****

**Jackson Harper, Anthony Karlin, Frederic Stresau, Quy Pham, Jacob Miller**

**Digital Forensics**

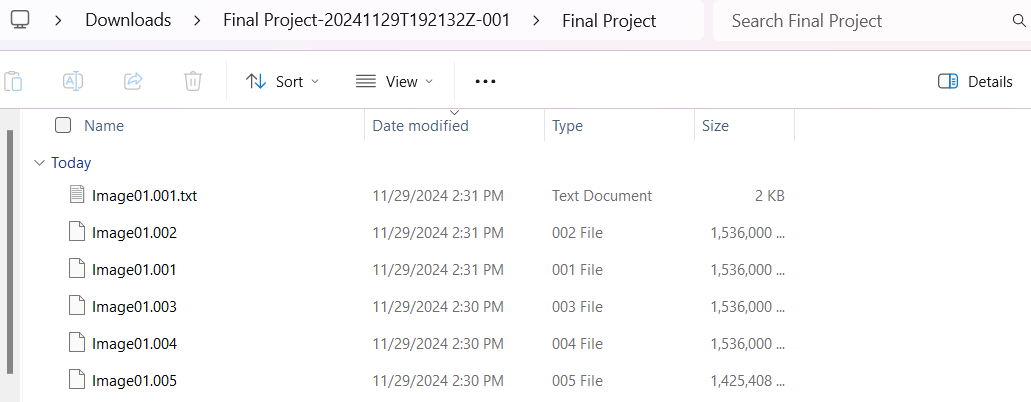
**Professor Ujan Mukhopadhyay**

**Final Project**

**12/02/2024**

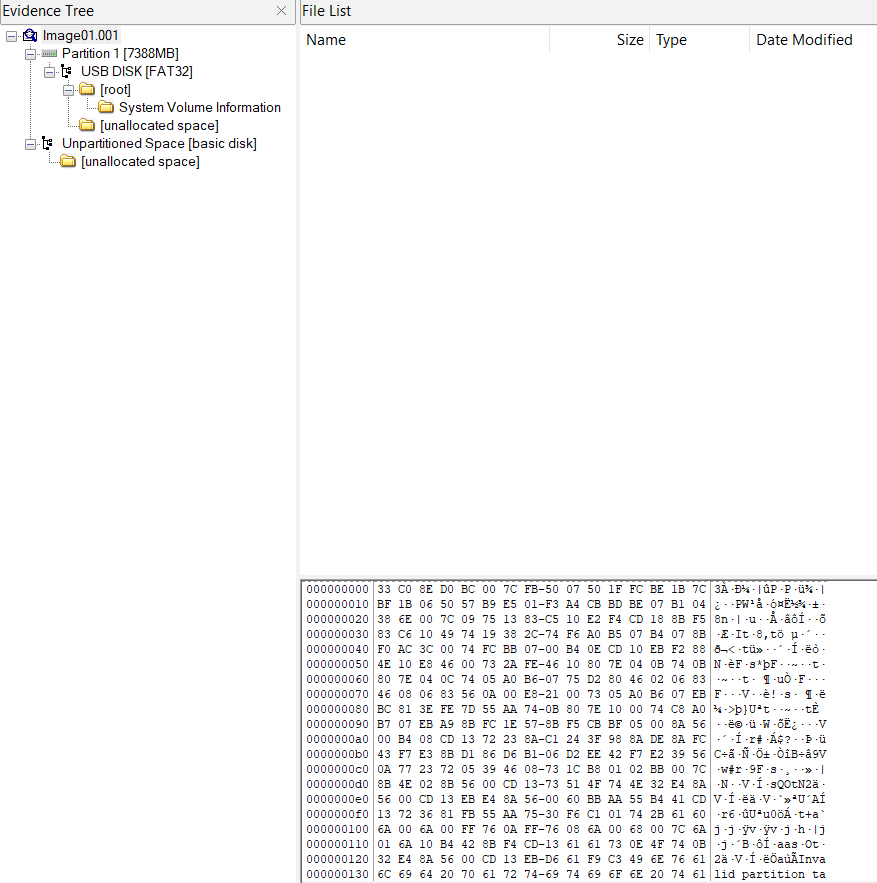
***Acquisition of the Device / Device Specifications***

Frederic Stresau received the flash drive from professor Ujan on Friday, November 8th, it is blue and red with a faded Superman decal and requires you to pull back the blue plastic to access the USB. Its serial number is listed as 067606A64090. The device is formatted in a FAT32 file format, which is to be expected as it is the standard for smaller storage devices like USB flash drive and memory cards. Once we received the drive, we created an image of it using the digital forensics software FTK Imager, the partitioned images of the drive are shown below.

****

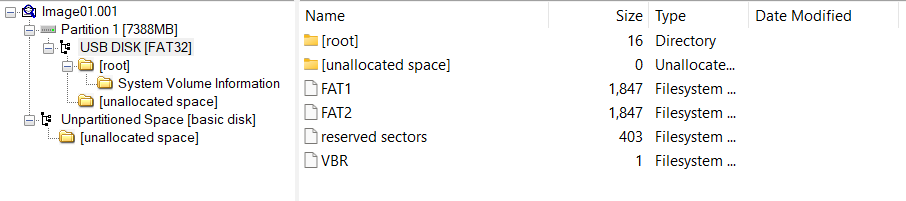
**Figure 1: The initial Image partitions of the USB drive**

We will analyze the image using FTK imager because this tool will allow us to view file structures and recover hidden or deleted files. The image file ‘Image01.001’ was part of a split image set (.001 to .005) and FTK imager is able to combine these files automatically. This tool will also allow us to view allocated and unallocated space.

