Tugas UAS Kemanan Informasi

Oleh :

Nama : Rusi Hartono

Nim : 1310651010

Kelas : 1065 - B

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

Tugas 1

Telekomunikasi Dan Keamanan Jaringan

Tujuan keamanan informasi ruang lingkup tentang Telekomunikasi dan Kemanan Jaringan adalah sebagai Jaringan Arsitektur dan Desin, Jaringan Perangkat dan Protokol dan yang terakhir sebagai jalur komunikasi yang aman bagi jaringan.

Dengan adanya telekomunikasi dan keamanan jaringan, itu sangat memudahkan kita dalam mengakses telekomunikasi di dunia maya semisal telekomunikasi online banking, dan dengan adanya telekomunikasi maka diperlukan sebuah keamanan informasi yang tujuannya menjaga kerahasiaan dan juga integritas dalam mengakses telekomunikasi, sehingga bias meminimalisir hal-hal kejahatan yang tidak di inginkan.

Konsep dasar

Konsep dasar dalam keamanan jaringan ini adalah kita harus mengetahui dasar dasar dalam jaringan seperti :

1. LAN, WAN, MAN, dan PAN
2. Internet, Intranet, and Extranet
3. Lapisan OSI Layer
4. Dan banyak lagi dasar-dasar dalam jaringan

Perangkat dan protocol jaringan

Dalam protocol jaringan ini dapat penggunaannya dapat dikombinasikan antara perangkat keras dan perangkat lunak. Perangkat dan protocol jaringan ini adalah salah satu pendukung dalam keamanan jaringan seperti :

1. Bridges
2. Switch
3. Router
4. Firewall
5. Packet filter
6. Statefull firewall
7. Dan lain lain

Komunikasi aman

Setelah menjelaskan dasar konsep dasar, perangkat dan protocol pada jaringan. Selanjutnya yaitu menjelaskan komunikasi aman pada jaringan, melindungi data adalah hal yang sangat kompleks yang harus dihadapi dalam mengamankan datayang tujuannya untuk menjaga kerahasiaan maupun integritas dari data tesebut.

Dalam komunikasi yang aman yang perlu diperhatikan adalah :

1. protocol otentikasi dan kerangka kerja.
   Dan perngkat pendukung protocol otentikasi dan kerangka kerja adalah:

   a. PAP dan CHAPS

b. 802.1X dan EAP
c. VPN
d. PPP
e. IPsec
f. SSL dan TLS
g. VoIP

2. Wireless Local Area Networks (WLANs)
   WLANs ini tugasnya adalah mengirimkan informasi melalui elektomagnetik gelombang. Dan perangkat pendukung pada WLANs adalah:
   a. FHSS, DSSS, and OFDM
   b. 802.11 abgn
   c. WEP
   d. 802.11i
   e. RFID
   f. Bluetooth

Tugas 2

DIGITAL FORENSIK

Pengertian DIGITAL FORESNSIK

Berdasarkan Undang Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), segala aktivitas digital yang menyangkut informasi dan transaksi elektronik memiliki payung hukum dan dapat dijadikan sebagai alat bukti yang sah di pengadilan. Sejalan dengan hal tersebut maka diperlukan suatu mekanisme pembuktian yang legal dan dapat dipertanggungjawabkan secara hukum.

Digital forensik merupakan kombinasi ilmu hukum dan ilmu komputer yang digunakan untuk mengidentifikasi, mengumpulkan dan menganalisa data atau informasi dari suatu sistem komputer, jaringan, komunikasi nirkabel dan perangkat penyimpanan yang dapat digunakan sebagai barang bukti dalam penegakan hukum.

Prinsip kerja dari digital forensik mirip dengan yang dilakukan oleh kepolisian dalam mengusut bukti tindak kejahatan dengan menelusuri fakta-fakta yang ada. Yang membedakan adalah pada digital forensik proses dan kejadiannya terdapat dalam dunia maya atau pada dunia nyata dengan fokus pada aktivitas yang mengarah pada barang bukti digital.

