BAB II
TINJAUAN PUSTAKAN

2.1 Tinjauan Pustaka

Berdasarkan penelitian yang dilakukan, memiliki acuan dari beberapa penelitian terdahulu menjadi sangat penting karena dapat mencegah dari adanya suatu duplikasi dalam penelitian yang sedang dikerjakan. Adanya penelitian sebelumnya dapat juga menjadi sebuah landasan dan referensi berpikir untuk penelitian yang dikerjakan.

Adapun penelitian-penelitian terdahulu yang membahas mengenai *digital forensic*, khususnya pada bagian *digital forensic* dan android *forensic* secara umum dengan menggunakan berbagai macam metode dan *software* banyak dijadikan referensi dalam mengerjakan penelitian ini.

Berikut merupakan beberapa penelitian terdahulu:

Penelitian yang dilakukan oleh Ikhsan Zuhriyanto, Anton Yudhana, dan Imam Riadi dengan judul "Perancangan *Digital Forensic* pada Aplikasi Twitter Menggunakan Metode *Live Forensic*s" [8]. Penelitian ini membahas tentang penggunaan *digital forensic* dalam menyelidiki kejahatan siber pada platform media sosial, khususnya Twitter. Perkembangan sosial media, khususnya Twitter juga di barengi dengan meningkatnya angka kejahatan siber yang terjadi. Kejahatan siber yang terjadi memerlukan proses *digital forensic* untuk proses mencari barang bukti secara *digital* mengenai kasus yang terjadi. Penelitian ini menggunakan metode *National institute of justice* (NIJ) sebagai metode penelitian dengan menggunakan FTK *Imager* sebagai *tool* pembantu penyelidikan. Hasil dari penelitian ini menyatakan bahwa hasil ekstraksi data melalui FTK Imager merupakan data valid dan dapat digunakan dalam *digital forensic* sebagai barang bukti. Bukti seperti *username* dan profil *picture* juga terekstrak dengan baik dari *database* dengan memanfaatkan *file* log yang tersimpan secara lokal pada masing-masing komputer atau *device* di mana akun tersebut dibuat.

Penelitian lainnya oleh Riadi imam, Sunardi, dan Sahiruddin yang berjudul "Perbandingan *Tool Forensic* Data *Recovery* Berbasis Android

Menggunakan Metode NIST" [9]. Penelitian ini menggunakan dua *tool forensic* yaitu Wondershare dr. Fone *for* Android dan Oxygen *Forensic*s Suite 2014. *Tools* tersebut digunakan untuk melakukan sebuah uji *forensic* pada *smartphone* yang menjadi sebuah barang bukti pada simulasi kasus penggerebekan terduga penjualan narkoba dengan barang bukti yang ditemukan berupa dua *smartphone* yang digunakan oleh pelaku. Penelitian ini menjelaskan bahwa kedua *tools forensic* yang digunakan menghasilkan hasil yang berbeda pada proses *recovery* data pada *smartphone* tersangka. Pada *tool* Wondershare tingkat data dapat *recovery* terhadap data yang dihapus pada *smartphone* pertama mencapai angka 31%, dan 67% data dapat di *recovery* pada *tools* Oxygen *Forensic*. Kemudian pada *smartphone* kedua tingkat *recovery* data mencapai 35% pada *tools* Wondershare dan 69% pada Oxygen *Forensic*.

Penelitian selanjutnya yang menjadi referensi yaitu penelitian dari Kadek Dwi Oka Mahendra dan I Komang Ari Mogi yang berjudul "*Digital forensic Analysis of* Michat *Applications on Android as Digital Proof in Handling Online Prostitution Cases*" [10]. Penelitian ini membahas tentang bagaimana sebuah aplikasi pesan bernama michat sering dijadikan sebuah alat untuk melakukan sebuah tindak prostitusi online. Hal ini terjadi di mana kedua belah pihak saling melakukan percakapan hingga terjadi suatu kesepakatan. Hal ini itu tentunya dapat ditindak lanjuti untuk kemudian diusut lebih lanjut oleh petugas atau lembaga berwenang. Proses *digital forensic* menjadi satu hal yang berperan penting dalam penanganan kasus seperti ini, seperti pada penelitian ini, proses *digital forensic* dilakukan dengan *tool Mobile*dit *Forensic* Express dan Sys*Tools* SQLite *Viewer*. Proses dilakukan dengan mengekstrak data aplikasi melalui *Mobile*dit *Forensic* Express, kemudian selanjutnya dilakukan koleksi dari hasil data yang telah di ekstrak. Hasil data tersebut di koleksi dengan menggunakan Sys*Tools* SQLite *Viewer* yang dapat membaca isi dari *database* Michat yang telah terpasang pada *smartphone*. Pada *database* tersebut dapat ditemukan beberapa informasi penting seperti Uid, *nickname*, tanggal lahir, dan lain-lain sesuai yang

