JURNAL ILMIAH TEKNOLOGI INFORMASI DAN KOMUNIKASI (JTIK) VOL 15, No.1, Maret 2024, pp. 98 - 111
p-ISSN : 2087-0868 (media cetak)
e-ISSN : 2598-9707 (media online)
http://ejurnal.provisi.ac.id/index.php/JTIKP

ANALISIS BUKTI DIGITAL PADA APLIKASI DISCORD DESKTOP DENGAN MENGGUNAKAN FRAMEWORK DFRWS

Mukti Wibowo[1], Mohammad Raffli Firmansyah[2], Rezar Surya Efendi[3]
[1]Politeknik Siber dan Sandi Negara
Bogor, Jawa Barat, Indonesia, (0251) 8541754, e-mail: mukti.wibowo@student.poltekssn.ac.id
[2] Politeknik Siber dan Sandi Negara
Bogor, Jawa Barat, Indonesia, (0251) 8541754, e-mail: mohammad.raffli@student.poltekssn.ac.id
[3] Politeknik Siber dan Sandi Negara
Bogor, Jawa Barat, Indonesia, (0251) 8541754, e-mail: rezar.surya@student.poltekssn.ac.id

ARTICLE INFO

Article history:

Received : 5 – Februari - 2024
Received in revised form : 15 – Februari - 2024
Accepted : 21 – Februari - 2024
Available online : 1 – Maret - 2024

ABSTRACT

A *Currently, various communication platforms are available, and one of them is Discord. Discord is utilized by users to interact and share various types of content. However, Discord is often implicated in the distribution of inappropriate content that goes against Discord regulations. This can lead to cybercrime cases such as Child Sexual Abuse Material (CSAM). The main challenge faced is the recovery of digitally deleted data through these communication platforms. The objective of this research is to analyze digital evidence in the form of deleted text messages, images, and documents in the chat rooms of the desktop-based Discord application. The research method employed is the Live Forensic Technique, applying the DFRWS (Digital Forensics Research Workshop) method. The digital forensic analysis process is conducted using the digital forensic tool Magnet Axiom. The research results indicate that the accuracy of digital evidence analysis using Magnet Axiom reaches 94.11%. A total of 16 digital evidence items were successfully recovered out of the total 17 items available.*

Keywords: Discord, DFRWS, Live forensic, Magnet Axiom

1. PENDAHULUAN

Layanan teknologi sedang berkembang, termasuk pengembangan pesan instan. Discord merupakan salah satu aplikasi layanan pesan instan yang sangat populer digunakan. Menurut Tom's Guide, Discord menjadi aplikasi layanan perpesanan yang populer di kalangan orang-

Received 5 – Februari - 2024; Revised 15 – Februari - 2024; Accepted 21 – Februari - 2024

p-ISSN : 2087-0868 e-ISSN : 2598-9707

orang yang gemar bermain permainan *online* dan streaming pada layanan Twitch. Namun karena kemudahan penggunaannya, aplikasi ini juga populer digunakan oleh banyak orang dari kalangan lainnya sebagai aplikasi konferensi video. Hingga saat ini, jumlah pengguna Discord yang teregistrasi sudah mencapai lebih dari 196 juta orang [1]. Jumlah aktivitas kriminal di aplikasi Discord meningkat selama beberapa tahun terakhir. Dengan layanan terenkripsinya, discord digunakan sebagai kanal pesan yang mempromosikan praktik-praktik yang dilarang seperti penjualan kartu kredit, narkoba, sumberdaya peretas, dan layanan *doxing* [2]. Bentuk kejahatan lainnya yang sering terjadi di discord adalah kejahatan yang berkaitan dengan *Child Sexual Abuse Material* (CSAM) [3].

Forensik digital bertujuan untuk membantu dalam penemuan dan analisis fakta serta bukti digital terkait suatu kejadian. *Live forensic* adalah teknik yang melibatkan analisis data secara waktu nyata dalam suatu sistem yang biasanya disimpan di RAM atau ditransmisikan melalui jaringan [4].

Dalam penelitian forensik digital, penting untuk memiliki efektivitas, efisiensi, dan pendekatan yang terstruktur, disertai dengan langkah-langkah yang signifikan. Pada penelitian ini kami menggunakan kerangka kerja DFRWS (*Digital Forensics Research Workshop)* sebagai panduan dalam melaksanakan proses forensik digital. DFRWS merupakan *framework* dengan kerangka forensik standar serta konsisten sehingga mudah digunakan pengguna dan mudah dipahami pengguna baik teknis maupun non teknis. Selain itu, framework ini dapat diandalkan untuk menemukan bukti digital dan menyediakan sistem terpusat untuk merekam informasi yang dikumpulkan [5].

Aplikasi yang digunakan untuk melakukan forensik pada penelitian ini adalah Magnet Axiom. Pada penelitian Leonardo [6] penggunaan Magnet Axiom direkomendasikan untuk proses forensik baik dengan akses root ataupun tidak. Pada penelitian Dedek [7] disebutkan bahwa Magnet Axiom teruji dapat mengembalikan berkas data sebanyak 100% dari total 29 berkas yang diujinya. Oleh karena itu pada penelitian ini Magnet Axiom akan digunakan pada proses forensik terhadap aplikasi Discord desktop untuk mengetahui performanya.

