Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus

Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence

Wahyudi Agustiono[1]*, **Dini Wulan Suci**[2], **Novi Prastiti**[3]
Program Studi Sistem Informasi, Universitas Trunojoyo Madura, Indonesia[123]
wahyudi.agustiono@trunojoyo.ac.id[1], dewees2811@gmail.com[2], prastitinovi@trunojoyo.ac.id[3]

Abstrak

Perkembangan teknologi informasi tidak hanya memberikan dampak positif, tetapi juga membuka peluang kecurangan yang memicu munculnya kejahatan digital. Salah satu kejahatan digital yang paling sering terjadi yaitu carding dengan menggunakan bukti elektronik seperti flashdisk dan harddisk. Pada umumnya pelaku akan berusaha mencoba menghilangkan jejak kejahatannya dengan menghapus seluruh file yang tersimpan baik di flashdisk ataupun hardisk yang dapat dijadikan barang bukti. Apabila hal ini terjadi, maka akan menyulitkan para penegak hukum untuk mengungkapkan kejahatan tersebut oleh karena hilangnya barang bukti digital. Oleh karena itu, penelitian ini bertujuan melakukan investigasi bagaimana memulihkan data yang telah dihapus menggunakan metode NIST SP 800-86, yang terdiri dari empat tahapan: Pengumpulan, Pemeriksaan, Analisis, dan Pelaporan. Penelitian ini memanfaatkan FTK *Imager* untuk membantu proses akuisisi data yang dihilangkan pada media penyimpanan. Untuk simulasi pemulihan data dilakukan lima kali pengujian dengan interval waktu dua minggu di setiap pengujian. Simulasi ini bertujuan untuk membuktikan efektivitas dan batasan dari metode yang digunakan dalam pemulihan data yang dihapus. Analisis menunjukkan bahwa data hasil pemulihan kemudian dianalisis menggunakan *Autopsy*. Hasil forensik menunjukkan bahwa FTK *Imager* dan *Autopsy* mampu memulihkan bukti yang dihapus secara permanen (*Shift+Delete*) dengan tingkat keberhasilan 100%. Namun demikian, data yang dihapus melalui pemformatan tidak dapat dipulihkan, dengan tingkat keberhasilan 0%.
Kata kunci: Analisis Forensik Digital; *Autopsy*; *Cybercrime*; FTK *Imager*; NIST SP 800-86.

Abstract

The development of information technology not only brings positive impacts but also opens opportunities for fraud, leading to the emergence of digital crimes. One of the most common digital crimes is carding, which uses electronic evidence such as flash drives and hard drives. Generally, perpetrators will try to erase all stored files on flash drives or hard drives that could be used as evidence to cover their tracks. If this happens, it makes it difficult for law enforcement to uncover the crime due to the loss of digital evidence. Therefore, this study aims to investigate how to recover deleted data using the NIST SP 800-86 method, which consists of four stages: Collection, Examination, Analysis, and Reporting. This study utilizes FTK Imager to assist in the data acquisition process on the storage media. For the data recovery simulation, five tests were conducted with a two-week interval between each test. This simulation aims to demonstrate the effectiveness and limitations of the method used in recovering deleted data. The analysis indicates that the recovered data is then analyzed using Autopsy. Forensic results show that FTK Imager and Autopsy can recover permanently deleted evidence (Shift+Delete) with a success rate of 100%. However, data deleted through formatting cannot be recovered, with a success rate of 0%..
Keywords: Autopsy; Cybercrime; Digital Forensic Analysis; FTK Imager; NIST SP 800-86.

Naskah diterima 3 Juni 2024; direvisi 8 Agustus 2024; dipublikasi 1 September 2024.

1. Pendahuluan

Saat ini teknologi informasi berkembang sangat pesat karena telah menjadi bagian penting yang tidak terpisahkan dalam setiap lini kehidupan manusia. Salah satu manfaat positif dari penggunaan teknologi informasi adalah kemampuannya untuk mempermudah individu atau kelompok dalam melakukan berbagai aktivitas melalui proses digitalisasi. Kemajuan ini semakin pesat dengan hadirnya internet yang memfasilitasi munculnya dunia siber (*cyber*) [1]. Namun demikian, sebagaimana dunia nyata, terdapat dampak negatif yang berpotensi muncul akibat penyalahgunaan teknologi informasi oleh individu atau kelompok yang tidak bertanggung jawab yang dapat menimbulkan kerugian material yang nyata dan sering disebut sebagai kejahatan siber (*cybercrime*) [2]. Secara sederhana *cybercrime* ini merupakan suatu aktivitas yang mentargetkan teknologi informasi sebagai media perantara dalam melancarkan aksi kejahatan, seperti melakukan peretasan terhadap jaringan, *spamming*, serangan DoS, pencurian data, merusak informasi pribadi orang lain, dan lain sebagainya [3].

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

Serupa dengan kejahatan di dunia nyata, tindak kejahatan siber ini akan meninggalkan rekam jejak dari aktivitas yang dilakukan dapat dijadikan sebagai barang bukti atau petunjuk pengungkapan. Namun berbeda dengan kejahatan di dunia nyata, barang bukti yang ditinggalkan pada kasus *cybercrime* terbagi menjadi dua kategori, yaitu barang bukti elektronik dan digital [4]. Barang bukti elektronik adalah rekam jejak dari suatu aktivitas kejahatan yang memiliki bentuk nyata fisik dan umumnya berupa perangkat elektronik atau penyimpanan *(storage device)*. Sedangkan bukti digital merupakan rekam jejak dari kasus kejahatan siber yang dapat berbentuk *file* dokumen, *history*, atau *log* aktifitas yang berisi data atau informasi mengenai aktivitas *cybercrime* yang didapat melalui proses ekstraksi atau pengambilan data yang berada dalam bukti elektronik yang sebelumnya telah diidentifikasi.

Sebagaimana yang telah disebutkan bahwa barang bukti yang ditinggalkan dari kasus *cybercrime* berbeda dengan bukti yang didapat dari kasus kejahatan konvensional, maka dari itu proses perlakuan dan pengungkapan bukti elektronik maupun bukti digital perlu adanya penanganan khusus. Hal ini dikarenakan karakteristik dan kondisi barang bukti digital yang tidak kasat mata, rapuh, mudah mengalami perubahan, dan alterasi [5]. Karena adanya resiko mengalami perubahan atau kebocoran data, maka barang bukti elektronik dan digital harus disimpan dan didokumentasikan dengan baik melalui proses forensik digital [6].Risiko perusakan atau bahkan penghilangan tersebut semakin tinggi apabila para penegak hukum yang menangani *cybercrime* ini tidak memahami bagaimana cara memperlakukan dan memproses barang bukti digital yang sesuai dengan kerangka kerja atau standar yang berlaku.

Sebagai contoh semakin maraknya kasus kejahatan yang melibatkan jaringan internet sebagai alat untuk menyerang atau mencuri data pribadi korban. Dari berbagai macam kejahatan siber ini, carding adalah salah satu yang paling marak dan pada umunya menimbulkan dampak atau kerugian yang besar bagi korban. Carding adalah tindakan kejahatan siber di bidang perbankan, yang mana pelaku secara ilegal membobol dan mencuri nomor atau identitas kartu kredit milik orang lain secara *illegal* [7]. Dalam proses penanganan kasus kejahatan carding, para penyidik akan memerlukan pengumpulan barang bukti yang dilakukan dengan teknik *imaging*. Salah satu barang bukti yang dapat dilakukan *imaging* yaitu perangkat penyimpanan seperti *harddisk* dan *flashdisk*, yang selanjutnya akan digunakan sebagai bukti untuk membawa kasus *cybercrime* ke pengadilan. Dalam beberapa kasus carding, pelaku menggunakan perangkat penyimpanan eksternal untuk menyimpan bukti kejahatannya, hal ini dikarenakan penyimpanan eksternal cenderung memiliki kapasistas penyimpanan data yang besar namun mudah untuk dibawa kemanapun [8] *Harddisk* dan *flashdisk* merupakan media penyimpanan eksternal yang sering digunakan karena sifat *portable* dan kapasitas penyimpanan datanya yang besar.