**

**Figure 2 : The first image partition and subfolders shown in FTK Imager**

***Find all the files - hidden, deleted, encrypted, and logs***

****

**Figure 3: Image Partition 1 (USB DISK[FAT32]**

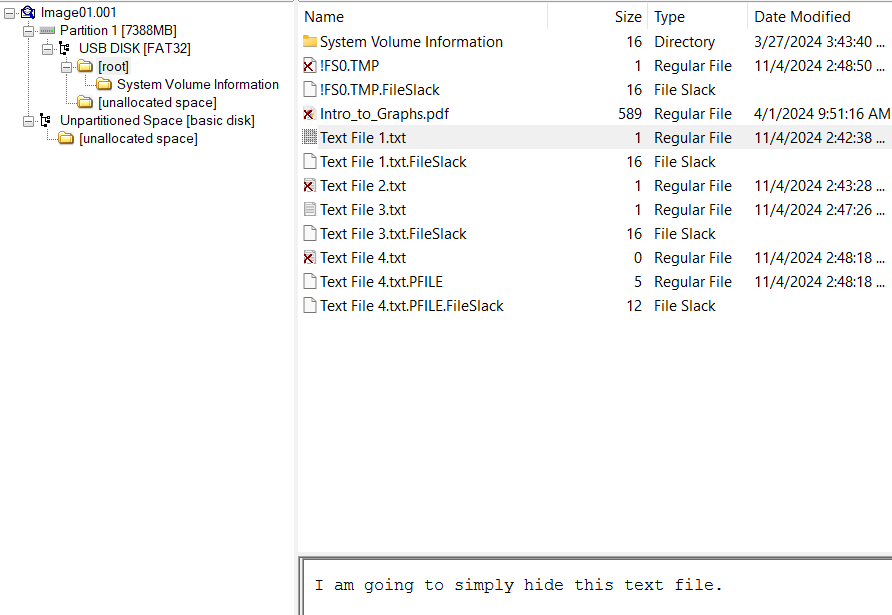
**fig. 1
**

**Figure 4: Image Partition 1 (root)**

When the image was created and viewed in imaging software we were able to see that there were previously 4 different text files on the hard drive, as shown above. These text files are text file 1, text file 2, text file 3, and text file 4, some of which seem to have corresponding files associated with them.

When analyzing the image we can see there are some files that have been deleted and have an ‘x’ over the file icon. For some of these deleted files we were able to view the plaintext and hex contents of the file. There were some deleted files that appeared to have no remaining contents when attempting to view the plaintext and hex contents of the file. We were able to view the contents of the files that were not yet deleted.

***Text File 1***

****

**Figure 5: Text File 1 contents**

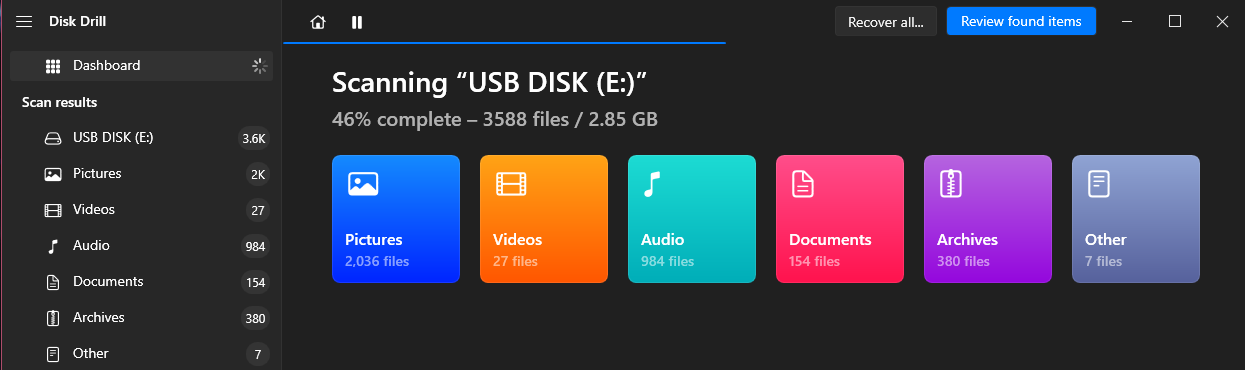
As you can see above the file was just hidden and when using FTK Imager, we are able to access it. The contents “I am going to simply hide this text file” were discovered and shown above.

***Text File 2***

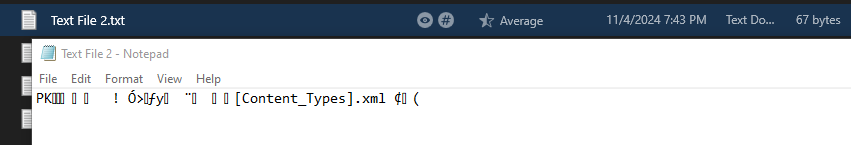
****

**Figure 6: Text File 2 shown as deleted in FTK Imager**

When analyzing file 2 we found that it seemed to have been deleted. In order to recover it we used a software named Disk Drill, which was able to recover old and deleted files from the hard drive.

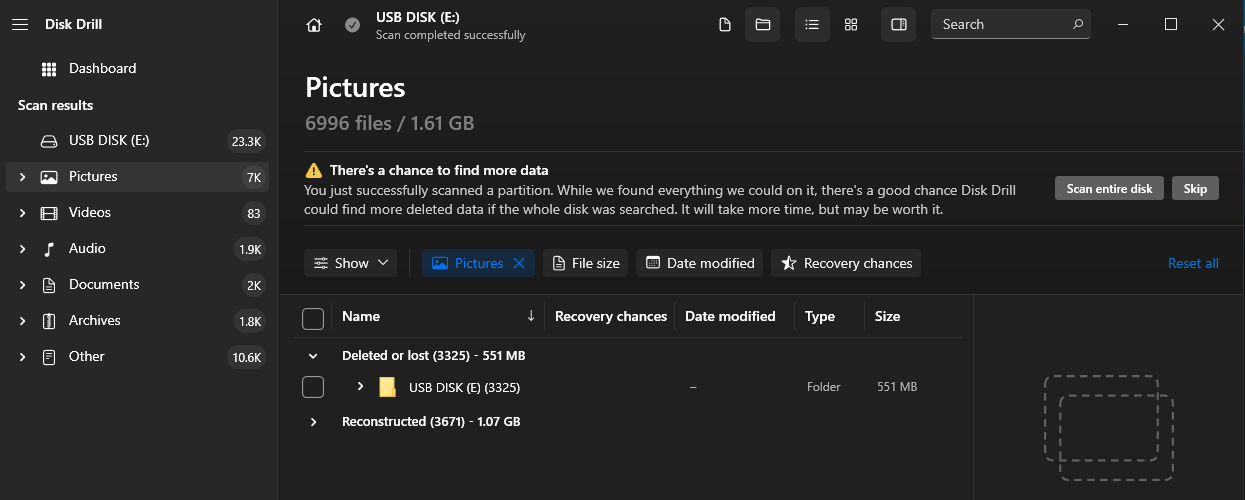
****

**Figure 7: Disk Drill software scanning the flashdrive**

****

**Figure 8: Text file 2 contents remnants**

When the recovery process was complete, we were able to access the previously deleted text file 2, however, it appears that when the data was deleted parts of the file were irreparably damaged. This is because when a file is deleted from a flash drive, the contents in the memory of the drive are still existing in that location, but the drive no longer protects that segment of the memory. This was the case for the text from the recovered text file 2, as can be seen above. This file was more than likely referencing an .xml file, as shown by the trailing text that was left over. It can be assumed that the text before it was possibly overwritten by the system once the file was deleted.

