Assignment *02*

David Murillo Santiago
Professor Ervin
IS-4483
16 February 2024

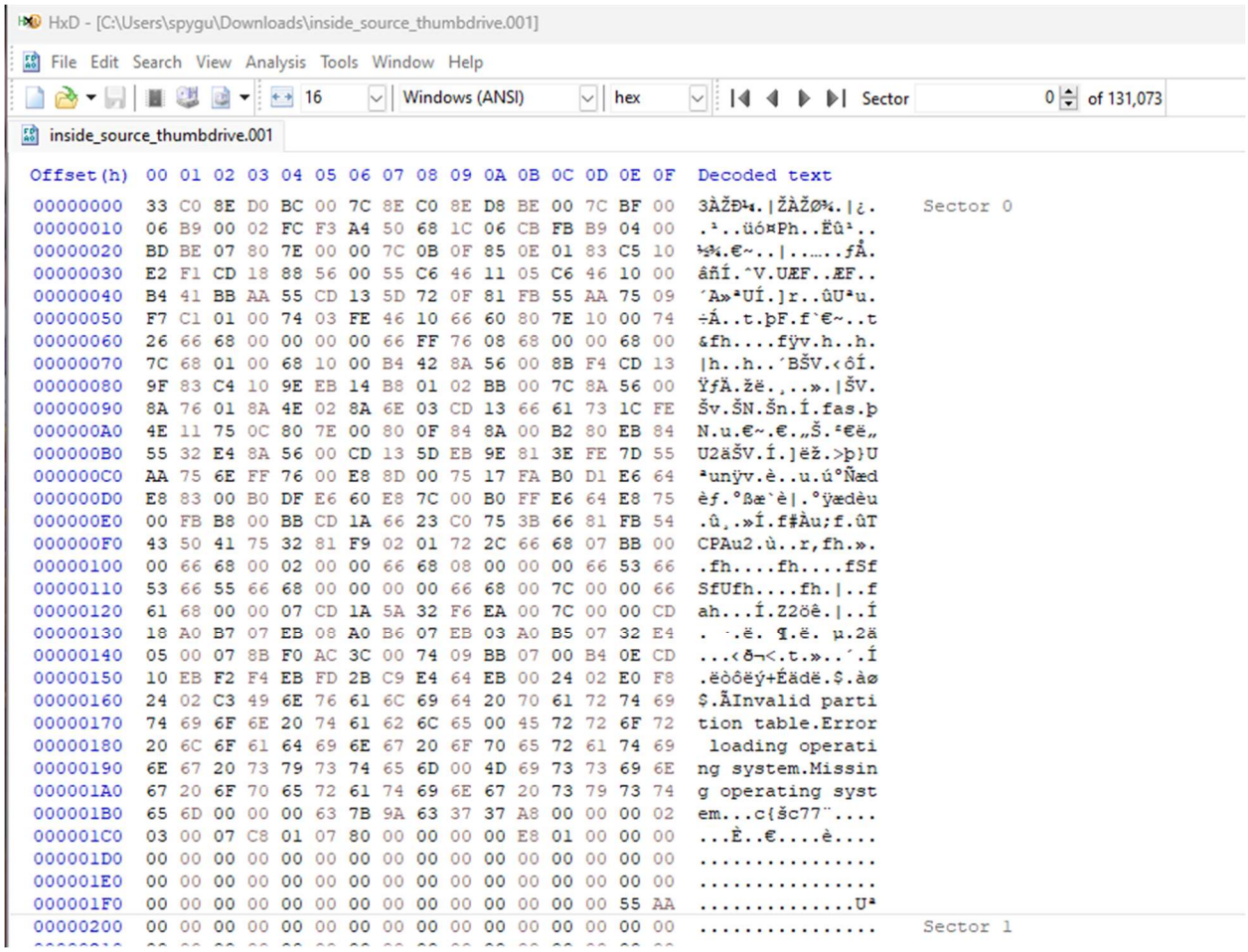
INTRODUCTION

In this assignment I will use HxD Hex Editor to extract information embedded within File Slack of various files.

PROCESS

Step *1: Download the thumbdrive image and open it on HxD.*

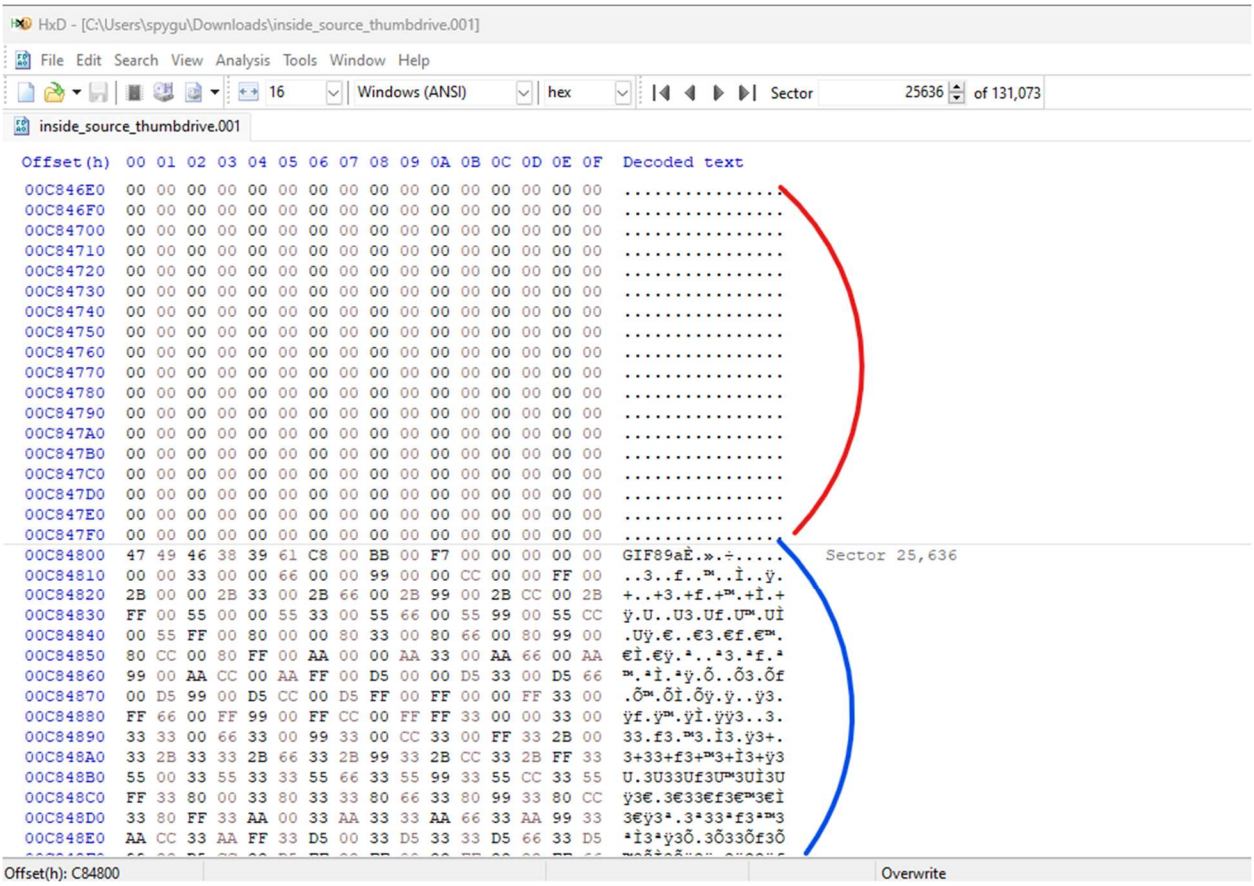
To begin, I downloaded the thumbdrive file from the “assignment 2” OneDrive and opened it with HxD Hex Editor.



