



## HxD GUIDED EXERCISE

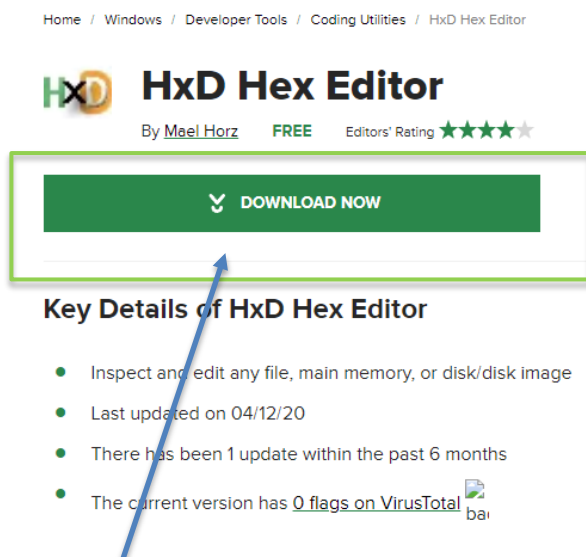
This exercise is intended for the HMFA Virtual Live course and carves content from a file

Video walkthrough available on the Tool Walkthrough Playlist at <https://youtube.com/@hexordia>

To get started download HxD Hex Editor from this website: [https://download.cnet.com/HxD-Hex-Editor/3000-2352\\_4-10891068.html](https://download.cnet.com/HxD-Hex-Editor/3000-2352_4-10891068.html)

Prior to installation, verify the hash value to the known good from the syllabus for students enrolled in the HMFA Virtual Live course. The MD5 hash value for the HxDSetup.zip version 2.5.0.0 is 2656E38DB1789CDA0B7E2F1BB7E0E74A.

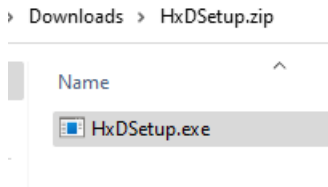
**\*\*IF YOU ALREADY HAVE HxD INSTALLED, PLEASE MOVE ON TO [SET UP AND USE. INSTALLATION](#)**



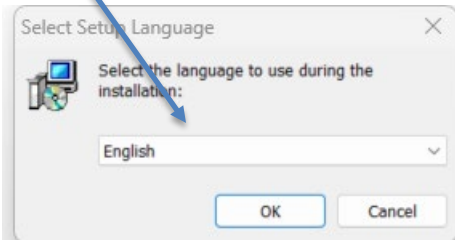
Click “download now”, there will be a re-redirect to another page, however the download should begin immediately (depending on the computer settings).

Once downloaded, there should be a file named “HxDSetup.exe. Double click to open or right click and select “open.” There may be a user control pop up asking if HxD is authorized to make changes. If “no” is selected the download will not open. If “yes” is selected the setup page will begin.

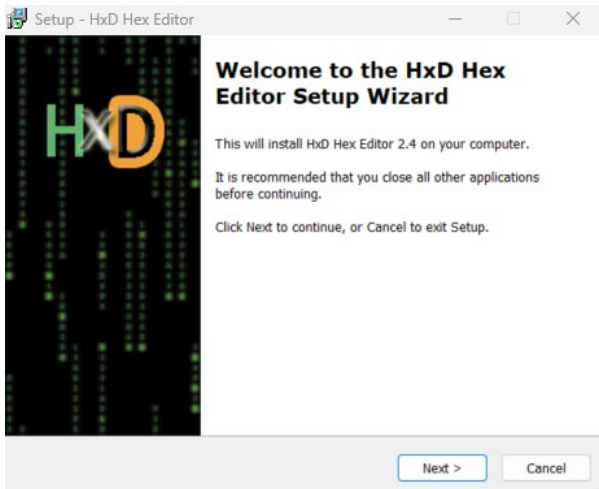




Select language.

