ITIS 5250
Parag Mhatre
Lab 11/16/2018

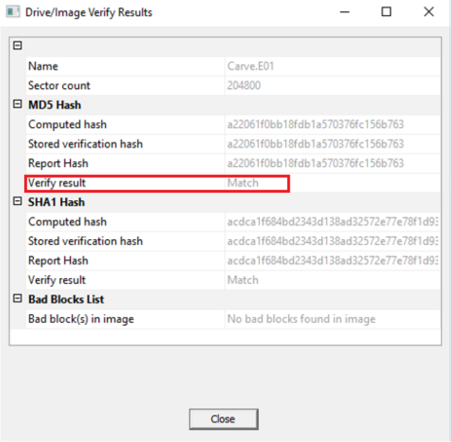
Overview

In this lab, I will be examining two Forensic Images – **“Carve.E01”** and **“Deleted.E01”.** I will perform various operations and examinations using the FTK (Forensic Toolkit) and HxD (Hex Editor) after verifying and matching Hash values. The purpose of this examination is to find the Jpeg files that are in both the forensic images. I also must recover certain files using carving options and find the oldest metadata date of the JPEGs present in the given image files.

Forensic Acquisition & Exam Preparation

I moved the image files from the shared folder in the Forensics Lab, 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** and HxD editor. The MD5 Hash of both the images are as given below:

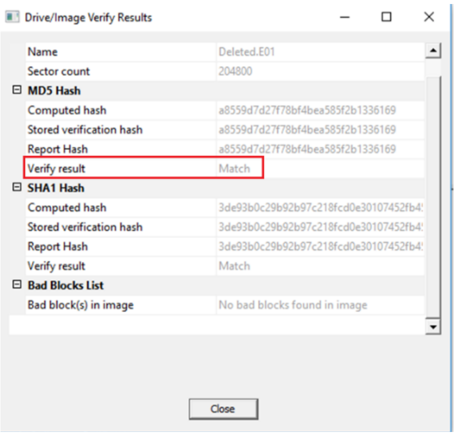
Carve.E01:



Drive/Image Verify Results

Name	Carve.E01
Sector count	204800
MD5 Hash	
Computed hash	a22061f0bb18fdb1a570376fc156b763
Stored verification hash	a22061f0bb18fdb1a570376fc156b763
Report Hash	a22061f0bb18fdb1a570376fc156b763
Verify result	Match
SHA1 Hash	
Computed hash	acdca1f684bd2343d138ad32572e77e78f1d93
Stored verification hash	acdca1f684bd2343d138ad32572e77e78f1d93
Report Hash	acdca1f684bd2343d138ad32572e77e78f1d93
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Deleted.E01:



Drive/Image Verify Results

Name	Deleted.E01
Sector count	204800
MD5 Hash	
Computed hash	a8559d7d27f78bf4bea585f2b1336169
Stored verification hash	a8559d7d27f78bf4bea585f2b1336169
Report Hash	a8559d7d27f78bf4bea585f2b1336169
Verify result	Match
SHA1 Hash	
Computed hash	3de93b0c29b92b97c218fcd0e30107452fb4
Stored verification hash	3de93b0c29b92b97c218fcd0e30107452fb4
Report Hash	3de93b0c29b92b97c218fcd0e30107452fb4
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Findings and Report (Forensic Analysis)

Using the FTK Imager, I mounted the “Carve.E01” on the disk as a physical disk and found the Logical drive labeled **“TEST2”** as **Drive E**:.

