Investigasi Forensik Digital terhadap Artefak pada Platform Discord Web pada Browser Cache Menggunakan Enhanced Generic Computer Forensic Investigation Model (EGCFIM)

Mikhail Ashshidiqie Rachman
23917006

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

Investigasi Forensik Digital terhadap Artefak pada Platform Discord Web pada Browser Cache Menggunakan Enhanced Generic Computer Forensic Investigation Model (EGCFIM)

Mikhail Ashshidiqie Rachman
23917006

Yogyakarta, Febuari 2026

Pembimbing

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

Lembar Pengesahan Penguji

Investigasi Forensik Digital terhadap Artefak pada Platform Discord Web pada Browser Cache Menggunakan Enhanced Generic Computer Forensic Investigation Model (EGCFIM)

Mikhail Ashshidiqie Rachman
23917006

Yogyakarta, Febuari 2026

Tim Penguji,

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

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

Fietyata Yudha, S.Kom., M.Kom., Ph.D.
Penguji II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia

Ir. Irving Vitra Paputungan, ST., M.Sc., Ph.D

Abstrak

Investigasi Forensik Digital terhadap Artefak pada Platform Discord Web pada Browser Cache Menggunakan Enhanced Generic Computer Forensic Investigation Model (EGCFIM)

Perkembangan platform komunikasi daring seperti Discord memberikan kemudahan interaksi bagi pengguna, namun juga berpotensi dimanfaatkan untuk berbagai bentuk kejahatan siber. Dalam proses investigasi, bukti digital menjadi elemen penting, terutama ketika pelaku menghapus data untuk menghilangkan jejak aktivitasnya. Salah satu sumber bukti yang dapat dimanfaatkan adalah artefak digital yang tersimpan pada browser cache saat Discord diakses melalui peramban web. Penelitian ini bertujuan untuk mengidentifikasi serta membandingkan kemampuan pemulihan artefak digital Discord dari browser cache menggunakan beberapa tools forensik digital. Penelitian ini menggunakan pendekatan live forensic dengan kerangka kerja Enhanced Generic Computer Forensic Investigation Model (EGCFIM). Proses investigasi dilakukan pada tiga browser, yaitu Google Chrome, Mozilla Firefox, dan Microsoft Edge, dengan menggunakan tools Autopsy, ChromeCacheView, dan MZCacheView. Skenario penelitian melibatkan simulasi aktivitas pengguna di Discord seperti pengiriman pesan teks, penggunaan emoji dan stiker, serta pengiriman file media. Hasil penelitian menunjukkan bahwa artefak digital seperti username, user ID, server/channel ID, pesan teks, timestamp, dan file media masih dapat dipulihkan dari browser cache meskipun data telah dihapus oleh pengguna. Selain itu, terdapat perbedaan kemampuan masing-masing tools dalam mengekstraksi artefak dari setiap browser. Temuan ini menunjukkan bahwa browser cache dapat menjadi sumber bukti digital penting dalam investigasi forensik pada platform Discord berbasis web.

Kata kunci

recovery file, browser cache, live forensic, forensic tools, forensics investigation model.

Abstract

Digital Forensic Investigation of Discord Web Platform Artifacts in Browser Cache Using the Enhanced Generic Computer Forensic Investigation Model (EGCFIM)

The development of online communication platforms such as Discord has facilitated user interaction but also creates opportunities for various forms of cybercrime. In the investigation process, digital evidence becomes a crucial element, especially when perpetrators delete data to eliminate traces of their activities. One potential source of evidence is digital artifacts stored in the browser cache when Discord is accessed through a web browser. This study aims to identify and compare the capability of recovering Discord digital artifacts from browser cache using several digital forensic tools. This research employs a live forensic approach using the Enhanced Generic Computer Forensic Investigation Model (EGCFIM) framework. The investigation process was conducted on three web browsers: Google Chrome, Mozilla Firefox, and Microsoft Edge, using the forensic tools Autopsy, ChromeCacheView, and MZCacheView. The research scenario involved simulated user activities on Discord, including sending text messages, using emojis and stickers, and sharing media files. The results show that digital artifacts such as username, user ID, server/channel ID, text messages, timestamps, and media files can still be recovered from the browser cache even after the data has been deleted by the user. In addition, differences were found in the capability of each tool to extract artifacts from different browsers. These findings indicate that browser cache can serve as an important source of digital evidence in forensic investigations involving the web-based Discord platform.

Keywords

recovery file, browser cache, live forensic, forensic tools, forensics investigation model.

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, September 2025

Mikhail Ashshidiqie Rachman

Daftar Publikasi

Publikasi yang dihasilkan:

Rachman, Mikhail Ashshidiqie & Prayudi, Yudi. (2026). “Comparative Analysis of Discord Artifact Recovery from Browser Cache Using Improved Generic Computer Forensic Investigation Model (GCFIM)”, Jurnal Teknik Informatika (JUTIF), Volume 7 Number 4, Augustus 2026.

Kontributor	Jenis Kontribusi
Mikhail Ashshidiqie Rachman	Mendesain eksperimen (60%) Menulis *paper* (70%)
Dr. Yudi Prayudi, S.Si., M. Kom.	Mendesain eksperimen (40%) Menulis dan mengedit *paper* (30%)

Halaman Kontribusi

Penelitian ini melibatkan kontribusi dari berbagai pihak sebagai berikut:

1. Amang Sjamsjiar Rachman ST., MT., MSS. Melakukan review kritis terhadap hasil interpretasi data penelitian.

Halaman Persembahan

Segala puji bagi Allah SWT, Tuhan semesta alam, dengan penuh kerendahan hati, saya menyampaikan rasa syukur ke hadirat Allah SWT atas limpahan rahmat, taufik, serta hidayah-Nya, sehingga tesis ini dapat terselesaikan dengan baik. Shalawat dan salam semoga senantiasa tercurah kepada Nabi Muhammad SAW, teladan sepanjang masa dalam menuntut ilmu dan mengamalkannya.

Tesis ini saya persembahkan kepada:

1. Allah SWT, sumber segala kekuatan, serta Rasulullah SAW yang menjadi teladan dalam keteguhan dan keikhlasan. Tanpa pertolongan dan bimbingan-Mu, tak mungkin satu halaman pun dari tesis ini dapat terwujud.
2. Kedua orang tuaku tercinta, yang selalu menyertai langkahku dengan doa, kesabaran, dan kasih sayang yang tiada henti. Aku menyadari takkan pernah mampu membalas semua pengorbanan kalian. Semoga ijazah ini dapat menjadi persembahan kecil sebagai wujud terima kasih yang tulus.
3. Para dosen dan staf MI UII, atas ilmu, arahan, serta kritik yang membangun. Setiap bimbingan dan nasihat Bapak/Ibu telah menjadi bagian penting dalam tersusunnya karya ini.
4. Rekan-rekan seperjuangan Magister Informatika UII angkatan 2023, khususnya teman-teman Forensika Digital, terima kasih atas kebersamaan, kerja sama, dan semangat yang telah mewarnai perjalanan akademik ini.
5. Semua pihak yang tidak dapat disebutkan satu per satu, atas segala bentuk perhatian, dukungan, serta masukan yang diberikan. Setiap sumbangsih, sekecil apa pun, merupakan bagian berharga dari proses ini.

Semoga Allah membalas setiap kebaikan dengan ganjaran yang terbaik.

Kata Pengantar

Assalamu'alaikum warahmatullahi wabarakatuh.

Segala puji serta syukur penulis panjatkan ke hadirat Allah SWT, Tuhan Yang Maha Esa, atas limpahan rahmat, taufik, dan hidayah-Nya sehingga penulis dapat menyelesaikan tesis ini dengan baik. Berkat ridho-Nya, penulis diberi kesempatan untuk menuntaskan penelitian ini sesuai dengan yang direncanakan. Tesis dengan judul *"Investigasi Forensik Digital terhadap Artefak Discord Web pada Browser Cache Menggunakan Enhanced Generic Computer Forensic Investigation Model (EGCFIM)"* disusun sebagai salah satu syarat guna menyelesaikan studi pada Program Magister serta memperoleh gelar Magister Komputer. Penyusunan tesis ini tidak terlepas dari dukungan, arahan, dan bantuan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada :

1. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D., selaku Rektor Universitas Islam Indonesia, yang telah memberikan kesempatan untuk menimba ilmu di kampus ini.
2. Bapak Dr. Yudi Prayudi, S.Si., M.Kom., selaku dosen pembimbing yang dengan penuh kesabaran memberikan arahan, bimbingan, serta masukan berharga dalam penyusunan penelitian ini.
3. Teman - teman seperjuangan dari Magister Informatika Fakultas Teknologi Industri Universitas Islam Indonesia, khususnya Konsentrasi Forensika Digital Angkatan XXVIII, atas kebersamaan, semangat, dan kerja sama yang menjadi bagian penting dalam perjalanan akademik ini.

Penulis menyadari sepenuhnya bahwa dalam penyusunan tesis ini masih terdapat banyak kekurangan. Oleh sebab itu, kritik, saran, serta masukan yang bersifat membangun sangat penulis harapkan demi kesempurnaan karya ini di masa mendatang.

Wassalamu'alaikum warahmatullahi wabarakatuh.

Yogyakarta, 21 September 2025

Mikhail Ashshidiqie Rachman

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

GCFIM	- Generic Computer Forensic Investigation Model
EGCFIM	- Enhanced Generic Computer Forensic Investigation Model
DFRWS	- Digital Forensics Research Workshop
NIJ	- National Institute of Justice
API	- Application Programming Interface
CPU	- Central Processing Unit
FTK	- Forensic Toolkit
ID	- Identifier
JSON	- JavaScript Object Notation
MD5	- Message Digest Algorithm 5
NIST	- National Institute of Standards and Technology
RAM	- Random Access Memory
SHA-256	- Secure Hash Algorithm 256-bit
SSD	- Solid State Drive
URL	- Uniform Resource Locator
VPN	- Virtual Private Network
TOR	- The Onion Router
DNS	- Domain Name System
IP	- Internet Protocol

BAB I
Pendahuluan

1.1 Latar Belakang

Era digital telah secara fundamental mengubah cara manusia berinteraksi, berkomunikasi, dan mengakses informasi. Internet, sebagai infrastruktur utama peradaban modern, telah meruntuhkan batas-batas geografis dan temporal, memungkinkan konektivitas global yang belum pernah terjadi sebelumnya. Manfaatnya merambah ke berbagai sektor kehidupan, mulai dari pendidikan, bisnis, hingga hiburan, menciptakan ekosistem digital yang dinamis dan terus berkembang. Dalam konteks komunikasi interaktif, berbagai platform telah muncul dan mendominasi lanskap digital, memfasilitasi pertukaran pesan secara instan dan real-time. Salah satu platform yang menonjol dalam beberapa tahun terakhir adalah Discord.

Kemajuan teknologi informasi, khususnya internet, telah merevolusi cara manusia berkomunikasi dan berinteraksi secara global. Platform komunikasi real-time seperti Discord telah mengalami pertumbuhan eksponensial, menjadi bagian integral dari kehidupan sosial dan aktivitas online, terutama di kalangan komunitas gamer. Data dari Statista (2023) menunjukkan bahwa pengguna aktif bulanan Discord mencapai angka yang signifikan, mendekati 150 juta, dibandingkan dengan angka 140 juta pada tahun 2021. Pertumbuhan ini mencerminkan adopsi platform tersebut di berbagai wilayah dan demografi. Selain manfaatnya, platform ini juga rentan terhadap aktivitas kejahatan siber, seperti penipuan, pelecehan seksual, pornografi, dan cyberbullying Kejahatan siber di platform komunikasi real-time seperti Discord, yang sering melibatkan pertukaran pesan teks dan file, membutuhkan pendekatan forensik digital untuk pengumpulan dan analisis bukti (National Institute of Standards and Technology, 2020). Ancaman ini semakin menguat di tengah perkembangan teknologi yang memungkinkan pengguna untuk menghapus data secara mudah, sehingga mengidentifikasi dan memulihkan bukti digital menjadi sangat krusial

Discord, yang awalnya populer di kalangan komunitas gamers, telah mengalami pertumbuhan eksponensial dan meluas ke berbagai kelompok pengguna, termasuk komunitas pendidikan, profesional, dan organisasi sosial. Platform ini menawarkan fitur komunikasi yang kaya, termasuk obrolan teks, panggilan suara, dan video konferensi, yang semuanya dapat diakses secara gratis. Data terbaru menunjukkan bahwa pada tahun 2021,

Discord melayani sekitar 140 juta pengguna aktif bulanan, sebuah angka yang mencerminkan peningkatan signifikan sebesar 40% dibandingkan tahun sebelumnya (Discord Inc., 2022). Pertumbuhan ini tidak hanya terbatas pada jumlah pengguna, tetapi juga pada infrastruktur platform, dengan 13,5 juta server aktif tercatat pada tahun 2021, menunjukkan peningkatan sebesar 6,7 juta server dibandingkan tahun 2020 (Discord Inc., 2022). Angka-angka ini menggarisbawahi peran sentral Discord dalam ekosistem komunikasi digital global.

Namun, di balik kemudahan dan manfaat yang ditawarkan, perkembangan pesat platform komunikasi seperti Discord juga membawa serta kompleksitas baru, terutama terkait dengan potensi penyalahgunaan dan aktivitas ilegal. Seiring dengan popularitasnya yang meroket, Discord juga terindikasi menjadi sarang bagi konten yang tidak pantas dan aktivitas yang melanggar hukum. Laporan dari berbagai lembaga keamanan siber dan penelitian akademis secara konsisten menyoroti peningkatan kasus cybercrime yang memanfaatkan platform ini, termasuk penipuan (scamming), pelecehan seksual (sexual harassment), penyebaran materi pornografi, dan cyberbullying (Smith & Jones, 2021; Cybercrime Observatory, 2023). Keberadaan konten-konten semacam ini tidak hanya merusak reputasi platform, tetapi juga menimbulkan ancaman serius bagi keamanan dan kesejahteraan penggunanya.

Dalam menghadapi lanskap digital yang semakin kompleks ini, kemampuan untuk mengungkap dan membuktikan insiden atau kejahatan siber menjadi sangat krusial. Di sinilah peran forensik digital menjadi sangat vital. Forensik digital adalah cabang ilmu komputer yang berfokus pada identifikasi, pengumpulan, analisis, dan pelaporan bukti digital yang dapat digunakan dalam proses hukum atau investigasi internal. Analisis forensik pada aplikasi komunikasi seperti Discord memerlukan pemahaman mendalam tentang struktur data, mekanisme penyimpanan, dan artefak yang ditinggalkan oleh aktivitas pengguna.

Penelitian sebelumnya telah menunjukkan bahwa analisis forensik pada aplikasi Discord dapat dilakukan dengan mempresentasikan struktur caching serta log aktivitas pengguna. Alat forensik seperti DiscFor telah dikembangkan dan diimplementasikan untuk mengekstrak data dari file lokal Discord dan penyimpanan cache, yang kemudian dapat dianalisis lebih lanjut(Motylinski et al., 2020). Pentingnya forensik aplikasi semakin meningkat seiring dengan maraknya kejahatan dunia maya yang memanfaatkan perangkat lunak komunikasi sebagai sarana operasionalnya.

Lebih lanjut, analisis forensik sering kali melibatkan investigasi terhadap artefak yang ditinggalkan oleh penggunaan peramban web (web browser), seperti Google Chrome, Mozilla Firefox, dan Opera, terutama dalam mode penjelajahan anonim (Incognito Mode). Proses forensik digital pada peramban web berfokus pada identifikasi bukti digital seperti riwayat penjelajahan, URL, kredensial pengguna (nama pengguna dan kata sandi), serta data lainnya yang dapat memberikan gambaran tentang aktivitas online pengguna (Garcia & Lee, 2019). Metode yang umum digunakan meliputi tahapan preservasi, akuisisi data, dan analisis bukti digital, sesuai dengan pedoman standar seperti yang dikeluarkan oleh National Institute of Justice (NIJ) (NIJ, 2004). Pedoman NIJ menguraikan siklus hidup forensik digital yang mencakup persiapan, pengumpulan data, pemeriksaan, analisis, dan pelaporan. Temuan bukti digital dari peramban web dapat mencakup akun yang digunakan, bookmark, dokumen yang diakses, riwayat pencarian, email, gambar, stempel waktu (timestamp), kata sandi, dan URL yang dikunjungi.

Penelitian yang secara spesifik mengkaji aplikasi Discord yang diakses melalui peramban web, seperti Google Chrome, juga telah dilakukan. Metode eksperimental sering digunakan untuk memulihkan artefak digital yang ditinggalkan oleh aktivitas pengguna di platform tersebut. Dalam konteks pengumpulan bukti digital, membangun garis waktu (timeline) aktivitas menjadi elemen krusial dalam setiap proses forensik digital. Garis waktu yang akurat memungkinkan peneliti untuk merekonstruksi urutan kejadian dan menetapkan korelasi antara berbagai aktivitas yang terjadi.

Selain metode yang umum digunakan, kerangka kerja seperti Digital Forensics Research Workshop (DFRWS) juga telah diakui efektivitasnya dalam menganalisis bukti digital pada aplikasi media sosial (DFRWS, 2001). Namun, penelitian yang berfokus pada analisis bukti digital pada Discord yang diakses melalui peramban web sering kali mengadopsi metodologi yang berbeda, seperti Metode NIST SP 800-86 yang menggabungkan teknik live forensics (NIST, 2008). Metode NIST SP 800-86 terdiri dari empat tahap utama: Collection (Pengumpulan), Examination (Pemeriksaan), Analysis (Analisis), dan Report (Pelaporan). Pendekatan ini sangat relevan ketika sumber data yang akan dianalisis masih aktif atau ketika investigasi perlu dilakukan tanpa mengganggu sistem yang sedang berjalan.

Urgensi presisi dalam forensik digital semakin mendesak mengingat sifat dinamis dari ancaman siber dan kompleksitas teknis dari platform modern. Kejahatan siber terus berevolusi, memanfaatkan celah keamanan dan fitur-fitur baru dalam perangkat lunak komunikasi. Oleh karena itu, kemampuan untuk secara akurat dan efisien mengidentifikasi,

mengekstrak, dan menganalisis bukti digital sangat penting untuk mendukung proses penegakan hukum, investigasi internal perusahaan, dan penanggulangan insiden keamanan siber.

Meskipun demikian, terdapat kesenjangan signifikan dalam literatur penelitian yang secara komprehensif membahas analisis forensik bukti digital yang terhapus dari platform Discord ketika diakses melalui berbagai peramban web, dengan fokus pada kemampuan pemulihan data dan perbandingan efektivitas berbagai alat forensik. Sebagian besar penelitian yang ada cenderung berfokus pada satu jenis peramban web atau pada aplikasi desktop Discord secara terpisah. Kurangnya penelitian yang mengintegrasikan analisis lintas peramban web untuk platform Discord meninggalkan pertanyaan terbuka mengenai bagaimana artefak digital yang terhapus dari interaksi Discord melalui peramban yang berbeda dapat dipulihkan dan dianalisis secara efektif. Teknologi forensik dikembangkan untuk menemukan penjahat dengan mengumpulkan bukti berdasarkan model forensik digital yang secara umum diklasifikasikan ke dalam beberapa tahap: identifikasi, pengumpulan, pengawetan, analisis, laporan, dan penyajian (Hamad, N., et al., 2022).

Penelitian forensik digital terhadap platform komunikasi seperti Discord memiliki urgensi yang tinggi. Kesenjangan yang ada dalam literatur saat ini terletak pada kurangnya studi yang komprehensif mengenai pemulihan bukti digital yang terhapus dari platform Discord, khususnya yang diakses melalui beragam browser web. Meskipun beberapa penelitian telah meneliti analisis forensik pada browser web seperti Google Chrome dan Mozilla Firefox (Awan et al., 2022), penelitian yang menyoroti pemulihan bukti digital terhapus di Discord, dan penerapannya pada berbagai browser, masih terbatas. Hal ini menjadi penting karena kebutuhan praktis untuk mengungkap dan menangani kasus kejahatan siber di platform ini, yang memerlukan pemahaman mendalam tentang cara memulihkan bukti yang dihapus. Penelitian ini berusaha mengisi kesenjangan tersebut dengan fokus pada pemulihan bukti digital dari aplikasi Discord yang terhapus, menggunakan berbagai tools forensik dan metode pemulihan data.

Penelitian-penelitian sebelumnya tentang forensik digital pada platform komunikasi seperti Discord (Iqbal et al., 2021), (Motylinski et al., 2020),WhatsApp(Amelia & Riadi, 2021), dan Facebook (Dwi, 2023) umumnya terbatas pada analisis aplikasi desktop atau satu jenis browser tertentu, serta belum membahas pemulihan data terhapus secara mendalam. Penelitian ini mengisi celah tersebut dengan membandingkan kinerja beberapa alat forensik (Autopsy, ChromeCacheView, dan MZ Cache View) dalam memulihkan pesan teks dan gambar yang terhapus dari Discord di tiga browser berbeda (Chrome, Firefox, Edge).

Pendekatan ini tidak hanya memperluas temuan sebelumnya dengan cakupan yang lebih luas, tetapi juga memberikan panduan praktis bagi penyidik dalam memilih alat terbaik berdasarkan jenis browser yang digunakan pelaku.

Sebagai ilustrasi nyata (Kausar & Nadilla, 2026) mengenai potensi penyalahgunaan *platform* Discord, baru-baru ini Polda Metro Jaya mendalami kasus dugaan penipuan investasi kripto yang terjadi melalui sebuah grup aplikasi Discord, di mana korban bergabung dalam grup tersebut dan menerima tawaran trading dengan janji keuntungan fantastis hingga 300–500 persen, namun setelah melakukan investasi senilai miliaran rupiah justru mengalami kerugian besar dan melaporkannya ke pihak kepolisian untuk diselidiki lebih lanjut. Kasus ini menunjukkan bahwa Discord tidak hanya menjadi media komunikasi biasa, tetapi juga dapat dimanfaatkan oleh pihak tak bertanggung jawab sebagai sarana untuk menjebak korban melalui tawaran investasi yang menyesatkan. Situasi semacam ini mempertegas pentingnya penelitian untuk memahami artefak digital yang tertinggal dalam penggunaan Discord versi web, terutama melalui browser cache, karena jejak komunikasi yang terekam secara tidak sadar di sisi klien dapat menjadi bukti digital penting dalam mendukung proses investigasi kejahatan siber seperti penipuan investasi. Dengan memahami bagaimana artefak komunikasi dan media tersimpan dan dapat direcover dari cache browser, penelitian ini tidak hanya memberikan kontribusi ilmiah dalam forensik digital berbasis web, tetapi juga memberikan wawasan praktis yang relevan bagi penegak hukum dalam menangani kasus serupa di masa depan.

Penelitian ini memiliki urgensi tinggi mengingat maraknya kasus kejahatan siber di platform Discord seperti *cyberbullying*, pelecehan seksual, dan penyebaran konten ilegal, di mana pelaku kerap menghapus bukti digital. Fokus pada pemulihan pesan teks dan gambar yang terhapus di tiga browser berbeda (Google Chrome, Mozilla Firefox, Microsoft Edge) menjadikan temuan penelitian ini relevan secara praktis bagi penyidik forensik digital. Selain itu, penelitian ini melengkapi celah pada studi-studi sebelumnya yang umumnya terbatas pada analisis aplikasi desktop atau satu jenis browser tertentu. Dengan membandingkan efektivitas alat forensik seperti Autopsy, ChromeCacheView, dan MZ CacheView, penelitian ini tidak hanya memperkaya khazanah akademis tetapi juga memberikan panduan operasional dalam investigasi kasus-kasus berbasis Discord.

1.2 Rumusan Masalah

Dalam penelitian ini, peneliti berfokus untuk mengkaji penggunaan beberapa perangkat alat forensik, yaitu Autopsy, MZCacheView, dan ChromeCacheView, guna

mengetahui sejauh mana efektivitasnya dalam proses pemeriksaan serta analisis bukti digital. Selain itu, penelitian ini juga bertujuan untuk menguji kemampuan ketiga tools tersebut dalam mengembalikan pesan teks maupun file gambar yang telah terhapus dari browser ketika platform Discord diakses. Uji coba dilakukan pada tiga jenis browser berbeda, yaitu Mozilla Firefox, Google Chrome, dan Microsoft Edge, sehingga hasil yang diperoleh diharapkan dapat memberikan gambaran yang komprehensif mengenai reliabilitas dan konsistensi masing-masing perangkat forensik dalam menangani bukti digital yang berasal dari cache browser. Berdasarkan latar belakang di atas maka yang menjadi rumusan masalah adalah sebagai berikut:

1. Artefak digital apa saja yang dapat dihasilkan dari interaksi pengguna dengan platform Discord ketika diakses melalui peramban web Google Chrome, Mozilla Firefox, dan Microsoft Edge?
2. Sejauh mana efektivitas berbagai perangkat forensik digital, yaitu Autopsy, MZCacheView, dan ChromeCacheView, dalam memulihkan artefak Discord yang telah terhapus ketika diaplikasikan pada ketiga peramban tersebut?
3. Adakah perbedaan yang signifikan terkait jenis maupun tingkat kemudahan pemulihan artefak Discord yang terhapus pada masing-masing peramban web dengan tools yang dipakai pada Google Chrome, Mozilla Firefox, dan Microsoft Edge

1.3 Batasan Masalah

Berdasarkan rumusan masalah diatas, batasan penelitian ini meliputi :

1. Penelitian hanya berfokus pada platform Discord yang diakses melalui web browser, yaitu Google Chrome, Mozilla Firefox, dan Microsoft Edge
2. Artefak digital yang dianalisis dibatasi pada data yang tersimpan di dalam browser cache.
3. Aktivitas pengguna yang menjadi objek penelitian meliputi:
    a. Pengiriman pesan teks (termasuk pesan yang diedit, disematkan, spoiler, dan balasan)
    b. Penggunaan emoji dan stiker
    c. Pengiriman file media (gambar, video, dan dokumen).
4. Tools forensik yang digunakan dalam penelitian ini dibatasi pada Autopsy MZCacheView ChromeCacheView

5. Pendekatan penelitian menggunakan Enhanced Generic Computer Forensic Investigation Model (Enhanced GCFIM) yang mencakup tahapan: akuisisi, pemeriksaan, analisis, pelaporan, dan presentasi hasil.

1.4 Tujuan Penelitian

Tujuan utama penelitian ini dirancang untuk: mengidentifikasi, mengekstrak, dan menganalisis artefak digital yang ditinggalkan oleh interaksi pengguna dengan platform Discord ketika diakses melalui berbagai peramban web (Google Chrome, Mozilla Firefox, dan Microsoft Edge), dengan fokus khusus pada pemulihan data dengan enerapkan metode *Enhanced Generic Computer Forensic Investigation Model* dalam proses investigasi.

1.5 Manfaat Penelitian

Harapannya penelitian ini dapat memberikan manfaat untuk menjadi tambahan pengetahuan. Manfaat penelitian ini terdiri dari :

1. Memberikan kontribusi akademis dalam bidang forensik digital dengan menambah pemahaman mengenai pemanfaatan browser cache sebagai sumber artefak pada platform Discord.
2. Menjadi acuan praktis bagi investigator atau praktisi forensik digital dalam menentukan tools yang sesuai dengan karakteristik masing-masing browser.
3. Menyajikan perbandingan kemampuan browser (Google Chrome, Mozilla Firefox, dan Microsoft Edge) dalam menyimpan serta menyediakan artefak digital yang dapat dipulihkan.
4. Menunjukkan implementasi *Enhanced Generic Computer Forensic Investigation Model* dalam studi forensik digital berbasis browser cache.
5. Menyediakan referensi yang dapat digunakan dalam penelitian lanjutan maupun mendukung kebutuhan penegakan hukum terkait pembuktian digital.

1.6 Metode Penelitian

Penelitian ini perlu disusun langkah-langkah penyelesaian secara sistematik, adapun sistematika metodologi yang digunakan pada penelitian ini adalah sebagai berikut:

1. Tinjauan Pustaka

Tahap ini dilakukan untuk mengkaji teori, konsep, serta hasil penelitian terdahulu yang relevan. Tujuannya adalah memberikan dasar teoretis yang kuat bagi penelitian serta memperkuat kerangka berpikir yang digunakan.

2. Persiapan Alat dan Sistem

   Pada tahap ini dilakukan penyiapan perangkat keras, perangkat lunak, serta lingkungan penelitian yang dibutuhkan. Persiapan ini penting untuk memastikan proses penelitian dapat berjalan dengan lancar dan sesuai kebutuhan.

3. Skenario dan Simulasi Kasus

   Tahap ini berfokus pada perancangan skenario yang menggambarkan kondisi nyata, sehingga pengujian dapat dilakukan secara terarah. Simulasi kasus membantu memastikan bahwa setiap langkah penelitian memiliki relevansi dengan tujuan yang ingin dicapai.

4. Penerapan Metode

   Tahap akhir berupa pelaksanaan metode penelitian dengan menggunakan pendekatan forensik dan tools yang telah ditentukan. Proses ini dilakukan secara sistematis untuk memperoleh hasil yang valid, objektif, dan dapat dipertanggungjawabkan.

1.7 Sistematika Penulisan

Untuk memberikan kerangka konseptual dan memfasilitasi proses penyusunan penelitian ini, disusun sistematika penulisan dengan struktur sebagai berikut:

BAB I PENDAHULUAN

Berisi latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan penelitian, serta sistematika penulisan. Bab ini memberikan gambaran umum mengenai arah dan ruang lingkup penelitian.

BAB II TINJAUAN PUSTAKA

Menyajikan teori, konsep, serta hasil penelitian terdahulu yang relevan sebagai dasar dalam penyusunan kerangka berpikir. Bab ini juga berfungsi untuk memperkuat landasan teoretis penelitian.

BAB III METODOLOGI

Menguraikan pendekatan dan metode yang digunakan dalam penelitian, termasuk tahapan penelitian, skenario uji coba, serta perangkat keras dan perangkat lunak yang digunakan.

BAB IV HASIL DAN PEMBAHASAN

Berisi temuan penelitian yang diperoleh dari proses analisis serta pembahasan yang menghubungkan hasil penelitian dengan teori maupun penelitian terdahulu.

BAB V PENUTUP

Merupakan bagian akhir yang berisi kesimpulan dari penelitian yang telah dilakukan serta saran untuk penelitian selanjutnya maupun penerapan praktis.

BAB II

Tinjauan Pustaka

2.1 Penelitian Terdahulu

Pada penelitian terdahulu dengan judul "**Analisis Forensik Keamanan Data Pribadi pada Mode Privasi Browser Menggunakan Metode National Institute of Standards and Technology (NIST)**", peneliti menganalisis efektivitas mode privat pada browser Google Chrome dan Mozilla Firefox dalam melindungi data pribadi pengguna. Metode yang digunakan adalah NIST, yang terdiri dari empat tahap utama: Collection, Examination, Analysis, dan Reporting. Penelitian ini melibatkan empat skenario simulasi untuk mengevaluasi penyimpanan data sementara di memori (RAM) setelah penggunaan mode privat. Alat forensik seperti Belkasoft RAM Capture, Volatility Memory Forensic, dan WinHex digunakan untuk mengumpulkan dan menganalisis bukti digital. Hasil penelitian menunjukkan bahwa meskipun mode privat mencegah penyimpanan riwayat penelusuran dan data pengguna di hard disk, informasi sensitif seperti akun dan kata sandi masih dapat diakses dari RAM dalam kondisi tertentu, terutama saat browser masih berjalan. Temuan ini mengungkap keterbatasan mode privat dalam melindungi privasi pengguna sepenuhnya, sehingga penelitian ini merekomendasikan penggunaan alat tambahan, penutupan browser segera setelah penggunaan, serta peningkatan kesadaran pengguna tentang risiko kebocoran data. Studi ini juga menyarankan penelitian lanjutan untuk menguji lebih banyak browser dan lingkungan virtual guna memperkuat temuan (Syukri et al., 2025)

Pada penelitian terdahulu dengan judul "**Analisis Aktivitas Cyber Bullying Pengguna Facebook Melalui Browser Chrome dengan Pendekatan Live Forensics**", peneliti menggunakan metode Live Forensics berbasis kerangka kerja NIST (National Institute of Standards and Technology) untuk mengumpulkan dan menganalisis bukti digital terkait kasus cyber bullying di platform Facebook. Tahapan penelitian meliputi Collection (pengumpulan bukti melalui RAM imaging, log file, cache, dan riwayat browser), Examination (pemeriksaan integritas bukti dengan FTK Imager dan Browser History Viewer), Analysis (identifikasi pola aktivitas cyber bullying seperti timestamp, komentar, dan kredensial login), serta Reporting (penyusunan laporan forensik sesuai UU ITE Pasal 27 Ayat 3). Alat utama yang digunakan antara lain FTK Imager v4.7.1 untuk akuisisi memori dan Browser History Viewer v1.4.1 untuk ekstraksi riwayat browsing. Hasil penelitian menunjukkan bahwa pendekatan live forensics efektif mengungkap jejak digital pelaku, termasuk waktu akses, konten penghinaan, dan identitas akun, yang dapat dijadikan bukti

hukum. Temuan ini memperkuat pentingnya teknik forensik proaktif dalam investigasi kejahatan siber berbasis media sosial (Dwi, 2023).

Pada penelitian terdahulu dengan judul "**Analisis Live Forensics Keamanan Browser pada Marketplace (Studi Kasus: Tokopedia dan Bukalapak)**", peneliti menganalisis keamanan data pada aktivitas belanja online dengan pendekatan live forensik. Metode yang digunakan adalah National Institute of Justice (NIJ) yang terdiri dari lima tahap: Identification (penyiapan skenario kasus), Collection (pengumpulan data volatile menggunakan Magnet RAM Capture), Examination (pemeriksaan integritas data dengan FTK Imager), Analysis (korelasi artefak digital), dan Reporting (penyimpulan hasil). Penelitian ini melibatkan 30 akun email di 30 perangkat berbeda untuk mengakses Tokopedia dan Bukalapak melalui tiga browser (Google Chrome, Mozilla Firefox, dan Opera) dalam mode public dan private. Alat utama yang digunakan meliputi FTK Imager untuk analisis memori dan Magnet RAM Capture untuk akuisisi data volatile. Hasil penelitian menunjukkan Mozilla Firefox memiliki indeks keamanan tertinggi (47% artefak terdeteksi) saat mengakses kedua marketplace, sedangkan Chrome paling rentan (54% untuk Tokopedia, 67% untuk Bukalapak). Temuan kritis meliputi kebocoran data sensitif seperti email, password, dan riwayat transaksi yang tersimpan di RAM, bahkan dalam mode private. Penelitian ini merekomendasikan penggunaan Mozilla Firefox untuk aktivitas belanja online guna meminimalkan risiko kebocoran data (Sarsono & Indrayani, 2024).

Pada penelitian terdahulu dengan judul **"Forensic Investigation of Event Logs by Automatic Anomaly Detection"**, peneliti mengusulkan sebuah kerangka kerja otomatis untuk mendeteksi anomali dalam timeline forensik yang dibangun dari berkas log. Penelitian ini menggunakan tiga pendekatan utama: deteksi anomali berbasis kluster dengan mempertimbangkan properti statistik seperti frekuensi dan laju kedatangan, pembentukan model baseline aktivitas normal menggunakan teknik deep learning berupa deep autoencoders, serta analisis sentimen pesan log untuk mengidentifikasi anomali dengan memanfaatkan attention-based deep learning dan gated recurrent unit (GRU). Selain itu, penelitian ini juga mengatasi masalah ketidakseimbangan kelas dalam data log dengan metode Tomek link. Hasil deteksi anomali dari ketiga metode tersebut kemudian digabungkan menggunakan teknik weighted majority voting dan divisualisasikan dalam timeline forensik untuk memudahkan analisis investigator. Eksperimen yang dilakukan pada berbagai dataset publik menunjukkan bahwa kerangka kerja ini memiliki kinerja yang lebih unggul dibandingkan metode deteksi anomali log lainnya. Alat yang digunakan dalam penelitian ini meliputi bidirectional long short-term memory (BLSTM) untuk parsing log

otomatis, deep autoencoders untuk pemodelan baseline, serta GRU dan attention mechanism untuk analisis sentimen (Studiawan, 2020).

Berikut disajikan penelitian terdahulu yang berkaitan dengan judul, fokus penelitian serta hasil, seperti diperlihatkan pada Tabel 1.1.

Tabel 1. 1 Review Penelitian Terdahulu

No	Judul	Fokus Penelitian	Hasil
1	Analisis Live Forensics Keamanan Browser pada Marketplace (Studi Kasus : Tokopedia dan Bukalapak)	Mengevaluasi keamanan data pengguna saat belanja online di Tokopedia dan Bukalapak dengan menganalisis jejak login di browser (Chrome, Firefox, Opera) menggunakan teknik *live forensics*. Fokus pada perbandingan mode *public* vs *incognito*.	- **Firefox** paling aman: Temuan artefak paling sedikit (47% di Tokopedia, 47% di Bukalapak). - **Chrome** paling rentan: Temuan artefak terbanyak (54% di Tokopedia, 67% di Bukalapak). - Bukalapak meninggalkan lebih banyak jejak (60%) dibanding Tokopedia (51%).
2	Analisis Aktivitas Cyber Bullying Pengguna Facebook melalui Browser Chrome dengan Pendekatan Live Forensic	Meneliti jejak digital kasus cyber bullying di Facebook melalui browser Chrome dengan teknik *live forensics* untuk mengumpulkan bukti seperti pesan, komentar, dan riwayat login yang bisa digunakan untuk laporan hukum.	-- Berhasil mengumpulkan bukti digital seperti: - Timestamp akses Facebook (contoh: 11 Juli 2023, pukul 15:51:13). - Email login korban (jaimehagensen@outlook.co.id). - Konten komentar bullying. - Bukti valid secara forensik dengan hash MD5/SHA1. - Bukti dapat digunakan untuk pelaporan sesuai Pasal 27 Ayat (3) UU ITE.
3	Analisis Forensik Keamanan Data Pribadi pada Mode Privasi Browser Menggunakan	Mengevaluasi efektivitas mode privat di browser (Chrome & Firefox) dalam melindungi data pribadi, khususnya	- Skenario 1 (browser masih terbuka): Akun Gmail dan password berhasil diekstrak dari RAM. - Skenario 2-4 (browser ditutup/reboot): Tidak

	Metode National Institute of Standards and Technology (NIST)	apakah informasi sensitif seperti akun dan password masih bisa diambil dari RAM meski mode privat aktif	ditemukan bukti, kecuali timestamp. - Firefox lebih konsisten menghapus data RAM dibanding Chrome.
4	Discord Server Forensics: Analysis and Extraction of Digital Evidence	Penelitian ini berfokus pada analisis forensik digital untuk mengumpulkan bukti dari aplikasi Discord, khususnya dari cache dan log aktivitas.	- Berhasil memulihkan berbagai jenis file (pesan teks, gambar, dll.) dari cache dengan akurasi tinggi. - DiscFor lebih unggul dari CCV dalam hal kelengkapan data dan fitur laporan. - Log aktivitas berisi info berguna seperti email dan ID server, meski sebagian data terenkripsi.
5	Digital Forensic Acquisition and Analysis of Discord Applications	Meneliti artefak digital forensik yang dapat dipulihkan dari aplikasi Discord, termasuk pesan teks, gambar, audio, dan video, serta mengembangkan alat baru bernama DiscFor untuk ekstraksi data secara forensik.	- DiscFor berhasil memulihkan lebih banyak data dibanding tools lain (seperti ChromeCacheView), termasuk file terpisah seperti audio/video. - Cache menyimpan data hingga 30 hari, termasuk pesan dan lampiran. - Log aktivitas berisi info seperti email, tetapi tidak menyimpan password.
6	Forensic Browser on Facebook Services using National Institute of Standards Technology Method	Menganalisis bukti digital penyebaran konten hoax di Facebook melalui browser Chrome dengan metode live forensics untuk mengungkap jejak aktivitas pelaku seperti	- Berhasil mengumpulkan bukti digital berupa: - Email pelaku (beritahoax@gmail.com). - Password akun Facebook (Berita12345). - Caption posting hoax dan komentar korban.

		posting, komentar, dan riwayat akses.	- Cache gambar dan timestamp akses. - Tingkat keberhasilan: 50% untuk teks/link, 50% untuk gambar.
7	Browser Forensics on Web-based Tiktok Applications	Mencari bukti digital (seperti teks, foto, video, username, dan link) dari postingan yang dihapus di TikTok melalui browser Chrome untuk kasus kejahatan seperti pencemaran nama baik atau cyberbullying.	Berhasil mendapatkan 80% bukti seperti teks caption, username pelaku/korban, foto profil, thumbnail video, dan link aktivitas TikTok. Namun, video utuh gagal diperoleh (20% gagal).
8	Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques	Mengevaluasi artefak browser (seperti riwayat, cache, cookie) yang bisa dipulihkan dari berbagai mode penjelajahan (normal, privat, portabel) di browser populer seperti Chrome, Firefox, Brave, Tor, dan Edge, untuk keperluan forensik digital.	Makalah ini berkontribusi pada pemahaman tentang analisis forensik peramban dan mengidentifikasi area-area utama untuk meningkatkan perlindungan privasi dan metodologi forensik. - Mode normal menyimpan artefak terbanyak (riwayat, unduhan, kata kunci pencarian). - Mode privat masih meninggalkan jejak seperti cookie dan data sementara di memori. - Mode portabel menyimpan data di folder lokal, tetapi bisa hilang jika perangkat dicabut. - Chrome dan Edge meninggalkan artefak paling banyak, sementara Tor paling sedikit. - Tool seperti FTK Imager dan SQLite Browser efektif untuk ekstraksi data.

9	Digital forensic analysis of discord on google chrome	Menganalisis jejak digital (artefak) yang ditinggalkan oleh aplikasi Discord saat digunakan melalui browser Google Chrome, termasuk pesan, pengaturan akun, informasi pembayaran, dan media yang diunggah.	Analisis berbagai artefak seperti informasi pembayaran, pesan terkirim, pengaturan akun, percakapan, lampiran yang diunggah, dan banyak lagi, yang semuanya dapat digunakan dalam investigasi forensik. - Informasi Akun: ID pengguna, username, token login, dan pengaturan tema bisa dipulihkan dari local storage dan cache. - Pembayaran: Detail kartu kredit (4 digit terakhir, alamat penagihan) ditemukan di cache tanpa enkripsi. - Pesan & Media: Konten pesan, lampiran (gambar, video), serta waktu pengiriman tersimpan di cache. - Aktivitas Lain: Jejak panggilan video, server yang diikuti, dan emoji yang digunakan juga bisa dilacak. - Temuan Krusial: Token login Discord bisa digunakan untuk mengakses akun tanpa kata sandi, dan data sensitif seperti info pembayaran rentan bocor.
10	Browser Forensic of Extortion Case on WhatsApp Web using National Institute of Justice Method	Meneliti kasus pemerasan via WhatsApp Web dengan mencari bukti digital seperti chat yang dihapus, foto profil, dan riwayat akses.	- **Informasi Akun**: ID pengguna, username, token login, dan pengaturan tema bisa dipulihkan dari local storage dan cache. - **Pembayaran**: Detail kartu kredit (4 digit terakhir, alamat penagihan) ditemukan di cache tanpa enkripsi. - **Pesan & Media**: Konten pesan, lampiran (gambar, video),

			serta waktu pengiriman tersimpan di cache. - **Aktivitas Lain**: Jejak panggilan video, server yang diikuti, dan emoji yang digunakan juga bisa dilacak. - **Temuan Krusial**: Token login Discord bisa digunakan untuk mengakses akun tanpa kata sandi, dan data sensitif seperti info pembayaran rentan bocor.
11	Forensic Web Analysis on The Latest Version of Whatsapp Browser	Menganalisis artefak digital di versi terbaru WhatsApp Browser untuk keperluan forensik, seperti percakapan, file media, dan data panggilan, serta mengeksplorasi metode pemulihan data yang terenkripsi.	Berhasil memulihkan dan menganalisis artefak seperti percakapan yang terhapus, file media, dan data panggilan. Beberapa alat bisa memulihkan data dengan sempurna, sementara lainnya memiliki keterbatasan.
12	WhatsApp Web Client Live Forensics Technique	Mengembangkan teknik forensik langsung (*live forensics*) untuk mengekstrak data dari sesi WhatsApp Web yang aktif di browser, termasuk pesan, kontak, dan file media, tanpa perlu akses ke perangkat mobile.	Berhasil mengekstrak data WhatsApp Web secara langsung dari browser, bahkan dalam keadaan offline. Data disimpan dalam format JSON dan ZIP, siap untuk analisis forensik lebih lanjut.
13	Analisis Forensik Digital Pada Whatsapp Dan	Mengungkap bukti digital berupa audio dan video yang terhapus di	- Magnet Axiom: Paling efektif (100% audio/video di WhatsApp, tapi hanya 8.33%

	Facebook Menggunakan Metode NIST	WhatsApp dan Facebook Messenger untuk kasus kejahatan seperti penjualan narkoba.	audio dan 5% video di FB Messenger). - Belkasoft: 50% audio dan 41% video di WhatsApp; 8.33% audio dan 41% video di FB Messenger. - Oxygen: 16.67% audio dan 23.5% video di WhatsApp; gagal di FB Messenger. - MOBILedit: Gagal mengembalikan data (0%).
14	Komparatif Web-based Instant Messaging Vulnerability Menggunakan Metode Association of Chief Police Officers	Membandingkan tingkat kerentanan (*vulnerability*) aplikasi WhatsApp, Telegram, dan Skype berbasis web terhadap akuisisi data pribadi oleh pelaku *cybercrime*.	- Skype Web paling rentan: 92% data bisa diambil (termasuk pesan teks, gambar, nomor telepon, dan user ID). - WhatsApp & Telegram Web: Sama-sama 67% (hanya pesan teks, nomor telepon, dan user ID). - FTK Imager lebih efektif mengambil data gambar dibanding OSForensic..
15	Privacy Preserving Internet Browsers: Forensic Analysis of Browzar	Mengevaluasi klaim privasi total dari Browzar (browser privasi) dan membandingkannya dengan mode penyamaran di Google Chrome dan Mozilla Firefox, termasuk analisis forensik untuk menemukan jejak aktivitas yang tersisa.	- Browzar: Meski mengklaim "tanpa jejak", jejak seperti pencarian (beer, scotch) dan folder sisa (Browzar) ditemukan di RAM, pagefile.sys, dan WebCacheV01.dat. - Chrome & Firefox: Mode penyamaran menghapus riwayat lokal, tetapi jejak tetap ada di RAM dan pagefile.sys. - Browzar meninggalkan lebih banyak artefak dibanding Chrome/Firefox, membuatnya lebih rentan terhadap investigasi forensik.

Penelitian-penelitian sebelumnya telah banyak mengkaji aspek forensik digital pada platform komunikasi maupun layanan berbasis web. Misalnya, studi tentang keamanan data

pribadi pada mode privat browser menunjukkan bahwa meskipun riwayat penelusuran tidak tersimpan di hard disk, informasi sensitif seperti akun dan kata sandi masih dapat dipulihkan dari RAM. Penelitian lain mengenai aktivitas *cyberbullying* di Facebook melalui browser Chrome menegaskan efektivitas *live forensics* dalam mengungkap artefak digital berupa komentar, *timestamp*, hingga identitas akun pelaku. Sementara itu, kajian forensik pada marketplace online menyoroti adanya perbedaan tingkat keamanan antar browser, di mana Mozilla Firefox dinilai lebih konsisten dalam melindungi data dibandingkan Chrome.

Dalam konteks aplikasi komunikasi, beberapa penelitian mulai mengarahkan perhatian pada Discord, baik melalui aplikasi desktop maupun peramban web. Temuan menunjukkan bahwa alat khusus seperti DiscFor maupun ChromeCacheView dapat memulihkan pesan, gambar, bahkan metadata interaksi, meskipun masih terdapat keterbatasan ketika data sudah dihapus atau terenkripsi. Namun demikian, sebagian besar penelitian terdahulu hanya berfokus pada satu platform atau satu jenis browser, sehingga belum memberikan gambaran komprehensif mengenai perbandingan lintas browser. Celah inilah yang coba diisi oleh penelitian ini, dengan menghadirkan pendekatan komparatif menggunakan beberapa tools forensik (Autopsy, MZCacheView, dan ChromeCacheView) serta kerangka kerja Enhanced GCFIM, untuk menganalisis dan memulihkan artefak digital Discord yang diakses melalui tiga browser berbeda: Google Chrome, Mozilla Firefox, dan Microsoft Edge.

