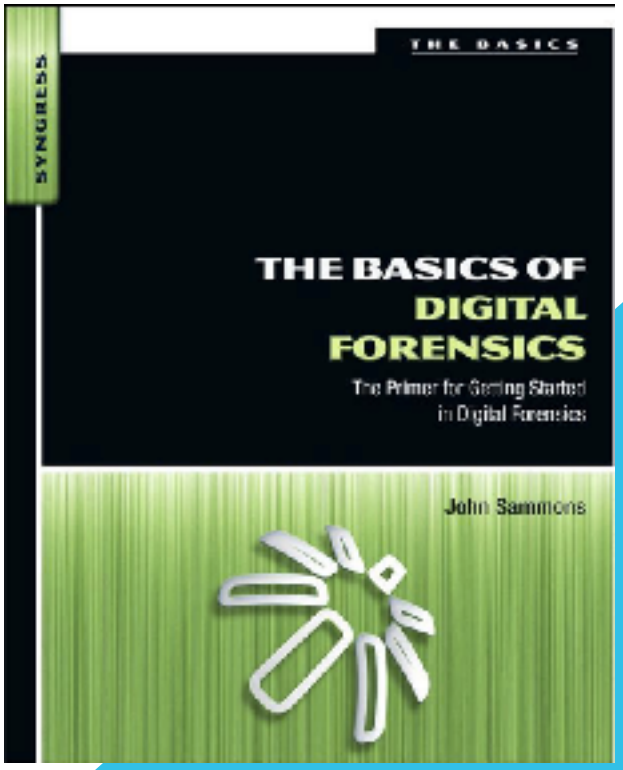


6. ANTIFORENSICS

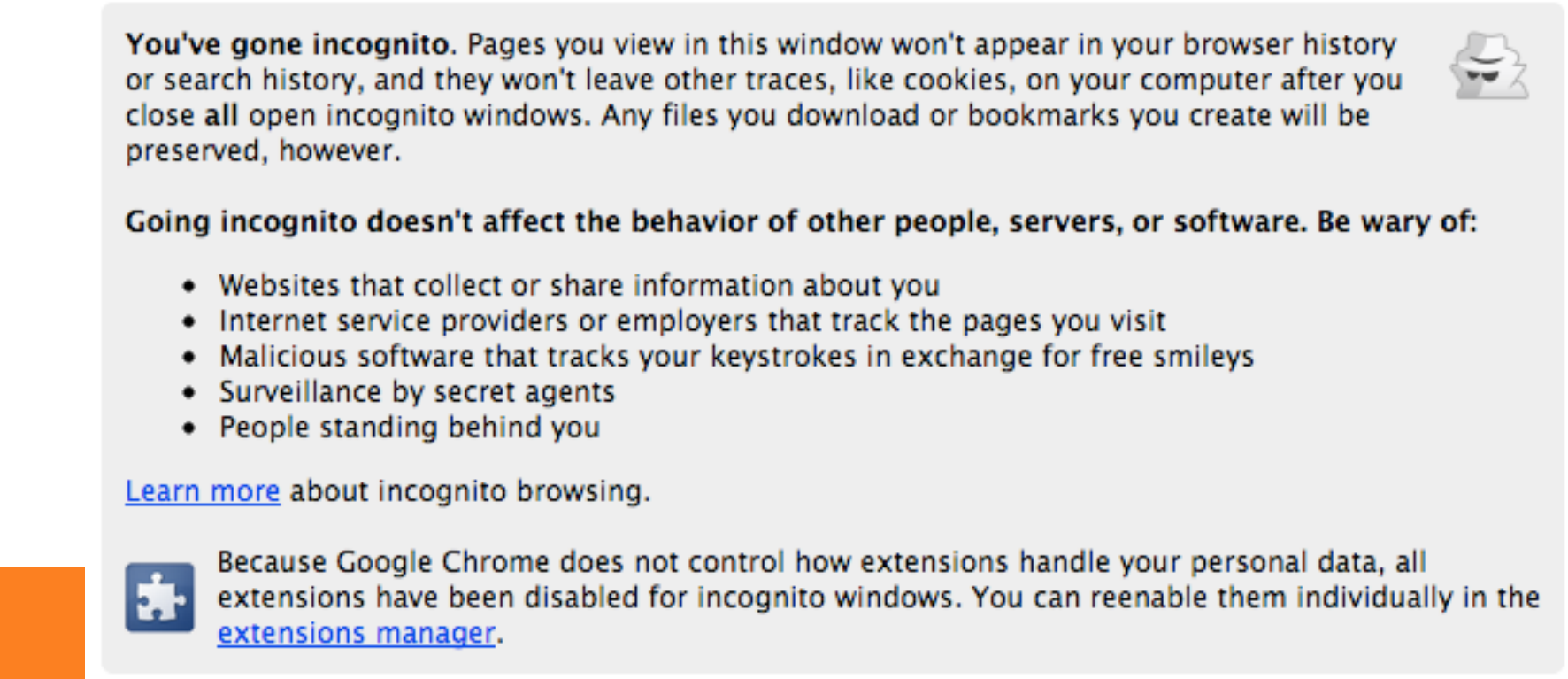
TOPIK

- Encryption
- Breaking Encryption
- Hiding and Destroying Data

ANTIFORENSICS

- Teknik untuk memanipulasi, menghapus, atau mengaburkan data digital untuk membuat pemeriksaan menjadi sulit, memakan waktu, atau hampir mustahil

PRIVATE BROWSING



METODA PRIVACY SEDERHANA

- **Lemah, relatif tidak efektif**
  - Delete cookies
  - Clear temporary internet files
  - Clear history
  - Merubah filenames dan extensions
  - Menyimpan file dalam direktori yang tidak terkait
- **Tantangan sebenarnya bagi pemeriksa forensik**
  - Menyembunyikan file dalam file lain (**steganography**)
  - **Encryption**

ENCRYPTION

MEMPROTEKSI SECRETS

- Kita semua membutuhkan enkripsi untuk
  - Credit card #s
  - Passwords
  - Medical data
- Tanpa enkripsi, Web akan kurang berguna

DEFENISI ENCRYPTION

- Enkripsi mengkonversi data dari plaintext (dapat dibaca) ke ciphertext (acak)
