MODUL 10

DIGITAL FORENSIK

10.1 Tujuan Praktikum

1. Dapat mengetahui fungsi-fungsi Digital Forensik
2. Dapat menggunakan Tools Digital Forensik
3. Dapat mengembalikan data yang telah dihapus

10.2 Alat dan Bahan

1. Laptop
2. Mouse
3. Autopsy
4. Recuva

10.3 Dasar Teori

10.3.1 Digital Forensik

Digital Forensik adalah penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti/informasi yang secara magnetis tersimpan/disandikan pada komputer atur media penyimpanan digital sebagai alat bukti dalam mengungkapkan kasus kejahatan yang dapat dipertanggungjawabkan secara hukum.

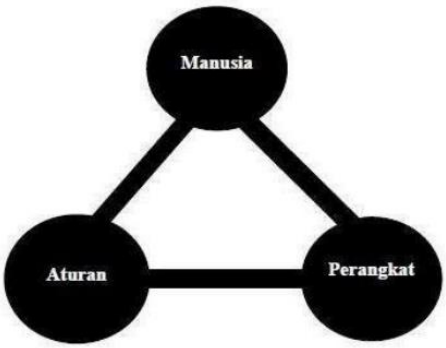
Digital forensik banyak dibutuhkan dalam berbagai keperluan, bukan hanya pada kasus-kasus kriminal yang melibatkan hukum. Secara umum kebutuhan digital forensik dapat diklasifikasikan sebagai berikut:

1. Keperluan investigasi tindak criminal dan perkara pelanggaran hukum.
2. Rekontruksi duduk perkara insiden keamanan komputer.
3. Upaya-upaya pemulihan kerusakan sistem.
4. *Troubleshooting* yang melibatkan *hardware* maupun software.

10.3.2 Komponen Digital Forensik

Komponen pada digital forensik pada umumnya hampir sama dengan bidang yang lain. Komponen ini mencakup manusia (*people*),

perangkat/peralatan (*equipment*) dan aturan (*protocol*) yang dirangkai, dikelola dan diberdayakan sedemikian rupa dalam Upaya mencapai tujuan akhir dengan segala kelayakan dan kualitas sebagaimana bisa dilihat pada gambar berikut:



Komponen Digital Forensik

Manusia yang diperlukan dalam komputer forensik merupakan pelaku yang tertunya mempunyai kualifikasi tertentu untuk mencapai kualitas yang diinginkan. Belajar forensic tidak sama dengan menjadi ahli dalam bidang forensic. Dibutuhkan lebih dari sekedar pengetahuan umum tentang komputer, tetapi juga pengalaman (*experience*) disamping berbagai pelatihan (*training*) pada materi-materi digital forensik yang telah ditempuh dan dibuktikan dengan sertifikat-sertfikat pendukung.

Ada tiga kelompok sebagai pelaku digital forensik:

1. *Collection Specialist*, yang bertugas mengumpulkan barang bukti berupa *digital evidence*.
2. *Examiner,* tingkatkan ini hanya memiliki kemampuan sebagai penguji terhadap media dan mengekstrak data.
3. *Investigator,* tingkatan ini sudah masuk ke dalam tingkatan ahli atau sebagai penyidik.

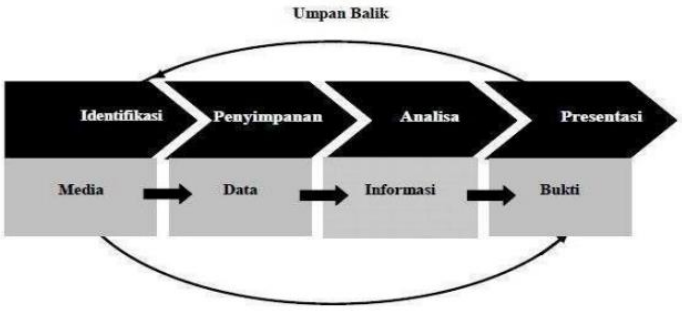
10.3.3 Tahapan pada Digital Forensik

Ada berbagai tahapan pada proses implementasi digital forensik. Secara garis besar dapat diklasifikasikan kepada empat tahapan, yaitu:

1. Identifikasi bukti digital
2. Penyimpanan bukti digital

3. Analisa bukti digital
4. Presentasi

Keempat tahapan ini secara terurut dan berkesinambungan digambarkan pada gambar berikut ini:



Tahapan Digital Forensik

10.3.4 Identifikasi Bukti Digital

Pada tahap ini bukti-bukti yang mendukung penyelidikan dikumpulkan. Penyelidikan dimulai dari identifikasi di mana bukti itu berada, di mana disimpan, dan bagaimana penyimpanannya untuk mempermudah penyelidikan. Media digital yang bisa dijadikan sebagai barang bukti mencakup sebuah sistem komputer, media penyimpanan (seperti *flashdisk, pen drive, hard disk,* atau CD-ROM), PDA, *handphone, smart card, sms, e-mail, cookies, source code, windows registry, web browser bookmark, chat log,* dokumen, *log file,* atau bahkan sederetan paket yang berpindah dalam jaringan komputer.

