Analisis Bukti Digital Pada Discord Browser Menggunakan Teknik Live Forensic Dengan Metode NIST SP 800-86

Mohammad Yan Fikri Hendrawan[1], Subektiningsih[2], Arifiyanto Hadinegoro[3*]

[1]*Fakultas Ilmu Komputer, Teknik Komputer, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia*
[2,3]*Fakultas Ilmu Komputer, Informatika, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia*

[1]mohammad.hendrawan@students.amikom.ac.id
[2*]subektiningsih@amikom.ac.id (penulis korespondensi)
[3]arifiyanto@amikom.ac.id

Abstrak— Platform komunikasi sangat beragam, sebagai contoh adalah *Discord*. Pengguna memanfaatkan platform Discord untuk chat dan berbagi konten. Namun, dalam platform Discord sering terindikasi distribusi konten tidak layak, konten yang tidak sesuai dengan peraturan dari Discord. Hal ini dapat memicu kasus *cybercrime* seperti; *sexual harassment*, *cyber bullying*, dan *hacking.* Dalam investigasi tindak kejahatan memerlukan bukti digital untuk dianalsis. Tantangan yang dialami berupa data digital yang telah dihapus melalui platform komunikasi yang digunakan. Tujuan dalam penelitian ini adalah untuk menganalisis bukti digital berupa pesan teks serta gambar atau foto yang telah dihapus pada *room chat* platform Discord berbasis website. Teknik yang digunakan adalah *live forensic* menggunakan Metode NIST SP 800-86. Fokus dalam penelitian ini adalah membandingkan bukti digital yang diperoleh dari berbagai browser yang digunakan untuk mengakses Discord. Eksperimen melalui penyusunan scenario dengan mengakses Discord melalui berbagai browser, antara lain; Google Chrome, Mozilla Firefox, dan Microsoft EDGE. Tahap analisis menggunakan *forensic tools* Chrome Cache View, MZ Cache View, FTK Imager, dan Autopsy. Bukti digital berupa *username, time* dan pesan teks serta gambar yang telah dihapus dari Discord dengan diakses menggunakan ketiga browser tersebut dapat ditemukan menggunakan kombinasi *forensic tools* tersebut. Nilai Persentase akurasi tools Autopsy dan Chrome Cache View sebesar 75 %, FTK Imager 50%, dan MZ Cache View 25%. Akurasi pada MZ Cache View paling sedikit dikarenakan tools tersebut hanya dapat digunakan pada browser Mozilla Firefox. Dalam analisis bukti digital kombinasi penggunaan *forensic tools* dapat dilakukan mendapatkan informasi lengkap sebagai pembuktian insiden. Penelitian selanjutnya dapat dikembangkan dengan teknik yang berbeda untuk memperoleh bukti digital yang lebih bervariasi.
Kata kunci— discord; browser; live forensic; NIST; bukti digital

Abstract— Communication platforms are very diverse, for example, Discord. Users use the Discord platform to chat and share content. However, on the Discord platform, there are often indications of the distribution of inappropriate content that does not comply with Discord's regulations. This can trigger cybercrime cases such as sexual harassment, cyberbullying, and hacking. Investigating crimes requires digital evidence to be analyzed. The challenge experienced is in the form of digital data deleted through the communication platform. This research aims to analyze digital evidence in the record of text messages and images or photos that have been deleted in chat rooms on the website-based Discord platform. The technique used is live forensics using the NIST SP 800-86 method. This research focuses on comparing digital evidence obtained from various browsers used to access Discord. Experiment by preparing scenarios by accessing Discord via various browsers, including Google Chrome, Mozilla Firefox, and Microsoft EDGE. The analysis stage uses forensic tools Chrome Cache View, MZ Cache View, FTK Imager, and Autopsy. Digital evidence in the form of usernames, times, text messages, and images that have been deleted from Discord by accessing these three browsers can be found using a combination of these forensic tools. The accuracy percentage value of the Autopsy and Chrome Cache View tools is 75%, FTK Imager 50%, and MZ Cache View 25%. The accuracy of MZ Cache View is minimal because this tool can only be used in the Mozilla Firefox browser. In digital evidence analysis, a combination of forensic tools can be used to obtain complete information as proof of the incident. Future research can be developed with different techniques to obtain more varied digital evidence.
Keywords— discord; browser; live forensic; NIST; digital evidence

