PERTEMUAN V

IT FORENSIK

5.1 Forensik Teknologi Informasi

Forensik yang identik dengan tindakan kriminal, sampai saat ini hanya sebatas identifikasi, proses, dan analisa pada bagian umum. Untuk kejahatan komputer di Indonesia, forensik di bidang komputer biasanya dilakukan tanpa melihat apa isi di dalam komputer. Justru lebih banyak bukti jika forensik di dalam komputer itu di indetifikasi.

Terminologi forensik komputer sendiri adalah suatu proses mengidentifikasi, memelihara, menganalisa, dan mempergunakan bukti digital menurut hukum yang berlaku (Moroni Parra, 2002). Forensik komputer yang kemudian meluas menjadi forensik teknologi informasi masih jarang digunakan oleh pihak berwajib, terutama pihak berwajib di Indonesia.

5.2 Bukti Digital (*Digital Evidence*)

Bukti digital adalah informasi yang didapat dalam bentuk/format digital **(Scientific Working Group on Digital Evidence, 1999)**. Bukti digital ini bisa berupa bukti yang riil maupun abstrak (perlu diolah terlebih dahulu sebelum menjadi bukti yang riil). Beberapa contoh bukti digital antara lain :

- E-mail, alamat e-mail
- Wordprocessor/spreadsheet files
- Source code dari perangkat lunak
- Files berbentuk image (.jpeg, .tif, dan sebagainya)
- *Web browser bookmarks, cookies*
- Kalender, *to-do list*

5.2.1 Empat Elemen Kunci Forensik dalam Teknologi Informasi

Adanya empat elemen kunci forensik dalam teknologi informasi2 adalah sebagai berikut :

1. Identifikasi dari Bukti Digital

Merupakan tahapan paling awal forensik dalam teknologi informasi. Pada tahapan ini dilakukan identifikasi di mana bukti itu berada, di mana bukti itu disimpan, dan bagaimana penyimpanannya untuk mempermudah tahapan selanjutnya. Banyak pihak yang mempercayai bahwa forensik di bidang teknologi informasi itu merupakan forensik pada komputer. Sebenarnya forensik bidang teknologi informasi sangat luas, bisa pada telepon seluler, kamera digital, *smart cards*, dan sebagainya. Memang banyak kasus kejahatan di bidang teknologi informasi itu berbasiskan komputer. Tetapi perlu diingat, bahwa teknologi informasi tidak hanya komputer/internet.

2. Penyimpanan Bukti Digital

   Termasuk tahapan yang paling kritis dalam forensik. Pada tahapan ini, bukti digital dapat saja hilang karena penyimpanannya yang kurang baik. Penyimpanan ini lebih menekankan bahwa bukti digital pada saat ditemukan akan tetap tidak berubah baik bentuk, isi, makna, dan sebagainya dalam jangka waktu yang lama. Ini adalah konsep ideal dari penyimpanan bukti digital.

3. Analisa Bukti Digital

   Pengambilan, pemrosesan, dan interpretasi dari bukti digital merupakan bagian penting dalam analisa bukti digital. Setelah diambil dari tempat asalnya, bukti tersebut harus diproses sebelum diberikan kepada pihak lain yang membutuhkan. Tentunya pemrosesan di sini memerlukan beberapa skema tergantung dari masing-masing kasus yang dihadapi.

4. Presentasi Bukti Digital

   Adalah proses persidangan di mana bukti digital akan diuji otentifikasi dan korelasi dengan kasus yang ada. Presentasi di sini berupa penunjukan bukti digital yang berhubungan dengan kasus yang disidangkan. Karena proses penyidikan sampai dengan proses persidangan memakan waktu yang cukup lama, maka sedapat mungkin bukti digital masih asli dan sama pada saat diidentifikasi oleh investigator untuk pertama kalinya.

5.2.2 Manajemen Bukti

Jika ditelusuri lebih jauh, forensik itu sendiri merupakan suatu pekerjaan identifikasi sampai dengan muncul hipotesa yang teratur menurut urutan waktu. Sangat tidak mungkin forensik dimulai dengan munculnya hipotesa tanpa ada penelitian yang mendalam dari bukti-

bukti yang ada. Investigator harus mampu menyaring informasi dari bukti yang ada tetapi tanpa merubah keaslian bukti tersebut.

