FORENSICS V2 LAB SERIES

Lab 10: Steganography and Alternate Data Streams

Document Version: 2021-01-14

Contents

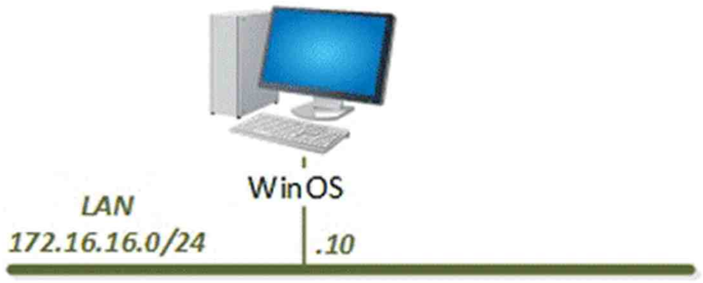
Introduction

In digital forensics, data hiding techniques are commonly reviewed to ensure that nothing is overlooked. Steganography and Alternate Data Streams (ADS) are data hiding techniques that attempt to mislead investigators by hiding potential evidence in seemingly unimportant files.

Objectives

- Learn what steganography and ADS are
- How to identify a file hidden in another file
- Learn how to review ADSs and identify hidden files within them
- Learn how to create your own ADS and file within a file

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.

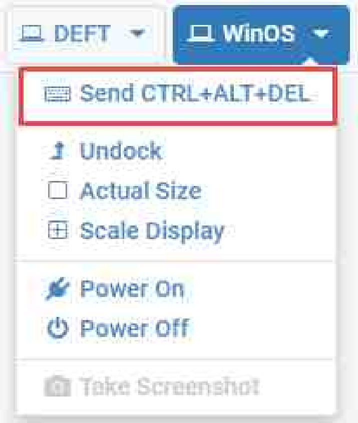
Virtual Machine	**IP Address / Subnet Mask**	**Account** (if needed)	**Password** (if needed)
Caine	172.16.16.30	caine	Train1ng$
CSI-Linux	172.16.16.40	csi	csi
DEFT	172.16.16.20	deft	Train1ng$
WinOS	172.16.16.10	Administrator	Train1ng$

1 Steganography – Creating a Message Inside a File

New anti-forensic techniques are always being discovered and utilized to hide, manipulate, and destroy data. Steganography is one such technique, and even though it is not new, it is very effective in hiding data in plain sight. It is commonly used for transmitting illicit files and communicating secretly. In this exercise, we will teach you how to place a message inside a file. We will also teach you how to embed a file within another file. One of the easiest ways to do this is by using a hex editor. In this exercise, we will use HxD.

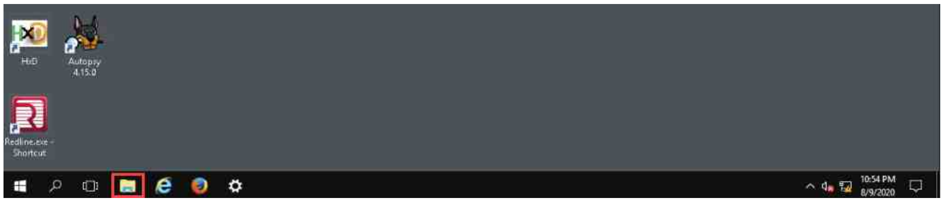
Before we begin this exercise, it is important to point out that you can damage files doing this. The exercise should not be performed on evidence items, as it can severely compromise the authenticity of a file. It is purely for providing a deeper understanding of what simple steganography looks like.

1. 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.

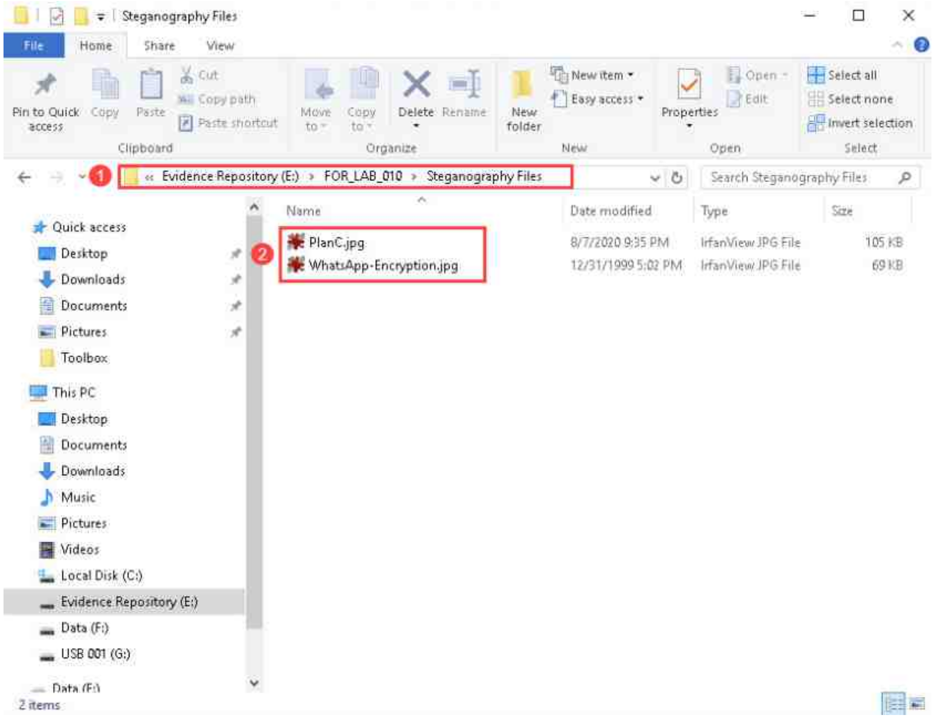


   b. Log in as `Administrator` using the password: `Train1ng$`

2. Let us begin by looking at the files we want to examine in their native format. Once we are done, we can view them in the hex editor. Begin by opening Windows File Explorer. Do this by clicking the File Explorer icon from the taskbar as highlighted below.

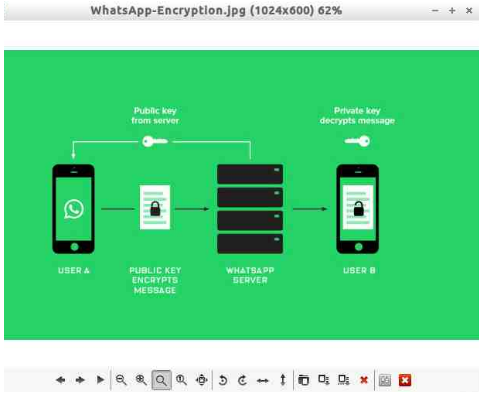


3. In File Explorer, browse to This PC > Evidence Repository (E:) > FOR_LAB_010 > Steganography Files, as highlighted in item 1 below. There you will see two files, PlanC.jpg and WhatsApp-Encryption.jpg. Double-click each file to open it, as seen in item 2 below.

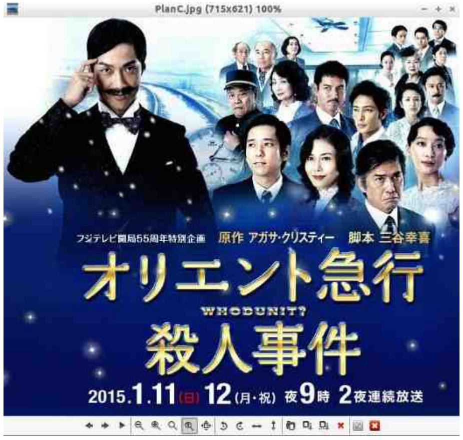


Name	Date modified	Type	Size
PlanC.jpg	8/7/2020 9:35 PM	IrfanView JPG File	105 KB
WhatsApp-Encryption.jpg	12/31/1999 5:02 PM	IrfanView JPG File	69 KB

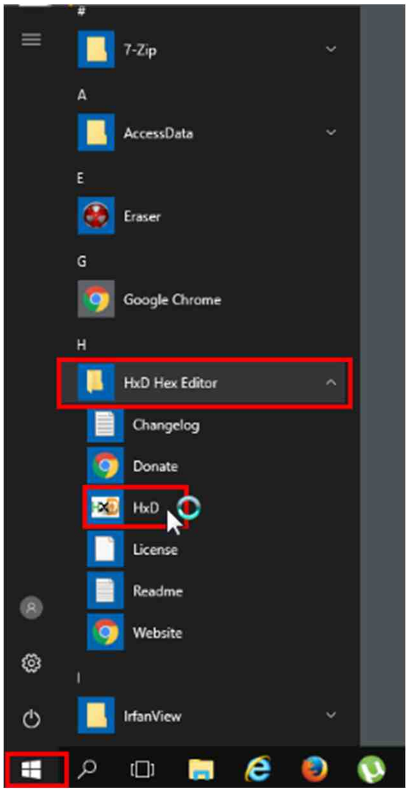
WhatsApp-Encryption.jpg


WhatsApp-Encryption.jpg (1024x600) 62%
Public key from server
Private key decrypts message
USER A
PUBLIC KEY ENCRYPTS MESSAGE
WHATSAPP SERVER
USER B

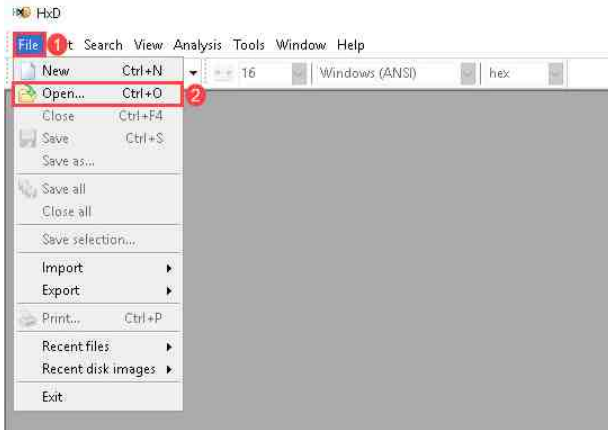
PlanC.jpg


PlanC.jpg (715x621) 100%
フジテレビ開局55周年特別企画 原作 アガサ・クリスティー 脚本 三谷幸喜
オリエント急行
WHODUNIT?
殺人事件
2015.1.11(日) 12(月・祝) 夜9時 2夜連続放送

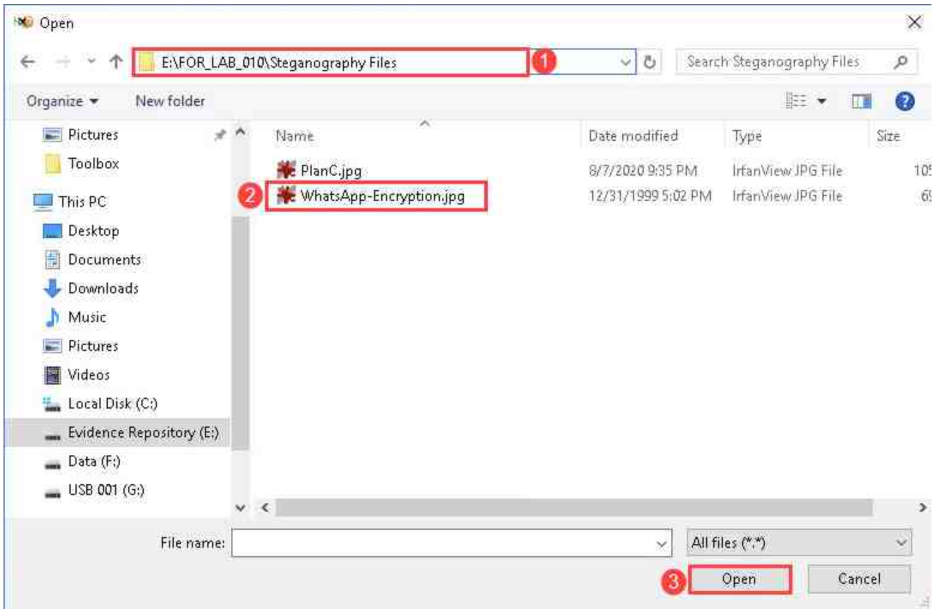
4. Now that you have seen the contents of the files through Windows File Explorer, let us take a deeper look using HxD. Let us launch the HxD program from the windows menu by navigating to Start Menu > HxD Hex Editor > HxD. Alternatively, you can open HxD Hex Editor from the Desktop by double-clicking the icon called HxD.



