Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 1, November 2024, Page 472-479
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i1.6125

Investigasi File Carving pada Media Penyimpanan Menggunakan Framework Computer Forensic Investigative Process

La Jupriadi Fakhri[1,*], Imam Riadi[2], Anton Yudhana[3]

[1]Program Studi Teknik Informatika, Universitas Muhammadiyah Sorong, Sorong, Indonesia
[2]Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[3]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
Email: [1,*] fakhrikmt@um-sorong.ac.id, [2]imam.riadi@is.uad.ac.id, [3]eyudhana@ee.uad.ac.id
Email Penulis Korespondensi: fakhrikmt@um-sorong.ac.id
Submitted: 24/10/2024; Accepted: 30/11/2024; Published: 30/11/2024

Abstrak−Salah satu pemanfaatan media penyimpanan digital di era digital yang masih populer hingga saat ini adalah penggunaan flashdisk sebagai sarana transfer data antar perangkat komputer. Flashdisk sering digunakan sebagai barang bukti dalam kasus investigasi digital. Risiko kehilangan data merupakan salah satu masalah utama sering yang dihadapi masyarakat. Kehilangan data terjadi karena berbagai alasan, seperti kesalahan pengguna, kegagalan perangkat, serangan malware, atau tindakan kriminal seperti peretasan. Teknik file carving digunakan untuk memulihkan file yang hilang atau terhapus dari media penyimpanan digital dengan perangkat lunak Foremost. Namun, begitu banyak jenis file terkadang sulit untuk memilih jenis file mana yang akan dipulihkan dan bagaimana memastikan keaslian file tersebut. Penelitian ini menggunakan Framework Computer Forensic Investigative Process (CFIP) pada flashdisk yang digunakan sebagai barang bukti dalam suatu perkara pidana. Perangkat lunak Foremost digunakan untuk melakukan teknik file carving pada flashdisk. Hasil penelitian menunjukkan bahwa proses akuisisi data menggunakan DC3DD berhasil menghasilkan bukti digital dengan nilai hash yang identik dengan file aslinya. Perangkat lunak Foremost berhasil memulihkan berbagai jenis file, seperti 9 file gambar dengan tipe file jpg, 5 file audio dengan tipe file mp3, dan 5 file dokumen dengan tipe file pdf. Foremost menunjukkan tingkat keberhasilan yang tinggi, dengan akurasi file carving sebesar 90% untuk file gambar, dan 62,5% untuk file audio dan dokumen. Rata-rata tingkat keberhasilan perangkat lunak Foremost dalam mengembalikan barang bukti adalah 73,08%.

Kata Kunci: File Carving; Foremost; Flashdisk; Investigasi; CFIP

Abstract−One of the uses of digital storage media in the digital era that is still popular today is the use of flash drives as a means of transferring data between computer devices. Flash disks are often used as evidence in digital investigation cases. The risk of losing data is one of the main problems that society often faces. Data loss occurs for various reasons, such as user error, device failure, malware attack, or criminal acts such as hacking. The file carving technique is used to recover lost or deleted files from digital storage media with Foremost software. However, with so many file types, it is sometimes difficult to choose which file types to recover and how to ensure the authenticity of the files. This study uses the Computer Forensic Investigative Process (CFIP) Framework on a flash drive, which is used as evidence in a criminal case. Foremost software is used to perform file carving techniques on flash drives. The results showed that the data acquisition process using DC3DD succeeded in producing digital evidence with a hash value that is identical to the original file. Foremost software successfully recovered various file types, such as 9 image files with jpg file type, 5 audio files with mp3 file type, and 5 document files with pdf file type. Foremost shows a high success rate, with file carving accuracy of 90% for image files, and 62.5% for audio files and documents. The average success rate of Foremost software in returning evidence is 73.08%.

Keywords: File Carving; Foremost; Flashdisk; Investigation; CFIP

1. PENDAHULUAN

Perkembangan teknologi informasi dipengaruhi oleh era digital yang semakin maju menyebabkan peningkatan signifikan dalam penggunaan media penyimpanan elektronik seperti *hard disk*, USB *drive*, dan kartu memori dalam kehidupan sehari-hari [1]–[4]. Penggunaan media penyimpanan elektronik membawa dampak yang luas dalam berbagai sektor individu maupun organisasi. Peningkatan penggunaan media penyimpanan digital menghadirkan tantangan baru dalam menghadapi situasi seperti data penting dapat hilang, terhapus secara tidak sengaja, atau bahkan disebabkan oleh tindakan kriminal [5].

Risiko kehilangan data menjadi salah satu masalah utama yang dihadapi dalam era digital. Kehilangan data terjadi karena berbagai alasan, seperti kesalahan pengguna, kegagalan perangkat, serangan *malware*, atau tindakan kriminal seperti *hacking* [6]. Beberapa kasus kehilangan data memiliki konsekuensi serius bagi individu atau organisasi apalagi data yang hilang merupakan data rahasia perusahan atau instansi. Oleh karena itu dibutuhkan metode memulihkan data yang hilang atau terhapus untuk melindungi data dengan aman.

