Forensik Jaringan Terhadap Serangan DDOS Menggunakan Metode *Network Forensic Development Life Cycle*

Raden Hario Wahyu Murti [a,1,*], Imam Riadi [b,2], Nuril Anwar [c,3], Taufiq Ismail [d,4]

[a,b,c,d] Program Studi S1 Informatika, Universitas Ahmad Dahlan, Jl. Ringroad Selatan, Bantul, Yogyakarta, Indonesia
[1] raden1600018071@webmail.uad.ac.id*; [2] imam.riadi@is.uad.ac.id; [3] nuril.anwar@tif.uad.ac.id; [4] taufiq.ismail@tif.uad.ac.id
* Penulis Korespondensi

ABSTRAK

Teknologi informasi dan komunikasi merupakan elemen penting dalam kehidupan masa kini yang telah menjadi bagian bagi berbagai sektor kehidupan dan memberi andil besar terhadap perubahan yang mendasar. Sekelompok orang atau organisasi yang tidak bertanggung jawab dapat menggunakan *internet* untuk mengganggu atau merusak suatu *website* sehingga menyebabkan *overload* pada *router* dan membuat *website* tidak dapat diakses. Metode penyerangan ini disebut dengan DDoS *(Distributed Denial of Service*). Tujuan penelitian ini adalah mengidentifikasi keamanan jaringan pada *router* dan mendapatkan karakteristik barang bukti digital pada *router* untuk keperluan forensik. Penelitian ini menggunakan metode *Network Forensic Development Life Cycle* (NFDLC) yang memiliki pada lima tahapan utama yaitu *Initiation, Acquisition, Implemetation, Operations,* dan *Disposation*. *Tools* yang digunakan pada penelitian adalah menggunakan Wireshark yang bertugas *monitoring* serangan DDoS terhadap serangan *router* dan melakukan investigasi untuk mendapatkan barang bukti digital berupa hasil serangan yang masuk ke servertrak. Hasil temuan barang bukti digital yang didapat pada *monitoring* ubuntu server tercatat menerima 84.407 paket pada serangan pertama dengan IP Address 10.10.1.2 dan menerima 359.510 paket pada serangan kedua dengan Ip Address 10.10.1.4 dan hasil monitoring windows server tercatat menerima 2.305.835 paket pada serangan pertama dengan IP Address 10.10.1.2 dan menerima 94.120 paket pada serangan kedua dengan Ip Address 10.10.1.4.

Kata Kunci
DDos
Forensik
NFDLC
Router
Website

1. Pendahuluan

Teknologi informasi dan komunikasi merupakan elemen penting dalam kehidupan keseharian pada saat ini. Peranan teknologi informasi pada aktivitas manusia pada saat ini memang begitu besar. Teknologi informasi telah menjadi fasilitas utama bagi kegiatan berbagai sektor kehidupan dimana memberikan andil besar terhadap perubahan-perubahan yang mendasar [1]. Manusia mulai memanfaatkan internet untuk berbagai macam kegiatan diantaranya membuat website tertentu seperti Jual Beli Online, Forum, dan sebagainya [2]. Membuat server tersendiri atau berbayar kepada penyedia jasa layanan untuk mendapatkan memperluas jangkauan, kecepatan jasa layanan dan konektivitas dalam menunjang website

Sekelompok orang atau organisasi yang tidak bertanggung jawab dapat menggunakan internet untuk mengganggu atau merusak suatu website sehingga menyebabkan *overload* pada *router* dan membuat orang lain tidak dapat mengakses website [3]. Metode penyerangan ini disebut *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS). Dengan program yang didapatkan dari internet, seseorang dapat melancarkan serangan DoS atau DDoS terhadap suatu jaringan yang diinginkan.

