Jurnal
Kolaborasi Riset Sarjana

Artikel

Analisis Forensik Jaringan pada *Router* Berbasis Log Menggunakan Metode *Live Forensic*

Fadhilah Dhinur Aini [1], Ari Peryanto [2] dan Yuwono Fitri Widodo [3]
1, 2, 3 Informatika, Univeristas Madani, Bantul, Yogyakarta, Indonesia
* Korespondensi: fadhilah.da@umad.ac.id

Abstrak: Pemanfaatan teknologi jaringan salah satu fasilitas yang mudah di jangkau secara luas. Jaringan *router* menjadi penghubung antar dua perangkat mengirimkan paket data dari satu jaringan ke jaringan lainnya. Penelitian ini menggunakan Simulasi dengan perangkat laptop utama dilakukan tes *ping* ke jaringan IP 172.16.10.1 untuk dihubungkan ke *router* dengan metode *live forensic* bertujuan untuk menganalisis data yang mencurigakan melalui jaringan *router* dengan mengakses PC *client IP address* 54.255.213.29 dengan memanfaatkan akses protokol *DNS* yang terhubung *tools wireshark* untuk menemukan hasil barang bukti *digital log* yang mencatat secara *real-time*.

Kata kunci: Laptop; Jaringan; wireshark; Router; Live Forensik

***Received**: 9 Oktober 2024*
***Revised**: 31 Desember 2024*
***Accepted**: 30 April 2025*
***Published**: 6 Mei 2025*

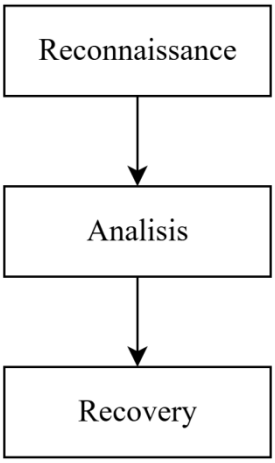
Pendahuluan

Ilmu forensik telah banyak melibatkan dunia digital dewasa ini (Al Hakim et al., 2022; Charan et al., 2022; Pratama, 2020; Ramadhani et al., 2017; Utami et al., 2021; Widodo & Sugiantoro, 2018; Wolverton, 2016). Salah satunya ialah forensik jaringan, yakni menganalisis lalu lintas jaringan untuk mencegah terjadinya penyalahgunaan teknologi oleh serangan yang tidak bertanggung jawab (Adawiah & Abror, 2025). Serangan dilakukan melalui fasilitas jaringan *internet public* untuk mendapatkan informasi kepentingan pribadi maupun anggota tim. Kasus kejahatan jaringan internet mengakibatkan *down server* hingga terjadi kerusakan pada jaringan *router* (Ponno, 2023). Sistem jaringan yang terhubung pada *router* dapat menyimpan identitas pengiriman data antar jaringan lain. Pusat data yang diinginkan untuk melakukan tindakkan kejahatan dapat menyebabkan kerusakan jaringan yang terhubung menggunakan *router* sehingga mudah dikendalikan. *Router* digunakan dalam proses jaringan berbasis teknologi protokol *TCP/IP address* untuk mengirimkan *data packet*. Log dapat di analisis pengiriman data mencurigakan melalui jaringan internet menyebabkan akses ke komputer terputus (Ponno, 2023).

Metodologi

Forensik Jaringan

Jaringan forensik merupakan proses *monitoring* dan analisis lalu lintas jaringan untuk mengumpulkan *packet*. Informasi bukti kejahatan jaringan forensik menurut hukum sebagai tugas-tugas penting yang banyak di pakai oleh organisasi, bisnis dan audit lalu lintas internet sesuai kebutuhan forensik (Ramadhan et al., 2024).



Gambar 1. Alur jaringan forensik

Tahapan Gambar 1 yaitu proses pengumpulan data informasi melalui data non-volatil dan menyelidiki aksi kejahatan melalui jaringan internet dengan mengirimkan *packet* secara ilegal. Di tahapan berikut analisis merupakan proses analisa log data dari berbagai jaringan yang dilalui oleh *victim* dan *time-lining* dari informasi yang diperoleh, kemudian dilakukan pemulihan data yang telah hilang (Ramadhan et al., 2024).

