

BAB II

TINJAUAN PUSTAKA

2.1 Studi Literatur

Forensik digital adalah bidang keilmuan yang berfokus pada teknik pengumpulan, analisis, dan pelaporan bukti yang diperoleh dari perangkat elektronik. Bidang ini mencakup berbagai kegiatan, seperti pemulihan data yang terhapus dan analisis jejak digital yang ditinggalkan oleh pengguna[16]. Forensik digital memiliki peran yang sangat penting dalam penyelidikan kejahatan siber, karena dapat mendukung kinerja lembaga penegak hukum dalam mengidentifikasi pelaku dan menguatkan bukti tindak pidana yang dilakukan. Selain itu, aspek hukum juga sangat krusial dalam forensik digital, karena bukti yang ditemukan harus sesuai dengan standar hukum agar dapat diterima di pengadilan[17].

Metode NIST 800-86 adalah pedoman yang dikeluarkan oleh National Institute of Standards and Technology untuk mendukung proses investigasi forensik digital. Penerapan metode ini difokuskan pada upaya untuk memastikan bahwa setiap tahapan pengumpulan dan analisis bukti digital dilakukan secara sistematis dan dapat dipertanggungjawabkan. Panduan ini menguraikan tahapan penting seperti *Collection, Examination, Analysis, dan Reporting*, yang masing-masing memiliki prosedur dan tujuan yang jelas [15]. Manfaat utama dari metode NIST 800-86 adalah meningkatkan kredibilitas dan keabsahan bukti digital, meskipun terdapat tantangan, seperti keterbatasan alat forensik dan kompleksitas data yang harus dianalisis [1].

Instagram dan Telegram merupakan dua aplikasi sarana berinteraksi yang umum digunakan di lingkungan pengguna internet. Kedua platform ini banyak digunakan untuk berbagi informasi, namun tidak jarang dimanfaatkan untuk kegiatan ilegal. Proses pengumpulan bukti digital dari Instagram dan Telegram memerlukan teknik forensik yang tepat, seperti live forensics dan analisis terhadap data yang tersimpan [18]. Tantangan utama dalam memperoleh bukti forensik dari aplikasi ini adalah adanya enkripsi data dan kemungkinan penghapusan pesan oleh pengguna, yang dapat menghambat kelancaran investigasi [11].

Sejumlah penelitian telah membahas penerapan forensik digital pada Instagram dan Telegram. Beberapa studi menunjukkan bahwa Instagram sering kali lebih efektif dalam memulihkan bukti digital dibandingkan Telegram, dengan tingkat keberhasilan yang lebih tinggi dalam mengakses data yang telah dihapus [19]. Beberapa kasus penipuan yang melibatkan Instagram dan Telegram sebagai sarana komunikasi juga telah dianalisis, memperlihatkan bagaimana kedua platform ini dapat digunakan untuk kegiatan kriminal. Penelitian-penelitian sebelumnya menekankan pentingnya penggunaan alat forensik yang tepat serta penerapan metode NIST untuk memperbaiki hasil investigasi [3]. Tabel 2.1 memuat ringkasan hasil dari sejumlah penelitian sebelumnya.

Tabel 2.1 Refrensi Terdahulu

No	Judul Penelitian	Hasil Penelitian	Metode	No. Kutipan
1	Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus	Penelitian ini mengkaji pemulihan data yang dihapus menggunakan metode NIST SP 800-86. Hasil uji coba menunjukkan bahwa data yang dihapus dengan Shift+Delete dapat dipulihkan sepenuhnya (100% berhasil) pada flashdisk dan harddisk, sementara data yang dihapus melalui Format tidak dapat dipulihkan. Waktu pemulihan bervariasi, dengan flashdisk memerlukan 8-9 menit dan harddisk 43 menit 40 detik. Temuan ini menekankan pentingnya memilih metode	NIST 800-86	[13]

		penghapusan yang tepat dan perlunya pengembangan teknik forensik digital untuk pemulihan data dan efisiensi pada media besar.		
2	Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86	Penelitian ini menganalisis forensik digital pada aplikasi Instagram dan TikTok menggunakan metode NIST 800-86 untuk memperoleh bukti digital dengan memanfaatkan berbagai tools forensik. Pada Instagram, <i>MOBILedit Forensic Express</i> berhasil mengidentifikasi 1 bukti dari 45 data awal (0,02%), Autopsy menemukan 12 bukti (26%), dan FTK <i>Imager</i> memperoleh 26 bukti (56%). Sedangkan pada TikTok, <i>MOBILedit Forensic Express</i> menemukan 1 bukti dari 37 data awal (0,02%), Autopsy berhasil mengidentifikasi 11 bukti (29%), dan FTK <i>Imager</i> memperoleh 27 bukti (71%).	NIST 800-86	[1]
3	Analisis dan investigasi forensik aplikasi instagram dan threads dalam	Penelitian ini menganalisis forensik digital mengenai konten dan postingan pornografi di Instagram dan	NIST 800-86	[15]