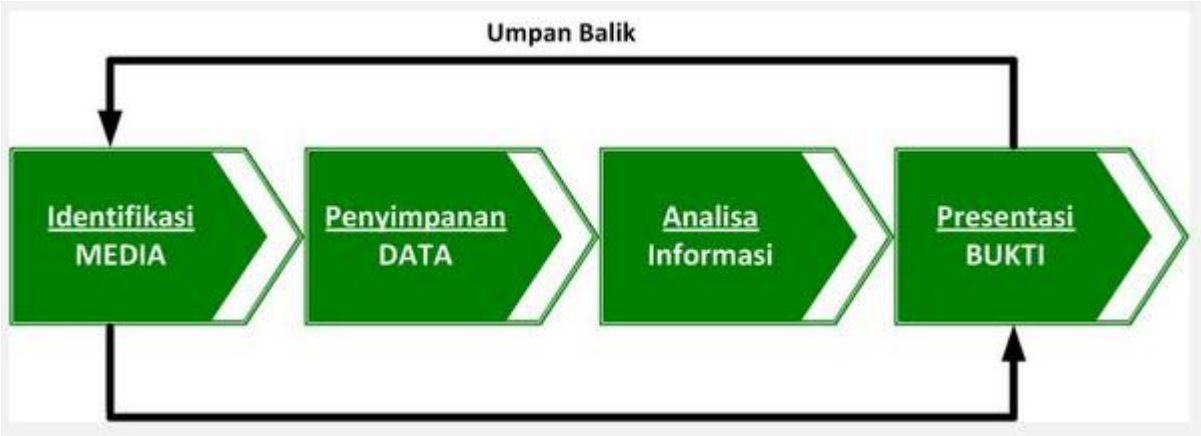
Secara garis besar tujuan utama dari digital forensik yaitu untuk membantu proses pemulihan dan analisa serta mempresentasikan barang bukti digital dengan sedemikian rupa sehingga dapat dipergunakan sebagai alat bukti yang sah di mata hukum. Selain itu digital forensik juga bertujuan untuk mendukung proses identifikasi barang bukti digital dengan jangka waktu yang singkat.

Dalam dunia kriminal terdapat sebuah istilah "tidak ada kejahatan yang tidak meninggalkan jejak". Ada banyak sekali hal atau objek yang bisa menjadi petunjuk dalam setiap tindak kriminal yang dilakukan dengan menggunakan teknologi komputer antara lain:

- *Log file* atau catatan aktivitas penggunaan komputer yang tersimpan dalam sistem operasi;
- File-file yang telah dihapus secara sistem namun secara teknikal masih bisa dipulihkan dengan menggunakan cara-cara dan perlengkapan tertentu;
- Catatan digital yang dimiliki oleh perangkat jaringan komputer seperti IDS (*Intrusion Detection System*) dan IPS (*Intrusion Prevention System*);
- Berbagai media penyimpanan yang berisi data atau informasi *backup* dari sistem utama;
- Rekam jejak interaksi dan lalu lintas data melalui jaringan komputer dari satu lokasi ke lokasi lain dan lain sebagainya.
- Lokasi pelaku ketika sedang melakukan tindak kriminal;
- Perangkat yang digunakan dalam melakukan tindak kriminal;
- Sasaran atau target dari pelaku tindak kriminal;
- Waktu dan durasi tindakan kriminal;
- Modus operandi yang digunakan;
- Hal-hal apa saja yang dilanggar dalam aktivitas tindak kejahatan tersebut.

Cara kerja DIGITAL FORENSIK

1. Tahapan tahapan cara kerja digital forensic



Keterangan:

1. Identifikasi Bukti Digital (*Acquisition*)
   Tahap ini merupakan tahap yang sangat menentukan dalam proses penyelidikan. Segala bukti yang dapat digunakan untuk mendukung proses penyelidikan dikumpulkan. Proses penyelidikan dimulai dari dimana bukti itu berada, dimana bukti itu disimpan dan bagaimana cara penyimpanannya. Pada tahap ini biasanya para penyelidik menggunakan *tools* berupa perangkat lunak seperti *Forensic Acquisition Utilities, Ftime, LiveView, Netcat, ProDiscover DFT, Psloggedon, UnxUtils*, dan lain sebagainya.

