



Intro to WinHex



Graphical User Interface

The screenshot shows the WinHex application window titled "WinHex - [Hard disk 0, Partition 2]". The interface includes a menu bar (File, Edit, Search, Position, View, Tools, Specialist, Options, Window, Help), a toolbar with various icons, and a tab control showing "Hard disk 0" and "Hard disk 0:22". The main area is divided into three panes: a Directory Browser showing a file list, a HEX Display showing raw data, and a Text Display showing the interpreted text. A Data Interpreter popup is visible over the Text Display. The right side features an Info Pane with drive statistics, and the bottom has a Status Bar with sector, offset, block, and size information.

Toolbar

Tab Control

Directory Browser

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
Path unknown							
\$Extend		0.5 KB	08/16/2009 22:26:16	08/16/2009 22:26:16	08/16/2009 22:26:16	SH	6291478
\$Recycle.Bin	Bin	4.1 KB	07/13/2009 22:18:56	02/10/2010 17:30:54	02/10/2010 17:30:54	SH	32904
(Root directory)		12.3 KB	07/13/2009 21:38:56	06/11/2010 20:36:42	06/11/2010 20:36:42	SH	16
boot		4.1 KB	07/23/2009 01:11:06	08/17/2009 02:51:57	08/17/2009 02:51:57	SH	592
Config.Msi	Msi	4.0 KB	06/11/2010 12:12:08	06/11/2010 13:54:34	06/11/2010 13:54:34	SH	1706040
Documents and Settings		48 B	07/14/2009 00:08:56	07/14/2009 00:08:56	07/14/2009 00:08:56	PSHX	6340844
HP		424 B	08/16/2009 23:01:29	01/05/2010 04:17:37	01/05/2010 04:17:37	H	6313298
Intel		144 B	03/11/2010 21:50:01	03/11/2010 21:50:01	03/11/2010 21:50:01		99422642

HEX Display

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000002000	49	4E	44	58	28	00	09	00	47	FB	06	20	01	00	00	00
0000002010	00	00	00	00	00	00	00	00	40	00	00	00	38	08	00	00
0000002020	E8	0F	00	00	00	00	00	00	04	77	04	05	00	05	00	00
0000002030	CB	01	69	00	00	00	CA	01	00	00	00	00	00	00	00	00
0000002040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000002050	00	00	00	00	00	00	00	00	04	00	00	00	00	00	04	00
0000002060	68	00	52	00	00	00	00	00	05	00	00	00	00	00	05	00
0000002070	42	E4	E7	7A	EA	1E	CA	01	42	E4	E7	7A	EA	1E	CA	01
0000002080	42	E4	E7	7A	EA	1E	CA	01	42	E4	E7	7A	EA	1E	CA	01
0000002090	00	10	00	00	00	00	00	00	00	0A	00	00	00	00	00	00
00000020A0	06	00	00	00	00	00	00	00	08	03	24	00	41	00	74	00
00000020B0	74	00	72	00	44	00	65	00	66	00	00	00	00	00	00	00
00000020C0	08	00	00	00	00	00	08	00	68	00	52	00	00	00	00	00
00000020D0	05	00	00	00	00	00	05	00	42	E4	E7	7A	EA	1E	CA	01
00000020E0	42	E4	E7	7A	EA	1E	CA	01	42	E4	E7	7A	EA	1E	CA	01

Text Display

INDX(Gû
@ 8
è
È i E
h R
Bäçzê Ê Bäçz
Bäçzê Ê Bäçz
\$
t r D e f
h R
Bäçzê Ê
Bäçzê Ê Bäçzê Ê

Data Interpreter

- 8 Bit (±): 73
- 16 Bit (±): 20041
- 24 Bit (±): 4476489
- 32 Bit (±): 1480871497
- DOS Date: 02/04/2024 09:50:18

