p-ISSN : 2406-7733
e-ISSN : 2597-9922

ANALISIS FORENSIK DIGITAL SERANGAN DDOS MENGGUNAKAN METODE ISSAF DAN NIST

Wiwin Aswawarman[1], Elvi Saktiawati Salemaku[2], Hasmina Tari Mokui[3], Mustarum Musaruddin[4]
[1,2]Program Studi Manajemen Rekayasa, Program Pascasarjana, Universitas Halu Oleo
[3]Jurusan Teknik Elektro, Fakultas Teknik, Universitas Halu Oleo
[4]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo
Jl. H.E.A. Mokodompit, Kelurahan Kambu, Kecamatan Kambu, Kota Kendari, Indonesia
E-mail: wiwinaswawarman25@gmail.com[1], salemakuelvisaktiawati@gmail.com[2], *hasmina.mokui@uho.ac.id[3], mustarum@uho.ac.id[4]

Abstrak - Perkembangan teknologi informasi yang pesat membuka celah meningkatnya kejahatan siber, khususnya serangan *Distributed Denial of Service* (DDoS). Berdasarkan laporan Cloudflare Radar, volume serangan HTTP DDoS meningkat sebesar 65% pada kuartal ketiga 2023 dibandingkan kuartal sebelumnya. Di Indonesia, Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 1,6 miliar anomali trafik pada 2021, sebagian besar terindikasi sebagai serangan siber termasuk DDoS yang menargetkan institusi pendidikan dan pemerintahan. Penelitian ini bertujuan menganalisis proses terjadinya serangan DDoS pada web server Universitas Nahdlatul Ulama Sulawesi Tenggara (UNUSULTRA) dan mengungkap bukti digital melalui pendekatan forensik digital. Penelitian menggunakan dua metode yaitu *Information System Security Assessment Framework* (ISSAF) untuk simulasi serangan penetrasi menggunakan KARMA-DDoS, dan *National Institute of Standards and Technology* (NIST) untuk investigasi forensik menggunakan Wireshark dan NetworkMiner. Hasil menunjukkan simulasi serangan DDoS berhasil mengganggu layanan *web server*, dibuktikan dengan munculnya pesan *error establishing a database connection*. Bukti digital berupa alamat IP penyerang, paket ICMP, pola trafik mencurigakan, dan koneksi SSL masif berhasil diidentifikasi serta direkonstruksi secara kronologis. Penelitian ini mengintegrasikan *dual framework* (ISSAF+NIST) dengan *dual tools* forensik (Wireshark+NetworkMiner) pada *web server* Universitas Nahdlatul Ulama Sulawesi Tenggara, sehingga dapat menjadi rujukan penguatan sistem keamanan jaringan di lingkungan akademik.

Kata Kunci: DDoS, Digital Forensik, ISSAF, NIST

I. PENDAHULUAN

Perkembangan teknologi informasi yang pesat membawa kemudahan dalam penyebaran informasi, namun juga membuka celah bagi meningkatnya kejahatan siber. Keamanan informasi mencakup tiga aspek utama yang dikenal sebagai prinsip CIA *Triad*: kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Ketiga aspek ini menjadi fondasi utama dalam perancangan sistem keamanan informasi modern, terutama dalam menghadapi ancaman siber yang terus berkembang (Harahap et al., 2023). Berdasarkan data Badan Siber dan Sandi Negara (BSSN) tahun 2021, tercatat 332 aduan insiden keamanan siber. Pada tahun yang sama, BSSN mendeteksi lebih dari 1,6 miliar anomali trafik yang terindikasi sebagai aktivitas serangan siber, dengan sektor pemerintahan dan pendidikan menjadi yang paling terdampak. Laporan *Cloudflare* Radar menunjukkan bahwa volume serangan HTTP *Distributed Denial of Service* (DDoS) meningkat sebesar 65% pada kuartal ketiga 2023 dibandingkan kuartal sebelumnya, dipicu oleh kampanye serangan hipervolumetrik yang menargetkan berbagai layanan internet secara global (Cloudflare, 2023).

