# **BRISTOL COMMUNITY COLLEGE** CIT-155 Intro to Computer Forensics

## WinHex Tutorial

The Specialist version of WinHex is the baby brother of the X-Ways Forensics software package. WinHex is not only an extraordinarily powerful hex editor, but Specialist has several powerful tools to help in the low-level analysis of media and file systems. This low-level analysis is important for the understanding of both the logical structures of a file system and the limitation of manual methods for computer forensics examinations -- particularly as disk drives and other storage media grow larger and larger.

This tutorial will cover some of the essential functions of WinHex Specialist that will be useful in our course. These functions include:

- Sanitizing media and verifying the initialization
- Restoring a disk image
- Opening an image file as a disk
- Logical structure templates
- The data interpreter
- Gather free space
- Copying blocks and creating files
- Exporting a file list

## Sanitizing media and verifying the initialization

WinHex can be used to wipe target media to prepare it prior to copying an image. The software can also be used to verify that the wiping has been successful. This example describes how to overwrite the contents of a USB thumb drive with all zeroes:

- 1. Insert the target USB flash media into a USB port.
- 2. Start WinHex.
- 3. Open the USB drive using the Tools, Open Disk... command (or press the F9 key). Be sure to select the USB drive as a *physical* device.

Edit Disk
Cojical Drive Letters (C.), HD0 (D.) Removable medium (E.), RM 1 Physical Media HD0: Hitachi HTS721080G9SA00 (74.5 GB) RM1: USB v2.0Flash Disk (126 MB, USB) Optical drive 0
<u>OK</u> Cancel <u>H</u> elp

4. Use the Edit, Fill Disk Sectors... command (or press control-L<sup>1</sup>) to zero-fill all sectors on the USB drive.

Fill Disk Sectors		X
<ul> <li>Fill with hex values</li> <li>Simple pseudo-random numbers Range: 0 to 255 (0255)</li> <li>Simulate encrypted data</li> <li>Cryptogr. secure pseudo-random (slow)</li> </ul>	Passes: Pass #1	A <u>d</u> d Dejete < 0x <u>0</u> 0 < <u>D</u> oD
<u>Q</u> K C <u>a</u> ncel		Help
Filling sectors		×
80%		
approx. ½n 55 MB/min	nin. left	

<sup>&</sup>lt;sup>1</sup> The "control" character may also be denoted by the "^" character, so that "^L" should be interpreted at control-L.

5. Visually verify that the drive has been zero-filled. The most effective way to do this is with the Tools, Analyze Disk command (F2).



A window will open that appears to be blank; what it shows is the relative occurrence of the 256 bit patterns from 0x00-0xFF. If you move your mouse all the way to the left of the screen until you see the display indicate *00h*, you should see the middle figure indicate *100%* and the "Occurrences" value indicates *(maximum!)*.



6. You can calculate the hash value of a medium using the Tools, Compute Hash... command (^F2). You can select from a number of hash algorithms, but MD5 and SHA-1 are the most common for digital forensics applications.



Hashing	X
38%	
approx. 1½min. left 56 MB/min	
HDE /428 5#1	
MD5 (128 DIC)	
for USB v2.0Flash Disk:	
8EF55098CD2E1AD15F08715595D3C804	
Close	

Note that WinHex can also be used to securely wipe individual files. For this function, see Tools, File Tools, Wipe Securely...

## Restoring a disk image

A disk image can be restored using the File, Restore Image command.

1. Select the image file, which can be in .001, .ctr, .dd, .img, or .whx (WinHex Backup) format.

Select Target Disk	×
Logical Drive Letters (C), HD0 (D) Removable medium (E:), RM 1 [mod1-1.dd] Physical Media HD0: Hitachi HTS721080G9SA00 (74.5 GB) RM1: USB v2.0Flash Disk (126 MB, USB) Optical drive 0	
<u>D</u> K C <u>a</u> ncel <u>H</u> elp	]

2. Select the appropriate output medium.

Clone Disk (Copy Sectors)	×
Source: medium [mod1-1.dd] (1.4 MB) Destination: medium Removable medium 1, USB v2.0Flash Disk (1)	Copy entire medium Start sector (source): Contemporation Start sector (destination): Number of sectors to copy: 2880
✓ Log procedure silently (no error messages)	Avoid damaged areas. Skip range:
Write pattern for damaged source sectors: UNRE	EADABLESECTOR
Simultaneous I/O (faster, if source and destination are	different physical media)
<u>OK</u> C <u>a</u> ncel	<u>H</u> elp

3. Confirm that the source is the image file and the destination medium is correct, and click OK.

WinHex		×
(	2,880 sector(s) successfully copied.	
	<u>O</u> K	

You can open a disk using the Tools, Open Disk command (F9).

## Opening an image file as a disk

An image file can be opened directly and used as if it were from a disk.

- 1. Open the image file using the File, Open command (^O).
- 2. Use the Specialist, Interpret Image File As Disk command to have the file open as if it were the original disk

WinHex - [[mod1-1.dd]	11					15.0 🔲 🗖 🗙
📾 File Edit Search Position	n View Tools	Specialist O	ontions Window He	-In		_ 7 ×
		1015	a da 67 67 aa			
		010	HEX COB HEX 844		S 🚽 🖓 📖	
[mod1-1.dd]						
X						8+1=9 files, 5 dir.
Name 🔺	Ext.	Size	Created	Modified	Accessed A	ttr. 1st sector
(Root directory)		7.0 KB				19
DIR1		0.5 KB		09/21/2000 13:50:58		38
DIR2		0.5 KB		09/21/2000 13:51:00		39
DIR3		0.5 KB		09/21/2000 13:51:04		40
DIR4		0.5 KB		09/21/2000 13:51:38		56
[mod1-1 dd]	Offset	0 1	2 3 4 5	5789A	BCDEF	🔽 🔍 📩
File system: FAT12	00000000	<b>₽</b> В 3С 9	90 4D 53 57 4	94E 342E 31	00 02 01 01 00	B< MSWIN4.1
Volume label: MOD1-1	00000010	02 E0 0	00 40 OB FO O	9 00 12 00 02	$00 \ 00 \ 00 \ 00 \ 00$	.à.@.ð
	00000020	00 00 0	00 00 00 00 2	900 154F0B	4D 4F 44 31 2D	)0.MOD1-
Default Edit Mode	00000030	31 20 2	20 20 20 20 4	5 41 54 31 32	20 20 20 33 C9	1 FAT12 3E
State. Oliginal	00000040	SE DI E	BC FC 7B 16 U	7 BD 78 00 CS	76 UU 1E 56 16	∎N%u{%x.AvV.
Undo level: 0	00000050	1E DD 0	22 US 89 7E U 20 7C C( AF E	J 89 4E UZ BI	UB FC F3 A4 U5	VC". "". N. ±. UO4.
Undo reverses: n/a	00000080	E9 7E 0	JU 7C C8 45 F1	5 UF 30 4E 24	7D 20 0D CI 33	.72. [#ED.0N≎] A A~ A.fi  f. Uij
Alloc, of visible drive space:	00000070	75 06 8	30 CA 02 88 51	5 MI 10 70 88	35 07 88 57 FC 73 FD 33 C9 FF	u É V X sí3Éb
	000000000	06 D8 2	7D 8A 46 10 9	3 F7 66 16 03	46 1C 13 56 1E	Ø}F -f F V
Cluster No.: n/a Root sector	000000A0	03 46 0	DE 13 D1 8B 7	5 11 60 89 46	FC 89 56 FE B8	.F. N.v. FuVb.
DOUT SECTOR	000000B0	20 00 E	77 E6 8B 5E 01	3 03 C3 48 F7	F3 01 46 FC 11	.÷æ ^ÃH÷ó.Fü.
6 I.V.I. 14.I	000000000	4E FE 6	61 BF 00 07 E	3 28 01 72 3E	38 2D 74 17 60	Nþaćè(.r>8-t.`
Shapshot taken 14 days ago	000000D0	B1 0B E	BE D8 7D F3 A	561743D4E	74 09 83 C7 20	±.¾Ø}ó¦at=Nt.∎Ç
Total capacity: 1.4 MB	000000E0	3B FB 7	72 E7 EB DD F1	E OE D8 7D 7B	A7 BE 7F 7D AC	;ûrçëŸþ.Ø}{S¾∎}¬
1,474,560 bytes	000000F0	98 O3 E	FO AC 98 40 7	4 OC 48 74 13	B4 OE BB 07 00	∎.ð-∎@t.Ht.´.»
	00000100	CD 10 E	EB EF BE 82 71	DEB E6 BE 80	7D EB E1 CD 16	I.ëï¼ }ëæ¾ }ëáI.
Bytes per cluster: 512	00000110	5E 1F 6	56 8F 04 CD 1	9 BE 81 7D 8B	7D 1A 8D 45 FE	".t∎.1.%∎}∎}.∎Ep
Total clusters: 2,847	00000120	72 D7 D	JD F7 E1 03 40 73 00 02 70 0	0 FC 13 56 FE	EL 04 E8 C2 00	Na.FU.VDI.CA.
Bytes per sector: 512	00000130	8B 46 1	18 &2 26 05 9	5 92 33 D2 F7	F6 91 F7 F6 42	IX8p.Kr.Sj.j. IF ∧& ∎130±81±8B
Usable sectors: 2,847	00000150	87 CA E	77 76 1A 8A F	2 84 E8 C0 CC	02 0A CC B8 01	
First data sector: 33	00000160	02 80 7	7E 02 0E 75 0	1 B4 42 8B F4	8A 56 24 CD 13	. [~u. B ô V\$1.
Display time zone: original	00000170	61 61 7	72 OA 40 75 0	L 42 03 5E 0B	49 75 77 C3 03	aar.@u.B.^.IuwA.
Mode: hexadecimal	00000180	18 01 2	27 OD OA 49 61	E 76 61 6C 69	64 20 73 79 73	'Invalid sys
Character set: ANSI ASCII	00000190	74 65 6	SD 20 64 69 7	3 6B FF OD OA	44 69 73 6B 20	tem diskÿDisk
Offsets: hexadecimal	000001A0	49 2F 4	4F 20 65 72 7	2 6F 72 FF 0D	OA 52 65 70 6C	I∕O errorÿRepl
Bytes per page: 32x16=512	000001B0	61 63 6	55 20 74 68 6	5 20 64 69 73	6B 2C 20 61 6E	ace the disk, an
Window #: 1	000001C0	64 20 7	74 68 65 6E 2	0 70 72 65 73	73 20 61 6E 79	d then press any
No. of windows: 1	00000100	20 68 6	55 79 UD UA 01	JUU 49 4F 20	20 20 20 20 20 20	key10
	000001E0	00 41 5	53 4D 53 44 41 55 00 07 60 6	153 202020 21 21 2020	53 57 53 /F UI	SISNEDUE SYSL.
2	00000120	00 41 1		DOM UUE7 3B	rr 00 00 55 AA	.m» Ij.e;yu= 💌
Sector 0 of 2880	Offset:		0	= 235 Block:		n/a Size: n/a

