BAB II
TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Ada beberapa penelitian sebelumnya yang dijadikan refrensi bagi penulis antara lain:

Penelitian yang dilakukan oleh (Harahap et al., 2024) penelitian ini membuktikan bahwa semua media sosial rentan terhadap teknik *phishing*. Berbagai halaman dapat dengan mudah di-*cloning* untuk mengelabui pengguna, yang menyebabkan peningkatan insiden penipuan online. *Phishing* sering dilakukan dengan cara yang semakin canggih, membuat banyak pengguna tidak menyadari bahwa mereka sedang menjadi target. Oleh karena itu, diimbau kepada seluruh pengguna media sosial untuk selalu berhati-hati dan memperhatikan URL saat mengakses laman tertentu. Pengguna juga sebaiknya tidak sembarangan membagikan informasi pribadi dan selalu memverifikasi keaslian sumber sebelum memberikan data sensitif.

Penelitian yang dilakukan oleh (Hoiriyah et al., 2016) peneliti memberitahu bahwa Email rentan dan sangat mudah untuk dipalsukan untuk mengelabui korban. Bagian email yang mudah dimanipulasi adalah *header* email, *Field header* yang sering digunakan untuk memanipulasi adalah *From* dan *Date*. Pengalabuan atau pemalsuan ini biasa dikenal dengan istilah *Email Spoofing*. saja. Pendeteksian adanya *Email Spoofing* dapat dilakukan dengan metode header analisis dengan menggunakan *field-field* yang mengandung infomasi yang dibutuhkan seperti *From*, *Message-ID*, *Received*, *Date*.

Penelitian yang dilakukan oleh (Kadam & Hattarge, 2020) Serangan email phishing adalah ancaman yang terus berlanjut bagi masyarakat dan menjadi semakin canggih. Filter spam tidak akan pernah sepenuhnya efektif, jadi tergantung pada masing-masing untuk membaca konteks pesan dan mencari sesuatu yang mencurigakan, oleh karena itu sangat penting bagi Anda untuk mendidik orang untuk memahami dan menganalisis cara kerja phishing dan apa yang harus dilakukan jika mereka menerima email berbahaya.

Penelitian yang dilakukan oleh (Suryana et al., 2016) Email spoofing dapat dikirimkan dengan memanfaatkan layanan web hosting yang menyediakan fasilitas pengiriman email menggunakan Bahasa pemrograman PHP. Email spoofing dapat dikirimkan pada semua layanan email yang dominan digunakan, seperti gmail, yahoo mail, outlook atau hotmail dan mail.com.

Penelitian yang dilakukan oleh (Primukti et al., 2025) berfokus pada analisis data yang tersimpan di memori komputer melalui simulasi aktivitas pengguna pada aplikasi TikTok berbasis web. Dalam penelitian ini, peneliti melakukan akuisisi memori (RAM) menggunakan aplikasi FTK Imager untuk mengambil snapshot memori perangkat yang digunakan. Proses dimulai dengan pengguna menyalakan komputer yang terhubung ke internet dan mengakses situs resmi TikTok melalui browser Google Chrome. Setelah berhasil login dan berinteraksi dengan berbagai fitur aplikasi, FTK Imager digunakan untuk menangkap gambar memori, di mana pengguna memilih opsi "Capture Memory" dan menentukan perangkat memori yang akan dianalisis. Selama akuisisi, FTK Imager melakukan hashing pada file hasil akuisisi untuk memastikan integritas data. Hasil dump memori yang dihasilkan kemudian dianalisis menggunakan editor heksadesimal HxD, yang memungkinkan peneliti untuk mencari pola data tertentu, seperti string teks dan metadata, serta mengidentifikasi data sensitif yang mungkin tersembunyi dalam memori, termasuk informasi login dan aktivitas

pengguna. Penelitian ini memberikan wawasan penting tentang metode statis dalam forensik memori, khususnya dalam konteks aplikasi berbasis web.

