BAB II
TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Pada penelitian yang telah dilakukan Julian & Sutabri (2023) mengkaji fenomena umum kejahatan pencurian data digital, di mana pelaku kerap menghapus berkas untuk menyamarkan aktivitas ilegal, sehingga menuntut adanya teknik pemulihan data yang akurat untuk mendukung proses hukum. Tujuan utama studi ini adalah mengevaluasi kinerja metode NIST SP 800-86 dalam memulihkan data terhapus serta merumuskan pedoman operasional bagi praktisi forensik digital. Metode penelitian mengadopsi kerangka kerja NIST SP 800-86 melalui empat fase prosedural: (1) pengambilan sampel bukti digital (flashdisk terformat), (2) ekstraksi data menggunakan perangkat lunak Autopsy, (3) analisis kritis terhadap data yang berhasil diambil, dan (4) penyusunan laporan hasil investigasi.

Hasil eksperimen menunjukkan bahwa Autopsy mampu memulihkan 81,42% dari total 70 berkas yang dihapus, mencakup beragam format seperti dokumen (DOCX, XLSX, PDF), teks (TXT), audio (MP3), video (MP4), dan gambar (PNG), dengan seluruh data terpulihkan terbukti autentik melalui pemeriksaan integritas berbasis hash. Temuan ini mengonfirmasi bahwa integrasi metode NIST SP 800-86 dan aplikasi Autopsy memberikan solusi terstruktur dan terpercaya dalam pemulihan bukti digital, sehingga memperkuat kapabilitas investigasi forensik dalam menangani tindak pidana cyber.

Dalam penelitian lain yang dilakukan Julian *et al*. (2023) Penelitian ini menyoroti permasalahan yang semakin berkembang dalam ranah kejahatan digital, khususnya kasus pencurian data perusahaan yang membutuhkan proses investigasi guna memperoleh bukti digital yang valid. Sebagai upaya penanganan, penelitian ini mengadopsi metode dari National Institute of Standards and Technology (NIST) yang mencakup empat tahap utama, yaitu proses pengumpulan data, pemeriksaan, analisis, serta pelaporan hasil. Pada

penelitian ini, lima perangkat lunak pemulihan data, yaitu Autopsy, Recuva, Stellar, Puran, dan Easus, diuji untuk mengevaluasi efektivitas masing-masing dalam mengembalikan data yang telah terhapus dari media *flashdisk* yang sebelumnya diformat.

Hasil penelitian menunjukkan bahwa aplikasi Autopsy berhasil mengembalikan 83% dari file yang diuji, sementara Recuva, Puran, dan Easus masing-masing mengembalikan 66%, dan Stellar hanya 33%. Temuan ini menegaskan bahwa Autopsy lebih efektif dalam menemukan dan memulihkan data dibandingkan dengan aplikasi lainnya. Penelitian ini memiliki tingkat relevansi yang tinggi dengan topik analisis bukti digital yang dihapus, karena secara langsung menguji efektivitas berbagai alat dalam mengembalikan data yang hilang akibat tindakan kejahatan digital. Hasil yang diperoleh memberikan wawasan penting bagi praktisi digital forensik dalam memilih alat yang tepat untuk investigasi kejahatan digital.

Dalam penelitian lain yang dilakukan Dasmen *et al*. (2024) membahas permasalahan yang semakin serius terkait meningkatnya kasus cyberbullying di kalangan remaja, di mana pelaku kerap menghapus bukti digital yang umumnya tersimpan dalam media flashdisk. Kondisi ini menjadi tantangan tersendiri dalam proses penyelidikan dan pembuktian hukum, sehingga diperlukan metode yang efektif untuk memperoleh kembali bukti digital yang telah dihapus. Penelitian ini menggunakan metode National Institute of Standards and Technology (NIST) SP 800-86 yang terdiri dari tahapan pengumpulan dan pengamanan barang bukti berupa flashdisk, pemulihan data yang terhapus menggunakan perangkat lunak forensik Autopsy, analisis terhadap data yang berhasil diperoleh, serta penyusunan laporan hasil temuan. Berdasarkan hasil penelitian, Autopsy mampu mengembalikan seluruh data yang dicari dengan tingkat keberhasilan 100 persen dari lima berkas yang terdiri atas empat file berekstensi PNG dan satu file berekstensi MP4. Hasil tersebut membuktikan bahwa metode dan tools yang digunakan efektif dalam proses pemulihan bukti digital yang telah terhapus. Dengan demikian, penelitian ini memberikan kontribusi yang signifikan dalam bidang analisis

forensik digital, khususnya dalam upaya pemulihan bukti dari flashdisk, serta menjadi referensi penting dalam penanganan kasus cyberbullying maupun kejahatan siber lainnya.