3. Note in the display above the presence of the directory browser, which are the lines that show the directories and files. Clicking on a directory or file will move you to that location. If the directory browser is not displayed, use the View, Show, Directory Browser command (^F7) or click on the

#### Usage hints:

- a. Note in the display above that the width of the screen is set to show 16 columns, numbers 0-F. This is the best setting to ensure a view of 16 bytes per line.
- b. Note also that 32 lines are shown here (offset 0x0000-0x01F0). You can display any number of lines that you would like but 32 lines is 512 bytes, or exactly 1 sector (see the sector counter at the lower left of the screen). With this number of lines, the display goes to the top of a new sector every time you hit Page Down.
- c. Note that the values listed in the offset column are in hexadecimal. If you click anywhere in the column, the numbers to change to decimal. Keeping the values in hex is probably simpler. As an aside, 0x200 = 512, which is the size of a sector.

#### Logical structure templates

WinHex provides a number of templates that make the interpretation of logical structures much simpler for the user. Indeed, while the user can always see -- and change -- the raw hex values,

the templates make interpretation that much simpler. For our course purposes, the most useful templates are those for the master boot record (MBR) and directories.

The **\_\_\_\_** icon can be used to expose a pulldown menu such as:

Boot sector Boot sector (template) FAT 1
FAT 2
Root directory Root directory (template)
MOD1-1 (0 B) Search directory (up) Search directory (down)

Clicking on *Boot sector* will move you to the boot sector portion of the image, whereas clicking on *Boot sector (template)* will show you the boot sector and provide an interpretation of all of the fields.

🗱 WinHex - [[mod1-1.0	dd]]		15.0 📃 🗖 🗙
🌍 File Edit Search Posi	ition View Tools Specialist Option	s Window Help	_ 8 ×
n 🚅 🗏 🎒 😭 🗽 .	🗆 🗠 🚉 🖻 1012 🛛 👪 🏄	. 16 💥 🏘 丨 🗕 🗗 🖨 📥 🗌 🕰	馬 🧼 💷 🔎 🛛 🔠 🖉 🖌 🌒
[mod1-1.dd] GCKtest.zip	🐺 Boot Sector FAT, Base Offse	t: 0 🔀	
N	Offset Title	Value	8+1=9 files, 5 dir.
Name 🔺	0 IMP instruction	EP 2C 90	Attr. 1st sector
(Root directory)	o SMF Instruction	ED 3C 3U	19
🚞 DIR1	3 UEM	M3W1W4.1	38
DIR2			39
DIR3	BIOS Parameter Block		40
DIR4	B Bytes per sector	512	56 💌
[mod1-1 dd]	D Sectors per cluster	1	DEF 🗸 🔍 🔺
File system: FAT	E Reserved sectors	1	1 01 00 ë< MSWIN4.1
Volume label: MOD	10 Number of FATs	2	0 00 00 .à.@.ð
Defects Eds Media	11 Root entries	224	4 31 2D)O.MOD1-
State: origi	13 Sectors (under 32 MB)	2880	U 33 C9 1 FAT12 3E
oldio. oligi	15 Media descriptor (hex)	FO	E 55 15 $\mathbb{N}^{2}$ $\mathbb{N}^{2}$ $\mathbb{N}^{2}$ $\mathbb{N}^{2}$ $\mathbb{N}^{2}$ $\mathbb{N}^{2}$ $\mathbb{N}^{2}$ $\mathbb{N}^{2}$ $\mathbb{N}^{2}$
Undo level:	16 Sectors per FAT	9	B C1 99 36 LAFFE 8NS3 4
Undo reverses.	18 Sectors per track	18	A 57 FC è~. të:fi.lf:.tVu
Alloc. of visible drive space:	1A Heads	2	3 C9 FE u. Ê. V. Ã.sí3Éþ
Cluster No.:	1C Hidden sectors	0	3 56 1E .∅}∎F.∎÷fFV.
Boot sec	20 Sectors (over 32 MB)	0	6 FE B8 .FÑ∎v.`∎Fü∎Vþ,
	. ,		= 6 FC 11 .÷æ ^AH÷ó.Fü.
Snapshot taken 14 days a	24 BIOS drive (bex HD=8)	00	4 17 50 Npac $e(.r>8-t.$
	25 (Upused)	0	$F$ 7D AC : $\hat{u}rc \in \hat{V}h$ $\hat{a}l < \hat{s}_{1}l$
I otal capacity: 1.4	26 Ext boot signature (29b	29	B 07 00 1.8-10t.Ht. (
1,474,300 by	27 Volume serial number (d	189732096	✓ 1 CD 16 1.ëï¾ }ëæ¾ }ëá1.
Bytes per cluster: 51	12 UUUUU110 5E 1F 66 8	F U4 CD 19 BE 81 7D 8B 7D 1A	8D 45 FE ^.f∎.Í.¾∎}∎}.∎Eþ
Total clusters: 2,84	47 00000120 8A 4E 0D H	7 E1 03 46 FC 13 56 FE B1 04	E8 C2 00 ∎N.÷á.Fü.Vþ±.èÅ.
Bytes per sector: 51	12 00000130 72 D7 EA (	0 02 70 00 52 50 06 53 6A 01	6A 10 91 r×ēp.RP.Sj.j.'
Usable sectors: 2,84	47 00000140 8B 46 18 4	6 1  8	F7 F6 42 『F.0@.』 30+0 +05 CC B8 01 『Êニャ 』と言われ 主
First data sector:	33 00000160 02 80 7E (	2 DE 75 D4 B4 42 88 F4 8A 56	24 CD 13 BOLVSÍ.
Display time zone: origin	al 00000170 61 61 72 0	A 40 75 01 42 03 5E 0B 49 75	77 C3 O3 aar.@u.B.^.IuwÃ.
Mode: hexadecim	al 00000180 18 01 27 (	D 0A 49 6E 76 61 6C 69 64 20	73 79 73'Invalid sys
Character set: ANSI ASC	CII 00000190 74 65 6D 3	0 64 69 73 6B FF 0D 0A 44 69	73 6B 20 tem diskÿDisk
Offsets: hexadecim	al 000001A0 49 2F 4F 2	0 65 72 72 6F 72 FF 0D 0A 52	65 70 6C I/O errorÿRepl
bytes per page: 32(16=5)	000001B0 61 63 65 2	0 /4 68 65 20 64 69 /3 6B 2C	20 bl bE ace the disk, an
Window #:	1 000001C0 64 20 74 6	0 05 05 20 70 72 65 73 73 20 9 05 04 00 00 49 45 20 20 20	20 20 20 key TO
IND. OF WINDOWS:	000001E0 53 59 53 4	D 53 44 4F 53 20 20 20 53 59	53 7F 01 SYSMSDOS SYSL
-	000001F0 00 41 BB (	0 07 60 66 6A 00 E9 3B FF 00	00 55 AA .A»`fj.é;ÿUª 👽
Sector 0 of 2880	Offset:	0 = 235 Block:	n/a Size: n/a

Similarly, clicking on *FAT1*, *FAT2*, and *Root directory* will move the display to those portions of the image. Clicking on *Root directory (template)* moves to the root directory and provides an interpretation of the field of each directory entry; click on the left and right arrows to go back or forward within the directory.

