



**Analisis dan Rekonstruksi Forensik Serangan DDoS pada Jaringan
IPv6 Berbasis Framework *Digital Forensic Framework for
Reviewing and Investigating Cyber Attack (D4I)***

Frendi Yusroni Romadhona

23917012

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2026

Lembar Pengesahan Pembimbing

Analisis dan Rekonstruksi Forensik Serangan DDoS pada Jaringan IPv6 Berbasis Framework *Digital Forensic Framework for Reviewing and Investigating Cyber Attack (D4I)*

Frendi Yusroni Romadhona

23917012

Yogyakarta, 23 Januari 2026



Dr. Ahmad Luthfi, S.Kom., M.Kom.

Lembar Pengesahan Penguji

Analisis dan Rekonstruksi Forensik Serangan DDoS pada Jaringan IPv6 Berbasis Framework *Digital Forensic Framework for Reviewing and Investigating Cyber Attack (D4I)*

Frengdi Yusroni Romadhona

23917012

Yogyakarta, 23 Januari 2026

Tim Penguji,

Dr. Ahmad Luthfi, S.Kom., M.Kom.

Ketua

Dr. Yudi Prayudi, S.Si., M.Kom.

Anggota I

Dr. Feri Wijayanto, S.T., M.T.

Anggota II

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia

Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

Analisis dan Rekonstruksi Forensik Serangan DDoS pada Jaringan IPv6 Berbasis Framework *Digital Forensic Framework for Reviewing and Investigating Cyber Attack* (D4I)

Serangan *Distributed Denial of Service* (DDoS) pada jaringan IPv6 menjadi ancaman serius bagi keberlangsungan infrastruktur jaringan dan proses bisnis organisasi, terutama seiring dengan peningkatan migrasi dari protokol IPv4 ke IPv6. Serangan ini berpotensi menyebabkan kelumpuhan total pada layanan jaringan melalui anomali lalu lintas dan eksploitasi protokol yang sulit dideteksi. Namun, metode investigasi forensik yang ada saat ini masih memiliki keterbatasan dalam menangani karakteristik unik serangan IPv6 secara efektif. Penelitian ini mengimplementasikan pendekatan investigasi forensik terintegrasi yang menggabungkan metode *Live Forensics* dengan *Digital Forensic Framework for Reviewing and Investigating Cyber Attack* (D4I). Metode *Live Forensics* diterapkan untuk melakukan akuisisi data volatil (seperti log CPU, memori, dan trafik jaringan) secara *real-time* tanpa mengganggu operasional sistem. Selanjutnya, Framework D4I digunakan untuk menganalisis artefak yang diakuisisi tersebut melalui pemetaan *Cyber Kill Chain* (CKC) dan konstruksi *Chain of Artifacts* (CoA) guna merekonstruksi modus operandi serangan. Penelitian dilakukan melalui simulasi empat skenario serangan DDoS IPv6 (*Redirect Flood*, *Echo Flood*, *TCP Connect Flood*, dan *Neighbour Advertisement Flood*) pada lingkungan terkendali. Hasil penelitian menunjukkan bahwa metode yang diusulkan efektif dalam mendeteksi dan membedakan karakteristik serangan, baik yang menargetkan saturasi infrastruktur (*router*) maupun kelelahan sumber daya (*resource exhaustion*) pada *endpoint* server. Visualisasi rantai artefak berhasil membuktikan hubungan kausalitas serangan dan menyajikan laporan investigasi lengkap berbasis 5W1H. Penelitian ini memberikan kontribusi signifikan dalam penyediaan strategi forensik yang sistematis untuk mitigasi ancaman keamanan pada ekosistem jaringan IPv6.

Kata kunci

IPv6, DDoS, *Live Forensics*, D4I Framework, *Cyber Kill Chain*, Investigasi Forensik.

Abstract

Forensic Analysis and Reconstruction of DDoS Attacks on IPv6 Networks Based on the Digital Forensic Framework for Reviewing and Investigating Cyber Attack (D4I)

Distributed Denial of Service (DDoS) attacks on IPv6 networks pose a serious threat to network infrastructure and business continuity, particularly with the increasing migration from IPv4 to IPv6. These attacks can cause total service paralysis through traffic anomalies and protocol exploitation that are difficult to detect. However, current forensic investigation methods remain limited in effectively handling the unique characteristics of IPv6 attacks. This research implements an integrated forensic investigation approach combining the Live Forensics method with the Digital Forensic Framework for Reviewing and Investigating Cyber Attack (D4I). Live Forensics was applied to acquire volatile data (such as CPU logs, memory and network traffic) in real-time without disrupting system operations. Subsequently, the D4I Framework was utilized to analyze these artifacts through Cyber Kill Chain (CKC) mapping and Chain of Artifacts (CoA) construction to reconstruct the attack modus operandi. The study was conducted by simulating four IPv6 DDoS attack scenarios (Redirect Flood, Echo Flood, TCP Connect Flood, and Neighbor Advertisement Flood) in a controlled environment. The results demonstrate that the proposed method is effective in detecting and distinguishing attack characteristics, whether targeting infrastructure saturation (router) or resource exhaustion on the server endpoint. The artifact chain visualization successfully proved the causality of the attacks and provided a comprehensive investigation report based on 5W1H. This research contributes significantly to providing a systematic forensic strategy for mitigating security threats in the IPv6 network ecosystem..

Keywords

IPv6, DDoS, Live Forensics, D4I Framework, Cyber Kill Chain, Forensic Investigation.

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, 23 Januari 2026



Frendi Yusroni Romadhona



Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dalam penulisan tesis ini.

Realtime Forensic Analysis of Neighbor Advertisement (NA) Flood Attacks Targeting IPv6 Networks: A D4I Framework-Based Approach

Romadhona, Luthfi, (2026),

Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi (E-ISSN: 2807-5935) for Volume 5, Issue 1.

Kontributor	Jenis Kontribusi
Frengi Yusroni Romadhona	Mendesain eksperimen (70%) Menulis <i>paper</i> (100%)
Ahmad Luthfi	Mendesain eksperimen (30%) Mereview Artikel

Halaman Kontribusi

Penyelesaian tesis ini tidak terlepas dari kontribusi, dukungan, dan bimbingan berbagai pihak. Dengan segala kerendahan hati, penulis menyampaikan penghargaan dan rasa terima kasih yang setinggi-tingginya kepada:

1. Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom., selaku Dosen Pembimbing. Terima kasih atas dedikasi waktu, ketajaman analisis, serta arahan strategis yang diberikan di tengah kesibukan beliau. Bimbingan yang konstruktif dan diskusi mendalam yang terjalin telah menjadi fondasi utama bagi penulis dalam menyelesaikan penelitian ini dengan baik dan tepat arah.
2. Dewan Penguji Tesis, Bapak Dr. Yudi Prayudi, S.Si., M.Kom., Bapak Dr. Feri Wijayanto, S.T., M.T., dan Ibu Erika Ramadhani, S.T., M.Eng. Terima kasih atas evaluasi kritis, saran konstruktif, dan validasi akademik yang diberikan mulai dari tahap seminar proposal, kemajuan, hingga sidang akhir. Masukan berharga dari Bapak dan Ibu menjadi elemen krusial dalam penyempurnaan kualitas substansi dan metodologi tesis ini.
3. Keluarga kecil tercinta, kedua orang tua dan saudara. Terima kasih yang tak terhingga atas doa yang tidak pernah putus, kasih sayang yang tulus serta dukungan moral dan materiil yang tiada henti. Kehadiran dan motivasi keluarga menjadi landasan terkuat dan sumber energi bagi penulis untuk terus melangkah menyelesaikan pendidikan ini hingga tahap akhir.
4. Rekan-rekan Seperjuangan Angkatan FD-28 serta seluruh keluarga besar Magister Informatika UII. Terima kasih atas atmosfer akademik yang kolaboratif, diskusi intelektual yang mencerahkan, serta semangat kebersamaan dan persaudaraan yang telah terjalin selama masa studi ini.

Halaman Persembahan

Bismillāhirrahmānirrahīm

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat, karunia, dan hidayah-Nya. Shalawat serta salam senantiasa tercurah kepada Nabi Muhammad SAW. Atas izin dan ridho Allah SWT, penulis dapat menyelesaikan tesis ini dengan baik. Oleh karena itu, dengan penuh rasa syukur dan ketulusan, karya ini penulis persembahkan kepada:

1. Orang tua tercinta, Ayahanda Siswaji, S.Sos. dan Ibunda Dra. Lilik Hardiyani, sebagai pilar utama dalam kehidupan penulis yang senantiasa memberikan cinta tanpa syarat, doa yang tiada henti, serta pengorbanan yang tulus demi keberhasilan penulis.
2. Istri tercinta, Tanty Yanuar Widiyanti, S.Kom., M.Eng., serta anak-anak tersayang, Thalita Shofia Lathifah Romadhona, Muhammad Althaf Amrullah Romadhona dan Ahmad Rafif Fahrudin Romadhona, atas kepercayaan, kesabaran, semangat serta kasih sayang yang menjadi sumber kekuatan utama dalam menyelesaikan pendidikan dan penelitian ini.
3. Dosen pembimbing, Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom., Bapak Dr. Yudi Prayudi, M.Kom., serta Ibu Erika Ramadhani, S.T., M.Eng., yang telah memberikan bimbingan, ilmu pengetahuan, arahan, serta dukungan selama proses penyusunan tesis ini.
4. Keluarga tercinta, Kakak Wahyu Hermawan, S.T., serta Adik Firdaus Khusnul Muzaki, S.T. dan Aliza Husna Izzati, S.Tr.Kom., yang senantiasa memberikan dukungan moral dan energi positif kepada penulis.
5. Rekan-rekan dan sahabat, khususnya teman-teman FD 28 UII, PUSFID UII, Tim NDC BSI UII, serta Tim PTIPD UIN Sunan Kalijaga Yogyakarta, atas kebersamaan, semangat, dan dukungan yang telah diberikan.
6. Seluruh keluarga, sahabat, dan pihak lain yang tidak dapat penulis sebutkan satu per satu, terima kasih atas doa, bantuan, dan dukungan yang telah diberikan selama proses penyusunan tesis ini.

Semoga Allah SWT membalas seluruh kebaikan dengan pahala yang berlipat ganda dan menjadikan karya ini bermanfaat bagi pengembangan ilmu pengetahuan.

Kata Pengantar

Assalamualaikum Wr Wb.

Puji syukur atas kehadiran Allah SWT yang selalu mencurahkan hidayah dan taufiqnya kepada seluruh ciptaanNya. Alhamdulillahirabbil'alamiin, telah selesai Tesis ini disusun sebagai syarat untuk meraih gelar Magister Informatika di Universitas Islam Indonesia (UII) Yogyakarta konsentrasi Forensika Digital (FD) pada Fakultas Teknologi Industri. Study dan tugas penelitian tidak sampai pada tahap ini tanpa pemberian kesempatan dan keterlibatan pihak lain. Untuk ucapan rasa terima kasih kepada:

1. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D. sebagai rektor Universitas Islam Indonesia (UII) yang memberikan ruang dan waktu kepada penulis untuk menempuh pendidikan di UII.
2. Bapak Prof. Dr. Ir. Hari Purnomo., M.T., IPU, ASEAN.Eng. sebagai Dekan Fakultas Teknologi Industri (FTI) Universitas Islam Indonesia (UII) yang memberikan dukungan kebutuhan fasilitas proses awal hingga penyelesaian studi magister.
3. Bapak Irving Vitra Paputungan , S.T., M.Sc., Ph.D Sebagai Ketua Program Studi Informatika Program Magister Fakultas Teknologi Industri UII yang senantiasa mengarahkan mahasiswa memperhatikan segala aktivitas perkuliahan dan menyelesaikan tesis.
4. Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom. sebagai dosen pembimbing yang berkontribusi banyak dalam bentuk pemikiran, saran dan motivasi proses penelitian dari pra penelitian hingga akhir.
5. Civitas Fakultas Teknologi Industri dan Magister Informatika UII yang berkontribusi langsung dan tidak langsung dalam studi magister serta penyelesaian penelitian ini.
6. Istri dan anak-anak, serta Ayah, Ibu, Kakak dan Adik yang senantiasa mencurahkan kasih sayang setiap saat. Seluruh keluarga, kerabat yang memberikan dukungan berupa doa yang baik.
7. Mahasiswa MI secara umum dan mahasiswa konsentrasi Forensika Digital secara khusus yang sama-sama berjuang dan memberi energi positif secara langsung maupun tidak langsung.

Wassalamualaikum wr.wb.

Daftar Isi

Lembar Pengesahan Pembimbing	i
Lembar Pengesahan Penguji.....	ii
Abstrak.....	iii
Pernyataan Keaslian Tulisan	v
Daftar Publikasi	vi
Halaman Kontribusi.....	vii
Halaman Persembahan	viii
Kata Pengantar.....	ix
Daftar Isi	x
Daftar Tabel.....	xiii
Daftar Gambar	xiv
Glosarium	xv
BAB 1 Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	8
1.3 Batasan Masalah	8
1.4 Tujuan Penelitian	9
1.5 Manfaat Penelitian	9
1.6 Metodologi Penelitian	10
1.7 Sistematika Penulisan	11
BAB 2 Tinjauan Pustaka	13
2.1 Landasan Teori.....	13
2.1.1 Forensika Digital dan <i>Network Forensics</i>	13
2.1.2 Internet Protokol versi 6 (IPv6).....	14
2.1.3 <i>Live Forensics</i> dan <i>Order of Volatility</i>	15

2.1.4	Serangan <i>Distributed Denial of Service</i> (DDoS).....	16
2.1.5	Framework <i>Digital Forensic Framework for Reviewing and Investigating Cyber Attack</i> (D4I).....	16
2.1.6	Analisis dan Rasionalisasi Pemilihan Framework D4I	18
2.2	Penelitian Terdahulu	20
2.3	Kerangka Konseptual (<i>Conceptual Framework</i>).....	35
BAB 3 Metodologi		37
3.1	Langkah-langkah Penelitian.....	37
3.1.1	Studi Pustaka	37
3.1.2	Persiapan dan Alat	38
3.1.3	Simulasi Serangan	38
3.1.4	Monitoring <i>Traffic</i>	39
3.1.5	Akuisisi Data	39
3.1.6	Analisis Forensik	40
3.1.7	Laporan Analisis.....	42
3.1.8	Definisi Operasional dan Parameter Evaluasi	42
BAB 4 Hasil dan Pembahasan.....		44
4.1	Persiapan dan Alat	44
4.2	Simulasi Serangan.....	48
4.2.1	Tujuan Simulasi.....	48
4.2.2	Skenario Simulasi	48
4.3	Monitoring Trafik dan Performa Sistem.....	51
4.3.1	Monitoring Realtime traffic pada <i>Router</i>	51
4.3.2	Monitoring <i>Traffic</i> pada <i>Server Target</i>	53
4.4	Pengumpulan Data	54
4.5	Akuisisi, Preservasi dan Pemeriksaan Artefak	57
4.5.1	Identifikasi bukti digital (<i>Identification</i>)	57

4.5.2	Pengumpulan (<i>Collection</i>) dan Akuisisi (<i>Acquisition</i>) bukti digital	57
4.5.3	Preservasi (<i>preservation</i>) bukti digital	58
4.5.4	Pemeriksaan Data Mentah (<i>Raw</i>) Artefak Serangan	60
4.6	Analisis Forensik	76
4.6.1	Fase 1 - Pemetaan Artefak ke Fase <i>Cyber Kill Chain</i> (CKC)	77
4.6.2	Fase 2 - Analisis Investigasi	85
4.7	Laporan Analisis	94
4.8	Pembahasan Temuan Utama dan Relevansi Forensik	99
BAB 5 Kesimpulan dan Saran.....		101
5.1	Kesimpulan	101
5.2	Saran	102
Daftar Pustaka.....		103

Daftar Tabel

Tabel 1.1. Data statistik IPv6 APNIC, sumber : (Huston, 2025)	2
Tabel 1.2. Perbandingan antara IPv4 dan IPv6, sumber : (Saad, 2016)	3
Tabel 2.1. Perbandingan Kapabilitas Framework Forensik	18
Tabel 2.2. Ulasan Penelitian Terdahulu.....	21
Tabel 3.1. Daftar Aktor, Sistem Operasi dan <i>Tools</i>	38
Tabel 3.2. Paramater deteksi DDoS. (Sumber : Haseeb-ur-rehman et al., 2023).....	40
Tabel 3.3. Pertanyaan dan jawaban 5W-1H pada investigasi serangan DDoS IPv6.....	42
Tabel 4.1. Spesifikasi <i>Hardware</i>	44
Tabel 4.2. Spesifikasi komputer <i>Attacker</i>	45
Tabel 4.3. Spesifikasi komputer <i>Zombie</i>	45
Tabel 4.4. Spesifikasi <i>Router</i>	46
Tabel 4.5. Spesifikasi komputer investigator.	47
Tabel 4.6. Spesifikasi komputer <i>Monitoring</i>	47
Tabel 4.7. Spesifikasi Server Target.....	48
Tabel 4.8. CPU, IRQ dan <i>Disk Usage</i> pukul 22:20 – 22.25 WIB.	61
Tabel 4.9. CPU, IRQ dan <i>Disk Usage</i> pukul 22:32 – 22.37 WIB.	62
Tabel 4.10. CPU, IRQ dan <i>Disk Usage</i> pukul 23:13 – 23.20 WIB.	63
Tabel 4.11. CPU, IRQ dan <i>Disk Usage</i> pukul 23:31 – 23.38 WIB.	63
Tabel 4.12. CPU, IRQ dan <i>Disk Usage</i> pukul 00:02 – 00.10 WIB.	64
Tabel 4.13. Ringkasan trafik jaringan pukul 22:20 – 22.25 WIB.	66
Tabel 4.14. Ringkasan trafik jaringan pukul 22:32 – 22.37 WIB.	66
Tabel 4.15. Ringkasan trafik jaringan pukul 23:13 – 23.20 WIB.	67
Tabel 4.16. Ringkasan trafik jaringan pukul 23:31– 23:38 WIB.	67
Tabel 4.17. Ringkasan trafik jaringan pukul 00:02 – 00.10 WIB.	67
Tabel 4.18. Ringkasan <i>CPU Usage</i> pukul 22:10 – 22.20 WIB.	68
Tabel 4.19. Ringkasan <i>CPU Usage</i> pukul 22:32 – 22.37 WIB.	68
Tabel 4.20. Ringkasan <i>CPU Usage</i> pukul 23:13 – 23.20 WIB.	69
Tabel 4.21. Ringkasan <i>CPU Usage</i> pukul 23:31– 23:38 WIB.....	69
Tabel 4.22. Ringkasan <i>CPU Usage</i> pukul 00:02 – 00.10 WIB.	70
Tabel 4.23. Rata – rata <i>Memory Usage</i> pukul 22:10 – 22.20 WIB.	70
Tabel 4.24. Rata – rata <i>Memory Usage</i> pukul 22:32 – 22.37 WIB.	71
Tabel 4.25. Rata – rata <i>Memory Usage</i> pukul 23:13 – 23.20 WIB.	71
Tabel 4.26. Rata – rata <i>Memory Usage</i> pukul 23:31– 23:38 WIB.	71
Tabel 4.27. Rata – rata <i>Memory Usage</i> pukul 00:02 – 00.10 WIB.	72
Tabel 4.28. Koneksi ke server pukul 22.10 – 22.20 WIB.	72
Tabel 4.29. Koneksi ke server pukul 22:32 – 22.37 WIB.	73
Tabel 4.30. Koneksi ke server pukul 23.13 - 23.20 WIB.	74
Tabel 4.31. Koneksi ke server pukul 23:31– 23:38 WIB.	75
Tabel 4.32. Koneksi ke server pukul 00:02 – 00.10 WIB.	76
Tabel 4.33. Pemetaan Artefak ke Fase <i>Cyber Kill Chain</i> (CKC) Serangan pertama.	78
Tabel 4.34. Pemetaan Artefak ke Fase <i>Cyber Kill Chain</i> (CKC) Serangan kedua.	80
Tabel 4.35. Pemetaan Artefak ke Fase <i>Cyber Kill Chain</i> (CKC) Serangan ketiga.	81
Tabel 4.36. Pemetaan Artefak ke Fase <i>Cyber Kill Chain</i> (CKC) Serangan keempat.	83
Tabel 4.37. Perbandingan hasil analisis Rantai Artefak (CoA) keempat serangan.	93
Tabel 4.38. Hasil investigasi forensik terhadap serangan DDoS pada jaringan IPv6.	95

Daftar Gambar

Gambar 1.1. Statistik IPv6 Google, Sumber : (Google, 2025).....	1
Gambar 1.2. IPv6 <i>Vulnerability Classes</i> , Sumber : (Tayyab et al., 2020)	4
Gambar 1.3. Metodologi penelitian.....	11
Gambar 2.1. Fase dalam forensika digital, sumber (Kent et al., 2006)	13
Gambar 2.2. <i>Conceptual framework</i> penelitian.....	36
Gambar 3.1. Tahapan Metodologi Penelitian, sumber : (Pollitt, 2019).....	37
Gambar 3.2. Simulasi serangan DDoS IPv6.....	39
Gambar 3.3. Alur akuisisi <i>Live Forensic</i> , sumber : (Kumar et al., 2016)	40
Gambar 3.4. Tahapan <i>Cyber-Kill-Chain</i> (CKC), sumber: (Dimitriadis et al., 2020).....	41
Gambar 3.5. Tahapan Pemeriksaan dan Analisis D4I, sumber: (Dimitriadis et al., 2020) .	41
Gambar 4.1. Data awal <i>resource</i> router pukul 22:10 – 22.20 WIB.....	51
Gambar 4.2. Data <i>resource</i> router pukul 22:32 – 22.37 WIB.	52
Gambar 4.3. Data <i>resource</i> router pukul 00:02 – 00.10WIB	53
Gambar 4.4. Skema Pengumpulan Data.....	54
Gambar 4.5. Hasil file output pada penyimpanan router.....	55
Gambar 4.6. <i>Capture</i> lalu lintas jaringan router port 37008	56
Gambar 4.7. Hasil <i>capture cpu load, memory, bandwidth</i> dan lalu lintas data server	57
Gambar 4.8. Proses pengumpulan artefak serangan menggunakan sFTPCClient	58
Gambar 4.9. File hasil akuisisi yang belum memiliki <i>hash</i>	59
Gambar 4.10. File hasil akuisisi yang sudah memiliki nilai <i>hash</i>	60
Gambar 4.11. salah satu contoh <i>hash properties</i>	60
Gambar 4.12. <i>Resource Usage</i> 2025-05-10 pukul 22:20 – 22.25 WIB.....	61
Gambar 4.13. <i>Resource Usage</i> 2025-05-10 pukul 22:32 – 22.37 WIB.....	62
Gambar 4.14. <i>Resource Usage</i> 2025-05-10 pukul 23:13– 23:20 WIB.	63
Gambar 4.15. <i>Resource Usage</i> 2025-05-10 pukul 23:31– 23:38 WIB.	64
Gambar 4.16. <i>Resource Usage</i> 2025-05-11 pukul 00:02 – 00.10 WIB.....	65
Gambar 4.17. Tampilan <i>Traffic Capture</i> pukul 22:10 – 22.20 WIB.....	72
Gambar 4.18. Tampilan <i>Traffic Capture</i> pukul 22:02 – 00.10 WIB.....	73
Gambar 4.19. Tampilan <i>Traffic Capture</i> pukul 23.13 - 23.20 WIB.....	74
Gambar 4.20. Tampilan <i>Traffic Capture</i> pukul 23:31– 23:38 WIB.....	75
Gambar 4.21. Tampilan <i>Traffic Capture</i> pukul 00:02 – 00.10 WIB.....	76
Gambar 4.22. Hasil konstruksi CoA untuk serangan pertama / <i>ICMPv6 Redirect Flood</i> ...	88
Gambar 4.23. Hasil konstruksi CoA untuk serangan kedua / <i>ICMPv6 Request Flood</i>	89
Gambar 4.24. Hasil konstruksi CoA untuk serangan ketiga / <i>TCP Connect Flood</i>	90
Gambar 4.25. Hasil konstruksi CoA untuk serangan keempat / <i>DDoS NA</i>	91

Glosarium

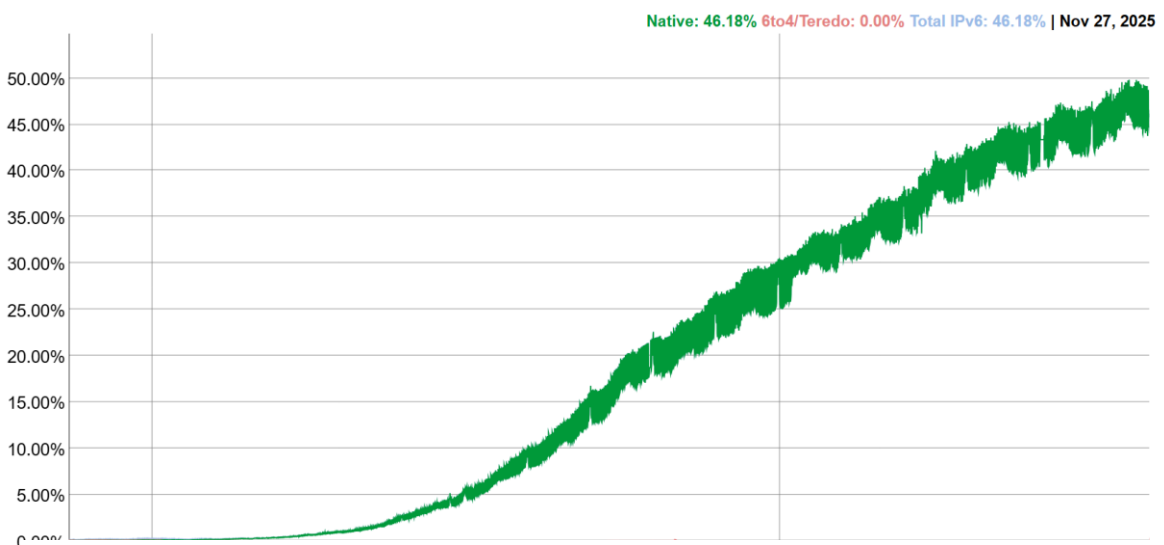
IPv6	- Internet Protocol Version 6
IPv4	- Internet Protocol Version 4
IANA	- Internet Assigned Numbers Authority
APNIC	- Asia-Pacific Network Information Centre
NIR	- National Internet Registry
RIR	- Regional Internet Registry
DoS	- Denial of Service
DDoS	- Distributed Denial of Service
DHCPv6	- Dynamic Host Configuration Protocol for IPv6
SLAAC	- Stateless Address Autoconfiguration
IPSec	- Internet Protocol Security
ICMPv6	- Internet Control Message Protocol for IPv6
NDP	- Neighbor Discovery Protocol
RA	- Router Advertisement
MLD	- Multicast Listener Discovery

BAB 1

Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi internet yang sangat pesat dan pertumbuhan pengguna yang semakin meningkat membuat transisi *Internet Protocol version 4* (IPv4) ke *Internet Protocol version 6* (IPv6) di lingkungan global semakin meningkat (A. Naagas & P. Gamilla, 2022). Peningkatan ini disebabkan beberapa faktor seperti mulai habisnya alokasi alamat IPv4 yang didistribusikan oleh IANA (*Internet Assigned Numbers Authority*) dan meningkatnya kebutuhan pengguna untuk terkoneksi ke jaringan internet yang membutuhkan ruang alamat IP yang lebih besar (Huston, 2025). Kondisi tersebut membuat beberapa organisasi dan penyedia layanan internet / ISP (*Internet Service Provider*) di seluruh dunia melakukan migrasi dan adaptasi menggunakan Internet Protocol version 6 (IPv6). Sampai dengan akhir tahun 2025, penggunaan IPv6 mengalami peningkatan yang signifikan. Menurut data statistik yang dikelola oleh Google per 27 November 2025 yang bersumber pada (Google, 2025) pengguna yang melakukan akses ke layanan Google menggunakan IPv6 sebesar 46,18% dari total trafik seperti terlihat pada gambar 1.1 berikut.



Gambar 1.1. Statistik IPv6 Google, Sumber : (Google, 2025)

Menurut data yang dihimpun oleh APNIC (*Asia Pacific Network Information Centre*) yang diambil dari (Huston, 2025), saat ini statistik pengguna IPv6 global per tanggal 15 juli 2024 mencapai 38,21% dengan sampel 716.352.249 pengguna yang meliputi lima benua seperti terlihat pada Tabel 1.1 berikut.

Tabel 1.1. Data statistik IPv6 APNIC, sumber : (Huston, 2025)

Code	Region	IPv6 Capable	IPv6 Preferred	Sample
XA	World	38.21%	36.99%	716,352,249
XD	Asia	44.69%	43.04%	405,140,776
XC	Americas	43.48%	42.84%	128,115,398
XF	Oceania	38.94%	36.08%	5,341,391
XE	Europe	32.08%	31.04%	102,899,992
XG	Unclassified	9.47%	9.43%	27,969
XB	Africa	2.54%	2.46%	74,854,221

Dari data tersebut dapat dilihat bahwa tren penggunaan IPv6 sebagai protokol untuk terhubung ke jaringan global / internet mengalami kenaikan yang signifikan. Untuk mempercepat adopsi dan migrasi dari IPv4 ke IPv6 beberapa usaha telah dilakukan oleh NIR (National Internet Registry) dan RIR (*Regional Internet Registry*) seperti melakukan pembatasan alokasi IPv4 untuk ISP (*Internet service Provider*) baru atau organisasi yang mengajukan AS Number, membebaskan biaya berlangganan untuk IPv6 dan melakukan sosialisasi dan training ke pengguna (Huston, 2022).

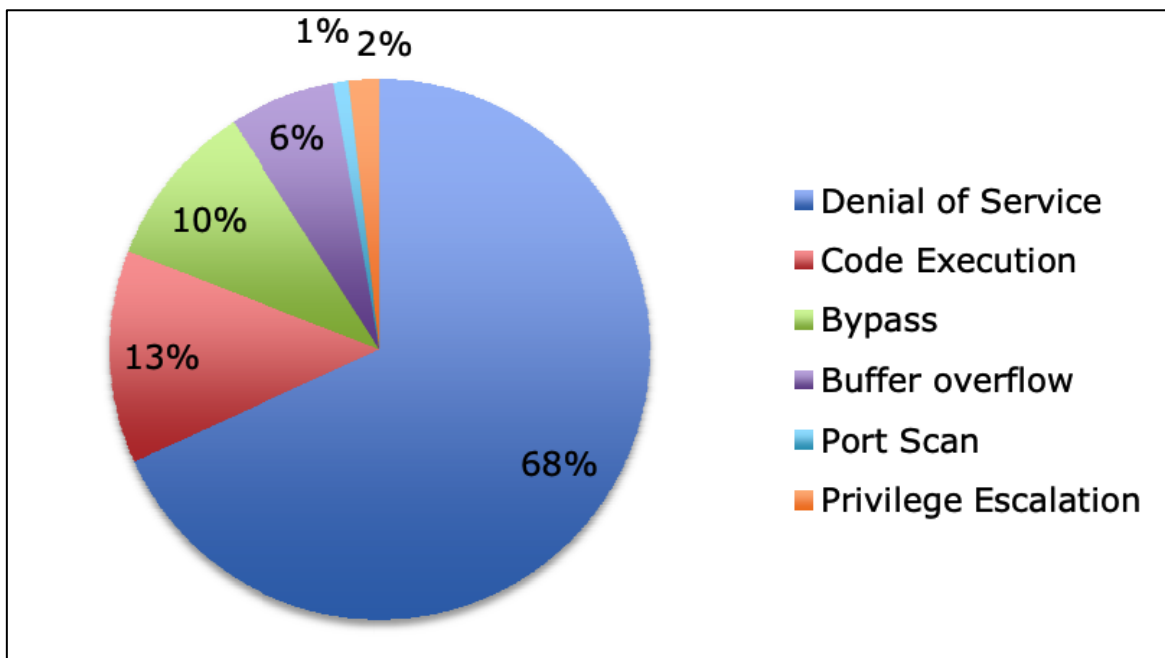
Internet Protocol versi 6 (IPv6) pertama kali diperkenalkan ke publik pada tahun 1997 dengan draf spesifikasi RFC2460. kemudian IETF melakukan pembaharuan standar spesifikasi IPv6 sebagai protokol internet global melalui draf RFC8200 (Saad, 2016). IPv6 menjawab keterbatasan alamat IP dengan menyediakan address space sebesar 128-bit dibandingkan dengan IPv4 yang memiliki panjang address space 32-bit (Elejla et al., 2022a). Selain itu IPv6 juga memiliki beberapa fitur yang menjadi kelebihan seperti, header yang lebih simpel, End-to-End Connectivity, konfigurasi otomatis dengan Stateless Address Auto-configuration (SLAAC) dan DHCPv6, tidak ada broadcast traffic serta adanya fitur security IPsec (Saad, 2016). Perbandingan spesifikasi antara IPv4 dan IPv6 bisa dilihat pada Tabel 1.2 berikut.

Tabel 1.2. Perbandingan antara IPv4 dan IPv6, sumber : (Saad, 2016)

	IPv4	IPv6
Addressing	32 bits	128 bits
Address Resolution	ARP	ICMPv6 NS/NA
Auto Configuration	DHCP&ICMP RS/RA	ICMPv6 RS/RA & DHCPv6
Fault Isolation	ICMP	ICMPv6
IPSec Support	Optional	Recomended
Fragmentation	Both in hosts and routers	Only in hosts

Dalam proses komunikasinya dengan host lain, IPv6 menggunakan *Internet Control Message Protocol version 6* (ICMPv6) yang didefinisikan oleh (Postel, 1981). ICMPv6 merupakan protokol inti dalam IPv6 yang digunakan untuk mengirim pesan dan informasi operasional untuk menggantikan dan memperluas fungsi ICMP pada IPv4 (Tayyab et al., 2020). Fungsi ICMPv6 digunakan untuk melakukan diagnosa jaringan seperti *Ping*, pengiriman pesan kesalahan (*error message*) seperti *Destination Unreachable* dan *Packet Too Big*, pengalokasian alamat IPv6 (SLAAC) serta jalur routing dengan fitur *Neighbor Discovery Protocol* (NDP) yang menggantikan *Address Resolution Protocol* (ARP) pada IPv4.

Seiring dengan berkembangnya ekosistem IPv6, muncul tantangan baru dalam aspek keamanan. Salah satunya yakni ancaman serangan DoS/DDoS pada jaringan IPv6 yang berdampak pada aspek *Availability* sebuah layanan. *Internet Control Message Protocol for IPv6* (ICMPv6) sebagai bagian integral dari protokol IPv6 yang berfungsi untuk melakukan diagnosis dan *error reporting* memiliki kelemahan yang membuatnya rentan terhadap berbagai ancaman keamanan. Salah satu ancaman paling fatal dalam protokol IPv6 adalah serangan *ICMPv6 Distributed DoS* (DDoS) (A. Naagas & P. Gamilla, 2022). DDoS bekerja dengan cara membanjiri mesin server target dengan banyak paket untuk menghabiskan sumber daya mesin, bandwidth dan membuat server target berhenti beroperasi. *Arbor network*, salah satu perusahaan yang bergerak dibidang infrastruktur keamanan jaringan mengungkapkan, serangan DDoS ICMPv6 pertama kali pada tahun 2011 (Tayyab et al., 2020). menurut data dari *National Vulnerability Database* (NVD), DDoS masih menjadi serangan utama dalam jaringan IPv6 seperti yang ditunjukkan dalam gambar 1.2 berikut.