2. **Penyimpanan Bukti Digital (*Preservation*)**
   Tahapan ini mencakup penyimpanan dan penyiapan barang bukti yang ada, termasuk melindungi barang bukti dari kerusakan, perubahan, dan penghilangan oleh pihak-pihak tertentu. Barang bukti yang digunakan harus asli dan belum mengalami proses apapun ketika diserahkan kepada ahli digital forensik untuk dianalisa. Pada tahap ini diperlukan kemampuan yang tinggi dari seorang ahli digital forensik karena kesalahan kecil pada penanganan bukti digital dapat tidak diakui di pengadilan. Pada tahap ini biasanya seorang ahli digital forensik akan melakukan kloning (penggandaan secara persisi, satu banding satu) pada setiap bukti digital dan hasil kloning tersebut yang akan digunakan dalam tahap analisa bukti digital untuk mencegah terjadinya perubahan pada bukti digital.

3. **Analisa Bukti Digital (*Analysis*)**
   Tahapan ini dilaksanakan dengan melakukan analisa secara mendalam terhadap bukti-bukti yang ada. Data-data yang diperiksa dalam tahapan ini dapat berupa alamat website yang pernah dikunjungi, email, file *spreadsheet* dan *wordprocessing*, file gambar dan foto, file yang dihapus maupun di format, *registry*, file yang disembunyikan (*hidden file*), *event viewer*, dan log-log aplikasi. Pada tahap ini biasanya para penyelidik menggunakan *tools* berupa perangkat lunak seperti *Event Log Parser*, *Explore2FS*, *Libpff*, *Md5Deep, Outport, Pasco*, dan lain sebagainya

4. **Presentasi (*Presentation)***
   Pada tahapan ini merupakan tahap untuk menyajikan dan menguraikan laporan hasil penyelidikan yang telah dilakukan. Hasil laporan yang disajikan akan sangat menentukan dalam proses penetapan hukum. Oleh karena itu harus dipastikan bahwa laporan yang disajikan sudah benar-benar akurat, teruji dan terbukti.

