Journal of Information Systems Management and Digital Business(JISMDB)
Volume 1, No 3 – April 2024
ISSN 3026-1449

ANALISIS FORENSIK APLIKASI DISCORD PADA ANDROID BERDASARKAN ACPO FRAMEWORK

Aura Nirmala[1], Mahaputra Giovani [2], Jeckson Sidabutar[3]
[1,2,3]Politeknik Siber dan Sandi Negara
[1]aura.nirmala@student.poltekssn.ac.id [2]mahaputra.giovani@student.poltekssn.ac.id
[3]jeckson.sidabutar@poltekssn.ac.id

Received: 26-01-2024	Revised: 02-02-2024	Approved: 30-03-2024

ABSTRAK

Discord, sebagai platform komunikasi populer di kalangan para gamers, seringkali menjadi wadah bagi komunitas-komunitas untuk berinteraksi Sayangnya, popularitasnya juga menarik perhatian para penjahat yang memanfaatkannya untuk melancarkan aksi kejahatan seperti penipuan dan penyebaran konten ilegal. Oleh karena itu, menjadi penting untuk melakukan analisis forensik guna mengumpulkan bukti digital yang sah dalam konteks hukum. Penelitian ini bertujuan mengumpulkan bukti digital dari aplikasi Discord mobile melalui simulasi kejahatan pada virtual machine Android. Metode yang digunakan melibatkan live forensics dengan tools seperti MOBILedit dan Autopsy, dengan kerangka kerja ACPO sebagai panduan tahapan forensik. Dari empat skenario kejahatan yang disimulasikan, tiga skenario berhasil menghasilkan bukti digital sebesar 57,8%, sementara satu skenario tidak menghasilkan bukti digital (0%). Penelitian ini menjadi kontribusi penting dalam ilmu forensik, khususnya dalam ranah mobile forensics, mengingat mayoritas penelitian sebelumnya fokus pada aplikasi Discord di sistem operasi Windows atau berbasis web.

Kata Kunci: *Android, Autopsy, Discord, Framework ACPO, Forensik, MOBILedit*

PENDAHULUAN

Pengguna android terus berkembang, menunjukkan dominasi yang berkelanjutan di pasar perangkat mobile global (*Mobile Operating System Market Share Worldwide | Statcounter Global Stats*, n.d.). Salah satu platform populer adalah Discord, terutama di perangkat Android (Afdal et al., 2022). Discord dikenal sebagai aplikasi komunikasi, khususnya di antara pemain video game, menyediakan fitur obrolan suara, video, pesan teks, serta berbagi gambar, video, dan tautan melalui pesan pribadi, grup, atau server komunitas (Anderson, 2019). Namun, aplikasi ini juga disalahgunakan untuk kegiatan kriminal, seperti penyebaran konten ilegal dan kejahatan siber seperti penipuan, pemerasan, dan pencurian data (*Discord Forensics*, n.d.). Discord telah mengambil tindakan dengan memblokir grup dan menutup komunitas yang melanggar ketentuan (Afdal et al., 2022).

Forensik digital merupakan ilmu atau metode yang digunakan untuk menyelidiki dan mengungkap kejahatan terutama dalam lingkup digital (Iman et al., 2020). Beberapa penelitian telah menganalisis aplikasi Discord dari sudut pandang forensik digital, namun mayoritas berfokus pada platform Windows atau web. Penelitian pertama (Afdal et al., 2022) membahas analisis forensik pada aplikasi Discord berbasis Windows dengan menggunakan metode National Institute of Standards Technology (NIST) dan tools yang digunakan tool FTK Imager. Selanjutnya, penelitian kedua (Iqbal et al., 2021; Motylinski et al., 2020) berfokus pada analisis forensik pada sisi klien Discord, memanfaatkan tools DiscFor yang dirancang untuk ekstraksi, analisis, dan penyajian data Discord serta konversi file data ke format yang mudah dibaca. Penelitian ketiga (Gupta et al., 2023) mengungkap hasil forensik aplikasi Discord pada browser dengan menunjukkan bahwa Discord menggunakan mekanisme penyimpanan yang serupa di desktop maupun browser, menggunakan metode eksperimen quasi-pretest-posttest. Terakhir, penelitian keempat (Moffitt et al., 2021) memeriksa struktur aplikasi Discord pada Android dengan metodologi analisis yang merinci aspek komunikasi, struktur data, protokol komunikasi, dan metode investigasi.

