BAB II
LANDASAN TEORI

2.1 Penelitian Sebelumnya

Penelitian terdahulu adalah sesuatu penting dalam melakukan penelitian agar dapat mengetahui hubungan antara penelitian yang dilakukan penulis dengan penelitian terdahulu yang sudah ada. Penelitian terdahulu yang pertama berjudul "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode *National Institute Of Justice* (NIJ)" oleh Imam Riadi dkk pada tahun 2018. Penulis berujuan untuk mendapatkan barang bukti digital dari kedua *smartphone* guna sebagai barang bukti elektronik dari kejahatan yang menunjukan *cyberbulling.* Metode dalam mencari bukti digital menggunakan metode NIJ (*National Institute Of Justice*). Penelitian ini, dengan menggunakan *tools* OXYGEN Forensic peneliti mendapatkan data yang dapat diakusisi seluruhnya pada media Instagram dalam *smartphone* tersebut [8].

Penelitian selanjutnya yang ditinjau adalah "Investigasi Bukti Digital Aplikasi WeChat Menggunakan *Framework Integrated Digital Forensics Proses Model* (IDFPM) Berbasis SNI 27037:2014" yang dilakukan oleh Soni, Eka Ramadhan, Desti Mualfah di tahun 2021. Penulis bertujuan untuk menjelaskan tahapan dalam proses penyelidikan bukti digital percakapan/pesan pada *WeChat* dan pencarian data dan metadata bukti digital yang ada dalam barang bukti tindak pidana, berupa ancaman menggunakan aplikasi WeChat. Metode yang digunakan dalam penelitian ini adalah *Framework Integrated Digital Forensics Proses Model* (IDFPM) Berbasis SNI 27037:2014. Penelitian ini berhasil mendeskripsikan bukti digital berupa percakapan verbal dalam aplikasi *WeChat* [9].

Maghvirna Rafika Dhewi Qibriya dkk pada penelitiannya yang berjudul "ANALISIS FORENSIK DIGITAL PADA APLIKASI INSTANT MESSAGING DI SMARTPHONE BERBASIS ANDROID UNTUK BUKTI DIGITAL" pada tahun 2021 melakukan penelitian mencari bukti digital pada aplikasi pesan WhatsApp dan Telegram. Penelitian menggunakan metode NIST (*National Institute of Standards and Technology*). Penelitian dilakukan dengan menganalisis

bukti digital pada aplikasi pesan WhatsApp dan Telegram, hasil yang didapatkan dalam penelitian ini adalah hanya bukti digital pada aplikasi pesan WhatsApp yang valid dan dapat dibuktikan validitasnya [10].

Penelitian lain, dengan judul "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode *National Institute of Standards and Technology* (NIST)" yang diteliti oleh Imam Riadi, Rusydi Umar, Muhammad Irwan Syahib pada tahun 2021. Penulis menggunakan metode NIST (*National Institute of Standards and Technology*), tujuan dilakukannya penelitian untuk pembuktian mencari bukti digital pada aplikasi Viber pada pelaku kejahatan yang telah menghapus barang bukti di akusisi kembali dengan menggunakan *tools* forensik dengan metode NIST. Hasil dari penelitian ini mendapatkan hasil penggunaan *tools* MOBILedit Forensic Express dan Belkasoft berhasil mendapatkan bukti digital [2].

Dalam penelitian "Analisis Forensik Aplikasi Dropbox pada Android menggunakan Metode NIJ pada Kasus Penyembunyian Berkas" yang diteliti oleh Saleh Khalifah dan kawan kawan pada tahun 2020, pada penelitian ini penulis membandingkan hasil dengan *tools* yang berbeda menggunakan metode NIJ. Hasil dari penelitian ini penulis mendapatkan *Tools* MOBILedit Forensik dan OXYGEN Forensik hanya dapat membaca akun pengguna media penyimpanan *Google Drive*, ekstensi lainya hanya dapat dibaca dengan tools OXYGEN Forensik [11].