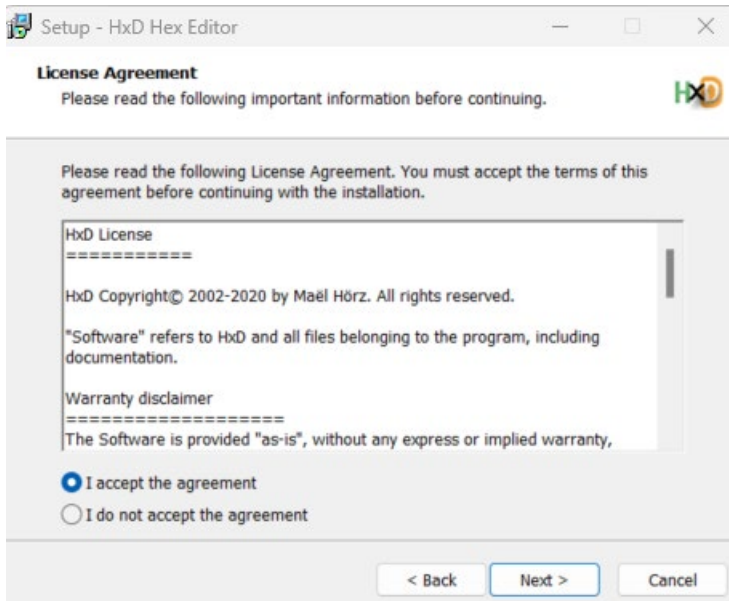


Select "next".

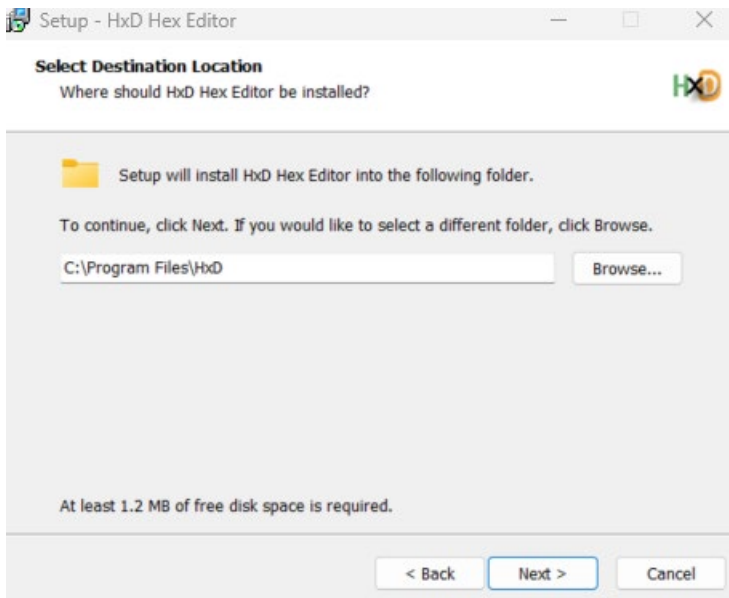


"Accept" and click "next."



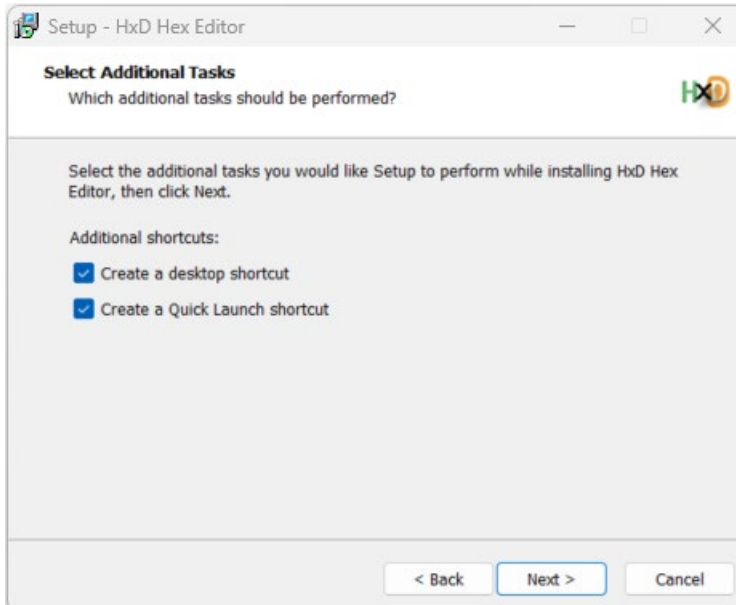


There will be a Select Destination Location (where the program will be saved). Default is program files. Select “browse” to change location. If utilizing the default, select “next.”

