Project 8: NTFS Data Runs (25 points)

Tujuan

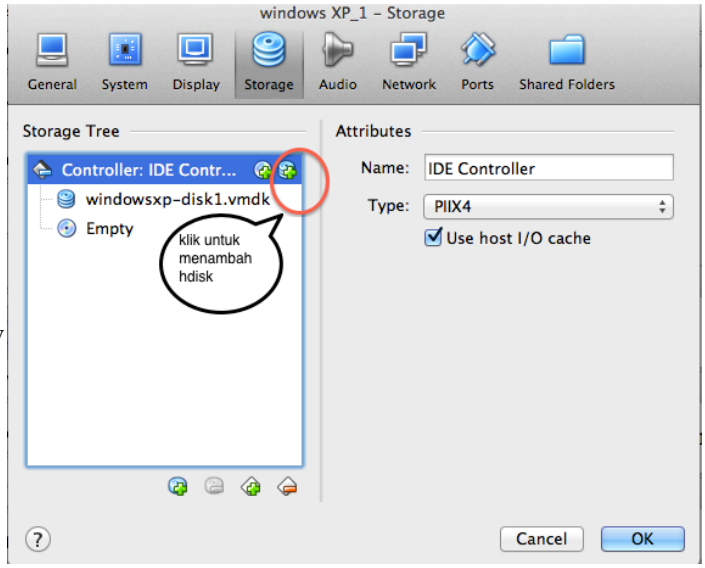
Untuk mempelejari struktur direktori pada level biner.

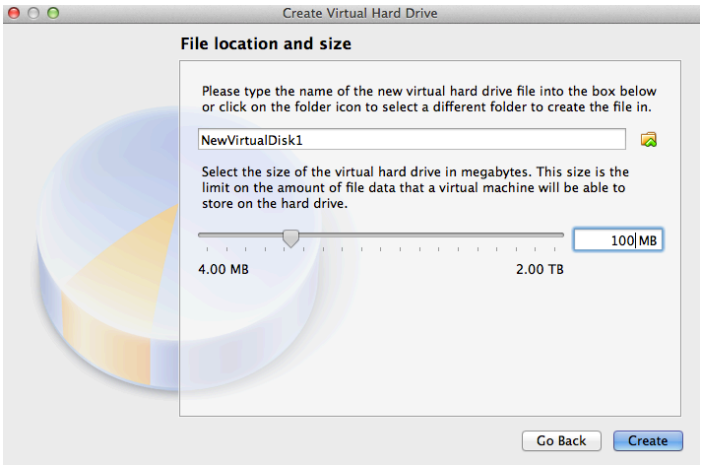
Kebutuhan Project

- 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

1. 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.
3. 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.
4. 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.





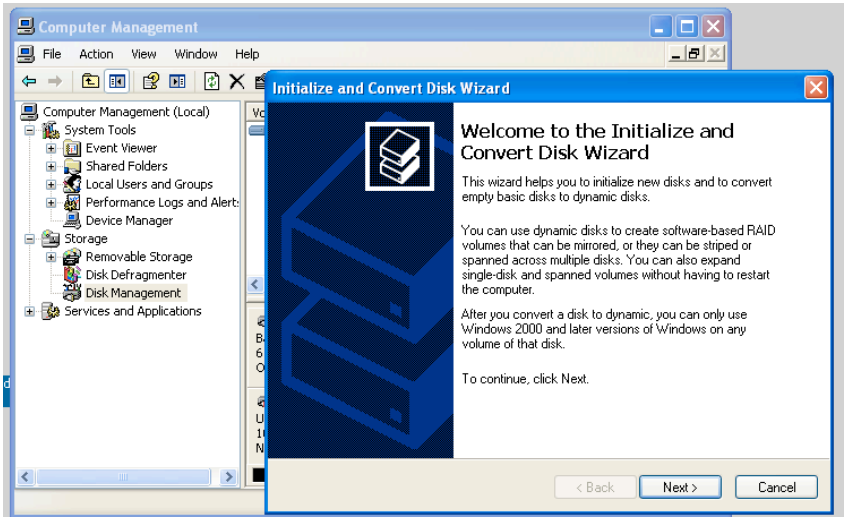
6. Klik tombol **Create.** Maka akan kembali ke jendela setingan Windows-XP-SP3. Klik tombol OK di pojok kanan bawah. Maka jendela akan kembali ke jendela VirtualBox.

Membersihkan Disk Secara Forensic

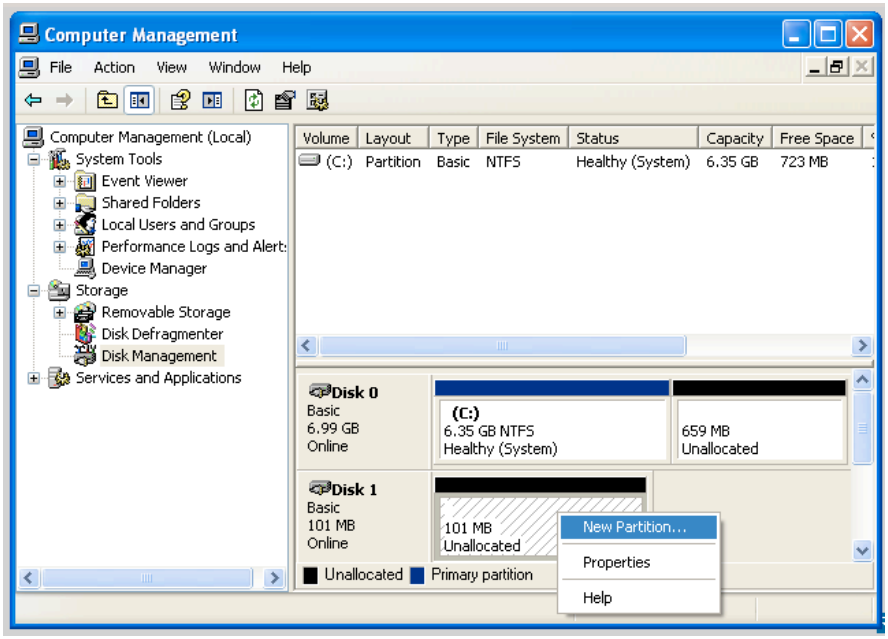
7. Jalankan Komputer WindowsXP SP3 virtual.
8. Windows bisa mengakses disk. Tapi jangan anggap disk yang baru dibuat tersebut clean—disk kadang-kadang masih berisi data lama (ingat hasil di Project 1).
9. Jadi kita lakukan pembersihan dengan cara forensic, menulis 00 pada tiap byte.
10. Pada komputer 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

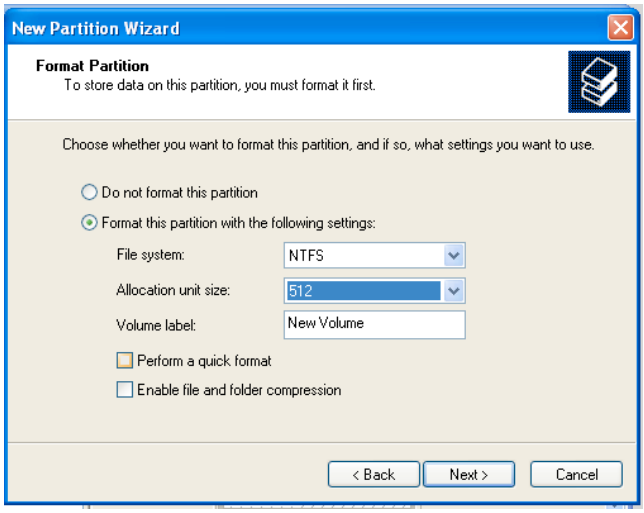
15. Pada komputer virtual, click **Start**.
16. Klik kanan "**My Computer**" dan click **Manage**.
17. Pada panel sebelah kiri dari Computer Management, click "**Disk Management**".
18. "Initialize and Convert Disk Wizard" akan terbuka, seperti pada gambar.
19. Click **Next**.
20. Pada menu "Select Disks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



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, dan click **Next**.

