FORENSICS V2 LAB SERIES

Lab 07: Data Carving

Document Version: 2021-01-14

Contents

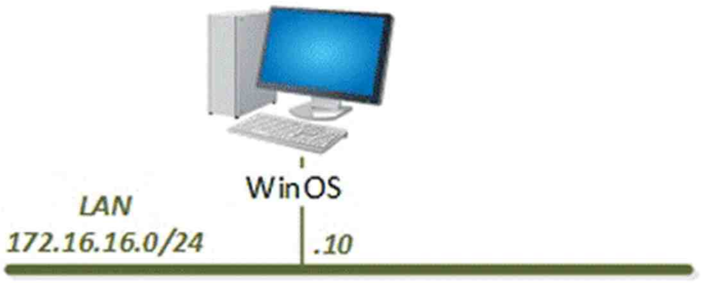
Introduction

Data recovery can be considered a facet of digital forensics. Potential evidence gets deleted all the time and may linger in unallocated space. To access these files, advanced data recovery methods known as data carving must be used. This process involves identifying certain characters, called file signatures, in seemingly nonsensical data. In this lab, we will get you familiar with file signatures and teach you how to carve the data out.

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

Lab Topology



Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

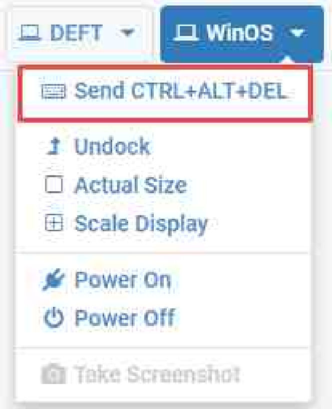
Virtual Machine	IP Address / Subnet Mask	Account (if needed)	Password (if needed)
Caine	172.16.16.30	caine	Train1ng$
CSI-Linux	172.16.16.40	csi	csi
DEFT	172.16.16.20	deft	Train1ng$
WinOS	172.16.16.10	Administrator	Train1ng$

1 Getting to Know File Signatures

File signatures help programs identify and interpret the data within files. They work together with file extensions to make accessing digital content seamless. Forensic examiners utilize file signatures to locate files on systems and to verify what a file really is and what it may contain. We touched a little on file signatures in Lab 2, so you should be a little familiar with the concept. In this lab, we will go a little deeper and identify some more file signatures. We will also learn to manually carve them out and save them as files. The manual carving method is normally time-consuming and, as such, not the most productive use of analysis time. There are many tools out there that can carve data automatically and do a very good job of it. This introduction to manual carving is to ensure that you learn the basics and understand what the automated carver is doing in the background. Later in the exercise, we will use the automated carver, and then we can compare the results.

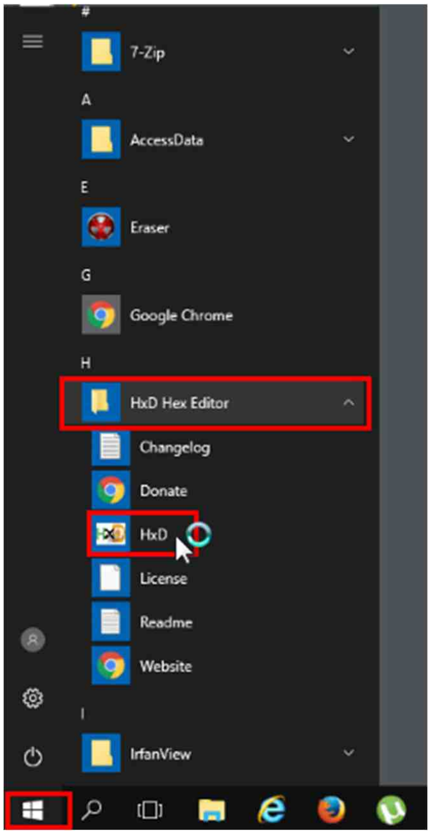
Let us get started by opening the hex editor called HxD Hex Editor and Disk Editor.

1. To begin, launch the WinOS virtual machine to access the graphical login screen.
   a. Select Send CTRL+ALT+DEL from the dropdown menu to be prompted with the login screen.

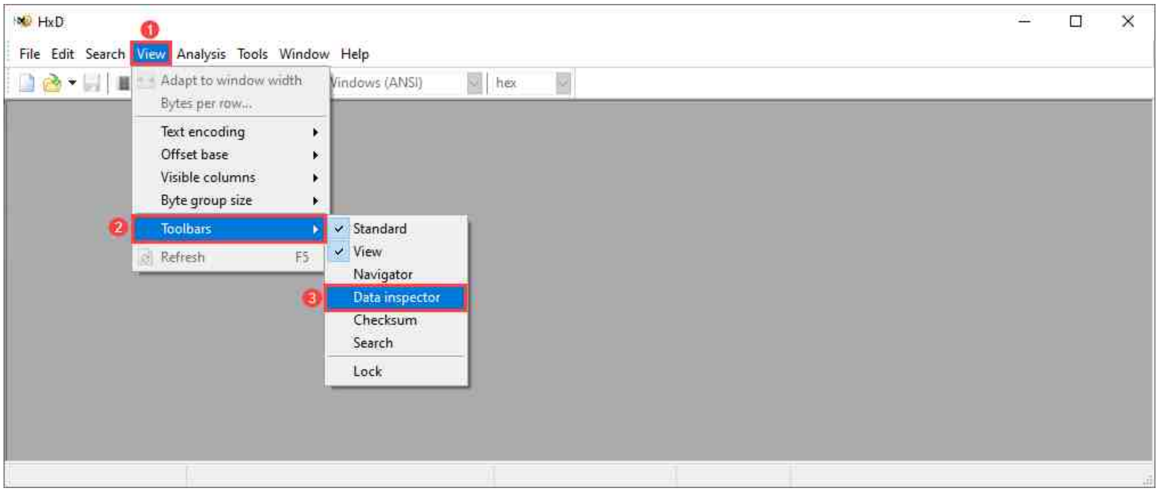


   b. Log in as `Administrator` using the password: `Train1ng$`

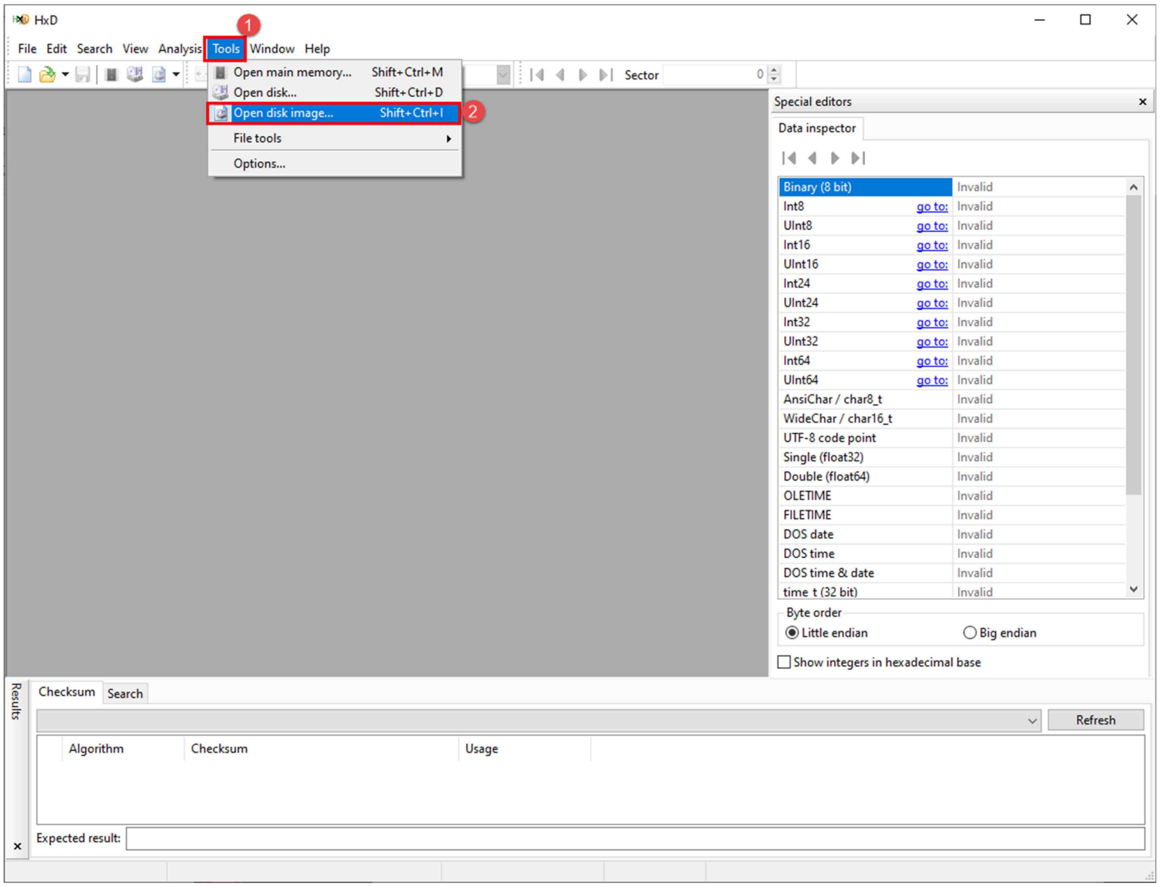
2. Once you are logged into the VM, launch the HxD program from the windows menu by navigating to Start Menu > HxD Hex Editor. Alternatively, you can open HxD Hex Editor from the Desktop by double-clicking the icon called HxD:



3. HxD will open and since you are familiar with it from the previous labs, let us begin by verifying that the Data inspector tab is enabled. To do this, navigate to View > Toolbars as seen in items 1 and 2. Once there, review the submenu that appears. If the Data Inspector option seen in item 3 does not have a checkmark beside it, then click it. If it does have a checkmark, then exit the menu by clicking on an empty area outside of the menu.



4. Now let us move on to loading our Forensic Evidence File (FEF). To do this, click the Open disk image option from the Tools dropdown menu, as seen in items 1 and 2 in the screenshot below.

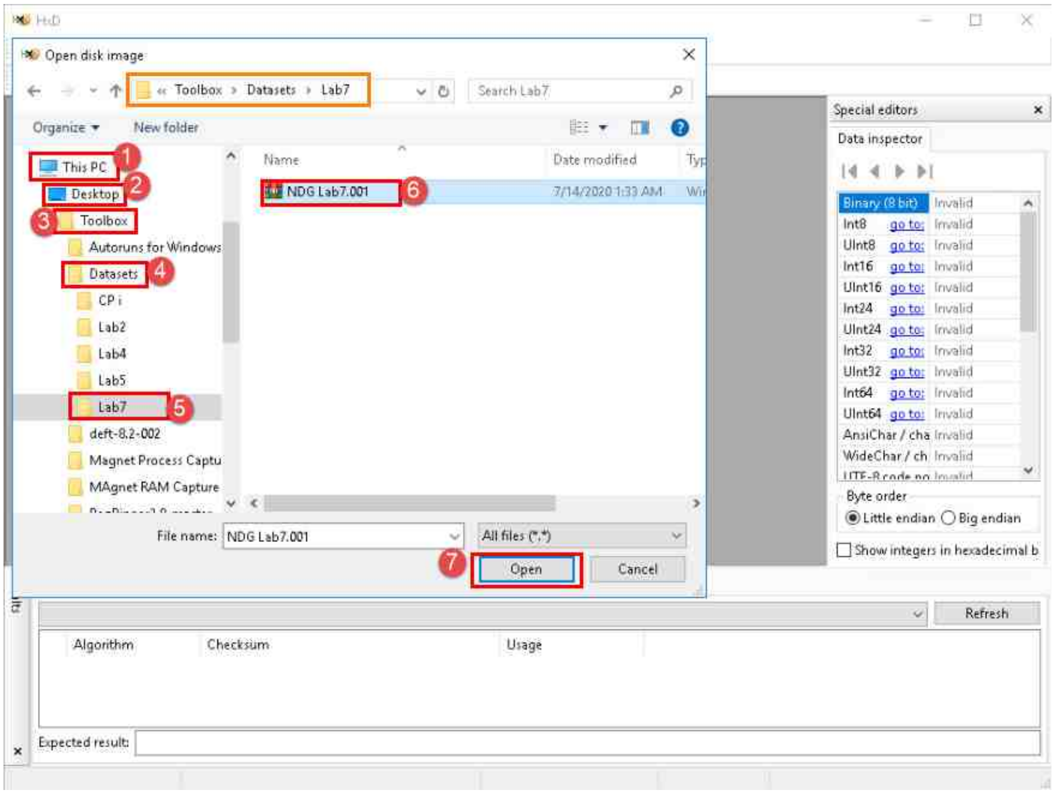

HxD
File Edit Search View Analysis Tools Window Help
1
Open main memory... Shift+Ctrl+M
Open disk... Shift+Ctrl+D
Open disk image... Shift+Ctrl+I
2
File tools
Options...
Sector 0
Special editors
Data inspector
Results
Checksum
Search
Refresh
Algorithm
Checksum
Usage
Expected result:

Binary (8 bit)		Invalid
Int8	go to:	Invalid
UInt8	go to:	Invalid
Int16	go to:	Invalid
UInt16	go to:	Invalid
Int24	go to:	Invalid
UInt24	go to:	Invalid
Int32	go to:	Invalid
UInt32	go to:	Invalid
Int64	go to:	Invalid
UInt64	go to:	Invalid
AnsiChar / char8_t		Invalid
WideChar / char16_t		Invalid
UTF-8 code point		Invalid
Single (float32)		Invalid
Double (float64)		Invalid
OLETIME		Invalid
FILETIME		Invalid
DOS date		Invalid
DOS time		Invalid
DOS time & date		Invalid
time_t (32 bit)		Invalid

Byte order
● Little endian ○ Big endian

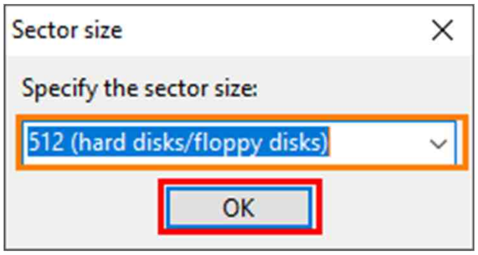
□ Show integers in hexadecimal base

5. The Open disk image window will appear. Use this window to browse to This PC > Desktop and double-click the folder Toolbox > Datasets > Lab7. This will open the folder revealing an FEF. Select the file called Lab007.001 and click the Open button as highlighted below.



File name: NDG Lab7.001

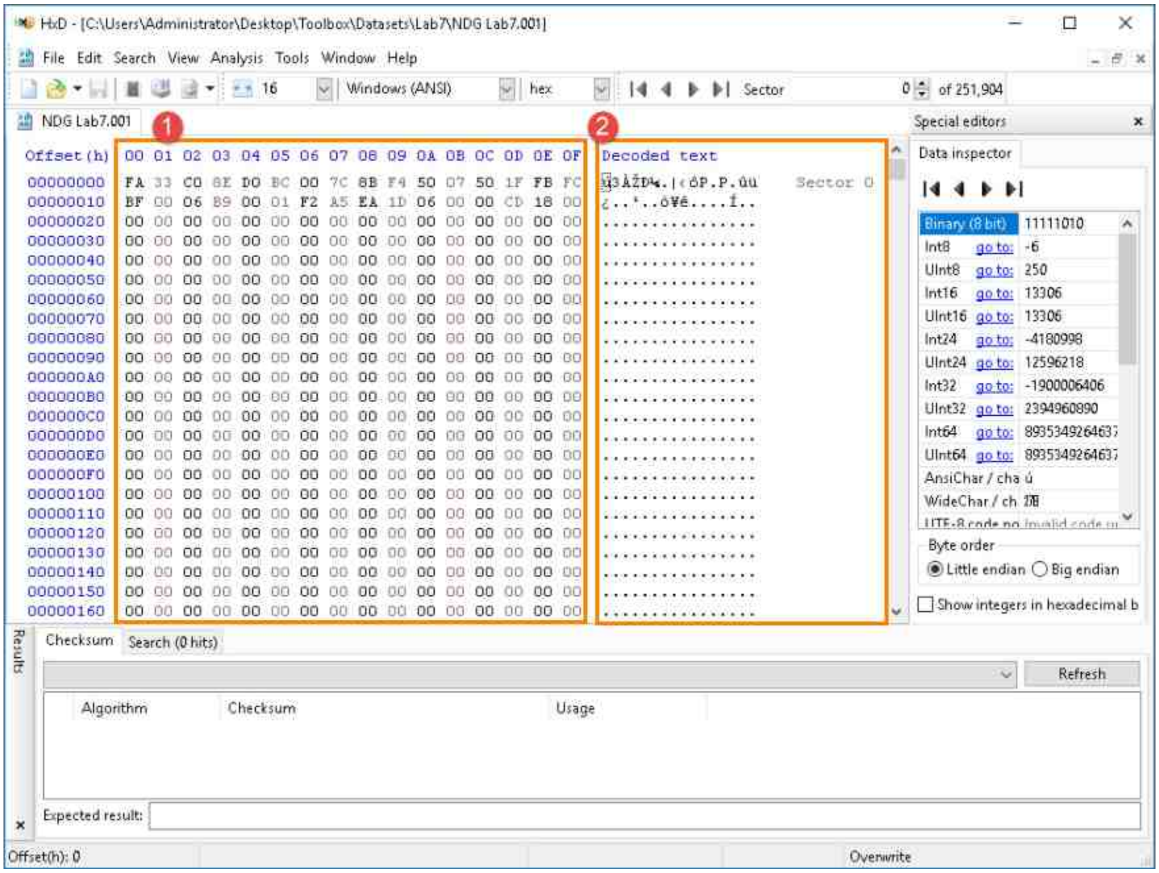
6. The Sector size window will appear. This window allows you to select the sector size of the image. In this lab, we will leave the option as 512 (hard disks/floppy disks) and click OK as highlighted below.



Specify the sector size: 512 (hard disks/floppy disks)

Do NOT change the specified sector size from 512 Bytes

7. You will see the window below appear. As you can see in the screenshot below, the view pane now contains the hexadecimal representation on the left of the pane. This is highlighted as item 1 below. Immediately beside the hexadecimal values is the Decoded text view, highlighted as item 2.



```
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  ................
```

Binary (8 bit)		11111010
Int8	go to:	-6
UInt8	go to:	250
Int16	go to:	13306
UInt16	go to:	13306
Int24	go to:	-4180998
UInt24	go to:	12596218
Int32	go to:	-1900006406
UInt32	go to:	2394960890
Int64	go to:	893534926463
UInt64	go to:	893534926463
AnsiChar / cha		ú
WideChar / ch		㏺
UTF-8 code po		Invalid code u

Byte order
● Little endian ○ Big endian

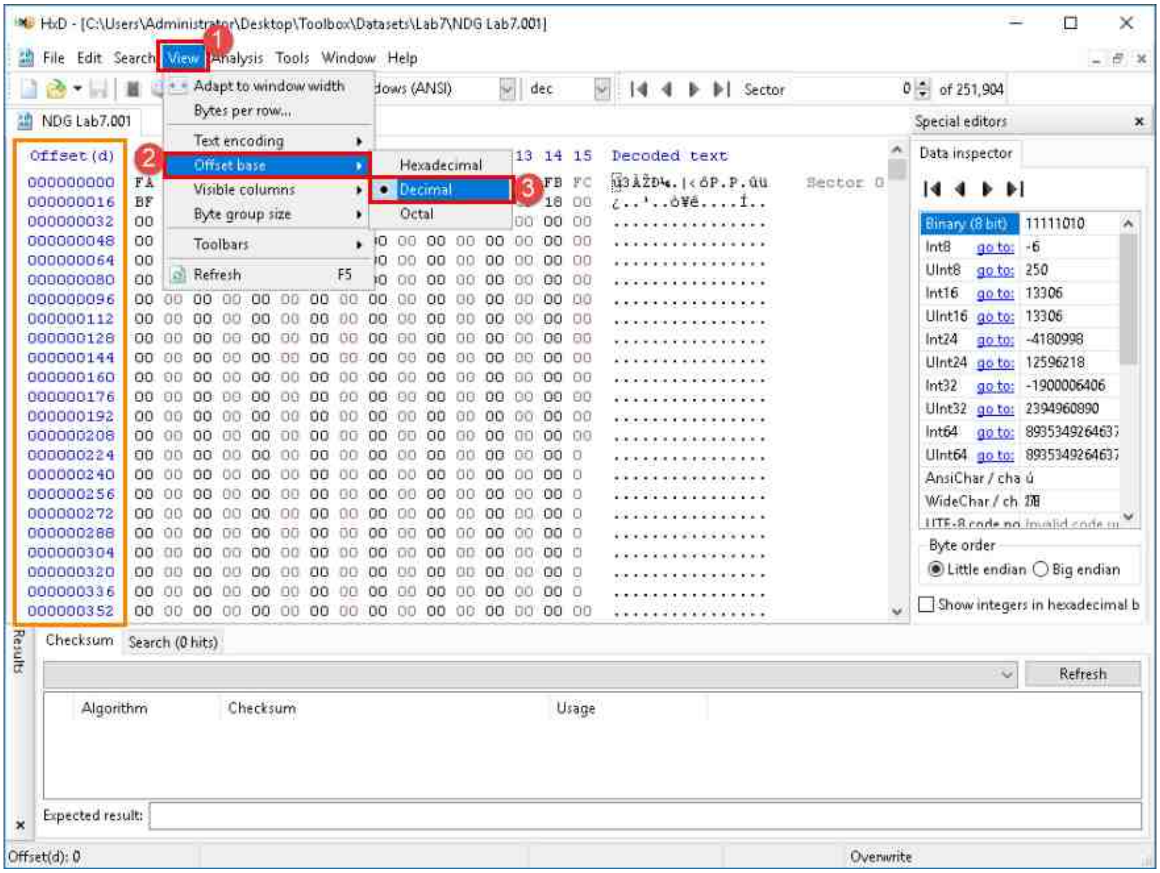
□ Show integers in hexadecimal b

8. Now that we have the data loaded, let us take a quick look at some very common file signatures. As we mentioned earlier, file signatures are data that can be found within a file and is used to identify what kind of file it is. It is important to note that some file signatures have a header (the beginning of the file) and a footer (the end of the file). Some signatures do not, which makes it even tougher to determine the end of the file. In this exercise, we will search for 3 of the most common filetypes out there, using their signatures.

   The filetypes we will be using are XLSX, PDF, and JPEG. The table below contains the file headers for each of these filetypes in both hexadecimal and raw text.

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

9. We will use the data from the table to search for and carve each file. Normally, we would immediately highlight the data and export it once you see a file header, but that is very time consuming and can be a trial-and-error process. Instead, let us limit the number of tries by using the file offsets. First, let us ensure that the Offset base is set to Decimal. To do this, click the View dropdown menu option from the menu bar and hover over the Offset base option, then select Decimal as highlighted in items 1, 2, and 3 below.



Offset base: ● Decimal

```
Offset(d)                                         13 14 15   Decoded text
000000000  FA                                        FB FC   û3ÅŽÐ¼.|<óP.P.ûu    Sector 0
000000016  BF                                        18 00   ¿..'..ò¥ê....î..
000000032  00                                     00 00 00   ................
000000048  00                   0 00 00 00 00 00 00 00 00   ................
000000064  00                   0 00 00 00 00 00 00 00 00   ................
000000080  00                   0 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 0    ................
000000240  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0    ................
000000256  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0    ................
000000272  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0    ................
000000288  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0    ................
000000304  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0    ................
000000320  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0    ................
000000336  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0    ................
000000352  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Binary (8 bit)		11111010
Int8	go to:	-6
UInt8	go to:	250
Int16	go to:	13306
UInt16	go to:	13306
Int24	go to:	-4180998
UInt24	go to:	12596218
Int32	go to:	-1900006406
UInt32	go to:	2394960890
Int64	go to:	893534926463
UInt64	go to:	893534926463
AnsiChar / cha		ú
WideChar / ch		㓺
UTF-8 code po		Invalid code u

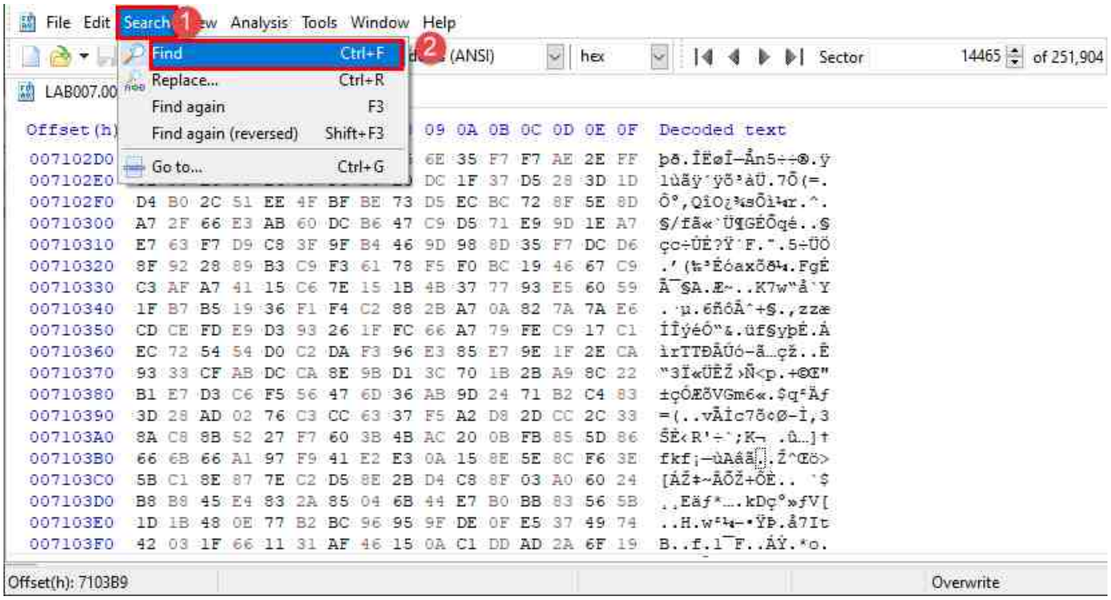
● Little endian ○ Big endian

□ Show integers in hexadecimal b

Offset(d): 0

2 Carving XLSX Files

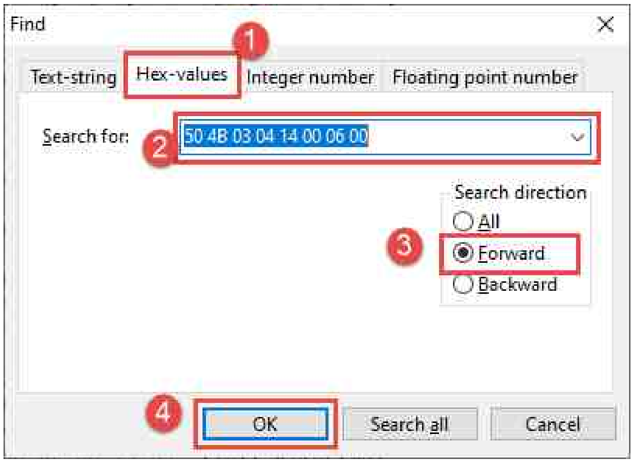
1. Now that we have that correct, let us start with the XLSX file. We will use the Find feature in HxD to jump to the beginning of the file so we can note the offset. Do this by clicking the Search dropdown menu from the menu bar and then clicking Find from the menu as highlighted in items 1 and 2 below. You can also open Find by typing Ctrl+F.