Intansi pemerintah merupakan lembaga yang harus melindungi data dengan aman karena sering terjadi penyerangan atau pencurian data oleh pihak yang tidak bertanggung jawab. Penanganan kehilangan data dapat ditangani oleh tenaga profesional salah satunya adalah ahli forensik [7], [8]. Beberapa kasus tindak pidana membutuhkan ahli forensik terutama dalam bidang digital [9]–[12]. Penting bagi penyidik forensik digital untuk mengembangkan pengetahuan dan keterampilan untuk mengatasi tantangan memulihkan data yang hilang. Perkembangan teknologi informasi yang cepat mengharuskan untuk mengikuti tren terbaru dalam metode dan alat forensik digital. Selain itu, pengembangan praktik investigasi yang lebih baik juga menjadi tujuan penting, di mana hasil penelitian dan penemuan baru dapat memberikan pemahaman yang lebih baik tentang penggunaan

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 1, November 2024, Page 472-479
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i1.6125

metode pemulihan data dalam investigasi forensik digital. Penyidik dapat menghadapi tantangan yang muncul dalam era digital lebih efektif dan memberikan kontribusi positif dalam pengembangan praktik investigasi yang lebih baik di masa depan dengan penerapan metode forensik.

Salah satu metode yang sering digunakan dalam forensik digital untuk memulihkan data yang hilang atau terhapus adalah teknik *file carving*. *File carving* adalah proses yang memungkinkan pemulihan data dari media penyimpanan berdasarkan tanda-tanda atau pola tertentu [13]–[16]. Perangkat lunak *foremost* memiliki beberapa fitur yang berguna dalam proses pemulihan data. Fitur-fitur tersebut termasuk kemampuan untuk mendeteksi berbagai jenis file seperti gambar, video, *audio*, dokumen, dan lainnya. Selain itu, perangkat lunak ini juga dapat mengatasi fragmentasi data, yang sering terjadi dalam media penyimpanan yang rusak atau terhapus [17]. Dengan demikian, perangkat lunak *foremost* menjadi pilihan yang tepat dalam melakukan *file carving* pada media penyimpanan dalam penelitian ini. Proses pemulihan data memerlukan keterampilan dan pengetahuan khusus dalam menggunakan teknik alat forensik digital. Selain itu, kompleksitas media penyimpanan yang berbeda, seperti sistem *file* yang digunakan, format data, dan kemungkinan terjadinya fragmentasi data, juga menjadi tantangan dalam mengidentifikasi, merekonstruksi, dan memulihkan data yang hilang dengan akurasi dan keberhasilan yang tinggi. Namun, dalam konteks investigasi forensik digital, masih terdapat beberapa tantangan yang perlu diatasi. Tantangan tersebut antara lain kompleksitas media penyimpanan yang berbeda, kemampuan mengidentifikasi dan merekonstruksi file yang hilang, serta ketepatan dan keakuratan dalam proses investigasi. Penelitian ini akan menggunakan *Framework Computer Forensic Investigative Process* (CFIP) untuk mengatasi permasalahan *File carving*. CFIP adalah sebuah model investigasi forensik komputer yang dikembangkan oleh *International Association of Computer Investigative Specialists* (IACIS). IACIS adalah sebuah organisasi nirlaba yang didirikan pada tahun 1990 oleh sekelompok investigator komputer dan ahli forensik digital yang ingin mengembangkan standar industri dan metode investigasi yang terstruktur dalam bidang forensik komputer. *Framework* ini menyediakan pendekatan sistematis dan terstruktur untuk melakukan investigasi forensik komputer, termasuk dalam konteks *file carving* pada media penyimpanan. *Framework* ini diharapkan dapat membuat proses investigasi menjadi lebih terarah, efisien dalam memulihkan data yang hilang atau terhapus.

Penelitian sebelumnya terkait kejahatan *cyber* dalam menemukan bukti digital telah banyak dilakukan salah satunya oleh Syahib dkk, menggunakan *framework National Institute of Standards Technology* (NIST) untuk akuisisi bukti digital aplikasi *viber* menggunakan *tools Mobiledit Forensic*, penelitian ini berhasil menemukan data akun, kontak, pesan teks, riwayat panggilan, gambar dan video dari perangkat *smartphone* pelaku [18]. Penelitian lainnya yang dilakukan oleh Qibriya dkk, menggunakan *framework* NIST untuk analisis forensik bukti digital pada aplikasi *instant messaging* menggunakan *tools Mobiledit Forensic Express*, *FTK Imager* dan *Autopsy* [19]. Penelitian yang dilakukan oleh Rusydi dkk, menggunakan *framework Digital Forensic Research Workshop* (DFRWS) untuk perbandingan *tools* forensik pada aplikasi dompet digital dalam menemukan bukti digital terkait informasi aktivitas transaksi menggunakan *tools Autopsy* dan *Belkasoft Evidence Center*, hasil penelitian ini menemukan data *tool Autopsy* sebesar 47,05% sedangkan pada *tool forensic Belkasoft Evidence Center* sebesar 41,17% [20]. Penelitian yang dilakukan oleh Wahyudi dkk, menggunakan *framework* DFRWS untuk mengungkap dan menguji keaslian bukti digital menggunakan *tools FTK Imager* dan *JPEGSNOOP* [21]. Penelitian yang dilakukan Putra dkk, menggunakan *framework* NIST untuk akuisisi bukti digital dan deteksi keaslian citra pada *WhatsApp* menggunakan *tools Magnet Axiom* dan *ForensicallyBeta*, hasil penelitian ini menemukan data akun, kontak, pesan teks, riwayat panggilan dan gambar dari perangkat *smartphone* pelaku [22].

Berdasarkan penelitian sebelumnya sebagian besar terkait dengan *artifact* barang bukti pada *smartphone* yang akan dijadikan barang bukti dan *framework* yang dipakai adalah forensik *mobile*. Tujuan dari penelitian ini adalah melakukan analisis untuk menemukan *artifact* barang bukti yang yang sudah dihapus pada media penyimpanan dengan teknik *file carving* menggunakan perangkat lunak *Foremost* dan *Framework Computer Forensic Investigative Process*. Penelitian ini diharapkan dapat memberikan informasi dan teknik baru dalam forensik digital pada media penyimpanan.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Metode penelitian yang digunakan adalah *Computer Forensic Investigative Process* (CFIP). Tahapan yang dikembangkan oleh CFIP sebagai pedoman dalam melakukan proses investigasi barang bukti digital terdiri dari empat tahapan yaitu *acquisition*, *identification*, *evaluation*, dan *admission* yang dapat dilihat pada Gambar 1.