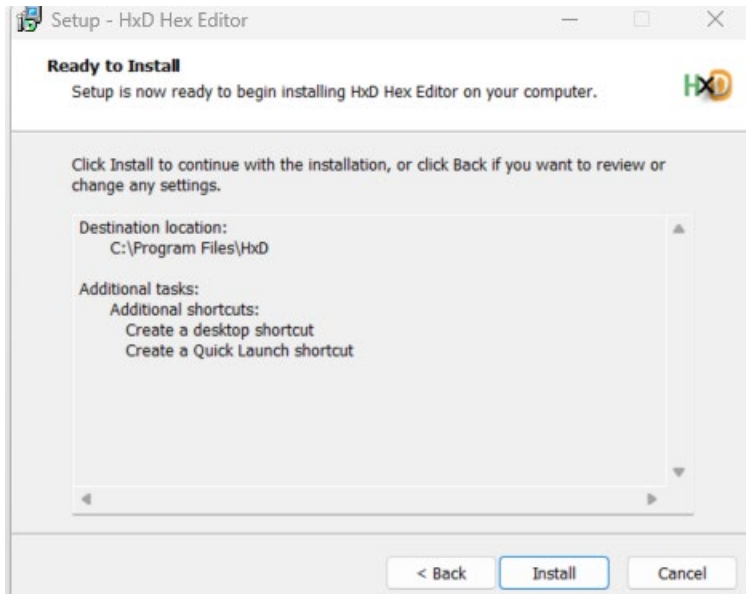


Next is optional shortcuts. Select “next.”



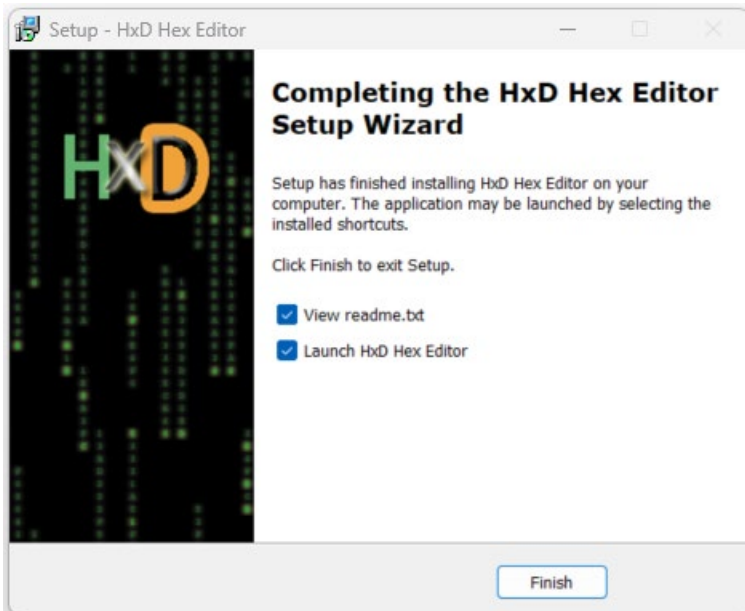


Select "install."



Selection option(s) of choice and select "finish."

