BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

2.1.1 Penelitian oleh Sarjimin, dkk. (2021)

Penelitian yang berjudul Perbandingan Tool Forensik pada Mozilla Firefox *Private* Mode Menggunakan Metode NIST,dilakukan oleh Sarjimin,dkk pada tahun 2021. Penelitian ini difokuskan untuk mencari bukti digital pada peramban Firefox mode *InPrivate* pada Linux Mint 19.3 dengan *tool* forensik Autopsy dan Belkasoft menggunakan metode *National Institute of Standards and Technology* (NIST). Pada penelitian ini ada 6 item parameter item percobaaan, yaitu kata kunci kucing,kata kunci harimau,kata kunci burung cendrawasih, kunjungan web facebook.com ,akun Gmail, dan kata sandi Gmail. Hasil penelitian ini menyimpulkan bahwa Belkasoft tidak dapat menghasilkan log yang diharapkan, sedangkan Autopsy bisa mendapatkan log yang diharapkan dengan persentase 83 %. Penelitian ini juga menegaskan lagi walaupun pengguna menggunakan peramban mode *private*, informasi tetap bisa diambil melalui RAM. [8]

2.1.2 Penelitian oleh Tri Rochmadi, dkk. (2021)

Penelitian yang berjudul Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar ,dilakukan oleh Tri Rochmadi pada tahun 2019. Penelitian ini dilakukan untuk menganalisa anti forensik pada peramban browzar dengan metode *live forensik*.Hasil dari penelitian ini dapat disimpulkan bahwa ditemukan riwayat, tanda waktu, dan kata sandi pada peramban browzar dengan tool WinHex dan Volatility Memory Forensic.[1]

2.1.3 Penelitian oleh Anton Yudhana, dkk. (2020)

Penelitan yang berjudul Analisis *Live Forensics* Aplikasi Media Sosial Pada Browser Menggunakan Metode *Digital Forensics Research Workshop*, dilakukan oleh Anton Yudhana ,dkk pada tahun 2020. Penelitian ini bertujuan untuk menganalisa bukti digital pada twitter dengan cara *live forensic* selanjutnya bukti digital akan dianalisa dengan menggunakan metode *Digital Forensics Research Workshop* menggunakan aplikasi FTK Imager. Berdasarkan dari hasil langkah-

langkah yang dikerjakan maka, dapat disimpulkan bahwa proses analisis data di media sosial Twitter dapat dikatakan memiliki bukti digital berupa bukti data yang valid.[9]

2.1.4 Penelitian oleh Ratri Ayunita Kinasih, dkk. (2020)

Analisis Keamanan Browser Menggunakan Metode *National Institute of Justi*ce, dilakukan oleh Ratri Ayunita Kinasih , dkk pada tahun 2020. Penelitian ini dilakukan untuk menganalisis keamanan pada browser Google Chrome, Mozilla Firefox, and Microsoft Edge menggunakan metode *National Institute of Justice.* Penelitian ini menggunakan teknik *live forensik* untuk akuisisi data , lalu data atau bukti digital yang didapat akan dianalisi menggunakan aplikasi FTK Imager sebagai tools forensics . Hasil pada penelitian ini dapat disimpulkan bahwa peramban Google Chrome, Mozilla Firefox, and Microsoft Edge tidak aman untuk mengakses facebook, karena peramban tersebut dapat mendeteksi *email* dan kata sandi facebook. Sedangkan untuk mengakses instagram browser Mozilla Firefox lebih aman digunakan karena tidak terdeteksi kata sandinya.[10]

2.1.5 Penelitian oleh Ilhami Algi Plianda, dkk. (2022)

Penelitian Analisa dan Perbandingan Performa Tool Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp, dilakukan oleh Ilhami Algi Plianda, dkk pada tahun 2022. Penelitian ini bertujuan untuk menganalis perbandingan performa *tool* forensik digital pada *instant message* Whatsapp di *smartphone* Samsung GT-S5282 menggunakan *tool* Oxygen Forensic dan MOBILedit. Penelitian ini menggunakan metode *National Institute of Standards and Technology* (NIST) dan menggunakan FTK Imager untuk proses imaging pada device. Hasil dari penelitian ini menunjukkan MOBILedit lebih unggul dari pada Oxygen Forensic dalam recovery data dengan rincian , MOBILedit mendapat bukti digital berupa 2 gambar, 1 video, 1 voice note, 2 log dan 10 *database* dengan artian semua data dapat dikembalikan. Sedangkan hasil ekstraksi data dengan Oxygen Forensics mendapatkan data 10 kontak, 1 video, 20 pesan chat, 1 panggilan, 21 event log dan 2 file data, dengan status data berhasil di restore hingga 6 kontak.[11]

