BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Pada bab ini, dilakukan tinjauan pada literatur penelitian sebelumnya mengenai digital forensik guna mengumpulkan referensi dan informasi terkait dengan penelitian ini.

Tabel 2. 1 *Journal Mapping*

No	Judul Penelitian	Peneliti	Metode	Pembahasan	Hasil
1	A Novel Digital Forensik Framework for Data Breach Investigation (2023)	Arif Rahman Hakim, Kalamullah Ramli, Teddy Surya Gunawan, Susila Windarta	D4I	Jurnal tersebut membahas masalah peningkatan tren pelanggaran data dan dampaknya terhadap organisasi, khususnya perusahaan kecil dan menengah. Masalah utama yang diangkat adalah tantangan dalam menyelidiki insiden pelanggaran data secara efisien dan efektif. Untuk mengatasi masalah ini, jurnal tersebut	Hasil penelitian dari jurnal tersebut menunjukkan bahwa kerangka kerja digital forensik baru yang diusulkan berhasil memberikan jawaban komprehensif terhadap pertanyaan investigasi 5W1H (Who, What, When, Where, Why, How). Studi kasus yang disajikan dalam penelitian ini juga menunjukkan bahwa kerangka kerja tersebut dapat diterapkan

				mengusulkan kerangka kerja digital forensik baru yang menggunakan fase kerusakan data (DBB) untuk mengkategorikan artefak dan meningkatkan analisis 5W1H (Who, What, When, Where, Why, How). Kerangka kerja ini dirancang untuk memberikan jawaban komprehensif terhadap pertanyaan investigasi 5W1H dan memfasilitasi proses analisis yang lebih tepat dan menyeluruh.	dengan baik dalam berbagai insiden pelanggaran data, memberikan hasil yang lebih tepat dan menyeluruh. Selain itu, penelitian ini menyoroti dampak finansial dari pelanggaran data yang terus meningkat secara global, terutama bagi perusahaan kecil dan menengah.
2	D4I - Digital forensik framework	Athanasios Dimitriad	D4I	Pembahasan masalah pada jurnal tersebut	Berdasarkan hasil pembahasan kerangka kerja

	for reviewing and investigating cyber attacks (2020)	is, Nenad Ivezic, Boonserm Kulvatunyou, Ioannis Mavridis		adalah kurangnya kerangka kerja yang sistematis dan terperinci untuk meninjau dan menyelidiki serangan siber. Proses digital forensik yang ada saat ini tidak cukup mendetail dalam menggambarkan fase pemeriksaan dan analisis yang diperlukan untuk investigasi serangan siber, sehingga sulit bagi pemeriksa digital forensik untuk mengikutinya dengan mudah.	D4I, Keterbatasan Alat Cerdas, Model CKC, Kategorisasi Artefak, dll., menunjukkan bahwa kerangka kerja D4I menawarkan solusi yang lebih terstruktur dan terperinci untuk investigasi serangan siber, yang dapat membantu perusahaan melindungi data sensitif mereka dari ancaman siber yang semakin kompleks.
3	Analisis Media Sosial Facebook Lite dengan *tool*s Forensik menggunaka	Rauhulloh Ayatulloh Khomeini Noor Bintang,	NIST	Pembahasan masalah pada jurnal tersebut mencakup proses mendapatkan data forensik yang dapat	Hasil pembahasan masalah pada jurnal tersebut menunjukkan bahwa penelitian berhasil mendapatkan data

	n Metode NIST (2020)	Rusydi Umar, Anton Yudhana		dipertanggungjawabkan di pengadilan. Penelitian ini menggunakan perangkat *smartphone* dengan sistem operasi Android dan alat forensik MOBILedit Forensik untuk mengumpulkan barang bukti digital. Hasil yang diperoleh dari alat forensik ini meliputi akun ID, gambar, audio, dan video.	forensik yang dapat dipertanggungjawabkan di pengadilan. Proses pengumpulan barang bukti digital dilakukan melalui perangkat *smartphone* dengan sistem operasi Android menggunakan alat forensik MOBILedit Forensik. Hasil yang diperoleh dari alat forensik ini meliputi akun ID, gambar, audio, dan video..
4	Analisis Pencarian Data *Smartphone* Menggunakan NIST Untuk Penyelidikan Digital (2023)	Riya Majalista, Tata Sutabri	NIST	Pembahasan masalah pada jurnal ini adalah mengenai analisis pencarian data pada *smartphone* menggunakan metode National Institute of Standards and	Hasil pembahasan masalah pada jurnal ini menunjukkan bahwa penggunaan metode National Institute of Standards and Technology (NIST) dalam analisis data

