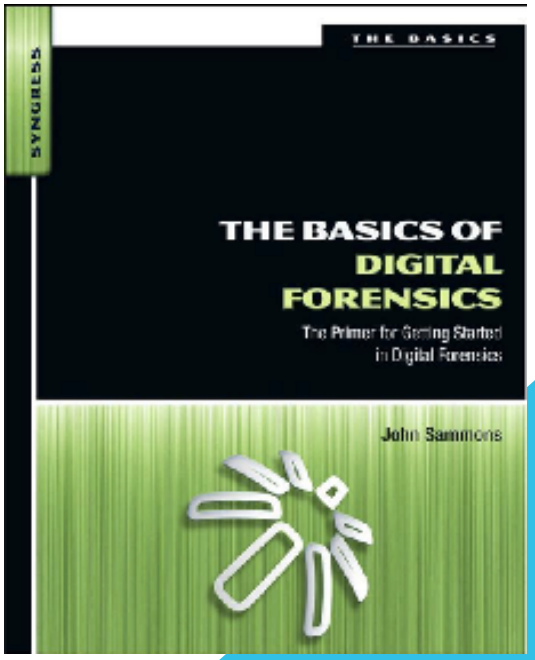


2. KEY TECHNICAL CONCEPTS BAGIAN 2

ACTIVE, LATENT, AND ARCHIVAL DATA

ACTIVE DATA

- Data – sistem operasi dapat "melihat" dan menggunakannya
- File dan folder yang tampak di Windows Explorer
- Berada di ruang yang dialokasikan
- Dapat diambil dengan cara menyalin file

LATENT DATA

- Data yang telah dihapus atau sebagian sudah ditimpa
- Tidak terlihat melalui OS
- Tidak muncul dalam Windows Explorer
- Bitstream atau forensik image diperlukan untuk memperoleh data ini

ARCHIVAL DATA

- Disebut juga Backups
- Biasanya disimpan di
  - External hard drives
  - DVDs
  - Magnetic tapes
  - Cloud backup services seperti Iron Mountain atau Symform

LEGACY ARCHIVAL DATA

- Dibuat dengan software atau hardware yang tidak lagi di produksi
- Untuk memperoleh data, Anda perlu untuk mendapatkan perangkat lama
  - User's groups
  - eBay

Image: PDP-11 at Defcon 17

- Link http://revdisk.org/gallery/index.php?/Defcon_PDP11_02

COMPUTER FILE SYSTEMS

FILE SYSTEM

- Melacak sektor yang digunakan dan yang kosong
- Lokasi setiap file
- Filename
- Tanggal terakhir diubah
- Permission (izin)

FAT (FILE ALLOCATION TABLE)

- File system Paling lama dan paling sederhana
- FAT12 (untuk floppy disks)
- FAT16 (2 GB max. partition size)
  - 4 GB pada Win 2000 (link Ch 2p: FAT16 vs. FAT32)
- FAT32 (umum digunakan di USB drives)
  - Tidak digunakan untuk Windows XP or later
- FATX untuk the X-Box
- exFAT digunakan untuk Windows CE
  - Link Ch 2o: File Allocation Table - Wikipedia

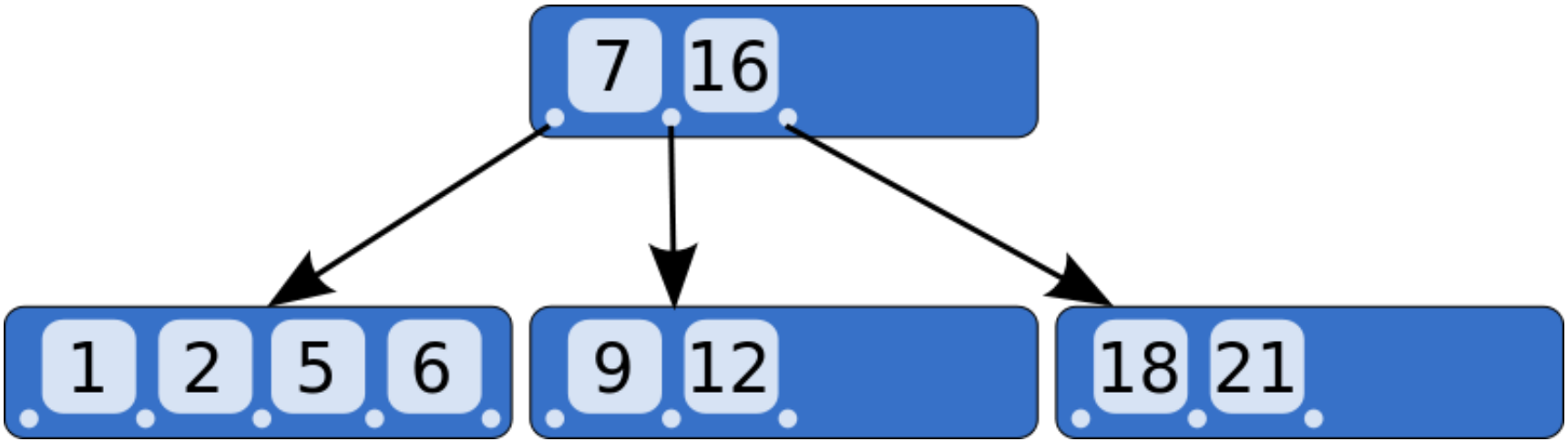
NTFS (NEW TECHNOLOGY FILE SYSTEM)

