ANALISIS PERBANDINGAN FILE CARVING DENGAN METODE NIST

Doddy Teguh Yuwono [1], Yunanri W [2]

[1)] Prodi Ilmu Komputer, Fakultas Teknik Universitas Muhammadiyah Palangka Raya
Jl. RTA. Milono Km. 1,5 Palangka Raya, Kalimantan Tengah, 73112

[2)] Departemen Teknik Informatika, Universitas Teknologi Sumbawa
Jl. Raya Olat Maras, Batu Alang, Moyo Hulu, Pernek, Moyohulu, Kabupaten Sumbawa, NTB. 84371
Email: doddy.zha09@gmail.com , yunanri.w@uts.ac.id.

ABSTRAK

Pemulihan data adalah bagian terpenting dari Digital Forensic. Bagi penyidik negara untuk menghasilkan bukti yang sah di pengadilan sangat penting dan wajib. Memori Flash, Hard Disk Drive (HDD) dan Solid State Drive (SDD) adalah beberapa Media Penyimpanan yang digunakan sebagai tempat untuk meletakkan semua jenis data dan informasi dalam berbagai format file digital. Karena bentuk digitalnya sehingga memungkinkan berbagai format file digital disembunyikan, dihapus, dan bahkan diformat di media penyimpanan, sedangkan semua data dan informasi harus ditemukan oleh penyelidik negara.

Prinsip dasar data atau informasi digital jika telah disalin pada Memori Flash, Hard Disk Drive (HDD) dan Solid State Drive (SDD) tidak akan pernah hilang secara permanen dan bahkan data atau informasi digital hilang karena dihapus, diformat dengan cepat atau sistem macet. Jadi, mengembalikan data sangat mungkin. Dalam penelitian ini, tes dilakukan menggunakan Foremost, FTK Imager, dan Scalpel, yang merupakan Alat OpenSource yang dapat digunakan pada sistem operasi Propietary dan OpenSource. Metode yang digunakan adalah Institut Teknologi Standar Nasional (NIST). NIST memiliki panduan kerja yang sangat baik tentang kebijakan dan standar untuk memastikan setiap Penguji mengikuti alur kerja yang sama, sehingga pekerjaan mereka didokumentasikan dan hasilnya dapat ditinjau dan dapat dipertahankan saat pelaporan sebelum dijadikan sebagai bukti yang valid. Hasil penelitian ini membuktikan bahwa Foremost, FTK Imager, dan Scalpel dapat mengembalikan data yang dihapus, disembunyikan, dan diformat.

Kata kunci : Digital Forensic, Examiner, Foremost, FTK Imager, Scalpel, NIST.

ABSTRAK

Data recovery is the most important part of Digital Forensic. For state investigators to produce valid evidence in court is very important and mandatory. Flash Memory, Hard Disk Drive (HDD) and Solid State Drive (SDD) are some of the Storage Media that are used as a place to put all types of data and information in various digital file formats. Because of its digital form so that it allows various digital file formats to be hidden, deleted and even formatted on the storage media, while all the data and information must be found by state investigators.

The basic principle of digital data or information if it has been copied on Flash Memory, Hard Disk Drive (HDD) and Solid State Drive (SDD) will never be permanently lost and even digital data or information is lost because it is deleted, formatted quickly or the system crashes. So returning data is very possible. In this study, the test was performed using Foremost, FTK Imager, and Scalpel, which are Opensource Tools that can be used on Propietary and Opensource operating systems. The method used is the National Institute of Standards Technology (NIST). NIST has an excellent work guide on policies and standards to ensure each Examiner follows the same workflow, so that their work is documented and the results can be reviewed and can be maintained when reporting before serving as valid evidence. The results of this study prove that Foremost, FTK Imager, and Scalpel can restore deleted, hidden and formatted data.

