BAB II

LANDASAN TEORI

2.1 Digital Forensik

Forensik digital adalah penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti/informasi yang disimpan/dikodekan pada komputer atau media penyimpanan digital sebagai bukti dalam kasus pidana yang sah (Saputra, 2017).

Pengertian forensik digital adalah penerapan ilmu dan teknologi informasi untuk pembuktian hukum, yang dalam hal ini terdiri dari pembuktian kejahatan yang dilakukan dengan perangkat komputer untuk mendapatkan bukti digital yang dapat digunakan untuk menangkap pelakunya (Kiswanto, 2014).

2.2 *Autopsy*

Autopsy merupakan program yang dapat mengetahui informasi tersembunyi dalam suatu file, termasuk tanggal pembuatan, perubahan akses dan penghapusan suatu file. Aplikasi ini menawarkan alur kerja yang mudah dipahami untuk pengguna di bidang penegakan hukum, militer, intelijen, keamanan *cyber*, dan pemeriksa bisnis. Semua yang dibutuhkan oleh aplikasi ini adalah gambar disk dari perangkat yang akan dianalisis (Riski Ardiningtias, 2021).

2.3 National Institute of Justice *(NIJ)*

Penggunaan metode penelitian ini mengadaftasi dari metode analisis forensik dari *National Institute of Justice* (NIJ). Metode ini digunakan untuk menjelaskan

bagaimana tahapan penelitian yang dilakukan sehingga alur penelitian bisa selesai secara sistematis dan dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada. Menurut Roni Anggara disebutkan melakukan teknik forensik dan analisis forensik berdasarkan metode yang benar akan memiliki keberhasilan hampir 100% dalam mengumpulkan data forensik (Riadi et al., 2017).

Tahapan metode dari *National Institute of Justice* (NIJ) ini terbagi menjadi lima tahapan yakni *identification, collection, examination, analysis, dan reporting* (Faiz et al., 2017), secara lengkap dipaparkan sebagai berikut:

1. Tahap *Identification*

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. Tahap ini merupakan proses identifikasi, pelabelan, perekaman, untuk menjaga keutuhan barang bukti.

2. Tahap *Collection*

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

3. Tahap *Examination*

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.

4. Tahap *Analysis*

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.

5. Tahap *Reporting*

Tahap *reporting* atau tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Tahapan 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 forensic.

2.4 *Digital Evidence*

Merupakan sebuah istilah yang merujuk untuk sebuah data yang disimpan maupun dikirimkan melalui *Devices* tertentu, seperti personal computer (PC), laptop, smartphone dsb (Riadi, 2017). Bukti digital ini bersifat *volatile*, rapuh dan mudah terjadinya alterasi. Jika tidak diproses dengan cara yang tepat, alterasi yang terjadi pada bukti tersebut akan mengarah pada integritas bukti itu sendiri. Dan pada akhirnya bukti tersebut akan tidak berguna karena tidak valid menurut hukum (J. Sammons, 2015).

2.5 *Ftk Imager*

Ftk Imager adalah sebuah aplikasi yang digunakan dalam dunia forensik digital untuk mengoperasikan sistem akuisisi data yang dikembangkan oleh perusahaan Access Data. Sistem pengumpulan data itu sendiri merupakan suatu sistem yang bertugas untuk mengambil, mengumpulkan dan menyiapkan informasi serta mengolahnya untuk menghasilkan informasi yang diinginkan.

2.6 Checksum

checksum adalah nilai numerik yang dihasilkan dari suatu algoritma *checksum* yang digunakan untuk memverifikasi integritas data dan metode yang digunakan untuk mendeteksi kesalahan atau perubahan data yang terjadi selama transmisi atau penyimpanan. *Checksum* sering digunakan dalam berbagai aplikasi seperti protokol komunikasi jaringan, *transfer file*, penyimpanan data, dan lainnya. Algoritma *checksum* yang umum digunakan meliputi CRC (*Cyclic Redundancy Check*), MD5 (*Message Digest 5*), SHA-1 (*Secure Hash Algorithm 1*), dan SHA-256 (*Secure Hash Algorithm 256*).

2.7 Penelitian Terkait

Tabel 2. 1 Penelitian Terkait

No	Peneliti	Metode dan *Tools*	Judul Penelitian	Hasil Penelitian
1	Riski Yudhi Prasongko, Anton Yudhana, Abdul Fadil (2018)	*National Institute of Standard Technology (NIST)* dan *tools MobilEdit Forensic*	Analisa Forensik Aplikasi *Kakaotalk* menggunakan Metode *National Institute of Standard Technology (NIST)*	Mengetahui barang bukti digital pada kasus *Cybercrime*
2	Mulia Fitriana, Khairan AR, Jiwa Malem Marsya (2020)	*National Institute of Standard Technology (NIST)* dan *tools FTK Imager*	Penerapan Metode *National Institute of Standard Technology (NIST)* dalam analysis forensic digital untuk penaganan *Cybercrime*	Mengetahui barang bukti digital pada kasus *Cybercrime*
3	Imam Riadi, Anton Yudhana,Muhamad Caesar Febriansyah Putra (2017)	*National Institute of Standard Technology (NIST)* dan *tools Oxygen Forensic*	Analisis *Recovery* bukti digital *Instagram Messengger* menggunakan metode *National Institute of Standard Technology (NIST)*	Mengetahui barang bukti digital pada kasus *Cybercrime*
4	Anton Yudhana, Rusydi Umar, Ahwan Ahmadi (2019)	*National Institute of Standard Technology (NIST)* dan *tools MobilEdit Forensic*	*Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method*	Mengetahui barang bukti digital pada kasus *Cybercrime*
5	Saleh Khalifa Saad, RusydiUmar, Abdul Fadlil (2020)	*National Institute of Standard Technology (NIST)* dan *tools*	Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode *NIST*	membandingkan direktori dan database dibuat dari aktivitas-aktivitas tersebut
6	Mustafa, Imam Riadi, Rusydi Umar (2018)	*National Institute of Standard Technology (NIST)* dan *tools Aid4Mail Forensic*	Rancangan Investigasi Forensik *E-mail* Dengan Metode *National Institute*	Mengetahui aktivitas pengiriman *E-mail* palsu

			of Standard Technology (NIST)	
7	Rusydi Umar, Sahiruddin (2019)	*National Institute of Standard Technology (NIST)* dan *tools Wondershare dr. Fone for Android, Oxygen Forensic Suite 2014*	Metode *NIST* Untuk Analisis Forensik Bukti Digital Pada Perangkat Android	Mengetahui barang bukti digital pada kasus *Cybercrime*
8	Gregorius Hendita Artha Kusuma, Yusuf Fadhilah (2019)	*National Institute of Standard Technology (NIST)*	Analisis Forensik Digital *E-Commerce* pada *Website* Rental Mobil Menggunakan Metode *NIST*	Mengetahui bahwa *web* tersebut adalah penipu
9	Doddy Teguh Yuwono, Siti Juhairiah, Sonedi (2019)	*National Institute of Standard Technology (NIST)* dan *tools FTK Imager, Autopsy*	Analisis *File Carving* Pada *File System* Dengan Metode *National Institute of Standard Technology (NIST)*	Mengetahui *File-file* yang telah terhapus
10	Muhammad Abdul Aziz Imam Riadi , Rusydi Umar (2018)	*National Institute of Justice (NIJ)* dan *tools FTK Imager*	Analisis Forensik *Line Messengger* berbasis *Web* menggunakan *Framework National Institute of Justice (NIJ)*	Mengetahui barang bukti digital pada kasus *Cybercrime*
11	Anton Yudhana, Abdul Fadlil, Muhammad Rizki Setyawan (2017)	*National Institute of Standard Technology (NIST)* dan *tools Oxygen Forensic Suite 2014, Belkasoft Evidience Center*	Analisis Recovery Bukti Digital Skype berbasis Smartphone Android Menggunakan Framework NIST	Mengembalikan barang bukti digital pada kasus *Cybercrime*
12	Arsyian Aldi Warsito (2020)	*NIST MEASUREMENT S*	Analisis Kinerja *Autopsy* pada *Smartphone* berbasis Android Menggunakan *NIST MEASUREMENT S*	Mengembalikan barang bukti digital pada kasus *Cybercrime*