- Algoritma adalah proses matematis untuk mengenkripsi dan mendekripsi pesan
- Key adalah nilai yang diperlukan untuk mengenkripsi dan mendekripsi data, biasanya berupa serangkaian bit acak, yang kadang-kadang berasal dari kata sandi atau frasa sandi

CAESAR CIPHER

Menggeser setiap huruf satu karakter ke depan

ABCDEFGHIJKLMNOPQRSTUVWXYZ

BCDEFGHIJKLMNOPQRSTUVWXYZA

CCSF –> DDTG

ROT13

- Menggeser setiap huruf 13 karakter ke depan

ABCDEFGHIJKLMNOPQRSTUVWXYZ

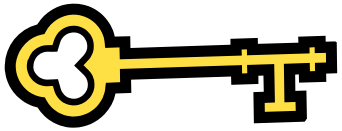
NOPQRSTUVWXYZABCDEFGHIJKLM

CCSF –> PPFS → CCSF

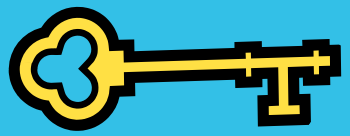
- Enkripsi dengan ROT13 dua kali akan mengembalikan Anda ke plaintext
- Algoritma dekripsi = Algoritma Enkripsi
- Sangat lemah-membingungkan, bukan enkripsi
- Digunakan dalam registry key TypedURLs, dan password dalam versi awal Netscape (Link Ch 6a: ROT13 - Wikipedia)

SYMMETRIC CRYPTOGRAPHY

- Satu kunci untuk encrypts dan decrypts data
- Cleartext dengan Key menjadi Ciphertext

