Analisis Forensik Serangan Email Phishing Menggunakan Metode Analisis Dinamis Pada Transaksi Fiverr

Rifky Lana Rahardian[1], Anggun Nugroho[2], I Wayan Raka Putra Yana[3]
Institut Teknologi dan Bisnis (ITB) STIKOM BALI
e-mail: [1]rifky@stikom-bali.ac.id, [2]anggun@stikom-bali.ac.id, [3]rakaputray20@gmail.com

Diajukan: 12 Desember 2025; Direvisi: 12 April 2026; Diterima: 09 Mei 2026

Abstrak

Fiverr memfasilitasi komunikasi secara real-time terhadap penyedia jasa dengan klien, namun kemudahan tersebut menimbulkan ancaman kejahatan siber. Ancaman utama yang dihadapi adalah email phishing yang menyerupai pesan transaksi terhadap jasa yang ditawarkan. Penelitian ini melakukan investigasi terhadap email phishing tersebut menggunakan metode Analisis Dinamis berdasarkan pedoman NIST SP 800-86. Hasil analisis menunjukkan bahwa tautan pada email mengarahkan korban ke halaman web tiruan berisi detail produk dan form pembayaran. Melalui Analisis Dinamis, investigasi ini berhasil mendapatkan artefak digital berupa antarmuka halaman phishing, struktur komunikasi jaringan, dan source code situs phishing. Temuan artefak ini membuktikan penggunaan metode Analisis Dinamis dapat digunakan untuk mengidentifikasi aktivitas anomali dan mengamankan bukti digital pada email phishing.

Kata kunci: *Fiverr, Email Phishing, NIST SP 800-86, Dynamic Analysis, Forensik Digital.*

Abstract

Fiverr facilitates real-time communication between service providers and clients. However this convenience poses a cybercrime threat. The main threat faced is phishing emails that resemble transaction messages for the offered services. This research conducts an investigation into the phishing email using the Dynamic Analysis method based on the NIST SP 800-86 guidelines. The analysis results show that the link in the email directs the victim to a fake web page containing product details and a payment form. Through Dynamic Analysis, this investigation successfully obtained digital artifacts in the form of the phishing page interface, network communication structure, and the source code of the phishing site. The discovery of these artifacts proves that the use of the Dynamic Analysis method can be used to identify anomalous activities and secure digital evidence in phishing emails.

Keywords*: Fiverr, Email Phishing, NIST SP 800-86, Dynamic Analysis, Digital Forensics.*

1. Pendahuluan

Fiverr adalah *platform* penyedia jasa yang menjadi penghubung antara penyedia jasa dengan klien di seluruh dunia [1]. *Platform* ini menjual berbagai jasa seperti pembuatan website, desain grafis, pemeliharaan perangkat lunak dan sebagainya. Fiverr memiliki fitur kirim pesan secara *real-time* yang memudahkan komunikasi antara klien dengan penjual [2]. Dengan adanya Fiverr dapat memudahkan penjual jasa dalam menjual jasanya dan memudahkan klien untuk menemukan penyedia jasa sesuai kriteria yang dibutuhkan. Kemudahan yang diberikan oleh Fiverr memunculkan risiko keamanan pada transaksi yang terjadi bagi penyedia jasa yang berpotensi menjadi target kejahatan siber. Salah satu bentuk kejahatannya adalah *phishing* yang menyerupai email resmi dari Fiverr yang dapat mengelabuhi korban untuk mengklik tautan yang berbahaya[3]. Bentuk serangan ini sangat merugikan penyedia jasa maupun klien karena berpotensi menimbulkan kebocoran data serta kerugian finansial akibat transaksi palsu atau pencurian data [4]. Serangan *phishing* yang umum dilakukan adalah email *phishing,* dirancang sedemikian rupa sehingga tampak berasal dari perusahaan atau organisasi yang sebenarnya [5]. Beberapa organisasi telah mencatat laporan phishing yang terjadi di Indonesia atau luar negeri yaitu, Indonesia Anti-Phishing Data Exchange (IDADX) mencatat pada periode *Ocotber - December* tahun 2023, terjadi 8.161 kasus *phishing[6]*, selanjutnya dari Anti-Phishing Working Group (APWG) mencatat pada periode *Ocotber – December* tahun 2024 jumlah laporan serangan *phishing* setiap bulannya yang terjadi di Amerika Serikat

mencapai 989.123 serangan[7] dan laporan dari BSSN pada tahun 2023 juga mencatat adanya sebanyak 6 juta percobaan serangan *phishing* terhadap pengguna internet di Indonesia[8].

