

Presentasi Data Forensik

Disusun untuk memenuhi tugas Manajemen Investigasi Tindak Kriminal

(dr. Handayani DU, M.Sc. SpF.)



Fathirma'ruf

13917213

PROGRAM PASCASARJANA TEKNIK INFORMATIKA

FAKULTAS TEKNIK INDUSTRI

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2014

BAB I

PENDAHULUAN

1.1. Presentasi Data Forensik

Dalam bidang forensik, khususnya forensika digital memiliki standart dalam proses penanganan barang bukti, hal tersebut dilakukan agar dalam proses penyelidikan, data – data yang diperoleh berasal dari sumber yang dapat dipercaya, sehingga tidak terdapat manipulasi bentuk, isi, dan kualitas data digital.

Dalam persidangan pengelolaan keadilan dan peran seorang penyelidik baik penyelidik secara umum maupun penyelidik di bidang digital adalah untuk menyajikan fakta–fakta, kemungkinan-kemungkinan yang mendukung (membantu), sehingga tingkat kepercayaan pengadilan bergantung pada penyelidik dan kemampuannya dalam meyajikan hal-hal teknis terkait dengan barang bukti dan pembuktian secara jelas, factual dan obyektif.

1.2. Perumusan Masalah

Dalam proses investigasi sebagai bentuk kegiatan dalam melakukan forensik hal yang terpenting adalah mendapatkan, mengolah, dan menyajikan data berdasarkan metode ilmiah, serta bagaimana menganggap bahwa peranan data adalah salah satu hal yang terpenting dalam proses investigasi, dengan tujuan agar dapat dipertanggung jawabkan di persidangan

1.3. Tujuan Penulisan

Menjelaskan bagaimana proses atau langkah dalam mendapatkan, mengolah, dan menyajikan data, sebagai bentuk barang bukti untuk mendukung suatu fakta, teori, teknik yang dapat digunakan dalam proses persidangan

BAB II

PEMBAHASAN

2.1. Peranan data sebagai barang bukti

untuk membantu pengungkapan suatu kejahatan melalui pengungkapan bukti-bukti yang sah menurut undang-undang dan peraturan yang berlaku. Sesuai dengan kemajuan jaman, berbagai tindakan kejahatan dan kriminal moderen dewasa ini melibatkan secara langsung maupun tidak langsung teknologi informasi dan komunikasi.

2.2. Proses Penanganan data Forensik

Proses penanganan barang bukti hingga presentasi data dalam digital forensik diantaranya yaitu :

1. Preserving (Memelihara dan mengamankan data)

Merupakan serangkaian aktifitas yang dilakukan oleh penyidik untuk menjamin agar data-data yang diperoleh tidak berubah.

2. Confirming (Menetapkan data)

Merupakan serangkaian kegiatan untuk menetapkan data-data yang berhubungan dengan kasus yang telah terjadi.

3. Identifying (Mengenali data)

Merupakan serangkaian kegiatan untuk melakukan proses identifikasi terhadap data-data yang sudah ada, agar dapat dipastikan bahwa data tersebut memang unik dan asli sesuai dengan yang terdapat pada tempat kejadian perkara. Untuk data digital misalnya melakukan identifikasi dengan teknik hashing (membuat sidik jari terhadap barang bukti)

4. Analyzing (Meneliti data)

Merupakan proses untuk meneliti data-data yang telah terkumpul. Untuk data digital analisa data yang dilakukan diantaranya yaitu memeriksa data yang terhapus, tersembunyi, terenkripsi, dan history akses internet seseorang yang tidak dapat dilihat oleh masyarakat umum.

5. Recording (Mencatat data)

Melakukan pencatatan terhadap data-data hasil temuan dan hasil analisis, sehingga nantinya data tersebut dapat dipertanggung jawabkan atau dapat di rekonstruksi ulang (jika diperlukan) atas temuan barang bukti tersebut.

6. Presenting (Mempresentasikan data)

Merupakan kegiatan yang dilakukan oleh penyidik untuk memberikan atau mempresentasikan hasil temuannya kepada pihak yang berwajib atau di depan persidangan. Biasanya presentasi data dilakukan oleh seorang ahli forensik untuk menjelaskan ha-hal yang susah dipahami oleh kalangan umum, sehingga data-data tersebut dapat membantu proses penyelidikan untuk menemukan tersangka, atau mengungkap suatu kasus yang terjadi.