Keywords : Digital Forensic, Examiner, Foremost, FTK Imager, Scalpel, NIST

1. PENDAHULUAN

Kejahatan dunia maya adalah kegiatan yang menjadikan teknologi alat atau media untuk melakukan kejahatan, seperti peretasan jaringan, mencuri informasi, menghapus informasi, menyembunyikan informasi, dan menghancurkan informasi. Hasil kejahatan umumnya disembunyikan di media penyimpanan untuk digunakan dalam pencurian, pengintaian, penindasan dan penipuan. Media Penyimpanan adalah perangkat atau alat yang memiliki fungsi untuk menyimpan data atau program, di mana data atau program yang tersimpan masih dapat dibuka, dibaca, diedit, dihapus, disembunyikan, diformat menggunakan komputer atau laptop. Penjahat dunia maya dalam menutupi atau menghilangkan jejak mereka cenderung memilih untuk menghapus, menyembunyikan, dan memformat semua data yang dikumpulkan dalam kejahatan yang dilakukan (Rana et al., 2017)

Dalam proses menghapus / menghapus file sebenarnya file tidak berarti data dihapus secara permanen dari media penyimpanan. Tapi itu hanya memberitahu komputer bahwa ruang yang ditempati oleh data tersedia untuk ditimpa / diisi / ditimpa oleh data lain. Sehingga file dapat dikembalikan dengan mudah ke bentuk aslinya, asalkan tidak ada file lain yang telah ditimpa. Kapasitas media penyimpanan yang terus tumbuh memiliki kapasitas penyimpanan yang lebih besar juga. Ini memungkinkan pengguna untuk menggunakan semua ruang penyimpanan yang tersedia, sehingga proses menimpa cenderung hanya dilakukan dalam proses pemformatan (Putra, Fadlil dan Riadi, 2017).

Ini menyebabkan file dihapus, meninggalkan fragmen file yang masih aman dan disimpan bahkan jika mereka tidak utuh. Jika disamakan dengan file terkompresi yang ada di media penyimpanan, file yang dikompresi saat dihapus akan tetap dalam bentuknya. Pencarian di media penyimpanan tidak akan memberikan hasil. Meskipun Anda telah memasukkan kata kunci yang terkandung dalam file yang dihapus. File yang mengalami sedikit fragmentasi (terfragmentasi) cenderung lebih mudah untuk dipulihkan / pulih (Yuwono, Fadlil dan Sunardi, 2019). Penempatan sistem file yang baik memberikan lebih banyak manfaat, termasuk informasi yang dihapus atau dihapus dapat bertahan lebih lama dari yang diharapkan oleh penggunanya. (Yudhana, Riadi and Anshori, 2018)

Microsoft, yang merupakan produsen OS Windows memperkenalkan NTFS. NTFS adalah Sistem File standar yang digunakan untuk media penyimpanan pada Hard Disk dan SSD pada OS Windows. NTFS dipilih karena memiliki kecepatan proses transfer data yang baik dan tentu saja dukungan dari Microsoft. Meskipun media penyimpanan Hard Disk menggunakan standar Sistem File NTFS, media penyimpanan lain seperti Flash disk juga dapat mengimplementasikan NTFS. Penggunaan NTFS pada flash umumnya diperlukan saat membuat media yang dapat di-boot. Misalnya, untuk membuat paket instalasi OS (Riadi, Sunardi; dan Rauli, 2018)

Hasil analisis struktur data, isi folder dan komposisi aplikasi adalah jawaban dalam mengungkap kasus kejahatan digital sesuai dengan skenario yang telah dibuat di bagian desain, kemudian dilakukan di bagian implementasi , serta dalam Analisis sehingga bukti digital termasuk pengumpulan data digital penting dapat disajikan dan dapat dilaporkan sebagai bukti digital (Riadi, Umar dan Nasrulloh, 2018).

Berdasarkan latar belakang masalah yang diuraikan, penelitian ini berfokus pada analisis File Carving yang merupakan proses mencari file dalam aliran data berdasarkan pengetahuan format file dalam Sistem File tertentu, daripada metadata menggunakan NIST (National Institute of Metode Standar Teknologi), sedangkan penelitian ini dilakukan menggunakan Foremost, FTK Imager, dan Scalpel, yang merupakan alat opensource yang dapat digunakan pada Sistem Operasi Proprietary dan opensource.