I opened the thumbdrive file with HxD. This will allow me to view the information in the file slack of the thumbdrive.

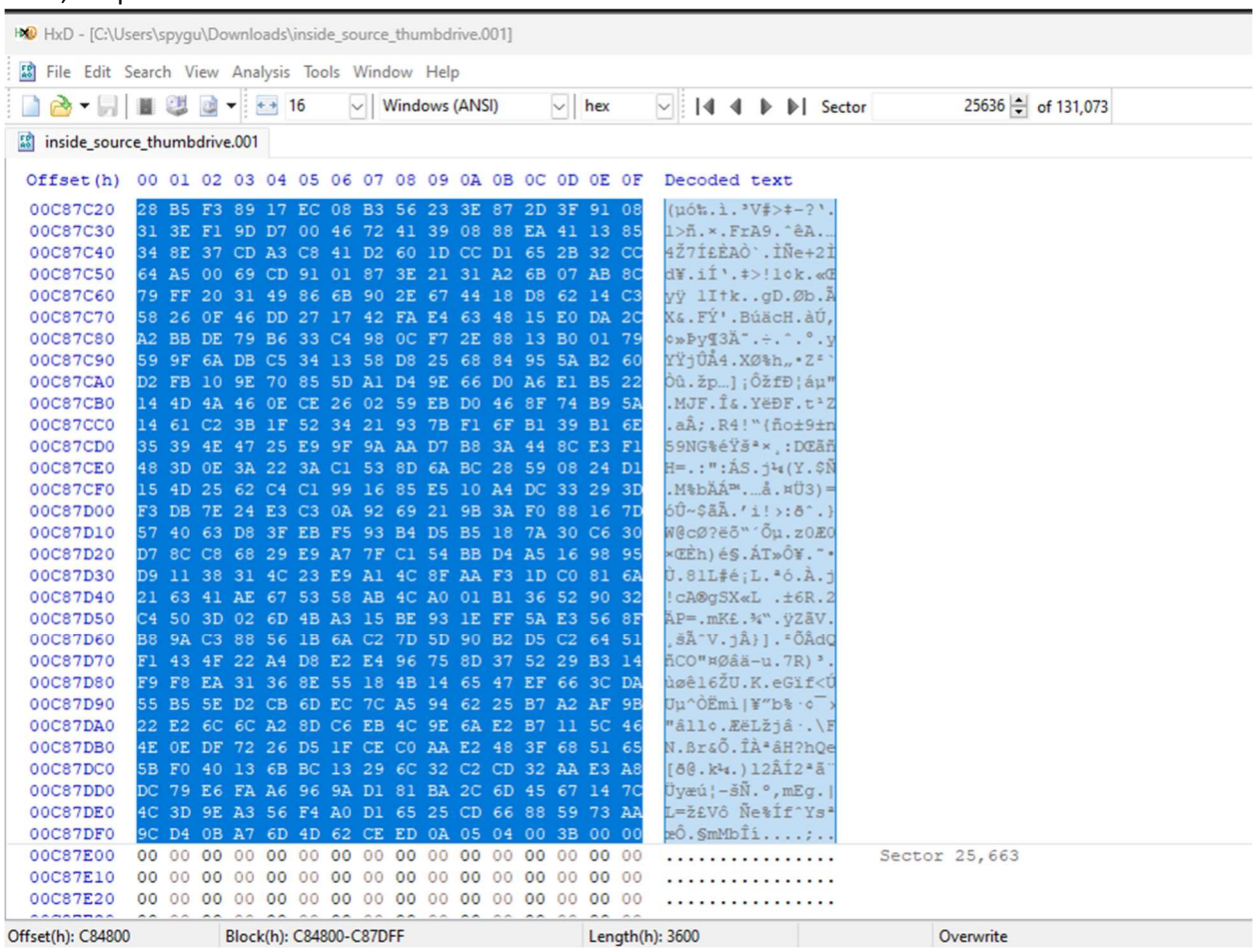
Step *2: Examine File Slack.*

Next, I searched for the “C1dwIEQW-gc.jpg” file whose starting sector was at 25472. Because the information I am looking for is in the file slack, I needed to head to the end of the file.