Tabel 2. 1 Penelitian Sebelumnya

No	Penulis	Tahun	Judul	Metode	Persamaan	Perbedaan	Kesimpulan
1.	Imam Riadi, Anton Yudhana, Muhamad Caesar Febriansyah Putra	2018	Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode *National Institute Of Justice* (NIJ)	Metode penelitian menggunakan NIJ (*National Institute Of Justice)*	Penggunaan *Tools* dalam memperloleh bukti digital sama.	Objek yang diteliti berbeda.	Metode NIJ (*National Institute Of Justice)* dengan menggunakan *tools* OXYGEN Forensic didapatkan hasil sesuai dengan yang diinginkan yaitu bukti digital dari objek yang diteliti.
2.	Soni, Eka Ramadhan, Desti Mualfah	2021	Investigasi Bukti Digital Aplikasi WeChat Menggunakan *Framework Integrated Digital Forensics Proses Model* (IDFPM) Berbasis SNI 27037:2014	Metode penelitian menggunakan *Framework Integrated Digital Forensics Proses Model* (IDFPM) Berbasis SNI 27037:2014	Objek yang diteliti sama yaitu *WeChat.* Tools yang digunakan sama.	Metode dalam penyelidikan berbeda	Penelitian ini berhasil mendeskripsikan bukti digital berupa pesan percakapan *Cyberbullying* secara verbal pada aplikasi pesan *WeChat*.
3.	Maghvirna Rafika Dhewi Qibriya, Awalludiyah Ambarwati, Kunto Eko Susilo	2021	ANALISIS FORENSIK DIGITAL PADA APLIKASI INSTANT MESSAGING DI SMARTPHONE BERBASIS ANDROID UNTUK BUKTI DIGITAL	Metode penelitian menggunakan *National Institute of Standards and Technology* (NIST)	Metode yang digunakan sama.	*Tools* yang digunakan dalam memperloleh bukti digital berbeda.	Penelitian ini hanya berhasil mendapatkan bukti digital pada aplikasi WhatsApp.
4.	Imam Riadi, Rusydi Umar, Muhammad Irwan Syahib	2021	Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode *National*	Metode penyelidikan menggunakan	Metode penyelidikan sama. *Tools* yang digunakan dalam	Objek yang diteliti berbeda.	Analisis dengan menggunakan *tools* MOBILedit Forensic Express pada penelitian ini berhasil mendapatkan bukti digital.

No	Penulis	Tahun	Judul	Metode	Persamaan	Perbedaan	Kesimpulan
			Institute of Standards and Technology (NIST)	*National Institute of Standards and Technology* (NIST)	memperloleh bukti digital sama.		
5.	Saleh Khalifah Saad, Rusydi Umar, AbdulFadlil	2020	Analisis Forensik Aplikasi Dropbox pada Android menggunakan Metode NIJ pada Kasus Penyembunyian Berkas	Metode penelitian menggunakan NIJ (*National Institute Of Justice)*	Penggunaan *Tools* dalam memperloleh bukti digital sama.	Objek yang diteliti berbeda	*Tools* MOBILedit Forensik dan OXYGEN Forensik hanya dapat membaca akun pengguna media penyimpanan *Google Drive*, ekstensi lainya hanya dapat dibaca dengan tools OXYGEN Forensik.

2.2 Landasan Teori

2.2.1 Digital Forensik

Forensik adalah suatu kegiatan dalam investigasi dan memberikan fakta yang berhubungan dengan tindak kejadian kriminal serta permasalahan hukum lainnya [9] . Digital forensik adalah masih satu keluarga dari ilmu forensik yang berkaitan dengan bukti legal yang ditemukan di perangkat digital untuk kepentingan pembuktian hukum dalam membuktikan kejahatan digital sehingga pembuktian yang ditemukan dapat menjerat pelaku kejahatan [12].

