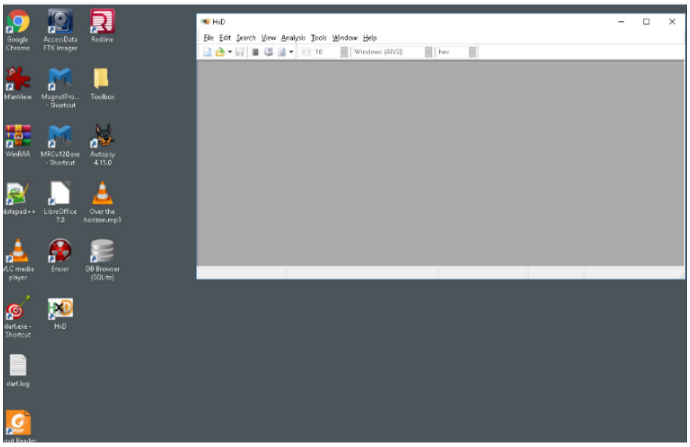
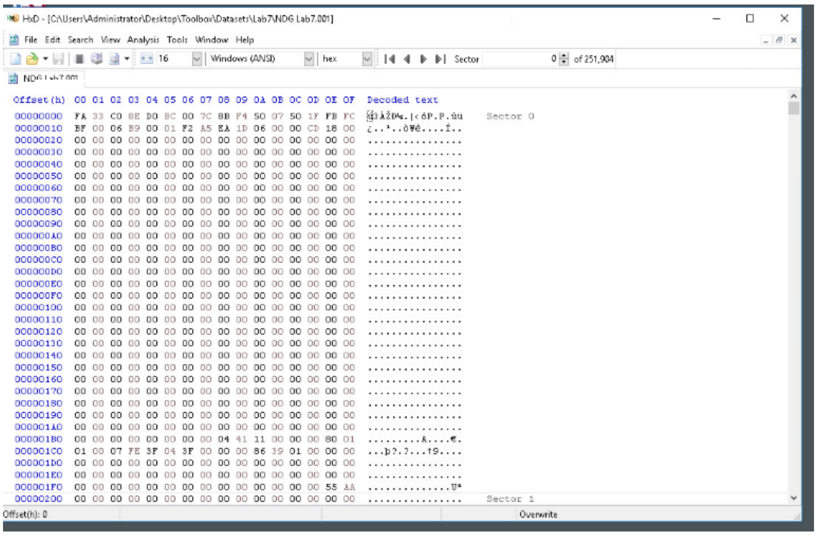
Lab 7 – Data Carving

Objectives

- How to identify files using signatures
- How to manually carve files using a hex editor
- How to use an automated tool to perform data carving



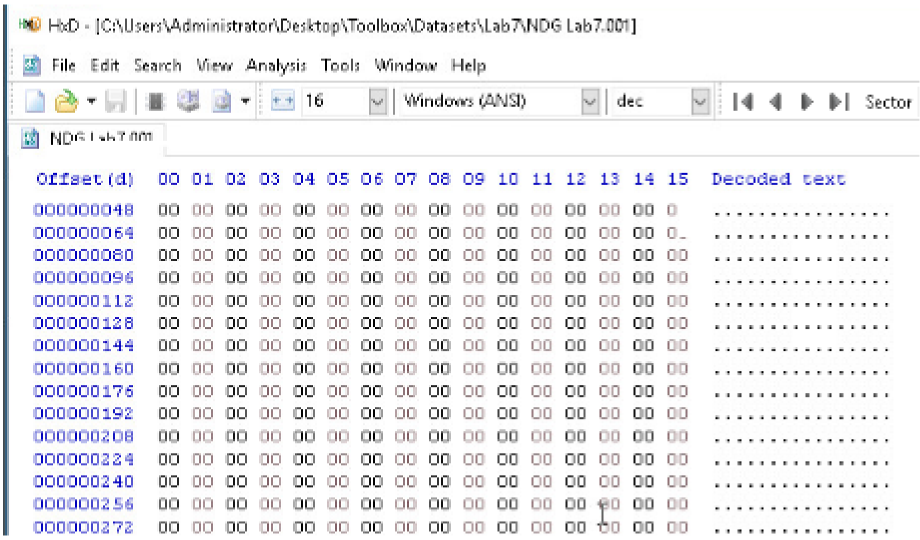
Opening a disk image


HxD - [C:\Users\Administrator\Desktop\Toolbox\Datasets\Lab7\NDG Lab7.001]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
Sector
0
of 251,904
NDG Lab7.001

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  FA 33 C0 8E D0 BC 00 7C 8B F4 50 07 50 1F FB FC  ú3ÀŽÐ¼.|‹ôP.P.ûü     Sector 0
00000010  BF 00 06 B9 00 01 F2 A5 EA 1D 06 00 00 CD 18 00  ¿..¹..ò¥ê....Í..
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001B0  00 00 00 00 00 00 00 00 04 41 11 00 00 00 80 01  .........A....€.
000001C0  01 00 07 FE 3F 04 3F 00 00 00 86 39 01 00 00 00  ...þ?.?...†9....
000001D0  00 00 00 00 00 00 00 00 00 00 00 00 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  ..............Uª
00000200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................     Sector 1
Offset(h): 0                                          Overwrite
```

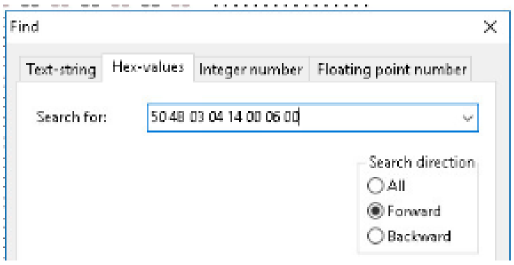
File Extension	Hexadecimal file header	Raw text translation	Hexadecimal file footer	Raw text translation
DOCX, XLSX, PPTX	50 4B 03 04 14 00 06 00	PK......	50 4B 05 06 (PK..) followed by 18 additional Bytes	PK......
PDF	25 50 44 46	%PDF	0A 25 25 45 4F 46 0A 25 25 45 4F 46 0A 0D 0A 25 25 45 4F 46 0D 0A 0D 25 25 45 4F 46 0D *NOTE:* There may be multiple footers so be sure to get the last one.	.%%EOF .%%EOF. ..%%EOF.. .%%EOF.
JPEG	FF D8 FF E0	ÿØÿà	FF D9	ÿÙ

Using data from table to search for and carve each file. We limit file offsets, setting this to decimal.


HxD - [C:\Users\Administrator\Desktop\Toolbox\Datasets\Lab7\NDG Lab7.001]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
dec
Sector
NDG Lab7.001

```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text
000000048  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0   ................
000000064  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0_  ................
000000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000096  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000112  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000128  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000144  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000176  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000192  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000208  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000224  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000240  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000256  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000272  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

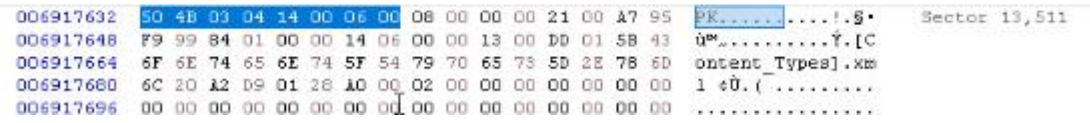
Carving XLSX Files



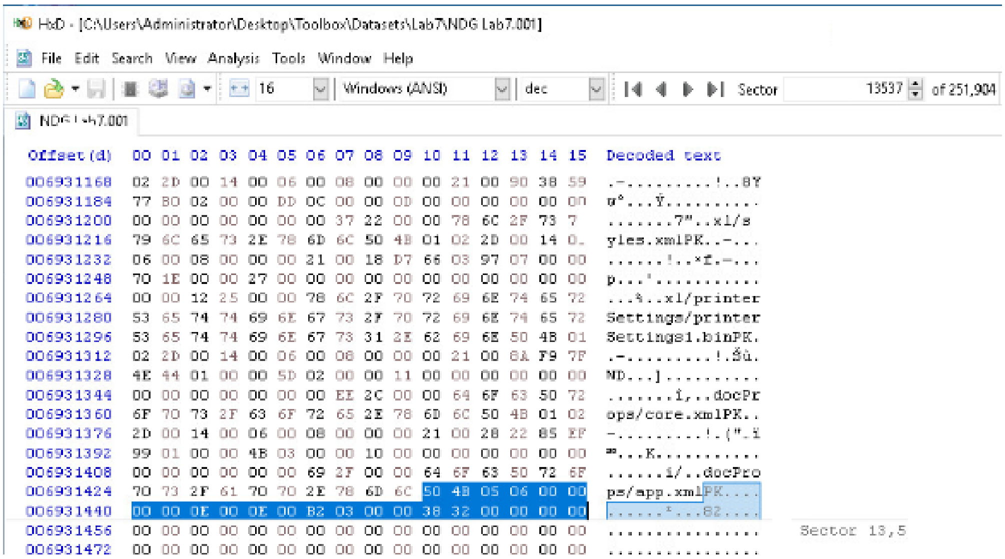
Search for: 50 4B 03 04 14 00 06 00

Search for the XLSX file signature. To do this, type 50 4B 03 04 14 00 06 00 in the search field highlighted as item

