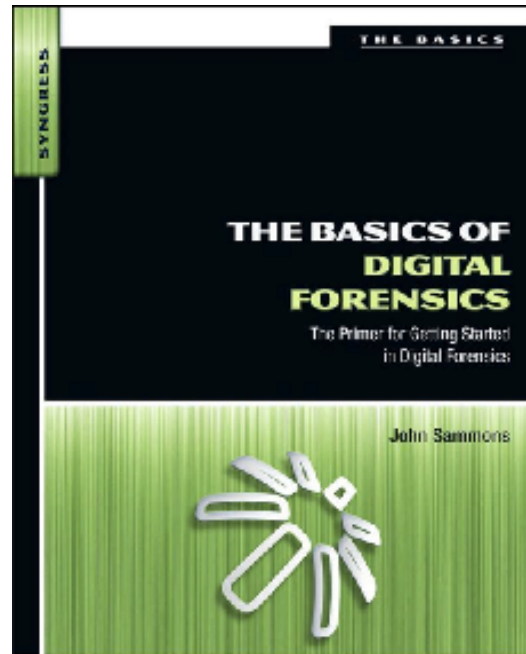




2. KEY TECHNICAL CONCEPTS BAGIAN 2



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.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](#)

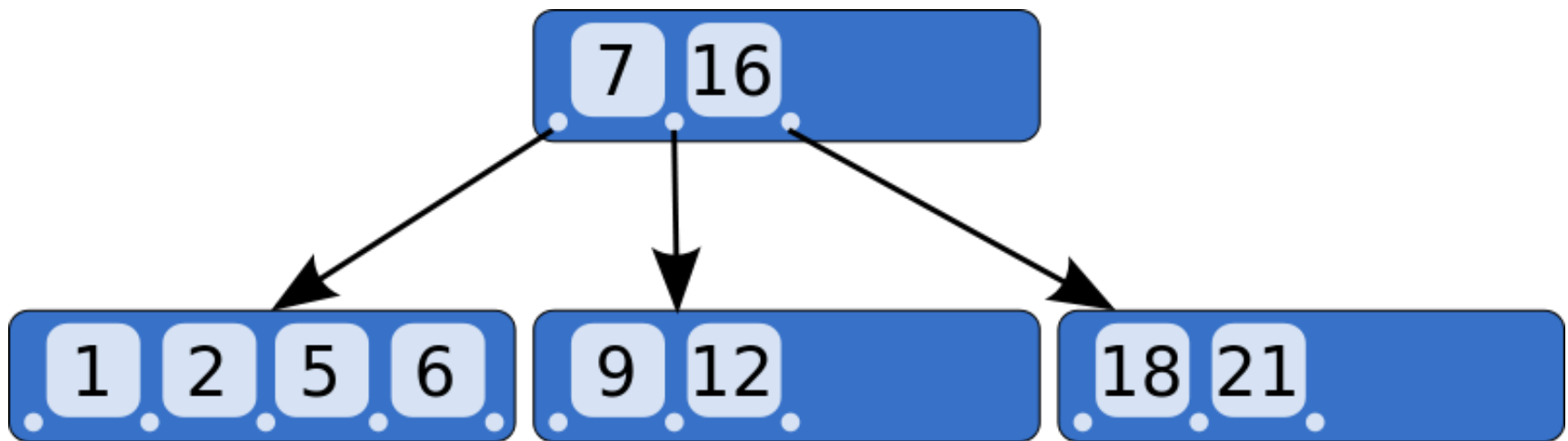
NTFS (NEW TECHNOLOGY FILE SYSTEM)

- 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 DATA
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 bertahan-tahun

Meskipun di Overwrite belum tentu semua datanya hilang !

