

ABSTRAK

Kehilangan data pada SD Card sering terjadi akibat *human error* seperti penghapusan atau pemformatan. Meskipun banyak penelitian terdahulu mengevaluasi tool pemulihan data, sebagian besar hanya berfokus pada kuantitas file yang berhasil dipulihkan (*file carving rate*) dan menggunakan validasi *hash* MD5 yang rentan terhadap *collision*, sehingga mengabaikan tingginya *noise* dan kerusakan struktur *biner* file hasil pemulihan. Kesenjangan (*gap*) yang ditemukan adalah belum adanya evaluasi komprehensif yang mengintegrasikan validasi integritas mutlak (SHA-256), pengukuran kemiripan struktural untuk file rusak (*fuzzy hashing* TLSH), serta uji keterbacaan visual secara terotomatisasi. Penelitian ini menganalisis integritas file hasil pemulihan pada SD Card exFAT menggunakan pendekatan eksperimental komparatif berbasis kerangka kerja NIST SP 800-86 melalui skenario penghapusan biasa, *quick format*, dan *overwrite* dengan PhotoRec, Autopsy, dan DMDE. Hasil penelitian menunjukkan efektivitas tool sangat bergantung pada skenario kerusakan. DMDE paling optimal untuk penghapusan biasa dengan *F1-Score* 99,81%, sementara Autopsy unggul pada *quick format* dengan *F1-Score* 99,06%. Terkait tingkat keterbacaan visual (*Readability Rate*), seluruh tool menunjukkan ketahanan tinggi di atas 99%, di mana PhotoRec konsisten mencapai 100% tanpa ada file yang tidak dapat dibuka. Namun, analisis kerusakan struktural *biner* (TLSH) mengungkap fakta krusial: residu dari PhotoRec murni adalah *noise* dengan tingkat kemiripan sangat rendah (0%-9%), sedangkan residu dari DMDE pada seluruh skenario di atas 75%. Temuan ini membuktikan bahwa file yang gagal divalidasi dengan *hash* SHA-256 belum tentu hancur total secara visual maupun struktural, sehingga integrasi *dual hashing* ini memberikan parameter evaluasi kualitas pemulihan yang jauh lebih objektif dan menyeluruh.

Kata Kunci : Pemulihan Data, SD Card, SHA-256, Uji Keterbacaan, TLSH, Python, NIST SP 800-86.

ABSTRACT

SD card data loss frequently results from human errors such as accidental deletion or formatting. While previous studies have evaluated data recovery tools, most have focused primarily on the quantity of successfully recovered files (file carving rate) and relied on MD5 hash validation, which is susceptible to collisions thereby overlooking issues like high noise levels and binary structural corruption in the recovered files. A research gap exists regarding the lack of comprehensive evaluations that integrate absolute integrity validation (SHA-256), structural similarity measurements for corrupted files (TLSH fuzzy hashing), and automated visual readability testing. This study analyzes the integrity of files recovered from exFAT SD cards using a comparative experimental approach based on the NIST SP 800-86 framework, testing standard deletion, quick format, and overwrite scenarios with PhotoRec, Autopsy, and DMDE. The results demonstrate that tool effectiveness depends heavily on the data loss scenario. DMDE performed optimally for standard deletion (F1-Score: 99.81%), while Autopsy excelled in quick format scenarios (F1-Score: 99.06%). Regarding visual readability, all tools exhibited high resilience (exceeding 99%), with PhotoRec consistently achieving 100%, meaning no recovered files were unopenable. However, binary structural corruption analysis (TLSH) revealed a crucial insight: recovered fragments from PhotoRec consisted purely of noise with very low similarity (0%–9%), whereas fragments from DMDE maintained similarity levels above 75% across all scenarios. These findings demonstrate that files failing SHA-256 hash validation are not necessarily completely destroyed either visually or structurally indicating that integrating dual hashing provides a far more objective and comprehensive set of parameters for evaluating recovery quality.

Keyword: Data Recovery, SD Card, SHA-256, Readability Test, TLSH, Python, NIST SP 800-86.