**ITIS 5250**

**Pooja Haridasyam**

**Lab 2**

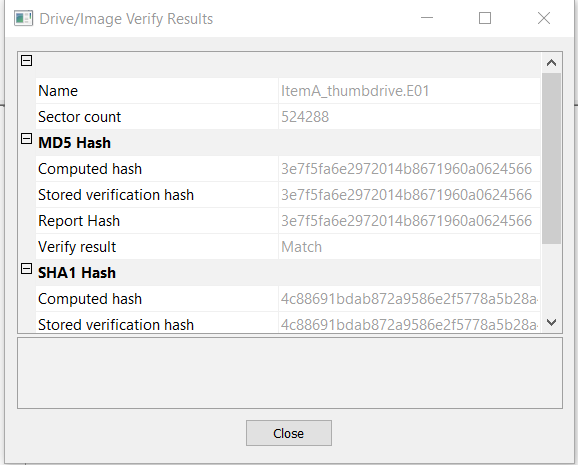
**03/03/2023**

**Overview**

In this laboratory, I'll analyze the Forensic Image called "ItemA\_thumbdrive.E01" which was provided to me by Officer Johns. I'll utilize the FTK (Forensic Toolkit) to conduct multiple procedures and investigations while ensuring its Hash values match. The main goal of this examination is to determine if the individual who owns the thumb drive was implicated in the Woodward theft.

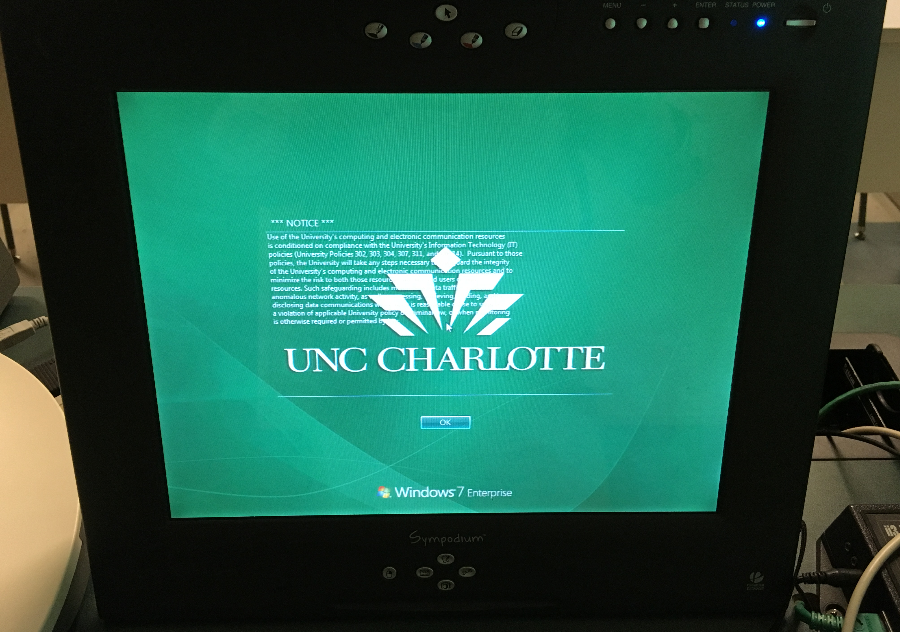
**Forensic Acquisition & Exam Preparation**

After downloading the image files from Canvas, I computed and confirmed their Hash values. The software tools employed to extract and access the data from the image are FTK Imager 4.1.1.1 and Forensic Toolkit 6.3. The MD5 Hash of both images is provided below:



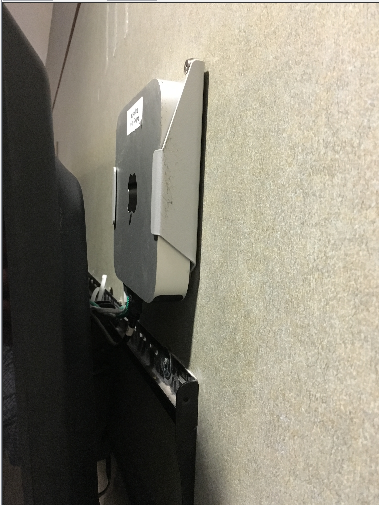
**Findings and Report (Forensic Analysis):**

Upon commencing the analysis of the image, I reviewed the files within and detected several photographs that were taken inside Woodward. These picture files can be found in the root directory of the thumb drive.