	mendapatkan bukti digital menggunakan metode nist 800-86	Threads menggunakan alat forensik seperti FTK <i>Imager</i> , Autopsy, dan <i>MOBILedit Forensic</i> menemukan 1 akun pengguna, 18 riwayat penelusuran kata kunci, 43 thumbnail yang diduga postingan, dan 846 file gambar. Proses dengan FTK <i>Imager</i> memakan waktu sekitar 16 menit, Autopsy membutuhkan 7 menit, dan <i>MOBILedit Forensic</i> hanya sekitar 6 menit. Dari segi akurasi, FTK <i>Imager</i> memiliki akurasi 0,09%, Autopsy 81%, dan <i>MOBILedit Forensic</i> 21%.		
4	Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada <i>Smartphone</i> Android Menggunakan Metode NIJ	Penelitian forensik pada aplikasi Facebook Messenger di perangkat Android menemukan bukti berupa akun, percakapan, dan gambar terkait kasus perdagangan liquid vape narkoba. Menggunakan metode NIJ dan alat forensik, bukti digital berhasil diekstrak dari perangkat Samsung Galaxy V+ SM-G318HZ dan Galaxy Trend Plus GT-S7580. <i>MOBILedit Forensic Express</i> dan <i>Magnet AXIOM</i> masing-masing	NIJ	[12]

		<p>berhasil mengekstrak 2 akun, 11 chat, dan 26 gambar dengan akurasi 100% untuk akun, 55% untuk chat, dan 86% untuk gambar. Sedangkan <i>Oxygen Forensic Suite 2014</i> hanya berhasil mengekstrak 2 akun, 1 chat, dan 26 gambar, dengan akurasi rendah untuk chat (5%). Hasil ini menunjukkan bahwa <i>MOBILedit Forensic Express</i> dan <i>Magnet AXIOM</i> lebih efektif dibandingkan <i>Oxygen Forensic Suite 2014</i> dalam ekstraksi bukti digital pada Facebook Messenger.</p>		
5	<p>Analisis Digital Forensik Recovery Data pada Flashdisk Menggunakan Metode <i>National Institute Of Justice</i> (NIJ)</p>	<p>Penelitian ini menyimpulkan bahwa <i>TestDisk</i> merupakan alat forensik yang sangat efektif dalam memulihkan file yang hilang atau terhapus, dengan tingkat keberhasilan 100% dalam menemukan bukti digital, seperti rekaman CCTV pelaku pencurian. Penulis menyarankan agar penelitian selanjutnya lebih spesifik dan mengembangkan aspek-aspek yang relevan, meskipun masih banyak kekurangan dalam penelitian ini. Disarankan</p>	NIJ	[20]

		untuk menggunakan alat forensik dengan hati-hati agar tidak merugikan pihak manapun.		
--	--	--	--	--

2.2 Digital Forensik

2.2.1 Pengertian Digital Forensik

Digital forensik merupakan bidang keilmuan yang konsentrasinya berada pada proses identifikasi, pengumpulan, analisis, serta pelaporan bukti elektronik dalam berbagai perangkat digital. Tujuan utama dari bidang ini adalah untuk mendukung investigasi hukum dengan memastikan bahwa bukti yang diperoleh tetap utuh, dapat diverifikasi, dan memenuhi standar yang dapat diterima dalam proses peradilan. Dalam praktiknya, digital forensik banyak digunakan dalam penyelidikan kasus kejahatan siber, pencurian data, hingga pelanggaran kebijakan perusahaan [21].

Sebagai bidang ilmu yang mengandalkan metode ilmiah, digital forensik mencakup berbagai teknik untuk menelusuri jejak digital yang tersimpan dalam komputer, perangkat seluler, jaringan, serta sistem penyimpanan berbasis cloud. Proses forensik ini melibatkan analisis metadata, pemulihan data yang telah dihapus, serta rekonstruksi aktivitas pengguna dalam mendapatkan gambaran yang lebih jelas mengenai suatu kejadian. Agar hasil investigasi dapat digunakan sebagai barang bukti, metode yang digunakan harus sesuai dengan standar forensik yang diakui secara internasional [22].