Pelaku *cybercrime* biasanya akan melakukan berbagai cara untuk menghilangkan barang bukti yang berhubungan dengan tindak kejahatan yang mereka lakukan. Salah satu cara untuk menghilangkan bukti tersebut dengan cara menghapus atau memformat data atau informasi yang berkaitan dengan tindakan yang dilakukan tidak dapat ditemukan. Teknik yang biasanya digunakan oleh para pelaku dalam melakukan penghapusan data ialah dengan menekan tombol *delete* dan mengosongkan *folder recycle bin* atau *trash* pada sistem, atau bisa disebut sebagai penghapusan berganda. Oleh sebab itu diperlukan adanya proses forensik yang bertujuan untuk memulihkan kembali data atau informasi yang telah dihapus oleh pelaku sehingga para penyidik dapat menyelesaikan suatu kasus *cybercrime* [9].

Modus opearandi kejahatan ini menunjukkan pentingnya penerapan standar keamanan untuk mencegah risiko siber. Dengan menerapkan standar keamanan yang ketat, seperti enkripsi data, autentikasi multi-faktor, dan pemantauan sistem secara terus-menerus, organisasi dapat mengurangi kerentanan terhadap serangan siber dan melindungi informasi sensitif. Salah satu standar kerangka kerja keamanan yang sering direkomendasikan adalah *National Institute of Standards and Technology* (NIST) *Special Publication* 800-86. Penggunaan metode NIST bertujuan membantu dan mempermudah pekerjaan penyidik dalam mengetahui alur penelitian secara sistematis dan lebih terstruktur, sehingga dapat dijadikan sebagai pedoman dalam menyelesaikan suatu persoalan yang ada [10].

Kajian pustaka menemukan berbagai penelitian penerapan standar keamanan NIST SP 800-86 untuk membantu analisis forensik kejahatan siber seperti pada aplikasi *whatsapp* [11][12], *cyber-bullying* [13], keamanan jaringan komputer [14], dompet digital [15] dan insiden SQL *injection* [16]. Penelitian-penelitian tersebut umumnya berfokus pada penerapan NIST untuk *live forensic* dimana proses pengumpulan dan analisis data dari sistem komputer atau perangkat yang sedang beroperasi, memori volatil seperti RAM, koneksi jaringan aktif, dan sistem file yang sedang digunakan. Penelitian *live forensic* tersebut menawarkan pengatahunan bagaimana melakukan analisis forensik pada berbagai macam kejahatan siber. Selain itu *live forensic* ini memungkinkan penyidik untuk melihat aktivitas yang sedang berlangsung dan memantau perubahan real-time, yang dapat memberikan wawasan penting dalam penyelidikan siber.

Namun demikian penelitian yang berbasis *live forensic* tersebut belum banyak membahas bagaimana risiko memodifikasi data selama proses pengumpulan dan kebutuhan untuk alat dan keahlian khusus untuk

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

memastikan integritas dan keakuratan data yang dikumpulkan. *Live forensic* kurang cocok untuk analisis kejahatan carding yang biasanya melibatkan data penting seperti nomor kartu kredit, informasi identitas, dan transaksi keuangan yang sering kali disimpan di media penyimpanan permanen seperti *hard drive* atau *flash drive*. Data pada media penyimpanan ini umumnya tidak berubah meskipun sistem dimatikan, sehingga lebih efektif diakses melalui *dead forensic*. Teknik *dead forensic* ini juga memungkinkan untuk mengakses, memulihkan, dan menganalisis data yang dihapus atau disembunyikan, yang sering kali merupakan bagian penting dari bukti dalam kasus carding. Tabel 1 berikut ini merangkum perbedaan antara penelitian pada konteks *life* dan *dead forensic.*

Tabel 1. Perbandingan *life* dan *dead forensic*

Aspek	Life Forensic	Dead Forensic
Keadaan Sistem	Sistem dalam keadaan menyala	Sistem dalam keadaan mati
Jenis Data yang Dikumpulkan	Data volatil (RAM, proses aktif, koneksi jaringan)	Data non-volatil (hard drive, flash drive)
Risiko Modifikasi Data	Tinggi, karena sistem sedang berjalan	Rendah, karena sistem dalam keadaan mati
Alat yang Digunakan	Tools khusus untuk menangani memori dan aktivitas langsung	Tools untuk mengakuisisi dan menganalisis penyimpanan permanen
Potensi Pengumpulan Bukti	Dapat mengumpulkan bukti aktivitas real-time	Dapat mengumpulkan bukti dari penyimpanan yang tidak berubah
Kemungkinan Gangguan Sistem	Berpotensi mengganggu operasi sistem	Tidak mengganggu karena sistem tidak aktif
Kerumitan Proses	Lebih rumit karena memerlukan keahlian khusus dan tindakan cepat	Relatif lebih sederhana karena tidak ada perubahan data
Keamanan dan Integritas Data	Berisiko karena data dapat berubah selama pengumpulan	Lebih aman karena data tidak berubah selama pengumpulan
Aplikasi Utama	Analisis insiden yang membutuhkan data real-time	Analisis insiden yang membutuhkan data dari penyimpanan permanen
Contoh Penggunaan	Investigasi serangan DoS, malware yang aktif	Investigasi pencurian data, pemulihan data yang dihapus

Berdasarkan hasil kajian pustaka di atas, penelitian ini bertujuan untuk melakukan analisis berbasis *dead digital forensic* dengan menggunakan metode NIST untuk memulihkan barang bukti yang dihapus. Metode NIST ini dipilih karena salah satu kerangka kerja standar yang direkomendasikan dan dijadikan sebagai pedoman dalam melakukan digital forensik.Terdapat empat tahapan pada NIST SP 800-86, yaitu pengumpulan, pemeriksaan, analisis, dan pelaporan. Untuk melakukan digital forensik dibutuhkan suatu *tools* dan metode yang mampu membantu proses penemuan barang bukti. Pada penelitian ini digunakan FTK *Imager* dan *Autopsy* untuk melakukan pemulihan terhadap data yang sebelumnya telah dihapus. Keduanya merupakan *tools* forensik yang memiliki peranan masing-masing dalam digital forensik. FTK *Imager* digunakan digunakan pada penelitian sebelumnya untuk melakukan proses *imaging* pada media penyimpanan dengan melakukan pengidentifikasian data yang ada dan pernah ada pada media penyimpanan, selanjutnya akan dilakukan penyalinan data dengan format *image*[17].Sementara itu *Autopsy* membantu penelitian ini dalam mengidentifikasi dan menganalisis *file image* agar dapat dipulihkan kembali seperti yang telah dilakukan oleh penelitian sebelumnya [18]. Untuk media penyimpanan yang akan dijadikan ujicoba *dead forensic* adalah SD *card*, SSD dan HDD.

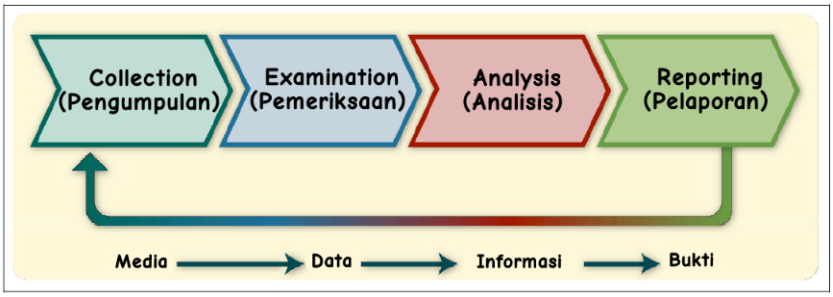
2. Metode Penelitian

Sebagaimana yang telah dijelaskan sebelumnya, penelitian ini menggunakan metode NIST dengan panduan *Special Publication* 800-86 yang memiliki 4 tahapan yaitu pengumpulan (*collection*), pemeriksaan (*examination*), analisis (*analysis*), dan pelaporan (*reporting*). Secara umum empat tahapan penelitian yang dilakukan mulai dari pengumpulan barang bukti sampai pelaporan terhadap bukti yang ditemukan, sehingga dapat menjadikan penelitian lebih terstruktur. Saat melakukan proses forensik, *system* harus dalam keadaan *running off* atau sistem tidak dalam keadaan berjalan sehingga meminimalisir terjadi perubahan atau kerusakan [19]. Untuk keterangan lebih jelas mengenai NIST SP 800-86 dapat dilihat pada Gambar 1.