Tabel 2. 1 Penelitian Terdahulu

No	Peneliti	Judul dan Tahun Terbit	Metode	Hasil Pembahasan	Perbedaan dengan penelitian yang dilakukan
1.	Sarjimin ,Herman , Anton Yudhana	Perbandingan Tool Forensik pada Mozilla Firefox Private Mode Menggunakan Metode NIST (2021)	*National Institute of Standar and Technology* (NIST)	Pada hasil penelitian perbandingan *forensic tool* antara Autopsy dan Belkasoft pada sistem operasi linux mint dengan studi kasus mozilla firefox private mode dapat disimpulkan bahwa Autopsy berhasil mendapatkan log yang diharapkan dengan presentase 83% , sedangkan Belkasoft tidak berhasil mendapatkan hasil yang di harapkan dengan presentase 0% .[8]	Studi kasus browser Mozilla Firefox private mode
2.	Tri Rochmadi	Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar(2019)	*Live Forensic*	Pada hasil analisis di browser browzar dapat ditemukan bukti digital berupa iwayat, tanda waktu, dan kata sandi dengan menggunakan *tool* WinHex dan Volatility Memory Forensic.[1]	Studi kasus adalah Browzar Menggunakan tool WinHex dan Volatility Memory Forensic Menggunakan metode *Live Forensic*
3.	Anton Yudhana , Imam Riadi , Ikhsan Zuhriyanto	Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research	*Digital Forensics Research Workshop (DFRWS)*	Berdasarkan beberapa hasil dari langkah langkah yang dilakukan, proses analisis data di media sosial Twitter dapat dikatakan memiliki bukti digital berupa bukti data yang valid.[9]	Studi kasus berfokus pada sosial media twitter Menggunakan metode *Digital Forensics Research Workshop (DFRWS)*

No	Peneliti	Judul dan Tahun Terbit	Metode	Hasil Pembahasan	Perbedaan dengan penelitian yang dilakukan
		Workshop (DFRWS)(2019)			
4.	Ratri Ayunita Kinasih, Arif Wirawan Muhammad, Wahyu Adi Prabowo	Analisis Keamanan Browser Menggunakan Metode National Institute of Justice (Studi Kasus: Facebook dan Instagram)(2020)	*National Institute of Justice (NIJ)*	Hasil penelitian saat ini menyimpulkan bahwa saat mengakses facebook , email dan kata sandi terdeteksi pada Google Chrome, Mozilla Firefox dan Microsoft Edge , jadi dapat disimpulkan bahwa browser kurang aman digunakan. Mozila firefox lebih aman digunakan untuk mengakses instagram karena tidak mendeteksi password jika dibandingkan dengan Mircrosoft Edge dan Google Chrome.[10]	Studi kasus befokus pada *Facebook* dan Instagram Menggunakan metode *National Institute of Justice (NIJ)*
5.	Ilhami Algi Plianda, Rini Indrayani	Analisa dan Perbandingan Performa Tools Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp (2022)	*National Institute of Standard and Technology* (NIST).	Hasil ekstraksi data dengan MOBILedit mendapat bukti digital berupa 2 gambar, 1 video, 1 voice note, 2 log dan 10 database dengan artian semua data dapat direstore. Sedangkan hasil ekstraksi data dengan Oxygen Forensics mendapatkan data 10 kontak, 1 video, 20 pesan chat, 1 panggilan, 21 event log dan 2 file data, dengan status data berhasil di restore hingga 6 kontak. Dapat disimpulkan bahwa pada skenario yg telah ditetapkan, MOBILedit lebih unggul dari pada Oxygen Forensic dalam *recovery* data.[11]	• Studi kasus befokus pada *instant messaging* Whatsapp pada smarphone samsung GT-S5282 Menggunakan *tools* MOBILedit dan Oxygen

2.2 Dasar Teori

2.2.1 Digital Forensik

Ilmu forensik adalah penggunaan teknik atau metode ilmiah untuk memberikan bukti yang benar di depan pengadilan atau pemeriksaan hukum terkait. Ilmu forensik juga digunakan untuk menjawab pertanyaan yang muncul pada saat proses penyelidikan tindak pidana, supaya nantinya kasus pidana yang terkait bisa dipertanggungjawabkan secara hukum. Digital forensik merupakan ilmu pengetahuan untuk mengidentifikasi atau menyelidiki bukti digital.[12] Digital Forensik adalah cabang dari ilmu forensik yang memfokuskan bukti-bukti yang berasal dari komputer atau sumber digital seperti file foto, *flash drive, hard disk*,surel,kata sandi ,log file, paket data dalam jaringan komputer.[13] Tujuan dari analisis digital forensik adalah untuk menganalisis dan mengamankan barang bukti digital untuk mendapat fakta yang aktual guna mendukung dalam proses penyelidikan pidana.[4]