Penelitian dengan kaitan sejenis pernah dilakukan oleh [9] dengan judul Analisa Malware Menggunakan Metode *Dynamic Analysis* Pada Jaringan Universitas Sam Ratulangi. Penelitian ini melakukan analisis terhadap perilaku malware yang dilakukan didalam sistem terisolasi menggunakan metode *dynamic analysis.* Hasilnya menunjukkan terjadinya aktivitas yang mencurigakan seperti menjalankan *file* wscript.exe, mengakses dan mengubah registry sistem, serta menduplikasi dirinya sendiri. Penelitian in imembuktikan bahwa metode *dynamic analysis* efektif untuk mendeteksi aktivitasa malware yang tidak dapat dilakukan oleh analisis statis. Penelitian dilakukan oleh [10] dengan judul Analisis Forensik *Digital* Pada Kasus *Cyberbullying* dengan Metode National Institute of Standard and Technology SP 800-86. Penelitian ini melakukan analisis forensik *digital* terhadap kasus *cyberbullying* dengan menggunakan metode NIST SP 800-86. Alat yang digunakan dalam melakukan analisis forensik adalah Autopsy yang digunakan untuk akuisisi, pemulihan, dan analisis bukti *digital* dan untuk melakukan validasi terhadap hasil temuan. Penelitian lainnya dilakukan oleh [11] dengan judul Malware *Behavior Analysis Using Static and Dynamic Analysis Approaches.*Penelitian ini melakukan integrasi penggunaan metode analisis statis dan dinamis untuk meningkatkan akurasi deteksi malware dengan menggunakan *dataset* 5000 sampel. Hasil dari penelitian menunjukkan 87% sampel malware menggunakan *code obfuscation* untuk menghindari deteksi, dan 95% menunjukkan aktivitas *runtime* mencurigakan.

Dengan adanya kasus email *phishing* yang terjadi, maka Penelitian ini mengusulkan pendekatan analisis dinamis (*dynamic analysis*) berbasis forensik *digital* untuk menginvestigasi serangan email *phishing* yang terjadi di *platform* Fiverr. Penggunaan analisis dinamis (*dynamic analysis*) tidak hanya menangkap kondisi sistem saat aktif, tetapi juga merekam perubahan pada aliran data dan respon jaringan secara real-time setelah tombol dalam email *phishing* di klik. Penelitian ini juga menggunakan fitur "Tampilkan Versi Asli" pada Gmail sebagai pengecekan dini, sehingga memberikan cara bagi pengguna umum agar aktif memeriksa keaslian email dam terhindar dari potensi serangan *phishing*. Penelitian ini bertujuan untuk melakukan analisis forensik menggunakan metode analisis dinamis untuk mengetahui apa yang sebenarnya terjadi saat tombol dalam email *phishing* diklik dan menggunakan NIST SP 800-86 sebagai pedoman forensik, serta berbagai *tools* yang tersedia di Kali Linux seperti Wireshark untuk menganalisis trafik jaringan, kombinasi proxychain dan tor *service* untuk mengakses situs *phishing*, dan VirtualBox untuk menjaga keamanan selama proses investigasi, serta penelitian ini diharapkan dapat memberi pemahaman yang lebih mendalam mengenai bagaimana serangan email *phishing* bekerja, serta bagaimana proses analisis forensik dapat digunakan untuk melakukan investigasi serangan tersebut.

