Topik: Rekayasa Komputer

Implementasi Teknik Komputer Forensik dalam Penelusuruan Identitas, Keaslian dan *Malware* dari Email Masuk".

Muhammad Dimas Putra,[a] Rahmat Novrianda Dasmen [a]

[a] *Teknik Komputer, Vokasi, Universitas Bina Darma, Kota Palembang, Sumatera Selatan, Indonesia*
E-mail: muhammaddimas090704@gmail.com

ABSTRAK

Direktorat Inovasi dan Inkubator Bisnis (DIIB) Universitas Bina Darma merupakan unit strategis yang berperan penting dalam mendorong pengembangan inovasi serta pengelolaan hak kekayaan intelektual (HKI) di lingkungan Universitas Bina Darma, Studi ini menelusuri forensik digital dalam melacak identitas, keaslian, dan potensi malware di dalam *email* yang mencurigakan. Dengan menggunakan metode investigasi *digital forensic research workshop* (DFRWS), penelitian ini menggunakan *tools* seperti MXToolbox, Whois Lookup, Talos Intelligence, Sucuri SiteCheck, dan VirusTotal. Setiap alat berkontribusi dalam investigasi header email, reputasi domain, sumber IP, dan keberadaan malware dalam lampiran. Data dikumpulkan dari email mencurigakan yang diterima oleh DIIB Universitas Bina Darma dan dianalisis melalui metode forensik statis dan dinamis. Investigasi mengungkapkan bahwa email tertentu menggunakan domain pengirim umum, protokol otentikasi yang gagal seperti SPF dan DKIM, dan berisi lampiran dari sumber yang tidak terverifikasi. Meskipun lampiran tersebut dipindai dengan bersih, analisis kontekstual menunjukkan indikator phishing yang tinggi. Penelitian ini menyumbangkan metode terstruktur untuk mengidentifikasi, memverifikasi, dan mendeteksi ancaman di dalam *email*, memberikan panduan teknis yang bermanfaat bagi praktisi dan institusi keamanan siber. Temuan ini menekankan pentingnya deteksi ancaman dini melalui forensik *email* untuk mencegah penipuan digital dan meningkatkan ketahanan keamanan informasi.

Kata Kunci: Forensik, DIIB, HKI, DFRWS, TOOLS, EMAIL