BAB II
LANDASAN TEORI

2.1 Media Penyimpanan

Media penyimpanannkomputer terdiri dari duaajenis mediaapenyimpanan yaitu *volatile memory* dan *Non-Volatile. Volatile Memory* akannkehilanganddata ketika aliranntidak ada daya listrik atau aliran listrikkterputus seperti pada *Dynamic Random-access Memory* (DRAM), *Random Access Memory* (RAM) *dannStatic Random-access Memory* (SRAM) *Non-Volatile Memory* memungkinkanndatayyang tersimpanntidak akan hilang ketika terjadi alirannlistrik mati atau terputusscontohnya berupa *HardDrive, Harddisk, Nand FlashsSolid State Drive (SSD), flashdisk USB* dan*nMicroSD* (Riadi et al., 2017b; Riadi, Umar, et al., 2018)

2.2 Digital Forensic

Digital Foresic adalahhsuatu ilmu teknologi komputer dengan tahap kerja forensik untuk menjabarkan langkah-langkah forensik yang akan dikerjakan dan dapat mengetahui jalan penelitian secara terstruktur, sehingga dapat jadikan rujukan dalam menyelesaikan masalah dalam menemukannbarang bukti elektronik dari tindakan kejahatannyang telah terjadi dengan menggunakannteknologi canggih untuk membuktikan kejahatanndengan menggunakannbukti elektronik yang diinvestigasi untuk melawan kejahatan (Fanani et al., 2022; Syahib et al., 2020a; Yudhana et al., 2018a).

Digital Forensics memiliki jenis yang berbeda seperti *Disc Forensic, Computer Forensic, Mobile Phone Forensic, Network Forensic Database Forensic*. Penelitian ini akan melakukan investigasi *Disc Forensic* yang berfokus pada bukti elektronik *microSD*.

2.2.1 *Disk Forensic*

Disk Forensic adalah bagian dari forensik berfokus pada analisis drive perangkat. Forensik memori berfokus pada analisis data yang terkandung dalam memori dari sistem yang sedang dipelajari (Uroz & Rodríguez, 2020). Tipe *digital*

forensic iniiberkaitan dengannmengekstraksi data yang ada didalam media penyimpananndengan memeriksa file yang aktif, dimodifikasi, atau dihapus. *Disk Forensic* termasuk *SD Card USB Stick, UFS* menggunakan memori *flash NAND CF Card* dan *eMMC* (Ahn & Lee, 2021).

Disk Forensic adalah identifikasi beberapa sumber bukti digital seperti hard disk dengan antarmuka seperti SATA/SCSI, Compact Disk, Disk Video Digital, Floppy disk, Ponsel, flash drive, PDA, Kartu SIM, penyimpanan USB, Pita Magnetik, media Zip drive dan lainnya, setelah menyita bukti digital di TKP (Prem et al., 2017).

2.3 Bukti Digital

Bukti digital adalah informasi yang dikirim atau disimpan dalam bentuk biner dari hasil investigasi dengan melakukan tahapan untuk melindungi barang bukti dan meminimalkan kerusakan selama investigasi sehingga barang bukti masih asli. Bukti diperlukan untuk menyelesaikan kasus, Sedangkan bukti elektronik sangat sensitif akan perubahan jika tidak ditangani dengan benar sehingga dapat mempengaruhi keasliannya. Semua jenis perubahan pada bukti elektronik menyebabkan bukti menjadi tidak berguna karena akan mengarah pada kesimpulan yang salah. Barang bukti elektronik melekat menjadi tiga prinsip utama dalam proses pengumpulan, yaitu: prinsip mengacu pada Standar Nasional Indonesia (SNI), yaitu ISO / IEC / 27037: 2014 dannjuga sudah diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Elektronika Informasi dan Transaksi (Forensik et al., 2018; Ichsan & Riadi, 2021; Riadi, Yudhana, & Putra, 2018).

