PERTEMUAN I

Pendahuluan Forensik Teknologi informasi

Copyright © March 2025

Computer Forensics and Investigations as a Profession

Copyright © March 2025

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***

Copyright © March 2025

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

Copyright © March 2025

Komputer Forensik

- Mengumpulkan dan analisa data dari sumber daya computer:
  - Sistem komputer
  - Jaringan komputer
  - Jalur komunikasi
  - Media penyimpanan
  - Aplikasi komputer

- Forensik komputer : mengabungkan keilmuan hukum dan komputer
- Forensik komputer = digital forensik

Copyright © March 2025

Definisi lebih lanjut

- Computer forensic adalah serangkaian metodologi yang digunakan dalam melakukan akuisisi (imaging), pengumpulan, analisa, serta presentasi bukti digital.
- Bukti digital mencakup setiap informasi elektronik yang disimpan atau diolah menggunakan teknologi komputer sehingga dapat digunakan untuk mendukung atau menolak tentang bagaimana sebuah insiden atau tindakan pelanggaran hukum terjadi.
- Karena keterlibatan proses computer forensic adalah setelah terjadinya

Copyright © March 2025

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

Copyright © March 2025

Kebutuhan Komputer Forensik

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

Copyright © March 2025

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),

Copyright © March 2025

CONTOH BARANG BUKTI DIGITAL

1. E-mail, Alamat e-mail
2. File Wordprocessor / spreadsheet
3. Source code perangkat lunak
4. File berbentuk image (.jpeg,.tif, dan sebagainya)
5. Web Browser bookmarks , cookies.
6. Kalender, to-do list

Copyright © March 2025

Aturan Standar Bukti Digital

1. Dapat Diterima.
2. Asli.
3. Lengkap.
4. Dapat Dipercaya.

Copyright © March 2025

Sumber Bukti Digital

- File terhapus
- Registry Windows
- File spool printer
- File hibernasi
- File temporer
- File Swap
- Cache Browser
- Partisi alternatif atau tersembunyi
- Beragam media storagedisk (floppy,tape, flash disk, dll)

Copyright © March 2025

Empat elemen kunci forensik dalam teknologi komputer

- Identifikasi dari Bukti Digital
- Tahapan paling awal forensik dalam teknologi informasi. Tahapan ini melakukan identifikasi dimana bukti itu berada, disimpan, dan bagaimana penyimpanannya untuk mempermudah tahapan selanjutnya.
- Penyimpanan Bukti Digital
- Penyimpanan ini lebih menekankan bahwa bukti digital pada saat ditemukan akan tetap tidak berubah baik bentuk, isi, makna, dan sebagainya dalam jangka waktu yang lama. Ini adalah konsep ideal dalam dari penyimpanan bukti digital.
- Analisa Bukti Digital
- Pengambilan, pemrosesan, dan interpretasi dari bukti digital adalah bagian dari analisa bukti digital yang sangat penting.
- Presentasi Bukti Digital
- Tahapan penyajian bukti bukti yang telah didapatkan dengan cara atau
- istilah yang dapat dipahami oleh para pengacara, para staff dan
- management yang bukan orang teknis dan sesuai dengan kriteria alat
- bukti yang sah.

Copyright © March 2025

Metodologi Forensik Teknologi Informasi

- ***Search and Seizure***

  Investigator harus terjun langsung ke lapangan dalam kasus yang dihadapi.

- **Pencarian Informasi**

  Dalam pencarian informasi ada beberapa tahap yang harus dilakukan :

  - Menemukan lokasi tempat kejadian perkara
  - Menggali informasi dari aktifitas yang tercatat dalam log di komputer.
  - Penyitaan media penyimpanan data (*data storages*) yang dianggap mampu membantu penyelidikan.

Copyright © March 2025

Cabang komputer forensik

- Disk Forensik : Penganalisissan data / pencarian data yang ada di dalam sebuah disk.
- System Forensik : Penganalisissan data di dalam sebuah system komputer.
- Network Forensik : Penganalisissan data sebuah komputer dari jaringan yang ada pada komputer tersebut.
- Internet Forensik : Penganalisissan data sebuah komputer dgn Menggunakan media internet.

Copyright © March 2025

Network forensik

- Memeriksa port, service dan log pada router serta aplikasi yang berjalan pada jaringan komputer TKP.

Copyright © March 2025

Data recovery

- Memulihkan informasi komputer yang telah dihapus dengan sengaja atau tidak sengaja.

Copyright © March 2025

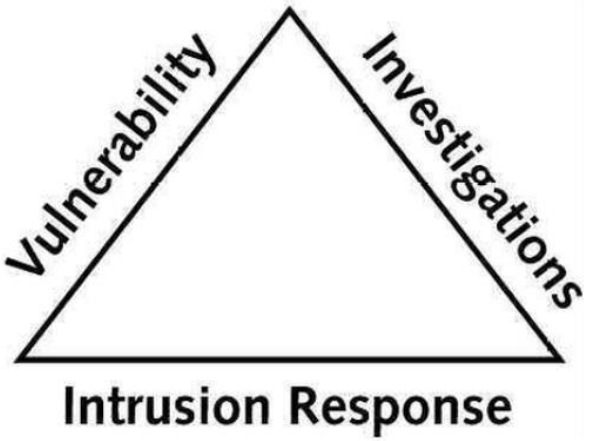
Disaster recovery

- Menggunakan teknik digital forensik untuk mengambil/mengembalikan informasi yang hilang pada komputer klien.

Copyright © March 2025

Tiga prilaku investigasi

- Menganalisa kerentanan dan manajemen resiko
- Deteksi serangan pada jaringan dan menanggapi serangan
- Komputer investigasi pada sistem



Copyright © March 2025

SELESAI

Copyright © March 2025

PERTEMUAN 2

Programmer dan ahli komputer forensik

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

Programmer vs Ahli Komputer Forensik

- Programmer ;
  - Bekerja melawan diri sendiri
  - Mencoba memperbaiki permasalahan yang kita buat sendiri

- Ahli Komputer Forensik
  - Bekerja menyelesaikan kejahatan komputer
  - Melawan seorang “programmer”

Copyright © March 2025

Keahlian Komputer Forensik dibutuhkan oleh :

- Jaksa Penuntut mempergunakan barang bukti komputer dalam kejahatan yang bermacam-macam, 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

Copyright © March 2025

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.

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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.
- 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

Copyright © March 2025

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.
- 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

Copyright © March 2025

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
- 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

Copyright © March 2025

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

Copyright © March 2025

Terima Kasih

Copyright © March 2025

PERTEMUAN 3

UU tentang Informasi dan Transaksi Elektronik (ITE)

Copyright © March 2025

Latar Belakang

- Pesatnya perkembangan dan kemajuan teknologi informasi, yang merupakan salah satu sebab perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah mempengaruhi lahirnya bentuk-bentuk perbuatan hukum baru.
- Penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara dan memperkokoh persatuan dan kesatuan nasional berdasarkan peraturan dan perundang2an demi kepentingan nasional.
- Pemanfaatan Teknologi Informasi berperan penting dalam perdagagngan dan pertumbuhan perekonomian nasional untuk memwujudkan kesejahteraan masyarakat.

Copyright © March 2025

Tujuan

- Berdasarkan latar belakang tadi, pemerintah perlu men-dukung pengembangan Teknologi Informasi melalui infra-struktur hukum dan pengaturannya, sehingga pemanfaat-an Teknologi Informasi dapat dilakukan secara aman, untuk mencegah penyalahgunaannya dengan memperha-tikan nilai-nilai agama dan sosial budaya masyarakat.
- Perkembangan tersebut telah melahirkan suatu hukum baru, yang dikenal dengan hukum siber atau telematika.
- Hukum siber (*cyber law*) secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan Teknologi Informasi dan Komunikasi (ICT=Information and Communication Technology)

Copyright © March 2025

Tanggung Jawab Pemerintah

- Secara Umum adalah mengamankan dan mensejahterakan rakyat (lihat pembukaan UUD NRI 45),
- UU KIP
  - Badan Publik wajib menyediakan, menerbitkan dan/atau menerbitkan informasi publik, berikut pembangunan sistem informasi dan dokumentasi untuk mengelola informasi publik secara baik dan efisien sehingga dapat diakses dengan mudah,
- UU ITE
  - Menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya,
- UU Perlindungan Konsumen
  - Menciptakan sistem perlindungan konsumen yang mengandung unsur kepastian hukum dan keterbukaan informasi serta akses untuk mendapatkan informasi.

Copyright © March 2025

Tanggung Jawab Penyelenggara

UU ITE Pasal 15 :

(1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.

(2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.

(3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

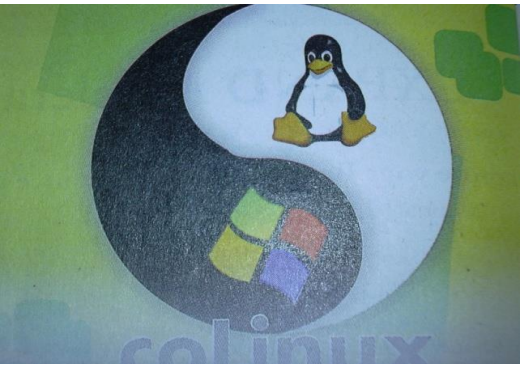
Copyright © March 2025

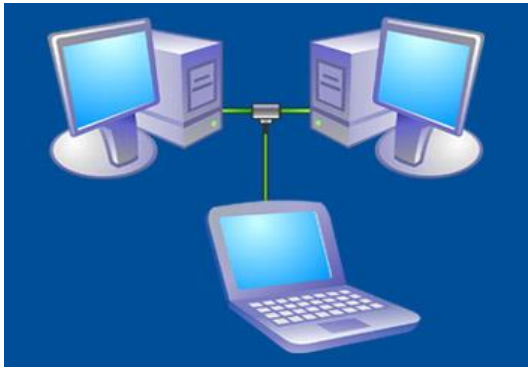
Peran Pemerintah dan Masyarakat

- Pemerintah memfasiliasi pemanfaatan Teknologi.
- Pemerintah melindungi kepentingan umum.
- Pemerintah menetapkan instansi yang memiliki data elektronik strategis untuk dilindungi.
- Masyarakat juga berperan dalam Teknologi Informasi.
- Peran masyarakat diselenggarakan lewat lembaga yang memiliki fungsi konsultasi dan mediasi.

