CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 9, No. 1, Mei 2026, hlm. 43-53

Analisis Forensik Digital Terhadap Kasus *Phishing* Pada Discord *Mobile* Menggunakan Metode OSCAR

Zulki Yanto Rivai[1], Anton Yudhana[2], Imam Riadi[3]

[1]Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[3]Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
Email: [1]zulki.rivai@gmail.com, [2]eyudhana@ee.uad.ac.id, [3]imam.riadi@is.uad.ac.id

Abstrak

Phishing merupakan bentuk kejahatan siber berbasis rekayasa sosial yang banyak memanfaatkan platform komunikasi digital, termasuk Discord *Mobile*. Penelitian ini bertujuan untuk menganalisis bukti digital pada kasus *phishing* di aplikasi Discord *Mobile* melalui penerapan metode OSCAR (*Obtain, Strategize, Collect, Analyze, Report*). Penelitian dilakukan menggunakan pendekatan eksperimental berupa simulasi skenario *phishing* pada perangkat Android yang telah di-*root*. Proses akuisisi dilakukan melalui teknik akuisisi fisik dengan memanfaatkan dua perangkat lunak forensik digital, yaitu *Oxygen Forensic Detective* dan *Mobiledit Forensic Express*. Artefak digital yang dianalisis meliputi komunikasi berbasis teks, tautan *phishing*, serta file media berupa gambar, video, dan dokumen PDF yang diekstraksi dari aplikasi Discord. Analisis difokuskan pada kemampuan masing-masing alat forensik dalam mengidentifikasi dan mengekstraksi artefak digital yang relevan dengan skenario kasus. Hasil penelitian menunjukkan bahwa *Oxygen Forensic Detective* memiliki tingkat efektivitas ekstraksi sebesar 86,3%, khususnya pada artefak komunikasi dan tautan *phishing*, sedangkan *Mobiledit Forensic Express* hanya mencapai efektivitas sebesar 18,1% namun lebih unggul dalam pemulihan file media. Perbedaan hasil tersebut dipengaruhi oleh kemampuan masing-masing alat dalam mengakses dan menganalisis struktur basis data aplikasi Discord. Penelitian ini menyimpulkan bahwa penerapan metode OSCAR dengan pendekatan multi-*tool* mampu meningkatkan kelengkapan dan keandalan hasil investigasi forensik digital pada kasus *phishing* di platform Discord *Mobile*.

Kata kunci: Forensik Digital, Discord, *Phishing,* OSCAR, *Mobiledit Forensic Express*, *Oxygen Forensic Detective*

Digital Forensic Analysis of Phishing Cases on Discord Mobile using OSCAR Method

Abstract

Phishing is a form of cybercrime based on social engineering that is increasingly common on digital communication platforms, including Discord Mobile. This study aims to analyze digital evidence in phishing cases on the Discord Mobile application by applying the OSCAR (Obtain, Strategize, Collect, Analyze, Report) method. The research method was carried out through a simulation of a phishing case scenario on a rooted Android device, with physical acquisition using two digital forensic tools, namely Oxygen Forensic Detective and Mobiledit Forensic Express. The data analyzed included communication artifacts and digital media in the form of chats, phishing links, images, videos, and PDF documents obtained from the Discord application. The analysis process focused on the ability of each forensic tool to extract and identify digital artifacts relevant to the case scenario. The results of the study show that Oxygen Forensic Detective has a digital evidence extraction effectiveness rate of 86.3%, especially for text-based communication artifacts and phishing links, while Mobiledit Forensic Express only achieved an effectiveness rate of 18.1% and was superior in recovering media files such as images, videos, and documents. Each tool's ability to access and analyze the Discord application database influences this effectiveness difference. The conclusion of this study indicates that the application of the OSCAR method combined with a multi-tool approach can improve the completeness and reliability of digital forensic investigation results in phishing cases on the Discord Mobile platform.

Keywords*: Digital Forensic, Discord, Phishing, OSCAR, Mobiledit Forensic Express, Oxygen Forensic Detective*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa manfaat besar bagi kita dalam berbagai bidang seperti bisnis, pendidikan, dan komunikasi serta hiburan lainnya (Muh et al., 2022). Dalam perkembangan teknologi banyak berkembang aplikasi komunikasi salah satunya Discord. Discord adalah aplikasi gratis untuk mengakses obrolan yang mirip dengan aplikasi jejaring lain seperti *Slack atau Skype*, yang memungkinkan pengguna berbicara secara *real time* menggunakan teks, suara, atau video (Tofik et al., 2024).

Discord memiliki banyak fitur yang membuatnya berbeda dari aplikasi serupa. Salah satu fitur tersebut adalah rapat video, seperti aplikasi *Google Meet* dan *Zoom* (Stephani Tauran & Swandy Aritonang, 2023). Namun aplikasi ini kerap disalah gunakan karena penggunaannya yang cukup populer di kalangan gamers. Bahkan, dalam *platform* Discord terdapat indikasi adanya potensi penyalahgunaan aplikasi untuk aktivitas yang melanggar hukum seperti penipuan, pornografi, sampai dengan pencurian data melalui tautan palsu yang lebih dikenal dengan *phishing* (Yan Fikri Hendrawan et al., 2023).

Pemilihan Discord sebagai objek penelitian didasarkan pada karakteristik teknis dan pola penggunaannya yang berbeda dibandingkan platform komunikasi lain seperti WhatsApp dan Telegram. Discord mendukung komunikasi terbuka melalui *channel* publik dan privat, integrasi tautan eksternal, serta berbagi berkas dalam ekosistem berbasis komunitas yang memungkinkan anonimitas relatif tinggi. Karakteristik tersebut menjadikan Discord lebih rentan terhadap penyebaran *phishing* secara masif dan menghadirkan tantangan forensik tersendiri dalam proses identifikasi, akuisisi, dan analisis bukti digital (Dzil Ikram & Koprawi, 2023).

Menurut Data TECHNICA sebanyak 70000 Data pribadi pemerintah yang bocor karena kejahatan *Phishing* (*Discord Says Hackers Stole Government IDs of 70,000 Users - Ars Technica*, n.d.). *Phishing* merupakan salah satu jenis serangan rekayasa sosial yang bertujuan untuk mengelabui korban agar memberikan informasi sensitif seperti nama pengguna, kata sandi, atau informasi pribadi lainnya. *Phishing* sebagai salah satu bentuk kejahatan siber merupakan tindakan penipuan yang tidak hanya memalsukan data melalui situs *web* palsu yang menyerupai situs resmi, tetapi juga dilakukan secara ilegal untuk memperoleh informasi pribadi atau rahasia milik korban (Ansyafa et al., 2024).

Dalam konteks penggunaan aplikasi Discord, *phishing* kerap dilakukan melalui pesan langsung (*direct message*) yang berisi tautan mencurigakan atau iming-iming hadiah, seperti *voucher game*, atau peningkatan akun. Pelaku memanfaatkan kepercayaan antar pengguna dalam komunitas Discord untuk menyebarkan tautan palsu yang mengarah ke situs penipuan yang menyerupai tampilan asli dari *website* resmi. Ketika korban memasukkan informasi *login* pada situs tersebut, kredensial mereka akan dicuri dan dapat digunakan untuk mengambil alih akun. Selain itu, akun yang telah diretas seringkali dimanfaatkan kembali untuk menyebarkan *phishing* ke kontak lain secara berantai.

