BAB II
TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Pada penelitian yang telah dilakukan oleh (Yudhana et al., 2018) telah melakukan skenario penelitian dengan menggunakan Smartphone Galaxy V+ SM- G31HZ. Skenario tersebut melibatkan proses rooting, instalasi aplikasi Facebook Messenger, pembuatan pesan, dan kemudian melakukan investigasi menggunakan alat forensik bernama Oxygen Forensic. Setelah itu, dilakukan analisis menggunakan ketiga perangkat lunak forensik tersebut, dan hasil analisis akan dilaporkan sebagai barang bukti. Metode yang digunakan dalam penelitian ini untuk menganalisis bukti digital adalah metode NIST (National Institute of Standards and Technology). Hasil yang telah diperoleh dari penelitian ini mencakup teks percakapan, gambar, dan audio. Dalam konteks penelitian ini, teks percakapan merujuk pada pesan-pesan yang dikirim melalui aplikasi Facebook Messenger, gambar merujuk pada gambar-gambar yang dikirim atau diterima, dan audio merujuk pada file audio yang terkait dengan percakapan atau aktivitas yang diamati.

Dalam penelitian lainnya dilakukan oleh (Yudhana et al., 2019) Berdasarkan hasil perbandingan dalam penelitian tersebut, ditemukan bahwa Magnet Axiom memiliki tingkat keberhasilan sebesar 75% dan Oxygen Forensic Suite sebesar 79% dalam melakukan analisis pada Facebook Messenger dengan menggunakan parameter metode NIST.

Dalam penelitian lainnya dilakukan oleh (R. N. Bintang et al., 2021) dilakukan pencocokan kinerja antara dua alat forensik digital, yaitu Magnet Axiom Forensics dan MOBILedit Forensics, pada aplikasi Facebook Lite yang diinstal pada Samsung Galaxy J2- SM-J200G. Tahapan proses forensik mengikuti pedoman NIST, meliputi pengumpulan, pemeriksaan, analisis, dan pelaporan. Hasil studi menunjukkan bahwa Magnet Axiom Forensics mencapai tingkat keberhasilan sebesar 57,14%, sementara

MOBILedit Forensics mencapai tingkat keberhasilan sebesar 85,71% dalam mengumpulkan dan menganalisis data dari aplikasi Facebook Lite. Untuk pengembangan penelitian selanjutnya, disarankan untuk menambahkan berbagai jenis alat forensik digital lainnya dalam analisis untuk mendapatkan hasil yang lebih komprehensif dan akurat. Selain itu, penelitian juga dapat mempertimbangkan penggunaan metode penelitian yang berbeda untuk memperoleh data yang lebih dapat diandalkan sebagai bukti forensik digital.

Dalam penelitian lainnya dilakukan oleh (Suhardjono et al., 2022) Penelitian dilakukan pada smartphone yang telah di-root dan sudah memiliki aplikasi Facebook Messenger. Kemudian, dilakukan proses penyelidikan menggunakan alat forensik bernama Oxygen Forensic. Proses analisis menggunakan metode NIST (National Institute of Standards and Technology), yang merupakan panduan dan kerangka kerja untuk analisis forensik digital. Dalam penelitian ini, hasil analisis yang diperoleh mencakup gambar, isi chat, dan suara. Gambar merujuk pada file gambar yang ada di aplikasi Facebook Messenger, isi chat merujuk pada pesan-pesan yang tercatat dalam aplikasi, dan suara merujuk pada file audio yang terkait dengan percakapan atau aktivitas yang diselidiki.