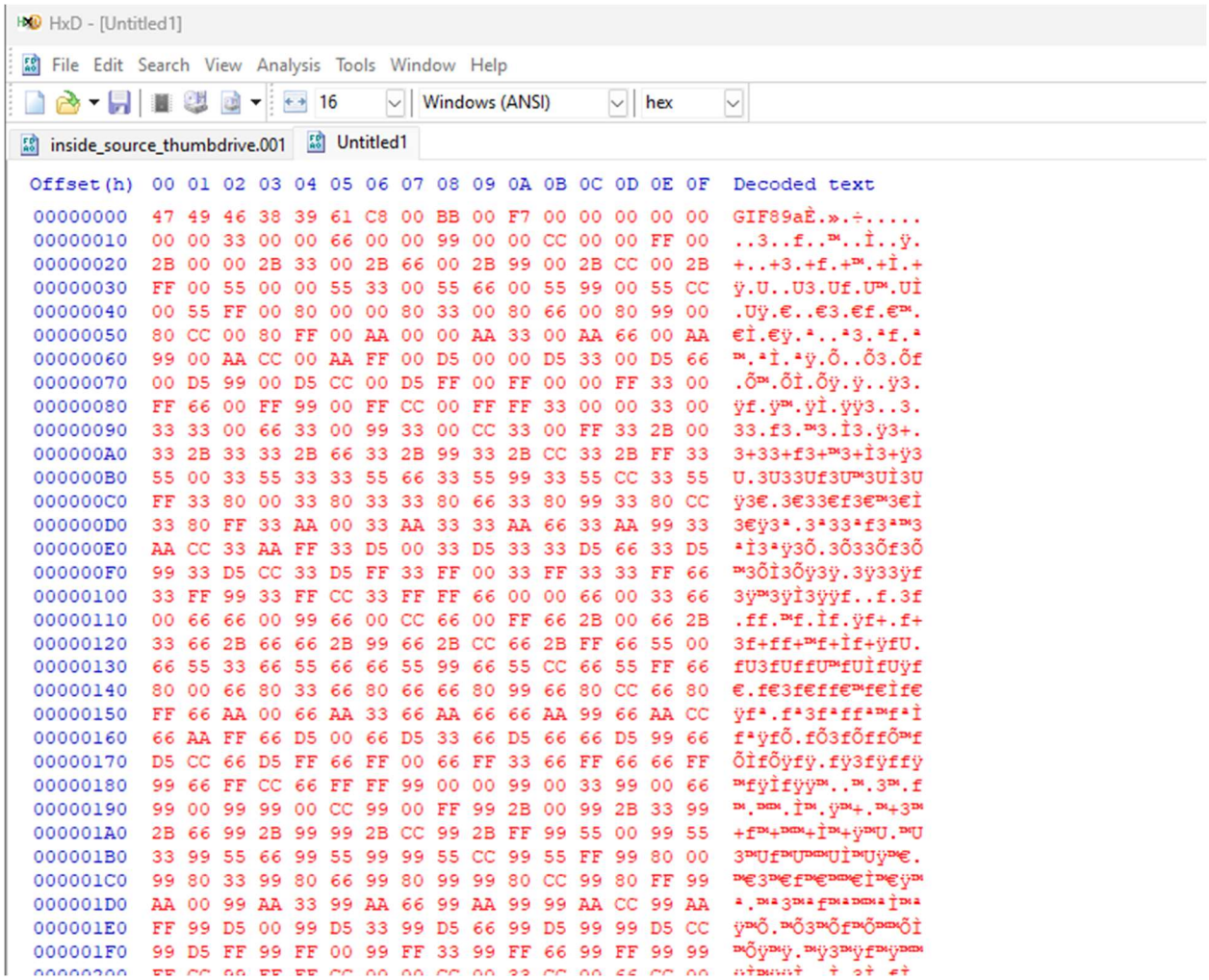


Because the file began at sector 25472, and the file was approximately 164 sectors long, I searched for the file slack which would be located on sector 25636. In the screenshot, the red represents the RAM slack that was overwritten by the file, and the blue represents the file slack which contains critical information.

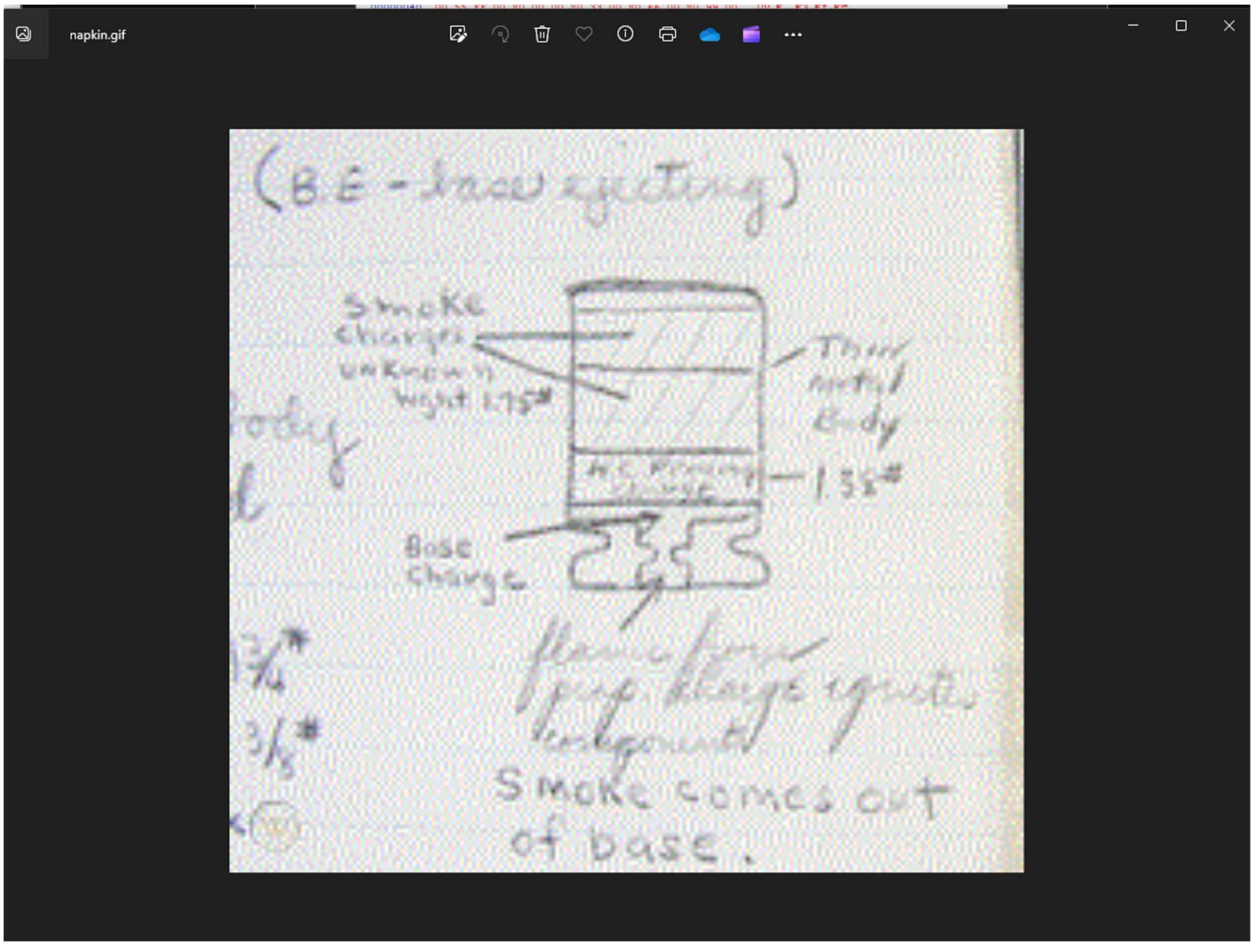
Next, I copied the contents of the file slack.