Pada tahap *collection* (pengumpulan), data yang terkait dengan barang bukti kasus tertentu diidentifikasi kemudian diberi label, direkam, dan dikumpulkan. Barang bukti yang telah diamankan akan diubah dalam bentuk berkas percakapan dengan format raw data menggunakan aplikasi forensik. Untuk menjaga keutuhan dan keaslian barang bukti digital agar tidak terjadi perubahan dan kerusakan perlu dilakukan tindakan kompresi

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

dan hashing, selanjutnya barang bukti akan diduplikasi menjadi *file image* yang disebut dengan proses akuisisi [20]. Setelah proses hashing dilakukan maka barang bukti akan diduplikasi menjadi *file image*, atau bisa disebut dengan proses *imaging*. Kemudian data yang telah dikumpulkan akan diproses ke tahap selanjutnya, yaitu penilaian atau pemeriksaan sesuai kebutuhan dengan tetap mempertahankan integritas data tersebut [21].



Gambar 1. Metode Penelitian berdasarkan NIST [22]

Pada fase kedua, yaitu *examination* (pemeriksaan) alat dan teknik forensik agar sesuai dengan jenis data yang dikumpulkan untuk dilakukan identifikasi dan mengekstrak informasi yang relevan sekaligus melakukan perlindungan terhadap integritasnya. Pemeriksaan dapat dilakukan menggunakan kombinasi alat otomatis dan proses manual. Tahap berikutnya *analysis* (analisis), proses ini melibatkan analisis hasil pemeriksaan untuk memperoleh suatu informasi yang dapat menjawab pertanyaan untuk dijadikan sebagai pendorong dalam melakukan pengumpulan dan pemeriksaan. Fase terakhir merupakan *reporting* (pelaporan) yang melibatkan hasil analisis dan presentase indeks agregatif untuk merepresentasikan tindakan yang perlu dilakukan, dan merekomendasikan perbaikan kebijakan [22].

Untuk mengetahui persentase dari jumlah bukti digital yang didapat, maka perlu dilakukan perhitungan indeks kuantitatif dalam penelitian ini. Semakin besar nilai indeks yang didapat, maka bukti yang berhasil ditemukan pada *harddisk* dan *flashdisk* semakin banyak. Perhitungan ini terbilang sangat sederhana dan mudah dihitung, karena tidak memerlukan faktor yang mempengaruhi naik turunnya angka indeks [23]. Searah dengan itu maka perhitungan indeks kuantitatif digunakan pada penelitian ini dengan Rumus 1 sebagai berikut.

$$I_A = \frac{\sum Q_n}{\sum Q_0} \times 100\% \quad (1)$$

Keterangan.
I_A : Indeks agregatif tidak tertimbang
$\sum Q_n$: Jumlah data hasil akuisisi
$\sum Q_0$: Jumlah data asli

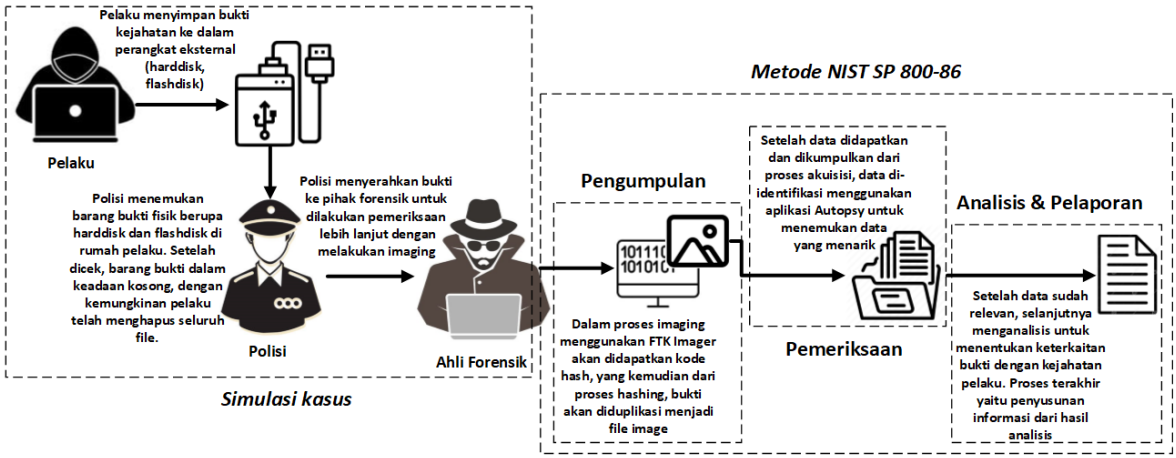
Berdasarkan rumus tersebut dapat dijelaskan bahwa Indeks agregatif tidak tertimbang (I_A) memberikan gambaran tentang efisiensi atau keberhasilan proses akuisisi data dengan membandingkan jumlah data yang diperoleh dengan jumlah data asli. Indeks ini sangat berguna dalam berbagai bidang, termasuk penelitian ilmiah dan analisis data, untuk mengevaluasi kualitas dan integritas proses pengumpulan data. Indeks ini dinyatakan dalam bentuk persentase (%), yang menunjukkan seberapa besar data hasil akuisisi ($\sum Q_n$) dibandingkan dengan data asli ($\sum Q_0$). $\sum Q_n$ adalah jumlah data hasil akuisisi yang merupakan total data yang berhasil dikumpulkan atau diperoleh melalui proses akuisisi. Sementara $\sum Q_0$ adalah jumlah data asli atau total data yang sebenarnya atau yang ada sebelum proses akuisisi.

Selanjutnya, untuk memulai proses digital forensik, perlu dilakukan perancangan penelitian. Adapun proses yang perlu ditetapkan pada penelitian ini berdasarkan kerangka yaitu skenario kasus, objek, metode dan tools yang dipresentasikan pada Gambar 2. Gambar 2 menunjukkan bahwa simulasi kasus merupakan poin utama dalam menentukan metode dan tools yang akan digunakan pada penelitian ini. Kasus yang dipilih merupakan salah satu bentuk kejahatan atas UU ITE yakni carding. Adapun metode yang digunakan yaitu NIST SP 800-86, dimana dalam '*Guide to integrating forensic techniques into incident*' menjelaskan bahwa metode NIST SP 800-86 digunakan untuk membantu dalam melakukan penyelidikan suatu insiden keamanan komputer dan memecahkan beberapa masalah operasional Teknologi Informasi (TI) [22].

