

Eliza Nip
CS477

Special Fergus-File Carving Report

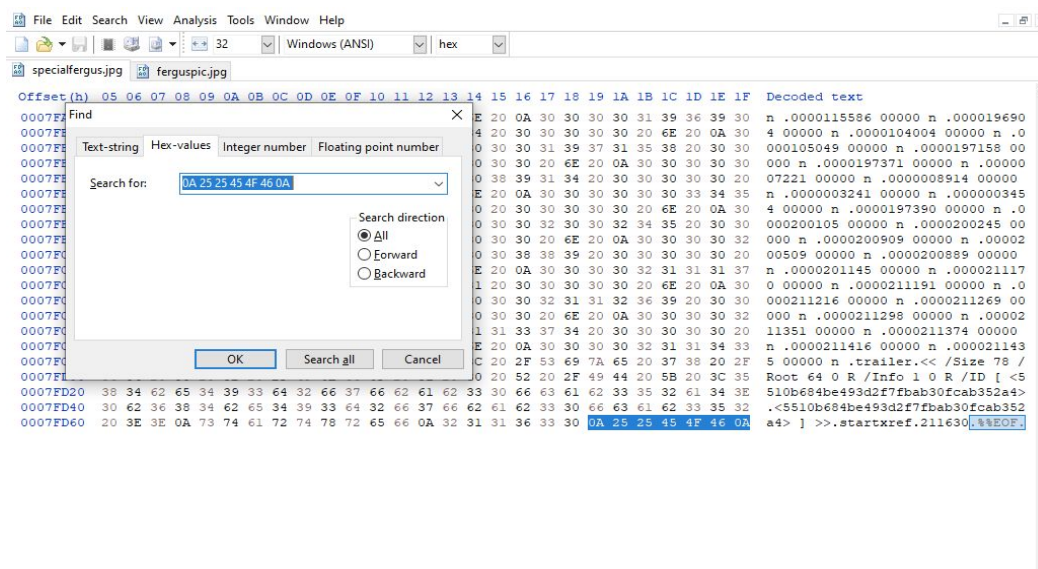
I began the assignment by opening the special fergus image with hex editor HxD. First thing I found before starting to carve is the information of the fergus picture. The photo was taken in 2019, May 3rd, around 6:53pm, using Apple iPhone XS. I was also able to find the exact camera that took the picture, which is the back dual camera on iPhone XS.

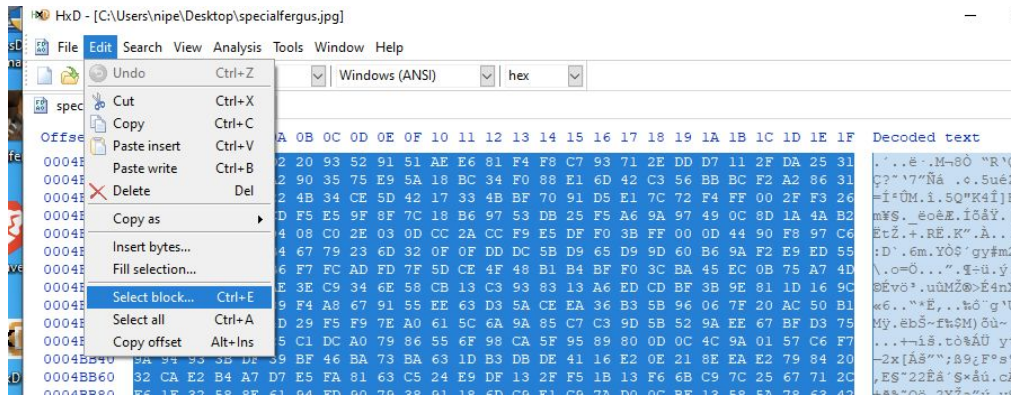
00000020	08	00	0A	01	0F	00	02	00	00	06	00	00	86	01	10	00	02	00	00	0A	00	00	00	8C	*+E
00000040	00	00	01	00	01	00	00	01	1A	00	05	00	00	01	00	00	96	01	1B	00	05	00	00	00	00	01
00000060	28	00	03	00	00	00	01	00	02	00	00	01	31	00	02	00	00	00	05	00	00	A6	01	32	00	02	...Z.(.....1..... 2..
00000080	00	00	AC	87	69	04	00	00	00	05	00	00	00	C0	88	25	00	04	00	00	00	01	00	00	07	2A+i.....Ã%.....*
000000A0	70	70	6C	65	00	69	50	68	6F	6E	65	20	58	53	00	00	00	00	48	00	00	01	00	00	00	48Apple iPhone XS.....H.....E
000000C0	32	2E	32	00	00	32	30	31	39	3A	30	35	3A	30	33	20	31	38	3A	35	33	3A	35	31	00	2012.2.2019:05:03 18:53:51.....
000000E0	00	00	01	00	00	02	46	82	9D	00	05	00	00	00	01	00	00	02	4E	88	22	00	03	00	00	01	...S.....F.....N".....
00000100	27	00	03	00	00	00	01	01	F4	00	00	90	00	00	07	00	00	00	00	32	32	32	31	90	03	026.....0221.....

