

BAB II TINJAUAN PUSTAKA

Pada BAB Tinjauan Pustaka akan dibahas beberapa Penelitian-penelitian yang berkaitan pada penelitian. (Subli et al., 2017) didalam penelitiannya melakukan pendekatan metadata, dengan proses ini investigator/penyidik digital forensik dapat melihat langsung metadata file secara umum dan juga dapat menemukan file-file berdasarkan korelasi file dengan parameter dari metadata file tersebut. Didalam penelitian yang dilakukan saat ini konsep yang akan diusulkan dan yang membedakan dengan penelitian sebelumnya adalah pada perubahan pencarian data yang lebih kompleks dan menambahkan beberapa fitur pada aplikasi yang dikembangkan dari aplikasi sebelumnya dengan meningkatkan algoritma dan identifikasi langsung untuk melihat bukti digital yang telah diedit menggunakan aplikasi.

(Ardiansyah & Marzuki, 2020) pada penelitian yang dilakukan menghasilkan Bagaimana mekanisme digital forensics research workshop untuk mendapatkan bukti digital dari solid state drive yang di hard format (atau di format). Bukti digital yang diperoleh menggunakan RercoverMyFiles dari hasil recovery solid state drive yang di hard format dengan kondisi fitur trim aktif yang berhasil di-recovery hanya 5 file dari 17 file yang disiapkan untuk pengujian, dengan persentase 29%. Sedangkan fitur trim nonaktif hanya 15 file dari 17 file dengan persentase 88% yang berhasil di-recovery.

(Ezz El-Din Hemdan & D. H. Manjaiah, 2018) pada penelitian ini memperkenalkan prinsip-prinsip Digital Forensik, Cara Mendeteksi Intrusi dan Internet of Things (IOT) serta membuat sebuah konsep dan metode yang dapat membantu penyelidik digital dan profesional keamanan untuk mengembangkan dan mengusulkan teknik dan metode ilmu data baru yang dapat disesuaikan dengan konteks unik lingkungan Internet of Things.

(Fahad Alanazi & Andrew Jones, 2015) pada penelitian ini dijelaskan bagaimana menggunakan metada untuk mendapatkan informasi, misalnya, penulis file, tanggal dan waktu pembuatan, berapa kali file telah dimodifikasi, termasuk kapan modifikasi itu

berlangsung. Menggunakan format dan jenis metadata yang berbeda untuk memvalidasi argumen hukum untuk bukti yang relevan. Selain itu dijelaskan juga Didalam kasus hukum, identifikasi bukti digital berupa metadata sangat penting untuk mendukung kasus, verifikasi dan pemeriksaan berbagai bentuk argumen hukum yang ada. Dasar-dasar penelitian sebelumnya yang menjadi tinjauan pustaka pada penelitian ini dirangkum dalam Tabel 2.1

Tabel 2. 1 Tinjauan Pustaka

No	Nama dan Tahun	Permasalahan	Akibat	Data	Metode	Kontribusi
1	(Subli, Sugiantoro & Prayudi, 2017)	Bagaimama merancang sistem/aplikasi dan menguji kinerja sistem/aplikasi metadata yang dibangun	Membangun sistem untuk dapat membaca metadata file secara umum dan korelasi file dengan salah satu parameter dari metadata file tersebut. Dengan teknik model pencarian metadata setiap file pada komputer.	Input File (docx, pdf, jpg, mp3, mp4, dd dan e01)	metode penelitian yang di bangun secara garis besar dibagi menjadi tiga tahapan yaitu tahapan pertama atau tahapan awal dimulai dari identifikasi masalah dan tinjauan pustaka, tahapan kedua atau tahapan perancangan dan pengujian sistem dimulai dari metode	Membangun sistem untuk dapat membaca metadata file secara umum dan korelasi file dengan salah satu parameter dari metadata file tersebut. Dengan teknik model pencarian metadata setiap file pada komputer.

					<p>pengumpulan data, analisis kebutuhan sistem, perancangan sistem, implementasi sistem dan</p> <p>pengujian metode, dan tahapan ketiga atau tahapan penyelesaian berupa kesimpulan atau penyusunan laporan dari penelitian</p>	
2	(Ardiansyah & Marza Ihsan Marzuki,2020)	Bagaimana mekanisme digital forensics research workshop untuk mendapatkan bukti digital dari solid state drive yang di hard format	Mensimulasikan proses investigasi yang efektif yang dapat dipergunakan dalam peroses investigasi komputer forensics pada media penyimpanan solid state drive yang di hard format untuk keperluan forensics	Bukti digital dokumen dan gambar sebanyak 17 file Dengan extension .doc, .docx, .xlsx, .pptx, .pdf, .txt, .jpg	<p>Model Investigasi Digital Forensics Research Workshop,</p> <ol style="list-style-type: none"> 1. Identification 2. Preservation 3. Collection 4. Examination 5. Analysis 	Mensimulasikan proses investigasi yang efektif yang dapat dipergunakan dalam peroses investigasi komputer forensics pada media penyimpanan solid state drive yang di hard format untuk keperluan forensics

