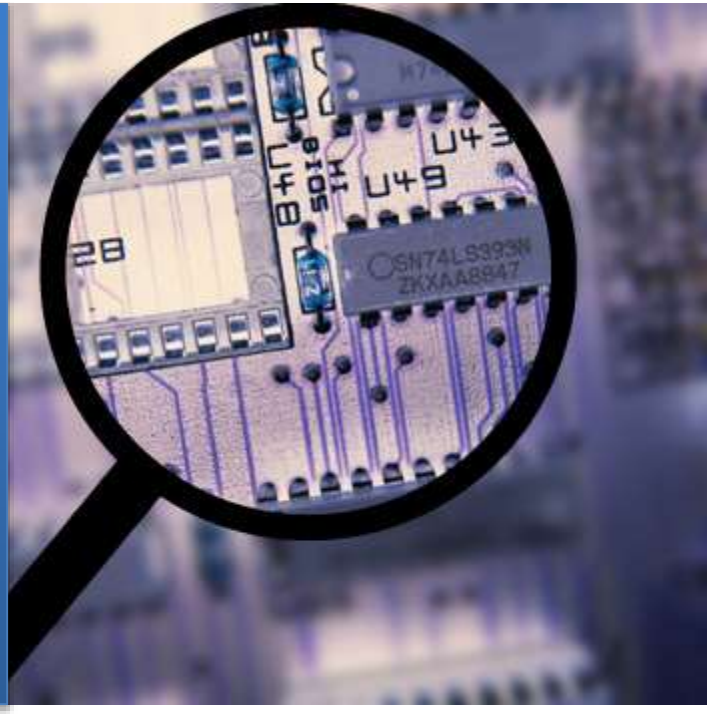
Gunadarma University

Pengenalan tool pendukung pekerjaan forensik



Hardware dan Software Forensic Tools

Informatics Engineering

Faculty Of
Industrial Technology

Computer Forensic Tools

Alat-alat yang digunakan untuk menganalisis data digital & membuktikan atau menyangkal suatu kegiatan kriminal

Tahapan Computer Forensic

- Acquisition – Images systems & gathers evidence
- Analysis – Examines data & recovers deleted content
- Presentation – Tools not used

- Bidang Investigasi komputer forensik mencakup melakukan capture dan analisis data digital untuk membuktikan apakah suatu kejahatan telah dilakukan atau belum.
- Ruang lingkup kejahatan dapat mencakup kejahatan komputer terkait serta kejahatan lainnya yang meninggalkan bukti dalam format digital.
- Ada tiga fase utama dari komputer forensik:
  - akuisisi,
  - analisis,
  - presentasi.
- Fokus presentasi ini terutama pada tahap akuisisi dan analisis; tahap yang secara langsung berhubungan dengan pengumpulan dan analisis.