The File Slack was 27 sectors long, so I copied the contents all the way to sector 25663.

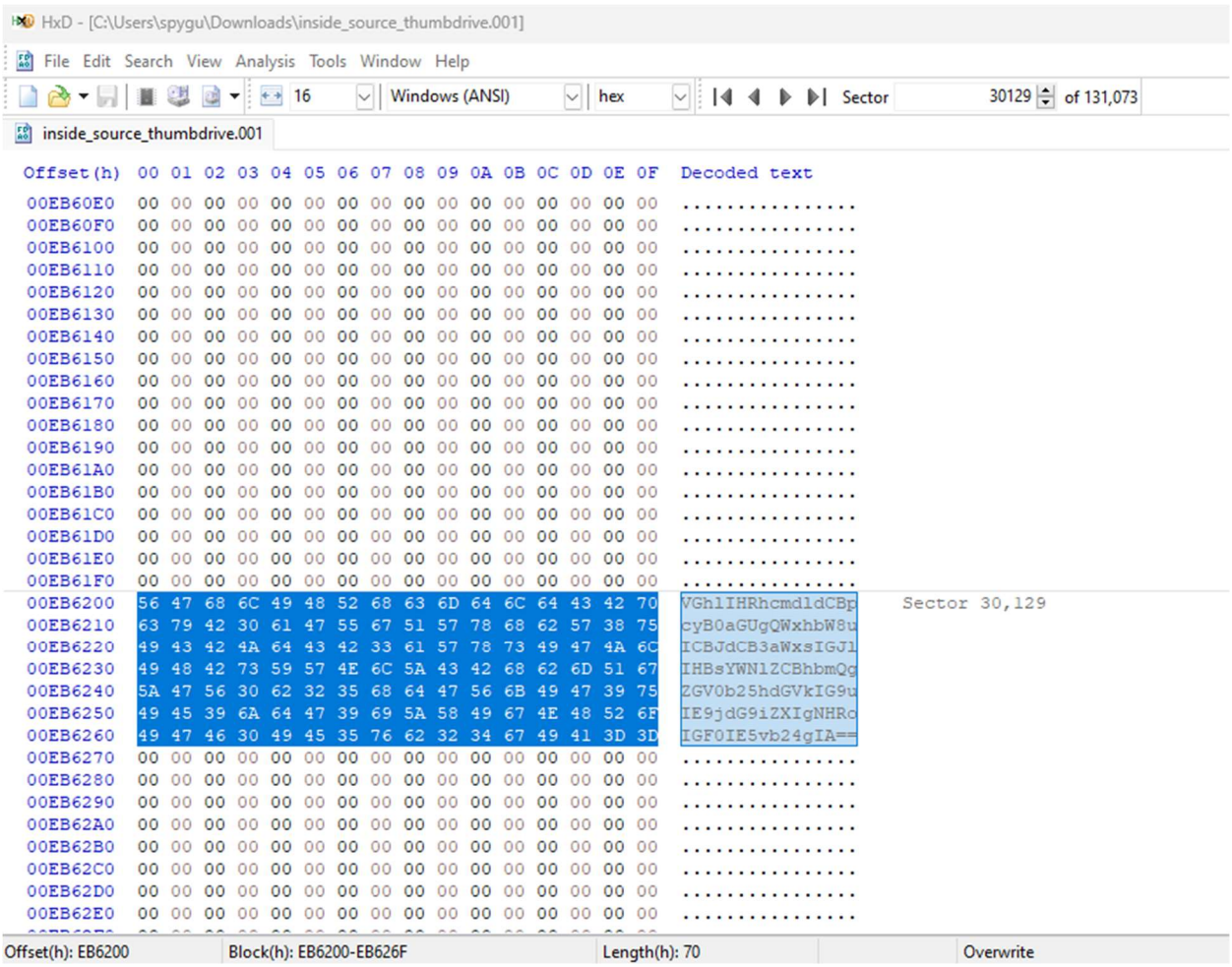


I then pasted the contents onto a new file.

