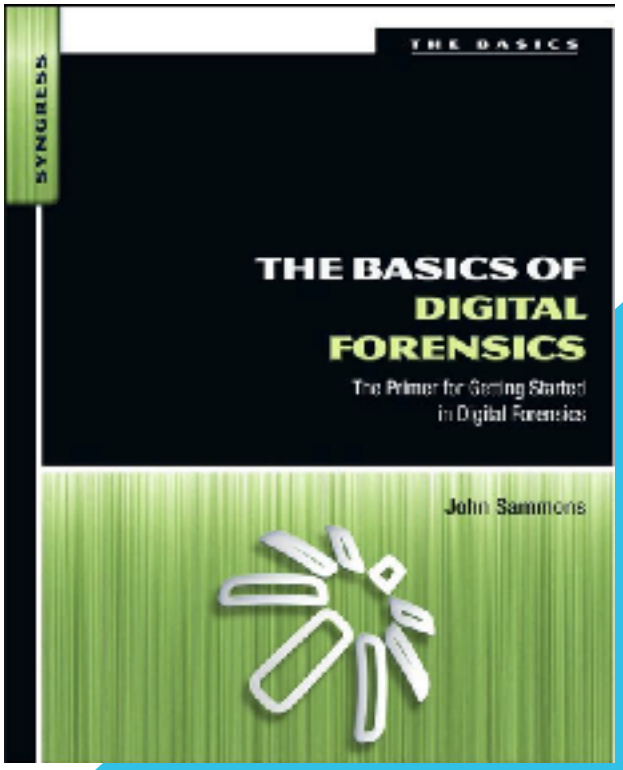


2. KEY TECHNICAL CONCEPTS

TOPIK

- **Operasi Dasar Komputer**
- **Bits & Bytes**
- **File Extensions & File Signatures**
- **Bagaimana Komputer Menyimpan Data**
- **RAM: Random Access Memory**
- **Volatilitas Data**

TOPICS

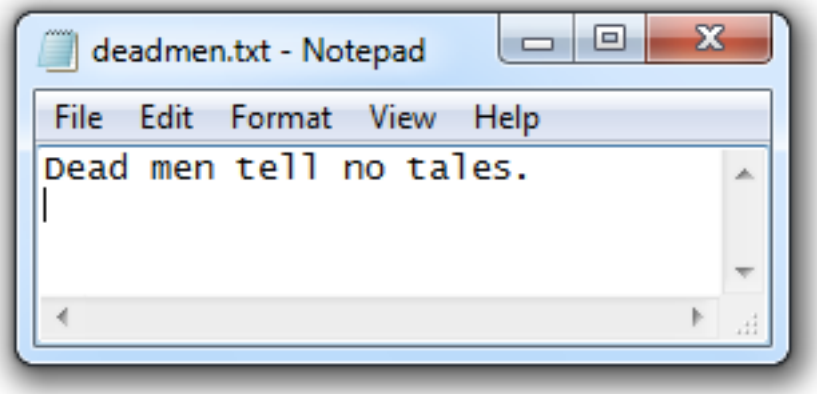
- **Perbedaan Antar Lingkungan Komputer**
- **Aktif, Laten, dan Data Arsip**
- **Alokasi dan Unlokasi Space**
- **Sistem File Komputer**

BITS & BYTES

BITS & BYTES

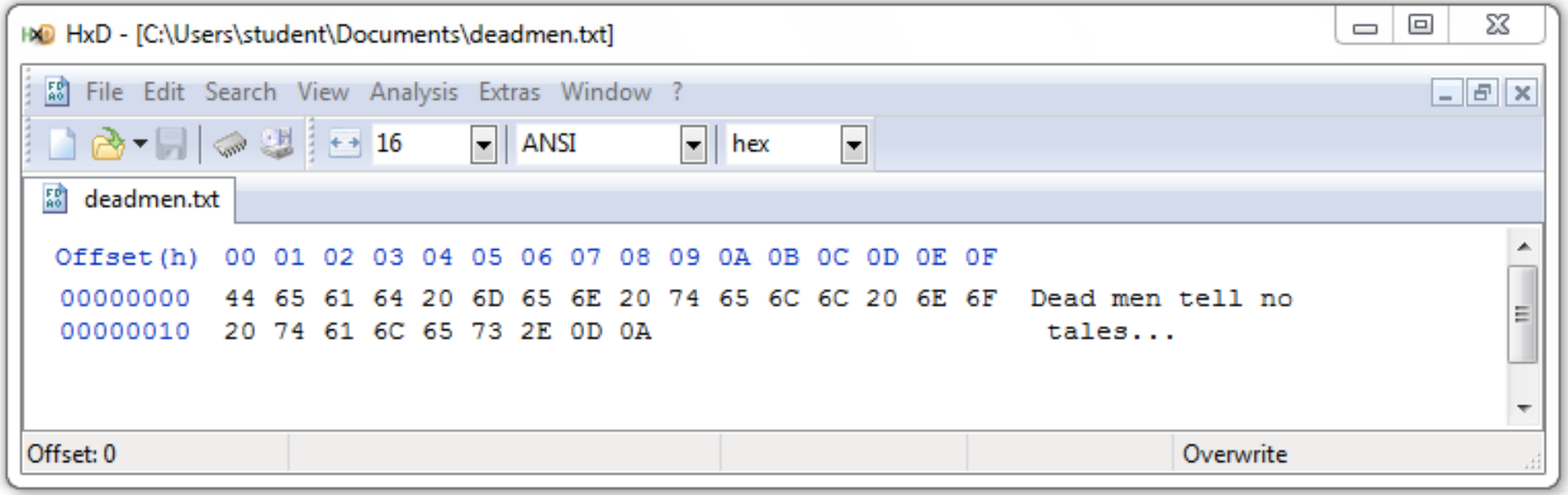
- Bit terdiri dari 0 atau 1
- Tiap 8 bits adalah byte
  - 00000000 sampai 11111111
  - Ada 256 kemungkinan bytes
  - Bisa ditulis sebagai angka 0 hingga 255 (desimal)
  - Dalam Hexadecimal, 00 hingga FF
- Binary Games

TEXT ASCII



- Satu byte tiap karakter
- 7 bits untuk encode character, satu bit paritas
- 94 printable characters
- Awalnya digunakan untuk Bahasa Inggris
- Diadaptasi oleh bahasa lainnya

