SAIN TEKOM
ISSN 2088-1770 (Print)
ISSN 2503-3247 (Online)
Vol. 16 No.1 (202x) 85-98

JURNAL
SAINTEKOM
Sains, Teknologi, Komputer, dan Manajemen

Analisis Bukti Digital pada Private Chat Synology Menggunakan Metode Live Forensik

Ryan Achmad Antama[1], *Abdul Hadi[2], Maura Widyaningsing[3]
[1,2, 3)]Teknik Informatika, STMIK Palangkaraya
Jl. G. Obos No. 114, Kota Palangka Raya, Kalimantan Tengah
Email: [1]ryanachmadan@gmail.com, [2]abdulhadi@stmikplk.ac.id, [3]maurawidya@gmail.com

ABSTRACT

The adoption of Network Attached Storage (NAS) based private communication platforms such as Synology Chat is increasing in organizations and may store valuable digital evidence. However, encryption and closed system architecture can limit evidence acquisition using conventional forensic approaches. This study applies network live forensics by proactively capturing network traffic and analyzing capture files to recover deleted chat messages and transferred files. The investigation follows the National Institute of Standards and Technology NIST framework consisting of collection, examination, analysis, and reporting using digital evidence including packet capture PCAP or packet capture next generation PCAPNG files, communication artifacts, and reconstructed file objects. An experimental method is conducted by comparing server-side capturing via Secure Shell SSH on the NAS server and external capturing from a device within the same Local Area Network LAN. Results show that server-side capturing is more effective for file reconstruction and message recovery under certain conditions, while external capturing provides limited artifacts and cannot reveal plain text messages.

Keywords: synology chat; NAS; network live forensics; NIST; digital evidence

ABSTRAK

Penggunaan platform komunikasi privat berbasis Network Attached Storage (NAS) seperti Synology Chat semakin meningkat di lingkungan organisasi dan berpotensi menyimpan bukti digital penting. Namun, enkripsi dan arsitektur sistem yang tertutup dapat membatasi akuisisi bukti menggunakan pendekatan forensik konvensional. Penelitian ini menerapkan network live forensics melalui perekaman lalu lintas jaringan secara proaktif dan analisis berkas tangkapan untuk memulihkan pesan chat serta file yang telah dihapus. Proses forensik mengacu pada kerangka National Institute of Standards and Technology NIST yang meliputi collection, examination, analysis, dan reporting dengan bukti digital berupa file tangkapan jaringan berformat packet capture PCAP atau packet capture next generation PCAPNG, artefak komunikasi, dan objek file transfer. Metode eksperimen dilakukan dengan membandingkan perekaman pada sisi server NAS melalui Secure Shell SSH dan perekaman dari perangkat luar server dalam jaringan Local Area Network LAN yang sama. Hasil menunjukkan perekaman sisi server lebih efektif untuk rekonstruksi file dan pemulihan pesan pada kondisi tertentu, sedangkan perekaman luar server menghasilkan artefak terbatas dan tidak menampilkan pesan plain text.

Kata kunci: synology chat; NAS; perekaman jaringan; NIST; bukti digital

Diterima Redaksi: 28-01-2026 | Selesai Revisi: 14-04-2026 | Diterbitkan Online: 31-03-2026

1. PENDAHULUAN

Perkembangan teknologi penyimpanan terpusat berbasis Network Attached Storage (NAS) mendorong organisasi mengintegrasikan layanan komunikasi internal dalam satu sistem terkelola. Synology Chat merupakan aplikasi pesan instan privat berbasis NAS yang menyediakan kontrol akses, integrasi layanan, serta dukungan keamanan. Data komunikasi yang dihasilkan berpotensi menjadi bukti digital penting dalam konteks hukum, seperti pelanggaran kebijakan internal maupun kebocoran data (Jafri et al., 2022; Malpani et al., 2025; Mpungu et al., 2024). Oleh karena itu, kesiapan forensik digital menjadi krusial untuk mendukung proses investigasi yang akurat dan dapat dipertanggung jawabkan.

Akuisisi bukti digital pada sistem ini menghadapi tantangan karena berjalan dalam kondisi aktif (live system), sehingga harus dilakukan tanpa mengganggu operasional serta mampu menangkap data yang dinamis dan volatil. Penelitian Fitriani Shabira dan Fachri (2025) menunjukkan keterbatasan dalam menangkap artefak pada perangkat aktif, sementara penelitian Fahrudin dan Zaida Muflih (2024) menyoroti kendala enkripsi pada aplikasi komunikasi seperti WhatsApp.

Namun, masih terdapat kesenjangan penelitian pada analisis forensik digital aplikasi komunikasi privat berbasis NAS. Penelitian sebelumnya umumnya berfokus pada aplikasi berbasis mobile dan belum banyak membahas artefak jaringan serta perbandingan metode akuisisi pada lingkungan NAS yang bersifat tertutup.

Penelitian ini mengusulkan pendekatan live forensics berbasis perekaman lalu lintas jaringan. Kebaruan penelitian terletak pada perbandingan metode server-side capture dan external capture dalam konteks NAS, yang masih jarang dikaji. Server-side capture memberikan akses langsung ke lalu lintas server, sedangkan external capture bergantung pada pemantauan trafik jaringan (Putra et al., 2023).

Kontribusi utama penelitian ini adalah membandingkan efektivitas kedua metode tersebut dalam memperoleh bukti digital, sekaligus mengidentifikasi artefak jaringan dan potensi pemulihan data. Tujuan penelitian ini adalah mengidentifikasi artefak forensik jaringan Synology Chat,

DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis

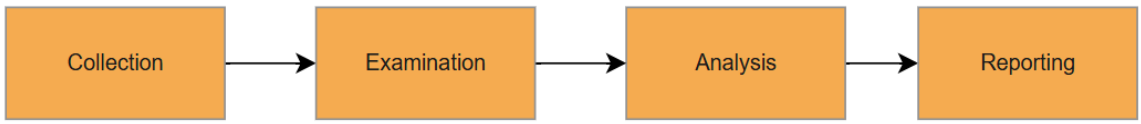
mengevaluasi potensi pemulihan data, serta menilai efektivitas metode akuisisi. Penelitian ini penting mengingat meningkatnya penggunaan sistem komunikasi privat berbasis NAS, sehingga diperlukan pendekatan forensik yang tepat.

Ruang lingkup penelitian ini dibatasi pada analisis artefak jaringan menggunakan metode *live forensics*. Penelitian tidak mencakup akuisisi memori volatile (RAM), analisis proses pada sistem *DiskStation Manager* (DSM), maupun ekstraksi dan analisis basis data internal seperti PostgreSQL atau SQLite.

2. METODE

Penelitian ini menggunakan pendekatan eksperimen dengan metode *live forensics* pada layanan private chat Synology Chat. Gambar 1 berisi proses investigasi mengacu pada kerangka kerja forensik NIST yang meliputi tahapan *collection, examination, analysis,* dan *reporting*. Penelitian dilakukan dengan membandingkan dua lokasi perekaman lalu lintas jaringan (*capture point*), yaitu server-side capture pada NAS melalui akses SSH dan external capture dari perangkat luar server namun masih berada dalam jaringan LAN yang sama. Perbandingan ini dilakukan untuk menguji pengaruh lokasi perekaman terhadap keberhasilan pemulihan bukti digital berupa pesan chat dan file yang telah dihapus pada tingkat aplikasi.

Lingkungan uji terdiri dari satu server NAS Synology yang menjalankan layanan Synology Chat serta dua perangkat klien sebagai pengguna uji. Sumber data penelitian berasal dari lalu lintas jaringan yang terbentuk saat pengguna pertama mengirimkan pesan teks dan file kepada pengguna kedua melalui Synology Chat. Setelah proses pengiriman selesai, pesan dan file dihapus melalui antarmuka aplikasi untuk mensimulasikan penghapusan bukti digital. Proses perekaman lalu lintas jaringan dilakukan menggunakan aplikasi Wireshark dan menghasilkan berkas *packet capture* (PCAP) berformat .pcapng pada masing-masing skenario perekaman. Selain itu, penelitian memanfaatkan akses Secure Shell (SSH)



Gambar 1. Framework NIST

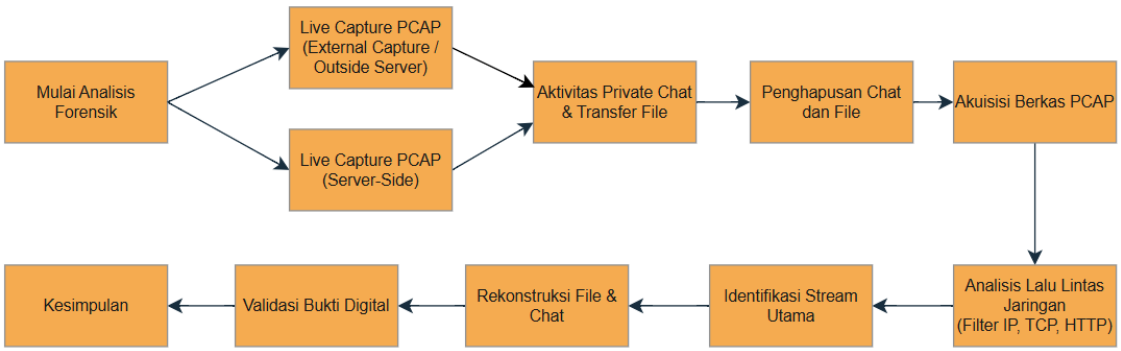
DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis

pada server untuk menjalankan perekaman jaringan pada skenario server-side capture, serta perhitungan hash Message Digest 5 MD5 pada sistem operasi untuk validasi integritas file hasil pemulihan.

Tahapan penelitian meliputi *setup, capture, analisis, validasi,* dan *interpretasi* dengan alur penelitian seperti Gambar 2. Pada tahap *setup*, peneliti menyiapkan layanan Synology Chat pada NAS, memastikan kedua klien dapat terhubung dalam jaringan LAN yang sama, serta menentukan alamat Internet Protocol (IP) yang digunakan pada komunikasi.

Pada tahap analisis, berkas tangkapan jaringan diperiksa melalui penyaringan paket berdasarkan alamat Internet Protocol (IP) sumber dan tujuan, pemeriksaan statistik menggunakan fitur Conversations, identifikasi stream utama pada protokol TCP, serta pemeriksaan konten komunikasi melalui fitur Follow TCP Stream untuk melihat kemungkinan keberadaan pesan dalam bentuk plain text. Untuk file, dilakukan pemeriksaan menggunakan fitur Export Objects pada protokol Hypertext Transfer Protocol HTTP untuk menilai apakah objek file dapat diekstraksi dari berkas tangkapan.

Pada tahap validasi, file hasil



Gambar 2. Alur Penelitian

Pada tahap *capture*, Wireshark digunakan untuk merekam lalu lintas jaringan pada dua skenario perekaman, yaitu perekaman langsung pada server NAS server-side capture dan perekaman dari perangkat luar server external capture. Hasil perekaman disimpan dalam format .pcapng.

ekstraksi yang berhasil dipulihkan diverifikasi menggunakan nilai hash MD5 untuk memastikan integritas bukti digital. Nilai hash MD5 dihitung pada setiap file hasil pemulihan dan dicatat sebagai identitas unik file bukti digital. Pada tahap interpretasi, hasil analisis dibandingkan antara skenario server-side

DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis

capture dan external capture untuk menentukan efektivitas masing-masing lokasi perekaman dalam memulihkan pesan chat dan file yang telah dihapus pada tingkat aplikasi.

3. HASIL DAN PEMBAHASAN

Penelitian ini membandingkan dua lokasi perekaman lalu lintas jaringan pada layanan private chat Synology, yaitu server-side capture melalui SSH pada NAS Synology dan external capture dari perangkat luar server dalam jaringan LAN yang sama. Pada kedua skenario dilakukan pengiriman pesan chat dan file antar pengguna, kemudian pesan dan file dihapus melalui antarmuka aplikasi untuk mensimulasikan penghapusan bukti digital. Pada skenario server-side capture, komunikasi Synology Chat berhasil diidentifikasi dan analisis Wireshark menunjukkan adanya stream dengan volume data besar yang mengindikasikan aktivitas transfer file. File yang dikirim dapat diekstraksi menggunakan fitur *Export Objects* dan berhasil dibuka kembali, sehingga rekonstruksi file dinyatakan berhasil. Selain itu, analisis payload menggunakan *Follow* Transmission Control Protocol (*TCP) Stream* menunjukkan bahwa pesan chat tertentu masih dapat ditemukan dalam bentuk plain text meskipun telah dihapus dari aplikasi.

Sebaliknya, pada skenario external capture, tidak ditemukan indikasi file maupun pesan chat yang dapat dipulihkan. Pemeriksaan *Export Objects HTTP* hanya menampilkan objek komunikasi seperti entry.cgi dan query.cgi tanpa adanya objek file, serta pencarian string pesan uji tidak menghasilkan temuan. Hal ini menunjukkan bahwa perekaman dari luar server tidak memberikan artefak yang cukup untuk rekonstruksi bukti digital, meskipun berada dalam jaringan LAN yang sama.

