ITIS 5250
Sneha Rangari
Lab 3
10/16/2018

Overview:

In this Lab, I have been given one file, namely "ItemA_thumbdrive.E01". I have been asked to make use of the "FTK Tool" along with "FTK Imager Tool" and "Google Maps" to find any information to show that a thief was scouting for items to steal from Woodward. I also have been asked to provide any photographs relevant to the investigation.

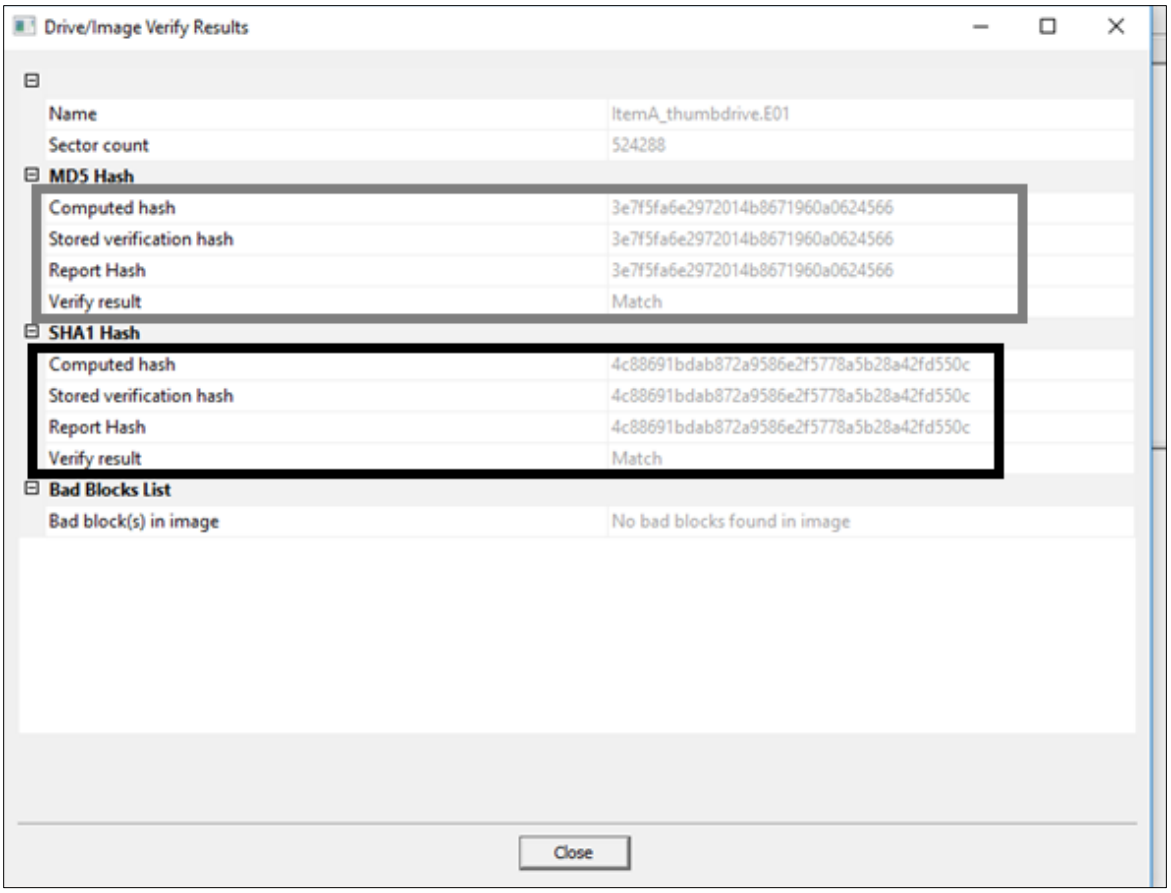
Forensic Acquisition & Exam Preparation:

I accessed the Forensic images in the Shared Folder on the network from the Forensics Lab in Cone 169. I accessed image named "ItemA_thumbdrive.E01" and its log file. The software used for accessing & extracting information from the image is FTK Imager 4.1.1.1. The first step undertaken after accessing the image files was the Hash verification along with description of image from txt file.

ItemA_thumbdrive.E01:

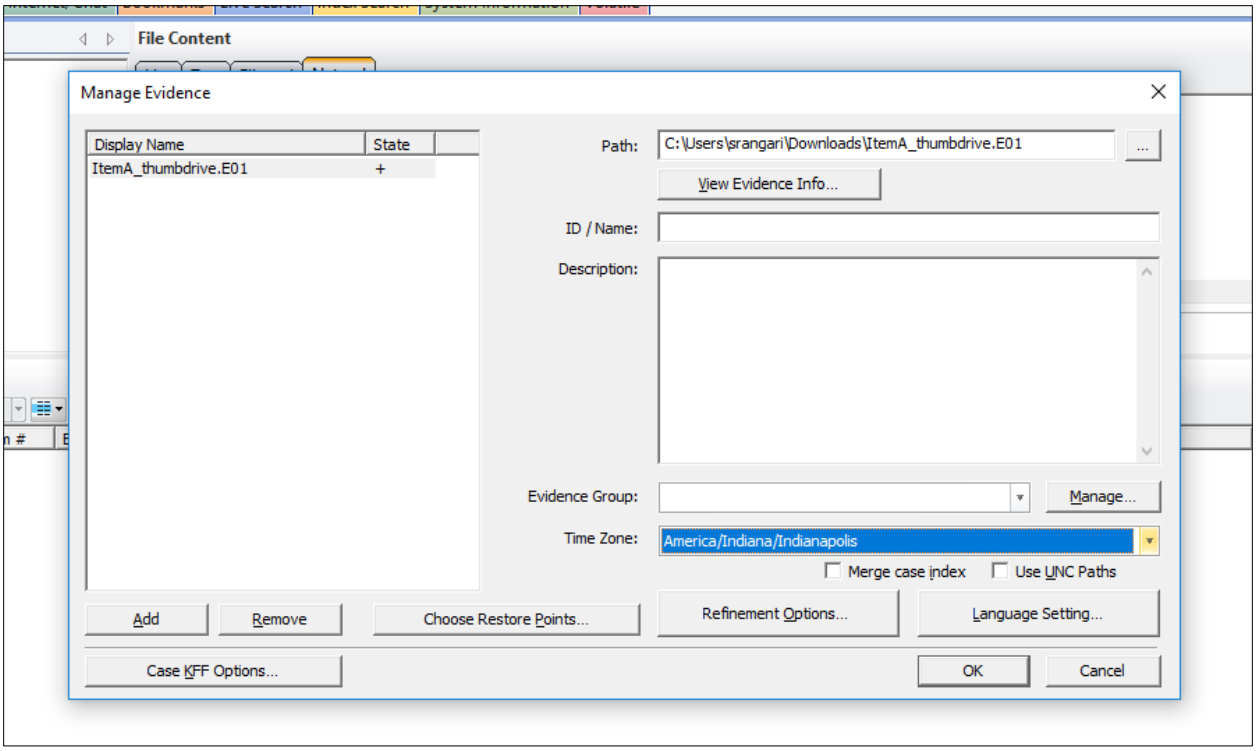
Case Information:
Acquired using: ADI3.2.0.0
Case Number: X_02232016
Evidence Number: ItemA
Unique description: A thumbdrive provided on consent
Examiner: Ofc. Jimmy Johns
Notes: This guy is definitely guilty!!

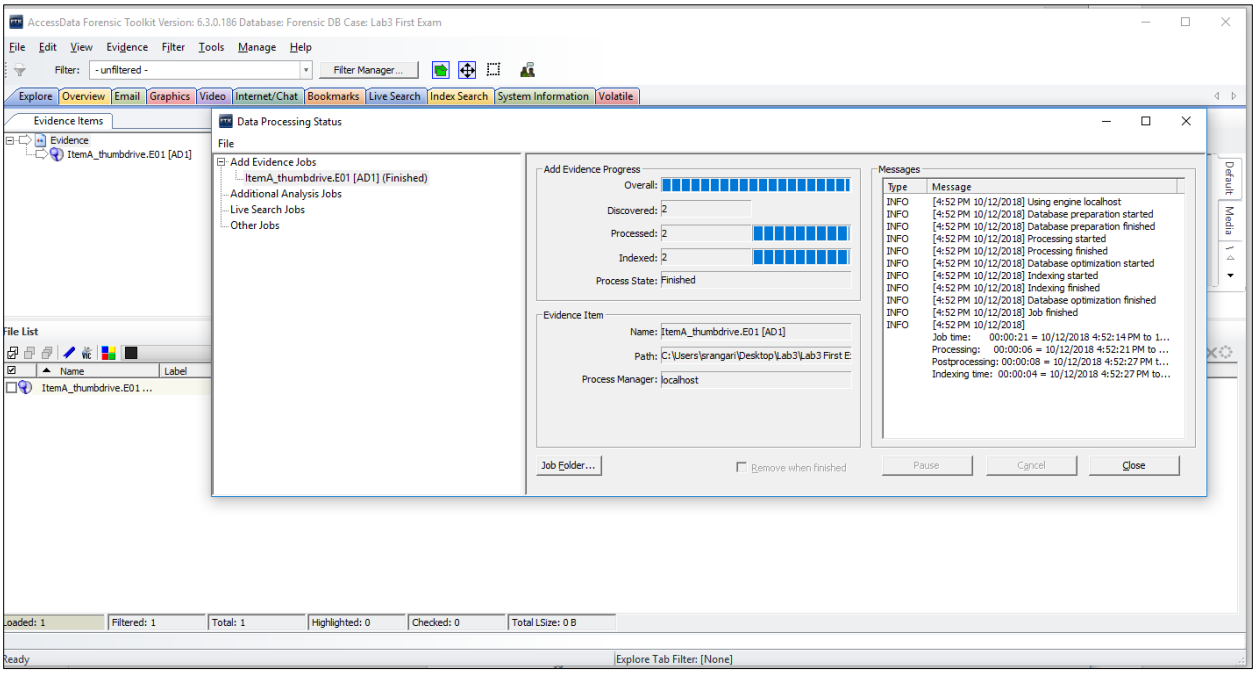
I loaded the forensic image which was made by officer Johns using subject's thumbdrive and used FTK Imager to verify hash.

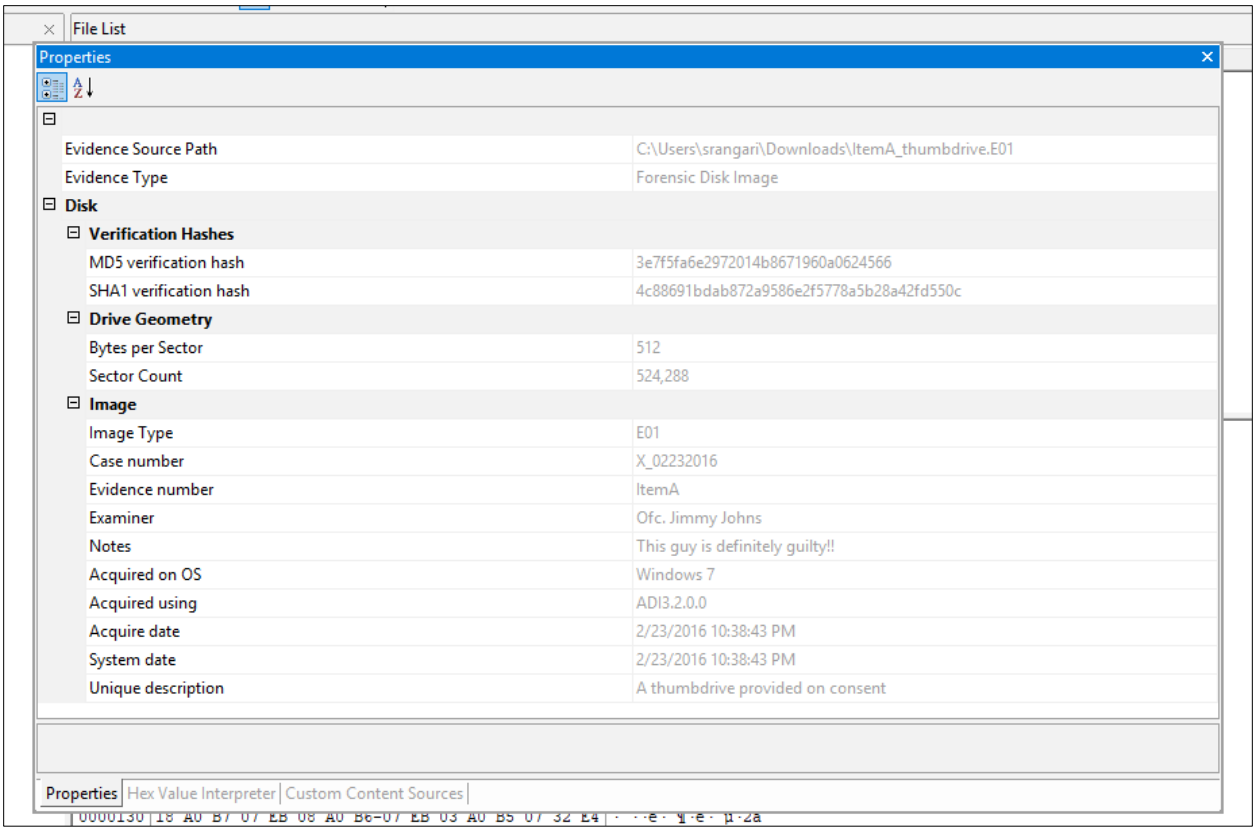


Where both the stored and computed hash value matched.

After that I created a new case in FTK by loading a ItemA_thumbdrive.E01 for evidence processing.