ASCII FILE DALAM HEXADECIMAL



20 hex = 32 decimal = SPACE

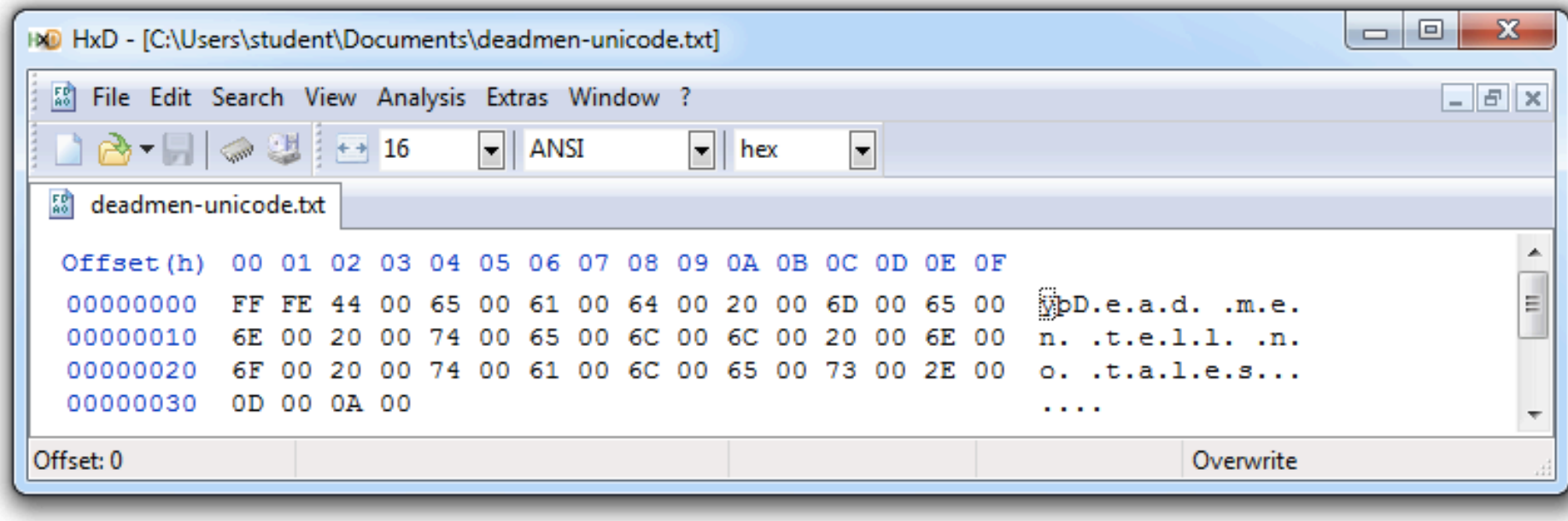
0D 0A = 13 10 = CR LF

ASCII

Binary	Oct	Dec	Hex	Abbr	[a]	[b]	[c]	Name
000 0000	000	0	00	NUL	$^{N}_{U}{}_{L}$	^@	\0	Null character
000 0001	001	1	01	SOH	$^{S}_{O}{}_{H}$	^A		Start of Header
000 0010	002	2	02	STX	$^{S}_{T}{}_{X}$	^B		Start of Text
000 0011	003	3	03	ETX	$^{E}_{T}{}_{X}$	^C		End of Text
000 0100	004	4	04	EOT	$^{E}_{O}{}_{T}$	^D		End of Transmission
000 0101	005	5	05	ENQ	$^{E}_{N}{}_{Q}$	^E		Enquiry
000 0110	006	6	06	ACK	$^{A}_{C}{}_{K}$	^F		Acknowledgment
000 0111	007	7	07	BEL	$^{B}_{E}{}_{L}$	^G	\a	Bell
000 1000	010	8	08	BS	$^{B}_{S}$	^H	\b	Backspace[d][e]
000 1001	011	9	09	HT	$^{H}_{T}$	^I	\t	Horizontal Tab[f]
000 1010	012	10	0A	LF	$^{L}_{F}$	^J	\n	Line feed
000 1011	013	11	0B	VT	$^{V}_{T}$	^K	\v	Vertical Tab
000 1100	014	12	0C	FF	$^{F}_{F}$	^L	\f	Form feed
000 1101	015	13	0D	CR	$^{C}_{R}$	^M	\r	Carriage return[g]

Ch 2a: ASCII - Wikipedia

UNICODE

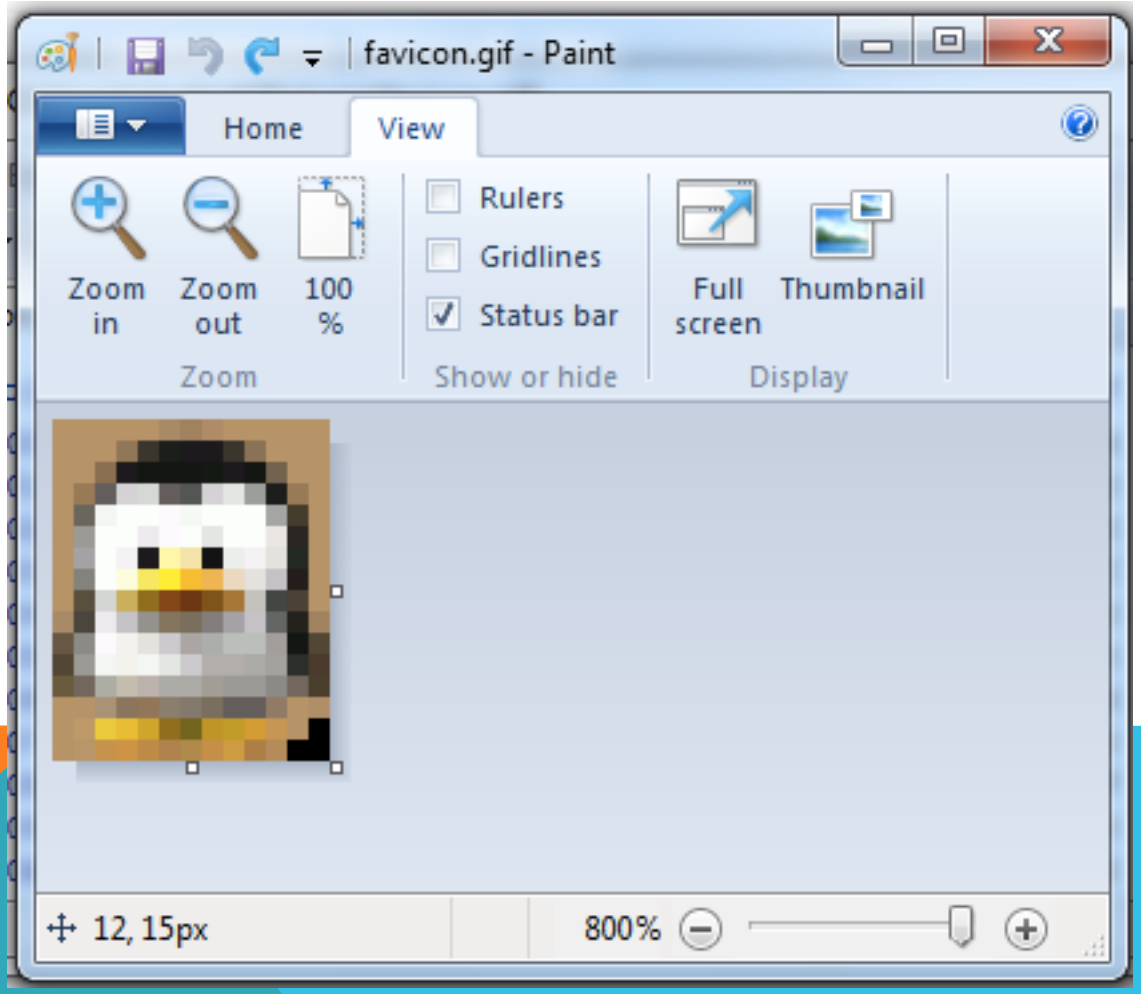


- Mengkodekan semua "commercially significant" languages
- Dua bytes tiap character
- FF FE merupakan awal dari Byte Order Mark

