BAB II

TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 *File*

File adalah berkas yang disimpan pada suatu perangkat berupa komputer atau *smartphone* yang dapat diakses dan diatur oleh pengguna (Pabokory dkk., 2016). *File* tidak selalu berupa berkas tertentu saja. Setiap berkas baik itu berkas Gambar, berkas video dan berkas aplikasi itu menjadi bagian dari *file*. Menurut Edi S. Mulyanta, *file* merupakan urutan data yang digunakan untuk melakukan *encode* informasi digital untuk urusan penyimpanan & pertukaran data (Prawiro, 2022).

File Carving

File Carving adalah bagian dari *Digital Forensic Examination* (DFE) dan merekonstruksi *file* berdasarkan isinya, daripada menggunakan *metadata* yang menunjuk kepada konten. Cara lain yang bisa dilakukan dengan memanfaatkan *file header* dan *file footer* untuk mengidentifikasi *file*. *File header* dan *file footer* direpresentasikan dengan cara tertentu dapat disebut *file signature* (Nugis, 2018).

File Header

Suatu *file* memiliki penanda yang mencakup awal *file* yaitu *file header* dan akhir data yaitu *file footer* yang dikenal sebagai *file signature* (Ali dkk., 2018). Sistem operasi atau perangkat lunak akan membaca

informasi yang terdapat pada *header* tersebut dan mengetahui tipe *file* dari sebuah *file*. Sebagian besar format standar *file* memiliki header dan footer unik yang digunakan dalam proses mengidentifikasi (Alherbawi dkk., 2013).

File Footer atau Trailer

File trailer adalah bagian penutup dari sebuah *file* dan merupakan penanda akhir sebuah *file*. Karena header dan footer berfungsi sebagai pengidentifikasi setiap tipe *file* (Neaimi dkk., 2020). *File footer* tidak ada hubungannya dengan 'angka ajaib', tetapi terkadang juga dapat dilihat dengan melihat konten *file* (Nugis, 2018).

2.1.2 *Signature*

Signature adalah sesuatu yang menjadi tanda unik untuk mempermudah dalam mengenali apa yang dimaksud, *signature* bisa berupa kata atau angka. Sebagai contoh signature dalam bentuk kata sering kita temui pada beberapa elemen bisnis yang bertujuan agar pelanggan mudah mengenali produk. Sedangkan *signature* berupa angka bisa kita jumpai pada *header* suatu *file* yang setiap ekstensi memiliki *signature* masing-masing sebagai mekanisme orisinalasi (Agung, 2016).

2.1.3 *File Signature*

File signature adalah nomor unik dalam *header* sebuah *file* yang digunakan untuk mengidentifikasi atau memverifikasi integritas konten dari sebuah *file. Pada* pengetahuan umum ekstensi *file* adalah akhiran berupa nama atau identitas

pada *file* komputer yang menunjukkan tipe *file*. Suatu *file* diidentifikasi oleh ekstensi, namun ada hal lain yang lebih mendalam untuk proses identifikasi suatu *file* yaitu dengan mengetahui *header* dari suatu *file (Eloff J., 2017)*.

Penggunaan *file signature* diperlukan untuk sistem komputer karena dengan jelas menunjukkan tipe *file* dan unik satu sama lain. Untuk memverifikasi tipe *file*, *file signature* dan ekstensi *file* setiap *file* harus cocok satu sama lain; jika tidak, itu dianggap tidak autentik (Neaimi dkk., 2020).

Magic Number

Magic number atau angka ajaib dapat diartikan kumpulan *byte* yang terdapat dalam *file* dan digunakan untuk mengidentifikasi *file*, biasanya *magic number* atau angka ajaib dapat temukan pada bagian awal dari digit angka. Setiap ekstensi *file* memiliki *magic number* yang berbeda-beda dan biasanya *magic number* itu terdiri dari 2-8 digit angka. *Magic number* juga dapat berfungsi untuk menentukan keaslian sebuah *file*. Penggunaan *magic number* sangat penting ketika akan melakukan identifikasi terkait dengan sebuah *file* (Kustian, 2023).

Magic number merupakan salah satu ilmu forensik yang membantu dalam pengolahan data digital (Rizal dkk., 2020). Pengertian *Magic number* dalam buku Tony Sammes "*Forensic Computing*" adalah suatu kode berupa angka heksadesimal untuk menentukan format suatu *file* data yang biasanya terletak di awal *file*. Tujuan *magic number* adalah meningkatkan pengelolaan informasi format *file* dan meningkatkan reliabilitas identifikasi tipe *file* (Underwood, 2009).