Dalam penelitian lainnya yang dilakukan oleh (Pribadi et al., 2023) dilakukan penyelidikan terhadap skenario yang melibatkan penggunaan smartphone POCO X3 yang tidak di-root, instalasi aplikasi Facebook Messenger, pembuatan pesan singkat, serta penerapan skenario penghapusan dan penghapusan aplikasi. Dalam penyelidikan ini, digunakan alat forensik digital MOBILedit Forensic Express PRO 7.2.0.17975 untuk melakukan analisis data. Metode yang digunakan adalah teknik NIST SP 800-101 R1, yang merupakan panduan dan kerangka kerja yang dikembangkan oleh NIST untuk analisis forensik digital. Berdasarkan hasil penelitian, ditemukan bukti berupa video, foto, dan informasi tentang aplikasi Facebook Messenger sebagai hasil investigasi. Namun, karena prosedur rooting tidak dilakukan atau smartphone dalam kondisi unroot,

tidak ditemukan bukti chat dan audio. Studi ini berhasil menemukan bukti digital tanpa perlu melakukan rooting pada perangkat (unrooted device). Namun, peneliti tidak dapat menemukan hasil analisis ketika aplikasi Facebook Messenger diuninstall dari perangkat.

Dalam penelitian lainnya yang dilakukan oleh (Widiandana et al., 2020) Berdasarkan hasil analisis dan percobaan yang dilakukan dalam penelitian, terbukti bahwa metode NIST dapat mempermudah proses investigasi forensik digital, mulai dari pengumpulan barang bukti hingga tahap pelaporan. Selain itu, metode Jaccard juga terbukti efektif dalam mengidentifikasi kasus bullying dengan tingkat yang berbeda. Hasil analisis menunjukkan bahwa terdapat variasi dalam presentase identifikasi kata-kata terkait pelaku bullying. Pelaku dengan presentase tertinggi memiliki 21% kata teridentifikasi dan 79% kata lainnya tidak teridentifikasi, sedangkan pelaku dengan presentase terendah memiliki 13% kata teridentifikasi dan 87% kata lainnya tidak teridentifikasi. Hasilnya menunjukkan kesamaan sebesar 100% antara perhitungan menggunakan aplikasi dan perhitungan secara manual. Hasil tersebut menunjukkan keakuratan dan konsistensi metode yang digunakan dalam penelitian. Metode NIST dan metode Jaccard dapat menjadi alat yang berguna dalam analisis forensik digital dan identifikasi kasus seperti bullying.

Dalam penelitian lainnya yang dilakukan oleh (Rahmansyah, 2021) Berdasarkan hasil penelitian yang dilakukan, dapat disimpulkan bahwa proses forensik mobile dapat membantu dalam menemukan beberapa barang bukti digital pada ponsel. Dalam konteks penelitian ini, ditemukan bahwa sebanyak 6 dari total 8 bukti yang diinginkan berhasil ditemukan pada aplikasi Instagram, sedangkan pada aplikasi Facebook hanya ditemukan 3 dari 8 bukti yang diinginkan. Dengan demikian, persentase keberhasilan dalam mendapatkan barang bukti digital pada aplikasi Instagram jauh lebih tinggi dibandingkan dengan aplikasi Facebook, yaitu sebesar 75% untuk Instagram dan 37,5% untuk Facebook. Selain itu, waktu yang dilakukan untuk melakukan proses forensik setelah barang bukti

dihapus juga mempengaruhi hasil yang diperoleh. Hal ini menunjukkan bahwa semakin lama waktu yang berlalu setelah penghapusan barang bukti, kemungkinan untuk mendapatkan barang bukti digital yang signifikan dapat berkurang. Oleh karena itu, kecepatan dalam melakukan proses forensik setelah penghapusan menjadi faktor penting dalam mengoptimalkan pengumpulan barang bukti digital yang valid dan relevan.