Ch 2c: Byte order mark - Wikipedia

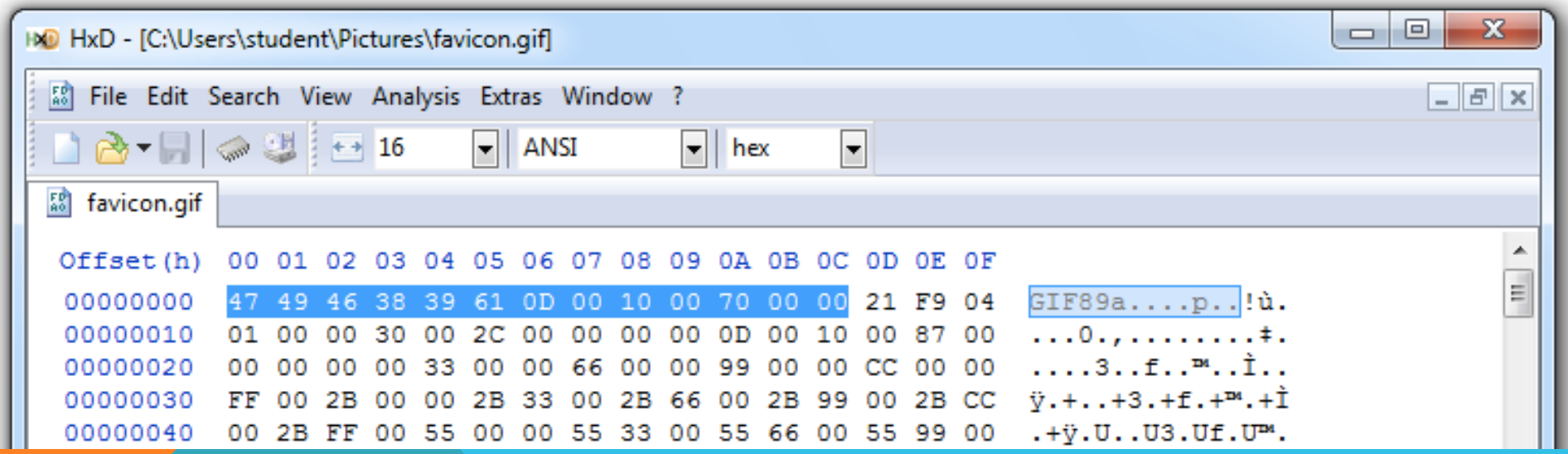
FILE HEADERS & FILE CARVING

GIF IMAGE (13X16 PIXELS)

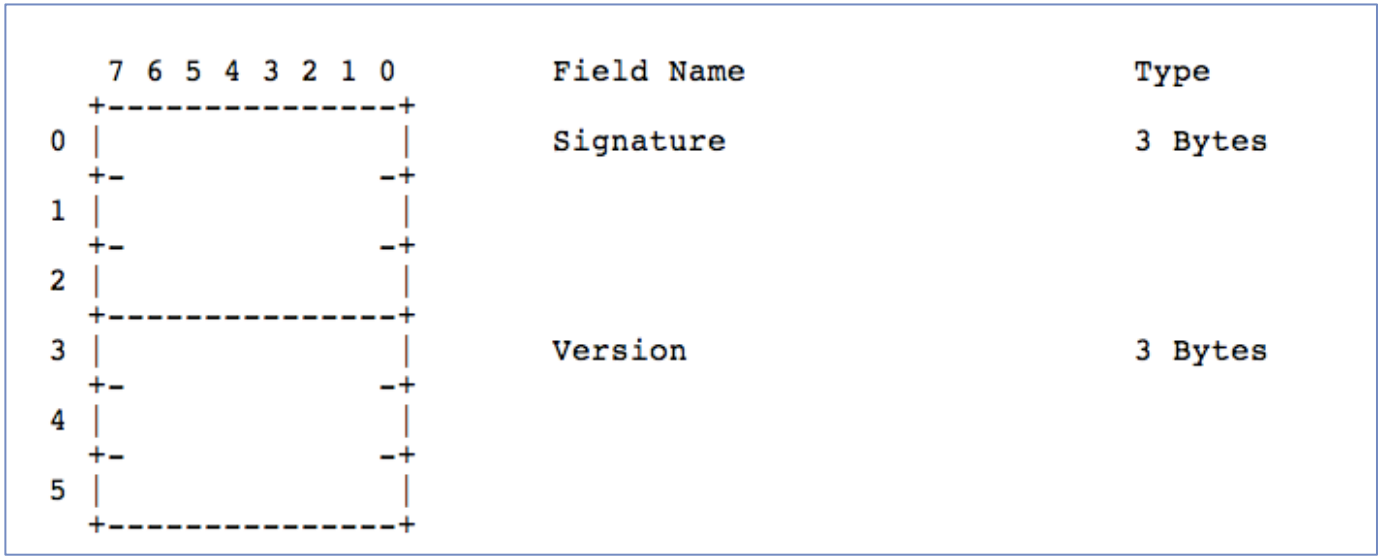


HEADER FILE GIF

- GIF89a – merupakan versi GIF
- 0D 00 10 00 – 13 pixels x 16 pixels



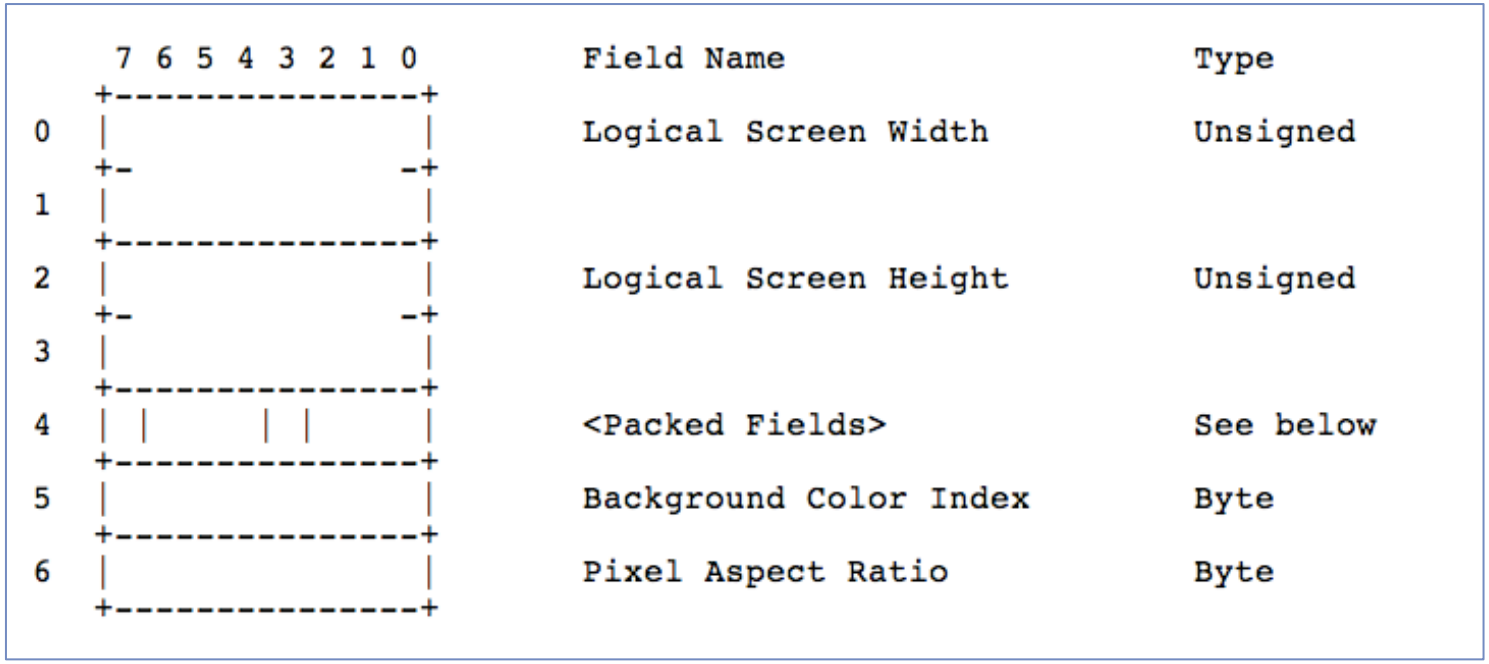
SPESIFIKASI GIF



```
   7 6 5 4 3 2 1 0        Field Name                    Type
  +---------------+
0 |               |       Signature                   3 Bytes
  +-             -+
1 |               |
  +-             -+
2 |               |
  +---------------+
3 |               |       Version                     3 Bytes
  +-             -+
4 |               |
  +-             -+
5 |               |
  +---------------+
```