Saat ini, begitu banyak cara untuk melakukan serangan terhadap suatu sistem jaringan. Dahulu untuk melakukan suatu serangan membutuhkan pengetahuan dan pemahaman teknis IT yang tinggi, akan tetapi

Jurnal Sarjana Teknik Informatika
Vol. 11., No. 3, Oktober 2023, pp. 107-112

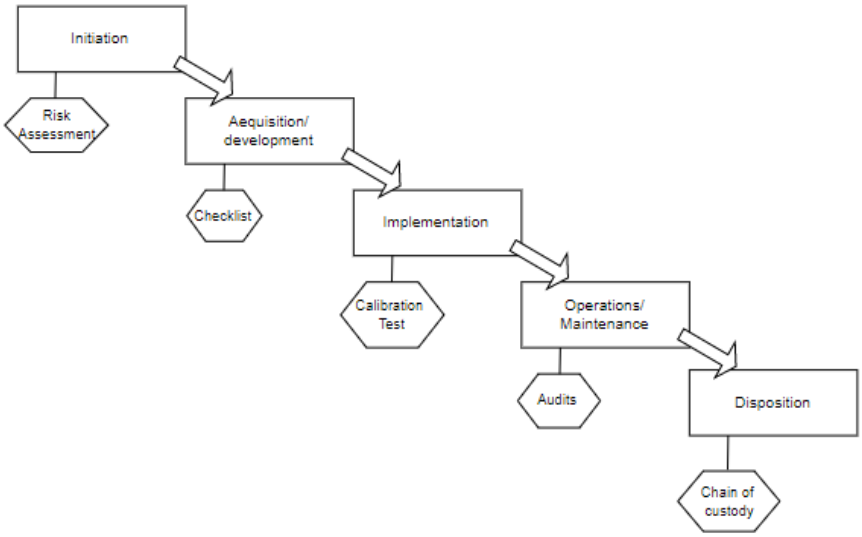
saat ini sangat mudah untuk melakukan serangan bukan hanya orang yang mempunyai *skill* yang tinggi. Metode dan alat-alat yang dipakai semakin banyak dan mudah digunakan bahkan untuk orang awam, maka semakin tinggi pula tingkat serangan yang terjadi terhadap sistem keamanan jaringan.

Salah satu jenis serangan yang masih sering digunakan adalah DoS dan DDoS. Dos merupakan serangan yang mengakibatkan sistem yang diserang mengalami gangguan [4]. Ganguan DoS bisa berupa kegagalan sistem, *halt*, *error request* bahkan kerusakan *hardware server* [5]. Serangan pada jaringan dilakukan dalam bentuk penyusupan dengan menggunakan berbagai macam jenis serangan jaringan komputer melalui *tools* yang dibuat secara mandiri ataupun *tools* yang di dapat dari *internet* [6]. Dari uraian tersebut dapat dipahami bahwa pentingnya melakukan analisis serangan pada *router* karena keamanan data menjadi hal penting dalam komunikasi data pada suatu sistem jaringan komputer.

DoS dan DDos merupakan serangan yang berbahaya karena akibat yang dihasilkan dari serangan berdampak luas. Serangan ini mudah dilaksanakan dengan *tools* yang minimum atau pengetahuan *scripting* yang tidak terlalu tinggi. Motif dari serangan DoS dan DdoS juga berbeda-beda sehingga mengakibatkan sukar untuk melacak pikah yang terlibat dalam serangan ini. Berdasarkan paparan terkait serangan pada jaringan komputer, diperlukan sebuah solusi untuk menyelesaikan permasalahan tersebut. Tulisan ilmiah ini memberikan solusi yaitu mekanisme untuk mempertahankan jaringan dari serangan DoS dan DDoS.