Tabel 2.1 Contoh *File* Signature atau Magic Number

No	Ekstensi *File*	*File Signature*	Deskripsi
1	DOCX	50 4B 03 04	Microsoft Office Document
2	JPG	FF D8 FF DB	Jpeg Image
3	PDF	25 50 44 46 2D	PDF Document
3	RTF	7B 5C 72 74 66 31	Rich Text Format

2.1.4 *Mime Type*

Multipurpose Internet Mail Extension (MIME) adalah mekanisme yang digunakan untuk mengirim berbagai informasi seperti teks, aplikasi, gambar, suara, video, dan lain-lain. MIME type mempunyai dua bagian, yaitu: *type* dan *subtype*. Kedua hal tersebut dipisahkan oleh *string* (/) (Santi dkk., n.d.). Contohnya, MIME *type* untuk *file* JPEG (*Joint Photographic Expert Group*) adalah *image* dan *subtype* adalah *jpeg*. Apabila digabungkan, MIME *type* yang lengkap adalah *image/jpeg*.

2.1.5 Perulangan (*Looping*)

Perulangan merupakan perulangan sejumlah aksi yang sama sebanyak jumlah yang ditentukan atau kondisi yang diinginkan oleh pembuatnya (Muhammad Romzi & Kurniawan, 2020).

Perulangan For

Perulangan *for* akan berjalan apabila diakhiri atau dipisahkan dengan tanda titik koma (;). Pernyatan bisa berupa pernyataan tunggal maupun

jamak. Jika berbentuk jamak, maka pernyataan-pernyataan tersebut harus diletakkan di antara kurung kurawal buka ({) dan kurung kurawal tutup (}) (Putri dkk., 2023).

Perulangan While

Perulangan *while* akan melakukan pengecekan kondisi terlebih dahulu sebelum dilakukan perulangan. Jika bernilai benar atau *true* maka perulangan akan dilakukan. Jika bernilai salah atau *false* maka perulangan tidak akan dilakukan. Blok *statement* tidak harus ada. Struktur tanpa *statement* akan tetap dilakukan selama kondisi masih benar atau *true*, Perulangan akan terus dilakukan sampai kondisi salah atau *false* (Putri dkk., 2023).

Perulangan While Do

Perulangan *while do* akan dilakukan minimal satu kali terlebih dahulu, kemudian dilakukan pengecekan selanjutnya terhadap kondisi. Jika kondisi benar atau true maka perulangan masih akan tetap berjalan. Perulangan dengan do while akan terus berjalan sampai kondisi salah atau *false* (Putri dkk., 2023).

2.2 Eksplorasi Jurnal

2.2.1 Review Jurnal

Merujuk Tabel 2.2 ditunjukan tahapan review jurnal penelitian ini yang bertujuan mendapatkan referensi untuk kelanjutan penelitian pada tahap selanjutnya.

Tabel 2. 2 Review Journal

No	Penulis/Tahun	Judul	Metode	State Of The Art
1	Mehdi Chehel Amirani, Mohsen Toorani And Ali A. Beheshti/2008	*A New Approach to Content-based File Type Detection*	*Principal Component Analysis* (PCA)	• Penelitian ini menerapkan *Principal Component Analysis* (PCA) dan jaringan saraf berfokus pada deteksi jenis *file* berbasis konten dengan menggunakan sampel *file doc, exe, gif, htm, jpg* dan *pdf*. • Tingkat klasifikasi total sebesar 98,33% diperoleh ketika mempertimbangkan

No	Penulis/Tahun	Judul	Metode	State Of The Art
				keseluruhan isi *file* dan tanpa spesifik ukuran *file*.
2	Michael Yip/2008	*Signature analysis and Computer Forensics*	Mengubah Ekstensi	• Penelitian ini menyajikan metode analisis informasi yang disebut analisis *file signature* dibutuhkan untuk menunjang proses *Computer Forensics*. • Proses yang dilakukan dengan membandingkan *file header* dan ekstensi dengan basis informasi *file header* beserta ekstensi yang dikenal dalam upaya untuk memverifikasi seluruh *file* di media penyimpanan dan menemukan yang mungkin disembunyikan.
3	Igor Santos, Yoseba K. Penya, Jaime Devesa and Pablo G. Bringas/2009	*N-grams-Based File Signature For Malware Detection*	*Signature-based detection*	• Penggunaan *N-grams* sebagai *file signature* dapat efektif dalam mendeteksi *malware*

No	Penulis/Tahun	Judul	Metode	State Of The Art
				yang tidak diketahui dengan tingkat kesalahan yang rendah. • *N-grams Based file signature* dengan panjang 4 *byte* memberikan rasio deteksi terbaik • Penelitian ini menunjukkan *file signature* berbasis *N-grams* dapat efektif dalam mendeteksi *malware* yang tidak diketahui
4	Rob Hegarty and John Haggerty/2015	*SlackStick: Signature-Based File Identification for Live Digital Forensics Examinations*		• Memperkenalkan pendekatan *SlackStick* yang baru dan efektif untuk mengidentifikasi *file* yang penting selama investigasi forensik digital secara langsung. • Pendekatan ini menggunakan skema *signature* alternatif yang tidak memerlukan pra-pemrosesan dari bukti digital.

No	Penulis/Tahun	Judul	Metode	State Of The Art
				• *SlackStick* otomatis berjalan dari perangkat eksternal seperti *flashdisk*
5	Osvaldo A. Rosso, Raydonal Ospin and Alejandro C. Frery/2016	*Classification and Verification of Handwritten Signatures with Time Causal Information Theory Quantifiers*		• Penelitian ini melakukan pendekatan baru untuk klasifikasi *signature* serta verifikasi bersumber pada tulisan tangan yang berasal dari teori data kausal waktu. • Penelitian ini tidak memerlukan perangkat keras yang sangat khusus yang mampu menangkap kecepatan, tekanan, orientasi. • Klasifikasi dilakukan oleh mesin vektor dukungan satu kelas yang dilatih dengan *signature* asli.
6	Moh. Subli , Bambang Sugiantoro, Yudi Prayudi /2017	*Metadata* Forensik Untuk Mendukung Proses Investigasi Digital	*Metadata*	• Penelitian ini dapat melihat langsung *metadata file* secara umum dan juga dapat menemukan *file-file* berdasarkan korelasi

No	Penulis/Tahun	Judul	Metode	State Of The Art
				file dengan parameter dari *metadata file* tersebut. • Membuat program untuk untuk melihat sejauh mana kemungkinan pemanfaatan *metadata* untuk mendukung proses investigasi digital • Pengujian sistem menggunakan tujuh macam tipe jenis *file* yang diuji yaitu DOCX, PDF, JPG, MP3, MP4, DD dan E01. • Karakteristik *metadata file* dibagi dalam tiga bagian; *metadata* secara *general*, *metadata* detail dan *metadata* nilai *checksum*. *Metadata* General terdiri dari lokasi *file*, nama *file, type file, owner* dan *computer.*

No	Penulis/Tahun	Judul	Metode	State Of The Art
7	Konstantinos Karampidis and Giorgos Papadourakis/2017	*File Type Identification Computational Intelligence for Digital Forensic*	*Computational Intelligence Techniques*	• Penelitian ini menerapkan Metodologi yang diusulkan pada tiga jenis *file* gambar yang paling umum (*jpg, png* dan *gif*) serta gambar *tiff* yang tidak terkompresi. • Menjelaskan cara kerja m*agic number* dan batasan-batasannya, termasuk fakta bahwa *magic number* hanya berfungsi pada jenis *file* biner. • Penelitian ini menyoroti masalah-masalah yang terkait dengan penggunaan ekstensi *file*, seperti mudahnya pemalsuan dan ketiadaan keharusan untuk menggunakan ekstensi pada sistem Linux.
8	Steve Mead/2018	*Unique File Identification in the*		• *National Software Reference Library (NSRL*) menyediakan *repositori* perangkat lunak yang dikenal, *file profil*, dan *signature file* untuk digunakan oleh penegak hukum

No	Penulis/Tahun	Judul	Metode	State Of The Art
		National Software Reference Library		serta organisasi lain yang ikut serta dengan penyelidikan forensik komputer. • Penelitian ini menyatakan bahwa kemungkinan kecil ada *crash file signature* dalam NSRL dan serangan terbaru terhadap algoritma *hash* tidak menimbulkan ancaman khusus terhadap NSRL.
9	Mohammed Al Neaimi, Hussam Al Hamadi, Chan Yeob Yeun, M. Jamal Zemerly/2020	*Digital Forensic Analysis of Files Using Deep Learning*	*Deep Learning*	• Penelitian ini menerapkan *deep learning* untuk menyelidiki pendekatan forensik mengidentifikasi jenis *file* dan mengatasi keterbatasan pendekatan sebelumnya. • Penelitian ini menyoroti proses deteksi jenis *file* berkonsentrasi pada dua informasi utama: label ekstensi *file* dan nilai heksadesimal dari konten *file* nilai heksadesimal memiliki *signature* dari jenis *file* yang ditempatkan di *header* dan *footer*.

