Project 9: Memperbaiki Partition Table dengan TestDisk (25 points)

Tujuan

Untuk meriksa Tabel Partisi Basic, merusaknya, dan memperbaikinya dengan TestDisk.

Kebutuhan Project

- Komputer Windows virtual, bisa XP atau 7. Instruksi di sini menggunakan VirtualBox dan Windows XP virtual machine.
- Jika menggunakan komputer di laboratorium Foresec gunakan komputer WinXPSP3, jangan WinXPSP1.

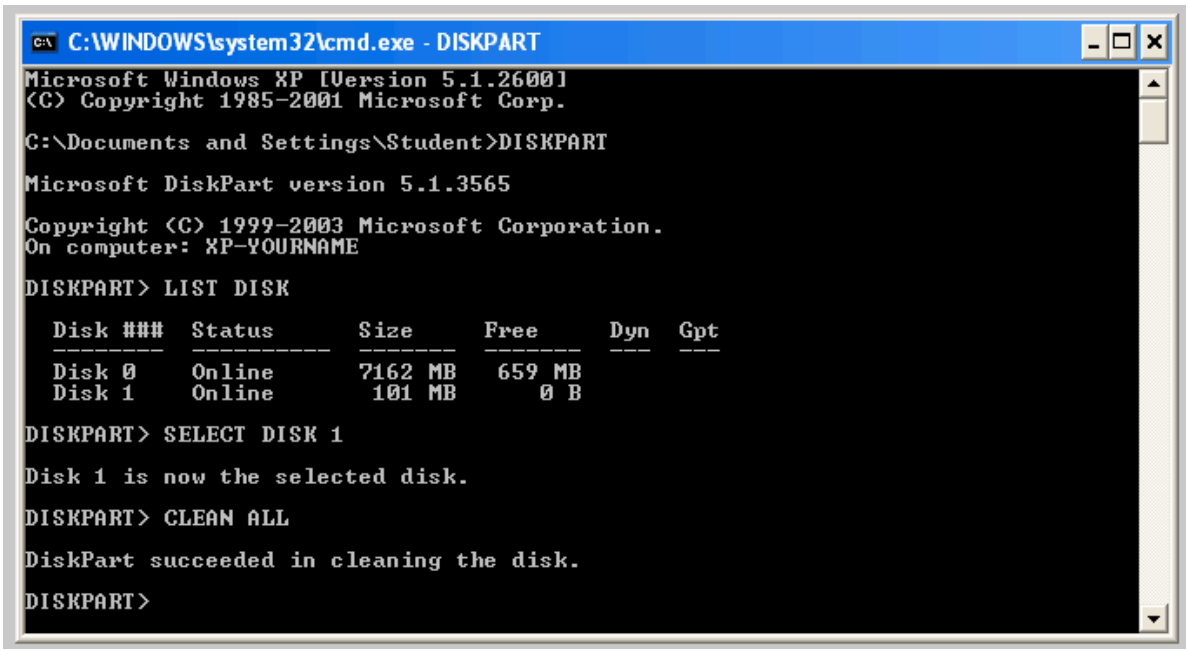
Menambahkan Small Disk ke Virtual Komputer

1) Jika sudah mengerjakan project sebelumnya (project 7), seharusnya sudah ada small virtual hard disk pada komputer Virtual. (Jika belum ada ikuti instruksi pada tutorial Project 7 langkah 1-6).

Membersihkan Disk Secara Forensic

2) Pada komputer virtual, click **Start**, **Run**.
   a) Pada kotak Run, ketikkan **CMD** dan tekan Enter untuk membuka Command Prompt.
   Pada jendela Command Prompt, ketikkan perintah berikut, diikutu dengan Enter tiap baris:

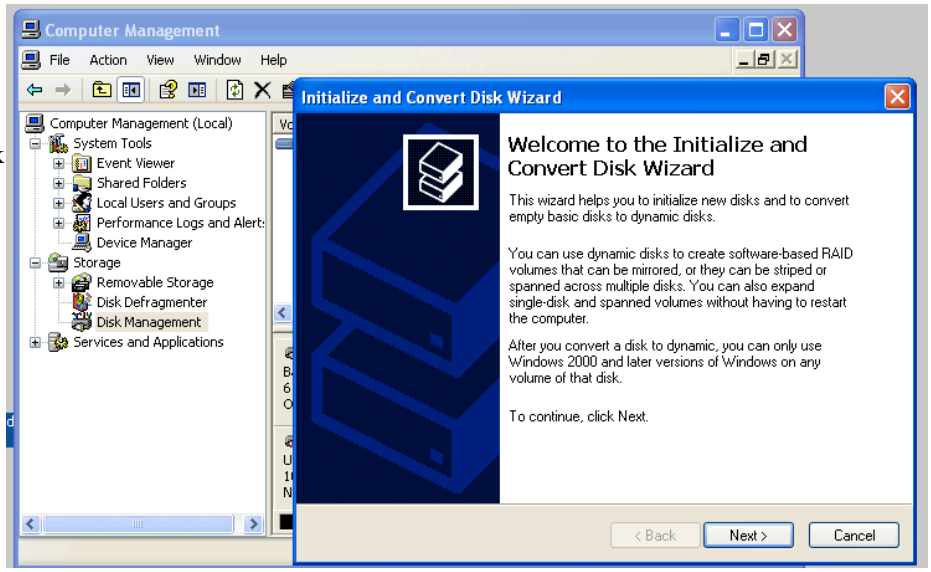
```
DISKPART
LIST DISK
```



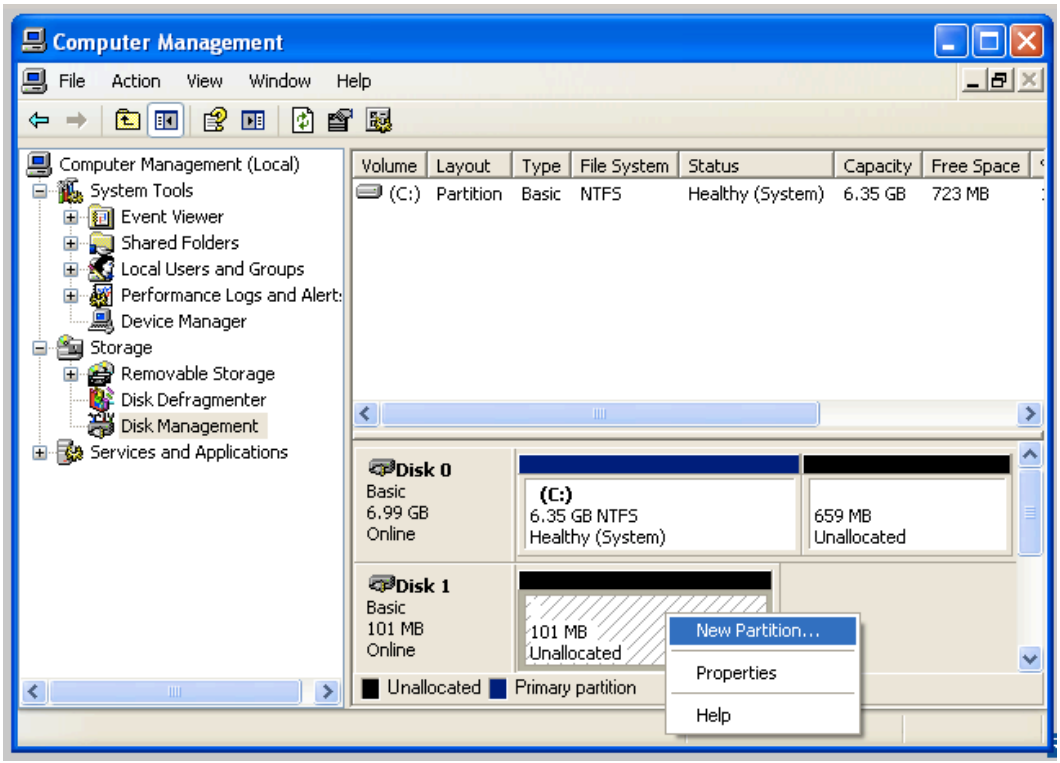
   b) Lihat output untuk mencari 100 MB disk yang akan dibersihkan.
   c) Pada jendela Command Prompt, masukkan perintah berikut, pastikan untuk memilih disk yang benar pada perintah yang pertama:

```
SELECT DISK 1
CLEAN ALL
```

Mengenali Disk yang Baru



3) Pada komputer virtual, click **Start**.
   a) Klik kanan "**My Computer**" dan click **Manage**.
   b) Pada panel kiri Computer Management, click "**Disk Management**".
   c) "Initialize and Convert Disk Wizard" terbuka, seperti berikut. Click **Next**.
   d) Pada menu "Select Disks to Initialize", click **Next**.
   e) Pada menu "Select Disks to Convert", click **Next**.
   f) Pada menu "Completing the Initialize and Convert Disk Wizard", click **Finish**.



