya serangan serupa di masa mendatang dan meningkatkan keamanan sistem secara keseluruhan

3. HASIL DAN PEMBAHASAN

3.1 Collection

Salah satu serangan ddos adalah serangan gangguan di mana saluran komunikasi mampu menonaktifkan saluran komunikasi sensor dari membawa sinyal dengan menghasilkan tabrakan. Tabrakan akan menyebabkan pesan komunikasi terganggu. Proses awal adalah apakah router masih dengan keadaan normal atau sudah ada serangan DDoS, dapat dilakukan melalui pengecekan melalui menu winbox dan wireshark. Untuk melakukan simulasi peneliti melakukan data awal untuk pembanding bahwa router masih dalam keadaan normal dan router sudah diserang. Untuk melihatnya klik IP+ klik recause pada menu winbox. Dapat dilihat pada gambar berikut:



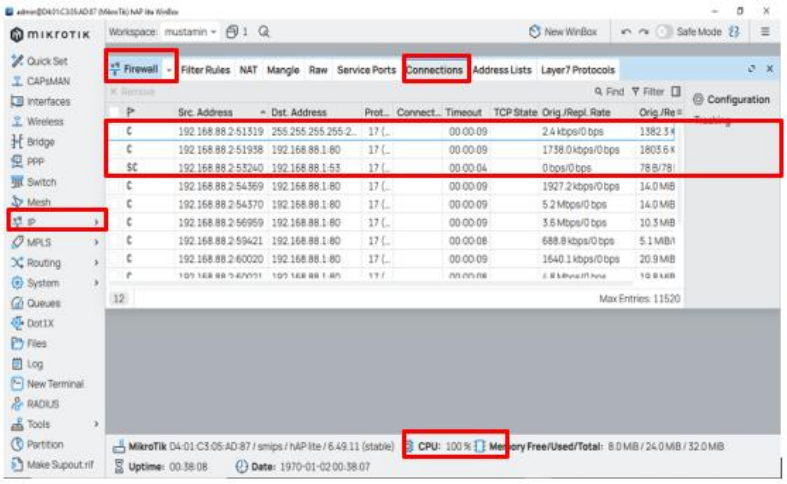
Gambar 2 Sebelum Ada Serangan DDos Di Winbox

Berdasarkan tampilan proses awal pengecekan Gambar 2, dapat disimpulkan belum ada serangan yang masuk dan menganggu lalu lintas jaringan pada router, pada aplikasi Wireshark dan masih dengan keadaan normal. Hal ini dapat di lihat dari kecepatan jaringan yang masih stabil pada IP router yang terhubung pada Wireshark. Langkah berikutnya adalah memulai simulasi serangan DDoS pada router mengunakan aplikasi LOIC (Loid Orbit Ion Canon) untuk mengetahui apakah serangan DDoS yang diluncurkan berhasil membuat jaringan Router mengalami perubahan atau tidak.

Setelah melakukan pengujian pengecekan awal terhadap lalu lintas jaringan pada Router, maka selanjutnya melakukan pengujian mengunakan aplikasi LOIC (Law Orbit Ion Canon) dijalankan Windows untuk melancarkan serangan. Dapat dilihat pada gambar berikut:

Gambar 3 LOIC Untuk Serangan DDoS

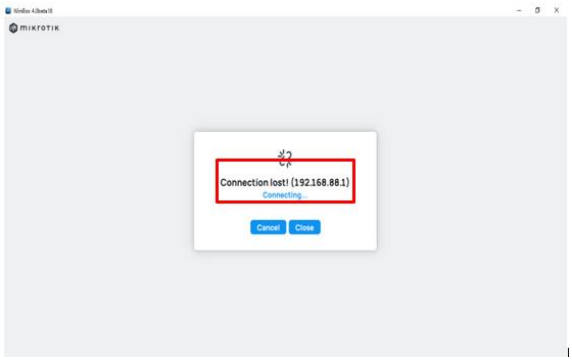
Berdasarkan tampilan Gambar 3 di atas, dapat dijelaskan bahwa aplikasi LOIC berhasil dijalankan dan siap melancarkan serangan ke jaringan Router yang menjadi target serang dengan memasukan ip address 192.168.88.1. Setelah dilakukan serangan, proses selanjutnya melakukan pengecekan serangan yang masuk pada Router melalui aplikasi Winbox dan Wireshark. Selanjutnya dilakukan pengecekan pada Winbox dan Wireshark, untuk melihat apakah serangan tersebut sudah terlihat atau belum. Untuk melihat serangan DDoS dengan cara klik IP+klik *firewall* pada menu Winbox. Dapat dilihat pada Gambar 4 berikut:



Gambar 4 Setelah Ada Serangan DDoS Di Winbox

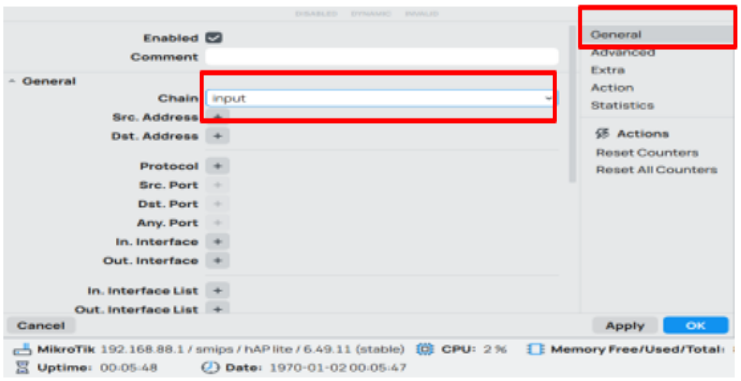
Gambar 4 menunjukkan kondisi router MikroTik setelah mengalami serangan DDoS, yang terdeteksi melalui fitur Connections pada menu IP > Firewall di Winbox. Terlihat bahwa sejumlah koneksi aktif berasal dari IP yang berulang, sebagian besar dari subnet yang sama (192.168.8.2), dengan pola lalu lintas yang tidak wajar, seperti throughput sebesar 0 bps/0 pps. Hal ini mengindikasikan adanya koneksi palsu yang sengaja dibentuk untuk membanjiri sistem. Dampaknya terlihat pada pemakaian CPU yang mencapai 100%, jauh di atas batas normal, yang menunjukkan bahwa proses penanganan koneksi membebani sumber daya router secara signifikan. Kondisi ini dapat menyebabkan router tidak mampu memproses lalu lintas jaringan secara optimal, yang berdampak pada turunnya kualitas layanan, latensi tinggi, bahkan kemungkinan putusnya koneksi internet. Dengan demikian, gambar ini memberikan bukti kuat bahwa serangan DDoS dapat melemahkan performa router dan mengganggu kestabilan jaringan secara keseluruhan.

Kemudian untuk mengentahui IP address penyerang yaitu 192.168.88.2 dengan membanjiri paket data dengan tujuan IP address 192.168.88.1. Tidak butuh waktu sekitar 3 jam membuat Router menjadi down, dapat dilihat pada tampilan Gambar 5



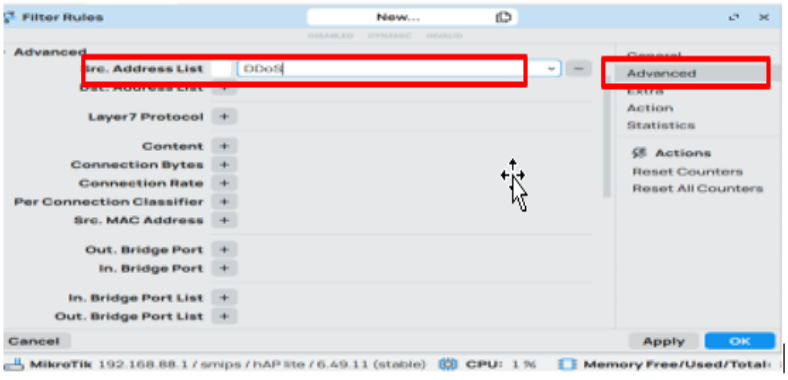
Gambar 5 Router down setelah Serangan DDoS

Gambar 5 menunjukan bahwa Router sudah Down dikarenakan tidak mampu menanggung kenaikan CPU dan Router berkerja terlalu maksimal. yang disebakan pengiriman data yang terus-menerus pada lalu lintas jaringan Router. Selanjutnya melakukan penanganan serangan DDoS dengan cara melakukan setingan kembali, agar router tidak berkerja lebih maksimal bahkan tidak akan mengalami down. Cara nya dengan memperkuat keamanan firewall dapat dilihat pada Gambar 6.



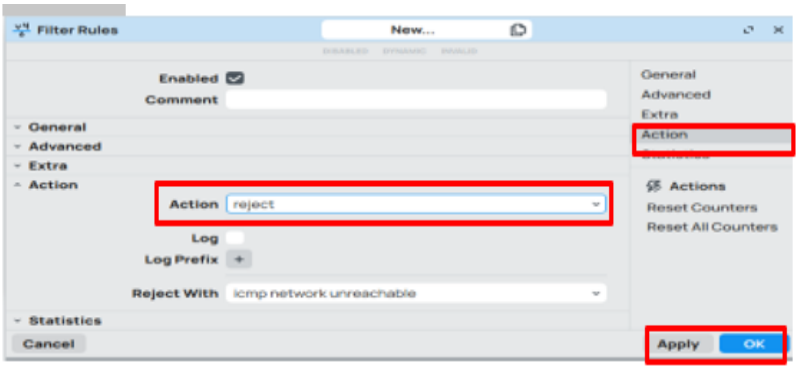
Gambar 6 winbox firewall Rules General

Pada Gambar 6, dapat dilihat bahwa *tab* yang aktif adalah General, yang merupakan bagian awal dari konfigurasi filter rule. Salah satu parameter penting di dalamnya adalah *Chain*, yang diatur ke nilai Input. Pengaturan ini berarti *rule firewall* akan diterapkan terhadap semua paket data yang masuk dan ditujukan langsung ke router MikroTik. Ini sangat berguna dalam upaya mitigasi serangan DDoS, karena serangan jenis ini biasanya membebani router secara langsung. Tab lain seperti *Advanced*, *Action*, dan *Statistics* juga disediakan untuk melengkapi *rule* ini dengan parameter lanjutan, tindakan terhadap trafik, dan statistik eksekusi *rule*. Selanjutnya *Advance* untuk melakukan keamanan *firewall* dapat dilihat pada Gambar 7.



