# BAB II TINJAUAN PUSTAKA

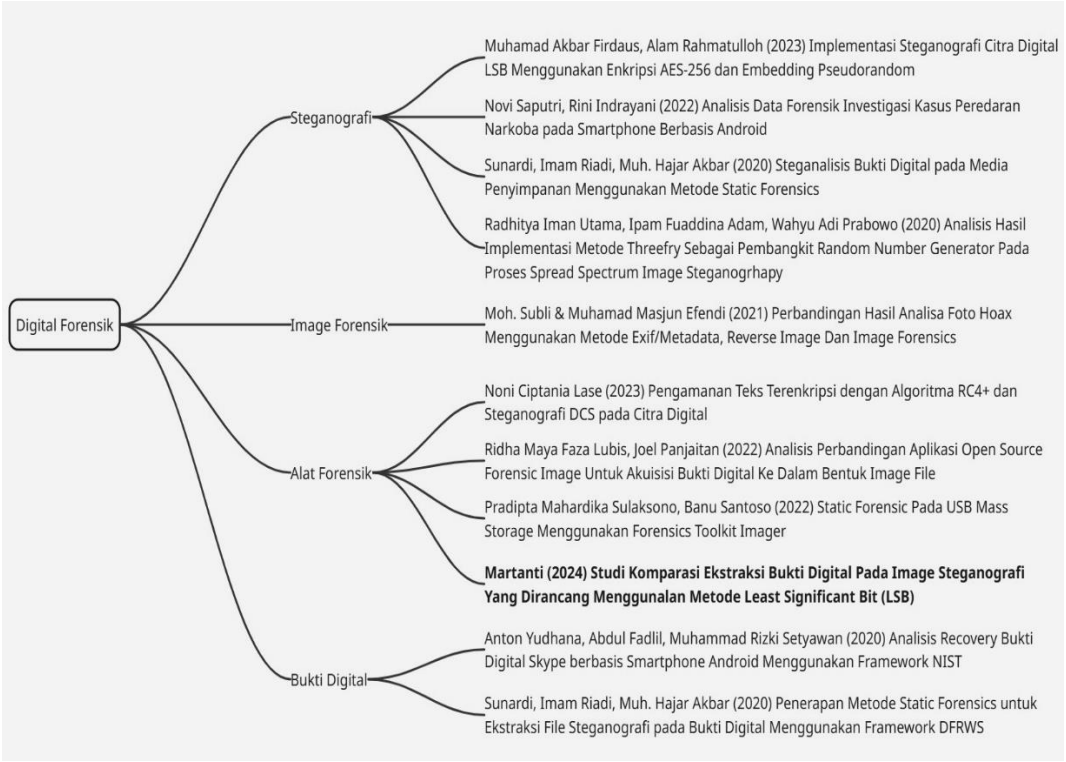
## A. Penelitian Terkait

Tabel 1 tabel penelitian terkait

| No | Nama (Tahun) | Judul |
|---|---|---|
| (1) | (2) | (3) |
| 1 | Anton Yudhana, Abdul Fadlil, Muhammad Rizki Setyawan (2020) [8] | Analisis Recovery Bukti Digital Skype berbasis Smartphone Android Menggunakan Framework NIST |
| 2 | Sunardi, Imam Riadi, Muh. Hajar Akbar (2020)[9] | Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS |
| 3 | Sunardi, Imam Riadi, Muh. Hajar Akbar (2020) [10] | Steganalisis Bukti Digital pada Media Penyimpanan Menggunakan Metode Static Forensics |
| 4 | Novi Saputri, Rini Indrayani (2022) [11] | Analisis Data Forensik Investigasi Kasus Peredaran Narkoba pada Smartphone Berbasis Android |
| 5 | Moh. Subli & Muhamad Masjun Efendi (2021) [4] | Perbandingan Hasil Analisa Foto Hoax Menggunakan Metode Exif/Metadata, Reverse Image Dan Image Forensics |
| 6 | Ridha Maya Faza Lubis, Joel Panjaitan (2022) [12] | Analisis Perbandingan Aplikasi Open Source Forensic Image Untuk Akuisisi Bukti Digital Ke Dalam Bentuk Image File |
| 7 | Pradipta Mahardika Sulaksono, Banu Santoso (2022) [13] | Static Forensic Pada USB Mass Storage Menggunakan Forensics Toolkit Imager |
| 8 | Radhitya Iman Utama, Ipam Fuaddina Adam, Wahyu Adi Prabowo (2020) [14] | Analisis Hasil Implementasi Metode Threefry Sebagai Pembangkit Random Number Generator Pada Proses Spread Spectrum Image Steganogrhapy |

