BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian sebelumnya ini menjadi salah satu sumber utama penulis untuk melakukan penelitian. Oleh karena itu, penelitian ini juga tidak lepas dari penelitian yang telah dilakukan sebelumnya yang mana berkaitan dengan pembahasan dalam penelitian ini. Berikut ini merupakan penelitian sebelumnya yang telah dipublikasikan di sejumlah jurnal dan terkait dengan penelitian penulis.

Pada penelitian pertama yang telah dilakukan sebelumnya oleh Nidiya Albarida (2020) yang berjudul "Perbandingan Analisis Forensik Digital Aplikasi Whatsapp Messenger Menggunakan Metode *National Institute Of Standards Technology* (NIST)". Pada penelitian ini disebutkan bahwa kasus prostitusi *online* yang diberitakan terjadi secara terus menerus oleh beberapa media di Indonesia, baik melalui internet, menggunakan *website* maupun jejaring sosial media seperti *Facebook, Whatsapp, Blackberry Messenger, Line Messenger* dan sebagainya. Perancangan analisis dilakukan semuanya digambarkan melalui *flowchart.* Sedangkan analisis dilakukan dengan menggunakan software *FTK Imager* dan *Whatsapp Viewer*. Hasil dari penelitian perbandingan analisis tersebut menghasilkan bahwa pengambilan data dari *Command Prompt* dan TWRP dengan software *FTK Imager* dan *Whatsapp Viewer* hasilnya sama bahwa pelaku terbukti melakukan kejahatan prostitusi *online*. Tujuan dari analisis ini dapat membantu pihak yang berkepentingan yaitu mengungkapkan kejahatan kasus prostitusi *online* dengan mendapatkan barang bukti digital yang akurat [9].

Penelitian kedua yang dilakukan oleh Rizqi Rahmansyah, Carudin, M.Kom, dan Azhari Ali Ridha, S.Kom.,MMSI (2021) yang berjudul "Perbandingan Hasil Investigasi Barang Bukti Digital Pada Aplikasi Facebook dan Instagram Dengan Metode NIST". Pada penelitian ini menjelaskan bahwa informasi yang dibagikan di media sosial tidak selalu akurat, ilmu *Mobile Forensic* diperlukan untuk

kepentingan investigasi melihat foto atau pesan teks yang dihapus yang mungkin berisi bukti digital dari orang-orang yang menyebarkan hoaks atau informasi palsu. Penelitian ini menggunakan metode NIST dimana tahapan dari metode ini terdiri dari *Collection, Examination, Analysis, Reporting*. Dalam perhitungan perbandingan persentase bukti digital penelitian ini, 75% bukti ditemukan di aplikasi Instagram, dibandingkan dengan hanya 37,5% bukti yang ditemukan di Facebook. Selain itu, hasil dari bukti digital yang dikumpulkan bergantung pada kapan prosedur forensik dilakukan setelah insiden penghapusan. [10].

Penelitian ketiga yang dilakukan oleh Wisnu A M, Siti U M, Dewi K (2017) yang berjudul "Analisa dan Perbandingan Bukti Forensik Aplikasi Sosial Media Facebook dan Twitter Pada Smartphone Android". Studi ini mencari dan membandingkan bukti dalam forensik pada platform media sosial Facebook dan Twitter, yang dapat diakses di *smartphone* Android. Twitter dan Facebook dipilih karena memiliki banyak fitur yang sama. 11 skenario yang dijalankan melalui metode simulasi yang digunakan dalam penelitian ini antara lain yaitu pengambilan file yang terhapus, pencarian bukti forensik berupa nama akun, lokasi, nomor telepon, tanggal lahir, foto profil, foto sampul, postingan berupa teks dan gambar, serta isi pesan pribadi berupa teks dan gambar. Temuan penelitian ini memperlihatkan bahwa seluruh bukti forensik ditemukan di aplikasi jejaring sosial Facebook, namun hanya akun, informasi lokasi, gambar profil, foto sampul, postingan seperti teks dan postingan berupa gambar yang ditemukan di aplikasi Twitter. [11].