Membuat Partisi NTFS 16 MB

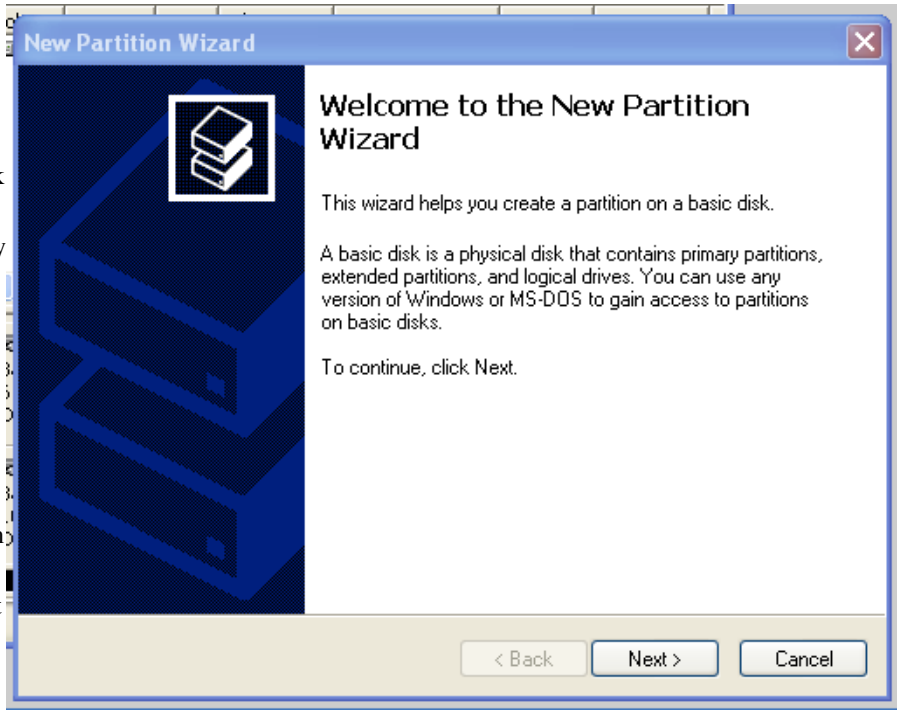
4) Pada Computer Management, di sisi kanan bawah, klik kanan space "Unallocated" pada new hard disk.
   a) Pada context menu, click "**New Partition...**", seperti terlihat di bawah.
   b) "New Partition Wizard" terbuka, seperti terlihat berikut.
   c) Click **Next**.

d) Pada menu "Select Partition Type", biarkan pilihan default "**Primary partition**" dan click **Next**.

e) Pada menu "Specify Partition Size", pilih ukuran **16** MB, seperti terlihat di bawah ini, dan click **Next**.

f) Pada menu "Assign Drive Letter or Path", pilih accept the default selection dan click **Next**.

g) Pada menu "Format Partition", terima pilihan default dan click **Next**.

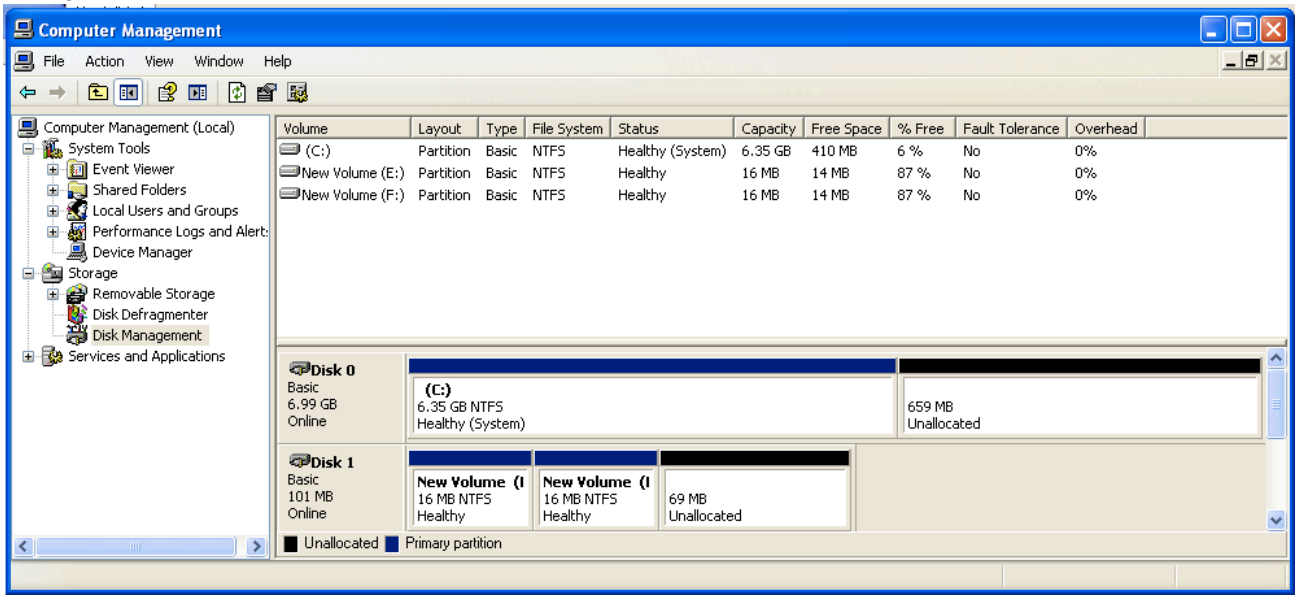


5) Pada menu "Completing the New Partition Wizard", click **Finish**.

Membuat Partisi 16 MB NTFS yang Lain

6) Ulangi proses untuk membuat 16 MB partisi yang kedua.

a) Computer Management seharusnya menjadi seperti berikut ini:

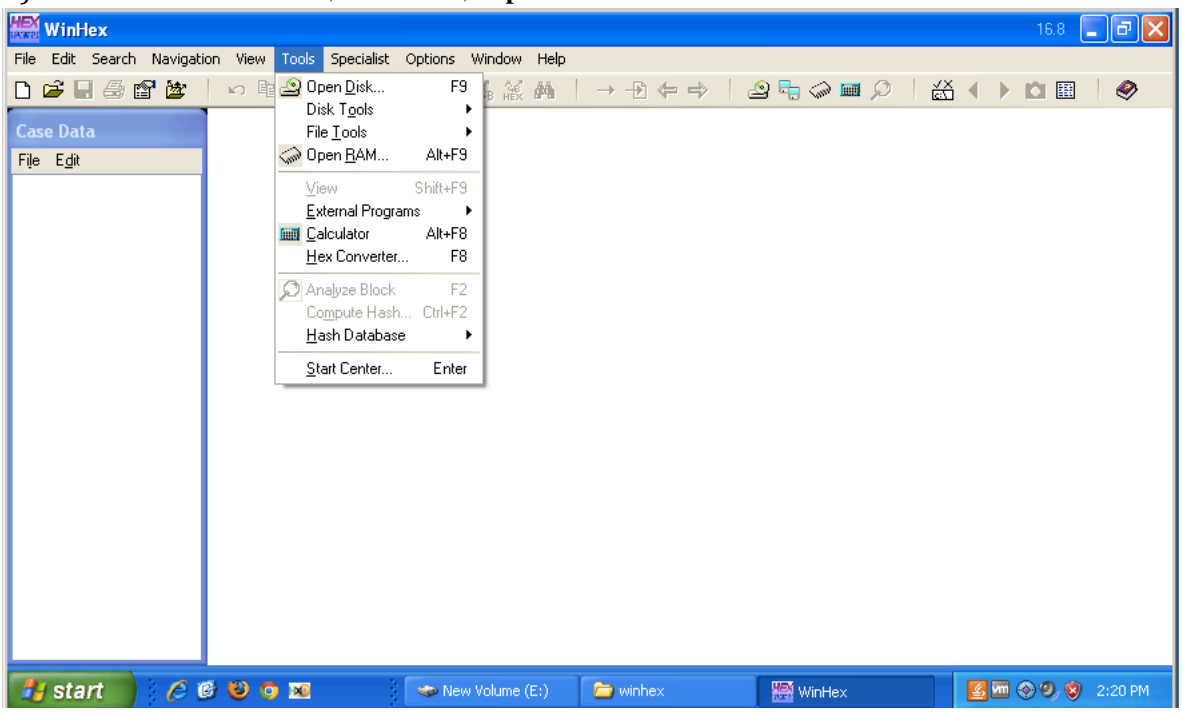


Mendapatkan WinHex

7) Seharusnya sudah ada WinHex dari project sebelumnya. Jika belum ada bisa di download di sini: http://winhex.com

Melihat Tabel Partisi pada WinHex

8) Dari menu WinHex menu, click **Tools**, "**Open Disk...**".

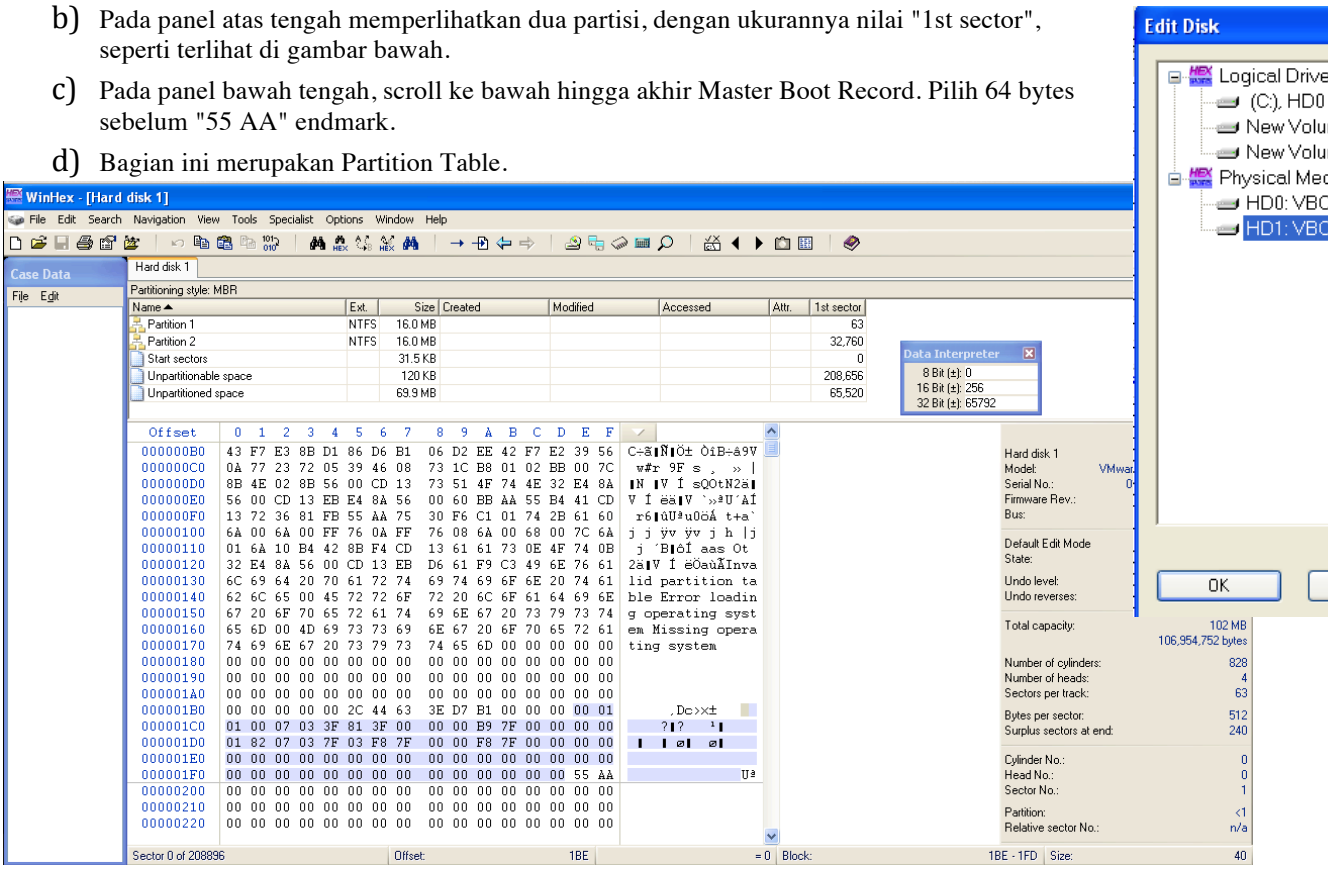


a) Pada kotak "Edit Disk" box, click "HD1: VBOXHARDDISK (100 MB)", seperti terlihat di bawah ini, kemudian click tombol **OK**.

b) Pada panel atas tengah memperlihatkan dua partisi, dengan ukurannya nilai "1st sector", seperti terlihat di gambar bawah.

c) Pada panel bawah tengah, scroll ke bawah hingga akhir Master Boot Record. Pilih 64 bytes sebelum "55 AA" endmark.

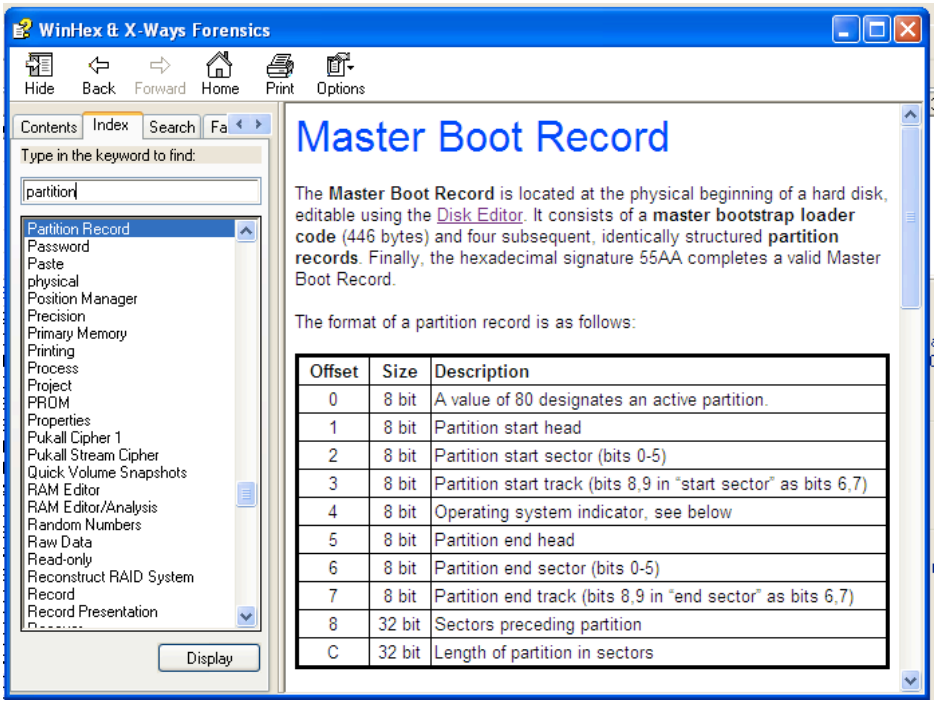
d) Bagian ini merupakan Partition Table.



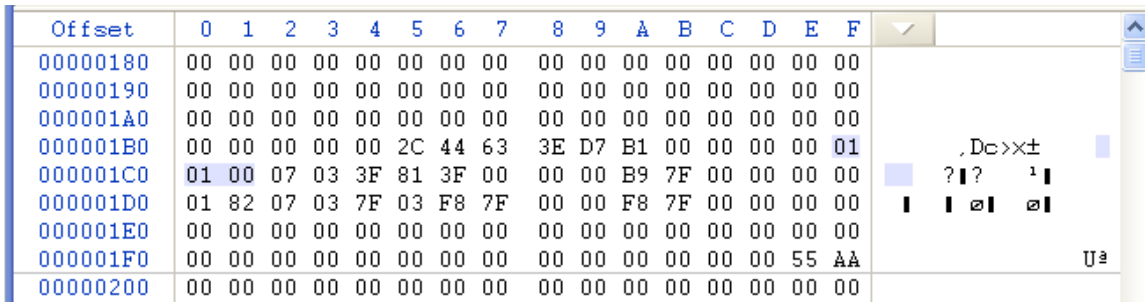
e) Sorot seperti di bawah, 32 bytes Partition Table yang digunakan.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000000B0	43	F7	E3	8B	D1	86	D6	B1	06	D2	EE	42	F7	E2	39	56
000000C0	0A	77	23	72	05	39	46	08	73	1C	B8	01	02	BB	00	7C
000000D0	8B	4E	02	8B	56	00	CD	13	73	51	4F	74	4E	32	E4	8A
000000E0	56	00	CD	13	EB	E4	8A	56	00	60	BB	AA	55	B4	41	CD
000000F0	13	72	36	81	FB	55	AA	75	30	F6	C1	01	74	2B	61	60
00000100	6A	00	6A	00	FF	76	0A	FF	76	08	6A	00	68	00	7C	6A
00000110	01	6A	10	B4	42	8B	F4	CD	13	61	61	73	0E	4F	74	0B
00000120	32	E4	8A	56	00	CD	13	EB	D6	61	F9	C3	49	6E	76	61
00000130	6C	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61
00000140	62	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E
00000150	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74
00000160	65	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61
00000170	74	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	00	00	00	00	00	2C	44	63	3E	D7	B1	00	00	00	00	01
000001C0	01	00	07	03	3F	81	3F	00	00	00	B9	7F	00	00	00	00
000001D0	01	82	07	03	7F	03	F8	7F	00	00	F8	7F	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA
00000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000220	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

f) WinHex help entry untuk Master Boot Record menjelaskan Partition Table record structure dengan jelas:



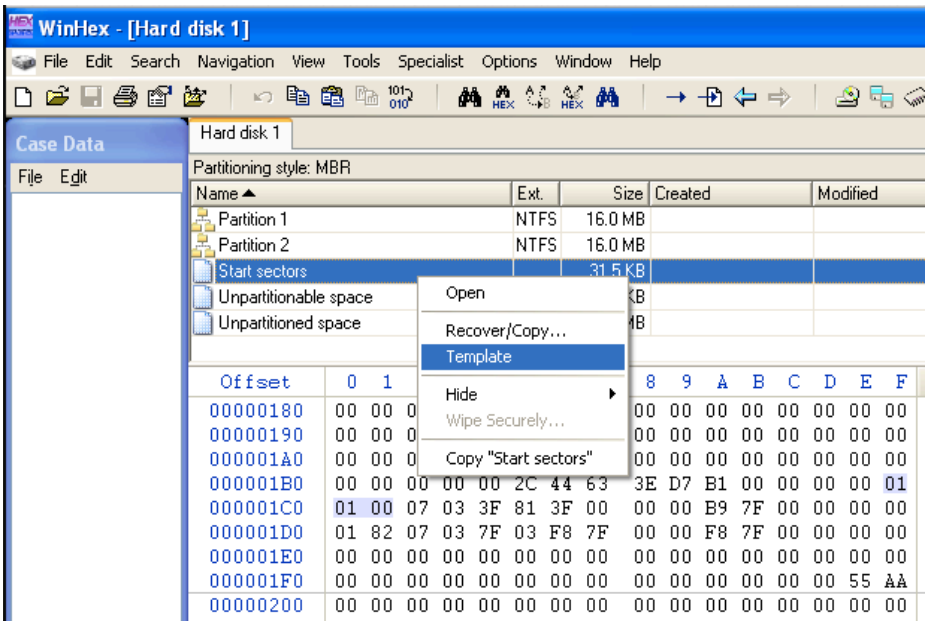
g) Ada dua indicator start-of-partition pada Partition Table.
Yang pertama asalah "CHS" format, berisi Cylinder, Head, dan Sector (tidak berurutan), seperti disorot di bawah ini:
(Cylinder juga disebut Track.)



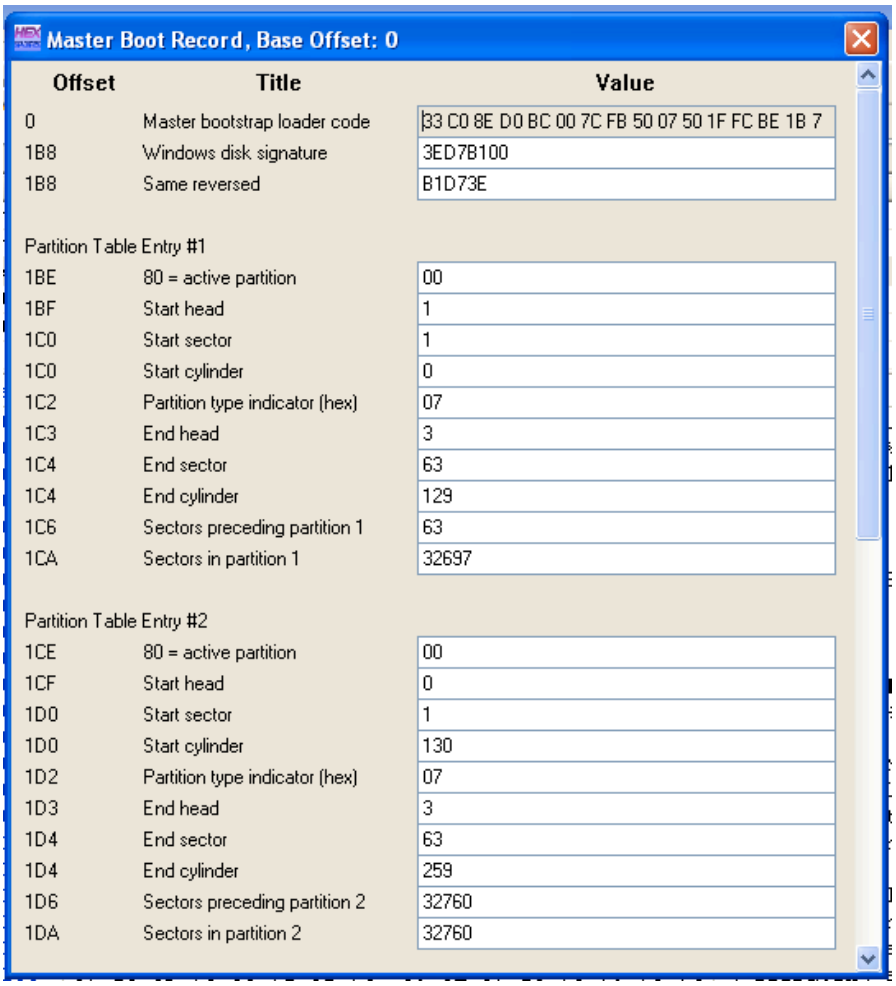
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	00	00	00	00	00	2C	44	63	3E	D7	B1	00	00	00	00	01
000001C0	01	00	07	03	3F	81	3F	00	00	00	B9	7F	00	00	00	00
000001D0	01	82	07	03	7F	03	F8	7F	00	00	F8	7F	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA
00000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Cukup jelas untuk hard disk controller, tapi tidak sederhana untuk digambarkan

h) Untuk memudahkannya, pada panel atas tengah, klik kanan "**Start section**" dan click **Template**, seperti di bawah ini:



i) Master Boot Record dan Partition Table terlihat dengan format yang lebih mudah dipahami, seprti di bawah ini:



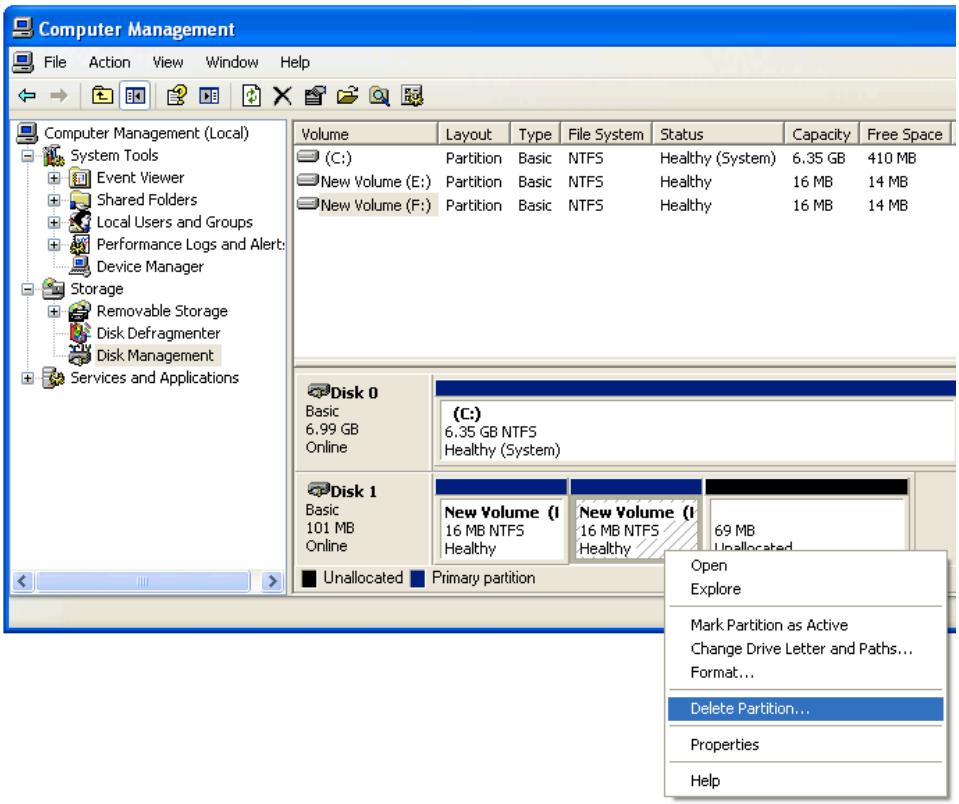
Offset	Title	Value
0	Master bootstrap loader code	33 C0 8E D0 BC 00 7C FB 50 07 50 1F FC BE 1B 7
1B8	Windows disk signature	3ED7B100
1B8	Same reversed	B1D73E
	Partition Table Entry #1	
1BE	80 = active partition	00
1BF	Start head	1
1C0	Start sector	1
1C0	Start cylinder	0
1C2	Partition type indicator (hex)	07
1C3	End head	3
1C4	End sector	63
1C4	End cylinder	129
1C6	Sectors preceding partition 1	63
1CA	Sectors in partition 1	32697
	Partition Table Entry #2	
1CE	80 = active partition	00
1CF	Start head	0
1D0	Start sector	1
1D0	Start cylinder	130
1D2	Partition type indicator (hex)	07
1D3	End head	3
1D4	End sector	63
1D4	End cylinder	259
1D6	Sectors preceding partition 2	32760
1DA	Sectors in partition 2	32760

Simpan Test File

9) Buka Notepad dan masukan nama kalian dalam file. Gunakan nama sendiri.
   a) Simpan file di drive F:, yang merupakan partisi kedua dari partisi 16 MB NTFS yang dibuat.
   b) Gunakan nama file YOURNAME.txt, seperti terlihat di bawah ini. Gunakan nama masing-masing.
   c) Tutup Notepad.

Delete Table Partition Table

10) Pada Computer Management, klik kanan partisi 16 MB yang dibuat dan click "**Delete Partition...**", seperti terlihat di bawah ini:

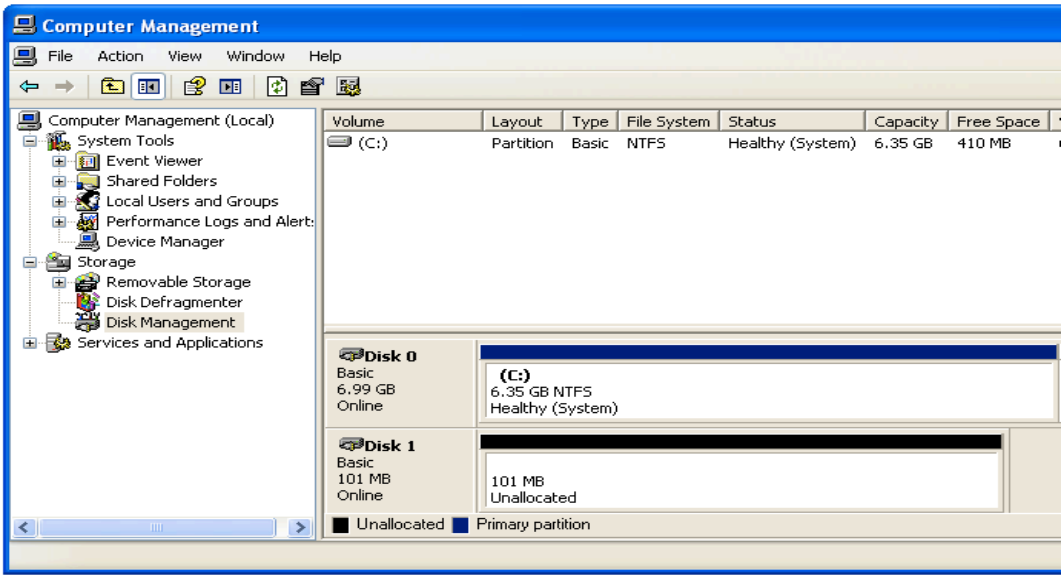


a) Kotak pesan akan muncul yang menampilkan peringatan "All data on this volume will be lost".

b) Click **Yes**.

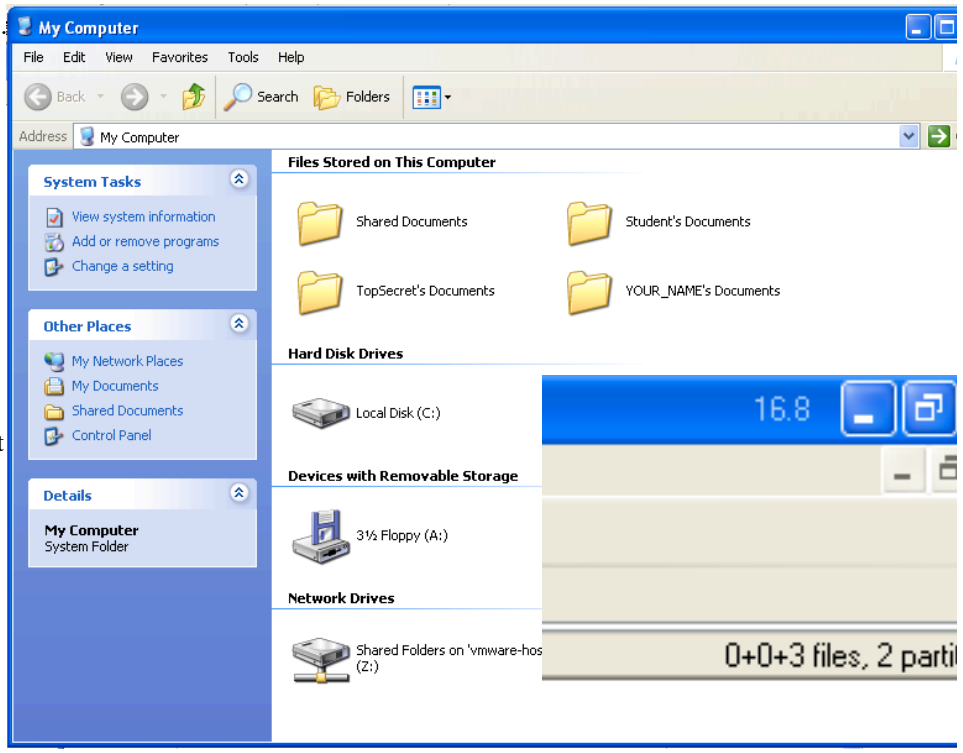
c) Ulangi untuk men-delete partisi 16 MB yang lain.

d) Sekarang terlihat "Unallocated" pada Disk Management, seperti terlihat di bawah ini:



Melihat Disk yang Rusak pada Windows Explorer

11) Click **Start**, "**My Computer**". Drive F: sudah hilang, seperti terlihat di bawah ini, dan file dengan nama kalian juga menghilang.



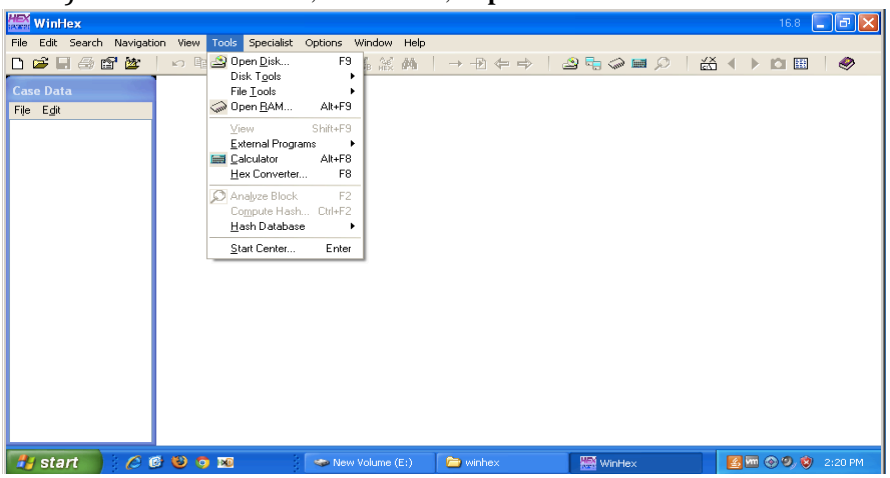
Melihat Disk yang Rusak dengan WinHex

12) Pada WinHex, cari pada sudut kanan atas jendela. Terdapat dua tombol X, seperti terlihat di samping.

a) Click yang bawah, tombol X abu-abu, jangan yang tombol merah.

b) Cara ini untuk menutup disk tanpa menutup WinHex, dan ini cara yang paling mudah untuk melakukan refresh untuk melihat disk. Sayangnya, "View", "Refresh" tidak berjalan di WinHex.

c) Dari menu WinHex, click **Tools**, "**Open Disk...**".

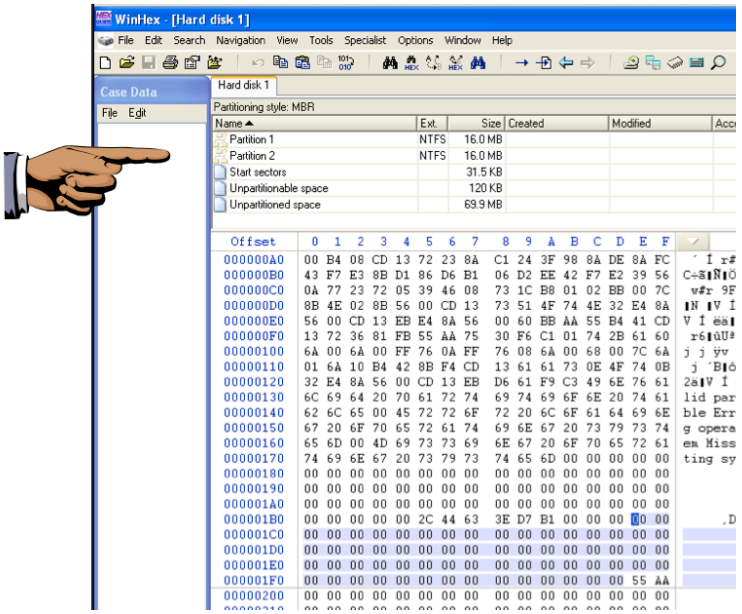


d) Pada kotak "Edit Disk" box, click "HD1: VBOXHARDDISK (100 MB)", kemudian click tombol **OK**.

e) Pada panel bawah, scroll down sampai ke akhir Master Boot Record dan sorot Partition Table, seperti terlihat di bawah ini.

f) Partition Table sudah dihapus dan hanya berisi nol.

g) Perhatikan panel atas pada WinHex masih memperlihatkan dua partisi meskipun abu-abu.



h) Hal ini terjadi karena partisi masih berisi Volume Boot Records yang bisa digunakan untuk rebuild partition table.

Simpan Screen Image

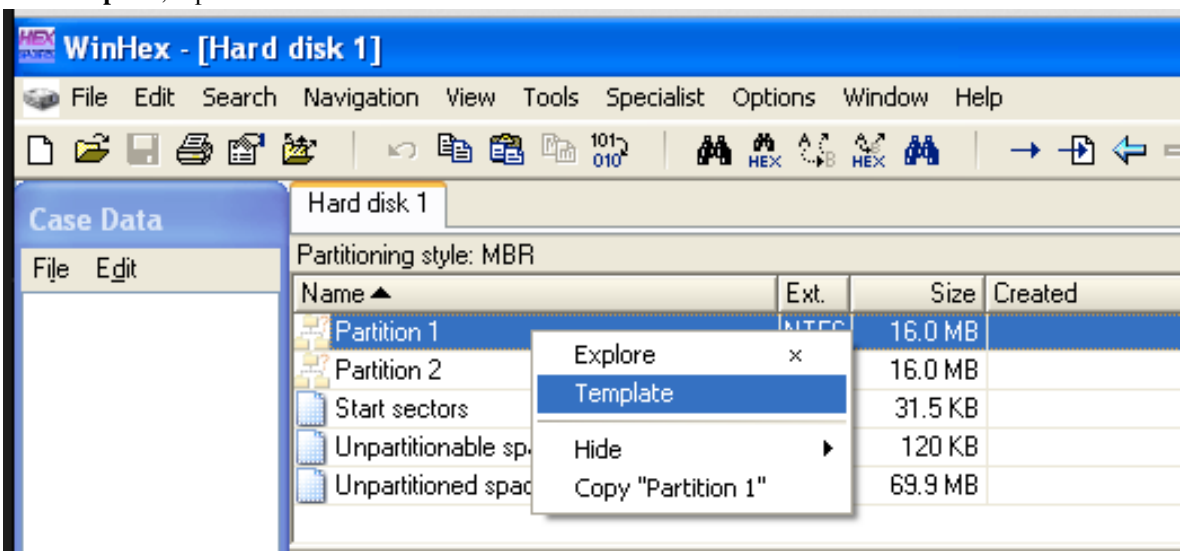
13) Pastikan screen yang memperlihatkan "Partition 1" dan "Partition 2" dengan icon kuning samar, terlihat seperti di atas.

a) Tekan PrintScrn untuk mengkopi seluruh desktop ke clipboard.
SUBMIT FULL DESKTOP UNTUK MENDAPATKAN POIN MAKSIMAL!

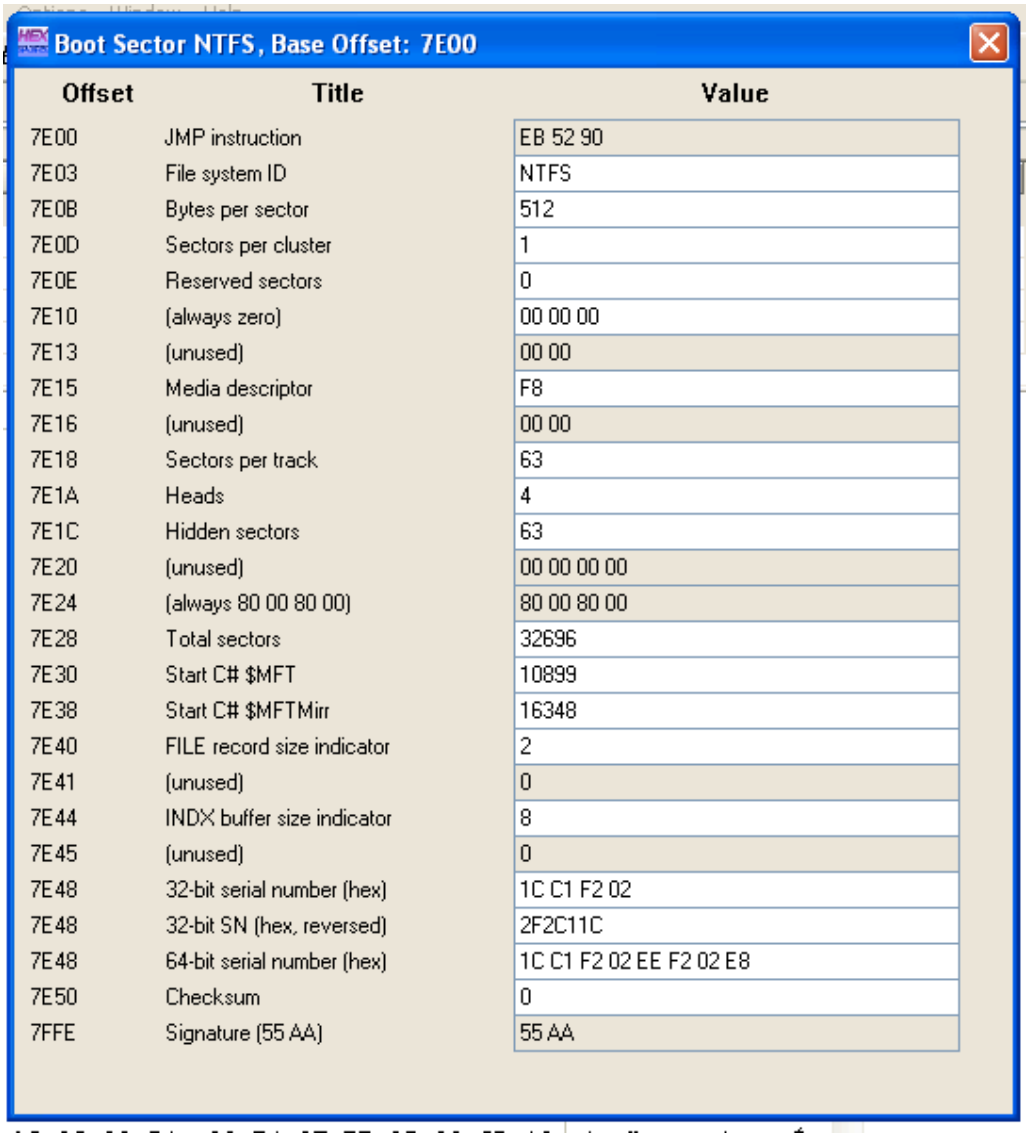
b) Simpan image dengan nama file "**NAMAKAMU_ Proj10a**".

Memeriksa Volume Boot Record

14) Untuk melihat Volume Boot Record, pada bagian atas tengah, klik kanan "**Partition 1**" dan click **Template**, seperti berikut:



a) Partition Boot Sector akan terlihat, seperti di bawah ini:



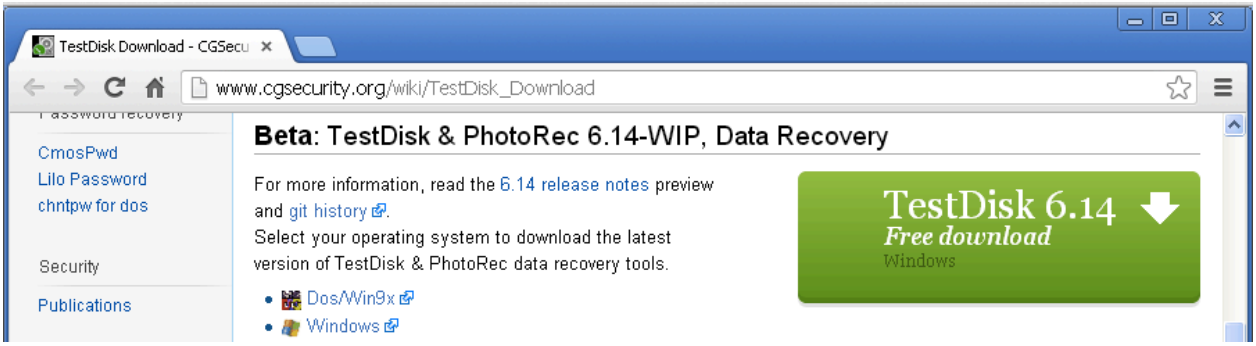
Offset	Title	Value
7E00	JMP instruction	EB 52 90
7E03	File system ID	NTFS
7E0B	Bytes per sector	512
7E0D	Sectors per cluster	1
7E0E	Reserved sectors	0
7E10	(always zero)	00 00 00
7E13	(unused)	00 00
7E15	Media descriptor	F8
7E16	(unused)	00 00
7E18	Sectors per track	63
7E1A	Heads	4
7E1C	Hidden sectors	63
7E20	(unused)	00 00 00 00
7E24	(always 80 00 80 00)	80 00 80 00
7E28	Total sectors	32696
7E30	Start C# $MFT	10899
7E38	Start C# $MFTMirr	16348
7E40	FILE record size indicator	2
7E41	(unused)	0
7E44	INDX buffer size indicator	8
7E45	(unused)	0
7E48	32-bit serial number (hex)	1C C1 F2 02
7E48	32-bit SN (hex, reversed)	2F2C11C
7E48	64-bit serial number (hex)	1C C1 F2 02 EE F2 02 E8
7E50	Checksum	0
7FFE	Signature (55 AA)	55 AA

b) Sangat mungkin menggunkan alamat Partition Boot Sector dan data pada komputer dengan nilai yang ada pada Partition Table.

c) Tapi kita tidak melakukannya secara manual – kita akan menggunakan recovery tool.

Download TestDisk

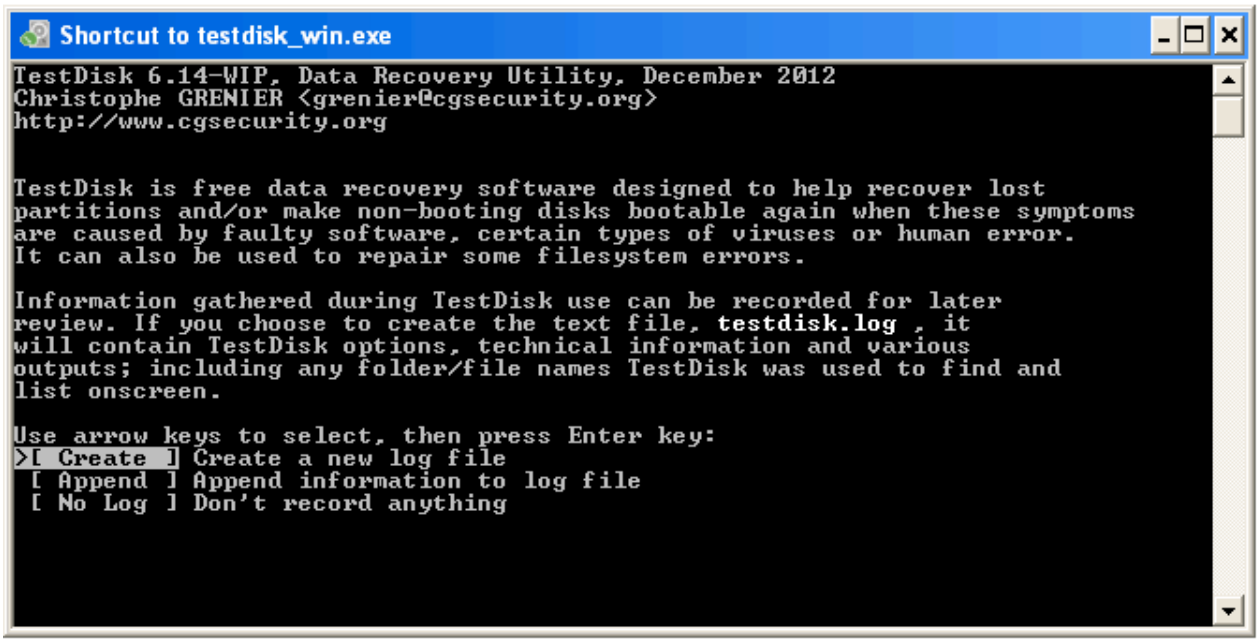
15) Buka browser dan arahkan ke http://www.cgsecurity.org/wiki/TestDisk_Download . Click tombol hijau besar untuk mendownload TestDisk, seperti berikut (sebelumnya sudah pernah kita gunakan pada Project 6):



a) Unzip TestDisk dan jalankan.

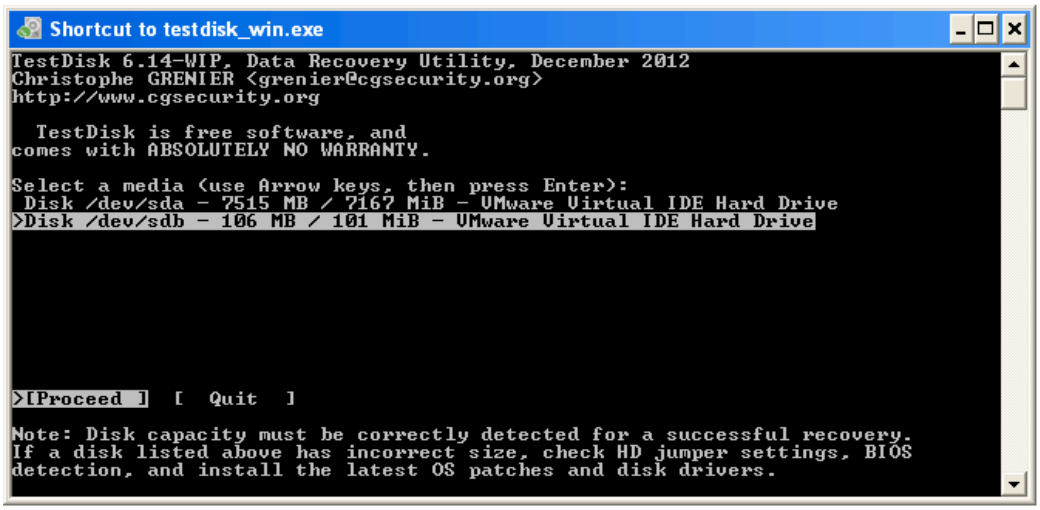
b) first screen akan menanyakan tempat file log.

c) Tekan Enter untuk menerima pilihan default.

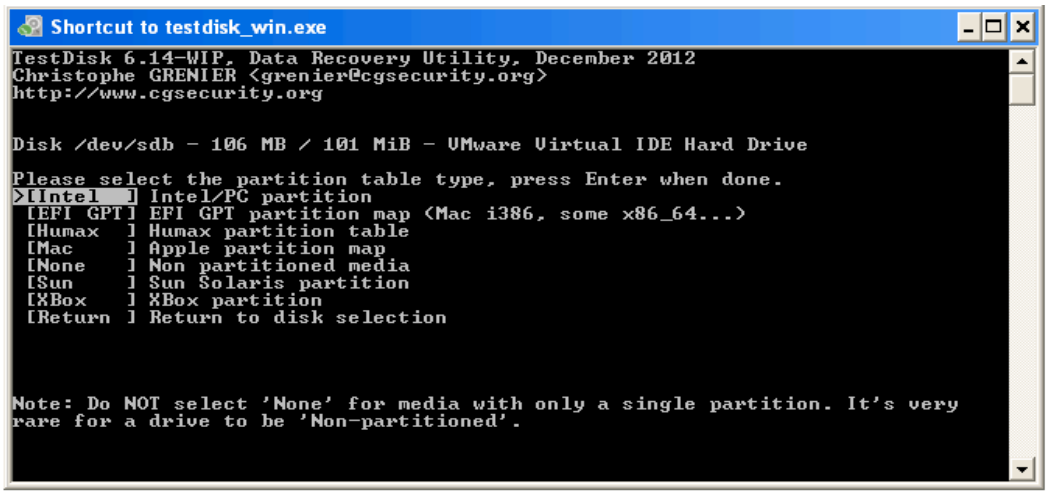


d) Pada next screen, tekan panah ke bawah untuk memilih 106 MB disk yang akan direpair.