🐺 WinHex - [[mod1-1.c	dd]]					15.0	
🥪 File Edit Search Posi	tion View Tools	Specialist Options	Window Help				_ 8 ×
□ ☞ 🗆 🖨 🗳 .	ю <b>h 🛱</b> h	1012	26 96 MA   -	• –₽ì <=⇒ │ ∠≤	<u>9 🖣 🧼 📠</u>		III 🤣
[mod1-1.dd] GCKtest.zip	🚟 FAT Directory	Entry, Base Of	fset: 2600		×		
Ν						8+1	=9 files, 5 dir.
Name 🔺	Record #: 0		> <u>Liose</u>			Attr. 1st sector	~
🚺 (Root directory)	Offset	Title	Va	lue		19	
DIR1	2600 Eilen:	me (blank-nadded)	MOD1-1			38	_
DIR2	2000 Filena 2600 Exter	nie (blank padded)	MODIFI			39	
DIR3	2000 EXIEN	ISION (Diank-paudeu	20			40	_
DIR4	200D UF =		20			56	×
[mod1-1.dd]	260B Attnb	utes (a-dir-vol-s-n	00101000		DEI	V 🔍 🛰	^
File system: FAT	2600 00 =	Never used, E5 = E	40		0 00 00	) MOD1-1 (	
Volume label: MOD	260C (reser	ved)	0		0 00 00	)n5)	
Defects Eds Mede	260E Creat	ion date & time	n/a	n/a	0 00 00	) åILE1	
State: origi	260D Cr. tin	ne refinement in 10-	0			J	
Uada Javali	2610 Acce	ss date (no time!)	n/a	n/a		1n5	
Undo level: Undo reverses:	2616 Upda	te date & time	09/21/2000	13:48:10		) FILE3	
	2614 (FAT	32) High word of cl	0		1 00 00	)Gn5){	
Alloc. of visible drive space:	261A 16-bit	cluster #	0		0 00 00	) FILE4	
Cluster No.:	261C File si	ze (zero for a direct	0		0 00 00	)Zn5)Ó	
Root direct					0 00 00	) DIR1	
						Jjn5)	
Snapshot taken 14 days a						) DIRZ	
<b>T</b>						) DIR3	
Total capacity: 1.4 1.474 560 by					0 00 00	)bn5)	
1,474,000 by					0 00 00	) DIR4	
Bytes per cluster: 51	2 00002710	00 00 00 00	) UU UU 73 6E	35 29 19 00 0	U UO OO O(	)sn5)	
Total clusters: 2,84	00002720					)	
Bytes per sector: 51	2 00002730						
Usable sectors: 2,84	00002740					,	
First data sector: 3	00002760				0 00 00 00	)	
Display time zone: origin	al 00002770	00 00 00 00	0 00 00 00 00	00 00 00 00 0	0 00 00 00	)	
Mode: hexadecim	al 00002780	00 00 00 00	00 00 00 00 00	00 00 00 00 0	0 00 00 00	)	
Character set: ANSI ASC	00002790	00 00 00 00	00 00 00 00 00	00 00 00 00 0	0 00 00 00	)	
Offsets: hexadecima	al 000027A0				0 00 00 00	)	
bytes per page. 52X 16=51	2 000027B0					J	
Window #:	00002700					1	
NO. OF WINDOWS:	000027E0					)	
	000027F0	00 00 00 00	0 00 00 00 00	00 00 00 00 0	0 00 00 00	)	~
Sector 19 of 2880	Offset:	260	0	= 77 Block:		n/a Size:	n/a

The pulldown menu also allows you to search for subdirectories, although there is no obvious way to see the directory template. If you want the directory template when perusing a subdirectory, use the View, Template Manager... command (alt-F12), select FAT Directory Entry, and click Apply!

WinHex - [[mod1-1.	dd]]										15.0	- <b>-</b> ×
🎯 Eile Edit Search Pos	ition <u>V</u> iew	<u>T</u> ools Specijalist	Options W	indow <u>H</u> el	P							_ 8 ×
🗅 🚅 🗐 🎒 😭 🕍	N 🖹	🛍 🖻 1012	🐴 🏯 😘	🙀 🙀	-> -	🖻 💠 🔿	-   🗠	3 🖶 🏟		<b>⊳</b>   ∰	۵ 🕨 📢	III 🤌 🛛
[mod1-1.dd] GCKtest.zip												
N											8+1	=9 files, 5 dir.
Name -		Ext. Size	Created		Modified		Access	ed	A	tr. 1st sec	tor	~
(Root directory)		7.0 KE	3							19		
🚞 DIR1		0.5 KE	3		09/21/20	0 13:50:58	3			38		_
DIR2		0.5 KE	3		09/21/20	00 13:51:00	)			39		
DIR3		0.5 KE	3		09/21/20	0 13:51:04	1			40		_
DIR4		0.5 KE	3		09/21/20	0 13:51:38	3			56		~
[mod1-1.dd]	044-		<u> </u>	л F (	7	- 0 X	- D - Q	E E	F	- X 🔍	- ma	~
File system: FAT	🚟 FAT Dir	rectory Entry, I	Base Offse	t: 4C40				🔀 D 00	00			
Volume label: MOD				~	_			0 00	00	]	n5)	_
Defeuilt Edit Made	Record #:	2		Ciose				0 00	00			
State: origin	Offset	Title			Value				00	j	n5)	
Unde lavali	4040	Filename Alank	anddad) Ell	E1				0.00	00	FILEI	n5) v	
Undo ievei: Undo reverses: n	4040	Filenanie (plank-	padded) Fit					0 00	00	åILE2		
	4048	Extension (blank	-padded					2 00	00	1	n5)!	
Alloc. of visible drive space:	4C4B	UF = LFN entry	20					0 00	00	FILE3		
Cluster No.:	4C4B	Attributes (a-d	ir-vol-s-h 00	100000				L 00	00	G	n5){	
DI	4C40	00 = Never used	i, E5 = E 46	5				0 00	00	FILE4		
	4C4C	(reserved)	0					D 00	00	Z	n5)0	
Snapshot taken 14 days a	4C4E	Creation date & t	ime n/	а	n/	3		0 00	00			
	4C4D	Cr. time refineme	nt in 10- 0					0 00	00			
Total capacity: 1.4 M	4C50	Access date (no	time!) n/	a	n/	в		0 00	00			
1,474,560 byt	4C56	Update date & ti	me 09	/21/2000	13	:48:56		0 00	00			
Bytes per cluster: 5	4C54	(FAT 32) High w	ord of cl 0					0 00	00			
Total clusters: 2,8	4C5A	16-bit cluster #	10	)				0 00	00			
Bytes per sector: 5	4C5C	File size (zero for	a direct 37	7				0 00	00			
Usable sectors: 2,8								0 00	00			
First data sector:									00			
Display time zono: origin								0.00	00			
Mode: hexadecin								0 00	00			
Character set: ANSI AS								0 00	00			
Offsets: hexadecin								0 00	00			
Bytes per page: 32x16=5			<del></del>	<del></del>	00 0		00 00	<b>, ,</b> 0 00	00			
Window #:	1 00004	DC0 00 00	00 00 0	0 00 00	00 0	00 00	00 00	00 00	00			
No. of windows:	2 00004		00 00 0	0 00 00 0 00 00	00 0	, 00 00 , 00 00	00 00	00 00	00			
	00004			0 00 00 N NN NN	00 0	, 00 00 1 00 00		, 00 00 1 00 00	00			~
Contar 20 of 2000	00004	Offect:	4040	00 00		D Block:	50 00		00	n/n Gi-		- n/a
360101 30 01 2000		Unset.	4040		=	DIOCK:				17a Siz	.c.	n/a

### The data interpreter

The data interpreter can be an invaluable aid when trying to determine the value of a field, particularly when the field spans more than one byte.

Data Interpreter	×
8 Bit (±): 70	
16 Bit (±): 18758	
32 Bit (±): 1162627398	

The Data Interpreter window, as shown above, indicates the 8-, 16-, and 32-bit value starting from the byte location where the cursor is currently highlighted.

Data Interpreter Options	
<ul> <li>8 bit, signed</li> <li>8 bit, unsigned</li> <li>16 bit, signed</li> <li>16 bit, unsigned</li> <li>24 bit, signed</li> <li>24 bit, unsigned</li> <li>32 bit, signed</li> <li>32 bit, unsigned</li> <li>64 bit, signed</li> </ul>	<ul> <li>DOS Date+Time (32 bit)</li> <li>Win32 FILETIME (64 bit)</li> <li>OLE 2.0 Date+Time (64 bit)</li> <li>ANSI SQL Date+Time (64 bit)</li> <li>UNIX/C Date+Time (32 bit)</li> <li>Min's instead of sec's</li> <li>HFS+ Date+Time (32 bit)</li> <li>Java Date+Time (64 bit)</li> <li>Time zone: 00:00</li> <li>Binary (8 bit)</li> </ul>
☐ <u>F</u> loat (=Single, 32 bit) ☐ <u>R</u> eal (48 bit) ☐ Doub <u>l</u> e (64 bit)	Assembler opcodes
Long Double (=Extend., 80)	Digit grouping

The values shown in the Data Interpreter can be configured using the Options, Data Interpreter... command (alt-F5). As shown above, the Data Interpreter is currently displaying 8-, 16-. and 32-bit unsigned values starting at the current cursor position; this is the WinHex default although many other interpretations can also be shown.

