BAB II
TINJAUAN PUSTAKA

A. Hasil Penelitian Terdahulu

Dalam penelitian sebelumnya yang dilakukan oleh (Yuliana et al., 2022) dengan judul "Analisis Bukti Digital *Cyberbullying* pada Media Sosial Menggunakan Metode *NIST* 800-101*".* Skenario *cyberbullying* dibuat pada aplikasi *instagram* dan *whatsapp* melalui *smartphone* yang tidak di lakukan proses *rooting*. Penelitian ini menggunakan *MOBILedit Forensic* dan apliksi *Autopsy* dengan metode NIST. Hasilnya menunjukan bahwa, *MOBILedit Forensic* tidak ditemukan barang bukti yang diminta di *instagram*, sedangkan *Autopsy* menemukan beberapa teks berupa komentar di *instagram* tetapi tidak menemukan gambar dan video. Di *whatsapp*, hanya ditemukan file stored-nya, teks tidak ditemukan.

Penelitian (Supardin et al., 2022) dengan judul "Analisis Perbandingan *Tools* Forensik Digital pada *Instagram Messenger* Menggunakan Metode *National Institute of Standards and Technology (NIST).*" Dalam penelitian ini, dua alat forensik, *MOBILedit Forensic* dan *Magnet Axiom Forensic*, untuk menentukan mana yang memiliki hasil yang lebih baik dalam mengumpulkan bukti digital dari kasus pornografii pada aplikasi *instagram messenger*. Hasil penelitian menunjuan bahwa *Magnet Axiom Forensic* memiliki tingkat akurasi yang lebih tinggi, mencapai 76,92%, sedangkan *MOBILedit Forensic* memiliki tingkat akurasi hanya 69,23%.

Penelitian yang dilakukan oleh (Ainur Rafiq et al., 2022) berjudul "Perbandingan *Forensic Tools* pada *Instagram* Menggunakan Metode *NIST".* bertujuan untuk mengumpulkan hasil dari *tools Belkasoft Evidence* dan *Magnet Axiom* untuk menangani kasus pencemaran nama baik pada aplikasi *instagram*

dengan menggunakan metode *NIST*. Hasil penelitian menunjukan bahwa *Magnet Axiom* performanya lebih baik daripada *Belkasoft Evidence*.

Penelitian yang dilakukan oleh (Rahmansyah, 2021) dengan judul "Perbandingan Hasil Investigasi Barang Bukti Digital pada Aplikasi *Facebook* dan *Instagram* dengan metode *NIST"*, bertujuan untuk mengidentifikasi dan membandingkan hasil bukti digital yang telah diperoleh dari aplikasi *Facebook* dan *Instagram* menggunakan *Magnet Axiom Process* dan *Magnet Axiom Examine*. Hasil peneltian menunjukan bahwa aplikasi *instagam* menghasilkan barang bukti digital lebih banyak daripada *facebook*. *Instagram* menemukan enam barang bukti dari total delapan, sedangkan *facebook* menerima tiga barang bukti digital. Dengan demikian presentase barang bukti yang dihasilkan *instgram* sebesar 75% dan *facebook* sebesar 37,5%.

Penelitian yang disebut oleh (Nasirudin et al., 2020) dengan judul "Analisis Forensik *Smartphone Android* Menggunakan Metode *NIST* dan *Tool MOBILedit Forensic Express"*. Penelitian ini memulai kasus dengan mengamankan barang bukti *smartphone andorid Samsung Galaxy* A8 dari kasus penggelapan dana belanja *sparepart*. dengan menggunakan *MOBILedit Forensic Express* dan metode *NIST*. Penelitian ini menemukan bahwa gambar, email, chat, kontak, dan profil pengguna adalah 75% dari data *smartphone* yang terdeteksi.