2. Metode Penelitian

Penelitian ini menggunakan metode analisis dinamis (*dynamic analysis*) untuk mengamati secara langsung aktivitas yang terjadi saat melakukan interaksi dengan email *phishing*. Dalam proses investigasi menggunakan pedoman NIST SP 800-86 agar proses berjalan dengan sistematis, mulai dari pengumpulan data hingga pelaporan hasil.

Gambar 1. Tahapan Penelitian

Adapun lima tahapan dalam metode analisis dinamis yang dipadukan dengan pedoman NIST SP 800-86 yaitu, pertama, persiapan lingkungan pengujian dimana lingkungan virtual disiapkan menggunakan VirtualBox dengan sistem operasi Kali Linux dan melakukan konfigurasi terhadap jaringan menggunakan kombinasi ProxyChains dan Tor Service untuk tetap menjaga anonimitas selama proses investigasi [12]. Kedua, akuisisi data dilakukan dengan cara mengakses email *phishing* melalui fitur "Tampilkan Versi Asli" pada Gmail untuk mendapatkan informasi detail mengenai header dan *direct link.* Ketiga, pengujian

interaksi secara langsung dengan melakukan interaksi secara langsung yang dilakukan dengan cara mengklik tombol yang terdapat pada email *phishing* dalam kondisi sistem aktif untuk mendapatkan aliran data menggunakan Wireshark serta pemantauan terhadap *redirect link* atau potensi unduhan otomatis. Keempat, analisis data dilakuakn terhadap log yang didapat dari Wireshark, alamat *IP,* dan *URL* dari situs *phishing*. Kelima, pelaporan hasil dengan melakukan penyusunan laporan berdasarkan pedoman NIST SP 800-86 yang berisi dokumentasi bukti *digital*, kronologi kejadian, dan kesimpulan dari hasil investigasi.

Sepanjang proses penelitian, verifikasi data menjadi langkah yang wajib dilakukan guna menjaga integritas bukti *digital* atau memastikan bahwa bukti *digital* tidak mengalami kontaminasi atau perubahan [13]. Validasi dilakukan dengan cara menggunakan fungsi hash (SHA256) pada setiap bukti *digital* segera setelah bukti *digital* diakuisisi dan setiap kali bukti *digital* dipindahkan atau disalin. Nilai hash awal yang didapat akan dijadikan pembanding terhadap hasil nilai hash dari salinan yang dibuat untuk memastikan tidak adanya perubahan sedikitpun pada barang bukti *digital* [14]. Proses validasi dan verifikasi data diulang pada setiap proses, mulai dari akuisisi, pemindahan ke virtual box hingga sebelum analisis. Pengulangan proses validasi pada barang bukti *digital* dilakukan secara sistematis dan didokumentasikan dengan baik untuk memastikan konsistensi dan keadaan barang bukti *digital* selama proses investigasi. Melakukan dokumentasi juga merupakan sebagai bukti prosedural yang menunjukkan bahwa standar forensik berdasarkan pedoman yang digunakan telah dipatuhi sehingga meningkatkan kredibilitas hasil investigasi [15].

2.1. Alat Dan Sistem Operasi

Dalam proses investigasi yang dilakukan di penelitian ini menggunakan beberapa alat dan 1 sistem operasi untuk menunjang kebutuhan investigasi sebagai berikut:

Tabel 1. Alat Dan Sistem Operasi

No	Alat / Sistem Operasi	Keterangan
1	Kali Linux	Sistem operasi yang digunakan untuk analisis forensik.
2	VirtualBox	Perangkat lunak yang digunakan untuk menjalankan sistem operasi secara virtual dan terisolasi.
3	Wireshark	Perangkat lunak untuk menangkap dan analisis trafik pada jaringan.
4	Tor Service	Perangkat lunak untuk anonimitas saat melakukan analisis terhadap situs *phishing.*
5	ProxyChains	Perangkat lunak untuk mengarahkan lalu lintas jaringan menggunakan Tor secara anonim.
6	Gmail	Perangkat lunak untuk menganalisis struktur email menggunakan fitur “Tampilkan Versi Asli”.
7	Browser	Perangkat lunak untuk mengakses situs *phishing* secara langsung.