Forensik terhadap aplikasi perpesanan Discord telah dilakukan pada beberapa penelitian. Pada penelitian Hendrawan [8], dilakukan analisis bukti digital terhadap Discord *browser-based* dengan metode NIST SP 800-86 dan teknik live forensic. Penelitian ini bertujuan untuk mengembalikan atau memperoleh bukti digital yang terhapus dari Discord *browser-based*. Penelitian ini menggunakan tools forensik FTK Imager, Autopsy, MZ Cache view, dan ChromeCacheView. Hasil dari penelitian ini adalah bukti digital yang telah dihapus berupa pesan teks dan gambar berhasil diperoleh. Informasi lainnya yang berhasil didapatkan berupa *timestamp* dan username pesan teks Discord. Nilai persentase akurasi setiap tools untuk mendapatkan kembali bukti digital meliputi 75% pada Autopsy dan ChromeCacheView, 50% pada FTK Imager, dan 25% pada MZ Cache View. Nilai akurasi perolehan bukti digital MZ Cache View paling kecil di antara *tools* lainnya dikarenakan tools tersebut hanya kompatibel terhadap browser Mozilla Firefox. Pada penelitian Ikram [9], dilakukan forensik terhadap aplikasi Discord dengan metode NIST menggunaakn tools FTK Imager, ChromeCacheView, dan Autopsy untuk menemukan pesan yang dihapus pada kasus kejahatan *sexual harassment* dan distribusi pornografi. Hasil dari penelitian ini menunjukkan tingkat akurasi file yang didapatkan menggunakan FTK Imager mencapai 16,67% dengan variabel yang didapatkan sebagai bukti adalah file gambar. Tingkat akurasi yang dimiliki ChromeCacheView mencapai 73,33% dengan variabel yang didapatkan sebagai bukti adalah file gambar, video, pesan teks, akun dan email. Sementara itu, untuk Autopsy tingkat akurasinya mencapai 33,33% dengan variabel yang didapatkan sebagai bukti adalah file gambar dan email. Berdasarkan hasilnya, penelitian tersebut menyarankan penggunaan ChromeCacheView pada proses forensik file cache dan aplikasi Discord untuk meningkatkan keberhasilan mendapatkan bukti digital utamanya pada kasus *sexual*

p-ISSN : 2087-0868 e-ISSN : 2598-9707

harassment dan distribusi pornografi. Pada penelitian tersebut juga disarankan untuk menguji penggunaan tools lain seperti Magnet Axiom pada skenario kasus yang sama.

Dari uraian yang telah disampaikan di atas, pada penelitian ini digunakan kerangka kerja FDRWS untuk melakukan proses forensik terhadap aplikasi Discord berbasis desktop dengan menerapkan *metode Live forensic*. Tools forensik yang digunakan pada penelitian ini adalah Magnet Axiom. Studi ini difokuskan pada hasil forensik digital dari aplikasi forensik Magnet Axiom terhadap Discord pada desktop yang beroperasi di sistem operasi Windows, dengan tujuan mengidentifikasi bukti aktivitas kriminal yang dilakukan oleh pelaku kejahatan CSAM

2. TINJAUAN PUSTAKA

2.1. Digital Forensic

Digital Forensic merupkan suatu cabang ilmu yang berfokus pada investigasi dan penemuan bukti digital dalam konteks suatu kejadian. Saat penyidik melakukan analisis, penting untuk menduplikasi suatu barang bukti yang ada [10]. Forensik bertujuan untuk mengidentifikasi tindakan dan metode pelaku kejahatan. Digital forensik didefinisikan sebagai metode yang berkaitan dengan pemulihan dan penyelidikan, dengan fokus pada sistem komputer yang menyimpan data yang dapat dijadikan sebagai barang bukti [10].

2.2. Live Forensic

Live forensics merupakan teknik analisis yang berkaitan dengan data yang sedang berjalan pada sistem atau data *volatile* yang disimpan dalam RAM atau berada di jaringan. Penggunaan metode *live forensics* bertujuan untuk mempercepat penanganan insiden, meningkatkan integritas data, dan menggunakan kapasitas memori yang lebih rendah [11]. Terdapat banyak alat (*tools*) yang dapat digunakan dalam melakukan *live forensics* untuk menganalisis data.

2.3. Digital Forensics Research Workshop (DFRWS)

DFRWS merupakan framework dengan kerangka forensik standar serta konsisten sehingga mudah digunakan pengguna dan mudah dipahami pengguna baik teknis maupun non teknis. Selain itu, framework ini dapat diandalkan untuk menemukan bukti digital dan menyediakan sistem terpusat untuk merekam informasi yang dikumpulkan [5]. DFRWS memiliki enam fase, dimulai dari identifikasi, preservasi, pengumpulan, pemeriksaan, analisis, dan fase terakhir yaitu presentasi [12].

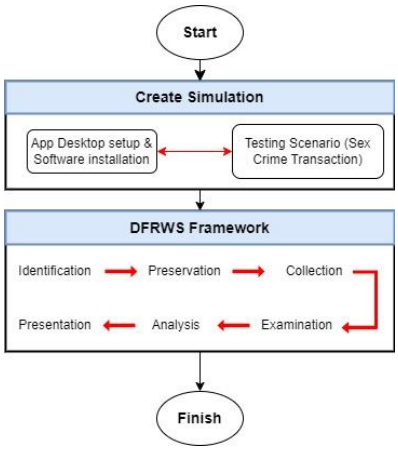
2.4. Discord

Discord merupakan sebuah sarana komunikasi secara digital yang dibuat di Amerika pada tahun 2015. Discord ini sudah sangat familiar dikalangan *gamers* di dunia. Discord juga sama dengan sarana komunikasi digital pada lainnya seperti LINE, Whatssapp, maupun Telegram. Namun discord ini ditujukan untuk sebuah komunitas walaupun ada juga fitur untuk berkomunikasi pribadi. Para pengguna discord sangat menikmati dari fitur – fitur yang disediakan seperti *voice channel* yang bisa digunakan untuk mengobrol lewat suara atau video. Walaupun discord masih baru dan kalah saing dengan platform yang lain, discord merupakan sebuah platform yang sangat menyenangkan apabila digunakan dalam jumlah orang yang banyak. Inovasi yang diberikan oleh discord pun sangat menarik. Selain itu, discord di Indonesia juga sudah mulai populer dikalangan para *influencer, content creator*, komunitas ataupun organisasi sebuah perkumpulan [13].

