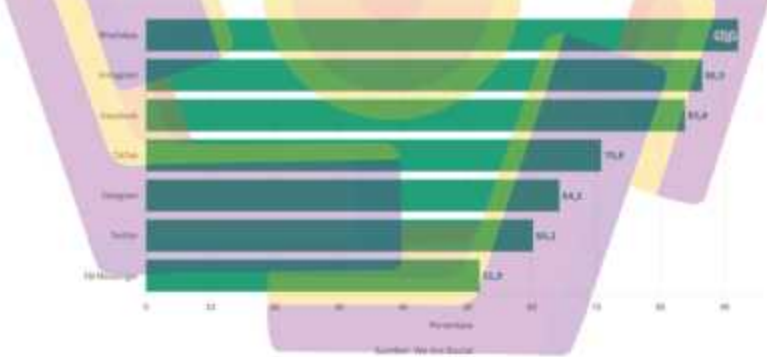
BAB I
PENDAHULUAN

1.1 Latar Belakang

Meskipun memberikan kemudahan dan kenyamanan dalam berinteraksi, penggunaan *aplikasi Whatsapp* berbasis *web* juga membawa risiko baru yang terkait dengan *online threats* yang semakin bervariasi dan kompleks. Ancaman-ancaman tersebut mencakup penipuan, peretasan, penyebaran informasi palsu, dan aktivitas kriminal lainnya yang berpotensi merugikan individu maupun masyarakat pada umumnya.

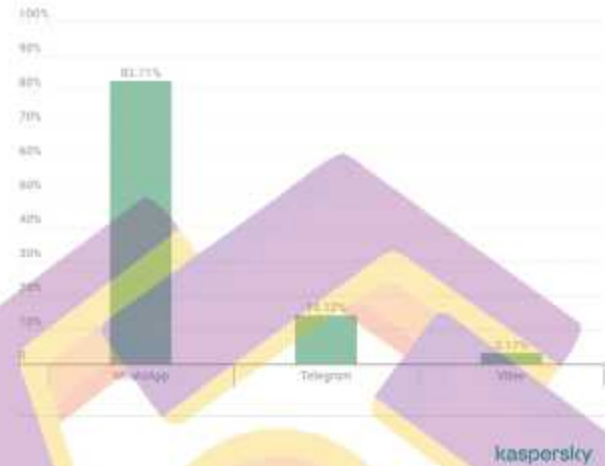
Whatsaap di Indonesia masih menjadi media sosial yang paling banyak digunakan oleh masyarakat, persentase pengguna mencapai 92,1% per Januari 2023. Seperti yang di laporkan We Are Social dalam DataIndonesia.id menunjukan bahwa penggunaan WhatsApp berada paling tertinggi seperti yang di tunjukan pada gambar 1.1.



Gambar 1.1 Media Sosial Paling Sering Digunakan di Indonesia 2023

Uraian sebelumnya menjelaskan bahwa banyak ancaman online yang semakin bervariasi dan kompleks, ancaman tersebut bisa berupa penipuan, peretasan, penyebaran informasi palsu. Telah dilaporkan pada tahun 2022 pesan ancaman dengan lampiran berupa tautan phishing dan 82.71% berasal dari WhatsApp. Data

yang dilaporkan Kaspersky. Pada gambar 1.2 berikut.



Gambar 1.2 Pesan Ancaman dengan lampiran berupa tautan (Phishing)

Kemudian sejak Tahun 2020, terdokumentasikan sejumlah insiden terkait kejahatan siber yang terkait dengan penggunaan WhatsApp. Kejahatan tersebut mencakup laporan penipuan, pencurian data, dan aduan peretasan sistem elektronik. Dalam konteks penegakan hukum oleh Dittipidsiber di bawah naungan Bareskrim Polri, jenis kejahatan siber ini terbagi menjadi dua kategori utama, yaitu computer crime dan computer-related crime.

Data statistik menunjukkan terdapat total 15.367 aduan melalui portal patroli siber sejak tahun 2020 hingga saat ini, dengan kerugian mencapai Rp 1,23 triliun.