Proses investagi melibatkan beberapa alat pendukung dan 1 sistem operasi yang saling berkaitan untuk mencapai hasil yang maksimal dengan tetap mengutamakan anonimitas untuk keamanan dan lingkungan yang terisolasi agar tidak mempengaruhi sistem utama yang digunakan.

3. Hasil dan Pembahasan

Hasil dari analisis dan penggunaan metode analisis dinamis (*Dynamic Analysis*) menemukan koneksi aktif ke dua alamat IPv4 46.4.32.184 dan 135.181.63.118, sebuah halaman web yang menyerupai website fiverr, sebuah *link* yang terdapat pada tombol di struktur email dan *source code* dari halaman website. Semua barang bukti yang ditemukan telah di-hash. Proses pengujian dilakukan melalui Proxychain dan Tor untuk anonimitas menyebabkan hasil tangkapan .pcap tidak dapat memperlihatkan hostname / DNS.

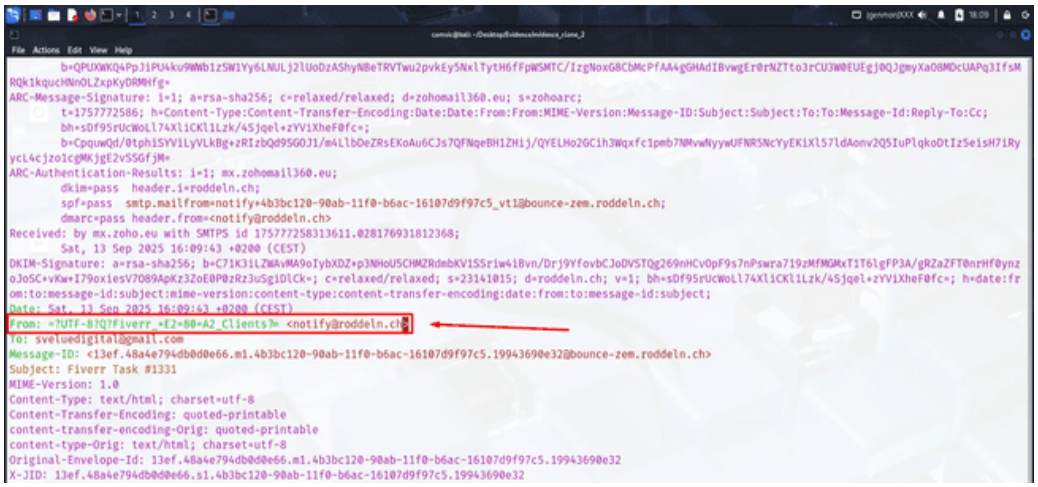
3.1. *Chain Of Custody*

1. Akuisisi Awal: Email phishing diunduh secara langsung dari platform Gmail dengan format .eml pada tanggal 15 September 2025. Hasil pengunduhan langsung dilakukan verifikasi hash menggunakan SHA256 sebagai acuan integritas barang bukti.
2. Penyimpanan *File*: *File* hasil unduhan ditempatkan pada *folder* khusus bernama “mail“ pada perangkat utama.

3. Perubahan Format: *File* .eml dikompres menjadi Evidence_Fiverr_01.zip dan dilakukan pengecekan terhadap nilai hash menggunakan SHA256 untuk memastikan tidak ada kontaminasi atau perubahan.
4. Pemindahan Barang Bukti Ke VM: Evidence_Fiverr_01.zip dipindahkan ke vm untuk dilakukan analisis lebih lanjut dan dilakukan pengecekan terhadap nilai hash menggunakan SHA256 untuk memastikan tidak ada kontaminasi atau perubahan. Pemindahan dilakukan pada 15 September 2025.
5. Proses Duplikasi: Dilakukan proses duplikasi sebanyak dua kali pada barang bukti Evidence_Fiverr_01.zip dan dilakukan pengecekan terhadap nilai hash menggunakan SHA256 untuk memastikan tidak ada kontaminasi atau perubahan. Duplikasi dilakukan untuk mencegah terjadinya kontaminasi terhadap barang bukti utama saat dilakukan proses analisis.
6. Ekstraksi Dan Analisis: Barang bukti hasil ekstraksi dilakukan pengecekan hash menggunakan SHA256 sebelum dilakukan analisis.
7. Proses Lanjutan: Setiap *output* analisis (*file* HTML, .tar, .pcap, dsb.) yang dihasilkan juga dilakukan pengecekan nilai hash menggunakan SHA256 untuk memastikan tidak ada kontaminasi atau perubahan serta didokumentasikan secara runtut termasuk waktu dan tempat.
8. Pencatatan: Semua hasil hash dicantumkan pada tabel Tabel 2 Daftar Barang Bukti Beserta Hasil Hash.