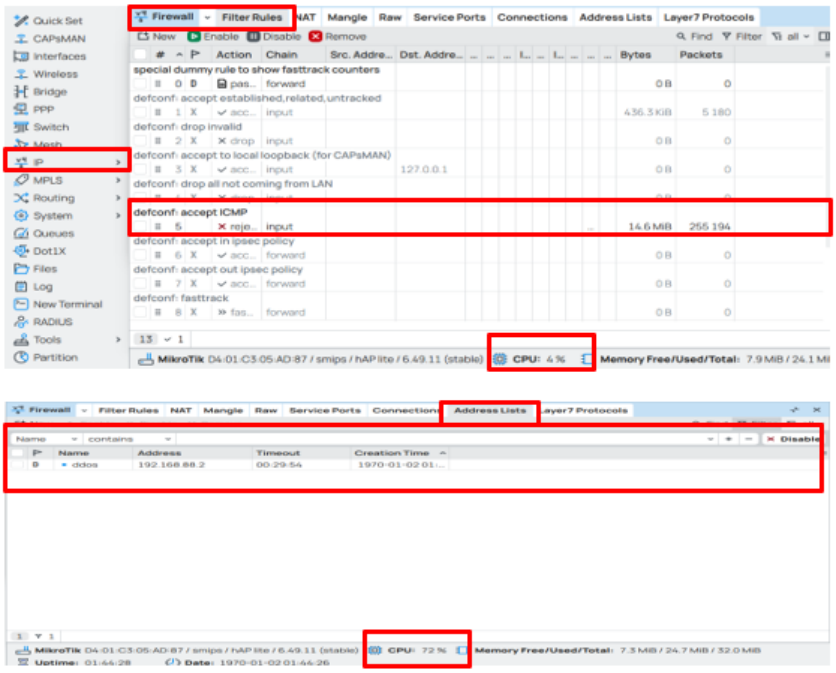
Gambar 7 winbox firewall Rules Advanced

Pada Gambar 7 menunjukkan bahwa rule firewall akan berlaku hanya terhadap alamat IP sumber (source IP) yang sudah dimasukkan ke dalam address list dengan nama DDoS. Address list "DDoS" biasanya berisi IP-IP yang terdeteksi melakukan serangan DDoS terhadap router atau jaringan. Dalam kasus ini, hanya Src. Address List yang digunakan, artinya filter ini berfokus untuk memblokir IP yang masuk daftar hitam (blacklist DDoS). Kemudian tap selanjutnya Action untuk melakukan keamanan firewall dapat dilihat pada Gambar 8.



Gambar 8 winbox firewall Rules Action

Pada Gambar 8 Tab Action berfungsi untuk menentukan tindakan apa yang akan dilakukan terhadap trafik yang memenuhi kondisi pada tab General dan Advanced. Dan Reject berarti paket akan ditolak, dan sistem akan mengirim balasan ke pengirim berupa notifikasi bahwa koneksi ditolak.

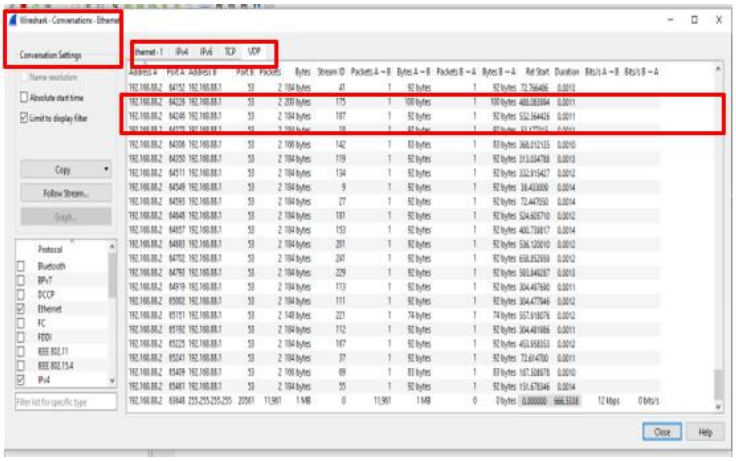


Gambar 9 Konfigurasi firewall winbox sesudah diserang DDoS

Pada Gambar 9 konfigurasi firewall MikroTik yang menunjukkan kombinasi antara Filter Rules dan Address List. *Rule* yang ditampilkan berada pada *chain* input, yang berarti memfilter semua trafik yang ditujukan langsung ke router. Dalam konfigurasi ini, daftar IP yang dicurigai melakukan serangan (misalnya DDoS) dimasukkan ke dalam address list dengan nama ddos. Address list ini kemudian dapat digunakan dalam rule lainnya (di tab Advanced), misalnya untuk melakukan aksi *drop* atau *reject*. Penggunaan address list memungkinkan sistem firewall menjadi

