Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 599−608
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9034

Penerapan Digital Forensic Research Workshop Framework pada Layanan Virtual Machine

Asruddin Asruddin[1,2,*], Imam Riadi[3], Rusydi Umar[1]

[1]Program Studi Informatika, Universitas Ahmad Dahlan, Yogyakarta
Jl. Ringroad Selatan, Kragilan, Tamanan, Kec. Banguntapan, Kabupaten Bantul, Yogyakarta, Indonesia.
[2]Program Studi Sistem Komputer, Universitas Bung Karno, Jakarta
Jl. Kimia No.20 10, RT.10/RW.1, Pegangsaan, Kec. Menteng, Kota Jakarta Pusat, Jakarta, Indonesia
[3]Program Studi Sistem Informasi, Universitas Ahmad Dahlan,Yogyakarta
Jl. Ringroad Selatan, Kragilan, Tamanan, Kec. Banguntapan, Kabupaten Bantul, Yogyakarta, Indonesia.
Email: [1,*]2537083018@webmail.uad.ac.id , [2]imam.riadi@is.uad.ac.id, [3]rusydi@mti.uad.ac.id
Email Penulis Korespondensi: 2537083018@webmail.uad.ac.id
Submitted: **25/12/2025**; Accepted: **31/01/2026**; Published: **31/01/2026**

Abstrak−Serangan ICMP flooding merupakan serangan denial-of-service yang membanjiri target dengan paket ICMP berintensitas tinggi sehingga menurunkan ketersediaan layanan. Pelaporan investigasi forensik jaringan secara end-to-end dari identifikasi hingga presentasi bukti masih terbatas. Penelitian ini menerapkan kerangka Digital Forensic Research Workshop (DFRWS) yang mencakup Identification, Preservation, Collection, Examination, Analysis, dan Presentation untuk investigasi ICMP flooding pada lingkungan virtualisasi terkontrol. Artefak utama berupa PCAP baseline (5 run) dan PCAP serangan (5 run) dianalisis menggunakan capinfos untuk memperoleh durasi tangkapan (T), jumlah paket (N), laju paket rata-rata (pps), dan ukuran berkas. Hasil analisis menunjukkan trafik baseline (aktivitas normal sistem pada lab VM) konsisten pada 9 pps selama 58,91 s dengan ukuran berkas sekitar 66 kB, sedangkan trafik serangan menghasilkan 2.000 pps selama 6,39 s dengan ukuran berkas rata-rata sekitar 18,2 MB. Perbandingan kedua kondisi menghasilkan faktor peningkatan laju paket F = 2000/9 = 222× dan peningkatan ukuran berkas sekitar 280× (18,2 MB berbanding 66 kB). Lonjakan pps yang ekstrem pada kondisi serangan merepresentasikan karakter serangan volumetrik yang secara operasional berkorelasi dengan resource exhaustion dan penurunan availability layanan, sehingga artefak PCAP tidak hanya menunjukkan anomali statistik, tetapi juga mendukung pembuktian kejadian serangan denial-of-service. Seluruh run serangan menunjukkan pps > 1.000 (5/5; 100%) dan seluruh run baseline stabil pada 9 pps (5/5; 100%), sehingga artefak PCAP memenuhi karakter bukti volumetrik yang konsisten. Prosedur preservasi berupa pengaturan read-only dan verifikasi hash SHA-256 menjaga integritas dan keterlacakan penanganan artefak, sehingga mendukung admissibility sebagai bukti digital yang sah pada eksperimen virtual machine terkontrol.

Kata Kunci: ICMP Flooding; DFRWS; Forensik Jaringan; Virtualisasi; PCAP

Abstract−ICMP flooding is a denial-of-service attack that overwhelms a target with high-rate ICMP packets, degrading service availability. End-to-end network forensic reporting from identification to evidence presentation remains limited. This study applies the Digital Forensic Research Workshop (DFRWS) process model - Identification, Preservation, Collection, Examination, Analysis, and Presentation - to investigate ICMP flooding in a controlled virtualized environment. Primary artifacts consist of baseline PCAPs (5 runs) and attack PCAPs (5 runs) analyzed using capinfos to extract capture duration (T), packet count (N), average et rate (pps), and file size. Results indicate that the baseline traffic (normal system activity in the VM laboratory) at 9 pps over 58.91 s with approximately 66 kB file size, while attack traffic reaches 2,000 pps over 6.39 s with an average file size of approximately 18.2 MB. Comparison of both conditions yields a packet-rate amplification of F = 2000/9 = 222× and a file-size increase of approximately 280× (18.2 MB versus 66 kB). The extreme pps spike observed during the attack condition reflects a volumetric attack pattern that operationally correlates with resource exhaustion and reduced service availability, indicating that the PCAP artifacts support not only statistical anomaly detection but also event-level evidence of a denial-of-service incident. All attack runs exceed 1,000 pps (5/5; 100%), and all baseline runs remain stable at 9 pps (5/5; 100% [1]), indicating consistent volumetric evidence. Preservation procedures using read-only storage and SHA-256 hashing ensure artifact integrity and traceability, thereby supporting the admissibility of the PCAPs as valid digital evidence in controlled virtual machine experiments.

Keywords: ICMP Flooding; DFRWS; Network Forensics; Virtualization; PCAP

1. PENDAHULUAN

Serangan denial-of-service (DoS) dan distributed denial-of-service (DDoS) merupakan ancaman serius terhadap aspek ketersediaan (availability) layanan jaringan dan sistem informasi. Serangan ini bekerja dengan membanjiri target menggunakan trafik dalam jumlah besar sehingga sumber daya sistem tidak mampu melayani permintaan yang sah. Salah satu bentuk DoS yang masih banyak dijumpai dan relatif mudah direalisasikan adalah ICMP flooding atau ping flood, yaitu serangan volumetrik yang meningkatkan laju paket (packet rate) ICMP secara ekstrem menuju sistem target [1], [2]. ICMP flooding masih relevan sebagai objek penelitian meskipun tergolong serangan klasik, ICMP flooding masih relevan sebagai objek penelitian karena dampaknya mudah diamati dan sering digunakan baik dalam skenario nyata maupun eksperimen laboratorium.

Trafik jaringan yang direkam selama kejadian serangan umumnya disimpan dalam bentuk packet capture (PCAP) pada penanganan insiden keamanan. File PCAP berfungsi sebagai sumber data untuk analisis teknis dan deteksi serangan, serta memiliki potensi sebagai artefak bukti digital [3], [4], [5]. PCAP dapat diperlakukan sebagai bukti forensik jika jaminan integritas data, keterlacakan proses, serta dokumentasi akuisisi, penyimpanan, analisis,

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 599−608
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9034

dan penyajian data terpenuhi. Hasil analisis trafik berisiko menjadi observasi teknis yang sulit dipertanggungjawabkan secara forensik apabila pendekatan investigasi terstruktur tidak diterapkan.