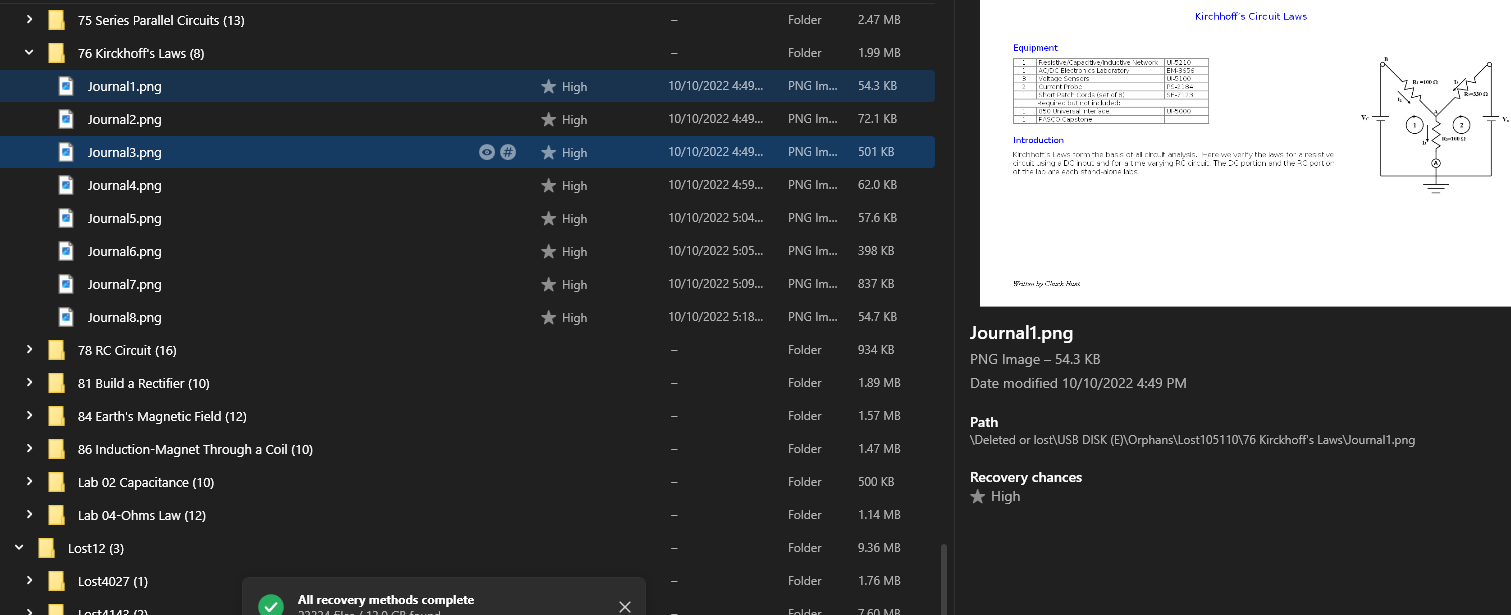


**Figure 9: Disk Drill discovering more deleted/hidden files.**

However, when looking deeper into the results of the recovery software, we were able to find that 23.3K files were able to be recovered. These files were mostly PII, some of which included homework files, family photos, home movies, and even Minecraft mod packs all relating back to a current/former student at Florida Poly, Timothy Jefferson Freeman. Blurred examples can be seen below.



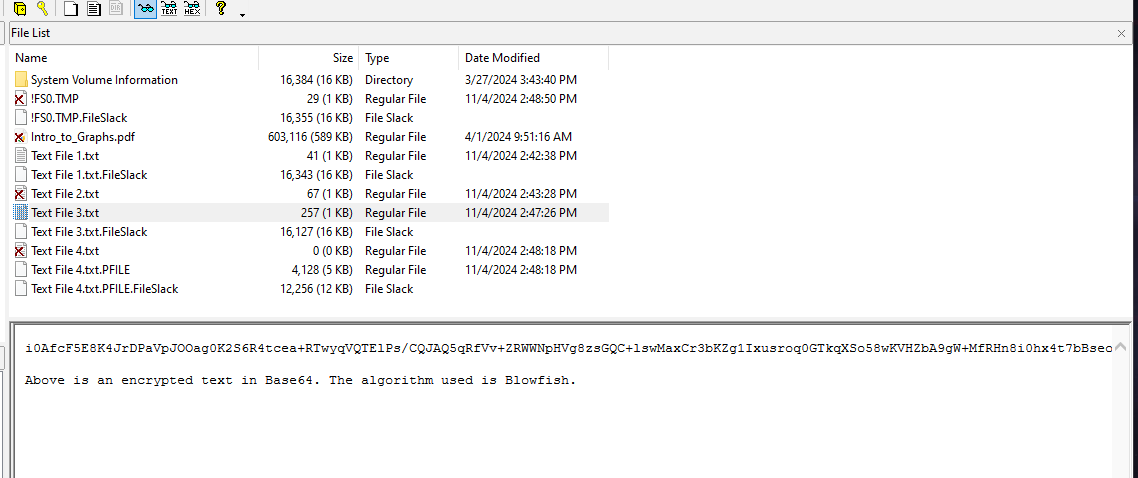
**Figure 10: PII photo found on drive (Blurred for privacy of the student)**



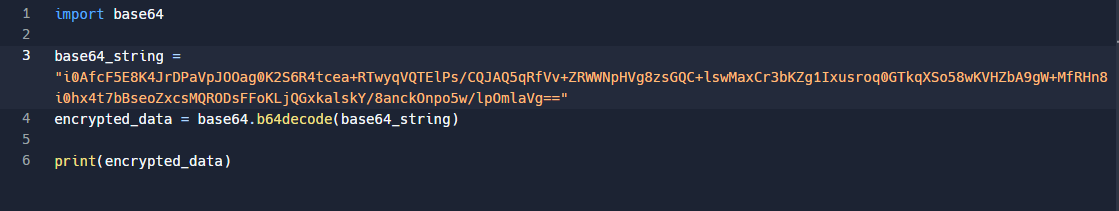
**Figure 11: Multiple Homework Journal files from when the student took Physics 2**

***Text File 3***

Text file 3 was also hidden similarly to text file 1, but this text file listed a random string of characters followed by a description stating that it was an encrypted text in Base64, using the algorithm Blowfish. This is shown in the figure below.