(Sunde, 2022) melakukan penelitian yang berfokus terhadap objektivitas pemeriksa dan kepastian bukti dalam forensik digital melalui survei terhadap banyak partisi, dalam konteks forensik digital, di mana perangkat digital dapat menyimpan informasi yang pasti untuk investigasi, penting untuk memastikan bahwa proses analisis dilakukan dengan objektivitas dan teliti. Penelitian ini menyoroti beberapa temuan yang menunjukan tentang bagaimana para praktisi menangani hipotesis dan informasi kontekstual sebelum dan sesudah analisis. Salah satu temuan penting adalah bahwa 45% dari praktisi yang disurvei tidak memulai analisis dengan hipotesis tidak bersalah. Selain itu, 34% praktik tidak menerapkan teknik untuk mempertahankan objektivitas, dan 38% tidak menggunakan teknik untuk menguji atau mengontrol keandalan bukti. Penelitian ini menggarisbawahi bahwa kesalahan dari analisis forensik sering terjadi dari bias teknik maupun non-teknis, yang dapat mengarah pada kesimpulan yang salah. Pentingnya memastikan dengan menggunakan alat ganda muncul sebagai cara utama untuk memastikan keaslian bukti.penelitian ini menggunakan prinsip bahwa setiap orang dianggap tidak bersalah hingga terbukti sebaliknya. Ini berarti bahwa setidaknya satu hipotesis dibuat oleh para praktisi harus mencakup kemungkinan bahwa orang tersebut tidak bersalah. Meskipun para praktisi menyadari adanya risiko bias dalam analisis mereka, hanya 34% dari mereka yang mengaplikasikan teknik untuk tetap objektif. Temuan ini sangat penting untuk memahami praktik di bidang forensik digital, dan menunjukkan bahwa ada kebutuhan untuk mengembangkan prosedur yang lebih baik dalam mengurangi kesalahan dan meningkatkan manajemen kualitas. Dengan mengetahui cara para praktisi mengelola informasi yang ada dan

menjaga objektivitas serta keaslian selama analisis, penelitian ini memberikan pandangan berharga untuk praktik forensik.

Penelitian yang dilakukan oleh (Santoso & Sulaksono, 2022) Penelitian terdahulu menunjukkan bahwa penerapan metode statis dalam forensik digital, khususnya dalam proses recovery bukti digital, dapat dilakukan secara efektif dengan memanfaatkan framework yang telah terstandarisasi, seperti NIST. Dalam studi tersebut, dilakukan serangkaian pengujian sebanyak 20 kali pada setiap perangkat menggunakan alat FTK Imager, yang menghasilkan akurasi recovery bukti digital mencapai 100% pada ketiga perangkat yang diuji. Hasil ini menunjukkan bahwa kombinasi antara metode statis, framework yang tepat, dan alat yang sesuai sangat direkomendasikan untuk digunakan dalam pemeriksaan kasus-kasus yang berkaitan dengan forensik digital, terutama dalam konteks pemulihan bukti digital. Penelitian ini menegaskan pentingnya pendekatan sistematis dalam forensik digital untuk memastikan integritas dan keakuratan data yang diperoleh.

Penelitian yang dilakukan oleh (Alshammari, 2023) Penelitian terdahulu ini mengusulkan model deteksi dan investigasi untuk mendeteksi serangan pada HDD, yang terdiri dari tiga fase: deteksi, pengambilan, dan analisis. Dalam fase deteksi, FTK Imager digunakan untuk mengidentifikasi bukti serangan dengan mengakuisisi data dari HDD, seperti nama volume dan jumlah sektor. Jika terdapat ketidaksesuaian, ini menunjukkan kemungkinan adanya perusakan pada HDD. Pada fase pengambilan, FTK Imager dan HashMyFiles digunakan untuk menangkap bukti yang relevan. Fase analisis kemudian memanfaatkan FTK Imager untuk memeriksa bukti dan memberikan informasi tentang jenis serangan, metode yang digunakan, dan tersangka. Penelitian ini menunjukkan bahwa model yang diusulkan efektif dalam mendeteksi dan menganalisis serangan HDD, serta memberikan keuntungan bagi organisasi dalam pencegahan dan mitigasi serangan.

Penelitian ini menegaskan pentingnya pendekatan sistematis dalam forensik digital untuk mengidentifikasi dan menangani serangan HDD secara efektif.