The default byte ordering is Little Endian, meaning the first byte in the field is the arithmetically least significant byte (LSB) and the last byte in the field is the arithmetically most significant byte (MSB). By way of example, suppose a three-byte had the following hex values:

00 1C 22

With a Little Endian interpretation, most common on Intel processors, these three bytes represent the number 0x221C00 (decimal 2,235,392). With a Big Endian interpretation, these bytes represent the number 0x001C22 (decimal 7,202).

WinHex - [[mod1-1.dd]]						15.0 🔳 🗖 🔀
Eile Edit Search Position View	<u>T</u> ools Sp	ecialist <u>C</u>	Options <u>W</u> indow	<u>H</u> elp		- 8 ×
머 🚅 🗐 🚑 😭 🙋 🗆 🗠 📭	💼 🗈 !	012 d	🗛 🧟 🎊 🏄 🍐	<b>↓</b> → + <b>P</b> <= ⇒	🔄 🗠 🕞	Q 🛛 🚓 🖌 🕨 💼 🔲 🥔
mad1-1 ddl CCléast de			W HEX 1990 HEX W		~	
[mod - 1.dd] GCRtest.zip						
\DIR1				[		3+1=4 files, 0 dir.
Name A	Ext. S	ize	Created	Modified	Accessed A	ttr. 1st sector
 3 au 5a		0.5.100		00/01/0000 10 40 04		12
		0.5 KB		09/21/2000 13:49:34	A	42
		3// B		09/21/2000 13:48:56	A	41
FILE3		3/9 8		09/21/2000 13:50:14	A	44
FILE4		211.6		03/21/2000 13:50:52	A	43
[mod1-1.dd] Of t	set	0 1	2 3 4 5	6789A	BCDEF	
File system: FAT12 0000	4C00	2E 20	20 20 20 20	20 20 20 20 20 20	10 00 00 00 00	· · · · · · · 🔳
Volume label: MOD1-1 0000	4C10	00 00 1	00 00 00 00	5D 6E 35 29 07	00 00 00 00 00	]n5)
Default Edit Mode	4C20	2E 2E :	20 20 20 20 20	20 20 20 20 20 20 TD CE 25 20 20	10 00 00 00 00	1
State: original 0.000	4030	10 UU I 16 10		ор ов. 35 29 UU ор ор ор ор		jn5)
	4040	46 47 4	46 45 31 20			FILEI
Undo level: 0 0000	4060	55 49 .	4C 45 32 20	20 20 20 20 20 20 20		≜TTF2
0100 reverses. 11/a 0000	4C70			31 6E 35 29 0B	00 21 02 00 00	1n5) /
Alloc. of visible drive space: 0000	4C80	46 49	4C 45 33 20		20 00 00 00 00	FILE3
Chuster No. 7 0000	4C90	00 00	00 00 00 00	47 6E 35 29 0D	00 7B 01 00 00	Gn5)
DIR1 000	4CA0	46 49	4C 45 34 20	20 20 20 20 20 20	20 00 00 00 00	FILE4
\ 0000	4CB0	00 00 0	00 00 00 00	5A 6E 35 29 0E	00 D3 00 00 00	Zn5)Ó
0000	4CC0	00 00	00 00 00 00	00 00 00 00 00	$00 \ 00 \ 00 \ 00 \ 00$	
Shapshot taken 14 days ago 0000	4CD0	00 00	00 00 00 00	00 00 00 00 00	$00 \ 00 \ 00 \ 00 \ 00$	
Total capacity: 1.4 MB 0000	4CE0	00 00 1	00 00 00 <mark>Data 1</mark>	nterpreter	00 00	
1,474,560 bytes 0000	4CF0	00 00	00 00 00 8B	t (+): 123	00 00	
0000	4D00	00 00 1	00 00 00 16 B	t (±): 379	00 00	
Bytes per cluster: 512 0000	4D10		00 00 00 32 B	t (±): 379	00 00	
Total clusters: 2,84/ 0000	4D20		00 00 00 00			
Bytes per sector: 512	4D30			JU UU UU UU UU UU		
Usable sectors: 2,847	4050		00 00 00 00	, , , , , , , , , , , , , , , , , , ,		
First data sector: 33 0000	4D60	00 00 I	00 00 00 00	00 00 00 00 00 00 00		
Display time zone: original 0000	4D70				00 00 00 00 00	
Mode: hexadecimal 0000	4D80	00 00 1	00 00 00 00	00 00 00 00 00	00 00 00 00 00	
Character set: ANSI ASCII 0000	4D90	00 00 1	00 00 00 00	00 00 00 00 00	00 00 00 00 00	
Offsets: hexadecimal 0000	4DA0	00 00 0	00 00 00 00	00 00 00 00 00	$00 \ 00 \ 00 \ 00 \ 00$	
Bytes per page: 32x16=512 0000	4DB0	00 00 0	00 00 00 00	00 00 00 00 00	$00 \ 00 \ 00 \ 00 \ 00$	
Window #: 1 0000	4DC0	00 00	00 00 00 00	00 00 00 00 00	$00 \ 00 \ 00 \ 00 \ 00$	
No. of windows: 2 0000	4DD0	00 00	00 00 00 00	00 00 00 00 00	00 00 00 00 00	
0000	4DE0	00 00 1	00 00 00 00	0 00 00 00 00	00 00 00 00 00	
	4DF0	00 00	00 00 00 00	00 00 00 00 00 00	00 00 00 00 00	•••••••••••••••••••••••••••••••••••••••
Sector 38 of 2880	Offset:		4C9C	= 123 Block:		n/a Size: n/a

An example in the use of the data interpreter is shown in the screen shot above. In this example, the cursor is highlighting byte offset 0x4C9C. This screen shows entries in a subdirectory listing; the specific byte that is highlighted is byte 28in the directory entry for a file named FILE3; byte offsets 28-31 in the directory entry represent the file length.

The Data Interpreter shows the following:

- The 8-bit value (i.e., byte offset 28 alone or 0x7B) is 123
- The 16-bit value (i.e., byte offsets 28-29 or 0x017B) is 379
- The 32-bit value (i.e., byte offsets 28-31 or 0x0000017B) is 379

Since the file length field is a 32-bit field starting at byte offset 28, we want the 32-bit interpretation. By the way, this can be verified by looking at the directory listing above that clearly shows FILE3's length to be 379.

Finally, if you close the Data Interpreter mini-window and want to reopen it later, use the View, Show command and check the Data Interpreter box.

## Gather free space

One essential function when doing the analysis of a disk drive is to examine the information in unallocated space to find remnants of deleted files. In the WinHex vernacular, *unallocated space* is called *free space*; for our purposes, the two terms are synonymous.

Gathering free space in WinHex is very easy. Once an image or disk is opened, merely use the Specialist, Gather Free Space... command. When the Split Output Window dialogue box appears, choose some value that makes sense for your storage capabilities; any value between 100 KB and 4 MB is probably ok.

Split Output File	
Desired file	<u>s</u> ize:
2	мв 💌
	Cancel

Gathering file slack space is equally easy; use the Specialist, Gather Slack Space... command.

Note: When specifying the output file name, it is best to place the file in a directory of its own. The reason is that many disk carving utilities, such as Simple Carver Lite, use the contents of an entire directory as the input rather than individual files. Placing the Free Space (and Slack Space) files in their own directory provides some protection against accidentally including files from some other source other than the image.

## Copying blocks and creating files

The ability to export user-defined blocks of data as files is an important one in WinHex. This section will describe how to define a block of data, export a single block of data as a file, and export multiple blocks of data into a single file.