5. HxD will open and since you are familiar with it from the previous labs, let us dive right in by loading our first JPG file, WhatsApp-Encryption.jpg. Begin by navigating to File > Open as highlighted in items 1 and 2 below.

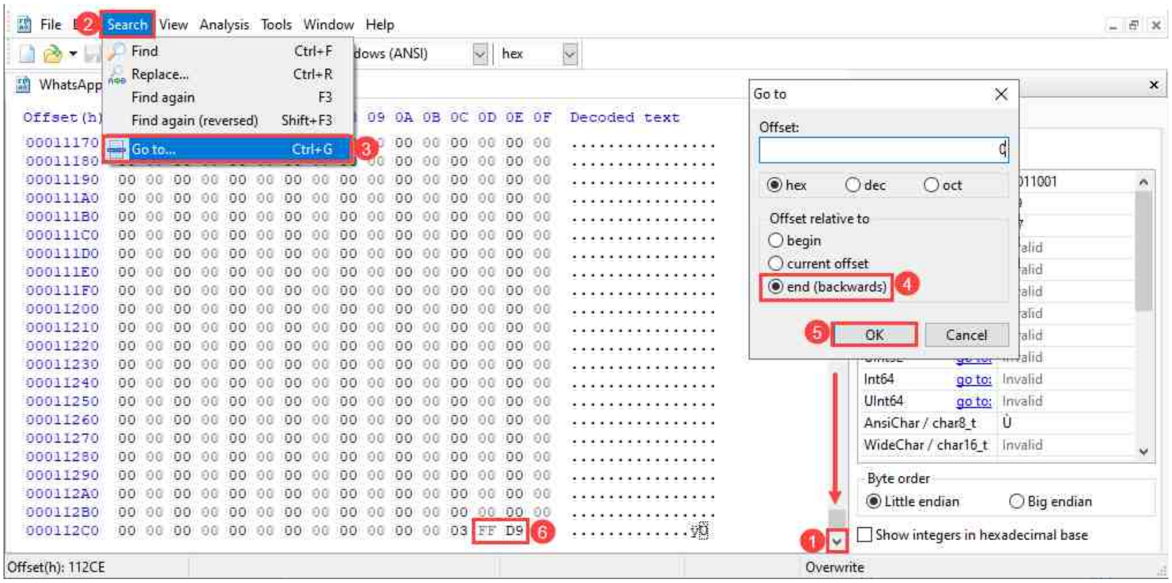


6. The Open window will appear. Browse to Evidence Repository (E:) > FOR_LAB_010 > Steganography Files as seen in item 1 below. Once there, click the file called WhatsApp-Encryption.jpg and then click Open, as seen in items 2 and 3 below.



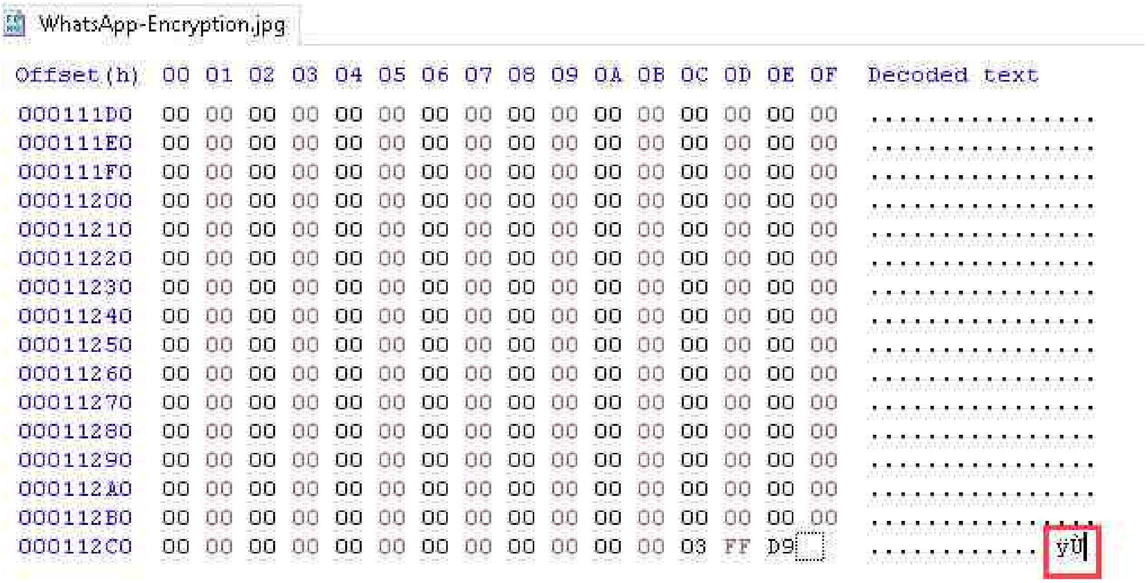
Name	Date modified	Type	Size
PlanC.jpg	8/7/2020 9:35 PM	IrfanView JPG File	10
WhatsApp-Encryption.jpg	12/31/1999 5:02 PM	IrfanView JPG File	6

7. The file will now open in the main GUI. Begin by scrolling to the end of the file by clicking the arrow as highlighted in item 1 below or by using the mouse wheel until you get to the bottom of the page. Alternatively, you can use the Go to dialogue by navigating to Search > Go to… as seen in items 2 and 3. Once the Go to window appears, click the radio button beside end (backwards) and then click OK as seen in items 4 and 5. You can confirm that you are at the end of this file by reviewing the end of file marker. Since this is a JPG file, the end of file signature is 0xFF D9, as seen in item 6 below.



```
Offset(h)                                09 0A 0B 0C 0D 0E 0F  Decoded text
00011170                                 00 00 00 00 00 00 00  ................
00011180                                 00 00 00 00 00 00 00  ................
00011190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000111A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000111B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000111C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000111D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000111E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000111F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011210  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011220  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011230  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011240  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011250  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011260  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011270  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011280  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011290  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000112A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000112B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000112C0  00 00 00 00 00 00 00 00 00 00 00 00 03 FF D9     .............ÿÙ

Offset(h): 112CE
```

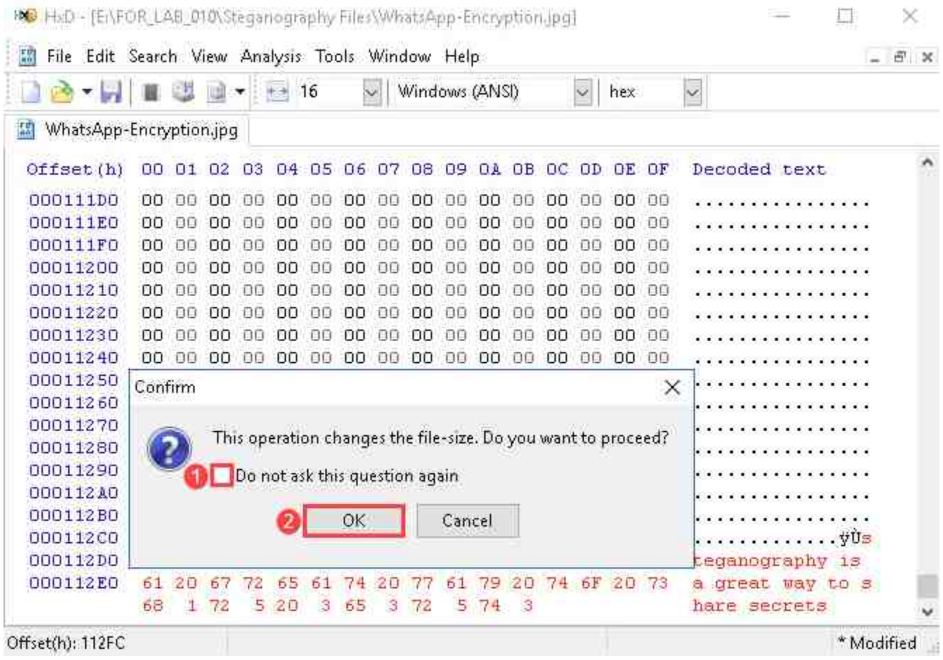
8. Adding data to a file can change the hash value and file size. If an investigator is familiar with the specific file, for example, a system file, they will be able to determine that something is unusual about the file. When placing messages in plain text in a file, you can use any area that has a NULL value or 0x00. Even then, it is best practice to place data at the end of the file, although this will change the size of the file. In this exercise, we will type a message at the end of this JPG file. To do this, click the last value in the text view pane as highlighted below.