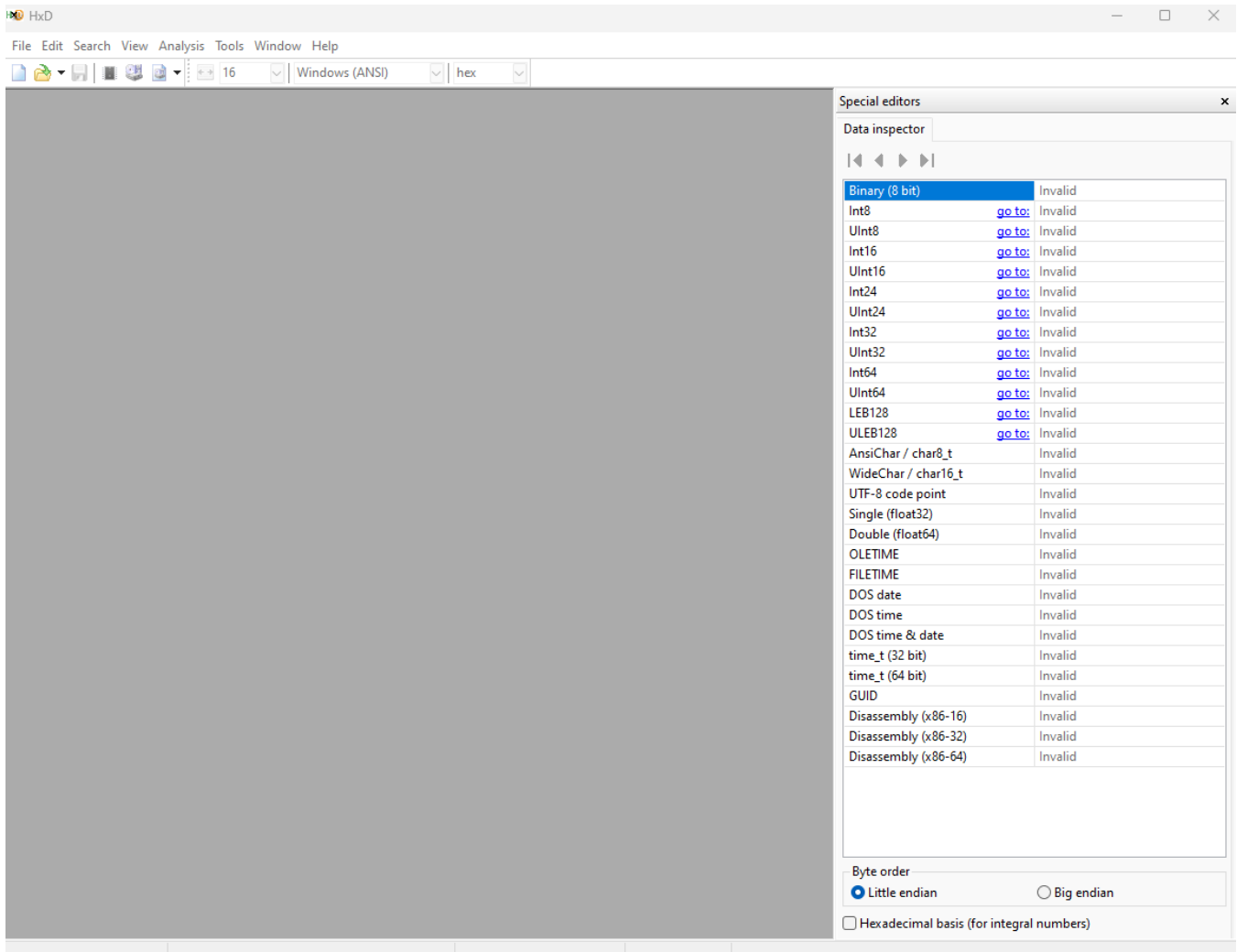




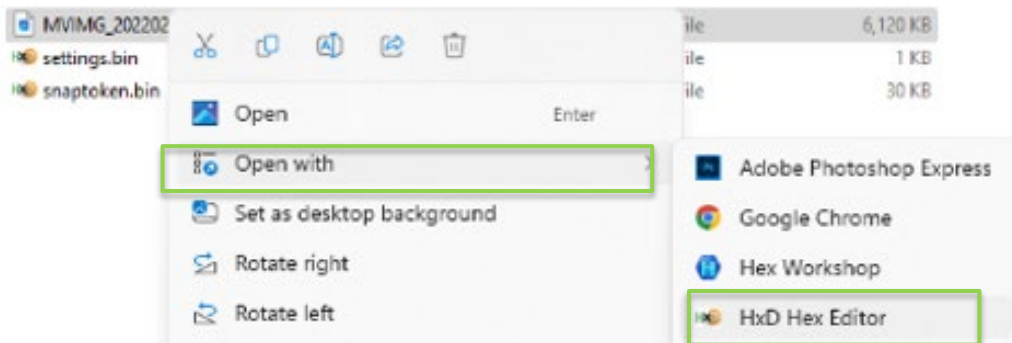
## SET UP AND USE

This is what the HxD program should look like.