2. Metode

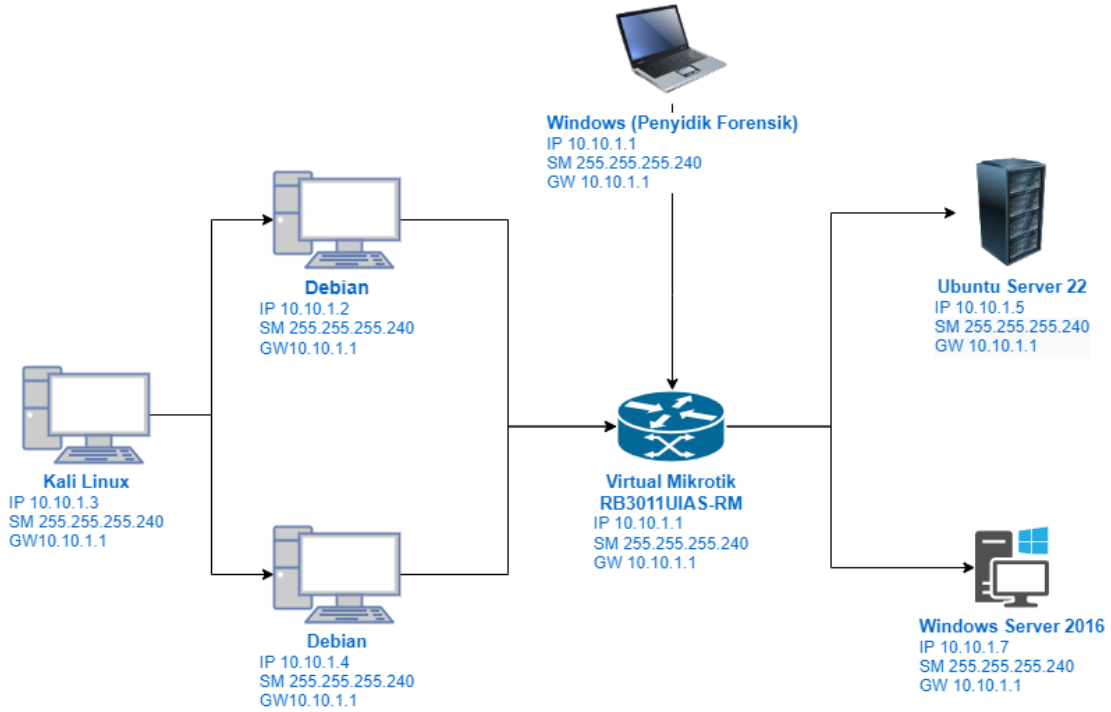
Penelitian ini melakukan simulasi kasus untuk mencoba proses investigasi *router* teradap serangan DDoS dengan mengimplementasikan metode *Network Forensik Development Life Cycle* (NFDLC). Simulasi kasus bertujuan untuk melakukan pengujuan terhadap serangan DDoS terhadap router dan melakukan investigasi untuk mendapatkan *Log Activity* dan *IP Address List* penyerang untuk dijadikan sebagai barang bukti atau tindak kejahatan. Proses analisis forensik dalam penelitian ini mengambil fokus utama pada analisis serangan DDoS pada *router* menggunakan aplikasi Wireshark untuk keperluan proses penarikan data atau informasi mengenai *Log Activity* dan *IP Address List* dari penyerang. Hasil pelaporan adalah menjelaskan kondisi *router* sebelum diserang dan sesudah diserang sebagai mekanisme analisis serangan DDoS. Tahapan penelitian dijabarkan seperti pada Gambar 1.



