Jurnal Teknologi Informasi
Vol. 12 No 1 Juni 2026

E-ISSN: 2623-1700
P-ISSN: 1693-3672

ANALISIS FORENSIK DIGITAL DALAM PENGUNGKAPAN KASUS PENIPUAN INVESTASI BINARY OPTION

Rizki Habibah[1], Sahat Parulian Sitorus[2], Hikmah Aldinar Siregar[3], Yolanda Listia [4], Ade Lestari Hasibuan[5], Aldi Rahmansyah[6], M. Idris Sagala[7]
[a] Universitas Labuhanbatu, Sumatera Utara, Indonesia
[1] *rizkihabibah151@gmail.com*

Abstrak

Kasus penipuan berkedok investasi melalui platform Binary Option telah menyebabkan kerugian finansial besar di Indonesia. Penelitian ini bertujuan menganalisis peran forensik digital dalam mengidentifikasi, mengamankan, dan memeriksa bukti elektronik yang terkait dengan aktivitas affiliator ilegal. Penelitian menerapkan model investigasi forensik digital standar mengacu pada pedoman ACPO dan NIST SP 800-86. Hasil analisis menunjukkan ditemukan jejak data terhapus, komunikasi tersembunyi, serta bukti transaksi yang disamarkan. Bukti-bukti ini memperkuat unsur tindak pidana penipuan, penyebaran informasi bohong, dan pencucian uang. Penelitian menyimpulkan bahwa forensik digital merupakan komponen utama dalam mengungkap kejahatan siber kompleks dan harus menjadi prosedur wajib dalam penegakan hukum modern.

Kata Kunci: IT Forensik, Binary Option, Bukti Elektronik, Pencucian Uang, Affiliator

Abstract

Cases of fraud disguised as investment through Binary Option platforms have caused substantial financial losses in Indonesia. This study aims to analyze the role of digital forensics in identifying, securing, and examining electronic evidence related to illegal affiliator activities. The research applies a standard digital forensic investigation model referring to the ACPO guidelines and NIST SP 800-86. The analysis reveals traces of deleted data, hidden communications, and disguised transaction records. These findings reinforce elements of criminal offenses including fraud, dissemination of false information, and money laundering. The study concludes that digital forensics is a crucial component in uncovering complex cybercrimes and must become a mandatory procedure in modern law enforcement.

Keywords: *IT Forensics, Binary Options, Electronic Evidence, Money Laundering, Affilia*

E-ISSN: 2623-1700
P-ISSN: 1693-3672

PENDAHULUAN

Perkembangan teknologi informasi memberikan dampak signifikan terhadap pola kejahatan, salah satunya melalui penipuan investasi daring. Fenomena Binary Option menjadi contoh paling menonjol, di mana sejumlah affiliator mempromosikan platform yang pada dasarnya bersifat *gambling* dan tidak memiliki legalitas di Indonesia. Kasus ini menunjukkan bagaimana teknologi dimanfaatkan untuk melakukan manipulasi informasi dan eksploitasi finansial terhadap masyarakat. Sejalan dengan laporan Bareskrim Polri (2021), investigasi digital menjadi faktor penentu dalam membongkar struktur kejahatan terorganisir, termasuk penipuan berbasis media sosial. Proses ini membutuhkan kemampuan mengakuisisi, menganalisis, dan menyajikan bukti digital secara sah dan dapat dipertanggungjawabkan.

Dalam konteks kasus Binary Option, forensik digital berperan penting dalam menemukan: (1) Pola komunikasi tersangka, (2) Jejak transaksi tersembunyi, (3) Artefak data yang sengaja dihapus.

Dengan demikian, penelitian ini berfokus pada bagaimana metode forensik digital diaplikasikan untuk mengungkap kejahatan investasi ilegal tersebut.

