**VCLass Komputer Forensik**

1. Sebutkan dan jelaskan masing Kejahatan yang menjadikan system dan fasilitas TI sebagai sasaran!
2. Sebutkan ancaman terhadap system computer berdasarkan fungsi system computer!
3. Sebutkan dan jelaskan undang-undang yang mengatur tentang Informasi dan Transaksi Elektronik!
4. Sebutkan klasifikasi kebutuhan digital forensik!
5. Simpulkan definisi digital forensik, dan sebutkan pembagian ilmu digital forensic!
6. Jelaskan tentang *Chain of custody!*
7. *Jelaskan tahapan digital forensic!*
8. *Berikan contoh tools dari Identifikasi Bukti Digital, jelaskan*
9. *Jelaskan Bitstream image!*
10. *Sebutkan sertifikat kehalian yang harus dimiliki seorang digital forensic!*

Jawab :

1. Pencurian data pribadi, pembuatan dan penyebaran virus komputer, pembobolan situs, cyberwar dll

2. Ancaman terhadap System Computer :

– Interupsi :Sumber daya sistem komputer dihancurkan atau menjadi tak tersedia atau tak berguna. Interupsi merupakan ancaman terhadap ketersediaan. Contoh :  
o Penghancuran bagian perangkat keras, seperti harddisk  
o Pemotongan kabel komunikasi

– Intersepsi :Pihak tak diotorisasi dapat mengakses sumber daya. Intersepsi merupakan ancaman terhadap keterahasiaan. Pihak tak diotorisasi dapat berupa orang atau progaram komputer. Contoh :  
o Penyadapan untuk mengambil data rahasia.  
o Mengkopi file tanpa diotorisasi

– Modifikasi :Pihak tak diotorisasi tidak hanya mengakses tapi juga merusak sumber daya. Modifikasi merupakan ancaman terhadap integritas. Contoh :  
o Mengubah nilai-nilai file data  
o Mengubah program sehingga bertindak secara beda  
o Memodifikasi pesan-pesan yang ditransmisikan pada jaringan

– Fabrikasi : Pihak tak diotorisasi menyisipkan atau memasukkan objek-objek palsu ke sistem. Fabrikasi merupakan ancaman terhadap integritas. Contoh :  
o Memasukkan pesan-pesan palsu ke jaringan  
o Penambahan record ke file.

3. Undang-undang yang mengatur tentang Informasi dan Transaksi Elektronik:

Secara umum, materi Undang-Undang Informasi dan Transaksi Elektronik (UUITE) dibagi menjadi dua bagian besar, yaitu pengaturan mengenai informasi dan transaksi elektronik dan pengaturan mengenai perbuatan yang dilarang. Pengaturan mengenai informasi dan transaksi elektronik mengacu pada beberapa instrumen internasional, seperti UNCITRAL Model Law on eCommerce dan UNCITRAL Model Law on eSignature. Bagian ini dimaksudkan untuk mengakomodir kebutuhan para pelaku bisnis di internet dan masyarakat umumnya guna mendapatkan kepastian hukum dalam melakukan transaksi elektronik. Beberapa materi yang diatur, antara lain: 1. pengakuan informasi/dokumen elektronik sebagai alat bukti hukum yang sah (Pasal 5 & Pasal 6 UU ITE); 2. tanda tangan elektronik (Pasal 11 & Pasal 12 UU ITE); 3. penyelenggaraan sertifikasi elektronik (certification authority, Pasal 13 & Pasal 14 UU ITE); dan 4. penyelenggaraan sistem elektronik (Pasal 15 & Pasal 16 UU ITE).

4. Klasifikasi kebutuhan digital forensic :

Secara umum kebutuhan digital forensik dapat diklasifikasikan sebagai berikut:

* Keperluan investigasi tindak kriminal dan perkara pelanggaran hukum.
* Rekonstruksi duduk perkara insiden keamanan komputer.
* Upaya-upaya pemulihan kerusakan sistem.
* Troubleshooting yang melibatkan hardware maupun software
* Keperluan untuk memahami sistem ataupun berbagai perangkat digital dengan lebih baik.

5. Digital Forensic : penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti/informasi yang secara magnetis tersimpan/disandikan pada komputer atau media penyimpanan digital yang berguna untuk alat bukti yang sah dalam pengadilan.

Pembagian ilmu digital forensic :

* Firewall forensics
* Network Forensics
* Database Forensics
* Mobile Device Forensics

6. Chain of Custody adalah kronologis pendokumentasian barang bukti, dari mulai di temukan di TKP hingga penduplikasian dan penyimpanannya bsik secara ataupun digital.

7. Tahapan – tahapan digital forensic :

* Pengumpulan : Mengumpulkan dan mendapatkan bukti-bukti yang mendukung penyelidikan
* Pemeliharaan : Memelihara dan menyiapkan bukti-bukti yang ada termasuk melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu.
* Analisa : Melakukan analisa secara mendalam terhadap bukti-bukti yang ada, di-explore kembali kedalam sejumlah skenario yang berhubungan dengan tindak pengusutan
* Presentasi : Menyajikan dan menguraikan secara detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa secara mendalam dan dapat dipertanggung jawabkan

8. TeskDisk : adalah salah satu program yang dapat digunakan untuk mengembalikan (recover) partisi yang hilang.

9. Bitstream Image : Salinan hard drivesecara bit per bit atau dapat dikatakan sebagai sekumpulan file yang dapat digunakan untuk membuat Salinan persis dari hard drive. Bitstream Image dapat dibaca oleh sebagian besat alat yang digunakan oleh computer forensic untuk menganalisis hard drive seperti Encasr, FTK, ProDiscover, dll

10. Sertifikat kehalian yang harus dimiliki seorang digital forensic :

* *Certified Information System Security Professional* (CISSP)
* *Certified Forensics Analyst* (CFA)
* *Experienced Computer Forensic Examiner* (ECFE)
* *Certified Computer Examiner* (CCE)
* *Computer Hacking Forensic Investigator* (CHFI) dan
* *Advanced Information Security* (AIS).