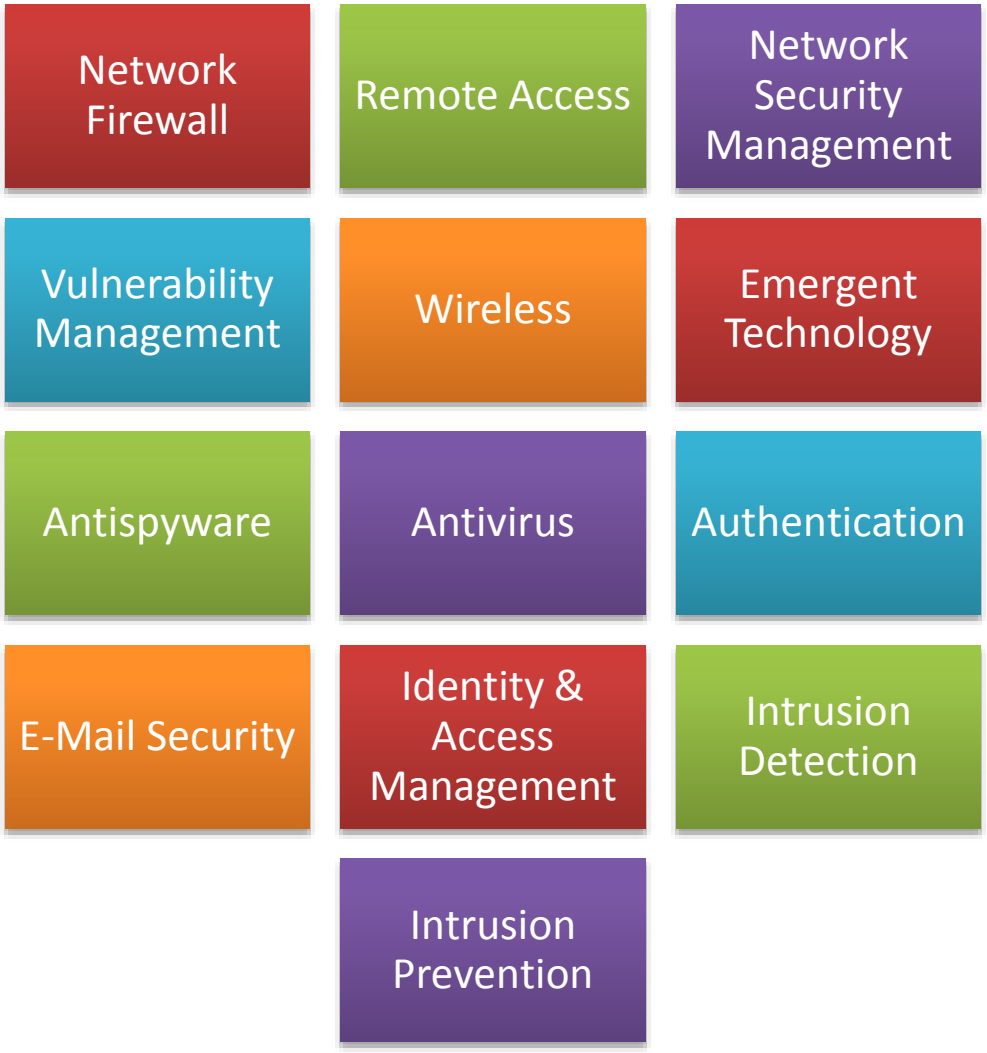
Admissibility of Forensic Evidence in Court

Data harus relevan & handal

- Keandalan bukti yang dikumpulkan oleh alat dinilai oleh hakim dalam sidang pra-peradilan
- Data yang di sajikan dalam persidangan dapat mewakili fakta

Ada dua kriteria yang diperlukan dalam hukum adalah apakah diperlukan pendapat ilmuwan dalam praktek-praktek pengumpulan dan analisis data yang ada dan membuktikan bahwa data adalah reliabel.

Artinya, data dapat diandalkan untuk mewakili fakta.



Jenis Security Software

Security tools adalah suatu aplikasi perangkat lunak yang digunakan untuk menjaga akses dan penggunaan media digital diluar otorisasi.

Tool ini digunakan oleh perorang/individu, usaha menengah, perusahaan dan instansi.

Walaupun bukan software forensik, Ada beberapa langkah pengamanan yang harus dilakukan tanpa mendahului investigasi.