diberikan saat melakukan registrasi. Selain itu, melalui Sys*Tools* SQLite *Viewer* juga dapat ditemukan rincian percakapan antara pengguna dan lawan pesan yang kemudian dapat dijadikan barang bukti atas tindak kriminal prostitusi *online*.

Penelitian berikutnya dengan menggunakan metode *National institute of justice* (NIJ) yaitu penelitian berjudul "*Forensic Mobile* pada *Smartwatch* Berbasis Android" oleh Roni Anggara Putra, Abdul Fadlil, dan Imam Riadi [11]. Penelitian ini membahas tentang penggunaan *smartwatch* berbasis android yang sudah semakin banyak digunakan. Selain itu penggunaan *smartwatch* yang dapat menjadi pendamping sebuah *smartphone* memiliki fungsi yang berbagai macam, seperti menerima panggilan telepon langsung yang masuk dari *smartphone*, menerima dan membalas pesan masuk, dan masih banyak lagi. Langkah investigasi pada *smartwatch* memiliki proses dan cara yang sama saat melakukan investigasi *forensic* pada *smartphone*. Di penelitian ini investigasi dilakukan dengan menggunakan *tools Mobile*dit *forensic* dan metasploit. Hasil investigasi dilakukan dengan menggunakan sebuah bantuan kabel data saat menggunakan *tools mobile*dit *forensic* agar semua *file* yang ditransfer dapat diproses secara sempurna dan tidak ada gangguan, dan untuk metasploit dapat menggunakan koneksi jaringan wifi. Hasil yang didapatkan dari proses investigasi dengan dua *tools* tersebut berada di angka mendekati 100% data terkumpul. Data-data tersebut berupa data-data penting berupa pesan singkat, data kontak, dan data panggilan. Namun kedua *tools* tersebut memiliki kekurangan yang sama, yaitu kedua *tools* yang digunakan tidak dapat melakukan proses *recovery* terhadap data yang telah di hapus atau hilang pada *smartwatch* yang dijadikan objek penelitian.

Penelitian lain yang menjadi referensi yaitu penelitian yang juga dikerjakan oleh Imam Riadi, Sunardi, dan Sahiruddin yang menggunakan metode *National institute of justice* (NIJ) dengan judul "Analisis *Forensic Recovery* pada *Smartphone* Android Menggunakan Metode *National institute of justice* (NIJ)" [12]. Penelitian ini menggunakan 3 *tools forensic* yaitu

*Mobile*dit *Forensic*, Wondershare dr.Fone for Android, dan Belkasoft Evidance Center, untuk melakukan proses ekstraksi pada *smartphone* yang menjadi barang bukti. Ketiga *tools* yang digunakan dalam uji coba pada penelitian ini memiliki hasil ekstraksi yang berbeda-beda pada uji coba dengan menggunakan *smartphone* berjenis Samsung Galaxy J5 dengan sistem operasi berbasis Android versi 5.1 Lollipop. Pengujian menggunakan *tools Mobile*dit *Forensic*s, hasilnya yaitu data hanya dapat ditampilkan saja pada perangkat *smartphone*, akan tetapi data tersebut tidak dapat dikembalikan ketika sudah terhapus. Kemudian pada *tools* Wondershare dr. Fone *for* Android data yang dapat di kembalikan berupa kontak, *log* panggilan, dan pesan. Untuk data berupa gambar dan video tidak dapat di *recovery*. Kemudian pengujian dengan menggunakan *tools* terakhir yaitu Belkasoft *Evidance Center* menghasilkan data berupa kontak dan log panggilan dapat di *recovery* secara utuh, namun data berupa pesan, gambar dan video tidak dapat dilakukan.

