BAB I
PENDAHULUAN

1.1 Latar Belakang

Transformasi teknologi informasi telah mengubah budaya kerja yang lebih produktif baik individu maupun organisasi, yang semakin hari semakin modern, pesatnya perkembangan teknologi informasi ditandai dengan munculnya cloud computing, atau komputasi awan. cloud computing merupakan sebuah media penyimpanan dalam bentuk non fisik yang mana seluruh data milik pengguna akan di simpan didalam server dan pengguna dapat mengakses data mereka kapan saja dan dimana saja asalkan terhubung dengan internet, Selain dengan ukuran media yang lebih kecil, kapasitas penyimpanan yang ditawarkan oleh cloud computing ini juga jauh lebih besar dibandingkan penyimpanan secara fisik seperti Flasdisk, Hardsiks, CD dan sejenisnya.[1]

Kehadiran cloud seperti google drive pertama kali diluncurkan oleh Google pada tanggal 24 April 2012 dimana Google Drive memungkinkan pengguna menyinkronisasi data dengan perangkat lain serta dapat berbagi akses dengan layanan Google lainnya. Kepopuleran Google Drive dikarenakan layanan ini terintegrasi dengan layanan google lainnya, seperti Google Docs, Spreadsheet, dll sehingga memberikan kemudahan untuk penggunanya. Selain itu layanan ini menyediakan 15 GB kapasitas penyimpanan untuk versi free. Pada juli 2018 pengguna dari layanan ini tercatat 1 miliar pengguna aktif [2], [3].

Meski google drive pengguna terbanyak dalam layanan cloud tetapi resiko yang ditimbulkan juga besar mengingat banyaknya data dan tingkat sensitifitas data pengguna yang tersimpan di google drive ini cukup tinggi. Layanan ini juga memiliki tingkat kemanan yang kuat tetapi tidak menutup kemungkinan terjadinya kebocoran data atau informasi akibat kelalaian dari *user* yang telah menshare ke publik, tindakan seperti ini beresiko membuka celah terhadap penyalahgunaan data, pencurian data, dan kejahatan siber (*cybercrime*) yang kian semakin meningkat. Hal ini juga mendorong penelitian ini dilakukan guna

mengetahui jejak artefak yang ditinggalkan oleh pelaku kejahatan penyalahgunaan data pada google drive sehingga dapat menjadi bukti yang kuat untuk persidangan [2], [4].

Salah satu *studi case Cyber Crime* yang memanfaatkan Google Drive terjadi pada Sky Lakes Medical Center di Oregon, St. Lawrence Health System di New York, dan Dickinson County Healthcare System di Michigan dan Wisconsin, yang menjadi target serangan Ryuk Ransomware. Insiden ini menyebabkan gangguan dalam pelayanan pasien, sehingga mereka terpaksa harus melakukan proses pelayanan secara manual karena akses ke sistem mereka terhambat. Ryuk Ransomware beroperasi dengan cara melakukan phishing melalui email yang menyertakan tautan ke Google Drive; ketika tautan tersebut dibuka dan diaktifkan, maka komputer korban akan terinfeksi[5], [6].

Dengan maraknya tindak kejahatan pada lingkungan cloud computing maka perlu dilakukan tindakan digital forensik sebagai upaya mitigasi resiko tindak kejahatan. Digital forensik adalah ilmu baru yang bertujuan untuk pengumpulan dan analisis data dari bukti digital yang terdapat di berbagai sumber daya komputer untuk menemukan fakta dari kejadian, maka dari itu digital forensik sangat diperlukan untuk membantu mendeteksi adanya tindakan kejahatan yang terjadi di area cloud, mengingat cloud computing sendiri merupakan sumber daya yang digunakan sebagai sumber penyimpanan daya secara terpusat pada sebuah server[7], [8]. Sebagai contoh, Di sebuah kantor, seorang staff yang bertanggungjawab atas pengelolaan data terlibat dalam penyalahgunaan dokumen kantor dengan cara memanipulasi data, namun direktur telah menyadari adanya perubahan pada dokumen tersebut serta memiliki pengetahuan tentang kode asli dari dokumen sebelum di ubah oleh karyawan tersebut. Dengan begitu direktur yang dibantu tim forensiknya mulai melakukan investigasi terhadap dokumen tersebut. Pada KUHP pasal 372 yang mengatur tentang tindak pidana penggelapan berbunyi "Barang siapa dengan sengaja dan melawan hukum memiliki barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, tetapi yang ada dalam kekuasaannya bukan karena

kejahatan diancam karena penggelapan, dengan pidana penjara paling lama 4 tahun atau pidana denda paling banyak Rp900 ribu"[9].

Dalam pelaksanaan tindakan forensik digital mesti melalui beberapa tahap berdasarkan metode yang akan digunakan, penggunaan metode yang tepat dalam forensik akan mencatat setiap langkah dari setiap proses untuk meminimalisir tahapan yang terlewatkan sekaligus menguji apakah penerapan metode tersebut cocok dalam penelitian yang dilakukan. Dalam forensik digital terdapat banyak metode yang digunakan dengan tahapan yang berbeda satu sama lain. Salah satu metode yang digunakan dalam lingkup forensik digital ialah ACPO[10].