I. PENDAHULUAN

Keberadaan *Internet* memudahkan manusia dalam berkomunikasi dan berinteraksi secara global, serta membawa manfaat dalam bidang pendidikan, bisnis maupun hiburan *(entertainment)*. Hal ini sejalan dengan perkembangan aplikasi dalam berkomunikasi, salah satunya adalah *Discord* [1]. Platform Discord dapat diakses gratis untuk melakukan percakapan antar pengguna secara *real time* menggunakan teks, suara atau video. Platfrom Discord dapat diakses melalui browser dengan 140 juta pengguna aktif bulanan pada tahun 2021. Jumlah pengguna pada tahun 2021 tersebut meningkat sebesar 40% dari tahun sebelumnya. Platform Discord pada tahun 2021 mempunyai 13,5 juta server aktif, yang artinya mengalami peningkatan sebesar 6,7 juta dari tahun 2020 [2]. Platfrom Discord lebih populer di kalangan gamers [3]. Bahkan, dalam platfrom Discord terindikasi adanya konten-konten yang tidak layak, sehingga dapat memicu berbagai kasus *cybercrime*, seperti penipuan; *sexual harrasemengt,* pornografi, dan *cyber bullying* [4]. Insiden ataupun kejahatan pada dunia maya dapat diungkapkan melalui pendekatan forensik digital [1]

Analisis forensik digital pada aplikasi Discord dilakukan oleh [2] dengan mempresentasikan struktur caching serta log aktivitas pada Discord. *Tools* forensic yang diimplementasikan adalah DiscFor, digunakan untuk mengekstrak data dari file Discord lokal dan penyimpanan cache untuk selanjutnya dilakukan analisis. Forensik pada aplikasi menjadi penting karena kejahatan dunia maya memanfaatkan *software* komunikasi mengalami peningkatan [2]. Tool forensik digital Discfor juga pernah digunakan oleh [3] untuk menganalisis bukti digital pada aplikasi Discord. Dalam [4] melakukan penelitian artefak internet browser yang berupa Google Chrome, Mozilla Firefox, Opera dalam *Incognito Mode*. Proses forensik digital yang dilakukan oleh [4] berfokus melakukan analisis bukti digital pada browser yang berbeda-beda. Hasil forensik pada browser mode

incognito ini dapat diperoleh berbagai bukti digital, antara lain; riwayat penjelajahan, URL, kata sandi, dan nama pengguna. Proses yang dilakukan meliputi preservasi, tahap akuisisi, dan analisis bukti digital. Dalam [5] melakukan forensik web browser Google Chrome pada perangkat mobile Android untuk mengidentifikasi bukti digital. Metode dalam penelitian didasarkan pada pedoman National Institute of Justice (NIJ) antara lain; persiapan, pengumpulan data, pemeriksaan, dilanjutkan dengan analisis dan terakhir adalah pelaporan. Temuan bukti digital dalam dalam web browser Google Chrome yaitu; akun, bookmark, dokumen, Riwayat pencarian, email, gambar, waktu, password, dan URL. Penelitian pada aplikasi Discord yang diakses menggunakan web browser Google Chrome juga pernah dilakukan oleh [6]. Metode ekperimental digunakan untuk memperoleh artefak yang dipulihkan pada platform Discord. Dalam proses pengumpulan bukti digital, *timeline* atau garis waktu menjadi hal penting selama proses forensic.

Metode forensik yang juga dapat diterapkan untuk investigasi adalah Digital Forensics Research Workshop (DFRWS). Dalam [7] menyatakan bahwa metode DFRWS efektif dalam menganalisis bukti digital pada aplikasi media sosial. Namun, pada penelitian analisis bukti digital pada Discord browser ini menggunakan metode yang berbeda, yaitu Metode *NIST SP 800-86* dengan teknik *live forensic*. NIST SP 800-86 terdiri dari 4 tahap, yaitu *Collection, Examination, Analysis, Report.* Insiden yang dilakukan investigasi berbasis skenario yang telah disusun. Skenarionya adalah pengguna Discord saling mengirimkan teks percakapan, file gambar. Selanjutnya, pesan dan file gambar tersebut akan dihapus. Tujuan dari penelitian ini adalah untuk memperoleh atau mengembalikan bukti digital yang telah dihapus pada platform Discord. Skenario diterapkan pada tiga browser yang berbeda, antara lain; Mozilla Firefox, Google Chrome, dan Microsoft Edge. Proses forensik menggunakan beberapa *tools*, antara lain; FTK Imager, Autopsy, MZ Cache view, dan Chrome Cache View. Bagaimana keempat tools forensic tersebut digunakan dalam pemeriksaan dan analisis bukti digital? Apakah pesan teks dan file gambar yang sudah terhapus pada platform Discord browser dapat kembalikan? Hal ini juga untuk membuktikan apakah keempat tools tersebut dapat digunakan pada ketiga jenis browser yang berbeda (Mozilla Firefox, Google Chrome, dan Microsoft Edge)