Tahapan ini merupakan tahapan yang sangat menentukan karena bukti-bukti yang didapatkan akan sangat mendukung penyelidikan untuk mengajukan seseorang ke pengadilan dan diproses sesuai hukum hingga akhirnya dijebloskan ke tahanan. Penelusuran bisa dilakukan untuk sekedar mencari “ada informasi apa disini?” sampau serinci pada “apa urutan peristiwa yang menyebabkan terjadinya situasi terkini?”.

Forensik pada dasarnya adalah pekerjaan identifikasi sampai dengan muncul hipotesa yang teratur menurut urutan waktu. Sangat tidak mungkin forensik dimulai dengan munculnya hipotesa tanpa ada penelitian yang

mendalam berdasarkan bukti-bukti yang ada. Dalam kaitan ini pada digital forensik dikenal istilah *chain of custody* dan *rules of evidence.*

Chain of custody artinya pemeliharaan dengan meminimalisir kerusakan yang diakibatkan karena investigasi. Tujuan dari *chain of custody* adalah:

- Menjamin bahwa bukti itu benar-benar masih asli (*authentic*).
- Pada saat persidangan, bukti masih bisa dikatakan seperti pada saat ditemukan karena biasanya jarak antara penyidikan dan persidangan relatif lama.

Beberapa hal yang menjadi pertimbangan sesuai dengan aturan *chain of custody* ini adalah:

1. Siapa yang mengumpulkan bukti?
2. Bagaimana dan di mana?
3. Siapa yang memiliki bukti tersebut?
4. Bagaimana penyimpanan dan pemeliharaan bukti itu?

Lalu sebagai alternatif penyelesaian ada beberapa cara yang bisa dilakukan, yaitu:

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

Sedangkan *rules of evidence* artinya pengaturan barang bukti di mana barang bukti harus memiliki keterkaitan dengan kasus yang diinvestigasi dan memiliki kriteria sebagai berikut:

- Layak dan dapat diterima (*Admissible*)

  Artinya barang bukti yang diajukan harus dapat diterima dan digunakan demi hukum, mulai dari kepentingan penyidikan sampai ke pengadilan.

- Asli (*Authentic*)

  Barang bukti harus mempunyai hubungan ketertarikan yang jelas secara hukum dengan kasus yang diselidiki dan bukan rekayasa.

- Akurat (*Accurate*)
  Barang bukti harus akurat dan dapat dipercaya.

- Lengkap (*Complete*)
  Bukti dapat dikatakan lengkap jika di dalamnya terdapat petunjuk-petunjuk yang lengkap dan terperinci dalam membantu proses investigasi.

10.3.5 Penyimpanan Bukti Digital

Tahapan ini mencakup penyimpanan dan penyiapan bukti-bukti yang ada, termasuk melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu. Bukti harus benar-benar steril artinya belum mengalami proses apapun Ketika diserahkan kepada ahli digital forensik untuk diteliri. Karena bukti digital bersifat sementara (*volatile*), mudah rusak, berubah dan hilang, maka pengetahuan yang mendalam dari seorang ahli digital forensik mutlak diperlukan. Kesalahan kecil pada penanganan bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan. Bahkan menghidupkan dan mematikan komputer dengan tidak hati-hati bisa saja merusak/merubah barang bukti tersebut.

10.3.6 Analisa Bukti Digital

Tahapan ini dilaksanakan dengan melakukan analisa secara mendalam terhadap bukti-bukti yang ada. Bukti yang telah didapatkan perlu di-*explore* kembali ke dalam sejumlah skenario yang berhubungan dengan tindak pengusutan, seperti:

1. Siapa yang telah melakukan?
2. Apa yang telah dilakukan?
3. Apa saja *software* yang digunakan?
4. Hasil proses apa yang dihasilkan?
5. Waktu melakukan?

Penelusuran bisa dilakukan pada data-data sebagai berikut: alamat URL yang telah dikunjungi, pesan e-mail atau Kumpulan e-mail yang terdaftar, program *word processing* atau format ekstensi yang dipakai, dokumen

spreadsheet yang dipakai, format gambar yang dipakai apabila ditemukan, file-file yang dihapus maupun diformat, *password, registry windows, hidden files, log event viewers,* dan *log application*. Termasuk juga pengecekan pada metadata. Kebanyak file mempunyai metadata yang berisi informasi yang ditambahkan mengenai file tersebut seperti *computer name*, total *edit time*, jumlah *editing session*, di mana dicetak, berapa kali terjadi penyimpanan (*saving*), tanggal dan waktu modifikasi.

Selanjutnya melakukan *recovery* dengan mengembalikan file dan folder yang terhapus, unformat drive, membuat ulang partisi, mengembalikan *password*, merekontruksi ulang halaman web yang pernah dikunjungi, mengembalikan email-email yang terhapus dan seterusnya.

10.3.7 Presentasi

Presentasi dilakukan dengan menyajikan dan menguraikan secara detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa secara mendalam dan dapat dipertanggung jawabkan secara hukum di pengadilan. Laporan yang disajikan harus di *crosscheck* langsung dengan saksi yang ada, baik saksi yang terlibat langsung maupun tidak langsung. Hasil laporan akan sangat menentukan dalam menetapkan seseorang bersalah atau tidak sehingga harus dipastikan bahwa laporan yang disajikan benar-benar akurat, teruji, dan terbukti.