BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Pada penelitian ini menggunakan beberapa bahan rujukan penelitian sebelumnya yang berkaitan dengan penelitian yang akan dilakukan. Sumber rujukan tersebut dapat berupa jurnal maupun buku elektronik untuk dijadikan panduan dalam menganalisis teknik *live forensics* pada aplikasi BiP *Messenger* untuk menemukan bukti digital.

Sebuah penelitian tentang analisis forensik pada aplikasi *Telegram* yang membahas tentang artefak yang dihasilkan oleh aplikasi *Telegram* pada sistem operasi *Android* dengan 3 jenis *smartphone* yaitu *Xiaomi Redmi Note 3G, Samsung Galaxy Note II LTE*, dan *Samsung Galaxy S4*, menggunakan metode akuisisi *smartphone* yang telah di *rooting*, dan hasilnya bahwa peneliti membaca, merekonstruksi, dan memberikan uraian kronologis dari pesan pengguna [3].

Penelitian tentang analisis forensik pada *Telegram* yang membahas evaluasi informasi pada aplikasi *Instant Messenger* versi desktop pada *MacOS* menggunakan metode analisis artefak dan analisis pengetahuan terbuka, dan hasilnya adalah adalah aplikasi *Instant Messenger* yang digunakan untuk penelitian tidak menyimpan data pengguna secara lokal tetapi di *cloud* [4].

Penelitian tentang identifikasi barang bukti pada *WhatsApp* membahas proses identifikasi bukti digital percakapan aplikasi *Dual Apps WhatsApp* pada ponsel *Xiaomi* menggunakan teknik *live forensics* dan mendapatkan hasil bahwa aplikasi *Andriller* dan *Laron* tidak dapat menemukan bukti percakapan *WhatsApp* pada ekosistem *Dual Apps* dan untuk menemukannya perlu menggunakan metode manual melalui *Android Debug Bridge* (*ADB*) [5].

Penelitian selanjutnya membahas tentang pencarian bukti digital *WhatsApp* pada sistem operasi *proprietary* menggunakan teknik *live forensics* dengan mengakuisisi RAM dan mendapatkan bukti digital berupa teks dan gambar dari pengirim yang sudah dihapus untuk menghilangkan bukti digital [6].

Lalu penelitian yang membahas tentang analisis bukti digital pada *Facebook* menggunakan metode *National Institute of Standard and Technoloy (NIST)* dengan *tools Oxygen Forensics* mendapatkan hasil berupa teks percakapan, waktu percakapan dikirim, pesan *audio*, gambar, namun tidak mendapatkan bukti berupa *video* [7].

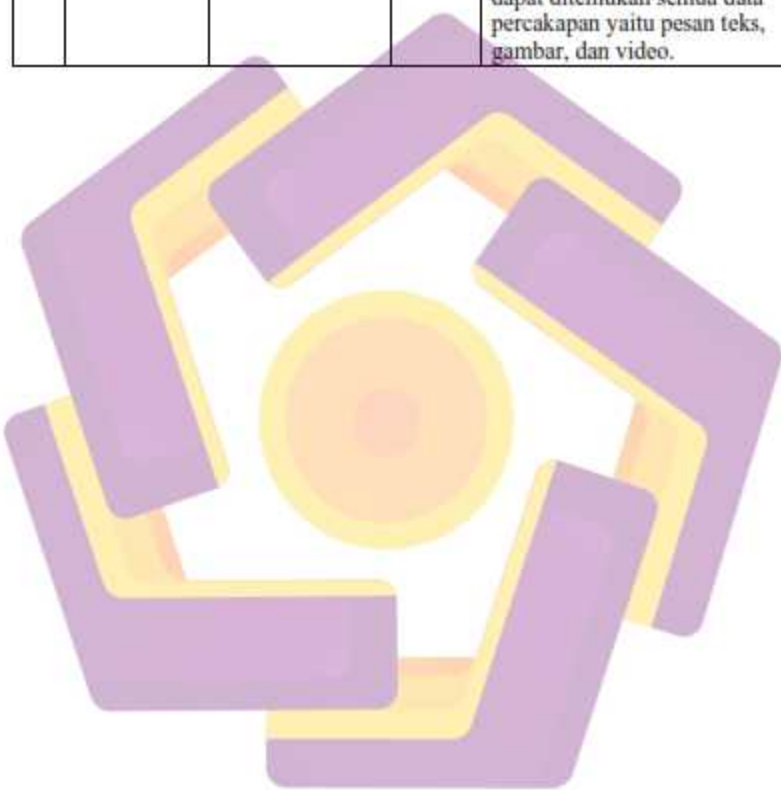
Berdasarkan hasil referensi di atas terdapat perbedaan yang akan dilakukan pada panelitian ini. Perbedaan tersebut adalah objek, metode, dan *tools* yang digunakan pada penelitian yang berjudul *"Analisis Teknik Live Forensics Pada Aplikasi BiP Messenger untuk Menemukan Barang Bukti Digital"*. Penulis menentukan penelitian terkait aplikasi BiP *messenger* untuk dianalisa dan menemukan barang bukti digital agar dapat dijadikan bukti digital dalam penyidikan yang akan diserahkan ke pengadilan. Penulis menggunakan analisis *live forensics* untuk proses pengambilan data pada *Random Access Memory* (RAM) dan hasil proses pengambilan data akan dianalisa menggunakan *WinHex* sehingga hasil bukti data digital dapat ditemukan.