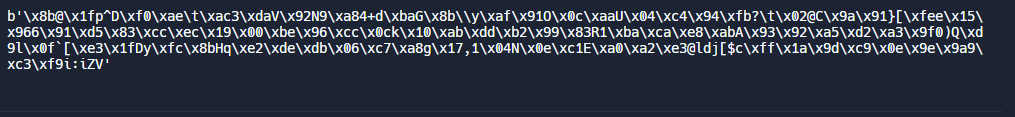
****

**Figure 12: Text File 3 Contents**

****

**Figure 13: Program that decodes base64**

This code completes a Base64 decoding process that gives an output “encrypted\_data” which is the raw ciphertext that is encrypted with the Blowfish algorithm.

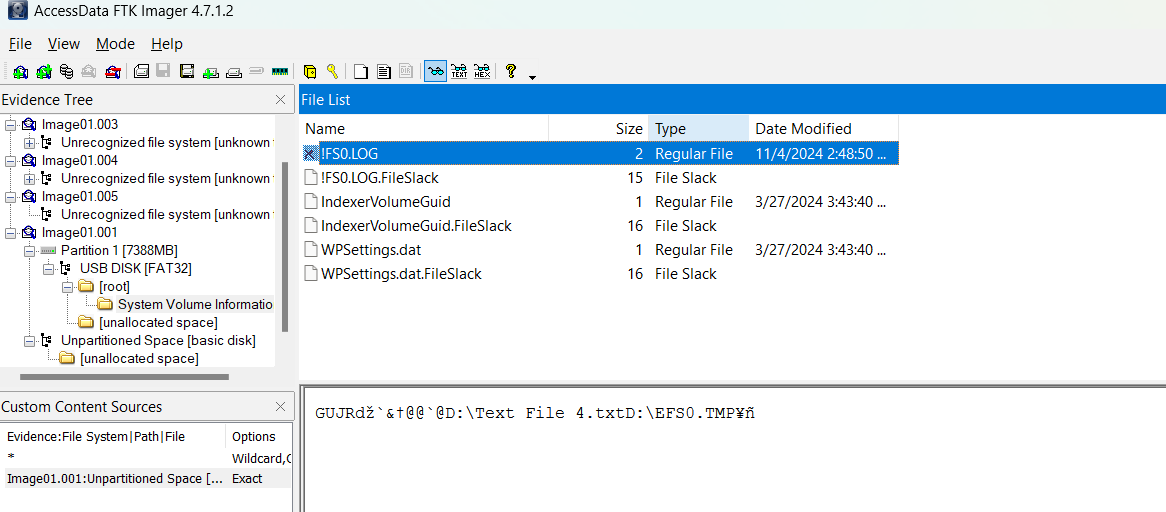
****

This is the raw ciphertext that is encrypted with the Blowfish algorithm. To continue the decryption, We will have to find the secret key that was used to encrypt the data. This secret key was nowhere to be found so to find the hidden message is impossible without it. Also, we do not know what mode of operation was done, this makes it impossible to decrypt the message.

**File 4**

lkasdklf;jas;lkdfjaklsdjflk;ajsdlk;fjsd

Figure : Text file 4 properties showing Ujan as the file owner and that it is encrypted.

