# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Integritas data merupakan salah satu aspek keamanan informasi (*CIA Triad*), Integritas data harus terjaga dengan baik karena jika integritas data lemah maka akan mudah dimanipulasi oleh pihak yang tidak bertanggung jawab. Bukti digital merupakan data ataupun informasi berhubungan dengan tindakan kriminal digital yang didapatkan oleh investigator, integritas dari bukti digital harus terjaga dengan baik, karena data tersebut akan dianalisis sebagai pembuktian apakah kasus tersebut terjadi sehingga dapat digunakan sebagai bukti, namun jika integritas bukti digital lemah maka data tersebut tidak diketahui apakah masih sesuai dengan keasliannnya sehingga tidak *valid* dan tidak dapat dilakukan analisis sebagai bukti. *Algoritma* yang biasa digunakan dalam integritas data diantaranya seperti Metode *Messafe-Digest algorithm 5 (MD5)* fungsi *hash kriptografi* yang digunakan seecara luas dengan hash *value 128-bit* pada *Standart Internet (RFC 1321), MD5* kerap digunakan pada berbagai aplikasi untuk pengujian integritas sebuah file.

Layanan *Cloud computing* kerap ditawarkan oleh perusahaan *Cloud Service Provider (CSP)* bertujuan untuk mempermudah serta memberi keuntungan pada setiap pengguna yaitu *self-service provisioning, Elasticity* dan *pay per use*, *cloud computing* terbagi menjadi tiga jenis layanan yang yaitu *platform as a service (PaaS), Infrastructure as a Service (IaaS*) serta *Software as a Service (SaaS),* dari jenis layanan tersebut *cloud computing* terbagi menjadi 4 bagian salah satunya yaitu

*private cloud*, perancangan *private cloud* bertujuan untuk kepentingan suatu organisasi atau perusahaan, salah satu keuntungan dari *private cloud* adalah perusahaan dapat mengontrol secara keseluruhan baik *infrastructure* maupun *hardware* untuk melakukan pengaturan serta mengelola sesuai kebutuhan *cloud computing* setiap perusahaan (Widiyasono et al., 2016), akan tetapi terdapat kekurangan dari *cloud computing* yaitu dari sisi integritas data hal tersebut dikarenakan media penyimpanan *cloud computing* terhubung dengan internet serta menyimpan berbagai data bersifat rahasia dan tidak boleh diketahui oleh orang yang tidak memiliki hak akses, namun pada beberapa kasus terdapat oknum - oknum tidak bertanggung jawab melakukan tindakan kejahatan bertujuan mendapatkan keuntungan sendiri (Chintia et al., 2018).

Banyak metode yang dapat digunakan dalam investigasi bukti digital seperti *SNI 27037:2014* (Rochmadi, 2019), *National Institute of Standard and Technology (NIST)* (H et al., 2020) diusulkan oleh banyak penelitian terdahulu (Riadi et al., 2021) dan *Digital Forensics Investigation Framework (DFIF)* (Madiyanto et al., 2017) metode ini memiliki beberapa tahapan terdiri dari *collection, examination, analysis, report* dan *documentation* (Adam et al., 2016), *Framework* ini digunakan sebagai pedoman untuk melakukan analisa serta menelusuri bukti digital pada sebuah tindak kejahatan yang bertujuan sebagai bukti pada persidangan. Setiap tahapan dari metode investigasi bukti digital terdapat pengecekan integritas pada data yang sudah dikumpulkan investigator.

Berdasarkan latar belakang yang telah diuraikan, penelitian ini akan melakukan pengujian integritas data bukti digital hasil tangkapan data pada layanan

private cloud computing menggunakan metode *Digital Forensics Investigation Framework (DFIF),* penggunaan metode tersebut dikarenakan masih sedikit penelitian yang menggunakan metode *Digital Forensics Investigation Framework (DFIF)* serta keterbaruan dari penelitan ini adalah pengujian integritas data dari hasil investigasi *private cloud*, sehingga dapat mengetahui tahapan – tahapan yang akan dilaksanakan pada *framwework* dan pengujian integritas data tersebut dapat bekerja dengan efektif.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah pada penelitian ini adalah :

1. Bagaimana teknik investigasi digital forensik pada layanan *private cloud?*
2. Bagaimana menguji integritas data bukti digital pada layanan *private cloud?*

## 1.3 Batasan Masalah

Penelitian ini menggunakan beberapa batasan masalah shingga penelitian dapat dilaksanakan secara spsifik. Batasan masalah pada penelitian ini, sebagai berikut :

1. Pengujian dilakukan pada server *private cloud* (*ownCloud).*
2. Studi kasus pada penelitian ini dilakukan secara simulasi pada sebuah lab jaringan computer.
3. Penelitian ini dilakukan pada sistem yang sudah dibangun dari awal, seperti jaringan internet seperti *server* maupun *client*.

## 1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Mengetahui implementasi metode *Digital Forensics Investigation Framework (DFIF)* untuk pengujian integritas data bukti digital pada layanan *private cloud.*
2. Mengetahui teknik pengujian integritas data bukti digital.

## 1.5 Manfaat Penelitian

Penelitan ini diharapkan dapat bermanfaat bagi seluruh pihak yang terkait, diantaraya :

1. Secara Aplikatif

a. Diharapkan dari penelitian ini bisa bermanfaat untuk menguji integritas data bukti digital pada layanan *private cloud.*

2. Secara Akademis

a. Mengetahui cara implementasi metode *Digital Forensics Investigation Framework (DFIF)* dalam pengujian integritas data bukti digital.

b. Mengetahui teknik pengujian integritas data bukti digital.

## 1.6 Metodologi Penelitian

Metodologi penelitian berisi mengenai waktu dan tempat penelitian, tahapan penelitian, pendekatan penelitian, jenis penelitian, variabel penelitian, serta objek penelitian. Metode untuk menyelesaikan penelitian ini diantaranya:

1. Studi Literatur, merupakan pengumpulan data-data serta sumber yang berhubungan dengan penelitian serta mengolah bahan penelitian. Studi literatur

didapatkan dari jurnal dan *e-proceeding* terkait metode dan *algoritma* yang digunakan, selain itu diperoleh dari buku dan internet serta dokumen yang berkaitan dengan objek penelitian.

3. Persiapan Sistem, mempersiapkan kebutuhan yang digunakan pada penelitian seperti persiapan perangkat digunakan.
4. Simulasi Studi Kasus, sekenario kasus kejahatan digital pada *private cloud.*
5. Pelaksanaan Penelitian yaitu yaitu melakukan investigasi pada studi kasus yang telah dibuat dengan menggunakan metode *Digital Forensics Investigation Framework (DFIF)* untuk pengujian integritas data pada bukti digital yang diperoleh.
6. Dokumentasi, membuat laporan mengenai hasil yang diperoleh dari penelitian yang telah dilakukan serta menarik kesimpulan.

## 1.7 Sistematika Penulisan

Adapun aturan dan sistematika penulisan yang digunakan dalam penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab pendahuluan ini berisi latar belakang yaitu gambaran secara garis besar tentang isi laporan, rumusan masalah, batasan permasalahan pada penelitian, tujuan penelitian, manfaat penelitian yang diperoleh, metode penelitian serta sistematika penulisan laporan tugas akhir.

BAB II LANDASAN TEORI

Bab ini berisi pembahasan teori - teori yang yang saling berhubungan dengan

penelitian seperti konsep serta metode dan algoritma yang tekait dengan peneltian ini. Pada bab ini juga berisi penjelasan dari penelitian sebelumnya yang relevan dengan penelitian ini.

BAB III METODOLOGI

Bab ini berisi uraian metode yang digunakan dalam melakukan penelitian, mulai dari waktu, objek penelitian, variabel penelitian, *matriks* penelitian serta tahapan-tahapan yang dilakukan pada penelitian ini.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi pemaparan hasil serta pembahasan terhadap perancangan pada bab sebelumnya, yaitu bagaimana alur pengujian integritas data bukti digital menggunakan metode *Digital Forensics Investigation Framework (DFIF)* pada layanan private cloud.

BAB V KESIMPULAN DAN SARAN

Bab ini merupakan bab terakhir berisi kesimpulan dan saran dari hasil penelitian, serta merupakan garis besar dari metode penelitian yang telah dilakukan. Kesimpulan adalah hasil akhir dari penelitian yang dilakukan, sedangkan Saran berisi tentang rekomendasi sesuai dengan keterbatasan yang ada pada sistem