

Lab Assignment



Cybersecurity Professional Program
Digital Forensics & Incident Response

Windows Dead Analysis

DFIR-06-L3
Image Carving

Copyright © 1996–2021 HackerU Ltd.
All Rights Reserved.

Lab Objective

Understand how to access hidden data and retrieve it using file carving techniques.

Lab Mission

Extract hidden information from an image file using **Binwalk** and a hex editor.

Lab Duration

20–30 minutes

Requirements

- Basic understanding of file carving

Resources

- Environment & Tools
 - VirtualBox
 - Windows 10
 - *Pscp.exe*
 - SIFT Workstation
- Extra Lab Files
 - *Cat.jpg*
 - *HxDSetup.exe*
 - PuTTY
- Extra Links
 - File size calculator: <https://toolstud.io/photo/filesize.php>
 - File signature list: https://en.wikipedia.org/wiki/List_of_file_signatures



Textbook References

- Chapter 6: Windows Dead Analysis
 - Section 5: File Carving

Lab Task: Investigate an Image and Find Hidden Data

You will need to employ your investigation skills for this task. Investigate the provided image and find the data hidden within it.

- 1 Make sure Windows 10 and SIFT have access to the internet by using two adapters, one for the internal network and one for the internet.
- 2 On the Windows 10 VM, go to <https://toolstud.io/photo/filesize.php> to examine the **Cat.jpg** image size and its file size. Compare the file size to its estimation on the website. You can see the image size and file size in the properties of the file.
- 3 Install **PuTTY** on the Windows 10 machine to transfer the document to the SIFT workstation via SSH on port 22.
- 4 Start the SSH service on the SIFT workstation with **sudo service ssh start** to transfer the **Cat.jpg** file to SIFT using **PSCP** for examination. Make sure you are in the proper directory on the Windows machine before running the command **"C:\Program Files\PuTTY\pscp.exe" -P 22 Cat.jpg sansforensics@[Ip]:/home/sansforensics/Desktop**.
- 5 On the SIFT machine, run **apt update** and then **sudo apt-get install -y binwalk**.
Note: You may need to run **sudo apt install -y binwalk --fix-missing**.
- 6 Examine **Cat.jpg** with the **binwalk** command.

Note: The result confirms multiple images are hidden within the JPEG; also, note the hexadecimals.

```
sansforensics@siftworkstation: ~/Desktop
$ binwalk Cat.jpg

DECIMAL      HEXADECIMAL     DESCRIPTION
-----
0            0x0             JPEG image data, JFIF standard 1.01
416788       0x65C14         JPEG image data, JFIF standard 1.01
998740       0xF3D54         JPEG image data, JFIF standard 1.01

sansforensics@siftworkstation: ~/Desktop
$
```

- 7 Install **HxD** to examine **Cat.jpg** and extract the hidden images.
- 8 Once you have **HxD** running, drag and drop **Cat.jpg** into **HxD**.