****

Reference to text file 4 in system volume information

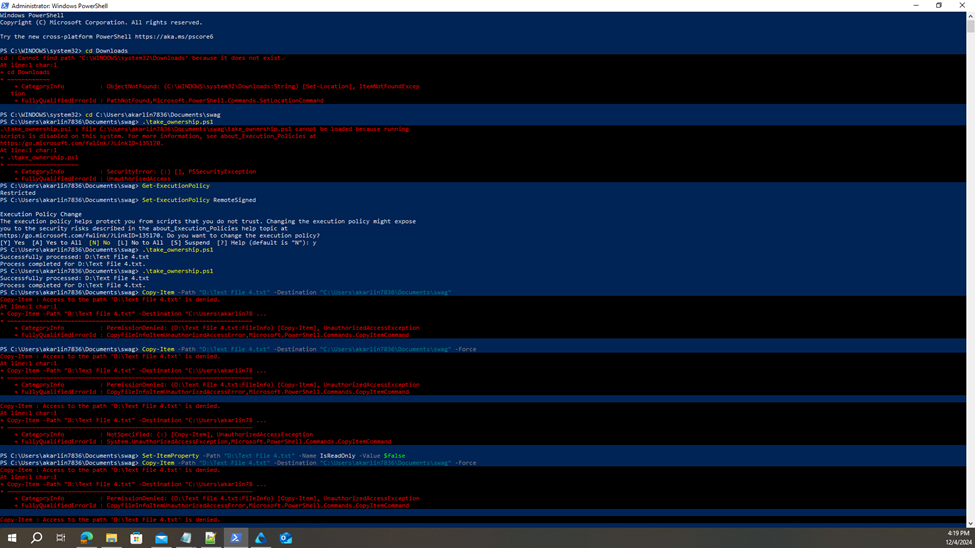
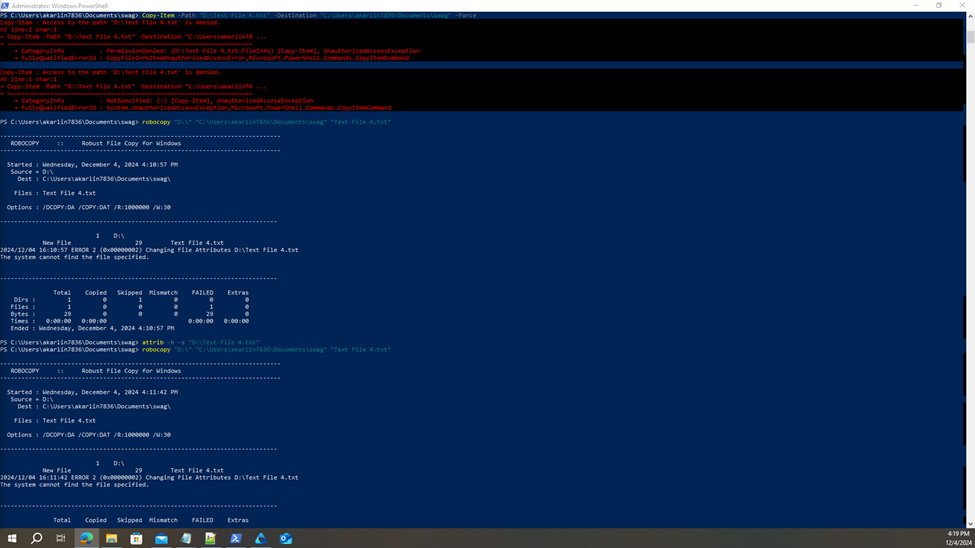
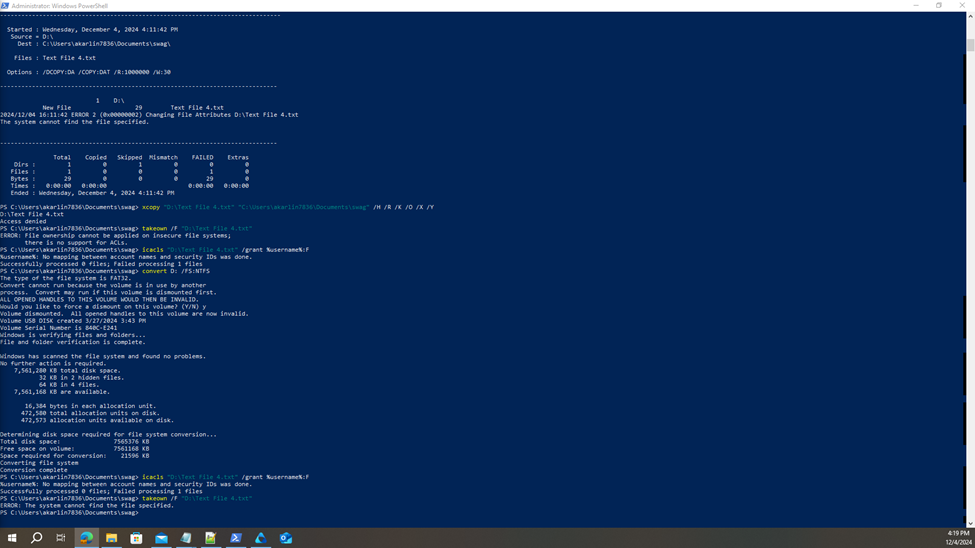
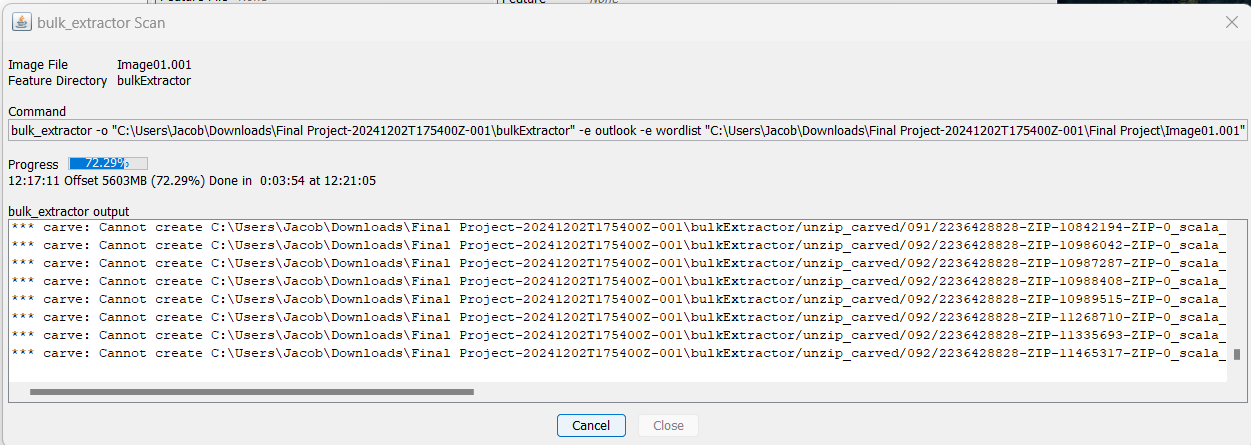
**  
  
**(Above 3 images all 1 figure) Figure : Powershell commands that were ran to try and take ownership of the file. It was only successful in converting the flash drive to NTFS (in a proper setup this would be done with the image, not the actual drive) and then copying the file.

  
Figure : Text File 4 after the flash drive was converted to NTFS, shows the new extension of PFILE

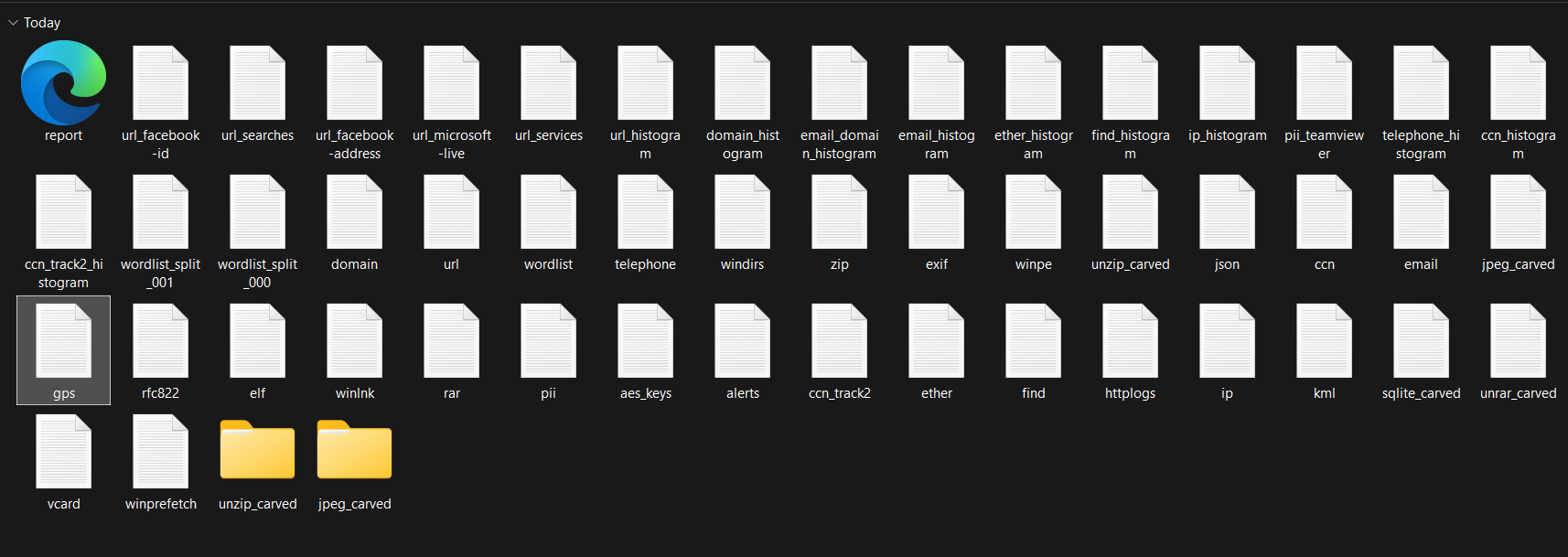
***Find out identities of all computers the device has been attached to.***

Being able to determine the identities of all the different computers the device has been attached to can be very difficult to do in forensics, especially without any knowledge of what computers it may have been attached to. However, we can view the System volume information to determine and infer information about the different connected hosts. Already we can tell that the flash drive is formatted and was accessed by Windows Operating System Host as the USB drive features the filesystem metadata folder System Volume Information, which is exclusive to windows hosts.