- Digunakan pada Win XP, 7, and Server
- Keuntungan
  - Journaling (recovers dari errors)
  - Encryption
  - Permissions
  - Uses B-Trees untuk pencarian yang lebih cepat

HFS+ (HIERARCHICAL FILE SYSTEM)

- Digunakan oleh produk Apple
- Juga menggunakan B-Trees
- Versi lain
  - HFS
  - HFSX

B-TREE



- Suatu cara menyimpan object sehingga mereka dapat dicari dengan cepat

Image From Wikipedia

ALLOCATED DAN
UNALLOCATED
SPACE

SPACE DI HARD DRIVE

Allocated

- Active data
- digunakan
- Bisa dilihat oleh OS

Unallocated

- Tidak lagi digunakan
- Slack space (Drive slack)
- Tidak terlihat di OS

SPACE DI HARD DRIVE

Host Protected Area dan Device Configuration Overlays

- Hidden area di hard drive
- Sulit untuk dideteksi
- Tidak digunakan oleh OS
- Penyimpanan device firmware dan data
- Diakses oleh firmware update untuk routine, yang bisa dirubah

DATA PERSISTANCE

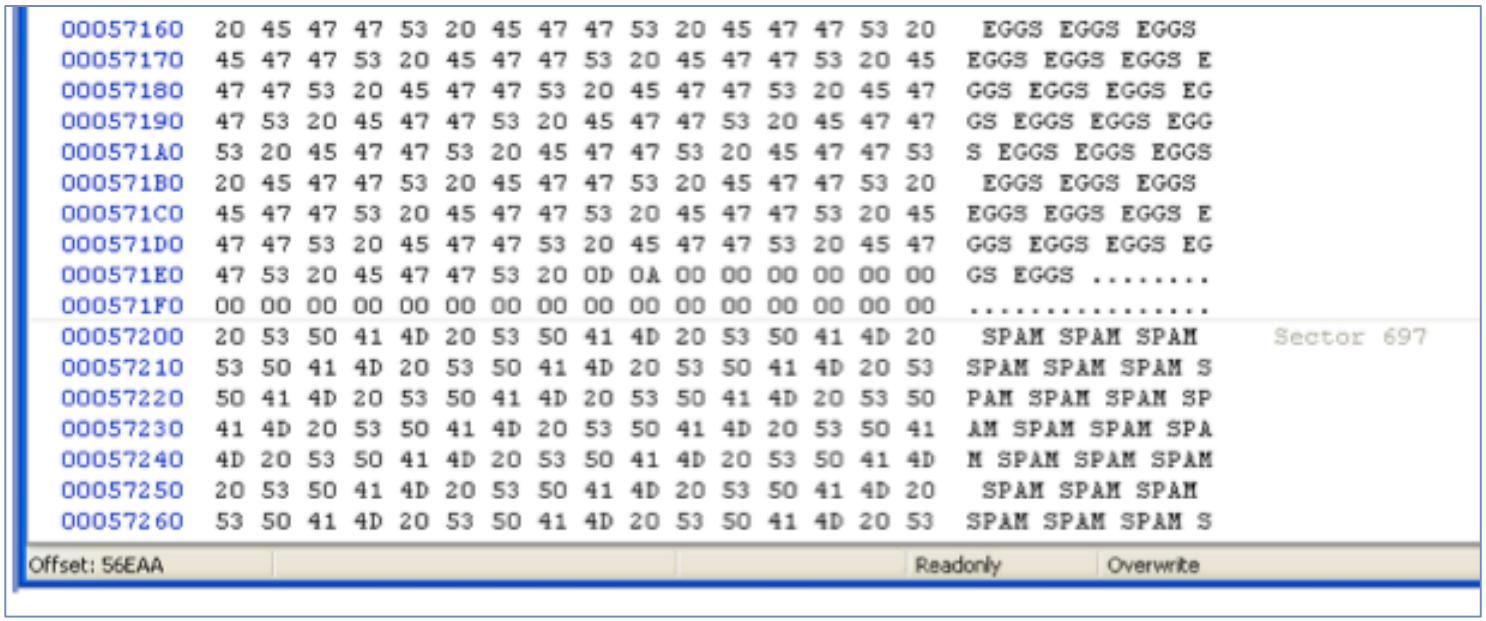
Data Lama Tertinggal di Slack Space

- Unallocated clusters
- Bertahan sampai drive di overwritten
- Bisa bertahun-tahun

Meskipun di Overwrite belum tentu semua datanya hilang !

- Jika file tidak menggunakan semua sectors

PROJECT 2



Sector	Contents	Technical Term
695	EGGS	Active data
696	EGGS + 0	Active data + RAM Slack
697	SPAM	File Slack

MAGNETIC DRIVE STORAGE

1 Sector = 512 bytes

- Semua data dibaca dan ditulis satu sector dalam satu waktu

Cluster

- Bervariasi, biasanya 4096 bytes = 8 sectors
- OS hanya bisa menggunakan space suatu cluster pada satu waktu