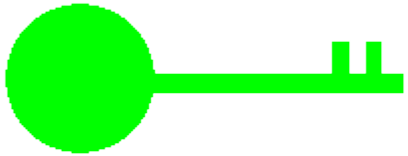
Winning Lotto #s:  aWDHOP#@-w9

- Ciphertext dengan Key menjadi Cleartext

aWDHOP#@-w9  Winning Lotto #s:

ALGORITMA ASYMMETRIC CRYPTOGRAPHY

- **Menggunakan dua kunci yang secara matematis berhubungan**
  - Data dienkripsi dengan salah satu kunci dapat didekripsi hanya dengan kunci lainnya
- **Nama lain untuk kriptografi kunci asimetrik adalah kriptografi kunci publik**
  - Public key: dikrtahui public (umum)

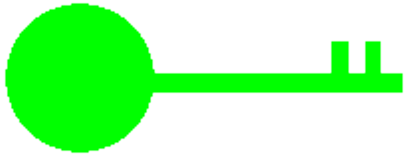


  - Private key: hanya diketahui owner

ASYMMETRIC CRYPTOGRAPHY

- Cleartext dengan Public Key menjadi Ciphertext

Winning Lotto #s:



aWDHOP#@-w9

- Ciphertext dengan Private Key menjadi Cleartext

aWDHOP#@-w9

Winning Lotto #s:

ALGORITHMA POPULAR

- Symmetric Encryption
  - DES, 3DES, AES, Blowfish
- Asymmetric Encryption
  - RSA, ECC, ElGamal
- Algoritma yang paling aman adalah open-source
  - Proprietary, secret algoritma rahasia hampir seringkali tidak aman

KEYS

- **Urutan bit acak**
  - Rentang nilai yang diijinkan disebut *keyspace*
- **Semakin besar *keyspace*, semakin aman kunci**
  - 8-bit key memiliki $2^8 = 256$ values dalam *keyspace*
  - 24-bit key memiliki $2^{24} = 16$ million values
  - 56-bit key memiliki $2^{56} = 7 \times 10^{16}$ values
  - 128-bit key memiliki $2^{128} = 3 \times 10^{38}$ values

BRUTE FORCE ATTACK

- **1997 kunci 56-bit bisa dipecahkan menggunakan brute force**
  - Menguji semua kemungkinan kunci 56-bit
  - Digunakan 14.000 komputer yang diatur melalui Internet
  - Butuh waktu 3 bulan

  See link http://en.wikipedia.org/wiki/EFF_DES_cracker

BERAPA BANYAK BITS YANG DIPERLUKAN?

- **Berapa banyak kunci yang bisa diuji oleh semua komputer di bumi dalam setahun?**
  - Pentium 4 processor: 10^9 cycles per second
  - 1 tahun = 3 x 10^7 seconds
  - Terdapat kurang lebih 10^{10} komputer di bumi
    - Satu untuk tiap orang
  - 10^9 x 3 x 10^7 x 10^{10} = 3 x 10^{26} perhitungan
  - 128 bits membutuhkan(3 x 10^{38} values)
    - Kecuali komputer bisa lebih cepat, atau seseorang bisa memecahkan algoritma

PANJANG KUNCI SECARA PRAKTIS

- Kunci privat 128 bit atau lebih secara praktis belum bisa dipecahkan sampai saat ini
- Kunci publik harus lebih panjang
  - 2048 bit adalah panjang minimum yang disarankan ukuran kunci untuk RSA (Link Ch 6b: NIST Special Publication 800-78-3 – recommends 2048 bits for RSA keys)

PRODUK ENKRIPSI YANG UMUM

- Windows 7: BitLocker dan EFS
- Apple: FileVault
- Linux: TrueCrypt

- Full Disk Encryption
  - Lebih aman
  - Tidak mengenkrip "boot partisi"
- File dan Folder enkripsi

ENCRYPTING FILE SYSTEM (EFS)

- Pada File Properties di Windows
- Mudah digunakan
- Menggunakan password untuk membuat kunci
- Bagian dari NTFS file system

BITLOCKER

- Mengenkripsi seluruh partisi sistem
- BitLocker To Go mengenkripsi stik USB
- Membutuhkan Windows 7 Ultimate
  - Tapi tersedia di semua versi Windows 8
- Menggunakan Trusted Platform Module chip
- Metode forensik Terbaik: seize the running, logged-in machine
  - Saat itu BitLocker didekripsi