Offset noted FEF



```
006917632  50 4B 03 04 14 00 06 00 08 00 00 00 21 00 A7 95  PK..........!.§•    Sector 13,511
006917648  F9 99 84 01 00 00 14 06 00 00 13 00 DD 01 5B 43  ù™„.........Ý.[C
006917664  6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D  ontent_Types].xm
006917680  6C 20 A2 D9 01 28 A0 00 02 00 00 00 00 00 00 00  l ¢Ù.( .........
006917696  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```



HxD - [C:\Users\Administrator\Desktop\Toolbox\Datasets\Lab7\NDG Lab7.001]

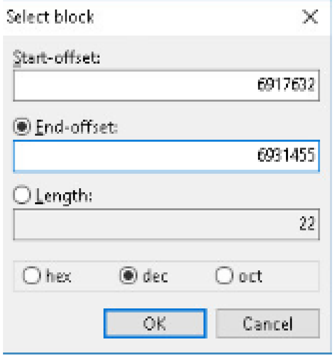
16 | Windows (ANSI) | dec | Sector 13537 of 251,904

NDG Lab7.001

```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text

006931168  02 2D 00 14 00 06 00 08 00 00 00 21 00 90 38 59  .-.........!..8Y
006931184  77 B0 02 00 00 DD 0C 00 00 0D 00 00 00 00 00 00  w°...Ý..........
006931200  00 00 00 00 00 00 00 37 22 00 00 78 6C 2F 73 7   .......7"..xl/s
006931216  79 6C 65 73 2E 78 6D 6C 50 4B 01 02 2D 00 14 0.  yles.xmlPK..-...
006931232  06 00 08 00 00 00 21 00 18 D7 66 03 97 07 00 00  ......!..×f.—...
006931248  70 1E 00 00 27 00 00 00 00 00 00 00 00 00 00 00  p...'...........
006931264  00 00 12 25 00 00 78 6C 2F 70 72 69 6E 74 65 72  ...%..xl/printer
006931280  53 65 74 74 69 6E 67 73 2F 70 72 69 6E 74 65 72  Settings/printer
006931296  53 65 74 74 69 6E 67 73 31 2E 62 69 6E 50 4B 01  Settings1.binPK.
006931312  02 2D 00 14 00 06 00 08 00 00 00 21 00 8A F9 7F  .-.........!.Šù.
006931328  4E 44 01 00 00 5D 02 00 00 11 00 00 00 00 00 00  ND...]..........
006931344  00 00 00 00 00 00 00 EE 2C 00 00 64 6F 63 50 72  .......î,..docPr
006931360  6F 70 73 2F 63 6F 72 65 2E 78 6D 6C 50 4B 01 02  ops/core.xmlPK..
006931376  2D 00 14 00 06 00 08 00 00 00 21 00 28 22 85 EF  -.........!.("…ï
006931392  99 01 00 00 4B 03 00 00 10 00 00 00 00 00 00 00  ™...K...........
006931408  00 00 00 00 00 00 69 2F 00 00 64 6F 63 50 72 6F  ......i/..docPro
006931424  70 73 2F 61 70 70 2E 78 6D 6C 50 4B 05 06 00 00  ps/app.xmlPK....
006931440  00 00 0E 00 0E 00 B2 03 00 00 38 32 00 00 00 00  ......²...82....
006931456  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................    Sector 13,5
006931472  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Using offset block



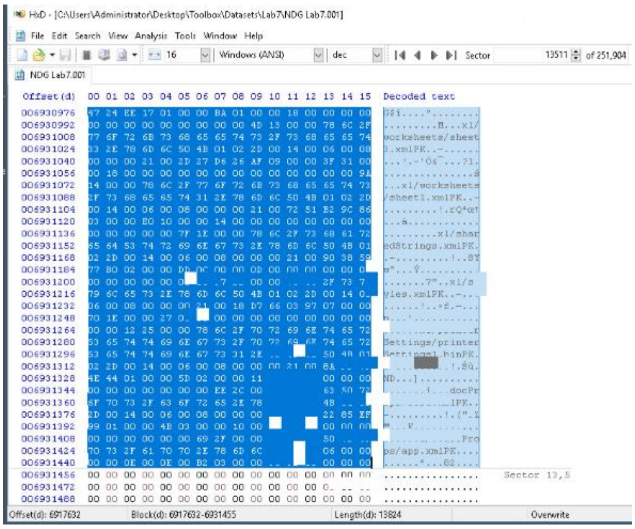
Select block

Start-offset: 6917632

● End-offset: 6931455

○ Length: 22

○ hex ● dec ○ oct



HxD - [C:\Users\Administrator\Desktop\Toolbox\Datasets\Lab7\NDG Lab7.001]

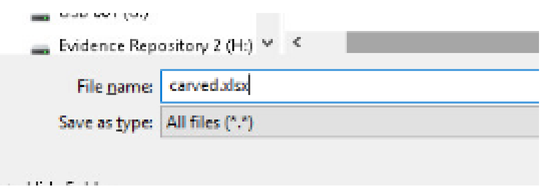
16 | Windows (ANSI) | dec | Sector 13511 of 251,904