3.1. Hasil Server-Side Capture

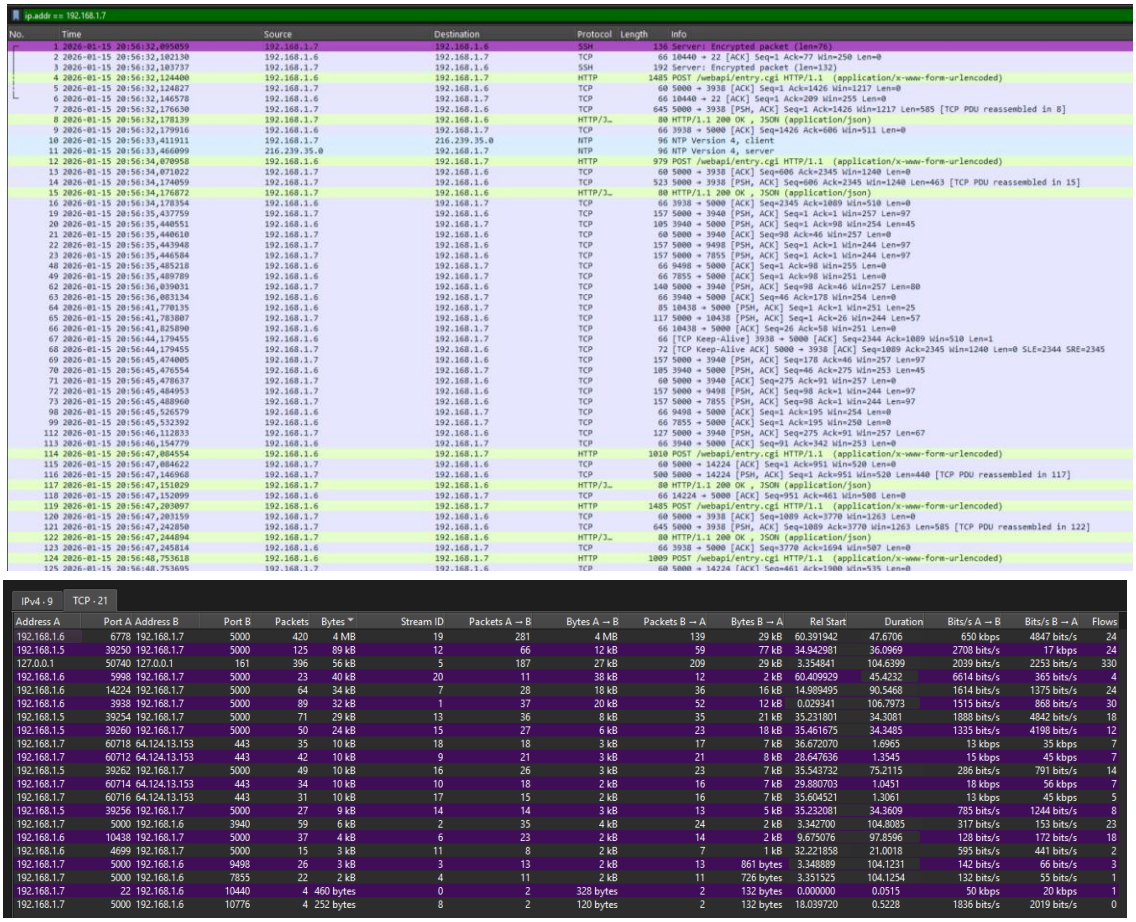
Pada skenario *server-side capture*, proses perekaman lalu lintas jaringan dilakukan langsung pada server NAS Synology melalui akses SSH sebelum aktivitas komunikasi berlangsung, sehingga seluruh artefak jaringan dapat terekam secara menyeluruh. Hasil penyaringan paket berdasarkan alamat IP yang relevan menunjukkan adanya komunikasi antara klien dan server Synology Chat, seperti dapat dilihat pada Gambar 3. Analisis

DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis

menggunakan fitur *TCP Conversations* menunjukkan adanya stream dengan volume data terbesar dapat dilihat pada Gambar 4.

Secara analitis, besarnya volume data pada stream ini mengindikasikan aktivitas transfer data intensif, seperti pengiriman file. Hal ini terjadi karena file yang dikirim akan menghasilkan payload berukuran besar dibandingkan pesan teks biasa, sehingga dapat diidentifikasi melalui karakteristik statistik trafik.

Tahap ekstraksi menggunakan *Export Objects HTTP* menghasilkan objek file seperti *image/png* (pdf.png dan txt.png) yang dapat dibuka kembali seperti ditunjukkan pada Gambar 5**.** Keberhasilan ini menunjukkan bahwa artefak file masih dapat direkonstruksi dari tangkapan jaringan pada sisi server.

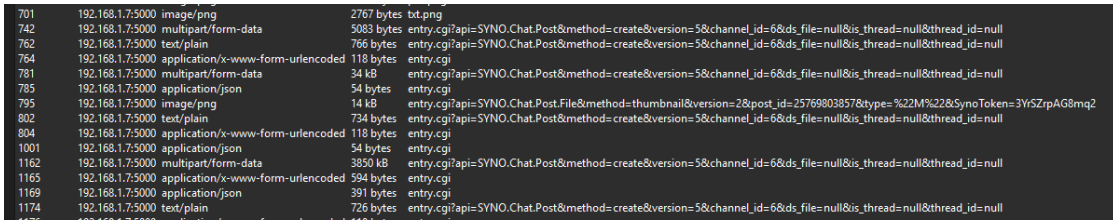


IPv4 · 9 TCP · 21

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	Flows
192.168.1.6	6778	192.168.1.7	5000	420	4 MB	19	281	4 MB	139	29 kB	60.391942	47.6706	650 kbps	4847 bits/s	24
192.168.1.5	39250	192.168.1.7	5000	125	89 kB	12	66	12 kB	59	77 kB	34.942981	36.0969	2708 bits/s	17 kbps	24
127.0.0.1	50740	127.0.0.1	161	396	56 kB	5	187	27 kB	209	29 kB	3.354841	104.6399	2039 bits/s	2253 bits/s	330
192.168.1.6	5998	192.168.1.7	5000	23	40 kB	20	11	38 kB	12	2 kB	60.409929	45.4232	6614 bits/s	365 bits/s	4
192.168.1.6	14224	192.168.1.7	5000	64	34 kB	7	28	18 kB	36	16 kB	14.989495	90.5468	1614 bits/s	1375 bits/s	24
192.168.1.6	3938	192.168.1.7	5000	89	32 kB	1	37	20 kB	52	12 kB	0.029341	106.7973	1515 bits/s	868 bits/s	30
192.168.1.5	39254	192.168.1.7	5000	71	29 kB	13	36	8 kB	35	21 kB	35.231801	34.3081	1888 bits/s	4842 bits/s	18
192.168.1.5	39260	192.168.1.7	5000	50	24 kB	15	27	6 kB	23	18 kB	35.461675	34.3485	1335 bits/s	4198 bits/s	12
192.168.1.7	60718	64.124.13.153	443	35	10 kB	18	18	3 kB	17	7 kB	36.672070	1.6965	13 kbps	35 kbps	7
192.168.1.7	60712	64.124.13.153	443	42	10 kB	9	21	3 kB	21	8 kB	28.647636	1.3545	15 kbps	45 kbps	7
192.168.1.5	39262	192.168.1.7	5000	49	10 kB	16	26	3 kB	23	7 kB	35.543732	75.2115	286 bits/s	791 bits/s	14
192.168.1.7	60714	64.124.13.153	443	34	10 kB	10	18	2 kB	16	7 kB	29.880703	1.0451	18 kbps	56 kbps	7
192.168.1.7	60716	64.124.13.153	443	31	10 kB	17	15	2 kB	16	7 kB	35.604521	1.3061	13 kbps	45 kbps	5
192.168.1.5	39256	192.168.1.7	5000	27	9 kB	14	14	3 kB	13	5 kB	35.232081	34.3609	785 bits/s	1244 bits/s	8
192.168.1.7	5000	192.168.1.6	3940	59	6 kB	2	35	4 kB	24	2 kB	3.342700	104.8085	317 bits/s	153 bits/s	23
192.168.1.6	10438	192.168.1.7	5000	37	4 kB	6	23	2 kB	14	2 kB	9.675076	97.8596	128 bits/s	172 bits/s	18
192.168.1.6	4699	192.168.1.7	5000	15	3 kB	11	8	2 kB	7	1 kB	32.221858	21.0018	595 bits/s	441 bits/s	2
192.168.1.7	5000	192.168.1.6	9498	26	3 kB	3	13	2 kB	13	861 bytes	3.348889	104.1231	142 bits/s	66 bits/s	3
192.168.1.7	5000	192.168.1.6	7855	22	2 kB	4	11	2 kB	11	726 bytes	3.351525	104.1254	132 bits/s	55 bits/s	1
192.168.1.7	22	192.168.1.6	10440	4	460 bytes	0	2	328 bytes	2	132 bytes	0.000000	0.0515	50 kbps	20 kbps	1
192.168.1.7	5000	192.168.1.6	10776	4	252 bytes	8	2	120 bytes	2	132 bytes	18.039720	0.5228	1836 bits/s	2019 bits/s	0