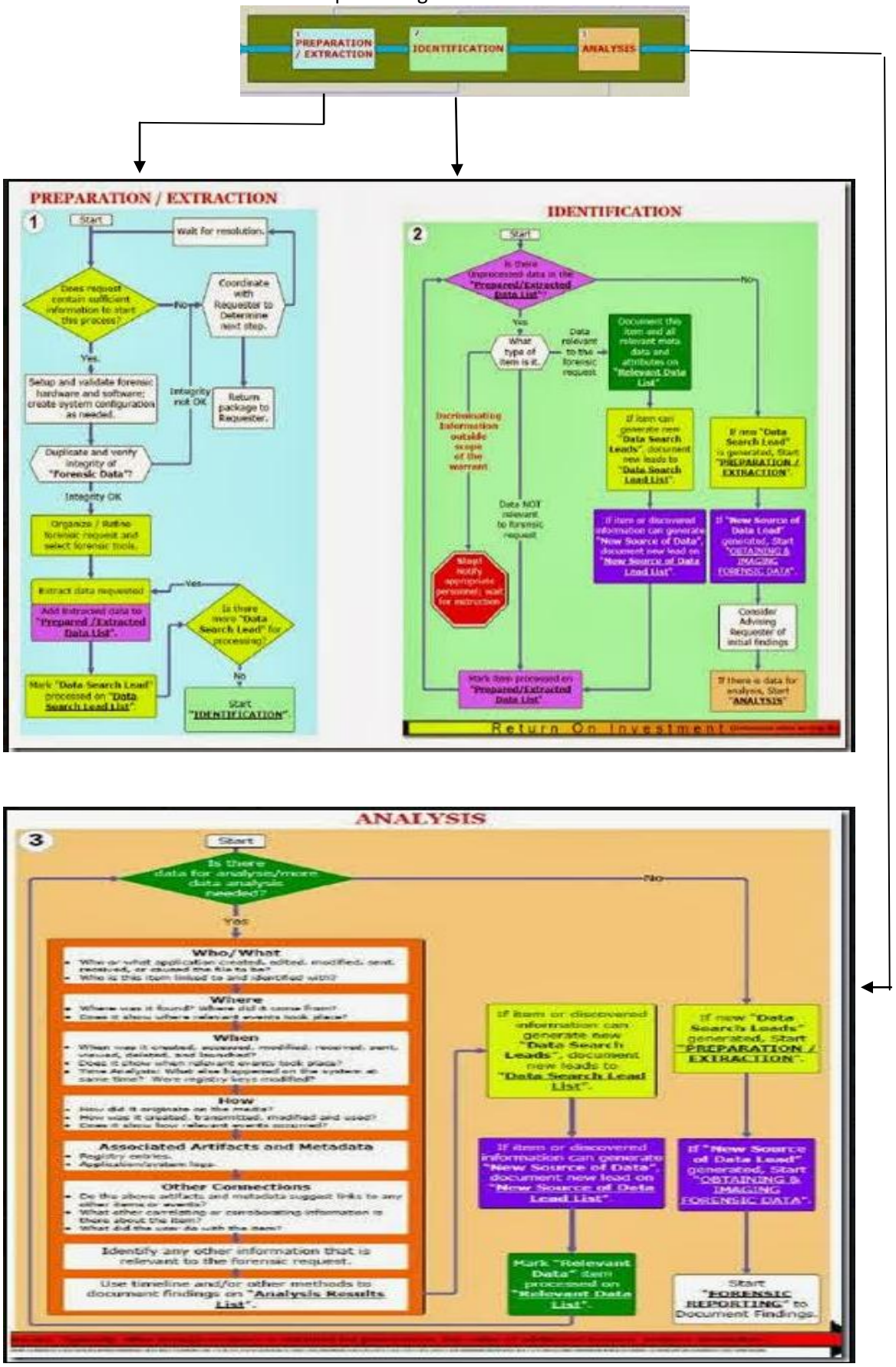
   Seiring dengan perkembangan teknologi informasi dan komunikasi, di masa yang akan datang objek penelitian dan cakupan dari digital forensik akan menjadi lebih luas lagi. Oleh karena itu keahlian dalam bidang digital forensik akan sangat dibutuhkan. Untuk menjadi seorang ahli dalam bidang digital forensik, seseorang harus memiliki pengetahuan yang mendalam tentang teknologi informasi dan komunikasi baik *hardware* maupun *software*. Seorang ahli digital forensik juga harus memiliki sertifikasi di bidang digital forensik sebelum dapat terjun langsung ke lapangan sebagai pengakuan keahlian yang dimilikinya. Sertifikasi dibidang digital forensik antara lain CHFI (*Computer Hacking Forensic Investigator*) dari EC-Council, GCIH (GIAC *Certified Incident Handler*) dan GCFA (GIAC *Certified Forensic Analyst*) dari SANS *Institue*, dan ENCE (EnCase Certified Examiner) dari Guidance Software.

Metodologi Digital Forensik menurut DFRWS (Digital Forensic Research Workshop) :

Dalam metode ini metede yang digunakan adalah :
" Identification, preservation, examination, analysis, presentation, and decision".
Dan untuk mengetahui metodologinya adalah sebagai berikut:

Keterangan:
Didalam alur proses metode tersebut terdapat alur data yang sangat berkaitan dimana didalam metode tersebut terdapat data forensik, dan kemudian data tersebut diminta selanjutnya data tersebut di siapkan untuk proses identifikasi suatu data tersebut dan selanjutnya data tersebut diananlisis, setelah melakukan penganalisis maka hasil dari data tersebut keluar dan hasil data tersebut dilaporkan selanjutnya melakukan analisis tingkatan dari kasus tersebut.

Dan dibawah ini adalah ikhtisar dari proses digital forensik:



Referensi

http://www.bppk.kemenkeu.go.id/publikasi/artikel/419-artikel-teknologi-informasi/19840-digital-forensik-“no-log,no-crime”.