BAB II
TINJAUAN PUSTAKA

2.1. Penelitian Sebelumnya

Dibawah ini peneliti menggunakan beberapa penelitian sebelumnya yang akan digunakan sebagai *studi literatur* dan referensi peneliti dalam menyelesaikan penelitian ini :

Tabel 2.1 Penelitian Terkait

No	Judul, Nama penulis, Tahun	Isi	Perbedaan dengan penelitian yang dilakukan
1.	Identifikasi Bukti *Digital* WhatsApp pada Sistem Operasi *Proprietary* Menggunakan *Live Forensics*, Imam Riadi, Sunardi, dan Muhammad Ermansyah Rauli (2018)[9].	Penelitian ini membahas bertujuan untuk menemukan bukti *digital* terkait kasus penipuan *online shop*. Bukti digital tersebut dapat diperoleh menggunakan salah satu *tools* forensik yaitu FTK Imager dan menerapkan teknik forensik digital yaitu *live forensics* pada *Random Access Memory* (RAM).	Perbedaan yang dilakukan dengan peneliti lakukan yaitu studi kasus yang diteliti.
2.	Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook Dan Twitter Pada *Smartphone* Android, Wisnu Ari Mukti, Siti Ummi Masruroh dan	Pada penelitian ini menjalankan 11 skenario diantaranya adalah pengembalian file yang dihapus, pencarian bukti *forensic* berupa nama akun, lokasi, nomor telpon,	Perbedaan dengan penelitian yang dilakukan peneliti ialah dengan mencari

No.	Judul, Nama penulis, Tahun	Isi	Perbedaan dengan penelitian yang dilakukan
	Dewi Khairani (2018)[10]	tanggal lahir, *photo profil*, *cover photo*, *posting* berupa *chat*, *posting* berupa gambar, isi *private message* berupa *chat* dan *isi private message* berupa gambar.	bukti pada *sistem* operasi windows 10 serta pada *facebook messenger web* menggunakan FTK Imager dan Metode *National Institute of Justice* (NIJ).
3.	Analisis Forensik *Digital E-Commerce* pada *Website* Rental Mobil Menggunakan Metode NIST, Gregorius Hendita Artha Kusuma dan Yusuf Fadhilah (2019)[9].	Penelitian ini membahas bagaimana mengatasi agar tidak terkena *cybercrime* pada *website* www.jetstarrental.com untuk mengatasi transaksi palsu dengan melakukan beberapa tahapan analisis *forensic*.	Perbedaan dengan peneliti lakukan ialah studi kasus dan objek yang berbeda.

No.	Judul, Nama penulis, Tahun	Isi	Perbedaan dengan penelitian yang dilakukan
4.	LINE Messenger pada *Smartphone Android* sebagai Rujukan dalam Menyediakan Barang Bukti yang Kuat dan *Valid* di Indonesia, Syukur Ikhsani dan Bekti Cahyo Hidayanto (2016)[9].	WhatsApp dan Line Messenger. Dengan melakukan eksperimen dan mendapatkan data utama berupa *database* berisikan kontak dan percakapan dan artefak *file* penyusun aplikasi.	dilakukan yaitu studi kasus dan metode investigasi yang digunakan.
5.	Analisis Investigasi Forensik WhatsApp *Messenger Smartphone* Terhadap WhatsApp Berbasis *Web*, Nuril Anwar dan Imam Riadi (2017)[9].	Penelitian ini membahas tentang eksplorasi barang bukti (*digital evidence*) percacakapan pada WhatsApp yang akan menjadi acuan akan tindak kejahatan penyadapan telekomunikasi.	Perbedaan dengan penelitian yang dilakukan peneliti ialah dengan mencari bukti pada *sistem* operasi windows 10 serta pada *facebook web* menggunakan FTK Imager dan metode *National Institute of Justice* (NIJ).