Salah satu kerangka kerja yang banyak dijadikan acuan dalam forensik digital adalah Digital Forensic Research Workshop (DFRWS) process model. Model ini mendefinisikan enam tahapan utama investigasi forensik, yaitu Identification, Preservation, Collection, Examination, Analysis, dan Presentation. Kerangka DFRWS bertujuan memastikan bahwa bukti digital ditangani secara sistematis dari awal hingga akhir sehingga proses investigasi dapat direkonstruksi dan diaudit. Model ini banyak digunakan sebagai landasan konseptual dalam penelitian forensik digital meskipun bersifat umum dan tidak spesifik pada domain jaringan, model ini banyak digunakan sebagai landasan konseptual dalam penelitian forensik digital, termasuk forensik jaringan [6], [7].

Penelitian terkait menunjukkan bahwa sebagian besar studi mengenai serangan DoS masih berfokus pada aspek deteksi atau karakterisasi trafik. Berbagai penelitian menitikberatkan pada ekstraksi fitur statistik, analisis flow, atau penerapan metode machine learning untuk membedakan trafik normal dan trafik serangan. Pendekatan tersebut bermanfaat untuk tujuan deteksi, tetapi sering kali tidak mengaitkan hasil analisis secara eksplisit dengan tahapan investigasi forensik end-to-end. Selain itu, banyak studi menggunakan dataset publik atau dataset sintetis [8], [9] yang tidak selalu menyediakan konteks investigasi kasus tunggal yang terkontrol, seperti baseline terukur dan serangan terukur pada lingkungan yang sama [10], [11], [12], [13], [14].

Beberapa penelitian forensik jaringan telah mengintegrasikan analisis trafik dengan pendekatan forensik, termasuk pada konteks Internet of Things (IoT) dan jaringan terdistribusi [15], [16], [17], [18]. Akan tetapi, konteks lingkungan dan fokus penelitian tersebut berbeda dengan skenario ICMP flooding pada lingkungan virtualisasi berbasis virtual machine (VM). Lingkungan VM memberikan keunggulan berupa kontrol penuh terhadap topologi jaringan, peran sistem (attacker, victim, dan monitoring), serta kondisi eksperimen, sehingga lebih sesuai untuk penelitian forensik yang menekankan keterlacakan dan repeatability [19]. Meskipun virtualisasi dapat menimbulkan variasi akibat clock drift dan penggunaan sumber daya bersama (shared resources), lingkungan VM pada penelitian ini dipilih justru untuk mengisolasi dan mengendalikan variabel-variabel pengganggu tersebut melalui konfigurasi yang seragam, sehingga hasil tiap run tetap konsisten dan dapat diulang.

Meskipun penelitian sebelumnya telah membahas analisis forensik jaringan berbasis PCAP, terdapat kesenjangan yang jelas pada integrasi proses investigasi secara end-to-end. Penelitian oleh Riadi dkk [1] dan Sikos [2] menegaskan pentingnya analisis paket jaringan dalam forensik digital, namun tidak menyajikan eksperimen serangan ICMP flooding yang terukur dalam lingkungan terkontrol. Studi [3] dan [4] telah memanfaatkan PCAP untuk analisis forensik, termasuk dengan pendekatan statistik dan Social Network Analysis (SNA), tetapi belum memetakan tahapan investigasi secara sistematis berdasarkan kerangka Digital Forensic Research Workshop (DFRWS) dari Identification hingga Presentation.

Selain itu, penelitian forensik jaringan pada konteks IoT [2] berada pada lingkungan dan karakteristik ancaman yang berbeda, sehingga belum menjawab kebutuhan investigasi ICMP flooding dalam lingkungan virtual machine yang memungkinkan kontrol variabel dan pengujian berulang. Lebih lanjut, studi-studi tersebut belum secara eksplisit memperlakukan PCAP sebagai bukti digital yang diverifikasi integritasnya melalui mekanisme preservasi formal seperti pengaturan read-only dan hashing kriptografis.

Dengan demikian, terdapat gap penelitian berupa belum adanya implementasi investigasi ICMP flooding berbasis PCAP yang: (1) menerapkan kerangka DFRWS secara lengkap dan eksplisit, (2) membandingkan kondisi baseline dan serangan secara kuantitatif dalam lingkungan virtualisasi yang sama, serta (3) memverifikasi artefak sebagai bukti digital melalui prosedur preservasi yang terdokumentasi. Penelitian ini dirancang untuk mengisi gap tersebut.

Penelitian ini bertujuan untuk mengimplementasikan kerangka DFRWS pada investigasi forensik serangan ICMP flooding berbasis artefak PCAP di lingkungan virtualisasi. Eksperimen dilakukan menggunakan lab VM terkontrol yang terdiri dari VM attacker, VM victim, dan VM monitoring, dengan beberapa run baseline dan run serangan untuk memastikan keterulangan hasil. Diharapkan penelitian ini dapat memberikan kontribusi berupa contoh investigasi forensik ICMP flooding yang sistematis, terukur, dan dapat dipertanggungjawabkan, serta memperkuat posisi PCAP sebagai artefak bukti dalam forensik jaringan.

Penelitian ini berkontribusi dengan menyajikan implementasi investigasi forensik jaringan berbasis kerangka Digital Forensic Research Workshop (DFRWS) secara end-to-end pada kasus serangan ICMP flooding di lingkungan virtualisasi. Melalui eksperimen terkontrol dengan baseline dan serangan yang diulang, artefak packet capture (PCAP) diperlakukan sebagai bukti forensik yang terverifikasi melalui mekanisme pelestarian, hashing, serta analisis kuantitatif. Pendekatan ini menunjukkan bahwa PCAP tidak hanya berfungsi sebagai data teknis analisis trafik, tetapi dapat diposisikan sebagai bukti forensik yang dapat direkonstruksi dan direplikasi.