Gambar 4. Statistik TCP Converstation pada server-side capture sebagai indikasi stream utama

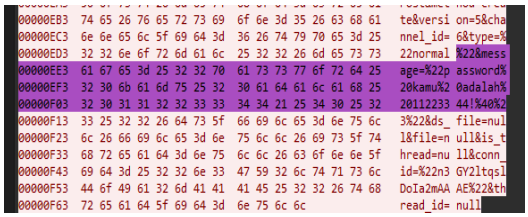
DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis



701	192.168.1.7:5000	image/png	2767 bytes	txt.png
742	192.168.1.7:5000	multipart/form-data	5083 bytes	entry.cgi?api=SYNO.Chat.Post&method=create&version=5&channel_id=6&ds_file=null&is_thread=null&thread_id=null
762	192.168.1.7:5000	text/plain	766 bytes	entry.cgi?api=SYNO.Chat.Post&method=create&version=5&channel_id=6&ds_file=null&is_thread=null&thread_id=null
764	192.168.1.7:5000	application/x-www-form-urlencoded	118 bytes	entry.cgi
781	192.168.1.7:5000	multipart/form-data	34 kB	entry.cgi?api=SYNO.Chat.Post&method=create&version=5&channel_id=6&ds_file=null&is_thread=null&thread_id=null
785	192.168.1.7:5000	application/json	54 bytes	entry.cgi
795	192.168.1.7:5000	image/png	14 kB	entry.cgi?api=SYNO.Chat.Post.File&method=thumbnail&version=2&post_id=25769803857&type=%22M%22&SynoToken=3YrSZrpAG8mq2
802	192.168.1.7:5000	text/plain	734 bytes	entry.cgi?api=SYNO.Chat.Post&method=create&version=5&channel_id=6&ds_file=null&is_thread=null&thread_id=null
804	192.168.1.7:5000	application/x-www-form-urlencoded	118 bytes	entry.cgi
1001	192.168.1.7:5000	application/json	54 bytes	entry.cgi
1162	192.168.1.7:5000	multipart/form-data	3850 kB	entry.cgi?api=SYNO.Chat.Post&method=create&version=5&channel_id=6&ds_file=null&is_thread=null&thread_id=null
1165	192.168.1.7:5000	application/x-www-form-urlencoded	594 bytes	entry.cgi
1169	192.168.1.7:5000	application/json	391 bytes	entry.cgi
1174	192.168.1.7:5000	text/plain	726 bytes	entry.cgi?api=SYNO.Chat.Post&method=create&version=5&channel_id=6&ds_file=null&is_thread=null&thread_id=null

Gambar 5. Hasil Export Objects pada Server-side Capture

Secara teknis, hal ini terjadi karena perekaman dilakukan pada titik di mana server memproses data. Pada arsitektur komunikasi berbasis HTTPS/TLS, data memang dienkripsi saat transmisi, namun di sisi server data akan berada dalam kondisi terdekripsi saat diproses oleh aplikasi. Kondisi ini memungkinkan Wireshark menangkap representasi file dalam bentuk yang עדיין dapat diekstraksi. Analisis payload menggunakan *Follow TCP Stream* seperti terlihat pada Gambar 6.



```
00000EB3  74 65 26 76 65 72 73 69  6f 6e 3d 35 26 63 68 61  te&versi on=5&cha
00000EC3  6e 6e 65 6c 5f 69 64 3d  36 26 74 79 70 65 3d 25  nnel_id= 6&type=%
00000ED3  32 32 6e 6f 72 6d 61 6c  25 32 32 26 6d 65 73 73  22normal %22&mess
00000EE3  61 67 65 3d 25 32 32 70  61 73 73 77 6f 72 64 25  age=%22p assword%
00000EF3  32 30 6b 61 6d 75 25 32  30 61 64 61 6c 61 68 25  20kamu%2 0adalah%
00000F03  32 30 31 31 32 32 33 33  34 34 21 25 34 30 25 32  20112233 44!%40%2
00000F13  33 25 32 32 26 64 73 5f  66 69 6c 65 3d 6e 75 6c  3%22&ds_ file=nul
00000F23  6c 26 66 69 6c 65 3d 6e  75 6c 6c 26 69 73 5f 74  l&file=n ull&is_t
00000F33  68 72 65 61 64 3d 6e 75  6c 6c 26 63 6f 6e 6e 5f  hread=nu ll&conn_
00000F43  69 64 3d 25 32 32 6e 33  47 59 32 6c 74 71 73 6c  id=%22n3 GY2ltqsl
00000F53  44 6f 49 61 32 6d 41 41  41 45 25 32 32 26 74 68  DoIa2mAA AE%22&th
00000F63  72 65 61 64 5f 69 64 3d  6e 75 6c 6c              read_id= null
```

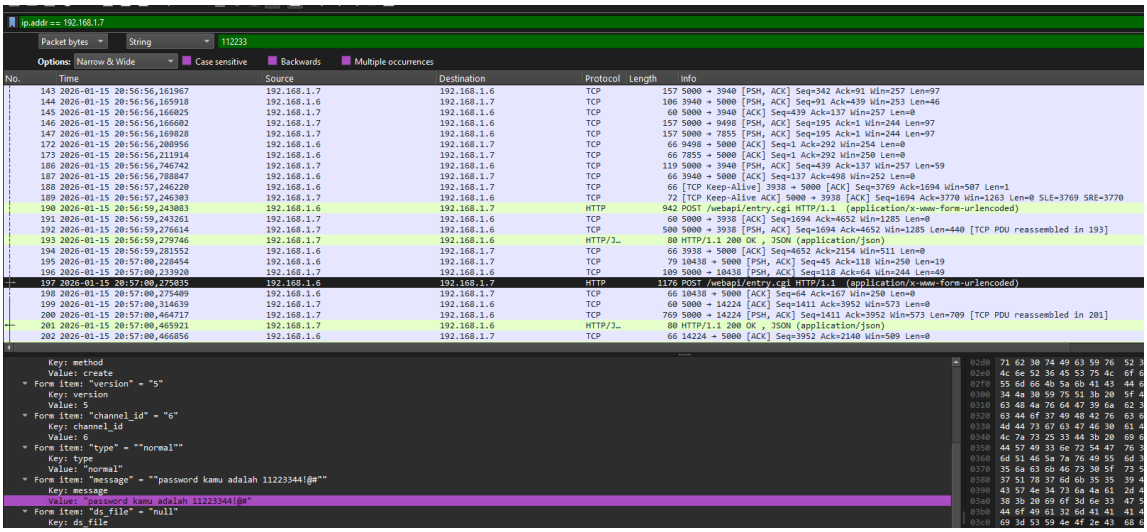
Gambar 6. Hasil Follow TCP Stream pada server-side capture

Pencarian string menunjukkan bahwa pesan "11223344!@#" dapat ditemukan dalam payload komunikasi ditunjukkan pada Gambar 7. Temuan ini memperlihatkan bahwa sebagian konten komunikasi masih dapat muncul dalam bentuk yang dapat dibaca (*plain text*) pada sisi server. Secara analitis, hal ini dapat terjadi karena tidak seluruh lapisan komunikasi diamankan secara end-to-end pada level payload, atau terdapat komunikasi internal (misalnya Application Programming Interface (API) request/response) yang telah didekripsi oleh server sebelum dikirimkan kembali.

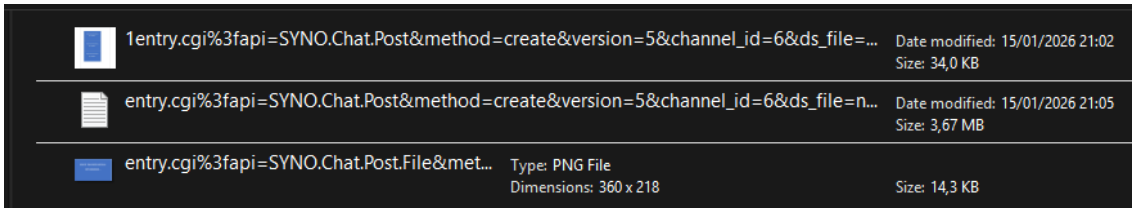
Hasil pada Gambar 7 juga menunjukkan bahwa Wireshark mampu mengarahkan investigator ke paket spesifik yang mengandung string tersebut. Hal ini penting secara forensik karena memungkinkan analisis dilanjutkan ke tingkat yang lebih detail, seperti pemeriksaan packet details, frame number, dan timestamp untuk menyusun kronologi komunikasi. Dengan demikian, investigator dapat menentukan kapan pesan dikirim, antara siapa komunikasi berlangsung, dan dalam sesi TCP yang mana.

Secara keseluruhan, keberhasilan pada skenario ini (dibuktikan kembali melalui file hasil ekstraksi pada Gambar 8, terjadi karena lokasi perekaman

DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis



Gambar 7. Temuan Pesan Chat Plaintext pada Server-side Capture



Gambar 8. Bukti File hasil Ekstraksi Tersimpan

berada di dalam *trust boundary* sistem, yaitu pada server yang memiliki akses terhadap data sebelum atau setelah proses enkripsi. Dengan kata lain, keterbatasan *network capture* terhadap data terenkripsi dapat diminimalkan karena capture dilakukan pada titik strategis yang memiliki visibilitas terhadap payload asli.

3.2. Hasil External Capture

Pada skenario *external capture*, perekaman dilakukan dari perangkat di luar server namun masih dalam jaringan LAN yang sama. Tujuannya adalah untuk menguji apakah bukti digital tetap dapat dipulihkan tanpa akses langsung ke server. Setelah dilakukan pengiriman dan penghapusan pesan serta file, hasil analisis *Export Objects HTTP* hanya menampilkan objek komunikasi API seperti *entry.cgi* dan *query.cgi* dengan tipe *application/json* dan *application/x-www-form-urlencoded*. Temuan ini dapat dilihat pada Gambar 9. Tidak ditemukan objek file yang dapat diekstraksi.

Secara analitis, hal ini terjadi karena data yang ditangkap pada posisi ini merupakan data yang sedang ditransmisikan dalam kondisi terenkripsi menggunakan TLS. Berbeda dengan server-side capture, pada external

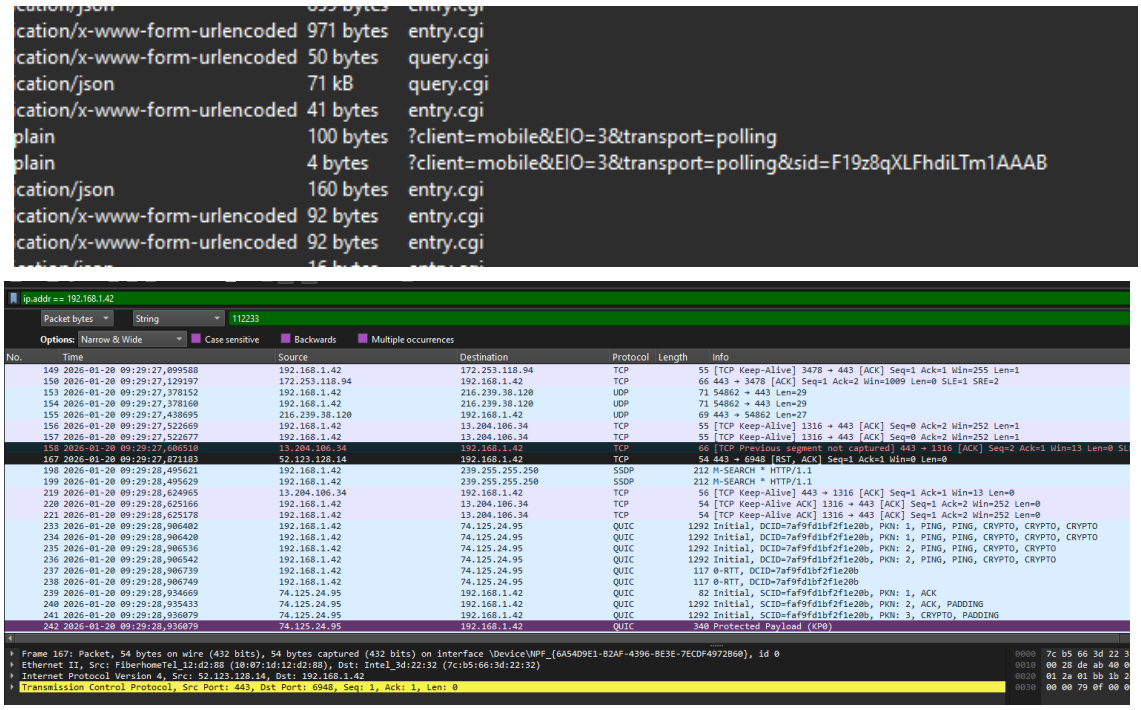
DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis

capture investigator tidak memiliki akses ke proses dekripsi, sehingga payload yang ditangkap hanya berupa ciphertext. Akibatnya, Wireshark tidak dapat merekonstruksi file karena tidak dapat menginterpretasikan isi data terenkripsi tersebut.

Pencarian string "112233" juga tidak menghasilkan temuan yang dapat dilihat pada Gambar 10, yang mengindikasikan bahwa pesan chat tidak tersedia dalam bentuk plain text pada lalu lintas jaringan yang ditangkap. Hal ini konsisten dengan konsep enkripsi, di mana isi komunikasi disembunyikan selama transmisi sehingga tidak dapat dibaca tanpa kunci dekripsi.

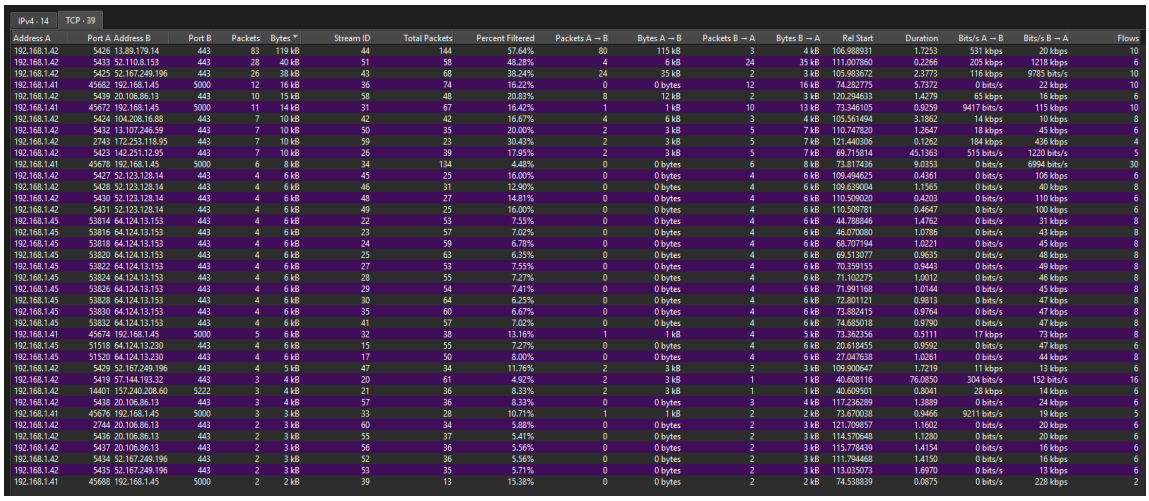
Meskipun demikian, analisis *TCP Conversations* tetap menunjukkan adanya aktivitas komunikasi jaringan pada Gambar 11. Ini menunjukkan bahwa koneksi antara klien dan server tetap terjadi, namun tidak memberikan artefak yang cukup untuk analisis forensik lebih lanjut. Dengan kata lain, external capture hanya memberikan visibilitas pada metadata komunikasi (seperti IP, port, dan volume trafik), tetapi tidak pada isi komunikasi.

Secara keseluruhan, keterbatasan pada skenario ini disebabkan oleh dua faktor utama: (1) penggunaan enkripsi TLS yang melindungi payload selama



Gambar 10. Hasil Pencarian String "112233" pada External Capture tidak ditemukan

DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis



IPv4 · 14 TCP · 39

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	Flows
192.168.1.42	5426	13.89.179.14	443	83	119 kB	44	144	57.64%	80	115 kB	3	4 kB	106.988931	1.7253	531 kbps	20 kbps	10
192.168.1.42	5433	52.110.8.153	443	28	40 kB	51	58	48.28%	4	6 kB	24	35 kB	111.007860	0.2266	209 kbps	1218 kbps	6
192.168.1.42	5425	52.167.249.196	443	26	38 kB	43	68	38.24%	24	35 kB	2	3 kB	105.983672	2.3773	116 kbps	9785 bits/s	10
192.168.1.41	45682	192.168.1.45	5000	12	16 kB	36	74	16.22%	0	0 bytes	12	16 kB	74.282775	5.7372	0 bits/s	22 kbps	10
192.168.1.42	5439	20.106.86.13	443	10	15 kB	58	48	20.83%	8	12 kB	2	3 kB	120.294633	1.4279	65 kbps	16 kbps	6
192.168.1.41	45672	192.168.1.45	5000	11	14 kB	31	67	16.42%	1	1 kB	10	13 kB	73.346105	0.9259	9417 bits/s	115 kbps	10
192.168.1.42	5424	104.208.16.88	443	7	10 kB	42	42	16.67%	4	6 kB	3	4 kB	105.561494	3.1862	14 kbps	10 kbps	8
192.168.1.42	5432	13.107.246.59	443	7	10 kB	50	35	20.00%	2	3 kB	5	7 kB	110.747820	1.2647	18 kbps	45 kbps	6
192.168.1.42	2743	172.253.118.95	443	7	10 kB	59	23	30.43%	2	3 kB	5	7 kB	121.440306	0.1262	184 kbps	436 kbps	4
192.168.1.42	5423	142.251.12.95	443	7	10 kB	26	39	17.95%	2	3 kB	5	7 kB	69.715814	45.1363	515 bits/s	1220 bits/s	5
192.168.1.41	45678	192.168.1.45	5000	6	8 kB	34	134	4.48%	0	0 bytes	6	8 kB	73.817436	9.0353	0 bits/s	6994 bits/s	30
192.168.1.42	5427	52.123.128.14	443	4	6 kB	45	25	16.00%	0	0 bytes	4	6 kB	109.494625	0.4361	0 bits/s	106 kbps	6
192.168.1.42	5428	52.123.128.14	443	4	6 kB	46	31	12.90%	0	0 bytes	4	6 kB	109.639004	1.1565	0 bits/s	40 kbps	8
192.168.1.42	5430	52.123.128.14	443	4	6 kB	48	27	14.81%	0	0 bytes	4	6 kB	110.509020	0.4203	0 bits/s	110 kbps	6
192.168.1.42	5431	52.123.128.14	443	4	6 kB	49	25	16.00%	0	0 bytes	4	6 kB	110.509781	0.4647	0 bits/s	100 kbps	6
192.168.1.45	53814	64.124.13.153	443	4	6 kB	22	53	7.55%	0	0 bytes	4	6 kB	44.788846	1.4762	0 bits/s	31 kbps	8
192.168.1.45	53816	64.124.13.153	443	4	6 kB	23	57	7.02%	0	0 bytes	4	6 kB	46.070080	1.0786	0 bits/s	43 kbps	8
192.168.1.45	53818	64.124.13.153	443	4	6 kB	24	59	6.78%	0	0 bytes	4	6 kB	68.707194	1.0221	0 bits/s	45 kbps	8
192.168.1.45	53820	64.124.13.153	443	4	6 kB	25	63	6.35%	0	0 bytes	4	6 kB	69.513077	0.9635	0 bits/s	48 kbps	8
192.168.1.45	53822	64.124.13.153	443	4	6 kB	27	53	7.55%	0	0 bytes	4	6 kB	70.359155	0.9443	0 bits/s	49 kbps	8
192.168.1.45	53824	64.124.13.153	443	4	6 kB	28	55	7.27%	0	0 bytes	4	6 kB	71.102275	1.0012	0 bits/s	46 kbps	8
192.168.1.45	53826	64.124.13.153	443	4	6 kB	29	54	7.41%	0	0 bytes	4	6 kB	71.991168	1.0144	0 bits/s	45 kbps	8
192.168.1.45	53828	64.124.13.153	443	4	6 kB	30	64	6.25%	0	0 bytes	4	6 kB	72.801121	0.9813	0 bits/s	47 kbps	8
192.168.1.45	53830	64.124.13.153	443	4	6 kB	35	60	6.67%	0	0 bytes	4	6 kB	73.882415	0.9764	0 bits/s	47 kbps	8
192.168.1.45	53832	64.124.13.153	443	4	6 kB	41	57	7.02%	0	0 bytes	4	6 kB	74.685018	0.9790	0 bits/s	47 kbps	8
192.168.1.41	45674	192.168.1.45	5000	5	6 kB	32	38	13.16%	1	1 kB	4	5 kB	73.362356	0.5111	17 kbps	73 kbps	8
192.168.1.45	51518	64.124.13.230	443	4	6 kB	15	55	7.27%	0	0 bytes	4	6 kB	20.618455	0.9592	0 bits/s	47 kbps	6
192.168.1.45	51520	64.124.13.230	443	4	6 kB	17	50	8.00%	0	0 bytes	4	6 kB	27.047638	1.0261	0 bits/s	44 kbps	8
192.168.1.42	5429	52.167.249.196	443	4	5 kB	47	34	11.76%	2	3 kB	2	3 kB	109.900647	1.7219	11 kbps	13 kbps	6
192.168.1.42	5419	57.144.193.32	443	3	4 kB	20	61	4.92%	2	3 kB	1	1 kB	40.608116	76.0850	304 bits/s	152 bits/s	16
192.168.1.42	14401	157.240.208.60	5222	3	4 kB	21	36	8.33%	2	3 kB	1	1 kB	40.609501	0.8041	28 kbps	14 kbps	6
192.168.1.42	5438	20.106.86.13	443	3	4 kB	57	36	8.33%	0	0 bytes	3	4 kB	117.236289	1.3889	0 bits/s	24 kbps	6
192.168.1.41	45676	192.168.1.45	5000	3	3 kB	33	28	10.71%	1	1 kB	2	2 kB	73.670038	0.9466	9211 bits/s	19 kbps	5
192.168.1.42	2744	20.106.86.13	443	2	3 kB	60	34	5.88%	0	0 bytes	2	3 kB	123.709857	1.1602	0 bits/s	20 kbps	6
192.168.1.42	5436	20.106.86.13	443	2	3 kB	55	37	5.41%	0	0 bytes	2	3 kB	114.570648	1.1280	0 bits/s	20 kbps	6
192.168.1.42	5437	20.106.86.13	443	2	3 kB	56	36	5.56%	0	0 bytes	2	3 kB	115.778439	1.4154	0 bits/s	16 kbps	6
192.168.1.42	5434	52.167.249.196	443	2	3 kB	52	36	5.56%	0	0 bytes	2	3 kB	111.794468	1.4150	0 bits/s	16 kbps	6
192.168.1.42	5435	52.167.249.196	443	2	3 kB	53	35	5.71%	0	0 bytes	2	3 kB	113.035073	1.6970	0 bits/s	13 kbps	6
192.168.1.41	45688	192.168.1.45	5000	2	2 kB	39	13	15.38%	0	0 bytes	2	2 kB	74.538839	0.0875	0 bits/s	228 kbps	2

Gambar 11. Statistik TCP Conversations pada External capture

transmisi, dan (2) posisi capture yang berada di luar sistem sehingga tidak memiliki akses terhadap data dalam kondisi terdekripsi. Hal ini menjelaskan mengapa, meskipun berada dalam jaringan LAN yang sama, bukti digital berupa isi pesan dan file tidak dapat direkonstruksi.

3.3 Perbandingan Hasil dan Pembahasan

Berdasarkan hasil pengujian, lokasi perekaman (capture point) berpengaruh signifikan terhadap keberhasilan pemulihan bukti digital pada layanan private chat Synology. Pada skenario *server-side capture*, artefak komunikasi lebih lengkap sehingga memungkinkan ekstraksi file (Gambar 4) dan pemulihan pesan plain text (Gambar 6). Sebaliknya, *external capture* hanya menangkap komunikasi API tanpa objek file (Gambar 8) dan pesan plain text (Gambar 9). Hal ini menegaskan bahwa perekaman di sisi server lebih efektif dibandingkan eksternal meskipun dalam jaringan yang sama seperti yang ditampilkan pada Tabel 1.

Tabel 1. Perbandingan Hasil Server-Side Capture dan External Capture

Aspek	Server-Side Capture	External Capture
Lokasi Capture	Dalam server (*trust boundary*)	Di luar server (LAN)
Status Data	Terdekripsi saat diproses	Terenkripsi (TLS)
Ekstraksi File	Berhasil (image/png ditemukan)	Tidak berhasil
Pesan (*plaintext*)	Ditemukan (“11223344!@#”)	Tidak ditemukan
Visibilitas Payload	Tinggi	Tidak tersedia
Visibilitas Metadata	Tersedia	Tersedia
Analisis Forensik	Mendalam (file + isi pesan)	Terbatas (hanya metadata)
Efektivitas Pemulihan Bukti	Tinggi	Rendah

DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis

File hasil ekstraksi pada *server-side capture* divalidasi menggunakan hash MD5, dan perbandingannya dengan *external capture* ditampilkan pada Tabel 2.

Tabel 2. Hash MD 5

No	Nama File	Format	Side Capture	MD5 (Server-side)	External Capture	MD5 (Outside)
1	Bukti data 1	.pdf	Berhasil dipulihkan	*2D9E72155 E43FFF96D BF9F1645A 21549*	Tidak ditemukan objek file	-
2	Bukti data 2	.txt	Berhasil dipulihkan	*34B8F3B25 14AED5A8A 8932DCD2B 89761*	Tidak ditemukan objek file	-
3	Bukti data 3	.png	Berhasil dipulihkan	*F689731C9 CCEA1036E CA9550119 CDA6A*	Tidak ditemukan objek file	-

4. KESIMPULAN

Penelitian ini menunjukkan bahwa metode *server-side capture* lebih efektif dibandingkan *external capture* dalam pemulihan bukti digital pada komunikasi privat Synology Chat. Melalui pendekatan ini, pesan chat berhasil diperoleh dalam bentuk *plain text* serta objek file dapat diekstraksi secara utuh, sementara pada *external capture* tidak ditemukan artefak serupa. Integritas bukti pada *server-side capture* juga dapat dipertanggungjawabkan melalui validasi hash MD5, sehingga meningkatkan keandalan hasil forensik.

Secara praktis, temuan ini menegaskan bahwa investigator forensik digital sebaiknya memprioritaskan akuisisi data langsung dari sisi server, khususnya pada sistem berbasis NAS, untuk memperoleh bukti yang lebih lengkap dan valid. Pendekatan ini relevan diterapkan dalam investigasi nyata seperti kasus pelanggaran kebijakan internal, kebocoran data, maupun analisis insiden keamanan yang melibatkan komunikasi privat.