Copyright © March 2025

Informasi Elektronik

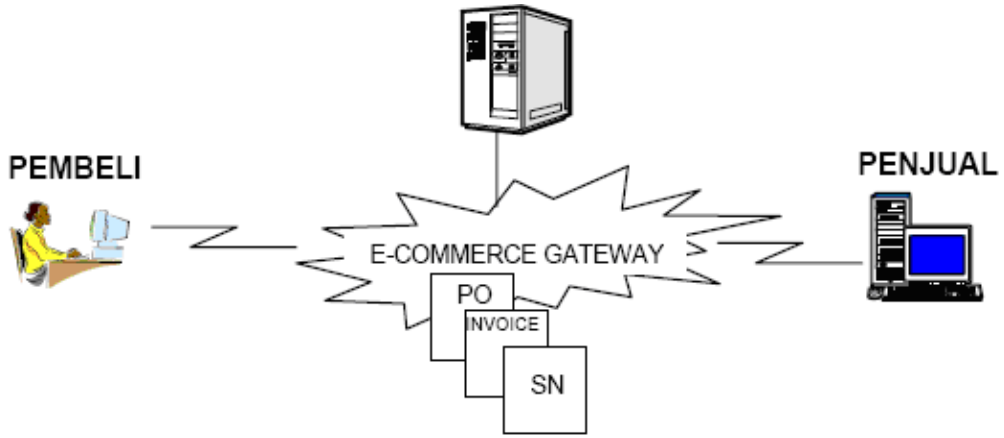




"Informasi elektronik adalah satu atau sekumpulan data elektronik termasuk tetapi tidak terbatas pada tulisan, suara atau gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya yang telah diolah sehingga mempunyai arti."

Copyright © March 2025

Transaksi Elektronik



"perbuatan hukum yang dilakukan dengan mengguna-kan komputer, jaringan komputer, atau media elek-tronik lainnya ".

Copyright © March 2025

Hak Kekayaan Intelektual

- Hak Cipta (Copyright) → ©
- Merek Dagang (Trade Mark) → ™
- Hak Paten (Registered) → ®
- Fair Use
- EULA (End User License Agreement)
- Freeware

Copyright © March 2025

Copyrigth ©

- Copyright © atau hak cipta dimaksudkan untuk melindungi karya cipta seseorang seumur hidup seniman atau pengarang. Hak cipta berakhir setelah 95 tahun.
- Karya cipta dapat berada dalam domain publik jika hak ciptanya telah berakhir/ kadaluwarsa.
- Karya cipta yang berada dalam domain publik, tidak berhak cipta dan dapat disalin dan disebarkan dengan bebas.
- Karya cipta yang diterbitkan sebelum 1 Januari 1978 tidak mempunyai hak cipta yang sah, dapat dianggap milik publik.

All rights reserved; no part of this publication may be reproduced or transmitted by any means, electronic, mechanical, photocopying or otherwise, without the prior permission of the publisher

First published in Great Britain in 2003
Bloomsbury Publishing Plc, 38 Soho Square, London W1D 3HB

Copyright © 2003 J.K. Rowling
Cover illustrations by Jason Cockcroft © 2003 Bloomsbury Publishing Plc

Harry Potter, names, characters and related indicia are copyright and trademark Warner Bros., 2000™

The moral right of the author has been asserted
A CIP catalogue record for this book is available from the British Library

ISBN 0 7475 5100 6

Typeset by Palimpsest Book Production Limited, Polmont, Stirlingshire

All paper used by Bloomsbury Publishing, including that in this book, is a natural, recyclable product made from wood grown in sustainable, well-managed forests. The manufacturing processes conform to the environmental regulations of the country of origin.

Printed in Great Britain by Clays Ltd, St Ives plc

First edition

www.bloomsbury.com/harrypotter

TradeMark ™

- TradeMark ™ atau Merek Dagang adalah nama atau simbol yang digunakan untuk mengidentifikasi sebuah produk.
- Perusahaan telah mengeluarkan banyak uang untuk membuat merek dagang mereka untuk pembuatan iklan supaya dikenal baik oleh masyarakat.

Copyright © March 2025

Registered ®

- Registered ® atau Hak Paten adalah sebuah merek dagang yang secara resmi dikenali dan didaftarkan di Badan Hukum.
- Badan Hukum di Amerika disebut US Patent and Trademark Office.

Copyright © March 2025

Hak Kekayaan Intelektual (lanjutan)

- Fair Use (Penggunaan Terbatas)

  Bagian-bagian dari karya berhak-cipta dapat direproduksi untuk kepentingan kritik, komentar, laporan berita, mengajar, ilmu pengetahuan atau riset tanpa melanggar hak cipta.

- EULA (End User Licence Agreement)

  Merupakan persetujuan yang sah antara manufaktur perangkat lunak dan pembeli yang menjelaskan tentang hak dan batasan.

- Freeware (Perangkat Lunak Gratis)

  Perangkat lunak berhak-cipta yang tidak menarik biaya penggunaan. Dapat disalin dan dibagi-bagikan, tetapi tidak boleh direvisi atau dijual ke pihak ketiga (third party).

Copyright © March 2025

Kejahatan Komputer (Cyber Crime)

- White Color Crime

  Kejahatan yang dilakukan oleh karyawan yang memiliki intelektual untuk mencuri identitas untuk menyamar menjadi seseorang supaya memperoleh akses ke rekening bank, atau untuk meminta jasa mahal atas nama mereka.

- Cybersquatting

  Pesaing/ orang membayar sejumlah kecil uang pendaftaran dan kemudian menawarkan untuk menjual kembali nama domain dengan sejumlah besar uang.

Copyright © March 2025

Kejahatan Komputer (Cyber Crime)

- Cyberstalking

  Penggunaan internet, email dan chatroom untuk mengganggu seseorang.

- Cybersmearing

  Penyebaran informasi yang disalah gunakan untuk merusak reputasi seseorang atau perusahaan.

- Pembajakan

  Mendapatkan musik gratis, video dan perangkat lunak tanpa membayar royalti kepada pengarang dan artis.

Copyright © March 2025

Kasus Prita Mulyasari

- Digugat pihak RS Omni Internasional Tangerang, karena telah melanggar UU RI No. 11 Tahun 2008 Pasal 27 ayat (3) tentang ITE : “Setiap orang dengan sengaja dan tanpa hak mendistri-busikan dan/ atau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik yang memiliki muatan peng-hinaan dan/ atau pencemaran nama baik”.
- UU RI No. 11 Tahun 2008 Pasal 45 ayat (1) tentang ITE : “Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3) atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Copyright © March 2025

Kasus Prita Mulyasari (lanjutan)

- Dibela dengan Pasal 310 KUHP ayat (1) Barang siapa sengaja menyerang kehormatan atau nama baik seseorang dengan menuduhkan sesuatu hal, yang maksudnya terang supaya hal itu diketahui umum, diancam karena pencemaran dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah, (2) Jika hal itu dilakukan dengan tulisan atau gambaran yang disiarkan, dipertunjukan atau ditempelkan di muka umum, maka diancam karena pencemaran dengan pidana paling lama satu tahun empat bulan atau pidana denda paling banyak empat ribu lima ratus rupiah, (3) Tidak merupakan pencermaran atau pencemaran tertulis, jika perbuatan jelas dilakukan demi kepentingan umum atau karena terpaksa untuk membela diri.

Copyright © March 2025

Kasus Prita Mulyasari (lanjutan)

- Prita Mulyasari sebenarnya dapat melakukan tuntutan berupa ganti rugi atas penanganan yang keliru dari RS Omni Internasional seperti yang ditegaskan dalam UU RI No. 8 Tahun 1999 Pasal 19 tentang Perlindungan Konsumen :

(1) Pelaku usaha bertanggung jawab memberikan ganti rugi atas kerusakan, dan/ atau kerugian konsumen akibat mengkonsumsi barang, dan/ atau jasa yang dihasilkan atau diperdagangkan.

Copyright © March 2025

Kasus Prita Mulyasari (lanjutan)

(2) Ganti rugi sebagaimana dimaksud pada ayat (1) dapat berupa pengembalian uang atau penggantian barang, dan/ atau jasa yang sejenis atau setara nilainya, atau perawatan kesehatan dan/ atau pemberian santunan yang sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

(3) Pemberian ganti rugi dilaksanakan dalam tenggang waktu 7 (tujuh) hari setelah tanggal transaksi.

(4) Pemberian ganti rugi sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak menghapuskan kemungkinan adanya tuntutan pidana berdasarkan pembuktian lebih lanjut mengenai adanya unsur kesalahan.

(5) Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku apabila pelaku usaha dapat membuktikan bahwa kesalahan tersebut merukan kesalahan konsumen.

Copyright © March 2025

TERIMA KASIH

Copyright © March 2025

PERTEMUAN 4

Keterkaitan Forensik TI dengan Hukum Indonesia.

Copyright © March 2025

FORENSIK TI DALAM HUKUM INDONESIA

PENGERTIAN / UNSUR HUKUM

Ada beberapa pendapat mengenai pengertian hukum, dari beberapa pengertian tersebut hukum itu meliputi **beberapa unsur** sbb :

1. Aturan tentang tingkah laku masyarakat;
2. Dibuat oleh yang berwajib / berwenang ;
3. Berisi perintah dan larangan;
4. Bersifat memaksa;
5. Terhadap pelanggaran ada sanksi yang tegas.

TUJUAN HUKUM adalah menjamin adanya kepastian hukum dalam masyarakat yang bersendikan keadilan.

Copyright © March 2025

KATEGORI HUKUM

Hukum menurut isinya :

- **Hukum Privat (Hukum Sipil),** hukum yang mengatur hubungan / kepentingan antar perseorangan. Contoh ; Hukum Perdata, Hukum Dagang.
- **Hukum Publik (Hukum Negara),** hukum yang mengatur hubungan antara Negara dengan alat perlengkapan negara atau perseorangan (warga-negara). Contoh ; Hukum Pidana, Hukum Tata Negara.

Hukum menurut cara mempertahankannya :

- **Hukum Material**, hukum yang berisi peraturan berupa perintah dan larangan. Contoh ; Hukum Pidana (KUHPidana), Hukum Perdata (KUHPerdata).
- **Hukum Formal (Hukum Proses atau Hukum Acara),** hukum yang memuat peraturan tentang cara melaksanakan dan mempertahankan Hukum Material, yaitu cara-cara mengajukan suatu perkara ke Pengadilan hingga Putusan Hakim. Contoh ; Hukum Acara Pidana (KUHAPidana), Hukum Acara Perdata (KUHAPerdata).

- **Forensik TI dikategorikan sebagai bagian dari Hukum Acara Pidana**, karena memuat tentang cara-cara/ prosedur pembuktian terjadinya suatu pelanggaran / kejahatan di bidang TI agar dapat diajukan ke Pengadilan untuk mendapatkan Putusan Hakim.

Copyright © March 2025

Kebijakan penanggulangan kejahatan (cybercrime) dengan Hukum Pidana perlu memperhatikan hal-hal sbb : (Mas Wigrantoro Roes Setiyadi, 2000)

1. **Materi / substansi** :
   Apa saja yang dapat dinamakan sebagai tindak pidana di bidang TI.