NDG Lab7.001

```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text
006930976  47 24 EE 17 01 00 00 BA 01 00 00 18 00 00 00 00  G$î....º........
006930992  00 00 00 00 00 00 00 00 00 4D 13 00 00 78 6C 2F  .........M...xl/
006931008  77 6F 72 6B 73 68 65 65 74 73 2F 73 68 65 65 74  worksheets/sheet
006931024  33 2E 78 6D 6C 50 4B 01 02 2D 00 14 00 06 00 08  3.xmlPK..-......
006931040  00 00 00 21 00 2D 27 D6 26 AF 09 00 00 3F 31 00  ...!.-'Ö&¯...?1.
006931056  00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 9A  ...............š
006931072  14 00 00 78 6C 2F 77 6F 72 6B 73 68 65 65 74 73  ...xl/worksheets
006931088  2F 73 68 65 65 74 31 2E 78 6D 6C 50 4B 01 02 2D  /sheet1.xmlPK..-
006931104  00 14 00 06 00 08 00 00 00 21 00 72 51 B2 9C 86  .........!.rQ²œ†
006931120  03 00 00 E0 10 00 00 14 00 00 00 00 00 00 00 00  ...à............
006931136  00 00 00 00 00 7F 1E 00 00 78 6C 2F 73 68 61 72  .........xl/shar
006931152  65 64 53 74 72 69 6E 67 73 2E 78 6D 6C 50 4B 01  edStrings.xmlPK.
006931168  02 2D 00 14 00 06 00 08 00 00 00 21 00 90 38 59  .-.........!..8Y
006931184  77 B0 02 00 00 DD 0C 00 00 0D 00 00 00 00 00 0.  w°...Ý..........
006931200  00 00 00 00 00 0. .. .7 .. 00 00 .. .. 2F 73 7   .......7"..xl/s
006931216  79 6C 65 73 2E 78 6D 6C 50 4B 01 02 2D 00 14 0.  yles.xmlPK..-...
006931232  06 00 08 00 00 00 21 00 18 D7 66 03 97 07 00 00  ......!..×f.—...
006931248  70 1E 00 00 27 0.    00 00 00 00 00 00 00 00 00  p...'...........
006931264  00 00 12 25 00 00 78 6C 2F 70 72 69 6E 74 65 72  ...............r
006931280  53 65 74 74 69 6E 67 73 2F 70 72 69 6E 74 65 72  Settings/printer
006931296  53 65 74 74 69 6E 67 73 31 2E ..    .. 50 4B 01  Settings1.binPK.
006931312  02 2D 00 14 00 06 00 08 00 00 00 21 00 8A .. ..  .......!.Šù.
006931328  4E 44 01 00 00 5D 02 00 00 11          00 00 00  ND...]..........
006931344  00 00 00 00 00 00 00 EE 2C 00          63 50 72  .......î...docPr
006931360  6F 70 73 2F 63 6F 72 65 2E 78          4B .. ..  ..........lPK..
006931376  2D 00 14 00 06 00 08 00 00 00          22 85 EF  -.........!.("…ï
006931392  99 01 00 00 4B 03 00 00 10 00          00 00 00  ™...K...........
006931408  00 00 00 00 00 00 69 2F 00 00          50 .. ..  ..............Pro
006931424  70 73 2F 61 70 70 2E 78 6D 6C          06 00 00  ps/app.xmlPK....
006931440  00 00 0E 00 0E 00 B2 03 00 00 .. ..    00 00 00  ......²...82....
006931456  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................    Sector 13,5
006931472  00 00 00 00 00 00 00 00 00 00 00 00 00 0. .. ..  ................
006931488  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Offset(d): 6917632   Block(d): 6917632-6931455   Length(d): 13824   Overwrite

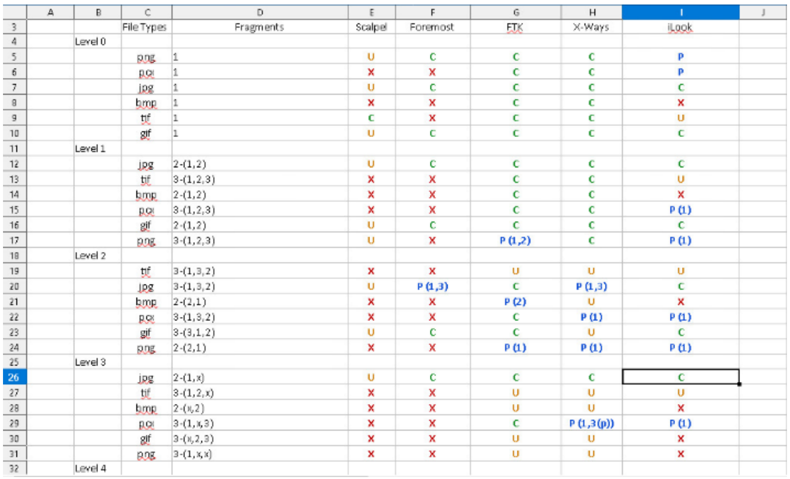
Saving and opening the carved file



Evidence Repository 2 (H:)

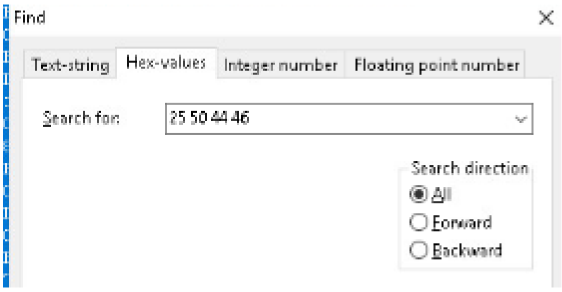
File name: carved.xlsx

Save as type: All files (*.*)



	A	B	C	D	E	F	G	H	I	J
3			File Types	Fragments	Scalpel	Foremost	FTK	X-Ways	iLook	
4		Level 0								
5			png	1	U	C	C	C	P	
6			pcx	1	X	X	C	C	P	
7			jpg	1	U	C	C	C	C	
8			bmp	1	X	X	C	C	X	
9			tif	1	C	X	C	C	U	
10			gif	1	U	C	C	C	C	
11		Level 1								
12			jpg	2-(1,2)	U	C	C	C	C	
13			tif	3-(1,2,3)	X	X	C	C	U	
14			bmp	2-(1,2)	X	X	C	C	X	
15			pcx	3-(1,2,3)	X	X	C	C	P (1)	
16			gif	2-(1,2)	U	C	C	C	C	
17			png	3-(1,2,3)	U	X	P (1,2)	C	P (1)	
18		Level 2								
19			tif	3-(1,3,2)	X	X	U	U	U	
20			jpg	3-(1,3,2)	U	P (1,3)	C	P (1,3)	C	
21			bmp	2-(2,1)	X	X	P (2)	U	X	
22			pcx	3-(1,3,2)	X	X	C	P (1)	P (1)	