Tabel 2.1 merupakan bahan rujukan yang digunakan oleh penulis dari riset sebelumnya terkait *digital forensics* pada aplikasi *Instan Messenger*.

Tabel 2. 1 List Riset Yang Telah Dilakukan

No	Peneliti	Judul	Tahun	Kontribusi Penelitian	Metode
1	Ike Yunia Pasa, Dedy Haryadi	Identifikasi Barang Bukti Percakapan Aplikasi Dual Apps Whatsapp Pada Ponsel Xiaomi Menggunakan Metode Nist Mobile Forensics	2018	Hasil penelitian yang diperoleh yaitu aplikasi *Andriller* dan *Laron* tidak dapat menemukan bukti percakapan *WhatsApp* pada ekosistem *Dual Apps* dan untuk menemukannya perlu menggunakan metode manual melalui *Android Debug Bridge* (*ADB*)	*NIST Mobile Forensics*
2	Anton Yudhana, Imam Riadi, Ikhwan Anshori	Analisis Bukti Digital Facebook Messenger Menggunakan Metode NIST	2018	Peneliti menggunakan *smartphone* pelaku tindak kejahatan untuk mendapatkan bukti digital menggunakan *tools Oxygen Forensic* dengan metode NIST. Hasil penelitian menggunakan *tools Oxygen Forensic* yang dilakukan pada smartphone tersebut adalah mendapatkan teks percakapan, waktu percakapan dikirim, pesan audio, gambar, namun tidak mendapatkan bukti berupa video.	*NIST Mobile Forensics*
3	Imam Riadi, Sunardi, Muhammad Ermansyah Rauli	Identifikasi Bukti Digital Whatsapp Pada Sistem Operasi *Proprietary* Menggunakan *Live Forensics*	2018	Hasil dari identifikasi dalam paper ini adalah kita dapat mendapatkan bukti digital berupa teks dan gambar dari pengirim yang sudah dihapus untuk menghilangkan bukti.	*Live Foresnics*
4	J. Gregorio, B. Alarcos, A. Gardel	Analisis forensik Telegram Messenger Desktop pada MacOS	2018	Karena termasuk aplikasi *desktop*, analisis forensik dilakukan berulang-kali. Aplikasi *Instant Messenger* tidak menyimpan data pengguna secara lokal tetapi di *cloud.*	Static Analysis
5	Penelitian ini	Analisis Teknik Live Forensics	2021	Mengetahui analisis *live forensics* pada BiP *messenger*	*Live Forensics*

		Untuk Menemukan Bukti Digital Pada BiP Messenger		untuk mendapatkan bukti digital. Hasil yang didapat bahwa pada percobaan 1 hanya menemukan data pesan teks sedangkan data berupa gambar dan video tidak dapat ditemukan. Pada percobaan 2 dapat ditemukan semua data percakapan yaitu pesan teks, gambar, dan video.	