2.2. Contoh penanganan data dalam kasus

Contoh kejahatan yang dimaksud dan erat kaitannya dengan kegiatan forensik komputer misalnya:

- Pencurian kata kunci atau “password” untuk mendapatkan hak akses;
- Pengambilan data elektronik secara diam-diam tanpa sepengetahuan sang empunya;
- Pemblokiran hak akses ke sumber daya teknologi tertentu sehingga yang berhak tidak dapat menggunakannya;
- Pengubahan data atau informasi penting sehingga menimbulkan dampak terjadinya mis-komunikasi dan/atau dis-komunikasi;
- Penyadapan jalur komunikasi digital yang berisi percakapan antara dua atau beberapa pihak terkait;

Berikut beberapa cara dan langkah dalam penanganan beberapa kasus tersebut yang dapat diolah dan dijadikan sebagai data dan di olah menjadi barang bukti untuk di sajikan di persidangan.

1. Log file atau catatan aktivitas penggunaan komputer yang tersimpan secara rapi dan detail di dalam sistem;
2. File yang sekilas telah terhapus secara sistem, namun secara teknikal masih bisa diambil dengan cara-cara tertentu;

3. Catatan digital yang dimiliki oleh piranti pengawas trafik seperti IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System);
4. Hard disk yang berisi data/informasi backup dari sistem utama;
5. Rekaman email, mailing list, blog, chat, dan mode interaksi dan komunikasi lainnya;
6. Beraneka ragam jenis berkas file yang dibuat oleh sistem maupun aplikasi untuk membantu melakukan manajemen file (misalnya: .tmp, .dat, .txt, dan lain-lain);
7. Rekam jejak interaksi dan trafik via internet dari satu tempat ke tempat yang lain (dengan berbasis IP address misalnya);
8. Absensi akses server atau komputer yang dikelola oleh sistem untuk merekam setiap adanya pengguna yang login ke piranti terkait; dan lain sebagainya.

Beraneka ragam jenis obyek tersebut selain dapat memberikan petunjuk atau jejak, dapat pula dipergunakan sebagai alat bukti awal atau informasi awal yang dapat dipergunakan oleh penyelidik maupun penyidik dalam melakukan kegiatan penelusuran terjadinya suatu peristiwa kriminal, karena hasil forensik dapat berupa petunjuk semacam:

1. Lokasi fisik seorang individu ketika kejahatan sedang berlangsung (alibi);
2. Alat atau piranti kejahatan yang dipergunakan;
3. Sasaran atau target perilaku jahat yang direncanakan;
4. Pihak mana saja yang secara langsung maupun tidak langsung terlibat dalam tindakan kriminal;
5. Waktu dan durasi aktivitas kejahatan terjadi;
6. Motivasi maupun perkiraan kerugian yang ditimbulkan;
7. Hal-hal apa saja yang dilanggar dalam tindakan kejahatan tersebut;
8. Modus operandi pelaksanaan aktivitas kejahatan; dan lain sebagainya.

BAB III

KESIMPULAN

Data adalah salah satu hal yang terpenting dalam proses investigasi dan pemecahan kasus, proses tersebut dimulai dari mendapatkan, mengolah, menyajikan dan mempresentasi data forensik merupakan langkah pelaporan dalam persidangan atas temuan forensik, kesahihan data forensik ditentukan oleh kriteria, struktur pelaporan, kapasitas penyidik, dengan menerapkan prosedur dalam presentasi data forensik

DAFTAR PUSTAKA

- Jack wiles, Anthony Reyes, Jesse Varsalone.2007. The Best Damn Cybercrime and Digital Forensics Book. United states Of America. Syngress Publishing.Inc
- Bertino, A.J. (2008). Forensics Science: Fundamental and Investigations
- Casey, E. (2011). Digital Evidence and Computer Crime : Forensics Science, Computers and the Internet
- <http://www.wongkebumen.com/2012/12/penanganan-barang-bukti-hingga.html>
- <http://folder.idsirtii.or.id/pdf/IDSIRTII-Artikel-ForensikKomputer.pdf>
- www.academia.edu/5526997/PEMANFAATANBARANGA_BUKTI_UNTUK_MENGUNGKAP_KASUS_KRIMINAL