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan salah satu kerangka kerja digital forensics yaitu DFRWS (*Digital Forensics Research Workshop*). Peneliti merancang tahapan penelitian yang dimulai dari membuat simulasi penelitian, analisis bukti digital dengan kerangka kerja DFRWS, dan yang terakhir hasil dari analisis dan komparasi. Berikut gambar alur proses penelitian dengan menggunakan kerangka kerja DFRWS.

p-ISSN : 2087-0868 e-ISSN : 2598-9707



Gambar 1. Alur Penelitian dengan Kerangka Kerja DFRWS

3.1 Create Simulation

Create Simulation merupakan tahap awal yang bertujuan untuk membuat simulasi penelitian sebagai suatu persiapan dalam memperoleh hasil analisis dari bukti digital. Pada tahap ini terdapat beberapa bagian didalamnya yaitu persiapan aplikasi yang akan dijadikan objek, instalasi *tool* forensik, dan percobaan skenario.

3.1.1. App Desktop Setup and Software Installation

Sebelum menyiapkan simulasi pengujian pada setiap skenario, laptop tetap dalam keadaan menyala karena pada penelitian ini akan dilakukan *live forensic* simulasi pengujian berikutnya dilakukan.

Tabe l. *Software* dan *Hardware*

No	Software dan Hardware	Deskripsi
1	Laptop	MSI Modern A10RAS, Windows 11
2	Discord versi 1.0.9021	Aplikasi perpesanan instan yang digunakan sebagai objek penelitian
3	Magnet Axiom versi 7.8	*Software* yang digunakan untuk mencari dan analisis bukti digital

3.1.2. Testing Scenario

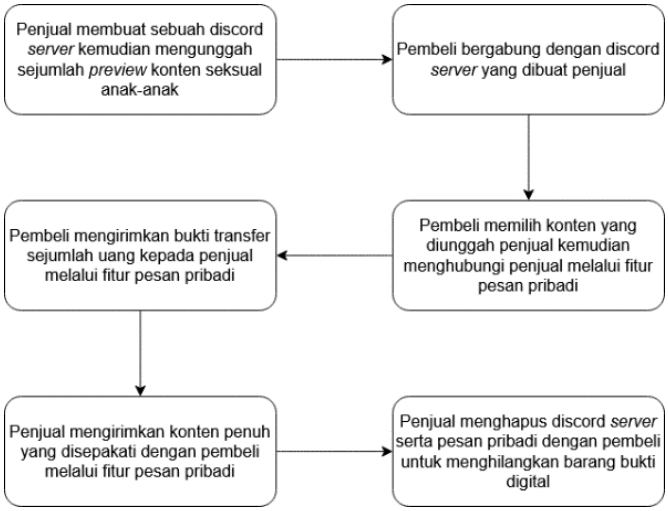
Sebelum dilakukan skenario pengujian, maka dilakukan simulasi skenario kejahatan dengan fitur-fitur yang ada di aplikasi Discord Desktop pada perangkat komputer pelaku. Beberapa fitur telegram yang dilibatkan dalam skenario kejahatan meliputi pengunggahan konten pada Discord server, percakapan pesan pribadi, pesan gambar, pesan video, dan pesan dokumen.

*Child Sexual Abuse Material (*CSAM) merupakan tindak kriminal yang marak terjadi di Discord. Pelaku kejahatan pedofilia memanfaatkan fitur komunitas dan fitur pesan yang tersembunyi pada aplikasi Discord untuk melakukan pertukaran konten seksual anak di bawah umur sebelum menculik anak tersebut, serta menipu dan memeras orang-orang yang mencari konten serupa [3]. Pada penelitian ini akan digunakan skenario kejahatan dari salah satu bentuk kriminalitas CSAM yang paling umum terjadi di Discord yakni transaksi konten seksual yang

p-ISSN : 2087-0868 e-ISSN : 2598-9707

melibatkan anak di bawah umur. Skenario ini melibatkan pihak penjual konten dan pembeli konten. Pihak penjual akan menampilkan konten seksual anak-anak melalui Discord server. Pihak pembeli kemudian akan bertukar pesan melalui fitur pesan pribadi dengan penjual untuk bernegosiasi terkait konten yang dibeli serta pembeli akan mengirimkan bukti transfer sejumlah uang pada transaksi tersebut. Untuk menghindari tuduhan, setelah transaksi penjual akan menghapus discord server serta pesan pribadi dengan pembeli sebagai upaya penghilangan bukti digital.

Gambar 2. Skenario Kejahatan



Gambar 3. Alur Skenario Kejahatan

Pelaksanaan skenario pengujian tidak mempunyai batasan waktu tertentu. Hal ini bertujuan untuk memudahkan dalam pengumpulan dan analisis data dengan menggunakan kerangka kerja DFRWS. Berikut tabel skenario pengujian yang akan dilakukan.

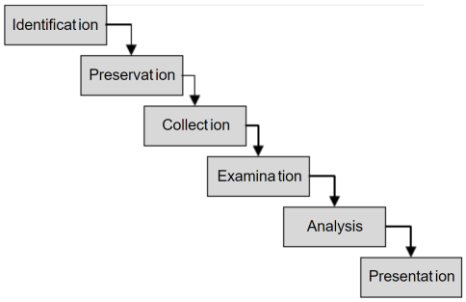
Tabel 2. Percobaan Skenario

Skenario Pengujian	Variabel	Kuantitas Data Pengujian
Penghapusan konten dan percobaan pemulihan dengan Magnet Axiom	Pesan Teks	10 *item*
	Gambar	4 *item*
	Video	2 *item*
	Dokumen pdf	1 *item*

p-ISSN : 2087-0868 e-ISSN : 2598-9707

3.2 Digital Forensics Process

Pada tahap ini akan dilakukan proses forensik digital dengan menggunakan kerangka kerja DFRWS (*Digital Forensics Research Workshop*). Kerangka kerjas DFRWS digunakan dalam proses penyelidikan bukti digital. DFRWS memiliki enam fase, dimulai dari identifikasi, preservasi, pengumpulan, pemeriksaan, analisis, dan fase terakhir yaitu presentasi. Metode DFRWS lebih jelas dan terperinci [12]. Menurut Sunardi [14], tahapan pada metode DFRWS dapat dijelaskan sebagai berikut:



Gambar 4. Proses DFRWS

3.2.1. Identification

Pada tahap ini dilakukan proses identifikasi tentang kebutuhan-kebutuhan apa saja yang harus dipersiapkan dalam melakukan penyelidikan dan pencarian bukti digital.

