"Aku lebih menghargai
orang yang **BERADAB**
daripada **BERILMU**.
Kalau hanya berlimu
IBLIS pun lebih tinggi
ilmunya daripada
~~MALAIKAT~~ **MANUSIA**."

Syekh Abdul Qadir Al-Jailani

Outline

Profesional Ethics in IT - Meet 4

- IT Forensik

Pendahuluan

- Forensik digunakan untuk mengungkap skandal yang terjadi pada suatu kasus dimana dugaan-dugaan sementara yang tadinya tidak memiliki bukti untuk ditelusuri.
- Identitas dan bukti kejahatan oleh tersangka tentunya akan disembunyikan sebaik-baiknya supaya tidak akan tertangkap oleh pihak berwajib.
- Dugaan kuat menjadi salah satu alasan dilakukannya forensik pada orang tersebut, pihak berwenang akan memeriksa secara menyeluruh mulai dari lingkungan, kenalan anda, dan bahkan barang-barang pribadi.
- Forensik sendiri mengalami perkembangan dimana penelusuran dilakukan dengan tool menggunakan teknologi terkini. Teknologi untuk analisis dan identifikasi untuk keperluan forensik dikembangkan tersendiri untuk mendukung kerja kepolisian, misalnya dipekerjakannnya seorang pakar IT untuk menggunakan komputer untuk keperluan forensik.

Komputer Forensik

- Forensik:
  Suatu proses ilmiah dalam mengumpulkan, menganalisa, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum.
- Forensik Komputer:
  Suatu proses mengidentifikasi, memelihara, menganalisa dan menggunakan bukti digital menurut hukum yang berlaku (Moroni Parra, 2002). Istilah ini kemudian meluas menjadi Forensik Teknologi Informasi
- Komputer forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan – penyaringan dan dokumentasi bukti komputer dalam kejahatan komputer
- Melakukan penyelidikan dan analisis komputer untuk menentukan potensi bukti legal

Komputer Forensik

- Mengumpulkan dan analisis data dari sumber daya komputer:
  - Sistem komputer
  - Jaringan komputer
  - Jalur komunikasi
  - Media penyimpanan
  - Aplikasi komputer
- Forensik komputer : mengabungkan keilmuan hukum dan komputer
- Forensik komputer = digital forensik

Data Elektronik dan Bukti Digital

- Data elektronik
  Dokumen, informasi keuangan, e-mail, job schedule, log, transkripsi voice-mail
- Bukti digital
  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)

Kebutuhan Komputer Forensik

- Keperluan investigasi tindak kriminal dan pelanggaran perkara pelanggaran
- Rekontruksi duduk perkara insiden keamanan komputer
- Upaya pemulihan akan kerusakan sistem
- Troubleshooting yang melibatkan hardware dan software
- Keperluan memahami sistem atau berbagai perangkat digital dengan lebih baik

Definisa Komputer Forensik

- Penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk mengekstrak dan memelihara barang bukti tindakan kriminal
- Menurut Judd robin: Penerapan secara sederhana dari penyelidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin
- Menurut New Technologies: Komputer forensik berkaitan dengan pemeliharaan, identifikasi, ekstraksi dan dokumentasi dari bukti-bukti komputer yang tersimpan dalam wujud informasi magnetik

Cabang IT Forensik

Pada praktiknya terdapat beberapa cabang pekerjaan untuk IT Forensik yang lebih spesifik seperti:

1. Database Forensik
   Mengumpulkan dan menganalisis database/table ataupun transaksi yang spesifik untuk merekonstruksi data atau event yang telah terjadi pada sisten. Sistem database yang memiliki fitur log audit akan memudahkan pekerjaan ini.
2. Network Forensik
   Melihat dan melakukan penelurusan terhadap traffic network untuk memeriksa kejanggalan. Contohnya pemeriksaan paket data yang meningkat secara tidak wajar dan kemungkinan terjadinya serangan DDoS.

Cabang IT Forensik

1. Mobile device Forensik
   Perkembangan penggunaan smartphone semakin meningkat, penyimpanan data pada setiap individu ataupun komunikasi yang dilakukan lewat device mobile dapat dilacak sepenuhnya berdasarkan history yang tercatat pada log system, misalnya smartphone berbasis android.
2. Fotografi Forensik
   Salah satu teknik forensik menggunakan analisa vektor untuk pembuktian media seperti video digital yang kualitasnya buruk. Pelaku memalsukan bukti menggunakan teknik pengolahan media seperti foto maupun video untuk menghindari kemungkinan dirinya menjadi terdakwa.

