Forensik Digital E-Learning Menggunakan Footprinting-Open Source Intelligence (OSINT)

Hidayat Muhammad Nur[1], Saifudin[2], Nuzul Imam Fadlilah[3], Sunanto[4]

[1,]Universitas Bina Sarana Informatika PSDKU Banyumas
Jl. Prof. DR. HR. Boenyamin No.106, Pabuaran, Kec. Purwokerto Utara, Kab. Banyumas
e-mail: [1]hidayat.hmm@bsi.ac.id , [2]saifudin@bsi.ac.id, [3]nuzul.nfh@bsi.ac.id, [4]sunanto.sun@bsi.ac.id

Artikel Info : Diterima : 28-05-2026 | Direvisi : 09-07-2026 | Disetujui : 11-07-2026

Abstrak - Keunggulan Ilmu Pengetahuan dan Teknologi memiliki ancaman keamanan sistem yang dapat munculkan kejahatan siber (*cybercrime*) menggunakan jaringan komputer. Penyalahgunaan kejahatan komputer mencakup, *SQL Injection, Cross Site Scripting* dan peretasan situs. Untuk itulah memetakan jaringan komunikasi pada sistem informasi berbasis web perlu dilakukan simulasi atau mitigasi pada sebuah sistem atau forensik digital. Proses forensik digital ini mengumpulkan informasi dari situs web (*footprinting*) dan jaringan komputer menggunakan metode dan sistem operasi *Open-Source,* adapun pengumpulan datanya menggunakan metode NIJ. Metode ini untuk mendapatkan barang bukti digital yang divisualisasikan ke bentuk *network mapping*. Hasil dari penelitian ini adalah rekomendasi untuk membantu administrator jaringan dalam mengambil keputusan berikut strategi keamanan sistem dan jaringan komputer melalui penguraian suatu kasus kejahatan siber yang berhasil terdeteksi.

Kata Kunci : Digital Forensik, E-learning, Maltego Open Source

Abstracts *- The advancement of science and technology poses a security threat to systems that can lead to cybercrime using computer networks. Computer crime abuse includes SQL Injection, Cross-Site Scripting, and website hacking. Therefore, mapping communication networks in web-based information systems requires simulation or mitigation in a system or digital forensics. This digital forensics process collects information from websites (footprinting) and computer networks using Open-Source methods and operating systems, while data collection uses the NIJ method. This method is used to obtain digital evidence that is visualized in the form of network mapping. The results of this study are recommendations to assist network administrators in making decisions and computer system and network security strategies through the analysis of a successfully detected cybercrime case.*

Keywords : Forensic Digital, E-learning, Maltego Open Source

PENDAHULUAN

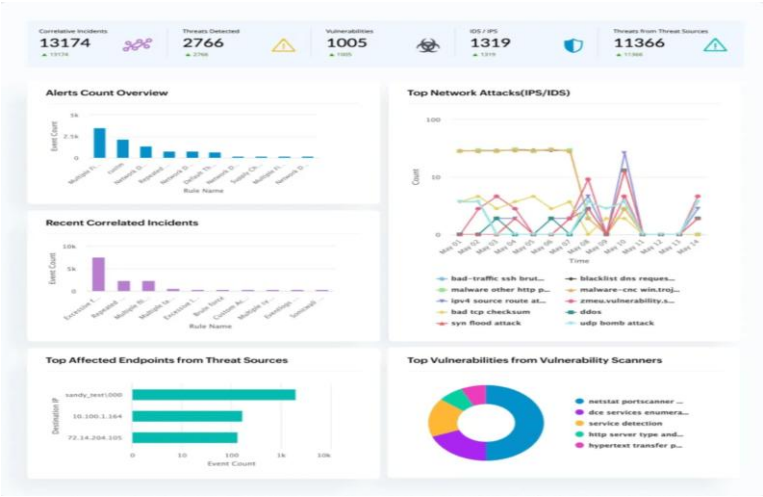
Ketika pemanfaatan teknologi yang “tanpa batas” tidak lagi hanya mengubah gaya hidup, tetapi telah menyebabkan disrupsi fundamental dalam sendi-sendi sosial, ekonomi, dan budaya global. Transformasi digital yang awalnya menjanjikan efisiensi dan konektivitas, kini menghadapi ujian terberatnya yaitu ketidakamanan eksistensial.

