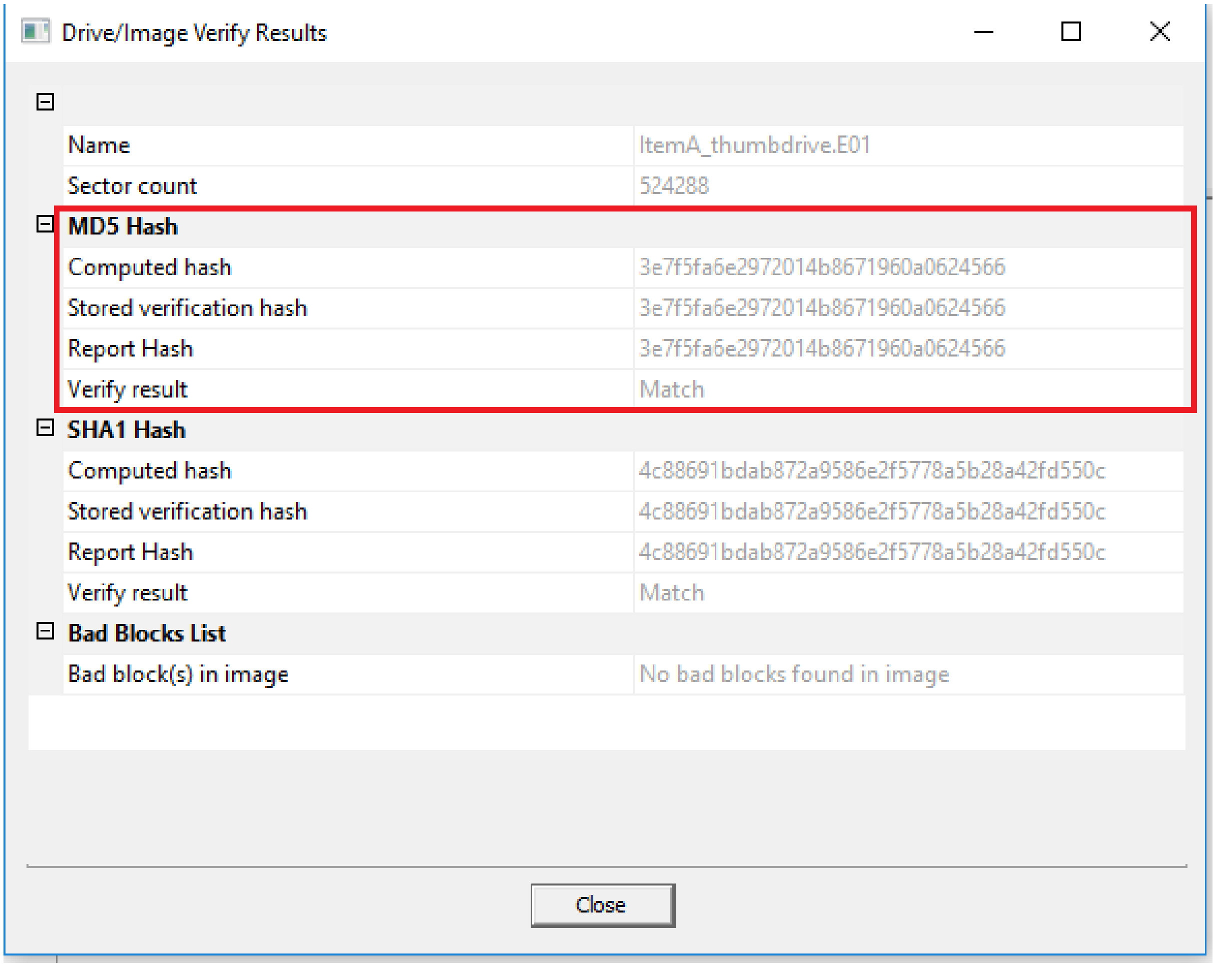
ITIS 5250
Parag Mhatre
Lab 10/12/2018

## Overview

In this lab, I will be examining the Forensic Image – **“ItemA_thumbdrive.E01”** given to me by Officer Johns. I will perform various operations and examinations using the FTK (Forensic Toolkit) after verifying & matching its Hash values.  The purpose of the examination is to find out if the owner of the thumb drive, was involved in the theft that happened in Woodward.

## Forensic Acquisition & Exam Preparation

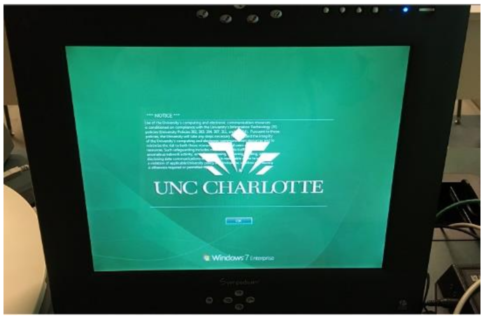
I downloaded the image files from Canvas, calculated and verified the Hash values of the files. The software used for accessing & extracting information from the image is **FTK Imager 4.1.1.1**  and **Forensic Toolkit 6.3.** The MD5 Hash of both the images are as given below:



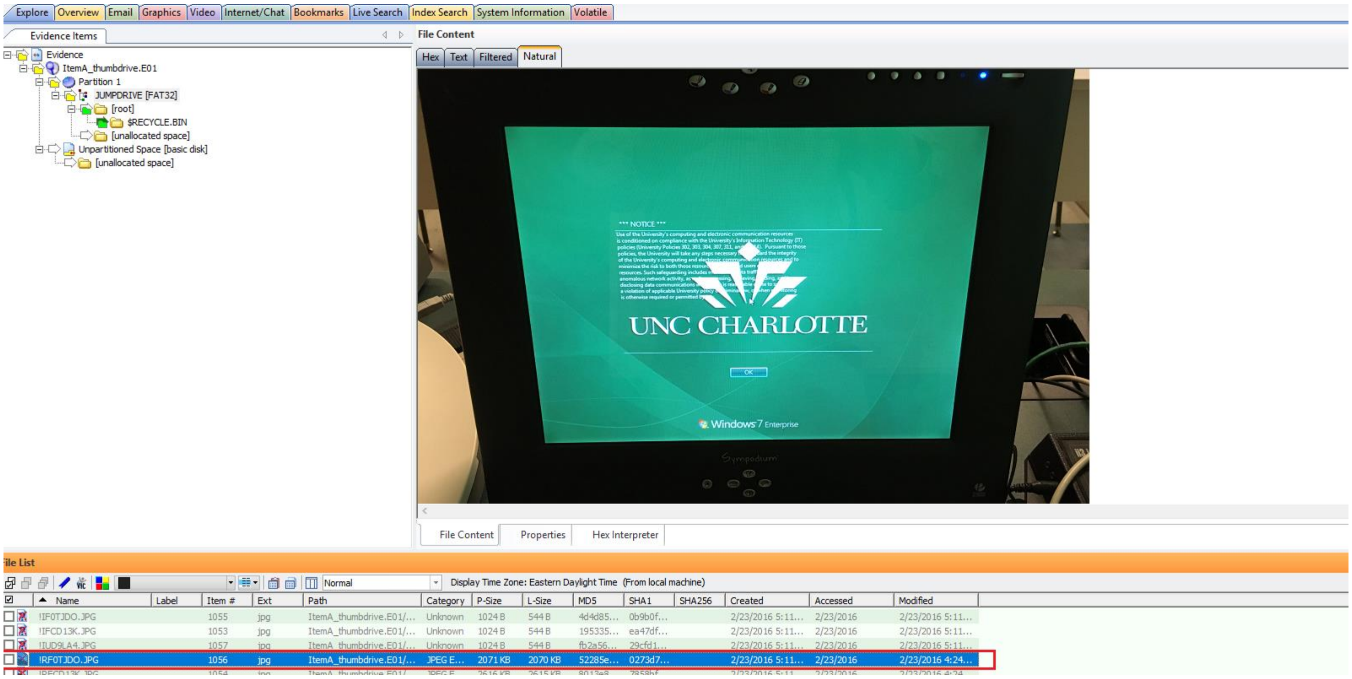
| | |
|---|---|
| Name | ItemA_thumbdrive.E01 |
| Sector count | 524288 |
| **MD5 Hash** | |
| Computed hash | 3e7f5fa6e2972014b8671960a0624566 |
| Stored verification hash | 3e7f5fa6e2972014b8671960a0624566 |
| Report Hash | 3e7f5fa6e2972014b8671960a0624566 |
| Verify result | Match |
| **SHA1 Hash** | |
| Computed hash | 4c88691bdab872a9586e2f5778a5b28a42fd550c |
| Stored verification hash | 4c88691bdab872a9586e2f5778a5b28a42fd550c |
| Report Hash | 4c88691bdab872a9586e2f5778a5b28a42fd550c |
| Verify result | Match |
| **Bad Blocks List** | |
| Bad block(s) in image | No bad blocks found in image |

