# **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

	WS\system32\cn	nd.exe - DIS	KPART				- 🗆 X
Microsoft W (C) Copyrig	indows XP [V ht 1985-2001	ersion 5.: Microsof	1.2600] t Corp.				
C:\Document:	s and Settin	gs∖Studen	t>DISKPAR	T			
Microsoft D	iskPart vers	ion 5.1.3	565				
Copyright ( On computer	C> 1999-2003 : XP-Yournam	Microsof E	t Corpora	tion.			
DISKPART> L	IST DISK						
Disk ###	Status	Size	Free	Dyn	Gpt		
Disk Ø Disk 1	Online Online	7162 MB 101 MB	659 MB Ø B				
DISKPART> S	ELECT DISK 1						
Disk 1 is n	ow the selec	ted disk.					
DISKPART> C	LEAN ALL						
DiskPart su	cceeded in c	leaning t	he disk.				
DISKPART>							-

- 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



- 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.

- Project 9 Memperbaiki Partition Table dengan TestDisk
  - 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.
  - Pada menu "Assign f) Drive Letter or Path", pilih accept the default selection) and click Next.
  - Pada menu "Format g) 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:

📙 Computer Management										
🗐 File Action View Window H	telp									_ 8 ×
	1 😼									
Computer Management (Local) Computer Management (Local) Computer Management (Local) Computer Management Cocal Users and Groups Cocal Users Cocal Users and Groups Cocal Users Cocal Users Coc	Volume (C:) New Volume (E:) New Volume (F:) Volume (F:) Volume (F:) Volume (F:) Volume (F:)	Layout Type Partition Basic Partition Basic Partition Basic Case Generation 6.35 GB NTFS Healthy (Systen	File System NTFS NTFS NTFS	Status Healthy (System) Healthy Healthy	Capacity 6.35 GB 16 MB 16 MB	Free Space 410 MB 14 MB 14 MB	% Free 6 % 87 % 87 % 659 MB Unalloc	Fault Tolerance No No No	Overhead 0% 0% 0%	
	Basic 101 MB Online	New Volume ( 16 MB NTFS Healthy	I New Yolu 16 MB NTF Healthy	me (I 5 69 MB Unallocate	d					~
<	Unallocated	Primary partition								