2.2 Forensika Digital

Pengungkapan suatu tindak kejahatan harus dilakukan dengan melakukan forensika digital agar barang bukti digital dapat ditemukan seperti media *storage* dan digital media untuk dibawa di pengadilan [8]. Forensika komputer atau forensika digital merupakan metode atau ilmu komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, komunikasi, jaringan, dan perangkat penyimpanan elektronik [9]. Sehingga di barang bukti tersebut dapat dibawa di dalam pengadilan hukum. Ilmu forensika telah berkembang dari waktu ke waktu karena ilmu ini merupakan ilmu *modern* di dunia teknologi informasi sehingga belum banyak ahli forensika digital yang ada di Indonesia.

Digital forensics dibagi menjadi *static forensics* dan *live forensics*. *Static forensics* merupakan proses forensik untuk penyelidikan barang bukti elektronik yang diolah menjadi gambar *bit-by-bit*. Proses tersebut berlangsung pada *system* yang tidak beroperasi (*off*). Statis forensik digunakan untuk investigasi *imaging product* dan mengkaji barang bukti yang didapat, seperti *deleted files*, histori peramban, *network connection*, *accessed files*, dan histori *log in* pengguna [10].

Sedangkan *live forensics* merupakan prosedur forensik dilakukan dengan cara mengumpulkan data *volatile* (mudah hilang) dan barang bukti digital tersebut dikaji ketika *system* sedang berjalan. Metode ini memiliki tujuan agar fungsionalitas *system* tidak terpengaruh ketika melakukan analisa barang bukti sehingga, sehingga selama proses analisa digital fungsi yang dioperasikan sistem tidak terganggu [10].

Seiring dengan pesatnya perkembangan teknologi, penyalahgunaan terhadap informasi atau data elektronik juga semakin *marak* terjadi. Penyalahgunaan tersebut dapat dibawa ke pengadilan dengan adanya UU No. 11 Tahun 2008 tentang *Electronic Transaction*. Barang bukti digital atau bukti elektronik tidak dapat dihindarkan ketika sudah masuk ke pengadilan. Demi mendapatkan barang bukti elektronik tersebut, lembaga atau badan hukum harus menggunakan jasa orang-orang ahli dalam bidang komputer atau pada bidang

tertentu seperti pemrograman, jaringan, keamanan, peretasan, dan aspek lain terkait *digital forensics* [11].

2.3 Bukti digital

Bukti yang disimpan dapat berupa informasi atau data ketika proses penyidikan dilakukan. Menurut [12] bukti digital diuraikan sebagai *electronic information* yang diakumulasikan ketika investigasi atas suatu perkara seperti *online banking transaction, photos, audio, web history, e-mail,* maupun *video*.

2.4 *Live Forensics*

Live forensics merupakan metode analisis *Random Access Memory* (RAM) yang berkaitan dengan data yang terdapat pada sistem atau data *volatile* yang tersimpan pada RAM [13]. Jika sistem mati dan adanya kemungkinan tertimpanya data penting pada RAM oleh aplikasi lain, maka data *volatile* pada RAM dapat hilang sehingga butuhkan ketelitian dan kecermatan dalam teknik *live forensics*. Metode *live forensics* dapat digunakan untuk menjaga keutuhan dan orisinilitas data *volatile* tanpa menghilangkan data yang mungkin menjadi barang bukti.

Dalam sepuluh tahun terakhir teknik *live forensics* telah mengalami perkembangan seperti menganalisis isi memori untuk mendapatkan gambaran dan informasi lebih banyak tentang proses *running application* [14]. *Random Access Memory* (RAM) juga menerapkan teknik *live forensics*. Metode tersebut bertujuan agar penanganan penyelidikan memerlukan waktu yang singkat, keaslian informasi semakin terjaga, metode *encryption* yang digunakan memiliki kemungkinan dapat dibaca, serta penggunaan *memory space* dapat dikurangi daripada menggunakan teknik *traditional forensics* [15].