Gambar 1. Tahapan dari Simulasi dengan NFDLC

2.1. Mekanisme Investigasi

Tahap investigasi diawali dengan tahap (*Preparation*) yaitu tahap awal untuk mengetahui suatu tindak kejahatan, hak akses pada barang bukti yang ada di Tempat Kejadian Perkara (TKP), dan mempersiapkan alat dan bahan untuk kegiatan investigasi [7]. Pada tahap kedua adalah tahap (*Inciden Response*) yaitu tahap melakukan penanganan barang bukti yang ditemukan di TKP agar barang bukti yang ditemukan tidak terkontaminasi hal lain yang dapat merubah keaslian barang bukti [8]. Pada tahap ketiga adalah tahap (*Laboratorium Process*) yaitu tahap untuk mendapatkan informasi digital yang akan dianalisis untuk memperkuat barang bukti pada kasus kejahatan [9], untuk mendapatkan informasi peneliti mengguakan FTK Imager, MD5 Checker, Wireshark dan Autopsy. Pada tahap keempat adalah tahap (*Presentation*) yaitu tahapan akhir dalam proses investigasi digital [10]. Pada tahap ini merupakan proses pembuatan laporan terkait hasil analisis yang dilakukan pada tahap sebelumnya dan memastikan bahwa setiap proses yang dilakukan tersebut telah sesuai dengan aturan hukum yang berlaku. Dalam skenario penelitian terdiri dari beberapa tahapan yang dijabarkan seperti pada Gambar 2.

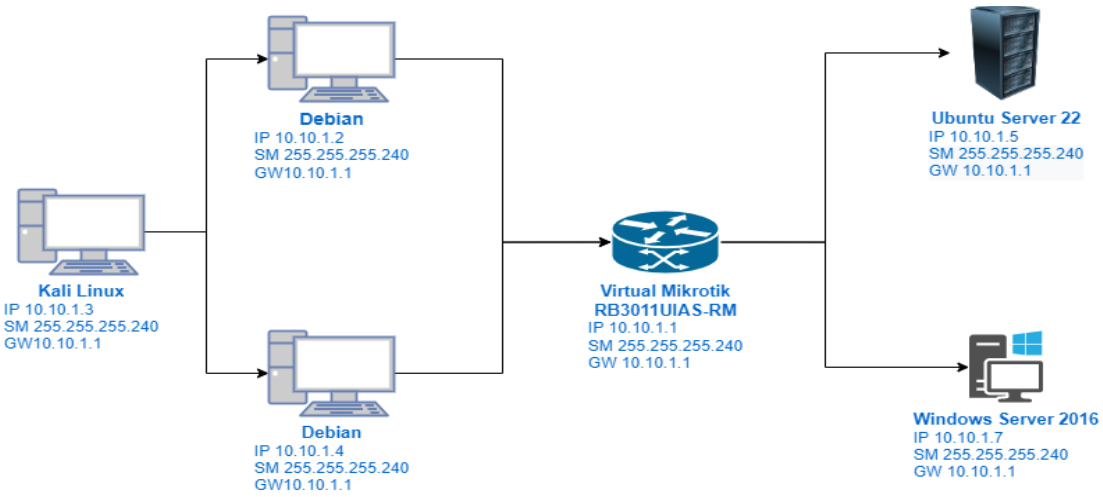


Gambar 2. Skenario Penelitian

2.1. Mekanisme Penyerangan DdoS pada Router

Serangan DDoS pada *router* digunakan dengan mekanisme mengirikan *zombie* secara terus menerus atau memanfaatkan kelemahan sistem dengan memaksa kapasitas pemroses yang berakibat sistem tidak lagi dapat bekerja normal untuk melemahkan sisten. Kali linux digunakan sebagai penyerang (*attacker*) yang akan mengirimkan serangan dengan mengirim *zombie* secara terus menerus ke windows server dan ubuntu server. Pada saat yang bersamaan secara otomatis server akan mengalami kebanjiran data dan server tidak akan bisa diakses secara normal. Serangan DDoS pada router mempunyai skema penyerangan yang dapat dilihat seperti pada Gambar 3.

