

Analisis Pemanfaatan Tools Forensik dalam Investigasi Credential Phishing pada Discord Web Menggunakan Metode OSCAR

Zulki Yanto Rivai¹, Anton Yudhana², Imam Riadi³

¹Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

²Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

³Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

¹2408048019@webmail.uad.ac.id, ²eyudhana@ee.uad.ac.id*, ³imam.riadi@is.uad.ac.id

Abstract

Credential phishing on Discord Web can generate digital traces across browser storage and network traffic, requiring appropriate forensic tools according to the characteristics of each evidence source. This study analyzes the utilization of forensic tools in investigating credential phishing on Discord Web using the OSCAR method, consisting of Obtain, Strategize, Collect, Analyze, and Report. A controlled experimental scenario was conducted using a phishing domain represented in browser and network artifacts as xn--discord-waa.online. FTK Imager was used to acquire the browser profile, while DB Browser for SQLite, Autopsy, and Wireshark were used for artifact examination. The results show that DB Browser for SQLite identified the phishing URL in browser History, Discord-related cookies, email, and username, while no phishing-domain cookie or saved login data was found. Autopsy identified the phishing domain, login.html, email, and username in browser storage artifacts. Wireshark identified DNS resolution, the phishing server IP address, and TLS SNI associated with the phishing domain and official Discord services. The findings demonstrate that each tool contributes different evidence according to the source and characteristics of the artifacts. The OSCAR method provides a structured workflow for positioning and utilizing forensic tools throughout the investigation.

Keywords: *credential phishing, Discord Web, forensic tools, browser forensics, OSCAR*

Abstrak

Credential phishing pada Discord Web dapat meninggalkan jejak digital pada berbagai sumber bukti, khususnya penyimpanan browser dan lalu lintas jaringan, sehingga diperlukan pemanfaatan tools forensik sesuai karakteristik sumber bukti yang diperiksa. Penelitian ini bertujuan menganalisis pemanfaatan tools forensik dalam investigasi credential phishing pada Discord Web menggunakan metode OSCAR yang terdiri atas Obtain, Strategize, Collect, Analyze, dan Report. Penelitian dilakukan melalui eksperimen terkontrol dengan skenario credential phishing menggunakan domain yang direpresentasikan dalam artefak browser dan jaringan sebagai xn--discord-waa.online. FTK Imager digunakan untuk melakukan akuisisi browser profile, sedangkan DB Browser for SQLite, Autopsy, dan Wireshark digunakan untuk pemeriksaan artefak. Hasil pemeriksaan menunjukkan bahwa DB Browser for SQLite menemukan URL phishing pada History, cookie terkait Discord, email, dan username, sedangkan cookie domain phishing dan data login tersimpan tidak ditemukan. Autopsy menemukan domain phishing, login.html, email, dan username pada artefak penyimpanan browser. Wireshark menemukan DNS, alamat IP server phishing, serta TLS SNI domain phishing dan layanan Discord resmi. Hasil tersebut menunjukkan bahwa setiap tools memberikan kontribusi berbeda berdasarkan sumber dan karakteristik artefak yang diperiksa. Penerapan OSCAR memberikan alur terstruktur dalam penempatan dan pemanfaatan tools selama proses investigasi.

Kata kunci: *credential phishing, Discord Web, forensic tools, browser forensics, OSCAR*

1. Pendahuluan

Perkembangan platform komunikasi berbasis web telah meningkatkan aktivitas pengguna dalam melakukan komunikasi, berbagi informasi, dan mengakses berbagai layanan digital. Salah satu platform yang banyak

digunakan adalah Discord yang menyediakan layanan komunikasi melalui browser maupun aplikasi. Aktivitas Discord yang dilakukan melalui browser dapat meninggalkan berbagai jejak digital pada media penyimpanan browser. Gupta et al. menunjukkan bahwa penggunaan Discord melalui Google Chrome pada

sistem Windows menghasilkan berbagai artefak, antara lain local storage, cache, informasi akun, percakapan, pesan, dan lampiran yang dapat digunakan sebagai sumber bukti dalam pemeriksaan forensik digital [1], [2], [3]. Keberadaan berbagai artefak tersebut menjadikan aktivitas pengguna pada Discord Web memiliki nilai forensik, terutama ketika platform digunakan dalam suatu aktivitas yang berkaitan dengan kejahatan siber [4], [5].

Salah satu ancaman yang memanfaatkan lingkungan komunikasi berbasis web adalah credential phishing. Serangan ini menggunakan halaman atau layanan palsu untuk mengelabui pengguna agar menyerahkan informasi autentikasi kepada pelaku [6], [7], [8]. Dalam pemeriksaan forensik, keberadaan aktivitas phishing tidak hanya dapat ditelusuri melalui alamat URL, tetapi juga melalui berbagai artefak yang terbentuk selama interaksi pengguna. History dapat menunjukkan alamat yang diakses, cookies dapat memberikan informasi mengenai aktivitas sesi, sedangkan Web Data, Login Data, cache, local storage, dan session storage dapat menyimpan jejak aktivitas pengguna pada browser [9], [10], [11]. Selain itu, komunikasi dengan infrastruktur phishing dapat meninggalkan bukti pada lalu lintas jaringan seperti DNS, alamat IP, dan TLS Server Name Indication (SNI). Kondisi tersebut menyebabkan bukti digital pada suatu kasus *phishing* dapat tersebar pada beberapa sumber dan memerlukan pemeriksaan menggunakan tools yang sesuai dengan karakteristik masing-masing sumber bukti.