# Findings and Report (Forensic Analysis)

Once I started examining the image, I checked the files on the and found a few picture files that were clicked from inside Woodward. The picture files are located inside the root folder of the thumb drive.



## Image 1:

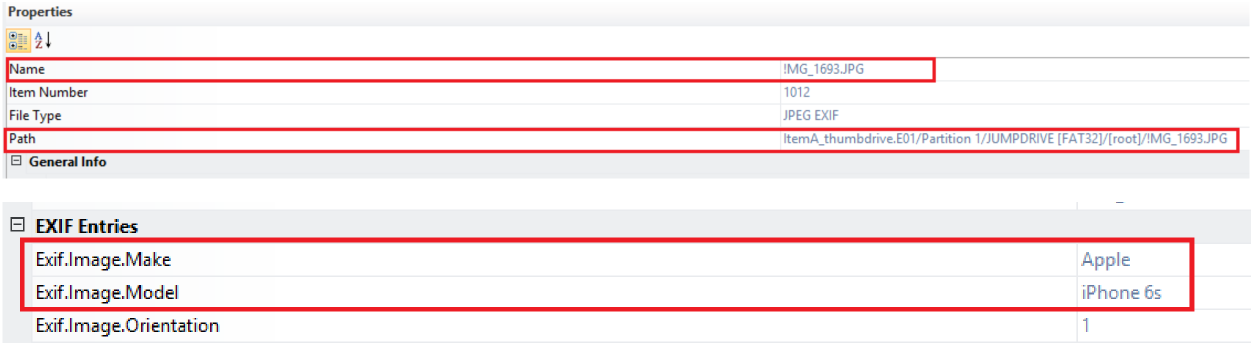


```
Evidence
  ItemA_thumbdrive.E01
    Partition 1
      JUMPDRIVE [FAT32]
        [root]
          $RECYCLE.BIN
        [unallocated space]
    Unpartitioned Space [basic disk]
      [unallocated space]
```

Display Time Zone: Eastern Daylight Time (From local machine)

| Name | Label | Item # | Ext | Path | Category | P-Size | L-Size | MD5 | SHA1 | SHA256 | Created | Accessed | Modified |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| !IF0TJDO.JPG | | 1055 | jpg | ItemA_thumbdrive.E01/... | Unknown | 1024 B | 544 B | 4d4d85... | 0b9b0f... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 5:11... |
| !IFCD13K.JPG | | 1053 | jpg | ItemA_thumbdrive.E01/... | Unknown | 1024 B | 544 B | 195335... | ea47df... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 5:11... |
| !IUD9LA4.JPG | | 1057 | jpg | ItemA_thumbdrive.E01/... | Unknown | 1024 B | 544 B | fb2a56... | 29cfd1... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 5:11... |
| !RF0TJDO.JPG | | 1056 | jpg | ItemA_thumbdrive.E01/... | JPEG E... | 2071 KB | 2070 KB | 52285e... | 0273d7... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 4:24... |
| !RFCD13K.JPG | | 1054 | jpg | ItemA_thumbdrive.E01/... | JPEG E... | 2616 KB | 2615 KB | 8013e8... | 7858bf... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 4:24... |

## The properties of the image are as follows:



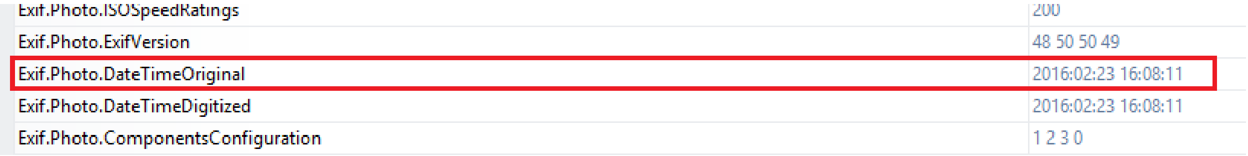
Properties

| | |
|---|---|
| Name | !IMG_1693.JPG |
| Item Number | 1012 |
| File Type | JPEG EXIF |
| Path | ItemA_thumbdrive.E01/Partition 1/JUMPDRIVE [FAT32]/[root]/!IMG_1693.JPG |

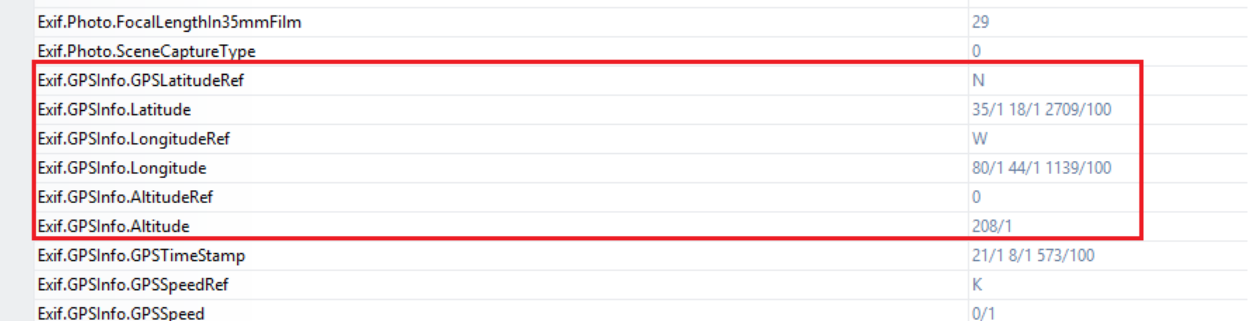
General Info

EXIF Entries

| | |
|---|---|
| Exif.Image.Make | Apple |
| Exif.Image.Model | iPhone 6s |
| Exif.Image.Orientation | 1 |