```
Offset(h)                                09 0A 0B 0C 0D 0E 0F  Decoded text
007102D0                                 6E 35 F7 F7 AE 2E FF  þð.ÎËøÎ–Ån5÷÷®.ÿ
007102E0                                 DC 1F 37 D5 28 3D 1D  1ùãÿ´ÿõ³àÜ.7Õ(=.
007102F0  D4 B0 2C 51 EE 4F BF BE 73 D5 EC BC 72 8F 5E 8D  Ô°,QîO¿¾sÕì¼r.^.
00710300  A7 2F 66 E3 AB 60 DC B6 47 C9 D5 71 E9 9D 1E A7  §/fã«`Ü¶GÉÕqé..§
00710310  E7 63 F7 D9 C8 3F 9F B4 46 9D 98 8D 35 F7 DC D6  çc÷ÙÈ?Ÿ´F.˜.5÷ÜÖ
00710320  8F 92 28 89 B3 C9 F3 61 78 F5 F0 BC 19 46 67 C9  .’(‰³ÉóaxõðÑ¼.FgÉ
00710330  C3 AF A7 41 15 C6 7E 15 1B 4B 37 77 93 E5 60 59  Ã¯§A.Æ~..K7w“å`Y
00710340  1F B7 B5 19 36 F1 F4 C2 88 2B A7 0A 82 7A 7A E6  .·µ.6ñôÂˆ+§.‚zzæ
00710350  CD CE FD E9 D3 93 26 1F FC 66 A7 79 FE C9 17 C1  ÍÎýéÓ“&.üf§yþÉ.Á
00710360  EC 72 54 54 D0 C2 DA F3 96 E3 85 E7 9E 1F 2E CA  ìrTTÐÂÚó–ã…çž..Ê
00710370  93 33 CF AB DC CA 8E 9B D1 3C 70 1B 2B A9 8C 22  “3Ï«ÜÊŽ›Ñ<p.+©Œ"
00710380  B1 E7 D3 C6 F5 56 47 6D 36 AB 9D 24 71 B2 C4 83  ±çÓÆõVGm6«.$q²Äƒ
00710390  3D 28 AD 02 76 C3 CC 63 37 F5 A2 D8 2D CC 2C 33  =(..vÃÌc7õ¢Ø-Ì,3
007103A0  8A C8 8B 52 27 F7 60 3B 4B AC 20 0B FB 85 5D 86  ŠÈ‹R'÷`;K¬ .û…]†
007103B0  66 6B 66 A1 97 F9 41 E2 E3 0A 15 8E 5E 8C F6 3E  fkf¡—ùAâã..Ž^Œö>
007103C0  5B C1 8E 87 7E C2 D5 8E 2B D4 C8 8F 03 A0 60 24  [ÁŽ‡~ÂÕŽ+ÔÈ.. `$
007103D0  B8 B8 45 E4 83 2A 85 04 6B 44 E7 B0 BB 83 56 5B  ¸¸Eäƒ*….kDç°»ƒV[
007103E0  1D 1B 48 0E 77 B2 BC 96 95 9F DE 0F E5 37 49 74  ..H.w²¼–•ŸÞ.å7It
007103F0  42 03 1F 66 11 31 AF 46 15 0A C1 DD AD 2A 6F 19  B..f.1¯F..ÁÝ.*o.
```

Offset(h): 7103B9

2. In the Find window, you can search using a variety of search methods. In this exercise, we will use the Hex-values tab to search for the hexadecimal file signatures. Let us click the Hex-values tab as highlighted as item 1 below. Now that you are in the Hex-values tab, let us 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 2 below. Ensure the radio button beside Forward is selected to ensure that it searches down from top to bottom (Since we are currently at the top). This is highlighted as item 3. Once you are done, click OK highlighted as item 4 below.

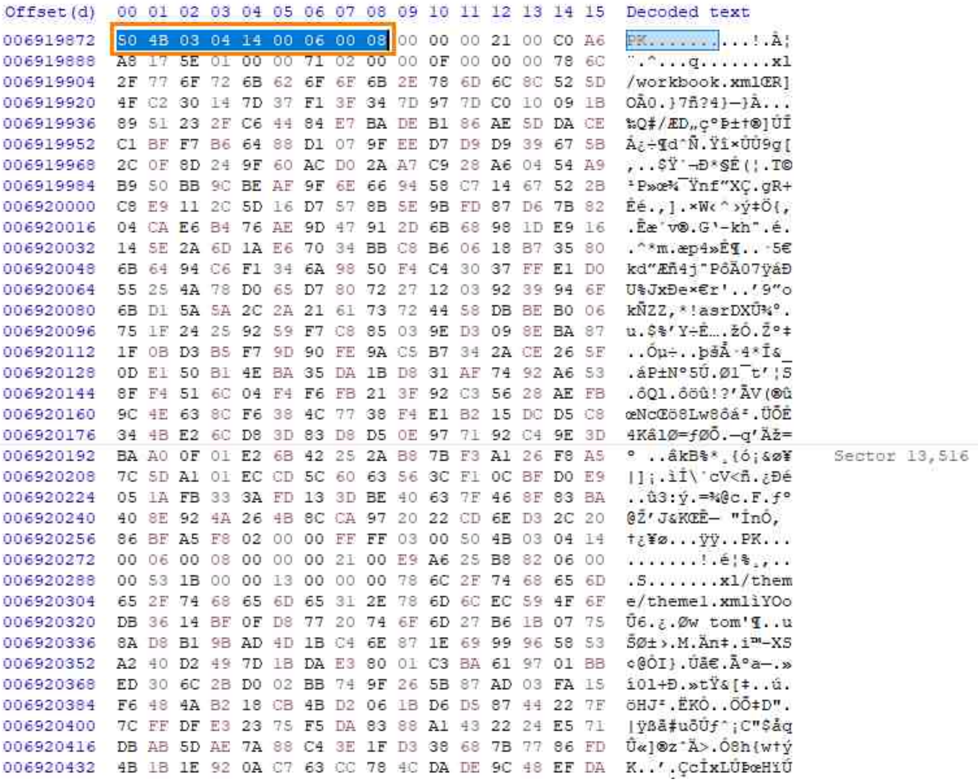


Search for: 50 4B 03 04 14 00 06 00

Search direction
○ All
● Forward
○ Backward

Hex search is not case sensitive.

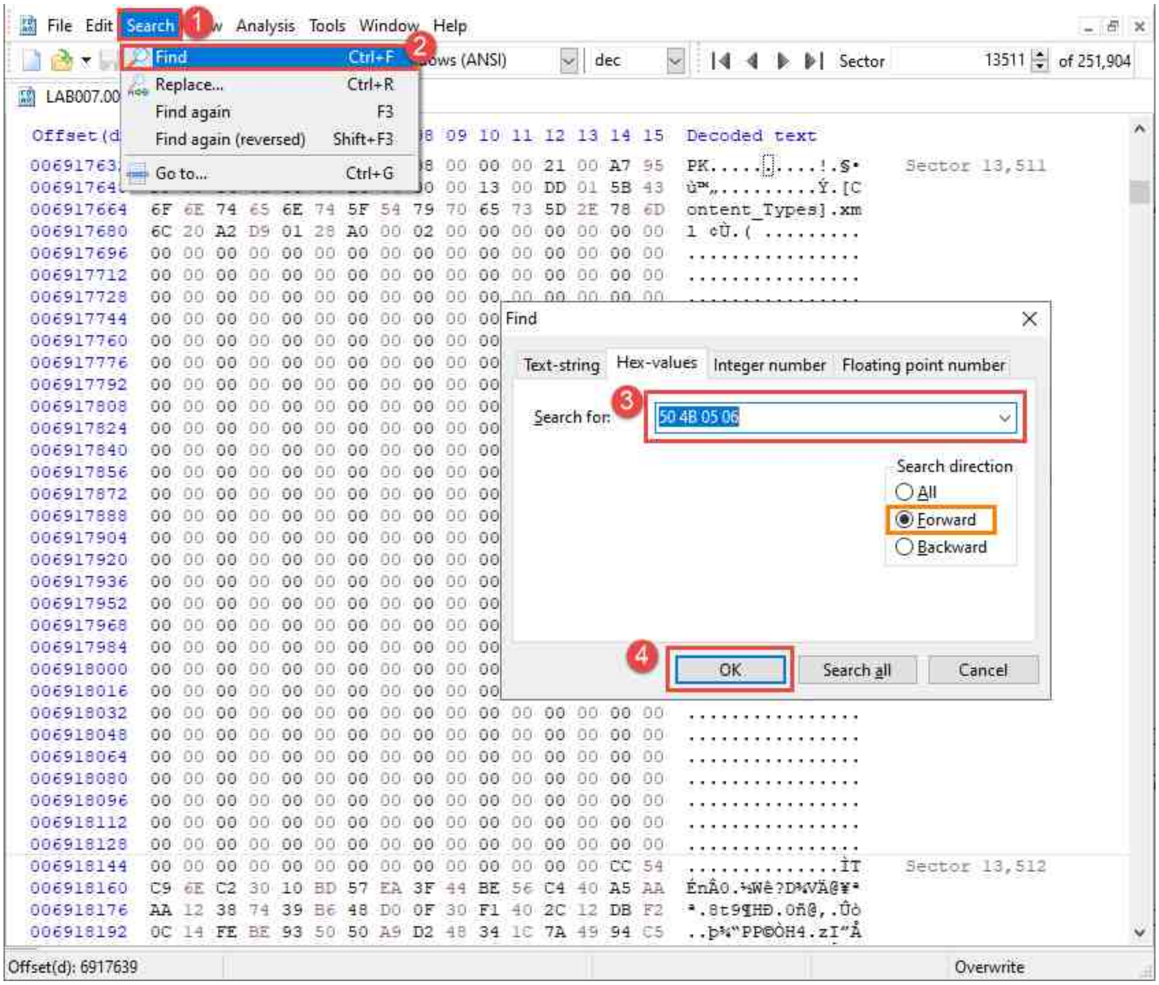
3. The search will take you to the beginning of the first Microsoft office document on the volume. As seen in the screenshot below, the offset for this document should be 6917632. Make a note of this as we will be coming back to the header to begin the highlighting.



```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text
006919872  50 4B 03 04 14 00 06 00 08 00 00 00 21 00 C0 A6  PK.........!.À¦
006919888  A8 17 5E 01 00 00 71 02 00 00 0F 00 00 00 78 6C  ¨.^...q.......xl
006919904  2F 77 6F 72 6B 62 6F 6F 6B 2E 78 6D 6C 8C 52 5D  /workbook.xmlŒR]
006919920  4F C2 30 14 7D 37 F1 3F 34 7D 97 7D C0 10 09 1B  OÂ0.}7ñ?4}—}À...
006919936  89 51 23 2F C6 44 84 E7 BA DE B1 86 AE 5D DA CE  ‰Q#/ÆD„ç°Þ±†®]ÚÎ
006919952  C1 BF F7 B6 64 88 D1 07 9F EE D7 D9 D9 39 67 5B  Á¿÷¶dˆÑ.ŸîרÙ9g[
006919968  2C 0F 8D 24 9F 60 AC D0 2A A7 C9 28 A6 04 54 A9  ,..$Ÿ`¬Ð*§É(¦.T©
006919984  B9 50 BB 9C BE AF 9F 6E 66 94 58 C7 14 67 52 2B  ¹P»œ¾¯Ÿnf”XÇ.gR+
006920000  C8 E9 11 2C 5D 16 D7 57 8B 5E 9B FD 87 D6 7B 82  Èé.,].×W‹^›ý‡Ö{‚
006920016  04 CA E6 B4 76 AE 9D 47 91 2D 6B 68 98 1D E9 16  .Êæ´v®.G‘-kh˜.é.
006920032  14 5E 2A 6D 1A E6 70 34 BB C8 B6 06 18 B7 35 80  .^*m.æp4»È¶..·5€
006920048  6B 64 94 C6 F1 34 6A 98 50 F4 C4 30 37 FF E1 D0  kd”Æñ4j˜PôÄ07ÿáÐ
006920064  55 25 4A 78 D0 65 D7 80 72 27 12 03 92 39 94 6F  U%JxÐe×€r'..’9”o
006920080  6B D1 5A 5A 2C 2A 21 61 73 72 44 58 DB BE B0 06  kÑZZ,*!asrDXÛ¾°.
006920096  75 1F 24 25 92 59 F7 C8 85 03 9E D3 09 8E BA 87  u.$%’Y÷È….žÓ.Ž°‡
006920112  1F 0B D3 B5 F7 9D 90 FE 9A C5 B7 34 2A CE 26 5F  ..Óµ÷..þšÅ·4*Î&_
006920128  0D E1 50 B1 4E BA 35 DA 1B D8 31 AF 74 92 A6 53  .áP±N°5Ú.Ø1¯t’¦S
006920144  8F F4 51 6C 04 F4 F6 FB 21 3F 92 C3 56 28 AE FB  .ôQl.ôöû!?’ÃV(®û
006920160  9C 4E 63 8C F6 38 4C 77 38 F4 E1 B2 15 DC D5 C8  œNcŒö8Lw8ôá².ÜÕÈ
006920176  34 4B E2 6C D8 3D 83 D8 D5 0E 97 71 92 C4 9E 3D  4KâlØ=ƒØÕ.—q’Äž=
006920192  BA A0 0F 01 E2 6B 42 25 2A B8 7B F3 A1 26 F8 A5  ° ..âkB%*¸{ó¡&ø¥      Sector 13,516
006920208  7C 5D A1 01 EC CD 5C 60 63 56 3C F1 0C BF D0 E9  |]¡.ìÍ\`cV<ñ.¿Ðé
006920224  05 1A FB 33 3A FD 13 3D BE 40 63 7F 46 8F 83 BA  ..û3:ý.=¾@c.F.ƒ°
006920240  40 8E 92 4A 26 4B 8C CA 97 20 22 CD 6E D3 2C 20  @Ž’J&KŒÊ— "ÍnÓ,
006920256  86 BF A5 F8 02 00 00 FF FF 03 00 50 4B 03 04 14  †¿¥ø...ÿÿ..PK...
006920272  00 06 00 08 00 00 00 21 00 E9 A6 25 B8 82 06 00  .......!.é¦%¸‚..
006920288  00 53 1B 00 00 13 00 00 00 78 6C 2F 74 68 65 6D  .S.......xl/them
006920304  65 2F 74 68 65 6D 65 31 2E 78 6D 6C EC 59 4F 6F  e/theme1.xmlìYOo
006920320  DB 36 14 BF 0F D8 77 20 74 6F 6D 27 B6 1B 07 75  Û6.¿.Øw tom'¶..u
006920336  8A D8 B1 9B AD 4D 1B C4 6E 87 1E 69 99 96 58 53  ŠØ±›.M.Än‡.i™–XS
006920352  A2 40 D2 49 7D 1B DA E3 80 01 C3 BA 61 97 01 BB  ¢@ÒI}.Úã€.Ã°a—.»
006920368  ED 30 6C 2B D0 02 BB 74 9F 26 5B 87 AD 03 FA 15  í0l+Ð.»tŸ&[‡..ú.
006920384  F6 48 4A B2 18 CB 4B D2 06 1B D6 D5 87 44 22 7F  öHJ².ËKÒ..ÖÕ‡D".
006920400  7C FF DF E3 23 75 F5 DA 83 88 A1 43 22 24 E5 71  |ÿßã#uõÚƒˆ¡C"$åq
006920416  DB AB 5D AE 7A 88 C4 3E 1F D3 38 68 7B 77 86 FD  Û«]®zˆÄ>.Ó8h{w†ý
006920432  4B 1B 1E 92 0A C7 63 CC 78 4C DA DE 9C 48 EF DA  K..’.ÇcÌxLÚÞœHïÚ
```

The offset for this file is unique to this FEF and would be different for other drives.

4. Now, let us jump to the footer of this file. As seen in the earlier table, the footer for the Microsoft Office document is 50 4B 05 06 (PK..) followed by 18 additional bytes. This means we will search for the hexadecimal value and add 18 bytes to it to get the offset of the footer. Let us open Find by clicking the Search dropdown menu from the menu bar and then clicking Find from the menu, as highlighted in items 1 and 2 below. You can also open Find by typing Ctrl+F. Once the Find window is open, type `50 4B 05 06` as highlighted in item 3 below. Ensure that the radio button beside Forward is selected, and then click OK as highlighted below.



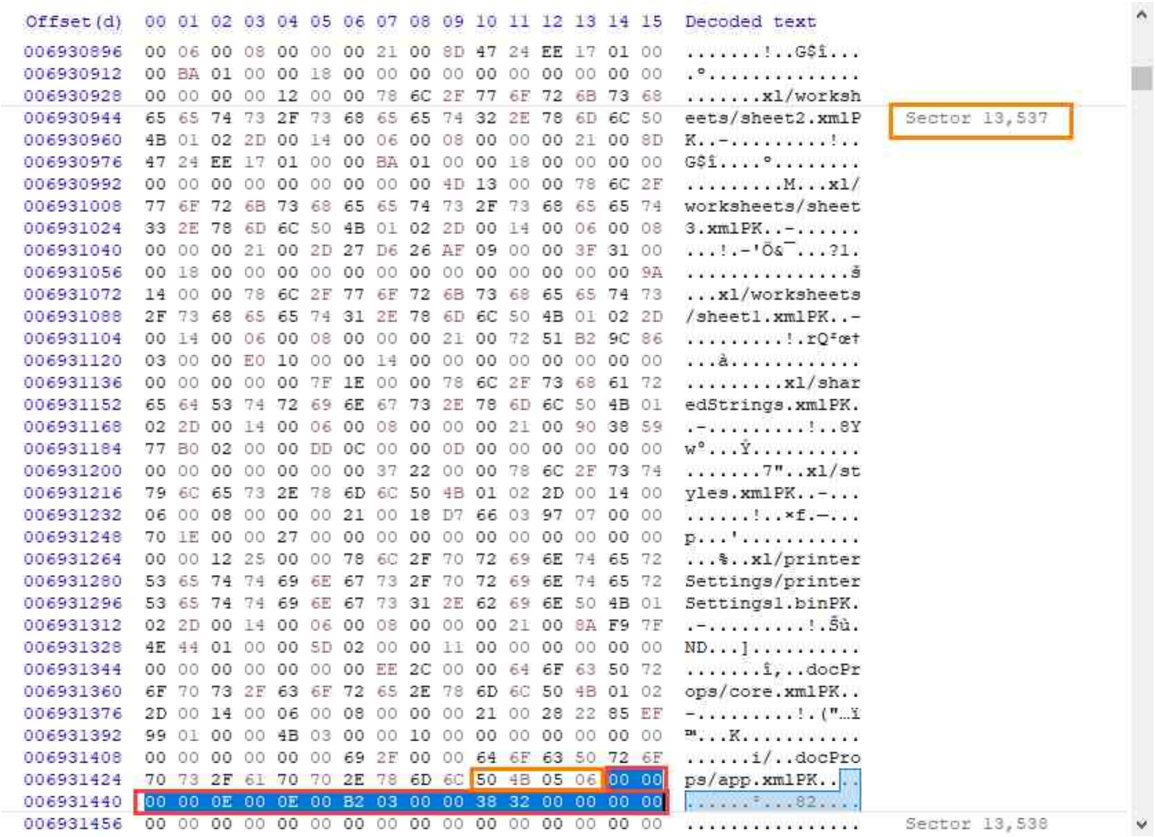
Search for: 50 4B 05 06

Search direction
○ All
● Forward
○ Backward

```
Offset(d                                   8 09 10 11 12 13 14 15   Decoded text
00691763                                   8 00 00 00 21 00 A7 95   PK.....:....!.§•      Sector 13,511
00691764                                   0 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   ................
006917712   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006917728   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006917744   00 00 00 00 00 00 00 00 00 00 00
006917760   00 00 00 00 00 00 00 00 00 00 00
006917776   00 00 00 00 00 00 00 00 00 00 00
006917792   00 00 00 00 00 00 00 00 00 00 00
006917808   00 00 00 00 00 00 00 00 00 00 00
006917824   00 00 00 00 00 00 00 00 00 00 00
006917840   00 00 00 00 00 00 00 00 00 00 00
006917856   00 00 00 00 00 00 00 00 00 00 00
006917872   00 00 00 00 00 00 00 00 00 00 00
006917888   00 00 00 00 00 00 00 00 00 00 00
006917904   00 00 00 00 00 00 00 00 00 00 00
006917920   00 00 00 00 00 00 00 00 00 00 00
006917936   00 00 00 00 00 00 00 00 00 00 00
006917952   00 00 00 00 00 00 00 00 00 00 00
006917968   00 00 00 00 00 00 00 00 00 00 00
006917984   00 00 00 00 00 00 00 00 00 00 00
006918000   00 00 00 00 00 00 00 00 00 00 00
006918016   00 00 00 00 00 00 00 00 00 00 00
006918032   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006918048   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006918064   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006918080   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006918096   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006918112   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006918128   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006918144   00 00 00 00 00 00 00 00 00 00 00 00 00 00 CC 54   ..............ÌT      Sector 13,512
006918160   C9 6E C2 30 10 BD 57 EA 3F 44 BE 56 C4 40 A5 AA   ÉnÂ0.½Wê?D¾VÄ@¥ª
006918176   AA 12 38 74 39 B6 48 D0 0F 30 F1 40 2C 12 DB F2   ª.8t9¶HÐ.0ñ@,.Ûò
006918192   0C 14 FE BE 93 50 50 A9 D2 48 34 1C 7A 49 94 C5   ..þ¾“PP©ÒH4.zI”Å
```

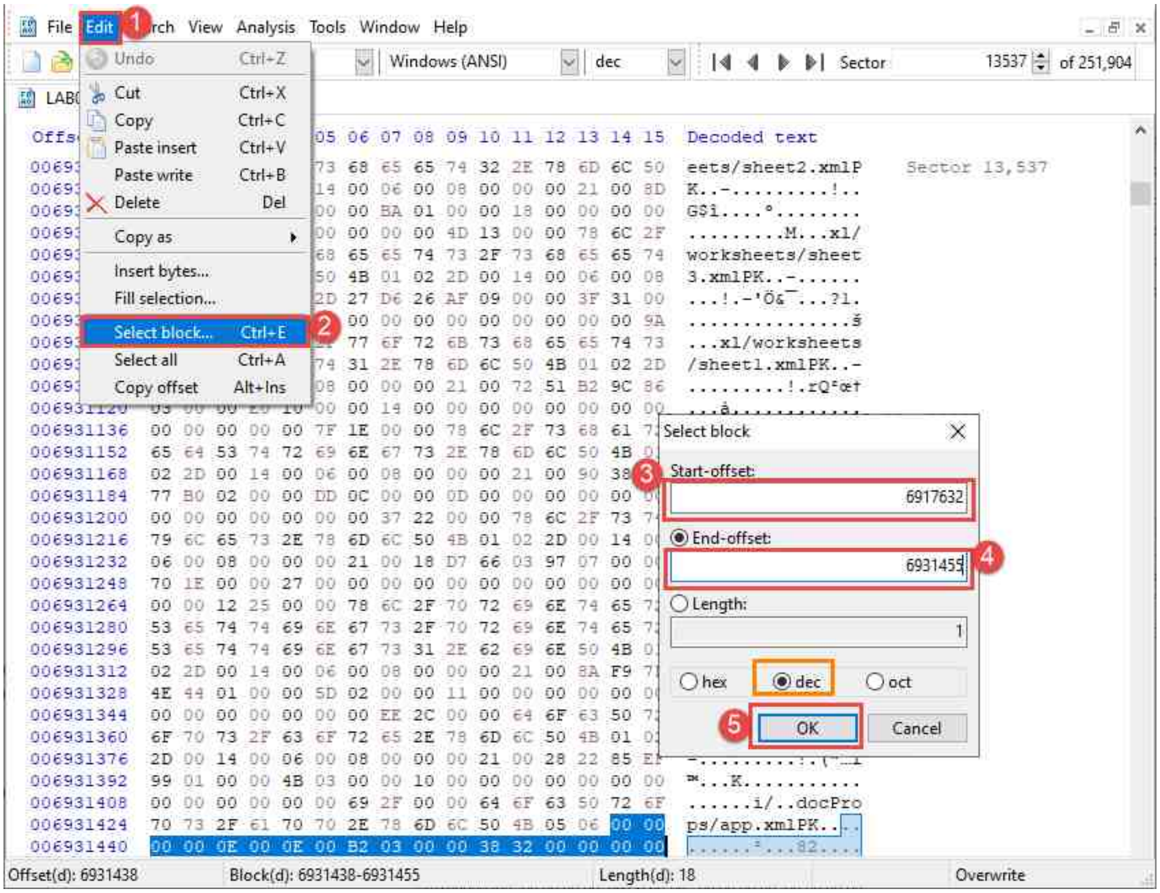
Offset(d): 6917639

5. You will be taken to the footer of this document. Now, look for the offset of the last character in our search term 0x50 4B 05 06. The offset for the 0x06 value should be 6931437. Now let us add 18 bytes to that value, which is equal to 6931455. Note this value as it is the location of the end of this file and sector 13,537.



```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text
006930896  00 06 00 08 00 00 00 21 00 8D 47 24 EE 17 01 00  ........!..G$î...
006930912  00 BA 01 00 00 18 00 00 00 00 00 00 00 00 00 00  .º..............
006930928  00 00 00 00 12 00 00 78 6C 2F 77 6F 72 6B 73 68  .......xl/worksh
006930944  65 65 74 73 2F 73 68 65 65 74 32 2E 78 6D 6C 50  eets/sheet2.xmlP   Sector 13,537
006930960  4B 01 02 2D 00 14 00 06 00 08 00 00 00 21 00 8D  K..-.........!..
006930976  47 24 EE 17 01 00 00 BA 01 00 00 18 00 00 00 00  G$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 00  w°...Ý..........
006931200  00 00 00 00 00 00 00 37 22 00 00 78 6C 2F 73 74  .......7"..xl/st
006931216  79 6C 65 73 2E 78 6D 6C 50 4B 01 02 2D 00 14 00  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 13,538
```

6. Now that you have the offsets, let us use the Select block feature to highlight the Start-offset and End-offset of the file. Let us open Select block by clicking the Edit dropdown menu from the menu bar and then clicking Select block from the menu as highlighted in items 1 and 2 below. You can also open Select block by typing Ctrl+E. Once the Select block window is open, type the Start-offset `6917632` and the End-offset `6931455` as highlighted in items 3 and 4 below. Ensure that the radio button beside dec is selected, and then click OK as highlighted below.