23			gif	3-(3,1,2)	U	C	C	U	C	
24			png	2-(2,1)	X	X	P (1)	P (1)	P (1)	
25		Level 3								
26			jpg	2-(1,x)	U	C	C	C	C	
27			tif	3-(1,2,x)	X	X	U	U	U	
28			bmp	2-(x,2)	X	X	U	U	X	
29			pcx	3-(1,x,3)	X	X	C	P (1,3(p))	P (1)	
30			gif	3-(x,2,3)	X	X	U	U	X	
31			png	3-(1,x,x)	X	X	U	U	X	
32		Level 4								

Carving PDF files

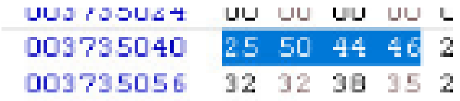


Search for: 25 50 44 46

File signature for PDF files

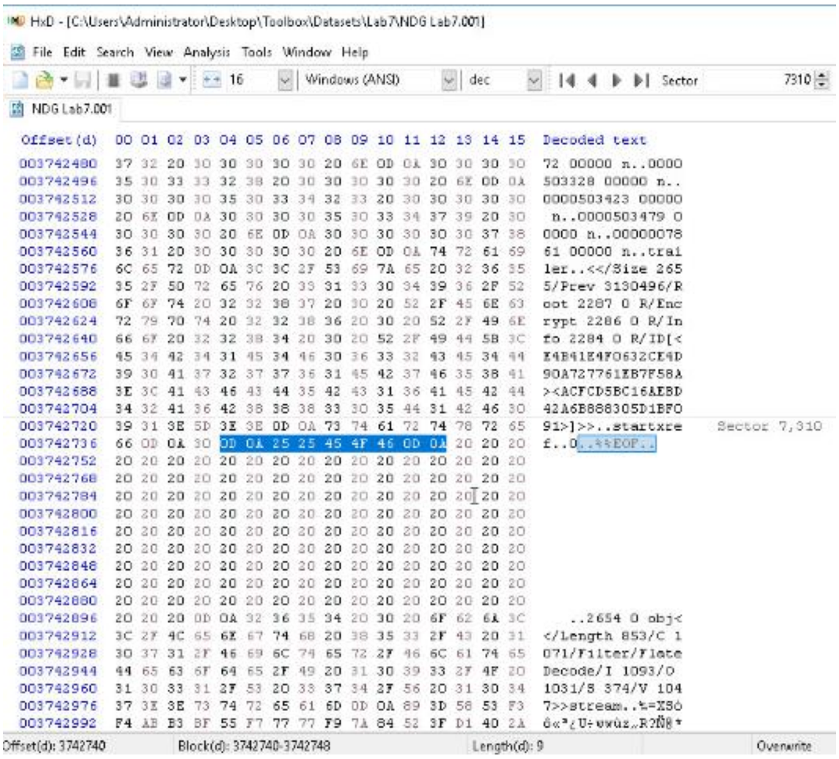
20 50 44 46

Below noted is the offset



```
003735024  00  00  00  00  0
003735040  25  50  44  46  2
003735056  32  32  38  35  2
```

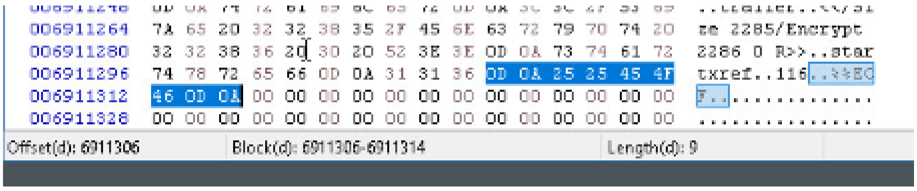
Searching for all the zeros to find the end of file


HxD - [C:\Users\Administrator\Desktop\Toolbox\Datasets\Lab7\NDG Lab7.001]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
dec
Sector
7310
NDG Lab7.001

```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text
003742480  37 32 20 30 30 30 30 30 20 6E 0D 0A 30 30 30 30  72 00000 n..0000
003742496  35 30 33 33 32 38 20 30 30 30 30 30 20 6E 0D 0A  503328 00000 n..
003742512  30 30 30 30 35 30 33 34 32 33 20 30 30 30 30 30  0000503423 00000
003742528  20 6E 0D 0A 30 30 30 30 35 30 33 34 37 39 20 30   n..0000503479 0
003742544  30 30 30 30 20 6E 0D 0A 30 30 30 30 30 30 37 38  0000 n..00000078
003742560  36 31 20 30 30 30 30 30 20 6E 0D 0A 74 72 61 69  61 00000 n..trai
003742576  6C 65 72 0D 0A 3C 3C 2F 53 69 7A 65 20 32 36 35  ler..<</Size 265
003742592  35 2F 50 72 65 76 20 33 31 33 30 34 39 36 2F 52  5/Prev 3130496/R
003742608  6F 6F 74 20 32 32 38 37 20 30 20 52 2F 45 6E 63  oot 2287 0 R/Enc
003742624  72 79 70 74 20 32 32 38 36 20 30 20 52 2F 49 6E  rypt 2286 0 R/In
003742640  66 6F 20 32 32 38 34 20 30 20 52 2F 49 44 5B 3C  fo 2284 0 R/ID[<
003742656  45 34 42 34 31 45 34 46 30 36 33 32 43 45 34 44  E4B41E4F0632CE4D
003742672  39 30 41 37 32 37 37 36 31 45 42 37 46 35 38 41  90A727761EB7F58A
003742688  3E 3C 41 43 46 43 44 35 42 43 31 36 41 45 42 44  ><ACFCD5BC16AEBD
003742704  34 32 41 36 42 38 38 38 33 30 35 44 31 42 46 30  42A6B888305D1BF0
003742720  39 31 3E 5D 3E 3E 0D 0A 73 74 61 72 74 78 72 65  91>]>>..startxre    Sector 7,310
003742736  66 0D 0A 30 0D 0A 25 25 45 4F 46 0D 0A 20 20 20  f..0..%%EOF..
003742752  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
003742768  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
003742784  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
003742800  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
003742816  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
003742832  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
003742848  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
003742864  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
003742880  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
003742896  20 20 20 0D 0A 32 36 35 34 20 30 20 6F 62 6A 3C     ..2654 0 obj<
003742912  3C 2F 4C 65 6E 67 74 68 20 38 35 33 2F 43 20 31  </Length 853/C 1
003742928  30 37 31 2F 46 69 6C 74 65 72 2F 46 6C 61 74 65  071/Filter/Flate
003742944  44 65 63 6F 64 65 2F 49 20 31 30 39 33 2F 4F 20  Decode/I 1093/O
003742960  31 30 33 31 2F 53 20 33 37 34 2F 56 20 31 30 34  1031/S 374/V 104
003742976  37 3E 3E 73 74 72 65 61 6D 0D 0A 89 3D 58 53 F3  7>>stream..‰=XSó
003742992  F4 AB B3 BF 55 F7 77 77 F9 7A 84 52 3F D1 40 2A  ô«³¿U÷wwùz„R?Ñ@*
```

Offset(d): 3742740 Block(d): 3742740-3742748 Length(d): 9 Overwrite

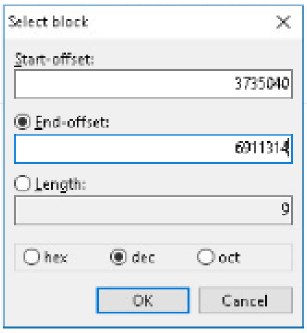
Found the actual end of the file