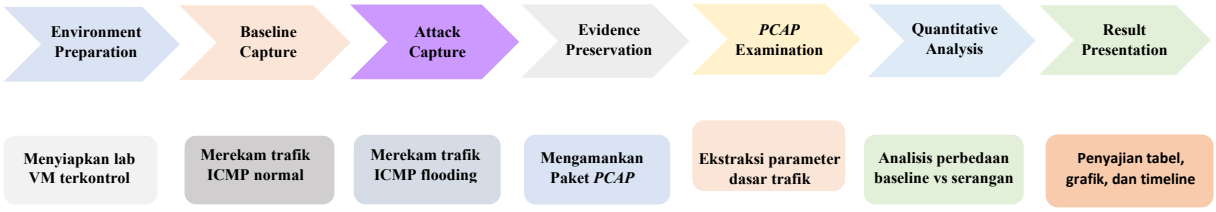
2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Tahapan penelitian merepresentasikan alur kerja eksperimental yang menggambarkan proses investigasi forensik jaringan secara operasional. Gambar 1 menampilkan ringkasan visual setiap aktivitas utama, sedangkan uraian berikut menjelaskan detail teknis dari masing-masing tahap. Alur kerja pada Gambar 1 merepresentasikan tahapan

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 599−608
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9034

eksperimen teknis yang selaras dengan prinsip investigasi forensik digital melalui pemetaan eksplisit terhadap fase Digital Forensic Research Workshop (DFRWS), yaitu Identification, Preservation, Collection, Examination, Analysis, dan Presentation. Pemetaan ini menjelaskan alur penelitian sebagai implementasi investigasi forensik jaringan secara end-to-end.



Gambar 1. Tahapan Penelitian

Tabel 2. Pemetaan Aktivitas Investigasi terhadap Fase DFRWS

Aktivitas Investigasi	Fase DFRWS
Identifikasi sumber bukti jaringan (NIC VM monitoring) dan penentuan ruang lingkup insiden	Identification
Akuisisi trafik normal	Collection
Akuisisi trafik serangan	Collection
Pengamanan artefak digital	Preservation
Pemeriksaan artefak PCAP	Examination
Analisis karakteristik trafik	Analysis
Pelaporan hasil investigasi	Presentation

Tahap pertama adalah Environment Preparation, yaitu persiapan lingkungan eksperimen dengan menyiapkan laboratorium virtualisasi yang terkontrol. Pada tahap ini ditetapkan peran sistem sebagai virtual machine (VM) attacker, VM victim, dan VM monitoring. Konfigurasi ini bertujuan memastikan bahwa seluruh proses pengambilan data dilakukan dalam lingkungan yang terisolasi, konsisten, dan dapat direproduksi.

Tahap berikutnya adalah Baseline Capture, yaitu proses perekaman trafik jaringan ICMP dalam kondisi normal tanpa adanya aktivitas serangan. Perekaman dilakukan menggunakan tcpdump pada VM monitoring untuk memperoleh karakteristik trafik dasar. Data baseline ini berfungsi sebagai representasi kondisi normal dan menjadi acuan pembanding utama dalam analisis selanjutnya. Proses perekaman diulang dalam beberapa run untuk menjamin keterulangan (repeatability) hasil.

Tahap Attack Capture dilakukan melalui perekaman trafik jaringan pada saat serangan ICMP flooding dijalankan secara terkontrol. Serangan dihasilkan menggunakan parameter yang konsisten pada setiap run sehingga karakteristik trafik yang dihasilkan dapat dibandingkan secara langsung dengan data baseline. Seluruh trafik serangan direkam dalam bentuk file PCAP menggunakan mekanisme yang sama dengan tahap baseline capture.

Tahap selanjutnya adalah Evidence Preservation, di mana seluruh file PCAP hasil perekaman diamankan sebagai artefak bukti digital [13]. Pada tahap ini, file PCAP disimpan dalam kondisi read-only dan diverifikasi menggunakan nilai hash SHA-256. Langkah ini bertujuan menjaga integritas dan keaslian artefak agar tidak mengalami perubahan selama proses pemeriksaan dan analisis berlangsung.

Tahap PCAP Examination dilakukan dengan mengekstraksi parameter dasar trafik dari setiap file PCAP. Parameter yang diperoleh meliputi durasi perekaman, jumlah paket ICMP, laju paket rata-rata (packets per second), serta ukuran file. Pemeriksaan awal ini bersifat deskriptif dan bertujuan menghasilkan data kuantitatif dasar yang menjadi input bagi tahap analisis lanjutan.

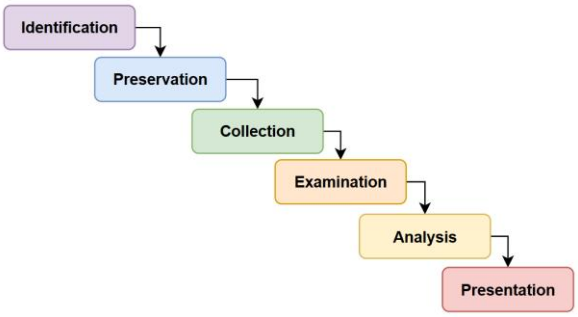
Tahap Quantitative Analysis difokuskan pada analisis perbedaan karakteristik trafik antara kondisi baseline dan kondisi serangan. Analisis dilakukan dengan membandingkan nilai laju paket ICMP dan parameter terkait secara per-run, kemudian diringkas dalam bentuk nilai rata-rata. Pendekatan ini digunakan untuk memperkuat konsistensi temuan dan mengurangi potensi bias pengukuran.

Tahap terakhir adalah Result Presentation, yaitu penyajian hasil investigasi dalam bentuk tabel dan grafik, serta rekonstruksi timeline forensik sederhana yang menggambarkan transisi trafik dari kondisi normal menuju kondisi serangan. Penyajian hasil ini bertujuan mendukung pelaporan forensik yang sistematis, transparan, dan mudah dipahami.

2.2 Penerapan Kerangka DFRWS

Kerangka Digital Forensic Research Workshop (DFRWS) digunakan dalam penelitian ini sebagai landasan metodologis forensik untuk memastikan bahwa proses investigasi artefak jaringan dilakukan secara sistematis, terstruktur, dan dapat ditelusuri. DFRWS menyediakan kerangka konseptual yang mengaitkan aktivitas investigasi teknis dengan prinsip-prinsip forensik digital, mulai dari identifikasi hingga penyajian bukti [6], [7] [20].

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 599−608
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9034



Gambar 2. Tahapan Framework DFRWS

Gambar 2 menampilkan tahapan proses dalam kerangka DFRWS yang digunakan sebagai acuan konseptual dalam penelitian ini. Kerangka ini berfungsi untuk menafsirkan dan menstrukturkan proses investigasi forensik jaringan secara menyeluruh, sehingga setiap aktivitas investigasi memiliki posisi yang jelas dalam alur forensik digital.

Dalam konteks penelitian ini, kerangka DFRWS digunakan sebagai acuan untuk mengklasifikasikan dan menafsirkan aktivitas investigasi forensik jaringan yang telah dijelaskan pada tahapan penelitian sebelumnya. Ringkasan pemetaan antara aktivitas investigasi dan fase DFRWS disajikan pada Tabel 2.