Gambar 1. Tahap dalam metode CFIP

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 1, November 2024, Page 472-479
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i1.6125

Gambar 1 Menunjukan tahapan penelitian yang akan dilakukan untuk melakukan analisis forensik pada penelitian ini dan berikut penjelasan dari setiap tahap.

a. *Acquisition*
   Pada tahap ini, bukti digital dikumpulkan dengan hati-hati dan sistematis dari berbagai sumber, seperti perangkat keras, perangkat lunak, dan jaringan. Akuisisi dapat dilakukan secara fisik dengan mengambil perangkat langsung, atau melalui metode logis dengan menggunakan perangkat lunak khusus. Tujuan akuisisi adalah mendapatkan salinan forensik yang akurat dan sah dari bukti digital, sambil memastikan integritasnya terjaga.
b. *Identification*
   Pada tahap ini dilakukan identifikasi dan memahami jenis, sifat, dan konteks bukti digital yang diperoleh. Identifikasi melibatkan pengklasifikasian dan kategorisasi data berdasarkan jenis file, format file, lokasi, waktu penciptaan, atau atribut lainnya. Hal ini membantu investigator untuk mengenali potensi bukti yang relevan.
c. *Evaluation*
   Tahap evaluasi merupakan proses mendalam untuk mengumpulkan informasi dari bukti digital yang ditemukan. Proses ini melibatkan pemulihan data yang terhapus, pemecahan kode, pemulihan informasi dari *file* yang rusak, analisis metadata, dan rekonstruksi aktivitas digital. Tujuan evaluasi adalah mengidentifikasi pola, hubungan, atau kejadian yang relevan dalam bukti digital untuk membentuk bukti yang kuat dalam kasus tersebut.
d. *Admission*
   Tahap admission merupakan proses penyusunan laporan forensik yang berisi temuan, metode analisis, dan kesimpulan. Laporan ini harus disajikan dengan jelas, akurat, mengikuti standar hukum, dan dapat digunakan sebagai bukti dalam proses hukum terkait tindak kejahatan *cyber* [23]–[25].

2.2 Alat dan Bahan

Alat dan bahan yang digunakan pada investigasi digital forensik sangatlah penting untuk memastikan integritas data tetap terjaga dan tidak terganggu. Alat dan bahan yang digunakan pada investigasi forensik *file carving* menggunakan metode CFIP disajikan pada Tabel 1.

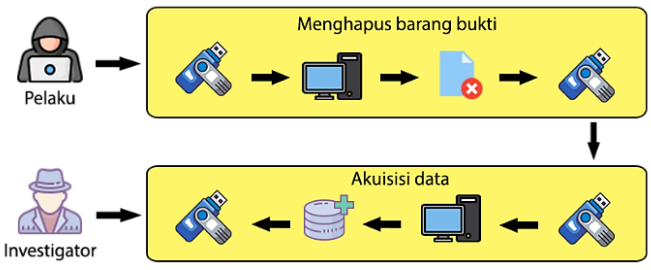
Tabel 1. Alat dan Bahan

Nama	Spesifikasi	Keterangan
Sistem Operasi	*Arc-Linux*	*Operating System*
Laptop	*Acer Nitro 5 core i5*	*Hardware*
USB Flashdisk	*Sandisk 7 Gb*	*Hardware*
DC3DD	*Tool Forensics OpenSource*	*Software*
Foremost	*Tool Forensics OpenSource*	*Software*

Tabel 1 menunjukkan perangkat keras dan perangkat lunak dalam melakukan investigasi *file carving*. Penggunaan perangkat lunak *DC3DD* dan *Foremost* juga sangat diperlukan untuk melakukan proses *acquisition* dan *recovery*. Penggunaan Alat dan bahan yang tepat diharapkan dapat mempermudah proses investigasi secara efisien sehingga diperoleh hasil yang dapat dipertanggungjawabkan.

2.3 Studi Kasus

Studi kasus bertujuan untuk memudahkan proses identifikasi saat melakukan analisis bukti digital. Barang bukti yang diamankan merupakan media penyimpanan berupa *flashdisk* dalam keadaan mati atau tidak sedang aktif (*off*) di komputer. Objek penelitian sebagai bukti digital yang digunakan merupakan hasil data fiktif penemuan tindak kejahatan dengan melibatkan media penyimpanan berupa sebuah *flashdisk* melalui metode *file carving*. Gambar 2 menunjukkan skenario terkait objek bukti elektronik berupa *flashdisk*.



Gambar 2. Skenario penemuan *Flashdisk* sebagai bukti digital

Gambar 2 menunjukkan seorang pelaku yang terlibat dalam tindak kejahatan pencucian uang. Pelaku ini menyimpan berbagai bukti terkait kejahatannya, termasuk daftar transaksi, foto pihak-pihak terkait, dan rekaman

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 1, November 2024, Page 472-479
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i1.6125

percakapan dengan pihak lain terkait dengan kegiatan kriminal yang dilakukannya. Informasi tentang kejahatan yang dilakukan oleh pelaku tersebut diketahui oleh polisi melalui pihak ketiga atau melalui laporan anonim dari individu yang bekerja di perusahaan pelaku. Selama proses penggeledahan, polisi menemukan sebuah *flashdisk* kosong. Untuk mengungkap data apa yang pernah disimpan di dalam *flashdisk* tersebut, tim penyelidik menggunakan metode *file carving* guna mendapatkan salah satu bukti yang terdapat di dalam *flashdisk* tersebut. Simulasi awal yang dilakukan adalah *quick format* pada *flashdisk* menggunakan *file system FAT32*. Selanjutnya *flashdisk* diisi dengan berbagai *file* berekstensi *pdf*, *jpg*, dan *mp3*. Informasi lengkap mengenai *file* yang disalin ke dalam *flashdisk* dapat ditemukan pada Tabel 2.

Tabel 2. *File* yang disalin ke dalam *Flashdisk*

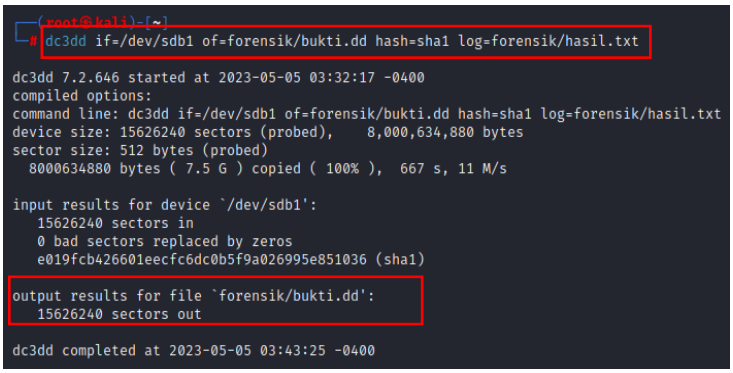
No	Nama *File*	*Format File*	Nilai *Hash* (*MD5*)
1	Gambar 1	*jpg*	d69b3cb77770d0f9fe4ac00fd88c7790
2	Gambar 2	*jpg*	9c1448ecc578e796ea8dd41819a7a584
3	Gambar 3	*jpg*	8e760c6624ede1e0c196a8cecda3a1fb
4	Gambar 4	*jpg*	958c9010cb0c4e61bebda8c3e4110b91
5	Gambar 5	*jpg*	7d1d037d48b2fe72a4dad3117c208582
6	Gambar 6	*jpg*	e9f08b33b25ce3e514c9d7aa899a887d
7	Gambar 7	*jpg*	fa250fbef2d97ba627fb294ba5eb574c
8	Gambar 8	*jpg*	72078bc9733df809664bcfa606f4d95d
9	Gambar 9	*jpg*	6f0801785d8cd74113dc9ab5d0af8155
10	Gambar 10	*jpg*	03ed38261563ca7e14874ced0cfa6daa
11	Audio 1	*mp3*	30bd2736b7783973863dc1c2db913169
12	Audio 2	*mp3*	ba406ef9734d5fdd6910ac1ac427bf80
13	Audio 3	*mp3*	817ed96ea4f4fd24169771acdfb9c0ea
14	Audio 4	*mp3*	db798d6b6d47e790afbb60058120a6ca
15	Audio 5	*mp3*	bd452566ded58cbd0e806ed56db053fd
16	Audio 6	*mp3*	cbd4fcd5db0aa5c0059f1b6409353366
17	Audio 7	*mp3*	86710fcc8748d46c6fb05c5a15833eb4
18	Audio 8	*mp3*	8ed974d04204265ffafee9dc8305647f
19	Dokumen 1	*pdf*	74abac532beb852d2cda61a444f907df
20	Dokumen 2	*pdf*	95bc17cf311ff9fe170a2cc4aacabd32
21	Dokumen 3	*pdf*	264eee817e1df2b11761fbda49c6e4b8
22	Dokumen 4	*pdf*	97b7e9dc35b8ce4cc677af4021d0f6e5
23	Dokumen 5	*pdf*	80f300626cd70f0c9e3273c93666a764
24	Dokumen 6	*pdf*	ac29cc6ebd22aa6165bf8f9e38690d4a
25	Dokumen 7	*pdf*	a0323007b43cde8d6a097f06999458f1
26	Dokumen 8	*pdf*	282e0d196f7d3c8a0032f00d7c9f47df

Tabel 2 menyajikan data simulasi yang disimpan pada sebuah *flashdisk*, data tersebut dihapus permanen menggunakan perintah (*shift + delete*). Selanjutnya, menggunakan perangkat lunak *DC3DD* untuk melakukan *imaging data* pada *flashdisk* target menggunakan metode *physical drive*. Setelah proses *imaging* selesai dilakukan analisis terhadap data hasil *imaging* tersebut.