Info Pane

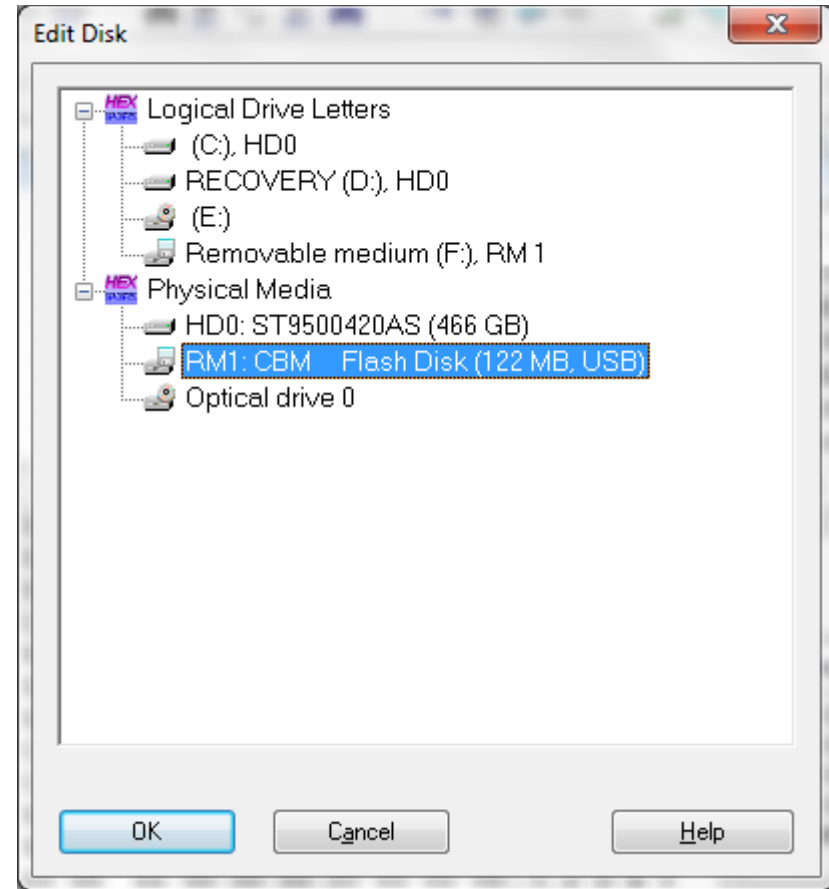
Hard disk 0, Partition 27% free
File system: NTFS
Default Edit Mode: original
State: original
Undo level: 0
Undo reverse: n/a
Alloc. of visible drive space:
Cluster No.: 2 (Root directory)
Snapshot taken 62 min. ago
Physical sector No.: 409616
Logical sector No.: 16

Status Bar

Sector 16 of 949194752 Offset: 2000 Block: n/a Size: n/a

Opening a disk

- ▶ If using Vista or Win7, must run WinHex with elevated permissions by selecting the “Run as Administrator” option when launching the program.
- ▶ Without elevated permissions, physical devices can not be accessed.
- ▶ From the WinHex GUI menu, select “Tools/Open Disk”
- ▶ Select the disk you wish to open and click “OK”



Opening a disk

WinHex - [Removable medium 1]

File Edit Search Position View Tools Specialist Options Window Help

Removable medium 1 Removable medium..., Volume

Partitioning style: unpartitioned (floppy/superfloppy/CD/DVD) 0 files, 1 partitions

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
Volume		100 MB					

Double-Click listed volumes or partitions to open Directory Browser

WinHex - [Removable medium 1, Volume]

File Edit Search Position View Tools Specialist Options Window Help

Removable medium 1 Removable medium..., Volume

0 min. ago 13+11=24 files, 5+3=8 dir.