```
006911248  0D 0A 74 72 61 69 6C 65 72 0D 0A 3C 3C 2F 53 69  ..trailer..<</Si
006911264  7A 65 20 32 32 38 35 2F 45 6E 63 72 79 70 74 20  ze 2285/Encrypt 
006911280  32 32 38 36 20 30 20 52 3E 3E 0D 0A 73 74 61 72  2286 0 R>>..star
006911296  74 78 72 65 66 0D 0A 31 31 36 0D 0A 25 25 45 4F  txref..116..%%EO
006911312  46 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00  F...............
006911328  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Offset(d): 6911306 Block(d): 6911306-6911314 Length(d): 9

Selected the block

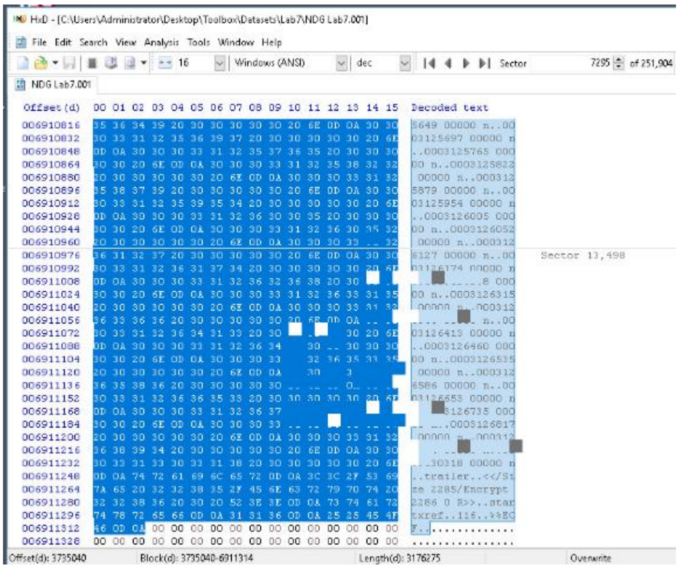


Start-offset: 3735040

● End-offset: 6911314

○ Length: 9

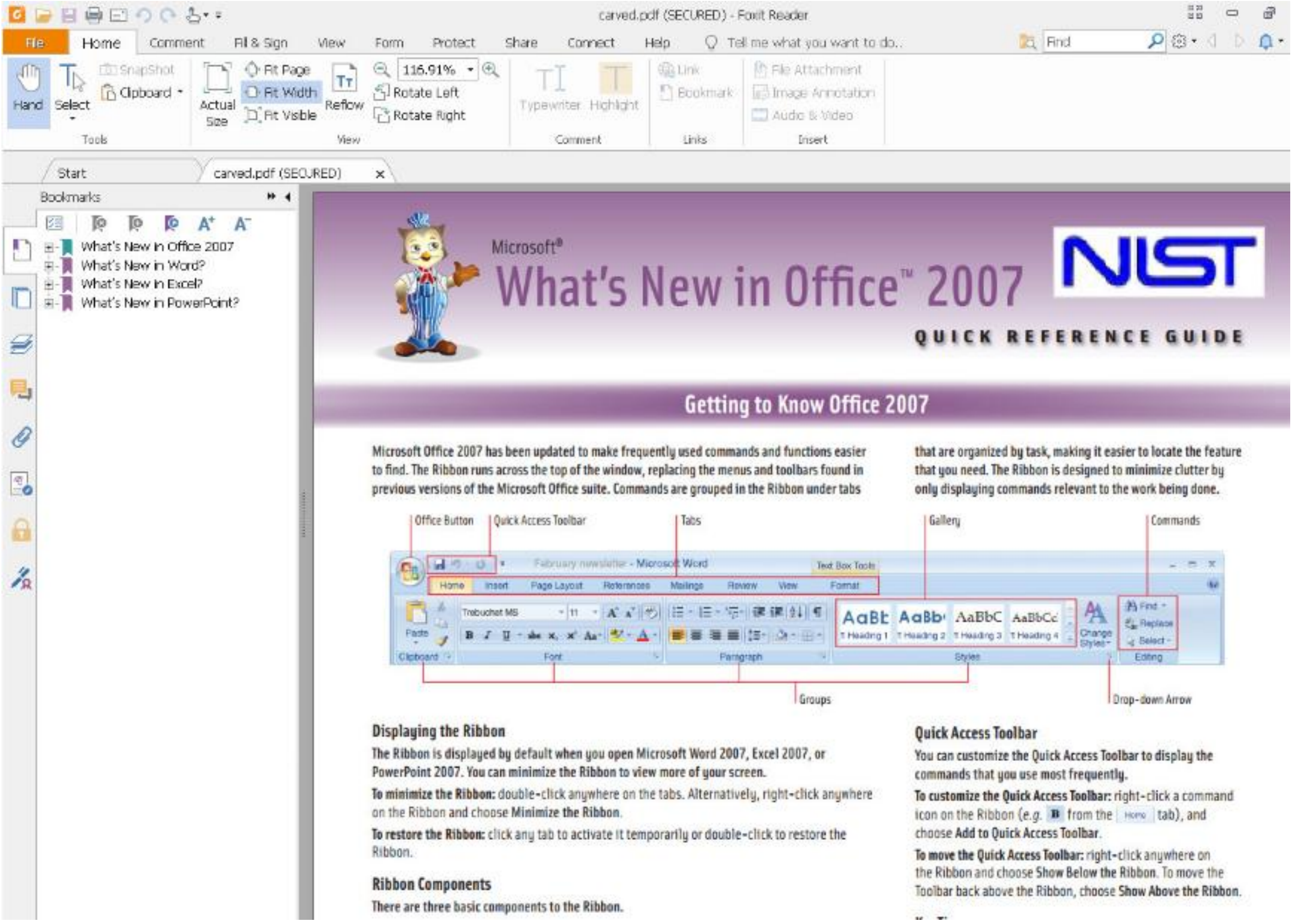
○ hex ● dec ○ oct


HxD - [C:\Users\Administrator\Desktop\Toolbox\Datasets\Lab7\NDG Lab7.001]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
dec
Sector
7295
of 251,904
NDG Lab7.001

```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text
006910816  35 36 34 39 20 30 30 30 30 30 20 6E 0D 0A 30 30  5649 00000 n..00
006910832  30 33 31 32 35 36 39 37 20 30 30 30 30 30 20 6E  03125697 00000 n
006910848  0D 0A 30 30 30 33 31 32 35 37 36 35 20 30 30 30  ..0003125765 000
006910864  30 30 20 6E 0D 0A 30 30 30 33 31 32 35 38 32 32  00 n..0003125822
006910880  20 30 30 30 30 30 20 6E 0D 0A 30 30 30 33 31 32   00000 n..000312
006910896  35 38 37 39 20 30 30 30 30 30 20 6E 0D 0A 30 30  5879 00000 n..00
006910912  30 33 31 32 35 39 35 34 20 30 30 30 30 30 20 6E  03125954 00000 n
006910928  0D 0A 30 30 30 33 31 32 36 30 30 35 20 30 30 30  ..0003126005 000
006910944  30 30 20 6E 0D 0A 30 30 30 33 31 32 36 30 35 32  00 n..0003126052
006910960  20 30 30 30 30 30 20 6E 0D 0A 30 30 30 33 .. 32   00000 n..000312
006910976  36 31 32 37 20 30 30 30 30 30 20 6E 0D 0A 30 30  6127 00000 n..00    Sector 13,498
006910992  30 33 31 32 36 31 37 34 20 30 30 30 30 30 20 6E  03126174 00000 n
006911008  0D 0A 30 30 30 33 31 32 36 32 36 38 20 30        ........8 000
006911024  30 30 20 6E 0D 0A 30 30 30 33 31 32 36 33 31 35  00 n..0003126315
006911040  20 30 30 30 30 30 20 6E 0D 0A 30 30 30 33 31 32   00000 n..000312
006911056  36 33 36 36 20 30 30 30 30 30 20 6E 0D 0A .. ..           n..00
006911072  30 33 31 32 36 34 31 33 20 30    ..    30 20 6E  03126413 00000 n
006911088  0D 0A 30 30 30 33 31 32 36 34    30 .. 30 30 30  ..0003126460 000
006911104  30 30 20 6E 0D 0A 30 30 30 33    32 36 35 33 35  00 n..0003126535
006911120  20 30 30 30 30 30 20 6E 0D 0A    30    3          00000 n..000312
006911136  36 35 38 36 20 30 30 30 30 30 .. .. .. 0. .. ..  6586 00000 n..00
006911152  30 33 31 32 36 36 35 33 20 30 30 30 30 30 20 6E  03126653 00000 n
006911168  0D 0A 30 30 30 33 31 32 36 37                      3126735 000
