Project 8: NTFS Data Runs (25 points)

Tujuan

Untuk mempelejari struktur direktori pada level biner.

Kebutuhan Project

- Komputer Windows machine, jenis apa saja. Tutorial di sini menggunakan Virtualbox dan Windows XP 3 sebagai guest OS.
- Jika di laboratorium Foresec gunakan komputer WinXPSP3, Jangan WinXPSP1, karena WinXPSP1 digunakan hanya untuk target penyerangan di Ethikal Hacking.
- Bisa juga mengerjakan project ini menggunakan komputer single physical machine dan gunakan USB flash drive sebagai target drive.

Menambahkan Small Hard Disk ke Komputer Virtual

- Jalankan Virtualbox. Klik kanan pada icon Windows XP-SP3 dalam keadaan: "Powered Off", seperti terlihat di sebelah kanan.
- 2. Click "Settings". Pada kotak "Virtual Machine Settings", click icon Storage.... Kemudian klik icon hardisk di pojok kanan untuk menambah hardisk sperti di gambar.
- Kemudian akan muncul pesan untuk menambah disk. Pilih Tab "Create new disk". Pilih "VDI (VirtualBox Disk Image". Kemudian klik Tombol "Continue" di pojok kiri bawah.
- Selanjutnya pilih "Dynamically allocated". Kemudian klik Tombol "Continue" di pojok kiri bawah.



5. Pada jendela File location and size, pada bagian ukuran hardisk, geser/isikan menjadi 100 MB, seperti gambar di bawah.

● ○ ○	Create Virtual Hard Drive
	File location and size
	Please type the name of the new virtual hard drive file into the box below or click on the folder icon to select a different folder to create the file in.
	NewVirtualDisk1
	Select the size of the virtual hard drive in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard drive. 100 MB 4.00 MB 2.00 TB
	Go Back Create

6. Klik tombol **Create.** Maka akan kembali ke jendela setingan Windows-XP-SP3. Klik tombol OK di pojok kanan bawah. Maka jendela akan kembali ke jendela VirtualBox.

25 Point

Membersihkan Disk Secara Forensic

- 7. Jalankan Komputer WindowsXP SP3 virtual.
- 8. Windows bisa mengakses disk. Tapi jangan anggap disk yang baru dibuat tersebut clean—disk kadang-kadang masih berisi data lama (ingat hasil di Project 1).
- 9. Jadi kita lakukan pembersihan dengan cara forensic, menulis 00 pada tiap byte.
- 10. Pada komputer virtual, click Start, Run.
- 11. Pada kotak Run, ketikkan CMD dan tekan Enter untuk membuka Command Prompt.
- 12. Pada jendela Command Prompt, ketikkan perintah berikut diikuti dengan Enter tiap baris: **DISKPART**

LIST DISK

- 13. Lihat output untuk mencari disk baru dengan ukuran 101 MB disk yang akan kita clean—seperti dicontoh, terlihat Disk 1. Hati-hati jangan salah disk!
- 14. Pada jendela Command Prompt, masukkan perintah berikut, pastikan memilih disk yang tepat pada perintah pertama:

SELECT DISK 1 CLEAN ALL

Mengenali Disk Baru

- 15. Pada komputer virtual, click Start.
- 16. Klik kanan "My Computer" dan click Manage.
- 17. Pada panel sebelah kiri dari Computer Management, click "Disk Management".
- 18. "Initialize and Convert Disk Wizard" akan terbuka, seperti pada gambar.
- 19. Click Next.
- 20. Pada menu "Select Disks to Initialize" screen, click Next.
- 21. Pada menu"Select Disks to Convert", click Next.
- 22. Pada menu "Completing the Initialize and Convert Disk Wizard", click **Finish**.

Mempartisi dan Memformat Drive Baru



🗏 Computer Management					
🗐 File Action View Window H	elp				_ 8 ×
	1 👪				
Computer Management (Local) Komputer Management (Local) Komputer Tools Kom	Volume Layout	Type File System Basic NTFS	Status Healthy (System)	Capacity 6.35 GB	Free Space 723 MB
Disk Defragmenter	<				>
🗈 🍰 Services and Applications					^
	Basic 6.99 GB Online	(C:) 6.35 GB NTFS Healthy (System)	6: U	59 MB nallocated	
	Cisk 1 Basic 101 MB Online	101 MB Unallocated	New Partition		~
<pre></pre>	Unallocated	Primary partition		_	
			Help		

- 23. Pada Computer Management, di sebelah kanan, klik right "Unallocated" space pada hard disk yang baru.
- 24. Pada context menu, click "New Partition...", seperti terlihat di gambar.
- 25. "New Partition Wizard" terbuka.
- 26. Click Next.
- 27. Pada menu "Select Partition Type", biarkan pilihan default "**Primary partition**" dan click **Next**.
- 28. Pada menu "Specify Partition Size", biarkan pilihan default dan click Next.
- 29. Pada menu "Assign Drive Letter or Path", biarkan pilihan default dan click Next.
- **30.** Pada menu "Format Partition", rubah "Allocation unit size" menjadi **512**, seperti terlihat di sisi kanan,

Ukuran tersebut membuat tiap cluster sama dengan sector (1 sector= 512 byte), sama seperti cara kerja floppy disks. Untuk disk yang berukuran besar hal ini tidak efisien karena memperlambat proses pembacaan disk, tapi untuk disk ukuran kecil tidak bermasalah hanya untuk menyederhanakan project.

- 31. Pada menu "Completing the New Partition Wizard", click Finish.
- 32. Tutup Computer Management.

Mendownload File Tes	t
-----------------------------	---

33. Pada komputer virtual, di browser, klik kanan FILE1.TXT pada link di di elearning simpan ke desktop.

E F	ILE1.1	XT - Not	epad		
File	Edit	Format	View	Help	
111	1111	111111	1111	111111111111111111111111111111111111111	11111

Format F Tost	Partition ore data on this partition, you	ı must format it first.		
Choo	se whether you want to form	at this partition, and if so, wh	iat settings you (vant to use.
С) Do not format this partition			
۲	Format this partition with the	e following settings:		
	File system:	NTFS	~	
	Allocation unit size:	512	~	
	Volume label:	New Volume		
	🔲 Perform a quick form	at		
	📃 Enable file and folder	compression		
			Mauto	Canad
			INEX(>	Carice

- 34. Ulangi proses untuk FILE2.TXT.
- **35.** Pada desktop, double-click **FILE1.TXT** untuk membuka file dengan Notepad.
- 36. Seperti yang bisa di lihat, file tersebut berisikan 1000 karakter "1" dalam satu baris.
- 37. Buka FILE2.TXT, maka terlihat isinya --1000 karakter "2".
- **38.** Tutup semua Notepad.



Mengkopi Test Files ke Partisi Baru

39. Click Start, "My Computer".

40. Double-click icon "New Volume".

41. Drag file **FILE1.TXT** dari desktop ke jendela "New Volume" dan drop.

42. Drag file **FILE2.TXT** dari desktop ke jendela "New Volume" dan drop.

43. Kedua file tersebut sekarang seharusnya terlihat pada drive yang baru, seperti terlihat di

gambar.

Install WinHex

- 44. Buka browser dan arahkan ke http://winhex.com, atau bisa di download di elearning. Simpan di desktop.
- 45. Pada jendela desktop, atau dimanapun file di simpan, klik kanan file **winhex.zip** dan click "**Extract All...**".
- 46. Pada kotak "Welcome to the Compressed (zipped) Folders Extraction Wizard" box, click Next, Next, Finish.
- 47. Folder dengan beberapa files terbuka. Double-click file **setup.exe**.
- 48. Pada menu "WinHex 16.8", di kanan bawah seperti terlihat di gambar, click tombol **English**.
- 49. Kemudian click tombol OK.
- 50. Pada kotak "Setup", click Yes. Pada kotak "WinHex" box, click Yes
- 51. WinHex akan terbuka , seperti pada gambar.

Melihat Data menggunakan WinHex

52. Dari menu WinHex, click Tools, "Open Disk...".



🗮 WinHex				16.8 🔳 🗗 🔀
File Edit Search Navigation View	w Tools Specialist Options \	Window Help		
	Open Disk F9 Disk Tools File Tools	■篆 桷 → ⊕ ← ⇒ 	2 🖣 🧼 🖬 🔎 🕌 🖄	() 🖄 🖩 🗍 🤣
File Edit	Open <u>B</u> AM Alt+F9			
rije c <u>a</u> u	View Shitt+F9 External Programs → Equivalator Alt+F8 Hex Converter F8 Analyze Block F2 Compute Hash Ctrl+F2 Hash Database → Start Center Enter	-		
🝠 start 🔰 🖉 🕲	🔘 🕺 🔍 🐼	Volume (E:) 📁 🗁 winhex	🔛 WinHex	🛃 🏧 🛞 🧐 🦁 2:20 PM

