BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, perkembangan teknologi telah mengalami kemajuan yang sangat pesat. Namun perkembangan yang demikian, ternyata diikuti pula dengan berkembangnya sisi *negative* dari penggunaan teknologi yang mengarah pada Tindakan-tindakan yang dilakukan menggunakan komputer, kejahatan pada dunia maya ini dikenal dengan istilah *cyber crime* (Fitriana et al., n.d.,2020). Menurut situs Direktorat Tindak Pidana Siber Bareskrim Polri (patrolisiber.id) dari bulan Januari 2022 sampai dengan Juli 2023 terdapat 6,350 total laporan yang diterima mengenai kejahatan *cyber crime* (Direktorat Tindak Pidana Siber Bareskrim Polri, 2023). Kasus *cyber crime* yang paling banyak dilaporkan diantaranya adalah pengancaman sebanyak 2,372 kasus dan perjudian sebanyak 1,884 kasus (Direktorat Tindak Pidana Siber Bareskrim Polri, 2023).

Cyber crime merupakan suatu kejahatan yang dilakukan dengan menjadikan komputer atau jaringan komputer sebagai alat atau media dalam melakukan tindak kejahatan seperti meretas jaringan, mencuri informasi, menghapus informasi, menyembunyikan informasi, dan merusak informasi (Rana, et al, 2017). Kasus kejahatan elektronik dan barang bukti elektronik berupa komputer yang melibatkan media penyimpanan, menjadi kasus yang harus diselesaikan oleh penyelidik guna mengungkap modus dan motif kejahatan terkait dengan barang bukti yang telah didapatkan (Riadi et al., 2019). Hasil dari kejahatan umumnya akan di sembunyikan kedalam media penyimpanan agar dapat dipergunakan kembali selanjutnya, akan tetapi dalam menutupi dan menghilangkan jejaknya pelaku *cyber crime* cenderung akan menghapus dan memformat semua data yang dikumpulkan dalam melakukan tindak kejahatan (Putra, et al, 2017).

Terdapat suatu cara dalam komputer forensik untuk mengatasi file yang hilang pada media penyimpanan dengan melakukan pemulihan data, dimana pemulihan tersebut menggunakan *tools* forensik. Pemulihan data umumnya di anggap sebagai proses menyelamatkan data sebagian atau keseluruhan dari media

penyimpanan yang rusak atau tidak dapat di akses (Andi offset, 2016). Pemulihan data dalam konteks forensik digital adalah proses dimana bukti digital dipulihkan untuk di gunakan di pengadilan. Karena itu, harus dilakukan sesuai dengan standar prosedur operasi, memanfaatkan alat yang divalidasi dan terverifikasi oleh otoritas yang sesuai, dan di dokumentasikan (Cosic, 2017)

Saat ini melakukan pengujian secara menyeluruh pada sebuah komputer menggunakan applikasi/software dan tools untuk mendapatkan barang bukti digital. Bukti digital mencakup sistem komputer, media penyimpanan hard disk, CD-ROM, dokumen elektronik, gambar JPEG dan paket-paket yang bergerak melalui jaringan. Bidang forensik digital memiliki banyak cabang seperti forensik jaringan, database forensik dan forensik mobile (Panjaitan, et al, n.d.,2021). Semakin banyak data yang ingin di *recovery* diperlukannya *tools* yang memiliki fitur pemeriksaan tidak terbatas, tetapi *tools* seperti ini bersifat berbayar. Maka dari itu penelitian ini akan menyajikan beberapa *tools open source* yang bisa digunakan untuk melakukan *recovery* file data yang berbasis Windows dan Linux.

Dari beberapa referensi penelitian yang ditemukan bisa disimpulkan bahwa penelitian sebelumnya yang terkait dengan tema yang akan di bahas yaitu forensik digital, menggunakan *tools-tools* untuk melakukan pemulihan data. Penggunaan tools forensik digital akan mendukung keberhasilan dalam melakukan proses investigasi, dengan mengkombinasikan beberapa tools agar tidak berpaku pada satu tools akan memaksimalkan dalam melakukan ekstraksi dari data (Ahmadi et al., 2021). Sebagaimana disebutkan, disetiap bidang diperlukan alat yang tepat untuk menyelesaikan suatu pekerjaan atau tugas. Khususnya dalam forensik digital, perangkat lunak adalah suatu alat yang paling berharga. Perangkat lunak di perlukan untuk mengekstrak data yang di butuhkan penyelidik forensik digital (Wilson & Chi, 2017).