Penelitian keempat yang dilakukan oleh Muhammad I S, Imam R, Rusydi U (2018) yang berjudul "Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan *Cybercrime* Menggunakan Metode Nist". Penelitian ini dilakukan menggunakan metode *National Institute of Standard and Technology* (NIST) yang dimulai dengan memasang Beetalk di dua smartphone yang sudah disiapkan, selanjutnya kami akan simulasikan obrolan antar Akun A dengan Akun B mengenai prostitusi online menggunakan smartphone Android. Setelah itu, dilakukannya proses *rooting* pada *smartphone* Android yang akan diakusisi, aplikasi kingroot

digunakan untuk proses *rooting* . Setelah itu melakukan pemilihan *tools* untuk mengambil data dari akun *Beetalk*. Pada penelitian ini *tools* yang digunakan untuk melakukan backup menggunakan *Mobiledit Forensic* sedangkan *tools* untuk tahap *Examination* menggunakan OXYGEN *Forensik*. Hasil dari penelitian ini adalah prosedur analisis dapat berfungsi dengan baik dan mendapatkan bukti digital dari aplikasi *Beetalk* pada *smartphone* Android yang digunakan sebagai objek penelitian selanjutnya. [12].

Penelitian kelima yang dilakukan oleh Yudhana, Anton Riadi, Imam Anshori, Ikhwan (2018) yang berjudul "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist". Tujuan dari penelitian ini adalah untuk menghilangkan semua jejak *cybercrime* dari *Facebook Messenger* di *smartphone* Android. Penelitian ini menggunakan metode *National Institute of Standards Technology* (NIST) lalu tools yang digunakan dalam penyelidikan ini yaitu Oxygen Forensic. Untuk memastikan bahwa setiap pemeriksa mengikuti alur kerja yang sama, NIST memberikan aturan kerja baik dalam kebijakan maupun standar. Hal ini memungkinkan untuk dokumentasi pekerjaan masing-masing pemeriksa serta hasil yang dapat di ulang dan dapat dipertahankan. Temuan penelitian ini menunjukkan bahwa *tools Oxygen Forensic* dapat mengumpulkan teks obrolan, waktu percakapan dikirim, pesan suara, dan foto, yang tidak didapatkan itu berupa video [13].

Penelitian keenam yang dilakukan oleh Muhammad Abdul Aziz, Imam Riadi, Rusydi Umar (2018) yang berjudul "Analisis Forensik Line Messenger Berbasis WEB Menggunakan Framework National Institute of Justice (NIJ)". Menurut penelitian ini, banyak pengguna perangkat lunak LINE messenger menghadapi berbagai *problem*, salah satunya adalah kejahatan dunia maya seperti perdagangan narkoba, *cyberbullying*, dan perdagangan manusia. Metode *National Institute of Justice* (NIJ) yang terdiri dari beberapa tahapan digunakan dalam penelitian ini. Tahapan tersebut adalah *Preparation, Collection, Examinition, Analysis dan Reporting*. Aplikasi LINE digunakan dalam penelitian ini merupakan versi berbasis web yang sinkronkan dengan versi Android. Hasil pada penelitian berupa log files,

bukti digital, dan cache dari simulasi kejahatan yang dikumpulkan dengan menyadap ponsel Android korban yang menjalankan program chat LINE. [14].

Penelitian ketujuh yang dilakukan oleh Syifa Riski Ardiningtias, Sunard, Herman (2021) yang berjudul "Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National Institute of Justice" Dilakukanya penelitian ini untuk mendapatkan sebuah bukti forensik tindak pidana penyebaran pornografi pada aplikasi media sosial Facebook *Messenger* yang akan diakses menggunakan aplikasi *smartphone*. Dalam penelitian ini menggunakan metode *National Institute of Justice* (NIJ) yang memberikan beberapa tahapan yaitu *tahap identification, preservation, collection, examination, analysis,* dan *presentation.* Pencarian barang bukti digital dilakukan dengan menggunakan perangkat pelaku kejahatan untuk menyebarkan pornografi dengan skenario kasus menggunakan 11 variabel yang berupa spesifikasi perangkat, akun Facebook Messenger, email, gambar, video dan audio. Hasil pada penelitian ini menunjukan Magnet Axiom lebih baik dengan akurasi 90,91% dibandingkan Belkasoft Evidence Center 46,66% [15].