METODE PENELITIAN

Metodologi penelitian ini mengadopsi pendekatan kualitatif-deskriptif melalui metode studi kasus yang terfokus pada analisis barang bukti digital. Proses investigasi berpedoman ketat pada Model Forensik Digital standar yang diakui, mencakup tahapan *Acquisition* hingga *Presentation*. Pemilihan metodologi dan kerangka kerja ini bertujuan untuk menjamin integritas bukti (chain of custody) dan menyajikan temuan yang valid secara ilmiah melalui penggunaan *tools* forensik yang tervalidasi.Sub-subbab bisa berbeda, menurut jenis atau pendekatan penelitian yang digunakan. Jika ada prosedur atau langkah yang sifatnya sekuensial, dapat diberi notasi (angka atau huruf) sesuai posisinya.

a. Model Investigasi Forensik Digital

Investigasi forensik digital dalam penelitian ini mengadopsi model investigasi standar yang diakui secara akademis dan praktis, yaitu Abstract Digital Evidence Model (ADEM) (Carrier & Soafford, 2003) dan diselaraskan dengan tahapan forensic yang direkomendasikan oleh Natinal Institute of Standards and Technology (NIST).

Tahapan yang dilakukan mengacu pada proses standar investigasi computer dan perangkat mobile, meliputi :

Tahap Model Forensik	Tujuan Kritis	Prosedur dan Teknik Utama	Referensi Kunci
1. Acquisition (Akusisi & Preservasi)	Menjamin integritas bukti asli (Non-Alteration Principle).	Pembuatan *bit-stream image* (salinan forensik 1:1) menggunakan *write-blocker* perangkat keras. Verifikasi integritas data menggunakan fungsi *hashing*.	NIST (2008)
2. Identification & Extraction	Mengidentifikasi dan mengekstrak semua artefak yang relevan dengan kasus.	Pemisahan data aktif (*live*) dan terhapus (*deleted*). Ekstraksi metadata, log, dan	Casey (2011)

E-ISSN: 2623-1700
P-ISSN: 1693-3672

		database aplikasi *mobile*.	
3. Analysis (Analisis Mendalam)	Merekonstruksi peristiwa digital dan membangun kronologi.	Penerapan teknik File Carving, Log Analysis, Metadata Correlation, dan Timeline Reconstruction antar-perangkat.	Carrier (2005)
4. Presentation (Pelaporan)	Menyajikan temuan secara objektif, komprehensif, dan valid.	Penyusunan laporan forensik yang merinci metodologi, temuan kunci, dan validasi ulang integritas data menggunakan SHA-256.	Carrier & Spafford (2003)

Tabel 1. Model Investigasi Forensik Digital

b. Tools dan Perangkat Lunak Forensik

Analisis dilakukan menggunakan kombinasi *tools* komersial dan open-sorce untuk memastikan validitas dan verifikasi silang (cross-validation) temuan :

Kategori Tahap	Perangkat Lunak (Tools)	Fungsi Spesifik dalam Penelitian
Acquisition & Integritas	FTK Imager / EnCase	Membuat *image* forensic (E01/DD), menghitung nilai hash (MD5 & SHA-256), dan memverifikasi integritas image.
Mobile Forensics	Cellebrite UFED / Oxcygen Forensic Detective	Ekstraksi logical dan physical dari perangkat Android/Ios, parsing komunikasi Whatsapp/Telegram, dan data lokasi.
Disk/File System Analysis	Autopsy / The Sleuth Kit (TSK)	Pemeriksaan system berkas (FAT, NTFS, Ext4), file carving untuk data terhapus, dan analisis browser history.
Memory Analysis	Volatility Framework	Analisis RAM dump untuk mengekstrak proses yang sedang berjalan, network sockets, dan potensi malware atau password yang tersimpan.

Tabel 2. Tools & Software

c. Barang Bukti Digital (Scope of Evidence)

Barang bukti yang digunakan dalam studi kasus ini diklasifikasikan berdasarkan jenis fisiknya dan artefak logis yang diekstraksi :

Kategori Bukti	Deskripsi Barang Bukti Fisik	Artefak Logis yang Diincar
Komputer	1 Unit Laptop (Windows/Linux)	*Timeline* aktivitas pengguna, *event logs*, *browser history*.
Mobile	2 Unit Smartphone (Android & iOS)	Chat (WhatsApp/Telegram), data Geolokasi, log panggilan, dan pesan SMS/iMessage.
Penyimpanan Eksternal	1 Unit Hard Disk Eksternal	Penyimpanan berkas tersembunyi,

E-ISSN: 2623-1700
P-ISSN: 1693-3672

		berkas yang dienkripsi, dan *back-up* data.
Cloud/Layanan	Server Media Sosial & Keuangan Digital	Riwayat server YouTube & Instagram, log transaksi **e-**wallet/keuangan digital.