Simulasi kasus dilakukan untuk merekontruksi aksi kejahatan yang dilakukan oleh pelaku tindak kriminal terhadap korbannya, dan mempermudah proses investigasi terhadap kasus cyber carding. Simulasi disusun berdasarkan analisis fungsional dari perangkat penyimpanan eksternal dan referensi terkait. Data hasil skenario akan dijadikan sebagai data awal untuk melakukan penelitian, yang kemudian akan dilakukan investigasi

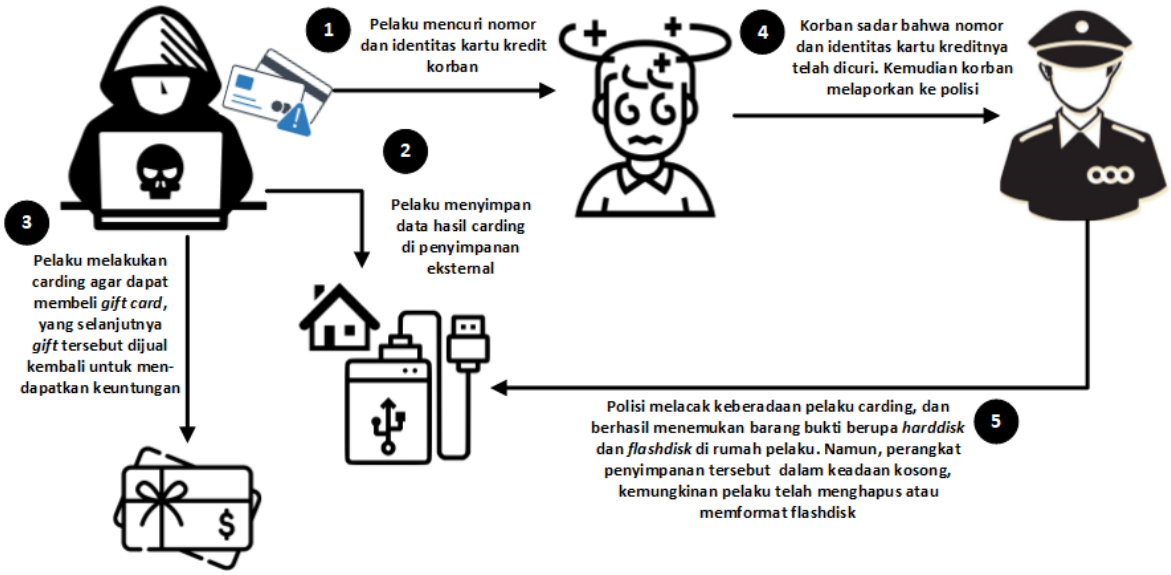
Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

barang bukti melalui proses analisis forensik. Berikut merupakan simulasi kasus yang dipresentasikan pada Gambar 3.



Gambar 2. Rencana Sekenario Simulasi

Objek yang digunakan pada penelitian ini yaitu flashdisk dan harddisk. Pemilihan objek dilakukan dengan berbagai pertimbangan fungsional, dimana flashdisk dan harddisk merupakan media penyimpanan berbentuk portable sehingga memiliki fleksibelitas untuk dibawa kemanapun, dan masih menjadi pilihan utama dalam penyimpanan data atau file. Selain itu, barang bukti elektronik tersebut memiliki potensi digunakan oleh pelaku dalam memperlancar kasus carding, hal ini karena memiliki kapasitas peyimpanan yang besar meskipun fisiknya berukuran kecil sehingga dapat memuat informasi seperti file dokumen, gambar atau foto, video, pesan email, riwayat pencarian, database dan masih banyak lainnya yang dapat dijadikan bukti digital dalam investigasi digital.



Gambar 3. Pelaksanaan Simulasi Kasus

Kasus pada penelitian ini, pelaku melakukan tindakan cybercrime berupa carding, dimana suatu tindakan penipuan atau pencurian nomor dan identitas kartu kredit milik orang lain yang diperoleh secara illegal. Pada umumnya, pencurian nomor dan identitas kartu kredit diperoleh dari website atau aplikasi. Pelaku nekat melakukan carding untuk membeli gift card prabayar, yang nantinya kartu gift tersebut akan dijual kembali supaya pelaku mendapatkan uang, dari tindakan tersebut mengakibatkan korban dirugikan secara materi [24].

Selanjutnya, pelaku menyimpan data hasil carding ke dalam perangkat penyimpanan eksternal, tujuannya agar mudah dibawa kemanapun karena ukurannya yang kecil dan memiliki ruang penyimpanan yang besar. Saat korban telah menyadari bahwa nomor dan identitas kartu kreditnya telah dicuri, korban melaporkan

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

tindakan tersebut ke polisi. Kemudian polisi melakukan investigasi untuk menemukan siapa dan dimana pelaku berada. Setelah polisi berhasil melacak pelaku carding, langkah berikutnya polisi mendatangi lokasi pelaku untuk dilakukan penggeledahan demi mencari barang bukti. Pada proses penggeledahan, ditemukan bukti berupa harddisk dan flashdisk, selanjutnya barang bukti tersebut akan disita untuk dilakukan pemeriksaan.

Setelah dilakukan pemeriksaan terhadap barang bukti yang ditemukan, hasilnya harddisk dan flashdisk dalam keadaan kosong. Diduga pelaku telah menghapus atau memformat bukti tersebut dengan tujuan menghilangkan barang bukti. Dari kejadian tersebut, polisi kemudian menyerahkan barang bukti ke pihak forensik untuk dilakukan recovery data dengan tujuan agar data yang telah dihapus dapat dipulihkan kembali. hal tersebut akan membuat para pelaku tindak kejahatan cybercrime dapat dihukum berdasarkan bukti yang ditemukan dengan mekanisme komputer forensik [25].

Selain itu, pembuatan skenario juga bertujuan sebagai penentu data awal yang akan dianalisis pada penelitian ini. Data yang disebut sebagai artefak (artifacts) merupakan data yang akan dilakukan perbandingan pada jumlah data awal dengan data akhir yang dihasilkan dari proses analisis forensik. Data ini berasal dari perangkat penyimpanan pelaku carding, yakni file dokumen, aplikasi, gambar, dan video. Adapun data yang digunakan untuk analisis digital forensik terdapat pada Tabel 2 berikut ini.

Tabel 2. Data Simulasi

No	Artefak	Jumlah Data Awal
1	Folder	1
2	File .pdf	4
3	File .docx	1
4	File .xlsx	1
5	File .pptx	1
6	Gambar .png	1
7	Gambar .jpg	1
8	Bukti video .mp4	1
9	Aplikasi .apk	1
Total		12

Tabel di atas menunjukkan bahwa terdapat dua belas (12) data dengan sembilan (9) ekstensi berbeda yang disimulasikan sebagai barang bukti. Ekstensi tersebut berupa satu folder, pdf dengan jumlah empat file, docx, xlsx, pptx, png, jpg, mp4, dan apk dengan jumlah masing-masing satu file. Kemudian, alat dan bahan yang digunakan untuk membantu proses investigasi digital forensik. Alat dan bahan yang digunakan harus sesuai dengan standar yang ditentukan oleh pihak hukum agar sah saat dibawa dan dijadikan sebagai bukti dipersidangan. Terdapat beberapa langkah untuk menentukan alat forensik agar dapat menemukan barang bukti digital, yakni:

1. Aplikasi yang digunakan harus sesuai dengan spesifikasi barang bukti
2. Dapat menampilkan keterangan lengkap mengenai file yang telah dihapus oleh pelaku
3. Alat yang digunakan tidak berbayar dan open source.

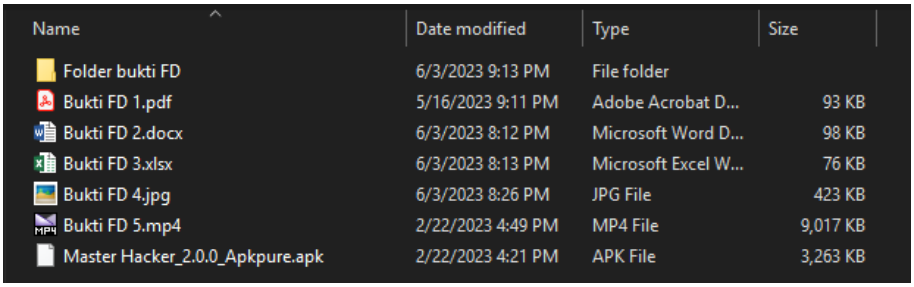
Dengan menggunakan tiga langkah di atas maka dilakukan simulasi sehingga didapatkan software dan hardware yang digunakan pada penelitian ini sebagaimana disampaikan pada Tabel 3.