Penelitian mengenai masalah forensik digital sangat relevan dengan keadaan saat ini yang semakin serba digital. Sehingga penelitian ini melakukan *recovery* data melalui pendekatan *static forensic*. *Static forensic* merupakan metode forensik yang digunakan untuk memperoleh bukti digital dengan melakukan

ekstraksi serta analisis setelah insiden terjadi, ataupun setelah sistem komputer dimatikan (*post incident*) (Pradipta et al., 2022). Pada penelitian ini menggunakan beberapa sampel pengujian yang digunakan sebagai barang bukti digital terbagi menjadi 11 jenis file dengan 6 ekstensi berbeda yaitu gambar (jpg,jpeg, png), video (mp4) dan dokumen (docx, xlsx, pdf). Selain itu *scenario* analisis data *recovery* yang dibuat dalam penelitian ini mengggunakan hasil imaging dari FTK Imager melalui *flash drive*, dan nantinya akan dilakukan proses *recovery* menggunakan bebera *tools* forensik seperti, Autopsy, Disk Drill, Foremost, PhotoRec dan WinHex.

Penelitian ini membandingkan beberapa parameter pada tools forensik yang akan digunakan untuk melakukan *recovery* data, dengan menggunakan standard forensik digital SNI ISO /IEC 27037:2014. Dimana hasil recovery tersebut akan dijadikan barang bukti untuk menyelesaikan kasus kejahatan *cyber crime* (Fitriana et al., n.d.,2020). Selain itu penelitian ini juga bertujuan dalam melakukan kinerja terhadap 6 perangkat lunak tersebut berdasarkan 3 parameter penilaian yaitu kecepatan proses pemulihan, jumlah file yang berhasil dipulihkan, dan kebenaran file yang dipulihkan.

1.2 Rumusan Masalah

1. Bagaimana hasil persentase atau tingkat keberhasilan dari tools FTK Imager, Autopsy, Disk Drill, Foremost, PhotoRec, WinHex melakukan recovery data?

1.3 Batasan Masalah

1. Sistem operasi yang digunakan pada penelitian ini adalah Windows 10 Pro dan Kali Linux 2021.
2. Tools yang digunakan untuk recovery data yaitu FTK Imager v4.7.1.2, Autopsy v4.19.3, Disk Drill v5.3.825.0, Foremost v1.5.7-11, PhotoRec v7.2-WIP, WinHex v20.8 SR-1 X86.

3. Penelitian ini menggunakan metode static forensic pada sebuah flash drive
4. Penelitian ini tefokus pada analisis kinerja perangkat lunak untuk melakukan recovery data.
5. Penelitian ini melakukan recovery data yang telah terhapus dan terformat.
6. Penelitian ini melakukan proses recovery hanya menggunakan file data berupa JPG,JPEG, PNG, MP4, DOCX, XLSX PDF.
7. Menggunakan standar forensik digital SNI ISO /IEC 27037:2014
8. Untuk skenario kasus mengangkat kasus pada CoursesHero ISSC458-Forensik Digital: Menyelidiki File data dan gambar.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitian ini adalah mendapatkan hasil persentase tingkat keberhasilan pada tools forensik untuk mendapatkan bukti digital, sehingga akan didapatkan hasil tools manakah yang paling efektif dalam melakukan recovery data.

1.5 Manfaat Penelitian

1. Menambah wawasan tentang ilmu forensik digital dalam melakukan *recovery* data.
2. Memberikan pemahaman tentang bagaimana melakukan *recovery* data menggunakan *tools* FTK Imager, Autopsy, Disk Drill, Foremost, PhotoRec, WinHex.
3. Memberikan rekomendasi *tools* yang paling efektif dalam melakukan *recovery* data sesuai dengan perbandingan dan tingkat efektifitas dari *tools* FTK Imager, Autopsy, Disk Drill, Foremost, PhotoRec, WinHex.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan meliputi :

1. BAB I PENDAHULUAN, berisi : Latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.
2. BAB II TINJAUAN PUSTAKA, berisi : literature review, tinjauan pustaka, dasar-dasar teori yang digunakan terkait digital forensik.
3. BAB III METODE PENELITIAN, berisi : penjelasan tentang tahapan pada alur penelitian, gambaran umum skenario kasus.
4. BAB IV HASIL DAN PEMBAHASAN, berisi : membahas hasil kinerja beberapa tools yang di gunakan untuk melakukan recovery data dengan metode static forensic dengan standard SNI ISO /IEC 27037:2014
5. BAB V PENUTUP, berisi : kesimpulan yang di ambil berdasarkan hasil dan pembahasan yang telah di uraikan dan menjawab pertanyaan dari rumusan masalah, serta rekomendasi untuk pengembangan penelitian selanjutnya.