3.2.2. Preservation

Pada tahap ini dilakukan proses pemeliharaan untuk menjaga bukti-bukti yang telah didapatkan dan memastikan keaslian atau integritas barang bukti agar terhindar dari pihak-pihak yang tidak berkenan, sehingga bukti tidak terkontaminasi dan benar-benar valid/sah.

3.2.3. Collection

Pada tahap ini dilakukan proses pengumpulan sampel-sampel bukti yang diduga berpotensi sebagai barang bukti yang kuat.

3.2.4. Examination

Pada tahap ini dilakukan analisis serta filterisasi data pada bagian tertentu dari sumber data, filterisasi dilakukan dengan syarat tidak mengubah keaslian data.

3.2.5. Analysis

Pada tahap ini dilakukan penentuan tentang asal-usul sumber data, siapa yang menciptakan data tersebut, lokasi data tersebut dihasilkan, bagaimana data tersebut dihasilkan dan alasan mengapa data tersebut dihasilkan.

3.2.6. Presentation

Pada tahap ini merupakan tahap terakhir dengan melaporkan serta mempresentasikan hasil analisis sehingga dapat dipahami oleh publik. Kesimpulan yang didapatkan akan ditulis dengan menghitung presentase dari bukti digital yang ditemukan berdasarkan variabel dan kuantitas bukti digital yang dianalisis dari *tool* yang digunakan.

$$\text{Pft} = \frac{\Sigma DE\ (obtained)}{\Sigma DE\ (required)} x\ 100\%$$

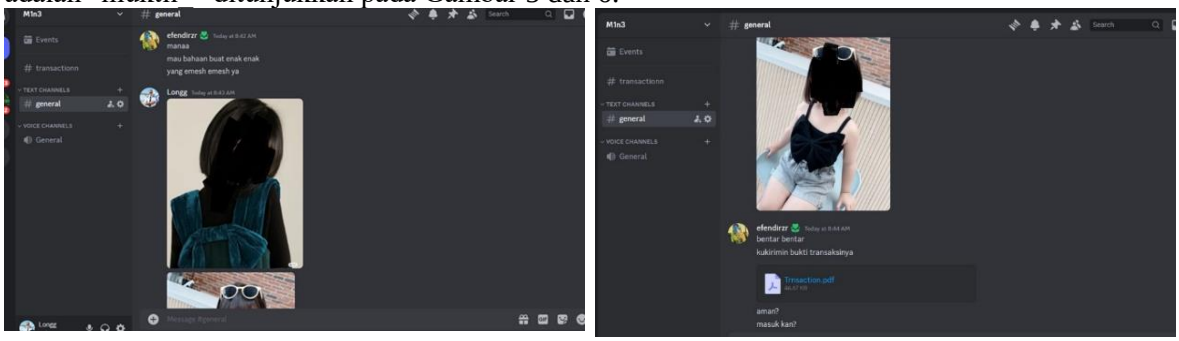
Keterangan:

Pft : Akurasi *forensic tool*
$\Sigma DE\ (obtained)$: Jumlah bukti digital yang diperoleh
$\Sigma DE\ (obtained)$: Jumlah bukti digital yang diperlukan

p-ISSN : 2087-0868 e-ISSN : 2598-9707

4. HASIL DAN PEMBAHASAN

Skenario kejahatan dilakukan oleh dua orang, yaitu orang1 adalah “efendirzr_” dan orang2 adalah “muktii_” ditunjukkan pada Gambar 5 dan 6.



Gambar 5. 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 [15] 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 [16].

4.1. Identification

Tahap identifikasi dimulai sebelum proses forensik dimulai, di mana penyelidik atau pihak yang menyelidiki pertama-tama mengidentifikasi atau menyiapkan data yang diperlukan yang terkait dengan kasus yang sedang diselidiki, kemudian menyiapkan alat forensik yang akan digunakan oleh penyelidik untuk mengambil bukti digital. Bukti digital digunakan oleh penyelidik untuk menjaga integritasnya dan menjamin keasliannya. Beberapa perangkat lunak dan perangkat keras yang diperlukan oleh penyelidik selama proses pencarian bukti digital dapat dilihat di Tabel 3

Tabel 3. Analisis Kebutuhan Penelitian

Hal yang dibutuhkan	Deskripsi	Kategori
Laptop Pelaku	Lenovo Yoga 6, Windows 11	Hardwre
Flashdisk	Sandisk Ultra USB 3.0 64 GB	Hardware
Magnet Axiom	Versi 7.8	Software
Discord Desktop	Instant messages application target (Version 1.0.9021)	Software

Tabel 3 menunjukkan berbagai alat forensik dan peralatan yang diperlukan untuk membantu dalam proses penyelidikan bukti digital. Data dalam tabel 1 menunjukkan bahwa perangkat lunak digunakan untuk membantu menganalisis proses pengambilan bukti digital. Sementara itu, perangkat keras digunakan untuk media yang digunakan penyelidik dalam mendapatkan bukti digital.

