UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

STANDAR METODOLOGI KOMPUTER FORENSIK

Pengantar Komputer Forensik teknologi Informasi

Pendahuluan

- Apakah diperlukan standarisasi komputer forensik ?
- Bahasa pemograman, sistem komputer, perangkat keras dan lunak sudah memiliki standarisasi !
- Organisasi sudah memiliki prosedur, metode, aturan dan berbagammacam proses !
- Masalah inkompatibilitas selalu muncul seirang perkembangan komputer dan komunikasi

Pendahuluan

- Kebutuhan akan standarisasi di level manapun, sudah menjadi kebutuhan.
- Di masa sekarang kebutuhan akan ahli komputer forensik menjadi penting untuk penegak hukum, pemerintah, perusahaan dan individu.
- Jadi dibutuhkan suatu standar metodologi yang pasti dalam analisis dan penyelidikan forensik komputer

Menurut David Morrow

- "Seperti halnya anda tidak memulai perjalanan jauh ke daerah asing tanpa peta jalan, jangan memulai penyelidikan tanpa memperhatikan rencana "
- Mengikuti metode standar merupakan hal penting demi kesuksesan dan efektifitas komputer forensik

Cakupan Standar Metodologi

- Pendefinisian
- Prinsip
- Proses dan metode
- Hasil
- Bahasa

Lima faktor

- Standar komputer foerensik mengacu pada lima faktor, yaitu :
  - Identifikasi subjek
  - Memperbaiki komputer
  - Mengungkapkan jalur komunikasi
  - Permintaan investigasi
  - Pengumpulan digital evidence lainnya

Perkembangan Standar Komputer forensik

- Tahun 1993 ; Diselenggarakan konferensi internasional computer evidence
- Tahun 1995 ; Usulan pembentukan IOCE (International organization of computer evidence)
- Tahun 1997 ; G8 dan IOCE menentukan pengembangan standar Computer evidence
- Tahun 1998 ; Muncul tanggapan dan memunculkan organisasi seperti SWG-DE, ACPO, FCG, ENSFI dan INTERPOL
- Tahun 1999 ; SWG-DE, ACPO, FCG, dan ENSFI membahan mengenai standar computer evidence di Eropa

Panduan Keprofesian

- Pengujian komputer forensik harus dilakukan secara menyeluruh
- Media pengujian harus disterilisasi
- Image bit dari media asli harus dibuat dan untuk dianalisa
- Intregritas dari media asli harus dipelihara selama penyelidikan

Akronim PPAD pada komputer Forensik

- Preserve the data to ensure the data is not changed
- Protect the evidence to ensure no one else has access to the evidence
- Analyze the data using forensically sound techniques
- Document everything

Syarat pengujian Forensik

- The international association of computer investigative spesialists – IACIS memberikan tiga syarat pengujian komputer forensik :
  - Penggunaan media forensik yang steril
  - Pengujian harus mempertahankan integritas media asli
  - Printout dan copy data hasil pengujian harus ditandai, dikenali dan disertakan

Hal yang diperlukan

- Peralatan dan keahlian harus disinkronisasikan dengan penegak hukum
- Dibutuhkan dokumentasi dan rangkaian penanganan barang bukti,serta cukup banyak variabel dalam kasus forensik
- Diperlukan :
  - Definisikan metodologi (aturan dan panduan)
  - Kerjakan sesuai metodologi tersebut

Kemampuan penyelidik

- Aspek untuk meningkatkan kemampuan penyelidik :
  - Lakukan pemeriksaan ulang dengan tool yang berbeda
  - Tetap berusaha objektif selama penyelidikan
  - Yakinkan langkah anda disetujui pihak manajemen dan hukum
  - Kaitkan barang bukti dengan hardware tertentu

Kemampuan penyelidik

- Buatlah log tertulis selama penyelidikan (logis dan akurat)
- Gunakan capture full screen
- Backup barang bukti
- Kumpulkan juga barang bukti pada tempat terpisah

Kebijakan dan Prosedur

- Personel
- Pertimbangan administratif
- Permintaan layanan
- Manajerial kasus
- Pemprosesan kasus
- Mengembangkan prosedur teknikal

Pertimbangan administratif

- Pertimbangan administratif yang diperlukan
  - Software
  - Ketersediaan Sumber daya
  - Pelatihan

Manajerial Kasus

- Buatlah prioritas tertentu dengan mempertimbangkan faktor :
  - Tidak kriminal
  - Tanggal persidangan
  - Batas waktu
  - Pertimbangan hukum
  - Ketersediaan sumber daya
  - Korban potensial
  - Volatile dan non-volatile evidence

Mengembangkan prosedur teknikal

- Langkah – langkah pengembangan dan menilai kelayakan suatu prosedur adalah :
  - Identifikasi tugas dan masalah
  - Mengajukan solusi
  - Pengetasan setiap solusi pada sample
  - Evaluasi hasil pengetesan
  - Menyempurnakan prosedur

SWG-DE

- SWG-DE : Scientific working group on digital evidence
- Dibentuk tahun 1998 oleh the federal crime laboratory directors group
- Fokus kerja pada forensik digital evidence

IOCE

- IOCE : The international organization computer evidence, didirikan tahun 1995
- Sebagai media atau sarana pertukaran informasi bagi para penegak hukum skala internasional mengenai investigasi kejahatan komputer dan masalah forensik

Prinsip IOCE

- Konsisten terhadap sistem perundangan
- Menggunakan bahan umum
- Berdaya tahan
- Berkemampuan untuk melewati batas – batas internasional
- Mampu menanamkan keyakinan terhadap untegritas evidence
- Dapat diaplikasikan pada setiap forensic evidence
- Aplikatif untuk setiap tingkatan mencakup individual, organisasi dan negara

IACIS

- IACIS : The international association of computer investigative specialist
- Organisasi internasional yang terdiri dari para penegak hukum profedional yang ditujukan untuk kepentingan edukasi spedifikasi ilmu komputer forensik

Terima Kasih