Dalam penelitian lain yang dilakukan Shah *et al*. (2022) bertujuan untuk mengidentifikasi data sisa (remnant data) yang masih tersimpan pada perangkat USB flashdisk bekas yang diperoleh dari pasar daring di Selandia Baru. Penelitian ini menggunakan tiga perangkat lunak forensik sumber terbuka, yaitu DC3DD, DCFLDD, dan Guymager, yang dievaluasi berdasarkan pedoman NIST SP 800-86 dan kerangka kerja Computer Forensic Tool Testing (CFTT). Dari 17 flashdisk yang dianalisis, sebanyak 88,23% masih mengandung informasi sensitif seperti foto pribadi, dokumen keuangan, data perusahaan, dan dokumen kontrak. Temuan ini menunjukkan bahwa sebagian besar pengguna belum melakukan penghapusan data secara menyeluruh sebelum menjual perangkat penyimpanan tersebut.

Hasil penelitian juga menunjukkan bahwa perangkat lunak Guymager memiliki kinerja paling cepat dan memenuhi sebagian besar kriteria fungsional berdasarkan standar forensik digital, meskipun penggunaan CPU dan memori lebih tinggi dibandingkan dengan dua perangkat lunak lainnya. Sebaliknya, DCFLDD dinilai kurang optimal karena tidak mampu mencatat log proses secara detail dan menghasilkan nilai hash yang dapat divalidasi dengan baik. Keseluruhan hasil ini menggarisbawahi pentingnya pemahaman terhadap keamanan informasi, khususnya terkait dengan potensi kebocoran data melalui perangkat penyimpanan portabel seperti flashdisk. Oleh karena itu, pendekatan forensik digital menjadi strategi penting dalam mendukung proses investigasi dan pemulihan data yang telah dihapus.

Dalam penelitian lain yang dilakukan oleh Zuo *et al*. (2020) penelitian ini merancang sistem bernama MAGNETO yang berfungsi untuk mengidentifikasi USB flash drive melalui analisis terhadap emisi magnetik tidak disengaja yang muncul saat perangkat terhubung ke komputer. Dalam uji coba terhadap 59 unit USB dari 17 merek ternama, MAGNETO berhasil mengenali merek dan model dengan tingkat akurasi mencapai 98,2%, serta

mampu membedakan perangkat individual dengan akurasi hingga 91,2%, meskipun berasal dari model yang sama. Proses identifikasi berlangsung sangat cepat, yaitu dengan waktu observasi sekitar 1 detik dan pemrosesan sekitar 11,5 milidetik, tanpa perlu mengakses atau mengubah *firmware* dari perangkat tersebut. Untuk mendeteksi emisi magnetik, digunakan alat seperti HackRF One Software Defined Radio (SDR) untuk pengukuran standar dan Rohde & Schwarz FSW8 Spectrum Analyzer untuk akurasi yang lebih tinggi. Seluruh data yang diperoleh dianalisis menggunakan perangkat lunak Matlab R2020a dengan menerapkan algoritma One-Class Support Vector Machine (SVM).

Hasil penelitian menunjukkan bahwa MAGNETO memiliki potensi sebagai sistem keamanan tambahan yang efektif dalam menghadapi ancaman dari USB berbahaya, seperti serangan BadUSB atau perangkat seperti Rubber Ducky. Sistem ini bersifat non-invasif, privat, dan kompatibel dengan perangkat read-only, menjadikannya cocok digunakan di lingkungan dengan standar keamanan tinggi, seperti infrastruktur kritis dan industri. Selain itu, penggunaan alat seperti Aaronia PBS2 EMC Probe untuk menangkap emisi magnetik serta pendekatan analisis berbasis statistik membuat MAGNETO mampu mengidentifikasi perubahan sekecil apa pun pada perangkat, termasuk akibat modifikasi *firmware* atau perbedaan *layout* papan sirkuit (PCB).

Untuk memperkuat landasan teoritis dan metodologis dalam penelitian ini, dilakukan penelaahan terhadap sejumlah penelitian terdahulu yang relevan dengan topik forensik digital dan pemulihan data. Penelitian-penelitian tersebut memberikan referensi penting mengenai pendekatan, teknik, serta hasil yang telah diperoleh oleh peneliti sebelumnya, sehingga dapat digunakan sebagai acuan dalam merancang metode dan skenario pada penelitian ini.