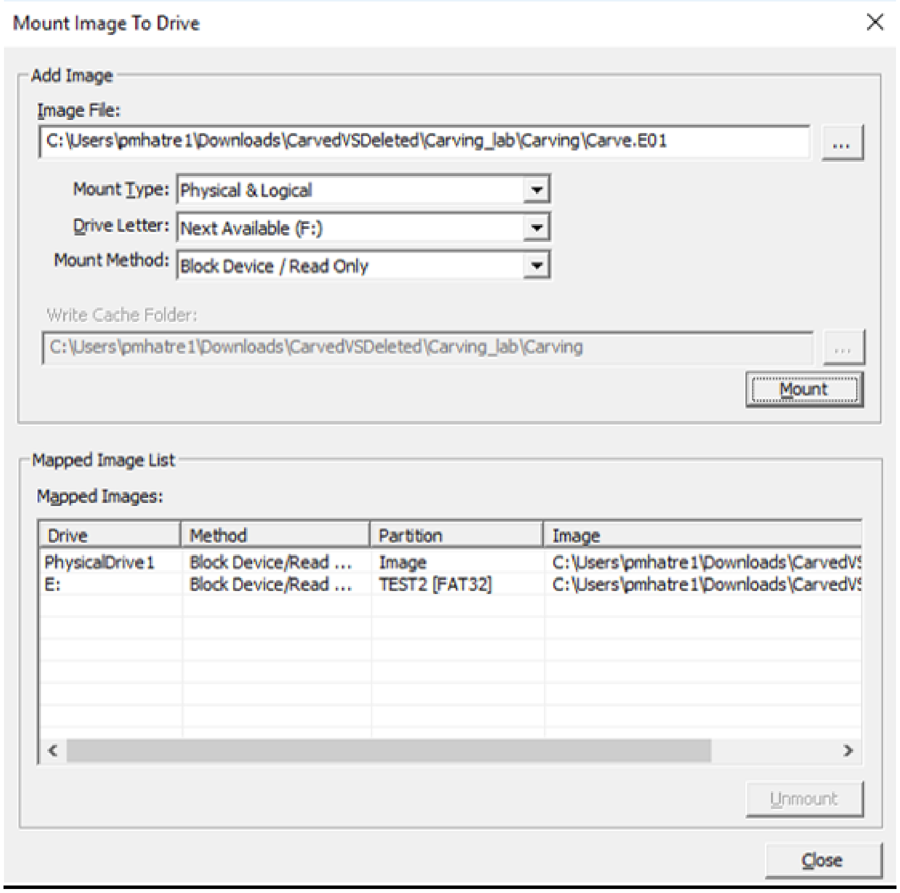


Image File: C:\Users\pmhatre1\Downloads\CarvedVSDeleted\Carving_lab\Carving\Carve.E01

Mount Type: Physical & Logical

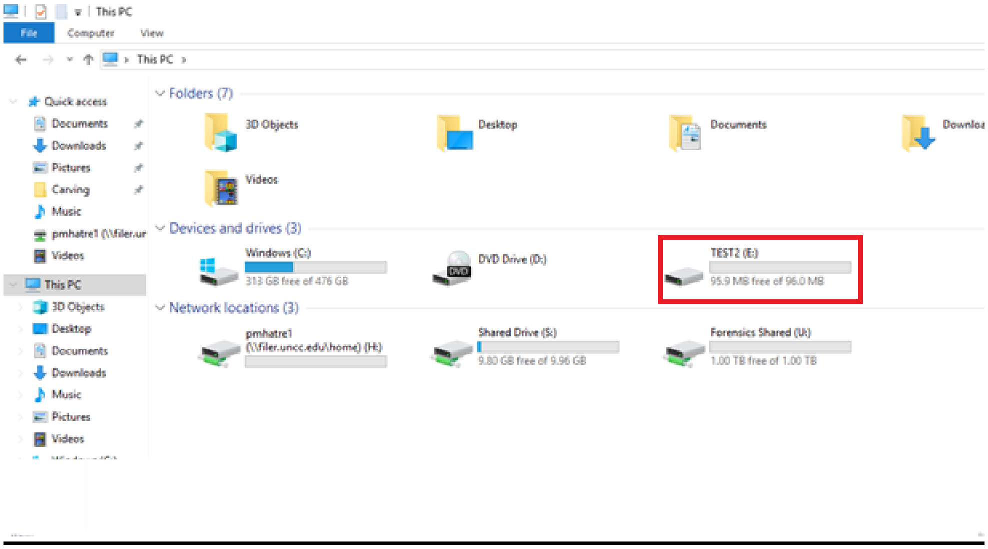
Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

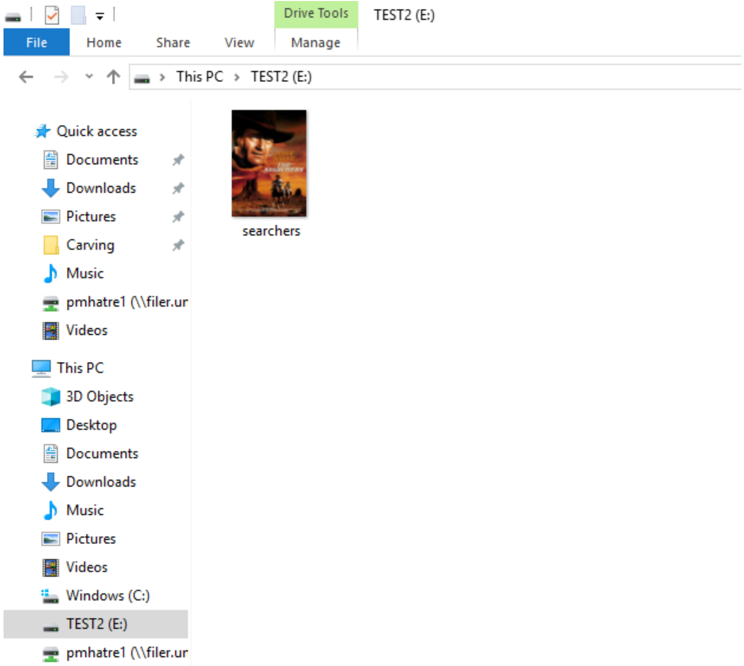
Write Cache Folder: C:\Users\pmhatre1\Downloads\CarvedVSDeleted\Carving_lab\Carving