No.	Judul, Nama penulis, Tahun	Isi	Perbedaan dengan penelitian yang dilakukan
6.	Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada *Smartphone Android*, Wisnu Ari Mukti, Siti Ummi Masruroh dan Dewi Khairani (2018)[10].	Pada penelitian ini menjalankan 11 skenario diantaranya adalah pengembalian *file* yang dihapus, pencarian bukti *forensic* berupa nama akun, lokasi, nomor telpon, tanggal lahir, *photo profil*, *cover photo*, *posting* berupa *text*, *posting* berupa gambar, isi *private message* berupa *text* dan isi *private message* berupa gambar.	Perbedaan dengan penelitian yang dilakukan peneliti ialah dengan mencari bukti pada *sistem* operasi windows 10 serta pada *web* menggunakan FTK Imager dan metode *National Institute of Justice* (NIJ).
7.	Perancangan Perbandingan *Live Forensics* Pada Keamanan Media Sosial Instagram, Facebook Dan Twitter Di	Pada penelitian ini melakukan perbandingan keamanan media sosial Instagram, Facebook dan Twitter di Windows 10 dengan menggunakan metode *National Institute of Justice* (NIJ) serta mencari	Perbedaan dengan penelitian yang dilakukan dengan peneliti ialah melakukan analisis dan pencarian bukti.

No.	Judul, Nama penulis, Tahun	Isi	Perbedaan dengan penelitian yang dilakukan
7.	Windows 10, Rauhulloh Ayatulloh Khomeini Noor Bintang, Rusydi Umar dan Anton Yudhana (2018)[11].	bukti *digital* pada masing-masing media sosial dan kemudian di analisis.	*digital* pada *facebook web* dan laptop di Windows 10.
8.	Analisis *Live Forensics* Untuk Perbandingan Aplikasi *Instant Messenger* Pada Sistem Operasi Windows 10, Tayomi Dwi Larasati dan Bekti Cahyo Hidayanto (2017)[11].	Pada penelitian ini dilakukan analaisis *live forensics* untuk mendapatkan bukti *digital* pada RAM, kemudian melakukan dilakukan pengujian skenario dengan cara eksperimen berupa data percakapan biasa dan penghapusan pesan atau percapan.	Perbedaan dengan penelitian yang dilakukan yaitu studi kasus dan metode investigasi yang digunakan yaitu metode *National Institute of Justice* (NIJ).

No.	Judul, Nama penulis, Tahun	Isi	Perbedaan dengan penelitian yang dilakukan
9.	Analisis Kelayakan *Integrated Digital Forensics Investigation Framework* Untuk Investigasi *Smartphone.* Yudi Prayudi dan Imam Riadi (2016)[12]	Dalam penelitian ini menganalisi sebuah studi kasus menggunakan metode investigasi *Inetgrated Digital Forensics Investigation Framework* untuk melakukan pencarian bukti sesuai dengan skenario yang ada serta disimpulakan metode ini.	Perbedaan dengan penelitian yang dilakukan peneliti adalah objek dan *varibel* yang didapatkan berbeda. yang didapatkan berbeda.

Berdasarkan penelitian sebelumnya yang terdapat pada Tabel 2.1 peneliti mendapatkan kesimpulan yang akan digunakan dalam pelaksanaan penelitian yaitu menggunakan *tools forensic* FTK Imager, lalu menggunakan teknik forensik yaitu *Live Forensic* yang mengambil data dari memori *volatile* pada *Random Access Memory* (RAM) dan menerapakan metode *National Institute of Justics* (NIJ) dalam pencarian bukti *digital*.

2.2. Dasar Teori

2.2.1 *Digital Forensics*

Digital Forensics adalah suatu disiplin ilmu turunan keamanan komputer yang membahas tentang temuan bukti digital setelah suatu peristiwa terjadi. *Digital forensic*s dapat dibagi lebih jauh menjadi *forensics* yang terkait dengan komputer (*host, server*), jaringan (*network*), aplikasi (termasuk *database*), dan perangkat (*digital devices*) masing-masing memiliki pendalaman tersendiri[13]. Kegiatan digital *forensics* sendiri adalah suatu proses mengidentifikasi, memelihara, menganalisa dan mempergunakan

bukti *digital* menurut hukum yang berlaku. ECCouncil, *Digital forensic*s menyatakan bahwa aplikasi ilmu komputer untuk pencarian kepastian hukum bagi perbuatan kriminal dan sejenisnya. Ilmu *Digital forensics* terdapat prinsip-prinsip dasar. Prinsip dasar *Digital forensics* menurut ACPO antara lain :