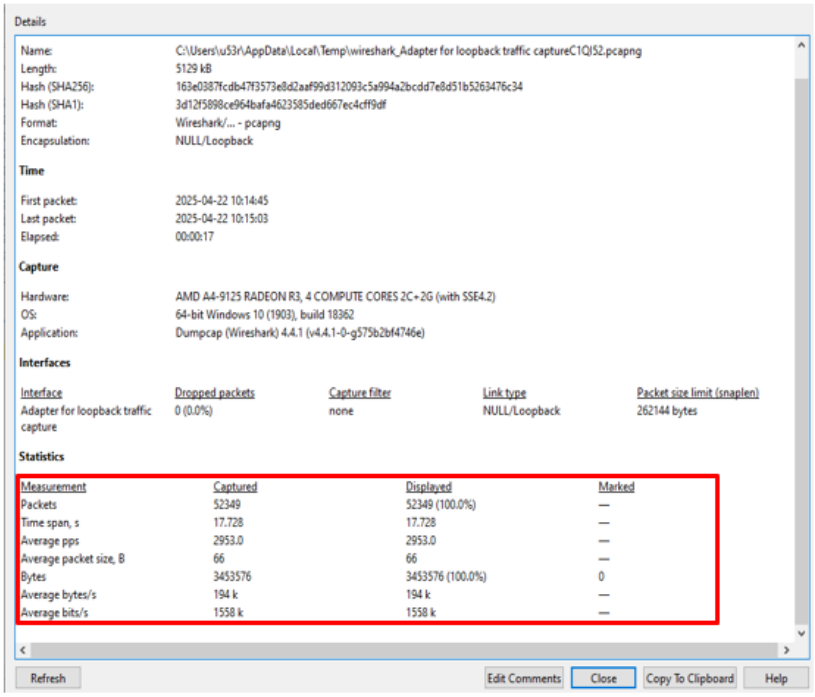
lebih efisien dan dinamis dalam mendeteksi serta memblokir ancaman jaringan. dan keadaan router normal dan serangan DDoS tidak berhasil membuat router down karena paket dikirim berhasil di tolak, dapat di lihat dari tingkat kenaikan CPU router awal saat di serang adalah 72 % hingga turun dengan keadaan normal hingga 4 %.

Selanjutnya dilakukan pengecekan identifikasi anomali mengunakan aplikasi Wireshark, untuk melihat peningkatan *traffic* yang singnifikan pada pola *traffic* yang tidak biasa dan data apa yang dikirim pada Router hingga menjadi Down. Untuk melihat data yang dikirim oleh DDoS di aplikasi Wireshark klik statistc+klik converasion pada menu Wireshark. Dapat dilihat pada tampilan Gambar 10 berikut:



Gambar 10 Tampilan setelah ada serangan DDoS pada Wireshark

Berdasarkan gambar 10 bahwa wireshark mampu membaca kinerja router yang menunjukkan adanya lalu lintas mencurigakan dalam bentuk serangan UDP flood, di mana sejumlah besar paket dikirim dalam waktu sangat singkat dari berbagai port menuju IP tertentu. Ini merupakan karakteristik dari serangan DDoS, yang bertujuan membanjiri sistem target agar tidak bisa melayani permintaan normal dari pengguna yang sah. Kemudian untuk melihat paket capture pada aplikasi wireshak yang telah diserang DDoS klik statistic+klik capture file propertis. Dapat dilihat pada gambar berikut:



Gambar 11 Tampilan setelah ada serangan DDoS pada Wireshark

Berdasarkan gambar 11 data statistik yang ditampilkan pada Wireshark, dapat disimpulkan bahwa telah terjadi lalu lintas jaringan yang tidak normal dengan indikator utama berupa jumlah paket yang sangat tinggi dan kecepatan pengiriman data di atas ambang wajar. Hal ini kuat mengindikasikan adanya serangan Distributed Denial of Service (DDoS), yang bertujuan untuk membanjiri sistem target dan menyebabkan gangguan layanan. Serangan tersebut mengirim paket dengan sangat banyak pada router dan ini dapat menyababkan router tidak dapat mengaturnya di karena data terserbut terlalu banyak. Dan ini salah satu alasannya kenapa router Down.

Setelah melakukan simulasi serangan DDoS pada Router dapat dideteksi dengan mengunakan *identifikasi anomaly* dengan mengunakan aplikasi winbox dan wireshark berhasil mendeteksi loncakan pengiriman data yang memberikan tanda tanda awal dari serangan DDoS. Berikut tabel analisis mengunakan apliaksi winbox dan wireshark:

Tabel 1 Hasil Analisis Serangan DDoS Pada Router Winbox

Analisis	Keterangan
Ip address penyerang	192.168.88.2
Kondisi CPU perangkat Jaringan yang belum diserang	1 %
Kondisi CPU perangkat jaringan yang sudah diserang	100 %
Serangan DDoS pada Router mengunakan aplikasi LOIC	Berhasil melakukan serangan