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
(Root directory)		16.0 KB					488
Fragmented Directory		4.0 KB	06/14/2010 21:17:14	06/14/2010 21:17:16	06/15/2010		520
New folder		0 B	06/14/2010 21:17:14	06/14/2010 21:17:16	06/14/2010		520
New folder		0 B	06/14/2010 22:33:18	06/14/2010 22:33:20	06/14/2010		3060
New folder		0 B	06/14/2010 22:33:32	06/14/2010 22:33:34	06/14/2010		3064
New Parent Folder		2.0 KB	06/14/2010 22:33:32	06/14/2010 22:33:34	06/15/2010		3064
Old Parent Folder		2.0 KB	06/14/2010 22:33:18	06/14/2010 22:33:20	06/14/2010		3060
This is a renamed folder		2.0 KB	06/14/2010 22:13:16	06/14/2010 22:13:18	06/14/2010		2984
active file.txt	txt	23 B	06/14/2010 22:17:54	06/14/2010 22:19:58	06/14/2010	A	3036

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	EB	3C	90	4D	53	44	4F	53	35	2E	30	00	02	04	02	00
00000010	02	00	02	00	00	F8	F3	00	3F	00	FF	00	00	00	00	00
00000020	FF	CC	03	00	80	00	29	34	95	37	5A	4E	4F	20	4E	41
00000030	4D	45	20	20	20	20	46	41	54	31	36	20	20	20	33	C9
00000040	8E	D1	BC	F0	7B	8E	D9	B8	00	20	8E	C0	FC	BD	00	7C
00000050	38	4E	24	7D	24	8B	C1	99	E8	3C	01	72	1C	83	EB	3A
00000060	66	A1	1C	7C	26	66	3B	07	26	8A	57	FC	75	06	80	CA
00000070	02	88	56	02	80	C3	10	73	EB	33	C9	8A	46	10	98	F7
00000080	66	16	03	46	1C	13	56	1E	03	46	0E	13	D1	8B	76	11
00000090	C0	89	46	FC	89	56	FE	B8	20	00	F7	E6	8B	5E	0B	03
000000A0	63	48	F7	F3	01	46	FC	11	4E	FE	61	BF	00	00	E8	E6
000000B0	00	72	39	26	38	2D	74	17	60	B1	0B	BE	A1	7D	F3	A6
000000C0	61	74	32	4E	74	09	83	C7	20	3B	FB	72	E6	EB	DC	A0
000000D0	FB	7D	B4	7D	8B	F0	AC	98	40	74	0C	48	74	13	B4	0E
000000E0	BB	07	00	CD	10	EB	EF	A0	FD	7D	EB	E6	A0	FC	7D	EB

Sector 0 of 249087 Offset: 0

Removable medium .99% free
File system: FAT16
Volume label: FAT16
Default Edit Mode: original
State: original
Undo level: 0
Undo reverses: n/a
Alloc. of visible drive space: n/a
Cluster No.: n/a
Boot sector
Snapshot taken: 0 min. ago
Used space: 1.3 MR
Size: n/a

Data Interpreter
8 Bit (±): -21
16 Bit (±): 15595
24 Bit (±): -7324437
32 Bit (±): 1301298411
DOS Date: 12/16/2018 07:39:22

Opening a forensic bit-stream image

- ▶ From the WinHex GUI menu, select “File/Open” or click on the “Open” button on the Toolbar
- ▶ Browse to your image file, select it and click “Open”
- ▶ You must tell WinHex that this file is an image of a disk so that can interpret the raw data.
 - ▶ From the menu, select “Specialist/Interpret Image File As Disk”



Opening a forensic bit-stream image

WinHex - [Exploring FAT.img]