Data dari awal tahun 2026 menunjukkan bahwa lanskap siber telah berubah drastis. Jika dulu penipuan online memanfaatkan kelengahan korban via pendekatan sosial (*social engineering)* seperti mencatut nama kerabat, kini ancaman telah berevolusi menjadi sistem otonom [1]. Laporan terbaru memperingatkan bahwa kita telah memasuki era “industrialisasi kejahatan siber,” di mana agen kecerdasan buatan (*AI*) mampu melakukan eksploitasi, negosiasi tebusan, hingga pelacakan data secara mandiri tanpa campur tangan manusia [2]. Akibatnya, gelombang serangan DDoS besar-besaran yang menempatkan Indonesia sebagai salah satu episentrumnya bukan hanya masalah teknis, melainkan cerminan perang dingin baru yang berbasis data [3].

Perubahan sosial yang terjadi pun bersifat masif. Budaya gotong royong tergerus oleh budaya curiga akibat maraknya deepfake dan “gendam digital” yang mengacaukan fakta [4]. Di sisi ekonomi, rantai pasok global menjadi target empuk *ransomware* yang melumpuhkan perusahaan sekelas Stryker Corporation, memaksa kita merestrukturisasi ulang arti kata “resiko” dalam perdagangan[5]. Sementara itu, budaya konsumsi masyarakat

bergeser menuju praktik mistisisme siber (*cyber mysticism*), mencari makna dan perlindungan melalui algoritma aplikasi ramalan, sebuah komodifikasi spiritual sebagai pelarian dari realitas dunia maya[6].

Berdasarkan data tren serangan siber 2026 bahwa ancaman semakin kompleks, canggih, dan sulit dideteksi [7]. Penelitian ini bertujuan melakukan forensi digital untuk identifikasi, analisa dan *infrastructur network mapping* pada suatu sistem informasi berbasis website[8] (*e-learning*).



Gambar 1. Ilustrasi Data detikInet & Badan Siber Sandi Negara

Gambar 1 detikInet dikutip dari situs BSSN menguraikan langkah strategis menghadapi 2026 bahwa diperlukan strategi penerapan zero trust, meningkatkan literasi keamanan, monitor ancaman secara real-time, perkuat keamanan cloud dan data, tanggap insiden, kolaborasi dan berbagi informasi [9].

Tentulah menjadi hal serius dan perlu dilakukan antisipasi dengan tepat perihal *cybercrime* ini, yang perlu diterapkan salah satunya apabila dalam sistem informasi e-learning ditemukan kasus *hacking* sehingga memerlukan barang bukti secara digital untuk inilah digital forensik sangat diperlukan.

SAFEnet dan Goodstats.id mencatat jumlah kasus-kasus dalam penerapan dan pemanfaatan sistem informasi berbasis web, di indonesia pada tahun 2024 mulai kasus *deface* hingga peretasan dijelaskan bahwa terdapat 15 jenis serangan siber teratas ditunjukkan pada gambar 2 berikut dibawah ini [10]:

Gambar 2. Top 15 Cyber Attack Type 2024

Ditampilkan pada gambar 2 diatas, bahwa 12 dari 15 serangan siber tersebut terjadi pada aplikasi berbasis web. Ini pentingnya digital forensik dalam membuktikan kasus di dunia maya yang memiliki ciri khasnya sendiri oleh seorang forensika sistem informasi dimana bukti digital yang telah dihapus dapat dipulihkan kembali [11].

Bukti digital merupakan bagian dari ilmu forensik yang digunakan pada investigas materi dan data disuatu perkara.