Penelitian berjudul "Analisis Bukti Digital *Facebook Messenger* Menggunakan Metode *NIST"* dilakukan oleh (Yudhana et al., 2018). Penelitian ini akan mengembalikan barang bukti kejahatan digital dari kasus perdagangan narkoba melalui aplikasi *facebook messenger*. Penelitian ini menggunakan *Oxygen Forensic*, yang digunakan dengan metode NIST. Penelitian ini menggunakan *smartphone Galaxy V+ SM-G31HZ*, dengan proses *rooting*, menginstal aplikasi *Facebook Messenger*, membuat pesan, dan melakukan investigasi dengan *Oxygen Forensic*. Hasil penelitian menunjukan bahwa *Oxygen Forensic* berhasil

mendapatkan gambar, pesan, audio, teks percakapan yang dikrimkan, tetapi tidak berhasil mendapatkan video.

Penelitan yang dilakukan oleh (Yin et al., 2019) dengan judul *"Forensic Analysis of Social Networks Based on Instagram"*. Penelitian ini bertujuan untuk menyelidiki versi web dan versi aplikasi dari *instagram* untuk melakukan analisis forensik terhadap perilaku pengguna di lingkungan *Windows 10* dan *Android*. Hasil dari penelitian ini menemukan bahwa dalam versi web atau *Windows 10* memiliki kontrol privasi yang berbeda. Dalam perlindungan data pengguna, *Mozilla Firefox* memberikan perlindungan tertinggi, diikuti oleh *Google Chrome*, dan yang terakhir adalah *Internet Explorer* yang memberikan perlindungan terendah.

Penelitian yang dilakukan oleh (Al Mutawa et al., 2022) dengan judul *"Forensic Analysis of Social Networking Applications on Mobile Devices"*. Penelitian ini berfokus untuk menganalisis tiga aplikasi jejaring sosial yang banyak digunakan pada *smartphone*, diantaranya *Facebook*, *Twitter,* dan *MySpace*. Pengujian dilakukan pada tiga *smartphone* yaitu *Blackberry, iPhone*, dan ponsel *Android*. Analisis forensik ditujukan untuk menentukan apakah aktivitas yang dilakukan melalui aplikasi ini disimpan di memori internal perangkat. Jika demikian, jangkauan, signifikasi, dan lokasi data yang dapat ditentukan dan diambil dari citra logis setiap perangkat ditentukan. Hasilnya menunjukan bahwa tidak ada jejak yang dapat dipulihkan dari perangkat *Blackberry*. Namun, *iPhone* dan ponsel *Android* menyimpan sejumlah besar data berharga yang dapat dipulihkan dan digunakan oleh penyelidik forensik.

B. Landasan Teori

1. Digital Forensic

Digital Forensic adalah aplikasi ilmu pengetahuan dan teknologi komputer yang digunakan untuk membuktikan kejahatan *digital* dalam konteks hukum untuk mendapatkan bukti yang dapat digunakan pelanggar. Intinya, digital forensik digunakan untuk menemukan bukti digital di berbagai sumber, seperti, lalu lintas, jaringan, penyimpanan sementara, penyimpanan permanen, USB, dan CD (Riadi et al., 2018).

Forensik Digital *(Digital Forensic)* (juga dikenal sebagai ilmu forensik digital) adalah salah satu cabang ilmu forensik yang terutama berfokus pada penyelidikan dan penemuan konten perangkat digital. Istilah ini awalnya hanya berarti forensik komputer, tetapi sekarang mencakup semua perangkat yang dapat menyimpan data digital (Aisyah et al., 2022)

2. Mobile Forensic

Proses pemulihan bukti digital dari perangkat seluler dengan metode dan kondisi forensik yang sesuai dikenal dengan *Mobile Forensic*. Karena meningkatnya penggunaan perangkat *mobile*, seperti *smartphone*, dengan berbagai jenis dan sistem operasi untuk kejahatan, forensik perangkat *mobile* sangat diperlukan untuk menangani kasus kejahatan yang berkaitan dengan perangkat *mobile*, khususnya *smartphone*. Kebutuhan akan *forensik* perangkat *mobile* meningkat seiring dengan meningkatnya layanan berbasis *mobile* dan jumlah penggunanya (Sunardi et al., 2019).