006911184  30 30 20 6E 0D 0A 30 30 30 33 .. .. .. .. .. ..  .. ...0003126817
006911200  20 30 30 30 30 30 20 6E 0D 0A 30 30 30 33 31 32   00000 n..000312
006911216  36 38 39 34 20 30 30 30 30 30 20 6E 0D 0A 30 30
006911232  30 33 31 33 30 33 31 38 20 30 30 30 30 30 20 6E  ..30318 00000 n
006911248  0D 0A 74 72 61 69 6C 65 72 0D 0A 3C 3C 2F 53 69  ..trailer..<</Si
006911264  7A 65 20 32 32 38 35 2F 45 6E 63 72 79 70 74 20  ze 2285/Encrypt 
006911280  32 32 38 36 20 30 20 52 3E 3E 0D 0A 73 74 61 72  2286 0 R>>..star
006911296  74 78 72 65 66 0D 0A 31 31 36 0D 0A 25 25 45 4F  txref..116..%%EO
006911312  46 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00  F...............
006911328  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Offset(d): 3735040 Block(d): 3735040-6911314 Length(d): 3176275 Overwrite

Saved file as pdf and opened



Getting to Know Office 2007

Microsoft Office 2007 has been updated to make frequently used commands and functions easier to find. The Ribbon runs across the top of the window, replacing the menus and toolbars found in previous versions of the Microsoft Office suite. Commands are grouped in the Ribbon under tabs that are organized by task, making it easier to locate the feature that you need. The Ribbon is designed to minimize clutter by only displaying commands relevant to the work being done.

Displaying the Ribbon

The Ribbon is displayed by default when you open Microsoft Word 2007, Excel 2007, or PowerPoint 2007. You can minimize the Ribbon to view more of your screen.

To minimize the Ribbon: double-click anywhere on the tabs. Alternatively, right-click anywhere on the Ribbon and choose **Minimize the Ribbon**.

To restore the Ribbon: click any tab to activate it temporarily or double-click to restore the Ribbon.

Ribbon Components

There are three basic components to the Ribbon.

Quick Access Toolbar

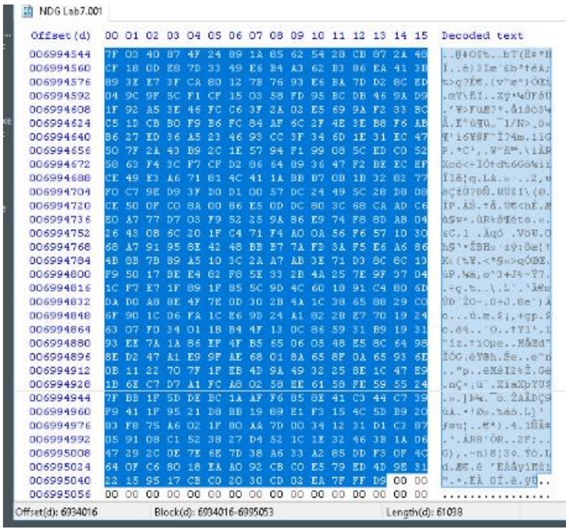
You can customize the Quick Access Toolbar to display the commands that you use most frequently.

To customize the Quick Access Toolbar: right-click a command icon on the Ribbon (*e.g.* **B** from the Home tab), and choose **Add to Quick Access Toolbar**.

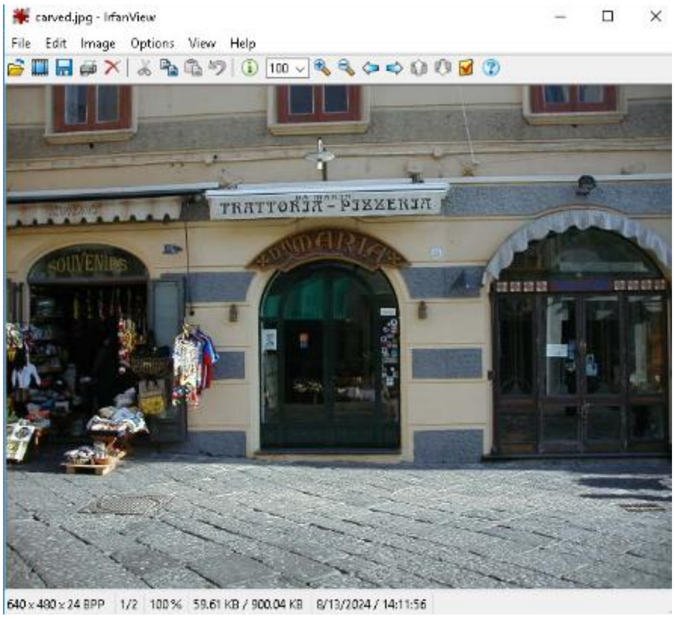
To move the Quick Access Toolbar: right-click anywhere on the Ribbon and choose **Show Below the Ribbon**. To move the Toolbar back above the Ribbon, choose **Show Above the Ribbon**.

Carving a JPG

Search for FF D8 FF E0 (file signature for JPG files) clicking forward as the file we are looking for is after the PDF file. Offset at 6934016. Footer for JPG is 0Xff d9 search "ff d9" and selected forward to see the footer that follows this header. Some hex values are false positive.

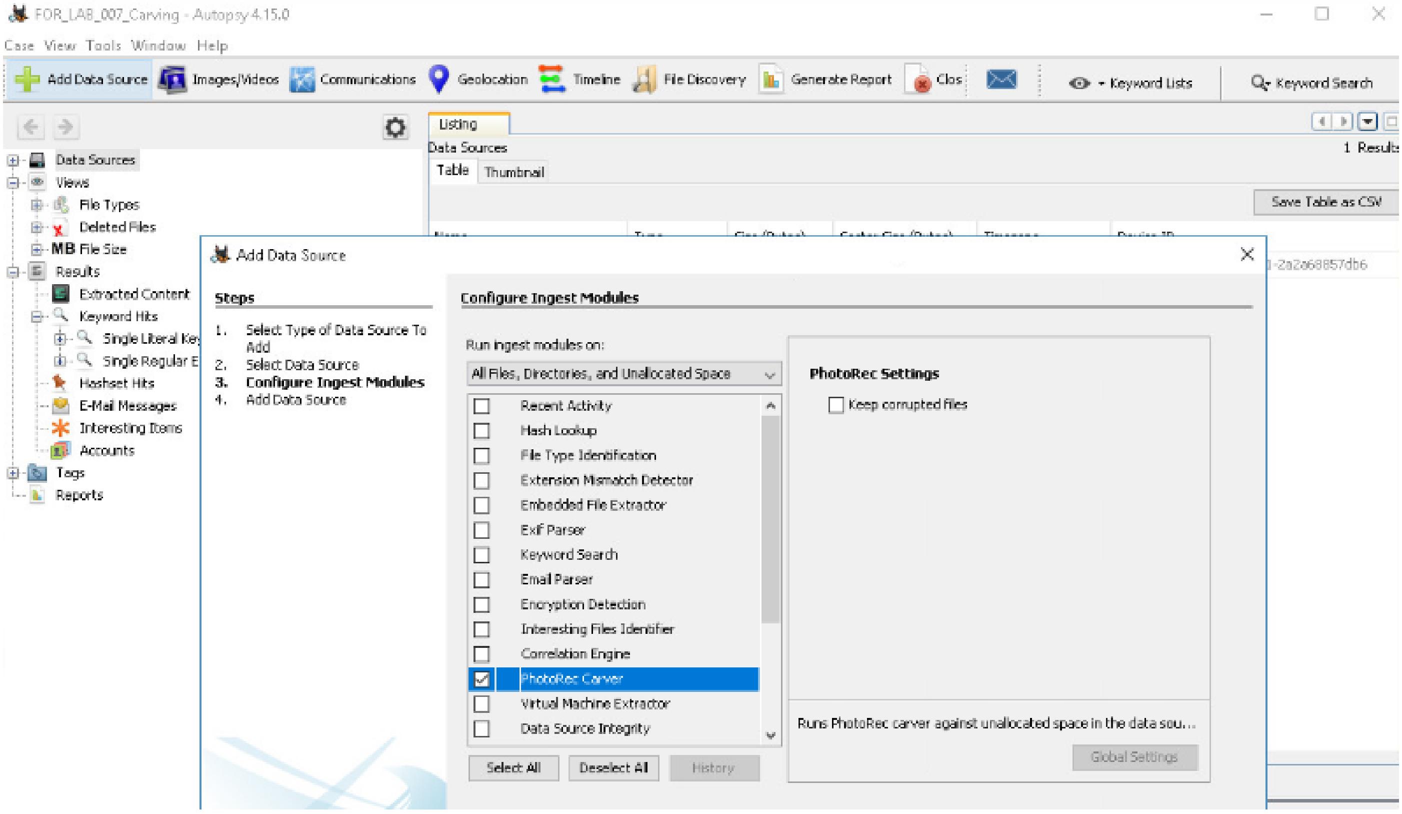