3. HASIL DAN PEMBAHASAN

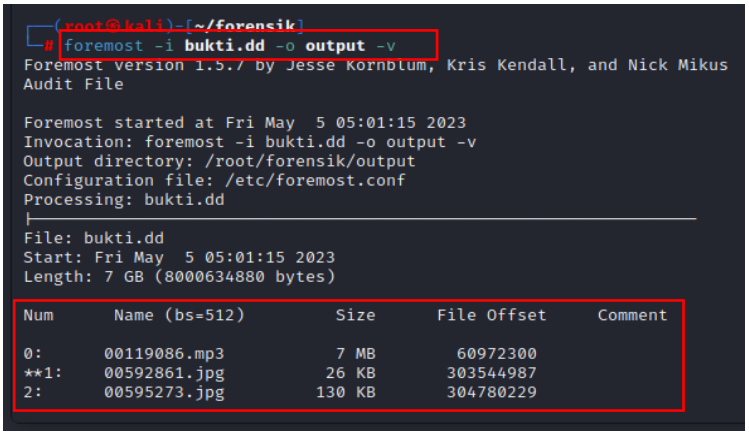
Tahapan pertama dalam metode CFIP adalah *acquisition*, di mana tim investigasi melakukan pengumpulan bukti fisik dan data pada media penyimpanan. Proses *cloning* menggunakan perangkat lunak *DC3DD* bertujuan membuat salinan bukti digital dari media penyimpanan seperti *flashdisk USB* dan mempertahankan integritas data agar data duplikasi identik dengan data asli. Sebelum memperoleh informasi dari *Flashdisk USB* yang ditunjukkan sebagai */dev/sdb1*, digunakan perintah *fdisk -l*. Kemudian proses *cloning* dilakukan menggunakan perintah *dc3dd if=/dev/sdb1 of=forensik/bukti.dd hash=sha1 log=/forensik/hasil.txt* seperti yang ditampilkan pada Gambar 3.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 1, November 2024, Page 472-479
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i1.6125



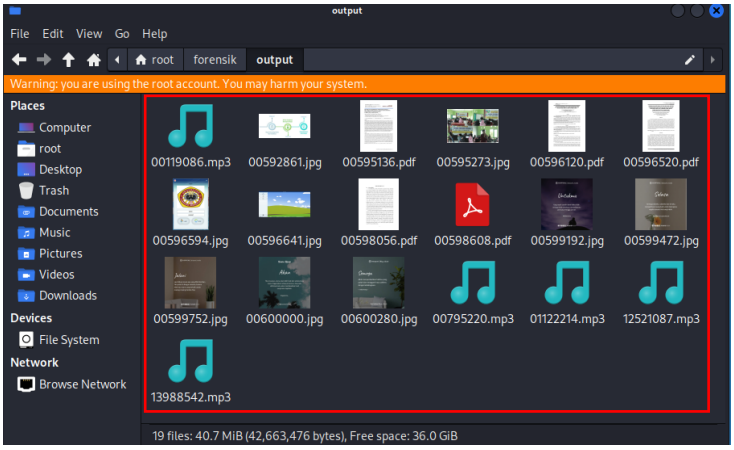
Gambar 3. Proses *Cloning Flashdisk USB* menggunakan *DC3DD*

Gambar 3 menyajikan hasil proses *cloning* yang diletakkan pada *folder forensik/bukti.dd* pada media penyimpan lokal, kemudian dibuatlah *folder* baru yang berisi *file* hasil dari proses *recovery file carving*. Proses *recovery file carving* dilakukan pada tahap kedua dalam proses investigasi forensik. Hal ini penting karena *file carving* harus dapat dibuka, dibaca, diedit dan digunakan sebagaimana mestinya. Tahap *identification* dilakukan menggunakan perangkat lunak *Foremost* yang berfungsi untuk pengembalian *file carving*. *Foremost* memiliki kemampuan untuk mengenali tipe *file* berdasarkan *signature* unik pada awal *file*, sehingga dapat mengembalikan *file carving* ke dalam bentuk yang dapat dibaca dan digunakan seperti semula. Setiap jenis *file* akan dikembalikan ke dalam folder tersendiri berdasarkan tipe filenya. Hal ini akan mempermudah proses identifikasi dan evaluasi pada tahap-tahap selanjutnya dalam proses investigasi forensik. Gambar 4 menampilkan proses pemulihan *file carving* menggunakan aplikasi *Foremost*.



Gambar 4. Proses pengembalian *File carving*

Gambar 4 menunjukkan hasil proses pengembalian *file carving*, di mana langkah selanjutnya adalah melakukan evaluasi terhadap hasil ekstraksi data yang diperoleh dari tahap *identification*. Tahap *evaluation* merupakan tahap ketiga dalam metode CFIP yakni berupa *file* direktori yang dipulihkan dengan menggunakan perangkat lunak *Foremost* untuk menghasilkan ekstraksi *file carving*. Beberapa *folder* berdasarkan tipe filenya kemudian digabungkan ke dalam satu *folder* seperti yang terlihat pada Gambar 5.



Gambar 5. Hasil ekstraksi *File carving*

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 1, November 2024, Page 472-479
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i1.6125

Tahap terakhir, yaitu pembuatan laporan manual oleh investigator dengan menggunakan hasil audit dari perangkat lunak *Foremost*. Laporan audit tersebut memuat rincian hasil ekstraksi selama proses penyelidikan dengan bukti yang telah dianalisis. Hasil pengujian dan investigasi pada media penyimpanan *flashdisk* dapat dijadikan alat bukti digital yang sah dan dapat dipertanggungjawabkan di persidangan. Tabel 3. menunjukkan data hasil *file carving* yang telah dianalisis pada media *flashdisk*.

