BAB II
TINJAUAN PUSTAKA

A. PENELITIAN TERDAHULU

Yudhana, dkk, (2018),Analisis Bukti Digital Facebook Messenger menggunakan metode *NIST. NIST* memiliki panduan kerja baik itu kebijaksanaan dan standar untuk menjamin setiap *examiner* mengikuti alur kerja yang sama sehingga pekerjaan mereka terdokumentasikan dan hasilnya dapat diulang dan dapat dipertahankan. Hasil penelitian ini *tool Oxygen forensic Detective* mendapatkan *text* percakapan, waktu percakapan dikirimkan, pesan audio, gambar.

Penelitian yang dilakukan oleh (Mustafa dkk, 2018) dengan menggunakan *National Institute of Standards and Technology* (*NIST*) dengan pendekatan *Header Analysis* menghasilkan pola pemalsuan *email* berupa subjek, alamat dan tanggal *email* yang palsu. Selain itu investigasi *email* forensik ini juga menghasilkan : 1. Alamat *email* pengirim *email* palsu; 2. Memeriksa *protocol* inisiasi pesan (HTTP, SMTP); 3. Memeriksa ID pesan; 4. Alamat IP pengirim. Aspek lain yang dapat control analisis *forensic* meliputi format penyimpanan alamat *email*, ketersediaan cadangan *email* ketika *email* tersebut dipindah dan protokol yang digunakan dalam menganalisis *email*.

Penelitian yang dilakukan oleh (Prasongko dkk,(2018)) yang menggunakan metode *NIST Mobile Forensic* dan alat-alat penelitian yang diharapkan dapat digunakan untuk melakukan analisis pada aplikasi KakaoTalk. Kemudian pada saat proses pengangkatan barang bukti digital dari *KakaoTalk* diperlukan tindakan *rooting* untuk *smartphone* Android. Bukti digital yang diharapkan dari proses pengangkatan analisis *forensic* dapat membantu proses penyelidikan suatu kejahatan digital.

Penelitian yang dilakukan oleh Imam Riadi, dkk, (2017), Analisis *forensic* digital yang digunakan pada Instagram untuk penanganan *cybercrime* menggunakan *National Institute of Standards and Technology (NIST).* Pada metode ini prosesnya diawali dengan beberapa langkah yakni, *collection, analysis,* dan *reporting.* Analisis yang dihasilkan merupakan gambaran dari semua proses

investigasi. Proses investigasi dilakukan pada perangkat pelaku menggunakan metode *NIST*.

Berdasarkan penelitian yang dilakukan oleh (Rusyidi Umar, dkk 2019) tentang analisis bukti digital pada *smartphone* android menggunakan *National Institute of Standards and Technology* (NIST) untuk menemukan bukti digital berupa data kontak, log panggilan, dan pesan yang telah di hapus pada smartphone Samsung galaxy J1 ace maka dapat disimpulkan bahwa recovery dengan *tool Wondershare* hanya mencapai 30%, sedangkan hasil *recovery* dengan *Oxygen forensik* mencapai 73% data yang terhapus dapat dikembalikan.

Penelitian yang dilakukan oleh Nasrulloh, dkk, (2017) Dalam melakukan tindakan *forensic* baik berupa langkah atau tahapan yang jelas dapat menggunakan salah satu metode dari *National Institute of Standards and Technology (NIST)* dengan rangkaian *forensic collection, examination, analysis* dan *reporting*. Analisa bukti digital juga harus memenuhi beberapa kriteria diantaranya individualitas, keterulangan, kehandalan, kinerja, kemampuan uji skalabilitas, dan standar kualitas.

Penelitian Hafid Wijaya, dkk, (2017),yang berjudul Analisis Forensik Digital Aplikasi Telegram Pada *Smartphone* Berbasis Android. Pada penelitian ini proses pengangkatan barang bukti digital dari aplikasi *Telegram* dengan menggunakan *MOBILedit Forensic Tool 7.0* dan menggunakan metode Mobile *Forensic* yang dibuat oleh *National Institute of Standard and Technology (NIST)*.