Menurut *EC-Council* forensik digital adalah aplikasi ilmu komputer dalam pencarian hukum bagi pelaku kriminal dan sejenisnya. Digital forensik memiliki prinsip-prinsip dasar berdasarkan ACPO (*Association of Chief Police Officers*). Prinsip dasar digital forensik menurut ACPO adalah [13]:

1. Lembaga hukum dan penegak hukum dilarang untuk mengubah bukti digital atau data yang tersimpan di media penyimpanan yang dibawa ke dalam proses pengadilan [13].
2. Penyidik yang akan melakukan investigasi dalam bukti digital yang tersimpan di media penyimpanan diharuskan memiliki keahlian atau kopetensi yang jelas dan relevan dalam melakukan implikasi dari tindakan yang dilakukan terhadap barang bukti [13].
3. Pemeriksaan dalam bukti digital harus memiliki catatan teknis dan praktis terhadap Langkah-langkah yang telah diterapkan, sehingga jika pemeriksaan dilakukan oleh pihak ketiga terhadap barang bukti mendapatkan hasil yang sama [13].

2.2.2 *Mobile Forensic*

Mobile Forensic merupakan bagian dari digital forensik yang terkait dalam pemulihan bukti digital dari perangkat *mobile* menggunakan cara yang sesuai dengan kondisi forensik [10]. *Mobile Forensic* mengambil data dari perangkat *mobile* yang digunakan sebagai barang bukti. Bukti – bukti yang telah dilakukan ekstraksi berupa nomor kontak, catatan panggilan, gambar/foto, video, audio, file, dan lain-lain dapat digunakan sebagai landasan untuk menyelidiki perkara hukum

oleh pihak yang berwenang. Barang bukti berupa perangkat *mobile* dapat diekstraksi dengan tools atau software khusus dalam *mobile Forensic* seperti MOBILedit Forensic [13].

2.2.3 Bukti Digital (*Digital Evidence*)

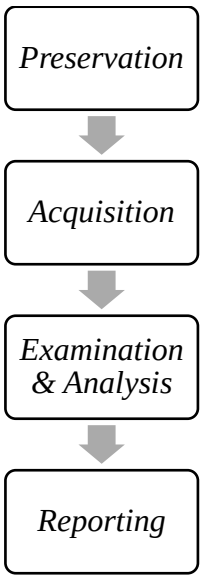
Bukti Digital (*Digital Evidence*) menurut situs NIJ (*National Institute Of Justice*) (https://nij.gov/) adalah informasi yang disimpan atau dikirimkan dalam bentuk biner yang dapat diandalkan di pengadilan. Bukti digital dapat ditemukan di penyimpanan komputer, ponsel, asisten pribadi digital (PDA), CD, dan kartu flash di kamera digital, dan tempat-tempat lainnya [14].

Kejahatan digital umumnya tidak akan jauh dari bukti digital, dengan memanfaatkan media sosial sebagai tempat dalam melakukan kejahatan. Bukti digital berisi tentang informasi yang dapat digunakan dalam membantu mengadili semua jenis kejahatan digital. Bukti digital harus ditangani dengan benar karena rentan dengan perubahan keaslianya jika tidak ditangani dengan baik. Semua jenis perubahan pada bukti digital akan memperngaruhi pada kesimpulan yang tidak valid [8].

2.2.4 NIST 800-101 R1

National Intitute Of Standards And Technology (NIST 800-101 R1) terdapat panduan untuk melakukan metode digital forensik terhadap perangkat *mobile*. NIST membuat rekomendasi sebuah metode dalam proses penanganan barang bukti digital yang dapat disajikan dalam pengadilan atau keperluan investigasi [15].

Penelitian ini menggunakan metode *National Intitute Of Standards And Technology* (NIST 800-101 R1) dengan panduan dari NIST yang berjudul "*Guidelines on Mobile Device Forensics*" yang telah diterbitkan pada tahun 2014. Panduan tersebut dikhususkan pada forensik perangkat seluler (*mobile*). Panduan ini memberikan pandangan mendalam pada perangkat seluler dan menjelaskan teknologi yang terlibat dan hubunganya dengan prosedur forensik [16].