3. *Cybercrime*

Cybercrime adalah tindakan kejahatan yang dilakuan di dunia maya. Ada beberapa jenis kejahatan pada *cybercrime*, diantaranya, akses tidak sah, konten ilegal, penyebaran virus, *cybercullying*, *carding*, *hacking* dan

cracking, *cyberspionase*, sabotase, pemerasan, *cybersquatting*, dan *cyber terrorism* (Siahaan, 2018).

4. Bukti Digital

Bukti digital adalah informasi yang dapat disimpan dalam bentuk atau format digital. Khususnya bukti digital yang berkatan dengan perangkat *mobile*, seperti *smartphone* dapat ditemukan dalam riwayat panggilan, buku telepon, SMS dan MMS, foto, audio, dan video. Bukti digital biasanya terkait dengan kejahatan digital seperti kejahatan yang memanfaatkan sosial media sebagai tempat melakukan kejahatan, sehingga bukti digital digunakan untuk membantu proses pengadilan. Bukti digital sangat rentan akan perubahan, sehingga setiap perubahan yang melibatkan bukti digital dapat menghasilkan kesimpulan yang salah atau bukti digital tidak akan berguna lagi (Yudhana et al., 2018).

5. *Recovery* Data

Recovery data adalah proses pemulihan data yang tidak bisa dibuka atau diakses, data hilang, rusak atau diformat. Data dapat dikembalikan dari *hardisk, flashdisk*, atau media penyimpanan lainnya seperti kamera digital, dan kamera video (Fitriana et al., 2020).

6. *Smartphone*

Smartphone merupakan perangkat *hybird* yang berfungsi sebagai ponsel dan hampir mirp seperti komputer dalam bentuk *gadget* yang lebih kecil. Perangkat ponsel pintar ini dapat menyimpan data yang sangat besar, bukan hanya *log* panggilan atau SMS, tetapi juga informasi tentang perilaku, kegiatan, dan penggunaan (Ariyanti et al., 2021).

7. Sosial Media

Media sosial adalah jenis media *online* yang memungkinkan orang untuk dengan mudah berbagi dan membuat konten, seperti blog, jejaring sosial, dunia virtual, wiki, dan forum. Jejaring sosial adalah situs web dimana setiap orang bisa membuat web page pribadi dan berkomunikasi dengan temen-teman mereka. *Facebook, Instagram,* dan *Twitter* adalah jaringan sosial terbesarb(Rafiq, 2020).

8. *Instagram*

Instagram merupakan gabungan dari kata *instan-telegram* yang dapat diartikan sebagai aplikasi untuk berbagi foto, video dan berbagi jejaring sosial media lainnya secara cepat (Supardin et al., 2022). *Instagram* adalah salah satu media sosial yang sedang banyak digunakan oleh pengguna *smartphone* saat ini. Banyak orang menggunakannya untuk berkomunikasi seperti meng-*upload* foto atau mengirim pesan yang mereka lakukan ke sesama pengguna *Instagram* lainnya (Caesar et al., 2018).

9. Metode NIST *Special Publication* 800-101 R1

Menurut (Ayers et al., 2014), Metode *National Institute of Standards and Technology (NIST) SP 800-101 R1* adalah salah satu tahap dalam forensik digital dimana pada metode ini mempunyai empat tahap. Tahapan investigasi digital forensik yang dikembangkan oleh *NIST* terdiri dari 4 (empat) buah tahapan yaitu:

a. *Preservation* (penjagaan), adalah tahap awal dimana pada tahap ini merupakan tahapan penjagaan pada barang bukti *smartphone* agar data tidak berubah dan tidak hilang saat proses forensik. Tahap terdiri dari beberapa prosedur diantaranya ada:
   1) *Securing and Evaluating The Scene* (Pengamanan dan Evaluasi TKP)