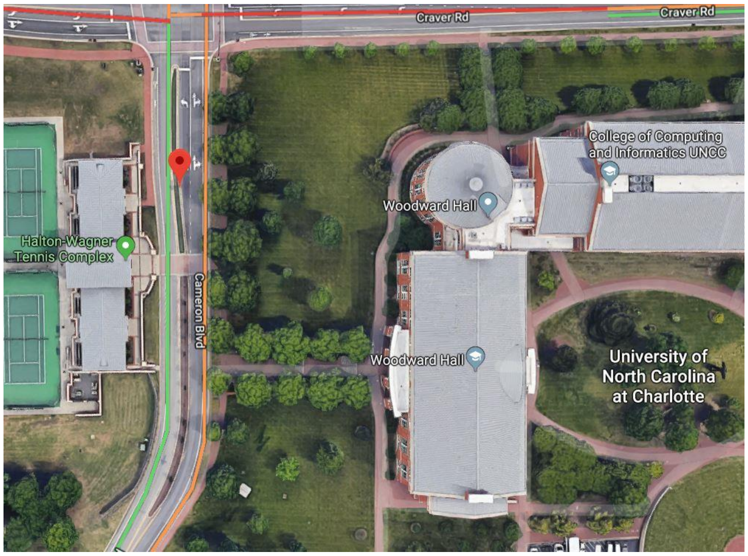


| | |
|---|---|
| Exif.Photo.ISOSpeedRatings | 200 |
| Exif.Photo.ExifVersion | 48 50 50 49 |
| Exif.Photo.DateTimeOriginal | 2016:02:23 16:08:11 |
| Exif.Photo.DateTimeDigitized | 2016:02:23 16:08:11 |
| Exif.Photo.ComponentsConfiguration | 1 2 3 0 |

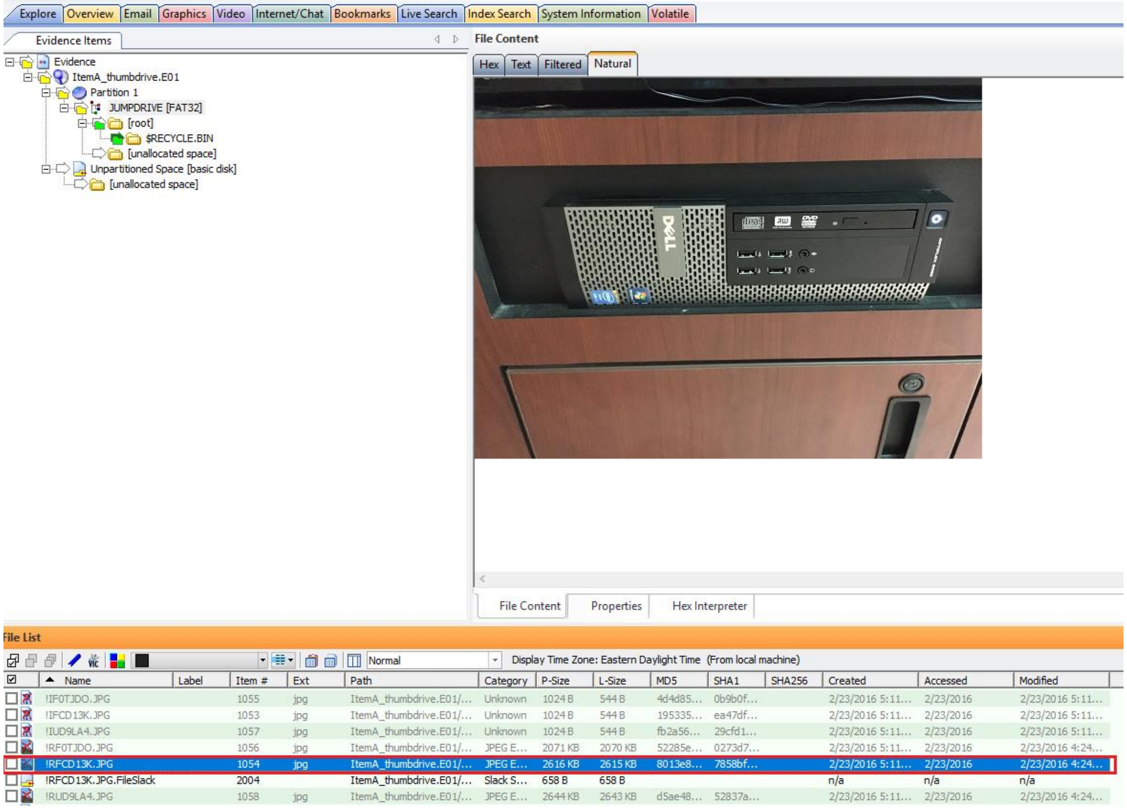


| | |
|---|---|
| Exif.Photo.FocalLengthIn35mmFilm | 29 |
| Exif.Photo.SceneCaptureType | 0 |
| Exif.GPSInfo.GPSLatitudeRef | N |
| Exif.GPSInfo.Latitude | 35/1 18/1 2709/100 |
| Exif.GPSInfo.LongitudeRef | W |
| Exif.GPSInfo.Longitude | 80/1 44/1 1139/100 |
| Exif.GPSInfo.AltitudeRef | 0 |
| Exif.GPSInfo.Altitude | 208/1 |
| Exif.GPSInfo.GPSTimeStamp | 21/1 8/1 573/100 |
| Exif.GPSInfo.GPSSpeedRef | K |
| Exif.GPSInfo.GPSSpeed | 0/1 |

**Name:** !MG_1693.JPG  
**Path:** ItemA_thumbdrive.E01/Partition 1/JUMPDRIVE [FAT32]/[root]/!MG_1693.JPG  
**Device:** Apple iPhone 6s  
**Date Clicked:** February 23rd 2016, 16:08:11  
**Latitude:** 35°18'27.1"N  
**Longitude:** 80°44'11.4"W


Craver Rd
Craver Rd
College of Computing and Informatics UNCC
Woodward Hall
Halton-Wagner Tennis Complex
Cameron Blvd
Woodward Hall
University of North Carolina at Charlotte

## Image 2:



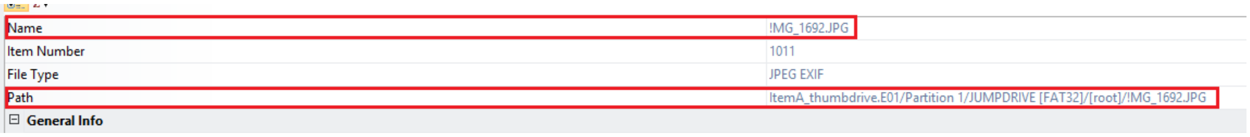
```
Evidence
  ItemA_thumbdrive.E01
    Partition 1
      JUMPDRIVE [FAT32]
        [root]
          $RECYCLE.BIN
        [unallocated space]
    Unpartitioned Space [basic disk]
      [unallocated space]
```

Normal

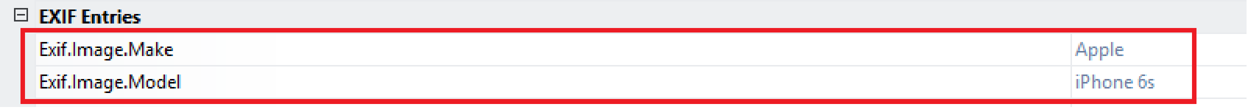
Display Time Zone: Eastern Daylight Time (From local machine)

| ☑ | Name | Label | Item # | Ext | Path | Category | P-Size | L-Size | MD5 | SHA1 | SHA256 | Created | Accessed | Modified |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | !IF0TJDO.JPG | | 1055 | jpg | ItemA_thumbdrive.E01/... | Unknown | 1024 B | 544 B | 4d4d85... | 0b9b0f... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 5:11... |
| □ | !IFCD13K.JPG | | 1053 | jpg | ItemA_thumbdrive.E01/... | Unknown | 1024 B | 544 B | 195335... | ea47df... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 5:11... |
| □ | !IUD9LA4.JPG | | 1057 | jpg | ItemA_thumbdrive.E01/... | Unknown | 1024 B | 544 B | fb2a56... | 29cfd1... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 5:11... |
| □ | !RF0TJDO.JPG | | 1056 | jpg | ItemA_thumbdrive.E01/... | JPEG E... | 2071 KB | 2070 KB | 52285e... | 0273d7... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 4:24... |
| □ | !RFCD13K.JPG | | 1054 | jpg | ItemA_thumbdrive.E01/... | JPEG E... | 2616 KB | 2615 KB | 8013e8... | 7858bf... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 4:24... |
| □ | !RFCD13K.JPG.FileSlack | | 2004 | | ItemA_thumbdrive.E01/... | Slack S... | 658 B | 658 B | | | | n/a | n/a | n/a |
| □ | !RUD9LA4.JPG | | 1058 | jpg | ItemA_thumbdrive.E01/... | JPEG E... | 2644 KB | 2643 KB | d5ae48... | 52837a... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 4:24... |