Jurnal Sarjana Teknik Informatika
Vol. 11., No. 3, Oktober 2023, pp. 107-112

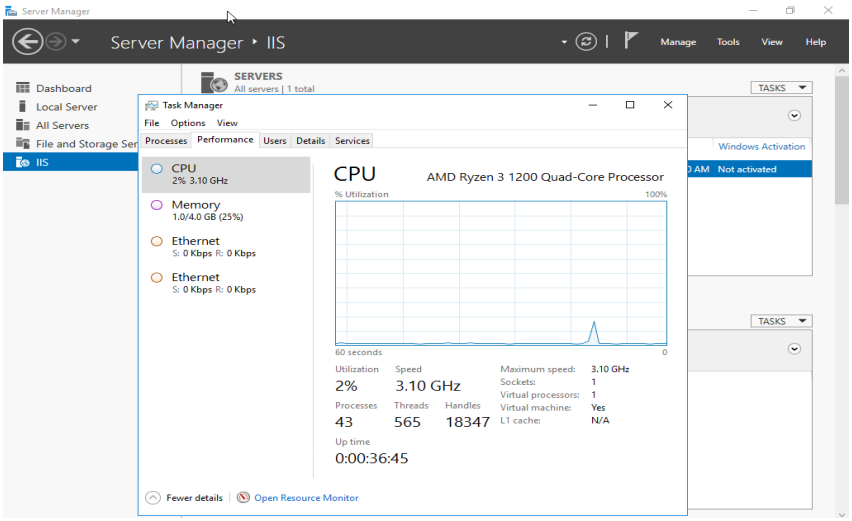


Gambar 3. Skema Penyerangan DdoS pada Router

3. Hasil dan Pembahasan

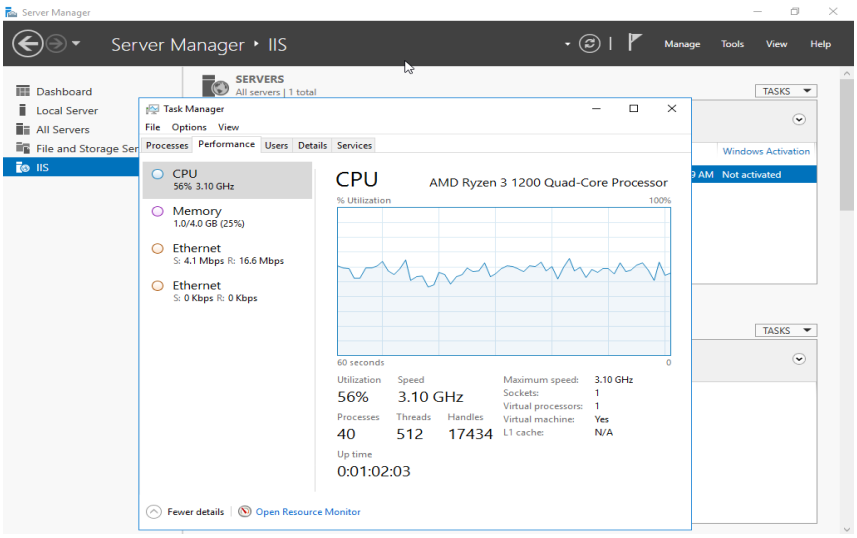
3.1. Hasil Simulasi Penyerangan pada Windows Server

Pembahasan meliputi investigasi dalam penelitian forensik digital terhadap serangan DDoS kepada windows server akan menunjukkan kondisi sebelum dan sesudah serangan DDoS yang dapat dilihat pada Gambar 4.



Gambar 4. Windows Server Sebelum Serangan DDoS

Pada Gambar 4 adalah data dari hasil *monitoring* windows server saat belum ada serangan DDoS, yang ditandai tidak terlihat ada peningkatan dalam utilitas CPU pada windows server. Setelah diamati selama 1 menit 40 detik mendapatkan hasil bahwa hanya ada kenaikan 1% sampai 2% dalam utilitas CPU. Hasil monitoring windows server setelah ada serangan dapat dilihat pada Gambar 5.