Untuk penelitian selanjutnya, disarankan melakukan eksplorasi pada berbagai skenario enkripsi, platform NAS yang berbeda, serta pengujian terhadap metode akuisisi lain guna memperluas generalisasi hasil dan meningkatkan efektivitas teknik forensik digital pada lingkungan komunikasi privat.

DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis

DAFTAR PUSTAKA

Aini, F. D., Peryanto, A., & Widodo, Y. F. (2025). Analisis Forensik Jaringan pada Router Berbasis Log Menggunakan Metode Live Forensic. *Jurnal Kolaborasi Riset Sarjana*, *2*(2), 29–35.

Fahrudin, A., & Zaida Muflih, G. (2024). Analisis Forensik Digital Pada Pesan Whatsapp Yang Terenkripsi Dengan Pretty Good Privacy (Pgp) Menggunakan Framework Dfrws. *Jati (Jurnal Mahasiswa Teknik Informatika)*, *9*(1), 780–787. https://doi.org/10.36040/jati.v9i1.12506

Fitriani Shabira, A., & Fachri, F. (2025). Analisis Forensik Digital Pada File Steganografi Menggunakan Ftk Imager Dan Winhex Dalam Kasus Peredaran Narkoba Dengan Live Forensics. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *10*(2), 228–240. https://doi.org/10.36341/rabit.v10i2.6020

Hendrawan, M. Y. F., Subektiningsih, S., & Hadinegoro, A. (2023). Analisis Bukti Digital Pada Discord Browser Menggunakan Teknik Live Forensic Dengan Metode NIST SP 800-86. *Jurnal Infomedia*, *8*(2), 94. https://doi.org/10.30811/jim.v8i2.4764

Hildayanti, N., & Riadi, I. (2019). Forensics Analysis of Router On Computer Networks Using Live Forensics Method. *International Journal of Cyber-Security and Digital Forensics*, *8*, 74–81. https://doi.org/10.17781/P002559

Imam Riadi, Abdul Fadlil, & Muhammad Immawan Aulia. (2020). Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST). *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *4*(5), 820–828. https://doi.org/10.29207/resti.v4i5.2224

Jafri, M. S., Raharjo, S., & Arief, M. R. (2022). Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones. *CCIT Journal*, *15*(1), 82–105. https://doi.org/10.33050/ccit.v15i1.1586

Mahendra, B. A., Utomo, Y. B., & Kurniadi, H. (2024). Implementasi Metode Forensik Jaringan Untuk Memonitoring Komputer Windows Server. *Journal of Information System and Computer*, *3*(1), 1–8. https://doi.org/10.32503/jiscomp.v3i1.5912

Malpani, R., Pande, A., & Deshmukh, Ms. S. (2025). Cyber Espionage Against Critical Infrastructure: A Case Study of Targeted Attacks on Indian State Load Dispatch Centres (SLDCs). *International Journal Of Scientific Research In Engineering And Management*, *09*(06), 1–9. https://doi.org/10.55041/IJSREM.NCFT013

Mpungu, C., George, C., & Mapp, G. (2024). *Digital Forensics Readiness in Big Data Wireless Networks: A Novel Framework*

DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis

and Incident Response Script for Linux-Hadoop Environments. Computer Science and Mathematics. https://doi.org/10.20944/preprints202407.1803.v1

Mu'Minin, M., & Anwar, N. (2020). Live Data Forensic Artefak Internet Browser (Studi Kasus Google Chrome, Mozilla Firefox, Opera Mode Incognito). *Buletin Sistem Informasi Dan Teknologi Islam (BUSITI)*, *1*(3), 130–138. https://doi.org/10.33096/busiti.v1i3.834

Rasyad, Grinaldy Yafi', Dedy Hariyadi, and Tri Febrianto. "Analisis Lalu Lintas Jaringan Terenkripsi dari Secure Instant Messaging Application: Studi Kasus pada Aplikasi Pesan Instan Synology Chat." *Cyber Security dan Forensik Digital* 5, no. 2 (2023): 71–76. https://doi.org/10.14421/csecurity.2022.5.2.3935.

Prawira, Y. P., & Samsudin, S. (2022). Live Forensics Analysis Of Malware Identified Email Crimes To Increase Evidence Of Cyber Crime. *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, *13*(2). https://doi.org/10.31849/digitalzone.v13i12.11570

Putra, I., Prayudi, Y., & Luthfi, A. (n.d.). *Live Forensics untuk mengenali Karakteristik Serangan File Upload Guna Meningkatkan Keamanan pada Web Server | JIIP - Jurnal Ilmiah Ilmu Pendidikan*. Retrieved February 17, 2026, from http://jiip.stkipyapisdompu.ac.id/jiip/index.php/JIIP/article/view/2173

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

Raharja, R., Alwi, E. I., & Gaffar, A. W. M. (2024). Analisis Digital Forensic Pada Aplikasi Whatsapp Menggunakan Metode National Institute Of Justice (Nij) Pada Smartphone Android. *Buletin Sistem Informasi dan Teknologi Islam*, *5*(2), 160–168. https://doi.org/10.33096/busiti.v5i2.2180

Rasyad, G. Y., Hariyadi, D., & Febrianto, T. (n.d.). *Analysis Of Encrypted Network Traffic From Secure Instant Messaging Application: Case Study On Synology Chat Instant Message Application*.

Rasyad, G. Y., Hariyadi, D., & Febrianto, T. (2023). Analisis Lalu Lintas Jaringan Terenkripsi dari Secure Instant Messaging Application: Studi Kasus pada Aplikasi Pesan Instan Synology Chat. *Cyber Security dan Forensik Digital*, *5*(2), 71–76. https://doi.org/10.14421/csecurity.2022.5.2.3935

Riadi, I., Sunardi, S., & Rauli, M. E. (2018). Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics. *Jurnal Teknik Elektro*, *10*(1), 18–22.

DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis

https://doi.org/10.15294/jte.v10i1.14070

Sunardi, S., Riadi, I., & Triyanto, J. (2021). Analisis Forensik Layanan Signal Private Messenger pada Smartwatch Menggunakan Metode National Institute of Justice. *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, *7*(3), 305–313. https://doi.org/10.26418/jp.v7i3.47740

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

Wibowo, M., Firmansyah, M. R., & Efendi, R. S. (2024). Analisis Bukti Digital Pada Aplikasi Discord Desktop Dengan Menggunakan Framework Dfrws: Live Forensic Discord Desktop Application with DFRWS Framework. *JURNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI*, *15*(1), 98–111. https://doi.org/10.51903/jtikp.v15i1.826

Yahya, A. Z., Dirman, Buru, D. J., & Sugiantoro, B. (2022). Analisis Bukti Digital Pada Random Access Memory Android Menggunakan Metode Live Forensic Kasus Penjualan Senjata Illegal. *Cyber Security dan Forensik Digital*, *5*(1), 6–11. https://doi.org/10.14421/csecurity.2022.5.1.1724

DOI: https://doi.org/10.33020/saintekom.v16i1.1016
Lisensi: CC BY-SA 4.0 | Copyright © 2026, Penulis