II. METODOLOGI PENELITIAN

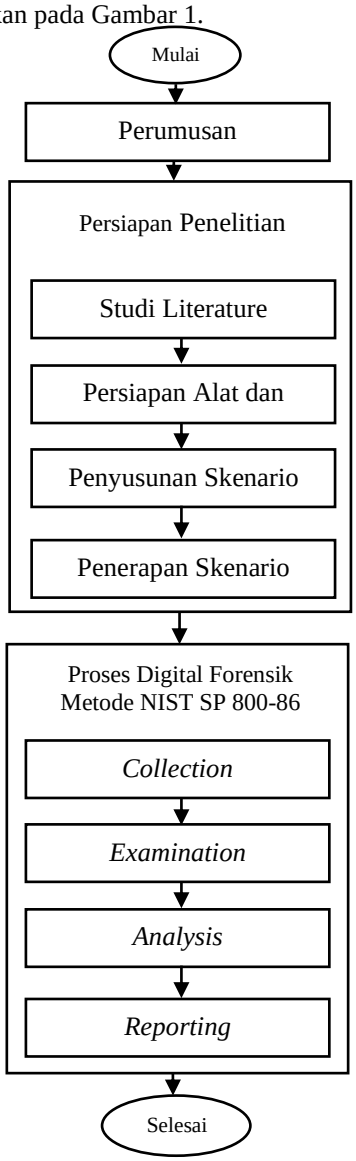
2.1 Skenario Insiden

Investigasi menggunakan skenario yang disusun berdasarkan insiden *body shamming* dan *harassment* yang terjadi pada Discord. Dalam [8] menyatakan bahwa *NBC News* melaporkan 165 kasus penuntutan atas CSAM *(Child Sexual Abuse Material)* melalui platform Discord, bahkan sejumlah orang dewasa memaksa remaja untuk mengirimkan gambar seksual.

Skenario diawali dengan terjadinya percakapan antar teman sekantor (orang1 dan orang2) di *room chat* Discord yang berbasis website. Percakapan ini di mulai saat orang1 mengirimkan gambar lucu, namun orang2 membalas percakapan berupa pesan teks dan gambar yang mengandung unsur *body shaming, sexual harrasement* dan *rasisme.* Hal tersebut membuat orang1 merasa terhina harga dirinya, sehingga membalas percakapan dengan maksud menyampaikan rasa sakit hatinya. Selanjutnya, orang1 melakukan *screenshoot* percakapan yang terjadi dan menyampaikan berkeinginan kepada orang2 bahwasannya akan melaporkan kejadian tersebut kepada Pihak Berwajib. Orang2 menjadi panik dan menghapus pesan teks dan gambar ejekan yang telah dikirimkan untuk menghilangkan bukti. Pada saat itu juga orang1 segera melaporkan kepada Pihak Berwajib dan setelah semua prosedur investigasi terpenuhi segera mendatangi rumah orang2. Selanjutnya, ditemukan barang bukti sebuah *personal computer* yang masih dalam kondisi menyala *(on)*. Orang2 menjadi panik dan meninggalkan rumah dengan terburu-buru, sehingga tidak mematikan atau *menshut-down* komputernya. Selanjutnya, tim forensik digital melakukan *live forensic* pada barang bukti (komputer dalam kondisi *on*) untuk memperoleh bukti digital dan membuktikan kebenaran dari insiden. Skenario ini diterapkan pada berbagai jenis browser yang berbeda, antara lain; Google Chrome, Mozilla Firefox, dan Microsoft EDGE.

2.2 Tahap Penelitian

Metode yang digunakan dalam penelitian adalah Dokumen Standar dari *National Institute of Standards and Technologi-Special Publication 800-86 atau NIST SP 800-86* [9]. Tahap Penelitian disajikan pada Gambar 1.



Gambar 1. Alur Penelitian

Tahap penelitian diawali dengan perumusan masalah yang didukung dengan studi literature terkait. Selanjutnya,

mempersiapkan alat dan bahan yang digunakan untuk menyelesaikan permasalahan. Tahap berikutnya menyusun dan menerapkan skenario berdasarkan masalah yang sudah dirumuskan. Berdasarkan skenario tersebut akan dilakukan forensik digital menggunakan Metode NIST SP 800-86 [9]. Tahap dalam NIST antara lain:

a. Collection adalah tahapan forensik pertama yang bertujuan mengumpulkan barang bukti dari Tempat Kejadian Perkara. Dalam skenario ini barang bukti berupa perangkat keras, *personal computer* milik orang2 diamankan. Proses selanjutnya melakukan akuisisi atau membuat salinan barang bukti digital supaya keaslian bukti pada perangkat asli tetap terjaga.
b. Examination merupakan tahap mengidentifikasi sumber data potensial untuk diolah menjadi informasi menggunakan *tools forensic* berupa; FTK Imager, Autopsy, MZCacheView, dan ChromeCacheView. Identifikasi dilakukan berdasarkan scenario yang sudah ditepakan pada tiga browser yang berbeda.
c. Analysis menjadi tahap berikutnya untuk mengekstrak informasi sesuai data potensial yang sudah diperiksa. Tujuan dari tahap analisis adalah untuk mendapatkan bukti digital, sehingga diperoleh informasi sebagai pembuktian insiden berdasarkan skenarion.
d. Reporting menjadi tahap terakhir dalam proses forensic. Pelaporan dari keseluruhan proses yang dilakukan supaya terdokumentasi dengan baik.