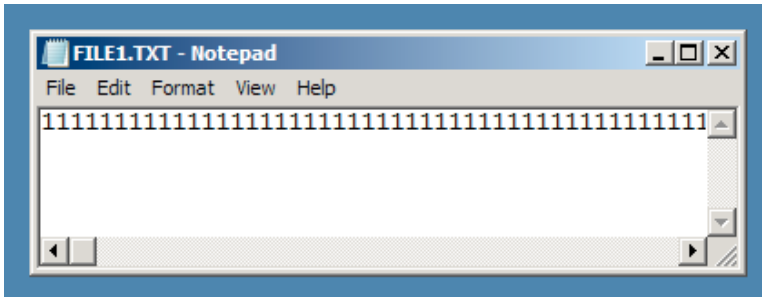


Ukuran tersebut membuat tiap cluster sama dengan sector (1 sector= 512 byte), sama seperti cara kerja floppy disks. Untuk disk yang berukuran besar hal ini tidak efisien karena memperlambat proses pembacaan disk, tapi untuk disk ukuran kecil tidak bermasalah hanya untuk menyederhanakan project.

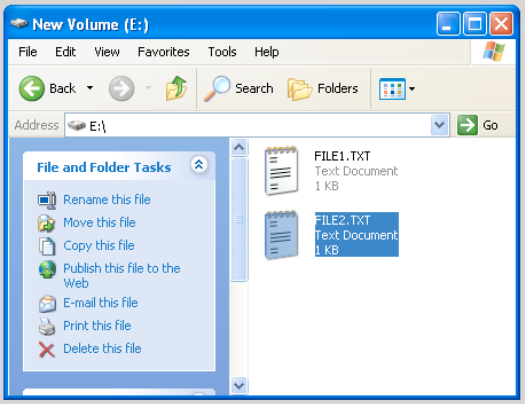
31. Pada menu "Completing the New Partition Wizard", click **Finish**.
32. Tutup Computer Management.

Mendownload File Test

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



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.

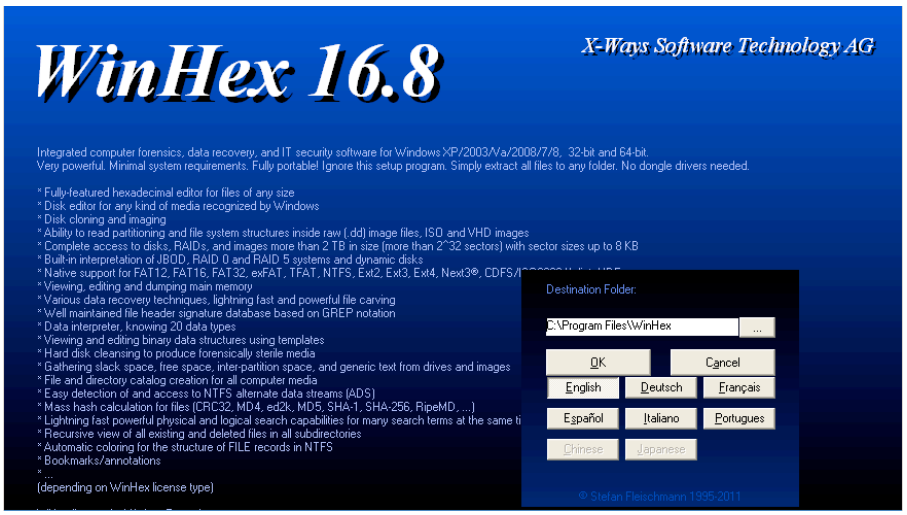


Mengkopi Test Files ke Partisi Baru

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

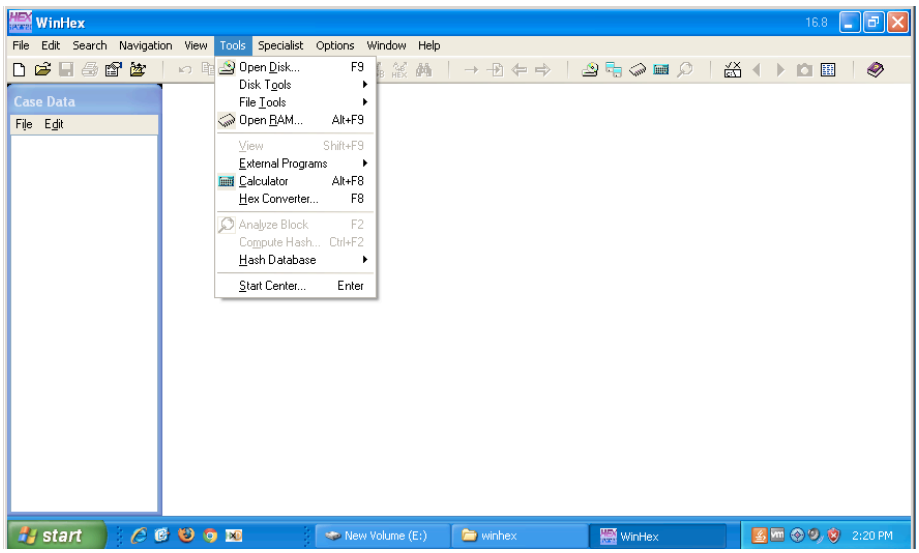
44. Buka browser dan arahkan ke http://winhex.com , atau bisa di download di elearning. Simpan di desktop.
45. Pada jendela desktop, atau dimanapun file di simpan, klik kanan file **winhex.zip** dan click "**Extract All...**".
46. Pada kotak "Welcome to the Compressed (zipped) Folders Extraction Wizard" box, click **Next**, **Next**, **Finish**.
47. Folder dengan beberapa files terbuka. Double-click file **setup.exe**.



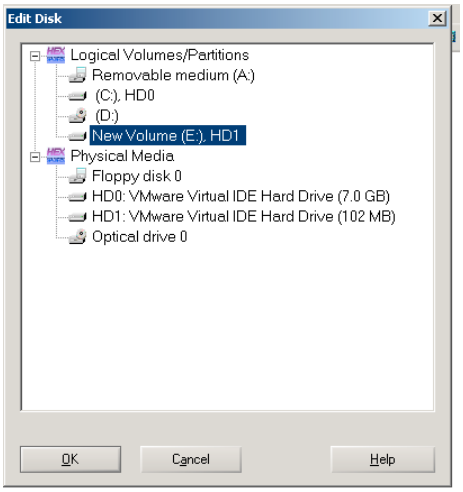
48. Pada menu "WinHex 16.8", di kanan bawah seperti terlihat di gambar, click tombol **English**.
49. Kemudian click tombol **OK**.
50. Pada kotak "Setup", click **Yes**. Pada kotak "WinHex" box, click **Yes**
51. WinHex akan terbuka , seperti pada gambar.

Melihat Data menggunakan WinHex

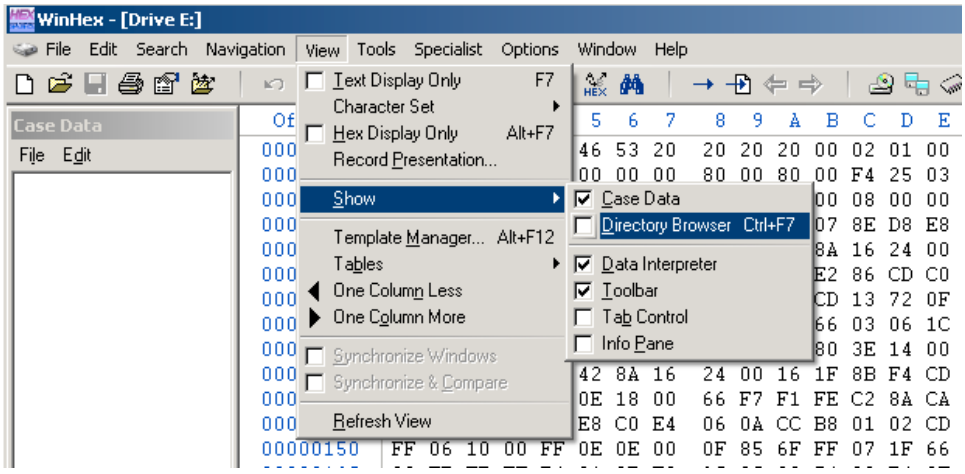
52. Dari menu WinHex, click **Tools**, "**Open Disk...**".