53. Pada kotak "Edit Disk", click "New Volume", seperti terlihat di bawah, dan click tombol OK.



54. Dari menu WinHex menu, click View, Show, "Directory Browser", seperti terlihat di bawah ini.



55. Panel Browser direktori akan muncul di bagian tengah atas jendela.

🚟 WinHex - [Drive E:]				16.8 <mark>– 🗆 ×</mark>
🥪 File Edit Search Nav	igation View Tools Specialist Options	Window Help		
D 🚅 🗏 🖨 🗳 🖄	- 🗠 🖻 🖻 🐘 🛛 🖊 🧥 🏷	≲ 畿 桷 │ → -Ð ⇐ ⇒ │	22 🐂 🗇 🎟 🔎 🛛 🔠 4 🕨 🛅 🔠 🖉	
Case Data	<u>\</u>		1 min. ago	12 files, 3 dir.
File Edit	Name 📥	Ext. Size Created	Modified Accessed Attr. 1st sector	<u> </u>
	\$AttrDef	2.5 KB 01/27/2013 12:19	01/27/2013 12:19: 01/27/2013 12:19: SH 68,759	
		0 B 01/27/2013 12:19	01/27/2013 12:19: 01/27/2013 12:19: SH	
	SBitmap	25.2 KB 01/27/2013 12:19	01/27/2013 12:19 01/27/2013 12:19 SH 103,258	
	Soot 8	8.0 KB 01/27/2013 12:19	01/27/2013 12:19: 01/27/2013 12:19: SH 0	
	SLogFile	2.0 MB 01/27/2013 12:19	01/27/2013 12:19: 01/27/2013 12:19: SH 64,663	
		32.0 KB 01/27/2013 12:19	01/27/2013 12:19: 01/27/2013 12:19: SH 68,775	
	SMFTMirr \$	4.0 KB 01/27/2013 12:19	01/27/2013 12:19: 01/27/2013 12:19: SH 103,162	
		0 B 01/27/2013 12:19	01/27/2013 12:19: 01/27/2013 12:19: SH	
	SUpCase \$	128 KB 01/27/2013 12:19	01/27/2013 12:19: 01/27/2013 12:19: SH 103,309	
	SVolume	0 B 01/27/2013 12:19	01/27/2013 12:19: 01/27/2013 12:19: ISH	
	FILE1.TXT	TXT 1.0 KB 01/27/2013 12:21	01/27/2013 11:14: 01/27/2013 14:45: IA 68,764	
	FILE2.TXT	TXT 1.0 KB 01/27/2013 12:21	01/27/2013 11:15: 01/27/2013 12:21: A 68,766	•
	Offset 0 1 2 3 4	156789AB	C D E F 10 11 12 13 14 15 16 17 18 19	1A 1B 🗸 🔍
	00000000 BB 52 90 4E 54	46 53 20 20 20 20 00 0	2 01 00 00 00 00 00 00 00 F8 00 00 3F 00	04 00 ëR∎NTFS Ø ?
	0000001C 3F 00 00 00 00	0 00 00 00 80 00 80 00 F	4 25 03 00 00 00 00 00 A7 0C 24 00 00 00	0 ? II ô% S
	00000038 FA 92 01 00 00	0 00 00 00 02 00 00 00 0	8 00 00 00 A7 53 B0 5C 73 B0	=== 0 ú′\$S*\s*\′
	00000054 FA 33 C0 8E D0	BC 00 7C FB B8 C0 07 8	E D8 E8 16 00 B8 00 0D 8E C0 8 BR(E) 21	0 ú3Å∎м û,Å ∥Øè , ∥Å3ŰÆ
	00000070 10 E8 53 00 68	00 0D 68 6A 02 CB 8A 1	6 24 00 B4 08 CD 13 73 05 B9 10 BB (1) 21227	F èSh hjEI\$ Is¹ÿÿ∎ñf
	0000008C B6 C6 40 66 0F	6 D1 80 E2 3F F7 E2 8	6 CD CO ED 06 41 66 0F B7 C9	0 ¶Æ@f ¶N∣A?÷A∣IAi Af Ef÷áf£
	000000A8 00 C3 B4 41 BE	3 AA 55 8A 16 24 00 CD 1	3 72 OF 81 FB 55 AA 75 09 F6 C1 01 74 04	FE 06 A'A≫ ² U∥ \$ I r ∎úU ² u öA t þ
	000000C4 14 00 C3 66 60	1 1E 06 66 A1 10 00 66 0	3 06 1C 00 66 3B 06 20 00 0F 82 3A 00 1E	66 6A Af' fi f f; I: fj
	000000E0 00 66 50 06 53	66 68 10 00 01 00 80 3	E 14 00 00 OF 85 OC 00 E8 B3 FF 80 3E 14	00 00 fP Sfh > e ³ ÿ >
	000000FC 0F 84 61 00 B4	42 8A 16 24 UU 16 1F 8	B F4 CD 13 66 58 5B 07 66 58 66 58 1F EB	2D 66 a B S OI fX fXfX e-f
	00000118 33 D2 66 0F B7	OF 18 00 66 F7 F1 FE C	2 8A CA 55 8B DU 55 C1 EA 10 F7 36 1A UU	85 D5 301 · 1+npa E1 D1AE +6 0
	00000134 8A 16 24 00 8A	LES CULLA UN UN CC BS U	I 02 CD I3 0F 82 I9 00 8C C0 05 20 00 8E	CU 55 I S TEAR I, I I IA IAT
	00000150 FF 05 10 00 FF	UE UE UU UF 85 6F FF U	/ 1F 66 61 C3 AU F8 U1 E8 U9 UU AU FB U1	ESUS Y Y DOY TAA Ø E U E
	Sector 0 of 206324	Offset	0 = 235 Block:	n/a Size: n/a

56. Gulung layar ke bawah untuk mencari FILE1.TXT dan FILE2.TXT, seperti terlihat di bawah.

- 57. Pada Directory Browser, click FILE1.TXT.
- 58. Pada panel bawah memperlihatkan raw hex data pada cluster pertama yang berisi data FILE1.TXT, seperti terlihat di bawah.

🚟 WinHex - [Drive E:]					16.8 <u>- D ×</u>
🧼 File Edit Search Nav	rigation View Tools Specialist Option	s Window Help			_ 8 ×
0 🖻 🗏 🖨 🗳 🖄	o 🖻 🖻 🖻 🎲 🖊 🎄 🤅	S 😹 🏘 👘 → 🕀	4 🕂 🛛 🕾 🖓 🎟 🔎	> 🖽 ◀ 🖆 🖽 🧇	
Face Data	N.				12 files, 3 dir.
Fig. Ech	Name 🔺	Ext. Size Cre	ated Modified	Accessed Attr. 1st sector	×
rec uga	SAttrDef	2.5 KB 017	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: SH 68,759	
		0 B 01/	27/2013 12:19: 01/27/2013 12:1	9 01/27/2013 12:19 SH	Data Interpreter 🛛 🗶
	SBitmap	25.2 KB 017	27/2013 12:19 01/27/2013 12:1	9 01/27/2013 12:19 SH 103,258	8 Bit (±): 49
	Boot \$	8.0 KB 017	27/2013 12:19 01/27/2013 12:1	9: 01/27/2013 12:19: SH 0	16 Bit (±) 12593
	SLogFile	2.0 MB 017	27/2013 12:19 01/27/2013 12:1	9: 01/27/2013 12:19: SH 64,663	32 B# (±): 825307441
	.smft	32.0 KB 017	27/2013 12:19 01/27/2013 12:1	9 01/27/2013 12:19 SH 68,775	
	SMFTMin SMFTMin	4.0 KB 017	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: SH 103,162	
		08 017	27/2013 12:19: 01/27/2013 12:1	9 01/27/2013 12:19 SH	
	SUpLase	128 KB U17	27/2013 12:19 01/27/2013 12:1	9 0172772013 12:19 SH 103,309	
	SV olume	UB UIZ	27/2013 12:19 01/27/2013 12:1	9 0172772013 12:19 ISH	
		TYT 1.0 KB 017	27/2013 12:21 01/27/2013 11:1	4	
	THEE2 TAT	1.0 10 10	072013 12.21 072772013 11.1	0 0172772013 12.21 M 00,700	
	Offset 0 1 2 3	45678	9 A B C D E F 1	0 11 12 13 14 15 16 17 18 19	/ 1A 1B 🗸 🔍 🔺
	02193800 31 31 31 31 3	1 31 31 31 31 3	1 31 31 31 31 31 31 3	1 31 31 31 31 31 31 31 31 31 31	. 31 31 1111111111111111111111111111111
	0219381C 31 31 31 31 3	1 31 31 31 31 31 3	1 31 31 31 31 31 31 31 3	1 31 31 31 31 31 31 31 31 31 31	. 31 31 1111111111111111111111111111111
		$1 \ 31 \ 31 \ 31 \ 31 \ 31 \ 31 \ 31 \ $	$1 \ 31 \ 31 \ 31 \ 31 \ 31 \ 31 \ 31 \ $	$1 \ 31 \ 31 \ 31 \ 31 \ 31 \ 31 \ 31 \ $	
		1 21 21 21 21 21 2	1 21 21 21 21 21 21 21 2	1 31 31 31 31 31 31 31 31 31 31 31	
	0219388C 31 31 31 31 3	1 31 31 31 31 31 3	1 31 31 31 31 31 31 31 3	1 31 31 31 31 31 31 31 31 31 31 31	31 31 111111111111111111111111111111111
	021938A8 31 31 31 31 3	1 31 31 31 31 31 3	1 31 31 31 31 31 31 3	1 31 31 31 31 31 31 31 31 31 31	31 31 111111111111111111111111111111111
	021938C4 31 31 31 31 3	1 31 31 31 31 3	1 31 31 31 31 31 31 3	1 31 31 31 31 31 31 31 31 31 31	. 31 31 11111111111111111111111111111
	021938E0 31 31 31 31 3	1 31 31 31 31 3	1 31 31 31 31 31 31 3	1 31 31 31 31 31 31 31 31 31 31	. 31 31 111111111111111111111111111111
	021938FC 31 31 31 31 3	1 31 31 31 31 3	1 31 31 31 31 31 31 3	1 31 31 31 31 31 31 31 31 31 31	. 31 31 11111111111111111111111111111
	02193918 31 31 31 31 3	1 31 31 31 31 3	1 31 31 31 31 31 31 3	1 31 31 31 31 31 31 31 31 31 31	. 31 31 111111111111111111111111111111
	02193934 31 31 31 31 3	1 31 31 31 31 3	1 31 31 31 31 31 31 3	1 31 31 31 31 31 31 31 31 31 31	. 31 31 1111111111111111111111111111111
	02193950 31 31 31 31 3	1 31 31 31 31 3	1 31 31 31 31 31 31 3	1 31 31 31 31 31 31 31 31 31 31	. 31 31 11111111111111111111111111111
	Sector 68764 of 206324	Offset:	2193800	= 49 Block:	n/a Size: n/a

- **59.** Perhatikan tanda icon kuning yang ditandai dengan kotak hijau pada gambar. (Memperlihatkan magnifying glass pada folder). Icon toggles memperlihatkan Directory Browser. Click.
- 60. Directory Browser menghilang, maka kita bisa melihat lebih jelas hex view, seperti di bawah.
- 61. Gulung ke atas beberapa baris pada hex view sehingga bisa terlihat dimana karakter "1" bermula, seperti terlihat di bawah.
- 62. Karakter 1 bermula pada sector. Nomor sector number terlihat pada kiri bawah –pada contoh, bermula pada Sector 68764.