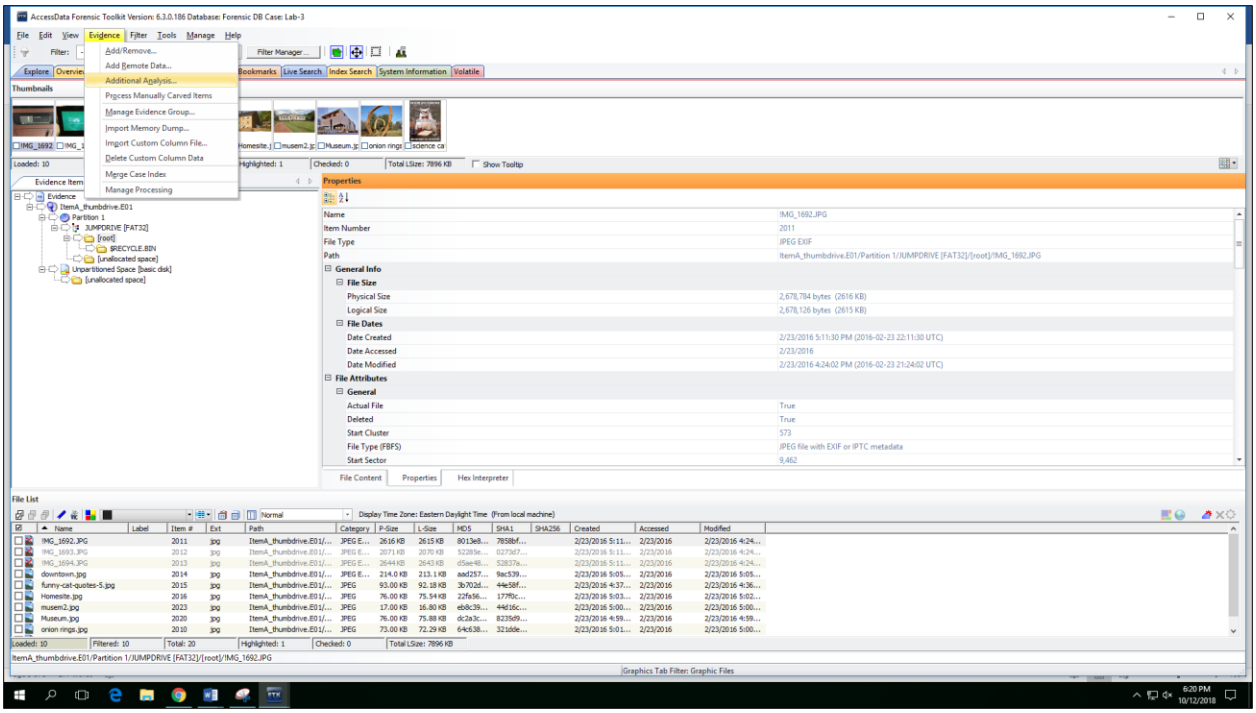

File Content
Manage Evidence
Display Name
State
ItemA_thumbdrive.E01
+
Path:
C:\Users\srangari\Downloads\ItemA_thumbdrive.E01
View Evidence Info...
ID / Name:
Description:
Evidence Group:
Manage...
Time Zone:
America/Indiana/Indianapolis
Merge case index
Use UNC Paths
Add
Remove
Choose Restore Points...
Refinement Options...
Language Setting...
Case KFF Options...
OK
Cancel

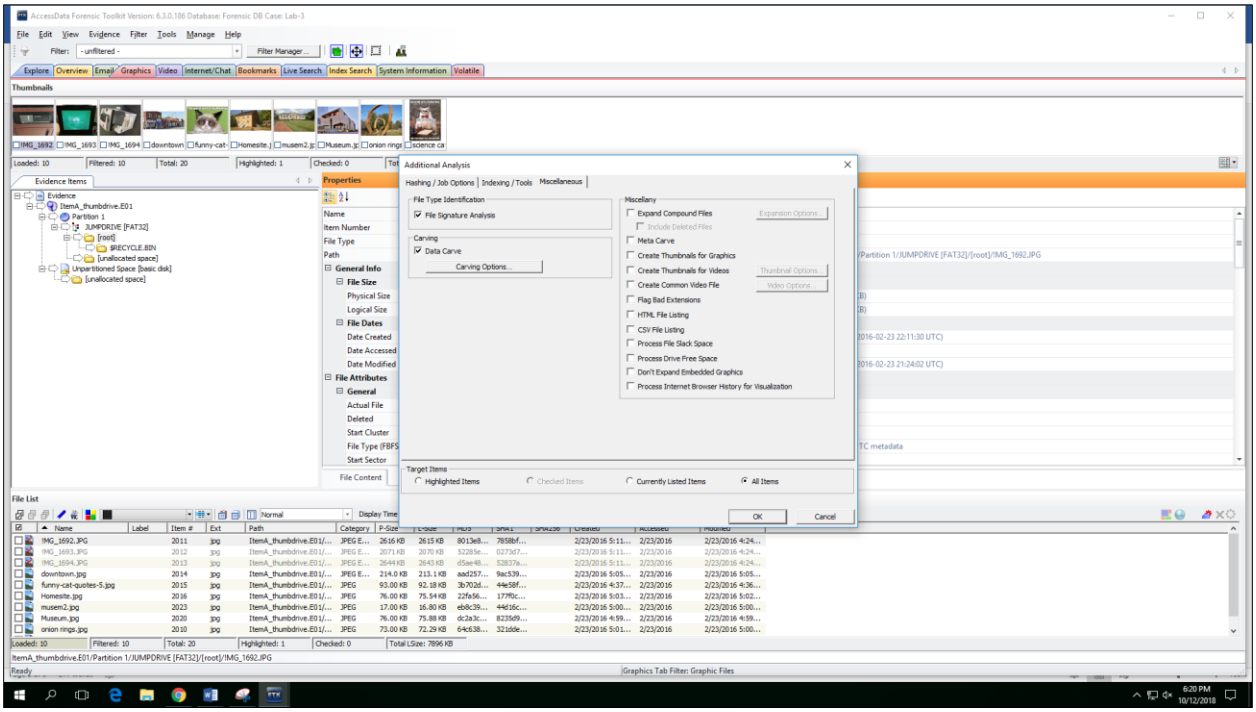

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3 First Exam
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Evidence Items
Evidence
ItemA_thumbdrive.E01 [AD1]
Data Processing Status
File
Add Evidence Jobs
ItemA_thumbdrive.E01 [AD1] (Finished)
Additional Analysis Jobs
Live Search Jobs
Other Jobs
Add Evidence Progress
Overall:
Discovered: 2
Processed: 2
Indexed: 2
Process State: Finished
Evidence Item
Name: ItemA_thumbdrive.E01 [AD1]
Path: C:\Users\srangari\Desktop\Lab3\Lab3 First E
Process Manager: localhost
Messages
Type
Message
INFO [4:52 PM 10/12/2018] Using engine localhost
INFO [4:52 PM 10/12/2018] Database preparation started
INFO [4:52 PM 10/12/2018] Database preparation finished
INFO [4:52 PM 10/12/2018] Processing started
INFO [4:52 PM 10/12/2018] Processing finished
INFO [4:52 PM 10/12/2018] Database optimization started
INFO [4:52 PM 10/12/2018] Indexing started
INFO [4:52 PM 10/12/2018] Indexing finished
INFO [4:52 PM 10/12/2018] Database optimization finished
INFO [4:52 PM 10/12/2018] Job finished
INFO [4:52 PM 10/12/2018]
Job time: 00:00:21 = 10/12/2018 4:52:14 PM to 1...
Processing: 00:00:06 = 10/12/2018 4:52:21 PM to ...
Postprocessing: 00:00:08 = 10/12/2018 4:52:27 PM t...
Indexing time: 00:00:04 = 10/12/2018 4:52:27 PM to...
Job Folder...
Remove when finished
Pause
Cancel
Close
File List
Name
Label
ItemA_thumbdrive.E01 ...
Loaded: 1
Filtered: 1
Total: 1
Highlighted: 0
Checked: 0
Total LSize: 0 B
Ready
Explore Tab Filter: [None]



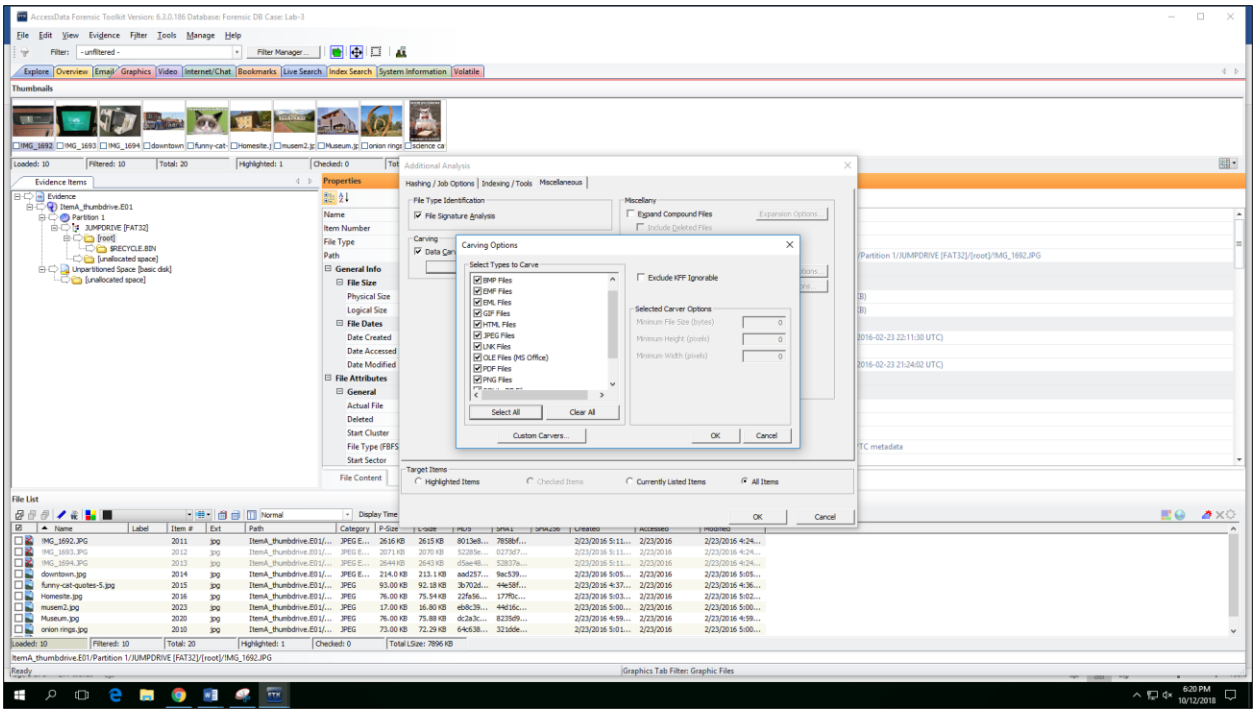
Findings and Report (Forensic Analysis)

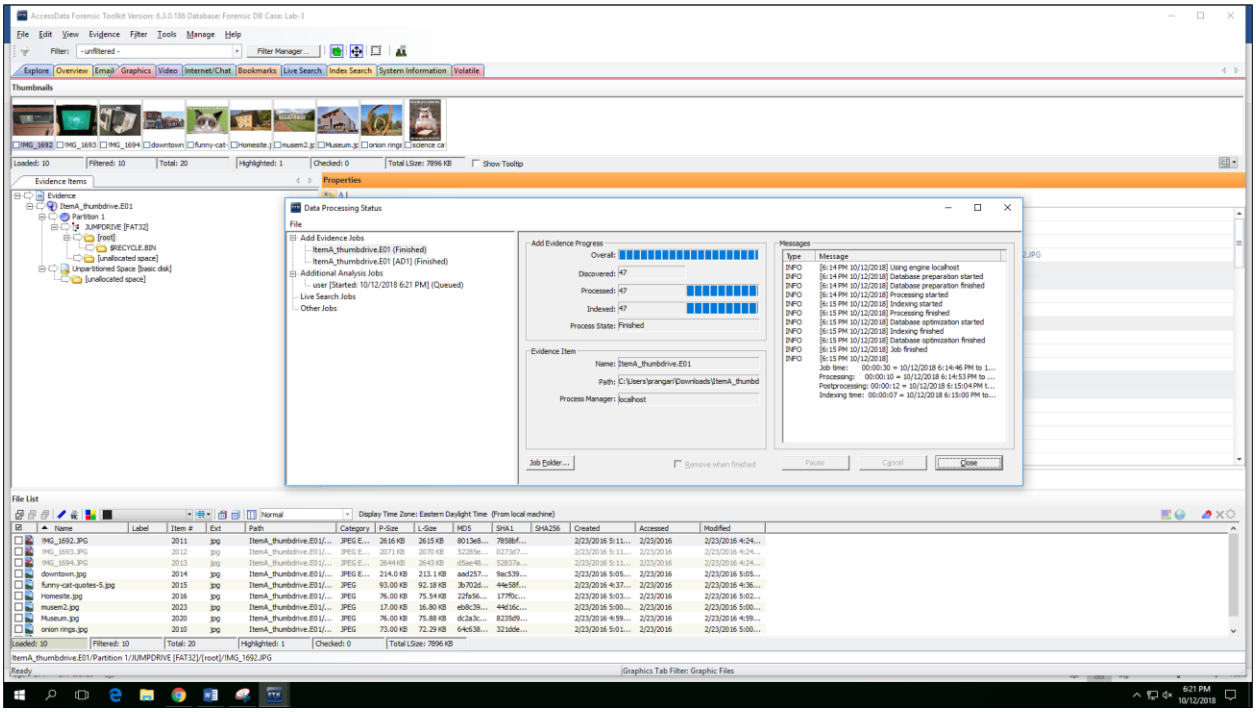
After loading the image into FTK, no pictures where found related to stolen items including Apple computers, Apple TVs, iPads and iPhones. Thus to investigate further I performed data **carving** operation which helps to look for data in the evidence that was deleted from the filesystem. To perform data carving I went to Evidence tab from where I performed Additional Analysis and selected Data carve option.





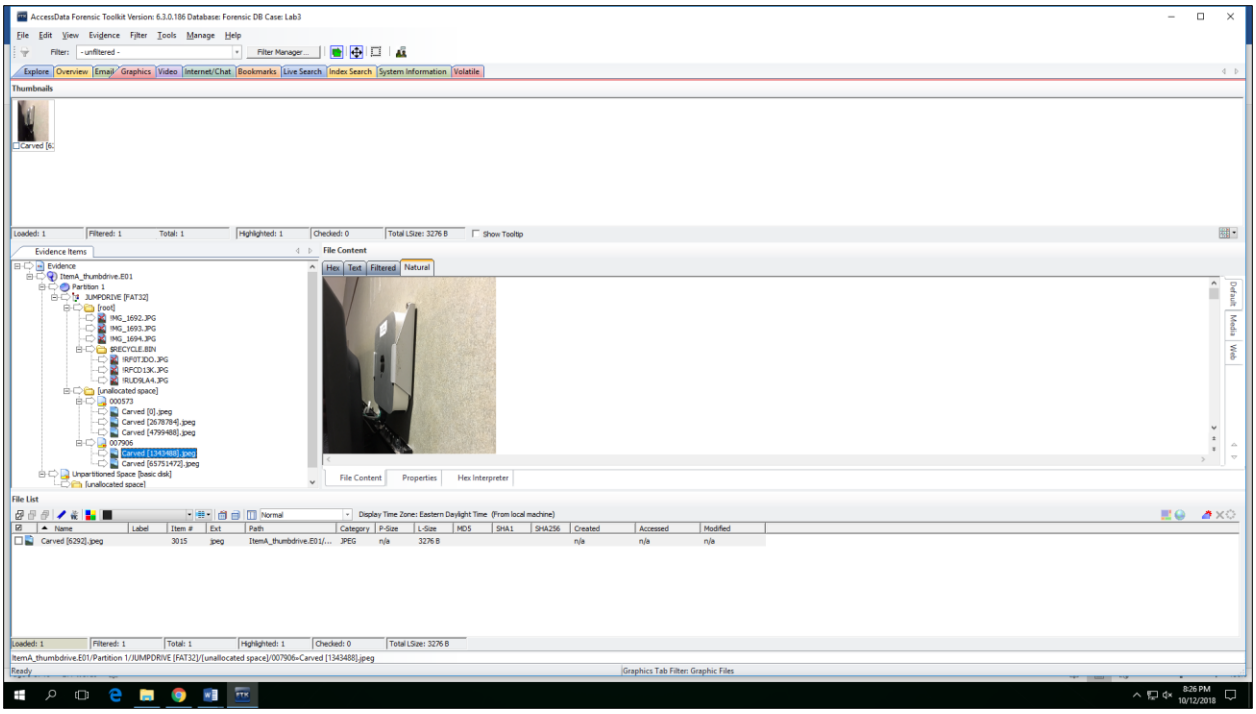
As I wanted to recover pictures of Apple device I selected all picture extension file options to carve.



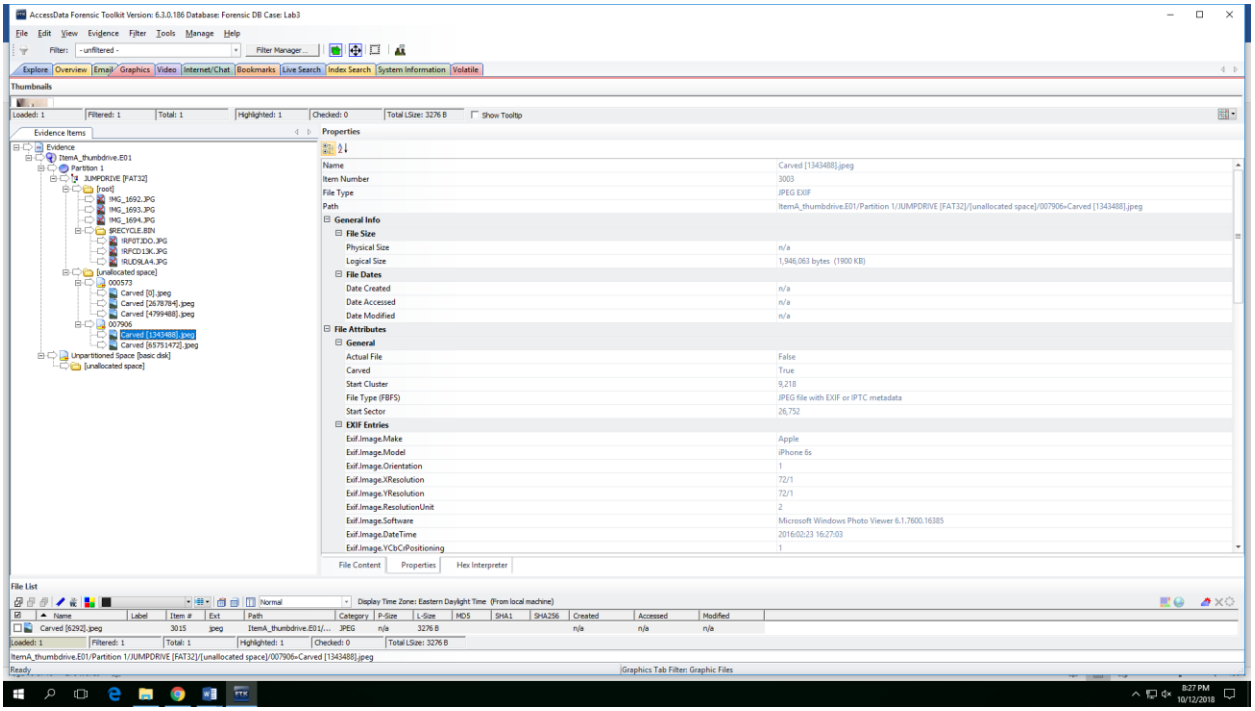


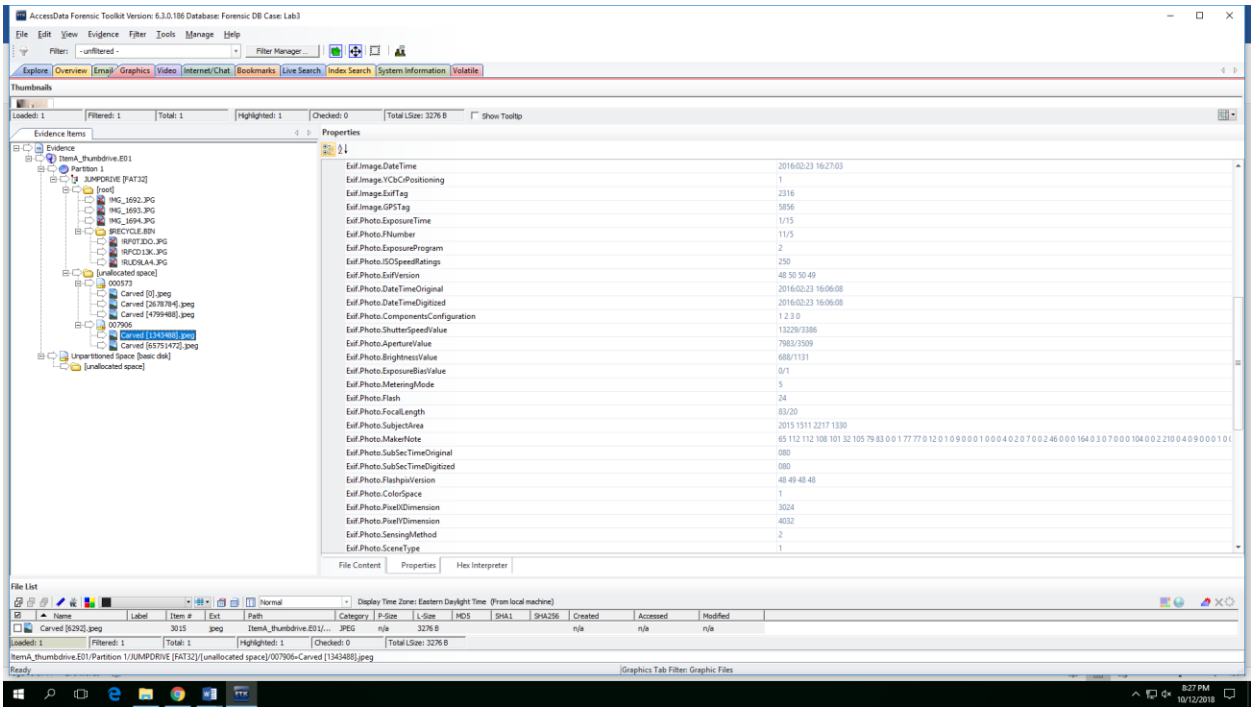
Thus, I recovered deleted pictures from the given image.

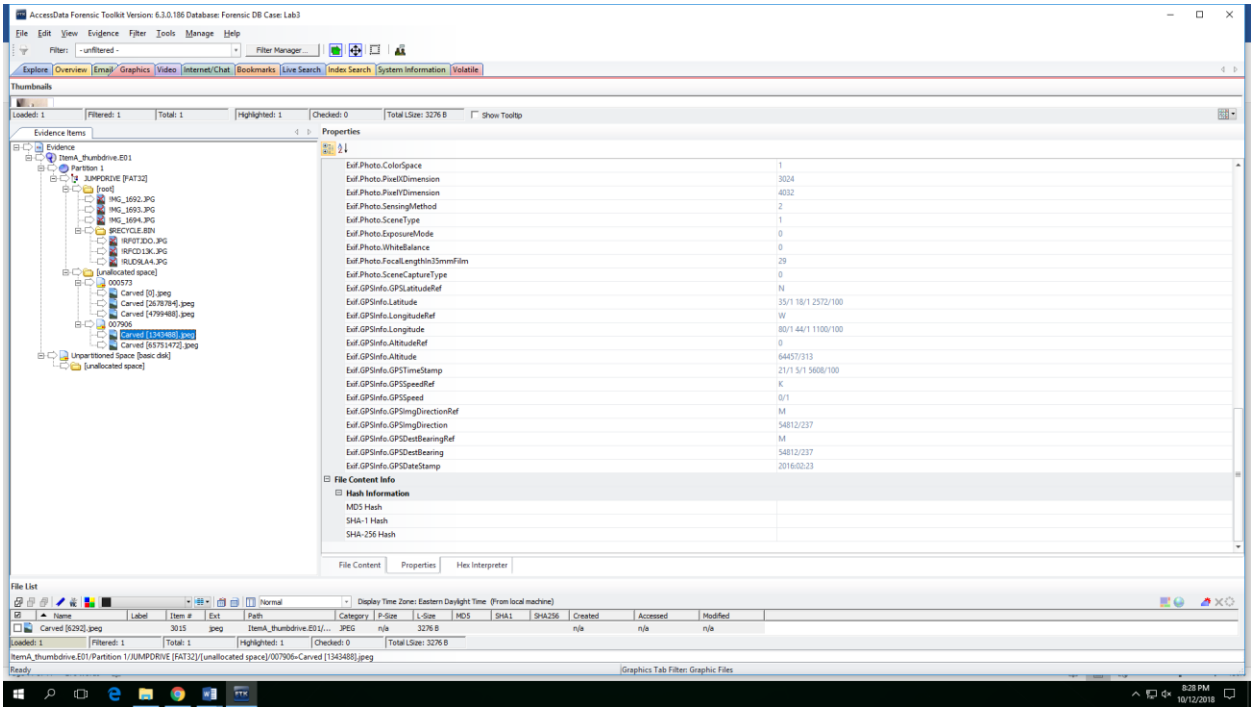
First Carved Image:



The following information was found after looking at **EXIF** information of these jpeg pictures under the properties tab:

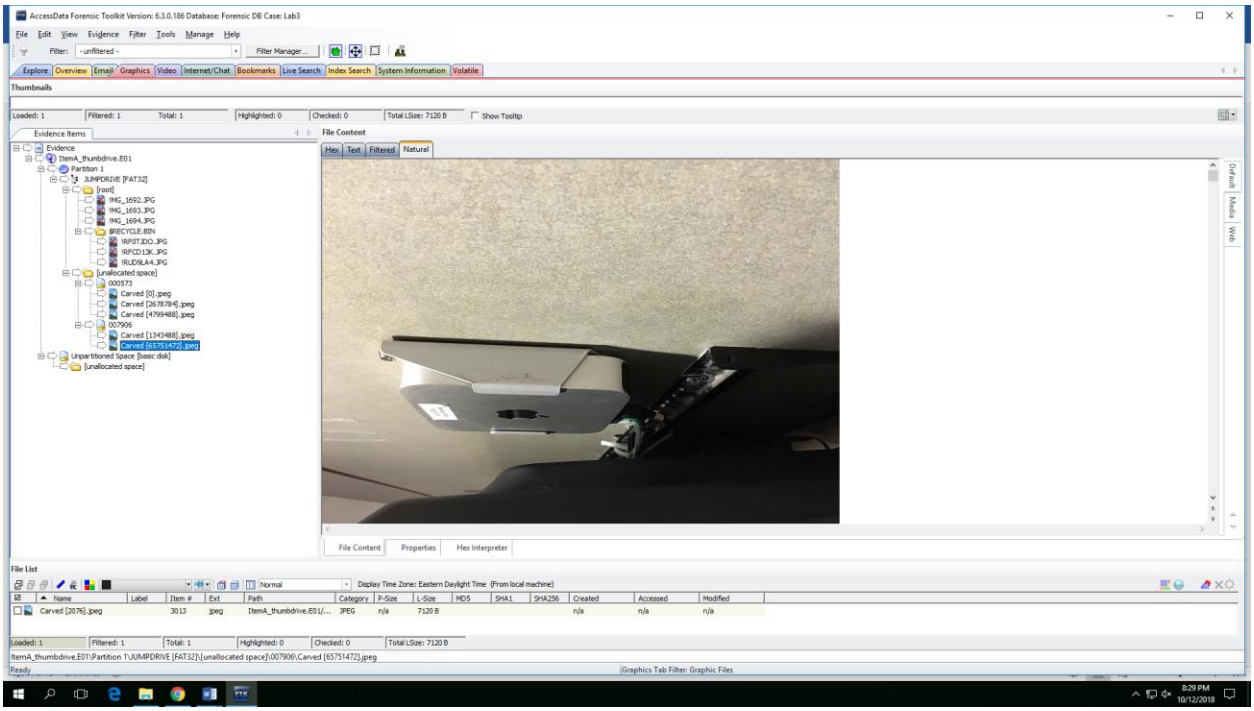


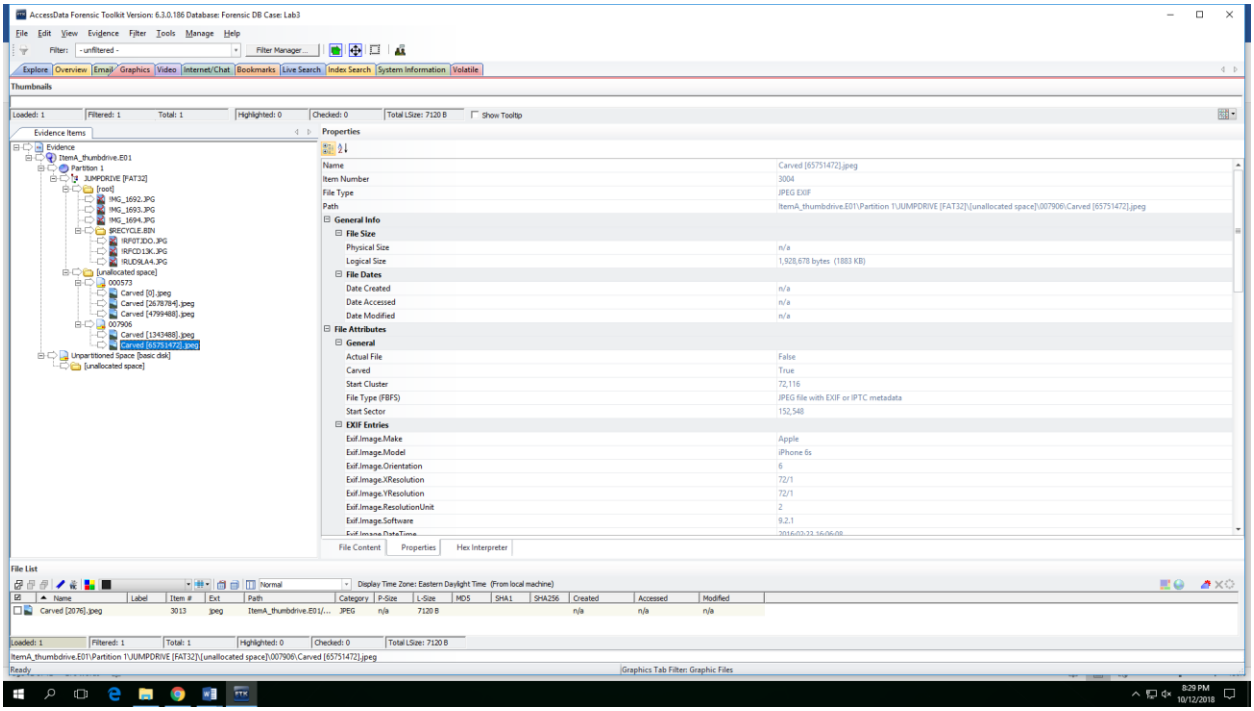


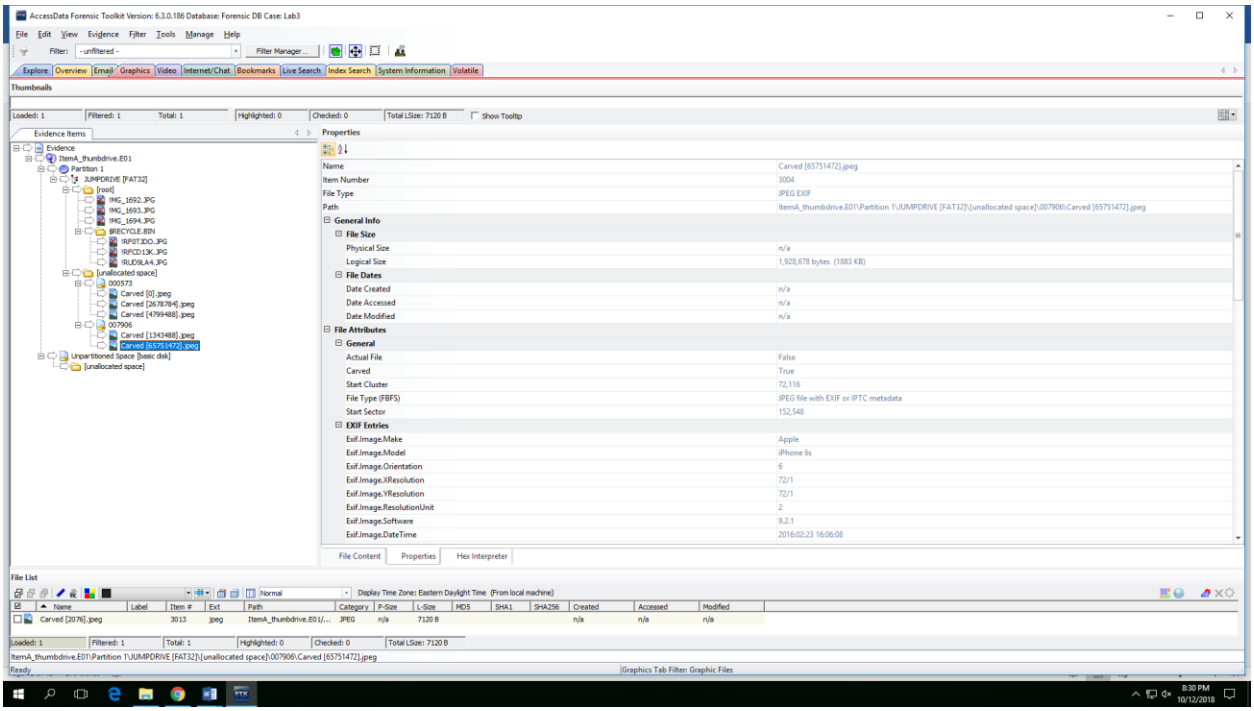


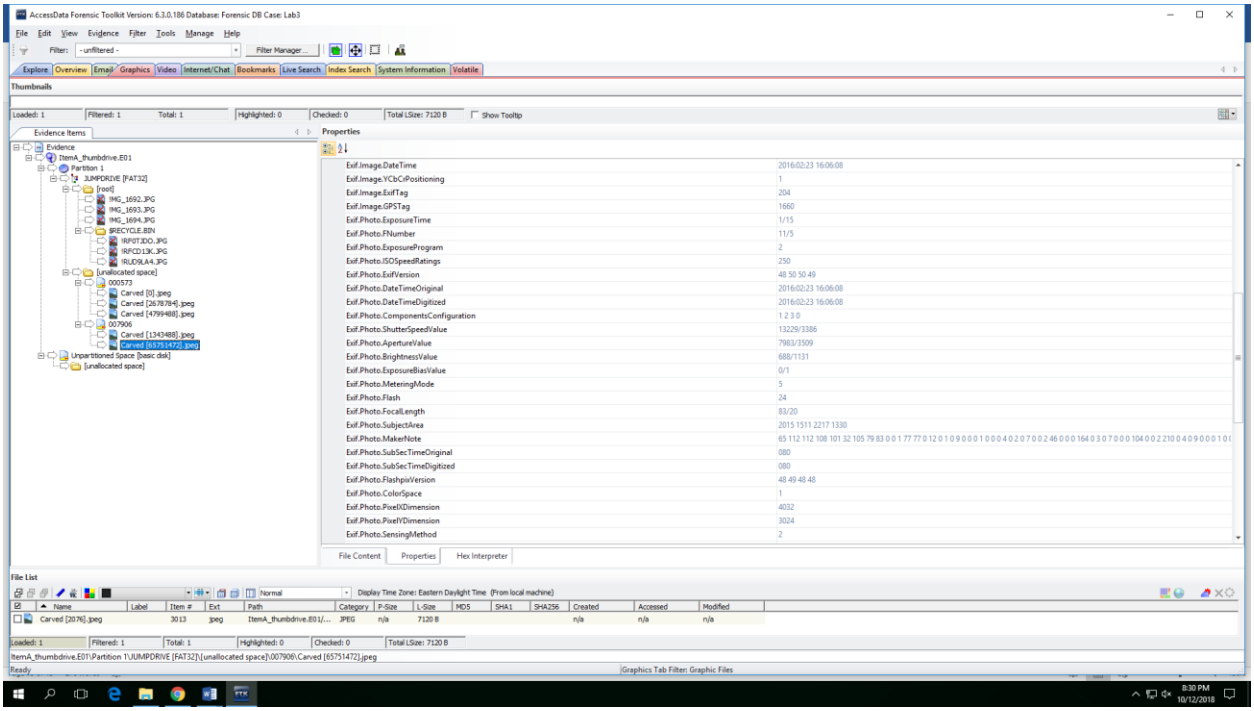
The above information shows **device model, date, time and GPS coordinates** of jpeg picture.

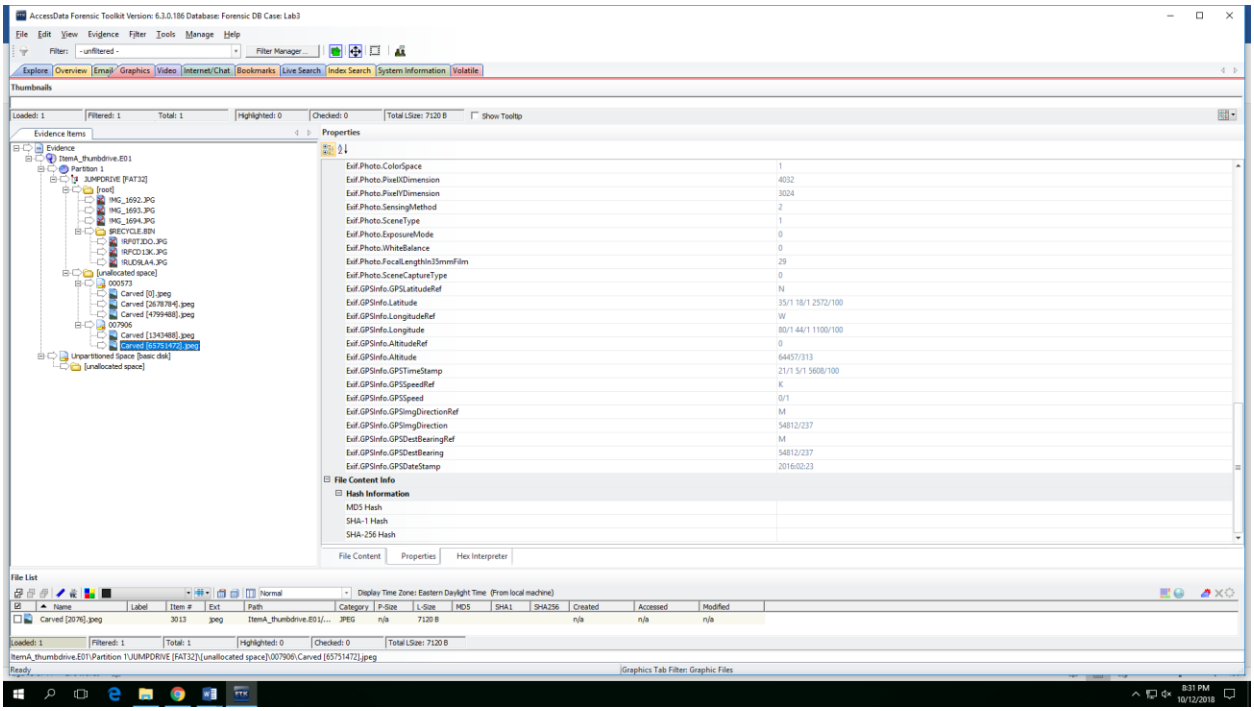
Second Carved Image:

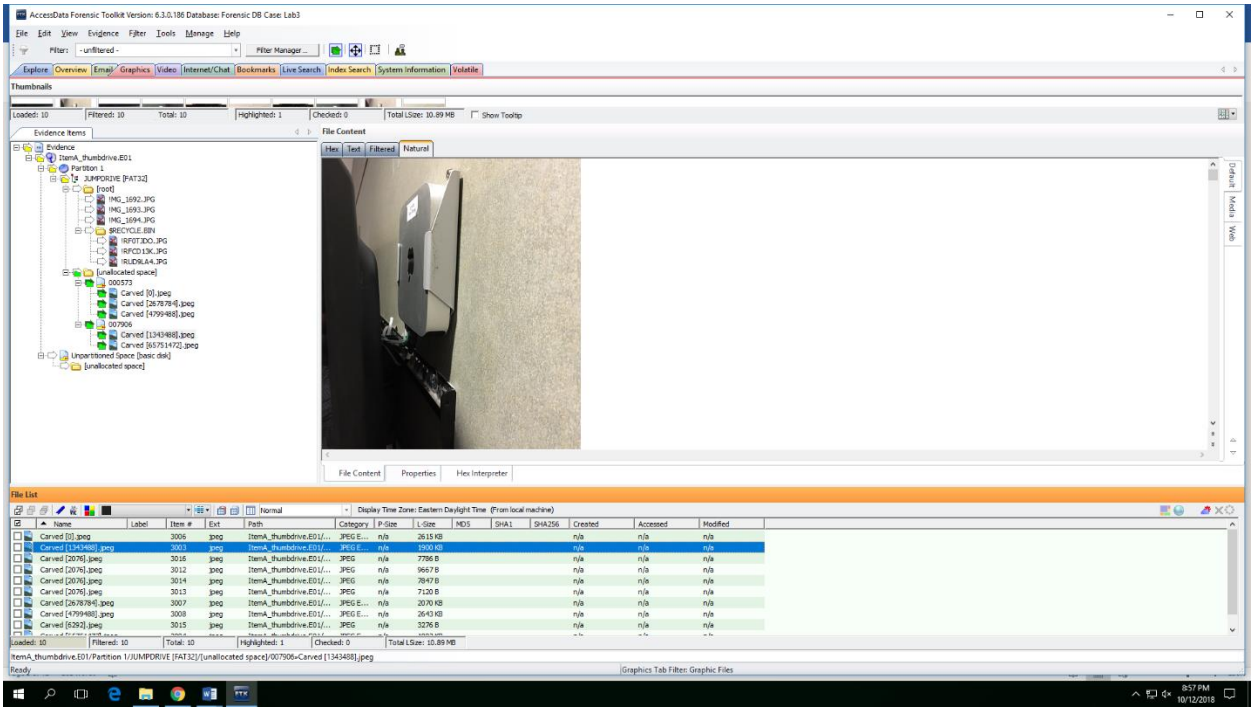

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
File Edit View Evidence Filter Tools Manage Help
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
Evidence Items
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Created Accessed Modified
Carved [2076].jpeg 3013 jpeg ItemA_thumbdrive.E01/... JPEG n/a 7120 B n/a n/a n/a
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[unallocated space]\007906\Carved [65751472].jpeg
Ready
Graphics Tab Filter: Graphic Files


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
File Edit View Evidence Filter Tools Manage Help
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
Evidence Items
Properties
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
File Size
Physical Size n/a
Logical Size 1,928,678 bytes (1883 KB)
File Dates
Date Created n/a
Date Accessed n/a
Date Modified n/a
File Attributes
General
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.Image.XResolution 72/1
Exif.Image.YResolution 72/1
Exif.Image.ResolutionUnit 2
Exif.Image.Software 9.2.1
File Content Properties Hex Interpreter
File List
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Created Accessed Modified
Carved [2076].jpeg 3013 jpeg ItemA_thumbdrive.E01/... JPEG n/a 7120 B n/a n/a n/a
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[unallocated space]\007906\Carved [65751472].jpeg
Ready
Graphics Tab Filter: Graphic Files

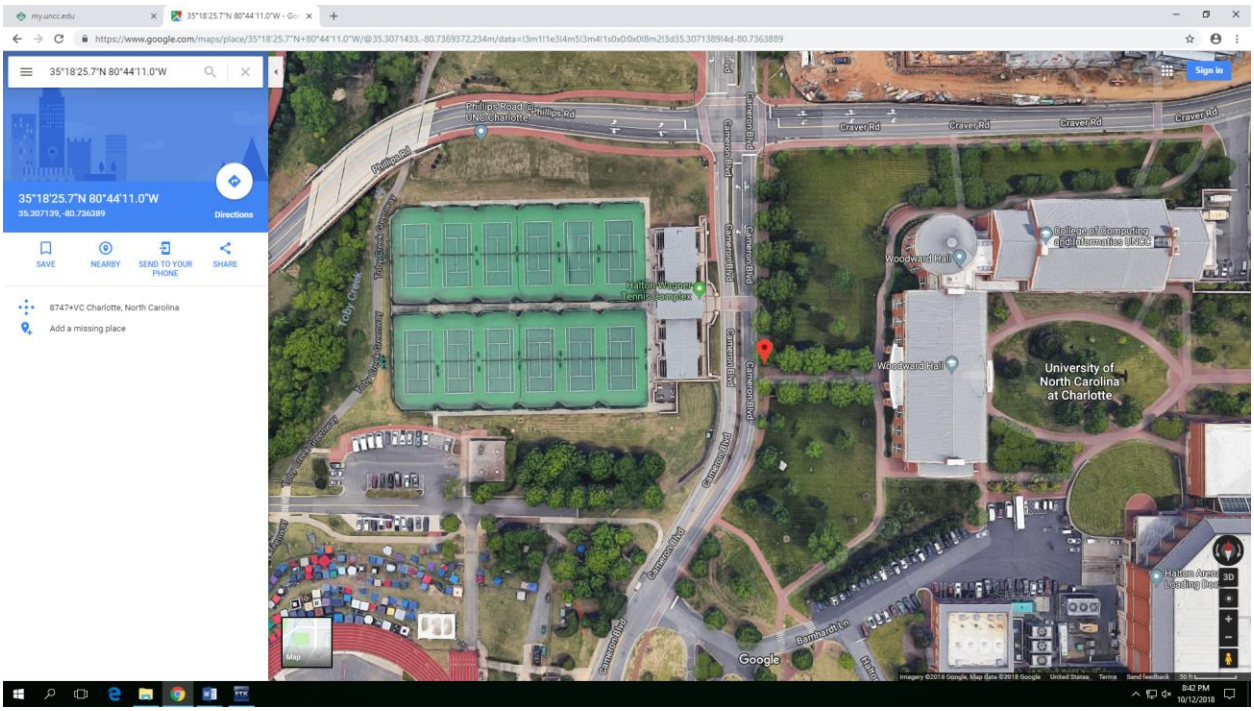

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
File Edit View Evidence Filter Tools Manage Help
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
Evidence Items
Properties
Name Carved [65751472].jpeg
Item Number 3004
File Type JPEG EXIF
Path ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[unallocated space]\007906\Carved [65751472].jpeg
General Info
File Size
Physical Size n/a
Logical Size 1,928,678 bytes (1883 KB)
File Dates
Date Created n/a
Date Accessed n/a
Date Modified n/a
File Attributes
General
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.Image.XResolution 72/1
Exif.Image.YResolution 72/1
Exif.Image.ResolutionUnit 2
Exif.Image.Software 9.2.1
Exif.Image.DateTime 2016:02:23 16:06:08
File Content Properties Hex Interpreter
File List
Carved [2076].jpeg 3013 jpeg ItemA_thumbdrive.E01/... JPEG n/a 7120 B n/a n/a n/a
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[unallocated space]\007906\Carved [65751472].jpeg
Graphics Tab Filter: Graphic Files
8:30 PM 10/12/2018


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
Properties
Exif.Image.DateTime 2016:02:23 16:06:08
Exif.Image.YCbCrPositioning 1
Exif.Image.ExifTag 204
Exif.Image.GPSTag 1660
Exif.Photo.ExposureTime 1/15
Exif.Photo.FNumber 11/5
Exif.Photo.ExposureProgram 2
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
Exif.Photo.BrightnessValue 688/1131
Exif.Photo.ExposureBiasValue 0/1
Exif.Photo.MeteringMode 5
Exif.Photo.Flash 24
Exif.Photo.FocalLength 83/20
Exif.Photo.SubjectArea 2015 1511 2217 1330
Exif.Photo.MakerNote 65 112 112 108 101 32 105 79 83 0 0 1 77 77 0 12 0 1 0 9 0 0 0 1 0 0 0 4 0 2 0 7 0 0 2 46 0 0 0 164 0 3 0 7 0 0 0 104 0 0 2 210 0 4 0 9 0 0 0 1 0 (
Exif.Photo.SubSecTimeOriginal 080
Exif.Photo.SubSecTimeDigitized 080
Exif.Photo.FlashpixVersion 48 49 48 48
Exif.Photo.ColorSpace 1
Exif.Photo.PixelXDimension 4032
Exif.Photo.PixelYDimension 3024
Exif.Photo.SensingMethod 2
File Content Properties Hex Interpreter
File List
Carved [2076].jpeg 3013 jpeg ItemA_thumbdrive.E01/... JPEG n/a 7120 B n/a n/a n/a
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[unallocated space]\007906\Carved [65751472].jpeg
Graphics Tab Filter: Graphic Files
8:30 PM 10/12/2018