(Agustiono et al., 2024) melakukan penelitian berjudul "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus". Penelitian ini bertujuan untuk menginvestigasi kemampuan metode NIST SP 800-86 dalam memulihkan data yang telah dihapus pada media penyimpanan seperti flashdisk dan harddisk. Hasil penelitian menunjukkan bahwa data yang dihapus menggunakan metode Shift+Delete dapat dipulihkan sepenuhnya dengan tingkat keberhasilan 100%, sementara data yang dihapus melalui metode Format tidak dapat dipulihkan sama sekali. Selain itu, waktu pemulihan juga dipengaruhi oleh jenis media penyimpanan: flashdisk memerlukan waktu lebih singkat dibandingkan harddisk. Temuan ini menyoroti efektivitas metode NIST dalam forensik statis serta pentingnya pengembangan alat dan teknik forensik yang lebih lanjut untuk pemulihan data yang telah diformat dan media berkapasitas besar. Penelitian ini memberikan kontribusi penting dalam memahami peran metode forensik digital dalam konteks penghapusan data.

Penelitian yang dilakukan oleh (Julian & Sutabri, 2023) menganalisis efektivitas penggunaan metode NIST SP 800-86 dalam proses digital forensik, khususnya untuk memulihkan data yang dihapus pada kasus pencurian data melalui media flashdisk. Penelitian ini menggunakan aplikasi Autopsy sebagai alat bantu utama dalam proses pemulihan data. Dari total 70 berkas yang disimulasikan sebagai bukti digital yang dihapus, Autopsy berhasil memulihkan sebanyak 57 berkas, yang terdiri dari berbagai jenis file seperti DOCX, XLSX, PDF, TXT, MP3, MP4, dan PNG. Hal ini menunjukkan tingkat keberhasilan sebesar 81,42% dalam proses pemulihan. Penelitian ini juga menyoroti keunggulan Autopsy sebagai aplikasi open source yang tidak hanya gratis digunakan, tetapi juga memiliki fitur yang cukup lengkap jika dibandingkan dengan aplikasi sejenis,

sehingga menjadikannya solusi yang layak untuk digunakan dalam analisis forensik digital berbasis metode statis.

Penelitian yang dilakukan oleh (Hamid et al., 2024) menggunakan pendekatan kerangka kerja NIST SP 800-86 dalam melakukan forensic recovery terhadap kasus prostitusi online yang melibatkan komunikasi digital melalui aplikasi WhatsApp. Dalam skenario penelitian, pelaku menghapus berbagai jenis bukti digital seperti pesan teks, gambar, kontak, dan log panggilan. Dengan memanfaatkan tools MobileEdit Forensic dan Oxygen Forensic SQLite Viewer, seluruh artefak digital yang dihapus berhasil dipulihkan dengan tingkat akurasi mencapai 100%. Meskipun hasilnya sangat optimal, peneliti juga menyoroti perlunya pengujian lebih lanjut pada skenario yang lebih kompleks, seperti pemulihan voice note, video, dan dokumen, serta penggunaan perangkat mobile yang berbeda. Penelitian ini menunjukkan efektivitas metode NIST dalam forensik perangkat mobile dan membuka peluang eksplorasi pada metode kerangka kerja forensik lain

B. Landasan Teori

1. Keamanan Siber

   Keamanan siber adalah praktek melindungi sistem, jaringan, program, perangkat, dan data dari serangan digital, akses tidak sah, kerusakan, atau pencurian. Saat ini keamanan siber menjadi salah satu pilar untuk menjaga keamanan dan stabilitas pada bidang ekonomi, ketergantungan terhadap teknologi yang selalu berkembang menjadi salah satu faktor utama dalam keamanan ekonomi dari serangan siber, perkembangan teknologi yang pesat juga memberikan dampak positif untuk mencegah dari serangan siber yang semakin marak dan variatif, sehingga perkembangan teknologi dapat meminimalisir terjadinya phising. (Fadillah et al., 2024)