🚟 WinHex - [Drive E:]					16.8 💶 🗙
🥪 File Edit Search Nav	rigation View To	Specialist Options Window Help			_ <u>_</u>
🗅 🖨 🖶 🖨 🖆	- in 🖪 🕄 🛛		(+ ⇒ 2 ≒ 🧼 🖬 🔎) 🔠 🖌 🕨 🛅 🖩 🤣	
Case Data	Offset	0 1 2 3 4 5 6 7 8 9	A B C D E F 1	0 11 12 13 14 15 16 17 18 19 1A 1B	✓ Q ▲
File Edit	02193790	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00	$0 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 \$	
	021937AC	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00	0 00 00 00 00 00 00 00 00 00 00 00	
	021937C8	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00	0 00 00 00 00 00 00 00 00 00 00 00	
	021937E4	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 01	0 00 00 00 00 00 00 00 00 00 00 00	
Data Interpreter 🛛 🗵	02193800	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
8 Bit (±): 49	0219381C	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
16 Bit (±): 12593	02193838	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
32 Bit (±): 825307441	02193854	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	02193870	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	0219388C	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 3:	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	021938A8	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	11111111111111111111111111111111
	021938C4	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	11111111111111111111111111111111
	021938E0	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	11111111111111111111111111111111
	021938FC	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	02193918	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	02193934	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
5t	02193950	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	0219396C	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	02193988	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	021939A4	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	021939C0	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	021939DC	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	021939F8	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	02193A14	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	02193A30	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	02193A4C	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	02193A68	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	02193A84	31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111
	Sector 68764 of 3	3324 Offset	2193800	= 49 Block:	n/a Sizer n/a
	00000 00104 011	Unade	2.00000	in proof.	100 0.00. 100

- 63. Gulung ke bawah Hex view sampai ketemu akhir karakter "1".
- 64. Seperti terlihat di bawah, karakter 1 memenuhi satu sector seluruhnya, dan hamper mengisi next sector (68765 pada contoh).

WinHex - [Drive E:]																							16.8	
Search Nav	igation View To	ols Spec	ialist	Options	Wind	ow He	þ						_		_	_								- 151 × 1
		1015	44		10.5	45	·	n 4	b	1.0			0		× 4	•	en r	50 I	0					
		···· 010*	arra	HEX	NS HEX	ara a		<u> </u>			1 -		~	L LC	<u>л</u> -	· ·			~					
Case Data	Offset	0 1	. 2	3 (1 5	ь 7	8	9	A B	C	D	E F	10	11 1	12 13	14	15	16 1	.7	18 1	9 1	A 1B		-
File E <u>d</u> it	021939A4	31 31	. 31	31 33	31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31	111111111111111111111111111111111111111	
	021939C0	31 31	. 31	31 33	31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31	111111111111111111111111111111111111111	
	021939DC	31 31	. 31	31 33	31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31	111111111111111111111111111111111111111	
1	021939F8	31 31	. 31	31 33	31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31	111111111111111111111111111111111111111	
Data Interpreter 🛛 🗶	02193A14	31 31	. 31	31 3:	31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31	111111111111111111111111111111111111111	
8 Bit (±): 49	02193A30	31 31	. 31	31 33	31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31	111111111111111111111111111111111111111	
16 Bit (±): 49	02193A4C	31 31	. 31	31 33	31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31	111111111111111111111111111111111111111	
32 Bit (±): 49	02193A68	31 31	. 31	31 33	1 31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31	111111111111111111111111111111111111111	
	02193A84	31 31	. 31	31 33	1 31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31	111111111111111111111111111111111111111	
	02193AA0	31 31	. 31	31 33	1 31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31	111111111111111111111111111111111111111	-
		31 31	31	31 3:	1 31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31	111111111111111111111111111111111111111	
			9 31	31 3.	1 31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	31 31	. 31	31	31 3	31	31 3	1 3	1 31		
	- 14	31 31	31	31 3.	1 31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	51 31	. 31	31	31 3	51	31 3	1 3	1 31		
	10	31 31	31	31 3.	1 31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	51 31	. 31	31	31 3	51	31 3	1 3	1 31		
	0020	31 31	. 31	31 3.	1 31	31 31	31	31 3	1 21	21	31 3	1 31	31	31 3	01 01 01 01	. 31	31	31 3	10	31 3	1 3	1 31		
	3848	31 31	31	31 3.	1 31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	51 31	. 31	31	31 3	51	31 3	1 3	1 31		
	02103804	31 31	31	31 3.	1 31	31 31	31	31 3	1 31	31	31 3	1 31	31	31 3	1 31	. 31	31	31 3	1	31 3	1 3	1 31		
	02193800	21 21	21	31 3.	1 21	21 21	21	21 2	1 21	21	31 3 31 3	1 21	21	21 2	21 21	. 31	21	31 3	21	21 2	1 3	1 21		
	02193890	31 31	21	31 3.	1 31	21 21	21	31 3	1 21	21	31 3 31 3	1 31	21	31 3	01 01 01 01	. 31	21	31 3	11	31 3	1 3	1 31		
	02193856	21 21	21	21 2	21	21 21	21	21 2	1 21	21	21 2	1 21	21	21 2	01 01	. 31	0.0	00 0	10	00 0	0 0	0 00	1111111111111111111111	
	02193004	00 00	0.00	00 01	0.00	00 00	00	00 0	0 00	0.0	00 0	0 00	22	22 2	22 22	. 00	22	22 2	22	22 2	2 2	2 22	222222222222222222222222222222222222222	
	021936F0	22 22	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	22 2	2 22	22 22	22	22 2	2 22	22	22 2	2 22	22	22 2	2 22	. 32	22	22 2	22	22 2	2 3	2 32	22222222222	
	02193020	32 32	. 32	35 3.	2 32	35 35	32	32 3	2 32	32	32 3	2 32	32	32 3	22 22	. 32	32	32 3	22	32 3	2 3	2 32	222222222222222222222222222222222222222	
	02192044	22 22	. 32	22 2	2 22	22 22	22	22 2	2 32	22	22 3	2 22	22	22 2	2 22	. 32	22	22 2	22	22 2	2 2	2 22	222222222222222222222222222222222222222	
	02193044	22 22	. 32	25 2.	2 22	22 22	22	22 2	2 22	22	22 3	2 22	22	22 2	22 22	22	22	22 3	22	22 2	2 3	2 22	222222222222222222222222222222222222222	
	02193070	32 32	32	35 3.	2 32	35 35	32	32 3	2 32	32	32 3	2 32	32	32 3	22 32	. 32	32	32 3	22	32 3	2 3	2 32	222222222222222222222222222222222222222	
	02193098	32 32	32	32 3	2 32	35 35	32	32 3	2 32	32	35 3	2 32	32	32 3	22 32	. 32	32	32 3	22	32 3	2 3	2 32	222222222222222222222222222222222222222	
	021/00/0	02 32		02 01		02 02	32	02 0	- 52	02	02 0	2 32	52		~ Ji	. 52	52	02 0	~~	02 0	2 3	2 32		-
	Sector 68765 of 2	205324				Offse	t			219	3BE7					= 4	9 Blo	ock:					n/a Size:	n/a
											_						-				_			

Simpan Screen Image

- 65. Pastikan screen memperlihatkan hex view yang menampilkan akhir dari karakter "1", beberapa bytes nol, dan awal dari karakter "2", sepereti di atas.
- 66. Tekan tombol PrintScrn untuk mengkopi seluruh desktop ke clipboard.

HARUS SUBMIT FULL-SCREEN IMAGE UNTUK MENDAPATKAN POIN MAKSIMAL!

67. Simpan dengan nama "NamaKamu_ Proj8a".

Melihat FILE2.TXT menggunakan WinHex

- 68. Gulung layar ke bawah untuk mencari akhir karakter "2".
- 69. Maka akan terlihat pola yang sama, memenuhi satu sector, dan hamper mengisi sector berikutnya, seperti berikut.