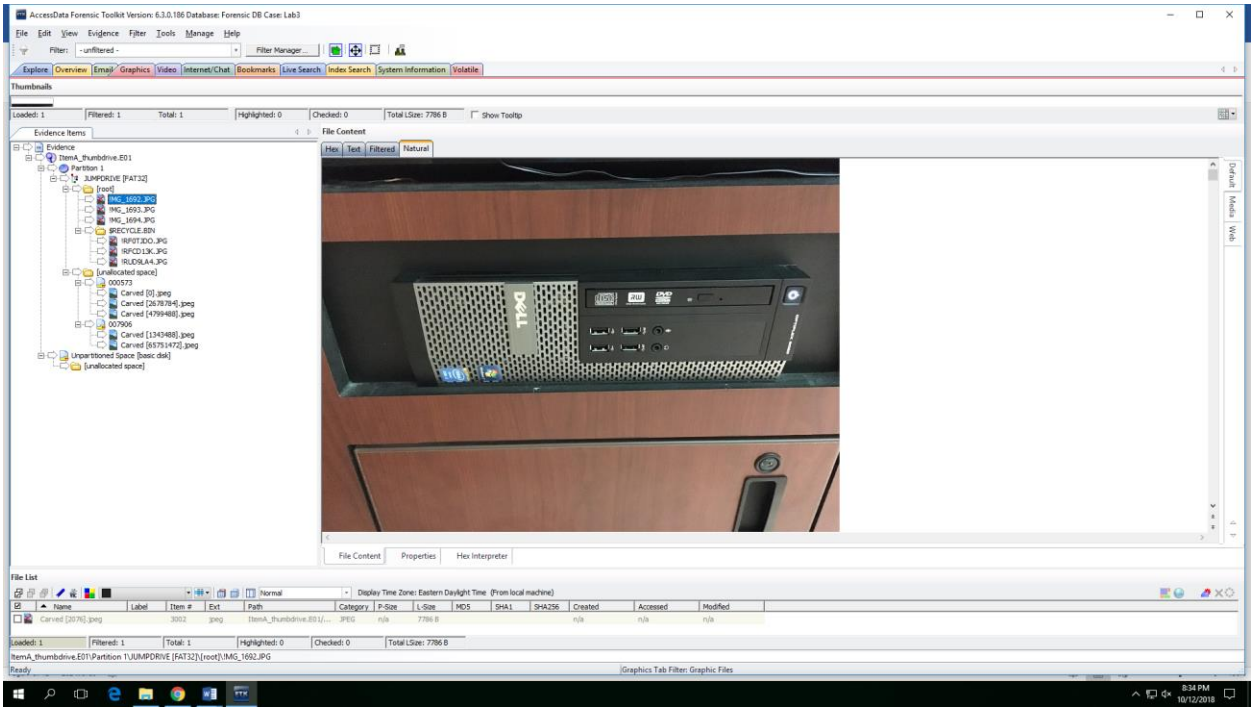


Later, I fed these coordinates into google maps and found that these jpeg pictures were captured at the following location:

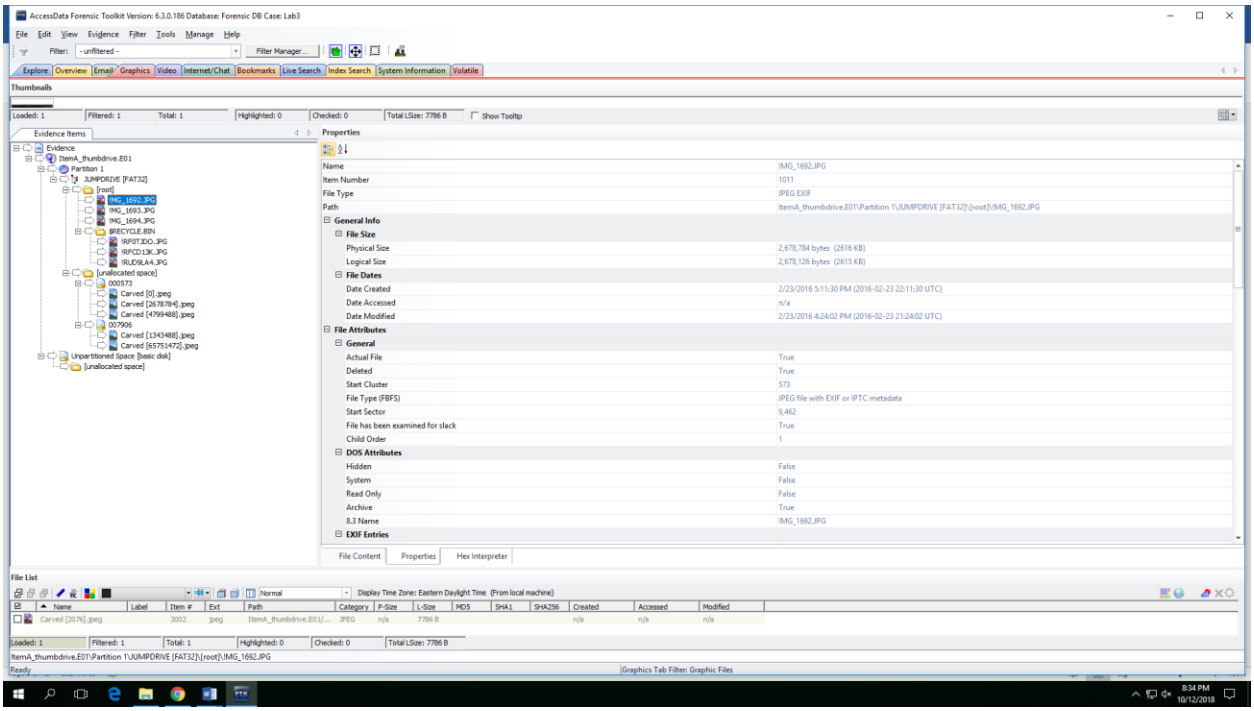


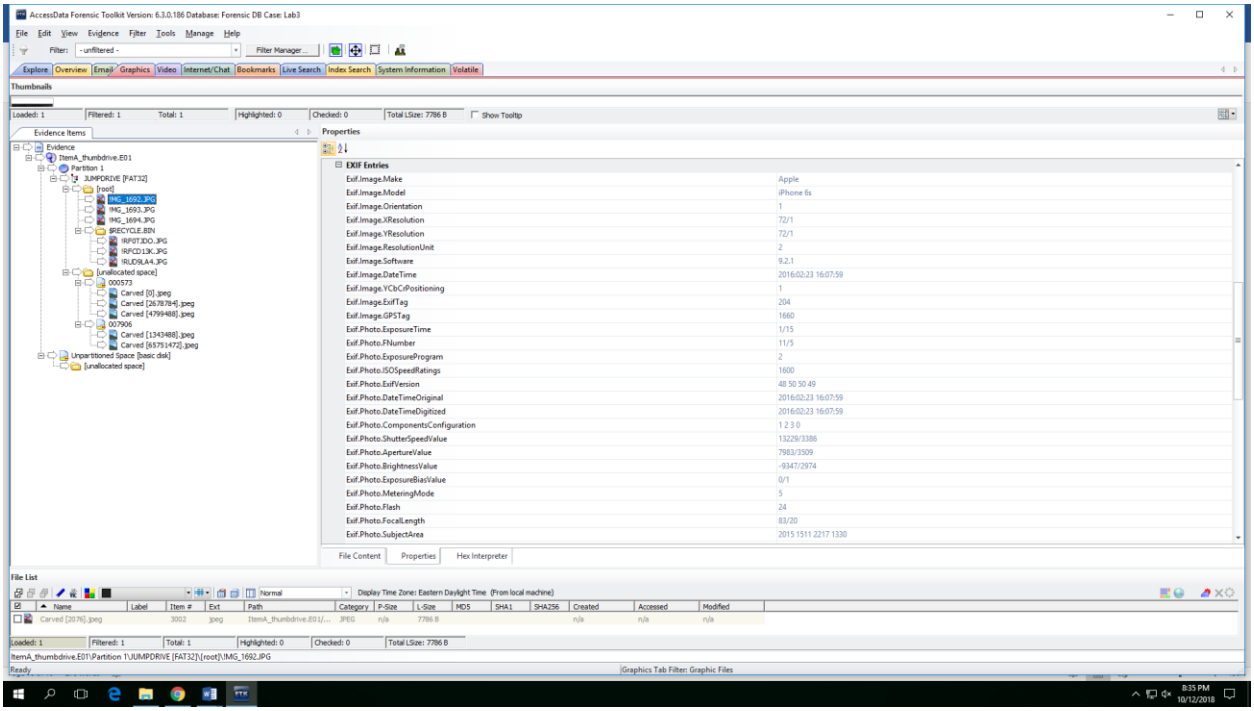
In the FTK, I also found **3** jpeg pictures in the recycle bin.

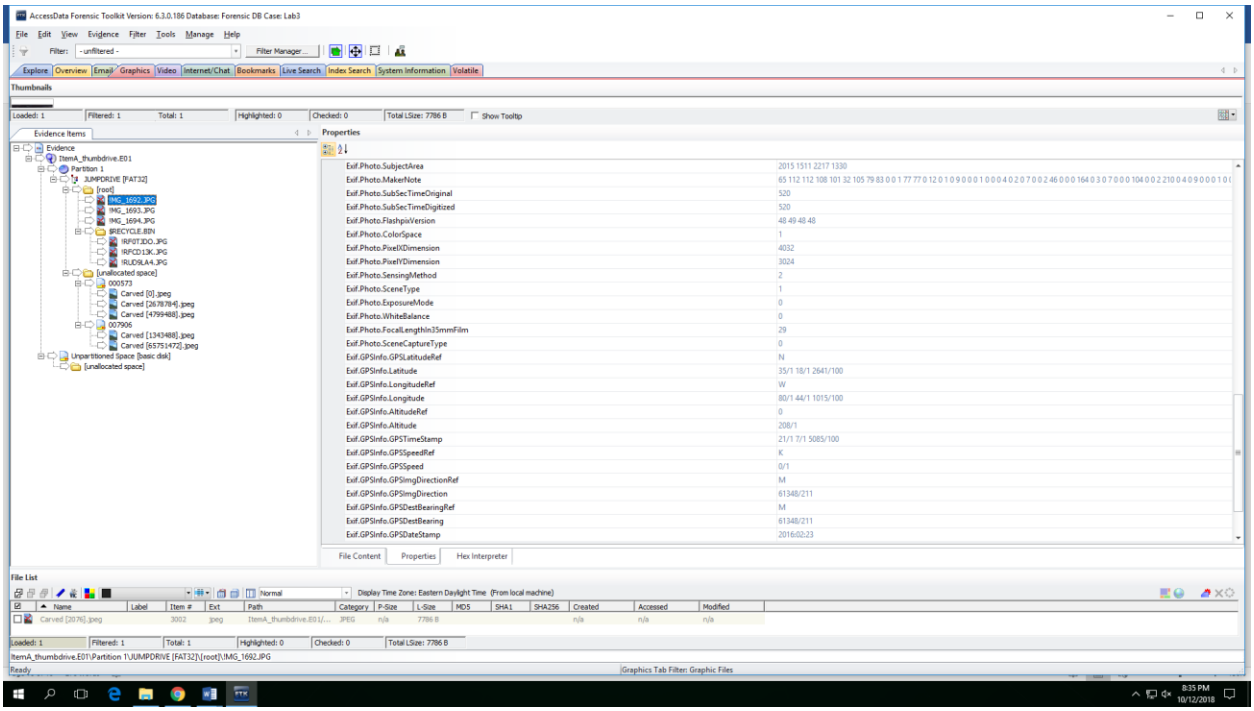
Image 1:



EXIF information of Image 1:


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
Properties
Name IMG_1692.JPG
Item Number 1011
File Type JPEG EXIF
Path ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[root]\IMG_1692.JPG
General Info
File Size
Physical Size 2,678,784 bytes (2616 KB)
Logical Size 2,678,126 bytes (2615 KB)
File Dates
Date Created 2/23/2016 5:11:30 PM (2016-02-23 22:11:30 UTC)
Date Accessed n/a
Date Modified 2/23/2016 4:24:02 PM (2016-02-23 21:24:02 UTC)
File Attributes
General
Actual File True
Deleted True
Start Cluster 573
File Type (FBFS) JPEG file with EXIF or IPTC metadata
Start Sector 9,462
File has been examined for slack True
Child Order 1
DOS Attributes
Hidden False
System False
Read Only False
Archive True
8.3 Name IMG_1692.JPG
EXIF Entries
File Content
Properties
Hex Interpreter
File List
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[root]\IMG_1692.JPG
8:34 PM
10/12/2018


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
Properties
EXIF Entries
Exif.Image.Make Apple
Exif.Image.Model iPhone 6s
Exif.Image.Orientation 1
Exif.Image.XResolution 72/1
Exif.Image.YResolution 72/1
Exif.Image.ResolutionUnit 2
Exif.Image.Software 9.2.1
Exif.Image.DateTime 2016:02:23 16:07:59
Exif.Image.YCbCrPositioning 1
Exif.Image.ExifTag 204
Exif.Image.GPSTag 1660
Exif.Photo.ExposureTime 1/15
Exif.Photo.FNumber 11/5
Exif.Photo.ExposureProgram 2
Exif.Photo.ISOSpeedRatings 1600
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.ShutterSpeedValue 13229/3386
Exif.Photo.ApertureValue 7983/3509
Exif.Photo.BrightnessValue -9347/2974
Exif.Photo.ExposureBiasValue 0/1
Exif.Photo.MeteringMode 5
Exif.Photo.Flash 24
Exif.Photo.FocalLength 83/20
Exif.Photo.SubjectArea 2015 1511 2217 1330
File Content
Properties
Hex Interpreter
File List
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[root]\IMG_1692.JPG
8:35 PM
10/12/2018


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
File Edit View Evidence Filter Tools Manage Help
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
Evidence Items
Properties
Exif.Photo.SubjectArea 2015 1511 2217 1330
Exif.Photo.MakerNote 65 112 112 108 101 32 105 79 83 0 0 1 77 77 0 12 0 1 0 9 0 0 0 1 0 0 0 4 0 2 0 7 0 0 2 46 0 0 0 164 0 3 0 7 0 0 0 104 0 0 2 210 0 4 0 9 0 0 0 1 0 (
Exif.Photo.SubSecTimeOriginal 520
Exif.Photo.SubSecTimeDigitized 520
Exif.Photo.FlashpixVersion 48 49 48 48
Exif.Photo.ColorSpace 1
Exif.Photo.PixelXDimension 4032
Exif.Photo.PixelYDimension 3024
Exif.Photo.SensingMethod 2
Exif.Photo.SceneType 1
Exif.Photo.ExposureMode 0
Exif.Photo.WhiteBalance 0
Exif.Photo.FocalLengthIn35mmFilm 29
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
Exif.GPSInfo.GPSSpeedRef K
Exif.GPSInfo.GPSSpeed 0/1
Exif.GPSInfo.GPSImgDirectionRef M
Exif.GPSInfo.GPSImgDirection 61348/211
Exif.GPSInfo.GPSDestBearingRef M
Exif.GPSInfo.GPSDestBearing 61348/211
Exif.GPSInfo.GPSDateStamp 2016:02:23
File Content Properties Hex Interpreter
File List
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[root]\IMG_1692.JPG
Ready
Graphics Tab Filter: Graphic Files