In order to gain a deeper insight into what locations the hosts have been connected to the HDD, the software Bulk Extractor was used, which explores file metadata and repairs any information it can find and reports it.

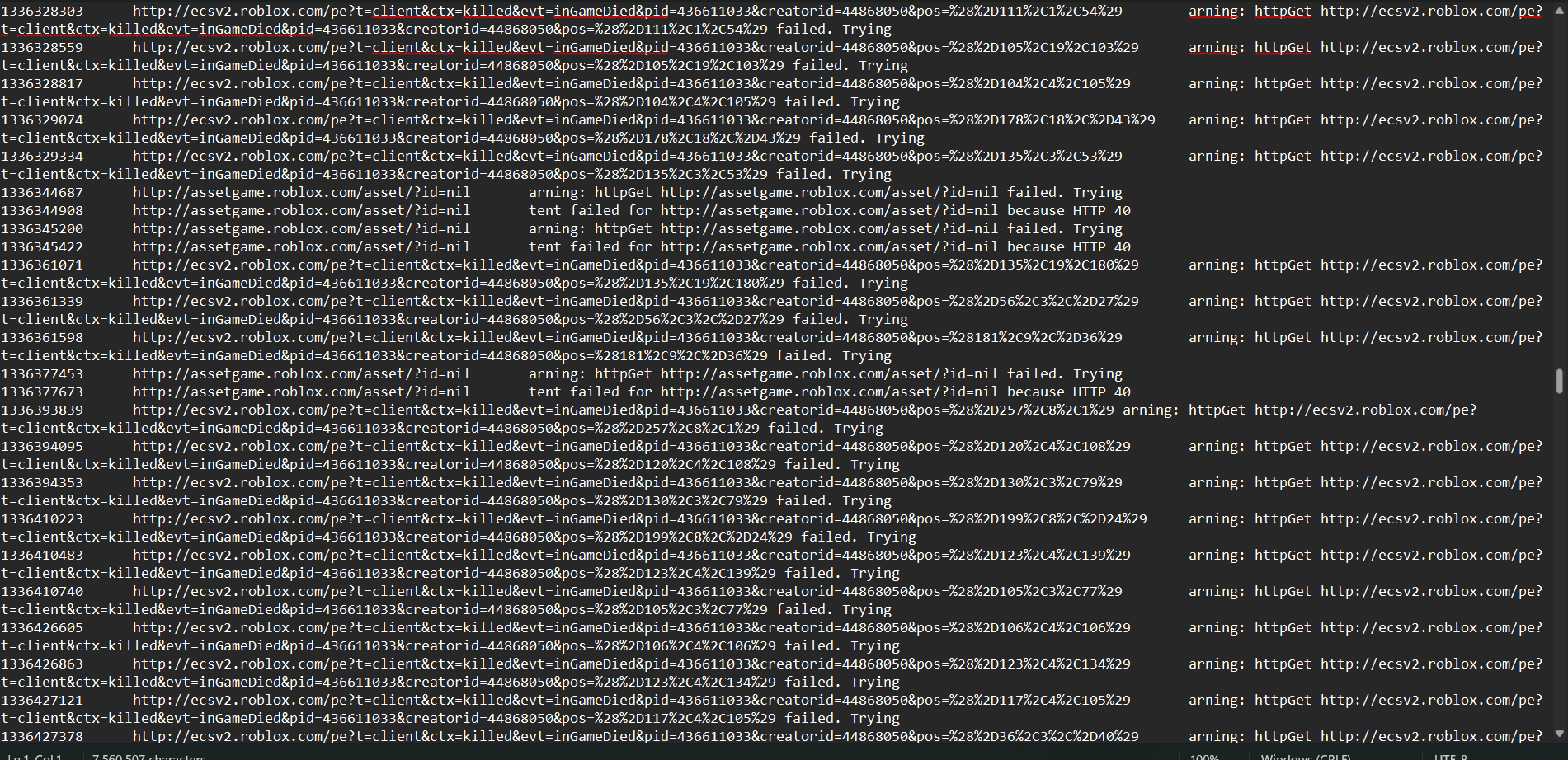
****

**Figure : Bulk Extractor software running a scan on the image**

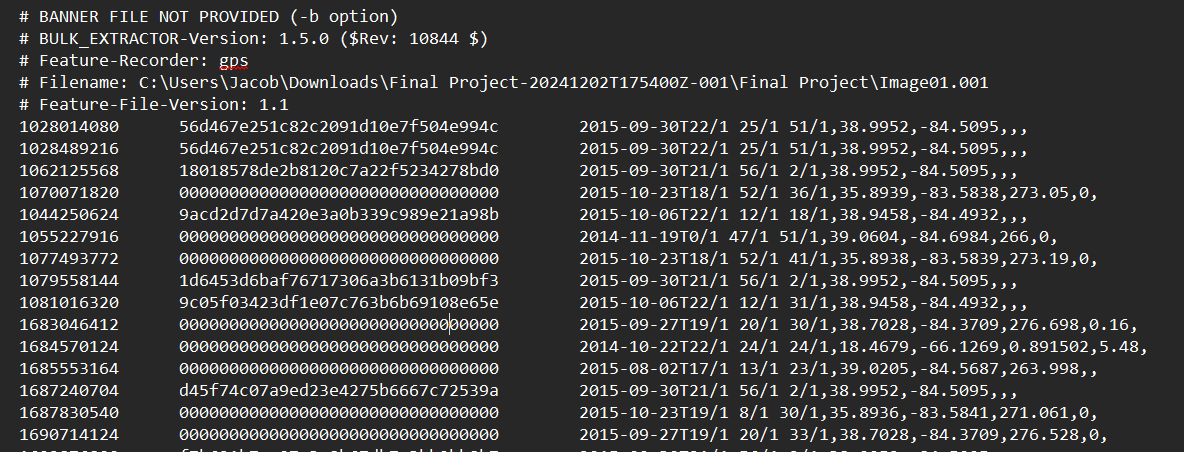
****

**Figure : Final Report folder from bulk extractor scan**

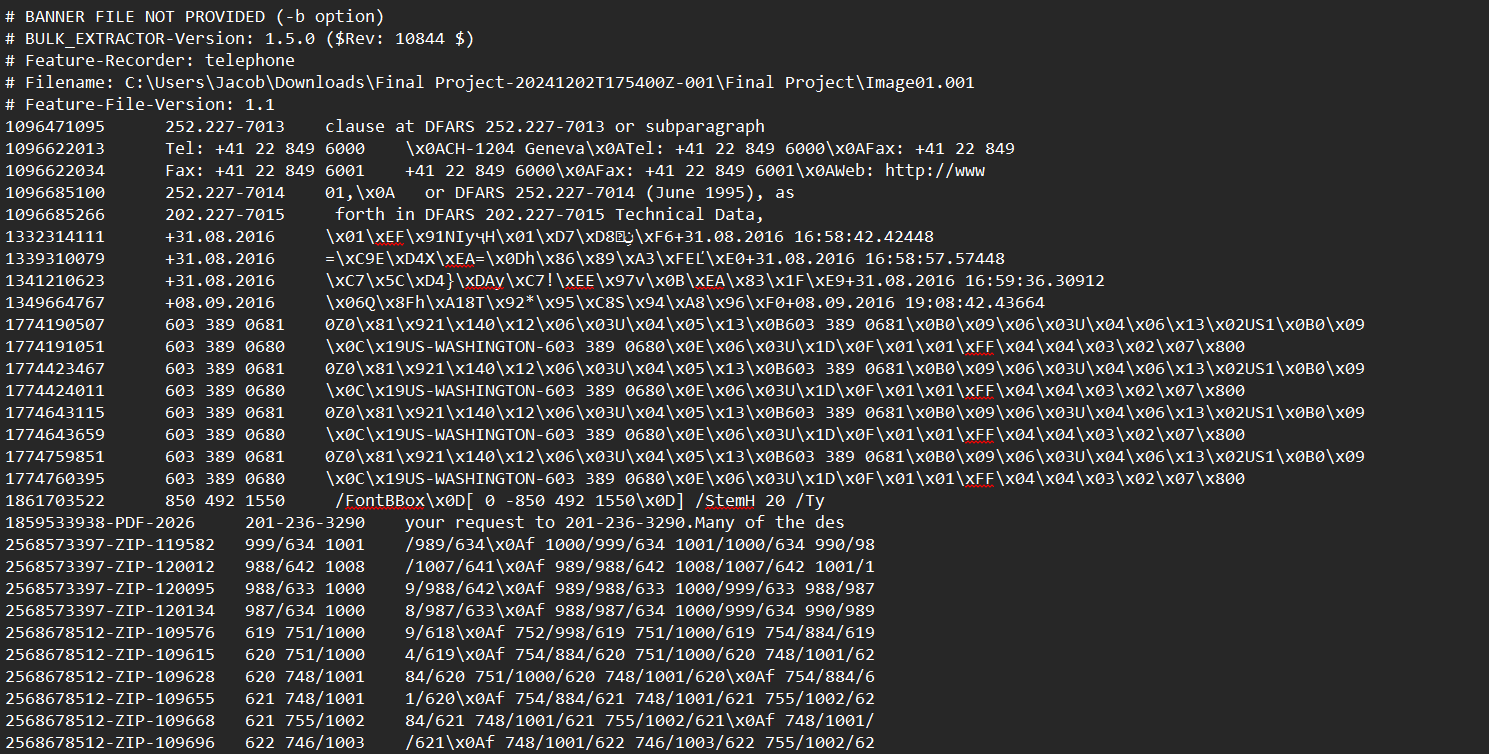
