

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

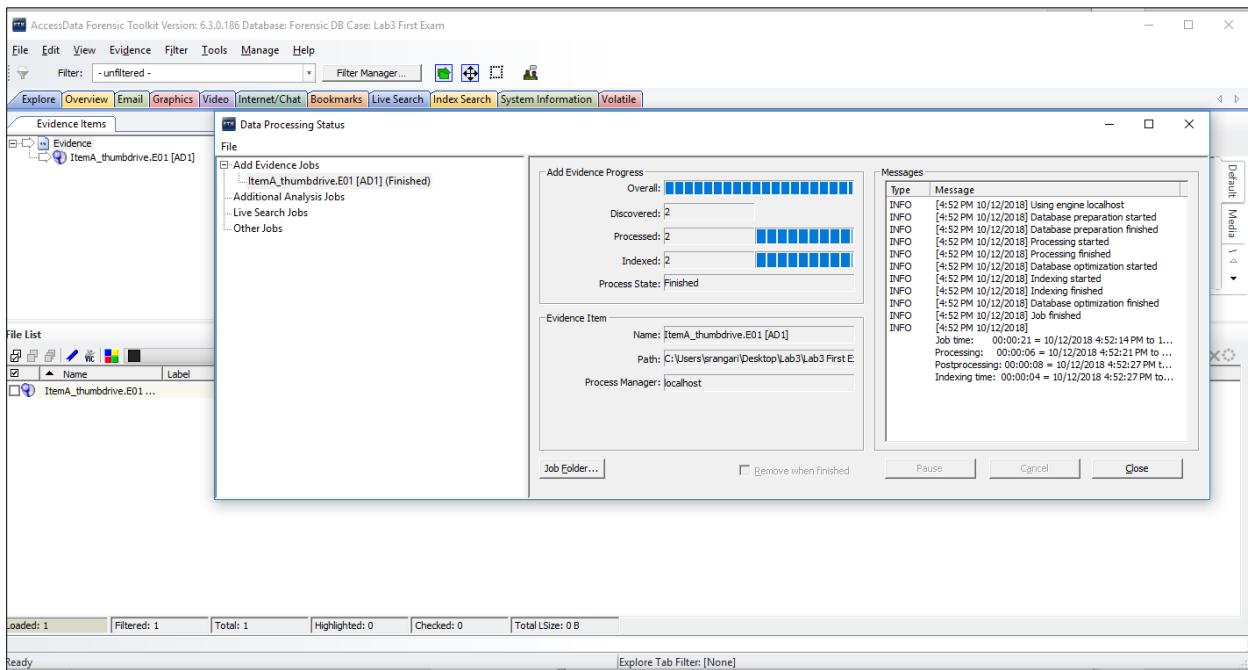
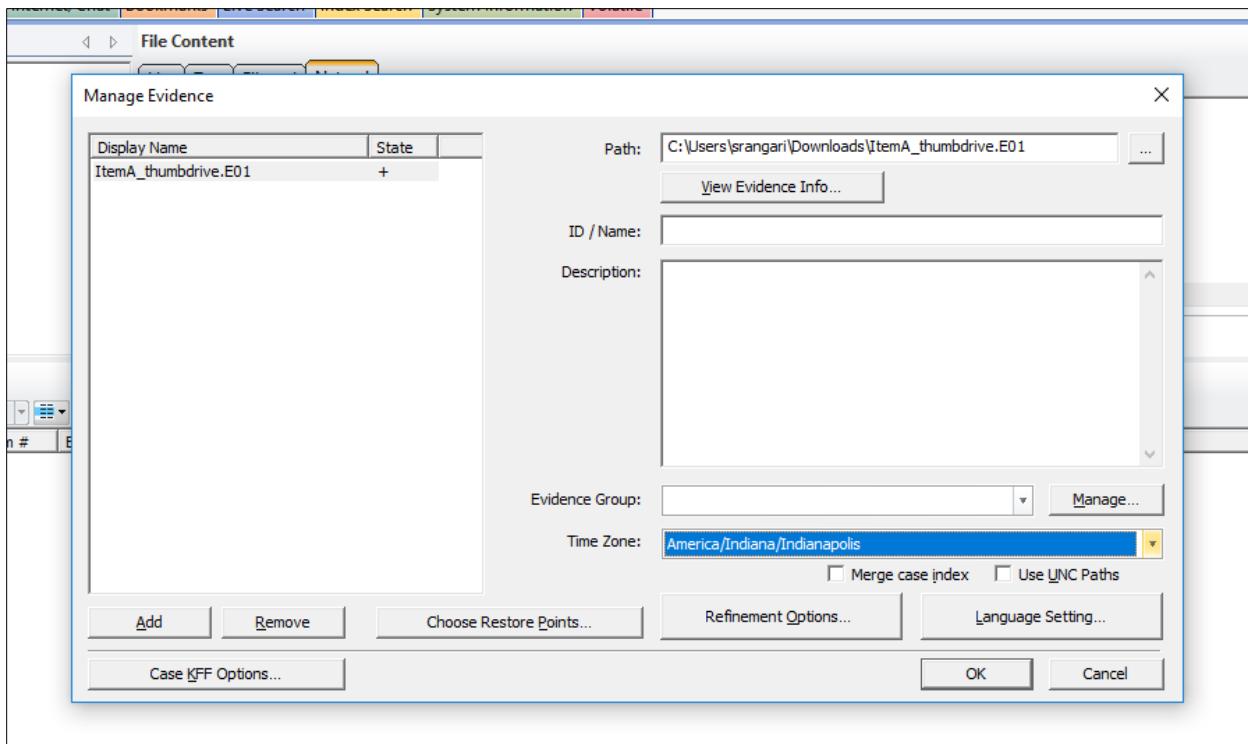
Notes: This guy is definitely guilty!!

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

Drive/Image Verify Results	
<input type="checkbox"/>	
Name	ItemA_thumbdrive.E01
Sector count	524288
<input type="checkbox"/> MD5 Hash	
Computed hash	3e7f5fa6e2972014b8671960a0624566
Stored verification hash	3e7f5fa6e2972014b8671960a0624566
Report Hash	3e7f5fa6e2972014b8671960a0624566
Verify result	Match
<input type="checkbox"/> SHA1 Hash	
Computed hash	4c88691bdb872a9586e2f5778a5b28a42fd550c
Stored verification hash	4c88691bdb872a9586e2f5778a5b28a42fd550c
Report Hash	4c88691bdb872a9586e2f5778a5b28a42fd550c
Verify result	Match
<input type="checkbox"/> Bad Blocks List	
Bad block(s) in image	No bad blocks found in image
<input type="button" value="Close"/>	

Where both the stored and computed hash value matched.

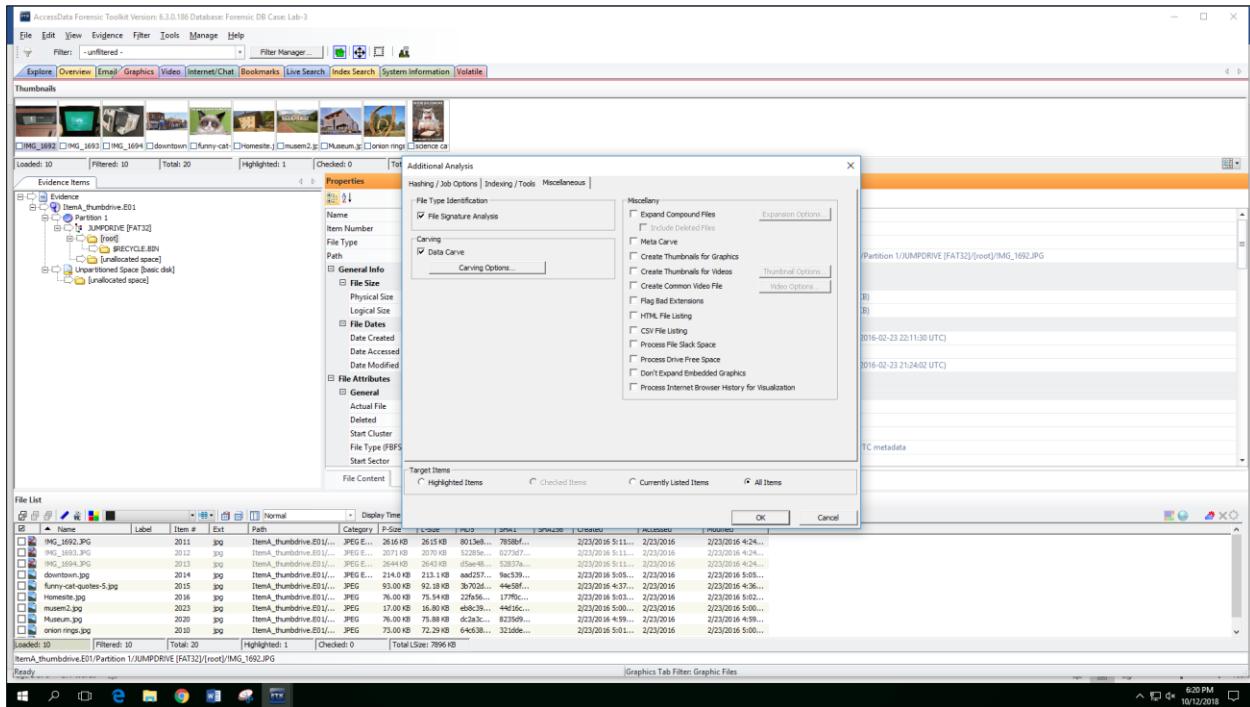
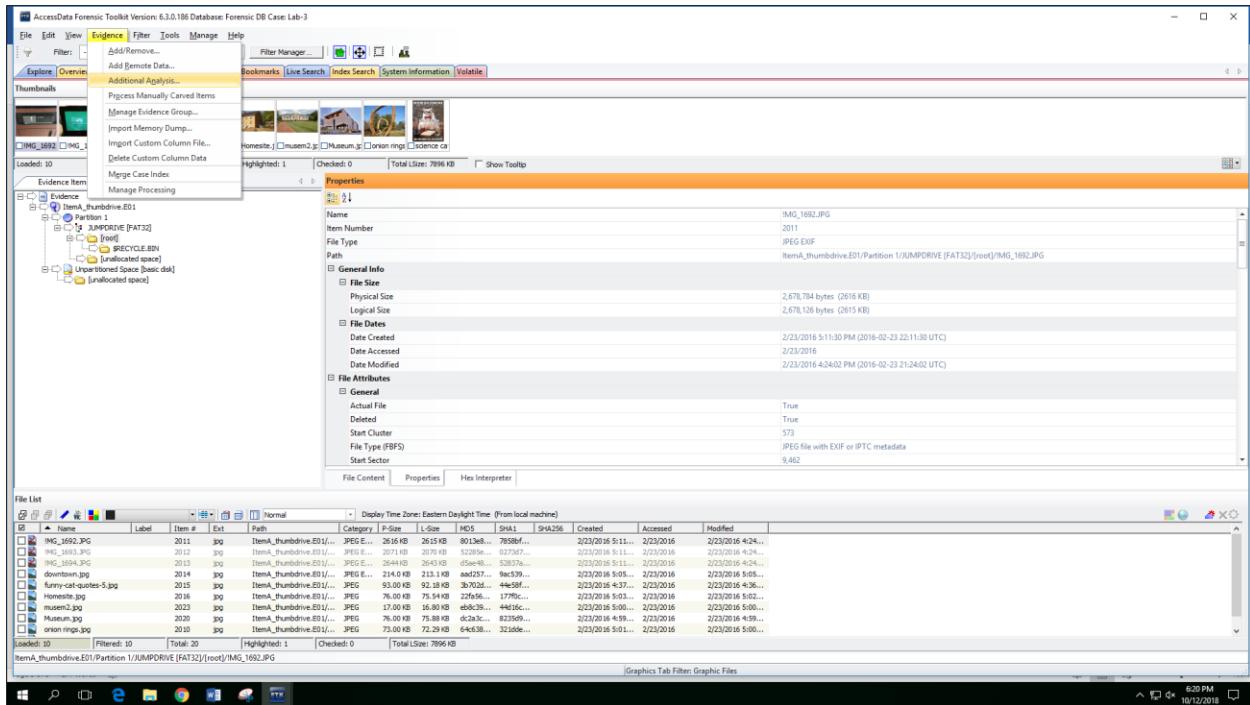
After that I created a new case in FTK by loading a ItemA_thumbdrive.E01 for evidence processing.