Ch 2d: GIF Specification (halaman8)

SPESIFIKASI GIF

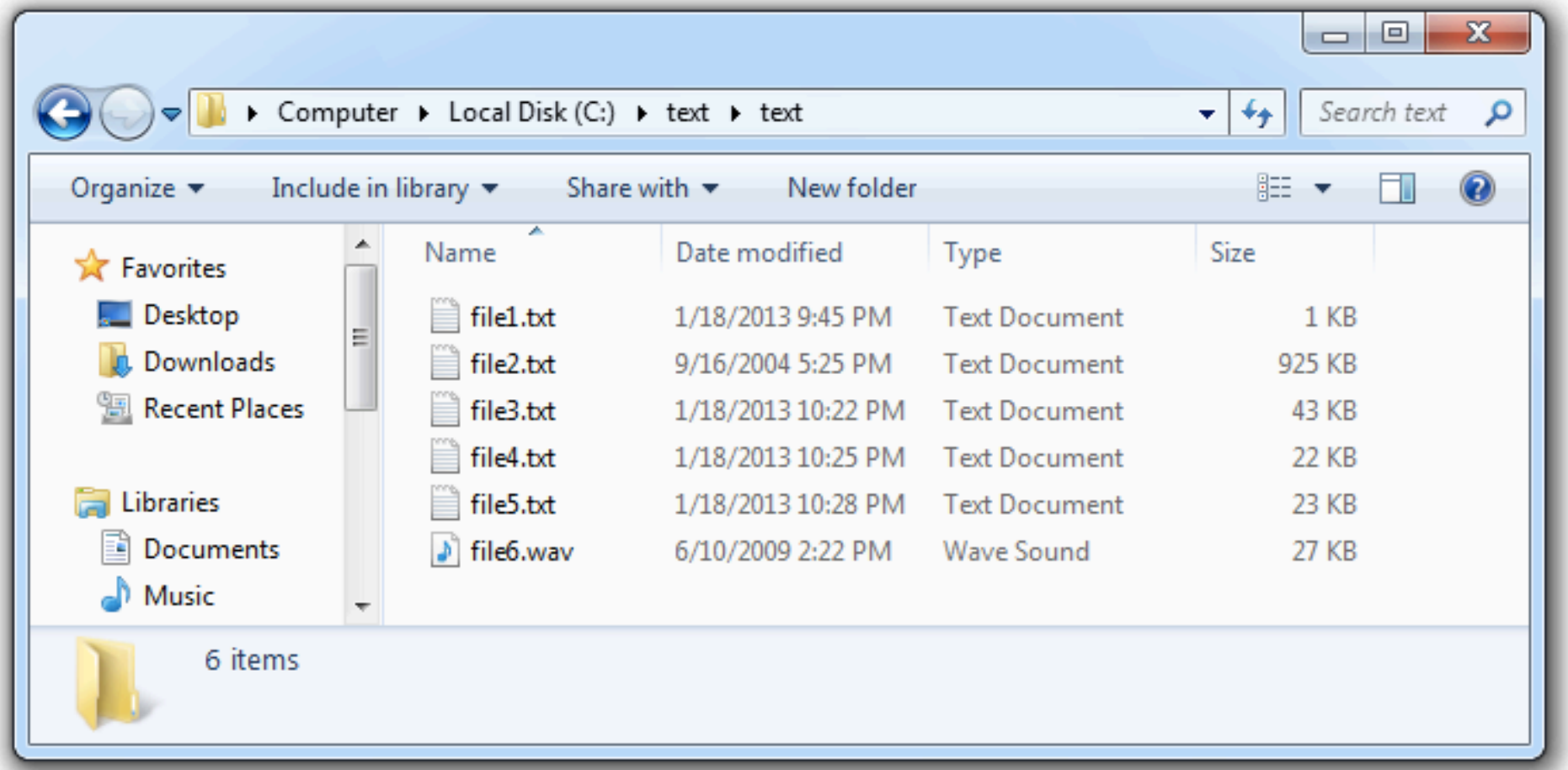


Ch 2d: GIF Specification

FILE CARVING

- Rebuilding files dengan mengatur kembali potongan data yang ditemukan di disk
- Bergantung pada file header dan footer
- Dilakukan secara otomatis oleh beberapa forensic suites seperti FTK dan EnCase
- Banyak tools lain yang bisa untuk mengcarving (menyusun potongan) files

PROJECT X1: MENGIDENTIFIKASI JENIS FILE

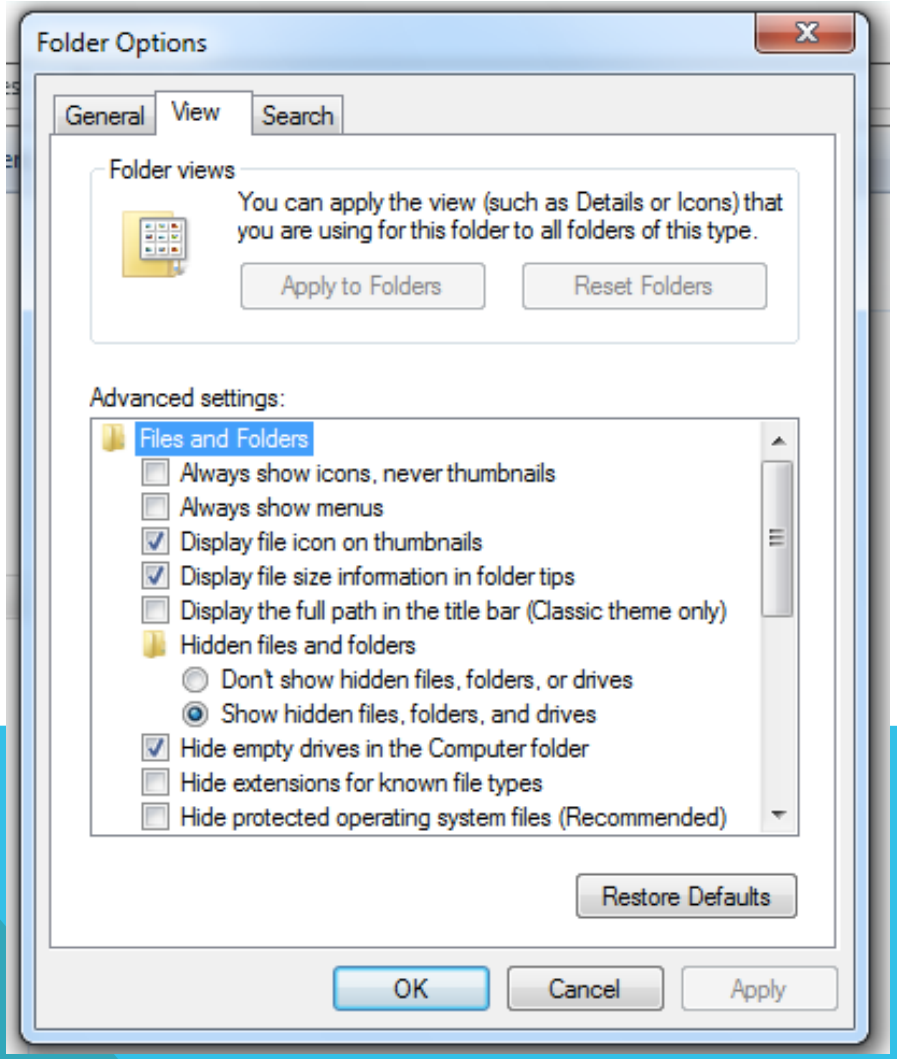


FILE EXTENSIONS & FILE SIGNATURES

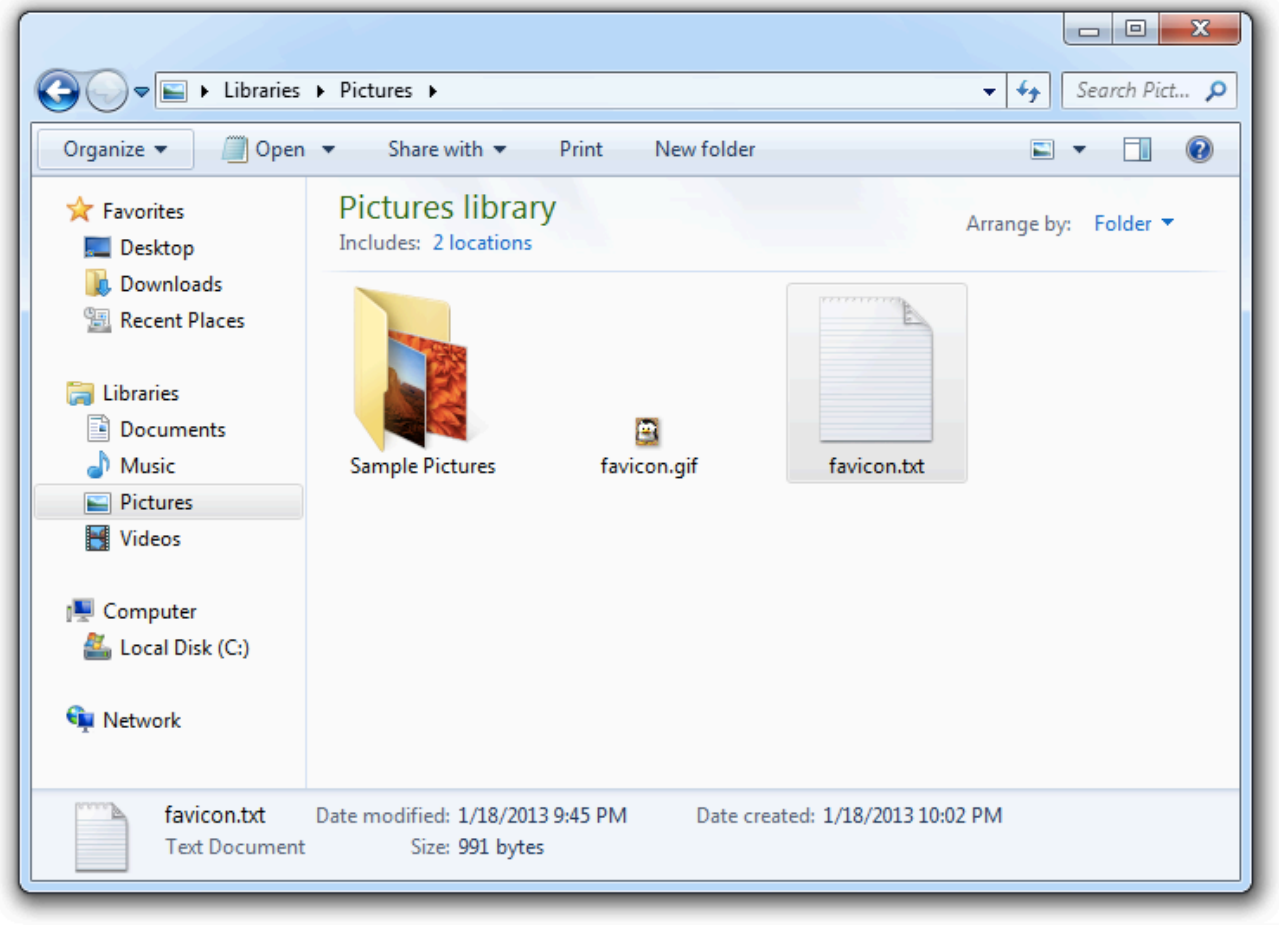
FILE EXTENSIONS

- Biasanya terdiri dari 3 karakter
- Terdapat di ujung nama file, setelah tanda titik
- Di sembunyikan di Windows by default
- Digunakan untuk menentukan jenis file, icon, dan aplikasi default

