BAB 1
Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat selain membawa dampak positif juga membawa dampak negatif bersamanya. Dampak negatif tersebut antara lain adalah pemanfaatan teknologi informasi untuk melakukan tindak kejahatan atau yang lebih kita kenal dengan istilah *cybercrime*. *Cybercrime* adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan. Komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. *Cybercrime* selalu berkembang seiring dengan perkembangan teknologi informasi. Semakin pesat perkembangan teknologi, sedemikian pesat pula perkembangan *cybercrime*.

Dengan latar belakang sains dan teknologi, nyatanya pelaku *cybercrime* tidak selalu memiliki latar belakang pendidikan yang tinggi. SH misalnya, yang saat ditangkap polisi karena kejahatan *cyber* yang dilakukannya masih berusia 19 tahun hanya memiliki ijazah formal SD dan mempelajari trik-trik *hacking* secara otodidak dari situs-situs di internet. SH akhirnya ditangkap oleh kepolisian karena telah membobol situs tiket.com dan menyebabkan pengelola situs tersebut mengalami kerugian 1 Milyar Rupiah ("Fakta-fakta hacker Haikal bobol ratusan situs hingga direkrut Polri | merdeka.com," n.d.). Fakta ini semakin memperkuat kenyataan bahwa *cybercrime* dapat dengan mudah berkembang seiring dengan mudahnya akses teknologi oleh semua orang.

Namun, seperti aktivitas kejahatan lainnya, *cybercrime* pasti akan meninggalkan jejak/bukti yang dapat dijadikan bahan investigasi. Serapi dan sejeli apapun kejahatan yang dilakukan, pasti akan meninggalkan bukti walau sangat kecil. Hanya saja yang menjadi bukti dalam *cybercrime* ini kebanyakan adalah barang bukti digital *(digital evidence)*. Bukti digital didefinisikan sebagai informasi yang didapat dalam bentuk/format digital (Scientific Working Group on Digital Evidence, 1999), baik berupa bukti yang riil maupun abstrak (perlu diolah terlebih dahulu sebelum menjadi bukti yang riil).

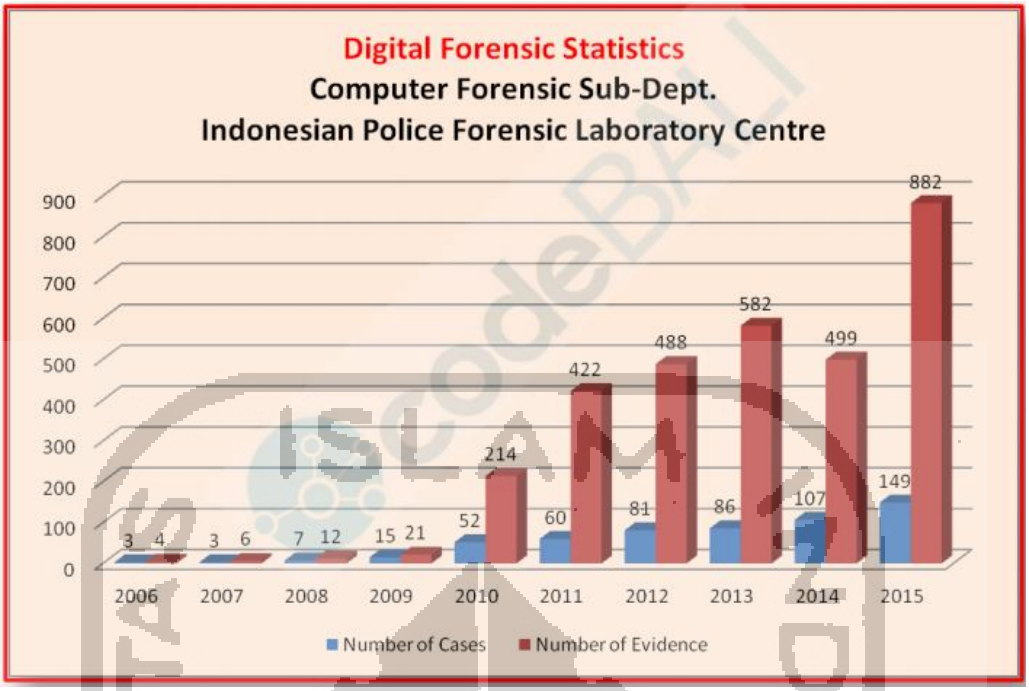
Bukti digital masih dianggap lemah karena hanya ada dalam representasi biner, dan tanpa mekanisme perlindungan yang memadai, data tersebut dapat dengan mudah dimanipulasi. Dalam prakteknya, pembuktian dalam hukum pidana merupakan sesuatu yang sangat vital perannya, mengingat dalam KUHAP (Kitab Undang-Undang Acara Pidana)

peran suatu bukti sangat berpengaruh kepada pertimbangan hakim. Berdasarkan UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) hukum Indonesia telah mengakui alat bukti elektronik atau digital sebagai alat bukti yang sah di pengadilan. Lebih lanjut, untuk dapat diakui sebagai alat bukti yang sah pasal 6 UU ITE menyebutkan :