Teknik yang digunakan dalam proses forensik digital adalah. *live forensic*, suatu teknik analisis terhadap data yang masih berjalan pada system *(data bersifat volatile)* yang tersimpan pada Random *Access Memory* (RAM) atau pada jaringan komputer yang sedang beroperasi. Investigasi secara *live forensic* lebih terjamin dalam mendapatkan barang bukti digital.[10]

III. HASIL DAN PEMBAHASAN

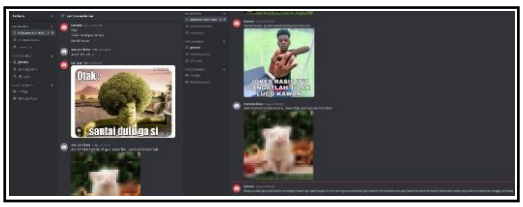
Semua tautan *hypertext* dan bagian *bookmark* akan dihapus. Jika paper perlu merujuk ke alamat email atau URL di artikel, mak

Penelitian diawali dengan mengulas studi literatur terkait digital forensic menggunakan teknik live forensic. Tahap berikutnya mempersiapkan alat dan bahan untuk eksperimen yang disajikan pada Tabel 1

TABEL I
ALAT DAN BAHAN

Perangkat Keras	Perangkat Lunak
Personal Computer	1. Platform Discord Berbasis Website
1. Processor: AMD Ryzen 3 2200	2. Browser Google Chrome
2. RAM Kingstone Fury 8GB	3. Browser Mozilla Firefox
3. Storage Kingstone 256GB SATA 3 SSD	4. Browser Microsoft EDGE
4. Motherboard GA-AB350M-Gaming 3	5. Digital Forensic Tools:
5. Graphics Card GeForce GTX 1050 2GB	a. AccessData FTK Imager
6. Power Supply Cooler Master MWE 450 Bronze V2	b. Autopsy
7. Display LG 55cm/22" Monitor	c. ChromeCacheView
	d. MZCacheView

Tahap berikutnya adalah implementasi dari skenario insiden yang telah disusun. Skenario dimulai dari dua orang (orang1 dan orang2) yang memulai percakapan pada Discord melalui browser. Percakapan tersebut dilakukan menggunakan tiga browser, antara lain; Google Chrome, Mozilla Firefox, dan Microsoft EDGE. Percakapan yang dilakukan oleh kedua orang tersebut, yaitu orang1 adalah "kumara" dan orang2 adalah "manusia biasa" ditunjukkan pada Gambar 2.



Gambar 2. Implementasi Skenario Insiden

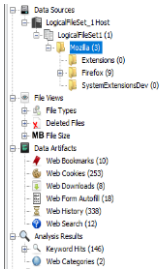
Berdasarkan skenario insiden tersebut dilakukan proses digital forensic dengan teknik *live forensic*, hal ini dikarenakan kondisi Tempat Kejadian Perkara Digital yang berupa *personal computer* masih dalam keadaan menyala (on). Berdasarkan [11] menyatakan bahwa Tempat Kejadian Perkara fisik maupun digital dapat dilakukan proses investigasi secara bersamaan. Penanganan Tempat Kejadian Perkara, Penanganan dan pencatatan barang bukti, serta proses forensik harus dilakukan secara sistematis [12]. Oleh sebab itu, dalam penelitian ini menggunakan metode terstruktur NIST SP 800-86 [9].

3.1 Collection

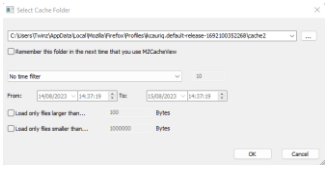
Bukti digital yang dikumpulkan berupa data dalam folder *Cache*. File yang berada dalam folder tersebut adalah file sementara yang tersimpan pada browser. Berdasarkan skenario, sebagian besar isi dari percakapan sudah di hapus. Sehingga, Pengumpulan bukti ini bertujuan untuk memperoleh isi dari percakapan tersebut, berupa pesan teks dan gambar. Pengumpulan bukti dari browser Mozilla Firefox ada dalam direktori *C:\Users\Twinz\AppData\Local\Mozilla.* Hal ini juga berlaku untuk browser Google Chrome dan Microsoft Edge.