- Jika file tidak menggunakan semua sectors



PROJECT 2

00057160	20 45 47 47 53 20 45 47 47 53 20 45 47 47 53 20	EGGS EGGS EGGS	
00057170	45 47 47 53 20 45 47 47 53 20 45 47 47 53 20 45	EGGS EGGS EGGS E	
00057180	47 47 53 20 45 47 47 53 20 45 47 47 53 20 45 47	GGG EGGS EGGS EG	
00057190	47 53 20 45 47 47 53 20 45 47 47 53 20 45 47 47	GS EGGS EGGS EGG	
000571A0	53 20 45 47 47 53 20 45 47 47 53 20 45 47 47 53	S EGGS EGGS EGGS	
000571B0	20 45 47 47 53 20 45 47 47 53 20 45 47 47 53 20	EGGS EGGS EGGS	
000571C0	45 47 47 53 20 45 47 47 53 20 45 47 47 53 20 45	EGGS EGGS EGGS E	
000571D0	47 47 53 20 45 47 47 53 20 45 47 47 53 20 45 47	GGG EGGS EGGS EG	
000571E0	47 53 20 45 47 47 53 20 0D 0A 00 00 00 00 00 00	GS EGGS	
000571F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
00057200	20 53 50 41 4D 20 53 50 41 4D 20 53 50 41 4D 20	SPAM SPAM SPAM	Sector 697
00057210	53 50 41 4D 20 53 50 41 4D 20 53 50 41 4D 20 53	SPAM SPAM SPAM S	
00057220	50 41 4D 20 53 50 41 4D 20 53 50 41 4D 20 53 50	PAM SPAM SPAM SP	
00057230	41 4D 20 53 50 41 4D 20 53 50 41 4D 20 53 50 41	AM SPAM SPAM SPA	
00057240	4D 20 53 50 41 4D 20 53 50 41 4D 20 53 50 41 4D	M SPAM SPAM SPAM	
00057250	20 53 50 41 4D 20 53 50 41 4D 20 53 50 41 4D 20	SPAM SPAM SPAM	
00057260	53 50 41 4D 20 53 50 41 4D 20 53 50 41 4D 20 53	SPAM SPAM SPAM S	
Offset: 56EAA Readonly Overwrite			

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

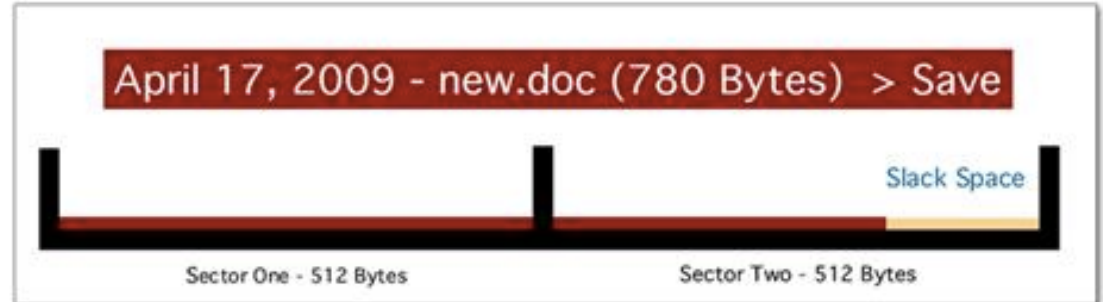


Figure 2.8 Note the slack space. This fragment of data can be recovered.

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 memamatkan seluruh data diproteksi
 - Microsoft BitLocker
 - Apple FileVault
 - TrueCrypt (Open Source)
- 

PROJECT 8: NTFS DATA RUNS

WinHex - [Drive E:]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data

File Edit

Data Interpreter

8 Bit (±): 1
16 Bit (±): 1
32 Bit (±): 65537

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0219C600	46	49	4C	45	30	00	03	00	F6	20	10	00	00	00	00	00	FILE0
0219C610	01	00	01	00	38	00	01	00	58	01	00	00	00	04	00	00	8 X
0219C620	00	00	00	00	00	00	00	00	04	00	00	00	1E	00	00	00	
0219C630	09	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	
0219C640	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	H
0219C650	8A	37	A4	DE	CB	FC	CD	01	FB	89	81	A2	C2	FC	CD	01	77pEuf 011cAuf
0219C660	13	5C	1D	D8	C8	FC	CD	01	8A	37	A4	DE	CB	FC	CD	01	\ 0Euf 77pEuf
0219C670	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0219C680	00	00	00	00	04	01	00	00	00	00	00	00	00	00	00	00	
0219C690	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	00	0 p
0219C6A0	00	00	00	00	00	00	02	00	54	00	00	00	18	00	01	00	T
0219C6B0	05	00	00	00	00	00	05	00	8A	37	A4	DE	CB	FC	CD	01	77pEuf
0219C6C0	8A	37	A4	DE	CB	FC	CD	01	8A	37	A4	DE	CB	FC	CD	01	77pEuf 77pEuf
0219C6D0	8A	37	A4	DE	CB	FC	CD	01	00	00	00	00	00	00	00	00	77pEuf
0219C6E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	
0219C6F0	09	03	46	00	49	00	4C	00	45	00	32	00	2E	00	54	00	FILE2 . T
0219C700	58	00	54	00	00	00	00	00	80	00	00	00	48	00	00	00	X T H
0219C710	01	00	00	00	00	00	03	00	00	00	00	00	00	00	00	00	
0219C720	01	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	@
0219C730	00	04	00	00	00	00	00	00	E8	03	00	00	00	00	00	00	è
0219C740	E8	03	00	00	00	00	00	00	31	02	9E	0C	01	00	01	00	è 1
0219C750	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	ÿÿÿÿÿG
0219C760	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0219C770	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0219C780	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0219C790	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0219C7A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0219C7B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Sector 68835 of 206324

Offset: 219C74C

= 1