As shown above, there was a massive report generated by bulk extractor, with a majority of the data dating all the way back to 2014. This includes carved jpeg images, as well as references to other human readable data in the meta data including email addresses, phone numbers, windows directories/when files were opened, geotagged locations where the device was used, Credit card numbers, and a whole lot of other information. I will compile some examples below of the data found.



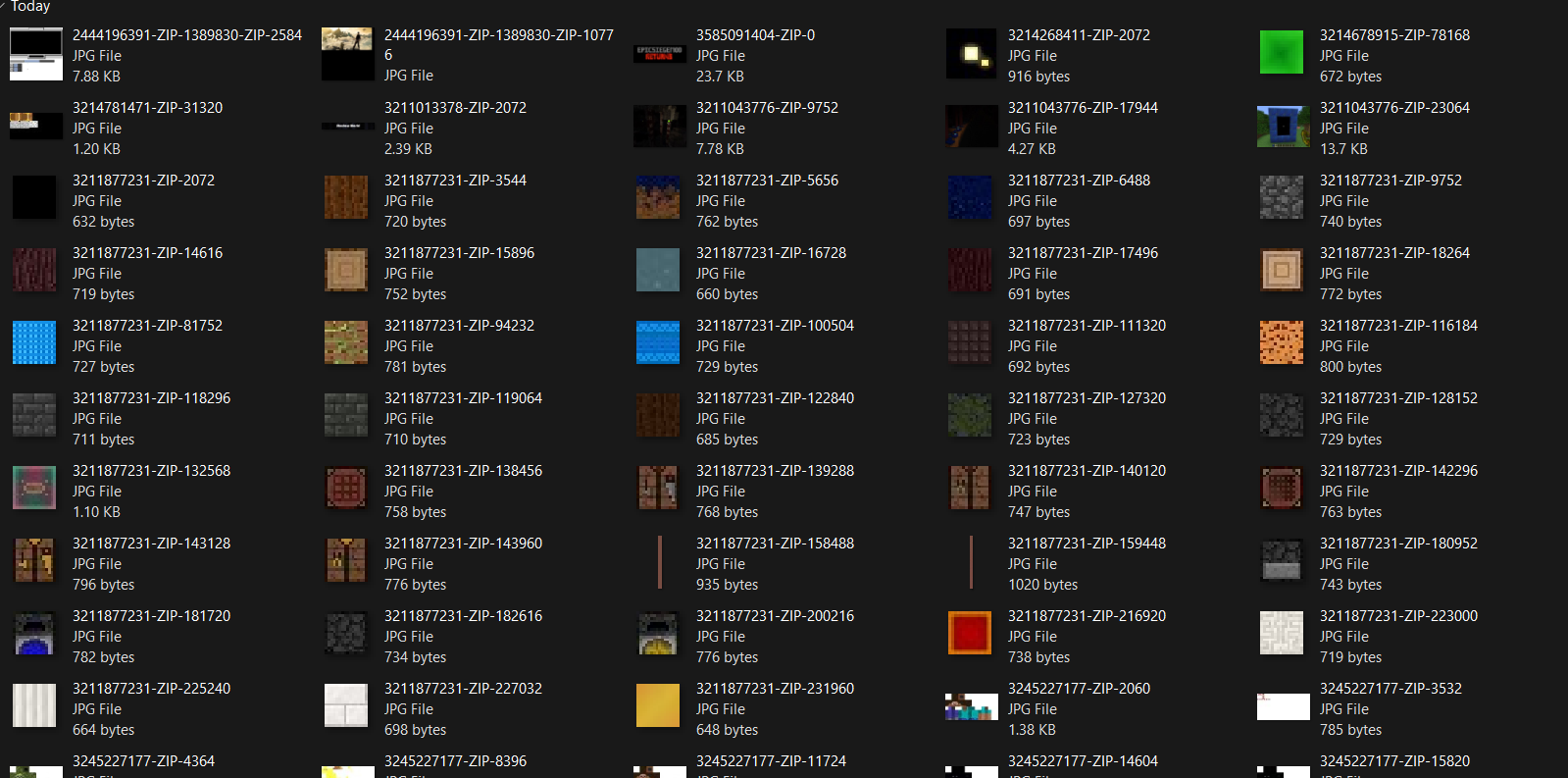
**Figure : Visited URLs and associated memory found with bulk extractor**