Tabel 3. *Hardware* dan *Software*

No	Alat dan Bahan	Deskripsi	Detail
1	Laptop	Perangkat yang digunakan untuk proses akuisisi dan analisis *harddisk* dan *flashdisk*	Lenovo ideapad 110, Sistem operasi Windows 10, 64 bit
2	*Flashdisk*	Perangkat yang digunakan sebagai objek penelitian	Vandisk 8 GB dan 4 GB
3	*Harddisk*	Perangkat yang digunakan sebagai objek penelitian	M-TECH, 80 GB
4	Acces Data FTK Imager	Aplikasi yang digunakan untuk melakukan proses akuisisi dan *imaging* data	FTK Imager for windows versi 4.7.2.1
5	Autopsy	Aplikasi yang digunakan untuk analisis hasil imaging	Autopsy for windows versi 4.19.3

Penelitian ini menggunakan tujuh ekstensi file berbeda yaitu folder, pdf, docx, apk, png, xlsx, dan mp4, yang selanjutnya akan diinputkan ke dalam harddisk dan flashdisk, seperti yang tertera pada Gambar 4 berikut ini.

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2



Name	Date modified	Type	Size
Folder bukti FD	6/3/2023 9:13 PM	File folder	
Bukti FD 1.pdf	5/16/2023 9:11 PM	Adobe Acrobat D...	93 KB
Bukti FD 2.docx	6/3/2023 8:12 PM	Microsoft Word D...	98 KB
Bukti FD 3.xlsx	6/3/2023 8:13 PM	Microsoft Excel W...	76 KB
Bukti FD 4.jpg	6/3/2023 8:26 PM	JPG File	423 KB
Bukti FD 5.mp4	2/22/2023 4:49 PM	MP4 File	9,017 KB
Master Hacker_2.0.0_Apkpure.apk	2/22/2023 4:21 PM	APK File	3,263 KB

Gambar 4. File simulasi dalam perangkat penyimpanan

File tersebut disimulasikan sebagai bukti digital terhapus, dimana *file* akan dihilangkan dari media penyimpanan sehingga tidak akan bisa diakses oleh perangkat komputer. Pada proses penghapusan, penulis menggunakan dua (2) metode penghapusan yaitu "**Shift+Delete**" dan "**Format**".

1. **Shift+Delete**
   Metode ini hanya akan menghapus *file* sebanyak satu kali. Meski demikian, *file* akan terhapus secara permanen dari lokasi asalnya tanpa melewati *recycle bin* dan hanya menyisakan bentuk fisiknya saja, sehingga *file* akan sulit untuk dipulihkan kembali.
2. **Format**
   Pada penelitian ini menggunakan pemformatan tingkat *file* (*High-Level Formatting*), dimana seluruh data yang ada dalam media penyimpanan akan terhapus, kemudian secara otomatis struktur dan direktori perangkat penyimpanan akan diatur ulang. Hal ini mengakibatkan bukan hanya referensi *file* saja yang dihapus, namun struktur dan informasi *file* juga akan terhapus.

Proses pengujian digital forensik dilakukan dengan rentan waktu yang berbeda antara tahap penghapusan dan proses akuisisi, hal ini bertujuan untuk mengetahui apakah rentan waktu antara penghapusan permanen dan akuisisi mempengaruhi hasil *recovery* pada *file* yang pernah tersimpan dalam perangkat penyimpanan *harddisk* dan *flashdisk.*

1. Perlakuan pertama, dilakukan penghapusan permanen (Shift+Delete dan Format) seluruh *file* dengan rentan waktu 1 hari antara penghapusan dan proses forensik
2. Perlakuan kedua, dilakukan penghapusan permanen (Shift+Delete dan Format) seluruh *file* dengan rentan waktu 2 minggu antara penghapusan dan proses forensik
3. Perlakuan ketiga, dilakukan penghapusan permanen (Shift+Delete dan Format) seluruh *file* dengan rentan waktu 4 minggu antara penghapusan dan proses forensik
4. Perlakuan keempat, dilakukan penghapusan permanen (Shift+Delete dan Format) seluruh *file* dengan rentan waktu 6 minggu antara penghapusan dan proses forensik
5. Perlakuan kelima, dilakukan penghapusan permanen (Shift+Delete dan Format) seluruh *file* dengan rentan waktu 8 minggu antara penghapusan dan proses forensik

Data yang sudah dihapus masih tersimpan dalam *storage*, hanya saja akses untuk menuju data tersebut dihilangkan karena ruang yang dipakai data tersebut kembali ke *free storage*. Selain itu, data yang sudah dihapus memiliki batas waktu tertentu bertempat di *recycle.*

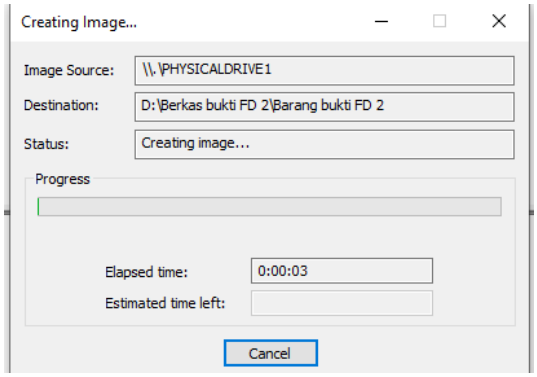
3. Hasil dan Pembahasan

Pengujian barang bukti flashdisk dan harddisk dilakukan sesuai dengan prosedur metode NIST SP 800-86, dimana terdapat empat tahapan pengujian yang akan dijelaskan sebagai berikut.

3.1 Proses Pengumpulan Data

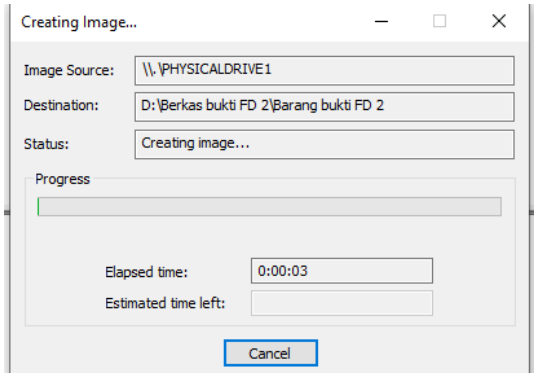
Tahap awal yang perlu dilakukan adalah mengumpulkan barang bukti digital yang tersimpan atau pernah tersimpan pada bukti elektronik dengan melakukan akuisisi data. Pengakuisisian dilakukan dengan cara imaging atau pencitraan, dimana seluruh file yang ada pada flashdisk dan harddisk akan disalin secara physical (sektor per sektor), sehingga akan menghasilkan disk image yang sama dengan bukti secara physical. Tujuan imaging adalah untuk menjaga keaslian barang bukti sampai ke penyidik sehingga dapat dipertanggungjawabkan di pengadilan. Aplikasi yang digunakan untuk melakukan proses imaging adalah FTK Imager. FTK Imager merupakan tool forensik yang dirancang untuk membuat dan melakukan analisis salinan bukti forensik dari media penyimpanan digital. Berikut ini tampilan proses imaging yang disajikan pada Gambar 5.

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2



Gambar 5. Proses Imaging

Pada Gambar 6 menunjukkan hasil dari proses imaging tersebut akan didapatkan file salinan dengan format RAW dari seluruh data yang ada dan pernah ada diperangkat penyimpanan.