WhatsApp-Encryption.jpg

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

000111D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000111E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000111F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011210  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011220  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011230  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011240  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011250  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011260  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011270  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011280  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011290  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000112A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000112B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000112C0  00 00 00 00 00 00 00 00 00 00 00 00 03 FF D9     .............ÿÙ
```

9. Once the cursor is in the correct position, begin typing the message: `steganography is a great way to share secrets` (or type a message of your choice). Once you start typing, a prompt will appear that warns you that the file size will change. Click the checkbox beside the Do not ask this question again message, and then click OK and continue to type the message.



HxD - [E:\FOR_LAB_010\Steganography Files\WhatsApp-Encryption.jpg]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
WhatsApp-Encryption.jpg

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

000111D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000111E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000111F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011210  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011220  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011230  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011240  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00011250                                                   ................
00011260                                                   ................
00011270                                                   ................
00011280                                                   ................
00011290                                                   ................
000112A0                                                   ................
000112B0                                                   ................
000112C0                                                   .............ÿÙs
000112D0                                                   teganography is
000112E0  61 20 67 72 65 61 74 20 77 61 79 20 74 6F 20 73  a great way to s
          68  1 72  5 20  3 65  3 72  5 74  3              hare secrets
```

Confirm

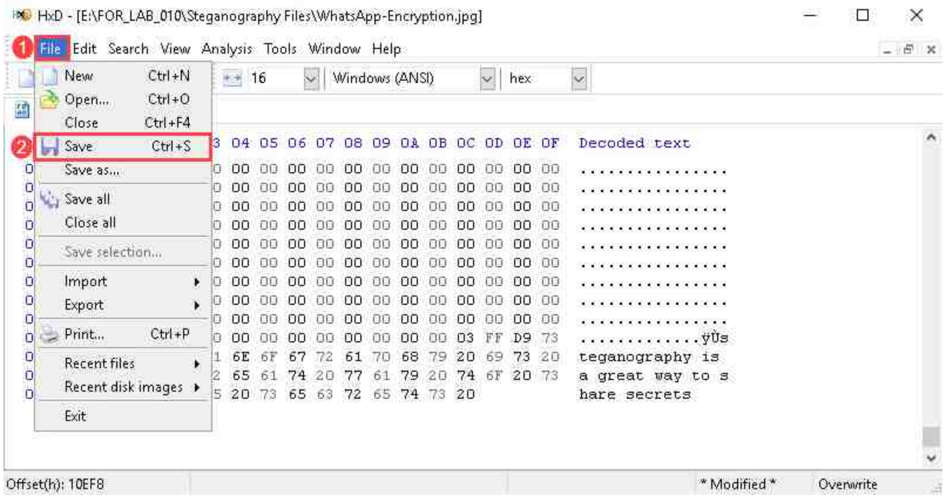
This operation changes the file-size. Do you want to proceed?

1 ☐ Do not ask this question again

2 OK Cancel

Offset(h): 112FC * Modified

10. When you are done typing your message, save the file by browsing to File > Save, highlighted in items 1 and 2 below. Alternatively, you can use Ctrl+S.

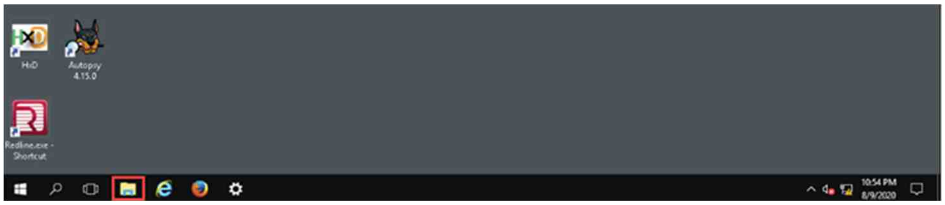


```
3 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F   Decoded text
0 00 00 00 00 00 00 00 00 00 00 00 00   ................
0 00 00 00 00 00 00 00 00 00 00 00 00   ................
0 00 00 00 00 00 00 00 00 00 00 00 00   ................
0 00 00 00 00 00 00 00 00 00 00 00 00   ................
0 00 00 00 00 00 00 00 00 00 00 00 00   ................
0 00 00 00 00 00 00 00 00 00 00 00 00   ................
0 00 00 00 00 00 00 00 00 00 00 00 00   ................
0 00 00 00 00 00 00 00 00 00 00 00 00   ................
0 00 00 00 00 00 00 00 00 00 00 00 00   ................
0 00 00 00 00 00 00 00 00 03 FF D9 73   .............ÿÙs
1 6E 6F 67 72 61 70 68 79 20 69 73 20   teganography is
2 65 61 74 20 77 61 79 20 74 6F 20 73   a great way to s
5 20 73 65 63 72 65 74 73 20            hare secrets
```

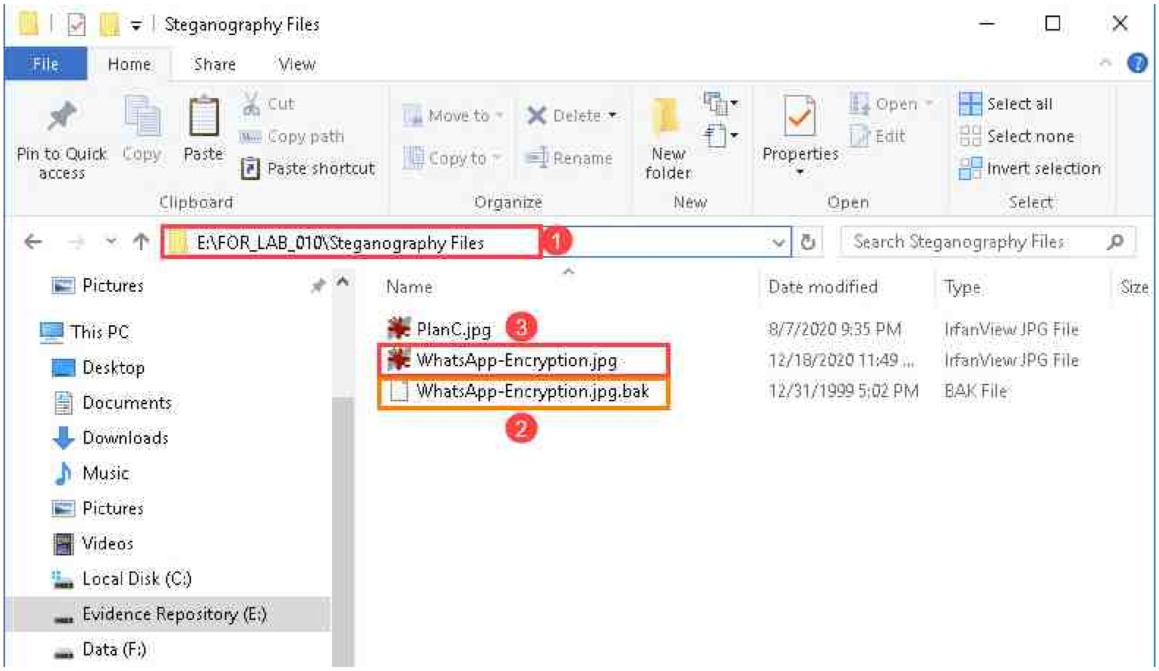
Please Note

Steganography (an anti-forensic technique) is used to hide, manipulate and destroy data. It is not practiced by forensics examiners. However, it is important to know how it is done.

11. That was it. The message is saved in the file and can be sent to someone who knows that a hidden message is there. You can look at the file again to look for changes. To do this, double-click the File Explorer icon from the Desktop, as highlighted below.



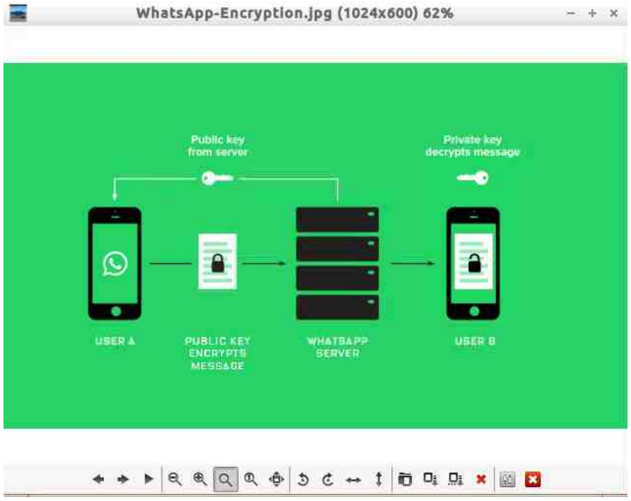
12. In File Explorer, browse to Evidence Repository (E:) > FOR_LAB_010 > Steganography Files, as seen in item 1. You will see the file you edited called WhatsApp-Encryption.jpg in this folder. Whenever HxD is used to edit a file, it creates a backup file with the extension .bak in the same folder, as seen in item 2 below. Let us double-click the file we edited called WhatsApp-Encryption.jpg, as seen in item 3 below.



E:\FOR_LAB_010\Steganography Files

Name	Date modified	Type	Size
PlanC.jpg	8/7/2020 9:35 PM	IrfanView JPG File	
WhatsApp-Encryption.jpg	12/18/2020 11:49 ...	IrfanView JPG File	
WhatsApp-Encryption.jpg.bak	12/31/1999 5:02 PM	BAK File	

13. If you followed the instructions correctly, your file will open like nothing happened, as seen below.

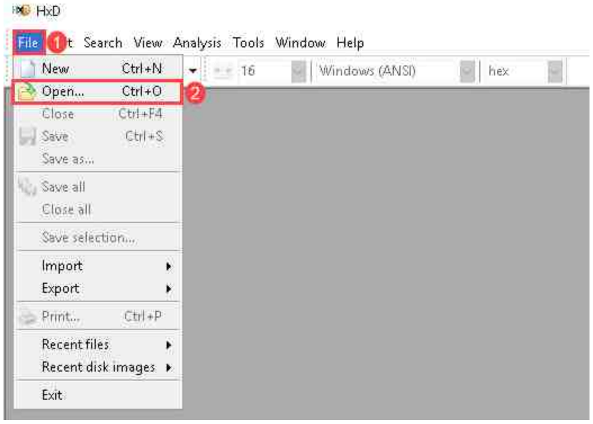


14. The only way to see the message you typed is to view the file’s contents in hex or raw text view. This is because most picture viewers stop at the end of file signature 0xFF D9 and will ignore all data after that.
15. Now let us look at the other file and try to extract some data from it.

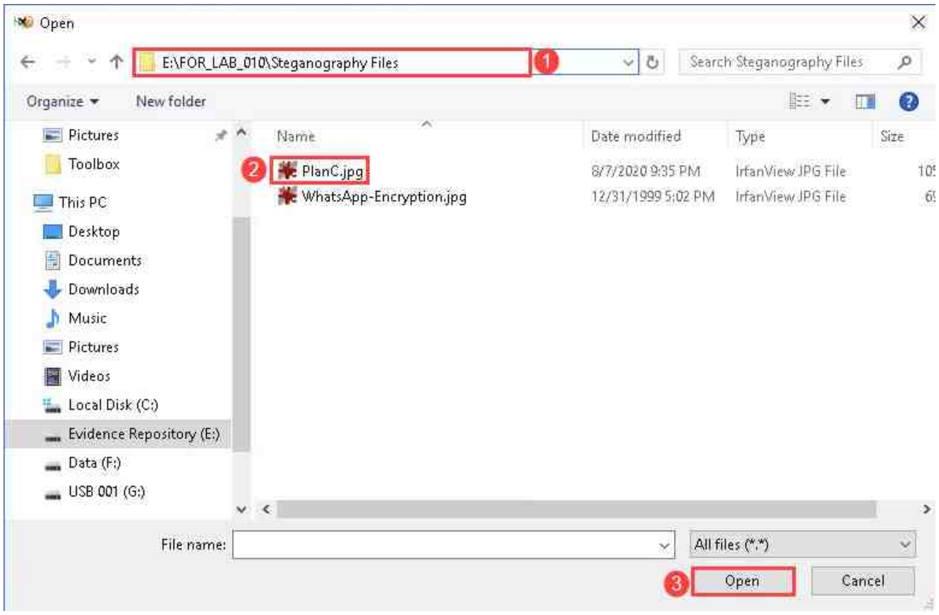
2 Steganography – Extracting a File from Within Another File

In this exercise, we will be extracting a file from within the file called PlanC.jpg. This is a file that was previously modified and contains another file within it. For simplicity, this one only contains a single PNG file, but it is common to find formats such as ZIP, XLSX, DOCX, and many other file types. Being able to identify the file signatures will allow you to identify and extract the correct data when the need arises.