File Edit Search Position View Tools Specialist Options Window Help

Removable medium 1 Exploring FAT.img

Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F

00000000 EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 04 02 00 < MSDOS5.0

00000010 02 00 02 00 00 F8 F3 00 3F 00 FF 00 00 00 00 00

00000020 FF CC 03 00 80 00 29 34 95 37 5A 4E 4F 20 4E 41 yI |)4I7ZNO NA

00000030 4D 45 20 20 20 20 46 41 54 31 36 20 20 20 33 C9 ME FAT16 3E

00000040 8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C

00000050 38 4E 24 7D 24 8B C1 99 E8 3C

00000060 66 A1 1C 7C 26 66 3B 07 26 8A

00000070 02 88 56 02 80 C3 10 73 EB 33

00000080 66 16 03 46 1C 13 56 1E 03 46

00000090 60 89 46 FC 89 56 FE B8 20 00

000000A0 03 48 F7 F3 01 46 FC 11 4E FE

000000B0 00 72 39 26 2D 74 17 60 B1

000000C0 61 74 32 4E 74 09 83 C7 20 3B

000000D0 FB 7D B4 7D 8B F0 AC 98 40 74

000000E0 BB 07 00 CD 10 EB EF A0 FD 7D

000000F0 E1 CD 16 CD 19 26 8B 55 1A 52

00000100 3B 00 72 E8 5B 8A 56 24 BE 0B

00000110 3D 7D C7 46 F4 29 7D 8C D9 89

00000120 06 96 7D CB EA 03 00 00 20 0F

00000130 66 03 46 1C 66 8B D0 66 C1 EA

00000140 4A 4A 8A 46 0D 32 E4 F7 E2 03

00000150 4A 52 50 06 53 6A 01 6A 10 91

00000160 D2 F7 F6 91 F7 F6 42 87 CA F7

00000170 C0 CC 02 0A CC B8 01 02 80 7E

00000180 8B F4 8A 56 24 CD 13 61 61 72

00000190 5E 0B 49 75 06 F8 C3 41 BB 00

Page 1 of 306569 Offset:

Before
Interpreting
as a Disk

WinHex - [[Exploring FAT.img]]

File Edit Search Position View Tools Specialist Options Window Help

Removable medium 1 Exploring FAT

13+11=24 files, 5+3=8 dir.

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
(Root directory)		16.0 KB					488
Fragmented Directory		4.0 KB	06/14/2010 21:17:14	06/14/2010 21:17:16	06/15/2010		520
New folder		0 B	06/14/2010 21:17:14	06/14/2010 21:17:16	06/14/2010		520
New folder		0 B	06/14/2010 22:33:18	06/14/2010 22:33:20	06/14/2010		3060
New folder		0 B	06/14/2010 22:33:32	06/14/2010 22:33:34	06/14/2010		3064
New Parent Folder		2.0 KB	06/14/2010 22:33:32	06/14/2010 22:33:34	06/15/2010		3064
Old Parent Folder		2.0 KB	06/14/2010 22:33:18	06/14/2010 22:33:20	06/14/2010		3060
This is a renamed folder		2.0 KB	06/14/2010 22:13:16	06/14/2010 22:13:18	06/14/2010		2984
active file.txt	.txt	23 B	06/14/2010 22:17:54	06/14/2010 22:19:58	06/14/2010	A	3036

Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F

00000000 EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 04 02 00 < MSDOS5.0

00000010 02 00 02 00 00 F8 F3 00 3F 00 FF 00 00 00 00 00

00000020 FF CC 03 00 80 00 29 34 95 37 5A 4E 4F 20 4E 41 yI |)4I7ZNO NA

00000030 4D 45 20 20 20 20 46 41 54 31 36 20 20 20 33 C9 ME FAT16 3E

00000040 8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C

00000050 38 4E 24 7D 24 8B C1 99 E8 3C

00000060 66 A1 1C 7C 26 66 3B 07 26 8A

00000070 02 88 56 02 80 C3 10 73 EB 33

00000080 66 16 03 46 1C 13 56 1E 03 46

00000090 60 89 46 FC 89 56 FE B8 20 00

000000A0 03 48 F7 F3 01 46 FC 11 4E FE

000000B0 00 72 39 26 2D 74 17 60 B1

000000C0 61 74 32 4E 74 09 83 C7 20 3B

000000D0 FB 7D B4 7D 8B F0 AC 98 40 74

000000E0 BB 07 00 CD 10 EB EF A0 FD 7D

Sector 0 of 249087 Offset: 0 = 235 Block: n/a

[Exploring FAT.img]
File system: FAT16
Volume label: FAT16

Default Edit Mode: original
State: original
Undo level: 0
Undo reverses: n/a
Alloc. of visible drive space:
Cluster No.: n/a
Boot sector
Snapshot taken 14 hours ago
Total capacity: 122 MB
Size: n/a

Data Interpreter
8 Bit (±): -21
16 Bit (±): 15595
24 Bit (±): -7324437
32 Bit (±): 1301298411
DOS Date: 12/16/2018 07:39:22

After
Interpreting
as a Disk

Viewing Files/Folders

- ▶ To view the Hex/Text of any file or folder on a disk or in a forensic image, simply click on the file/folder in the Directory Browser.
- ▶ Scroll up/down through file/folder using scroll bar to the right of the “Text Display” window in the GUI.
- ▶ The icons in the Directory Browser for each file/folder indicate the “status” of the file/folder, as to whether it is an active file, deleted file but recoverable, deleted file that is overwritten and not recoverable, file was moved/renamed, etc.



Viewing Files/Folders

The screenshot shows the WinHex application window titled "WinHex - [Removable medium 1, Volume]". The menu bar includes File, Edit, Search, Position, View, Tools, Specialist, Options, Window, and Help. The toolbar contains various icons for file operations and editing. The main window displays a file list for "Removable medium 1" and "Removable medium..., Volume". The file list shows a folder "This is a renamed folder" and several files, including "active file.txt", "deleted file.txt", and "Fragmented Text File - Copied but copy is not fragme...". The file "deleted file.txt" is selected, and its contents are displayed in the hex editor view. The hex editor shows the file's data in hexadecimal and ASCII format. A "Data Interpreter" window is open, showing the file's properties, including its size, date, and time. The status bar at the bottom indicates the current sector, offset, and block information.

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
This is a renamed folder		2.0 KB	06/14/2010 22:13:16	06/14/2010 22:13:18	06/14/2010		2984
active file.txt	txt	23 B	06/14/2010 22:17:54	06/14/2010 22:19:58	06/14/2010	A	3036
active file.txt	txt	0 B	06/14/2010 22:17:54	06/14/2010 22:17:56	06/14/2010	A	
deleted file.txt	txt	24 B	06/14/2010 22:20:13	06/14/2010 22:20:14	06/14/2010	A	3040
deleted file.txt	txt	23 B	06/14/2010 22:18:06	06/14/2010 22:18:08	06/14/2010	A	3040
deleted file.txt	txt	0 B	06/14/2010 22:20:13	06/14/2010 22:20:14	06/14/2010	A	
deleted file.txt	txt	0 B	06/14/2010 22:18:06	06/14/2010 22:18:08	06/14/2010	A	
Fragmented Text File - Copied but copy is not fragme...	txt	18.9 KB	06/14/2010 22:13:38	06/14/2010 22:12:14	06/14/2010	A	2988
Fragmented Text File - Copy.txt	txt	18.9 KB	06/14/2010 22:13:38	06/14/2010 22:12:14	06/14/2010	A	2988

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0017C000	4E	65	77	20	54	65	78	74	20	46	69	6C	65	20	6F	76
0017C010	65	72	77	72	69	74	69	6E	67	20	63	6C	75	73	74	65
0017C020	72	20	36	33	32	2C	20	77	68	69	63	68	20	70	72	65
0017C030	76	69	6F	75	73	6C	79	20	63	6F	6E	74	61	69	6E	65
0017C040	64	20	22	64	65	6C	65	74	65	64	20	66	69	6C	65	2E
0017C050	74	78	74	22	20	61	6E	64	20	6E	6F	77	20	74	68	65
0017C060	20	66	69	6C	65	20	69	73	20	64	65	6C	65	74	65	64
0017C070	20	61	6E	64	20	6F	76	65	72	77	72	69	74	74	65	6E
0017C080	20	69	6E	73	74	65	61	64	20	6F	66	20	6A	75	73	74
0017C090	20	64	65	6C	65	74	65	64	2E	20	20	00	00	00	00	00
0017C0A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0017C0B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0017C0C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0017C0D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0017C0E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Removable medium ..99% free
File system: FAT16
Volume label: FAT16
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Alloc. of visible drive space:
Cluster No.: 632
to overwrite a previous file.txt
Snapshot taken 9 min. ago
Used space: 1.3 MB
Size: n/a