🚟 WinHex - [Drive E:]					
🥪 File Edit Search Nav	igation View Tools Sj	Specialist Options Window Help			_ <u>5</u> ×
D 🖻 🗏 🖨 🗳 🖄	🗆 🗠 💼 💼 🗤 101-	📅 🏘 🚓 🕼 💒 👭 -	• 🕂 🗢 🚽 🕺 🕰 💭 🖬	🔎 🛛 🛋 🖡 🏷 🛍 🔛	
Case Data	Offset 0	0 1 2 3 4 5 6 7	8 9 A B C D E F	10 11 12 13 14 15 16 17 18 19 1.	. 1B 🗸 🔍 🔺
File Edit	02193E04 32	2 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 22222222222222222222222222222222
	02193E20 32	2 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 22222222222222222222222222222222
	02193E3C 32	2 32 32 32 32 32 32 32 32 3	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 222222222222222222222222222222222
	02193E58 32	2 32 32 32 32 32 32 32 32 3	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 22222222222222222222222222222222
Data Interpreter 🗵	02193E74 32	2 32 32 32 32 32 32 32 32 3	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 22222222222222222222222222222222
8 Bit (±): 50	02193E90 32	2 32 32 32 32 32 32 32 32 3	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 222222222222222222222222222222222
16 Bit (±): 50	02193EAC 32	2 32 32 32 32 32 32 32 32 3	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 222222222222222222222222222222222
32 Bit (±): 50	02193EC8 32	2 32 32 32 32 32 32 32 32 3	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 222222222222222222222222222222222
	02193EE4 32	2 32 32 32 32 32 32 32 32 3	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 2222222222222222222222222222222
	02193F00 32	2 32 32 32 32 32 32 32 32 3	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 22222222222222222222222222222222222
	02193F1C 32	$2 \ 32 \ 32 \ 32 \ 32 \ 32 \ 32 \ 32 \ $	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 222222222222222222222222222222222222
	02193F38 32	$2 \ 32 \ 32 \ 32 \ 32 \ 32 \ 32 \ 32 \ $	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 222222222222222222222222222222222222
	02193554 32	2 32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 222222222222222222222222222222222222
	02193570 32	2 32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 222222222222222222222222222222222222
	02193F8C 32	2 32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 222222222222222222222222222222222222
	02193FA8 32	2 32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32	32 222222222222222222222222222222222222
	02193FC4 32	2 32 32 32 32 32 32 32 32 3	32 32 32 32 32 32 32 32 32		
	02193FE0 32	2 32 32 32 32 32 32 32 32 32			00 22222222
	02193FFC 00				00
	02194010 00				00
	02194054 00				00
	02194060 00				00
	02194088 00				00
	02194084 00				00
	02194000 00				00
	021940DC 00				00
	021940F8 00				00
	Sector 68767 of 206324	24 Offset:	2193FE7	= 50 Block:	n/a Size: n/a

70. Berikut ringkasan data layout:

Sector Contents ----- 68764 1s 68765 1s and 0s 68766 2s 68767 2s and 0s

Pada kanan atas WinHex terdapat tombol X, seperti terlihat di gambar. Click tombol X bagian bawah. Tutup "New Volume" drive. Click tombol X yang lain. Untuk menutup WinHex.

Menambah File FILE1.TXT

- 71. Pada komputer virtual, click Start, "My Computer".
- 72. Double-click icon "New Volume" untuk membuka volume.
- 73. Double-click icon **FILE1.TXT** untuk membuka file di Notepad.
- 74. Pada Notepad, click Edit, "Select All", seperti di gambar.
- 75. Di Notepad, click Edit, Copy.
- 76. Di Notepad, click Edit, Paste.
- 77. Di Notepad, click Edit, Paste lagi.
- 78. Di Notepad, click File, Save.
- 79. Tutup Notepad.

Melihat File Fragmen di WinHex

- 80. Pada komputer virtual, click Start, "All Programs", WinHex.
- 81. Dari menu WinHex, click Tools, "Open Disk...".







- 82. Pada kotak "Edit Disk", click "New Volume", dan click tombol OK.
- 83. Dari menu WinHex, click View, Show, "Directory Browser".
- 84. Kotak pops up yang menampilkan snapshot sudah digunakan, seperti pada gambar. Directory Browser sebenarnya bekerja dari copy data yang disebut Snapshot, bukan dari original disk.
- 85. Kita barusan merubah disk, sehingga snapshot yang lama menjadi tidak akurat.
- 86. Jadi click "Take a new one".
- 87. Panel Directory Browser muncul di taengah atas jendela.
- 88. Gulung ke bawah untuk mencari FILE1.TXT dan FILE2.TXT.
- 89. Pada Directory Browser, click FILE1.TXT.
- 90. Perhatikan FILE1 sekarang berukuran 2.0 KB, seperti berikut.

🚟 WinHex - [Drive E]						
🥪 File Edit Search Nat	rigation View Tools Specialist Options	Window Help			_ @ ×	
🗅 🚅 🗏 🎒 😭 🖄	- 🕫 🛍 🖻 🐘 🛔 🗛 🙏 🕯	\$ ∰ ∰ → +Ð 😓	🔿 ⊴ 堤 🥥 🎟 🔎 👸 🖣	۰ 🗈 🗉 🛛 🤌		
Case Data	N.		0 min. ago		12 files, 3 dir.	
Ella Eslà	Name 🔺	Ext. Size Created	Modified Accessed	Attr. 1st sector	×	
nie cyk	\$AttrDef	2.5 KB 01/27/20	13 12:19: 01/27/2013 12:19: 01/27/2013	12:19: SH 68,759		
		0 B 01/27/20	13 12:19: 01/27/2013 12:19: 01/27/2013	12:19: SH		
	Bitmap	25.2 KB 01/27/20	13 12:19: 01/27/2013 12:19: 01/27/2013	12:19: SH 103,258		
Data Interpreter 🛛 📕	Boot \$	8.0 KB 01/27/20	13 12:19: 01/27/2013 12:19: 01/27/2013	12:19: SH 0		
8 Bit (±): 49	SLogFile	2.0 MB 01/27/20	13 12:19: 01/27/2013 12:19: 01/27/2013	12:19: SH 64,663		
16 Bit (±): 12593		32.0 KB 01/27/20	13 12:19: 01/27/2013 12:19: 01/27/2013	12:19: SH 68,775		
32 Bit (±): 825307441	SMFTMirr \$	4.0 KB 01/27/20	13 12:19: 01/27/2013 12:19: 01/27/2013	12:19: SH 103,162		
		0 B 01/27/20	13 12:19: 01/27/2013 12:19: 01/27/2013	12:19: SH		
	SUpCase	128 KB 01/27/20	13 12:19: 01/27/2013 12:19: 01/27/2013	12:19: SH 103,309		
	Volume	0 B 01/27/20	13 12:19: 01/27/2013 12:19: 01/27/2013	12:19: ISH		
	FILE1.TXT	TXT 2.0 KB 01/27/20	13 12:21: 01/27/2013 15:59: 01/27/2013	15:59: IA 68,764		
	FILE2.TXT	TXT 1.0 KB 01/27/20	13 12:21: 01/27/2013 11:15: 01/27/2013	12:21: A 68,766	•	
	Offset 0 1 2 3	1567894	A B C D E F 10 11 12 13	14 15 16 17 18 19 1A 1H	3 🗸 🔍 🔺	
	02193800 31 31 31 31 3	31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31 31	1 1111111111111111111111111111111111111	
	0219381C 31 31 31 31 3	1 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111	
	02193838 31 31 31 31 3	31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111	
	02193854 31 31 31 31 3	1 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31 31	11111111111111111111111111111111	
	02193870 31 31 31 31 3	1 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31	1111111111111111111111111111111111111	
	0219388C 31 31 31 31 3	31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111	
	021938A8 31 31 31 31 3	. 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111	
	021938C4 31 31 31 31 3	1 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31 31	1 1111111111111111111111111111111111111	
	021938E0 31 31 31 31 3	1 31 31 31 31 31 31 31	1 31 31 31 31 31 31 31 31 31 31 31	31 31 31 31 31 31 31 31 31	111111111111111111111111111111111111111	
	021938FC 31 31 31 31 3					
		1 31 31 31 31 31 31 31 1 31 31 31 31 31 31 31				
		L 31 31 31 31 31 31 31 31	1 01 01 01 01 01 01 01 01 01 01 01	01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01		
	31 31 31 31 31 3	. SI SI SI SI SI SI		51 51 51 51 51 51 51 51	· · · · · · · · · · · · · · · · · · ·	
<u> </u>	Sector 68764 of 206324	Offset:	2193800	= 49 Block:	n/a Size: n/a	

L

- 91. Click icon kuning untuk menyembunyikan Directory Browser, seperti yang dilakukan sebelumnya.
- 92. Gulung ke bawah melewati dua sectors karakter "1".
- 93. Gulung ke bawah melewati dua sectors karakter "2".
- 94. Seharusnya ada dua sectors karakter "1" yang lain di bawah karakter "2" seperti terlihat di bawah ini.
- 95. Ringkasan data layout:

Sector	Contents
68764	1s
68765	1s
68766	2s
68767	2s and 0s
68768	1s
68769	1s and 0s

Melihat MFT Record

96. Click icon kuning kecil untuk melihat Directory Browser lain.

- 97. Gulung ke bawah.
- 98. Klik kanan FILE2.TXT.