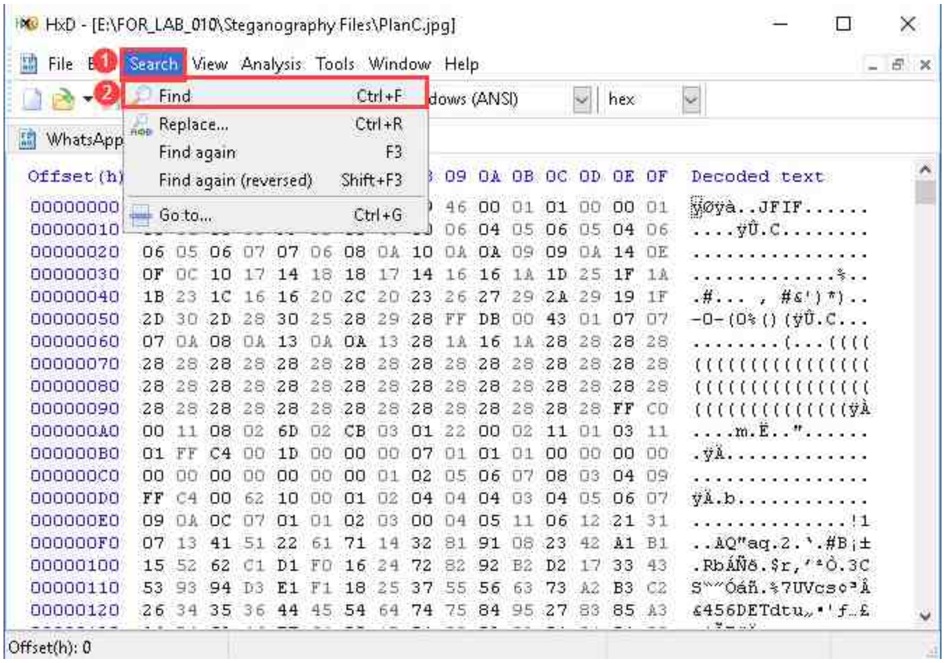
1. Let us begin by opening the file called PlanC.jpg in HxD. If you closed HxD, reopen it, and then navigate to File > Open, as highlighted in items 1 and 2 below.



2. The Open window will appear. Browse to Evidence Repository (E:) > FOR_LAB_010 > Steganography Files as seen in item 1 below. Once there, click the file called PlanC.jpg and then click Open as seen in items 2 and 3 below.

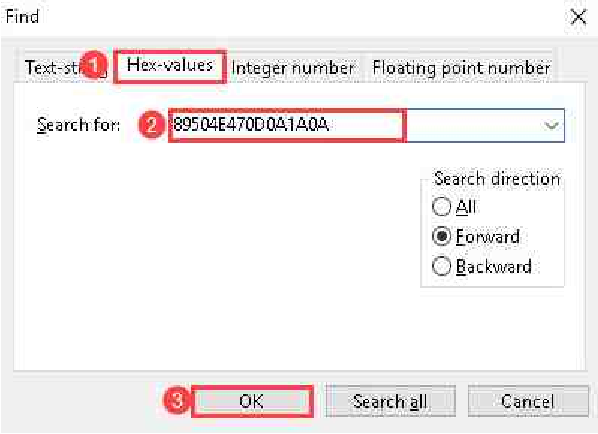


3. The file called PlanC.jpg will now open in HxD and you will see the hex and text representation of the file populate the main GUI window. Now that the file is open, let us search for the PNG signature. To do this, open the Find window by navigating to Edit > Find as seen in items 1 and 2 below. Alternatively, you can use Ctrl+F.



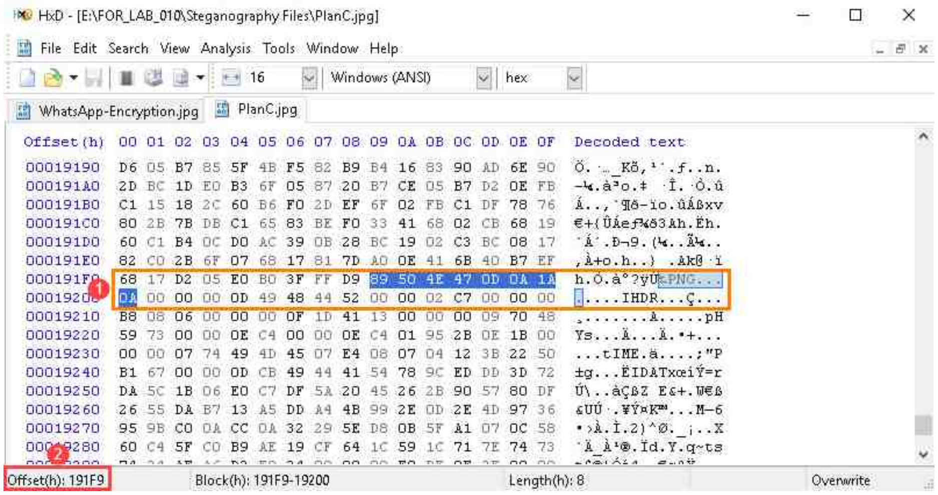
```
Offset (h)                           9 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000                             9 46 00 01 01 00 00 01  ÿØÿà..JFIF......
00000010                             0 06 04 05 06 05 04 06  ....ÿÛ.C........
00000020  06 05 06 07 07 06 08 0A 10 0A 0A 09 09 0A 14 0E  ................
00000030  0F 0C 10 17 14 18 18 17 14 16 16 1A 1D 25 1F 1A  .............%..
00000040  1B 23 1C 16 16 20 2C 20 23 26 27 29 2A 29 19 1F  .#... , #&')*)..
00000050  2D 30 2D 28 30 25 28 29 28 FF DB 00 43 01 07 07  -0-(0%()(ÿÛ.C...
00000060  07 0A 08 0A 13 0A 0A 13 28 1A 16 1A 28 28 28 28  ........(...((((
00000070  28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28  ((((((((((((((((
00000080  28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28  ((((((((((((((((
00000090  28 28 28 28 28 28 28 28 28 28 28 28 28 28 FF C0  ((((((((((((((ÿÀ
000000A0  00 11 08 02 6D 02 CB 03 01 22 00 02 11 01 03 11  ....m.Ë.."......
000000B0  01 FF C4 00 1D 00 00 00 07 01 01 01 00 00 00 00  .ÿÄ.............
000000C0  00 00 00 00 00 00 00 01 02 05 06 07 08 03 04 09  ................
000000D0  FF C4 00 62 10 00 01 02 04 04 04 03 04 05 06 07  ÿÄ.b............
000000E0  09 0A 0C 07 01 01 02 03 00 04 05 11 06 12 21 31  ..............!1
000000F0  07 13 41 51 22 61 71 14 32 81 91 08 23 42 A1 B1  ..AQ"aq.2.‘.#B¡±
00000100  15 52 62 C1 D1 F0 16 24 72 82 92 B2 D2 17 33 43  .RbÁÑð.$r‚’²Ò.3C
00000110  53 93 94 D3 E1 F1 18 25 37 55 56 63 73 A2 B3 C2  S“”Óáñ.%7UVcs¢³Â
00000120  26 34 35 36 44 45 54 64 74 75 84 95 27 83 85 A3  &456DETdtu„•'ƒ…£
```

4. When the Find window opens, click the Hex-values tab as highlighted in item 1 below and type `89 50 4E 47 0D 0A 1A 0A` in the Search for field. Then click OK, as seen in items 2 and 3. The value you typed is the header for PNG files and will take you to the beginning of a PNG file if it exists inside the file.



Search for: 89504E470D0A1A0A

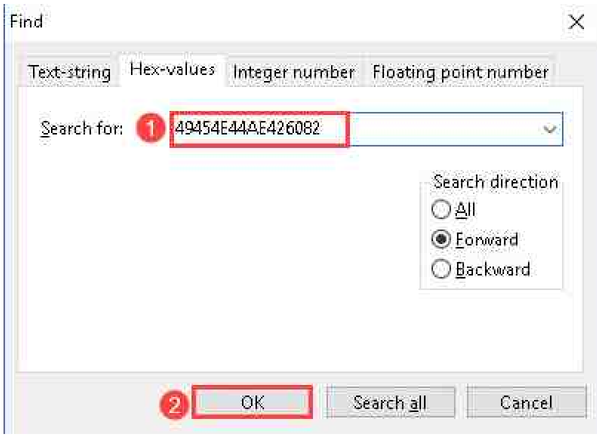
5. If you did everything correctly, you will be taken to the beginning of a PNG file, as seen below. Now that we have seen a header, let us note the offset, 0x191F9, as seen in item 2 below, and move on to searching for the end of file signature.


HxD - [E:\FOR_LAB_010\Steganography Files\PlanC.jpg]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
WhatsApp-Encryption.jpg
PlanC.jpg
1
2