Define	bl	lock
./		

🚟 WinHex - [[mod1-1.dd]	]]					15.0 🔲 🗖 🔀
Eile Edit Search Position	n <u>V</u> iew <u>T</u> ools	Specialist Options	<u>W</u> indow <u>H</u> elp			_ = ×
D 🚅 🗏 🎒 🗳 📗	io 🖻 🚉 🕅	101-2 <b>644 64</b>	🕼 🏤 🏘 💧	→ 🕂 😓 🔿	🔄 🔤 🥪 📠 .	오 🛛 🕁 🖌 🕨 🛅 🔳 🖉
[mod1-1.dd] GCKtest.zip						
\DIR1						3+1=4 files, 0 dir.
Name 🗠	Ext.	Size Created	Mo	odified	Accessed At	tr. 1st sector
<u>.</u>						
?) ?ILE2		0.5 KB	09.	0/21/2000 13:49:34	A	42
FILE1		377 B	09.	0/21/2000 13:48:56	A	41
FILE3		379 B	09.	/21/2000 13:50:14	A	44
FILE4		211 B	09	/21/2000 13:50:52	A	45
[mod1-1.dd] 99% free	Offset	0 1 2 3	4 5 6	7 8 9 A	B C D E F	A A A A A A A A A A A A A A A A A A A
File system: FAT12	00005400	54 68 69 73	20 69 73 2	20 61 20 73	69 6D 70 6C 65	This is a simple 📄
Volume label: MOD1-1	00005410	20 74 65 78	74 20 66 6	69 6C 65 20	63 61 6C 6C 65	text file calle
Defects Edit Media	00005420	64 20 66 69	6C 65 20 3	32 2E 54 68	69 73 20 69 73	d file 2.This is
State: original	00005430	20 61 20 73	69 6D 70 6	5C 65 20 74	65 78 74 20 66	a simple text f
State. Original	00005440	59 50 55 20	63 61 60 6	50 55 54 20	55 59 50 55 20 20 72 40 45 70	The called file
Undo level: 0	00005450	60 65 20 74	67 73 20 6	27 66 69 60 27 73 20 61	20 73 89 8D 70	2.1HIS IS a SIMP le text file cal
Undo reverses: n/a	00005400	60 65 64 20	66 69 60 6	5 20 32 2E	05 28 85 81 80 0D 04 54 68 69	led file 2 Thi
Alloc, of visible drive space;	00005480	73 20 69 73	20 61 20 7	73 69 6D 70	6C 65 20 74 65	s is a simple te
Cluster No : 11	00005490	78 74 20 66	69 6C 65 2	20 63 61 6C	6C 65 64 20 66	xt file called f
211 F2 (deleted)	000054A0	69 6C 65 20	32 2E 54 6	68 69 73 20	69 73 20 61 20	ile 2.This is a
\DIR1\	000054B0	73 69 6D 70	6C 65 20 7	74 65 78 74	20 66 69 6C 65	simple text file
Separate taken 14 dave age	000054C0	20 63 61 6C	6C 65 64 2	20 66 69 6C	65 20 32 2E 54	called file 2.T
Shapahot taken ing daya ago	000054D0	68 69 73 20	69 73 20 6	61 20 73 69	6D 70 6C 65 20	his is a simple
Used space: 12.0 KB	000054E0	74 65 78 74	20 66 69 6	6C 65 20 63	61 6C 6C 65 64	text file called
12,288 bytes	000054F0	20 66 69 6C	65 20 32 2	2E UD UA 54	68 69 73 20 69	file 2This i
Free space: 1.4 MB	00005500	73 20 61 20	73 69 60 7	70 6C 65 20	74 65 78 74 20 20 66 60 60 60	s a simple text
1,445,376 bytes	00005510	20 32 25 54	48 69 73 2	20 60 63 64 20 69 73 20	20 00 07 00 05 61 20 73 69 6D	2 This is a sim
Total capacity: 1.4 MB	00005530	70 60 65 20	74 65 78 7	74 20 66 69	6C 65 20 63 61	ple text file ca
1.474.560 bytes	00005540	6C 6C 65 64	20 66 69 6	5C 65 20 32	2E OD OA 54 68	lled file 2 Th
	00005550	69 73 20 69	73 20 61 2	20 73 69 6D	70 6C 65 20 74	is is a simple t
Bytes per cluster: 512	00005560	65 78 74 20	66 69 6C 6	55 20 63 61	6C 6C 65 64 20	ext file called
Free clusters: 2,823	00005570	66 69 6C 65	20 32 2E 0	DD 0A 54 68	69 73 20 69 73	file 2This is
Total clusters: 2,847	00005580	20 61 20 73	69 6D 70 6	6C 65 20 74	65 78 74 20 66	a simple text f
Bytes per sector: 512	00005590	69 6C 65 20	63 61 6C 6	6C 65 64 20	66 69 6C 65 20	ile called file
Usable sectors: 2,847	000055A0	32 2E 54 68	69 73 20 6	69 73 20 61	20 73 69 6D 70	2.This is a simp
First data sector: 33	000055B0	6C 65 20 74	65 78 74 2	20 66 69 6C	65 20 63 61 6C	le text file cal
Display time zone:	000055C0	6C 65 64 20	66 69 6C 6	55 20 32 2E	OD 0A 54 68 69	led file 2Thi
Mode: bevadecimal	000055D0	73 20 69 73	20 61 20 7	73 69 6D 70	6C 65 20 74 65	s is a simple te
Character set: ANSLASCI	000055E0	78 74 20 66	69 6C 65 2	20 63 61 6C	6C 65 64 20 66	xt file called f
Offeete: hevadecimal	000055F0	69 6C 65 20	32 2E 54 6	69 73 20	69 73 20 61 20	ıle 2.This is a 💌
Sector 42 of 2880	Offset:	5400		= 84 Block:		n/a Size: n/a

Defining a block of data is relatively straight-forward. The screen shot above shows sector 42, which is byte offsets 0x5400-55FF. Note that the cursor is highlighting the first byte in the sector. There are at least three ways to define this block:

a. Note the starting and ending byte offsets. Use the Edit, Define Block... command, enter the beginning and end offset numbers, and click OK.

Define Block						
Beginning: 5400 < Beginning of bloc ♥ End: 55FFI < End of block ♥ In all open <u>f</u> iles						
<u>D</u> K C <u>a</u> ncel						

b. Position the cursor over the first byte in the block; then, either press alt-1 *or* right-click and select Beginning of block. Now, position the cursor over the last byte in the block, then either press alt-2 *or* right-click and select End of block.

Beginning of block	Alt+1
End of block	Alt+2
Edit	
Add Bookmark	

c. Select the block as you would text in a document; place the cursor over the first byte of the block, hold down the SHIFT key, drag the cursor to the last byte in the block, and then release the SHIFT key.

Regardless of the method, the block will display as highlighted, per the screen shot below.

WinHex - [[mod1-1.dd]]																15	.0		
Eile Edit Search Position	<u>V</u> iew <u>T</u> oo	ls Spec <u>i</u> ali	st Op	otions	Windo	w <u>H</u> e	lp											-	Ξ×
D 🛎 🖩 🎒 🖀 🗎 🖌	o 🖻 🛱	010 010	ĝą	HEX	В не	<b>4</b>	→	• - 🕑	<b>\</b>	▶	2	<b>b</b> ŵ		$\rho$	₫ 4	►	<b>(</b> )		<i>.</i>
[mod1-1.dd] GCKtest.zip																			
\DIR1																	3+1=4	4 files	, 0 dir.
Name 🗠	E	xt. Size	0	Created			Modifie	ed		Acc	essed		At	tr. 1:	st sector				
<u> </u>																·			
?) ?ILE2		0.	5 KB				09/21/	/2000	13:49:3	34			А	42	2				
FILE1		3	77 B				09/21/	2000	13:48:5	6			А	4	1				
FILE3		3	79 B				09/21/	2000	13:50:1	4			А	44	4				
FILE4		2	11 B				09/21/	2000	13:50:5	i2			А	45	5				
[mod1-1.dd] 99% free	Offset	0	1	2 3	4	5 e	7	8	9	A B	С	DE	F			~		^	
File system: FAT12	0000540	0 54	68 6	9 73	20 6	69 73	20	61	20 73	3 69	6D 7	0 60	65	This	is a	sim	ple		
Volume label: MOD1-1	0000541	0 20	746	5 78	74 3	20 66	69	6C	65 20	) 63	61 6	C 60	65	tex	t fil	e ca	lle		
	0000542	64	20 6	6 69	6C (	65 20	32	2E	54 6	3 69	73 2	0 69	73	d fi	le 2.	This	is		
Default Edit Mode	0000543	0 20	61 2	0 73	69 6	6D 70	1 6C	65	20 7	4 65	78 7	4 20	66	as	imple	tex	t f		
State: onginal	0000544	0 69	6C 6	5 20	63 6	61 6C	C 6C	65	64 21	0 66	69 6	C 65	20	ile	calle	d fi	le		
Undo level: 0	0000545	0 32	2E 5	4 68	69 3	73 20	1 69	73	20 6:	1 20	73 6	9 6E	70	2.Th	is is	as	imp		
Undo reverses: n/a	0000546	0 6C	65 2	0 74	65 3	/8 /4	20	66	69 60	5 65 7 00	20 6	3 61	6C	le t	ext f	ile i	cal		
Allee, of visible drive appear	0000547	0 50	65 6 20 7	4 20	20 1	59 BU 14 DC	, 65	20	32 ZI	5 UD	UA S	4 68	69	lea	IIIe	2	Ini		
Alloc, of visible drive space.	0000548	0 73	20 6 74 2	7 / 3 N 66	20 0	ST 20	20	67	61 60	J 60 7 60	65 2	0 74 4 20	65	S 15	ile e	mpie	te d f		
Cluster No.: 11	0000545	0 69	74 Z	5 20	32 1	2E 54	68	69	73 21	2 60 1 69	73 2	94 ZU	20	ile	2 Thi	ante e ie	-		
/ILE2 (deleted)	0000548	80 73	69 6	D 70	60 8	55 20	1 74	65	78 7	1 20	66 6	9 60	65	sime	le te	3 13 vt f	ile		
URIX	0000540	20	63 6	1 6C	6C (	65 64	20	66	69 60	C 65	20 3	2 28	54	cal	led f	ile	2.T		
Snapshot taken 14 days ago	000054E	0 68	69 7	3 20	69 3	73 20	61	20	73 6	9 6D	70 6	C 65	20	his	is a	simp	le		
Land appage 12.0 KP	000054E	0 74	65 7	8 74	20 6	66 69	6C	65	20 63	3 61	6C 6	C 65	64	text	file	cal	led		
12.0 Kb 12.0 Kb	000054F	0 20	66 6	9 6C	65 3	20 32	2E	0D	0A 5-	4 68	69 7	3 20	69	fil	е 2	.Thi	s i		
5	0000550	0 73	20 6	1 20	73 6	69 6I	) 70	6C	65 21	) 74	65 7	8 74	20	sа	simpl	e te	xt		
Free space: 1.4 MB	0000551	0 66	69 6	C 65	20 0	63 61	. 6C	6C	65 6	1 20	66 6	9 60	65	file	e call	ed f	ile		
1,440,576 Dytes	0000552	20	32 2	E 54	68 6	69 73	20	69	73 21	) 61	20 7	3 69	6D	2.T	his i	sa	sim		
Total capacity: 1.4 MB	0000553	0 70	6C 6	5 20	74 6	65 78	74	20	66 6	9 6C	65 2	0 63	61	ple	text	file	ca		
1,4/4,560 bytes	0000554	0 6C	6C 6	5 64	20 6	56 69	1 6C	65	20 33	2 2E	OD C	A 54	68	lled	l file	2	. Th		
Bytes per cluster: 512	0000555	0 69	73 2	0 69	73 2	20 61	20	73	69 61	2 70	6C 6	5 20	74	18 1	sas (1)	impl	e t		
Free clusters: 2.823	0000556	0 65	78 7 CO CI	4 20 C (F	55 1	о9 БС ра ав	, 65 , 0D	20	53 5.	L 60	50 E	5 64	20	ext	tile	call This	ed		
Total clusters: 2,847	0000557	0 00	07 0 41 0	0 72	20 .	52 28 SD 70	. 00	CE CE	24 0	0 07 1 65	70 7	0 07	66	TILE	; 2	Inis	15		
Butes per sector: 512	0000558	0 69	60 E	5 20	63 6	50 70 51 60	60	65	64 21	± 05 1 66	69.6	4 20 C 65	20	ile	calle	d fi	le		
Usable sectors: 2847	0000553	0 32	2E 5	4 68	69 1	73 20	1 69	73	20 6	1 20	73 6	9 60	20	2 Th	ie ie		imp		
First data sector: 33	000055F	30 6C	65 2	0 74	65 3	78 74	20	66	69 60	C 65	20 6	3 61	6C	le t	ext f	ile	cal		
	0000550	0 6C	65 6	4 20	66 6	69 6C	65	20	32 21	E OD	OA 5	4 68	69	led	file	2	Thi		
Display time zone: original	0000550	0 73	20 6	9 73	20 6	51 20	73	69	6D 7	) 6C	65 2	0 74	65	s is	asi	mple	te		
Mode: hexadecimal	000055E	0 78	74 2	0 66	69 6	6C 65	20	63	61 60	C 6C	65 6	4 20	66	xt f	ile c	alle	d f		
Offecte: ANSTASCII	000055F	0 69	6C 6	5 20	32 2	2E 54	68	69	73 20	) 69	73 2	0 61	20	ile	2.Thi	s is	a	¥	
Sector 42 of 2880	Offs	et:		55FF				= 32	Block				540	0 - 55FF	Size:				200