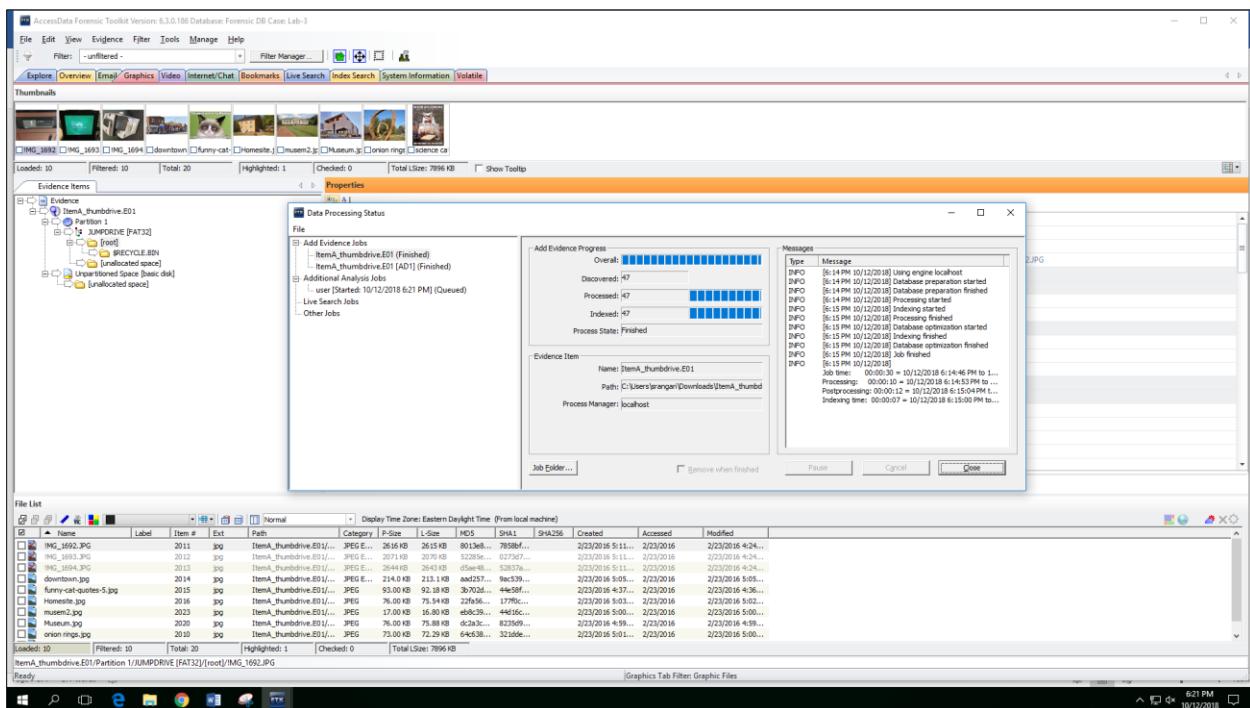
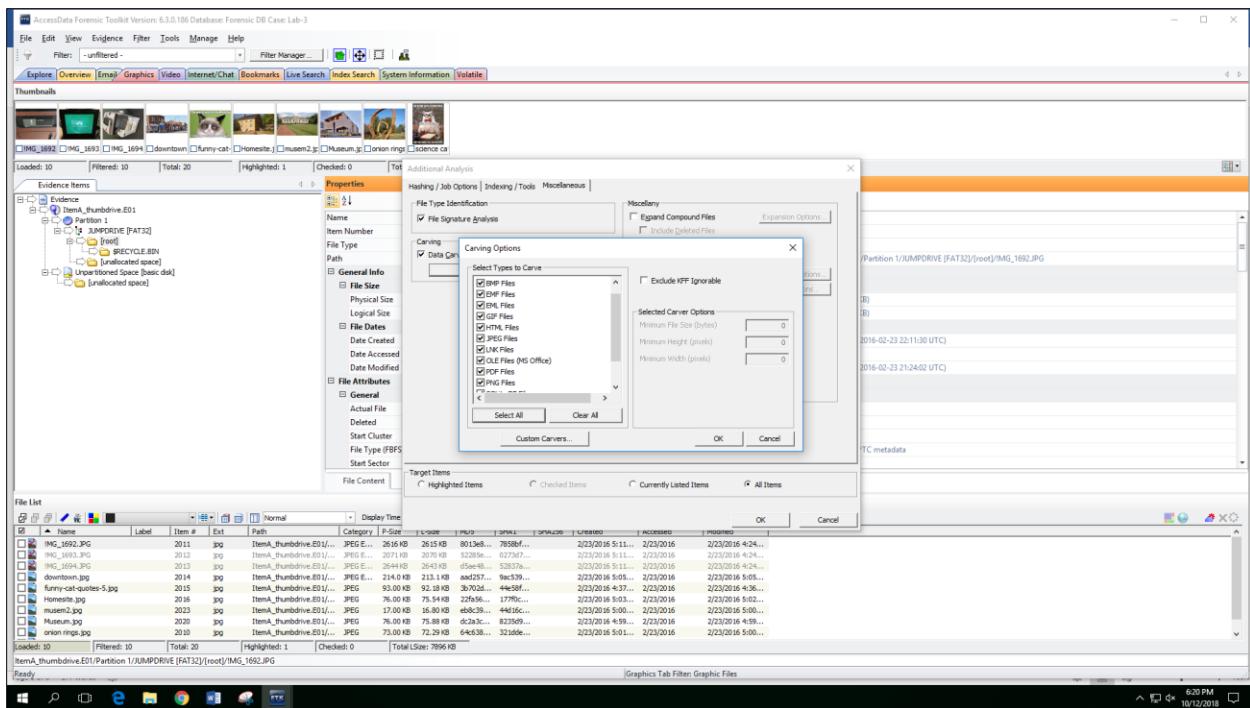
Properties	
	Evidence Source Path C:\Users\srangari\Downloads\ItemA_thumbdrive.E01
Disk	
	Evidence Type Forensic Disk Image
	MD5 verification hash 3e7f5fa6e2972014b8671960a0624566
	SHA1 verification hash 4c88691bdab872a9586e2f5778a5b28a42fd550c
	Bytes per Sector 512
	Sector Count 524,288
Image	
	Image Type E01
	Case number X_02232016
	Evidence number ItemA
	Examiner Ofc. Jimmy Johns
	Notes This guy is definitely guilty!!
	Acquired on OS Windows 7
	Acquired using AD13.2.0.0
	Acquire date 2/23/2016 10:38:43 PM
	System date 2/23/2016 10:38:43 PM
	Unique description A thumbdrive provided on consent
<hr/>	
<hr/>	
Properties Hex Value Interpreter Custom Content Sources	
00000130 18 AU B1 01 EB 08 AU B6-07 EB 03 AU B5 07 32 E4 . . e - y - e - u - 2a	

Findings and Report (Forensic Analysis)

After loading the image into FTK, no pictures were 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.

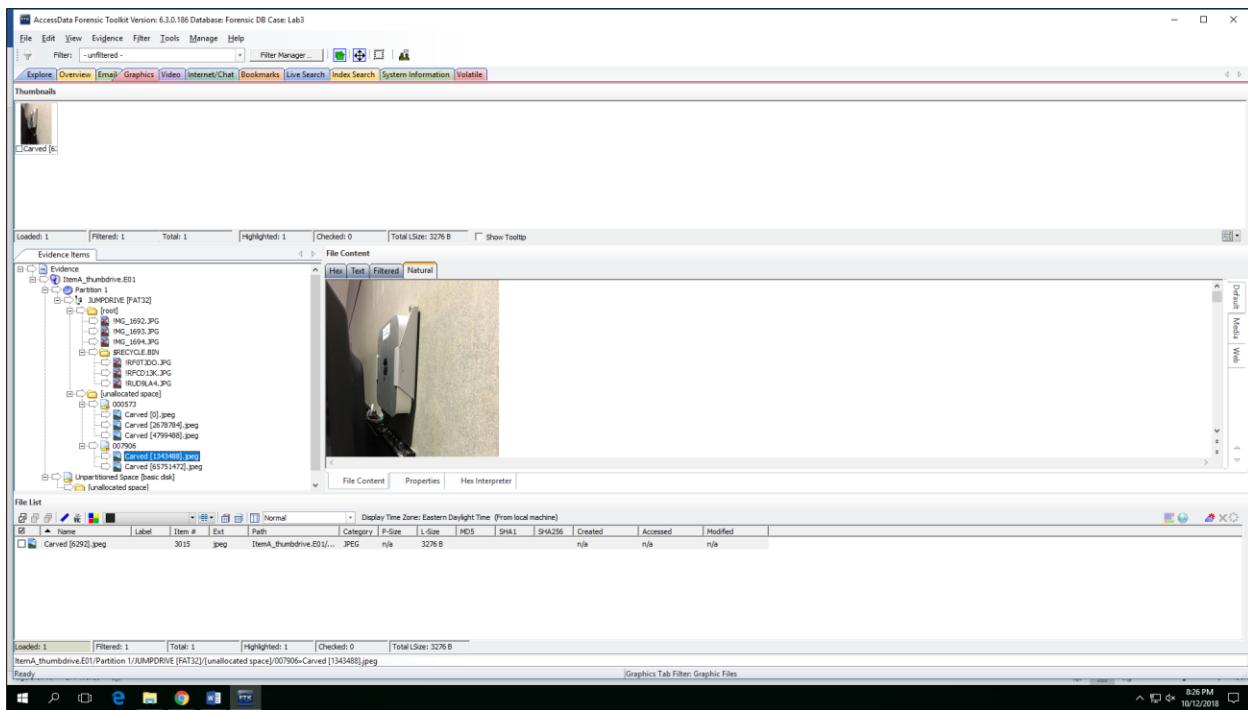


As I wanted to recover pictures of Apple device I selected all picture extension file options to carve.