Alat dan Bahan

Router salah satu alat yang digunakan untuk mengirimkan *packet* melalui jaringan ke jaringan utama. Fungsi *router* merupakan penghubung antar jaringan komputer dan ke komputer untuk menganalisis data mencurigakan. Proses *router* memiliki fitur yaitu *open system interconnection* sebagai *packet filtering router* yang dapat memblokir lalu lintas jaringan data diakses secara *broadcast strom* sehingga mampu memperlambat akses kinerja jaringan internet (Damayanti & Hikmah, 2022).

Penggunaan *tools wireshark* untuk menganalisis barang bukti serta mengamati mengirimkan data melalui jaringan yang terhubung ke *router*. *Wireshark* dapat meng-*capture* data mencurigakan yang dikirimkan melalui jaringan yang tersambung dengan komputer. Sehingga hasil yang diperoleh berupa barang bukti digital log (Damayanti & Hikmah, 2022).

Penelitian terkait oleh Mandown menjelaskan aplikasi jaringan forensik *NetworkMiner* dan *Wireshark* dalam investigasi untuk mengekstrak dan menganalisis paket *file* yang direkam pada jaringan Universitas Nitroba mendapatkan bukti yang jelas, beralasan dan pasti digunakan untuk mengungkap pelaku pengiriman pesan ancaman tersebut (Mandowen, 2016).

Penelitian terkait oleh Tasmi et al. menjelaskan tentang *network* forensik untuk menganalisis *traffic* data *game online* bertujuan untuk menganalisis jenis lalu lintas data pada *game online* dengan menggunakan *tool wireshark* untuk *sniffing packet* data dan memvalidasi *user* pengguna jaringan (Tasmi et al., 2022).

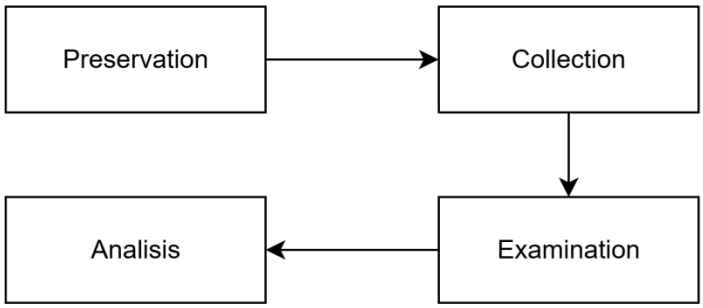
Penelitian terkait oleh Putri dan Istiyanto menjelaskan analisis forensik jaringan studi kasus serangan *SQL Injection* pada server UGM dengan hasil yang telah dilakukan, terdapat 68 *IP address* yang melakukan tindakan ilegal *SQL Injection* pada server *website* UGM, penyerangan memanfaatkan celah keamanan untuk mencuri data dari server tersebut (Putri & Istiyanto, 2012).

Penelitian terkait oleh Rahmana dan Akmalb tentang forensik jaringan untuk investigasi kejahatan siber, penelitian ini menunjukkan *Snort* sebagai sistem deteksi intrusi jaringan (NIDS), efektif dalam mendeteksi ancaman dari dalam dilingkungan jaringan linux (Rahmana & Akmalb, 2024).

Penelitian terkait oleh Jalu Abror et al. adalah *firewall next generation* terbilang lebih efektif dibandingkan *firewall* tradisional. Fitur tambahan mampu memantau dan mengontrol *traffic* jaringan dengan baik sehingga akses tidak mudah di bobol yang mengakibatkan kebocoran data (Adawiah & Abror, 2025).

Metode

Penelitian ini menggunakan metode *live forensic* dengan proses respons insiden, investigasi, dan analisa jaringan forensik. Beberapa tahapan yang digunakan dalam penelitian ini diilustrasikan pada Gambar 2.