Dari penjelasan mengenai beberapa penelitian terdahulu yang telah dipaparkan, berikut ringkasan penelitian yang menjadi referensi ditujukan pada tabel 2.1 di bawah ini:

Tabel 2. 1 Penelitian Terdahulu

No.	Judul	Tahun	Peneliti	Objek Penelitian	Metode	Hasil
1.	Perancangan *Digital forensic* pada Aplikasi Twitter Menggunakan Metode *Live Forensic* [8]	2018	Ikhsan Zuhriyanto, Anton Yudhana, dan Imam Riadi	Aplikasi Twitter	*Live Forensic*	1. Melakukan uji *Live forensic* pada sebuah akun Twitter dapat dilakukan dengan menggunakan *tools* pembantu seperti FTK Imager. 2. Hasil uji dengan menggunakan *tools* mendapatkan sebuah *database* yang kemudian dapat di akses melalui FTK Imager. 3. *Database* yang bersifat lokal tersebut mengandung sebuah *user* id, yang di mana *user* id tersebut merupakan representasi *string* dari *username* pengguna serta nama dari pengguna Twitter tersebut. Kemudian pada bagian *log file* dan *cache* ketika ditelusuri lebih lanjut, maka dapat didapatkan pula gambar dan foto profil pengguna.

No.	Judul	Tahun	Peneliti	Objek Penelitian	Metode	Hasil
2.	Perbandingan *Tool Forensic* Data *Recovery* Berbasis Android Menggunakan Metode NIST [9]	2020	Imam Riadi, Sunardi, dan Sahiruddin	*Smartphone* Android, Samsung J5 Android 5.1, Samsung J1 Ace Android 5.1	National Institute of Standard and Technology (NIST)	1. Perbandingan hasil *recovery tool* pada masing-masing *smartphone* yang digunakan memiliki perbedaan. 2. Pada *smartphone* pertama dengan menggunakan *tools* Wondershare didapatkan 31% data dapat di *recovery*, dan pada *tool* Oxygen dengan 67% data dapat di *recovery*. 3. Pada *smartphone* kedua, 35% data dapat di*recovery* dengan menggunakan *tool* wondershare, dan 69% ter-*recovery* dengan menggunakan *tool* Oxygen.
3.	*Digital forensic Analysis of* Michat *Applications on* Android *as Digital Proof in Handling Online Prostitution Cases* [10]	2021	Kadek Dwi Oka Mahendra dan I Komang Ari Mogi	*Smartphone* Android, Aplikasi instan Messenger MiChat	*National institute of justice* (NIJ)	1. Menggunakan *Mobile*dit *Forensic* Express untuk melakukan investigasi terhadap data yang ada di dalam *smartphone*. Hasil yang didapatkan berupa *database* dari aplikasi MiChat yang telah terpasang pada *smartphone*.

No.	Judul	Tahun	Peneliti	Objek Penelitian	Metode	Hasil
						2. *Database* yang didapatkan tersebut kemudian diolah ke dalam Sys*Tools* SQLite *Viewer*. Hasil dari pengolahan tersebut mendapatkan histori berupa uid, hingga pada histori percakapan antara pengguna dan yang lain. Bukti ini kemudian dapat dijadikan sebuah barang bukti.
4.	Forensik *Mobile* Pada *Smartwatch* Berbasis Android [11]	2017	Roni Anggara Putra, Abdul Fadlil, dan Imam Riadi	*Smartwatch* berbasis Android	National Instutite of Justice (NIJ)	1. Penggunaan *tool Mobile*dit *Forensic* dan Metasploit untuk melakukan uji *forensic* pada *smartwatch* mendapatkan hasil di mana hampir 100% data dapat di*recovery* . 2. Kedua *tool* memiliki kelemahan di mana *tool* tersebut tidak dapat melakukan pengembalian data-data yang sudah hilang pada *smartwatch* yang diteliti.

No.	Judul	Tahun	Peneliti	Objek Penelitian	Metode	Hasil
5.	Analisis *Forensic Recovery* pada *Smartphone* Android Menggunakan Metode *National institute of justice* (NIJ)	2019	Imam Riadi, Sunardi, dan Sahiruddin.	Samsung J5 dengan sistem operasi Android versi 5.1	*National institute of justice* (NIJ)	1. Penelitian menggunakan 3 *tool* yaitu *Mobile*dit *Forensic*s, Wondershare dr. Fone for Android, dan Belkasoft *Evidence Center* dengan menggunakan *sample data* yang dimasukkan ke dalam *smartphone* yang digunakan. 2. Terdapat hasil yang berbeda beda dari masing-masing *tools* yang digunakan dalam tahap pengujian. 3. *Mobile*dit *forensic*s tidak dapat mengembalikan data yang telah dihapus, sedangkan pada *tool* wondershare dan belkasoft data berupa kontak, log panggilan, dan pesan dapat dikembalikan meskipun sudah terhapus sebelumnya. 4. Semua *tools* yang digunakan pada penelitian ini tidak cukup baik dalam