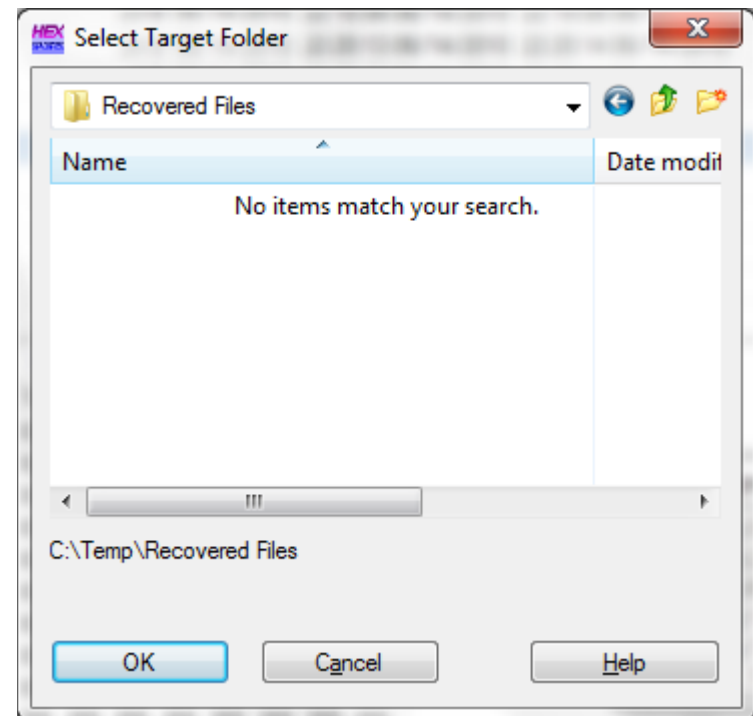
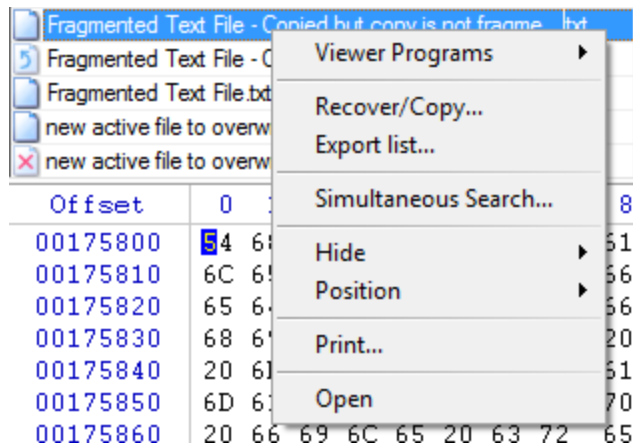
New Text File overwriting cluster 632, which previously contained "deleted file.txt" and now the file is deleted and overwritten instead of deleted.

8 Bit (±): 78
16 Bit (±): 25934
24 Bit (±): 7824718
32 Bit (±): 544695630
DOS Date: 03/23/1996
12:42:28

Sector 3040 of 249087
Offset: 17C000
= 78
Block: n/a
Size: n/a

Copying out (Recovering) Files/Folders

- ▶ In the Directory Browser, right-click on the desired file/folder and select Recover/Copy and select the path you wish to recover/copy the files to.