| | | |
|---|---|---|
| 9 | Noni Ciptania Lase (2023)[15] | Pengamanan Teks Terenkripsi dengan Algoritma RC4+ dan Steganografi DCS pada Citra Digital |
| 10 | Muhamad Akbar Firdaus, Alam Rahmatulloh (2023) [16] | Implementasi Steganografi Citra Digital LSB Menggunakan Enkripsi AES-256 dan Embedding Pseudorandom |

Berdasarkan tabel diatas, berikut Mind Map Penelitian terkait :




Gambar 1. Mind Map penelitian terkait

## B. Landasan Teori

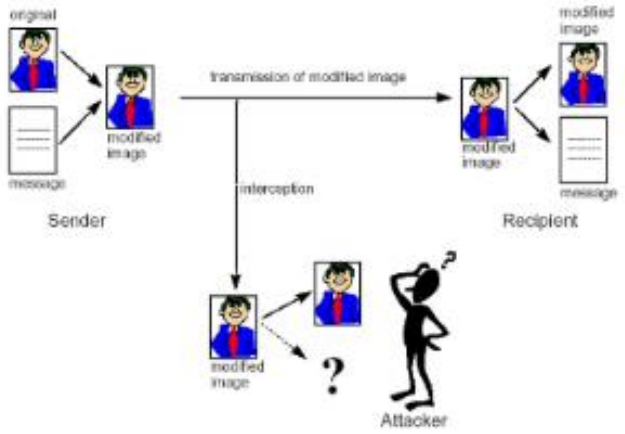
1. Steganografi

Steganografi berasal dari kata Yunani "steganos" (menyembunyikan) dan "graphien" (tulisan). Menurut Ben Le (2002) dan Rinaldi Munir (2004), Steganografi adalah seni dan ilmu menyembunyikan pesan rahasia agar tidak terdeteksi oleh indera manusia. Proses ini membutuhkan dua komponen: wadah penampung dan data rahasia. Di zaman Yunani kuno, Steganografi digunakan dengan menulis pesan rahasia di kepala budak yang botak. Pesan tersembunyi saat rambut tumbuh kembali. Bangsa Romawi menggunakan tinta tidak tampak untuk menulis pesan yang hanya terbaca dengan memanaskan kertas. [16]. Steganografi digital menggunakan media seperti gambar, suara, teks, dan video untuk menyembunyikan data rahasia. Proses menyembunyikan data disebut encoding, dan pengambilan data disebut decoding. Penambahan kunci opsional dapat meningkatkan keamanan. Dalam beberapa negara dengan undang-undang penyensoran, Steganografi digunakan untuk menyembunyikan pesan dalam media digital. Secara hukum, teknik ini melindungi informasi pribadi dan sensitif, namun juga dapat digunakan untuk kejahatan[16].

Zöllner et al. menyatakan bahwa Steganografi bukan hanya seni, tetapi juga ilmu pengetahuan yang berkaitan dengan menyembunyikan komunikasi. Sistem Steganografi ini menyembunyikan isi data di dalam sampul media yang tidak dapat diduga oleh orang biasa, sehingga tidak menimbulkan kecurigaan pada orang yang melihatnya [15]. Menurut Provos dan Honeyman, tujuan Steganografi modern adalah untuk mempertahankan media yang tidak dapat dideteksi. Namun, kelemahan sistem Steganografi membuat jejak di sampul media dapat ditemukan. Meskipun isi rahasia tidak diungkapkan, perubahan sampul media dapat mengubah sifat statistik sehingga para peneliti dapat menemukan distorsi yang dihasilkan dari proses media stego yang memiliki sifat statistik. Proses untuk mencari dan menemukan penyimpangan dalam media yang distorsi disebut "steganalisis statistik"[15].