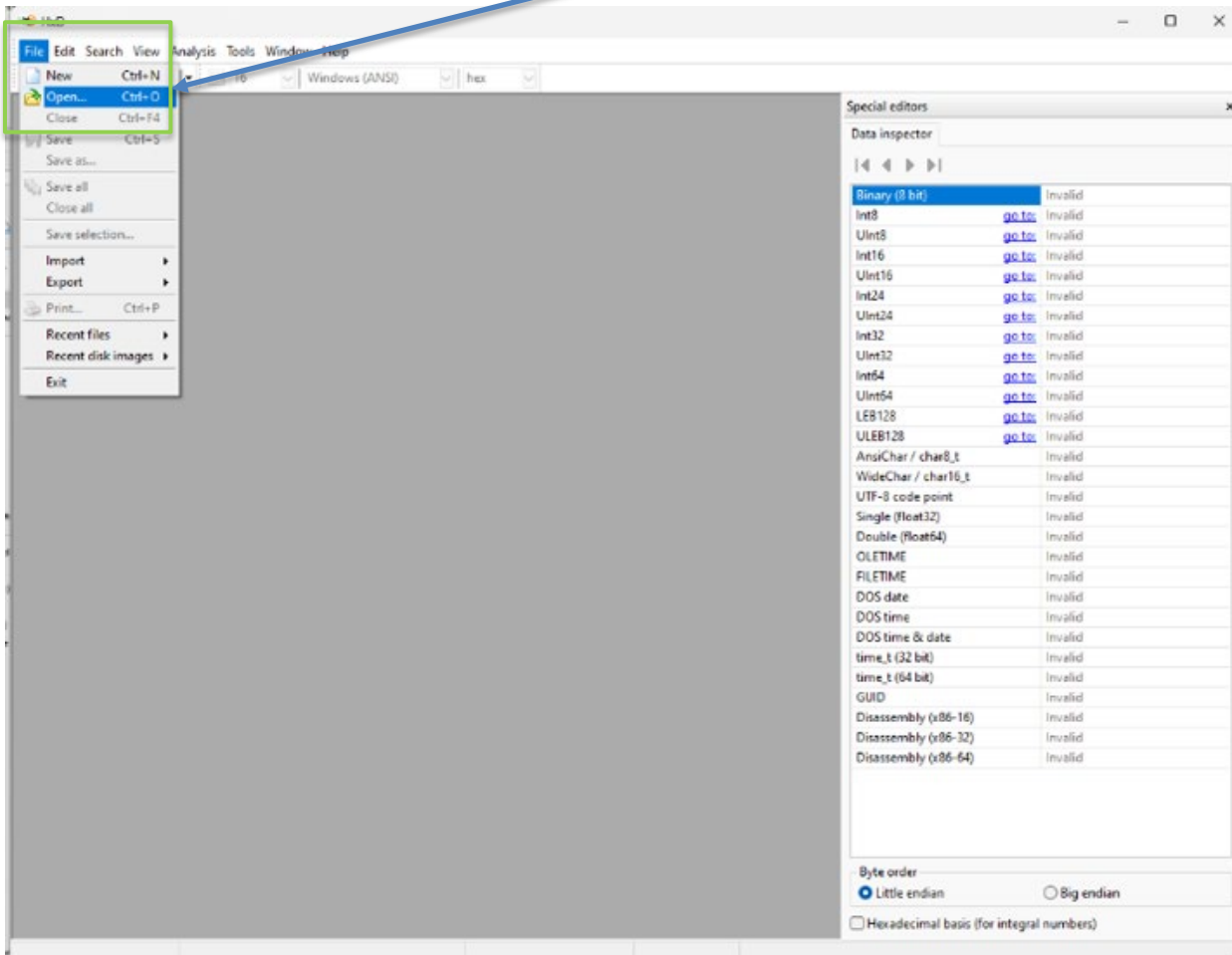


A file can be opened a couple different ways. Either right click the document and select “open” with (select HxD Editor).





Or select “file” (within the HxD Editor) and select “open”. Then navigate to wherever the file of choice is saved.









Highlight the start byte and then navigate to “edit and “select block”, it will automatically put the offsets at that location for start and end.

Example:

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
003D06D0	6E	9D	BC	BD	A8	09	6E	F9	C7	61	4B	98	AB	68	5A	31	n.4s".nuÇaK"«hZ1
003D06E0	B5	BB	19	1A	56	28	46	19	8F	7A	70	65	30	79	B3	15	us...V(F...zpe0v?
003D06F0	54	27	11	48	7A	F1	DB	1F	D6	AB	C1	7B	69	34			
003D0700	56	49	08	99	92	65	2D	80	7D	31	ED	ED	50	E2			
003D0710	A8	B6	82	28	E4	6F	2D	A4	21	DF	6E	70	DE	83			
003D0720	56	A4	2E	52	0B	BD	4A	DA	F2	FF	00	CD	85	42			
003D0730	7B	94	33	60	C8	FD	FE	80	7F	9C	55	C8	56	51			
003D0740	DC	04	BE	39	E4	FF	00	15	73	57	5A	8A	2D	D8			
003D0750	84	91	BB	FE	EE	E9	8E	0A	9E	E3	D8	7F	87	E5			
003D0760	D5	27	B4	2C	AB	23	08	73	B5	58	0E	7E	B4	42			
003D0770	BB	33	62	58	26	91	FC	87	4F	94	2F	DC	51	81			
003D0780	DA	A1	B9	B5	60	16	48	64	F2	C8	20	18	D8	E4			
003D0790	FE	94	D8	B5	30	FB	56	59	59	E6	5C	F9	6D	9C			
003D07A0	94	CB	8B	CB	79	EE	0B	41	1B	43	72	AA	04	92			
003D07B0	07	A6	3B	9A	94	AC	54	99	1C	E2	16	87	CD	82			
003D07C0	91	E4	DB	22	2B	60	1F	7F	A5	41	3A	B1	8C	05			
003D07D0	BF	0E	A1	7A	11	56	6F	65	8D	CA	21	40	2E	45			
003D07E0	F1	ED	9A	66	52	46	52	23	DA	81	71	22	B7	0C	AF	FC	nisfRFR#U.q" . . u
003D07F0	5F	87	1F	8D	5C	4C	CC	E1	A6	C2	F2	49	E4	38	47	23	+.. \Liá;ÀòIà8G#
003D0800	E6	DC	C7	A5	67	5F	69	37	36	C9	E6	5B	49	E7	C5	8F	æÜÇ#g_i76Èæ[IçÁ.
003D0810	9A	15	4C	15	6F	AD	6E	D9	B3	4A	12	46	88	EC	96	73	š.L.o.nÜ³J.F^i-s
003D0820	1E	76	E4	81	EA	3E	94	B2	20	8D	48	B6	95	58	23	60	.v.â>"^ .HQ•X#`
003D0830	3E	7A	9F	E9	5B	73	D8	9E	54	7F	FF	D9	00	00	18		>zŸé[s0žT.yü...]
003D0840	66	74	79	70	6D	70	34	32	00	00	00	00	69	73	6F	6D	ftypmp42....isom
003D0850	6D	70	34	32	00	00	0A	24	6D	6F	6F	76	00	00	00	6C	mp42...9moov...1
003D0860	6D	76	68	64	00	00	00	00	DF	2D	DA	75	DF	2D	DA	75	mvhd....B-Ÿh;B-Ÿh;