# **Mendapatkan WinHex**

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

Edit Disk

🚟 Logical Drive

🕳 (C:), HD0

😅 New Volu 😅 New Volu

# 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.

1157	-	-									Physical Me
🚟 WinHex - [Hard	disk 1]										
🌍 File Edit Search	Navigation View	Tools Specialist Opt	ions Wind	low Help							
🗅 📽 🗟 🎒 😭	🖄   🗠 🖿	🖀 🖻 1912 🕴 👫 🐔	. 🖓 нех	₩ → ⊕ ⇔	🔄 🔤 🤇	≥ 🖬 🔎 🗎 🖌 🕨	<b>İ</b>				
Case Data	Hard disk 1										
File Edit	Partitioning style: M	1BR									
	Name 🔺		Ext.	Size Created	Modified	Accessed	Attr. 1st :	sector			
	Artition 1		NTFS	16.0 MB				63		1	
	Partition 2		NTFS	16.0 MB			3	32,760 Data	Intorprotor		
	Start sectors			31.5 KB				0	Di (c) O		
	Unpartitionable	space		120 KB			20	08,656 8	Bit (±): 0 Bit (±): 256	- 1	
	Unpartitioned s	pace		69.9 MB			6	65,520 32	Bit (+): 65792		
	Offset	0 1 2 3 4	5 6	7 8 9 A B C	DEF		^				
	000000B0	43 F7 E3 8B D1	86 D6 I	B1 06 D2 EE 42 F7	E2 39 56	C÷ã∎Ñ∎Ö± ÒîB÷â9V				Hard disk 1	
	000000000	OA 77 23 72 05	39 46 1	08 73 1C B8 01 02	BB 00 7C	v#r9Fs, »∣				Model: VMwar.	
	000000D0	8B 4E 02 8B 56	00 CD :	13 73 51 4F 74 4E	32 E4 8A	∎N ∎V I sQOtN2a				Serial No.: 0	
	000000E0	56 00 CD 13 EB	E4 8A 9	56 00 60 BB AA 55	B4 41 CD	V I ealV '≫ªU'AI				Firmware Rev.:	
	0000000000	13 72 36 81 FB	55 AA	75 30 F6 CI 01 74	2B 61 60	rbluusuuoa t+a				bus.	1
	00000100	5A UU 5A UU FF	OD EA C	CD 13 (1 (1 73 0E	4E 74 0B	] ] yv yv ] n []				Default Edit Mode	
	00000110	32 FA 83 56 00	CD 13 1	CD 13 61 61 73 0E	4F 74 0D	2ä∎V ÍäÖaù∛Trua				State:	
	00000130	6C 69 64 20 70	61 72	74 69 74 69 6F 6F	20 74 61	lid partition ta				Lindo level:	
	00000140	62 6C 65 00 45	72 72 1	6F 72 20 6C 6F 61	64 69 6E	ble Error loadin				Undo reverses:	
	00000150	67 20 6F 70 65	72 61	74 69 6E 67 20 73	79 73 74	q operating syst					
	00000160	65 6D 00 4D 69	73 73	69 6E 67 20 6F 70	65 72 61	em Missing opera				Total capacity:	102 MB
	00000170	74 69 6E 67 20	73 79 1	73 74 65 6D 00 00	00 00 00	ting system					106,954,752 bytes
	00000180	00 00 00 00 00	00 00 0	00 00 00 00 00 00	00 00 00					Number of cylinders:	828
	00000190	00 00 00 00 00	00 00 0	00 00 00 00 00 00	00 00 00					Number of heads:	4
	000001A0	00 00 00 00 00	00 00 1	00 00 00 00 00 00	00 00 00					Sectors per track:	63
	000001B0	00 00 00 00 00	2C 44	63 3E D7 B1 00 00	00 00 01	,Dc>×±				Bytes per sector:	512
	000001C0	U1 UU U7 03 3F	81 3F	UU UU UU B9 7F 00	00 00 00	7 <b>1</b> 7 <b>1</b>				Surplus sectors at end:	240
	000001D0	01 82 07 03 7F	03 F8	/F UU UU F8 7F UU	00 00 00					C.F.J. N.	
	000001E0		00 00 0		00 00 00	Па				Uyinger No.: Head Max	U
	00000200		00 00 1		00 05 44	03				Sector No.:	1
	00000210									D. 00	
	00000220		00 00 1		00 00 00					Partition:	<1
							*			melauve sector No.:	n/a
	Sector 0 of 20889	6	0	Offset	1BE	=	0 Block:		18	E - 1FD Size:	40

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

Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	× .
000000B0	43	F7	E3	8B	D1	86	D6	B1	06	D2	ΕE	42	F7	E2	39	56	C÷ã∎Ñ∎Ö± ÒîB÷â9V 📃
000000000	ΟA	77	23	72	05	39	46	08	73	1C	B8	01	02	BB	00	7C	w#r 9F s , »
000000D0	8B	4E	02	8B	56	00	CD	13	73	51	4F	74	4E	32	E4	8A	∎N ∎V Í sQOtN2ä∎
000000E0	56	00	CD	13	EB	E4	8A	56	00	60	BB	AA	55	B4	41	CD	V Í ëä∎V `≫ªU′AÍ
000000F0	13	72	36	81	FB	55	AA	75	30	F6	C1	01	74	2B	61	60	r6∎ûUªu0öÁ t+a`
00000100	6A	00	6A	00	$\mathbf{FF}$	76	ΟÀ	FF	76	08	6A	00	68	00	7C	6A	j j ÿv ÿv j h  j
00000110	01	6A	10	B4	42	8B	F4	CD	13	61	61	73	0E	4F	74	0B	j ´B∎ôÍ aas Ot
00000120	32	E4	8A	56	00	CD	13	EΒ	D6	61	F9	C3	49	6E	76	61	2ä∎V Í ëÖaùÃInva
00000130	6C	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61	lid partition ta
00000140	62	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E	ble Error loadin
00000150	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
00000160	65	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61	em Missing opera
00000170	74	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00	ting system
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	ЗE	D7	B1	00	00	00	00	01	,Dc>x±
000001C0	01	00	07	03	ЗF	81	ЗF	00	00	00	B9	7F	00	00	00	00	? <b> </b> ? <sup>1</sup>
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	Ωa
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:

Image: Index Forward Home       Frint       Options         Contents       Index Search Fa       Image: Print       Options         Type in the keyword to find:       Image: Print       Image:	💕 WinHex & X-Ways Forensi	cs				$\times$
Contents       Index       Search       Fa         Type in the keyword to find:       Partition         Partition       Image: Partition         Partition       Image: Physical Position Manager       Precision         Precision       Precision         Primary Memory       Priming         Properties       Properties         Pukal Cipher 1       Pukal Stream Cipher         Quick Volume Snapshots       RAM Editor/Analysis         Radom Numbers       Radom Numbers         Record Presentation       St bit Partition end head         6       8 bit Partition end track (bits 8,9 in "end sector" as bits 6,7)         8       32 bit Sectors preceding partition         Contents       Contents	Hide Back Forward Home	Pri	nt Options			
Partition         Partition Record         Pastword         Paste         physical         Position Manager         Precision         Primary Memory         Printing         Process         Project         PRIM         Properties         Pukall Stream Cipher         Quick Volume Snapshots         RAM Editor/Analysis         Random Numbers         Rad-only         Record resentation         Record resentation         Construct RAID System         Record resentation            Displan            Displan            Displan            Displan            Project PROM            Pukal Stream Cipher            Quick Youme Snapshots         Radoonly            Record resentation <td>Contents Index Search Fa</td> <td>&gt;</td> <td>Mas</td> <td>ster</td> <td>Boot Record</td> <td><b>^</b></td>	Contents Index Search Fa	>	Mas	ster	Boot Record	<b>^</b>
Precision         Primary Memory         Printing         Process         Project         PROM         Properties         Pukall Cipher 1         Pukall Stream Cipher         Quick Volume Snapshots         RAM Editor/Analysis         Ramdom Numbers         Raw Data         Read-only         Record Presentation         Proced         Project         Project         Pukall Stream Cipher         Quick Volume Snapshots         RAM Editor/Analysis         Raw Data         Record Presentation         Project         Record Presentation         Project	Partition Partition Record Password Paste physical Position Manager		The Mast editable u code (44 records. Boot Rec	er Boot sing the 6 bytes) Finally, ord.	Record is located at the physical beginning of a hard disk, <u>Disk Editor</u> . It consists of a master bootstrap loader and four subsequent, identically structured partition the hexadecimal signature 55AA completes a valid Master	
Project       Project         Project       PROM         Properties       0       8 bit       A value of 80 designates an active partition.         Pukal Cipher 1       Pukal Stream Cipher       2       8 bit       Partition start head         Quick Volume Snapshots       3       8 bit       Partition start sector (bits 0-5)         Quick Volume Snapshots       3       8 bit       Partition start track (bits 8,9 in "start sector" as bits 6,7)         Random Numbers       3       8 bit       Partition end head         Record Record Presentation        6       8 bit       Partition end track (bits 8,9 in "end sector" as bits 6,7)         Record Presentation         3       32 bit       Sectors preceding partition         C       32 bit       Sectors preceding partition        C       32 bit       Length of partition in sectors	Precision Primary Memory Printing Processo		The forma	at of a pa	artition record is as follows:	