2. **Kebijakan Formulasi**
   Apakah peraturan hukuman pidana bagi kejahatan bidang TI akan berada di dalam atau di luar KUHP.

Kebijakan Hukum Pidana :

Kriminalisasi :

Suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana) (Barda Nawawi Arief, 2003)

Copyright © March 2025

Asas Legalitas (*Principle of Legality*) :
Asas yang menentukan bahwa tidak ada perbuatan yang dilarang dan diancam dengan pidana jika tidak ditentukan terlebih dahulu dalam perundang-undangan (Moeljatno, 2000)

Asas berlakunya hukum pidana menurut tempat (Pasal 2 – 9 KUHP) :

a. **Asas Teritorial**
   UU Hukum Pidana Indonesia berlaku terhadap setiap orang yang melakukan pelanggaran / kejahatan di dalam wilayah RI.
b. **Asas Nasional Aktif**
   UU Hukum Pidana Indonesia berlaku juga bagi warga negara Indonesia yang berada di luar negeri.
c. **Asas Nasional Pasif**
   UU Hukum Pidana Indonesia berlaku bagi WNI maupun WNA diluar RI. Disini kepentingan hukum suatu negara yang dilanggar, misal : pemalsuan uang Indonesia, materai, cap negara dll
d. **Asas Universal**
   UU Hukum Pidana Indonesia dapat juga diberlakukan thd perbuatan jahat yang bersifat merugikan keselamatan internasional

Copyright © March 2025

Kebijakan Formulasi terhadap tindak pidana mayantara :

1. **Kejahatan biasa diatur dalam KUHP**
   Jika tindak pidana mayantara merupakan kejahatan biasa (ordinary crime) yang dilakukan dengan komputer teknologi tinggi (high-tech), penanggulangannya cukup dengan KUHP, baik melalui amandemen KUHP maupun perubahan KUHP secara menyeluruh.

2. **Kejahatan baru diatur dalam UU Khusus**
   Jika tindak pidana mayantara dianggap sebagai kejahatan kategori baru (new category of crime) yang membutuhkan suatu kerangka hukum yang baru dan komprehensif untuk mengatasi sifat khusus teknologi yang sedang berkembang dan tantangan baru yang tidak ada pada kejahatan perlu diatur secara tersendiri di luar KUHP.

Copyright © March 2025

Peraturan mengenai Cybercrime / Kejahatan mayantara diIndonesia

1.KONSEP KUHP YANG BARU (RUU KUHP **)**

a.Buku I (Ketentuan Umum)

Pasal 174 :

"**Barang** adalah benda berwujud termasuk air dan uang giral, dan benda tidak berwujud termasuk listrik, gas, data dan program komputer, jasa, jasa telepon, jasa telekomunikasi, atau jasa komputer."

Pasal 178 :

"**Anak kunci** adalah alat yang digunakan untuk membuka kunci,termasuk kode rahasia, kunci masuk komputer, kartu magnetik, atau signal yang telah diprogram yang dapat digunakan untuk membuka sesuatu oleh orang yang diberi hak untuk itu."

Pasal 188 :

"**Surat** adalah selain surat yang tertulis di atas kertas, juga surat atau Data yang tertulis atau tersimpan dalam disket, pita magnetik, atau

media penyimpanan komputer atau media penyimpanan data elektronik lain."

Copyright © March 2025

Pasal 189 :
"**Ruang** adalah bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu."
Pasal 190 :
"**Masuk** adalah termasuk mengakses komputer atau masuk ke dalam sistem komputer."
Pasal 191 :
"**Jaringan Telepon** adalah termasuk jaringan komputer atau sistem komunikasi komputer."

b. Buku II Konsep KUHP

Pasal 263 : menyadap pembicaraan di ruangan tertutup dengan alat bantu teknis
Pasal 264 :memasang alat bantu teknis untuk tujuan mendengar/ merekam pembicaraan
Pasal 266 : merekam gambar dengan alat bantu teknis di ruangan tidak untuk umum
Pasal 546 : Merusak/ membuat tidak dapat dipakai bangunan untuk sarana/ prasarana pelayanan umum (a.l. bangunan telekomunikasi/ komunikasi lewat satelit/ komunikasi jara jauh)
Pasal 641-642 : Pencucian uang

Copyright © March 2025

2. UU KHUSUS CYBERCRIME / KEJAHATAN MAYANTARA

a. **RUU TIPITI** (Tindak Pidana Di Bidang Teknologi Informasi)

Hal- hal yang merupakan **Pelanggaran** dalam Undang-Undang ini (Bab V):

1. MemanfaatkanTeknologi Informasi dengan melawan hukum.
2. Melakukan intersepsi dengan melawan hukum.
3. Sengaja dan melawan hukum merusak atau mengganggu data yang tersimpan dalam alat penyimpan data elektronik yang tersusun sebagai bagian dari sistem komputer.
4. Sengaja menghilangkan bukti–bukti elektronik yang dapat dijadikan alat bukti sah di pengadilan yang terdapat pada suatu sistem informasi atau sistem komputer.
5. Sengaja merusak atau mengganggu sistem informasi, sistem komputer, jaringan komputer, dan Internet.
6. Memanfaatkan Tteknologi Informasi untuk menipu, menghasut, memfitnah, menjatuhkan nama baik seseorang atau organisasi.
7. Memanfaatkan Teknologi Informasi untuk menyebarkan gambar, tulisan atau kombinasi dari keduanya yang mengandung sifat – sifat pornografi.
8. Memanfaatkan Teknologi Informasi untuk membantu terjadinya percobaan, atau persekongkolan yang menjurus pada kejahatan.
9. Setiap badan hukum penyelenggara jasa akses Internet atau penyelenggara layanan Teknologi Informasi, baik untuk keperluan komersial maupun keperluan internal perusahaan, dengan sengaja tidak menyimpan atau tidak dapat menyediakan catatantransaksi elektronik sedikitnya untuk jangka waktu 2 tahun.

Copyright © March 2025

2. UU KHUSUS CYBERCRIME / KEJAHATAN MAYANTARA

a. RUU TIPITI (Tindak Pidana Di Bidang Teknologi Informasi)

- **Pelanggaran Pemanfaatan Teknologi Informasi** (Bab VI)

Pasal 9 : Kejahatan terhadap nyawa dan keselamatan negara
Pasal 10 : Pencurian
Pasal 11 : Mengakses tanpa hak
Pasal 12 : Mengakses tanpa hak terhadap sistem informasi strategis
Pasal 13 : Pemalsuan identitas
Pasal 14 : Mengubah dan memalsukan data
Pasal 15 : Mengubah data yang merugikan orang lain
Pasal 16 : Perbuatan asusila
Pasal 17 : Pornografi anak - anak
Pasal 18 : Bantuan kejahatan
Pasal 19 : Mengakses tanpa hak terhadap komputer yang dilindungi
Pasal 20 : Teror

Copyright © March 2025

a. RUU TIPITI (Tindak Pidana Di Bidang Teknologi Informasi)

- **Tindak Pidana Yang Berkaitan Dengan Teknologi Informasi Sebagai Sasarannya** (Bab VII) :

  Pasal 21 : Intersepsi
  Pasal 22 : Merusak Situs Internet
  Pasal 23 : Penyadapan Terhadap Jaringan Komunikasi Data
  Pasal 24 : Pemalsuan Nomor Internet Protocol
  Pasal 25 : Merusak Database atau Enkripsi
  Pasal 26 : Penggunaan Nama Domain Tidak Sah
  Pasal 27 : Penyalah-gunaan Surat Elektronik
  Pasal 28 : Pelanggaran Hak Cipta.
  Pasal 29 : Pelanggaran Hak Privasi

Copyright © March 2025

b. UU ITE (Informasi dan Transaksi Elektronik) No. 11 Th. 2008

Bab I	Ketentuan Umum
Bab II	Asas dan Tujuan
Bab III	Informasi, Dokumen dan Tanda Tangan Elektronik
Bab IV	Penyelenggaraan Sertifikasi Elektronik dan Sistem Elekronik
Bab V	Transaksi Elektronik
Bab VI	Nama Domain, Hak Kekayaan Intelektual dan Perlindungan Hak Pribadi
Bab VII	Perbuatan yang Dilarang
Bab VIII	Penyelesaian Sengketa
Bab IX	Peran Pemerintah dan Peran Masyarakat
Bab X	Penyidikan
Bab XI	Ketentuan Pidana
Bab XII	Ketentuan Peralihan
Bab XIII	Ketentuan Penutup

Copyright © March 2025

PERATURAN INTERNASIONAL MENGENAI CYBER LAW :

1. **Konvensi tentang Kejahatan Cyber (Convention on Cyber Crime)**

   oleh Uni Eropa (Council of Europe) di Budapest, Hongaria pada tgl 23 November 2001 mengatur tentang delik mayantara sbb: (Mardjono Reksodiputro, 2002:3-4)

   a. Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer termasuk didalamnya: mengakses sistem komputer tanpa hak, tanpa hak menangkap/mendengar pengiriman dan pemancaran, tanpa hak merusak data, tanpa hak mengganggu sistem, menyalahgunakan perlengkapan.
   b. Delik-delik yang berhubungan dengan komputer (pemalsuan dan penipuan dengan komputer)
   c. Delik-delik yang bemuatan pornografi anak
   d. Delik-delik yang berhubungan dengan hak cipta.

Copyright © March 2025

PERATURAN INTERNASIONAL MENGENAI CYBER LAW :

2. **Komisi Franken** tahun 1987 dan Kaspersen dari Belanda merumuskan sembilan bentuk penyalahgunaan komputer :
   a. Tanpa hak memasuki sistem komputer
   b. Tanpa hak mengambil data komputer
   c. tanpa hak mengetahui
   d. tanpa hak menyelin
   e. tanpa hak mengubah
   f. mengambil data
   g. tanpa hak mempergunakan peralatan
   h. sabotase sistem komputer
   i. mengganggu telekomunikasi.