99. Pada context menu, click Navigation, "Go To FILE Record", sperti di gambar berikut ini.

🚟 WinHex - [Drive E:]				168 <u>- D ×</u>
🥪 File Edit Search Nav	igation View Tools Specialist Options	Window Help		_ <u>-</u> <u>-</u> ×
🗅 🚅 🗟 🎒 🕍	🗆 🕫 🛍 🖻 🔛 🗍 👫 🥼 🖞	: ‱ 桷 │ → ⊕ ⇔ │	♀ 🗯 🔎 🖬 🔎 🛗 🗮 🗎 🍕	>
Case Data	<u>\</u>		3 min. ago	12 files, 3 dir.
File Edit	Name 🔺	Ext. Size Created	Modified Accessed Attr. 1s	t sector
· -	AttrDef	2.5 KB 01/27/2013 12:1	9: 01/27/2013 12:19: 01/27/2013 12:19: SH	68,759
		0 B 01/27/2013 12:1	9: 01/27/2013 12:19: 01/27/2013 12:19: SH	
	📃 \$Bitmap	25.2 KB 01/27/2013 12:1	9 01/27/2013 12:19 01/27/2013 12:19 SH	03,258
Data Interpreter 🛛 📕	SBoot \$	8.0 KB 01/27/2013 12:1	9 01/27/2013 12:19 01/27/2013 12:19 SH	0
8 Bit (±): 50	SLogFile	2.0 MB 01/27/2013 12:1	9: 01/27/2013 12:19: 01/27/2013 12:19: SH	64,663
16 Bit (±): 12850		32.0 KB 01/27/2013 12:1	9: 01/27/2013 12:19: 01/27/2013 12:19: SH	68,775
32 Bit (±): 842150450	SMFTMirr \$	4.0 KB 01/27/2013 12:1	9: 01/27/2013 12:19: 01/27/2013 12:19: SH	03,162
		0 B 01/27/2013 12:1	9: 01/27/2013 12:19: 01/27/2013 12:19: SH	
	SUpCase	128 KB 01/27/2013 12:1	9: 01/27/2013 12:19: 01/27/2013 12:19: SH	03,309
	SVolume	0 B 01/27/2013 12:1	9: 01/27/2013 12:19: 01/27/2013 12:19: ISH	
	FILE1.TXT	TXT 2.0 KB 01/27/2013 12:2	21 01/27/2013 15:59 01/27/2013 15:59 IA	68,764
	FILEZ IXI	1.0 KB 01/2//2013 12:2	21: U172772013 11:15 U17	
	Offset 0 1 2 3 4	56789AB	C D E F 10 11 Viewer Programs	🔸 1A 1B 🗸 🔍
	02193C00 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 Open	32 32 222222222222222222222222222222222
	02193C1C 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 32	32 32 222222222222222222222222222222222
	02193C38 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 into	2 32 32 2222222222222222222222222222222
	02193C54 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 Hide	• 32 32 22222222222
	02193C70 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 Mavigation	Go to beginning or nie 2222222222
	02193C8C 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 Greate Hash Set	List Clusters 222222222
	U2193CA8 32 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 Wipe Securely	G0 T0 FILE Record 2222222222
		32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 - Comu "01/27/2012 12/21	" Find parent object 2222222222
	02173CE0 32 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 Copy U1/2//2013 12:21	See selected item from volume root
	02193010 32 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32 32 3	32 3 Jump to Jom # 1222222222
		32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32 32 3	32 3 Sathurssard offent 222222222
	02193050 32 32 32 32 32 32	32 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32 32 3	32 3 Denote with the 2222222222
				v v v v v v v v v v v v v v v v v v v
<u> </u>	Sector 68766 of 206324	Offset:	2193C00 = 50 Block:	n/a Size: n/a

100. Master File Table (MFT) record berisi informasi tentang FILE2.TXT.

101. Tiap MFT record berawal dengan text ASCII "FILE0".

102. Arahkan ke text, sehingga tampilan menjadi seperti pada gambar berikut.

🚟 WinHex - [Drive E:]																				16.8	- II X
🥪 File Edit Search Nav	vigation View To	ols Specialist	Options	Window	Help																_ 8 ×
🗅 🚅 🗏 🖨 🗳 🖄	i in 🛍 🛍 🛙	1012 🖉	ላ 🧥 😘	HEX 🐴		🖻 💠 🖻) 🗳	} 🖏 👘 🖩		ž	∢ ≻	Ď 🖽		>							
Case Data	Offset	0 1 2	3 4	5 6	7 8	9 A	B C	DEF	10	11 12	13 14	15 16	5 17	18 1	9 1A 1B	Q					•
File Edit	0219C600	46 49 4C	45 3	00 03 0	00 F6	20 10	00 00	00 00 00	01	00 01	00 38	3 00 01	00	58 0	1 00 00	FILE0 ö			8	Х	
	0219C61C	00 04 00	00 00	00 00	00 00	00 00	00 04	00 00 00	1E	00 00	00 09	9 00 00	00 (00 0	0 00 00						
	0219C638	10 00 00	00 60	00 00 1	00 00	00 00	00 00	00 00 00	48	00 00	00 18	8 00 00	00 (8A 3	7 A4 DE	`		н		∎7¤Þ	
	0219C654	CB FC CD	01 FB	89 81 4	A2 C2	FC CD	01 13	5C 1D D8	C8	FC CD	01 8A	A 37 A4	I DE	CB F	'C CD 01	EüI û∎oĂi	I \	ØÉüÍ	∎7¤⊧	Eüİ	
Data Interpreter 🛛 🗵	0219C670	20 00 00	00 00	00 00 1	00 00	00 00	00 00	00 00 00	00	00 00	00 04	01 00	0 00	00 0	0 00 00						
8 Bit (±): 48	0219C68C	00 00 00	00 00	00 00 1	00 00	00 00	00 30	00 00 00	70	00 00	00 00	0 00 00	00	00 0	0 02 00	_	0	P			
16 Bit (±): 48	02190648	54 00 00	00 18	00 01 0	00 05	00 00	00 00	00 05 00	8A OD	37 A4	DE CE	B FC CL	0 01	8A 3	7 A4 DE	T	÷	[7A] ≪⊳∺∵≠	ÞEul	удр	
32 Bit (±): 196656	02190604	CB FC CD	A8 10	37 A4 I	DE CB	FC CD	00 00	37 A4 DE	CB	BC CD	01 00	00 00	00 00	45 0	0 00 00	Eul 74PE0	1 10	PEul	тт	E 0	
	0219C6E0	00 00 00	00 00	00 00 0	00 20		00 00	00 00 00	40	03 46	00 45	00 40	. 00	45 0	0 32 00	TVT			ΤL	E 2	
	021908FC	26 00 54	00 50	00 54 0	00 00		00 00	00 00 00 00 00 00	40		00 01	. 00 00 1 00 00	000	00 0	4 00 00			л a			-
	02190724		00 00	02 00 1	00 01	00 00	00 50	00 00 00	- 40	00 00	00 00	02 95	, 00 , 00	01 0	0 01 00	~	à	4	1.		
	02190750	77 77 77	FF 82	79 47	11 00	00 00	00 00	00 00 00	00	00 00	00 00	00 00	00	00 0	0 00 00	0000106	0				
	02190760	00 00 00	00 00	00 00 1	00 00	00 00	00 00	00 00 00	00	00 00	00 00	00 00	00	00 0	0 00 00	,,,,,,,,,					
	0219C788	00 00 00	00 00	00 00 1	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	0 00	00 0	0 00 00						
	0219C7A4	00 00 00	00 00	00 00 1	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	00	00 0	0 00 00						
	0219C7C0	00 00 00	00 00	00 00	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	00 0	00 0	0 00 00						
	0219C7DC	00 00 00	00 00	00 00 0	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	00 (00 0	0 00 00						
	0219C7F8	00 00 00	00 00	00 09 0	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	00 (00 0	0 00 00						
	0219C814	00 00 00	00 00	00 00 0	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	00 (00 0	0 00 00						
	0219C830	00 00 00	00 00	00 00 0	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	00 0	00 0	0 00 00						
	0219C84C	00 00 00	00 00	00 00 1	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	00 (00 0	0 00 00						
	0219C868	00 00 00	00 00	00 00 1	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	00 (00 0	0 00 00						
	0219C884	00 00 00	00 00	00 00 1	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	0 00	00 0	0 00 00						
	0219C8A0	00 00 00	00 00	00 00 1	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	0 00	00 0	0 00 00						
	0219C8BC	00 00 00	00 00	00 00 1	00 00	00 00	00 00	00 00 00	00	00 00	00 00	0 00 00	0 00	00 0	0 00 00						
	02190808	00 00 00	00 00	00 00 0	00 00	00 00	00 00	00 00 00	00	00 00	00 00	, ,, ,, ,,	000	00 0							
	02190884	00 00 00	00 00	00 00 1	00 00	00 00	00 00	00 00 00	00	00 00	00 00	00 00	00	00 0	0 00 00						-1
	Sector 68835 of 2	206324		Of	fset		219	C604			= 4	18 Block			2"	90600 - 2190604	Size:				5

MFT Record Header

- 103. MFT Record dimulai dengan 56-byte header.
- 104. Yang kita butuhkan menghitung 56 bytes dari titik ini. Akan lebih mudah dengan hanya menampilkan 16 bytes tiap baris
- 105. Dari menu WinHex, click **Options**, **General**.
- 106. Pada sisi kanan, di tengah, masukkan 16 pada kotak "bytes per line", seperti terlihat di bawah.

107. Chek OK.		
neral Uptions		
 Restore last window arrangement³ recent documents in list Items in Windows context menu³ Allow multiple program instances³ Do not update file time Open data windows maximized WinHex context menu Show file icons³ Save program settings in .cfg file³ 	Folder for temporary files: C:\DDCUME^1\Student\LOC Folder for images and backup files: C:\DDCUME^1\Student\LOC Default when adding images Folder for cases and projects: Folder for templates and scripts: Ender for internal back database	Generate 0x 0000A with Enter Generate Tabs with Tab key C0x20 substitute character: Display bytes as text one by one Hexadecimal offsets Virtual addresses in RAM editor Display page separators ³ 16 bytes per line 3 bytes groups
 Number partitions by disk location Auto-detect deleted partitions Sector reading cache Check for surplus sectors Alternative disk access method ³ Substitute pattern for unreadable sectors: UNREADABLESECTOR 	Gallery: Show pictures in archives Gallery: Allow auxiliary thumbnails Preferred thumbnail size: 80	Search hit highlighting in File mode ³ Auto coloring for FILE records etc. ² Block background color: Record background color: Annotation color: Highl. modified bytes: Font: Courier
<u>Q</u> K C <u>a</u> ncel		Notation <u>H</u> elp

- 108. WinHex sekarang menampilkan hanya 16 bytes tiap baris, di beri label 0 meskipun F pada baris "Offset" di atas menu, seperti terlihat di gambar bawah.
- 109. Click pada byte: **46** pertama.
- 110. Tekan Shift key dan tekan panah ke bawah di keyboard tiga kali. Perintah ini memilih tiga baris dari 16 bytes dari total of 48 bytes.
- 111. Tekan dan tahan Shift key, tekan panah kanan sampai bytes 0 hingga 7 pada baris tersebut.