No.	Judul	Tahun	Peneliti	Objek Penelitian	Metode	Hasil
						melakukan *recovery* terhadap *file* berupa gambar dan video.
6.	Analisa Perkembangan *Digital Forensic* Dalam Penyelidikan *Cybercrime* di Indonesia (*Systematic Review*) [13]	2020	Nur Iman, Aris Susanto, dan Rahmat Inggi	Jurnal-jurnal penelitian mengenai *Digital forensic*.	*Systematic Review*	Hasil dari penelitian ini memaparkan tentang bagaimana perkembangan *digital forensic* di Indonesia. Kejahatan siber menjadi salah satu yang sangat banyak terjadi. Dan berdasarkan jurnal yang telah dikumpulkan pada 3 sumber *database* berbeda, terdapat 3 kejahatan yang paling banyak ditangani yaitu berkaitan dengan *Live forensic*, *network forensic*, dan *mobile forensic*. Sedangkan pada bidang *computer forensic* dan *database forensic* masih jarang dibahas berdasarkan jumlah jurnal yang ada pada ketiga *database* yang digunakan.
7.	*Forensic Cloud* Untuk Google Drive [14]	2019	Syafiq Irfan Isnaindar dan Erika Ramadhani	Google Drive	*Literature Review*	Menggunakan tiga literatur berbeda dalam penelitian ini, didapatkan bahwa tidak kejahatan peretasan *cloud drive* dapat terjadi. Pencurian data seperti gambar, video, *file* , dan lain-lain sering sekali terjadi.

No.	Judul	Tahun	Peneliti	Objek Penelitian	Metode	Hasil
						Namun kehilangan data tersebut dapat di telusuri dengan menggunakan *cloud forensic* yaitu menggunakan *tool* seperti Axiom magnet, FTK *Imager*, Oxygen *Forensic* yang masing-masing memiliki kekurangan dan kelebihan masing-masing.
8.	Metode NIST Untuk Analisis *Forensic* Bukti *Digital* pada Perangkat Android [15]	2019	Rusydi Umar dan Sahiruddin	*Smartphone* Android Samsung J1 Ace berbasis android 5.1	National Institute of Standard and Technology (NIST)	1. Menggunakan dua *tool* untuk uji coba *digital forensic* yaitu Wondershare dan Oxygen *forensic*. 2. Pengujian dilakukan dengan memasukkan *sample data* ke dalam *smartphone* yang digunakan. 3. Hasil dari kedua *tool* memiliki perbedaan di mana pada *tool* wondershare, sebanyak 30% dari total data asli yang terhapus dapat di*recovery*, sedangkan pada *tool* Oxygen *forensic*, sebanyak 73% dari total data asli yang terhapus dapat di*recovery*.

2.2 Landasan Teori

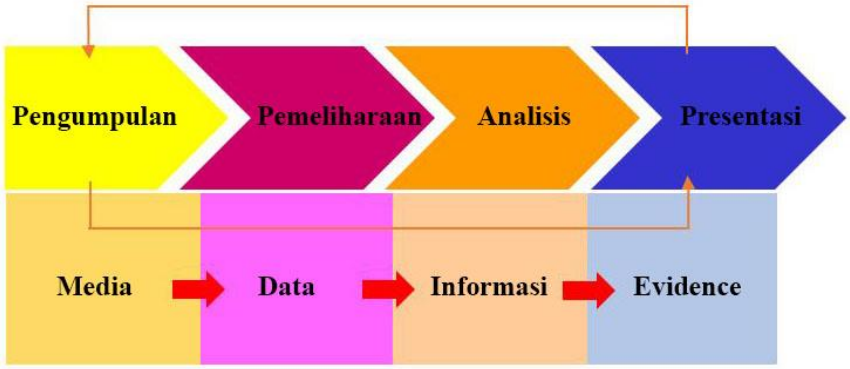
Dalam melakukan penelitian, dibutuhkan banyak landasan agar penelitian yang dilakukan menjadi sebuah penelitian yang valid, adapun landasan yang dipakai pada penelitian ini, yaitu sebagai berikut:

2.2.1 *Digital forensic*

Digital forensic adalah penggunaan ilmu dan metode untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasikan dan mempresentasikan barang bukti *digital* yang terkait dengan suatu kasus yang terjadi untuk kepentingan rekonstruksi kejadian serta keabsahan proses peradilan [15]. *Digital forensic* sendiri merupakan bidang ilmu pengetahuan yang digunakan untuk membantu sebuah proses penegakan keadilan melalui proses penerapan ilmu atau sains.