2.2.2 Barang Bukti Digital

Barang bukti digital merupakan suatu elemen penting dalam digital forensik yang berfungsi sebagai barang bukti untuk kasus kejahatan dunia maya, dan barang bukti digital tidak selalu dalam bentuk fisik yang sebenarnya, sehingga keputusannya belum jelas[4].Barang bukti digital juga merupakan sumber informasi yang ada pada suatu perangkat.[14] Barang bukti digital dapat juga dijelaskan sebagai data yang di dihasilkan atau ditemukan pada barang elektronik manapun seperti *smartphone,* komputer, tablet. Setiap perangkat elektronik yang dikombinasikan dengan teknologi IoT merupakan sumber potensial dari bukti digital dan sangat penting untuk penyelidikan forensik. Pakar forensik mengumpulkan, mengidentifikasi, dan menyimpan bukti dari sumber-sumber ini untuk melacak pelaku kejahatan dan menyajikannya di pengadilan. Selain itu, potongan bukti digital terbukti berguna dalam menguatkan penyelidikan pada kasus.[4]

2.2.3 Analisis *Dead Forensic*

Dead Forensic merupakan teknik akuisisi bukti digital yang membutuhkan data yang tersimpan secara permanen dalam suatu perangkat keras penyimpanan seperti harddisk.[5] Teknik *dead forensic* memungkinkan penyelidik untuk memulihkan file yang dihapus atau rusak dari disk drive dan media penyimpanan lainnya. Teknik ini lebih akurat daripada menggunakan teknik *live forensic* karena data yang salah disimpan dalam harddisk komputer selama akuisisi dapat dengan mudah diperbaiki.

2.2.4 *Qutebrowser*

Qutebrowser merupakan peramban internet yang berbasis pada *python* dan *QT-engine.* Peramban ini bersifat *open source* yang dibuat oleh Florian Bruhin sebagai *primary author*[2]. Tidak seperti pada peramban umumnya, *Qutebrowser* merupakan browser yang memiliki tampilan yang minimalis yang berfokus pada penggunaan keyboard, yang artinya peramban ini difokuskan untuk pengguna *power-user* tidak untuk pengguna peramban pada umumnya. Walaupun *Qutebrowser* merupakan peramban yang minimalis tetapi, seiring berjalannya waktu fitur-fitur tertentu ditambahkan pada peramban ini, seperti *adblock*, Pada *Qutebrowser*, pengguna *power-user* juga dapat mengkostumisasi *workflow* pada peramban untuk menyesuaikan kebutuhan pengguna[2].

2.2.5 *LibreWolf*

Librewolf merupakan *free libre open source software* berasal dari *fork* Mozilla Firefox yang berfokus pada privasi, keamanan, dan kebebasan pengguna. [3]*LibreWolf* dibuat untuk menambah proteksi melawan pelacakan dengan meningkatkan sisi keamanannya. Hal ini bisa terwujud karena *LibreWolf* menggunakan pengaturan privasi dan keamanan khusus. *LibreWolf* bertujuan untuk menghilangkan semua telemetri , pengumpulan data dan menonaktifkan fitur yang anti dengan kebebasan seperti DRM.[3] Mesin pencarian yang digunakan pada *LibreWolf* adalah mesin pencarian yang mengedepankan privasi dari penggunanya seperti DuckDuckGo, Searx, dan Qwant , tidak menutup

kemungkinan pengguna dapat menambahkan mesin pencarian yang bersifat *proprietary* seperti Google , Yahoo, dan Bing.

2.2.6 Kejahatan Dunia Maya

Kejahatan dunia maya atau biasa yang disebut *cybercrime* merupakan tindak kejahatan yang dilakukan menggunakan jaringan komputer atau secara digital dengan menyalahgunakan teknologi digital sebagai alat kejahatan utamanya.[15] Kejahatan ini dikaitkan dengan penggunaan teknologi informasi yang tidak terbatas dan memiliki karakteristik teknologi yang kuat berdasarkan tingkat keamanan dan keandalan informasi yang dikirimkan dan diakses oleh konsumen internet.[16] Ini dapat melibatkan berbagai macam kejahatan, mulai dari meretas informasi pribadi individu, penipuan, hingga terorisme. Contoh kejahatan dunia maya sebagai berikut:

1. *Carding*

   Carding merupakan tindak kejahatan kriminal dimana pelaku mencuri nomor kartu kredit korban dan disalahgunakan dalam transaksi[15]
2. *Cyber Terrorism*

   Cyber Terrorism merupakan tindak kriminal yang dilakukan oleh pelaku untuk mengancam suatu pemerintahan atau perorangan. [15]
3. *Unauthorized Access*

   Akses tidak sah merupakan tindak infiltrasi secara illegal ke pada suatu sistem jaringan personal komputer, contohnya probing & port. [15]
4. *Illegal Contents*

   Konten illegal penyebaran data/warta melalui internet yang melanggar hukum sebagai akibatnya mengganggu ketertiban umum. [15]
5. *Data forgery*

   Data Foregery merupakan aktivitas pemalsuan data krusial yg tersedia pada internet. [15]
6. *Cyber Espionage, Sabotage and Etortion.*

   Cyber espionage adalah suatu aktivitas penyadapan sistem jaringan personal komputer target menggunakan memanfaatkan jaringan internet.