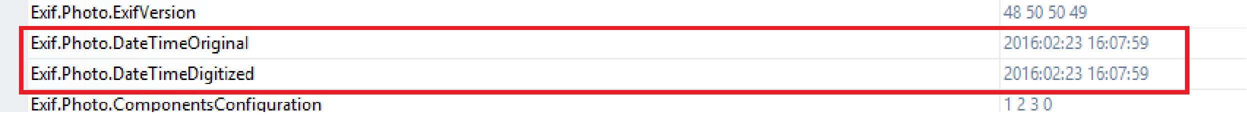
## The properties of the image are as follows:



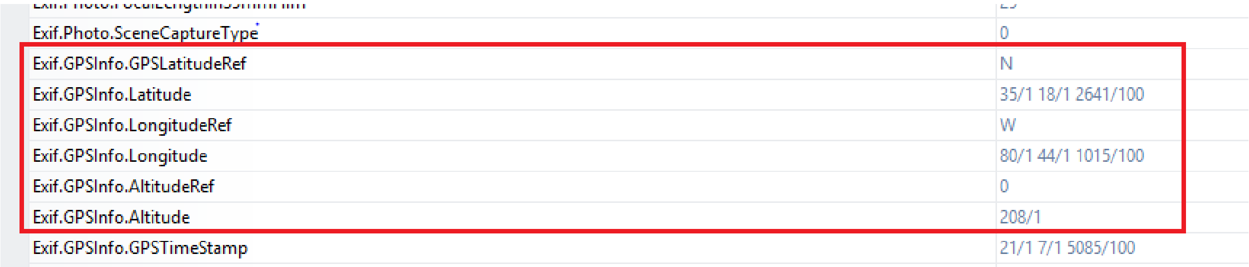
| | |
|---|---|
| Name | !MG_1692.JPG |
| Item Number | 1011 |
| File Type | JPEG EXIF |
| Path | ItemA_thumbdrive.E01/Partition 1/JUMPDRIVE [FAT32]/[root]/!MG_1692.JPG |
| ⊟ General Info | |



| ⊟ EXIF Entries | |
|---|---|
| Exif.Image.Make | Apple |
| Exif.Image.Model | iPhone 6s |

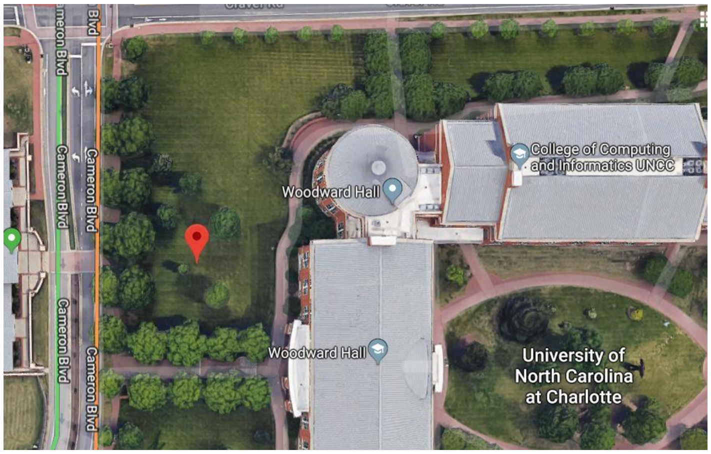


| | |
|---|---|
| Exif.Photo.ExifVersion | 48 50 50 49 |
| Exif.Photo.DateTimeOriginal | 2016:02:23 16:07:59 |
| Exif.Photo.DateTimeDigitized | 2016:02:23 16:07:59 |
| Exif.Photo.ComponentsConfiguration | 1 2 3 0 |

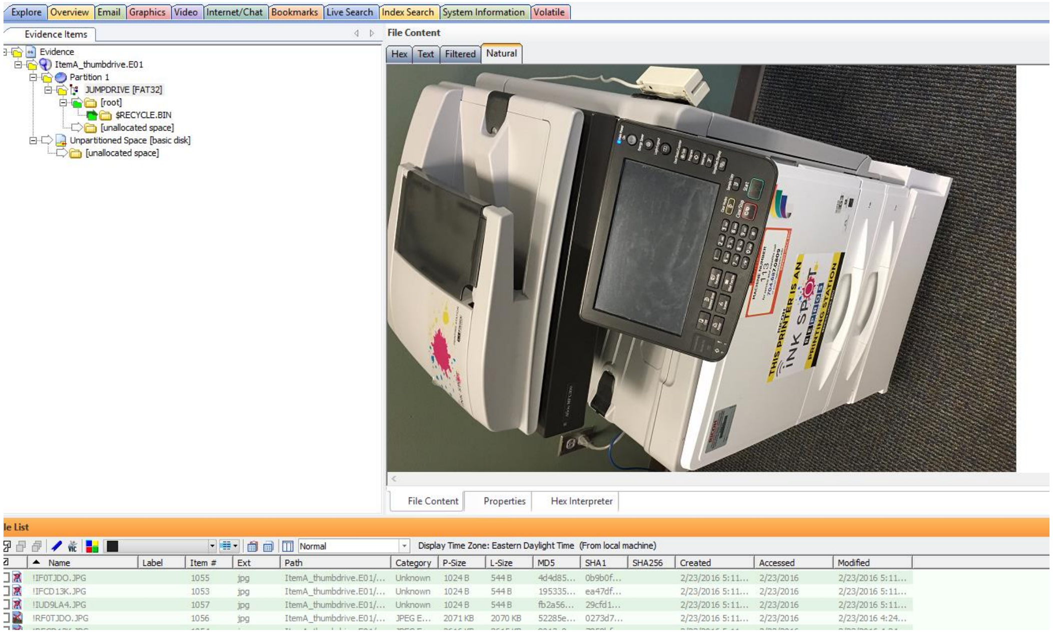


| | |
|---|---|
| Exif.Photo.SceneCaptureType | 0 |
| Exif.GPSInfo.GPSLatitudeRef | N |
| Exif.GPSInfo.Latitude | 35/1 18/1 2641/100 |
| Exif.GPSInfo.LongitudeRef | W |
| Exif.GPSInfo.Longitude | 80/1 44/1 1015/100 |
| Exif.GPSInfo.AltitudeRef | 0 |
| Exif.GPSInfo.Altitude | 208/1 |
| Exif.GPSInfo.GPSTimeStamp | 21/1 7/1 5085/100 |