Investigasi yang akan dilakukan yaitu berjenis *disk forensic* dengan barang bukti elektronik berupa *microSD* sebagai parameter pengujian metode investigasi.

2.4 Metode Investigasi

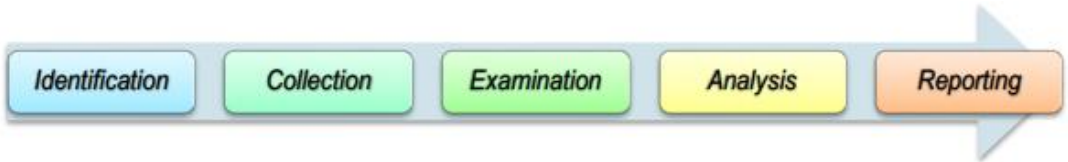
Penelitian yang berkaitan dengan metode investigasi digital forensik sudah banyak dijelaskan pada penelitian sebelumnya dan sudah banyak pilihan metode yang dapat diterapkan pada *digital forensic*. Penelitian mengenai metode *digital*

forensic yang telah dipelajari dapat menghasilkan metode baru berdasarkan penelitian sebelumnya atau dapat dilakukan perbandingan metode dengan kompabilitas metode investigasi *digital forensic*, prosedur investigasi *digital forensic* terhadap bukti, metode pengumpulan dan analisis, analisis perilaku *cybercrime* dan verifikasi kasus analisis bukti serta prosedur yuridis peradilannya. mengimplematasikan teknik forensik dan analisa forensik berdasarkan dengan metode yang tepat akan memiliki tingkat keberhasilan hampir 100% dalam mengumpulkan data forensik (Riadi, Umar, et al., 2018).

Berkaitan dengan metode investigasi digital forensik yang dipilih lalu proses penguasaan barang bukti dan legalitas, aspek hukum disetiap tahapan dari metode yang telah diterapkan oleh investigator yanggterlibat dalam penanganan bukti elektronik menjadi kunci utama dalam suksesnya investigasi forensic digital dan investigasi bukti elektronik harus memenuhi standar bukti dan diterimanya tuntutan untuk penuntutan yang sukses (Faiz & Prabowo, 2018a; Riskiyadi, 2020)

2.5 *National Institute Justice* (NIJ)

Awal mula *The National Institute of Law Enforcement and Criminal Justice* didirikan pada 21 Oktober 1968, sebagai komponen dari *Law Enforcement Assistance Administration* (LEAA) dan pada tahun 1978 dilakukan perubahan nama menjadi *National Institute of Justice* (NIJ) hingga saat ini. NIJ ini mempunyai lima tahap dalam proses forensic mulai dari *identification*(persiapan), *collection*(koleksi), *examination*(pemeriksaan), *analysis*(analisis), dan *reporting*(pelaporan). Menurut penelitian sebelumnya disebutkan pengumpulkan data dengan tingkat keberhasilan yang sangat akurat dengan melakukan teknik forensik dan analisa forensik berdasarkan metode yang tepat (Riadi, Yudhana, & Putra, 2018; Saad et al., 2020; Yudhana et al., 2018b).



Gambar 2. 1 Alur Investigasi Metode *National Institute Of Justice* (Riadi, Umar and Nasrulloh, 2018)

2.6 *National Institute of Standartd and Technology* (NIST)