```
Offs                          05 06 07 08 09 10 11 12 13 14 15  Decoded text
00693                         73 68 65 65 74 32 2E 78 6D 6C 50  eets/sheet2.xmlP    Sector 13,537
00693                         14 00 06 00 08 00 00 00 21 00 8D  K..-.........!..
00693                         00 00 BA 01 00 00 18 00 00 00 00  G$i....°........
00693                         00 00 00 00 4D 13 00 00 78 6C 2F  .........M...xl/
00693                         68 65 65 74 73 2F 73 68 65 65 74  worksheets/sheet
00693                         50 4B 01 02 2D 00 14 00 06 00 08  3.xmlPK..-......
00693                         2D 27 D6 26 AF 09 00 00 3F 31 00  ...!.-'Ö&¯...?1.
00693                         00 00 00 00 00 00 00 00 00 00 9A  ...............š
00693                            77 6F 72 6B 73 68 65 65 74 73  ...xl/worksheets
00693                         74 31 2E 78 6D 6C 50 4B 01 02 2D  /sheet1.xmlPK..-
00693                         08 00 00 00 21 00 72 51 B2 9C 86  .........!.rQ²œ†
006931120                     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 7
006931152  65 64 53 74 72 69 6E 67 73 2E 78 6D 6C 50 4B 0
006931168  02 2D 00 14 00 06 00 08 00 00 00 21 00 90 38
006931184  77 B0 02 00 00 DD 0C 00 00 0D 00 00 00 00 00 0
006931200  00 00 00 00 00 00 00 37 22 00 00 78 6C 2F 73 7
006931216  79 6C 65 73 2E 78 6D 6C 50 4B 01 02 2D 00 14 0
006931232  06 00 08 00 00 00 21 00 18 D7 66 03 97 07 00 0
006931248  70 1E 00 00 27 00 00 00 00 00 00 00 00 00 00 0
006931264  00 00 12 25 00 00 78 6C 2F 70 72 69 6E 74 65 7
006931280  53 65 74 74 69 6E 67 73 2F 70 72 69 6E 74 65 7
006931296  53 65 74 74 69 6E 67 73 31 2E 62 69 6E 50 4B 0
006931312  02 2D 00 14 00 06 00 08 00 00 00 21 00 8A F9 7
006931328  4E 44 01 00 00 5D 02 00 00 11 00 00 00 00 00 0
006931344  00 00 00 00 00 00 00 EE 2C 00 00 64 6F 63 50 7
006931360  6F 70 73 2F 63 6F 72 65 2E 78 6D 6C 50 4B 01 0
006931376  2D 00 14 00 06 00 08 00 00 00 21 00 28 22 85 E
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....
```

Offset(d): 6931438 | Block(d): 6931438-6931455 | Length(d): 18

Select block

Start-offset: 6917632

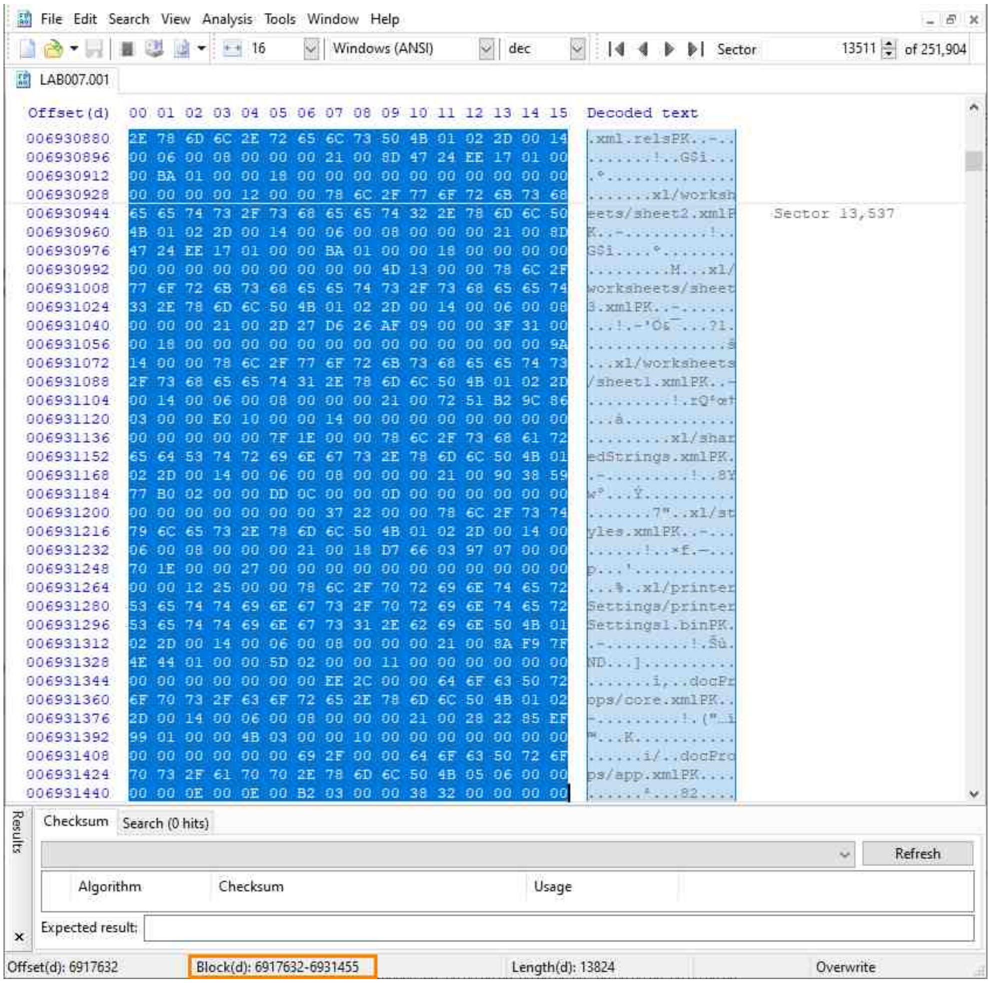
● End-offset: 6931455

○ Length: 1

○ hex ● dec ○ oct

Ensure you delete all spaces behind the Start-offset and End-offset values before clicking OK.

7. Select block will highlight from the file header of the Microsoft Office file we identified earlier. Use the Block value in the status bar highlighted below to observe the Start and End offsets, which marks the length of the file. The Block value should look like this Block(d): 6917632-6931455.

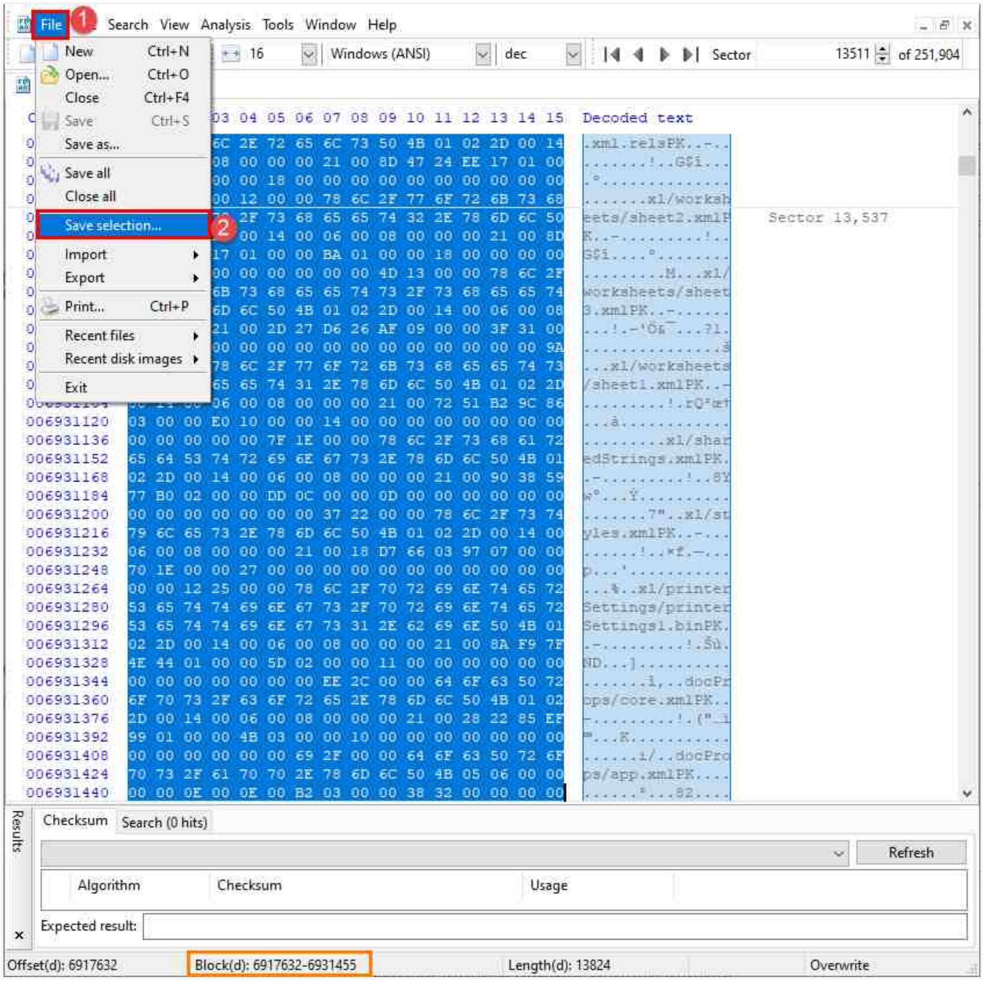


```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15   Decoded text

006930880  2E 78 6D 6C 2E 72 65 6C 73 50 4B 01 02 2D 00 14   .xml.relsPK..-..
006930896  00 06 00 08 00 00 00 21 00 8D 47 24 EE 17 01 00   .......!..G$i...
006930912  00 BA 01 00 00 18 00 00 00 00 00 00 00 00 00 00   .°..............
006930928  00 00 00 00 12 00 00 78 6C 2F 77 6F 72 6B 73 68   .......xl/worksh
006930944  65 65 74 73 2F 73 68 65 65 74 32 2E 78 6D 6C 50   eets/sheet2.xmlP      Sector 13,537
006930960  4B 01 02 2D 00 14 00 06 00 08 00 00 00 21 00 8D   K..-.........!..
006930976  47 24 EE 17 01 00 00 BA 01 00 00 18 00 00 00 00   G$i....°........
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 00   w°...Ý..........
006931200  00 00 00 00 00 00 00 37 22 00 00 78 6C 2F 73 74   .......7"..xl/st
006931216  79 6C 65 73 2E 78 6D 6C 50 4B 01 02 2D 00 14 00   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....
```

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

8. Great, that was not too hard, was it? Let us save this selection as a file by browsing to the File dropdown menu from the menu bar and clicking Save Selection as highlighted in items 1 and 2 below. This will open the Save selection as window.



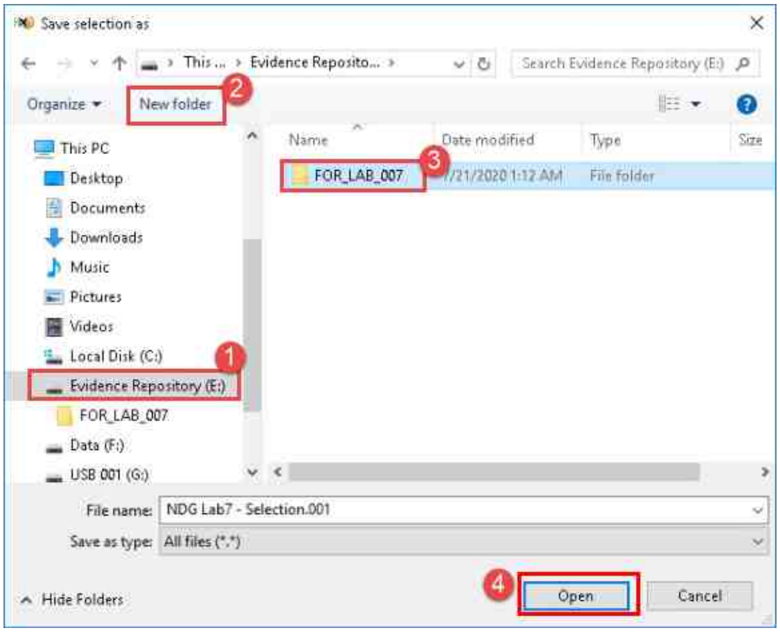
16 | Windows (ANSI) | dec | Sector 13511 of 251,904

```
           03 04 05 06 07 08 09 10 11 12 13 14 15   Decoded text
           6C 2E 72 65 6C 73 50 4B 01 02 2D 00 14   .xml.relsPK..-..
           08 00 00 00 21 00 8D 47 24 EE 17 01 00   ........!..G$î...
           00 00 18 00 00 00 00 00 00 00 00 00 00   .°..............
           00 12 00 00 78 6C 2F 77 6F 72 6B 73 68   ........xl/worksh
              2F 73 68 65 65 74 32 2E 78 6D 6C 50   eets/sheet2.xmlP    Sector 13,537
              00 14 00 06 00 08 00 00 00 21 00 8D   K..-.........!..
           17 01 00 00 BA 01 00 00 18 00 00 00 00   G$î....°........
           00 00 00 00 00 00 4D 13 00 00 78 6C 2F   .........M...xl/
           6B 73 68 65 65 74 73 2F 73 68 65 65 74   worksheets/sheet
           6D 6C 50 4B 01 02 2D 00 14 00 06 00 08   3.xmlPK..-......
           21 00 2D 27 D6 26 AF 09 00 00 3F 31 00   ...!.-'Ö&¯...?1.
           00 00 00 00 00 00 00 00 00 00 00 00 9A   ...............š
           78 6C 2F 77 6F 72 6B 73 68 65 65 74 73   ...xl/worksheets
           65 65 74 31 2E 78 6D 6C 50 4B 01 02 2D   /sheet1.xmlPK..-
           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 00   w°...Ý..........
006931200  00 00 00 00 00 00 00 37 22 00 00 78 6C 2F 73 74   .......7"..xl/st
006931216  79 6C 65 73 2E 78 6D 6C 50 4B 01 02 2D 00 14 00   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....
```

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

Please ensure that you select Save Selection and NOT Save as.

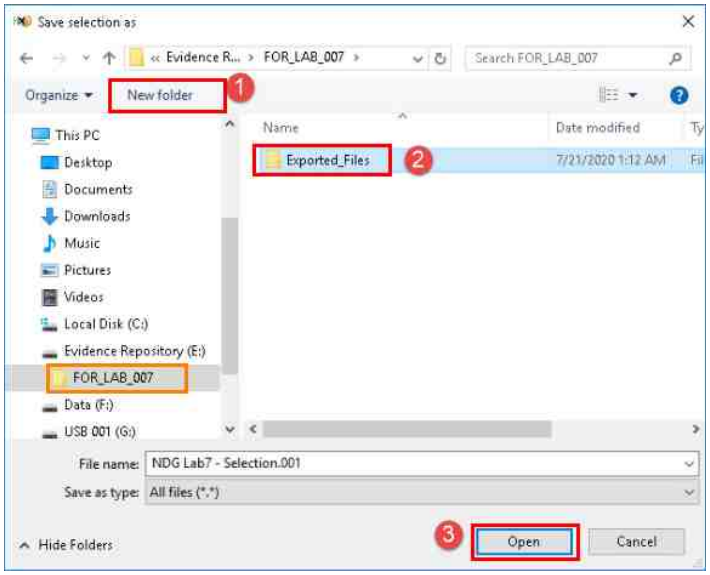
9. In the Save selection as window, we can browse to the desired location and save the file. Let us do this by browsing to the (E:) drive labeled Evidence Repository, click the Make New Folder button, then name the folder `FOR_LAB_007` and click Open as highlighted in items 1, 2, 3, and 4, respectively.



File name: NDG Lab7 - Selection.001

Save as type: All files (*.*)

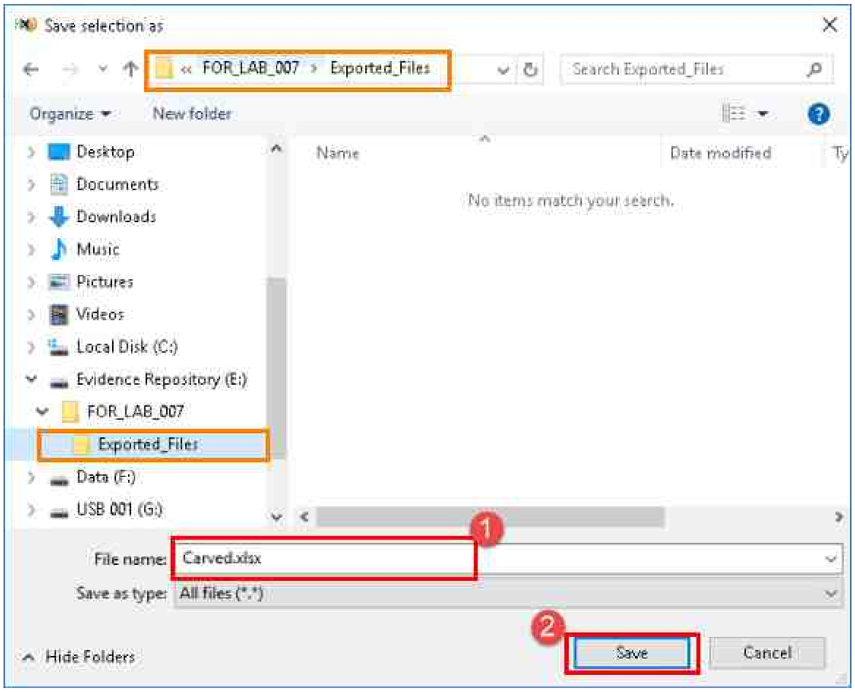
10. You should now be inside the folder FOR_LAB_007. Let us create another folder to store the carved file. Click Make New Folder button again as highlighted in item 1. Name this new folder `Exported_Files` as highlighted in item 2 and then click Open as highlighted at item 3 below.



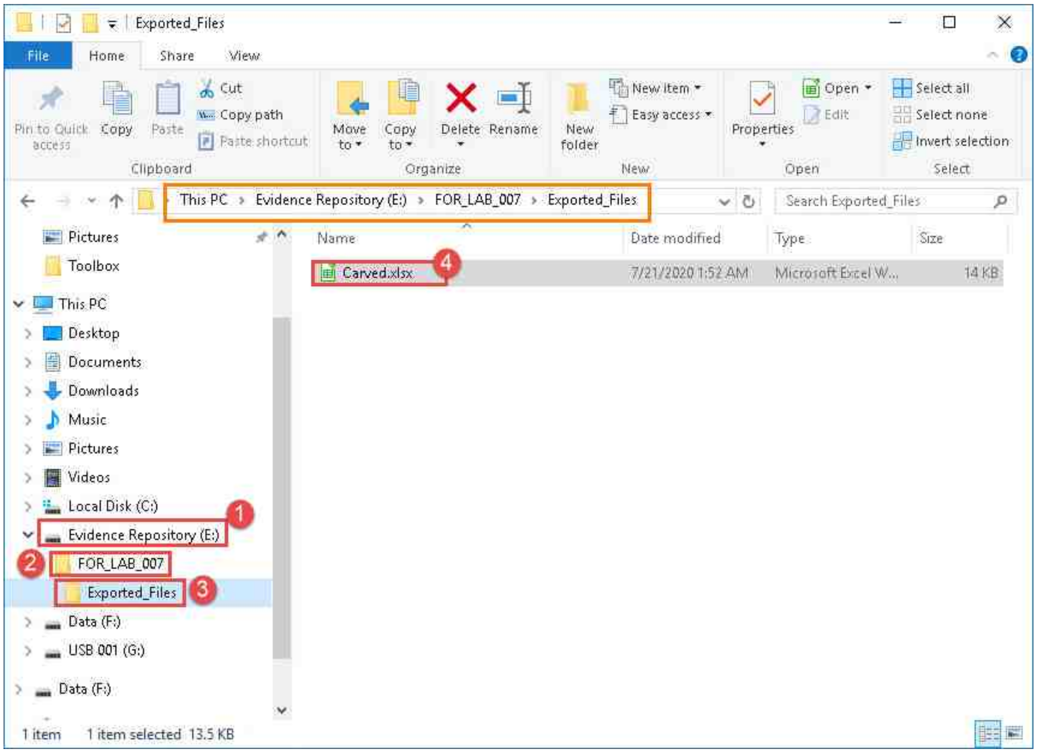
File name: NDG Lab7 - Selection.001

Save as type: All files (*.*)

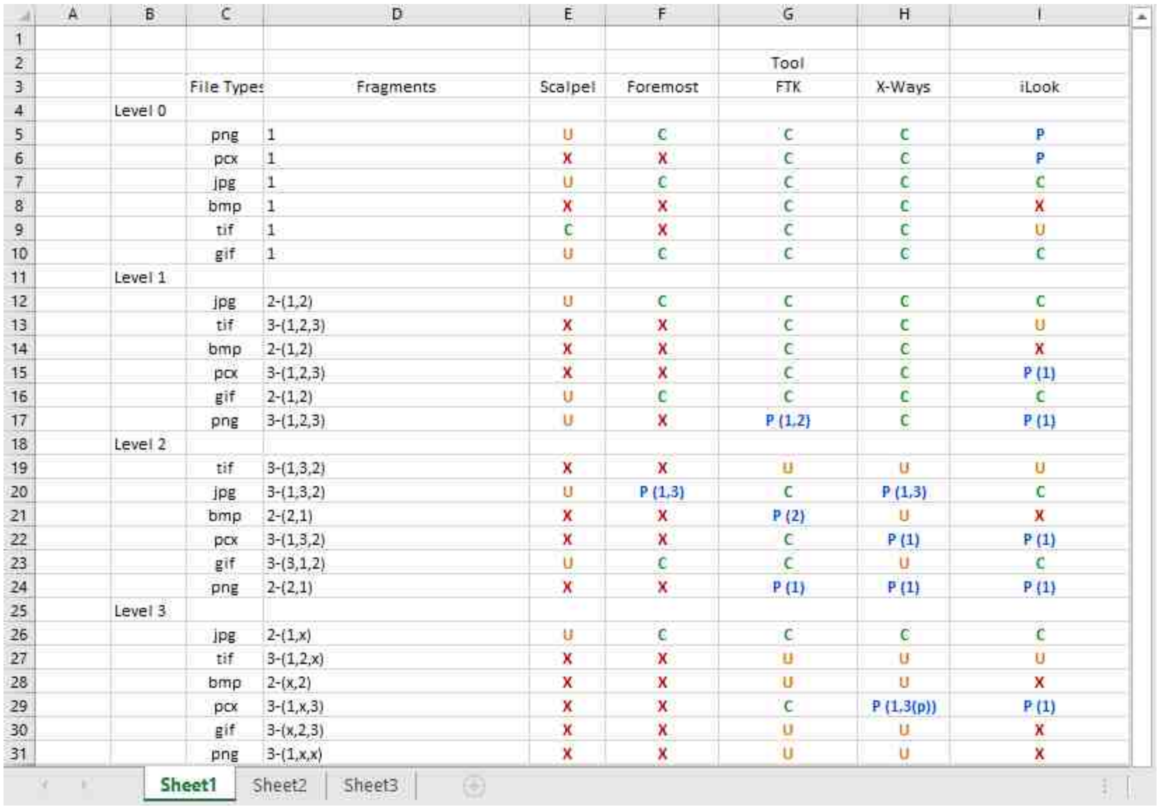
11. Now that we are in the Exported_Files folder, let us save the file. To do this, type the name `Carved.xlsx` and then click Save as highlighted in items 1 and 2 below.



12. Now browse to the location of the file by opening Windows File Explorer and browsing to the path Evidence Repository (E:) > FOR_LAB_007 > Exported_Files and double-clicking the file you saved, called Carved.xlsx.



13. If you successfully carved the file, it should look like the one below. The file should open without any errors, which would mean you successfully carved the file.

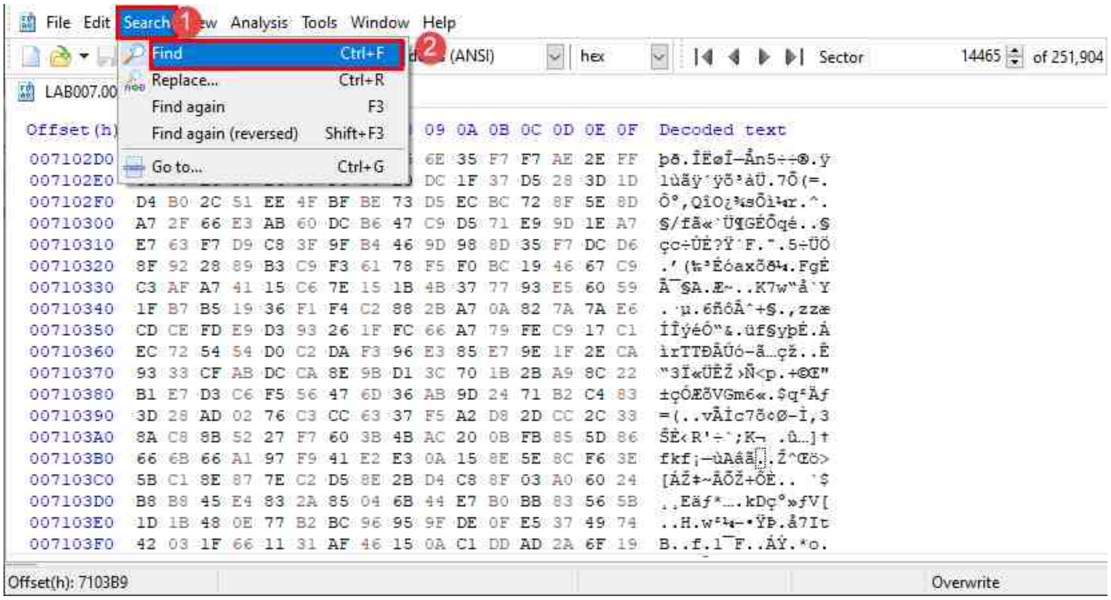


	A	B	C	D	E	F	G	H	I
1									
2							Tool		
3			File Types	Fragments	Scalpel	Foremost	FTK	X-Ways	iLook
4		Level 0							
5			png	1	U	C	C	C	P
6			pcx	1	X	X	C	C	P
7			jpg	1	U	C	C	C	C
8			bmp	1	X	X	C	C	X
9			tif	1	C	X	C	C	U
10			gif	1	U	C	C	C	C
11		Level 1							
12			jpg	2-(1,2)	U	C	C	C	C
13			tif	3-(1,2,3)	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

Note the size of the carved file. The full file size is 14KB. If the file you carve is smaller than this size the file may not open. Simply review the instructions again and see where you went wrong.

3 Carving PDF Files

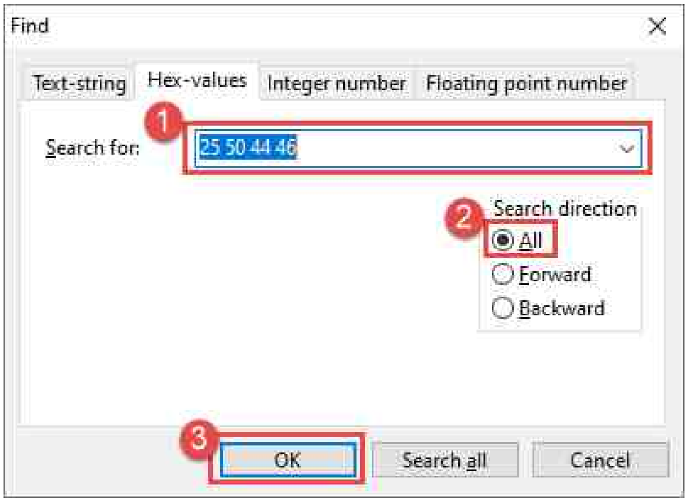
1. Now let us carve a couple more filetypes to get you some practice. HxD should still be open; if not, reopen it and open Find by clicking the Search dropdown menu from the menu bar and then clicking Find from the menu as highlighted in items 1 and 2 below. You can also open Find by typing Ctrl+F.



```
Offset(h)                                    09 0A 0B 0C 0D 0E 0F  Decoded text
007102D0                                     6E 35 F7 F7 AE 2E FF  þð.ÎËøÎ–Ån5÷÷®.ÿ
007102E0                                     DC 1F 37 D5 28 3D 1D  lùãÿ´ÿõ³àÜ.7Õ(=.
007102F0  D4 B0 2C 51 EE 4F BF BE 73 D5 EC BC 72 8F 5E 8D  Ô°,QîO¿¾sÕì¼r.^.
00710300  A7 2F 66 E3 AB 60 DC B6 47 C9 D5 71 E9 9D 1E A7  §/fã«`Ü¶GÉÕqé..§
00710310  E7 63 F7 D9 C8 3F 9F B4 46 9D 98 8D 35 F7 DC D6  çc÷ÙÈ?Ÿ´F.˜.5÷ÜÖ
00710320  8F 92 28 89 B3 C9 F3 61 78 F5 F0 BC 19 46 67 C9  .’(‰³ÉóaxõðĽ.FgÉ
00710330  C3 AF A7 41 15 C6 7E 15 1B 4B 37 77 93 E5 60 59  Ã¯§A.Æ~..K7w“å`Y
00710340  1F B7 B5 19 36 F1 F4 C2 88 2B A7 0A 82 7A 7A E6  .·µ.6ñôÂˆ+§.‚zzæ
00710350  CD CE FD E9 D3 93 26 1F FC 66 A7 79 FE C9 17 C1  ÍÎýéÓ“&.üf§ypÉ.Á
00710360  EC 72 54 54 D0 C2 DA F3 96 E3 85 E7 9E 1F 2E CA  ìrTTÐÂÚó–ã…çž..Ê
00710370  93 33 CF AB DC CA 8E 9B D1 3C 70 1B 2B A9 8C 22  “3Ï«ÜÊŽ›Ñ<p.+©Œ"
00710380  B1 E7 D3 C6 F5 56 47 6D 36 AB 9D 24 71 B2 C4 83  ±çÓÆõVGm6«.$q²Äƒ
00710390  3D 28 AD 02 76 C3 CC 63 37 F5 A2 D8 2D CC 2C 33  =(..vÃÌc7õ¢Ø-Ì,3
007103A0  8A C8 8B 52 27 F7 60 3B 4B AC 20 0B FB 85 5D 86  ŠÈ‹R'÷`;K¬ .û…]†
007103B0  66 6B 66 A1 97 F9 41 E2 E3 0A 15 8E 5E 8C F6 3E  fkf¡—ùAâã..Ž^Œö>
007103C0  5B C1 8E 87 7E C2 D5 8E 2B D4 C8 8F 03 A0 60 24  [ÁŽ‡~ÂÕŽ+ÔÈ.. `$
007103D0  B8 B8 45 E4 83 2A 85 04 6B 44 E7 B0 BB 83 56 5B  ¸¸Eäƒ*….kDç°»ƒV[
007103E0  1D 1B 48 0E 77 B2 BC 96 95 9F DE 0F E5 37 49 74  ..H.w²¼–•ŸÞ.å7It
007103F0  42 03 1F 66 11 31 AF 46 15 0A C1 DD AD 2A 6F 19  B..f.1¯F..ÁÝ.*o.