Tabel 3. Hasil investigasi *File carving*

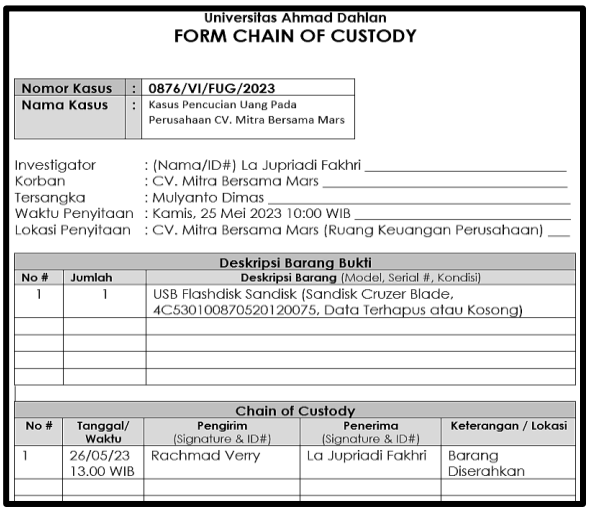
No	Nama File Foremost	Nama *File* Asli	Nilai *Hash* (*MD5*)	Validasi Hash
1	00592861.jpg	Gambar 1.jpg	d69b3cb77770d0f9fe4ac00fd88c7790	*valid*
2	00595273.jpg	Gambar 2.jpg	9c1448ecc578e796ea8dd41819a7a584	*valid*
3	00596594.jpg	Gambar 3.jpg	8e760c6624ede1e0c196a8cecda3a1fb	*valid*
4	00596641.jpg	Gambar 4.jpg	958c9010cb0c4e61bebda8c3e4110b91	*valid*
5	00599192.jpg	Gambar 5.jpg	7d1d037d48b2fe72a4dad3117c208582	*valid*
6	00599472.jpg	Gambar 6.jpg	e9f08b33b25ce3e514c9d7aa899a887d	*valid*
7	00599752.jpg	Gambar 7.jpg	fa250fbef2d97ba627fb294ba5eb574c	*valid*
8	00600000.jpg	Gambar 8.jpg	72078bc9733df809664bcfa606f4d95d	*valid*
9	00600280.jpg	Gambar 9.jpg	6f0801785d8cd74113dc9ab5d0af8155	*valid*
10	00119086.mp3	Audio 1.mp3	30bd2736b7783973863dc1c2db913169	*valid*
11	00795220.mp3	Audio 2.mp3	ba406ef9734d5fdd6910ac1ac427bf80	*valid*
12	01122214.mp3	Audio 3.mp3	817ed96ea4f4fd24169771acdfb9c0ea	*valid*
13	12521087.mp3	Audio 7.mp3	86710fcc8748d46c6fb05c5a15833eb4	*valid*
14	13988542.mp3	Audio 8.mp3	8ed974d04204265ffafee9dc8305647f	*valid*
15	00595136.pdf	Dokumen 1.pdf	74abac532beb852d2cda61a444f907df	*valid*
16	00596120.pdf	Dokumen 2.pdf	95bc17cf311ff9fe170a2cc4aacabd32	*valid*
17	00596520.pdf	Dokumen 5.pdf	80f300626cd70f0c9e3273c93666a764	*valid*
18	00598056.pdf	Dokumen 6.pdf	ac29cc6ebd22aa6165bf8f9e38690d4a	*valid*
19	00598608.pdf	Dokumen 7.pdf	a0323007b43cde8d6a097f06999458f1	*valid*

Tabel 3 menyajikan hasil investigasi *file carving* yang terdiri dari *file image* dengan *format jpg* sebanyak 9, *file audio* sebanyak 5 dengan *format mp3*, dan *document* berformat *pdf* sebanyak 5. Tingkat keberhasilan / akurasi proses *file carving* oleh alat forensik *Foremost* dinyatakan dalam Tabel 4.

Tabel 4. Persentasi keberhasilan pengembalian *File carving*

Bukti Digital	Tipe *File*	Bukti Yang Ditemukan	Bukti Yang Disalin	Persentasi Keberhasilan
File Gambar	.jpg	9	10	90%
File Audio	.mp3	5	8	62,5%
File Dokumen	.pdf	5	8	62,5%
Rata-rata				73,08%

Tabel 4 menyajikan persentasi keberhasilan diukur dari sebelum dan sesudah proses forensik dilakukan. *Foremost* hanya melakukan pencarian berdasarkan potongan memori tanpa ada pengulangan jika terdapat *header* dan *footer* yang berbeda potongan memorinya. Kemudian *Chain of Custody* digunakan sebagai panduan yang menunjukkan bagaimana bukti digital dikumpulkan, dianalisis, dan dijaga agar dapat digunakan sebagai bukti di pengadilan. Hasil dari dokumen *Chain of Custody* yang telah dibuat ditampilkan pada Gambar 6.



Universitas Ahmad Dahlan
FORM CHAIN OF CUSTODY

Nomor Kasus	:	0876/VI/FUG/2023
Nama Kasus	:	Kasus Pencucian Uang Pada Perusahaan CV. Mitra Bersama Mars

Investigator : (Nama/ID#) La Jupriadi Fakhri
Korban : CV. Mitra Bersama Mars
Tersangka : Mulyanto Dimas
Waktu Penyitaan : Kamis, 25 Mei 2023 10:00 WIB
Lokasi Penyitaan : CV. Mitra Bersama Mars (Ruang Keuangan Perusahaan)

Deskripsi Barang Bukti

No #	Jumlah	Deskripsi Barang (Model, Serial #, Kondisi)
1	1	USB Flashdisk Sandisk (Sandisk Cruzer Blade, 4C530100870520120075, Data Terhapus atau Kosong)

Chain of Custody

No #	Tanggal/ Waktu	Pengirim (Signature & ID#)	Penerima (Signature & ID#)	Keterangan / Lokasi
1	26/05/23 13.00 WIB	Rachmad Verry	La Jupriadi Fakhri	Barang Diserahkan

Gambar 6. *Form Chain of Custody*

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 1, November 2024, Page 472-479
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i1.6125

Gambar 6 menunjukkan catatan rinci tentang setiap individu yang memiliki kepemilikan atas bukti tersebut, termasuk tanggal, waktu, dan lokasi. Sangat penting dalam menjaga integritas dengan tujuan barang bukti tersebut tidak diubah-ubah, atau dirusak dengan cara apa pun. Hal ini disajikan pada *form Chain of Custody*, kemudian dapat digunakan pada proses persidangan sebagai hasil dari investigasi *file carving* pada media penyimpanan *flashdisk* yang telah didokumentasikan dengan benar dalam investigasi digital forensik.