Penelitian mengenai browser forensics telah menunjukkan bahwa kemampuan memperoleh artefak dapat berbeda berdasarkan browser, kondisi penggunaan, dan tools yang digunakan. Alotibi et al. melakukan pemeriksaan terhadap beberapa browser menggunakan tools forensik seperti Autopsy, AXIOM, dan XRY untuk memperoleh dan menganalisis artefak browser. Penelitian tersebut menunjukkan bahwa proses pemeriksaan browser dapat menghasilkan artefak yang berbeda bergantung pada lingkungan dan pendekatan pemeriksaan yang digunakan [12], [13]. Chand et al. juga melakukan evaluasi terhadap teknik dan tools dalam web browser forensics serta menunjukkan bahwa browser dapat meninggalkan berbagai artefak yang memiliki nilai dalam investigasi digital [14]. Hasil penelitian tersebut memperlihatkan pentingnya pemilihan dan pemanfaatan tools dalam memperoleh informasi dari berbagai sumber artefak browser.

Pada lingkungan Discord, penelitian forensik juga telah diarahkan secara lebih khusus pada kasus phishing. Aqil dan Riadi melakukan analisis forensik terhadap serangan phishing pada Discord Web menggunakan metode National Institute of Standards and Technology (NIST). Penelitian tersebut menggunakan Wireshark untuk menangkap lalu lintas jaringan, FTK Imager untuk memperoleh artefak pada host, DB Browser for SQLite untuk menganalisis browser history, serta WHOIS untuk

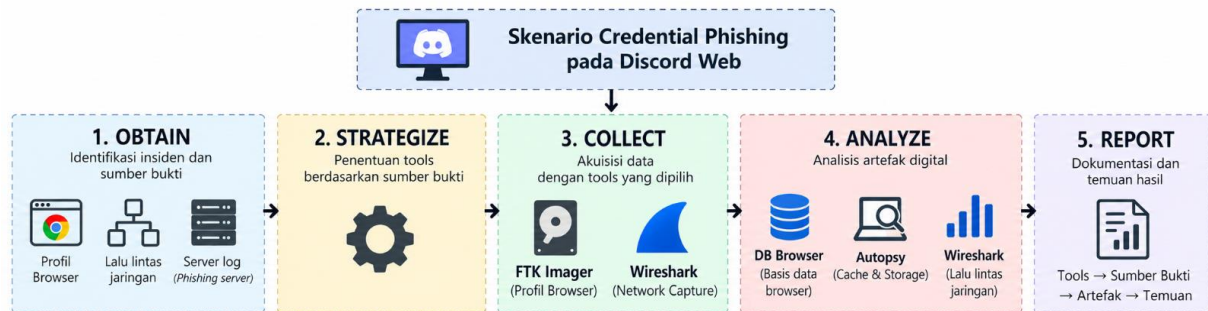
memperoleh informasi domain [15]. Hasil penelitian menunjukkan bahwa proses pemeriksaan dapat memperoleh URL phishing, waktu kunjungan, perubahan konfigurasi DNS lokal, kredensial pada lingkungan eksperimen, dan informasi registrasi domain [15]. Meskipun demikian, kajian tersebut menempatkan tools sebagai bagian dari tahapan pemeriksaan berbasis NIST, sehingga fungsi setiap tools terhadap karakteristik sumber bukti dan jenis artefak belum dibahas secara terstruktur dalam satu alur investigasi.

Berdasarkan kondisi tersebut, diperlukan suatu pendekatan yang dapat menggambarkan pemanfaatan tools forensik secara sistematis sejak penentuan sumber bukti, proses akuisisi, pemeriksaan artefak, hingga pelaporan hasil. Penelitian ini menggunakan metode OSCAR yang terdiri dari Obtain, Strategize, Collect, Analyze, dan Report untuk mengorganisasi proses investigasi credential phishing pada Discord Web [16], [17]. FTK Imager digunakan untuk memperoleh browser profile sebagai sumber bukti, DB Browser for SQLite digunakan untuk memeriksa database browser, Autopsy digunakan untuk memeriksa cache dan storage artifacts, sedangkan Wireshark digunakan untuk memeriksa lalu lintas jaringan. Hasil dari masing-masing tools kemudian dianalisis berdasarkan hubungan antara sumber bukti, jenis artefak, dan kontribusinya terhadap identifikasi aktivitas credential phishing.

Penelitian ini bertujuan menganalisis pemanfaatan tools forensik dalam investigasi credential phishing pada Discord Web menggunakan metode OSCAR. Analisis diarahkan untuk mengetahui penerapan setiap tahap OSCAR, mengidentifikasi artefak yang diperoleh dari masing-masing tools, serta menjelaskan kontribusi artefak tersebut dalam mendukung pemeriksaan aktivitas phishing. Dengan demikian, penelitian ini menjawab bagaimana metode OSCAR diterapkan dalam investigasi credential phishing pada Discord Web, bagaimana tools forensik dimanfaatkan berdasarkan sumber bukti dan jenis artefak, serta bagaimana artefak yang diperoleh berkontribusi terhadap identifikasi aktivitas credential phishing.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan eksperimen forensik digital untuk menganalisis pemanfaatan tools forensik dalam investigasi credential phishing pada Discord Web. Eksperimen dilakukan dalam lingkungan yang dikendalikan dengan mensimulasikan aktivitas credential phishing pada Discord Web. Proses investigasi menggunakan metode OSCAR yang terdiri atas Obtain, Strategize, Collect, Analyze, dan Report. Setiap tahapan digunakan untuk mengatur proses identifikasi sumber bukti, pemilihan tools, akuisisi evidence, pemeriksaan artefak, serta dokumentasi temuan forensik. Alur penelitian dan hubungan antara skenario, tahapan OSCAR, serta tools yang digunakan ditunjukkan pada Gambar 1.