3.2. Temuan

1. Email & *Link*



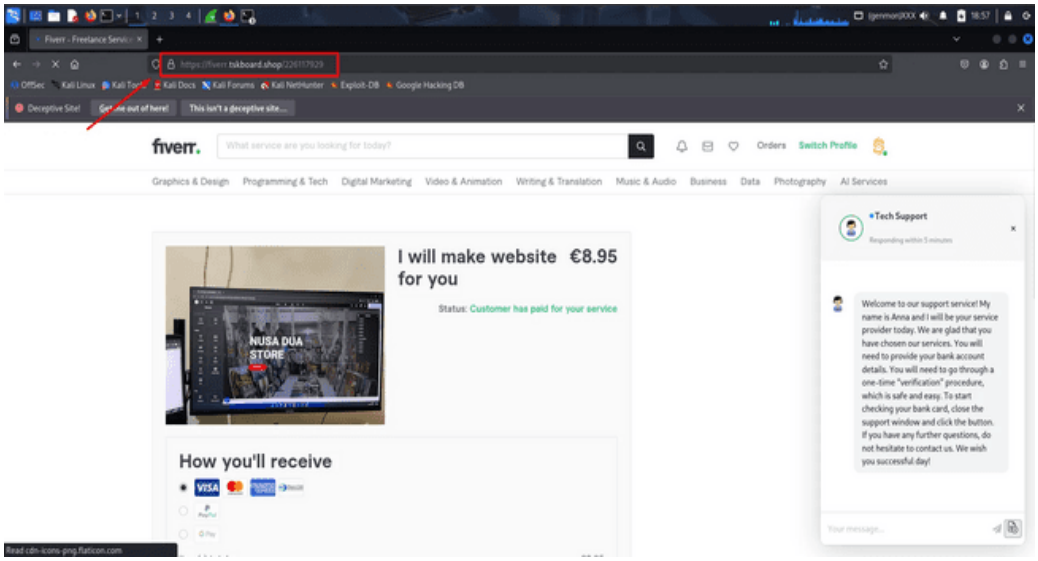
Gambar 2. Temuan Pengirim Email

Hasil analisis mendapati bagin *form* pada struktur email terdapat alamat pengirim yaitu notify@roddeln.ch.

Gambar 3. Temuan *Link* Di Tombol Email

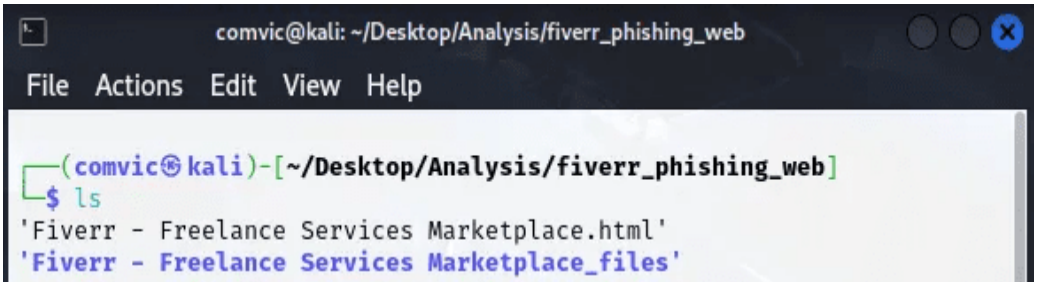
Hasil analisis mendapati bagin tombol pada struktur email terdapat link yang mengarah ke https://fiverr.roddeln.ch/urls/VVQWqMT9Q.