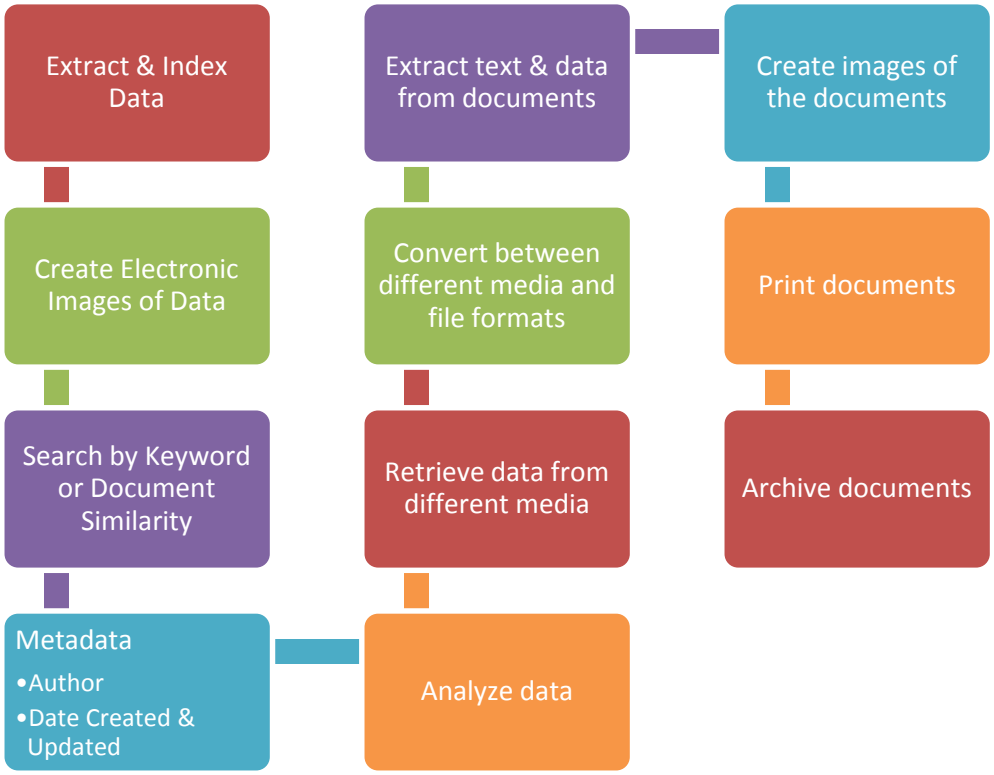
Jenis Forensic Software

- Acquisition Tools
- Data Discovery Tools
- Internet History Tools
- Image Viewers
- E-mail Viewers
- Password Cracking Tools
- Open Source Tools
- Mobile Device tools (PDA/Cell Phone)
- Large Storage Analysis Tools

Ada banyak tool standard yang digunakan oleh ahli komputer dalam upaya untuk melacak apa yang terjadi, ketika terjadi dan siapa kemungkinan pelaku.

Demikianlah bagaimana perangkat lunak forensik diklasifikasikan.

Electronic Data Discovery Tools



Electronic Data Discovery tools, disingkat DAQ, membantu dalam pemulihan data yang mungkin telah dihapus tapi tidak sepenuhnya dihilangkan dari sistem komputer. Ekstraksi data adalah pengumpulan data dan pengindeksan data menjadi kelompok-kelompok yang memungkinkan dilakukan analisis data. Penciptaan data elektronik harus menjadi salah satu langkah pertama dalam penyelidikan forensik. Pencarian dapat dilakukan baik dengan mencari string data atau jenis file atau kesamaan file. Metadata adalah data yang menggambarkan data seperti siapa yang menciptakan file, kapan diciptakan, ukuran file, waktu ketika diperbarui atau diakses.

Electronic data discovery tools tidak terbatas hanya menemukan data dan metadata. Beberapa fungsi alat akuisisi data tercantum di atas.

Internet History Tools

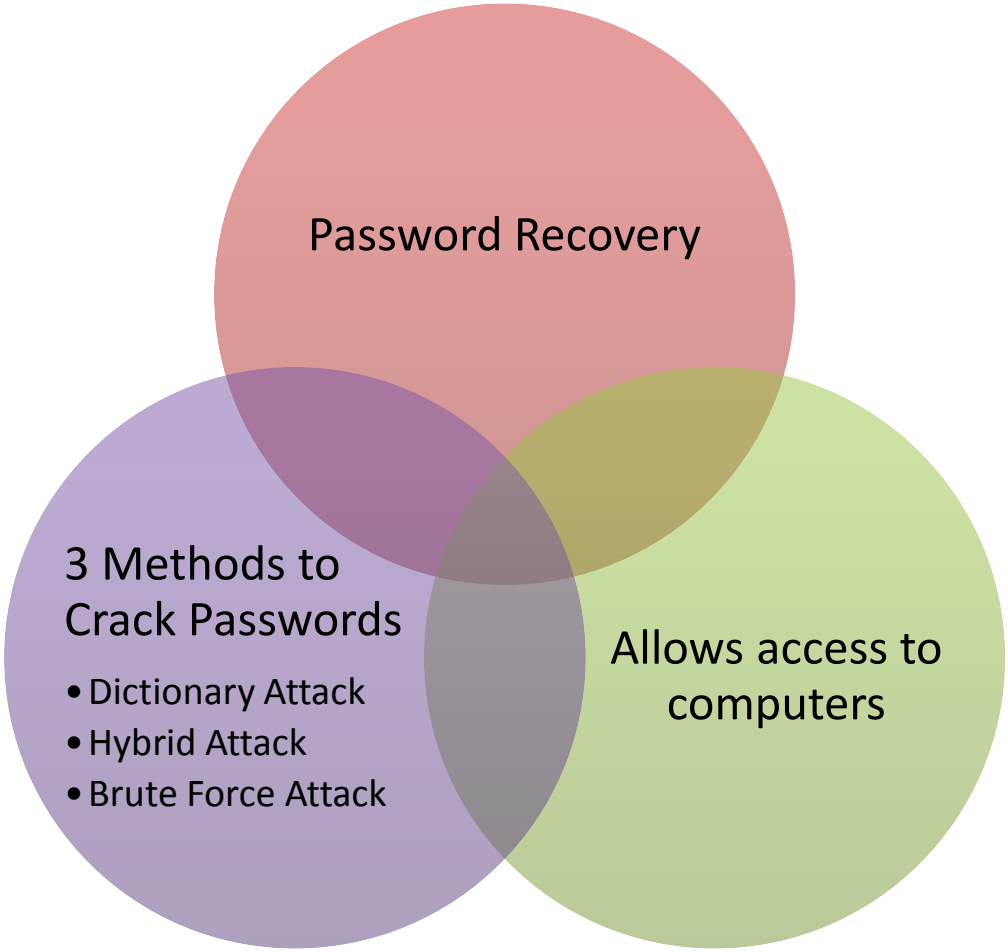
Internet history tools berguna dalam pelacakan bagaimana pengguna telah menggunakan internet dan situs di internet mana saja yang diakses. Kemampuan tool ini terbatas, karena tidak dapat menentukan bahwa suatu site telah diakses dengan hanya melalui pencarian sederhana kecuali ada beberapa situs yang mirip kontennya.