National Institute of Standards and Technology (NIST) didirikan pada tahun 1901 dan sekarang menjadi bagian dari departemen perdagangan AS. NIST adalah salah satu laboratorium ilmu fisika tertua di negara AS. Kongres membentuk badan tersebut untuk menghilangkan tantangan besar bagi daya saing industri AS pada saat itu infrastruktur pengukuran kelas dua yang tertinggal di belakang kemampuan Inggris, Jerman, dan saingan ekonomi lainnya. Jaringan listrik pintar dan catatan kesehatan elektronik hingga jam atom, nanomaterial canggih, dan chip komputer, produk dan layanan yang tak terhitung banyaknya bergantung pada teknologi, pengukuran, dan standar yang disediakan oleh *National Institute of Standards and Technology*. Metode NIST digunakan untuk dilakukan proses investigasi pada bukti digital atau proses untuk mendapatkan informasi dari bukti digital (Riadi et al., 2017b). NIST memiliki empat tahap proses investigasi yaitu *Collection*, *examination*, *Analysis* dan *Report* (Asyaky et al., 2018; Riadi, Yudhana, et al., 2021; Syahib et al., 2020b).

Gambar 2. 2 Alur Investigasi *Metode National Institute Of Standard And Technology* (Syahib, Riadi and Umar, 2020a)

2.7 State Of The Art

Tabel 2. 1 *State Of The Art*

No.	Nama Peneliti	Judul Penelitian	Metode / *Frameworks*	Tools	Hasil Penelitian
1.	Nova Setiawan, Ahmad R Pratama, Erika Ramadhani (2022)	Metode Live Forensics Untuk Investigasi Serangan Formjacking Pada *Website E-Commerce*	*National Institute of Justice* (NIJ) *live Forensic*	*FTK Imager*	Penelitian ini melakukan pengujian pada empat web browser yaitu Opera, Microsoft Edge, Mozila Firefox dan Google Chrome. Hasil investigasi detail pada kartu kredit mendapatkan Nama, Nomor Kartu Kredit dan CVV dari proses investigasi bahwa formjacking dapat berjalan pada keempat browser dan dapat mengirimkan paket data berupa detail dari kartu kredit melalui perintah yang berada dalam kode Javascript.

Lanjutan Tabel 2.1 *State Of The Art*

No.	Nama Peneliti	Judul Penelitian	Metode / *Frameworks*	Tools	Hasil Penelitian
2.	Muhammad Irwan Syahib, Imam Riadi, Rusydi Umar (2020)	Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode *National Institute Of Standards Technology (NIST)*	*National Institute of Standards Technology (NIST)*	*MOBILedit Forensics*	Penelitian ini, skenario kasus yang dibuat berupa mengirim pesan percakapan dari pelaku ke target, diantaranya berupa pesan taks, gambar dan video dan data berupa pesan percakapan yang telah dihapus oleh pelaku beserta akun dan riwayat panggilan berhasil didapat, bukti digital yang didapatkan pada proses investigasi yaitu: Akun & Kontak, Riwayat panggilan, Pesan teks, Foto dan Video.
3.	Saleh Khalifah Saad, Rusydi Umar, AbdulFadli (2020)	Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIJ Pada Kasus Penyembunyian Berkas Standards Technology	*National Institute of Justice (NIJ)*	*MOBILedit Forensics* dan *Oxygen Forensic*	Penelitian ini melakukan perbandingan *tools MOBILedit Forensics* dan *Oxygen Forensic*. Penelitian ini *Oxygen* dan *Mobiledit Forensic* ada yang bisa membaca *account* pengguna media penyimpanan *Google Drive* sisanya dari ekstensi file dan jenis file yang bisa di buka hanya di miliki satu tool saja yaitu *Oxygen Forensics.*

Lanjutan Tabel 2.1 *State Of The Art*

No.	Nama Peneliti	Judul Penelitian	Metode / *Frameworks*	Tools	Hasil Penelitian
4.	Moh. Riskiyadi (2020)	Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime	*National Institute of Justice (NIJ)*	*FTK Imager* dan *Autopsy*	Penelitian ini melakukan investigasi d*isk forensics* dengan barang bukti elektronik berupa *flash disk.* Proses dilakukan dengan mencari data atau *file* yang tersembunyi atau dihapus pada *flash disk* oleh pelaku. Proses investigasi mendapatkan hasil dengan nilai hash yang berbeda dari masing-masing perlakuan.
5.	Rizdqi Akbar Ramadhan, Panji Rachmat Setiawan, Dedy Hariyadi (2022)	Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework	ISO/IEC 27037:2012 dan NIST SP800-86	*X-way Forensics*	NIST SP 800-86 juga menyebutkan proses pengamanan bukti digital yang disimpan pada media penyimpanan di komputer. Namun tidak dijelaskan lebih detail seperti pada ISO/IEC 27037:2021.