Berbagai penelitian telah dilakukan untuk memahami karakteristik dan dampak serangan DDoS. Penelitian forensik jaringan menggunakan metode ADDIE dan HIDS menunjukkan bahwa serangan *Slowloris* memiliki dampak paling signifikan terhadap performa web server IIS, dengan pola pembukaan koneksi HTTP secara berulang tanpa menyelesaikan proses permintaan sehingga menghabiskan sumber daya server (Suharti et al., 2022). *Penetration testing* terhadap *website* Program Studi Pendidikan Teknologi Informasi menggunakan Slowloris dan C2 menunjukkan bahwa serangan DDoS dapat menyebabkan *website down* akibat kehabisan sumber daya, serta direkomendasikan peningkatan keamanan melalui penambahan kuota socket dan pengujian berkala (Madina & Fadhli, 2024). Penelitian lain menggunakan Wireshark menganalisis serangan DDoS *Ping of Death* dan menemukan bahwa serangan dilakukan dengan mengirimkan paket ICMP berukuran besar yang dapat menyebabkan sistem target mengalami crash (Pratama & Servanda, 2024). Metode Jaringan Saraf Tiruan (JST) dengan pendekatan *fixed moving window* menghasilkan tingkat akurasi 95% dalam mengenali serangan DDoS (Ridho & Arman, 2020). Implementasi HoneyPy dan Maltrail menunjukkan kemampuan efektif dalam mendeteksi aktivitas serangan DoS pada server (Alfidzar & Zen, 2022). Implementasi IDS berbasis Wireshark berhasil melakukan *real-*

p-ISSN : 2406-7733
e-ISSN : 2597-9922

time network monitoring dan mendeteksi IP penyerang (Aldafian et al., 2025). Penelitian lain menunjukkan bahwa serangan Slow HTTP DoS menggunakan SlowHTTPTest meningkatkan waktu respons server hingga 700–900% dan menyebabkan rata-rata kegagalan permintaan 83,6% (Zebua et al., 2025).

Dari sisi *framework* forensik, penelitian menggunakan metode *Live Forensics* pada serangan DDoS jenis DNS *Flooding* berhasil mengidentifikasi pola serangan dan alamat IP penyerang (Putra et al., 2023). Akuisisi bukti digital aplikasi Viber menggunakan *framework* NIST membuktikan konsistensi dan kemampuan replikasinya dalam proses forensik digital (Syahib et al., 2023). Penerapan NIST dalam analisis forensik digital terbukti mampu menyediakan tahapan investigasi yang terstruktur dan sistematis (Matondang & Maulana, 2023). Pengujian keamanan menggunakan framework ISSAF pada website SMK Al-Kautsar membuktikan relevansi ISSAF dalam konteks pengujian keamanan aplikasi web (Andriyan et al., 2023).

Analisis terhadap penelitian-penelitian terdahulu mengungkap *research gap* sebagai berikut: (1) sebagian besar penelitian hanya menggunakan satu *framework* forensik seperti NIST atau *Live Forensics* tanpa mengintegrasikannya dengan framework pengujian penetrasi terstruktur seperti ISSAF; (2) penggunaan *dual-tools* forensik Wireshark dan NetworkMiner secara bersamaan dan komparatif dalam satu studi masih sangat terbatas; (3) objek penelitian umumnya berupa server lokal atau lingkungan terkontrol, bukan *web server* perguruan tinggi aktif yang dilindungi layanan CDN. Oleh karena itu, penelitian ini dilaksanakan dengan dua tujuan: (1) menganalisis proses terjadinya serangan DDoS pada *web server* UNUSULTRA melalui simulasi menggunakan framework ISSAF; (2) menerapkan *framework* NIST untuk mengungkap dan merekonstruksi bukti digital serangan secara sistematis menggunakan Wireshark dan NetworkMiner.

Hasil penelitian diharapkan memberikan implikasi praktis dan akademis yang signifikan. Secara praktis, temuan ini dapat menjadi referensi bagi institusi pendidikan di Indonesia dalam membangun prosedur investigasi forensik DDoS yang terstandarisasi, khususnya untuk *web server* yang dilindungi layanan CDN. Secara akademis, pendekatan *dual-framework* ISSAF dan NIST yang dikombinasikan dengan *dual tools* Wireshark dan NetworkMiner menawarkan model metodologis yang dapat diadopsi dan dikembangkan lebih lanjut pada objek penelitian yang lebih beragam.

II. TINJAUAN PUSTAKA

Serangan *Distributed Denial of Service* (DDoS) merupakan bentuk serangan siber yang bertujuan melumpuhkan layanan dengan cara membanjiri target menggunakan trafik dari banyak sumber secara bersamaan. Serangan DDoS dapat dikategorikan berdasarkan lapisan OSI yang diserang: serangan lapisan jaringan (*Layer* 3/4) seperti ICMP Flood dan SYN Flood, serta serangan lapisan aplikasi (*Layer* 7) seperti HTTP *Flood* dan *Slowloris* yang lebih sulit dideteksi karena menyerupai trafik normal (Madina & Fadhli, 2024; Suharti et al., 2022; Zebua et al., 2025).

Digital forensik adalah proses pengumpulan, pemeriksaan, analisis, dan pelaporan bukti digital secara ilmiah dan dapat dipertanggungjawabkan secara hukum. Dalam konteks forensik jaringan, bukti digital umumnya berupa *file* pcap yang merekam seluruh lalu lintas jaringan dalam rentang waktu tertentu (Putra et al., 2023; Syahib et al., 2023).