Salah satu tantangan utama dalam menghadapi ancaman *online* yaitu kemampuan pelaku kejahatan menyembunyikan *jejak digital*. Mereka mampu menggunakan berbagai teknik *anti-forensik* untuk menghapus atau merahasiakan bukti-bukti *digital* yang mungkin menjadi alat untuk mengidentifikasi identitas, aktivitas mereka. Pada situasi ini, perhatian khusus tertuju pada *aplikasi WhatsApp Web* karena popularitasnya yang tinggi dan potensi penggunaannya dalam merencanakan serta melaksanakan tindakan kriminal.

Penelitian ini bertujuan untuk menginvestigasi kemungkinan *teknik anti-forensik* yang dapat dimanfaatkan oleh para pelaku dalam menggunakan *aplikasi WhatsApp Web* dalam konteks *online threats*. Dengan menerapkan metode *Live Forensic*, penelitian ini akan mencoba mengumpulkan data secara *real-time* dari *WhatsApp Web* yang diakses melalui beberapa *browser*, dan menggunakan pendekatan metodologi *Association of Chief Police Officers (ACPO)* untuk mengatasi *online threats*.

Harapannya, penelitian ini akan memberikan kontribusi dalam memahami teknik *anti-forensik* yang mungkin digunakan pada *aplikasi WhatsApp Web* dalam situasi *online threats*. Melalui penerapan metode *Live Forensic* dan pendekatan ACPO, penelitian ini diharapkan mampu memperkuat upaya investigasi terhadap *online threats* yang terus berkembang.

1.2 Rumusan Masalah

Mengacu pada konteks latar belakang permasalahan yang telah diuraikan, maka terbentuklah rumusan masalah dalam penelitian ini, yaitu:

1. Bagaimana pola *investigasi* barang bukti *digital forensik* yang masih tersimpan pada *random-access memory* (RAM) dalam mengidentifikasi kasus *online threats* pada pesan *Whatsapp* berbasis *Web*.
2. Bagaimana menggunakan metode *Association of Chief Police Officers* (ACPO) dalam menyelesaikan kasus.
3. Bagaimana hasil perbandingan penggunaan antar browser dalam mengungkap skenario *online threats* pada *platform Whatsapp Web*.
4. Bagaimana proses analisa perolehan artefak dalam pencarian barang bukti pada pembuktian kejahatan *online threats* pada *Whatsapp Web* dengan menggunakan bukti *digital memory* RAM.

1.3 Batasan Masalah

Dalam rangka menitikberatkan pada permasalahan ini, maka cakupan pembahasan dalam penelitian ini terbatas pada:

1. Proses akuisisi data menggunakan *teknik live forensic* yang hanya bisa

dilakukan saat komputer masih dalam keadaan hidup dalam hal ini terdapat di *Virtual Box*.

2. *Tools* yang digunakan untuk melakukan akuisisi adalah FTK *Imager*, *dd*, MD5 *Checker*, HxD *Editor*
3. Analisis kasus kejahatan digital yang dilakukan hanya berfokus pada *Whatsapp berbasis web*, yang disimulasikan dengan mengirim pesan ancaman.
4. Metode yang digunakan adalah *Association of Chief Police Officers* (ACPO)
5. Skenario simulasi penelitian dilakukan pada *windows 7* dalam hal ini dijadikan sebagai perangkat komputer yang dipakai pelaku.
6. Analisis barang bukti digital dilakukan dengan teknik *string filtering*.
7. Barang bukti yang dicari adalah transkrip pesan yang diubah dan tersimpan pada *file*.
8. Menggunakan *browser Firefox, Opera*, dan *Chrome*
9. Menggunakan skenario aktivitas *mode Incognito* dan Tanpa *mode Incognito* pada *browser*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang ada diatas, adapun tujuan penelitian ini:

1. Membantu *investigator* dalam pengangkatan barang bukti *digital forensik* dan membantu dalam mengidentifikasi kasus *online threats* pada *instant messaging Whatsapp berbasis web*.
2. Menggunakan *metode Association of Chief Police Officers* (ACPO)
3. Mencoba menemukan data dan barang bukti *digital forensik* pada *aplikasi instant messaging Whatsapp berbasis web*.