Berdasarkan penelitian terdahulu yang telah dijelaskan pada bagian pendahuluan [18]–[22], dua penelitian yang menggunakan *framework DFRWS*, berhasil mengungkap bukti yang dihapus pada media penyimpanan *flashdisk* dengan menggunakan sistem operasi *Windows 8.1* dan perangkat lunak *Forensic Tool Kit (FTK) Imager* dan *JPEGSNOOP* [21]. Studi kasus lainnya melibatkan pencarian informasi atau dokumen elektronik yang berpotensi menjadi bukti digital pada aplikasi dompet digital menggunakan sistem operasi *Windows 10* dan perangkat lunak yang digunakan adalah *Autopsy* dan *Belkasoft Evidence Center* [20]. Tiga penelitian lain menggunakan *framework NIST* untuk melakukan analisis forensik digital pada aplikasi *instant messaging* di platform *Android*, perangkat lunak yang digunakan meliputi *MOBILedit Forensic Express*, *FTK Imager*, dan *Autopsy* [19]. Studi kasus lainnya mencakup akuisisi bukti digital pada aplikasi *Viber* dengan menggunakan perangkat lunak *Mobiledit Forensic* [18], serta akuisisi bukti digital dan deteksi keaslian citra pada WhatsApp dengan menggunakan perangkat lunak *Magnet Axiom*, *Axiom Examine*, dan *ForensicallyBeta* untuk menganalisis gambar bukti [22]. Sedangkan untuk penelitian yang dilakukan pada *paper* ini berhasil mengatasi permasalahan berdasarkan studi kasus *file carving* pada media penyimpanan *flashdisk* dengan fokus penelitian pengembalian barang bukti digital menggunakan *framework CFIP* menggunakan perangkat lunak *DC3DD* dan *Foremost*. Rata-rata tingkat keberhasilan yang diperoleh dari keseluruhan *file* yang berhasil dikembalikan adalah 73,08%. Namun, untuk memperkuat hasil penelitian ini, perlu dilakukan percobaan pada studi kasus lainnya di masa depan agar metode ini dapat diterapkan dengan baik.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa teknik investigasi forensik digital seperti *file carving* menggunakan perangkat lunak *Foremost* pada media penyimpanan *flashdisk* dapat menjadi alternatif dalam upaya mendapatkan bukti yang sah dalam kasus kriminal atau investigasi digital. Proses akuisisi data menggunakan perangkat lunak *DC3DD* berhasil menghasilkan bukti digital dengan nilai *hash* yang identik dengan *file* aslinya. Penelitian ini menunjukkan bahwa *Foremost* dapat memulihkan berbagai jenis *file*, termasuk 9 *file* gambar dalam format *jpg*, 5 *file audio* dalam format *mp3*, dan 5 *file* dokumen dalam format *pdf*. *Foremost* menunjukkan tingkat keberhasilan yang tinggi, dengan akurasi *file carving* sebesar 90% untuk 9 *file* gambar dengan tipe *file jpg*, dan 62,5% untuk *file audio* dan dokumen dalam format *mp3* dan *pdf*. Rata-rata tingkat keberhasilan perangkat lunak *Foremost* dalam mengembalikan barang bukti adalah 73,08%. Oleh karena itu, teknik investigasi forensik digital seperti *file carving* dengan menggunakan perangkat lunak *Foremost* dapat menjadi kombinasi teknik investigasi yang sangat berguna bagi para penyidik dalam upaya mengumpulkan bukti yang sah dan dapat digunakan dalam persidangan.

REFERENCES

[1] A. R. Trilaksono, "Efektivitas Penggunaan Google Drive Sebagai Media Penyimpanan Di Kalangan Mahasiswa," *J. Digit. Teknol. Inf.*, vol. 1, no. 2, pp. 91–197, 2020, doi: 10.32502/digital.v1i2.1651.

[2] H. Dhika, T. Akhirina, D. Mustari, and F. Destiawati, "Pemanfaatan Teknologi Cloud Computing sebagai Media Penyimpanan Data," *J. PkM Pengabdi. Kpd. Masy.*, vol. 2, no. 03, pp. 221–226, 2019, doi: 10.30998/jurnalpkm.v2i03.3144.

[3] M. K. Anam and H. Ulayya, "Implementasi dan Analisa SARDrive Sebagai Media Penyimpanan Cloud," *JUITA J. Inform.*, vol. 8, no. 1, pp. 83–90, 2020, doi: 10.30595/juita.v8i1.5748.

[4] A. Yudhana, I. Riadi, and S. Suharti, "Network Forensics Against Volumetric-Based Distributed Denial of Service Attacks on Cloud and the Edge Computing," *Int. J. Saf. Secur. Eng.*, vol. 12, no. 5, pp. 577–588, 2022, doi: 10.18280/ijsse.120505.

[5] I. Riadi, S. Sunardi, and S. Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, p. 87, 2019, doi: 10.30872/jurti.v3i1.2292.

[6] R. N. Dasmen and F. Kurniawan, "Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial," *Techno.Com*, vol. 20, no. 4, pp. 527–539, 2021, doi: 10.33633/tc.v20i4.5170.

[7] D. Frananda, . F., and H. Bakir, "Strategi Penyidik Mengatasi Kendala Dalam Mengumpulkan Alat Bukti Tindak Pidana Pornografi Melalui Media Elektronik," *UNES J. Swara Justisia*, vol. 5, no. 3, pp. 210–217, 2021, doi: 10.31933/ujsj.v5i3.217.