Gambar 1.2. IPv6 *Vulnerability Classes*, Sumber : (Tayyab et al., 2020)

Berdasarkan *Cyber Security Watch Survey* tahun 2014 (A. Naagas & P. Gamilla, 2022), peningkatan jumlah insiden keamanan cenderung lebih cepat dibandingkan kemampuan perusahaan untuk menghadapi serangan. Laporan ini menyatakan bahwa serangan *DoS/DDoS flooding* pada jaringan IPv6 merupakan ancaman siber utama. Menurut penelitian (Bdair Alghuraibawi et al., 2021) saat ini teknik untuk mengamankan jaringan IPv6 baik secara ofensif maupun defensif lebih sedikit dibandingkan dengan protokol IPv4. Begitu pun dengan teknik untuk melakukan investigasi forensik pada kejadian siber pada jaringan IPv6 cenderung lebih sedikit dibandingkan IPv4.

Dalam proses investigasi forensik serangan DDoS pada jaringan IPv6, penggunaan forensika jaringan (*Network Forensics*) menjadi hal yang penting. Proses forensik ini tidak hanya membantu mengidentifikasi sumber serangan tetapi juga mendokumentasikan bukti-bukti digital yang dapat digunakan dalam proses hukum (Al-Dhaqm et al., 2021). Dalam mengungkap kejahatan siber, digital forensik menerapkan 4 (empat) tahapan yaitu: Pengumpulan (*Acquisition*), Pemeliharaan (*Preservation*), Analisa (*Analysis*), Presentasi (*Presentation*) (Aisyah et al., 2022a). Menurut penelitian (Nicolls et al., 2016), investigasi forensik terhadap serangan DDoS pada jaringan IPv6 memiliki keunikan tersendiri dibandingkan dengan jaringan IPv4 dikarenakan perbedaan dalam struktur alamat dan protokol yang digunakan. Penggunaan Network Forensics pada insiden serangan DDoS IPv6

juga sebagai upaya untuk mengembangkan metode deteksi dan mitigasi yang lebih efektif. Penelitian (Alim et al., 2018a) menunjukkan bahwa analisis forensik yang mendalam dengan melibatkan pengumpulan data secara real-time dan analisis jaringan dapat mengungkap pola-pola serangan yang sebelumnya tidak terlihat.

Salah satu metode dalam forensika jaringan (*Network Forensics*) yang digunakan dalam investigasi serangan DDoS pada jaringan IPv6 adalah *Live Forensics*. Penggunaan *Live Forensics* dalam investigasi serangan DDoS pada jaringan IPv6 sangat penting untuk mengumpulkan bukti digital seperti aktivitas memori dan lalu lintas jaringan secara real-time saat serangan sedang berlangsung, sehingga meminimalkan risiko kehilangan informasi kritis yang dapat terjadi jika pengumpulan data dilakukan setelah serangan berakhir (Prayogo & Riadi, 2020). *Live Forensics* memiliki kelebihan dalam mengidentifikasi pola yang digunakan oleh penyerang dengan tingkat akurasi yang lebih tinggi, terutama dalam jaringan IPv6 yang memiliki kompleksitas lebih besar dibandingkan IPv4. Studi menunjukkan bahwa tanpa *Live Forensics*, banyak jejak digital yang penting hilang atau menjadi sulit diinterpretasikan mengingat sifat dinamis dari lalu lintas jaringan IPv6 dan teknik penyamaran yang sering digunakan oleh penyerang (Alim et al., 2018a).

Untuk meningkatkan akurasi dan efektifitas dalam proses investigasi forensik serangan DDoS pada jaringan IPv6, diperlukan integrasi antara metode *Live Forensic* dengan framework digital forensik / *Digital Forensics Framework* (DFF). Penelitian yang dilakukan oleh (Triawan Adi Cahyanto et al., 2022) dan (Syamsuddin & Syamsuar, 2023) menyoroti bahwa *Live Forensics* menghadapi tantangan dalam mengumpulkan bukti dari memori volatil, dimana proses pengambilan artefak sering kali tidak diiringi oleh analisis yang sistematis terhadap semua data yang ada. Hal ini menunjukkan bahwa analisis mendalam sering kali diabaikan saat pengumpulan bukti secara cepat. Oleh karena itu, integrasi *Live Forensics* dengan framework digital forensik menjadi sangat penting untuk mencapai tujuan dari forensik digital yakni terjawabnya pertanyaan 5WH (*What, Who, When, Where, Why* dan *How*) melalui proses forensik digital (Hakim et al., 2023). Sejauh ini, berbagai metode dan framework telah diusulkan, namun belum ada yang secara universal diakui sebagai praktik terbaik. Sistematisasi proses dalam beberapa framework tersebut umumnya dimulai dengan pengumpulan artefak dan diakhiri dengan pelaporan barang bukti (Aisyah et al., 2022b). Menurut penelitian berbasis *review* oleh (Khanafseh et al., 2019), Berbagai framework yang diusulkan dalam beberapa tahun terakhir seperti *Generic Process Model for Network Forensics* (GPMNM), *Cyber Forensic Field triage Process Model* (CFFTPM), *Systematic Digital forensic Investigation Model* (SRDFIM) dan *Digital Forensic*

Framework for Reviewing and Investigating Cyber Attack (D4I) yang menawarkan pendekatan fase dan detail yang beragam dalam investigasi forensik. Menurut penelitian (Rogers et al., 2006) framework investigasi *Cyber Forensic Field triage Process Model* (CFFTPM) memiliki fitur untuk mengidentifikasi, menganalisis dan menginterpretasikan bukti digital secara cepat dengan berfokus pada pengurangan waktu yang dibutuhkan dalam proses investigasi. Di sisi lain, framework *Generic Process Model for Network Forensics* (GPMNM) menawarkan pendekatan yang sistematis dalam investigasi jaringan komputer mencakup beberapa tahap penting, seperti persiapan, deteksi, respons insiden, pengumpulan dan pelestarian data, analisis serta presentasi dan pelaporan (Joshi & Pilli, 2016). Penelitian oleh (Agarwal et al., 2011) mengusulkan *Framework Systematic Digital forensic Investigation Model* (SRDFIM) yang mencakup sebelas fase yang membantu dalam pengolahan barang bukti yang bersifat dinamis untuk menjawab rekonstruksi peristiwa, serta dapat memastikan integritas bukti digital. Sedangkan penelitian (Dimitriadis et al., 2020a) mengusulkan framework *Digital Forensic Framework for Reviewing and Investigating Cyber Attack* (D4I) untuk menyempurnakan framework yang sudah ada dengan menambahkan kategorisasi artefak berdasarkan *Cyber Kill Chain* (CKC) untuk memudahkan eksaminasi dan analisis. Oleh karena itu, integrasi metode *Live Forensics* dengan framework yang tepat dapat meningkatkan efektifitas deteksi dan analisa forensik dalam merespons serangan DDoS pada jaringan IPv6.

Berdasarkan penelitian terdahulu terdapat sejumlah solusi yang dapat diimplementasikan untuk melakukan deteksi dan investigasi forensik pada serangan DDoS. Diantaranya penelitian yang dilakukan oleh (Alim et al., 2018b) menggunakan *metode Live Forensic* untuk deteksi DDoS pada MikroTik Routerboard untuk memperoleh bukti digital berupa sumber alamat IP penyerang, *Timestamp* dan jenis paket. Namun pada penelitian ini masih terbatas pada jaringan IPv4 dan tanpa menggunakan framework forensika digital dalam proses analisis dan pengolahan artefak. Penelitian yang dilakukan oleh (Hui et al., 2011) membahas tentang deteksi serangan DDoS menggunakan *flow detection* dan melakukan SSL/TTL monitoring pada jaringan IPv6. Namun pada hasil penelitian tersebut tidak dapat diketahui apakah trafik tersebut merupakan trafik asli atau DDoS hanya berdasarkan besaran request. Penelitian (Kumar et al., 2016) berfokus pada *traffic forensic* pada beberapa sensor *wireless* berbasis IPv6 yang berpotensi menjadi sumber serangan DDoS, namun penelitian tersebut dilakukan setelah serangan terjadi (*Post Incident Analysis*). Pendekatan lain juga dilakukan oleh (Suharti et al., 2022) dengan menggabungkan metode ADDIE dan HIDS untuk mendeteksi trafik DDoS pada jaringan IPv4, metode

tersebut berhasil melakukan deteksi DDoS dengan akurasi 98,91%. Namun pengujian tersebut terbatas pada sistem operasi *Windows* (IIS Server) dan jaringan IPv4.

Untuk mengatasi kesenjangan tersebut, penelitian ini mengimplementasikan pendekatan investigasi yang mengintegrasikan metode *Live Forensics* dengan *Digital Forensic Framework for Reviewing and Investigating Cyber Attack* (D4I). Framework D4I dipilih karena keunggulannya dalam mengkategorikan artefak serangan ke dalam fase *Cyber Kill Chain* (CKC) dan membangun rantai bukti (*Chain of Artifacts*) yang dapat memvisualisasikan hubungan sebab-akibat dari serangan.

Untuk memvalidasi pendekatan ini, peneliti telah membuat skenario simulasi serangan DDoS pada jaringan IPv6. Simulasi menggunakan *Mikrotik Cloud Host Router* (CHR) sebagai router utama. Tools analisis jaringan seperti *Wireshark* digunakan untuk menangkap dan menganalisis paket jaringan secara mendetail yang memungkinkan peneliti untuk mengidentifikasi pola-pola anomali selama serangan berlangsung. Selain itu, komputer dengan sistem operasi kali linux akan digunakan sebagai platform untuk menjalankan serangan dan menggunakan server linux sebagai target serangan dengan memanfaatkan beberapa host sebagai *zombie* untuk melakukan amplifikasi serangan DDoS di jaringan IPv6. Selain itu peneliti memastikan lingkungan simulasi yang realistis dan sesuai dengan skenario dunia nyata.

Dalam proses pemeriksaan dan analisa serangan DDoS di jaringan IPv6, penulis menggunakan framework D4I dengan dua fase utama. Fase pertama yakni kategorisasi artefak hasil investigasi *Live Forensics* dan mapping ke dalam CKC (*Cyber Kill Chain*). Fase kedua yakni melakukan pemeriksaan dan analisa artefak menggunakan enam langkah D4I meliputi *Choose, Identify, Correlate, Construct Chain of correlated Artifacts* (CoA), *Repeat* dan *Analyze CoA*. Metode ini tidak hanya mendeteksi serangan dengan lebih cepat, tetapi juga untuk mengolah artefak digital yang dihasilkan guna memahami pola-pola serangan yang kompleks pada serangan DDoS di jaringan IPv6.

Dalam penelitian ini, pendekatan tersebut telah diterapkan dan diuji melalui simulasi serangan DDoS pada jaringan IPv6 yang mencakup berbagai skenario serangan volumetrik dan protokol. Penelitian ini tidak hanya berhasil mendeteksi serangan secara real-time, tetapi juga membuktikan efektivitas D4I dalam merekonstruksi modus operandi serangan dan menjawab pertanyaan investigasi 5W1H (*What, Who, When, Where, Why, How*) secara komprehensif. Hasil penelitian ini memberikan kontribusi signifikan berupa strategi investigasi forensik yang terstruktur dan valid untuk menghadapi ancaman keamanan pada ekosistem jaringan IPv6 yang terus berkembang.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Kompleksitas Serangan pada Ekosistem IPv6 Migrasi ke jaringan IPv6 memperluas permukaan serangan (*Attack Surface*) dengan munculnya vektor ancaman baru yang mengeksploitasi fitur protokol dan sulit dideteksi oleh mekanisme keamanan konvensional karena volume ruang alamat yang besar dan pola trafik yang dinamis.
2. Metode forensik tradisional (*Dead Forensics*) memiliki keterbatasan dalam investigasi serangan DDoS IPv6 yang memungkinkan resiko hilangnya artefak volatil yang krusial (seperti koneksi jaringan aktif, proses di memori RAM dan status *Neighbor Cache*) yang diperlukan untuk atribusi serangan secara akurat.
3. Bagaimana mengolah data mentah (*Raw Data*) dari hasil akuisisi sehingga menjadi informasi yang valid sehingga mampu mengungkap modus operandi serangan secara utuh.

Berdasarkan latar belakang dan rumusan masalah yang telah diuraikan, penelitian ini dirancang untuk menjawab pertanyaan-pertanyaan berikut:

1. Bagaimana formulasi model integrasi *Live Forensics* pada fase *Identification* dalam siklus framework D4I untuk mengakuisisi artefak volatil serangan DDoS IPv6 secara *real-time* tanpa mendisrupsi layanan jaringan?
2. Bagaimana kapabilitas *Cyber Kill Chain* (CKC) dan *Chain of Artifacts* (CoA) dalam framework D4I untuk merekonstruksi kausalitas serangan serta memetakan perbedaan karakteristik dampak (*Point of Failure*) antara serangan volumetrik dan serangan protokol pada infrastruktur IPv6?
3. Bagaimana efektifitas pendekatan forensik berbasis integrasi *Live Forensics* dan framework D4I ditinjau dari aspek kelengkapan rekonstruksi, validitas atribusi dan komprehensivitas laporan investigasi berbasis 5W1H (*What, Who, When, Where, Why, How*)?

1.3 Batasan Masalah

Agar pembahasan penelitian ini tetap fokus dan terarah, ditetapkan batasan-batasan masalah sebagai berikut:

1. Penelitian ini difokuskan pada empat jenis skenario serangan *Distributed Denial of Service* (DDoS) pada jaringan IPv6 yang meliputi serangan volumetrik (*ICMPv6 Echo Request Flood* dan *Redirect Flood*), serangan berbasis protokol (*ICMPv6*

Neighbor Advertisement Flood) dan serangan pada lapisan transport (*TCP Connect Flood*). Penelitian tidak mencakup serangan pada lapisan aplikasi (Layer 7) seperti HTTP Flood.

2. Pendekatan forensik yang digunakan dibatasi pada integrasi metode *Live Forensics* untuk akuisisi data volatil dan framework D4I (*Digital Forensic Framework for Reviewing and Investigating Cyber Attack*) untuk analisis artefak. Metode forensik tradisional (*dead forensics*) seperti analisis image hard disk pasca-insiden tidak menjadi fokus dalam penelitian ini.
3. Implementasi dan pengujian dilakukan dalam lingkungan laboratorium simulasi terkendali menggunakan virtualisasi (PNETLab/VMware) dengan topologi jaringan yang merepresentasikan infrastruktur sederhana (Router Mikrotik dan Server Ubuntu).
4. Evaluasi dampak serangan dibatasi pada parameter kinerja sistem utama yaitu penggunaan CPU, Memori dan Bandwidth pada router dan server target serta analisis paket jaringan (PCAP). Analisis dampak finansial, reputasi organisasi atau aspek legal formal dari serangan tidak dibahas dalam penelitian ini.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dipaparkan di atas, tujuan dari penelitian ini adalah untuk:

- a. Merumuskan model integrasi *Live Forensics* dalam siklus D4I untuk menangani volatilitas bukti IPv6.
- b. Menganalisis karakteristik serangan dan merekonstruksi kausalitas dampak menggunakan visualisasi Chain of Artifacts (CoA).
- c. Mengevaluasi efektivitas metode investigasi berdasarkan parameter kelengkapan, validitas dan standar pelaporan 5W1H.

1.5 Manfaat Penelitian

- a. Manfaat Sosial
 1. Menyediakan prosedur operasional standar (SOP) bagi administrator jaringan dan tim *Incident Response* (CSIRT) dalam melakukan akuisisi bukti digital volatil secara aman tanpa mematikan layanan kritis.
 2. Hasil penelitian membantu pengelola infrastruktur IT untuk membedakan karakteristik serangan—apakah serangan menargetkan infrastruktur (router) atau

endpoint (server)—sehingga strategi mitigasi yang diambil dapat lebih tepat sasaran dan efisien.

3. Meningkatkan kesadaran mengenai vektor ancaman baru pada protokol IPv6 yang memerlukan pengawasan sumber daya komputasi (CPU/RAM) secara ketat, bukan hanya sekadar memantau bandwidth.

b. Manfaat Ilmiah

1. Memberikan kontribusi pada literatur forensik digital dengan mengisi kesenjangan (*gap*) penelitian terkait investigasi serangan DDoS pada protokol IPv6 yang masih terbatas, khususnya dalam penerapan metode *Live Forensics*.
2. Membuktikan bahwa framework D4I yang semula dirancang untuk investigasi intrusi (*malware/APT*), dapat diadaptasi secara efektif untuk investigasi serangan DDoS melalui modifikasi pemetaan *Cyber Kill Chain* (CKC).
3. Menghasilkan model visualisasi *Chain of Artifacts* (CoA) yang teruji mampu merekonstruksi hubungan sebab-akibat (*Causality*) antara vektor serangan dengan dampak spesifik pada sumber daya sistem.

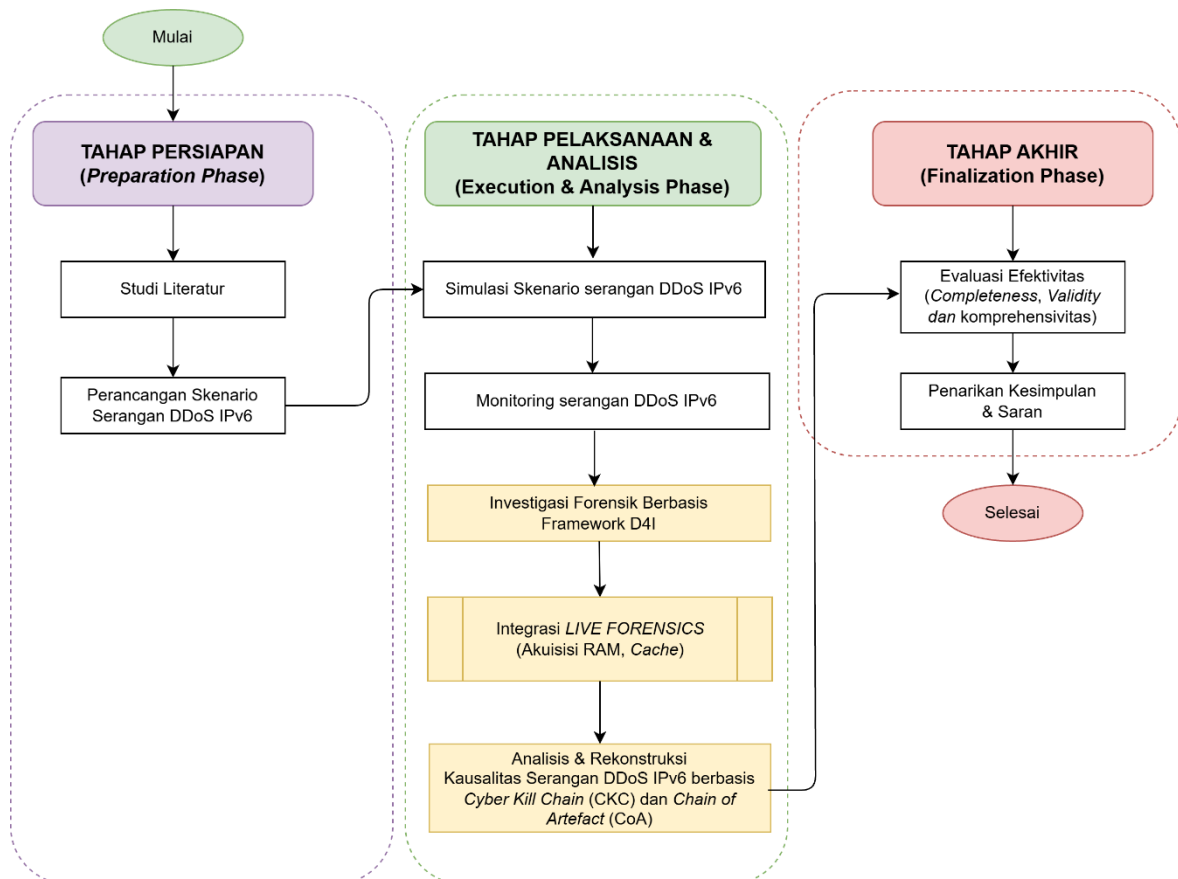
Adapun luaran utama dari penelitian ini berupa publikasi artikel ilmiah pada jurnal nasional terakreditasi SINTA. Publikasi ini bertujuan untuk mendiseminasikan temuan empiris mengenai efektivitas integrasi metode *Live Forensics* dan framework D4I dalam merekonstruksi insiden serangan *Distributed Denial of Service* (DDoS) pada ekosistem jaringan IPv6. Artikel hasil penelitian ini diharapkan dapat memberikan kontribusi teoritis dengan memperkaya literatur forensik digital, khususnya terkait adaptasi model *Cyber Kill Chain* untuk serangan berbasis protokol. Selain itu, publikasi ini juga ditujukan sebagai referensi teknis bagi komunitas akademisi dan praktisi keamanan siber dalam mengembangkan strategi mitigasi dan investigasi yang responsif terhadap ancaman pada infrastruktur jaringan IPv6 dimasa depan.

1.6 Metodologi Penelitian

Untuk menjaga validitas hasil dan menjaga arah penelitian agar tetap sistematis, penelitian ini dilaksanakan melalui alur kerja terstruktur yang divisualisasikan pada Gambar 1.3. Metodologi penelitian diklasifikasikan ke dalam tiga tahapan fundamental, yaitu:

1. Tahap Persiapan (*Preparation Phase*): Tahap ini diawali dengan studi literatur mendalam terkait kerentanan protokol IPv6 dan arsitektur forensik, dilanjutkan dengan perancangan topologi jaringan simulasi serta skenario serangan (*Volumetric & Protocol Attacks*) menggunakan simulator PnetLAB pada infrastruktur VMware.

2. Tahap Pelaksanaan dan Analisis (*Execution and Analysis Phase*): Tahapan ini merupakan inti ini menerapkan proses investigasi berbasis framework D4I (*Digital Forensic Framework for Reviewing and Investigating Cyber Attack*) yang diintegrasikan dengan metode *Live Forensics*. Fokus utama pada tahap ini adalah akuisisi artefak volatil (seperti RAM dan Neighbor Cache) pada fase *Identification*, diikuti dengan rekonstruksi kausalitas serangan menggunakan fitur *Chain of Artifacts* (CoA).
3. Tahap Akhir (*Finalization Phase*): Tahap ini mencakup evaluasi efektivitas metode investigasi berdasarkan parameter kelengkapan rekonstruksi, validitas atribusi, dan komprehensivitas laporan, yang diakhiri dengan penarikan kesimpulan.



Gambar 1.3. Metodologi penelitian

1.7 Sistematika Penulisan

Untuk memberikan gambaran yang komprehensif dan terstruktur mengenai alur penelitian, sistematika penulisan tesis ini disusun ke dalam lima bab utama sebagai berikut:

BAB I PENDAHULUAN

Bab ini menguraikan fondasi dasar penelitian yang meliputi latar belakang permasalahan mengenai urgensi keamanan pada transisi protokol IPv6, rumusan masalah yang berfokus pada integrasi forensik, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan tesis.

BAB II TINJAUAN PUSTAKA

Bab ini memaparkan landasan teori dan studi literatur yang menjadi basis ilmiah penelitian. Pembahasan mencakup arsitektur protokol IPv6 dan kerentanannya (ICMPv6 dan *Neighbor Discovery Protocol*), taksonomi serangan DDoS serta analisis komparatif framework forensik digital. Pada bab ini juga diuraikan justifikasi pemilihan framework D4I (*Digital Forensic Framework for Reviewing and Investigating Cyber Attack*) sebagai kerangka kerja utama penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan kerangka operasional dan tahapan penelitian secara rinci. Uraian dimulai dari perancangan skenario serangan (*Volumetric* dan *Protocol Attacks*), desain topologi simulasi, hingga formulasi model integrasi metode *Live Forensics* ke dalam siklus D4I. Bab ini juga menetapkan definisi operasional terkait parameter evaluasi efektivitas investigasi.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil implementasi dan analisis mendalam terhadap artefak serangan yang ditemukan. Pembahasan difokuskan pada rekonstruksi kausalitas serangan menggunakan *Cyber Kill Chain* (CKC) dan visualisasi *Chain of Artifacts* (CoA), analisis perbedaan dampak pada infrastruktur router dan server serta evaluasi efektivitas metode usulan berdasarkan indikator kelengkapan rekonstruksi, validitas atribusi, dan komprehensivitas laporan (5W1H).

BAB V PENUTUP

Bab ini memuat kesimpulan akhir yang merupakan sintesis jawaban atas rumusan masalah, serta implikasi teoretis dari temuan penelitian. Bagian ini diakhiri dengan saran konstruktif untuk pengembangan penelitian selanjutnya di bidang forensik jaringan masa depan.

BAB 2

Tinjauan Pustaka

2.1 Landasan Teori

2.1.1 Forensika Digital dan *Network Forensics*

Digital forensics atau forensika digital merupakan disiplin ilmu yang berfokus pada identifikasi, pengumpulan, analisis dan pelestarian bukti digital dalam rangka penyelidikan kriminal atau insiden keamanan siber (Agarwal et al., 2011). Dalam era dimana kejahatan melibatkan bukti digital dan serangan siber serta melibatkan berbagai teknologi, forensika digital memiliki peran penting dalam mengungkap bukti-bukti yang tersembunyi yang digunakan oleh penyerang. Menurut penelitian (Nicolls et al., 2016), penggunaan forensika digital dalam konteks jaringan IPv6 menjadi aspek penting karena kompleksitas dan skala ruang alamat yang besar yang sering dimanfaatkan oleh penyerang untuk menyembunyikan jejak mereka dan memperluas serangan mereka di seluruh jaringan. Menurut (Kent et al., 2006), *National Institute of Standard and Technology* (NIST) mendefinisikan proses forensika digital dalam beberapa fase / langkah seperti terdapat pada gambar 2.1 berikut.



Gambar 2.1. Fase dalam forensika digital, sumber (Kent et al., 2006)

- a. *Collection* / Pengumpulan : bertujuan untuk mengidentifikasi sumber-sumber data potensial yang relevan dengan insiden tersebut dan kemudian memberi label dan mencatatnya. Setelah itu, data yang ada di sumber-sumber tersebut harus diperoleh dengan tetap menjaga integritas sumber.
- b. *Examination* / Pemeriksaan : proses penilaian data yang diperoleh dari fase Pengumpulan dan mengekstraksi data yang relevan dengan insiden dengan tetap menjaga integritasnya.
- c. *Analysis* / Analisa : pengelolaan informasi yang diekstraksi oleh pemeriksa untuk menjawab pertanyaan 5WH atau menentukan bahwa tidak ada atau sebagian kesimpulan yang dapat diambil.
- d. *Reporting* / Pelaporan : proses pembuatan laporan dan mempresentasikan prosedur, metode dan alat yang digunakan dalam investigasi serta hasil dari tahap analisa.

Dalam perkembangannya, forensika digital terbagi menjadi beberapa sub-disiplin, salah satunya adalah *Network Forensics*. Menurut Palmer (2001), *Network Forensics* berfokus pada pemantauan dan analisis lalu lintas jaringan komputer baik lokal maupun internet (WAN) untuk mengumpulkan bukti, mendeteksi intrusi / gangguan atau pembuktian pelanggaran keamanan. Berbeda dengan forensik tradisional yang berfokus pada data statis (*data at rest*), *Network Forensics* berhubungan dengan data yang dinamis dan bergerak (*data in motion*) yang memiliki volatilitas tinggi (Pilli et al., 2010; Casey, 2011).

Network Forensics berperan penting dalam pengungkapan dan investigasi serangan *Distributed Denial of Service* (DDoS), khususnya dalam konteks jaringan yang kompleks seperti IPv6. Peran utama *Network Forensics* yaitu mengidentifikasi sumber serangan, memahami pola lalu lintas yang mencurigakan dan mengumpulkan bukti yang dapat digunakan untuk menelusuri dan menghentikan serangan. Sebagaimana diuraikan oleh (S. Singh & Singh, 2023) forensika digital memungkinkan peneliti untuk menganalisis log jaringan, paket-paket yang ditangkap, dan data lainnya untuk mengidentifikasi alamat IP penyerang, metode yang digunakan, serta waktu dan durasi serangan. Penelitian (Caviglione et al., 2022) juga menekankan bahwa dalam lingkungan IPv6, di mana teknik penyamaran seperti spoofing IP dan penggunaan jaringan botnet semakin umum, forensika digital harus lebih adaptif dan canggih untuk mengungkap jejak digital penyerang. Selain itu, penelitian (Nicolls et al., 2016) menunjukkan bahwa forensika digital yang dilakukan secara menyeluruh dan tepat waktu sangat penting untuk memastikan bahwa bukti yang dikumpulkan dapat mendukung upaya mitigasi dan tindakan hukum terhadap pelaku serangan DDoS.

2.1.2 Internet Protokol versi 6 (IPv6)

IPv6 atau *Internet Protocol version 6* adalah versi terbaru dari protokol internet yang dirancang untuk menggantikan IPv4 yang telah digunakan sejak awal pengembangan internet dan saat ini telah kehabisan *resource* (Huston, 2022). IPv6 diciptakan untuk mengatasi keterbatasan ruang alamat pada IPv4 dengan menyediakan ruang alamat yang jauh lebih besar yaitu 128 bit dibandingkan dengan 32 bit pada IPv4 yang memungkinkan hingga 340 undecillion alamat (Kasunic, 2022). Struktur header IPv6 juga mengalami perubahan untuk meningkatkan efisiensi dan fleksibilitas dalam perutean. Header IPv6 lebih sederhana dibandingkan dengan IPv4, namun dilengkapi dengan opsi *Extension Headers* yang dapat digunakan untuk menambahkan informasi seperti autentikasi, enkripsi dan fragmentasi paket (Kasunic, 2022). Salah satu komponen penting dalam IPv6 adalah *Internet*

Control Message Protocol version 6 (ICMPv6). protokol ICMPv6 memiliki fungsi vital dalam manajemen jaringan seperti mekanisme resolusi alamat IPv6 melalui *Neighbor Discovery Protocol* (NDP) yang diatur dalam RFC 4861. NDP menggantikan fungsi ARP pada IPv4 dengan menggunakan pesan *Neighbor Solicitation* (NS) dan *Neighbor Advertisement* (NA) untuk memetakan alamat IP ke alamat MAC (Narten et al., 2007). Namun, mekanisme NDP memiliki kerentanan inheren karena kurangnya autentikasi bawaan pada pesan tersebut. Kerentanan ini memungkinkan penyerang untuk melakukan *spoofing* atau pemalsuan pesan *Neighbor Advertisement* yang dapat memanipulasi tabel *neighbor cache* target. Eksploitasi terhadap celah ini dapat menyebabkan kondisi *Denial of Service* (DoS) pada target tanpa memerlukan volume lalu lintas yang besar karena target akan kehabisan sumber daya untuk memproses pembaruan *cache* palsu tersebut (Naagas & Gamilla, 2022).

2.1.3 Live Forensics dan Order of Volatility

Metode akuisisi data dalam forensik digital dikategorikan menjadi *Dead Forensics* dan *Live Forensics*. *Live Forensics* adalah teknik investigasi yang dilakukan pada sistem yang masih berjalan (*running state*) untuk merespons insiden secara *real-time*. Metode ini menjadi krusial dalam penanganan insiden seperti DDoS, karena mematikan sistem (*shutdown*) akan menghilangkan seluruh data yang tersimpan dalam memori volatil, seperti koneksi jaringan aktif dan proses yang berjalan di RAM (Alim et al., 2018).

Penerapan Live Forensics harus mematuhi prinsip *Order of Volatility* (OoV) sebagaimana dijelaskan dalam dokumen standar RFC 3227. Prinsip ini menegaskan bahwa pengumpulan bukti harus memprioritaskan data yang paling mudah hilang. Urutan volatilitas dari yang tertinggi ke terendah adalah:

1. Register dan cache prosesor.
2. Tabel routing, tabel ARP/NDP, tabel proses, kernel statistik, dan memori (RAM).
3. Data sistem sementara (*temporary file systems*).
4. Disk atau media penyimpanan data.
5. Log sistem dan konfigurasi topologi fisik (Brezinski & Killalea, 2002).

Dalam penelitian ini, kepatuhan terhadap RFC 3227 sangat esensial karena artefak kunci serangan DDoS seperti lonjakan penggunaan CPU dan manipulasi tabel *Neighbor Discovery Protocol* (NDP) berada pada lapisan memori (RAM) dan status jaringan yang akan hilang seketika jika sistem di-restart.

2.1.4 Serangan *Distributed Denial of Service* (DDoS)

Distributed Denial of Service (DDoS) adalah jenis serangan siber yang bertujuan untuk melumpuhkan suatu sistem, jaringan, atau layanan dengan cara membanjiri target dengan lalu lintas internet yang besar hingga sistem tersebut tidak mampu menangani beban dan akhirnya menjadi tidak dapat diakses / lumpuh (Suharti et al., 2022). Serangan DDoS menggunakan berbagai teknik, seperti pengiriman paket data yang besar secara terus-menerus, serangan volumetrik yang menghabiskan *bandwidth* serta serangan pada lapisan aplikasi yang bertujuan untuk menghabiskan sumber daya *server* (Sood & Llm, 2020). Serangan ini sering dilakukan melalui jaringan *botnet* yang terdiri dari ribuan hingga jutaan perangkat yang terinfeksi *malware* dan dikendalikan oleh penyerang untuk melakukan serangan secara bersamaan. Menurut penelitian oleh (Elejla et al., 2022b), serangan DDoS dapat dibagi menjadi beberapa kategori utama, yakni serangan volumetrik, serangan pada layer aplikasi, dan serangan berbasis protokol. Masing-masing jenis serangan memiliki karakteristik unik dan memerlukan pendekatan mitigasi yang berbeda.

Serangan DDoS tidak hanya menyebabkan gangguan layanan, tetapi juga dapat berdampak signifikan pada keamanan dan keandalan jaringan serta sistem TI. Kerentanan terhadap serangan DDoS sering kali disebabkan oleh infrastruktur yang tidak memiliki prosedur atau mekanisme pertahanan yang memadai untuk menangani lonjakan lalu lintas yang tiba-tiba. Sebagai contoh, penelitian oleh (Zhang et al., 2020) menunjukkan bahwa serangan DDoS dapat menyebabkan penurunan performa jaringan secara drastis, membuat organisasi kehilangan reputasi, hilangnya pendapatan dan kepercayaan dari pelanggan. Selain itu, serangan DDoS juga dapat digunakan sebagai pengalih perhatian sementara penyerang melancarkan serangan lain yang lebih berbahaya, seperti pencurian data atau infiltrasi jaringan. (Hui et al., 2011; Sood & Llm, 2020; Zhang et al., 2020) juga menekankan bahwa infrastruktur jaringan IPv6 menghadapi tantangan tambahan, karena protokol baru ini memiliki vektor serangan baru yang belum sepenuhnya dipahami oleh banyak organisasi.