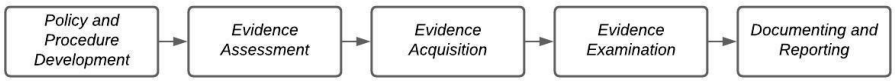
Disebutkan pada tahapan penelitian dan analisa mengadaptasi dan implementasi metode forensik software pembeku drive *shadow defender* dari *National Institute of Justice* (NIJ) untuk mendapatkan bukti digital dengan kondisi presentase keberhasilan 28,7% [12], investigasi forensik e-mail spoofing menggunakan header analysis pada pihak ketiga dengan mengubah identitas pengirim email [13], berikut juga penelitian perbandingan kinerja perangkat lunak file carving dengan metode NIST dimana melakukan performansi perangkat lunak Autopsy untuk mengembalikan data dengan melihat tingkat keberhasilan (akurasi) file carving tertinggi 100% pada file dokumen dan 90% pada file format .png dan .jpeg (2021) [14].

Forensik digital dalam penelitian ini menggunakan aplikasi Maltego Graph ver. 4.11.3, bahwa perangkat lunak ini adalah berbasis Open Source Intelligence (OSINT) yakni alat analisis tautat grafis untuk mengumpulkan dan menghubungkan informasi untuk tugas investigasi. Perangkat lunak maltego penulis kenal dari tahun 2022 dapat melakukan *footprinting* yaitu mengumpulkan memperbanyak informasi dari situs web[15]. Sistem operasi yang dipergunakan dalam menjalankan perangkat lunak Maltego Graph yaitu Kali Linux.

MATERIAL DAN METODE PENELITIAN

Pada langkah selanjutnya perlu diuraikan adalah meteri dan *tools* yang penulis pergunakan sebagai berikut :

1. Satu unit laptop dengan proc i5 bersistem operasi Kali Linux, adalah distribusi Linux yang dirancang untuk forensik digital dan pengujian penetrasi. Dikelola dan didanai oleh Offensive Security berbasis Linux debian. Kali linux mendapatkan popularitas di komunitas Orang Siber karena rangkaian alat yang komprehensif dirancang untuk analisis kerentanan (*vulnerability*) dan rekayasa bali (*reverse engineering*).
2. Perangkat lunak Maltego Graph ver. 4.11.3, untuk analisis kebutuhan footprinting dari situs web.
3. Koneksi Internet Indihome.
4. Situs website E-learning, dalam penelitian menggunakan situs web yang dirancang khusus untuk keperluan e-learning beralamatkan di https://elearning.xxx.ac.id.
5. Di penelitian ini dipergunakan metode analisa forensik dari National Institute of Justice (NIJ).
6. Pada dokumen NIJ, ada 5 tahapan dalam aktifitas digital forensic (lihat gambar 3) berikut.



Gambar 3. Langkah-langkah Forensik Digital

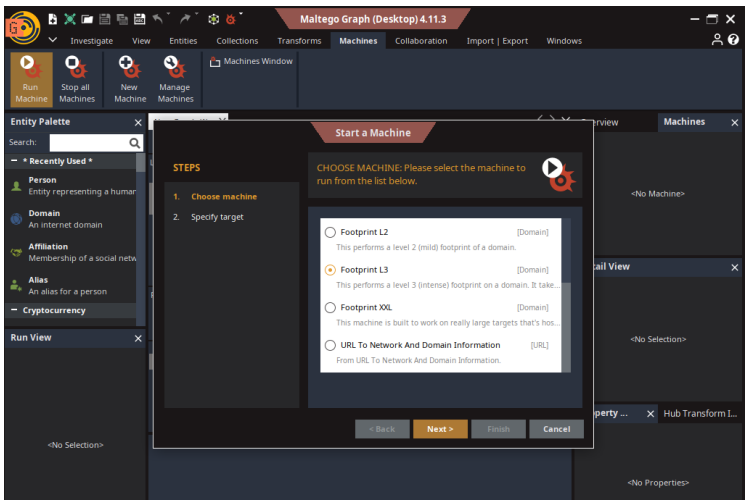
Penjelasan 5 tahapan forensik digital secara detail didasarkan pada langkah-langkah berikut :