APPLE FILEVAULT

- 128 bit AES
- Dapat mengenkripsi seluruh drive
- Keys dapat diback up dengan Apple

TRUECRYPT

- Free software open-source
- Berjalan pada Linux, Mac, atau Windows
- Dapat mengenkripsi sebagian atau seluruh disk
- Bisa menggunakan AES, Serpent, atau Twofish
- Menggunakan Kunci 256-bit

BREAKING ENCRYPTION

MEMECAHKAN PASSWORDS

- Tanya ke user
- Brute force attack
  - Menggunakan setiap kemungkinan kombinasi karakterGunakan setiap kemungkinan kombinasi karakter
- Dictionary attack
  - Menggunakan password dari kamus password yang umum
- Reset Passwords
  - Memungkinkann dengan hak administrator atau tool hacking seperti UBCD
  - Tidak akan membuat Anda mendapatkan file EFS-dienkripsi

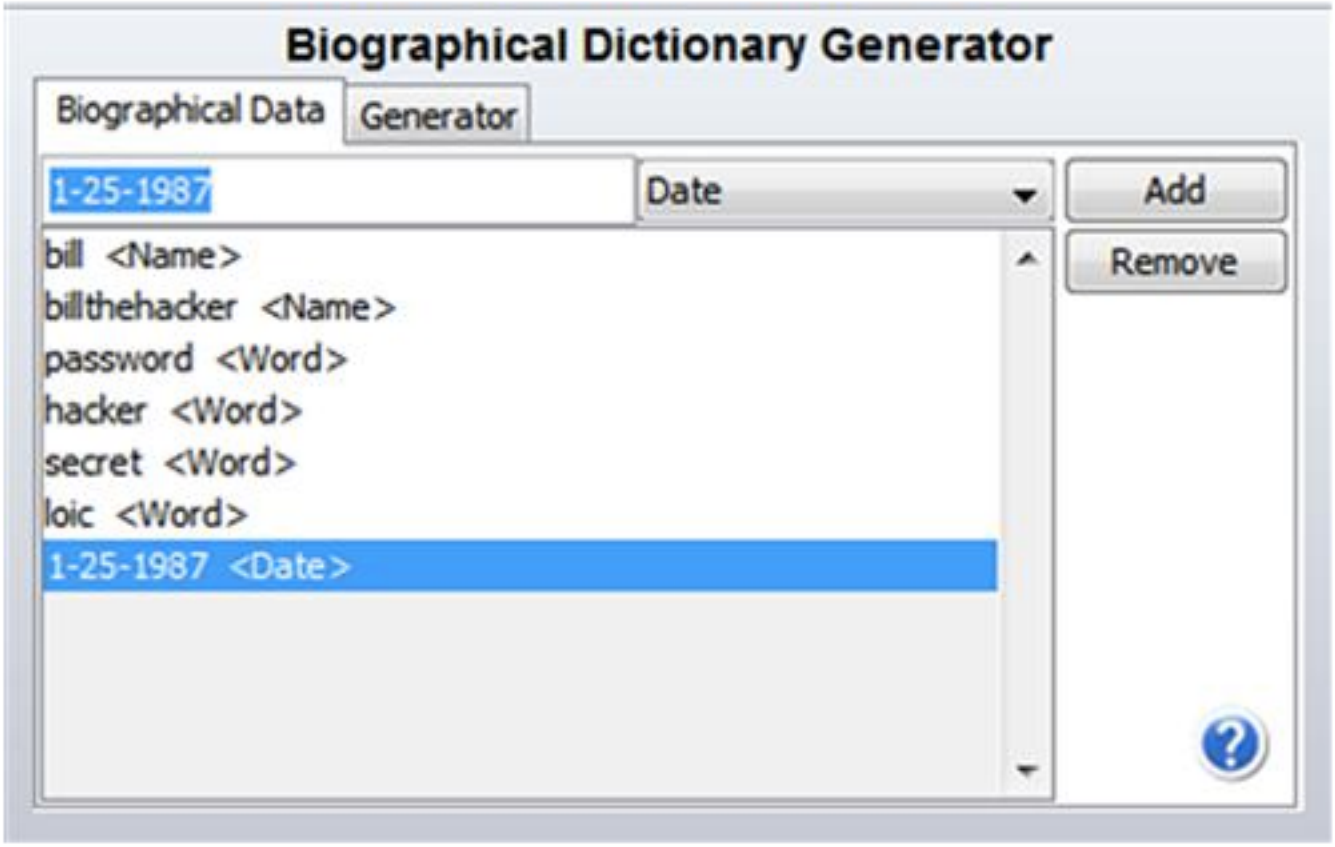
CUSTOM DICTIONARY

- Mengakuisisi hard disk (dan RAM, jika mungkin) dari komputer bukti
- Ekstrak semua string
- Menggunakannya sebagai kamus sandi

PASSWORD CRACKING TOOLS

- Password Recovery Toolkit (PRTK) dari AccessData
- John the Ripper
- Cain
- Ophcrack
- Hashcat (di Backtrack)

PRTK'S BIOGRAPHICAL DICTIONARY GENERATOR



1	b25billthehacker	251987secret
25	billthehacker251b	251987 secret
1987	billthehacker125b	secret1987h
1251987	b251billthehacker	h1987secret
billbill	b125billthehacker	secret198725h
bill bill	25billthehacker1b	secret251987h
bill-bill	25b1billthehacker	h198725secret
bill_bill	1billthehacker25b	h251987secret
billb	1b25billthehacker	1987secret25h
bill b	billthehacker1b25	1987h25secret
bill-b	b1billthehacker25	25secret1987h
bill_b	billthehacker25b1	25h1987secret
billbillthehacker	b25billthehacker1	secret25h1987
bill billthehacker	billthehacker25bill	h25secret1987
bill-billthehacker	bill25billthehacker	secret1987h25
bill_billthehacker	billthehacker251bill	h1987secret25
billb	billthehacker125bill	secret1987
bill b	bill251billthehacker	secret 1987
bill-b	bill125billthehacker	1987secret