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

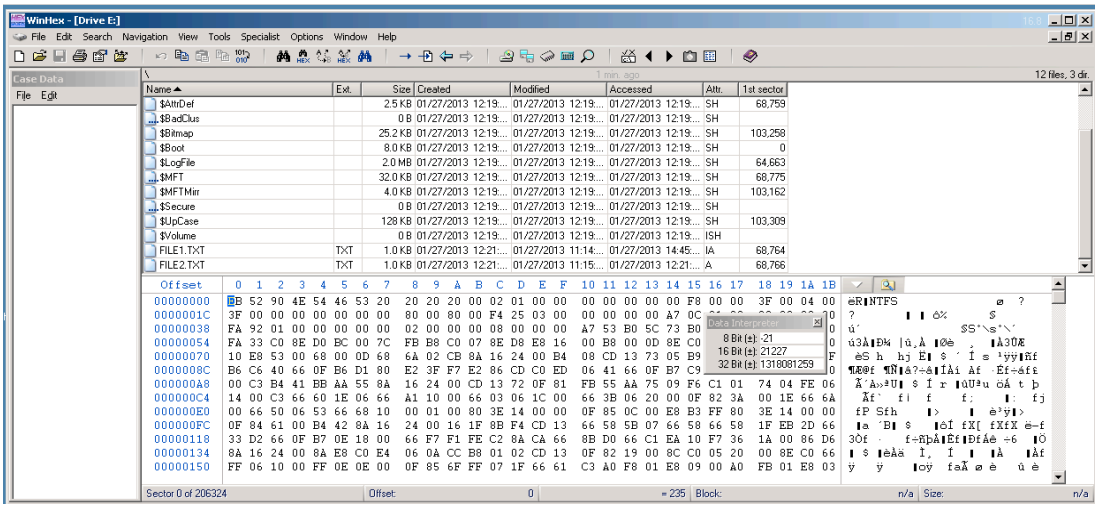


54. Dari menu WinHex menu, click **View**, **Show**, "**Directory Browser**", seperti terlihat di bawah ini.

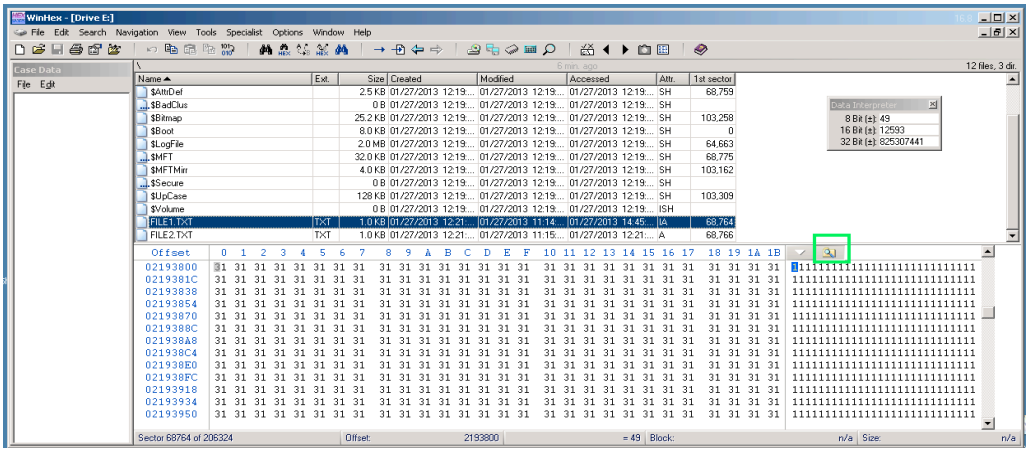


55. Panel Browser direktori akan muncul di bagian tengah atas jendela.

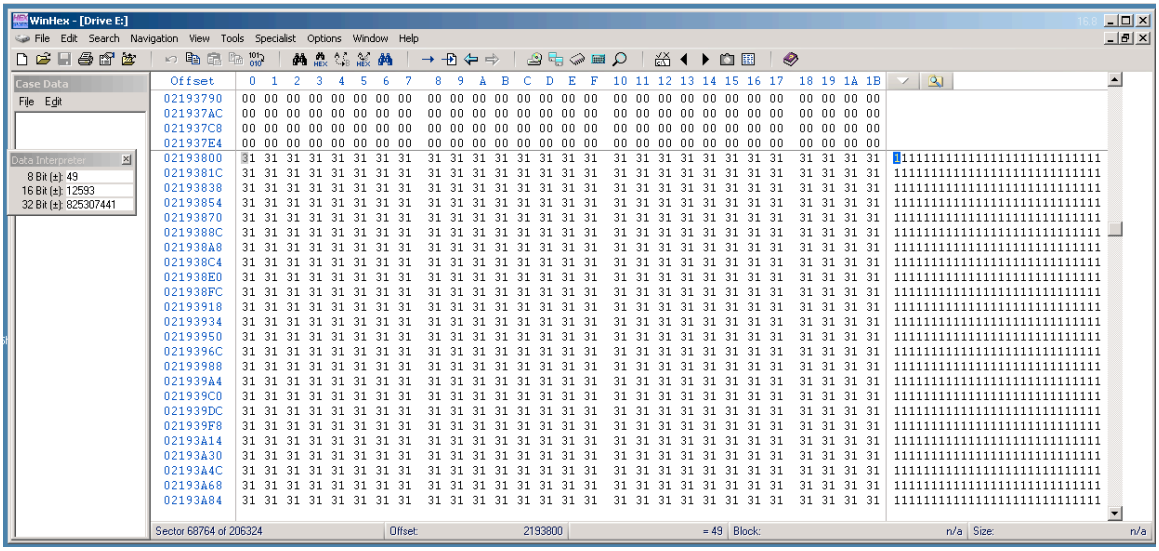
56. Gulung layar ke bawah untuk mencari FILE1.TXT dan FILE2.TXT, seperti terlihat di bawah.



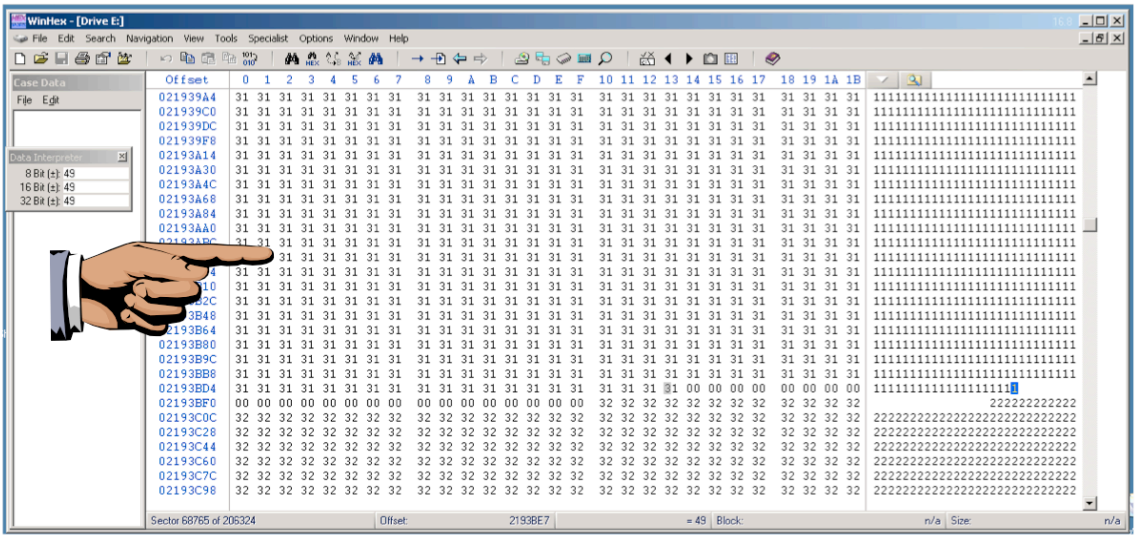
57. Pada Directory Browser, click **FILE1.TXT**.
58. Pada panel bawah memperlihatkan raw hex data pada cluster pertama yang berisi data FILE1.TXT, seperti terlihat di bawah.