Oleh karena ini diperlukan tindakan untuk mengungkap aktivitas kejahatan digital pada aplikasi *Mobile* (Riadi et al., 2023), (Dzil Ikram & Koprawi, 2023). Pendekatan forensik digital dapat digunakan untuk menemukan insiden atau kejahatan di dunia maya (Yan Fikri Hendrawan et al., 2023). Dalam forensik digital terdapat berbagai cabang spesialisasi, salah satunya adalah *Mobile* forensik. Bidang ini berfokus pada proses identifikasi, ekstraksi, dan pemulihan bukti digital yang tersimpan di perangkat *Mobile*, seperti *smartphone* atau tablet. Tujuannya adalah memperoleh data yang relevan secara forensik dan dapat dipertanggung jawabkan secara hukum dalam proses investigasi (Yudhana et al., 2022).

Salah satu pendekatan sistematis yang digunakan dalam investigasi forensik digital adalah metode OSCAR. Kerangka kerja ini terdiri dari lima tahapan utama: *Obtain, Strategize, Collect, Analyze,* dan *Report*, yang dirancang untuk memandu proses forensik secara terstruktur dan menyeluruh (Agustian Akbar et al., 2024). Metode ini menekankan pentingnya pemahaman konteks insiden sejak awal, strategi yang tepat dalam akuisisi data, hingga pelaporan hasil analisis yang sah secara hukum. OSCAR telah banyak diterapkan dalam berbagai penelitian, termasuk pada analisis insiden siber seperti *phishing* dan penyalahgunaan aplikasi komunikasi digital (Qureshi et al., 2021a).

Data yang telah dihapus menjadi tantangan tersendiri dalam proses forensik digital, terutama karena keterbatasan waktu dalam proses akuisisi data dan kebutuhan akan keahlian teknis untuk menangani dinamika teknologi yang terus berkembang (Dzil Ikram & Koprawi, 2023). Dalam investigasi *phishing* pada aplikasi Discord *Mobile*, fokus analisis tidak hanya terbatas pada data yang secara langsung tersimpan di perangkat, tetapi juga mencakup elemen lain dalam ekosistem aplikasi. Hal ini meliputi rekam jejak aktivitas pengguna, metadata dari pesan yang dikirim maupun diterima, koneksi jaringan yang digunakan selama komunikasi berlangsung, dan informasi tambahan yang mungkin tersimpan di sisi *server* Discord sebagai bagian dari *infrastruktur cloud-based* yang dimilikinya (Kara, 2022), (Wibowo et al., 2024). Kondisi *smartphone* dan alat yang digunakan dalam proses forensik sangat berpengaruh terhadap pengumpulan bukti (Ermin et al., 2023).

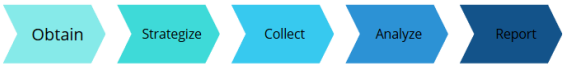
Alat forensik digital seperti *Belkasoft* dan *Mobiledit Forensic Express* telah menjadi fokus penelitian dalam analisis bukti digital. Penelitian sebelumnya menggunakan *Mobiledit Forensic Express* dan *Belkasoft* menunjukan indeks persentase dari barang bukti yang didapat pada *smartphone*

dengan kondisi *root* sebesar 100% dan 83,33 % (Ichsan & Riadi, 2021). *Mobiledit Forensic Express* lebih banyak menemukan data dibandingkan dengan tools *Belkasoft* (Zaida Muflih, 2023).

Penelitian ini dikembangkan dari penelitian sebelumnya yang membandingkan performa alat forensik digital pada perangkat Android dalam proses akuisisi dan analisis bukti digital. Berbeda dengan penelitian terdahulu yang umumnya menggunakan kerangka kerja NIST atau pendekatan konvensional, penelitian ini mengintegrasikan metode OSCAR sebagai kerangka utama investigasi forensik digital. Selain melakukan perbandingan kuantitatif efektivitas *Mobiledit Forensic Express* dan *Oxygen Forensic Detective*, penelitian ini menempatkan analisis artefak dalam konteks kasus *phishing* pada aplikasi Discord *Mobile* dengan mengaitkan hasil ekstraksi pada rekonstruksi *timeline* kejadian, potensi penerapan anti-forensik, serta implikasi *admissibility* bukti digital. Dengan demikian, kebaruan penelitian ini terletak pada integrasi metode, alat, dan analisis artefak berbasis kronologi dalam konteks *phishing* pada platform komunikasi modern.

2. METODE PENELITIAN

Penelitian ini akan menerapkan metode OSCAR yang merupakan salah satu model proses investigasi dalam bidang digital forensik yang dikembangkan untuk membantu penyidik atau analis digital dalam melakukan penanganan terhadap insiden secara sistematis dan terstruktur (Agustian Akbar et al., 2024), yang diilustrasikan pada Gambar 1.



Gambar 1. Metode Penelitian

Pendekatan yang digunakan dalam penelitian ini adalah dengan simulasi skenario penelitian yang dirancang untuk merepresentasikan kasus *phishing* pada aplikasi Discord *Mobile.* OSCAR merupakan nama akronim dari lima tahapan utama, *Obtian, Strategize, Collect, Analyze, Report* yang digunakan dalam proses investigasi digital (Shah, 2023). Gambar 1 dengan penjelasan sebagai berikut:

1. *Obtain,* tahap ini bertujuan untuk melakukan identifikasi awal terhadap keberadaan bukti digital dan mengumpulkan semua yang diperlukan (Yulistina et al., 2025). Biasanya, tentang lokasi dan jenis data yang berpotensi menjadi bukti digital (Agustian Akbar et al., 2024).
2. *Strategize,* pada tahap ini melakukan pembuatan rencana secara rinci tentang bagaimana melakukan penyelidikan. Hal ini dilakukan dengan berbagai kriteria karena bukti dari berbagai sumber memiliki tingkat volatilitas yang berbed (Spiekermann & Keller, 2023).
3. *Collect,* tahap ini melakukan proses akuisisi bukti digital dari perangkat yang terlibat dalam insiden, dengan memastikan metode ekstraksi yang digunakan tidak mengubah data asli (Qureshi et al., 2021). Tahapan ini juga melibatkan evaluasi terhadap konteks insiden, termasuk perolehan dan prioritas sumber bukti, dokumentasi bukti, dan pelestarian bukti asli (FFaizal & Luthfi, 2024).
4. *Analyze*, bukti digital yang telah diamankan kemudian dianalisis menggunakan berbagai teknik digital forensik untuk mengungkap fakta-fakta teknis dari insiden, seperti pelaku, metode serangan, dan dampak yang ditimbulkan (Hidayah et al., 2025).
5. *Report*, tahap akhir adalah menyusun laporan investigasi yang jelas, objektif, dan dapat dipertanggungjawabkan secara hukum. Laporan harus mencakup kronologi kejadian, temuan forensik, metode yang digunakan, dan kesimpulan (Pratama Putra et al., 2024).