Dalam ranah hukum, digital forensik memainkan peran krusial dalam membantu aparat penegak hukum mengungkap berbagai kasus yang melibatkan teknologi informasi seperti penipuan daring, peretasan, serta penyampaian pesan bernada kebencian di ranah media sosial. Dengan menggunakan teknik forensik digital, penyidik dapat menelusuri asal-usul komunikasi, mengidentifikasi pemilik akun, serta membuktikan keterlibatan individu dalam suatu tindakan melanggar hukum. Keakuratan dan keabsahan

data yang diperoleh melalui digital forensik menjadikannya alat yang sangat penting dalam menangani kejahatan berbasis teknologi [23].

2.2.2 Tujuan Digital Forensik

Tujuan utama penggunaan digital forensik adalah untuk memperkuat proses peradilan dengan menyediakan data elektronik yang kredibel dan layak untuk disajikan dan diterima dalam persidangan. Dalam investigasi kriminal, keakuratan bukti menjadi faktor kunci dalam mengungkap fakta dan memastikan keadilan [21]. Digital forensik berperan dalam mengumpulkan, mengamankan, serta menganalisis data yang relevan dalam memastikan bahwa kebenaran materiil dari suatu kasus dapat terungkap. Dengan adanya metode forensik yang tepat, proses hukum dapat berjalan lebih efektif dan transparan [22].

Forensik digital memiliki tujuan utama dalam mengumpulkan serta menganalisis data elektronik yang berhubungan dengan tindak kejahatan, sehingga dapat menghadirkan bukti yang valid dan dapat dipertanggungjawabkan dalam proses peradilan. Peran forensik digital dalam mengungkap kasus seperti penipuan, penyebaran konten ilegal dan kejahatan dunia maya semakin krusial, terutama seiring dengan meningkatnya aktivitas pengguna di berbagai platform media sosial seperti Instagram dan Telegram [11].

2.3 Metode NIST 800-86

Proses memperoleh informasi dari bukti digital dilakukan dengan menerapkan metode (*National Institute of Standards and Technology*) NIST. Langkah awal dimulai dengan pemeriksaan terhadap data yang telah dikumpulkan, kemudian mengekstrak data dari media penyimpanan dan mengonversinya ke dalam format yang kompatibel dengan perangkat lunak forensik. Selanjutnya, data yang telah diekstrak dianalisis untuk mengubahnya menjadi informasi yang sesuai terhadap kebutuhan. Tahap akhir melibatkan transformasi informasi tersebut menjadi bukti yang dapat digunakan dalam penyelidikan, di mana hasil analisis disajikan ke dalam tindakan yang sesuai selama proses pelaporan [12].

Metode (*National Institute of Standards and Technology*) NIST terdiri dari 4 tahapan yaitu *Collection, Examination, Analysis, Reporting* yang akan dijelaskan sebagai berikut:

1. *Collection*

Tahap ini berfokus pada identifikasi, pengumpulan, dan akuisisi bukti digital. Perangkat keras yang berisi data terkait suatu kasus kejahatan digital dikumpulkan untuk dianalisis lebih lanjut. Selama proses ini, setiap langkah harus dilakukan dengan cermat untuk menjaga integritas data agar tetap utuh dan dapat digunakan dalam investigasi selanjutnya [9].

2. *Examination*

Examination adalah proses mengekstrak data dari barang bukti menggunakan perangkat lunak forensik yang terpercaya. Tahap ini bertujuan untuk memastikan bahwa data yang diperoleh tetap akurat, utuh, dan dapat dipertanggungjawabkan dalam investigasi [15].

3. *Analysis*

Tahapan ini berfokus pada pengolahan data yang sebelumnya telah dikumpulkan dan diperiksa akan dianalisis secara mendalam. Evaluasi dilakukan untuk menemukan pola, hubungan, dan informasi penting yang dapat mendukung proses penyelidikan lebih lanjut [18].

4. *Reporting*

Tahap terakhir dalam metode ini adalah pembuatan laporan berdasarkan hasil analisis. Laporan ini mencakup temuan utama dari investigasi, data yang berhasil diperoleh, serta kesimpulan yang dapat digunakan sebagai bukti dalam proses hukum atau penyelidikan lebih lanjut [24].

2.4 Tools Digital Forensik

Tools digital forensik berperan penting dalam mengumpulkan, menganalisis, dan memvalidasi bukti dalam investigasi kejahatan siber. Pemilihan alat yang tepat sangat krusial untuk memastikan keakuratan dan keandalan data. Beberapa tools yang umum digunakan meliputi *FTK Imager, Autopsy, dan MOBILedit Forensic Express*, yang masing-masing memiliki fungsi spesifik dalam proses investigasi.

Dengan menggunakan tools ini, penyidik dapat memperoleh bukti digital secara efisien dan memastikan integritas data tetap terjaga [25].