1. Policy and Procedure Development
   Pengembangan kebijakan dan prosedur dalam forensik digital adalah kerangka kerja yang memandu para penyelidik dalam mengidentifikasi, mengumpulkan, menganalisis, dan melaporkan bukti digital secara legal dan sesuai standar. Kebijakan memastikan kepatuhan hukum, sementara prosedur memberikan panduan teknis untuk menjaga integritas bukti. Untuk objek forensik digital ini untuk keperluan keamanan tidak diberikan gambaran konkrit dan menyeluruh.
2. Evidence Assessment
   Evidence Assessment dalam forensik digital adalah proses evaluasi kritis terhadap bukti digital yang ditemukan untuk menentukan keaslian, integritas, dan relevansinya terhadap suatu kejadian atau tindak pidana. Tujuannya adalah memastikan bukti tersebut valid, dapat diterima.
3. Evidence Acquisition
   Evidence acquisition (akuisisi bukti) dalam digital forensik adalah proses mengidentifikasi, mengumpulkan, dan menyimpan bukti digital dari perangkat elektronik. Tujuannya adalah membuat salinan data sedikit demi sedikit yang akurat dan identik dengan aslinya, sehingga keutuhan dan keasliannya tetap terjaga.
4. Evidence Examination
   Pemeriksaan Bukti (Pemeriksaan Bukti) adalah tahap inti dalam forensik digital untuk mengekstraksi, memproses, dan menganalisis data mentah dari perangkat *machine*. Tujuannya adalah merekonstruksi kejadian serta menemukan fakta valid yang sah dapat diterima.
5. Documenting and Reporting
   Documenting (dokumentasi) dan *Reporting* (pelaporan) adalah tahap akhir yang penting dalam forensik digital untuk memastikan barang bukti. Dokumentasi pencatatan setiap langkah teknis yang dilakukan, sementara pelaporan merangkum temuan agar dapat dipahami oleh awam.

HASIL DAN PEMBAHASAN

Pada bagian ini, objek penelitian yang dipergunakan yaitu sebuah situs web e-learning untuk kepentingan uji fungsi forensik digital untuk menghimpun informasi dan memetakan koneksi jaringan dengan maksud melancarkan metode identifikasi, analisa dan pengumpulan data dalam mendapatkan barang bukti digital.

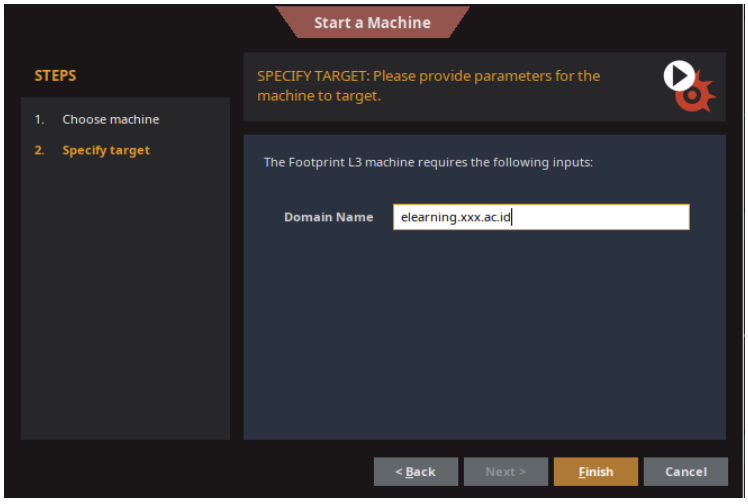
Urutan langkah ke-1 ialah buka perangkat lunak Maltego Graph, *New graph worksheet* dilanjutkan dengan pilih menu *machine,* klik *run machine*. Lihat tampilan gambar 4 berikut :