Mapped Images:

Drive	Method	Partition	Image
PhysicalDrive1	Block Device/Read ...	Image	C:\Users\pmhatre1\Downloads\CarvedV:
E:	Block Device/Read ...	TEST2 [FAT32]	C:\Users\pmhatre1\Downloads\CarvedV:

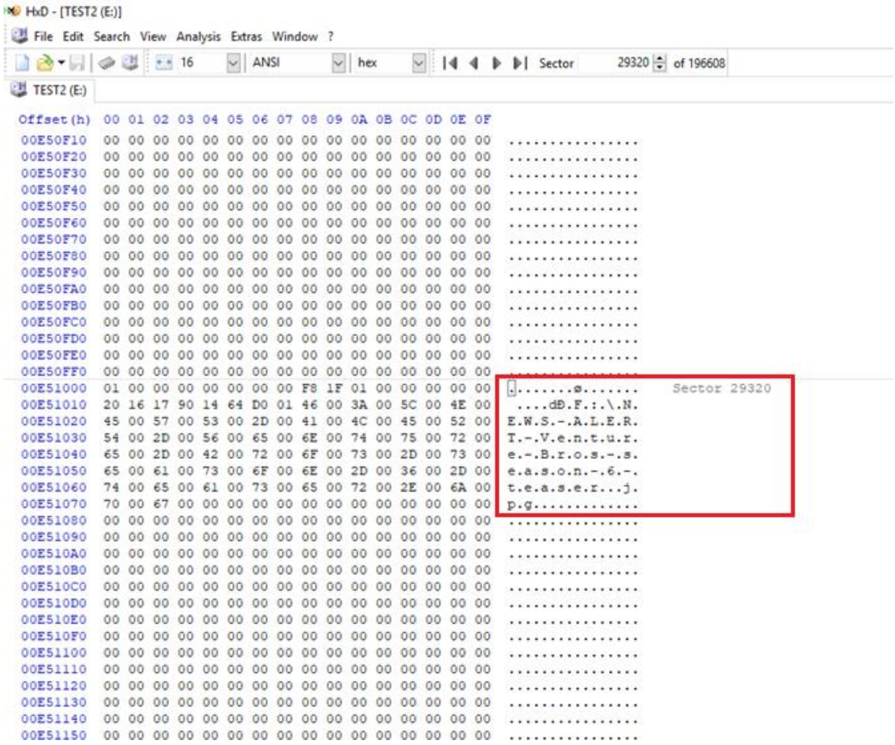


I opened the TEST2 and found the following movie poster in the disk.



(a) From what movie is this poster?