3.2 Examination

Tahap berikutnya adalah *Examination* yang dilakukan menggunakan *forensic tools* antara lain; AccessData FTK Imager, Autopsy, MZCacheView, dan ChromeCacheView. Data yang diperoleh melalui tahap *collection*, yaitu file cache dilakukan pemeriksaan menggunakan berbagai forensic tools tersebut. Tujuan dari pemeriksaan ini adalah untuk mendapatkan informasi dari bukti digital yang berupa folder cache dari masing-masing browser yang digunakan untuk mengakses platform discord berbasis website. Tahap pertama dalam pemeriksaan menggunakan AccessData FTK Imager adalah menambahkan "evidence item" yang berupa "content of a folder" dari file cache browser. Pemeriksaan berikutnya menggunakan Autopsy. Tahap pertama adalah membuat case baru untuk menyimpan detail informasi dari insiden. Selanjutnya, menambahkan sumber data yang berupa LogicalFileSet berupa folder cache. Tampilan dari pemeriksaan sumber data pada Autopsy ditunjukkan pada Gambar 3. Pemeriksaan selanjutnya dilakukan menggunakan tools MZCacheView dan ChromeCacheView terhadap sumber data yang sama, yaitu "Folder Cache". Tahap ini ditunjukkan pada Gambar 4.

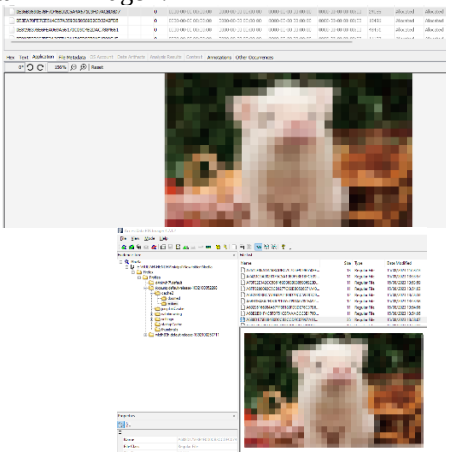


Gambar 3. Pemeriksaan pada Autopsy



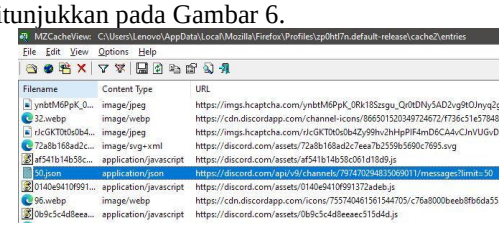
Gambar 4. Pemeriksaan pada MZCacheView

Pemeriksaan dilakukan secara manual dengan mengecek satu per satu setiap file cache yang ada di dalam "folder cache browser". Pada pemeriksaan menggunakan Autopsy ditemukan file File cache yang berisi file dengan identifier *0E36B3690E7BF7D46BD2C5A4A671C9FD7ACBD8D7* yang ternyata berupa file "Gambar" yang dikirimkan oleh "manusia biasa". Temuan ini ditunjukkan pada Gambar 5. File Gambar tersebut juga ditemukan saat pemeriksaan menggunakan AccessData FTK Imager .



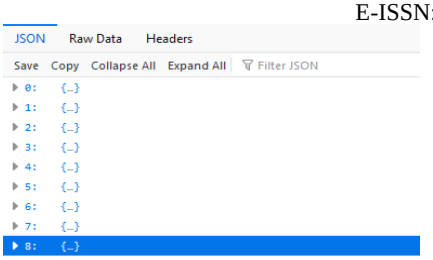
Gambar 5. Hasil Pemeriksaan pada FTK Imager dan Autopsy

Pemeriksaan dilanjutkan untuk mendapatkan data percakapan pada room chat Discord. Fokus pemeriksaan pada file *"json"* untuk mencari pesan teks. Pemeriksaan secara manual menemukan file json dengan nama "50.json" seperti yang ditunjukkan pada Gambar 6.



Gambar 6. Hasil Pemeriksaan pada MZCacheView

Pemeriksaan file 50.json menggunakan browser Mozilla Firefox. Dalam pemeriksaan ditemukan pesan teks sebanyak 9 baris pesan yang dikirimkan oleh "manusia biasa" kepada "kumara"seperti pada Gambar 7.



Gambar 7. Baris Percakapan Hasil Pemeriksaan

Dalam setiap baris percakapan berisi detail pesan yang dikirimkan oleh pengguna Discors. Pemeriksaan dilakukan pada setiap baris percakapan. Dalam baris percakapan berisi *id, type, content, channel_id* yang berupa identitas dan isi dari percakapan. Dalam pemeriksaan juga ditemukan keterangan tentang "author" yang berupa id dan *username*, seperti pada Gambar 8.