Editing data

- ▶ You must place WinHex into either Default Edit Mode or In-Place Edit Mode to make changes.
 - ▶ From the menu, select Options/Edit Mode
 - ▶ In Default Edit Mode you must click the “Save” button to commit any data changes you make.
 - ▶ In In-Place Edit Mode changes take place immediately as you type them.
- ▶ Changes can be made by typing HEX characters into the Hex Display window or typing text characters into the Text Display window.
- ▶ Disks or data (selected bytes) can be **wiped** using the Edit /Fill Disk Sectors or Edit Fill Block option from the menu.

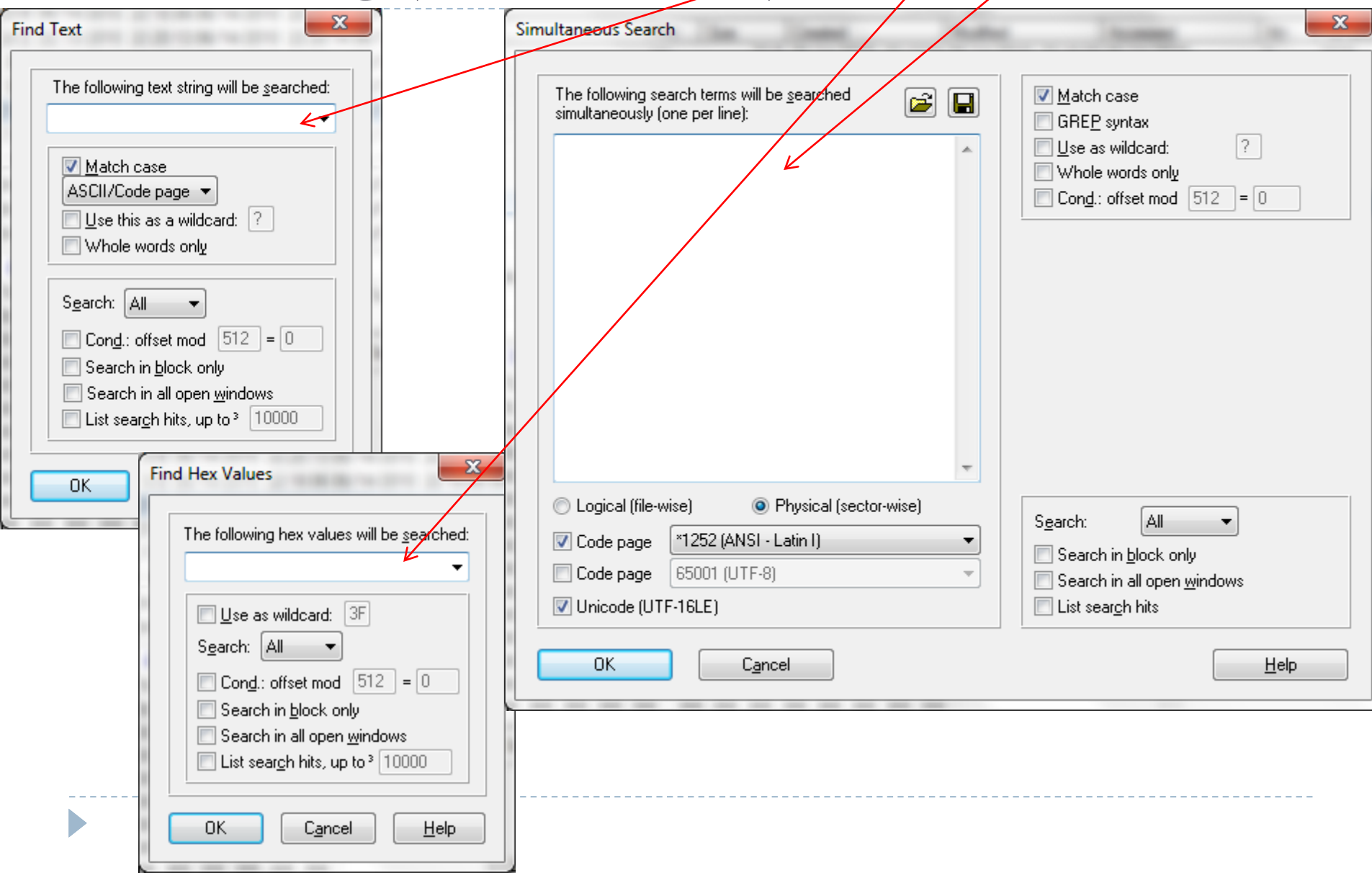


Searching (HEX/Text)

- ▶ Click on appropriate toolbar button or select appropriate option from Search menu to open Find Text, Find HEX Values search dialog boxes to search for a single string or value.
 - ▶ Use F3 key to continue search using same option(s).
- ▶ Use the Simultaneous Search option to search for multiple strings or values in a single search operation.
 - ▶ Allows you to perform a logical or physical search. Logical searching will find strings/values that are not contiguous due to file fragmentation.
- ▶ “List Search Hits” check box will search the whole disk/image and provide you a listing of “hits”.



Searching (Hex or Text)



Status Bar and Info Pane

▶ The status bar tells you:

- ▶ Sector # of selected byte
- ▶ Offset (from beginning of disk/partition) of selected byte
- ▶ Offset range of highlighted bytes
- ▶ Size (in bytes) of block of highlighted bytes

▶ Info bar tells you:

- ▶ A variety of information about the disk or image you have opened
- ▶ The cluster # and name of file/folder/disk area that the selected byte belongs to.
- ▶ Current edit status (i.e. Read-Only, Default Edit mode, In-Place Edit mode) and many other application settings...

Removable medium ..99% free
File system: FAT16
