UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

Profesi Ahli Forensik TI

Pengantar Komputer Forensik Teknologi Informasi

Pendahuluan

- Meningkatnya kejahatan dibidang TI, menyebabkan profesi atau keahlian yang berkaitan dengan masalah pengungkapan adanya kejahatan ini dibutuhkan.
- Seorang analisis forensik dalam pekerjaannya membantu penegak hukum atau pimpinan keamanan perusahaan

Pandangan Ahli

- Menurut James O. Holly [National computer forensics lab Ernst & Young
  - Anda perlu membuka pintu untuk pemprosesan administratif, sipil atau kriminal dam merespon kejahatan komputer, dan penyelidik perlu menangani insiden dari awal sampai masuk kepersidangan
- www. pcforensics.com
  - Data yang sudah dihapus masih bisa dihidupkan lagi

Pandangan Ahli

- Menurut Thomas Welch [The information security management handbook]
  - Praktisi keamanan komputer harus mempedulikan teknologi dan faktor legal yang berdampak pada sistem dan penggunanya, termasuk masalah penyelidikan dan penegakan hukum

Programmer vs Ahli Komputer Forensik

- Programmer ;
  - Bekerja melawan diri sendiri
  - Memcoba memperbaiki permasalahan yang kita buat sendiri
- Ahli Komputer Forensik
  - Bekerja menyelesaikan kejahatan komputer
  - Melawan seorang “programmer”

Keahlian Komputer Forensik dibutuhkan oleh :

- Jaksa Penuntut : menggunakan barang bukti komputer dalam kejahatan, seperti obat bius, pornografi anak, pembunuhan, dan penggelapan keuangan
- Detektif swasta bisa mempergunakan rekaman pada sistem komputer untuk melacak kasus penggelapan, perceraian, diskriminasi dan pelecehan.
- Perusahaan asuransi bisa mengurangi biaya dengan bukti komputer yang menyatakan kemungkinan penggelapan pada insiden, kebakaran, atau kompensasi pekerja

Keahlian Komputer Forensik dibutuhkan oleh :

- Perusahaan menyewa ahli komputer forensik untuk menentukan bukti yang berkaitan dengan pelecehan seksual, penipuan, pencurian rahasia dagang, dan informasi rahasia internal lainnya
- Petugas penegak hukum sering memerlukan bantuan dalam persiapan penggeledahan dan penyitaan perangkat komputer.
- Perorangan kadang menyewa ahli komputer forensik untuk mendukung klaim pemutusan kerja, pelecehan seksual atau dikriminasi umur.

PENGETAHUAN YANG DIPERLUKAN AHLI FORENSIK

- Dasar-dasar hardware dan pemahaman bagaimana umumnya sistem operasi bekerja
- Bagaimana partisi drive, *hidden partition*, dan di mana tabel partisi bisa ditemukan pada sistem operasi yang berbeda
- Bagaimana umumnya *master boot record* tersebut dan bagaimana *drive geometry*
- Pemahaman untuk *hide, delete, recover* file dan directory bisa mempercepat pemahaman pada bagaimana tool forensik dan sistem operasi yang berbeda bekerja.
- Familiar dengan header dan ekstension file yang bisa jadi berkaitan dengan file tertentu

KRITERIA AHLI FORENSIK

- Menurut Peter Sommer [Virtual City Associates Forensic Technician]
  - Metode yang berhati-hati pada pendekatan pencatatan rekaman
  - Pengetahuan komputer, hukum dan prosedur legal
  - Keahlian untuk mempergunakan utility
  - Kepedulian teknis dan memahami implikasi teknis dari setiap tindakan

KRITERIA AHLI FORENSIK

- Penguasaan bagaimana modifikasi bisa dilakukan pada data
- Berpikiran terbuka dan mampu berpandangan jauh
- Etika yang tinggi
- Selalu belajar
- Selalu mempergunakan data dalam mengambil kesimpulan

Aktivitas Penyelidik Forensik

- Perlindungan sistem komputer selama pengujian forensik dari semua kemungkinan perubahan, kerusakan, korupsi data, atau virus
- Temukan semua file pada sistem. Termasuk file normal, terhapus, *hidden, pasword-protected*, dan terenkripsi.
- *Recovering* file terhapus sebisa mungkin.
- Ambil isi file *hidden* juga file *temporary* atau *swap* yang dipergunakan baik oleh sistem operasi atau program aplikasi
- Lakukan akses (jika dimungkinkan secara legal) isi dari file terproteksi atau terenkripsi