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00019190  D6 05 B7 85 5F 4B F5 82 B9 B4 16 83 90 AD 6E 90  Ö.·…_Kõ,¹´.ƒ..n.
000191A0  2D BC 1D E0 B3 6F 05 87 20 B7 CE 05 B7 D2 0E FB  -¼.à³o.‡ ·Î.·Ò.û
000191B0  C1 15 18 2C 60 B6 F0 2D EF 6F 02 FB C1 DF 78 76  Á..,`¶ð-ïo.ûÁßxv
000191C0  80 2B 7B DB C1 65 83 BE F0 33 41 68 02 CB 68 19  €+{ÛÁeƒ¾ð3Ah.Ëh.
000191D0  60 C1 B4 0C D0 AC 39 0B 28 BC 19 02 C3 BC 08 17  `Á´.Ð¬9.(¼..Ã¼..
000191E0  82 C0 2B 6F 07 68 17 81 7D A0 0E 41 6B 40 B7 EF  ‚À+o.h..} .Ak@·ï
000191F0  68 17 D2 05 E0 B0 3F FF D9 89 50 4E 47 0D 0A 1A  h.Ò.à°?ÿÙ‰PNG...
00019200  0A 00 00 00 0D 49 48 44 52 00 00 02 C7 00 00 00  .....IHDR...Ç...
00019210  B8 08 06 00 00 00 0F 1D 41 13 00 00 00 09 70 48  ¸.......A.....pH
00019220  59 73 00 00 0E C4 00 00 0E C4 01 95 2B 0E 1B 00  Ys...Ä...Ä.•+...
00019230  00 00 07 74 49 4D 45 07 E4 08 07 04 12 3B 22 50  ...tIME.ä....;"P
00019240  B1 67 00 00 0D CB 49 44 41 54 78 9C ED DD 3D 72  ±g...ËIDATxœíÝ=r
00019250  DA 5C 1B 06 E0 C7 DF 5A 20 45 26 2B 90 57 80 DF  Ú\..àÇßZ E&+.W€ß
00019260  26 55 DA B7 13 A5 DD A4 4B 99 2E 0D 2E 4D 97 36  &UÚ·.¥Ý¤K™...M—6
00019270  95 9B C0 0A CC 0A 32 29 5E D8 0B 5F A1 07 0C 58  •›À.Ì.2)^Ø._¡..X
00019280  60 C4 5F C0 B9 AE 19 CF 64 1C 59 1C 71 7E 74 73  `Ä_À¹®.Ïd.Y.q~ts
```

Offset(h): 191F9 Block(h): 191F9-19200 Length(h): 8 Overwrite

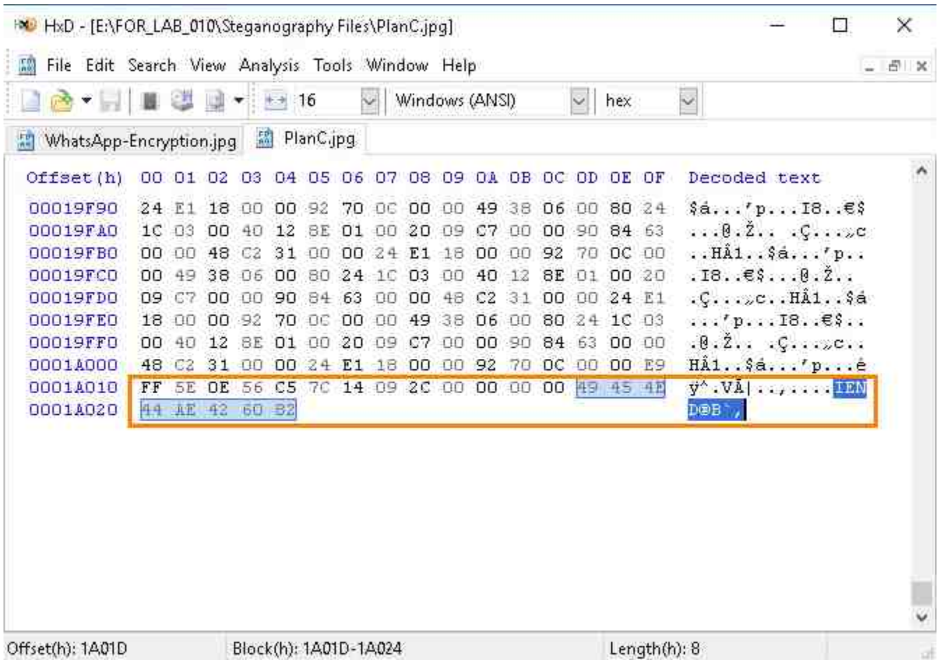
6. Go back to the Find window and type `49 45 4E 44 AE 42 60 82` in the Search for field and then click OK as seen in items 1 and 2 below.



Search for: 49454E44AE426082

Search direction
○ All
● Forward
○ Backward

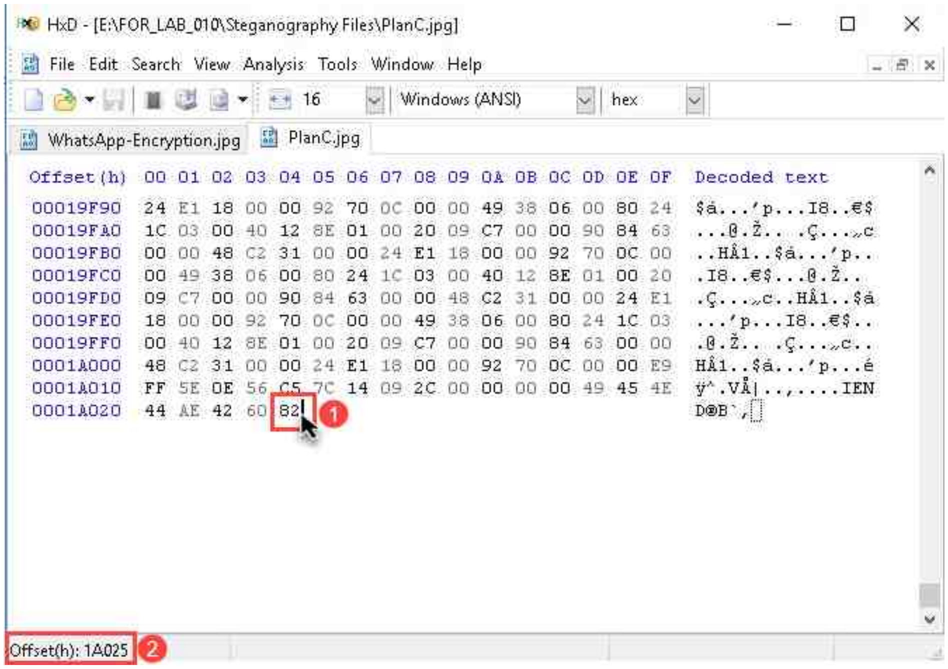
7. You will now be taken to the end of file signature (footer) for this file. As you can see, this value is at the end of the file PlanC.jpg. This is a good indicator that the PNG file was placed at the end of the JPG file.


HxD - [E:\FOR_LAB_010\Steganography Files\PlanC.jpg]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
WhatsApp-Encryption.jpg
PlanC.jpg

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00019F90  24 E1 18 00 00 92 70 0C 00 00 49 38 06 00 80 24  $á...’p...I8..€$
00019FA0  1C 03 00 40 12 8E 01 00 20 09 C7 00 00 90 84 63  ...@.Ž.. .Ç...„c
00019FB0  00 00 48 C2 31 00 00 24 E1 18 00 00 92 70 0C 00  ..HÂ1..$á...’p..
00019FC0  00 49 38 06 00 80 24 1C 03 00 40 12 8E 01 00 20  .I8..€$...@.Ž..
00019FD0  09 C7 00 00 90 84 63 00 00 48 C2 31 00 00 24 E1  .Ç...„c..HÂ1..$á
00019FE0  18 00 00 92 70 0C 00 00 49 38 06 00 80 24 1C 03  ...’p...I8..€$..
00019FF0  00 40 12 8E 01 00 20 09 C7 00 00 90 84 63 00 00  .@.Ž.. .Ç...„c..
0001A000  48 C2 31 00 00 24 E1 18 00 00 92 70 0C 00 00 E9  HÂ1..$á...’p...é
0001A010  FF 5E 0E 56 C5 7C 14 09 2C 00 00 00 00 49 45 4E  ÿ^.VÅ|..,....IEN
0001A020  44 AE 42 60 82                                   D®B`‚
```

Offset(h): 1A01D   Block(h): 1A01D-1A024   Length(h): 8

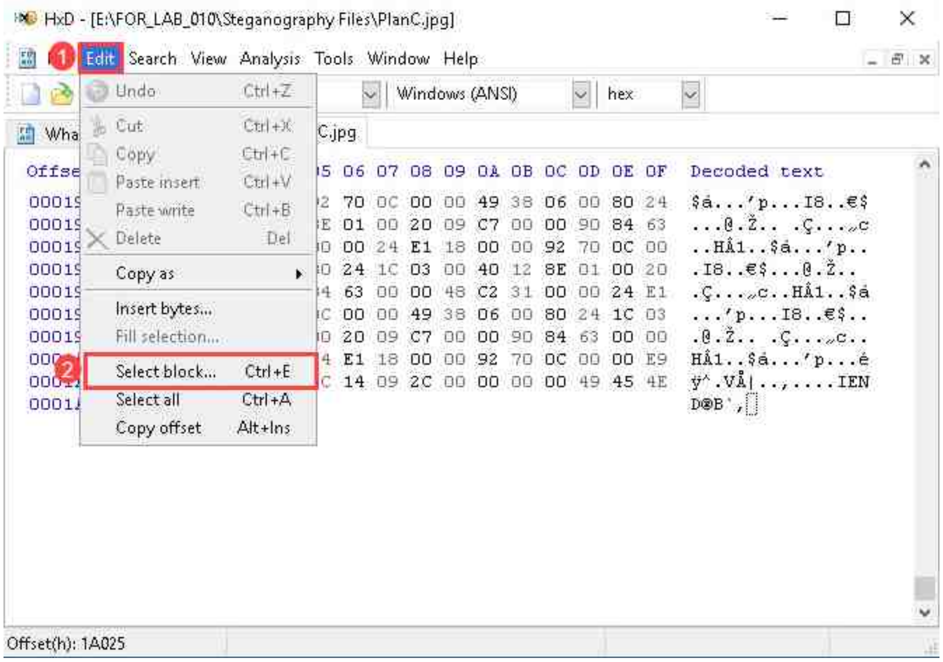
8. Let us note the offset by clicking the last value as seen in item 1 below. This will reveal the offset in the status bar, as seen in item 2. Note this offset as this denotes the end of the PNG file.


HxD - [E:\FOR_LAB_010\Steganography Files\PlanC.jpg]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
WhatsApp-Encryption.jpg
PlanC.jpg
1
2

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00019F90  24 E1 18 00 00 92 70 0C 00 00 49 38 06 00 80 24  $á...’p...I8..€$
00019FA0  1C 03 00 40 12 8E 01 00 20 09 C7 00 00 90 84 63  ...@.Ž.. .Ç...„c
00019FB0  00 00 48 C2 31 00 00 24 E1 18 00 00 92 70 0C 00  ..HÂ1..$á...’p..
00019FC0  00 49 38 06 00 80 24 1C 03 00 40 12 8E 01 00 20  .I8..€$...@.Ž..
00019FD0  09 C7 00 00 90 84 63 00 00 48 C2 31 00 00 24 E1  .Ç...„c..HÂ1..$á
00019FE0  18 00 00 92 70 0C 00 00 49 38 06 00 80 24 1C 03  ...’p...I8..€$..
00019FF0  00 40 12 8E 01 00 20 09 C7 00 00 90 84 63 00 00  .@.Ž.. .Ç...„c..
0001A000  48 C2 31 00 00 24 E1 18 00 00 92 70 0C 00 00 E9  HÂ1..$á...’p...é
0001A010  FF 5E 0E 56 C5 7C 14 09 2C 00 00 00 00 49 45 4E  ÿ^.VÅ|..,....IEN
0001A020  44 AE 42 60 82                                   D®B`‚
```

Offset(h): 1A025

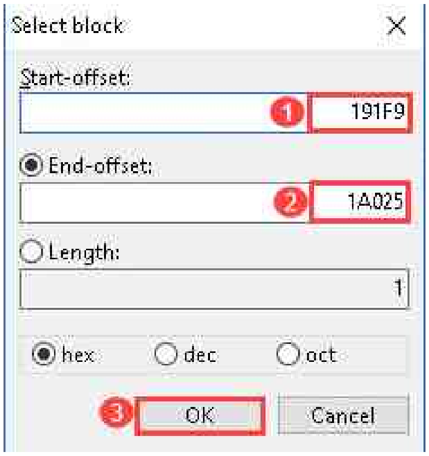
9. Now let us use the Select block feature to highlight the data between the first and last byte offsets. To do this, navigate to Edit > Select block as seen in items 1 and 2 below. Alternatively, you can use Ctrl+E.



