

Challenge Title: The Cat Ate My Homework

Author: MaryEllen Kennel/aka @icanhaspii

Points: 100

Difficulty: Easy

Summary:

This challenge is designed to be an easy stego/forensics-carving exercise which utilizes a hex editor to carve out a docx file stuffed inside of a file jpeg file:

1. Initial Screen:

Fun fact: Cats enjoy gnawing on paper! This innocent little creature ate my homework, can you help me recover it?



Photo Credit: Chloe Regas

Solution:

1. Open the cat image file in a hex editor (I used HxD: <https://mh-nexus.de/en/hxd>):

The screenshot shows the HxD hex editor interface with the file 'IMG_20250705_234750_Edited3_Stuffed.jpg' open. The 'hex' tab is selected. The left pane displays the raw hex data, and the right pane shows the corresponding 'Decoded text'. The text includes standard header information like JFIF and ICC profiles, followed by image data and a series of null bytes at the end.

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00000000	FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01	ÿØÿà..JFIF.....
00000010	00 01 00 00 FF E2 01 D8 49 43 43 5F 50 52 4F 46ÿâ.ØICC_PROF
00000020	49 4C 45 00 01 01 00 00 01 C8 00 00 00 00 04 30	ILE.....È.....0
00000030	00 00 6D 6E 74 72 52 47 42 20 58 59 5A 20 07 E0	..mntrRGB XYZ .à
00000040	00 01 00 01 00 00 00 00 00 00 61 63 73 70 00 00acsp..
00000050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

2. Locate the end-of-image marker - For JPEGs, this marker is typically FF D9:

The screenshot shows the HxD hex editor interface with the same file open. A 'Find' dialog box is overlaid on the window. The 'Text-string' tab is selected, and the search term 'FF D9' is entered. The 'Forward' search direction is selected. The search results are shown in the main pane, with the marker 'FF D9' found near offset 0x00000060.

3. Copy all the hex data of the DOCX file:

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0002D2B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0002D2C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0002D2D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0002D2E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0002D2F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0002D300	FF	D9	50	4B	03	04	14	00	00	00	08	00	AF	98	49	4A	yÙPK.....~"IJ
0002D310	8D	13	30	EA	3A	01	00	00	A7	02	00	00	10	00	00	00	..0è:...\$.....
0002D320	64	6F	63	50	72	6F	70	73	2F	61	70	70	2E	78	6D	6C	docProps/app.xml
0002D330	AD	92	C1	4E	C3	30	0C	86	5F	25	CA	9D	B6	E3	30	A1	.'ÁÑÄ0.t %È.¶ä0;
0002D340	69	ED	84	D6	03	07	40	48	1B	E3	1C	12	77	8D	48	E2	ii,Ö..@H.ä..w.Hâ
0002D350	28	F1	46	FB	6C	1C	78	24	5E	01	A5	43	6B	81	1B	E2	(ñFÜl.x§^.%Ck..å
0002D360	FA	F9	CB	1F	DB	F2	C7	DB	FB	72	D5	59	C3	8E	10	A2	úúÈ.ÜòçÜûrÖYÄZ.c
0002D370	46	57	F2	59	56	70	06	4E	A2	D2	6E	5F	F2	03	35	17	FWòYVp.N«Ön_ò.5.
0002D380	57	9C	45	12	4E	09	83	0E	4A	DE	43	E4	AB	6A	29	FC	WæE.N.f.JPCä«j)ü
0002D390	E2	21	A0	87	40	1A	22	EB	AC	71	B1	E4	2D	91	5F	E4	â! #@."ë-qïä-' ä
0002D3A0	79	94	2D	58	11	33	F4	E0	3A	6B	1A	0C	56	50	CC	30	y"-X.3ðà:k..VPÍO
0002D3B0	EC	73	6C	1A	2D	A1	46	79	B0	E0	28	BF	2C	8A	79	0E	isl.-;Fy°à(,Šy.
0002D3C0	1D	81	53	A0	2E	FC	39	90	9F	12	17	47	FA	6B	A8	42	..S .ü9.Ý..Gúk"ß
0002D3D0	99	FA	8B	BB	6D	EF	C7	3C	E1	FF	B3	C9	61	0B	D7	DE	"ù«»miÇ<áý'Éa..xß
0002D3E0	1B	2D	05	69	74	D5	9D	96	01	23	36	C4	9E	30	28	D6	.-.itÖ.-.#6ÄZ0(Ö
0002D3F0	60	60	D4	02	7B	85	E7	65	FE	43	4D	4F	6B	94	1B	90	``Ö.{...çepCMOK"..\
0002D400	87	A0	A9	AF	8A	C1	98	92	64	6C	A4	30	B0	0E	E8	AB	+ @-ŠÁ''d1#0°.é«
0002D410	46	98	08	83	33	B2	64	AC	D1	7A	E1	7A	96	9F	FC	56	F".f3:d-Ñzáz-ÝüV
0002D420	04	50	35	CA	A9	7F	66	C9	B8	E9	3D	04	A3	DD	4B	50	.P5È@.fÉ,é=.fÝK\
0002D430	B7	C2	ED	41	4D	CC	DF	B5	AF	01	77	A7	F3	A8	66	F3	·AiAMÍBü-.w§ó"fó
0002D440	AC	28	8A	53	AB	13	9C	AC	2D	58	6F	04	41	75	9F	16	-,(SS«.œ→-Xo.AuÝ.
0002D450	69	32	85	64	07	EF	5C	48	D6	6D	0A	7F	F4	5B	AC	13	i2..d.i\Höm..ô[→.
0002D460	19	7F	FE	CE	07	34	5E	57	F5	09	50	4B	03	04	14	00	..þi.4^Wö.PK....
0002D470	00	00	08	00	44	59	53	5B	9C	EA	1D	62	5D	01	00	00DYS[œ..b]...
0002D480	9A	02	00	00	11	00	00	00	64	6F	63	50	72	6F	70	73	š.....docProps
0002D490	2F	63	6F	72	65	2E	78	6D	6C	95	92	4B	4E	C3	30	14	/core.xml.'KNÄ0.
0002D4A0	45	B7	12	79	9E	38	6E	E8	CF	4A	83	C4	6F	02	95	90	E..yž8nèÍJfÄo..•.
0002D4B0	40	02	31	33	F6	6B	EA	4F	64	BF	92	74	6D	0C	58	@.13ökkèOdż'tm.X	
0002D4C0	12	5B	40	0D	6D	0A	88	09	33	FB	DD	7B	8F	75	6D	7F	.@[ø.m.^3üÝ{.um.
0002D4D0	BC	BD	97	A7	AD	35	C9	2B	84	A8	BD	9B	11	96	E5	24	þ-\$.5É+,.“¾».-å\$
0002D4E0	01	27	BD	D2	6E	39	23	1B	5C	A4	13	72	5A	95	D2	07	.'¾Òn9#.\\x.rZ•Ø.
0002D4F0	88	0D	BF	86	80	1A	62	D2	5A	F3	22	57	72	46	56	88	“þæ hòzä"WW-ÈV"



HxD - [C:\Users\myjob\Desktop\New folder (2)\IMG_20250705_234750_Edited3_Stuffed.jpg]

File Edit Search View Analysis Tools Window Help

16 Windows (ANSI) hex

IMG_20250705_234750_Edited3_Stuffed.jpg

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
004571B0	00 44 59 53 5B AB 81 50 7C E7 07 00 00 4E 1B 00	.DYS[<.P ç...N..
004571C0	00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 64d
004571D0	1A 00 00 77 6F 72 64 2F 74 68 65 6D 65 2F 74 68	...word/theme/th
004571E0	65 6D 65 31 2E 78 6D 6C 50 4B 01 02 14 00 14 00	emel.xmlPK....
004571F0	00 00 08 00 00 00 21 00 5B 6D FD 93 03 01 00 00!..[mý"...
00457200	F1 01 00 00 14 00 00 00 00 00 00 00 00 00 00 00 00	ñ.....
00457210	00 00 7E 22 00 00 77 6F 72 64 2F 77 65 62 53 65	...~"..word/webSe
00457220	74 74 69 6E 67 73 2E 78 6D 6C 50 4B 01 02 14 00	ttings.xmlPK....
00457230	14 00 00 00 08 00 44 59 53 5B C2 85 64 82 AC 06DYS[À..d,-.
00457240	00 00 A2 28 00 00 11 00 00 00 00 00 00 00 00 00 00	...c(.....
00457250	00 00 00 00 B3 23 00 00 77 6F 72 64 2F 64 6F 63'#.word/doc
00457260	75 6D 65 6E 74 2E 78 6D 6C 50 4B 01 02 14 00 14	ument.xmlPK....
00457270	00 00 00 08 00 44 59 53 5B 7C F9 82 12 E3 00 00DYS[ù,.ä..
00457280	00 41 02 00 00 0B 00 00 00 00 00 00 00 00 00 00 00	.A.....
00457290	00 00 00 AA 2A 00 00 5F 72 65 6C 73 2F 2E 72 65	...**.._rels/.re
004572A0	6C 73 50 4B 01 02 14 00 14 00 00 00 08 00 44 59	lsPK.....DY
004572B0	53 5B 1E 82 9D 33 FD 00 00 00 B4 03 00 00 1C 00	S[.,.3ý...`.....
004572C0	00 00 00 00 00 00 00 00 00 00 00 00 00 B6 2B 00 00¶+..
004572D0	77 6F 72 64 2F 5F 72 65 6C 73 2F 64 6F 63 75 6D	word/_rels/docum
004572E0	65 6E 74 2E 78 6D 6C 2E 72 65 6C 73 50 4B 01 02	ent.xml.relsPK..
004572F0	14 00 14 00 00 00 08 00 3D 5C 53 5B 05 F1 4D 70=\\$[.ñMp
00457300	C5 6E 42 00 B2 70 42 00 0F 00 00 00 00 00 00 00 00	ÀnB.=pB.....
00457310	00 00 00 00 00 00 ED 2C 00 00 6D 65 64 69 61 2Fi,,media/
00457320	69 6D 61 67 65 2E 70 6E 67 50 4B 01 02 14 00 14	image.pngPK....
00457330	00 00 00 08 00 3D 5C 53 5B A5 9F 32 A3 5A 01 00=\\$[Ý2£Z..
00457340	00 4D 05 00 00 13 00 00 00 00 00 00 00 00 00 00 00	.M.....
00457350	00 00 00 DF 9B 42 00 5B 43 6F 6E 74 65 6E 74 5F	...B>B.[Content
00457360	54 79 70 65 73 5D 2E 78 6D 6C 50 4B 05 06 00 00	_Types].xmlPK....
00457370	00 00 0C 00 0C 00 FE 02 00 00 6A 9D 42 00 00 00þ...j.B...



The screenshot shows the HxD Hex Editor interface. A context menu is open over a selected block of text, with 'Copy' highlighted. The menu also includes options like Undo, Cut, Paste insert, Paste write, Delete, Fill selection..., Select block..., Select all, and Copy offset.

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00304F10	0A DA 9C B1 CC 2B EA 5C D1 B2 2D 79 AD 3E 9C 91	.Úoe+ì+è\Ñ=‐y.>œ'
00304F20	48 BB 68 DB EC 5F 47 48 C7 36 9F 7D 4B 36 8E 7D	H»hÜì_GHç6Ý}K6Ž
00304F30	E1 78 C0 42 97 DF DD 70 FF 9C E3 53 8F 67 BE FC	áxÀB‐ßÝþœäS.g%ü
00304F40	FD 3E 79 5D 7D 2B DD 5F B3 7F 26 93 DF 3E 1D 37	ý>y]}+Ý „.“.“B>.7
00304F50	44 7E 71 C1 21 7D ED F9 1B 2B 4C 7F AE B3 0D 7D	D~qÁ!)íü.+L.Ø„.)
00304F60	99 DE 3A E7 49 D4 B6 B8 15 A5 2B 93 9D 27 D2 2C	„p:çIÖg „. „. „. „.
00304F70	84 9A DA DB 4D EE FC 3C EC BC DE DB F6 FE D0 F7	„šÚUMiù
00304F80	D0 E3 AB 92 40 A4 DD 0D 5F 1A EA 28 60 18 12 52	Đä«’@HÝ
00304F90	8A 08 81 71 3A 4F 38 4D 27 C4 34 28 BB B5 B1 DC	Š..q:08
00304FA0	30 07 70 D0 FA EC 99 8E 5A 6B 1B F3 4D AD 45 41	0.pĐùí™
00304FB0	14 65 B5 4D C7 59 99 67 5A 51 7B 6F AD 5A 56 52	.euMÇY™
00304FC0	7B F2 92 67 E4 B2 00 54 90 88 B0 DC 6E 18 46 C6	{ò'gä“.
00304FDO	34 10 4A BD A1 E4 19 81 05 21 0A A4 15 24 07 A3	4.J¶;ä.
00304FE0	C4 08 22 D1 10 47 58 D1 A4 40 5A 45 CB CA 1A 87	Ä.”Ñ.GX
00304FF0	A6 EB B4 26 62 E1 60 77 80 2A B3 58 3F 69 88 71	;ë`&bá`
00305000	D0 CD 89 B2 18 28 47 F5 08 D7 E7 39 24 10 57 65	ĐÍ‰“.(G
00305010	D8 E1 80 79 5E 30 8D 03 9A 90 32 A3 B3 86 A2 C9	Øá€y^0.
00305020	45 C3 BD E7 92 91 A2 6E 50 49 71 C4 CB F5 8A 21	EA‰ç’ `c
00305030	0D 1A 12 38 26 A4 F1 6C 61 87 15 BC BE AE EA 4F	...8&ñ