**Name:** !MG_1692.JPG<br>
**Path:** ItemA_thumbdrive.E01/Partition 1/JUMPDRIVE [FAT32]/[root]/!MG_1692.JPG<br>
**Device:** Apple iPhone 6s<br>
**Date Clicked:** February 23rd 2016, 16:07:59<br>
**Latitude:** 35°18'26.41"N<br>
**Longitude:** 80°44'10.15"W


Cameron Blvd
College of Computing and Informatics UNCC
Woodward Hall
Woodward Hall
University of North Carolina at Charlotte

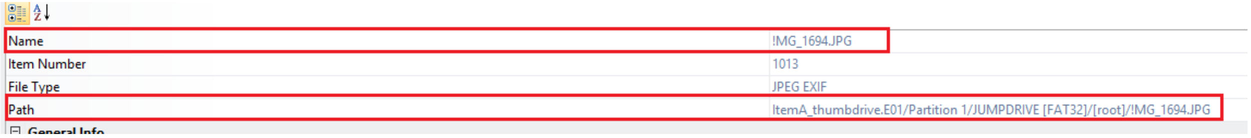
## Image 3:



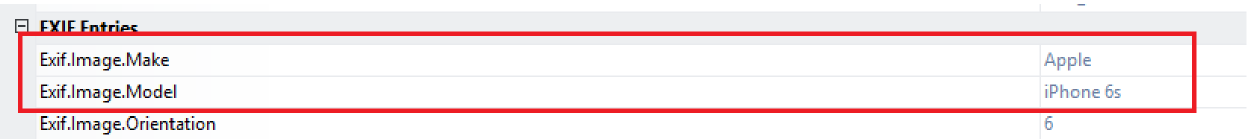
Display Time Zone: Eastern Daylight Time (From local machine)

| Name | Label | Item # | Ext | Path | Category | P-Size | L-Size | MD5 | SHA1 | SHA256 | Created | Accessed | Modified |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| !IF0TJDO.JPG | | 1055 | jpg | ItemA_thumbdrive.E01/... | Unknown | 1024 B | 544 B | 4d4d85... | 0b9b0f... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 5:11... |
| !IFCD13K.JPG | | 1053 | jpg | ItemA_thumbdrive.E01/... | Unknown | 1024 B | 544 B | 195335... | ea47df... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 5:11... |
| !IUD9LA4.JPG | | 1057 | jpg | ItemA_thumbdrive.E01/... | Unknown | 1024 B | 544 B | fb2a56... | 29cfd1... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 5:11... |
| !RF0TJDO.JPG | | 1056 | jpg | ItemA_thumbdrive.E01/... | JPEG E... | 2071 KB | 2070 KB | 52285e... | 0273d7... | | 2/23/2016 5:11... | 2/23/2016 | 2/23/2016 4:24... |

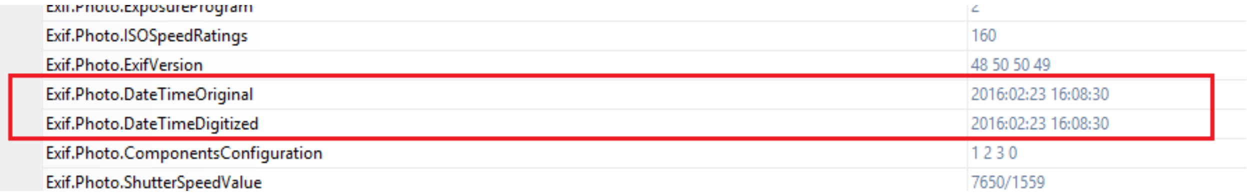
## The properties of the image are as follows:



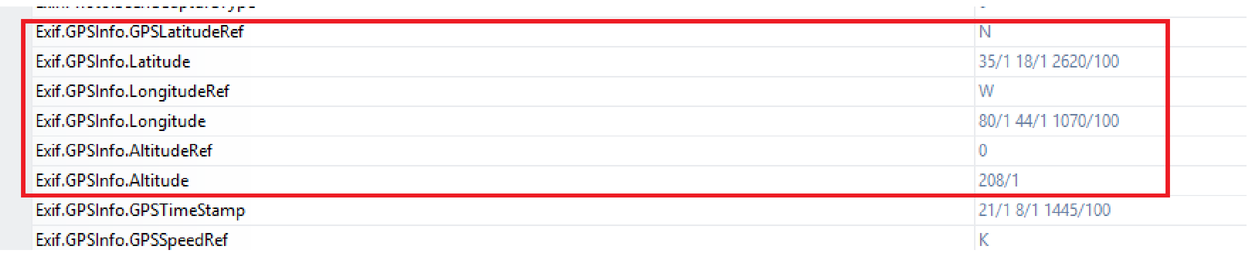
| | |
|---|---|
| Name | !MG_1694.JPG |
| Item Number | 1013 |
| File Type | JPEG EXIF |
| Path | ItemA_thumbdrive.E01/Partition 1/JUMPDRIVE [FAT32]/[root]/!MG_1694.JPG |
| ⊟ General Info | |



| | |
|---|---|
| ⊟ EXIF Entries | |
| Exif.Image.Make | Apple |
| Exif.Image.Model | iPhone 6s |
| Exif.Image.Orientation | 6 |

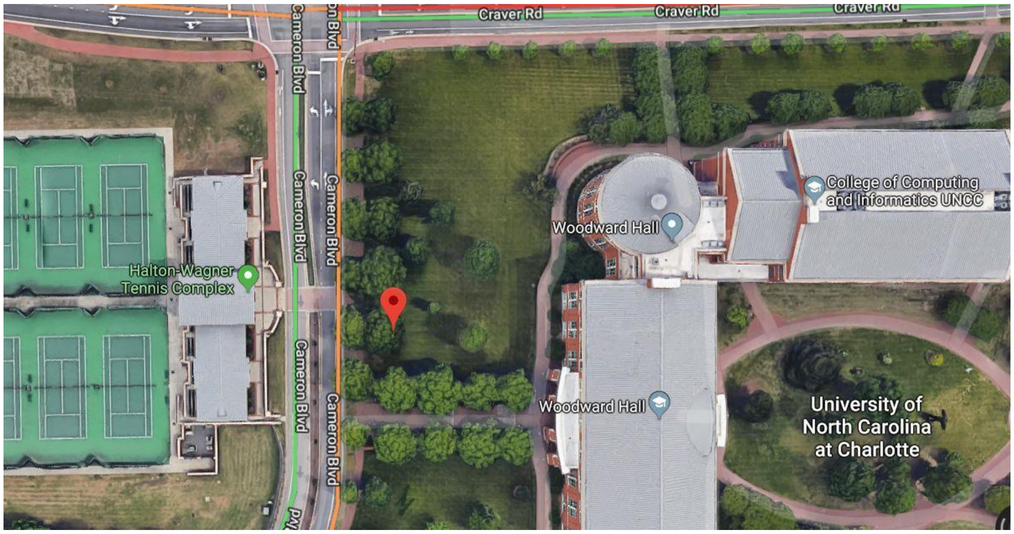


| | |
|---|---|
| Exif.Photo.ExposureProgram | 2 |
| Exif.Photo.ISOSpeedRatings | 160 |
| Exif.Photo.ExifVersion | 48 50 50 49 |
| Exif.Photo.DateTimeOriginal | 2016:02:23 16:08:30 |
| Exif.Photo.DateTimeDigitized | 2016:02:23 16:08:30 |
| Exif.Photo.ComponentsConfiguration | 1 2 3 0 |
| Exif.Photo.ShutterSpeedValue | 7650/1559 |