Metode ini dikembangkan untuk memastikan bahwa proses pengumpulan, analisis, dan pelaporan bukti digital dilakukan dengan pendekatan yang komprehensif namun tetap menjaga validitas dan integritas data sebagai alat bukti di ranah hukum (Agustian Akbar et al., 2024).

2.1 Alat dan bahan

Proses penelitian ini memerlukan beberapa alat yang dapat dilihat pada Tabel 1.

Tabel 1. Alat Penelitian

No	Perangkat	Sistem Operasi	Status	Kegunaan
1	Redmi 3	Android 6.0.1	*Rooted*	Objek Penelitian
2	Laptop accer	Windows 11 64 bit	AMD RYZEN 3 8.00GB RAM	Workstation untuk analisis forensik
3	USB Conector			Penghubung smartphone dengan workstation

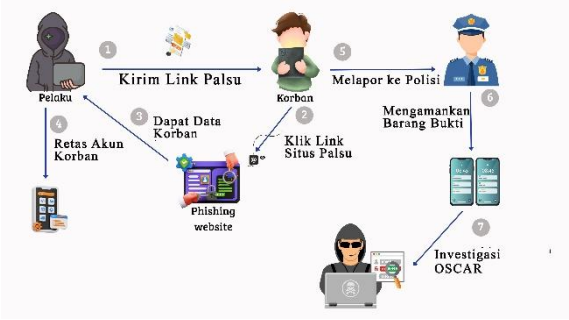
Beberapa *software* yang digunakan pada penelitian ini terbagi menjadi *software test,* sistem operasi, alat forensik, dan alat analisis yang dapat dilihat pada Tabel 2.

Tabel 2. Bahan Pendukung

No	Alat Forensik	Versi	Kegunaan
1	Discord *Mobile*	279.13	*Software test*
2	Windows 11		Sistem operasi *workstation*
3	*Mobiledit Forensic Express*		Alat forensik & analisis
4	*Oxygen Forensic*		Alat forensik & analisis
5	*Android Debugging Bridge*	1.4.3	Komunikasi antara *smartphone* dengan komputer

2.2 Skenario Penelitian

Dalam skenario ini, pelaku memanfaatkan *smartphone* untuk melakukan aksi *phishing* terhadap korban. Setelah pelaku berhasil diamankan, perangkat Android yang digunakan disita sebagai barang bukti guna menunjang proses investigasi dan pembuktian di pengadilan, ilustrasi skenario ditunjukkan pada Gambar 2.



Gambar 2. Skenario Kejadian Kasus *Phishing* Pada Discord

Gambar 2 merupakan skenario kejadian yang mengsimulasikan kasus *phshing* pada Discord dalam 7 tahapan utama, dengan penjelasan sebagai berikut:

1. Pelaku *phishing* mengirim *chat* promosi palsu ke dalam *channel* Discord.
   Pada tahap awal, pelaku menyebarkan pesan promosi palsu ke dalam saluran komunikasi (*channel*) di aplikasi Discord. Pesan tersebut dibungkus dengan iming-iming seperti hadiah gratis untuk menarik perhatian pengguna.
2. Korban klik tautan *phishing* dan mengunjungi situs web palsu.
   Korban yang tertarik dengan isi pesan, menghubungi pelaku melalui pesan pribadi (*direct message*) untuk menanyakan lebih lanjut tentang tawaran. Dalam percakapan ini, pelaku berupaya meyakinkan korban dengan bahasa persuasif dan menciptakan kesan kredibel agar korban bersedia mengisi tautan yang dibagikan. Setelah merasa yakin, korban mengklik tautan dan diarahkan ke situs *web* palsu yang telah disiapkan oleh pelaku. Situs ini dirancang menyerupai situs resmi untuk mengecoh korban agar merasa aman.
3. Pelaku mengumpulkan data penting.
   Saat korban memasukkan informasi pribadi seperti *email*, *username*, dan kata sandi ke dalam situs palsu, data tersebut langsung terekam dan dikumpulkan oleh pelaku. Informasi ini menjadi pintu masuk bagi pelaku untuk mengakses akun korban dan menjalankan aksinya lebih jauh.
4. Pelaku menggunakan identitas korban.
   Setelah memperoleh data kredensial korban, pelaku berpotensi menyamar sebagai korban untuk melakukan berbagai aktivitas ilegal, seperti menyebarkan *phishing* ke pengguna lain, mengakses data pribadi, atau memperjualbelikan akun. Sebagai bagian dari upaya menghindari pelacakan dan memperlambat proses investigasi, pelaku dalam skenario ini diasumsikan melakukan tindakan pasca kejadian berupa penghapusan aplikasi Discord dari perangkat yang digunakan. Tindakan tersebut merepresentasikan potensi penerapan teknik anti-forensik sederhana yang umum dilakukan dalam kasus kejahatan siber berbasis aplikasi komunikasi.
5. Korban melapor ke pihak kepolisian.
   Setelah menyadari bahwa dirinya menjadi korban *phishing*, korban melapor ke pihak kepolisian untuk menindaklanjuti insiden tersebut secara hukum.
6. Polisi menangkap pelaku dan mengumpulkan barang bukti.
   Pihak kepolisian melakukan penyelidikan hingga berhasil menangkap pelaku. Mengamankan barang bukti berupa ponsel milik korban, yang berisi riwayat komunikasi dengan pelaku. Jika memungkinkan, perangkat yang digunakan pelaku juga dikumpulkan sebagai barang bukti untuk dianalisis lebih lanjut.
7. Barang bukti dianalisis menggunakan metode OSCAR.
   Barang bukti yang telah dikumpulkan kemudian dianalisis menggunakan tahapan metode OSCAR, yang terdiri dari lima tahapan utama: *Obtain, Strategize, Collect, Analyze,* dan *Report.*

Proses ini dilakukan dengan bantuan tools seperti *Mobiledit* dan *Oxygen forensic*, yang memungkinkan penyidik untuk mengekstraksi serta menganalisis data dari perangkat *Mobile*, termasuk pemulihan pesan Discord, identifikasi tautan *phishing*, serta pencarian artefak digital yang berkaitan dengan aktivitas pelaku. Hasil dari analisis ini menjadi bukti penting dalam penyelidikan kasus *phishing* melalui aplikasi Discord dan berperan dalam proses penegakan hukum terhadap kejahatan siber yang terjadi pada platform komunikasi digital.

2.3 Metode Perbandingan

Perbandingan ini dilakukan dengan berbagai alat forensik digital berdasarkan data forensik yang tersedia. Tujuan metode ini adalah untuk menentukan hasil analisis dalam bentuk angka kuantitatif dengan menggunakan rumus persentase yang terdapat dalam persamaan (1).

$$P_{ar} = \frac{\sum Vfount}{\sum Vtotal} \; x \; 100 \qquad (1)$$

Keterangan:
P_{ar}= Indeks akurasi alat forensik yang digunakan.
$Vtotal$ = Jumlah parameter material yang terdeteksi.
$Vfount$ = Jumlah total parameter material yang digunakan.