Gambar 1. Alur Penelitian

Gambar 1 menunjukkan bahwa proses penelitian dimulai dari skenario credential phishing pada Discord Web dan dilanjutkan melalui lima tahapan OSCAR. Tahap *Obtain* digunakan untuk mengidentifikasi sumber bukti, *Strategize* menentukan tools berdasarkan karakteristik sumber bukti, *Collect* melakukan akuisisi evidence, *Analyze* melakukan pemeriksaan artefak, dan *Report* mendokumentasikan hubungan antara tools, sumber bukti, artefak, dan temuan [16]. Pembagian tersebut menjadi dasar pelaksanaan eksperimen pada penelitian ini.

2.1. Skenario Penelitian

Skenario penelitian menggunakan lingkungan Discord Web dengan aktivitas *credential phishing* yang dilakukan secara terkontrol. Skenario melibatkan browser pada perangkat korban, halaman *phishing*, phishing server, serta aktivitas akses terhadap Discord Web. Domain yang digunakan dalam skenario phishing adalah `xn--discord-waa.online` sebagai domain tujuan halaman *phishing*.

Proses eksperimen diawali dengan aktivitas pengiriman dan akses tautan *phishing* oleh pengguna pada perangkat korban. Pengguna kemudian mengakses halaman *phishing* melalui browser dan melakukan interaksi pada halaman tersebut menggunakan data credential dummy. Aktivitas tersebut menghasilkan jejak digital pada browser, lalu lintas jaringan, dan phishing server. Setelah aktivitas pada halaman *phishing* dilakukan, aktivitas akses Discord Web digunakan sebagai bagian dari rangkaian kejadian yang diperiksa dalam penelitian.

Sumber bukti yang digunakan meliputi *browser profile*, *network capture*, dan *phishing server log*. *Browser profile* mencakup artefak *History*, *Cookies*, *Web Data*, *Login Data*, *Cache*, *Local Storage*, dan *Session Storage*. *Network capture* digunakan untuk memperoleh lalu lintas komunikasi yang berkaitan dengan aktivitas akses domain *phishing* dan Discord. Sementara itu, *phishing server log* digunakan sebagai sumber informasi aktivitas permintaan terhadap infrastruktur *phishing*.

2.2. Tahapan Investigasi Menggunakan OSCAR

Proses investigasi dilakukan menggunakan metode OSCAR yang terdiri atas lima tahapan, yaitu *Obtain*, *Strategize*, *Collect*, *Analyze*, dan *Report*. Penerapan

setiap tahap disesuaikan dengan aktivitas eksperimen dan kebutuhan pemeriksaan bukti digital.

Pada tahap *Obtain*, dilakukan identifikasi terhadap insiden credential phishing dan sumber bukti yang tersedia. Sumber bukti yang ditentukan meliputi *browser profile* pada perangkat korban, lalu lintas jaringan, dan *phishing server log*. *Browser profile* digunakan sebagai sumber artefak aktivitas pengguna, *network traffic* sebagai sumber bukti komunikasi, sedangkan *phishing server log* digunakan sebagai sumber catatan permintaan terhadap infrastruktur *phishing*.

Tahap *Strategize* digunakan untuk menentukan *tools* yang sesuai dengan karakteristik sumber bukti. FTK Imager digunakan untuk memperoleh browser profile, Wireshark digunakan untuk memperoleh *network capture*, DB Browser for SQLite digunakan untuk memeriksa *database browser*, dan Autopsy digunakan untuk memeriksa artefak pada cache dan *storage browser*.

Pada tahap *Collect*, proses akuisisi dilakukan terhadap sumber bukti yang telah ditentukan. FTK Imager digunakan untuk melakukan akuisisi *browser profile* yang selanjutnya digunakan sebagai sumber pemeriksaan artefak browser. Wireshark digunakan untuk melakukan network capture selama aktivitas eksperimen sehingga menghasilkan PCAP sebagai sumber *network evidence*.

Tahap *Analyze* dilakukan terhadap *evidence* yang telah diperoleh pada tahap *Collect*. DB Browser for SQLite digunakan untuk memeriksa database History, Cookies, Web Data, dan Login Data. Autopsy digunakan untuk memeriksa History, Cache, Local Storage, dan Session Storage. Wireshark digunakan untuk menganalisis network capture untuk mengidentifikasi DNS, IP server phishing, TLS SNI domain phishing, dan TLS SNI Discord resmi.

Tahap *Report* digunakan untuk menyusun hasil pemeriksaan dalam bentuk hubungan antara tools, sumber bukti, artefak, dan temuan forensik. Hasil dari setiap pemeriksaan didokumentasikan dan dipetakan berdasarkan fungsi tools serta artefak yang diperoleh [18]. Pemetaan tersebut digunakan untuk menjelaskan

kontribusi masing-masing tools dalam pemeriksaan *credential phishing* pada Discord Web.

2.3. Sumber Bukti dan Tools Forensik

Sumber bukti dalam penelitian dikategorikan berdasarkan lokasi terbentuknya artefak dan karakteristik data yang diperiksa. Browser profile merupakan sumber utama artefak pada perangkat korban dan diperoleh melalui proses akuisisi menggunakan FTK Imager. Hasil akuisisi tersebut kemudian diperiksa menggunakan DB Browser for SQLite dan Autopsy. Network capture diperoleh dan dianalisis menggunakan Wireshark, sedangkan phishing server log digunakan sebagai sumber catatan aktivitas pada infrastruktur phishing.

Hubungan antara sumber bukti, tools, fungsi, dan objek pemeriksaan yang digunakan dalam penelitian ditampilkan pada Tabel 1.