*Note: Press <ESC> to clear the block highlighting.* 

## Copy block to a file

Copying the block to a file is also relatively straight-forward. Use the Edit, Copy Block, Into New File command (control-shift-N) and provide a file name. The new file will open in WinHex.

🚟 WinHex - [file111.txt]						15.0 📃 🗖 🔀
Eile Edit Search Position	n <u>V</u> iew <u>T</u> ools S	Specialist Options	<u>W</u> indow <u>H</u> elp			_ 8 ×
🗅 📽 🗏 🎒 😭 🖉 🗌	io 🖻 🛱 🖿	1012 <b># #</b> HEX	S 💥 🖊	→⊕⇔⇒	/ 🔤 🖓 🎟 🖌	)   🔠 🖌 🕨 🛅 🗏 🧇
[mod1-1.dd] GCKtest.zip file1	11.txt					
file111.bxt	Offset	0 1 2 3	4 5 6	7 8 9 A	BCDEF	
C:\My Documents\Word\c3di\(	00000000	54 68 69 73	20 69 73 2	0 61 20 73	69 6D 70 6C 65	This is a simple
File size: 0.5 KB	00000010	20 74 65 78	74 20 66 6	9 6C 65 20 2 2E 54 68	63 61 6C 6C 65 69 73 20 69 73	text file calle d file 2 This is
512 bytes	00000030	20 61 20 73	69 6D 70 6	C 65 20 74	65 78 74 20 66	a simple text f
Default Edit Mode	00000040	69 6C 65 20	63 61 6C 6	C 65 64 20	66 69 6C 65 20	ile called file
State: original	00000050	32 2E 54 68 6C 65 20 74	65 78 74 2	9 73 20 61 0 66 69 6C	20 73 69 6D 70 65 20 63 61 6C	2.1his is a simp le text file cal
Undo level: 0	00000070	6C 65 64 20	66 69 6C 6	5 20 32 2E	OD OA 54 68 69	led file 2Thi
Undo reverses: n/a	00000080	73 20 69 73	20 61 20 7	3 69 6D 70	6C 65 20 74 65	s is a simple te
Creation time: 06/26/2008	00000090		69 6C 65 2	0 63 61 60	6C 65 64 20 66	xt file called f
21:08:40	000000B0	73 69 6D 70	6C 65 20 7	4 65 78 74	20 66 69 6C 65	simple text file
Last write time: 06/26/2008	00000000	20 63 61 6C	6C 65 64 2	0 66 69 6C	65 20 32 2E 54	called file 2.T
21:08:40	000000D0	68 69 73 20	69 73 20 6	1 20 73 69	6D 70 6C 65 20	his is a simple
Attributes: 21:08:40A	000000E0	20 66 69 6C	65 20 32 2	E OD OA 54	68 69 73 20 69	file 2This i
icons: U	00000100	73 20 61 20	73 69 6D 7	0 6C 65 20	74 65 78 74 20	s a simple text
Mode: hexadecimal	00000110	66 69 6C 65	20 63 61 6	C 6C 65 64	20 66 69 6C 65	file called file
Character set: ANSI ASCII Offsets: bevadecimal	00000120	20 32 2E 54	68 69 73 2 74 65 78 7	U 69732U 4206669	61 20 73 69 6D 6C 65 20 63 61	2.This is a sim ple text file ca
Bytes per page: 39x16=624	00000140	6C 6C 65 64	20 66 69 6	C 65 20 32	2E OD OA 54 68	lled file 2Th
Window #: 3	00000150	69 73 20 69	73 20 61 2	0 73 69 6D	70 6C 65 20 74	is is a simple t
No. of windows: 3	00000160	65 78 74 20	66 69 6C 6		6C 6C 65 64 20	ext file called
Clipboard: available	00000180	20 61 20 73	69 6D 70 6	C 65 20 74	65 78 74 20 66	a simple text f
TEMP folder: 33.8 GB free	00000190	69 6C 65 20	63 61 6C 6	C 65 64 20	66 69 6C 65 20	ile called file
UME~1\gck\LOCALS~1\Temp	000001A0	32 2E 54 68	69 73 20 6	9 73 20 61	20 73 69 6D 70	2. This is a simp
	000001E0	6C 65 64 20	66 69 6C 6	5 20 32 2E	OD OA 54 68 69	led file 2Thi
	000001D0	73 20 69 73	20 61 20 7	3 69 6D 70	6C 65 20 74 65	s is a simple te
	000001E0	78 74 20 66	69 6C 65 2	0 63 61 6C	6C 65 64 20 66	xt file called f
	00000160	69 6C 65 20	32 2E 54 6	8 69 73 20	69 /3 ZU 61 ZU	ile 2.1his is a
Page 1 of 1	Offset:		1	= 84 Block:		n/a Size: n/a

Export multiple blocks of data into a single file

Exporting multiple blocks of data into a single file is relatively simple but is a multi-step process.