Adanya dua istilah dalam manajemen (barang) bukti antara lain :

a. The Chain of Custody

Satu hal terpenting yang perlu dilakukan investigator untuk melindungi bukti adalah *the chain of custody*. Maksud istilah tersebut adalah pemeliharaan dengan meminimalisir kerusakan yang diakibatkan karena investigasi. Barang bukti harus benar - benar asli atau jika sudah tersentuh investigator, pesan-pesan yang ditimbulkan dari bukti tersebut tidak hilang.

Tujuan dari *the chain of custody* adalah :

1. Bukti itu benar-benar masih asli/orisinil
2. Pada saat persidangan, bukti masih bisa dikatakan seperti pada saat ditemukan. (biasanya jarak antara penyidikan dan persidangan relatif lama)

Untuk menjaga bukti itu pada mekanisme *the chain of custody* ini, dilakukan beberapa cara :

1. Gunakan catatan yang lengkap mengenai keluar-masuk bukti dari penyimpanan
2. Simpan di tempat yang dianggap aman.
3. Akses yang terbatas dalam tempat penyimpanan.
4. Catat siapa saja yang dapat mengakses bukti tersebut.

b. Rules of Evidence

Manajemen bukti kejahatan komputer juga mengenal istilah “Peraturan Barang Bukti” atau *Rules of Evidence*. Arti istilah ini adalah barang bukti harus memiliki hubungan yang relevan dengan kasus yang ada.

Dalam *rules of evidence*, terdapat empat persyaratan yang harus dipenuhi, antara lain :

1. Dapat Diterima (*Admissible*). Harus mampu diterima dan digunakan demi hukum, mulai dari kepentingan penyidikan sampai dengan kepentingan pengadilan.
2. Asli (*Authentic*). Bukti tersebut harus berhubungan dengan kejadian/kasus yang terjadi dan bukan rekayasa.
3. Lengkap (*Complete*). Bukti bisa dikatakan bagus dan lengkap jika di dalamnya terdapat banyak petunjuk yang dapat membantu proses investigasi.

4. Dapat Dipercaya (*Believable & Reliable*). Bukti dapat mengatakan hal yang terjadi di belakangnya. Jika bukti tersebut dapat dipercaya, maka proses investigasi akan lebih mudah. Walau relatif, dapat dipercaya ini merupakan suatu keharusan dalam penanganan perkara.

5.2.3 Metodologi Forensik Teknologi Informasi

Metodologi yang digunakan dalam menginvestigasi kejahatan dalam teknologi informasi dibagi menjadi dua, yaitu :

a. *Search & Seizure*

Investigator harus terjun langsung ke dalam kasus yang dihadapi, dalam hal ini kasus teknologi informasi. Diharapkan investigator mampu mengidentifikasi, menganalisa, dan memproses bukti yang berupa fisik. Investigator juga berwenang untuk melakukan penyitaan terhadap bukti yang dapat membantu proses penyidikan, tentunya di bawah koridor hukum yang berlaku.

b. Pencarian Informasi

Beberapa tahapan dalam pencarian informasi khususnya dalam bidang teknologi informasi :

1. Menemukan lokasi tempat kejadian perkara
2. Investigator menggali informasi dari aktivitas yang tercatat dalam log di komputer
3. Penyitaan media penyimpanan data (*data storages*) yang dianggap dapat membantu proses penyidikan

Walaupun terlihat sangat mudah, tetapi dalam praktek di lapangan, ketiga tahapan tersebut sangat sulit dilakukan. Investigator yang lebih biasa ditempatkan pada kasus kriminal non-teknis, lebih terkesan terburu-buru mengambil barang bukti dan terkadang barang bukti yang dianggap penting ditinggalkan begitu saja. Dalam menggali informasi yang berkaitan dengan kasus teknologi informasi, peran investigator dituntut lebih cakap dan teliti dalam menyidik kasus tersebut. Celah yang banyak tersedia di media komputer menjadikan investigator harus mengerti trik-trik kasus teknologi informasi.