Offset(h): 7103B9
```

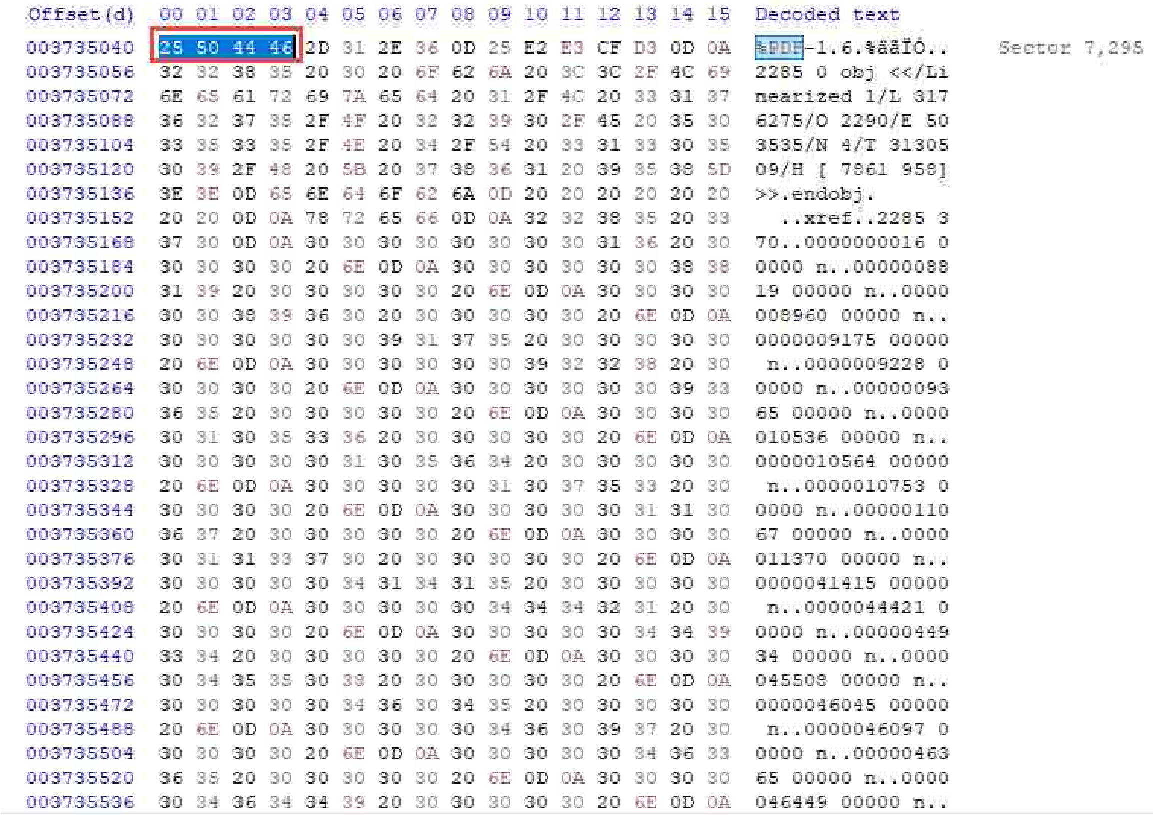
2. Once the Find window is open, type `25 50 44 46` as highlighted at item 1 below. This is the file signature for PDF files. Let us click the radio button beside All this time as the file we are looking for is located before the previous XLSX file we carved. This can be seen in item 2 below. Once everything is correct, then click OK highlighted as item 3 below to start the search.



Search for: 25 50 44 46

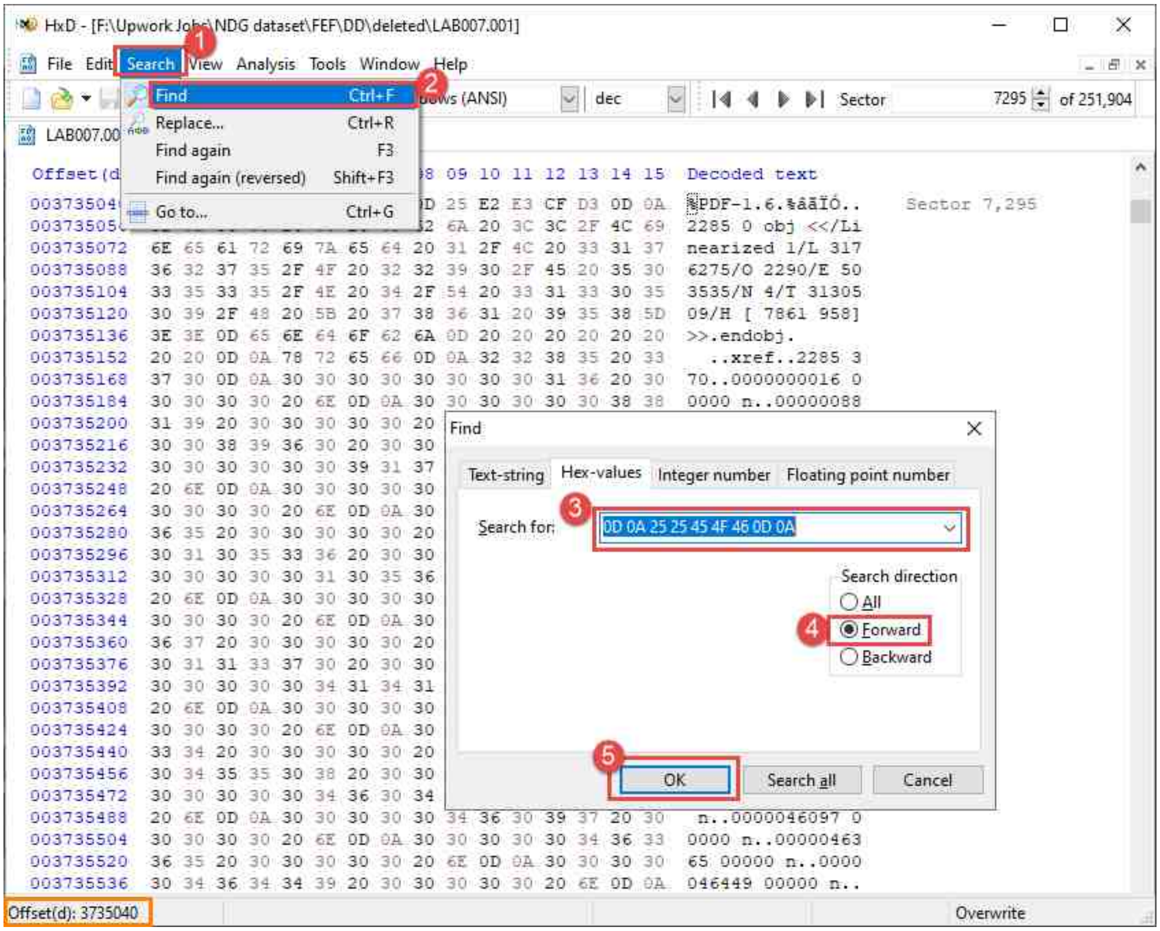
Search direction
● All
○ Forward
○ Backward

3. The search will take you to the beginning of the PDF document on the volume. As seen in the screenshot below, the offset for this document should be 3735040. As you did before, make a note of this as we will be coming back to the header to begin the highlighting.



```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text
003735040  25 50 44 46 2D 31 2E 36 0D 25 E2 E3 CF D3 0D 0A  %PDF-1.6.%âãÏÓ..     Sector 7,295
003735056  32 32 38 35 20 30 20 6F 62 6A 20 3C 3C 2F 4C 69  2285 0 obj <</Li
003735072  6E 65 61 72 69 7A 65 64 20 31 2F 4C 20 33 31 37  nearized 1/L 317
003735088  36 32 37 35 2F 4F 20 32 32 39 30 2F 45 20 35 30  6275/O 2290/E 50
003735104  33 35 33 35 2F 4E 20 34 2F 54 20 33 31 33 30 35  3535/N 4/T 31305
003735120  30 39 2F 48 20 5B 20 37 38 36 31 20 39 35 38 5D  09/H [ 7861 958]
003735136  3E 3E 0D 65 6E 64 6F 62 6A 0D 20 20 20 20 20 20  >>.endobj.
003735152  20 20 0D 0A 78 72 65 66 0D 0A 32 32 38 35 20 33    ..xref..2285 3
003735168  37 30 0D 0A 30 30 30 30 30 30 30 30 31 36 20 30  70..0000000016 0
003735184  30 30 30 30 20 6E 0D 0A 30 30 30 30 30 30 38 38  0000 n..00000088
003735200  31 39 20 30 30 30 30 30 20 6E 0D 0A 30 30 30 30  19 00000 n..0000
003735216  30 30 38 39 36 30 20 30 30 30 30 30 20 6E 0D 0A  008960 00000 n..
003735232  30 30 30 30 30 30 39 31 37 35 20 30 30 30 30 30  0000009175 00000
003735248  20 6E 0D 0A 30 30 30 30 30 30 39 32 32 38 20 30   n..0000009228 0
003735264  30 30 30 30 20 6E 0D 0A 30 30 30 30 30 30 39 33  0000 n..00000093
003735280  36 35 20 30 30 30 30 30 20 6E 0D 0A 30 30 30 30  65 00000 n..0000
003735296  30 31 30 35 33 36 20 30 30 30 30 30 20 6E 0D 0A  010536 00000 n..
003735312  30 30 30 30 30 31 30 35 36 34 20 30 30 30 30 30  0000010564 00000
003735328  20 6E 0D 0A 30 30 30 30 30 31 30 37 35 33 20 30   n..0000010753 0
003735344  30 30 30 30 20 6E 0D 0A 30 30 30 30 30 31 31 30  0000 n..00000110
003735360  36 37 20 30 30 30 30 30 20 6E 0D 0A 30 30 30 30  67 00000 n..0000
003735376  30 31 31 33 37 30 20 30 30 30 30 30 20 6E 0D 0A  011370 00000 n..
003735392  30 30 30 30 30 34 31 34 31 35 20 30 30 30 30 30  0000041415 00000
003735408  20 6E 0D 0A 30 30 30 30 30 34 34 34 32 31 20 30   n..0000044421 0
003735424  30 30 30 30 20 6E 0D 0A 30 30 30 30 30 34 34 39  0000 n..00000449
003735440  33 34 20 30 30 30 30 30 20 6E 0D 0A 30 30 30 30  34 00000 n..0000
003735456  30 34 35 35 30 38 20 30 30 30 30 30 20 6E 0D 0A  045508 00000 n..
003735472  30 30 30 30 30 34 36 30 34 35 20 30 30 30 30 30  0000046045 00000
003735488  20 6E 0D 0A 30 30 30 30 30 34 36 30 39 37 20 30   n..0000046097 0
003735504  30 30 30 30 20 6E 0D 0A 30 30 30 30 30 34 36 33  0000 n..00000463
003735520  36 35 20 30 30 30 30 30 20 6E 0D 0A 30 30 30 30  65 00000 n..0000
003735536  30 34 36 34 34 39 20 30 30 30 30 30 20 6E 0D 0A  046449 00000 n..
```

4. Now, let us jump to the footer of this file. As seen in the earlier table, the footer for the PDF document can vary, but the one we will use is 0D 0A 25 25 45 4F 46 0D 0A. Let us open Find by clicking the Search dropdown menu from the menu bar and then clicking Find from the menu as highlighted in items 1 and 2 below. You can also open Find by typing Ctrl+F. Once the Find window is open, type `0D 0A 25 25 45 4F 46 0D 0A` as highlighted in item 3 below. Ensure that the radio button beside Forward is selected as we want the footer signature that follows this header. This is highlighted as item 4. Once you are done, click OK as highlighted in item 5 below.

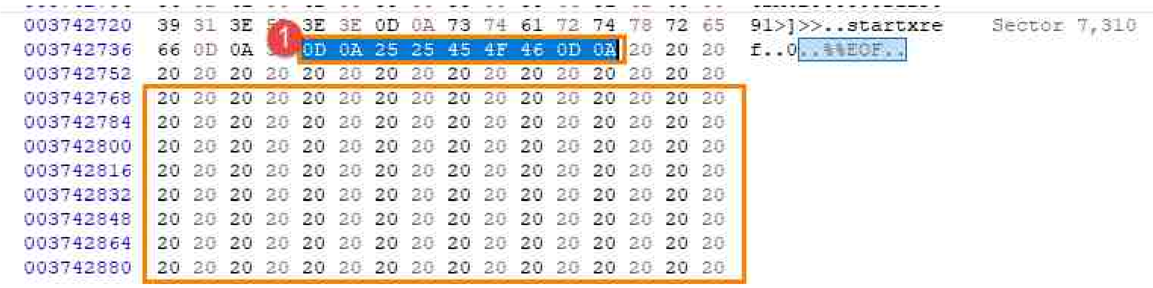


Search for: 0D 0A 25 25 45 4F 46 0D 0A

```
Offset(d                      08 09 10 11 12 13 14 15  Decoded text
00373504                       D 25 E2 E3 CF D3 0D 0A  %PDF-1.6.%âãÏÓ..     Sector 7,295
00373505                      32 6A 20 3C 3C 2F 4C 69  2285 0 obj <</Li
003735072  6E 65 61 72 69 7A 65 64 20 31 2F 4C 20 33 31 37  nearized 1/L 317
003735088  36 32 37 35 2F 4F 20 32 32 39 30 2F 45 20 35 30  6275/O 2290/E 50
003735104  33 35 33 35 2F 4E 20 34 2F 54 20 33 31 33 30 35  3535/N 4/T 31305
003735120  30 39 2F 48 20 5B 20 37 38 36 31 20 39 35 38 5D  09/H [ 7861 958]
003735136  3E 3E 0D 65 6E 64 6F 62 6A 0D 20 20 20 20 20 20  >>.endobj.
003735152  20 20 0D 0A 78 72 65 66 0D 0A 32 32 38 35 20 33    ..xref..2285 3
003735168  37 30 0D 0A 30 30 30 30 30 30 30 30 31 36 20 30  70..0000000016 0
003735184  30 30 30 30 20 6E 0D 0A 30 30 30 30 30 30 38 38  0000 n..00000088
003735200  31 39 20 30 30 30 30 30 20
003735216  30 30 38 39 36 30 20 30 30
003735232  30 30 30 30 30 30 39 31 37
003735248  20 6E 0D 0A 30 30 30 30 30
003735264  30 30 30 30 20 6E 0D 0A 30
003735280  36 35 20 30 30 30 30 30 20
003735296  30 31 30 35 33 36 20 30 30
003735312  30 30 30 30 30 31 30 35 36
003735328  20 6E 0D 0A 30 30 30 30 30
003735344  30 30 30 30 20 6E 0D 0A 30
003735360  36 37 20 30 30 30 30 30 20
003735376  30 31 31 33 37 30 20 30 30
003735392  30 30 30 30 30 34 31 34 31
003735408  20 6E 0D 0A 30 30 30 30 30
003735424  30 30 30 30 20 6E 0D 0A 30
003735440  33 34 20 30 30 30 30 30 20
003735456  30 34 35 35 30 38 20 30 30
003735472  30 30 30 30 30 34 36 30 34
003735488  20 6E 0D 0A 30 30 30 30 30 34 36 30 39 37 20 30   n..0000046097 0
003735504  30 30 30 30 20 6E 0D 0A 30 30 30 30 30 34 36 33  0000 n..00000463
003735520  36 35 20 30 30 30 30 30 20 6E 0D 0A 30 30 30 30  65 00000 n..0000
003735536  30 34 36 34 34 39 20 30 30 30 30 30 20 6E 0D 0A  046449 00000 n..
```

Offset(d): 3735040

5. With these files, we must be cautious as there may be hex values that are false positives highlighted at item 1 below. To ensure you are at the end of the file, look for all zeros after the last character in the footer, which is 0x0A.

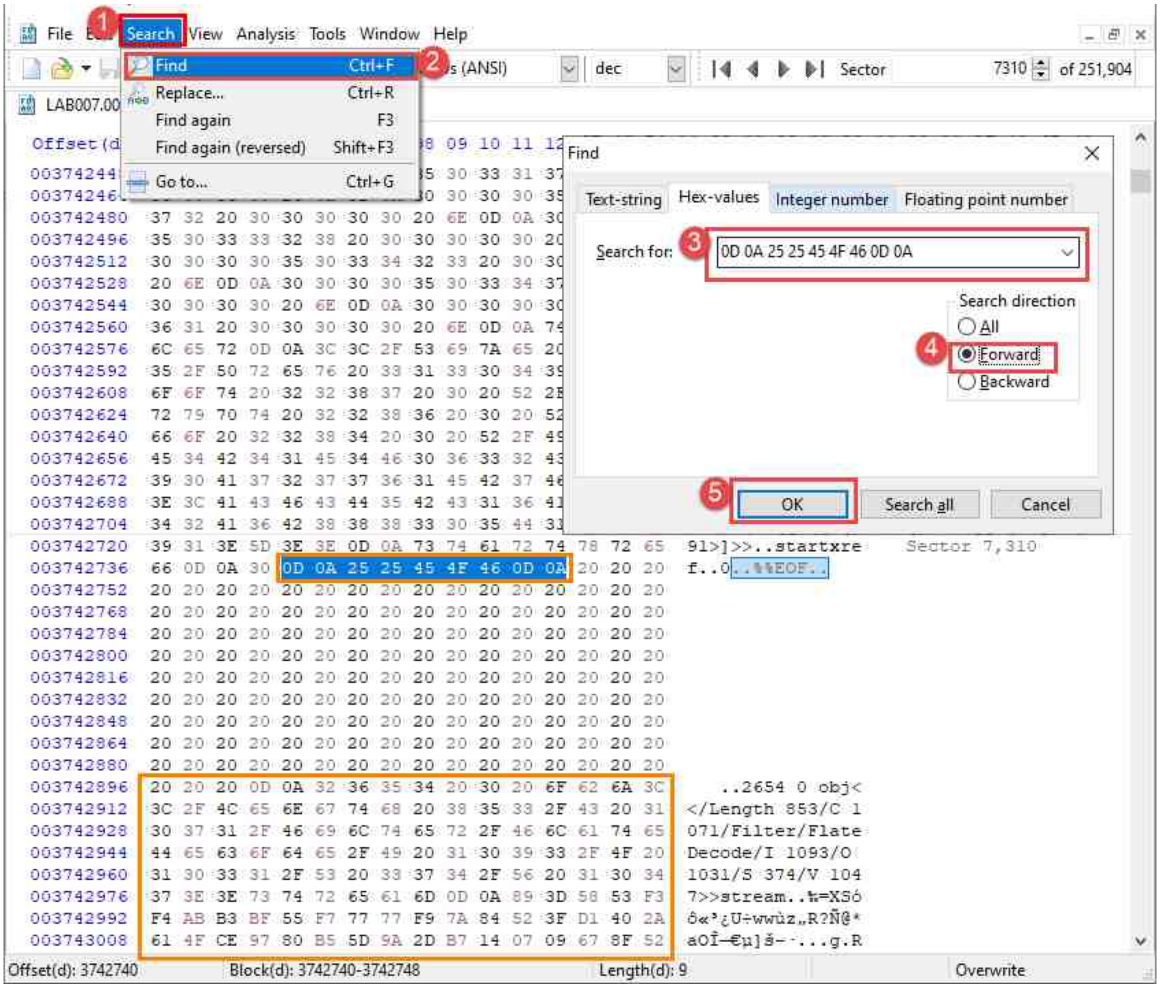


```
003742720  39 31 3E 5D 3E 3E 0D 0A 73 74 61 72 74 78 72 65  91>]>>..startxre    Sector 7,310
003742736  66 0D 0A 30 0D 0A 25 25 45 4F 46 0D 0A 20 20 20  f..0..%%EOF..
003742752  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
003742768  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
003742784  20 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
```

Please Note

This is not the end of the file. The hex values are blank spaces and we are looking for zeros at the end of the file to the end of the sector.

6. Let us continue our search to locate the end of the file. Open the Search dropdown menu from the menu bar and then click Find as highlighted in items 1 and 2 below. You can also open Find by typing the Ctrl+F. Once the Find window is open, the last typed string `0D 0A 25 25 45 4F 46 0D 0A` should still be present, as highlighted in item 3 below. Ensure that the radio button beside Forward is selected as we want the footer signature that follows this header. This is highlighted as item 4. Once you are done, click OK as highlighted in item 5 below.



Search for: 0D 0A 25 25 45 4F 46 0D 0A

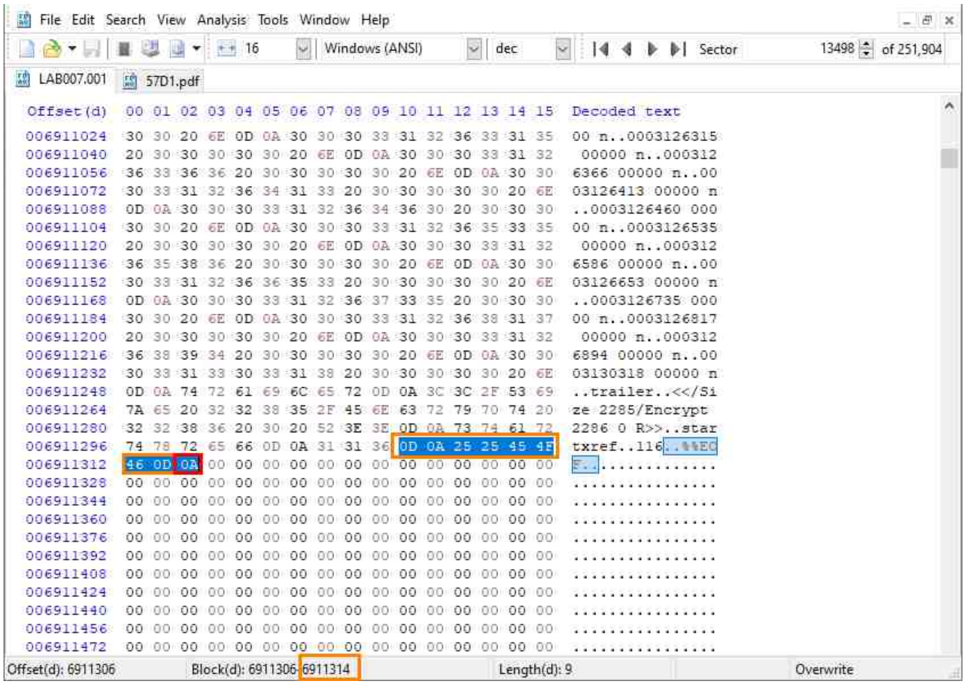
Search direction
○ All
● Forward
○ Backward

```
Offset(d                                  08 09 10 11 12
00374244                                  35 30 33 31 37
00374246                                  30 30 30 30 35
003742480  37 32 20 30 30 30 30 30 20 6E 0D 0A 30
003742496  35 30 33 33 32 38 20 30 30 30 30 30 20
003742512  30 30 30 30 35 30 33 34 32 33 20 30 30
003742528  20 6E 0D 0A 30 30 30 30 35 30 33 34 37
003742544  30 30 30 30 20 6E 0D 0A 30 30 30 30 30
003742560  36 31 20 30 30 30 30 30 20 6E 0D 0A 74
003742576  6C 65 72 0D 0A 3C 3C 2F 53 69 7A 65 20
003742592  35 2F 50 72 65 76 20 33 31 33 30 34 39
003742608  6F 6F 74 20 32 32 38 37 20 30 20 52 2F
003742624  72 79 70 74 20 32 32 38 36 20 30 20 52
003742640  66 6F 20 32 32 38 34 20 30 20 52 2F 49
003742656  45 34 42 34 31 45 34 46 30 36 33 32 43
003742672  39 30 41 37 32 37 37 36 31 45 42 37 46
003742688  3E 3C 41 43 46 43 44 35 42 43 31 36 41
003742704  34 32 41 36 42 38 38 38 33 30 35 44 31
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@*
003743008  61 4F CE 97 80 B5 5D 9A 2D B7 14 07 09 67 8F 52  aOÎ—€µ]š-·...g.R
```

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

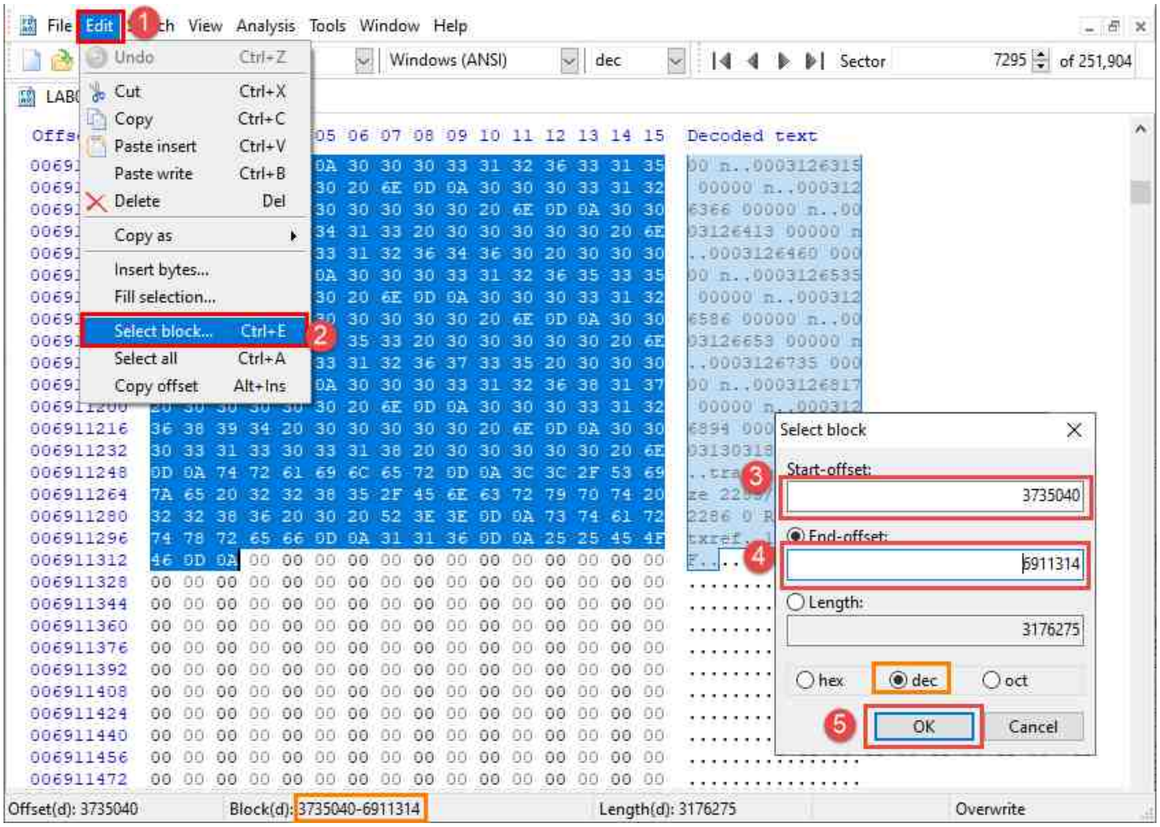
The data continues beyond the false positive.

7. You should now be at the real footer, look for the offset of the last character in our search term 0x0D 0A 25 25 45 4F 46 0D 0A. The offset for the 0x0A value should be 6911314. Note this value as it is the location of the end of this file.