B. LANDASAN TEORI

1. Digital Forensik

Menurut Al-Azhar (2012) komputer atau digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (*pro justice)*, yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi atau *computer crime* secara ilmiah (*scientific)* hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut. Hal yang perlu di pahami seorang ahli forensik digital adalah prinsip dasarnya, dalam hal ini *ACPO* (*Association Of Chief Police Officiers)* England

Wales dan Nireland adalah suatu lembaga hukum di United Kingdom (UK) bidang penegakan hukum menyatakan bahwa prinsip-prinsip dasar sebagai berikut:

1. *Tidak ada tindakan yang diambil oleh lembaga penegak hukum atau agen mereka yank boleh mengubah data yang disimpan di media penyimpanan komputer yang selanjutkan dapat diajukan di pengadilan*
2. *Dalam keadaan dimana seseorang merasa perlu untuk mengakses data asli yang disimpan di komputer atau media penyimpanan, orang tersebut harus kompeten untuk melakukannya dan mampu memberikan bukti yang menjelaskan relevansi dan implikasi dari tindakan mereka*

2. *Oxygen* Forensik

Oxygen Forensik adalah aplikasi forensik khusus untuk mobile dengam dukungan berbagai jenil mobile *smartphone*. *Oxygen* mengextrak sebagian besar informasi dengan cara yang efisien. *Tool* ini memiliki sistem *reporting* yang baik sehingga pemeriksa bisa membaca rincian detail dari bukti yang di dapat.(Riadi dkk, (2018)

3. Android

Menurut Safaat (2011) android adalah sistem operasi untuk telepon seluler yang berbasis Linux. Android menyediakan *platform* terbuka bagi para pengembang buat menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam peranti bergerak. Awalnya, Google Inc. membeli Android Inc., pendatang baru yang membuat peranti lunak untuk ponsel. Kemudian untuk mengembangkan Android, dibentuklah *Open Handset Alliance*, konsorsium dari 34 perusahaan peranti keras, peranti lunak, dan telekomunikasi, termasuk Google, HTC, Intel, Motorola, Qualcomm, T-Mobile, dan Nvidia.

4. Facebook

Facebook adalah situs jejaring sosial yang memudahkan anda terhubung dan berbagi dengan keluarga dan teman secara online. Facebook dibangun oleh Marc Zuckerberg pada tahun 2004. Pada jejaring sosial Facebook pengguna dapat memposting komentar, berbagi foto dan link ke berita atau konten menarik lainnya di Web, seperti : bermain game, chatting dan bahkan dapat streaming video langsung. Konten bersama dapat diakes secara pubik atau hanya dapat

dibagi diantara kelompok atau teman atau keluarga, atau hanya dengan satu orang, tergantung pilihan anda. Facebook adalah jaringan sosial terbesar di dunia, dengan lebih dari 1 milliar pengguna di seluruh dunia.(Yudhana, 2018)

5. Telegram

Telegram adalah Aplikasi pesan Chatting yang memungkinkan pengguna untuk mengirimkan pesan chatting rahasia yang dienkripsi end-to-end sebagai keamanan tambahan. Dengam telegram juga dapat berbagi lebih dari sekedar gambar dan video, tetapi juga memungkinkan mentransfer dokumen atau mengirimkan lokasi kepada teman dengan mudah.Telegram merupakan aplikasi terbaik dari semua,cepat,ringan,tidak ada iklan dan gratis, telegram sangat mirip dengan Whatsapp dan bisa menjadi alternatif dari Whatsapp.(Wijaya,2016)

6. Bukti *Digital*

Riadi, et al. (2018) menyatakan bahwa bukti digital adalah informasi yang disimpan atau di kirim dalam bentuk biner yang dapat diandalkan di Pengadilan. Khusus untuk bukti digital berhubungan dengan mobile seperti *smartphone* dapat ditemukan di *call history, phonebook, SMS dan MMS, Photo, Audio, Video* dan lainlainnya. Bukti digital umumnya terkait dengan kejahatan digital seperti kejahatan yang memanfaatkan sosial media sebagai tempat melakukan kejahatan, sehingga Bukti digital digunakan untuk membantu dalam mengadili semua jenis kejahatan digital . Bukti digital sangat rentan akan perubahan sehingga dapat mempengaruhi keasliannya jika tidak ditangani dengan benar. Semua jenis perubahan yang mengandung bukti digital akan mengarah pada kesimpulan salah, atau bukti tidak akan berguna.