Information System Security Assessment Framework (ISSAF) adalah kerangka kerja komprehensif untuk evaluasi keamanan sistem informasi yang dilaksanakan melalui tiga fase utama: perencanaan dan persiapan (*planning and preparation*), penilaian (*assessment*), dan pelaporan (*reporting*). Fase *assessment* mencakup pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, pengujian penetrasi, dan eskalasi hak akses (Andriyan et al., 2023; Madina & Fadhli, 2024). ISSAF banyak digunakan dalam penelitian keamanan karena menyediakan panduan teknis yang terinci dan terstruktur.

National Institute of Standards and Technology (NIST) menyediakan panduan investigasi forensik digital melalui empat tahapan utama: *collection* (pengumpulan), *examination* (pemeriksaan), *analysis* (analisis), dan *reporting* (pelaporan). *Framework* ini bersifat fleksibel sehingga dapat diterapkan pada berbagai jenis insiden siber dan telah terbukti menghasilkan investigasi yang sistematis, terstruktur, dan dapat dipertanggungjawabkan secara hukum (Fitriana et al., 2020; Matondang & Maulana, 2023; Riadi et al., 2021).

Wireshark adalah *tools* analisis protokol jaringan *open-source* yang mampu menangkap dan menganalisis lalu lintas jaringan secara *real-time* maupun dari *file* hasil tangkapan (pcap). Wireshark mendukung filter BPF dan *display filter* yang memungkinkan isolasi paket berdasarkan protokol, alamat IP, atau flag TCP tertentu (Aldafian et al., 2025; Hanipah & Dhika, 2020). NetworkMiner adalah *tools* forensik jaringan pasif yang menganalisis file pcap untuk mengekstrak informasi host, sesi koneksi, *file* yang ditransfer, kredensial,

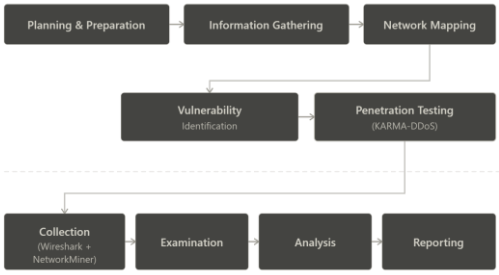
p-ISSN : 2406-7733
e-ISSN : 2597-9922

dan metadata paket tanpa melakukan injeksi trafik aktif (Mahalini et al., 2022).

Beberapa penelitian relevan yang menjadi landasan studi ini antara lain: Suharti et al. (2022) yang menerapkan ADDIE dan HIDS pada serangan Slowloris; Madina & Fadhli (2024) yang melakukan *penetration testing* DDoS pada *website* pendidikan; Syahib et al. (2023) yang menggunakan NIST untuk akuisisi bukti digital aplikasi Viber; serta Andriyan et al. (2023) yang menerapkan ISSAF pada pengujian keamanan website. Penelitian-penelitian tersebut secara umum menggunakan *single framework* dan objek server lokal, berbeda dengan pendekatan *dual-framework* pada web server aktif yang diterapkan dalam penelitian ini.

III. METODE PENELITIAN

Penelitian ini mengadopsi pendekatan eksperimental dengan desain simulasi serangan siber terkendali (*controlled cyber-attack simulation*). Objek penelitian adalah *web server* aktif Universitas Nahdlatul Ulama Sulawesi Tenggara (UNUSULTRA) dengan domain *unusultra.ac.id*, yang telah memperoleh izin resmi dari institusi sebagai syarat pelaksanaan *white-hat penetration testing*. Penelitian dilaksanakan dari Mei hingga Juli 2025. Dua framework digunakan secara berurutan: (1) ISSAF untuk fase simulasi serangan dan penilaian keamanan; (2) NIST untuk fase investigasi forensik digital. Gambar 1 menyajikan alur kerja penelitian secara keseluruhan.



Gambar 1. Alur Kerja Penelitian (*Framework* ISSAF + NIST)

A. Skenario Pengujian

Serangan DDoS dirancang menggunakan skenario yang terstruktur sebagaimana tersaji pada Tabel 1. Skenario ini dipilih karena mencerminkan kondisi serangan nyata pada *web server* yang dilindungi layanan CDN, sehingga hasil forensik yang diperoleh memiliki relevansi praktis yang tinggi.