Tabel 1. Sumber Bukti dan Pemanfaatan Tools

Sumber Bukti	Tools	Fungsi	Objek Pemeriksaan
Browser profile	FTK Imager	Akuisisi	History, Cookies, Web Data, Login Data, Cache, Local Storage, Session Storage
Browser database	DB Browser for SQLite	Analisis database	History, Cookies, Web Data, Login Data
Browser storage	Autopsy	Analisis artefak	History, Cache, Local Storage, Session Storage
Network capture	Wireshark	Akuisisi dan analisis jaringan	DNS, IP, TLS SNI
Phishing server log	—	Sumber pendukung	Request dan aktivitas server

Tabel 1 menunjukkan bahwa setiap tools memiliki fungsi yang berbeda sesuai dengan karakteristik sumber bukti. FTK Imager ditempatkan pada proses akuisisi browser profile, sedangkan DB Browser for SQLite dan Autopsy digunakan pada tahap pemeriksaan dengan objek yang berbeda. Wireshark digunakan untuk memperoleh sekaligus menganalisis network evidence. Phishing server log digunakan sebagai sumber pendukung karena pada eksperimen ini tidak terdapat tools khusus yang digunakan untuk melakukan analisis terhadap log tersebut.

2.4. Analisis Artefak

Analisis artefak dilakukan terhadap browser evidence dan network evidence yang telah diperoleh pada tahap *Collect*. Pemeriksaan dilakukan dengan menyesuaikan tools terhadap jenis dan lokasi artefak. Hasil pemeriksaan kemudian dicatat berdasarkan jenis artefak, keberadaan temuan, serta keterkaitannya dengan aktivitas *credential phishing*.

Pada DB Browser for SQLite, pemeriksaan dilakukan terhadap database History, Cookies, Web Data, dan Login Data. Pada History, pemeriksaan diarahkan untuk mengidentifikasi URL yang berkaitan dengan aktivitas phishing. Pemeriksaan Cookies digunakan untuk mengidentifikasi cookie yang berkaitan dengan layanan Discord dan memeriksa keberadaan cookie dari domain phishing. Web Data diperiksa untuk memperoleh informasi pengguna yang tersimpan pada database, sedangkan Login Data diperiksa untuk mengetahui keberadaan data login yang tersimpan.

Pada Autopsy, pemeriksaan diarahkan pada History, Cache, Local Storage, dan Session Storage. History digunakan untuk melihat jejak akses, sedangkan Cache dan storage digunakan untuk mengidentifikasi artefak yang terbentuk dari interaksi pengguna dengan halaman web. Artefak yang diperiksa meliputi domain phishing, halaman login.html, email dummy, username, serta jejak yang berkaitan dengan Discord.

Pada Wireshark, pemeriksaan dilakukan terhadap PCAP yang diperoleh selama eksperimen. Analisis diarahkan pada DNS, alamat IP server phishing, TLS SNI domain phishing, dan TLS SNI Discord resmi. Hasil pemeriksaan jaringan digunakan untuk mengidentifikasi komunikasi yang berkaitan dengan infrastruktur phishing dan aktivitas akses terhadap layanan Discord.

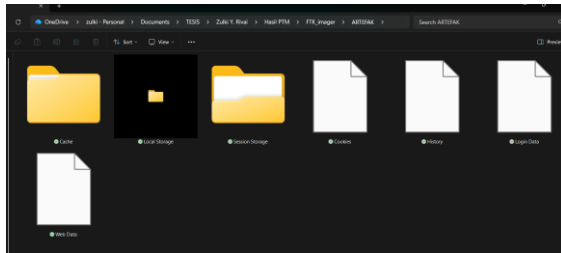
Seluruh hasil pemeriksaan kemudian disusun dalam pemetaan tools–sumber bukti–artefak–temuan. Pemetaan tersebut digunakan sebagai dasar analisis pada bagian Hasil dan Pembahasan untuk menjelaskan bagaimana masing-masing tools berkontribusi terhadap pemeriksaan *credential phishing* pada Discord Web.

3. Hasil dan Pembahasan

Hasil penelitian diperoleh dari pemeriksaan terhadap *browser profile* dan *network capture* yang dihasilkan selama skenario *credential phishing* pada Discord Web. Pemeriksaan dilakukan menggunakan FTK Imager pada tahap akuisisi, kemudian dilanjutkan menggunakan DB Browser for SQLite, Autopsy, dan Wireshark untuk memperoleh dan menganalisis artefak digital. Hasil pemeriksaan setiap sumber bukti selanjutnya digunakan untuk mengetahui kontribusi masing-masing tools terhadap identifikasi aktivitas *credential phishing*.

3.1. Hasil Akuisisi *Browser Profile* Menggunakan FTK Imager

Tahap akuisisi dilakukan terhadap *browser profile* pada perangkat korban menggunakan FTK Imager. Akuisisi bertujuan memperoleh sumber bukti browser secara utuh untuk digunakan pada tahap pemeriksaan berikutnya. Hasil akuisisi menunjukkan bahwa *browser profile* yang diperoleh terdiri atas beberapa sumber artefak, yaitu Cache, Local Storage, Session Storage, Cookies, History, Login Data, dan Web Data. Struktur hasil akuisisi tersebut ditunjukkan pada Gambar 2.



Gambar 2. Hasil akuisisi *browser profile* menggunakan FTK Imager.

Gambar 2 menunjukkan bahwa proses akuisisi menghasilkan beberapa komponen penyimpanan browser yang menjadi sumber pemeriksaan pada tahap berikutnya. File History, Cookies, Login Data, dan Web Data tersedia sebagai database, sedangkan Cache, Local Storage, dan Session Storage tersedia sebagai direktori penyimpanan. Hasil akuisisi tersebut kemudian digunakan sebagai sumber pemeriksaan menggunakan DB Browser for SQLite dan Autopsy.