Tabel 2.1 berikut menyajikan ringkasan dari beberapa penelitian terdahulu yang menjadi pijakan dalam penyusunan kerangka penelitian ini. Ringkasan ini mencakup nama peneliti, tahun publikasi, fokus penelitian, metode yang digunakan, serta hasil temuan utama yang diperoleh. Melalui perbandingan tersebut, dapat diketahui posisi dan kontribusi penelitian ini dalam memperluas cakupan kajian yang telah ada.

Tabel 2. 1 Penelitian terdahulu

Judul Penelitian	Penulis	Metode	Kelebihan	Kekurangan	Hasil
Analisa Kinerja Aplikasi Digital Forensik Pengembalian Data Menggunakan Metode NIST SP 800-86	Julian & Sutabri (2023)	NIST SP 800-86 dengan tool Autopsy	Mampu memulihkan 81,42% data terhapus secara autentik dengan verifikasi hash	Belum menguji berbagai skenario penghapusan data	Autopsy efektif untuk pemulihan file .docx, .xlsx, .pdf, .txt, .mp3, .mp4, .png
Perbandingan Kinerja Aplikasi Pengembalian Data Untuk Digital Forensik Dengan Metode National Institute of Standards and Technology	Julian *et al*. (2023)	NIST SP 800-86 dengan Autopsy, Recuva, Stellar, Puran, Easus	Autopsy terbukti paling efektif (83% pemulihan) dibanding tool lain	Tidak menguji faktor waktu pemrosesan	Memberikan insight penting bagi pemilihan tool forensik digital
Analisis Forensik Digital Pada Kasus Cyberbullying dengan Metode National Institute of Standard and Technology SP 800-86	Dasmen *et al*. (2024)	NIST SP 800-86 dengan Autopsy	Tingkat keberhasilan 100% untuk 5 file (4 PNG, 1 MP4)	Skala uji coba kecil (hanya 5 file)	Menunjukkan efektivitas metode NIST dalam kasus cyberbullying
Forensic Investigation of Remnant Data on USB Storage Devices Sold in New Zealand	Shah *et al*. (2022)	NIST SP 800-86 & CFTT dengan DC3DD, DCFLDD, Guymager	Guymager paling cepat dan akurat dalam akuisisi data	DCFLDD kurang dalam log & validasi hash	88,23% flashdisk bekas masih mengandung data sensitif
Fingerprinting USB Flash Drives via Unintentional Magnetic Emissions	Zuo *et al*. (2020)	Identifikasi dengan analisis emisi magnetik (MAGNETO + SVM)	Akurasi tinggi (98,2%) identifikasi merek & model	Bukan metode pemulihan data, hanya identifikasi perangkat	Cocok sebagai sistem keamanan untuk mendeteksi perangkat berbahaya

Berdasarkan ringkasan penelitian terdahulu yang disajikan dalam tabel, dapat diketahui bahwa berbagai studi telah banyak dilakukan terkait implementasi metode digital forensik dalam mengungkap kasus kejahatan siber. Beberapa di antaranya menggunakan pendekatan berbasis metode NIST SP 800-86, serta memanfaatkan tools seperti FTK Imager, Autopsy, atau aplikasi forensik lainnya untuk proses akuisisi dan analisis data. Hasil dari penelitian-penelitian tersebut umumnya menunjukkan bahwa metode forensik digital efektif dalam memulihkan atau mengidentifikasi bukti digital yang telah dihapus.

Namun demikian, sebagian besar penelitian yang telah dikaji masih terbatas pada jenis kasus tertentu atau hanya menerapkan satu skenario metode penghapusan data. Selain itu, belum banyak studi yang secara eksplisit melakukan perbandingan tingkat keberhasilan pemulihan data berdasarkan variasi metode penghapusan seperti *Delete*, *Shift+Delete*, dan *Quick Format* dalam suatu kondisi yang terkontrol dan sistematis.

Sebagai tindak lanjut atas keterbatasan tersebut, kajian ini dirancang untuk menyimulasikan beberapa metode penghapusan data guna mengukur efektivitas pemulihan menggunakan pendekatan NIST SP 800-86. Pendekatan ini memungkinkan pengujian dilakukan secara berlapis dan terstruktur, sehingga hasil yang diperoleh dapat memberikan gambaran yang lebih menyeluruh terhadap performa masing-masing metode dalam konteks forensik digital.