2.3 Metode Analisis Kuantitatif

Analisis kuantitatif difokuskan pada pengukuran laju paket ICMP sebagai indikator utama serangan ICMP flooding. Laju paket dihitung menggunakan persamaan:

$$pps = \frac{N}{T} \quad (1)$$

Laju paket rata-rata atau packets per second (pps) merepresentasikan jumlah paket ICMP yang terekam per satuan waktu dalam proses perekaman trafik jaringan. Nilai pps dihitung berdasarkan jumlah paket ICMP yang berhasil direkam (N) selama periode perekaman tertentu, kemudian dibagi dengan durasi proses capture (T) yang diukur dalam satuan detik. Dengan demikian, N menyatakan total paket ICMP yang tercatat dalam file PCAP, sedangkan T menunjukkan lamanya waktu perekaman berlangsung. Kombinasi kedua parameter tersebut menghasilkan nilai pps sebagai indikator kuantitatif intensitas trafik jaringan.

Mengukur tingkat peningkatan trafik akibat serangan dibandingkan dengan kondisi normal (baseline), digunakan faktor peningkatan sebagai berikut:

$$F = \frac{pps_{attack}}{pps_{baseline}} \quad (2)$$

Hasil perhitungan laju paket dan faktor peningkatan digunakan untuk membandingkan karakteristik trafik antara kondisi normal dan kondisi serangan serta mendukung pembuktian forensik jaringan berbasis data kuantitatif.

F merupakan faktor peningkatan yang menyatakan perbandingan intensitas trafik antara kondisi serangan dan kondisi normal dalam satuan kali. Nilai F diperoleh dengan membandingkan laju paket rata-rata pada kondisi serangan (pps_{attack}) terhadap laju paket rata-rata pada kondisi baseline ($pps_{baseline}$)). Parameter pps_{attack} merepresentasikan jumlah paket ICMP per detik saat serangan berlangsung, sedangkan $pps_{baseline}$ menunjukkan laju paket per detik dalam kondisi normal. Perbandingan kedua nilai tersebut menghasilkan besaran peningkatan trafik yang secara kuantitatif menggambarkan dampak serangan terhadap sistem.

Hasil perhitungan laju paket dan faktor peningkatan digunakan untuk membandingkan karakteristik trafik antara kondisi normal dan kondisi serangan serta mendukung pembuktian forensik jaringan berbasis data kuantitatif.

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil dan pembahasan investigasi forensik jaringan terhadap serangan ICMP flooding berbasis artefak packet capture (PCAP). Penyajian hasil disusun mengikuti urutan fase Digital Forensic Research Workshop (DFRWS) untuk memastikan bahwa setiap temuan dapat ditelusuri secara metodologis, mulai dari identifikasi artefak hingga penyajian bukti forensik.

3.1 Tahapan Identification

Tahap Identification bertujuan mengidentifikasi karakteristik awal trafik jaringan yang direkam sebagai artefak forensik. Pada tahap ini, artefak PCAP diidentifikasi berdasarkan dua kondisi, yaitu kondisi normal (baseline) dan kondisi serangan ICMP flooding. Setiap kondisi direkam sebanyak lima kali (run) untuk menjamin keterulangan hasil.

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 599–608
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9034

3.2 Tahapan Preservation

Tahap Preservation difokuskan pada pengamanan artefak digital guna memastikan integritas dan keaslian data tetap terjaga selama proses investigasi forensik. Seluruh berkas PCAP hasil perekaman trafik jaringan disimpan dalam kondisi read-only sebagai mekanisme perlindungan awal terhadap perubahan yang tidak sah. Selain itu, integritas data diverifikasi melalui perhitungan nilai hash menggunakan algoritma SHA-256.

```
root@debian:/home/rudi/icmpmonitoring# ls -l icmp_lab_output/evidence/*.pcap
-r--r--r-- 1 root root 24226152 Dec 19 11:43 icmp_lab_output/evidence/EVD_001_attack_run01.pcap
-r--r--r-- 1 root root 21157062 Dec 19 11:44 icmp_lab_output/evidence/EVD_002_attack_run02.pcap
-r--r--r-- 1 root root 12802722 Dec 19 11:45 icmp_lab_output/evidence/EVD_003_attack_run03.pcap
-r--r--r-- 1 root root 21219756 Dec 19 11:45 icmp_lab_output/evidence/EVD_004_attack_run04.pcap
-r--r--r-- 1 root root 13639614 Dec 19 11:46 icmp_lab_output/evidence/EVD_005_attack_run05.pcap
-r--r--r-- 1 root root    67056 Dec 19 11:38 icmp_lab_output/evidence/EVD_006_baseline_run01.pcap
-r--r--r-- 1 root root    67284 Dec 19 11:40 icmp_lab_output/evidence/EVD_007_baseline_run02.pcap
-r--r--r-- 1 root root    67056 Dec 19 11:41 icmp_lab_output/evidence/EVD_008_baseline_run03.pcap
-r--r--r-- 1 root root    66600 Dec 19 11:42 icmp_lab_output/evidence/EVD_009_baseline_run04.pcap
-r--r--r-- 1 root root    64092 Dec 19 11:43 icmp_lab_output/evidence/EVD_010_baseline_run05.pcap
root@debian:/home/rudi/icmpmonitoring#
```

Gambar 3. File PCAP kondisi read-only

Gambar 3 menunjukkan berkas PCAP yang disimpan dalam kondisi read-only. Kondisi ini berfungsi sebagai bukti bahwa artefak digital telah diamankan secara operasional sehingga tidak dapat dimodifikasi selama proses penyimpanan dan analisis.

```
root@debian:/home/rudi/icmpmonitoring# sha256sum icmp_lab_output/evidence/*.pcap
f2847999674c7616891bd7585134a53d85e38085645123b07acbbe8211df7ae0  icmp_lab_output/evidence/EVD_001_attack_run01.pcap
c4dd7fb41bc08828541fb371c13435e8f33a09e77aa1c9d593c4357c58a8a894  icmp_lab_output/evidence/EVD_002_attack_run02.pcap
4815c99240e7dae63f7744e6b9ea13550bb35a7a6e61aa5387907f913b848f1b  icmp_lab_output/evidence/EVD_003_attack_run03.pcap
f46af129b5b403efca2c07e01bc3a3838d99da2d1b15ee3bd8bf553ec1c6c1ea  icmp_lab_output/evidence/EVD_004_attack_run04.pcap
571f058a389f2bac2c822857a6d5b05b44fcfadeb8cc9d0a3c965224b67f8d1c  icmp_lab_output/evidence/EVD_005_attack_run05.pcap
1cd18933f9d24f162386e6c3b4ff94b6c231b3e7f11f984ffcf99736e7eff030  icmp_lab_output/evidence/EVD_006_baseline_run01.pcap
9b008cd0d278109505aeeb41df1ace4d2cb1b936ee5b2d84b685fec056888242  icmp_lab_output/evidence/EVD_007_baseline_run02.pcap
df0ef3d8393fed23d7ae33122e9a94dfa0c4832761ed951a0f02489378aaa1f1  icmp_lab_output/evidence/EVD_008_baseline_run03.pcap
3630eab981c6b27d77ef323724f96e20317590a63946c18b3a7a18dd4de9f2d6  icmp_lab_output/evidence/EVD_009_baseline_run04.pcap
3323d1609be32146e7b413c95962c2cd523ac1fea15cc9fccec62e93c6b28df2  icmp_lab_output/evidence/EVD_010_baseline_run05.pcap
root@debian:/home/rudi/icmpmonitoring#
```

Gambar 4. File PCAP menggunakan nilai hash SHA-256

Gambar 4 memperlihatkan hasil verifikasi integritas berkas PCAP menggunakan nilai hash SHA-256. Verifikasi ini berfungsi sebagai bukti kriptografis bahwa artefak PCAP tetap identik sejak tahap akuisisi hingga tahap analisis, sehingga setiap perubahan terhadap data dapat terdeteksi.