Dengan demikian, FTK Imager berfungsi sebagai *acquisition tool* dalam penelitian ini. Hasil dari tahap tersebut bukan berupa interpretasi artefak, tetapi berupa sumber bukti yang dapat diperiksa lebih lanjut menggunakan *tools* pemeriksaan yang sesuai.

3.2. Hasil Pemeriksaan Browser Database Menggunakan DB Browser for SQLite

Pemeriksaan terhadap *browser database* dilakukan menggunakan DB Browser for SQLite. Pemeriksaan diarahkan pada History, Cookies, Web Data, dan Login Data untuk mengidentifikasi jejak akses, informasi layanan, informasi pengguna, serta keberadaan data login yang tersimpan. Ringkasan hasil pemeriksaan database tersebut ditampilkan pada Tabel 2.

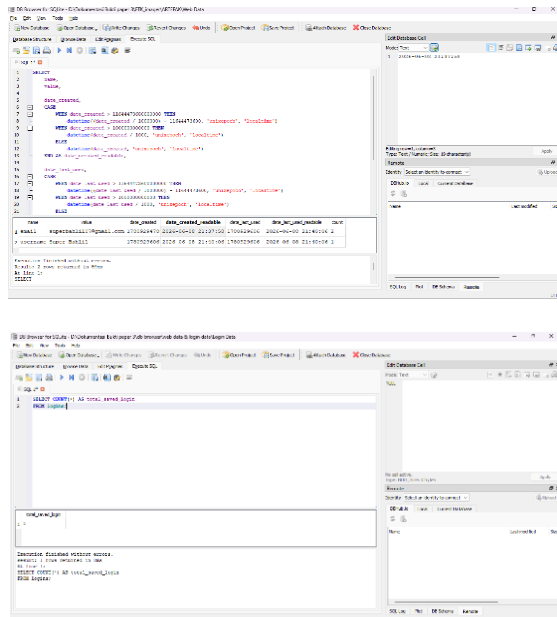
Tabel 2. Hasil Pemeriksaan browser database menggunakan DB Browser for SQLite

Artefak	Hasil Pemeriksaan	Temuan
History	Diperiksa menggunakan kueri SQL	https://xn--dscord-waa.online/ ditemukan
Cookies	Diperiksa berdasarkan domain	discord.com, .discordapp.com, .discord.gg, dan .discordapp.net ditemukan
Cookies	Pemeriksaan domain phishing	Cookie xn--dscord-waa.online tidak ditemukan
Web Data	Diperiksa menggunakan kueri SQL	Email ditemukan
Web Data	Diperiksa menggunakan kueri SQL	Username ditemukan
Login Data	Pemeriksaan tabel logins	0 record
Login Data	Kueri berdasarkan domain dan atribut terkait	Tidak ditemukan data login

Tabel 2 menunjukkan bahwa pemeriksaan DB Browser menghasilkan beberapa artefak yang berkaitan dengan aktivitas pengguna. Pada History ditemukan URL <https://xn--dscord-waa.online/>, yang menjadi salah satu indikator akses terhadap domain *phishing*. Pemeriksaan Cookies menemukan beberapa domain resmi Discord, tetapi tidak menemukan cookie dari domain *phishing*. Kondisi tersebut menunjukkan bahwa keberadaan aktivitas *phishing* tidak selalu disertai dengan terbentuknya cookie dari domain tersebut.

Pemeriksaan Web Data menghasilkan informasi berupa email dan username. Sebaliknya, pemeriksaan Login Data menghasilkan 0 record, sehingga tidak ditemukan *credential* yang tersimpan pada tabel logins. Hasil tersebut menunjukkan bahwa ketiadaan data login tersimpan tidak menghilangkan kemungkinan adanya aktivitas *credential phishing*, karena bukti aktivitas masih dapat diperoleh dari sumber browser lainnya.

Hasil pemeriksaan History dan Web Data juga didokumentasikan melalui kueri SQL pada DB Browser. Pemeriksaan tersebut ditampilkan pada Gambar 3 untuk memperlihatkan proses identifikasi artefak secara langsung dari database.



Gambar 3. Hasil kueri DB Browser terhadap Web Data dan Login Data.
 Gambar 3 memperlihatkan bahwa kueri terhadap Web Data menghasilkan dua informasi pengguna, yaitu email dan username, sedangkan pemeriksaan Login Data tidak menghasilkan data login. Hasil tersebut memperlihatkan bahwa DB Browser dapat digunakan untuk melakukan pemeriksaan langsung terhadap struktur database browser dan mengidentifikasi data yang relevan maupun kondisi ketika artefak yang dicari tidak tersedia.

3.3. Hasil Pemeriksaan Cache dan Storage Menggunakan Autopsy

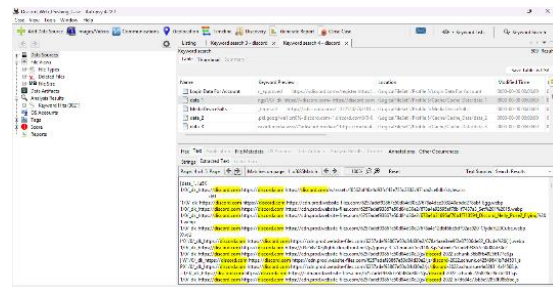
Pemeriksaan berikutnya dilakukan menggunakan Autopsy terhadap artefak yang berada pada History, Cache, Local Storage, dan Session Storage. Pemeriksaan diarahkan untuk mengidentifikasi jejak aktivitas Discord dan interaksi dengan domain *phishing*. Hasil pemeriksaan pada artefak browser tersebut dirangkum pada Tabel 3.