Digital forensic merupakan proses untuk menemukan barang bukti dalam bentuk *digital*, dimanah untuk mendapatkan barang bukti tersebut dibutuhkan beberapa proses dengan menggunakan berbagai alat bantu untuk investigasi. *Digital forensic* memiliki banyak cabang atau jenis berdasarkan media atau subjek investigasinya, seperti *network forensic*, email *forensic*, *mobile forensic*, dan lain-lain [15].

Proses dalam mencari barang bukti *digital* memiliki tahapan-tahapan berdasarkan metodologi yang digunakan. Metode-metode yang digunakan pun berbeda-beda seperti metode dari National Institute of Standard and Technology (NIST), *National institute of justice* (NIJ), dan *Digital Forensics Research Workshop* (DFRWS) di mana masing-masing metode memiliki tahapan berbeda dalam melakukan proses investigasi *digital forensic* [16] akan tetapi metode tersebut umumnya meliputi empat tahapan umum yang dilakukan pada *digital forensic*, adapun empat tahapan tersebut yaitu:



Gambar 2. 1 Tahapan investigasi *Forensic*

a. *Assessment*

Tahap pertama adalah tahap *assessment* atau pemeriksaan. Pemeriksaan ini meliputi penilaian terhadap bukti-bukti yang ada kemudian menggolongkannya sebagai penunjang terhadap sebuah kasus. Penggolongan yang dimaksud merupakan penggolongan apakah bukti yang ada dapat membantu meringankan atau memberatkan suatu kasus.

b. *Acquisition*

Tahap kedua adalah tahap *acquisition* atau tahap akuisisi bukti *digital*. Proses ini merupakan proses penting dikarenakan bukti *digital* sangat rentan dan mudah rusak atau bahkan hilang.

c. *Examination*

Tahap ketiga adalah tahap *examination*, tahap ini merupakan tahap di mana bukti yang sebelumnya di akuisisi kemudian di ekstrak atau dipulihkan ke dalam bentuk yang dapat dimengerti kemudian akan dijadikan barang bukti dalam sebuah persidangan.

d. *Documenting and Reporting*

Tahap keempat adalah tahap dokumentasi dan laporan. Tahap ini merupakan tahap di mana semua hasil investigasi yang berupa bukti dibuatkan dokumentasi dan laporannya

sehingga dapat di jadikan acuan oleh investigator selanjutnya [16].

2.2.2 *Mobile forensic*

Mobile forensic merupakan salah satu cabang dari *digital forensic* yang melakukan analisis untuk memperoleh bukti-bukti *digital* dari suatu perangkat seluler atau *mobile* seperti ponsel, *smartphone*, *tablet*, dan lain-lain. *Mobile forensic* dibagi menjadi beberapa jenis berdasarkan parameter tertentu yang dimiliki pada sebuah barang bukti seperti jenis ponsel, sistem operasi, *password*, dan enkripsi yang digunakan.

Dalam pelaksanaan *mobile forensic*, beberapa metode dan proses dapat digolongkan menjadi:

a. Metode manual

Metode ini umumnya dilakukan secara manual oleh seorang ahli *forensic*, di mana barang bukti berupa ponsel atau *smartphone* dipindai dan diselidiki langsung agar data pada barang bukti dapat dilihat, diakses, dan diamati langsung oleh ahli *forensic*. Namun metode ini memiliki kelemahan di mana metode ini rentan terhadap kesalahan-kesalahan yang disebabkan oleh ahli *forensic* yang menangani.

b. Metode *logical*

Metode ini merupakan cara cepat untuk mengekstrak data dari *file* yang dimiliki oleh pengguna secara langsung. Metode ini dapat dengan mudah dilakukan dengan menggunakan *tools forensic* seluler. Selain ini ukuran data hasil ekstraksi lebih kecil karena data diperoleh dari memori. Kelemahan dari metode ini yaitu rentan terhadap data yang dihapus dari perangkat hingga tidak dapat dipulihkan.

c. Metode *physical*

Metode ini langsung menggunakan *tools forensic* untuk mengekstrak data dari memori *flash* pada sebuah perangkat seluler.