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.



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).



Simpan Screen Image

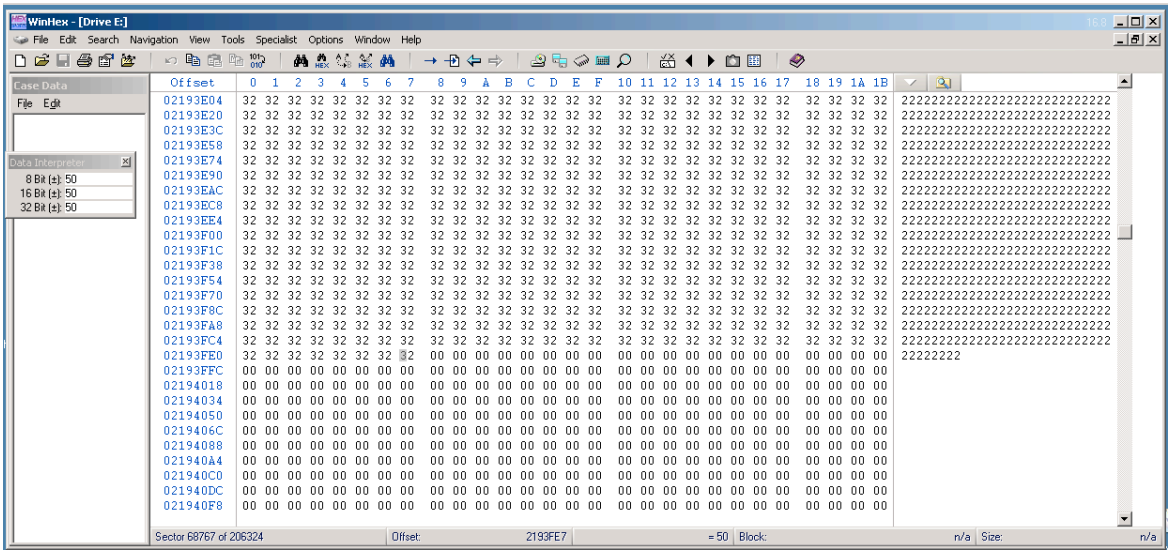
65. Pastikan screen memperlihatkan hex view yang menampilkan akhir dari karakter "1", beberapa bytes nol, dan awal dari karakter "2", sepereti di atas.
66. Tekan tombol PrintScrn untuk mengkopi seluruh desktop ke clipboard.

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.



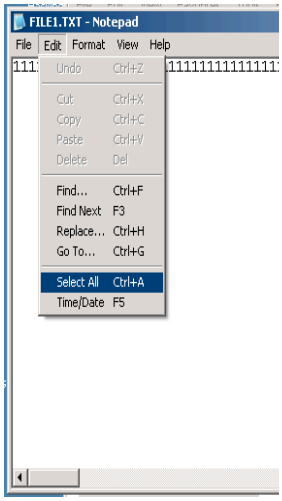
70. Berikut ringkasan data layout:

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.

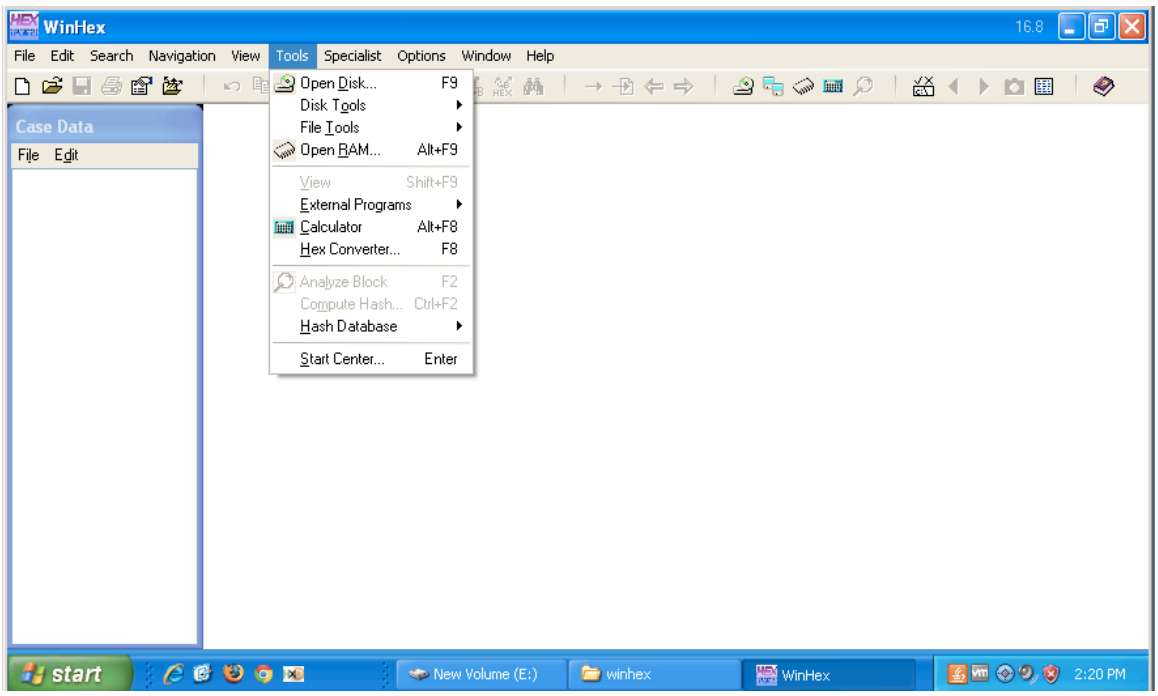
Menambah File FILE1.TXT

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.



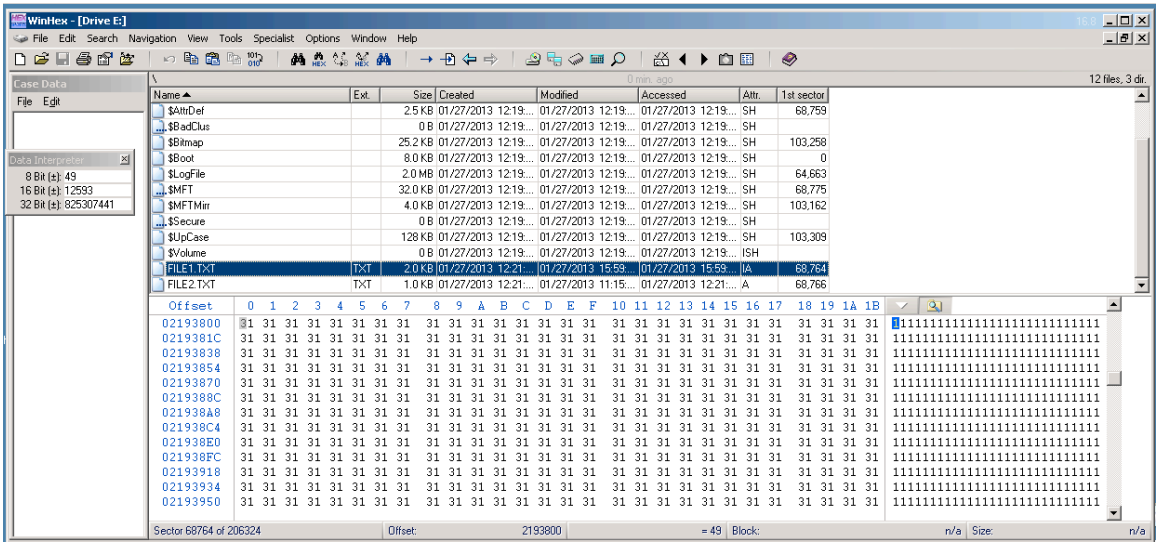
Melihat File Fragmen di WinHex

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.