> *"Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan."*

Untuk memenuhi kriteria tersebut, perlu adanya metode standar dalam pengambilan data dan pemrosesan barang bukti data digital. Metode standar dalam pengambilan data dan pemrosesan barang bukti data digital telah banyak dibicarakan dalam literatur-literatur tentang forensika digital. Kepolisian Republik Indonesia (POLRI) sendiri juga telah memiliki *Standart Operational Procedure* (SOP) untuk pengambilan data dan pemrosesan barang bukti digital. Salah satu prosedur dalam penanganan bukti digital yang masih belum banyak dibahas adalah mengenai penyimpanan barang bukti digital (*Preserving Digital Evidence*).

Penyimpanan barang bukti digital termasuk tahapan yang paling kritis dalam forensik digital. Dalam prosedur pengamanan barang bukti kejahatan *cyber*, pemeriksa diharuskan untuk membuat *image* forensik atau salinan *hard drive* tersangka ke perangkat penyimpanan yang aman. Ini berarti pemeriksa membutuhkan media untuk menyimpan data yang relevan pada *storage* lain yang memiliki kapasitas minimal sama besar dengan *hard drive* tersangka. Mengingat aktivitas *cybercrime* semakin meningkat, bukti yang disita dalam aktivitas tersebut juga semakin banyak, sebagaimana yang ditunjukkan dalam Gambar 1.1. Seiring dengan meningkatnya kuantitas bukti digital, kualitas bukti yang semakin baik juga memerlukan lebih banyak *space* dalam *storage* untuk penyimpanannya. Oleh karena itu *storage* yang dibangun harusnya memiliki konsep bertumbuh yang memudahkan penambahan *storage* atau dengan kata lain memiliki kemampuan dalam peningkatan skalabilitas yang baik.



Gambar 1.1 Chart jumlah kasus dan jumlah barang bukti digital yang ada di Indonesia dari tahun 2006 - 2015 (Al-Azhar, 2016) data disampaikan dalam Code Bali International Cyber Security Conference 2016

Tantangan lain dalam hal penyimpanan barang bukti adalah menjaga agar bukti digital terjaga integritas dan kredibilitasnya. Penyimpanan bukti digital pada umumnya lebih menekankan bahwa bukti digital pada saat ditemukan akan tetap tidak berubah baik bentuk, isi, makna, dan sebagainya dalam jangka waktu yang lama. Bentuk, isi, dan makna bukti digital hendaknya disimpan dalam tempat yang steril untuk benar-benar memastikan tidak ada perubahan-perubahan. Hal ini vital untuk diperhatikan, karena sedikit perubahan saja dalam bukti digital, akan mengubah juga hasil penyelidikan. Bukti digital secara alami bersifat sementara (*volatile*), sehingga keberadaannya jika tidak teliti akan sangat mudah sekali rusak, hilang, berubah, dan atau mengalami kecelakaan (Shinder & Cross, 2008).

Oleh karena itu, laboratorium forensik perlu memiliki tempat penyimpanan bukti digital (*digital evidence storage*) yang aman, memadai dan berdedikasi dengan solusi penyimpanan yang besar. Keamanan bukti digital dalam hal ini dapat diukur dengan kriteria keamanan informasi yang meliputi *confidentiality*, *integrity*, dan *availability*. Tempat penyimpanan bukti digital juga haruslah dapat bekerja secara otomatis sehingga mengurangi kewajiban pemeriksa atau penyidik dalam menjalankan tugas-tugas administrasi yang berkaitan dengan sistem. Selanjutnya penyimpanan bukti digital harus mengakomodir kebutuhan pemeriksa dan penyidik yang mungkin terpisah secara geografis untuk dapat

melakukan tugasnya dalam penyidikan *digital forensic* serta kebutuhan pemeriksa atau penyidik akan kemudahan akses terhadap *digital evidence* agar bila diperlukan *digital evidence* dapat diperiksa di tempat lain untuk menjalani penyidikan selanjutnya.

Berdasarkan pemaparan diatas, pembangunan penyimpanan bukti digital (*digital evidence storage*) haruslah memenuhi unsur berikut :

- Memiliki skalabilitas yang baik
- Memiliki perlindungan data yang baik
- Memiliki kemampuan dalam melindungi integritas data.
- Mudah diakses dari lokasi yang jauh.