4. If you see the following error, you can just hit “OK”:

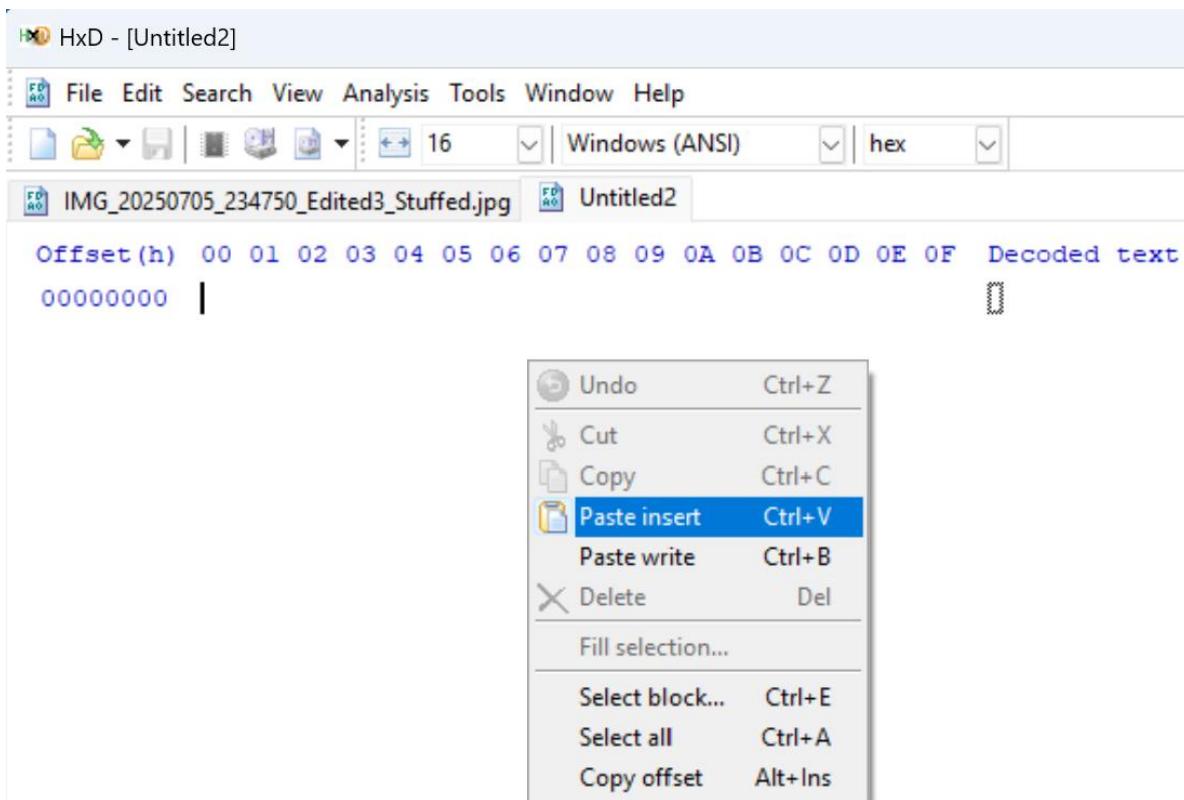


5. Open a new tab in your hex editor:

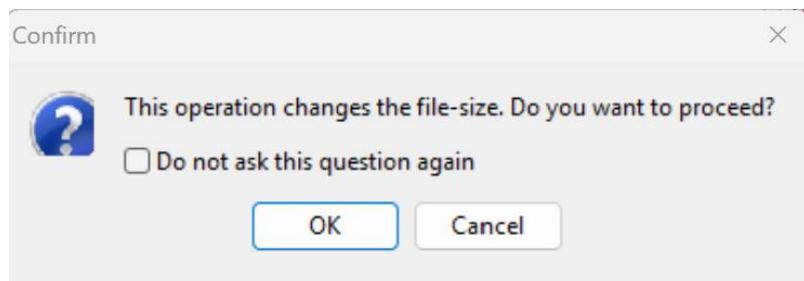
The screenshot shows the HxD Hex Editor interface with a new tab named 'd3_Stuffed.jpg'. The 'File' menu is open, displaying options such as New, Open..., Save, Save as..., and Save all. The main window shows the file's content in hex and ASCII formats.

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
3	5B AB 81 50 7C E7 07 00 00 4E 1B 00	.DYS[«.P ç...N..
0	0 00 00 00 00 00 00 00 00 00 00 00 00 64d
7	6F 72 64 2F 74 68 65 6D 65 2F 74 68	...word/theme/th