2. Digital Forensik

Digital forensik adalah cabang ilmu forensik yang berfokus pada identifikasi, pengumpulan, analisis, dan penyajian bukti digital. Bukti digital ini dapat ditemukan di perangkat elektronik seperti komputer, ponsel, atau laptop. Tujuan utama digital forensik adalah untuk mengumpulkan bukti yang sah secara hukum untuk digunakan dalam: Investigasi kriminal, Penyelesaian sengketa hukum, Penyelidikan internal di organisasi, Pemulihan data yang hilang atau dihapus. Digital forensic mencakup berbagai bidang, seperti komputer, perangkat mobile, jaringan, dan media penyimpanan. Bukti-bukti yang dikumpulkan dalam digital forensik dapat berupa email, pesan teks, file dokumen, metadata, dan aktivitas online lainnya. (Ode Muhram, 2025)

Menurut (Hariyadi et al., 2022) , forensik digital adalah bidang ilmu yang berfokus pada pemeriksaan barang bukti elektronik atau digital dengan tujuan mengidentifikasi serta mengungkap fakta sebagai bagian dari Upaya penegakan hukum atau peraturan yang berlaku. Metode ini menggunakan pendekatan ilmiah untuk menginvestigasi bukti digital guna mendukung penyelesaian suatu permasalahan yang kompleks serta memastikan kepatuhan terhadap regulasi yang berlaku.

Menurut (Anabelle et al., 2024) Secara umum, forensik digital adalah teknik yang digunakan untuk menjelaskan kondisi artefak digital pada saat tertentu. Artefak digital ini dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM), dokumen elektronik (misalnya pesan email atau gambar JPEG), atau bahkan paket-paket data yang bergerak secara berurutan dalam suatu jaringan. Bidang forensik digital juga memiliki beberapa cabang, seperti forensik firewall, forensik jaringan, forensik basis data, dan forensik perangkat mobile. Dalam konteks hukum, teknik forensik digital sering digunakan untuk menyelidiki sistem komputer milik terdakwa (dalam kasus pidana) atau tergugat (dalam kasus perdata). Penerapannya meliputi pemulihan data dari perangkat keras atau perangkat lunak yang

mengalami kerusakan, penyelidikan terhadap sistem komputer setelah terjadinya pembobolan, serta analisis untuk mengetahui bagaimana penyerang mendapatkan akses dan jenis serangan yang dilakukan. Selain itu, forensik digital juga dapat digunakan untuk memahami cara kerja sistem komputer dalam rangka debugging maupun optimisasi kinerja.

3. Metode Forensik Digital

Menurut (Hariyadi et al., 2022) ,metode forensik yang sering digunakan dalam forensik digital diantaranya adalah sebagai berikut:

a. *National Institute of Standars and Technology* (NIST) merupakan standar yang digunakan untuk menganalisis barang bukti, salah satunya yang menjadi pedoman yaitu NIST SP 800-86, memberikan petunjuk teknis dalam investigasi forensik digital yang terdiri dari 4 tahapan, yaitu ada *acquisition* (mengidentifikasi, mengumpulkan, dan melindungi data asli), *examination* (menggunakan alat dan Teknik untuk mengidentifikasi informasi relevan), *analysis* (melakukan analisis yang teliti kepada barang bukti serangan), dan terakhir adalah *reporting* (Menyusun laporan investigasi dari seluruh proses kegiatan dan memberikan identifikasi tentang kelemahan dan perbaikan)
b. Standar Nasional Indonesia (SNI) adalah standarisasi forensik digital yang sering digunakan, SNI menggunakan 2 data standarisasi, yaitu SNI ISO/IEC 27037:2014 yang mengatur tata kelola forensik digital dari proses identifikasi, pengumpulan barang bukti elektronik, akuisisi barang bukti digital, dan preservasi, lalu untuk SNI ISO/IEC 27042:2015 mengatur tata Kelola forensik digital seperti analisis dan penyajian laporan.
c. *National Institute of Justice* (NIJ) merupakan sebuah organisasi yang menyediakan pedoman dan standar dalam investigasi forensik digital, metode NIJ memiliki 5 tahapan yang hampir

sama seperti metode lainnya yaitu seperti identification, collection, examination, analysis, dan reporting.

Metode forensik digital lainnya juga masih sering digunakan seperti Association of Chief Police Officers (ACPO), Digital Forensikss Research Workshop (DFRWS), Systematic Digital Forensiks Investigation Model (SRDFIM), Integrated Digital Forensik Investigation Framework (IDFIF), dan Integrated E-mail Forensik Analysis Framework (IEFAF).