Select block

Start-offset:

End-offset:

Length:

hex  dec  oct

OK Cancel

Then either select the start offset or end offset to change. When selecting the end-off set make sure the final byte is selected.

MVIMG\_20220212\_164314.jpg

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
005F9B80	3F	00	7C	0C	BF	40	45	94	B6	00	EE	16	36	D3	29	80	? .   . ¿@E"q.i.6ó)€
005F9B90	3F	04	6C	7F	3F	A0	5A	03	3B	00	17	50	40	80	7A	36	?Äl.? Z.;.P@€z6
005F9BA0	BB	CF	1A	80	3F	00	84	D7	BE	40	81	98	B6	00	A0	0A	»İ.€?..*%@.~q. .
005F9BB0	36	3E	FE	80	3F	EC	68	7F	3F	80	F1	FE	3A	A0	BC	4F	6>.€?ih.?€Ÿp: 40
005F9BC0	40	80	CC	3B	BB	5A	18	80	3F	00	94	E2	BE	80	7F	9C	@€İ;»Z.€?."á%€..æ
005F9BD0	B6	00	E8	FB	35	9E	32	80	3F	9A	65	7F	3F	60	91	F2	q.èù5ž2€?še.?'`ò
005F9BE0	3A	50	72	40	40	80	C0	3E	BB	BE	15	80	3F	00	74	C9	:PrM@€À»»%€.€?.tÉ
005F9BF0	BE	00	F4	9F	B6	00	00	E1	35	E5	36	80	3F	A8	62	7F	%.òŸq..á5á6€?"b.
005F9C00	3F	60	C0	E3	3A	40	BC	4F	40	00	E3	3F	BB	40	13	80	?`Àá:€40€.á?»@€.€
005F9C10	3F	00	8C	CC	BE	00	03	A3	B6	00	3A	C7	35	E2	3A	80	? .@İ%..áq.:Ç5á:€
005F9C20	3F	43	60	7F	3F	70	DF	D2	3A	40	40	57	40	80	54	3F	?C`.?ÀBò:@€W@€T?
005F9C30	BB	D7	10	80	3F	00	20	DE	BE	C0	7B	A5	B6	00	58	AE	»*.€?. P%À{#q.X0
005F9C40	35	7C	3E	80	3F	54	5E	7F	3F	E0	75	C1	3A	C0	33	5E	5 >€?T^.?àuÁ:Á3^
005F9C50	40	00	E4	3D	BB	8D	0E	80	3F	00	A0	B3	BE	00	79	A7	@.á»...€?. '>%y\$
005F9C60	B6	00	AC	96	35	BB	41	80	3F	18	80	08	20	80	06	28	q.~5»A€?.€. €. (
005F9C70	AE	AA	BC	FB	F5	10	30	02									@*4úò.0[]

Example:





Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000001E0	00	43	55	00	00	91	92	02	00	07	00	00	00	4A	55	00	.CU..V.....JU.
000001F0	00	92	92	02	00	07	00	00	00	51	55	00	00	00	A0	07	''.....QU....
00000200	00	04	00	00	00	30	31	30	30	01	A0	03	00	01	00	00	.....0100.....
00000210	00	01	00	00	00	02	A0	04	00	01	00	00	00	C0	0F	00	.....Ä.....
00000220	00	03	A0	04	00	01	00	00	00	D0	0B	00	00	05	A0	04	.....Ð.....
00000230	00	01	00	00	00	60	55	00	00	17	A2	03	00	01	00	00	.....U...c.....
00000240	00	02	00	00	00	01	A3	07	00	01	00	00	00	01	00	00	.....É.....
00000250	00	01	A4	03	00	01	00	00	00	01	00	00	00	02	A4	03	..#.....#.....
00000260	00	01	00	00	00	00	00	00	00	03	A4	03	00	01	00	00	.....#.....
00000270	00	00	00	00	00	04	A4	05	00	01	00	00	00	58	55	00	.....#.....XU.
00000280	00	05	A4	03	00	01	00	00	00	1B	00	00	00	06	A4	03	..#.....#.....
00000290	00	01	00	00	00	00	00	00	00	08	A4	03	00	01	00	00	.....#.....
000002A0	00	00	00	00	00	09	A4	03	00	01	00	00	00	00	00	00	.....#.....
000002B0	00	0A	A4	03	00	01	00	00	00	00	00	00	00	0C	A4	03	..#.....#.....
000002C0	00	01	00	00	00	03	00	00	00	00	00	00	00	D5	01	00	.....ö.....
000002D0	00	40	42	0F	00	B4	00	00	00	64	00	00	00	32	30	32	.@B...'.d...202