Gambar 6. Laporan kode hash

Selain itu, pada proses imaging juga menghasilkan kode hash, dimana kode ini didapatkan dari proses hashing yang dilakukan oleh FTK Imager. Proses hashing dilakukan untuk memastikan bahwa salinan forensik dari media penyimpanan tidak mengalami perubahan ataupun kerusakan selama proses imaging, sehingga salinan dapat dijadikan sebagai barang bukti dan dapat dipertanggungjawabkan keasliannya. Terdapat dua tipe kode hash yang dihasilkan yaitu MD5 dan SHA1. Keduanya merupakan kode hash yang digunakan untuk melakukan validasi file dengan memperhatikan status computed dan report, apabila keduanya match maka data yang disalin masih bersifat original dan tidak mengalami perubahan

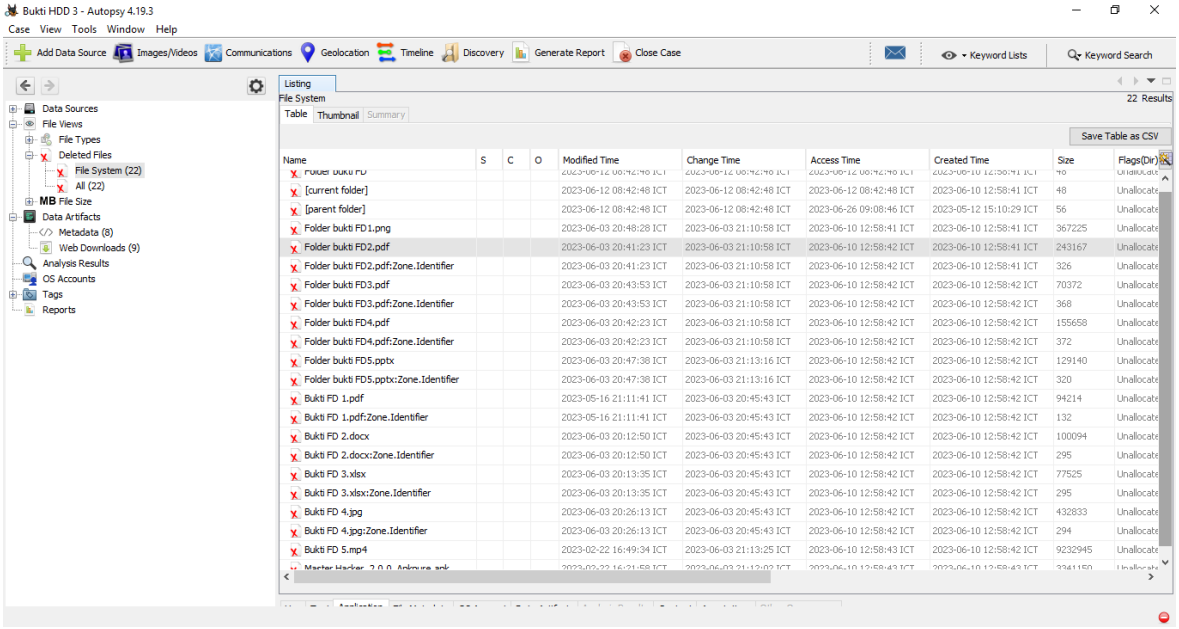
3.2 Proses Pemeriksaan

Setelah melakukan tahapan pengumpulan bukti digital dengan menyalin semua data yang ada di media penyimpanan dengan cara imaging, kemudian dari proses tersebut menghasilkan file salinan dengan format RAW yang akan digunakan pada tahapan analisis. Langkah berikutnya yaitu melakukan pemeriksaan menggunakan aplikasi Autopsy dengan mengimport file imaging, dan secara otomatis sistem akan mengekstrak file salinan tersebut untuk dilakukan visualisasi data dan recovery data yang telah dihapus oleh pelaku. Pemeriksaan dilakukan untuk mengetahui beberapa hal seperti:

1. Data yang berhasil ditemukan, merupakan data pada perangkat harddisk dan flashdisk yang sebelumnya telah dihapus, namun dapat dipulihkan kembali untuk dilakukan pemeriksaan dengan mempertimbangkan jenis data maupun jumlah data.
2. Data yang dapat dibuka, merupakan data pada perangkat harddisk dan flashdisk yang berhasil ditemukan, dengan kondisi data tidak mengalami kerusakan saat dibuka, seperti hilangnya sebagian teks, gambar rusak, corrupt atau kondisi lainnya yang berpengaruh terhadap keutuhan isi dari data.

File image dimasukkan ke dalam aplikasi Autopsy untuk dilakukan parsing pada keseluruhan isi file image, sehingga menghasilkan partisi-partisi yang terstruktur agar dapat dilakukan analisis lebih lanjut untuk mendapatkan informasi yang relevan dengan data forensik. File image yang berhasil diidentifikasi sebagai data source akan menghasilkan beberapa laporan seperti metadata, artefak, timeline activity, dan laporan forensik seperti Gambar 7.

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2



Gambar 7. Hasil pemulihan data

3.3 Proses Analisis

Tahapan analisis merupakan poin penting yang harus dilakukan dalam proses penyelidikan forensik. Bukti digital yang telah berhasil dikumpulkan dan dilakukan pemeriksaan secara menyeluruh, selanjutnya dilakukan analisis dengan melakukan evaluasi dan menafsirkan bukti digital untuk memperoleh informasi mengenai aktivitas yang terjadi pada perangkat harddisk dan flashdisk.

Dalam penelitian ini, proses digital forensik pada perangkat flashdisk dan harddisk dilakukan sebanyak lima (5) kali pengujian dengan jangka waktu yang berbeda disetiap pengujian. Pada pengujian pertama memiliki rentang waktu satu (1) hari antara proses penghapusan dan pemulihan data, pengujian kedua memiliki rentang waktu dua (2) minggu antara proses penghapusan dan pemulihan data, pengujian ketiga memiliki rentang waktu empat (4) minggu antara proses penghapusan dan pemulihan data, pengujian keempat memiliki rentang waktu enam (6) minggu antara proses penghapusan dan pemulihan data, dan pengujian kelima memiliki rentang waktu delapan (8) minggu antara proses penghapusan dan pemulihan data. Namun, yang dijadikan sebagai acuan dasar penelitian ini adalah pada hasil pengujian terakhir yaitu kelima, dimana proses penghapusan dan pemulihan data memiliki rentang waktu delapan (8) minggu. Tabel 4 berikut ini merupakan hasil analisis digital forensik pada flashdisk dan harddisk.

Tabel 4. Hasil pemulihan data

Artefak	Jumlah Data Awal	*Flashdisk* (Shift+Delete)	*Harddisk* (Shift+Delete)	*Flashdisk* (Format)	*Harddisk* (Format)
Folder	1	✓	✓	✗	✗
.pdf	1	✓	✓	✗	✗
.docx	4	✓	✓	✗	✗
.xlsx	1	✓	✓	✗	✗
.pptx	1	✓	✓	✗	✗
.png	1	✓	✓	✗	✗
.jpg	1	✓	✓	✗	✗
.mp4	1	✓	✓	✗	✗
.apk	1	✓	✓	✗	✗
Total	12	12	12	0	0

Saat melakukan pengujian untuk menemukan barang bukti yang ada pada harddisk dan flashdisk dengan perlakuan **Shift+Delete**, aplikasi FTK Imager dan Autopsy dapat menemukan sembilan (9) dari sembilan (9) ekstensi data simulasi dengan total file yang dapat dipulihkan adalah 12, selain itu keseluruhan data yang dipulihkan dapat diakses sehingga bisa dilakukan investigasi terhadap isi konten barang bukti. Sedangkan pada harddisk dan flashdisk dengan perlakuan **Format** tidak berhasil menemukan satupun ekstensi data. Dalam

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

pengujian untuk menemukan jumlah data, FTK Imager dan Autopsy menemukan keseluruhan file dari dua belas (12) file yang digunakan pada harddisk dan flashdisk dengan perlakuan **Shift+Delete**, sedangkan pada harddisk dan flashdisk dengan perlakuan **Format** tidak berhasil menemukan file satupun.