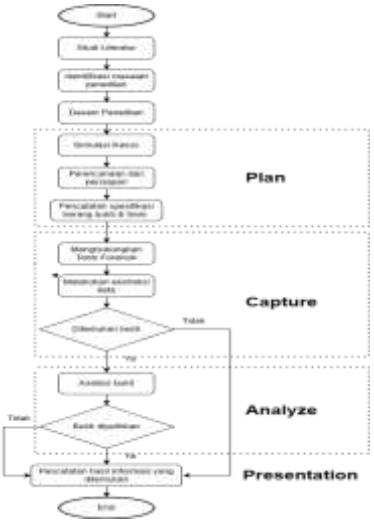
Penelitian sebelumnya menggunakan framework National Institute of Standards

Technology (NIST) atau framework internal, dan mayoritas fokus pada PC (Windows) dan Chrome (Web Application). Penelitian pada platform mobile, khususnya Android, masih jarang dilakukan. Kesenjangan analisis forensik terutama terletak pada kurangnya penelitian pada platform mobile. Oleh karena itu, penelitian ini mengisi kekosongan ini dengan fokus pada pengembangan metodologi forensik pada Discord Mobile (Android). Penelitian akan menggunakan ACPO sebagai framework analisis forensik untuk mengembangkan teknik yang relevan untuk penanganan kasus pada platform komunikasi ini. Dalam penelitian (Jafri et al., 2022) menunjukkan bahwa framework ACPO menunjukkan persentase kesuksesan dalam mendapatkan bukti digital sebesar 66,6% dibandingkan dengan framework NIST yang memiliki persentase sebesar 57,1%. Kemudian framework ACPO juga dipakai oleh beberapa peneliti dalam melakukan forensik mobile seperti penelitian (Ermin et al., 2023) melakukan forensik aplikasi DANA, penelitian (Riadi et al., 2023) melakukan forensik aplikasi MiChat, dan penelitian (Safitri et al., 2023) melakukan forensik pada aplikasi IMO instant messaging.

Tujuan dilakukannya penelitian ini adalah untuk melakukan analisis bukti digital pada aplikasi android yaitu Discord Mobile. Dalam penelitian ini menggunakan virtual machine android yang sudah diroot, namun hal yang dilakukan sama seperti melakukan forensik pada mesin aslinya. Dalam melakukan pengujian analisis bukti digital dilakukan dengan beberapa skenario. Tools yang digunakan untuk melakukan analisis forensik digital adalah MOBILedit dan Autopsy. MOBILedit merupakan alat forensik yang memungkinkan penyidik untuk memperoleh secara logic, mencari, dan memeriksa perangkat ponsel (Nasirudin et al., 2020). Alat ini menggunakan beberapa mekanisme konektivitas terutama konektivitas nirkabel dibandingkan dengan alat sejenis. Sedangkan, Autopsy merupakan software forensik yang dirancang untuk mengekstrak, memulihkan, menganalisis, melakukan triase data dari berbagai perangkat seluler serta memungkinkan untuk pengumpulan bukti real-time dan analisis data sensitif (Dedy Hariyadi, 2022). Diharapkan, penelitian ini akan memberikan kontribusi signifikan dalam pengembangan teknik forensik yang relevan untuk menangani kasus-kasus yang melibatkan aplikasi komunikasi ini, khususnya pada platform mobile Android.

METODE PENELITIAN

Tujuan utama dari penelitian ini adalah untuk mengumpulkan bukti digital dari aplikasi Discord di smartphone berbasis Android menggunakan ACPO Framework dan menggunakan alat forensik MOBILedit dan Autopsy untuk melakukan analisis. Penelitian ini menggunakan pendekatan kualitatif dan kuantitatif. Untuk memperoleh data dan pengolahannya menggunakan pendekatan kualitatif dan untuk menguji hasilnya menggunakan pendekatan kuantitatif. Sumber data yang digunakan dalam penelitian ini berdasarkan skenario yang dibuat dengan aplikasi Discord.



Gambar 1. Desain penelitian

A. ACPO Framework

ACPO Framework adalah kerangka kerja forensik digital yang dikembangkan oleh ACPO (Association of Chief Police Officers) bekerja sama dengan 7Safe untuk memperoleh bukti digital yang valid dalam kasus pengadilan (Ermin et al., 2023). Kerangka kerja ini memiliki tahapan seperti pada Gambar 2.