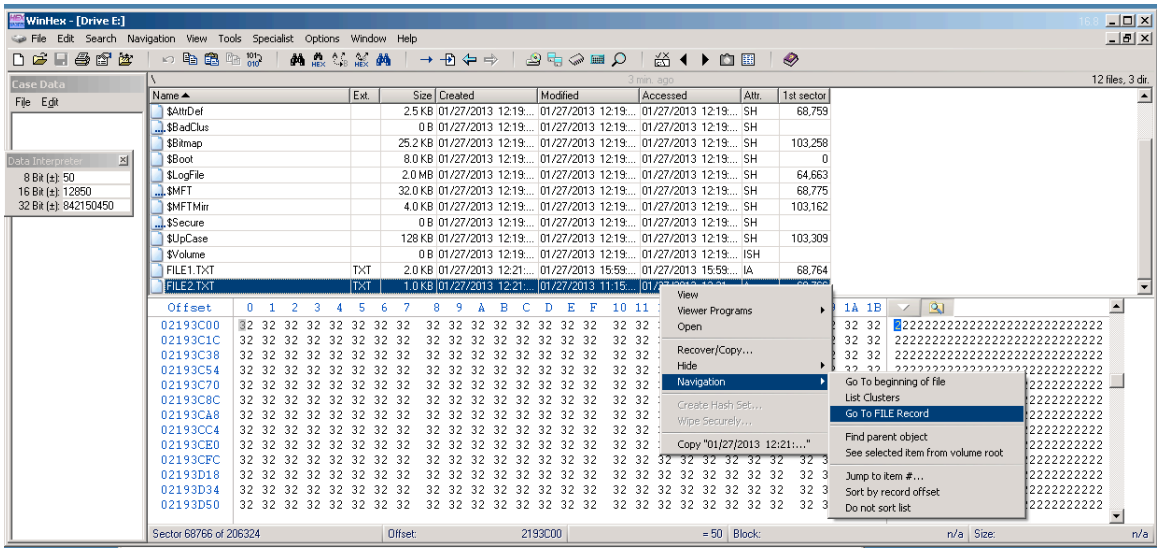


91. Click icon kuning untuk menyembunyikan Directory Browser, seperti yang dilakukan sebelumnya.
92. Gulung ke bawah melewati dua sectors karakter "1".
93. Gulung ke bawah melewati dua sectors karakter "2".
94. Seharusnya ada dua sectors karakter "1" yang lain di bawah karakter "2" seperti terlihat di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

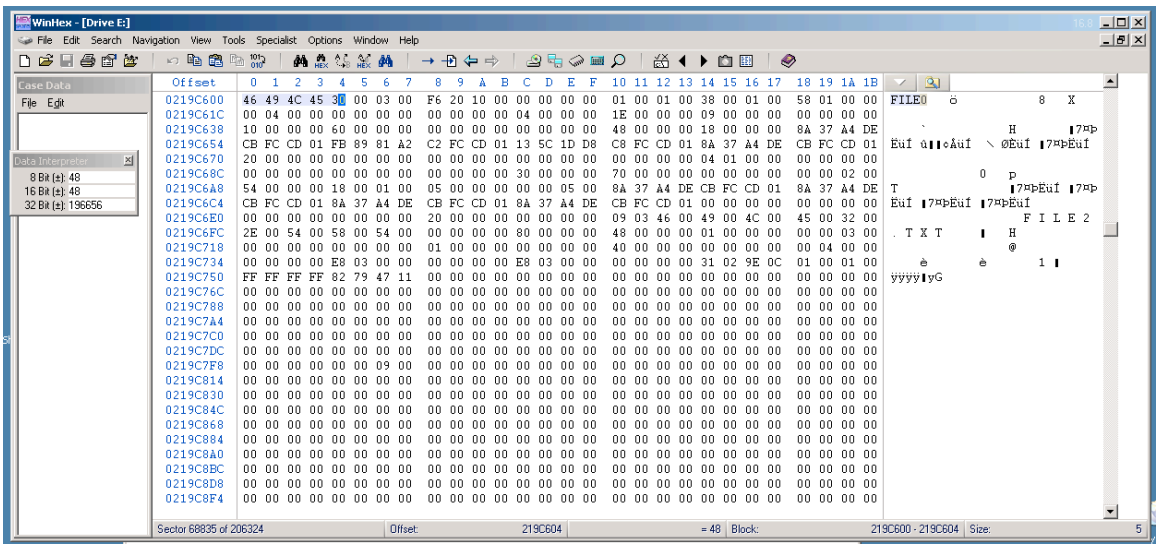
Sector	Contents
68764	1s
68765	1s
68766	2s
68767	2s and 0s
68768	1s
68769	1s and 0s

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.



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.



MFT Record Header

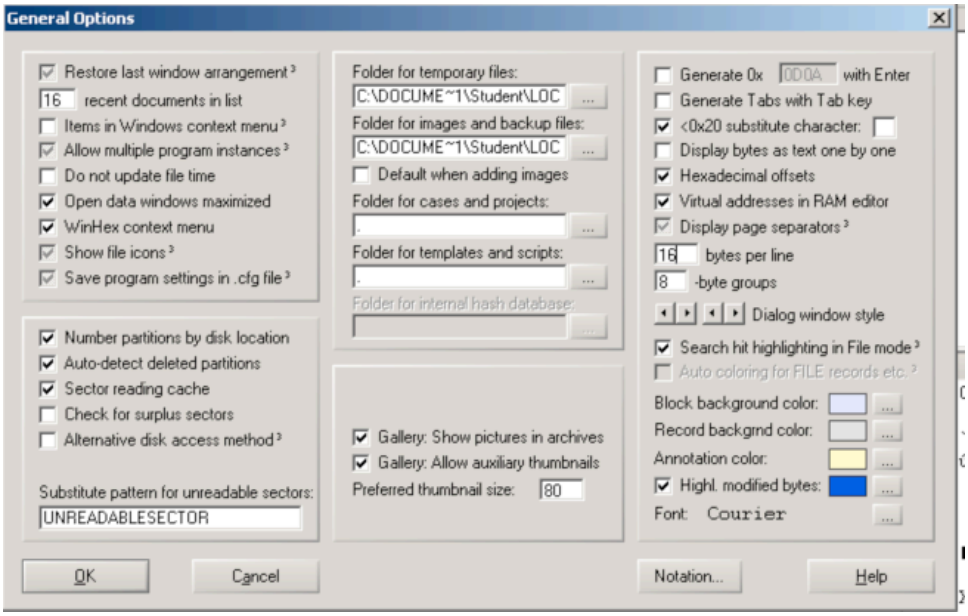
103. MFT Record dimulai dengan 56-byte header.

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. Click **OK**.