1. Lembaga hukum dan atau petugasnya dilarang mengubah data digital yang tersimpan dalam media penyimpanan yang selanjutnya dibawa ke pengadilan.
2. Seseorang yang merasa perlu mengakses *data digital* yang tersimpan dalam media penyimpanan barang bukti, maka orang tersebut harus jelas kompetensi, relevansi dan implikasi dari tindakan yang dilakukan terhadap barang bukti.
3. Catatan teknis dan praktis mengenai langkah-langkah yang dilakukan terhadap media penyimpanan selama proses pemeriksaan dan analisa berlangsung, jika terdapat pihak ketiga yang melakukan investigasi terhadap media penyimpanan tersebut mendapatkan hasil yang sama. Penanggung jawab dari investigasi memiliki seluruh tanggung jawab dari keseluruhan proses pemeriksaan dan juga analisis dan dapat memastikan bahwa keseluruhan proses berlangsung sesuai dengan hukum yang berlaku.
4. Seseorang yang bertanggung jawab terhadap investigasi kasus maupun pemeriksaan dan analisis barang bukti elektronik harus dapat memastikan bawah proses yang berlangsung sesuai dengan hukum yang berlaku dan prinsip-prinsip dasar sebelumnya (prinsip 1,2 dan 3) dapat diaplikasikan dengan baik[14]

2.2.2 *Cybercrime*

Cybercrime atau tindak kriminal yang dapat disimpulkan sebagai perbuatan melawan hukum yang dilakukan dengan memanfaatkan perkembangan teknologi seperti jaringan perangkat elektronik sebagai alat atau perangkat elektronik sebagai alat, kemudian perangkat elektronik juga dapat sebagai objek untuk melakukan tindak kejahatan. Dalam memperoleh keuntungan maupun tidak, serta ada unsur untuk merugikan pihak lain.

Dalam *cybercrime* sendiri memiliki kategori, untuk mendalami apa yang dimaksud dengan *cybercrime* salah satunya adalah dengan membagi *cybercrime* menjadi 2 kelompok, yaitu : *Violent/potentially violent* dan *Non-Violent*, *Violent/potentially violent* adalah penyalahgunaan komputer yang akan berdampak secara fisik pada orang lain. Secara garis besar *cybercrime* terbagi menjadi 3 kelompok utama, yaitu:

a. *Cyberterrorism,* yaitu kegiatan yang mengarah pada aktivitas terorisme dengan memanfaatkan media *cyberspace*

b. *Cyberbullyng*, yaitu upaya untuk menimbulkan ketakutan pada diri seseorang dengan merendahkan kehormatan orang lain.

c. *Child Pornography*, kejahatan ini melibatkan tiga kelompok yaitu mereka yang terlibat untuk *create, distribute,* dan akses material pornografi.

Non-violent adalah penyalahgunaan komputer yang tidak berdampak langsung pada fisik seseorang, namun lebih pada kerugian secara sistemik. Dapat dibagi kedalam 5 kelompok, yaitu:

a. *Cybertrespass*, yaitu akses terhadap *resource* komputer secara illegal

b. *Cybertheft,* yaitu pencurian informasi atau data penting. Sejumlah aktivitas yang dapat dikategorikan dalam *cybertheft* adalah :

   1. *Emblezzlement* (penggunaan uang atau property perusahaan yang tidak seharusnya, misalnya mengubah status kepemilikan *data/transfer* secara illegal, *Industrial Espionage*, yaitu akses illegal untuk mendapatkan data-data penting perusahaan/organisasi.
   2. *Plagiarism*, yaitu pengakuan karya orang lain sebagai karya individu

3. *Privacy*, termasuk didalamnya adalah *copyright software, music, movies,* dan *book.*

c. *Identify theft,* pencurian data-data *personal* (*bank account, credit card, email*). DNS *cache poisoning*, manipulasi DNS *cache* sehingga mengganggu transmisi jaringan

d. *Cyberfraud,* umumnya berupa undangan email uuntuk bekerjasama dalam hal investasi, sosial dan pertolongan

e. *Destructive crime,* yaitu aktivitas yang berdampak pada kerusakan atau kehilangan data seperti : *virus, trojan, hacking,* DoS.

Others crime, penawaran jasa prostitusi, judi *online*, penjualan obat-obat terlarang, *money laundering,* penawaran barang-barang yang tidak lazim diperjualbelikan dalam wilayah hukum tertentu.

2.2.3 *Komputer Forensik*

Menurut Judd Robin, seorang ahli komputer forensik: "Penerapan secara sederhana dari penyelidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin". *New Technologies* memperluas definisi Robin dengan : "Komputer forensik berkaitan dengan pemeliharaan, identifikasi, ekstraksi dan dokumentasi dari bukti-bukti komputer yang tersimpan dalam wujud infromasi *magnetic*". Barang bukti yang berasal dari komputer telah muncul dalam persidangan hampir 30 tahun. Awalnya, hakim menerima bukti tersebut tanpa melakukakn perbedaan dengan bentuk lainnya. Sesuai dengan kemajuan teknologi komputer, perlakuan serupan dengan bukti tradisional akhirnya menjadi bermasalah. Bukti-bukti komputer mulai masuk kedalam dokumen resmi hukum lewat *US Federal Rules of Evidence* pada tahun 1976. Selanjutnya dengan berbagai perkembangan yang terjadi muncul beberapa dokumen hukum lainnya, antara lain adalah[15]:

1. *The Electronic Communication Privacy Act* 1986, berkatian dengan penyadapan peralatan elektronik.

2. *The Komputer Security Act* 1987 (*Public Law* 100-235), berkaitan dengan keamanan sistem komputer pemerintahan.
3. *Economic Espionage Act* 1996, berhubungan dengan pencurian rahasia dagang. Pembuktian dalam dunia maya memiliki karakteristik tersendiri. Dalam hal ini sifat alami dari teknologi komputer memunungkinkan pelaku kejahatan untuk menyembunyikan jejaknya. Karena itulah salah satu upaya untuk mengungkap kejahatan komputer adalah lewat pengujian sistem yang berperan sebagai seorang detektif dan bukannya sebagai seorang *user*. Kejahatan komputer (*Cybercrime*) tidak mengenal batas geografis, aktifivitas ini bisa dilakukan dari jarak dekat, ataupun dari jarak ribuan kilometer dengan hasil yang serupa. Penjahat biasanya selangkah lebih maju daripada penegak hukum, dalam melindungi diri dan menghancurkna barang bukti. Untuk itu tugas ahil komputer *forensic* untuk menegakkan hukum dengan mengamankan barang bukti, rekontruksi kejahatan, dan menjamin jika bukti yang dikumpulkan akan berguna di persidangan.

2.2.4 *Digital Evidence* (Bukti Digital)

Bukti digital meliputi informasi tentang komputer, *file audio*, rekaman *video*, dan gambar *digital*. Bukti ini sangat penting dalam kejahatan komputer dan *internet*, tetapi juga berharga untuk pengenalan wajah, *photo* di tempat kejadian perkara dan perekam pengawasan [16].

Penggunaan bukti *digital* telah meningkat dalam beberapa dekade terakhir sebagian pengadilan telah memungkinkan penggunaan *e-mail*, *photo digital*, dokumen pengolah kata, *history* pesan *instant*, *file* yang disimpan dari *program* akuntansi, *spreadsheet*, *history internet browser*, *database*, isi dari memori komputer, komputer *backup*, hasil cetakan komputer, trek *global positioning sistem*, *log* dari kunci elektronik sebuah hotel pintu, dan *digital video* atau *audio file*.

Bukti *digital* sangat diperlukan dalam proses persidangan, ini digunakan untuk dokumentasi pendukung karena masih banyaknya yang belum paham

pentingnya bukti *digital*, oleh karena itu yang berhak melakukan *forensic* adalah mereka yang paham dalam mengolah data, menganalisa dan menguji bukti *digital* karena akan dapat menjadi pendukung dalam kasus di persidangan.

2.2.5 *Random Access Memory* (RAM)

RAM merupakan sebuah tipe penyimpanan komputer yang isinya dapat diakses dalam waktu yang tetap tidak memperdulikan letak data tersebut dalam memori. RAM berperan penting dalam dilakukannya memori *forensic* dikarenakan *forensic* memori melibatkan penangkapan dan analisis memori *volatile* seperti RAM[17].