Rumus ini menghitung tingkat akurasi dari alat forensik dengan membandingkan jumlah parameter yang berhasil dideteksi dengan jumlah total parameter yang digunakan. Nilai yang dihasilkan

dinyatakan dalam bentuk persentase, yang menunjukkan seberapa efektif alat forensik dalam mengidentifikasi bukti atau material yang relevan dalam proses investigasi digital (Ayatulloh et al., 2021).

3. HASIL DAN PEMBAHASAN

Studi ini berhasil mendapatkan bukti digital melalui proses analisis dan ekstraksi data pada aplikasi seluler Discord. Hasil analisis akan disajikan menggunakan skema OSCAR.

3.1 *Obtain*

Pada tahap ini, melakukan penelusuran awal terhadap perangkat uji untuk mengetahui lokasi dan jenis data yang berpotensi menjadi bukti digital. Berdasarkan variabel penelitian yang telah ditetapkan, data yang diidentifikasi meliputi *chat*, tautan, gambar, video, dan dokumen berformat PDF yang terdapat pada aplikasi serta media penyimpanan perangkat. Hasil identifikasi awal tersebut menjadi dasar dalam proses akuisisi data yang disajikan pada Tabel 3.

Tabel 3. Data Barang Bukti

No	Kategori Data	Total Data
1	*Chat*	17
2	Tautan	1
3	Gambar	2
4	Video	1
5	Dokumen (pdf)	1

Tabel 3 menampilkan parameter penelitian yang menjadi fokus pencarian pada perangkat smartphone pelaku dalam kasus *phishing* melalui aplikasi Discord. Parameter tersebut digunakan sebagai acuan utama dalam proses investigasi untuk mengidentifikasi dan memperoleh bukti digital yang relevan. Setiap parameter mencakup jenis data penting seperti *chat,* tautan, gambar, video, dan dokumen berformat PDF yang berpotensi menunjukkan aktivitas *phishing* yang dilakukan. Peneliti memanfaatkan parameter ini untuk menelusuri jejak digital komunikasi dan pertukaran *file* yang terjadi pada aplikasi Discord. Seluruh data yang berhasil ditemukan kemudian dianalisis menggunakan perangkat lunak forensik digital sesuai kebutuhan penyelidikan. Keberadaan data yang sesuai dengan parameter penelitian menjadi faktor penting dalam menentukan arah serta hasil analisis forensik. Adapun perangkat pelaku yang dijadikan sumber bukti digital ditampilkan secara rinci pada Gambar 3.

Gambar 3. Barang Bukti Fisik

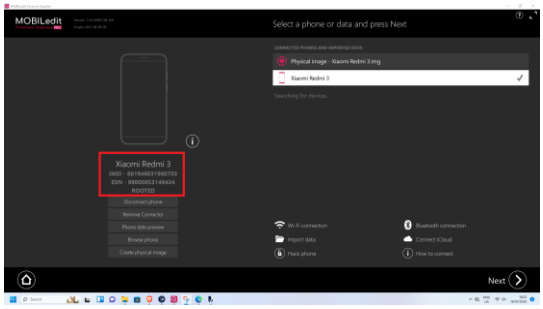
Gambar 3 memperlihatkan perangkat *smartphone* Android yang digunakan sebagai objek utama dalam penelitian ini, sekaligus menjadi bukti fisik pada kasus *phishing* yang dilakukan melalui aplikasi Discord. Perangkat tersebut merupakan milik pelaku simulasi kasus dan berfungsi sebagai sumber utama perolehan data digital. Ponsel berada dalam kondisi sudah dilakukan proses *root* untuk memberikan akses penuh terhadap sistem *file* selama akuisisi data, sehingga memungkinkan pengambilan artefak digital secara menyeluruh dari aplikasi Discord.

3.2 *Strategize*

Pada tahap ini, Dilakukan penyusunan pendekatan teknis yang sistematis agar proses akuisisi dan analisis bukti digital dapat berjalan efektif dan sesuai dengan tujuan penelitian.

Fokus utama strategi ini adalah membuktikan efektivitas metode akuisisi fisik (*physical acquisition*) dalam memperoleh artefak digital dari aplikasi Discord yang digunakan dalam simulasi kasus *phishing*. Perangkat uji yang digunakan adalah *smartphone* Redmi 3 dalam kondisi sudah di-*root*, sehingga memungkinkan akses penuh terhadap sistem *file* internal. Pemilihan kondisi *rooted* dilakukan dengan tujuan memaksimalkan kemungkinan pengambilan data, termasuk *file* yang tersembunyi atau sudah dihapus. Dalam strategi ini, juga menetapkan variabel utama bukti digital yang akan dicari, yaitu *chat*, gambar, video, dan dokumen PDF, yang merepresentasikan aktivitas komunikasi dan interaksi pada aplikasi Discord.

1. Persiapan Perangkat dan Deteksi Awal
   Langkah pertama dalam tahap strategi adalah memastikan bahwa perangkat uji dapat terdeteksi dengan baik oleh perangkat lunak forensik. Proses ini dilakukan dengan menghubungkan smartphone Redmi 3 ke komputer menggunakan kabel USB, kemudian menjalankan aplikasi *Mobiledit Forensic Express* untuk memverifikasi konektivitas perangkat sampai ada tampilan seperti pada Gambar 4.

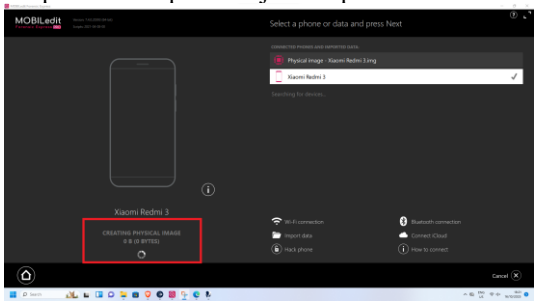


Gambar 4. Perangkat Redmi 3 Terdeteksi *Rooted*

Gambar 4 memperlihatkan kondisi awal ketika perangkat berhasil terbaca dalam keadaan *rooted*, yang menandakan bahwa sistem siap untuk dilakukan akuisisi fisik. Kondisi ini merupakan bagian penting dari strategi awal, karena memastikan perangkat

forensik dapat mengakses seluruh struktur data internal tanpa batasan sistem operasi.

2. Penentun Metode Akuisisi
   Langkah berikutnya adalah menentukan metode akuisisi yang akan digunakan. Berdasarkan rancangan strategi, metode *physical acquisition* dipilih karena mampu menyalin seluruh isi memori internal perangkat dalam bentuk citra digital (*image file*) yang utuh. Tampilan awal pemilihan opsi ditunjukkan pada Gambar 5.



Gambar 5. *Create Physical Image* pada *Mobiledit Forensic Express*.

Gambar 5 menunjukkan tahap pemilihan opsi *Create Physical Image* pada aplikasi *Mobiledit Forensic Express* sebagai bagian dari rencana akuisisi. Tahap ini menandai kesiapan sistem untuk melakukan proses pencitraan data (*imaging*) secara menyeluruh pada tahap berikutnya (*Collect*).

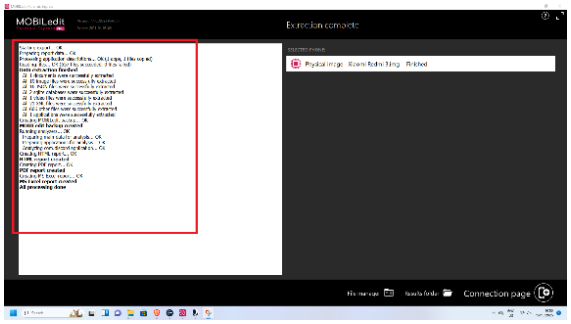
3. Rencana Eksekusi dan Pembagian Peran *Tools*
   Dalam tahap perencanaan strategi, peneliti menetapkan penggunaan dua perangkat lunak forensik, yaitu *Mobiledit Forensic Express* v7.4.0 dan *Oxygen Forensic Detective* v17.1.0, yang dijalankan secara terpisah pada perangkat uji yang sama. Kedua *tools* tersebut diterapkan untuk melakukan akuisisi fisik guna memperoleh citra lengkap dari memori perangkat sebagai dasar analisis forensik.
   Pendekatan ini dirancang untuk membandingkan keefektifan masing-masing tools dalam mengekstraksi artefak digital yang berkaitan dengan simulasi kasus *phishing* pada aplikasi Discord.

Seluruh strategi yang telah direncanakan pada tahap ini menjadi dasar pelaksanaan proses akuisisi data pada tahap *Collect*. Dengan memastikan kesiapan perangkat, pemilihan metode yang tepat, serta pembagian fungsi masing-masing *tools,* peneliti dapat melanjutkan proses investigasi secara sistematis tanpa mengubah integritas data digital pada perangkat uji.

3.3 *Collect*

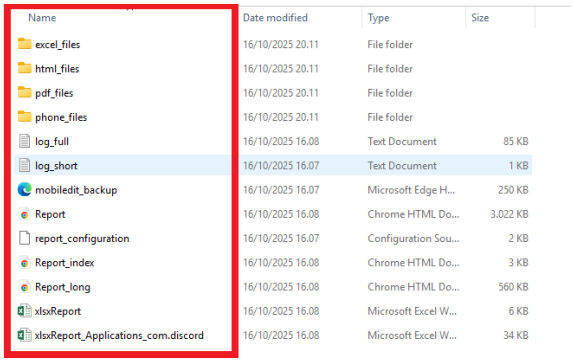
Tahap *Collect* merupakan proses pengumpulan bukti digital yang telah ditentukan pada tahap *Strategize*. Fokus utama tahap ini adalah melaksanakan akuisisi data secara fisik dari perangkat uji menggunakan dua alat forensik, yaitu *Mobiledit Forensic Express* v7.4.0 dan *Oxygen Forensic Detective* v17.1.0**.**

Langkah pertama dalam tahap *Collect* dilakukan dengan menjalankan akuisisi fisik melalui *Mobiledit Forensic Express*. Metode *physical acquisition* dipilih karena mampu menyalin seluruh isi memori internal perangkat dalam bentuk citra digital (*image file*). Selama proses berlangsung, perangkat lunak menampilkan status aktivitas dan estimasi waktu yang dibutuhkan untuk menyelesaikan proses pencitraan. Gambar 6 menunjukkan tampilan proses akuisisi yang sudah berhasil.



Gambar 6. Proses Akuisisi *Mobiledit Forensic Express*

Gambar 6. menampilkan proses akuisisi selesai, *Mobiledit Forensic Express* menghasilkan struktur folder berisi berkas hasil ekstraksi yang mencakup berbagai format *file*, seperti laporan (*Report*), log aktivitas proses ekstraksi (*log_full, log_short*), serta direktori yang memuat hasil konversi data ke dalam bentuk Excel, HTML, PDF, dan *phone_files*. Seluruh berkas berfungsi sebagai hasil keluaran yang mendokumentasikan isi memori perangkat secara terstruktur dan siap untuk dianalisis lebih lanjut seperti pada Gambar 7.

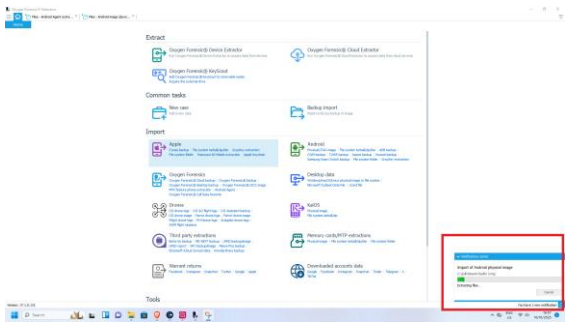


Gambar 7. File Hasil Ekstraksi *Mobiledit Forensic Express*

Gambar 7 memperlihatkan tampilan hasil akhir proses akuisisi, di mana seluruh data hasil ekstraksi telah tersimpan dalam direktori kasus. Berkas-berkas tersebut menjadi bahan utama dalam tahap analisis, guna menelusuri bukti digital seperti percakapan, gambar, video, dan dokumen PDF yang relevan dengan skenario penelitian.

Sebagai pembanding, proses akuisisi juga dilakukan menggunakan *Oxygen Forensic Detective* dengan metode serupa. *Oxygen* melakukan proses ekstraksi terhadap seluruh sistem *file* dan area penyimpanan aplikasi, termasuk data pengguna, *log*

aktivitas, dan artefak komunikasi. Proses akuisisi menggunakan *Oxygen Forensic Detective* dapat dilihat pada Gambar 8.

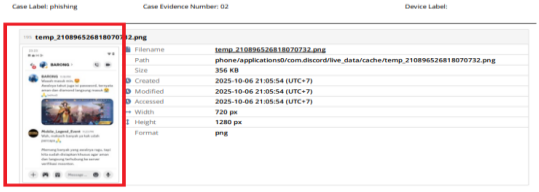


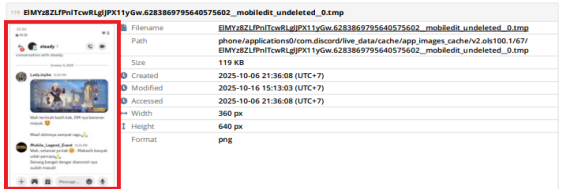
Gambar 8. Proses Akuisisi *Oxygen Forensic Detective*

Gambar 8 menunjukkan proses akuisisi data menggunakan *Oxygen Forensic Detective* yang berlangsung secara otomatis hingga seluruh data perangkat berhasil disalin dan disimpan dalam format yang siap dianalisis pada tahap *Analyze*. Setelah proses akuisisi oleh kedua alat forensik selesai, dilakukan validasi awal untuk memastikan hasil ekstraksi terekam secara utuh dan tidak mengalami perubahan, melalui pemeriksaan metadata, kesesuaian ukuran data dengan kapasitas memori perangkat, serta identifikasi potensi kesalahan pembacaan. Langkah ini bertujuan menjaga integritas dan keaslian bukti digital. Tahap *Collect* menghasilkan dua set data digital dari *Mobiledit* dan *Oxygen* yang selanjutnya digunakan sebagai bahan utama pada tahap *Analyze* untuk pemeriksaan, pengelompokan, dan perbandingan efektivitas kedua tools.