```
Offse  )5 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
0001S  )2 70 0C 00 00 49 38 06 00 80 24  $á...’p...I8..€$
0001S  )E 01 00 20 09 C7 00 00 90 84 63  ...@.Ž.. .Ç...„c
0001S  )0 00 24 E1 18 00 00 92 70 0C 00  ..HÅ1..$á...’p..
0001S  )0 24 1C 03 00 40 12 8E 01 00 20  .I8..€$...@.Ž..
0001S  )4 63 00 00 48 C2 31 00 00 24 E1  .Ç...„c..HÂ1..$á
0001S  )C 00 00 49 38 06 00 80 24 1C 03  ...’p...I8..€$..
0001S  )0 20 09 C7 00 00 90 84 63 00 00  .@.Ž.. .Ç...„c..
000    4 E1 18 00 00 92 70 0C 00 00 E9  HÅ1..$á...’p...é
000    C 14 09 2C 00 00 00 00 49 45 4E  ÿ^.VÅ|..,....IEN
0001/                                    D®B`,
```

Offset(h): 1A025

10. In the Select block window, type the respective offsets as seen in items 1 and 2 below and then click OK as seen in item 3. This will highlight the entire area between these two offsets.



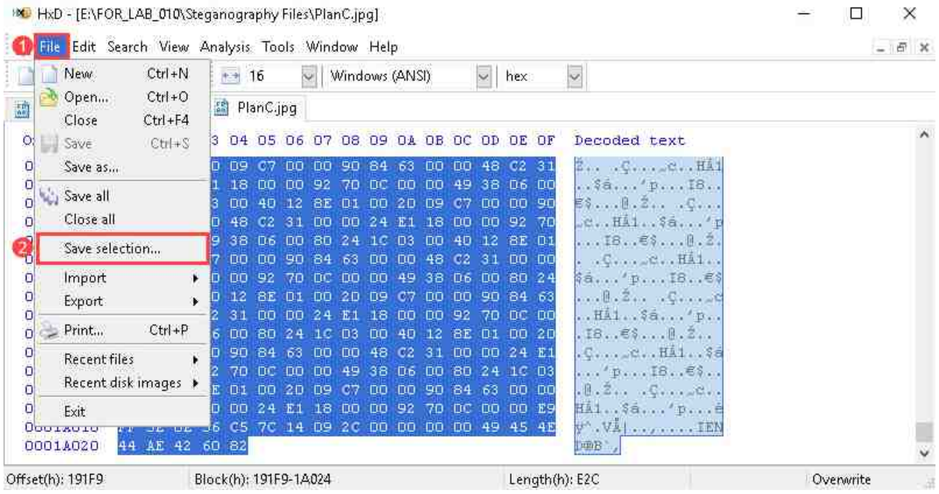
Start-offset: 191F9

● End-offset: 1A025

○ Length: 1

● hex ○ dec ○ oct

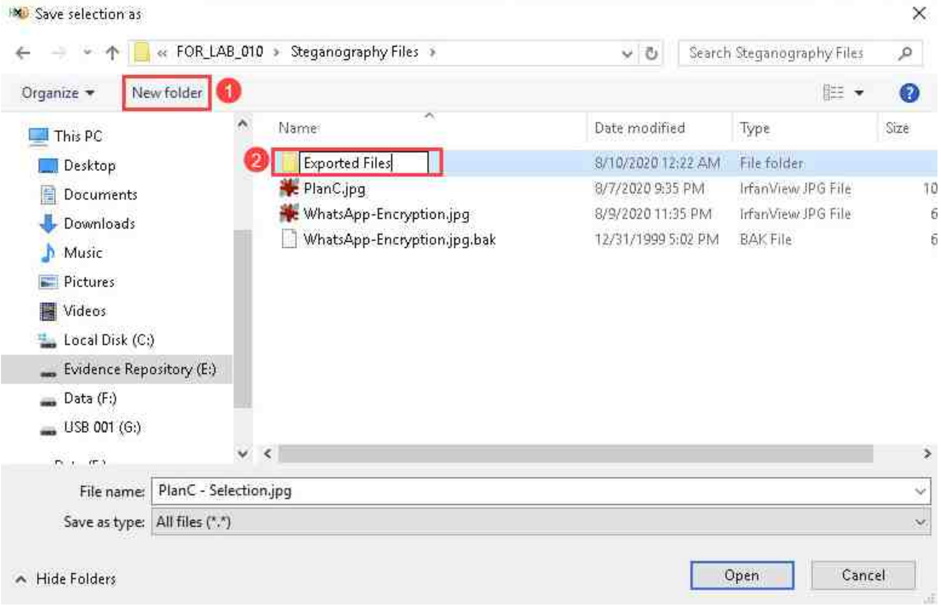
11. Now that the file is highlighted, let us export it. To do this, navigate to File > Save selection as seen in items 1 and 2 below.



HxD - [E:\FOR_LAB_010\Steganography Files\PlanC.jpg]

Offset(h): 191F9 Block(h): 191F9-1A024 Length(h): E2C Overwrite

12. The Save selection as window will appear. Browse to Evidence Repository (E:) > FOR_LAB_010 > Steganography Files and click New Folder to create a new folder as seen in item 1 below. Name this new folder `Exported Files` as seen in item 2.



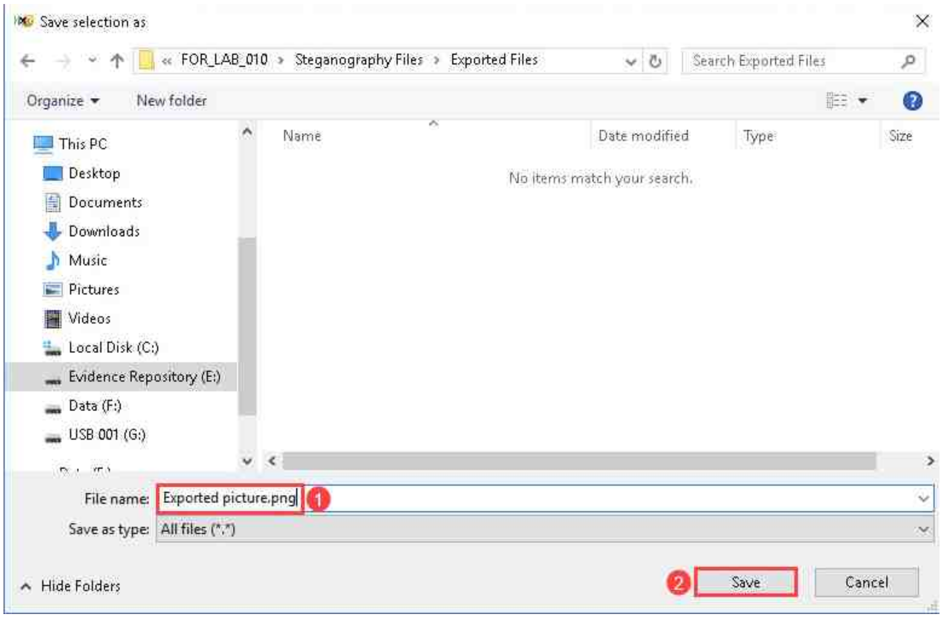
Name	Date modified	Type	Size
Exported Files	8/10/2020 12:22 AM	File folder	
PlanC.jpg	8/7/2020 9:35 PM	IrfanView JPG File	10
WhatsApp-Encryption.jpg	8/9/2020 11:35 PM	IrfanView JPG File	6
WhatsApp-Encryption.jpg.bak	12/31/1999 5:02 PM	BAK File	6

File name: PlanC - Selection.jpg

Save as type: All files (*.*)

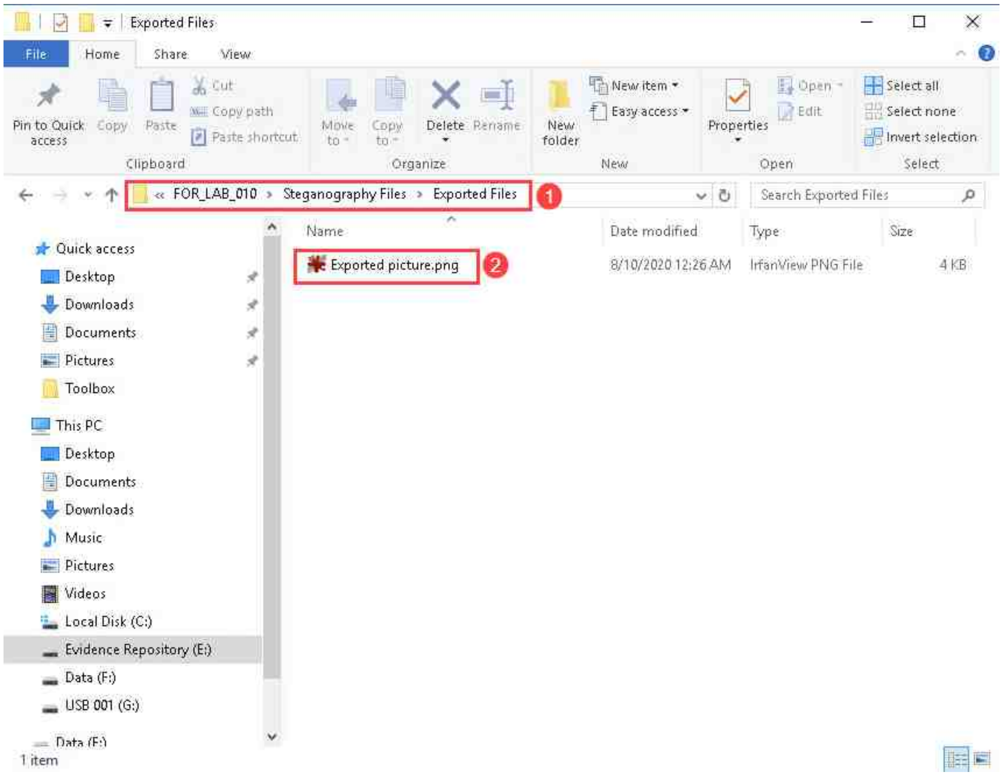
13. Double-click the Exported Files folder to open it.

14. Now that we are in the Exported Files folder, let us save the file here. Type `Exported picture.png` in the File name field and then click Save, as seen in items 1 and 2 below.



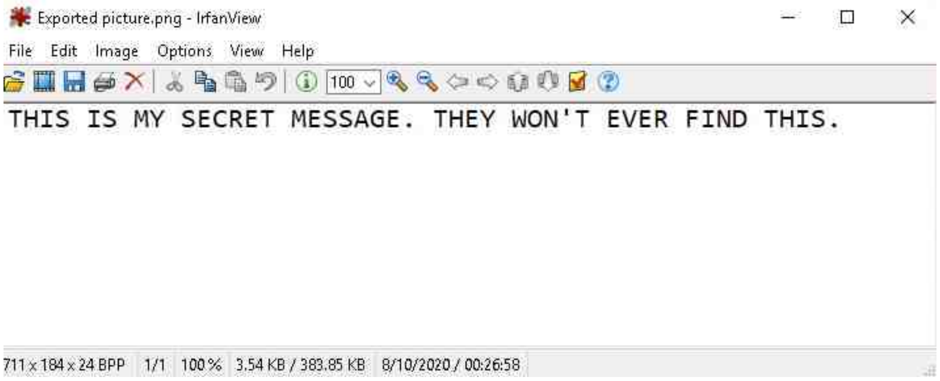
File name: Exported picture.png
Save as type: All files (*.*)

15. This will save the PNG file we found in the JPG file. Let's take a look at the file we exported by opening File Explorer and navigating to This PC > Evidence Repository (E:) > FOR_LAB_010 > Steganography Files > Exported Files and double-clicking on the file called Exported picture.png, as seen in items 1 and 2 below.



Name	Date modified	Type	Size
Exported picture.png	8/10/2020 12:26 AM	IrfanView PNG File	4 KB

16. If you did everything correctly, the file will open as you see below. This is a picture file that was embedded within another picture file and is not easily detectable without specialized software or in-depth knowledge of steganography.


Exported picture.png - IrfanView
File Edit Image Options View Help
100

THIS IS MY SECRET MESSAGE. THEY WON'T EVER FIND THIS.

711 x 184 x 24 BPP | 1/1 | 100 % | 3.54 KB / 383.85 KB | 8/10/2020 / 00:26:58

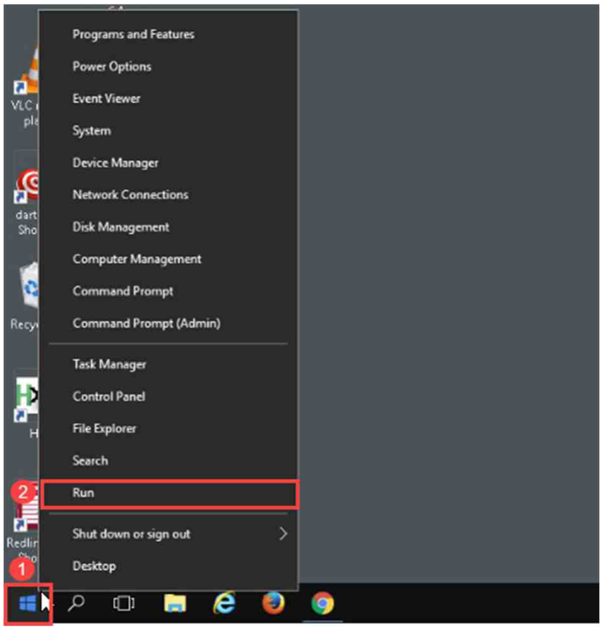
17. This exercise is now complete. We will now move on to Alternate Data Streams (ADS).

3 Alternate Data Streams – Hiding a Message in a File's Data Stream

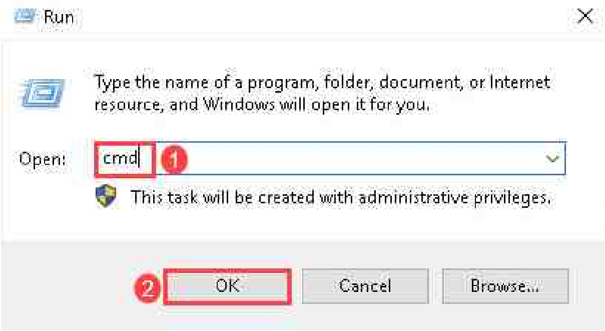
There are many anti-forensic techniques out there. Hiding data within Alternate Data Streams (ADS) is another simple anti-forensic method that can be done with very little investment. ADSs are file attributes that are only found on NTFS file systems and are not visible using traditional methods. They are often used as a hiding place for malware and other potentially unwanted programs, which means they should be considered in forensic examinations.

In this exercise, we will teach you how to hide a file within another file's data stream. We will also teach you the command to use to detect this data as well. All these commands will be done using the Windows command line so let us begin by opening it.

1. Begin by right-clicking on the Start button and click the Run option from the context menu that appears as seen in items 1 and 2 below.



1. When the Run window appears, type `cmd` and click OK as seen in items 1 and 2 below. This will open the Windows command prompt with administrative privileges.



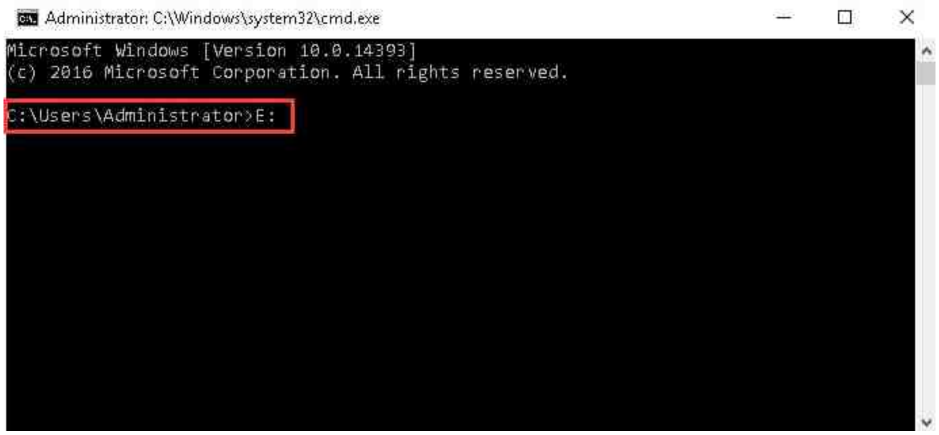
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

This task will be created with administrative privileges.

2. Once the command line window appears, we will change the directory to the path where the files we want to manipulate are. First, let us change to drive E:\ by typing the following command:

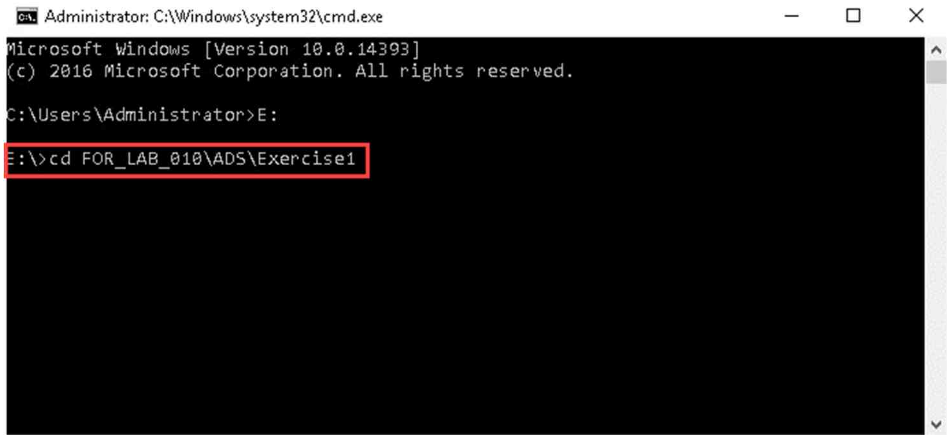
```
E:
```



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>E:
```