Image & E-Mail

- Views Files
- Converts Files
- Catalogs Files
- Side by Side File Comparisons

Image and E-mail viewers memungkinkan investigator forensik untuk meliahat images dan E-mails dan men-capture sebagai bukti. Hampir semua image and E-mail viewers memiliki kemampuan untuk melihat and mengakses multiple image and E-mail .

Password Cracking Tools



Dictionary Attack – Adalah suatu file kamus (suatu file text yang penuh oleh kata-kata) yang dimuat pada aplikasi cracking, yang dijalankan terhadap user account yang ditemukan oleh application tersebut. Karena sebagai besar password seringkali tergolong sederhana, dengan menjalankan sebuah dictionary attack seringkali cukup untuk pekerjaan cracking .

Hybrid Attack – Suatu hybrid attack akan menambahkan angka atau symbol pada suatu nama file dalam melakukan cracking suatu password. Banyak orang mengubah password menambahkan angka di password mereka. Pola yang biasa digunakan adalah sebagai berikut: password bulan pertama adalah "cat"; password bulan kedua adalah "cat1"; password bulan ketiga adalah "cat2"; dan seterusnya.

Brute Force Attack - A *brute force* attack adalah bentuk serangan yang paling menyeluruh, meskipun mungkin sering memakan waktu lama tergantung pada kompleksitas dari password. Beberapa serangan brute force dapat berlangsung seminggu tergantung pada kompleksitas dari password.

Open Source Tools

Tool Open Source, sering diklasifikasikan sebagai freeware and shareware. Mereka mudah ditemukan dan tersedia di internet.

Tool open source juga dapat digunakan secara luas dan kode dapat dilihat dan dinilai oleh para ahli di lapangan untuk memverifikasi nilainya.

Mobile Device Tools

- Number and variety of toolkits considerably more limited than for computers
- Require examiner to have full access to device
- Most tools focus on a single function
- Deleted data remains on PDA until successful HotSync with computer

Investigasi Digital forensic pada mobile devices sudah dimulai.

Karena perangkat ini memiliki beberapa perbedaan dengan komputer, maka diperlukan alat yang berbeda.

Pada saat ini alat yang tersedia masih sedikit untuk penyelidikan.

Forensic Tool Suites

- Parben
- The Coroner's Toolkit (TCT)
- The Sleuth Kit (TSK)
- EnCase
- Forensic Toolkit (FTK)
- Maresware

Forensic tool suites are sejenis tipe aplikasi.

Banyak tools komersial yang tersedia tetapi harganya cukup mahal.