Data tersebut diakses secara langsung lalu kemudian dikumpulkan, dan untuk data yang telah terhapus memiliki kemungkinan untuk dipulihkan. *Tools* yang digunakan pada proses ini merupakan *tools* tertentu yang dapat melewati beberapa sistem keamanan pada perangkat seluler.

d. Metode *file system*

Metode ini mengekstrak langsung *file system* pada sebuah perangkat seluler yang bersangkutan. Pada proses ini, data dan informasi yang ada pada seluruh aplikasi perangkat seluler juga di ekstraksi [17].

2.2.3 Cybercrime

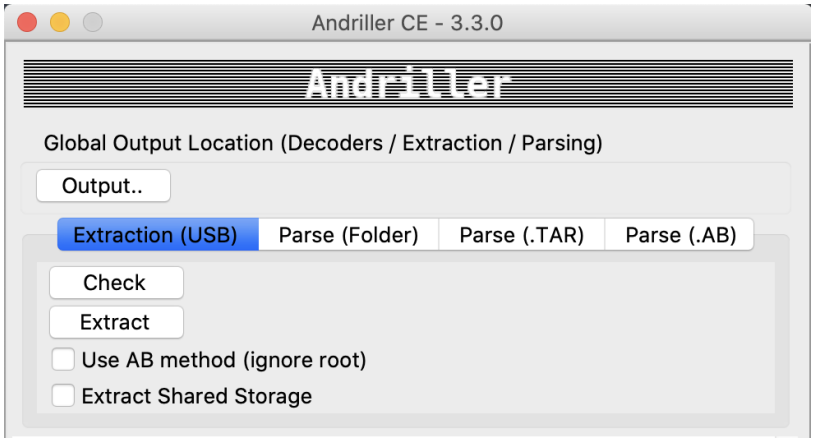
Cybercrime atau yang biasa dikenal dengan kejahatan siber merupakan suatu tindak kejahatan yang melibatkan komputer maupun perangkat jaringan dalam prosesnya. Kejahatan siber dilakukan secara *online*, dengan menargetkan siapa pun sebagai korban hingga menyebabkan suatu kerugian, bahkan dapat mempengaruhi kondisi mental dan kerugian secara finansial [18].

Kejahatan siber memiliki banyak jenis dan bentuk seperti akses ilegal terhadap sebuah sistem komputer atau servis, *cyber bullying*, konten ilegal, pemalsuan data, spionase, penipuan, kejahatan atas kekayaan intelektual yang dimiliki pihak lain di internet, dan masih banyak lagi [19].

2.2.4 Andriller

Andriller merupakan sebuah perangkat lunak yang bersifat *open-source* dengan kumpulkan alat *forensic* untuk *smartphone*. Andriller berfungsi melakukan akuisisi data secara *read-only*, dan bersifat non-destruktif dari perangkat android.

Andriller memiliki banyak fitur seperti *lockscreen cracking*, *decoder* data aplikasi, *decode database*, dan ekstraksi data ke dalam format yang dapat dibaca pada HTML format dan Excel [20].