2.1.5 Framework *Digital Forensic Framework for Reviewing and Investigating Cyber Attack* (D4I)

Digital Forensic Framework for Reviewing and Investigating Cyber Attack (D4I) adalah framework yang diusulkan oleh (Dimitriadis et al., 2020a) untuk melengkapi proses forensik yang dirancang untuk memperkuat proses investigasi serangan siber, terutama pada tahapan pemeriksaan (*Examination*) dan analisis. D4I bertujuan untuk memberikan panduan yang lebih rinci dan sistematis kepada para ahli forensik digital dalam melakukan penyelidikan

terhadap serangan siber. Framework ini tidak menggantikan proses forensik yang ada, tetapi melengkapinya dengan langkah-langkah yang lebih spesifik untuk mengatasi kelemahan dalam investigasi tradisional yang sering kali kurang detail dalam dua tahapan tersebut. Framework ini juga dirancang agar bersifat *Attack-Agnostic* yang berarti dapat digunakan untuk menyelidiki berbagai jenis serangan, termasuk serangan dengan teknik yang belum pernah terlihat sebelumnya (seperti serangan *zero-day*). D4I dapat diterapkan di berbagai lingkungan yang membuatnya fleksibel dalam berbagai konteks infrastruktur jaringan. terdapat dua pilar dalam framework D4I sebagai berikut.

a. Kategorisasi Artefak Digital

Aktifitas pertama dalam framework D4I yakni mengkategorikan artefak-artefak digital yang ditemukan selama penyelidikan ke dalam langkah-langkah yang sesuai dalam *Cyber-Kill-Chain* (CKC) (Hakim et al., 2023). Dengan cara ini, setiap jejak digital atau artefak yang ditinggalkan oleh serangan dapat dengan cepat diidentifikasi dan dihubungkan dengan fase tertentu dari serangan. *Cyber-Kill-Chain* (CKC) merupakan sebuah model yang digunakan untuk mendeskripsikan langkah-langkah yang diambil oleh penyerang selama serangan siber yang terdiri dari tujuh fase yakni :

- 1) *Reconnaissance* (Pengintaian)
- 2) *Weaponization* (Persenjataan)
- 3) *Delivery* (Pengiriman)
- 4) *Exploitation* (Eksploitasi)
- 5) *Installation* (Instalasi)
- 6) *Command and Control* (C2)
- 7) *Actions on Objective*

b. Langkah pemeriksaan (*Examination*) dan analisa (*Analysis*)

Menurut (Nurdin & Ramadhani, 2024) definisi pemeriksaan (*Examination*) dan analisa (*Analysis*) yakni serangkaian instruksi untuk melakukan pemeriksaan dan analisis secara mendalam. Langkah ini mempermudah proses identifikasi artefak yang relevan, menemukan korelasi antar artefak, serta menyusun urutan kejadian serangan. Pendekatan ini memungkinkan investigator untuk membangun *Chain of Artifacts* (CoA) yang merupakan rangkaian bukti yang saling terkait dan dapat memberikan pemahaman lebih jelas tentang modus operandi serangan. Langkah-langkah utama dalam proses pemeriksaan dan analisis ini adalah sebagai berikut:

- 1) Pemilihan Fase CKC
- 2) Identifikasi Artefak
- 3) Korelasi Artefak
- 4) Membangun *Chain of Artifacts* (CoA)
- 5) Ulangi Proses untuk Semua Fase CKC
- 6) Analisis *Chain of Artifacts* (CoA)

Metode langkah-demi-langkah ini memastikan bahwa investigasi forensik dilakukan secara sistematis dan terstruktur, sehingga investigator dapat menghubungkan artefak dan menyusun alur serangan.

2.1.6 Analisis dan Rasionalisasi Pemilihan Framework D4I

Dalam menentukan kerangka kerja investigasi yang paling sesuai untuk kasus serangan DDoS pada jaringan IPv6, penelitian ini melakukan studi analisis komparatif terhadap beberapa standar framework forensik yang umum digunakan, yaitu SRDFIM, GPMNF, CFFTPM dan D4I. Pemilihan framework yang tepat sangat penting karena karakteristik serangan DDoS IPv6 yang melibatkan banyak tahapan (*multi-stage*) dan membutuhkan rekonstruksi kausalitas yang kuat. Tabel 2.1 berikut menyajikan perbandingan kapabilitas antara framework tradisional dengan framework D4I berdasarkan literatur terkini.

Tabel 2.1. Perbandingan Kapabilitas Framework Forensik

Fitur / Karakteristik	SRDFIM (Agarwal et al., 2011)	GPMNF (Pilli et al., 2010)	CFFTPM (Rogers et al., 2006)	D4I (Dimitriadis et al., 2020)
Kepanjangan	<i>Systematic Digital Forensic Investigation Model</i>	<i>Generic Process Model for Network Forensics</i>	<i>Cyber Forensic Field Triage Process Model</i>	<i>Digital Forensic Framework for Reviewing & Investigating Cyber Attack</i>
Fokus Utama	Process-Centric. Menstandarisasi tahapan investigasi agar sistematis dan konsisten.	Process-Centric. Fokus pada tahapan penanganan bukti spesifik jaringan (log, trafik).	Process-Centric. Fokus pada pemeriksaan di lapangan (<i>on-site</i>) untuk	Attack-Centric. Fokus pada pemetaan perilaku penyerang dan rekonstruksi alur serangan.

			mendapatkan petunjuk awal.	
Model Dasar	Siklus 11 Fase (Preparation s.d. Review)	Siklus 9 Fase (Preparation s.d. Incident Response)	6 Fase Triage (Planning, Triage, User Profile, etc.)	Integrasi <i>Cyber Kill Chain</i> (7 Fase) + <i>Chain of Artifacts</i> .
Kelebihan	Sangat komprehensif untuk prosedur hukum dan standarisasi kerja tim.	Spesifik untuk menangani volume data jaringan yang besar.	Sangat cepat untuk identifikasi awal (<i>time-critical</i>).	Mampu memvisualisasikan hubungan sebab-akibat (<i>Causality</i>).
Keterbatasan pada Kasus DDoS IPv6	Pendekatan terlalu linear/kaku, sulit memetakan serangan multi-tahap yang kompleks.	Fokus pada <i>koleksi</i> data jaringan, kurang dalam <i>rekonstruksi</i> motif/perilaku serangan.	Kedalaman analisis terbatas (hanya triage), tidak cukup untuk pembuktian <i>root cause</i> .	Membutuhkan pemahaman mendalam tentang pola serangan (<i>Threat Intelligence</i>).
Kesesuaian dengan IPv6 DDoS	Rendah. Tidak spesifik menangani volatilitas protokol.	Sedang. Bisa menangkap trafik, tapi lemah di korelasi dampak.	Rendah. Serangan IPv6 butuh analisis memori mendalam, bukan sekadar triage cepat.	Tinggi. Fitur <i>Chain of Artifacts</i> (CoA) krusial untuk menghubungkan anomali protokol dengan dampak sistem.

Berdasarkan perbandingan di atas, framework lain seperti SRDFIM, GPMNF dan CFFTPM dikategorikan sebagai model *Process-Centric*. Kelebihan model ini adalah pada kepatuhan prosedur hukum (*Chain of Custody*), namun memiliki keterbatasan dalam memandu investigator untuk menghubungkan serpihan bukti yang terpisah menjadi satu skenario serangan yang utuh (*reconstruction*).

Pemilihan framework D4I (*Digital Forensic Framework for Reviewing and Investigating Cyber Attack*) dalam penelitian ini didasarkan pada kebutuhan spesifik untuk menangani kompleksitas serangan siber modern yang tidak dapat diakomodasi oleh

framework forensik yang berbasis *Process-Centric* seperti SRDFIM, GPMNF dan CFFTPM. Terdapat dua alasan mengapa D4I menjadi pendekatan yang paling relevan untuk investigasi serangan DDoS pada jaringan IPv6:

1. **Pergeseran Paradigma dari *Process-Centric* ke *Attack-Centric*:** Sebagaimana dijelaskan oleh Dimitriadis et al. (2020), framework seperti SRDFIM, GPMNF dan CFFTPM bersifat *Process-Centric*, yang menitik beratkan pada standarisasi prosedur penanganan bukti (*collection, examination, analysis*) untuk keperluan hukum. Pendekatan ini cenderung linear dan parsial, sehingga seringkali gagal merekonstruksi serangan multi-tahap (*multi-stage attacks*) seperti DDoS. Sebaliknya, D4I dirancang dengan pendekatan *Attack-Centric* yang mengintegrasikan konsep *Cyber Kill Chain*. Hal ini memungkinkan investigator untuk memetakan perilaku penyerang di setiap fase mulai dari *Reconnaissance* hingga *Action on Objectives* sehingga fokus investigasi tidak hanya pada pencarian bukti, melainkan juga bagaimana alur serangannya.
2. **Urgensi *Chain of Artifacts* (CoA) dalam Lingkungan Volatil:** Tantangan utama forensik IPv6 adalah volatilitas bukti (seperti *Neighbor Cache* pada serangan NDP Flood) yang tidak memiliki persistensi log jangka panjang. Framework konvensional seringkali menciptakan gap informasi karena memperlakukan bukti secara terisolasi. D4I mengatasi kelemahan ini melalui fitur Chain of Artifacts (CoA), yang menyatakan adanya korelasi kausalitas antar bukti digital yang berbeda (misalnya: menghubungkan lonjakan penggunaan RAM server dengan paket ICMPv6 spesifik di jaringan). Tanpa mekanisme CoA yang dimiliki D4I, rekonstruksi serangan yang utuh pada protokol stateless seperti IPv6 sulit dicapai secara valid.

2.2 Penelitian Terdahulu

Berikut merupakan review penelitian terdahulu yang berkaitan dengan serangan DDoS pada jaringan IPv6, *Live Forensics* pada jaringan IPv6 dan framework *Digital Forensic Framework for Reviewing and Investigating Cyber Attack* (D4I) yang disajikan pada Tabel 2.2 berikut.

Tabel 2.2. Ulasan Penelitian Terdahulu

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
1	Traffic Forensic for IPv6-Based Wireless Sensor Network and the Internet of Think (Kumar et al., 2016)	Penelitian ini bertujuan membuat <i>framework</i> untuk menganalisis lalu lintas jaringan IPv6 secara <i>real-time</i> dan mengidentifikasi pola serangan yang berpotensi, seperti serangan DDoS pada jaringan <i>wireless</i> dengan menggunakan teknik deteksi berbasis entropy dan metode forensik lainnya.	1. Teknik <i>network forensic</i> yang dikembangkan untuk jaringan <i>wireless</i> berbasis IPv6 dan lingkungan Internet of Things mampu mengidentifikasi pola serangan DDoS dengan efektif. 2. Metode deteksi berbasis entropy yang digunakan dalam analisis real-time lalu lintas jaringan, memberikan hasil yang akurat dalam mengidentifikasi anomali yang menunjukkan adanya serangan.	1. Penelitian ini hanya terbatas pada jaringan <i>wireless</i> berbasis IPv6. 2. Pendekatan deteksi yang diusulkan tidak cukup adaptif untuk menangani berbagai jenis serangan DDoS yang lebih kompleks. 3. Validasi dan pengujian <i>framework</i> yang diusulkan mungkin juga dibatasi oleh skenario simulasi yang digunakan dan mungkin tidak sepenuhnya mewakili kondisi jaringan dunia nyata.
2	Feature Selection for Detecting ICMPv6-Based	Tujuan penelitian dalam paper ini adalah untuk mengembangkan	Hasil penelitian menunjukkan bahwa metode yang diusulkan,	1. pendekatan ini bergantung pada algoritma <i>Binary Flower</i>

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
	DDoS Attacks Using Binary Flower Pollination Algorithm (Hasan Bdair Aighuraibawi et al., 2023)	metode deteksi serangan DDoS berbasis ICMPv6 dengan menggunakan algoritma Binary Flower Pollination (BFPA). BFPA digunakan untuk memilih parameter deteksi yang paling relevan. Untuk meningkatkan akurasi deteksi serangan pada jaringan IPv6 dengan mengurangi jumlah fitur yang tidak penting, sehingga sistem deteksi bisa bekerja lebih efisien dan efektif.	yaitu <i>Binary Flower Pollination Algorithm</i> (BFPA), berhasil meningkatkan akurasi deteksi serangan DDoS berbasis ICMPv6. Prosentase keberhasilan deteksi mencapai 97,95% dengan menggunakan 9 fitur terpilih, dibandingkan dengan akurasi 96,71% ketika menggunakan semua 19 fitur. Dengan demikian, BFPA tidak hanya meningkatkan akurasi deteksi tetapi juga mengurangi jumlah fitur yang dibutuhkan, sehingga meningkatkan efisiensi sistem deteksi.	<i>Pollination</i> (BFPA) yang memiliki keterbatasan dalam hal pemilihan fitur optimal dalam skenario yang lebih kompleks atau dengan dataset yang lebih beragam. 2. bahwa metode yang diusulkan telah diuji dalam lingkungan simulasi dan belum divalidasi sepenuhnya dalam pengaturan dunia nyata, yang berarti efektivitasnya dalam skenario yang lebih beragam masih perlu dieksplorasi lebih lanjut
3	Attacking and Online Forensic in IPv6 Network (Göbel & Göbel, 2008)	Tujuan dari penelitian ini adalah untuk menguji sistem keamanan dalam jaringan IPv6 dengan membuat simulasi penyerangan	Hasil pengujian pada paper ini menunjukkan kesuksesan dalam penyerangan dengan dua jenis skenario, yakni serangan DDoS	1. <i>Framework</i> 6Foren telah membantu mengatasi banyak tantangan, namun uji coba

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
		ATS_ICMP_6 pada jaringan IPv6 menggunakan ICMP6 Message serta melakukan forensika jaringan online menggunakan 6Foren framework untuk menemukan artefak serangan berupa jenis packet, rekonstruksi serangan dan jenis message yang dikirim penyerang.	menggunakan paket ICMP6 error message dan ICMPv6 Destination Unreacheble attack pada jaringan berbasis IPv6. Selanjutnya penulis juga berhasil melakukan online forensic menggunakan 6Foren untuk mendeteksi kegagalan system dan artefak serangan pada beberapa protocol seperti HTTP,FTP,SMTP dan POP3.	tetap terbatas pada sejumlah dataset tertentu. 2. Kompleksitas algoritma yang dikembangkan tetap menjadi tantangan, terutama dalam lingkungan dengan sumber daya komputasi terbatas. 3. Belum adanya pengujian pada protocol yang terlindungi seperti HTTPS,SSL dan Secure POP3
4	Computer Forensics Field Triage Process Model (CFFTPM) (Rogers et al., 2006)	Tujuan dari penelitian ini adalah mengusulkan framework forensik digital dengan fokus pada investigasi di tempat yang sensitif terhadap waktu. Berbeda dengan metode forensik tradisional yang sering kali melibatkan penyitaan	Hasil dari penelitian ini menunjukkan bahwa Computer Forensics Field Triage Process Model (CFFTPM) telah terbukti sangat efektif dalam berbagai kasus di dunia nyata, terutama dalam situasi yang memerlukan	1. Model CFFTPM tidak selalu dapat digunakan dalam semua situasi investigasi. Model ini dirancang untuk digunakan dalam kasus yang mendesak, di mana waktu adalah faktor yang sangat kritis.

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
		sistem dan menganalisisnya di laboratorium kemudian, CFFTPM memungkinkan identifikasi, analisis, dan interpretasi bukti secara langsung di lokasi kejadian.	informasi investigatif secara cepat. Model ini mampu menyediakan bukti yang dapat digunakan secara langsung di tempat kejadian untuk mendukung penyelidikan, wawancara dengan tersangka, dan pengambilan keputusan yang kritis dalam waktu singkat.	2. Adanya keterbatasan secara legal dan teknis dalam penerapan framework ini seperti adanya surat perintah, ketersediaan alat forensik dan lingkungan teknologi yang kompleks. 3. Adanya potensi bahwa pengujian di lapangan tidak seteliti pengujian di laboratorium, yang mempengaruhi penerimaan bukti di pengadilan.
5	Systematic Digital Forensic Investigation Model (SRDFIM) (Agarwal et al., 2011)	Tujuan dari penelitian ini adalah mengembangkan Systematic Digital Forensic Investigation Model (SRDFIM) yang bertujuan memberikan kerangka kerja yang konsisten, standar, dan sistematis dalam proses investigasi forensik digital. Penelitian ini dimaksudkan	Hasil dari penelitian ini menunjukkan bahwa Systematic Digital Forensic Investigation Model (SRDFIM) yang dikembangkan berhasil memberikan kerangka kerja yang lebih terstruktur dan sistematis untuk proses investigasi forensik	1. SRDFIM masih memerlukan pengujian lebih lanjut dalam berbagai skenario investigasi forensik digital. 2. Framework ini memerlukan adaptasi seiring dengan kemajuan teknologi yang terus berubah, sehingga perlu

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
		untuk mengatasi beberapa kelemahan dari metodologi yang ada sebelumnya dan menyediakan solusi yang lebih terstruktur dalam investigasi kejahatan digital.	digital. Model ini membantu mengatasi beberapa kekurangan dalam metodologi sebelumnya dan memperkenalkan tahapan-tahapan investigasi yang lebih rinci, mulai dari persiapan hingga analisis dan presentasi bukti.	diperbarui untuk menghadapi tantangan baru seperti volume data yang besar, virtualisasi, dan enkripsi. 3. Keterampilan investigator yang diperlukan untuk menerapkan model ini secara efektif juga menjadi batasan, karena penerapan yang berhasil sangat bergantung pada kemampuan investigator dalam menggunakan alat forensik yang tepat dan mematuhi prosedur yang ketat
6	Integrated digital forensic process model (IDFPM) (Kohn et al., 2013)	Tujuan dari penelitian ini adalah mengusulkan sebuah framework standar yang dapat digunakan oleh penyelidik dalam investigasi forensik digital secara konsisten dan terstruktur. Model ini dirancang untuk mengatasi kurangnya	Hasil penelitian ini menunjukkan bahwa model IDFPM yang diusulkan berhasil memfasilitasi penyelidik dengan pendekatan yang lebih sistematis dan seragam dalam menangani bukti digital dalam 4 fase yakni	Batasan dari model IDFPM adalah tantangan dalam mengadaptasi model ini terhadap teknologi yang terus berkembang, seperti komunikasi terenkripsi dan lingkungan virtual yang berskala besar. Model ini membutuhkan

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
		keseragaman dalam metode forensik digital yang ada serta menyediakan pendekatan yang dapat diterima secara universal oleh komunitas forensik. Dengan adanya model ini diharapkan proses investigasi forensik dan bukti yang dikumpulkan dapat digunakan dalam persidangan hukum tanpa adanya kesulitan terkait prosedur atau terminologi yang berbeda-beda	<i>Preparation, Incident Handling, Digital Forensic Investigation</i> dan <i>Presentation</i> . Model ini memastikan bahwa proses investigasi dilakukan secara benar, dan bukti yang dikumpulkan dapat diterima di pengadilan, meningkatkan kredibilitas dan akurasi hasil investigasi.	pembaruan secara berkala untuk bisa menyesuaikan dengan perubahan teknologi tersebut agar tetap relevan dan efektif dalam menangani kejahatan siber yang semakin kompleks
7	D4I - Digital forensics framework for reviewing and investigating cyber attacks (Dimitriadis et al., 2020b)	Tujuan dari penelitian ini adalah mengembangkan kerangka kerja D4I yang dirancang untuk meningkatkan proses investigasi forensik siber, khususnya pada fase pemeriksaan dan analisis. Kerangka kerja ini bertujuan untuk melengkapi proses forensik digital yang sudah ada, bukan	Hasil dari penelitian ini menunjukkan bahwa kerangka kerja D4I dapat meningkatkan efisiensi dan akurasi dalam investigasi forensik siber. D4I memungkinkan penyelidik untuk mengkategorikan artefak digital ke dalam fase-fase Cyber-Kill-Chain (CKC), dan membantu	1. Penggunaan semi-otomatisasi dalam analisis artefak masih memerlukan keterampilan dan pengalaman dari penyelidik forensik untuk melakukan korelasi yang tepat antara artefak dan fase serangan. 2. Penerapan D4I pada kasus nyata menghadapi tantangan

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
		menggantikannya, dengan menyediakan metode langkah demi langkah yang lebih rinci dan semi-otomatis untuk mengidentifikasi artefak serangan dan melakukan korelasi di antara fase-fase serangan yang didefinisikan dalam <i>Cyber-Kill-Chain</i> (CKC)	memetakan pola serangan secara lebih jelas dan terstruktur. Secara keseluruhan, D4I mampu memperkuat proses investigasi dengan meminimalkan kesalahan analisis dan meningkatkan konsistensi penyelidikan	terkait kompleksitas infrastruktur jaringan yang berbeda-beda, serta kesulitan dalam mengadaptasi kerangka ini terhadap serangan yang lebih kompleks atau berlapis. 3. D4I masih memerlukan pengujian lebih lanjut untuk kasus-kasus serangan dengan skala besar dan sistem yang lebih heterogen
8	Investigasi Forensika Digital WhatsApp Scam Dengan Menggunakan Framework D4I (Nurdin & Ramadhani, 2024)	Penelitian ini bertujuan untuk melakukan investigasi forensik digital pada kasus penipuan melalui aplikasi WhatsApp menggunakan framework D4I. Fokus utama penelitian adalah pada tahap pemeriksaan dan analisis dengan memanfaatkan kerangka D4I yang diharapkan dapat meningkatkan efektivitas dalam mengidentifikasi,	Hasil penelitian menunjukkan bahwa penerapan framework D4I efektif dalam mengidentifikasi tahapan serangan sesuai dengan model Cyber Kill Chain (CKC). Investigasi dimulai dari tahap pengintaian (reconnaissance) hingga eksekusi akhir serangan (action on objective). Dalam kasus penipuan WhatsApp ini,	

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
		mengkategorikan, dan mengkorelasikan artefak-artefak digital dari penipuan yang terjadi. Penelitian ini mencontohkan modus penipuan yang menggunakan file ".apk" palsu seperti "undangan pernikahan.apk" untuk mencuri data pribadi korban, termasuk kode OTP (One-Time Password)	penyelidik mampu melacak jejak digital penipuan seperti instalasi aplikasi palsu, permintaan akses SMS, dan pengiriman data penting ke server penyerang melalui aplikasi bot Telegram. Analisis lebih lanjut juga menunjukkan bahwa penyerang menggunakan rekayasa sosial (social engineering).	
9	Forensic Model for DDoS Attack (Luo et al., 2020)	Penelitian ini bertujuan untuk mengembangkan teknik forensik yang efektif untuk mendeteksi dan menganalisis serangan Distributed Denial of Service (DDoS) berbasis botnet, terutama yang menggunakan protokol komunikasi Internet Relay Chat (IRC). Model ini dirancang untuk mengatasi tantangan dalam mengidentifikasi dan melacak sumber serangan DDoS di jaringan	1. Teknik ini berhasil meningkatkan tingkat pengenalan skala serangan hingga 93% dengan menggunakan kombinasi analisis vektor serangan botnet dan teknik penandaan paket terfragmentasi (Fragmented Packet Marking System/FMS).	1. Penerapan metode ini dalam jaringan nyata dengan skala yang lebih besar dan variasi topologi yang lebih kompleks masih perlu diuji lebih lanjut. Skalabilitas model ini dalam menangani volume data yang sangat besar dan jumlah node yang jauh lebih banyak tetap menjadi tantangan

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
		besar dan kompleks dengan menggunakan simulasi jaringan NS2 dan teknik penandaan paket yang terfragmentasi. fokus utama dari penelitian ini adalah untuk meningkatkan akurasi pengenalan skala serangan dan jalur serangan melalui teknik analisis berbasis vektor serangan dan penandaan paket.	2. Penggunaan NS2 yang mencakup lebih dari 2000 node jaringan dan berbagai skenario serangan DDoS, memungkinkan simulasi yang lebih realistis dan penilaian yang lebih akurat terhadap efektivitas model forensik dalam lingkungan jaringan yang terkontrol.	2. Model forensic ini berfokus pada deteksi botnet yang menggunakan IRC sebagai protokol komunikasi. Dengan semakin berkembangnya teknologi botnet yang ada, penyempurnaan metode forensic perlu dilakukan dari segi adaptasi dan perluasan metode yang digunakan.
10	Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard (Alim et al., 2018)	Tujuan penelitian ini adalah untuk mendeteksi, menganalisis, dan mengumpulkan bukti <i>digital</i> secara langsung / real-time dengan mengimplementasikan metode Live Forensics serangan Denial of Service (DoS) pada perangkat Routerboard ketika serangan DoS sedang berlangsung, tanpa harus menginterupsi sistem yang diserang.	1. Metode <i>Live Forensic</i> yang diusulkan berhasil mendeteksi serangan DoS pada Routerboard secara real-time. Penelitian menggunakan aplikasi Wireshark untuk memantau lalu lintas jaringan dan mendeteksi aktivitas mencurigakan yang berkaitan	1. Meskipun metode <i>Live Forensic</i> memberikan banyak manfaat, dalam implementasinya cukup kompleks dan memerlukan pengetahuan teknis yang mendalam tentang perangkat jaringan dan alat forensik. Hal ini bisa menjadi tantangan dalam situasi di

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
		Pendekatan ini dirancang untuk mengatasi tantangan dalam memperoleh bukti yang akurat dan lengkap selama serangan berlangsung, yang sering kali hilang atau tidak dapat diakses jika sistem dimatikan.	dengan serangan DoS, seperti peningkatan mendadak dalam lalu lintas DNS flooding. Hal ini memungkinkan analisis langsung dan pengambilan bukti <i>digital</i> selama serangan berlangsung, yang krusial untuk investigasi forensic. 2. Selama serangan DoS, penelitian ini juga menganalisis dampak serangan terhadap kinerja Routerboard, termasuk peningkatan beban CPU dan penggunaan memori yang signifikan. Temuan menunjukkan bahwa beban CPU meningkat hingga 99% dan penggunaan memori meningkat secara signifikan setelah serangan terjadi, yang	mana sumber daya atau keahlian terbatas. 2. Penggunaan metode <i>Live Forensic</i> berisiko terhadap kemungkinan modifikasi data selama proses pengumpulan bukti, karena sistem tetap berjalan selama serangan dan investigasi. Ini dapat mempengaruhi integritas data yang dikumpulkan dan menimbulkan tantangan dalam pembuktian di pengadilan. 3. Penelitian ini difokuskan pada perangkat Routerboard dan hasilnya mungkin tidak sepenuhnya dapat digeneralisasikan untuk semua jenis perangkat

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
			mengindikasikan bahwa serangan tersebut berdampak langsung pada kinerja jaringan. 3. Live forensik memungkinkan pengumpulan bukti <i>digital</i> penting seperti log aktivitas dan daftar alamat IP penyerang selama serangan terjadi.	jaringan atau skenario serangan yang berbeda
11	Router Forensic Analysis against Distributed Denial of Service (DDoS) Attacks (Prayogo & Riadi, 2020)	Penelitian ini bertujuan untuk melakukan analisis forensik pada serangan Distributed Denial of Service (DDoS) yang menargetkan perangkat router. Fokus utama dari penelitian ini adalah untuk mengembangkan pendekatan berbasis model <i>network forensic</i> untuk mendeteksi, menganalisis, dan mengumpulkan bukti <i>digital</i> yang berkaitan dengan serangan	1. Dengan menggunakan alat seperti Snort, Wireshark, Elasticsearch, Kibana, dan Logstash, penelitian ini berhasil mendeteksi dan mengumpulkan bukti <i>digital</i> terkait dengan serangan DDoS pada router. Penelitian ini menemukan bahwa serangan DDoS terjadi pada port 80 dengan total 126.286	1. Implementasi model <i>network forensic</i> yang digunakan dalam penelitian ini memerlukan konfigurasi yang kompleks serta memerlukan pemahaman mendalam tentang alat forensik yang digunakan. 2. Penelitian ini sangat bergantung pada penggunaan alat-alat tertentu seperti Snort,

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
		DDoS yang terjadi pada router. Penelitian ini menggunakan Model Proses <i>Generic Network Forensic</i> , yang mencakup tahapan mulai dari persiapan hingga presentasi hasil analisis, untuk memastikan bahwa bukti yang dikumpulkan dapat digunakan dalam konteks hukum.	paket serangan yang terdeteksi. 2. Tahapan forensik yang dilakukan mencakup deteksi, pengumpulan, pemeriksaan, analisis, investigasi, dan presentasi. Hasil analisis menunjukkan peningkatan lalu lintas jaringan yang signifikan selama serangan DDoS, yang mempengaruhi kinerja router secara drastis. 3. Metode <i>live forensics</i> yang digunakan memungkinkan pengumpulan bukti secara real-time tanpa harus mematikan sistem yang diserang. Ini sangat penting untuk menjaga integritas data dan memastikan bahwa bukti	Wireshark, dan Kibana. Keterbatasan dari alat-alat ini, seperti ketidakmampuan untuk mendeteksi semua jenis serangan atau keterbatasan dalam skala jaringan, dapat mempengaruhi hasil yang diperoleh. 3. Meskipun penelitian ini berhasil dalam mendeteksi dan menganalisis serangan DDoS pada router, hasilnya mungkin tidak sepenuhnya berlaku untuk semua jenis router atau skenario jaringan. Pengujian lebih lanjut diperlukan untuk memastikan bahwa metode ini dapat diadaptasi untuk berbagai jenis perangkat dan konfigurasi jaringan.

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
			tidak hilang atau rusak selama proses pengumpulan.	
12	Forensic-Aware Anti-DDoS Device (Tseung & Chow, 2018)	Penelitian ini bertujuan untuk mengembangkan dan mengevaluasi perangkat anti-DDoS yang juga memiliki kemampuan forensik, yang disebut Forensic-Aware Anti-DDoS Device. Perangkat ini dirancang untuk tidak hanya melindungi jaringan dari serangan DDoS, tetapi juga secara simultan menangkap dan menyimpan data lalu lintas jaringan untuk analisis forensik tanpa mengganggu kinerja jaringan. Tujuan utamanya adalah untuk menyediakan solusi yang proaktif dalam melacak dan menghentikan serangan DDoS sebelum serangan tersebut berkembang, sekaligus mengumpulkan bukti forensik yang	1. Perangkat ini menggunakan mekanisme <i>live packet capture</i> dengan fungsi penangkapan paket yang disediakan oleh sistem operasi Linux dan menggunakan teknologi Bloom filter yang disesuaikan untuk memfilter lalu lintas yang mencurigakan berdasarkan fitur yang diidentifikasi melalui algoritma machine learning. Pengujian menunjukkan bahwa perangkat ini mampu meng-capture data lalu lintas jaringan tanpa menyebabkan penurunan kinerja jaringan yang signifikan.	1. Meskipun perangkat ini efektif dalam lingkungan pengujian, implementasi di jaringan nyata dengan lalu lintas yang lebih tinggi mungkin memerlukan perangkat keras yang lebih canggih, seperti penggunaan RAID untuk menangani kecepatan lalu lintas yang lebih tinggi dari 1 Gbps. Latensi yang ditimbulkan oleh perangkat ini juga perlu diukur dan dievaluasi lebih lanjut. 2. Pengujian perangkat ini dilakukan terutama dalam kondisi laboratorium. Oleh karena itu, validasi lebih lanjut

No	Penelitian	Tujuan	Hasil	Batasan Penelitian
		dapat digunakan oleh lembaga penegak hukum.	2. Perangkat ini mengintegrasikan teknik anti-DDoS berbasis machine learning dengan mekanisme forensik yang memungkinkan pengumpulan data serangan secara real-time. Sistem ini melakukan learning dari lalu lintas jaringan yang masuk dan secara otomatis memperbarui konfigurasi. Pengujian menunjukkan bahwa pendekatan ini dapat mendeteksi dan memblokir paket serangan DDoS secara efektif sambil tetap mengumpulkan data forensik yang diperlukan.	diperlukan di lingkungan operasional nyata dengan variasi skenario serangan dan konfigurasi jaringan yang lebih luas untuk memastikan efektivitas dan keandalannya. 3. Efektivitas perangkat sangat bergantung pada akurasi algoritma pembelajaran mesin dalam mengekstraksi fitur yang relevan dari lalu lintas jaringan. Kesalahan dalam proses ini dapat menyebabkan false positives atau false negatives dalam deteksi serangan, yang memerlukan penyesuaian parameter dan algoritma yang lebih tepat untuk berbagai jenis serangan.

Berdasarkan tinjauan literatur di atas terdapat kesenjangan penelitian (*research gap*) yang signifikan:

1. Penelitian terdahulu tentang IPv6 (seperti Kumar et al. dan Bdair Alghuraibawi et al.) cenderung berfokus pada deteksi otomatis, namun kurang mendalam pada aspek rekonstruksi forensik.
2. Penelitian tentang *Live Forensics* DDoS (seperti Alim et al.) umumnya masih terpaku pada protokol IPv4 dan berhenti pada tahap pengumpulan data tanpa analisis lanjutan menggunakan framework terstruktur.
3. Framework D4I terbukti efektif untuk kasus aplikasi (seperti WhatsApp Scam), namun validitasnya dalam menangani serangan DDoS volumetrik dan protokol pada jaringan IPv6 belum teruji secara empiris.

Oleh karena itu, penelitian ini mengisi kesenjangan tersebut dengan mengintegrasikan metode *Live Forensics* (untuk akuisisi data volatil IPv6) dan framework D4I (untuk analisis terstruktur) guna merekonstruksi serangan DDoS IPv6 secara komprehensif.

2.3 Kerangka Konseptual (*Conceptual Framework*)

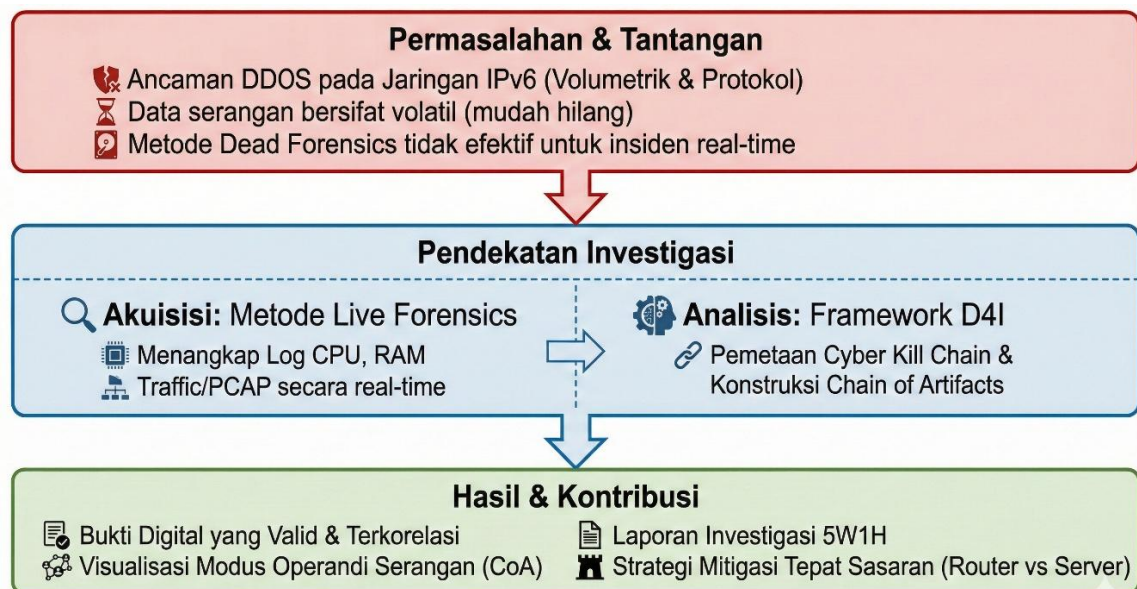
Kerangka konseptual dalam penelitian ini dibangun berdasarkan urgensi keamanan infrastruktur jaringan IPv6 yang menghadapi ancaman serangan *Distributed Denial of Service* (DDoS) yang semakin kompleks. Sebagaimana dijelaskan dalam tinjauan pustaka, migrasi masif ke IPv6 membuka permukaan serangan baru, khususnya serangan yang mengeksploitasi fitur protokol seperti *Neighbor Discovery Protocol* (NDP) dan ICMPv6.

Permasalahan mendasar yang diidentifikasi adalah ketidakefektifan metode *dead forensics* dalam menangani insiden serangan DDoS IPv6 yang sedang berlangsung (*on-going*). Pendekatan *dead forensics* yang berbasis pada analisis pasca-insiden (*post-mortem*) sering kali gagal menangkap bukti digital yang bersifat volatil seperti proses yang berjalan di memori (RAM), status koneksi jaringan aktif dan beban CPU secara *real-time*.

Untuk mengatasi kesenjangan tersebut, penelitian ini mengusulkan pendekatan integratif yang menggabungkan metode *Live Forensics* dengan framework D4I (*Digital Forensic Framework for Reviewing and Investigating Cyber Attack*). Logika penelitian ini dimulai dengan penerapan metode *Live Forensics* sebagai mekanisme akuisisi data. Metode ini memungkinkan investigator untuk "membekukan" dan mengamankan keadaan sistem saat serangan terjadi, memastikan bahwa artefak krusial seperti lonjakan trafik anomali dan manipulasi tabel *neighbor cache* dapat tersimpan dengan aman.