No	Penulis/Tahun	Judul	Metode	State Of The Art
				Sedangkan untuk penjahat yang ingin menyembunyikan informasi sensitif, lebih mudah untuk mengubah ekstensi *file*, yang diizinkan oleh sebagian besar sistem operasi yang dikenal. • Hasil pengujian mendapatkan nilai akurasi di atas 98.75% dengan menggunakan 3 model pengujian. Batasan penelitian ini menggunakan 8 ekstensi sebagai pengujian.
10	Ardiansyah, Nila Hardi, Windu Gata/2020	Identifikasi *File* JPEG dengan Metode *Signature-Based*	*Signature-Based Carving*	• Penelitian menjelaskan identifikasi dan *recovery file* JPEG dengan metode *Signature Based Carving*, sebuah metode *carving* yang paling sederhana, dengan sebuah model diagram *Finite State Automata* (FSA), sebuah model algoritma dasar dalam teori komputasi.

No	Penulis/Tahun	Judul	Metode	State Of The Art
				• Pengujian penelitian menggunakan data berupa *disk image* yang disediakan untuk publik dari DigitalCorpora.org. • Hasil penelitian model FSA tersebut dapat mengidentifikasi dan melakukan *recovery file* JPEG dengan metode *Signature-Based Carving* dengan syarat dan kondisi; tidak terfragmentasi dan memiliki *header* dan *footer* yang utuh.
11	Randi Rizal, Ruuhwan, Septian Chandra/2020	*Signature File Analysis Using The National Institute Standard Technology Method Base on Digital Forensic Concepts*	*National Institute Standard Technology*	• Penelitian menyoroti *file signature* atau angka ajaib adalah salah satu teknik ilmu forensik yang membantu dalam memproses data digital. • Penelitian menggunakan metode National *Institute Standards Technology* untuk menganalisis keaslian data digital dan metode pembuktian untuk memperoleh

No	Penulis/Tahun	Judul	Metode	State Of The Art
				bukti yang valid selama proses identifikasi data atau isi *file*. • Penelitian menggunakan aplikasi Access Data FTK *Imager* versi 4.2.0 dan *winhex* versi 18.6 untuk melakukan proses investigasi. • Hasil penelitian ini *file signature* dapat digunakan untuk investigasi kasus dalam mengidentifikasi dan memverifikasi jenis *file* sehingga *file* yang telah dimodifikasi dapat dipulihkan dan dapat dibaca oleh sistem operasi dengan memeriksa jenis *file* melalui nilai heksadesimal dalam *file header* (awalan *file*) yang menunjukkan karakteristik masing- masing jenis *file* sehingga jenis *file* dapat ditemukan dan *file* tersebut dapat dibaca oleh sistem operasi.

No	Penulis/Tahun	Judul	Metode	State Of The Art
12	Fakhrul Rifqi Darmawan/2024	Identifikasi File Ekstensi Berdasarkan Metadata Pada Aplikasi File Signature Analyzer 2.0	*Looping*	• Penelitian ini menggunakan algoritma pengulangan untuk mendapatkan ekstensi yang sesuai melalui aplikasi *File Signature Analyzer* 2.0. • Penelitian ini mendukung 196 ekstensi dan 268 *signature* • Pengujian penelitian ini menggunakan 246 *file* orisinal dan 250 *file* modifikasi dengan metode *merubah* ekstensi dan menghilangkan ekstensi.

2.2.2 Jurnal Terdekat

Merujuk tabel 2.3 ditunjukan jurnal terdekat sebagai referensi perbandingan dengan penelitian sebelumnya

Tabel 2.3 Jurnal Terdekat

No	Penulis/Tahun	Judul	Tujuan	Persamaan Penelitian Terkait dengan Penelitian yang dilakukan	Perbedaan Penelitian Terkait dengan Penelitian yang dilakukan
1	Mehdi Chehel Amirani, Mohsen Toorani And Ali A. Beheshti/2008	*A New Approach to Content-based File Type Detection*	Mendeteksi jenis *file* dan pengelompokan jenis *file* berdasar kepada PCA dan jaringan Saraf	Peneliti memiliki tujuan yang sama yaitu untuk mendeteksi *file*.	Penelitian terkait : Mendeteksi jenis *file* dan mengelompokan *file*. Penelitian yang dilakukan : Mendeteksi orisinalitas ekstensi *file.*
2	Michael Yip/2008	Signature analysis and Computer Forensics	Menganalisis data berdasar kepada *signature file* untuk	Peneliti memiliki tujuan yang sama untuk menganalisis *file* berdasar kepada *signature* untuk	Penelitian terkait : Menganalisa jenis *file* ekstensi menggunakan metode merubah

