ITIS 4250 / 5250

Shivani Sathe

Lab # 3

18th October 2021

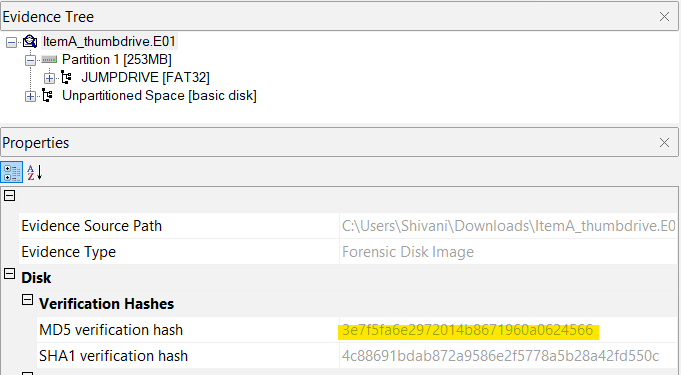
**Overview:**

On October 18, 2021, Officer Jimmy Johns of the UNCC Police Department provided me with a forensic image that was made of the subject’s thumb drive which was provided on subject’s consent. Officer Johns has determined that to further the investigation, a forensic analysis to be conducted to provide any photographs relevant to the theft of computer equipments, Apple devices in particular from University of North Carolina at Charlotte.

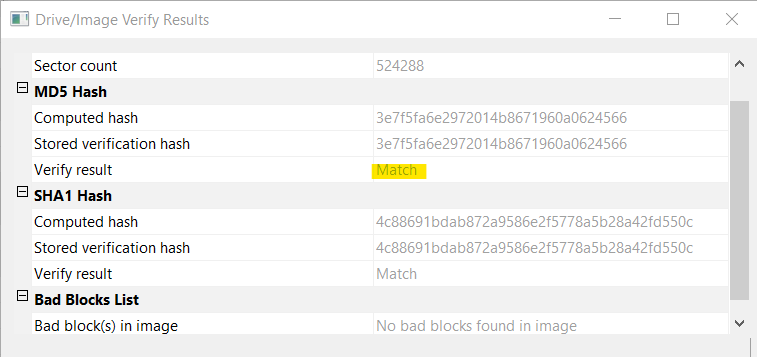
For reference, a thief has been repeatedly stealing computer equipment from classrooms and buildings at the University of North Carolina at Charlotte. Particular items stolen include Apple computers, Apple TVs, iPads and iPhones. Officer Johns along with several people noticed and pointed a shifty looking individual around Woodward Hall from where items have gone missing or reported stolen. Officer Johns stopped him on his bike and found an iPhone 6s in his pocket which he did not provide. His backpack contained several iPads, a Mac Mini with a sticker scraped off and an Apple laptop computer which Officer Johns seized later with a warrant.

**Forensic Acquisition & Exam Preparation**

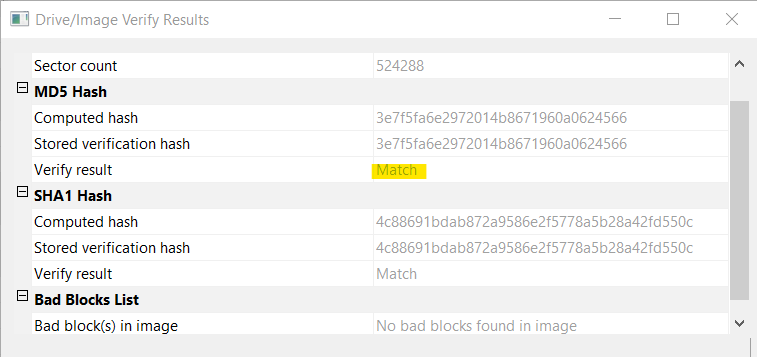
To begin the analysis, Windows 10, 64-bit system with 8GB RAM was used with. The forensic image file ItemA\_thumbdrive.E01" was downloaded from canvas - Files - Labs - Lab 3 Files. Access Data FTK Imager 4.5.0.3 was used to load the image and the MD5 hash value was verified before starting the analysis and after its completion. Later, with the help Autopsy 4.19.1 further analysis was conducted.



MD5 hash after loading image



MD5 hash before analysis



MD5 hash after analysis

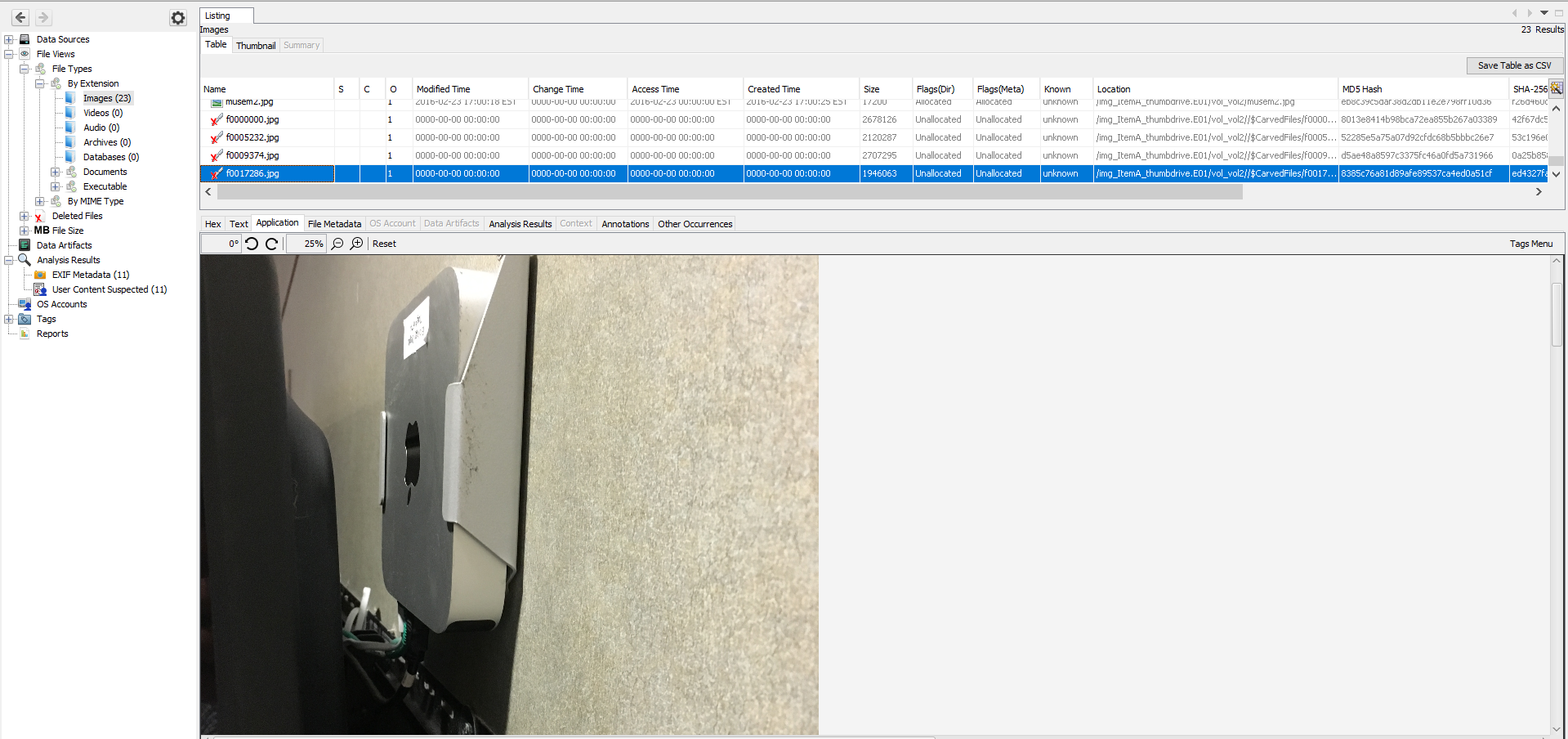
**Findings and Report (Forensic Analysis)**

Autopsy was used and a new case was created by following below steps to load the forensic image file ItemA\_thumbdrive.E01:

* Add Data Source
* Select Disk Image
* Browse Disk Image path
* Select all ingest modules
* Click on Finish

1. Photographs of Apple devices.

Once image was loaded, the files were scanned through on basis of extension types. 23 picture files were present out of which below picture of Apple device was found.

