BAB II
LANDASAN TEORI

2.1 Penelitian Terkait

Penelitian sebelumnya berfungsi untuk analisa serta membedakan dengan penelitian yang sedang dilakukan, penelitian ini berhubungan dengan Analisis Penanganan Barang bukti digital dan memaparkan alur penelitian yang digambarkan dalam diagram *fishbone* dan *roadmap* penelitian.

Hasil-hasil penelitian yang dilakukan oleh peneliti lain dapat juga dimasukkan sebagai pembanding dari hasil yang akan dicobakan disini (Hasibuan, 2007)

2.2 *Literatur Review*

Berdasarkan permasalahan yang telah di rumuskan, maka dibuatlah *literatur review* dari jurnal penelitian sebelumnya yang berkaitan dengan cara penanganan barang bukti digital. Tabel 2.1 merupakan penelitian yang dilakukan oleh peneliti sebelumnya mengenai penanganan barang bukti digital.

Penelitian yang telah dilakukan sebagai dasar mengenai penanganan barang bukti digital diantaranya berjudul "Penerapan Metode *National Institute Of Standards And Technology* (NIST) Dalam Analisis *Forensic Digital* Untuk Penanganan *Cyber Crime* Ditinjau Dari Aspek Hukum Yang Berlaku (Fitriana et al., 2020), pada penelitiannya berhasil mengembalikan *chat* dari *whatsapp* yang dihapus menggunakan aplikasi *whatsapp viewer*.

Penelitian yang berjudul "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap *Cybercrime*" (Riskiyadi, 2020), Hasil dari penelitianya yaitu Penggunaan *FTK Imager* dan *Autospy* mampu mengakuisisi dan menganalisis *file* yang dihapus permanen maupun *file* yang tersimpan sebelum *flash disk* diformat ulang.

Penelitian lain yang berjudul Analisis *Forensik Line Messenger* Berbasis *Web* Menggunakan *Framework National Institute Of Justice (NIJ)* (Aziz et al., 2018) Dalam penelitianya Berhasil diperoleh lokasi *file log, cache*, dan bukti digital dari simulasi tindak kejahatan yang didapatkan melalui proses penyadapan aplikasi LINE *messenger* berbasis *android* milik korban.

Buku-buku dan jurnal referensi ini dapat berisi uraian singkat atau penunjukan nama dari bacaan tertentu. Bahan acuan yang digunakan adalah jurnal-jurnal dan buku mengenai *Digital Evidence* dan *forensic digital*.

Tabel 2.1 merupakan hasil dari study *literature* yang telah dilakukan. Delapan Belas penelitian yang telah dilakukan menjelaskan mengenai bagaimana melakukan Penanganan Barang Bukti Digital. Lima dari dua belas penelitian Penanganan *Digital Evidence* pada tabel 2.1 mendekati dengan penelitian "Analisis Penanganan Barang Bukti Digital (*Digital Evidence*) Untuk Mendukung Proses Penyidikan Kasus Kejahatan Dengan Metode *National Institute Of Justice* (*NIJ*)" ditunjukkan pada tabel 2.1.

Tabel 2.1 Penelitian Terdekat

No.	Penerbit / Tahun	Judul	Masalah	Metode	*State Of The Art*
1.	Mulia Fitriana/2019	Penerapan Metode *National Institute Of Standards And Technology* (NIST) Dalam Analisis *Forensic Digital* Untuk Penanganan *Cyber Crime* Ditinjau Dari Aspek Hukum Yang Berlaku	Akuisisi data Barang bukti digital dari *Whatsapp*, untuk mengembalikan chat yang terhapus	• NIST (*National Institute of Standards and Technology*).	Mengembalikan *chat* yang terhapus menggunakan aplikasi *whatsapp viewer* kemudian menghubungkannya dengan aspek hukum.
2.	Moh. Riskiyadi/2020	*Investigasi Forensik* Terhadap Bukti Digital Dalam Mengungkap *Cybercrime*	*carding* dengan bukti *elektronik flash disk*, dilakukan penghapusan file didalamnya	Penelitian ini menggunakan *metode static forensic* dengan *framework* dari *National Institute of Justice* (NIJ)	Penggunaan *FTK Imager* dan *Autospy* mampu mengakuisisi dan menganalisis file yang dihapus permanen maupun file yang tersimpan sebelum *flash disk* diformat ulang. Sedangkan penghapusan permanen dan penggunaan *password* pada *flash disk* dengan *tools BitLocker Drive Encryption*, kedua tools tersebut tidak dapat mengakuisisi dan menganalisis file yang dihapus permanen ataupun diformat ulang