B. Landasan Teori

1. Digital Forensik

Menurut Rachmie (2020) digital forensik adalah cabang ilmu forensik yang digunakan dalam penyelidikan dan investigasi suatu kasus melalui analisis data dan konten yang terdapat pada perangkat digital. Penelitian ini bertujuan untuk mengkaji bagaimana penerapan ilmu digital forensik oleh penyidik dapat mendukung proses identifikasi suatu kasus, dengan tujuan untuk menemukan alat bukti secara cepat dan akurat, serta mengungkap alasan dan motivasi di balik tindakan pelaku

2. Bukti Digital

Menurut Riadi *et al*. (2017) bukti digital merupakan jenis informasi yang sangat rentan, mudah berubah, dan bersifat sementara jika tidak ditangani secara tepat. Keberadaan bukti digital sangat krusial dalam berbagai tindak pidana, tidak hanya terbatas pada kejahatan berbasis komputer. Oleh sebab itu, diperlukan tindakan preventif seperti menjaga perangkat dalam kondisi terisolasi guna mencegah risiko terhapus atau terjadinya perubahan data dalam bentuk apa pun. Bukti digital dapat ditemukan dalam berbagai media penyimpanan seperti hard disk, flashdisk, hingga perangkat seluler. Umumnya, bukti digital berwujud dalam format biner yang memiliki kekuatan hukum dan dapat dipertanggungjawabkan di pengadilan.

Mengacu pada undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), bukti digital dikategorikan sebagai informasi elektronik dan dokumen elektronik. Oleh karena itu, dalam upaya mengungkap suatu tindak pidana yang melibatkan data digital, fokus utama penyidik adalah menemukan, menganalisis, dan meneliti setiap file yang berkaitan secara detail dan terukur.

3. *Flashdisk*

Dalam Rianto & Dozan (2020), Mulyanto menyatakan bahwa flashdisk merupakan perangkat penyimpanan data yang bekerja menggunakan antarmuka USB (Universal Serial Bus) sebagai media penghubungnya. Perangkat ini dirancang secara praktis dan ringan, dengan dimensi sekitar 50 x 15 x 6 mm, bahkan kini ukurannya semakin kecil dengan kapasitas penyimpanan yang jauh lebih besar hingga mencapai 1 terabyte. Flashdisk memanfaatkan teknologi memori flash tipe NAND yang memungkinkan proses baca dan tulis data secara berulang. Selain portabel, perangkat ini juga dikenal memiliki kapasitas penyimpanan yang bervariasi, mulai dari 128 megabyte hingga mencapai 64 gigabyte pada perkembangan awalnya, dan terus meningkat seiring perkembangan teknologi.

4. *Recovery Data*

Menurut Mega (2023) recovery data (pemulihan data) merujuk pada proses mengembalikan data yang hilang atau terhapus dari perangkat penyimpanan seperti *hard drive*, USB drive, atau kartu memori. Data dapat hilang disebabkan oleh berbagai faktor, termasuk kerusakan perangkat keras, serangan virus atau *malware*, kesalahan manusia, atau kegagalan perangkat lunak. Proses pemulihan data dimulai dengan mengidentifikasi penyebab hilangnya data dan menilai apakah data tersebut masih dapat dipulihkan. Namun, tidak semua data dapat dipulihkan, dan proses pemulihan dapat menjadi mahal tergantung pada tingkat kerusakan atau jenis data yang hilang.

5. *Cybercrime*

Menurut Christian et al., (2021) *cybercrime* merupakan bentuk kejahatan yang muncul akibat penyalahgunaan teknologi informasi. Beberapa ahli berpendapat bahwa *cybercrime* identik dengan kejahatan komputer (*computer crime*). Departemen Kehakiman Amerika Serikat (The United States Department of Justice) mendefinisikan kejahatan

komputer sebagai "setiap tindakan ilegal yang memerlukan pengetahuan mengenai teknologi komputer dalam perencanaan, penyelidikan, atau penuntutannya.