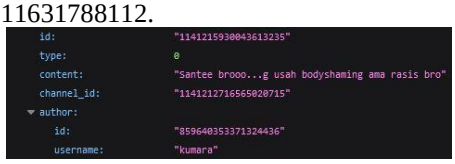
Gambar 8. Keterangan Pengguna

3.3 Analysis

Tahap analisis dilakukan menggunakan kombinasi *forensic tools* untuk memperoleh semua informasi yang dapat dijadikan pembuktian insiden. Analisis dilakukan untuk mencari informasi berdasarkan data hasil pemeriksaan. Pada baris ke-4 di gambar 7 berisi sapaan dari "manusiabiasa" di room chat Discord, yang dibalas oleh "Kumara". Percakapan berlanjut dengan perkenalan diri dari "kumara", namun ditanggapi dengan respon negatif oleh "manusia biasa". Pengguna dengan id "kumara" berusaha menegur, namun dijawab oleh "manusiabiasa" dengan pesan dan gambar yang cenderung *body shimming* dan mengarah ke *harrasement*. Pesan yang menjadi pemicu insiden ditunjukkan Gambar 9.

Gambar 9. Hasil Analisis Pemicu Insiden

Pesan negatif "manusiabiasa" ditanggapi dengan respon yang baik oleh "kumara" berupa kalimat "sante broo… g usah bodyshaming ama rasis bro" dengan id pesan 1141215930043613235, seperti yang ditunjukkan pada Gambar 10. Namun, "manusiabiasa" tetap memberikan respon negatif, sehingga "kumara" memberikan pesan chat terakhir akan melaporkan kejadian tersebut kepada Pihak Berwajib. Bagian ini ditunjukkan pada gambar 11 dengan id pesan 1141216811631788112.



Gambar 10. Respon Baik kumara Atas Pesan Negatif manusiabiasa

Gambar 11. Respon Kumara akan Melaporkan Kejadian

Dalam pemeriksaan menggunakan ChromeCacheView dan MZCacheView ditemukan "file gambar" yang termasuk dalam kategori "attachment" dengan id 1141216167873224836 pada Gambar 12.

Gambar 12. Temuan "File Gambar'

File Gambar tersebut tidak dapat diextract menggunakan *tools* ChromeCacheView dan MZCacheView, oleh sebab itu, pemeriksaan lanjutan dilakukan menggunakan *tools* Autopsy dan AccessData FTK Imager. Hasil "file gambar" yang diextract menggunakan Autopsy dan FTK Imager ditunjukkan pada Gambar 5. "File Gambar" tersebut ditemukan pada Folder "Cache2" -> "Entries".

3.4 Reporting

Laporan berdasarkan tahap *collection, examination, analysis* untuk menyajikan temuan informasi. Temuan berdasarkan proses analisis di sajikan pada Tabel 2.

TABEL 2
TEMUAN BUKTI DIGITAL PERCAKAPAN PLATFORM DISCORD

Akun Pengguna Discord		Temuan	Keterangan
id	username		
114100363263713283 0	manusiabiasa 255	Pesan Text *"Diem brisik lu! Ni foto mirip lu, dasar b**i, kulit kok kek kulit b**i."*	Pemicu Insiden
		Gambar *(image)* 	Pemicu Insiden
859640353371324436	kumara	Pesan Text	Pesan balasan
		Gambar *(image)* 	Pesan balasan

Berdasarkan proses forensik digital menggunakan Metode NIST SP 800-86 berhasil memperoleh bukti digital berdasarkan pesan yang telah dihapus pada discord berbasis website. Perolehan bukti digital dilakukan menggunakan kombinasi *tools* forensik. Eksperimen dilakukan menggunakan tiga browser yang berbeda, yaitu Google Chrome, Mozilla Firefox, dan Microsoft EDGE. Persentase akurasi masing-masing *forensic tools* menggunakan perhitungan sebagai berikut:

$$\text{Pft} = \frac{\sum DE(obtained)}{\sum DE(required)} \times 100\ \%$$

Keterangan:
Pft : Akurasi *forensic tools*
∑DE (obtained) : Jumlah bukti digital yang diperoleh
∑DE (required) : Jumlah bukti digital yang diperlukan

TABEL 3
PEROLEHAN BUKTI DIGITAL PADA BROWSER GOOGLE CHROME

Temuan Bukti Digital	Parameter	Autopsy	FTK Imager	Chrome Cache View	MZ Cache View
Pesan Teks	*deleted*	√	√	√	-
Image	*deleted*	√	√	-	-
Username	-	-	-	√	-
Time	-	√	-	√	-

Bukti digital yang berhasil diperoleh pada Browser Google Chrome ditunjukkan pada Tabel 3. Pesan teks dan file gambar yang telah dihapus berhasil didapatkan dengan kombinasi tools forensik. Hanya tools MZCacheView yang tidak memperoleh bukti digital apapun. Persentase akurasi *forensic tools* pada browser Google Chrome ditunjukan Tabel 4.