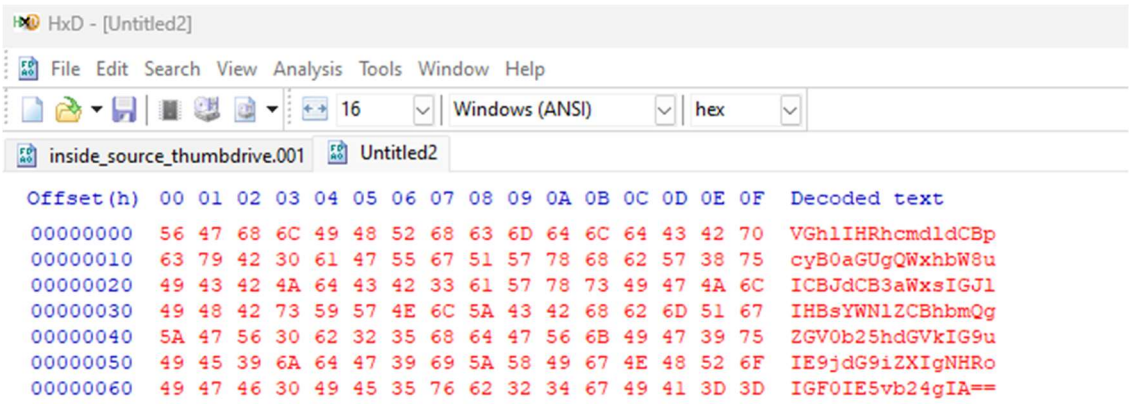


After saving the new file as a gif, I was able to open the file and view the original contents that were not overwritten by the image file.

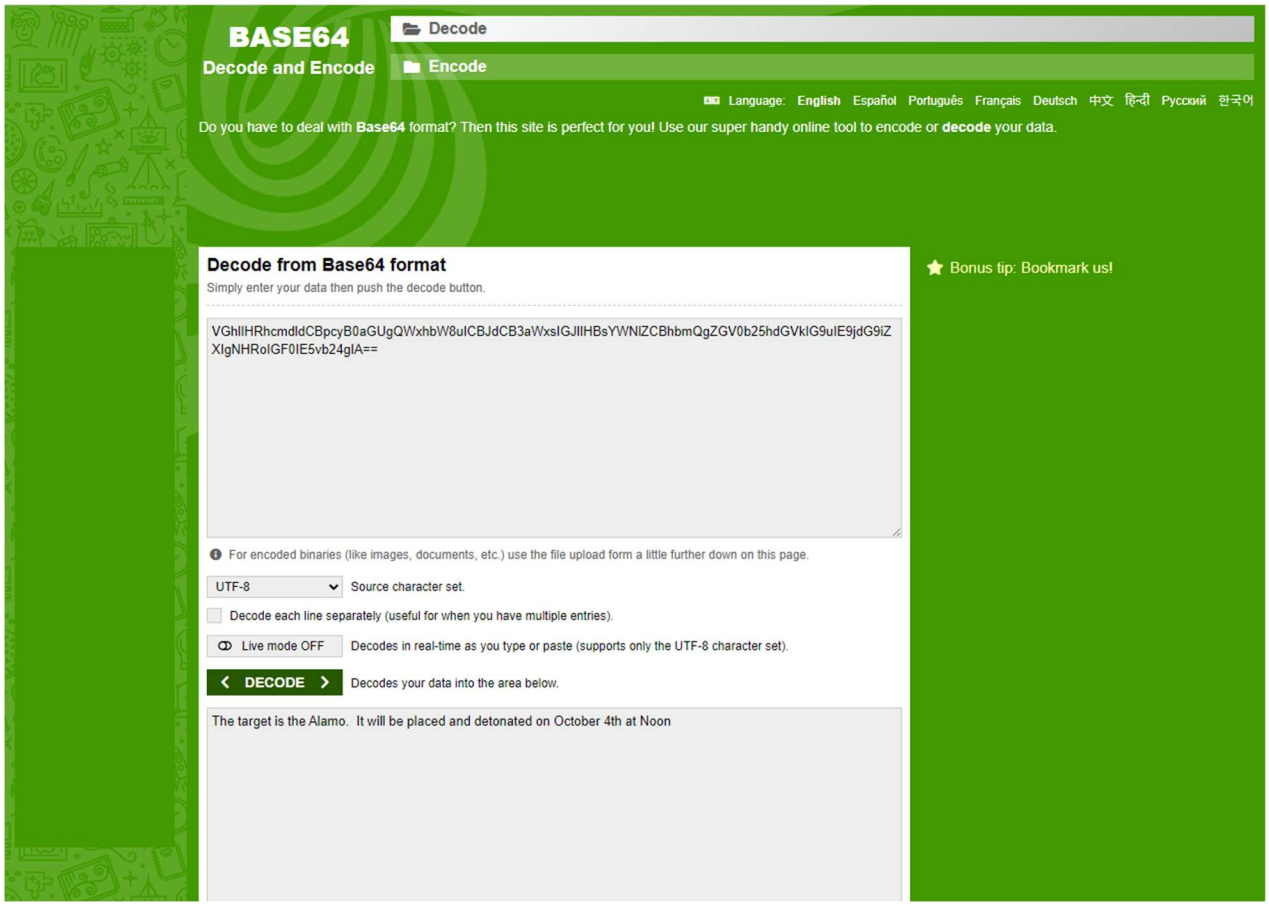
Next, I located the next image file on the thumb drive.



The file's starting sector was 29536 and the file was 593 sectors long, therefore I searched for the file slack at sector 30129.



I extracted the contents of the file "slack", but it appears to be encoded in Base64. This is evident because the standard output translation to the right of the hex values seems to be encoded. Base64-encoded data often ends with "=" as seen in the translation.



I then copied the encoded data and pasted it onto a Base64 decoder. Upon decoding, the data read "The target is the Alamo. It will be placed and detonated on October 4th at Noon."

