**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

**Session 12**

**Principles and Investigations of Computer Forensics for risk mitigation**

**Computer Forensic Methodology**

Process forensic pada dasarnya dibagi menjadi tiga step yaitu:

1. Pengumpulan bukti bukti
2. Menganalisa bukti bukti
3. Membuat laporan dari analisa bukti bukti

Perlu diingat tujuan dari forensic adalah untuk membawa bukti bukti dalam persidangan.

**Pengumpulan bukti bukti**

Step ini adalah step yang paling penting dan yang harus dilakukan pertama tama. Dalam step ini kita harus mengidentifikasikan dan mengumpulkan materi baik itu hardware ataupun software yang berhubungan dengan incident. Perlu di catat bahwa semua materi ini tidak boleh cacat atau dicopy, semua materi ini akan dibawa ke lab untuk dilakukan analisa. Cara membawa materi atau bukti bukti ini harus juga diperhatikan. Terutama terhadap materi yang bisa rusak oleh gelombang elektromanetik. Siapkan plastic dan box yang anti static untuk menyimpan materi atau barang bukti ini. Foto atau dokumentasi pada saat pengumpulan bukti bukti ini juga tidak kalah pentingnya. Setiap kantong plastic atau box tempat bukti harus diberi tag yang mengandung arti, sehingga kita tahu apa dan bagaimana saat benda atau materi tersebut pertama kali ditemukan. Pada saat tiba ditempat kejadian, yang pertama kali dilakukan adalah merekam kondisi tempat incident baik dengan video ataupun dengan foto. Jangan pernah merubah sebuah benda pada saat pertama kali tiba di tempat incident. Apabila ada computer yang menyala, jangan dimatikan atau jangan log out sebelum di analisa oleh orang yang ahli forensic. Bukan hanya computer saja, tetapi semua alat atau hardware yang menyala tidak boleh dimatikan atau log out.

Kadang kala kita juga harus memeriksa computer staff yang mungkin ada kaitannya dengan incident, maka perlu di perhatikan pada saat membuat perjanjian kontrak kerja sebaiknya ada salah satu pasal yang menyatakan bahwa staff bersedia untuk di periksa computer nya untuk keperluan forensic.

Orang orang yang diberi tugas untuk melakukan forensic ini harus juga dilengkapi dengan tools, seperti external harddrive, flash untuk back up dan application atau software pendukungnya seperti software untuk melakukan imaging. Tergantung situasi, ada kalanya kita bisa membawa hardware ke lab atau jika tidak memungkinkan maka kita harus melakukan imaging di tempat.

Terakhir buatlah list dari materi yang akan dibawa ke lab dan dimintakan persetujuan dari orang yang bertanggung jawab pada area tersebut

**Menganalisa bukti bukti**

Sebelum menganalisa materi atau bukti yang diambil dari area kejadian, maka pertama kalinya kita harus membuat image dari bukti tersebut dan juga dibuatkan hash nya kalau diperlukan. Sehingga seorang investigator bekerja untuk menganalisa bukti dari hasil imaging, bukan dari materi atau bukti asli dari tempat incident. Buatlah catatan tentang semua step yang dilakukan dan juga semua hasil yang ditemukan dalam proses analisa barang bukti ini. Biasanya kita mengacu pada who, what dan where. Artinya informasi apa yang sudah ditemukan saat menganalisa materi atau barang bukti tersebut. Dimana informasi tersebut ditemukan, apakah pada folder tertentu atau file tertentu dan siapa yang membuat file atau folder tersebut.

**Membuat laporan dari analisa bukti bukti**

Terakhir adalah membuat laporan berkaitan dengan temuan dari analisa materi. Kemudian laporan ini diserahkan kebagian legal untuk dibuatkan atau dijadikan sebagai bukti dalam sidang di pengadilan.