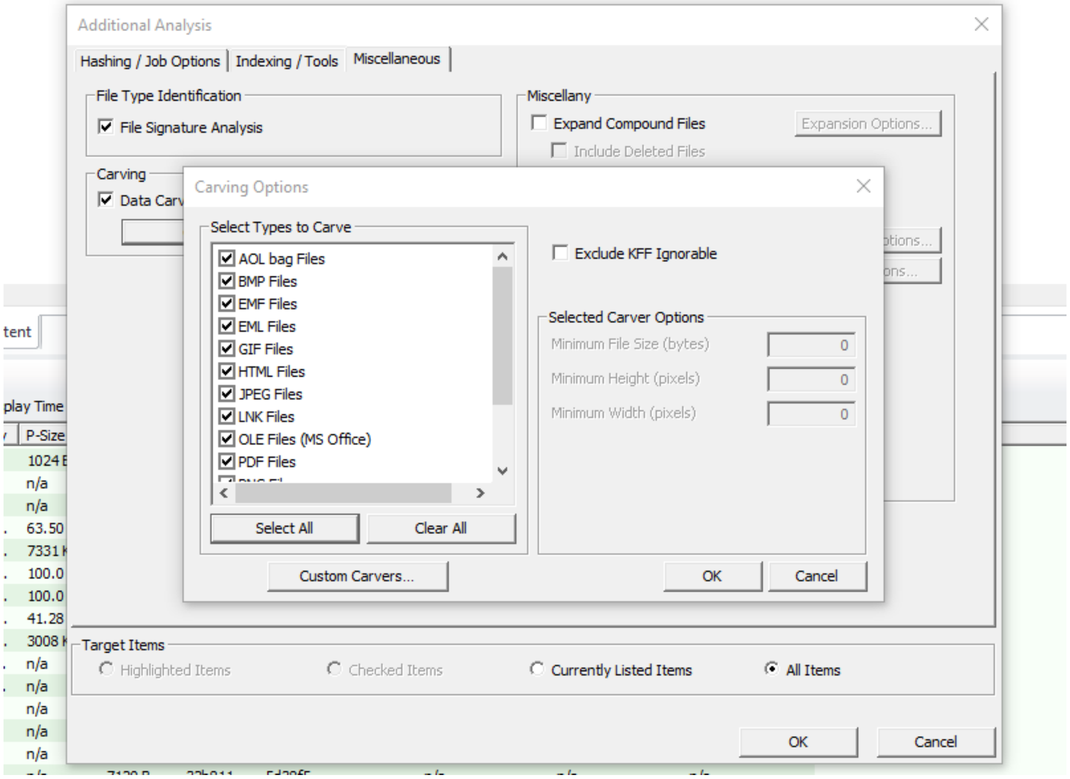


| | |
|---|---|
| Exif.GPSInfo.GPSLatitudeRef | N |
| Exif.GPSInfo.Latitude | 35/1 18/1 2620/100 |
| Exif.GPSInfo.LongitudeRef | W |
| Exif.GPSInfo.Longitude | 80/1 44/1 1070/100 |
| Exif.GPSInfo.AltitudeRef | 0 |
| Exif.GPSInfo.Altitude | 208/1 |
| Exif.GPSInfo.GPSTimeStamp | 21/1 8/1 1445/100 |
| Exif.GPSInfo.GPSSpeedRef | K |

**Name:** !MG_1694.JPG
**Path:** ItemA_thumbdrive.E01/Partition 1/JUMPDRIVE [FAT32]/[root]/!MG_1694.JPG
**Device:** Apple iPhone 6s
**Date Clicked:** February 23rd 2016, 16:08:30
**Latitude:** 35°18'26.20"N
**Longitude:** 80°44'10.70"W



Furthermore, I performed **File Carving** via FTK and discovered some more files which were previously deleted.



Additional Analysis

Hashing / Job Options | Indexing / Tools | Miscellaneous

File Type Identification
☑ File Signature Analysis

Miscellany
□ Expand Compound Files — Expansion Options...
□ Include Deleted Files

Carving
☑ Data Carv

Carving Options

Select Types to Carve
☑ AOL bag Files
☑ BMP Files
☑ EMF Files
☑ EML Files
☑ GIF Files
☑ HTML Files
☑ JPEG Files
☑ LNK Files
☑ OLE Files (MS Office)
☑ PDF Files

Select All | Clear All

□ Exclude KFF Ignorable

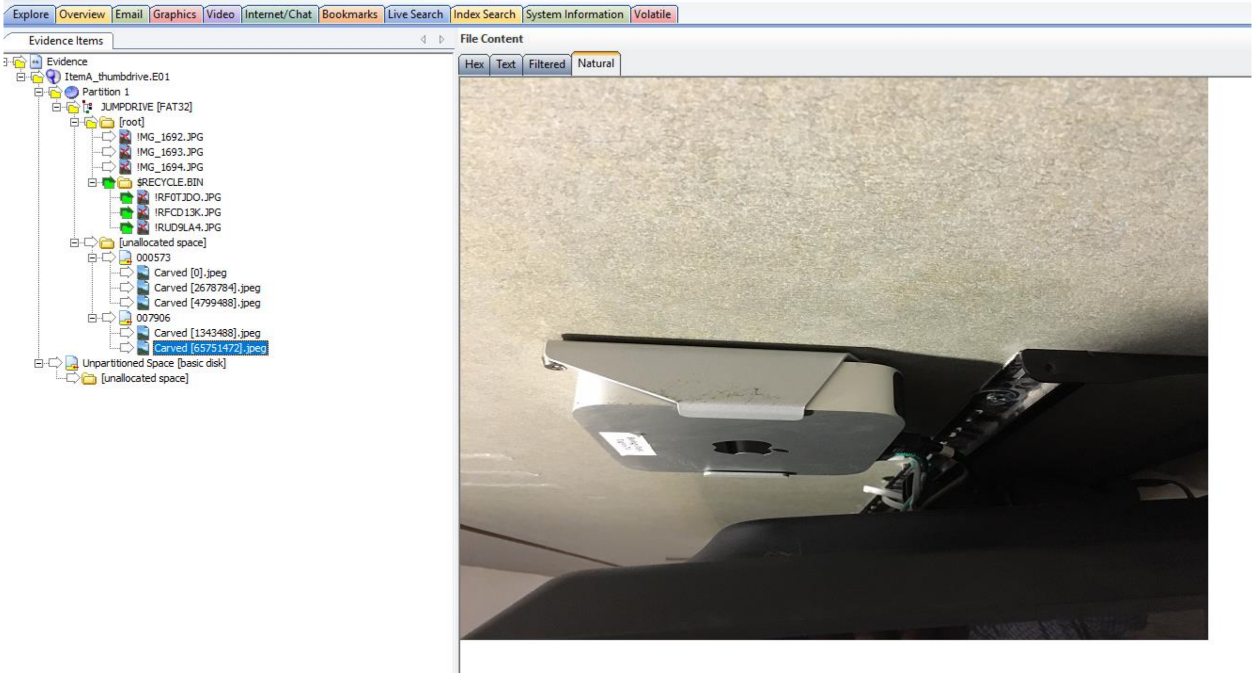
Selected Carver Options
Minimum File Size (bytes): 0
Minimum Height (pixels): 0
Minimum Width (pixels): 0

Custom Carvers... | OK | Cancel

Target Items
○ Highlighted Items ○ Checked Items ○ Currently Listed Items ● All Items

OK | Cancel

## Image 4 (Carved):



Explore | Overview | Email | Graphics | Video | Internet/Chat | Bookmarks | Live Search | Index Search | System Information | Volatile