3.	Muhammad Abdul Aziz/2018	Analisis Forensik Line *Messenger* Berbasis Web Menggunakan *Framework National Institute Of Justice (NIJ)*	*Cybercrime* yang terjadi pada aplikasi line *massenger*	NIJ	Berhasil diperoleh lokasi *file log, cache*, dan bukti digital dari simulasi tindak kejahatan yang didapatkan melalui proses penyadapan aplikasi *LINE messenger* berbasis *android* milik korban.
4.	Imam Riadi/2019	Analisis *Forensik Recovery pada Smartphone Android*	proses forensik untuk mengembalikan data yang telah dihapus pada *smartphone* yang dijadikan sebagai barang bukti.	NIJ	Data yang telah dihapus pada perangkat *smartphone android* masih dapat dikembalikan menggunakan *tool Wondershare* dan *Bekasoft*
5.	Imam Riadi/2018	Analisis Forensik Digital Pada *Frozen Solid State Drive* Dengan Metode *National Institute Of Justice* (NIJ)	Mengembalikan file dalam *SSD* yang hilang setelah di *restart* pada *SSD* yang di bekukan.	NIJ	Hasil eksaminasi pada *drive* SSD yang dibekukan (*frozen drive*), menggunakan OS Forensic, file yang di scenariokan tidak di temukan. Pengujian menggunakan Autopsy, data-data yang di scenariokan ditemukan pada directory lain, ditemukan riwayat browser pada saat examinasi menggunakan *winhex*.

Tabel 2.1 merupakan tabel penelitian terdekat yang telah dilakukan sebelumnya yang berhubungan dengan analisis Penanganan barang bukti digital. Penelitian yang telah dilakukan sebagai dasar penelitian terdekat ini diantaranya berjudul "Penerapan Metode National *Institute Of Standards And Technology (NIST)* Dalam *Analisis Forensic* Digital Untuk Penanganan *Cyber Crime* Ditinjau Dari Aspek Hukum Yang Berlaku" yang dilakukan oleh Mulia Fitriana (2019) menerangkan bahwasannya Akuisisi data pada aplikasi *whatsapp* menggunakan aplikasi *whatsapp viewer* kemudian menghubungkannya dengan aspek hukum.

Tabel 2.2 matrik Penelitan

No	Peneliti/ tahun	Judul	Ruang Lingkup																						
			Framework					Aplikasi *messenger*			Media			*Tools Forensik*											
			NIST	ACPO	NIJ	DFIF	GCFIM	Whatsapp	Messenger Fb	Line	HDD	USB	SSD	*Belkasoft Evidence Center*	*FTK Imager*	*Magnet Axiom*	*Autopsy*	*Mobile edit forensic*	*Wondershare dr.phone*	*Winhex*	*Wireshark*	*Xlite*	*OS Forensic*	*Whatsapp viewer*
1	Mulia Fitriana/ 2019	Penerapan Metode *National Institute Of Standards And Technology* (NIST) Dalam Analisis Forensic Digital Untuk Penanganan *Cyber Crime* Ditinjau Dari Aspek Hukum Yang Berlaku	√					√			√	√			√										√
2	Ahwan Ahmadi/ 2019	Perbandingan Hasil Tool Forensik Pada *File Image Smartphone Android* Menggunakan Metode NIST	√											√											

3	Syifa Riski Ardiningtias/2021	Investigasi Digital Pada *Facebook Messenger* Menggunakan *National Institute Of Justice*			√				√									√	√					
4	Moh. Riskiyadi/2020	Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap *Cybercrime*			√						√	√			√		√							
5	Muhammad Abdul Aziz/2018	Analisis Forensik *Line Messenger* Berbasis Web Menggunakan *Framework National Institute Of Justice* (NIJ)			√					√	√	√			√									
6	Muh. Hajar Akbar/2019	Analisis Bukti Digital Pada Flash Disk Drive Menggunakan *Metode Generic Computer Forensic Investigation* Model (GCFIM)					√				√	√					√			√				
7	Anton Yudhana/2019	*Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method*	√								√	√				√		√						

8	Muhammad Arsad/2016	Analisis Data *Digital Evidence* pada Layanan *Voice Over Internet Protocol (VoIP)*				√															√	√		
9	Yuri V. Akay/2020	*Computer Forensics and Cyber Crime Handling*																						
10	Rizdqi Akbar Ramadhan/2021	Implementasi Metode National Institute of Justice (NIJ) Pada Fitur *Trim Solid State Drive (SSD)* Dengan Objek Eksperimental Sistem Operasi *Windows, Linux dan Macintosh*			√								√		√		√							
11	Imam Riadi/2019	Analisis Forensik *Recovery* pada *Smartphone Android* Menggunakan Metode *National Institute Of Justice* (NIJ)			√									√				√	√					
12	Muhammad sidik Asyaky/2018	Analisis dan Perbandingan Bukti Digital Aplikasi *Instant Messenger* Pada Android	√					√	√	√					√									