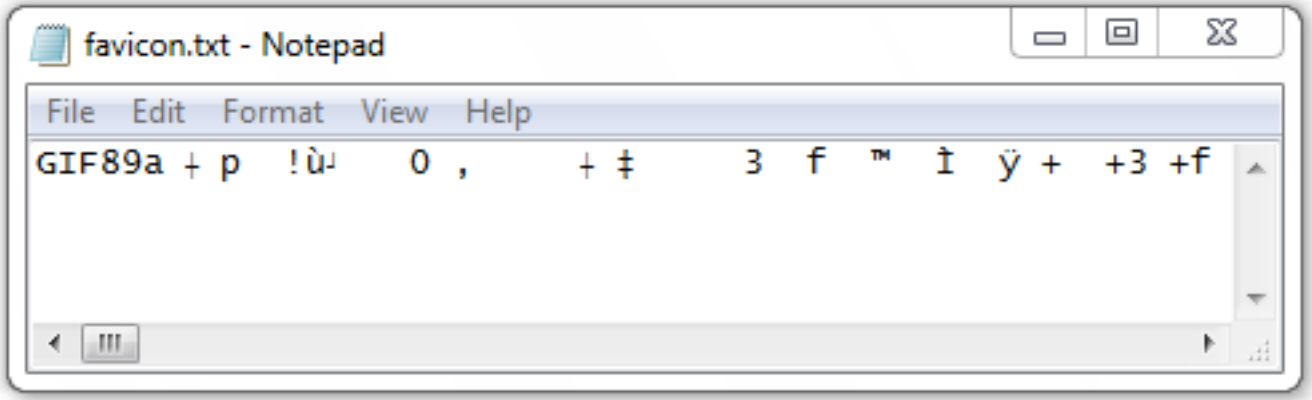
MENYEMBUNYIKAN FILE EXTENSION



MEMPERBAIKI FILE EXTENSION

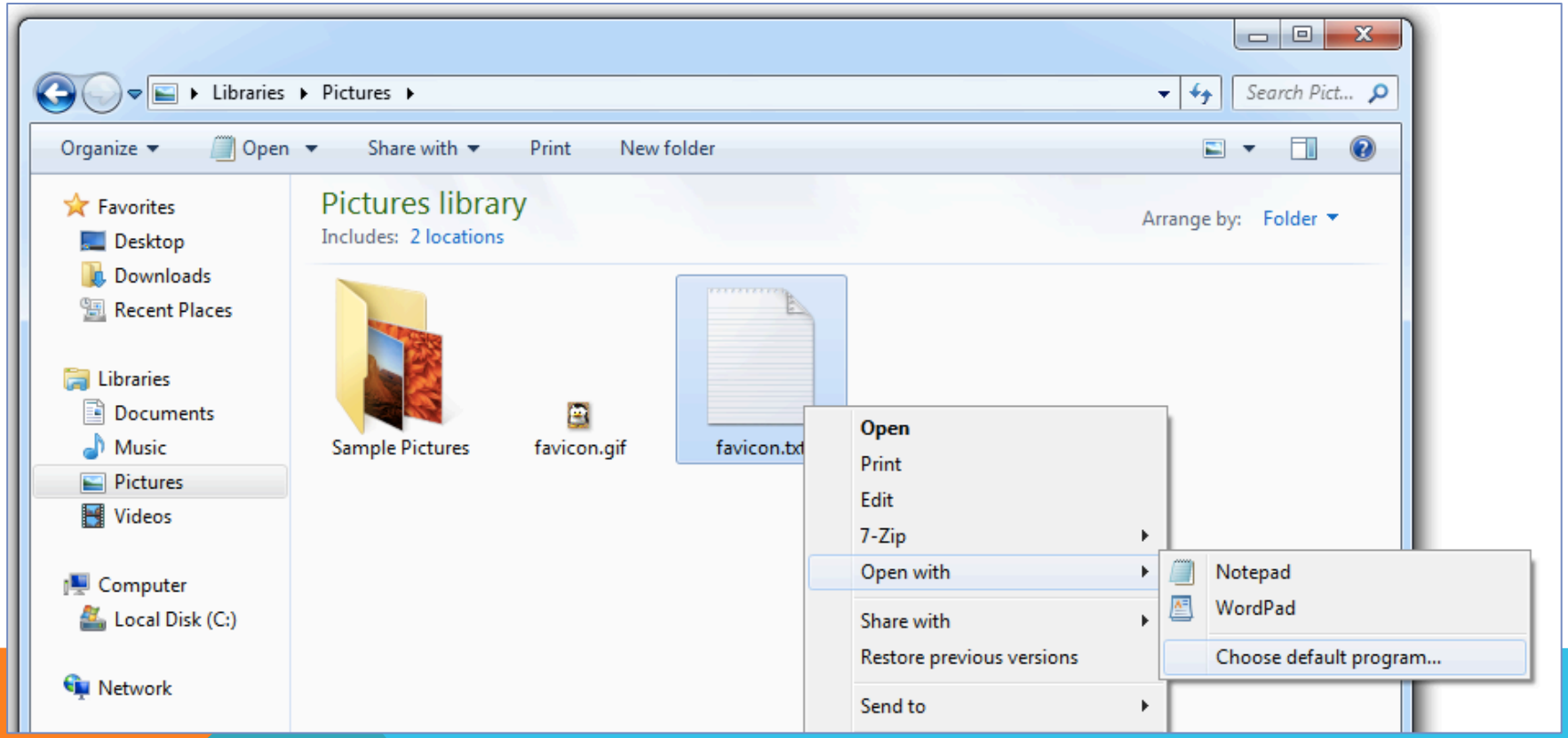


DEFAULT APPLICATION YANG SALAH



- Serangkaian bytes bisa diterjemahkan dalam bentuk ASCII

BUKA DENGAN...


Libraries ▸ Pictures ▸
Search Pict...
Organize
Open
Share with
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Pictures library
Includes: 2 locations
Arrange by: Folder
Sample Pictures
favicon.gif
favicon.txt
Open
Print
Edit
7-Zip
Open with
Share with
Restore previous versions
Send to
Notepad
WordPad
Choose default program...

BAGAIMANA KOMPUTER MENYIMPAN DATA?

STORAGE METHODS

- Electromagnetism
  - Hard disks dan floppy disks
- Microscopic Electrical Transistors
  - SSDs, USB flash drives, SD cards, dll.
- Reflecting Light
  - CDs, DVDs, Blu-ray
- Contoh di atas termasuk nonvolatile – mereka tetap menyimpan data tanpa daya listrik

MAGNETIC DISKS

- Platter berputar di 7.000 rpm sampai 15.000 rpm
- Spindle sebagai porosnya
- Read/write head menggunakan electromagnet yang dipasang ke lengan actuator

Image from textbook

DISK CONTROLLER CARD

- Menyimpan dan mengambil data dari platters
- Dikendalikan oleh firmware yang disimpan dalam Tempat yang terlindungi
- Gambar dari http://static.ddmcdn.com/gif/ide-controller2.jpg

FLASH MEMORY

Terbuat dari transistor

Solid State Devices (SSD)

- Lebih cepat daripada hard disk
- Menggunakan daya lebih sedikit
- lebih mahal

OPTICAL STORAGE

- Microscopic pits encode bits
- Area between pits disebut lands
- Terdapat satu track spiral panjang untuk seluruh disk
- Data dibaca dengan sinar laser

Link

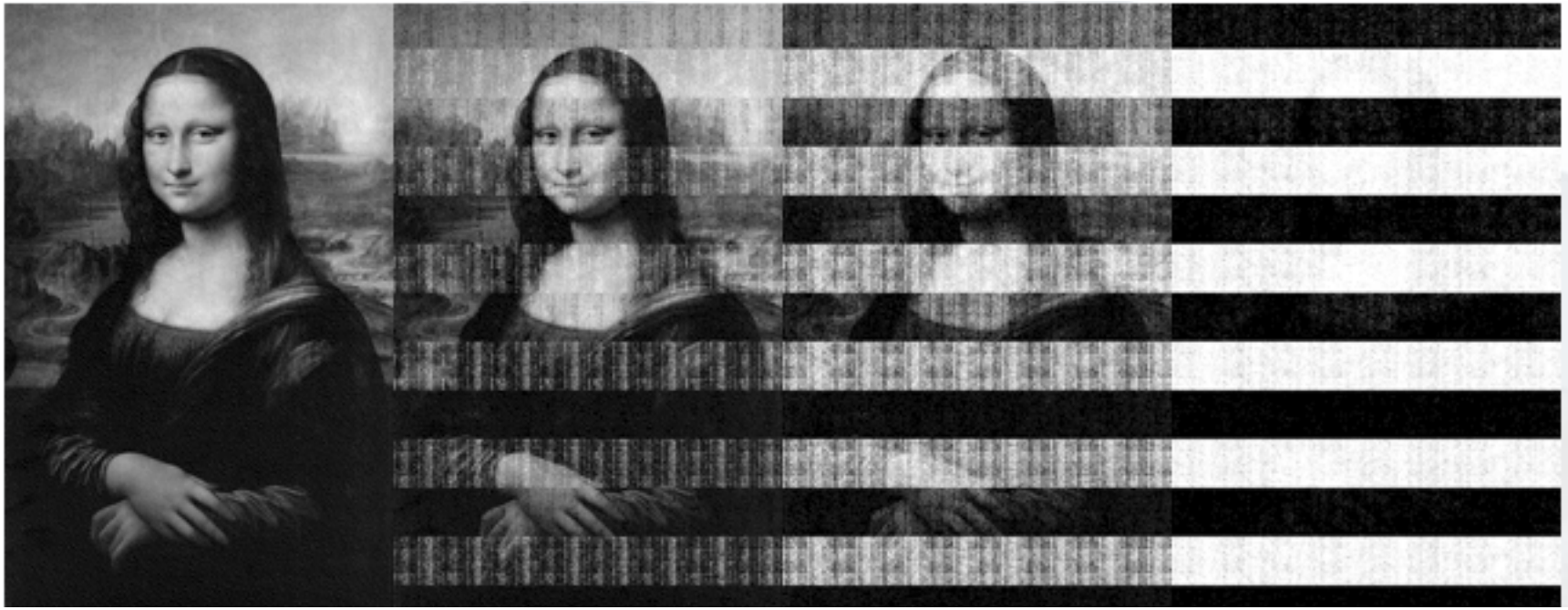
Ch 2e: Compact Disc - Wikipedia

- Image from http://www.backgroundsy.com/file/large/blu-ray-disc-isolated.jpg

VOLATILE V. NONVOLATILE MEMORY

- Memori merupakan media penyimpanan jangka pendek
- Media penyimpanan (hard disk, SSD, dan disk optik) merupakan nonvolatile-data yang disimpan tanpa aliran listrik
- RAM merupakan main system memory
  - RAM termasuk volatile-data hilang saat listrik padam

VOLATILITY RAM



5 sec 30 sec 60 sec 5 min

Link

Ch 2f: Princeton study on data retention in RAM

RAM FORENSICS

- RAM berisi bukti penting yang biasanya tidak tertulis di hard disk
  - Instant messages
  - Network connections
  - Running processes
- Tapi tidak ada time-stamps pada isi RAM
  - Bisa membingungkan