9

Note: There is evidence of a JPEG File Interchange Format (JFIF). This may hint at the existence of an embedded data stream. At this stage, a researcher may conclude there are more images hidden in the **Cat.jpg** file.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00065B20	2B	00	D9	3C	63	D6	3C	9F	19	DF	E7	09	B6	70	3E	70	+..Ü<c0<Ÿ.Ĳç.Ÿp>p
00065B30	98	6B	82	67	2C	85	75	E7	3F	CC	ED	86	9F	B6	43	F1	"k,q,~uq?İitŸŸCñ
00065B40	9F	58	E3	FA	CD	96	F8	C8	57	CE	18	77	F7	F6	73	A7	>Xáúİ-ŷEWİ.w>psŸ
00065B50	5E	8B	70	FC	7F	59	CE	7A	73	7D	B7	B7	1D	A6	42	35	İXpü.Yİzs>...;BS
00065B60	D7	F5	89	F0	4C	04	35	D6	7F	9F	E3	00	F3	EB	01	3A	*0t&L.5Ö.Yä.öe..
00065B70	F1	87	67	AF	F7	17	07	F7	9D	1D	5C	7F	BC	02	1F	FC	ñt+g÷÷÷÷\..4..ü
00065B80	EC	2E	F7	80	21	4C	E5	F5	60	05	03	5A	FE	71	BF	73	İ..€İ:Läö~..Zpqqs
00065B90	9E	71	E5	FB	D6	42	34	77	FC	E1	9B	9B	C8	6F	13	F6	ŽqäüÖB&wüa>>ëo.?
00065BA0	6F	A6	6A	9A	4C	14	0E	CD	53	98	7F	39	AI	1D	E6		oİj>A...DS~.9İ;æ
00065BB0	8A	66	C9	7A	E3	37	57	D6	13	3F	39	43	47	EB	9B	1B	Šfz&Z&WÖ..9CGe>.
00065BC0	BD	7F	79	B9	BF	39	C5	F3	9B	5C	79	C3	91	C0	41	9C	4.yİ>9AÖ>)yÄ.A&æ
00065BD0	F3	9C	33	64	BB	CE	33	E7	39	97	6	6F	BE	1C	FC	33	ö&3d>İ3ç9-æoŸ.ü3
00065BE0	4E	35	A7	39	7D	33	63	7D	CC	4C	CE	6F	9C	E6	7C	FF	NŠ9>3c>İLİo&ıŸ
00065BF0	00	59	76	7C	FF	00	59	FE	E6	DC	E3	AD	9C	FF	00	DC	.YvİŸ.Yp&Ü.æŸ.Ü
00065C00	16	CE	B0	D3	E9	9C	71	71	8E	8D	6A	05	D6	DF	DB	84	.İ'æ&eqqZ.c.Ö&Ü.
00065C10	9E	9F	FF	D9	FF	00	88	FF	E0	00	10	4A	46	49	46	00	ëŸyüŸöŸä..JULİE
00065C20	01	00	00	01	00	01	00	00	FF	DB	00	43	00	05	03	04ŸÜ.C.....
00065C30	04	04	03	05	04	04	04	05	05	06	07	0C	08	07	07	
00065C40	07	07	0F	0B	0B	09	0C	11	0F	12	12	11	0F	11	11	13
00065C50	16	1C	17	13	14	1A	15	11	11	18	21	18	1A	1D	1D	1F!
00065C60	1F	1F	13	17	22	24	22	1E	24	1C	1E	1F	1E	FF	DB	00"s".s.....ŸÜ.
00065C70	43	01	05	05	05	07	06	07	0E	08	0E	0E	1E	14	11	14	C.....
00065C80	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E
00065C90	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E
00065CA0	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E
00065CB0	1E	1E	FF	C2	00	11	08	06	4A	07	80	03	01	22	00	02	..ŸÄ.....J.e.."
00065CC0	11	01	03	11	01	FF	C4	00	1C	00	00	02	03	01	01	01ŸÄ.....
00065CD0	01	00	00	00	00	00	00	00	00	02	03	01	04	05	00	ŸÄ.....
00065CE0	06	07	08	FF	C4	00	1A	01	00	03	01	01	01	01	00	00	..ŸÄ.....
00065CF0	00	00	00	00	00	00	00	00	00	01	02	03	04	05	06	FF	Ü.....İŸ.....Ÿ
00065D00	DA	00	0C	03	01	00	02	10	03	10	00	00	01	CD	7D	7F	Ü.....İŸ.....
00065D10	12	DE	E4	BD	8C	60	18	19	81	B0	88	48	27	BA	42	04	.Pa&Ÿ.....°H°B.
00065D20	C0	00	0C	01	62	60	C1	E9	80	89	99	08	9E	E1	4F	74	Ä...b'Ä&eŸ™.Ž&Ot
00065D30	8F	A7	B8	3A	7A	43	A7	B9	93	3D	22	E9	82	0E	9E	90	.S.:zCS2°="é,ž.
00065D40	E9	EE	08	89	80	00	60	02	D6	C5	82	94	E4	A1	09	7A	éİ.ŸE...ÖÄ,"äİ;z
00065D50	13	AD	E5	C5	74	AB	A2	C2	25	A1	2E	54	0B	03	00	18	..°Ä&e&Ÿİ.T....
00065D60	98	08	5E	80	98	Ä&E	4F	12	43	C5	C0	B9	E8	6B	BB		..ë&°İdO.CÄ&°è&°
00065D70	B8	5D	13	02	E8	98	0E	8E	E0	EE	08	EE	E6	47	4C),.è°.Žäİİİ&GL

10

Note: The beginning of a JPEG is **FF D9** and the end of a JPEG is **FF D8 FF**.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000F3D00	FC	36	66	F3	S2	69	F1	1D	3E	88	6D	39	66	AF	A9	AB	u6f0Rin.>m9f'@ec
000F3D10	FE	E2	3A	9C	7E	21	B7	BF	89	C1	39	78	9B	7C	C3	8F	p8:~!-!tA9(> A
000F3D20	7F	FC	33	48	EC	F5	37	9A	3E	A7	3F	FE	76	7A	9F	C2	.u3Hl07S>\$?pvzY
000F3D30	6F	F1	35	9C	9F	7F	F9	76	9B	7C	4F	9E	3F	B9	FC	23	of5ep.<u> 0E?#
000F3D40	BF	C4	74	7B	9F	B3	FF	00	8D	1F	1D	B8	36	3D	43	5E	At(Y*y...U6?C
000F3D50	D3	F0	9F	D4	B8	D8	FF	E0	00	10	4A	46	49	46	00	01	08Y60yA.JRIF..