Tabel 2 Hasil Analisis Serangan DDoS Pada Router Winbox firewall

Analisis	**Keterangan**
Ip address penyerang	192.168.88.2
Kondisi CPU perangkat Jaringan yang belum diserang	1 %
Kondisi CPU perangkat jaringan yang sudah diserang	72 % sampai 4 %
Serangan DDoS pada Router mengunakan aplikasi LOIC	Berhasil melakukan serangan

Tabel 3 Analsisis Serangan DDoS Pada Router Wireshark

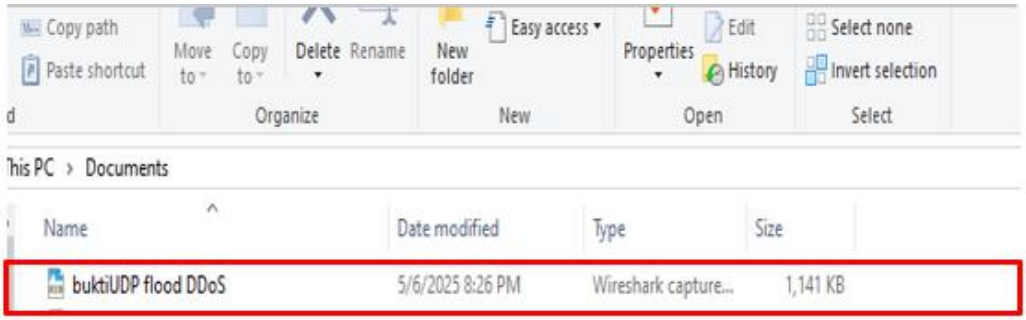
Analisis	Keterangan
Ip address penyerang	192.168.88.2
Paket yang dikirim	*UDP flooding*
Paket capture	52349 (100%)
Serangan DDoS pada router mengunakan aplikasi LOIC	Berhasil melakukan serangan dan dibaca oleh wireshark

Tabel 4 perbedaan analisis winbox dan wireshark

Aspek analisis	**Router winbox dan firewall**	**Router wireshark**
IP address penyerang	192.168.88.2	192.168.88.2
Kondisi CPU sebelum diserang	1 % dan 1 %	Tidak dianalisis
Kondisi CPU sesudah diserang	100 % dan 72 % sampai 4 %	Tidak dianalisis
Aspek analisis	Router winbox dan firewall	Router wireshark
Jenis paket yang dikirim	Tidak disebutkan	UDP flooding
Jumlah peket yang ditangkap	Tidak disebutkan	52349 (100%)

Hasil serangan menggunakan LOIC	Berhasil melakukan serangan	Berhasil melakukan serangan

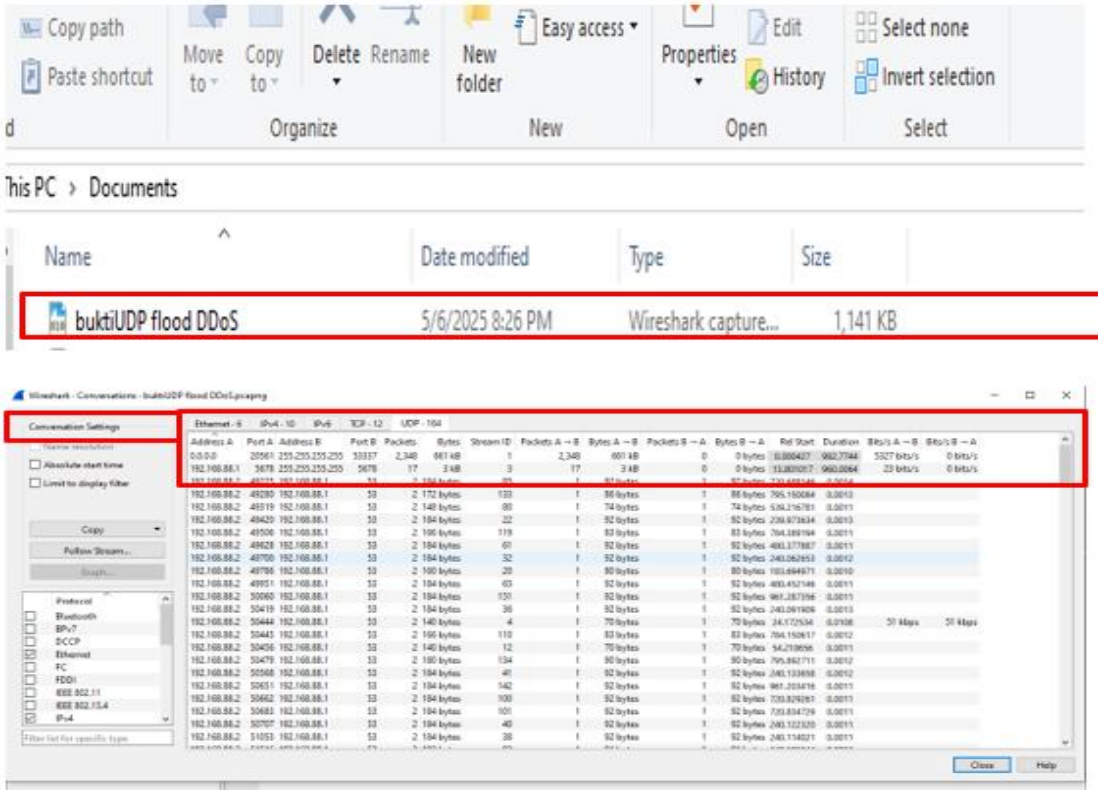
Selanjutnya dilakukan penyimpanan file pcap hasi dari monitoring jaringan yang mendeteksi serangan DDoS dan memberikan waktu kapan serangan terjadi seperti pada gambar di bawah. Pada Gambar 12 diatas dapat dijelaskan bahwa pada tanggal 5/6/2025 telah berhasil melakukan pengambilan data terhadap router yang diserang oleh pihak yang tidak bertanggung jawab.