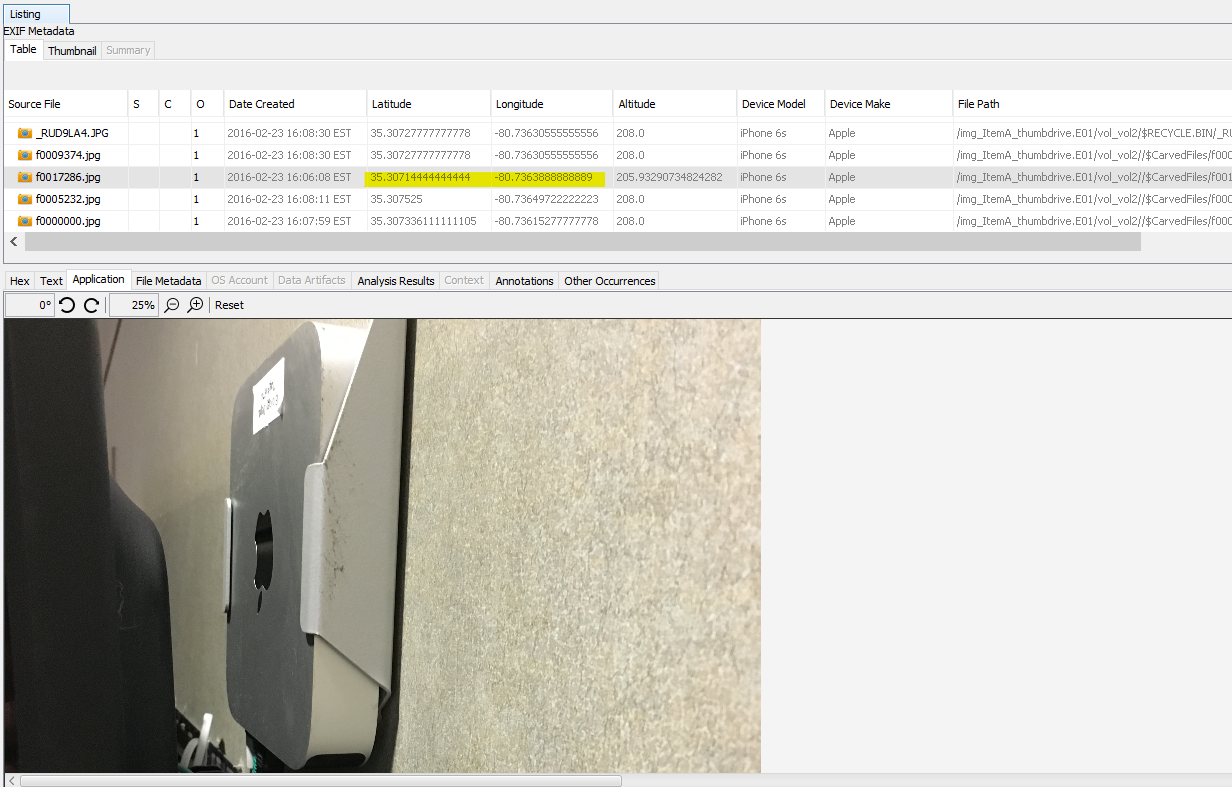


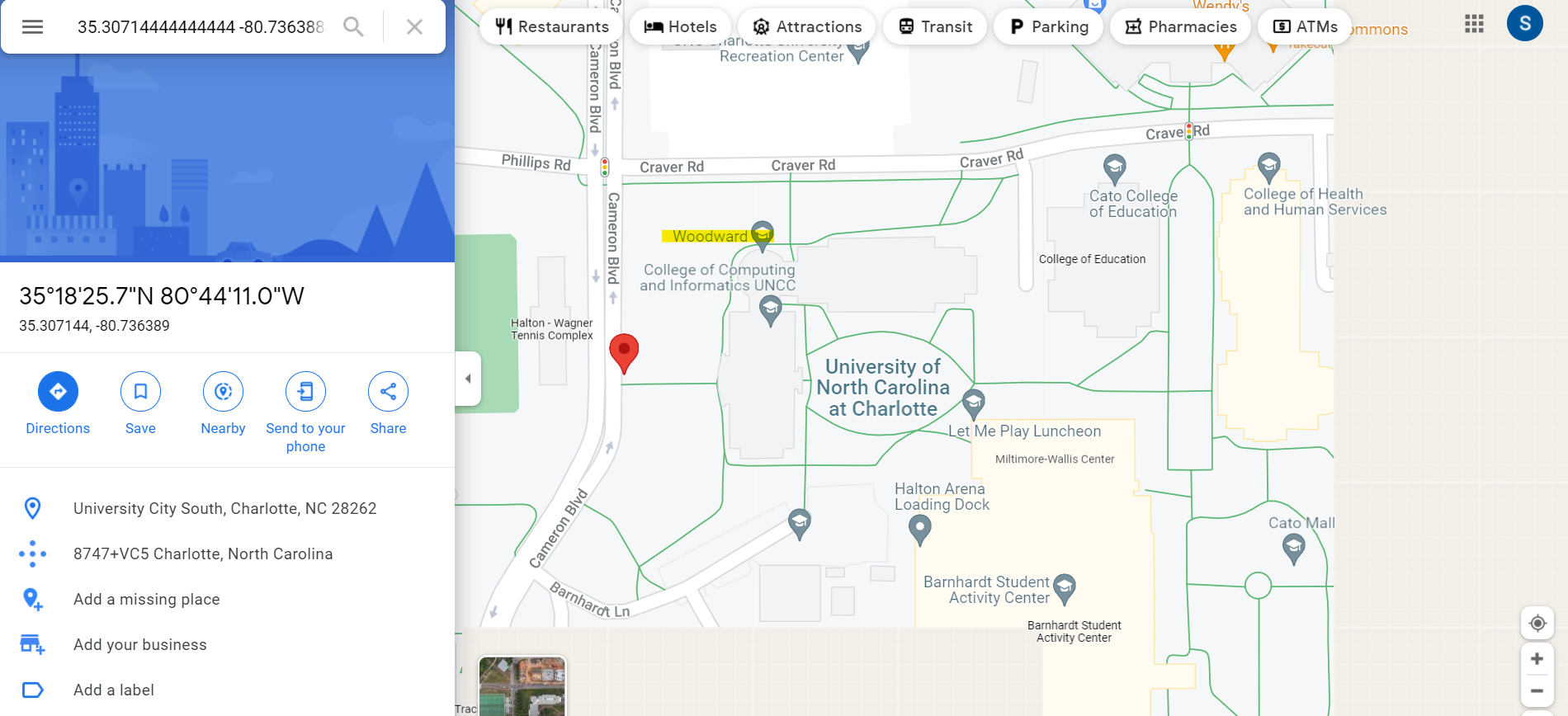
1. Location information of those devices.

The location information of the devices was found using below steps:

* Expand Analysis Results Tab
* Select Exif Metadata

The location coordinates in terms of longitude and latitude were found for the Apple device picture. Entering the coordinates on google maps, it shows the location of the picture was taken near **Woodward Hall**.



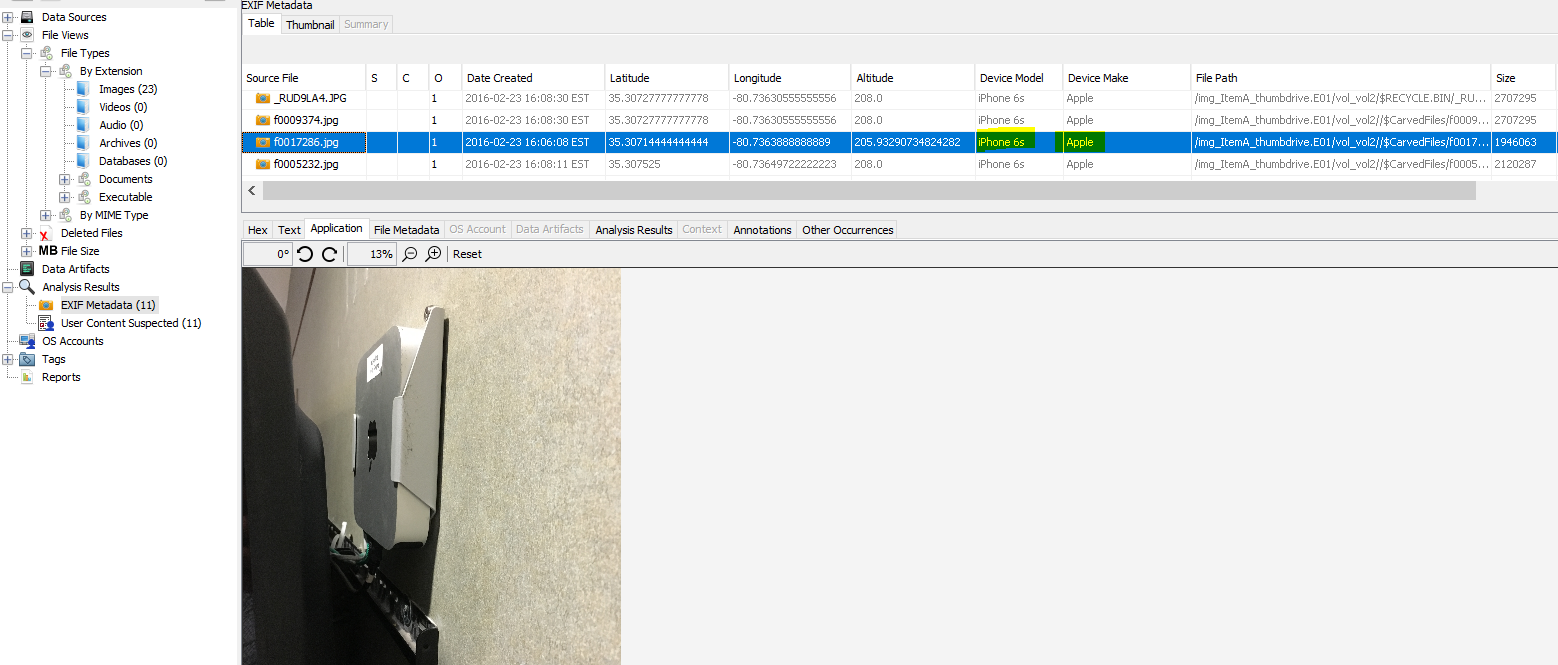


1. Make/model of the camera device used to make the photos.

Steps:

* Expand Analysis Results Tab
* Select Exif Metadata

The Make of camera device is “**Apple**” and the device model is “**iPhone 6s**”



1. Any content in the picture that might help identify the device.

Zooming into the picture of the Apple device, a sticker of “**Biology Dept, Tag#674**”

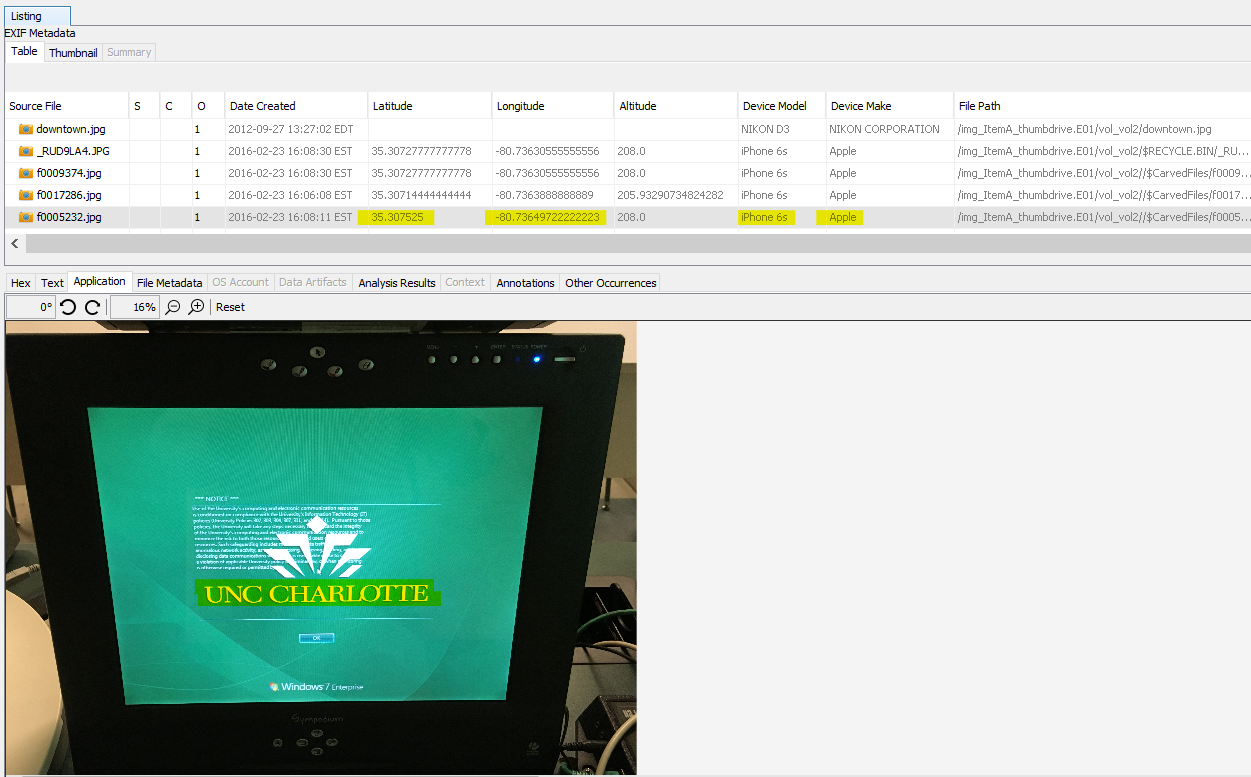
was observed which could be helpful in identifying the device.