COMPUTING ENVIRONMENTS

EMPAT KATEGORI

- Stand-alone
- Networked
- Mainframe
- Cloud

STAND-ALONE

Komputer yang tidak terhubung ke komputer lain

- Contohnya laptop yang tidak terhubung ke Wi-Fi atau data selular
- TAPI sekarang jaringan ada di mana-mana, bahkan dalam BART atau dalam pesawat

JARINGAN

- Komputer yang terhubung ke minimal satu komputer lain
- Barang Bukti bisa terdapat pada server dan juga pada perangkat jaringan maupun pada komputer lokal
- Saat ini Hampir setiap komputer terkoneksi ke jaringan

MAINFRAME

- Komputer handal yang digunakan pada perusahaan, atau digunakan bersama oleh banyak pengguna
- Ditempatkan pada pusat data center atau colocation center

Image from http://danialsharifudin.blogspot.com/2012/08/classification-of-computer.html

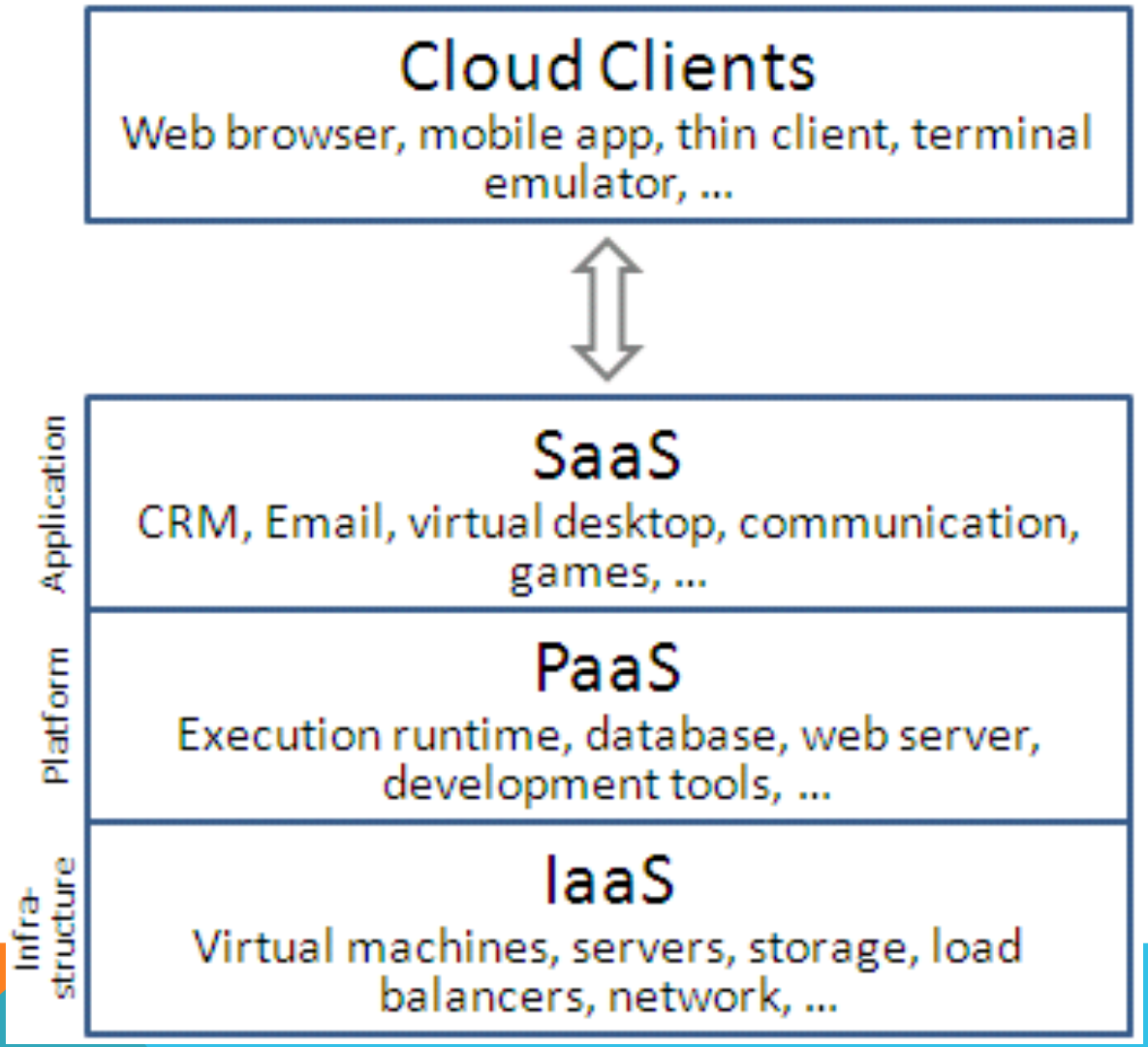
CLOUD COMPUTING

CONTOH CLOUD COMPUTING

- Gmail
- Facebook
- Twitter
- Amazon Web Services
- CloudFlare

LAYANAN CLOUD

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)



Ch 2m: Cloud computing - Wikipedia

IAAS

- Layanan CLOUD yang paling dasar
- Outsources hardware yang dibutuhkan
  - Servers, storage, routers, switches…

Contoh:

- Amazon EC2
- Windows Azure Virtual Machines
- Google Compute Engine
- Rackspace Cloud
  - Ch 2m: Cloud computing - Wikipedia

PAAS

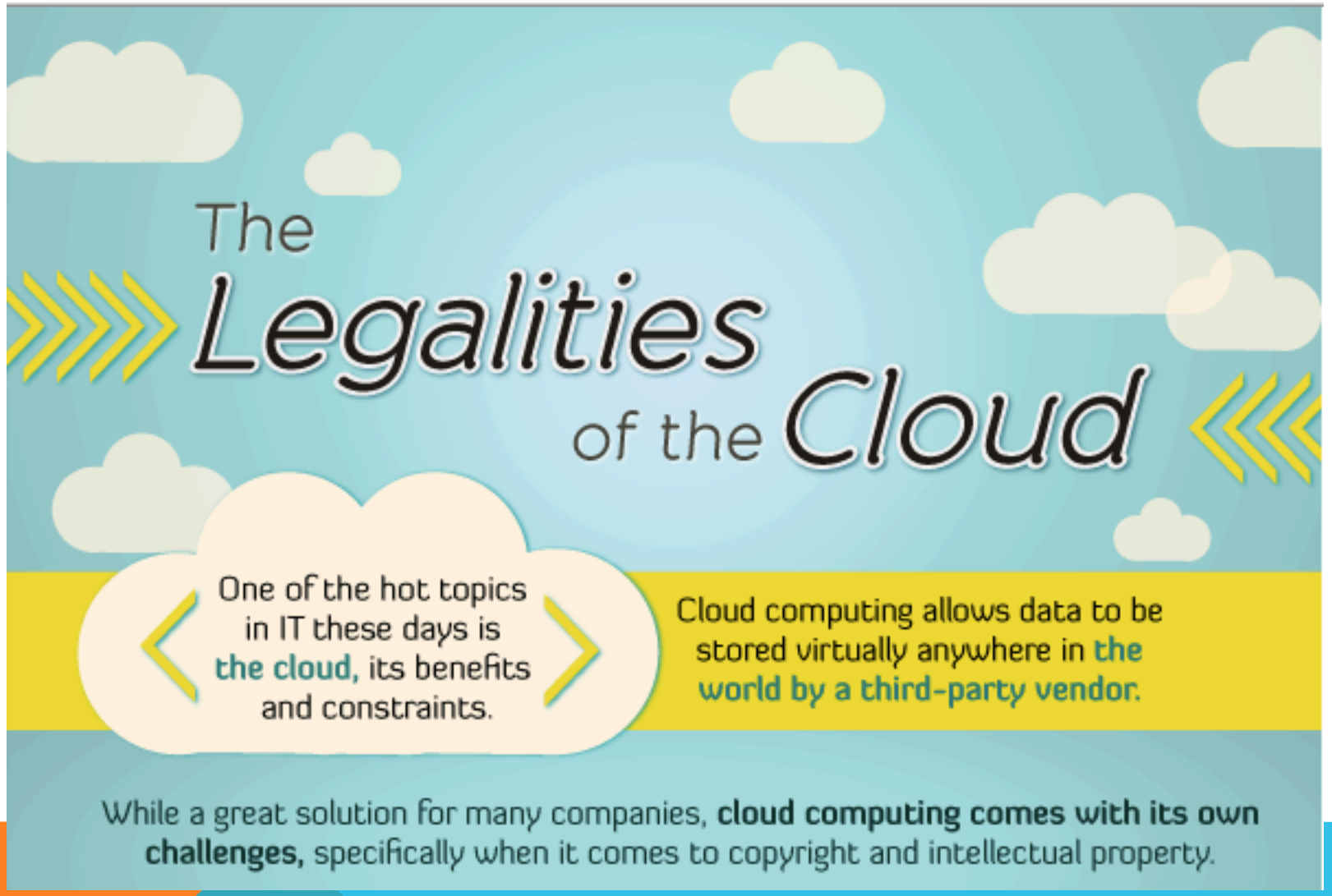
- **Menyediakan computing platform**
  - OS, programming language execution, database, and Web server