Gambar 4. Dashboard Maltego Graph 4.11.3

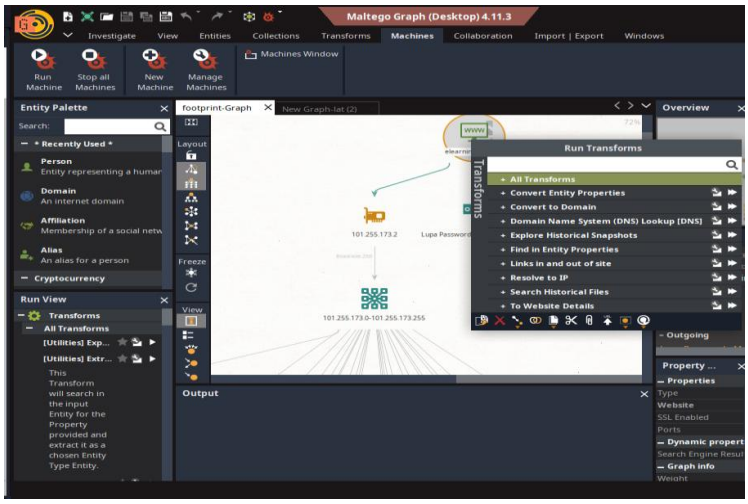
Pilihan menu machine yaitu Footprint L3 di Maltego berguna untuk melakukan pengumpulan informasi (pengintaian) tingkat lanjut (intens) pada suatu domain guna memperoleh data yang sangat lengkap dan ekstensif secara otomatis. Fitur ini bertindak sebagai skrip otomatis (Mesin) yang akan menggali target Anda lebih dalam daripada level di bawahnya (L1 dan L2). Berikut beberapa kegunaan spesifik dari Footprint L3: 1. Pemetaan Komprehensif: Menemukan subdomain, alamat IP, Nameserver, dan catatan DNS yang terhubung ke domain utama target. 2. Ekspansi Cepat: Menghemat waktu investigasi dalam menjalankan serangkaian Transformasi (metode pencarian) secara berantai untuk memperluas grafik investigasi. 3. Persiapan Pengujian Penetrasi: diandalkan pada tahap awal untuk memetakan sejauh mana celah atau permukaan serangan pada infrastruktur target

Urutan langkah ke-2 ialah inputkan nama situs web elearning pada kolom Domain Name, kemudian klik tombol Finish seperti di tampilan gambar 5 ini :



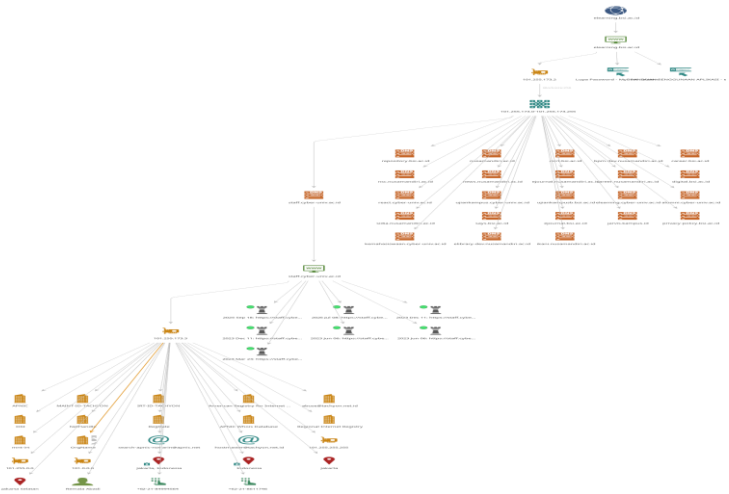
Gambar 5. Input Domain Name

Menjalankan profil footprint L3 ini akan mengeksekusi serangkaian transform secara otomatis untuk mencari subdomain, server DNS, hingga catatan kepemilikan. Ini yang disebut analisis visual, dimana maltego akan membuat grafik berbasis nod dan tautan (link). Pola koneksi, alamat IP yang terhubung dengan doman, serta relasi antar data.