				Technology (NIST) untuk penyelidikan digital forensik. Penelitian ini bertujuan untuk menganalisis informasi yang dapat digunakan sebagai dasar ilmu forensik dalam membantu penyelesaian kasus kejahatan dunia maya. Fokus utama adalah pada data yang tersimpan di aplikasi WhatsApp, seperti kontak, percakapan, gambar, dan foto, yang diharapkan dapat menjadi bukti suatu tindakan kejahatan yang terjadi di dunia maya.	smartphone dapat membantu penyelidikan digital forensik dengan efektif. Data yang dianalisis, terutama dari aplikasi WhatsApp, termasuk kontak, percakapan, gambar, dan foto, dapat digunakan sebagai bukti dalam kasus kejahatan dunia maya. Penelitian ini menekankan pentingnya prosedur yang tepat dalam pengumpulan dan analisis data untuk memastikan keabsahan bukti yang ditemukan.
5	Akuisisi Bukti Digital	Imam Riadi,	NIST	Permasalahan yang dibahas	Hasil penelitian pada jurnal

	Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST) (2021)	Rusydi Umar, Muhammad Irwan Syahib		dalam jurnal ini adalah bagaimana melakukan akuisisi bukti digital dari aplikasi Viber Messenger pada perangkat Android menggunakan metode National Institute of Standards and Technology (NIST). Penelitian ini bertujuan untuk membuktikan apakah bukti-bukti digital yang telah dihapus atau dihilangkan oleh pelaku kejahatan dapat diakuisisi kembali	tersebut menunjukkan bahwa alat forensik MOBILedit Forensik Express dan Belkasoft berhasil mendapatkan bukti digital dengan persentase 100% untuk akun, kontak, gambar, dan video. Namun, untuk bukti digital berupa chat, kedua alat tersebut hanya berhasil mendapatkan 50%. Sementara itu, alat forensik Autopsy tidak memberikan hasil yang diharapkan dalam proses ekstraksi, dengan kata lain, aplikasi Autopsy memberikan hasil nol (zero result)
6	Analisis Web Phising Menggunaka	Sutarti, Siswanto, dan	Network Forensic	Permasalahan yang dibahas adalah tentang	Hasil dari penelitian yang dibahas dalam

	n Metode Network Forensic dan Block Acces Situs Dengan Router Mikrotik (2022)	Ariansyah Bachtiar.		analisis web phishing menggunakan metode forensik jaringan dan pemblokiran akses situs dengan router Mikrotik. Fokus utama dari penelitian ini adalah pada keamanan jaringan dan pemulihan data dalam konteks digital forensik, dengan penekanan pada konsep Chain of Custody untuk menjaga integritas barang bukti. Selain itu, jurnal ini menjelaskan cara kerja web phishing, sumber ancaman, dan teknik yang digunakan oleh penyerang untuk	jurnal tersebut menunjukkan beberapa temuan penting terkait analisis dan pencegahan aktivitas phishing. Penelitian ini berhasil mengidentifikasi domain dan alamat IP yang terlibat dalam aktivitas phishing dengan menggunakan alat analisis jaringan seperti Wireshark. Selain itu, konfigurasi pada router Mikrotik berhasil memblokir akses ke situs phishing yang teridentifikasi, sehingga meningkatkan keamanan jaringan. Penelitian ini juga menekankan pentingnya

				mencuri informasi sensitif. Penelitian ini melibatkan penggunaan alat seperti Wireshark untuk menganalisis aktivitas phishing dan konfigurasi router Mikrotik untuk memblokir situs phishing. Tujuan dari penelitian ini adalah untuk meningkatkan keamanan jaringan dan memberikan pemahaman tentang serangan phishing, khususnya di lingkungan Sekolah Menengah Kejuruan Swasta (SMKS) YP 17 Cilegon.	forensik jaringan dalam mendeteksi dan mencegah serangan phishing, serta menyarankan penelitian lebih lanjut dengan alat tambahan dan pengembangan aplikasi peringatan untuk meningkatkan perlindungan terhadap kejahatan siber.

7	Analisis Perbandingan Tools forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop (2021)	Ikhsan Zuhriyanto, Anton Yudhana, dan Imam Riadi	DFRWS	Jurnal tersebut membahas investigasi forensik digital yang dilakukan pada *smartphone* Evercross B75, dengan fokus pada ekstraksi dan analisis data dari aplikasi Twitter. Studi ini menyoroti pentingnya forensik digital dalam mengidentifikasi dan menjaga bukti digital, terutama dalam konteks meningkatnya kejahatan siber di media sosial seperti Twitter. Hasil penelitian menunjukkan bahwa MOBILedit Forensic Express lebih efektif	Hasil dari penelitian tersebut menunjukkan bahwa perangkat lunak forensik digital MOBILedit Forensic Express lebih efektif dibandingkan dengan Belkasoft Evidence Center dalam mengidentifikasi bukti digital dari aplikasi Twitter pada *smartphone*. MOBILedit Forensic Express mencapai tingkat akurasi sebesar 85,75%, sedangkan Belkasoft Evidence Center hanya mencapai 43,75%.

				untuk investigasi forensik digital pada *smartphone*.	
8	Investigasi dan Analisis Forensik Digital Pada Percakapan Grup Whatsapp Menggunakan NIST-86 dan Support Vector Machine (2020)	M. Wahyu Indriyanto, Dedy Hariyadi, dan Muhammad Habibi.	NIST-86	Permasalahan yang dibahas dalam jurnal ini adalah tentang studi forensik digital dan analisis percakapan grup WhatsApp menggunakan kerangka kerja NIST SP 800-86 dan algoritma Support Vector Machine (SVM). Studi ini menyoroti tingginya penggunaan WhatsApp sebagai platform untuk kejahatan siber di Indonesia, sehingga diperlukan klasifikasi konten	Hasil dari penelitian tersebut menunjukkan bahwa analisis menggunakan algoritma Support Vector Machine (SVM) berhasil mengklasifikasikan percakapan grup WhatsApp dengan persentase sekitar 96,21% sebagai konten negatif. Persentase ini dapat dijadikan indikator awal dalam mendeteksi kualitas percakapan yang bersifat negatif, sehingga dapat membantu penyidik dalam mengambil tindakan penyidikan yang lebih intensif.

				percakapan yang efektif untuk membantu investigasi. Penelitian ini mencapai akurasi klasifikasi sekitar 96,21% untuk konten negatif dalam percakapan grup, menunjukkan potensinya sebagai indikator awal untuk mengidentifikasi percakapan berbahaya. Metodologi yang digunakan meliputi tahap pengumpulan, pemeriksaan, analisis, dan pelaporan, dengan fokus pada prapemrosesan data teks untuk analisis sentimen menggunakan SVM.	

9	Analisis dan Deteksi *Malware* menggunakan Metode *Malware* Analisis Dinamis dan *Malware* Analisis Statis	Triawan Adi Cahyanto, Victor Wahanggara, dan Darmawan Ramadana.	Analisa *Malware* Statis dan Dinamis	Jurnal tersebut membahas analisis dan deteksi *malware*, khususnya jenis *malware* Poison Ivy, menggunakan dua metode utama: analisis dinamis dan analisis statis. Analisis Dinamis adalah metode ini melibatkan eksekusi *malware* dalam lingkungan yang aman, seperti virtual lab, untuk mengamati perilakunya. Alat seperti Regshot dan Cuckoo Sandbox digunakan untuk memantau perubahan sistem dan aktivitas jaringan yang dilakukan oleh *malware*.	Hasil penelitian tersebut menunjukkan bahwa *malware* Poison Ivy memiliki karakteristik khas *malware*, termasuk modifikasi sistem dan operasi yang tersembunyi. Melalui analisis dinamis dan statis, ditemukan bahwa Poison Ivy melakukan modifikasi registry, membuat file baru, dan melakukan komunikasi jaringan dengan server. Analisis dinamis menggunakan alat seperti Regshot dan Cuckoo Sandbox mengungkapkan perubahan sistem dan aktivitas jaringan,

				Analisis ini mengungkapkan bahwa Poison Ivy membuat file baru, memodifikasi registry, dan melakukan komunikasi jaringan dengan server. Analisis Statis adalah metode ini melibatkan analisis kode sumber *malware* tanpa menjalankannya. Alat seperti `strings` dan IDA Pro digunakan untuk mengekstraksi dan menganalisis kode, mengidentifikasi karakteristik dan perilaku *malware* melalui analisis string dan bahasa assembly.	sementara analisis statis dengan alat seperti `strings` dan IDA Pro memberikan wawasan tentang kode sumber dan mekanisme kerja *malware*. Kedua metode analisis ini memberikan informasi yang saling melengkapi tentang perilaku *malware*. Penelitian ini juga merekomendasikan peningkatan pelatihan dalam teknik analisis statis dan eksplorasi teknik lanjutan seperti Reverse Engineering untuk analisis *malware*.

Pada tabel 2.1 ditampilkan mengenai literatur utama yang membahas analisa digital forensik menggunakan berbagai metode dan *framework.* Setiap penelitian yang dicantumkan dalam tabel ini diuraikan berdasarkan judul penelitian, tahun penelitian, penulis, metode, pembahasan dan hasil. Tabel ini berfungsi sebagai referensi perbandingan metode dan *framework* dalam analisa digital forensik, termasuk alat yang digunakan serta alur yang akan diterapkan dalam penelitian ini.

2.2 Kajian Pustaka

2.2.1 Digital Forensik

Digital forensik adalah salah satu cabang ilmu forensik yang proses identifikasi, pengumpulan, analisis, dan interpretasinya pada bukti digital untuk mendukung proses hukum. Proses ini melibatkan penggunaan berbagai alat dan teknik untuk mengidentifikasi pola, hubungan, dan informasi relevan dari data elektronik yang terkait dengan kejahatan atau insiden keamanan yang terjadi dalam lingkungan komputer atau jaringan.

Menurut pedoman *National Institute of Standards and Technology* (NIST) [10]**,** analisis forensik digital adalah proses ilmiah untuk mengumpulkan, menganalisis, dan menafsirkan bukti digital untuk mendukung penyelidikan hukum. Bukti digital dapat berupa data apa pun yang disimpan atau ditransmisikan secara elektronik, seperti dokumen, foto, video, audio, logfile, metadata, dan lain-lain.

2.2.2 Artefak Digital

Artefak digital adalah segala jenis data atau informasi yang dihasilkan, disimpan, atau diproses oleh perangkat digital yang dapat digunakan sebagai bukti dalam investigasi digital forensik. Artefak digital dapat berupa file, metadata, log aktivitas, rekaman percakapan, riwayat penelusuran, jejak digital, atau bahkan informasi cache yang tersisa di suatu perangkat [11].

2.2.3 *Malware*

Malware (malicious software) adalah perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, mencuri data, atau mendapatkan akses tanpa izin ke sistem komputer. *Malware* dibagi menjadi beberapa macam berdasarkan fungsinya seperti virus, *worm, trojan, ransomware, adware, spyware,* dan lain-lain [12]. Suatu *malware* dapat memiliki beberapa fungsi yang bergantung pada tujuan dari pembuatannya.

2.2.4 MOBILedit Express Forensic Tools

MOBILedit Forensik adalah perangkat lunak forensik yang digunakan oleh penyidik dan profesional keamanan untuk mengakses dan menganalisis data dari perangkat mobile, seperti ponsel, tablet, dan perangkat lain yang dapat menyimpan data digital. Pada penelitian ini, MOBILedit Express *tool*s digunakan untuk membantu dalam pengumpulan, pemrosesan, dan analisis data yang mungkin menjadi bukti dalam investigasi kriminal atau keamanan [13].

2.2.5 MobSF

Mobile Security Framework (MobSF) adalah framework pengujian otomatis berbasis *open-source* yang mampu melakukan analisis statis dan dinamis pada aplikasi. MobSF menghasilkan laporan yang memberikan informasi detail mengenai keamanan aplikasi Android tersebut [14]. Pada penelitian ini, MobSF digunakan sebagai *tool* deteksi dini *malware* pada sistem android.

2.2.6 Jadx GUI

Jadx GUI adalah *tool*s forensik berbasis GUI untuk mengekstraksi file dengan format .apk untuk mendapatkan data mengenai *classes, manifest file, metadata information* dan *media files* yang fokus pada aplikasi yang dikembangkan untuk Android [15]. Pada penelitian ini, Jadx GUI digunakan untuk mengektraksi dan dekompilasi file apk tanpa perlu menggunakan apk*tool*.