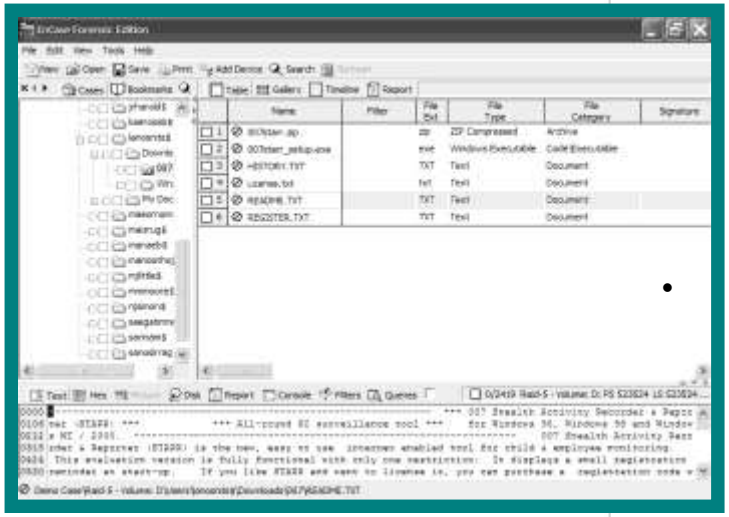
The Coroner's Toolkit and The Sleuth Kit adalah satu-satunya open source suites yang tersedia.

EnCase

Dikembangkan untuk penegakan hukum
Dibangun di sekitar manajemen kasus
berbasis Windows antarmuka pengguna grafis (GUI)
Multi Fitur

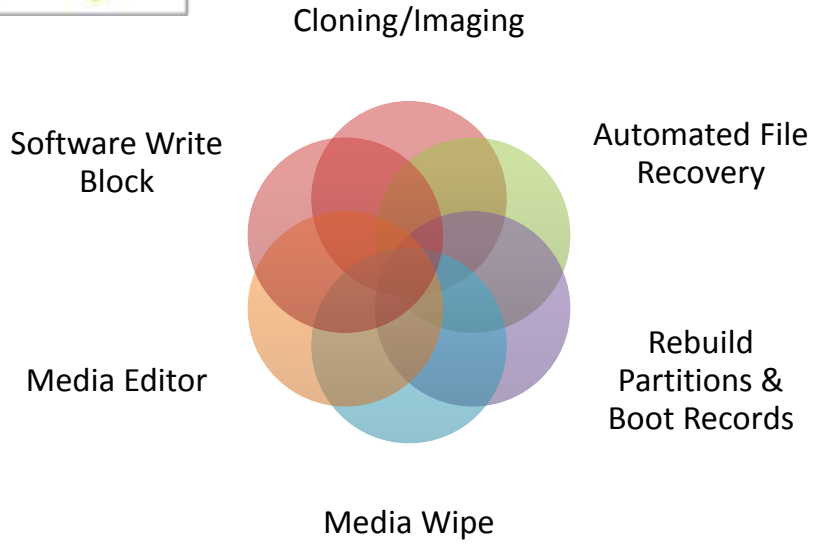
Encase Features:

- Automated Analysis
- Multiple Sorting Fields
- Filter Conditions
- Queries
- View "Deleted" Files
- Built-in Registry Viewer
- Encrypted Volumes
- Hardware Analysis
- Log File Analysis
- Event File Analysis
- File Signature Analysis



- EnCase is a Forensic Tool Suite. Adalah suatu paket software yang menyediakan multiple tool forensik. Hal yang pertama dilakukan oleh software ini adalah menciptakan file case.
- Ada beberapa fasilitas yang dapat digunakan oleh forensik investigator, seperti: Enterprise Edition – melakukan monitoring secara terpusat dan investigasi real-time; Snapshot – meng-capture kontent RAM, menjalankan programs, membuka files and ports; Mengatur hasil menjadi file case & menyediakan case management for berbagai kasus; Mengelola chain of custody;
- Tools for merespon ancaman yang muncul; Mendukung penyelidikan real-time dan post-mortem

ByteBack



ByteBack adalah suatu disk imaging and validasi tool, yang memungkinkan seorang investigator komputer forensik untuk mendapatkan data dan validasi integritasnya.

Forensic Toolkit (FTK)

Another Tool Suite
Acquires & Examines Electronic Data
Imaging Tool
File Viewer

- Forensic Toolkit adalah salah satu toolset yang powerful untuk mendapatkan dan memeriksa data.