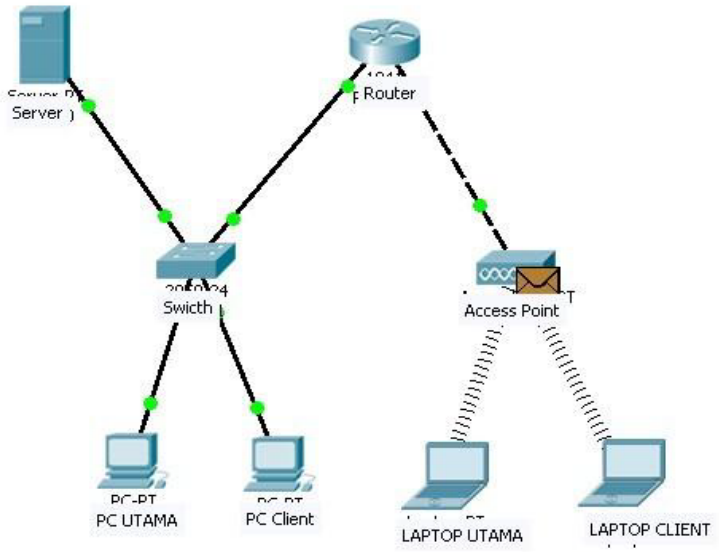
Gambar 2. Tahapan Penelitian

Tahapan meliputi proses *preservation* yaitu barang bukti digital dan pengamanan data yang telah di temukan agar tidak terjadi kehilangan sehingga bisa dilakukan pada tahapan kedua yaitu *collection* mengidentifikasi atau menginvestigasi data yang mencurigakan untuk di kumpulkan data berupa pesan dan menganalisis data yang dihasilkan melalui *capture wireshark* untuk dijadikan barang bukti *file Log* dengan metode *live forensic*.

Hasil dan Pembahasan

Simulasi Kasus Penelitian

Penelitian ini melakukan proses simulasi menggunakan *router* untuk mengirimkan *packet tracer* yang terhubung ke beberapa *device* diatur sesuai *IP address* lalu di konfigurasikan ke perangkat laptop utama, laptop *client*, PC utama dan *PC Client* yang terakses ke jaringan atau belum. Kemudian dilakukan pengujian jaringan melalui laptop utama berupa pesan *ping* untuk mengetahui akses jaringan ke *router* terhubung. Serangan menggunakan PC utama mengirimkan *packet* ke *PC Client* untuk memblokir akses jaringan DNS menjadi *error packet* seperti yang digambarkan pada Gambar 3.



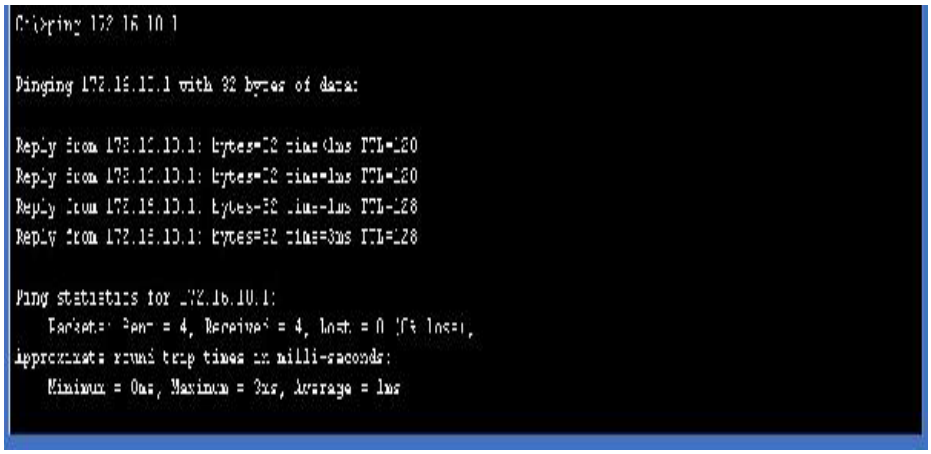
Gambar 3. Simulasi *Router Packet Tracer*

Proses konfigurasi alamat *IP address* jaringan pada server ke *router server*, *router* ke *switch* dan *router* ke PC dan Laptop sehingga akses jaringan bisa saling berhubungan yang ditunjukkan pada Tabel 1.