Aktivitas Penyelidik Forensik

- Analisa semua data yang relevan pada area spesial di disk. Misal *unnalocated* (tidak terpakai, tapi mungkin menyimpan data sebelumnya), *slack space* (area di akhir file pada *last cluster* yang mungkin menyimpan data sebelumnya juga)
- Cetak semua analisis keseluruhan dari sistem komputer, seperti halnya semua file yang relevan dan ditemukan. Berikan pendapat mengenai layout sistem, struktur file yang ditemukan, dan informasi pembuat, setiap usaha menyembunyikan, menghapus, melindungi, mengenkripsi informasi, dan lainnya yang ditemukan dan nampak relevan dengan keseluruhan pengujian sistem komputer.
- Berikan konsultasi ahli dan kesaksian yang diperlukan

KARAKTERISTIK SEORANG AHLI FORENSIK

- Pendidikan, pengalaman dan sertifikasi merupakan kualifikasi yang baik untuk profesi komputer forensik. Pendidikan dengan pengalaman memberikan kepercayaan yang diperlukan untuk membuat keputusan dan mengetahui keputusan yang tepat. Sertifikasi menunjukkan bahwa pendidikan dan pengalamannya merupakan standar yang tinggi dan dapat dipahami.

KARAKTERISTIK SEORANG AHLI FORENSIK

- Yakinkan pada setiap tindakan dan keputusan, agar mencukupi untuk kesaksian di pengadilan
- Semua proses dilakukan dengan menyeluruh
- Memiliki pengetahuan yang banyak mengenai bagaimana *recover* data dari berbagai tipe media

KARAKTERISTIK SEORANG AHLI FORENSIK

- Mampu memecah password dari aplikasi dan sistem operasi yang berbeda dan mempergunakannya untuk penyelidikan
- Perlu pengetahuan yang memadai, tanpanya bisa terjadi kesalahan yang akan membuat barang bukti ditolak di pengadilan. Barang bukti bisa dirusak, diubah, atau informasi yang berharga terlewat.

KARAKTERISTIK SEORANG AHLI FORENSIK

- Obyektif dan tidak bias, harus *fair* pada penyelidikan, dengan fakta yang akurat dan lengkap
- Inovatif dan memiliki kemampuan interpersonal yang baik
- Memiliki kemampuan verbal dan oral yang baik
- Menggunakan penalaran dan logika yang tepat

SERTIFIKASI AHLI FORENSIK TI

- EnCase Certified Examiner Program (EnCE) http://www.iacis.com
- Computer Forensics External Certification (CCE) , http//:www.giac.org/certifications/ security/gcfa.php
- GCFA – GIAC Certified Forensics Analyst http//:www.giac.org/certifications/security/gcfa.php
- Q/FE Qualified Forensics Expert http://www.securityuniversity.net/certification. htm

SERTIFIKASI AHLI FORENSIK TI

- TruSecure ICSA Certified Security Associate http://www.icsalabs.com
- CCE – Certified Computer Examiner http://www. certified-computer-examiner.com/
- Computer Forensic Training Online http://www.kennesaw.edu/coned/sci/for_online.htm

Kesimpulan

- Ahli komputer forensik merupakan suatu bidang pekerjaan yang akan banyak dibutuhkan
- Ahli komputer forensik merupaka area kerja relatif baru dan akan berkembang
- Ahli komputer forensik dibutuhkan keahlian khusus, pengalaman dan jam terbang

Terima Kasih

TUGAS

- Jelaskan mengapa seorang ahli komputer forensik sangat dibutuhkan ?
- Hal apa saja yang dikerjakan seorang ahli komputer forensik ?
- Hal apa yang dibutuhkan untuk menjadi seorang ahli komputer forensik?
- Seorang ahli komputer forensik memiliki keahlian recover data, jelaskan ?
- Jelaskan, mengapa seorang ahli komputer foerensik harus memiliki keahlian dibidang hukum dan prosedur legal ?