

Abstrak

Dalam kegiatan forensik digital, usaha untuk menjaga integritas atau keutuhan bukti digital menjadi perhatian yang penting. Salah satu usaha untuk menjaga integritas bukti digital adalah memastikan bahwa *secondary storage* yang digunakan untuk menyimpan hasil penggandaan bukti digital, dalam keadaan benar-benar kosong agar bukti digital tersebut tidak terkontaminasi. Cara untuk mengosongkan *secondary storage* dapat dilakukan melalui teknik penghapusan yang sesuai dengan kaidah forensik.

Pada penelitian ini dilakukan uji teknik penghapusan pada *secondary storage* secara manual (menggunakan teknik *shift delete* dan *format*) serta menggunakan teknik *wiping* dengan *file system* NTFS. Pada pengujian teknik penghapusan *wiping* menggunakan metode *one zero pass* dengan tools *Active Kill Disk*. Pengujian dilakukan melalui uji *recovery* data menggunakan perangkat lunak *Disk Drill Pro*. Hasil pengujian bertujuan untuk membandingkan tiga teknik penghapusan data yang tepat digunakan untuk mengosongkan *secondary storage* berdasarkan ada tidaknya data yang berhasil dipulihkan kembali. Setelah menganalisis hasil pengujian, penulis membuat visualisasi cara kerja teknik penghapusan dalam bentuk perancangan *story board* animasi yang berfungsi untuk menjelaskan perbandingan teknik penghapusan kepada orang-orang dengan latar belakang non-IT. Berdasarkan hasil penelitian, teknik penghapusan *shift delete* dan *format* tidak benar-benar mengosongkan *secondary storage*, sedangkan teknik penghapusan *wiping* dapat mengosongkan *secondary storage* yang sesuai dengan kaidah forensik digital.

Kata Kunci: *Forensik Digital, Secondary Storage, Wiping.*