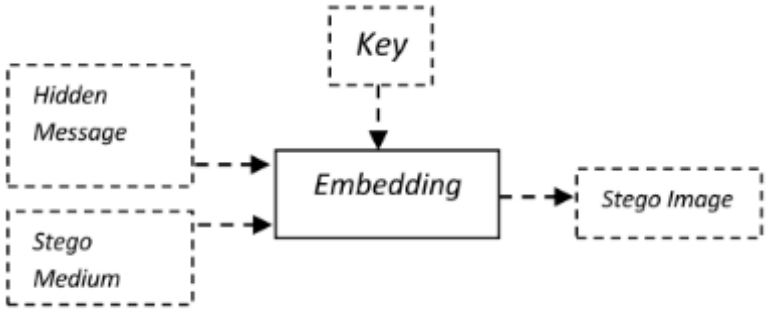
Arryawan (2010) menyatakan bahwa Steganografi adalah seni menyamarkan data. Istilah itu berasal dari kata Yunani "stagonos", yang berarti tertutup atau tercover, dan "grafi", yang berarti tulisan. Jadi Steganografi adalah seni atau ilmu untuk menyembunyikan pesan atau data rahasia di dalam data atau media yang tampaknya biasa sehingga sulit untuk mengetahuinya. Menurut Krenn (2004), Steganografi didefinisikan sebagai seni menyembunyikan informasi di dalam informasi. Sementara itu, menurut Minhajuddin (2011), Steganografi didefinisikan sebagai seni atau teknik untuk menyembunyikan informasi sedemikian rupa sehingga hanya penerima yang dapat melihatnya. Tujuan dari Steganografi adalah merahasiakan dan menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi [17].

Setelah pemboman gedung World Trade Center di Amerika Serikat, teknik Steganografi menjadi sangat populer. Dilaporkan bahwa teroris saat itu menyembunyikan aktivitas terorisnya, seperti memberikan perintah untuk melakukan aktivitas teroris pada bulletin boards dan website porno, dan mengunggah foto-foto target[18].




Gambar 2. Proses Steganografi [15]

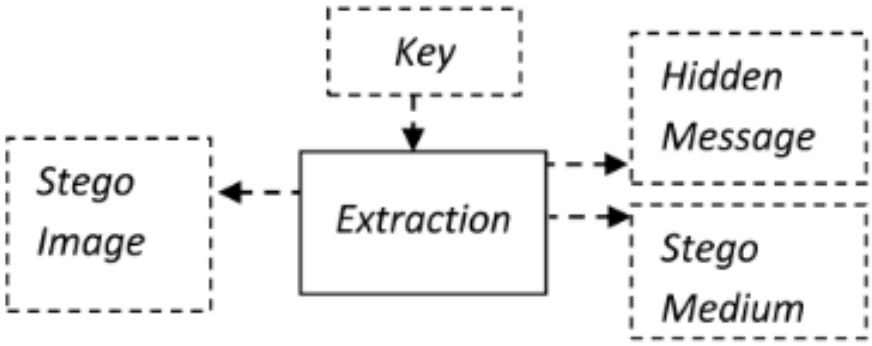
Pada gambar 2 merupakan proses Steganografi yang dilakukan oleh stegalisis (orang yang melakukan Steganografi). Biasanya terdiri dari dua proses: Embedding atau Encoding (menyembunyikan pesan rahasia) dan Extraction atau Decoding (mengambil pesan tersembunyi). Proses-proses ini sebanding dengan enkripsi dan dekripsi dalam kriptografi [15].




Gambar 3. *Embedding* [16]

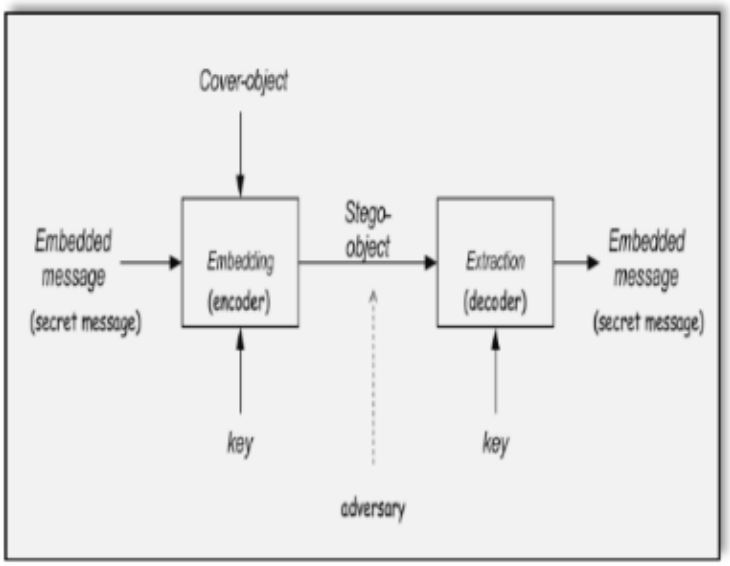
Gambar 3 merupakan salah satu proses Steganografi, yaitu embedding yang merupakan pesan ke dalam media image dengan ditambahkan kunci untuk pengamanan data. Proses diawali dari penanaman pesan rahasia ke dalam file gambar dengan ditambahkan kunci sebagai pengamannya, setelah itu file gambar hasilnya akan terbuat. Secara kasat mata file gambar sebelum

disisipkan pesan dengan file gambar yang sudah disisipkan tidak akan terlihat[16]




Gambar 4. Ekstraksi [16]

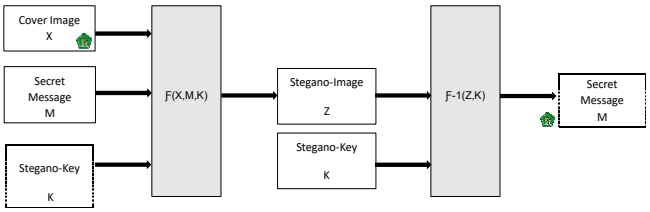
Pada gambar 4 merupakan proses ekstraksi pada image hasil Steganografi dengan memasukkan kunci yang sama sehingga didapatkan kembali pesan tersembunyi. Dapat dilihat bahwa embedding merupakan proses membungkus pesan, dan extraction adalah proses mengeluarkan pesan yang terbungkus untuk dapat dibaca[16].




Gambar 5. Cara Kerja Steganografi [11]

Cara Steganografi Berfungsi dengan menggunakan salah satu properti adalah cover, atau wadah, dan yang kedua adalah data atau pesan yang disembunyikan. Salah satu cara untuk meningkatkan keamanan data yang disimpan adalah dengan menambah properti kunci rahasia. Ini dapat menjadi

kunci simetris atau privat. Berkas Steganografi biasanya disebut berkas stego (stego file) atau stego objek[11].




Gambar 6. Model Sistem Steganografi Modern

Provos & Honeyman [5] berpendapat tujuan Steganografi modern adalah untuk mempertahankan suatu media yang tidak bisa mendeteksi, tetapi karena sistem Steganografi masih memiliki kelemahan yang meninggalkan jejak dibelakang sampul media sehingga dapat ditemukan. Sekalipun isi rahasia tidaklah diungkapkan, keberadaan tentang memodifikasi sampul media dapat merubah sifat statistik, jadi para peneliti dapat mendeteksi distorsi dihasil dari proses media stego dengan sifat stastistik. Maka proses untuk pencarian dan mendeteksi penyimpangan di dalam media yang distorsi disebut sebagai "*Statistical Steganalysis*"[15]. Menurut Munir (2006) Terdapat beberapa istilah yang berkaitan dengan Steganografi: 1. *Hiddentext* atau *Embedded message*, yaitu pesan yang disembunyikan; 2. *Covertext* atau *cover-object* atau file carrier, yaitu pesan yang digunakan untuk menyembunyikan *embedded message*; 3. *Stegotext* atau *steg-object* atau *stegofile*, yaitu pesan yang berisi *embedded message* [17]

2. Metode *Least Significant Bit* (LSB)

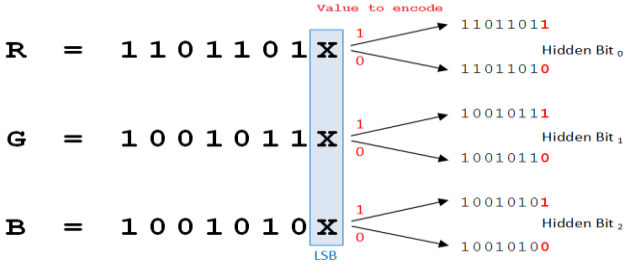
*Least Significant Bit* (LSB) adalah bit yang berada di posisi paling kanan dalam representasi biner suatu bilangan. Bit ini memiliki nilai tempat terkecil dibandingkan bit-bit lainnya, sehingga perubahan pada LSB memiliki dampak yang minimal terhadap nilai keseluruhan bilangan tersebut.

Metode LSB adalah teknik yang sangat populer dalam Steganografi, yaitu seni dan ilmu menyembunyikan informasi di dalam media lain, seperti gambar, audio, atau video. Dengan kata lain, metode ini digunakan untuk menyisipkan data rahasia (misalnya, teks, gambar, atau bahkan kode) ke dalam media tertentu tanpa mengubah secara signifikan tampilan atau kualitas media tersebut.

Untuk gambar berwarna 32-bit sama dengan LSB Pada gambar berwarna pada umumnya, pada gambar diganti dengan bit pesan. pada sistem ini gambar dimasukkan dan dilakukan penyisipan pesan kemudian dimasukkan ukuran

pixel di mana x dan y mewakili koordinat ruang dan nilai f pada koordinat (x,y) mewakili kecerahan dan informasi warna foto32-bit[19].

Metode *Least Significant Bit* (LSB) merupakan metode Steganografi yang sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai covertext. Pada susunan bit didalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (MSB) dan bit yang paling kurang berarti (LSB)[20]. Sebagai contoh byte 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angaka bit 0 (terahir, digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu atau lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti[20]. Mata manusia tidak dapat membedakan perubahan kecil tersebut Sistem sandi RC4 dikembangkan oleh Ronald Rivest pada tahun 1984 merupakan sistem sandi stream yang paling banyak digunakan misalnya pada protokol SSL/TLS, (Stalling, 2006). RC4 merupakan sistem sandi stream berorientasi byte. Masukkan algoritma enkripsi RC4 merupakan sebuah byte, kemudian dilakukan operasi XOR dengan sebuah byte kunci, dan menghasilkan sebuah byte sandi[20].




Gambar 7. *Least Significant Bit* [15]

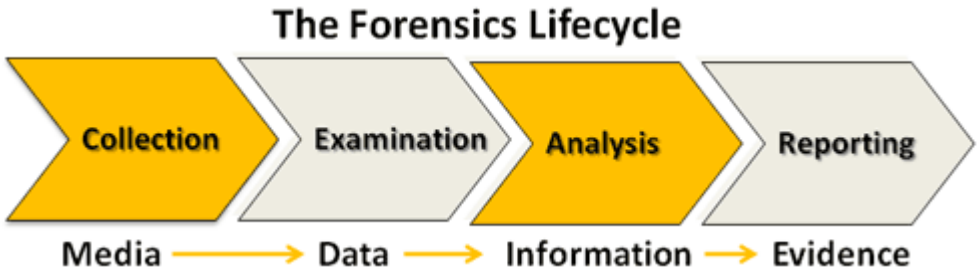
Cara kerja metode LSB yaitu mengubah bit redundan cover image yang tidak berpengaruh signifikan dengan bit dari pesan rahasia. Kelebihan dari *Least Significant Bit* (LSB) adalah Kurang mencurigakan dimata manusia, Mudah untuk diimplemtasikan, dan *High perpetual transparency*, sedangkan Kekurangan LSB adalah *robustness*, dan Sensitif terhadap *filtering*, serta *Scalling*, rotasi, penambahan *noise* pada gambar, dan *cropping* dapat merusak pesan rahasia[21].

3. *Forensic Digital*

Bidang ilmu forensik citra digital akan membantu para penegak hukum,intelijen, investigasi swata dan media. Semakin majunya teknologi image pada saat ini mengangkat isu-isu baru dan tantangan dalam menentukan keaslian image. Forensik citra digital merupakan salah satu metode ilmiah pada

bidang penelitian yang bertujuan untuk mendapatkan fakta-fakta pembuktian dalam menentukan keaslian image (Yuli Sulistyo, Riadi, & Yudhana, 2018)[4].