3. **Resolusi PBB No, 55 / 63**
   Berisi tentang memerangi tindakan kriminal penyalah-gunaaan TI

4. **APEC** (Asia Pasific Economy Cooperation) **Cybercrime Strategy**

Copyright © March 2025

BEBERAPA CONTOH CYBERLAW

MALAYSIA :

- Computer Crime Act (Akta Kejahatan Komputer) 1997
- Communication and Multimedia Act (Akta Komunikasi dan Multimedia) 1998
- Digital Signature Act (Akta Tandatangan Digital) 1997

SINGAPORE :

- The Electronic Act (Akta Elektronik) 1998
- Electronic Communication Privacy Ac t (Akta Privasi Komunikasi Elektronik) 1996

AMERIKA :

- US Child Online Protection Act (COPA) : Adult verification required on porn sites.
- US Child Pornography Protection Act : Extend law to include computer — generated child porn.
- US Child Internet Protection Act (CIPA) : Requires Schools & Libraries to filter
- US New Laws and Rulemaking : Spam, Deceptive Marketing Tactics, Mouse trapping

Copyright © March 2025

Terima Kasih

Copyright © March 2025

PERTEMUAN 5

Metode Komputer Forensik Dan Tip Komputer Forensik

Copyright © March 2025

Pemodelan Forensik

- Model forensik melibatkan tiga komponen :
  - Manusia [People]
  - Peralatan [Equipment]
  - Aturan [Protocol]

Copyright © March 2025

Manusia

- Manusia berhubungan dengan brainware
- Kriteria :
  - Computer forensic examiner
  - Computer investigator
  - Digital evidence collection specialist

Copyright © March 2025

Computer Forensic Examiner

- Melakukan pengujian terhadap media original
- Mengekstrak data bagi investigator untuk di review
- Dibutuhkan 4 sampai 6 minggu pelatihan

Copyright © March 2025

Computer Investigator

- Harus memiliki pengalaman ayng sudah teruji dan ahli
- Memahami jaringan komputer, internet, komunikasi dan teknologi komputer dan informasi
- Dibutuhkan sampai 2 minggu pelatihan

Copyright © March 2025

Digital evidence collection specialist

- Sebagai fist responder
- Mendapatkan dan menghadirkan bukti komputer mencakup media penyimpanan
- Dibutuhkan 2 sampai 3 hari pelatihan

Copyright © March 2025

Peralatan

- Dibutuhkan peralatan guna mendapatkan bukti – bukti (evidence) yang berkualitas dan bersih
- Jenis peralatan :
  - Perangkat lunak
  - Perangkat keras
  - Media penyimpanan

Copyright © March 2025

Aturan

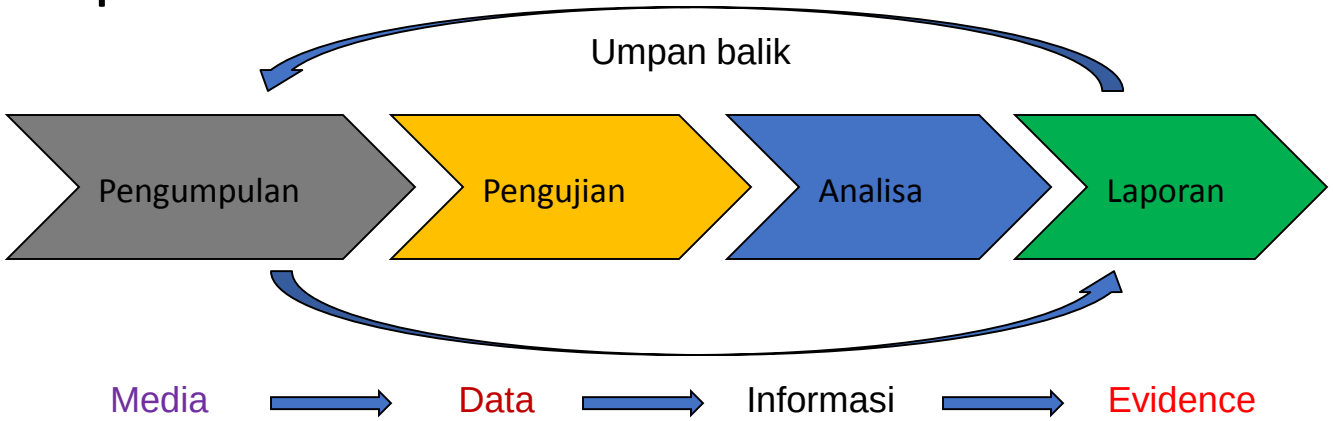
- Merupakan hal yang terpenting
- Aturan :
  - Aturan dalam mengali
  - Aturan mendapatkan
  - Aturan menganalisa
  - Aturan penyajian laporan
- Pemahaman hukum dan etika

Copyright © March 2025

Tahap Komputer Forensik

- Pengumpulan
- Pengujian
- Analisa
- Laporan

Jangan lupa umpan balik



Copyright © March 2025

Pengumpulan Data

- Mengidentifikasi sumber – sumber potensial dan bagaimana kemudian data dikumpulkan
- Data bertumpu pada
  - Personal computer
  - Mobile computer
  - Jaringan komputer
  - Media penyimpanan
  - Integrasi penyimpanan

Copyright © March 2025

Pengumpulan Data

- Pengumpulan data mencakup
  - Identifikasi
  - Penamaan
  - Perekaman
  - Mendapatkan data

Copyright © March 2025

Langkah yang dibutuhkan

- Membuat perencanaan untuk mendapatkan data
  - Kemiripan nilai
  - Volatility (Volatile)
  - Upaya dalam mendapatkan data
- Mendapatkan data
- Analisa integritas data

Copyright © March 2025

Pengujian

- Melakukan pengujian, menilai dan mengekstrak kepingan informasi yang relevan dari data – data yang dikumpulkan
- Tahap ini melibatkan :
  - Bypassing fitur – fitur sistem
  - Filtrasi (eliminasi data)
  - Meng-exclude file
  - Mengalokasi file
  - Mengekstrak file

Copyright © March 2025

Analisa

- Melakukan analisa untuk merusmuskan kesimpulan dalam menggambarkan informasi
- Cakupan analisa :
  - Identifikasi user di luar pengguna
  - Identifikasi lokasi
  - Identifikasi barang
  - Identifikasi kejadian
  - Menentukan bagaimana komponen terelasi satu dengan lainnya

Copyright © March 2025

Dokumentasi dan Laporan

- Merepresentasikan informasi yang merupakan hasil dari proses analisis
- Faktor yang mempengaruhi reporting
  - Alternative explanation (penjelasan alternatif)
  - Audience consideration (pertimbangan peserta)
  - Actionable information

Copyright © March 2025

Tip Pemberlakuan Forensik

1. Konsisten menjadi suatu keharusan dalam setiap proses forensik
2. Tahapan forensik mungkin tidak seluruhnya mendapatkan effort yang sama
3. Analisa memperhatikan berbagai sumber daya potensial
4. Examiner harus memiliki kejelian dalam mengalokasi sebaran data yang mungkin
5. Examiner harus mempertimbangkan setiap alternatif yang reliable

Copyright © March 2025

Tip Pemberlakuan Forensik

6. Dibutuhkan tindakan proaktif dalam mengumpulkan data – data yang berharga
7. Examiner harus menghadirkan data melalui standar yang sudah didefinisikan
8. Pertimbangkan setiap tahapan
9. Keputusan harus dibut mencakup kebutuhan dalam mengunmpulkan data dan menangani bukti dengan serangkaian cara tertentu
10. Examiner harus menggunakan pendekatan yang ilmiah dalam mempelajari data

Copyright © March 2025

Tip Pemberlakuan Forensik

11. Buat detail, langkah mendapatkan dan dokumentasi jika bukti dibutuhkan dalam hukum dan persidangan
12. Examiner harus melaklukan review kembali proses yang sudah dilaksanakan dan dapat dipertanggungjawabkan

Copyright © March 2025

Tip Umum

- Tip umum dalam menangani dan menganalisa bukti untuk menjaga keutuhan dan kelayakan data
  1. Jangan terlebih dahulu menyalakan komputer untuk alasan apapun
  2. Hubungi agen yang bersangkutan untuk menganalisa
  3. Lekatkan – tandai evidence tape
  4. Miliki surat izin untuk melakukan analisa terhadap komputer dan data

Copyright © March 2025

Tip Umum

5. Pernyataan tertulis yang sah atau ringkasan kasus untuk melegalkan examiner untuk bekerja
6. Buat daftar kata – kata untuk melakukan pencarian
7. Lupakan kata “tepat waktu” dalam komputer forensik
8. Konsisten terhadap kasus dn identifikasi kepentingan
9. Orang – orang yang menggunakan komputer alokasi ke ruang komputer untuk dilakukan indikasi

Copyright © March 2025

Tip Umum

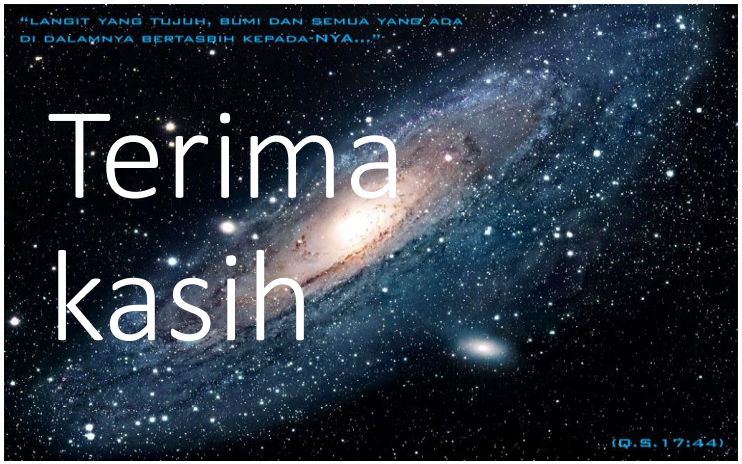
10. Indikasi apakah komputer terintegrasi dengan jaringan atau tidak
11. Indikasikan apakah terdapat encryption atau password protection
12. Indikasikan skill komputer user yang komputernya diambil untuk komputer forensik
13. Secara umum hanya komputer dan media penyimpan untuk keperluan forensik

Copyright © March 2025

Tip Bagi Pemula

- Investigasi sederhana
- Hubungi pihak yang berwenang
- Amankan lokasi
- Minumlisasi interupsi terhadap lokasi
- Jangan jalankan program apapun
- Jangan biarkan user menggunakan komputer
- Kumpulkan dan dokumentasikan sumber data lainnya
- Amankan barang yang berhubungan dengan bukti
- Mulailah dokumentasi chain of custody

Copyright © March 2025



Copyright © March 2025

PERTEMUAN 6

Standar Metodologi Komputer Forensik

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

Cakupan Standar Metodologi

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

Copyright © March 2025

Lima faktor

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

Kemampuan penyelidik

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

Copyright © March 2025

Kebijakan dan Prosedur

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

Copyright © March 2025

Pertimbangan administratif

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

Copyright © March 2025

PERTEMUAN 11

PENANGANAN INSIDEN FORENSIK DAN FREEZING THE SCENE

Copyright © March 2025

PRA INSIDEN

- Jenis insiden menurut the information security management :
  - Virus
  - Unauthorized access
  - Pencurian atau kehilangan kepercayaan pada informasi
  - Serangan denial of service pada sistem
  - Korupsi informasi

Copyright © March 2025

PERSIAPAN

- Pengunaan beberapa tool untuk mencegah penyusupan dengan deteksi
- Backup sistem
- Kebijakan password
- Kebijakan keamanan sistem
- Lakukan instalasi patch security
- Pergunakan security– auditing tools
- Pelajari sistem lebih lama
- Aktifkan fasilitas logging dan accounting
- Lakukan audit dan pengujian pada sistem secara rutin