Tabel 1. Skenario Pengujian

Parameter	Detail
Target URL	https://unusultra.ac.id
Tools Serangan	KARMA-DDoS
Layer Serangan	*Layer* 7 (*Application Layer*)
Metode	*Bypass Cloudflare Attack*
Jumlah *Thread*	100
Durasi Serangan	60 detik (1 menit)
Platform Penyerang	Kali Linux 2024.4
Tools Forensik	Wireshark v4.0.8 + NetworkMiner
Format Bukti	.pcap, .pcapng, .pdf

B. *Framework* ISSAF (Simulasi Serangan)

ISSAF dilaksanakan melalui tiga fase sebagai berikut:

Fase 1 – Planning and Preparation: Perancangan ruang lingkup pengujian, perolehan izin resmi dari pihak UNUSULTRA, dan persiapan lingkungan uji. Tahap ini penting secara etis dan hukum untuk memastikan pengujian dilakukan dalam batas yang sah.

Fase 2 – Assessment: Terdiri dari empat langkah berurutan: (a) *Information Gathering* menggunakan Nmap, Shodan, Whois, Sublist3r, dan theHarvester; (b) *Network Mapping* mengidentifikasi *port* dan layanan aktif menggunakan Nmap; (c) *Vulnerability Identification* menggunakan Acunetix 13; dan (d) *Penetration Testing* menggunakan KARMA-DDoS pada Layer 7 OSI dengan metode *Bypass Cloudflare Attack*.

Fase 3 – Reporting: Dokumentasi seluruh temuan dari fase *Assessment* sebagai bahan evaluasi dan rekomendasi keamanan.

C. *Framework* NIST (Investigasi Forensik Digital)

Framework NIST digunakan untuk memandu investigasi forensik digital melalui empat tahapan:

(1) ***Collection***: Pengumpulan bukti digital dari rekaman paket jaringan menggunakan Wireshark (format .pcap) dan NetworkMiner (format .pdf) selama simulasi serangan berlangsung.

(2) ***Examination***: Identifikasi data yang berpotensi menjadi bukti dengan menyaring lalu lintas mencurigakan, mengidentifikasi pola trafik abnormal, dan menganalisis komunikasi antar host.

(3) ***Analysis***: Analisis mendalam terhadap data yang dikumpulkan untuk menemukan elemen yang dapat dijadikan barang bukti, meliputi identifikasi IP penyerang, jenis protokol serangan, dan volume trafik.

(4) ***Reporting***: Penyusunan laporan tertulis yang berisi hasil analisis forensik, kronologi serangan berbasis *timestamp*, bukti pendukung, dan rekomendasi mitigasi.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

D. Teknik Analisis Data

Analisis data dilakukan secara kuantitatif dan kualitatif secara bersamaan. Secara kuantitatif, data pcap dianalisis menggunakan filter Wireshark untuk mengukur volume paket, distribusi panjang paket (*Packet Lengths*), dan statistik hierarki protokol (*Protocol Hierarchy Statistics*). Filter yang digunakan meliputi: (1) *icmp* untuk mengisolasi paket ICMP Echo Request dan Echo Reply; (2) *tcp.port == 443* untuk menganalisis koneksi HTTPS; (3) *ip.src == 10.0.2.15* untuk mengidentifikasi paket dari host penyerang.

Secara kualitatif, pola serangan diidentifikasi berdasarkan karakteristik trafik abnormal: pengiriman paket masif dari satu sumber IP dalam rentang waktu singkat, pola RST-ACK yang berulang, serta lonjakan *burst rate* yang tidak wajar. Suatu paket diklasifikasikan sebagai bukti serangan apabila memenuhi minimal dua kriteria: (a) berasal dari IP penyerang yang teridentifikasi; (b) memiliki pola pengiriman berulang dalam interval sangat singkat (<0,5 detik); (c) mengakibatkan respons TCP RST-ACK dari server target.

IV. HASIL DAN PEMBAHASAN

A. Hasil Pengujian Framework ISSAF

1) Information Gathering

Pemindaian alamat IP publik menggunakan Nmap menghasilkan alamat 104.21.17.74. Melalui Shodan diperoleh IP privat 192.250.235.154. Hasil Whois menunjukkan domain terdaftar atas nama Pandi-DO1990991 dengan penyedia PT Cloud Hosting Indonesia (care@idcloudhost.co.id). Enumerasi subdomain menggunakan Sublist3r berhasil mengidentifikasi 16 subdomain aktif (Tabel 2), sedangkan theHarvester mengungkap enam alamat email terkait domain.