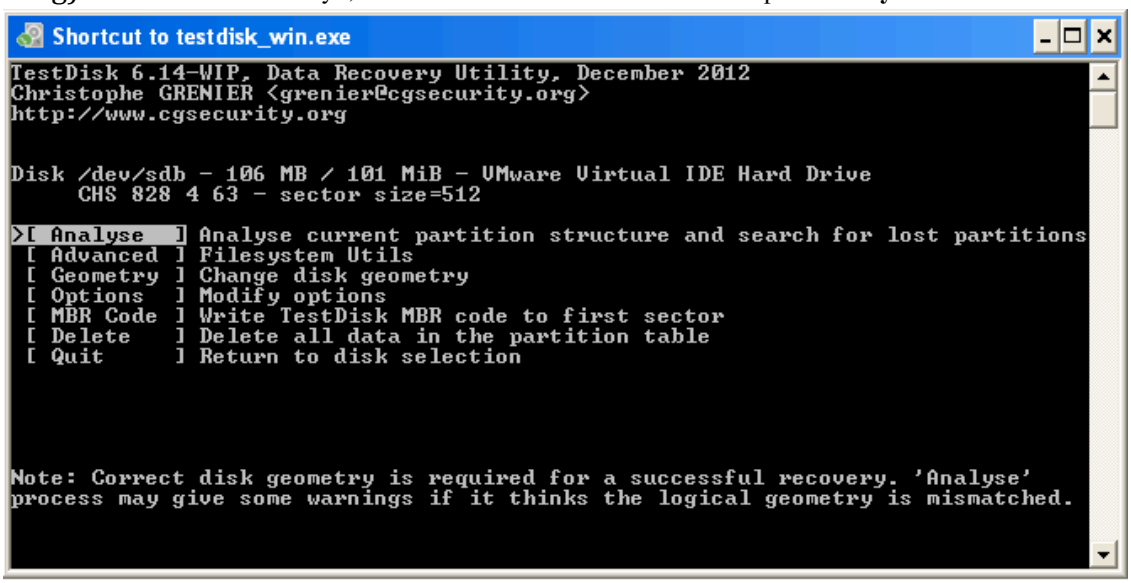
e) Kemudian tekan Enter.



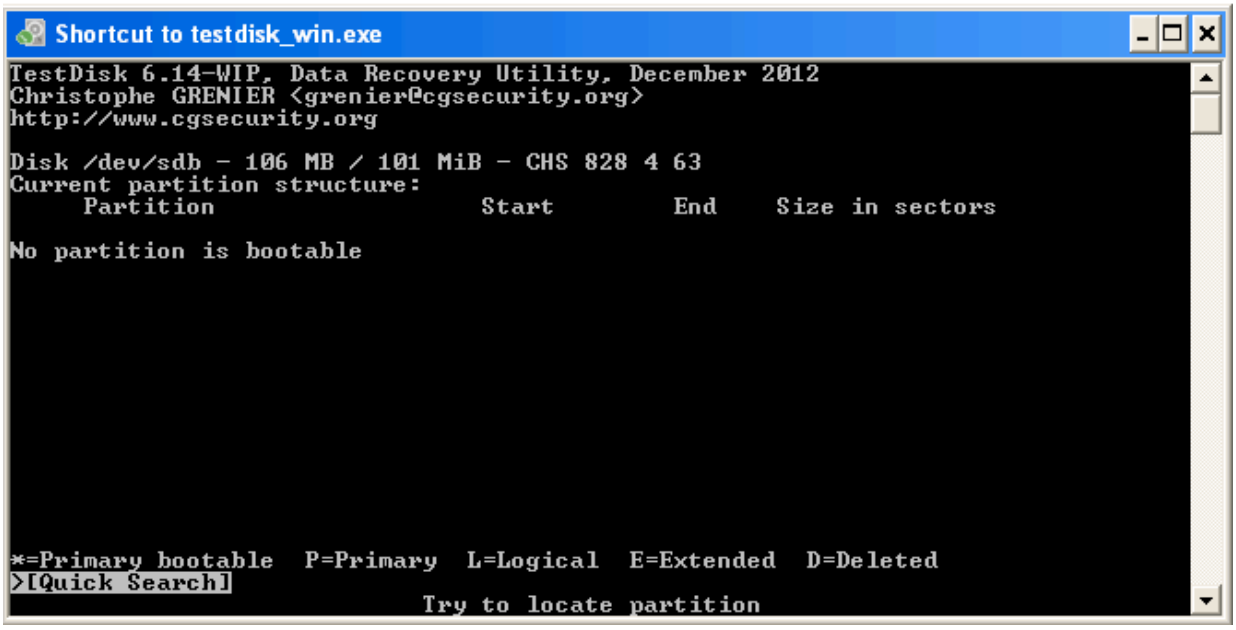
f) Pada screen berikutnya, tekan Enter untuk menerima default option **Intel**.



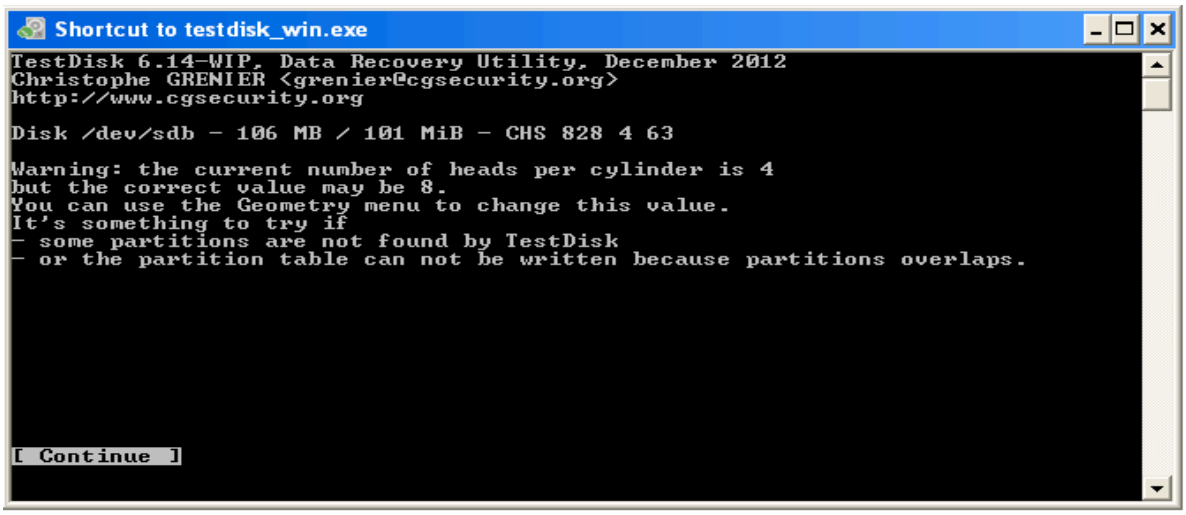
g) Pada screen berikutnya, tekan Enter untuk menerima default option **Analyze**.



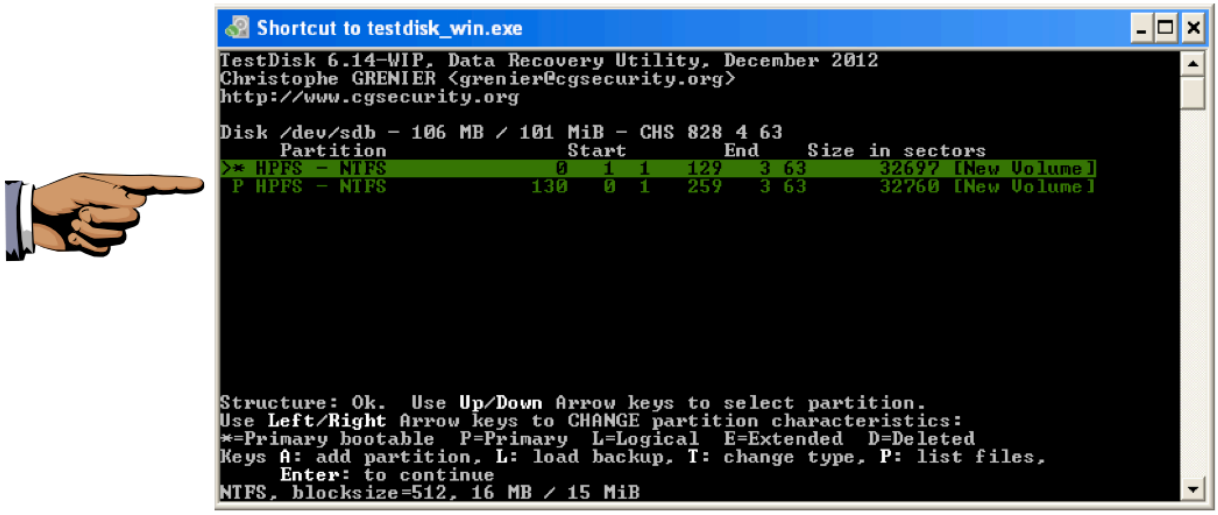
h) Pada screen berikutnya, tekan Enter untuk menerima default option "**Quick Search**".



i) Pada menu berikutnya, Tekan Enter untuk menerima default option **Continue**.



j) Pada menu berikutnya meperlihatkan parisi yang direcover berwarna hijau. Berarti benar, tekan Enter untuk melanjutkan.



Simpan Screen Image

16) Pastikan dua baris teks berwarna hijau, terlihat seperti di atas.

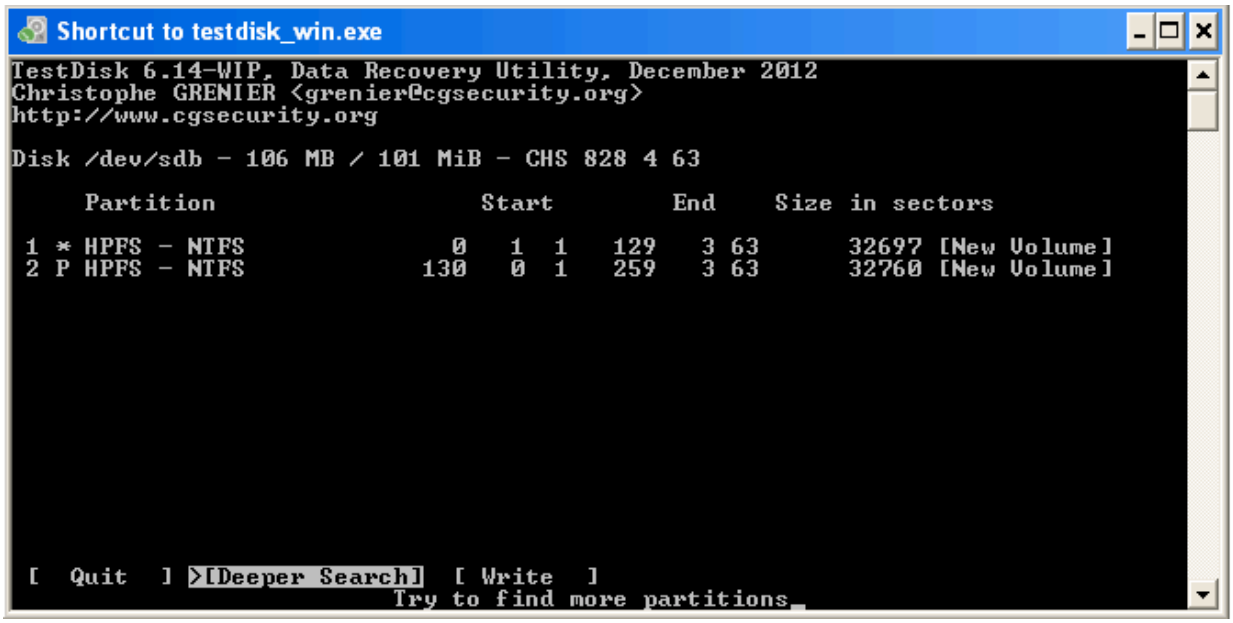
a) Tekan PrintScrn untuk mengkopi seluruh desktop ke clipboard.
SUBMIT FULL DESKTOP UNTUK MENDAPATKAN POIN MAKSIMAL!

b) Simpan image dengan nama file "**NAMAKAMU_ Proj10b**".