PROM         Properties         Pukal Cipher 1         Pukal Stream Cipher         Quick Volume Snapshots         RAM Editor/Analysis         Random Numbers         Raw Data         Record Presentation         Record Presentation         Properties         Pukal Stream Cipher         Quick Volume Snapshots         Radom Numbers         Raw Data         Record Presentation         Partition         Partition end track (bits 8,9 in "end sector" as bits 6,7)         8 bit         Partition end track (bits 8,9 in "end sector" as bits 6,7)         8 bit         Partition end track (bits 8,9 in "end sector" as bits 6,7)         8 32 bit         Sectors preceding partition         C         Stable         C         Record Presentation	Project		Offset	Size	Description	
1       8 bit       Partition start head         Pukal Cipher 1       2       8 bit       Partition start sector (bits 0-5)         Quick Volume Snapshots       3       8 bit       Partition start sector (bits 0.5)         RAM Editor       3       8 bit       Partition start track (bits 8.9 in "start sector" as bits 6.7)         Random Numbers       8       bit       Operating system indicator, see below         Second Presentation       5       8 bit       Partition end head         Record Presentation       6       8 bit       Partition end track (bits 8.9 in "end sector" as bits 6.7)         8       32 bit       Sectors preceding partition         C       32 bit       Length of partition in sectors	PROM Properties		0	8 bit	A value of 80 designates an active partition.	
Pukall Stream Cipher         Quick Volume Snapshots         RAM Editor         Radmeditor         Record         Record Presentation         Record Presentation         C         32 bit         Sectors preceding partition         C         32 bit         Length of partition in sectors	Pukall Cipher 1		1	8 bit	Partition start head	
3       8 bit       Partition start track (bits 8,9 in "start sector" as bits 6,7)         RAM Editor       4       8 bit       Operating system indicator, see below         Raw Data       5       8 bit       Partition end head         Record Presentation       6       8 bit       Partition end track (bits 8,9 in "end sector" as bits 6,7)         Record Presentation       3       32 bit       Sectors preceding partition         Displan       C       32 bit       Length of partition in sectors	Pukall Stream Cipher		2	8 bit	Partition start sector (bits 0-5)	
RAM Editor/Analysis         Ram Data         Read-only         Read-only         Record Presentation         Source         Displan	RAM Editor		3	8 bit	Partition start track (bits 8,9 in "start sector" as bits 6,7)	
Saw Data         Read-only         Record Presentation         Saw Data         Record Presentation         Say Data         Say Data         Record Presentation         Say Data         Say Data         Record Presentation         Say Data	RAM Editor/Analysis		4	8 bit	Operating system indicator, see below	
Read-only         Record         Ret	Raw Data		5	8 bit	Partition end head	
Record         7         8 bit         Partition end track (bits 8,9 in "end sector" as bits 6,7)           Record Presentation         Image: Sector secto	Read-only Reconstruct RAID Sustem		6	8 bit	Partition end sector (bits 0-5)	
Record Presentation         8         32 bit         Sectors preceding partition           Display         C         32 bit         Length of partition in sectors	Record		7	8 bit	Partition end track (bits 8,9 in "end sector" as bits 6,7)	
Display C 32 bit Length of partition in sectors	Record Presentation		8	32 bit	Sectors preceding partition	
	Display	וו	С	32 bit	Length of partition in sectors	

