TUGAS KEAMANAN JARINGAN KOMPUTER

“Digital Forensics”

Devi Purnama

09011281320016

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Digital Forensics

Sumber : https://www.youtube.com/watch?v=8NlyOFgFvh8

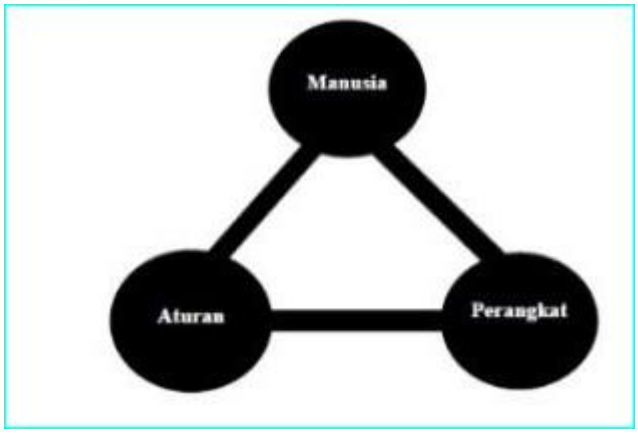
Judul : **Mobile Digital Forensics for Law Enforcement**

Digital Forensics

digital forensik dapat digunakan untuk atribut bukti tersangka tertentu, mengkonfirmasi alibi atau pernyataan, menentukan niat, mengidentifikasi sumbersumber (misalnya, dalam kasus hak cipta), atau mengotentikasi dokumen. Penyelidikan jauh lebih luas dalam lingkup dari area lain dari analisis forensik (dimana biasa tujuannya adalah untuk memberikan jawaban atas serangkaian pertanyaan sederhana) sering melibatkan waktu-baris kompleks atau hipotesis.

Komponen Digital Forensics

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:



Tahapan pada Digital Forensics Ada berbagai tahapan pada proses implementasi digital forensik. Namun menurut Kemmish secara garis besar dapat diklasifikasikan kepada empat tahapan, yaitu:

1. Identifikasi bukti digital
2. Penyimpanan bukti digital

3. Analisa bukti digital
4. Presentasi

Pada video Mobile Digital Forensics for Law Enforcement di jelaskan bahwa permintaan digital forensics apakah commersial, untuk menyelidiki penipuan / kejahatan dengan mengidentifikasi bukit digital yang berada di TKP. Bukti digital akan di bawa ke laboraturium forensik untuk memungkinkan informasi yang mencurigakan pada blacklogs. Setiap kejahatan memiliki jejak digital yang umum dari perangkat elektronik dapat menyimpan secara digital, hal ini yang akan memudakan polisi utuk mencari jejak dari sebua kejahatan. Setelah bukti yang telah di dapatkan maka ada dasar strategi forensics yang dapat dipraktekan saat digunakan adalah dengan bag tag dan mengirim perangkat ke laboraturium forensics untuk analisis dan menemukan bukit dari sebuah kejahatan. Sebelum perangkat digital di bawa ke laboratorium ada beberapa hal yang harus di perhatikan, pastikan persiapan semua tools forensics yang dipergunakan secara resmi, periksa kerja semua peralatan lab agar berfungsi dengan baik, seperti macbook (360 Gb), USB Trumb Drever 16GB, iPad 64 GB, PC Laptop 250 GB, Portable HDD 500 GB, PC Netbook 128 GB, GPRS Device 4 GB, Memory Card 8 GB, Smart Phone, PC Tower 1 TB (bagged & removed for analysis).
Pilih ahli forensics yang tepat yang mampu meberikan kesaksian dan penjelasan yang baik untuk mempertahankan bukti. Pastika tools untuk tidak dalam mengakses sistem file dari media bukti, setelah selesai simpan barang bukti di tempat yang aman. Tool forensics harus bekerja baik dan tidak mengubah data Di samping itu, komunitas komputer forensik harus menerima tool dan hasilnya. Tool yang sama kadang dipergunakan untuk melakukan pemantauan dan audit pada jaringan. Tool kit untuk pengujian forensik memungkinkan untuk mengumpulkan dan analisis data, seperti tcpdump, Argus, NFR, tcpwrapper, sniffer, nstat, tripwire, diskcopy (/v pada DOS), DD pada Unix. Karena ahli hukum percaya bit lebih mudah dipalsukan daripada kertas.