Association of Chief Police Officers (ACPO) ialah sebuah organisasi swasta yang telah berdiri pada tahun 1948, yang bertujuan mengembangkan praktik kepolisian di Inggris, Wales dan Irlandia Utara, yang melibatkan 44 otoritas kepolisian di ketiga negara tersebut, dalam mengungkap kejahatan dan menjadi salah satu solusi dalam investigasi forensik digital, karena framework ini menyediakan metodologi terstandar untuk akuisisi, analisis, dan preservasi bukti digital. Pada Penelitian sebelumnya dengan judul : Analisis Penggunaan Metode ACPO *(Association of Chief Police Officer)* pada Forensik WhatsApp. Dan analisis forensik digital pada skype berbasis windows 10 menggunakan framework ACPO. menunjukkan bahwa ACPO efektif dalam mengekstraksi artefak digital seperti log akses, riwayat edit, dan file yang terhapus pada platform seperti WhatsApp dan Discord [11], [12].

Penelitian ini bertujuan untuk menganalisis bagaimana framework *Association of Chief Police Officer* (ACPO) diterapkan dalam investigasi forensik digital terhadap jejak penyalahgunaan data. Dengan melakukan simulasi kasus pada skenario penyalahgunaan data di google drive, penelitian ini diharapkan memberikan wawasan tentang pola artefak digital yang dapat dijadikan bukti hukum, seperti timestamp unggah, riwayat modifikasi, metadata serta log dari aktivitas.

1.2 Rumusan Masalah

Dari latar belakang masalah yang ada, maka dapat dirumuskan rumusan masalah pada penelitian ini sebagai berikut:

Bagaimana Menganalisis Forensik Digital Berbasis Framework Acpo Terhadap Jejak Penyalahgunaan Data Pada Layanan Cloud Google Drive?

1.3 Batasan Masalah

Untuk memperkecil ruang pembahasan pada penelitian ini, maka perlu dirumuskan Batasan masalah, Adapun Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Penelitian hanya difokuskan pada layanan cloud storage Google Drive sebagai objek studi menggunakan email students amikom.
2. Framework yang digunakan dalam analisis forensik dibatasi pada ACPO Good Practice Guide for Digital Evidence.
3. Penelitian menggunakan lingkungan simulasi atau data uji, bukan data real dari insiden nyata, untuk menghindari pelanggaran hukum.
4. Penelitian ini tidak membahas serangan malware secara mendalam, tetapi hanya difokuskan pada jejak penyalahgunaan data yang ditinggalkan dari aktivitas pada google drive.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai oleh peneliti pada penelitian ini ialah untuk menganalisis bagaimana framework ACPO diterapkan dalam investigasi forensik digital terhadap jejak penyalahgunaan data pada Google Drive, sehingga bisa dijadikan sebagai barang bukti digital yang sah.

1.5 Manfaat Penelitian

Pada penelitian ini diharapkan memberikan manfaat serta kontribusi baik secara teoritis maupun secara praktis bagi pengguna layanan google drive, secara teoritis dapat dijadikan sebagai literatur untuk menerapkan framework ACPO dalam ekosistem cloud dan pemetaan kerentanan sistem Google Drive terhadap

eksploitasi data. sedangkan secara praktis dapat memberikan rekomendasi protokol forensik berbasis ACPO secara teknis dalam mengungkap jejak penyalahgunaan data, serta mendorong alat pengembangan forensik yang khusus untuk cloud.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun berdasarkan penulisan karya ilmiah. Metode ini dilakukan agar penyusunan skripsi lebih teratur dan mudah dipahami, Adapun sistematika penulisan pada skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN, Pada bab ini membahas tentang latar belakang masalah, rumusan masalah, Batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, bab ini menjelaskan tinjauan Pustaka dari penelitian terdahulu yang terkait dengan penelitian ini, serta membahas beberapa dasar-dasar teori yang relevan yang digunakan dalam penyusunan skripsi ini, seperti forensik digital, bukti digital serta tools yang digunakan dalam proses investigasi.

BAB III METODE PENELITIAN, bab ini berisikan tentang gambaran umum tentang jenis penelitian, objek penelitian, pendekatan penelitian, dan alur penelitian yang digunakan melalui skenario kasus yang telah di rancang guna menjawab permasalahan yang ada.

BAB IV HASIL DAN PEMBAHASAN, Berisi:menyajikan hasil dari penelitian secara jelas berdasarkan temuan yang dilakukan, serta memberikan rekomendasi untuk peningkatan keamanan data.

BAB V PENUTUP, Berisi: kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian dan diharapkan penelitian selanjutnya bisa mengembangkan lebih lanjut tentang penelitian ini.