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
001E0EA0	C2	AA	42	17	85	B7	93	07	26	0E	64	74	DE	70	45	0A	Å*B...".&.dt&PpE.
001E0EB0	41	08	E3	DD	95	D0	3B	A7	FF	00	30	41	50	F5	15	3D	A.âÿ•D;Sÿ.OAP&.=
001E0EC0	B8	58	51	87	40	EB	5D	EB	6E	25	04	5D	94	60	FA	E3	.XQ+@e]en%.]"`úã
001E0ED0	B6	2B	21	13	61	CC	C7	BB	03	00	A2	8C	DB	35	8B	6E	q+!.aİÇ»...c@U5<n
001E0EE0	1F	84	1F	93	28	91	9B	0C	7F	7D	62	D3	A7	9F	1F	33	.."(')>..}b0\$ÿ.3
001E0EF0	FF	D9	4A	46	49	46	00	01	01	00	00	01	00	01	00	00	JFIF.....

- 11 Make sure the hex is highlighted to use it properly. You will be subtracting **1E0EF2** by **F3D54**. This should give the result **ED19E**.
- 12 Select the beginning of the image **F3D4**, then select length and put **ED19E**, the length found when subtracting the two hexadecimal numbers. This will highlight the image, which you should copy. Create a new hex file, paste the copied hex, and save the document as **carved1.jpg**.
- 13 To find the other hidden JPEG, you need to find the beginning and end of the image. Perform a search again for the **FF D8** values. Subtract the values again to get the highlighted image, which you should copy and paste to new a hex document. Save the file as **carved2.jpg**.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000F3D00	FC	36	66	F3	52	69	F1	1D	3E	88	6D	39	66	AF	A9	AB	ü6fôRiã.>~m9f@«
000F3D10	FE	E2	3A	9C	7E	21	B7	FB	89	C1	39	7B	9B	7C	C3	8F	pâ:α~!·ûttA9(> jÃ.
000F3D20	7F	FC	33	48	EC	F5	37	9A	3E	A7	3F	FE	76	7A	9F	C2	.ü3H1ö7\$>\$?pvzYÃ
000F3D30	6F	F1	35	9C	FE	7F	F9	76	9B	7C	4F	E9	3F	B9	FC	23	oñ5œp.ùv> Oé?~ü#
000F3D40	B7	C4	74	7B	9F	B3	FF	00	8D	1F	11	DB	36	3D	43	5E	·Ät{ÿ'y...Ü6=C^
000F3D50	D3	F0	9F	D4	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	ÔäYÖÛÿà..JFIF..

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00065BC0	BD	7F	79	B9	BF	39	C5	F3	9B	5C	79	C3	91	C0	41	9C	¼.y'¿9Ãó> yÃ'ÃAœ
00065BD0	F3	9C	33	64	BB	CE	33	E7	39	97	C6	6F	B6	1C	FC	33	ôœ3d»İ3q9-Eo£.ü3
00065BE0	4E	35	A7	39	7D	33	63	7D	CC	4C	CE	6F	9C	E6	7C	FF	N5\$9}3c}İLİœœ y
00065BF0	00	59	76	7C	FF	00	59	FE	E6	DC	E3	AD	9C	FF	00	DC	.Yv y.YpœÜâ.œy.U
00065C00	16	CE	B0	E3	E9	9C	71	8E	8D	6B	05	D6	DF	DB	84		.İ°âœœqqZ.k.ÔâÜ.
00065C10	E9	9F	FF	D9	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	éÿyÜÛÿà..JFIF..

- 14 Switch back to **text-string** in the **Ctrl+F** search to further investigate the provided **Cat.jpg** file for more information using a string search in **HxD**. Search for the fourth JFIF string in the documented image. Note that the fourth is incomplete compared to the other files.
- 15 Copy from the JFIF to the bottom of the hex document. Paste the copied hex to a new hex file and add the beginning hex to the file and then save as **carved3.jpg**. Compared to the other JFIFs, you should note that what is missing is **FF D8 FF E0 00 10**.

16 You have found all the hidden images within ***Cat.jpg***.

Hints

Lab Task: Investigate an Image and Find Hidden Data

- Use the machine's network options to configure the network adapter for internet access.
- Inspect the image properties to view its dimensions.
- Start the SSH service in SIFT.
- Ensure the SIFT and Windows 10 machines are on the same network.
- Use "**C:\Program Files\PuTTY\pscp.exe**" -P 22 **Cat.jpg sansforensics@[SIFT Box IP]:/home/sansforensics/Desktop** to transfer files with PSCP.
- Use APT Package Manager to install **Binwalk**.
- The **Binwalk** results are locations of potential data to be extracted.
- Follow the basic installation of **HxD**.
- Import the **.jpg** file to the editor.
- Look for JFIF, which is interchangeable with JPEG.
- Use the Windows Calculator to calculate the length of the files by subtracting the hex values.
- To select the correct range, right-click the start position and then click to select a block.
- Copy the selected content and paste it in a new file to be saved.
- Use **HxD**'s string search capability to search for additional images.
- Use all methods learned in the file carving section, calculate the image size, and extract it.
- Note the patterns of the images to fill in the missing hex for the last image.
- You should have a total of four images.