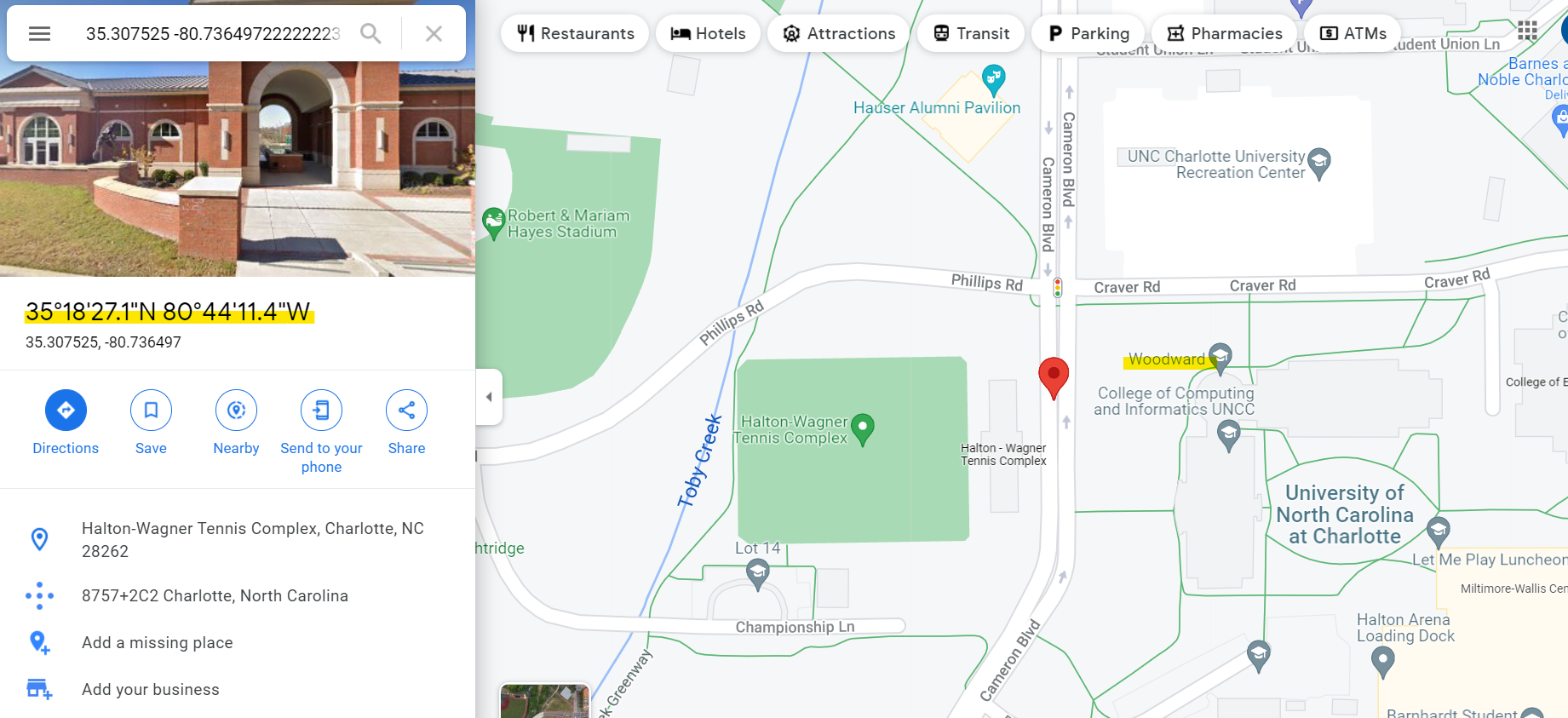
1. Any other pictures whose content might be relevant to the theft of Apple devices.

