Nama : kholil anggara

Nim : 09011181320031

Introduction to digital forensics

Dapat saya simpulkan bahwa introduction to digital forensics dimana muculnya disiplin dalam keamanan komputer tidak ada standar dan beberapa penelitian investigasi yang terjadi setela insiden itu dan kembali ke adaan berkerja penyelidikan internal harus didasarkan pada kebijakan ir dapat menyebabkan investigasi kriminal dengan dukungan analog dengan dilakukan tkp di dunia nyata tujuan nya ialah untuk memulikan sebayak bukti tanpa mengubah tkp investigasi harus mendokumentasikan sebayak mungkin untuk menjaga chain of custody dan menetukan apakah kejadian yang sebenarnya terjadi atau tidak Tujuannya adalah untuk mengekstrak data dari bukti-bukti yang diperoleh blok yang tidak terisi Mark blok sebagai dialokasikan untuk menipu sistem file ruang yang tidak terpakai pada akhir file jika tidak berakhir pada batas blok ruang yang tidak digunakan dalam struktur data sistem file Data tersembunyi dalam data lain lokasi yang tidak terpakai atau tidak relevan digunakan untuk menyimpan informasi Yang paling umum tetapi juga dapat digunakan pada file executable, meta data, ruang sistem file slack Tergantung pada metode enkripsi, mungkin tidak layak untuk mendapatkan informasi. Menemukan kunci sering pendekatan yang lebih baik. Seorang tersangka mungkin terdorong untuk mengungkapkan kunci oleh hukum. Mencari data tersembunyi atau dienkripsi sulit dan bahkan mungkin mustahil. Ada beberapa Penyidik harus melihat petunjuk lain yaitu software steganografi, software kripto, sejarah perintah Bahkan jika file benar-benar dihapus dari disk, mungkin masih meninggalkan jejak web cache direktori sementara blok data yang dihasilkan dan tergantung pada tujuan dari penyelidikan Mencari bahan selundupan Merekonstruksi peristiwa yang terjadi Menentukan apakah sistem dikompromikan analisis Karangan Mencari file tertentu Database ilegal properti yang dicuri Menentukan apakah file yang ada adalah ilegal koleksi Musik atau film download Membutuhkan pengetahuan khusus dari sistem file dan OS. Data dapat dienkripsi, tersembunyi, dikaburkan Kebingungan akhiran file menyesatkan nama file yang menyesatkan lokasi yang tidak biasa Kemudian pencatat waktu tidak bisa memesan peristiwa yang terjadi di interval waktu yang sama Beberapa sistem yang berbeda jam hanyut E-mail header dan zona waktu Mencari file Kapasitas penyimpanan mendekati besarnya terrabyte Berpotensi jutaan file untuk menyelidiki rekonstruksi acara Puluhan, ratusan peristiwa Menentukan siapa atau apa jenis orang membuat file. Program (Virus, Tojans, Sniffers / penebang) E-mail (Pemerasan, Pelecehan, kebocoran Informasi) Jika orang

yang sebenarnya tidak dapat ditentukan, hanya menentukan tingkat keterampilan penulis mungkin penting. Seorang penyidik yang dilakukan analisis mungkin harus muncul di pengadilan sebagai saksi ahli. Untuk penyelidikan internal, laporan atau presentasi mungkin diperlukan. Antangan menyajikan materi dalam hal sederhana sehingga juri atau CEO dapat memahaminya.