Langkah preservasi yang ditunjukkan pada Gambar 3 dan Gambar 4 berfungsi sebagai bukti (proof of integrity) bahwa artefak PCAP tidak mengalami perubahan sejak tahap identifikasi hingga tahap analisis. Dengan demikian, Artefak memenuhi prinsip chain of custody dan praktik akuisisi bukti digital [25], termasuk pendekatan berbasis standar NIST dan analisis forensik komunikasi digital [21], [22], [23].

3.3 Tahapan Collection

Tahap Collection dilakukan dengan mengelompokkan dan mengorganisasi artefak PCAP berdasarkan kondisi trafik, yaitu baseline dan serangan ICMP flooding. Pengelompokan ini dilakukan secara konsisten pada setiap run untuk memastikan keterbandingan antar artefak. Proses koleksi ini bertujuan memudahkan pemeriksaan dan analisis lanjutan, serta memastikan bahwa seluruh artefak yang relevan telah terhimpun secara sistematis.

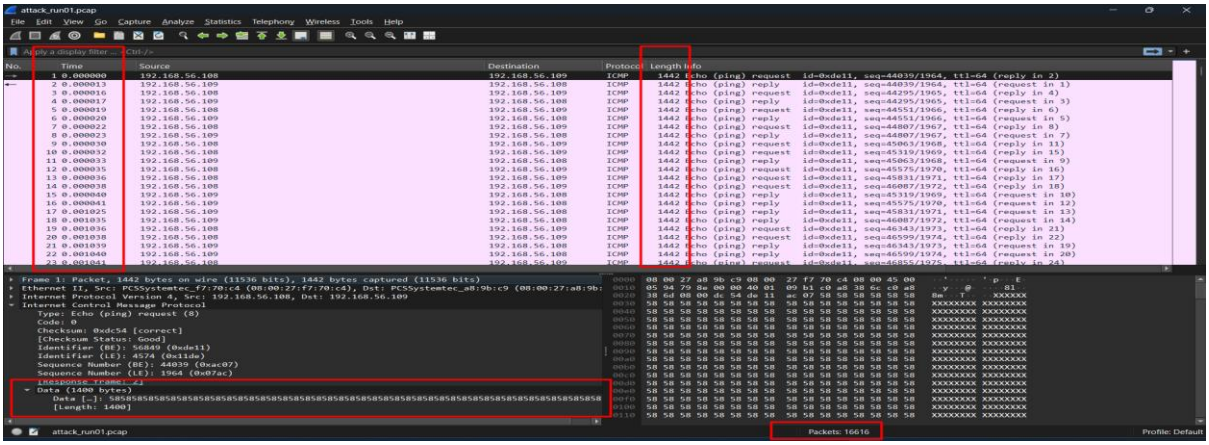
3.4 Tahapan Examination

Tahap Examination bertujuan melakukan pemeriksaan teknis terhadap artefak PCAP untuk memperoleh parameter dasar trafik serta karakteristik paket ICMP yang terekam. Pemeriksaan ini bersifat deskriptif dan menjadi dasar untuk analisis kuantitatif pada tahap berikutnya, Parameter yang diekstraksi pada tahap Examination meliputi:
a. durasi perekaman (capture duration, T),
b. jumlah paket ICMP (number of packets, N),
c. laju paket rata-rata (average packet rate, pps), dan
d. Ukuran file PCAP.

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 599−608
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9034

3.4.1 Pemeriksaan Struktur Paket ICMP (Wireshark)

Pemeriksaan paket dilakukan menggunakan Wireshark untuk mengidentifikasi karakteristik teknis paket ICMP. Gambar 5 menampilkan contoh paket ICMP pada kondisi serangan (attack_run01.pcap), yang menunjukkan ukuran paket besar (±1442 bytes) dengan payload maksimal (±1400 bytes) dan interval pengiriman sangat rapat. Karakteristik ini mengindikasikan trafik berintensitas tinggi yang berbeda dari perilaku ICMP echo request normal.



Gambar 5. Paket ICMP pada kondisi serangan ICMP flooding (attack_run01.pcap)

Paket ICMP pada kondisi baseline memiliki ukuran lebih kecil, payload minimal, dan interval pengiriman yang lebih longgar. Ringkasan pembeda teknis antara baseline dan serangan disajikan pada Tabel 3.

Tabel 3. Pembeda Karakteristik Paket ICMP (hasil Wireshark)

Aspek Pembeda	Baseline	ICMP Flooding
Ukuran paket	98 bytes	1442 bytes
Payload	minimal	maksimal (1400 B)
Interval waktu	ratusan ms	mikrodetik
Packet rate	±9 pps	>1.000 pps
Tujuan trafik	connectivity check	resource exhaustion
Pola	periodik	flooding

Temuan pada pemeriksaan paket ini menegaskan adanya perbedaan perilaku ICMP pada tingkat paket (packet-level), sebelum dilakukan pembuktian kuantitatif pada tahap Analysis.

3.4.2 Ekstraksi Parameter Dasar Trafik

Hasil ekstraksi parameter dasar untuk seluruh artefak PCAP (5 baseline dan 5 serangan) ditunjukkan pada Tabel 4.

Tabel 4. Hasil Pemeriksaan Parameter Dasar Trafik dari Artefak PCAP

Run	Kondisi	Durasi (detik)	Jumlah Paket	Avg Packet Rate (pps)	Ukuran File
1	ICMP Flooding	8,196	16.613	2.027	24 MB
2	ICMP Flooding	7,378	14.505	1.966	21 MB
3	ICMP Flooding	5,876	8.781	1.494	12 MB
4	ICMP Flooding	5,505	14.550	2.643	21 MB
5	ICMP Flooding	4,995	9.355	1.872	13 MB
1	Baseline	59,156	588	9	67 kB
2	Baseline	59,243	590	9	67 kB
3	Baseline	59,024	588	9	67 kB
4	Baseline	58,588	584	9	66 kB
5	Baseline	58,518	562	9	64 kB

Nilai pps pada tabel mengikuti output capinfos, sedangkan nilai N pada run serangan diselaraskan terhadap pps dan durasi (T) untuk menghindari inkonsistensi pelaporan.