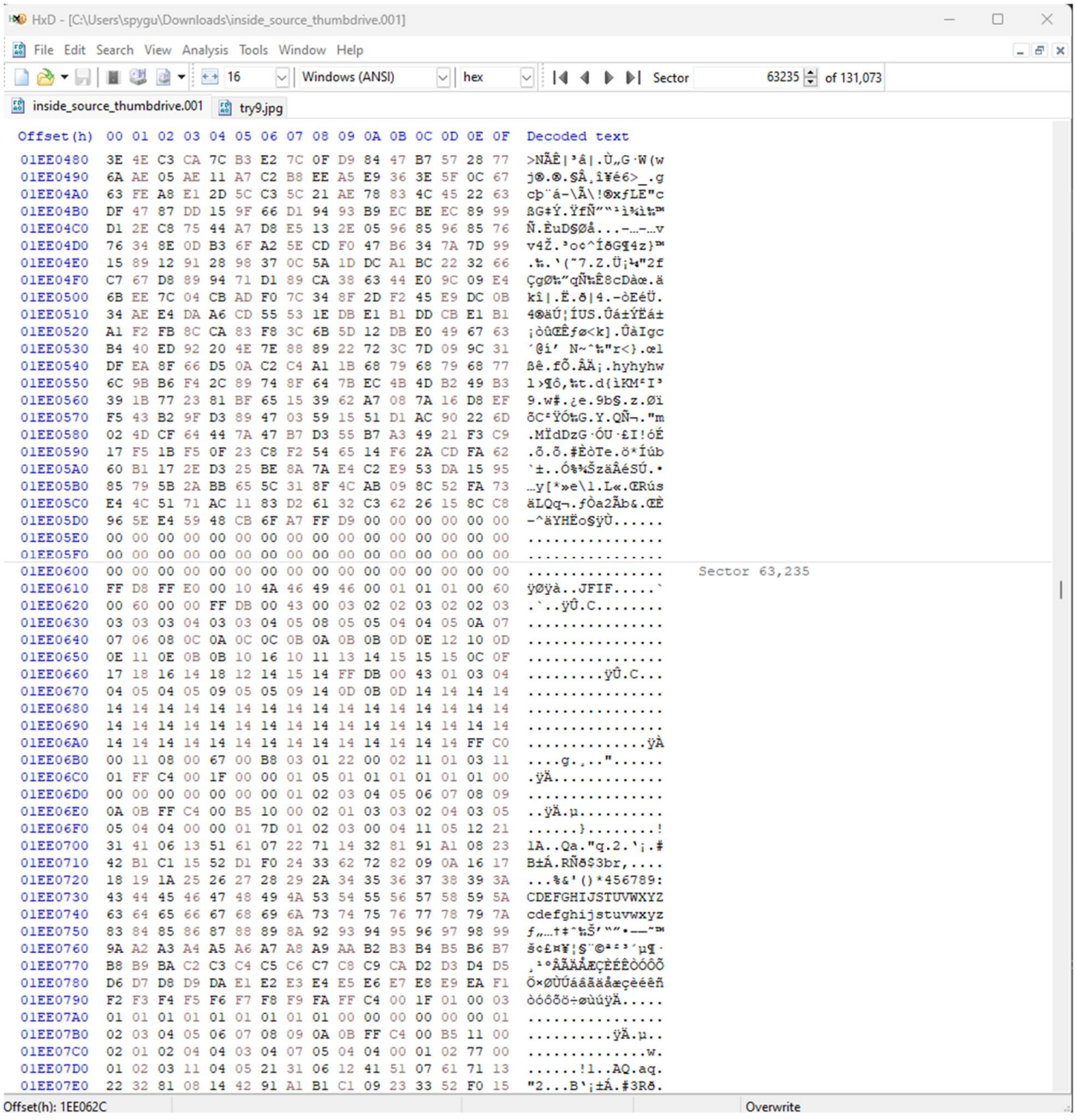
Next, I needed to find the phone number hidden in the file slack of one of the following files.

Filename	Size in Bytes	Starting Sector
Y81_LvzzDrM.jpg	339240	12864
Y-ZPu23vE_Q.jpg	384768	13536
1jj7wpZKf_A.jpg	581183	14304
7dyp4OxAluM.jpg	799824	18528
cL3hhw4Ol5k.jpg	634656	26368
fG64rnKIryM.jpg	734890	30144
koYuRh-jE6U.jpg	583666	35200
OGJU0rK2i_4.jpg	603879	58048
Pyut03Gn98w.jpg	312794	62624
Q8XWnPkOsKs.jpg	636847	63264

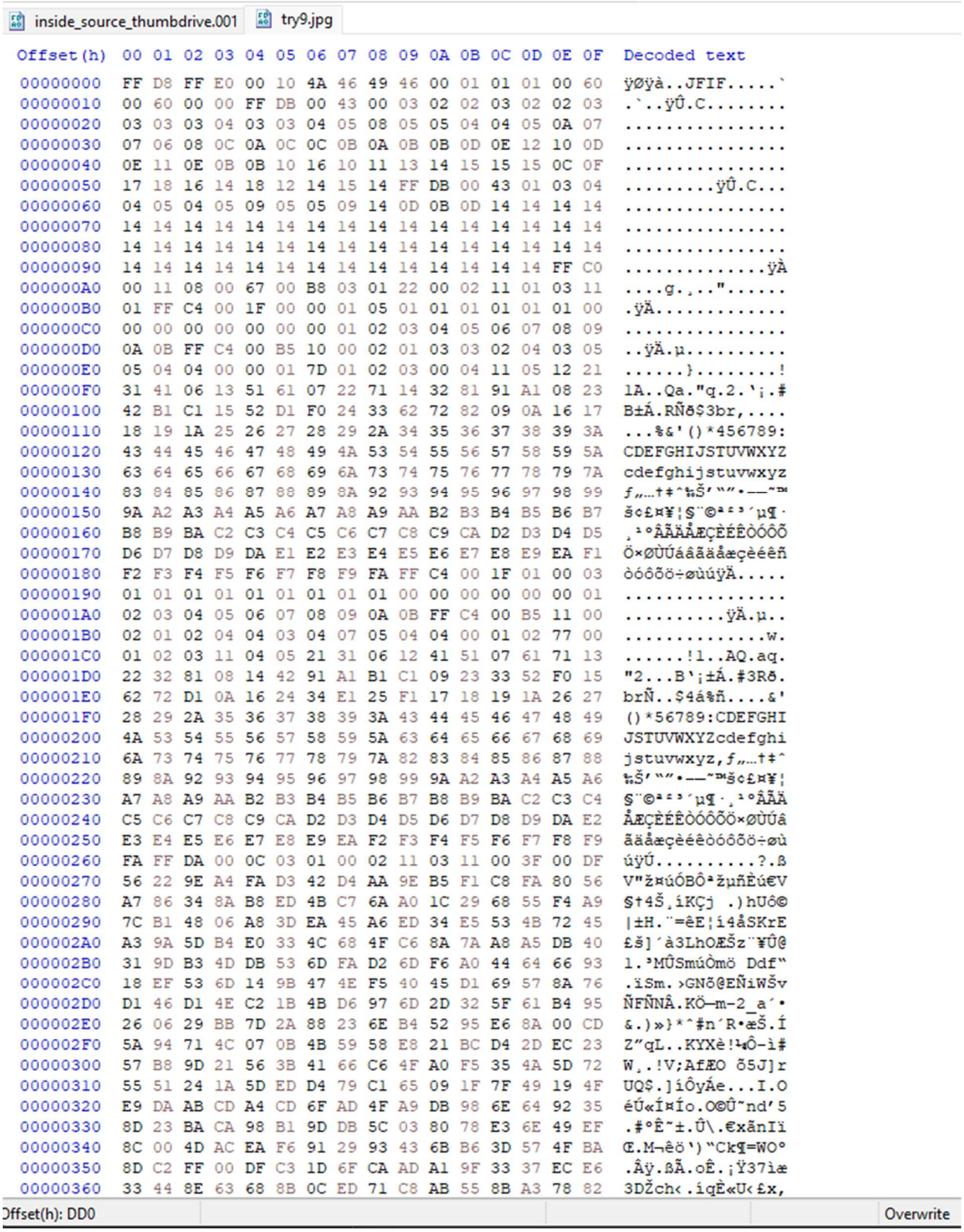
Size in Bytes	Starting Sector	Required Sectors	Expected Ending Sector
339240	12864	663	13527
384768	13536	752	14288
581183	14304	1135	15439
799824	18528	1562	20090
634656	26368	1240	27608
734890	30144	1435	31579
583666	35200	1140	36340
603879	58048	1179	59227
312794	62624	611	63235
636847	63264	1244	64508