Gambar 12 file log wireshark

3.2 Examination

Pada tahap ini file log yang telah diambil dan akan diperiksa apakah log aktifitas yang tercacat pada file tersebut adalah aksi serangan DDoS yang sesuai dengan insiden yang terjadi. Dapat dilihat pada Gambar 13.



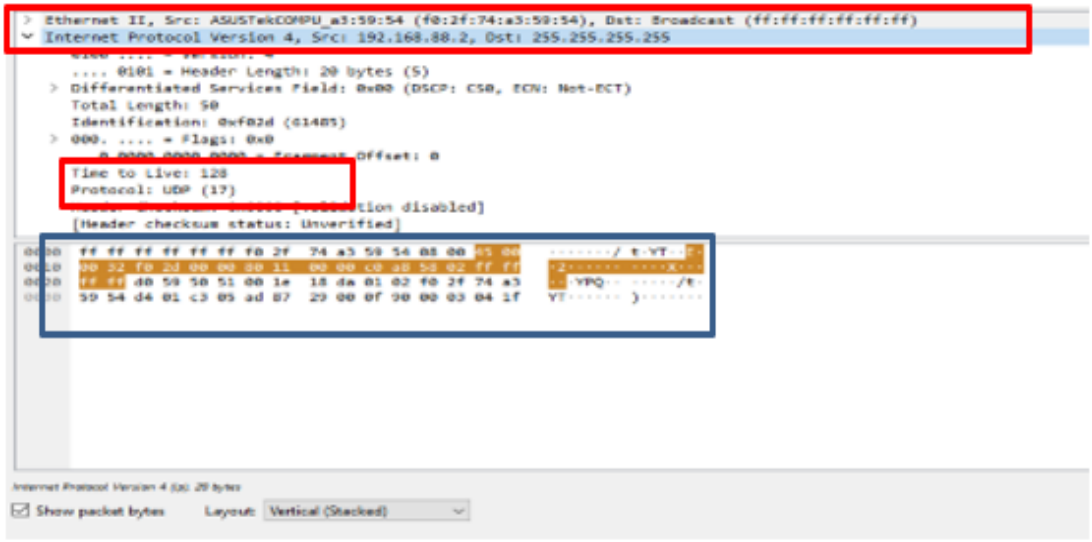
Gambar 13 Data serangan DDoS

Setelah melakukan pemeriksaan data seperti gambar 13 yang di ambil dari file log pada wireshak yang di simpan pada tanggal 5/6/2025 bahwa bukti tersebut memang benar adanya, menunjukkan hasil analisis data serangan DDoS menggunakan aplikasi Wireshark, dengan file bukti bernama buktiUDP flood DDoS. Dari tampilan jendela Conversations Wireshark, terlihat adanya lonjakan trafik UDP yang berasal dari berbagai alamat IP sumber menuju alamat tujuan tertentu. Data pada kolom Packets, Bytes, dan Packets/s menunjukkan bahwa terjadi pengiriman paket dalam jumlah sangat besar dalam waktu singkat, yang merupakan karakteristik khas dari serangan UDP flood DDoS.

Beberapa alamat IP mengirim ribuan paket dengan total data mencapai ratusan kilobyte dalam durasi yang sangat singkat, bahkan dalam hitungan detik. Hal ini mengonfirmasi bahwa trafik yang ditangkap bukan merupakan lalu lintas normal, melainkan serangan yang dirancang untuk membanjiri jaringan dan membebani sistem target. Serangan ini dapat menyebabkan gangguan layanan, keterlambatan respon, hingga kerusakan pada sistem jika tidak segera ditangani.