13	Sidik Madiyanto, Husni Mubarok, Nur Widiyasono (2017)	*IDFIF v2* dan *tools Magnet Axiom*	Proses Investigasi *Mobile Forensik* Pada *Smartphone* Berbasis *IOS*	Mengembalikan barang bukti berupa pesan teks pada kasus *Cybercrime*
14	Muh Fadli Hasa, Anton Yudhana, Abdul Fadlil (2019)	*Static Forensic* dan *tools Ftk Imager, Autopsy*	Analisis Bukti Digital Pada Storage Secure Digital Card Menggunakan Metode Static Forensic	Mengembalikan barang bukti berupa file PDF, PNG, MP4, Doc, Zip, dan metadata file pada kasus *Cybercrime*
15	Andria,Saifulloh (2022)	*Exiftool*	Forensik Metadata Foto Sebagai Alat Bukti Digital	Mencari metadata dari foto hasil editing

Tabel 2.1 adalah hasil *study literature* yang telah dilakukan sebelum penelitian dilakukan. Tabel 2.1 semua menjelaskan tentang bagaimana melakukan analisis dan investigasi pada kasus *Cybercrime. Study literature* yang telah dilakukan akan membantu dalam penelitian ini.

Tabel 2. 2 Penelitian Terkait

No	**Peneliti**	**Metode dan *Tools***	**Judul Penelitian**	**Hasil Penelitian**
1	Muh Fadli Hasa, Anton Yudhana, Abdul Fadlil (2019)	*Static Forensic* dan *tools Ftk Imager, Autopsy*	Analisis Bukti Digital Pada Storage Secure Digital Card Menggunakan Metode Static Forensic	Mengembalikan barang bukti berupa file PDF, PNG, MP4, Doc, Zip, dan metadata file pada kasus *Cybercrime*
2	Muhammad Abdul Aziz Imam Riadi , Rusydi Umar (2018)	*National Institute of Justice (NIJ)* dan *tools FTK Imager*	Analisis Forensik *Line Messengger* berbasis *Web* menggunakan *Framework National Institute of Justice (NIJ)*	Mengetahui barang bukti digital pada kasus *Cybercrime*

3	Usulan penelitian yang akan dilakukan oleh Muamar Sidik Husni Mubarok Nur Widyasono (2023)	*National Institute of Justice (NIJ)* dan *tools FTK Imager, autospy*	Analisis Integritas Data Digital Evidencs Pada Hasil Proses Akuisisi Data Portable Storage Menggunakan Metode *National Institute Of Justice* (NIJ)	Mengakuisisi barang bukti dari portable storage dan menjaga keutuhan metadata yaitu nilai hash dan timetamps.

Tabel 2.2 adalah penelitian yang telah dilakukan sebelumnya mengenai proses insvestigasi *cybercrime.* Penelitian yang berjudul "Analisis Bukti Digital Pada *Storage Secure Digital Card* Menggunakan Metode *Static Forensic*" dengan penulis (Muh Fadli Hasa, Anton Yudhana dan Abdul Fadlil, 2019). Tahapan yang dilakukan menggunakan metode *Static Forensic* dan dibantu dengan tools *Ftk Imager, Autopsy* sehingga mampu mengungkap kejahatan yang terjadi pada *Storage Secure Digital Card* dengan mencari barang bukti digital berupa file PDF, PNG, MP4, Doc, Zip, dan metadata file yang telah dihapus.