Copyright © March 2025

PROSEDUR PENANGANAN INSIDEN

- Bagaimana mengamankan dan menjaga barang bukti
- Dimana dan bagaimana mencari barang bukti
- Daftar yang dipersiapkan untuk laporan menyeluruh
- Daftar orang untuk keperluan pelaporan
- Daftar software yang digunakan
- Daftar ahli

Copyright © March 2025

PROSEDUR PENANGANAN INSIDEN SECARA SEDERHANA

- Menurut Scott Grace " Computer incident response and computer forensics overview" :
  - Amankan lingkungan
  - Shutting down komputer
  - Label barang bukti
  - Dokumentasikan barang bukti
  - Transportasikan barang bukti
  - Dokumentasikan rangkaian penyimpanan

Copyright © March 2025

PROSEDUR PENANGANAN INSIDEN

- Jika ahli forensik tidak dimiliki atau tidak berada ditempat dan terdapat insiden, yang harus dilakukan oleh seorang staff :
  - Membuat image
  - Analisis forensik dilakukan semua dari copy
  - Memelihara rincian media dalam proses

Copyright © March 2025

FASE MERESPON INSIDEN

- Fase 1 : Persipan
- Fase 2 : Identifikasi
- Fase 3 : Pengisian Fase
- Fase 4 : Pembasmian Fase
- Fase 5 : Pemulihan Fase
- Fase 6 : Tindak lanjut

Copyright © March 2025

EMERGENCY ACTION CARD

1. Tetap tenang sehingga terhindari kesalahan fatal
2. Buatlah catatan yang baik dan relevan
3. Beritahu orang yang tepat dan carilah pertolongan
4. Tetapkan kebijakan orang – orang terpercaya yang boleh tahu
5. Gunakan jalur komunikasi terpisah dari sistem yang mengalami compromise

Copyright © March 2025

EMERGENCY ACTION CARD

6. Isolasi maslah sehingga tidak bertambah buruk
7. Buat backup sistem
8. Temukan sumber masalah
9. Kembali ke pekerjaan semula setelah backup terjamin dan lakukan restore sistem
10. Belajar dari pengalaman

Copyright © March 2025

PEMROSESAN BARANG BUKTI

- Menurut Lori Willer “ Computer forensics”, panduan :
  1. Shut down komputer, dan perlu dipertimbangkan keruksakan proses yang berjalan dibackground
  2. Dokumentasikan konfigurasi hardware dari sistem
  3. Pindahkan sistem komputer ke lokasi yang aman
  4. Buat backup bit dari hard disk dan floppy

Copyright © March 2025

PANDUAN

5. Uji otentifikasi data dari semua penyimpanan
6. Dokumentasikan tanggal dan waktu yang berhubungan dengan file komputer
7. Buat daftar key word pencarian
8. Evaluasi swap file
9. Evaluasi file slack, dari dump memori yang terjadi selama file ditutup
10. Evaluasi unallocated space – erased file

Copyright © March 2025

PANDUAN

11. Pencarian keyword pada file, file slack dn unallocated space
12. Dokumentasikan nama file (atribut tanggal dan file)
13. Identifikasikan anomali file, program dan storage
14. Evaluasi fungsionalitas program untuk mengetahui kegunaannya
15. Dokumentasikan temuan dan software yang dipergunakan
16. Buat copy dari software yang dipergunakan

Copyright © March 2025

TAHAPAN PEMROSESAN BARANG BUKTI

- Menurut Jim Mc Millan, lima tahapam pemrosesan barang bukti :
  - Persiapan
  - Snapshot
  - Transport
  - Pengujian
  - Analisa

Copyright © March 2025

PERSIAPAN

- Sterilkan semua media dari virus
- Pastikan semua tool forensik bisa dipergunakan secara resmi
- Periksa kerja semua peralatan lab
- Pilih ahli forensik yang tepat dan mampu memberikan kesaksian dan penjelasan di persidangan

Copyright © March 2025

SNAPSHOT

- Foto lingkungan
- Catat rinciannya
- Foto barang bukti
- Dokumentasikan konfigurasi hardware
- Labeli barang bukti sesuai metodologi
- Foto barang bukti lagi setelah dilabeli
- Dokumentasikan apa terjadi

Copyright © March 2025

TRANSPORT

- Lakukan pengemasan secara aman
- Foto dan dokumentasikan penanganan barang bukti meninggalkan tempat kejadian sampai ke lab pengujian

Copyright © March 2025

PENGUJIAN

- Lakukan unpack sesuai metodologi
- Lakukan uji visual dan catat setiap konfigurasi yang tidak semestinya
- Buatlah image hard disk
- Setelah menbuat image simpan barang bukti di tempat aman dan catat
- Lakukan pembuat image kedua

Copyright © March 2025

ANALISA

- Analisa barang bukti dilakukan secara dua level :
  - Level fisik
  - Level logic
- Perhitungan rangkaian kepercayaan – chain of evidence

Copyright © March 2025

RANGKAIAN KEPERCAYAAN

- Shell
- Command
- Dynamic libraries
- Device driver
- Kernel
- Controller
- Hardware

Copyright © March 2025

FREEZING THE SCENE

Mengumpulkan bukti-bukti dengan mengamankan lokasi dari setiap aktifitas yang dapat merusak atau menghilangkan barang bukti

Copyright © March 2025

FREEZING THE SCENE

Menurut Judd Robbins dari “An Explanation of Computer Forensics” mensyaratkan hal berikut:

-Barang bukti tidak rusak atau terpengaruh oleh prosedur yang dipergunakan untuk penyelidikan.

-Tidak terinfeksi virus komputer selama proses analisis.

-Bukti-bukti yang relevan dan ekstraksinya, ditangani dan dilindungi dari kerusakan mekanis atau elektromekanis lebih jauh.

-Penerapan pemeliharaan

-Membatasi dampak pada operasi bisnis

-Semua informasi client yang diperoleh selama eksplorasi forensik dihargai secara etis dan tidak diumumkan

Copyright © March 2025

SELESAI

Copyright © March 2025

PERTEMUAN 10

Hukum Pembuktian Kejahatan Teknologi Informasi

Copyright © March 2025

HUKUM PEMBUKTIAN KEJAHATAN TEKNOLOGI INFORMASI

- **HUKUM PEMBUKTIAN** :
  - Merupakan sebagian dari hukum acara pidana yang mengatur **macam-macam alat bukti yang sah** menurut hukum, **sistem yang dianut** dalam pembuktian, **syarat-syarat** dan **tata cara mengajukan bukti** tersebut serta kewenangan hakim untuk menerima, menolak dan menilai suatu pembuktian
- **SUMBER HUKUM PEMBUKTIAN :**

1. Undang-undang (UU No. 8 Tahun 1981 ttg Hukum Acara Pidana/ KUHAP)
2. Doktrin atau ajaran
3. Jurisprudensi

Copyright © March 2025

HUKUM PEMBUKTIAN KEJAHATAN TEKNOLOGI INFORMASI

- **Alat Bukti**
  - Segala seuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut, dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan oleh terdakwa.
- **Sistem Pembuktian**
  - Pengaturan tentang macam-macam alat bukti yang boleh dipergunakan, penguraian alat bukti dan dengan cara-cara bagaimana alat bukti tersebut dipergunakan dan dengan cara bagaimana hakim harus membentuk keyakinannya

Copyright © March 2025

TUJUAN DAN GUNA PEMBUKTIAN

- **Bagi Penuntut Umum**,
  - Pembuktian adalah merupakan usaha untuk meyakinkan hakim yakni berdasarkan alat bukti yang ada, agar **menyatakan seorang terdakwa bersalah** sesuai dengan surat atau catatan dakwaan.
- **Bagi Terdakwa atau Penasehat Hukum**,
  - Pembuktian merupakan usaha sebaliknya, untuk meyakinkan hakim, yakni berdasarkan alat bukti yang ada, agar **menyatakan terdakwa dibebaskan** atau dilepaskan dari tuntutan hukum atau meringankan pidananya. Untuk itu terdakwa atau penasehat hukum jika mungkin harus mengajukan alat-alat bukti yang menguntungkan atau meringankan pihaknya. Biasanya bukti tersebut di sebut bukti kebalikan.
- **Bagi Hakim**
  - Atas dasar pembuktian tersebut yakni dengan adanya alat-alat bukti yang ada dalam persidangan baik yang berasal dari Penuntut Umum atau Penasehat Hukum/ Terdakwa dibuat **dasar untuk membuat keputusan**

Copyright © March 2025

ALAT BUKTI

- Pada dasarnya seluruh kegiatan dalam proses hukum penyelesaian perkara pidana, sejak penyidikan sampai putusan adalah berupa kegiatan yang berhubungan dengan **pembuktian** atau kegiatan **untuk membuktikan**.
- Mencari bukti sesungguhnya adalah mencari alat bukti. Bukti yang terdapat pada alat bukti itu kemudian dinilai oleh pejabat penyelidik untuk menarik kesimpulan, apakah bukti yang ada itu menggambarkan suatu peristiwa yang diduga tindak pidana ataukah tidak
- **ALAT BUKTI** menurut **UU INFORMASI DAN TRANSAKSI ELEKTRONIK** :
- Pasal 5 (1) dan (2) UU ITE :
  - **Informasi Elektronik** dan/atau **Dokumen Elektronik** dan/atau **hasil cetaknya** merupakan **alat bukti hukum yang sah**.
- PasaL 44 UU ITE :
  - **Alat bukti penyidikan, penuntutan dan pemeriksaan** di pengadilan adalah sbb :
    - Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dana
    - Alat bukti lain berupa **Informasi Elektronik** dan/atau **Dokumen Elektronik**.

Copyright © March 2025

SUMBER BUKTI DIGITAL

- Selain deskripsi undang-undang ITE tersebut, dikenal pula alat bukti digital. Atribut-atribut khas serta identitas dalam sebuah proses kejahatan dalam dunia komputer dan internet inilah yang disebut dengan bukti-bukti digital.

- Tiga kategori besar **SUMBER BUKTI DIGITAL**, yaitu :
  - **Open Computer Systems**
  - **Communication Systems**
  - **Embedded Computer Systems**

Copyright © March 2025

Open Computer Systems

- Perangkat-perangkat yang masuk dalam kategori jenis ini adalah apa yang kebanyakan orang pikir sebagai **perangkat komputer**. Sistem yang memiliki media penyimpanan, keyboard, monitor, dan pernak-pernik yang biasanya ada di dalam komputer masuk dalam kategori ini. Seperti misalnya laptop, desktop, server, dan perangkat-perangkat sejenis lain.
- Perangkat yang memiliki sistem media penyimpanan yang kian membesar dari waktu ke waktu ini merupakan sumber yang kaya akan bukti-bukti digital. Sebuah file yang sederhana saja pada sistem ini dapat mengandung informasi yang cukup banyak dan berguna bagi proses investigasi. Contohnya detail seperti kapan file tersebut dibuat, siapa pembuatnya, seberapa sering file tersebut di akses, dan informasi lainnya semua merupakan informasi penting.