Lanjutan Tabel 2.1 *State Of The Art*

No.	Nama Peneliti	Judul Penelitian	Metode / *Frameworks*	Tools	Hasil Penelitian
6.	Imam Riadi, Anton Yudhana, Mush'ab Al Barra (2021)	Forensik Mobile Pada Layanan Media Sosial Linkedin	*NIST (National Institute of Standard and Technology).*	*Autopsy* dan *MOBILedit Forensics*	Skenario investigasi yang dijalankan yaitu penyelidikan laporan kasaus hoax dari korban yang menjadi target kejahatan, pengumpulan sample berupa akun LinkedIn dan ponsel pelaku dengan hasil investigasi telah menemukan bukti digital berupa log activity dan status update,117 password WiFi,1117 download history,2263 panggilan telepon, 1 file terhapus, 1ffile disembunyikan dan 1 file dimunculkan.
7.	Irfan Fathur Rohman, Nur Widiyasono, Rohmat Gunawan (2019)	Simulasi Analisis Bukti Digital Aplikasi Skype Berbasis Android Menggunakan NIST SP 800-101 R1	*NIST SP 800-101 R1*	*FTK Imager*	Penelitian ini melakukan 14 skenario yang dijalankan telah berhasil melakukan 11 skenario investigasi. Bukti digital masih dapat ditemukan dan dilengkapi dengan data-data pendukung yang tersimpan pada database aplikasi Skype.

Lanjutan Tabel 2.1 *State Of The Art*

No.	Nama Peneliti	Judul Penelitian	Metode / *Frameworks*	Tools	Hasil Penelitian
8.	Tri Rochmadi (2019)	Deteksi Bukti Digital Pada Adrive Cloud Storage Menggunakan Live Forensic	NIST *(National Institute of Standar and Technology)*	*FTK Imager* dan *Autoopsy*	Hasil yang diperoleh dalam penelitian ini dengannlive forensik bukti digital pada penggunaan cloud Adrive dapat terdeteksi dari akuisisi dan analisisppada RAM, darihhasil penelitian tersebut bukti digital berupa lokasi instalasi Adrive dan hasil pendeteksian Adrive tersebut ditemukan sebuah file dokumen yang dibagikan setelah file tersebut diunggah ke cloud storage Adrive.
9.	Muh Fadli Hasa, Anton Yudhana dan Abdul Fadlil (2019)	Analisis Bukti Digital Pada Storage Secure Digital Card Menggunakan Metode Static Forensic	*National Institute of Justice (NIJ)*	*FTK Imager* dan *Autopsy*	Barang bukti yang ditemukan pada SD Card dengan cara hapus Shift+Delete yang menggunakan FTK Imager dan *Autopsy* yaitu berupa file PDF, PNG, MP4, Doc, dan Zip, Sedangkan pada memori dengan cara hapus Wipe Data, FTK Imager dan *Autopsy* hanya mendapatkan file residu.