FTK Features:

- **Easy to use**
- **Advanced Searching**
- **E-mail Analysis**
- **Zip file Analysis**
- **File Filter**
- **Register**

Maresware

Collection of Tool rather than Tool Suite

Main Difference – Tools are Stand-Alone & Called as Needed

4 Notable Tools

- Declasfy
- Brandit
- Bates_no
- Upcopy

- Maresware contains the tools routinely used by computer forensic investigators. Similar to competitor tools with the difference that this is really a collection of tools, rather than a suite. The tools can be called out and used as needed for specific tasks. No specific order is needed to use them, as in EnCase, in which you must create a case prior to doing any other activity.
- Declasfy – Disk wiping tool that overwrites physical media in compliance with U.S. Department of Defense standards
- Brandit – Brands hard disks with ownership information; useful in tracing and identifying stolen hard drives
- Bates_no – Adds identifying numbers to document file names, making it easier to manage records and files (case management)
- Upcopy – Copies entire directories from source to destination without changing any attributes or time/date stamps

Paraben

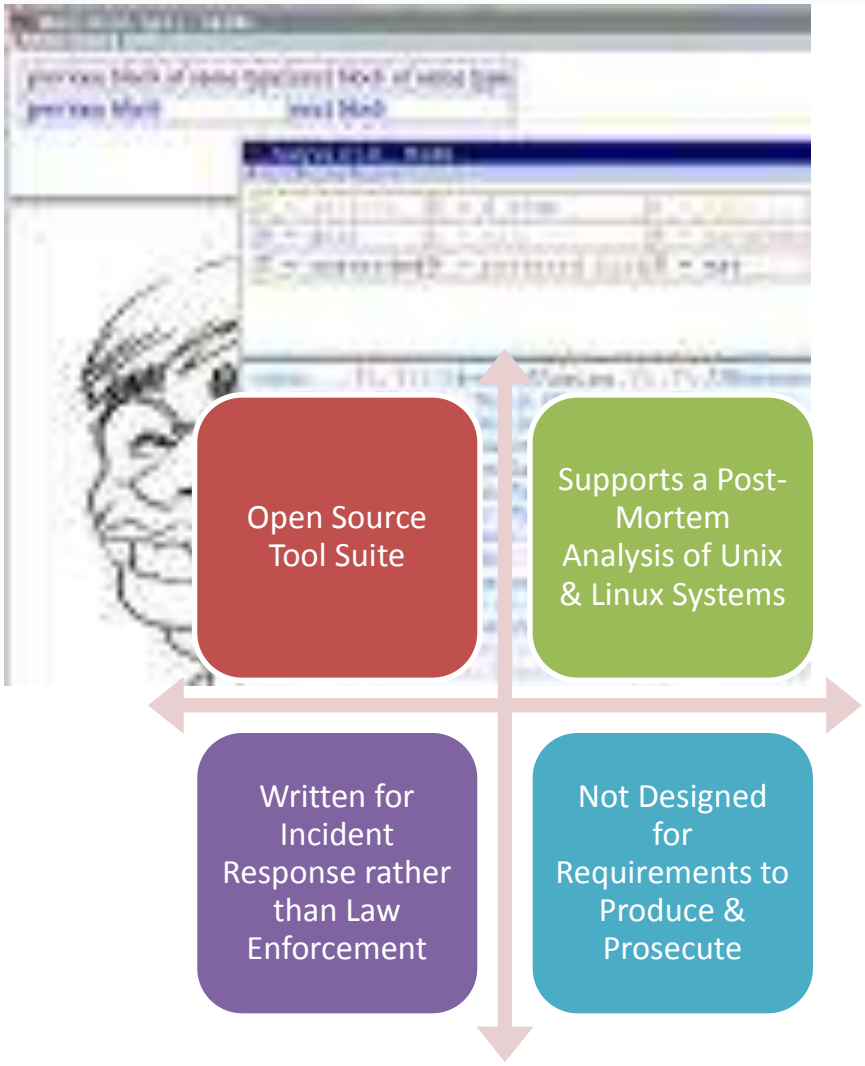
Collection of Stand-Alone Tools

Made up of 10 Individual Software Tool Sets

Purchased Separately, Price Break for Multiple Tool Purchases

Frequently Used with Mobile Devices

- Product ini adalah pilihan favorit untuk investigasi forensik pada PDA and handphone.
- Investigasi Mobile device berbeda dengan investigasi pada komputer dan Parben merupakan produk teratas pada bidang ini.
- Tool yang disediakan oleh Parben adalah sebagai berikut: Forensic Replicator, Forensic Sorter, Network E-mail Examiner, E-Mail Examiner, Decryption Collection, Text Search, Case Agent Companion, PDA Seizure, dan Cell Seizure.