TABEL 4
PERSENTASE AKURASI PEROLEHAN BUKTI DIGITAL PADA BROWSER GOOGLE CHROME

Persentase Akurasi	Autopsy	FTK Imager	Chrome Cache View	MZ Cache View
∑DE (obtained)	3	2	3	0
∑DE (required)	4	4	4	4
Pft	3 x 100% 4 = 75 %	2 x 100% 4 = 50 %	3 x 100% 4 = 75 %	0 x 100% 4 = 0 %
Average		**50 %**		

TABEL 5
PEROLEHAN BUKTI DIGITAL PADA BROWSER MOZILLA FIREFOX

Temuan Bukti Digital	Parameter	Autopsy	FTK Imager	Chrome Cache View	MZ Cache View
Pesan Teks	*deleted*	√	√	√	√
Image	*deleted*	√	√	-	-
Username	-	-	-	√	√
Time	-	√	-	√	√

Bukti digital yang berhasil diperoleh pada Browser Mozilla Firefox ditunjukkan pada Tabel 5. Proses forensik pada browser mozilla berhasil mendapatkan data dari pesan teks dan file gambar yang telah dihapus. Semua tools forensik memperoleh bukti digital yang digunakan sebagai pembuktian insiden. Persentase akurasi *forensic tools* pada browser Mozilla Firefox ditunjukan Tabel 6.

TABEL 6
PERSENTASE AKURASI PEROLEHAN BUKTI DIGITAL PADA BROWSER MOZILLA FIREFOX

Persentase Akurasi	Autopsy	FTK Imager	Chrome Cache View	MZ Cache View
∑DE (obtained)	3	2	3	3
∑DE (required)	4	4	4	4
Pft	3 x 100% 4 = 75 %	2 x 100% 4 = 50 %	3 x 100% 4 = 75 %	3 x 100% 4 = 75 %
Average		**68.75 %**		

Bukti digital yang berhasi diperoleh pada Browser Microsoft EDGE ditunjukkan pada Tabel 7. Hasil perolehan bukti digital pada browser Microsoft EDGE sama dengan ekperimen pada browser Google Chrome.

TABEL 7

PEROLEHAN BUKTI DIGITAL PADA BROWSER MICROSOFT EDGE

Temuan Bukti Digital	Parameter	Autopsy	FTK Imager	Chrome Cache View	MZ Cache View
Pesan Teks	*deleted*	√	√	√	-
Image	*deleted*	√	√	-	-
Username	-	-	-	√	-
Time	-	√	-	√	-

Persentase akurasi *forensic tools* pada browser Google Chrome ditunjukan Tabel 8.

TABEL 8
PERSENTASE AKURASI PEROLEHAN BUKTI DIGITAL PADA BROWSER MICROSOFT EDGE

Persentase Akurasi	Autopsy	FTK Imager	Chrome Cache View	MZ Cache View
∑DE (obtained)	3	2	3	0
∑DE (required)	4	4	4	4
Pft	3 x 100% / 4 = 75 %	2 x 100% / 4 = 50 %	3 x 100% / 4 = 75 %	3 x 100% / 4 = 0 %
Average		**50 %**		

Berdasarkan hasil eksperimen terhadap ketiga browser dinyatakan bahwa penggunaan kombinasi tools forensik dapat dilakukan untuk mendapatkan bukti digital yang diperlukan sebagai pembuktian insiden. Hal ini dikarekan tidak semua tools dapat memperoleh bukti digital. Pada browser Google Chrome dan Microsoft EDGE mempunyai kecenderungan serupa dalam kombinasi penggunaan tools forensik dan perolehan bukti digital. Rata-rata persentase akurasi dari kombinasi tools Autopsy, FTK Imager, Chrome Cache View, dan MZ Cache View adalah 50%. Pada Browser Mozilla Firefox mempunyai rata-rata akurasi kombinasi penggunaan tools forensik 68.75%. Akurasi persentase juga dapat ditinjau berdasarkan penggunaan masing-masing tools forensik pada ketiga browser, dengan hasil pada Tabel 9.

TABEL 9
PERSENTASE AKURASI TOOLS FORENSIK PADA KETIGA BROWSER

Browser	Autopsy	FTK Imager	Chrome Cache View	MZ Cache View
Google Chrome	75 %	50 %	75 %	0 %
Mozilla Firefox	75 %	50 %	75 %	75 %
Microsoft Edge	75 %	50 %	75 %	0 %
Average	**75 %**	**50 %**	**75 %**	**25 %**

Pada penggunaan ketiga browser (Google Chrome, Mozilla Firefox, Microsoft Edge) tools forensik Autopsy dan Chrome Cache View mempunyai nilai akurasi yang sama sebesar 75%, FTK Imager 50% dan MZ Cache View adalah 25%. MZ Cache View mempunyai rata-rata persentase akurasi paling sedikit dalam peroleh bukti digital, karena tools tersebut hanya dapat digunakan pada Browser Mozilla Firefox. Tahap analisis bukti digital yang dilakukan sesuai prosedur, metode yang tepat, dan dengan mengkominasikan berbagai tool forensik dapat dilakukan untuk mendapatkan informasi yang valid [13].