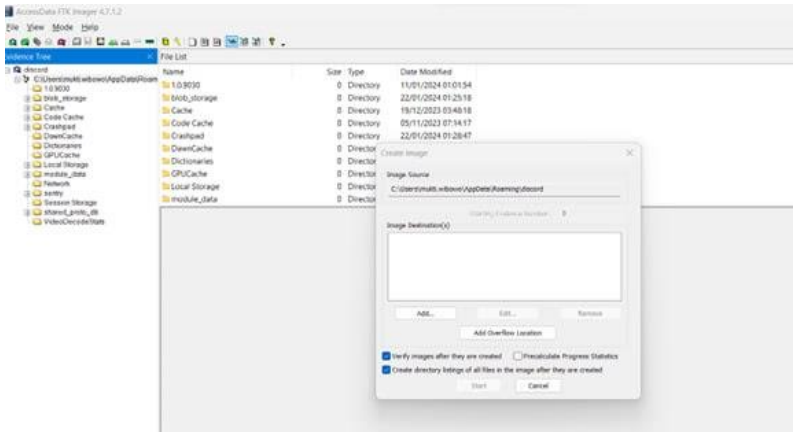
4.2. Preservation

Barang bukti digital memiliki sifat mudah berubah, serta memiliki risiko hilang serta mengalami kerusakan [17]. Oleh karena itu, dilakukan proses pelestarian untuk menjaga dan

p-ISSN : 2087-0868 e-ISSN : 2598-9707

mengamankan keaslian barang bukti fisik yang telah diperoleh pada tahap identifikasi, sehingga integritas data tetap terjaga hingga proses analisis dilakukan. Proses pelestarian dilaksanakan dengan melakukan akuisisi barang bukti menggunakan metode *static acquisition*, yang melibatkan *cloning* atau *imaging* terhadap media penyimpanan data (barang bukti fisik). Proses cloning dilakukan dengan menyalin data secara bitstream image, yang artinya menyalin setiap bit secara berurutan dari data asli, termasuk *temporary file*, *hidden file*, dan bahkan file yang ter-*overwrite* pada media baru.

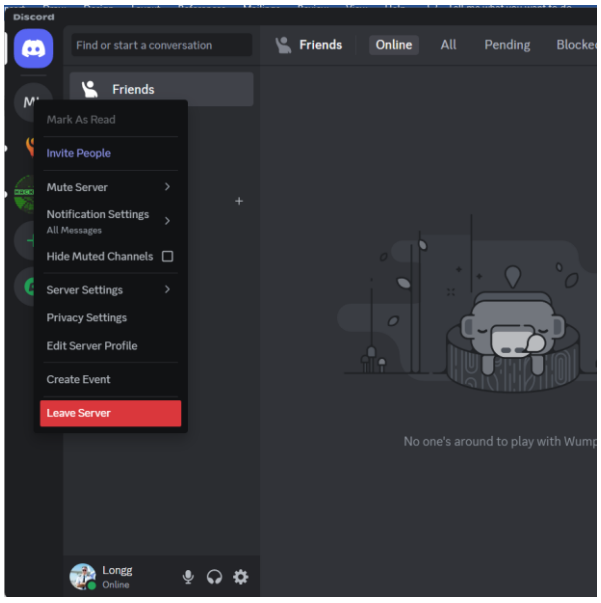
Proses akuisisi data pada barang bukti fisik, seperti flash disk, diimplementasikan dengan menggunakan alat (tool) FTK Imager, sebagaimana terlihat dalam Gambar 7.



Gambar 6. Akuisisi dengan FTK Imager

4.3. Collection

Bukti digital yang dikumpulkan berupa data dalam folder Cache. File yang berada dalam folder tersebut adalah file sementara yang tersimpan pada aplikasi Discord. Berdasarkan skenario, grup dan isi dari percakapan sudah di hapus sehingga pengumpulan bukti ini bertujuan untuk memperoleh isi dari percakapan tersebut, berupa pesan teks, gambar dan file. Pengumpulan bukti dari aplikasi Discord ada dalam direktori C:\Users\mukti.wibowo\AppData\Roaming\discord.

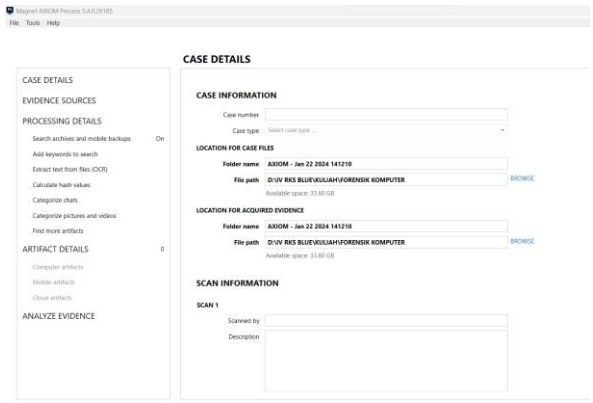


Gambar 7. Keluar dari Server Chat

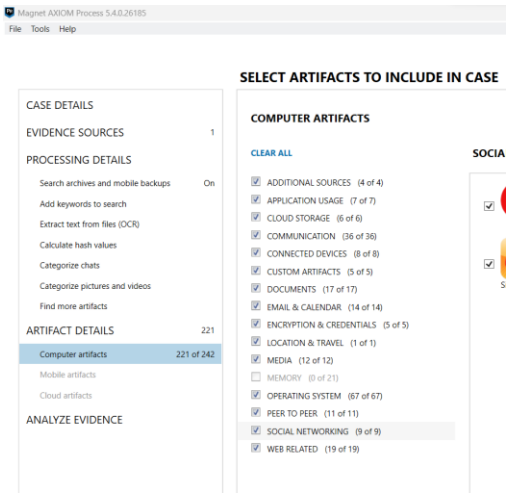
p-ISSN : 2087-0868 e-ISSN : 2598-9707

4.4. Examination

Data yang diperoleh melalui tahap collection, yaitu *file cache* dilakukan pemeriksaan menggunakan Magnet Axiom *forensic tools*. Tujuan dari pemeriksaan ini adalah untuk mendapatkan informasi dari bukti digital yang berupa folder cache dari aplikasi Discord berbasis desktop. Pemeriksaan dimulai dengan menggunakan Magnet Axiom Process dengan membuat *case* baru untuk menyimpan detail informasi dari insiden seperti yang ditunjukkan pada Gambar 9. Selanjutnya, menambahkan sumber bukti pada komputer yaitu folder *cache* discord pada direktori C:\Users\mukti.wibowo\AppData\Roaming\discord. Kemudian untuk pencarian artefak digital pada *case* tersebut dilakukan pemilihan jenis artefak yang akan dicari seperti pada Gambar 10, memasukkan semua jenis artefak agar mendapatkan bukti digital yang maksimal.