```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text
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 30 30  6366 00000 n..00
006911072  30 33 31 32 36 34 31 33 20 30 30 30 30 30 20 6E  03126413 00000 n
006911088  0D 0A 30 30 30 33 31 32 36 34 36 30 20 30 30 30  ..0003126460 000
006911104  30 30 20 6E 0D 0A 30 30 30 33 31 32 36 35 33 35  00 n..0003126535
006911120  20 30 30 30 30 30 20 6E 0D 0A 30 30 30 33 31 32   00000 n..000312
006911136  36 35 38 36 20 30 30 30 30 30 20 6E 0D 0A 30 30  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 33 35 20 30 30 30  ..0003126735 000
006911184  30 30 20 6E 0D 0A 30 30 30 33 31 32 36 38 31 37  00 n..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  6894 00000 n..00
006911232  30 33 31 33 30 33 31 38 20 30 30 30 30 30 20 6E  03130318 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  ................
006911344  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006911360  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006911376  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006911392  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006911408  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006911424  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006911440  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006911456  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006911472  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    Overwrite
```

8. Now that you have the offsets, let us use the Select block feature to highlight the Start-offset and End-offset of the file. Let us open Select block by clicking the Edit dropdown menu from the menu bar and then clicking Select block from the menu as highlighted in items 1 and 2 below. You can also open Select block by typing Ctrl+E. Once the Select block window is open, type the Start-offset `3735040` and the End-offset `6911314` as highlighted in items 3 and 4 below. Ensure that the radio button beside dec is selected and then click OK as highlighted at item 5 below.



```
Offs  05 06 07 08 09 10 11 12 13 14 15   Decoded text
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
006911248   0D 0A 74 72 61 69 6C 65 72 0D 0A 3C 3C 2F 53 69
006911264   7A 65 20 32 32 38 35 2F 45 6E 63 72 79 70 74 20
006911280   32 32 38 36 20 30 20 52 3E 3E 0D 0A 73 74 61 72
006911296   74 78 72 65 66 0D 0A 31 31 36 0D 0A 25 25 45 4F
006911312   46 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00
006911328   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006911344   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006911360   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006911376   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006911392   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006911408   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006911424   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006911440   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006911456   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006911472   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Select block

Start-offset: 3735040

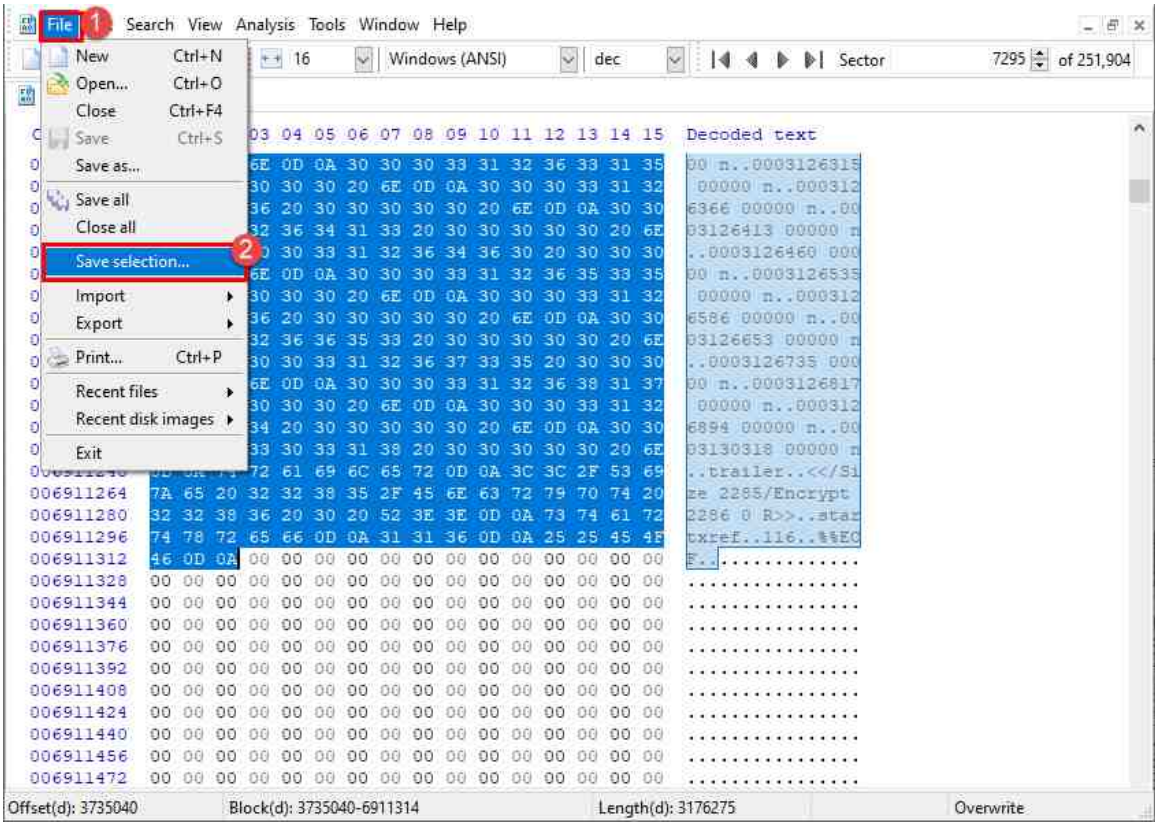
● End-offset: 6911314

○ Length: 3176275

○ hex ● dec ○ oct

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

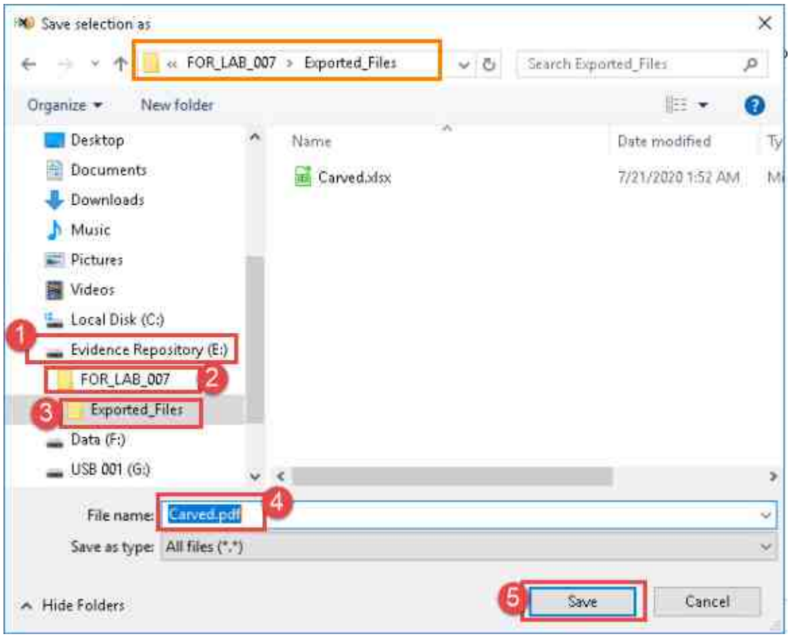
9. Like we did before with the first document. Let us save this selection as a file by browsing to the File dropdown menu from the menu bar and clicking Save Selection as highlighted in items 1 and 2 below. This will open the Save selection as window.



```
           03 04 05 06 07 08 09 10 11 12 13 14 15   Decoded text
           6E 0D 0A 30 30 30 33 31 32 36 33 31 35   00 n..0003126315
           30 30 30 20 6E 0D 0A 30 30 30 33 31 32    00000 n..000312
           36 20 30 30 30 30 30 20 6E 0D 0A 30 30   6366 00000 n..00
           32 36 34 31 33 20 30 30 30 30 30 20 6E   03126413 00000 n
            0 30 33 31 32 36 34 36 30 20 30 30 30   ..0003126460 000
           6E 0D 0A 30 30 30 33 31 32 36 35 33 35   00 n..0003126535
           30 30 30 20 6E 0D 0A 30 30 30 33 31 32    00000 n..000312
           36 20 30 30 30 30 30 20 6E 0D 0A 30 30   6586 00000 n..00
           32 36 36 35 33 20 30 30 30 30 30 20 6E   03126653 00000 n
           30 30 33 31 32 36 37 33 35 20 30 30 30   ..0003126735 000
           6E 0D 0A 30 30 30 33 31 32 36 38 31 37   00 n..0003126817
           30 30 30 20 6E 0D 0A 30 30 30 33 31 32    00000 n..000312
           34 20 30 30 30 30 30 20 6E 0D 0A 30 30   6894 00000 n..00
           33 30 33 31 38 20 30 30 30 30 30 20 6E   03130318 00000 n
              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   ................
006911344  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006911360  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006911376  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006911392  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006911408  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006911424  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006911440  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006911456  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006911472  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
```

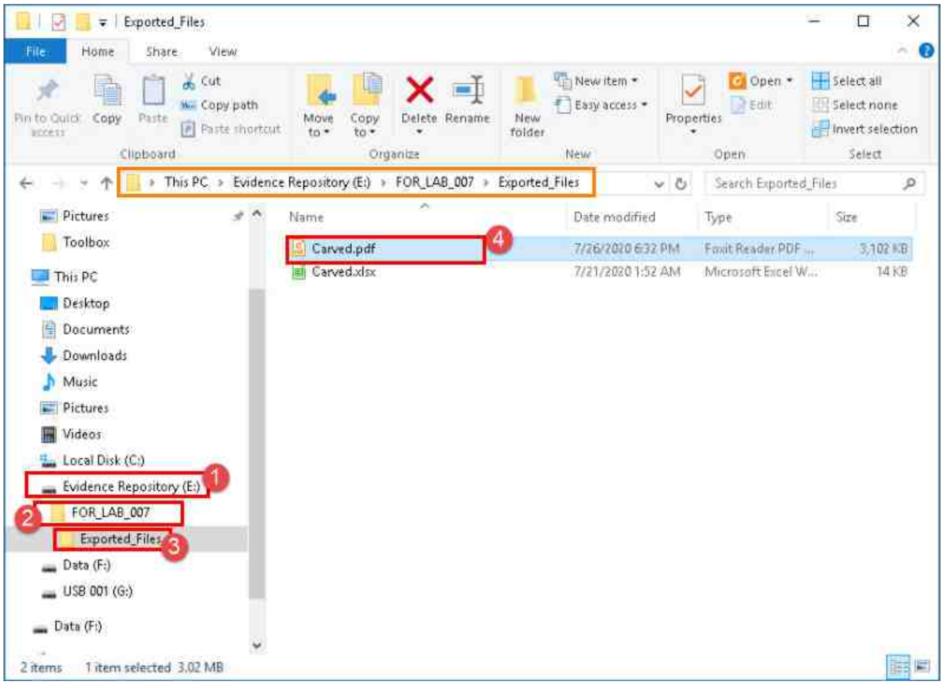
10. Now let us save the file. To do this, browse to the location of the folder Exported_Files using the path Evidence Repository (E:) > FOR_LAB_007 as highlighted in items 1, 2, and 3 below. Type the name `Carved.pdf` and then click Save as highlighted in items 4 and 5.



File name: Carved.pdf

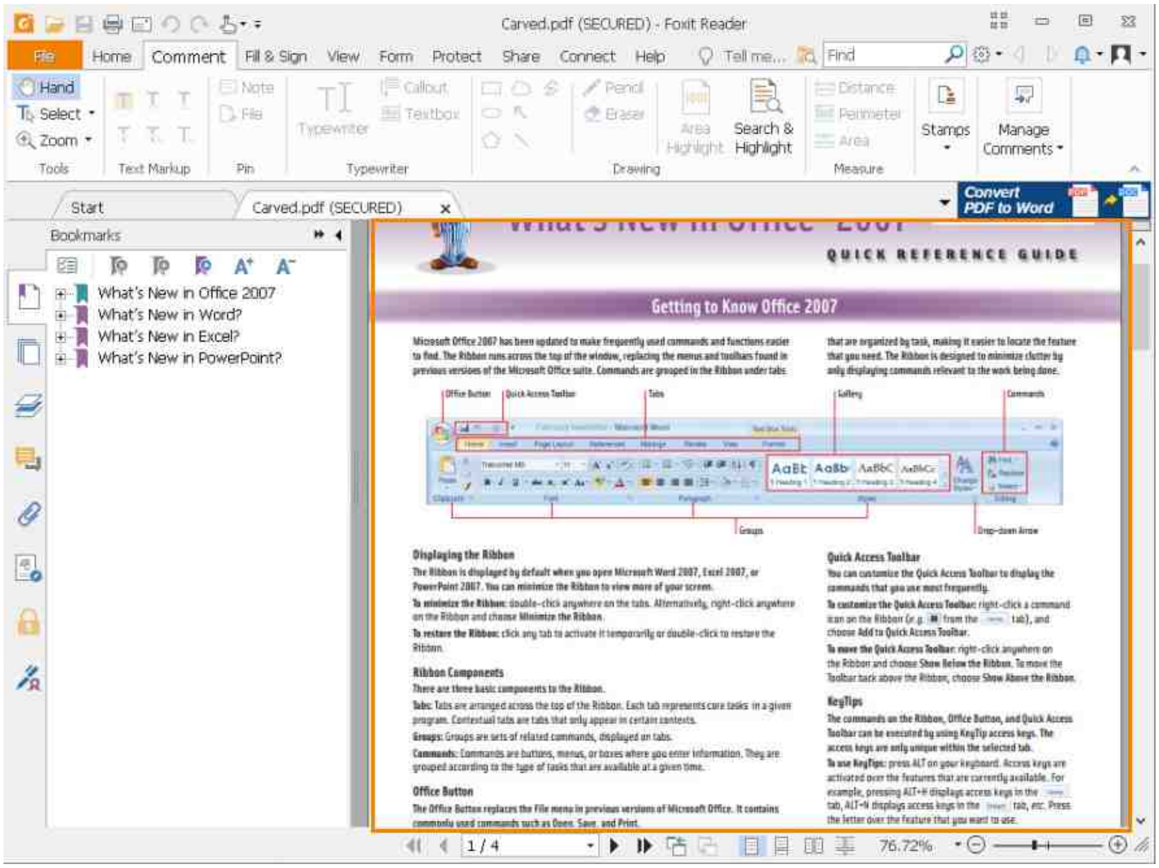
Save as type: All files (*.*)

11. Now browse to the location of the file by opening Windows' File Explorer and browsing to the path Evidence Repository (E:) > FOR_LAB_007 > Exported_Files and double-clicking the file you saved, called Carved.pdf as highlighted at items 1, 2, 3, and 4.



Name	Date modified	Type	Size
Carved.pdf	7/26/2020 6:32 PM	Foxit Reader PDF ...	3,102 KB
Carved.xlsx	7/21/2020 1:52 AM	Microsoft Excel W...	14 KB

12. If you successfully carved the file, it should look like the one below. The file should open without any errors, which would mean you successfully carved the file.



QUICK REFERENCE GUIDE

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.

Tabs: Tabs are arranged across the top of the Ribbon. Each tab represents core tasks in a given program. Contextual tabs are tabs that only appear in certain contexts.

Groups: Groups are sets of related commands, displayed on tabs.

Commands: Commands are buttons, menus, or boxes where you enter information. They are grouped according to the type of tasks that are available at a given time.

Office Button

The Office Button replaces the File menu in previous versions of Microsoft Office. It contains commonly used commands such as Open, Save, and Print.

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. from the 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**.

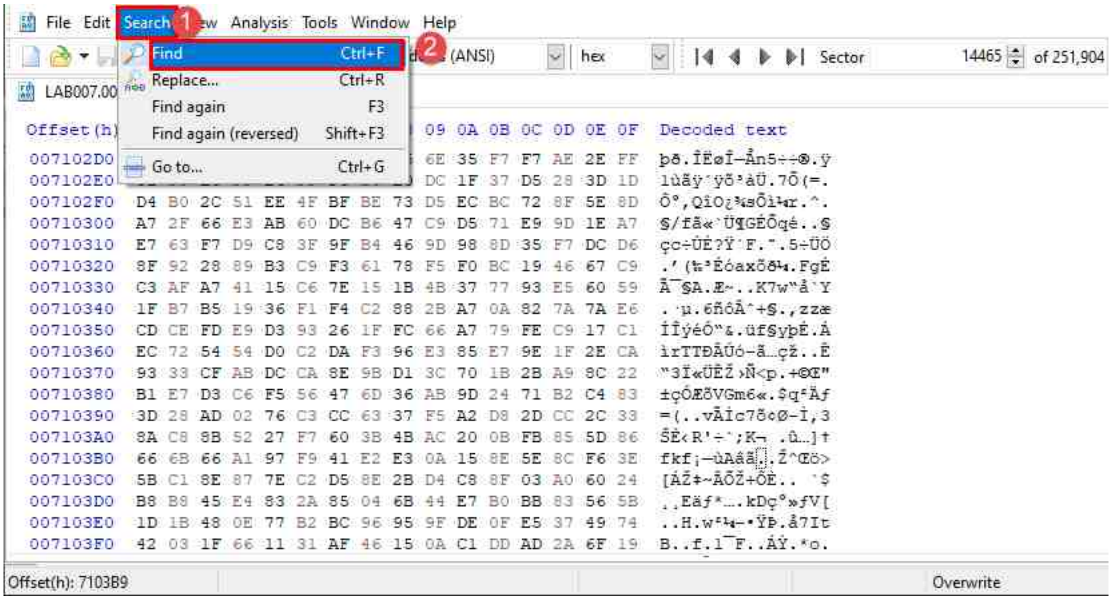
KeyTips

The commands on the Ribbon, Office Button, and Quick Access Toolbar can be executed by using KeyTip access keys. The access keys are only unique within the selected tab.

To use KeyTips: press ALT on your keyboard. Access keys are activated over the features that are currently available. For example, pressing ALT+H displays access keys in the tab, ALT+N displays access keys in the tab, etc. Press the letter over the feature that you want to use.

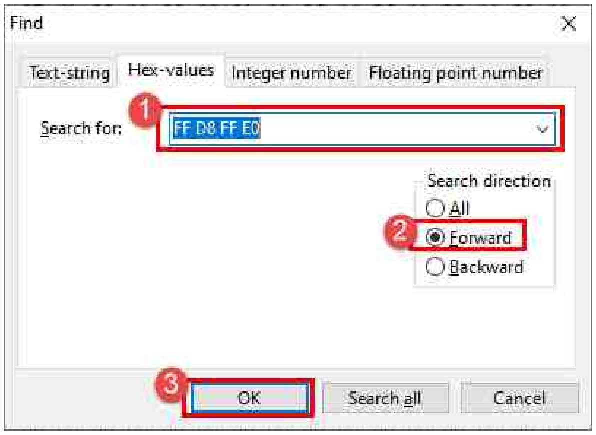
4 Carving JPG Files

1. Now let us carve one more filetype. This time we will do JPG. HxD should still be open; if not, reopen it and open Find by clicking the Search dropdown menu from the menu bar and then clicking Find from the menu as highlighted in items 1 and 2 below. You can also open Find by typing Ctrl+F.



```
Offset(h)                             09 0A 0B 0C 0D 0E 0F  Decoded text
007102D0                              6E 35 F7 F7 AE 2E FF  þð.ÎËøÎ–Ån5÷÷®.ÿ
007102E0                              DC 1F 37 D5 28 3D 1D  1ùãÿ´ÿõ³àÜ.7Õ(=.
007102F0  D4 B0 2C 51 EE 4F BF BE 73 D5 EC BC 72 8F 5E 8D  Ô°,QîO¿¾sÕì¼r.^.
00710300  A7 2F 66 E3 AB 60 DC B6 47 C9 D5 71 E9 9D 1E A7  §/fã«`Ü¶GÉÕqé..§
00710310  E7 63 F7 D9 C8 3F 9F B4 46 9D 98 8D 35 F7 DC D6  çc÷ÙÈ?Ÿ´F.˜.5÷ÜÖ
00710320  8F 92 28 89 B3 C9 F3 61 78 F5 F0 BC 19 46 67 C9  .’(‰³ÉóaxõðŒ.FgÉ
00710330  C3 AF A7 41 15 C6 7E 15 1B 4B 37 77 93 E5 60 59  Ã¯§A.Æ~..K7w“å`Y
00710340  1F B7 B5 19 36 F1 F4 C2 88 2B A7 0A 82 7A 7A E6  .·µ.6ñôÂˆ+§.‚zzæ
00710350  CD CE FD E9 D3 93 26 1F FC 66 A7 79 FE C9 17 C1  ÍÎýéÓ“&.üf§yþÉ.Á
00710360  EC 72 54 54 D0 C2 DA F3 96 E3 85 E7 9E 1F 2E CA  ìrTTÐÂÚó–ã…çž..Ê
00710370  93 33 CF AB DC CA 8E 9B D1 3C 70 1B 2B A9 8C 22  “3Ï«ÜÊŽ›Ñ<p.+©Œ"
00710380  B1 E7 D3 C6 F5 56 47 6D 36 AB 9D 24 71 B2 C4 83  ±çÓÆõVGm6«.$q²Äƒ
00710390  3D 28 AD 02 76 C3 CC 63 37 F5 A2 D8 2D CC 2C 33  =(..vÃÌc7õ¢Ø-Ì,3
007103A0  8A C8 8B 52 27 F7 60 3B 4B AC 20 0B FB 85 5D 86  ŠÈ‹R'÷`;K¬ .û…]†
007103B0  66 6B 66 A1 97 F9 41 E2 E3 0A 15 8E 5E 8C F6 3E  fkf¡—ùAâã..Ž^Œö>
007103C0  5B C1 8E 87 7E C2 D5 8E 2B D4 C8 8F 03 A0 60 24  [ÁŽ‡~ÂÕŽ+ÔÈ.. `$
007103D0  B8 B8 45 E4 83 2A 85 04 6B 44 E7 B0 BB 83 56 5B  ¸¸Eäƒ*….kDç°»ƒV[
007103E0  1D 1B 48 0E 77 B2 BC 96 95 9F DE 0F E5 37 49 74  ..H.w²¼–•ŸÞ.å7It
007103F0  42 03 1F 66 11 31 AF 46 15 0A C1 DD AD 2A 6F 19  B..f.1¯F..ÁÝ.*o.
Offset(h): 7103B9
```

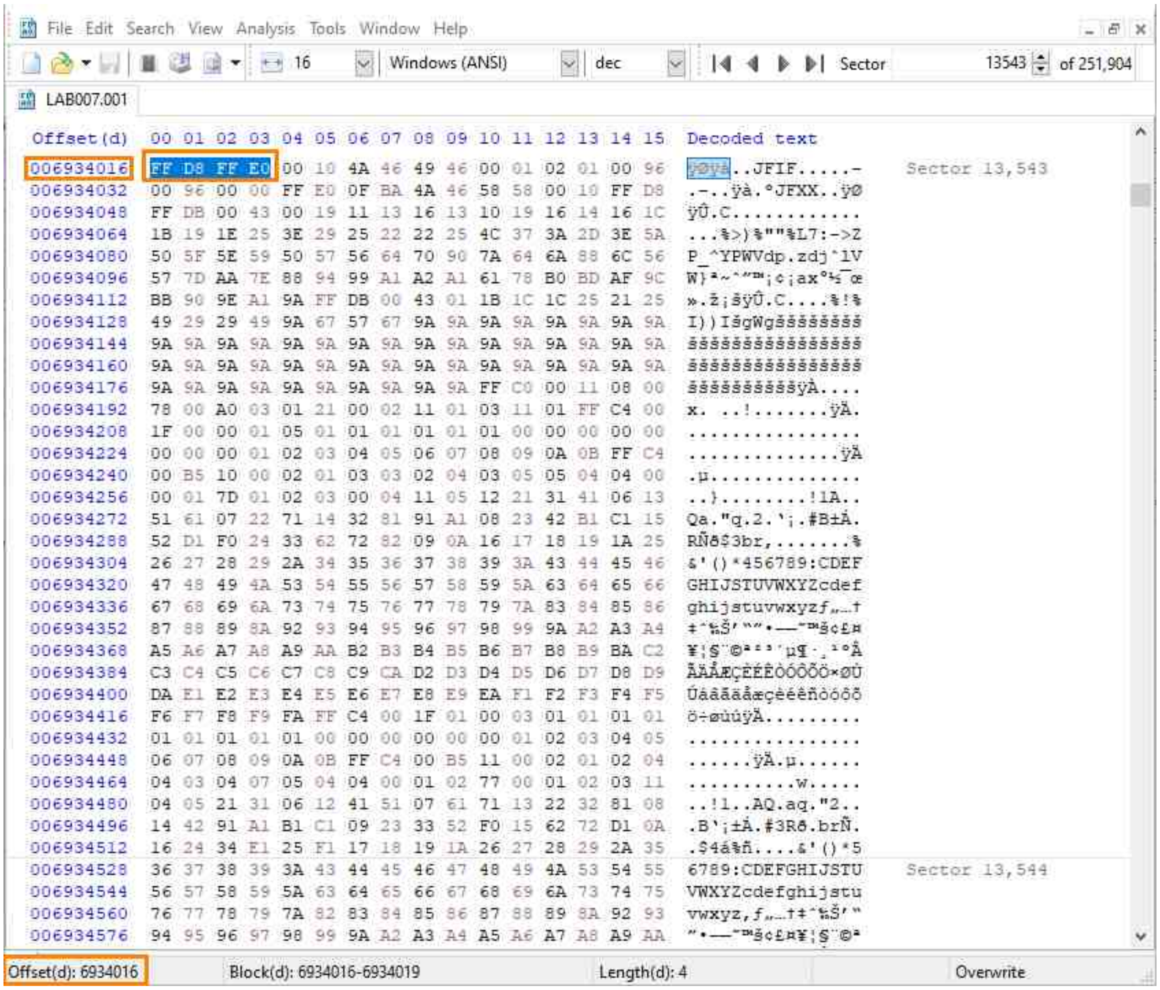
2. Once the Find window is open, type `FF D8 FF E0` highlighted as item 1 below. This is the file signature for JPG files. Let us click the radio button beside Forward this time as the file we are looking for is located after the previous PDF file we carved. This is highlighted as item 2. Once you are done, click OK highlighted as item 3 below.