3.3 Analisis

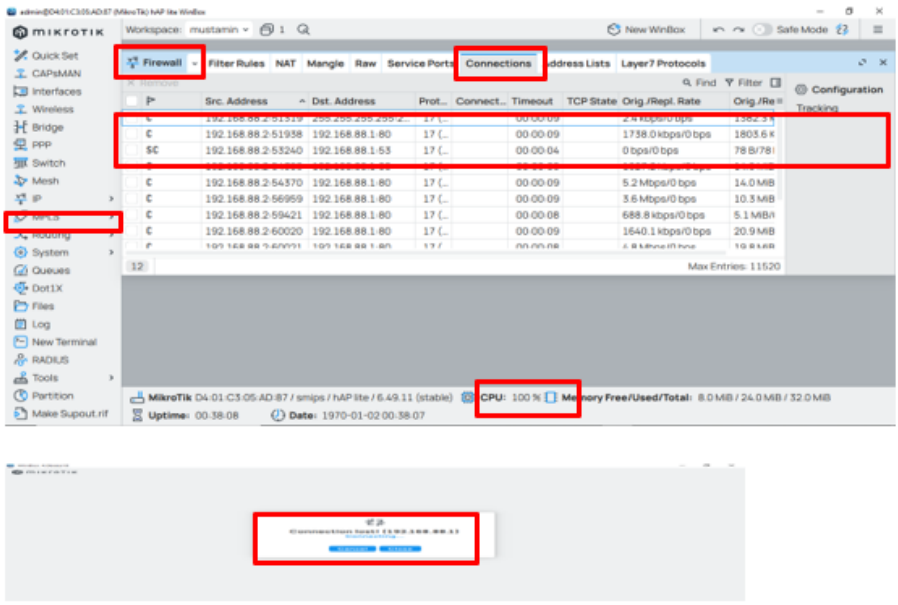
Analisis menjadi satu tahap dan implementasi ke dalam perspektif yaitu perspektif mengunakan tool wireshark. Dengan mengadopsi perspektif ini, penelitian akan mendapkatkan sudut pandang yang beragam dalam menganalisis serangan atau aktifitas mencurigakan dalam jaringan. Ini akan membantu dalam mengidentifikasi, memahami, dan merespon serangan secara lebih efektif.



Gambar 14 Analisis pada wireshark

Pada Gambar 14 menunjukan bahwa dapat diketahui IP address client yaitu 198.168.88.2 yang berarti IP address tersebut adalah sebuah serangan yang sedang berlangsung yang digunakan *attacker*.

Kemudian dengan menggirim paket UDP flood secara terus-menerus, time to live yang artinya jumlah serangan 128 yang sedang berjalan. Dan pada kontak warna biru menjelaskan tentang persentase hexadecimal dari paket data yang dikirim oleh attaker. Kemudian analisis terhadap sebuat router dan dampaknya jika serangan DDoS sedang berlanjut. Untuk melihatnya kita dapat menggunakan winbox. Dapat dilihat pada gambar berikut:



Gambar 15 Analisis pada winbox

Pada Gambar 15 terlihat pada menu winbox klik IP lalu kemudian klik filewall lalu klik connection seperti pada gambar diatas tujaunnya yaitu untuk melakukan analisis terhadap serangan yang telah terjadi pada router yang diatur oleh winbox mikrotik. Setelah melakukan analisis dapat dilihat bahwa telah terjadi sebuah serangan IP Address penyerang yaitu 192.168.88.2 dengan menyerang IP Address router yaitu 192.168.88.1 dengan time out 00:00:09 dan menggalami kenaikan CPU hingga 100% dan tidak butuh waktu lama *router* mengalami *down* karena tidak mampu menanggung kenaikan *traffic* yang terus meningkat seperti pada Gambar 15.

3.4 Reporting

Setelah melakukan tahapan-tahapan dengan metode network forensic maka pada tahap ini dibuat sebuah laporan. Proses pelaporan ini dilakukan agar bukti yang telah dikumpulkan dapat diterima pada proses pengadilan. Dalam proses report ini barang bukti harus dijelaskan secara rinci. Salah satu tindakan agar barang bukti dapat diterima dipersidangan adalah barang bukti harus dicatat secara detail bagaimana cara mendapatkannya dan bagaimana cara pemprosesannya dari barang bukti tersebut. Untuk itu perlu melakukan manajemen barang bukti dengan menerapkan dokumen *chain of custody*. Dokumen *chain of custody* ini belum memiliki standarisasi yang baku. Salah satu model dokumen *chain of custody* yang dapat digunakan dapat dilihat pada gambar berikut.

FORMULIR PENERIMAAN BARANG BUKTI

Informasi Kasus(1)

No Kasus : 04/DDoS/IT/2025 | Hari/Tanggal : 5/6/2025

Lokasi Kasus : server utama komputer/Sulawesi tenggara

Yang Menyerahkan(2)

Nama Jelas	Hari/Tanggal	Jam	Paraf
1. Muhammad Imruddin	Senin,5/06/2025	14:30--WIB	-----
2.			
3.			

Yang Menerima(3)

Nama Jelas	Hari/Tanggal	Jam	Paraf
1. Ridwan (petugas IT forensik)	Senin,5/06/2025	15:00-WIB	----
2.			
3.			

Deskripsi Singkat Kasus(4) :

Telah terjadi serangan Distributed Denial of Service (DDoS) pada server utama Komputer pada tanggal 6 juni 2025 pukul 13:45 WIB. Serangan mengakibatkan gangguan akses layanan selama ±45 menit. Dari hasil analisa awal dengan Wireshark dan MikroTik Winbox, ditemukan aktivitas trafik abnormal (puluhan ribu koneksi per detik) dari berbagai IP anonim. Barang bukti berupa file .pcap hasil capture trafik, log firewall MikroTik, dan tangkapan layar (screenshot) telah diserahkan kepada tim IT Forensik untuk penyelidikan lebih lanjut.

