BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi dan komunikasi pada era digital ini bisa dilihat dari meningkatnya penggunaan perangkat digital. Dari berbagai manfaat positif yang dapat digunakan atau dimanfaatkan, tetapi banyak juga dampak negatif dari pekembangan teknologi dan komunikasi. Salah satunya, banyak terjadinya kasus kejahatan, pembullyan, juga temasuk pelecehan seksual. Pelecehan seksual dapat tejadi kepada siapa saja dan dimana saja. Pelecehan seksual merupakan hal mengerikan, tetapi zaman sekarang banyak terjadi pelecehan seksual yang tidak hanya terjadi di dunia nyata tetapi juga terjadi didunia maya atau biasa disebut *cyber sexual harassment*. Teknologi yang berkembang dapat memberikan dampak positif maupun negative dalam aspek kehidupan manusia tergantung cara penerapan teknologi tersebut[1]. Melakukan tindakan pidana melalui pemanfaatan teknologi jaringan biasa disebut dengan *cybercrime*. Kejahatan dalam bidang komputer (*cybercrime*) merupakan aktivitas yang mencakup berbagai tindakan kejahatan yang masih terus meningkat hingga saat ini. Kejahatan siber memanfaatkan teknologi komputer yang dimanfaatkan sebagai alat atau media untuk melakukan tindak kejahatan seperti pencurian dan penghapusan data atau informasi, peretasan jaringan, perusakan pada aset digital dan kejahatan lainnya. Umumnya hasil dari tindak kejahatan tersebut disimpan dalam suatu media penyimpanan data. Di ranah kejahatan dunia maya, pelaku kejahatan memilih untuk menghapus bukti aktivitas ilegal mereka dengan menghapus, menyembunyikan, dan menformat semua data yang telah mereka kumpulkan[2].

Media penyimpanan merupakan salah satu bentuk dari berkembangnya teknologi, yang berguna untuk menyimpan data dan informasi. Berbagai macam jenis, bentuk, dan kapasitas dari media penyimpanan, salah satu media penyimpanan yaitu *flashdisk/flashdrive*. Data dan informasi bisa disimpan pada media *flashdisk* karena data atau berkas dapat berbentuk digital dan fisik yang

membedakan keduanya ialah format[3]. Sehingga *flashdisk* bisa menjadi salah satu media yang digunakan untuk menyimpan data kejahatan dan salah satu *device* yang mudah ditemukan dan gampang dalam pemakaiannya dengan cara menghubungkan langsung pada komputer atau laptop. Selain kegunaannya dan bentuknya yang sangat mudah untuk dibawa kemana-mana, tetapi hal ini juga bisa menjadikan *flashdisk* sebagai media untuk melakukan kejahatan. *Flashdisk* juga dapat dijadikan sebagai barang bukti tindak kejahatan[4]. Adanya berbagai motif dan cara baru yang dilakukan pelaku kejahatan dalam memanfaatkan teknologi untuk melancarkan aksi kejahatan yang dilakukan.

Salah satu jenis kejahatan dalam *cybercrime* yaitu penyalahgunaan teknik steganografi. Steganografi merupakan salah satu teknik anti forensik yang digunakan untuk menyembunyikan pesan atau informasi yang bersifat rahasia dengan cara menyisipkan pesan rahasia tersebut dalam suatu media (gambar, video, audio, file dokumen dan lainnya) agar keamanan informasi tersebut dapat terjaga [5]. Teknik steganografi merupakan cara menyembunyikan informasi atau data dalam suatu media. Dengan adanya teknik ini akan memudahkan orang-orang dalam menyembunyikan data pribadi mereka sehingga tidakan diketahui oleh orang lain atau pihak lain. Dibandikan dengan memanfaatkan teknik steganografi dengan baik dalam proses pertukaran pesan atau informasi melalui jaringan atau internet untuk melindungi informasi dari pihak yang tidak memiliki hak, tetapi banyak pelaku kejahatan yang menggunakan teknik steganografi sebagai teknik anti forensik yang bertujuan untuk menutupi tindak kejahatan[6]. Untuk mengurangi dampak buruk dari penggunaan teknik steganografi tersebut, maka dikembangkanlah teknik steganalisis. Steganalisis merupakan suatu ilmu atau teknik untuk mengungkap dan mengidentifikasi teknik steganografi. Tujuan utama dari steganalisis adalah untuk dapat mengekstraksi informasi atau data yang disisipkan, mengidentifikasi paket yang dicurigai, mengetahui apakah suatu media memiliki infomasi atau data yang disembunyikan atau tersembunyi. Berbagai teknik yang dapat digunakan dalam analisis file steganografi, salah satunya dengan melakukan analisis histogram. Analisis histogram dalam steganalisis merupakan suatu teknik untuk mengidentifikasi dan mendeteksi keberadaan data atau informasi

tersembunyi dalam media gambar berupa grafik yang dapat menunjukan frekuensi perubahan pixel dalam suatu gambar. Histogram akan menunjukan distribusi intensitas pixel pada gambar. Saat terdapat data atau infomasi yang tersembunyi pada media gambar menggunakan teknik steganografi, maka terjadi perubahan pixel pada gambar dan hal tersebut juga dapat mengubah histogram gambar[7].

Terkait dengan adanya teknik dan metode baru dalam *cybercrime*, maka penelitian ini mengangkat kasus penggunaan teknik steganografi dalam tindak kejahatan *cyber sexual harassment* karena terjadi banyaknya kejadian pelecehan seksual yang terjadi melalui dunia maya seperti *platform* digital. Kejahatan siber terkait pelecehan seksual banyak terjadi seperti penyebaran foto atau video pribadi milik seseorang sebagai bahan ejekan atau lelucon bahkan sampai memperjualbelikan data pribadi tersebut. Oleh karena itu, peneliti memilih kasus *sexual harassment* yang terjadi didunia maya bertujuan untuk meningkatkan kewapadaan terhadapat data dan informasi pribadi. Dalam penelitian ini bentuk pelecehan seksual yang dimaksud yaitu penyebaran data pribadi korban dan terjadi transtaksi elektronik terkait data tersebut. Penelitian ini akan melakukan analisis pada bukti digital berupa beberapa file foto yang tersimpan pada *flashdisk* dan file-file foto tersebut telah dimanupulasi menggunakan teknik steganografi. Metode *National Institute of Standards and Technology* (NIST) menjadi acuan dalam proses identifikasi dan analisis kasus *cyber sexual harassment*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan dapat dirumuskan: bagaimana proses analisis barang bukti digital terhadap file steganografi yang terdapat dalam *flashdisk* menggunakan metode *National Institute of Standards and Technology* (NIST) terkait kasus *cyber sexual harassment*?

1.3 Batasan Masalah

Agar penelitian ini berjalan lebih fokus dan teratur, maka diperlukan batasan masalah. Adapun beberapa batasan masalah yang akan ditetapkan adalah sebagai berikut :

a. Penelitian ini akan menganalisis file steganografi
b. Penelitian dilakukan dalam bentuk skenario kasus (bukan kasus asli).
c. Media barang bukti yang digunakan dalam penelitian ini berupa sebuah *flashdisk.*
d. *Recovery* dan ekstraksi data hanya pada data yang telah terhapus.
e. Melakukan akuisisi menggunakan tool FTK *Imager, recovery* menggunakan Autopsy dan analisis file steganografi menggunakan OpenStego Dan Steganographystudio.
f. Metode yang digunakan yaitu *National Institute of Standards and Technology* (NIST).

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah mendapatkan bukti digital berupa file rahasia yang disembunyikan menggunakan teknik steganografi sebagai bentuk investigasi kasus *cyber sexual harassment.*

1.5 Manfaat Penelitian

Manfaat yang ingin dicapai dari penelitian ini berdasarkan latar belakang, rumusan masalah, batasan masalah dan tujuan penelitian yaitu sebagai berikut:

a. Membantu menganalisis dan mengidentifikasi kasus kejahatan yang melibatkan teknik steganografi dalam kasus *cybercrime.*
b. Untuk mengetahui seberapa efektif tools yang digunakan dalam penelitian ini.
c. Bisa menjadi referensi pada penelitian berikutnya mengenai steganografi, steganalisis dan *cyber sexual harassment.*

1.6 Sistematika Penelitian

Sistematika penelitian bertujuan untuk memastikan bahwa penelitian dilakukan secara metodologis, hasilnya valid, dan laporan penelitian jelas serta dapat dipahami oleh pembaca atau pihak-pihak yang berkepentingan. Komponen sistematika penelitian sebagai berikut:

BAB I PENDAHULUAN

Bagian pendahuluan ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bagian tinjauan pustaka terdiri dari literatur review, penjelasan mengenai forensik digital, tinjauan dari penelitian sebelumnya, teknik forensik seperti steganografi dan steganalisis, referensi jurnal, buku dan laporan tesis/skripsi.

BAB III METODE PENELITIAN

Bagian metode penelitian terdiri dari alur penelitian, skenario dan simulasi kasus, tahapan yang dilakukan dalam menganalisis bukti forensik digital dan metode yang digunakan.

BAB IV HASIL DAN PEMBAHASAN

Bagian hasil dan pembahasan akan menjelaskan mengenai hasil analisis dari semua proses yang telah dijalankan, mulai dari proses akuisisi, pengujian, analisis dan terakhir pelaporan hasil.

BAB V KESIMPULAN DAN SARAN

Bagian kesimpulan dan saran merupakan proses terakhir dalam penelitian dengan memberikan kesimpulan pada penelitian yang telah dilakukan dan memberikan saran agar peneliti selanjutnya dapat melakukan penelitian lebih lanjut dari penelitian ini