No	Penulis/Tahun	Judul	Tujuan	Persamaan Penelitian Terkait dengan Penelitian yang dilakukan	Perbedaan Penelitian Terkait dengan Penelitian yang dilakukan
			mendukung proses forensik komputer.	mendukung proses forensik.	*signature* secara langsung melalui aplikasi *winhex editor.* Penelitian yang dilakukan : Menganalisa jenis *file* ekstensi berdasar kepada metadata *file* menggunakan aplikasi *file signature analyzer 2.0* yang membuat proses analisa menjadi otomatis.

No	Penulis/Tahun	Judul	Tujuan	Persamaan Penelitian Terkait dengan Penelitian yang dilakukan	Perbedaan Penelitian Terkait dengan Penelitian yang dilakukan
3	Konstantinos Karampidis and Giorgos Papadourakis/2017	*File Type Identification Computational Intelligence for Digital Forensic*	Mengidentifikasi jenis *file* yang mengalami proses modifikasi dengan menggunakan teknik kecerdasan komputasi. Menggunakan tiga jenis tipe *file* gambar (jpg, png dan tiff).	Peneliti memiliki topik yang sama yaitu mendeteksi jenis file dan melakukan pengujian dengan mengubah file dalam perspektif forensik digital.	Penelitian terkait : Mengidentifikasi jenis *file* dengan teknik kecerdasan komputasi dan diterapkan kepada tipe *file* gambar. Penelitian yang dilakukan : Mengidentifikasi ekstensi *file* dengan teknik *looping* dan diterapkan kepada tipe *file* gambar, video,

No	Penulis/Tahun	Judul	Tujuan	Persamaan Penelitian Terkait dengan Penelitian yang dilakukan	Perbedaan Penelitian Terkait dengan Penelitian yang dilakukan
					dokumen, buku digital, audio, huruf dan *file* terkompresi.
4	Mohammed Al Neaimi, Hussam Al Hamadi, Chan Yeob Yeun, M. Jamal Zemerly/2020	*Digital Forensic Analysis of Files Using Deep Learning*	Menyelidiki pendekatan forensik untuk mengidentifikasi jenis *file* dan mengembangkan pendekatan baru berdsar kepada *deep learning*	Peneliti memiliki topik yang sama yaitu mengidentifikasi jenis *file*.	Penelitian terkait : Mengidentifikasi jenis file berdsar kepada *deep learning.* Penelitian yang dilakukan : Mengidentifikasi jenis ekstensi *file* berdasar kepada metadata.

No	Penulis/Tahun	Judul	Tujuan	Persamaan Penelitian Terkait dengan Penelitian yang dilakukan	Perbedaan Penelitian Terkait dengan Penelitian yang dilakukan
5	Ardiansyah, Nila Hardi, Windu Gata/2020	Identifikasi *File* JPEG dengan Metode *Signature-Based* Carving dalam Model Automata	Menggunakan *file* jpeg sebagai acuan identifikasi untuk proses digital forensik menggunakan metode *signature based carving*.	Peneliti memiliki topik yang sama yaitu identifikasi *file* untuk proses forensik digital.	Penelitian terkait : Menggunakan file jpeg sebagai identifikasi untuk proses forensik digital dengan menggunakan metode signature based carving. Penelitian yang dilakukan : Menggunakan tipe file gambar, video, dokumen, buku digital, audio, huruf dan *file* terkompresi

No	Penulis/Tahun	Judul	Tujuan	Persamaan Penelitian Terkait dengan Penelitian yang dilakukan	Perbedaan Penelitian Terkait dengan Penelitian yang dilakukan
					sebagai acuan identifikasi untuk proses forensik digital dengan berdasar kepada metadata.
6	Randi Rizal, Ruuhwan, Septian Chandra/2020	*Signature File Analysis Using The National Institute Standard Technology Method Base on Digital Forensic Concepts*	Menganalisis keaslian data digital dan metode pembuktian untuk memperoleh bukti yang valid selama proses identifikasi	Peneliti memiliki tujuan yang sama untuk menganalisis keaslian file berdasar kepada signature file.	Penelitian terkait : Menggunakan aplikai access data FTK Imager versi 4.2.0 dan WinHex versi 18.6 sebagai acuan untuk proses identifikasi file.

