ABSTRAK

Peningkatan aktivitas kejahatan siber yang menggunakan web server untuk tujuan ilegal, seperti penyebaran hoaks, hosting online gambling ilegal, dan distribusi malware, menunjukkan kebutuhan mendesak akan kerangka kerja forensik digital yang terstandarisasi. Metode saat ini, seperti pemblokiran IP sederhana, tidak mampu menjamin integritas dan keabsahan bukti digital. Penelitian ini mengusulkan framework penyitaan dan akuisisi yang dirancang untuk menangani web server, baik Virtual Private Server (VPS) maupun berbasis cloud, dengan fokus pada akuisisi langsung (live acquisition) untuk menjaga data volatil dan meminimalkan gangguan layanan. Framework ini mengatasi tantangan utama melalui penekanan pada otorisasi hukum, identifikasi jenis server, pemilihan alat forensik yang tepat, validasi integritas bukti menggunakan hashing, dokumentasi Chain of Custody yang teliti, serta penyimpanan data yang aman. Efektivitas framework diuji melalui simulasi penyitaan server VPS yang digunakan untuk menyebarkan hoaks dan akuisisi jarak jauh server cloud yang terlibat dalam aktivitas ilegal. Hasil simulasi menunjukkan keberhasilan dalam menjaga integritas bukti dan kepatuhan hukum, meskipun terdapat keterbatasan pada lingkungan cloud multi-tenant dan otomatisasi dokumentasi Chain of Custody. Validasi oleh Subject Matter Experts (SME) menunjukkan bahwa framework ini sudah kuat, namun masih perlu optimalisasi untuk konteks cloud-native. Studi ini merupakan langkah signifikan menuju standarisasi prosedur penyitaan web server, guna memastikan bukti digital tetap sah, utuh, dan dapat diterima di pengadilan.

Kata kunci: Forensik Digital, Penyitaan Web Server, Akuisisi Langsung, Integritas Bukti, Chain of Custody