ABSTRAK

IMPLEMENTASI DAN ANALISIS SISTEM FORENSIK DIGITAL PADA *LINUX VULNERABLE MACHINE* MENGGUNAKAN FRAMEWORK *FORENSICS* ZACHMAN

Oleh
Leonardo Taufan Sontani
1202160380
(Program Studi S1 Sistem Informasi)

Seiring dengan perkembangan teknologi, metode peretasan semakin banyak dan meningkat setiap tahunnya. Pada 2022, BSSN menemukan adanya 976 juta serangan yang masuk ke jaringan internet Indonesia. Berdasarkan Peraturan Pemerintah, pemilik sistem elektronik harus memiliki sistem untuk pencegahan dan penanggulangan peretasan sistemnya. Berdasarkan saran dari BSSN, Forensik Digital harus dilakukan pada 24 jam pertama setelah serangan ditemukan. Oleh karena itu, forensik digital membutuhkan strategi dan perangkat lunak yang tepat untuk mempercepat pemeriksaan kasus.

Penelitian ini menganalisis log sistem dari *Linux Vulnerable Machine* dalam kemampuannya untuk mencatat kejadian peretasan. Penelitian ini juga membandingkan kinerja tiga program forensik digital gratis atau memiliki versi *trial* (Autopsy, FTK Imager, OSForensics) untuk mencari barang bukti digital. Percobaan dilakukan dengan melakukan penyerangan pada *Linux Vulnerable Machine* menggunakan *walkthrough* yang kemudian dilakukan tindakan forensik berdasarkan *framework.*

Berdasarkan percobaan tersebut, didapat bahwa *access.log* merupakan log prioritas untuk dianalisis. *Access.log* mencatat banyak log yang menunjukkan kronologi saat server diserang, seperti alamat IP dan waktunya. Berdasarkan kemampuannya untuk melakukan *imaging,* analisis data, dan pencarian data terhapus, FTK Imager lebih unggul dalam tindakan forensik digital.

Kata kunci: forensik digital, *framework*, FORZA, Typhoon, *log*.