BAB I
PENDAHULUAN

1.1 Latar Belakang

Dunia digital telah begitu meresap begitu dalam di kehidupan manusia sehingga kini telah menjadi salah satu pilar yang sangat penting dalam memenuhi berbagai kebutuhan. Banyak kalangan menganggap dunia digital sebagai dunia keduanya yang tidak bisa dipisahkan dari kehidupan sehari-hari. Penggunaan secara global inilah yang telah membuat dunia digital menjadi wadah utama untuk menyimpan data yang bersifat pribadi dan rahasia dikarenakan kelebihannya yang terketak pada keefisienan dan keringkasan dalam mentransfer serta menyimpan dokumen, data, dan informasi dari satu titik ke titik lainnya. Namun sebaliknya kelebihan efisien inilah yang menjadi kelemahan utama dari penggunaan dunia digital. Data yang tersebar di dunia maya dapat dengan mudah dicuri atau di salin oleh pelaku kejahatan cybercrime. Tujuan mereka seringkali bersifat merugikan dan bahkan mengancam nyawa orang disekitarnya, seperti pencurian data rahasia, penjualan informasi pribadi, pencemaran nama baik, dan berbagai tindakan kejahatan lainnya yang dilakukan untuk kepentingan pribadi pelaku cybercrime. Akibatnya, korban tidak hanya mengalami kerugian secara materi, tetapi juga bisa berujung dengan korban mengalami tekanan psikologis yang parah bahkan juga berakhir dengan hilangnya nyawa korban atau orang di sekirarnya[1].

Beberapa upaya pemerintah dalam menjaga privasi data masyarakat guna menekan kasus kerugian dalam dunia digital melibatkan serangkaian langkah, seperti himbauan peringatan mengenai batasan penggunaan media sosial, mengedukasi masyarakat mengenai pengguaan media sosial secara bijak, dan pembentukan landasan hukum yang berkaitan dengan teknologi informasi digital. Namun tantangan terus berkembang seiring dengan perkembangan teknologi memerlukan respons yang lebih proaktif.

File media seperti JPG, PNG, MP3,PDF, DOC, PPTX, MP4 dan lain lain adalah suatu format file umum yang banyak digunakan di berbagai kalangan data

dengan format file ini adalah standar yang digunakan untuk berbagai penggunaan dalam menunjang kehidupan dan pekerjaan, sehingga file-file seperti ini yang sangat berpotensi untuk dilakukan penyisipan pesan dalam melakukan tindak kejahatan yang bersifat informatif dan privat.

Sebagai langkah dalam menanggapi kasus ini, pemerintah membentuk tim forensik digital yang berperan khusus dalam mengidentifikasi dan mengumpulkan bukti digital. Dengan harapan, tim inilah yang nantinya akan memperkuat penegakan hukum terkait kejahatan digital dan menemukan bukti yang sah ke dalam rana peradilan.

Di indonesia sendiri pengaturan tentang barang bukti digital telah tertuang dalam Undang-Undang Republik Indonesia *Nomor 11 Tahun 2008* Tentang **Informasi dan Transaksi Elektronik (UU ITE) Pasal 6 yang berbunyi**, *"Dalam hal terdapat ketentuan lain selain yang diatur dalam pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau lisan Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerapkan suatu keadaan"*[2].

Dalam ranah penegakan hukum, digital forensik menjadi komponen vital, terutama dalam menghadapi tindak kejahatan digital. Terdapat tren pelaku kejahatan cybercrime yang berusaha menghilangkan jejak atau barang bukti digital dengan menghapus atau memformat media penyimpanan data. Dengan peran digital forensik, penyidik dapat mengatasi tantangan ini dengan melakukan deteksi, pengumpulan, dan analisis data digital. Proses ini memungkinkan rekonstruksi kejadian, pemulihan data yang terhapus, dan menyajikan bukti digital yang sah di ranah hukum. Pengembangan praktik digital forensik menjadi semakin penting untuk menjaga keadilan dan efektivitas penegakan hukum di era digital yang terus berkembang[3].

Penelitian ini diharapkan dapat membantu penyelidikan dalam penanganan bukti digital forensik dan membantu dalam mengidentifikasi kasus *recovery* data pada perangkat penyimpanan fisik menggunakan metode *NIST*, pada kasus

Steganografi end of file Bit berupa media file gambar *(PNG), audio (MP3), dan video (MP4)* yang telah di sisipkan pesan mencurigakan. Pelaku melakukan format data dan penyidik akan mengakuisisi data untuk melakukan penyelidikan[4].

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang ada, maka rumusan masalah dalam penelitian ini adalah bagaimana cara untuk mengetahui pesan yang terkandung pada file barang bukti yang sudah dihapus pada SD Card dengan menggunakan metode National Institute Of Standards Technology (NIST) SP 800-SP

1.3 Batasan Masalah

Sesuai dengan masalah yang terlah dirumuskan, maka batasan dalam penelitian ini yaitu:

1. Pelaksanaan proses kerangka kerja National Institute of Standards and Technology (*NIST*) yang terfokus pada bukti digital yang ditemukan dalam SD card.
2. Penggunaan alat perangkat lunak forensik digital *Autopsy* sebagai sarana untuk ekstraksi bukti digital dari SD card dalam rangka mendukung proses investigasi.
3. data yang dianalisis berfokus pada 3 jenis fle (*PNG*), audio (MP3), dan video (*MP4*).
4. Penemuan dan verifikasi integritas file bukti, yang melibatkan gambar (*PNG*), audio (MP3), dan video (*MP4*), dengan menggunakan Command Prompt (CMD) serta metode hash MD5 sebagai media untuk memastikan keabsahan dan keutuhan data yang dihasilkan.
5. Pencarian barang bukti berfokus pada variabel yang sudah di tetapkan.

1.4 Tujuan Penelitian

Sesuai dengan masalah yang telah dirumuskan, maka tujuan dari penelitian ini yaitu:

a) Untuk mengamankan bukti digital SD card yang telah direcovery menggunakan framework *NIST* pada tools *Autopsy*.

b) Memukan plaintext yang disisipkan pada file yang terkandung didalam SD card yang telah di format
c) Mengetahui integritas file barang bukti berupa gambar (*PNG*), audio (MP3), dan video (*MP4*) dari hasil ekstraksi yang telah disisipkan plaintext menggunakan *Steganografi* End Of File.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Menambah wawasan seputar dunia ilmu forensik khususnya dalam bidang Digital forensik yang dapat digunakan untuk mendapatkan bukti digital pada media penyimpanan SD Card yang berisi Plaintext disebuah file media gambar (*PNG*), Audio (MP3), dan Vidio (*MP4*).
2. Memberikan pemahaman tentang penerapan pada metode *NIST* sebagai framework dalam menangani kasus kriminal *Steganografi* end of file.
3. Menambah literasi pada penelitian tentang dunia forensik digital, khususnya pada framework NIST (National Institute Standards Technology)

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

Menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II Landasan Teori

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

BAB III Metodologi Penelitian

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

BAB IV Pembahasan dan Hasil

Menjelaskan tentang Data hasil akhir pengujian berupa gambar, table, dengan pembahasan dan analisis yang dilakukan pada tools Hex Editor Neo dan *Autopsy*.

BAB V Penutup

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