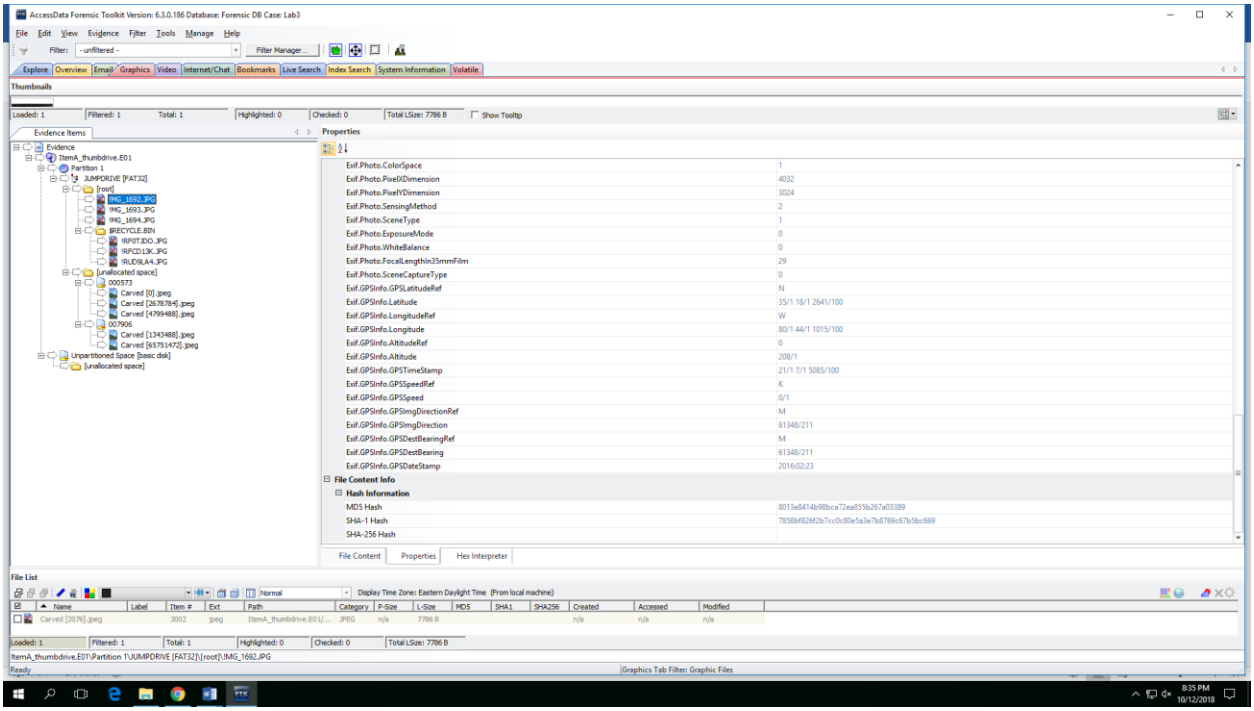
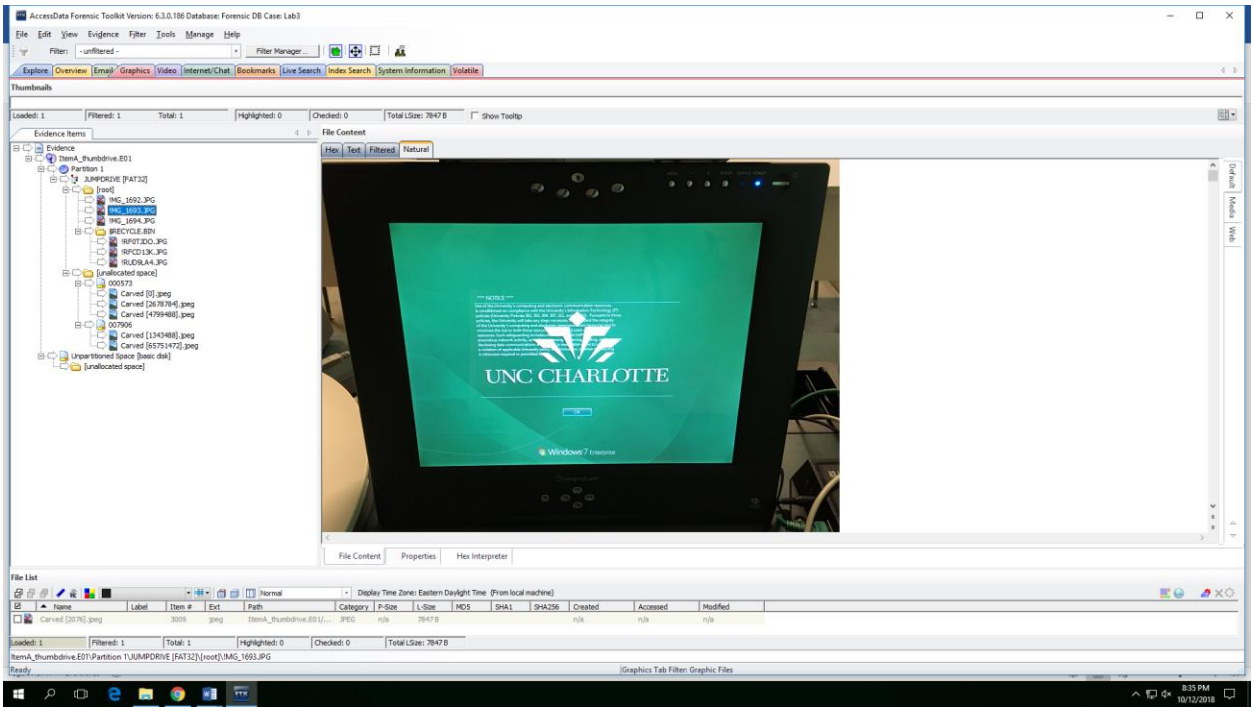
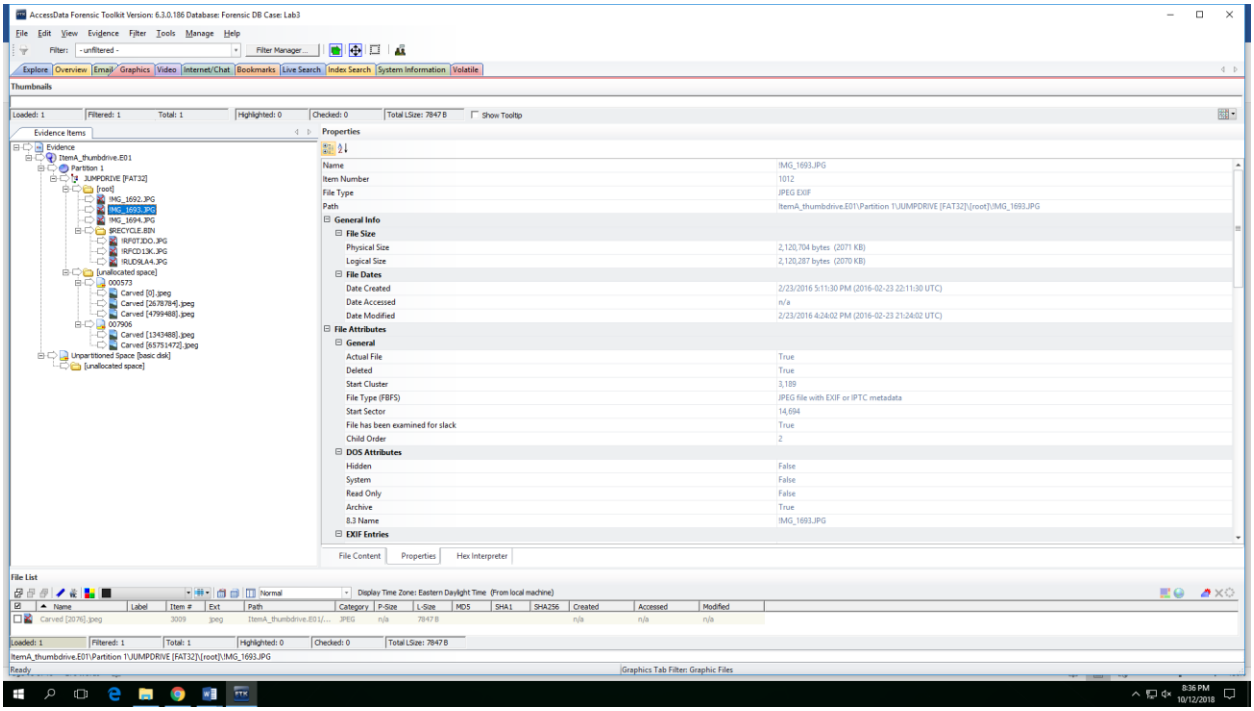
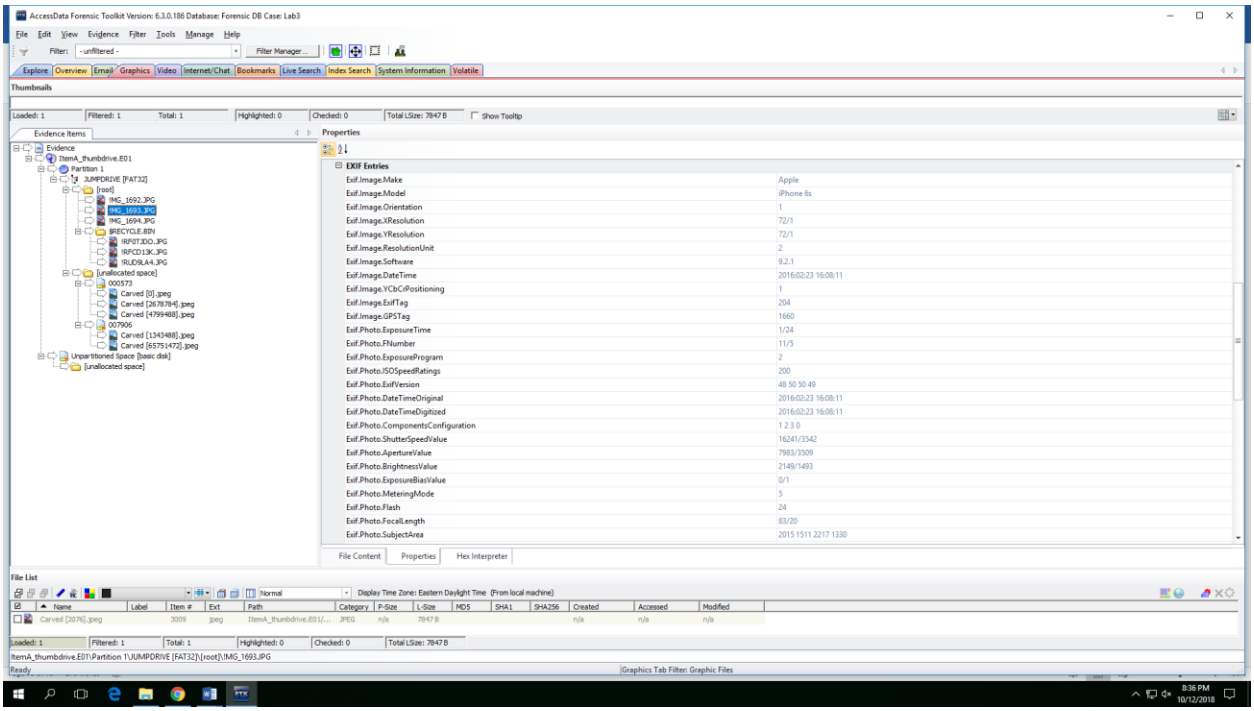

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
File Edit View Evidence Filter Tools Manage Help
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
Evidence Items
Properties
Exif.Photo.ColorSpace 1
Exif.Photo.PixelXDimension 4032
Exif.Photo.PixelYDimension 3024
Exif.Photo.SensingMethod 2
Exif.Photo.SceneType 1
Exif.Photo.ExposureMode 0
Exif.Photo.WhiteBalance 0
Exif.Photo.FocalLengthIn35mmFilm 29
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
Exif.GPSInfo.GPSSpeedRef K
Exif.GPSInfo.GPSSpeed 0/1
Exif.GPSInfo.GPSImgDirectionRef M
Exif.GPSInfo.GPSImgDirection 61348/211
Exif.GPSInfo.GPSDestBearingRef M
Exif.GPSInfo.GPSDestBearing 61348/211
Exif.GPSInfo.GPSDateStamp 2016:02:23
File Content Info
Hash Information
MD5 Hash 8013e8414b98bca72ea855b267a03389
SHA-1 Hash 7858bf826f2b7cc0c80e5a3e7b8769c67b5bc669
SHA-256 Hash
File Content Properties Hex Interpreter
File List
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[root]\IMG_1692.JPG
Ready
Graphics Tab Filter: Graphic Files

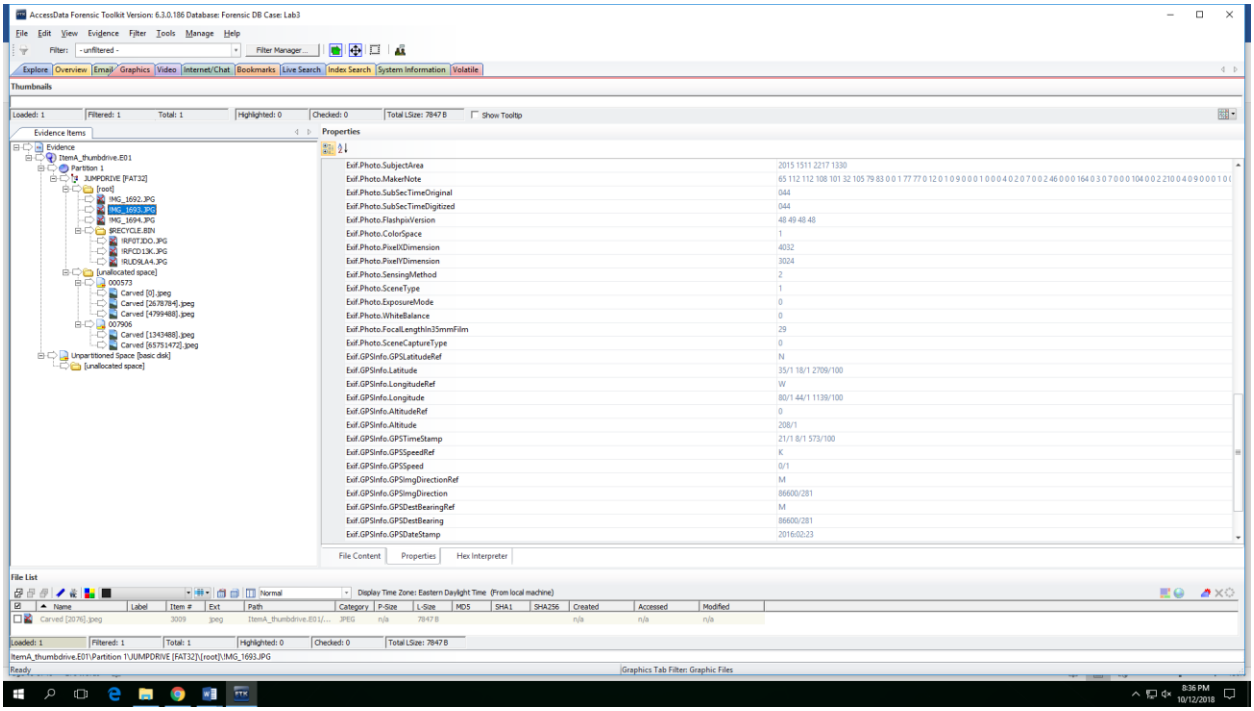
Image 2:



EXIF information of Image 2:




AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
File Edit View Evidence Filter Tools Manage Help
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
Evidence Items
Properties
EXIF Entries
Exif.Image.Make Apple
Exif.Image.Model iPhone 6s
Exif.Image.Orientation 1
Exif.Image.XResolution 72/1
Exif.Image.YResolution 72/1
Exif.Image.ResolutionUnit 2
Exif.Image.Software 9.2.1
Exif.Image.DateTime 2016:02:23 16:08:11
Exif.Image.YCbCrPositioning 1
Exif.Image.ExifTag 204
Exif.Image.GPSTag 1660
Exif.Photo.ExposureTime 1/24
Exif.Photo.FNumber 11/5
Exif.Photo.ExposureProgram 2
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.ShutterSpeedValue 16241/3542
Exif.Photo.ApertureValue 7983/3509
Exif.Photo.BrightnessValue 2149/1493
Exif.Photo.ExposureBiasValue 0/1
Exif.Photo.MeteringMode 5
Exif.Photo.Flash 24
Exif.Photo.FocalLength 83/20
Exif.Photo.SubjectArea 2015 1511 2217 1330
File Content Properties Hex Interpreter
File List
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[root]\IMG_1693.JPG
Ready
Graphics Tab Filter: Graphic Files
8:36 PM
10/12/2018


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
File Edit View Evidence Filter Tools Manage Help
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
Evidence Items
Properties
Exif.Photo.SubjectArea 2015 1511 2217 1330
Exif.Photo.MakerNote 65 112 112 108 101 32 105 79 83 0 0 1 77 77 0 12 0 1 0 9 0 0 0 1 0 0 0 4 0 2 0 7 0 0 2 46 0 0 0 164 0 3 0 7 0 0 0 104 0 0 2 210 0 4 0 9 0 0 0 1 0 (
Exif.Photo.SubSecTimeOriginal 044
Exif.Photo.SubSecTimeDigitized 044
Exif.Photo.FlashpixVersion 48 49 48 48
Exif.Photo.ColorSpace 1
Exif.Photo.PixelXDimension 4032
Exif.Photo.PixelYDimension 3024
Exif.Photo.SensingMethod 2
Exif.Photo.SceneType 1
Exif.Photo.ExposureMode 0
Exif.Photo.WhiteBalance 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
Exif.GPSInfo.GPSImgDirectionRef M
Exif.GPSInfo.GPSImgDirection 86600/281
Exif.GPSInfo.GPSDestBearingRef M
Exif.GPSInfo.GPSDestBearing 86600/281
Exif.GPSInfo.GPSDateStamp 2016:02:23
File Content Properties Hex Interpreter
File List
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[root]\IMG_1693.JPG
Ready
Graphics Tab Filter: Graphic Files
8:36 PM
10/12/2018

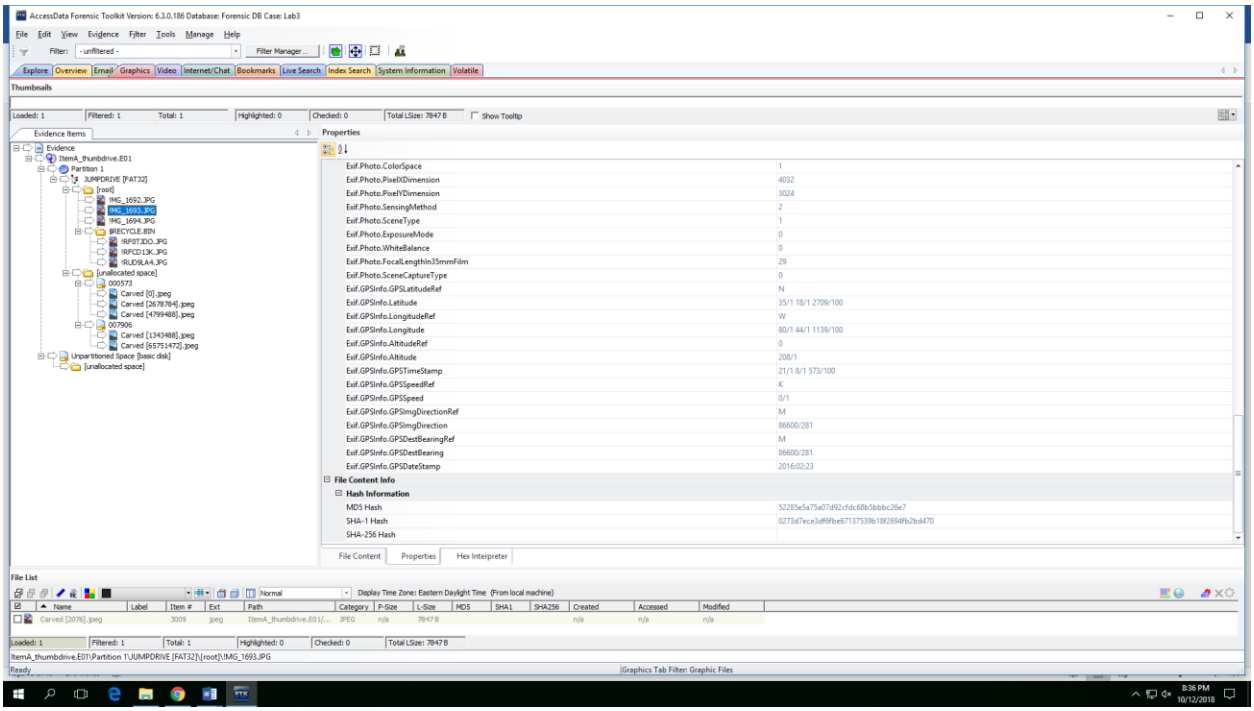
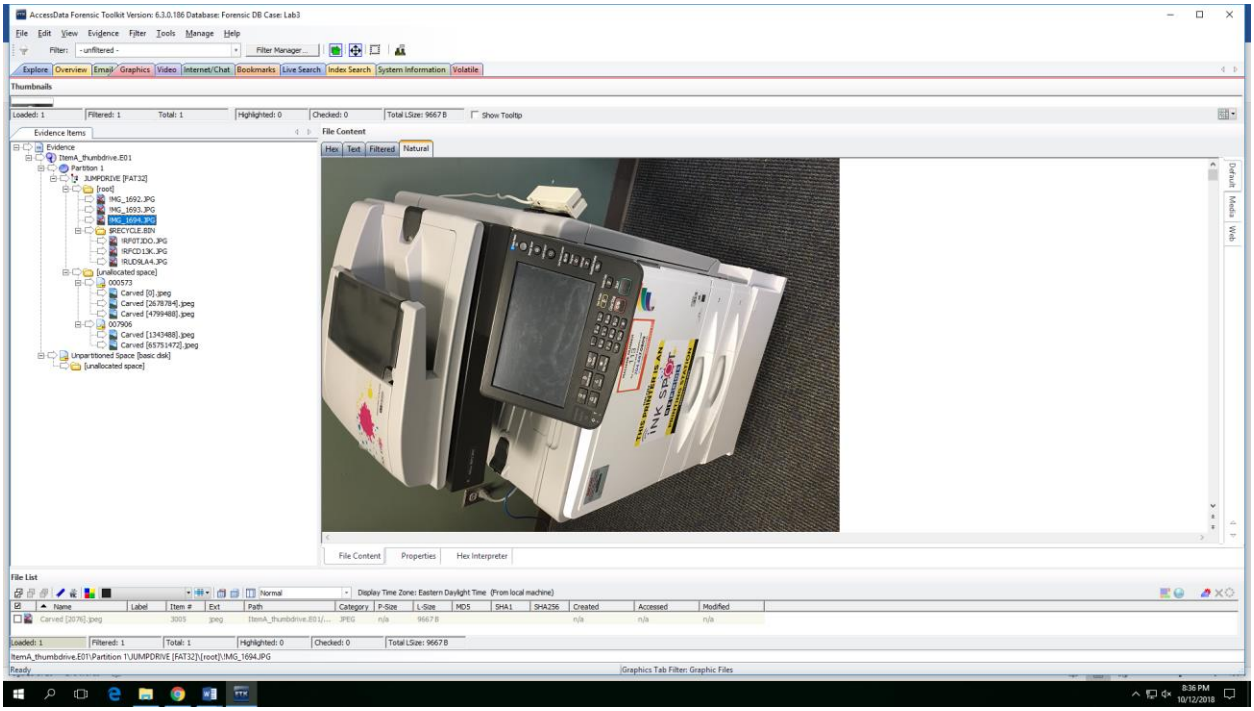
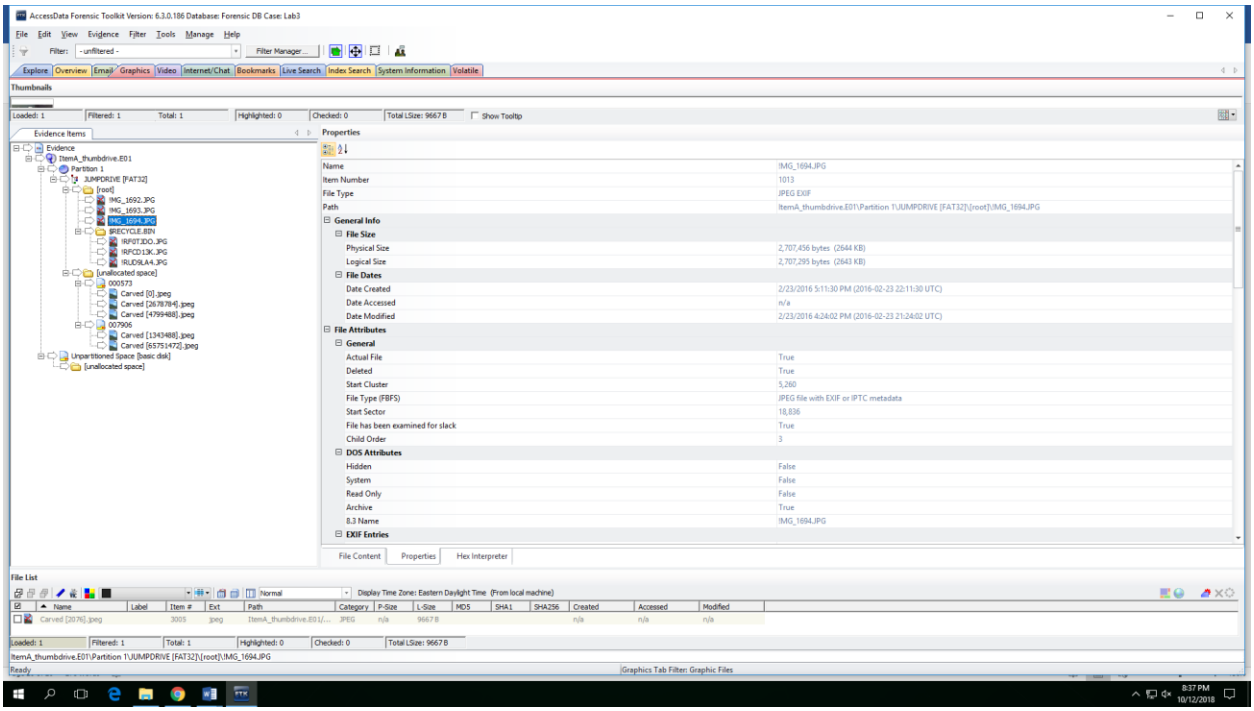
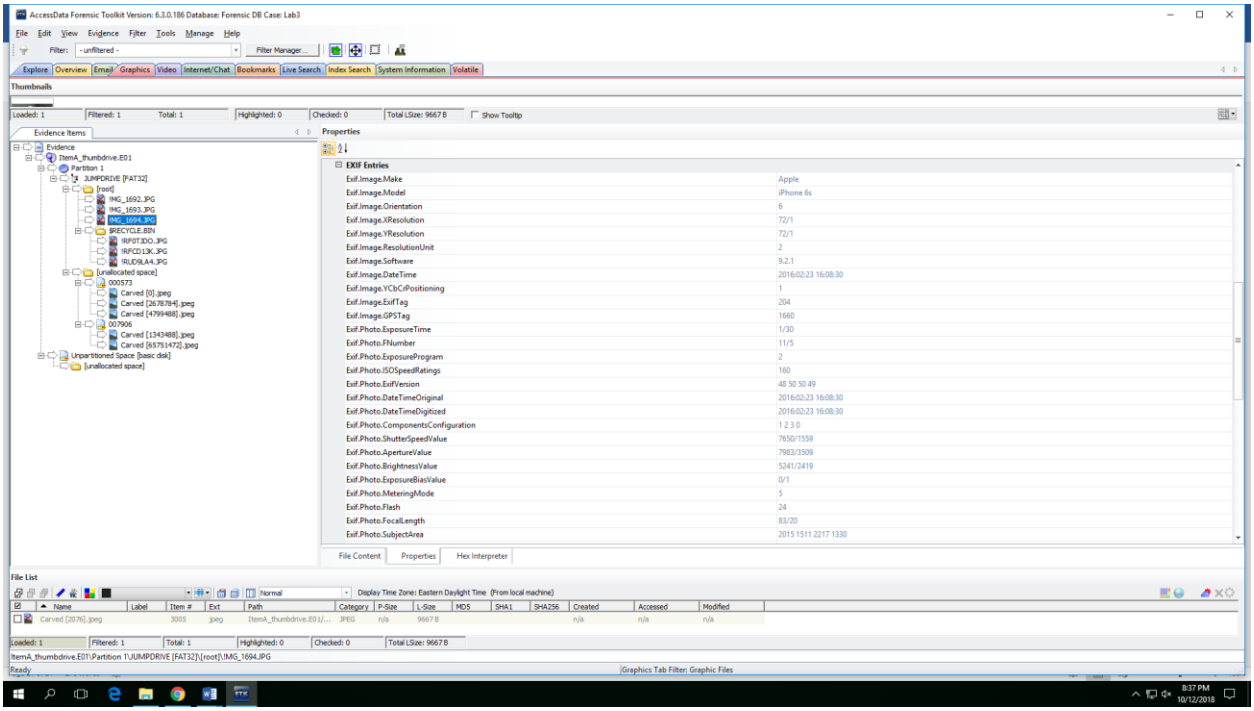


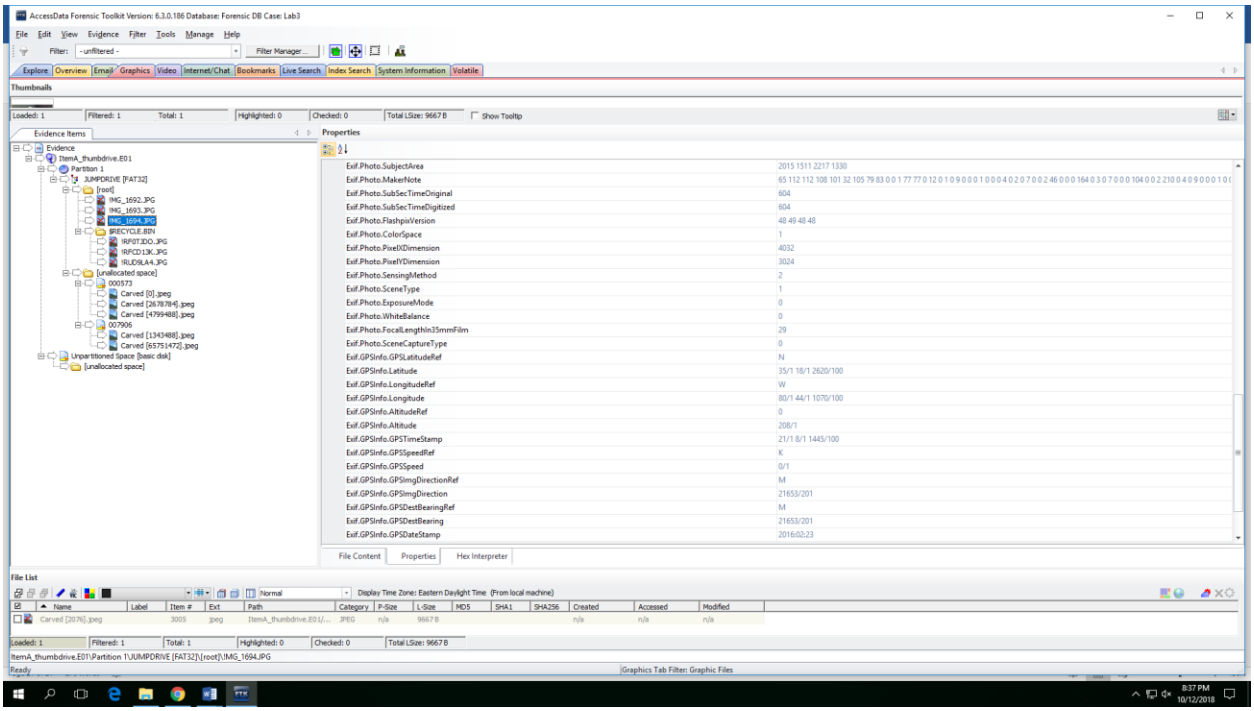
Image 3:

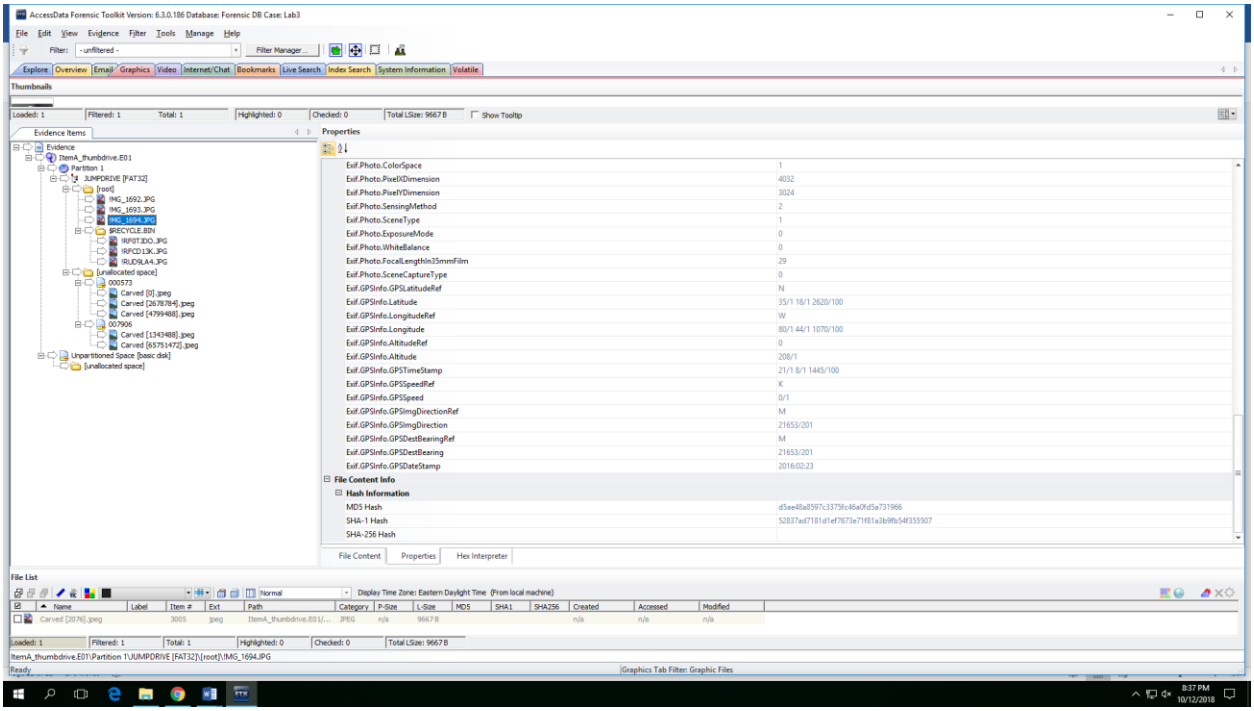


EXIF information of Image 3:


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
Properties
Name IMG_1694.JPG
Item Number 1013
File Type JPEG EXIF
Path ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[root]\IMG_1694.JPG
General Info
File Size
Physical Size 2,707,456 bytes (2644 KB)
Logical Size 2,707,295 bytes (2643 KB)
File Dates
Date Created 2/23/2016 5:11:30 PM (2016-02-23 22:11:30 UTC)
Date Accessed n/a
Date Modified 2/23/2016 4:24:02 PM (2016-02-23 21:24:02 UTC)
File Attributes
General
Actual File True
Deleted True
Start Cluster 5,260
File Type (FBFS) JPEG file with EXIF or IPTC metadata
Start Sector 18,836
File has been examined for slack True
Child Order 3
DOS Attributes
Hidden False
System False
Read Only False
Archive True
8.3 Name IMG_1694.JPG
EXIF Entries
File Content
Properties
Hex Interpreter
File List
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[root]\IMG_1694.JPG
Ready
Graphics Tab Filter: Graphic Files


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3
Properties
EXIF Entries
Exif.Image.Make Apple
Exif.Image.Model iPhone 6s
Exif.Image.Orientation 6
Exif.Image.XResolution 72/1
Exif.Image.YResolution 72/1
Exif.Image.ResolutionUnit 2
Exif.Image.Software 9.2.1
Exif.Image.DateTime 2016:02:23 16:08:30
Exif.Image.YCbCrPositioning 1
Exif.Image.ExifTag 204
Exif.Image.GPSTag 1660
Exif.Photo.ExposureTime 1/30
Exif.Photo.FNumber 11/5
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.Photo.ApertureValue 7983/3509
Exif.Photo.BrightnessValue 5241/2419
Exif.Photo.ExposureBiasValue 0/1
Exif.Photo.MeteringMode 5
Exif.Photo.Flash 24
Exif.Photo.FocalLength 83/20
Exif.Photo.SubjectArea 2015 1511 2217 1330
File Content
Properties
Hex Interpreter
File List
ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[root]\IMG_1694.JPG
Ready
Graphics Tab Filter: Graphic Files

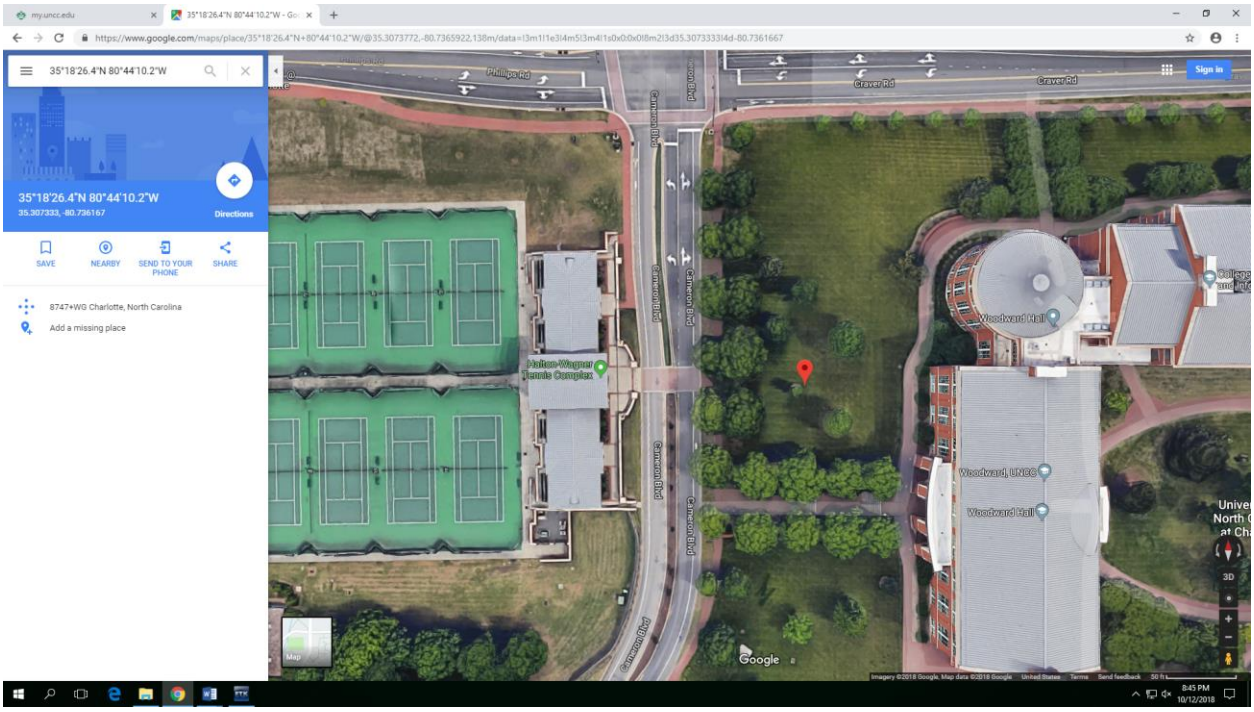




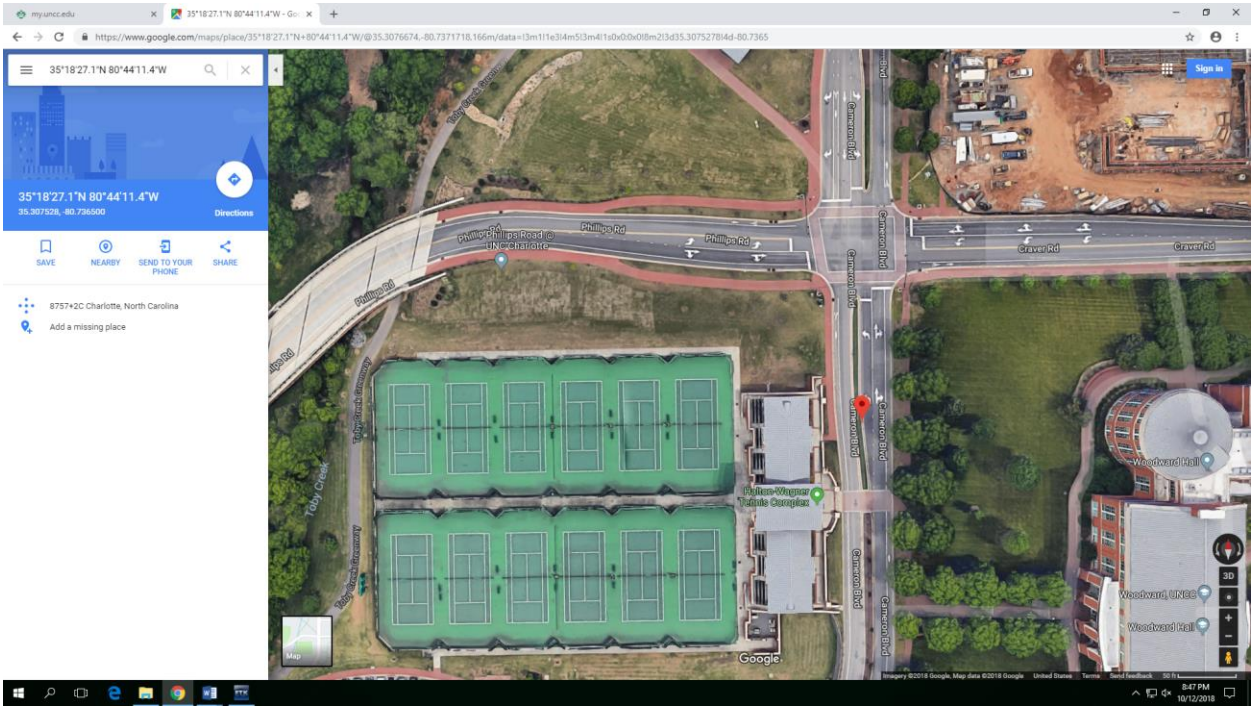
Looking at the **EXIF** information of these **3** pictures, I found out device model, date, time and GPS coordinates.

Then I located the GPS coordinates of all these pictures into google maps and found out the specific locations.

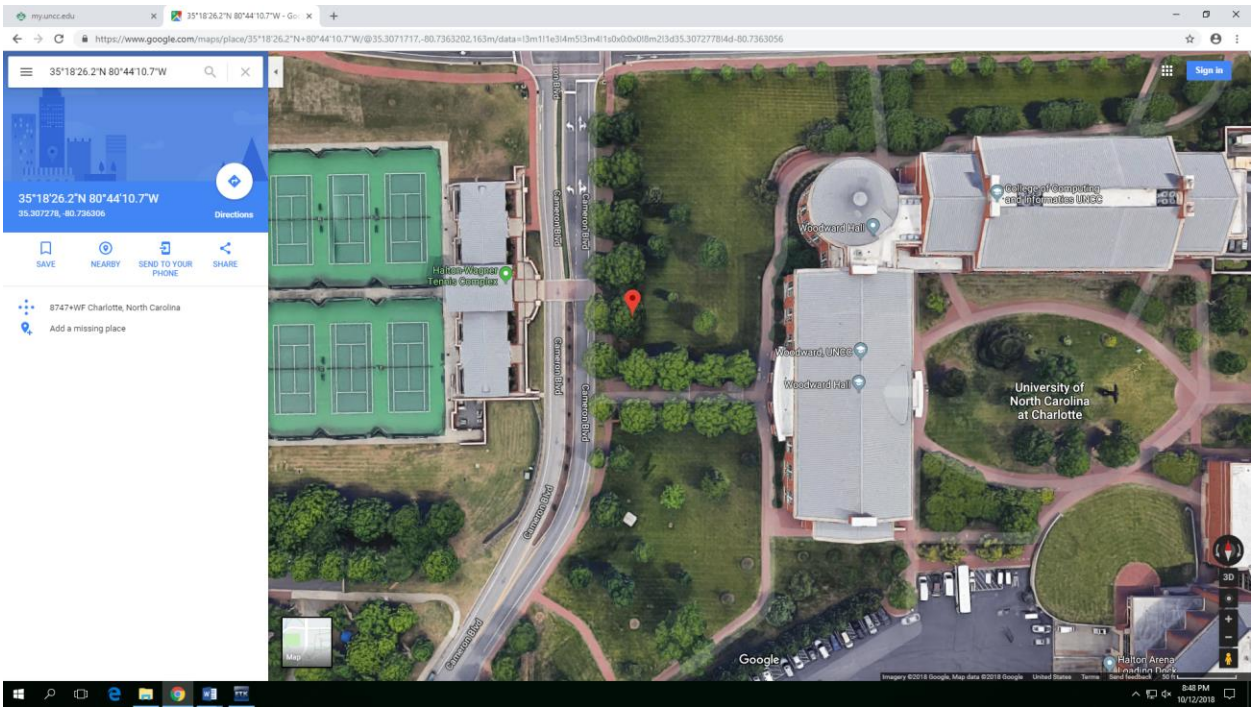
Location for Image 1:



Location for Image 2:



Location for Image 3:



Conclusion

After obtaining and verifying the forensic images, I performed operation using FTK Imager Tool to find information like the Hash verification of the Forensic Image. Then I performed various operations using FTK Tool for Data carving to recover deleted pictures from the given image. Also looking at the **EXIF** information of pictures, I found out device model, date, time and GPS coordinates. Later using GPS coordinates I have found out the specific locations.

The information I found was as follows:

1. Both the stored and computed hash value of a given Forensic Image matched.
2. Using Data carving deleted pictures from the given image were recovered.
3. **EXIF** information of pictures gives device model, date, time and GPS coordinates.
4. Locating GPS coordinates of all these pictures into google maps I have found out the specific locations

Thus, by finding above information I have showed that the individual was scouting for items to steal from Woodward.