Tabel 4 menunjukkan bahwa trafik baseline memiliki pola stabil dengan laju paket rendah dan durasi perekaman yang relatif konstan. Trafik serangan ICMP flooding menunjukkan lonjakan jumlah paket dan laju paket yang signifikan meskipun durasi perekaman lebih singkat. Variasi laju paket pada kondisi serangan (1.494-2.643 pps), khususnya nilai tertinggi pada run ke-4, mengindikasikan adanya fluktuasi performa yang dipengaruhi oleh dinamika alokasi sumber daya virtualisasi dan penjadwalan hypervisor, meskipun seluruh run tetap menunjukkan karakter serangan volumetrik yang juga diamati pada penelitian IDS/IPS dan mitigasi ICMP flooding [24], [25], [26]. Perbedaan ini menjadi indikator awal terjadinya anomali trafik jaringan.

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 599−608
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9034

3.5 Tahapan Analysis

Tahap Analysis difokuskan pada pembuktian kuantitatif deskriptif terhadap perbedaan karakteristik trafik antara kondisi baseline dan kondisi serangan ICMP flooding.

3.5.1 Rekapitulasi Rata-Rata

Rekapitulasi rata-rata lima kali percobaan ditunjukkan pada Tabel 5.

Tabel 5. Rata-Rata Baseline vs ICMP Flooding

Kondisi	Durasi Rata-rata (s)	Paket Rata-rata	PPS Rata-rata	Ukuran File Rata-rata
Baseline	58,91	582	9	66 kB
ICMP Flooding	6,39	12.761	2.000	18,2 MB

Rekapitulasi ini menunjukkan adanya perbedaan yang sangat signifikan antara kedua kondisi.

3.5.2 Perhitungan Laju Paket

Laju paket dihitung menggunakan Persamaan (1):

$$pps = \frac{N}{T} \quad (1)$$

Laju paket rata-rata atau packets per second (pps) merepresentasikan jumlah paket ICMP yang terekam per satuan waktu dalam proses perekaman trafik jaringan. Nilai pps dihitung berdasarkan jumlah paket ICMP yang berhasil direkam (N) selama periode perekaman tertentu, kemudian dibagi dengan durasi proses capture (T) yang diukur dalam satuan detik. Dengan demikian, N menyatakan total paket ICMP yang tercatat dalam file PCAP, sedangkan T menunjukkan lamanya waktu perekaman berlangsung. Kombinasi kedua parameter tersebut menghasilkan nilai pps sebagai indikator kuantitatif intensitas trafik jaringan.
Sebagai contoh, pada run pertama serangan ICMP flooding diperoleh:

$$pps = \frac{16.613}{8,196} = 2.027 \text{ pps}$$

Perbedaan kecil dengan nilai yang ditampilkan oleh capinfos dipahami sebagai efek pembulatan dan metode perhitungan durasi rata-rata oleh perangkat lunak.

3.5.3 Faktor Peningkatan Serangan

Faktor peningkatan laju paket dihitung menggunakan Persamaan (2).

$$F = \frac{pps_{attack}}{pps_{baseline}} \quad (2)$$

F merupakan faktor peningkatan yang menyatakan perbandingan intensitas trafik antara kondisi serangan dan kondisi normal dalam satuan kali. Nilai F diperoleh dengan membandingkan laju paket rata-rata pada kondisi serangan (pps_{attack}) terhadap laju paket rata-rata pada kondisi baseline ($pps_{baseline}$). Parameter pps_{attack} merepresentasikan jumlah paket ICMP per detik saat serangan berlangsung, sedangkan $pps_{baseline}$ menunjukkan laju paket per detik dalam kondisi normal. Perbandingan kedua nilai tersebut menghasilkan besaran peningkatan trafik yang secara kuantitatif menggambarkan dampak serangan terhadap sistem. Berdasarkan nilai rata-rata pada Tabel 5, diperoleh $pps_{attack} = 2000$pps dan $pps_{baseline} = 9$pps, sehingga:

$$F = \frac{2000}{9} = 222.22 \approx 222 \times$$

Nilai tersebut menunjukkan bahwa serangan ICMP flooding meningkatkan intensitas trafik sekitar 222 kali dibandingkan kondisi normal.

3.5.4 Korelasi Ukuran File PCAP

Ukuran file PCAP berfungsi sebagai indikator pendukung selain laju paket. Artefak serangan menghasilkan ukuran file rata-rata 18,2 MB, sedangkan baseline hanya sekitar 66 kB. Korelasi ini memperkuat karakter serangan flooding sebagai serangan volumetrik yang menghasilkan lonjakan trafik dalam waktu singkat.

3.6 Tahapan Presentation

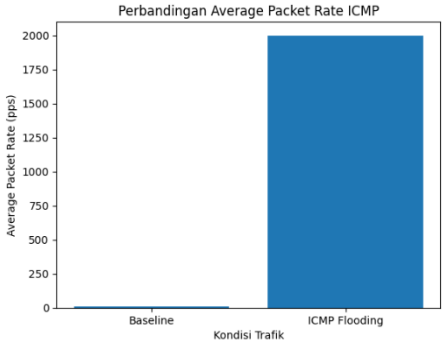
Tahap Presentation bertujuan menyajikan bukti forensik jaringan dalam bentuk visual yang mudah dipahami, sehingga perbedaan antara kondisi normal dan kondisi serangan dapat diamati secara langsung oleh pembaca.

3.6.1 Grafik Perbandingan

Gambar 6 menunjukkan kontras yang jelas antara kondisi baseline dan kondisi serangan. Nilai average packet rate pada baseline berada pada kisaran rendah dan stabil (~9 pps), sedangkan pada kondisi ICMP flooding meningkat

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 599−608
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9034

drastis (~2000 pps). Visualisasi ini memperkuat bukti bahwa trafik serangan bersifat volumetrik dan berbeda signifikan dari kondisi normal.



Gambar 6. Perbandingan Baseline dan ICMP Flooding

3.6.2 Rekonstruksi Timeline Serangan

Rekonstruksi timeline menempatkan artefak PCAP sebagai bukti kejadian serangan yang dapat ditelusuri secara kronologis. Artefak baseline dan artefak serangan membentuk tiga fase kejadian yang dibedakan menggunakan indikator kuantitatif (pps, jumlah paket, durasi) dan indikator pendukung (ukuran berkas), serta mekanisme preservasi (read-only dan hash SHA-256).

Fase 1 - Kondisi awal (baseline evidence).