Dalam penelitian lainnya yang dilakukan oleh (Ramadhan et al., 2022) Berdasarkan hasil penelitian di atas, dapat disimpulkan bahwa integrasi standardisasi NIST SP-800-86 dan ISO/IEC 27037:2012 dalam kerangka forensik digital memiliki beberapa kelebihan. Integrasi ini memperkuat kerangka kerja forensik digital dengan mempertimbangkan faktor kritis, waktu, personel, kapasitas media penyimpanan, dan sifat kerentanan sistem perangkat digital. Kerangka kerja yang dihasilkan menjadi lebih komprehensif karena menggabungkan tahapan-tahapan yang sesuai dengan kaidah dasar forensik digital, baik dalam proses pengumpulan maupun pengamanan barang bukti elektronik dan digital. Dengan menggunakan standardisasi ini, proses forensik digital dapat dilakukan secara lebih terstruktur dan terstandarisasi, sehingga meningkatkan keandalan dan validitas hasil forensic. Namun, perlu dicatat bahwa penelitian ini memiliki kelemahan yaitu framework hasil integrasi standar NIST SP-800-86 dan ISO/IEC 27037:2012 belum diuji lapangan dengan Aparat Penegak Hukum. Oleh karena itu, penting untuk melanjutkan penelitian dan menguji implementasi kerangka kerja ini oleh Tim Forensik Digital Aparat Penegak Hukum dalam situasi nyata.

Dalam penelitian lainnya yang dilakukan oleh (Irhash Ainur Rafiq et al., 2022) Berdasarkan hasil penelitian tersebut, ditemukan bahwa dalam penggunaan aplikasi forensik Belkasoft Evidence dan Magnet Axiom pada smartphone Android, aplikasi Magnet Axiom menunjukkan performa yang lebih optimal dengan nilai kinerja sebesar 83,3%. Hal ini mengindikasikan bahwa Magnet Axiom mampu mengakuisisi artefak yang telah hilang dengan lebih baik dibandingkan dengan aplikasi forensik lainnya dalam

penelitian tersebut. Untuk pengembangan penelitian berikutnya, disarankan untuk menggunakan metode baru yang dapat meningkatkan efektivitas dan efisiensi proses forensik digital. Selain itu, kondisi smartphone yang sudah di-root dapat dipertimbangkan sebagai bagian dari penelitian untuk mendapatkan hasil yang lebih baik lagi. Dengan demikian, penelitian selanjutnya dapat menggali lebih dalam dan mengoptimalkan penggunaan aplikasi forensik serta mempertimbangkan faktor-faktor yang dapat mempengaruhi hasil akuisisi artefak, seperti kondisi perangkat dan metode yang digunakan.

B. Landasan Teori

1. Facebook

   Facebook telah menjadi fenomena besar dalam dunia sosial dan mempengaruhi kehidupan banyak orang di seluruh dunia. Sebagai salah satu platform media sosial terbesar, Facebook telah mengubah cara kita berkomunikasi, berinteraksi, dan berbagi informasi.

   Sedangkan pengertian Facebook adalah sebuah situs jejaring sosial atau platform media sosial yang dirancang untuk memfasilitasi interaksi dan komunikasi antar pengguna di dunia maya. Dengan menggunakan Facebook, pengguna dapat membuat profil pribadi, berbagi pemikiran, foto, dan video, serta berinteraksi dengan teman, keluarga, dan orang lain yang terhubung dalam jaringan sosial mereka.

2. Digital Forensik

   Forensik digital adalah cabang ilmu forensik yang fokus pada penemuan, analisis, dan penyelidikan terhadap bukti digital yang ditemukan pada perangkat elektronik seperti komputer, ponsel, tablet, dan perangkat digital lainnya. Tujuan forensik digital adalah untuk memperoleh bukti yang dapat dipertanggungjawabkan secara hukum dan digunakan dalam proses investigasi, penuntutan, atau persidangan (Pribadi et al., 2023).

Prayudi & Ashari menyatakan bahwa Digital forensik melibatkan proses menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi, dan mempresentasikan barang bukti digital. Tujuan utama dari digital forensik adalah untuk mendukung proses penegakan hukum pidana, terutama dalam konteks persidangan (Sudirman, 2019).