Pada tabel 2.1 akan menampilkan penelitian terdahulu secara lebih jelas berupa judul, penelitian terdahulu dan penelitian yang akan dilakukan.

Tabel 2.1 Penelitian Terdahulu

No	Judul Penelitian	Perbedaan	
		Penelitian Terdahulu	**Penelitian yang akan Dilakukan**
1.	Perbandingan Analisis Forensik Digital Aplikasi Whatsapp Messenger Menggunakan Metode National Institute Of Standards Technology (NIST)	• Obyek penelitian: Whatsapp Messenger • Metode: NIST SP 800-86 • Tools: *FTK Imager* • Hasil bukti: Gambar dan teks pesan	• Obyek penelitian: *MiChat* dan *Telegram* • Metode: NIST SP 800-101 • Tools:, *Mobiledit Forensic* Express dan *FTK Imager*
2.	Perbandingan Hasil Investigasi Barang Bukti Digital Pada Aplikasi Facebook dan Instagram Dengan Metode NIST	• Obyek penelitian: Facebook dan Instagram • Metode: NIST SP 800-86 • Tools: Magnet Axiom Proccess • Hasil bukti: Berupa gambar, *caption* atau status dan pesan instan.	• Obyek penelitian: *MiChat* dan *Telegram* • Metode: NIST SP 800-101 • Tools: *Mobiledit Forensic* Express dan *FTK Imager*
3.	Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter Pada Smartphone Android	• Obyek penelitian: Facebook dan Twitter • Metode: simulasi • Tools: Wondershare Dr. Fone for Android • Hasil bukti pada aplikasi facebook: Nama akun, nomor telepon, data lokasi, tanggal lahir, cover photo, photo profile, posting berupa teks, posting berupa gambar, private message berupa gambar dan private message berupa teks. • Hasil bukti pada aplikasi Twitter: Nama akun, data lokasi, photo profile, cover photo, tweet (posting) berupa teks dan tweet (posting) berupa gambar	• Obyek penelitian: *MiChat* dan *Telegram* • Metode: National Institute Of Standards Technology • Tools: *Mobiledit Forensic* Express dan *FTK Imager*

No	Judul Penelitian	Perbedaan	
		Penelitian Terdahulu	**Penelitian yang akan Dilakukan**
4.	Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan *Cybercrime* Menggunakan Metode Nist	• Obyek penelitian: Beetalk • Metode: NIST SP 800-86 • Tools: MOBILedit Forensik dan OXYGEN Forensik • Hasil bukti: riwayat percakapan, gambar, dokumen, dan video	• Obyek penelitian: *MiChat* dan *Telegram* • Metode: NIST SP 800-101 • Tools: Penelitin saat ini menambahkan tools *FTK Imager*
5.	Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist	• Obyek penelitian: Facebook Messenger • Metode: NIST SP 800-86 • Tools: *Mobiledit Forensic* Pro • Hasil bukti: text percakapan, gambar dan audio	• Obyek penelitian: *MiChat* dan *Telegram* • Metode: NIST SP 800-101 • Tools: Penelitian saat ini menambahkan tools *FTK Imager*
6.	Analisis Forensik Line Messenger Berbasis WEB Menggunakan Framework National Institute of Justice (NIJ)	• Obyek penelitian: LINE messenger • Metode: National Institute of Justice (NIJ) • Tools: *FTK Imager* • Hasil penelitian: cache file, log dan bukti digital dari simulation tindak crime yang didapat melalui penyadapan aplikasi LINE android milik korban	• Obyek penelitian: *MiChat* dan *Telegram* • Metode: National Institute Of Standards Technology • Tools: penelitian saat ini menambahkan tools *Mobiledit Forensic*
7.	Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android	• Obyek penelitian: Facebook Messenger • Metode: National Institute of Justice (NIJ)	• Obyek penelitian: *MiChat* dan *Telegram* • Metode: National Institute Of Standards Technology • Tools: *Mobiledit Forensic* dan *FTK Imager*

No	Judul Penelitian	Perbedaan	
		Penelitian Terdahulu	**Penelitian yang akan Dilakukan**
	Menggunakan Kerangka Kerja National Institute of Justice	• Tools: Magnet Axiom dan Belkasoft Evidence Center • Hasil penelitian: spesifikasi perangkat, akun Facebook Messenger, audio, gambar, email, dan video	