6. Paste the copied Docx data directly into the new tab of the Hex Editor:

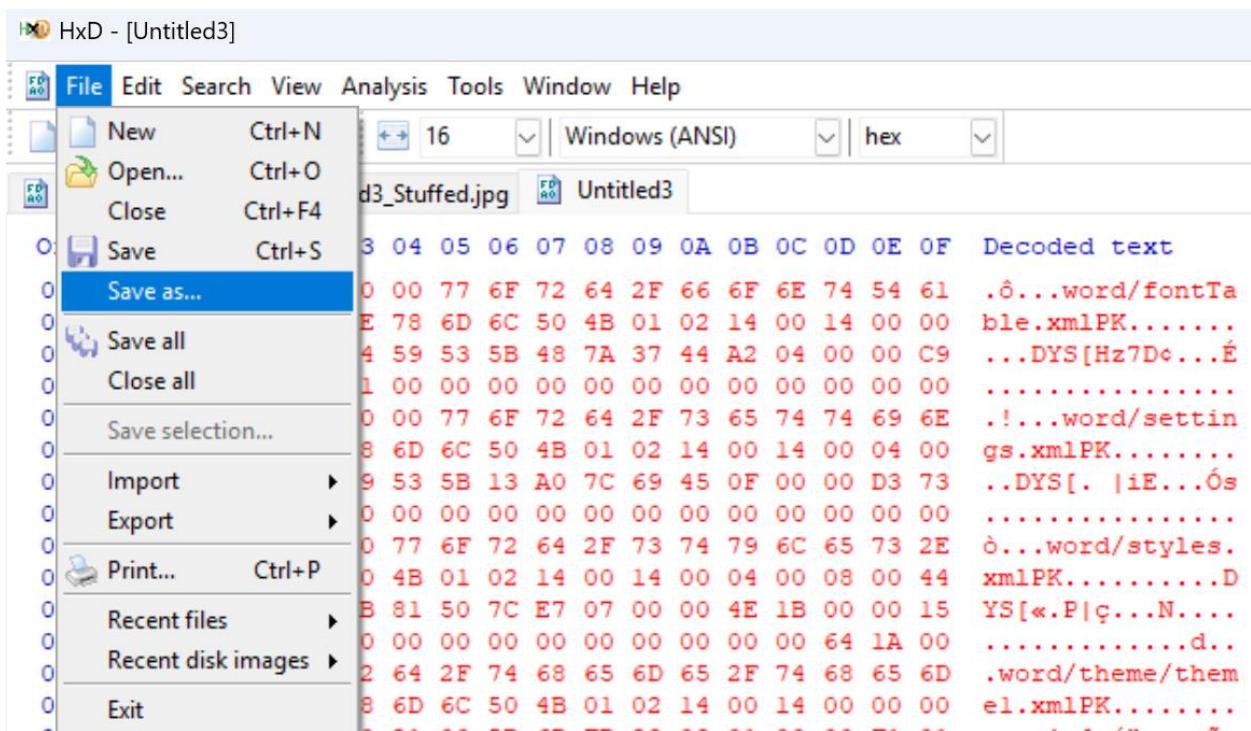


7. If you see the following error, you can just hit “OK”:

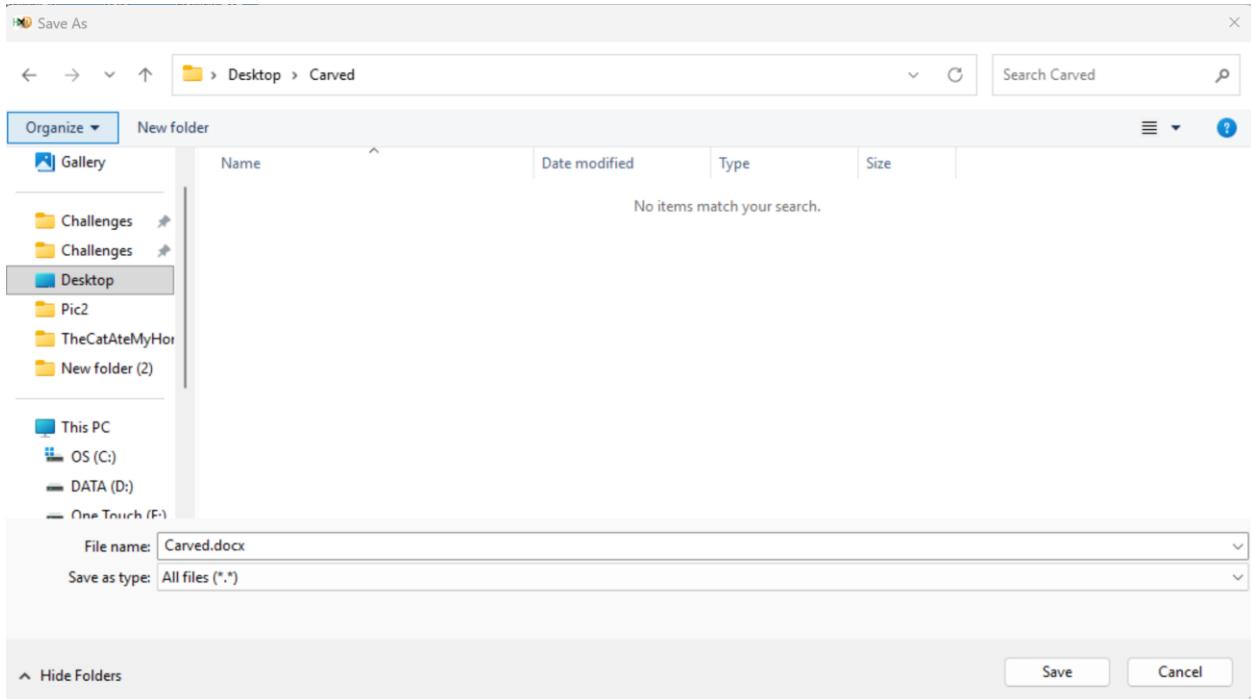


Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00429E10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429E20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429E30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429E40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429E50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429E60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429E70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429E80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429E90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429EA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429EB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429EC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429ED0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429EE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429EF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429F00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429F10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429F20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429F30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429F40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429F50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429F60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429F70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429F80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429F90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429FA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429FB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429FC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429FD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429FE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00429FF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0042A000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0042A010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0042A020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0042A030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0042A040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0042A050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0042A060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0042A070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

8. Choose “Save as” in your hex editor:



9. Choose “Save as type” All and give it the .docx extension - I named mine “Carved.docx”:



10. Hit “Save” and you should end up with a fully functional .docx file:



Carved.docx

- 11. When you open the newly carved file, “Carved.docx”, you should see the flag revealed inside the homework assignment:**

Homework Assignment: Forensics 101

This little guy might look cuddly and cute...but he assisted my cat in eating my homework!



Photo Credit: Chloe Regas

The flag is: **csawctf{C@ts_Luv_3@7ing_p@per!}.**

- 12. Flag:**

csawctf{C@ts_Luv_3@7ing_p@per!}.

End of Report