2.2 Dasar Teori

2.2.1 Digital Forensik

Forensik komputer muncul sebagai respons terhadap meningkatnya kejahatan yang dilakukan dengan memanfaatkan sistem komputer, baik sebagai objek kejahatan, instrumen yang digunakan untuk melakukan kejahatan, maupun sebagai tempat penyimpanan bukti terkait kejahatan. Jejak forensik komputer dapat ditelusuri kembali ke tahun 1984, ketika laboratorium FBI dan lembaga penegak hukum lainnya mulai mengembangkan program untuk memeriksa bukti komputer. Sejak itu, kelompok riset seperti *Computer Analysis and Response Team* (CART), *Scientific Working Group on Digital Evidence* (SWGDE), *Technical Working Group on Digital Evidence* (TWGDE), dan *National Institute of Justice* (NIJ) telah dibentuk untuk mendiskusikan ilmu forensik komputer sebagai suatu disiplin, termasuk kebutuhan akan pendekatan standar dalam pemeriksaan. Forensik digital sendiri didefinisikan sebagai penggunaan metode yang berasal dari ilmu pengetahuan dan terbukti

dalam proses pengamanan, pengumpulan, validasi, identifikasi, analisis, interpretasi, dan penyajian bukti digital yang berasal dari sumber digital. Tujuan dari proses ini adalah untuk memfasilitasi atau memajukan rekonstruksi peristiwa yang terbukti kriminal atau membantu mengantisipasi tindakan tidak sah yang diketahui mengganggu operasi yang direncanakan. Salah satu elemen penting dari forensik digital adalah **kredibilitas bukti digital.** Bukti digital meliputi bukti komputer, audio digital, video digital, ponsel, mesin faks digital, dan lain-lain. Dalam pengaturan hukum, bukti diharapkan memiliki integritas, keaslian, reproduktifitas, non-interferensi, dan minimisasi.

Forensik digital mengacu pada proses sistematis dalam mengamankan, mengidentifikasi, mengekstrak, dan mendokumentasikan bukti komputer yang dapat digunakan sebagai bukti hukum. Ini melibatkan penerapan keahlian teknologi untuk mengungkap bukti dari berbagai media digital, seperti komputer, ponsel, server, dan jaringan. Dengan membekali tim forensik dengan teknik dan peralatan canggih, forensik digital memungkinkan mereka untuk secara efektif menyelesaikan kasus-kasus rumit yang melibatkan aspek digital (Vaddi et al., 2024).

Dalam proses penyelidikan dan penyidikan, forensik digital berfungsi sebagai alat bantu penting bagi penyidik. Peran ini sejalan dengan landasan hukum yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta Kitab Undang-Undang Hukum Acara Pidana. Dalam lingkup hukum acara pidana, proses verifikasi kebenaran peristiwa yang dilaporkan, yang dilakukan oleh hakim melalui bukti-bukti sah yang diajukan, dikenal sebagai proses pembuktian (Rosmaida & Bakhtiar, 2025)

2.2.2 Discord

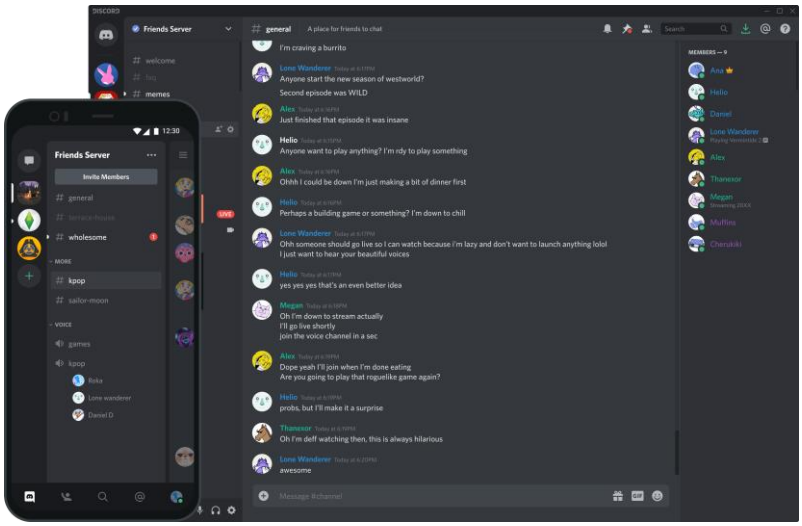
Discord merupakan sebuah aplikasi komunikasi berbasis internet yang dirancang untuk memfasilitasi percakapan melalui teks, suara, maupun video secara real-time. Platform ini pertama kali diperkenalkan pada tahun 2015 oleh Jason Citron dan Stanislav Vishnevskiy dengan tujuan awal sebagai sarana komunikasi komunitas gamer. Discord merupakan salah satu platform komunikasi daring yang mengalami pertumbuhan pengguna yang sangat pesat sejak pertama kali diperkenalkan pada tahun 2015. Data (Turner, 2024) menunjukkan bahwa jumlah pengguna terdaftar Discord meningkat secara signifikan dari sekitar 25 juta pengguna pada tahun 2016 menjadi 90 juta pada tahun 2017, kemudian terus bertambah hingga mencapai 130 juta pada tahun 2018 dan 250 juta pada tahun 2019. Pertumbuhan ini berlanjut pada tahun-tahun berikutnya dengan 300 juta pengguna pada tahun 2020, 370 juta pada tahun 2021, serta 456 juta pada tahun 2022. Pada tahun 2023 jumlah pengguna telah

mencapai 563 juta, kemudian meningkat menjadi 614 juta pada tahun 2024, dan diperkirakan mencapai sekitar 689 juta pengguna pada tahun 2025. Peningkatan jumlah pengguna yang konsisten ini menunjukkan bahwa Discord telah berkembang menjadi salah satu platform komunikasi digital yang sangat populer dan digunakan secara luas oleh berbagai komunitas di seluruh dunia, tidak hanya untuk kegiatan hiburan seperti gim daring, tetapi juga untuk komunikasi komunitas, pendidikan, hingga aktivitas profesional. Popularitas yang tinggi tersebut menjadikan Discord sebagai platform yang relevan untuk diteliti dalam konteks forensik digital, karena tingginya jumlah pengguna juga meningkatkan potensi munculnya berbagai aktivitas yang meninggalkan jejak artefak digital.

Year	Registered Users (in millions)
2025*	689
2024*	614
2023	563
2022	456
2021	370
2020	300
2019	250
2018	130
2017	90
2016	25

Gambar 2. 1 Pengguna Discord

Namun, seiring perkembangannya, Discord tidak hanya digunakan oleh kalangan gamer, melainkan juga oleh komunitas belajar, profesional, maupun organisasi yang membutuhkan media komunikasi daring yang fleksibel. Discord menyediakan berbagai fitur seperti kanal teks dan suara, berbagi layar (*screen sharing*), integrasi bot untuk otomatisasi, serta dukungan terhadap media berupa gambar, video, dan dokumen. Salah satu keunggulan utama Discord adalah kemampuannya dalam membangun komunitas melalui sistem server yang dapat dikelola dengan beragam tingkatan peran dan izin pengguna.



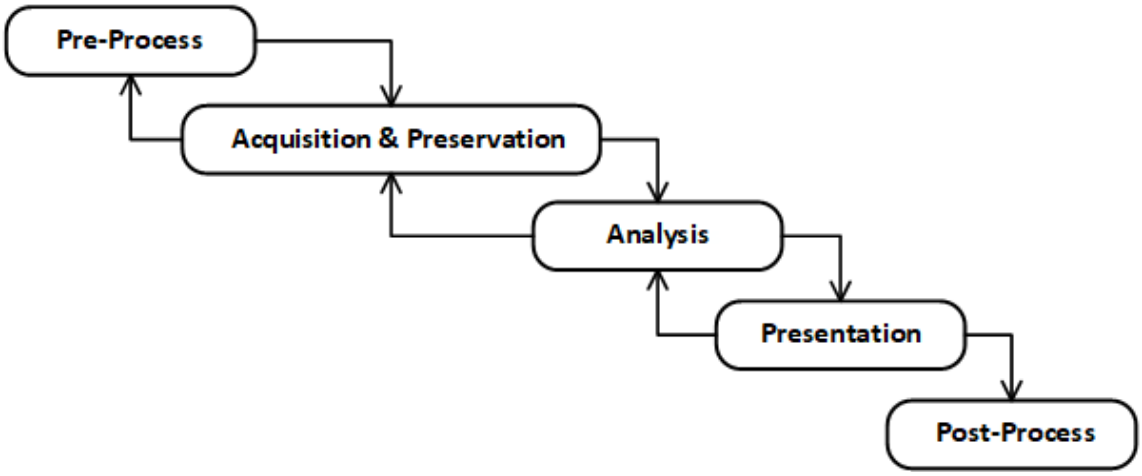
Gambar 2. 2 Aplikasi Discord

Dalam perkembangannya, Discord telah mengalami transformasi signifikan, dari sekadar aplikasi pesan instan menjadi sebuah platform sosial yang terintegrasi dengan berbagai layanan pihak ketiga, termasuk Spotify, Twitch, hingga integrasi API untuk kebutuhan pengembangan bot. Hingga kini, Discord terus berinovasi dengan menambahkan fitur-fitur baru seperti *Stage Channel*, *Threads*, dan dukungan *Nitro* untuk pengalaman komunikasi yang lebih personal, sekaligus memperkuat posisinya sebagai salah satu platform komunikasi digital yang paling banyak digunakan secara global. Dengan pertumbuhan pesat jumlah penggunanya, Discord tidak hanya relevan sebagai aplikasi sosial, tetapi juga menjadi objek penelitian penting dalam bidang keamanan dan forensik digital karena interaksi di dalamnya meninggalkan jejak data yang dapat dianalisis lebih lanjut untuk kepentingan investigasi maupun akademis.

2.2.3 Generic Computer Forensic Investigation Model (GCFIM)

GCFIM terdiri dari lima fase yaitu Pra-Proses, Akuisisi & Pelestarian, Analisis, Presentasi, dan Pasca-Proses (Yusoff, Y., et al., 2011).

Fase 1 GCFIM dikenal sebagai **Pre-Process**. Tugas yang dilakukan dalam fase ini berkaitan dengan semua pekerjaan yang perlu dilakukan sebelum investigasi aktual dan pengumpulan data resmi. Di antara tugas yang harus dilakukan adalah mendapatkan persetujuan yang diperlukan dari otoritas terkait, menyiapkan dan menyiapkan alat yang akan digunakan dan lain-lain.



Gambar 2. 3 Diagram Alir GCFIM

Fase 2 dikenal sebagai **Acquisition dan Preservation**. Tugas yang dilakukan dalam fase ini terkait dengan mengidentifikasi, memperoleh, mengumpulkan, mengangkut, menyimpan, dan melestarikan data. Secara umum, fase ini adalah tempat semua data yang relevan diambil, disimpan, dan disediakan untuk fase berikutnya.

Fase 3 dikenal sebagai **Analysis**. Ini adalah bagian utama dan pusat dari proses investigasi forensik komputer. Fase ini memiliki jumlah fase terbanyak dalam kelompoknya sehingga mencerminkan fokus sebagian besar model yang ditinjau memang pada fase analisis. Berbagai jenis analisis dilakukan pada data yang diperoleh untuk mengidentifikasi sumber kejahatan dan akhirnya menemukan orang yang bertanggung jawab atas kejahatan tersebut.

Fase 4 dikenal sebagai **Presentation**. Temuan dari fase analisis didokumentasikan dan disajikan kepada pihak berwenang. Jelas, fase ini sangat penting karena kasus tersebut tidak hanya harus disajikan dengan cara yang dipahami dengan baik oleh pihak yang disajikan, tetapi juga harus didukung dengan bukti yang memadai dan dapat diterima. Hasil utama dari fase ini adalah untuk membuktikan atau membantah dugaan tindak pidana.

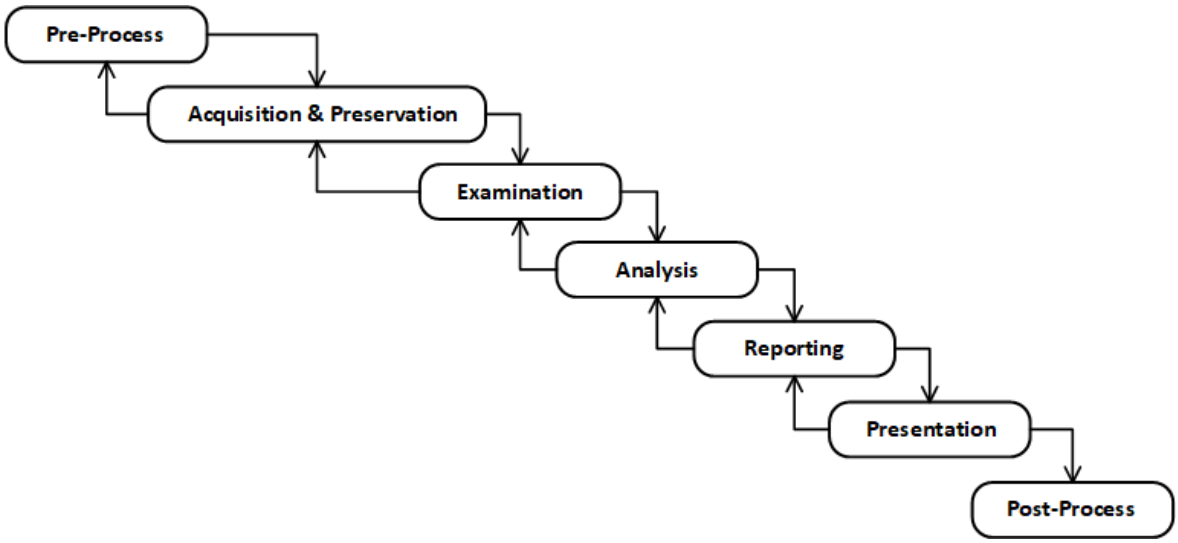
Fase 5 dikenal sebagai **Post-Process**. Fase ini berkaitan dengan penutupan investigasi yang tepat. Bukti digital dan fisik perlu dikembalikan dengan benar kepada pemilik yang sah dan disimpan di tempat yang aman, jika perlu. Peninjauan proses investigasi harus dilakukan agar pelajaran dapat dipelajari dan digunakan untuk perbaikan investigasi di masa mendatang.

Alih-alih berpindah secara berurutan dari satu fase ke fase lainnya, kemampuan untuk kembali ke fase sebelumnya harus selalu ada. Berhadapan dengan situasi yang terus berubah dalam hal tempat kejadian perkara (fisik dan digital), alat investigasi yang

digunakan, alat kejahatan yang digunakan, dan tingkat keahlian para penyidik. Karena itu, sangat diharapkan untuk dapat kembali ke fase sebelumnya yang telah dilakukan, tidak hanya untuk memperbaiki kelemahan, tetapi juga untuk memperoleh hal/informasi baru.

2.2.4 Enhanced/Improved Computer Forensic Investigation Model (GCFIM)

Pada penelitian sebelumnya, (Hamad & Jazzar, 2024)mengamati steganografi sebagai salah satu teknik anti-forensik yang kerap digunakan pelaku kejahatan siber untuk



menyembunyikan pesan di dalam file digital, sehingga menyulitkan proses identifikasi bukti asli. Untuk menjawab tantangan ini, mereka mengembangkan *Improved Generic Computer Forensic Investigation Model* (GCFIM) yang terdiri dari tujuh tahapan, mulai dari pra-proses hingga pasca-proses, dengan fleksibilitas untuk kembali ke tahap sebelumnya bila diperlukan. Penelitian ini menguji 20 file dengan pesan tersembunyi menggunakan FEX Imager, OSForensics, WinHex, Hiderman, dan StegSpy. Hasilnya, StegSpy dan Hiderman berhasil mendeteksi 18 file, OSForensics efektif menemukan *mismatched files*, dan WinHex memverifikasi integritas data. Hal ini menunjukkan bahwa penerapan GCFIM yang disempurnakan dengan dukungan perangkat forensik mampu meningkatkan efektivitas investigasi digital terhadap teknik anti-forensik.

Gambar 2. 4 Enhanced GFCIM

Gambar 2.4 menunjukkan 7 (tujuh) fase GCFIM yang telah ditingkatkan (*enhanced*) atau disebut **EGCFIM**, yaitu: pre-processing, acquistion & preservation, examination, analysis, reporting, presentation, dan post-process. Berikut penjelasan setiap fasenya:

1. **Fase *Pre-Processing***

Fase ini mencakup semua pekerjaan persiapan yang harus dilakukan sebelum investigasi dan pengumpulan data formal dimulai. Persetujuan dari otoritas terkait dan persiapan alat yang digunakan merupakan salah satu kegiatan tersebut.

2. **Fase *Acquisition & Preservation***

Fase ini meliputi pencarian, pengumpulan, penyimpanan, dan pemeliharaan perangkat elektronik yang ditemukan di lokasi kejadian perkara yang mungkin berisi data seperti komputer, telepon pintar, dan drive USB. Sebagai aturan umum, selama fase ini, penyidik harus mengumpulkan dan melindungi temuan penting apa pun sebagai persiapan untuk langkah berikutnya.

3. **Fase *Examination***

Akuisisi data dan ekstraksi data merupakan dua operasi utama dalam fase ini (Khweiled, R., et al., 2021). Jenis sumber data, seperti komputer, telepon pintar, USB, atau perangkat elektronik lainnya, harus dipertimbangkan saat mengumpulkan data menggunakan alat akuisisi data, perangkat lunak, dan perangkat keras. Setiap sumber data memiliki cara unik dalam mengumpulkan informasi, sehingga ada berbagai pendekatan. Perangkat lunak dan alat stasiun kerja forensik digital digunakan untuk melakukan fase ekstraksi data. Data yang diperoleh kemudian digunakan untuk analisis lebih lanjut dan ekstraksi bukti yang relevan.

4. **Fase *Analysis***

Fase ini merupakan inti dan bagian utama dari investigasi forensik komputer, yang akan dibahas. Analisis dilakukan terhadap data untuk mengetahui dari mana kejahatan itu berasal dan siapa yang melakukannya, pemeriksaan data yang diperoleh untuk menentukan asal kejahatan dan tujuan kejahatan, dan kemudian orang yang melakukannya dapat ditemukan. Hasil dari fase analisis dicatat dan diberikan kepada pihak berwenang yang sesuai.

5. **Fase *Reporting***

Pada fase ini, laporan komprehensif dibuat berdasarkan analisis hasil. Laporan ini mencakup metode yang digunakan untuk mendapatkan hasil, klarifikasi tentang bagaimana alat dan metode dipilih, dan pernyataan tentang apakah metode lain perlu dilakukan. Tujuan laporan adalah untuk memberikan informasi faktual kepada orang yang tepat dan membantu mereka mengetahui apa yang terjadi. Selain itu, laporan harus ditulis dengan cara yang memudahkan orang yang bukan ahli di bidang forensik digital untuk memahaminya. Laporan lisan memberi tahu hasil akhir

tentang ada atau tidaknya bukti untuk membantu penyelidikan. Selain itu, laporan menjelaskan fakta apa pun yang tidak jelas.

6. **Fase *Presentation***

Analis forensik mengirimkan laporan yang dibuat pada langkah sebelumnya ke pihak berwenang dan penyidik yang tepat untuk mengetahui apakah laporan tersebut dapat diterima atau tidak di pengadilan. Langkah ini penting karena argumen tidak hanya harus disajikan dengan cara yang mudah dipahami oleh orang yang diberi argumen, tetapi juga harus didukung oleh bukti yang sesuai dan dapat diterima. Hasil utama dari fase ini adalah membuktikan atau menolak dugaan kegiatan ilegal.

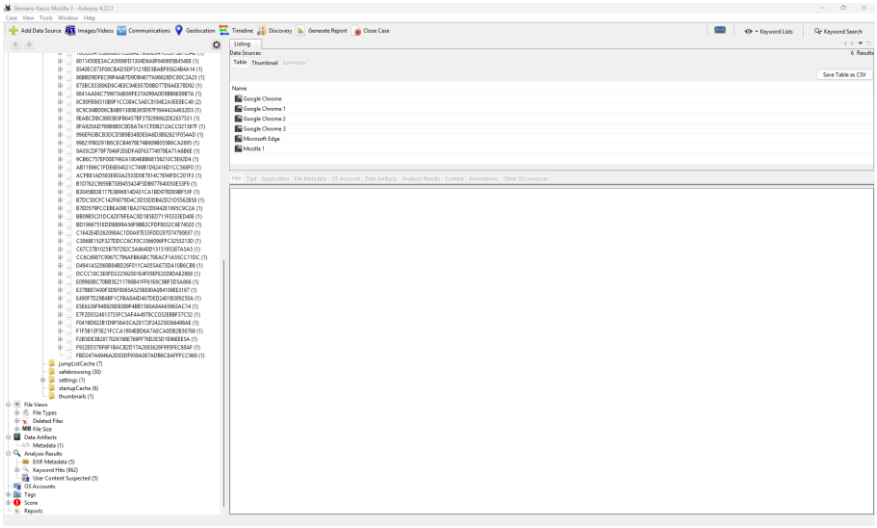
7. **Fase *Post-Process***

Ketika investigasi dilakukan dengan benar, fase ini adalah tentang bagaimana menyelesaikannya dengan benar. Bukti digital atau fisik perlu dikembalikan ke pemilik yang sah, atau disimpan di tempat yang aman jika perlu. Harus ada tinjauan ulang terhadap proses investigasi sehingga pelajaran dapat dipelajari dan digunakan untuk membuat investigasi berikutnya menjadi lebih baik. Skenario yang selalu berkembang dalam hal tempat kejadian perkara (baik fisik maupun digital), alat investigasi yang digunakan, instrumen kriminal yang digunakan, dan tingkat keterampilan penyidik. Akibatnya, sangat diinginkan untuk kembali ke fase sebelumnya yang telah kita selesaikan, tidak hanya untuk memperbaiki kekurangan tetapi juga untuk mempelajari informasi baru.

2.2.5 Autopsy

Autopsy merupakan perangkat lunak open-source yang dirancang untuk membantu proses investigasi forensik digital, khususnya dalam analisis sistem file dan artefak yang tersimpan pada perangkat penyimpanan. Aplikasi ini dikembangkan pertama kali pada tahun 2000 oleh Brian Carrier sebagai antarmuka grafis dari *The Sleuth Kit (TSK)*, sebuah kumpulan utilitas forensik berbasis command line. Seiring perkembangannya, Autopsy terus dikembangkan hingga kini menjadi salah satu platform analisis forensik digital yang banyak digunakan oleh peneliti, praktisi keamanan, maupun aparat penegak hukum di seluruh dunia. Autopsy menyediakan beragam fitur yang mendukung proses investigasi, seperti analisis sistem file, pencarian kata kunci, pemeriksaan *web artifacts* (riwayat penelusuran, cache, cookie), analisis e-mail, pengelolaan *hash set* untuk deteksi file, serta integrasi dengan berbagai modul eksternal yang memperluas fungsionalitasnya. Keunggulan utama dari Autopsy terletak pada kemampuannya untuk menampilkan data dalam antarmuka grafis

yang intuitif, sehingga memudahkan penyidik dalam menelusuri bukti digital tanpa harus menggunakan perintah terminal yang kompleks.



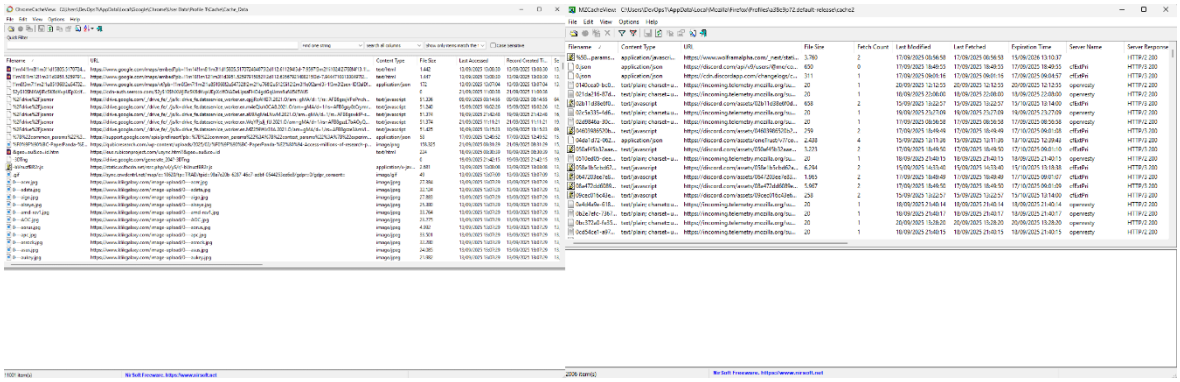
Gambar 2. 5 Antarmuka Autopsy

Selain itu, Autopsy juga mendukung manajemen kasus secara terorganisasi, memungkinkan pengguna untuk menyimpan, mengelompokkan, dan mendokumentasikan bukti dalam sebuah proyek investigasi yang sistematis. Hingga kini, Autopsy telah berkembang menjadi salah satu standar de facto dalam dunia forensik digital karena sifatnya yang gratis, fleksibel, dan terus dikembangkan oleh komunitas maupun sponsor institusi keamanan. Dengan keberadaannya, Autopsy tidak hanya membantu mempercepat proses investigasi digital, tetapi juga memberikan kontribusi penting bagi dunia pendidikan dan penelitian, karena dapat digunakan sebagai media pembelajaran praktik forensik digital secara langsung.

