ABSTRAK

Salah satu kegiatan anti forensic untuk mengamankan data adalah dengan melakukan penghapusan data dari media penyimpanan, yang dapat membuat para penegak hukum kesulitan untuk mengumpulkan bukti-bukti digital. Pada praktik nya ada banyak metode yang dapat membuat penghapusan data tersebut benar-benar aman dan tidak mudah untuk dipulihkan dengan berbagai tools recovery, salah satunya adalah dengan wiping data. Metode penghapusan dengan teknik wiping data, dalam kegiatan anti forensic biasanya digunakan pada media penyimpanan yang menyimpan data ilegal yang berkaitan dengan bukti tindak kejahatan. Jika pada media penyimpanan ini berisi data tindak kejahatan maka pemilik data tersebut akan berusaha untuk melakukan menyembunyikan atau menghapus data tersebut, salah satunya dengan metode wiping data, selain data utama ada juga data lain yang akan terhapus dalam perangkat penyimpanan jika menggunakan metode wiping data, yang mencakup metadata dan tracedata. Dalam upaya membantu kegiatan forensic memahami tools wiping data, pada pengujian tugas akhir ini akan diambil enam tools atau aplikasi sampel yang telah dipilih sebelumnya yang dapat melakukan data wiping pada media penyimpanan, dengan tujuan untukmembandingkan hasil data wiping antara tools atau aplikasi tersebut lalu dianalisa kelebihan dan kekurangannya untuk keperluan sebagai data untuk kegiatan forensic. Metode yang diambil pada sampel tools atau aplikasi adalah metode-metode Zero Overwrite, Random DataOverwrite, U.S. DoD 5220.22-M (E), U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's Algorithm. Metode-metode ini dapat menghapus dan menimpa data sehingga data tidak dapat dibaca oleh orang yang tidak berwenang, sehingga dapat dipakai untuk mencegah pengungkapan kejahatan.

Kata Kunci: Anti Forensic, Wiping Data, Media Penyimpanan, Penghapusan