Selanjutnya, data mentah yang diperoleh dari proses *Live Forensics* tersebut tidak dapat memberikan makna investigatif jika tidak dianalisis secara terstruktur. Oleh karena itu, kerangka pemikiran ini menempatkan framework D4I sebagai mesin analisis utama. Melalui D4I, artefak-artefak yang terfragmentasi akan dipetakan ke dalam fase *Cyber Kill Chain* (CKC) untuk memahami tahapan serangan, mulai dari *Reconnaissance* hingga *Actions on Objectives*. Proses ini dilanjutkan dengan *konstruksi Chain of Artifacts* (CoA) untuk memvisualisasikan hubungan sebab-akibat (*causality*) antara vektor serangan dengan dampak kerusakan pada infrastruktur (Router) maupun endpoint (Server).

Hasil akhir dari kerangka pemikiran ini adalah tersusunnya laporan investigasi yang komprehensif yang mampu menjawab pertanyaan 5W1H (*What, Who, When, Where, Why, How*) serta memberikan rekomendasi mitigasi yang spesifik berdasarkan karakteristik serangan yang teridentifikasi. Alur kerangka pemikiran penelitian ini divisualisasikan pada Gambar 2.2.



Gambar 2.2. *Conceptual framework* penelitian

BAB 3

Metodologi

3.1 Langkah-langkah Penelitian

Berdasarkan pada latar belakang penelitian, penulis mengusulkan metode penelitian dengan merujuk pada *Digital forensics Research Workshop* (DFRWS) yang terdiri dari enam tahapan, yaitu identifikasi (*Identification*), persiapan (*Preservation*), Pengumpulan artefak (*Collection*), eksaminasi (*Examination*), analisa (*Analysis*), dan pelaporan (*Presentation*) (Pollitt, 2019). Metodologi ini akan menjelaskan alur penelitian dari awal hingga akhir. Langkah-langkah penelitian dibuat secara sistematis sehingga mudah dipahami dan bisa menjadi panduan yang jelas untuk menyelesaikan permasalahan terkait serangan DDoS. Langkah - langkah penelitian ini dijelaskan pada gambar 3.1 berikut.



Gambar 3.1. Tahapan Metodologi Penelitian, sumber : (Pollitt, 2019)

3.1.1 Studi Pustaka

Pada tahapan ini dilakukan studi pustaka dengan mengumpulkan referensi yang bersumber dari buku, jurnal dan artikel ilmiah. studi pustaka ini bertujuan untuk memahami perkembangan terkini terkait serangan DDoS pada IPv6, *Live Forensic* dan Framework *Digital Forensic Framework for Reviewing and Investigating Cyber Attack* (D4I) yang mencakup teori, metode dan temuan. Dengan menelaah literatur yang ada, peneliti dapat memperbarui pengetahuan, membangun dasar teori dan merumuskan konsep penelitian. Pada penelitian ini, peneliti menerapkan pendekatan *Systematic Literature Review* (SLR)

atau Tinjauan Literatur Sistematis untuk meneliti karakteristik serangan DDoS pada jaringan IPv6 serta mengevaluasi bagaimana *Live Forensics* dan framework D4I dapat diterapkan dengan tujuan untuk mengidentifikasi dan mengumpulkan bukti digital secara real-time selama serangan berlangsung serta menganalisis artefak serangan dengan menggunakan pendekatan *Cyber-Kill-Chain* (CKC) yang diharapkan dapat meningkatkan efisiensi investigasi, menjaga integritas bukti, dan menghasilkan strategi mitigasi yang efektif pada jaringan IPv6.

3.1.2 Persiapan dan Alat

Pada tahapan ini peneliti menyiapkan alat dan laboratorium simulasi yang dibutuhkan untuk melakukan simulasi serangan *Distributed Denial of Service* (DDoS) pada jaringan IPv6. lab tersebut berjalan dalam *server* VMware berisi Pnetlab sebagai aplikasi simulasi jaringan. Pada laboratorium simulasi tersebut melibatkan beberapa dengan keterangan seperti pada tabel 3.1 berikut.

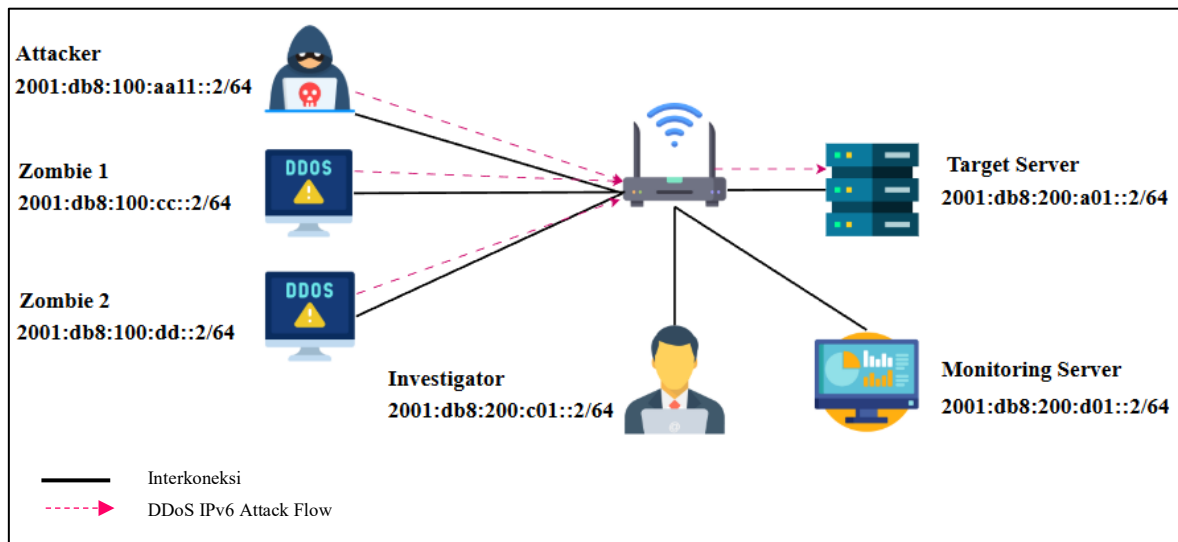
Tabel 3.1. Daftar Aktor, Sistem Operasi dan *Tools*

Aktor	Sistem Operasi	<i>Tools</i>
<i>Attacker</i> / Penyerang	Kali Linux 2024	THC-IPv6, nping, fping6
<i>Agen</i> / <i>Zombie</i>	Ubuntu Server 22.04	THC-IPv6, nping, fping6
<i>Router</i>	Mikrotik CHR versi 6.9.4	Winbox, Webfig
Komputer Investigator	Ubuntu Desktop 21.04	tftpd, Wireshark, winbox
Server Monitoring	Ubuntu <i>Server</i> 22.04	Zabbix
Server target	Ubuntu <i>Server</i> 22.04	Wireshark, Webmin

3.1.3 Simulasi Serangan

Tahapan ini bertujuan untuk mensimulasikan serangan *Distributed Denial of Service* (DDoS) pada jaringan IPv6. Skenario serangan DDoS yang akan dilaksanakan yakni memposisikan penyerang dan server target terkoneksi pada jaringan berbasis IPv6. Selanjutnya, komputer penyerang dan komputer *zombie* akan melakukan percobaan serangan DDoS dengan beberapa skenario dan dilakukan sebanyak empat kali percobaan untuk mengetahui polarisasi dan variasi serangan. Server monitoring akan digunakan untuk mengidentifikasi anomali pada trafik jaringan dan melihat pola serangan DDoS pada jaringan IPv6 yang terjadi. Komputer Investigator digunakan untuk mengidentifikasi

anomali pada trafik jaringan, melihat pola serangan DDoS pada jaringan IPv6 yang terjadi dan melakukan akuisisi dan analisa forensik. Detail topologi jaringan dalam simulasi serangan ini bisa dilihat pada gambar 3.2 berikut.



Gambar 3.2. Simulasi serangan DDoS IPv6

3.1.4 Monitoring Traffic

Tahapan monitoring *traffic* bertujuan untuk memantau aktivitas serangan dan melihat potensi artefak pada router dan server target. Monitoring pada router menggunakan *tools* winbox dan pada server target menggunakan *tools* wireshark. Sedangkan server monitoring akan menggunakan *tools* Zabbix untuk menganalisa data trafik jaringan yang terkumpul secara realtime baik sebelum maupun pada saat terjadi serangan DDoS. Tahapan monitoring ini bertujuan untuk mengamati dan menganalisis lalu lintas jaringan.

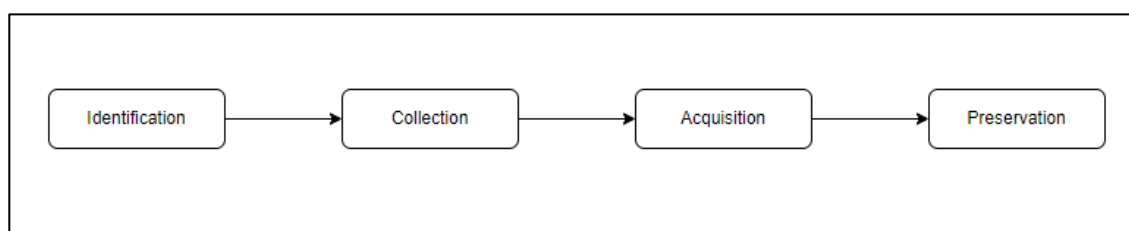
3.1.5 Akuisisi Data

Pada tahapan ini, peneliti melakukan akuisisi data-data serangan pada router utama dan server target dengan tujuan untuk mendapatkan log artefak serangan DDoS IPv6. Proses ini dilakukan dengan memeriksa beberapa parameter akuisisi. Penulis menggunakan beberapa parameter DDoS yang digunakan dalam deteksi berdasarkan penelitian yang dilakukan oleh (Haseeb-ur-rehman et al., 2023) seperti yang terlihat pada tabel 3.2 berikut.

Tabel 3.2. Paramater deteksi DDoS. (Sumber : Haseeb-ur-rehman et al., 2023)

No	Parameter	Potensi sumber artefak
1	<i>Source Address</i> atau sumber alamat penyerang.	• <i>Router</i> • <i>Server web</i>
2	<i>Destination Address</i> atau tujuan alamat penyerang.	• <i>Router</i> • <i>Server web</i>
3	<i>Package type</i> atau tipe paket serangan.	• <i>Router</i> • <i>Server web</i>
4	<i>Volume package</i> atau besaran paket.	• <i>Router</i>
5	<i>Traffic Rate</i> atau rata-rata lalu lintas jaringan.	• <i>Router</i>
7	<i>Timestamp</i> atau catatan waktu serangan.	• <i>Router</i> • <i>Server web</i>

Beberapa tools yang digunakan dalam tahapan akuisisi yakni mikrotik winbox untuk menangkap traffic flow dan wireshark, mpstat, vmstat dan tcpdump untuk mencatat log dan menganalisis pola serangan. Pada tahapan ini penulis menggunakan metode *Live Forensic* yang bertujuan untuk mengidentifikasi, koleksi, akuisisi dan preservasi artefak serangan secara realtime dan tanpa mengganggu operasional jaringan dengan tahapan seperti pada gambar 3.3.



Gambar 3.3. Alur akuisisi *Live Forensic*, sumber : (Kumar et al., 2016)

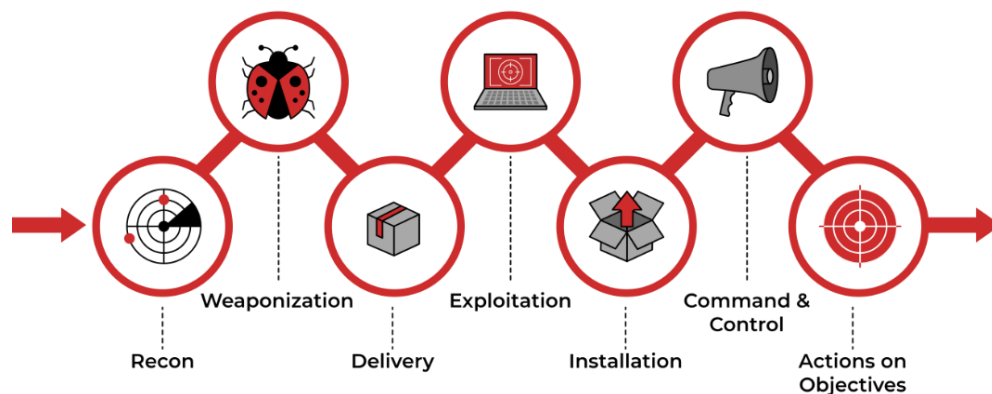
3.1.6 Analisis Forensik

Proses analisa dilakukan untuk memperoleh hasil dari akuisisi yang dilakukan. Data yang diperoleh dari proses akuisisi akan dianalisis untuk mengidentifikasi pola lalu lintas jaringan yang tidak normal atau mencurigakan. Tujuan dari analisis ini adalah untuk mendeteksi potensi serangan atau aktivitas DDoS, pemindaian port, atau trafik jaringan yang anomali. Pada tahap ini akan dilakukan analisa forensik dari beberapa sumber seperti log

traffic Wireshark dan log performa dari Zabbix/System menggunakan framework *Digital Forensic Framework for Reviewing and Investigating Cyber Attack* (D4I) oleh (Dimitriadis et al., 2020c) yang terdiri dari dua tahap / fase sebagai berikut :

1. Kategorisasi Artefak Digital dan Pemetaan ke *Cyber-Kill-Chain* (CKC).

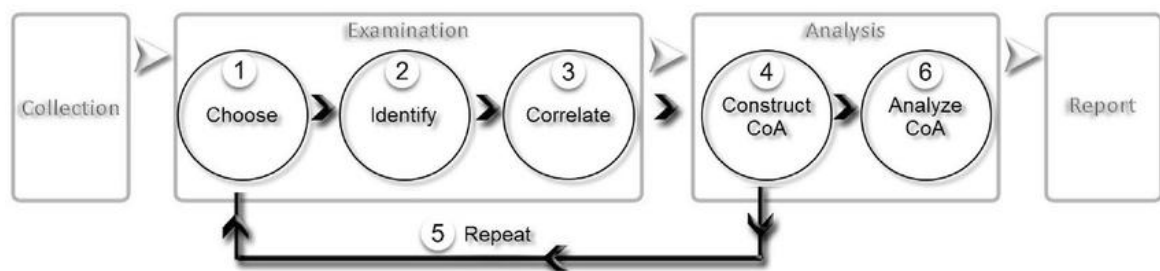
Pada tahap ini peneliti akan melakukan pengumpulan dan kategorisasi artefak bukti atau jejak yang ditinggalkan oleh serangan, seperti file log, file sistem, atau data trafik dan mengklasifikasikan artefak-artefak ini ke dalam tahapan *Cyber-Kill-Chain* (CKC) seperti yang telah dijelaskan dalam dasar teori framework D4I seperti pada gambar 3.4 berikut.



Gambar 3.4. Tahapan *Cyber-Kill-Chain* (CKC), sumber: (Dimitriadis et al., 2020)

2. Langkah-Langkah Pemeriksaan dan Analisis

Pada tahap ini peneliti akan melakukan pemeriksaan dan analisa artefak yang telah dikategorisasi pada tahap awal untuk menggali informasi dan memahami apa yang sebenarnya terjadi selama serangan berlangsung. Dalam proses pemeriksaan dan analisis ini akan dilakukan beberapa langkah seperti yang telah dijelaskan dalam dasar teori framework D4I yang terlihat pada gambar 3.5 sebagai berikut



Gambar 3.5. Tahapan Pemeriksaan dan Analisis D4I, sumber: (Dimitriadis et al., 2020)

3.1.7 Laporan Analisis

Setelah tahap analisa dengan framework D4I selesai, dilakukan pendokumentasian hasil analisa forensik yang mencakup jawaban atas pertanyaan 5W1H dalam investigasi serangan DDoS IPv6 ini. Penulis menggunakan parameter berdasarkan penelitian (Luo et al., 2020; Tseung & Chow, 2018) untuk memetakan setiap jawaban dari pertanyaan 5W1H hasil investigasi, seperti yang disajikan dalam tabel 3.3 berikut.

Tabel 3.3. Pertanyaan dan jawaban 5W-1H pada investigasi serangan DDoS IPv6

Pertanyaan	Langkah - Langkah identifikasi
What (Apa)	Identifikasi parameter <i>Source, Destination, package type</i>
Who (Siapa)	Identifikasi parameter <i>Source, Destination</i> .
When (Kapan)	Identifikasi parameter <i>Timestamp</i> .
Where (Dimana)	Identifikasi parameter <i>Source, Destination</i> .
Why (Mengapa)	Identifikasi parameter <i>Source, Destination dan Traffic Rate</i> .
How (Bagaimana)	Identifikasi parameter <i>Volume Package, Traffic Rate</i> .

3.1.8 Definisi Operasional dan Parameter Evaluasi

Untuk memastikan objektivitas dalam interpretasi hasil penelitian, parameter kualitatif yang digunakan sebagai tolok ukur keberhasilan metode investigasi didefinisikan dengan merujuk pada standar literatur forensik digital sebagai berikut:

1. **Efektivitas (*Effectiveness*)**: Dalam konteks forensik digital, efektivitas tidak hanya diukur dari kinerja sistem, melainkan dari keberhasilan rekonstruksi peristiwa. Mengacu pada kerangka kerja *Event-Based Digital Forensic Investigation* oleh (Carrier & Spafford, 2004), efektivitas didefinisikan sebagai kemampuan metode investigasi dalam merekonstruksi fase kejadian (*event reconstruction*) secara utuh untuk menguji hipotesis awal. Berdasarkan definisi tersebut, metode dalam penelitian ini dinyatakan "Efektif" apabila memenuhi indikator:
 - a. **Kontinuitas**: Mampu menjaga rantai bukti (*Chain of Evidence*) tanpa adanya missing link dari fase awal (*Reconnaissance*) hingga dampak akhir.
 - b. **Kausalitas**: Mampu memvisualisasikan hubungan sebab-akibat melalui *Chain of Artifacts* (CoA), sehingga akar masalah (*root cause*) serangan dapat dibuktikan secara logis.

2. **Komprehensivitas (*Comprehensiveness*):** Komprehensivitas merujuk pada kelengkapan elemen informasi dalam laporan akhir. Berdasarkan studi komparasi model investigasi oleh (Yusoff et al., 2011), fase pelaporan (*reporting*) dinyatakan sukses jika mampu mempresentasikan temuan yang menjawab seluruh dimensi kejadian secara eksplisit [2]. Penelitian ini menetapkan standar komprehensivitas berbasis elemen 5W1H, yaitu:
 - a. *What*: Jenis serangan dan teknik yang digunakan.
 - b. *Who*: Atribusi pelaku.
 - c. *Where*: Lokasi dampak spesifik (Infrastruktur vs Endpoint).
 - d. *When*: Waktu kejadian (Timestamp tersinkronisasi).
 - e. *Why*: Akar penyebab teknis kegagalan sistem.
 - f. *How*: Modus operandi eksekusi serangan.
3. **Validitas (*Validity*):** Validitas dalam penelitian ini mengacu pada konsep Atribusi Teknis (*Technical Attribution*) yang dirumuskan oleh (Rid & Buchanan, 2015a). Menurut Rid & Buchanan, validitas atribusi tercapai ketika investigator mampu menghubungkan artefak digital dengan aktor ancaman melalui identifikasi *tools*, *infrastructure*, dan *tradecraft*. Oleh karena itu, hasil investigasi dinyatakan "Valid" jika metode yang digunakan mampu:
 - a. Mengidentifikasi signature spesifik dari alat serangan (*attack tools*).
 - b. Membedakan secara presisi antara trafik pengguna sah (*legitimate*) dan trafik berbahaya (*malicious*) untuk meminimalkan false positive.

BAB 4

Hasil dan Pembahasan

Pada bab ini penulis membahas langkah - langkah penelitian yang dilakukan serta proses analisa dan hasil yang didapatkan. Pembahasan pada bab ini meliputi mempersiapkan alat dan lingkungan skenario serangan DDoS ICMPv6, melakukan simulasi serangan *Distributed Denial of Service* (DDoS) berbasis ICMPv6 dan TCP pada jaringan IPv6, melakukan pemantauan (*monitoring*) lalu lintas jaringan dan sumberdaya pada router dan server, melakukan akuisisi potensi artefak pada router dan server, melakukan analisa pada hasil akuisisi artefak serangan menggunakan framework *Digital Forensic Framework for Reviewing and Investigating Cyber Attack* (D4I) dan pembuatan analisa dengan konsep 5W1H.

4.1 Persiapan dan Alat

Pada tahap ini, penulis mempersiapkan lingkungan penelitian yang terdiri dari alat (*tools*) dan laboratorium yang dibutuhkan untuk melakukan simulasi serangan *Distributed Denial of Service* (DDoS) pada jaringan IPv6. Penelitian ini menggunakan software simulasi jaringan PNETLab versi 4.2.10. yang berjalan pada server VMware versi 8.0.3.00400 dengan spesifikasi Hardware seperti pada Tabel 4.1. berikut.

Tabel 4.1. Spesifikasi *Hardware*.

No	Hardware	Spesifikasi
1	CPU	16 CPU(s), 846 MHz used
2	Memory	32 GB, 3 GB memory active
3	Hard Disk	200 GB Thin Provision
4	Network	vlan1100 (internal VSwitch)
5	VM Host	VMware vSphere Hypervisor version 8.0.3.00400

Untuk menjalankan skenario serangan *Distributed Denial of Service* (DDoS) pada jaringan IPv6 ini, terdapat beberapa aktor seperti pada gambar 3.2 dengan keterangan spesifikasi sebagai berikut :

a. Komputer Penyerang (*Attacker*)

Fungsi komputer penyerang adalah untuk menciptakan *Distributed Denial of Service (DDoS)*. Adapun spesifikasi *attacker* seperti yang terlihat pada Tabel 4.2 berikut.

Tabel 4.2. Spesifikasi komputer *Attacker*.

No	Hardware	Spesifikasi
1	CPU	2x 1 Core CPU(s), QEMU virtual CPU
2	Memory	4 GB
3	Hard Disk	80 GB
4	Mac Address	50:e5:dd:00:04:00
5	IPv6 Address	2001:db8:100:aa11::2/64
6	OS	Kali Linux 2024.04 Debian
7	Tools	thc-ipv6, nmap 7.95, fping

b. Komputer *Zombie*

Fungsi komputer *zombie* digunakan untuk mendistribusikan serangan secara terkoordinasi untuk meningkatkan volume dan dampak serangan pada server target. Adapun spesifikasi komputer zombie digunakan seperti yang terlihat pada Tabel 4.3 berikut.

Tabel 4.3. Spesifikasi komputer *Zombie*.

No	Hardware	Spesifikasi
1	CPU	2x 1 Core CPU(s), QEMU virtual CPU
2	Memory	4 GB
3	Hard Disk	60 GB
4	Mac Address	50:30:bd:00:07:00
5	IPv6 Address	2001:db8:100:cc::2/64, 2001:db8:100:dd::2/64
6	OS	Ubuntu Server 22.04.2 LTS
7	Tools	sshd server, thc-ipv6, nmap 7.95, fping

c. Router

Fungsi router dalam skenario ini adalah untuk memproses trafik yang masuk dan keluar jaringan. Adapun spesifikasi router yang digunakan seperti yang terlihat pada tabel 4.4 berikut.

Tabel 4.4. Spesifikasi *Router*

No	Hardware	Spesifikasi
1	CPU	1 Core CPU(s), 1899 Mhz
2	Memory	256 MB
3	Hard Disk	90 MB
4	Mac Address	Eth1 : 50:c0:c0:00:0c:00 (to - attacker) Eth2 : 50:c0:c0:00:0c:01 (to - investigator) Eth3 : 50:c0:c0:00:0c:02 (to – svr monitoring) Eth4 : 50:c0:c0:00:0c:03 (to – svr target) Eth5 : 50:c0:c0:00:0c:04 (to – zombie-01) Eth6 : 50:c0:c0:00:0c:05 (to – zombie-02)
5	IPv6 Address	Eth1 : 2001:db8:100:aa11::1/64 Eth2 : 2001:db8:200:c01::1/642 Eth3 : 2001:db8:200:d01::1/64 Eth4 : 2001:db8:200:a01::2/64 Eth5 : 2001:db8:100:cc::1/64 Eth6 : 2001:db8:100:dd::2/64
6	OS	Mikrotik CHR version 7.18.2 stable
7	Tools	Winbox, Webfig

d. Komputer Investigator

Komputer investigator berfungsi untuk mengevaluasi dan menganalisa dampak serangan serta melakukan proses akuisisi dan analisis forensik. Spesifikasi komputer monitoring yang digunakan terlihat pada Tabel 4.5.

Tabel 4.5. Spesifikasi komputer investigator.

No	Hardware	Spesifikasi
1	CPU	2x 1 Core CPU(s), QEMU virtual CPU
2	Memory	4 GB
3	Hard Disk	80 GB
4	Mac Address	50:0c:6c:00:0a:00
5	IPv6 Address	2001:db8:200:c01::2/64
6	OS	Ubuntu Desktop 21.04
7	Tools	SFTPCClient, Winbox, Browser

e. *Server Monitoring*

Fungsi utama dari server monitoring adalah memantau penggunaan sumber daya router secara *realtime*. Spesifikasi yang digunakan pada *Server Monitoring* terlihat pada Tabel 4.6. berikut.

Tabel 4.6. Spesifikasi komputer *Monitoring*.

No	Hardware	Spesifikasi
1	CPU	2x 1 Core CPU(s), QEMU virtual CPU
2	Memory	4 GB
3	Hard Disk	60 GB
4	Mac Address	50:d2:57:00:0b:00
5	IPv6 Address	2001:db8:200:d01::2/64
6	OS	Ubuntu Server 22.04.2 LTS
7	Tools	Zabbix Server 6.42.1

f. *Server Target*

Fungsi utama server target dalam skenario ini adalah untuk mensimulasikan dampak serangan DDoS pada server yang nyata. Spesifikasi Server target yang digunakan terlihat pada tabel 4.7.

Tabel 4.7. Spesifikasi Server Target.

No	Hardware	Spesifikasi
1	CPU	2x 1 Core CPU(s), QEMU virtual CPU
2	Memory	4 GB
3	Hard Disk	60 GB
4	Mac Address	50:2a:76:00:09:00
5	IPv6 Address	2001:db8:200:a01::2/64
6	OS	Ubuntu Server 22.04.2 LTS
7	Tools	Webmin Version 2.303

4.2 Simulasi Serangan

4.2.1 Tujuan Simulasi

Tujuan dari simulasi serangan ini adalah untuk mengamati dampak serangan DDoS pada jaringan berbasis IPv6 dan mengumpulkan artefak forensik yang akan digunakan untuk analisis lebih lanjut. Artefak yang dimaksud meliputi data mengenai penggunaan sumber daya pada perangkat yang terlibat dalam percobaan, seperti *router* MikroTik dan *server* target.

4.2.2 Skenario Simulasi

Simulasi serangan dijalankan dengan empat jenis serangan berbeda yang melibatkan beberapa aktor, yaitu Komputer Penyerang (*attacker*), Komputer zombie-01, Komputer zombie-02, Router MikroTik dan Server target. Skenario ini dimulai pada tanggal 10 Mei 2025 pukul 22:16:00 WIB dengan alur sebagai berikut :

1. Pengamatan Awal

Sebelum dimulainya serangan, dilakukan pengamatan terhadap data *resource* dari router dan server selama sepuluh menit mulai pukul 22:16 - 22:26 WIB. Pengamatan ini bertujuan untuk mendapatkan *baseline* atau data dasar penggunaan CPU, memori dan bandwidth pada router serta server target. Data ini digunakan sebagai referensi untuk membandingkan dampak dari serangan yang dilakukan.

2. Serangan Pertama : Flooding *Redirect Message* Menggunakan Tools *thc-ipv6*

Redirect Message Attack adalah bagian dari ICMPv6-based attack yang memanfaatkan fitur protokol IPv6 yakni ICMPv6 Type 137. Secara normal pesan ini digunakan oleh router untuk menginformasikan host tentang rute yang lebih optimal ke suatu tujuan

(RFC 4861). Serangan ini dilakukan dengan menggunakan tools `thc-ipv6` dengan perintah:

```
atk-flood_redir6 eth0 -F -a 2001:db8:200:a01::2 2001:db8:200:a01::1
```

Keterangan :

- a. **atk-flood_redir6** : tools untuk melakukan serangan redirect flood pada IPv6.
- b. **eth0 / ens3** : Interface jaringan yang digunakan untuk serangan.
- c. **-F** : Mode flood (mengirim paket tanpa interval).
- d. **-a 2001:db8:200:a01::2** : Alamat IPv6 target serangan (server target).
- e. **2001:db8:200:a01::1** : Alamat IPv6 router yang akan disalahkan (spoofed).

Perintah ini akan Membanjiri target (2001:db8:200:a01::2) dengan paket ICMPv6 *Redirect* dan memalsukan bahwa paket tersebut berasal dari router (2001:db8:200:a01::1). Serangan ini dilakukan secara bertahap selama enam menit, dengan urutan attacker menyerang selama dua menit, diikuti dengan zombie-01 menyerang selama dua menit dan kemudian zombie-02 menyerang selama dua menit seperti yang terlihat pada gambar X,Y dan Z.

3. Serangan Kedua: Flooding Menggunakan ICMPv6 *Echo Request Flood*.

Serangan kedua dilakukan dengan cara mengirimkan paket *ICMPv6 Echo Request* (*ping6*) secara paralel dan massal menggunakan tools `fping6` untuk mengirimkan paket besar dalam waktu singkat. Serangan ini dilakukan dengan perintah:

```
fping6 -c 100000 -p 10 -b 1000 2001:db8:200:a01::2
```

Keterangan :

- a. **fping6** : Nama tools untuk mengirimkan flood paket ICMPv6 Echo Request.
- b. **-c 100000** : Mengirim total 100,000 paket ping.
- c. **-p 10** : Interval antar paket: 10 milidetik (100 paket/detik).
- d. **-b 1000** : Ukuran paket 1000 byte.
- e. **2001:db8:200:a01::2** : Alamat IPv6 server target yang diserang

Perintah ini akan mengirimkan DDoS ICMPv6 menggunakan `fping6` untuk membanjiri target (2001:db8:200:a01::2) dengan paket ping besar (1000 byte) secara massal dan cepat. Serangan ini juga dilaksanakan dalam urutan yang sama seperti serangan pertama, dengan attacker menyerang selama 2 menit, diikuti oleh zombie-01 selama 2 menit dan zombie-02 selama 2 menit.

4. Serangan Ketiga : *TCP Connect Flood (IPv6)* Menggunakan *nping*

Serangan ketiga dilakukan dengan cara mengirimkan *flooding* paket TCP IPv6 *Connect* secara paralel dan massal dengan target aplikasi webmin (Port 10000) menggunakan tools nmap ping (*nping*). Serangan ini dilakukan dengan perintah:

```
nping --tcp-connect -6 -p 10000 --rate 1000 2001:db8:200:a01::2 -c 10000
```

Keterangan :

- a. **nping** : Nama tools untuk mengirimkan flooding paket TCP IPv6 *Connect*.
- b. **--tcp-connect** : Membuat koneksi TCP lengkap (3-way handshake).
- c. **-6** : Menggunakan protokol IPv6.
- d. **-p 10000** : Menyerang port 10000 (Webmin).
- e. **--rate 1000** : Total 10.000 koneksi yang dibuat.
- f. **2001:db8:200:a01::2** : Alamat IPv6 server target yang diserang.
- e. **-c 10000** : Total 10.000 koneksi yang dibuat.

Tujuan dari serangan ini untuk membebani antrian koneksi server port 10000 dengan cara membuka koneksi TCP penuh (3-way *handshake*) ke port 10000 yang berdampak pada beban antrian koneksi (*connection queue*) di server menjadi tinggi dan terjadi *Exhaustion memory* dan CPU. Sama seperti serangan-serangan sebelumnya, serangan ini dilaksanakan selama 6 menit, dengan fase serangan yang terdiri dari attacker, zombie01 dan zombie02 masing-masing selama 2 menit.

5. Serangan Keempat : *Flooding Menggunakan atk6-flood_advertise6*

Serangan ketiga dilakukan dengan cara membanjiri server target menggunakan paket ICMPv6 Type 136 (*Neighbor Advertisement*) palsu menggunakan *THC-IPv6 Attack Suite*. Serangan ini dilakukan dengan perintah:

```
atk6-flood_advertise6 eth0/ens3 2001:db8:200:a01::2
```

Keterangan :

- a. **atk6-flood_advertise6** : Nama tool untuk membanjiri target dengan paket NA palsu.
- b. **ens3 / eth0** : Interface jaringan yang digunakan untuk serangan
- c. **2001:db8:200:a01::2** : Alamat IPv6 target yang akan dibanjiri paket NA.

Tujuan dari serangan ini untuk mengirim *flooding* paket NA palsu ke target secepat mungkin dan mengklaim bahwa semua alamat IPv6 di jaringan dimiliki oleh *attacker*. Target akan

memperbarui *Neighbor Cache*-nya dengan informasi salah. Seperti serangan sebelumnya, serangan ini dilakukan selama 6 menit, dengan setiap fase serangan (attacker, zombie01, zombie02) berlangsung selama 2 menit.

4.3 Monitoring Trafik dan Performa Sistem

Tujuan utama dari monitoring trafik dan performa sistem ini adalah untuk mengidentifikasi dan mencatat perubahan dalam pola trafik jaringan yang dapat terjadi akibat serangan serta mengumpulkan data terkait penggunaan sumber daya (*resource*) pada perangkat router dan server target. Dalam tahap ini, traffic yang melewati router dimonitoring menggunakan *tools monitoring* zabbix dan Winbox.

4.3.1 Monitoring Realtime traffic pada Router

Monitoring pada router dilakukan dalam tiga tahap, yaitu sebelum serangan dimulai, saat serangan berlangsung dan setelah serangan untuk memantau perubahan sumber daya pada CPU, memori, serta bandwidth. Router dihubungkan menggunakan SNMP (*Simple Network Management Protocol*) ke server pemantauan berbasis Zabbix.

Berdasarkan pengamatan yang dilakukan selama lima menit pertama sebelum serangan dimulai yakni mulai pukul Data awal resource server dan router pada lima menit awal bisa dilihat pada Gambar 4.1 berikut.



Gambar 4.1. Data awal *resource* router pukul 22:10 – 22:20 WIB.

Gambar 4.1 menunjukkan data awal rata - rata penggunaan CPU pada server adalah 2.6% dan penggunaan *Memory* pada server berkisar 304 Mb dari total 3.82 GB. Sedangkan rata penggunaan CPU pada router adalah 1% sampai dengan 3%, penggunaan memory berkisar 216Mb sampai 218Mb serta traffic yang menuju ke arah server maksimal 48Kbps.

Pada pukul 22:30 – 22:40 WIB, terpantau adanya kenaikan signifikan pada penggunaan CPU, yang mencapai 80-100%, penggunaan memori naik menjadi sekitar 238MB dan bandwidth rata-rata pada interface yang mengarah ke server meningkat secara drastis, dengan rata-rata antara 30-60 Mbps seperti yang terlihat pada Gambar 4.2 berikut.



Gambar 4.2. Data *resource* router pukul 22:32 – 22:37 WIB.

Pada pukul 23:13 – 23:20 WIB, terdapat kenaikan signifikan pada penggunaan CPU, yang berkisar antara 86% hingga 100%. Penggunaan memori mengalami peningkatan pada kisaran antara 230MB hingga 237Mb dan bandwidth rata-rata pada interface yang mengarah ke server antara 1 - 3 Mbps.