🗱 WinHex - [Drive E:]																				
🥪 File Edit Search Nav	igation View Too	ols Spe	cialist	Opti	ons	Win	wob	Help)											
🗅 🖻 🖩 🎒 🖆 🕍	i in 📭 😤 🛙	1015 n117	(jul	1.8	25	A.P.	¢4		\rightarrow -	1	þ =	⇒	6	9 6	6	ə 📖	Ø	÷ è	()	C
Case Data	Offset	0	1 2	3	4	5	6	7	8	9	A	в	С	D	E	F	 Q 			
File Edit	0219C600	46 4	9 4C	45	30	00	03	00	F6	20	10	00	00	00	00	00	FILEO	ö		
140 236	0219C610	01 0	0 01	00	38	00	01	00	58	01	00	00	00	04	00	00	8	Х		
	0219C620	00 0	0 00	00	00	00	00	00	04	00	00	00	1E	00	00	00				
	0219C630	09 0	0 00	00	00	00	00	00	10	00	00	00	60	00	00	00				
Data Interpreter	0219C640	00 0	0 00	00	00	00	00	00	48	00	00	00	18	00	00	00		Η		
8 Bit (+): 0	0219C650	8A 3	7 A4	DE	CB	FC	CD	01	FB	89	81	A2	C2	FC	CD	01	∎7¤ÞËüÍ	û	∎¢Åü1	:
16 Bit (+): 4096	0219C660	13 5	C 1D	D8	C8	FC	CD	01	8A	37	Α4	DE	CB	FC	CD	01	∖ ØÈüÍ	17	¤þËu1	:
32 Bit (+): 4096	0219C670	20 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	0219C680	00 0	0 00	00	04	01	00	00	00	00	00	00	00	00	00	00				
	0219C690	00 0	0 00	00	00	00	00	00	30	00	00	00	70	00	00	00		0	P	
	0219C6A0	00 0	0 00	00	00	00	02	00	54	00	00	00	18	00	01	00		Т		
	0219C6B0	05 0	0 00	00	00	00	05	00	8A	37	Α4	DE	CB	FC	CD	01		17	¤þËu1	:
	0219C6C0	8A 3	7 À4	DE	CB	FC	CD	01	8A	37	Α4	DE	CB	FC	CD	01	¶7¤þËüÍ	17	¤þËu1	:
	0219C6D0	8A 3	7 À4	DE	CB	FC	CD	01	00	00	00	00	00	00	00	00	7¤ÞÉü1			
	0219C6E0	00 0	0 00	00	00	00	00	00	20	00	00	00	00	00	00	00				
	0219C6F0	09 0	3 46	00	49	00	4C	00	45	00	32	00	2E	00	54	00	FII	Ε	2.1	:
	0219C700	58 0	0 54	00	00	00	00	00	80	00	00	00	48	00	00	00	Х Т		н	
	0219C710	01 0	0 00	00	00	00	03	00	00	00	00	00	00	00	00	00				
	0219C720	01 0	0 00	00	00	00	00	00	40	00	00	00	00	00	00	00		0		
	0219C730	00 0	4 00	00	00	00	00	00	E8	03	00	00	00	00	00	00		è		
	0219C740	E8 0	3 00	00	00	00	00	00	31	02	9E	0C	01	00	01	00	è	1		
	0219C750	FF F	F FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	ÿÿÿÿ∎yG	;		
	0219C760	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	0219C770	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	0219C780	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	0219C790	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	0219C7A0	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	0219C7B0	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00				
																				•
	Sector 68835 of 2	06324						Offs	set:					21	9063	7				= 0

112. Perintah ini memilih 56 bytes dari MFT record header, seperti terlihat di bawah.

Informasi Standard (10\$nbsp;00\$nbsp;00\$nbsp;00)

113. Pada next section merupakan bagian "Standard Information".

114. Tiap section dari MFT dimulai dengan empat-byte identifier—pada contoh 10 00 00 00.

115. Jenis MFT attribute bisa dilihat di sini, from <u>http://grayscale-</u>

research.org/new/pdfs/NTFS%20forensics.pdf

Attribute Name	Hexidecimal Value
Unused	0x00
Standard Information	0x10
File Name	0x30
Object ID	0x40
Security Descriptor	0x50
Volume Name	0x60
Volume Information	0x70
Data	0x80
Index Root	0x90
Index Allocation	0xa0
Bitmap	0xb0
Reparse Point	0xc0
EA Information	0xd0
EA	0xe0
Property Set	0xf0
Logged Utility Stream	0x100

Figure 2.7 MFT Record Attribute Type Table

116. Pada empat bytes berikutnya mengindikasikan panjang section, dalam hexadecimal, dimulai dengan least significant byte.

117. Selanjutnya delapan bytes yang disorot di bawah ini memperlihatkan Standard Information section panjang 60 bytes.

		1	3	0	5													_		
lex - [Drive E:]																				
Edit Search Nav	rigation View Too	ols Speci	alist (Options	Wind	low	Help													
D 🖼 🗏 🖨 🖆 🖄	l in 🗈 🖀 🛙	010	ġ9	HEX 2	в	茵		→ -	•	;	⇒	6	9 6	5	2 🔟	Ω	1	ă ·	• •	()
Case Data	Offset	0 1	2	3 4	5	6	7	8	9	Å	в	С	D	E	F	~		Г		
File Edit	0219C600	46 49	4C	45 30	00	03	00	F6	20	10	00	00	00	00	00	FIL	ΞO	ö		
140 524	0219C610	01 00	01	00 38	00	01	00	58	01	00	00	00	04	00	00		8	Х		
	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				`	
Data Interpreter	0219C640	00 00	00	00 00	00	00	00	48	00	00	00	18	00	00	00			Η		
8 Bit (+): 0	0219C650	8A 37	À4	DE CB	FC	CD	01	FB	89	81	₿2	C2	FC	CD	01	[7¤]	pËüÍ	û	I¢Åü	1
16 Bit (+): 0	0219C660	13 5C	1D	D8 C8	FC	CD	01	8Å	37	Α4	DE	CB	FC	CD	01	1	ðÈüÍ	17	/¤þËü	1
32 Bit (±): 0	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			Т		
	0219C6B0	05 00	00	00 00	00	05	00	8A	37	Α4	DE	CB	FC	CD	01			17	/¤þÉu	Í
	0219C6C0	8A 37	À4	DE CB	FC	CD	01	8Å	37	Α4	DE	CB	FC	CD	01	[7¤]	₽ËüÍ	17	/¤þEu	1
	0219C6D0	8A 37	À4	DE CB	FC	CD	01	00	00	00	00	00	00	00	00	[7¤]	ÞÉüÍ			
	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	F	ΙL	Е	2.	Т
+	0219C700	58 00	54	00 00	00	00	00	80	00	00	00	48	00	00	00	ΧТ		ı	Н	
	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			0		
	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	AAA	j∎yG			
	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					- 1
	Sector 68835 of 2	06324					Offe	etr					21	9063	F					=
<u></u>	00000 0000 012	00027					0113	<u> </u>					21							- (

118. Sorot seluruh Standard Information section. Terdiri dari enam baris 16 bytes, seperti terlihat di bawah.

25	Point

🚟 WinHex - [Drive E:]																				
🧼 File Edit Search Nav	igation View Too	ls Specia	alist	Optic	ns	Wind	low	Help												
🗅 😅 🗐 🎒 🕍	in 🖪 😭 🛛	010	ĝġ	HEX	25	HEX	44		→ -	Ð <	₽ =	⇒	6	9 6	5	2 🔟	Q d	× ř		î 🖩
Case Data	Offset	0 1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	× 🔍			
File Edit	0219C600	46 49	4C	45	30	00	03	00	F6	20	10	00	00	00	00	00	FILEO	ö		
140 624	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			`	
Data Interpreter	0219C640	00 00	00	00	00	00	00	00	48	00	00	00	18	00	00	00		H		
8 Bit (+): 0	0219C650	8A 37	À4	DE	CB	FC	CD	01	FB	89	81	A2	C2	FC	CD	01	7¤ÞEu1	û	∣¢ÅüÍ	
16 Bit (+): 12288	0219C660	13 5C	1D	D8	C8	FC	CD	01	8À	37	À4	DE	CB	FC	CD	01	∖ ØÈü1	17	¤þEuÍ	
32 Bit (±): 12288	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	0	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		Т		
	0219C6B0	05 00	00	00	00	00	05	00	8À	37	Δ4	DE	CB	FC	CD	01		17	¤þEuÍ	
	0219C6C0	8A 37	À4	DE	CB	FC	CD	01	8A	37	À4	DE	CB	FC	CD	01	7¤þEul	17	¤þEuÍ	
	0219C6D0	8A 37	À4	DE	CB	FC	CD	01	00	00	00	00	00	00	00	00	7¤ÞEu1			
	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	FII	. E	2.T	
8	0219C700	58 00	54	00	00	00	00	00	80	00	00	00	48	00	00	00	Х Т		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		(U		
	0219C730	00 04	00	00	00	00	00	00	E8	03	00	00	00	00	00	00		è	-	
	02190740	E8 03	00	00	00	00	00	00	31	02	9E	UC	01	00	01	00	e	1		
	02190750	FF FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	AAAA AG	,		
	02190760	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	02190770	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	02190780	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	02190790	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	0219C/AU	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	0219C/B0	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				-
	Sector 68835 of 2	06324						Offs	et:					21	9069	7				= 0

File Name section

- 119. Section berikutnya dimulai dengan 30 00 00 00 dan panjang 70 bytes, seperti terlihat di bawah.
- 120. Pilih section tersebut.
- 121. Perhatikan nama file yang terbaca di akhir section: FILE2.TXT.
- 122. Karakter ini merupakan karakter Unicode, terdapat 00 byte setelah setiap karakter yang terbaca.