2.8 Matriks Penelitian

Tabel 2. 2 Matriks Penelitian

No	Peneliti	Judul	Ruang Lingkup																										
			Metode							Device								Tools											
										Storage				Desktop		Smart phone													
			End to End Digital	*The Advance Data*	*SNI 27037:2014*	*National Institute of*	*National Institute of*	McKemmish	ISO/IEC 27037:2012	FlashDisk	Solid State	*MicroSD*	Cloud Storage	PC	Notebook	HandPhone	Tablet	*Belkasoft Evidence*	*Network Minner*	*AccessData FTK Imager*	*Autopsy*	*Oxygen Forensics*	*Mobiledit Forensics*	*Encase Acquisition*	*Cscpkt*	*WinHex*	*OS*Forensik	*RapidManner*	*Wireshark*	*X-way Forensics*
1.	Nova Setiawan, Ahmad R Pratama , Erika Ramadhani (2022)	Metode Live Forensics Untuk Investigasi Serangan Formjacking Pada Website E-Commerce					√							√	√					√									

Lanjutan Tabel 2.2 Matriks Penelitian

No	Peneliti	Judul	Ruang Lingkup																							
			Metode							Device								Tools										
										Storage				Desktop		Smart phone												
			End to End Digital	*The Advance Data*	*SNI 27037:2014*	*National Institute of*	*National Institute of*	McKemmish	ISO/IEC 27037:2012	FlashDisk	Solid State	*MicroSD*	Cloud Storage	PC	Notebook	HandPhone	Tablet	*Belkasoft Evidence*	*Network Minner*	*AccessData FTK Imager*	*Autopsy*	*Oxygen Forensics*	*Mobiledit Forensics*	*Encase Acquisition*	*Cscpkt*	*WinHex*	OSForensik	*RapidManner*	*Wireshark*	*X-way Forensics*
2.	Muhammad Irwan Syahib, Imam Riadi, Rusydi Umar (2020)	Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute Of Standards Technology (NIST)				√										√	√						√							

Lanjutan Tabel 2.2 Matriks Penelitian

No	Peneliti	Judul	Ruang Lingkup																								
			Metode							Device								Tools											
			End to End Digital	*The Advance Data*	*SNI 27037:2014*	*National Institute of*	*National Institute of*	McKemmish	ISO/IEC 27037:2012	Storage				Desktop		Smart phone		*Belkasoft Evidence*	*Nework Minner*	*AccessData FTK Imager*	*Autopsy*	*Oxygen Forensics*	*Mobiledit Forensics*	*Encase Acquisition*	*Cscpkt*	*WinHex*	OSForensik	*RapidManner*	*Wireshark*	*X-way Forensics*
										FlashDisk	Solid State	*MicroSD*	Cloud Storage	PC	Notebook	HandPhone	Tablet													
3.	Saleh Khalifah Saad, Rusydi Umar, AbdulFadli (2020)	Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIJ Pada Kasus Penyembunyian Berkas Standards Technology				√								√	√	√	√					√	√						

Lanjutan Tabel 2.2 Matriks Penelitian

No	Peneliti	Judul	Ruang Lingkup																										
			Metode							Device								Tools												
										Storage				Desktop		Smart phone														
			End to End Digital	*The Advance Data*	*SNI 27037:2014*	*National Institute of*	*National Institute of*	McKemmish	ISO/IEC 27037:2012	FlashDisk	Solid State	*MicroSD*	Cloud Storage	PC	Notebook	HandPhone	Tablet	*Belkasoft Evidence*	*Network Minner*	*AccessData FTK Imager*	*Autopsy*	*Oxygen Forensics*	*Mobiledit Forensics*	*Encase Acquisition*	*Cscpkt*	*WinHex*	OSForensik	*RapidManner*	*Wireshark*	*X-way Forensics*
4.	Moh. Riskiyadi (2020)	Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime					√			√										√	√								

Lanjutan Tabel 2.2 Matriks Penelitian

No	Peneliti	Judul	Ruang Lingkup																										
			Metode							Device								Tools											
										Storage				Desktop		Smart phone													
			End to End Digital	*The Advance Data*	*SNI 27037:2014*	*National Institute of*	*National Institute of*	McKemmish	ISO/IEC 27037:2012	FlashDisk	Solid State	*MicroSD*	Cloud Storage	PC	Notebook	HandPhone	Tablet	*Belkasoft Evidence*	*Network Minner*	*AccessData FTK Imager*	*Autopsy*	*Oxygen Forensics*	*Mobiledit Forensics*	*Encase Acquisition*	*Cscpkt*	*WinHex*	*OS*Forensik	*RapidManner*	*Wireshark*	*X-way Forensics*
5.	Rizdqi Akbar Ramadhan, Panji Rachmat Setiawan, Dedy Hariyadi (2022)	Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework				√			√		√									√									√