Tabel 3. Hasil pemeriksaan artefak menggunakan Autopsy

Sumber Artefak	Temuan	Kontribusi Forensik
History	Discord resmi dan domain <i>phishing</i>	Menunjukkan jejak akses
Cache	xn--dscord-waa.online	Mengidentifikasi jejak domain <i>phishing</i>
Cache	login.html	Menunjukkan keberadaan halaman login <i>phishing</i>

Sumber Artefak	Temuan	Kontribusi Forensik
Local Storage	Jejak Discord	Menunjukkan aktivitas pada penyimpanan browser
Session Storage	xn--dscord-waa.online	Menunjukkan jejak interaksi dengan domain <i>phishing</i>
Session Storage	login.html	Mendukung identifikasi halaman <i>phishing</i>
Session Storage	Email dummy	Menunjukkan data yang digunakan pada sesi
Session Storage	Username	Menunjukkan informasi pengguna pada sesi

Tabel 3 menunjukkan bahwa Autopsy menghasilkan artefak yang lebih berorientasi pada file dan penyimpanan browser. Keberadaan domain xn--dscord-waa.online pada Cache dan Session Storage, serta ditemukannya login.html, memberikan bukti tambahan mengenai interaksi browser dengan halaman *phishing*. Email dummy dan username yang ditemukan pada Session Storage juga memberikan konteks terhadap aktivitas yang dilakukan pada halaman tersebut. Salah satu hasil pemeriksaan Cache pada Autopsy ditampilkan pada Gambar 4. Gambar tersebut memperlihatkan hasil pencarian artefak yang berkaitan dengan domain dan halaman *phishing*.



Gambar 4. Hasil pemeriksaan artefak Cache menggunakan Autopsy.

Gambar 4 menunjukkan bahwa pemeriksaan Cache menggunakan Autopsy dapat mengidentifikasi artefak yang berkaitan dengan domain *phishing* dan halaman login.html. Temuan tersebut melengkapi hasil pemeriksaan History menggunakan DB Browser karena menunjukkan bahwa aktivitas terhadap domain tidak hanya tercatat sebagai riwayat akses, tetapi juga meninggalkan data pada penyimpanan sementara browser.

3.4. Hasil Analisis Network Evidence Menggunakan Wireshark

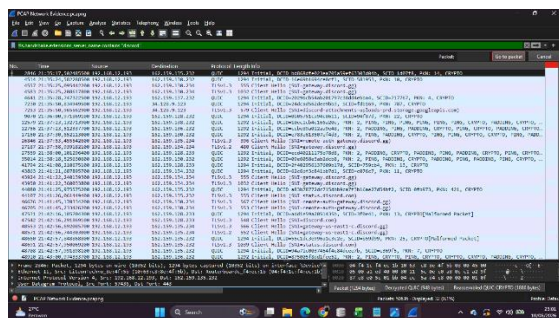
Selain artefak pada browser, penelitian menganalisis *network evidence* menggunakan Wireshark. Analisis dilakukan terhadap PCAP yang diperoleh selama proses eksperimen. Pemeriksaan diarahkan pada DNS, alamat IP server *phishing*, TLS SNI domain *phishing*, dan TLS SNI Discord resmi. Hasil pemeriksaan *network evidence* ditampilkan pada Tabel 4.

Tabel 4. Hasil analisis network evidence menggunakan Wireshark

Artefak Jaringan	Hasil	Kontribusi Forensik
DNS	Domain <i>phishing</i> teridentifikasi	Menunjukkan proses resolusi domain
IP	IP server <i>phishing</i> teridentifikasi	Mengidentifikasi tujuan komunikasi
TLS SNI	Domain <i>phishing</i> teridentifikasi	Mendukung identifikasi komunikasi ke domain <i>phishing</i>
TLS SNI	Discord resmi teridentifikasi	Menunjukkan komunikasi dengan layanan Discord

Tabel 4 menunjukkan bahwa Wireshark menghasilkan bukti dari lapisan jaringan yang tidak diperoleh melalui pemeriksaan database browser. DNS memberikan informasi mengenai resolusi domain, sedangkan alamat IP menunjukkan tujuan komunikasi. TLS SNI memberikan informasi nama domain yang menjadi tujuan komunikasi pada koneksi TLS, baik domain *phishing* maupun Discord resmi.

Hasil pemeriksaan DNS, IP, dan TLS SNI kemudian didokumentasikan melalui beberapa tampilan analisis Wireshark. Contoh hasil pemeriksaan tersebut ditunjukkan pada Gambar 5.



Gambar 5. Hasil Analisis Menggunakan Wireshark
Gambar 5 memperlihatkan bahwa analisis PCAP menghasilkan beberapa indikator komunikasi jaringan yang berkaitan dengan domain *phishing* dan layanan Discord. Hasil ini memberikan perspektif berbeda dari artefak browser karena menunjukkan aktivitas pada

tingkat komunikasi jaringan. Dengan demikian, Wireshark melengkapi pemeriksaan yang dilakukan terhadap *browser evidence*.

3.5. Pemetaan Pemanfaatan Tools terhadap Artefak

Setelah seluruh sumber bukti diperiksa, hasilnya dipetakan untuk melihat hubungan antara *tools*, sumber bukti, artefak, dan kontribusi terhadap pemeriksaan. Pemetaan ini merupakan bagian penting untuk menunjukkan bagaimana setiap *tools* digunakan sesuai karakteristik sumber bukti. Hasil pemetaan ditampilkan pada Tabel 5.