2. METODE PENELITIAN

Metode yang digunakan untuk menganalisis bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital adalah metode NIST. Transformasi pertama terjadi ketika data yang dikumpulkan diperiksa, kemudian mengekstraksi data dari media dan mengubahnya menjadi format yang dapat diproses oleh alat forensik. Kedua, data ditransformasikan menjadi informasi melalui analisis. Akhirnya, transformasi informasi menjadi analogi bukti dengan mentransfer pengetahuan menjadi tindakan menggunakan informasi yang dihasilkan oleh analisis dalam satu atau beberapa cara selama fase pelaporan. (Yuwono, Fadlil dan Sunardi, 2019).

Gambar 1. Metode NIST

Berdasarkan gambar 1 ini dapat dijelaskan tahap seluler Analisis Forensik sebagai berikut:

Collection adalah melabeli, mengidentifikasi, merekam, dan mengambil data dari sumber data yang relevan dengan prosedur yang sesuai agar tidak mengubah keaslian data dan untuk menjaga integritas data.

Pemeriksaan adalah pengolahan data yang dikumpulkan, pada tahap ini adalah bagaimana menggunakan kombinasi forensik dari berbagai skenario, baik otomatis dan manual, serta menilai dan merilis data sesuai dengan kebutuhan penelitian sambil menjaga integritas data.

Analisis adalah tahap memeriksa hasil menggunakan metode teknis yang dibenarkan sesuai dengan prosedur dan hukum.

Laporan adalah melaporkan hasil analisis yang meliputi persiapan, pengujian, penggambaran tindakan yang diambil, dan hasil yang diperoleh dari penelitian

3. HASIL DAN PEMBAHASAN

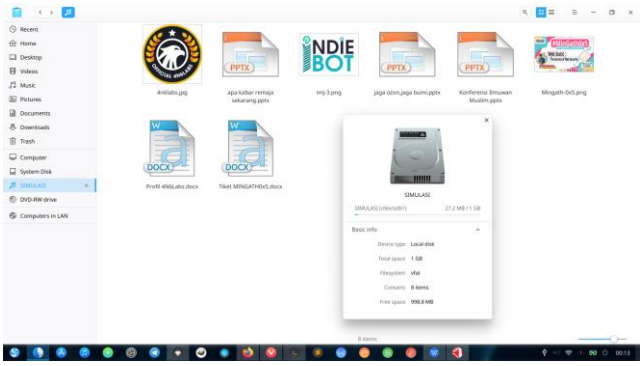
Dari penelitian yang dilakukan, menggunakan Foremost, FTK Imager, dan Scalpel diperoleh hasil dalam bentuk data yang telah dihapus atau diformat pada media penyimpanan. Berikut ini adalah informasi tabel 1 tentang OS, perangkat keras dan perangkat lunak yang diperlukan dalam penelitian ini.

Tabel 1. Alat dan Bahan

No	Bahan	Keterangan
1	Laptop	● Acer Aspire E14 ● Asus
2	OS	● Win-7 Home Premium ● Deepin
3	USB FlashDISK	Sandisk 1 Gb
4	FTK Imager	Forensics Opensource Tool
5	Foremost	Forensics Opensource Tool
6	Scalpel	Forensics Opensource Tool

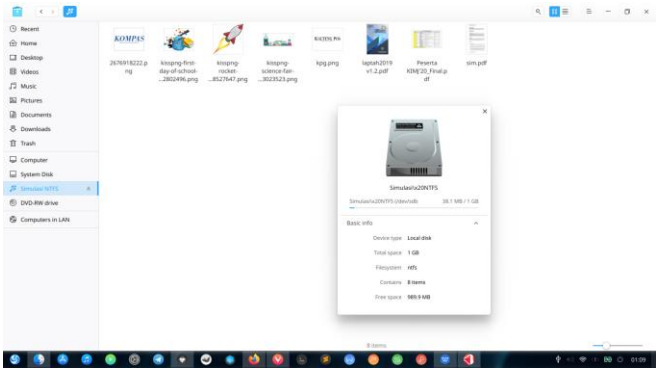
A. Collection

Dalam proses simulasi pengumpulannya menggunakan media penyimpanan Flashdisk yang diatur dengan kapasitas penyimpanan 1 Gb. Sistem file digunakan untuk penelitian menggunakan FAT-32 dan NTFS.



Gambar 2. Media penyimpanan dengan sistem file FAT32

Pada Gambar 2 informasi dapat diperoleh tentang media penyimpanan yang digunakan untuk pengujian adalah Flashdisk dengan kapasitas 1 Gb. Dalam media penyimpanan ini sistem file yang digunakan adalah FAT32, dalam media penyimpanan ini ada beberapa file yang disimpan sebelum proses penghapusan dan pemformatan.

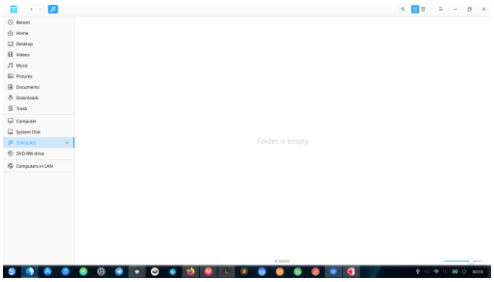


Gambar 3. Media penyimpanan dengan sistem file NTFS

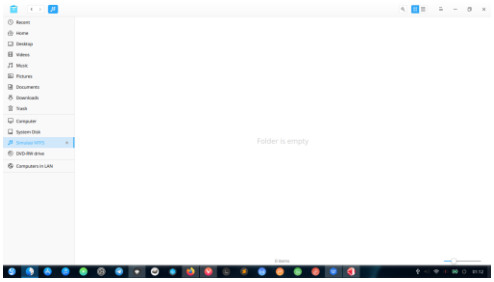
Pada Gambar 3 informasi dapat diperoleh tentang media penyimpanan yang digunakan untuk pengujian adalah Flashdisk dengan kapasitas 1 Gb. Dalam media penyimpanan ini sistem file yang digunakan adalah NTFS, dalam media penyimpanan ini ada beberapa file yang disimpan sebelum dihapus dan diformat.

B. Examination

Proses pemeriksaan terdapat pengujian pada media penyimpanan Flashdisk dengan merek Sandisk yang memiliki kapasitas penyimpanan 1 Gb menggunakan Foremost dan Scalpel.

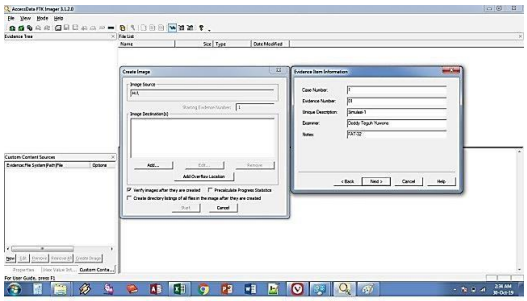


Gambar 4. Memeriksa Media Penyimpanan Direktori FAT32



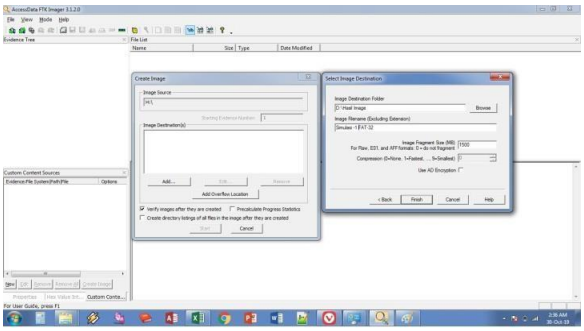
Gambar 5. Memeriksa Media Penyimpanan Direktori NTFS

Pada Gambar 4 dan 5, itu adalah tampilan dari isi media penyimpanan yang telah kosong karena file yang dihapus di dalamnya dan kemudian diformat. Selanjutnya adalah proses kloning media penyimpanan, proses ini adalah langkah untuk memastikan bahwa tidak ada perubahan data pada file digital yang disebabkan oleh kegiatan pemulihan File Carving. Kloning yang bertujuan menjaga aspek integritas dalam duplikasi data akan identik dengan data asli dengan menggunakan FTK Imager. Jika proses pencadangan logis dilakukan, dikhawatirkan akan ada perubahan untuk mendokumentasikan perangko waktu atau bahkan mengubah keaslian data. Tahap awal dalam proses kloning adalah memeriksa direktori media penyimpanan seperti yang ditunjukkan pada Gambar 6.