Dalam konteks yuridis, digital forensik memainkan peran penting dalam memastikan kesahihan dan keandalan dokumen elektronik sebagai alat bukti dalam proses penegakan hukum pidana. Dalam banyak kasus, dokumen elektronik seperti pesan teks, email, rekaman suara, atau file digital lainnya dapat menjadi bukti yang relevan dalam kasus pidana. Digital forensik memungkinkan penyelidikan yang mendalam terhadap dokumen elektronik tersebut untuk memastikan keasliannya dan memverifikasi integritasnya. Proses digital forensik melibatkan pengumpulan, analisis, dan interpretasi data digital dengan menggunakan metode dan alat yang sesuai (Noffezar et al., 2019).

3. *NIST (National Institute of Standards and Technology) SP 800-101 R1*

Metode yang digunakan untuk melakukan analisis forensik, yaitu menggunakan pendekatan *National Institute of Standards and Technology (NIST).* Pendekatan ini memperjelas alur penelitian sehingga proses penelitian yang terstruktur dapat dilakukan dan digunakan sebagai panduan untuk menyelesaikan masalah yang sudah ada (R. A. Bintang et al., 2020). Panduan *Special Publication 800-101 Revision 1* berjudul "*Guidelines on Mobile Device Forensics*" yang diterbitkan pada tahun 2014 merupakan pendekatan yang digunakan dalam penelitian ini oleh National Institute of Standards and Technology (NIST). Panduan ini hanya berlaku untuk forensik perangkat seluler. Dengan memberikan analisis menyeluruh tentang perangkat seluler dan menguraikan teknologi yang terlibat dan bagaimana hubungannya dengan prosedur forensik, buku panduan ini menjembatani kesenjangan dengan memberikan pandangan mendalam. Tahapan dari metode NIST

Special Publication 800-101 Revision 1, yaitu: *Preservation, Acquisition, Examination & Analysis*, dan *Reporting sebagai berikut:* (Ayers et al., 2014)

1) *Preservation* (Pemeliharaan): Tahap ini melibatkan tindakan untuk memastikan keutuhan dan keaslian bukti digital yang ditemukan. Tujuannya adalah untuk memastikan bahwa bukti tersebut tidak berubah atau terpengaruh selama proses investigasi.
    a. *Securing and Evaluating the Scene* (Mengamankan dan mengevaluasi TKP)

        Merupakan tahapan yang paling penting dalam berbagai keadaan, termasuk kecelakaan, tempat kejadian perkara, atau skenario darurat, mengamankan dan menganalisis lokasi. Selain melindungi integritas bukti dan informasi untuk investigasi atau tindakan selanjutnya, menjaga dan menganalisis tempat kejadian dengan benar membantu memastikan keselamatan responden pertama, pengamat, dan kemungkinan korban.
    b. *Documenting the Scene* (Mendokumentasikan TKP)

        Merupakan komponen penting dalam penyelidikan baik itu TKP, TKP kecelakaan, atau kejadian lain yang memerlukan perekaman ekstensif untuk tujuan analitis dan hukum. Dokumentasi yang tepat membantu dalam pelestarian bukti, memberikan laporan yang akurat tentang keadaan tempat kejadian, dan membantu para penyelidik mengumpulkan apa yang terjadi.
    c. *Isolation* (Isolasi TKP)

        Merupakan situasi yang terjadi ketika mengisolasi orang, objek, atau lokasi dari wilayah sekitar atau populasi umum selama krisis atau situasi berbahaya. Dalam konteks penegakan hukum, isolasi TKP

melibatkan pengepungan dan pengamanan area tempat terjadinya kejahatan. Hal ini mencegah akses yang tidak sah dan kontaminasi barang bukti, sehingga memastikan integritas penyelidikan.

d. *Packaging, Transporting, and Storing Evidence, and Triage* (Pengemasan, Pengangkutan, dan Penyimpanan Barang Bukti, dan Triase)

Dalam pengelolaan barang bukti di berbagai investigasi, khususnya dalam penegakan hukum, forensik, dan medis, triase, pengemasan, pemindahan, dan penyimpanan adalah proses yang penting. Setiap tindakan melindungi integritas dan penerimaan barang bukti untuk investigasi atau prosedur hukum selanjutnya.

e. *On-Site Triage Processing* (Pemrosesan Triase di Tempat)