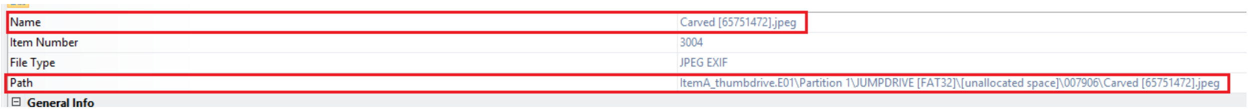
Evidence Items

```
Evidence
  ItemA_thumbdrive.E01
    Partition 1
      JUMPDRIVE [FAT32]
        [root]
          !MG_1692.JPG
          !MG_1693.JPG
          !MG_1694.JPG
          $RECYCLE.BIN
            !RF0TJDO.JPG
            !RFCD13K.JPG
            !RUD9LA4.JPG
        [unallocated space]
          000573
            Carved [0].jpeg
            Carved [2678784].jpeg
            Carved [4799488].jpeg
          007906
            Carved [1343488].jpeg
            Carved [65751472].jpeg
    Unpartitioned Space [basic disk]
      [unallocated space]
```

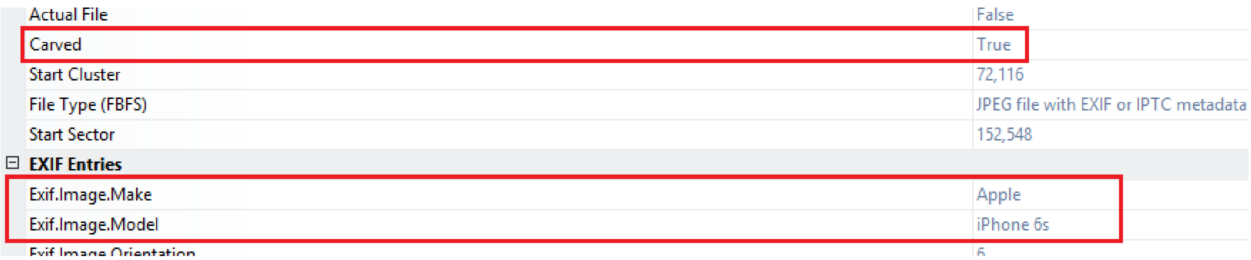
File Content

Hex | Text | Filtered | Natural

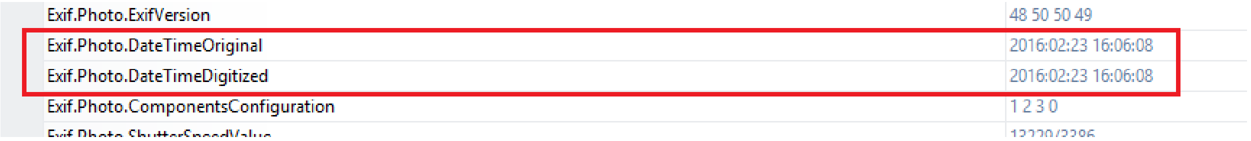
## The properties of the image are as follows:



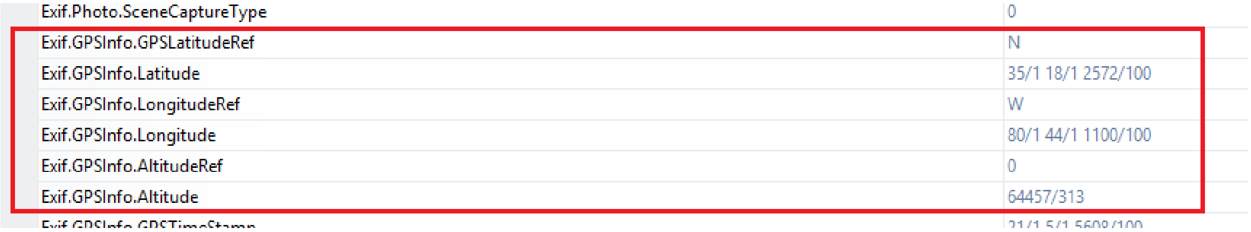
| | |
|---|---|
| Name | Carved [65751472].jpeg |
| Item Number | 3004 |
| File Type | JPEG EXIF |
| Path | ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[unallocated space]\007906\Carved [65751472].jpeg |
| ⊟ General Info | |



| | |
|---|---|
| Actual File | False |
| Carved | True |
| Start Cluster | 72,116 |
| File Type (FBFS) | JPEG file with EXIF or IPTC metadata |
| Start Sector | 152,548 |
| ⊟ EXIF Entries | |
| Exif.Image.Make | Apple |
| Exif.Image.Model | iPhone 6s |
| Exif.Image.Orientation | 6 |

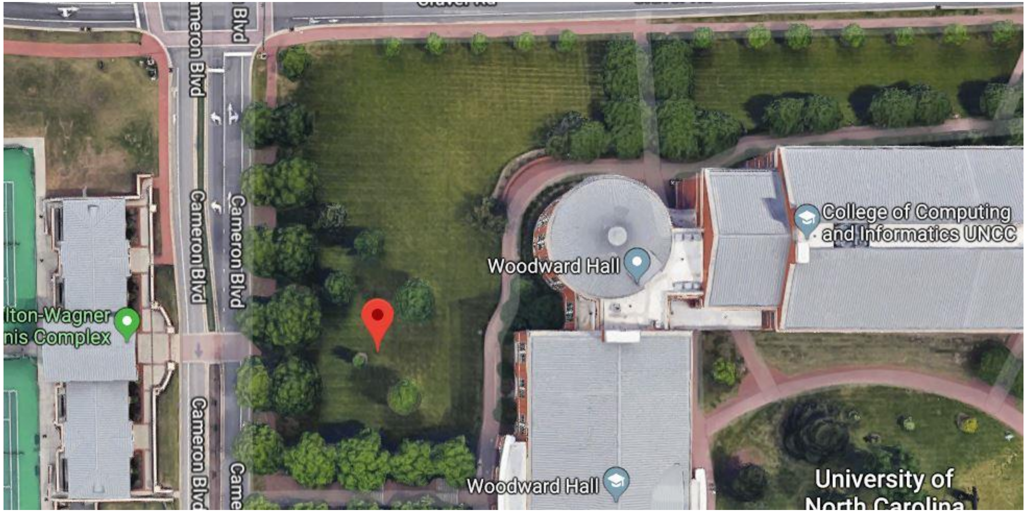


| | |
|---|---|
| Exif.Photo.ExifVersion | 48 50 50 49 |
| Exif.Photo.DateTimeOriginal | 2016:02:23 16:06:08 |
| Exif.Photo.DateTimeDigitized | 2016:02:23 16:06:08 |
| Exif.Photo.ComponentsConfiguration | 1 2 3 0 |
| Exif.Photo.ShutterSpeedValue | 13220/3386 |