Gambar 2. Hasil *Tools* Nmap



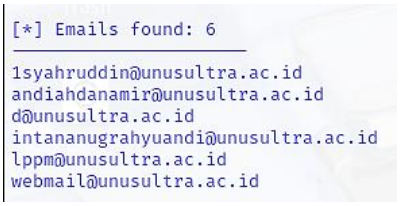
Gambar 3. Hasil *Tools* Shodan



Gambar 4. Hasil *Tools* Whois



Gambar 5. Hasil Enumerasi Subdomain Sublist3r



Gambar 6. Hasil theHarvester

Tabel 2. Subdomain Website unusultra.ac.id

No	Subdomain
1	www.unusultra.ac.id
2	cpanel.unusultra.ac.id
3	febi.unusultra.ac.id
4	fh.unusultra.ac.id
5	fisip.unusultra.ac.id
6	fmipa.unusultra.ac.id
7	ft.unusultra.ac.id
8	jurnal.unusultra.ac.id
9	ljm.unusultra.ac.id
10	lppm.unusultra.ac.id
11	mail.unusultra.ac.id
12	pmb.unusultra.ac.id
13	siakad.unusultra.ac.id
14	siakad2.unusultra.ac.id
15	sister.unusultra.ac.id
16	webmail.unusultra.ac.id

2) Network Mapping

Pemindaian *port* menggunakan Nmap menemukan delapan port aktif sebagaimana tersaji pada Tabel 3. Keberadaan port 21 (FTP) menjadi perhatian khusus karena protokol FTP tidak mengenkripsi data yang ditransmisikan sehingga rentan terhadap penyadapan. Port 1723 yang menggunakan PPTP juga memiliki kelemahan pada mekanisme enkripsi dan autentikasi. Kedua port ini

p-ISSN : 2406-7733
e-ISSN : 2597-9922

berpotensi menjadi vektor serangan yang dapat dieksploitasi lebih lanjut.

```
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp open  pptp
8080/tcp open  http-proxy
8443/tcp open  https-alt
```

Gambar 7. Hasil Network Mapping Nmap

Tabel 3. Port Terbuka pada Web Server UNUSULTRA

No	Port	Service
1	21/tcp	FTP
2	53/tcp	DNS
3	80/tcp	HTTP
4	443/tcp	HTTPS
5	554/tcp	RTSP
6	1723/tcp	PPTP
7	8080/tcp	HTTP-Proxy
8	8443/tcp	HTTPS-alt

3) Vulnerability Identification

Identifikasi kerentanan menggunakan Acunetix 13 menemukan 6 jenis kerentanan (Tabel 4). Kerentanan paling signifikan adalah tidak adanya perlindungan CSRF (*Cross-Site Request Forgery*) pada formulir HTML, dikategorikan *Medium* karena berpotensi dieksploitasi untuk memanipulasi tindakan pengguna yang telah terautentikasi. Kerentanan *Clickjacking* akibat tidak dikonfigurasinya *header X-Frame-Options* dikategorikan *Low*. Cookie tanpa atribut *HttpOnly* berpotensi diakses oleh skrip klien seperti JavaScript, membuka risiko pembajakan sesi pengguna.



Gambar 8. Hasil Scan Kerentanan Acunetix 13

Tabel 4. Jenis dan Tingkat Kerentanan Website

Jenis Kerentanan	Level
HTML form without CSRF protection	*Medium*
Clickjacking: X-Frame-Options header missing	*Low*
Cookie(s) without HttpOnly flag set	*Low*
Content Security Policy (CSP) not implemented	*Informational*
Possible username or password disclosure	*Informational*
Reverse proxy detected	*Informational*

4) Penetration Testing (Simulasi Serangan DDoS)

Pengujian penetrasi dilakukan menggunakan KARMA-DDoS pada Kali Linux dengan metode *Bypass Cloudflare Attack* Layer 7 OSI, 100 *thread*, durasi 60 detik terhadap target https://unusultra.ac.id. *Layer* 7 dipilih karena serangan pada lapisan aplikasi lebih sulit dideteksi oleh mekanisme perlindungan DDoS berbasis volume.

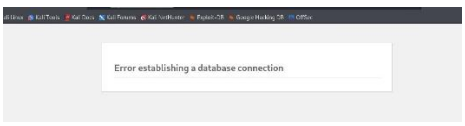


Gambar 9. Tools KARMA-DDoS di GitHub



Gambar 10. Proses Serangan DDoS pada URL Target UNUSULTRA

Hasil pengujian menunjukkan serangan berhasil menimbulkan gangguan layanan pada *web server*. Saat mengakses domain target melalui browser, muncul pesan *"error establishing a database connection"*, yang mengindikasikan server tidak mampu menangani lonjakan permintaan yang dikirimkan secara masif dalam waktu singkat.