After analyzing the picture of Fergus(specialfergus.jpg), I found that beside the picture of Fergus, there's also a pdf file hiding under the jpg file. The pdf file includes two pictures of Fergus, one of them is a flipped version of the picture of Fergus(specialfergus.jpg).

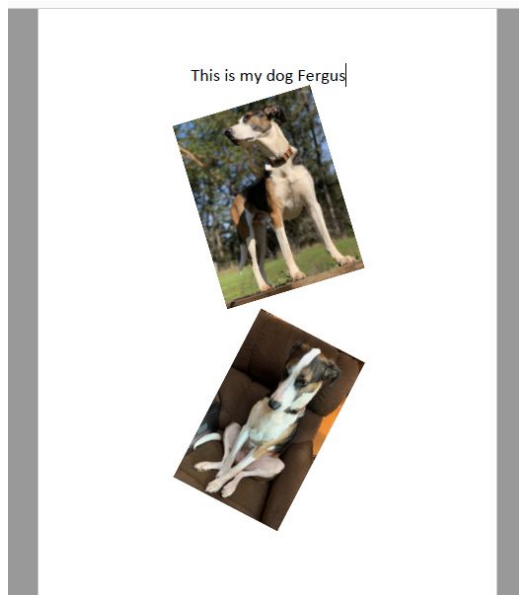
At first, I didn't know where to begin. Using the file signature table, I know that the trailer of jpg is FF09. I did a search to locate all the FF09. With the help of a search function, I was able to find the first image. I didn't really need to find the first image. However, by doing that, I can filter out search results that aren't relevant, since I know exactly where I should begin to investigate.

While searching, I found one part of the decoded text said “PDF”, that indicates that there is a pdf file in this specialfergus.jpg. I found the hex of PDF by highlighting the decoded text “PDF”. I compared that with the file signatures table and found the list of trailers for the PDF file. Since I don’t know which one is the correct one, I performed a search on each of the trailers to see if there’s any match. I found the match on my third attempt, the end-of-file mark that I found is “0D 0A 25 25 45 4F 46 0D 0A”. I used the select block function to quickly select the PDF block.





I created a new file named “fergus.pdf” in HxD, pasted the selected block to the file. By opening the file with pdf reader, I got the following:



I was amazed by the fact that you can hide so much under a jpg file. I was also really surprised that data like the device that used to take photos and when they were taken can be found on the jpg hex file. One thing that I found interesting in the pdf file is that I found 4 hidden images on the pdf file. I am not sure what those are, I didn’t see any other jfif files beside the two photos of Fergus in HxD. I tried to copy the image and it looks very blurry. I guess it is part of the background of these two photos.

One of the “hidden” image looks like this:

