BAB I PENDAHULUAN

A. Latar Belakang

Steganografi adalah teknik menyembunyikan informasi di dalam media digital seperti gambar, audio, atau video, sehingga keberadaan pesan tidak terdeteksi oleh pihak lain. Berbeda dengan kriptografi yang menyamarkan isi pesan, steganografi menyamarkan eksistensi pesan itu sendiri. Teknik ini penting untuk menjaga privasi, menghindari sensor, serta melindungi data dalam komunikasi rahasia atau keperluan autentikasi digital.

Kejahatan siber merupakan aktivitas ilegal yang dilakukan oleh pelaku dengan memanfaatkan teknologi sistem informasi dan jaringan komputer, yang secara langsung menyerang sistem informasi korban. Kejahatan ini terbagi menjadi dua kategori: kejahatan terhadap sistem komputer dan kejahatan menggunakan jaringan komputer[1]. Fenomena ini merupakan sisi gelap dari kemajuan teknologi yang berdampak luas pada berbagai aspek kehidupan.

Berdasarkan data BSSN (Badan Sandi dan Siber Negara), dari Januari hingga Agustus 2020, tercatat hampir 190 juta upaya serangan siber di Indonesia, naik empat kali lipat dibanding periode yang sama tahun sebelumnya yang hanya mencatat 39 juta serangan. Menurut data POLRI, pada April 2020, terdapat 937 kasus kejahatan siber yang dilaporkan. Kasus tertinggi meliputi konten provokatif, ujaran kebencian sebanyak 473 kasus, penipuan online 259 kasus, dan konten pornografi 82 kasus.

Badan Siber dan Sandi Negara (BSSN) mencatat serangan siber tahun 2020 angka mencapai angka 495,3 juta atau meningkat 41 persen dari tahun sebelumnya 2019 yang sebesar 290,3 juta. Sama halnya dengan Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim), yang melihat adanya peningkatan laporan kejahatan siber. Dimana pada tahun 2019 terdapat 4.586 laporan polisi diajukan melalui Patrolisiber (laman web Bareskrim untuk melaporkan kejahatan siber) meningkat dari tahun sebelumnya 4.360 laporan pada 2018.

Pada 2022, tindak pidana kejahatan siber di Indonesia meningkat signifikan dibandingkan periode yang sama di 2021. Berdasarkan data e-MP Robinopsnal Bareskrim Polri, sejak 1 Januari hingga 22 Desember 2022, tercatat 8.831 kasus kejahatan siber ditindak oleh kepolisian, meningkat 14 kali lipat dibandingkan dengan 612 kasus pada periode yang sama di 2021. Polda Metro Jaya menjadi satuan kerja dengan jumlah penindakan terbanyak, yaitu 3.709 perkara. Penanganan kasus kejahatan siber ini diakui berbeda dari kasus pidana lainnya, karena kompleksitas dan sifatnya yang sering kali lintas negara[3].

Ruang lingkup kejahatan siber sangat penting untuk diperhatikan, karena perkembangan internet yang pesat sejalan dengan munculnya berbagai modus

kejahatan. Beberapa ruang lingkup kejahatan siber meliputi pembajakan, penipuan, pencurian, pornografi, pelecehan, pemfitnahan, dan pemalsuan. Kejahatan cybercrime ini seringkali meninggalkan jejak digital yang tersembunyi dalam berbagai bentuk file, salah satunya adalah image Steganografi [1].

Salah satu jenis alat yang digunakan dalam Steganografi adalah image forensic. Bidang ini membantu penegak hukum, intelijen, investigasi swasta, dan media. Kemajuan teknologi citra saat ini menimbulkan tantangan baru dalam menentukan keaslian gambar. Image forensic merupakan metode ilmiah yang bertujuan untuk memperoleh fakta pembuktian dalam menentukan keaslian gambar.

Metode yang digunakan dalam penelitian ini adalah *Least Significant Bit* (LSB) digunakan dalam Steganografi pada foto dengan mengganti bit gambar asli dengan bit informasi yang tersembunyi. Metode ini menghasilkan gambar yang tampak identik dengan aslinya bagi indera manusia. Dalam pendekatan LSB, bit paling tidak signifikan dalam data biner digunakan untuk menyisipkan pesan informasi ke dalam file gambar. Bit ini terletak di akhir urutan bit, di sebelah kanan, sehingga memungkinkan penyisipan data tanpa mengubah tampilan visual gambar secara signifikan[5].

Autopsy adalah aplikasi forensik digital open-source yang digunakan untuk menganalisis dan memulihkan bukti digital dari berbagai perangkat penyimpanan, berguna dalam investigasi forensik untuk menemukan file, metadata, dan aktivitas yang relevan[6].

Dalam penelitian ini, alat yang digunakan mencakup Sleuth Kit (+Autopsy) dan FTK Imager, yang memungkinkan pemulihan data sesuai skenario awal. Alat-alat ini berfungsi untuk akuisisi dan analisis, dapat diterapkan pada LSB di bagian akuisisi dan preservasi, serta memiliki kelebihan seperti sumber terbuka, antarmuka grafis yang ramah pengguna, dan modularitas melalui sistem plug-in. [7].

Dari latar belakang diatas, maka peneliti akan meneliti hasil perbandingan FTK Imager, sehingga peneliti akan meneliti dengan judul "STUDI KOMPARASI EKSTRAKSI BUKTI DIGITAL PADA *IMAGE* STEGANOGRAFI YANG DIRANCANG MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT* (LSB)"

B. Rumusan Masalah

1. Bagaimana cara merancang Steganografi Menggunakan metode *Least Significant Bit* (LSB) ?
2. Bagaimana perbandingan Alat forensik antara Autopsy dan FTK Imager untuk mengekstraksi bukti digital Steganografi?

C. Batasan Masalah

Batasan masalah membahas mengenai :

1. Penelitian ini hanya fokus pada Perancangan *Image* Steganografi dengan metode *Least Significant Bit* (LSB).
2. Penelitian ini menggunakan data rahasia dengan format teks berbasis metadata EXIF, format data rahasia lain tidak akan diuji.

D. Tujuan Penelitian

Tujuan Penelitian ini bertujuan untuk:

1. Merancang alat Steganografi menggunakan metode *Least Significant Bit* (LSB) untuk menyembunyikan informasi dalam gambar digital.
2. Membandingkan alat forensik Autopsy dan FTK Imager dalam mengekstraksi bukti digital dari gambar yang telah disembunyikan informasi menggunakan alat Steganografi tersebut.

E. Manfaat Penelitian

1. Manfaat Teoritis

Penelitian ini diharapkan memberikan kontribusi dalam disiplin ilmu forensik digital dengan mengembangkan pemahaman yang lebih mendalam mengenai faktor-faktor yang mempengaruhi alat forensik dalam mengekstraksi bukti digital dari gambar yang menggunakan Steganografi metode *Least Significant Bit* (LSB). Selain itu, penelitian ini juga dapat memperkaya literatur mengenai teknik-teknik forensik digital khususnya dalam konteks penggunaan alat-alat seperti Autopsy dan FTK Imager.

2. Manfaat Praktis

Secara praktis, hasil penelitian ini dapat memberikan manfaat langsung bagi profesional forensik, lembaga penegak hukum, dan industri keamanan informasi. Rekomendasi yang dihasilkan dari penelitian ini dapat membantu dalam pemilihan alat forensik yang optimal untuk investigasi digital, meningkatkan efektivitas dan efisiensi proses identifikasi dan ekstraksi bukti digital dari file Steganografi