I created the following Excel table to determine the ending sector address for the image files. I calculated this by dividing the size of the file in bytes by 512 bytes (the standard size of a sector) to determine the required number of sectors for the file. I rounded these values up to the nearest whole number, reflecting the allocation practice of most file systems. The slack space within the final sector occupied by the file includes any remaining data, and the file slack refers to the space from the end of the file to the end of the last cluster allocated to it.

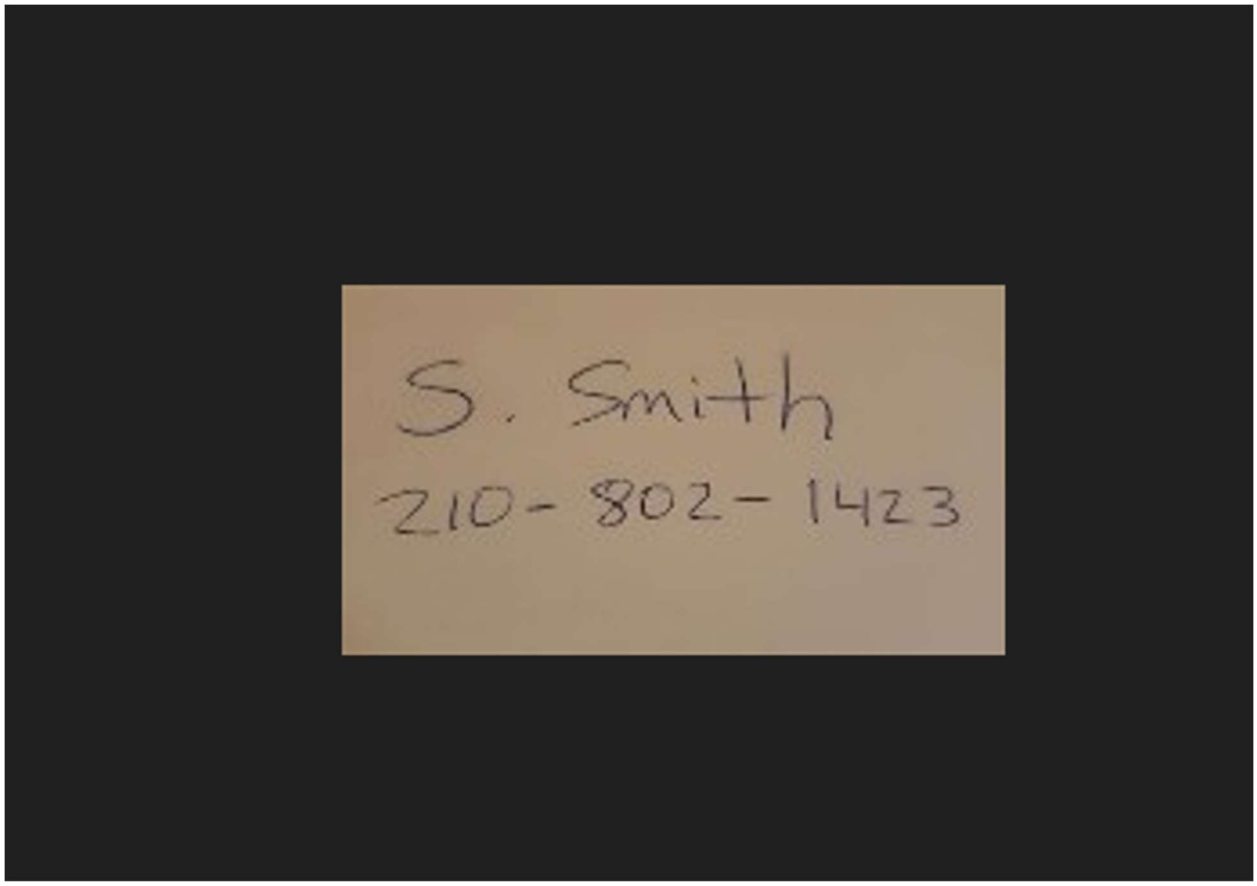
After determining the expected ending sector address for each of the files, I went file by file to determine which file may hold the information I am looking for.



After going file by file, I found that there was an image file within the file slack of "Pyut03Gn98w.jpg".