Artefak baseline (baseline_run01-baseline_run05) menunjukkan kondisi awal sistem sebelum gangguan. File baseline memiliki durasi tangkapan konsisten 58,518-59,243 detik, jumlah paket 562-590 paket, laju paket stabil 9 pps, dan ukuran berkas kecil 64-67 kB. Konsistensi pada seluruh run baseline (5/5) menunjukkan kondisi awal berada pada keadaan normal dan layak menjadi pembanding forensik.

Fase 2 - Kejadian serangan (attack evidence window).

Artefak serangan (attack_run01–attack_run05) menunjukkan perubahan trafik yang bersifat tiba-tiba dan ekstrem. Durasi tangkapan berada pada rentang 4,995-8,196 detik dengan laju paket meningkat pada seluruh run menjadi 1.494-2.643 pps. Jumlah paket serangan berada pada rentang 8.781-16.613 paket per run dan ukuran berkas meningkat menjadi 12-24 MB. Kombinasi pps tinggi, jumlah paket besar, durasi singkat, dan lonjakan ukuran berkas menunjukkan karakter serangan volumetrik ICMP flooding.

Fase 3 - Terminasi kejadian (post-attack boundary).

Batas akhir kejadian ditunjukkan oleh berakhirnya window tangkapan pada artefak serangan dan tidak adanya artefak lain pada dataset yang mempertahankan pps tinggi setelahnya. Pemisahan yang tegas antara baseline dan serangan menunjukkan kejadian bersifat event-based dan memiliki rentang waktu yang dapat direkonstruksi.

Timeline ini menghubungkan artefak (PCAP baseline/serangan) dengan indikator kuantitatif (pps, N, T) serta indikator pendukung (ukuran berkas) sehingga urutan kejadian dapat diaudit. Penyajian kronologis ini memperkuat fase Presentation pada DFRWS karena memudahkan penelusuran bukti dari kondisi awal, kejadian serangan, hingga terminasi kejadian.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa artefak packet capture (PCAP) tidak hanya berfungsi sebagai data teknis analisis trafik, tetapi dapat dikonversi secara sistematis menjadi bukti forensik jaringan yang memenuhi prinsip Chain of Custody melalui penerapan kerangka Digital Forensic Research Workshop (DFRWS). Penerapan kerangka Digital Forensic Research Workshop (DFRWS) memungkinkan proses investigasi ditelusuri secara sistematis dari tahap identifikasi hingga penyajian bukti. Hasil pemeriksaan kuantitatif menunjukkan trafik baseline yang konsisten pada laju paket 9 pps dengan durasi rata-rata 58,91 detik dan ukuran berkas sekitar 66 kB. Trafik serangan ICMP flooding menghasilkan laju paket rata-rata 2.000 pps dengan durasi 6,39 detik dan ukuran berkas sekitar 18,2 MB. Perbandingan kedua kondisi menghasilkan faktor peningkatan laju paket sebesar F = 222× (2000/9) dan peningkatan ukuran berkas sekitar 280×, yang menunjukkan karakter serangan volumetrik. Identifikasi serangan menunjukkan konsistensi pada seluruh run serangan dengan laju paket di atas 1.000 pps (5/5; 100%), sedangkan seluruh run baseline menunjukkan trafik stabil pada 9 pps (5/5; 100%). Mekanisme preservasi menggunakan pengaturan read-only dan verifikasi hash SHA-256 menjaga integritas artefak sehingga bukti dapat direkonstruksi dan direplikasi pada eksperimen virtual machine terkontrol. Secara ilmiah, penelitian ini memberikan kontribusi pada dua aspek utama. Pertama, kontribusi metodologis berupa penerapan kerangka Digital Forensic Research Workshop (DFRWS) secara eksplisit dan terintegrasi pada investigasi forensik jaringan berbasis PCAP dalam skenario ICMP flooding, sehingga memperjelas pemetaan tahapan Identification hingga Presentation dalam konteks forensik jaringan. Kedua, kontribusi empiris berupa penyajian desain eksperimen

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 599–608
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9034

multi-run dengan pembandingan kuantitatif antara kondisi baseline dan serangan dalam lingkungan virtualisasi yang sama, yang mendukung aspek repeatability, rekonstruktabilitas, serta penguatan posisi PCAP sebagai artefak bukti digital yang terverifikasi. Keterbatasan penelitian terletak pada cakupan jenis serangan yang dibatasi pada ICMP flooding dan penggunaan parameter kuantitatif dasar. Penelitian selanjutnya dapat memperluas topologi jaringan, menguji variasi DoS/DDoS, dan menambahkan analisis berbasis fitur atau flow untuk memperkuat pembuktian forensik jaringan. Analisis lanjutan juga dapat dikembangkan menggunakan pendekatan Graph Neural Network [27] serta diperluas pada arsitektur jaringan ICN atau satelit dengan karakteristik distribusi trafik yang berbeda [28].