Pada pukul 23:31– 23:38 WIB, terlihat adanya kenaikan penggunaan CPU antara 81% hingga 99%. Penggunaan memori juga menunjukkan peningkatan antara 230MB hingga 235MB. Selain itu, bandwidth rata-rata pada interface yang mengarah ke server mencapai 1.3 hingga 1.5 Mbps, yang menunjukkan adanya beban berat pada router.

Pada pukul 00:02 – 00:10 WIB, terdapat kenaikan pada penggunaan CPU, yang berkisar antara 21% hingga 100%. Penggunaan memori juga menunjukkan peningkatan, dengan kisaran antara 223MB hingga 226MB. Sementara itu, bandwidth rata-rata pada interface yang mengarah ke server tercatat sebesar 4.7 Mbps seperti yang terlihat pada gambar 4.3 berikut.



Gambar 4.3. Data *resource* router pukul 00:02 – 00.10 WIB

4.3.2 Monitoring *Traffic* pada *Server Target*

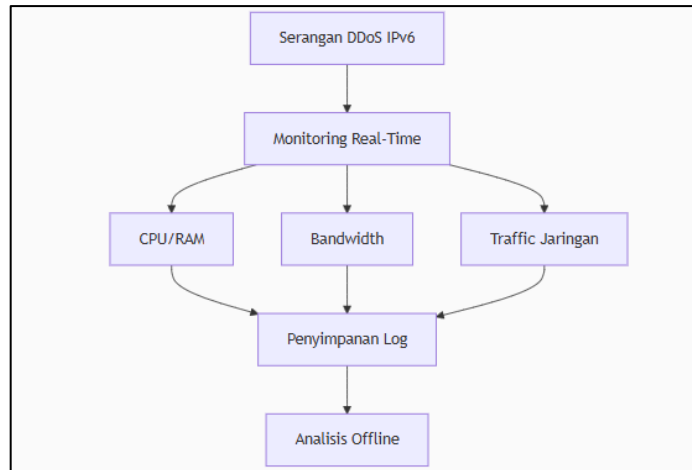
Monitoring pada server dilakukan dengan menggunakan beberapa alat yang terinstal untuk mengamati penggunaan sumber daya secara real-time selama serangan berlangsung. Alat-alat yang digunakan meliputi *mpstat* untuk memantau penggunaan CPU, *vmstat* untuk memantau penggunaan memori, serta *tcpdump* untuk memantau trafik jaringan.

- Tools ***mpstat*** digunakan untuk mendapatkan informasi terkait kinerja CPU meliputi statistik penggunaan CPU untuk proses sistem, pengguna dan idle sehingga dapat diketahui dampak serangan terhadap penggunaan CPU selama serangan.
- Tools ***vmstat*** digunakan untuk mengamati penggunaan memori dan proses-proses yang berjalan termasuk informasi tentang swap, buffer dan paging untuk melihat dampak serangan terhadap ketersediaan dan penggunaan memori pada server.
- Tools ***tcpdump*** digunakan untuk memantau dan menangkap trafik jaringan yang masuk dan keluar dari server.

Tools ini dijalankan secara terus-menerus selama serangan berlangsung dan hasilnya akan diambil saat tahap akuisisi data untuk dianalisis lebih lanjut pada langkah akuisisi dan analisis di poin 4.6. Data yang diperoleh akan memberikan gambaran mengenai pengaruh serangan terhadap kinerja server, termasuk CPU load, penggunaan memori dan trafik jaringan yang terjadi selama serangan .

4.4 Pengumpulan Data

Selama periode serangan, peneliti menjalankan *script* pada router dan server target untuk mengumpulkan data penggunaan sumber daya dengan alur seperti pada Gambar 4.4. *Script* tersebut dirancang untuk mengukur dan merekam *CPU usage*, *memory usage*, disk I/O dan trafik jaringan yang diterima oleh perangkat.



Gambar 4.4. Skema Pengumpulan Data

Untuk melakukan pengumpulan data *CPU Load* dan *Timestamp* pada router, peneliti membuat *script* “mikrotik-cpu” yang dimasukan dalam router mikrotik sebagai berikut.

```
# Set interval waktu pengambilan data (2 detik)
:local interval 2

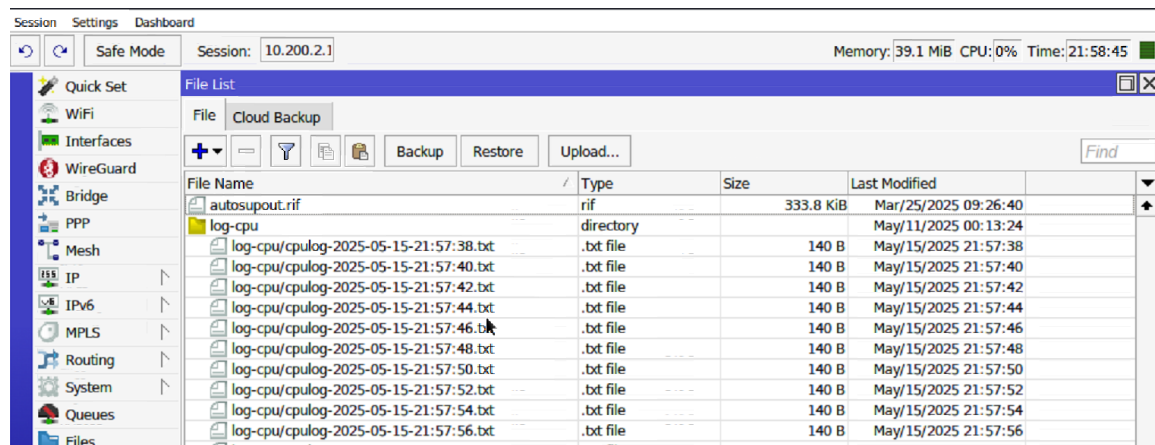
# Loop untuk mengambil data CPU setiap 2 detik
:while (true) do={
    # Ambil timestamp saat ini
    :local timestamp [/system clock get time]
    :local date [/system clock get date]

    # Format nama file dengan timestamp (misalnya cpulog-2025-05-08-12-30-00.txt)
    :local filename ("cpulog-" . [:pick $date 0 10] . "-" . [:pick $timestamp 0 8] . ".txt")

    # Ambil data CPU dan simpan ke file
    /system resource cpu print file=$filename

    # Tunggu selama 2 detik
    :delay $interval
}
```

Sedangkan hasil file output script pada penyimpanan router bisa dilihat pada Gambar 4.5 berikut.



Gambar 4.5. Hasil file output pada penyimpanan router

Script diatas akan menghasilkan output file “cpulog-YYYY-MM-DD-HH_MM_SS.txt” setiap 2 detik yang berisi log cpu dan timestamp dengan contoh sebagai berikut.

```
# 2025-05-10 22:35:06 by RouterOS 7.18.2
# software id =
#
Columns: CPU, LOAD, IRQ, DISK
# CPU   LOAD  IRQ  DISK
0  cpu0  100% 59%  0%
```

Selain mengambil data cpu dan timestamp, penulis juga mengambil data lalu lintas jaringan yang terhubung ke interface komputer penyerang, zombie-01, zombie-02 dan server target menggunakan fitur *packet sniffer* yang terdapat dalam router yang kemudian dihubungkan ke komputer investigator dengan *port 37008* dengan konfigurasi sebagai berikut.

```
/tool sniffer
set file-limit=100000KiB file-name=traffic filter-cpu=0 filter-dst-ipv6-
address=::/0 filter-interface=eth1,eth4,eth5,eth6 \
filter-src-ipv6-address=::/0 memory-limit=10000KiB streaming-enabled=yes
streaming-server= 2001:db8:200:c01::2 port:37008
```

Setelah terhubung via *port 37008*, secara otomatis komputer investigator bisa melihat paket apa saja yang melewati router dari penyerang dan zombie ke server target menggunakan tools *Wireshark* dan memungkinkan untuk mengakusisi data lalu lintas jaringan dalam format *.pcap* seperti terlihat pada gambar 4.6 berikut.

The screenshot shows a Wireshark interface capturing traffic on eth0 (UDP port 37008). The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
31	2025-05-13 10:02:18.3945...	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	133	55386 → 10000 [ACK]
32	2025-05-13 10:02:18.3955...	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.3	213	Change Cipher Spec,
33	2025-05-13 10:02:18.3966...	2001:db8:200:a01::2	2001:db8:200:c01::2	TLSv1.3	388	Application Data
34	2025-05-13 10:02:18.3967...	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.3	789	Application Data
35	2025-05-13 10:02:18.4384...	2001:db8:200:a01::2	2001:db8:200:c01::2	TCP	133	10000 → 55386 [ACK]
36	2025-05-13 10:02:18.4403...	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	133	55386 → 10000 [ACK]
37	2025-05-13 10:02:18.6917...	2001:db8:200:a01::2	2001:db8:200:c01::2	TLSv1.3	186	Application Data
38	2025-05-13 10:02:18.6924...	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	133	55386 → 10000 [ACK]
39	2025-05-13 10:02:18.6938...	2001:db8:200:a01::2	2001:db8:200:c01::2	TLSv1.3	387	Application Data, Ap
40	2025-05-13 10:02:18.6946...	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	133	55386 → 10000 [ACK]
41	2025-05-13 10:02:19.2783...	2001:db8:200:a01::2	2001:db8:200:c01::2	TLSv1.2	157	Application Data
42	2025-05-13 10:02:19.2818...	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	161	Application Data
43	2025-05-13 10:02:19.2821...	2001:db8:200:a01::2	2001:db8:200:c01::2	TCP	133	10000 → 51122 [ACK]
44	2025-05-13 10:02:19.8789...	10.200.2.1	10.200.2.2	IPv4	1514	Fragmented IP protoc
45	2025-05-13 10:02:19.8796...	10.200.2.1	10.200.2.2	IPv4	1514	Fragmented IP protoc
46	2025-05-13 10:02:19.8807...	10.200.2.1	10.200.2.2	IPv4	1514	Fragmented IP protoc
47	2025-05-13 10:02:19.8818...	2001:db8:200:a01::2	2001:db8:200:c01::2	TCP	133	[TCP Previous segmer
48	2025-05-13 10:02:19.8821...	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	133	[TCP ACKed unseen se
49	2025-05-13 10:02:19.8823...	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	133	[TCP ACKed unseen se
50	2025-05-13 10:02:19.8826...	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	133	[TCP ACKed unseen se
51	2025-05-13 10:02:19.8829...	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.3	157	Application Data
52	2025-05-13 10:02:19.8832...	2001:db8:200:a01::2	2001:db8:200:c01::2	TCP	121	10000 → 55386 [RST]
53	2025-05-13 10:02:25.5700...	fe80::52c0:c0ff:fe0...	ff02::1	MNDP	285	5678 → 5678 Len=176
54	2025-05-13 10:02:25.5796...	fe80::52c0:c0ff:fe0...	ff02::1	MNDP	285	5678 → 5678 Len=176
55	2025-05-13 10:02:25.5802...	fe80::52c0:c0ff:fe0...	ff02::1	MNDP	285	5678 → 5678 Len=176
56	2025-05-13 10:02:25.5831...	fe80::52c0:c0ff:fe0...	ff02::1	MNDP	285	5678 → 5678 Len=176

Gambar 4.6. Capture lalu lintas jaringan router port 37008

Untuk melakukan pengumpulan data *CPU Load*, *Memory*, *Bandwidth* dan lalu lintas data yang menuju ke server target, peneliti membuat script *bash* bernama “start-monitoring.sh” yang dijalankan pada server secara *realtime* sebagai berikut.

```
#!/bin/bash
# Filename: start_monitoring.sh

# Start packet capture
tcpdump -i ens3 -w "start_traffic_$(date +%Y%m%d_%H%M%S).pcap" &

# Start CPU monitoring
mpstat 1 300 > "start_cpu_usage_$(date +%Y%m%d_%H%M%S).log" 2>&1 &

# Start memory monitoring
vmstat 1 300 > "start_memory_usage_$(date +%Y%m%d_%H%M%S).log" 2>&1 &

# Start bandwidth monitoring
sudo iftop -i ens3 -t -s 300 > "start_bandwidth_iftop_$(date +%Y%m%d_%H%M%S).log" 2>&1 &

echo "Monitoring started. Use 'pkill tcpdump mpstat vmstat iftop' to stop."
```

Setelah selesai dijalankan, *script* tersebut akan menghasilkan empat *file* yang berisi data *CPU Load*, *Memory*, *Bandwidth Usage* dan lalu lintas data berdasarkan waktu pengambilan seperti terlihat pada Gambar 4.6 berikut.

```

root@server:~# ls -l | grep start_
-rw-r--r-- 1 root    root      4272 May 11 00:07 start_bandwidth_iftop_20250511_000157.log
-rw-r--r-- 1 root    root     29359 May 11 00:06 start_cpu_usage_20250511_000157.log
-rw-r--r-- 1 root    root     27032 May 11 00:06 start_memory_usage_20250511_000157.log
-rw-r--r-- 1 tcpdump tcpdump 83030130 May 11 00:10 start_traffic_20250511_000157.pcap
root@server:~#

```

Gambar 4.7. Hasil *capture cpu load, memory, bandwidth* dan lalulintas data server

Setiap serangan dijalankan secara berurutan sesuai dengan skenario yang telah direncanakan. Setelah serangan selesai, data hasil pengamatan pada router dan server akan diakuisisi dan dianalisis ditahapan selanjutnya.

4.5 Akuisisi, Preservasi dan Pemeriksaan Artefak

Pada tahapan akuisisi, preservasi dan pemeriksaan Artefak, peneliti menerapkan metode *Live Forensic* untuk mengelola artefak dari simulasi serangan DDoS pada jaringan IPv6 yang didapatkan. Metode *Live Forensic* digunakan dengan tujuan utama untuk melakukan identifikasi (*identification*), koleksi (*Collection*), akuisisi (*Acquisition*), preservasi (*Preservation*) serta pemeriksaan awal pada artefak digital yang dihasilkan secara real-time tanpa mengganggu atau menghentikan operasional jaringan dan perangkat yang sedang berfungsi.

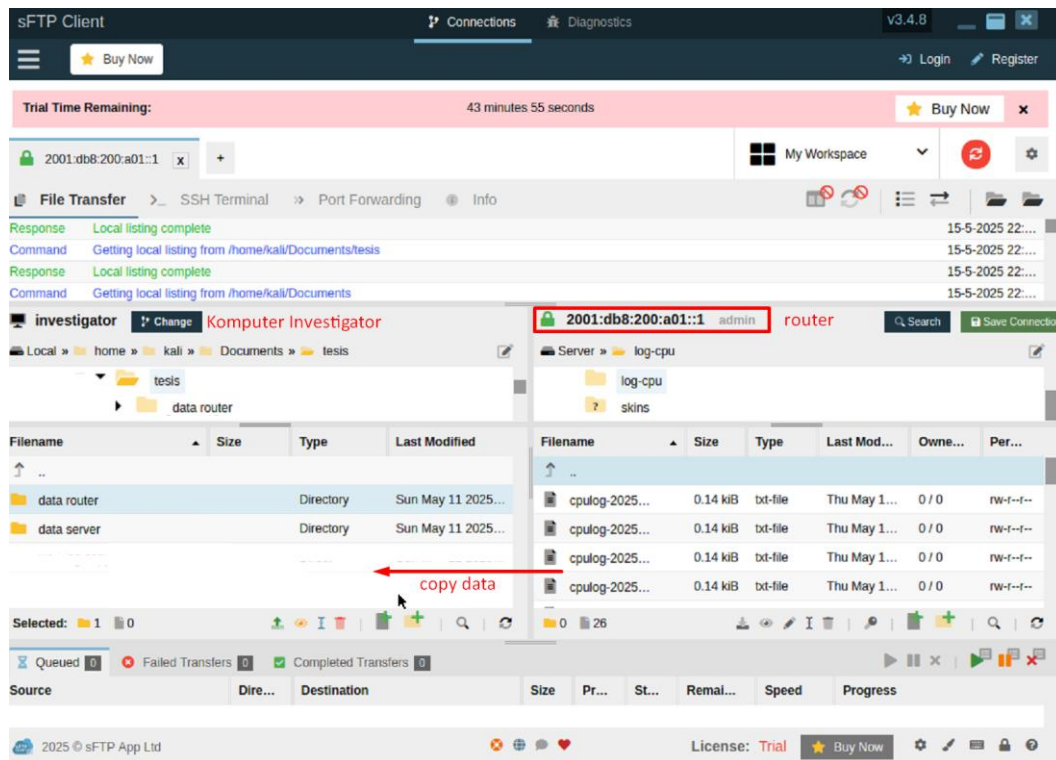
4.5.1 Identifikasi bukti digital (*Identification*)

Identifikasi artefak bertujuan untuk mengumpulkan bukti digital yang relevan dengan pola dan karakteristik serangan. Fokus utama identifikasi bukti digital terdiri dari beberapa parameter seperti alamat sumber (*Source Address*), alamat tujuan (*Destination Address*) tipe paket (*Package Type*) dan *volume traffic*, yang bersumber dari perangkat jaringan (*router*) dan server target.

4.5.2 Pengumpulan (*Collection*) dan Akuisisi (*Acquisition*) bukti digital

Pada tahap ini dilakukan proses koleksi dan akuisisi menggunakan alat dan metodologi yang *non-intrusif* untuk memastikan integritas data tetap terjaga. Data serangan yang terkumpul dari server dan router selanjutnya diambil menggunakan tools *sFTPClient* seperti yang terlihat pada Gambar 4.8 kemudian disimpan dalam direktori secara terstruktur. Proses

koleksi dan akuisisi yang dilakukan secara terstruktur dapat meminimalkan gangguan terhadap operasional jaringan, sehingga memenuhi prinsip *Live Forensics*.



Gambar 4.8. Proses pengumpulan artefak serangan menggunakan sFTPCliet

4.5.3 Preservasi (*preservation*) bukti digital

Pada tahapan preservasi hasil akuisisi pada serangan DDoS berbasis IPv6, dilakukan dengan cara melakukan *generate hash* pada artefak yang dikumpulkan menggunakan *script* “forensic-prop.bash” berikut.

```
#!/bin/bash
# Cek argumen
if [ "$#" -ne 1 ]; then
    echo "Usage: $0 <file_path>"
    exit 1
fi
FILE="$1"
OUTPUT="${FILE}_forensic_properties.txt"
```

```

# Verifikasi file
if [ ! -f "$FILE" ]; then
    echo "Error: File $FILE not found!"
    exit 1
fi

# Ambil metadata
FILE_NAME=$(basename "$FILE")
DATE_CREATED=$(stat -c %w "$FILE" 2>/dev/null || date -r "$FILE" "+%Y-%m-%d %H:%M:%S")

# Hitung hash
MD5=$(md5sum "$FILE" | awk '{print $1}')
SHA1=$(sha1sum "$FILE" | awk '{print $1}')
SHA256=$(sha256sum "$FILE" | awk '{print $1}')
SHA512=$(sha512sum "$FILE" | awk '{print $1}')

# Tulis hasil ke file
echo "=== FORENSIC PROPERTIES ===" > "$OUTPUT"
echo "File Name: $FILE_NAME" >> "$OUTPUT"
echo "Created Date: $DATE_CREATED" >> "$OUTPUT"
echo "MD5: $MD5" >> "$OUTPUT"
echo "SHA-1: $SHA1" >> "$OUTPUT"
echo "SHA-256: $SHA256" >> "$OUTPUT"
echo "SHA-512: $SHA512" >> "$OUTPUT"

echo "Forensic properties saved to: $OUTPUT"

```

Setelah itu, script tersebut dijalankan dengan perintah

```
# ./forensic-prop.bash <path file>
```

Maka secara otomatis *script* akan membuat data *timestamp* dan *hash value* pada setiap file yang telah diakuisisi. Terlihat list file pada folder sebelum dilakukan hashing pada Gambar 4.9.



```

File  Actions  Edit  View  Help
(root@investigator)-[~]
# ls /home/kali/Documents/tesis/data\ server/serangan-01/start_*
'/home/kali/Documents/tesis/data server/serangan-01/start_bandwidth_iftop_20250510_223116.log'
'/home/kali/Documents/tesis/data server/serangan-01/start_cpu_usage_20250510_223116.log'
'/home/kali/Documents/tesis/data server/serangan-01/start_memory_usage_20250510_223116.log'
'/home/kali/Documents/tesis/data server/serangan-01/start_traffic_20250510_223116.pcap'

```

Gambar 4.9. File hasil akuisisi yang belum memiliki *hash*

Kemudian dilakukan proses hasing menggunakan script seperti pada gambar 4.10.

```
(root@investigator)-[~]
# ./forensic-prop.bash /home/kali/Documents/tesis/data\ server/serangan-01/start_bandwidth_iftop_20250510_223116.log
Forensic properties saved to: /home/kali/Documents/tesis/data server/serangan-01/start_bandwidth_if
top_20250510_223116.log_forensic_properties.txt

(root@investigator)-[~]
# ./forensic-prop.bash /home/kali/Documents/tesis/data\ server/serangan-01/start_cpu_usage_20250510_223116.log
Forensic properties saved to: /home/kali/Documents/tesis/data server/serangan-01/start_cpu_usage_20
250510_223116.log_forensic_properties.txt

(root@investigator)-[~]
# ./forensic-prop.bash /home/kali/Documents/tesis/data\ server/serangan-01/start_memory_usage_20250510_223116.log
Forensic properties saved to: /home/kali/Documents/tesis/data server/serangan-01/start_memory_usage
_20250510_223116.log_forensic_properties.txt

(root@investigator)-[~]
# ./forensic-prop.bash /home/kali/Documents/tesis/data\ server/serangan-01/start_traffic_20250510_223116.pcap
Forensic properties saved to: /home/kali/Documents/tesis/data server/serangan-01/start_traffic_2025
0510_223116.pcap_forensic_properties.txt
```

Gambar 4.10. File hasil akuisisi yang sudah memiliki nilai *hash*.

Pada Gambar 4.11 berikut merupakan salah satu contoh *hash properties* pada file `start_bandwidth_iftop_20250510_223116.log_forensic_properties.txt`.

```
(root@investigator)-[~]
# cat /home/kali/Documents/tesis/data\ server/serangan-01/start_bandwidth_iftop_20250510_223116.l
og_forensic_properties.txt
== FORENSIC PROPERTIES ==
File Name: start_bandwidth_iftop_20250510_223116.log
Created Date: 2025-05-10 22:54:18.260000000 +0700
MD5: 4f1b0585361d221607a8fb8712c074cf
SHA-1: 78af755171f2a659e0043bb0b62714b64c30ac06
SHA-256: c220068d549902158b9a3e2d58f0a12db4e7ca8fe3cc2f780db83936ff1240d6
SHA-512: 798a7bb8e62b7dd6995da91ca0776c8853a6e9dc6c699dd1034dd93ab92b74ef8691a437074364702ccfaff907
1ab29f9efdacbd4d0eb94e7fa7c729c99aed045
```

Gambar 4.11. salah satu contoh *hash properties*.

Proses ini dilakukan pada semua artefak dari hasil akuisis router dan server untuk menjaga integritas, keaslian dan keutuhan data/artefak digital yang telah dikumpulkan selama proses koleksi sehingga data tersebut tetap *admissible* (dapat diterima secara hukum) dan tidak mengalami perubahan.

4.5.4 Pemeriksaan Data Mentah (*Raw*) Artefak Serangan

Selanjutnya dilakukan pemeriksaan awal terhadap keseluruhan raw artefak yang dikumpulkan dari *router* dan *server* target. Pemeriksaan awal ini bertujuan untuk mendapatkan gambaran umum mengenai kondisi dan aktivitas *router* dan *server* selama periode serangan, mengidentifikasi anomali atau pola mencurigakan yang signifikan pada data *log* performa dan lalu lintas jaringan serta menentukan artefak-artefak kunci yang paling

informatif dan relevan untuk analisis lebih lanjut. Adapun pemeriksaan artefak digital ini akan difokuskan pada hasil artefak yang diambil dari router dan server target sebagai berikut.

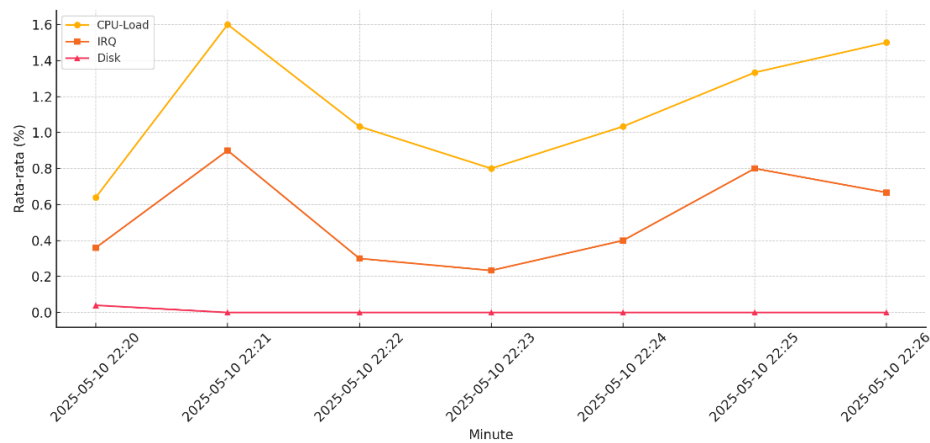
1. Pemeriksaan Artefak Router

Dilakukan pemeriksaan pada hasil Log data historis penggunaan CPU, IRQ dan Disk Usage yang dihasilkan oleh router. Observasi awal pada artefak ini menunjukkan pada tanggal 2025-05-10 pukul 22:20 – 22.25 WIB sebelum terjadi serangan terlihat penggunaan CPU, IRQ dan Disk Usage normal dengan penggunaan resource seperti terlihat pada tabel 4.8 berikut.

Tabel 4.8. CPU, IRQ dan *Disk Usage* pukul 22:20 – 22.25 WIB.

Timestamp	CPU-Load	IRQ	Disk
2025-05-10 22:20	0.6 %	0.36	0.04
2025-05-10 22:21	1.6 %	0.90	0.00
2025-05-10 22:22	1.0 %	0.30	0.00
2025-05-10 22:23	0.8 %	0.23	0.00
2025-05-10 22:24	1.0 %	0.40	0.00
2025-05-10 22:25	1.3 %	0.80	0.00
2025-05-10 22:26	1.5 %	0.67	0.00

Sedangkan visualisasi grafik rata-rata CPU Load, IRQ dan Disk per menit untuk data router sebelum serangan bisa dilihat pada Gambar 4.12 berikut.



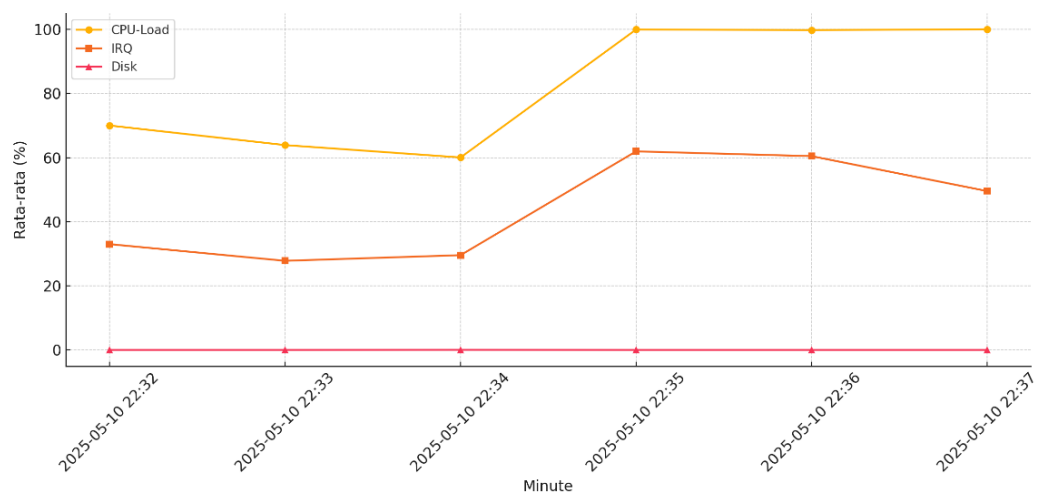
Gambar 4.12. *Resource Usage* 2025-05-10 pukul 22:20 – 22.25 WIB.

Pada tanggal 2025-05-10 pukul 22:32 – 22:37 WIB terdapat lonjakan signifikan penggunaan CPU, IRQ dan Disk Usage mencapai 80-100% seperti terlihat pada hasil ekstraksi log router di tabel 4.9 berikut.

Tabel 4.9. CPU, IRQ dan Disk Usage pukul 22:32 – 22:37 WIB.

Timestamp	CPU-Load	IRQ	Disk
2025-05-10 22:32	70.00	33.00	0.00
2025-05-10 22:33	63.90	27.80	0.00
2025-05-10 22:34	60.03	29.57	0.03
2025-05-10 22:35	99.93	61.93	0.00
2025-05-10 22:36	99.76	60.45	0.00
2025-05-10 22:37	100.00	49.56	0.00

Sedangkan visualisasi grafik rata-rata CPU Load, IRQ dan Disk per menit pada tanggal 2025-05-10 pukul 22:32 – 22:37 WIB pertama bisa dilihat pada Gambar 4.13 berikut.



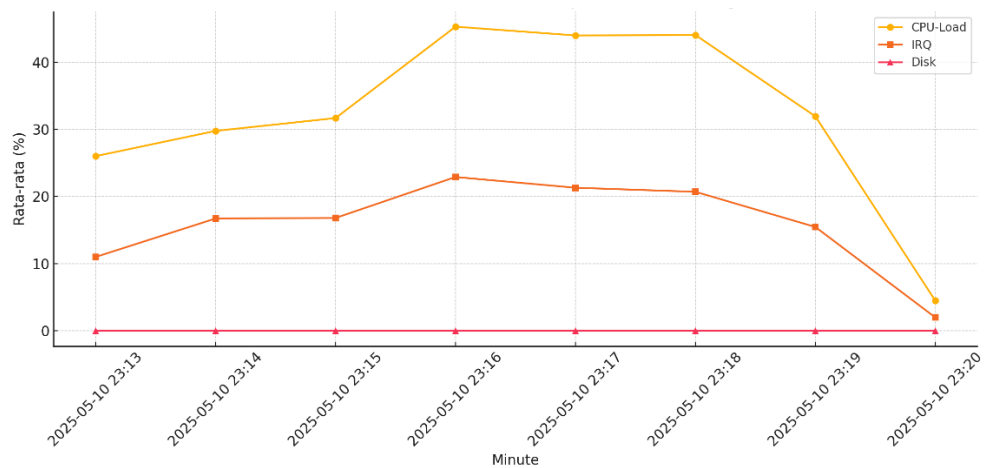
Gambar 4.13. *Resource Usage* 2025-05-10 pukul 22:32 – 22:37 WIB.

Selanjutnya pada tanggal 2025-05-10 pukul 23:13 – 23:20 WIB terdapat lonjakan penggunaan CPU, IRQ dan Disk Usage mencapai 26-45% seperti terlihat pada hasil ekstraksi log router di Tabel 4.10 berikut.

Tabel 4.10. CPU, IRQ dan Disk Usage pukul 23:13 – 23:20 WIB.

<i>Timestamp</i>	<i>CPU-Load</i>	<i>IRQ</i>	<i>Disk</i>
2025-05-10 23:13	26.00	11.00	0.0
2025-05-10 23:14	29.76	16.72	0.0
2025-05-10 23:15	31.67	16.80	0.0
2025-05-10 23:16	45.27	22.90	0.0
2025-05-10 23:17	43.97	21.30	0.0
2025-05-10 23:18	44.03	20.70	0.0
2025-05-10 23:19	31.93	15.47	0.0
2025-05-10 23:20	4.50	2.00	0.0

Sedangkan visualisasi grafik rata-rata CPU Load, IRQ dan Disk per menit pada tanggal 2025-05-10 pukul 23:13 – 23:20 WIB bisa dilihat pada Gambar 4.14 berikut.



Gambar 4.14. *Resource Usage* 2025-05-10 pukul 23:13– 23:20 WIB.

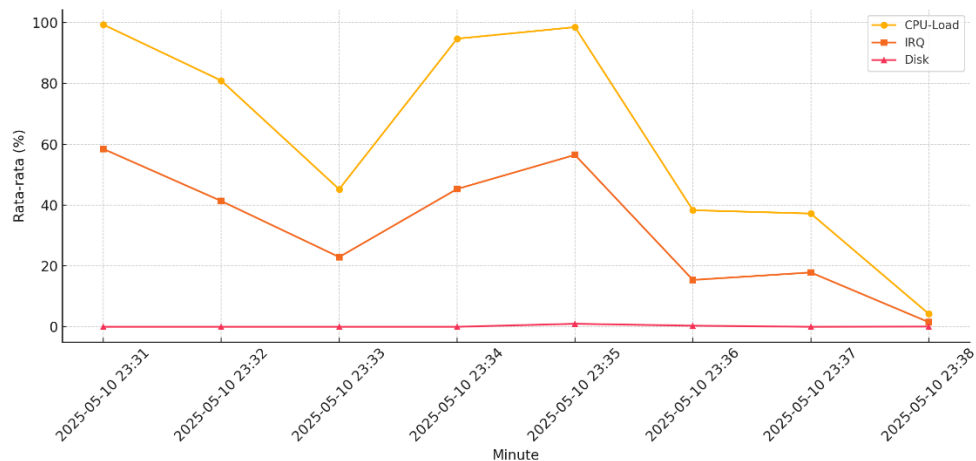
Pada tanggal 2025-05-10 pukul 23:31 – 23:38 WIB terdapat lonjakan penggunaan CPU, IRQ dan Disk Usage mencapai 37 - 99% seperti terlihat pada hasil ekstraksi log router di Tabel 4.11 berikut.

Tabel 4.11. CPU, IRQ dan Disk Usage pukul 23:31 – 23:38 WIB.

<i>Timestamp</i>	<i>CPU-Load</i>	<i>IRQ</i>	<i>Disk</i>
2025-05-10 23:31	99.3 %	58.4 %	0 %
2025-05-10 23:32	80.9 %	41.3 %	0 %

Timestamp	CPU-Load	IRQ	Disk
2025-05-10 23:33	45.2 %	22.9 %	0 %
2025-05-10 23:34	94.7 %	45.3 %	0 %
2025-05-10 23:35	98.5 %	56.5 %	1 %
2025-05-10 23:36	38.3 %	15.4 %	0.4 %
2025-05-10 23:37	37.2 %	17.8 %	0 %
2025-05-10 23:38	4.2 %	1.5 %	0.07 %

Sedangkan visualisasi grafik rata-rata CPU Load, IRQ dan Disk per menit pada tanggal 2025-05-10 pukul 23:31 – 23:38 WIB bisa dilihat pada Gambar 4.15 berikut.



Gambar 4.15. *Resource Usage* 2025-05-10 pukul 23:31– 23:38 WIB.

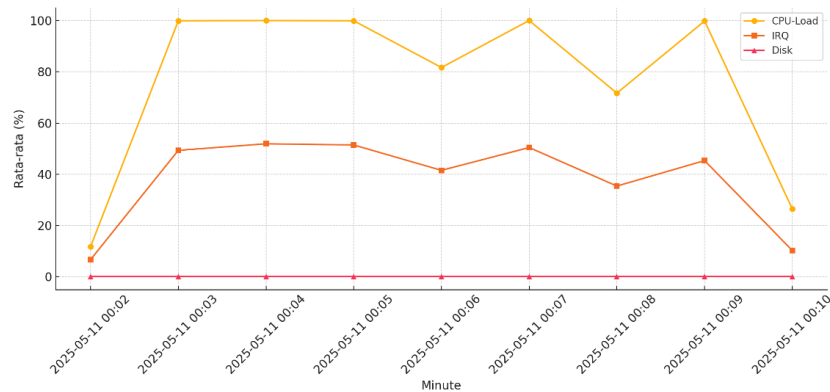
Selanjutnya pada tanggal 2025-05-10 pukul 00:02 – 00:10 WIB terdapat lonjakan penggunaan penggunaan CPU, IRQ dan Disk Usage mencapai 11 - 100% seperti terlihat pada hasil ekstraksi log router di Tabel 4.12 berikut.