1.5 Manfaat Penelitian

Diharapkan dalam *investigasi* kasus *online threats* melalui *aplikasi WhatsApp Web* akan memberikan pandangan tentang cara mengumpulkan dan menganalisis bukti *digital* secara *real-time*. Hal ini akan membantu para penegak hukum dan ahli *forensik digital* dalam mengatasi tantangan *investigasi* dalam dunia *digital* yang terus berkembang.

1.6 Sistematika Penulisan

Sistematika penulisan pada penelitian ini disusun untuk memberikan gambaran umum mengenai penelitian yang akan dijalankan. Dapat dijelaskan sebagai berikut:

BAB I PENDAHULUAN

Di Bagian pendahuluan ini akan dijelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Menjelaskan tentang teori-teori forensik, meninjau hasil penelitian sebelumnya, teori penunjang, referensi jurnal, buku dan laporan skripsi

BAB III METODE PENELITIAN

Menjelaskan tentang metode penelitian, tahap-tahap yang dilakukan untuk analisis forensik pada objek penelitian, gambaran umum objek penelitian.

BAB IV HASIL DAN PEMBAHASAN,

Menjelaskan tentang hasil dan analisis yang dilakukan pada Whatsapp berbasis web.

BAB V PENUTUP

Mengambil kesimpulan dari hasil penelitian yang telah dilakukan dan menyampaikan saran agar penelitian selanjutnya dapat melakukan penembangan lebih lanjut tentang penelitian ini.

BAB II
TINJAUAN PUSTAKA

2.1 Studi Literatur

Banyak studi yang relevan dengan penelitian ini memiliki hubungan erat dengan temuan dari penelitian sebelumnya yang telah dilakukan sebelumnya. Temuan ini akan digunakan sebagai materi pembanding dan analisis. Penulis akan merujuk pada penelitian sebelumnya sebagai sumber referensi untuk memperluas cakupan analisis dalam penelitian yang sedang dilakukan.

Pliandi, I. A., & Indrayani, R. (2022) melakukan penelitian dengan judul *Analisa dan Perbandingan Performa Tools Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp*. Penelitian ini dilakukan untuk mengetahui perbandingan *tools forensik* yang digunakan untuk mengungkap kejahatan *cybercrime* yang melakukan *anti forensic* yang mana dilakukan dalam *aplikasi whatsapp berbasis Web* [1].

Moh. Riskiyadi (2020) melakukan penelitian dengan judul *Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime*. Penelitian ini dilakukan untuk mengungkap *cybercrime* dengan *tools digital forensic* FTK *Imager* dan *Autospy*. Dengan hasil penelitian menunjukkan FTK *Imager* dan *Atospy* mampu mengakuisisi dan menganalisa *file* yang dihapus permanen maupun file yang tersimpan sebelum *flashdisk* diformat ulang [2].

Sarjimin, Herman, & Yudhan (2021) melakukan penelitian dengan judul *Perbandingan Tool Forensik pada Mozilla Firefox Private Mode Menggunakan Metode NIST*. Penelitian ini dilakukan untuk mengungkap bahwa layanan *browsing* secara *privat* yang disediakan *Mozilla Firefox* nyatanya tidak *privat* secara menyeluruh. Artefak *digital* masih dapat ditemukan dalam RAM dan dianalisa dengan menggunakan berbagai macam *tools* untuk *forensic* berhasil mendapat data *log browser* sebesar 81% [3].

Utami, S. D., Carudin, & Ridha,A. A. (2021) melakukan penelitian dengan judul *Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus*

Penipuan Transaksi Elektronik. Penelitian ini dilakukan untuk membuktikan kasus penipuan transaksi elektronik pada *Whatsapp web* dengan menggunakan metode *Live forensic*. Dengan kondisi barang bukti berupa laptop dalam keadaan menyala (*on*) [4].