CONTOH

File berukuran besar: 4000 bytes

- Ditulis ke disk
- Menggunakan 8 sectors = 1 cluster

Delete BIG file

Menyimpan file SMALL pada cluster yang sama

- SMALL file: 1000 bytes
- Hanya menggunakan 2 clusters

DRIVE SLACK

Sector	Before	After
200	BIG	SMALL
201	BIG	SMALL
202	BIG	BIG
203	BIG	BIG
204	BIG	BIG
205	BIG	BIG
206	BIG	BIG
207	BIG	BIG

ERROR IN TEXTBOOK

Discussion from Fig. 2.5 through 2.8 is wrong

Book says a 780 byte file only overwrites 780 bytes on disk, when it actually overwrites 1024 bytes

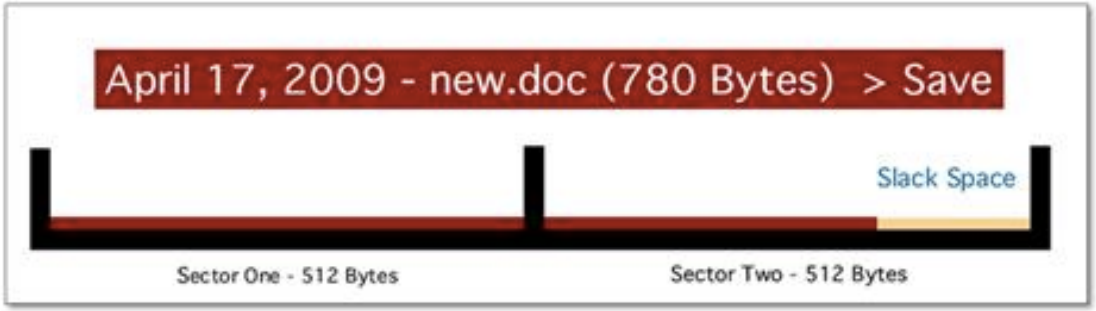


Figure 2.8 Note the slack space. This fragment of data can be recovered.

PAGE FILE (SWAP SPACE)

Digunakan untuk virtual memory

- Penyimpanan sementara ketika komputer kehabisan RAM
- Windows meletakkan data bahkan saat RAM tidak penuh
- Page file juga meloading data lama dari swap kembali ke RAM
- Bisa ditemukan data lama di dalam RAM

ISI PAGE FILE POTENSIAL

- Passwords
- Potongan gambar atau dokumen
- Apa saja dari RAM
- Tapi tidak ada timestamp, sehingga sulit untuk menghubungkannya dengan user atau kejadian tertentu

HIBERFIL.SYS

Berisi keseluruhan isi RAM

- Diisi saat komputer hibernates

ENKRIPSI DISK KESELURUHAN

Karen file page dan Hiberfil

- Sulit menentukan dimana lokasi data tersimpan

Whole Disk Encryption

- Satu-satunya cara mematikan seluruh data diproteksi
- Microsoft BitLocker
- Apple FileVault
- TrueCrypt (Open Source)

PROJECT 8: NTFS DATA RUNS