3	(Ezz El-Din Hemdan & D. H. Manjaiah, 2018)	Bagaimana melakukan proses investigasi forensik berbasis Internet of Things (IOT)	memperkenalkan prinsip-prinsip Digital Forensik, Cara Mendeteksi Intrusi dan Internet of Things (IOT) serta membuat sebuah konsep dan metode yang dapat membantu penyelidik digital dan profesional keamanan untuk mengembangkan dan mengusulkan teknik dan metode ilmu data baru yang dapat disesuaikan dengan konteks unik lingkungan Internet of Things	Data Internet, Data Cloud dan Data Perangkat yang berhubungan dengan jaringan	Data Science Road Map (DSRM)	memperkenalkan prinsip-prinsip Digital Forensik, Cara Mendeteksi Intrusi dan Internet of Things (IOT) serta membuat sebuah konsep dan metode yang dapat membantu penyelidik digital dan profesional keamanan untuk mengembangkan dan mengusulkan teknik dan metode ilmu data baru yang dapat disesuaikan dengan konteks unik lingkungan Internet of Things
---	--	---	--	---	------------------------------	--

4	(Fahad Alanazi & Andrew Jones, 2015)	Bagaimana menggunakan metada untuk mendapatkan informasi, misalnya, penulis file, tanggal dan waktu pembuatan, berapa kali file telah dimodifikasi, termasuk kapan modifikasi itu berlangsung.	Didalam kasus hukum,identifikasi bukti digital berupa metadata sangat penting untuk mendukung kasus, verifikasi dan pemeriksaan berbagai bentuk argumen hukum yang ada.	Gambar Dengan Format GIF, JPEG, music (Mp3 dan AAC) , Format Document Ms Office 2007	Menggunakan format dan jenis metadata yang berbeda untuk memvalidasi argumen hukum untuk bukti yang relevan.	Didalam kasus hukum,identifikasi bukti digital berupa metadata sangat penting untuk mendukung kasus, verifikasi dan pemeriksaan berbagai bentuk argumen hukum yang ada.
---	--	--	---	---	--	---

5	(Raghavan, Sriram & Raghavan, S. V. 2014)	Bagaimana menyajikan studi sistematis kontemporer alat forensik dan analisis menggunakan tinjauan berbasis hipotesis untuk mengidentifikasi berbagai fungsi yang didukung oleh alat-alat digital forensik	menyajikan studi sistematis forensik kontemporer dan alat analisis untuk memeriksa dan menganalisis bukti digital serta mempresentasikan sistem hipotesis yang menggunakan alat tertentu yang dapat dipelajari untuk mengidentifikasi berbagai kemampuan yang disediakan untuk memeriksa satu atau lebih sumber bukti digital.	gambar forensik, folder, file log, dan dump paket jaringan harus dianalisis, pemeriksaan artefak dan metadata	Menggunakan AssocGEN yang menggunakan metadata untuk menentukan hubungan antara artefak milik files, logs dan network packet dumps, dan mengidentifikasi asosiasi metadata ke grup artefak yang terkait.	menyajikan studi sistematis forensik kontemporer dan alat analisis untuk memeriksa dan menganalisis bukti digital serta mempresentasikan sistem hipotesis yang menggunakan alat tertentu yang dapat dipelajari untuk mengidentifikasi berbagai kemampuan yang disediakan untuk memeriksa satu atau lebih sumber bukti digital.
6	(Alfiansyah Imanda Putra, Rusydi Umar, Abdul Fadlil, 2018)	Bagaimana menganalisis metada video menggunakan tool EXIFTOOL	membandingkan metadata rekaman video asli dan kemudian selanjutnya tahap Processing Exiftool, dimana tahap ini adalah proses membaca metadata	Terdapat 7 macam file yang sudah dijadikan sampel yaitu DOCX, PDF,	Metode Localization Tampering	membandingkan metadata rekaman video asli dan kemudian selanjutnya tahap Processing Exiftool, dimana tahap ini adalah proses membaca metadata

			video dengan exiftool dan tahap akhir adalah analisa hasil metadata	JPG, MP3, MP4, DD dan E01		video dengan exiftool dan tahap akhir adalah analisa hasil metadata
7	(Ii Sopiandi, 2017)	Bagaimana menggali informasi metada	Menggunakan beberapa tools forensik seperti http://fotoforensics.com dan Google Image untuk mendapatkan informasi terkati metada	Data Berupa docx, pdf, mp3, jpg, mp4, DD dan E01	Menggunakan Metode Errol Level Analysis	Menggunakan beberapa tools forensik seperti http://fotoforensics.com dan Google Image untuk mendapatkan informasi terkati metada
8	(Subli, Sugiantoro & Prayudi, 2017)	Bagaimana menggali informasi metada	Bagaimana merancang sistem dan menguji kinerja sistem metadata yang dibangun	Data Berupa Sampel Foto Ekstensi Jpg	Membangun sistem pembacaan korelasi file	Membangun sistem untuk dapat membaca metadata file secara umum dan korelasi file dengan salah satu parameter dari metadata file tersebut. Dengan teknik model pencarian metadata setiap file pada komputer.