a) Tes DNA atau sidik jari dari pengguna atau pemilik perangkat *smartphone*.
b) Mengidentifikasi fitur dan masalah perangkat *smartphone*.
c) Melakukan pemeriksaan menyeluruh pada perangkat *smartphone* seperti kartu memori eksternal, UICC, dan komputer pribadi yang berhubungan dengan perangkat *smartphone* pengguna.
d) Wawancara dengan pemilik perangkat *smartphone* diperlukan jika ada kata sandi atau pola yang diperlukan untuk mengakses data pada perangkat *smartphone*.
e) *Reset Master* dapat dilakukan dari jarak jauh, tetapi saat mengamankan perangkat *mobile*, jangan aktifkan kode *reset master* untuk mengamankan semua data. Isolasi jaringan mencegah data perangkat dihapus atau diubah.
f) Perangkat *smartphone* yang mungkin mengalami kondisi yang rumit dibutuhkan penanganan oleh petugas forensik khusus.
g) Jika perangkat *smartphone* terendam cairan yang tidak bersifat kaustik, maka dilakukan pelepasan baterai.
h) Jika kerusakan pada perangkat *smartphone* menganggu proses pengambilan data, komponen atau perintah dapat diperbaiki untuk mengembalikannya ke kondisi awal.

2) *Dokumenting The Scene* (Pendokumentasian Barang Bukti)
a) Semua bukti harus diidentifikasi dan dicatat dengan akurat.
b) Bahan non-elektronik seperti faktur pembelian, buku petunjuk, dan tempat dus perangkat *smartphone* dapat membantu untuk mengetahui spesifikasi perangkat.
c) Mengambil foto tempat kejadian dan perangkat elektorni yang ditemukan untuk membantu penyidikan.

d) Ketika mendokumentasikan bukti, hindari menyentuh atau mencemari perangkat *smartphone*.
e) Jika perangkat *smartphone* ditemukan dengan layar yang terdapat tampilan harus didokumntasikan.

3) *Isolation* (Isolasi)

Beberapa perangkat *smartphone* dapat melakukan penguncian atau menghapus data dari jarak jauh dengan mengiriman perintah melalui pesan teks, tetapi untuk melakukannya, pengguna harus meonaktifkan konektivitas jaringan perangkat. Selain itu, untuk mencegah data diubah, seperti menambah koordinat lokasi GPS baru ke lokasi petugas forensik. Ada 3 metode dasar untuk mengisolasi perangkat seluler yaitu:

a) Mengubah jaringan pernagkat ke "Mode Pesawat".
b) Nonaktfkan perangkat *smartphone*.
c) Tempatkan perangkat *smartphone* di tempat yang aman.

Namun, saat perangkat *smartphone* dinonaktifkan, diperluan untuk mengaktifkan kode autentifikasi seperti UICC PIN atau kode keamanan pada perangkat *smartphone*, yang dalam hal ini dapat mempersulit proses *acquisition* (pengumpulan) dan menunda *examination* (pemeriksaan).

4) Packaging, Transporting and Storing Evidence (Pengemasan, Pengangkutan, dan Penyimpanan Barang Bukti)

Petugas forensik harus menyegel wadah perangkat dengan label yang sesuai dengan spesifikasi agensi setelah perangkat *smartphone* disita. Karena perangkat *smartphone* dapat berubah-ubah, maka harus segera diperiksa di laboratorium forensik untuk pemrosesan. Fasilitas penyimpanan yang dapat diandalkan diperlukan dengan menyedikan lingkungan yang sesuai untuk peranngkat *smartphone*.

semua bukti harus disimpan dalam wadah tertutup yang aman dengan kontrol akses.

5) *On-site Triage Processing* (Pemrosesan Triase Ditempat)

Pemeriksaan harus segera dilakukan jika perangkat *smartphone* ditemukan dalam kondisi dimana layarnya tidak terkunci atau baterinya tidak habis. Ini berarti bahwa perangkat terkunci sudah terhubung dengan perangkat *smartphone.*

6) *Generic On-Site Decision tree*

Pada tahap ini digunakan pohon keputusan sebagai pedoman untuk lembaga dan organisasi untuk meyelaraskan sesuai dengan kebijakan dan praktik.

b. *Acquistion* (Akusisi Data), adalah tahapan dimana dilakukannya proses pengumpulan informasi dari perangkat *smartphone* dan media yang relevan. Dalam proses *acquisition* dilakukan beberapa tahap yaitu:

1) *Mobile Device Indentification* (Identifikasi Perangkat Seluler)
   a) *Device chacarter indentification*
   b) *Device interface identification*
   c) *Device label identification (IMEI, ESN, ICCID of the UISS, FCC ID dan MEID)*
   d) *Carrier indentification*
   e) *Reverse lookup*

2) *Tool Selection and Expectations* (Pemilihan Alat dan Ekspetasi)

Alat forensik yang digunakan sebagian besar menentukan proses *acquisition* pada perangkat *smartphone*. alat forensik yang digunakan harus memenuhi kriteria penilaian berikut:

   a) *Usability*
   b) *Comprehensive*
   c) *Deterministic*
   d) *Verifiable*

e) Tested

3) Mobile Device Memory Acquisiton (Akuisisi Memori Perangkat Seluler)

Harap dipastikan bahwa data yang diminta, seperi log telepon atau gambar galeri telah disimpan sebelum pemulihan data perangkat *smartphone*. Proses *acquisition* harus dilakukan jika perangkat *smartphone* dalam kondisi menyala sebelum dilakukan *physical acquisition.* Jika perangkat ditemuan dalam kondisi mati , maka dilakukan *physical acquisition* terlebih dahulu sebelum dilakukan *acquisition.*

4) Tangential Equipment (Peralatan Tangensial)

Perangkat tangensial mencakup perangkat yang berisi memori dan dikaitkan dengan perangkat seluler. Tiga kategori yang utama adalah kartu memori, komputer host tempat perangkat seluler telah menyinkronkan kontennya dan penyimpanan berbasis *cloud*.

5) Cloud Based services for Mobile Device (Layanan Berbasis *Cloud* untuk Perangkat seluler)

Layanan berbasis *cloud* ini adalah kombinasi dari jaringan seluler dan komputasi awan yang memungkinkan aplikasi dan data pengguna disimpan di *cloud* yaitu server internet, daripada memori perangkat seluler.

c. *Examination* (Pemeriksaan Data) *& Analysis* (Analisis Data), adalah tahap inti dari metode ini dimana pada tahap *examination* adalah tahap pemeriksaan langkah-langkah dalam menemukan hasil dari akuisisi, dan kemudian pada tahap ini akan dianalisis sesuai dengan prosedur yang berlaku. Dalam proses ini ada beberapa tahapan diantaranya adalah:

1) Potential Evidence (Bukti Potensial)

Beberapa cakupan bukti digital perangkat *smartphone*, termasuk:

a) Subscriber and eqipment identifiers

Analisis Forensik Digital…, Aprilia Aniq Maharani Faiqoh, Fakultas Teknik dan Sains UMP, 2023

b) *Date/time, language, and other things*
c) *Phonebook/contact information*
d) *Calendar information*
e) *Text messages*
f) *Outgoing, incoming, and missed call logs*
g) *Electronic mail*
h) *Photos*
i) *Audio and video recordings*
j) *Multi-media messages*
k) *Instant messaging*
l) *Web browsing activities*
m) *Electronic document*
n) *Social media related data*
o) *Application related data*
p) *Location information*
q) *Geolocation data*

Dua jenis penyelidikan forensik biasanya dilakukan. Jenis pertama adalah ketika peristiwa terjadi tetapi identitas pelaku tidak diketahui, seperti peretasan. Jenis kedua adalah ketika tersangka dan peristiwa diketahui. Setelah memahami latar belakang kejadian, pemeriksa forensik dan analisis dapat merujuk pada tujuan berikut:

a) Kumpulkan informasi orang yang terlibat (*Who*).
b) Tentukan jenis peristiwa yang terjadi secara pasti (*What*).
c) Buat garis waktu kejadian (*When*).
d) Ungkap informasi yang menjelaskan mengapa terjadi pelanggaran (*Why*)
e) Temukan alat yang digunakan (*How*).