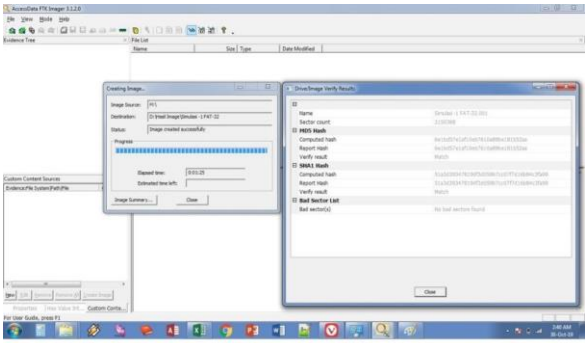
Gambar 6. Memeriksa Media Penyimpanan Direktori

Setelah mengetahui posisi direktori media penyimpanan yang akan dikloning, tentukan folder di mana output dari media penyimpanan dikloning. seperti pada Gambar 7:

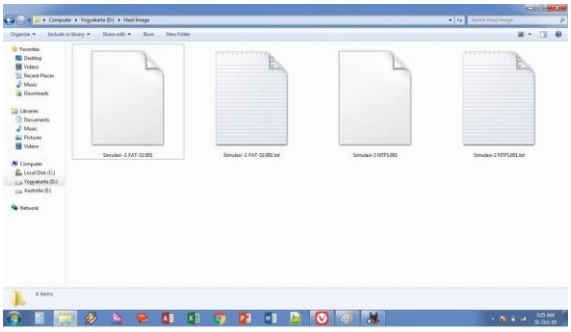


Gambar 7. Direktori Media Kloning Proses Penyimpanan Media

Dalam Gambar 8, menunjukkan bahwa proses kloning telah selesai.



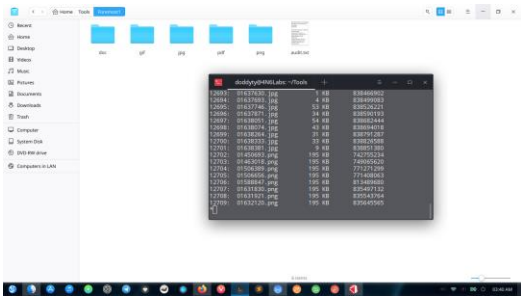
Gambar 8. proses kloning telah selesai



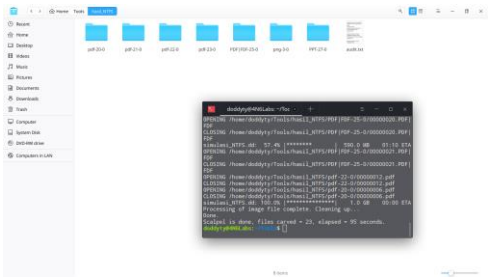
Gambar 9. proses kloning telah selesai

Pada Gambar 9, menunjukkan hasil kloning dari media penyimpanan

Pada Gambar 10 dan 11, proses mengembalikan File Carving, File Carving itu sendiri adalah kumpulan file yang telah dihapus, disembunyikan dan diformat, sehingga file tersebut tidak utuh dan perlu disusun ulang secara terstruktur sehingga dapat dikembalikan utuh seperti file asli yang dapat dibuka, dibaca, diedit dan diedit dan digunakan sebagaimana mestinya. (Mahant dan Meshram, 2012)



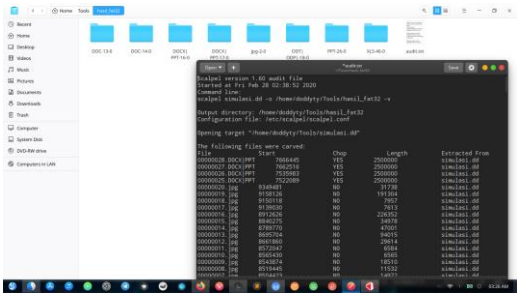
Gambar 10. Proses mengembalikan File Carving dengan Scalpel