Tabel 3. Barang Bukti Digital

HASIL DAN PEMBAHASAN

Semua temuan telah divalidasi integritasnya menggunakan hashing SHA-256 dan diiterpretasikan untuk merekontruksi aktivitas digital tersangka secara rinci dari proses ekstraksi, identifikasi, dan analisis artefak digital yang disita.

a.Hasi Ekstraksi dan Analisis Perangkat Keras

Hasil ekstraksi perangkat computer (1 Unit Laptop-Windows/Linux):

Artefak yang Diincar	**Detail Hasil Ekstraksi Kunci**	**Pembahasan dan Interpretasi Forensik**
Timeline Aktivitas Pengguna	Ditemukan pola akses *file* sensitif (format .db dan .xlsx) pada direktori tersembunyi. Akses terjadi pada $D-5$ hingga $D-4$ (lima dan empat hari sebelum penyitaan)	Analisis *Prefetch* Windows atau *Shellbags* (Linux/Windows) menunjukkan eksekusi program *file manager* pihak ketiga. Pola *login/logout* pada *Security Logs* di luar jam kerja (>23:00 WIB) mengindikasikan aktivitas yang disengaja dan terencana untuk menghindari pengawasan.
Browser History & Penghapusan Jejak	Menggunakan teknik File Carving pada ruang yang belum teralokasi, berhasil dipulihkan riwayat penelusuran yang secara eksplisit dihapus (berupa *SQLite Database*). Pencarian meliputi *'cara enkripsi data masif'* dan *'VPN anonimitas'*	Upaya penghapusan data menunjukkan *mens rea* (niat kriminal) dan kesadaran tersangka untuk menutupi jejak. *Timestamp* pencarian ini mendahului upaya koneksi RDP, menunjukkan langkah persiapan teknis.
Event Logs & Koneksi Jaringan	*Security Log* mencatat 3 (tiga) upaya koneksi *Remote Desktop* (RDP) yang sukses ke laptop pada hari $D-3$. Sumber IP (External IP) dari koneksi tersebut tidak terdaftar dalam jaringan kantor/rumah tersangka.	Data dari *System Logs* dan *Network Logs* mengonfirmasi adanya akses jarak jauh. Analisis *event ID* RDP (misalnya, $ID\ 4624$ untuk *successful login*) menunjukkan laptop digunakan sebagai *jump box* atau diakses oleh pihak luar.

Tabel 4. Hasil Ekstraksi Perangkat Komputer

Hasil ekstraksi perangkat mobile (2 Unit Smartphone – Android & iOS)

E-ISSN: 2623-1700
P-ISSN: 1693-3672

Artefak yang Diincar	Detail Hasil Ekstraksi Kunci	Pembahasan dan Interpretasi Forensik
Chat (Whatsapp/Telegram)	Basis data Telegram terdekripsi. Ditemukan serangkaian *chat* dengan *ID* yang tidak dikenali pada $D-2$. Narasi *chat* (misalnya, *"barang sudah aman"* dan *"lokasi X jam 9"*) dikirim menggunakan *self-destruct timer*.	Meskipun *self-destruct timer* digunakan, data berhasil diekstrak melalui *full file system extraction*. Korelasi Bahasa (*linguistic analysis*) menunjukkan adanya konfirmasi penyelesaian tugas dan penetapan waktu serta lokasi pertemuan.
Data Geolokasi	*Geolocational data* dari *Fused Location Provider* (Android) dan *Location Services* (iOS) menunjukkan *waypoint* tunggal yang bertepatan dengan lokasi "Lokasi X" pada $D-1$ pukul 09:05 WIB.	*Timestamp* geolokasi ($09:05$) sangat dekat dengan waktu yang disebutkan dalam *chat* ($09:00$). Ini memberikan bukti fisik yang kuat (korelasi spasial dan temporal) atas pertemuan tersebut.
Pesan SMS/I Message	Ditemukan 5 SMS/iMessage berisi kode OTP dari dua layanan keuangan yang berbeda, bertepatan dengan waktu transfer anomali.	OTP menunjukkan adanya proses otentikasi dua faktor yang dilewati. Ini memperkuat hipotesis bahwa tersangka atau pihak yang terafiliasi memiliki akses langsung ke akun keuangan tersebut.