bill_b	25billthehacker1bill	1987 secret
	25bill1billthehacker	

MEMECAHKAN BITLOCKER

- Cold Boot Attack
  - Membekukan RAM dan recover key
- Melepaskan chip TPM dan memulihkan kunci dengan

- Keduanya exotic, impractical attacks
- Pengguna mungkin telah memback up kunci di akun Microsoft (Ch Ch 6c: View Your BitLocker Recovery Key in Your Microsoft Account/)

STEGANOGRAPHY

STEGANOGRAPHY

- Menyembunyikan file payload dalam file carrier lain
- Digunakan oleh Osama Bin Laden dan mata-mata Rusia

(link Ch)

Ch 6d: Busted Alleged Russian Spies Used Steganography To Conceal Communications

Busted Alleged Russian Spies Used Steganography To Conceal Communications

'Deep-cover' Russian intelligence agents hid electronic messages behind computer images

Jun 29, 2010 | 06:46 PM | 0 Comments

To date, forensics and security experts have mostly considered steganography too complex to be much of a mainstream threat. But a study by Purdue University in late 2007 found that some criminals, indeed, were using steganography tools, mainly in child pornography and financial fraud activities. Purdue's preliminary research showed proof that steganography tools were installed on convicted criminals' computers in some cases.

STEGANOGRAPHY DETECTION TOOLS

Check Out Our Industry-Leading Steganalysis Products and Services:

StegAlyzerAS
Steganography Analyzer Artifact Scanner

Detect files and registry entries associated with steganography applications!

StegAlyzerSS
Steganography Analyzer Signature Scanner

Detect files containing steganography and extract the hidden information!

StegAlyzer FS

StegAlyzerFS
Steganography Analyzer Field Scanner

Perform rapid field triage for steganography artifacts and signatures!

StegAlyzerRTS
Steganography Analyzer Real-Time Scanner

Detect steganography artifacts and signatures in real-time over a network!

