1. Pendahuluan

Latar Belakang

Pada beberapa tahun terakhir komputasi awan, khususnya layanan *cloud storage* telah menjadi bagian yang penting dari industri teknologi informasi [1]. Meskipun demikian, banyak perusahaan yang tetap berhati-hati dalam memindahkan data ke lingkungan *public cloud storage* karena masalah seperti kedaulatan data dan keamanan data. Karena kekhawatiran yang terkait dengan penggunaan *public cloud storage, private cloud storage* semakin umum digunakan oleh organisasi besar sepreti universitas dan organisasi yang berurusan dengan data sensitive pengguna [2]. Layanan komputasi awan seperti layanan *cloud storage* dapat dieksploitasi oleh penjahat. Misalnya menyembunyikan jejak criminal, menyimpan materi illegal, berbagi konten *copyright*, dan menyimpan data yang memberatkan secara hukum di *cloud storage* [2] – [4]. Eksploitasi ini menunjukkan ada kebutuhan untuk melakukan penelitian mengenai *cloud storage forensic*. Beberapa penelitian telah dilakukan mengenai forensik digital pada komputasi awan. [4] mengusulkan *digital forensic framework* umum untuk komputasi awan. [3], [5] – [7] menganalisis artefak yang ditemukan pada perangkat yang menggunakan layanan *public cloud storage*. [8] melakukan investigasi menggunakan metode standar *forensik digital* pada *private cloud* storage. [9] membuat *digital forensic investigation framework* berdasarkan SNI 27073: 2014 untuk *server-side private cloud computing*. Beberapa penelitian meyediakan *digital forensic framework* untuk produk *private cloud storage* seperti owncloud [1] dan seafile [2]. Dari beberapa penelitian yang telah disebutkan sebelumnya dapat dilihat walaupun langkah dasar *forensik digital* tetap sama, keadaan selama investigasi dan konfigurasi lingkungan *cloud* yang berbeda membutuhkan metode investigasi yang berbeda. Teknologi telah berkembang dan menghadirkan tantangan tersendiri bagi individu/organisasi yang bekerja di bidang pengetahuan forensik digital. Walaupun penelitian penting untuk memajukan bidang pengetahuan forensik digital, mengembangkan alat dan pedoman untuk situasi tertentu yang membantu praktek forensik digital adalah faktor yang penting untuk pelaksana forensik digital [10]. Sebagian besar *cloud forensic framework* yang ada terlalu umum, atau kaku untuk mengakomodasi sifat *private cloud* yang dapat dikostumisasi. Selain itu, *framework* yang bersifat umum berpusat pada klien dan gagal menyediakan hubungan antara penyidikan sisi klien dan sisi server, dimana faktor tersebut penting dalam investigasi *private cloud*. Oleh karena itu *framework* yang diusulkan oleh [2] digunakan dalam TA ini.

Topik dan Batasannya

Penelitian ini berupaya untuk memberikan pemahaman mendalam tentang artefak yang tersedia bagi peneliti dan pelaksana forensik digital saat melakukan analisis pada lingkungan *private cloud storage* pada klien dan server. Salah satu produk perangkat lunak *cloud* yang menyediakan fitur-fitur yang juga disediakan oleh produk *public cloud storage* dan paket perangkat lunak *open source* adalah Nextcloud. Karakteristik ini menjadikan Nextcloud sebagai *platform* perangkat lunak yang tepat untuk studi kasus penelitian forensik *private cloud storage*.

Untuk pengumpulan data *private cloud* berlaku kerangka hukum dan prosedur khusus yang dapat berbeda dari satu negara ke negara lain. Ketika penyidik tidak memiliki izin dari *user* untuk mengakses data *private cloud*, penyidik harus beralih ke penyedia layanan. Dalam hal ini, kepemilikan data dapat dipertanyakan. Tetapi dapat ditentukan bahwa user adalah pemilik data, seperti halnya kepemilikan peralatan yang disimpan di gudang pihak ketiga. Dalam kasus seperti itu, penyidik kemudian dapat beralih ke teknologi forensik yang dapat memberikan akses ke data *private cloud* dengan memanfaatkan detail login yang telah didapatkan dari sumber yang tersedia. Dengan arsitektur internet yang kompleks, tidak mungkin untuk mengetahui apakah data berada di pusat data tertentu yang dioperasikan oleh penyedia layanan *cloud* atau apakah data di-*cache* di server penyedia layanan internet. Karena kekurangan kepastian pada hal ini, beberapa sistem hukum menggunakan kehadiran *virtual* yang berarti selama penyedia *cloud* menyediakan layanan di negara di mana aturan dapat diterapkan pada data dan penegakan hukum, akses ke data tersebut berada di bawah otoritas hukum lokal yang relevan. Untuk dapat menyerahkan data di pengadilan, data harus diambil secara forensik. Data dapat dengan mudah dihapus oleh seseorang yang memiliki akses ke akun pribadi, dan dengan demikian, dapat mengulangi proses akuisisi data *private cloud* dan mendapatkan hasil yang sama mungkin menjadi tantangan. Sistem hukum perlu mengakui bahwa ketika berurusan dengan data *cloud*, mungkin tidak ada jalan lain selain mengambil *snapshot* dari data yang ada di *cloud* pada waktu tertentu. Situasi ini mirip dengan kasus pembunuhan yang terjadi di sebuah taman di mana polisi tidak dapat menyita seluruh taman dan hanya bisa melestarikannya apa adanya. Sehingga tindakan diambil untuk mendokumentasikan taman sedekat mungkin dengan waktu kejahatan.

Tujuan

TA ini melalukan serangkaian percobaan forensik digital untuk mendapatkan artefak yang dapat ditemukan di *hard drive* klien setelah menggunakan layanan *private cloud storage*, artefak yang dapat ditemukan di *hard drive* server setelah digunakan sebagai *private cloud storage* dan menentukan artefak yang dapat digunakan untuk menghubungkan klien dan server *private cloud storage*.

Organisasi Tulisan

Bagian Studi Terkait akan memberikan teori/studi/literatur pendukung TA ini. Selanjutnya, bagian Lingkungan Percobaan Forensik Digital menjelaskan lingkungan percobaan forensik digital, *mock data* yang digunakan dan definisi artefak pada klien dan server. Setelah itu bagian Evaluasi memaparkan hasil pengujian dan analisis dari hasil pengujian. Akhirnya kesimpulan akhir dari seluruh TA ini diterangkan pada bab Kesimpulan.