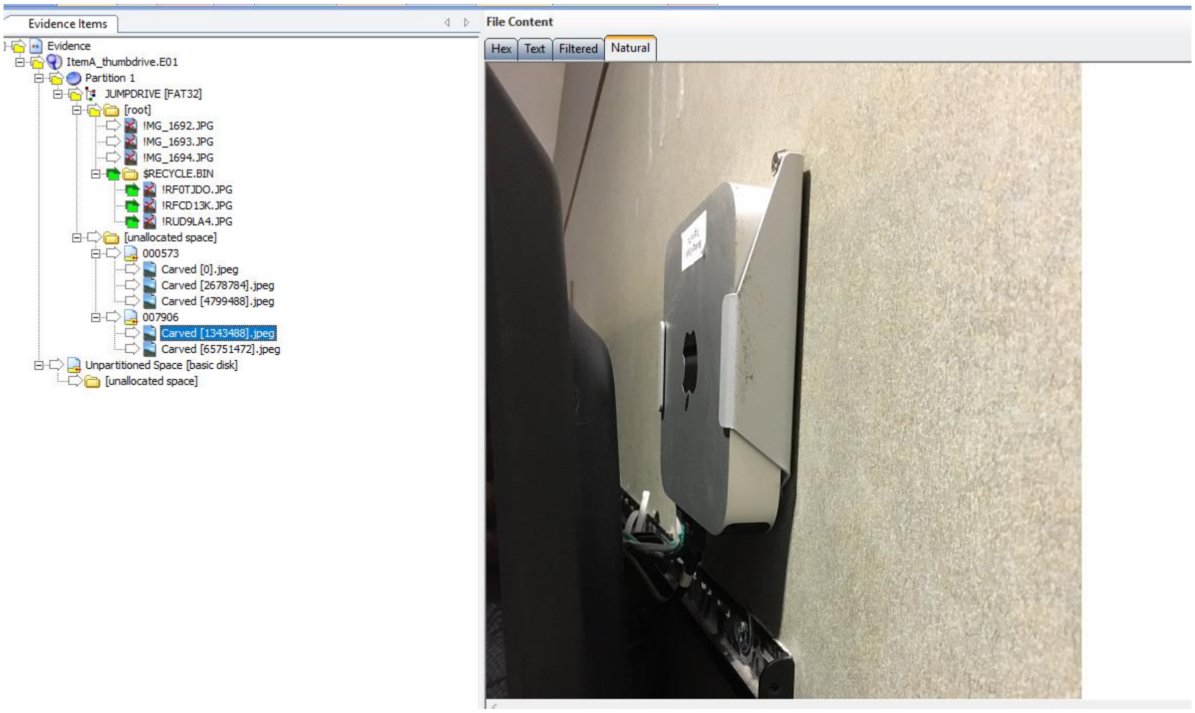
| | |
|---|---|
| Exif.Photo.SceneCaptureType | 0 |
| Exif.GPSInfo.GPSLatitudeRef | N |
| Exif.GPSInfo.Latitude | 35/1 18/1 2572/100 |
| Exif.GPSInfo.LongitudeRef | W |
| Exif.GPSInfo.Longitude | 80/1 44/1 1100/100 |
| Exif.GPSInfo.AltitudeRef | 0 |
| Exif.GPSInfo.Altitude | 64457/313 |
| Exif.GPSInfo.GPSTimeStamp | 21/1 5/1 5608/100 |

**Name:** Carved [65751472].jpeg
**Path:** ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[unallocated space]\007906\Carved [65751472].jpeg
**Device:** Apple iPhone 6s
**Date Clicked:** February 23rd 2016, 16:06:08
**Latitude:** 35°18'26.41"N
**Longitude:** 80°44'10.15"W

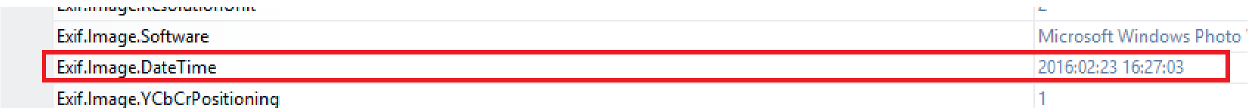


## Image 5:

I found another picture file – **“Carved [1343488].jpeg”**. This seems a modified version of the **Image 4**.

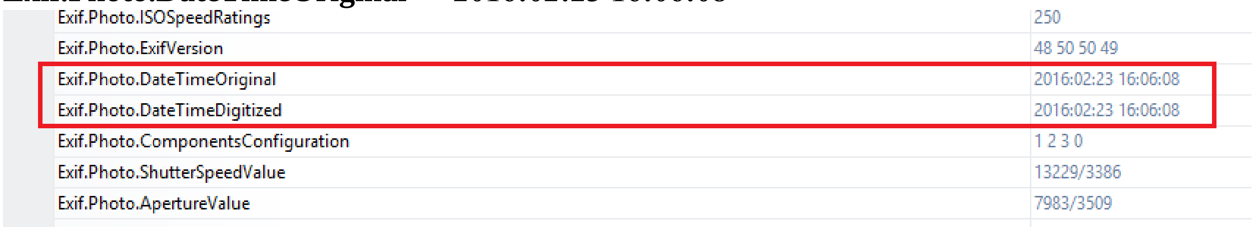


```
Evidence
  ItemA_thumbdrive.E01
    Partition 1
      JUMPDRIVE [FAT32]
        [root]
          !MG_1692.JPG
          !MG_1693.JPG
          !MG_1694.JPG
          $RECYCLE.BIN
            !RF0TJDO.JPG
            !RFCD13K.JPG
            !RUD9LA4.JPG
        [unallocated space]
          000573
            Carved [0].jpeg
            Carved [2678784].jpeg
            Carved [4799488].jpeg
          007906
            Carved [1343488].jpeg
            Carved [65751472].jpeg
    Unpartitioned Space [basic disk]
      [unallocated space]
```



| | |
|---|---|
| Exif.Image.ResolutionUnit | 2 |
| Exif.Image.Software | Microsoft Windows Photo |
| Exif.Image.DateTime | 2016:02:23 16:27:03 |
| Exif.Image.YCbCrPositioning | 1 |

The “Image 5” was carved with a on record **“Exif.Image.DateTime”** of **February 23rd, 2016 at 16:27:03**. But it is a modified version of “Image 4” as seen in the Properties: **Exif.Photo.DateTimeOriginal** – **“2016:02:23 16:06:08”**



| | |
|---|---|
| Exif.Photo.ISOSpeedRatings | 250 |
| Exif.Photo.ExifVersion | 48 50 50 49 |
| Exif.Photo.DateTimeOriginal | 2016:02:23 16:06:08 |
| Exif.Photo.DateTimeDigitized | 2016:02:23 16:06:08 |
| Exif.Photo.ComponentsConfiguration | 1 2 3 0 |
| Exif.Photo.ShutterSpeedValue | 13229/3386 |
| Exif.Photo.ApertureValue | 7983/3509 |

## Conclusion:

I examined the image of the thumb drive which was given to me by Officer Johns, **verified** and examined it. In my findings, I found some picture (image) files which showed that the pictures were from inside Woodward. Furthermore, I also performed **Data carving** and recovered a deleted image which **directly linked the accused with Apple devices from Woodward**. My findings are as follows:

**Image 1** – Picture of a screen from inside Woodward. The properties show that it was clicked from/around Woodward on February 23rd 2016, 16:08:11 and was clicked from an Apple iPhone 6S.

**Image 2** – Picture of a CPU from inside Woodward. The properties show that it was clicked from/around Woodward on February 23rd 2016, 16:07:59 and was clicked from an Apple iPhone 6S.

**Image 3** – Picture of a Copy Machine from inside Woodward. The properties show that it was clicked from/around Woodward on February 23rd 2016, 16:08:30 and was clicked from an Apple iPhone 6S.

**Image 4 (Carved)** – Picture of an Apple box/device with a sticker on it's body from inside Woodward. The properties show that it was clicked from/around Woodward on February 23rd 2016, 16:06:08 and was clicked from an Apple iPhone 6S.

**Image 5 (Carved)** – A modified version of Image 4 which was modified on February 23rd, 2016 at 16:27:03.