Penanganan data dan informasi pada RAM harus dilakukan dengan hati-hati karena data dan informasi tersebut bisa hilang jika sistem mati. Data dan informasi yang terdapat pada RAM yang berpotensi menjadi bukti *digital* bisa didapat. Upaya untuk mendapatkan bukti *digital* terkait kasus kejahatan yang terjadi dikenal sebagai *forensic digital*[9].

2.2.6 *National Institute Of Justice* (NIJ)

Salah satu metode dalam pengumpulan bukti *digital*, metode ini untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat dikehatui alur dan langkah-langkah yang akan digunakan dalam penelitian secara sistematis sehingga dalat dijadikan pedoman dalam menyelesaikan permasalahan yang ada. Tahapan metode dari *National Institute Of Justice* (NIJ) ini terbagi menjadi lima tahapan yakni *identification, collection, examination, analysis,* dan *reporting.* Penjelasan dari kelima tahapan metode ini sebagai berikut[18] :

Gambar 2. 1 Metode *National Institute Of Justice* (NIJ)

1. **Tahap *Identification* (Identifikasi)**

   Tahap *identification* atau tahap identifikasi merupakan kegiatan pemilahan barang bukti tindak kejahatan digital dan pemilahan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses identifikasi, pelabelan, perekaman untuk menjaga keutuhan barang bukti.

2. **Tahap *Collection* (Pengumpulan)**

   Tahap *collection* atau tahap pengumpulan merupakan serangkaian kegiatan mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan *digital*. Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari adanya perubahan.

3. **Tahap *Examination* (Pemeliharaan)**

   Tahap *examination* atau tahap pemeriksaan ini merupakan tahap pemeriksaan data yang dikumpulkan secara *forensic* baik secara otomatis atau manual, serta memastikan bahwa data yang didapat berupa *file* tersebut asli sesuai dengan yang didapat pada tempat kejadian kejahatan komputer, untuk itu pada *file digital* perlu dilakukan identifikasi dan *validasi file* dengan teknik *hashing*.

4. **Tahap *Analysis* (Analisis)**

   Tahap *analysis* atau tahap meneliti ini dilakukan setelah mendapatkan *file* atau data *digital* yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara *detail* dan komprehensif dengan metode yang dibenarkan secara teknik dan hukum unutk dapat membuktifkan data tersebut digunakan sebagai barang bukti *digital* serta dapat dipertanggungjawabkan secara ilmiah dan secara hukum.

5. Tahap *Reporting* (Pelaporan)

Tahap *reporting* atau tahap pelaporan dilakukan setalah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai *tools*, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, *tools*, atau aspek pendukung lainnya pada proses tindakan *digital forensic*[18].

2.2.7 *Facebook Messenger Web*

Facebook merupakan salah satu jejaring sosial yang memiliki banyak pengguna, di Indonesia sendiri pengguna *Facebook* saat ini telah digunakan hingga 130 juta orang[19]. *Facebook Messenger Web* dapat digunakan untuk melakukan perkcapakan dengan menggunakan akun *Facebook* yang sering disebut *Facebook Messenger* yang dapat melakukan percapakan dengan akun *Facebook* lainnya, *fitur* yang terdapat dalam *Facebook Messenger* yaitu dapat mengirim pesan, gambar, *audio*, *sticker* hingga *video*. Didapatkan dari laman *id-id.facebook.com* 10.294.270 suka dan 97.438 orang membicarakan aplikasi ini. *Facebook Messenger* dapat digunakan melalui *web facebook.com.*

2.2.8 FTK Imager

Access Data Forensik Tools Kit Imager atau biasa disebut "AD FTK Imager" merupakan salah satu *tools* yang digunakan dalam dunia *forensic* digital untuk melakukan sistem akuisisi data yang dikembangkan oleh perusahaan *AccessData*. Dimana sistem akuisisi itu sendiri merupakan suatu sistem yang berfungsi untuk mengambil, mengumpulkan dan menyiapkan data, hingga memprosesnya untuk menghasilkan data yang dikehendaki[8].