While scanning through the Files on the basis of extension types, pictures of 2 more devices which belonged to UNCC were found.

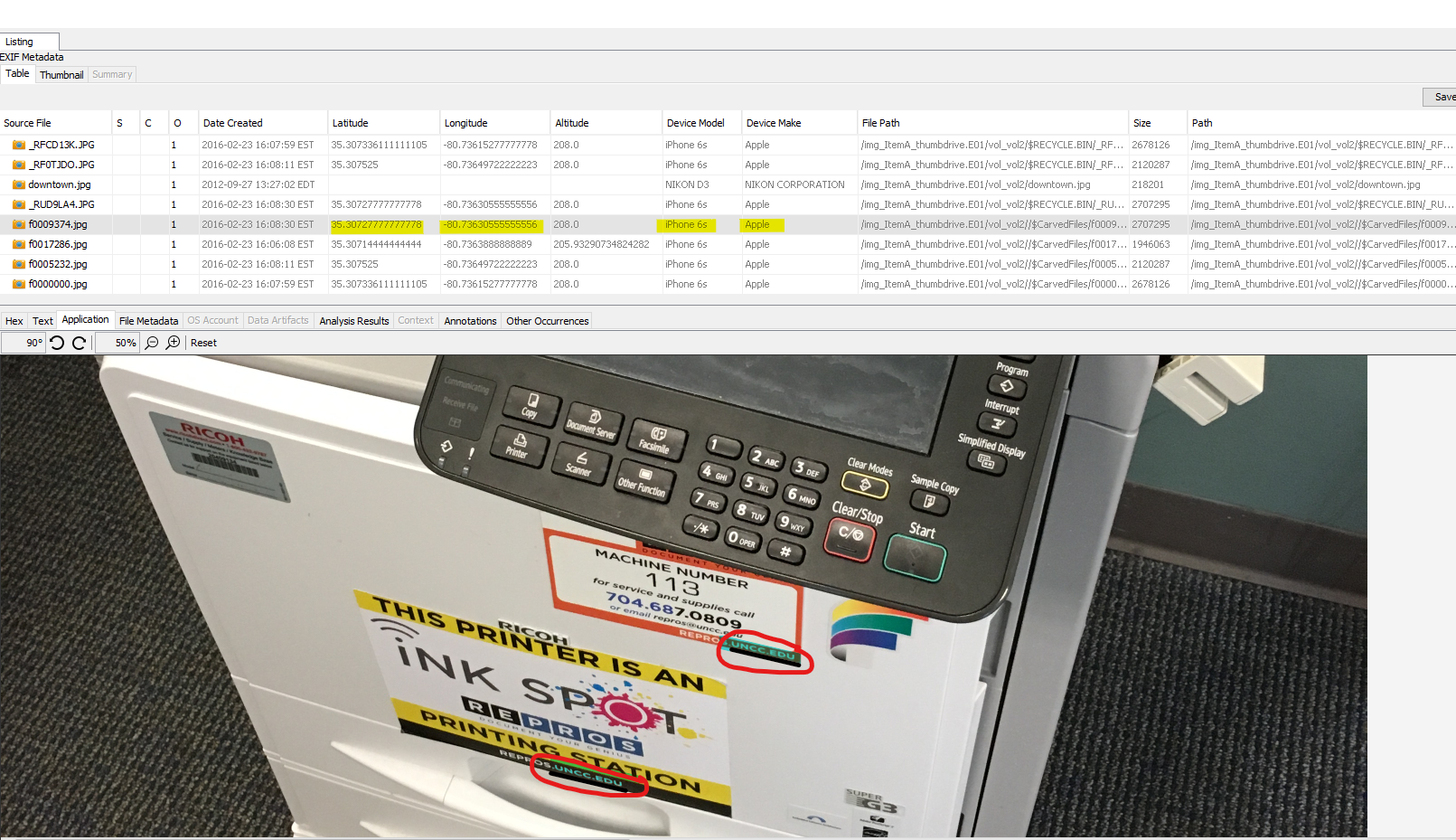
Under the Analysis Results, from Exif Metadata, the device make and model number as well as the location coordinates suggested the pictures were taken near Woodward Hall with Apple iPhone 6s device.