2.2.6 ChromeCacheView dan MZCacheView

ChromeCacheView dan MZCacheView merupakan perangkat lunak ringan yang dikembangkan oleh NirSoft dan banyak dimanfaatkan dalam bidang forensik digital untuk menganalisis file cache pada peramban web. ChromeCacheView dirancang khusus untuk mengekstrak dan menampilkan file cache yang tersimpan di Google Chrome serta browser berbasis Chromium lainnya, seperti Microsoft Edge. Aplikasi ini memungkinkan peneliti atau praktisi forensik untuk melihat rincian file cache, termasuk URL sumber, jenis file, ukuran, tanggal akses terakhir, hingga lokasi penyimpanan file pada sistem. Sementara itu, MZCacheView memiliki fungsi serupa tetapi ditujukan untuk browser Mozilla Firefox. Dengan menggunakan aplikasi ini, pengguna dapat menelusuri artefak digital berupa

gambar, dokumen, script, maupun file lain yang pernah diakses melalui browser. Kedua aplikasi ini memiliki keunggulan dalam hal kesederhanaan dan portabilitas, karena tidak memerlukan instalasi kompleks dan dapat langsung dijalankan pada sistem Windows.



Gambar 2. 6 Antarmuka ChromeCacheView dan MZCacheView

Dalam perkembangannya, ChromeCacheView dan MZCacheView tidak hanya berguna bagi pengguna umum yang ingin melihat atau menyalin kembali data dari cache browser, tetapi juga menjadi salah satu tools penting dalam proses investigasi forensik digital. Hal ini disebabkan karena cache browser sering kali menyimpan bukti penting dari aktivitas pengguna di internet, termasuk interaksi pada platform komunikasi seperti Discord, yang dapat mencakup pesan, media, maupun tautan yang diakses. Dengan demikian, penggunaan ChromeCacheView dan MZCacheView dalam ranah forensik digital membantu memperkuat proses identifikasi, akuisisi, dan analisis bukti, sekaligus menambah alternatif bagi penyidik dalam mengungkap artefak digital yang mungkin tidak dapat diekstraksi oleh tools forensik konvensional.

2.2.7 *Live Forensic*

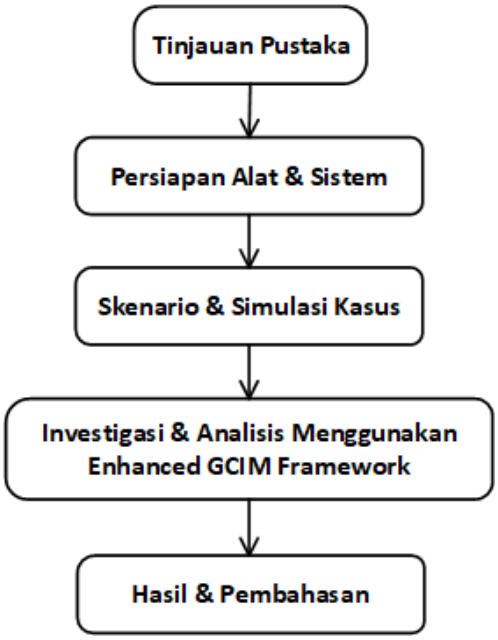
Live forensic adalah salah satu cabang dalam forensik digital yang berfokus pada proses pengumpulan, analisis, dan pelestarian bukti digital dari sistem yang masih dalam kondisi aktif atau sedang berjalan. Tidak seperti pendekatan *dead forensic* yang dilakukan pada perangkat dalam keadaan mati dengan menyalin seluruh isi media penyimpanan, live forensic dilakukan ketika perangkat dalam keadaan hidup sehingga memungkinkan penyidik memperoleh data yang bersifat volatile, seperti *Random Access Memory (RAM)*, koneksi jaringan aktif, proses yang sedang berjalan, daftar pengguna yang login, hingga file sementara yang mungkin akan hilang ketika sistem dimatikan. Konsep live forensic muncul karena keterbatasan metode tradisional yang tidak mampu merekonstruksi data volatil,

padahal data tersebut sering kali menjadi kunci penting dalam sebuah investigasi, misalnya untuk melacak komunikasi real-time, aktivitas malware, atau akses tidak sah ke dalam sistem. Dalam perkembangannya, live forensic menjadi semakin relevan seiring meningkatnya penggunaan layanan berbasis cloud, komunikasi instan, serta aplikasi web yang menyimpan data hanya sementara pada cache atau memori. Namun, metode ini juga menghadapi tantangan serius, seperti risiko terjadinya perubahan data selama proses akuisisi yang dapat memengaruhi keabsahan bukti di pengadilan. Oleh karena itu, penerapan live forensic harus mengikuti standar dan prosedur yang ketat, termasuk penggunaan tools yang andal serta pencatatan proses secara detail untuk menjaga integritas bukti. Dengan demikian, live forensic tidak hanya berperan sebagai pelengkap metode tradisional, tetapi juga sebagai langkah penting dalam mengungkap bukti digital yang sifatnya cepat hilang, sekaligus memperkaya praktik investigasi forensik modern.

BAB III
Metodologi

3.1 Metodologi Penelitian

Untuk mencapai tujuan dan menjawab permasalahan penelitian, diperlukan tahapan-tahapan penelitian agar dapat menyelesaikan masalah. Berikut metodologi penelitian yang akan dilaksanakan, yang secara umum dijelaskan dalam diagram Gambar 3.1. Pada penelitian ini, tahapan penelitian yang dilakukan untuk pengambilan bukti digital adalah menggunakan pendekatan metode *live forensic* yang dapat dilihat pada Gambar 3.1.



Gambar 3. 1 Metodologi Penelitan

3.2 Tinjauan Pustaka

Tinjauan pustaka merupakan tahap awal penelitian yang bertujuan untuk memberikan landasan teoritis serta arah dalam pelaksanaan studi. Pada tahap ini, peneliti menelaah literatur yang relevan, termasuk teori forensik digital, konsep *live forensic*, model Enhanced Generic Computer Forensic Investigation Model (Enhanced GCFIM), serta penelitian terdahulu terkait pemanfaatan tools seperti Autopsy, MZCacheView, dan ChromeCacheView. Selain itu, pembahasan juga mencakup karakteristik platform Discord serta mekanisme penyimpanan cache pada browser Google Chrome, Mozilla Firefox, dan Microsoft Edge. Melalui tinjauan pustaka ini, peneliti dapat mengidentifikasi celah

penelitian, menyusun kerangka berpikir, serta memperkuat kebaruan dan relevansi penelitian dalam konteks forensik digital.

3.3 Persiapan Alat dan Sistem

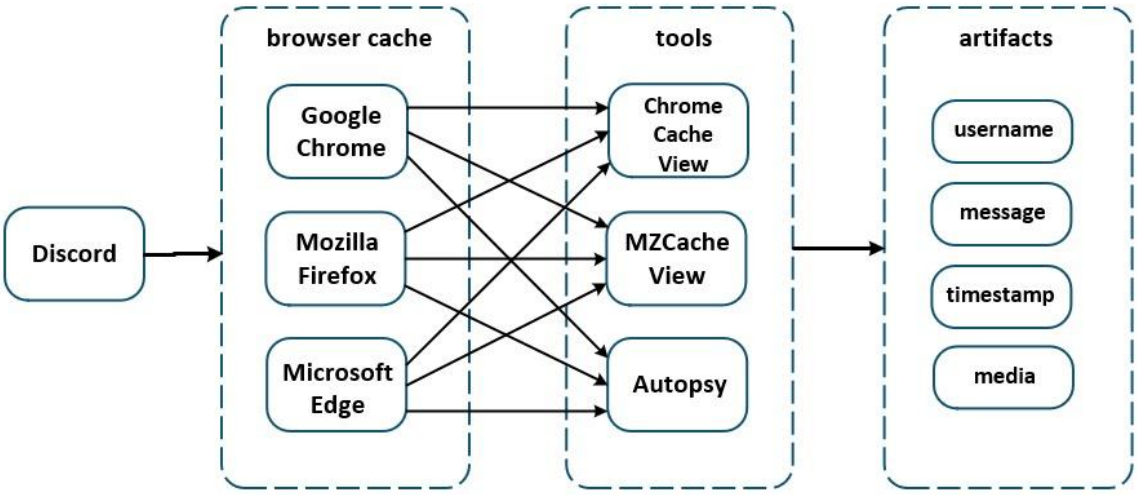
Agar penelitian dapat berjalan dengan baik, diperlukan alat dan sistem pada komputer sebagai perlengkapan untuk menunjang penelitian. Peralatan dan sistem yang digunakan dalam penelitian ini sebagai berikut:

Tabel 3. 1 Perangkat dan Sistem yang Digunakan dalam Penelitian

Hardware	Software
1. Laptop HP ZBook 15u G5 : Processor Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz 2.1 GHz Memory 1 TB SSD / 32 GB RAM Sistem Operasi Windows 11 Pro 64-bit 2. Personal Computer Processor Intel(R) Xeon(R) CPU E5-2698 v3 @ 2.30GHz (64 CPUs), ~2.3GHz Memory 2 TB SSD / 128 GB RAM Sistem Operasi Windows 11 Pro 64-bit	1. Google Chrome Version 140.0.7339.128 2. Mozilla Firefox 142.0.1 (64-bit) 3. Microsoft Edge 142.0.1 (64-bit) 4. Autopsy 4.22.1 5. ChromeCacheView v2.52 6. MZCacheView v2.22

3.4 Skenario dan Simulasi Kasus

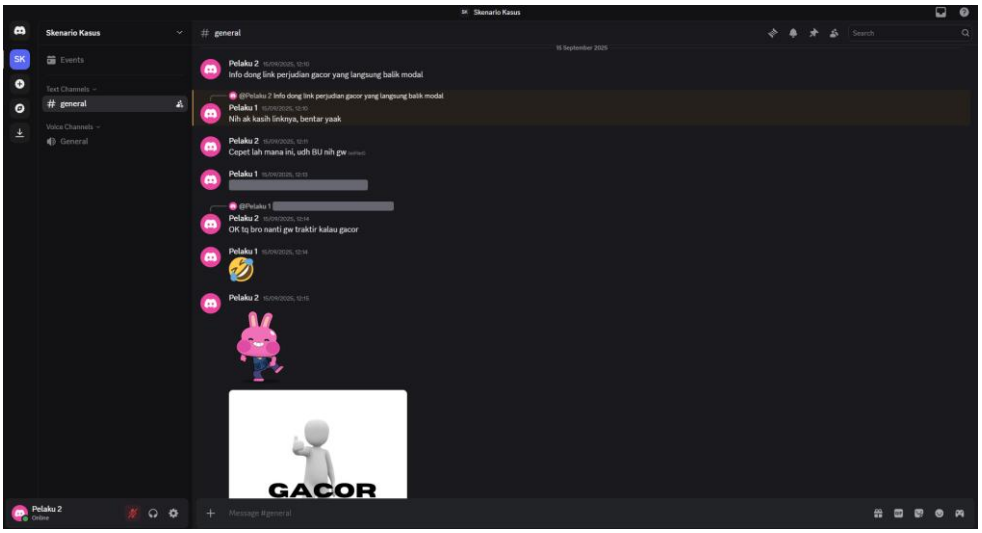
Penelitian ini juga menggunakan sebuah skenario yang menjadi acuan pelaksanaan kasus. Penelitian ini dirancang untuk menganalisis bukti digital pada platform Discord yang diakses melalui browser web, dengan fokus pada pemulihan pesan teks dan gambar yang telah dihapus. Skenario yang digunakan melibatkan percakapan antara dua pengguna di ruang chat Discord, di mana salah satu pengguna berinteraksi dengan pengguna lain . Komputer pelaku tetap menyala saat investigasi, memungkinkan tim forensik melakukan analisis langsung (live forensic) untuk mengumpulkan bukti dari cache browser.



Gambar 3. 2 Skenario Kasus

Pada skenario uji coba ini yang ada pada gambar 3.2 interaksi pengguna dengan platform Discord melalui peramban web seperti Google Chrome, Mozilla Firefox, atau Microsoft Edge menghasilkan sejumlah artefak digital yang dapat dianalisis menggunakan berbagai *tools* forensik. Pengujian difokuskan pada tiga bentuk aktivitas utama, yaitu pengiriman pesan, penggunaan emoji dan stiker, serta unggahan media. Pada tahap pengiriman pesan, sistem diuji melalui variasi jenis pesan, mencakup pesan teks biasa, pesan yang disematkan (*pinned message*), pesan yang telah diedit, pesan tersembunyi atau berformat *spoiler*, serta pesan balasan (*reply message*). Aktivitas kedua menekankan pada pemanfaatan emoji dan stiker sebagai bentuk komunikasi visual yang turut meninggalkan jejak pada cache maupun log peramban. Sementara itu, pada aktivitas ketiga dilakukan uji unggahan media berupa gambar, dokumen, dan video yang merepresentasikan bentuk konten digital beragam yang lazim digunakan dalam komunikasi daring. Ketiga aktivitas ini menjadi objek pemeriksaan dalam proses analisis data untuk mengidentifikasi sejauh mana artefak digital dapat direkonstruksi kembali.

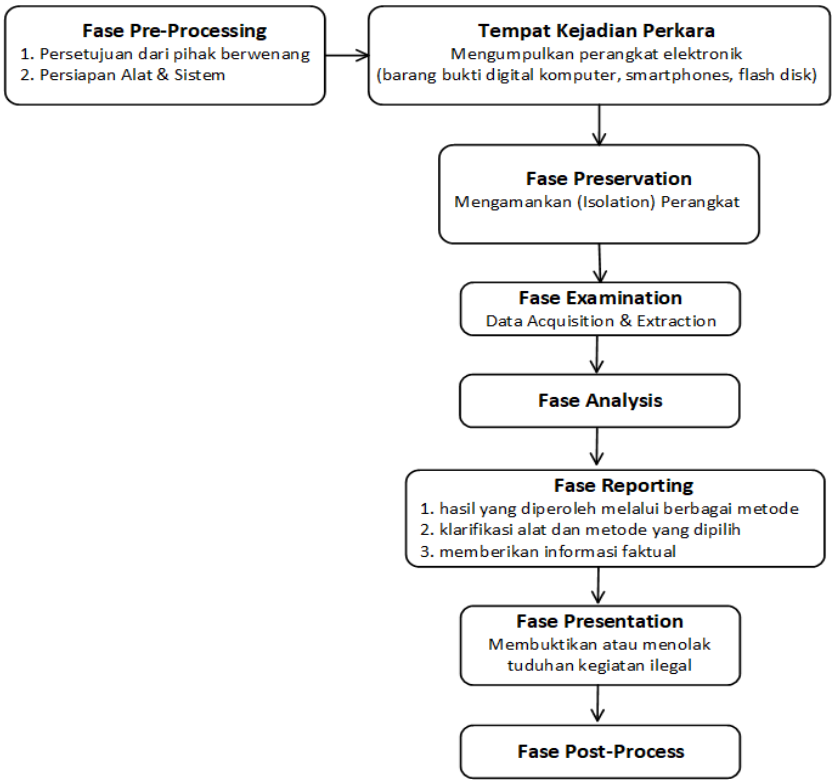
Skenario pengujian pada penelitian ini dirancang untuk merepresentasikan berbagai aktivitas pengguna pada platform Discord berbasis web. Aktivitas yang diuji meliputi pengiriman pesan teks, pengeditan dan penghapusan pesan, penggunaan emoji atau stiker, serta pengiriman dan pengunduhan file media. Variasi aktivitas tersebut bertujuan untuk menghasilkan artefak digital yang beragam pada browser cache sehingga proses analisis forensik dapat dilakukan secara lebih komprehensif. Dengan adanya beberapa skenario aktivitas tersebut, penelitian ini tidak hanya mengamati satu jenis interaksi pengguna, tetapi juga berbagai bentuk aktivitas yang umum dilakukan dalam penggunaan Discord.



Gambar 3. 3 Simulasi Interaksi pada Discord

3.5 Penerapan Metode Enhanced GCFIM

Penerapan metode Enhanced Generic Computer Forensic Investigation Model (Enhanced GCFIM) dalam penelitian ini dilakukan sebagai kerangka utama untuk mengatur proses investigasi forensik digital secara sistematis.



Gambar 3. 4 Diagram Alir EGCFIM

Model ini digunakan mulai dari tahap akuisisi data dengan pendekatan *live forensic*, yakni pengumpulan artefak digital dari browser cache dalam kondisi sistem yang masih aktif. Setelah itu dilakukan tahap pemeriksaan dan analisis, di mana tools forensik seperti Autopsy, MZCacheView, dan ChromeCacheView dimanfaatkan untuk mengekstraksi serta mengidentifikasi artefak Discord yang tersimpan pada cache browser Google Chrome, Mozilla Firefox, dan Microsoft Edge. Proses analisis tidak hanya berfokus pada kemampuan tools dalam memulihkan artefak, tetapi juga pada perbandingan hasil antar browser untuk melihat perbedaan reliabilitas penyimpanan data. Selanjutnya, hasil temuan tersebut didokumentasikan dalam tahap pelaporan, yang bertujuan menyajikan bukti digital secara valid, terstruktur, dan dapat dipertanggungjawabkan baik secara akademis maupun dalam konteks hukum. Dengan demikian, penerapan Enhanced GCFIM dalam penelitian ini memberikan kerangka kerja yang komprehensif sekaligus menjaga integritas bukti sepanjang tahapan investigasi.

3.6 Parameter

Dalam penelitian ini, parameter perbandingan ditetapkan secara konseptual berdasarkan nilai evidensial artefak dalam konteks investigasi forensik digital. Artefak yang dibandingkan meliputi identitas pengguna (username dan ID), konteks komunikasi (server/channel ID), isi percakapan (message), serta media yang dikirimkan. Parameter tersebut dipilih karena merepresentasikan elemen utama dalam pembuktian aktivitas komunikasi digital dan memiliki relevansi langsung terhadap proses identifikasi pelaku, rekonstruksi peristiwa, serta validasi interaksi pada platform Discord Web. Dengan demikian, perbandingan antar browser tidak dilakukan secara arbitrer, melainkan berdasarkan artefak yang secara forensik memiliki nilai pembuktian yang signifikan.

3.6.1 Username dan User ID

Parameter identitas pengguna yang meliputi username dan user ID dipilih sebagai salah satu dasar perbandingan karena memiliki nilai evidensial yang tinggi dalam investigasi forensik digital. Dalam konteks komunikasi daring, identitas akun merupakan elemen fundamental yang menghubungkan suatu aktivitas dengan subjek tertentu. Username berfungsi sebagai identitas tampilan (display identity), sedangkan user ID merupakan identitas unik yang bersifat sistem-generated dan tidak berubah, sehingga memiliki tingkat reliabilitas yang lebih tinggi dalam proses pembuktian.

Berdasarkan hasil analisis terhadap file cache browser, artefak username dan user ID ditemukan dalam struktur data JSON yang merupakan respons API dari Discord Web. Data tersebut tersimpan sebagai bagian dari metadata pesan, yang mencakup informasi pengirim, waktu pengiriman, serta konteks percakapan. Keberadaan kedua artefak ini menunjukkan bahwa meskipun pesan telah dihapus dari antarmuka aplikasi, informasi identitas pengguna masih dapat direkonstruksi selama data cache belum tertimpa oleh proses penyimpanan baru.

3.6.2 Server/Channel ID

Parameter server ID dan channel ID dipilih sebagai dasar perbandingan karena memiliki peran penting dalam merekonstruksi konteks komunikasi pada platform Discord. Dalam investigasi forensik digital, identifikasi isi pesan saja tidak cukup tanpa mengetahui lokasi atau ruang komunikasi tempat interaksi tersebut berlangsung. Server ID merepresentasikan komunitas atau ruang besar tempat pengguna berinteraksi, sedangkan channel ID menunjukkan sub-ruang percakapan yang lebih spesifik. Kedua elemen ini memungkinkan investigator mengaitkan suatu pesan dengan konteks sosial dan struktur komunikasi tertentu.

3.6.3 Message/Text

Parameter message atau isi percakapan merupakan komponen utama dalam investigasi komunikasi digital karena merepresentasikan substansi interaksi antar pengguna. Dalam konteks forensik, isi pesan memiliki nilai pembuktian yang tinggi karena dapat menunjukkan maksud, pola komunikasi, maupun indikasi aktivitas tertentu. Oleh karena itu, parameter ini dijadikan salah satu dasar utama dalam perbandingan antar browser.

Berdasarkan hasil analisis terhadap file cache, artefak pesan ditemukan dalam struktur data JSON yang merupakan respons API Discord Web. Data tersebut mencakup konten pesan asli, pesan yang telah diedit, balasan (reply), pinned message, serta pesan dengan format tertentu seperti spoiler. Meskipun pesan telah dihapus dari tampilan aplikasi, jejaknya masih dapat ditemukan dalam cache selama data tersebut belum tertimpa oleh proses penyimpanan baru. Hal ini menunjukkan bahwa browser menyimpan respons komunikasi dalam bentuk data terstruktur sebelum direnderer ke antarmuka pengguna.

3.6.4 Timestamp

Timestamp merupakan informasi waktu yang menunjukkan kapan suatu aktivitas terjadi dalam sistem. Dalam konteks platform Discord, timestamp digunakan untuk menandai waktu pengiriman pesan, interaksi pengguna, maupun proses pemuatan data pada aplikasi. Informasi ini menjadi salah satu artefak penting dalam investigasi forensik digital karena dapat membantu merekonstruksi urutan kejadian berdasarkan aktivitas yang dilakukan oleh pengguna.

Pada Discord Web, data timestamp dapat ditemukan dalam file cache browser yang tersimpan dalam format JSON. Informasi waktu ini biasanya berkaitan dengan aktivitas percakapan seperti waktu pengiriman pesan atau waktu pemuatan konten pada halaman Discord. Analisis terhadap artefak timestamp bertujuan untuk mengidentifikasi kapan aktivitas komunikasi terjadi sehingga dapat membantu penyelidik dalam menyusun kronologi kejadian selama proses investigasi digital.

3.6.5 Media

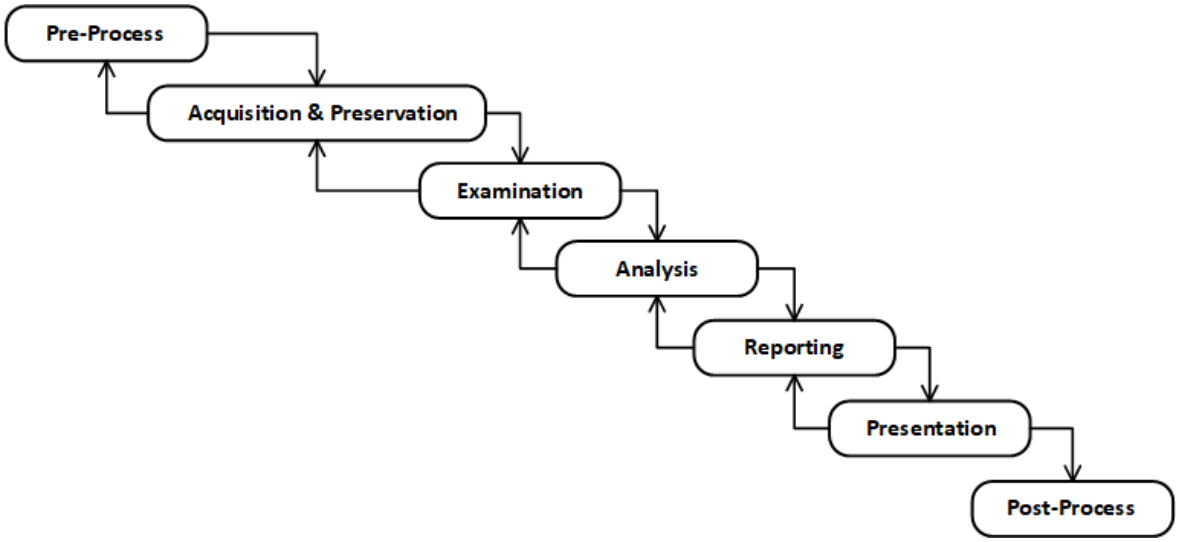
Parameter media mencakup file non-teks yang dikirimkan melalui Discord Web, seperti gambar, dokumen, dan video. Dalam konteks forensik digital, artefak media memiliki nilai pembuktian yang signifikan karena dapat merepresentasikan konten visual maupun dokumen yang berkaitan langsung dengan aktivitas komunikasi. Oleh karena itu, media dijadikan salah satu parameter perbandingan untuk menilai sejauh mana browser cache menyimpan artefak file yang dikirimkan melalui platform.

BAB IV

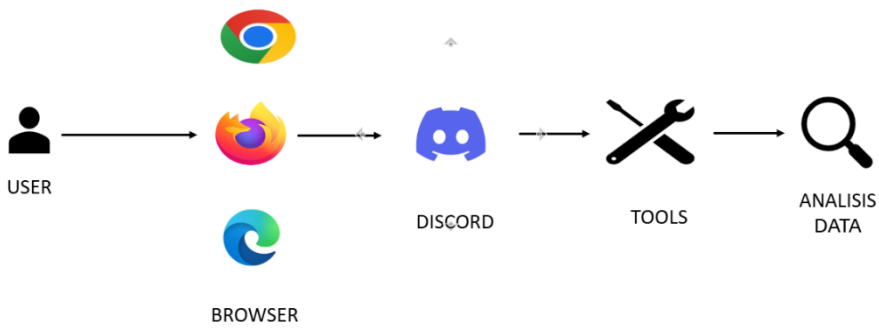
Hasil dan Pembahasan

4.1 Penggunaan Metode dan Skenario Kasus

Metode Enhanced GCFIM (Enhanced Generic Computer Forensic Investigation Model) diterapkan dalam penelitian ini untuk mencapai tujuan dan menjawab permasalahan penelitian dengan memastikan pendekatan forensik yang terstruktur, dimulai dari identifikasi bukti, akuisisi data, analisis, hingga pelaporan. Eksperimen dilakukan menggunakan tiga browser berbeda—Google Chrome, Mozilla Firefox, dan Microsoft Edge—untuk membandingkan efektivitas pemulihan data. Alat forensik seperti Autopsy, digunakan untuk mengekstrak bukti yang terhapus, termasuk username, timestamp, dan konten percakapan. Hasilnya menunjukkan bahwa kombinasi alat forensik dapat mengungkap bukti digital yang kritis, meskipun tingkat akurasi bervariasi tergantung pada browser dan alat yang digunakan.

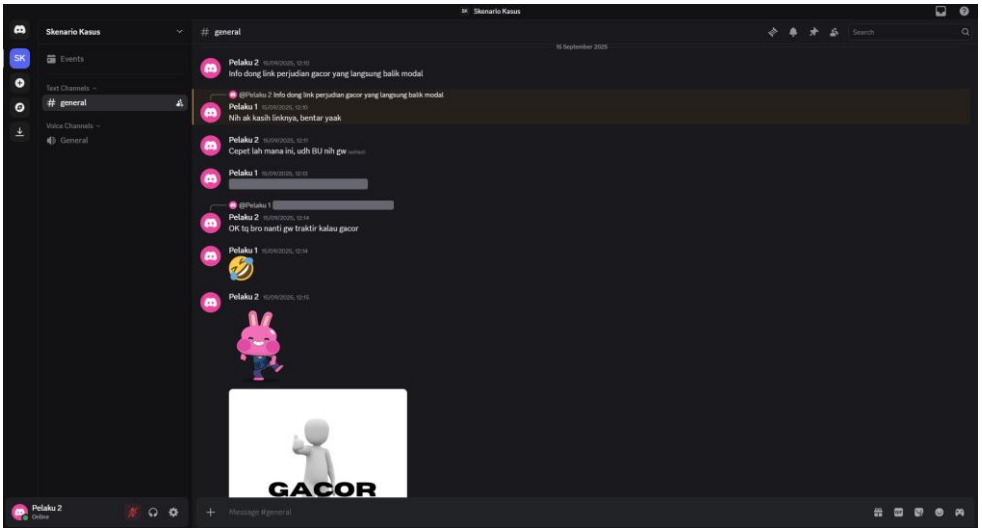


Gambar 4. 1 Enhanced GCFIM



Gambar 4. 2 Skenario Kasus

Pada skenario uji coba ini yang tertera pada gambar 4.2 interaksi pengguna dengan platform Discord melalui peramban web seperti Google Chrome, Mozilla Firefox, atau Microsoft Edge menghasilkan sejumlah artefak digital yang dapat dianalisis menggunakan berbagai *tools* forensik. Pengujian difokuskan pada tiga bentuk aktivitas utama, yaitu pengiriman pesan, penggunaan emoji dan stiker, serta unggahan media. Pada tahap pengiriman pesan, sistem diuji melalui variasi jenis pesan, mencakup pesan teks biasa, pesan yang disematkan (*pinned message*), pesan yang telah diedit, pesan tersembunyi atau berformat *spoiler*, serta pesan balasan (*reply message*). Aktivitas kedua menekankan pada pemanfaatan emoji dan stiker sebagai bentuk komunikasi visual yang turut meninggalkan jejak pada cache maupun log peramban. Sementara itu, pada aktivitas ketiga dilakukan uji unggahan media berupa gambar, dokumen, dan video yang merepresentasikan bentuk konten digital beragam yang lazim digunakan dalam komunikasi daring. Ketiga aktivitas ini menjadi objek pemeriksaan dalam proses analisis data untuk mengidentifikasi sejauh mana artefak digital dapat direkonstruksi kembali.



Gambar 4. 3 Simulasi Interaksi

4.1.1 Fase *Pre-Processing*

Fase ini meliputi berbagai kegiatan awal yang harus dipersiapkan sebelum proses investigasi dan pengumpulan data dilakukan secara resmi. Pada tahap ini, peneliti memastikan bahwa segala kebutuhan telah tersedia, mulai dari pemilihan metode, penentuan instrumen penelitian, hingga kesiapan alat bantu analisis. Dalam penelitian ini, terdapat beberapa perangkat dan bahan yang digunakan yaitu:

Tabel 4. 1 Perangkat dan Sistem yang Digunakan dalam Penelitian

Hardware	Software
1. Laptop HP ZBook 15u G5 : Processor Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz 2.1 GHz Memory 1 TB SSD / 32 GB RAM Sistem Operasi Windows 11 Pro 64-bit 2. Personal Computer Processor Intel(R) Xeon(R) CPU E5-2698 v3 @ 2.30GHz (64 CPUs), ~2.3GHz Memory 2 TB SSD / 128 GB RAM Sistem Operasi Windows 11 Pro 64-bit	1. Google Chrome Version 140.0.7339.128 2. Mozilla Firefox 142.0.1 (64-bit) 3. Microsoft Edge 142.0.1 (64-bit) 4. Autopsy 4.22.1 5. ChromeCacheView v2.52 6. MZCacheView v2.22

4.1.2 Fase *Acquisition and Preservation*

Fase ini adalah langkah dalam proses mengidentifikasi bukti di tempat kejadian perkara, yang diikuti oleh proses pengumpulan dan pelestarian keaslian bukti. Tujuannya adalah untuk melindungi bukti terhadap perubahan bentuk fisik atau data dengan menyimpannya di tempat yang aman. Bukti digital yang dikumpulkan berupa data dalam folder Cache. File yang berada dalam folder tersebut adalah file sementara yang tersimpan pada browser seperti yang ditunjukkan pada tabel 4.2 dibawah ini :

Tabel 4. 2 Direktori Akuisisi Cache Browser

Browser	Direktor Akuisisi
Mozilla Firefox	*C:\Users\DevOps1\AppData\Local\Mozilla\Firefox\Profiles\a38e9p72.default-release*.
Google Chrome	*C:\Users\DevOps1\AppData\Local\Google\Chrome\User Data\Profile 1\Cache\Cache Data*
Microsoft Edge	*C:\Users\DevOps1\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data*

Langkah selanjutnya yang dilakukan adalah memastikan keaslian dan integritas bukti digital yang telah diperoleh dari cache browser. Proses ini dilakukan melalui perhitungan nilai hash dengan algoritma MD5 dan SHA-256 sebagaimana ditunjukkan pada Tabel 4.3.

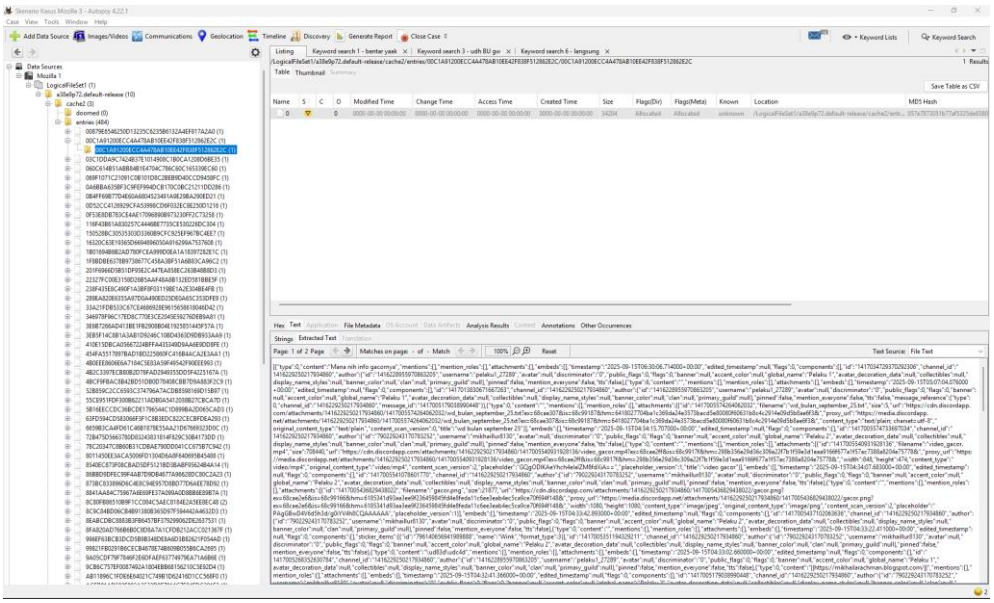
Nilai hash yang dihasilkan dari masing-masing file image, baik pada Google Chrome, Mozilla Firefox, maupun Microsoft Edge, berfungsi sebagai penanda unik yang menjamin bahwa data tidak mengalami perubahan sejak pertama kali diakuisisi hingga dianalisis. Dengan demikian, penerapan hash tidak hanya berperan sebagai metode verifikasi teknis, tetapi juga memberikan legitimasi hukum karena dapat digunakan untuk membuktikan bahwa bukti digital yang dipresentasikan adalah autentik dan belum dimodifikasi. Artefak file yang berisi interaksi antara pengguna pada platform Discord terdapat pada file yang bernama ***50.json***

Tabel 4. 3 Nilai Hash File Image dari Browser Cache

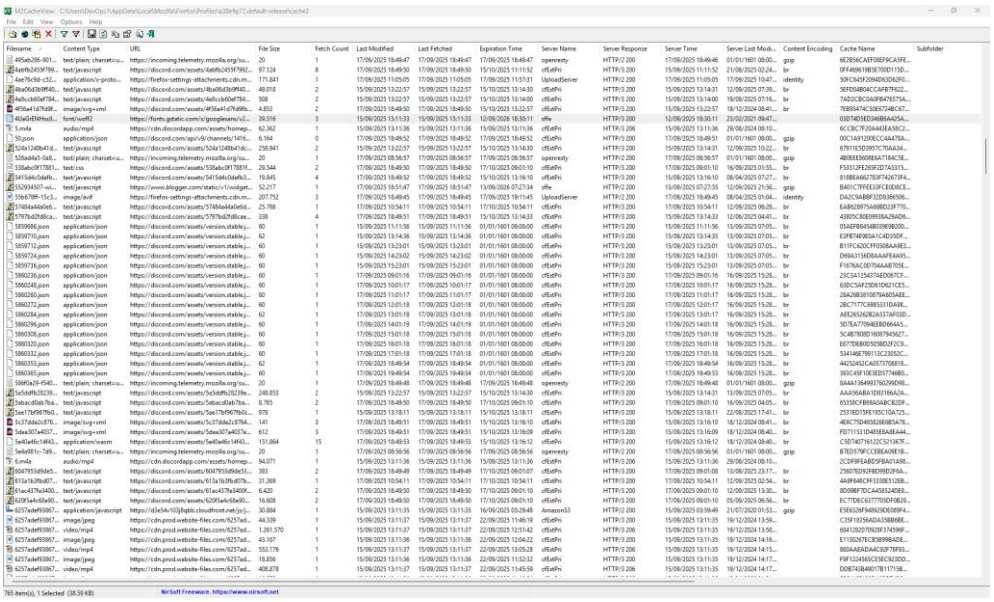
Image File	**MD5**	**SHA-256**
Google Chrome	13010c0b7c5ac8b4 0ab027b017ffe975	56f5b0ef768196c92486ac53926d794 464bd2850a4a48ac1c026abbc3ec73bc9
Mozilla Firefox	ef4c0cfcadb9f 522233d8d8ff45bd448	462dc3de5d65a40d7cf175d 06b3c02756fdf422fabd42a9e53473a182b423323
Microsoft Edge	7d5a7385bd0aa 956a39c86b7ab1353ca	662090f9687a5784c51fac71 72cf15fb6b06e906d3fbf264aa93dc10a6032fa2

4.1.3 Fase *Examination*

Fase ini berfokus pada proses identifikasi, ekstraksi, dan analisis awal terhadap artefak digital yang telah diperoleh dalam tahap sebelumnya. Pada fase ini, data yang terkumpul diperiksa secara sistematis guna memastikan integritas serta keaslian informasi yang diperoleh, sehingga dapat dipastikan bahwa bukti digital tetap valid dan tidak mengalami modifikasi yang tidak sah. Selain itu, pemeriksaan dilakukan dengan metode yang sesuai dengan standar forensik, termasuk penggunaan perangkat lunak maupun teknik analisis yang relevan Pemeriksaan dilakukan secara manual dengan menelusuri setiap file cache yang terdapat pada browser Mozilla Firefox. Pada Mozilla Firefox, ditemukan sebanyak 484 file cache yang tersimpan di dalam folder *\cache2\entries*. File-file tersebut berisi jejak digital aktivitas pengguna yang diakses melalui browser yang diakuisisi dengan Autopsy, sebagaimana ditunjukkan pada Gambar 4.4 , dan juga jejak digital yang diakuisis dengan MZCacheView yang ditunjukkan pada Gambar 4.5

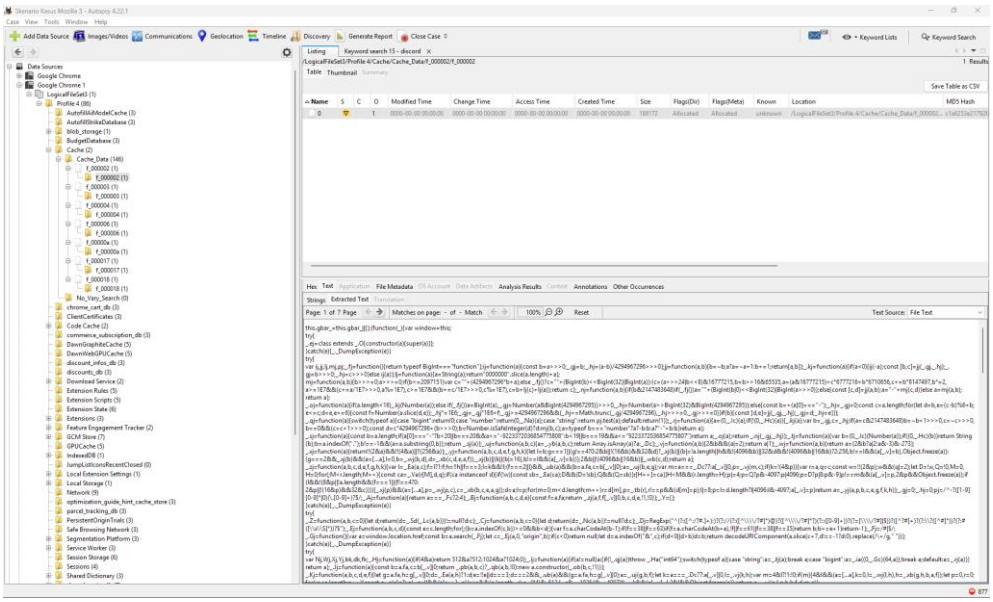


Gambar 4. 4 File Cache Mozilla Firefox dengan Autopsy

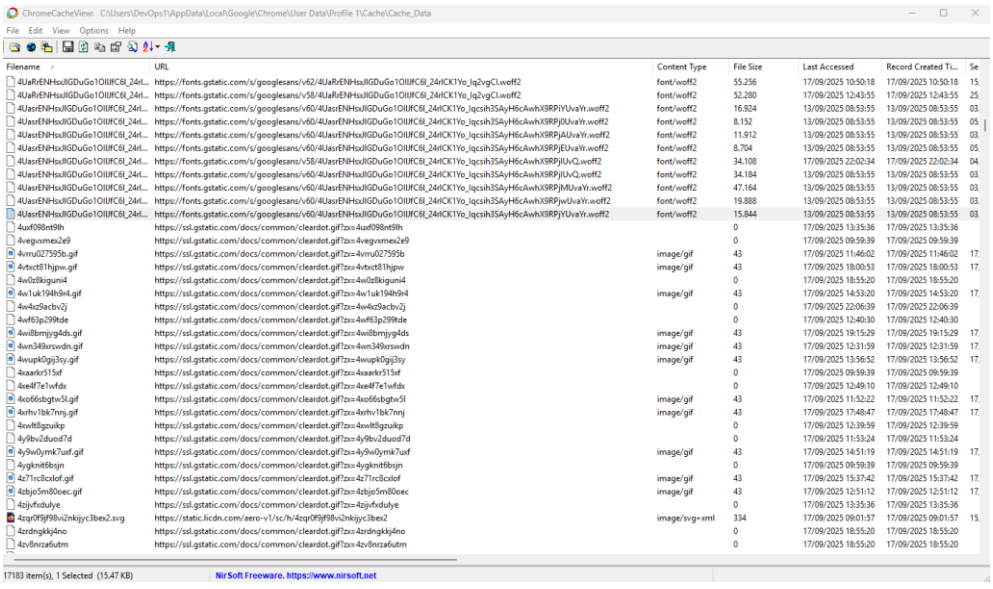


Gambar 4. 5 File Cache Mozilla Firefox dengan MZCacheView

Pada Google Chrome, ditemukan sebanyak 146 file cache yang tersimpan di dalam folder *Cache\Cache_Data*. File-file tersebut berisi jejak digital aktivitas pengguna yang diakses melalui browser yang diakuisisi dengan Autopsy, sebagaimana ditunjukkan pada Gambar 4.6 , dan juga jejak digital yang diakuisis dengan ChromeCacheView yang ditunjukkan pada Gambar 4.7.

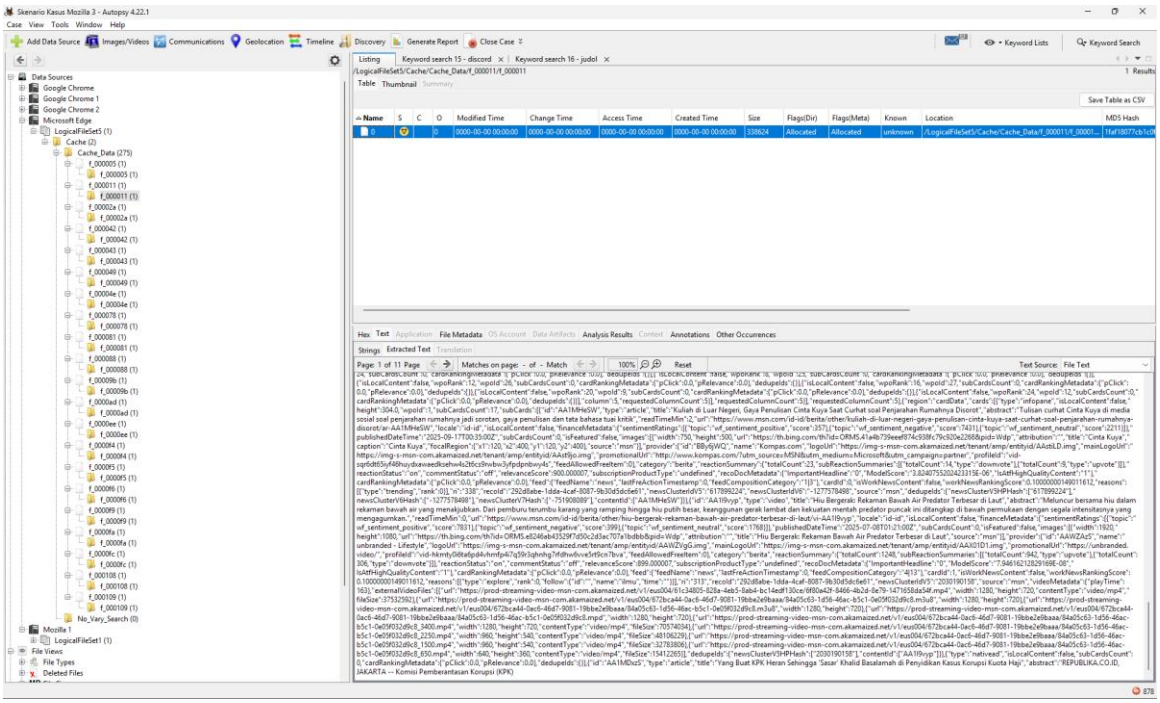


Gambar 4. 6 File Cache Google Chrome dengan Autopsy

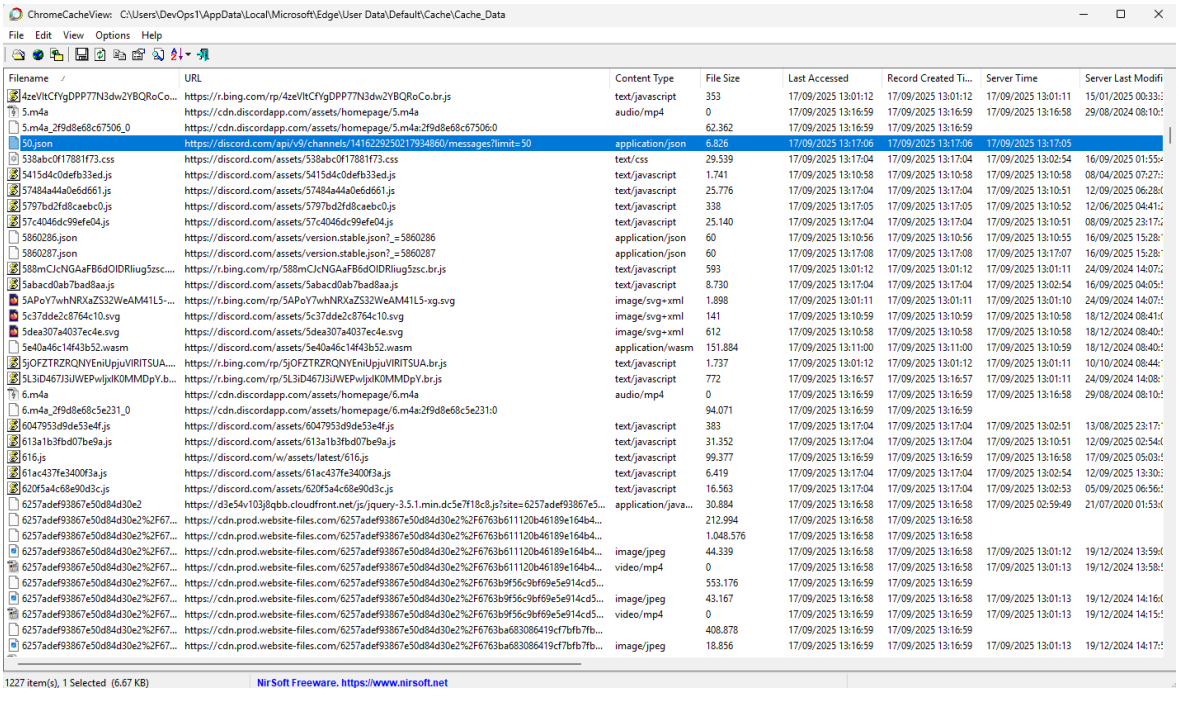


Gambar 4. 7 File Cache Google Chrome dengan ChromeCacheView

Pada Microsoft Edge, ditemukan sebanyak 275 file cache yang tersimpan di dalam folder *Cache\Cache_Data*. File-file tersebut berisi jejak digital aktivitas pengguna yang diakses melalui browser yang diakuisisi dengan Autopsy, sebagaimana ditunjukkan pada Gambar 4.8 , dan juga jejak digital yang diakuisis dengan ChromeCacheView yang ditunjukkan pada Gambar 4.9.



Gambar 4. 8 File Cache Microsoft Edge dengan Autopsy



Gambar 4. 9 File Cache Microsoft Edge dengan ChromeCacheView

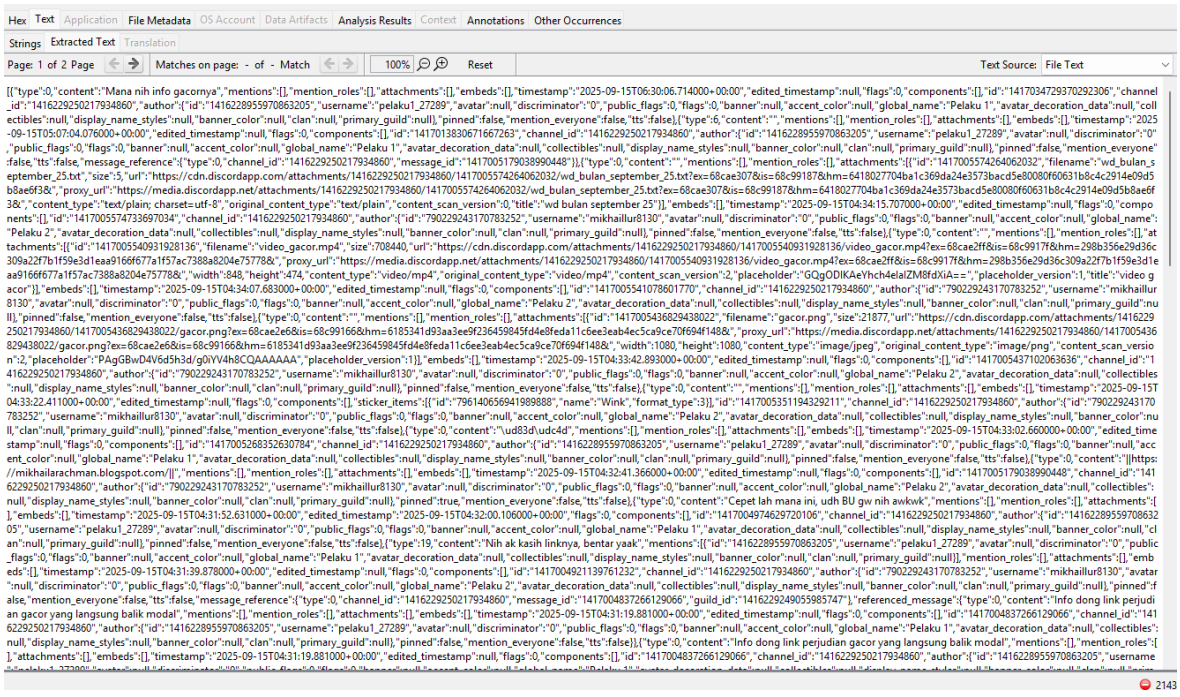
4.1.4 Fase *Analysis*

Dalam proses penelitian forensik digital ini pada platform Discord berbasis website, artefak utama yang menjadi fokus pemeriksaan meliputi pesan, username, waktu, dan detail percakapan. Pesan dapat berupa teks maupun gambar/foto yang dikirimkan oleh pengguna,

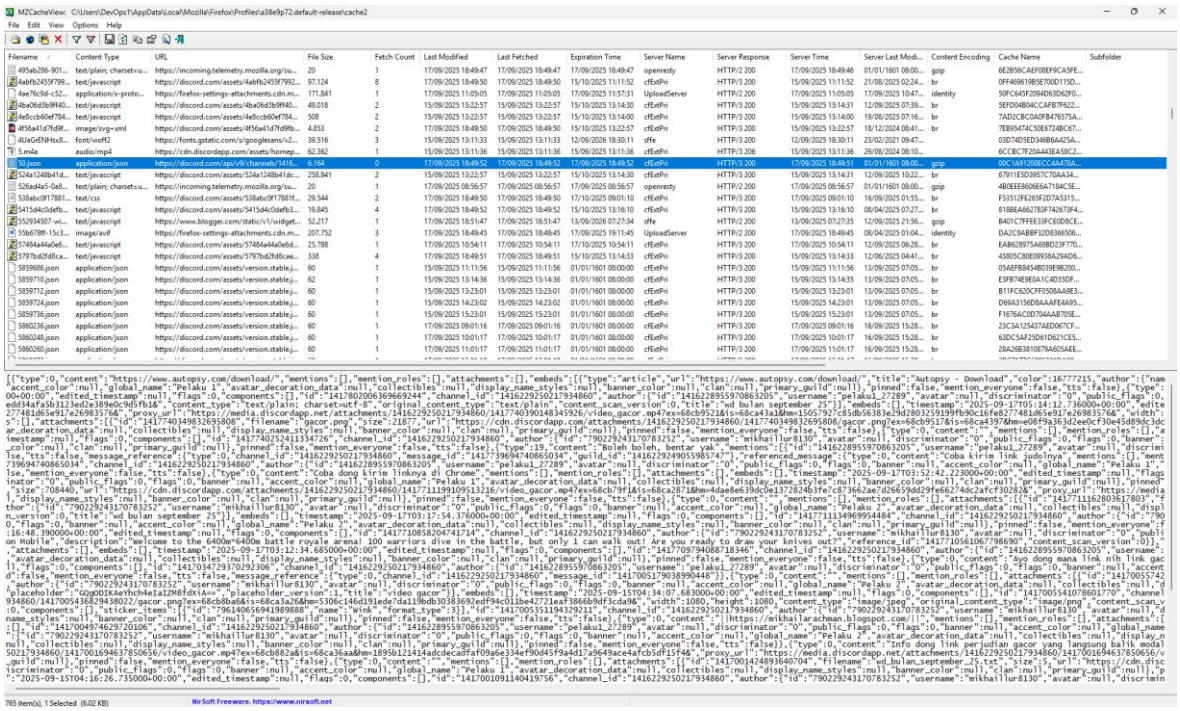
sedangkan username berfungsi untuk mengidentifikasi pihak yang terlibat dalam komunikasi. Informasi waktu atau timestamp menjadi elemen penting untuk merekonstruksi kronologi percakapan secara akurat. Selain itu, setiap baris percakapan juga mengandung informasi detail seperti ID, tipe data, isi pesan, serta channel_id yang menunjukkan lokasi spesifik interaksi tersebut terjadi. Keempat komponen ini menjadi bagian fundamental dalam memastikan integritas data serta mendukung analisis pada platform Discord.

4.1.4.1 Mozilla Firefox

Pada browser Mozilla Firefox, ditemukan sebuah file cache dengan dalam folder dengan nama ***00C1A91200ECC4A478AB10EE42F838F512862E2C***, yang berisi percakapan antara pelaku pada platform Discord yang diakses pada browser Mozilla Firefox yang diakuisis dengan Autopsy yang dapat dilihat pada gambar 4.10, dan juga dengan MZCacheView pada gambar 4.11 dengan nama file ***50.json***



Gambar 4. 10 Artefak Recovery dengan Autopsy



Gambar 4. 11 Artefak Recovery dengan MZCacheView

Hasil temuan artefak juga memperlihatkan interaksi antar pelaku seperti mengirim pesan teks, menggunakan emoji dan stiker, serta mengirim media, seperti gambar, video, dan video.

1. **Mengirim Text Message**

Gambar 4.12 dan 4.13 menunjukkan cuplikan berkas cache dengan artefak yang berkaitan dengan pengiriman pesan teks. Di sini, kita dapat melihat dengan jelas pesan yang dikirim, penulis pesan, ID kanal tempat pesan tersebut dikirim, dan *timestamp* pesan. Ini berarti penyelidik dapat mengungkap pesan tersebut, siapa pengirimnya, ke mana pesan tersebut dikirim, dan kapan pesan tersebut dikirim.

Gambar 4. 12 Text Message Hasil Recovery dengan Autopsy

Gambar 4. 13 Text Message Recovery dengan dengan MZCacheView

Jika pesan telah disematkan (pinned message), maka properti yang disematkan akan menjadi "***true***," seperti yang ditunjukkan pada Gambar 4.14 dan Gambar 4.15

Gambar 4. 14 Pinned Message Recovery dengan Autopsy

Gambar 4. 15 Pinned Message Recovery dengan MZCacheView

Demikian pula, jika pesan diubah (*edited*), maka *timestamp* yang diedit akan ditampilkan di berkas cache dengan waktu pesan diperbarui, seperti yang ditunjukkan pada Gambar 4.16 dan Gambar 4.17

Gambar 4. 16 Edited Message Recovery dengan Autopsy

Gambar 4. 17 Edited Message Recovery dengan MZCacheView

Discord memungkinkan penggunanya untuk mengirim pesan spoiler (pesan tersembunyi). Tag spoiler digunakan untuk mengirim pesan tersembunyi kepada pengguna. Tag spoiler dapat dikenali dengan dua garis vertikal (||) sebelum dan sesudah pesan spoiler, seperti yang ditunjukkan pada Gambar 4.18 dan Gambar 4.19

Gambar 4. 18 Spoiler Message Recovery dengan Autopsy

Gambar 4. 19 Spoiler Message Recovery dengan MZCacheView

Terakhir, artefak balasan pesan juga ditemukan dalam cache. Beberapa artefak penting meliputi referensi pesan (pesan yang dibalas), *timestamp*, dan konten balasan yang

berkaitan dengan balasan pesan, seperti yang ditunjukkan pada Gambar 4.20 dan Gambar 4.21

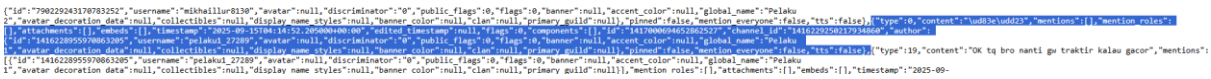
Gambar 4. 20 Reply Message Recovery dengan Autopsy

Gambar 4. 21 Reply Message Recovery dengan dengan MZCacheView

2. Menggunakan Emoji dan Sticker

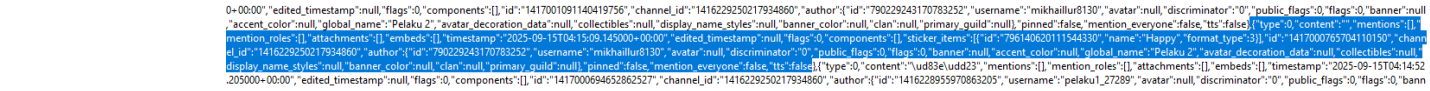
Penggunaan emoji dan stiker dapat mengungkapkan banyak informasi psikologis tentang seseorang. Selain itu, suasana hati pengguna selama percakapan juga dapat disimpulkan melalui emoji sehingga menjadi sumber intelijen yang vital selama investigasi forensik. Gambar 4.22 dan Gambar 4.23 menunjukkan artefak utama meliputi emoji dan *timestamp* penggunaannya. Serupa dengan bagaimana reaksi emoji terhadap pesan digambarkan dalam karakter Unicode yang dikodekan JSON, penggunaan emoji akan memasukkan nama emoji yang digunakan dalam format yang sama pada kalimat "content ", yang berupa *\ud83e\udd23*, dengan merujuk pada emoji " 🤣 " atau *"ROLLING ON THE FLOOR LAUGHING"*

Gambar 4. 22 Penggunaan *Emoji* Recovery dengan Autopsy



Gambar 4. 23 Penggunaan *Emoji* Recovery dengan MZCacheView

Discord memiliki paket stikernya sendiri yang dapat digunakan pengguna, yang disimpan dalam cache. Gambar 4.24 dan Gambar 4.25 menunjukkan semua artefak yang dipulihkan dar berkas cache terkait penggunaan stiker. Artefak tersebut meliputi ID dan nama stiker "Happy", yang dapat digunakan untuk mencari lebih lanjut jenis stiker menggunakan informasi paket stiker yang tersimpan dalam cache.

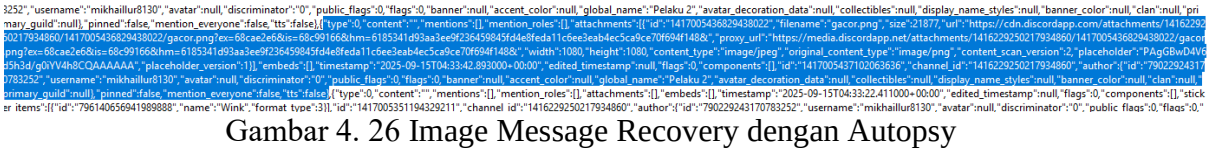


Gambar 4. 24 Penggunaan *Sticker* Recovery dengan dengan Autopsy

Gambar 4. 25 Penggunaan *Sticker* Recovery dengan MZCacheView

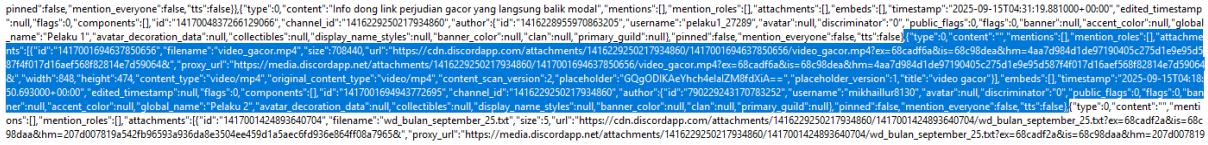
3. Mengirim Media File

Mengirim lampiran merupakan fungsi umum aplikasi media sosial, yang sering digunakan pengguna untuk mengirimkan media digital kepada pengguna lain. Artefak tentang penggunaan media dapat menghasilkan banyak informasi bermanfaat untuk investigasi forensik. Gambar 4.26 – Gambar 4.31 menunjukkan file cache dengan artefak yang terkait dengan penggunaan media saat berinteraksi dengan sesama dengan juga mencakup ID dan tinggi lebar untuk gambar dan video.



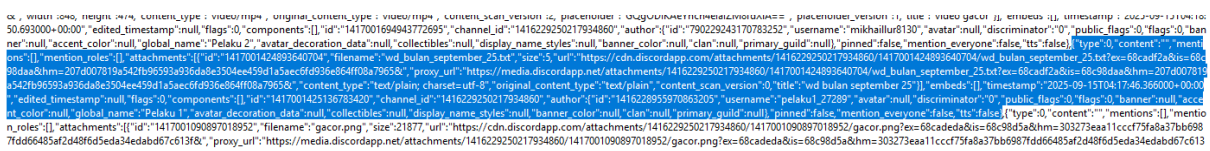
Gambar 4. 26 Image Message Recovery dengan Autopsy

Gambar 4. 27 Image Message Recovery dengan MZCacheView



Gambar 4. 28 Video Message Recovery dengan Autopsy

Gambar 4. 29 Video Message Recovery dengan dengan MZCacheView

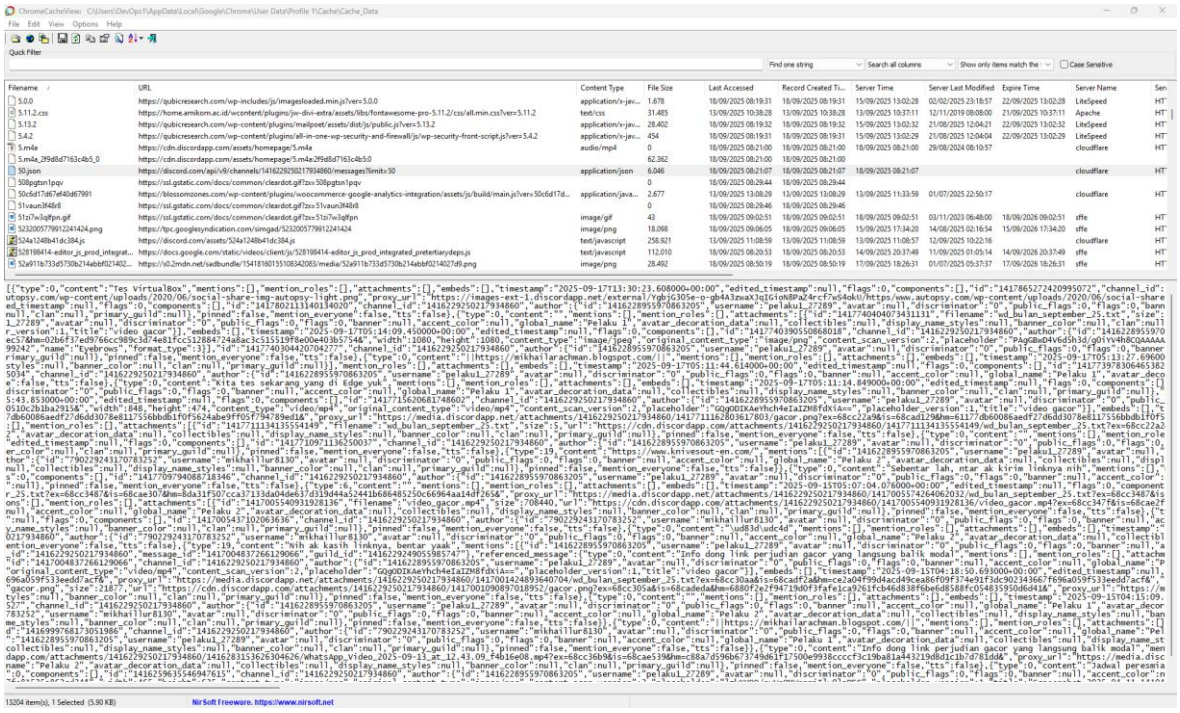


Gambar 4. 30 Document Message Recovery dengan Autopsy

Gambar 4. 31 Document Message Recovery dengan MZCacheView

4.1.4.2 Google Chrome

Dalam penelitian ini, artefak interaksi pada platform Discord yang diakses melalui web tidak selalu dapat ditemukan secara konsisten pada setiap browser. Pada Mozilla Firefox, artefak tersebut berhasil diekstraksi dengan menggunakan tools Autopsy dan MZCacheView. Namun, pada Google Chrome, artefak tidak teridentifikasi melalui Autopsy, melainkan baru dapat ditemukan dengan memanfaatkan tools ChromeCacheView. Temuan ini menunjukkan adanya perbedaan mekanisme penyimpanan cache dan manajemen data pada masing-masing browser, sehingga pemilihan tools yang tepat menjadi faktor penting dalam keberhasilan proses akuisisi dan analisis artefak digital. Artefak file yang berisi interaksi antara pengguna pada platform Discord terdapat pada file yang bernama ***50.json*** yang berhasil diakuisisi dengan tools ChromeCacheView.



Gambar 4. 32 Artefak Recovery dengan ChromeCacheView pada Google Chrome

1. Mengirim Text Message

Gambar 4.33 menunjukkan cuplikan berkas cache dengan artefak yang berkaitan dengan pengiriman pesan teks. Di sini, kita dapat melihat dengan jelas pesan yang dikirim, penulis pesan, ID kanal tempat pesan tersebut dikirim, dan *timestamp* pesan. Ini berarti

penyelidik dapat mengungkap pesan tersebut, siapa pengirimnya, ke mana pesan tersebut dikirim, dan kapan pesan tersebut dikirim.

Gambar 4. 33 Text Message Recovery dengan dengan ChromeCacheView

Jika pesan telah disematkan (pinned message), maka properti yang disematkan akan menjadi "***true***," seperti yang ditunjukkan pada Gambar 4.34

Gambar 4. 34 Pinned Message Recovery dengan ChromeCacheView

Demikian pula, jika pesan diedit, maka *timestamp* yang diedit akan ditampilkan di berkas cache dengan waktu pesan diperbarui, seperti yang ditunjukkan pada Gambar 4.35

Gambar 4. 35 Edited Message Recovery dengan ChromeCacheView

Discord memungkinkan penggunanya untuk mengirim pesan spoiler (pesan tersembunyi). Tag spoiler digunakan untuk mengirim pesan tersembunyi kepada pengguna. Tag spoiler dapat dikenali dengan dua garis vertikal (||) sebelum dan sesudah pesan spoiler, seperti yang ditunjukkan pada Gambar 4.36

Gambar 4. 36 Spoiler Message Recovery dengan ChromeCacheView

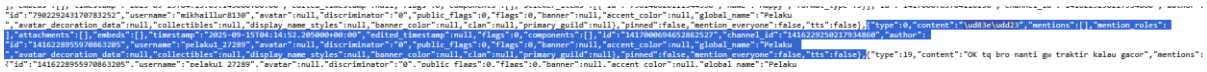
Terakhir, artefak balasan pesan juga ditemukan dalam cache. Beberapa artefak penting meliputi referensi pesan (pesan yang dibalas), *timestamp*, dan konten balasan yang berkaitan dengan balasan pesan, seperti yang ditunjukkan pada Gambar 4.37

Gambar 4. 37 Reply Message Recovery dengan ChromeCacheView

2. Menggunakan Emoji dan Sticker

Penggunaan emoji dan stiker dapat mengungkapkan banyak informasi psikologis tentang seseorang. Selain itu, suasana hati pengguna selama percakapan juga dapat disimpulkan melalui emoji sehingga menjadi sumber intelijen yang vital selama investigasi

forensik. Gambar 4.38 menunjukkan artefak utama meliputi emoji dan *timestamp* penggunaannya. Serupa dengan bagaimana reaksi emoji terhadap pesan digambarkan dalam karakter Unicode yang dikodekan JSON, penggunaan emoji akan memasukkan nama emoji yang digunakan dalam format yang sama pada kalimat "content ", yang berupa *\ud83e\udd23*, dengan merujuk pada emoji "🤣" atau *"ROLLING ON THE FLOOR LAUGHING"*.



Gambar 4. 38 Penggunaan *Emoji* Recovery dengan ChromeCacheView

Discord memiliki paket stikernya sendiri yang dapat digunakan pengguna, yang disimpan dalam cache. Gambar 4.39 menunjukkan semua artefak yang dipulihkan dar berkas cache terkait penggunaan stiker. Artefak tersebut meliputi ID dan nama stiker "*Happy*", yang dapat digunakan untuk mencari lebih lanjut jenis stiker menggunakan informasi paket stiker yang tersimpan dalam cache.

Gambar 4. 39 Penggunaan *Sticker* Recovery dengan ChromeCacheView

3. Mengirim Media File

Mengirim lampiran media merupakan fungsi umum aplikasi media sosial, yang sering digunakan pengguna untuk mengirimkan media digital kepada penggunalain. Artefak tentang penggunaan media dapat menghasilkan banyak informasi bermanfaat untuk investigasi forensik. Gambar 4.40 – Gambar 4.42 menunjukkan file cache dengan artefak yang terkait dengan penggunaan media saat berinteraksi dengan sesama dengan juga mencakup ID dan tinggi lebar untuk gambar dan video.