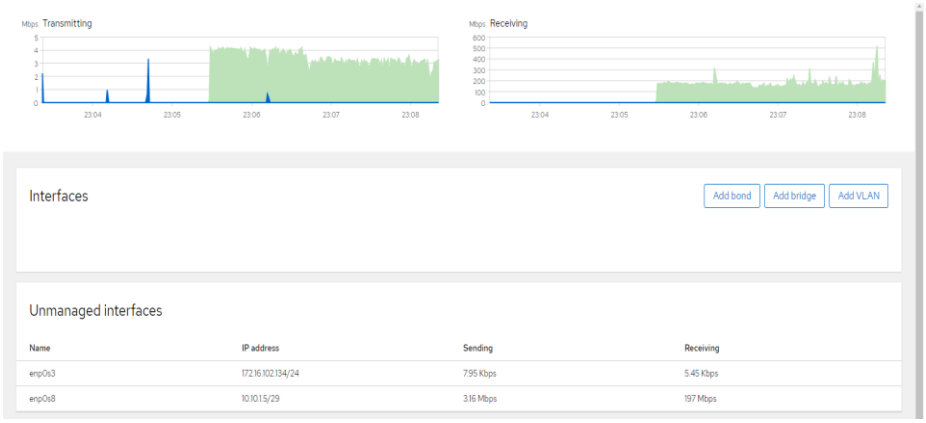


Gambar 5. Windows Server Setelah Serangan DDoS

Pada Gambar 5 adalah data dari hasil *monitoring* windows server yang dihasilkan pada saat melakukan simulasi DdoS, yang ditandai peningkatan utilitas CPU dari 1% sampai 2% menjadi 52% sampai 56% dalam kurun waktu 1 menit 19 detik. Hasil analisis mengidentifikasi peningkatan ulititas penggunaan prosessor yang sangat tinggi yaitu sebesar 50%, kondisi ini berhasil mengidentifikasi bentuk serangan DDoS.

3.2. Hasil Simulasi Penyerangan pada Ubuntu Server

Pembahasan investigasi DDoS yang dilakukan melalui windows server dikuatkan dengan investigasi melalui Ubuntu server. Hasil investigasi melalui Ubuntu server dapat dilihat pada Gambar 6.



Gambar 6. Windows Server Setelah Serangan DDoS

Pada Gambar 6 adalah hasil *monitoring* Ubuntu server saat keadaan mendapat serangan DDoS Ripper dan MHDDoS. Data yang didapatkan pada saat ubuntu server diserang adalah data yang masuk (RX) sebanyak 197 Mbps dan data yang dikirim atau dikeluarkan (TX) sebanyak 3,16 Mbps. Data *packet per second* (P/S) yang masuk per detik sebanyak 1391 packet.

Kondisi normal dari RX yaitu sebanyak 0,2 sampai 0,4. Kondisi normal dari TX yaitu sebanyak 0,2 sampai 0,5. Kondisi normal dari P/S yaitu sebanyak 0 sampai 20 packet. Analisis lebih lanjut dari proses penyerangan melalui Ubuntu server yaitu awal serangan DDoS Ripper dan MHDDoS berhasil mengirim kurang lebih 1500 packet. Hasil serangan akan mengganggu *traffic* pada server menjadi meningkat pesat dan mengalami *overload* melalui serangan secara terus menerus.

4. Kesimpulan

Berdasarkan hasil penelitian mengenai upaya forensik digital melalui *Network Forensic Development Life Cycle* menghasilkan kesimpulan yaitu:

1. Hasil identifikasi masalah keamanan jaringan menggunakan *Network Forensic Development Life Cycle* dapat melakukan *monitoring* ulititas penggunaan prosessor serta *monitoring* kondisi data yang dikirimkan (RX), data yang diterima (TX), dan jumlah *data packet* pada *traffic* server.
2. Hasil simulasi *monitoring* mengidentifikasi peningkatan utilitas prosessor dan *traffic server* yang mengganggu kinerja atau *traffic overload* melalui serangan secara terus menerus.