Lanjutan Tabel 2.2 Matriks Penelitian

No	Peneliti	Judul	Ruang Lingkup																								
			Metode							Device								Tools											
			End to End Digital	*The Advance Data*	*SNI 27037:2014*	*National Institute of*	*National Institute of*	McKemmish	ISO/IEC 27037:2012	Storage				Desktop		Smart phone		*Belkasoft Evidence*	*Network Minner*	*AccessData FTK Imager*	*Autopsy*	*Oxygen Forensics*	*Mobiledit Forensics*	*Encase Acquisition*	*Cscpkt*	*WinHex*	*OS*Forensik	*RapidManner*	*Wireshark*	*X-way Forensics*
										FlashDisk	Solid State	*MicroSD*	Cloud Storage	PC	Notebook	HandPhone	Tablet													
6.	Imam Riadi, Anton Yudhana, Mush'ab Al Barra (2021)	Forensik Mobile Pada Layanan Media Sosial Linkedin				√								√	√	√	√				√		√						

Lanjutan Tabel 2.2 Matriks Penelitian

No	Peneliti	Judul	Ruang Lingkup																										
			Metode							Device								Tools												
			End to End Digital	*The Advance Data*	*SNI 27037:2014*	*National Institute of*	*National Institute of*	McKemmish	ISO/IEC 27037:2012	Storage				Desktop		Smart phone		*Belkasoft Evidence*	*Network Minner*	*AccessData FTK Imager*	*Autopsy*	*Oxygen Forensics*	*Mobiledit Forensics*	*Encase Acquisition*	*Cscpkt*	*WinHex*	OSForensik	*RapidManner*	*Wireshark*	*X-way Forensics*
										FlashDisk	Solid State	*MicroSD*	Cloud Storage	PC	Notebook	HandPhone	Tablet													
7.	Irfan Fathur Rohman, Nur Widiyasono, Rohmat Gunawan (2019)	Simulasi Analisis Bukti Digital Aplikasi Skype Berbasis Android Menggunakan NIST SP 800-101 R1				√										√	√				√								

Lanjutan Tabel 2.2 Matriks Penelitian

No	Peneliti	Judul	Ruang Lingkup																										
			Metode							Device								Tools												
										Storage				Desktop		Smart phone														
			End to End Digital	*The Advance Data*	*SNI 27037:2014*	*National Institute of*	*National Institute of*	McKemmish	ISO/IEC 27037:2012	FlashDisk	Solid State	*MicroSD*	Cloud Storage	PC	Notebook	HandPhone	Tablet	*Belkasoft Evidence*	*Network Minner*	*AccessData FTK Imager*	*Autopsy*	*Oxygen Forensics*	*Mobiledit Forensics*	*Encase Acquisition*	*Cscpkt*	*WinHex*	*OS*Forensik	*RapidManner*	*Wireshark*	*X-way Forensics*
8.	Tri Rochmadi (2019)	Deteksi Bukti Digital Pada Adrive Cloud Storage Menggunakan Live Forensik				√							√							√	√								