🚟 WinHex - [[mod1-1.dd]]			15.0 📃 🗖 🔀
File Edit Search Position View Tools	Spec <u>i</u> alist <u>O</u> ptions <u>W</u> indow <u>H</u>	elp	_ & ×
BCIDAR MALOR BAR	1015 AA # AC & AA	$  \rightarrow \oplus (a \rightarrow b)   \rightarrow $	🖬 🔿   🖄 4 🕨 🖄 🗐   🤌
	010° birna Hex ∿¥B Héx birna	· • • • • • • • • • • • • • • • • • • •	
[mod1-1.dd] GCKtest.zip file111.txt			
\DIR1			3+1=4 files, 0 dir.
Name A Ext.	Size Created	Modified Accessed	Attr. 1st sector
🚞			
?) ?ILE2	0.5 KB	09/21/2000 13:49:34	A 42
FILE1	377 B	09/21/2000 13:48:56	A 41
FILE3	379 B	09/21/2000 13:50:14	A 44
FILE4	211 B	09/21/2000 13:50:52	A 45
[mod1-1.dd] 99% free Offset	0 1 2 3 4 5	6789ABCDE	F 🔽 🔯
File system: FAT12 00005A00	54 68 69 73 20 69 7	3 20 61 20 73 69 6D 70 6C	65 This is a simple 📄
Volume label: MOD1-1 00005A10	20 74 65 78 74 20 6	6 69 6C 65 20 63 61 6C 6C	65 text file calle
00005A20	64 20 66 69 6C 65 2	0 34 2E 0D 0A 20 20 20 20	20 d file 4
Default Edit Mode 00005A30	20 20 20 20 20 20 2	0 20 20 20 20 20 20 20 20 20	20
State: onginal 00005A40	20 20 20 20 20 20 2	0 20 20 20 20 20 20 20 20 20	20
Undo level: 0 00005A50	20 20 20 20 54 68 6	9 73 20 69 73 20 61 20 73	69 This is a si
Undo reverses: n/a 00005A60	6D 70 6C 65 20 74 6	5 78 74 20 66 69 6C 65 20	63 mple text file c
Alles of visible divergences	61 6C 6C 65 64 2U 6	6 69 6C 65 2U 34 2E UD UA	20 alled file 4
Alloc. of Visible drive space: 00005A80	20 20 20 20 20 20 20 2		20
Cluster No.: 14 00005A90			20 20 This is
FILE4 00005AA0	20 20 20 20 20 20 20 2	0 20 34 66 67 73 20 67 73 C 25 30 74 25 76 74 30 22	20 Inis is
\DIR1\ 00005AC0	6C 65 20 63 61 6C 6		34 le called file 4
Snapshot taken 14 days ago 00005AD0			
00005AE0			00
Used space: 12.0 KB 00005AF0			00
12,288 bytes 00005B00	00 00 00 00 00 00 0		00
Free space: 1.4 MB 00005B10	00 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00	00
1,445,376 bytes 00005B20	00 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00	00
Total capacity: 1.4 MB 00005B30	00 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00	00
1,474,560 bytes 00005B40	00 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00	00
00005B50	00 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00	00
Bytes per cluster: 512 00005B60	00 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00	00
Total clusters: 2,623 00005B70	00 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00	00
00005880			00
Bytes per sector: 512 00005B90			00
Eirst data sector: 2,04/ 00005BAU			00
00005BB0			00
Display time zone: original			00
Mode: hexadecimal 00005BE0			00
Character set: ANSI ASCII 00005BE0			00
Sector 45 of 2880	54D2	= 10 Block:	5400 - 54D2 Size: D3

The first step is to define and export the first block into a file as described above. Suppose we now wanted to append bytes 0x5A00-5AD2 to the file created in the last step. Start by defining the new block using one of the three methods described above.

Next, copy the block into the clipboard using the Edit, Copy Block, Normally command (^C).

WinHex - [file111.txt]					15.0 🔲 🗖 🔀
🚟 File Edit Search Position	n <u>V</u> iew <u>T</u> ools	Spec <u>i</u> alist <u>O</u> ptions	<u>W</u> indow <u>H</u> elp		_ 8 ×
D 🗃 🗐 🎒 🔛 🖕 🗌	60 🖹 🛱 🕅	1010 M HEX	🕼 💒 🏘   → 🕀	😓 🔿   🖄 🐂 🧼 🎟	🔎   🔠 🖡 🕨 🖄 🌾
[mod1-1.dd] GCKtest.zip file1	11.txt				
file111 tyt	Offset	0 1 2 3	4 5 6 7 8	9 A B C D E F	
C:\My Documents\Word\c3di\(	00000000	54 68 69 73	20 69 73 20 61	20 73 69 6D 70 6C 65	This is a simple
Electre: 0.5 KD	00000010	20 74 65 78	74 20 66 69 6C	65 20 63 61 6C 6C 65	text file calle
512 bytes	00000020	20 61 20 73	60 65 20 32 2E	20 74 65 78 74 20 66	a file 2.1nis is a simple text f
	00000040	69 6C 65 20	63 61 6C 6C 65	64 20 66 69 6C 65 20	ile called file
Default Edit Mode State: original	00000050	32 2E 54 68	69 73 20 69 73	20 61 20 73 69 6D 70	2.This is a simp
Unde level: 0	00000060	6C 65 20 74		69 6C 65 2U 63 61 6C	le text file cal
Undo reverses: n/a	00000080	73 20 69 73	20 61 20 73 69	6D 70 6C 65 20 74 65	s is a simple te
o	00000090	78 74 20 66	69 6C 65 20 63	61 6C 6C 65 64 20 66	xt file called f
Creation time: 06/26/2008 21:08:40	00000040	69 6C 65 20	32 2E 54 68 69	73 20 69 73 20 61 20	ile 2.This is a
Last write time: 06/26/2008	00000080	20 63 61 6C	6C 65 64 20 66	78 74 20 66 69 60 65 69 60 65 20 32 2E 54	simple text file called file 2 T
21:08:40	000000D0	68 69 73 20	69 73 20 61 20	73 69 6D 70 6C 65 20	his is a simple
Attributes: 21:08:40A	000000E0	74 65 78 74	20 66 69 6C 65	20 63 61 6C 6C 65 64	text file called
Icons: 0	000000F0	20 66 69 6C	65 20 32 2E 0D	OA 54 68 69 73 20 69	file 2This i
Mode: bevadecimal	00000110	66 69 6C 65	20 63 61 6C 6C	65 64 20 66 69 6C 65	file called file
Character set: ANSI ASCII	00000120	20 32 2E 54	68 69 73 20 69	73 20 61 20 73 69 6D	2.This is a sim
Offsets: hexadecimal	00000130	70 6C 65 20	74 65 78 74 20	66 69 6C 65 20 63 61	ple text file ca
bytes per page: 35X16=624	00000140	69 73 20 69	20 66 69 60 65	20 32 2E UD UA 54 68 69 6D 70 6C 65 20 74	lled file 2lh is is a simple f
Window #: 3 No. of windows: 3	00000160	65 78 74 20	66 69 6C 65 20	63 61 6C 6C 65 64 20	ext file called
	00000170	66 69 6C 65	20 32 2E 0D 0A	54 68 69 73 20 69 73	file 2This is
Clipboard: available	00000180		69 6D 70 6C 65	20 74 65 78 74 20 66	a simple text f
TEMP folder: 33.8 GB free	00000130	32 2E 54 68	69 73 20 69 73	20 61 20 73 69 6D 70	2. This is a simp
UME TYCK/LUCALS TYTEMP	000001B0	6C 65 20 74	65 78 74 20 66	69 6C 65 20 63 61 6C	le text file cal
	000001C0	6C 65 64 20	66 69 6C 65 20	32 2E OD OA 54 68 69	led file 2Thi
	00000100	73 20 69 73	20 61 20 73 69 69 6C 65 20 63	6D 70 6C 65 20 74 65 61 6C 6C 65 64 20 66	s is a simple te xt file called f
	000001F0	69 6C 65 20	32 2E 54 68 69	73 20 69 73 20 61 20	ile 2. This is a
Page 1 of 1	Offset:	1FF	= 32	Block:	n/a Size: n/a

Finally, click on the tab corresponding to the file where the data is to be added, click on the last byte of the file, and then use the Edit, Clipboard Data, Paste command ( $^V$ ). Since we want the data at the end of the block, click YES when the dialogue box above appears.

WinHex	
2	Do you want the clipboard data to be pasted at the end of the file (after offset 1FF)?
	Yes No