3.4 *Analyze*

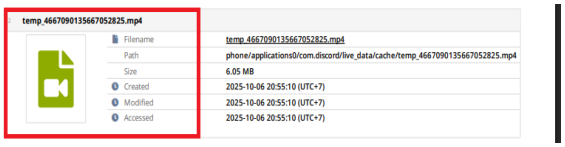
Tahap ini merupakan proses analisis terhadap hasil ekstraksi data yang diperoleh dari perangkat uji menggunakan *Mobiledit Forensic Express* v7.4.0 dan *Oxygen Forensic Detective* v17.1.0. Analisis dilakukan untuk menelusuri artefak digital yang relevan dengan variabel penelitian, yaitu *chat*, gambar, video, dan dokumen PDF, yang berasal dari aktivitas komunikasi pada aplikasi Discord. Proses ini bertujuan untuk mengidentifikasi bukti digital yang dapat digunakan untuk mendukung skenario kasus *phishing* yang telah disimulasikan. Hasil analisis awal terhadap artefak visual berupa gambar yang berhasil dipulihkan menggunakan *Mobiledit* dapat dilihat pada Gambar 9.





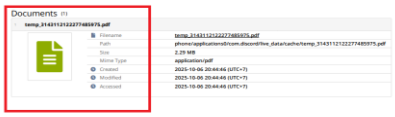
Gambar 9. Bukti Gambar dari *Mobiledit Forensic Express*

Gambar 9 menunjukkan hasil analisis terhadap artefak gambar yang berhasil dipulihkan menggunakan *Mobiledit Forensic Express*. Informasi metadata yang ditampilkan pada hasil ekstraksi meliputi nama *file*, ukuran, serta waktu pembuatan gambar. Data ini penting karena dapat menunjukkan kapan gambar diunggah atau diterima oleh pengguna dalam aplikasi Discord. Metadata tersebut berfungsi sebagai penunjuk waktu aktivitas digital dan membantu memastikan keaslian serta integritas *file* yang diperoleh. Selain artefak gambar, *Mobiledit* juga berhasil mengekstraksi bukti digital berupa video. Hasil pemulihan *file* video tersebut dapat dilihat pada Gambar 10.



Gambar 10. Bukti Video dari *Mobiledit Forensic Express*

Gambar 10 memperlihatkan hasil ekstraksi *file* video dari perangkat yang dianalisis melalui *Mobiledit Forensic Express*. Informasi yang muncul pada hasil analisis mencakup nama *file*, ukuran, durasi, dan waktu pembuatan video. Data tersebut membantu peneliti dalam mengidentifikasi aktivitas komunikasi berupa kiriman media video pada aplikasi Discord yang berkaitan dengan skenario *phishing*. *File* video yang ditemukan menjadi salah satu bukti pendukung untuk menunjukkan adanya interaksi multimedia antara pelaku dan korban dalam percakapan yang disimulasikan. Selain video, *Mobiledit* juga berhasil mengidentifikasi artefak berupa dokumen PDF, seperti ditunjukkan pada Gambar 11.

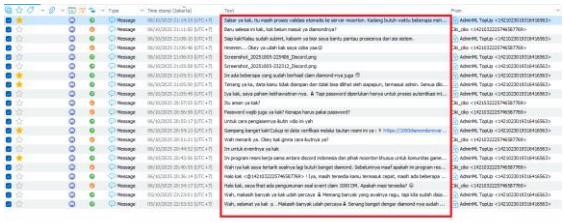


Gambar 11. Bukti Dokumen PDF dari *Mobiledit Forensic Express*

Gambar 11 menampilkan hasil temuan berupa dokumen PDF yang berhasil diekstraksi dari perangkat. Dokumen ini berisi data pendukung yang dikirimkan melalui aplikasi Discord dalam bentuk lampiran (*attachment*). Informasi metadata seperti nama *file*, ukuran, serta waktu pembuatan dokumen digunakan untuk memastikan keterkaitan *file* dengan konteks komunikasi yang dianalisis. Hasil ini

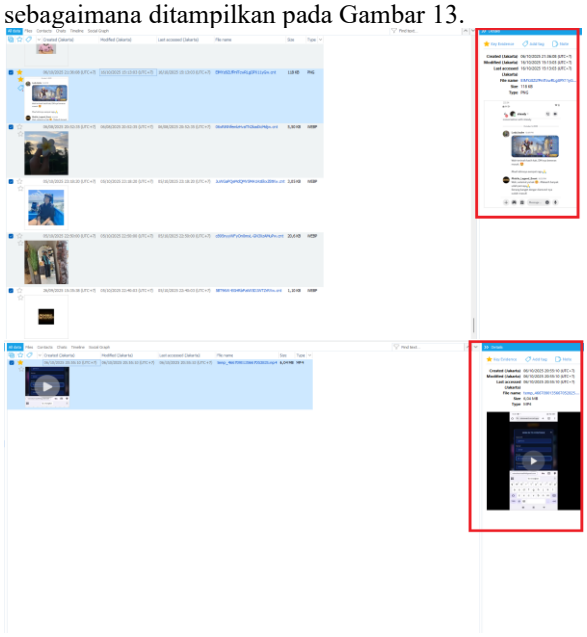
memperlihatkan bahwa *Mobiledit* mampu mengekstraksi berbagai tipe *file* dokumen secara utuh dengan tingkat keterbacaan tinggi.

Hasil analisis dilanjutkan menggunakan *Oxygen Forensic Detective* untuk mendapatkan bukti tambahan yang tidak terdeteksi oleh *Mobiledit*, terutama artefak komunikasi berbasis teks. *Oxygen* memiliki kemampuan untuk membaca basis data aplikasi (*application database*) secara lebih mendalam, sehingga memungkinkan pemulihan data *chat* dan aktivitas komunikasi lainnya. Bukti percakapan yang berhasil diekstraksi menggunakan *Oxygen Forensic Detective* dapat dilihat pada Gambar 12.



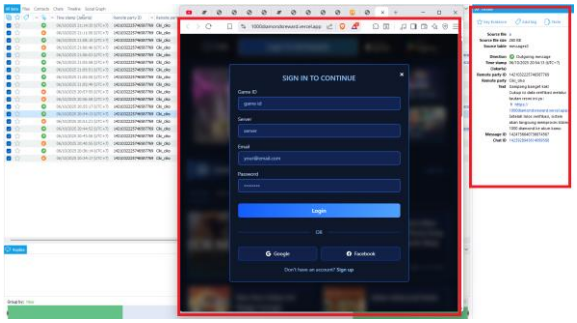
Gambar 12. Bukti *Chat* dari *Oxygen Forensic Detective*

Gambar 12 menunjukkan hasil ekstraksi percakapan (*chat*) antara akun pelaku dan korban pada aplikasi Discord. Setiap entri pesan menampilkan informasi penting seperti nama pengguna, waktu pengiriman, dan isi pesan. Data ini berfungsi sebagai bukti utama dalam simulasi kasus *phishing* karena menunjukkan pola komunikasi yang digunakan pelaku untuk mengirim tautan berbahaya kepada korban. Hasil ini juga menunjukkan bahwa *Oxygen Forensic Detective* memiliki kemampuan analisis yang lebih komprehensif dalam memulihkan data berbasis teks dibandingkan *Mobiledit*. *Oxygen Forensic Detective* juga berhasil memulihkan data media seperti gambar dan video dari perangkat uji, sebagaimana ditampilkan pada Gambar 13.