SARC Certified Steganography Examiner

Certified Steganography Examiner Training
Raise Your Threshold of Perception

Learn how to effectively detect and extract steganography!

Link Ch 6e

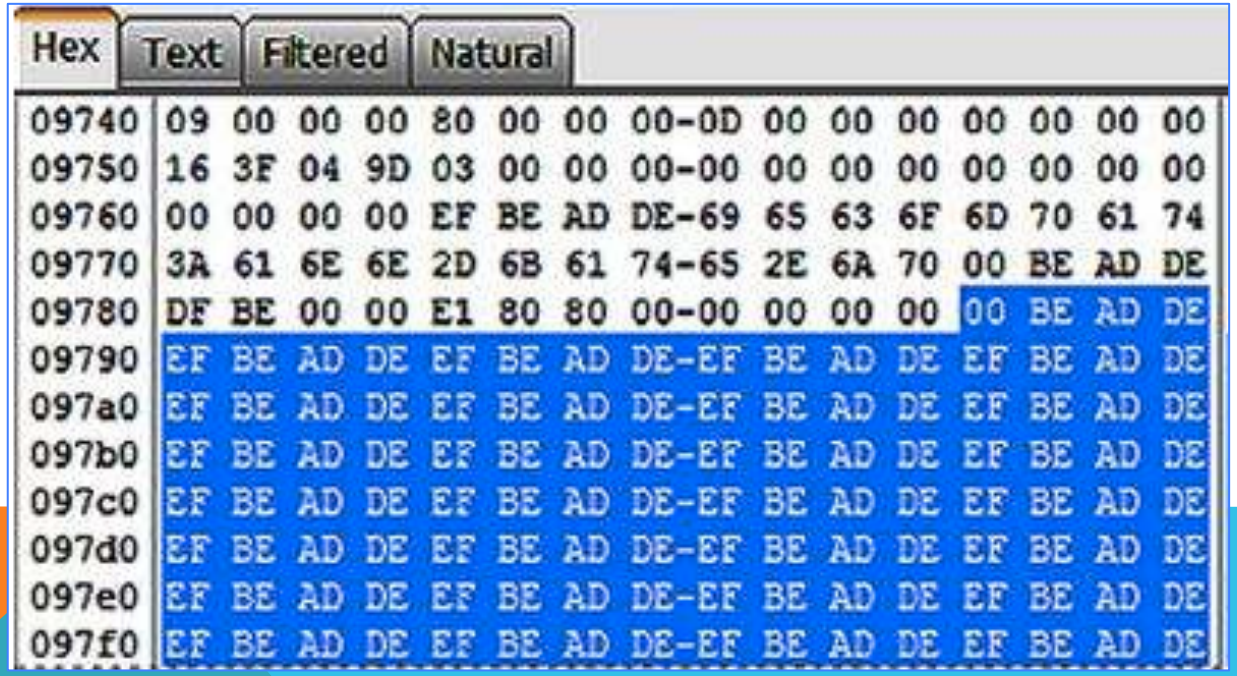
MENYEMBUNYIKAN DAN MERUSAK DATA

MERUSAK DATA

- Drive Wiping
  - Darik's Boot and Nuke (DBAN)
  - Window Washer
  - Evidence Eliminator
  - Mac OS X Secure Erase
    - Banyak lagi
- Beberapa tools menghapus seluruh disk, beberapa tools hanya menghapus file atau blok yang tidak terpakai, yang lain hanya menghapus header & footer
- Keberadaan tool ini dapat dianggap sebagai barang bukti memberatkan di pengadilan
  - Terutama jika tool digunakan sebelum penyitaan barang bukti

BEBERAPA TOOLS WIPERS MENGGUNKAN POLA BERULANG

- Ini adalah tanda adanya penghapusan disk



DEFRAGMENTASI

- Memindahkan cluster untuk merapikan disk
- Membuat file bisa terbuka lebih cepat
- Mengakibatkan beberapa sektor akan ditimpa
- Secara Otomatis dilakukan setiap minggu di Windows 7