13	Imam Riadi/2018	Analisis Forensik Digital Pada *Frozen Solid State Drive* Dengan Metode *National Institute Of Justice* (NIJ)			√							√			√						√	√	
14	Sri Mulyani /2022	Analisis fungsi basis data berbentuk file msgstore.db.crypt dalam aplikasi *whatsapp*	√					√															
15	Mahendra Ananda Pratam/ 2017	Eksistensi hasil uji forensik digital dalam sistem pembuktian Perkara pidana																					
15	Zulkarnaen Akbar/2016	*Whatsapp forensics* pada *android smartphone: a survey*						√															
16	Ikhwan Anshori/ 2021	Analisis Barang Bukti Digital Aplikasi *Facebook Messenger* Pada *Smartphone Android* Menggunakan Metode NIJ						√															
17	Sunardi/ 2021	*Forensics Mobile* Layanan *WhatsApp*			√			√										√					

		pada *Smartwatch* Menggunakan Metode *National Institute of Justice*																					
18	Cosimo Anglano /2015	*Forensic Analysis of WhatsApp Messenger on Android Smartphones*						√							√	√							
19	Curkan Irawan/ 2022	Analisis Penanganan Barang Bukti Digital (*Digital Evidence*) Untuk Mendukung Proses Penyidikan Kasus Kejahatan Dengan Metode *National Institute Of Justice* (NIJ)			√			√				√			√									√

Tabel 2.2 Menunjukan matrik penelitian terkait penanganan *Digital Evidence* yang telah dilakukan sebelumnya. Keterbaruan dari penelitian dengan judul "analisi penanganan barang bukti digital (*digital evidence*) untuk mendukung proses penyidikan kasus kejahatan dengan metode *national institute of justice* (NIJ) menggunakan simulasi yang dilakukan pada aplikasi *whatsapp*.

2.4 Teori Pendukung Penelitian

2.4.1 Barang Bukti dan Alat Bukti

Barang bukti adalah suatu benda yang berupa fisik baik yang bergerak maupun tidak bergerak, yang berwujud maupun yang tidak berwujud yang mempunyai hubungan dengan kejadian tindak pidana. Benda-benda yang dapat disita seperti yang disebutkan dalam Pasal 39 ayat (1) KUHAP dapat disebut sebagai barang bukti (Afiah, 1989)

Menurut Undang-undang No.1 tahun 1981 tentang hukum acara pidana pasal 184 ayat 1 disebutkan bahwa alat bukti yang sah adalah:

1) Keterangan Saksi
2) Keterangan Ahli
3) Surat
4) Petunjuk
5) Keterangan Terdakwa

Kelima alat bukti tersebut digunakan oleh aparat penegak hukum dalam memeriksa dan mengungkap suatu perkara pidana. Sama halnya dengan alat bukti yang terdapat pada Pasal 5 Ayat (1) UU ITE No 11 Tahun 2008 di pasal tersebut telah dijelaskan bahwa *"Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"*.

Alat bukti sangat penting untuk mencari dan menemukan kebenaran materiil atas perkara sidang yang ditangani, dan menjaga integritas suatu alat bukti sangat dibutuhkan apalagi menyangkut barang bukti digital yang mana telah diketahui bahwa barang bukti digital mudah terkontaminasi atau bersifat *volatil*, mudah hilang atau mudah dimanipulasi.

2.4.2 Jenis Barang Bukti Digital

Keberadaan barang bukti sangat penting dalam investigasi kasus-kasus *computer crime* maupun *computer related crime* karena dengan barang bukti investigator dan *forensic analyst* dapat mengungkap kasus-kasus dengan kronologis yang lengkap, untuk kemudian melacak keberadaan pelaku dan menangkapnya. Posisi barang bukti sangat strategis, sehingga investigator dan *forensic analyst* harus paham jenis-jenis barang bukti, supaya ketika datang ke tempat kejadian perkara (TKP) yang berhubungan dengan *computer crime* dan *computer related crime*, dapat mengenali keberadaan barang bukti tersebut untuk kemudian diperiksa dan dianalisis lebih lanjut. (Army, 2020)