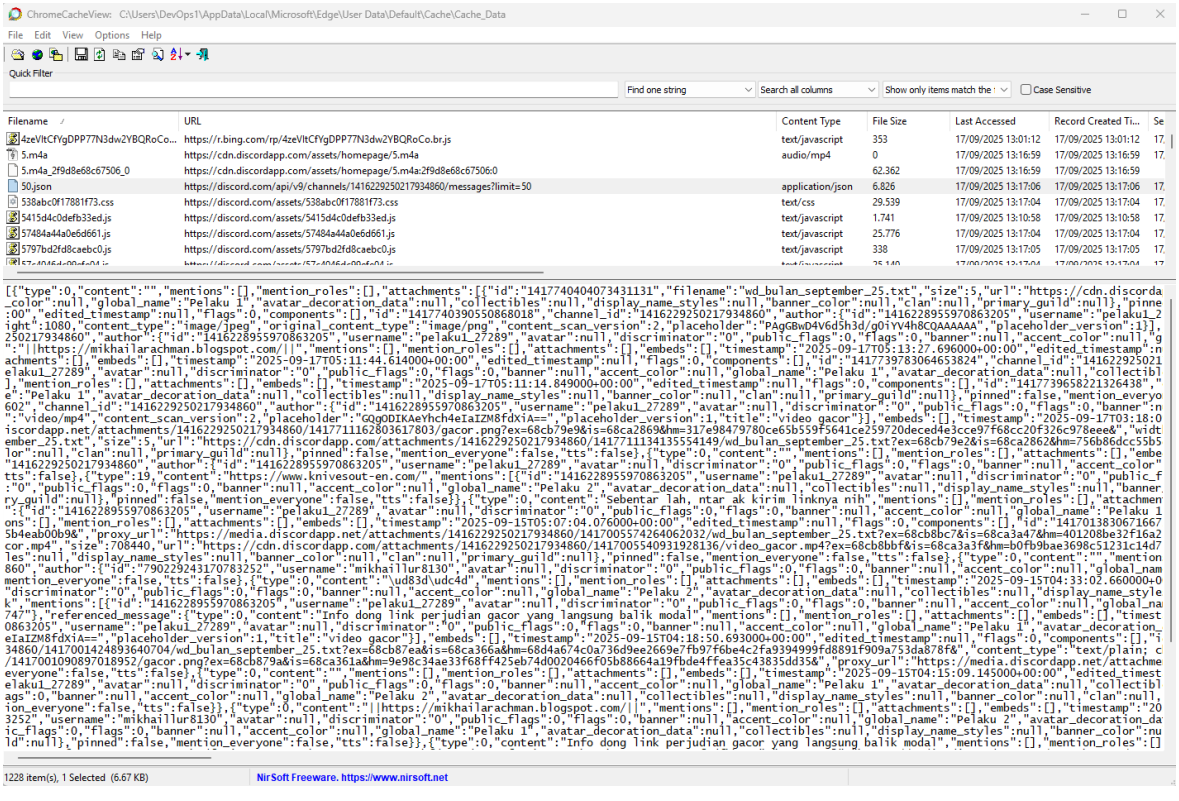
Gambar 4. 40 Image Message Recovery dengan ChromeCacheView

Gambar 4. 41 Video Message Recovery dengan ChromeCacheView

Gambar 4. 42 Document Message Recovery dengan ChromeCacheView

4.1.4.3 Microsoft Edge

Pada pemeriksaan artefak digital yang diakses melalui peramban Microsoft Edge, penelitian ini tidak berhasil menemukan artefak interaksi Discord dengan menggunakan *tools* Autopsy. Namun penggunaan *tools* ChromeCacheView juga dapat diterapkan pada Microsoft Edge karena hal ini dimungkinkan karena Chrome dan Edge sama-sama berbasis *Chromium engine*, sehingga struktur dan mekanisme penyimpanan cache yang digunakan keduanya serupa. Oleh karena itu, ChromeCacheView dapat diaplikasikan secara efektif tidak hanya pada Google Chrome, tetapi juga pada Microsoft Edge untuk mengekstraksi artefak digital yang tersimpan dalam file cache. Artefak file yang berisi interaksi antara pengguna pada platform Discord terdapat pada file yang bernama ***50.json*** yang berhasil diakuisisi dengan tools ChromeCacheView.



Gambar 4. 43 Artefak Recovery dengan ChromeCacheView pada Microsoft Edge

1. Mengirim Text Message

Gambar 4.44 menunjukkan cuplikan berkas cache dengan artefak yang berkaitan dengan pengiriman pesan teks. Di sini, kita dapat melihat dengan jelas pesan yang dikirim,

penulis pesan, ID kanal tempat pesan tersebut dikirim, dan *timestamp* pesan. Ini berarti penyelidik dapat mengungkap pesan tersebut, siapa pengirimnya, ke mana pesan tersebut dikirim, dan kapan pesan tersebut dikirim.

Gambar 4. 44 Text Message Recovery dengan ChromeCacheView

Jika pesan telah disematkan (pinned message), maka properti yang disematkan akan menjadi "***true***," seperti yang ditunjukkan pada Gambar 4.45

Gambar 4. 45 Pinned Message Recovery dengan ChromeCacheView

Demikian pula, jika pesan diedit, maka *timestamp* yang diedit akan ditampilkan di berkas cache dengan waktu pesan diperbarui, seperti yang ditunjukkan pada Gambar 4.46

Gambar 4. 46 Edited Message Recovery dengan ChromeCacheView

Discord memungkinkan penggunanya untuk mengirim pesan spoiler (pesan tersembunyi). Tag spoiler digunakan untuk mengirim pesan tersembunyi kepada pengguna. Tag spoiler dapat dikenali dengan dua garis vertikal (||) sebelum dan sesudah pesan spoiler, seperti yang ditunjukkan pada Gambar 4.47

Gambar 4. 47 Spoiler Message Recovery dengan ChromeCacheView

Terakhir, artefak balasan pesan juga ditemukan dalam cache. Beberapa artefak penting meliputi referensi pesan (pesan yang dibalas), *timestamp*, dan konten balasan yang berkaitan dengan balasan pesan, seperti yang ditunjukkan pada Gambar 4.48

Gambar 4. 48 Reply Message Recovery dengan ChromeCacheView

2. Menggunakan Emoji dan Sticker

Penggunaan emoji dan stiker dapat mengungkapkan banyak informasi psikologis tentang seseorang. Selain itu, suasana hati pengguna selama percakapan juga dapat disimpulkan melalui emoji sehingga menjadi sumber intelijen yang vital selama investigasi

forensik. Gambar 4.49 menunjukkan artefak utama meliputi emoji dan *timestamp* penggunaannya. Serupa dengan bagaimana reaksi emoji terhadap pesan digambarkan dalam karakter Unicode yang dikodekan JSON, penggunaan emoji akan memasukkan nama emoji yang digunakan dalam format yang sama pada kalimat "content ", yang berupa *\ud83e\udd23*, dengan merujuk pada emoji "🤣" atau *"ROLLING ON THE FLOOR LAUGHING"*.

Gambar 4. 49 Penggunaan *Emoji* Recovery dengan ChromeCacheView

Discord memiliki paket stikernya sendiri yang dapat digunakan pengguna, yang disimpan dalam cache. Gambar 4.50 menunjukkan semua artefak yang dipulihkan dar berkas cache terkait penggunaan stiker. Artefak tersebut meliputi ID dan nama stiker "*Happy*", yang dapat digunakan untuk mencari lebih lanjut jenis stiker menggunakan informasi paket stiker yang tersimpan dalam cache.

Gambar 4. 50 Penggunaan *Sticker* Recovery dengan ChromeCacheView

3. Mengirim Media File

Mengirim lampiran media merupakan fungsi umum aplikasi media sosial, yang sering digunakan pengguna untuk mengirimkan media digital kepada penggunalain. Artefak tentang penggunaan media dapat menghasilkan banyak informasi bermanfaat untuk investigasi forensik. Gambar 4.51 – Gambar 4.53 menunjukkan file cache dengan artefak yang terkait dengan penggunaan media saat berinteraksi dengan sesama dengan juga mencakup ID dan tinggi lebar untuk gambar dan video.

Gambar 4. 51 Image Message Recovery dengan ChromeCacheView

Gambar 4. 52 Video Message Recovery dengan ChromeCacheView

Gambar 4. 53 Document Message Recovery dengan ChromeCacheView

Untuk mengetahui tingkat keberhasilan masing-masing tools forensik dalam mengekstraksi artefak Discord dari cache browser, penelitian ini menggunakan metode pengukuran berbasis persentase keberhasilan. Berdasarkan hasil identifikasi dan akuisisi artefak menggunakan alat forensik, dilakukan analisis komparatif mengenai efektivitas pemulihan di berbagai browser. Tabel 4.4 merangkum tingkat keberhasilan pemulihan artefak digital di Mozilla Firefox, Google Chrome, dan Microsoft Edge. Tingkat keberhasilan dihitung menggunakan persamaan:

$$n = \frac{x}{y} \times 100\%$$

di mana $\boldsymbol{x}$ merepresentasikan jumlah bukti digital yang berhasil diekstraksi/dipulihkan dari artefak Discord, sedangkan $\boldsymbol{y}$ menyatakan total jumlah bukti digital yang seharusnya (artefak yang seharusnya teridentifikasi). Hasil perhitungan ini kemudian dinyatakan dalam bentuk persentase untuk memberikan gambaran kuantitatif mengenai efektivitas setiap tools forensik.

Tabel 4. 4 Perolehan Bukti Digital pada Browser

Browser	**Artefak yang teridentifikasi**	**Artefak yang berhasil dipulihkan**	**Artefak yang berhasil dipulihkan parsial**
Mozilla Firefox	Username, Message, Channel ID, Timestamp, Media	Username, Message, Timestamp, Channel ID, Media (image, document)	Media (Video)
Google Chrome	Username, Message, Channel ID, Timestamp, Media	Username, Message, Timestamp, Channel ID, Media (image, document)	Media (Video)
Microsoft Edge	Username, Message, Channel ID,Timestamp, Media	Username, Message, Channel ID, Timestamp, Media (image, document)	Media (Video)

Keterangan:

• Berhasil dipulihkan menunjukkan artefak yang diekstrak dengan konten lengkap dan dapat dibaca.

• Berhasil sebagian / parsial dipulihkan dipulihkan menunjukkan artefak yang terdeteksi tetapi tidak lengkap, terfragmentasi, atau tidak memiliki metadata kontekstual.

Tabel 4. 5 Perolehan Bukti Digital pada Mozilla Firefox

Artefak yang berhasil dipulihkan	**Autopsy**	**Chrome Cache View**	**MZ Cache View**
Username	✓	-	✓
Message	✓	-	✓
Server Channel ID	✓	-	✓
Timestamp	✓	-	✓
Media (Gambar)	✓	-	✓
Media (Video)	✓	-	✓
Media (Dokumen)	✓	-	✓
X	7	0	7
Y	7	7	7
N	100%	0%	100%

Berdasarkan Tabel 4.5, hasil perolehan bukti digital pada browser Mozilla Firefox menunjukkan bahwa tools **Autopsy** dan **MZCacheView** berhasil memulihkan seluruh jenis artefak yang dianalisis dalam penelitian ini. Artefak yang berhasil diperoleh meliputi **username, message, server channel ID, timestamp, serta media berupa gambar, video, dan dokumen** yang tersimpan dalam cache browser. Kedua tools tersebut menunjukkan hasil yang konsisten dengan jumlah artefak berhasil ditemukan sebanyak **7 dari 7 parameter**, sehingga menghasilkan tingkat keberhasilan sebesar **100%**. Sebaliknya, tools **ChromeCacheView** tidak berhasil memperoleh artefak pada browser Mozilla Firefox, sehingga menghasilkan tingkat keberhasilan **0%**. Hal ini disebabkan karena ChromeCacheView dirancang untuk membaca struktur cache pada browser berbasis **Chromium**, sementara Mozilla Firefox menggunakan mekanisme penyimpanan cache yang berbeda. Dengan demikian, hasil ini menunjukkan bahwa proses akuisisi artefak pada Mozilla Firefox lebih efektif dilakukan menggunakan tools yang mendukung struktur cache Firefox seperti Autopsy dan MZCacheView.

Tabel 4. 6 Perolehan Bukti Digital pada Google Chrome

Artefak yang berhasil dipulihkan	Autopsy	Chrome Cache View	MZ Cache View
Username	-	✓	-
Message	-	✓	-
Server Channel ID	-	✓	-
Timestamp	-	✓	-
Media (Gambar)	-	✓	-
Media (Video)	-	✓	-
Media (Dokumen)	-	✓	-
X	0	7	0
Y	7	7	7
N	0%	100%	0%

Tabel 4. 7 Perolehan Bukti Digital pada Microsoft Edge

Artefak yang berhasil dipulihkan	Autopsy	Chrome Cache View	MZ Cache View
Username	-	✓	-
Message	-	✓	-
Server Channel ID	-	✓	-
Timestamp	-	✓	-
Media (Gambar)	-	✓	-
Media (Video)	-	✓	-
Media (Dokumen)	-	✓	-
X	0	7	0
Y	7	7	7
N	0%	100%	0%

Berdasarkan Tabel 4.6, hasil perolehan bukti digital pada browser **Google Chrome** menunjukkan bahwa artefak digital berhasil dipulihkan menggunakan tools **ChromeCacheView**. Artefak yang berhasil diperoleh meliputi **username, message, server channel ID, timestamp, serta media berupa gambar, video, dan dokumen** yang tersimpan dalam cache browser. ChromeCacheView berhasil menemukan seluruh parameter artefak yang dianalisis dengan jumlah **7 dari 7 artefak** sehingga memperoleh tingkat keberhasilan **100%**. Sementara itu, tools **Autopsy** dan **MZCacheView** tidak berhasil memulihkan artefak pada browser Google Chrome sehingga menghasilkan tingkat keberhasilan **0%**. Hasil ini juga relevan dengan browser **Microsoft Edge** pada Tabel 4.7, karena Edge menggunakan engine **Chromium** yang sama dengan Google Chrome. Oleh karena itu, struktur penyimpanan cache pada kedua browser tersebut memiliki kesamaan,

sehingga proses pemulihan artefak digital juga lebih efektif dilakukan menggunakan **ChromeCacheView**.

Hasil ekstraksi artefak menggunakan MZCacheView dan Autopsy menunjukkan temuan data yang relatif sama. Hal ini dapat terjadi karena kedua tools tersebut melakukan proses analisis terhadap sumber data yang sama, yaitu file cache yang tersimpan pada direktori browser. MZCacheView dirancang secara khusus untuk membaca dan menampilkan isi cache browser Mozilla Firefox, sedangkan Autopsy merupakan platform digital forensik yang mampu melakukan analisis file sistem dan mengekstraksi artefak dari berbagai sumber data termasuk cache browser. Karena kedua tools mengakses file cache yang sama, artefak seperti pesan teks, metadata, atau file media yang tersimpan di dalam cache dapat teridentifikasi oleh keduanya. Perbedaan utama antara kedua tools tersebut lebih terletak pada metode penyajian data dan fitur analisis tambahan yang dimiliki oleh Autopsy sebagai platform forensik yang lebih komprehensif. Temuan ini menunjukkan bahwa penggunaan tools yang berbeda tidak selalu menghasilkan artefak yang berbeda, terutama ketika sumber data yang dianalisis berasal dari struktur penyimpanan yang sama. Oleh karena itu, pemilihan tools dalam investigasi digital forensik dapat disesuaikan dengan kebutuhan analisis tanpa mempengaruhi keberadaan artefak yang dapat dipulihkan.

Perbedaan ini mengindikasikan bahwa efektivitas tools forensik sangat dipengaruhi oleh kompatibilitas tools dengan mekanisme penyimpanan cache pada masing-masing browser. ChromeCacheView cenderung lebih optimal pada browser berbasis Chromium, yaitu Google Chrome dan Microsoft Edge, sementara Autopsy dan MZCacheView lebih efektif pada Mozilla Firefox yang memiliki struktur cache berbeda. Dengan demikian, hasil pengukuran ini menegaskan bahwa tidak terdapat satu tools yang unggul secara universal pada seluruh browser, melainkan diperlukan pemilihan tools yang sesuai dengan karakteristik browser yang dianalisis untuk memperoleh hasil pemulihan artefak yang optimal.

4.1.5 Fase *Reporting*

Fase *Reporting* dalam proses investigasi forensik digital merupakan tahap akhir yang berfokus pada penyusunan laporan hasil pemeriksaan secara komprehensif, sistematis, dan dapat dipertanggungjawabkan. Pada tahap ini, seluruh temuan yang diperoleh dari fase sebelumnya, mulai dari identifikasi, akuisisi, pemeriksaan, hingga analisis, didokumentasikan secara rinci dengan mencantumkan metode yang digunakan, bukti yang ditemukan, serta interpretasi hasil analisis. Laporan yang dihasilkan harus disusun dengan bahasa yang jelas, obyektif, dan sesuai dengan kaidah ilmiah maupun hukum, sehingga dapat

dipahami oleh pihak-pihak yang berkepentingan, termasuk penegak hukum, penyidik, maupun pengadilan. Dengan demikian, fase *Reporting* tidak hanya menjadi media penyampaian informasi, tetapi juga berfungsi sebagai bentuk pertanggungjawaban ilmiah atas proses investigasi yang telah dilakukan.

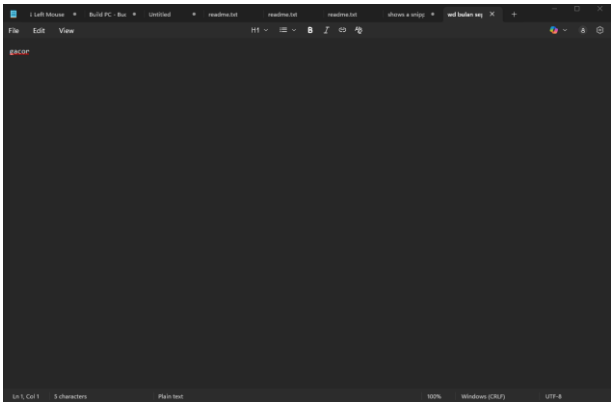
Tabel 4. 8 Nilai Hash File Image dari Browser Cache

Image File	**MD5**	**SHA-256**
Google Chrome	13010c0b7c5ac8b4 0ab027b017ffe975	56f5b0ef768196c92486ac53926d794 464bd2850a4a48ac1c026abbc3ec73bc9
Mozilla Firefox	ef4c0cfcadb9f 522233d8d8ff45bd448	462dc3de5d65a40d7cf175d 06b3c02756fdf422fabd42a9e53473a182b423323
Microsoft Edge	7d5a7385bd0aa 956a39c86b7ab1353ca	662090f9687a5784c51fac71 72cf15fb6b06e906d3fbf264aa93dc10a6032fa2

Pada fase *Reporting*, hasil perhitungan nilai hash dari file image browser cache yang ditampilkan pada Tabel 4.8 didokumentasikan sebagai bagian dari proses validasi integritas data. Nilai hash MD5 dan SHA-256 yang dihasilkan berfungsi untuk memastikan bahwa file image yang digunakan dalam penelitian tidak mengalami perubahan atau modifikasi selama proses akuisisi maupun analisis. Penyajian nilai hash ini juga memberikan bukti autentik yang dapat dipertanggungjawabkan secara ilmiah maupun hukum, sehingga meningkatkan keandalan temuan penelitian. Dengan demikian, dokumentasi nilai hash dalam laporan bukan hanya sekadar pelengkap, melainkan menjadi elemen penting untuk menjamin keaslian bukti digital yang diperoleh dari masing-masing browser.

Tabel 4. 9 Hasil Temuan Artefak Digital pada Browser Cache

Hasil Temuan	**Keterangan**
Username : pelaku1_27289 Global Name : Pelaku 1 ID : 1416228955970863205	Pengguna Discord 1
Username : mikhaillur8130 Global Name : Pelaku 2 ID : 790229243170783252	Pengguna Discord 2
Channel ID : 1416229250217934860	Server Discord untuk melakukan interaksi

Website Link : **https://mikhailarachman.blogspot.com/**	Website yang dikirim salah satu pengguna
Gambar dengan nama file : **gacor.png** 	Gambar yang dikirim pada 2025-09-17T05:13:59
Video dengan nama file : **video_gacor.mp4** 	Video yang dikirim pada 2025-09-17T05:14:09
Dokumen dengan nama file : **wd_bulan_september_25.txt** 	Dokumen yang dikirim pada 2025-09-17T03:17:54. File dengan format .txt yang berisi kata “gacor”

Hasil temuan artefak digital dari browser cache didokumentasikan secara rinci sebagaimana ditunjukkan pada Tabel 4.9. Temuan ini mencakup identitas pengguna Discord yang terlibat dalam percakapan, meliputi username, global name, serta ID yang melekat pada setiap akun. Selain itu, data juga memperlihatkan informasi *channel ID* yang digunakan sebagai media interaksi, tautan situs web yang dibagikan oleh pengguna, serta berbagai jenis media yang dikirim, seperti gambar, video, dan dokumen. Setiap artefak tidak hanya dicatat berdasarkan jenis dan nama file, tetapi juga disertai dengan keterangan waktu pengiriman untuk memperkuat konteks kronologis percakapan. Dokumentasi ini menjadi elemen

penting dalam laporan forensik karena memberikan gambaran menyeluruh mengenai aktivitas komunikasi yang terjadi, sekaligus mempertegas keterhubungan antarartefak yang ditemukan dengan subjek penelitian.

4.1.6 Fase *Presenting*

Hasil investigasi forensik digital dipaparkan secara jelas dan terstruktur dengan menekankan pada tiga aspek utama, yaitu tanggal dan waktu interaksi, penemuan bukti yang berharga, serta teknik khusus yang digunakan selama proses analisis. Penyajian informasi waktu yang tertera pada setiap artefak, seperti *timestamp* pengiriman pesan, gambar, maupun dokumen, memungkinkan penyusunan kronologi yang akurat atas aktivitas komunikasi yang terjadi. Bukti berharga yang ditemukan, antara lain berupa identitas pengguna, isi pesan, hingga media digital yang dikirimkan, dipaparkan sebagai temuan kunci yang mendukung validitas penelitian. Selain itu, teknik khusus yang digunakan, seperti penerapan *tools* forensik Autopsy, MZCacheView, dan ChromeCacheView, turut dijelaskan untuk menunjukkan metode analisis yang tepat sesuai dengan karakteristik masing-masing browser. Dengan demikian, fase *Presenting* tidak hanya menyajikan hasil temuan semata, tetapi juga memberikan gambaran utuh mengenai relevansi bukti, konteks kronologi, serta metode teknis yang mendukung keabsahan investigasi.

4.1.6.1 Tanggal dan Waktu Terjadi Interaksi

Dari **Hasil Temuan Artefak Digital pada Browser Cache**, tercatat beberapa *timestamp* pengiriman media, antara lain:

a. Gambar **gacor.png** dikirim pada **2025-09-17T05:13:59**

b. Video **video_gacor.mp4** dikirim pada **2025-09-17T05:14:09**

c. Dokumen **wd_bulan_september_25.txt** dikirim pada **2025-09-17T03:17:54**

4.1.6.2 Penemuan Bukti

Bukti digital yang berhasil ditemukan dalam penelitian ini meliputi:

1. **Identitas pengguna Discord**:
    a. Username: *pelaku1_27289 (Global Name: Pelaku 1, ID: 1416228955970863205)*
    b. Username: *mikhaillur8130 (Global Name: Pelaku 2, ID: 790229243170783252)*

2. **Channel ID**: *1416229250217934860*
3. **Website link**: *https://mikhailarachman.blogspot.com/*
4. **Media**: Gambar (*gacor.png*), Video (*video_gacor.mp4*), dan Dokumen (*wd_bulan_september_25.txt*).

4.1.6.3 Teknik yang Digunakan

Investigasi ini menggunakan pendekatan Enhanced GCFIM (Enhanced Generic Computer Forensic Investigation Model) dengan pengujian langsung melalui skenario kasus pada browser (Google Chrome, Mozilla Firefox, Microsoft Edge). Proses forensik dilakukan pada cache aktif browser untuk mengekstraksi artefak secara langsung menggunakan Autopsy, MZCacheView, dan ChromeCacheView dengan metode *Live Forensic*.

4.7 Fase *Post-Process*

Fase *Post-Process* dalam investigasi forensik digital ini merupakan tahap penutup setelah seluruh rangkaian investigasi selesai dilakukan, mulai dari akuisisi, pemeriksaan, analisis, hingga pelaporan dan penyajian hasil. Pada tahap ini, peneliti melakukan evaluasi terhadap efektivitas metode dan *tools* yang digunakan, seperti Autopsy, MZCacheView, dan ChromeCacheView, dalam mengekstraksi artefak dari cache browser Google Chrome, Mozilla Firefox, dan Microsoft Edge. Fase *post-process* juga mencakup kegiatan pengarsipan bukti digital, termasuk hasil perhitungan hash, artefak percakapan, serta dokumen pendukung lain, agar dapat dipertanggungjawabkan secara ilmiah maupun hukum di kemudian hari. Dengan adanya tahapan ini, seluruh proses investigasi tidak hanya menghasilkan temuan yang valid, tetapi juga memastikan bahwa data telah terjaga integritasnya, terdokumentasi dengan baik, dan siap untuk dijadikan rujukan pada penelitian selanjutnya maupun keperluan proses peradilan.