Search for: FF D8 FF E0

Search direction: ● Forward

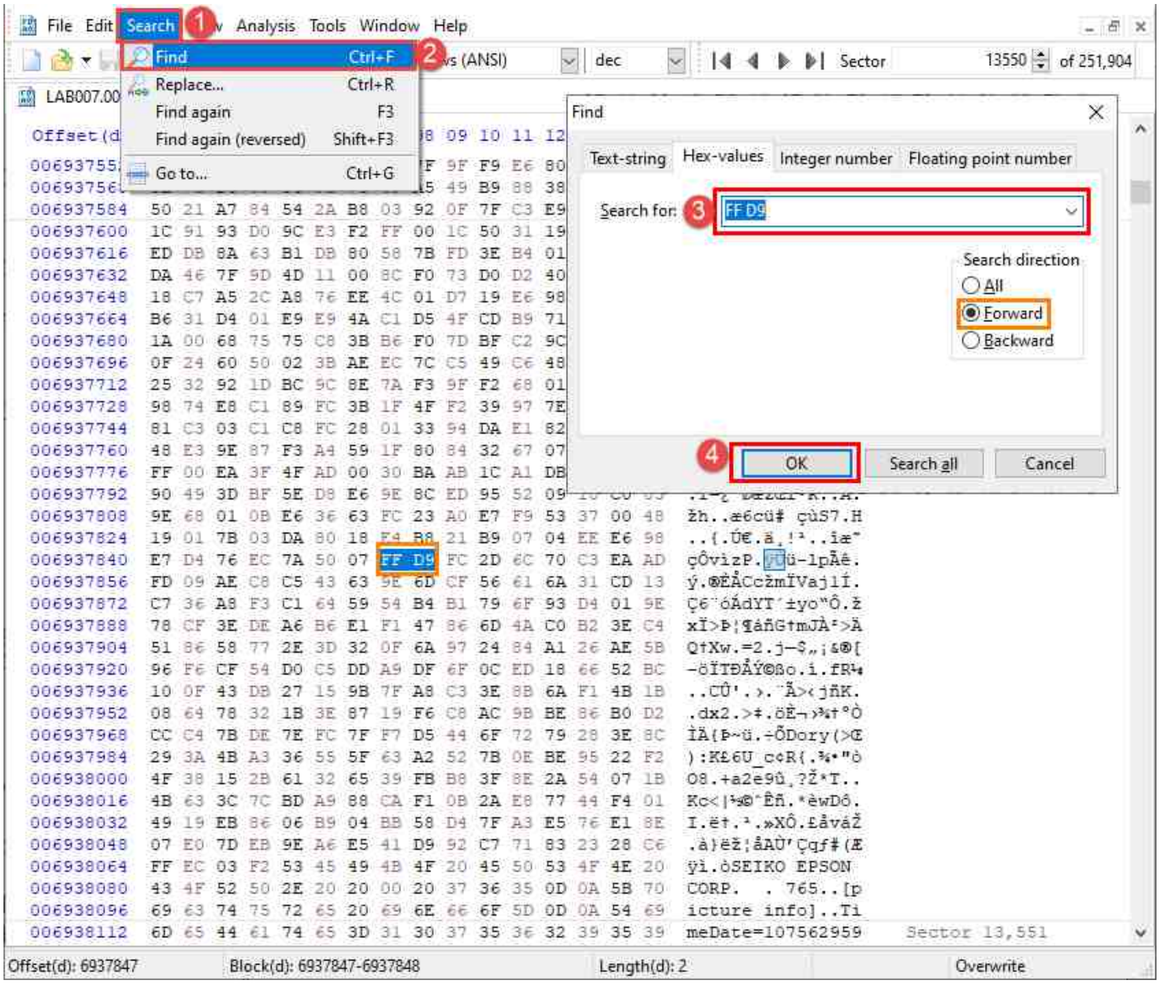
3. The search will take you to the beginning of the next JPG file on the volume. As seen in the screenshot below, the offset for this document should be 6934016. As you did before, make a note of this as we will be coming back to the header to begin the highlighting.



```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text
006934016  FF D8 FF E0 00 10 4A 46 49 46 00 01 02 01 00 96  ÿØÿà..JFIF.....–     Sector 13,543
006934032  00 96 00 00 FF E0 0F BA 4A 46 58 58 00 10 FF D8  .–..ÿà.ºJFXX..ÿØ
006934048  FF DB 00 43 00 19 11 13 16 13 10 19 16 14 16 1C  ÿÛ.C............
006934064  1B 19 1E 25 3E 29 25 22 22 25 4C 37 3A 2D 3E 5A  ...%>)%""%L7:->Z
006934080  50 5F 5E 59 50 57 56 64 70 90 7A 64 6A 88 6C 56  P_^YPWVdp.zdjˆlV
006934096  57 7D AA 7E 88 94 99 A1 A2 A1 61 78 B0 BD AF 9C  W}ª~ˆ”™¡¢¡ax°½¯œ
006934112  BB 90 9E A1 9A FF DB 00 43 01 1B 1C 1C 25 21 25  ».ž¡šÿÛ.C....%!%
006934128  49 29 29 49 9A 67 57 67 9A 9A 9A 9A 9A 9A 9A 9A  I))IšgWgšššššššš
006934144  9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A  šššššššššššššššš
006934160  9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A 9A  šššššššššššššššš
006934176  9A 9A 9A 9A 9A 9A 9A 9A 9A 9A FF C0 00 11 08 00  ššššššššššÿÀ....
006934192  78 00 A0 03 01 21 00 02 11 01 03 11 01 FF C4 00  x. ..!.......ÿÄ.
006934208  1F 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00  ................
006934224  00 00 00 01 02 03 04 05 06 07 08 09 0A 0B FF C4  ..............ÿÄ
006934240  00 B5 10 00 02 01 03 03 02 04 03 05 05 04 04 00  .µ..............
006934256  00 01 7D 01 02 03 00 04 11 05 12 21 31 41 06 13  ..}........!1A..
006934272  51 61 07 22 71 14 32 81 91 A1 08 23 42 B1 C1 15  Qa."q.2.‘¡.#B±Á.
006934288  52 D1 F0 24 33 62 72 82 09 0A 16 17 18 19 1A 25  RÑð$3br‚.......%
006934304  26 27 28 29 2A 34 35 36 37 38 39 3A 43 44 45 46  &'()*456789:CDEF
006934320  47 48 49 4A 53 54 55 56 57 58 59 5A 63 64 65 66  GHIJSTUVWXYZcdef
006934336  67 68 69 6A 73 74 75 76 77 78 79 7A 83 84 85 86  ghijstuvwxyzƒ„…†
006934352  87 88 89 8A 92 93 94 95 96 97 98 99 9A A2 A3 A4  ‡ˆ‰Š’“”•–—˜™š¢£¤
006934368  A5 A6 A7 A8 A9 AA B2 B3 B4 B5 B6 B7 B8 B9 BA C2  ¥¦§¨©ª²³´µ¶·¸¹ºÂ
006934384  C3 C4 C5 C6 C7 C8 C9 CA D2 D3 D4 D5 D6 D7 D8 D9  ÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙ
006934400  DA E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1 F2 F3 F4 F5  Úáâãäåæçèéêñòóôõ
006934416  F6 F7 F8 F9 FA FF C4 00 1F 01 00 03 01 01 01 01  ö÷øùúÿÄ.........
006934432  01 01 01 01 01 00 00 00 00 00 00 01 02 03 04 05  ................
006934448  06 07 08 09 0A 0B FF C4 00 B5 11 00 02 01 02 04  ......ÿÄ.µ......
006934464  04 03 04 07 05 04 04 00 01 02 77 00 01 02 03 11  ..........w.....
006934480  04 05 21 31 06 12 41 51 07 61 71 13 22 32 81 08  ..!1..AQ.aq."2..
006934496  14 42 91 A1 B1 C1 09 23 33 52 F0 15 62 72 D1 0A  .B‘¡±Á.#3Rð.brÑ.
006934512  16 24 34 E1 25 F1 17 18 19 1A 26 27 28 29 2A 35  .$4á%ñ....&'()*5
006934528  36 37 38 39 3A 43 44 45 46 47 48 49 4A 53 54 55  6789:CDEFGHIJSTU     Sector 13,544
006934544  56 57 58 59 5A 63 64 65 66 67 68 69 6A 73 74 75  VWXYZcdefghijstu
006934560  76 77 78 79 7A 82 83 84 85 86 87 88 89 8A 92 93  vwxyz‚ƒ„…†‡ˆ‰Š’“
006934576  94 95 96 97 98 99 9A A2 A3 A4 A5 A6 A7 A8 A9 AA  ”•–—˜™š¢£¤¥¦§¨©ª
```

Offset(d): 6934016 Block(d): 6934016-6934019 Length(d): 4

4. Now, let us jump to the footer of this file. As seen in the earlier table, the footer for the JPG file is 0xFF D9. As with the PDF files, we must be cautious as there may be hex values that are false positives. To ensure you are at the end of the file, look for all zeros between the last hex value in the footer, 0xD9, and the end of the sector.
5. Let us open Find again by clicking the Search dropdown menu from the menu bar and then clicking Find from the menu as highlighted in items 1 and 2 below. You can also open Find by typing Ctrl+F. Once the Find window is open, type `FF D9` as highlighted below. Ensure that the radio button beside Forward is selected as we want the footer that follows this header. This is highlighted as item 3. Once you are done, click OK highlighted as item 4 below.



Find

Search for: FF D9

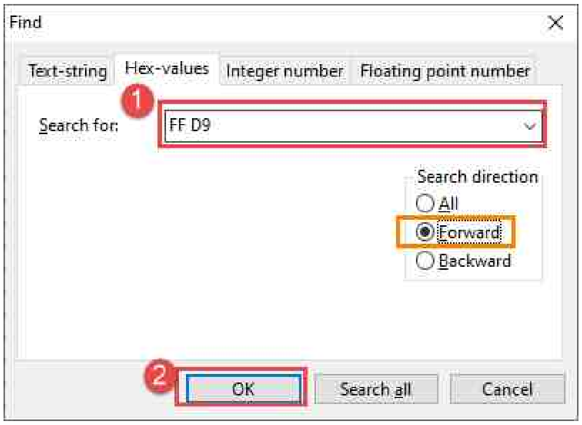
Search direction
○ All
● Forward
○ Backward

```
Offset(d                             08 09 10 11 12
00693755                           F 9F F9 E6 80
00693756                            5 49 B9 88 38
006937584  50 21 A7 84 54 2A B8 03 92 0F 7F C3 E9
006937600  1C 91 93 D0 9C E3 F2 FF 00 1C 50 31 19
006937616  ED DB 8A 63 B1 DB 80 58 7B FD 3E B4 01
006937632  DA 46 7F 9D 4D 11 00 8C F0 73 D0 D2 40
006937648  18 C7 A5 2C A8 76 EE 4C 01 D7 19 E6 98
006937664  B6 31 D4 01 E9 E9 4A C1 D5 4F CD B9 71
006937680  1A 00 68 75 75 C8 3B B6 F0 7D BF C2 9C
006937696  0F 24 60 50 02 3B AE EC 7C C5 49 C6 48
006937712  25 32 92 1D BC 9C 8E 7A F3 9F F2 68 01
006937728  98 74 E8 C1 89 FC 3B 1F 4F F2 39 97 7E
006937744  81 C3 03 C1 C8 FC 28 01 33 94 DA E1 82
006937760  48 E3 9E 87 F3 A4 59 1F 80 84 32 67 07
006937776  FF 00 EA 3F 4F AD 00 30 BA AB 1C A1 DB
006937792  90 49 3D BF 5E D8 E6 9E 8C ED 95 52 09
006937808  9E 68 01 0B E6 36 63 FC 23 A0 E7 F9 53 37 00 48  žh..æ6cü# çùS7.H
006937824  19 01 7B 03 DA 80 18 F4 B8 21 B9 07 04 EE E6 98  ..{.Ú€.ä¸!¹..îæ˜
006937840  E7 D4 76 EC 7A 50 07 FF D9 FC 2D 6C 70 C3 EA AD  çÔvìzP.ÿÙü-lpÃê.
006937856  FD 09 AE C8 C5 43 63 9E 6D CF 56 61 6A 31 CD 13  ý.®ÈÅCcžmÏVaj1Í.
006937872  C7 36 A8 F3 C1 64 59 54 B4 B1 79 6F 93 D4 01 9E  Ç6¨óÁdYT´±yo“Ô.ž
006937888  78 CF 3E DE A6 B6 E1 F1 47 86 6D 4A C0 B2 3E C4  xÏ>Þ¦¶áñG†mJÀ²>Ä
006937904  51 86 58 77 2E 3D 32 0F 6A 97 24 84 A1 26 AE 5B  Q†Xw.=2.j—$„¡&®[
006937920  96 F6 CF 54 D0 C5 DD A9 DF 6F 0C ED 18 66 52 BC  –öÏTÐÅÝ©ßo.í.fR¼
006937936  10 0F 43 DB 27 15 9B 7F A8 C3 3E 8B 6A F1 4B 1B  ..CÛ'.›.¨Ã>‹jñK.
006937952  08 64 78 32 1B 3E 87 19 F6 C8 AC 9B BE 86 B0 D2  .dx2.>‡.öÈ¬›¾†°Ò
006937968  CC C4 7B DE 7E FC 7F F7 D5 44 6F 72 79 28 3E 8C  ÌÄ{Þ~ü.÷ÕDory(>Œ
006937984  29 3A 4B A3 36 55 5F 63 A2 52 7B 0E BE 95 22 F2  ):K£6U_c¢R{.¾•"ò
006938000  4F 38 15 2B 61 32 65 39 FB B8 3F 8E 2A 54 07 1B  O8.+a2e9û¸?Ž*T..
006938016  4B 63 3C 7C BD A9 88 CA F1 0B 2A E8 77 44 F4 01  Kc<|½©ˆÊñ.*èwDô.
006938032  49 19 EB 86 06 B9 04 BB 58 D4 7F A3 E5 76 E1 8E  I.ë†.¹.»XÔ.£åváŽ
006938048  07 E0 7D EB 9E A6 E5 41 D9 92 C7 71 83 23 28 C6  .à}ëž¦åAÙ'Çqƒ#(Æ
006938064  FF EC 03 F2 53 45 49 4B 4F 20 45 50 53 4F 4E 20  ÿì.òSEIKO EPSON 
006938080  43 4F 52 50 2E 20 20 00 20 37 36 35 0D 0A 5B 70  CORP.  . 765..[p
006938096  69 63 74 75 72 65 20 69 6E 66 6F 5D 0D 0A 54 69  icture info]..Ti
006938112  6D 65 44 61 74 65 3D 31 30 37 35 36 32 39 35 39  meDate=107562959     Sector 13,551
```

Offset(d): 6937847 Block(d): 6937847-6937848 Length(d): 2 Overwrite

The 0xFF D9 values highlighted are the false positive that was mentioned earlier. If you stop here you will not be able to see the image file

6. Since the first hit was a false positive, let us open Find again using the Search dropdown menu or by typing Ctrl+F. The previously typed search should already be in the Search for slot, if not, retype the values `FF D9` as highlighted in item 1. Once you are done, click OK highlighted as item 2 below.



Find

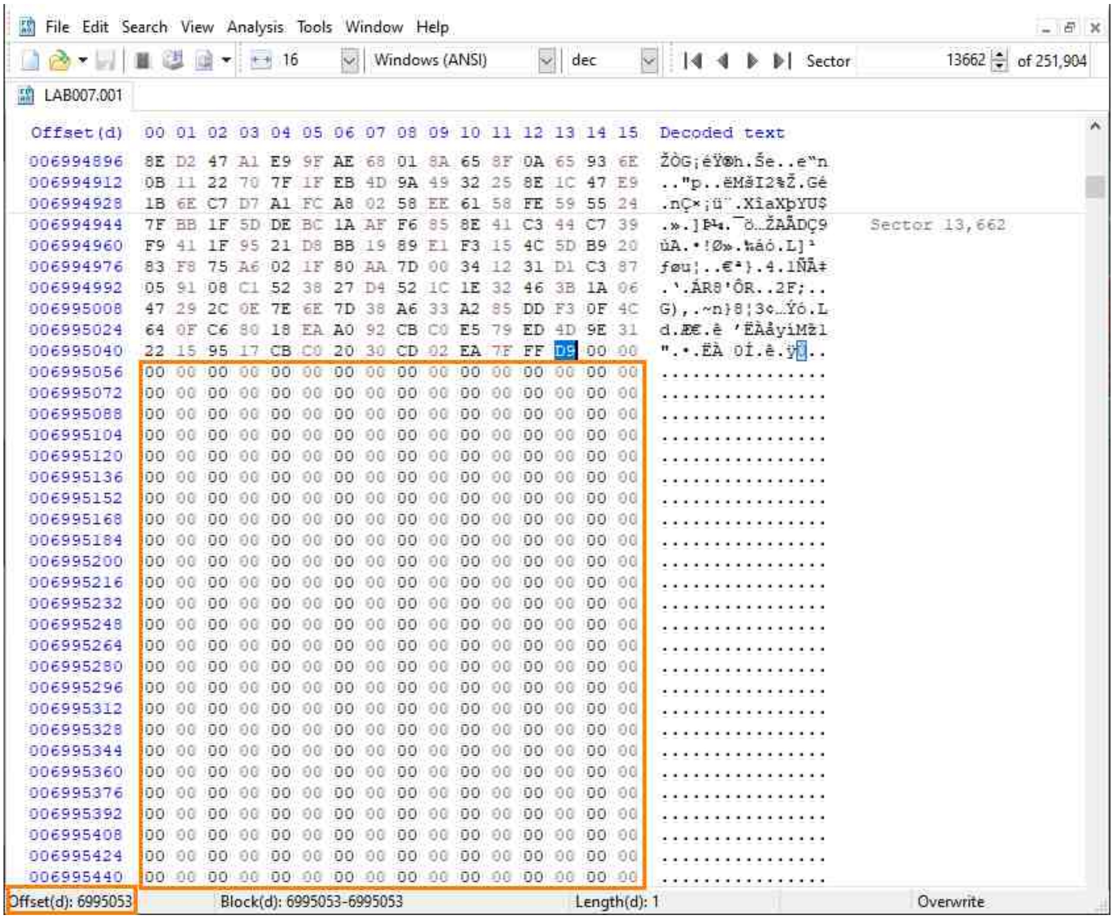
Text-string | Hex-values | Integer number | Floating point number

1 Search for: FF D9

Search direction
○ All
● Forward
○ Backward

2 OK | Search all | Cancel

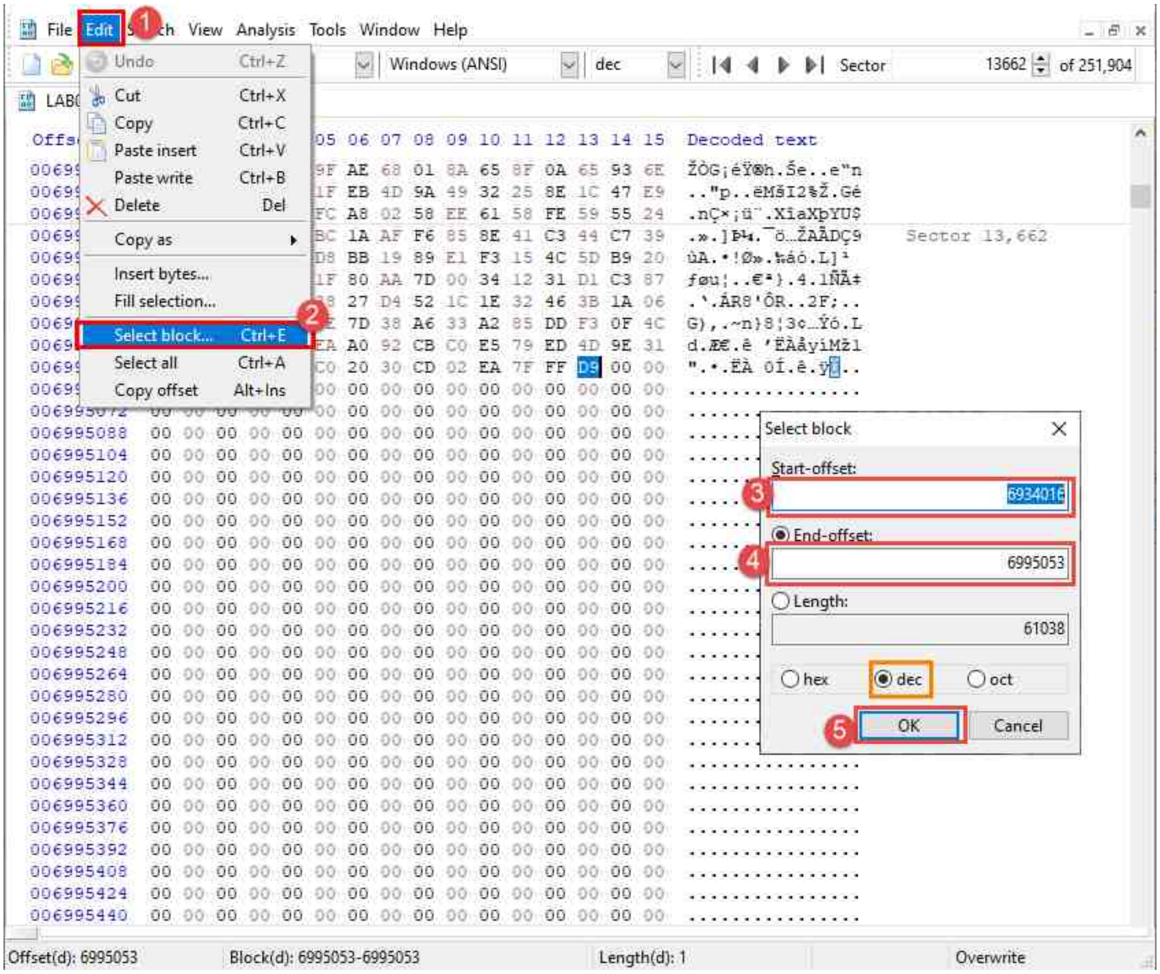
7. Remember to look out for the zeros between the hex value 0xD9 and the end of the sector. Once you get to the correct footer, look for the offset of the last character in our search term 0xFF D9. The offset for the 0xD9 value should be 6995053. Note this value as it is the location of the end of this file.



```
Offset(d)  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15  Decoded text
006994896  8E D2 47 A1 E9 9F AE 68 01 8A 65 8F 0A 65 93 6E  ŽÒG¡éŸ®h.Še..e"n
006994912  0B 11 22 70 7F 1F EB 4D 9A 49 32 25 8E 1C 47 E9  .."p..ëMšI2%Ž.Gé
006994928  1B 6E C7 D7 A1 FC A8 02 58 EE 61 58 FE 59 55 24  .nÇ×¡ü¨.XîaXþYU$
006994944  7F BB 1F 5D DE BC 1A AF F6 85 8E 41 C3 44 C7 39  .».]Þ¼.¯ö…ŽAÃDÇ9   Sector 13,662
006994960  F9 41 1F 95 21 D8 BB 19 89 E1 F3 15 4C 5D B9 20  ùA.•!Ø».‰áó.L]¹ 
006994976  83 F8 75 A6 02 1F 80 AA 7D 00 34 12 31 D1 C3 87  ƒøu¦..€ª}.4.1ÑÃ‡
006994992  05 91 08 C1 52 38 27 D4 52 1C 1E 32 46 3B 1A 06  .'.ÁR8'ÔR..2F;..
006995008  47 29 2C 0E 7E 6E 7D 38 A6 33 A2 85 DD F3 0F 4C  G),.~n}8¦3¢…Ýó.L
006995024  64 0F C6 80 18 EA A0 92 CB C0 E5 79 ED 4D 9E 31  d.Æ€.ê 'ËÀåyíMž1
006995040  22 15 95 17 CB C0 20 30 CD 02 EA 7F FF D9 00 00  ".•.ËÀ 0Í.ê.ÿÙ..
006995056  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995072  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995088  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995104  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995136  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995152  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995168  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995184  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995216  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995232  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995248  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995264  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995280  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995296  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995312  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995328  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995344  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995360  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995376  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995392  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995408  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995424  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006995440  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Offset(d): 6995053    Block(d): 6995053-6995053    Length(d): 1    Overwrite
```

If you see other values after the last hex value 0xFF D9, then press the Ctrl+F button to Find Next which will take you to the next occurrence of the search term in the FEF.

8. Just as we did before, let us use Select block feature to highlight the Start-offset and End-offset of the file. Let us open Select block by clicking the Edit dropdown menu from the menu bar and then clicking Select block from the menu as highlighted in items 1 and 2 below. You can also open Select block by typing Ctrl+E. Once the Select block window is open, type the Start-offset `6934016` and the End-offset `6995053` as highlighted in items 3 and 4 below. Ensure that the radio button beside dec is selected and then click OK as highlighted at item 5 below.



```
Offs        05 06 07 08 09 10 11 12 13 14 15   Decoded text
00699       9F AE 68 01 8A 65 8F 0A 65 93 6E   ŽÒG¡éŸ®h.Še..e"n
00699       1F EB 4D 9A 49 32 25 8E 1C 47 E9   .."p..ëMšI2%Ž.Gé
00699       FC A8 02 58 EE 61 58 FE 59 55 24   .nÇ×¡ü¨.XîaXþYU$
00699       BC 1A AF F6 85 8E 41 C3 44 C7 39   .».]Þ¼.¯ö…ŽAÃDÇ9     Sector 13,662
00699       D8 BB 19 89 E1 F3 15 4C 5D B9 20   ùA.•!Ø».‰áó.L]¹
00699       1F 80 AA 7D 00 34 12 31 D1 C3 87   ƒøu¦..€ª}.4.1ÑÃ‡
00699       8 27 D4 52 1C 1E 32 46 3B 1A 06    .`.ÁR8'ÔR..2F;..
0069        E 7D 38 A6 33 A2 85 DD F3 0F 4C    G),.~n}8¦3¢…Ýó.L
0069        EA A0 92 CB C0 E5 79 ED 4D 9E 31   d.Æ€.ê 'ËÀåyíMž1
00699       C0 20 30 CD 02 EA 7F FF D9 00 00   ".•.ËÀ 0Í.ê.ÿÙ..
00699       00 00 00 00 00 00 00 00 00 00 00   ................
00699507    00 00 00 00 00 00 00 00 00 00 00   ......
006995088   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995104   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995120   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995136   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995152   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995168   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995184   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995200   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995216   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995232   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995248   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995264   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995280   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995296   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995312   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
006995328   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006995344   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006995360   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006995376   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006995392   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006995408   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006995424   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
006995440   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Select block

Start-offset: 6934016

● End-offset: 6995053

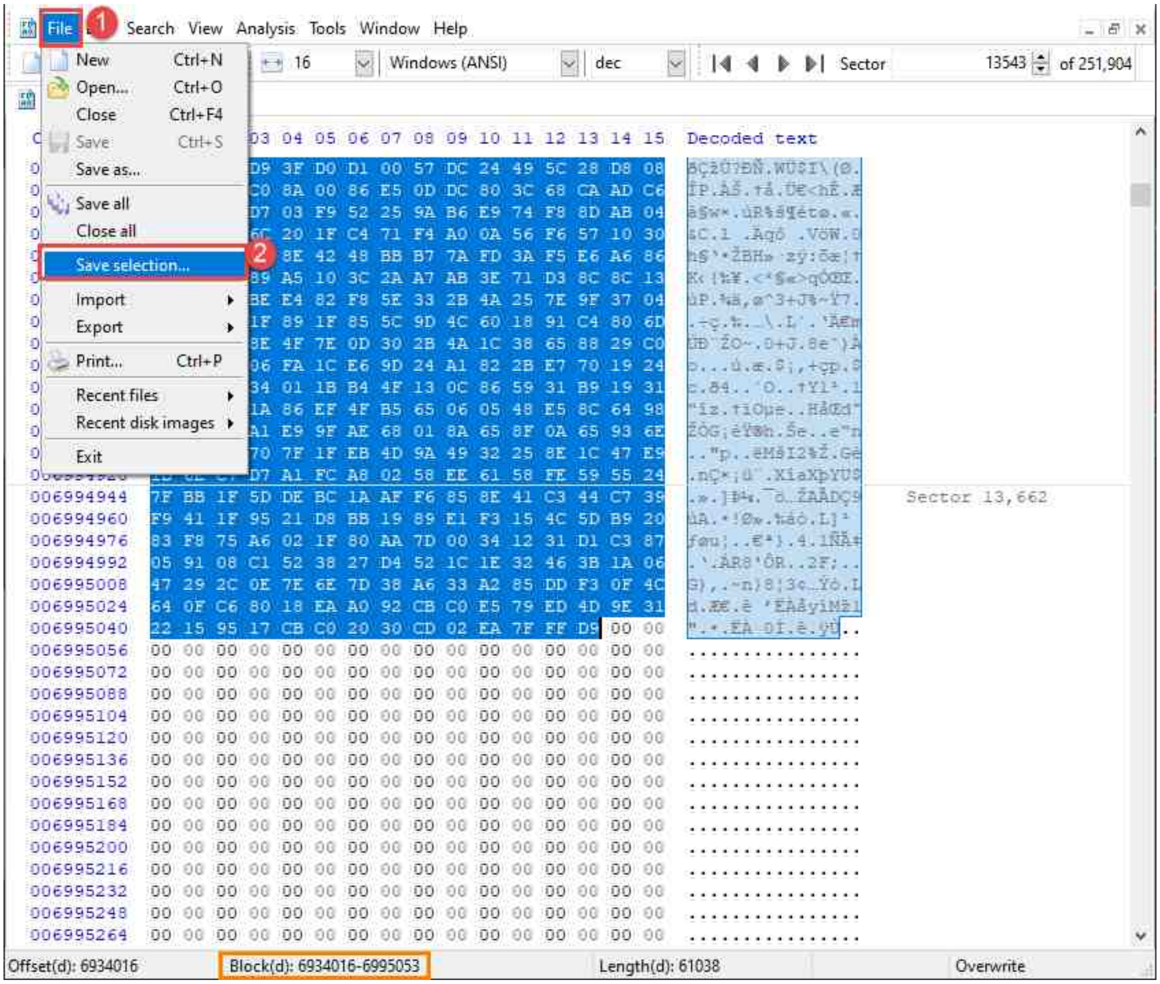
○ Length: 61038

○ hex ● dec ○ oct

OK Cancel

Offset(d): 6995053 | Block(d): 6995053-6995053 | Length(d): 1 | Overwrite

9. As we did with the first and the second documents, let us save this selection as a file by browsing to the File dropdown menu from the menu bar and clicking Save Selection as highlighted in items 1 and 2 below. This will open the Save selection as window.

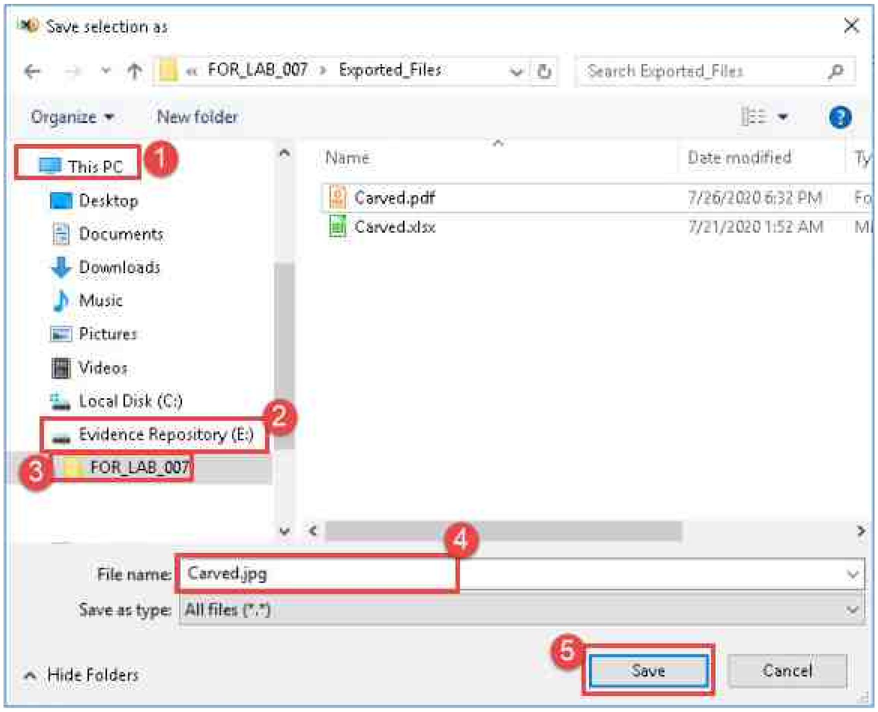


```
006994944  7F BB 1F 5D DE BC 1A AF F6 85 8E 41 C3 44 C7 39
006994960  F9 41 1F 95 21 D8 BB 19 89 E1 F3 15 4C 5D B9 20
006994976  83 F8 75 A6 02 1F 80 AA 7D 00 34 12 31 D1 C3 87
006994992  05 91 08 C1 52 38 27 D4 52 1C 1E 32 46 3B 1A 06
006995008  47 29 2C 0E 7E 6E 7D 38 A6 33 A2 85 DD F3 0F 4C
006995024  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
006995072  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995088  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995104  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995136  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995152  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995168  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995184  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995216  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995232  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995248  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
006995264  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 | Overwrite

Use the Block value in the status bar highlighted above to determine if you have highlighted the beginning and end of the file. The Block value should look like this Block(d): 6934016 - 6995053.