Klasifikasi barang bukti digital forensik menurut Ibid dalam Eddy Army (Army, 2020) adalah sebagai berikut:

a. Barang Bukti Elektronik

   Barang bukti ini bersifat fisik dan dapat dikenali secara visual, oleh karena itu investigator dan *forensic analyst* harus sudah memahami untuk kemudian mengenali masing-masing barang bukti elektronik ketika sedang melakukan proses *searching* (pencarian) barang bukti di TKP. Jenis-jenis barang bukti elektronik diantaranya, Komputer PC, *laptop/notebook, netbook, tablet, handphone, smartphone, flash disk/thumb drive, floppy disk,harddisk,cd/dvd, router, switch, hub,kamera video, cctv, digital recorder,music/video player.*

b. Barang Bukti Digital

Barang bukti ini bersifat digital yang diekstrak atau di-recover dari barang bukti elektronik. Barang bukti ini di dalam UU ITE dikenal dengan istilah Informasi Elektronik dan Dokumen Elektronik. Jenis barang bukti inilah yang harus dicari oleh *forensic analyst* untuk kemudian dianalisis secara teliti keterkaitan masing-masing file dalam rangka mengungkap kasus kejahatan yang berkaitan dengan barang bukti elektronik. Contoh barang bukti digital diantaranya, *logical file, deleted file, lost file, file slack, log file, encrypted file, steganography file, office file, audio file, video file, image file, email, user id dan password, SMS, MMS, Call Logs*

2.4.3 Definisi Barang Bukti Digital (*Digital Evidence*)

Dalam website National Institute Of Justice (www.nij.gov) pengertian bukti digital yakni informasi yang disimpan atau ditransmisikan dalam bentuk biner yang dapat diandalkan di pengadilan. Bukti digital tersebut dapat ditemukan pada *hard drive* komputer, ponsel, asisten pribadi digital (PDA), CD, dan kartu flash di kamera digital, dan tempat-tempat lainnya.

2.4.4 Karakteristik Bukti Digital

Bukti Digital tidak dapat langsung dijadikan barang bukti pada proses peradilan, karena menurut sifat alamiahnya bukti digital sangat tidak konsisten. Bukti digital dapat dijadikan barang bukti dalam proses peradilan maka diperlukan sebuah standar data digital yang dapat dijadikan barang bukti dan metode standar dalam pemrosesan barang bukti sehingga bukti digital dapat dijamin keasliannya dan dapat dipertanggung jawabkan (Watrianthos, et al., 2021).

Menurut J. Richter (Richter, Kuntze, & Rudolph, 20),ada lima karakteristik bukti digital, yaitu *Admissible* (Layak), *Authentic* (Asli), *Complete* (Lengkap), *Reliabel* (Dapat dipercaya) dan *Believable* (Terpercaya). Adapun penjelasan untuk masing-masing karakteristik adalah sebagai berikut :

a. *Admissible* (layak dan dapat diterima)

   Barang bukti digital harus sesuai dengan fakta dan masalah yang terjadi, serta barang bukti yang diajukan harus dapat diterima dan digunakan demi hukum, mulai dari kepentingan penyidikan sampai ke pengadilan.

b. *Authentic* (asli)

   Barang bukti harus mempunyai hubungan keterkaitan yang jelas secara hukum dengan kasus yang diselidiki dan barang bukti bukan hasil rekayasa. Selain itu, barang bukti digital harus dapat dibuktikan dalam pengadilan bahwa barang bukti tersebut masih asli dan tidak pernah diubah-ubah.

c. *Complete* (lengkap)

   Barang bukti harus lengkap dan dapat membuktikan tindakan jahat yang dilakukan pelaku kejahatan.

d. *Reliable* (dapat dipercaya)

   Barang bukti yang dikumpulkan harus dapat dipercaya. Pengumpulan barang bukti dan analisis yang dilakukan harus sesuai prosedur dan dilakukan dengan jujur. Barang bukti tidak boleh meragukan dan benar benar harus dapat dipercaya. Kuncinya semua harus sesuai dengan prosedur SOP (Standar Operasional Prosedur) yang berlaku.

e. *Believable* (terpercaya)

Barang bukti dan presentasi yang dilakukan di pengadilan harus dapat dimengerti oleh hakim dan dapat dipercaya. Sehngga penyampaian barang bukti di pengadilan harus menggunakan bahasa awam yang dapat dimengerti oleh hakim.

Barang bukti yang akan diajukan ke pengadilan, haruslah memenuhi kelima karakteristik tersebut untuk dapat diterima oleh hakim. Kelima karakteristik tersebut haruslah mengikuti *Chain of Custody* yang sesuai agar terpenuhi. Seperti yang telah diketahui bahwa *Chain of Custody* adalah catatan dokumentasi barang bukti, sejak barang bukti ditemukan di tempat kejadian perkara hingga sampai pada proses duplikasi dan penyimpanan barang bukti tersebut baik itu secara fisik maupun digital.

Chain of custody digunakan untuk menjaga orisinalitas atau keaslian barang bukti. Bukan hanya itu saja, *chain of custody* juga digunakan agar barang bukti yang telah didapatkan, dan dianalisis sesuai dengan prosedur dan SOP yang berlaku untuk karakteristik bukti digital *Reliable*.

Ada tiga karakteristik barang bukti yang memiliki ketergantungan dengan *chain of custody*, yaitu keaslian barang bukti, kelengkapan barang bukti, dapat dipercayanya barang bukti tersebut. History perjalanan barang bukti dari mana sampai mana, maka bisa melihat bahwa barang bukti tersebut asli, barang bukti tersebut lengkap, dan barang bukti tersebut sesuai dengan prosedur dan SOP yang ada.

2.4.5 Prosedur Penanganan Barang Bukti Digital

Prinsip dasar dan prosedur digital *forensic* memegang peranan penting untuk mengarahkan pemeriksaan digital forensic tetap berada pada jalur yang benar. Memiliki *hardware/software,* namun tidak memahami tentang prinsip dasar dan prosedur digital forensic, maka bisa jadi akan melangkah ke arah yang salah dalam pemeriksaan digital *forensic* itu sendiri. Analogi untuk hal ini adalah penggunaan senjata. Seseorang memiliki senjata yang canggih, namun tidak paham prosedur bagaimana cara menggunakannya dengan benar, maka tidak akan maksimal menggunakannya, atau malah bisa jadi senjata itu akan mencelakai dirinya atau orang lain. (Cahyadri, 2021)

Banyak guidelines di dunia internasional yang membahas hal ini, yang kebanyakan di antara mereka disponsori oleh pemerintah. Penegak hukum sebagai acuan bagi aparatnya di dalam bertindak yang benar dan prosedural di dalam melakukan investigasi *computer crime* dan *computer-related crime* serta menganalisis barang bukti. Diantara banyak *guidelines* tersebut, ada beberapa yang sering menjadi acuan para professional *digital forensic* karena diterima dan aplikatif (Cahyadri, 2021), yaitu:

a. NIJ *Forensic Examination of Digital Evidence: A Guide for Law Enforcement (*selanjutnya disebut *Framework Forensic Examination of Digital Evidence* NIJ)

Framework Forensic Forensic Examination of Digital Evidence NIJ ditujukan sebagai panduan untuk digunakan oleh aparat penegak hukum yang bertanggung jawab atas pemeriksaan bukti digital. Panduan ini tidak terkait

dengan keseluruhan aspek, tetapi hanya berkaitan dengan situasi umum yang dihadapi selama pemeriksaan bukti digital. *Framework* ini dapat digunakan sebagai panduan untuk membantu lembaga dalam mengembangkan kebijakan dan prosedur mereka sendiri.

Framework Forensic Examination of Digital Evidence NIJ, dikatakan bahwa teknologi berkembang dengan sangat pesat sehingga panduan ini paling baik disesuaikan dengan konteks teknologi dan praktik yang ada. Saat menangani bukti digital, prinsip forensik dan *procedural* umum yang harus diterapkan adalah sebagai berikut :

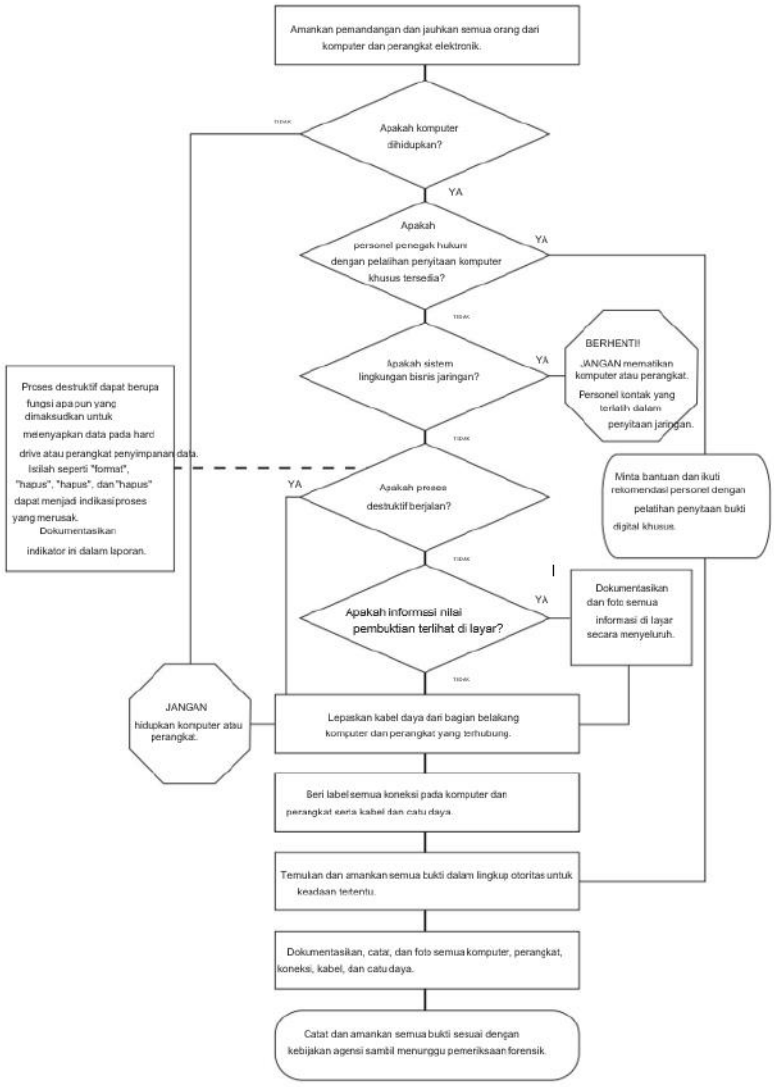
1) Tindakan yang diambil untuk mengamankan dan mengumpulkan bukti digital tidak boleh mempengaruhi integritas bukti tersebut.
2) Orang yang melakukan pemeriksaan bukti digital harus terlatih.
3) Kegiatan yang berkaitan dengan penyitaan, pemeriksaan, penyimpanan, atau transfer bukti digital harus didokumentasikan, diawetkan, dan tersedia untuk ditinjau. Setiap tahapan, *examiner* harus menyadari kebutuhan untuk melakukan pemeriksaan yang akurat dan tidak memihak terhadap bukti digital.

Framework Forensic Examination of Digital Evidence NIJ memberikan prinsip-prinsip dalam bagaimana tahapan dalam pemrosesan terhadap bukti digital, sebagai berikut :

1) Identifikasi (*Identification*). Pemeriksa forensik komputer harus menilai bukti digital secara menyeluruh sehubungan dengan ruang lingkup kasus untuk menentukan tindakan yang harus diambil.

2) Koleksi *(Collection)*. Bukti digital pada dasarnya adalah rapuh *(fragile)* dan dapat diubah, dirusak, atau dihancurkan oleh penanganan atau pemeriksaan yang tidak tepat. Pemeriksan yang paling baik adalah dilakukan pada salinan bukti asli. Bukti asli harus diperoleh dengan cara yang memberikan perlindungan dan menjaga integritas bukti.

Dalam Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition terdapat *flowchart* proses *collecting digital evidence*.



Gambar 2.1 *Flowchart collecting digital evidence*

3) Pemeriksaan (*Examination*). Tujuan dari proses pemeriksaan adalah untuk mengekstrak dan menganalisis bukti digital. Ekstraksi mengacu pada pemulihan data dari medianya. Analisis mengacu pada interpretasi data yang dipulihkan dan meletakkannya dalam format yang logis dan dapat digunakan. Pada Tahap ini dilakukan pemeriksaan bukti digital yang didapatkan melalui proses forensik dengan cara manual maupun otomatis dan untuk memastikan bukti digital yang diperoleh tersebut orisinal sama seperti yang diperoleh di tempat terjadinya kejahatan.
4) Analisis. Setelah bukti digital melewati proses *examination* selanjutnya bukti digital yang diperoleh dianalisa dengan detail menggunakan metode yang telah diakui secara ilmiah dan secara hukum agar dapat menentukan nilai signifikansi bukti digital tersebut.
5) Pelaporan (*Reporting*). setelah melalui tahap analisis dari bukti digital yang diperoleh, kemudian dilakukan reporting dari hasil analisis tersebut.

Framework Forensic Examination of Digital Evidence NIJ menerapkan lima topik yang menjelaskan langkah-langkah dasar yang diperlukan untuk melakukan pemeriksaan *computer forensics* dengan disertai saran untuk menyesuaikan dengan urutannya. Dokumentasi tertulis sebagai langkah terakhir, tetapi semestinya dokumentasi terus berlanjut selama seluruh proses pemeriksaan. Langkah-langkah yang terdapat dalam Framework ini adalah sebagai berikut :

1) Pengembangan kebijakan dan prosedur (*Policy and Procedure Development*)

Bagian ini lebih condong kepada segi manajemen dari badan yang menaungi *Digital Forensics*, termasuk juga personel yang harus dilatih secara khusus,

dukungan dana, membangun program pelatihan yang tepat, serta pengembangan teknik-teknik terkait penanganan bukti digital yang baik oleh karenanya dibutuhkan pengembangan kebijakan dan prosedur.