Tabel 1. Tahapan konfigurasi *router* ke perangkat

Jenis Perangkat	***IP Address***	***Gateway***
Server	*FastEthernet* 0 : 192.168.10.1/24 *FastEthernet* 0/0 : 192.168.10.254/24	192.168.10.254
Router Server	*FastEthernet* 0/1 : 172.16.10.254/24	-
PC Utama	*FastEthernet* 0 : 192.168.10.7/24	192.168.10.254
PC Client	*FastEthernet* 0 :54.255.213.29/24	192.168.10.254
Access Point	*Port 0* *Port 1*	-
Laptop Utama	*Wireless* : 172.16.10.1/16	172.16.10.2
Laptop 2	Wireless : 172.16.10.2/16	172.16.10.254

Setelah melakukan konfigurasi untuk menghubungkan perangkat komputer dan *routing* melalui testing (*ping*) *IP address* dari laptop utama seperti pada Gambar 4 di bawah ini.

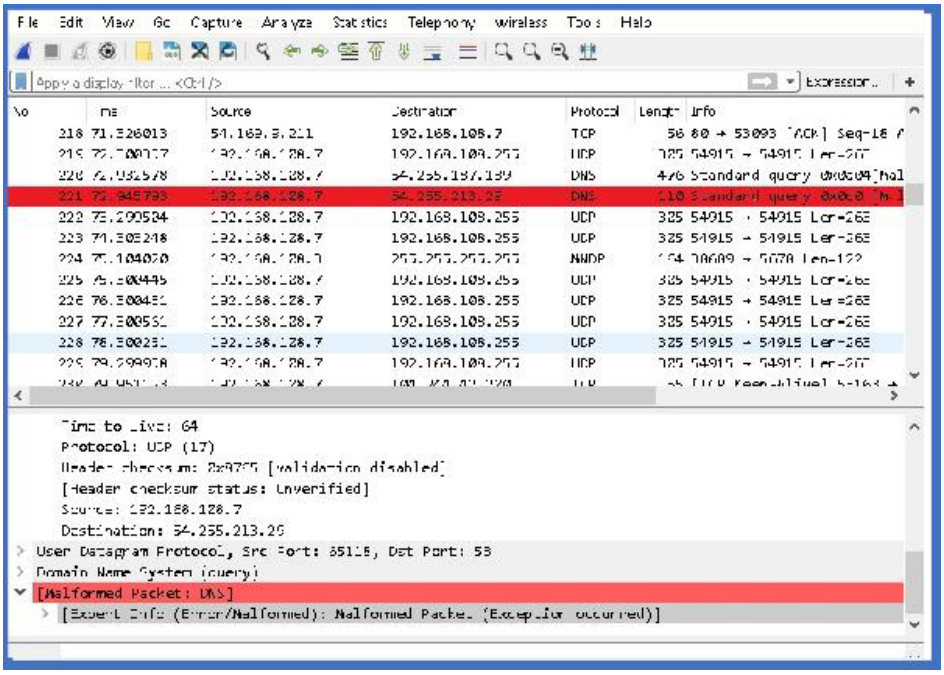


Gambar 4. Testing Akses Jaringan Ping *IP address*

Proses testing menggunakan *IP address* 172.16.10.1 berhasil terakses ke jaringan yang dihubungkan ke Laptop utama. Pesan *ping* untuk mengetahui pengiriman *packet* ke laptop *client* merespons pesan *ping* tersebut.

Pembahasan

Hasil rancangan *router* didapatkan bukti pengiriman pesan mencurigakan atau *packet tracer* melalui *capture tools wireshark* seperti Gambar 5 di bawah ini.



Gambar 5. Testing Akses Jaringan *Ping* pada *IP address*

Hasil dari proses *capture* seperti pada Gambar 5 ditunjukkan berwarna merah merupakan analisa *live forensic* menggunakan *tools wireshark* didapatkan bukti pengiriman *packet* mencurigakan yang dikirimkan ke *PC client* dengan *IP Address* 54.255.213.29 menggunakan protokol DNS dan waktu kejadiannya tercatat. Proses dilanjutkan tahapan analisis dari hasil *capture* dengan *timeline* ±10 jam untuk mendapatkan bukti *file log* seperti pada Gambar 6.