10. In the Save selection as window, browse to the folder you created earlier at ThisPC > Evidence Repository > FOR_LAB_007 > Exported_Files. Type the name `carved.jpg` and then click Save as highlighted in items 1, 2, 3, 4, and 5, respectively.

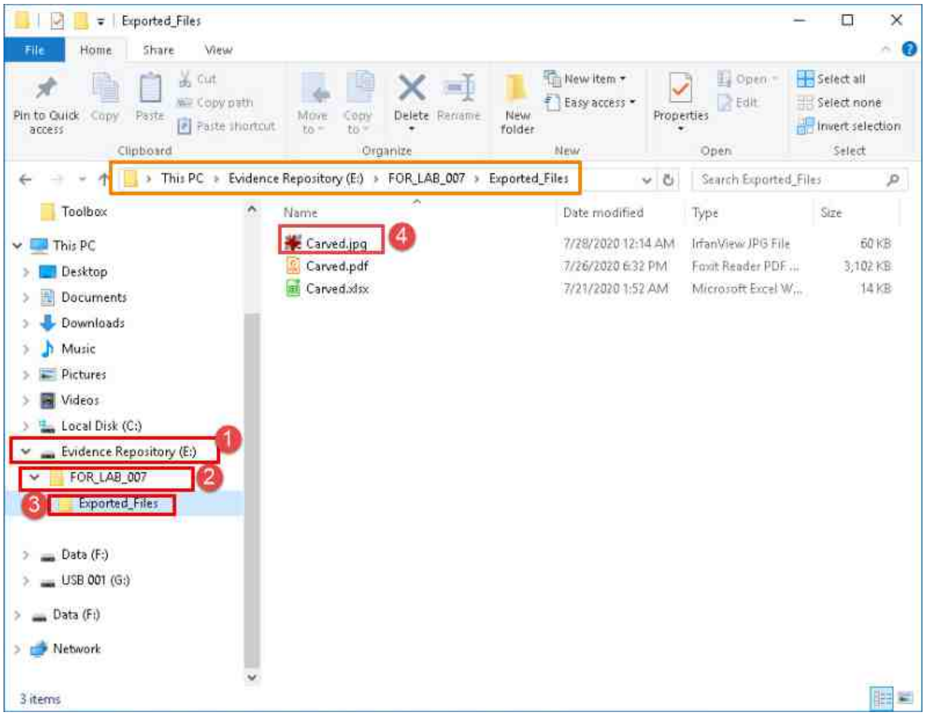


Name	Date modified	Ty
Carved.pdf	7/26/2020 6:32 PM	Fo
Carved.xlsx	7/21/2020 1:52 AM	Mi

File name: Carved.jpg

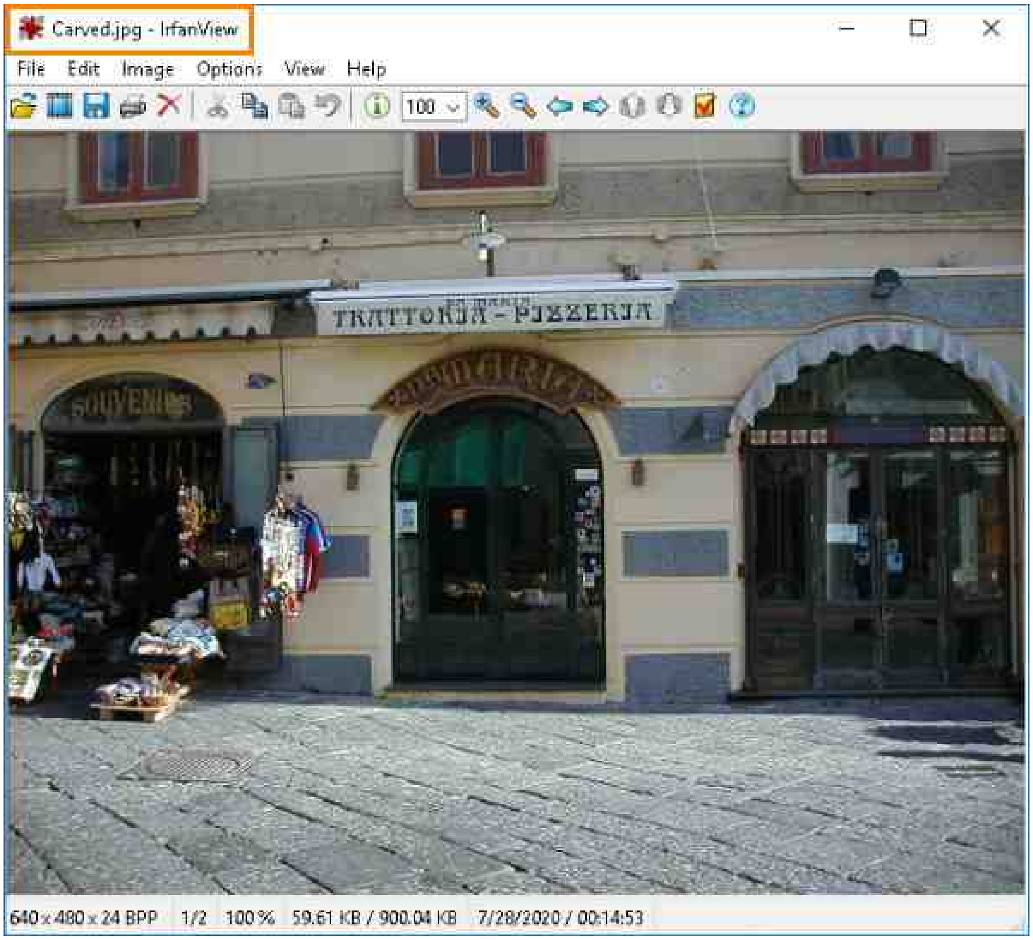
Save as type: All files (*.*)

11. Now browse to the location of the file by opening Windows File Explorer and browsing to the path Evidence Repository (E:) > FOR_LAB_007 > Exported_Files and double-clicking the file you saved, called `carved.pdf` as highlighted at items 1, 2, 3, and 4.



Name	Date modified	Type	Size
Carved.jpg	7/28/2020 12:14 AM	IrfanView JPG File	60 KB
Carved.pdf	7/26/2020 6:32 PM	Foxit Reader PDF ...	3,102 KB
Carved.xlsx	7/21/2020 1:52 AM	Microsoft Excel W...	14 KB

12. If you successfully carved the file, it should look like the one below. The file should open without any errors, which would mean you successfully carved the file.

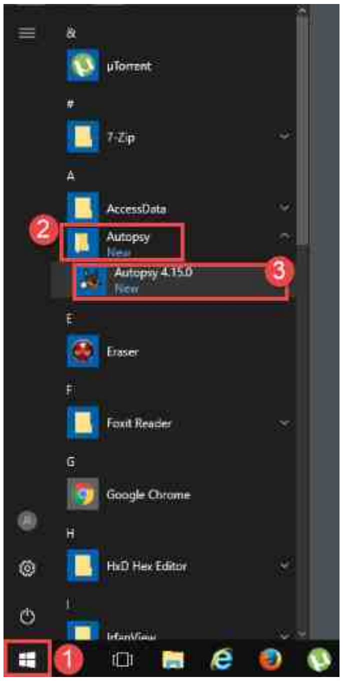

Carved.jpg - IrfanView
File Edit Image Options View Help
100
TRATTORIA - PIZZERIA
SOUVENIRS
640 x 480 x 24 BPP 1/2 100 % 59.61 KB / 900.04 KB 7/28/2020 / 00:14:53

13. This task was quite tedious but rewarding. In practice, examiners need to be able to view and interpret hex/raw text values. Practicing manual file carving is a great way to become familiar with different types of signatures and file content. It is by no means efficient, however. In the next exercise, we will teach you how to automate carving using Autopsy Forensics.
14. We will now move on to the next exercise. Before continuing, close the HxD and any other open windows by clicking the X at the top-right corner of the windows.

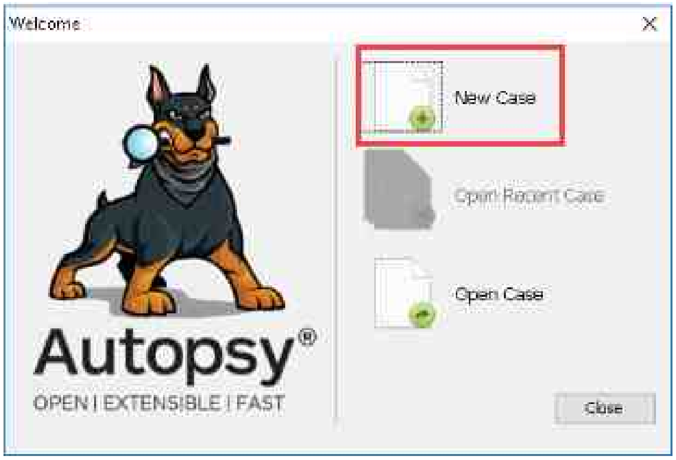
5 File Carving with Autopsy

File carving is normally done using automated programs because of practicality. We will walk you through automating the process and comparing the results you got from manual carving with the results from automated carving.

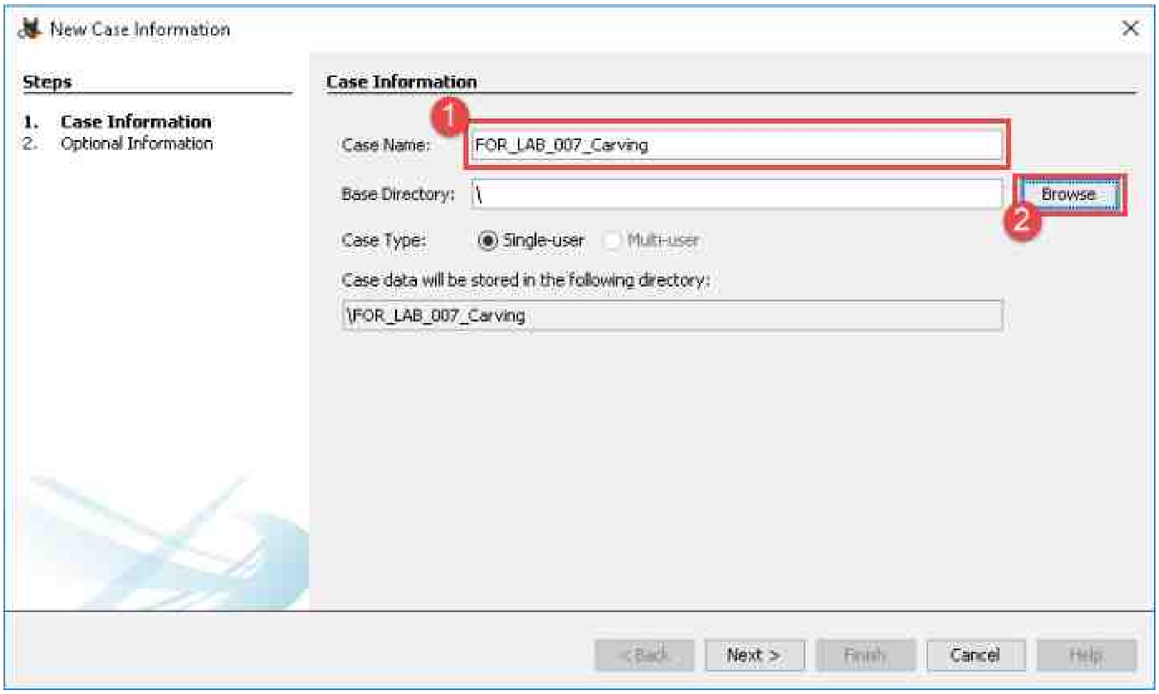
1. Launch the Autopsy program from the Start menu by navigating to Start > Autopsy > Autopsy 4.15.0. Alternatively, you can open Autopsy from the Desktop by clicking the Autopsy icon:



2. The Welcome window will appear; click New Case as highlighted below. This will open the New Case Information window.



3. In the New Case Information window, enter the name `FOR_LAB_007_Carving` as the Case Name, as highlighted in item 1 below. Next, let us change the Base Directory by clicking Browse as highlighted in item 2 below.


New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: FOR_LAB_007_Carving

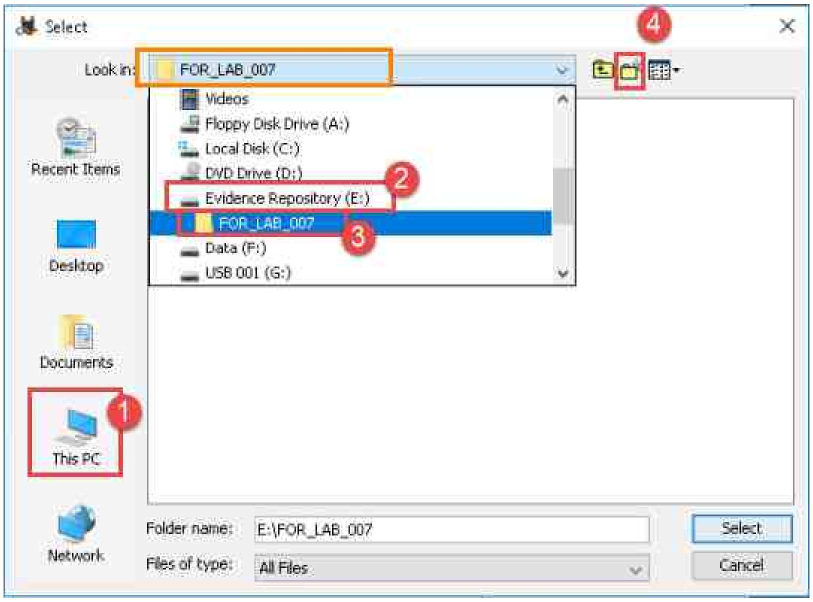
Base Directory: \

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

\FOR_LAB_007_Carving

4. In the Select window, we can browse to the desired location for our case folder. Let us do this by browsing to the folder FOR_LAB_007 that you created earlier at ThisPC > Evidence Repository > FOR_LAB_007 as highlighted in items 1, 2, and 3, respectively. Once there, create a new folder by clicking the Make New Folder button as highlighted in item 4.


Select

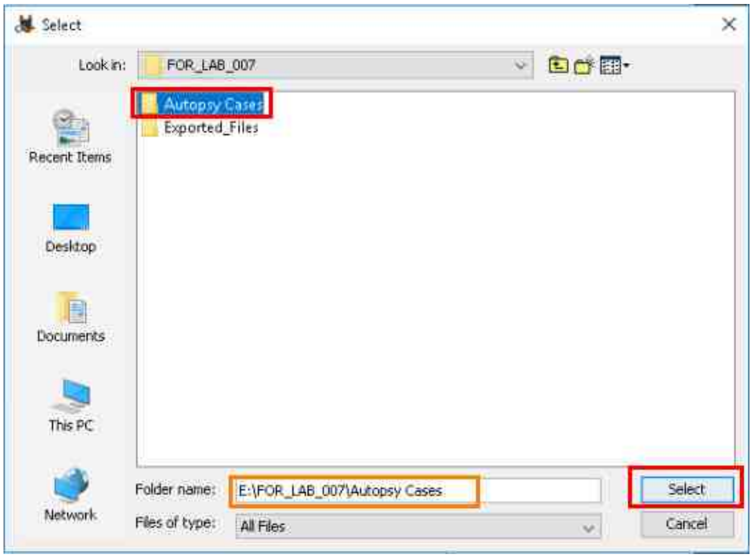
Look in: FOR_LAB_007

Videos
Floppy Disk Drive (A:)
Local Disk (C:)
DVD Drive (D:)
Evidence Repository (E:)
FOR_LAB_007
Data (F:)
USB 001 (G:)

Folder name: E:\FOR_LAB_007

Files of type: All Files

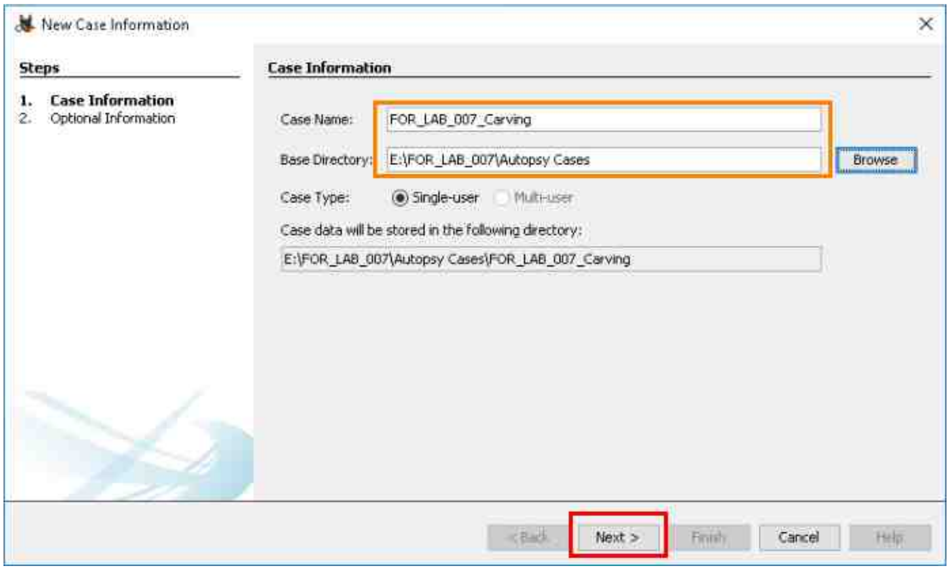
5. Name this new folder `Autopsy Cases` and then select it by clicking it once and then click the Select button as highlighted below. This will add the location to the Base Directory field in the New Case information window.



Folder name: E:\FOR_LAB_007\Autopsy Cases

Files of type: All Files

6. Once you are back to the New Case Information window, verify that all the fields are correct and then click Next as highlighted below.



Case Name: FOR_LAB_007_Carving

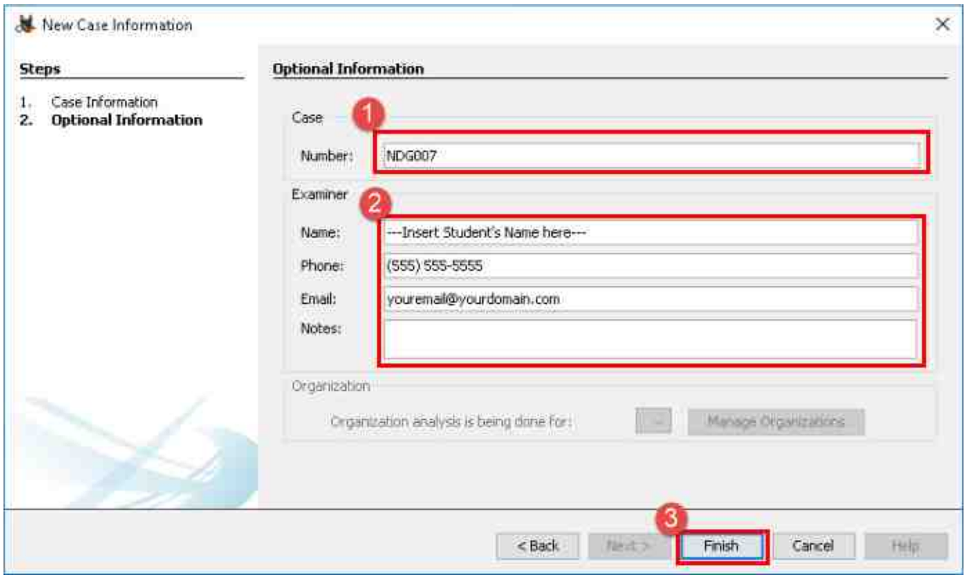
Base Directory: E:\FOR_LAB_007\Autopsy Cases

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

E:\FOR_LAB_007\Autopsy Cases\FOR_LAB_007_Carving

7. The next window in the New Case wizard is the Optional Information window. Here you can type more information about the case and examiner. Fill out the information with your details where highlighted as items 1 and 2 below and click Finish as highlighted at item 3.



Number: NDG007

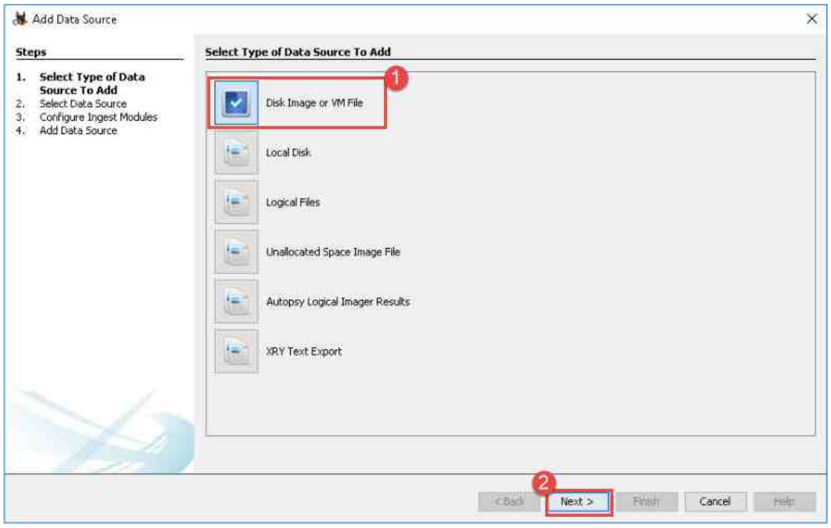
Name: ---Insert Student's Name here---

Phone: (555) 555-5555

Email: youremail@yourdomain.com

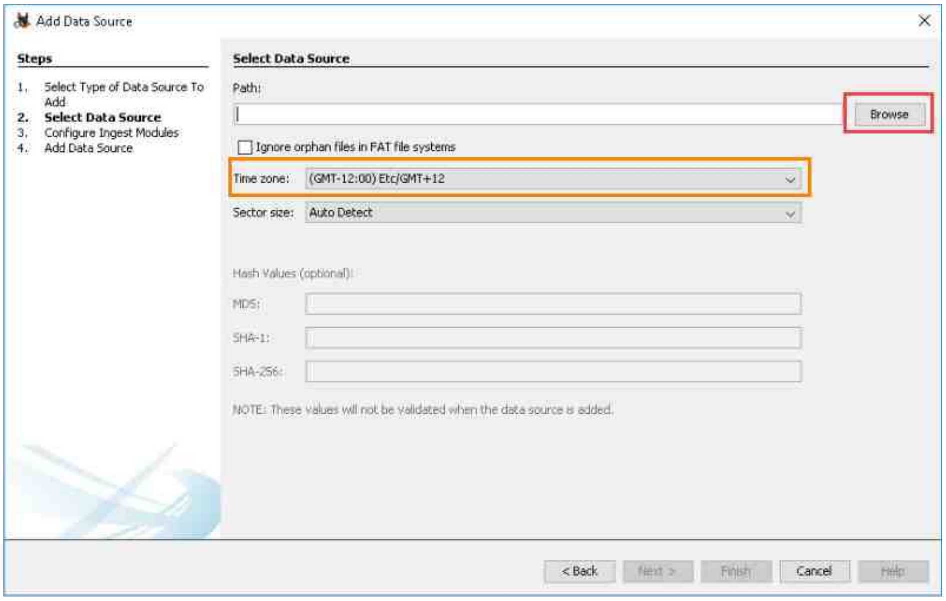
Even though this section is for Optional Information, case notes are always import.

8. You will now be taken to the Add Data Source window. Here you can choose between different evidence sources. In this exercise, we will be using an FEF so let us leave that as default as well and click Next as highlighted below.


Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Type of Data Source To Add
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help
1
2

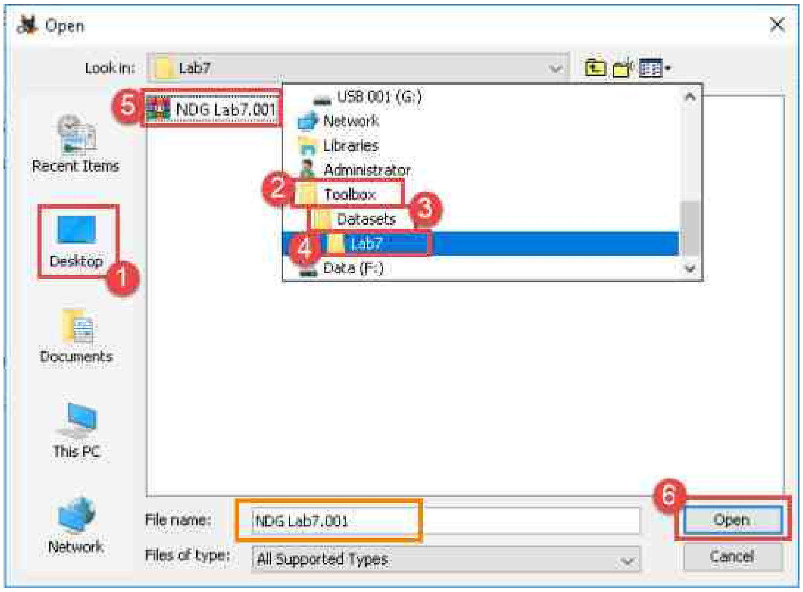
☑ Disk Image or VM File

9. The next window will allow you to choose the image you want to add to the case. Click the Browse button highlighted below to open the Open window that allows you to browse for the FEF.

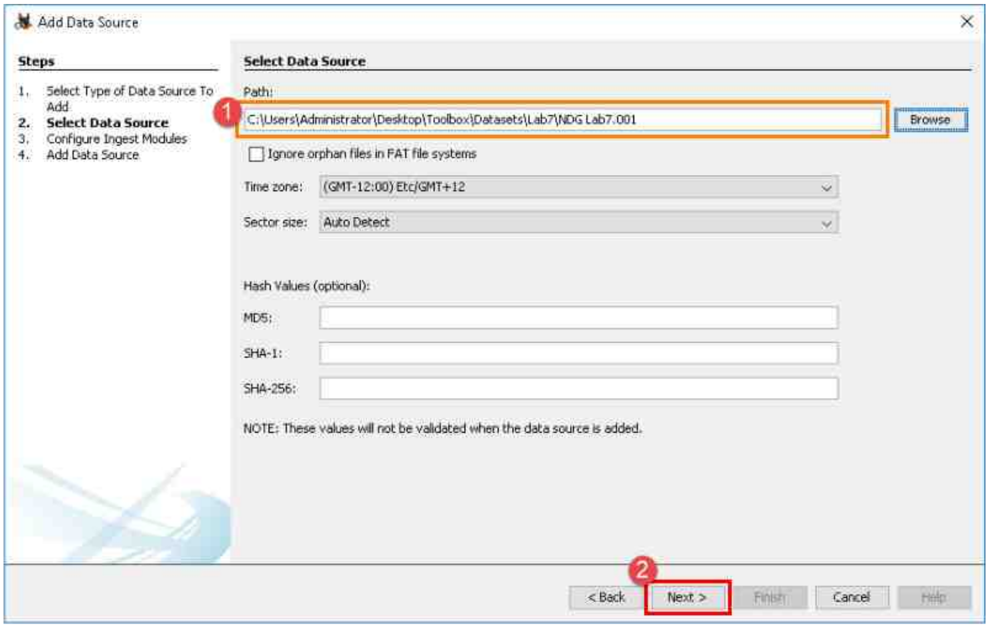

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Data Source
Path:
Browse
□ Ignore orphan files in FAT file systems
Time zone: (GMT-12:00) Etc/GMT+12
Sector size: Auto Detect
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
NOTE: These values will not be validated when the data source is added.
< Back
Next >
Finish
Cancel
Help

Use the dropdown menu to select your time zone.

10. In the Open window, browse to Desktop > Toolbox > Datasets > Lab 7 and click the file called NDG Lab7.001 as highlighted in items 1, 2, 3, 4, and 5, and then click Open as highlighted in item 6 below.



11. The image path will now appear in the Path field highlighted as item 1 below. We will leave the other options as is and click Next highlighted as item 2 below.



C:\Users\Administrator\Desktop\Toolbox\Datasets\Lab7\NDG Lab7.001

□ Ignore orphan files in FAT file systems

Time zone: (GMT-12:00) Etc/GMT+12

Sector size: Auto Detect

Hash Values (optional):

MD5:

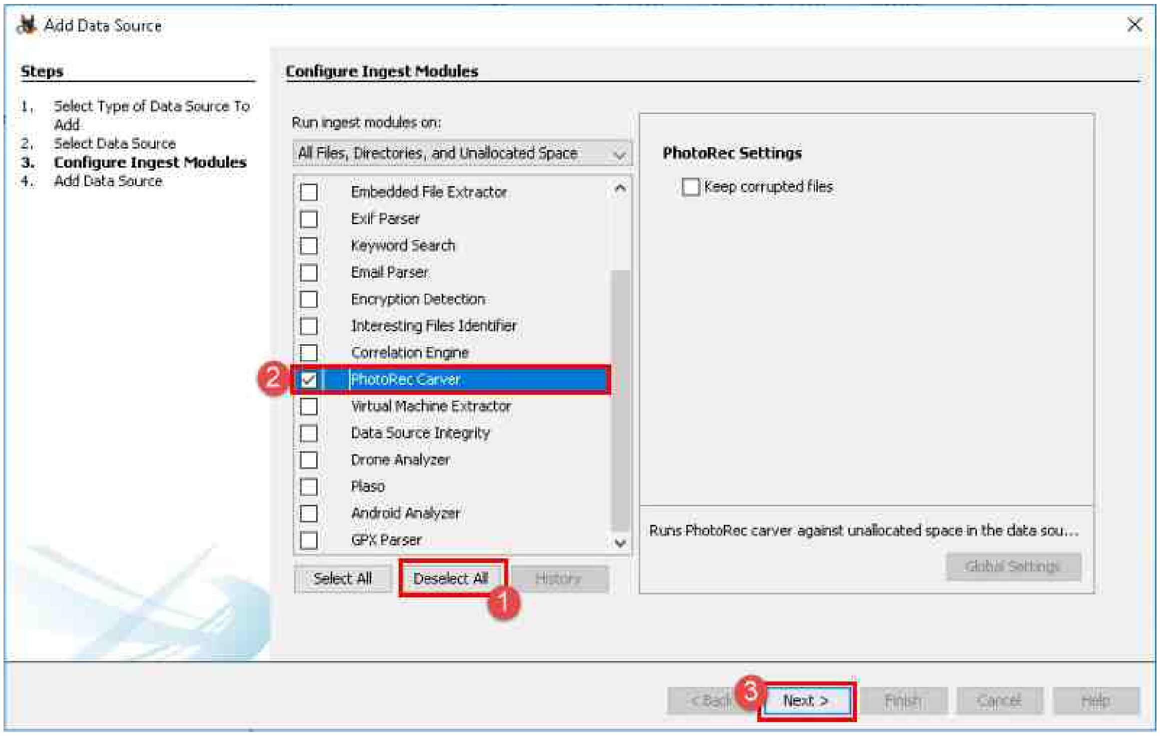
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

12. You will be taken to the Configure Ingest Modules step of the case creation process. As you know, Autopsy uses Ingest Modules to extract different types of data from data sources. The extracted data is then displayed in the main GUI window after the process is complete.

13. Click the Deselect All button highlighted as item 1 below to remove any previously selected modules. We will only use the Photorec Carver Ingest Module, highlighted as item 2 below. This module allows you to carve files from the FEF. The only option in this Ingest Modules is Keep corrupt files, which toggles whether Autopsy should keep and display corrupted carved files. Let us leave it off and click Next highlighted as item 3 below. This process will carve all the files it can from this volume and provide the results as soon as it is done.



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

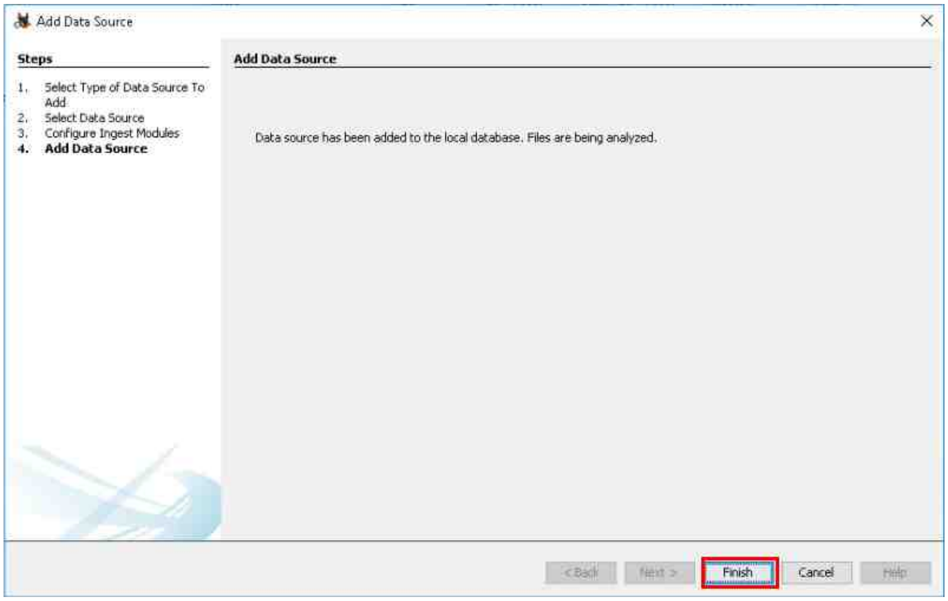
□ Embedded File Extractor
□ Exif Parser
□ Keyword Search
□ Email Parser
□ Encryption Detection
□ Interesting Files Identifier
□ Correlation Engine
☑ PhotoRec Carver
□ Virtual Machine Extractor
□ Data Source Integrity
□ Drone Analyzer
□ Plaso
□ Android Analyzer
□ GPX Parser

PhotoRec Settings

□ Keep corrupted files

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

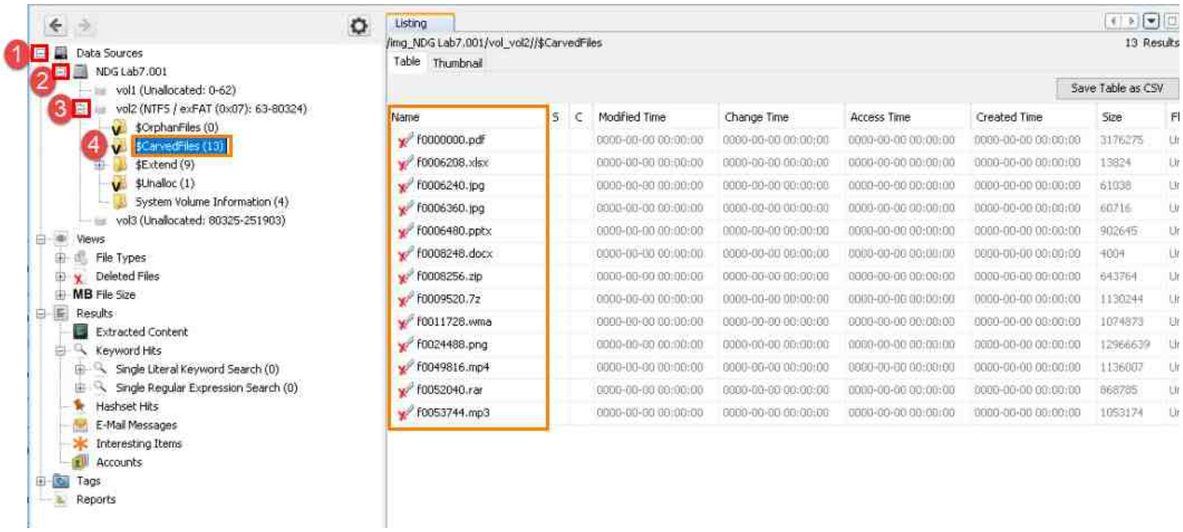
14. You will be presented with the final screen, indicating that the files are being analyzed. Click Finish as highlighted below:



Data source has been added to the local database. Files are being analyzed.

You can use the status bar in the bottom-right corner to see the progress of the carve.

15. You will now be taken to the Autopsy main window. Once the carve is done, you can find the results in the tree pane. The results of the file carve will be added to the case and can be found by clicking the + sign beside Data Sources to expand it, as highlighted in item 1 below. Next, expand the image file by clicking the + sign beside LAB007.001 as highlighted in item 2 below. Finally, let us expand the NTFS / exFAT volume by clicking the + beside vol2 (NTFS / exFAT (0x07): 63-80324) as highlighted in item 3 below. You will see 5 folders in the root of this volume. Click the one called $CarvedFiles (13), as highlighted in item 4 below, to reveal the carved files.



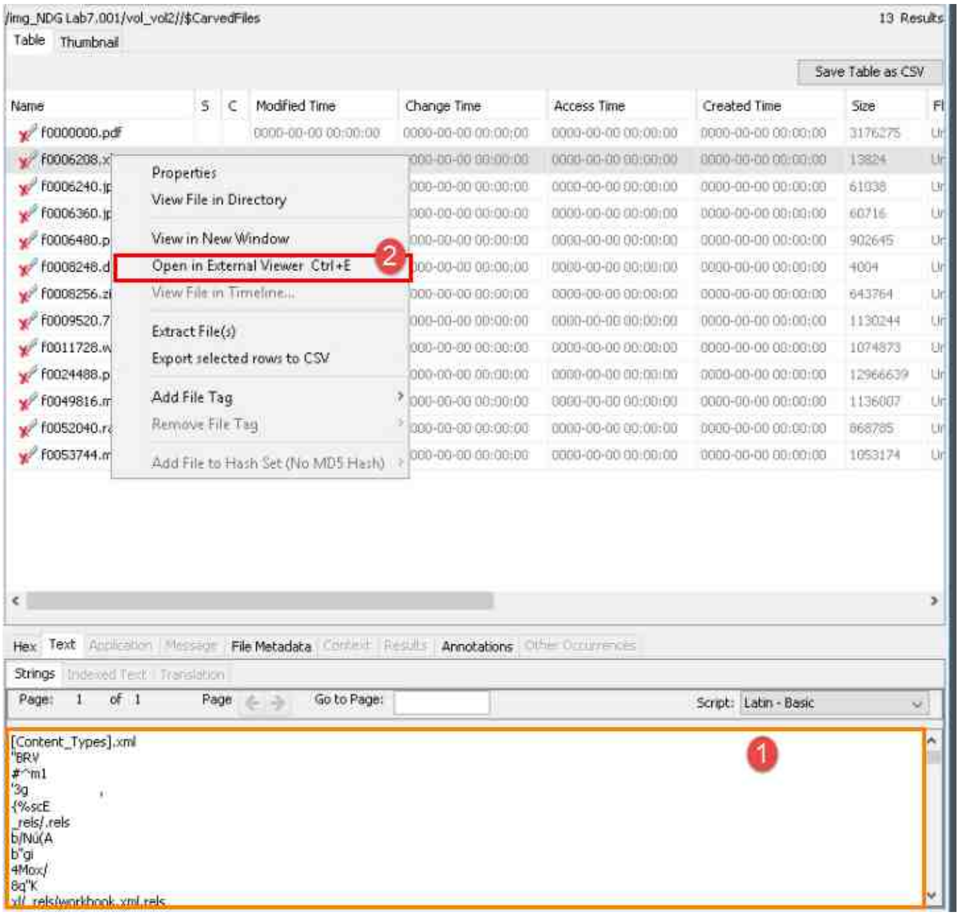
/img_NDG Lab7.001/vol_vol2//$CarvedFiles

13 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Fl
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur

Autopsy displays a number in brackets to denote the number of files within a tree pane entry.

16. As you can see in the list, there were 13 deleted files that were carved from unallocated space. Each of these files contains legitimate data. You can click on certain files to view their content in the view pane as highlighted in item 1 below. There is also a way to view these files using an external file viewer. To do this, select the file you would like to view and right-click on it and click Open in External Viewer as highlighted in item 2 below. Alternatively, you can use Ctrl+E. This will open the file using the computer's associated viewer. During your search, you will find familiar files, the ones you carved in the previous exercises.

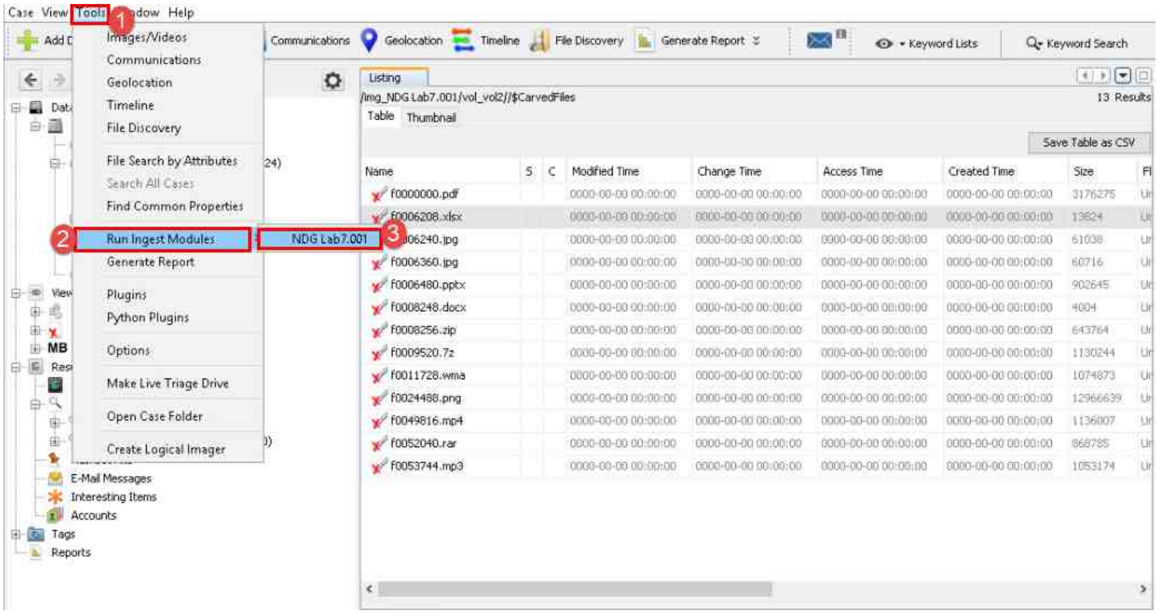


Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Fl
f0000000.pdf			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3176275	Ur
f0006208.x				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13824	Ur
f0006240.jp				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	61038	Ur
f0006360.jp				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	60716	Ur
f0006480.p				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	902645	Ur
f0008248.d				00-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4004	Ur
f0008256.zi				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	643764	Ur
f0009520.7				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1130244	Ur
f0011728.w				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1074873	Ur
f0024488.p				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12966639	Ur
f0049816.m				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1136007	Ur
f0052040.ra				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	868785	Ur
f0053744.m				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1053174	Ur

```
[Content_Types].xml
"BRV
#^m1
'3g
{%scE
_rels/.rels
b/Nú(A
b"gi
4Mox/
8q"K
xl/_rels/workbook.xml.rels
```

The names of carved files will not be the original file name. Different programs have different naming conventions. Autopsy uses Photorec Carver which uses cluster/block number for naming files and will rename the file if there is enough metadata embedded within the file to do so. To find out more, check out: https://www.cgsecurity.org/testdisk.pdf

17. 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.

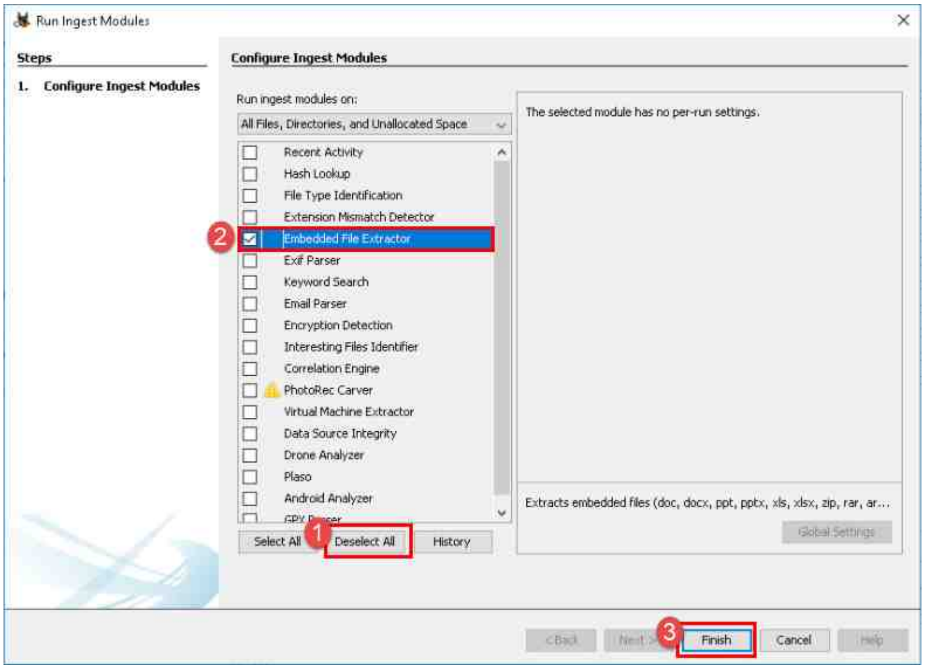


/img_NDG Lab7.001/vol_vol2//$CarvedFiles

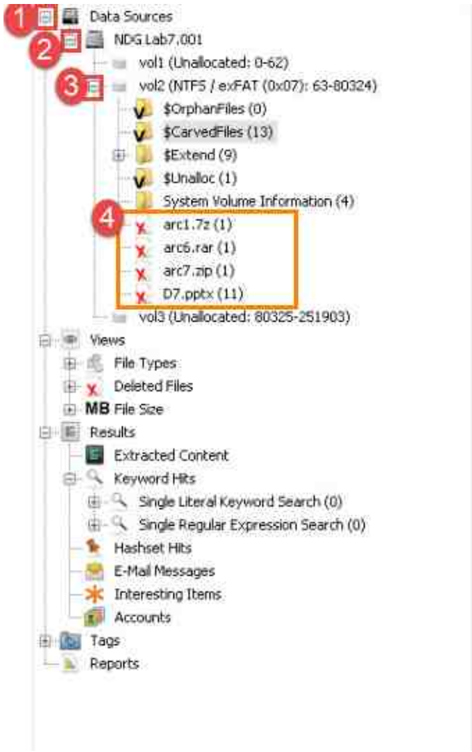
13 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Fl
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	Ur
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	Ur
06240.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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur
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	Ur

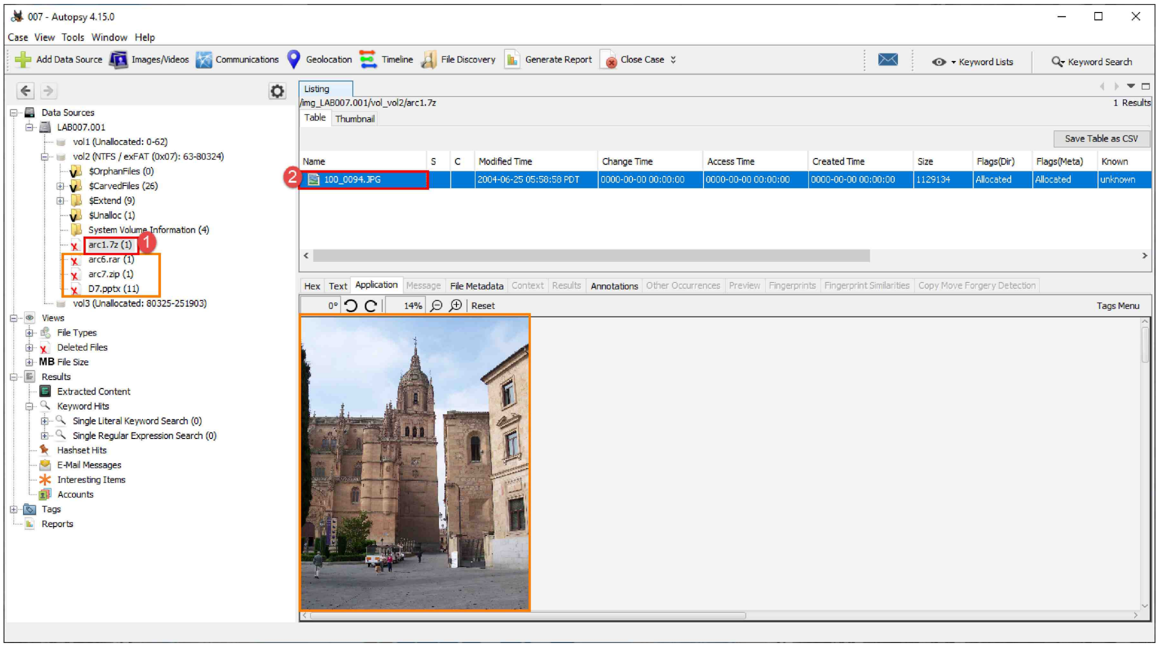
18. Now that we are back in the Run Ingest Modules window, let us use the Embedded File Extractor Ingest Module. Let us begin by clicking the Deselect All button highlighted as item 1 below to remove any previously selected modules. Then click the checkbox beside Embedded File Extractor as highlighted in item 2 below. This module will expand all archive \ compound files and add their content to the case. It has no additional settings so let us just run it by clicking Finish as highlighted in item 3 below.



19. You will once again be taken back to the Autopsy main window. Once the module is done, you can find the results in the tree pane. The results are located in the root volume it found the files in. It should still be at that location, but if it is not, then it can be found by clicking the + sign beside Data Sources to expand it, as highlighted in item 1 below. Next, expand the image file by clicking the + sign beside LAB007.001 it as highlighted in item 2 below. Finally, let us expand the NTFS / exFAT volume by clicking the + beside vol2 (NTFS / exFAT (0x07): 63-80324) as highlighted in item 3 below. You will see the results appear below the folders as highlighted in item 4 below.



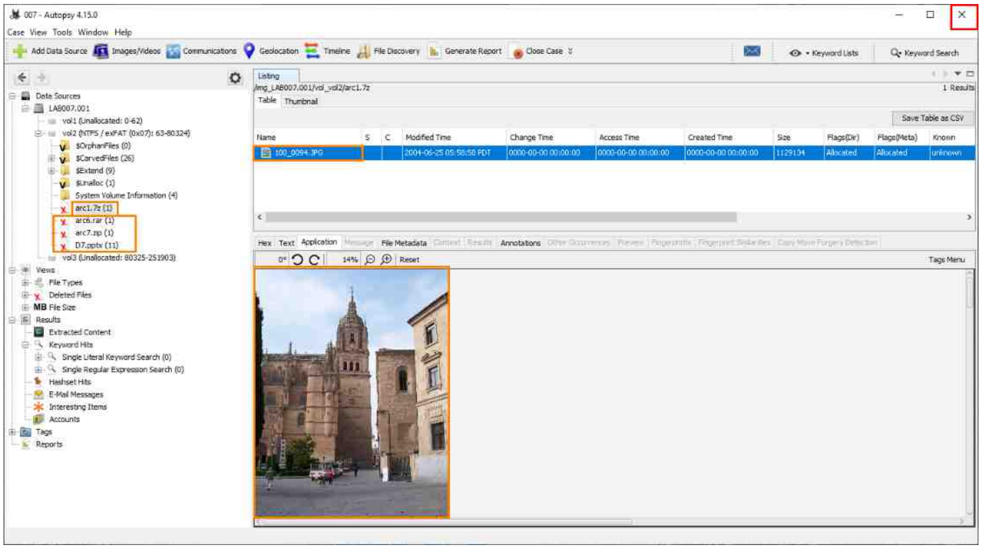
20. You can view the content of each of these archive\compound files by clicking them, as highlighted at item 1 below.



Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
100_0094.JPG			2004-06-25 05:58:58 PDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1129134	Allocated	Allocated	unknown

21. In this exercise, you learned how to use Autopsy to carve files and expand compound files. These techniques are almost always necessary in full forensic examinations. Understanding how they work will help you become an efficient forensic expert.

22. The exercise is now done; close the Autopsy program by clicking the X at the top-right corner of the main window as highlighted below. Close any other windows that are open as well.



Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
100_0094.JPG			2004-06-25 05:58:58 PDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1129134	Allocated	Allocated	unknown