2) Evidence Assesment

Proses ini prosedur yang ditetapkan adalah melakukan pemeriksaan menyeluruh dengan melihat surat perintah penggeledahan atau otoritas hukum lainnya, detail kasus, perangkat keras dan perangkat lunak, bukti potensial yang dicari, dan keadaan yang melingkupi akuisisi bukti yang akan diperiksa.

Dijelaskan bahwa dalam melakukan penilaian terhadap kasus diperlukan :

a. Peninjauan terhadap permintaan penyelidik;
b. Berkonsultasi dengan penyidik tentang kasus tersebut dan beritahu apa yang memungkinkan atau yang tidak mungkin untuk ditemukan oleh pemeriksaan *forensic*.

3) Akuisisi bukti (*Evidence Acquisition)*

Framework Forensic Examination of Digital Evidence NIJ memberikan prinsip bahwa bukti digital pada dasarnya bersifat rapuh dan dapat diubah, dirusak, atau dihancurkan dengan penanganan atau pemeriksaan yang tidak tepat. Dibutuhkan tindakan pencegahan khusus untuk mengamankan bukti elektronik. Kegagalan untuk melakukan tindakan pengamanan tersebut dapat membuat bukti elektronik tidak dapat digunakan atau menghasilkan kesimpulan yang tidak akurat. Prosedur yang dilakukan adalah mendapatkan bukti digital asli dengan cara memberikan perlindungan dan pengamanan terhadap bukti digital.

4) Pemeriksaan bukti (*Evidence Examination*)

Framework Forensic Examination of Digital Evidence NIJ memberikan prinsip forensik yang berlaku umum saat memeriksa bukti digital, yaitu :

a) Jenis kasus dan media yang berbeda kemungkinan memerlukan metode pemeriksaan yang berbeda.
b) Orang yang melakukan pemeriksaan bukti digital harus dilatih untuk tujuan tersebut.

Saat melakukan pemeriksaan bukti, pertimbangan untuk melakukan langkah-langkah berikut :

- Persiapan
- Ekstraksi
- Analisis data yang diekstraksi
- Kesimpulan

5) Pendokumentasian dan pelaporan (*Documenting and Reporting*)

Framework Forensic Examination of Digital Evidence NIJ memberikan prinsip bahwa pemeriksa bertanggung jawab untuk melaporkan temuannya serta hasil analisis pemeriksaan bukti digital yang akurat dan lengkap. Dokumentasi adalah proses yang berkelanjutan selama pemeriksaan untuk mencatat secara akurat langkah-langkah yang diambil selama pemeriksaan bukti digital.

Prosedur yang ditetapkan adalah bahwa semua dokumentasi harus lengkap, akurat dan komprehensif seperti :

- Catatan pemeriksa
- Laporan pemeriksa
- Ringkasan temuan
- Rincian temuan
- Bahan pendukung
- Glosarium

b. ***ACPO Good Practice Guide for Digital Evidence***

ACPO Good Practice Guide for Digital Evidence digunakan sebagai panduan tentang Best Practice dalam penanganan bukti digital yang diadopsi dan digunakan oleh kesatuan polisi di Inggris, Wales, dan Irlandia Utara. Panduan ini ditujukan sebagai pedoman untuk personel penegak hukum di Britania Raya ketika berurusan dengan bukti digital.

Prinsip-prinsip Bukti Digital dalam *ACPO Good Practice Guide for Digital Evidence* adalah :

1) Lembaga penegak hukum , orang yang bekerja didalamnya, atau personel tidak diperbolehkan melakukan sesuatu yang dapat mengubah data untuk kemudian digunakan di persidangan.
2) Keadaan di mana dianggap perlu untuk mengakses data asli, maka orang tersebut haruslah orang yang kompeten untuk melakukannya dan mampu memberikan bukti yang menjelaskan relevansi dan implikasi dari tindakannya (mengakses data asli).
3) Audit Trail dan catatan lain atas semua proses yang diterapkan kepada bukti digital harus dibuat dan disimpan. Pihak ketiga harus independen dapat memeriksa proses tersebut dan mencapai hasil yang sama.
4) Orang yang bertanggung jawab atas investigasi memiliki tanggung jawab secara keseluruhan untuk memastikan bahwa hukum dan prinsip-prinsip ini ditaati.

Gambar 2.2 Tahapan kerangka kerja ACPO

Tahapan-tahapan dalam *ACPO Good Practice Guide for Digital Evidence* adalah perencanaan (*Plan*), perolehan (*Capture*), Analisis (*Analyse*), dan menghadirkan bukti (*Present*).

c. Prinsip Dan Prosedur Dasar Penanganan Bukti Digital Dalam Computer *Crime* Dan *Compute Related Crime*

Menurut Muhammad Nuh Al-Azhar (Al-Azhar, 2012), proses penanganan awal barang bukti dalam digital forensic di TKP sebagai berikut :

a) *Preparations* (persiapan)

Sebelum ke TKP untuk melaksanakan penggeledahan kasus yang berkaitan dengan barang bukti elektronik, maka analisis forensic dan investigator terlebih dahulu menyiapkan hal-hal atau peralatan yang nantinya dibutuhkan selama proses penggeledahan di tempat kejadian.