Penelitian yang berjudul "Analisis Forensik *Line Messengger* berbasis *Web* menggunakan *Framework National Institute of Justice (NIJ)*" oleh (Muhammad Abdul Aziz Imam Riadi dan Rusydi Umar, 2018) di mana penelitian melakukan analisis proses investigasi terhadap Cybercrime pada *Line Messenger* berbasis *Web* dengan menggunakan metode *National Institute of Justice (NIJ)* dan dibantu dengan *tools FTK Imager.*

Berdasarkan uraian di atas ada beberapa persamaan penelitian sebelumnya dengan penelitian yang sedang dilakukan yaitu metode penelitian yang diginakan menggunakan *National Institute of Justice (NIJ)* dan menggunakan *tools FTK*

Imager dan autospy. Adapun keterbaruan dari penelitian ini yang berbeda dari terdahulu adalah melakukan akuisisi data pada *portable storage* dengan menjaga integritas metadata yaitu *hash* dan *timetamps* file dengan menggunakan metode *National Institute of Justice (NIJ)*.

2.8 Matriks Penelitian

Tabel 2. 3 Matriks Penelitian

No	Judul	Peneliti	Tahun	Ruang Lingkup											
				Metode				Tools Forensic							
				NIST	NIJ	IDFIF v2	Static Forensic	MobilEdit	FTK Imager	Oxygen Forensic	Aid4Mail	Wondershare	Autospy	Magnet Axiom	Exiftool
1	Analisa Forensik Aplikasi *Kakaotalk* menggunakan Metode *National Institute of Standard Technology (NIST)*	Riski Yudhi Prasongko, Anton Yudhana, Abdul Fadil	2018	✓				✓							
2	Penerapan Metode *National Institute of Standard Technology (NIST)* dalam analysis forensic digital untuk penaganan *Cybercrime*	Mulia Fitriana, Khairan AR, Jiwa Malem Marsya	2020	✓					✓						

3	Analisis *Recovery* bukti digital *Instagram Messengger* menggunakan metode *National Institute of Standard Technology (NIST)*	Imam Riadi, Anton Yudhana,Muhamad Caesar Febriansyah Putra	2017	✓						✓					
4	Digital Evidence Identification on Google Drive in Android Device Using *NIST Mobile Forensic Method*	Anton Yudhana, Rusydi Umar, Ahwan Ahmadi	2019	✓				✓							
5	Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode *NIST*	Saleh Khalifa Saad, RusydiUmar, Abdul Fadlil	2020	✓											
6	Rancangan Investigasi Forensik *E-mail* Dengan Metode *National Institute of Standard Technology (NIST)*	Mustafa, Imam Riadi, Rusydi Umar	2018	✓							✓				
7	Metode *NIST* Untuk Analisis Forensik Bukti Digital Pada Perangkat Android	Rusydi Umar, Sahiruddin	2019	✓						✓		✓			

8	Analisis Forensik Digital *E-Commerce* pada *Website* Rental Mobil Menggunakan Metode *NIST*	Gregorius Hendita Artha Kusuma, Yusuf Fadhilah	2019	✓											
9	Analisis *File Carving* Pada *File System* Dengan Metode *National Institute of Standard Technology (NIST)*	Doddy Teguh Yuwono, Siti Juhairiah, Sonedi	2019	✓					✓				✓		
10	Analisis Forensik *Line Messengger* berbasis *Web* menggunakan *Framework National Institute of Justice (NIJ)*	Muhammad Abdul Aziz Imam Riadi , Rusydi Umar	2018		✓				✓						
11	Analisis Recovery Bukti Digital Skype berbasis Smartphone Android	Anton Yudhana, Abdul Fadlil, Muhammad Rizki Setyawan	2017	✓						✓					

12	Analisis Kinerja *Autopsy* pada *Smartphone* berbasis Android Menggunakan *NIST MEASUREMENTS*	Arsyian Aldi Warsito	2020	✓											
13	Proses Investigasi *Mobile Forensik* Pada *Smartphone* Berbasis *IOS*	Sidik Madiyanto, Husni Mubarok, Nur Widiyasono	2017			✓								✓	
14	Analisis Bukti Digital Pada Storage Secure Digital Card Menggunakan Metode Static Forensic	Muh Fadli Hasa, Anton Yudhana, Abdul Fadlil	2019				✓		✓				✓		
15	Forensik Metadata Foto Sebagai Alat Bukti Digital	Andria,Saifulloh	2022												✓