[8] N. Darwis, "Kriminology Pada Bidang Kebijakan 'Cyber Security,'" *J. Ilm. Huk. Dirgant.*, vol. 9, no. 2, pp. 24–46, 2019, doi: 10.35968/jh.v9i2.353.

[9] W. Prasetya and P. Priyana, "Pertimbangan Hakim Atas Penghadiran Bukti Digital Forensik dalam Perkara Kejahatan Fraud," *Wajah Huk.*, vol. 5, no. 2, pp. 448–459, 2021, doi: 10.33087/wjh.v5i2.472.

ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 6, No. 1, November 2024, Page 472-479
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v6i1.6125

[10] S. Rachmie, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website," *LITIGASI*, vol. 21, no. 21, pp. 104–127, Jul. 2020, doi: 10.23969/litigasi.v21i1.2388.
[11] A. Ganaro, "Fungsi Digital Forensik Bagi Satreskrim Polres Agam Dalam Penyidikan Tindak Pidana Judi Online," *UNES Law Rev.*, vol. 3, no. 2, pp. 194–200, 2021, doi: 10.31933/unesrev.v3i2.166.
[12] A. Yudhana, A. D. Cahyo, L. Y. Sabila, A. C. Subrata, and I. Mufandi, "Spatial distribution of soil nutrient content for sustainable rice agriculture using geographic information system and Naïve Bayes classifier," *Int. J. Smart Sens. Intell. Syst.*, vol. 16, no. 1, pp. 1–14, 2023, doi: 10.2478/ijssis-2023-0001.
[13] D. Teguh Yuwono, S. Juhairiah, and S. Sonedi, "Analisis File Carving Pada File System Dengan Metode National Institute Of Standards And Technology (NIST)," *Pros. SNRT (Seminar Nas. Ris. Ter.*, vol. 4, no. 1, pp. 85–92, 2019.
[14] A. K. Pratama, C. Carudin, and D. Yusup, "Analisis Perbandingan Perangkat Lunak Forensik Digital untuk File Carving dalam Mengungkap Barang Bukti Digital," *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 6, no. 2, pp. 109–120, 2021, doi: 10.32528/justindo.v6i2.5101.
[15] D. T. Yuwono, A. Fadlil, and S. Sunardi, "Performance Comparison of Forensic Software for Carving Files using NIST Method," *J. Teknol. dan Sist. Komput.*, vol. 7, no. 3, pp. 89–92, Jul. 2019, doi: 10.14710/jtsiskom.7.3.2019.89-92.
[16] I. Riadi, A. Yudhana, and G. P. I. Fanani, "Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation," *Int. J. Saf. Secur. Eng.*, vol. 13, no. 1, pp. 11–19, Feb. 2023, doi: 10.18280/ijsse.130102.
[17] D. T. Yuwono and Yunanri, "Analisis Perbandingan File Carving Dengan Metode NIST," *J. Sains Komput. dan Teknol. Inf.*, vol. 2, no. 2, pp. 1–6, 2020, doi: 10.33084/jsakti.v2i2.1472.
[18] M. I. Syahib, I. Riadi, and R. Umar, "Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST)," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 4, no. 1, pp. 170–178, 2020, doi: 10.30645/j-sakti.v4i1.196.
[19] M. R. D. Qibriya, A. Ambarwati, and K. E. Susilo, "Analisis Forensik Digital Pada Aplikasi Instant Messaging Di Smartphone Berbasis Android Untuk Bukti Digital," *J. Teknol. Inf.*, vol. 5, no. 2, pp. 114–121, 2021, doi: 10.36294/jurti.v5i2.2200.
[20] R. Umar, A. Yudhana, and M. N. Fadillah, "Perbandingan Tools Forensik pada Aplikasi Dompet Digital," *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 2, pp. 242–250, Sep. 2022, doi: 10.26798/jiko.v6i2.621.
[21] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Mengungkap Dan Menguji Keaslian Bukti Digital Pada Kejahatan Cybercrime Dengan Metode Digital Forensic Research Workshop," *J. Apl. Teknol. Inf. dan Manaj.*, vol. 2, no. 2, pp. 120–127, 2021, doi: 10.31102/jatim.v2i2.1068.
[22] I. P. Wiratama, A. Suharso, and C. Rozikin, "Akuisisi Bukti Digital Dan Deteksi Keaslian Citra Pada Whatsapp Menggunakan Metode NIST Dan ELA," *J. Sains Komput. Inform.*, vol. 5, no. 2, pp. 712–726, 2021, doi: 10.30645/j-sakti.v5i2.370.
[23] H. Herman, A. Yudhana, and F. Anggraini, "Acquisition of Android-Based TikTok Digital Evidence Using the National Institute of Justice Method," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 1, pp. 89–96, 2023, doi: 10.25126/jtiik.2023106416.
[24] A. Yudhana, R. Umar, and A. B. Fawait, "Decision Making Using the MABAC Method to Determine the Leading Small and Medium Industry Centers in Yogyakarta," *Ingénierie des systèmes d Inf.*, vol. 27, no. 6, pp. 887–893, 2022, doi: 10.18280/isi.270604.
[25] R. Y. Prasongko, A. Yudhana, and I. Riadi, "Analysis of the Use of the ACPO (Association of Chief Police Officer) Method in WhatsApp Forensics," *J. Sains Komput. Inform. (J-SAKTI*, vol. 6, no. 2, pp. 1112–1120, 2022, doi: 10.30645/j-sakti.v6i2.520.