4. *Memory Forensics*

Memory forensic adalah bagian dari digital forensik yang fokus pada analisis data volatile yang terdapat dalam Random Access Memory (RAM) sebuah perangkat. Proses ini melibatkan pengambilan "memory dump," yang merupakan snapshot dari memori saat perangkat sedang berjalan, dan menganalisis output tersebut untuk menemukan bukti terkait aktivitas pengguna, malware, atau serangan siber. Memori forensik dapat mengumpulkan data secara real-time yang berkaitan dengan sistem operasi, serta mengekstraksi berbagai jenis informasi dari memori, termasuk proses memori, image identification, networking, registry, dll. (Primukti et al., 2025)

5. Email

Menurut (Rahma & Riadi, 2022) surat Elektronik, atau email, merupakan layanan internet yang sangat populer dan sering digunakan oleh banyak orang, baik di dalam organisasi maupun perusahaan. Dalam bentuknya yang paling sederhana, email adalah metode untuk mengirim, menerima, dan menyimpan pesan melalui sistem komunikasi elektronik, khususnya internet. Definisi ini menjelaskan bahwa surat elektronik ditulis, dikirim, dan diterima secara elektronik .

6. *Phising*

Phising merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara

tidak langsung memberikan semua informasi yang dibutuhkan oleh sang penjebak. Phishing termasuk dalam kejahatan cyber crime, dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer. Seiring perkembangan zaman, tindak kriminal juga semakin merebak di seluruh dunia. Sehingga ancaman yang banyak terjadi saat ini juga melalui komputer.(Dm et al., 2022)

7. *Email Spoofing*

   Email Spoofing merupakan salah satu media untuk melakukan penyebaran tautan yang berisikan website phising yang akan diakses oleh korban. Untuk melakukan *Email Spoofing* penyerang memerlukan alamat email atau server yang dapat digunakan sebagai media serangan. Setelah memiliki alamat email atau server penyerang diharuskan memiliki template email yang dapat menyakinkan bahwa korban merasa harus membuka link phising tersebut. Setelah itu penyerang diharuskan memiliki daftar email yang akan dijadikan korban penyerangan *Email Spoofing*. (Ansyafa et al., 2024)

8. Volatility

   Menurut (Nyholm et al., 2022) dalam membahas alat forensik memori volatil, tidak mungkin mengabaikan Volatility—sebuah kerangka kerja sumber terbuka berbasis Python untuk menganalisis *memory dumps* . Volatility mampu menganalisis *memory dumps* dari mesin Windows, Linux, atau Macintosh, mendukung berbagai jenis format file dump, dan memiliki antarmuka pemrograman aplikasi (API) yang dapat diperluas. Kerangka kerja ini juga memiliki fungsionalitas penciptaan fitur yang sangat baik serta efisiensi implementasi yang cukup baik.

   Volatility telah berkembang menjadi kerangka kerja terbesar dan paling didukung karena basis kontributor yang luas serta plugin-plugin yang ditulis secara independen, banyak di antaranya dirancang untuk forensik yang spesifik terhadap platform tertentu . Kerangka kerja ini, bersama banyak plugin-nya—terutama yang digunakan untuk

menganalisis sistem Windows—telah cukup matang dan stabil untuk dapat lolos dari pengujian *fuzz testing*.

9. *Metode Forensics*

   Metode statis bisa disebut juga Dead Forensics, merupakan salah satu jenis metode dari forensik digital yang memperoleh bukti digital dengan melakukan ekstraksi serta analisis setelah insiden terjadi. Sedangkan menurut Mamoona , *static forensics* merupakan pendekatan secara tradisional untuk melakukan proses forensic setelah diperolehnya *dump memory* pada sistem. (Santoso & Sulaksono, 2022).

10. Mitigasi

    Mitigasi TI menekankan pada tindakan awal dalam suatu proyek untuk mencegah terjadinya kejadian yang tidak diinginkan atau mengurangi konsekuensi dari kejadian tersebut. (Farmadika et al., 2024)