6. *Carding*

Menurut Kaimuddin *et al*. (2023) carding adalah praktik berbelanja dengan menggunakan nomor dan identitas kartu kredit orang lain yang diperoleh secara ilegal, biasanya melalui pencurian data di internet. Pelaku dari tindakan ini disebut sebagai carder. Kejahatan ini juga dikenal dengan istilah cyberfraud, yang merujuk pada penipuan di dunia maya. Secara umum, carding bersifat non-kekerasan, meskipun dampak yang ditimbulkannya dapat sangat signifikan. Carding termasuk dalam kategori kejahatan siber berdasarkan aktivitasnya. Salah satu contohnya adalah penggunaan nomor rekening orang lain untuk melakukan pembelian online demi keuntungan pribadi, setelah pelaku (carder) berhasil mencuri informasi rekening dari korban.

7. NIST SP 800-86

Kent *et al*. (2006), menjelaskan bahwa proses forensik digital terdiri dari empat tahapan utama yang saling berkesinambungan, yaitu pengumpulan data (*collection*), pemeriksaan data (*examination*), analisis data (*analysis*), dan pelaporan (*reporting*). Melalui pendekatan ini, pihak terkait dapat menjalankan proses deteksi, penanganan, dan pemulihan insiden keamanan secara lebih sistematis dan efisien. Kent et al. (2006) menjelaskan bahwa diperlukan penetapan kebijakan, prosedur operasional, serta kesiapan sumber daya manusia yang memiliki kompetensi di bidang forensik digital. Kompetensi tersebut mencakup penguasaan terhadap perangkat forensik, pengelolaan data yang bersifat sensitif, serta kemampuan untuk bekerja sama dengan berbagai unit, seperti bidang hukum, keamanan fisik, dan teknologi informasi, agar proses investigasi dapat dilaksanakan secara sah dan dapat dipertanggung jawabkan.

8. *FTK Imager*

Menurut Mega (2023) ftk imager adalah perangkat lunak forensik yang digunakan untuk memperoleh salinan forensik atau gambar dari perangkat penyimpanan data, seperti *hard drive*, USB drive, dan kartu memori. Gambar forensik ini selanjutnya dapat digunakan untuk melakukan analisis forensik terhadap data yang terdapat pada perangkat penyimpanan tersebut. FTK Imager dikembangkan oleh AccessData, sebuah perusahaan yang menyediakan solusi forensik digital dan keamanan informasi. Perangkat lunak ini dapat digunakan oleh para profesional forensik, penyelidik keamanan informasi, atau individu yang ingin memulihkan data yang hilang dari perangkat penyimpanan. Selain itu, FTK Imager juga berfungsi sebagai alat untuk melakukan analisis forensik pada gambar forensik yang telah dibuat.

9. *Autopsy*

Menurut Mega (2023) autopsy adalah perangkat lunak forensik sumber terbuka (*open source*) yang digunakan untuk analisis forensik pada perangkat lunak, perangkat keras, dan data digital. Perangkat lunak ini dikembangkan oleh Basis Technology Corp dan diperbarui secara berkala oleh komunitas pengembang terbuka. Autopsy dapat digunakan pada berbagai sistem operasi, termasuk Windows, Linux, dan MacOS. Perangkat lunak ini sangat bermanfaat bagi para profesional forensik, seperti penegak hukum, tim investigasi keamanan informasi, atau individu yang ingin melakukan analisis forensik pada perangkat lunak atau data digital. Selain itu, Autopsy juga menyediakan berbagai *plugin* yang membantu pengguna untuk memperluas fungsi perangkat lunak sesuai dengan kebutuhan mereka.

10. Perbandingan FTK Imager dan Autopsy

FTK Imager dan Autopsy adalah dua perangkat lunak forensik yang sering digunakan untuk analisis forensik pada data digital. Tabel

2.2 di bawah ini menunjukkan perbandingan antara FTK Imager dan Autopsy secara umum.

Tabel 2. 2 Perbandingan FTK Imager dan Autopsy

Aspek	**FTK Imager**	**Autopsy**
Fitur	lebih menekankan pada proses pengambilan dan pembuatan gambar forensik dari perangkat penyimpanan.	lebih menekankan pada analisis data digital dan dilengkapi dengan fitur pencarian serta visualisasi data yang canggih.
Tampilan	lebih sederhana dan mudah digunakan	lebih kompleks dengan banyak pilihan dan fitur yang lebih banyak
Ketersediaan	*Windows*	*Windows, Linux, dan MacOS*
Penggunaan	Sesuai untuk digunakan oleh para profesional forensik yang telah berpengalaman dengan perangkat lunak forensik.	Mudah digunakan dan dapat digunakan oleh orang yang tidak memiliki latar belakang teknis yang kuat dalam forensik digital