Implementasi yang ideal dari permasalahan tersebut adalah repositori terpusat tempat bukti disimpan dan dipelihara, yang memungkinkan bukti diakses secara aman dari lokasi yang jauh. Hal itu dimungkinkan dengan pengembangan tempat penyimpanan barang bukti digital (*digital evidence storage*) berbasis *network*. Sedangkan dalam kaitannya mengenai skalabilitas, hal itu dapat dicapai dengan metode *clustered storage*. *Clustered storage* menjanjikan *performance*, *scalability* and *reliability* yang lebih baik dari sistem *storage* lainnya.

1.2 Permasalahan

Beberapa penelitian tentang pengembangan *digital evidence storage* yang berbasis *network* telah dilakukan oleh beberapa peneliti seperti Davis et al. (2005) yang merancang arsitektur *digital evidence custodian* (DEC) menggunakan teknologi *Network Attached Storage* (NAS) dan *Storage Area* Network (SAN), serta Ali et al. (2019) yang membuat sistem Chain of Custody Reflex yang menggunakan SAN sebagai konsep arsitektur penyimpanan terpusat berbasis jaringan dan teknologi berbasis web. Namun, penelitian tersebut belum membahas mengenai kebutuhan kemudahan dalam penambahan *storage* sedangkan sebagaimana kita ketahui bersama, kelemahan penggunaan teknologi NAS dan SAN adalah kemampuan skalabilitas yang terbatas.

Di sisi lain, saat ini telah banyak penelitian tentang *storage system* yang menggunakan *software defined storage* (SDS) alih-alih teknologi penyimpanan tradisional seperti SAN dan NAS. SDS menawarkan hal yang lebih baik dari segi aspek biaya, kelincahan (*agility*), skalabilitas, reliabilitas, dan multi-tenancy. Dalam hal skalabilitas, penyimpanan tradisional hanya dapat diskalakan hingga maksimal 4 – 8 *controller*,

sedangkan SDS dapat menskalakan hingga ratusan ribu node - yang artinya secara teoritis dapat diskalakan tanpa batas (Chinnaraju, 2018).

Oleh karena itu, penggunaan SDS untuk mengganti SAN dan NAS dalam hal pembangunan sistem *storage* barang bukti digital dapat menjadi solusi lain yang dapat mengakomodir kebutuhan akan kemudahan dalam penambahan *storage*.

Salah satu SDS yang banyak dibahas dalam penelitian mengenai kemampuan skalabilitasnya yang sangat baik adalah Ceph. Gudu (2014) telah membuktikan kemampuan skalabilitas Ceph dengan menambahkan *Object Storage Daemon* (OSD) pada sistem berjalan hingga berjumlah 20 OSD (10 node). Dari penelitian yang dilakukan tersebut, kinerja Ceph meningkat secara stabil seiring dengan penambahan jumlah OSD.

Dengan beberapa keunggulan Ceph sebagai SDS dibandingkan dengan penyimpanan tradisional seperti NAS dan SAN seperti yang diutarakan dalam penelitian-penelitian sebelumnya, penulis bermaksud untuk membangun tempat penyimpanan barang bukti digital dengan menggunakan *Software Defined Storage* Ceph sebagai alternatif dalam pembangunan barang bukti digital berbasis *network*.

1.3 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah yang akan dibahas adalah :

1. Bagaimana membangun penyimpanan bukti digital yang dapat mengakomodir penambahan *storage* tanpa mengganggu fungsi sistem yang berjalan (memiliki skalabilitas yang baik)?
2. Bagaimana membangun penyimpanan bukti digital yang dapat diakses dengan mudah oleh perangkat yang terkoneksi internet?
3. Bagaimana membangun penyimpanan bukti digital yang memenuhi kriteria keamanan informasi berupa *confidentiality*, *integrity*, dan *availability*?

1.4 Batasan Masalah

Agar permasalahan tidak terlalu luas, maka penelitian ini dibatasi pada beberapa topik permasalahan diantaranya :

1. Penelitian dilakukan dengan membangun *server virtual* untuk penyimpanan barang bukti digital.
2. *Server* virtual yang dibangun dapat dengan mudah diakses oleh perangkat yang

terkoneksi internet.

3. Untuk mengakomodasi kebutuhan akan *clustered storage*, *software defined storage* yang digunakan dalam penelitian ini adalah Ceph.
4. Untuk memudahkan manajemen layanan dan sinkronisasi file barang bukti digital antara file hasil akuisisi dan Ceph *cluster* digunakan *software* ownCloud

1.5 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut :

1. Membangun penyimpanan bukti digital yang dapat mengakomodir kemudahan penambahan *storage* tanpa mengganggu fungsi sistem yang berjalan.
2. Membangun penyimpanan bukti digital yang dapat diakses dengan mudah oleh perangkat yang terkoneksi internet.
3. Membangun penyimpanan bukti digital yang memenuhi kriteria keamanan informasi berupa *confidentiality*, *integrity*, dan *availability*.