2.2 Dasar Teori

2.2.1 Digital Forensik

Proses pengambilan, pemulihan, penyimpanan, dan analisis data atau dokumen elektronik dari sistem elektronik maupun media penyimpanan menggunakan alat serta metode yang didukung oleh ilmu pengetahuan untuk menggunakan data tersebut sebagai alat bukti di pengadilan dikenal sebagai digital forensik. Dalam investigasi forensik digital, kemungkinkan akan mendapatkan data yang hilang, mempelajari kapan file terakhir diubah, dan menemukan perangkat apa yang ditautkan ke komputer dan aplikasi apa yang diinstal, bahkan jika pengguna telah menghapus program tersebut. [16].

2.2.2 Bukti Digital

Bukti digital merupakakn barang bukti lanjutan yang sudah didapatkan dari bukti elektronik sebelumnya. Bukti digital sangat beragam, seiring dengan perkembangan teknologi semakin banyak aplikasi atau sistem yang digunakan untuk membantu penyelidikan. Bukti digital adalah semua file atau log yang ada pada perangkat komputer atau yang ada di media penyimpanan, contohnya seperti file dokumen yaitu doc, ppt, xls dan lainnya. Selain file dokumen ada juga terdapat beberapa jenis file yang lain seperti file audio, video, database, dan log yang ada dalam komputer tersebut [17]. Tujuan pengumpulan bukti adalah untuk membantu mengidentifikasi asal serangan, memperbaiki kerusakan yang diakibatkan serangan, dan menyajikan bukti sebagai kesaksian dalam pengandilan agar dapat memudahkan dalam mengambil keputusan [18]. Untuk mengenai alat bukti elektronik yang sah KUHAP belum mengatur secara resmi, akan tetapi untuk legalitas alat bukti elektronik terdapat dalam UU ITE yang diatur dalam BAB III tentang Informasi, Dokumentasi, dan Tanda Tangan Elektronik, serta Pasal 44 UU ITE. Pasal 5 ayat (1) mengatur bahwa Informasi dan Dokumen Elektronik merupakan perluasan dari alat bukti elektronik yang sudah diterima dalam sistem hukum pembuktian di Indonesia [19] .

2.2.3 Android

Android yaitu sebuah OS untuk perangkat mobile seperti komputer tablet dan *smartphon* yang berbasis *Linux* [20]. Agar pengguna bisa berinteraksi dengan perangkat serta menjalankan aplikasi yang sudah terinstal di dalamnya, OS dapat dianggap sebagai jembatan antara perangkat dan pengguna. Android menawarkan untuk para pengembang platform untuk membangun aplikasi yang mereka inginkan. [21].

2.2.4 *Telegram*

Penyedia layanan pesan singkat *Telegram* diperkenalkan pada tahun 2013 oleh Nikolai dan Durov. Saat berkomunikasi secara online, mengunggah file, video, dan bertukar foto, aplikasi *Telegram Messenger* menggunakan koneksi internet WiFi atau GPRS/3G/4G dan tidak membutuhkan pulsa seperti SMS [22]. *Telegram* mendukung sistem operasi *smartphone* pada *Android, iPhone/iPad, Windows Phone*, serata dapat digunakan melalui laptop dengan OS *PC/Mac/Linux, macOS* dan dapat juga melalui *Web-browser*. Tidak banyak perbedaan antara aplikasi *Whatsapp* dan *Telegram*.

Kelebihan dan kekurangan pada aplikasi *Telegram* dibandingkan dengan layanan *messenger* yang lainnya [23].

1. Kekurangan aplikasi pada *Telegram* yaitu belum memiliki fitur *voice call* dikarenakan aplikasi *Telegram* untuk saat ini masih fokus pada pengiriman pesan, segala jenis media ukuran besar, dan jenis file.
2. Kelebihan pada aplikasi *Telegram* yaitu
    a. Aplikasi tanpa biaya (tidak ada iklan)
    b. Dalam pengiriman pesan lebih cepat (berbasis *cloud*)
    c. Lebih mudah digunakan karena ukuran aplikasi lebih kecil.
    d. Dapat mentransfer file hingga ukuran 1.5 GB, termasuk foto, video,file berbentuk (doc, zip, mp3 dan lainnya)
    e. Grup dapat menampung lebih dari 200 pengguna dan dapat di tingkatkan menjadi *Supergroups* yang berkapasitas sampai dengan 5000 orang.
    f. Terdapat fitur *Channel* sebagai proses penyiaran (*broadcasting*).