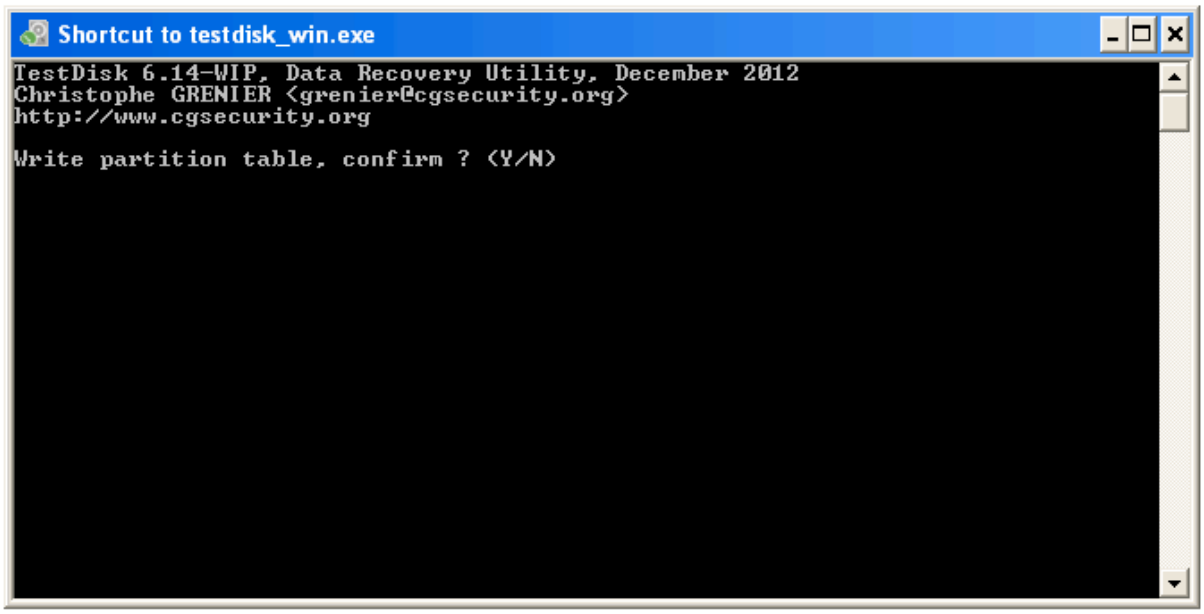
Menyelesaikan Recovery

17) Layar berikutnya memperlihatkan detail partition table yang baru.

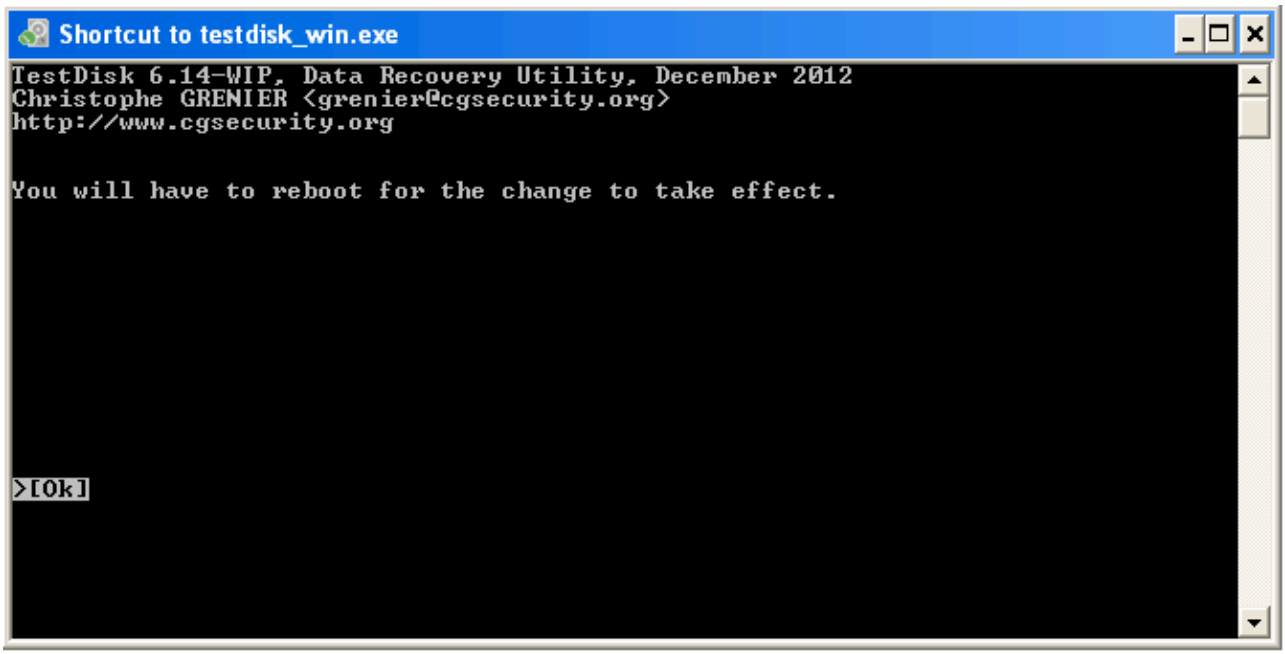
a) Tekan **W** untuk menulis table partition yang baru.



b) Pada next screen, tekan **Y** untuk Write partition table yang baru.



c) Pada next screen, tekan Enter.

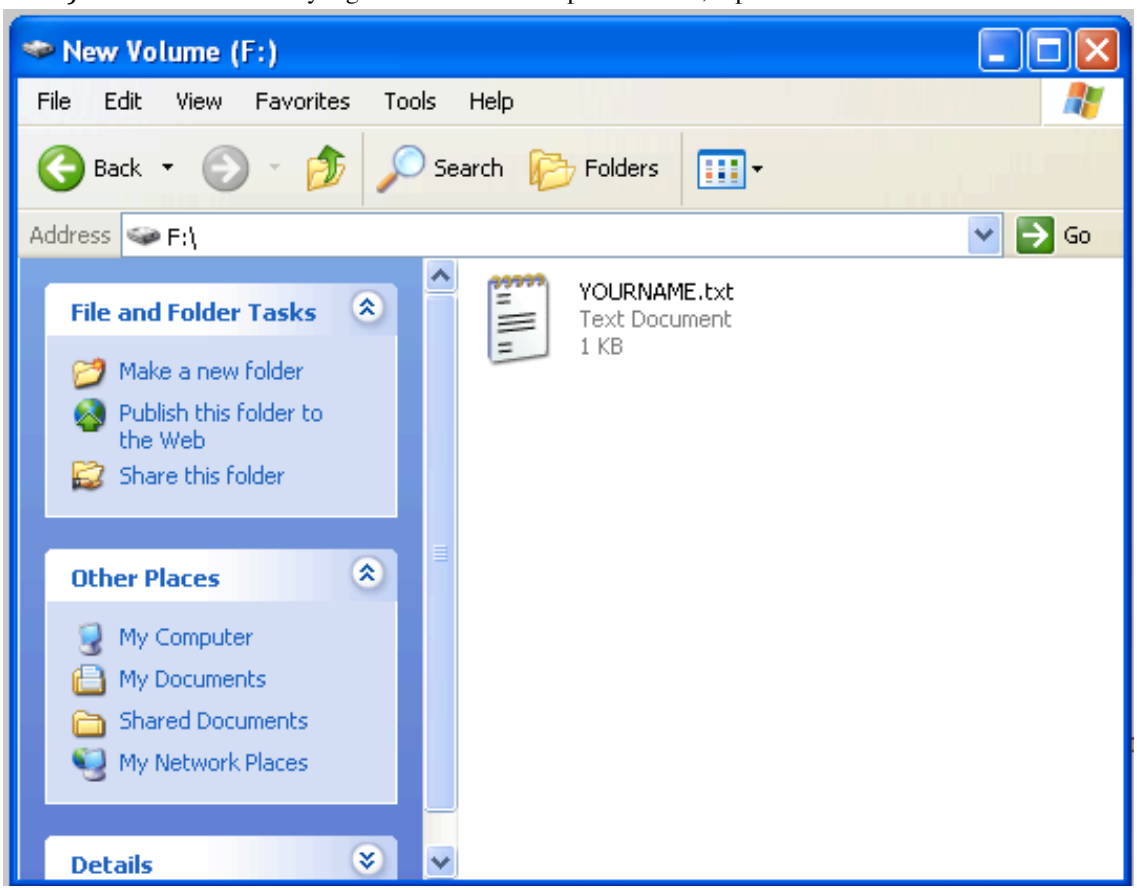


18) Tutup semua windows dan restart virtual machine.

Melihat File yang di Recovered

19) Click **Start**, "**My Computer**".

a) Buka drive F:. File yang sudah direcovered pasti terlihat, seperti berikut ini:



Mengumpulkan Project

Project 9 Memperbaiki Partition Table dengan TestDisk 25 points

Kirim melalui elearning

Last modified: 19-4-2013