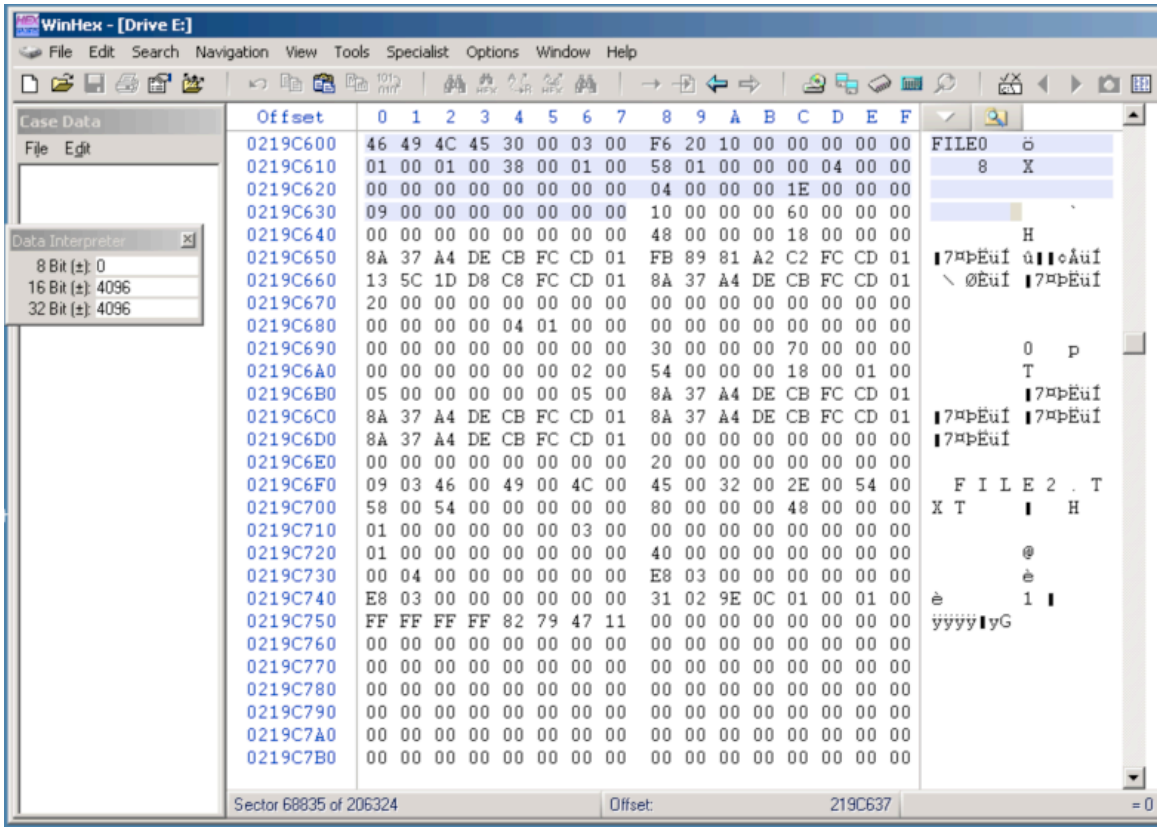
108. WinHex sekarang menampilkan hanya 16 bytes tiap baris, di beri label 0 meskipun F pada baris "Offset" di atas menu, seperti terlihat di gambar bawah.

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.

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.

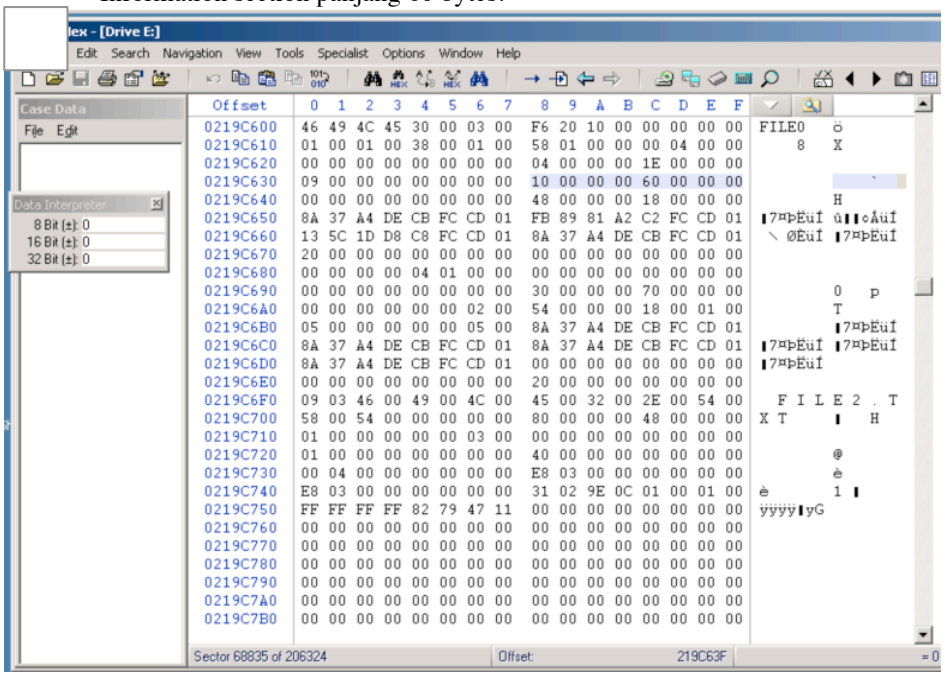
115. Jenis MFT attribute bisa dilihat di sini, from http://grayscale-research.org/new/pdfs/NTFS%20forensics.pdf

Figure 2.7 MFT Record Attribute Type Table

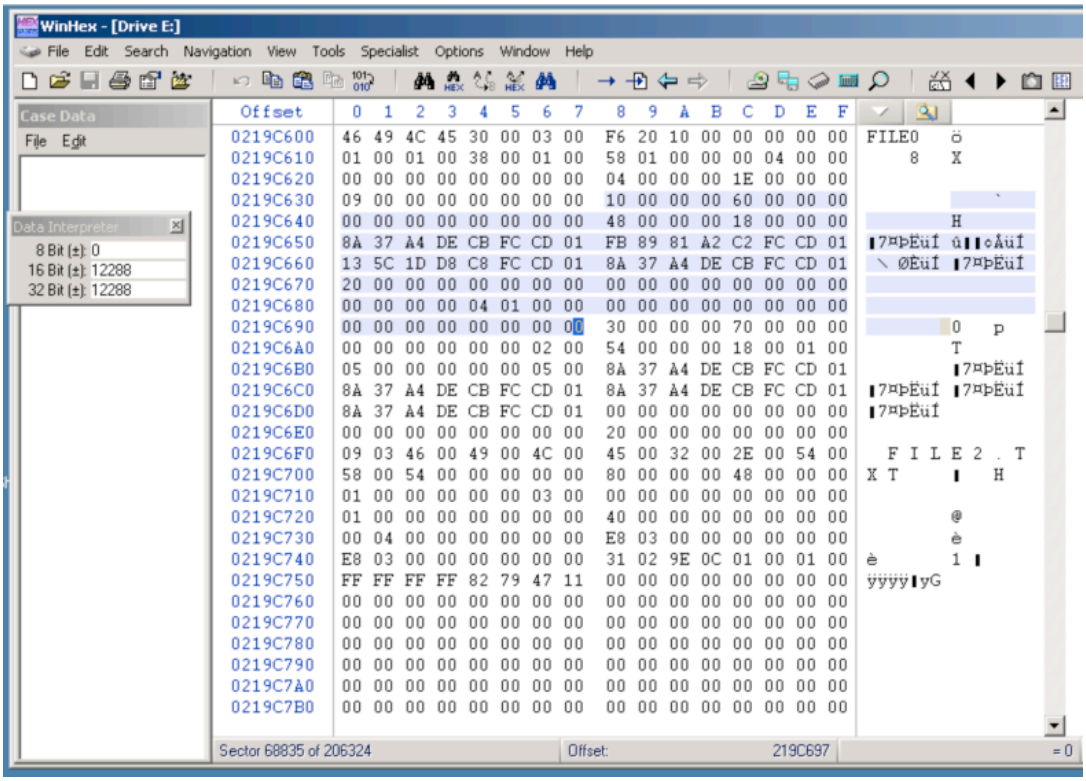
Attribute Name	Hexidecimal Value
Unused	0x00
Standard Information	0x10
File Name	0x30
Object ID	0x40
Security Descriptor	0x50
Volume Name	0x60
Volume Information	0x70
Data	0x80
Index Root	0x90
Index Allocation	0xa0
Bitmap	0xb0
Reparse Point	0xc0
EA Information	0xd0
EA	0xe0
Property Set	0xf0
Logged Utility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

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.