Gambar 6. Proses Footprinting

Prosedur footprint meliputi memindai menemukan macam-macam informasi spesifik dengan situs web *e-learning* yang di uji fungsi forensik digital, antara lain : IP Address, Name Server, Domain, Koneksi Jaringan. Selanjutnya juga detail *network mapping* di tampilkan pada gambar 7 berikut :



Gambar 7. *Footprinting Result*

Penjelasan hasil footprinting pada gambar 7 diatas ialah *koneksi network mapping* dan informasi detail dari proses forensik digital pada situs e-learning atau target. Kemudian Maltego menampilkan sesuai dengan pemintaan, dengan detail :

1. 1 *NS Records* pada situs e-learning target. NS merupakan singkatan dari nameserver yaitu suatu database atau server dan didalamnya terdapat domain name IP Address. Mempunyai artian bahwa NS record yang terlihat sebagai titik awal bagi peretas untuk memetakan infrastruktur target dan merencanakan serangan. Pelaku siber menggunakannya untuk menemukan server yang paling rentan, membajak subdomain, atau melakukan serangan manipulasi lalu lintas.
2. *Block Size*. Ukuran rentang alamat IP besar berisi 256 ruang IP. Mempunyai pengertian sebagai berikut:
   a. Pada situs target kejahatan siber dapat menjadi sumber kerentanan serius, terutama terkait dengan kelemahan algoritma kriptografi lama seperti 3DES atau Blowfish.
   b. Sistem keamanan memecah data menjadi potongan-potongan tetap yang disebut blok.
   c. Ukuran blok terlalu kecil, potongan data yang dienkripsi kemungkinan besar akan memiliki hasil sama (*collision*) apabila dienkripsi dengan kunci yang sama.
   d. Penyerang dapat menggunakan pola hasil enkripsi yang berulang untuk menebak dan mencuri sebagian data asli.

3. Memiliki relevansi dengan 24 domain, keterkaitan banyak domain pada situs target menjadi sumber kerentanan siber (*attack surface*), mempersulit pemantauan, menciptakan titik lemah. Dengan detail penjelasan antara lain :
   a. Pembajakan sub-domain, sud-domain yang tidak lagi digunakan dapat diklaim oleh peretas untuk menyebarkan *phishing* atau *malware*.
   b. Keamanan yang terfragmentasi, domain yang dikelola secara terpisah seringkali memiliki standar keamanan (SSL, kata sandi, perlindungan DNS) yang tidak seragam.
   c. Rantai kerentanan, Peretas mengekploitasi domain sekunder yang lemah sebagai pintu masuk untuk melakukan *lateral movement* (gerakan lateral) ke domain utama atau pusat data.
   d. Kesulitan otentikasi. Banyaknya domain menyulitkan penerapan perlindungan email seperti SPF, DKIM, dan DMARC sercara menyeluruh, sehingga memudahkan penipuan identitas.

4. Integrasi Asia Pacific Network Information Center (APNIC). Pengelola IP dan AS di kawasan Asia Pasific. Penjelasan ada 2 seperti berikut :
   a. Informasi mengenai pengelola pada situs dapat menjadi celah kerentanan karena memudahkan penjahat siber memetakan infrastruktur, merancang serangan tertarget (seperti DDoS), hingga melakukan rekayasa social atau peniruan identitas.
   b. Data kepemilikan biasanya bersifat public dan mudah diakses melalui basis data pencarian.

5. Integrasi American Registry for Internet Numbers (ARIN). Regional Internet Registry (RIR), pengelola alokasi IP dan nomor sistem otonom untuk wilayah Amerika Utara dan Sebagian Karibia.
   a. Alternatif menggunakan informasi pengelola RIR atau pendaftar domain resmi dapat menjadi sumber kerentanan siber jika informasi kontak administratif atau data WHOIS terlihat public, dikarenakan penjahat siber dapat mengekploitasi data untuk melakukan *social engineering*, *doxxing*, atau pembajakan infrastruktur.
   b. Pembajakan domain, alamat email administratif yang terlihat dapat menjadi target serangan *phising* untuk mengambil alih kendali domain.
   c. Serangan tertarget dan rekayasa sosial.

6. 3 Internet Service Provider (ISP). Diketahuinya atau kebocoran informasi ISP ini membuka jenis kerentanan utama yaitu :
   a. Penyerang dapat mengetahui lokasi fisik server atau datacenter target
   b. Membantu peretas memahami infrastruktur jaringan untuk menyusup ke dalam sistem internal perusahaan.