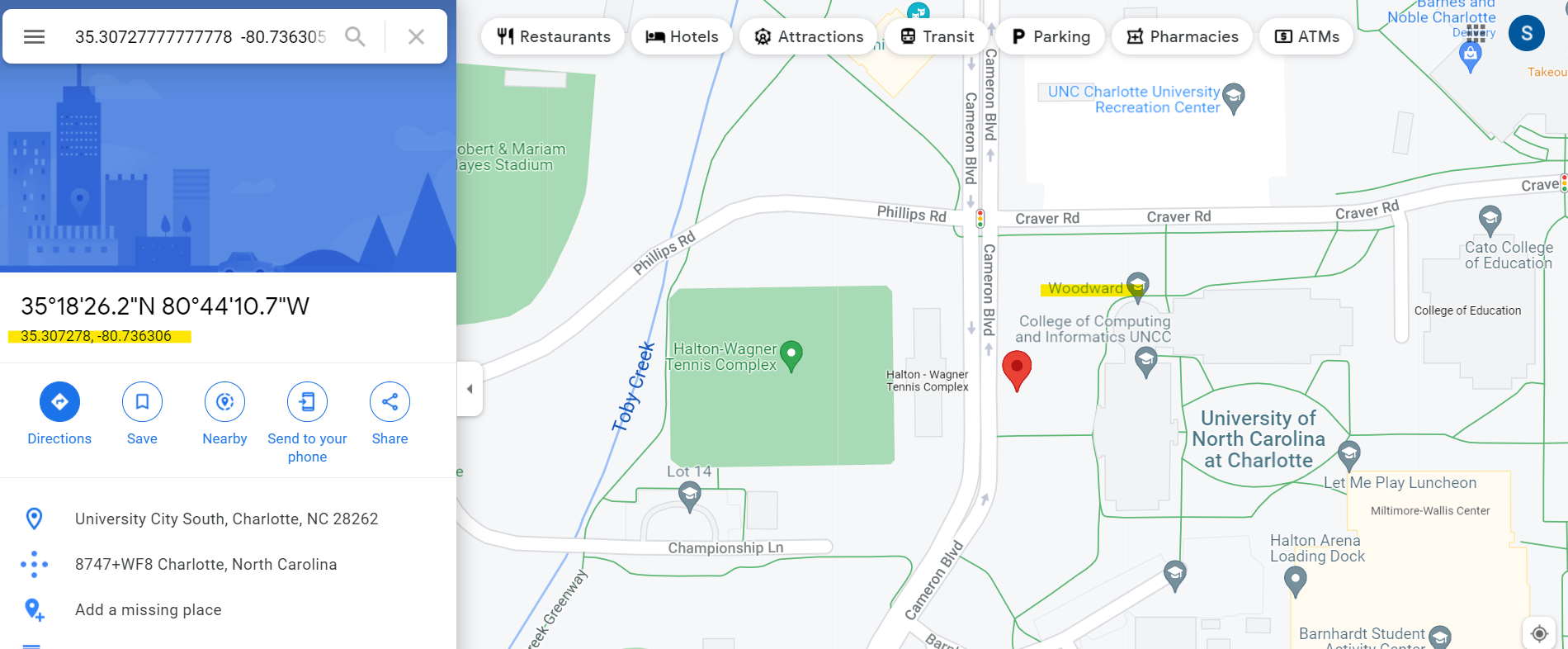
Windows 7 computer with “UNC CHARLOTTE” on display and its Exif Metadata



Latitude and longitude information of “Windows 7 computer” on google maps



Printer with “uncc.edu” stamped on it and its Exif Metadata



Latitude and longitude information of “Printer” on google maps

**Conclusion:**

Overall, in this lab I was asked to provide photographs relevant to the theft case of Apple devices and computer equipments reported at the University of North Carolina at Charlotte. To begin the analysis, the image was loaded using AccessData FTK Imager 4.5.0.3 on a Windows 10 Machine and the hash value of image was verified to conclude that it was not tampered before the analysis process. All the questions regarding this case were successfully answered with the help of Autopsy. At the end of analysis, metadata from pictures of Windows 7 computer, printer and

Apple TV shows that the pictures were taken from an Apple iPhone 6s. By entering the latitude and longitude information on Google Maps found in the Exif Metadata of all the pictures, it shows they are taken near Woodward Hall at University of North Carolina at Charlotte.

The image was again verified using AccessData FTK Imager to ensure it is not altered. No evidence has been retained. The forensic image, and answered questions regarding it, were returned to Office Jimmy Johns.