Forensic Digital merupakan disiplin ilmu ditujukan untuk melakukan identifikasi, mengumpulkan serta melakukan analisis bukti digital setelah serangan terjadi. Ilmu ini memiliki tujuan untuk menentukan identitas pelaku tindak kriminal, tindakan apa yang mereka lakukan, bagaimana cara mereka melakukan serta apa motivasi mereka melakukan tindak kriminal tersebut. Digital forensics juga bisa disebut sebuah metode yang berkaitan dengan kegiatan recovery serta proses penyelidikan pada sebuah bukti digital yang ditemukan. Selama sebuah sistem computer menyimpan data, dan data tersebut menyimpan informasi serta dapat dijadikan barang bukti maka disitulah digital forensic diperlukan. Selama dua dekade terakhir digital forensic mulai meningkat secara signifikan popularitas di kalangan pemerintah dan lembaga penegak hukum[13].




Gambar 8. *Lifecycle forensics*[22]

Palmer (2001) mendefinisikan digital forensik sebagai tindakan yang mencakup pengumpulan, identifikasi, pengambilan, validasi, analisis, interpretasi, dokumentasi, dan presentasi bukti digital dari sumber digital dalam upaya merekonstruksi peristiwa kriminal atau membantu antisipasi tindakan ilegal[16]. Digital forensik adalah bukti yang mendukung pembuktian fakta dan mengungkap kejadian berdasarkan bukti statistik yang meyakinkan, menurut Casey (2014)[16]. Marcella mendefinisikan forensik digital sebagai tindakan yang berkaitan dengan pengamanan, identifikasi, pengambilan/penyaringan, dan dokumentasi barang bukti digital dalam kejahatan komputer. Istilah ini agak baru dalam bidang komputer dan teknologi, tetapi telah muncul di luar bidang teknologi (dalam konteks penelitian). Digital forensik, menurut Budhisantoso, adalah kombinasi ilmu hukum dan pengetahuan komputer yang digunakan untuk mengumpulkan dan menganalisis data dari perangka penyimpanan, jaringan, sistem komputer, dan komunikasi nirkabel sehingga dapat digunakan sebagai bukti dalam penegakan hukum[11].

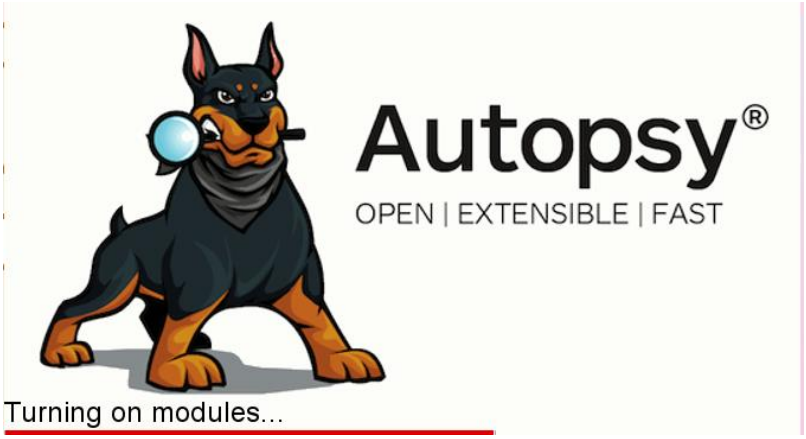
Penggunaan digital forensik adalah metode atau prosedur pengumpulan bukti digital, yang mencakup pengamanan, identifikasi, pengambilan,

dokumentasi, dan pembuatan laporan. Dalam kasus kejahatan, bukti digital ini dapat dipresentasikan di pengadilan untuk penegakan hukum. Agar digital forensik dianggap legal, mereka harus mengikuti prosedur yang berlaku. Jika tidak, operasi ini akan dianggap ilegal dan tidak sah[16].

Dengan demikian, digital forensik dapat didefinisikan sebagai metode analisis dan investigasi yang digunakan untuk mengidentifikasi, mengumpulkan, memeriksa, dan menyimpan informasi atau bukti yang disimpan secara magnetis pada komputer atau media penyimpanan digital. Ini digunakan sebagai alat bukti dalam mengungkap kasus kejahatan yang dapat dipertanggungjawabkan secara hukum[11].