Mu'Minin, & Nuril Anwar (2020) melakukan penelitian dengan judul *Live Data Forensic Artefak Internet Browser (Studi Kasus Google Chrome, Mozilla Firefox, Opera Mode Incognito)*. Penelitian ini dilakukan untuk mendapatkan bukti *digital* berupa *Bookmarks*, *Cookies*, *E-mail*, *History*, *Image*, *Timestamp*, *Password*, URL, *Search History*. Dimana didapat melalui proses *Live forensic* pada bagian RAM [5].

M. Ainul Yaqin, Triawan Adi Cahyanto,& Nur Qadariyah Fitriyah (2021) melakukan penelitian dengan judul *Metode Live Memory Acquisition untuk Pencarian Artefak Digital Perangkat Memori Laptop Berdasarkan Simulasi Kasus Kejahatan Siber*. Penelitian ini dilakukan untuk mendapat bukti *digital* dari tiga *artefak* yang berada dengan *informasi* ID *Email*, *password email*, ID *Facebook*, *password facebook*, ID *paypal*, *password paypal*, *Link* URL [6].

Tabel 2.1 Keaslian Penelitian

No	Judul penelitian	Nama Penulis	Tahun Publikasi	Hasil Penelitian	Perbandingan Penelitian
1	*Analisa dan Perbandingan Performa Tools Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp*	Pliandi, I. A., & Indrayani, R.	2022	Penelitian ini dilakukan untuk mengetahui perbandingan tools forensik yang digunakan untuk mengungkap kejahatan cybercrime yang melakukan anti forensic yang mana dilakukan dalam aplikasi whatsapp.	Penelitian dilakukan pada Whatsapp berbasis Web yang dibuka dari beberapa browser yang berbeda
2	*Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime*,	Riskiyadi, M	2020	Hasil penelitian menunjukkan FTK Imager, Atospy dapat mengakuisisi dan menganalisa file yang dihapus permanen dan file yang tersimpan sebelum flashdisk diformat ulang	Penelitian dilakukan dengan menggunakan metode *Association of Chief Police Officers* (ACPO)

3	Perbandingan Tool Forensik pada Mozilla Firefox Private Mode Menggunakan Metode NIST	Sarjimin, Herman, & Yudhan	2021	Penelitian ini mengungkap bahwa layanan browsing secara privat yang disediakan Mozilla Firefox nyatanya tidak privat secara menyeluruh. Artefak digital masih dapat ditemukan dalam RAM dan dianalisa dengan menggunakan berbagai macam tools untuk forensic berhasil mendapat data log browser sebesar 81%.	Penelitian dilakukan dengan menggunakan browser Opera, Chrome dan Mozilla Firefox.
4	Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik	Syaza Dyah Utami, Carudin, dan Azhari Ali Ridha	2021	Hasil penelitian berupa teks percakapan, filename gambar, file video, timeslamp, history, no rekening pelaku, dan no handphone korban. merupakan bukti digital untuk kasus dari proses Live forensic dengan imaging pada RAM.	Penelitian dilakukan dengan adanya teknik anti forensic untuk menghilangkan jejak pelaku.

5	Live Data Forensic Artefak Internet Browser (Studi Kasus Google Chrome, Mozilla Firefox, Opera Mode Incognito)	Minin, M., & Anwar, N	2020	Hasil penelitian menunjukkan ketiga browser menghasilkan kesimpulan yang sama. Dapat ditemukan bukti digital berupa Bookmarks, Cookies, E-mail, History, Image, Timestamp, Password, URL, Search History.	Penelitian menggunakan skenario chat dengan menggunakan *Whatsapp berbasis* Web. Dan menghasilkan bukti digital berupa chat yang dibuat pelaku
6	Metode Live Memory Acquisition untuk Pencarian Artefak Digital Perangkat Memori Laptop Berdasarkan Simulasi Kasus Kejahatan Siber	M. Ainul Yaqin, Triawan Adi Cahyanto,& Nur Qadariyah Fitriyah	2021	Penelitian ini ditemukan hasil bukti digital dengan metode Live Memory Acquisition 100% pada media sosial Instagram, 57,14% pada media sosial facebook.	Penelitian dilakukan dengan menerapkan metode anti forensic untuk menghilangkan jejak pelaku.