Cabang IT Forensik

Cabang pekerjaan IT forensik tidak hanya terbatas pada keempat hal tersebut. Pengumpulan fakta, penelusuran, dan melakukan pembuktian terhadap hal yang abu-abu adalah hal utama yang dilakukan oleh ahli forensik. Perkembangan teknologi maupun jaman akan terus memperbanyak variasi penyelidikan menggunakan media komputerisasi. Gabungan logika, pengalaman, pengetahuan, dan rasa keadilan yang tinggi menjadikan bidang ini menjadi suatu seni untuk mengungkap kasus-kasus hukum.

Investigasi

Menurut Judd Robbins, seorang pakar forensik, urutan langkah untuk mengambil bukti secara digital adalah sebagai berikut:

- Mengamankan sistem komputer untuk meyakinkan agar data dan peralatan komputer tidak dapat diakses oleh pihak yang tidak berwenang ataupun tidak berkepentingan. Jika sistem terhubung dengan internet maka segera putuskan koneksi tersebut.
- Pastikan seluruh file, yang tersembunyi ataupun tidak terenkripsi di copy. Proses investigasi akan memerlukan data-data tersebut.
- Mengembalikan sebanyak mungkin file yang telah terhapus menggunakan tool pendeteksi file.
- Mencari dan menemukan file tersembunyi.
- Melakukan decrypt pada data yang terproteksi.

Investigasi

- Menganalisa area disk yang normalnya tidak dapat diakses tetapi dapat dijadikan tempat persembunyian data.
- Dokumentasikan seluruh langkah sebagai bukti bahwa investigasi dilakukan tanpa merusak data-data yang ada.
- Meyiapkan kesaksian yang diperlukan pada proses pengadilan.

Anti Forensik

- Bila terdapat IT forensik yang melakukan investigasi data, terdapat Anti Forensik yang berusaha untuk melawannya. Anti forensik akan mengamankan data-data yang telah tersimpan agar tidak sampai kepada pihak-pihak yang ingin melakukan penyadapan. Apakah anda masih ingat kasus pembongkaran atas penyadapan telepon Presiden SBY oleh amerika? Profesi IT forensic menjadi salah satu yang dipanggil untuk dilakukannya konsultasi.
- Teknik-teknik yang dapat di pakai untuk Anti Forensik terbilang lebih beragam, misalnya untuk melakukan perlindungan data perusahaan ataupun penghilangan jejak transaksi yang dilakukan.

Anti Forensik

Beberapa teknik yang digunakan untuk anti forensik:

- Enkripsi
  Enkripsi adalah teknik klasik untuk mengubah format yang akan dikirimkan kepada pihak lain agar hanya dapat di baca oleh penerima saja. Dengan teknik dan tool enkripsi yang baik data-data yang telah di ubah formatnya walaupun telah tercuri oleh pihak ketiga, namun tidak dapat untuk dibaca ataupun diakses paket datanya.
- Steganografi
  Seni untuk menyembunyikan data dalam bentuk lain dalah steganografi. Data tersebut di sembunyikan dan dikirimkan dalam bentuk format file lain. Teknik ini dilakukan untuk mengelabui para forensik, contohnya adalah mengubah format extensi file menjadi mp3 agar dikira mengirimkan lagu namun sebenarnya bukan file lagu.

Anti Forensik

- Hash Collision
  Hash digunakan sebagai identitas suatu file. Algoritma hash yang umumnya digunakan adalah md5. Dalam komputer forensik, hash dipakai untuk integritas suatu file. Pada maret 2005, Xiayun Wang dan Hong Bo Yu berhasil membuat dua file berbeda dengan hash md5 yang sama. Ilmu komputer forensic pun akan semakin sulit menentukan data yang original.
- Process Dump
  Bermain aman di memory tanpa menyentuh area penyimpanan seperti hard disk. Dengan melakukan sesuatu pada memory proses tracking akan menjadi tidak mungkin untuk dilakukan karena sistem hanya menyimpan data-data tersebut secara sementara ketika komputer di gunakan dan tak akan meninggalkan jejak untuk di track.

- Clear Imprint
  Menghilangkan jejak aktivitas seperti pada proses penggunaan layanan internet. Menggunakan IP address privat dan ISP yang hanya bekerja sama dengan pengguna. Para hacker menggunakan cara tersebut untuk menghilangkan jejak percobaan pembobolan suatu sistem ketika melakukan aksinya.

Tugas

- Buat makalah tentang tools yang digunakan ahli forensik minimal 10 tools.
- Isi makalah penjelasan tentang:
  - Makna dari tool forensik (1/2 – 1 halaman)
  - Penjelasan masing-masing dari 10 tools (minimal 5 halaman)
  - Ukuran huruf judul makalah 16 times new roman
  - Ukuran huruf sub judul makalah 14 times new roman
  - Ukuran huruf isi makalah 12 times new roman
- Tugas diupload di student site paling lambat tgl 1 Juni 2023 jam 01.00

Makanan yang sedap ada diruang tamu
Orang yang beradap sudah pasti berilmu