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	В	С	D	E	F	$\overline{}$				/
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		, De i	>×±		
000001C0	01	00	07	03	ЗF	81	ЗF	00	00	00	В9	7F	00	00	00	00		?∎?	1		
000001D0	01	82	07	03	7F	03	F8	7F	00	00	F8	7F	00	00	00	00	1	Ø	ø		
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				Ωa	
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:

MEX	11.1.43																
🚟 WinHex - [Hard	disk 1 j																
🌍 File Edit Search	Navigation View	Too	ols :	Speci	ialist	Opt	ions	Wir	ndow	Help							
D 🖻 🗏 🎒 😭 I	🖄   🗠 🗎 (		a 10	12	ĝ.	HE	×	в не	( <b>M</b>		<b>→</b>	Ð	4	⇒	6	<u>s</u> 5	h 🖓
Case Data	Hard disk 1																
File Edit	Partitioning style: M	IBR															
1.10 1.24	Name 🔺						Ext.		S	ize (	Create	ed			Mo	dified	
	📇 Partition 1						NTE	-S	16.01	MB							
	📇 Partition 2						NTE	-S	16.0	MB							
	Start sectors			_					31.5	КВ							
	Unpartitionable	spac	е		Оре	n				КB							
	Unpartitioned s	pace			Rec	over	/Cop <sup>.</sup>	y		1B							
					Tem	plate	э –										
	Offset	0	1		Hide					8	- 9	A	В	С	D	Е	F
	00000180	00	00	0	Wie	- - 50	rurak	,		00	00	00	00	00	00	00	00
	00000190	00	00	0_	- vvip			/		00	00	00	00	00	00	00	00
	000001A0	00	00	0	Сор	iy "St	art s	ector	's"	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	ЗF	00	00	00	В9	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	λÀ
	00000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

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

🕽 Untit

YOUR NA

🚟 Master B	oot Record, Base Offset: 0		×	
Offset	Title	Value	^	
0	Master bootstrap loader code	33 C0 8E D0 BC 00 7C FB 50 07 50 1F FC BE 1B 7		I
1B8	Windows disk signature	3ED7B100		I
1B8	Same reversed	B1D73E		l
Partition Table	e 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		I
1C4	End cylinder	129		
1C6	Sectors preceding partition 1	63		
1CA	Sectors in partition 1	32697		
Partition Table	e Entru #2			ľ
1CF	80 = active partition	00		
1CF	Start head	0		
1D0	Start sector	1		
1D0	Start cylinder	130		
1D2	Partition type indicator (hex)	07		
1D3	Endhead	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 masingmasing.
  - 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:

E Computer Management File Action View Window F ← → € ■ P P → ▼	elp						
Computer Management (Local)  Computer Management (Local)  Computer Viewer   Volume (C:) New Volume (E:) New Volume (F:)	Layout Partition Partition Partition	Type Basic Basic Basic	File System NTFS NTFS NTFS	Status Healthy (System) Healthy Healthy	Capacity 6.35 GB 16 MB 16 MB	Free Space 410 MB 14 MB 14 MB	
Services and Applications	CPDisk 0 Basic 6.99 GB Online CPDisk 1 Basic 101 MB Online	(C:) 6.35 GB N Healthy (S New Yold 16 MB NTH Healthy	ITFS 5ystem) <b>Ime (I</b> =5	New Yolu 16 MB NTF Healthy	me () 5 () Open	d	
	Unallocated I	Primary part	ition		Explore Mark Partition Change Drive Format Delete Partitio Properties	as Active Letter and	Paths

- 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:

🖳 Computer Management							
🗐 File Action View Window H	lelp						
← →  E II 22 II 22 E	1 😼						
Computer Management (Local)  Computer Management (Local)  System Tools  Computer Viewer  Computer Server Viewer  Computer Server	Volume (C:)	Layout Partition	Type Basic	File System NTFS	Status Healthy (System)	Capacity 6.35 GB	Free Space /
urrefield Services and Applications	Cisk 0 Basic 6.99 GB Online	<b>(C:)</b> 6.35 GB N Healthy (S	ITFS 5ystem)				
	Cisk 1 Basic 101 MB Online	101 MB Unallocate	ed				
< >	Unallocated 📕 I	Primary parti	ition				