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:

This screenshot shows the same forensic toolkit interface, but the Properties tab is active. It displays detailed EXIF metadata for a selected JPEG file. Key details include the file name (Carved [1343488].jpg), physical size (1,946,063 bytes), logical size (1,946,063 bytes), and file type (JPEG EXIF). The EXIF entries section lists various fields such as ExifImage.Maker (Apple), ExifImage.Model (iPhone 6s), and ExifImage.Orientation (1).

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

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 1 Checked: 0 Total LSize: 3276 B Show Tooltips

Evidence Items

ItemA_thumdrive.E01

- Partition 1
 - JUMPDRIVE [FAT32]
 - [root]
 - IMG_1692.JPG
 - IMG_1693.JPG
 - IMG_1694.JPG
 - RECYCLE.BIN
 - RFID100.JPG
 - RFID101.JPG
 - RFID102.JPG
 - RFID103.JPG
 - 000573
 - [root]
 - Carved [0].jpg
 - Carved [267974].jpg
 - Carved [1499488].jpg
 - 007906
 - [root]
 - Carved [1343488].jpg
 - Carved [5571472].jpg
 - [unpartitioned space]
 - [unallocated space]
 - Unpartitioned Space [Basic Disk]
 - [unallocated space]

Properties

ExifImage.DateTime	2016/02/23 16:27:03
ExifImage.YCbCrPositioning	1
ExifImage.ExifTag	3216
ExifImage.GPSInfo	5856
ExifPhoto.ExposureTime	1/15
ExifPhoto.Number	11/9
ExifPhoto.ExposureProgram	2
ExifPhoto.ISOSpeedRatings	250
ExifPhoto.SOFRating	48 50 50 49
ExifPhoto.SOFRating	2016/02/23 16:06:08
ExifPhoto.DateOriginal	2016/02/23 16:06:08
ExifPhoto.DateDigitized	1 2 3 0
ExifPhoto.ComponentsConfiguration	13229/3186
ExifPhoto.ShutterSpeedValue	7983/3599
ExifPhoto.ApertureValue	688/1131
ExifPhoto.BrightnessValue	0/1
ExifPhoto.ExposureBiasValue	5
ExifPhoto.MeteringMode	24
ExifPhoto.Flash	83/20
ExifPhoto.FocalLength	2015/1511 22:17 1330
ExifPhoto.SubjectArea	65 112 112 108 101 32 105 79 83 0 1 77 0 12 0 1 0 9 0 0 1 0 0 4 0 2 0 7 0 0 2 4 6 0 0 1 6 0 3 0 7 0 0 1 0 4 0 2 2 0 4 0 9 0 0 1 0
ExifPhoto.MakeNote	080
ExifPhoto.SubSecTimeOriginal	080
ExifPhoto.SubSecTimeDigitized	ExifPhoto.FlashFwVersion
ExifPhoto.FlashFwVersion	48 49 48 48
ExifPhoto.ColorSpace	1
ExifPhoto.PixelDimension	3024
ExifPhoto.PixelDimension	4032
ExifPhoto.SensingMethod	2
ExifPhoto.SceneType	ExifPhoto.WhiteBalance
ExifPhoto.WhiteBalance	0
ExifPhoto.FocalLengthIn35mmFilm	29
ExifPhoto.SceneCaptureType	0
ExifGPSInfo.GPSLatitudeRef	N
ExifGPSInfo.GPSLatitude	35/1 18/1 2572/100
ExifGPSInfo.LongitudeRef	W
ExifGPSInfo.Longitude	80/1 44/1 1100/100
ExifGPSInfo.AltitudeRef	0
ExifGPSInfo.Altitude	64457/313
ExifGPSInfo.GPSTimeStamp	21/1 3/1 5608/100
ExifGPSInfo.GPSSpeedRef	K
ExifGPSInfo.GPSSpeed	0/1
ExifGPSInfo.GPSSpeedDirectionRef	M
ExifGPSInfo.GPSSpeedDirection	54812/237
ExifGPSInfo.GPSCellBeamingRef	M
ExifGPSInfo.GPSCellBeaming	54812/237
ExifGPSInfo.GPSCellBeaming	2016/02/23

File Center Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	HDS	SHA1	SHA256	Created	Accessed	Modified
Carved [6292].jpg	3015	jpeg	ItemA_thumdrive.E01\...	JPEG	n/a	3276 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

loaded: 1 Filtered: 1 Total: 1 Highlighted: 1 Checked: 0 Total LSize: 3276 B

ItemA_thumdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[unallocated space]\007906-Carved [1343488].jpg

Ready

Graphics Tab Filter: Graphic Files

8:07 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

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 1 Checked: 0 Total LSize: 3276 B Show Tooltips

Evidence Items

ItemA_thumdrive.E01

- Partition 1
 - JUMPDRIVE [FAT32]
 - [root]
 - IMG_1692.JPG
 - IMG_1693.JPG
 - IMG_1694.JPG
 - RECYCLE.BIN
 - RFID100.JPG
 - RFID101.JPG
 - RFID102.JPG
 - RFID103.JPG
 - 000573
 - [root]
 - Carved [0].jpg
 - Carved [267974].jpg
 - Carved [1499488].jpg
 - 007906
 - [root]
 - Carved [1343488].jpg
 - Carved [5571472].jpg
 - [unpartitioned space]
 - [unallocated space]
 - Unpartitioned Space [Basic Disk]
 - [unallocated space]

Properties

ExifPhoto.ColorSpace	1
ExifPhoto.PixelDimension	3024
ExifPhoto.PixelDimension	4032
ExifPhoto.SensingMethod	2
ExifPhoto.SceneType	1
ExifPhoto.ExposureMode	0
ExifPhoto.WhiteBalance	0
ExifPhoto.FocalLengthIn35mmFilm	29
ExifPhoto.SceneCaptureType	0
ExifGPSInfo.GPSLatitudeRef	N
ExifGPSInfo.GPSLatitude	35/1 18/1 2572/100
ExifGPSInfo.LongitudeRef	W
ExifGPSInfo.Longitude	80/1 44/1 1100/100
ExifGPSInfo.AltitudeRef	0
ExifGPSInfo.Altitude	64457/313
ExifGPSInfo.GPSTimeStamp	21/1 3/1 5608/100
ExifGPSInfo.GPSSpeedRef	K
ExifGPSInfo.GPSSpeed	0/1
ExifGPSInfo.GPSSpeedDirectionRef	M
ExifGPSInfo.GPSSpeedDirection	54812/237
ExifGPSInfo.GPSCellBeamingRef	M
ExifGPSInfo.GPSCellBeaming	54812/237
ExifGPSInfo.GPSCellBeaming	2016/02/23

File Center Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	HDS	SHA1	SHA256	Created	Accessed	Modified
Carved [6292].jpg	3015	jpeg	ItemA_thumdrive.E01\...	JPEG	n/a	3276 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

loaded: 1 Filtered: 1 Total: 1 Highlighted: 1 Checked: 0 Total LSize: 3276 B

ItemA_thumdrive.E01\Partition 1\JUMPDRIVE [FAT32]\[unallocated space]\007906-Carved [1343488].jpg

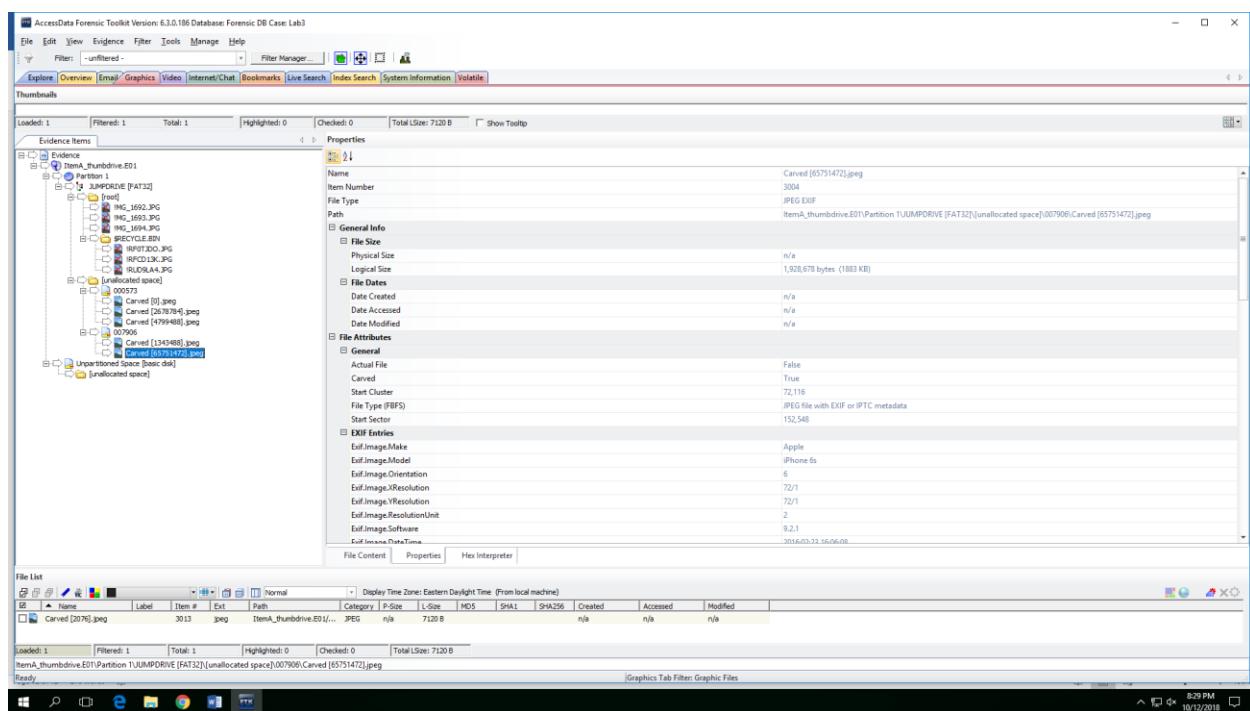
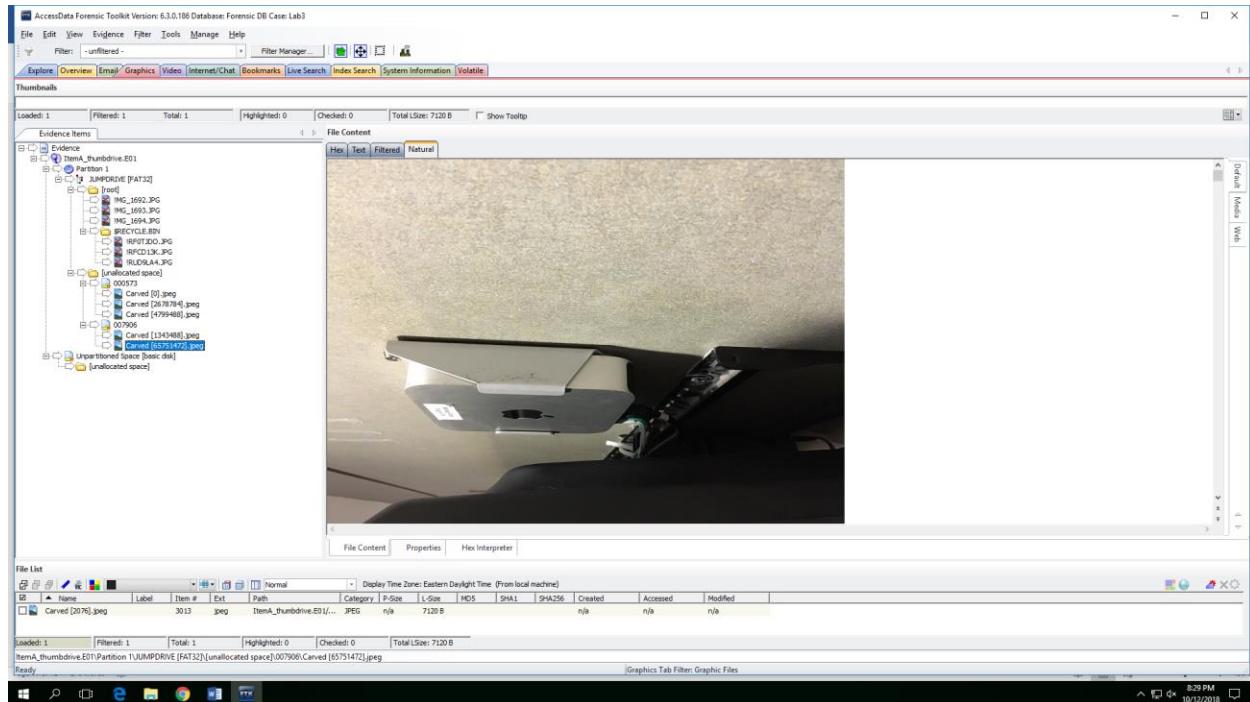
Ready

Graphics Tab Filter: Graphic Files

8:08 PM 10/12/2018

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

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7120 B Show Tooltip

Evidence Items

- itemA_thumddrive.E01
 - Partition 1
 - JUMPDRIVE [FAT32]
 - [root]
 - IMG_1692.JPG
 - IMG_1693.JPG
 - IMG_1694.JPG
 - RECYCLE.BIN
 - RFCD103.JPG
 - RFCD104.JPG
 - RFCD105.JPG
 - 000573
 - Carved [0].jpg
 - Carved [20784].jpg
 - Carved [20794].jpg
 - Carved [207948].jpg
 - 007906
 - Carved [124480].jpg
 - Carved [65751472].jpg
 - Unpartitioned Space [basic disk]
 - [unallocated space]

Properties

Name	Carved [65751472].jpg
Item Number	3004
File Type	JPEG EXIF
Path	itemA_thumddrive.E01\Partition JUMPDRIVE [FAT32]\[unallocated space]\007906\Carved [65751472].jpg
General Info	
File Size	n/a
Physical Size	1,928,678 bytes (1.883 KB)
Logical Size	
Date Created	n/a
Date Accessed	n/a
Date Modified	n/a
File Attributes	
General	False
Actual File	True
Carved	72,116
Start Cluster	152,548
File Type (FATFS)	JPEG file with EXIF or IPTC metadata
Start Sector	
EXIF Entries	
ExifImage.Make	Apple
ExifImage.Model	iPhone 6s
ExifImage.Orientation	6
ExifImage.Resolution	72/1
ExifImage.ResolutionUnit	2
ExifImage.Software	9.2.1
ExifImage.DateTime	2016/02/23 16:06:08

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].jpg	3013	.jpeg	itemA_thumddrive.E01\...	JPEG	n/a	7120 B					n/a	n/a	n/a

loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7120 B

ItemA_thumddrive.E01\Partition JUMPDRIVE [FAT32]\[unallocated space]\007906\Carved [65751472].jpg

Ready

8:59 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

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7120 B Show Tooltip

Evidence Items

- itemA_thumddrive.E01
 - Partition 1
 - JUMPDRIVE [FAT32]
 - [root]
 - IMG_1692.JPG
 - IMG_1693.JPG
 - IMG_1694.JPG
 - RECYCLE.BIN
 - RFCD103.JPG
 - RFCD104.JPG
 - RFCD105.JPG
 - 000573
 - Carved [0].jpg
 - Carved [20784].jpg
 - Carved [20794].jpg
 - Carved [207948].jpg
 - 007906
 - Carved [124480].jpg
 - Carved [65751472].jpg
 - Unpartitioned Space [basic disk]
 - [unallocated space]

Properties

ExifImage.DateTime	2016/02/23 16:06:08
ExifImage.CbColorPositioning	1
ExifImage.ExifTag	204
ExifImage.GPSTag	1660
ExifImage.ExposureTime	1/15
ExifPhoto.Number	11/5
ExifPhoto.ExposureProgram	2
ExifPhoto.ISOSpeedRatings	250
ExifPhoto.ExifVersion	48 50 50 49
ExifPhoto.DateTimeOriginal	2016/02/23 16:06:08
ExifPhoto.DateTimeDigitized	2016/02/23 16:06:08
ExifPhoto.ComponentsConfiguration	1 2 3 0
ExifPhoto.ShutterSpeedValue	1325/3386
ExifPhoto.ApertureValue	7983/3509
ExifPhoto.BrightnessValue	688/131
ExifPhoto.ExposureBiasValue	0/1
ExifPhoto.MeteringMode	5
ExifPhoto.Flash	24
ExifPhoto.FocalLength	83/20
ExifPhoto.SubjectArea	2015/11/22 17:13:30
ExifPhoto.MakeNote	65 112 112 108 101 32 105 79 83 0 1 77 77 0 12 0 10 9 0 0 1 0 0 0 4 2 0 7 0 2 46 0 0 164 0 3 0 7 0 0 104 0 0 2 2 10 0 4 0 9 0 0 101
ExifPhoto.SubsecTimeOriginal	080
ExifPhoto.SubsecTimeDigitized	080
ExifPhoto.PixelXDimension	48 49 48 48
ExifPhoto.PixelYDimension	3024
ExifPhoto.ColorSpace	1
ExifPhoto.PixelDimension	4032
ExifPhoto.SensingMethod	3024

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].jpg	3013	.jpeg	itemA_thumddrive.E01\...	JPEG	n/a	7120 B					n/a	n/a	n/a

loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7120 B

ItemA_thumddrive.E01\Partition JUMPDRIVE [FAT32]\[unallocated space]\007906\Carved [65751472].jpg

Ready

8:59 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

Filter: -unfiltered- Filter Manager

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

Thumbnails

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7120 B Show Tooltip

Evidence Items

- itemA_thumddrive.E01
 - Partition 1
 - Unallocated [FAT32]
 - [root]
 - IMG_1692.JPG
 - IMG_1693.JPG
 - IMG_1694.JPG
 - IMG_1695.JPG
 - RECYCLE.BIN
 - REF01.DOC
 - REF01.DOC
 - REF01A.JPG
 - 000573
 - Carved [0].jpg
 - Carved [2076].jpg
 - Carved [2076].jpg
 - Carved [479488].jpg
 - 007906
 - Carved [134488].jpg
 - Carved [65751472].jpg
 - Unpartitioned Space [Basic disk]
 - [Unallocated space]

Properties

Exif.Photo.ColorSpace	1
Exif.Photo.PixelDimension	4032
Exif.Photo.PixelDimension	3024
Exif.Photo.SensingMethod	2
Exif.Photo.SceneType	1
Exif.Photo.ExposureMode	0
Exif.Photo.WhiteBalance	0
Exif.Photo.FocalLengthIn3mmFilm	29
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
Exif.GPSInfo.GPSSpeedRef	K
Exif.GPSInfo.GPSSpeed	0/1
Exif.GPSInfo.GPSSpeedingRef	M
Exif.GPSInfo.GPSSpeeding	54812/237
Exif.GPSInfo.GPSDestBearingRef	M
Exif.GPSInfo.GPSDestBearing	54812/237
Exif.GPSInfo.GPSDateStamp	2016/02/23

File Content

Hash Information

 - MD5 Hash
 - SHA-1 Hash
 - SHA-256 Hash

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].jpg	3013	.jpeg	itemA_thumddrive.E01\...	JPEG	n/a	7120 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7120 B

itemA_thumddrive.E01\Partition 1\Unallocated [FAT32]\007906\Carved [65751472].jpg

Ready

8:51 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

Filter: -unfiltered- Filter Manager

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

Thumbnails

Loaded: 10 Filtered: 10 Total: 10 Highlighted: 1 Checked: 0 Total LSize: 10.89 MB Show Tooltip

Evidence Items

- itemA_thumddrive.E01
 - Partition 1
 - Unallocated [FAT32]
 - [root]
 - IMG_1692.JPG
 - IMG_1693.JPG
 - IMG_1694.JPG
 - IMG_1695.JPG
 - RECYCLE.BIN
 - REF01.DOC
 - REF01.DOC
 - REF01A.JPG
 - 000573
 - Carved [0].jpg
 - Carved [2076].jpg
 - Carved [2076].jpg
 - Carved [479488].jpg
 - 007906
 - Carved [134488].jpg
 - Carved [65751472].jpg
 - Unpartitioned Space [Basic disk]
 - [Unallocated space]

Properties

File Content



File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Carved [0].jpg	3005	.jpg	itemA_thumddrive.E01\...	JPEG	n/a	2610 KB	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Carved [2076].jpg	3010	.jpg	itemA_thumddrive.E01\...	JPEG	n/a	2786 KB	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Carved [2076].jpg	3012	.jpg	itemA_thumddrive.E01\...	JPEG	n/a	9667 KB	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Carved [2076].jpg	3014	.jpg	itemA_thumddrive.E01\...	JPEG	n/a	2047 KB	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Carved [2076].jpg	3015	.jpg	itemA_thumddrive.E01\...	JPEG	n/a	7250 KB	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Carved [2076].jpg	3007	.jpg	itemA_thumddrive.E01\...	JPEG	n/a	2070 KB	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Carved [479488].jpg	3008	.jpg	itemA_thumddrive.E01\...	JPEG	n/a	2643 KB	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Carved [65751472].jpg	3015	.jpg	itemA_thumddrive.E01\...	JPEG	n/a	3276 KB	n/a	n/a	n/a	n/a	n/a	n/a	n/a

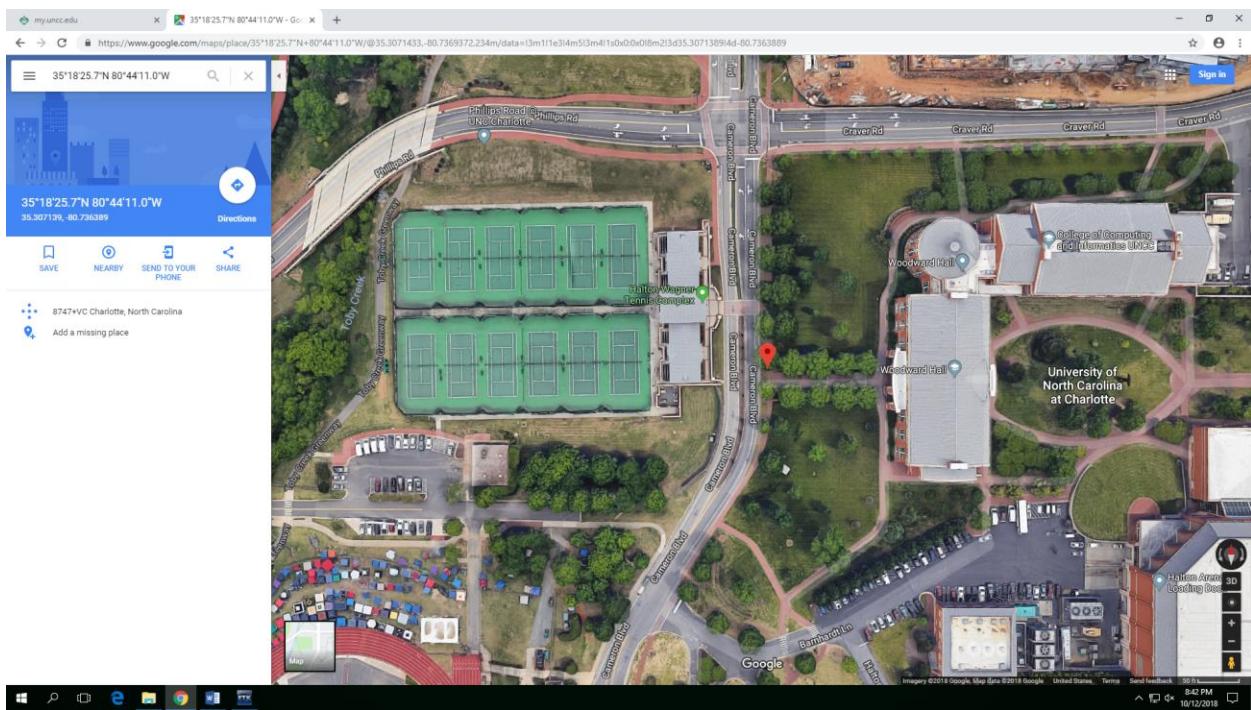
loaded: 10 Filtered: 10 Total: 10 Highlighted: 1 Checked: 0 Total LSize: 10.89 MB

itemA_thumddrive.E01\Partition 1\Unallocated [FAT32]\007906\Carved [134488].jpg

Ready

8:57 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:

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Carved [0].jpg	3002	jpeg	ItemA_Thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\root\IMG_1692.JPG	JPEG	n/a	7786 B					n/a	n/a	n/a
Carved [267984].jpg	3003	jpeg	ItemA_Thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\root\IMG_1693.JPG	JPEG	n/a	7786 B					n/a	n/a	n/a
Carved [479940].jpg	3005	jpeg	ItemA_Thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\root\IMG_1694.JPG	JPEG	n/a	7786 B					n/a	n/a	n/a

EXIF information of Image 1:

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3

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

Thumbnails

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7786 B Show Tooltips

Evidence Items

- itemA_thumdrive.E01
 - Partition 1
 - JUMPDRIVE [FAT32]
 - [root]
 - IMG_1692.JPG
 - IMG_1693.JPG
 - IMG_1694.JPG
 - RECYCLE.BIN
 - RFCD103.JPG
 - RFCD104.JPG
 - RFCD105.JPG
 - RFCD106.JPG
 - [unallocated space]
 - 000573
 - Carved [0].jpg
 - Carved (267974).jpg
 - Carved (279948).jpg
 - 007996
 - Carved (134348).jpg
 - Carved (557147).jpg
 - Unpartitioned Space [base disk]
 - [unallocated space]

Properties

Name: IMG_1692.JPG
Item Number: 1011
File Type: JPEG EXIF
Path: itemA_thumdrive.E01\Partition JUMPDRIVE [FAT32]\[root]\IMG_1692.JPG

General Info

Physical Size	2,678,784 bytes (2616 KB)
Logical Size	2,678,126 bytes (2613 KB)

Date

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: False Start Cluster: 573 File Type: (FATFS) 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

ExifImage.Make	Apple
ExifImage.Model	iPhone 6s
ExifImage.Orientation	1
ExifImage.Resolution	72/1
ExifImage.ResolutionUnit	2
ExifImage.Software	9.2.1
ExifImage.DateTime	2016/02/23 16:07:59
ExifImage.YCbCrPositioning	1
ExifImage.ExifTag	204
ExifImage.GPSTag	1660
ExifPhoto.ExposureTime	1/15
ExifPhoto.Number	11/5
ExifPhoto.ExposureProgram	2
ExifPhoto.ISOSpeedRatings	1600
ExifPhoto.Firmware	48 50 50 49
ExifPhoto.DateTimeOriginal	2016/02/23 16:07:59
ExifPhoto.DateTimeDigitized	2016/02/23 16:07:59
ExifPhoto.ComponentsConfiguration	1 2 3 0
ExifPhoto.ShutterSpeedValue	1/329/3386
ExifPhoto.ApertureValue	7983.359
ExifPhoto.ExposureTimeValue	-0:01/2974
ExifPhoto.SceneCaptureType	0/1
ExifPhoto.MeteringMode	5
ExifPhoto.Flash	24
ExifPhoto.FocalLength	83/20
ExifPhoto.SubjectArea	2015/1511/22/17 13:00

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (267974).jpg	3002	.jpg	itemA_thumdrive.E01\...	JPEG	n/a	7786 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	
------	-------	--------	-----	------	----------	--------	--------	-----	------	--

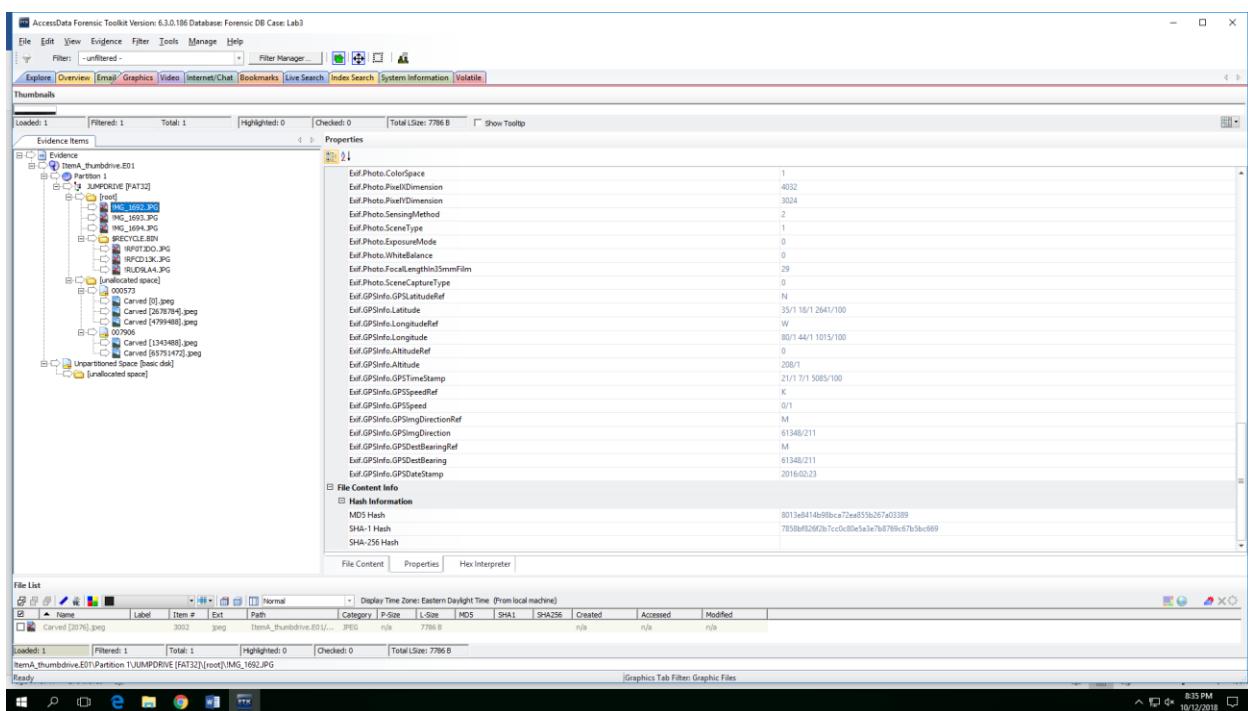
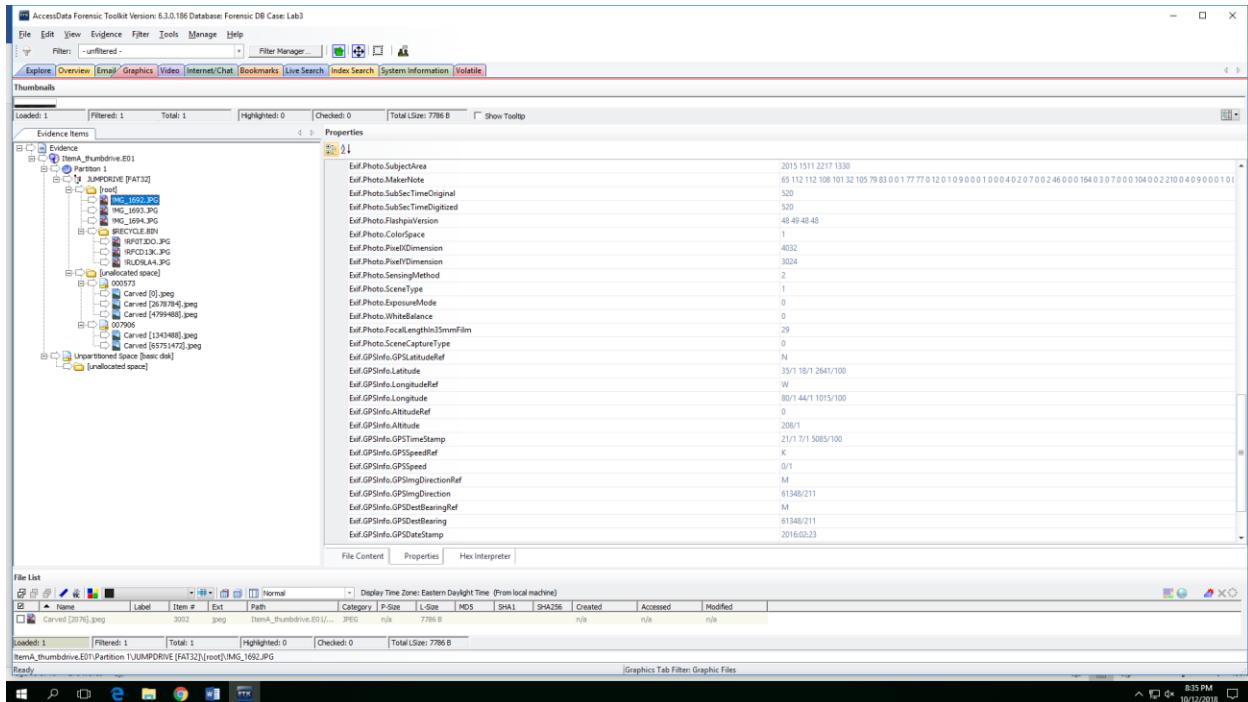
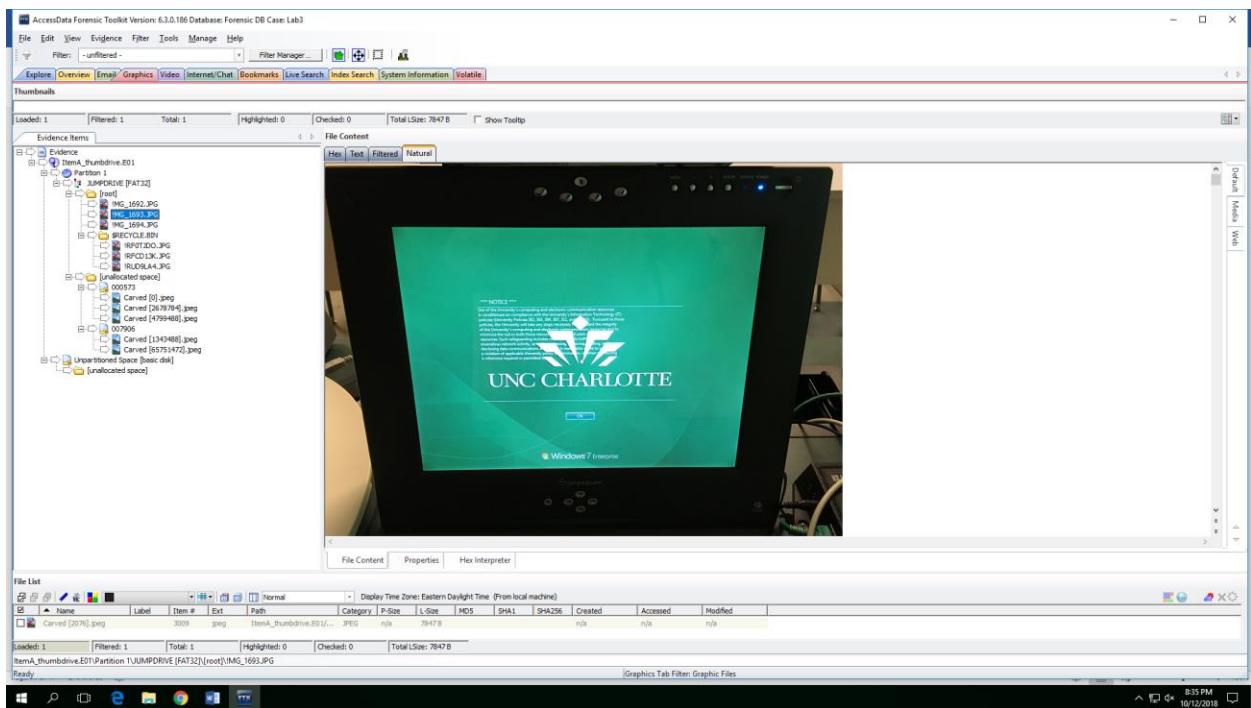


Image 2:



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

Filter: -unfiltered- Filter Manager

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

Thumbnails

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7847 B Show Tooltip

Evidence Items

itemA_thumdrive.E01

Partition TUJUMPDRIVE [FAT32]

- root
 - IMG_1693.JPG
 - IMG_1693.JPG
 - IMG_1693.JPG
 - IMG_1693.JPG
 - PRECYCLE.BIN
 - REF01D0.JPG
 - REF01D1.JPG
 - REF01D2.JPG
 - REF01D3.JPG
 - REF01D4.JPG
 - [unallocated space]
 - 000573
 - Carved [0].jpg
 - Carved [207974].jpg
 - Carved [207974].jpg
 - 007996
 - Carved [134948].jpg
 - Carved [5571472].jpg
 - [unpartitioned Space [basic disk]]
 - [unallocated space]

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Carved [0].jpg	3009	jpeg	itemA_thumdrive.E01\Partition TUJUMPDRIVE [FAT32]\[root]\IMG_1693.JPG		JPEG	n/a	7847 B				n/a	n/a	n/a

loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7847 B

itemA_thumdrive.E01\Partition TUJUMPDRIVE [FAT32]\[root]\IMG_1693.JPG

Ready

8:53 PM 10/12/2018

Properties

IMG_1693.JPG

File Number: 1012

File Type: JPEG EXIF

File Path: itemA_thumdrive.E01\Partition TUJUMPDRIVE [FAT32]\[root]\IMG_1693.JPG

General Info

File Size

- Physical Size: 2,120,704 bytes (2071 KB)
- Logical Size: 2,120,287 bytes (2070 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

DOS Attributes

- Hidden: False
- System: False
- Read Only: False
- Archive: True
- 8.3 Name: IMG_1693.JPG

EXIF Entries

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Carved [0].jpg	3009	jpeg	itemA_thumdrive.E01\Partition TUJUMPDRIVE [FAT32]\[root]\IMG_1693.JPG		JPEG	n/a	7847 B				n/a	n/a	n/a

loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7847 B

itemA_thumdrive.E01\Partition TUJUMPDRIVE [FAT32]\[root]\IMG_1693.JPG

Ready

8:58 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

Filter: -unfiltered- Filter Manager

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

Thumbnails

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7847 B Show Tooltip

Evidence Items

ItemA_thumdrive.E01

- Partitions
 - 1 JUMPDRIVE [FAT32]
 - [root]
 - IMG_1692.JPG
 - IMG_1694.JPG
 - RECYCLE.BIN
 - REF0100.JPG
 - REF0101.JPG
 - REF0102.JPG
 - REF0103.JPG
 - [unallocated space]
 - 000573
 - Carved [0].jpg
 - Carved (267974).jpg
 - Carved (279948).jpg
 - 007996
 - Carved (1343480).jpg
 - Carved (5571472).jpg
 - Unpartitioned Space [base disk]
 - [unallocated space]

Properties

Exif Entries

Exif.Image.Make	Apple
Exif.Image.Model	iPhone 6s
Exif.Image.Orientation	1
Exif.Image.Resolution	72/1
Exif.Image.Resolution	72/1
Exif.Image.ResolutionUnit	2
Exif.Image.Software	9.2.1
Exif.Image.DateTime	2016/02/23 16:08:11
Exif.Image.VCDOrientation	1
Exif.Image.ExifTag	204
Exif.Image.GPStag	1660
Exif.Photo.ExposureTime	1/24
Exif.Photo.Number	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

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Carved (2076).jpg	3009	.jpg	ItemA_thumdrive.E01\...	JPEG	n/a	7847 B					n/a	n/a	n/a

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7847 B

ItemA_thumdrive.E01\Partition 1\JUMPDRIVE [FAT32]\IMG_1693.JPG

Ready

8:56 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

Filter: -unfiltered- Filter Manager

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

Thumbnails

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7847 B Show Tooltip

Evidence Items

ItemA_thumdrive.E01

- Partitions
 - 1 JUMPDRIVE [FAT32]
 - [root]
 - IMG_1692.JPG
 - IMG_1694.JPG
 - RECYCLE.BIN
 - REF0100.JPG
 - REF0101.JPG
 - REF0102.JPG
 - REF0103.JPG
 - [unallocated space]
 - 000573
 - Carved [0].jpg
 - Carved (267974).jpg
 - Carved (279948).jpg
 - 007996
 - Carved (1343480).jpg
 - Carved (5571472).jpg
 - Unpartitioned Space [base disk]
 - [unallocated space]

Properties

Exif Entries

Exif.Photo.SubjectArea	2015.1511.2217.1330
Exif.Photo.MakeNote	65112112.108.101.32.105.79.83.0.1.77.77.0.12.0.1.0.9.0.0.0.1.0.0.4.0.2.0.7.0.2.4.6.0.0.1.6.0.3.0.7.0.0.1.0.4.0.2.2.1.0.4.0.9.0.0.0.1.
Exif.Photo.SubSecTimeOriginal	044
Exif.Photo.SubSecTimeDigitized	044
Exif.Photo.FlashSyncVersion	49.49.49.48
Exif.Photo.ColorSpace	1
Exif.Photo.PixelDimension	4032
Exif.Photo.PixelDimension	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	35/1.18/1.2708/100
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.GPSOffsetRef	K
Exif.GPSInfo.GPSOffset	0/1
Exif.GPSInfo.GPSSpeedRef	M
Exif.GPSInfo.GPSSpeed	86600/281
Exif.GPSInfo.GPSTimeDirectionRef	M
Exif.GPSInfo.GPSTimeDirection	86600/281
Exif.GPSInfo.GPSElevationRef	M
Exif.GPSInfo.GPSElevation	86600/281
Exif.GPSInfo.GPSTimeStamp	2016/02/23

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).jpg	3009	.jpg	ItemA_thumdrive.E01\...	JPEG	n/a	7847 B					n/a	n/a	n/a

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7847 B

ItemA_thumdrive.E01\Partition 1\JUMPDRIVE [FAT32]\IMG_1693.JPG

Ready

8:56 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

Filter: -unfiltered- Filter Manager

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

Thumbnails

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7847 B Show Tooltips

Evidence Items

ItemA_thumbdrive.E01

- Partitions
 - Unpartitioned [FAT32]
 - root
 - IMG_1692.JPG
 - IMG_1693.JPG
 - RECYCLE.BIN
 - RFID100.JPG
 - RFID101.JPG
 - RFID102.JPG
 - RFID103.JPG
 - Unallocated space
 - 000573
 - Carved [0].jpg
 - Carved [20794].jpg
 - Carved [207948].jpg
 - 007996
 - Carved [134480].jpg
 - Carved [5571472].jpg
 - Unpartitioned Space [basic disk]
 - [Unallocated space]

Properties

Exif Photo.ColorSpace 1

Exif Photo.PixelDimension 4032x3024

Exif Photo.SensingMethod 2

Exif Photo.SceneType 1

Exif Photo.ExposureMode 0

Exif Photo.WhiteBalance 0

Exif Photo.FocalLengthIn3mmFilm 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 6/1 573/100

Exif GPSInfo.GPSSpeedRef K

Exif GPSInfo.GPSSpeed 0/1

Exif GPSInfo.GPSTimeDirectionRef M

Exif GPSInfo.GPSTimeDirection 86600/281

Exif GPSInfo.GPSDestBearingRef M

Exif GPSInfo.GPSDestBearing 86600/281

Exif GPSInfo.GPSDateStamp 2016/02/23

File Content Info Hash Information MD5 Hash 52285e1a73a07d92cfdc68c3bbc2fe7

SHA-1 Hash 0273a7ece3df9fbef77137539b192694fb2bd470

SHA-256 Hash

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved [0].jpg	3009	.jpg		ItemA_thumbdrive.E01\...\\IMG_1693.JPG	JPEG	n/a	7847 B					n/a	n/a

loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 7847 B

ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\root\IMG_1693.JPG

Ready

8:58 PM 10/12/2018

Image 3:

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3

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

Thumbnails

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 9667 B Show Tooltips

Evidence Items

ItemA_thumbdrive.E01

- Partitions
 - Unpartitioned [FAT32]
 - root
 - IMG_1692.JPG
 - IMG_1693.JPG
 - RECYCLE.BIN
 - RFID100.JPG
 - RFID101.JPG
 - RFID102.JPG
 - RFID103.JPG
 - Unallocated space
 - 000573
 - Carved [0].jpg
 - Carved [20794].jpg
 - Carved [207948].jpg
 - 007996
 - Carved [134480].jpg
 - Carved [5571472].jpg
 - Unpartitioned Space [basic disk]
 - [Unallocated space]

Properties

File Content

Hex Text Filtered Natural

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved [0].jpg	3009	.jpg		ItemA_thumbdrive.E01\...\\IMG_1694.JPG	JPEG	n/a	9667 B					n/a	n/a

loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 9667 B

ItemA_thumbdrive.E01\Partition 1\JUMPDRIVE [FAT32]\root\IMG_1694.JPG

Ready

8:58 PM 10/12/2018

EXIF information of Image 3:

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3

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

Thumbnails

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 9667 B Show Tooltip

Evidence Items

- ItemA_thumdrive.E01
 - Partition 1
 - JUMPDRIVE [FAT32]
 - [root]
 - IMG_1692.JPG
 - IMG_1693.JPG
 - IMG_1694.JPG
 - RECYCLE.BIN
 - RFCD130.JPG
 - RFCD134.JPG
 - RFCD144.JPG
 - [unallocated space]
 - 000573
 - Carved [0].jpg
 - Carved (267974).jpg
 - Carved (279948).jpg
 - 007996
 - Carved (134488).jpg
 - Carved (5571472).jpg
 - Unpartitioned Space [base disk]
 - [unallocated space]

Properties

Name: IMG_1694.JPG
Item Number: 1013
File Type: JPEG EXIF
Path: ItemA_thumdrive.E01\Partition JUMPDRIVE [FAT32]\[root]\IMG_1694.JPG

General Info

Physical Size	2,707,456 bytes (2644 KB)
Logical Size	2,707,295 bytes (2643 KB)

Date

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: False Start Cluster: 5,260 File Type (FATFS): 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

ExifImage.Make	Apple
ExifImage.Model	iPhone 6s
ExifImage.Orientation	6
ExifImage.Resolution	72/1
ExifImage.ResolutionUnit	72/1
ExifImage.Software	2
ExifImage.DateTime	9.2.1
ExifImage.YCbCrPositioning	2016/02/23 16:08:30
ExifImage.ExifTag	1
ExifImage.GPSTag	204
ExifImage.ExposureTime	1660
ExifImage.ExposureTime	1/30
ExifPhoto.Number	11/5
ExifPhoto.ExposureProgram	2
ExifPhoto.ISOSpeedRatings	160
ExifPhoto.FNumber	48 50 50 49
ExifPhoto.DateTimeOriginal	2016/02/23 16:08:30
ExifPhoto.DateTimeDigitized	2016/02/23 16:08:30
ExifPhoto.ComponentPCConfiguration	1 2 3 0
ExifPhoto.ShutterSpeedValue	7650/1539
ExifPhoto.ApertureValue	7983/3509
ExifPhoto.ExposureTime	5241/2419
ExifPhoto.SceneCaptureType	0/1
ExifPhoto.MeteringMode	5
ExifPhoto.Flash	24
ExifPhoto.FocalLength	83/20
ExifPhoto.SubjectArea	2015/1511/22/17 13:00

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (2076).jpg	3005	.jpg	ItemA_thumdrive.E01\...	JPEG	n/a	9667 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 9667 B

ItemA_thumdrive.E01\Partition JUMPDRIVE [FAT32]\[root]\IMG_1694.JPG

Ready

8:57 PM 10/12/2016

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Lab3

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

Thumbnails

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 9667 B Show Tooltip

Evidence Items

- ItemA_thumdrive.E01
 - Partition 1
 - JUMPDRIVE [FAT32]
 - [root]
 - IMG_1692.JPG
 - IMG_1693.JPG
 - IMG_1694.JPG
 - RECYCLE.BIN
 - RFCD130.JPG
 - RFCD134.JPG
 - RFCD144.JPG
 - [unallocated space]
 - 000573
 - Carved [0].jpg
 - Carved (267974).jpg
 - Carved (279948).jpg
 - 007996
 - Carved (134488).jpg
 - Carved (5571472).jpg
 - Unpartitioned Space [base disk]
 - [unallocated space]

Properties

Exif Entries

ExifImage.Make	Apple
ExifImage.Model	iPhone 6s
ExifImage.Orientation	6
ExifImage.Resolution	72/1
ExifImage.ResolutionUnit	72/1
ExifImage.Software	2
ExifImage.DateTime	9.2.1
ExifImage.YCbCrPositioning	2016/02/23 16:08:30
ExifImage.ExifTag	1
ExifImage.GPSTag	204
ExifImage.ExposureTime	1660
ExifImage.ExposureTime	1/30
ExifPhoto.Number	11/5
ExifPhoto.ExposureProgram	2
ExifPhoto.ISOSpeedRatings	160
ExifPhoto.FNumber	48 50 50 49
ExifPhoto.DateTimeVersion	2016/02/23 16:08:30
ExifPhoto.DateTimeOriginal	2016/02/23 16:08:30
ExifPhoto.DateTimeDigitized	2016/02/23 16:08:30
ExifPhoto.ComponentPCConfiguration	1 2 3 0
ExifPhoto.ShutterSpeedValue	7650/1539
ExifPhoto.ApertureValue	7983/3509
ExifPhoto.ExposureTime	5241/2419
ExifPhoto.SceneCaptureType	0/1
ExifPhoto.MeteringMode	5
ExifPhoto.Flash	24
ExifPhoto.FocalLength	83/20
ExifPhoto.SubjectArea	2015/1511/22/17 13:00

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved (2076).jpg	3005	.jpg	ItemA_thumdrive.E01\...	JPEG	n/a	9667 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 9667 B

ItemA_thumdrive.E01\Partition JUMPDRIVE [FAT32]\[root]\IMG_1694.JPG

Ready

8:57 PM 10/12/2016

Screenshot of AccessData Forensic Toolkit Version 6.3.0.186 Database: Forensic DB Case: Lab3

The screenshot shows the Evidence Items pane with the following details:

- Evidence:** ItemA_thumddrive.E01
- Partition:** Partition 1 (FAT32)
- File List:** Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 9667 B
- Properties:** A large table showing EXIF and GPS metadata for a single JPEG file.

	Value
Exif.Photo.SubjectArea	2015/11/11 22:17:13
Exif.Photo.MakeNote	63 112 112 108 101 32 105 79 83 0 1 77 77 0 120 109 0 0 1 0 0 4 0 2 0 7 0 2 4 6 0 0 16 0 3 0 7 0 0 10 4 0 2 2 1 0 4 0 9 0 0 0 1
Exif.Photo.SubsecTimeOriginal	604
Exif.Photo.SubsecTimeDigitized	604
Exif.Photo.FlashpixVersion	48 49 49 48
Exif.Photo.ColorSpace	1
Exif.Photo.PixelWidth	4032
Exif.Photo.PixelHeight	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 2620/100
Exif.GPSInfo.LongitudeRef	W
Exif.GPSInfo.Longitude	89/1 44/1 1070/100
Exif.GPSInfoAltitudeRef	0
Exif.GPSInfoAltitude	208/1
Exif.GPSInfo.GPSTimeStamp	21/1 8/1 1445/100
Exif.GPSInfo.GPSSpeedRef	K
Exif.GPSInfo.GPSSpeed	0/1
Exif.GPSInfo.GPSImgDirectionRef	M
Exif.GPSInfo.GPImgDirection	21653/201
Exif.GPSInfo.GPSDestBeearingRef	M
Exif.GPSInfo.GPSDestBeearing	21653/201
Exif.GPSInfo.GPDateStamp	2016/02/23

File List:

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Carved [0].jpg	3005	.jpeg	ItemA_thumddrive.E01\...	JPEG	n/a	9667 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Properties:

	Value	
File Content	Properties	Hex Interpreter

Screenshot of AccessData Forensic Toolkit Version 6.3.0.186 Database: Forensic DB Case: Lab3

The screenshot shows the Evidence Items pane with the following details:

- Evidence:** ItemA_thumddrive.E01
- Partition:** Partition 1 (FAT32)
- File List:** Loaded: 1 Filtered: 1 Total: 1 Highlighted: 0 Checked: 0 Total LSize: 9667 B
- Properties:** A large table showing EXIF and GPS metadata for a single JPEG file.