Gambar 13. Bukti Gambar dan Video dari *Oxygen Forensic Detective*

Gambar 13 menampilkan bukti tambahan berupa gambar dan video yang berhasil dipulihkan oleh *Oxygen Forensic Detective*. Hasil ekstraksi menunjukkan metadata lengkap seperti nama *file*, ukuran, serta waktu pengiriman, yang dapat digunakan untuk mengonfirmasi kesesuaian waktu aktivitas antara pesan teks dan *file* media yang dikirimkan. Artefak ini membantu memperkuat korelasi antara aktivitas komunikasi dan bukti media digital yang ditemukan. Selain media tersebut, *Oxygen* juga berhasil mendeteksi tautan *phishing* yang dikirimkan oleh pelaku beserta tampilan situs berbahaya yang diakses melalui tautan tersebut, sebagaimana ditunjukkan pada Gambar 14.



Gambar 14. Bukti Tautan dan Tampilan Situs *Phishing* dari *Oxygen Forensic Detective*

Gambar 14 memperlihatkan hasil identifikasi tautan *phishing* yang ditemukan pada pesan Discord beserta tampilan halaman situs *phishing* yang diakses melalui tautan tersebut. Informasi yang ditampilkan mencakup *teks* pesan, alamat URL, waktu pengiriman, dan pratinjau visual situs tujuan. Bukti ini menjadi salah satu artefak paling signifikan karena tidak hanya menunjukkan keberadaan tautan mencurigakan, tetapi juga memperlihatkan bagaimana situs palsu tersebut ditampilkan kepada korban. Adanya informasi ini, proses analisis dapat menelusuri pola serangan *phishing* secara lebih komprehensif, termasuk teknik rekayasa sosial yang digunakan pelaku untuk mengarahkan korban ke situs berbahaya.

Berdasarkan hasil analisis artefak digital yang diperoleh, perbedaan efektivitas antara *Oxygen Forensic Detective* dan *Mobiledit Forensic Express* dipengaruhi oleh arsitektur penyimpanan data aplikasi Discord yang berbasis basis data SQLite dan mekanisme sinkronisasi berbasis *cloud*. *Oxygen Forensic Detective* memiliki kemampuan parsing aplikasi yang memungkinkan ekstraksi data terstruktur dari basis data internal, sehingga lebih efektif dalam memulihkan artefak komunikasi seperti chat dan tautan *phishing*. Sebaliknya, *Mobiledit Forensic Express* lebih berfokus pada ekstraksi sistem file tingkat rendah dan pemulihan data media, sehingga kurang optimal dalam mendeteksi artefak komunikasi berbasis teks.

Artefak digital yang berhasil dipulihkan juga memungkinkan rekonstruksi kronologi kejadian *phishing* pada Discord *Mobile*. Metadata waktu pada

artefak chat, tautan *phishing*, dan media digital menunjukkan urutan kejadian yang saling berkaitan, mulai dari pengiriman pesan promosi palsu, komunikasi lanjutan melalui *direct message*, hingga akses ke situs *phishing*. Selain itu, penghapusan aplikasi Discord setelah kejadian dapat dikategorikan sebagai bentuk anti-forensik tingkat dasar. Namun, hasil penelitian menunjukkan bahwa artefak digital masih dapat dipulihkan melalui akuisisi fisik pada perangkat Android yang telah di-*root*, terutama dari area *cache* dan basis data aplikasi, sehingga teknik anti-forensik sederhana tidak sepenuhnya efektif.

3.5 *Report*

Tahap *Report* merupakan bagian akhir dari proses investigasi digital yang menampilkan hasil akuisisi dan analisis bukti digital yang diperoleh menggunakan *Mobiledit Forensic Express* dan *Oxygen Forensic Detective*. Seluruh artefak digital yang berhasil dideteksi, seperti pesan teks, gambar, video, dan dokumen PDF, disusun dalam bentuk laporan yang terverifikasi dan dapat dipertanggungjawabkan. Pada tahap ini juga dilakukan pengukuran efektivitas kedua tools dalam mendeteksi variabel bukti digital yang telah ditetapkan.

Untuk menilai kemampuan kedua perangkat lunak, digunakan perhitungan efektivitas yang membandingkan jumlah variabel bukti yang berhasil ditemukan terhadap total variabel bukti yang ditentukan dalam penelitian.

Berdasarkan persamaan (1), diperoleh hasil perhitungan efektivitas sebagai berikut:

Oxygen Forensic Detective

$$p_{ar} = \left(\frac{19}{22}\right) x\ 100\% = 86{,}3\%$$

Mobiledit Forensic Express

$$p_{ar} = \left(\frac{4}{22}\right) x\ 100\% = 18{,}1\%$$

Hasil lengkap perbandingan efektivitas kedua tools ditampilkan pada Tabel 4 untuk memperjelas kemampuan masing-masing alat dalam proses akuisisi dan analisis bukti digital.

Tabel 4. Hasil Perbandingan Efektivitas Tools Forensik dalam Analisis Aplikasi Discord

Kategori Data	Jumlah	*Oxygen Forensic Detective*	*Mobiledit Forensic Express*
Chat	17	16	0
Tautan	1	1	0
Gambar	2	1	2
Video	1	1	1
Dokumen (pdf)	1	0	1
Total	22	19	4
Presentase	100 %	86,3 %	18,1 %

Perbedaan tingkat efektivitas antara kedua alat forensik pada Tabel 4 menunjukkan bahwa karakteristik artefak digital memengaruhi keberhasilan investigasi. *Oxygen Forensic Detective* lebih efektif dalam mendeteksi artefak komunikasi dan tautan *phishing*, sedangkan *Mobiledit Forensic Express* lebih optimal dalam pemulihan artefak media. Temuan ini menunjukkan bahwa penggunaan satu alat forensik saja belum cukup untuk merekonstruksi seluruh bukti digital secara komprehensif, sehingga pendekatan multi-tool diperlukan untuk meningkatkan kelengkapan dan keandalan hasil investigasi.

Bukti digital yang diperoleh berpotensi memenuhi prinsip *admissibility* karena proses identifikasi, akuisisi, dan analisis dilakukan secara sistematis menggunakan metode OSCAR melalui teknik *physical acquisition* tanpa memodifikasi data asli. Dokumentasi proses ekstraksi dan metadata memungkinkan setiap artefak ditelusuri ke sumber dan konteks waktunya, sehingga mendukung keaslian (*authenticity*) dan integritas (*integrity*) bukti digital serta berpotensi dipertanggungjawabkan dalam proses hukum.