No	Penulis/Tahun	Judul	Tujuan	Persamaan Penelitian Terkait dengan Penelitian yang dilakukan	Perbedaan Penelitian Terkait dengan Penelitian yang dilakukan
			data berdasar kepada signature file.		Peneltiian yang dilakukan : Menggunakan aplikasi file signature analyzer 2.0 sebagai acuan untuk proses identifikasi file ekstensi secara otomatis yang mendukung 196 ekstensi dan 269 signature file.

2.2.3 Matriks Penelitian

Merujuk tabel 2.4 ditunjukan matriks penelitian sebagai perbandingan penelitian yang dilakukan dengan penelitian sebelumnya dari beberapa aspek dalam ruang lingkup penelitian yang dilakukan.

Tabel 2.4 Matriks Penelitian

No	Peneliti/Tahun	Judul	Ruang Lingkup Peneltian											
			Preparation		Metode	Implementasi		Tipe *File*						
			Identifikasi	Verifikasi	Analisis *Signature File*	*Signature File*	Forensik	*Image*	*Video*	*Audio*	Terkompresi	Dokumen	Huruf	*E-book*
1	Mehdi Chehel Amirani, Mohsen Toorani And Ali A. Beheshti/2008	*A New Approach to Content-based File Type Detection*	√		√	√		√				√		

No	Peneliti/Tahun	Judul	Ruang Lingkup Peneltian											
			Preparation		**Metode**	**Implementasi**		**Tipe *File***						
			Identifikasi	Verifikasi	Analisis *Signature File*	*Signature File*	Forensik	*Image*	*Video*	*Audio*	Terkompresi	Dokumen	Huruf	*E-book*
2	Michael Yip/2008	*Signature analysis and Computer Forensics*	√	√	√	√	√	√				√		
3	Konstantinos Karampidis and Giorgos Papadourakis/2017	*File Type Identification Computational Intelligence for Digital Forensic*	√		√	√	√	√						

No	Peneliti/Tahun	Judul	Ruang Lingkup Peneltian											
			Preparation		Metode	Implementasi		Tipe *File*						
			Identifikasi	Verifikasi	Analisis *Signature File*	*Signature File*	Forensik	*Image*	*Video*	*Audio*	Terkompresi	Dokumen	Huruf	*E-book*
4	Mohammed Al Neaimi, Hussam Al Hamadi, Chan Yeob Yeun, M. Jamal Zemerly/2020	*Digital Forensic Analysis of Files Using Deep Learning*	√	√			√	√	√	√		√		

No	Peneliti/Tahun	Judul	Ruang Lingkup Peneltian											
			Preparation		**Metode**	**Implementasi**		**Tipe *File***						
			Identifikasi	Verifikasi	Analisis *Signature File*	*Signature File*	Forensik	*Image*	*Video*	*Audio*	Terkompresi	Dokumen	Huruf	*E-book*
5	Ardiansyah, Nila Hardi, Windu Gata/2020	Identifikasi *File* JPEG dengan Metode *Signature-Based Carvi*ng dalam Model Automata	√		√	√		√						

No	Peneliti/Tahun	Judul	Ruang Lingkup Peneltian											
			Preparation		Metode	Implementasi		Tipe *File*						
			Identifikasi	Verifikasi	Analisis *Signature File*	*Signature File*	Forensik	*Image*	*Video*	*Audio*	Terkompresi	Dokumen	Huruf	*E-book*
6	Randi Rizal, Ruuhwan, Septian Chandra/2020	*Signature File Analysis Using The National Institute Standard Technology Method Base on Digital Forensic Concepts*	√		√		√	√				√		

No	Peneliti/Tahun	Judul	Ruang Lingkup Peneltian											
			Preparation		**Metode**	**Implementasi**		**Tipe *File***						
			Identifikasi	Verifikasi	Analisis *Signature File*	*Signature File*	Forensik	*Image*	*Video*	*Audio*	Terkompresi	Dokumen	Huruf	*E-book*
7	Fakhrul Rifqi Darmawan/2024	Identifikasi File Ekstensi Berdasarkan Metadata Pada Aplikasi File Signature Analyzer 2.0	√	√	√	√	√	√	√	√	√	√	√	√