2.2 Forensic Digital

Forensik digital merupakan bidang pengetahuan yang fokus pada identifikasi, pengumpulan, *analisis*, *interpretasi*, dan penyajian bukti elektronik dengan tujuan mengungkap dan memahami kejahatan serta aktivitas ilegal yang terjadi melalui perangkat elektronik dan lingkungan *digital*. Prinsip-prinsip *forensik* klasik diterapkan dalam lingkungan *digital*, bertujuan untuk menghasilkan informasi sah dan dapat diterima di pengadilan.

Tahapan dalam *forensik digital* melibatkan *proses* yang mendalam:

1. Pengumpulan Bukti Digital: Spesialis *forensik digital* mengumpulkan bukti *elektronik* terkait kasus dari perangkat keras dan perangkat lunak.
2. *Akuisisi* dan Perlindungan: *Integritas* bukti digital dijaga saat salinan diambil untuk memastikan tidak ada perubahan.
3. Analisis Mendalam: Data dianalisis secara detail untuk mengidentifikasi informasi yang relevan, termasuk pemulihan data yang dihapus.
4. Pemulihan *Data*: Teknik khusus digunakan untuk memulihkan *data* yang telah dihapus.
5. *Validasi* dan *Rekonsiliasi*: Bukti *divalidasi* dan *dianalisis* untuk memastikan keaslian dan *integritasnya*.
6. Pemahaman Konteks: Konteks dari bukti harus dipahami untuk mengerti arti dari aktivitas atau *file* dalam kasus.
7. Rekonstruksi Kronologi: Urutan peristiwa dianalisis untuk memahami bagaimana kejahatan dilakukan.
8. Pelaporan dan Kesaksian: Hasil analisis disajikan dalam laporan yang bisa dimengerti oleh *non-teknis* dan bisa digunakan sebagai bukti di pengadilan.

Gambar 2.1 Beberapa teknik digital forensic

Forensik digital digunakan dalam berbagai kasus, termasuk kejahatan siber, peredaran narkotika *online*, pencurian *data*, penipuan, dan lainnya. Keahlian dalam *forensik digital* sangat penting dalam mengungkap dan mengatasi tindakan kriminal di dunia *digital* yang semakin terhubung.

2.3 Bukti Digital

Bukti *digital* mengacu pada data atau informasi elektronik yang digunakan sebagai alat atau elemen bukti dalam *investigasi* hukum, proses peradilan, atau audit keamanan. Bukti *digital* terdiri dari berbagai bentuk data elektronik, termasuk berkas, pesan teks, surel, catatan aktivitas, jejak jaringan, dan rekaman transaksi. Pentingnya bukti digital semakin menonjol dalam era digital ini, di mana hampir semua aspek kehidupan manusia terhubung dengan teknologi. Bukti digital menjadi pijakan sentral dalam menetapkan kebenaran suatu peristiwa atau kegiatan, serta dapat membantu mengidentifikasi pelaku, mengungkap motif, dan memperkuat argumen dalam proses peradilan atau *investigasi*.

2.4 *Association of Chief Police Officers (ACPO)*

Kerangka kerja ACPO (*Association of Chief Police Officers*) merupakan pedoman yang dibuat oleh lembaga kepolisian Inggris dengan tujuan mendukung investigasi dan analisis forensik digital. Kerangka kerja ini memberikan pendekatan

metodologi yang terstruktur untuk mengumpulkan, menganalisis, dan mengelola bukti digital dalam rangka penyelidikan tindak kejahatan. Proses ini melibatkan langkah-langkah yang terperinci dalam pengumpulan bukti, analisis, dan pembuatan catatan dokumen untuk memastikan bahwa proses *forensik digital* dilaksanakan dengan *akurasi*, konsistensi, dan keandalan. Kerangka kerja ACPO juga mencakup panduan tentang cara menjalankan tindakan *forensik digital* sesuai standar tinggi serta prinsip hukum dan etika.

2.5 Live Forensics

Forensik Digital Langsung (*Live Forensic*) merupakan pendekatan dalam investigasi *digital* yang melibatkan akuisisi dan analisis bukti dari sistem yang sedang aktif atau berjalan. Berbeda dengan pendekatan *forensik* konvensional yang mengharuskan pemeriksaan perangkat yang dimatikan atau diambil dari *jaringan*, *metode live forensic* memungkinkan pengumpulan *data* dari sistem yang masih aktif dan berfungsi. Dengan demikian, ini memungkinkan peneliti atau penyelidik untuk memeriksa informasi dalam lingkungan yang mungkin lebih mendekati keadaan nyata.

Beberapa karakteristik dari metode *Live Forensic*:

1. Pengumpulan *Data Real-time*: Dalam metode ini, data diambil dari sistem yang berjalan secara *real-time*. Ini memungkinkan pengumpulan data yang mungkin tidak akan terlihat setelah sistem dimatikan.
2. Meminimalkan Gangguan: Saat melakukan *Live Forensic*, upaya akan dilakukan untuk meminimalkan gangguan atau perubahan pada *sistem* yang sedang *diinvestigasi*. Hal ini penting untuk memastikan *integritas* bukti.
3. Mengumpulkan *Data Volatile*: Metode ini dapat membantu dalam mengumpulkan data *volatile* yang tidak akan tersedia setelah *sistem* dimatikan, seperti informasi yang disimpan dalam RAM.
4. Pemantauan Aktivitas: *Investigator* dapat memantau *aktivitas sistem* secara langsung dan mengamati apa yang sedang berlangsung, seperti proses yang *aktif*, koneksi *jaringan*, dan *aktivitas* lainnya.

5. *Analisis Data* Dalam Konteks: Karena sistem masih aktif, *investigator* dapat menganalisis *data* dalam konteks yang sesungguhnya. Ini membantu dalam memahami interaksi dan dinamika *sistem*.
6. Penting untuk Keadaan Darurat: Metode *Live Forensic* seringkali digunakan dalam situasi darurat atau kasus yang memerlukan respons cepat, seperti *insiden* keamanan *cyber* yang sedang berlangsung.

2.6 Virtual Box

Virtual Box merupakan perangkat lunak *virtualisasi* yang memungkinkan pengguna untuk menciptakan dan menjalankan beberapa mesin *virtual* (VM) pada satu komputer fisik. Fungsinya adalah untuk mengizinkan pengguna memasang dan menjalankan *sistem operasi* yang berbeda secara simultan dalam lingkungan virtual yang *terisolasi*. Dengan *VirtualBox*, pengguna diberikan kesempatan untuk menguji perangkat lunak, menjalankan *aplikasi* yang sudah usang, melakukan eksperimen dengan *sistem operasi* yang baru, serta melakukan berbagai jenis pengembangan dan penelitian tanpa memerlukan perangkat keras tambahan.

2.7 Windows 7

Windows 7 merupakan sebuah *sistem operasi* yang dikembangkan oleh *Microsoft* dan dirilis pada tahun 2009. *Sistem operasi* ini menggantikan *Windows Vista* dan menawarkan peningkatan dalam hal performa, *stabilitas*, serta *fitur* baru seperti antarmuka yang lebih sederhana dan kemampuan untuk mengatur jendela dengan mudah menggunakan *Aero Snap*. *Windows 7* juga memiliki peningkatan dalam hal keamanan dan manajemen pengguna melalui fitur *User Account Control (UAC)*. Meskipun sudah ada *versi Windows* yang lebih baru, *Windows 7* tetap digunakan oleh beberapa pengguna karena kehandalan performanya dan kompatibilitasnya dengan perangkat keras yang lebih lama.

2.8 Whatsapp

WhatsApp adalah platform pesan *instan* yang memungkinkan pengguna untuk berkomunikasi melalui teks, suara, dan media lainnya. *Aplikasi* ini menawarkan *enkripsi end-to-end* untuk menjaga *privasi* pesan. Fitur lainnya termasuk panggilan suara, panggilan video, status, dan *stiker*. *WhatsApp* digunakan secara luas di seluruh

dunia dan telah menjadi salah satu *aplikasi* komunikasi paling populer. Meskipun awalnya dikenal untuk penggunaan pribadi, *WhatsApp* juga telah digunakan dalam konteks bisnis dan profesional.

2.9 Online Threats

Ancaman *online* pada pesan merujuk pada potensi bahaya yang dapat muncul saat berkomunikasi melalui platform pesan *online*, seperti pesan teks, *email*, atau *aplikasi* pesan *instan*. Ancaman tersebut mencakup risiko seperti serangan *phishing*, penyebaran informasi palsu, peretasan akun, atau pencurian data pribadi melalui pesan yang berisi tautan atau lampiran berbahaya. Dalam konteks ini, pesan dapat dijadikan sarana untuk menyebarkan *malware*, mengambil informasi penting, atau mempengaruhi penerima pesan. Keamanan *digital* sangat penting untuk melindungi *individu* dari ancaman *online* yang terkait dengan pesan.

2.10 FTK Imager

FTK *Imager* merupakan perangkat lunak *forensik digital* yang berperan dalam mengambil dan menyalin data dari berbagai media penyimpanan elektronik, seperti hard disk, perangkat *USB*, dan media lainnya. Perangkat lunak ini dikembangkan oleh *AccessData*, sebuah perusahaan yang fokus pada solusi *forensik digital*. Dalam konteks penyelidikan dan analisis *forensik*, FTK *Imager* memiliki peran krusial karena memungkinkan pengguna untuk membuat salinan *forensik* dari data asli tanpa merusak atau mengubahnya.

Dengan menggunakan FTK *Imager*, seorang penyelidik mampu menciptakan salinan data dalam bentuk *bit-by-bit* dari media penyimpanan dan menghasilkan *file* gambar yang mencakup seluruh informasi dari media tersebut. Keberadaan salinan ini memungkinkan penyelidik untuk melakukan analisis lebih mendalam tanpa mempengaruhi integritas data asli. FTK *Imager* juga mendukung berbagai format *file* gambar forensik, termasuk *EnCase E01*, *Raw*, dan *AFF*, sehingga dapat bekerja secara bersinergi dengan perangkat lunak forensik lainnya.

2.11 MD5 Checker

MD5 *Checker* adalah alat yang digunakan untuk menghitung dan *memverifikasi* nilai hash MD5 dari sebuah *file*. MD5 (*Message Digest Algorithm 5*) adalah fungsi hash *kriptografi* yang banyak digunakan untuk menghasilkan nilai *hash* dengan ukuran tetap dari data *input*. *Hash* MD5 sering digunakan untuk memverifikasi *integritas file* dengan membandingkan nilai *hash* yang dihitung dengan nilai *hash* asli yang diberikan oleh sumber *file*.

Alat MD5 *Checker* mengambil *file* sebagai *input* dan menghasilkan nilai *hash* MD5-nya, yang merupakan rangkaian karakter unik. Nilai *hash* ini berfungsi sebagai sidik jari *digital* dari konten *file* tersebut. Jika konten *file* berubah sedikit pun, bahkan modifikasi kecil, nilai *hash* MD5 juga akan berubah.

2.12 DD

DD (*Disk Dump*) adalah sebuah perangkat lunak yang beroperasi melalui baris perintah dan digunakan untuk menghasilkan salinan *data bit-by-bit* atau menciptakan salinan data dari satu lokasi ke lokasi lain dalam ukuran *blok*. Umumnya, ini dimanfaatkan untuk melindungi atau menggandakan data dari perangkat penyimpanan fisik, seperti hard disk atau perangkat USB, dengan membuat salinan data dalam bentuk file gambar yang dapat diinspeksi lebih lanjut. Selain itu, DD juga memiliki kemampuan untuk mengubah format data dan melaksanakan berbagai tugas lain terkait manipulasi data pada tingkat yang lebih rendah.

2.13 HxD Editor

HxD *Editor* berfungsi untuk melakukan *analisis* serta pemeriksaan *data* yang berada dalam format *heksadesimal* pada berbagai jenis *file*, termasuk *file sistem*, gambar *disk*, dan berkas lainnya yang terlibat dalam *investigasi forensik digital*. Melalui pemanfaatan HxD *Editor*, *investigator* dapat secara rinci mengamati isi dari berkas yang tengah dianalisis, mencari pola atau elemen mencurigakan, serta mengidentifikasi potensi bukti atau informasi yang relevan dalam situasi tersebut. Keahlian HxD Editor dalam menganalisis dan mengubah *data* dalam format *heksadesimal* menjadi sebuah instrumen yang amat berharga dalam menghimpun bukti *digital* dan menjalankan analisis *forensik*.

2.14 Browser

Sebuah peramban *web*, yang juga dikenal sebagai *browser*, merupakan sebuah program komputer yang digunakan untuk membuka dan menjelajahi halaman-halaman *web* di internet. Fungsi inti dari peramban *web* adalah menampilkan berbagai jenis konten *web* seperti teks, gambar, video, dan elemen *multimedia* lainnya kepada pengguna melalui antarmuka yang sederhana. Pengguna dapat memasukkan alamat situs *web* (URL) ke dalam peramban atau menggunakan mesin pencari untuk mencari informasi *online*. Selain itu, peramban memungkinkan pengguna berinteraksi dengan situs *web* melalui tautan, formulir, dan berbagai *fitur* lainnya seperti *email* dan pesan *instan*. Contoh-contoh peramban *web* yang populer meliputi *Google Chrome, Mozilla Firefox, Microsoft Edge, Safari*, dan *Opera*. Fungsi utama peramban adalah memberikan akses ke dunia internet dan fasilitas penjelajahan di dalamnya.

Gambar 2.2 Browser populer

2.15 Opera

Opera adalah peramban web yang menawarkan berbagai *fitur inovatif*. *Opera* memiliki *mode Turbo* yang memampatkan data saat penjelajahan *web*, sehingga cocok untuk koneksi *internet* lambat. Fitur lainnya termasuk VPN bawaan untuk keamanan lebih saat berselancar.

2.16 Mozilla Firefox

Firefox adalah peramban yang fokus pada keamanan dan *privasi* pengguna. Dia terkenal dengan dukungan kuat terhadap *ekstensi* atau *add-ons* yang memungkinkan pengguna menyesuaikan perambannya sesuai dengan kebutuhan. *Mozilla* menekankan penggunaan teknologi terbuka dan kebebasan dalam penggunaan perangkat lunak.

2.17 Chrome

Chrome adalah peramban *web* yang dikembangkan oleh *Google*. Ia terkenal karena kecepatan dan kinerjanya yang baik. Chrome memiliki dukungan yang kuat untuk *aplikasi web modern* dan fitur *sinkronisasi* dengan akun *Google*, memungkinkan pengguna untuk mengakses data dan pengaturan di berbagai perangkat.

2.18 Mode Incognito

Mode incognito adalah fitur yang ada di banyak peramban web seperti *Chrome, Firefox*, dll. Yang memungkinkan pengguna menjelajah *internet* tanpa meninggalkan jejak seperti sejarah penjelajahan atau *cookie*. Data yang diakses saat dalam mode ini tidak akan disimpan setelah sesi ditutup.

Gambar 2.3 Mode Incognito pada browser

2.19 Anti Forensic

Menurut Rogers (2006), yang ditulis Dalam jurnal Gary yang berjudul Anti forensics ad The Digital Investigator, anti forensik adalah sebuah tindakan negatif

yang dilakukan untuk mempengaruhi keberadaan, jumlah, dan kualitas barang bukti yang ada di lokasi kejadian atau membuat pemeriksaan terhadap barang bukti tersebut menjadi sulit diungkap bahkan hingga tidak mungkin untuk dilakukan. Sedangkan menurut Liu dan Brown (2006), bahwa anti forensik adalah pengaplikasian dari sebuah metode terhadap media digital untuk membuat informasi menjadi tidak valid di hadapan persidangan.

Gery C. Kessler menjelaskan bahwa anti forensik dapat dilihat dari 2 sudut pandang yaitu pelaku kejahatan bisa saja anti forensik karena sebuah tindakan untuk mempersulit dan diperolehnya sebuah bukti digital, tetapi sudut pandang yang lain bisa dinilai sebagai tindakan untuk memproteksi keamanan dari privasi mereka.