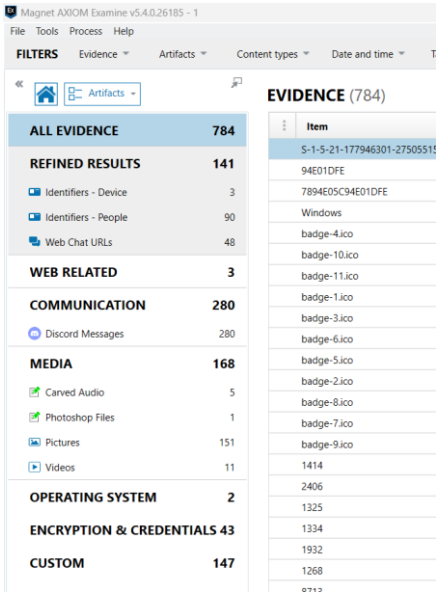
Gambar 8. *Create New Case*



Gambar 9. Pemilihan Jenis Artefak

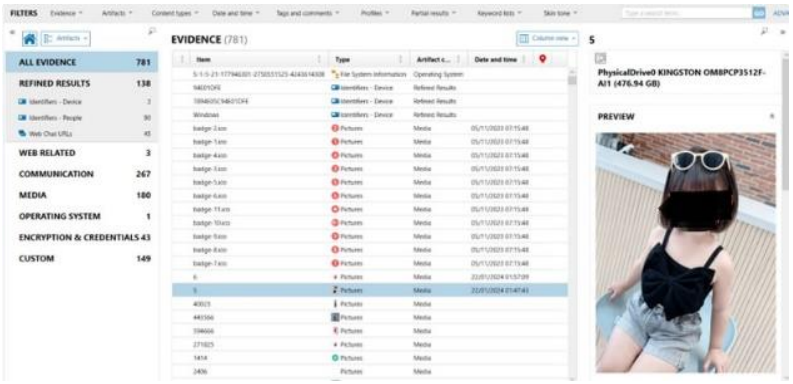
Pemeriksaan dilakukan secara manual dengan mengecek satu per satu pada jenis bukti digital yang didapatkan.

p-ISSN : 2087-0868 e-ISSN : 2598-9707

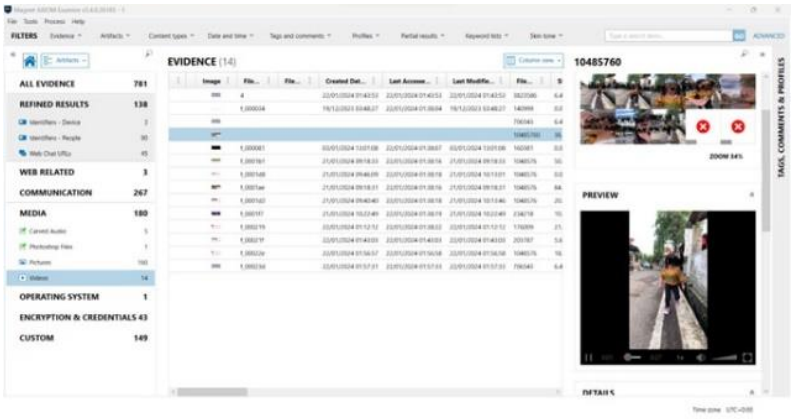


Gambar 10. Hasil Pemeriksaan Bukti Digital

Pada pemeriksaan pertama ditemukan beberapa file gambar dan video pada bukti digital "MEDIA" yang dikirimkan oleh "muktii_". Temuan ini ditunjukkan pada beberapa gambar berikut.



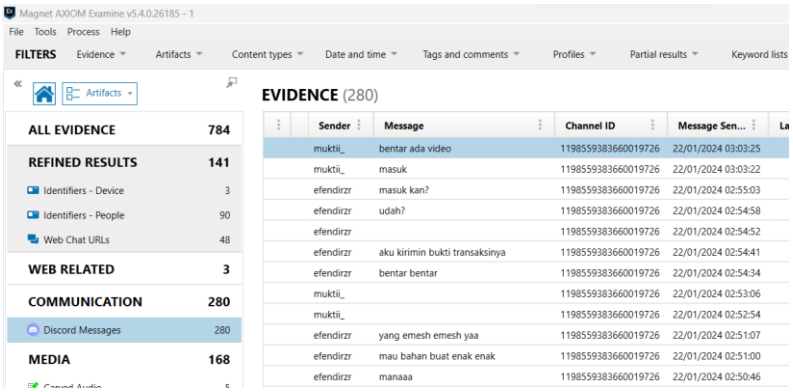
Gambar 11. Bukti Digital Gambar



p-ISSN : 2087-0868 e-ISSN : 2598-9707

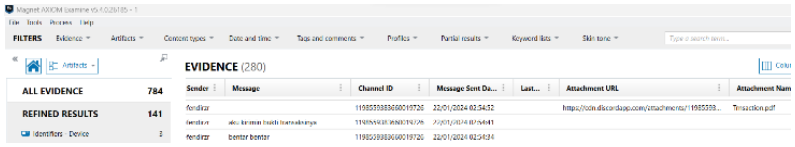
Gambar 12. Bukti Digital Video

Hasil percakapan antara “efendirzr_” dan “muktii_” ditemukan pada bukti digital “COMMUNICATION”. Terlihat ada 4 file gambar, 2 video, 1 dokumen pdf yang ada dalam percakapan tersebut.