```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
006994544  7F 03 40 87 4F 24 89 1A 85 62 54 28 CB 87 2A 48
006994560  CF 18 0D E8 7D 33 49 E6 B4 A3 62 B3 86 EA 41 3B
006994576  89 3E E7 3F CA 80 12 7B 76 93 E6 BA 7D D2 8C ED
006994592  04 9C 9F 5C F1 CF 15 03 58 FD 95 BC DB 46 9A D9
006994608  1F 92 A5 3E 46 FC C6 3F 2A 02 E5 69 9A F2 33 BC
006994624  C5 1D CB B0 F9 B6 FC 84 AF 6C 2F 4E 3E B8 F6 AB
006994640  B6 27 ED 36 A5 23 46 93 CC 3F 34 6D 1E 31 EC 47
006994656  50 7F 2A 43 B9 2C 1E 57 94 F1 99 08 5C ED C0 52
006994672  58 63 F4 3C F7 CF D2 86 64 89 36 47 F2 BE EC EF
006994688  CE 49 E3 A6 71 81 4C 41 1A BB B7 08 1B 32 82 77
006994704  F0 C7 9E D9 3F D0 D1 00 57 DC 24 49 5C 28 D8 08
006994720  CE 50 0F C0 8A 00 86 E5 0D DC 80 3C 68 CA AD C6
006994736  E0 A7 77 D7 03 F9 52 25 9A B6 E9 74 F8 8D AB 04
006994752  26 43 0B 6C 20 1F C4 71 F4 A0 0A 56 F6 57 10 30
006994768  68 A7 91 95 8E 42 48 BB B7 7A FD 3A F5 E6 A6 86
006994784  4B 8B 7B B9 A5 10 3C 2A A7 AB 3E 71 D3 8C 8C 13
006994800  F9 50 17 BE E4 82 F8 5E 33 2B 4A 25 7E 9F 37 04
006994816  1C F7 E7 1F 89 1F 85 5C 9D 4C 60 18 91 C4 80 6D
006994832  DA D0 A8 BE 4F 7E 0D 30 2B 4A 1C 38 65 88 29 C0
006994848  6F 90 1C D6 FA 1C E6 9D 24 A1 82 2B E7 70 19 24
006994864  63 07 F0 34 01 18 B4 4F 13 0C 86 59 31 B9 19 31
006994880  93 EE 7A 1A 86 EF 4F B5 65 06 05 48 E5 8C 64 98
006994896  8E D2 47 A1 E9 9F AE 68 01 8A 65 8F 0A 65 93 6E
006994912  0B 11 22 70 7F 1F EB 4D 9A 49 32 25 8E 1C 47 E9
006994928  1B 6E C7 D7 A1 FC A8 02 58 EE 61 58 FE 59 55 24
006994944  7F BB 1F 5D DE BC 1A AF F6 85 8E 41 C3 44 C7 39
006994960  F9 41 1F 95 21 D8 BB 19 89 E1 F3 15 4C 5D B9 20
006994976  83 F8 75 A6 02 1F 80 AA 7D 00 34 12 31 D1 C3 B7
006994992  05 91 08 C1 52 38 27 D4 52 1C 1E 32 46 3B 1A D6
006995008  47 29 2C 0E 7E 6E 7D 38 A6 33 A2 85 DD F3 0F 4C
006995024  64 0F C6 80 18 EA A0 92 CB C0 E5 79 ED 4D 9E 31
006995040  22 15 95 17 CB C0 20 30 CD 02 EA 7F FF D9 00 00
006995056  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset(d): 6934016    Block(d): 6934016-6995053    Length(d): 61038
```



640 x 480 x 24 BPP   1/2   100 %   59.61 KB / 900.04 KB   8/13/2024 / 14:11:56

File carving with Autopsy



FOR_LAB_007_Carving - Autopsy 4.15.0

Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

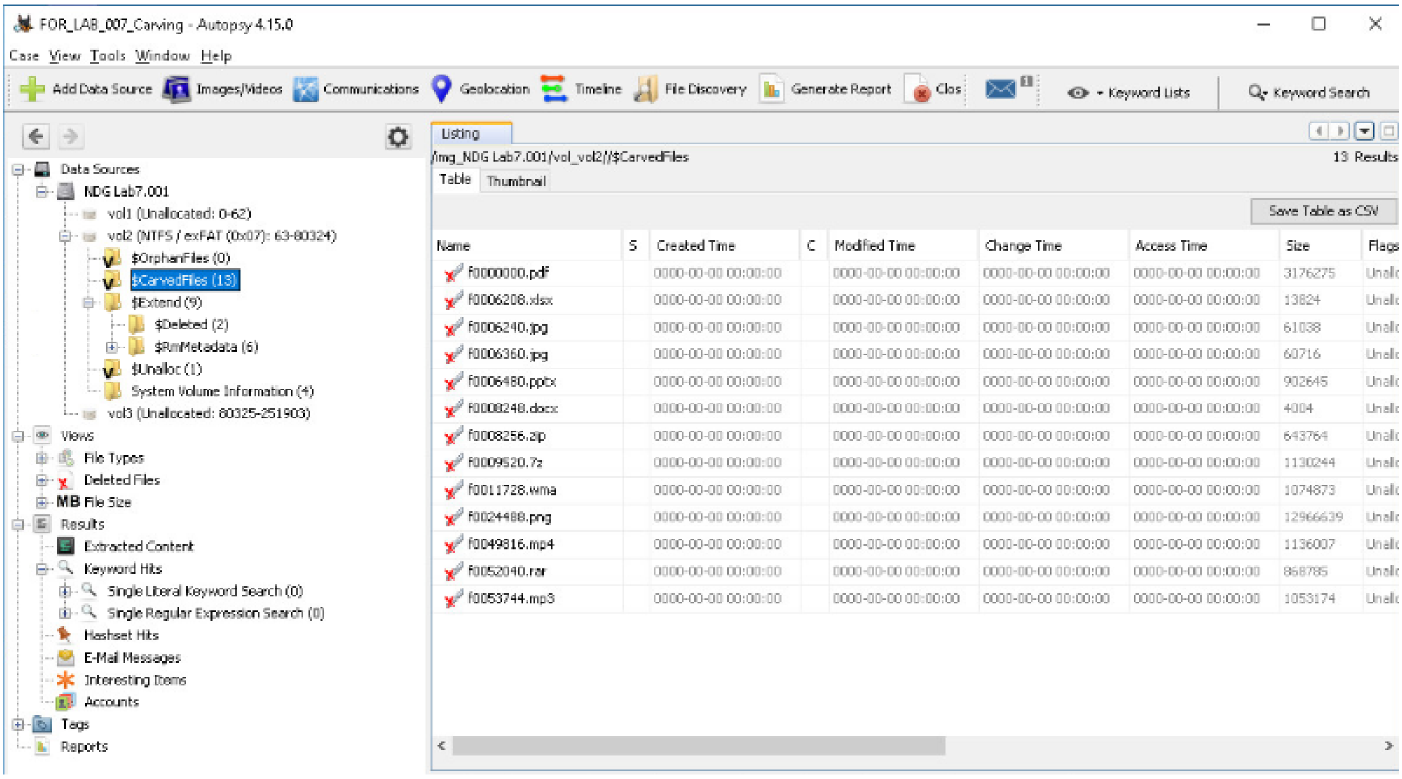
Run ingest modules on: All Files, Directories, and Unallocated Space

- ☐ Recent Activity
- ☐ Hash Lookup
- ☐ File Type Identification
- ☐ Extension Mismatch Detector
- ☐ Embedded File Extractor
- ☐ Exif Parser
- ☐ Keyword Search
- ☐ Email Parser
- ☐ Encryption Detection
- ☐ Interesting Files Identifier
- ☐ Correlation Engine
- ☑ PhotoRec Carver
- ☐ Virtual Machine Extractor
- ☐ Data Source Integrity

PhotoRec Settings

☐ Keep corrupted files

Runs PhotoRec carver against unallocated space in the data sou...



FOR_LAB_007_Carving - Autopsy 4.15.0

/img_NDG Lab7.001/vol_vol2//$CarvedFiles — 13 Results

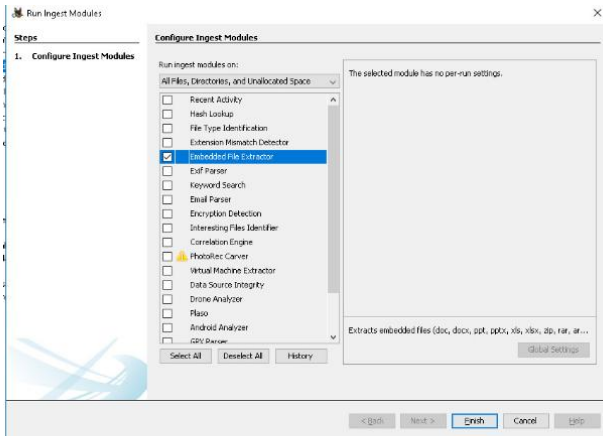
- Data Sources
  - NDG Lab7.001
    - vol1 (Unallocated: 0-62)
    - vol2 (NTFS / exFAT (0x07): 63-80324)
      - $OrphanFiles (0)
      - $CarvedFiles (13)
      - $Extend (9)
        - $Deleted (2)
        - $RmMetadata (6)
      - $Unalloc (1)
      - System Volume Information (4)
    - vol3 (Unallocated: 80325-251903)
- Views
- Results
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)

Name	S	Created Time	C	Modified Time	Change Time	Access Time	Size	Flags
f0000000.pdf		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3176275	Unall
f0006208.xlsx		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13824	Unall
f0006240.jpg		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	61038	Unall
f0006360.jpg		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	60716	Unall
f0006480.pptx		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	902645	Unall
f0008248.docx		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4004	Unall
f0008256.zip		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	643764	Unall
f0009520.7z		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1130244	Unall
f0011728.wma		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1074873	Unall
f0024488.png		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12966639	Unall
f0049816.mp4		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1136007	Unall
f0052040.rar		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	868785	Unall
f0053744.mp3		0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1053174	Unall

13 files carved from an unallocated space

As you can see, some of the files are archive files. Files that have the file extensions .ZIP, .RAR, .7z and even post 2007 *Microsoft Office* documents contain 1 or more files within them. Let us run an *Ingest Module* to add these files to the case so we can view them. To do this, click the **Tools** dropdown menu from the menu bar and navigate to **Run Ingest Modules;** hover over it to reveal the data sources sub-menu as highlighted in *items* **1** and **2**. Click the data source **LAB007.001** as highlighted in *item* **3** below. This will reopen the *Run Ingest Module* window.

Some of the files are archive files



Run Ingest Modules

Steps

1. Configure Ingest Modules

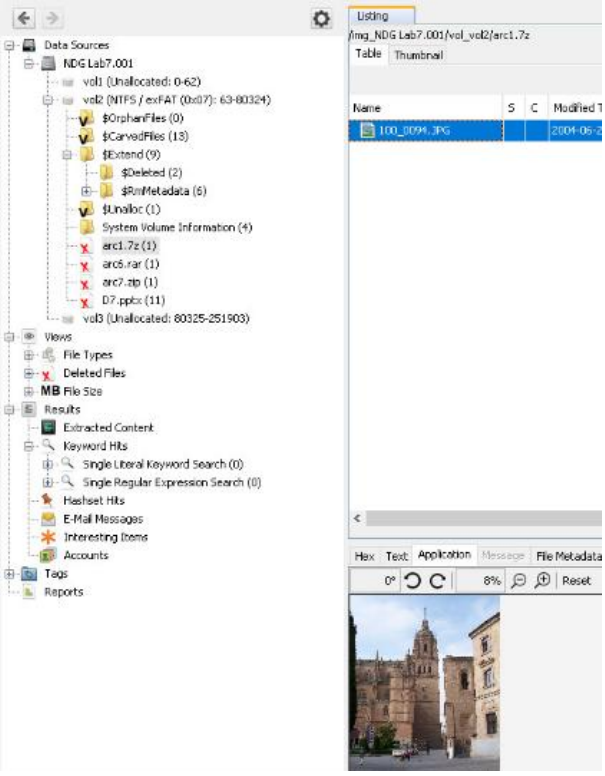
Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

- □ Recent Activity
- □ Hash Lookup
- □ File Type Identification
- □ Extension Mismatch Detector
- ☑ Embedded File Extractor
- □ Exif Parser
- □ Keyword Search
- □ Email Parser
- □ Encryption Detection
- □ Interesting Files Identifier
- □ Correlation Engine
- □ PhotoRec Carver
- □ Virtual Machine Extractor
- □ Data Source Integrity
- □ Drone Analyzer
- □ Plaso
- □ Android Analyzer
- □ GPX Parser

The selected module has no per-run settings.

Extracts embedded files (doc, docx, ppt, pptx, xls, xlsx, zip, rar, ar...