Coroner's Toolkit (TCT)

- Toolkit Coroner (TCT) tidak dirancang untuk memenuhi persyaratan yang ketat untuk menghasilkan dan mengelola bukti sidang.
- Salah satu fitur yang membuat suite ini berbeda adalah bahwa ia dapat berjalan di suatu live machine dan memberikan informasi tentang proses yang sedang berjalan dan membuka file.
- Fitur utama adalah Grave-Robber , Ils & mactime programs, Unrm & lazarus programs, dan Findkey

The Sleuth Kit (TSK)

- TSK dapat beroperasi pada OS Unix, Linux and Mac OS. Sleuth Kit sangat unik karena dapat menganalisis files dari Mac systems dan telah melalui testing pada Mac OS X.
- Seperti TCT, TSK memiliki kemampuan untuk menganalisis data pada system yang sedang berjalan.

Hardware Acquisition Tools

Various Hardware & Software platforms
- Collect Data
- Process Data
- Save Data
- Display Data in Meaningful Manner

- Alat akuisisi dapat perangkat keras dan juga perangkat lunak.
- Alat-alat ini dapat digunakan untuk membuat gambar yang "aman" untuk sistem yang dicurigai untuk dilakukan tindakan dan analisis selanjutnya.

Forensic Hardware

Workstations - Copy & Analysis
Drive Imaging System
Drive Wiper
Bridge
    Write Blocker
    SATA, SCSI, IDE, USB

- Workstations sering digunakan untuk menyalin sistem yang dicurigai untuk selanjutnya dianalisis. Proses ini dapat memakan biaya yang cukup mahal.
- Drive imaging hardware lebih murah dan memungkinkan untuk melakukan copy cepat suatu data dari sistem yang diselidiki.
- Wiper drive sering digunakan untuk overwrite semua data pada hard disk dan partisi. Bridges dapat mengakomodasi berbagai format. Hal ini digunakan untuk mencegah penulisan ke sistem.

Live CD Distros (Pen-Test, Forensics & Recovery)

- BackTrack
- Matriux
- CAINE Live CD
- DEFT Linux
- THE FARMER'S BOOT CD
- FCCU Gnu/Linux Boot CD
- grml
- Helix3 (Helix3 Pro)
- MacQuisition Boot CD
- Masterkey Linux
- PlainSight
- Recovery Is Possible
- SAFE Boot Disk
- SMART Linux
- SPADA
- Windows Forensic Environment (aka WinFE, Windows FE)

BackTrack
Sebuah Live CD yang dibangun di atas dari Ubuntu (versi awal dibangun di atas dari Slackware). Terbaru "pre-release" memiliki "modus forensik".
http://remote-exploit.org/backtrack.html

Matriux
Sebuah Live CD berdasarkan Debain memiliki banyak alat untuk forensik komputer dan respon insiden.
http://www.matriux.com/

Caine Live CD
Sebuah Live CD forensik dibangun di atas Ubuntu.
http://caine-live.net

Live CD Distros (Pen-Test, Forensics & Recovery)

- BackTrack
- Matriux
- CAINE Live CD
- DEFT Linux
- THE FARMER'S BOOT CD
- FCCU Gnu/Linux Boot CD
- grml
- Helix3 (Helix3 Pro)
- MacQuisition Boot CD
- Masterkey Linux
- PlainSight
- Recovery Is Possible
- SAFE Boot Disk
- SMART Linux
- SPADA
- Windows Forensic Environment (aka WinFE, Windows FE)

Cekatan Linux

Sebuah Live CD yang dibangun di atas Xubuntu dengan alat terbaik untuk forensik komputer dan respon insiden.

Ini adalah sistem hidup yang sangat ringan dan cepat dibuat untuk spesialis Forensik Komputer.