Volume label: FAT16

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space:
Cluster No.: n/a
Root directory

Snapshot taken 36 min. ago

Used space: 1.3 MB
1,331,200 bytes

Free space: 120 MB
125,933,568 bytes

Total capacity: 122 MB
127,532,544 bytes

Bytes per cluster: 2,048
Free clusters: 61,491
Total clusters: 62,141

Bytes per sector: 512
Usable sectors: 248,564
First data sector: 520

Physical disk: 1

Display time zone: original
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal

Interpreting HEX values

- ▶ In addition to using the Windows calculator to convert Hex to Decimal or Binary, we can also use the Data Interpreter that is built into WinHex.
- ▶ To change the list of items that Data Interpreter will list, select Options/Data Interpreter and select the desired date format and/or other integer types you wish to interpret.
- ▶ To use the Data Interpreter, simply click on the “left most” byte of any byte or group of bytes and the Data Interpreter will read the bytes to the right of the byte you click on and show the interpretation of those bytes.



Interpreting HEX values

01	61	00	63	00	74	00	69	00	76	00	0F	00	5A	65	00	a c t i v							
20	00	66	00	69	00	6C	00	65	00	00	00	2E	00	74	00	f i l e							
41	43	54	49	56	45	7E	31	54	58	54	20	00	5D	3B	B2	ACTIVE~1TXT							
CE	3C	CE	3C	00	00	7D	B2	CE	3C	77	02	17	00	00	00	Î<Î< }²Î<w							
E5	74	00	78	00	74	00	00	00	FF	FF	0F	00	A7	FF	FF	ât x t yy							
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF	FF	yyyyyyyyyyyy							
E5	64	00	65	00	6C	00	65	00	74	00	0F	00	A7	65	00	âd e l e t							
64	00	20	00	66	00	69	00	6C	00	00	00	65	00	2E	00	d f i l e							
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FFFFFFFFFFFFFF							

Data Interpreter

8 Bit (±): 125

16 Bit (±): -19843

24 Bit (±): -3231107

32 Bit (±): 1020179069

DOS Date: 06/14/2010

22:19:58