```
Data Sources
  NDG Lab7.001
    vol1 (Unallocated: 0-62)
    vol2 (NTFS / exFAT (0x07): 63-80324)
      $OrphanFiles (0)
      $CarvedFiles (13)
      $Extend (9)
        $Deleted (2)
        $RmMetadata (6)
      $Unalloc (1)
      System Volume Information (4)
      arc1.7z (1)
      arc6.rar (1)
      arc7.zip (1)
      D7.pptx (11)
    vol3 (Unallocated: 80325-251903)
Views
  File Types
  Deleted Files
  MB File Size
Results
  Extracted Content
  Keyword Hits
    Single Literal Keyword Search (0)
    Single Regular Expression Search (0)
  Hashset Hits
  E-Mail Messages
  Interesting Items
  Accounts
Tags
Reports
```

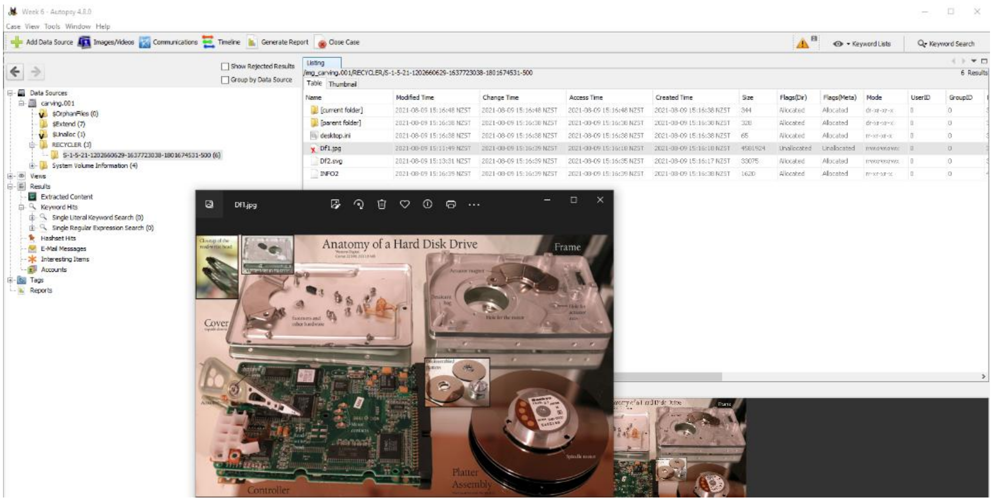
/img_NDG Lab7.001/vol_vol2/arc1.7z

Name	S	C	Modified T
100_0094.JPG			2004-06-2

File: 50mg and is a Windows Primary Partition

Using Autopsy, we extracted an image from the recycler (Df1.jpg)

1 file deleted further from recycle bin below



Week 6 - Autopsy 4.8.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Timeline | Generate Report | Close Case | Keyword Lists | Keyword Search

□ Show Rejected Results
□ Group by Data Source

- Data Sources
  - carving.001
    - $OrphanFiles (0)
    - $Extend (7)
    - $Unalloc (1)
    - RECYCLER (3)
      - S-1-5-21-1202660629-1637723038-1801674531-500 (6)
    - System Volume Information (4)
- Views
- Results
  - Extracted Content
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Accounts
- Tags
- Reports

Listing

/img_carving.001/RECYCLER/S-1-5-21-1202660629-1637723038-1801674531-500

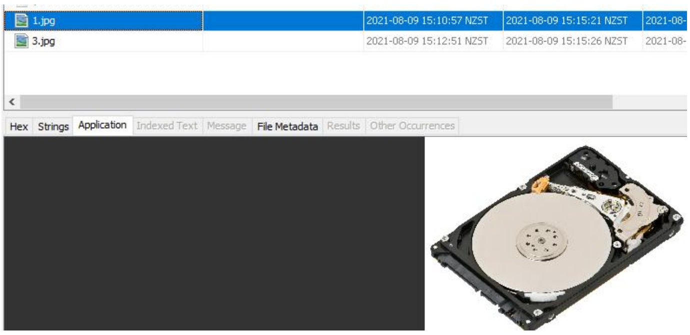
6 Results

Table | Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID	GroupID
[current folder]	2021-08-09 15:16:48 NZST	2021-08-09 15:16:48 NZST	2021-08-09 15:16:48 NZST	2021-08-09 15:16:38 NZST	344	Allocated	Allocated	dr-xr-xr-x	0	0
[parent folder]	2021-08-09 15:16:38 NZST	2021-08-09 15:16:38 NZST	2021-08-09 15:16:38 NZST	2021-08-09 15:16:38 NZST	328	Allocated	Allocated	dr-xr-xr-x	0	0
desktop.ini	2021-08-09 15:16:38 NZST	2021-08-09 15:16:38 NZST	2021-08-09 15:16:38 NZST	2021-08-09 15:16:38 NZST	65	Allocated	Allocated	r-xr-xr-x	0	0
Df1.jpg	2021-08-09 15:11:49 NZST	2021-08-09 15:16:39 NZST	2021-08-09 15:16:18 NZST	2021-08-09 15:16:18 NZST	4581924	Unallocated	Unallocated	rwxrwxrwx	0	0
Df2.svg	2021-08-09 15:13:31 NZST	2021-08-09 15:16:39 NZST	2021-08-09 15:16:35 NZST	2021-08-09 15:16:17 NZST	33075	Allocated	Allocated	rwxrwxrwx	0	0
INFO2	2021-08-09 15:16:39 NZST	2021-08-09 15:16:39 NZST	2021-08-09 15:16:39 NZST	2021-08-09 15:16:38 NZST	1620	Allocated	Allocated	r-xr-xr-x	0	0

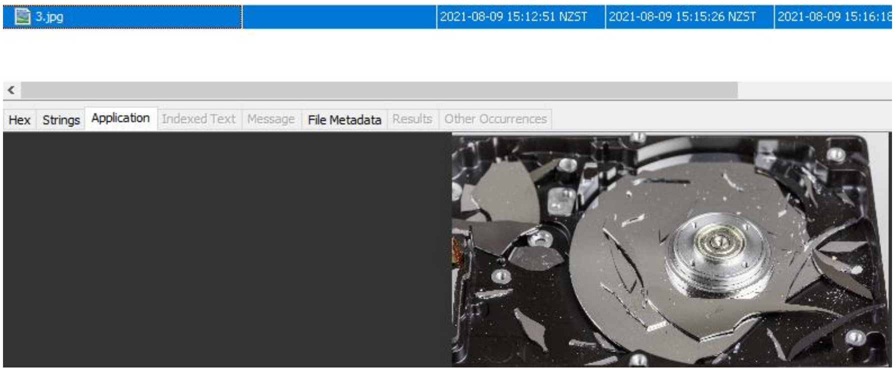
Df1.jpg

2 file images found that were deleted



1.jpg		2021-08-09 15:10:57 NZST	2021-08-09 15:15:21 NZST	2021-08-
3.jpg		2021-08-09 15:12:51 NZST	2021-08-09 15:15:26 NZST	2021-08-

Hex | Strings | Application | Indexed Text | Message | File Metadata | Results | Other Occurrences

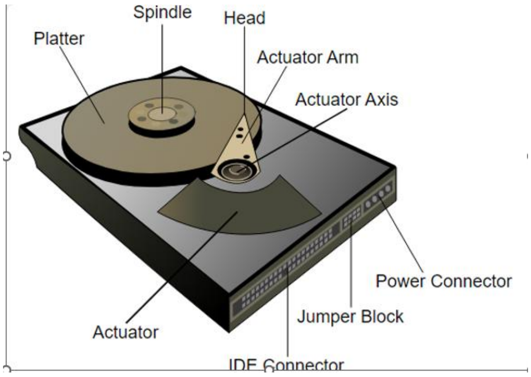


3.jpg		2021-08-09 15:12:51 NZST	2021-08-09 15:15:26 NZST	2021-08-09 15:16:18

Hex | Strings | Application | Indexed Text | Message | File Metadata | Results | Other Occurrences

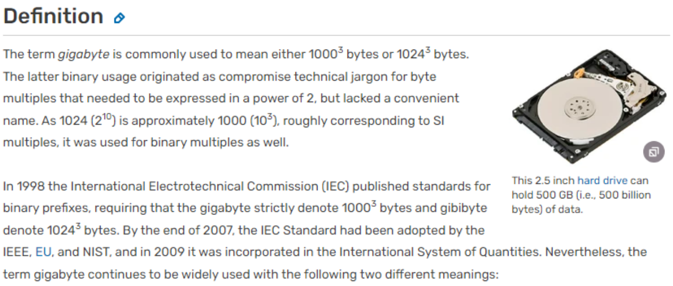
Image number 4 – extracted and opened via file explorer

The below image had an unusual file type as per svg in order to open in file explorer



File origins

1.jpg (Gigabyte | Ultimate Pop Culture Wiki | Fandom)



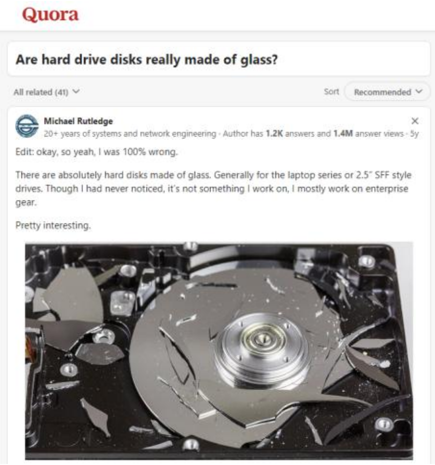
Definition

The term *gigabyte* is commonly used to mean either 1000^3 bytes or 1024^3 bytes. The latter binary usage originated as compromise technical jargon for byte multiples that needed to be expressed in a power of 2, but lacked a convenient name. As 1024 (2^{10}) is approximately 1000 (10^3), roughly corresponding to SI multiples, it was used for binary multiples as well.

This 2.5 inch hard drive can hold 500 GB (i.e., 500 billion bytes) of data.

In 1998 the International Electrotechnical Commission (IEC) published standards for binary prefixes, requiring that the gigabyte strictly denote 1000^3 bytes and gibibyte denote 1024^3 bytes. By the end of 2007, the IEC Standard had been adopted by the IEEE, EU, and NIST, and in 2009 it was incorporated in the International System of Quantities. Nevertheless, the term gigabyte continues to be widely used with the following two different meanings:

3.jpg (Are hard drive disks really made of glass? - Quora)



Quora

Are hard drive disks really made of glass?

All related (41) Sort Recommended

Michael Rutledge
20+ years of systems and network engineering · Author has **1.2K** answers and **1.4M** answer views · 5y

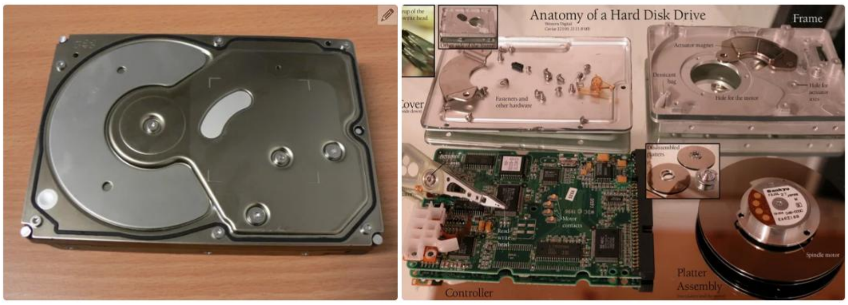
Edit: okay, so yeah, I was 100% wrong.

There are absolutely hard disks made of glass. Generally for the laptop series or 2.5″ SFF style drives. Though I had never noticed, it's not something I work on, I mostly work on enterprise gear.

Pretty interesting.

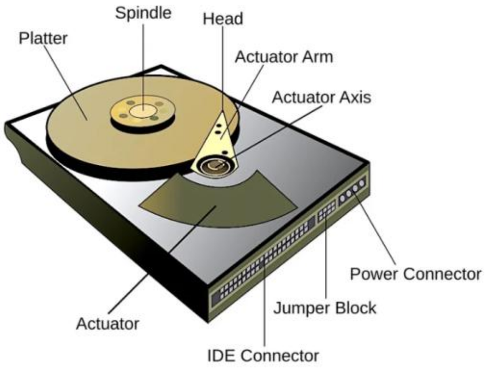
Df1 image (HDDJ: Turning an Old Hard Disk Drive Into a Rotary Input Device : 7 Steps (with Pictures) - Instructables)

Step 1: Crack Open a Hard Disk Drive



Df2 image (3 Different Types Of Hard Drives [Explained] - RankRed)

Inside the hard drives are one or more rotating platters coated with magnetic material. These platters are paired with magnetic heads, which move with an actuator arm to read and write data to the drive. Individual blocks of data can be stored and retrieved in random order.


Spindle
Head
Platter
Actuator Arm
Actuator Axis
Power Connector
Jumper Block
Actuator
IDE Connector