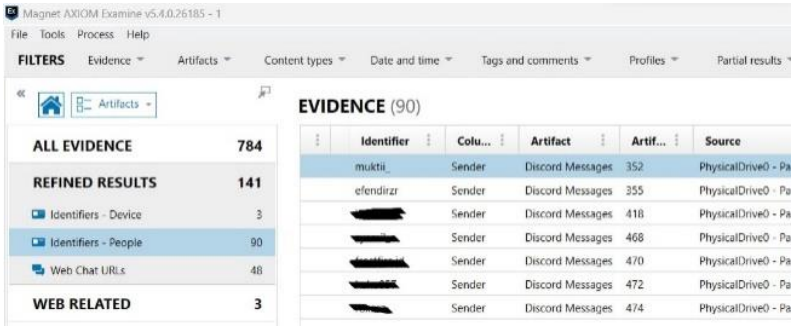
Gambar 13. Bukti Digital Percakapan

Dalam setiap baris percakapan berisi detail pesan yang dikirimkan oleh pengguna Discord. Pemeriksaan dilakukan pada setiap baris percakapan. Dalam baris percakapan berisi beberapa informasi penting seperti Sender, Message, Channel ID, Message Sent Date/Time, Attachment URL, dan Attachment Name. Sender berisi username dari pelaku kejahatan. Message berisi percakapan antara pelaku kejahatan. Sedangkan Attachment Name berisi keterangan file yang dikirimkan seperti pada Gambar 15, pelaku mengirimkan file transaksi dalam format pdf.



Gambar 14. Attachment Transaction File

Pada Evidence Magnet Axiom juga didapatkan akun pengguna discord pada bagian “Identifiers – People”. Temuan ini dapat dilihat pada Gambar 16.



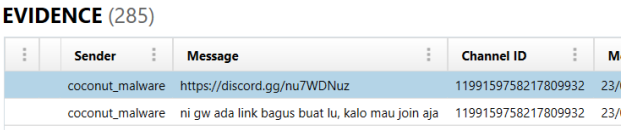
Gambar 15. Akun Pengguna Discord

4.5. Analysis

Tahap analisis dilakukan menggunakan *forensic tools* Magnet Axiom untuk memperoleh semua informasi yang dapat dijadikan pembuktian insiden. Analisis dilakukan untuk mencari

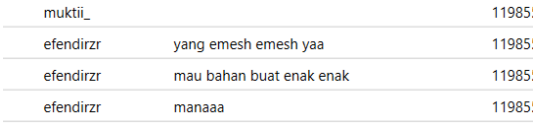
p-ISSN : 2087-0868 e-ISSN : 2598-9707

informasi berdasarkan data hasil pemeriksaan. Skenario dimulai oleh user “coconut_malware” yang men-*dirrect message* dengan inti pesan berupa ajakan untuk bergabung ke server yang berisi konten konten seksual pedofilia kepada user “efendirzr”, dapat dilihat pada Gambar 17.



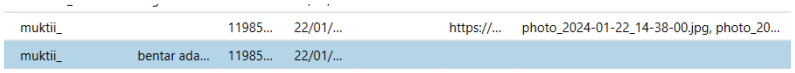
Gambar 16. Pesan Ajakan untuk Masuk ke Dalam Server Konten Pedofilia

Skenario berlanjut ketika user “efendirzr” bergabung ke server discord tersebut. Selanjutnya user “efendirzr” meminta konten-konten yang dijanjikan, dapat dilihat pada Gambar 18 berupa pesan yang dikirimkan oleh user “efendirzr”.



Gambar 17. Pesan Permintaan Konten dari User "efendirzr"

Kemudian dibalas oleh admin server atas nama “mukti” dengan konten seksual pedofilia bersamaan dengan itu user “efendirzr” melakukan transaksi pembayaran untuk mendapatkn konten konten tersebut dengan mengirimkan bukti pembayaran di server, yaitu file transaction.pdf, kemudian admin melanjutkan mengirimkan beberapa foto dan video. Selanjutnya untuk menghapus jejaknya, user “efendirzr” tersebut keluar dari server tersebut.



Gambar 18. Pengiriman Gambar dan Video dari Admin

Dalam pemeriksaan menggunakan Magnet Axiom ditemukannya seluruh isi percakapan dari proses transaksi konten seksual pedofilia yang dilakukan, bukti digital yang ditemukan dijelaskan pada Tabel 4.

4.6. Presentation

Berdasarkan proses forensik digital menggunakan Metode DFRWS (Digital Forensics Research Workshop) berhasil memperoleh bukti digital berdasarkan pesan yang telah dihapus pada discord berbasis desktop. Perolehan bukti digital dilakukan menggunakan tools forensik Magnet Axiom.

Bukti digital yang diperoleh pada Magnet Axiom ditunjukkan pada Tabel 4 Presentase *akurasi forensic tool* pada Magnet Axiom ditunjukkan pada Tabel 5.

Tabel 4. Perolehan Bukti Digital Pada Magnet Axiom Sesuai Kuantitas Variabel Pengujian

Temuan Bukti Digital (variabel)	Kuantitas	Parameter	Magnet Axiom
Pesan Teks	10 / 10	*deleted*	√
Gambar	4 / 4	*deleted*	√
Video	2 / 2	*deleted*	√
Dokumen	0 / 1	*deleted*	-

p-ISSN : 2087-0868 e-ISSN : 2598-9707

Pada pencarian bukti digital menggunakan Magnet Axiom didapatkan bukti digital yang lengkap berupa pesan teks, gambar, dan video. Sedangkan untuk dokumen yaitu file pdf hanya ditemukan dalam bukti pesan teks pada bagian attachment seperti yang sudah dijelaskan pada bagian analisis. File pdf tersebut tidak dapat terbaca sebagai bukti pada jenis bukti digital "Documents" yang ada di Magnet Axiom.

Tabel 5. Presentase Akurasi Perolehan Bukti Digital Pada Magnet Axiom

Presentase Akurasi	Magnet Axiom
$\Sigma DE\ (obtained)$	16
$\Sigma DE\ (required)$	17
Pft	16/17 x 100% = 94,11 %

Penggunaan *tools forensic* Magnet Axiom mempunyai nilai akurasi yang tinggi sebesar 94,11% dikarenakan 16 bukti digital dapat ditemukan dari total 17 bukti digital yang dijadikan variabel.