Gambar 11. Tampilan *Browser* Menunjukkan *"Error Establishing a Database Connection"*

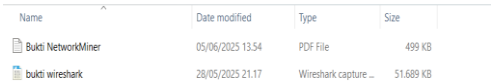
B. Analisis Forensik Digital (Framework NIST)

1) Collection (Pengumpulan Bukti)

Bukti digital dikumpulkan menggunakan Wireshark (format .pcap) dan NetworkMiner (format .pdf). Data yang berhasil dikumpulkan mencakup rekaman komunikasi antar *host*, pola lalu lintas yang mencurigakan, serta metadata paket data yang relevan untuk dianalisis lebih lanjut. Dua sesi

p-ISSN : 2406-7733
e-ISSN : 2597-9922

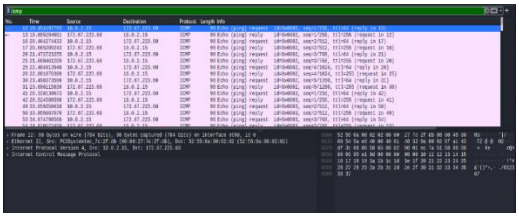
perekaman dilakukan: sesi pertama pada 26 Mei 2025 dan sesi kedua pada 4 Juni 2025.



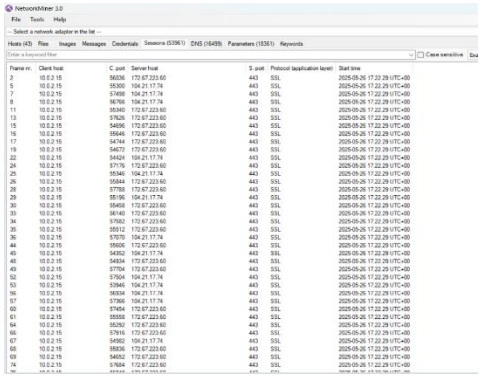
Gambar 12. Hasil Pengumpulan Bukti pada NetworkMiner dan Wireshark

2) Examination (Pemeriksaan Bukti)

Pemeriksaan Wireshark menunjukkan host IP 10.0.2.15 mengirimkan paket ICMP Echo Request secara berulang ke server IP 172.67.223.60 dengan karakteristik: (1) jenis komunikasi ICMP Echo Request dan Echo Reply; (2) panjang paket seragam 98 byte; (3) nilai TTL 64 untuk paket terkirim dan 255 untuk balasan; (4) interval antar paket hanya 0,2 detik, tipikal serangan *Ping Flood*. Pemeriksaan NetworkMiner menunjukkan koneksi ke dua IP server (172.67.223.60 dan 104.21.17.74) melalui port 443 dengan protokol SSL.



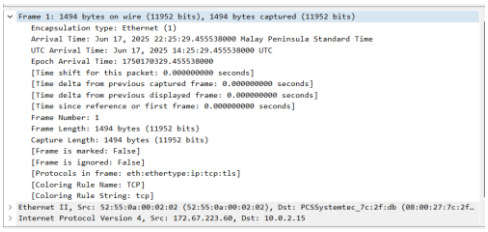
Gambar 13. Hasil Pemeriksaan Wireshark Paket ICMP *Echo Request* Berulang



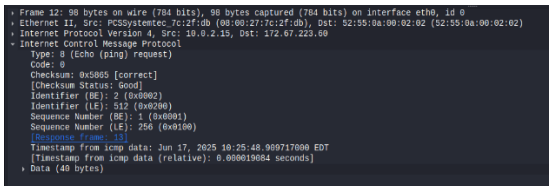
Gambar 14. Hasil Pemeriksaan NetworkMiner – Koneksi SSL ke Server Target

3) Analysis (Analisis Bukti)

Analisis paket Wireshark mendeteksi frame berukuran 1.494 byte menggunakan enkapsulasi Ethernet dengan protokol TCP yang dienkripsi TLS, dengan IP sumber 10.0.2.15 dan tujuan 172.67.223.60. Analisis ICMP memperlihatkan pengiriman paket tipe 8 (*Echo Request*) secara masif, karakteristik khas serangan DDoS berbasis ICMP yang bertujuan menghabiskan bandwidth dan sumber daya server.



Gambar 15. Analisis Detail *Frame* pada Wireshark



Gambar 16. Paket ICMP Echo Request Tipe 8

Analisis NetworkMiner menunjukkan host 10.0.2.15 mengirimkan 86.534 paket (total 6.794.425 byte) dan menerima 87.275 paket (15.095.993 byte), dengan 1.413 sesi koneksi keluar dan latensi 0,026 ms, mengindikasikan aktivitas jaringan yang sangat tinggi dan intensif.



Gambar 17. *Protocol Hierarchy Statistics*

Dari statistik hierarki protokol, Ethernet mendominasi dengan 100% dari total 321.182 paket dan 418.394.946 byte. IPv6 berkontribusi 45,9% dari jumlah paket. Keberadaan paket TCP [RST, ACK] berulang dari IP Cloudflare (172.67.223.60) mengindikasikan pemutusan koneksi paksa sebagai respons mitigasi aktif terhadap serangan.