Hex - [Drive E:]							
e Edit Search Na	vigation View To	ols Specialist	Options Window	Help			
□ 🛎 🖩 🖨 🖀 🕍	🗠 🗈 🛍 🛛	a 101	4 🏩 🕾 🔬 🏘		🔿 🗏 🙆 🖣 🥥 🖬	> ∴ 益 ↓ ▷	111
Care Data	Offset	0 1 2	3 4 5 6	7 8 9 A	BCDEF	× 3	•
Els E-D	02190600	46 49 40	45 30 00 03	00 F6 20 10	00 00 00 00 00	FILEO Ö	
Life E dir	02190610	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	`	
Data Interpreter X	0219C640	00 00 00	00 00 00 00	00 48 00 00	00 18 00 00 00	Н	
0 Pà (a): 0	0219C650	8A 37 A4	DE CB FC CD	01 FB 89 81	A2 C2 FC CD 01	7¤þËüÍ û ∣∘ÅüÍ	
16 Bit (+): -32768	0219C660	13 5C 1D	D8 C8 FC CD	01 8A 37 A4	DE CB FC CD 01	∖ ØÈüÍ ∎7¤þËüÍ	
32 Bit (±): 32768	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	Т	
	0219C6B0	05 00 00	00 00 00 05	00 8A 37 A4	DE CB FC CD 01	∎7¤ÞËüÍ	
	0219C6C0	8A 37 A4	DE CB FC CD	01 8Å 37 Å4	DE CB FC CD 01	¶7¤þEüÍ ¶7¤þEüÍ	
	0219C6D0	8A 37 A4	DE CB FC CD	01 00 00 00	00 00 00 00 00	7¤þÉúÍ	
	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	
H I	0219C700	58 00 54	00 00 00 00	00 80 00 00	00 48 00 00 00	ХТ Н	
	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	0	
	0219C730	00 04 00	00 00 00 00	00 E8 03 00	00 00 00 00 00	è	
	0219C740	E8 03 00		00 31 02 9E	OC 01 00 01 00	è 11	
	0219C750	FF FF FF	FF 82 79 47	11 00 00 00	00 00 00 00 00	yyyy∎yG	
	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		
	02190780	00 00 00		00 00 00 00			
	02190790						
	0219C7A0						
	0219C7B0	00 00 00	00 00 00 00	00 00 00 00	00 00 00 00 00		-
<u> </u>	Sector 68835 of 2	06324		Offset:	219C707		= 0

Data Section

123. Section berikutnya dimulai sengan 80 00 00 00 dan panjang 48 bytes, seperti terlihat di bawah.

124. Section ini menunjukkan dimana data sebenarnya disimpan di disk.

125. Pilih section tersebut.

🚟 WinHex - [Drive E:]						
🥪 File Edit Search Navi	igation View Too	ols Specialist Opt	ions Window	Help		
🗅 🖻 🗏 🎒 🖆 🕍	60 🗈 🔒 🛛	101 A	. 16 💒 🖊	→ - 🔁 😓 🖻	> 🛛 🚑 🤤 🛄	🛛 💒 🔸 🕨 🛄
Case Data	Offset	0 1 2 3	4 5 6	7 8 9 A	BCDEF	A 100 A
File E <u>d</u> it	0219C600	46 49 4C 45	30 00 03	00 F6 20 10	00 00 00 00 00	FILE0 ö
	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	
	02190630	09 00 00 00	00 00 00	00 10 00 00		н
Data Interpreter	02190640	93 27 34 DE	CP FC CD	00 40 00 00	A2 C2 EC CD 01	
8 Bit (±): 0	02190660	13 5C 1D D8	C8 FC CD	01 84 37 44	DE CB EC CD 01	V ØFijf 7¤ÞFijf
16 Bit (±): -256	0219C670	20 00 00 00	00 00 00	00 00 00 00		Cobul Prophat
32 DIL (I), -230	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 р 📕
	0219C6A0	00 00 00 00	00 00 02	00 54 00 00	00 18 00 01 00	Т
	0219C6B0	05 00 00 00	00 00 05	00 8Å 37 Å4	DE CB FC CD 01	∎7¤þÉüÍ
	0219C6C0	8A 37 A4 DE	CB FC CD	01 8Å 37 Å4	DE CB FC CD 01	¶7¤þÉüÍ ¶7¤þÉüÍ
	0219C6D0	8A 37 A4 DE	CB FC CD	01 00 00 00	00 00 00 00 00	7¤ÞÉuÍ
	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	хт н
	0219C710	01 00 00 00	00 00 03	00 00 00 00	00 00 00 00 00	
	02190720	01 00 00 00	00 00 00	00 40 00 00		6
	02190730	DU U4 UU UU	00 00 00	00 E8 03 00		e
	02190740	EC US UU UU	00 00 00	11 00 00 00		
	02190750		02 /9 4/			yyyy l yo
	02190770		00 00 00			
	02190780		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 2	06324		Offset:	219C74F	= 0

120. Delapan bytes telakini bensi Data Kun , seperu utunjukkan u bawan in	126.	Delapan b	oytes terakhir be	erisi "Data Run"	', seperti ditun	jukkan di bawah in
120. Delabali Deles le anifi dell'i Dala Null , sedetti utullukkali ul dawali li	126.	Delapan b	ovtes terakhir be	erisi "Data Run"	', seperti ditun	iukkan di bawah in

🚟 WinHex - [Drive E:]																					
🍛 File Edit Search Navi	gation View Too	ls Specia	list O	ptions	Wind	dow	Help)													
🗅 🖻 🗐 🎒 🕍	🗆 🗠 🛍 🖗	010	ĝů,	# 23	HEX	萬		→ -	₽ <	þ =	⇒	6	9 6	5) 🔟	2		ž	•		
Case Data	Offset	0 1	2	3 4	5	6	7	8	9	À	В	С	D	E	F						-
Fig. E.D	02190600	46 49	4C 4	5 30	0.0	03	0.0	F6	20	10	0.0	0.0	0.0	0.0	0.0	FT	LEO	č	i		_
Life E dir	0219C610	01 00	01 0	0 38	00	01	00	58	01	00	00	00	04	00	00		8	X	ŗ		
1	0219C620	00 00	00 0	0 00	00	00	00	04	00	00	00	1E	00	00	00		-	-			
1	0219C630	09 00	00 0	0 00	00	00	00	10	00	00	00	60	00	00	00						
Data Interpreter XI	0219C640	00 00	00 0	0 00	00	00	00	48	00	00	00	18	00	00	00			H	I		
0 D3 (4) 1	0219C650	8A 37	A4 D	E CB	FC	CD	01	FB	89	81	A 2	C2	FC	CD	01	17	¤ÞËü	ίÍΰ	III.	≎ÅüÍ	
16 Bit (+): 1	0219C660	13 5C	1D D	8 C8	FC	CD	01	8A	37	À4	DE	CB	FC	CD	01	\	ØÈü	iÍ I	7¤]	ÞËüÍ	
32 Bit (+): 65537	0219C670	20 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00						
	0219C680	00 00	00 0	0 04	01	00	00	00	00	00	00	00	00	00	00						_
1	0219C690	00 00	00 0	0 00	00	00	00	30	00	00	00	70	00	00	00			0	1	p	
1	0219C6A0	00 00	00 0	0 00	00	02	00	54	00	00	00	18	00	01	00			Т			
1	0219C6B0	05 00	00 0	0 00	00	05	00	8Å	37	Α4	DE	СВ	FC	CD	01			_ 1	7¤]	ÞEuÍ	
1	0219C6C0	8A 37	A4 D	E CB	FC	CD	01	8Å	37	Α4	DE	CB	FC	CD	01	17	¤ÞEu	iI I	7¤]	ÞEuÍ	
1	0219C6D0	8A 37	A4 D	E CB	FC	CD	01	00	00	00	00	00	00	00	00	17	¤ÞÉu	iÍ			
1	0219C6E0	00 00	00 0	0 00	00	00	00	20	00	00	00	00	00	00	00					_	
1	0219C6F0	09 03	46 0	0 49	00	4C	00	45	00	32	00	2E	00	54	00		FΙ	ΙE	2	. T	
1	0219C700	58 00	54 0	0 00	00	00	00	80	00	00	00	48	00	00	00	Х	Т			H	
1	0219C710	01 00	00 0	0 00	00	03	00	00	00	00	00	00	00	00	00						
1	0219C720	01 00	00 0	0 00	00	00	00	40	00	00	00	00	00	00	00			6			
1	02190730	00 04	00 0	0 00	00	00	00	E8	03	00	00	00	00	00	00			e .	•		
1	02190740	E8 U3	00 0	0 00	20	47	11	31	02	95	00	01	00	01	00	e		~ ¹			
1	02190750	FF FF	rr r 00 0	r 62	/9	4/	11	00	00	00	00	00	00	00	00	уу	уу∎у	G			
	02190760	00 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00						
1	02190770	00 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00						
1	02190780	00 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00						
	02190730	00 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00						
	0219C7B0	00 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00						
				0																	-
	Sector 68835 of 2	06324					Offs	set:					21	9C74	C 🗌						= 1

127. Dalam contoh ini, Data Run adalah

31 02 9E OC 01

- 128. Byte pertama seharusnya terbaca sebagai dua nilai individual hexadecimal:
 - 3: 3 bytes terakhir berisi starting cluster number
 - 1: 1 byte pertama berisi panjang bagian file, pada clusters.