1.6 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut :

1. Pengembangan keilmuan dalam kaitannya dengan *digital evidence preservation* (pemeliharaan bukti digital).
2. Pengembangan *storage* untuk menyimpan bukti digital.
3. Memberikan sumbangsih informasi tentang penggunaan Ceph dalam pembangunan *clustered storage*.
4. Mengembangkan penelitian-penelitian sebelumnya yang berkaitan dengan *digital evidence preservation, digital evidence storage,* dan *clustered storage*.
5. Bagi penulis, penelitian ini diharapkan dapat menambah wawasan, kualitas keilmuan baik dalam hal teori maupun praktek.

1.7 Metode Penelitian

Langkah-langkah yang ditempuh selama melakukan penelitian ini adalah sebagai berikut :

1. Studi Pustaka

   Studi pustaka dilakukan untuk mendapatkan informasi mengenai topik penelitian yang dapat bersumber dari dokumen, buku, artikel, atau bahan tertulis lainya yang berupa

teori, laporan penelitian, atau penemuan sebelumnya, baik bersifat *online* maupun *offline source* mengenai penyimpanan *digital evidence*, *storage cluster*, dan *software defined storage* serta informasi lain yang relevan dengan topik penelitian.

2. Perancangan

   Merupakan tahap perancangan *digital evidence storage* yang akan dibangun menggunakan *software defined storage*: Ceph *storage cluster*. Tahap perancangan ini meliputi proses analisa kebutuhan *hardware* dan *software* serta pembuatan topologi rancangan sistem *storage* yang akan dibangun sehingga dapat memenuhi kriteria yang telah ditentukan sebelumnya yaitu, *scalability*, *confidentiality*, *integrity*, dan *availability*.

3. Implementasi

   Pada tahap ini dilakukan implementasi perancangan yang telah dibuat sebelumnya hingga bisa digunakan untuk pengujian, yang meliputi pembuatan *Virtual Machine*, instalasi sistem operasi, instalasi dan konfigurasi Ceph *storage cluster* sebagai tempat penyimpanan barang bukti digital, serta instalasi dan konfigurasi *software* pendukung sesuai rancangan yang telah dibuat sebelumnya.

4. Pengujian Sistem

   Ada 4 skenario pengujian yang akan dijalankan dalam penelitian ini yaitu: uji skalabilitas, uji keamanan transfer data, uji sinkronisasi file dan uji saat node terputus. Skenario pengujian ini dirancang untuk menguji apakah sistem *storage* yang dibuat dapat memuhi kriteria *scalability*, *confidentiality*, *integrity*, dan *availability*.

1.8 Struktur Penulisan

Tahapan yang menjelaskan secara umum terkait sistematika penulisan yang berisi penjelasan secara ringkas terhadap kerangka penulisan yang digunakan.

BAB I PENDAHULUAN

Tahap awal dari penelitian berisi penjelasan terkait dengan latar belakang penelitian, penetapan judul, rumusan masalah, tujuan penelitian, manfaat penelitian, metode serta struktur penulisan yang digunakan. Dalam bagian ini juga dijelaskan mengenai temuan paling relevan dengan penelitian sebelumnya dan kontribusi ilmiah yang diharapkan.

BAB II KAJIAN PUSTAKA

Tahap ini menjelaskan tentang kajian atas pustaka yang relevan dengan penelitian dan rumusan masalah berupa manajemen penyimpanan bukti digital, pembangunan tempat

penyimpanan bukti digital berbasis *network*, pembangunan *clustered storage* menggunakan *software defined storage*, *software defined storage* yang memiliki skalabilitas yang sangat baik, serta peningkatan keamanan informasi terkait sistem *storage*.

BAB III METODOLOGI PENELITIAN

Menguraikan metode penelitian yang digunakan untuk memperoleh data dan informasi sesuai dengan topik penelitian.

BAB IV PEMBAHASAN

Hasil dan Pembahasan, berisi tentang pembahasan penyelesaian masalah yang diangkat yaitu dengan melakukan analisis berdasarkan pengujian sistem.

BAB V KESIMPULAN DAN SARAN

Kesimpulan dan Saran, memuat kesimpulan-kesimpulan dari hasil penelitian dan saran-saran yang perlu diperhatikan berdasar keterbatasan yang ditemukan serta asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.

DAFTAR PUSTAKA

.