3. Now that we are in drive E:\, type the following command to change directory to our destination folder.

```
cd FOR_LAB_010\ADS\Exercise1
```

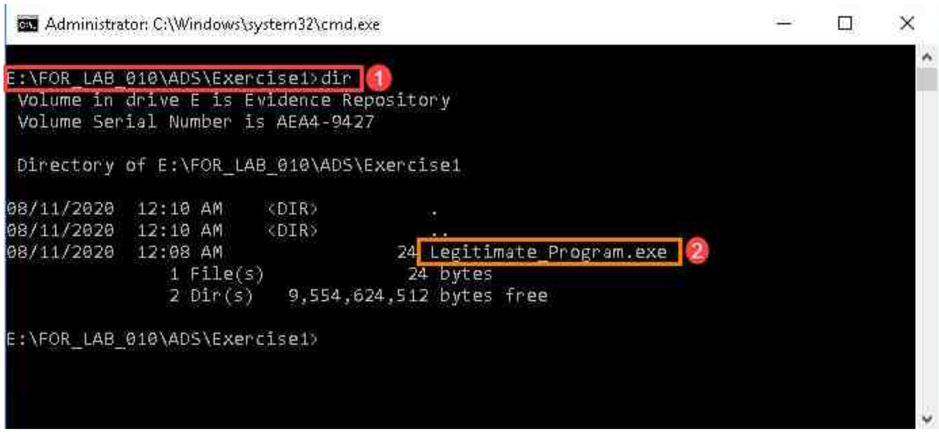


```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>E:

E:\>cd FOR_LAB_010\ADS\Exercise1
```

4. If you typed the command correctly, you will be taken to the folder called Exercise1. Now let us run the `dir` command to view the contents of the folder. See the command below and in the screenshot as item 1.

```
dir
```

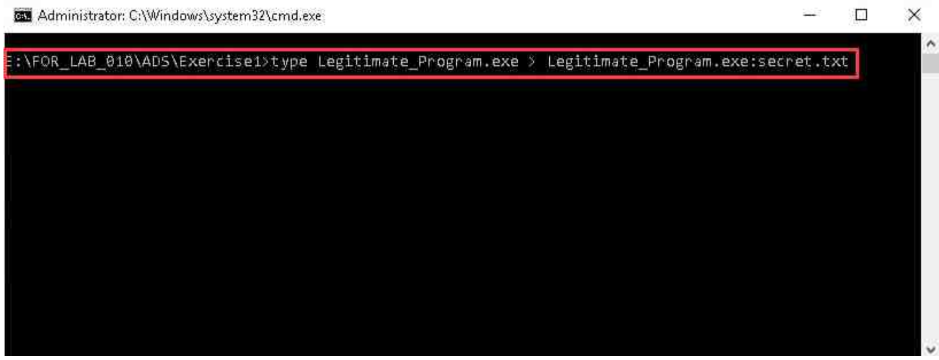
As you can see in item 2 below, there is 1 executable file in the folder. We will use ADS to hide a text file called secret.txt inside the one called Legitimate_Program.exe.



```
E:\FOR_LAB_010\ADS\Exercise1>dir
 Volume in drive E is Evidence Repository
 Volume Serial Number is AEA4-9427

 Directory of E:\FOR_LAB_010\ADS\Exercise1

08/11/2020  12:10 AM    <DIR>          .
08/11/2020  12:10 AM    <DIR>          ..
08/11/2020  12:08 AM                24 Legitimate_Program.exe
               1 File(s)             24 bytes
               2 Dir(s)   9,554,624,512 bytes free

E:\FOR_LAB_010\ADS\Exercise1>
```

5. The ADS command is very simple. Type the following command to create a text file in the data stream of Legitimate_Program.exe and then press Enter.