REFERENCES

[1] I. Riadi, S. Sunardi, and F. T. Fitri, "Spamming Forensic Analysis Using Network Forensics Development Life Cycle Method," INTENSIF J. Ilm. Penelit. Dan Penerapan Teknol. Sist. Inf., vol. 6, no. 1, pp. 108–117, Feb. 2022, doi: 10.29407/intensif.v6i1.16830.
[2] L. F. Sikos, "Packet Analysis for Network Forensics: A Comprehensive Survey," Forensic Sci. Int. Digit. Investig., vol. 32, p. 200892, Mar. 2020, doi: 10.1016/j.fsidi.2019.200892.
[3] S. Q. Ali Shah, F. Zeeshan Khan, and M. Ahmad, "The Impact and Mitigation of ICMP Based Economic Denial of Sustainability Attack in Cloud Computing Environment Using Software Defined Network," Comput. Netw., vol. 187, p. 107825, Mar. 2021, doi: 10.1016/j.comnet.2021.107825.
[4] W. Yunus and M. E. Lasulika, "Security System Analysis Against Flood Attacks Using TCP, UDP, and ICMP Protocols on Mikrotik Routers," Int. J. Adv. Data Inf. Syst., vol. 3, no. 1, pp. 11–19, Apr. 2022, doi: 10.25008/ijadis.v3i1.1231.
[5] M. Cermak, T. Fritzová, V. Rusňák, and D. Sramkova, "Using Relational Graphs for Exploratory Analysis of Network Traffic Data," Forensic Sci. Int. Digit. Investig., vol. 45, p. 301563, Jul. 2023, doi: 10.1016/j.fsidi.2023.301563.
[6] P. Rajesh, M. Ismail. Ismail. B., M. Alam, M. Tahernezhadi, and M. A., "Network Forensics Investigation in Virtual Data Centers Using ELK," in 2021 International Symposium on Electrical, Electronics and Information Engineering, Seoul Republic of Korea: ACM, Feb. 2021, pp. 175–179. doi: 10.1145/3459104.3459135.
[7] A. Yudhana, Imam Riadi, and Budi Putra, "Digital Forensic on Secure Digital High Capacity using DFRWS Method," J. RESTI Rekayasa Sist. Dan Teknol. Inf., vol. 6, no. 6, pp. 1021–1027, Dec. 2022, doi: 10.29207/resti.v6i6.4615.
[8] M. Komisarek, M. Pawlicki, T. Simic, D. Kavcnik, R. Kozik, and M. Choraś, "Modern NetFlow Network Dataset with Labeled Attacks and Detection Methods," in Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento Italy: ACM, Aug. 2023, pp. 1–8. doi: 10.1145/3600160.3605094.
[9] G. Aceto et al., "Synthetic and Privacy-preserving Traffic Trace Generation Using Generative AI Models for Training Network Intrusion Detection Systems," J. Netw. Comput. Appl., vol. 229, p. 103926, Sep. 2024, doi: 10.1016/j.jnca.2024.103926.
[10] I. S. Alansari, "A Detection and Investigation Model for the Capture and Analysis of Network Crimes," Eng. Technol. Appl. Sci. Res., vol. 13, no. 5, pp. 11871–11877, Oct. 2023, doi: 10.48084/etasr.6316.
[11] S. Aktar and A. Yasin Nur, "Towards DDoS Attack Detection Using Deep Learning Approach," Comput. Secur., vol. 129, p. 103251, Jun. 2023, doi: 10.1016/j.cose.2023.103251.
[12] A. A. Alashhab et al., "Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model," IEEE Access, vol. 12, pp. 51630–51649, 2024, doi: 10.1109/ACCESS.2024.3384398.
[13] S. Ratan Kumar and V. K. Vatsavayi, "Performance Analysis of Machine Learning Techniques for Server Health Monitoring Using Time Series Data Against DDOS Attacks," IEEE Access, vol. 13, pp. 53321–53346, 2025, doi: 10.1109/ACCESS.2025.3553558.
[14] A. Abualhassan, I. Rashid, F. Binbeshr, and M. Imam, "DDoS Attack Detection in IoT: A Comparative Resource and Performance Analysis of Deep Learning and Machine Learning Models," IEEE Access, vol. 13, pp. 116529–116547, 2025, doi: 10.1109/ACCESS.2025.3583855.
[15] D. Spiekermann and J. Keller, "Challenges of Network Forensic Investigation in Fog and Edge Computing," Future Internet, vol. 15, no. 10, p. 342, Oct. 2023, doi: 10.3390/fi15100342.
[16] H. Alazzam, O. AbuAlghanam, Q. M. Al-zoubi, A. Alsmady, and E. Alhenawi, "A New Network Digital Forensics Approach for Internet of Things Environment Based on Binary Owl Optimizer," Cybern. Inf. Technol., vol. 22, no. 3, pp. 146–160, Sep. 2022, doi: 10.2478/cait-2022-0033.
[17] Y. Salem and M. M. N. Hamarsheh, "Forensically Analyzing IoT Smart Camera Using MAoIDFF-IoT Framework," Forensic Sci. Int. Digit. Investig., vol. 51, p. 301829, Dec. 2024, doi: 10.1016/j.fsidi.2024.301829.
[18] T. Wu, F. Breitinger, and S. Niemann, "IoT Network Traffic Analysis: Opportunities and Challenges for Forensic Investigators?," Forensic Sci. Int. Digit. Investig., vol. 38, p. 301123, Oct. 2021, doi: 10.1016/j.fsidi.2021.301123.
[19] S. Batool, M. Aslam, E. Akpokodje, and S. F. Jilani, "A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments: Machine Learning, Deep Learning, and Federated Learning Perspectives," Electronics, vol. 14, no. 21, p. 4222, Oct. 2025, doi: 10.3390/electronics14214222.
[20] S. Sunardi, I. Riadi, R. Umar, and M. F. Gustafi, "Audio Forensics on Smartphone with Digital Forensics Research Workshop (DFRWS) Method," CommIT Commun. Inf. Technol. J., vol. 15, no. 1, pp. 41–47, Mar. 2021, doi: 10.21512/commit.v15i1.6739.
[21] Imam Riadi, Rusydi Umar, and M. I. Syahib, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)," J. RESTI Rekayasa Sist. Dan Teknol. Inf., vol. 5, no. 1, pp. 45–54, Feb. 2021, doi: 10.29207/resti.v5i1.2626.
[22] I. Riadi, Sunardi, and F. T. Nani, "Analisis Forensik pada Email Menggunakan Metode National Institute of Standards Technology," JISKA J. Inform. Sunan Kalijaga, vol. 7, no. 2, pp. 83–90, May 2022, doi: 10.14421/jiska.2022.7.2.83-90.

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 599–608
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9034

[23] M. Muammar, I. Riadi, and R. Umar, "Pengembangan Alat Forensik Whatsapp Menggunakan Android Debug Bridge Sebagai Metode Akuisisi Data," JIPI J. Ilm. Penelit. Dan Pembelajaran Inform., vol. 10, no. 2, pp. 1099–1110, Mar. 2025, doi: 10.29100/jipi.v10i2.5968.
[24] F. D. Setiawan Sumadi, A. R. Widagdo, A. F. Reza, and - Syaifuddin, "SD-Honeypot Integration for Mitigating DDoS Attack Using Machine Learning Approaches," JOIV Int. J. Inform. Vis., vol. 6, no. 1, p. 39, Mar. 2022, doi: 10.30630/joiv.6.1.853.
[25] I. M. Razzanda and Muhammad Koprawi, "Implementasi IDS dan IPS terhadap Serangan TCP Port Scanning dan ICMP Flooding," Indones. J. Comput. Sci., vol. 13, no. 4, Aug. 2024, doi: 10.33022/ijcs.v13i4.4212.
[26] F. Antony and R. Gustriansyah, "Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata," MATRIK J. Manaj. Tek. Inform. Dan Rekayasa Komput., vol. 21, no. 1, pp. 43–52, Nov. 2021, doi: 10.30812/matrik.v21i1.1078.
[27] R. Wang, J. Zhao, H. Zhang, L. He, H. Li, and M. Huang, "Network Traffic Analysis Based on Graph Neural Networks: A Scoping Review," Big Data Cogn. Comput., vol. 9, no. 11, p. 270, Oct. 2025, doi: 10.3390/bdcc9110270.
[28] Y. Yang, T. Song, W. Yuan, and J. An, "Towards Reliable and Efficient Data Retrieving in ICN-based Satellite Networks," J. Netw. Comput. Appl., vol. 179, p. 102982, Apr. 2021, doi: 10.1016/j.jnca.2021.102982.