7. *Cybercrime*

Riadi, et al. (2018) menyatakan bahwa *cybercrime* adalah kejahatan yang menggunakan informasi teknologi sebagai target kejahatan, dan digital forensik, pada dasarnya, menjawab pertanyaan: kapan, apa, siapa, di mana, bagaimana dan mengapa terkait dengan digital kejahatan. Ada banyak jenis *cybercrime*, salah satu contohnya adalah *cyberbullying*, istilah itu mengacu pada penggunaan teknologi informasi untuk menggertak orang untuk mengirim atau memposting teks bersifat

mengintimidasi atau mengancam orang lain . Pendapat peneliti yang lain *cyberbullying* yaitu upaya untuk menimbulkan ketakutan pada diri seseorang dengan merendahkan kehormatan orang lain . Penjahat dunia maya terus mengubah strategi mereka untuk menargetkan media sosial yang berkembang pesat. Penyalahgunaan media sosial dan pesan instan dalam layanan mobile memungkinkan penjahat dunia maya memanfaatkan layanan ini untuk tujuan jahat.

8. *National Institute of Standard and Technology (NIST)*

Sugiyono (2013), Metode penelitian yang digunakan adalah metode *NIST (National Institute of Standart and Technology)*. Metode tersebut terdapat beberapa tahapan diantaranya yaitu : Pengumpulan (*Collection*), Pengujian (*Examination*), Analisa (*Analysis*), Laporan (*Reporting*). Berikut adalah gambaran untuk alur metodologinya :

a. 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 perubahan.

b. Tahap *examination* atau tahap pemeriksaan ini merupakan tahap pemeriksaan data yang dikumpulkan secara forensik 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.

c. 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 untuk dapat membuktikan data tersebut. Hasil analisis terhadap data digital selanjutnya disebut digunakan sebagai barang bukti digital serta dapat dipertanggungjawabkan secara ilmiah dan secara hukum.

d. Tahap *reporting* atau tahap pelaporan dilakukan setelah 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 tool, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, tool, atau aspek pendukung lainnya pada proses tindakan digital forensik.

9. *Mobile* Forensik

Menurut Al-Azhar (2012) forensik ini berkaitan dengan jenis barang bukti elektronik yang berupa *handphone* dan *smartphone*. Pemeriksaan ini biasanya berkaitan dengan informasi digital yang tersimpan di barang bukti tersebut. Informasi yang penting ini [contoh: *call logs* misalnya panggilan masuk (*incoming*), keluar (*outgoing)* dan tidak terjawab (*missed*); SMS (*short message service)* misalnya pesan masuk (*inbox),* keluar (*sent*), dan rancangan (*draft),* e-mail, foto (gambar digital), video; dan lain-lain] diperlukan untuk mengetahui komunikasi di antara pelaku kejahatan atau pemetaan apa yang telah dilakukan para pelaku yang berkaitan dengan kejahatanya.

10. Cloud Storage

Cloud Storages adalah layanan penyimpanan file di internet yang mana file yang disimpan disitu dapat dikelola dari mana saja selama penggunanya terhubung ke cloud storage tersebut melalui internet. Konsep cloud storages sama seperti konsep file server pada suatu kantor perusahaan, hanya saja infrastruktur media storage tersebut dikelola oleh provider cloud dan pemanfaatannya dijadikan layanan penyimpanan file yang dapat diakses dari internet. Lenawati,(2018)