Gambar 2. Tahapan ACPO Framework

Tahapan-tahapan tersebut dijelaskan secara rinci sebagai berikut:

1. Plan
   Merupakan tahap perencanaan, dimana dilakukan perancangan segala sesuatu yang akan dilakukan selama penelitian berlangsung. Di dalamnya berisi pembuatan proses penelitian, dan menentukan software atau tools yang akan digunakan.
2. Capture
   Tahap ini melakukan akuisisi data atau mengkloning data dari smartphone yang digunakan dengan menggunakan tools yang tersedia.
3. Analyze
   Tahap ini menganalisa data yang telah didapatkan untuk mengetahui artefak apa saja yang dapat dimanfaatkan sebagai barang bukti digital.
4. Presentation
   Tahap ini adalah merilis data penelitian yang kini menjadi informasi yang relevan dan dapat dipertanggungjawabkan. Tindakan dan hasil penelitian diberikan secara lengkap. Saran-saran yang terkait dengan hasil penelitian juga diberikan.

B. Simulasi Kasus

Peneliti membuat simulasi kejahatan dengan menggunakan fitur-fitur Discord Mobile seperti channel percakapan, pesan pribadi, riwayat panggilan suara dan video, dan lampiran seperti foto, video dan dokumen. Pembuatan skenario dilakukan untuk mendapatkan bukti digital dengan tidak ada batasan waktu tertentu pada aplikasi Discord kemudian smartphone yang digunakan sudah diroot. Seperti yang ditunjukkan pada Tabel 1.

Tabel 1.
Tes yang dilakukan

No	Tes yang diujikan	Jumlah data yang di tes
1.	Tidak ada penghapusan data chat dalam aplikasi	57
2.	Penghapusan data chat pada aplikasi	
3.	Pada saat meninggalkan server Discord	
4.	Aplikasi Discord di Uninstall	

C. Perhitungan Bukti Digital

Penelitian ini akan menggunakan perhitungan untuk membandingkan tindakan yang telah disimulasikan dalam skenario. rumus yang digunakan adalah menghitung persentase bukti digital yang ditemukan setelah semua tahapan investigasi forensik digital dilakukan. Proses perhitungan persentase menggunakan persamaan yang diolah kembali dari penelitian (Surya et al., 2023) yang dirincikan sebagai berikut.

$$Pn = \frac{B}{N}\ x\ 100\% \qquad (1)$$

Deskripsi
Pn = persentase yang diharapkan dari skenario
B = jumlah bukti digital yang ditemukan
N = jumlah bukti digital yang dianalisis

HASIL DAN PEMBAHASAN

Penelitian ini berhasil mendapatkan bukti digital, dimana bukti digital tersebut didapatkan dari ekstraksi data dan analisis cache pada aplikasi Discord Mobile.

A. Plan

Pada proses ini, kami melakukan simulasi kasus dengan skema penipuan yang dimana rincian data bukti digitalnya sebagai berikut:

Tabel 2.
Rincian Data Skenario

Jenis Data	Jumlah Data
Pesan teks	48
Gambar	3
Video	3
Dokumen	3

Kemudian untuk melakukan analisis bukti digital, kami menggunakan beberapa alat dan tools, yaitu:

Tabel 3.
Alat dan Tools Penelitian

Nama alat/tools	Versi	Peran/Fungsi
Android Studio (Google Pixel 3A API 34)	Android 14	Obyek Penelitian
Laptop Acer Aspire 3	Windows 11 Pro 23H2	Host untuk virtual machine
Android Debug Bridge (ADB)	-	Akuisisi data
MOBILedit Forensic Express Pro	v7.4.0.20393	Analisis secara otomatis
Autopsy	4.21.0	Analisis secara manual
Discord Mobile	208.17 – Stable	Aplikasi yang diteliti

B. Capture

Pada tahapan ini kami melakukan akuisisi data atau mengkloning data dari smartphone yang digunakan (Google Pixel 3A API 34 – Android Studio) dengan menggunakan tools ADB (Android Debug Bridge). Berikut ini merupakan hasil dari proses capture data yang terlihat pada Gambar 3.

Gambar 3. Hasil proses capture data

Tabel berikut merupakan rincian proses dan hasil yang didapatkan dari proses capture yang dilakukan.

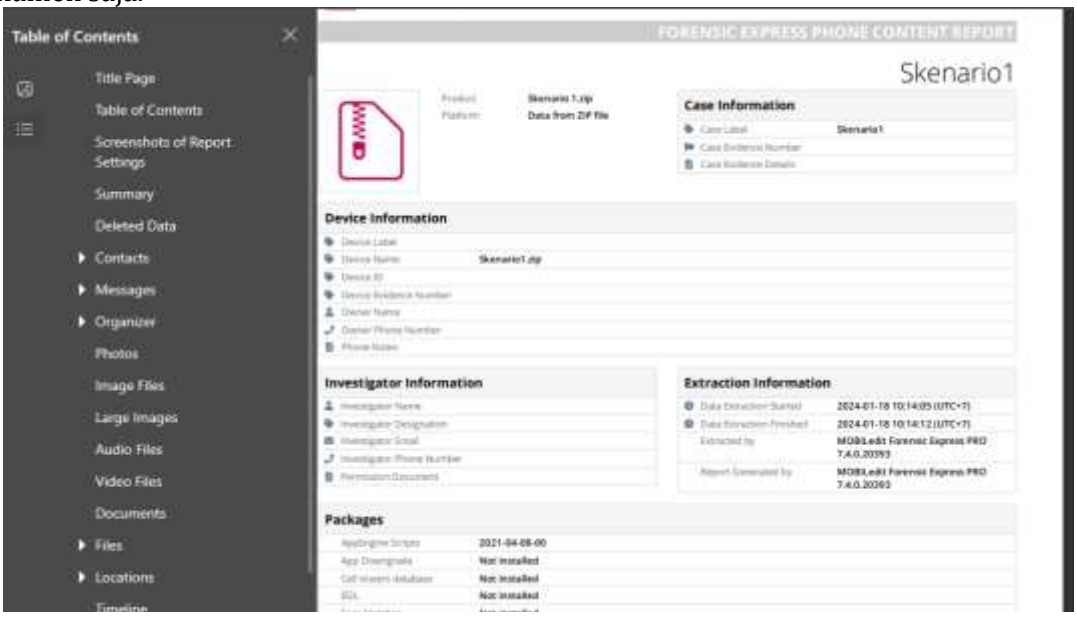
Tabel 4.
Hasil Akuisisi/Capture

File	Ukuran File	Hash (MD5)
Skenario 1.zip	242 MB	996a31d3d771d8f2dcca32819489788a
Skenario 2.zip	242 MB	009db915379bca5a94ca27aef4f6f83a
Skenario 3.zip	242 MB	24d3c81e0e3811ee729559a4642c5ba6
Skenario 4.zip	102 MB	886fa96da6ed22d37f512da267eef6eb

C. Analyze

Pada proses ini dilakukan analisis pada folder data yang di akuisisi pada tahapan sebelumnya. Dilakukan sebanyak dua kali analisis, yaitu:

1. Analisis secara otomatis dari MOBILedit, berhasil menemukan gambar, video, dan dokumen saja.



Gambar 4. Hasil analisis secara otomatis dengan MOBILedit

2. Analisis secara manual menggunakan Autopsy untuk menemukan ekstrak pesan teks pada cache aplikasi Discord.

Gambar 5. Proses analisis secara manual dengan Autopsy

D. Presentation

Setelah dilakukan tahapan analyze, dilakukan tahap presentation yang merupakan tahapan terakhir dari kerangka kerja ACPO. Pada tahap ini melaporkan hasil analisis bukti digital pada skenario 1, 2, 3, dan 4.

Tabel 5.
Hasil laporan

Bukti Digital	Skenario 1	Skenario 2	Skenario 3	Skenario 4
Gambar	2	2	2	0
Video	3	3	3	0
Dokumen	2	2	2	0
Pesan Teks	26	26	26	0
Total	57,8%	57,8%	57,8%	0%

Berikut adalah rincian untuk scenario 1, 2, dan 3 berdasarkan tabel hasil laporan:
Perhitungan akurasi bukti gambar yang didapatkan:

$$Pn = \frac{2}{3}\ x\ 100\% = 66{,}67\% \quad (2)$$

Perhitungan akurasi bukti video yang didapatkan:

$$Pn = \frac{3}{3}\ x\ 100\% = 100\% \quad (3)$$

Perhitungan akurasi bukti dokumen yang didapatkan:

$$Pn = \frac{2}{3}\ x\ 100\% = 66{,}67\% \quad (4)$$

Perhitungan akurasi bukti pesan teks yang didapatkan:

$$Pn = \frac{26}{48}\ x\ 100\% = 54{,}16\% \quad (5)$$

Sementara perhitungan akurasi bukti pada skenario 4 didapatkan 0 %.

KESIMPULAN

Setelah melakukan analisis bukti digital melalui serangkaian tahapan kerangka kerja ACPO dan mensimulasikan empat skenario, peneliti menyimpulkan bahwa hasil forensik digital dari aplikasi Discord mobile pada skenario pertama, di mana tidak terjadi perubahan atau penghapusan data uji, berhasil ditemukan bukti digital sebanyak 57,8% dari total 57 data yang diujikan. Selanjutnya, pada skenario kedua yang melibatkan penghapusan beberapa data pesan uji, bukti yang ditemukan ternyata serupa dengan skenario pertama. Hal serupa juga terjadi pada skenario ketiga, di mana pengguna keluar dari saluran server Discord sebelum dilakukan analisis forensik, dan bukti digital yang ditemukan sama dengan skenario satu dan dua. Namun, pada skenario keempat di mana aplikasi Discord sudah dihapus dari perangkat, hasil analisis tidak mengungkapkan bukti digital.

Penelitian ini mengungkap bahwa proses forensik terhadap bukti digital dari aplikasi Discord pada perangkat Android dapat dilakukan, tidak hanya terbatas pada sistem operasi Windows atau platform berbasis web. Diharapkan penelitian selanjutnya dapat memperluas cakupan dengan melakukan akuisisi bukti digital pada sistem operasi iOS atau melakukan forensik terhadap varian berbasis web yang terintegrasi dalam aplikasi mobile seperti Google Chrome.

DAFTAR PUSTAKA

Afdal, A. M., Salim, Y., & Rachman Manga', A. (2022). Analisis Bukti Digital Forensik pada

Discord Menggunakan Metode National Institute of Standards Technology. *Buletin Sistem Informasi Dan Teknologi Islam* , *3*(4), 293–300.

Anderson, M. (2019). *Discord and The Harbormen Gaming Community*. https://mayajanae.com/wp-content/uploads/2020/01/Discord-and-the-Harbormen-Gaming-Community.pdf

Dedy Hariyadi. (2022). *Buku Panduan Dasar Forensik Digital*. PENERBIT BASKARA MEDIA. https://www.researchgate.net/publication/365993681

Discord Forensics. (n.d.). Retrieved December 14, 2023, from https://oxygenforensics.com/en/resources/discord-forensics/

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. https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Gupta, K., Varol, C., & Zhou, B. (2023). Digital Forensic Analysis of Discord on Google Chrome. *Forensic Science International: Digital Investigation*, *44*. https://doi.org/10.1016/j.fsidi.2022.301479

Iman, N., Susanto, A., & Inggi, R. (2020). Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review). *Jurnal Telekomunikasi Dan Komputer*, *9*(3), 186. https://doi.org/10.22441/incomtech.v9i3.7210

Iqbal, F., Motylinski, M., & MacDermott, A. (2021, April 19). Discord Server Forensics: Analysis and Extraction of Digital Evidence. *2021 11th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2021*. https://doi.org/10.1109/NTMS49979.2021.9432654

Jafri, M. S., Raharjo, S., & Arief, M. R. (2022). *Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones*. *15*(1).

Mobile Operating System Market Share Worldwide | Statcounter Global Stats. (n.d.). Retrieved December 14, 2023, from https://gs.statcounter.com/os-market-share/mobile/worldwide

Moffitt, K., Karabiyik, U., Hutchinson, S., & Yoon, Y. H. (2021). Discord Forensics: The Logs Keep Growing. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, 993–999. https://doi.org/10.1109/CCWC51732.2021.9376133

Motylinski, M., MacDermott, A., Iqbal, F., Hussain, M., & Aleem, S. (2020, November 3). Digital Forensic Acquisition and Analysis of Discord Applications. *Proceedings of the 2020 IEEE International Conference on Communications, Computing, Cybersecurity, and Informatics, CCCI 2020*. https://doi.org/10.1109/CCCI49893.2020.9256668

Nasirudin, Sunardi, & Riadi, I. (2020). Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, *5*(1). http://openjournal.unpam.ac.id/index.php/informatika89

Riadi, I., Yudhana, A., & Galih Pramuja Inngam Fanani. (2023). Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *7*(2), 286–292. https://doi.org/10.29207/resti.v7i2.4547

Safitri, Y., Riadi, I., & Sunardi, S. (2023). Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *22*(3), 651–664. https://doi.org/10.30812/matrik.v22i3.2987

Surya, M., Sidabutar, J., & Qomariasih, N. (2023). Comparative Analysis of Recovery Tools For Digital Forensic Evidence Using NIST Framework 800-101 R1. *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*.