****

**Figure : Recorded Longitude and Latitude and associated memory locations found with bulk extractor**

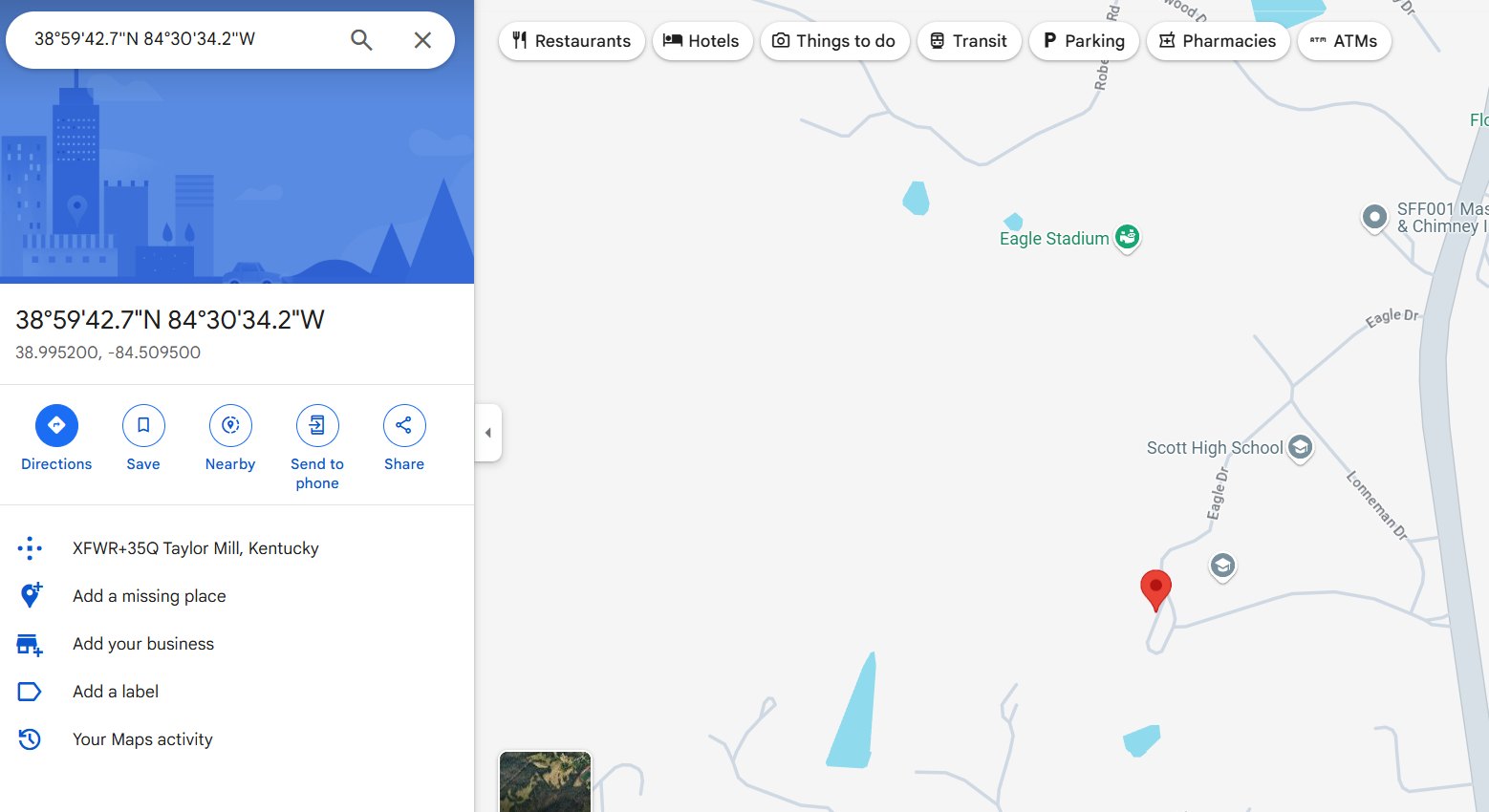
****

**Figure : Telephone numbers and associated memory locations found with bulk extractor**

****

**Figure : Carved JPEGs found with bulk extractor**

Using the geolocation tags in the gps section of the report, I was able to use the longitude and latitude values for where the host connected from. I found the most common accessed locations were outside of Cincinnati, Ohio, specifically at the middle school and high school in the area. I also found other locations like Right outside Pennsylvania where it was accessed. This was the closest I was able to get in terms of finding the identities of the computers the USB had been connected to.



**Figure : Location of one of the coordinates found with bulk extractor**

***Conclusion***

The digital forensics investigation on the HDD provided valuable information on the process of recovering and analyzing evidence. During the investigation, we used tools such as FTK imager, Disk Drill, and Bulk Extractor to analyze the image. With these tools we were able to recover hidden and deleted files and analyze any data that remained in these files. We were not able to fully recover some of the files due to overwriting, however, we were able to identify and recover information such as personal files and encrypted files.

This investigation showed how it is possible to recover hidden and deleted data using a variety of forensics tools. Furthermore, it also demonstrated the challenges that can be faced when trying to recover data, such as incomplete recoveries and encrypted content. This investigation process revealed how important it is to have a variety of recovery methods in order to have a successful investigation.