4. KESIMPULAN

Penelitian ini menganalisis proses investigasi forensik digital pada aplikasi Discord menggunakan metode OSCAR dalam skenario kasus *phishing*, dengan membandingkan kinerja *Mobiledit Forensic Express* dan *Oxygen Forensic Detective***.** Hasil penelitian menunjukkan bahwa *Oxygen Forensic Detective* memiliki efektivitas lebih tinggi dalam memperoleh artefak komunikasi seperti *chat* dan tautan *phishing* dengan persentase 86,3%**,** sedangkan *Mobiledit Forensic Express* hanya efektif 18,1% dalam mengekstraksi bukti berupa gambar, video, dan dokumen PDF. Temuan ini menegaskan bahwa tidak ada satu alat yang dapat merekonstruksi seluruh bukti digital secara komprehensif sehingga pendekatan *multi-tool* diperlukan dalam investigasi forensik digital, khususnya terhadap kejahatan siber berbasis rekayasa sosial pada platform komunikasi seperti Discord.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Direktorat Penelitian dan Pengabdian kepada Masyarakat (DPPM), Kementerian Pendidikan Tinggi, Sains, dan Teknologi Republik Indonesia, atas dukungan finansial yang diberikan melalui skema Penelitian Tesis Magister (PTM) dengan nomor kontrak 284/C3/DT.05.00/PL-BARU/2026.

DAFTAR PUSTAKA

Agustian Akbar, D., Rahdian, M., Kurnia, E., Genggam, R. M., Bintang, S., Purwoko, R., Siber, P., & Negara, S. (2024). Analisis Web *Phishing* Menggunakan Metode OSCAR Forensic (Studi Kasus: Follower

Instagram Gratis). *Jurnal Teknik Informatika (JTINFO)*, *3*(1), 18–24.

Ansyafa, K. Z., Fajarudin, M., Fadhil, M., & Neyman, S. N. (2024). Analisis Keamanan Media Sosial terhadap Serangan Phising Online menggunakan Metode Zphisher dan Social Engineering Toolkit. *Journal of Internet and Software Engineering*, *1*(4), 10. https://doi.org/10.47134/pjise.v1i4.2641

Ayatulloh, R., Noor, K., Umar, R., & Yudhana, A. (2021). *Assess of Forensic Tools on Android Based Facebook Lite with the NIST Method*. *8*(1), 1–9. https://doi.org/10.15294/sji.v8i1.

Discord says hackers stole government IDs of 70,000 users - Ars Technica. (n.d.). Retrieved December 25, 2025, from https://arstechnica.com/security/2025/10/discord-says-hackers-stole-government-ids-of-70000-users/

Dzil Ikram, F., & Koprawi, M. (2023). Forensic analysis on discord application using the National Institute of Standards and Technology (NIST) Method. *Jurnal Mandiri IT*, *12*(1), 20–28.

Ermin, Rizki Setyawan, M., & Tella, F. (2023). Forensic Analysis of Dana Applications using The ACPO Framework. *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)*, *8*(1), 1–8.

FFaizal, A., & Luthfi, A. (2024). Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis. *Journal of Information Systems and Informatics*, *6*(2), 701–718. https://doi.org/10.51519/journalisi.v6i2.717

Hidayah, A., Fachri, F., & Informatika, T. (2025). Analisis Bukti Digital Terhadap Kasus Prostitusi. *9*(1), 906–912.

Ichsan, A. N., & Riadi, I. (2021). *Mobile* Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method. *International Journal of Computer Applications*, *174*(18), 34–40. https://doi.org/10.5120/ijca2021921076

Kara, İ. (2022). Digital Forensic Analysis of Discord *Mobile* Application on Android Based Smartphones. *Acta Infologica*, *0*(0), 0–0. https://doi.org/10.26650/acin.1109682

Muh, A., Salim, Y., & Rachman, A. (2022). *Analisis Bukti Digital Forensik pada Discord Menggunakan Metode National Institute of Standards Technology*. *3*(4), 293–300.

Pratama Putra, P. A., Sukerti, N. K., & Putu Suniantara, I. K. (2024). Akusisi Forensik Digital Pada Aplikasi Google Drive Sebagai Bukti Digital Dalam Penyelidikan Kasus Pornografi. *Spinter*, *1*(2), 138–143.

Qureshi, S., Tunio, S., Akhtar, F., Wajahat, A., Nazir, A., & Ullah, F. (2021a). Network Forensics: A Comprehensive Review of Tools and Techniques. *International Journal of Advanced Computer Science and Applications*, *12*(5), 879–887. https://doi.org/10.14569/IJACSA.2021.01205103

Qureshi, S., Tunio, S., Akhtar, F., Wajahat, A., Nazir, A., & Ullah, F. (2021b). Network Forensics: A Comprehensive Review of Tools and Techniques. *International Journal of Advanced Computer Science and Applications*, *12*(5), 879–887. https://doi.org/10.14569/IJACSA.2021.01205103

Riadi, I., Ruslan, T., Industri, F. T., Dahlan, U. A., Industri, F. T., Dahlan, U. A., Informatika, T., Industri, F. T., & Dahlan, U. A. (2023). Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST. *13*(2), 286–292.

Shah, A. (2023). Evaluating Network Forensics Applying Advanced Tools. *International Journal of Advanced Engineering, Management and Science*, *9*(4), 01–09. https://doi.org/10.22161/ijaems.94.1

Spiekermann, D., & Keller, J. (2023). Challenges of Network Forensic Investigation in Fog and Edge Computing. *Future Internet*, *15*(10), 1–12. https://doi.org/10.3390/fi15100342

Stephani Tauran, I., & Swandy Aritonang, R. (2023). Penerapan Metode Tam Terhadap Media Komunikasi Discord Pada Peserta Mbkm Di Perusahaan Nodeflux. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*(3), 1666–1670.

https://doi.org/10.36040/jati.v7i3.6890

Tofik, A., Muflih, G. Z., & Informatika, T. (2024). Akuisisi Barang Bukti Digital Pada Aplikasi Discord. *8*(6), 12122–12128.

Wibowo, M., Firmansyah, M. R., & Efendi, R. S. (2024). Analisis Bukti Digital Pada Aplikasi Discord Desktop Dengan Menggunakan Framework Dfrws. *Jurnal Teknologi Informasi Dan Komunikasi*, *15*(1), 98–111. https://doi.org/10.51903/jtikp.v15i1.826

Yan Fikri Hendrawan, M., Subktiningsih, & Hadinegoro, A. (2023). Analisis Bukti Digital Pada Discord Browser Menggunakan Teknik Live Forensic Dengan Metode NIST SP 800-86. *Jurnal Infomedia: Teknik Informatika, Multimedia Dan Jaringan*, *8*(2), 94–99.

Yudhana, A., Riadi, I., & Prasongko, R. Y. (2022). Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS). *Jurnal Informatika: Jurnal Pengembangan IT*, *7*(1), 43–48. https://doi.org/10.30591/jpit.v7i1.3639

Yulistina, S. R., Nurmala, T., Supriawan, R. M. A. T., Juni, S. H. I., & Saifudin, A. (2025). Penerapan Teknik Boundary Value Analysis untuk Pengujian Aplikasi Penjualan Menggunakan Metode Black Box Testing. *Jurnal Informatika Universitas Pamulang*, *5*(2), 129. https://doi.org/10.32493/informatika.v5i2.5366

Zaida Muflih, G. (2023). Comparison of Forensic Tools on Social Media Services Using the Digital Forensic Research Workshop Method (DFRWS). *JIKO (Jurnal Informatika Dan Komputer)*, *6*(1), 52–61. https://doi.org/10.33387/jiko.v6i1.5872