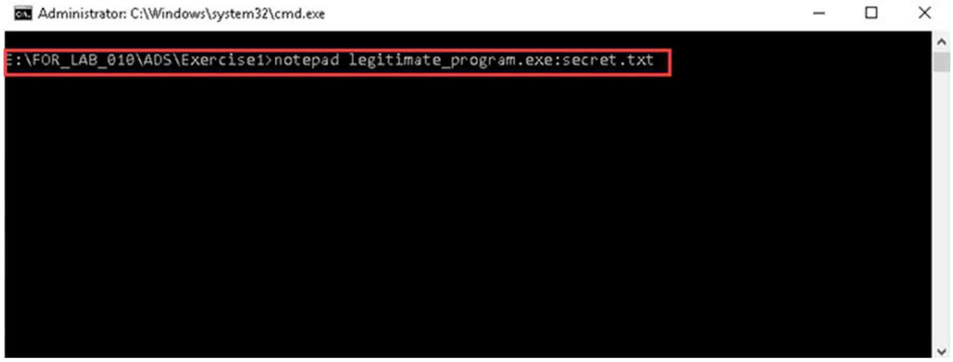
```
Type legitimate_program.exe > Legitimate_program.exe:secret.txt
```



```
E:\FOR_LAB_010\ADS\Exercise1>type Legitimate_Program.exe > Legitimate_Program.exe:secret.txt
```

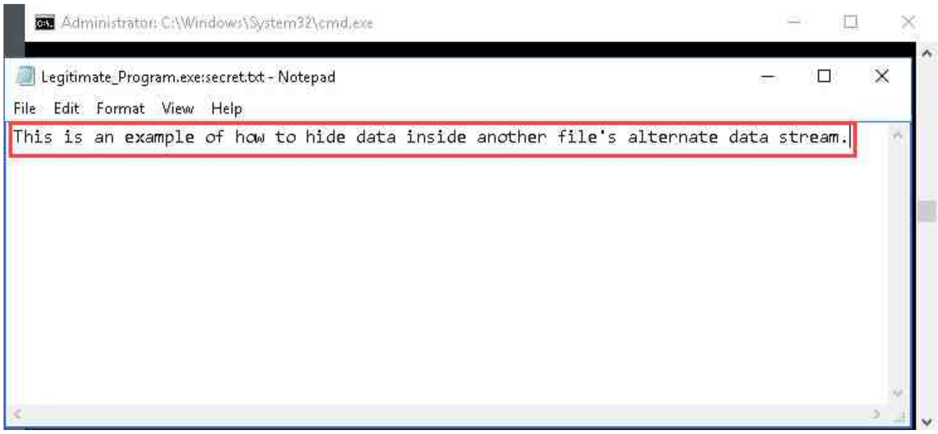
6. That was it. The file called secret.txt is now successfully stored in the data streams of the other program. If you run the command `dir`, you will not see this data. You can now open this file by typing the following command and pressing Enter.

```
Notepad legitimate_program.exe:secret.txt
```



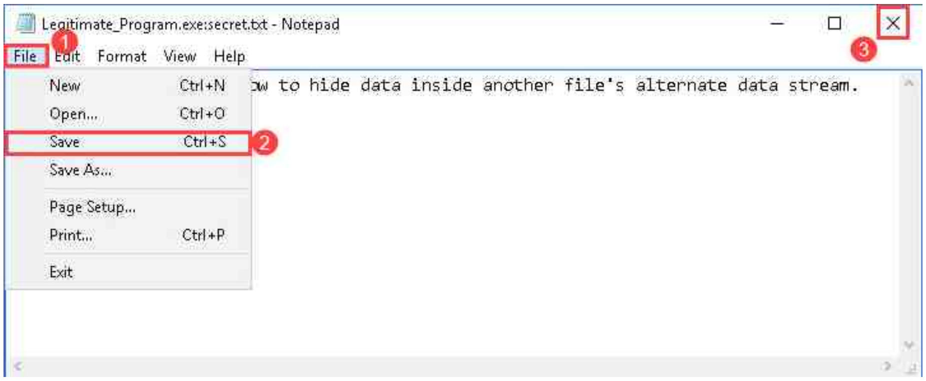
```
E:\FOR_LAB_010\ADS\Exercise1>notepad legitimate_program.exe:secret.txt
```

7. The command will open the secret.txt file. Let us type something inside the text file. You can create your own text, or you can type the sentence highlighted below. The file will grow, but it will remain in the data stream unless it, or its associated file, is deleted.


Administrator: C:\Windows\System32\cmd.exe
Legitimate_Program.exe:secret.txt - Notepad
File
Edit
Format
View
Help

This is an example of how to hide data inside another file's alternate data stream.

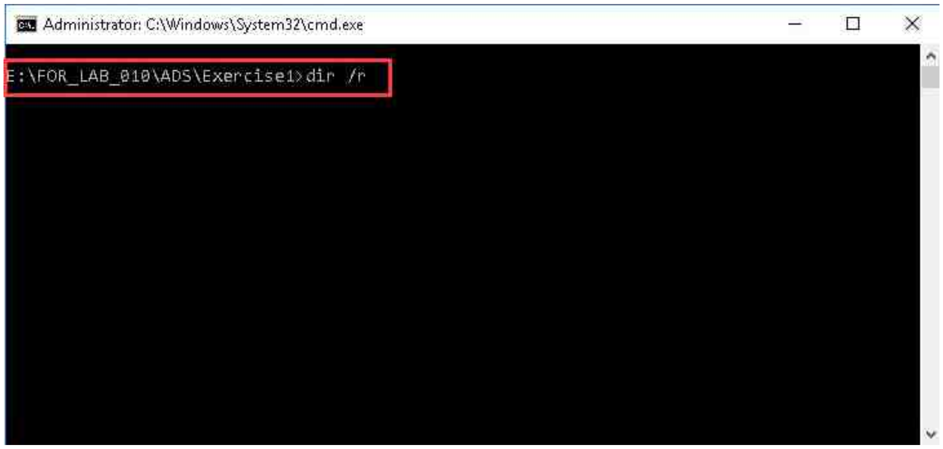
8. Once you are done typing, save the file and close it by navigating to File > Save, as seen in items 1 and 2 below. Once done, click the X highlighted in item 3 to close the file.



w to hide data inside another file's alternate data stream.

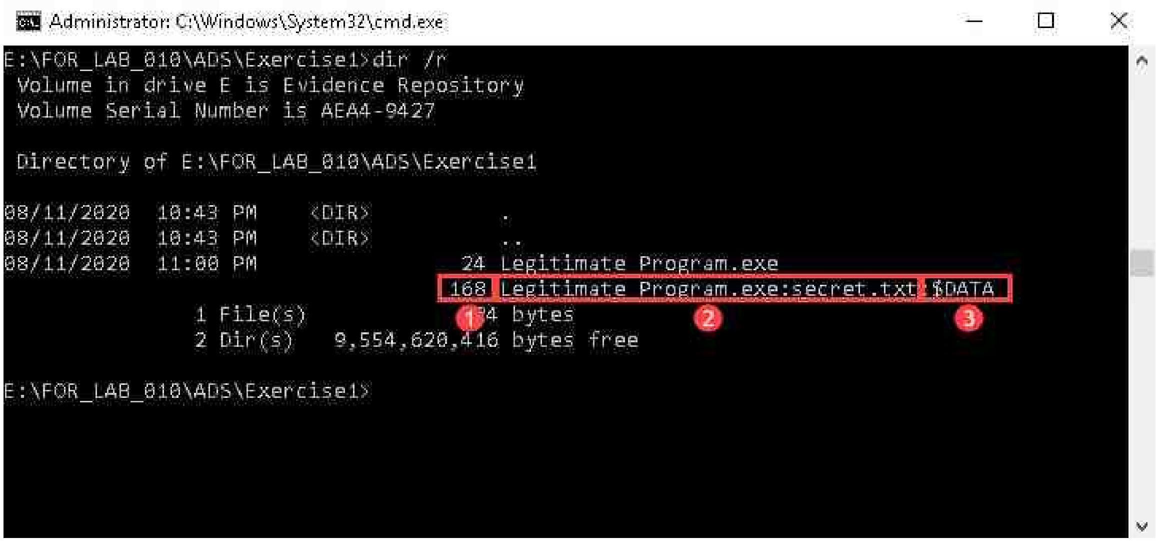
9. Next, let us do a file list command that can also show if a file has an ADS. The command prompt should still be open; if not, reopen it and type the following command. Once you are done, press Enter.

```
Dir /r
```



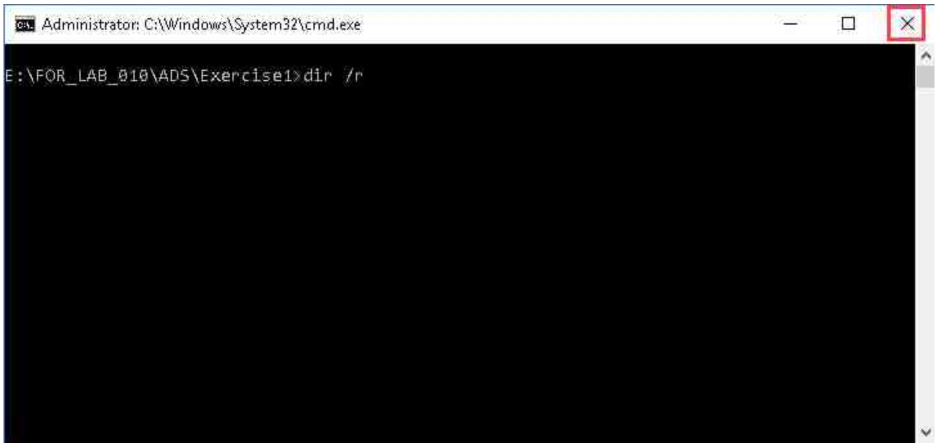
```
E:\FOR_LAB_010\ADS\Exercise1>dir /r
```

10. As you can see from the results of the file listing, there is now an additional file inside the directory. The file Legitimate_Program:secret.txt:$DATA was the file created when we ran the command that created the file within the ADS of the file Legitimate_Program.exe. As you can see in the screenshot below, the file has no dates and times associated with it, but it has a file size beside it highlighted as item 1. The file size is different from the size of its anchor file and is reported as such if you are looking at it through File Explorer. The portion highlighted as item 2 is the name of the file, while the one highlighted as item 3 is the attribute that identifies the listing as an ADS file. Whenever the ADS file is edited, the modified date for its anchor file gets updated as well.



```
E:\FOR_LAB_010\ADS\Exercise1>dir /r
 Volume in drive E is Evidence Repository
 Volume Serial Number is AEA4-9427

 Directory of E:\FOR_LAB_010\ADS\Exercise1

08/11/2020  10:43 PM    <DIR>          .
08/11/2020  10:43 PM    <DIR>          ..
08/11/2020  11:00 PM                24 Legitimate_Program.exe
                                   168 Legitimate_Program.exe:secret.txt:$DATA
               1 File(s)             24 bytes
               2 Dir(s)   9,554,620,416 bytes free

E:\FOR_LAB_010\ADS\Exercise1>
```

11. During this exercise, you learned how to create and identify ADS. As you learned, ADS and steganography can contain tons of data that is not easy to detect without proper training, tools, and a bit of luck. Hopefully, the knowledge you take away will better prepare you for these types of tricks.
12. The lab is now done. Close all the programs you had open by clicking the X at the top-right corner of each one, as seen below.



```
E:\FOR_LAB_010\ADS\Exercise1>dir /r
```