7. 4 lokasi jaringan dan 2 nomor telepon. Adapun elemen ini dapat diekploitasi menjadi celah keamanannya ialah :
   a. Eksploitasi celah keamanan spesifik, lokasi jaringan mengungkap bahwa situs menggunakan server lama atau belum diperbaharui (*uppatched*), peretas akan mencari celah zero-day atau kerentanan spesifik untuk menyusup ke database.
   b. Pemalsuan geolokasi/IP geolocation, penyerang memprofilkan wilayah operasional jaringan untuk melakukan siber yang disesuaikan secara regional.
   c. Pembajakan kartu SIM (SIM Swapping), menggunakan data nomor telepon yang terekspos, untuk mengelabui operator telekomunikasi untuk menduplikasi kartu SIM target. Dampaknya, bisa membajak kode OTP (*One-Time Password*).
   d. Pelacakan jejak digital terbalik (*Reverse OSINT*), sebuah nomor telepon tunggal dapat dilacak balik untuk menemukan email pribadi, akun media sosial, hingga lokasi rumah. Ini mempermudah peretasan berbasis personal (*spear-phising*).

Sehingga dari informasi tercantum bisa didapatkan bukti digital yang riil berdasarkan dari hasil yang diperlihatkan.

KESIMPULAN

Berdasarkan hasil penelitian yang menggunakan perangkat lunak maltego untuk *digital forensic* situs elearning, beberapa kesimpulan dapat diambil sebagai berikut : perangkat lunak Maltego dapat digunakan untuk kepentingan forensik digital bertujuan mengumpulkan informasi dan menggambarkan jejaring koneksi yang terikat dengan menjalankan metode footprinting ditentukan sesuai kebutuhan. Adapun beberapa informasi yang dapat diperlihatkan Maltego diantaranya seperti: Nameserver, Domain, Block IP hosting, ISP berserta Pengelola,

Lokasi keberadaan dan Nomor telepon. walhasil penelitian ini dapat digunakan sebagai resolusi dalam mengurus sebuah peristiwa yang membutuhkan muatan bukti digital. Informasi yang didapatkan dapat divisualisasikan dalam bentuk yang mudah dipahami.

Adapun saran atau langkah mitigasi untuk melindungi situs, untuk mencegah informasi tersebut disalahgunakan, pemilik situs atau tim keamanan siber wajib melakukan langkah-langkah perlindungan antara lain sebagai berikut :

1. Mengunakan layanan proxy/proksiCDN (layanan seperti *cloudflare, incapsula* atau *Akamai* dapat menyembunyikan alamat IP asli server utama dari publik guna mencegah DDoS.
2. Menggunakan nomor telepon virtual/gateway. Jangan memajang nomor telepon seluler pribadi atau admin di situs web. Gunakan nomor hotline resmi, nomor virtual, atau sistem contact form terenkripsi.
3. Terapkan kebijakan WHOIS Privacy, sembunyikan data registrasi domain (nama, email, nomor telepon pemilik) agar tidak bisa di intip pencarian WHOIS publik.
4. Edukasi sumber daya manusia/karyawan. Berikan pelatihan kesadaran keamanan digital secara berkala agar staf tidak mudah terkecoh oleh manipulasi psikologis via telepon atau pesan teks.
5. Pemantauan *Threat Intelligence*, lakukan pengecekan rutin pada basis data intelijen ancaman untuk melihat apakah IP atau AS sedang ditandai sebagai target.
6. Audit jaringan. Rutin melakukan pengujian sistem untuk memastikan tidak ada celah keamanan pada konfigurasi server.
7. Footprint (jejak digital), membuka detail sistem dimana jejak digital dapat mengungkap informasi sensitive seperti versi software server, sistem operasi yang digunakan, dan port jaringan yang terbuka. Untuk itu lakukaan pembaruan berkala, batasi informasi publik, dan gunakan *security headers*.