Merupakan evaluasi awal dan penanganan informasi atau bukti di lokasi kejadian. Dalam beberapa situasi, seperti TKP, kecelakaan, tanggap bencana, dan keadaan darurat medis, hal ini merupakan langkah penting. Para responden dan penyelidik dapat secara efisien mengambil tindakan yang tepat dengan menggunakan pemrosesan triase di tempat, yang membantu mengidentifikasi dan memprioritaskan bukti, informasi, atau aktivitas penting yang membutuhkan perhatian segera.

f. *Generic On-Site Decision Tree* (Pohon Keputusan Generik Di Tempat)

Untuk membantu para responden dan penyelidik dalam mengevaluasi dan merespons berbagai situasi secara sistematis, akan sangat membantu jika membuat pohon keputusan umum di lokasi. Pohon keputusan

memastikan tindakan yang tepat dilakukan berdasarkan kondisi yang terlihat, bukti yang ditemukan, atau informasi yang dapat diakses di sana.

2) *Acquisition* (Akuisisi): Tahap ini melibatkan pengumpulan bukti digital yang relevan dari sumber yang berbeda. Ini melibatkan proses pengambilan salinan bit-by-bit atau pengumpulan informasi yang berkaitan dengan bukti digital yang dapat digunakan untuk analisis lebih lanjut.

   a. *Mobile Device Identification* (Identifikasi Perangkat Seluler)

      Proses mengidentifikasi fitur-fitur khas dan spesifik dari perangkat seluler, seperti smartphone atau tablet, disebut sebagai identifikasi perangkat seluler. Identifikasi ini sangat penting dalam banyak situasi, seperti pekerjaan digital forensik, keamanan siber, dan pelacakan peralatan yang hilang atau dicuri.

   b. *Tool Selection and Expectations* (Pemilihan Alat dan Ekspektasi)

      Penggunaan alat untuk mengidentifikasi perangkat seluler tergantung pada tujuan, konteks, dan fakta-fakta tertentu dari investigasi atau tugas lainnya. Perangkat yang berbeda memiliki fungsi dan kemampuan yang berbeda pula, oleh karena itu penggunaannya harus sesuai dengan tujuan dan sasaran investigasi.

   c. *Mobile Device Memory Acquisition* (Akuisisi Memori Perangkat Seluler)

      Proses mendapatkan data dari memori perangkat seluler, yang sering disebut sebagai ekstraksi data atau pencitraan, disebut akuisisi memori perangkat seluler. Data ini dapat mencakup konten yang dibuat oleh pengguna, sistem file, aplikasi data, pengaturan, dan

informasi lain yang mungkin berharga untuk forensik, forensik digital, atau pengumpulan intelijen. Pencadangan memori yang andal sangat penting untuk memastikan keakuratan dan integritas data. Variasi prosedur tergantung pada jenis perangkat dan sistem operasi yang digunakan.

d. *Tangential Equipment* (Peralatan Tangensial)

Peralatan tangensial, kadang-kadang disebut sebagai peralatan yang menggambarkan alat atau perangkat yang tambahan atau terhubung ke sistem utama atau peralatan yang digunakan. Peralatan ini melakukan tugas khusus yang membantu atau meningkatkan prosedur atau tugas utama. Peralatan tangensial sering digunakan untuk meningkatkan fungsionalitas, keamanan, atau efisiensi di berbagai situasi dan industri.

e. *Cloud Based Services for Mobile Devices* (Layanan Berbasis Cloud untuk Perangkat Seluler)

Merupakan layanan dan program yang menggunakan teknologi komputasi awan untuk menyimpan, mengakses, dan mengelola data serta sumber daya secara online untuk perangkat seluler. Pengguna perangkat seluler dapat memanfaatkan layanan ini dengan berbagai cara, termasuk penyimpanan yang mudah, sinkronisasi data antar perangkat, kerja sama tim, dan aksesibilitas dari lokasi mana pun yang memiliki koneksi internet.