4) Reporting

Berdasarkan seluruh tahapan investigasi, rekonstruksi kronologi serangan DDoS berbasis *timestamp* disajikan pada Tabel 6 (halaman berikutnya). Pada sesi pertama (26 Mei 2025), serangan dimulai pukul 17:22:30.000 UTC. Trafik tereskalasi masif pada Frame 4–4.713 dengan interval <0,01 detik. Puncak dampak terkonfirmasi pada Frame 22.335 melalui paket ICMP *Destination Unreachable*, berkorelasi dengan pesan "*error establishing a database connection*" di browser.

Pada sesi kedua (4 Juni 2025), perekaman menghasilkan 321.182 paket. Filter *ip.dst == 104.21.17.74* mengidentifikasi 7.371 paket TCP SYN dan TLSv1.3 Client Hello dengan SNI=unusultra.ac.id, mengkonfirmasi serangan diarahkan spesifik ke domain target. Kemunculan paket TCP FIN-ACK massal pada akhir sesi

p-ISSN : 2406-7733
e-ISSN : 2597-9922

menandakan Cloudflare melakukan pemutusan koneksi paksa sebagai mitigasi aktif.

Tabel 5. Rekapitulasi Temuan Forensik Digital (NIST)

No	Data	Status	Keterangan
1	IP Address Penyerang	Ditemukan	IP 10.0.2.15 teridentifikasi sebagai sumber serangan.
2	Jenis Serangan	Ditemukan	Serangan DDoS berbasis protokol ICMP (Ping Flood) pada Layer 7.
3	Paket Serangan	Ditemukan	Distribusi paket masif dengan dominasi rentang 640–1.279 byte.
4	Serangan Gagal	Ditemukan	Paket TCP [RST,ACK] dari Cloudflare menunjukkan sebagian serangan dimitigasi.
5	Kronologi Serangan	Direkonstruksi	Timeline reconstruction berbasis timestamp tersedia pada Tabel 6.

Berdasarkan keseluruhan investigasi, kedua tujuan penelitian telah berhasil dicapai. Penerapan *framework* NIST terbukti efektif dalam mengungkap dan merekonstruksi insiden DDoS secara sistematis. Sebagai langkah mitigasi, disarankan penggunaan layanan Imperva DDoS Protection yang dilengkapi kecerdasan buatan untuk pemantauan trafik secara *real-time* dan mitigasi otomatis dari *layer* 3 hingga *layer* 7.

V. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian, serangan DDoS berprotokol ICMP pada *web server* Universitas Nahdlatul Ulama Sulawesi Tenggara terbukti menyebabkan gangguan kinerja sistem hingga kegagalan layanan. Penerapan *framework* forensik digital berbasis NIST melalui tahapan *collection, examination, analysis*, dan *reporting* berhasil mengidentifikasi bukti digital berupa jejak serangan, alamat IP pelaku, jenis dan volume paket serangan, serta rekonstruksi kronologi (*timeline reconstruction*) berbasis *timestamp* sebagaimana disyaratkan oleh tahap *Reporting* NIST.

Kebaruan penelitian ini terletak pada penerapan kombinasi *dual-framework* ISSAF dan NIST serta *dual tools* forensik Wireshark dan NetworkMiner pada *web server* perguruan tinggi aktif yang terhubung ke internet dan menggunakan layanan Cloudflare. Pendekatan tersebut memungkinkan proses simulasi serangan dan investigasi forensik dilakukan secara terintegrasi, berbeda dengan penelitian terdahulu yang umumnya berfokus pada satu framework atau satu tools forensik dalam lingkungan server lokal.

Meskipun demikian, penelitian ini memiliki keterbatasan yaitu simulasi serangan hanya dilakukan pada satu jenis DDoS, satu objek web server, dan durasi pengujian yang terbatas, sehingga belum sepenuhnya merepresentasikan kompleksitas ancaman siber pada lingkungan yang lebih luas.

Saran

Penelitian selanjutnya disarankan untuk:

1. Menguji berbagai variasi serangan DDOS pada infrastruktur yang lebih kompleks
2. Membandingkan metode forensik digital lain sebagai pembanding NIST
3. Mengintegrasikan teknologi *Machine Learning* untuk meningkatkan kecepatan dan akurasi deteksi maupun investigasi
4. Memperkuat sistem keamanan *web server* institusi pendidikan melalui penerapan mitigasi ddos berbasis pemantauan trafik secara *real-time* guna meningkatkan ketahanan terhadap serangan siber.