Copyright © March 2025

Communication Systems

- **Sistem telepon tradisional**, **komunikasi wireless**, **Internet**, **jaringan komunikasi data**, merupakan salah satu sumber bukti digital yang masuk dalam kategori ini. Sebagai contoh, jaringan Internet membawa pesan-pesan dari seluruh dunia melalui e-mail. Kapan waktu pengiriman e-mail ini, siapa yang mengirimnya, melalui mana si pengirim mengirim, apa isi dari e-mail tersebut merupakan bukti digital yang amat sangat penting dalam investigasi.

Copyright © March 2025

Embedded Computer Systems

- Perangkat telepon bergerak (**ponsel**), personal digital assistant (**PDA**), **smart card**, dan perangkat-perangkat lain yang tidak dapat disebut komputer tapi memiliki sistem komputer dalam bekerjanya dapat digolongkan dalam kategori ini. Hal ini dikarenakan bukti-bukti digital juga dapat tersimpan di sini. Sebagai contoh, sistem navigasi mobil dapat merekam ke mana saja mobil tersebut berjalan. Sensor dan modul-modul diagnosa yang dipasang dapat menyimpan informasi yang dapat digunakan untuk menyelidiki terjadinya kecelakaan, termasuk informasi kecepatan, jauhnya perjalanan, status rem, posisi persneling yang terjadi dalam lima menit terakhir. Semuanya merupakan sumber-sumber bukti digital yang amat berguna

Copyright © March 2025

Bersalah atau Tidak

- **Dasar pembenaran seseorang dapat dikatakan bersalah atau tidak** melakukan tindak pidana :
  1. perbuatannya dapat dipersalahkan atas kekuatan UU yang telah ada sebelumnya (asas legalitas),
  2. perbuatan tersebut didukung oleh kekuatan bukti yang sah (pembuktian)
  3. kepadanya dapat dipertanggung-jawabkan (unsur kesalahan).
- Pembuktian dalam hukum acara pidana bertujuan untuk mencari kebenaran materiil (kebenaran yang sesungguhnya).
- **ALAT BUKTI** menurut **KUHAP** Pasal 184 :

  a. Keterangan saksi
  b. Keterangan ahli
  c. Surat
  d. Petunjuk
  e. Keterangan terdakwa

Copyright © March 2025

TEORI PEMBUKTIAN

- **Pasal 183 KUHAP** secara tegas merumuskan bahwa ”Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya **dua alat bukti yang sah** ia memperoleh **keyakinan** bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya”.
- **Teori Pembuktian dalam Hukum Acara Pidana :**

➢ **Teori pembuktian berdasarkan Undang-Undang secara positif**

- Teori ini adalah pembuktian yang didasarkan hanya kepada **alat-alat pembuktian yang disebut UU**. Dikatakan **secara positif**, karena didasarkan **hanya pada UU**.

➢ **Teori pembuktian berdasarkan keyakinan hakim**

- Teori ini didasarkan kepada **keyakinan hati nurani hakim**, yang menetapkan bahwa terdakwa telah melakukan perbuatan yang didakwakan.

Copyright © March 2025

TEORI PEMBUKTIAN

- **Teori pembuktian berdasarkan keyakinan Hakim atas alasan yang logis**;
  - Menurut teori ini hakim dapat memutuskan seseorang bersalah berdasar keyakinannya, **keyakinan yang didasarkan kepada dasar-dasar pembuktian disertai dengan suatu kesimpulan** (*conclusi*) yang **berlandaskan kepada peraturan-peraturan pembuktian tertentu**. Sistem atau teori pembuktian ini disebut juga pembuktian bebas, karena hakim bebas untuk menyebut alasan-alasan keyakinannya (*vrije bewijstheorie*)
- **Teori pembuktian berdasarkan Undang-Undang secara negatif** ;
  - Teori ini di samping **berdasarkan alat-alat bukti yang sah** berdasarkan **Undang-Undang** juga alat bukti yang sah tersebut disertai dengan **keyakinan hakim**.
- Memperhatikan teori pembuktian tersebut di atas, maka nampak dengan jelas **rumusan Pasal 183 KUHAP didasarkan pada suatu teori pembuktian berdasarkan Undang-Undang secara negatif (*Negatief Wettelijk*).**

Copyright © March 2025

PEMBUKTIAN CYBERCRIME

- Berdasarkan **teori pembuktian berdasarkan Undang-Undang secara negatif (*Negatief Wettelijk*)** tersebut perkara *"Cyber Crime"* bila dikaitkan dengan Pasal 1 ayat (1) KUHP tentang asas legalitas juncto perintah undang-undang sebagaimana dirumuskan dalam Pasal 3 KUHAP, yang selengkapnya berbunyi " Peradilan dilakukan menurut cara yang diatur dalam undang-undang ini", maka penerapan sistem pembuktian yang dianut dalam KUHAP secara legalitas **tidak dapat mengakomodir alat bukti (terutama yang mirip dengan bukti surat)** sebagai kemungkinan dipergunakan dalam *Cyber Crime.*

Copyright © March 2025

PEMBUKTIAN CYBERCRIME

- Pendapat demikian setidaknya didasarkan alasan sebagai berikut :
  - **Masih dipertahankannya Asas Legalitas dalam Hukum Pidana Indonesia** ; Moelyatno menulis bahwa asas legalitas itu mengandung 3 pengertian, yaitu :
    1. Tidak ada perbuatan yang dilarang dan di ancam dengan pidana kalau hal itu terlebih dahulu belum dinyatakan dalam suatu aturan undang-undang ;
    2. Untuk menentukan adanya perbuatan pidana tidak boleh digunakan analogi (kiyas) ;
    3. Aturan-aturan hukum pidana tidak berlaku surut.

Copyright © March 2025

PEMBUKTIAN CYBERCRIME

- Menurut Groenhuijsen, ada **empat makna yang terkandung dalam asas legalitas** ini. Dua dari yang pertama ditujukan kepada **pembuat undang-undang** (*de wetgevende macht*), dan dua yang lainnya merupakan **pedoman bagi hakim**, yaitu :
  1. Pembuat UU tidak boleh memberlakukan suatu ketentuan pidana berlaku mundur.
  2. Semua perbuatan yang dilarang harus dimuat dalam rumusan delik sejelas-jelasnya.
  3. Hakim dilarang menyatakan bahwa terdakwa melakukan perbuatan pidana didasarkan pada hukum tidak tertulis atau hukum kebiasaan,
  4. Terhadap peraturan hukum pidana dilarang diterapkan analogi

Copyright © March 2025

PEMBUKTIAN CYBERCRIME

- Dikatakan selanjutnya bahwa asas ini dikenal dengan adagium " *Nullum delictum noella poena praevia sine lege peonali ".*
- *Nullum crimen sine lege* berarti tidak ada tindak pidana tanpa undang-undang dan
- *Nulla poena sine lege* berarti tidak ada pidana tanpa undang-undang.
- Jadi **undang-undang menetapkan dan membatasi perbuatan mana dan pidana (sanksi) mana yang dapat dijatuhkan kepada pelanggarnya**

Copyright © March 2025

Menilai Evidence

- Faktor yang menjadi pertimbangan :
  - Penilaian kasus
  - Onsite consideration
  - Analisa lokasi pemprosesan
  - Pertimbangan hukum
  - Analisa evidence

Copyright © March 2025

Analisa Evidence

- Lokasi ditemukan evidence
- Stabilitas media yang dilakukan pemeriksaan
- Menentukan bagaimana evidence didokumentasi
- Mengevaluasi lokasi media penyimpanan
- Memastikan kondisi dari evidence
- Menganalisa kebutuhan akan cadangan listrik

Copyright © March 2025

Pemeriksaan Evidence

- Pengujian dilakukan dengan tahap :
  - Persiapan sebagai langkah awal
  - Ekstraksi
  - Menganalisa data terekstrak
  - Kesimpulan

Copyright © March 2025

Perlindungan Barang Bukti

- Menurut Jim Mc Millan “ Banyak kasus tidak dibawa ke pengadilan karena barang bukti yang tidak memadai “
- Barang bukti komputer berupa :
  - Barang sensitif
  - Salah menangani akan rusak
  - Bersifat mekanis - elektromekanis

Copyright © March 2025

Ancaman terhadap barang bukti

- Menurut Jim Mc Millan “ Importance of a standard methodology in computer forensics “ :
  - Virus
  - Prosedur cleanup
  - Ancaman eksternal - lingkungan

Copyright © March 2025

Ancaman terhadap barang bukti

- Menurut Judd Robin “ An explanation of computer forensics “ mensyaratkan :
  - Barang bukti tidakakan rusak oleh prosedur penyelidikan
  - Tidak terinfeksi virus komputer
  - Barang bukti dilindungi dari keruksakan mekanis dan elektromekanis
  - Penerapan pemelihraan
  - Membatasi dampak pada operasi bisnis
  - Informasi client dihargai secara etis dan tidak diumumkan

Copyright © March 2025

Faktor yang tidak berkaitan dengan barang bukti secara fisik

- Rangkaian pemeliharaan
- Batasan waktu
- Informasi yang tidak diumumkan – informasi client
- Register, peripheral memori dan cache
- Memori (kernel dan fisik)
- Keadaan jaringan
- Proses yang sedang berjalan
- Disk
- Floppy disk dn media backup
- CD-Rom dan printout

Copyright © March 2025

Prinsip ketidakpastian Heisenberg

- Dan Farmer " Computer forensic analysis class hendouts " :

  "Melakukan pengujian sekumpulan atau suatu bagian dari sistem akan menimbulkan gangguan pada komponen lainnya, sehingga akan mustahil untuk melakukan *capture* keseluruhan sistem pada satu saat saja"

- Jim Mc Millan

  "Banyak barang bukti dalam bentuk terenkripsi atau hidden"

Copyright © March 2025

Copyright © March 2025

PERTEMUAN 11

PENANGANAN INSIDEN FORENSIK DAN FREEZING THE SCENE

Copyright © March 2025

PRA INSIDEN

- Jenis insiden menurut the information security management :
  - Virus
  - Unauthorized access
  - Pencurian atau kehilangan kepercayaan pada informasi
  - Serangan denial of service pada sistem
  - Korupsi informasi

Copyright © March 2025

PERSIAPAN

- Pengunaan beberapa tool untuk mencegah penyusupan dengan deteksi
- Backup sistem
- Kebijakan password
- Kebijakan keamanan sistem
- Lakukan instalasi patch security
- Pergunakan security– auditing tools
- Pelajari sistem lebih lama
- Aktifkan fasilitas logging dan accounting
- Lakukan audit dan pengujian pada sistem secara rutin

