TUGAS

KEAMANAN JARINGAN KOMPUTER

Nama : Dede Triseptiawan

Nim : 09011181320001

SISTEM KOMPUTER

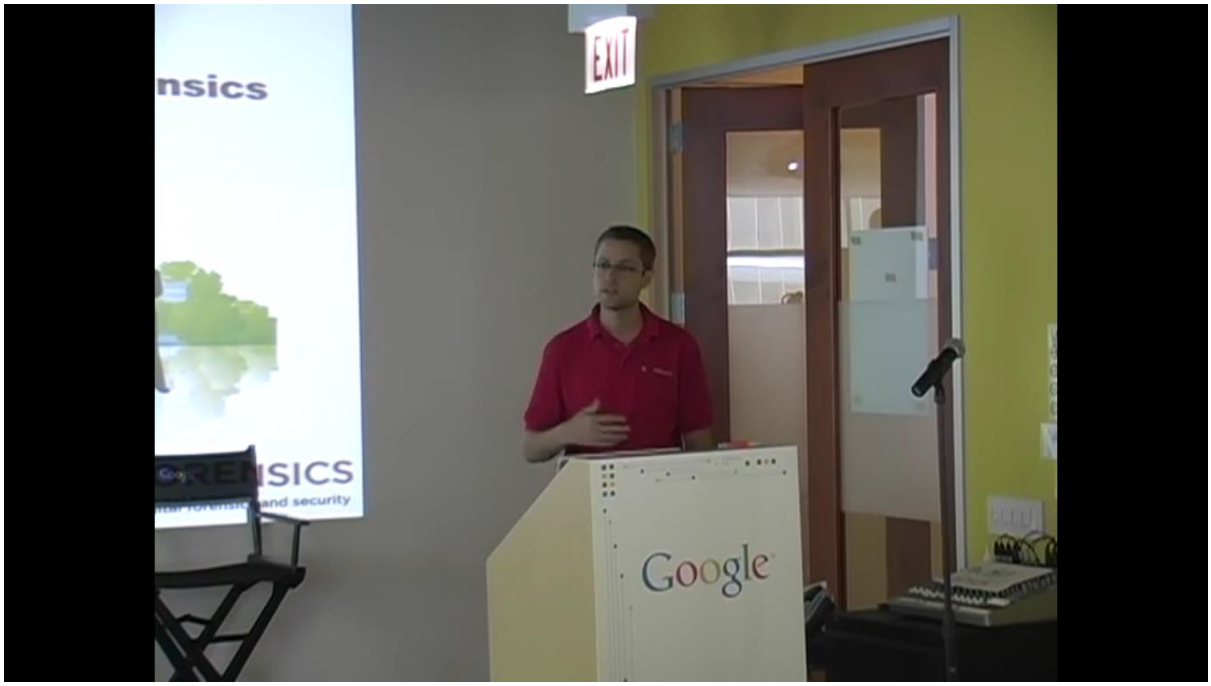
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Hasil analisa video teleconference tentang “digital forensic”

https://www.youtube.com/watch?v=rPd-HiEvhhw



Dengan judul “a geeks guide to digital forensics” atau bagaimana belajar untuk tidak takut dan suka terhadap hex editor. Oleh andrew hoog pada 16 juni 2011

Andrew hoog adalah seorang computer scientist, prev CIO, co-founder of viaforensics, dan seorang penulis dua buku tentang mobile forensics and security, seorang researcher, terhadap dua pending patent pada security and forensics, dan terhadap forensics ini andrew hoog mendapat multiple certifications, dan expert in federal and state court.

Digital forensics adalah cabang dari ilmu forensik yang menggunakan metode ilmiah. Dan digital forensics ini merupakan pemeliharaan, pemulihan, analisis dan pelaporan artefak digital termasuk informasi yang tersimpan di: komputer/ laptop, penyimpanan media(usb, cd, dvd, kamera, dll), handphone, dan dokumen elektronik.

Ada tipe yang biasanya digunakan.

- Reaktif : kasus pengadilan, penanganan insiden
- Proaktif : audit keamanan aplikasi mobile, pemantauan forensik berkelanjutan

Strategi akuisisi

Forensik analis dapat memperoleh / menerima data 3 cara yang berbeda

1. File backup : file backup disediakan dari "kustodian". ini dapat mencakup perangkat lunak backup dari perusahaan, File pst, itunes backup, dll
2. Akuisisi logical : salinan dari sistem berkas dibuat (yaitu tar.gz dari dan atau rekursif copy yang menjaga tanggal atau waktu)
3. Akuisisi fisik :
    a. Membuat sebuah replika digital yang tepat dari media penyimpanan
    b. Dapat memulihkan data yang dihapus
    c. Proses ini memerlukan alat analisis dan teknik khusus
    d. Firmware manajemen drive mungkin masih mempengaruhi akuisisi (FTL, bad blocks, dll)

Verivikasi gambar

1. Nilai hash : signature hex dihitung berdasarkan sekumpulan data
    - Nilai hash dapat digunakan untuk memverifikasi integritas gambar forensik. satu perubahan kecil dalam sumber akan menimbulkan efek "avalanche" nilai hash.
    - Untuk membuktikan bahwa dua set data adalah identik, nilai-nilai hash mereka harus sesuai.
    - Dalam beberapa contoh, nilai hash tidak stabil (nand flash) sehingga hash dari data seperti itu diekstrak diambil tapi belum tentu cocok jika sumber dicitrakan lagi.
2. Teknik hash pada umumnya
    - MD5 (nilai 128-bit)
    - SHA256 (nilai 256-bit)
3. md5 dari "andrew hoog" = 9bdbad9aecd74fce6e6bb48ee18100b8

Bagaimana memperoleh gambar forensik

1. jika mungkin, hubungkan drive ke write fisik blocker
    a. ini mencegah setiap menulis ke drive
    b. ada teknik perangkat lunak namun tidak efektif
    c. umumnya, tidak mungkin dengan perangkat nand Flash

2. forensik memperoleh perangkat dengan perangkat lunak
    a. open source: dd, dcfldd dan dc3dd (kita gunakan nanti)
    b. gratis: imager FTK dan banyak lainnya
    c. komersial: FTK, encase, dll
3. melakukan verifikasi sumber dan gambar dengan hash signiture dan merekam di chain of custody

"tipikal" langkah-langkah analisis forensik

1. membuat Kronologis semua peristiwa
    a. sistem file dimodifikasi, diakses, diubah dan menciptakan
    b. metadata dari file (gambar, dokumen, flash cookies, dll)
2. mount image dd read-only
3. menghasilkan daftar semua berkas (mengalokasikan dan dihapus)
4. menganalisis key file
5. memulihkan file dihapus
6. File carving
7. pencarian file, gambar dd, dll.
8. banyak teknik khusus