Tabel 4.12. CPU, IRQ dan Disk Usage pukul 00:02 – 00:10 WIB.

Timestamp	CPU-Load	IRQ	Disk
2025-05-11 00:02	11.79	6.72	0.0
2025-05-11 00:03	99.90	49.33	0.0
2025-05-11 00:04	99.97	51.90	0.0
2025-05-11 00:05	99.90	51.43	0.0
2025-05-11 00:06	81.67	41.53	0.0

Timestamp	CPU-Load	IRQ	Disk
2025-05-11 00:07	100.00	50.43	0.0
2025-05-11 00:08	71.67	35.40	0.0
2025-05-11 00:09	99.80	45.33	0.0
2025-05-11 00:10	26.50	10.25	0.0

Sedangkan visualisasi grafik rata-rata CPU Load, IRQ dan Disk per menit pada tanggal 2025-05-10 pukul 00:02 – 00.10 WIB bisa dilihat pada Gambar 4.16 berikut



Gambar 4.16. *Resource Usage* 2025-05-11 pukul 00:02 – 00.10 WIB.

Grafik dan tabel hasil dari pemeriksaan pada Log data historis penggunaan CPU, IRQ dan Disk Usage diatas akan dijadikan sebagai landasan analisis forensik menggunakan framework D4I pada poin 6.4.

2. Pemeriksaan Artefak Server Target

Pada tahapan ini dilakukan pemeriksaan pada server target. Artefak yang diperiksa yaitu log dan data lalu lintas jaringan yang dihasilkan oleh *script* “start-monitoring.sh” untuk melihat dampak langsung pada target. Artefak-artefak spesifik dari server target yang diidentifikasi meliputi:

- Capture Bandwidth (iftop)
- Log CPU Usage (mpstat)
- Log Memory Usage (vmstat)
- Traffic PCAP Server (tcpdump)

Pemeriksaan artefak pada server target dilakukan dengan urutan sebagai berikut.

a. Pemeriksaan *bandwith usage*

Pemeriksaan awal dilakukan pada artefak bandwidth server yang diambil dengan program *iftop* yakni “start_bandwidth_iftop_20250510_222003.log” untuk melihat rata – rata trafik jaringan pada tanggal 2025-05-10 pukul 22:20 – 22.25 dengan hasil seperti pada Tabel 4.13 berikut.

Tabel 4.13. Ringkasan trafik jaringan pukul 22:20 – 22.25 WIB.

Periode	Kirim	Terima	Total
2 detik	672 b	688 b	1.33 kb
10 detik	2.80 kb	794 b	3.57 kb
40 detik	32.3 kb	1.59 kb	33.9 kb
Kumulatif (300 detik)	616 kb	741 kb	

Dari tabel diatas dapat kita simpulkan bahwa besaran transaksi data rata – rata normal selama 5 menit adalah 616 Kb *upload* dan 741 Kb *download*.

Selanjutnya dilakukan pemeriksaan pada file artefak “start_bandwidth_iftop_20250510_223116.log” untuk melihat rata – rata bandwidth pada tanggal 2025-05-10 pukul 22:32 – 22.37 WIB seperti pada Tabel 4.14 berikut.

Tabel 4.14. Ringkasan trafik jaringan pukul 22:32 – 22.37 WIB.

Periode	Kirim	Terima	Total
2 detik	672 b	400 b	1.05 kb
10 detik	346 b	323 b	669 b
40 detik	5.04 kb	1.26 kb	6.30 kb
Kumulatif (300 detik)	27.4 kb	9.27 kb	

Dari tabel diatas dapat kita simpulkan bahwa besaran bandwidth mengalami penurunan drastis sebesar 27.4 kb *upload* dan 9.27 kb *download*.

Selanjutnya dilakukan pemeriksaan pada file “start_bandwidth_iftop_20250510_231355” untuk melihat rata – rata bandwidth pada tanggal 2025-05-10 pukul 23:13 – 23.20 WIB dengan hasil seperti pada Tabel 4.15 berikut.

Tabel 4.15. Ringkasan trafik jaringan pukul 23:13 – 23:20 WIB.

Interval	Kirim	Terima	Total
2 detik	823 Kb	823 Kb	1.61 Mb
10 detik	822 Kb	822 Kb	1.61 Mb
40 detik	821 Kb	821 Kb	1.60 Mb
Kumulatif (300 detik)	28.5 Mb	28.5 Mb	57.0 Mb

Dari tabel diatas dapat kita simpulkan bahwa besaran transaksi data mengalami kenaikan drastis yang tidak wajar sebesar 28.5 Mb *upload* dan 28.5 Mb *download*.

Selanjutnya dilakukan pemeriksaan pada file “start_bandwidth_iftop_20250510_233219” untuk melihat rata – rata bandwidth pada tanggal 2025-05-10 pukul 23:31– 23:38 WIB dengan hasil seperti pada Tabel 4.16 berikut.

Tabel 4.16. Ringkasan trafik jaringan pukul 23:31– 23:38 WIB.

Periode	Kirim	Terima	Total
2 detik	1.29 Mb	1.00 Mb	2.30 Mb
10 detik	1.25 Mb	705 Kb	1.94 Mb
40 detik	731 Kb	453 Kb	1.16 Mb
Kumulatif (300 detik)	17.9 Mb	15.2 Mb	33.1 Mb

Dari tabel diatas dapat kita simpulkan bahwa besaran transaksi data mengalami kenaikan drastis yang tidak wajar sebesar 17.9 Mb *upload* dan 15.2 Mb *download*.

Selanjutnya dilakukan pemeriksaan pada file “start_bandwidth_iftop_20250511_000157.log” untuk melihat rata – rata bandwidth pada tanggal 2025-06-11 pukul 00:02 – 00.10 WIB dengan hasil seperti pada Tabel 4.17 berikut.

Tabel 4.17. Ringkasan trafik jaringan pukul 00:02 – 00.10 WIB.

Periode	Kirim	Terima	Total
2 detik	0 b	288 b	288 b
10 detik	103 b	230 b	334 b
40 detik	26 b	188 Kb	188 Kb
Kumulatif (300 detik)	3.04 KB	4.71 Mb	4.71 Mb

Dari tabel diatas dapat kita simpulkan bahwa besaran transaksi data mengalami kenaikan wajar sebesar 3.04 Kb *upload* dan 4.71 Mb *download*.

b. Pemeriksaan *CPU Usage*.

Dilakukan pemeriksaan *cpu usage* server target pada artefak *start_cpu_usage_20250510_222003.log* pada tanggal 2025-05-10 pukul 22:10 – 22:20 WIB dengan hasil seperti pada tabel 4.18 berikut.

Tabel 4.18. Ringkasan *CPU Usage* pukul 22:10 – 22:20 WIB.

waktu	cpu usage (%)	cpu free (%)
22:10	1.22	98.70
22:12	1.28	98.65
22:14	1.23	98.74
22:16	1.12	98.80
22:18	1.22	98.71
22:20	1.28	98.65

Dari data tabel diatas dapat dilihat bahwa rata rata penggunaan CPU adalah 1.25%.

Selanjutnya dilakukan pemeriksaan *cpu load server* pada artefak “*start_cpu_usage_20250510_223116.log*” yang diambil pada tanggal 2025-05-10 pukul 22:32 – 22:37 WIB dengan hasil seperti pada Tabel 4.19 berikut.

Tabel 4.19. Ringkasan *CPU Usage* pukul 22:32 – 22:37 WIB.

waktu	rata-rata CPU Usage (%)	rata-rata CPU Free (%)
22:31	1.03	98.75
22:32	2.52	97.21
22:33	2.04	97.79
22:34	2.18	97.64
22:35	2.25	97.52

Dari data tabel diatas dapat dilihat bahwa terdapat kenaikan normal penggunaan CPU sebesar 1 – 2.5% dengan rata rata 2.0 %.

Selanjutnya dilakukan pemeriksaan *cpu load server* pada artefak “start_cpu_usage_20250510_231355.log” pada tanggal 2025-05-10 pukul 23:13 – 23.20 WIB dengan hasil seperti pada Tabel 4.20 berikut.

Tabel 4.20. Ringkasan *CPU Usage* pukul 23:13 – 23.20 WIB.

waktu	rata-rata CPU Usage (%)	rata-rata CPU Free (%)
23:13	3.53	95.72
23:14	1.56	97.62
23:15	1.65	97.77
23:16	1.68	97.76
23:17	3.59	95.74
23:18	1.65	97.63

Dari data Tabel diatas dapat dilihat bahwa terdapat kenaikan normal penggunaan CPU sebesar 1 – 3.5%.

Selanjutnya dilakukan pemeriksaan *cpu load server* pada artefak “start_cpu_usage_20250510_233219.log” pada 2025-05-10 pukul 23:31– 23:38 WIB seperti pada Tabel 4.21 berikut.

Tabel 4.21. Ringkasan *CPU Usage* pukul 23:31– 23:38 WIB.

waktu	rata-rata CPU Usage (%)	rata-rata CPU Free (%)
23:32	9.14	86.76
23:33	8.13	89.17
23:34	17.37	78.65
23:35	10.45	85.93
23:36	4.41	94.24
23:37	10.32	87.12

Dari data tabel diatas dapat dilihat bahwa terdapat kenaikan signifikan penggunaan CPU sebesar 8 - 17 % .

Selanjutnya dilakukan pemeriksaan *cpu load server* pada artefak “start_cpu_usage_20250511_000157.log” untuk melihat rata – rata penggunaan

CPU pada tanggal 2025-06-11 pukul 00:02 – 00.10 WIB seperti pada Tabel 4.22 berikut.

Tabel 4.22. Ringkasan *CPU Usage* pukul 00:02 – 00.10 WIB.

waktu	rata-rata CPU Usage (%)	rata-rata CPU Free (%)
00:01	1.25	97.98
00:02	2.23	97.10
00:03	20.18	52.91
00:04	50.10	47.93
00:05	50.08	47.96
00:06	50.24	48.05

Dari data tabel diatas dapat dilihat bahwa terdapat kenaikan signifikan penggunaan CPU pada sebesar 50 %.

c. Pemeriksaan *Memory Usage*

Dilakukan pemeriksaan *Memory Usage* pada artefak “start_memory_usage_20250510_222003.log” untuk melihat rata – rata penggunaan memory pada 2025-05-10 pukul 22:10 – 22.20 dengan hasil seperti pada Tabel 4.23 berikut.

Tabel 4.23. Rata – rata *Memory Usage* pukul 22:10 – 22.20 WIB.

Metrik Memory	Nilai Awal	Nilai Akhir	Penggunaan
Free Memory	2,531 MB	2,509 MB	22 MB
Buffer Memory	285 MB	285 MB	0 MB
Cache Memory	914 MB	915 MB	1 MB

Dari Tabel 4.23 dapat dilihat pemakaian *memory* normal pukul 22:10 – 22.20 WIB adalah 22 MB.

Selanjutnya Dilakukan pemeriksaan *Memory Usage* pada artefak “start_memory_usage_20250510_223116.log” untuk melihat rata – rata penggunaan Memory server pada 2025-05-10 pukul 22:32 – 22.37 WIB dengan hasil seperti pada tabel 4.24 berikut.

Tabel 4.24. Rata – rata *Memory Usage* pukul 22:32 – 22.37 WIB.

Metrik Memory	Nilai Awal	Nilai Akhir	Penggunaan
Free Memory	2,531 MB	2,505 MB	- 12 MB
Buffer Memory	285 MB	68 MB	0.2 MB
Cache Memory	914 MB	936 MB	0.1 MB

Dari Tabel 4.18 diatas dapat kita lihat pemakaian *Memory* cenderung mengalami penurunan dengan pemakaian 12 MB.

Selanjutnya Dilakukan pemeriksaan *Memory Usage* pada artefak “start_memory_usage_20250510_231355.log” untuk melihat rata – rata penggunaan *Memory* server pada 2025-05-10 pukul 23:13 – 23.20 WIB seperti pada Tabel 4.25 berikut.

Tabel 4.25. Rata – rata *Memory Usage* pukul 23:13 – 23.20 WIB.

Metrik Memory	Nilai Awal	Nilai Akhir	Penggunaan
Free Memory	2.441 MB	2.364 MB	- 77 MB
Buffer Memory	279 MB	279 MB	0 MB
Cache Memory	895 MB	954 MB	+ 59 MB

Dari Tabel 4.25 diatas dapat dilihat pemakaian *memory* meningkat signifikan sebesar 77 MB.

Selanjutnya Dilakukan pemeriksaan *Memory Usage* pada artefak “start_memory_usage_20250510_233219.log” untuk melihat rata – rata penggunaan *Memory* server pada 2025-05-10 pukul 23:31– 23:38 WIB seperti pada tabel 4.26 berikut.

Tabel 4.26. Rata – rata *Memory Usage* pukul 23:31– 23:38 WIB.

Metrik Memory	Nilai Awal	Nilai Akhir	Penggunaan
Free Memory	2,325 MB	2,309 MB	-15.8 MB
Buffer Memory	279.6 MB	279.7 MB	+ 0.1 MB
Cache Memory	965.9 MB	1,011.4 MB	+ 45.5 MB

Dari Tabel 4.26 diatas dapat kita lihat pemakaian *memory* cenderung normal sebesar 15.8 MB.

Selanjutnya Dilakukan pemeriksaan *Memory Usage* pada artefak “start_memory_usage_20250511_000157.log” untuk melihat rata – rata penggunaan Memory server pada tanggal 2025-06-11 pukul 00:02 – 00.10 WIB seperti pada Tabel 4.27 berikut.

Tabel 4.27. Rata – rata *Memory Usage* pukul 00:02 – 00.10 WIB.

Metrik Memory	Nilai Awal	Nilai Akhir	Penggunaan
Free Memory	2,434 MB	2,344 MB	- 89.5 MB
Buffer Memory	279.9 MB	279.9 MB	0 MB
Cache Memory	899.1 MB	943.6 MB	+ 44.5 MB

Dari Tabel 4.27 diatas dapat kita lihat pemakaian *memory* pada pukul 00:02 – 00.10 WIB naik secara signifikan mencapai 89.5 MB.

d. Pemeriksaan Trafik

Tahapan selanjutnya dilakukan pemeriksaan trafik yang menuju ke server target pada pada rentang waktu 2025-05-10 pukul 22:10 – 22.20 yang tercatat pada artefak “start_traffic_20250510_222003.pcap” dengan tampilan seperti terlihat pada Gambar 4.17 berikut.

7	2025-05-10 22:20:04.0	2001:db8:200:c01	2001:db8:200:a01	TCP	86	57442	→ 22	[ACK]	Seq=1	Ack=233	Win=499	Len=0	TSval=21567294	TSecr=3409248277
8	2025-05-10 22:20:04.0	2001:db8:200:c01	2001:db8:200:a01	TCP	86	57442	→ 22	[ACK]	Seq=1	Ack=277	Win=499	Len=0	TSval=21567295	TSecr=3409248277
33	2025-05-10 22:21:00.8	2001:db8:200:c01	2001:db8:200:a01	TCP	94	60280	→ 10000	[SYN]	Seq=0	Win=64000	Len=0	MSS=1440	SACK_PERM	TSval=21624180
34	2025-05-10 22:21:00.8	2001:db8:200:a01	2001:db8:200:c01	TCP	94	10000	→ 60280	[SYN, ACK]	Seq=0	Ack=1	Win=64260	Len=0	MSS=1440	SACK_PERM
35	2025-05-10 22:21:00.8	2001:db8:200:c01	2001:db8:200:a01	TCP	86	60280	→ 10000	[ACK]	Seq=1	Ack=1	Win=64096	Len=0	TSval=21624183	TSecr=3409305167
36	2025-05-10 22:21:01.0	2001:db8:200:c01	2001:db8:200:a01	HTTP	437	GET	/ HTTP/1.1							
37	2025-05-10 22:21:01.0	2001:db8:200:c01	2001:db8:200:a01	TCP	86	10000	→ 60280	[ACK]	Seq=1	Ack=352	Win=64128	Len=0	TSval=3409305280	TSecr=21624180
38	2025-05-10 22:21:01.0	2001:db8:200:c01	2001:db8:200:a01	TCP	117	10000	→ 60280	[PSH, ACK]	Seq=1	Ack=352	Win=64128	Len=91	TSval=3409305283	TSecr=21624180
39	2025-05-10 22:21:01.0	2001:db8:200:c01	2001:db8:200:a01	TCP	86	60280	→ 10000	[ACK]	Seq=352	Ack=1	Win=64096	Len=0	TSval=21624190	TSecr=3409305167
40	2025-05-10 22:21:01.0	2001:db8:200:a01	2001:db8:200:c01	TCP	209	10000	→ 60280	[PSH, ACK]	Seq=32	Ack=352	Win=64128	Len=123	TSval=3409305284	TSecr=21624180
41	2025-05-10 22:21:01.0	2001:db8:200:a01	2001:db8:200:c01	TCP	1514	10000	→ 60280	[ACK]	Seq=155	Ack=352	Win=64128	Len=1428	TSval=3409305285	TSecr=21624180
42	2025-05-10 22:21:01.0	2001:db8:200:a01	2001:db8:200:c01	HTTP	283	HTTP/1.0	200 Document follows (text/html)							
43	2025-05-10 22:21:01.0	2001:db8:200:c01	2001:db8:200:a01	TCP	86	10000	→ 60280	[RST, ACK]	Seq=1091	Ack=352	Win=64128	Len=0	TSval=3409305286	TSecr=21624180
44	2025-05-10 22:21:01.0	2001:db8:200:c01	2001:db8:200:a01	TCP	86	60280	→ 10000	[ACK]	Seq=352	Ack=155	Win=64096	Len=0	TSval=21624302	TSecr=3409305167
45	2025-05-10 22:21:01.0	2001:db8:200:a01	2001:db8:200:c01	TCP	74	10000	→ 60280	[RST]	Seq=155	Win=0	Len=0			
46	2025-05-10 22:21:01.2	2001:db8:200:c01	2001:db8:200:a01	TCP	94	60284	→ 10000	[SYN]	Seq=0	Win=64000	Len=0	MSS=1440	SACK_PERM	TSval=21624400
47	2025-05-10 22:21:01.2	2001:db8:200:c01	2001:db8:200:a01	TCP	94	10000	→ 60284	[SYN, ACK]	Seq=0	Ack=1	Win=64260	Len=0	MSS=1440	SACK_PERM
48	2025-05-10 22:21:01.2	2001:db8:200:a01	2001:db8:200:c01	TCP	86	60284	→ 10000	[ACK]	Seq=1	Ack=1	Win=64096	Len=0	TSval=21624495	TSecr=3409305476
49	2025-05-10 22:21:01.2	2001:db8:200:c01	2001:db8:200:a01	TLSv1	603	Client Hello								
50	2025-05-10 22:21:01.2	2001:db8:200:a01	2001:db8:200:c01	TCP	86	10000	→ 60284	[ACK]	Seq=1	Ack=518	Win=64128	Len=0	TSval=3409305486	TSecr=21624180
51	2025-05-10 22:21:01.2	2001:db8:200:c01	2001:db8:200:a01	TLSv1	1540	Server Hello, Change Cipher Spec, Application Data, Applicat.								
52	2025-05-10 22:21:01.2	2001:db8:200:c01	2001:db8:200:a01	TCP	86	60284	→ 10000	[ACK]	Seq=518	Ack=1455	Win=63488	Len=0	TSval=21624540	TSecr=3409305167
53	2025-05-10 22:21:01.2	2001:db8:200:c01	2001:db8:200:a01	TLSv1	166	Change Cipher Spec, Application Data								
54	2025-05-10 22:21:01.2	2001:db8:200:c01	2001:db8:200:a01	TLSv1	635	Application Data								
55	2025-05-10 22:21:01.2	2001:db8:200:c01	2001:db8:200:a01	TCP	635	[TCP Retransmission]	60284 → 10000 [PSH, ACK]	Seq=508	Ack=1455	Win=63488	Len=0			
56	2025-05-10 22:21:01.2	2001:db8:200:a01	2001:db8:200:c01	TCP	86	10000	→ 60284	[ACK]	Seq=1455	Ack=1147	Win=64128	Len=0	TSval=3409305560	TSecr=21624180

Gambar 4.17. Tampilan *Traffic Capture* pukul 22:10 – 22.20 WIB.

Setelah dilakukan *Summary* didapatkan hasil data trafik seperti pada Tabel 4.28 berikut.

Tabel 4.28. Koneksi ke server pukul 22.10 – 22.20 WIB.

Alamat sumber	Port tujuan	protocol	Sesi	Persentase
2001:db8:200:c01::2	22 (SSH)	TCP	42	6.4%
2001:db8:200:c01::2	10000 (WEBMIN)	TCP	607	92.2%

Dari Tabel 4.28 diatas terlihat bahwa hanya ada 1 host yang mengakses server dengan alamat 2001:db8:200:c01::2, protocol TCP dan port 22,1000 dengan total koneksi 658 sesi koneksi.

Selanjutnya dilakukan pemeriksaan trafik yang menuju ke server target pada pada rentang waktu 2025-05-10 pukul 22:32 – 22.37 WIB pada artefak “start_traffic_20250510_223116.pcap” seperti terlihat pada Gambar 4.18.

ip6.src == 2001::8 and ip6.dst == 2001:db8:200:a01::2						
No.	Time	Source	Destination	Protocol	Length	Info
2	2025-05-10 22:31:16.567796	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	86	57442 → 22 [ACK] Seq=1 Ack=125 Win=497 Len=0 TSval=22239847 TSecr=3
12	2025-05-10 22:31:20.504950	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
27	2025-05-10 22:31:41.217608	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
30	2025-05-10 22:32:01.904490	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
43	2025-05-10 22:32:22.776603	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
50	2025-05-10 22:32:43.450413	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
59	2025-05-10 22:33:04.131630	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
66	2025-05-10 22:33:25.120834	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
79	2025-05-10 22:33:45.872069	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
82	2025-05-10 22:34:06.605545	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
95	2025-05-10 22:34:27.256499	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
97	2025-05-10 22:34:27.471538	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	[TCP Spurious Retransmission] , Application Data
99	2025-05-10 22:34:27.684238	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	[TCP Spurious Retransmission] , Application Data
101	2025-05-10 22:34:28.124815	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	[TCP Spurious Retransmission] , Application Data
108	2025-05-10 22:34:47.899883	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
121	2025-05-10 22:35:08.658797	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	114	Application Data
123	2025-05-10 22:35:09.400321	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	94	57848 → 10000 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM=1 TSval=
125	2025-05-10 22:35:09.658719	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	94	57864 → 10000 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM=1 TSval=
128	2025-05-10 22:35:10.402364	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	94	[TCP Retransmission] 57848 → 10000 [SYN] Seq=0 Win=64800 Len=0 MSS=
130	2025-05-10 22:35:10.420772	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	86	57848 → 10000 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=22473693 TSecr=
131	2025-05-10 22:35:10.421045	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	86	[TCP Dup ACK 130#1] 57848 → 10000 [ACK] Seq=1 Ack=1 Win=64896 Len=0
132	2025-05-10 22:35:10.422488	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.3	707	Client Hello
136	2025-05-10 22:35:10.660758	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	94	[TCP Retransmission] 57864 → 10000 [SYN] Seq=0 Win=64800 Len=0 MSS=
138	2025-05-10 22:35:10.662413	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	86	57848 → 10000 [ACK] Seq=622 Ack=242 Win=64768 Len=0 TSval=22473937 TSecr=
139	2025-05-10 22:35:10.662637	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.3	166	Change Cipher Spec, Application Data
140	2025-05-10 22:35:10.662936	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.3	750	Application Data
143	2025-05-10 22:35:10.739331	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	86	57848 → 10000 [ACK] Seq=1366 Ack=497 Win=64640 Len=0 TSval=22474014
145	2025-05-10 22:35:10.989856	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	86	57848 → 10000 [ACK] Seq=1366 Ack=550 Win=64640 Len=0 TSval=22474263
147	2025-05-10 22:35:11.002115	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	86	57848 → 10000 [ACK] Seq=1366 Ack=804 Win=64512 Len=0 TSval=22474277
151	2025-05-10 22:35:11.710054	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	94	[TCP Retransmission] 57864 → 10000 [SYN] Seq=0 Win=64800 Len=0 MSS=

Gambar 4.18. Tampilan *Traffic Capture* pukul 22:02 – 00.10 WIB.

Setalah dilakukan *summary* pada artefak tersebut didapatkan hasil data trafik seperti pada tabel 4.29 berikut.

Tabel 4.29. Koneksi ke server pukul 22:32 – 22.37 WIB.

Alamat Sumber	Port Tujuan	protocol	sesi	Persentase
2001:db8:200:c01::2	10000 (WEBMIN)	TCP	142	100%

Dari tabel 4.29 diatas dapat diketahui bahwa hanya ada 1 host yang mengakses server dengan alamat 2001:db8:200:c01::2, protocol TCP, port 1000 serta terjadi penurunan sesi koneksi menjadi 142 sesi.

Selanjutnya dilakukan pemeriksaan trafik yang menuju ke server target pada 2025-05-10 pukul 23:13 – 23.20 yang terdapat pada artefak “start_traffic_20250510_231355.pcap” seperti terlihat pada Gambar 4.19.

No.	Time	Source	Destination	Protocol	Length	Info
460	2025-05-10 23:13:37.124831..	2001:db8:200:c01::2	2001:db8:200:a01::2	SSH	177	Client: Encrypted packet (len=44)
462	2025-05-10 23:13:37.131359..	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	133	57442 → 22 [ACK] Seq=45 Ack=37 Win=493 Len=0 TSval=24781872 TSecr=3412462072
463	2025-05-10 23:13:37.585950..	2001:db8:200:c01::2	2001:db8:200:a01::2	SSH	177	Client: Encrypted packet (len=44)
465	2025-05-10 23:13:37.590767..	2001:db8:200:c01::2	2001:db8:200:a01::2	TCP	133	57442 → 22 [ACK] Seq=89 Ack=97 Win=493 Len=0 TSval=24781533 TSecr=3412462532
467	2025-05-10 23:13:43.551598..	2001:db8:200:c01::2	2001:db8:200:a01::2	TLSv1.2	161	Application Data
469	2025-05-10 23:13:50.632670..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=0, hop limit=63 (no response found)
470	2025-05-10 23:13:50.633566..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=0, hop limit=64 (reply in 471)
473	2025-05-10 23:13:50.644841..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=1, hop limit=63 (reply in 474)
475	2025-05-10 23:13:50.644059..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=1, hop limit=64 (reply in 476)
477	2025-05-10 23:13:50.651929..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=2, hop limit=63 (reply in 478)
479	2025-05-10 23:13:50.652529..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=2, hop limit=64 (reply in 480)
481	2025-05-10 23:13:50.663200..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=3, hop limit=63 (reply in 482)
483	2025-05-10 23:13:50.664309..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=3, hop limit=64 (reply in 484)
485	2025-05-10 23:13:50.672532..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=4, hop limit=63 (reply in 486)
487	2025-05-10 23:13:50.673285..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=4, hop limit=64 (reply in 488)
489	2025-05-10 23:13:50.682847..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=5, hop limit=63 (reply in 490)
491	2025-05-10 23:13:50.683384..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=5, hop limit=64 (reply in 492)
493	2025-05-10 23:13:50.692827..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=6, hop limit=63 (reply in 494)
495	2025-05-10 23:13:50.693355..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=6, hop limit=64 (reply in 496)
497	2025-05-10 23:13:50.704200..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=7, hop limit=63 (reply in 498)
499	2025-05-10 23:13:50.704704..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=7, hop limit=64 (reply in 500)
501	2025-05-10 23:13:50.713358..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=8, hop limit=63 (reply in 502)
503	2025-05-10 23:13:50.713924..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=8, hop limit=64 (reply in 504)
505	2025-05-10 23:13:50.722978..	2001:db8:100:aa11::2	2001:db8:200:a01::2	ICMPv6	1109	Echo (ping) request id=0x6c59, seq=9, hop limit=63 (reply in 506)

Gambar 4.19. Tampilan *Traffic Capture* pukul 23.13 - 23.20 WIB.

Setelah dilakukan *summary* pada artefak tersebut didapatkan hasil data trafik seperti pada Tabel 4.30 berikut.

Tabel 4.30. Koneksi ke server pukul 23.13 - 23.20 WIB.

Alamat Sumber	Port Tujuan	<i>protocol</i>	Sesi	Persentase
2001:db8:200:c01::2	10000 (WEBMIN)	TCP	142	0.092%
2001:db8:100:aa11::2	-	ICMPv6 Echo (Ping)	74937	48.39%
2001:db8:100:dd::2	-	ICMPv6 Echo (Ping)	45458	29.35%
2001:db8:100:cc::2	-	ICMPv6 Echo (Ping)	34324	22.16%

Dari Tabel 4.30 diatas dapat diketahui bahwa terdapat 4 host yang mengakses server dengan sesi koneksi berjumlah 154,861 sesi dengan 154,719 merupakan paket ICMPv6 *Echo request* dengan ID yang sama (0x6c59).

Selanjutnya dilakukan pemeriksaan trafik yang menuju ke server target pada rentang waktu 2025-05-10 pukul 23:31– 23:38 pada artefak “start_traffic_20250510_231355.pcap” seperti terlihat pada Gambar 4.20 berikut.

No.	Time	Source	Destination	Protocol	Length	Info
4046.	372.465173015	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Dup ACK 40456981] 36291 → 10000 [ACK] Seq=2 Ack=2 Win=507 Len=0 TSval=3469115713 TSecr=3418397170
4046.	372.465481286	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Dup ACK 40457081] 42523 → 10000 [ACK] Seq=2 Ack=2 Win=507 Len=0 TSval=3469115713 TSecr=3418397169
4046.	378.573557743	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	121	46421 → 10000 [RST] Seq=2 Win=0 Len=0
4046.	378.573664258	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	121	35827 → 10000 [RST] Seq=2 Win=0 Len=0
4046.	378.573857345	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	121	46421 → 10000 [RST] Seq=2 Win=0 Len=0
4046.	378.573975757	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	121	35827 → 10000 [RST] Seq=2 Win=0 Len=0
4046.	380.626207880	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	33591 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.626571824	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	121	37611 → 10000 [RST] Seq=2 Win=0 Len=0
4046.	380.626923744	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	121	43157 → 10000 [RST] Seq=2 Win=0 Len=0
4046.	380.627270939	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	121	44045 → 10000 [RST] Seq=2 Win=0 Len=0
4046.	380.627724944	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	41407 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.627617340	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	46375 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.627999823	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	37265 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.628154836	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	41869 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.628426585	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	39065 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.628683711	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	42699 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.629138573	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Previous segment not captured] 42093 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.629478208	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Previous segment not captured] 33707 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.629829551	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Previous segment not captured] 36081 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.630151121	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Previous segment not captured] 43331 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.630359983	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Previous segment not captured] 38073 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.630795470	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	121	41883 → 10000 [RST] Seq=2 Win=0 Len=0
4046.	380.630781222	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Dup ACK 40463981] 31351 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.637064112	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	121	37611 → 10000 [RST] Seq=2 Win=0 Len=0
4046.	380.637423376	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	121	43157 → 10000 [RST] Seq=2 Win=0 Len=0
4046.	380.637734839	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	121	44045 → 10000 [RST] Seq=2 Win=0 Len=0
4046.	380.638056457	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Dup ACK 40464381] 41407 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.638156986	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Dup ACK 40464481] 46375 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.638704711	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Dup ACK 40464581] 37265 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.639077601	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Dup ACK 40464681] 41069 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.639441875	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Dup ACK 40464781] 39065 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.639846891	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Dup ACK 40464881] 42699 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.640305813	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Dup ACK 40464981] 42093 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599
4046.	380.640518883	2001:db8:200:a01::2	2001:db8:200:a01::2	TCP	133	[TCP Dup ACK 40465081] 33707 → 10000 [ACK] Seq=2 Ack=2 Win=64896 Len=0 TSval=3469123901 TSecr=3418431599

Gambar 4.20. Tampilan *Traffic Capture* pukul 23:31– 23:38 WIB.

Setelah dilakukan *summary* pada artefak serangan ketiga tersebut didapatkan hasil data trafik seperti pada Tabel 4.31 berikut.

Tabel 4.31. Koneksi ke server pukul 23:31– 23:38 WIB.

Alamat Sumber	Port Tujuan	protocol	Sesi	Persentase
2001:db8:200:c01::2	10000 (WEBMIN)	TCP	251	0.14%
2001:db8:100:aa11::2	10000 (WEBMIN)	TCP	101.284	56,76%
2001:db8:100:dd::2	10000 (WEBMIN)	TCP	22.122	12,40%
2001:db8:100:cc::2	10000 (WEBMIN)	TCP	54.810	30,71%

Dari Tabel 4.31 diatas dapat diketahui bahwa terdapat 4 host yang mengakses server dengan sesi koneksi berjumlah 222.708 sesi dengan 178.467 adalah TCP Port 10000 (*Webmin*). Hal tersebut menjadi indikator adanya anomali pada jalur koneksi yang menuju ke server target.

Selanjutnya dilakukan pemeriksaan trafik yang menuju ke webserver pada pada rentang waktu 2025-06-11 pukul 00:02 – 00.10 pada artefak “start_traffic_20250510_231355.pcap” seperti terlihat pada Gambar 4.21 berikut.

