ITIS 4250 / 5250

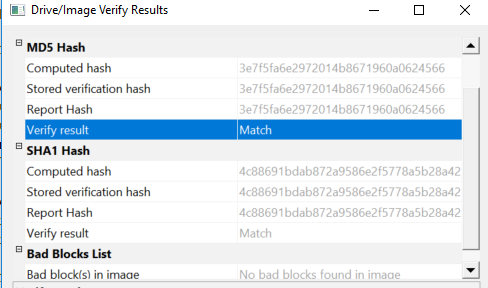
Lab # 3

10/9/2019

**Overview:**

Officer Jimmy Johns of the University of North Carolina Charlotte Police Department has tasked me to help him catch the criminal involved with the thief of an Apple Computer, Apple Tv’s, iPad and iPhone from Woodward hall on February 23rd, 2016. I have obtained a forensic image of a thumb drive owned by the potential suspect, this has been obtained by officer john during a traffic stop and I have received proper legal permissions to analyze the information found within the thumb drive for evidence.

**Forensic Acquisition & Exam Preparation**

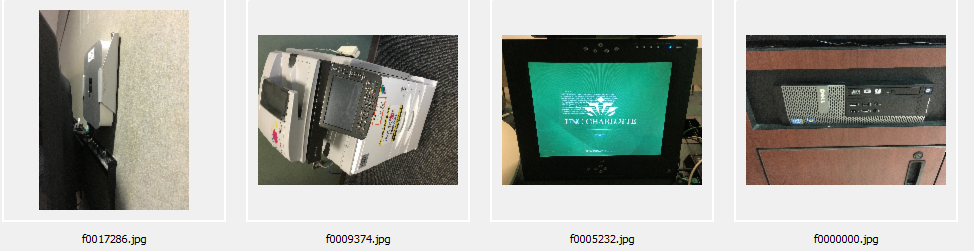
The first step was transferring the file ‘ItemA\_thumbdrive.E01’ from Canvas into a fresh folder on my work machine. My machine is a Lenovo Yoga 13 with 8gb of ddr4 ram along with an i5-8500. After transferring ‘ItemA\_thumbdrive.E01’ on my machine I verified the hash to make sure the file hasn’t been tampered with 

I have also installed Autopsy 4.12 which will be utilized in this lab.

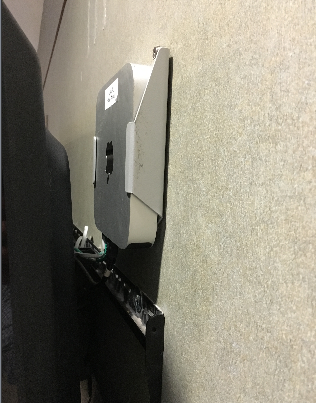
**Findings and Report (Forensic Analysis)**

After initial review of the drive it seems to contain 23 photos. 

Upon further inspection it seems that 16 of these 23 photos have been deleted. The remaining 7 photos that have not been deleted appear to be of buildings and “memes”. However, the deleted photos appear to be much more relevant to the case. Utilizing Autopsy, I was able to extract the EXIF Metadata from the deleted images, by doing this I was able to view the images and have found images of 2 computers, a printer, and a computer display



There is an image of a Mac Mini with a sticker



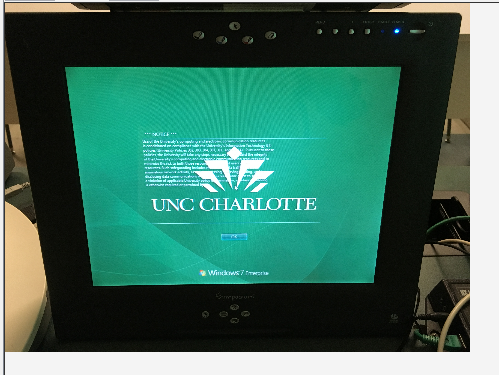
a large printer,



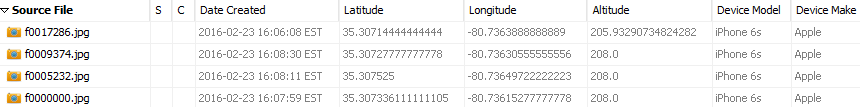
a Dell tower computer



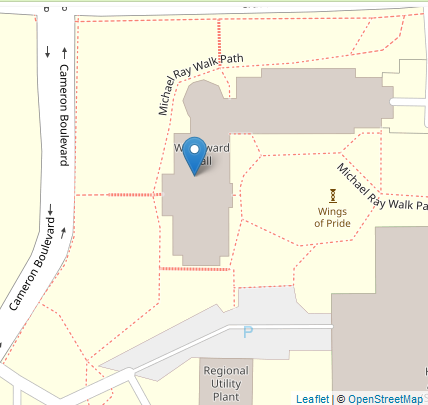
Computer display

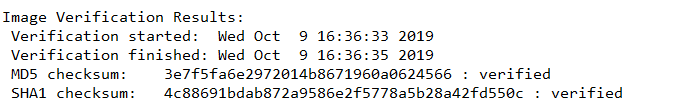


After further investigation of these 4 images I have discovered that they were all taken with an Apple iPhone 6s



I was also able to find the coordinates of the photos taken and when plotted on a map they are all within Woodward Hall.



I have re-verfied the image after concluding my investiagtion. 

**Conclusion:**

After investigating the forensic image ‘ItemA\_thumbdrive.E01’ which was given to me from officer John who received it from the suspect during a traffic stop along with finding other items from the suspect including an iPhone 6s, mac mini with sticker removed, apple laptop computer, and several iPads. I have found multiple pictures upon the drive; some were generic photos that contained “memes” and buildings. Other images which were found utilizing the exif metadata since they were deleted. These photos had a Dell tower computer, an Apple mac mini with a sticker on it, a monitor, and a printer. The photos were taken with an iPhone 6s within Woodward hall based upon the coordinates of the photo.