Contoh:

- AWS Elastic Beanstalk
- Heroku
- Google App Engine
- Windows Azure Compute
  - Link Ch 2m: Cloud computing - Wikipedia

SAAS

- Provider menginstal dan mengoperasikan perangkat lunak aplikasi di cloud
- Users mengakses software dari cloud clients
- Contoh:
  - Google Apps
  - Microsoft Office 365
  - Link Ch 2m: Cloud computing - Wikipedia



From link Ch 2g: Cloud Computing Legalities Infographic

Cloud Concerns

One of the biggest concerns of those using cloud systems is who owns that data and what copyright laws guide the information.

Who Owns the Data?

Ownership of material is covered by copyright, confidentiality and contract law

› Those laws differ by country

› Data is created in one country and stored in another

=

Who owns the information?

› Data is based on intellectual property, therefore owned by the creator of content. **Hardware, applications and operating systems belong to could provider.**

› U.S. law: Intellectual property owners have rights to their work that is a product of human intellect

From link Ch 2g: Cloud Computing Legalities Infographic

INSTAGRAM

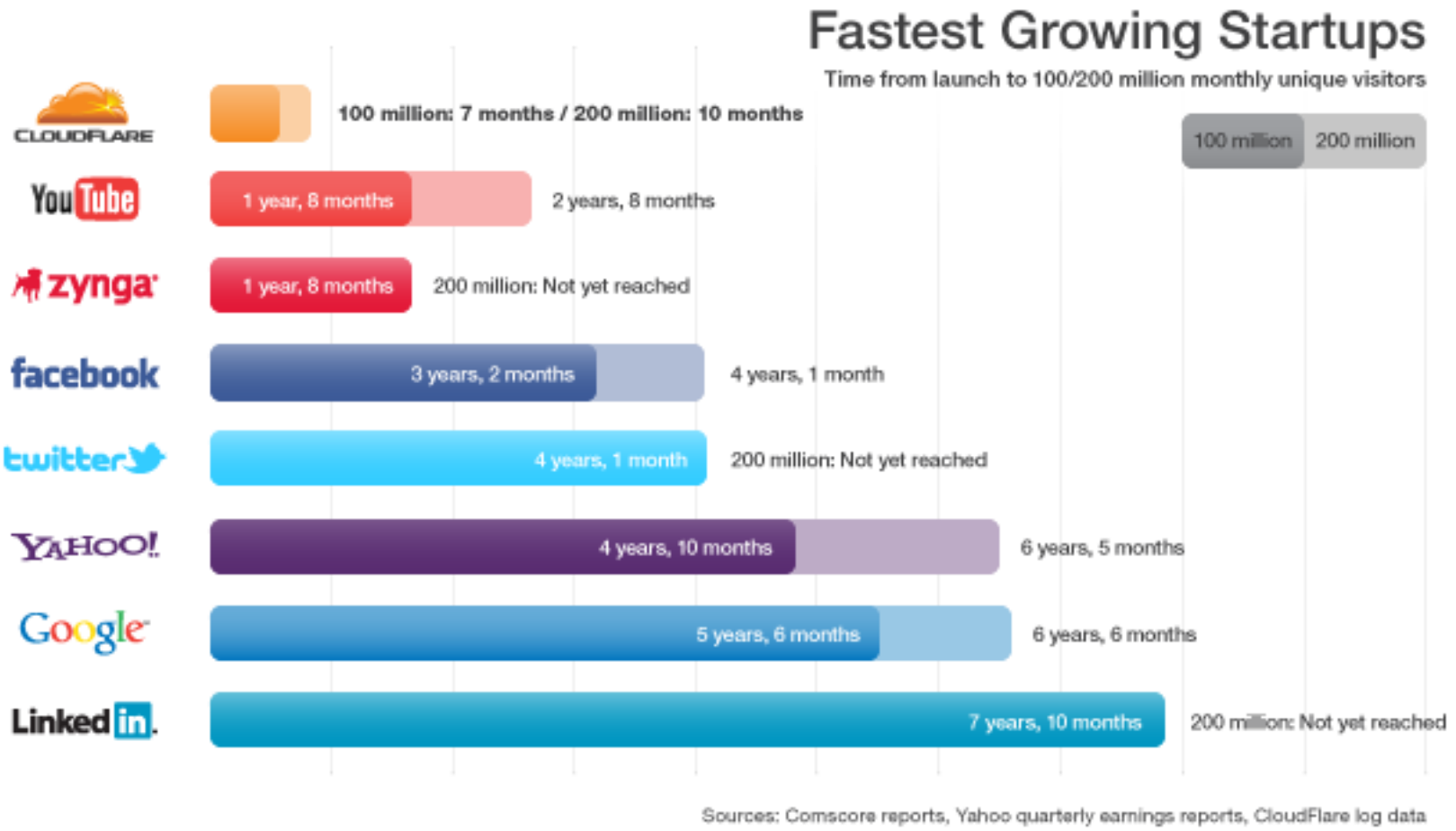
- Situs photo-sharing online
- Pada Dec. 2012, Instagram merubah terms of service
  - Perpetual rights (Hak abadi) untuk semua foto
  - Berhak untuk menjual foto kepada pemasang iklan tanpa bayaran atau pemberitahuan kepada pengguna
- Instagram kehilangan setengah Pengguna Harian dalam sebulan
  - Links

    Ch 2h: Instagram Wants To Sell Users' Photos Without Notice (Dec. 18, 2012)

    Ch 2i: Instagram Loses Almost Half Its Daily Users In a Month (Jan. 14, 2013)

AWS OUTAGE

- Dec. 24, 2012
- Netflix down, karena tergantung pada AWS (Link Ch 2j: Summary of the December 24, 2012 Amazon ELB Service Event in the US-East Region)
- Amazon beberapa kali terjadi major outages (gangguan layanan) (Link Ch 2k: Amazon Web Services - Wikipedia)



Link Ch 2I: Fastest Growing Startups (from 2011)

CLOUDFLARE GROWTH