Dalam hal mendapatkan bukti digital pada perangkat harddisk dan flashdisk, baik jenis data maupun jumlah data, aplikasi FTK Imager dan Autopsy mampu mengembalikan data yang dihapus dengan cara Shift+Delete. Hal ini karena pada proses penghapusan data menggunakan Shift+Delete sistem tidak sepenuhnya menghapus data dari media penyimpanan, melainkan hanya dihapus dari indeks file system dan menjadikan ruang yang ditempati oleh file tersebut berstatus "tersedia", yang artinya file sebenarnya masih ada dalam unallocated space, hanya saja jalur untuk mengakses file tersebut sudah tidak ada. Data yang telah dihapus cenderung tidak dapat diakses menggunakan cara biasa, oleh sebab itu untuk mengaksesnya memerlukan alat khusus, yaitu FTK Imager dan Autopsy. FTK Imager akan membaca harddisk dan flashdisk secara bit-for-bit untuk memastikan integritas dan akurasi pada proses pemulihan, sehingga didapatkan salinan isi harddisk dan flashdisk secara lengkap dan identik, termasuk data yang telah dihapus. Dari salinan tersebut, FTK Imager akan melakukan analisis pada file system untuk mengidentifikasi jejak file yang masih tersimpan dalam unallocated space. Selanjutnya, file yang berhasil diidentifikasi akan dipulihkan dan disimpan dalam file image. File image merupakan output dari proses imaging menggunakan FTK Imager yang berisi salinan dari seluruh isi harddisk dan flashdisk, termasuk file yang telah dipulihkan. Selanjutnya file image akan dianalisis menggunakan aplikasi Autopsy untuk pengindeksan seluruh isi file image dengan mencatat informasi mengenai metadata, struktur file, dan konten yang ada di dalam file image. Selain itu, Autopsy juga akan memulihkan data yang dihapus dalam file image dan melakukan analisis untuk mengidentifikasi informasi terkait data yang telah dipulihkan.

Namun untuk data yang dihapus dengan cara diformat, FTK Imager dan Autopsy tidak berhasil dalam melakukan pemulihan data. Hal ini disebabkan seluruh data yang ada di dalamnya akan dihapus dan tidak dapat diakses kembali. Faktor lain, pemformatan secara langsung akan mengatur ulang penyimpanan sehingga ruang yang ada pada harddisk dan flashdisk menjadi kosong, hal ini menyebabkan data yang sebelumnya pernah tersimpan menjadi sulit untuk dipulihkan karena file system, tabel alokasi, dan metadata yang diperlukan dalam identifikasi dan akses file sudah tidak ada lagi. Oleh sebab itu, FTK Imager tidak dapat mengakses, mengidentifikasi, dan menyalin data yang telah diformat pada barang bukti harddisk, dan menjadikan aplikasi Autopsy gagal dalam menganalisis data yang sudah di format.

3.4 Proses Analisis

Pada tahap ini, ahli forensik menyusun laporan terperinci dan lengkap mengenai hasil penyelidikan pada barang bukti harddisk dan flashdisk yang telah dilakukan pada tahap sebelumnya, menggunakan aplikasi FTK Imager untuk melakukan imaging data dan aplikasi Autopsy untuk mengekstraksi dan menganalisis file image. Berdasarkan Tabel 5 didapatkan laporan perbandingan dari hasil pemulihan seluruh data yang telah dihapus dengan beberapa kondisi seperti skenario pengujian, waktu pengujian, dan rata-rata waktu yang dibutuhkan dalam melakukan proses imaging.

Tabel 5. Presentase keberhasilan pemulihan data

Barang Bukti	Pengujian ke-					Rata-rata Kecepatan Proses
	1	2	3	4	5	
Flashdisk (Shift+Delete)	100%	100%	100%	100%	100%	8 - 9 menit
Harddisk (Shift+Delete)	100%	100%	100%	100%	100%	43 menit 40 detik
Flashdisk (Format)	0%	-	-	-	-	9 menit 5 detik
Harddisk (Format)	0%	-	-	-	-	43 menit 50 detik

Pada skenario 1, yakni dengan metode penghapusan dua kali dengan cara Shift+Delete yang dilakukan pada bukti elektronik harddisk dan flashdisk mendapatkan skor indeks agregatif 100% dari mulai pengujian ke-1 sampai ke-5. Maka dapat disimpulkan bahwa data yang dihapus dengan menggunakan fitur Shift+Delete memiliki tingkat akurasi yang tinggi dalam pemulihan, sehingga data yang telah dihapus dapat dikembalikan dan dibuka kembali. Dengan rata-rata waktu yang dibutuhkan untuk menyelesaikan proses imaging yakni 8-9 menit untuk perangkat flashdisk dengan storage 4GB, dan 43 menit 40 detik untuk perangkat harddisk dengan storage 80GB. Kecepatan waktu dipengaruhi oleh besar storage media penyimpanan, semakin besar ukurannya maka waktu yang dibutuhkan untuk menyelesaikan imaging lebih lama.

Pada skenario 2, yakni dengan metode pemformatan pada bukti elektronik harddisk dan flashdisk mendapatkan skor indeks agregatif 0% sejak pengujian ke-1. Maka dapat disimpulkan bahwa data yang dihapus dengan cara pemformatan memiliki tingkat akurasi yang sangat rendah dalam pemulihan, sehingga data yang telah dihapus tidak dapat dikembalikan dan dibuka kembali. Dengan rata-rata waktu yang dibutuhkan untuk

menyelesaikan proses imaging yakni 9 menit 5 detik untuk perangkat flashdisk dengan storage 8GB, dan 43 menit 50 detik untuk perangkat harddisk dengan storage 80GB.

Tabel 5 menunjukkan persentase keberhasilan pemulihan data dari flashdisk dan harddisk yang datanya dihapus dengan dua metode berbeda: menggunakan Shift+Delete dan melalui format. Analisis menunjukkan bahwa pemulihan data dari flashdisk dan harddisk yang dihapus menggunakan Shift+Delete menunjukkan keberhasilan 100% dalam semua pengujian. Sementara pemulihan data dari flashdisk dan harddisk yang dihapus melalui format tidak berhasil (0%). Rata-rata proses pemulihan flashdisk membutuhkan waktu lebih singkat (8-9 menit) dibandingkan harddisk (43 menit 40 detik). Ini menunjukkan bahwa ukuran media penyimpanan dan jumlah data yang tersimpan (lebih besar pada harddisk dibandingkan flashdisk) mempengaruhi waktu pemulihan. Semakin besar ukuran data dan kompleksitas media, semakin lama waktu yang diperlukan untuk pemulihan.

Meskipun pemulihan data yang dihapus melalui format tidak berhasil, waktu yang dibutuhkan untuk menjalankan proses pemulihan pada flashdisk dan harddisk juga menunjukkan perbedaan serupa. Flashdisk memerlukan waktu yang lebih singkat dibandingkan harddisk, yang sekali lagi menunjukkan bahwa ukuran media dan data mempengaruhi waktu pemulihan. Analisis menunjukkan bahwa waktu yang diperlukan untuk pemulihan data memang berkaitan dengan ukuran data yang tersembunyi dan kompleksitas media penyimpanan. Harddisk, dengan kapasitas yang lebih besar dan mungkin lebih banyak data, memerlukan waktu lebih lama untuk proses pemulihan dibandingkan dengan flashdisk yang memiliki kapasitas lebih kecil. Hal ini terlihat jelas dari perbandingan waktu pemulihan antara flashdisk dan harddisk untuk data yang dihapus dengan Shift+Delete maupun melalui format.

4. Kesimpulan

Penelitian ini bertujuan untuk melakukan investigasi bagaimana memulihkan data yang telah dihapus menggunakan metode NIST SP 800-86. Berdasarkan analisis hasil ujicoba menunjukkan bahwa data yang dihapus menggunakan Shift+Delete dapat dipulihkan sepenuhnya, dengan tingkat keberhasilan 100% pada flashdisk dan harddisk. Namun, data yang dihapus melalui Format tidak dapat dipulihkan, menunjukkan bahwa metode penghapusan ini lebih permanen. Selain itu, waktu pemulihan data bervariasi antara jenis media penyimpanan, dimana flashdisk memerlukan waktu yang lebih singkat (8-9 menit) dibandingkan dengan harddisk (43 menit 40 detik) ketika data dihapus menggunakan Shift+Delete. Temuan ini menyoroti pentingnya memilih metode penghapusan data yang sesuai dengan kebutuhan keamanan dan potensi kebutuhan pemulihan di masa depan. Penelitian ini juga menggarisbawahi perlunya pengembangan lebih lanjut dalam teknik forensik digital untuk meningkatkan kemampuan pemulihan data dari media yang telah diformat dan mengurangi waktu pemulihan pada media berkapasitas besar. Rekomendasi utama meliputi penggunaan teknik penghapusan data yang lebih aman, pengembangan alat forensik yang lebih canggih, dan pelatihan yang memadai bagi para profesional di bidang forensik digital. Penelitian ini memberikan kontribusi penting bagi pengembangan metode forensik digital dan pemahaman tentang proses pemulihan data yang telah dihapus.