DAFTAR PUSTAKA

Aldafian, A. N. A. S., Tahir, M., Firmansyah, M. E. N., & Khofifah, S. N. (2025). Implementasi IDS Wireshark untuk Deteksi Serangan DDoS SLOW HTTPS di Kali Linux. *Riset Teknik Informatika Dan Komputer*, *7*(2), 148–161. https://doi.org/https://doi.org/10.52005/restikom.v7i2.435

Alfidzar, H., & Zen, B. P. (2022). Implementasi HoneyPy Dengan Malicious Traffic Detection System (Maltrail) Guna Mendeteksi Serangan DOS Pada Server. *Journal of Informatics, Information System, Software Engineering and Applications*, *4*(2), 32–45. https://doi.org/https://doi.org/10.20895/inista.v4i2.534

Andriyan, S., Sidiq, M. F., & Zen, B. P. (2023). Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar Sulis. *Journal Informatic and Information Technology*, *2*(1), 1–13. https://doi.org/https://doi.org/10.20895/ledger.v2i1.996

Cloudflare. (2023). *DDoS Attack Trends for 2023 Q3*. Cloudflare Radar. https://radar.cloudflare.com/reports/ddos-2023-q3

Fitriana, M., AR, K., & Marsya, J. M. (2020). Penerapan Metode National Institute of Standards and Technology (NIST) dalam

p-ISSN : 2406-7733
e-ISSN : 2597-9922

Analisis Forensik Digital Untuk Penanganan Cyber Crime. *Jurnal Pendidikan Teknologi Informasi*, *4*(1), 29–39. https://doi.org/https://doi.org/10.22373/cj.v4i1.7241

Hanipah, R., & Dhika, H. (2020). Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark. *Journal of Computer and Information Technology*, *4*(1), 11–23.

Harahap, A. H., Andani, C. D., Christie, A., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *JMDP*, *1*(2), 73–83. https://doi.org/https://doi.org/10.38035/jmpd.v1i2.34

Madina, T. A., & Fadhli, M. (2024). Analisis Serangan DDOS pada Website Prodi Pendidikan Teknologi Informasi. *Jurnal Nasional Komputasi Dan Teknologi Informasi*, *7*(6), 1730–1736. https://doi.org/https://doi.org/10.32672/jnkti.v7i6.8273

Mahalini, I. A. M. P., Dewantara, I. B. K., Rakasiwi, N. P. D. R., Mahardika, N. M., Listartha, M. E., & Saskara, G. A. J. (2022). Analisis Kelayakan Tools Dengan Metode Penyerangan Distributed Denial of Service (DDOS). *Jurnal Teknologi Informasi*, *6*(2), 278–285.

Matondang, J., & Maulana, I. (2023). Analisis Perbandingan Perangkat Lunak Forensik Digital File Carving Menggunakan NIST. *Journal Of Social Science Research*, *3*(4), 2154–2165.

Pratama, N. A. S. P., & Servanda, Y. (2024). Analisis Serangan Forensik Terhadap Serangan DDoS Ping of Death Menggunakan Tools Nmap dan Hping3. *Jurnal Jurnal Sains Dan Teknologi (JSIT)*, *4*(2), 209–216. https://doi.org/https://doi.org/10.47233/jsit.v4i2.1842

Putra, I., Prayudi, Y., & Luthfi, A. (2023). Live Forensics untuk mengenali Karakteristik Serangan File Upload Guna Meningkatkan Keamanan pada Web Server. *Jurnal Ilmiah Ilmu Pendidikan*, *6*(6), 4387–4394. https://doi.org/https://doi.org/10.54371/jiip.v6i6.2173

Riadi, I., Umar, R., & Syahib, M. I. (2021). Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST). *Rekayasa Sistem Dan Teknologi Informasi*, *5*(1), 45–54. https://doi.org/https://doi.org/10.29207/resti.v5i1.2626

Ridho, M. A., & Arman, M. (2020). Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan. *Jurnal SISFOKOM (Sistem*, *9*(3), 373–379. https://doi.org/https://doi.org/10.32736/sisfokom.v9i3.945

Suharti, S., Yudhana, A., & Riadi, I. (2022). Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary Network Forensics DDoS Attack using ADDIE and HIDS Method on Proprietary Operating System. *Jurnal Manajemen, Teknik Informatika, Dan Rekayasa Komputer*, *21*(3), 567–582. https://doi.org/https://doi.org/10.30812/matrik.v21i3.1732

Syahib, M. I., Riadi, I., & Umar, R. (2023). Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST). *Jurnal Sains Komputer & Informatika*, *4*(1), 170–178.

Zebua, D. Y., Sayangi, C., Waruwu, C., Zebua, K., Zai, M., & Lase, A. (2025). Simulasi Serangan DOS Menggunakan Slowhttptest. *Jurnal Komputer Teknologi Informasi Sistem Komputer*, *4*(2), 409–419. https://doi.org/https://doi.org/10.62712/juktisi.v4i2.402