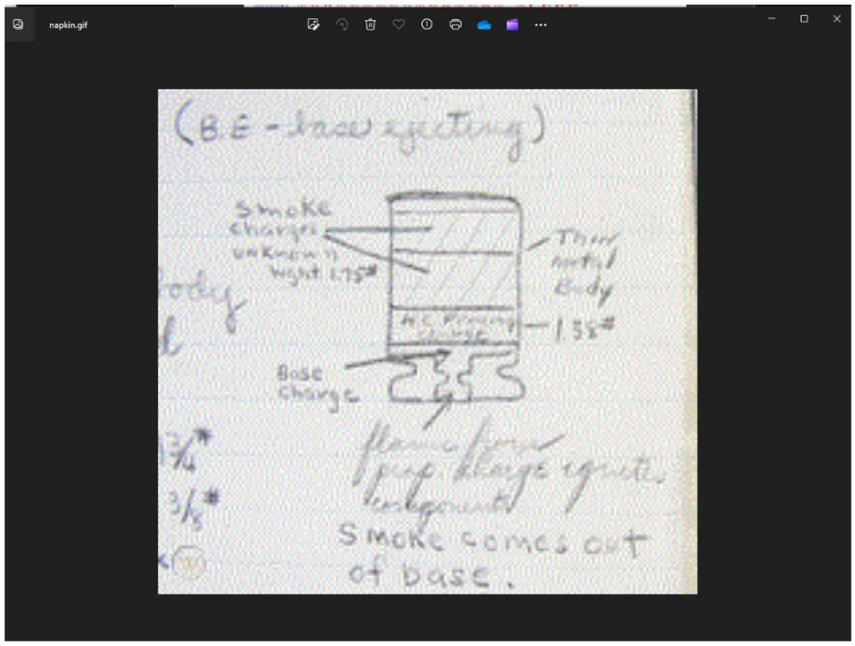
After finding the information in the file slack, I copied it and pasted it on a new file named "try9.jpg".



I saved the file as a jpg and opened the image. The image was of a name and phone number, "S. Simth" and "210-802-1423".

Therefore, I successfully found the name and phone number hidden within the file slack.

Step *3: Extracted Information.*

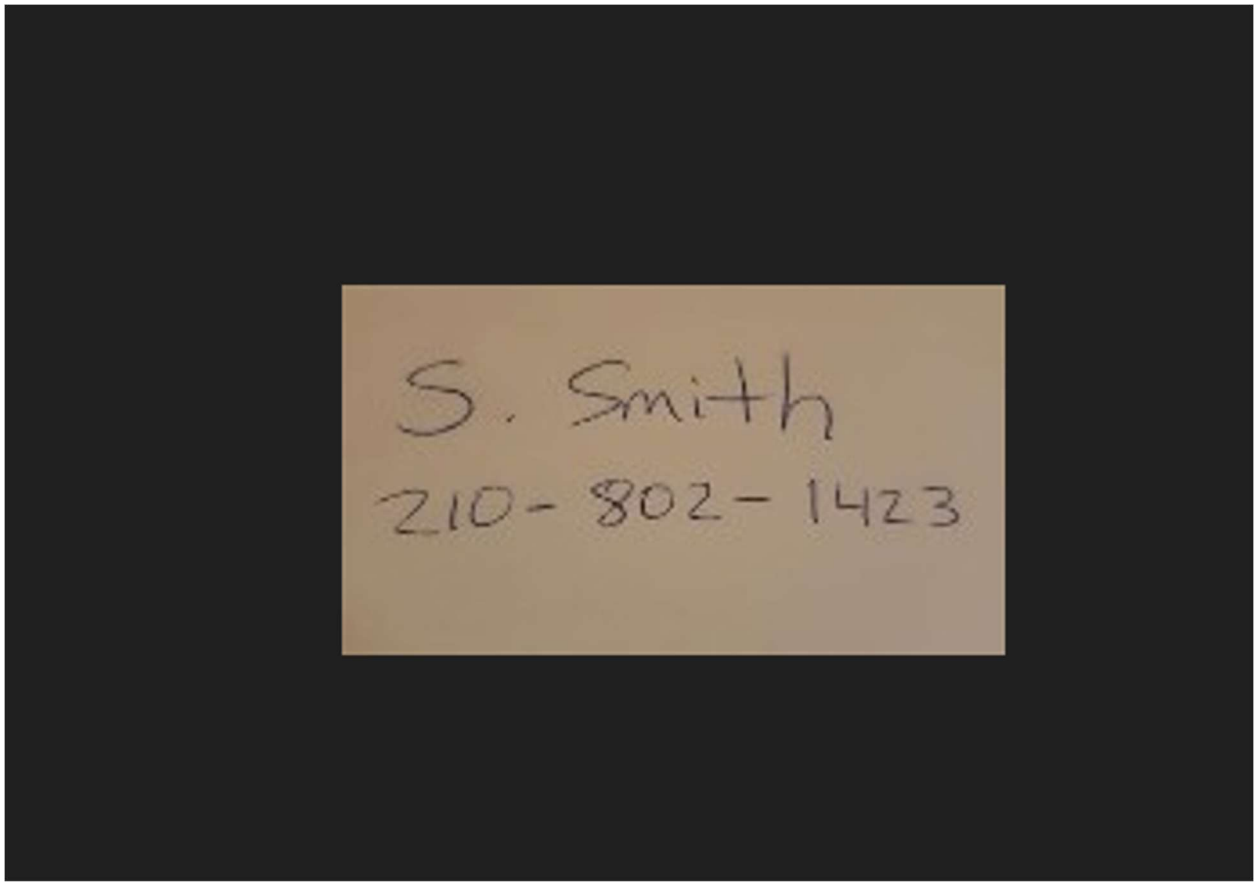


By extracting the gif file hidden in the thumb drive's file slack, I was able to extract the image of the bomb which was drawn on a napkin.

DECODE Decodes your data into the area below.

The target is the Alamo. It will be placed and detonated on October 4th at Noon

By decoding the base64 data, I was able to determine that the bomb was to be placed and detonated at the Alamo on October 4th.



I successfully located the name and phone number hidden within the file slack.

LIMITATIONS/CONCLUSION

I successfully found the information hidden within the file slack of the image files on the thumb drive.

REFERENCES

"Base64 Decode and Encode - Online." base64decode.org, 2024. https://www.base64decode.org/.

I used this website to decode the Base64 encrypted data.