Tabel 5. Pemetaan tools, sumber bukti, artefak, dan kontribusi forensik

Tools	Sumber Bukti	Artefak Utama	Kontribusi
FTK Imager	Browser profile	History, Web Data, Cache, Local Storage, Session	Cookies, Login, Local Session Akuisisi sumber bukti
DB Browser for SQLite	Browser database	History, Web Data, Login Data	Pemeriksaan database dan data terstruktur
Autopsy	Browser storage	History, Cache, Local Storage, Session	Pemeriksaan artefak file dan storage
Wireshark	PCAP	DNS, IP, TLS SNI	Pemeriksaan komunikasi jaringan

Tabel 5 menunjukkan adanya pembagian fungsi yang jelas di antara *tools* yang digunakan. FTK Imager menyediakan sumber bukti melalui proses akuisisi, sedangkan DB Browser for SQLite dan Autopsy melakukan pemeriksaan pada *browser evidence* dengan karakteristik objek yang berbeda. Wireshark memberikan pemeriksaan pada sumber bukti jaringan.

Hasil tersebut menunjukkan bahwa pemanfaatan *tools* dalam investigasi tidak diarahkan pada penggunaan satu *tools* untuk seluruh jenis bukti. Setiap *tools* ditempatkan berdasarkan karakteristik sumber evidence yang diperiksa. DB Browser for SQLite memberikan hasil pada struktur database, Autopsy memberikan hasil pada cache dan storage, sedangkan Wireshark memberikan bukti pada tingkat jaringan. Kombinasi tersebut menghasilkan cakupan pemeriksaan yang saling melengkapi dalam mengidentifikasi aktivitas *credential phishing*.

3.6. Pembahasan

Hasil penelitian memperlihatkan bahwa aktivitas *credential phishing* pada Discord Web menghasilkan artefak yang tersebar pada beberapa sumber bukti. Pada *browser evidence*, URL <https://xn--dscord-waa.online/> ditemukan pada History menggunakan DB Browser for SQLite dan jejak domain yang sama juga ditemukan pada pemeriksaan Autopsy. Selain itu, Autopsy menemukan login.html, email dummy, dan username pada artefak storage. Pada sisi jaringan, Wireshark menghasilkan DNS, IP server *phishing*, dan TLS SNI yang berkaitan dengan domain *phishing*.

Temuan tersebut menunjukkan bahwa satu jenis aktivitas dapat meninggalkan artefak pada lokasi yang berbeda. Ketika cookie dari domain *phishing* tidak ditemukan dan Login Data menghasilkan 0 record, pemeriksaan masih dapat memperoleh bukti dari History, Cache, Session Storage, dan *network evidence*. Kondisi tersebut menunjukkan pentingnya pemeriksaan terhadap beberapa sumber bukti dalam investigasi *credential phishing*.

Pemanfaatan *tools* pada penelitian ini juga menunjukkan adanya pembagian fungsi berdasarkan karakteristik artefak. FTK Imager berfungsi menyediakan sumber bukti untuk pemeriksaan, DB Browser for SQLite digunakan untuk membaca dan mengolah database browser, Autopsy digunakan untuk menelusuri artefak pada cache dan storage, sedangkan Wireshark digunakan untuk menganalisis komunikasi jaringan. Oleh karena itu, hasil penelitian menunjukkan bahwa pemanfaatan *tools* secara komplementer dapat memberikan gambaran bukti yang lebih luas dibandingkan pemeriksaan yang hanya berfokus pada satu sumber *evidence*.

4. Kesimpulan

Berdasarkan hasil penelitian, metode OSCAR yang terdiri atas *Obtain, Strategize, Collect, Analyze*, dan *Report* dapat diterapkan untuk mengorganisasi proses investigasi *credential phishing* pada Discord Web. Penerapan metode tersebut memberikan alur pemeriksaan yang terstruktur mulai dari identifikasi sumber bukti, penentuan *tools*, akuisisi *evidence*, analisis artefak, hingga dokumentasi temuan forensik.

Hasil penelitian menunjukkan bahwa setiap *tools* memiliki fungsi yang berbeda berdasarkan karakteristik sumber bukti yang diperiksa. FTK Imager digunakan untuk melakukan akuisisi *browser profile* yang mencakup History, Cookies, Web Data, Login Data, Cache, Local Storage, dan Session Storage. DB Browser for SQLite digunakan untuk memeriksa database browser dan berhasil mengidentifikasi URL <https://xn--dscord-waa.online/>, cookie yang berkaitan dengan layanan Discord, serta informasi berupa email dan username. Pemeriksaan Login Data tidak menghasilkan

data login tersimpan, sedangkan cookie dari domain *phishing* juga tidak ditemukan.

Autopsy menghasilkan artefak dari History, Cache, Local Storage, dan Session Storage. Pemeriksaan menemukan jejak domain xn--dscord-waa.online, halaman login.html, email dummy, dan username yang mendukung identifikasi interaksi browser dengan halaman *phishing*. Sementara itu, Wireshark menghasilkan artefak jaringan berupa DNS, IP server *phishing*, TLS SNI domain *phishing*, dan TLS SNI Discord resmi. Temuan tersebut menunjukkan bahwa pemeriksaan pada sumber browser dan jaringan memberikan informasi yang saling melengkapi dalam mengidentifikasi aktivitas *credential phishing*.

Dengan demikian, pemanfaatan FTK Imager, DB Browser for SQLite, Autopsy, dan Wireshark dalam alur OSCAR menunjukkan bahwa pemeriksaan forensik pada Discord Web tidak bergantung pada satu *tools*, tetapi memerlukan pemanfaatan *tools* berdasarkan karakteristik sumber bukti dan jenis artefak. Pemetaan antara tahapan investigasi, sumber bukti, *tools*, artefak, dan temuan memberikan gambaran mengenai kontribusi masing-masing *tools* dalam proses pemeriksaan *credential phishing* pada Discord Web.