Sedangkan *Sabotage* dan *extortion* adalah tindak kriminal yang dilakukan menggunakan cara menciptakan kerusakan atau gangguan terhadap suatu data juga sistem jaringan personal komputer yang terhubung menggunakan internet. [15]

7. *Cyber stalking*

   Cyber Stalking merupakan suatu aktivitas buat melecehkan target menggunakan memanfaatkan personal komputer. Kejahatan ini menyerupai terror menggunakan memanfaatkan media internet. [15]

2.2.7 *National Institute of Standar and Technology* (NIST) 800-86.

National Institute of Standar and Technology (NIST) merupakan salah satu metode yang digunakan dalam tahapan digital forensik. Metode NIST menjelaskan bagaimana setiap fase atau tahapan dilakukan, memahami proses dan alur investigasi, dan dapat digunakan sebagai referensi untuk menyelesaikan setiap masalah yang ditemukan dalam investigasi.[17] Langkah pada metode NIST dapat dijabarkan sebagai berikut:

8. *Collection*

   Pada tahap ini dilakukan untuk merekam, menangkap, melabeli, mengidentifikasi suatu bukti digital dari sumber yang tepat dengan mengikuti prosedur yang ada demi menjaga intergritas suatu data bukti digital. [18]

9. *Examination*

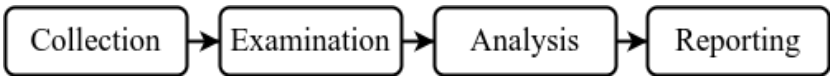
   Pada tahap pemeriksaan akan dilakukan pemrosesan dari kumpulan forensik dari dataset yang diperoleh dengan menggunakan kombinasi otomatis dan metode manual untuk mengevaluasi dan mengekstrak data yang diinginkan dengan mempertahankan integritas data.[18]

10. *Analysis*

    Pada tahap analisis, hasil pemeriksaan dengan menggunakan metode yang dibenarkan secara teknis dan hukum untuk mendapatkan informasi yang berguna dan menjawab pertanyaan- pertanyaan yang relevan untuk melakukan pengumpulan dan pemeriksaan. [19]

11. *Reporting*

    Pada tahap laporan hasil analisis, termasuk deskripsi tindakan yang digunakan, deskripsi pilihan alat dan prosedur, dan penentuan tindakan yang diperlukan.[19]



Gambar 2. 1 Alur Metode NIST 800-86.

2.2.8 Autopsy

Sleuth Kit Autopsy atau yang biasa disebut Autopsy adalah perangkat lunak open source dengan lisensi dibawah GNU General Public License Version 3 yang digunakan untuk kebutuhan digital forensik. Autopsy merupakan standar alat forensik dalam melakukan digital fotensik oleh penegak hukum.[20] Autopsy dapat mengindentifikasi, memeriksa, mengembalikan sebuah bukti data dari sebuah *hard disk* atau ponsel pintar.[21] Autopsy memberikan dukungan dari sumber data yang berformat disk images, *raw images*, *virtual machine images*, bahkan data lokal yang terdapat pada komputer atau laptop. Autopsy juga memiliki *ingest module* bawaan yang tersedia untuk menganalis dan mengeksrak data, tetapi tidak menutup kemungkinan bahwa autopsy dapat dipasangi *ingest module* pihak ke tiga.[21] Beberapa contoh alat autopsy memiliki beberapa alat yang memenuhi standar *ingest module* sebagai berikut:

1. *File Type Identification.*
2. *Recent Activity, and Hash database lookup.*
3. *Embedded File Extractor.*
4. *EXIF Parser.*
5. Surel *Parser.*
6. *Virtual Machine Extractor, and Photo Record Carver.*

2.2.9 Forensic Web Browser

Forensic Web Browser merupakan kegiatan untuk menginvestigasi dan menganalisis hasil dari penggunaan suatu peramban.[1] Fungsi *forensic web*

peramban adalah menemukan suatu bukti digital dari peramban berdasarkan apa yang diakses oleh suatu pengguna seperti riwayat,*cookie*,bookmark,file download.hasil dari forensik web peramban ini merupakan suatu bukti digital yang digunakan untuk menangkap atau melacak pelaku tindak kejahatan dunia maya.