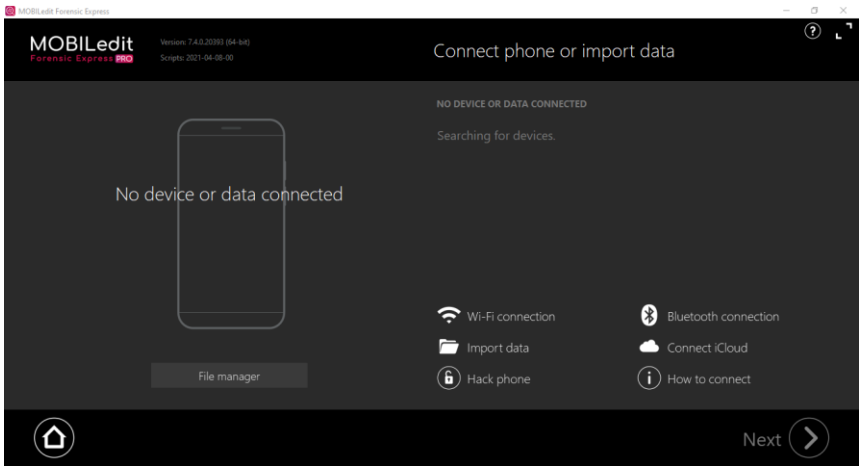


Gambar 2. 2 Tampilan Awal Andriller

2.2.5 *Mobile*dit *Forensic* Express Pro

*Mobile*dit *Forensic* merupakan perangkat lunak yang dapat digunakan untuk menjalankan suatu proses *digital forensic*. *Mobile*dit *forensic* memiliki banyak kegunaan terutama untuk melakukan ekstraksi data dari sebuah ponsel, *smartwatch*, maupun pada aplikasi atau layanan berbasis *cloud*. *Mobile*dit *forensic* menggunakan akuisisi data secara *physical* maupun *logical*, dengan analisis data, pemilihan data dengan dukungan ke berbagai perangkat.

*Mobile*dit *forensic* secara otomatis menggunakan protokol komunikasi dan teknik yang canggih untuk mendapatkan data yang maksimal dari setiap ponsel maupun sistem operasi. Hasil ekstraksi tersebut kemudian disajikan berupa laporan yang lengkap dan mudah dibaca [21].



Gambar 2. 3 *Mobile*dit Forensic Express Pro

2.2.6 *National institute of justice* (NIJ)

Metode *National institute of justice* (NIJ) merupakan metode *digital forensic* yang membagi proses *forensic* ke dalam lima tahap yaitu *identification*, *collection*, *examination*, *analysis*, dan *Report* yang secara lengkap dijelaskan sebagai berikut:

a. Identification

Proses identifikasi merupakan proses pemilihan barang bukti tindak kejahatan yang akan di tindak lanjuti untuk mendukung proses penyelidikan sebuah kejahatan *digital*. Bukti *digital* yang dipilih kemudian dilakukan proses identifikasi, pelabelan, perekaman untuk menjaga keutuhan barang bukti.

b. Collection

Tahap ini merupakan kegiatan untuk mengumpulkan data-data yang dapat mendukung proses penyelidikan untuk pencarian barang bukti kejahatan *digital*. Ditahap ini, terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari suatu perubahan yang mungkin terjadi.

c. Examination

Tahap ini juga disebut tahap pemeriksaan data yang dikumpulkan secara *forensic* baik otomatis maupun secara manual dengan memastikan data yang diperoleh berupa *file* tersebut asli dan sesuai

dengan yang didapat pada tempat kejadian kejahatan siber. Pada *file* yang bersifat *digital*, perlu dilakukan proses identifikasi berupa validasi *file* dengan teknik *hashing*.

d. Analysis

Proses ini dilakukan setelah mendapatkan *file* atau data *digital* yang diinginkan dari proses pemeriksaan sebelumnya. Data tersebut dianalisis secara mendetail dan komprehensif dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut. Hasil dari proses analisis inilah yang akan digunakan sebagai barang bukti *digital* yang dapat dipertanggung jawabkan secara ilmiah dan secara hukum.

e. Reporting

Tahap terakhir yaitu pelaporan barang bukti *digital* yang telah ditemukan melalai beberapa tahap sebelumnya. Proses pelaporan ini meliputi penggambaran tindakan yang dilakukan, *tool* yang digunakan, serta metode yang digunakan kemudian memberikan rekomendasi mengenai perbaikan kebijakan, metode, *tools* atau aspek pendukung lain pada proses *digital forensic* [16].

2.2.7 Android

Android merupakan sistem operasi yang digunakan dibanyak perangkat *mobile* seperti HP dan tablet. Android dimulai pada 2007 yang dikembangkan oleh *Open Handset Alliance* yang merupakan konsorsium yang terdiri dari 84 perusahaan, seperti di antaranya yaitu Google, Intel, Sony, dan Samsung.

Sejak diluncurkan pada tahun 2008 melalui HP pertama yang menggunakan sistem operasi android, HTC Dream, android sudah memiliki banyak versi, mulai dari android versi 1.0 hingga yang paling baru yaitu android versi 13 Tiramisu yang diperkenalkan pertama kali pada 10 Februari 2022. *Platform* android menggunakan Linux kernel sebagai dasar program.