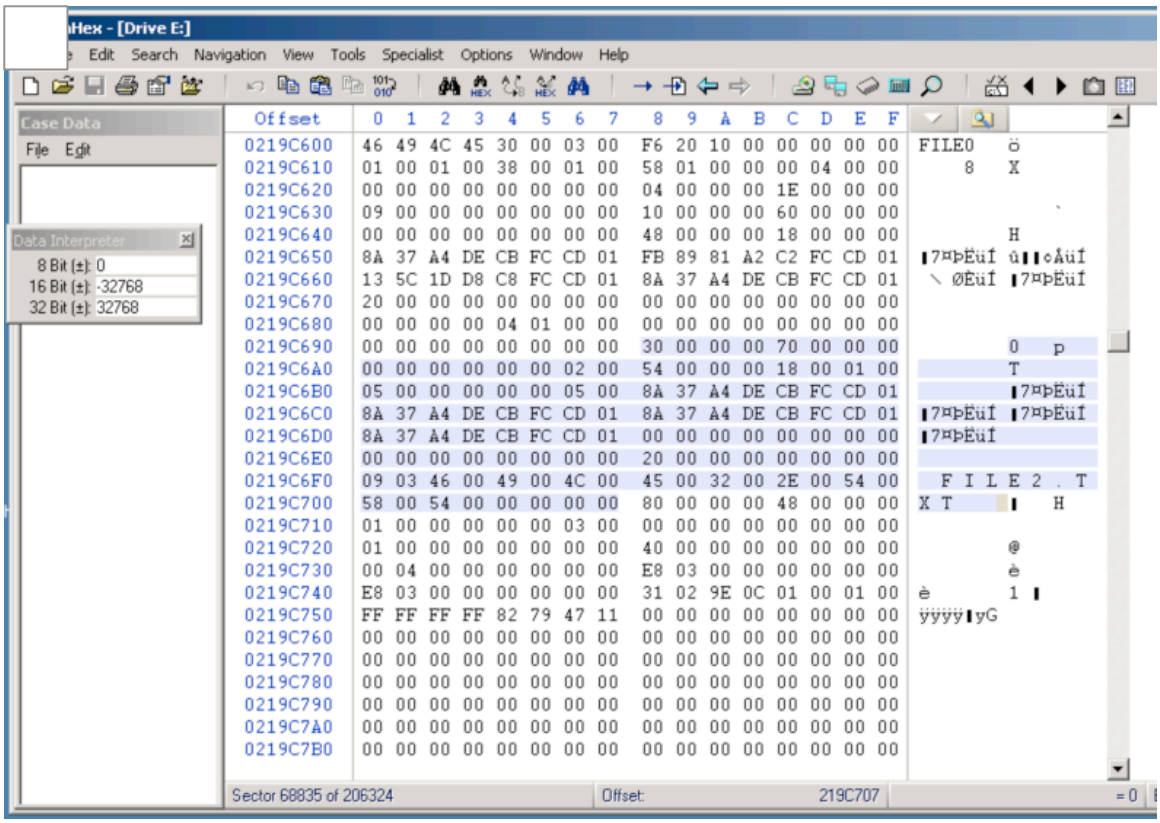


118. Sorot seluruh Standard Information section. Terdiri dari enam baris 16 bytes, seperti terlihat di bawah.



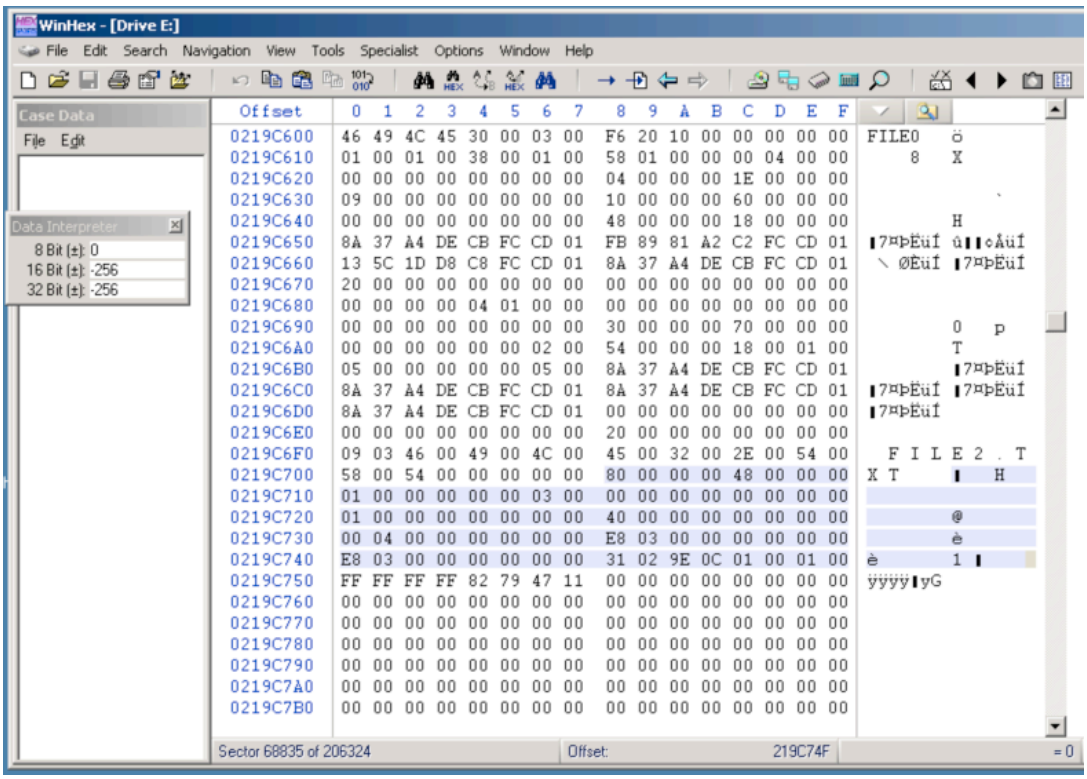
File Name section

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.