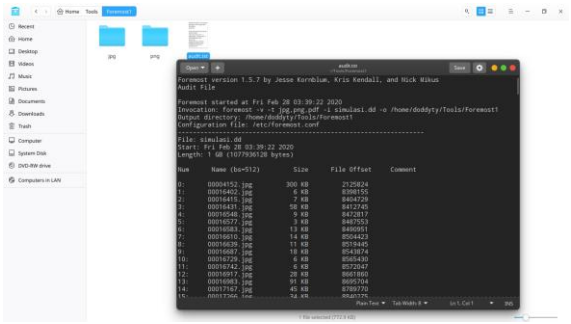
Gambar 11. Proses mengembalikan File Carving dengan Foremost

C. Analysis

Pada proses menganalisis file yang telah dipulihkan menggunakan Foremost dan Scalpel, seperti pada Gambar 12 dan 13, Stempel waktu akan diperiksa.



Gambar 12. Proses menganalisis file yang telah dipulihkan menggunakan Scalpel



Gambar 13. Proses menganalisis file yang telah dipulihkan menggunakan Foremost

D. Laporan

Pada tahap pelaporan hasil analisis telah dilakukan, hasil-hasil berikut yang telah ditemukan dari proses Carving File Pemulihan tercantum dalam Tabel 2.

Tabel 2 Scalpel and Foremost Test Results

No	Name	Information	
		FAT-32	NTFS
1	File Deleted	√	√
2	File Hidden	√	√
3	Formatted file	√	√

4. KESIMPULAN DAN SARAN

Foremost dan Scalpel dapat menampilkan file yang telah dihapus dan diformat. Keuntungan menggunakan Scalpel selama proses media penyimpanan forensik, Scalpel menghasilkan Pengembalian yang lebih baik bila dibandingkan dengan Foremost, keduanya menyediakan laporan audit yang menjelaskan semua tahapan dan proses analisis dalam memperoleh dan mengembalikan file yang telah dihapus, disembunyikan dan diformat pada media penyimpanan

DAFTAR PUSTAKA

Mahant, S. H. and Meshram, B. B. (2012) 'NTFS Deleted Files Recovery: Forensics View', IRACST -International Journal ofComputer Science and Information Technology & Security, 2(3),pp.491–497. Available at: http://ijcsits.org/papers/Vol2no32012/1vol2no3.pdf.

Putra, R. A., Fadlil, A. and Riadi, I. (2017) 'Forensik Mobile Pada Smartwach Berbasis Android', JURTI, pp. 41–47. doi: 25798790

Rana, N. et al. (2017) 'Taxonomy of Digital Forensics : Investigation Tools and Challenges Department of Computer Science and Engineering Accendere Knowledge Management Services Pvt . Ltd ., India', Computers and Society. Available at: https://arxiv.org/ftp/arxiv/papers/1709/1709.06529.pdf

Riadi, I., Umar, R. and Nasrulloh, I. M. (2018) 'Analisis Forensik Digital Pada Frozen Slod State Drive Dengan Metode National Institute of Justice (Nij)', 3(May), pp. 70–82. doi: 10.21831/elinvo.v3i1.19308.

Riadi, I., Sunardi; and Rauli, E. (2018) 'Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics', Scientific Journal of Informatics (SJI) UNNES, 10(1), pp. 18–22.

DT Yuwono, S Juhairiah, S Sonedi (2019), Analisis File Carving Pada File System Dengan Metode National Institute Of Standards And Technology (NIST)', Seminar Nasional Riset Terapan 4, POLIBAN A85-A92 Available at: http://e-prosiding.poliban.ac.id/index.php/snrt/article/view/408/354

Yudhana, A., Riadi, I. and Anshori, I. (2018) 'Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist', 3(1), pp. 13–21.

Yuwono, D. T., Fadlil, A. and Sunardi (2019) 'Performance Comparison of Forensic Software for Carving Files using National Institute of Standards and Technology (NIST) Method', Jurnal Teknologi dan Sistem Komputer, 7(03). doi: 10.14710/jtsiskom.7.3.2019.%p