🚟 WinHex - [file111.txt]					15.0 🔳 🗖 🗙
🚟 Eile Edit Search Position	n <u>V</u> iew <u>T</u> ools	Specialist Options	<u>W</u> indow <u>H</u> elp		_ 8 ×
D 🖻 🖥 🎒 🖆 📗	🗤 🖻 💼 🕅	101- 010 MA HEX	않 🔣 🏘 📋 -	→ 🕂 😓 👌 🕴 🏖 🖶 🧼 🎟 🗴	) 🛛 🖓 🖌 🕨 🖄 🖉
[mod1-1.dd] GCKtest.zip file1	11.bt				
0-111+4	Offset	0 1 2	3 4 5 6 7	89ABCDEF	
C:\My Documents\Word\c3di\(	00000090	78 74 20 6	69 6C 65 20	63 61 6C 6C 65 64 20 66	xt file called f
	000000A0	69 6C 65 2	) 32 2E 54 68	69 73 20 69 73 20 61 20	ile 2.This is a
File size: 0.7 KB	000000B0	73 69 6D 7	) 6C 65 20 7 <b>4</b>	65 78 74 20 66 69 6C 65	simple text file
723 bytes	000000000	20 63 61 6	C 6C 65 64 20	66 69 6C 65 20 32 2E 54	called file 2.T
Default Edit Mode	000000D0	68 69 73 2	0 69 73 20 61	20 73 69 6D 70 6C 65 20	his is a simple
State: modified	000000E0	74 65 78 7	1 20 66 69 6C	65 20 63 61 6C 6C 65 64	text file called
Linda laval: 1	000000000000000000000000000000000000000	20 66 69 6	, 65 20 32 2E 1 72 69 60 70	UD UA 54 68 69 73 20 69	file 2lhis i
Undo reverses: data pasting	00000100	66 69 60 6	, /3 67 60 /0 5 20 63 61 60		s a simple text file called file
ondo roveraca. data pasting	00000110	20 32 28 5	1 68 69 73 20	69 73 20 61 20 73 69 6D	2 This is a sim
Creation time: 06/26/2008	00000130	70 60 65 2	00 05 70 20	20 66 69 60 65 20 63 61	nle text file ca
21:08:40	00000140	6C 6C 65 6	20 66 69 6C	65 20 32 2E 0D 0A 54 68	lled file 2Th
Last write time: 06/26/2008	00000150	69 73 20 6	73 20 61 20	73 69 6D 70 6C 65 20 74	is is a simple t
21:08:40	00000160	65 78 74 2	) 66 69 6C 65	20 63 61 6C 6C 65 64 20	ext file called
Attributes: 21:08:40A	00000170	66 69 6C 6	5 20 32 2E OD	OA 54 68 69 73 20 69 73	file 2This is
Icons: 0	00000180	20 61 20 7	8 69 6D 70 6C	65 20 74 65 78 74 20 66	a simple text f
	00000190	69 6C 65 2	) 63 61 6C 6C	65 64 20 66 69 6C 65 20	ile called file
Mode: hexadecimal	000001A0	32 2E 54 6	3 69 73 20 69	73 20 61 20 73 69 6D 70	2.This is a simp
Character set: ANSI ASCII	000001B0	6C 65 20 7	65 78 74 20	66 69 6C 65 20 63 61 6C	le text file cal
Offsets: hexadecimal	000001C0	6C 65 64 2	1 66 69 6C 65	20 32 2E UD UA 54 68 69	led file 2Thi
bytes per page. 33x16=624	00000100	73 20 69 7	3 ZU 61 ZU 73		s is a simple te
Window #: 3	000001E0	69 60 65 2	) 07 00 03 20 ) 33 35 54 60		ile 2 This is a
No. of windows: 3	00000120	54 68 69 7	20 69 73 20	61 20 73 69 6D 70 6C 65	The 2.100 is a
Clipboard: 211 B	00000210	20 74 65 7	3 74 20 66 69	6C 65 20 63 61 6C 6C 65	text file calle
	00000220	64 20 66 6	6C 65 20 34	2E OD OA 20 20 20 20 20	d file 4
IEMP folder: 33.8 GB free	00000230	20 20 20 2	20 20 20 20 20	20 20 20 20 20 20 20 20 20	
OME TYPER LOCALS TYTEMP	00000240	20 20 20 2	20 20 20 20	20 20 20 20 20 20 20 20 20	
	00000250	20 20 20 2	54 68 69 73	20 69 73 20 61 20 73 69	This is a si
	00000260	6D 70 6C 6	5 20 74 65 78	74 20 66 69 6C 65 20 63	mple text file c
	00000270	61 6C 6C 6	5 64 20 66 69	6C 65 20 34 2E 0D 0A 20	alled file 4
	00000280	20 20 20 2	0 20 20 20 20	20 20 20 20 20 20 20 20 20	
	00000290	20 20 20 2	0 20 20 20 20	20 20 20 20 20 20 20 20 20	
	000002A0	20 20 20 2	20 20 20 20 20 0 CD 20 CC 25	54 68 69 73 20 69 73 20	This is
	00000280	61 20 73 6			a simple text fi
	00000200	212 010 04	0 01 00 00 05	04 20 00 07 00 05 20 34	re carled file 4
	000002D0	ZE OD OA			
Page 1 of 2	Offset:	1	F	= 32 Block: 20	0-2D2 Size: D3

Additional blocks can be added by following these same steps. Be sure to save the updated file; data added to the file that has *not* yet been saved will be displayed in **blue**.

Note: This same method will work to paste the second block anywhere in the file.

## Exporting a file list

The directory browser feature of WinHex is a great way to navigate around the medium or image file. Copying the directory browser information provides a nice way to build a list of all of the files found in the image. The only bad part is that WinHex only allows you to grab one directory at a time, namely the one that is displayed; thus, if you want to get multiple directories, it is a multi-step process.

Suppose you want to get a complete directory listing of an image with to create an Excel spreadsheet listing all files and their attributes. The following steps will accomplish this:

Navigate to the root directory and highlight the entire directory browser section. Right-click and select Export list...

Recover/Copy Export list	
Simultaneous Search	ı
Hide	•
Position	•
Open	

When the dialogue box opens, be sure to select Unicode (you may have to first unselect HTML). Use this opportunity to highlight the fields that you want to save.

Export list	×
Fields to output:	Name Description Ext.  Path  Size Created Modified Accessed Record update Deletion
☐ <u>H</u> TML ✔ Unicode	Attr. Links 1st sector ID Int. ID Int. parent  Hash 
<u><u> </u></u>	Cancel

After clicking OK, you need to provide a file name.

Continue navigating to the subdirectories on the medium and repeat these steps. Be sure that you select unique file names when you save subsequent files.

To create the file list in an Excel spreadsheet, do the following:

Open the first export file from Excel. Since it is a text file, you will see the Text Import Wizard dialog box; click on FINISH to open the file.

Open the second file just as you did the first file. Copy the contents of the second file and paste into the first. Repeat for the remaining files; open, copy the contents, and paste into the first file. After this somewhat tedious process, you will have a spreadsheet with the complete file list. Add additional comments, as desired.

Wigrosoft Event ESEvenet mod 1 via												ſ	
[변] Elle Edit View Insert Format Tools Data Window Help Adobe PDF Type a question for help 🚽 🗗 🗡										- 8 ×			
ED 😂 🗆 D. LAI D. 199 (B. L. D. (B 201 (C	- 5	4	85%	- 6	· • :	Arial	• 10	- B		-8-	<b>*.0</b>	.00   3> -	A - 1
		- 2									.00	⇒.0   <u>~~</u> .	
🗄 🖕 SnagIt 🔠   Window 🚽 🗧 🛅 🛄 🖄 🖄 🖉 🥸 🖄   🌫 🏷   🖉 🔩 🕼   🖤 Reply with Changes End Review 🗧 🗄 📆 🖏 💂													
A B	C	D	F	F	G	н		1	к		м	N	0 -
1 Name Description	Ext.	Type	Evidence object	Path	Size	Created	Modified	Accessed	Deletion	Attr.	Links	1st sector	Comme ^
2 (Root directory) root directory					7.0 KB							19	
3 DIR1 existing directory				١	0.5 KB		09/21/2000 13:50					38	
4 DIR2 existing directory				١	0.5 KB		09/21/2000 13:51					39	
5 DIR3 existing directory				١	0.5 KB		09/21/2000 13:51					40	
6 DIR4 existing directory				۱	0.5 KB		09/21/2000 13:51					56	
7 ?ILE1 previously ex. file, contents may have changed				۱	377 B		09/21/2000 13:48			Α		33	
8 FILE2 existing file				۱	0.5 KB		09/21/2000 13:49			Α		34	
9 FILE3 existing file			1	۱	379 B		09/21/2000 13:50			Α		36	
10 FILE4 existing file			1	۱	211 B		09/21/2000 13:50			A		37	
11 Boot sector virtual file listed for examination purposes				۱	0.5 KB							0	
12 FAT 1 virtual file listed for examination purposes				۱	4.5 KB							1	
13 FAT 2 virtual file listed for examination purposes				۱	4.5 KB							10	
14 Free space virtual file listed for examination purposes				۱	1.4 MB								
15 Idle space virtual file listed for examination purposes			1	۱									
16 ?ILE2 previously ex. file, contents may have changed			1	\DIR1	0.5 KB		09/21/2000 13:49			A		42	
17 FILE1 existing file			1	\DIR1	377 B		09/21/2000 13:48			A		41	
18 FILE3 existing file				\DIR1	379 B		09/21/2000 13:50			A		44	
19 FILE4 existing file				\DIR1	211 B		09/21/2000 13:50			A		45	
20 ?ILE3 previously ex. file, contents may have changed				DIR2	379 B		09/21/2000 13:50			A		49	
21 FILE1 existing file				DIR2	377 B		09/21/2000 13:48			A		46	
22 FILE2 existing file				DIR2	0.5 KB		09/21/2000 13:49			A		47	
23 FILE4 existing file				VDIR2	211 B		09/21/2000 13:50			A		50	
24 PLE1 previously ex. file, contents may have changed				UIR3	3// 8		09/21/2000 13:48			A		51	
25 FILE2 existing file	_			UIR3	0.5 KB		09/21/2000 13:49			A		52	
20 FILES existing file				DIRG	3/9 0		09/21/2000 13:50			A		54	
22 FILE4 existing file					2110		09/21/2000 13:50			A .		50	
20 FILE1 existing file	-				0.5 KP		09/21/2000 13:40			~		57	
30 FILE3 existing file	-	-			379 B		09/21/2000 13:50			2		00	
31 FILE4 existing file					211 B	-	09/21/2000 13:50			Δ		61	
32 okieting no				Dirich H	2.110		00/21/2000 10:00			^		01	~
If ← → Pi FSExport mod1-1													
Ready													