2.2.5 *MiChat*

MiChat PTE Limited, yang berbasis di Singapura, membuat aplikasi *MiChat*. Di *Google Play Store*, aplikasi *MiChat* telah diunduh lebih dari 10 juta kali. Pengguna dapat terhubung satu sama lain menggunakan program perpesanan gratis *MiChat Messenger* [24]. Meskipun tampilan aplikasi ini mengingatkan pada aplikasi *WeChat*, fitur teman aplikasi *MiChat* tidak bergantung pada aplikasi *WeChat*. Ketika ada pengguna aplikasi lain di dekatnya, hingga jarak 30 km, aplikasi ini akan berfungsi. Dengan cara ini, kami dapat menentukan apakah ada pengguna *MiChat* lain yang menggunakan aplikasi di sekitar [25].

2.2.6 Metode NIST 800-101

Metode *National Institute Of Standards Technology* (NIST), merupakan kerangka kerja yang memiliki aturan standar dan praktik terbaik untuk mengelola risiko yang terkait dengan berbagai jenis ilmu pengetahuan dan teknologi informasi menjadikannya kerangka kerja yang sering digunakan [26]. Metode ini digunakan untuk menjabarkan bagaimana tahapan demi tahapan secara rinci dan sistematis, sehingga dapat menyelesaikan masalah yang ada. Tujuan dari metode ini digunakan untuk mempertahakan hasil yang didapatkan sehingga bisa dijadikan sebagai barang bukti hukum [27]. Tahapan pada metode *National Institute of Standards And Technology (NIST) Spesial Publication 800-101 Revision 1* sebagai berikut[28] :

Gambar 2. 1 *Metode NIST Spesial Publication 800-101 Revision 1*

1. *Preservation*

Pada tahapan ini akan dilakukan pengamanan terhadap ponsel atau barang bukti sesuai dengan mengikuti prosedur agar tetap menjaga keaslian data. Data ini akan dilakukan identifikasi serta pelabelan saat penelitian berlangsung.

2. *Acquisition*

Tahap ini merupakan tahapan pengumpulan data setelah dianalisis menggunakan teknik forensik baik secara otomatis maupun manual, serta

mengevaluasi dan mengeluarkan data yang diperlukan sekaligus tetap melindungi integritas data.

3. *Examination & Analysis*

Pada tahap ini agar dapat memperoleh data yang bisa digunakan sebagai barang bukti terkait kasus, maka data diperiksa dan dianalisis sesuai dengan aturan.

4. *Reporting*

Pada tahap ini hasil pemeriksaan yang didapatkan pada penyelidikan yang berisi tentang hasil analisa barang bukti dilaporkan sehingga bukti tersebut dapat membantu dalam proses penyelidikan untuk menemukan tersangka.

2.2.7 *FTK Imager*

FTK Imager (*Forensic Toolkit Imager*) merupakan produk *AcessData* yang terkenal dengan paket lengkap dikarenakan dapat mengoperasikan saat penyilidik menggunakan teknik *live* atau *static* [29]. *AccesData FTK Imager* ini dapat meng-akuisisi atau melakukan *imaging* suatu file, *direktori*, *partisi* atau *physical disk* untuk keperluan forensik. *AccesData FTK Imager* merupakan salah satu *tools live acquisition* yang dapat menjamin keaslian data [30].

2.2.8 *Mobiledit Forensic* Express

Software bernama *Mobiledit Forensic Express* digunakan untuk mengekstrak, memeriksa, dan melaporkan hasil ekstraksi data dari ponsel [31]. *Tool* ini memakai beberapa prosedur konektivitas terutama pada konektivitas nirkabel dibandingkan dengan *tool* sejenis. *Software* ini mampu mengambil data dari sistem telepon serta jenis data lainnya termasuk daftar kontak dan pesan. [32].