REFERENSI

[1] I. W. Ardiyasa and A. T. Ndok, “Penetration Testing Keamanan Sistem Informasi Berbasis Web dengan Metode OSSTMM,” *Semin. Nas. Corisindo*, pp. 348–353, 2023, [Online]. Available: https://stmikpontianak.org/ojs/index.php/corisindo/article/view/197

[2] F. M, “Analisis Komprehensif terhadap Framework dan Alat Penetration Testing: Tren, Tantangan dan Peluang Title,” *IJEERE Indones. J. Electr. Eng. Renew. Energy*, vol. 4, no. 1, pp. 15–22, 2024, [Online]. Available: https://journal.irpi.or.id/index.php/ijeere

[3] C. Surya, E. Aribowo, A. Dahlan, Y. JlRingroad Selatan, and T. Yogyakarta, “Analysis Of SIPS.BAWASLU.GO.ID Web Security Level Using OWASP ZAP And Acunetix,” vol. 1, no. 1, pp. 1–8, 2020, [Online]. Available: http://journal.uad.ac.id/index.php/JIFO/index10.26555/jifo.v115i1.xxx

[4] S. Pomalingo, B. Sugiantoro, and Y. Prayudi, “Data Visualisasi Sebagai Pendukung Investigasi Media Sosial,” *Ilk. J. Ilm.*, vol. 11, no. 2, pp. 143–151, 2019, doi: 10.33096/ilkom.v11i2.443.143-151.

[5] H. Prasetyo, “Cyber Community, Cyber Cultures : Arsitektur Sosial Baru Masyarakat Modern,” *Ultim. J. Ilmu Komun.*, vol. 4, no. 1, pp. 29–38, 2012, doi: 10.31937/ultimacomm.v4i1.409.

[6] N. K. Illahi and R. Aditia, “Analisis Sosiologis Fenomena dan Realitas Pada Masyarakat Siber,” *J. Multidisiplin Dehasen*, vol. 1, no. 2, pp. 75–82, 2022, doi: 10.37676/mude.v1i2.2217.

[7] A. Bibliometrik, M. Risiko, and S. Siber, “Jurnal Inovasi Informatika (JII) Menggunakan Tableau dan Vosviewer,” vol. 08, no. April, pp. 9–22, 2026.

[8] R. Al, R. Bintang, and T. I. Widyawan, “Pengujian Kerentanan Website Menggunakan Metode Penetration Testing Dengan OWASP (Studi Kasus : Pemerintah Kabupaten Semarang) Website Vulnerability Testing Using the Penetration Testing Method with OWASP (Case Study : Semarang Regency Government),” vol. 8, no. 2, pp. 106–115, 2025.

[9] N. Nukman, Y. Prayudi, and F. Yudha, “Pengembangan Framework Digital Forensics Investigation (FDFI) Pada Sosial Media Dengan Metode System Development Life Cycle (SDLC),” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 3, pp. 1852–1860, 2022, doi: 10.35957/jatisi.v9i3.2151.

[10] A. Suhaemin and M. Muslih, “KARAKTERISTIK CYBERCRIME DI INDONESIA,” *EduLaw J. Islam. Law Yurisprudance*, vol. 5, no. 2, pp. 15–26, 2023.

[11] F. Medeline, E. Rusmiati, and R. H. Ramadhani, “Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial,” *PAMPAS J. Crim. Law*, vol. 3, no. 3, pp. 310–325, 2023, doi:

10.22437/pampas.v3i3.19691.

[12] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[13] M. A. Sutisna *et al.*, "ANALISISA FORENSIK PADA E-MAIL SPOOFING Abstraksi," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 38–43, 2018.

[14] R. Dwitama, A. R. Kadisi, R. Tri, S. Nabila, S. Informasi, and U. Semarang, "EVALUASI KINERJA FILE CARVING BERBASIS NIST PADA MEDIA FLASHDISK MENGGUNAKAN AUTOPSY , RECUVA , DAN," vol. 10, no. 3, 2026.

[15] Bunga Islamiya Putri, "ANALISIS DIGITAL FORENSIK PADA DIGITAL FOOTPRINT UNTUK IDENTIFIKASI PELAKU CYBERCRIME DENGAN FRAMEWORK FDFI." JuSTISe: Journal Data Science, Technology, Informatics and Security, 2023. [Online]. Available: https://e-journal.ukri.ac.id/index.php/justise/article/view/3272