Penelitian ini perlu melakukan kajian secara lebih lanjut terkait karakteristik bukti digital pada *router* sebagai laporan atau hasil temuan forensik digital. Bukti karakteristik forensik digital meliputi serangan yang masuk, serangan yang diterima, log activity, dan IP address list penyerangan.

Deklarasi

Kontribusi Penulis. Semua penulis berkontrbusi secara bersama-sama dengan kontributor utama dalam artikel ini. Semua penulis membaca dan menyetujui versi akhir dari artikel yang diajukan.
Pernyataan Sponsor. Tidak ada penulis yang menerima dana atau hibah dari lembaga atau badan pendanaan untuk penelitian ini.
Konflik Kepentingan. Penulis menyatakan tidak ada konflik kepentingan.
Informasi Tambahan. Tidak ada informasi tambahan dalam artikel ini.

Daftar Pustaka

[1] I. Rusydi, "Peranan Perkembangan Teknologi Informasi dan Komunikasi dalam Kegiatan Pembelajaran dan Perkembangan Dunia Pendidikan," *War. Dharmawangsa*, no. 53, pp. 1–14, 2017, doi: https://doi.org/10.46576/wdw.v0i53.272.

[2] L. Y. Siregar and M. I. P. Nasution, "Perkembangan Teknologi Informasi Terhadap Peningkatan Bisnis Online," *J. Ilm. Manaj. dan Bisnis*, vol. 2, no. 1, pp. 71–75, 2020, doi: https://doi.org/10.30606/hjimb.

[3] R. Hermawan, "Analisis Konsep dan Cara Kerja Serangan Komputer Distributed Denial of Service (DDoS)," *Fakt. Exacta*, vol. 5, no. 1, pp. 1–14, 2015, doi: http://dx.doi.org/10.30998/faktorexacta.v5i1.186.

[4] M. D. Erlangga and A. Prihanto, "Analisis Reliabilitas Multiserver Menggunakan Load Balancing dengan Metode Denial Of Service," *J. Informatics Comput. Sci.*, vol. 3, no. 03, pp. 258–266, Dec. 2021, doi: 10.26740/jinacs.v3n03.p258-266.

[5] S. Sutarti and K. Khairunnisa, "Perancangan dan Analisis Keamanan Jaringan Nirkabel dari Serangan DSoS (Distributed Denial Of Service) Berbasis Honeypot," *J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 4, no. 2, pp. 9–16, 2017.

[6] S. Aji, A. Fadlil, and I. Riadi, "Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 11, Jun. 2017, doi: 10.26555/jiteki.v3i1.5665.

[7] R. Inggi, B. Sugiantoro, and Y. Prayudi, "Penerapan System Development Life Cycle (SDLC) dalam Mengembangkan Framework Audio Forensik," *semanTIK*, vol. 4, no. 2, pp. 193–200, 2018, doi: 10.5281/zenodo.2528444.

[8] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Analisis Kelayakan Integrated Digital Forensics Investigation Framework Untuk Investigasi Smartphone," *J. Buana Inform.*, vol. 7, no. 4, Oct. 2016, doi: 10.24002/jbi.v7i4.767.

[9] A. R. Supriyono, B. Sugiantoro, and Y. Prayudi, "EKSPLORASI BUKTI DIGITAL PADA SMART ROUTER MENGGUNAKAN METODE LIVE FORENSICS," *Infotekmesin*, vol. 10, no. 2, pp. 1–8, Jul. 2019, doi: 10.35970/infotekmesin.v10i2.48.

[10] M. N. Faiz, W. A. Prabowo, and M. F. Sidiq, "Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal," *J. Informatics, Inf. Syst. Softw. Eng. Appl.*, vol. 1, no. 1, pp. 62–70, 2018, doi: 10.20895/INISTA.V1I1.