No.	Time	Source	Destination	Protocol	Length	Info
25	2025-05-11 00:02:51.765746531	2001:db8:100:aa11:218:dfff:fe6:d769	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:dfff:fe6:d769
26	2025-05-11 00:02:51.76574656	2001:db8:100:aa11:218:dfff:fece:8d17	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:dfff:fece:8d17
27	2025-05-11 00:02:51.765804043	2001:db8:100:aa11:218:81ff:fe23:c3a	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:81ff:fe23:c3a
28	2025-05-11 00:02:51.765825372	2001:db8:100:aa11:218:90ff:fe1:d3	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:90ff:fe1:d3
29	2025-05-11 00:02:51.765860477	2001:db8:100:aa11:218:93ff:fe1a:5167	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:93ff:fe1a:5167
30	2025-05-11 00:02:51.765912300	2001:db8:100:aa11:218:e7ff:fec3:1a61	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:e7ff:fec3:1a61
31	2025-05-11 00:02:51.765958635	2001:db8:100:aa11:218:30ff:fe21:ff64	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:30ff:fe21:ff64
32	2025-05-11 00:02:51.766013120	2001:db8:100:aa11:218:49ff:feb2:a047	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:49ff:feb2:a047
33	2025-05-11 00:02:51.766092563	2001:db8:100:aa11:218:a8ff:fe77:b07e	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:a8ff:fe77:b07e
34	2025-05-11 00:02:51.766149699	2001:db8:100:aa11:218:46ff:fe3d:95c7	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:46ff:fe3d:95c7
35	2025-05-11 00:02:51.766199425	2001:db8:100:aa11:218:61ff:feal:2f1	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:61ff:feal:2f1
36	2025-05-11 00:02:51.766248508	2001:db8:100:aa11:218:82ff:fe0f:c415	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:82ff:fe0f:c415
37	2025-05-11 00:02:51.766299406	2001:db8:100:aa11:218:2aff:fe15:7c11	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:2aff:fe15:7c11
38	2025-05-11 00:02:51.766495614	2001:db8:100:aa11:218:d8ff:fe96:7216	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:d8ff:fe96:7216
39	2025-05-11 00:02:51.766495713	2001:db8:100:aa11:218:b8ff:fe71:7a01	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:b8ff:fe71:7a01
40	2025-05-11 00:02:51.766495786	2001:db8:100:aa11:218:23ff:fe1a:48cb	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:23ff:fe1a:48cb
41	2025-05-11 00:02:51.766495959	2001:db8:100:aa11:218:92ff:fe9:49d8	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:92ff:fe9:49d8
42	2025-05-11 00:02:51.766548002	2001:db8:100:aa11:218:36ff:fedc:9f97	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:36ff:fedc:9f97
43	2025-05-11 00:02:51.766605953	2001:db8:100:aa11:218:7fff:feal:8801	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:7fff:feal:8801
44	2025-05-11 00:02:51.766700568	2001:db8:100:aa11:218:b1ff:fe4c:17db	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:b1ff:fe4c:17db
45	2025-05-11 00:02:51.766700668	2001:db8:100:aa11:218:61ff:fe93:ec3a	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:61ff:fe93:ec3a
46	2025-05-11 00:02:51.766743627	2001:db8:100:aa11:218:2aff:fe5f:50a2	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:2aff:fe5f:50a2
47	2025-05-11 00:02:51.766823583	2001:db8:100:aa11:218:d0ff:fecc:e3f4	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:d0ff:fecc:e3f4
48	2025-05-11 00:02:51.766829079	2001:db8:100:aa11:218:e5ff:fe2c:b77	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:e5ff:fe2c:b77
49	2025-05-11 00:02:51.766939289	2001:db8:100:aa11:218:25ff:fe09:4f5b	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:25ff:fe09:4f5b
50	2025-05-11 00:02:51.766939405	2001:db8:100:aa11:218:e7ff:feee:f367	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:e7ff:feee:f367
51	2025-05-11 00:02:51.766974439	2001:db8:100:aa11:218:90ff:fe7b:6841	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:90ff:fe7b:6841
52	2025-05-11 00:02:51.767036175	2001:db8:100:aa11:218:c8ff:fe7f:1c29	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:c8ff:fe7f:1c29
53	2025-05-11 00:02:51.767125780	2001:db8:100:aa11:218:13ff:fe08:633d	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:13ff:fe08:633d
54	2025-05-11 00:02:51.767170270	2001:db8:100:aa11:218:67ff:feb3:1f38	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:67ff:feb3:1f38
55	2025-05-11 00:02:51.767228169	2001:db8:100:aa11:218:76ff:feb2:2c63	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:76ff:feb2:2c63
56	2025-05-11 00:02:51.767275955	2001:db8:100:aa11:218:2eff:feeb:da53	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:2eff:feeb:da53
57	2025-05-11 00:02:51.767359494	2001:db8:100:aa11:218:f4ff:fe29:afdc	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:f4ff:fe29:afdc
58	2025-05-11 00:02:51.767399075	2001:db8:100:aa11:218:17ff:fe2a:43ab	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:17ff:fe2a:43ab
59	2025-05-11 00:02:51.767454831	2001:db8:100:aa11:218:27ff:fe28:b33b	2001:db8:200:a01::2	ICMPv6	133	Neighbor Advertisement 2001:db8:100:aa11:218:27ff:fe28:b33b

Gambar 4.21. Tampilan *Traffic Capture* pukul 00:02 – 00.10 WIB.

Setelah dilakukan *Summary* pada artefak serangan keempat tersebut didapatkan hasil data trafik seperti pada Tabel 4.32 berikut.

Tabel 4.32. Koneksi ke server pukul 00:02 – 00.10 WIB.

Alamat Sumber	Port Tujuan	protocol	Sesi	Persentase
2001:db8:200:c01::2	10000 (WEBMIN)	TCP	12	0.0094%
2001:db8:200:c01::2	22 (SSH)	TCP	4	0.0031%
2001:db8:100:aa11::/64	-	ICMPv6-NA	127.048	99.987%

Dari Tabel 4.32 diatas dapat diketahui bahwa ada 2 blok IPv6 yang mengakses server dengan sesi koneksi berjumlah 127.064 sesi dengan 127.048 adalah ICMPv6 *Network Advertisement*.

Selanjutnya hasil dari grafik dan tabel *Capture Bandwidth* (iftop), *Log CPU Usage* (mpstat), *Log Memory Usage* (vmstat) dan *traffic PCAP Server* (tcpdump) diatas akan dijadikan sebagai landasan analisis forensik menggunakan framework D4I pada poin 6.4.

4.6 Analisis Forensik

Pada tahap ini, dilakukan investigasi mendalam terhadap seluruh artefak digital yang telah berhasil diakuisisi selama serangan. Proses investigasi ini mengadopsi kerangka kerja D4I (*Digital Forensics framework for Reviewing and Investigating cyber-attacks*) yang dilakukan secara sistematis. Pada tahap ini, artefak-artefak yang telah diidentifikasi,

diakuisisi dan diperiksa pada bagian 4.6 akan dianalisis secara mendalam menggunakan dua pilar utama dari framework D4I (*Digital Forensics framework for Reviewing and Investigating cyber-attacks*) dengan langkah – langkah berikut:

- Fase 1 (*Examination*) yang terdiri dari aktifitas kategorisasi, pemetaan dan korelasi (*Choose, Identify & Correlate*) artefak menggunakan *Cyber Kill Chain* (CKC).
- Fase 2 (*Analysis*) yang terdiri dari aktifitas investigasi meliputi pembuatan visualisasi/diagram rantai artefak dan penjelasan rantai artefak (*Construct CoA, Analyze CoA*).

4.6.1 Fase 1 - Pemetaan Artefak ke Fase *Cyber Kill Chain* (CKC)

Setelah dilakukan pemeriksaan awal artefak digital yang dapat dilihat pada tabel dan grafik pada tahap 4.6, selanjutnya setiap artefak kunci akan dipetakan ke dalam tujuh (7) fase *Cyber Kill Chain* (CKC) yang relevan. Proses pemetaan ini bertujuan untuk menyaring, mengidentifikasi serta mengkategorikan bukti digital sesuai dengan tahapan serangan yang terjadi, sesuai dengan pilar pertama framework D4I. Model CKC standar pada dasarnya dirancang untuk melacak serangan intrusi seperti APT atau serangan *malware* yang memiliki alur linier. Serangan DDoS khususnya *flooding* volumetrik memiliki modus operandi yang berbeda. Oleh karena itu beberapa fase CKC diadaptasi agar relevan dengan skenario serangan DDoS IPv6 meliputi:

1. *Reconnaissance* (R): Aktivitas pemindaian oleh penyerang untuk mengidentifikasi target IPv6 yang valid.
2. *Weaponization* (W): Persiapan tools serangan pada komputer attacker dan zombie.
3. *Delivery* (D): Pengiriman banjir paket masif. Artefak utamanya adalah deteksi awal lonjakan bandwidth di router dan log PCAP yang menunjukkan trafik serangan.
4. *Exploitation* (E): Fase ini diadaptasi dari eksploitasi kerentanan software menjadi eksploitasi protokol (ICMPv6) dan sumber daya (CPU/Memori). Artefak utamanya adalah lonjakan CPU pada router atau server.
5. *Installation* (I): Keberadaan tools serangan yang telah disiapkan pada host zombie.
6. *Command & Control* (C2): Dalam skenario ini, tidak ada artefak langsung yang teridentifikasi, seperti yang juga dicatat dalam tabel pemetaan.

7. *Actions on Objective* (A): Tujuan akhir yaitu kelumpuhan layanan (*denial of service*). Artefak utamanya adalah metrik yang membuktikan kelumpuhan (misal: CPU 100%, penurunan drastis trafik wajar atau kehabisan memori)

Pada kasus serangan pertama, artefak yang telah teridentifikasi dipetakan kedalam fase CKC seperti terlihat pada Tabel 4.33. berikut.

Tabel 4.33. Pemetaan Artefak ke Fase *Cyber Kill Chain* (CKC) Serangan pertama.

Fase CKC	Kategori Artefak	Artefak Teridentifikasi
<i>Reconnaissance</i> (R)	Log Sistem / Trafik Jaringan	Adanya Log pada router yang menampilkan aktivitas <i>scanning</i> atau <i>probing</i> dari alamat IP penyerang yakni, 2001:db8:100:aa11::2, 2001:db8:100:cc::2, 2001:db8:100:dd::2 sebelum waktu serangan yang mengindikasikan upaya pengintaian awal oleh penyerang untuk mengidentifikasi target atau kerentanan,
<i>Weaponization</i> (W)	Informasi Alat Serangan	Penggunaan tools serangan berbasis IPv6 pada komputer penyerang dan zombie yang mengakibatkan adanya lonjakan CPU load pada router.
<i>Delivery</i> (D)	Trafik Jaringan (File PCAP)	Terjadi lonjakan <i>bandwidth</i> yang mengarah ke server (rata-rata 30-60 Mbps) pada periode serangan pada tanggal 2025-05-10 pukul 22:30 - 22:40 WIB dan terdapat log pengiriman paket serangan dalam volume tinggi dari sumber penyerang/zombie ke jaringan target.
	Data Paket (PCAP)	Adanya paket ICMPv6 Type 137 (Redirect Message) yang dikirimkan ke server target (2001:db8:200:a01::2) mengonfirmasi jenis paket serangan dan teknik serangan spoofing yang digunakan.

<i>Exploitation (E)</i>	Metrik Kinerja Sistem (CPU, Memori)	Lonjakan penggunaan CPU Router (80-100%) dan peningkatan memori Router (sekitar 238MB) pada periode serangan menunjukkan beban sumber daya yang berlebihan pada router yang menjadi indikator bahwa serangan berhasil memengaruhi kemampuan sistem untuk memproses data secara normal.
<i>Installation (I)</i>	Tidak teridentifikasi	Tidak ada artefak yang teridentifikasi secara langsung karena serangan DDoS berbasis <i>flooding</i> tidak melibatkan instalasi <i>malware</i> persisten atau <i>backdoor</i> pada sistem korban.
<i>Command dan Control (C2)</i>	Log Sistem / File Sistem	Tidak ada artefak yang teridentifikasi secara langsung dikarenakan serangan DDoS berbasis <i>flooding</i> tidak melibatkan instalasi <i>malware</i> persisten atau <i>backdoor</i> pada sistem korban.
<i>Actions on Objective (A):</i>	Ketersediaan Layanan / Kinerja	Terjadi penurunan <i>session</i> dan <i>bandwidth</i> server target (27.4 kb <i>upload</i> dan 9.27 kb <i>download</i>) pada periode serangan yang menyebabkan server tidak dapat diakses yang menunjukkan adanya serangan yang mengganggu ketersediaan atau fungsionalitas sistem.
	<i>Timestamp</i> Kejadian	Menetapkan garis waktu terjadinya gangguan layanan. <i>Timestamp</i> serangan pertama pada tanggal 2025-05-10 pukul 22:32 - 22:37 WIB.
	Identitas Sumber & Target	Mengidentifikasi aktor yang terlibat dalam kejadian serangan. Alamat IPv6 Attacker/Zombie 2001:db8:100:aa11::2, 2001:db8:100:cc::2, 2001:db8:100:dd::2. Sedangkan target serangan adalah 2001:db8:200:a01::2

Selanjutnya pada serangan kedua, artefak yang didapatkan dipetakan kedalam fase CKC seperti terlihat pada tabel 4.34.

Tabel 4.34. Pemetaan Artefak ke Fase *Cyber Kill Chain* (CKC) Serangan kedua.

Fase CKC	Kategori Artefak	Artefak Teridentifikasi
<i>Reconnaissance</i> (R)	Log Sistem / Trafik Jaringan	Log jaringan yang menunjukkan aktivitas <i>scanning</i> atau <i>probing</i> dari alamat IP 2001:db8:100:aa11::2, 2001:db8:100:cc::2, 2001:db8:100:dd::2 sebelum waktu serangan mengindikasikan upaya penyerang untuk mengidentifikasi target atau kerentanan.
<i>Weaponization</i> (W)	Informasi Serangan Alat	Penggunaan tools serangan berbasis IPv6 pada komputer penyerang dan zombie yang mengakibatkan adanya lonjakan CPU load pada router.
<i>Delivery</i> (D)	Trafik Jaringan (PCAP)	Adanya lonjakan <i>bandwidth</i> router yang mengarah ke server rata-rata 1-3 Mbps pada periode serangan menjadi indikator pengiriman paket serangan dalam volume tinggi dari penyerang/zombie ke target
	Data Paket (PCAP)	Terdapat 154.719 paket ICMPv6 Echo Request (Ping) dari IP 2001:db8:100:aa11::2, 2001:db8:100:dd::2 dan 2001:db8:100:cc::2 dengan ID yang sama (0x6c59) dalam <i>Traffic Capture</i> server target.
<i>Exploitation</i> (E)	Metrik Kinerja Sistem (CPU, Memori)	Lonjakan signifikan penggunaan CPU Router (86-100%) dan peningkatan memori Router (230-237MB) pada periode serangan menunjukkan beban yang berlebihan akibat upaya eksploitasi fitur protokol atau volume trafik yang membanjiri.

<i>Installation (I)</i>	-	Tidak ada artefak yang teridentifikasi secara langsung dikarenakan Serangan DDoS berbasis <i>flooding</i> ICMPv6 umumnya tidak melibatkan instalasi <i>malware</i> persisten atau <i>backdoor</i> pada sistem korban
<i>Command dan Control (C2)</i>	-	Tidak ada artefak yang teridentifikasi secara langsung dikarenakan serangan DDoS <i>flooding</i> ICMPv6 biasanya tidak memerlukan saluran <i>Command and Control</i> berkelanjutan setelah paket diluncurkan.
<i>Actions on Objective (A)</i>	Ketersediaan Layanan	Kenaikan drastis <i>bandwidth</i> server target (28.5 Mb <i>upload</i> dan 28.5 Mb <i>download</i>) dan penurunan kinerja layanan pada server target yang disebabkan oleh pembanjiran trafik.
	Timestamp Kejadian	<i>Timestamp</i> dari semua anomali yang teridentifikasi pada 2025-05-10 pukul 23:13 - 23:20 WIB
	Identitas Sumber & Target	Mengidentifikasi aktor yang terlibat dalam kejadian serangan. Alamat IPv6 penyerang/zombie (2001:db8:100:aa11::2, 2001:db8:100:cc::2, 2001:db8:100:dd::2) dan alamat target (2001:db8:200:a01::2)

Selanjutnya pada serangan ketiga, artefak yang didapatkan dipetakan kedalam fase CKC seperti terlihat pada Tabel 4.35. berikut.

Tabel 4.35. Pemetaan Artefak ke Fase *Cyber Kill Chain* (CKC) Serangan ketiga.

Fase CKC	Kategori Artefak	Keterangan
<i>Reconnaissance (R)</i>	Log Sistem Jaringan / Trafik Jaringan	Log jaringan yang menunjukkan aktivitas scanning atau probing dari alamat IP 2001:db8:100:aa11::2, 2001:db8:100:cc::2, 2001:db8:100:dd::2 sebelum waktu serangan

		mengindikasikan upaya penyerang untuk melihat port yang terbuka (seperti port 10000 untuk Webmin) sebelum meluncurkan serangan.
<i>Weaponization (W)</i>	Informasi Alat Serangan	Penggunaan <i>tool</i> yang mampu melakukan TCP <i>connect flood</i> secara efisien ke port target.
<i>Delivery (D)</i>	Trafik Jaringan (PCAP)	Lonjakan <i>bandwidth</i> router yang mengarah ke server (rata-rata 1.3-1.5 Mbps) pada periode serangan tanggal 2025-05-10 pukul 24:01 - 24:10
		Deteksi 178.467 sesi koneksi TCP Port 10000 (Webmin) dari 4 host sumber 2001:db8:200:c01::2, 2001:db8:100:aa11::2, 2001:db8:100:dd::2, 2001:db8:100:cc::2) dalam <i>Traffic Capture</i> server target.
<i>Exploitation (E)</i>	Metrik Kinerja Sistem (CPU, Memori)	Lonjakan penggunaan CPU Router (81-99%) dan peningkatan memori Router (230-235MB) pada periode serangan menunjukkan beban sumber daya yang berlebihan pada perangkat jaringan akibat upaya eksploitasi dan volume trafik yang membanjiri.
	Respons Sistem / Metrik Kinerja	Kenaikan signifikan penggunaan CPU server target (8-17% dengan rata-rata 10%) pada periode serangan. Mengindikasikan bahwa server target dipaksa untuk memproses koneksi TCP dalam jumlah besar, yang membebani CPU
<i>Installation (I)</i>	-	Tidak ada artefak yang teridentifikasi secara langsung dari jenis serangan DDoS berbasis TCP <i>connect flood</i> karena tidak melibatkan

		instalasi <i>malware</i> persisten atau <i>backdoor</i> pada sistem korban.
<i>Command dan Control</i> (C2)	-	Tidak ada artefak yang teridentifikasi secara langsung dari jenis serangan DDoS TCP <i>connect flood</i> karena tidak memerlukan saluran <i>Command and Control</i> berkelanjutan setelah paket diluncurkan.
<i>Actions on Objective</i> (A):	Ketersediaan Layanan / Kinerja	Kenaikan drastis pada <i>bandwidth</i> server target (17.9 Mb <i>upload</i> dan 15.2 Mb <i>download</i>) akibat volume paket yang tinggi
	Timestamp Kejadian	<i>Timestamp</i> dari semua anomali yang teridentifikasi pada tanggal 2025-05-10 pukul 23:31 - 23:38 WIB
	Identitas Sumber & Target	Mengidentifikasi aktor yang terlibat dalam kejadian serangan. Alamat IPv6 penyerang/zombie (2001:db8:100:aa11::2, 2001:db8:100:cc::2, 2001:db8:100:dd::2) dan alamat target (2001:db8:200:a01::2)

Selanjutnya pada serangan keempat, artefak yang didapatkan dipetakan kedalam fase CKC seperti terlihat pada Tabel 4.36. berikut.

Tabel 4.36. Pemetaan Artefak ke Fase *Cyber Kill Chain* (CKC) Serangan keempat.

Fase <i>Cyber Kill Chain</i> (CKC)	Kategori Artefak	
<i>Reconnaissance</i> (R)	Log Sistem Jaringan / Trafik Jaringan	Log firewall atau IDS/IPS yang menampilkan aktivitas <i>scanning</i> atau <i>probing</i> dari alamat IP penyerang/zombie sebelum serangan teridentifikasi.
<i>Weaponization</i> (W)	D4I	Penggunaan pada Komputer Penyerang dan Zombie yang mampu melakukan

		<i>flood</i> paket ICMPv6 Neighbor Advertisement (NA) palsu.
<i>Delivery</i> (D)	Trafik Jaringan (PCAP)	Lonjakan <i>bandwidth</i> router yang mengarah ke server (3 Mbps) pada periode serangan 2025-05-11 pukul 00:02 - 00:10 WIB).
	Data Paket (PCAP)	Terdeteksi 127.048 sesi ICMPv6 Neighbor Advertisement (NA) dari blok IPv6 2001:db8:100:aa11::/64 dalam <i>Traffic Capture</i> server target.
<i>Exploitation</i> (E)	Metrik Kinerja Sistem (CPU, Memori)	Lonjakan penggunaan CPU Router (21-100%) dan peningkatan memori Router (223-226MB) dan Kenaikan signifikan penggunaan CPU server target (2-50%) dengan rata-rata 39.59%. serta peningkatan penggunaan memori server target sebesar 89.5 MB pada periode serangan
<i>Installation</i> (I)	-	Tidak ada artefak yang teridentifikasi secara langsung karena serangan DDoS berbasis <i>flooding</i> ICMPv6 NA umumnya tidak melibatkan instalasi <i>malware</i> persisten pada sistem korban
<i>Command dan Control</i> (C2)	-	Tidak ada artefak yang teridentifikasi secara langsung karena tujuan penyerang adalah membebani sumber daya sistem target.
<i>Actions on Objective</i> (A):	Ketersediaan Layanan / Kinerja	Kenaikan drastis <i>bandwidth</i> server target (4.71 Mb <i>download</i>) akibat volume paket yang tinggi serta penurunan kinerja sistem yang signifikan akibat dari lonjakan CPU dan memori.

	Timestamp Kejadian	<i>Timestamp</i> dari anomali yang teridentifikasi pada tanggal 2025-05-11 pukul 00:02 - 00:10 WIB.
	Identitas Sumber & Target	Alamat IPv6 penyerang adalah (2001:db8:100:aa11::/64) dan target (2001:db8:200:a01::2)

Setelah semua artefak teridentifikasi dan terpetakan ke dalam fase CKC yang relevan, selanjutnya investigasi dilanjutkan ke fase 2 dari framework D4I yakni menganalisis korelasi antar artefak-artefak ini untuk membangun Rantai Artefak (CoA) dan merekonstruksi serangan.

4.6.2 Fase 2 - Analisis Investigasi

Setelah dilakukan pemetaan dan identifikasi artefak ke dalam fase CKC, selanjutnya dilakukan analisis dan investigasi untuk merekonstruksi serangan dan memahami modus operandi yang mencakup langkah-langkah (3) *Correlate*, (4) *Construct* CoA, dan (6) *Analyze* CoA.

1. Korelasi Artefak (*Correlate*)

Langkah ini bertujuan untuk menemukan hubungan dan membangun garis waktu (*timeline*) kejadian yang terpadu. Dalam konteks investigasi ini, korelasi utama dilakukan dengan menautkan tiga atribut data utama yang diperoleh, yakni.

- Timestamp* (Waktu): Menghubungkan log performa (CPU/Memori) pada router dan server dengan log trafik jaringan (PCAP) yang terjadi pada rentang waktu yang identik.
- Alamat Jaringan / IPv6 *Address* (Sumber & Tujuan): Menghubungkan alamat IPv6 sumber (Attacker/Zombie) dan tujuan (Server/Router) yang sama di berbagai artefak.
- Karakteristik Serangan (Jenis Paket & Dampak): Menghubungkan jenis paket serangan spesifik (misal: ICMPv6 Tipe 137 atau Tipe 136) dengan dampak spesifik yang terukur (misal: lonjakan CPU 100% atau kelelahan memori).

Korelasi ini dapat membantu investigator memastikan bahwa dua peristiwa terjadi bersamaan dan membuktikan hubungan sebab-akibat (kausalitas) antara paket serangan dan dampak yang ditimbulkan. Analisis korelasi pada setiap serangan adalah sebagai berikut:

1. Serangan Pertama (*Redirect Flood*).

Ditemukan adanya korelasi pada timestamp serangan (22:32 - 22:37 WIB) dengan tiga artefak kunci sebagai berikut.

- a. Terdapat *flooding* paket ICMPv6 Tipe 137 (Redirect) yang teridentifikasi di file PCAP.
- b. Terdapat lonjakan pada CPU Router hingga 80-100%.
- c. Penurunan drastis bandwidth dan sesi pada Server Target.

Korelasi ini membuktikan bahwa serangan Tipe 137 secara efektif mengeksploitasi router sebagai *bottleneck*, melumpuhkan sumber dayanya dan menyebabkan denial of service ke server target.

2. Serangan kedua (*Echo Flood*)

Ditemukan korelasi pada timestamp 23:13 - 23:20 WIB dengan tiga artefak kunci sebagai berikut.

- a. Terdapat 154.719 paket ICMPv6 *Echo Request* (Tabel 4.16) yang berasal dari tiga alamat IPv6 (2001:db8:100:aa11::2, 2001:db8:100:dd::2, 2001:db8:100:cc::2).
- b. Terdapat Lonjakan pada CPU Router hingga 86-100%.
- c. Lonjakan bandwidth pada Server Target hingga 57.0 Mb.

Korelasi ini membuktikan adanya serangan volumetrik terdistribusi yang berhasil mengeksploitasi sumber daya CPU router dan membanjiri bandwidth server.

3. Serangan ketiga (*TCP Connect Flood*)

Ditemukan korelasi pada timestamp 23:31 - 23:38 WIB dengan tiga artefak kunci sebagai berikut:

- a. Terdapat 178.467 sesi TCP yang menargetkan Port 10000 (Webmin) seperti terlihat pada Tabel 4.17.
- b. Terdapat Lonjakan CPU Router hingga 81-99% seperti terlihat pada Tabel 4.10.
- c. Terdapat Lonjakan CPU Server Target yang signifikan (rata-rata 10%, naik dari 1.25%) seperti terlihat pada Tabel 4.15.

Korelasi ini menunjukkan bahwa serangan ketiga memiliki karakteristik yang lebih canggih (lapisan aplikasi) dimana eksploitasi tidak hanya terjadi pada router tetapi juga berhasil membebani proses pada server target.

4. Serangan keempat (*Neighbor Advertisement Flood*).

Ditemukan korelasi pada timestamp 00:02 - 00:10 WIB dengan tiga artefak kunci sebagai berikut:

- a. Terdapat 127.048 paket ICMPv6 NA (Tipe 136) dari blok alamat 2001:db8:100aa11::/64 seperti terlihat pada Tabel 4.18.
- b. Adanya dampak eksploitasi pada Server Target meliputi lonjakan CPU Server hingga 50% seperti terlihat pada Tabel 4.16 dan peningkatan penggunaan Memori Server sebesar 89.5 MB seperti terlihat pada Tabel 4.21.

Korelasi ini membuktikan bahwa serangan *Neighbor Advertisement Flood* berhasil mengeksploitasi sumber daya endpoint (server) secara langsung dengan membanjiri dan meracuni Neighbor Cache server yang berdampak pada konsumsi memori dan CPU.

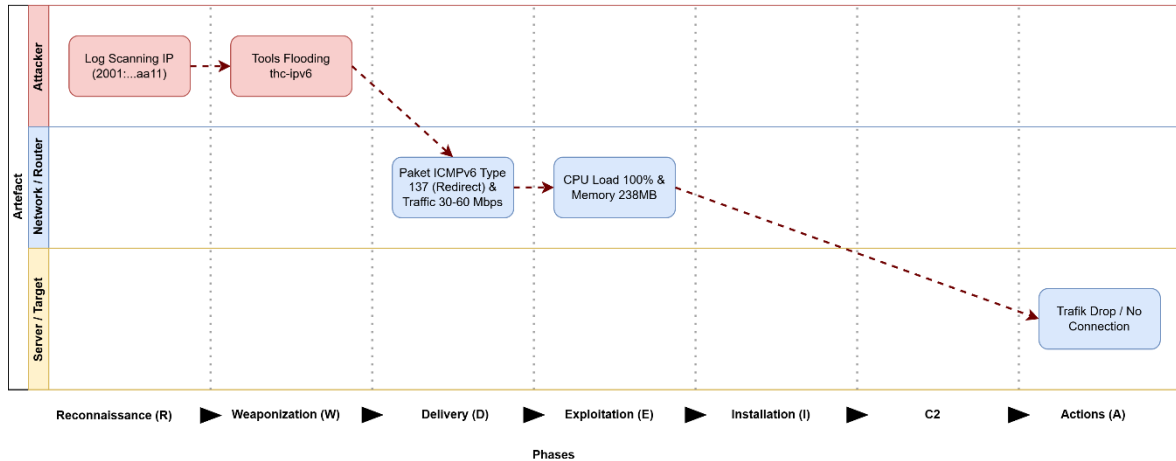
Dari korelasi yang telah teridentifikasi pada empat serangan diatas, diketahui "mata rantai" yang valid untuk menghubungkan artefak-artefak yang tadinya terisolasi. Langkah selanjutnya adalah membangun Rantai Artefak (*Construct CoA*) untuk memvisualisasikan alur serangan secara utuh.

2. Konstruksi Rantai Artefak (*Construct CoA*)

Setelah artefak-artefak dari setiap skenario serangan berhasil dikorelasikan berdasarkan timestamp, alamat dan karakteristiknya, investigasi dilanjutkan ke langkah keempat dari framework D4I, yaitu *Construct CoA* (Membangun Rantai Artefak).

Tujuan utama dari langkah ini adalah untuk menyusun mata rantai (*Chain of Artefact*) dari artefak yang telah terkorelasi menjadi sebuah alur visual yang utuh. Tahapan ini merupakan tahapan yang fundamental untuk merepresentasikan modus operandi serangan dan jejak digital yang ditinggalkan penyerang secara sistematis. Pada penelitian ini, Rantai Artefak (CoA) dibangun pada setiap kejadian serangan dengan visualisasi rantai artefak sebagai berikut.

a. Visualisasi rantai artefak (CoA) serangan pertama / *ICMPv6 Redirect Flood*

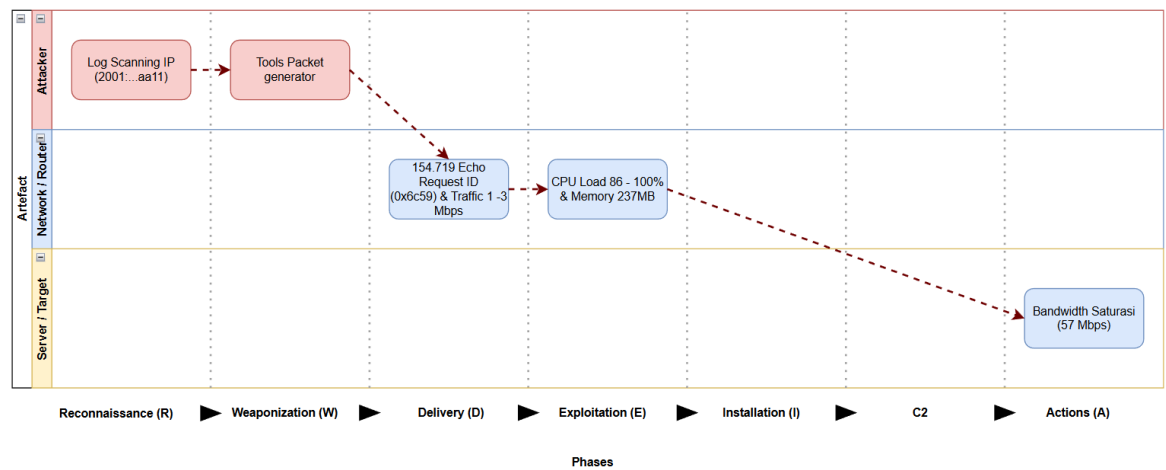


Gambar 4.22. Hasil konstruksi CoA untuk serangan pertama / *ICMPv6 Redirect Flood*

Berdasarkan visualisasi Rantai Artefak pada Gambar 4.22, modus operandi serangan *ICMPv6 Redirect Flood* dapat direkonstruksi secara utuh. Rantai serangan (garis merah putus-putus) menunjukkan alur sebagai berikut:

1. Serangan dimulai dengan aktivitas pemindaian (*Reconnaissance*) yang diikuti oleh eksekusi tools thc-ipv6 pada fase *Weaponization*.
2. Titik kritis terjadi pada fase *Delivery* di mana tools tersebut membanjiri jaringan dengan paket spesifik ICMPv6 Tipe 137 (*Redirect*). Artefak ini berkorelasi vertikal dengan lonjakan bandwidth router (30-60 Mbps).
3. Rantai serangan menunjukkan garis langsung dari paket Tipe 137 menuju lonjakan CPU Router hingga 100% pada fase *Exploitation*. Hal ini membuktikan bahwa router menjadi *bottleneck* karena dipaksa memproses pesan *redirect* palsu dalam jumlah masif. Sedangkan penggunaan memori (238MB) merupakan dampak sekunder.
4. Akibat habisnya sumber daya pemrosesan (CPU) pada router sehingga lalu lintas yang sah tidak dapat diteruskan ke server target.
5. (*Actions on Objective*) dampak dari serangan tersebut berupa penurunan trafik secara drastis pada server target yang mengonfirmasi terjadinya kondisi *Denial of Service* (DoS).

b. Visualisasi rantai artefak (CoA) serangan kedua / *ICMPv6 Echo Request Flood*



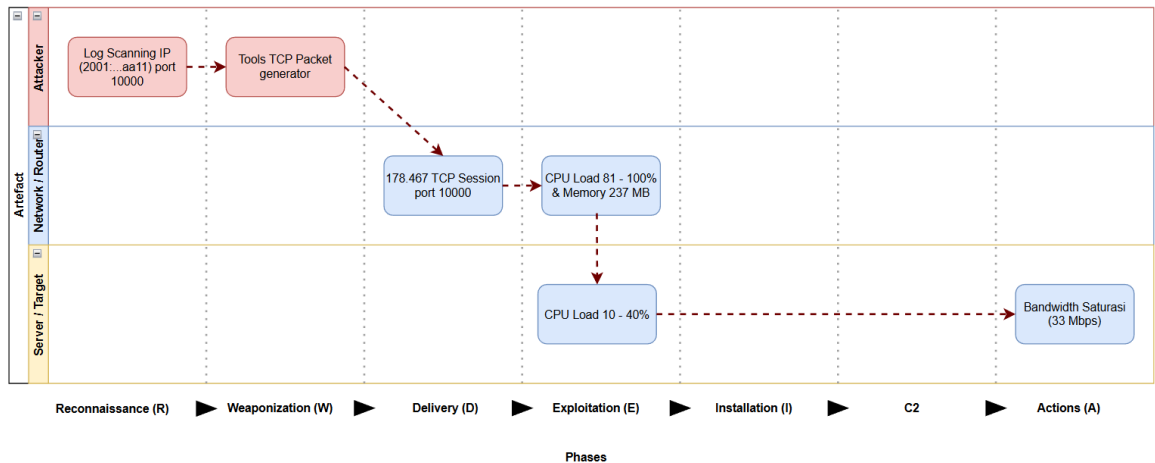
Gambar 4.23. Hasil konstruksi CoA untuk serangan kedua / *ICMPv6 Echo Request Flood*

Berdasarkan visualisasi Rantai Artefak pada Gambar 4.23, modus operandi serangan *ICMPv6 Echo Request Flood* menunjukkan karakteristik serangan DDoS volumetrik. Alur yang terbentuk dari rantai serangan (garis merah putus-putus) adalah sebagai berikut:

1. Penyerang melakukan pengintaian / *Reconnaissance* untuk menentukan target.
2. Pada fase *Weaponization*, penyerang menggunakan tools packet generator / *fping6* atau sejenis yang mengindikasikan motif *attacker* untuk membanjiri target dengan paket ICMPv6 yang valid secara protokol namun masif secara volume.
3. Pada fase *Delivery*, terdeteksi pengiriman 154.719 paket *Echo Request* dengan ID identik (0x6c59). Artefak ini berkorelasi dengan peningkatan bandwidth router (1-3 Mbps).
4. Pada fase *Exploitation*. Paket ICMPv6 tersebut menyebabkan lonjakan CPU Router hingga 100%. Hal tersebut membuktikan bahwa router terbebani oleh proses routing dan inspeksi paket ICMPv6 dalam jumlah besar. Disisi lain, penggunaan memori router (237MB) merupakan dampak sekunder.
5. Pada fase *Actions*. Artefak menunjukkan kenaikan drastis bandwidth pada server target hingga total 57 Mbps (28.5 Mbps upload/download).