5. KESIMPULAN DAN SARAN

Teknik *live forensic* diterapkan pada platform Discord berbasis desktop untuk memperoleh bukti digital yang telah dihapus oleh pengguna. Eksperimen dilakukan dengan penyusunan skenario kejahatan CSAM. Proses forensik menggunakan *tool* Magnet Axiom dengan menerapkan metode DFRWS dengan tahapan *identification, preservation, collection, examination, analysis,* dan *presentation*. Berdasarkan hasil proses forensic digital diperoleh bukti digital berupa pesan teks, gambar, dan video yang telah dihapus dari platform Discord. Sedangkan untuk dokumen yaitu file pdf hanya ditemukan dalam bukti pesan teks pada bagian attachment seperti yang sudah dijelaskan pada bagian analisis. File pdf tersebut tidak dapat terbaca sebagai bukti pada jenis bukti digital "Documents" yang ada di Magnet Axiom. Sedangkan informasi lain yang dapat diperoleh adalah username akun, tanggal dan waktu, dan lampiran file dari chat pada Discord. Nilai Persentase akurasi tools Magnet Axiom sebesar 94,11 % dengan temuan bukti digital 16 item dari total 17 item. Penelitian selanjutnya dapat dikembangkan dengan teknik atau metode yang berbeda untuk memperoleh bukti digital yang lebih bervariasi. Selain itu, dapat juga dikombinasikan dengan menggunakan berbagai *tools* forensik yang ada untuk mengkomparasi hasil dari setiap *tools* terhadap bukti digital yang ditemukan.

6. DAFTAR PUSTAKA

[1] A. Wawro, "Discord: Everything You Need to Know." Accessed: Jan. 22, 2024. [Online]. Available: https://www.tomsguide.com/us/what-is-discord,review-5203.html

[2] CloudSek, "The Rise of Cybercrime on Telegram and Discord and the Need for Continuous Monitoring." Accessed: Jan. 22, 2024. [Online]. Available: https://www.cloudsek.com/blog/the-rise-of-cybercrime-on-telegram-and-discord-and-the-need-for-continuous-monitoring

[3] B. Goggin, "Child predators are using Discord, a popular app among teens, for sextortion and abductions." Accessed: Jan. 22, 2024. [Online]. Available: https://www.nbcnews.com/tech/social-media/discord-child-safety-social-platform-challenges-rcna89769

[4] S. Azizah, S. A. Ramadhona, and K. W. Gustitio, "Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST," REPOSITOR, vol. 2, no. 10, pp. 1400–1405, 2020.

[5] Sunardi, I. Riadi, and M. Hajar Akbar, "Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS," JURNAL RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 1, no. 3, pp. 576–583, 2017.

[6] A. Leonardo and R. Indrayani, "The Comparison Performance of Digital Forensic Tools Using Additional Root Access Options," Jurnal Ilmiah Teknik Elektro Komputer dan Informatika, vol. 7, no. 3, p. 512, Jan. 2022, doi: 10.26555/jiteki.v7i3.22381.
[7] D. Julian, A. Wijaya, and T. Sutabri, "Perbandingan Kinerja Aplikasi Pengembalian Data Untuk Digital Forensik Dengan Metode National Institute of Standards and Technology," Digital Transformation Technology (Digitech), vol. 3, no. 1, pp. 210–218, 2023, doi: 10.47709/digitech.v3i1.2727.
[8] M. Y. F. Hendrawan, Subektiningsih, and A. Hadinegoro, "Analisis Bukti Digital Pada Discord Browser Menggunakan Teknik Live Forensic Dengan Metode NIST SP 800-86," Jurnal Infomedia: Teknik Informatika, Multimedia & Jaringan, vol. 8, no. 2, pp. 94–99, 2023.
[9] F. Dzil Ikram and M. Koprawi, "Forensic analysis on discord application using the National Institute of Standards and Technology (NIST) Method," Jurnal Mandiri IT, vol. 12, no. 1, pp. 20–28, 2023, [Online]. Available: www.ejournal.isha.or.id/index.php/Mandiri
[10] P. M. Sulaksono, and B. Santoso, "Static Forensic Pada USB Mass Storage Menggunakan Forensics Toolkit Imager," Jurnal Komputer Terapan vol. 8, no. 1, pp. 132-142, 2022, doi: 10.35143/jkt.v8i1.5334.
[11] R. Umar, A. Yudhana, and M. N. Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," in Prosiding Konferensi Nasional Ke- 4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM), 2016, pp. 207–211.
[12] I. Riadi, A. Yudhana, and G. P. I. Fanani, "Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework," Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 7, no. 2, pp. 286–292, Mar. 2023, doi: 10.29207/resti.v7i2.4547.
[13] Discord. (2022) Company - Discord. https://discord.com/company ((accessed Jan. 21, 2024).
[14] S. Sunardi, I. Riadi, and M. H. Akbar, "Steganalisis Bukti Digital pada Media Penyimpanan Menggunakan Metode Static Forensics," Jurnal Nasional Teknologi dan Sistem Informasi, vol. 6, no. 1, pp. 1–8, May 2020, doi: 10.25077/TEKNOSI.v6i1.2020.1-8.
[15] H. I. Bulbul, 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, Dec. 2013, doi: 10.1016/j.forsciint.2013.09.007.
[16] Subektiningsih, Y. Prayudi, and I. Riadi, "Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation," International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 7, no. 3, pp. 294–304, 2018, [Online]. Available: https://www.researchgate.net/publication/326741793
[17] A. Syauqi, I. Riadi, and Y. Prayudi, "Validasi Policy Statement pada Lemari Penyimpanan Bukti Digital (LPBD)," Journal of Education Informatic Technology and Science (JeITS), vol. 1, no. 2, pp. 27–37, 2019.