Copyright © March 2025

PROSEDUR PENANGANAN INSIDEN

- Bagaimana mengamankan dan menjaga barang bukti
- Dimana dan bagaimana mencari barang bukti
- Daftar yang dipersiapkan untuk laporan menyeluruh
- Daftar orang untuk keperluan pelaporan
- Daftar software yang digunakan
- Daftar ahli

Copyright © March 2025

PROSEDUR PENANGANAN INSIDEN SECARA SEDERHANA

- Menurut Scott Grace " Computer incident response and computer forensics overview" :
  - Amankan lingkungan
  - Shutting down komputer
  - Label barang bukti
  - Dokumentasikan barang bukti
  - Transportasikan barang bukti
  - Dokumentasikan rangkaian penyimpanan

Copyright © March 2025

PROSEDUR PENANGANAN INSIDEN

- Jika ahli forensik tidak dimiliki atau tidak berada ditempat dan terdapat insiden, yang harus dilakukan oleh seorang staff :
  - Membuat image
  - Analisis forensik dilakukan semua dari copy
  - Memelihara rincian media dalam proses

Copyright © March 2025

FASE MERESPON INSIDEN

- Fase 1 : Persipan
- Fase 2 : Identifikasi
- Fase 3 : Pengisian Fase
- Fase 4 : Pembasmian Fase
- Fase 5 : Pemulihan Fase
- Fase 6 : Tindak lanjut

Copyright © March 2025

EMERGENCY ACTION CARD

1. Tetap tenang sehingga terhindari kesalahan fatal
2. Buatlah catatan yang baik dan relevan
3. Beritahu orang yang tepat dan carilah pertolongan
4. Tetapkan kebijakan orang – orang terpercaya yang boleh tahu
5. Gunakan jalur komunikasi terpisah dari sistem yang mengalami compromise

Copyright © March 2025

EMERGENCY ACTION CARD

6. Isolasi maslah sehingga tidak bertambah buruk
7. Buat backup sistem
8. Temukan sumber masalah
9. Kembali ke pekerjaan semula setelah backup terjamin dan lakukan restore sistem
10. Belajar dari pengalaman

Copyright © March 2025

PEMROSESAN BARANG BUKTI

- Menurut Lori Willer “ Computer forensics”, panduan :
  1. Shut down komputer, dan perlu dipertimbangkan keruksakan proses yang berjalan dibackground
  2. Dokumentasikan konfigurasi hardware dari sistem
  3. Pindahkan sistem komputer ke lokasi yang aman
  4. Buat backup bit dari hard disk dan floppy

Copyright © March 2025

PANDUAN

5. Uji otentifikasi data dari semua penyimpanan
6. Dokumentasikan tanggal dan waktu yang berhubungan dengan file komputer
7. Buat daftar key word pencarian
8. Evaluasi swap file
9. Evaluasi file slack, dari dump memori yang terjadi selama file ditutup
10. Evaluasi unallocated space – erased file

Copyright © March 2025

PANDUAN

11. Pencarian keyword pada file, file slack dn unallocated space
12. Dokumentasikan nama file (atribut tanggal dan file)
13. Identifikasikan anomali file, program dan storage
14. Evaluasi fungsionalitas program untuk mengetahui kegunaannya
15. Dokumentasikan temuan dan software yang dipergunakan
16. Buat copy dari software yang dipergunakan

Copyright © March 2025

TAHAPAN PEMROSESAN BARANG BUKTI

- Menurut Jim Mc Millan, lima tahapam pemrosesan barang bukti :
  - Persiapan
  - Snapshot
  - Transport
  - Pengujian
  - Analisa

Copyright © March 2025

PERSIAPAN

- Sterilkan semua media dari virus
- Pastikan semua tool forensik bisa dipergunakan secara resmi
- Periksa kerja semua peralatan lab
- Pilih ahli forensik yang tepat dan mampu memberikan kesaksian dan penjelasan di persidangan

Copyright © March 2025

SNAPSHOT

- Foto lingkungan
- Catat rinciannya
- Foto barang bukti
- Dokumentasikan konfigurasi hardware
- Labeli barang bukti sesuai metodologi
- Foto barang bukti lagi setelah dilabeli
- Dokumentasikan apa terjadi

Copyright © March 2025

TRANSPORT

- Lakukan pengemasan secara aman
- Foto dan dokumentasikan penanganan barang bukti meninggalkan tempat kejadian sampai ke lab pengujian

Copyright © March 2025

PENGUJIAN

- Lakukan unpack sesuai metodologi
- Lakukan uji visual dan catat setiap konfigurasi yang tidak semestinya
- Buatlah image hard disk
- Setelah menbuat image simpan barang bukti di tempat aman dan catat
- Lakukan pembuat image kedua

Copyright © March 2025

ANALISA

- Analisa barang bukti dilakukan secara dua level :
  - Level fisik
  - Level logic
- Perhitungan rangkaian kepercayaan – chain of evidence

Copyright © March 2025

RANGKAIAN KEPERCAYAAN

- Shell
- Command
- Dynamic libraries
- Device driver
- Kernel
- Controller
- Hardware

Copyright © March 2025

FREEZING THE SCENE

Mengumpulkan bukti-bukti dengan mengamankan lokasi dari setiap aktifitas yang dapat merusak atau menghilangkan barang bukti

Copyright © March 2025

FREEZING THE SCENE

Menurut Judd Robbins dari “An Explanation of Computer Forensics” mensyaratkan hal berikut:

-Barang bukti tidak rusak atau terpengaruh oleh prosedur yang dipergunakan untuk penyelidikan.

-Tidak terinfeksi virus komputer selama proses analisis.

-Bukti-bukti yang relevan dan ekstraksinya, ditangani dan dilindungi dari kerusakan mekanis atau elektromekanis lebih jauh.

-Penerapan pemeliharaan

-Membatasi dampak pada operasi bisnis

-Semua informasi client yang diperoleh selama eksplorasi forensik dihargai secara etis dan tidak diumumkan

Copyright © March 2025

SELESAI

Copyright © March 2025

PERTEMUAN 6

Standar Metodologi Komputer Forensik

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

Cakupan Standar Metodologi

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

Copyright © March 2025

Lima faktor

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

Kemampuan penyelidik

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

Copyright © March 2025

Kebijakan dan Prosedur

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

Copyright © March 2025

Pertimbangan administratif

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

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

Copyright © March 2025

Copyright © March 2025

PERTEMUAN 13

KEAMANAN DALAM BIDANG TI Di SISI PENGGUNA

Copyright © March 2025

KEAMANAN DALAM BIDANG TEKNOLOGI INFORMASI

- Keamanan dalam penggunaan komputer dan internet sangat tergantung minimal pada 3 pihak, yaitu :
  1. Pengguna - user
  2. Fasilitator (penyedia layanan) komputer / internet/ Penyelenggara Sistem Elektronik
  3. Penyedia produk (teknologi), yaitu perusahaan pembuat perangkat lunak (software)

Copyright © March 2025

KEAMANAN PADA SISI PENGGUNA

- Kesadaran pengguna komputer / internet tentang keamanan fasilitas yang digunakan merupakan hal terpenting / utama karena pada akhirnya Pengguna-lah yang biasanya paling banyak menjadi korban.
- **Penggunaan Password**
  - Password mudah ditebak, misal ; menggunakan nama anggota keluarga, tempat/ tanggal lahir, nomor telepon dll.
  - Password terlalu singkat dan umum, semakin sedikit dan umum karakter yang digunakan akan semakin mudah password ditebak. Metode *brute force attack* telah umum dipakai untuk menjebol password file-file Ms. Office, zip, rar, sistem operasi dll.

Copyright © March 2025

KEAMANAN PADA SISI PENGGUNA

- **Phising (Spoofing)**
  - Dalam dunia hacking, teknik phising (dari kata fishing : memancing)/ spoofing bertujuan untuk mengecoh / menipu pengguna seolah-olah telah membuka situs asli, padahal situs palsu, misal situs www.klikbca.com dipalsukan menjadi wwwklikbca.com, kilkbca.com, clickbca.com, klickbca.com, dan klikbac.com.
  - Metode phising juga dilakukan secara aktif, misalnya dengan mengirim email palsu berisi informasi tertentu dan penerima email dapat mengklik link yang disediakan dalam email tersebut, misalnya email tentang software terbaru, request teman, menang hadiah dsb.

Copyright © March 2025

Cara menghindari phising

- Usahakan selalu login menggunakan bookmark atau ketik sendiri dengan benar dan teliti pada web browser.
- Sebisa mungkin tidak melakukan login dari link, atau periksa dahulu keaslian link situs tersebut.
- Jika login pertama gagal, segera periksa halaman web sekarang dan sebelumnya, jika terbukti palsu segera ganti password.
- Pengguna Mozilla Firefox dapat menginstal add on anti phising, misal; PhishTank SiteChecker, kunjungi https://addons.mozilla.org/en-US/firefox/addon/3840.

Copyright © March 2025

KEAMANAN DI TEMPAT PUBLIK

- Jika terpaksa harus koneksi internet melalui warnet, waspadai adanya indikasi penggunan program penyadapan dalam komputer yang kita gunakan, misal ;
  - **Keylogger**, merupakan program yang merekam setiap ketikan pada keyboard, termasuk saat login dan mengisi password.
  - **Sniffing**, merupakan kegiatan penyadapan yang dilakukan saat membuka situs yang tidak menggunakan enkripsi, sehingga semua data akan mudah terekam mentah2 karena tanpa terenkripsi. Situs yang telah menggunakan enkripsi ditandai dengan alamat yang diawali https://, bukan http://.
  - **DNS**, merupakan program yang dapat membelokkan situs yang kita ketik ke situs yang lain.
- Antisipasi untuk menghindari penyadapan adalah dengan menggunakan warnet terpercaya, hindari menyimpan password dalam web browser, hapus semua data history setelah browsing.

Copyright © March 2025

KEAMANAN PADA SITUS DAN SOFTWARE

- **Kesalahan pada Penyedia Layanan Web**
- Pencegahan yang dapat dilakukan atas kesalahan Penyedia Layanan Web ini, yaitu :
    - Gunakan password yang berbeda untuk situs yang berbeda, minimal memiliki 3 password untuk keperluan berbeda sesuai urgensinya.
    - Manfaatkan fitur-fitur sekuriti/ keamanan yang disediakan oleh penyedia layanan web, misal pada mail Yahoo terdapat fitur Sign Seal untuk mencegah phising.
    - Jangan gunakan fitur yang berlebihan dan membebaskan pengguna lain untuk berbuat banyak, misalnya setiap testimoni dalam Friendster harus di-approve secara manual.
    - Sering-sering membaca artikel tentang sekuriti di internet.
    - Gunakan penyedia layanan web yang kredibel, telah banyak digunakan, dan dapat diandalkan.