Gambar 2. 1 Metode NIST 800-101 R1

a. *Preservation*

Tahap pertama yang dilakukan adalah *preservation* atau penjagaan. Tahap ini dilakukan dengan penjagaan perangkat yang menjadi kebutuhan untuk dilakukannya proses analisis forensik [17], seperti mempersiapkan barang bukti yang akan dianalisis, mengamankan perangkat seluler yang akan dilakukan investigasi [7]. Pengamanan data pada perangkat seluler dapat dilakukan dengan isolasi dengan cara mengaktifkan *airplane mode* pada perangkat seluler [16].

b. *Acquisition*

Tahap *Acquisition* atau akusisi, adalah proses kloning atau *imaging* terhadap data perangkat seluler yang menjadi barang bukti [16] [18]. Tujuan dilakukannya ini adalah untuk melindungi kebutuhan barang bukti sehingga dapat melakukan pemeriksaan yang mendalam lebih lanjut terhadap barang bukti tersebut [17].

c. *Examination & analysis*

Tahap *Examination & analysis* adalah pemeriksaan dan analisis dilakukan. Tahapan ini diperlukan untuk mengungkap bukti digital yang mungkin disembunyikan atau dikaburkan dalam poses analisis forensik. Proses ini berguna untuk mengidentifikasi keterkaitan suatu barang bukti dengan kasus yang sedang ditangani. Setelah dilakukan pemeriksaan, dilakukan

analisis data secara detail dan komprehensif dengan menggunakan metode yang dibenarkan secara hukum dan dapat ditarik kesimpulan data yang berkaitan dengan kasus penyidikan [18] [17].

d. *Reporting*

Tahap terakhir adalah tahap reporting atau tahap pelaporan, digunakan untuk melaporkan hasil analisis dan kesimpulan yang didapatkan dalam penyelidikan suatu kasus [16]. Tahap proses persiapan ringkasan yang terperinci atau lengkap dari keseluruhan langkah yang telah dilakukan dari proses sebelumnya dan kesimpulan yang diperoleh dalam penyelidikan suatu kasus [19].

2.2.5 Autopsy

Autopsy adalah sebuah perangkat lunak dalam proses digital forensik yang *open source* mendukung tipe file system file NTFS, FAT, Ext2/3/4, HFS/HFS+, dan UFS, untuk menyelidiki dari input (file gambar, disk local atau file logis). Autopsy memiliki antarmuka pengguna yang mudah dipahami dalam pemrosesan dan *plug in* yang digunakan dalam koleksi Sleuth Kit. Autopsy sering digunakan dalam proses digital forensik static karena aplikasi ini hanya membutuhkan citra gambar untuk menganalisisnya [20].

2.2.6 MOBILedit Forensic

MOBILedit Forensic adalah *tools* yang dikembangkan oleh *Compelson Labs* digunakan dalam penyelidikan atau pengambilan data pada *smartphone*. *Tools* ini dapat membaca pesan, membaca SIM *Card*, catatan panggilan, dan lainnya. Instalasi MOBILedit Forensic tidak terlalu sulit dilakukan. Untuk dapat menghubungkan *tools* dan *smartphone* dapat menggunakan koneksi *wireless* atau dengan kabel. MOBILedit Forensic akan menginstal aplikasi kecil di ponsel untuk menarik data. Data yang diekstrak dibatasi hanya kontak, riwayat panggilan, pesan, dan *file* [21].

2.2.7 MiChat

Aplikasi MiChat dikembangkan oleh MICHAT PTE. LIMITED dan telah diunduh lebih dari 50 juta pengguna di *PlayStore*. MiChat adalah sebuah aplikasi pesan instan gratis yang memungkinkan *user* atau pengguna saling mengirim pesan serta dapat menemukan teman baru berdasarkan lokasi terdekat. Aplikasi ini mendukung pesan dalam bentuk teks, gambar/foto, dan video [22].

2.2.8 Facebook Messenger

Facebook Messenger aplikasi seluler yang dapat digunakan untuk olahpesan yang memfasilitasi sesama pengguna Facebook aplikasi ini seperti aplikasi lainnya yang memungkinkan pengguna dapat berinteraksi dengan sesama melalui pesan teks, foto, video, dan panggilan. Facebook Messenger telah diunduh lebih dari lima milyar kali di *PlayStore* [23].