		Prompt	Commad	
72	Wed Jul 10 10:08:47 202! Router 0	Router(config-sub#)#	int Fa010.	
73	Wed Jul 10 10:08:55 202! Router 0	Router(config-sub#)#	ip	
74	Wed Jul 10 10:09:16 202! Router 0	Router(config-sub#)#	encapsulation	encapsulation
75	Wed Jul 10 10:10:08 202! Router 0	Router(config-sub#)#	encapsulation dor1Q 5	encapsulation dor1Q 5
76	Wed Jul 10 10:10:14 202! Router 0	Router(config-sub#)#	encapsulation dor1Q 10	encapsulation dor1Q 10
77	Wed Jul 10 10:10:50 202! Router 0	Router(config-sub#)#	ip address 192.168.10.11 255.255.255.0	ip address 192.168.10.11 255.255.255.0
78	Wed Jul 10 10:11:17 202! Router 0	Router(config-sub#)#	ip address 192.168.10.12 255.255.255.0	ip address 192.168.10.12 255.255.255.0
79	Wed Jul 10 10:12:27 202! Router 0	Router(config-sub#)#	ip address 192.168.10.1 255.255.255.0	ip address 192.168.10.1 255.255.255.0
80	Wed Jul 10 10:13:08 202! Router 0	Router(config-sub#)#	int Fa0/0.24	interface FastEthernet0/0.24
81	Wed Jul 10 10:13:22 202! Router 0	Router(config-sub#)#	int Fa0/0.24	interface FastEthernet0/0.24
82	Wed Jul 10 10:13:48 202! Router 0	Router(config-sub#)#	encap dot1q 24	encapsulation dot1Q 24
83	Wed Jul 10 10:10:14 202! Router 0	Router(config-sub#)#	ip add 192.168.10.1	ip add 192.168.10.1
84	Wed Jul 10 10:14:27 202! Router 0	Router(config-sub#)#	end	end
85	Wed Jul 10 10:21:53 202! Router 0	Router#	configure terminal	configure terminal
86	Wed Jul 10 10:21:54 202! Router 0	Router(config)#	router int	router int
87	Wed Jul 10 10:21:55 202! Router 0	Router(config-router)#	end	end
88	Wed Jul 10 10:21:57 202! Router 0	Router#	configure terminal	configure terminal
89	Wed Jul 10 10:21:57 202! Router 0	Router(config)#	interface FastEthernet0/0	interface FastEthernet0/0
90	Wed Jul 10 10:21:57 202! Router 0	Router(config-if)#	exit	exit
91	Wed Jul 10 10:21:58 202! Router 0	Router(config)#	interface FastEthernet0/1	interface FastEthernet0/1
92	Wed Jul 10 10:21:58 202! Router 0	Router(config-if)#	exit	exit
93	Wed Jul 10 10:22:00 202! Router 0	Router(config)#	interface FastEthernet0/1	interface FastEthernet0/1

Gambar 6. Hasil *Log Packet*

Hasil penelitian ini dilihat Gambar 6, merupakan analisis serangan *DNS router* yang melakukan pengiriman *packet* melalui *IP address* tercatat sebagai data bukti *log realtime*. Analisis menggunakan metode *live forensic* menemukan bukti *packet* mencurigakan tidak terdeteksi atau *error*. Penelitian ini hampir serupa dengan penelitian sebelumnya yang menguji secara analisis forensik jaringan pada serangan *SQL Injection* pada server laman resmi kampus Universitas Gadjah Mada (Putri & Istiyanto, 2012).

Kesimpulan

Hasil penelitian analisis forensik jaringan pada *router* berbasis log menggunakan metode *live forensic* disimpulkan bahwa simulasi yang dilakukan mengetahui proses pengiriman *packet* yang mencurigakan melalui *router* dengan mengakses DNS server dari PC utama ke *PC client IP address* 54.255.213.29 sehingga barang bukti ditemukan sebagai data berupa *log*. *Log* mencatat aktivitas serangan yang dilakukan secara *realtime*, *IP address* server DNS dengan tujuan menerima *packet* mencurigakan dengan memblokir akses jaringan tersebut. Jaringan forensik membantu investigasi, analisis forensik digital. Bukti digital untuk memberikan akses *traffic* ke *router* ke PC dan laptop akan mengakibatkan gangguan jaringan atau data *error*. Selanjutnya penelitian ini bisa dapat difokuskan

pada forensik dengan keamanan jaringan komputer dan aplikasi yang mendukung, metode yang lebih menjangkau proses analisis penelitian-penelitian tersebut.