Setelah mengumpulkan dan menyimpan salinan data dari perangkat *smartphone*, proses selanjutnya adalah pencarian data

dengan alat forensik. Panduan penegakan hukum yang dibuat oleh Departemen Kehakiman Amerika Serikat menyarankan beberapa analisis data yang dihasilkan antara lain:

a) Ownership and possesion

b) Application and file

c) Analysis timeframe

d) Analysis data hiding analysis

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

Setelah salinan hasil akuisisi tersedia, selanjutnya adalah melakukan pencarian data, mengidentifikasi bukti, dan mengembangkan konten laporan akhir.

3) *Call and subscriber records*

Langkah ini dilalkukan untuk menangkap informasi yang diperlukan untuk menagoh pelanggan secara akurat, dalam hail ini seperti paket layanan prabayar, mendebit saldo dan hal lainnya yang berkaitan dengan layanan prabayar.

d. *Reporting*, dimana tahap ini merupakan tahap akhir atau ringkasan menyeluruh dari semua proses penelitian. Laporan hasil forensik harus mencakup semua data yang diperluan untuk membedakan kasus dan sumbernya, untuk memberikan penjelasan tentang hasil tes dan temuan, dan bertanggung jawan atas isinya. Secara umum, laporan dapat mengandung data seperti berikut:

1) Identtitias agen pelapor
2) Pengidentifikasian kasus atau nomor pengiriman
3) Penyelidik kasus
4) Identitas pengirim
5) Tanggal penerimaan bukti
6) Tanggal laporan

7) Daftar dekstiptif *item* yang diajuan untu pemeriksaan, termasuk nomor seri, merek dan model.
8) Identitas dan tanda tangan pemeriksa
9) Peralatan dan perlengkapan yang digunakan dalam pemeriksaan
10) Deskripsi singkat tentang langkah-langkah yang dilakukan selama pemeriksan, aeperti pencarian string, pencarian gambar grafik, dan memulihkan file yang terhapus
11) Bahan pendukung seperti cetakan barang bukti tertentu, salinan bukti, dan dokumentasi lacak.
12) Rincian temuan:
    a) File khusus yang terkait dengan permintaan
    b) File lain. Termasuk file yang dihapus, yang mendukung temuan
    c) Pencarian string, pencarian kata kunci, dan pencarian string teks
    d) Bukti terkait internet, seperti analisis lalu lintas situs web, log obrolan, *file cache*, email, dan ativitas grup berita.
    e) Analisis gambar grafis, indikator kepemilikan yang mencakup data registrasi program analisis data
    f) Deskripsi program yang relevan pada item yang diperiksa
    g) Teknik yang digunakan untuk menyembunyikan data seperti enkripsi, steganografi, atribut tersembunyi, partisi tersembunyi dan anomali nama file
    h) Laporan kesimpulan

10. *MOBILedit Forensic Express Pro*

MOBILedit Forensic Express Pro adalah paket multifungsi yang mencakup ektrasi ponsel, analisis data, dan pembuatan laporan. Sebuah program 64-bit yang menggunakan teknik akuisisi data logis dan fisik. Pemeriksaan individual dapat dilakukan pada sebagian perangkat seluler dan menghasilkan lapotan dalam berbagai format (*PDF, HTML, Excel*, dll.)

dengan menghubungkan telepon melalui kabel *USB, Wifi*, atau *Bluetooth* (Yuliana et al., 2022).

11. *SysTool SQLite Viewer*

SysTool SQLite Viewer adalah *tools* yang digunakan untuk membuka dan melihat file *database sqlite* pada sistem operasi *Windows*. Jika file *SQLite* dalam keadaan rusak, maka utilitas ini juga dapat memindai dan memperbaiki file *database* yang rusak dan menampilkan pratinjau item data dalam file tersebut. Tidak ada batasan ukuran file dari *database*. Ada item data seperti tabel, formulis, tampilan, dan kolom. *Tools* ini bisa mendapatkan laporan pemindaian file dimana detail seperi nama *database*, jumlah item yang dipindai dan presentase pemindaian akan ditampilkan. Ada beberapa tipe data yang dipulihkan dengan menggunakan *tools* ini seperti **.db, *.sqlite, *db3, *.sqlite3, *.fossil.*