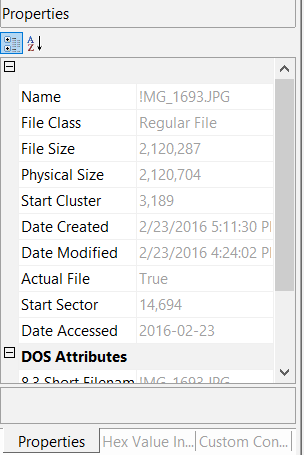


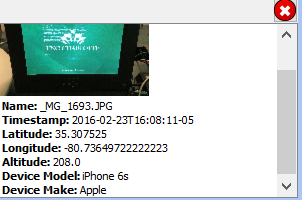


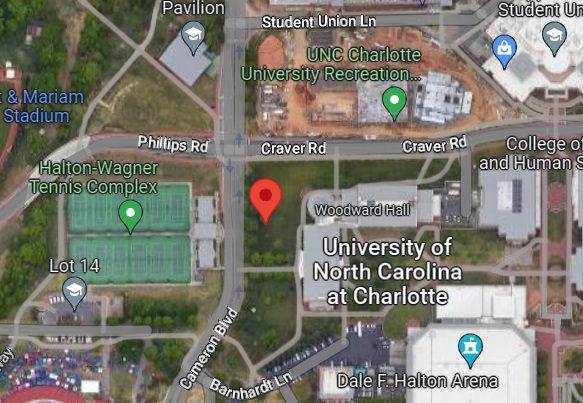


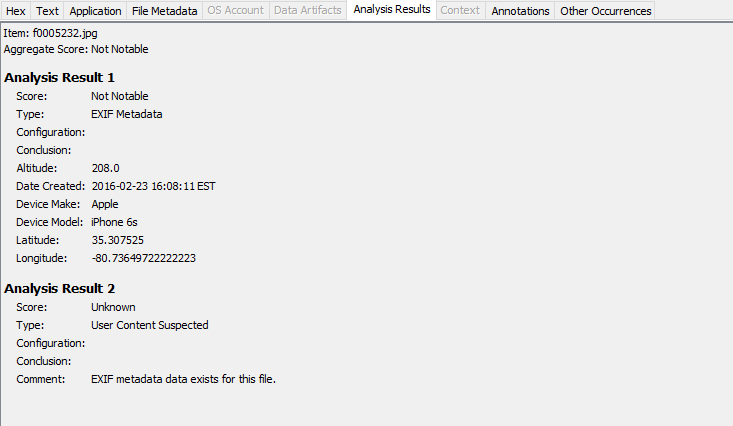


**Properties of image 1:**





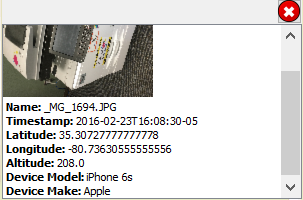


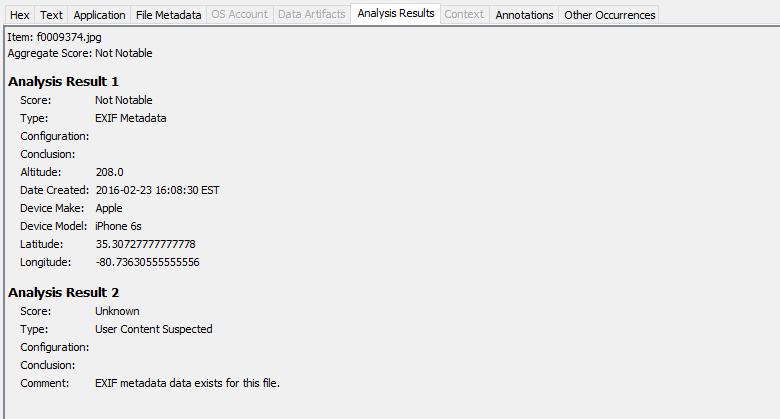


**Properties of image 2:**

**Image 2:**

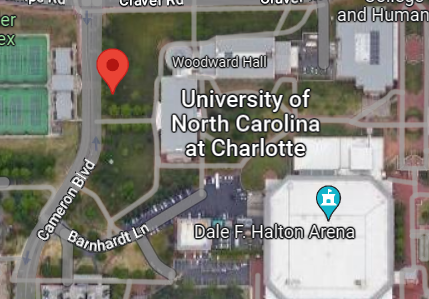




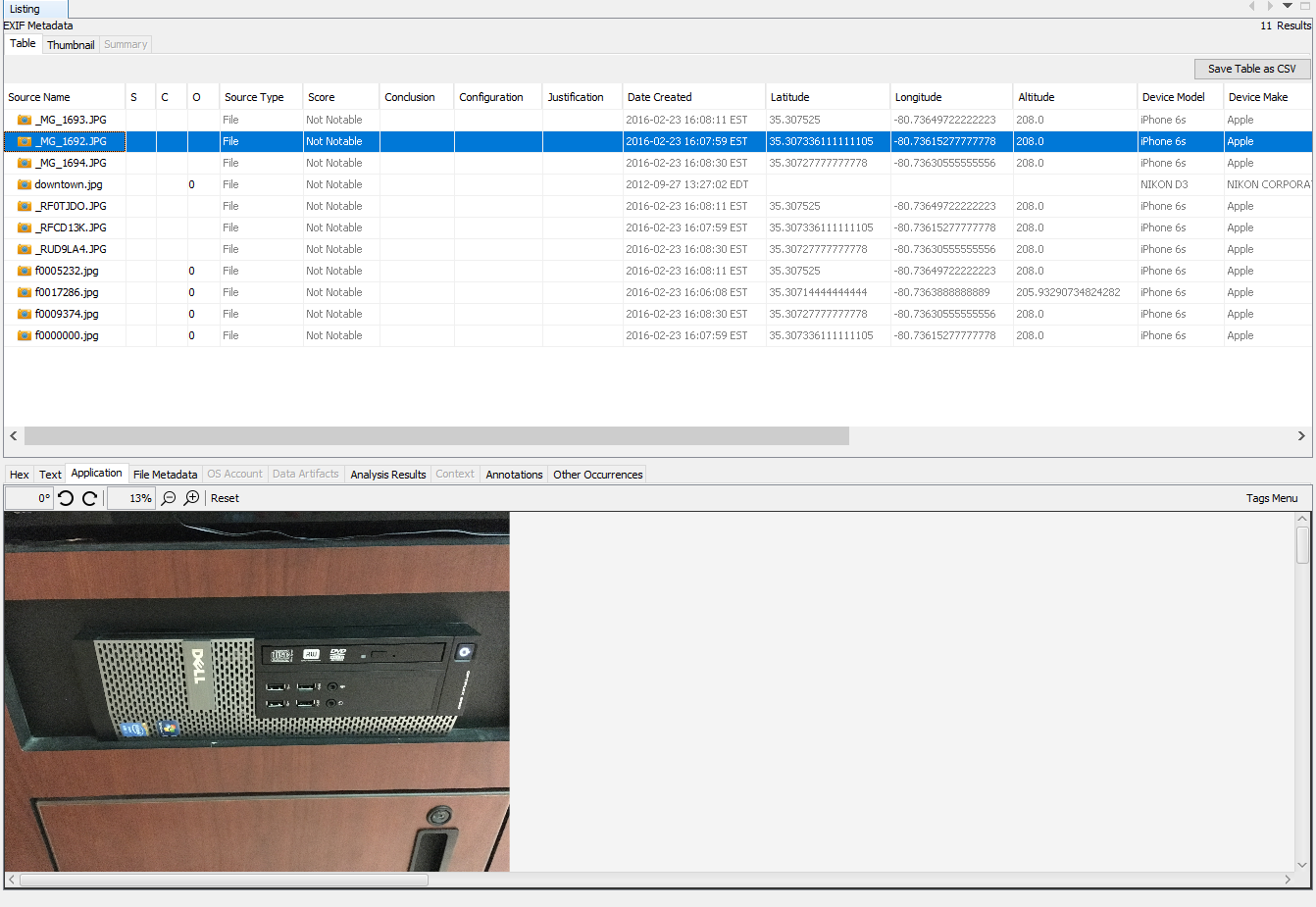


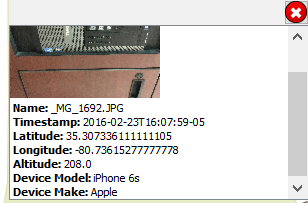
|  |  |
| --- | --- |
| Name: | /img\_ItemA\_thumbdrive.E01/vol\_vol2/$CarvedFiles/1/f0009374.jpg |
| Type: | Carved |

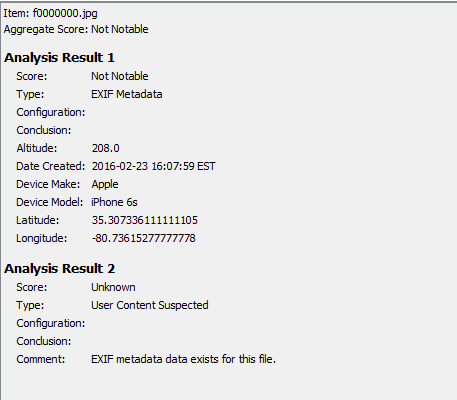
|  |  |  |  |
| --- | --- | --- | --- |
| Date Created: | 2016-02-23 16:08:30 EST |  |  |
|  |  |  |  |
|  |  |  |  |
| Device Make: | Apple |  |  |
| Device Model: | iPhone 6s |  |  |
| Latitude: | 35.30727777777778 |  |  |
| Longitude: | -80.73630555555556 |  |  |