Lanjutan Tabel 2.2 Matriks Penelitian

No	Peneliti	Judul	Ruang Lingkup																										
			Metode							Metode								Metode												
										Storage				Desktop		Smart phone														
			End to End Digital	*The Advance Data*	*SNI 27037:2014*	*National Institute of*	*National Institute of*	McKemmish	ISO/IEC 27037:2012	FlashDisk	Solid State	*MicroSD*	Cloud Storage	PC	Notebook	HandPhone	Tablet	*Belkasoft Evidence*	*Network Minner*	*AccessData FTK Imager*	*Autopsy*	*Oxygen Forensics*	*Mobiledit Forensics*	*Encase Acquisition*	*Cscpkt*	*WinHex*	OSForensik	*RapidManner*	*Wireshark*	*X-way Forensics*
9.	Muh Fadli Hasa, Anton Yudhana dan Abdul Fadlil (2019)	Analisis Bukti Digital Pada Storage Secure Digital Card Menggunakan Metode Static Forensic					√					√								√	√								

Dasar Pemikiran dari penelitian ini adalah mengacu dari penelitian sebelumnya yang terkait yaitu :

Penelitian yang dilakukan (Riadi, Umar and Nasrulloh, 2017) Mengevaluasi forensik terhadap bukti digital pada media penyimpanan utama, yaitu SSD, dalam situasi sistem komputer yang dilengkapi dengan perangkat lunak pembeku drive. Proses analisis forensik terhadap bukti digital dilakukan dengan menerapkan metode pengambilan data secara statis dan mengikuti langkah-langkah analisis forensik menggunakan metode National Institute of Standards and Technology (NIST) untuk memperoleh bukti digital.

Penelitian yang dilakukan (M. F. Hasa, Yudhana and Fadlil, 2019) melibatkan pemeriksaan dan pemulihan data yang hilang pada SD Card sebagai barang bukti. Data yang berhasil dipulihkan dibedakan berdasarkan metode penghapusan yang digunakan oleh pelaku. Informasi yang ditemukan dalam SD Card dapat dijadikan sebagai barang bukti dalam persidangan kasus kejahatan cyber.

Tabel 2.3 GAP

No	Judul Penelitian	Keterangan	Perbedaan
1	ANALISIS FORENSIK BUKTI DIGITAL PADA FROZEN SOLID STATE DRIVE DENGAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)	1. Menggunakan metode *National Institute Standard of Technology* (NIST). 2. Investigasi terhadap Penyimapanan *Solid State Drive* (SSD). 3. Menggunakan *tools FTK Imager* dan *Winhex*.	1. Menggunakan metode *National Institute of Justice* (NIJ) serta *National Institute Standard of Technology* (NIST). 2. Investigasi terhadap media penyimpanan *microSD*. 3. Menggunakan *tools Autopsy*.
2	ANALISIS BUKTI DIGITAL PADA STORAGE SECURE DIGITAL CARD MENGGUNAKAN METODE STATIC FORENSIC	1. Menggunakan metode *National Institute of Justice* (NIJ). 2. Investigasi terhadap *Secure Digital Card*. 3. Menggunakan *tools FTK imager* dan *Autopsy*.	1. Menggunakan metode *National Institute of Justice* (NIJ) serta *National Institute Standard of Technology* (NIST). 2. Investigasi terhadap *microSD.*

Penelitian ini, akan dilakukan sebuah studi analisa perbandingan dua metode yaitu NIJ dan NIST untuk proses investigasi *disk forensic* dengan barang bukti berupa *microSD*. Melakukan proses investigasi dengan dua metode tersebut akan menghasilkan sebuah hasil yang berbeda karena setiap metode mempunyai tahapan atau langkah-langkah investigasi yang berbeda. Proses investigasi yang telah dilakukan dari metode NIJ dan metode NIST telah mendapatkan hasil maka selanjutnya akan dilakukan sebuah perbandingan untuk mengetahui metode investigasi yang memperoleh hasil lebih maksimal dalam melakukan investigasi

disk forensic dengan barang bukti berupa *microSD*. Hasil analisis perbandingan yang dilakukan diharapkan akan menjadi rekomendasi untuk praktisi investigator dalam melakukan investigasi *disk forensic* dengan barang bukti elektronik berupa *microSD*.