Tabel 4. 10 Potensi Temuan Artefak Digital pada Browser Cache

Artefak Digital	**Browser**		
	Mozilla Firefox	**Google Chrome**	**Microsoft Edge**
Username	✓	✓	✓
ID	✓	✓	✓
Server Channel ID	✓	✓	✓
Message	✓	✓	✓
Media	✓	✓	✓

Potensi temuan artefak digital dari browser cache dideskripsikan secara sistematis sebagaimana tercantum pada Tabel 4.10. Hasil pengujian menunjukkan bahwa Mozilla Firefox, Google Chrome, dan Microsoft Edge sama-sama berpotensi menyimpan artefak digital yang meliputi username, ID pengguna, server channel ID, pesan percakapan, serta media yang dikirimkan. Keseluruhan artefak ini menjadi indikator penting dalam mengungkap aktivitas komunikasi pada platform Discord, di mana setiap komponen memberikan kontribusi berbeda dalam memperkuat konteks analisis forensik. Dengan demikian, dokumentasi potensi artefak pada berbagai browser tidak hanya memperlihatkan variasi jejak digital yang dapat diperoleh, tetapi juga menegaskan perlunya pendekatan multi-*tools* untuk memastikan kelengkapan hasil investigasi.

Tabel 4. 11 Perolehan Artefak Digital dengan Tools Forensik

Browser	**Tools**		
	Autopsy	**MZCacheView**	**ChromeCacheView**
Mozilla Firefox	✓	✓	-
Google Chrome	-	-	✓
Microsoft Edge	-	-	✓

Hasil perolehan artefak digital dengan menggunakan berbagai *tools* forensik ditunjukkan pada Tabel 4.11. Berdasarkan tabel tersebut, Mozilla Firefox terbukti dapat diekstraksi dengan baik menggunakan Autopsy maupun MZCacheView, sedangkan Google Chrome dan Microsoft Edge tidak menghasilkan artefak melalui kedua *tools* tersebut. Namun demikian, artefak dari Chrome dan Edge berhasil diperoleh dengan menggunakan ChromeCacheView, yang kompatibel dengan struktur cache berbasis *Chromium engine*. Temuan ini menegaskan bahwa setiap browser memiliki perbedaan dalam mekanisme penyimpanan cache, sehingga keberhasilan ekstraksi artefak sangat dipengaruhi oleh kecocokan antara browser dan *tools* yang digunakan. Oleh karena itu, pemilihan *tools* yang tepat menjadi faktor penting untuk memastikan integritas serta kelengkapan data dalam proses investigasi forensik digital.

4.8 Percobaan dengan Device Berbeda

Untuk meningkatkan validitas dan konsistensi hasil penelitian, eksperimen tambahan dilakukan dengan menggunakan skenario yang sama seperti pada percobaan sebelumnya.

Percobaan ulang ini bertujuan untuk memastikan bahwa artefak digital yang ditemukan benar-benar berasal dari aktivitas penggunaan Discord Web dan dapat direproduksi pada kondisi eksperimen yang serupa. Tahapan eksperimen dilakukan dengan prosedur yang sama, yaitu melakukan aktivitas komunikasi pada platform Discord melalui browser, kemudian melakukan proses akuisisi serta analisis terhadap data cache yang tersimpan pada sistem browser menggunakan tools forensik yang telah ditentukan dalam penelitian ini.

Berdasarkan hasil percobaan ulang tersebut, artefak digital yang ditemukan menunjukkan karakteristik yang konsisten dengan hasil eksperimen sebelumnya. Artefak yang berhasil diperoleh masih mencakup data interaksi pengguna seperti informasi percakapan, identitas pengguna, serta elemen komunikasi lainnya yang tersimpan dalam file cache browser. Hal ini menunjukkan bahwa aktivitas yang dilakukan pada platform Discord Web memang menghasilkan jejak digital yang dapat dianalisis melalui proses investigasi forensik pada browser. Meskipun demikian, terdapat perbedaan pada lokasi file cache tempat artefak tersebut ditemukan. Pada percobaan sebelumnya, artefak ditemukan tersimpan dalam file **50.json**, sedangkan pada percobaan ulang artefak yang serupa ditemukan pada file **30.json**. Selain itu, hasil perhitungan nilai hash pada kedua file tersebut juga menunjukkan nilai yang berbeda. Perbedaan nilai hash ini menandakan bahwa meskipun kedua file mengandung artefak dengan jenis informasi yang sama, struktur data atau isi file secara keseluruhan tidak identik. Hal ini dapat terjadi karena adanya perbedaan waktu pembuatan cache, proses penambahan data baru oleh browser, maupun mekanisme pengelolaan cache yang bersifat dinamis.

Dengan demikian, perbedaan nomor file dan nilai hash tersebut menunjukkan bahwa mekanisme penyimpanan cache pada browser tidak bersifat statis. Penomoran file cache serta isi data yang tersimpan dapat berubah tergantung pada aktivitas pengguna dan proses manajemen cache oleh sistem browser. Namun demikian, jenis artefak digital yang dihasilkan tetap konsisten dan masih dapat diidentifikasi melalui proses analisis forensik. Temuan ini memperkuat bahwa artefak dari aktivitas Discord Web dapat direcover dari cache browser meskipun berada pada file yang berbeda serta memiliki nilai hash yang tidak sama pada setiap percobaan.

Tabel 4. 12 Hasil Akuisisi Artefak pada Mozilla Firefox

Temuan Artefak	Autopsy	MZCacheView	ChromeCacheView
Text Message	✓	✓	-
Username	✓	✓	-

ID	✓	✓	-
Server Channel ID	✓	✓	-
Text Message	✓	✓	-
Emoji dan Sticker	✓	✓	-
Media	✓	✓	-

Berdasarkan Tabel 4.9, pada percobaan tambahan yang dilakukan pada browser Mozilla Firefox, artefak digital seperti text message, username, ID, server channel ID, emoji dan sticker, serta media berhasil diperoleh melalui proses analisis cache browser. Hasil akuisisi menunjukkan bahwa Autopsy dan MZCacheView mampu menampilkan artefak tersebut, sehingga kedua tools tersebut efektif digunakan untuk melakukan analisis artefak Discord Web pada Mozilla Firefox.

Tabel 4. 13 Hasil Akuisisi Artefak pada Google Chrome

Temuan Artefak	Autopsy	MZCacheView	ChromeCacheView
Text Message	-	-	✓
Username	-	-	✓
ID	-	-	✓
Server Channel ID	-	-	✓
Text Message	-	-	✓
Emoji dan Sticker	-	-	✓
Media	-	-	✓

Tabel 4. 14 Hasil Akuisisi Artefak pada Microsoft Edge

Temuan Artefak	Autopsy	MZCacheView	ChromeCacheView
Text Message	-	-	✓
Username	-	-	✓
ID	-	-	✓
Server Channel ID	-	-	✓
Text Message	-	-	✓
Emoji dan Sticker	-	-	✓

Media	-	-	✓

Berdasarkan Tabel 4.10, pada percobaan tambahan yang dilakukan pada browser Google Chrome, proses akuisisi artefak menunjukkan bahwa artefak digital seperti text message, username, ID, server channel ID, emoji dan sticker, serta media berhasil diperoleh menggunakan tools ChromeCacheView. Sementara itu, tools Autopsy dan MZCacheView tidak berhasil menampilkan artefak pada browser ini. Hasil ini juga berkaitan dengan browser Microsoft Edge pada Tabel 4.11 yang menggunakan engine Chromium yang sama dengan Google Chrome, sehingga pola dan hasil perolehan artefak yang ditemukan cenderung serupa dan dapat dianalisis menggunakan tools yang dirancang untuk membaca struktur cache berbasis Chromium.

4.9 Percobaan dengan Aplikasi Perpesan yang Lain

Perbandingan dengan aplikasi pesan berbasis web lainnya menunjukkan bahwa artefak digital yang ditemukan pada Discord tidak selalu dapat ditemukan pada platform komunikasi lain. Hal ini dapat disebabkan oleh perbedaan arsitektur sistem serta mekanisme penyimpanan data yang diterapkan oleh masing-masing aplikasi. Beberapa aplikasi pesan tidak menyimpan data percakapan atau metadata secara langsung pada browser cache, melainkan menggunakan metode penyimpanan lain seperti *local storage*, *IndexedDB*, atau penyimpanan yang telah dienkripsi. Selain itu, kebijakan pengelolaan cache pada setiap aplikasi juga dapat berbeda, di mana sebagian aplikasi hanya menyimpan sumber daya tertentu atau secara otomatis menghapus data cache dalam jangka waktu tertentu. Kondisi tersebut dapat menyebabkan artefak digital yang biasanya ditemukan pada cache browser saat mengakses Discord tidak ditemukan atau jumlahnya sangat terbatas pada aplikasi pesan lainnya. Oleh karena itu, meskipun metode analisis browser cache menggunakan tools forensik dapat diterapkan pada berbagai aplikasi berbasis web, hasil yang diperoleh tidak selalu sama karena dipengaruhi oleh mekanisme pengelolaan data yang berbeda pada setiap platform.

4.10 Implikasi Anti-Forensics pada Artefak

4.10.1 Implikasi Anti-Forensics: Penggunaan Mode Incognito

Salah satu bentuk potensi anti-forensics dalam konteks penggunaan Discord Web adalah pemanfaatan mode incognito atau private browsing pada browser. Mode ini

dirancang untuk membatasi penyimpanan riwayat penelusuran, cookie, serta cache setelah sesi ditutup, sehingga secara teknis dapat meminimalkan jejak digital yang tertinggal pada perangkat lokal. Dalam praktiknya, apabila pelaku mengakses Discord melalui mode incognito, artefak seperti pesan, metadata pengguna, maupun referensi media yang sebelumnya dapat ditemukan pada direktori cache reguler berpotensi tidak tersimpan secara permanen setelah jendela incognito ditutup.

Dari sudut pandang forensik digital, kondisi ini memiliki implikasi signifikan terhadap proses recovery artefak berbasis browser cache. Berbeda dengan mode normal yang menyimpan respons API dalam bentuk file cache terstruktur, mode incognito hanya menyimpan data secara sementara di memori atau ruang penyimpanan volatil selama sesi aktif berlangsung. Setelah sesi berakhir, sistem secara otomatis menghapus sebagian besar data tersebut, sehingga peluang pemulihan melalui analisis cache menjadi jauh lebih terbatas. Hal ini menunjukkan bahwa keberhasilan recovery sangat dipengaruhi oleh waktu akuisisi dan kondisi sistem saat pemeriksaan dilakukan.

Meskipun demikian, penggunaan mode incognito tidak sepenuhnya menghilangkan jejak digital. Dalam beberapa kondisi, artefak masih dapat ditemukan melalui analisis memori (live memory forensics) atau melalui sisa data yang belum sepenuhnya tertimpa pada media penyimpanan. Oleh karena itu, pemahaman terhadap mekanisme kerja mode incognito menjadi penting dalam merumuskan strategi investigasi yang lebih komprehensif. Pembahasan ini memperlihatkan bahwa aspek anti-forensics perlu dipertimbangkan dalam analisis artefak Discord Web, karena teknik sederhana seperti penggunaan mode incognito dapat secara signifikan memengaruhi ketersediaan bukti digital pada browser cache.

4.10.2 Implikasi Penggunaan VPN atau Jaringan Anonimisasi (Tor)

Selain penggunaan mode incognito, teknik lain yang berpotensi dimanfaatkan sebagai bentuk anti-forensics adalah penggunaan Virtual Private Network (VPN) atau jaringan anonimisasi seperti Tor. VPN bekerja dengan mengenkripsi lalu lintas jaringan dan menyembunyikan alamat IP asli pengguna, sedangkan Tor mengalihkan koneksi melalui beberapa node relai untuk meningkatkan anonimitas. Dalam konteks investigasi digital, teknik ini sering digunakan untuk menyamarkan lokasi geografis dan identitas jaringan pelaku.

Namun demikian, dalam penelitian ini yang berfokus pada artefak Discord Web berbasis browser cache, penggunaan VPN atau Tor tidak secara langsung menghilangkan artefak komunikasi yang tersimpan di sisi klien. Artefak seperti username, user ID, server/channel ID, isi pesan, serta referensi media tetap tersimpan dalam struktur JSON

cache karena proses rendering dan penyimpanan data terjadi setelah respons diterima oleh browser. Dengan kata lain, VPN dan Tor lebih berfungsi sebagai mekanisme anonimisasi jaringan (network-level anti-forensics), bukan sebagai mekanisme penghapusan artefak lokal pada perangkat pengguna. Meskipun demikian, penggunaan VPN atau Tor tetap memiliki implikasi signifikan dalam proses atribusi dan korelasi bukti. Investigator mungkin mengalami kesulitan dalam mengaitkan aktivitas komunikasi dengan alamat IP atau lokasi fisik tertentu, sehingga pembuktian menjadi lebih kompleks. Hal ini menunjukkan bahwa meskipun artefak lokal masih dapat ditemukan melalui analisis cache, dimensi jaringan tetap menjadi tantangan tersendiri dalam investigasi komprehensif. Oleh karena itu, pemahaman terhadap penggunaan VPN dan Tor perlu dipertimbangkan sebagai bagian dari analisis anti-forensics yang melengkapi temuan artefak berbasis browser cache dalam penelitian ini.

4.10.3 Implikasi Anti-Forensics: Overwriting Data pada Browser Cache

Salah satu bentuk anti-forensics yang bersifat tidak langsung namun signifikan adalah proses overwriting atau penimpaan data pada browser cache akibat aktivitas penggunaan selanjutnya. Browser secara otomatis mengelola kapasitas penyimpanan cache dengan mekanisme penggantian data lama menggunakan data baru ketika ruang penyimpanan mencapai batas tertentu. Akibatnya, artefak komunikasi Discord Web yang sebelumnya tersimpan dalam bentuk file cache dapat tertimpa dan hilang secara permanen tanpa adanya tindakan penghapusan eksplisit oleh pengguna.

Dalam konteks penelitian ini, kondisi overwriting memiliki implikasi penting terhadap keberhasilan recovery artefak. Artefak seperti pesan teks, metadata pengguna, maupun referensi media yang pada awalnya dapat ditemukan dalam struktur JSON cache berpotensi tidak lagi tersedia apabila telah tergantikan oleh aktivitas browsing berikutnya. Hal ini menunjukkan bahwa keberhasilan investigasi sangat dipengaruhi oleh faktor waktu akuisisi. Semakin lama jeda antara aktivitas komunikasi dan proses pemeriksaan forensik, semakin besar kemungkinan artefak telah tertimpa oleh data baru. Dari perspektif forensik digital, overwriting merupakan bentuk anti-forensics pasif karena tidak selalu dilakukan secara sadar oleh pelaku, namun tetap berdampak pada hilangnya bukti digital. Oleh karena itu, investigator perlu mempertimbangkan strategi akuisisi yang cepat serta penggunaan teknik analisis lanjutan, seperti carving pada ruang tidak teralokasi, untuk meningkatkan peluang pemulihan data yang telah terhapus secara logis. Pembahasan ini menegaskan bahwa dinamika manajemen cache browser menjadi faktor krusial dalam menilai kualitas dan keberlanjutan artefak Discord Web yang ditemukan.

BAB V
Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil pengujian diperoleh beberapa kesimpulanutama sebagai berikut:

1. Penelitian ini menunjukkan bahwa interaksi pengguna Discord Web meninggalkan artefak digital pada browser cache, meliputi teks percakapan (termasuk pesan yang diedit dan balasan), emoji, stiker, serta media berupa gambar dan dokumen, yang masih dapat diidentifikasi meskipun telah dihapus dari tampilan aplikasi.
2. Hasil penelitian menunjukkan bahwa efektivitas tools bervariasi, di mana Autopsy mendukung analisis yang lebih terstruktur, MZCacheView optimal untuk Mozilla Firefox, dan ChromeCacheView efektif untuk Google Chrome serta Microsoft Edge. Secara keseluruhan, masing-masing tools memiliki kelebihan dan keterbatasan, sehingga penggunaan secara kombinasi memberikan hasil yang lebih optimal.
3. Hasil penelitian menunjukkan adanya perbedaan pemulihan artefak Discord antar browser. Google Chrome dan Microsoft Edge yang berbasis Chromium menghasilkan pola artefak yang serupa, sedangkan Mozilla Firefox memiliki karakteristik cache berbeda sehingga menghasilkan variasi pemulihan yang unik. Temuan ini menegaskan bahwa mekanisme internal browser memengaruhi jenis dan tingkat kemudahan recovery artefak digital.

5.2 Saran

Untuk penelitian selanjutnya, disarankan agar ruang lingkup diperluas dengan melibatkan lebih banyak variasi lingkungan uji, seperti penggunaan versi terbaru browser maupun sistem operasi yang berbeda, guna melihat konsistensi hasil pemulihan artefak. Selain itu, penelitian ini masih berfokus pada cache browser sehingga artefak yang bersifat volatil, seperti data pada RAM atau aktivitas jaringan, belum dianalisis secara menyeluruh; aspek tersebut dapat menjadi peluang pengembangan di masa depan. Tools yang digunakan juga terbatas pada Autopsy, MZCacheView, dan ChromeCacheView, sehingga penelitian selanjutnya dapat mencoba integrasi dengan perangkat forensik lain, termasuk tools memori atau jaringan, untuk memperkaya hasil analisis. Penelitian lanjutan juga dapat menguji skenario aktivitas Discord yang lebih kompleks, seperti panggilan suara, video, atau penggunaan bot, agar temuan semakin representatif dengan kondisi penggunaan nyata. Dengan memperhatikan aspek-aspek tersebut, diharapkan penelitian berikutnya dapat

menghasilkan temuan yang lebih komprehensif dan memberikan kontribusi yang lebih besar bagi pengembangan bidang forensik digital.

Daftar Pustaka

Vaddi, K. S., Kamble, D., Vaingankar, R., Khatri, T., & Bhalerao, P. (2024). Enhancements in the world of digital forensics. Int J Artif Intell ISSN, 2252(8938), 8938.

Rosmaida, E., & Bakhtiar, H. S. (2025). Pentingnya Digital Forensik sebagai Upaya untuk Menganalisa Barang Bukti Elektronik Terhadap Proses Pembuktian Tindak Pidana Informasi dan Transaksi Elektronik. Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research, 2(1), 741-751.

Hamad, N., & Eleyan, D. (2022). Digital Forensics Tools Used in Cybercrime Investigation Comparative Analysis. 113–127. https://doi.org/https://doi.org/10.37896/JXAT14.04/314909

Studiawan, H. (2020). Forensic investigation of event logs by automatic anomaly detection (Doctoral dissertation, Murdoch University).

Sarsono, B., & Indrayani, R. (2024). Analisis live forensics Keamanan browser pada marketplace (Studi Kasus : Tokopedia Dan Bukalapak). Explore, 14(2), 125-129. https://doi.org/10.35200/ex.v14i2.126

Dwi, F. (2023). Analisis aktivitas cyber bullying pengguna Facebook melalui browser chrome dengan pendekatan live forensics. Jurnal TIMES, 12(1), 21-27. https://doi.org/10.51351/jtm.12.1.2023687

Syukri, M., Imam Riadi, & Tole Sutikno. (2025). Analisis Forensik Keamanan data Pribadi pada mode Privasi browser Menggunakan Metode National Institute of standards and technology (NIST). Jurnal PROCESSOR, 20(1). https://doi.org/10.33998/processor.2025.20.1.2012

Iqbal, F., Motylinski, M., & MacDermott, A. (2021). Discord server forensics: Analysis and extraction of digital evidence. 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 1-8. https://doi.org/10.1109/ntms49979.2021.9432654

Motylinski, M., MacDermott, A., Iqbal, F., Hussain, M., & Aleem, S. (2020). Digital forensic acquisition and analysis of discord applications. 2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), 1-7. https://doi.org/10.1109/ccci49893.2020.9256668

Herawati, C. K., & Riadi, I. (2021). Forensic browser on Facebook services using National Institute of standards technology method. International Journal of Computer Applications, 183(30), 17-24. https://doi.org/10.5120/ijca2021921683

Pandela, T., & Riadi, I. (2020). Browser forensics on web-based TikTok applications. International Journal of Computer Applications, 175(34), 47-52. https://doi.org/10.5120/ijca2020920897

Chand, R. R., Sharma, N. A., & Kabir, M. A. (2025). Advancing web browser forensics: Critical evaluation of emerging tools and techniques. SN Computer Science, 6(4). https://doi.org/10.1007/s42979-025-03921-6

Reza Febriana, & Ahmad Luthfi. (2023). Comparative study of cloud forensic investigation using ADAM and NIST 800-86 methods in private cloud computing. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 7(5), 1097-1110. https://doi.org/10.29207/resti.v7i5.5279

Gupta, K., Varol, C., & Zhou, B. (2023). Digital forensic analysis of discord on Google chrome. Forensic Science International: Digital Investigation, 44, 301479. https://doi.org/10.1016/j.fsidi.2022.301479

Amelia, C., & Riadi, I. (2021). Browser forensic of extortion case on WhatsApp web using National Institute of justice method. International Journal of Computer Applications, 183(42), 36-42. https://doi.org/10.5120/ijca2021921823

Utomo, D. S., Prayudi, Y., & Ramadhani, E. (2023). Forensic web analysis on the latest version of WhatsApp browser. Journal of Computer Networks, Architecture and High Performance Computing, 5(1), 359-367. https://doi.org/10.47709/cnahpc.v5i1.2286

Hariyadi, D., Indriyanto, M. W., & Habibi, M. (2020). Investigasi Dan Analisis Forensik Digital Pada Percakapan Grup Whatsapp Menggunakan NIST Sp 800-86 dan Support Vector Machine. Cyber Security dan Forensik Digital, 3(2), 34-38. https://doi.org/10.14421/csecurity.2020.3.2.2193

Soares, A. M. (2022). WhatsApp web client live forensics technique. Proceedings of the 8th International Conference on Information Systems Security and Privacy, 629-636. https://doi.org/10.5220/0011006400003120

Hanaputra, R. R., Sa'adah, K., & Purwoko, R. (2024). Identifikasi digital evidence dalam transaction fraud pada WhatsApp desktop berdasarkan NIST SP 800-86: Studi Kasus Bisnis Properti. JURNAL FASILKOM, 14(2), 332-338. https://doi.org/10.37859/jf.v14i2.7100

Ruslan, T., Riadi, I., & Sunardi, S. (2023). Analisis Forensik digital Pada WhatsApp Dan Facebook Menggunakan Metode NIST. JURNAL FASILKOM, 13(02), 286-292. https://doi.org/10.37859/jf.v13i02.5540

Muhammad Abdul Aziz, Wicaksono Yuli Sulistyo, & Sri Rahayu Astari3. (2021). Komparatif anti Forensik Aplikasi instant messaging Berbasis web Menggunakan Metode association of chief police officers (ACPO). JURISTIK (Jurnal Riset Teknologi Informasi dan Komputer), 1(01), 8-15. https://doi.org/10.53863/juristik.v1i01.341

Warren, C., El-Sheikh, E., & Le-Khac, N. (2017). Privacy preserving internet browsers: Forensic analysis of Browzar. Computer and Network Security Essentials, 369-388. https://doi.org/10.1007/978-3-319-58424-9_21

Dargahi, T., Dehghantanha, A., & Conti, M. (2017). Forensics analysis of Android mobile VoIP apps. Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, 7-20. https://doi.org/10.1016/b978-0-12-805303-4.00002-2

Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. Digital Investigation, 11(3), 201-213. https://doi.org/10.1016/j.diin.2014.04.003

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models. International Journal of Computer Science and Information Technology, 3(3), 17–31. https://doi.org/10.5121/ijcsit.2011.3302.

Rosalina, V., Herli, D. (2015). Pengembangan Model Tahapan Digital Forensic Untuk Mendukung SERANG Sebagai Kota Bebas Cybercrime. Seminar Nasional Riset Terapan 2015 (SENASSET 2015).

Khweiled, R., & Jazzar, M. (2021). An Improved Framework For Cyberbullying Investigation Process on WhatsApp application. J. Xi'an Univ. Archit. Technol., 13(9), 238-246. DOI: 10.37896/JXAT13.9/313822.

Rafiq, I. A., & Riadi, I. (2022). Perbandingan Forensic Tools pada Instagram Menggunakan Metode NIST. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *7*(2), 134-142.

Nadilla. (2026b, March 4). Polda Metro Jaya dalami kasus dugaan penipuan investasi kripto lewat grup aplikasi discord. *Antara News Kepri*. https://kepri.antaranews.com/berita/247285/polda-metro-jaya-dalami-kasus-dugaan-penipuan-investasi-kripto-lewat-grup-aplikasi-discord

Turner, A. (2022, March 1). *Discord Users: How Many People Use Discord (Apr 2023)*. Bank My Cell. https://www.bankmycell.com/blog/number-of-discord-users/

LAMPIRAN A