Live CD pertama dengan AFF, dhash dan Xplico.

http://www.deftlinux.net

PETANI'S THE CD BOOT

Sebuah Linux Live CD, dirancang dan dioptimalkan untuk melihat pratinjau data dengan cara forensik suara. Ini berisi sejumlah program praktisi forensik dapat memanfaatkan untuk melihat kedua sistem Windows dan Linux.

Live CD Distros (Pen-Test, Forensics & Recovery)

- BackTrack
- Matriux
- CAINE Live CD
- DEFT Linux
- THE FARMER'S BOOT CD
- FCCU Gnu/Linux Boot CD
- grml
- Helix3 (Helix3 Pro)
- MacQuisition Boot CD
- Masterkey Linux
- PlainSight
- Recovery Is Possible
- SAFE Boot Disk
- SMART Linux
- SPADA
- Windows Forensic Environment (aka WinFE, Windows FE)

FCCU GNU / Linux Boot CD
Sebuah Live CD yang dibangun di atas Debian Live dengan banyak alat dengan tujuan forensik.
http://www.lnx4n6.be

grml
Sebuah Live CD forensik dibangun di atas Debian.
http://grml.org

Helix3 (Helix3 Pro)
Sebuah Live CD yang dibangun di atas Ubuntu dengan alat khusus untuk respon insiden dan penemuan elektronik.
http://e-fense.com

MacQuisition Boot CD
Sebuah Live CD forensik dibangun untuk sistem pencitraan Macintosh.

Live CD Distros (Pen-Test, Forensics & Recovery)

- BackTrack
- Matriux
- CAINE Live CD
- DEFT Linux
- THE FARMER'S BOOT CD
- FCCU Gnu/Linux Boot CD
- grml
- Helix3 (Helix3 Pro)
- MacQuisition Boot CD
- Masterkey Linux
- PlainSight
- Recovery Is Possible
- SAFE Boot Disk
- SMART Linux
- SPADA
- Windows Forensic Environment (aka WinFE, Windows FE)

Masterkey Linux
Sebuah Live CD Linux dibangun di atas Slackware menampilkan berbagai macam alat bebas dan sumber terbuka, fokus pada kedua Respon Insiden dan Pemeriksaan Forensik Komputer.
http://masterkeylinux.com

PlainSight
Sebuah Live CD forensik dibangun di atas Knoppix.
http://www.plainsight.info

Pemulihan Apakah Kemungkinan
Sebuah Live CD Linux dengan sejumlah aplikasi pemulihan seperti TestDisk, PhotoRec, dll
http://www.tux.org/pub/people/kent-robotti/looplinux/rip/

Live CD Distros (Pen-Test, Forensics & Recovery)

- BackTrack
- Matriux
- CAINE Live CD
- DEFT Linux
- THE FARMER'S BOOT CD
- FCCU Gnu/Linux Boot CD
- grml
- Helix3 (Helix3 Pro)
- MacQuisition Boot CD
- Masterkey Linux
- PlainSight
- Recovery Is Possible
- SAFE Boot Disk
- SMART Linux
- SPADA
- Windows Forensic Environment (aka WinFE, Windows FE)

AMAN Boot Disk

Yang forensik suara pertama dan hanya tersedia secara komersial Boot Windows disk.

Termasuk built-in mendukung driver, akses ke sistem file NTFS dan built-in perangkat lunak memblokir menulis.

http://www.forensicsoft.com/catalog/product.php

SMART Linux

Dua Live CD dibangun di atas dari Slackware dan Ubuntu. Termasuk alat-alat forensik SMART dan lainnya.

http://asrdata2.com

Live CD Distros (Pen-Test, Forensics & Recovery)

- BackTrack
- Matriux
- CAINE Live CD
- DEFT Linux
- THE FARMER'S BOOT CD
- FCCU Gnu/Linux Boot CD
- grml
- Helix3 (Helix3 Pro)
- MacQuisition Boot CD
- Masterkey Linux
- PlainSight
- Recovery Is Possible
- SAFE Boot Disk
- SMART Linux
- SPADA
- Windows Forensic Environment (aka WinFE, Windows FE)

SPADA

Sebuah Live CD forensik dibangun di atas Knoppix.

http://spada-cd.info

Jendela Forensik Lingkungan (alias WinFE, Windows FE)

Sebuah CD Windows forensik didasarkan didasarkan dari Lingkungan Pra-Instalasi Windows.