1. *Autopsy*

Autopsy sebagai aplikasi forensik digital yang digunakan sebagai alat untuk mengakses, memeriksa, serta mengorganisir bukti digital dalam proses investigasi kejahatan siber. Perangkat ini membantu penyidik dalam mengekstrak informasi penting dari berbagai sumber, termasuk file yang dihapus, metadata, dan aktivitas sistem, sehingga mempermudah proses penyelidikan [15].

2. *FTK Imager*

FTK Imager merupakan perangkat lunak forensik yang digunakan untuk menganalisis hard drive dan mengidentifikasi berbagai jenis data, termasuk email yang telah dihapus serta teks yang dienkripsi. Selain itu, *FTK Imager* juga dilengkapi dengan fitur imaging yang memungkinkan pembuatan salinan forensik dari hard drive untuk keperluan investigasi [25].

3. *MOBILedit Forensic Express*

MOBILedit Forensic Express salah satu aplikasi berbasis Windows yang dirancang untuk mengakses, mengumpulkan, dan menganalisis data dari perangkat seluler. Perangkat lunak ini memungkinkan penyidik mengekstrak bukti digital dari *smartphone*, seperti pesan teks, log panggilan, kontak, serta data lainnya yang relevan dengan kasus kejahatan digital, sehingga mendukung proses investigasi secara menyeluruh [18].

2.5 Media Sosial

Media sosial merupakan layanan berbasis internet yang menyediakan platform bagi pengguna untuk terhubung, berinteraksi secara sosial, dan berinteraksi tanpa terhalang oleh jarak geografis atau batasan waktu. Pesatnya perkembangan media sosial tidak hanya terjadi di negara maju, tetapi juga di negara berkembang seperti Indonesia, di mana jumlah pengguna media sosial terus meningkat setiap tahunnya. Kemudahan akses internet dan perkembangan teknologi telah mendorong

masyarakat untuk semakin aktif dalam menggunakan berbagai platform media sosial [26].

Dalam digital forensik, media sosial menjadi sumber utama untuk mengumpulkan, menganalisis, dan menyimpan berbagai data digital, seperti informasi pengguna, foto, video, serta bukti elektronik lainnya. Data yang tersedia secara publik dapat dimanfaatkan untuk mengidentifikasi pelaku kejahatan atau mengungkap suatu kasus, meskipun akses terhadap informasi lebih mendalam sering kali memerlukan izin resmi, seperti panggilan pengadilan. Meskipun demikian, informasi yang telah dipublikasikan secara terbuka tetap menjadi aset berharga dalam investigasi, karena dapat memberikan petunjuk penting yang membantu penyelidik dalam merangkai kronologi kejadian dan mengungkap fakta yang relevan [15].

1. Aplikasi Instagram

Instagram adalah salah satu layanan jejaring sosial yang sangat populer dan digunakan di seluruh dunia, terutama diminati oleh kalangan muda. Di platform ini pengguna dapat berbagi foto dan video serta berinteraksi secara sosial dengan orang lain melalui berbagai fitur yang disediakan. Fitur utama seperti "*Feeds*" digunakan untuk membagikan konten secara permanen, sementara "*Instastory*" memungkinkan unggahan yang tersedia dalam rentang waktu 24 jam. Selain itu, terdapat "*IGTV*" untuk mengunggah video berdurasi lebih panjang dan "*Reels*" yang memungkinkan pembuatan video pendek hingga 15 detik, memberikan ruang bagi pengguna untuk menampilkan kreativitas mereka. Dengan beragam fitur yang ditawarkan, Instagram tidak hanya menjadi sarana berbagi momen pribadi, tetapi juga alat untuk interaksi sosial, komunikasi, serta pembelajaran, sehingga menjadikannya platform yang multifungsi dalam kehidupan sehari-hari [27].

2. Aplikasi Telegram

Telegram sendiri sebagai aplikasi pesan instan berbasis cloud dan open source yang memungkinkan pengguna mengirim pesan, foto, video, serta

dokumen berukuran besar secara gratis. Salah satu keunggulannya adalah kemampuan mengirim file hingga 1,5 GB per file, lebih besar dibandingkan aplikasi sejenis. Selain itu, fitur "Channel" memungkinkan penyebaran informasi ke banyak orang, sementara "Group Chat" dapat menampung hingga 200.000 anggota, menjadikannya ideal untuk diskusi dan kolaborasi dalam skala besar. Telegram juga menawarkan fitur "Bot" untuk berbagai keperluan otomatisasi, seperti pengingat dan berita, serta menyediakan keamanan tinggi dengan enkripsi end-to-end untuk percakapan rahasia. Dengan beragam fitur ini, Telegram selain berperan sebagai aplikasi komunikasi instan, platform ini juga sebagai media komunikasi yang mendukung efisiensi, privasi, dan kolaborasi [28].