2. Halaman Website Dan Unduhan



Gambar 4. Tampilan Halaman Website Dari *Link* https://fiverr.roddeln.ch/urls/VVQWqMT9Q

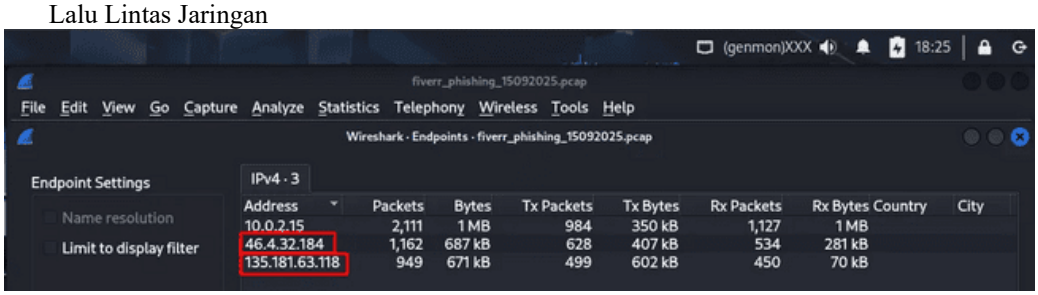
Hasil melakukan akses secara langsung menuju link Hasil analisis mendapati bagin tombol pada struktur email terdapat link yang mengarah ke https://fiverr.roddeln.ch/urls/VVQWqMT9Q mendapati tampilan sebuah halaman website.



Gambar 5. Hasil Unduhan Halaman Website

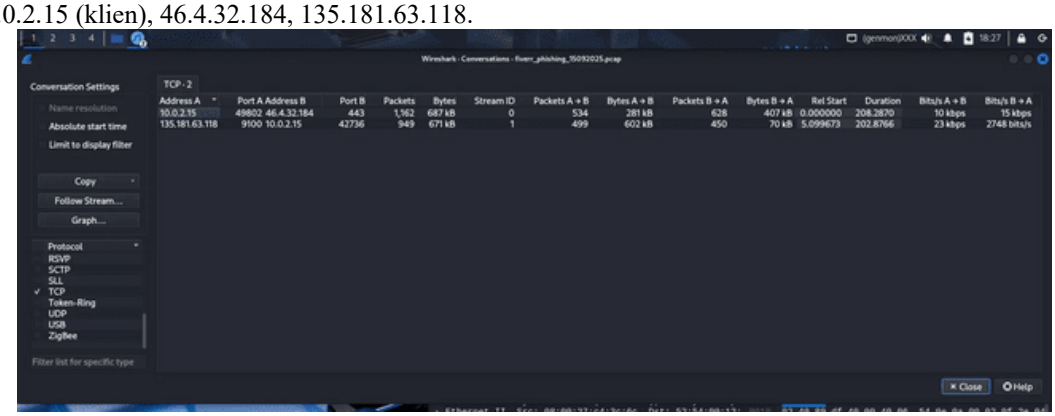
Hasil unduhan dari halaman website memberikan 1 *file* yang bernama Fiverr – Freelance Services Marketplace.html dan 1 *folder* dengan nama Fiverr – Freelance Services Marketplace_files dan didalam folder tersebut terdapat struktur halaman website, axios.min.js dan eye.js.

3. Lalu Lintas Jaringan



Gambar 6. Temuan IP Address

Hasil tangkapan wireshark terhadap lalu lintas jaringan adalah ditemukan 3 IP Address yaitu 10.0.2.15 (klien), 46.4.32.184, 135.181.63.118.



Gambar 7. Statistik *Conversations* TCP

Hasil tangkapan wireshark terhadap *conversations* TCP adalah ditemukan koneksi port 443 ke 46.4.32.184 dan koneksi port 9100 ke 135.181.63.118.