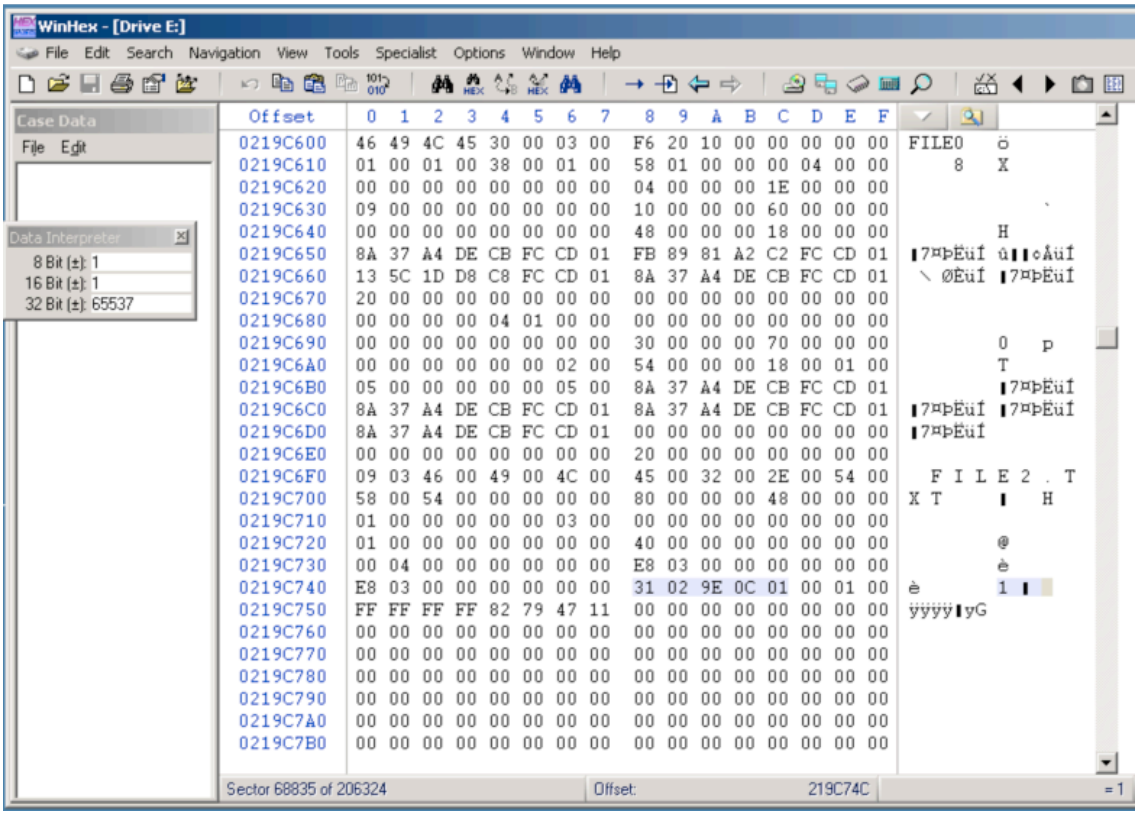


Data Section

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.



126. Delapan bytes terakhir berisi "Data Run", seperti ditunjukkan di bawah ini.

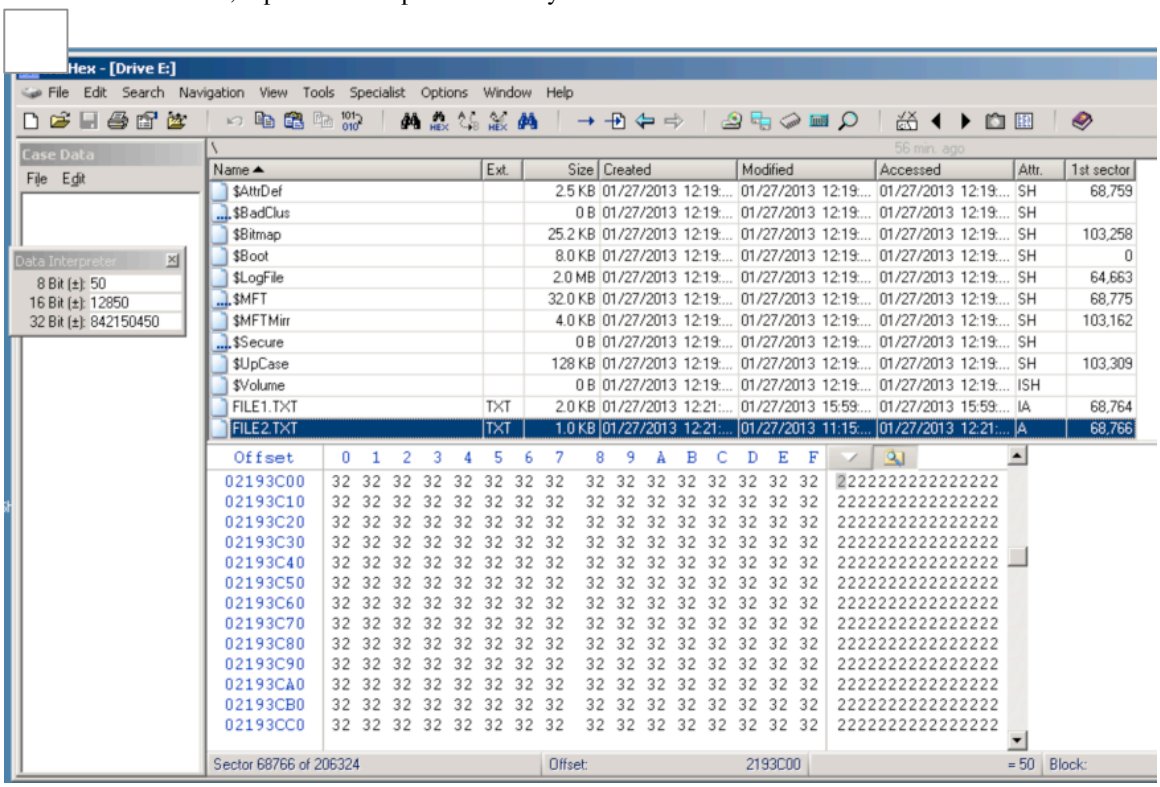


127. Dalam contoh ini, Data Run adalah

31 02 9E 0C 01

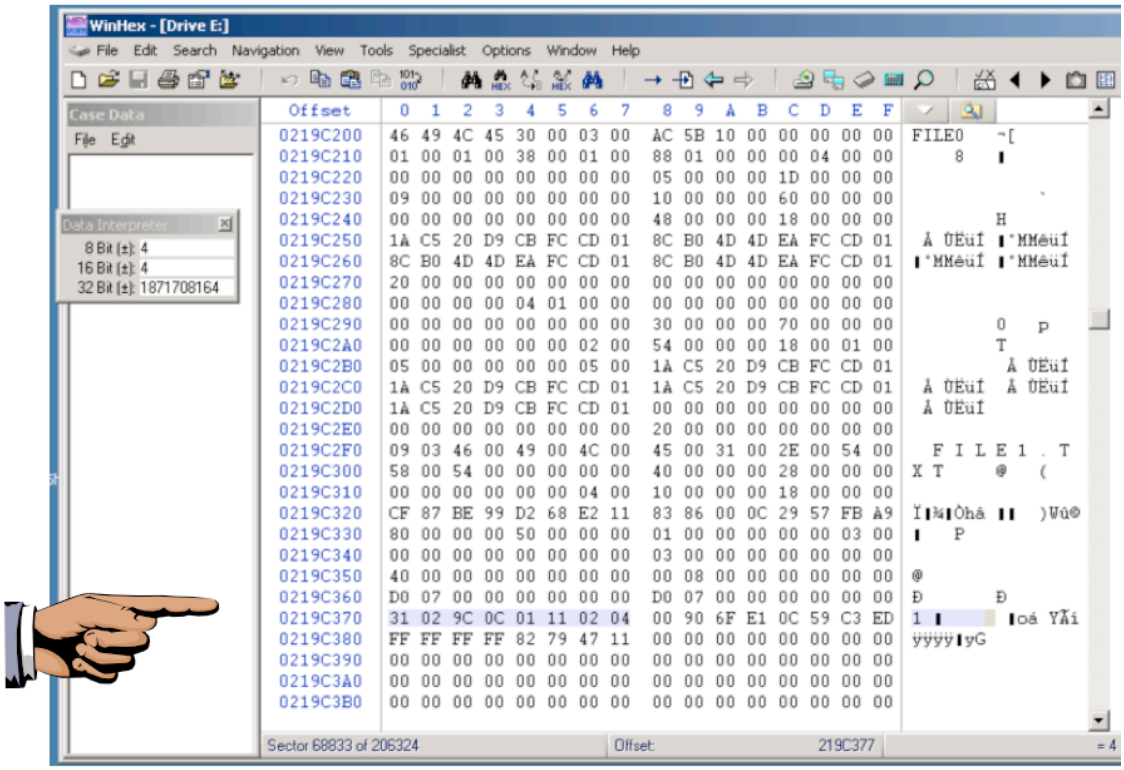
128. Byte pertama seharusnya terbaca sebagai dua nilai individual hexadecimal:
3: 3 bytes terakhir berisi starting cluster number
1: 1 byte pertama berisi panjang bagian file, pada clusters.

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:



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.



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