9	(Kumar et al., 2016)	Memverifikasi metada dengan gambar berdasarkan ketinggian GPS	memverifikasi metadata yang terkait dengan gambar dan melacak menggunakan fitur GPS berdasarkan Ketinggian GPS	Data Berupa Teks, Gambar, Audio dan Video	Menggunakan Metode Geo Tagging	Menggunakan Tools Geo Tagging untuk memverifikasi gambar
10	(Salama, Varadharajan & Hitchens, 2012)	Bagaimana menganalisis informasi metada	Menganalisis metadata yang bersumber dari internet yaitu foto, dokumen, camera, smartphone	Data Berupa Foto yang berada di internet	Menggunakan Beberapa metode analisa	Menggunakan beberapa tools forensik untuk mendapatkan informasi terkait metada
11	Dewi Yunita Sari, Yudi Prayudi, Bambang Sugiantoro (2017)	Bagaimana mendeteksi Keaslian Video Pada Handycam	Dapat Menganalisis Video pada handycam	Data berupa file berformat video	Menggunakan Metode Localization Tampering	Menjelaskan Konsep dasar dalam mendeteksi video pada handycam dengan membuat simulasi video tampering dengan attack dimana video asli dilakukan cropping, zooming, rotation, dan grayscale

12	Alfiansyah Imanda Putra , Rusydi Umar & Abdul Fadlil (2018)	Mendeteksi keaslian metadata menggunakan exiftool pada cmd	Mengetahui hasil analisa metadata dengan tipe data (mp4)	Data yang diambil berformat video dengan extensi (mp4)	Menggunakan metode perbandingan dengan tools Exiftool	membandingkan metadata rekaman video asli dan kemudian selanjutnya tahap Processing Exiftool, dimana tahap ini adalah proses membaca metadata video dengan exiftool dan tahap akhir adalah analisa hasil metadata.

13	Ezz El-Din Hemdan & Manjaiah D.H (2015)	Melakukan analisis forensik untuk barang bukti digital seperti foto digital dan dokumen	Hasil analisa file bukti digital seperti foto digital dan dokumen	Data yang diambil berupa foto digital dan dokumen	pendekatan analisis forensik	Dalam pendekatan ini, metadata yang dihasilkan dari barang bukti dan juga algoritma hash diterapkan untuk menghasilkan nilai hash untuk menjamin integritas data yang diunggah ke layanan cloud seperti ADrive, Box, Microsoft onedrive, Google Drive, Copy dan Dropbox
14	Moh. Riskiyadi (2020)	memberikan referensi terkait dengan kehandalan tools digital forensic dalam mengungkap cybercrime agar diperoleh bukti digital yang berintegritas, handal dan legal dalam proses litigasi	Tools FTK Imager dan Autopsy masih belum mampu melakukan akuisisi dan analisis Data dengan perlakuan Penghapusan permanen dan enkripsi (password) pada flash disk menggunakan tools bawaan Windows 10	Data yang diambil menggunakan tools FTK Imager dan Autospy	menggunakan metode static forensic dengan framework dari National Institute of	Menggunakan teknik investigasi forensik digital yang meliputi static forensic dan live forensic berhubungan dengan kasus yang lebih spesifik terkait

			yaitu BitLocker Drive Encryption			dengan alat atau media yang digunakan pelaku dalam melakukan tindakan cybercrime
15	Khairunnisak Nur Isnaini , Hamid Ashari & Adam Prayogo Kuncoro (2020)	membuktikan keaslian sebuah bukti digital untuk di analisa dengan memberikan ilustrasi secara detail peran Digital Forensik dalam mengungkap hasilnya sesuai dengan aturan hukum yang berlaku di Indonesia menggunakan alur kerja NIST	Metode NIST dapat diterapkan sebagai salah satu acuan standar Dalam proses pembuktian sebuah file Elektronik yang terindikasi sebagai bukti digital.	Data berupa file gambar dan video	Menggunakan metode NIST	metode video forensik selain NIST serta aplikasi pendukung pembuktian bukti digital masih memungkinkan untuk diimplementasikan. Sehingga dapat diperoleh keragaman cara pencarian bukti digital pada artefak data.

Usulan pada penelitian ini diantaranya adalah :

Membuat sebuah aplikasi pendukung didalam proses investigasi digital forensik menggunakan bahasa pemrograman java berbasis desktop , dimana pada aplikasi tersebut terdapat fitur seperti pembacaan korelasi metadata yang lebih detail. Serta dukungan penampilan foto pada file format gambar, hal ini memudahkan didalam melihat sebuah file bukti secara cepat dan tepat. Fitur lain adalah pendeteksi aplikasi photoshop , dalam kasus tertentu jika sebuah format gambar telah diedit menggunakan aplikasi photoshop maka aplikasi akan secara otomatis mendeteksi perubahan metadata tersebut. Aplikasi yang dibangun menggunakan bahasa pemrograman java (berbasis open source) sehingga dapat dikembangkan di kemudian hari, aplikasi ini juga dapat berjalan di berbagai sistem operasi diantaranya (windows , linux dan Mac Os). Namun pada penelitian ini pengujian aplikasi dilakukan pada sistem operasi windows.