3.3. Daftar Barang Bukti Dan Nilai Hash (SHA-256)

Tabel 2. Daftar Barang Bukti Beserta Hasil Hash

No	Nama *File*	SHA-256	Waktu
1	Fiverr Task #1331.eml	e6afc597b80390fee23c4bba4440ff32a93d04eb6cdbc7e70e93adb89fbc57b	15-Sep-2025 17:12 WITA
2	Evidence_Fiverr_01.zip	830f66ea19b617f86b8b8d5b0572bcbe0b2639c1dc22d4505426eb5c3f1ac7af	15-Sep-2025 17:18 WITA
3	Fiverr – Freelance Services Marketplace.html	4a0a985ce60a19ab2f7b8c9eb11e152b6b8b803f367fae781659ab1358a5761d	15-Sep-2025 19:54 WITA
4	Fiverr_Service_Web.tar	531b6722d11b3977b6369ebf793d3d409be3dd82ea6da0b7502c9617b98c7ac2	15-Sep-2025 19:58 WITA
5	fiverr_phishing_15092025.pcap	1f409716fe298bffa7750e61ac51876c8ba22e24083986b55b62375122cd4684	15-Sep-2025 19:05 WITA.
6	fiverr_phishing.tar	8d036f6828a2eeafc7b727f92acc9d37f61eed2c019a444f4cdcf04704409540	15-Sep-2025 19:28 WITA

4. Kesimpulan

Berdasarkan hasil penelitian dan analisis yang telah dilakukan terhadap email *phishing* pada transaksi Fiverr, maka dapat disimpulkan penerapan metode analisis dinamis (*Dynamic Analysis*) berhasil dilakukan dengan mengikuti pedoman NIST SP 800-86, yaitu *collection, examination, analysis, reporting*. Dengan mengikuti proses ini, peneliti memperoleh, memeriksa dan melakukan analisis terhadap barang bukti *digital* secara sistematis tanpa mengubah bukti asli. Hasil penggunaan metode analisis dinamis (*Dynamic Analysis*) mendapati sebuah halaman website yang menyerupai halaman website Fiverr, selanjutnya tangkapan wireshark menunjukkan adanya komunikasi dan ditemukan koneksi ke dua alamat IP yaitu 46.4.32.184 dan 135.181.63.118 menggunakan port 443 dan 9100 dan hasil analisis lainnya terhadap Fiverr Task #1331.eml adalah ditemukan pengirim email yaitu notify@roddeln.ch dan sebuah *link* https://fiverr.roddeln. Ch/urls/ VVQWqMT9Q. Penggunaan Proxychains dan Tor selama pengujian untuk menjaga anonimitas peneliti menyebabkan hasil tangkapan .pcap tidak dapat memperlihatkan hostname / DNS. Berdasarkan hasil temuan dan batasan masalah, saran untuk penelitian selanjutnya adalah untuk menyertakan evaluasi efektivitas terhadap metode investigasi lainnya melalui pengukuran indikator tingkat akurasi deteksi anomali atau kecepatan ekstraksi bukti *digital*. Melalui evaluasi terhadap beberapa metode investigasi tersebut, penelitian selanjutnya diharapkan memberikan hasil analisis yang lebih kritis dan komperhensif dalam menangani insiden kejahatan siber.

Daftar Pustaka

[1] S. Al Farisi, Y. Retno, and W. Utami, “Sentiment Analysis Of Fiverr Application Reviews Using Tf-Idf Feature,” *Jurnal Ilmiah Sinus (Jis*, Vol. 23, No. 1, Pp. 1693–1173, 2025, Doi: 10.30646/Sinus.V23i1.883.

[2] J. Brunzel, "An Empirical Analysis Of Linguistic Styles In New Work Services: The Case Of Fiverr.Com," *European Management Review*, Vol. 21, No. 1, Pp. 83–102, Mar. 2024, Doi: 10.1111/Emre.12562.