Gambar 16 Dokumen *Chain Of Custody*

4. KESIMPULAN

Metode *network* forensik yang diterapkan menggunakan Wireshark terbukti efektif dalam mendeteksi serangan DDoS. Wireshark mampu menangkap dan menganalisis seluruh paket data yang dikirim oleh penyerang, dengan hasil sebanyak 52.349 paket (100%) yang berhasil dicapture. Jenis serangan yang teridentifikasi adalah UDP flooding melalui aplikasi LOIC. Pemantauan menggunakan Winbox menunjukkan bahwa serangan DDoS berdampak signifikan terhadap performa perangkat router. Hal ini ditunjukkan dengan lonjakan penggunaan CPU dari 1% menjadi 100 %, yang mengindikasikan adanya lonjakan trafik tidak normal akibat serangan.

Penggabungan penggunaan Wireshark untuk analisis paket data dan Winbox untuk pemantauan kondisi perangkat memberikan hasil yang komprehensif dalam proses investigasi forensik jaringan. Kombinasi ini mampu mendeteksi serangan secara teknis dan dampaknya terhadap perangkat, sehingga sangat mendukung proses mitigasi dan dokumentasi insiden keamanan jaringan.Kesimpulan harus mengindikasikan secara jelas hasil-hasil yang diperoleh dan kelebihan dan kekurangannya.

5. SARAN

Untuk penelitian selanjutnya proses pengujian mengunakan wireshark dan winbox dalam mengidentifikasi serangan DDoS sangat terbukti efektif. Dengan ini saya mengucapkan banyak terima kasih kedapa dosen pembimbing yang telah banyak membantu dalam proses penelitian hingga dapat diselesaikan

DAFTAR PUSTAKA

[1] M. Na'im and A. Jum'ah, "Analisa Keamanan Dan Hukum Untuk Pelindungan Data Privasi," *CyberSecurity dan Forensik Digital*, vol. 1, no. 2, pp. 39–44, 2018, https://doi.org/10.14421/csecurity.2018.1.2.1370.

[2] A. Milenius, D. Marly, W . Ardiyasa, and W. K. Utama, "Analisis Keamanan Jaringan Dengan Menggunakan Metode Penetration Testing (Studi Kasus ITB STIKOM Bali)," *Prosiding Seminar Hasil Penelitian Informatika dan Komputer 2025*, vol. 2, no. 1, p. 2025, 2025.

[3] M. Adam, E. I. Alwi, and I. As'ad, "Analisis Forensik Terhadap Serangan Ddos Ping Of Death Pada Server," 2022.

[4] W. Agustiono, D. Wulan Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence," *Jurnal Teknologi dan Informasi (JATI)*, vol. 14, 2024, https://doi.org/10.34010/jati.v14i2.

[5] M. I. Aqilaa, D. Firdaus, and N. Naofal, "Identifikasi Serangan Lowrate Distributed Denial Of Services Dalam Jaringan Dengan Menggunakan Algoritma Adaboost," *Simpatik: Jurnal Sistem Informasi dan Informatika*, 2023, [Online]. Available: https://api.semanticscholar.org/CorpusID:259552303

[6] Akamai, "Application Security Research Report 2024 Download | Akamai," 2024.

[7] I. Riadi *et al.*, "Analisis Forensik Bukti Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Standards And Technology (NIST)," *Jurnal Insand Comtech*, vol. 2, no. 2, 2017.

[8] A. R. Supriyono, B. Sugiantoro, and Y. Prayudi, "Eksplorasi Bukti Digital Pada Smart Router Menggunakan Metode Live Forensics," *Jurnal Infotekmesin*, vol. 10, no. 02, 2019, https://doi.org/10.35970/infotekmesin.v10i2.48.

[9] R. H. W. Murti, I. Riadi, N. Anwar, and T. Ismail, "Forensik Jaringan Terhadap Serangan DDOS Menggunakan Metode Network Forensic Development Life Cycle," *JSTIE (Jurnal*

Sarjana Teknik Informatika) (E-Journal), vol. 11, no. 3, p. 107, Oct. 2023, https://doi.org/10.12928/jstie.v11i3.26544.

[10] I. G. N. A. W. Sucipta I Made Widhi; Muliantara, Agus, "ANALISIS KINERJA ANOMALY-BASED INTRUSION DETECTION SYSTEM (IDS) DALAM MENDETEKSI SERANGAN DOS (DENIAL OF SERVICES) PADA JARINGAN KOMPUTER," JELIKU (Jurnal Elektron. Ilmu Komput. Udayana), no. Volume 1 No 2-Nopember 2012, pp. 8–13, 2012, [Online]. Available: https://ojs.unud.ac.id/index.php/JLK/article/view/4894/3677.

[11] E. Muhati and D. Rawat, "Data-Driven Network Anomaly Detection with Cyber Attack and Defense Visualization," *Journal of Cybersecurity and Privacy*, vol. 4, no. 2, pp. 241–263, Jun. 2024, https://doi.org/10.3390/jcp4020012.

[12] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016, https://doi.org/10.1016/j.jnca.2015.11.016.