4. *Autopsy*

Autopsy adalah alat yang berfungsi sebagai antarmuka grafis untuk The Sleuth Kit (TSK). The Sleuth Kit (TSK) adalah seperangkat alat yang digunakan untuk menganalisis data pada disk drive, terutama untuk tujuan forensik digital, sebuah perangkat yang dibuat khusus untuk memenuhi kebutuhan analisis forensik digital.




Gambar 9. *The Sleuth Kit* (TSK) Autopsy version 4.22

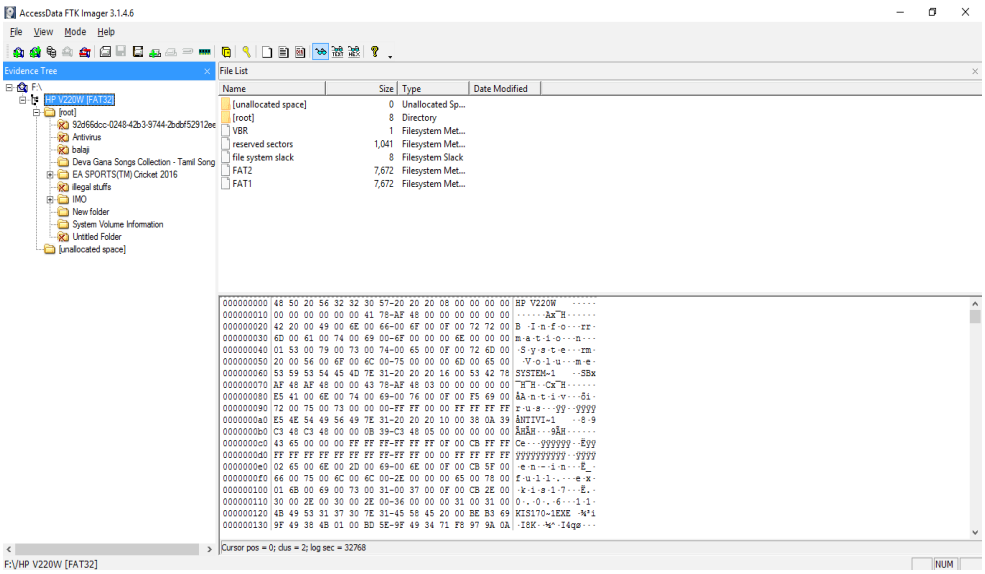
Autopsy memiliki berbagai fitur yang komprehensif untuk membantu penyelidik menemukan dan menganalisis bukti digital[18]. Palmer (2001) mendefinisikan digital forensik sebagai pekerjaan yang mencakup pengumpulan, identifikasi, pengambilan, validasi, analisis, interpretasi, dokumentasi, dan presentasi bukti digital dalam upaya merekonstruksi peristiwa kriminal atau mengantisipasi tindakan ilegal. Selain mendukung analisis sistem file yang berbeda, seperti NTFS, FAT, dan EXT, program ini memungkinkan pencarian kata kunci, penggambaran data, analisis timeline, dan pemeriksaan artefak web. Selain itu, Autopsy memiliki kemampuan untuk melakukan analisis email dan menggunakan filter set hash untuk menemukan file yang dikenal atau dicurigai[23]. Menurut Casey (2014), digital forensik adalah bukti yang mendukung pembuktian fakta.Dengan fitur-fiturnya,

Autopsy membantu penyelidik mengumpulkan dan menganalisis bukti digital dengan baik dan membuat laporan yang dapat diterima di pengadilan. Ini memastikan bahwa proses forensik dilakukan sesuai dengan hukum [23].

Autopsy merupakan tools umum bagi investigator dalam melakukan akuisisi pada storage. Dari hasil dari ekstrasi file pada Gambar 16 kemudian dilakukan proses validasi keaslian dengan pencocokkan nilai Hash menggunakan tools Autopsy dan HashMyFile. File yang tidak dapat diakuisisi dan file lain tidak menunjukkan perubahan pada nilai Hash setelah dicocokkan dengan nilai Hash dari aplikasi HashMyFile. Selain itu ekstensi file tertentu tidak dapat direcovery [23].