Select block ✕

Start-offset:

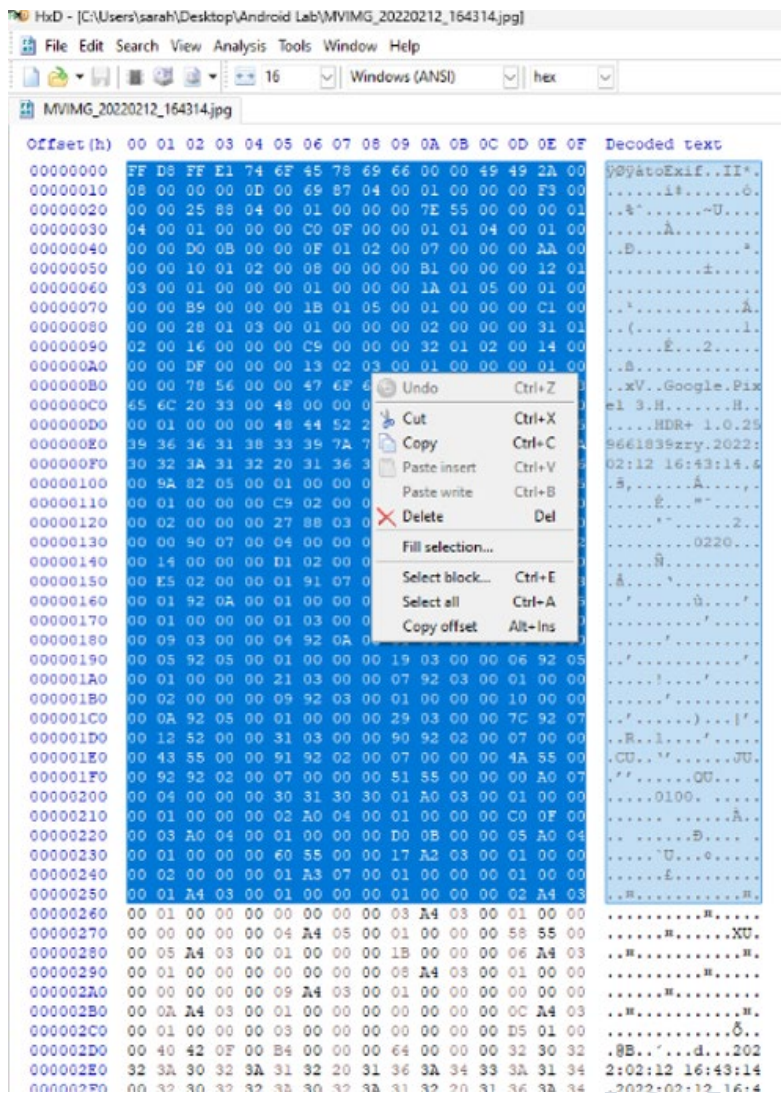
End-offset:

Length:

hex  dec  oct

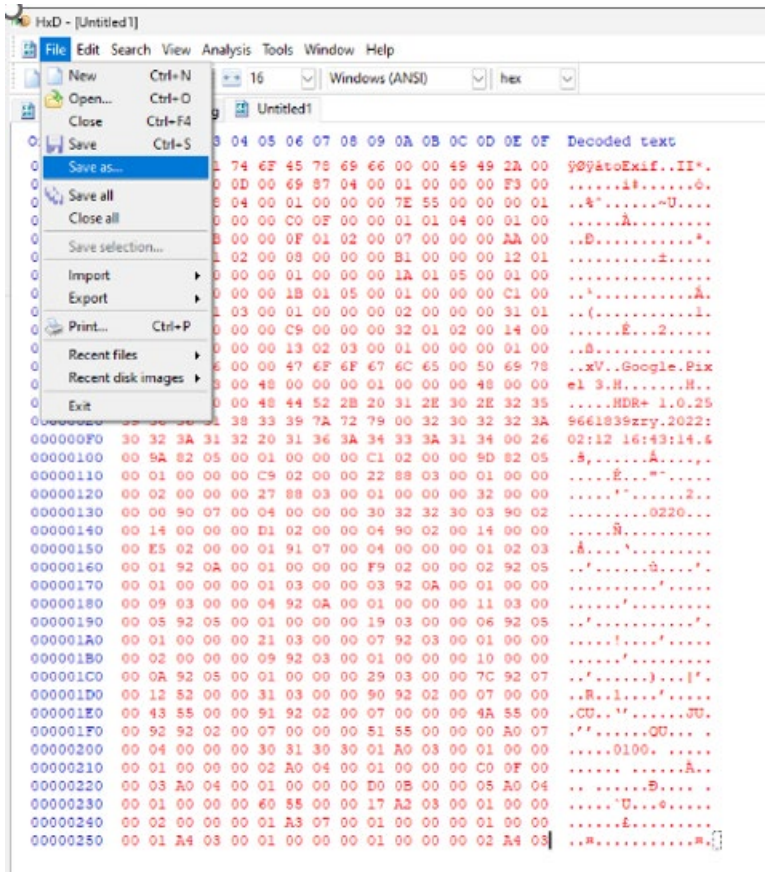
The last byte of the offset would be F based on the column it falls in.

Once the block is selected, right click and select "copy "(or CTRL-C).

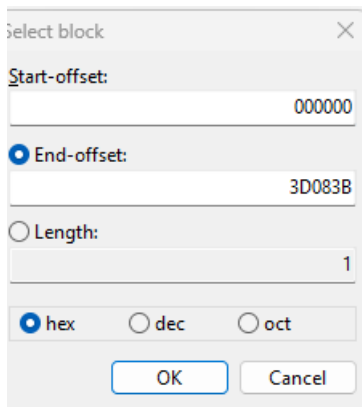




Select “file” and “new”. Paste copied bytes into new file. To save the file, click “file” and “save as” (name the document).

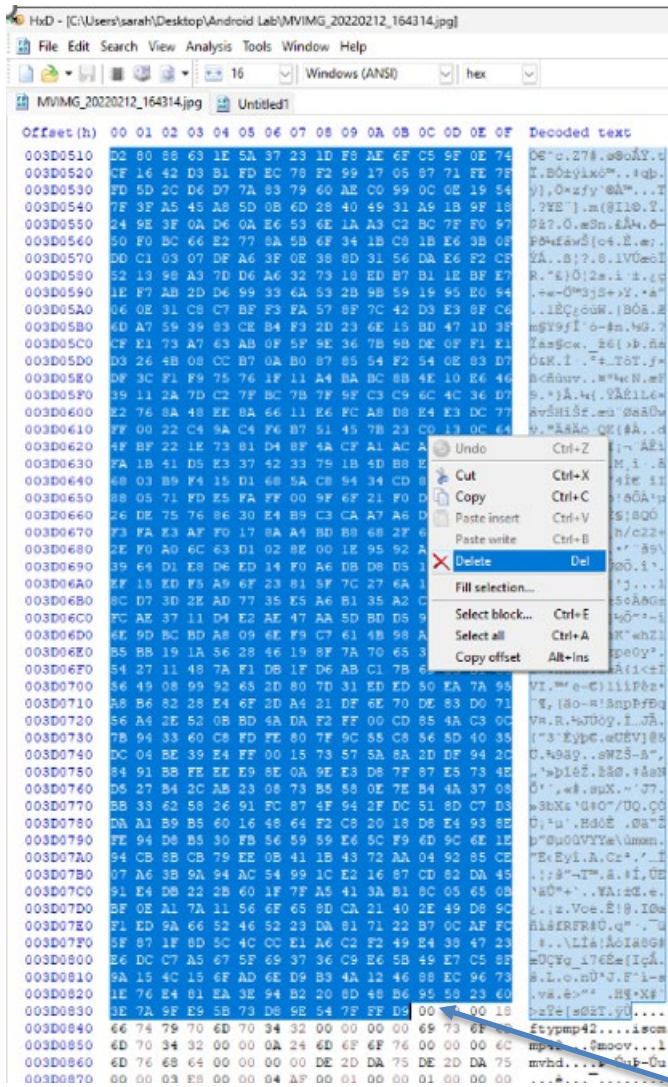


Of note, there is also an option to delete from the start of the offset to the top of the document. In the end offset location, enter the last digit before the file to be carved. The starting offset in this case will always be all zero’s (000000) click “ok” and the block will highlight.



You can now simply right click and select “delete”.





Then “file”, “save as” (name the document). This is the starting byte of the file to be carved out.