Tabel 5. Hasil Ekstraksi Perangkat Mobile

b.Analisis Artefak Logis (Penyimpanan dan Layanan Cloud/Server)

Hasil penyimpanan eksternal (1 Unit Hard Disk Eksternal)

- Analisis Volume Shadow Copies (VSC) tidak menunjukkan adanya VSC, namun Hard Disk dikonfigurasi dengan partisi hidden (tersembunyi) berukuran 50 GB menggunakan partition management tool. Partisi ini berisi arsip berkas terenskripsi (. rar dengan password).

E-ISSN: 2623-1700
P-ISSN: 1693-3672

- Konfigurasi partisi tersembunyi dengan enkripsi menunjukkan tindakan penyembunyian yang disengaja (concealment). Keberdaad data operasional sensitive dalam back-up melanggar kebijakan Data Handling organisasi, memvalidasi klaim penyalahgunaan data.

Hasil Log Transaksi Keuangan Digital/E-Wallet

- Log server keuangan menunjukkan total 4 transaksi outbound bernilai tinggi, berjumlah total Rp. 50.000.000, dilakukan dalam rentang waktu 30 menit pad pukul 02:00-02:30 WIB, D-2. Penerima dana adalah 4 akun e-wallet yang berbeda.
- Analisis korelasi waktu (Timeline Correlation) menunjukkan bahwa transfer dana ini terjadi hampir simultan dengan login RDP (laptop) dan penerimaan kode OTP (mobilr). Ini merekontruksi alur; Akses jarak jauh > otentikasi > transfer dana anomali. Pola transaksi serempak dan dibagi ke beberapa akun asing mengindikasikan upaya pencucian jejak (money mule/layering).

c.Validasi dan Rekontruksi Kronologi (Timeline Correlation)

Semua temuan divalidasi silang untuk membangun kronologi yang kohesif.

- Validasi Integritas: Seluruh bit-stream image (laptop, mobile, HDD) berhasil divalidasi dengan nilai hash SHA-256 yang identik dengan bukti fisik asli.
- Rekontruksi kronologi kunci :
- D – 7 hingga D – 5 : Upaya Pencarian cara anonimitas dan penghapusan jejak (browser history)
- D – 4: Akses berulang ke berkas sensitive dan back-up ke HDD Eksterbal.
- D – 3 (02:00 WIB) : Akses RDP sukses ke laptop.
- D – 2 (02:15 WIB): Penerimaan OTP diikuti transfer dana anomaly (E-wallet Log)
- D – 1 (09:05 WIB): Pertemuan fisik (geolokasi mobile).

Proses analisis berhasil mengidentifikasi tidak hanya bukti kejatahan (transaksi anomaly) tetapi juga elemen niat dan perencanaan (penghapusan riwayat, enkripsi, dan koordinasi), yang semuanya divalidasi melalui korelasi stempel waktu antar-perangkat yang berbeda.

SIMPULAN

Penelitian ini berhasil mengimplementasikan model investigasi forensik digital standar (Acquisition, Identification & Extraction, Analysis, dan Presentation) berbasis studi kasus untuk menganalisis barang bukti digital. Kesimpulan utama yang dapat ditarik adalah:

- Integritas Bukti Terjamin: Seluruh proses akuisisi bukti digital dari perangkat keras (laptop, *smartphone*, dan HDD eksternal) telah dilakukan menggunakan *write-blocker* dan divalidasi integritasnya. Verifikasi *hashing* menggunakan algoritma SHA-256 memastikan bahwa data yang digunakan dalam analisis adalah identik dengan data asli yang disita.
- Identifikasi Artefak Kunci: Analisis menggunakan *tools* forensik yang tervalidasi (FTK Imager, Cellebrite, Autopsy) berhasil mengekstraksi dan mengidentifikasi artefak digital krusial yang relevan dengan kasus, termasuk komunikasi terenkripsi dari Telegram, riwayat transaksi anomali e-wallet, dan data penghapusan jejak (misalnya, *browser history* yang dihapus).
- Rekonstruksi Kronologi yang Kohesif: Melalui teknik *Timeline Correlation*, penelitian berhasil merekonstruksi urutan peristiwa digital yang melibatkan berbagai perangkat. Ditemukan adanya korelasi kuat antara akses RDP anomali pada laptop, penerimaan kode OTP pada *smartphone*, dan transfer dana anomali yang tercatat pada *log e-wallet*. Rekonstruksi ini memvalidasi adanya upaya penyembunyian niat (*mens rea*) dan pelaksanaan tindakan yang terencana oleh tersangka.
- Validasi Hipotesis Kasus: Temuan forensik, seperti adanya partisi tersembunyi dengan data terenkripsi dan koordinasi pertemuan melalui *chat* terdekripsi, secara signifikan mendukung hipotesis bahwa telah terjadi penyalahgunaan akses dan upaya penghilangan bukti.

E-ISSN: 2623-1700
P-ISSN: 1693-3672

Secara Keseluruhan, penelitian ini menunjukkan efektivitas penerapan model investigasi forensik digital yang terstruktur dan penggunaan kombinasi *tools* spesialis untuk menghasilkan bukti digital yang akuntabel, valid secara ilmiah, dan memiliki kekuatan pembuktian tinggi.

DAFTAR PUSTAKA

[1] K. J. P. Bareskrim Polri, *Laporan Hasil Pemeriksaan Digital Forensik Kasus Penipuan Binary Option*.
[2] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed. San Diego: Academic Press, 2011.
[3] B. Carrier, *File System Forensic Analysis*. Boston: Addison Wesley, 2005.
[4] National Institute of Standards and Technology (NIST), "Guide to Integrating Forensic Techniques into Incident Response," *NIST Special Publication 800-86*, 2008.
[5] Peraturan Kepala Kepolisian Negara Republik Indonesia No. 10 Tahun 2010, *Tata Cara Penanganan dan Penyidikan Tindak Pidana Teknologi Informasi*.
[6] R. Z. Alamsyah, "Keterangan Ahli Digital Forensik dalam Sidang Kasus Penipuan Investasi *Binary Option*," (Kesaksian di Pengadilan Negeri, dikutip dari sumber berita).
[7] A. P. J. R. D. Hartono dan N. M. K. Ciptaningsih, "Analisis Bukti Digital dalam Kasus Tindak Pidana ITE menggunakan Metode ND-DFRM," *Jurnal Komputasi*, vol. 18, no. 1, pp. 25-34, 2021.
[8] Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). SAGE Publications. *(Digunakan sebagai referensi untuk pendekatan Kualitatif-Deskriptif berbasis Studi Kasus)*
[9] Sammes, A., & Jenkinson, B. (2007). *Forensic Computing: A Practitioner's Guide* (2nd ed.). Springer.
[10] Rachmawati, N., & Santosa, P. I. (Tahun Publikasi). Analisis Modus Operandi Penipuan Berbasis Investasi Online (Studi Kasus Binary Option). *Jurnal Keamanan Siber dan Forensik Digital, Vol (No), Hal*. (Contoh referensi jurnal terkait modus).
[11] Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (Digunakan sebagai dasar hukum ITE).
[12] Al-Diwani, A., & Al-Qutayri, M. (2019). Forensic Analysis of Social Media and Instant Messaging Applications. *International Journal of Computer Science and Network Security, 19*(5), 180-188.
[13] Mohammad, M. S., & Al-Zoubi, A. (2018). Digital Forensic Analysis of Financial Applications on Android Devices. *Journal of Digital Forensics, Security and Law, 13*(3), 5-20.
[14] Choo, K. K. R., & Smith, R. G. (2008). Criminal Exploitation of the Internet in the Twenty-First Century. *Journal of Computer-Mediated Communication, 14*(1), 1–28.
[15] Grabosky, P. N. (2001). Virtual criminality: Exploiting the internet for illicit gain. *Information & Communications Technology Law, 10*(3), 263–274.
[16] Karam, G. (2020). *Binary Options Fraud: Detecting and Disrupting the Scheme*. Wiley.