# 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

My Computer		
File Edit View Favorites Tools	Help	
🕝 Back 👻 🕥 👻 🏂 🔎 Se	earch 🝺 Folders 🛄 -	
ddress 😼 My Computer		💌 🄁 1
System Tasks 🙁	Files Stored on This Computer	
View system information	Shared Documents	Student's Documents
Change a setting	TopSecret's Documents	YOUR_NAME's Documents
Other Places	Hard Disk Drives	
My Network Places My Documents Shared Documents Control Panel	Local Disk (C:)	16.8 🔳 🗗
Details	Devices with Removable Storage	- 6
My Computer System Folder	31/2 Floppy (A:)	
	Network Drives	
	Shared Folders on 'vmware-hos (Z:)	0+0+3 files, 2 parti

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 abuabu.



🗈 🛍 🖻 🗤

Hard disk 1

🗛 🎎 🎎 🙀

WinHex - [Hard disk 1]

🗅 🚅 🗏 🎒 🖆 🖄

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:

🊟 WinHex - [Hard	disk 1]				
🐲 File Edit Search	Navigation View T	ools Specialist	Options N	Window He	lp
🗅 🗳 🗄 🎒 😭	💆 🗆 🗠 🛍	Da 1012	HEX AB	HEX 🚧 🗌	→ + + =
Case Data	Hard disk 1				
File Edit	Partitioning style: MBR				
	Name 🔺		Ext.	Size	Created
	📈 Partition 1		NITEC	16.0 MB	
	Reartition 2	Explore	×	16.0 MB	
	Start sectors	Template		31.5 KB	
	Unpartitionable sp.	Hide	•	120 KB	
	Unpartitioned space	Copy "Partition	ו 1"	69.9 MB	
				1	

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

🚟 Boot Sector NTFS, Base Offset: 7E00				
Offset	Title	Value		
7E00	JMP instruction	EB 52 90		
7E03	File system ID	NTFS		
7E0B	Bytes per sector	512		
7EOD	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 <u>http://www.cgsecurity.org/wiki/TestDisk\_Download</u>. 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.

 Shortcut to testdisk\_win.exe
 Isst Disk 6.14-WIP, Data Recovery Utility, December 2012 Christophe GRENIER {grenier@cgsecurity.org> http://www.cgsecurity.org
 Disk /deu/sdb - 106 MB / 101 MiB - UMware Uirtual IDE Hard Drive CHS 828 4 63 - sector size=512
 Analyse Analyse current partition structure and search for lost partitions [ Advanced ] Filesystem Utils [ Geometry ] Change disk geometry [ Options ] Modify options
 MBR Code ] Write TestDisk MBR code to first sector [ Delete ] Delete all data in the partition table
 [ Quit ] Return to disk selection
 Note: Correct disk geometry is required for a successful recovery. 'Analyse' process may give some warnings if it thinks the logical geometry is mismatched.

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.

#### 25 points

and the state of t				- 🗆 🗙
TestDisk 6.14-WIP, Data Reco Christophe GRENIER <grenier@ http://www.cgsecurity.org</grenier@ 	very Utility, Dec cgsecurity.org>	cember 2012		
Disk /dev/sdb - 106 MB / 101	MiB - CHS 828 4	63		
Partition	Start	End Size	in sectors	
1 * HPFS - NTFS 2 P HPFS - NTFS	0 1 1 129 130 0 1 259	3 63 3 63	32697 [New Volume] 32760 [New Volume]	
[ Quit ] >[Deeper Search] Tr	[ Write ] y to find more pa	artitions_		-

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

🖓 Shortcut to testdisk_win.exe	- 🗆 :	×
TestDisk 6.14-WIP, Data Recovery Utility, December 2012 Christophe GRENIER (grenier@cgsecurity.org) http://www.cgsecurity.org		
Write partition table, confirm ? (Y/N)		
		-

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**

Kirim melalui elearning

Last modified: 19-4-2013