3) *Examination & Analysis (*Pemeriksaan dan Analisis): Tahap ini melibatkan analisis terhadap bukti digital yang telah dikumpulkan. Ini melibatkan penggunaan alat dan teknik khusus untuk memeriksa, memulihkan, dan menganalisis data yang terkandung dalam bukti digital. Tujuannya adalah untuk

mengidentifikasi informasi yang relevan dan mengambil kesimpulan berdasarkan analisis tersebut.

a. *Potential Evidence* (Bukti Potensial)

Tergantung pada fokus investigasi atau jenis kejadian yang sedang diselidiki, potensi untuk menemukan bukti di perangkat seluler bisa sangat bervariasi. Data dalam jumlah besar disimpan di perangkat seluler, dan data ini dapat digunakan dalam berbagai konteks, termasuk proses peradilan, sengketa perdata, forensik digital, dan pengumpulan data intelijen.

b. *Applying Mobile Device Forensic Tools* (Menerapkan Alat Forensik Perangkat Seluler)

Dengan menggunakan perangkat lunak dan metode khusus, alat forensik perangkat seluler digunakan untuk mengumpulkan, memeriksa, dan menganalisis data dari perangkat seluler untuk tujuan peradilan atau investigasi. Program-program ini dibuat untuk mengatasi kesulitan khusus yang ditimbulkan oleh perangkat seluler, seperti banyaknya sistem operasi, pilihan penyimpanan, dan langkah-langkah keamanan.

c. *Call and Subscriber Records* (Catatan Panggilan dan Pelanggan)

Dalam investigasi telekomunikasi dan perangkat seluler, catatan panggilan dan pelanggan-juga disebut sebagai catatan detail panggilan (call detail record/CDR) dan catatan informasi pelanggan (subscriber information record/SIR)-merupakan bentuk bukti yang sangat penting. Catatan-catatan ini memberikan rincian yang mendalam tentang operasi komunikasi dan berguna untuk administrasi jaringan, pengumpulan informasi intelijen, dan investigasi kriminal.

4) *Reporting* (Pelaporan): Tahap terakhir ini melibatkan penyusunan laporan yang berisi hasil dari proses pemeriksaan dan analisis sebelumnya. Laporan ini berisi temuan, kesimpulan, dan rekomendasi yang relevan. Laporan ini dapat digunakan untuk memberikan informasi kepada pihak yang berkepentingan dan sebagai bukti dalam proses hukum atau investigasi yang lebih lanjut.

4. Bukti digital

Definisi bukti digital adalah informasi elektronik yang dikumpulkan dan digunakan sebagai bukti dalam konteks investigasi atau kasus hukum. Bukti digital dapat terdiri dari berbagai jenis data elektronik yang ditemukan atau dikumpulkan dari perangkat digital seperti komputer, ponsel cerdas, tablet, server, atau media penyimpanan lainnya (Qibriya et al., 2021).

5. MOBILEdit Forensik

MOBILedit merupakan salah satu alat forensik yang digunakan untuk memperoleh, mencari, dan memeriksa perangkat ponsel secara logis. Alat ini memiliki beberapa mekanisme konektivitas, terutama melalui konektivitas nirkabel, yang membedakannya dari alat forensik serupa. MOBILedit memungkinkan penyidik untuk mengakses dan memperoleh informasi sistem telepon dari perangkat ponsel yang sedang diselidiki. Alat ini dapat mengumpulkan berbagai data penting seperti daftar kontak, pesan teks, log panggilan, file multimedia, dan informasi lainnya yang terdapat di dalam perangkat ponsel. Selain itu, MOBILedit juga menyediakan fitur untuk menganalisis data yang telah diperoleh. Alat ini dapat membantu penyidik dalam mengidentifikasi pola, hubungan, dan informasi penting lainnya dari data yang diambil dari perangkat ponsel. alam konteks forensik digital, MOBILedit memiliki kelebihan dalam menggunakan konektivitas nirkabel, yang memungkinkan akses dan pengambilan data yang lebih fleksibel.