Daftar Pustaka

[1] M. S. F. Purwani, "Analisis Peran dan Penanggulangan Kejahatan Siber: Studi Kasus Spearphishing," *Restorative: Journal of Indonesian Probation and Parole System*, vol. 1, no. 1, pp. 33–45, 2023, doi: 10.61682/restorative.v1i1.5.

[2] M. F. Hasa, A. Yudhana, and A. Fadlil, "Analisis Bukti Digital pada Storage Secure Digital Card Menggunakan Metode Static Forensic," *Mobile and Forensics*, vol. 1, no. 2, pp. 76–84, 2019, doi: 10.12928/mf.v1i2.1217.

[3] H. Handrizal, "Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete dan Recuva Data Recovery untuk Digital Forensik," *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, vol. 1, no. 1, pp. 84–94, 2017, doi: 10.30645/j-sakti.v1i1.31.

[4] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital pada Frozen Solid State Drive dengan Metode National Institute of Justice (NIJ)," *Elinvo (Electronics, Informatics, and Vocational Education)*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[5] B. S. Santoso and P. M. Sulaksono, "Static Forensic pada USB Mass Storage Menggunakan Forensics Toolkit Imager," *Jurnal Komputer Terapan*, vol. 8, no. 1, pp. 132–142, 2022, doi: 10.35143/jkt.v8i1.5334.

[6] A. Ivanović, "The Way of Handling Evidence of Criminal Offences of Computer Crime," *Criminal Justice and Security in Central and Eastern Europe*, University of Maribor Press: Faculty of Criminal Justice and Security, p. 202, 2018.

[7] M. Y. DM, B. SM, and R. Parlina, "Analisis Kejahatan Carding dalam Bentuk Cyber Crime dan Perlindungan Hukum di Indonesia," *Jurnal Pendidikan dan Konseling (JPDK)*, vol. 4, no. 6, pp. 4203–4209, 2022, doi: 10.31004/jpdk.v4i6.8920.

[8] M. Riskiyadi, "Investigasi Forensik terhadap Bukti Digital dalam Mengungkap Cybercrime," *Cyber Security dan Forensik Digital*, vol. 3, no. 2, pp. 12–21, 2020, doi: 10.14421/csecurity.2020.3.2.2144.

[9] A. Anhar, G. Satrya, and F. Yulianto, "Analisis Perbandingan Keamanan Teknik Penghapusan Data pada Hardisk dengan Metode DoD 5220.22 dan Gutmann," *eProceedings of Engineering*, vol. 1, no. 1, 2014, doi: 10.34818/eoe.v9i5.18452.

[10] R. Ayatulloh, K. N. Bintang, R. Umar, and A. Yudhana, "Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST," vol. 21, no. 2, pp. 125–130, 2020, doi: 10.30595/techno.v21i2.8494.

[11] M. Rifqi, S. J. I. Ismail, and M. F. Rizal, "Analisis Forensik untuk Penanganan Cyber Crime pada Aplikasi Whatsapp Menggunakan Metode National Institute of Standard and Technology (Nist Sp 800-86)," *eProceedings of Applied Science*, vol. 10, no. 6, 2023. [Online]. Available: https://openlibrary.telkomuniversity.ac.id/pustaka/files/200705/jurnal_eproc/analisis-forensik-untuk-penanganan-cyber-crime-pada-aplikasi-whatsapp-menggunakan-metode-national-institute-of-standard-and-technology-nist-sp-800-86-.pdf

[12] D. Hariyadi, M. W. Indriyanto, and M. Habibi, "Investigasi dan Analisis Forensik Digital pada Percakapan Grup Whatsapp Menggunakan NIST SP 800-86 dan Support Vector Machine," *Cyber Security dan Forensik Digital*, vol. 3, no. 2, pp. 34–38, 2020, doi: 10.14421/csecurity.2020.3.2.2193.

[13] R. N. Dasmen, M. R. Pratama, H. Yasir, and A. Budiman, "Analisis Forensik Digital pada Kasus Cyberbullying dengan Metode National Institute of Standard and Technology SP 800-86," *Jurnal Ilmiah Informatika*, vol. 12, no. 01, pp. 68–73, 2024, doi: 10.33884/jif.v12i01.8344.

[14] G. Prakoso and A. K. Heikmakhtiar, "Analisis Keamanan Jaringan: ARP Spoofing dan DNS Spoofing dengan Metode National Institute of Standards and Technology," *Journal on Education*, vol. 6, no. 2, pp. 12895–12902, 2024, doi: 10.31004/joe.v6i2.4872.

[15] D. P. Harahap, "Implementasi Digital Forensik Aplikasi Dompet Digital dan Pesan Instan pada Android dengan Menggunakan Metode NIST," *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, vol. 6, no. 1, pp. 533–541, 2023, doi: 10.30865/komik.v6i1.5715.

[16] C. Asnawi, D. Hariyadi, U. S. Aesyi, and P. W. Cahyo, "Analisis dan Penanganan Insiden Siber SQL Injection Menggunakan Kerangka NIST SP 800-61R2 dan Algoritma Klusterisasi K-Means," *Jurnal Komtika (Komputasi dan Informatika)*, vol. 7, no. 2, pp. 134–144, 2023, doi: 10.31603/komtika.v7i2.10527.

[17] D. S. Yudhistira, I. Riadi, and Y. Prayudi, "Live Forensics Analysis Method for Random Access Memory on Laptop Devices," *International Journal of Computer Science and Information Security*, vol. 16, no. 4, pp. 188–192, 2018.

[18] A. P. Saputra, "Analisis Digital Forensik pada File Steganography (Studi Kasus: Peredaran Narkoba)," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 3, no. 1, 2017, doi: 10.28932/jutisi.v3i1.663.

[19] R. A. Ramadhan, Y. Prayudi, and B. Sugiantoro, "Implementasi dan Analisis Forensika Digital pada Fitur TRIM Solid State Drive," *Teknomatika*, vol. 9, no. 2, p. 13, 2017. [Online]. Available: https://ejournal.unjaya.ac.id/index.php/teknomatika/article/view/466

[20] M. W. Indriyanto, D. Hariyadi, M. Habibi, U. J. Achmad, and Y. Yogyakarta, "Investigasi dan Analisis Forensik Digital pada Percakapan Grup Whatsapp Menggunakan NIST SP 800-86 dan Support Vector Machine", *Cyber Security dan Forensik Digital*, vol. 3, no. 2, pp. 34-38, 2020, doi: 10.14421/csecurity.2020.3.2.2193.

[21] M. M. A. S. Mushlich, M. A. Izzuddin, and M. Ridwan, "Analisis Kinerja Aplikasi Forensik Open-Source pada Ponsel Cerdas Berbasis Android dalam Mendapatkan Bukti Digital," *Jurnal Inovasi Informatika*, vol. 6, no. 2, pp. 86–97, 2021, doi: 10.51170/jii.v6i2.175.

[22] K. Kent, S. Chevalier, T. Grance, and H. Dang, "SP 800-86. Guide to Integrating Forensic Techniques into Incident Response," *National Institute of Standards & Technology*, 2006. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

[23] I. Riadi, "Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST," vol. 7, no. 1, pp. 197–204, 2020, doi: 10.25126/jtiik.202071921.

[24] M. Riskiyadi, "Investigasi Forensik Terhadap Bukti Digital dalam Mengungkap Cybercrime," *Cyber Security dan Forensik Digital*, 2020, doi: 10.14421/csecurity.2020.3.2.2144.

[25] A. Yudhana, U. Ahmad, D. Yogyakarta, I. I. Riadi, and I. F. Ridho, "DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, 2018, doi: 10.14569/IJACSA.2018.091125.