Dari Visualisasi CoA diatas dapat disimpulkan bahwa serangan *Echo Request Flood* berhasil menciptakan kondisi *Denial of Service* melalui saturasi bandwidth di sisi server dan kelelahan CPU di sisi router.

c. Analisis rantai artefak (CoA) skenario ketiga / *TCP Connect Flood*



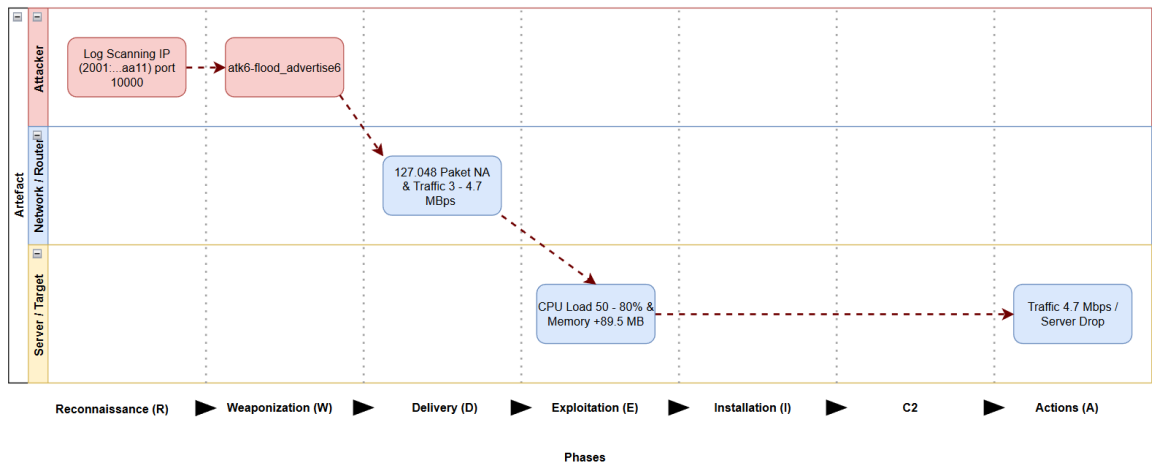
Gambar 4.24. Hasil konstruksi CoA untuk serangan ketiga / *TCP Connect Flood*

Visualisasi Rantai Artefak pada Gambar 4.24 mengungkapkan pergeseran karakteristik serangan dari volumetrik murni menjadi serangan berbasis protokol (*Protocol Abuse*). Alur kausalitas yang terbentuk adalah:

1. Berbeda dengan skenario sebelumnya, rantai dimulai dengan fase *Reconnaissance* yang spesifik menargetkan TCP Port 10000 (*Webmin*) diikuti dengan penggunaan
2. Pada fase *Weaponization*, penyerang menggunakan tool packet generator untuk mengirim paket DDoS berbasis TCPv6.
3. Pada fase *Delivery*, terdeteksi 178.467 sesi koneksi TCP yang membanjiri jaringan. Artefak ini berkorelasi dengan peningkatan bandwidth router sekitar 1.5 Mbps.
4. Titik kritis terlihat pada fase *Exploitation*. Rantai serangan menunjukkan percabangan dampak. Serangan ini tidak hanya menyebabkan lonjakan CPU Router (99%), tetapi juga membebani CPU Server Target (kenaikan rata-rata menjadi 10%). Hal tersebut menunjukkan bahwa serangan *TCP Connect Flood* memaksa server untuk mengalokasikan sumber daya guna memproses handshake TCP yang masuk.
5. Pada fase *Actions*, saturasi terjadi pada bandwidth server target dengan total trafik mencapai 33.1 Mb (Upload+Download), yang mengganggu akses terhadap layanan Webmin.

Dari Visualisasi CoA ini mengonfirmasi bahwa serangan *TCP Connect Flood* memiliki dampak hybrid, yaitu membebani infrastruktur jaringan (*Router*) sekaligus membebani sumber daya pemrosesan pada endpoint (*Server*).

d. Analisis rantai artefak (CoA) skenario keempat / *DDoS NA*



Gambar 4.25. Hasil konstruksi CoA untuk serangan keempat / *DDoS NA*

Visualisasi Rantai Artefak pada Gambar 4.25 memperlihatkan karakteristik serangan *Protocol Exploitation* yang menargetkan mekanisme *Stateless Address Autoconfiguration* (SLAAC) pada IPv6. Berdasarkan rantai yang terbentuk, serangan ini memiliki modus operandi sebagai berikut:

1. Pada fase Delivery, artefak menunjukkan adanya injeksi 127.048 paket *Neighbor Advertisement* (NA) palsu. Fakta menarik dari kasus ini, artefak pendukung (*Bandwidth Router*) hanya menunjukkan angka 3 Mbps. Hal tersebut membuktikan bahwa serangan ini tidak mengandalkan volume bandwidth yang besar untuk melumpuhkan target seperti pada skenario pertama dan kedua.
2. Adanya pergeseran target eksploitasi serangan yang ditunjukan oleh CoA. Jika pada skenario pertama dan kedua, garis rantai CoA pada fase *Exploitation* menunjuk CPU Router, pada skenario keempat, garis rantai terhubung langsung ke CPU Server yang menunjukkan kenaikan 50 - 80% dan Memori Server (+89.5 MB).
3. Korelasi vertikal antara paket NA dan lonjakan memori server mengindikasikan terjadinya *Resource Exhaustion*. Sistem operasi server dipaksa memproses ribuan klaim alamat palsu (*NA Spoofing*) yang membanjiri tabel *Neighbor Cache*. Proses validasi dan pembaruan tabel ini mengonsumsi siklus CPU dan memori secara intensif. Akibat habisnya sumber daya komputasi untuk memproses paket sampah tersebut, server gagal melayani permintaan yang sah, yang dikonfirmasi oleh artefak pada fase Actions.

Secara keseluruhan, penerapan langkah *Construct and Analyze CoA* pada keempat skenario berhasil membedakan karakteristik serangan secara presisi pada masing – masing skenario dengan keterangan sebagai berikut.

- a. Skenario pertama dan kedua (*Infrastructure Attacks*) bertujuan melumpuhkan jaringan dengan menghabiskan CPU Router (*Bottleneck* di Router).
- b. Skenario 3 (*Hybrid Attack*) yang menargetkan sumberdaya router dan server.
- c. Skenario 4 (*Endpoint/Protocol Attack*): Melumpuhkan host target secara langsung dengan menghabiskan Memori dan CPU Server (*Bottleneck* di Server).

Temuan ini memvalidasi bahwa framework D4I efektif dalam memetakan *root cause* serangan DDoS IPv6 yang bervariasi.

3. Analisis Rantai Artefak (*Analyze CoA*)

Langkah terakhir dalam fase analisis framework D4I adalah *Analyze CoA* (Menganalisis Rantai Artefak). Tujuan dari langkah ini adalah untuk menginterpretasikan Rantai Artefak yang telah dikonstruksi memahami karakteristik, dampak dan perbedaan modus operandi dari setiap skenario serangan yang diuji.

Berdasarkan visualisasi alur kausalitas pada keempat Rantai Artefak (CoA), ditemukan dua pola utama serangan DDoS pada jaringan IPv6 dalam penelitian ini, yaitu serangan yang menargetkan saturasi infrastruktur (*Infrastructure Saturation*) dan serangan yang menargetkan sumber daya endpoint (*Resource Exhaustion*).

- a. Serangan Saturasi Infrastruktur (*Infrastructure Saturation*).

Analisis terhadap CoA skenario pertama (*Redirect Flood*) dan skenario kedua (*Echo Request Flood*) menunjukkan pola serangan volumetrik yang memiliki dampak serupa. Garis rantai serangan (CoA) menunjukkan bahwa artefak serangan (Paket Tipe 137 dan *Echo Request*) berkorelasi dengan lonjakan CPU Router hingga 100%. Tingginya volume paket memaksa router untuk bekerja melebihi kapasitas pemrosesannya. Pada skenario pertama, router terbebani oleh pemrosesan pesan *redirect*, sementara pada skenario kedua, router terbebani oleh forwarding paket ping jumbo. Dampak yang dirasakan yakni penurunan trafik atau kelumpuhan pada sisi server target yang disebabkan oleh terputusnya jalur distribusi di hulu (router). Sedangkan server target hanya menerima dampak sekunder berupa hilangnya konektivitas yang sah.

- b. Serangan Hybrid.

Analisis CoA Skenario ketiga (*TCP Connect Flood*) pada Gambar 4.29 memperlihatkan pergeseran target serangan. Berbeda dengan dua skenario sebelumnya, rantai serangan

pada skenario ketiga ini bercabang. Serangan mampu membebani CPU Router berkisar 99% akibat tingginya packet rate dan berhasil menembus pertahanan jaringan serta membebani CPU Server sehingga mengalami kenaikan sekitar 10%.

c. Serangan Eksploitasi Protokol.

Garis rantai serangan (CoA) menunjukkan anomali di mana bandwidth router relatif rendah (3 Mbps), namun mampu melumpuhkan kinerja server. Adanya kenaikan CPU Server mencapai 50% dan Memori Server naik 89.5 MB) yang membuktikan bahwa injeksi paket *Neighbor Advertisement (NA)* berhasil memanipulasi mekanisme *Neighbor Discovery Protocol (NDP)* pada sistem operasi target. Server mengalami *Resource Exhaustion* (kelelahan sumber daya) karena dipaksa memproses ribuan entri tetangga (neighbor) palsu ke dalam tabel cache-nya.

Rangkuman perbandingan hasil analisis Rantai Artefak (CoA) karakteristik keempat serangan dapat dilihat pada Tabel 4.37.

Tabel 4.37. Perbandingan hasil analisis Rantai Artefak (CoA) keempat serangan.

Skenario Serangan	Vektor Serangan (<i>Delivery</i>)	Titik Eksploitasi (<i>Exploitation</i>)	Jenis Dampak (<i>Actions</i>)	Kesimpulan Analisis
Redirect Flood	Paket ICMPv6 Tipe 137 (Volumetrik)	CPU Router (100%)	Koneksi Terputus	Serangan Infrastruktur
Echo Flood	Paket ICMPv6 Echo Request (Volumetrik)	CPU Router (100%) & Bandwidth	Saturasi Bandwidth	Serangan Infrastruktur
TCP Flood	Sesi TCP SYN (Protocol L4)	CPU Router (99%) & CPU Server (10%)	Saturasi Layanan	Serangan Hibrida
NA Flood	Paket Neighbor Adv. (Protocol L3)	CPU Server (50%) & Memori Server	Resource Exhaustion	Serangan Endpoint

Hasil analisis CoA ini menunjukkan bahwa metode deteksi dan mitigasi DDoS pada jaringan IPv6 tidak bisa disamaratakan. Serangan volumetrik (Skenario 1 & 2) dapat dideteksi melalui pemantauan trafik router, namun serangan protokol (Skenario 4) memerlukan pemantauan mendalam pada kinerja sumber daya (CPU/RAM) di sisi endpoint server.

4.7 Laporan Analisis

Tahap akhir dari penerapan framework D4I adalah penyusunan laporan analisis (*Reporting*). Langkah ini bertujuan untuk mentransformasi temuan teknis dan analisis rantai artefak (CoA) yang telah dilakukan pada tahap sebelumnya menjadi informasi intelijen yang dapat dipahami secara hukum dan manajerial.

Berdasarkan integrasi metode Live Forensics untuk akuisisi data dan framework D4I untuk analisis, seluruh artefak digital yang ditemukan telah direkonstruksi untuk menjawab pertanyaan investigasi 5W1H (*Who, What, Where, When, Why, How*). Ringkasan komprehensif dari hasil investigasi forensik terhadap serangan DDoS pada jaringan IPv6 yang mencakup keempat skenario serangan yang diuji dapat dilihat pada Tabel 4.38.

Tabel 4.38. Hasil investigasi forensik terhadap serangan DDoS pada jaringan IPv6.

Fase (CKC)	Kategori	Temuan Artefak	Rantai Artefak (Konteks)	Pertanyaan (5W1H)	Keterangan (Jawaban Investigasi)
Reconnaissance	Identitas Sumber	Log Scanning dari IP: 2001:db8:100:aa11::2 (Attacker) 2001:db8:100:cc::2 (Zombie 1) 2001:db8:100:dd::2 (Zombie 2)	Sumber inisiasi serangan	<i>Who</i> (Siapa)	Serangan dikoordinasikan oleh satu host attacker yang mengendalikan dua host zombie yang teridentifikasi melalui log aktivitas awal.
Delivery	Jenis Serangan	Paket Trafik Jaringan (PCAP): - ICMPv6 Tipe 137 (Redirect) - ICMPv6 Echo Request - TCP SYN (Port 10000) - ICMPv6 Tipe 136 (NA)	Metode penyampaian serangan	<i>What</i> (Apa)	Terjadi serangan <i>Distributed Denial of Service</i> (DDoS) dengan 4 varian metode yakni <i>Redirect Flood</i> , <i>Echo Flood</i> , <i>TCP Connect Flood</i> dan <i>Neighbor Advertisement Flood</i> .
Delivery	Lokasi Kejadian	IP Tujuan (Target): - Router: 2001:db8:200:a01::1 - Server: 2001:db8:200:a01::2 - Interface: eth1-6 & ens3	Lokasi target dalam infrastruktur	<i>Where</i> (Dimana)	Serangan menargetkan infrastruktur jaringan inti (Router Mikrotik) dan <i>endpoint</i> layanan (Server Webmin Ubuntu).

Exploitation	Waktu Kejadian	Timestamp Log CPU & PCAP: Mulai: 10 Mei 2025, 22:32 WIB Berakhir: 11 Mei 2025, 00:10 WIB	Kronologi kejadian	When (Kapan)	Insiden berlangsung secara bertahap dalam rentang waktu tersebut, dengan setiap gelombang serangan berlangsung rata-rata 6-8 menit.
Exploitation	Dampak / Motivasi	Metrik Performa: - CPU Router: 99-100% - CPU Server: 50% - Memori Server: +89.5 MB	Tujuan teknis serangan	Why (Mengapa)	Penyerang bertujuan menghabiskan sumber daya (Resource Exhaustion) dan menghabiskan CPU serta Memori Server.
Weaponization	Modus Operandi	Tools: thc-ipv6, fping6, nping Teknik: Flooding Volumetrik Eksplorasi Protokol (SLAAC)	Cara pelaksanaan serangan	How (Bagaimana)	Penyerang membanjiri target dengan paket spoofing bervolume tinggi untuk memanipulasi tabel routing dan neighbor cache dan menyebabkan kegagalan pemrosesan pada target.

Tabel 4.38 menyajikan laporan komprehensif hasil investigasi forensik terhadap empat skenario serangan DDoS pada jaringan IPv6. Berdasarkan pemetaan artefak menggunakan framework D4I, penelitian ini berhasil merekonstruksi pola serangan secara utuh menggunakan aspek 5W1H mulai dari tahap *Reconnaissance* hingga *Actions on Objectives*. Berikut adalah analisis mendalam terhadap temuan tersebut:

1. Berdasarkan artefak log pada fase *Reconnaissance (R)*, penelitian ini berhasil mengatribusikan entitas penyerang (*Who*) yang berasal dari alamat 2001:db8:100:aa11::2, 2001:db8:100:cc::2, 2001:db8:100:dd::2. Aktivitas ini terekam (*When*) sesaat sebelum lonjakan trafik terjadi. Pola waktu yang berdekatan antara pemindaian jaringan dan dimulainya banjir paket mengindikasikan serangan yang terautomasi. Temuan ini konsisten dengan karakteristik pemindaian IPv6 yang dijelaskan oleh (Ullrich et al., 2015), di mana penyerang menghindari *brute-force* ruang alamat 2^{64} dan lebih memilih menargetkan alamat statis yang telah didapatkan sebelumnya. Artefak log scanning yang ditemukan pada tabel di atas mengonfirmasi bahwa penyerang menggunakan tools spesifik (seperti *thc-ipv6*) yang menargetkan alamat link-local atau global unicast yang terprediksi.
2. Pada fase *Delivery & Exploitation*, mengungkap bahwa serangan (*What*) yang dilancarkan terdiri dari dua jenis utama: serangan volumetrik (*Echo/Redirect Flood*) dan serangan protokol (*Neighbor Advertisement Flood*). Adapun teknik pelaksanaannya (*How*) melibatkan penggunaan *tools* spesifik untuk memanipulasi *header* ekstensi dan membanjiri target dengan paket kontrol palsu. yaitu:
 - a. Saturasi Infrastruktur (*Infrastructure Saturation*): Pada skenario serangan *ICMPv6 Redirect* dan *Echo Flood*, dampak utama terjadi pada perangkat Router (*Why*) dengan lonjakan beban CPU mencapai 99-100%. Hal ini terjadi karena Router dipaksa memproses paket kontrol ICMPv6 dalam jumlah masif (High PPS) yang melebihi kapasitas Control Plane. (Elejla et al., 2022a) dalam penelitiannya mengenai ICMPv6-based DDoS menegaskan bahwa serangan ini sangat efektif melumpuhkan perangkat jaringan (*Router/Switch*) karena protokol ICMPv6 merupakan komponen vital yang harus diproses oleh CPU perangkat.
 - b. Kelelahan Sumber Daya (*Resource Exhaustion*): Pada skenario serangan *Neighbor Advertisement (NA) Flood*, serangan berdampak server target secara langsung, ditandai dengan kenaikan penggunaan memori (RAM) sebesar +89.5 MB. Fenomena ini divalidasi oleh (Alsariera et al., 2022) yang menjelaskan

bahwa serangan berbasis *Neighbor Discovery Protocol* (NDP) mengeksploitasi celah desain IPv6 di mana node target wajib mengalokasikan memori untuk menyimpan entri *Neighbor Cache* dari setiap paket NA yang diterima. Akibatnya, server mengalami kondisi DoS bukan karena kehabisan bandwidth, melainkan karena kehabisan memori kernel untuk memproses koneksi baru (*Why*).

3. Investigasi juga berhasil mengatribusikan alat serangan (*attack tools*) yang digunakan, yaitu kombinasi THC-IPv6 dan fping6 (*How*). Penggunaan toolkit ini menunjukkan adanya serangan yang memanfaatkan fitur bawaan protokol IPv6. Sebagaimana dijelaskan oleh (Tayyab et al., 2020), tools seperti THC-IPv6 dirancang untuk memanipulasi header ekstensi IPv6 dan pesan NDP guna melewati mekanisme keamanan.

Integrasi *Cyber Kill Chain* (CKC) dalam D4I memungkinkan investigator untuk tidak hanya melihat "apa / *what*" yang terjadi, tetapi juga "di mana / *where*" posisi artefak kritis berada. Hal ini mendukung tesis (Dimitriadis et al., 2020d) selaku pengembang D4I, yang menyatakan bahwa pendekatan forensik berbasis *Attack-Centric* (berpusat pada serangan) mampu memberikan visibilitas yang lebih baik terhadap *Advanced Persistent Threat* (APT) maupun serangan *multi-stage DDoS* pada jaringan IPv6.

Keberhasilan merekonstruksi seluruh tahapan di atas membuktikan efektivitas framework D4I dalam merekonstruksi serangan secara utuh berdasarkan tiga indikator utama kualitas investigasi digital yakni Kelengkapan Rekonstruksi (*Completeness*), Validitas Atribusi" (*Attribution Validity*) dan Komprehensivitas Laporan / 5W1H.

1. (Carrier & Spafford, 2004) mendefinisikan bahwa tujuan akhir investigasi adalah "*Event Reconstruction*" yang menghubungkan bukti fisik dan digital untuk menguji hipotesis kejadian. Jika ada fase yang terputus, maka rekonstruksi dianggap gagal (*incomplete*). Integrasi akuisisi berbasis Live Forensic dan framework D4I berhasil menangkap artefak memori dan cache secara *real-time*. Hasilnya, visualisasi *Chain of Artifacts* (CoA) pada Gambar 4.25 mampu menghubungkan dan merekonstruksi seluruh fase serangan tanpa terputus.
2. Dalam pengukuran validitas atribusi (*Attribution Validity*), (Rid & Buchanan, 2015b) menekankan bahwa atribusi serangan siber memerlukan presisi teknis untuk menghubungkan artefak dengan aktor ancaman, terutama dalam kondisi serangan yang terautomasi. Efektivitas atribusi metode dapat dibuktikan melalui identifikasi benang merah yang saling berkaitan dalam tahapan *Cyber Kill Chain* (CKC).

3. Pada pengukuran komprehensivitas laporan berbasis 5W1H Mengacu pada prinsip pelaporan komprehensif oleh (Yusoff et al., 2011), yang menyatakan bahwa kualitas akhir investigasi dinilai dari kelengkapan elemen informasi yang disajikan. Pada penelitian ini, integrasi *Live Forensic* dan framework D4I berhasil menyajikan laporan secara menyeluruh berdasarkan standar laporan forensik 5W1H (*Who, What, Where, When, Why, How*) secara lengkap dan komprehensif.

4.8 Pembahasan Temuan Utama dan Relevansi Forensik

Dalam penelitian ini, penulis melakukan sintesis terhadap temuan lintas skenario serangan DDoS pada jaringan IPv6 untuk merumuskan pola serangan (*attack patterns*) dan implikasi forensik yang lebih mendalam. Penelitian ini tidak hanya bertujuan untuk mengidentifikasi artefak serangan, melainkan untuk mengevaluasi efektivitas pendekatan forensik baru dalam lingkungan IPv6. Berdasarkan sintesis hasil eksperimen lintas skenario, berikut adalah pembahasan mendalam mengenai efektivitas integrasi metodologis dan implikasinya terhadap praktik forensik modern:

1. Peran penting *Live Forensics* dalam Arsitektur D4I.

Temuan utama penelitian ini menegaskan bahwa efektivitas rekonstruksi serangan IPv6 sangat bergantung pada integrasi waktu-nyata (*real-time integration*).

- a. Framework D4I menyediakan peta jalan (roadmap) investigasi berbasis Attack-Centric, namun memiliki keterbatasan inherent dalam menangkap data volatil pada fase awal. Integrasi Live Forensics pada fase Identification terbukti efektif mengisi celah (gap) tersebut. Tanpa *Live Forensics*, artefak kunci seperti anomali *Neighbor Cache* (pada serangan NA Flood) akan hilang seketika saat perangkat mengalami restart atau crash, menyebabkan putusnya rantai bukti (*Broken Chain of Evidence*).
- b. Kombinasi ini memungkinkan investigator memvalidasi hipotesis serangan secara instan. Data volatil dari RAM memberikan konteks "apa yang sedang terjadi di memori", sementara struktur D4I memberikan konteks "di fase mana serangan ini berada". Sinergi inilah yang memungkinkan penelitian ini membedakan antara *Resource Exhaustion* (serangan memori) dan *Bandwidth Saturation* (serangan jaringan) dengan presisi.

2. Rekonstruksi Kausalitas Melalui *Chain of Artifacts* (CoA).

Kontribusi dari integrasi ini adalah kemampuan untuk memvisualisasikan kausalitas serangan yang tidak terlihat oleh metode forensik tradisional. Pada skenario serangan protokol (*Protocol Attacks*), metode konvensional seringkali gagal menjelaskan *root cause* karena trafik jaringan terlihat normal (*low bandwidth*). Melalui pendekatan D4I yang diperkuat data *Live Forensics*, penelitian ini berhasil membangun *Chain of Artifacts* (CoA) yang utuh. CoA secara eksplisit menghubungkan Vektor Serangan (Paket NA Palsu), Kerentanan Protokol (Mekanisme Stateless NDP) dan Dampak Sistem (Lonjakan Alokasi RAM). Visualisasi ini membuktikan bahwa kegagalan sistem bukan disebabkan oleh beban trafik, melainkan oleh eksploitasi protokol IPv6. Hal ini mengubah paradigma investigasi dari mencari jejak menjadi menjelaskan penyebab.

3. Implikasi terhadap Keamanan Jaringan IPv6

Temuan ini membawa implikasi bahwa model pertahanan IPv6 tidak dapat lagi mengandalkan mekanisme deteksi berbasis ambang batas (*threshold-based*) semata. Karakteristik "*Silent but Deadly*" pada DDoS IPv6 terbukti mampu melumpuhkan target (*Endpoint*) tanpa memicu alarm saturasi pada perangkat perantara (*Router*). Oleh karena itu, strategi forensik harus bergeser dari analisis pasca-insiden (*Post-Mortem*) menuju analisis berbasis perilaku protokol (*Behavioral Analysis*) yang dilakukan secara *live*. Pendekatan ini relevan untuk diterapkan pada infrastruktur kritis yang mengadopsi IPv6 di mana ketersediaan layanan (*Availability*) adalah prioritas utama.

BAB 5

Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil implementasi, pengujian, dan analisis yang telah dilakukan, penelitian ini menghasilkan kesimpulan sebagai jawaban atas pertanyaan penelitian sebagai berikut:

1. Penelitian ini berhasil merumuskan mekanisme integrasi dimana metode Live Forensics berperan sebagai teknik akuisisi data pada fase *Identification* dalam siklus D4I. Mekanisme ini terbukti mampu menangkap artefak dinamis IPv6 yang tidak dapat diperoleh melalui dead forensics, seperti anomali pada tabel *neighbor* (NDP Table) saat serangan berlangsung. Integrasi ini memungkinkan investigasi dilakukan secara real-time tanpa mematikan perangkat, sehingga kontinuitas layanan jaringan tetap terjaga selama proses akuisisi bukti.
2. Penerapan *Chain of Artifacts* (CoA) dalam framework D4I berhasil mengungkap perbedaan fundamental modus operandi dan *Point of Failure* dari skenario serangan DDoS IPv6:
 - a. Serangan Volumetrik terbukti menysasar ketersediaan infrastruktur (*Infrastructure Availability*) dengan membebani kapasitas pemrosesan perangkat jaringan.
 - b. Serangan Protokol terbukti mengeksploitasi logika protokol (*Protocol Logic*) yang menysasar sumber daya komputasi target akhir (*endpoint*). Temuan ini menjawab bahwa D4I mampu memetakan lokasi kegagalan (*Where*) dan akar penyebab (*Why*) yang berbeda pada setiap skenario serangan.
3. Pendekatan forensik yang diusulkan terbukti efektif dalam merekonstruksi kronologi insiden secara utuh. Visualisasi CoA mampu menghubungkan sebab-akibat antara aktivitas penyerang (fase *Weaponization*) dengan dampak kerusakan (fase *Action on Objectives*). Efektivitas terbukti dengan terpenuhinya standar investigasi 5W1H secara komprehensif, di mana elemen kausalitas (*Why*) dan modus operandi (*How*) dapat dijelaskan secara utuh.

Secara keseluruhan, penelitian ini menyimpulkan bahwa integrasi akuisisi *Live Forensics* dan analisis berbasis D4I terbukti efektif ditinjau dari tiga aspek yakni Kelengkapan Rekonstruksi, Validitas Atribusi, dan Komprehensivitas Laporan. Efektivitas ini diukur berdasarkan keberhasilan metode dalam menyusun rantai artefak (*Chain of Artifacts*) yang utuh tanpa terputus serta kemampuannya mengisolasi akar penyebab (*root cause*) serangan.

5.2 Saran

Penelitian ini telah berhasil mengimplementasikan integrasi metode Live Forensics dan framework D4I untuk investigasi serangan DDoS pada jaringan IPv6. Namun penulis menyadari bahwa penelitian ini masih memiliki keterbatasan. Oleh karena itu, terdapat beberapa saran untuk pengembangan penelitian selanjutnya, antara lain:

1. Pengembangan Otomatisasi Analisis D4I.

Dalam penelitian ini, proses korelasi dan konstruksi Rantai Artefak (CoA) masih dilakukan secara manual dan semi-otomatis. Penelitian selanjutnya disarankan untuk mengembangkan sistem atau algoritma yang mampu mengotomatisasi pembuatan visualisasi CoA seperti integrasi dengan teknologi *Machine Learning* atau *Artificial Intelligence* yang dapat membantu mendeteksi pola korelasi antar artefak secara lebih cepat dan akurat terutama dalam menghadapi volume data log yang sangat besar.

2. Perluasan Skenario Serangan IPv6.

Penelitian ini berfokus pada serangan flooding berbasis ICMPv6 dan TCP. Disarankan bagi peneliti selanjutnya untuk mengeksplorasi vektor serangan IPv6 yang lebih kompleks, seperti serangan pada lapisan aplikasi (Layer 7) melalui IPv6, serangan yang memanipulasi *Extension Headers* IPv6 atau serangan *Low-Rate* DDoS yang lebih sulit dideteksi dibandingkan serangan volumetrik.

3. Pengujian pada Lingkungan Fisik dan Skala Besar.

Simulasi dalam penelitian ini dilakukan menggunakan lingkungan virtualisasi (VMware/PNETLab). Untuk mendapatkan data performa yang lebih mendekati kondisi nyata di industri, disarankan untuk melakukan pengujian pada perangkat keras jaringan fisik (hardware *routers/switches*) atau lingkungan *cloud* berskala besar. Hal ini penting untuk melihat apakah perangkat keras khusus (ASIC) memiliki ketahanan yang berbeda terhadap serangan eksploitasi protokol dibandingkan router virtual.

4. Eksplorasi sistem operasi yang lebih beragam.

Penelitian ini menggunakan lingkungan berbasis Linux (Ubuntu dan Mikrotik). Mengingat perilaku penanganan protokol jaringan bisa berbeda antar sistem operasi, penelitian selanjutnya dapat memperluas cakupan investigasi pada sistem operasi lain seperti Windows Server atau sistem operasi perangkat jaringan proprietary lainnya untuk melihat variasi artefak yang dihasilkan.

Daftar Pustaka

- A. Naagas, M., & P. Gamilla, A. (2022). Denial of service attack: An analysis to IPv6 extension headers security nightmares. *International Journal of Electrical and Computer Engineering (IJECE)*, 12(3), 2922.
<https://doi.org/10.11591/ijece.v12i3.pp2922-2930>
- Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). *Systematic Digital Forensic Investigation Model*.
- Alim, M., Riadi, I., & Prayudi, Y. (2018). Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard. *International Journal of Computer Applications*, 180(35), 23–30. <https://doi.org/10.5120/ijca2018916879>
- Alsariera, Y. A., Adeyemo, V. E., Balogun, A. O., & Alazzawi, A. K. (2022). AI-Based Detection of Neighbor Discovery Protocol Flooding Attacks in IPv6 Networks. *IEEE Access*, 10, 28945–28956. <https://doi.org/10.1109/ACCESS.2022.3158652>
- Carrier, B., & Spafford, E. H. (2004). *An Event-Based Digital Forensic Investigation Framework*. Proceedings of the 4th Digital Forensic Research Workshop (DFRWS). http://www.dfrws.org/2004/proceedings/carrier_event.pdf
- Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020a). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array*, 5, 100015. <https://doi.org/10.1016/j.array.2019.100015>
- Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020b). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array (New York, N.Y.)*, 5, 10.1016/j.array.2019.100015.
<https://doi.org/10.1016/j.array.2019.100015>

- Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020c). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array*, 5, 100015. <https://doi.org/10.1016/j.array.2019.100015>
- Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020d). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array*, 5, 100015. <https://doi.org/10.1016/j.array.2019.100015>
- Elejla, O. E., Anbar, M., Hamouda, S., Belaton, B., Al-Amiedy, T. A., & Hasbullah, I. H. (2022a). Flow-Based IDS Features Enrichment for ICMPv6-DDoS Attacks Detection. *Symmetry*, 14(12), 2556. <https://doi.org/10.3390/sym14122556>
- Elejla, O. E., Anbar, M., Hamouda, S., Belaton, B., Al-Amiedy, T. A., & Hasbullah, I. H. (2022b). Flow-Based IDS Features Enrichment for ICMPv6-DDoS Attacks Detection. *Symmetry*, 14(12), 2556. <https://doi.org/10.3390/sym14122556>
- Göbel, O., & Göbel, O. (Eds.). (2008). *IMF 2008: IT incident management & IT forensics; proceedings of the 4th International Conference on IT Incident Management & IT-Forensics; September 23 - 25, 2008, Mannheim, Germany*. IMF, Bonn. Ges. für Informatik.
- Google. (2025). *IPv6 Adoption Statistics*. <https://www.google.com/intl/en/ipv6/statistics.html>
- Hakim, A. R., Ramli, K., Gunawan, T. S., & Windarta, S. (2023). A Novel Digital Forensic Framework for Data Breach Investigation. *IEEE Access*, 11, 42644–42659. <https://doi.org/10.1109/ACCESS.2023.3270619>
- Hasan Bdair Aighuraibawi, A., Manickam, S., Abdullah, R., Abdi Alkareem Alyasseri, Z., Khallel, A., Asaad Zebari, D., Mohammed Jasim, H., Mohammed Abed, M., & Hussein Arif, Z. (2023). Feature Selection for Detecting ICMPv6-Based DDoS

- Attacks Using Binary Flower Pollination Algorithm. *Computer Systems Science and Engineering*, 47(1), 553–574. <https://doi.org/10.32604/csse.2023.037948>
- Haseeb-ur-rehman, R. M. A., Aman, A. H. M., Hasan, M. K., Ariffin, K. A. Z., Namoun, A., Tufail, A., & Kim, K.-H. (2023). High-Speed Network DDoS Attack Detection: A Survey. *Sensors*, 23(15), 6850. <https://doi.org/10.3390/s23156850>
- Hui, W., Sun, Y., Liu, J., & Lu, K. (2011). DDoS/DoS Attacks and Safety Analysis of IPv6 Campus Network: Security Research under IPv6 Campus Network. 2011 *International Conference on Internet Technology and Applications*, 1–4. <https://doi.org/10.1109/ITAP.2011.6006421>
- Huston, G. (2022, May 4). The transition to IPv6: Are we there yet? *APNIC Blog*. <https://blog.apnic.net/2022/05/04/the-transition-to-ipv6-are-we-there-yet/>
- Huston, G. (2025). *IPv6 Capability Metrics: World*. <https://stats.labs.apnic.net/ipv6/XA>
- Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers & Security*, 38, 103–115. <https://doi.org/10.1016/j.cose.2013.05.001>
- Kumar, V., Oikonomou, G., & Tryfonas, T. (2016). Traffic forensics for IPv6-based Wireless Sensor Networks and the Internet of Things. 2016 *IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 633–638. <https://doi.org/10.1109/WF-IoT.2016.7845515>
- Luo, Y., Fu, X., Luo, B., Du, X., & Guizani, M. (2020). Forensic Model for DDoS Attack. *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 1–6. <https://doi.org/10.1109/GLOBECOM42002.2020.9348178>
- Nurdin, R., & Ramadhani, E. (2024). *Investigasi Forensika Digital WhatsApp Scam Dengan Menggunakan Framework D4I*. 11(1).
- Pollitt, M. (2019). *A Framework for Digital Forensic Science*.

- Prayogo, O. R., & Riadi, I. (2020). Router Forensic Analysis against Distributed Denial of Service (DDoS) Attacks. *International Journal of Computer Applications*, 175(39), 19–25. <https://doi.org/10.5120/ijca2020920944>
- Rid, T., & Buchanan, B. (2015a). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1–2), 4–37. <https://doi.org/10.1080/01402390.2014.977382>
- Rid, T., & Buchanan, B. (2015b). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1–2), 4–37. <https://doi.org/10.1080/01402390.2014.977382>
- Rogers, M., Goldman, J., Mislán, R., Wedge, T., & Debroya, S. (2006). Computer Forensics Field Triage Process Model. *The Journal of Digital Forensics, Security and Law*. <https://doi.org/10.15394/jdfsl.2006.1004>
- Saad, R. M. A. (2016). *ICMPv6 ECHO REQUEST DDoS ATTACK DETECTION FRAMEWORK USING BACK- PROPAGATION NEURAL NETWORK*.
- Sood, R., & Llm, P. (2020). *CYBER FORENSIC MANUAL FOR DENIAL-OF- SERVICE ATTACK*.
- Suharti, S., Yudhana, A., & Riadi, I. (2022). Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, 21(3), 567–582. <https://doi.org/10.30812/matrik.v21i3.1732>
- Tayyab, M., Belaton, B., & Anbar, M. (2020). ICMPv6-Based DoS and DDoS Attacks Detection Using Machine Learning Techniques, Open Challenges, and Blockchain Applicability: A Review. *IEEE Access*, 8, 170529–170547. <https://doi.org/10.1109/ACCESS.2020.3022963>
- Tseung, C. Y., & Chow, K. P. (2018). Forensic-Aware Anti-DDoS Device. *2018 IEEE Security and Privacy Workshops (SPW)*, 148–159. <https://doi.org/10.1109/SPW.2018.00030>

- Ullrich, J., Kieseberg, P., Krombholz, K., & Weippl, E. (2015). *On Reconnaissance with IPv6: A Pattern-Based Scanning Approach*. 186–192.
<https://doi.org/10.1109/ARES.2015.15>
- Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science & Information Technology (IJCSIT)*, 3(3), 17–31. <https://doi.org/10.5121/ijcsit.2011.3302>
- Zhang, X., Upton, O., Beebe, N. L., & Choo, K.-K. R. (2020). IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers. *Forensic Science International: Digital Investigation*, 32(Query date: 2024-05-26 18:44:27), 300926–300926. <https://doi.org/10.1016/j.fsidi.2020.300926>