Referensi

Adawiah, R., & Abror, J. M. (2025). SISTEM KEAMANAN JARINGAN KOMPUTER BERDASARKAN AHLI FORENSIK. *Jurnal Teknologi Informasi: Jurnal Keilmuan Dan Aplikasi Bidang Teknik Informatika*, *19*(1).

Al Hakim, R. R., Putri, E. R. C., Hidayah, H. A., Pangestu, A., & Riani, S. (2022). Current Evidence on Bioinformatics Role and Digital Forensics That Contribute to Forensic Science: Upcoming Threat. *Jurnal Riset Rumpun Matematika Dan Ilmu Pengetahuan Alam*, *1*(1), 25–32. https://doi.org/10.55606/jurrimipa.v1i1.157

Charan, P. V. S., Mohan Anand, P., Shukla, S. K., Selvan, N., & Chunduri, H. (2022). DOTMUG: A Threat Model for Target Specific APT Attacks-Misusing Google Teachable Machine. *10th International Symposium on Digital Forensics and Security, ISDFS 2022*. https://doi.org/10.1109/ISDFS55398.2022.9800780

Damayanti, T. H., & Hikmah, I. R. (2022). Network Forensic Serangan DoS pada Jaringan Cloud berdasarkan Generic Framework for Network Forensics (GFNF). *Edumatic: Jurnal Pendidikan Informatika*, *6*(2), 334–343.

Mandowen, S. A. (2016). Analisis forensik komputer pada lalu lintas jaringan. *Jurnal SAINS*, *16*(1), 14–20.

Ponno, J. D. (2023). Penerapan digital forensik dalam pembuktian pencemaran nama baik di dunia maya. *Lex Administratum*, *12*(1).

Pratama, Y. (2020). MAKING OF DIGITAL FORENSIC READINESS INDEX (DiFRI) MODELS TO MALWARE ATTACKS. *Cyber Security Dan Forensik Digital*, *3*(2), 1–5. https://doi.org/10.14421/CSECURITY.2020.3.2.2005

Putri, R. U., & Istiyanto, J. E. (2012). Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *6*(2), 101–112. https://doi.org/10.22146/IJCCS.2157

Rahmana, R., & Akmalb, G. L. (2024). Forensik Jaringan Untuk Investigasi Kejahatan Cyber. *Jurnal Riset Sistem Informasi*, *1*(3), 70–76.

Ramadhan, R. A., Tira, A. T., & Fadhilah, M. R. (2024). Network Forensic: Analysis of Client Attack and Quality of Service Measurement by ARP Poisoning using Network Forensic Generic Process (NFGP) Model. *SISTEMASI*, *13*(2), 713–727. https://doi.org/10.32520/STMSI.V13I2.3804

Ramadhani, S. S., Saragih, Y. M., Rahim, R., & Siahaan, A. P. U. (2017). Post-Genesis Digital Forensics Investigation. *International Journal of Scientific Research in Science and Technology*, *6*(3), 164–166.

Tasmi, T., Antony, F., & Ubaidillah, U. (2022). NETWORK FORENSIK UNTUK MENGANALISA TRAFIK DATA GAME ONLINE. *Klik - Jurnal Ilmu Komputer*, *3*(1), 50–58. https://doi.org/10.56869/KLIK.V3I1.352

Utami, S. D., Carudin, C., & Ridha, A. A. (2021). ANALISIS LIVE FORENSIC PADA WHATSAPP WEB UNTUK PEMBUKTIAN KASUS PENIPUAN TRANSAKSI ELEKTRONIK. *Cyber Security Dan Forensik Digital*, *4*(1), 24–32. https://doi.org/10.14421/CSECURITY.2021.4.1.2416

Widodo, W., & Sugiantoro, B. (2018). PENERAPAN FRAMEWORK HARMONISED DIGITAL FORENSIC INVESTIGATION PROCESS (HDFIP) UNTUK MENDAPATKAN ARTIFAK BUKTI DIGITAL PADA SMARTPHONE TIZEN. *Cyber Security Dan Forensik Digital*, *1*(2), 67–74. https://doi.org/10.14421/CSECURITY.2018.1.2.1352

Wolverton, M. (2016). Digital forensics in the library. *Nature*, *534*(7605), 139–140. https://doi.org/10.1038/534139a