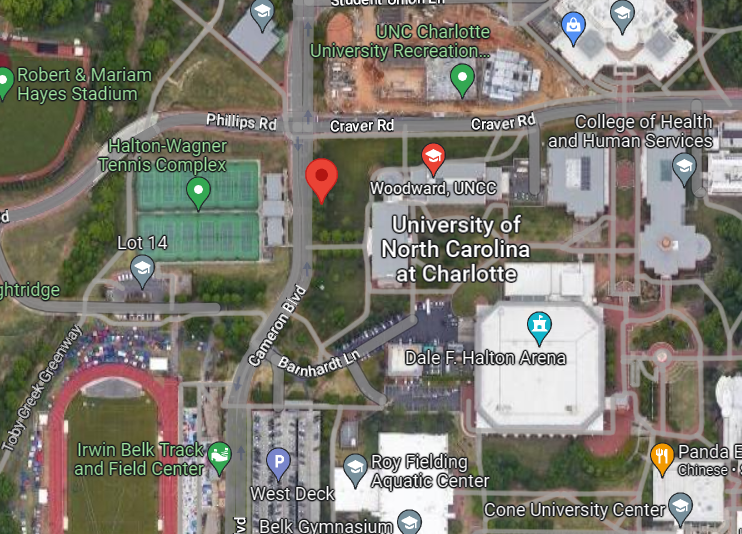


**Properties of image 3:**

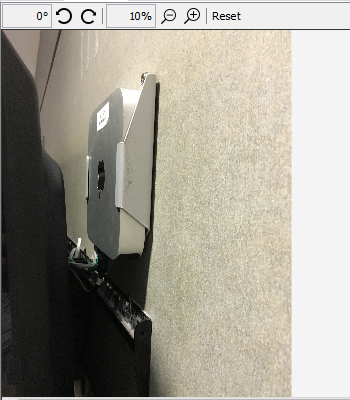


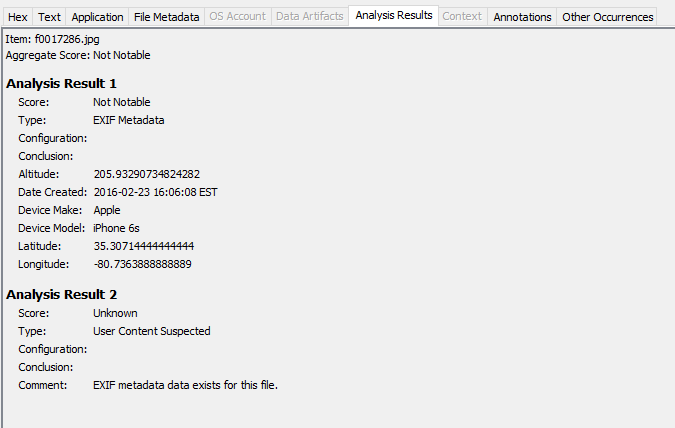


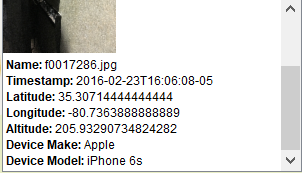


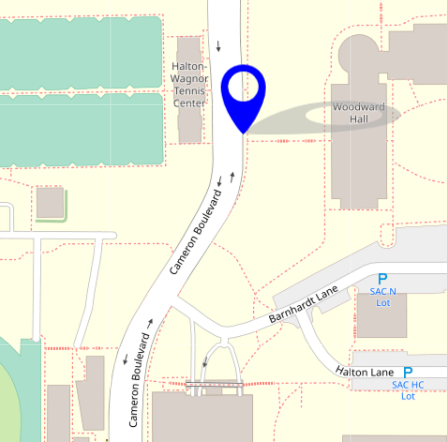


**Image 4:**









**Conclusion:**

I conducted an examination on the thumb drive image given to me by Officer Johns, ensuring its verification and examination. During my investigation, I discovered several picture files that exhibited their origin to be inside Woodward. Additionally, through Data carving, I successfully retrieved a deleted image that established a direct connection between the suspect and Apple devices from Woodward. My findings are summarized below:

**Image 1** - A photograph captured from an Apple iPhone 6S within or around Woodward, on February 23rd, 2016, at 16:08:11, depicting a screen.

**Image 2** - A photograph captured from an Apple iPhone 6S within or around Woodward, on February 23rd, 2016, at 16:08:30, portraying a Copy Machine.

**Image 3** - A photograph taken from an Apple iPhone 6S within or around Woodward, on February 23rd, 2016, at 16:07:59, showcasing a CPU.

**Image 4 (Carved)** - A photograph of an Apple device/box with a label affixed to its body, taken from inside Woodward, on February 23rd, 2016, at 16:06:08, using an Apple iPhone 6S.