	Value
Exif.Photo.ColorSpace	1
Exif.Photo.PixelWidth	4032
Exif.Photo.PixelHeight	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 2620/100
Exif.GPSInfo.LongitudeRef	W
Exif.GPSInfo.Longitude	89/1 44/1 1070/100
Exif.GPSInfoAltitudeRef	0
Exif.GPSInfoAltitude	208/1
Exif.GPSInfo.GPSTimeStamp	21/1 8/1 1445/100
Exif.GPSInfo.GPSSpeedRef	K
Exif.GPSInfo.GPSSpeed	0/1
Exif.GPSInfo.GPSImgDirectionRef	M
Exif.GPSInfo.GPImgDirection	21653/201
Exif.GPSInfo.GPSDestBeearingRef	M
Exif.GPSInfo.GPSDestBeearing	21653/201
Exif.GPSInfo.GPDateStamp	2016/02/23

File List:

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Carved [0].jpg	3005	.jpeg	ItemA_thumddrive.E01\...	JPEG	n/a	9667 B	n/a	n/a	n/a	n/a	n/a	n/a	n/a

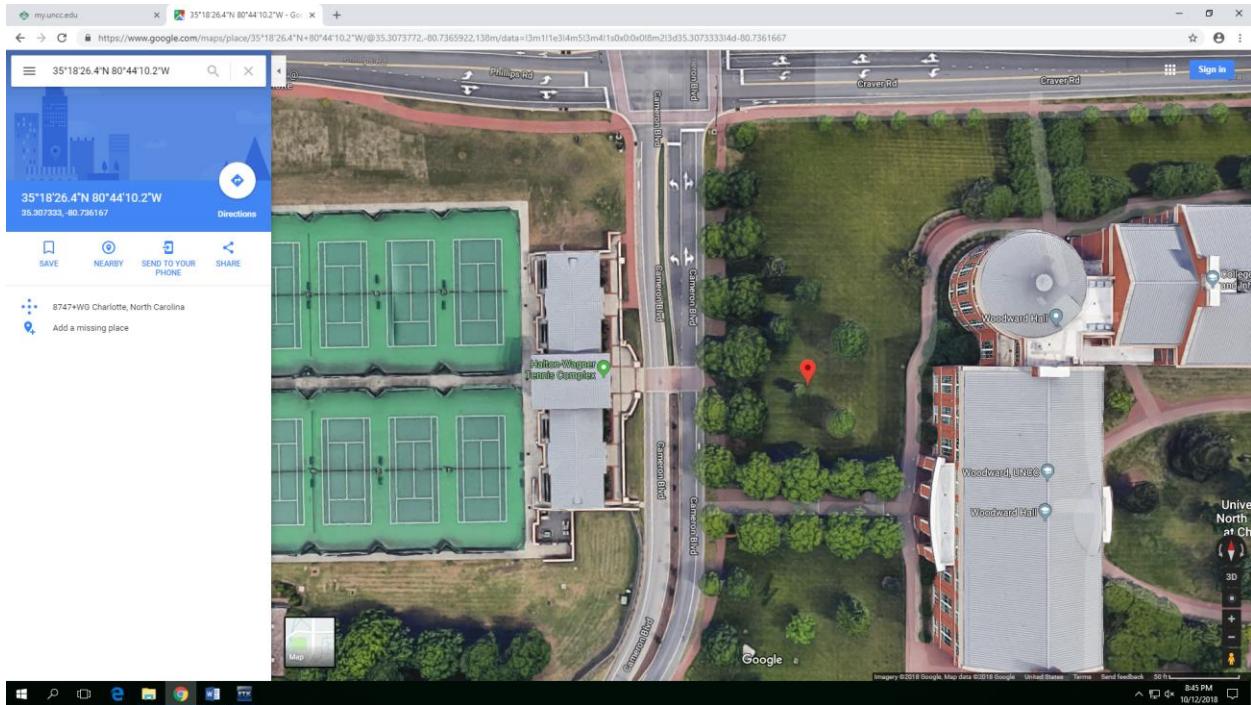
Properties:

	Value	
File Content	Properties	Hex Interpreter

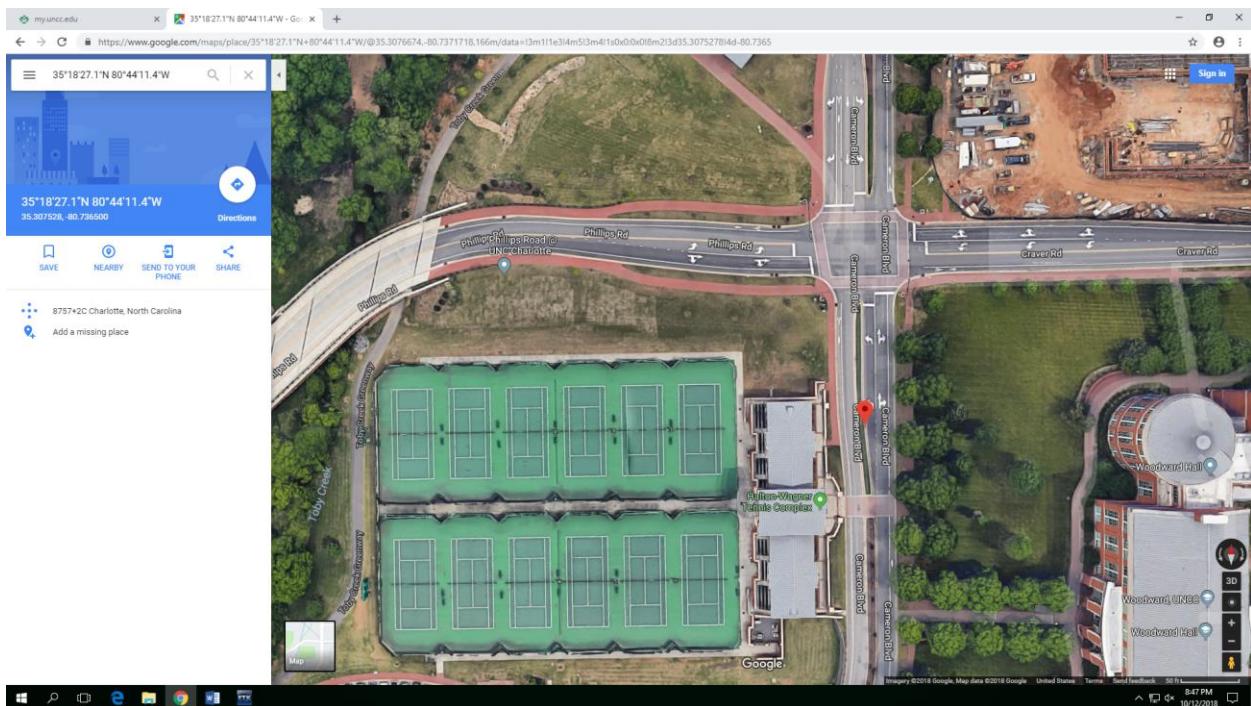
Looking at the **EXIF** information of these **3** pictures, I found out device model, date, time and GPS coordinates.

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

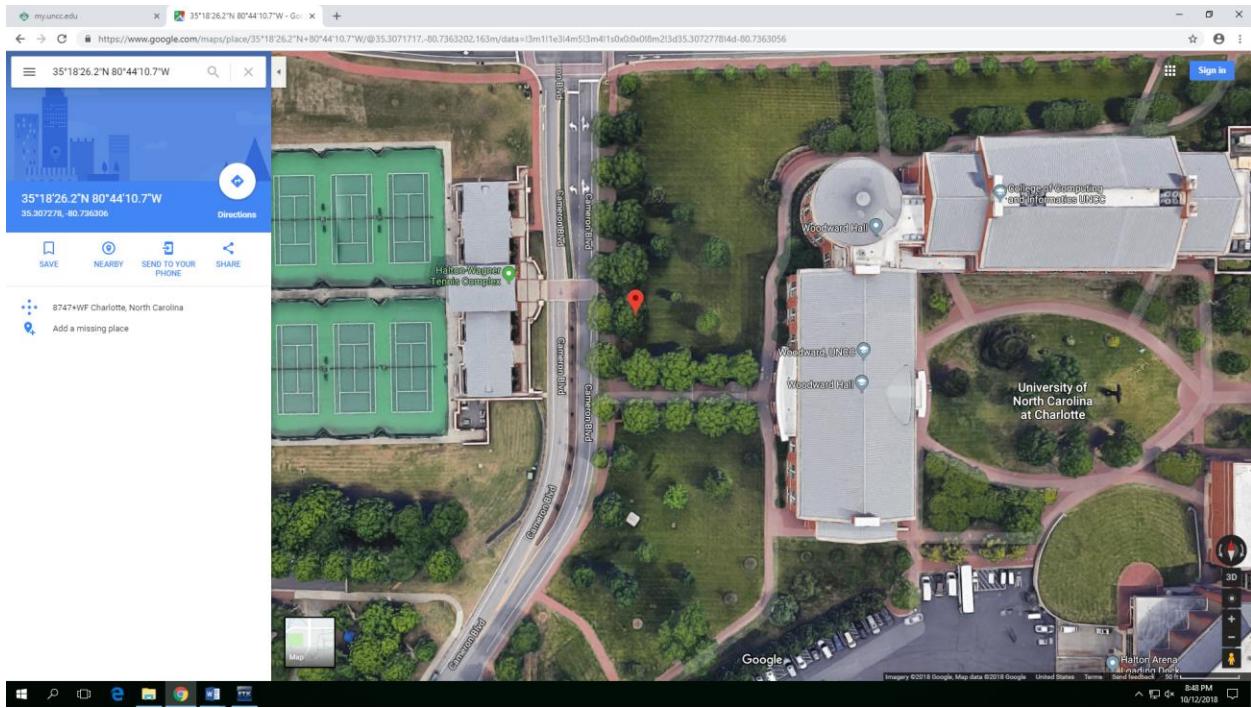
Location for Image 1:



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.