TUGAS KEAMANAN JARINGAN

" Resume Video Teleconference Mengenai Digital Forensic "

OLEH :

NAMA : MARDIAH

NIM : 09011281320005

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

INDERALAYA

2017

Defining a Digital Forensic Investigation

Oleh :

Brian D. Carrier

Purdue University / CERIAS

Investigasi digital telah terjadi dalam beberapa bentuk selama bertahun-tahun, namun tidak ada model ilmiah dari proses. Setelah semua itu, ada beberapa cara dan urutan di mana bukti-bukti dapat ditemukan. Penyidik tidak selalu perlu model untuk memecahkan suatu kasus, tetapi model ilmiah berguna untuk mengembangkan alat investigasi dan teknologi karena memungkinkan kita untuk mendefinisikan persyaratan dan mengidentifikasi apa daerah membutuhkan lebih banyak perhatian. Selanjutnya, ada pedoman untuk memasuki bukti teknis ke pengadilan AS yang mungkin memerlukan prosedur teknis yang akan diterbitkan dan telah dikenal tingkat kesalahan. Dalam pembicaraan ini, saya akan menyajikan gambaran dari model proses yang ada yang penyidik dapat menggunakan. Saya kemudian akan menyajikan temuan-temuan awal kami pada model yang lebih ilmiah yang didasarkan pada bagaimana bukti digital dibuat dan akan menunjukkan bagaimana hal itu dapat diterapkan pada model proses yang digunakan oleh praktisi. Kami model berbasis event memungkinkan kita untuk lebih jelas mendefinisikan persyaratan untuk peralatan investigasi, yang akan membantu dalam proses pengembangan dan pengujian.

1. Background

- Apa itu digital investigasi ?

  Adalah sebuah proses pengembangan dan pengujian hipotesis – hipotesis untuk menjawab pertanyaan tentang persitiwa digital sebelumnya
- Contoh pertanyaan dasar yang sering ditanyakan yaitu :
  1. Apa atau siapa penyebab dari peristiwa tersebut
  2. Kapan terjadinya peristiwa tersebut
  3. Mengapa terjadinya peristiwa tersebut
- Contoh investigasi
  1. Jaringan server yang rusak
  2. seorang karyawan melanggar kebijakan penggunaan komputer perusahaan
  3. seseorang mendownload gambar yang kurang baik di internet
  4. Seorang tersangka dalam kejahatan fisik memiliki komputer

2. Process Models

- DOJ Guidelines :
    1. Persiapan : menyiapkan perlengkapan dan tools
    2. Koleksi : mencari bukti digital yang memungkinkan pada lokasi
        - Mengambil atau mengcopy media digital
    3. Pemeriksaan : me – review media untuk bukti
    4. Analisa : me – review hasil pemeriksaan untuk hasil mereka pada kasus tersebut
    5. Laporan : dokumen hasil dari investigasi
- Incident Response Model :
    1. Persiapan
    2. Deteksi
    3. Respon awal (Verifikasi)
    4. Perumusan Strategi
    5. Sistem Duplikat
    6. Investigasi
    7. Secure Measure Implementation
    8. Jaringan Monitoring
    9. Pemulihan
    10. Pelaporan
- Crime Scene Model
    1. Berdasarkan proses TKP fisik:
    2. Pertahankan & mengisolasi TKP digital
    3. Survey TKP untuk bukti yang jelas
    4. Dokumen TKP
    5. Cari untuk bukti yang tersisa
    6. peristiwa merekonstruksi menentukan bagaimana bukti sampai di sana

3. Problem Definition

- Technical Requirement
    1. IR Model :
        - Bagaimana verifikasi yang berbeda dari investigasi?
    2. Crime Scene Model:
        - Bagaimana survei yang berbeda dari pencarian?

3. Fase Model Proses terlalu sewenang-wenang!
    - Apakah fase IR Investigasi meliputi Analisis DOJ dan Pemeriksaan?
    - Bagaimana Analisis DOJ berbeda dari kejahatan adegan Acara Rekonstruksi?

4. Proposed Solution

- Tentukan bidang teknis berdasarkan bagaimana bukti digital dibuat
- Mungkin tidak menyerupai model proses yang sebenarnya
- Tentukan persyaratan berdasarkan bidang teknologi

5. Our Approach

⇨ Digital Crime Scene Investigation

- Tujuan: untuk menentukan apa peristiwa digital terjadi dengan mengakui bukti digital
- Tiga jenis teknologi:
    - Kejahatan adegan pelestarian
    - Bukti pencarian
    - Rekonstruksi Acara

⇨ Digital Crime Scene Preservation

- Tujuan: mempertahankan keadaan sebanyak objek digital mungkin dokumen anf TKP
- Metode:
    - Tutup sistem itu dan menyalinnya
    - Sistem Cabut dari jaringan
    - Membunuh proses yang mencurigakan
    - Tidak melakukan apa-apa (tidak sangat efektif)

⇨ Digital evidence seraching

- Kita perlu menemukan bukti dari peristiwa
- Tujuan: untuk mengenali benda-benda digital yang berisi informasi tentang insiden itu
- Pendekatan:
    - Mengembangkan hipotesis
    - Tentukan karakteristik bukti
    - Bandingkan benda dengan target

⇨ Event reconstruction

- Kita mungkin perlu untuk menjawab bagaimana bukti sampai di sana
    - Pertahanan Trojan
- Tujuan: untuk menentukan peristiwa yang bukti ada dan telah dikumpulkan
- Tidak saat ini didukung oleh banyak alat-alat
- Pendekatan:
    - Menganalisis bukti
    - Menentukan penyebab dan efek peran itu bisa dimainkan
    - Membangun peristiwa sebab dan akibat benda
    - Peristiwa Urutan ke dalam rantai

6. Summary

1. Model Proses berguna untuk pelatihan dan pedoman
2. Tidak berguna untuk mendefinisikan kebutuhan teknologi
3. Pendekatan kami adalah untuk menentukan 3 daerah berdasarkan peristiwa