

ABSTRAK

Dalam dunia forensik digital, integritas data merupakan bagian yang penting untuk diperhatikan. Pada proses analisis data, terdapat aktifitas mengkaitkan *file system* ke sistem berkas utama pada sistem operasi atau yang biasa dikenal dengan istilah *mounting*. *Mounting* merupakan tahapan mengaitkan sistem berkas ke direktori utama sistem operasi untuk dapat diakses. Salah satu prosesnya, sistem operasi linux akan melakukan pendeteksian terhadap media penyimpanan dan melakukan *mounting* untuk mengakses *file system*. Disisi lain, proses pengenalan dan *mounting* tidak menjamin integritas data pada media penyimpanan. Penelitian ini akan melakukan analisis dan visualisasi pengenalan perangkat dan uji empiris pengaruh *mounting* terhadap integritas data untuk kebutuhan digital forensik. Pada pengujian, dilakukan analisis proses pengenalan perangkat berdasarkan referensi yang valid dan uji empiris *mounting* dengan metode *read only* dan tanpa *read only* di sistem operasi linux. Hasil pengujian bertujuan untuk melakukan visualisasi pengenalan perangkat dan melakukan perbandingan teknik *mounting* dengan *read only* dan tanpa *read only* serta pengaruhnya terhadap integritas data. Berdasarkan penelitian, didapatkan rangkuman proses pengenalan perangkat dan hasil analisis dari kedua teknik *mounting* yaitu mampu menjaga integritas data. Teknik *mounting* tanpa *read only* ditemukan fenomena yaitu mengubah nilai *hash* partisi sedangkan *mounting* dengan *read only* tidak mengubah nilai *hash* partisi.

Kata Kunci: *mounting*, linux, sistem operasi, integritas data, forensik