Sesuatu yang harus dipersiapkan dan dimiliki oleh analisis forensic dan investigator adalah :

- Administrasi penyidikan : seperti surat perintah penggeledahan dan surat perintah penyitaan.
- Kamera digital : digunakan untuk memotret TKP dan barang bukti secara *fotografi forensic* (foto umum, foto menengah dan foto *close up*).

- Peralatan tulis : untuk mencatat antara lain spesifikasi teknis komputer dan keterangan para saksi.
- Nomor, skala ukur, label lembaga, serta *stiker label* kosong : untuk menandai masing-masing barang bukti elektronik yg ditemukan di TKP.
- Formulir penerimaan barang bukti : digunakan untuk kepentingan *chain of custody* yaitu metodologi untuk menjaga keutuhan barang bukti dimulai dari tkp.
- *Triage tools :* digunakan untuk kegiatan *triage forensik* terhadap barang bukti komputer yang ditemukan dalam keadaan hidup (*on*).

b) Identifikasi Bukti Digital (*Identification/Collecting digital evidence*)

Tahapan yang dilakukan untuk identifikasi, dimana bukti itu berada, dimana bukti itu disimpan, bagaimana penyimpanannya dan mengumpulkan data sebanyak mungkin untuk mempermudah penyidikan

c) Penyimpanan Bukti Digital (*Preserving digital evidence*)

Bentuk dan isi bukti digital hendaknya disimpan dalam tempat yang steril. Untuk benar-benar memastikan tidak ada perubahan-perubahan, hal ini vital untuk diperhatikan. Karena sedikit perubahan saja dalam bukti digital, akan merubah juga hasil penyelidikan. Bukti digital secara alami bersifat sementara (*volatile*), sehingga keberadaannya jika tidak teliti akan sangat mudah sekali rusak, hilang, berubah, atau mengalami kecelakaan.

d) Menetapkan Data (*Confirming*)

Serangkaian kegiatan untuk menetapkan data-data yang berhubungan dengan kasus yang terjadi.

e) Mengenali Data (*Identifying*)

Serangkaian kegiatan untuk melakukan proses identifikasi terhadap data-data yang sudah ada agar memastikan bahwa data tersebut memang unik dan asli sesuai dengan yang terdapat pada tempat kejadian perkara.

2.4.6 *Data Recovery*

Data Recovery merupakan proses mengembalikan data dari kondisi yang rusak, gagal, atau tidak bisa diakses ke kondisi awal yang normal. *Data recovery* merupakan bagian penting dari analisis forensik yang harus dilakukan untuk mengetahui apa yang telah terjadi, dan mengambil kembali file data yang telah terhapus sebelumnya. (TIM, 2009)

2.4.7 *FTK Imager*

FTK (*forensic ToolKit*) merupakan salah satu *tools* forensik yang dapat membantu melakukan pengujian forensik yang baik di *system* operasi *windows*. *FTK* menyediakan penyaringan file dan fungsi search dan juga analisis *email*. Untuk memastikan kalau file yang dipakai bekerja belum berubah, penyidik bisa membandingkan suatu *hash* dari *file* asal dengan *file image*. *Hashing* ini akan memberikan suatu validitas matematis, sehingga suatu *image forensik* harus sesuai dengan yang aslinya. (Utdrartatmo, 2005)

2.4.8 *Whatsapp*

WhatsApp Messenger adalah aplikasi pesan untuk ponsel cerdas. *WhatsApp Messenger* merupakan aplikasi pesan lintas platform yang memungkinkan kita bertukar pesan tanpa pulsa, karena *WhatsApp Messenger* menggunakan paket data

internet. Aplikasi *WhatsApp Messenger* menggunakan koneksi internet 3G, 4G atau WiFi untuk komunikasi data. (AAT, 2010)

2.4.9 *Whatsapp Viewer*

Whatsapp Viewer adalah alat kecil yang dapat digunakan untuk membaca semua pesan dalam data penyimpanan sangat cepat dan semua pesan dapat dibaca tanpa proses dekripsi terlebih dahulu, hanya dengan database dan kunci *Whatsapp* diperoleh dari *smartphone* maka pesan *Whatsapp* akan terbaca semua. (Rahim, Siahaan, Manikandan, & Aryza, 2018)