



UNIVERSITAS GUNADARMA  
Fakultas Teknologi Industri  
Jurusan Teknik Informatika

# Pendahuluan Forensik TI

Pengantar Komputer Forensik Teknologi Informasi



# Pendahuluan

- Perkembangan Teknologi
  - Positif ; Memajuan dan kesejahteraan
  - Negatif ; Kemunduran dan kerugian
- Teknologi informasi dan komputer
  - Dalam perkembangannya telah membuka dimensi lain dari teknologi, yaitu kejahatan komputer
  - Istilah " Cybercrime "
- Cybercrime : memunculkan masalah baru



# Cybercrime

- Cybercrime : Kejahatan komputer
- Masalah baru
  - Mikro ; Perseorangan
  - Makro ; Komunal, publik dan efek domino
- Cybercrime perlu ditangani sebab ;
  - Sifat alami dari TI ; Memungkinkan pelaku kejahatan untuk menyembunyikan jejaknya
  - Cybercrime tidak memiliki batas goeografis
  - Dapat dilakukan secara jarak dekan atau jauh dan hasilnya sama



# Komputer Forensik

## ■ Forensik :

- Suatu proses ilmiah dalam mengumpulkan, menganalisa, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum.

## ■ Forensik Komputer:

- Suatu proses **mengidentifikasi, memelihara, menganalisa dan menggunakan bukti digital** menurut hukum yang berlaku (Moroni Parra, 2002). Istilah ini kemudian meluas menjadi ***Forensik Teknologi Informasi***



# Komputer Forensik ; Terminologi

- Komputer forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan – penyaringan dan dokumentasi bukti komputer dalam kejahatan komputer
- Melakukan penyelidikan dan analisis komputer untuk menentukan potensi bukti legal



# Komputer Forensik

- Mengumpulkan dan analisa data dari sumber daya komputer :
  - Sistem komputer
  - Jaringan komputer
  - Jalur komunikasi
  - Media penyimpanan
  - Aplikasi komputer
- Forensik komputer : mengabungkan keilmuan hukum dan komputer
- Forensik komputer = digital forensik<sub>6</sub>





# Data Elektronik ; Bukti Digital

- Data elektronik ;
  - Dokumen, informasi keuangan, e-mail, job schedule, log, transkripsi voice-mail
- Bukti digital
  - Informasi yang didapat dalam bentuk / format digital (Scientific Working Group on Digital Evidence, 1999), baik berupa bukti yang riil maupun abstrak ( perlu diolah terlebih dahulu sebelum menjadi bukti yang riil ),



# Kebutuhan Komputer Forensik

- Keperluan investigasi tindak kriminal dan pelanggaran perkara pelanggaran
- Rekonstruksi duduk perkara insiden keamanan komputer
- Upaya pemulihan akan kerusakan sistem
- Troubleshooting yang melibatkan hardware dan software
- Keperluan memahami sistem atau berbagai perangkat digital dengan lebih baik





# Definisi Komputer Forensik

- Penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk mengekstrak dan memelihara barang bukti tindakan kriminal
- Menurut Judd robin ; Penerapan secara sederhana dari penyelidikan komputer dan teknik analisisnya untuk menentukan bukti – bukti hukum yang mungkin



# Definisi Komputer Forensik

- Menurut New Technologies ;  
Komputer forensik berkaitan dengan pemeliharaan, identifikasi, ekstraksi dan dokumentasi dari bukti – bukti komputer yang tersimpan dalam wujud informasi magnetik



# Latar Belakang Komputer Forensik

- Bukti komputer dipersidang sudah ada sejak 40 tahun lalu
- Bukti komputer tersebut dalam persidangan diperlakukan serupa dengan bukti tradisional, menjadi ambigu
- Tahun 1976 US federal rules of evidence menyatakan permasalahan tersebut



# Contoh Hukum Berkaitan dengan kejahatan komputer

- Economic espionage act 1996
- The electronic communications privacy act 1986
- The computer security act 1987
- Undang-Undang No. 11 tahun 2008
- SK BI Nomor 27/164/KEP/DIR 31 maret 1995
- Undang-undang Nomor 8 Tahun 1999



# Spesifikasi Komputer Forensik

- Forensik Disk
- Forensik System
- Forensik Jaringan Komputer
- Forensik Internet





# Penerapan Komputer Forensik

## ■ Prinsip

- Harus ada prinsip yang menetapkan bahwa keahlian dan pengalaman lebih penting dari pada tools

## ■ Kebijakan

- Pertimbangkan kebijakan dalam melakukan investigasi komputer forensik

## ■ Prosedur dan metode

- Buat prosedur dan metode terhadap peralatan dan mendapatkan – mengumpulkan electronic evidence





# Bidang Keilmuan Forensik

- Forensik pathologi
- Forensik dentistry
- Forensik anthropology
- Forensik entomology
- Psikologi forensik
- Forensik kejiwaan
- Fingerprint analysis
- Forensik accounting
- Bloodstain pattern analysis
- Ballistics
- Forensik toxicology
- Forensik footwear evidence
- Questioned document examination
- Explosion analysis
- Forensik teknologi informasi
- Komputer forensik



# Kesimpulan

- Jika akan menyelesaikan suatu perkara “ misteri komputer “, maka lakukan pengujian sistem sebagai seorang detektif bukan sebagai seorang user.
- Kejahatan komputer memiliki sifat alamiah



# Kuis

- Jelaskan apa yang dimaksud dengan komputer forensik ?
- Jelaskan apa yang dimaksud dengan kejahatan komputer ?
- Mengapa kejahatan komputer perlu ditangani, jelaskan ?
- Jelaskan apa saja yang perlu diperhatikan dalam menerapkan komputer forensik ?
- Jelaskan mengapa dalam memecahkan kejahatan komputer harus sebagai seorang detektif ?



# Terima kasih