[3] M. Ali, "Stout In Business And Management (Sbm) The Future Of Work: A Review Of Remote, Hybrid, And Gig Employment Models Corresponding Author," 2026, Doi: 10.61424/J11xwe89.

[4] F. P. E. Putra, U. Ubaidi, A. Zulfikri, G. Arifin, And R. M. Ilhamsyah, "Analysis Of Phishing Attack Trends, Impacts And Prevention Methods: Literature Study," *Brilliance: Research Of Artificial Intelligence*, Vol. 4, No. 1, Pp. 413–421, Aug. 2024, Doi: 10.47709/Brilliance.V4i1.4357.

[5] Y. H. Lokapala, F. J. Nurfauzi, And Y. Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia," *Indonesian Journal Of Criminal Law And Criminology (Ijclc)*, Vol. 5, No. 1, Jun. 2024, Doi: 10.18196/Ijclc.V5i1.19853.

[6] A. Raihan, M. Fadhli, And L. Lindawati, "Implementation Of Deep Learning For Detecting Phishing Attacks On Websites With Combination Of Cnn And Lstm," *Jurnal Teknik Informatika (Jutif)*, Vol. 5, No. 5, Pp. 1451–1459, Oct. 2024, Doi: 10.52436/1.Jutif.2024.5.5.2446.

[7] R. Yuhand Pramudita, B. Darma Setiawan, And M. Data, "Kinerja Deteksi Tautan Website Phishing Menggunakan Isolation Forest," 2025. [Online]. Available: Http://J-Ptiik.Ub.Ac.Id

[8] A. Rumbruren And Y. Watofa, "Analysis Of The Responsibilities Of The Organizer Of The Electronic System In Case Of Data Breach," 2025. Doi: 10.56301/Awl.V7i2.1549.

[9] Virgiawan A. Manoppo, Arie S. M. Lumenta, And Stanley D. S. Karouw, "Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi," *Jurnal Teknik Elektro Dan Komputer*, Dec. 2020, Doi: 10.35793/Jtek.V9i3.29567.

[10] R. N. Dasmen, M. Reihan Pratama, H. Yasir, And A. Budiman, "Analisis Forensik Digital Pada Kasus Cyberbullying Dengan Metode National Institute Of Standard And Technology Sp 800-86," Mar. 2024. Doi: 10.33884/Jif.V12i01.8344.

[11] K. Khalda And D. K. Wibowo, "Malware Behavior Analysis Using Static And Dynamic Analysis Approaches," *Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi*, Vol. 4, No. 1, Pp. 1–8, Jan. 2025, Doi: 10.20885/Snati.V4.I1.1.

[12] C. Mirkute, S. Gaikwad, H. Virkar, M. S. C. Science, And B. K. Birla, "Enhancing Anonymity During Web Browsing With Tor Network," *Www.Irjmets.Com @International Research Journal Of Modernization In Engineering*, 1835, Doi: 10.56726/Irjmets63817.

[13] J. S. G. Sinaga, Nehemia Sitorus, And Steven Lukas Samosir, "Analisis Kinerja Algoritma Hash Pada Keamanan Data: Perbandingan Antara Sha-256, Sha-3, Dan Blake2," *Jurnal Quancom: Quantum Computer Jurnal*, Vol. 2, No. 2, Pp. 9–16, Dec. 2024, Doi: 10.62375/Jqc.V2i2.432.

[14] A. I. Putra, R. Umar, And A. Fadlil, "Penerapan Metode Localization Tampering Dan Hashing Untuk Deteksi Rekayasa Video Digital," *Jurnal Resti*, Vol. 5, No. 2, Pp. 400–406, Apr. 2021, Doi: 10.29207/Resti.V5i2.3015.

[15] Mohammad Rifqi, Setia Juli Irzal Ismail, And Mochammad Fahru Rizal, "Analisis Forensik Untuk Penanganan Cyber Crime Pada Aplikasi Whatsapp Menggunakan Metode National Institute Of Standard And Technology (Nist Sp 800-86)," Dec. 2023.