IV. KESIMPULAN

Teknik *live forensic* diterapkan pada platform Discord berbasis website untuk memperoleh bukti digital yang telah dihapus oleh pengguna. Eksperimen melalui penyusunan skenario dengan akses melalui browser yang berbeda-beda, yaitu; Google Chrome, Mozilla Firefox, dan Microsoft EDGE. Proses forensik menggunakan berbagai tools, antara lain; Chrome Cache View, MZ Cache View, FTK Imager, dan Autopsy. Menerapkan metode NIST SP 800-86 dengan tahapan *collection, examination, analysis, report* diperoleh bukti digital berupa pesan teks dan gambar yang telah dihapus dari platform Discord. Informasi lain yang dapat diperoleh adalah *username* dan *time* dari chat pada Discord. Dalam tahap forensik digital, kombinasi penggunaan *forensic tools* dapat dilakukan untuk memperoleh informasi yang lengkap sebagai pembuktian insiden. Dalam proses forensik dengan tools Chrome Cache View, FTK Imager, dan Autopsy dapat digunakan untuk memperoleh bukti digital berupa pesan teks yang telah dihapus dan username pada browser Google Chrome, Microsoft EDGE, dan Mozilla Firefox. Nilai Persentase akurasi tools Autopsy dan Chrome Cache View sebesar 75 %, FTK Imager 50%, dan MZ Cache View 25%. Akurasi pada MZ Cache View paling sedikit dikarenakan tools tersebut hanya dapat digunakan pada browser Mozilla Firefox. Penelitian selanjutnya dapat dikembangkan dengan teknik yang berbeda untuk memperoleh bukti digital yang lebih bervariasi.

REFERENSI

[1] S. Subektiningsih and D. Hariyadi, "The Role of Digital Forensic Experts in Cybercrime Investigations in Indonesia Based on The Scopus Research Index," *Build. Informatics, Technol. Sci.*, vol. 4, no. 3, pp. 1665–1670, 2022, doi: 10.47065/bits.v4i3.2638.

[2] F. Iqbal, M. Motylinski, and A. MacDermott, "Discord Server Forensics: Analysis and Extraction of Digital Evidence," *2021 11th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2021*, 2021, doi: 10.1109/NTMS49979.2021.9432654.

[3] M. Motylinski, A. MacDermott, F. Iqbal, M. Hussain, and S. Aleem, "Digital Forensic Acquisition and Analysis of Discord Applications," *Proc. 2020 IEEE Int. Conf. Commun. Comput. Cybersecurity, Informatics, CCCI 2020*, 2020, doi: 10.1109/CCCI49893.2020.9256668.

[4] M. Mu'Minin and N. Anwar, "Live Data Forensic Artefak Internet Browser (Studi Kasus Google Chrome, Mozilla Firefox, Opera Mode Incognito)," *Bul. Sist. Inf. dan Teknol. Islam*, vol. 1, no. 3, pp. 130–138, 2020, doi: 10.33096/busiti.v1i3.834.

[5] I. Riadi, Sunardi, and Sahiruddin, "Analisis Forensik Pada Platform Android Menggunakan Metode NIJ," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, pp. 87–95, 2019.

[6] K. Gupta, C. Varol, and B. Zhou, "Digital forensic analysis of discord on google chrome," *Forensic Sci. Int. Digit. Investig.*, vol. 44, p. 301479, 2023, doi: 10.1016/j.fsidi.2022.301479.

[7] A. Yudhana, I. Riadi, and I. Zuhriyanto, "Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," *J. TECHNO*, vol. 20, no. 2, pp. 125–130, 2019.

[8] R. M. Ummairah and A. Julianto, "Basmi Materi Pelecehan Seksual Anak, Discord Rilis Dua Fitur Keamanan Baru," *voi.id*, 2023. https://voi.id/teknologi/321563/basmi-materi-pelecehan-seksual-anak-discord-rilis-dua-fitur-keamanan-baru (accessed Nov. 07, 2023).

[9] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," *NIST Spec. Publ.*, no. August, pp. 800–886, 2006, doi: 10.6028/NIST.SP.800-86.

[10] T. Rochmadi, "Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar," *Indones. J. Bus. Intell.*, vol. 1, no. 1, p. 32, 2019, doi: 10.21927/ijubi.v1i1.878.

[11] H. Ibrahim, H. G. Yavuzcan, and M. Ozel, "Digital forensics : An Analytical Crime Scene Procedure Model (ACSPM)," *Forensic Sci. Int.*, vol. 233, no. 1–3, pp. 244–256, 2013, doi: 10.1016/j.forsciint.2013.09.007.

[12] Subektiningsih, Y. Prayudi, and I. Riadi, "Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 3, pp. 294–304, 2018, doi: 10.17781/p002463.

[13] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.