2.5 Tahapan Forensik

Tahapan forensik yang dilakukan penulis dalam penelitian ini adalah metode penelitian dari [16] yang menggunakan metode penelitian *National Institute of Justice* (NIJ) sebagai berikut:

a. *Identification*
b. *Collection*
c. *Examination*
d. *Analysis*
e. *Reporting*

Metode tersebut menguraikan bagaimana prosedur penelitian yang akan dilakukan sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan dengan mengetahui alur dan langkah-langkah penelitian secara sistematis.

Tahapan pertama diawali dengan *identification* yaitu melakukan identifikasi terhadap informasi digital yang membantu jalannya investigasi untuk mencari bukti digital pelaku kejahatan.

Pada proses *collection* semua barang bukti dikumpulkan untuk mendukung proses investigasi mencari bukti digital tindakan *cybercrime*. Proses ini integritas barang bukti dijaga agar tidak mengalami perubahan dan data yang diambil berasal dari sumber data yang relevan. Pada tahap *examination*, data yang dikumpulkan diperiksa secara forensik dan memastikan data tersebut otentik seperti yang ditemukan di lokasi kejadian.

Pada tahap *analysis* yaitu menganalisis data dengan lengkap. Dan tahap *reporting* yaitu hasil proses analisis dan pemeriksaan dilakukan pelaporan dan hasil analisis dijelaskan lalu informasi digital dipaparkan dan didokumentasikan dengan detail.

Lima tahapan tersebut akan diolah menjadi metodologi penelitian yang akan dijelaskan pada bagian selanjutnya.

2.7 Random Access Memory (RAM)

RAM atau *Random Access Memory* merupakan komponen penting di perangkat komputer maupun *smartphone*. Dengan RAM, sistem akan berjalan dengan cepat. RAM dapat mengakses data dengan cepat, tidak seperti *hard drive* yang lebih lambat tetapi menyediakan penyimpanan jangka panjang. Data yang terdapat pada RAM dapat dibaca dengan cepat. Dengan RAM, tindak kejahatan yang dilakukan menggunakan komputer dapat diketahui dari analisis data *volatile*.

Data *volatile* tersebut merupakan program yang menggambarkan aktivitas-aktivitas yang sedang terjadi pada program tersebut [17].

Data pada RAM dapat hilang jika dimatikan, maka penanganan data *volatile* tersebut harus ditangani dengan khusus dan hati-hati. *Tools* yang digunakan akan meninggalkan jejak yang kemungkinan dapat menimpa bukti penting yang terdapat pada memori. Banyak data yang tersimpan pada RAM seperti *network information, password and cryptography key, unencrypted content* yang dienkripsi pada disk, dan data yang di*hidden* [17].

2.8 BiP Messenger

BiP merupakan aplikasi *Instant Messenger* yang dapat digunakan pada berbagai *platfrom* seperti personal komputer, *smartphone*, dan tablet, secara gratis. BiP memiliki layanan yang mendukung pengiriman dan penerimaan beragam media seperti teks, foto, video, dokumen, lokasi, serta panggilan suara. Enkripsi yang digunakan adalah *end-to-end* sehingga pesan dan panggilan pengguna aman dan hanya penerima dan pengirim pesan yang mengetahui isi pesan tersebut, bahkan BiP tidak mengetahuinya [18].

Gambar 2. 1 BiP Messenger

2.9 Digital Forensics Tools

2.9.1. *WinHex*

WinHex merupakan *tool* yang diciptakan oleh *X-Ways Software Technology* bernama *editor hexadecimal*. *Editor hexadecimal* sangat membantu dalam bidang forensik komputer, pemulihan data, pemrosesan data *low-level*, dan keamanan IT. *Tool* tersebut dapat digunakan untuk penggunaan sehari-hari seperti

memeriksa dan mengedit semua jenis file, file yang dihapus dan data yang hilang dari *hard drive* dengan sistem file yang rusak atau dari kartu kamera digital dapat dipulihkan [19].

Gambar 2. 2 WinHex

2.9.2. *DumpIt*

DumpIt merupakan aplikasi yang digunakan untuk mendapatkan *dump* memori fisik pada *Windows*. Aplikasi ini dapat bekerja pada x84 (32-bit) dan x64 (64-bit). Terdapat pertanyaan konfirmasi sebelum *prompted* menjalankan *dump* memori [20].

Gambar 2. 3 DumpIt