Copyright © March 2025

KEAMANAN PADA SITUS DAN SOFTWARE

- **Kesalahan Software**
- Kesalahan dapat terjadi karena program yang diinstal pada komputer memiliki kelemahan yang dapat dieksploitasi, misalnya enkripsi PDF pada Adobe Acrobat dapat langsung dijebol dengan Password Recovery buatan ElcomSoft. Ditemukan nya kelemahan pada browser dan sistem operasi juga dapat membahayakan keamanan.

Copyright © March 2025

KEAMANAN PADA SITUS DAN SOFTWARE

- **Pencegahan gangguan keamanan akibat kesalahan program :**
  - Jangan terlalu banyak menginstal program apalagi jika tidak perlu, karena akan semakin rawan dengan masalah sekuriti, apalagi jika pembuat software kurang memperhatikan masalah keamanan.
  - Pastikan bahwa firewall selalu aktif untuk memblok port-port yang tidak perlu, sehingga meminimalkan serangan trojan, worm dan pengiriman data ilegal.
  - Gunakan program aplikasi versi terbaru yang sudah rilis (stabil

Copyright © March 2025

KEAMANAN PADA SITUS DAN SOFTWARE

- **Penipuan Produk**
- Terdapat Penyedia jasa dan produk palsu yang menyediakan program aplikasi anti virus palsu, padahal sebetulnya dikategorikan sebagai malware atau software/ program yang berbahaya bagi komputer.
- Pengguna harus lebih berhati-hati saat mendownload atau menginstal program, termasuk menjalankan semua file yang dapat dieksekusi, seperti **.**exe, **.**com, **.**bat.

Copyright © March 2025

PROGRAM-PROGRAM YANG MENGGANGGU KEAMANAN

- **ADWARE**, program iklan yang ikut menumpang dengan software tertentu. Setelah diinstal, program ini cenderung mengganggu seperti men-download dan menyangkan iklan-iklan secara otomatis.
- **SPYWARE**, program mata-mata yang mengirimkan informasi tanpa izin. Spyware dapat digunakan sebagai alat marketing, mencuri informasi, dan mengarahkan browser ke situs pengiklan.
- **WORM**, program yang memanfaatkan kelemahan jaringan dan mampu menduplikasikan diri tanpa campur tangan manusia. Akibatnya, bandwidth jaringan yang dimakan cukup besar dan mengakibatkan koneksi jaringan/ internet lamban, komputer tidak stabil dan sering restart

Copyright © March 2025

PROGRAM-PROGRAM YANG MENGGANGGU KEAMANAN

- **TROJAN**, program yang seperti memberi manfaat, namun dibalik itu bisa merusak sistem operasi atau data-data. Ketika software ini dijalankan, tanpa sadar data-data dicuri atau komputer kita dikendalikan oleh pembuat trojan.
- **VIRUS**, merupakan program yang bersifat mengganggu bahkan merusak komputer dan melakukan aktifitasnya secara sembunyi-sembunyi tanpa sepengetahuan pemilik komputer, juga dapat menduplikasikan diri untuk menyerang komputer lain, misalnya dengan media file sharing dan flash disk,

Copyright © March 2025

KEAMANAN SITUS

- Pemilik Situs atau Administrator Situs perlu memperhatikan masalah keamanan suatu situs agar tidak mengganggu pengguna-nya atau bahkan ditinggalkan pengguna. Beberapa bentuk serangan yang potensial mengancam keamanan, diantaranya adalah :
  - **Hacker Log**, dalam tahap ini seorang Hacker hanya mengamati atau mungkin dalam tahap pencarian celah keamanan (security hole)
  - **Warning Message**, Hacker dalam hal ini sudah menyusup ke dalam sistem dan memberikan pesan tertentu agar Admin memperbaiki celah keamanannya.

Copyright © March 2025

KEAMANAN SITUS

- **Deface Site**, Hacker sudah berhasil masuk kedalam sistem sepenuhnya dan tidak segan mengubah tampilan situs terkait.
- **Destroyed Site**, Hacker pada tahap ini tidak segan untuk menghapus data-dat penting, melumpuhkan situs sehingga tidak dapat diakses.

Copyright © March 2025

Pencegahan Gangguan Terhadap Situs

- Backup Database, segera backup database pada tempat yang aman, terutama untuk situs yang dinamis dan menggunakan banyak database.
- Update Sistem, segera update atau migrasi ke sistem yang lebih aman, terutama jika situs rawan tindak kejahatan dan banyak celah keamanan (security hole).
- Update Web Server ke versi terbaru yang sudah dipatch lubang keamanannya.
- Update Engine Web ke versi terbaru yang sudah dipatch keamanannya.
- Jangan Gunakan Nama Database yang Default.

Copyright © March 2025

Pencegahan Gangguan Terhadap Situs

- Jangan Gunakan Username dan Password Default,

  misal ; admin atau 123456.
- Memasang Firewall
- Lakukan Monitoring dan Cek Log secara berkala, meng-update patch keamanan dan mengecek berkas log karena tidak ada yang tahu kapan serangan terjadi.
- Lakukan keamanan intern dari pihak-pihak yang tidak berwenang, pisahkan ruangan server dengan ruangan lain.

Copyright © March 2025

SELESAI

Copyright © March 2025

TOOLS FORENSIK

Pengantar Komputer Forensik teknologi Informasi

Copyright © March 2025

Tool Forensik

Tool yang dipergunakan oleh ahli forensik harus **bekerja baik** dan **tidak mengubah data**. Di samping itu, **komunitas komputer forensik harus menerima tool dan hasilnya**.

Tool kit untuk pengujian forensik memungkinkan untuk **mengumpulkan dan analisis data**, seperti tcpdump, Argus, NFR, tcpwrapper, sniffer, nstat, tripwire, diskcopy (/v pada DOS), DD pada Unix.

Karena ahli hukum percaya bit lebih mudah dipalsukan daripada kertas, maka aturan utamanya adalah "*preserve then examine*".

Copyright © March 2025

Kategori software forensik

- Forensic software tools for Windows
- Image and Document Readers
- Data Recovery/Investigation
- Password Cracking
- Network Investigation
- Phone Investigation
- PDA Investigation
- Lab Tools
- Assessments utilities
- Foundstone SASS Tools
- Intrusion Detection Tools
- Scanning Tools
- Stress Testing Tools

Copyright © March 2025

Tool Forensik

- Contoh dari aplikasi yang dapat digunakan dalam komputer forensik, yaitu :
  - Encase www.guidancesoftware.com
  - Forensics toolkit www.accessdata.com
  - LoPe www.evidencetalks.com
  - Forager www.inforenz.com/software/forager.html
  - X-Ways Forensics www. x-ways.net/forensic/index-m.html

Copyright © March 2025

Tool Forensik

Beberapa tool untuk komputer forensik :

The Coroner Toolkit - Dan Farmer & Wietse Venema , www.fish.com
Byte Back - oleh TechAssist, http://www.toolsthatwork.com/
DriveSpy - http://www.digitalintel.com/
EnCase - oleh Guidance Software, http://www.encase.com/
Forensic ToolKit - http://www.accessdata.com/
Maresware Suite - http://www.dmares.com/
Drive Image Pro – PowerQuest
Linux "dd" - Red Hat
Norton Ghost 2000 – Symantec
SafeBack - New Technologies
SnapBack DatArrest oleh Columbia Data Products

Copyright © March 2025

Tool Forensik

SC Magazine merekomendasikan DriveSpy dan EnCAse ;

DriveSpy beroperasi pada lingkungan DOS dan memberikan semua tool yang diperlukan untuk melakukan **eksplorasi suatu media** dan **menemukan data yang relevan.**

EnCASE memiliki GUI yang menarik dan beroperasi pada image ketimbang bukti asli. EnCase juga mengikutsertakan fungsi pembangkitan laporan dan suatu feature yang sangat berguna yang mendukung bahasa pemrograman bernama Escript. EnCase, dari Guidance Software bisa **mengelola dan melihat semua bukti**. Terdapat feature untuk **mencatat siapa yang bekerja** dan kapan dengan data.

SafeBack dari New Technologies, Inc untuk **memelihara barang bukti** dipakai secara khusus oleh pihak penegak hukum AS

Copyright © March 2025

Tool Forensik

Terdapat bermacam vendor perangkat lunak forensik. Paket dari The New Technologies Corporate Evidence Processing Suite menyertakan :

- CRCND5: CRC (*checksum*) yang memvalidasi isi file.
- DISKSIG: CRC program yang memvalidasi image backup.
- FILELIST: Tool katalog disk untuk evaluasi komputer berdasarkan waktu
- FILTER I: Filter berkecerdasan dengan *fuzzy logic*.
- GETFREE: Tool pengumpulan *unallocated data.*

Copyright © March 2025

Tool Forensik

- GETSLACK: Tool pengumpulan untuk *file slack*.
- GETTIME: Program untuk dokumentasi waktu dan tanggal sistem sebagai barang bukti
- NTI-DOC: Program dokumentasi untuk merekam atribut, tanggal dan waktu file.
- SEIZED: Program untuk mengunci dan mengamankan komputer
- SHOWFL: Program untuk analisa keluaran daftar file
- Text Search Plus: Utility pencarian teks untuk menentukan letak kata kunci dari teks dan grafik

Copyright © March 2025

Tool Forensik

Key Computer Service menawarkan paket ;

- Program *password cracker*
- WIPER/WIPEDRV - Menghapus keseluruhan informasi secara lojik atau fisik dengan menulis setiap byte karakter.
- LISTDRV - utility yang menguji file FAT12, FAT16, dan FAT32 yang dibatasi koma dan tanda petik untuk disiapkan diimport ke database atau *spreadsheet.*
- CHKSUM - utility yang mengkalkulasi 64-bit *checksum* untuk drive fisik atau lojik

Copyright © March 2025

Tool Forensik

Key Computer Service menawarkan paket ;

- DISKIMAG - membuat copy image floppy untuk analisis
- FREESECS - Untuk mencari drive lojik spesifik tertentu untuk *free space* dan menyimpan informasi yang termuat di *unnalocated space* ke file..
- DISKDUPE- utility berbahasa assembly yang membuat copy forensik dari floppy disk
- DATASNIFFER- utility yang memotong file data dari file atau *unused space* (saat recovery dengan utility seperti FREESECS).

Copyright © March 2025

Tool Forensik

Alternatif lain ;

- Meski terdapat program khusus forensik yang tersedia, program seperti MS-DOS bisa merupakan tool forensik yang berguna. Misal perintah
  - DISKCOPY,
  - DEBUG,
  - UNDELETE, dan
  - UNFORMAT.

Copyright © March 2025

SELESAI

Copyright © March 2025