**5.** FTK Imager

Dampak negatif yang terjadi akibat mudahnya informasi menyebar salahsatunya yaitu informasi dapat dengan mudahnya di manipulasi, salah satunya adalah informasi berbentuk foto yang telah di rekayasa atau edit. Untuk mencegah hal tersebut dapat dilakukan analisis ke foto tersebut dengan image forensic. Dengan bantuan tools image forensic seperti FTK Imager bisa melihat metadata dari foto tersebut sehingga kita dapat dengan mudah mencari tahu sumber foto tersebut, dan dengan Forensically beta dapat dilakukan analysis dengan metode Error level analysis untuk melihat objek yang direkayasa (Rizky Al-Fajri, Caruddin & Yusup, 2021) [4].




Gambar 10. Akses Data FTK Imager

FTK Imager adalah alat forensik digital yang digunakan untuk mengidentifikasi, mengumpulkan, dan menganalisis bukti digital dari berbagai

perangkat penyimpanan. Alat ini memungkinkan penyelidik untuk membuat salinan bit-per-bit dari media digital, yang dapat digunakan untuk analisis lebih lanjut tanpa merusak data asli[24]. Menurut Palmer (2001), digital forensik melibatkan berbagai proses, termasuk pemeliharaan, identifikasi, pengambilan, validasi, analisis, interpretasi, dokumentasi, dan presentasi bukti digital. FTK Imager mendukung proses ini dengan menyediakan fitur untuk membuat image disk yang akurat, memverifikasi integritas data menggunakan hash, serta mengekstraksi file dan metadata penting dari berbagai sistem file[24]. Casey (2014) menyatakan bahwa digital forensik harus mampu mendukung pembuktian fakta dengan bukti statistik yang meyakinkan. Dengan kemampuan untuk melihat dan mengekstrak data dari berbagai format dan sistem file, serta membuat laporan yang dapat digunakan di pengadilan, FTK Imager menjadi alat yang sangat penting dalam proses forensik digital. Alat ini membantu memastikan bahwa semua bukti digital yang relevan dapat diidentifikasi, diambil, dan dianalisis secara menyeluruh, mendukung penegakan hukum dan investigasi keamanan siber dengan cara yang sah dan dapat diandalkan[24].

6. Python

   Dikutip dari dokumentasi Python sendiri[25]. Python adalah bahasa pemrograman tujuan umum yang ditafsirkan dan tingkat tinggi, diciptakan oleh Guido van Rossum dan pertama kali dirilis pada tahun 1991. Python menekankan keterbacaan kode dengan penggunaan spasi putih yang signifikan. Bahasa ini mendukung berbagai paradigma pemrograman seperti pemrograman prosedural, berorientasi objek, dan fungsional. Python dikenal dengan perpustakaan standarnya yang komprehensif dan sering digambarkan sebagai bahasa "termasuk baterai".

   Python 2.0, dirilis pada tahun 2000, memperkenalkan fitur-fitur seperti pemahaman daftar dan pengumpulan sampah dengan penghitungan referensi. Python 3.0, dirilis pada tahun 2008, adalah revisi utama yang tidak sepenuhnya kompatibel dengan versi sebelumnya. Penerjemah Python tersedia untuk banyak sistem operasi, dan CPython adalah implementasi referensi yang dikembangkan serta dipelihara oleh komunitas global.

   Python memiliki dukungan kuat untuk pemrograman fungsional, dengan fitur seperti fungsi filter, map, reduce, serta modul itertools dan functools. Filosofi inti bahasa ini diringkas dalam The Zen of Python (PEP 20), yang menekankan prinsip-prinsip seperti keterbacaan, kesederhanaan, dan keindahan kode.

   Python dirancang untuk menjadi sangat dapat dikembangkan, membuatnya populer sebagai sarana untuk menambahkan antarmuka yang dapat diprogram ke aplikasi yang ada. Nama Python sendiri adalah penghormatan kepada grup

komedi Inggris Monty Python, mencerminkan pendekatan bahasa ini yang menyenangkan dan mudah digunakan. Pengguna Python yang berpengetahuan sering disebut sebagai Pythonistas.