Ucapan Terimakasih

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 181/KPA/C4/KPT/2026.

Daftar Rujukan

- [1] K. Gupta, C. Varol, and B. Zhou, "Digital forensic analysis of discord on google chrome," *Forensic Science International: Digital Investigation*, vol. 44, p. 301479, Mar. 2023, doi: 10.1016/j.fsidi.2022.301479.
- [2] M. Davis, B. McInnes, and I. Ahmed, "Forensic investigation of instant messaging services on linux OS: Discord and Slack as case studies," *Forensic Science International: Digital Investigation*, vol. 42, p. 301401, Jul. 2022, doi: 10.1016/j.fsidi.2022.301401.
- [3] R. Melyanti, M. Iqbal, and M. Muhandi, "Sistem Informasi Manajemen Penelitian Dan Pengabdian Masyarakat Di Bagian P3M (Studi Kasus: Stmik Hang Tuah Pekanbaru)," *Jurnal Ilmu Komputer*, vol. 9, no. 2, pp. 165–176, 2020, doi: 10.33060/jik/2020/vol9.iss2.186.
- [4] A. Raza, M. Hussain, H. Tahir, M. Zeeshan, M. A. Raja, and K.-H. Jung, "Forensic analysis of web browsers lifecycle: A case study," *Journal of Information Security and Applications*, vol.

- 85, p. 103839, Sep. 2024, doi: 10.1016/j.jisa.2024.103839.
- [5] S. Berham and S. Morris, "A Critical Comparison Of Brave Browser And Google Chrome Forensic Artefacts," *Journal of Digital Forensics, Security and Law*, 2022, doi: 10.15394/jdfsl.2022.1752.
- [6] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterp. Inf. Syst.*, vol. 16, no. 4, pp. 527–565, Apr. 2022, doi: 10.1080/17517575.2021.1896786.
- [7] S. Asiri, Y. Xiao, S. Alzahrani, S. Li, and T. Li, "A Survey of Intelligent Detection Designs of HTML URL Phishing Attacks," *IEEE Access*, vol. 11, pp. 6421–6443, 2023, doi: 10.1109/ACCESS.2023.3237798.
- [8] M. Ahmed *et al.*, "PhishCatcher: Client-Side Defense Against Web Spoofing Attacks Using Machine Learning," *IEEE Access*, vol. 11, pp. 61249–61263, 2023, doi: 10.1109/ACCESS.2023.3287226.
- [9] P. Kumari, K. Shukla, and K. Modi, "Reconstructing User Activity Through Browser Forensics By Examining Techniques And Ethical Considerations," *Journal of Digital Security and Forensics*, vol. 2, no. 2, Dec. 2025, doi: 10.29121/digisecforensics.v2.i2.2025.67.
- [10] F. Paligu and C. Varol, "Browser Forensic Investigations of Instagram Utilizing IndexedDB Persistent Storage," *Future Internet*, vol. 14, no. 6, p. 188, Jun. 2022, doi: 10.3390/fi14060188.
- [11] A. Yudhana, I. Riadi, and S. Suharti, "Network Forensics Against Volumetric-Based Distributed Denial of Service Attacks on Cloud and the Edge Computing," *International Journal of Safety and Security Engineering*, vol. 12, no. 5, pp. 577–588, Oct. 2022, doi: 10.18280/ijss.120505.
- [12] R. R. Chand, J. Kumar, A. Prasad, and S. Chand, "Effectiveness of Forensic Tools in Extracting Web Browser Artifacts," in *2025 International Conference on Sustainable Technology and Engineering (i-COSTE)*, IEEE, Dec. 2025, pp. 1–5, doi: 10.1109/i-COSTE68047.2025.11467264.
- [13] A. M. Alotibi, S. Y. Altaaleedi, T. Zia, and E. U. H. Qazi, "Examining the Behavior of Web Browsers Using Popular Forensic Tools," *International Journal of Digital Crime and Forensics*, vol. 16, no. 1, pp. 1–22, Jul. 2024, doi: 10.4018/IJDCF.349218.
- [14] R. R. Chand, N. A. Sharma, and M. A. Kabir, "Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques," *SN Comput. Sci.*, vol. 6, no. 4, Apr. 2025, doi: 10.1007/s42979-025-03921-6.
- [15] F. N. Aqil and I. Riadi, "Forensic Analysis of Phishing Attacks on Discord Services using National Institute of Standards and Technology Method," *Int. J. Comput. Appl.*, vol. 187, no. 126, pp. 1–8, Jul. 2026, doi: 10.5120/ijca916b65015145.
- [16] Z. Y. Rivai, A. Yudhana, and I. Riadi, "Analisis Forensik Digital Terhadap Kasus Phishing Pada Discord Mobile Menggunakan Metode OSCAR," *CyberSecurity dan Forensik Digital*, vol. 9, no. 1, pp. 43–53, May 2026, doi: <https://doi.org/10.14421/csecurity.2026.9.1.566>.
- [17] D. A. Akbar, M. Rahdian, E. Kurnia, R. M. Genggam, S. Bintang, and R. Purwoko, "Analisis Web Phishing Menggunakan Metode Oscar Forensic (Studi Kasus: Follower Instagram Gratis)," *JTINFO: Jurnal Informatika*, vol. 3, no. 1, pp. 18–24, 2024, doi: <https://doi.org/10.02220/jtinfo.v3i1.855>.
- [18] R. P. Prambudi, I. Riadi, and Murinto, "Analisis Forensik Mobile pada Aplikasi E-Commerce Menggunakan Metode Association of Chief Police Officers," *Cyber Security dan Forensik Digital*, vol. 8, no. 1, pp. 44–52, Jun. 2025, doi: 10.14421/csecurity.2025.8.1.5234.