Terdapat 2 clusters di baris sini, tiap cluster # 9E 0C 01.

cluster # bytes merupakan notasi "Little Endian", sehingga harus dibalik urutannya, menghasilkan Cluster number 01 0c 9E.

Berarti 1x65536 + 12x256 + 9x16 + 14 = 68766, yang merupakan sector number untuk awalan FILE2.TXT, seperti terlihat pada Directory Browser berikut:

Hex - [Drive E:]						
🥪 File Edit Search Nav	igation View Tools Specialist Options	Window	Help			
🗅 🚅 🗐 🎒 🔛 🕍	🗠 🗈 🖀 🖻 👬 🖌 🗛 🤹 🖯	8 🔬 🚧	→ -Ð <	4 🔿 🕴 🖉 🖏 🖉 🗸) 🛛 🚓 🖌 🕨 🛄	. 🔗
Case Data	1				56 min. ago	
File Ed9	Name 🔺	Ext.	Size Create	ated Modified	Accessed At	tr. 1st sector
Lie Eğir	SAttrDef		2.5 KB 01/27	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: SH	1 68,759
			0 B 01/27.	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: SH	4
	\$Bitmap		25.2 KB 01/27	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: SH	103,258
Data Interpreter	Soot \$		8.0 KB 01/27	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: SH	4 0
8 Bit (±): 50	sLogFile		2.0 MB 01/27.	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: SH	64,663
16 Bit (±): 12850			32.0 KB 01/27	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: SH	68,775
32 Bit (±): 842150450	SMFTMirr \$		4.0 KB 01/27	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: SH	103,162
			0 B 01/27.	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: SH	4
	SUpCase \$		128 KB 01/27	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: SH	103,309
	SVolume \$		0 B 01/27	27/2013 12:19: 01/27/2013 12:1	9: 01/27/2013 12:19: ISI	Н
	FILE1.TXT	TXT	2.0 KB 01/27	27/2013 12:21: 01/27/2013 15:5	9: 01/27/2013 15:59: IA	68,764
	FILE2.TXT	TXT	1.0 KB 01/27	27/2013 12:21: 01/27/2013 11:1	5: 01/27/2013 12:21: A	68,766
	Offset 0 1 2 3 4	5 6	7 8 9	9 A B C D E F 🕓	× 🔍 🔺	
	02193C00 32 32 32 32 32	32 32	32 32 32	2 32 32 32 32 32 32 32	222222222222222222	
	02193C10 32 32 32 32 32	32 32	32 32 32	2 32 32 32 32 32 32 23	2222222222222222	
	02193C20 32 32 32 32 32	32 32	32 32 32	2 32 32 32 32 32 32 23	2222222222222222	
	02193C30 32 32 32 32 32	32 32	32 32 32	2 32 32 32 32 32 32 23	2222222222222222	
	02193C40 32 32 32 32 32	32 32	32 32 32	2 32 32 32 32 32 32 23	2222222222222222	
	02193C50 32 32 32 32 32	32 32	32 32 32	2 32 32 32 32 32 32 23	22222222222222222	
	02193C60 32 32 32 32 32	32 32	32 32 32	2 32 32 32 32 32 32 23	222222222222222222	
	02193C70 32 32 32 32 32	32 32	32 32 32	2 32 32 32 32 32 32 2	22222222222222222	
	02193C80 32 32 32 32 32	32 32	32 32 32	2 32 32 32 32 32 32 32 23	222222222222222222222222222222222222222	
		32 32	32 32 32	2 32 32 32 32 32 32 32 2	2222222222222222222	
	02193CAU 32 32 32 32 32 32	32 32	32 32 32	2 32 32 32 32 32 32 32	2222222222222222222	
		32 32	32 32 32 32	2 32 32 32 32 32 32 32 2	222222222222222222	
	52 52 52 52 52	52 52			-	
	Sector 68766 of 206324		Offset:	2193C00	= 50	Block:

Data Run untuk FILE1.TXT

- 129. Click icon kuning kecil untuk menampilkan kembali Directory Browser.
- 130. Klik kanan **FILE1.TXT**.
- 131. Pada context menu, click **Navigation**, "Go To FILE Record".
- 132. Cari MFT record seperti yang dilakukan sebelumnya, untuk mencari Data section dan File Run.
- 133. Kali ini File Run berisi dua sections: satu dimulai dengan dengan 31 dan satu lainnya dimulai dengan 11, seperti terlihat di bawah.
- 134. Porsi yang kedua lebih simple karena sector numbers bersifat relatif.
- 135. 11 02 04, yang berarti "dua lebih sectors, dimulai dengan empat sectors setelah previous block of data".
- 136. Pilih Data Run, termasuk delapan bytes, seperti berikut.

WinHex - [Drive E:]	ination View To	ols Special	ist Ontion	s Window	Help		
		1012	A 🎎 🕈	\$ #£ #4		l 4 → 2	
Case Data	Offset	0 1	2 3	4 5 6	7 8 9	9 A B C D E F	 A A
File Edit	0219C200	46 49	4C 45 3	0 00 03	00 AC 5E	B 10 00 00 00 00 00	FILE0 ¬[
	0219C210	01 00	01 00 3	8 00 01	00 88 01	1 00 00 00 04 00 00	8 1
	0219C220	00 00	00 00 0	0 00 00	00 05 00	0 00 00 1D 00 00 00	
	0219C230	09 00	00 00 0	0 00 00	00 10 00	0 00 00 60 00 00 00	,
ata Interpreter 🛛 🔟	0219C240	00 00	00 00 0	0 00 00	00 48 00	0 00 00 18 00 00 00	H
8 Bit (+): 4	0219C250	1Å C5	20 D9 C	B FC CD	01 8C B0	0 4D 4D EA FC CD 01	Å ÙÉuÍ ∎°MM⊜uÍ
16 Bit (±): 4	0219C260	8C B0	4D 4D E	A FC CD	01 8C B0	0 4D 4D EA FC CD 01	'*MMêüÍ *MMêüÍ
32 Bit (±): 1871708164	0219C270	20 00	00 00 0	0 00 00	00 00 00	0 00 00 00 00 00 00	
	0219C280	00 00	00 00 0	4 01 00	00 00 00	0 00 00 00 00 00 00	
	0219C290	00 00	00 00 0	0 00 00	00 30 00	0 00 00 70 00 00 00	0 p
	0219C2A0	00 00	00 00 0	0 00 02	00 54 00	0 00 00 18 00 01 00	T
	0219C2B0	05 00	00 00 0	0 00 05	00 1A C5	5 20 D9 CB FC CD 01	A UEuI
	0219C2C0	1Å C5	20 D9 C	B FC CD	01 1Å C5	5 20 D9 CB FC CD 01	A UEuI A UEuI
	0219C2D0	1Å C5	20 D9 C	B FC CD	01 00 00	0 00 00 00 00 00 00	A UEuI
	0219C2E0	00 00	00 00 0	0 00 00	00 20 00	0 00 00 00 00 00 00	
	0219C2F0	09 03	46 00 4	9 00 4C	00 45 00	0 31 00 2E 00 54 00	FILE1.T
	0219C300	58 00	54 00 0	0 00 00	00 40 00	0 00 00 28 00 00 00	XT @ (
	0219C310	00 00	00 00 0	0 00 04	00 10 00	0 00 00 18 00 00 00	
	0219C320	CF 87	BE 99 D	2 68 E2	11 83 86	6 00 0C 29 57 FB A9	I ¼ Ohâ II)∛ú©
	0219C330	80 00	00 00 5	0 00 00	00 01 00	0 00 00 00 00 03 00	I P
	0219C340	00 00	00 00 0	0 00 00	00 03 00	0 00 00 00 00 00 00	
	0219C350	40 00	00 00 0	0 00 00	00 00 08	8 00 00 00 00 00 00	0
The second secon	0219C360	D0 07	00 00 0	0 00 00	00 D0 07	7 00 00 00 00 00 00	Đ Đ
X	0219C370	31 02	9C 0C 0	1 11 02	04 00 90	0 6F E1 0C 59 C3 ED	1 Ioá YAi
	0219C380	FF FF	FF FF 8	2 79 47	11 00 00	0 00 00 00 00 00 00	AAAA AQ
	0219C390	00 00	00 00 0	U 00 00	00 00 00	U UU OO OO OO OO OO	
	0219C3A0	00 00	00 00 0	0 00 00	00 00 00	U UU OO OO OO OO OO	
	0219C3B0	00 00	00 00 0	0 00 00	00 00 00	u uu oo oo oo oo oo	
	Sealer 60022 - (.2	100000			Offeet	2100277	
1	Sector 68833 of 2	206324			Unset:	2190377	

Simpan Screen Image

137. Pastikan delapan bytes dipilih, dengan byte pertama **31** dan byte ke-enam **11**.

138. Tekan PrintScrn untuk mengkopi seluruh desktop ke clipboard.

HARUS SUBMIT FULL-SCREEN IMAGE UNTUK MENDAPATKAN POIN PENUH!

139. Simpan dengan nama file "NamaKamu_Proj8b".

Mengumpulkan Project

Kirim melalui elearning

Sources

http://www.epyxforensics.com/node/37 http://stam.blogs.com/8bits/2009/10/lab-ftk-imager-file-carving-using-the-mft-.html http://grayscale-research.org/new/pdfs/NTFS%20forensics.pdf

Last modified: 4-9-13