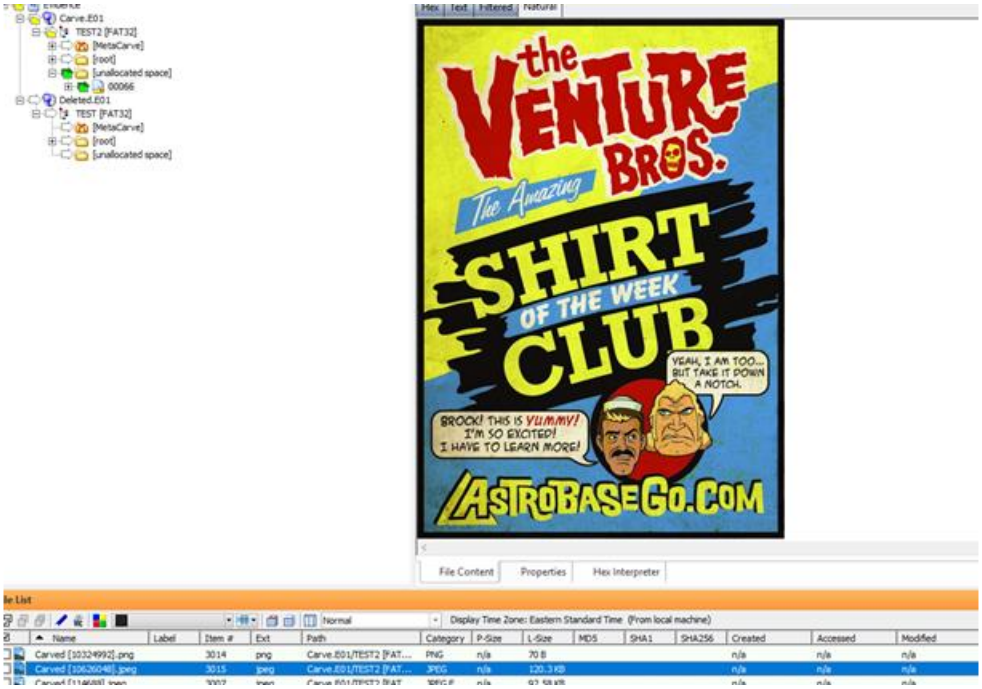
The movie poster is from **"Venture Bros Season 6 Teaser".** I found this in "TEST2" via HxD Editor at **sector 29,320.**



```
16   ANSI   hex   Sector   29320   of 196608

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00E50F10  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50F20  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50F30  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50F40  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50F50  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50F60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50F70  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50F80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50F90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50FA0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50FB0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50FC0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50FD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50FE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E50FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E51000  01 00 00 00 00 00 00 00 F8 1F 01 00 00 00 00 00  ........ø.......     Sector 29320
00E51010  20 16 17 90 14 64 D0 01 46 00 3A 00 5C 00 4E 00   ....dÐ.F.:.\.N.
00E51020  45 00 57 00 53 00 2D 00 41 00 4C 00 45 00 52 00  E.W.S.-.A.L.E.R.
00E51030  54 00 2D 00 56 00 65 00 6E 00 74 00 75 00 72 00  T.-.V.e.n.t.u.r.
00E51040  65 00 2D 00 42 00 72 00 6F 00 73 00 2D 00 73 00  e.-.B.r.o.s.-.s.
00E51050  65 00 61 00 73 00 6F 00 6E 00 2D 00 36 00 2D 00  e.a.s.o.n.-.6.-.
00E51060  74 00 65 00 61 00 73 00 65 00 72 00 2E 00 6A 00  t.e.a.s.e.r...j.
00E51070  70 00 67 00 00 00 00 00 00 00 00 00 00 00 00 00  p.g.............
00E51080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E51090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E510A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E510B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E510C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E510D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E510E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E510F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E51100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E51110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E51120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E51130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E51140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E51150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

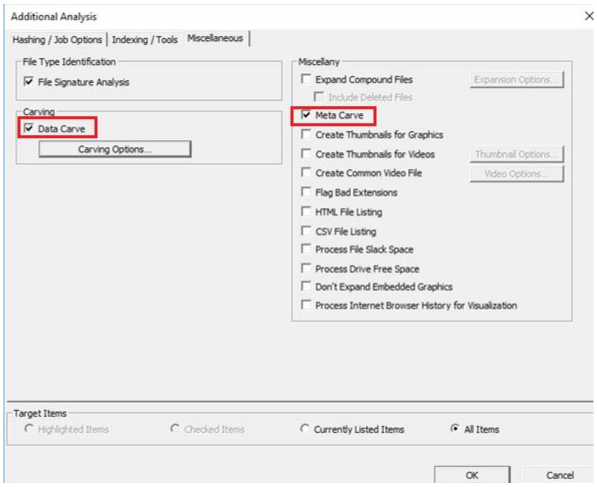
Poster of the movie(Carved during a later step):



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

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Carved [10324992].png		3014	png	Carve.E01/TEST2 [FAT...	PNG	n/a	70 B				n/a	n/a	n/a
Carved [10626048].jpeg		3015	jpeg	Carve.E01/TEST2 [FAT...	JPEG	n/a	120.3 KB				n/a	n/a	n/a
Carved [114688].jpeg		3007	jpeg	Carve.E01/TEST2 [FAT...	JPEG E...	n/a	92.58 KB				n/a	n/a	n/a

Further, I loaded up the images in FTK (Forensic Toolkit) and performed Data carving on “Carve.E01”. I recovered a list of images.

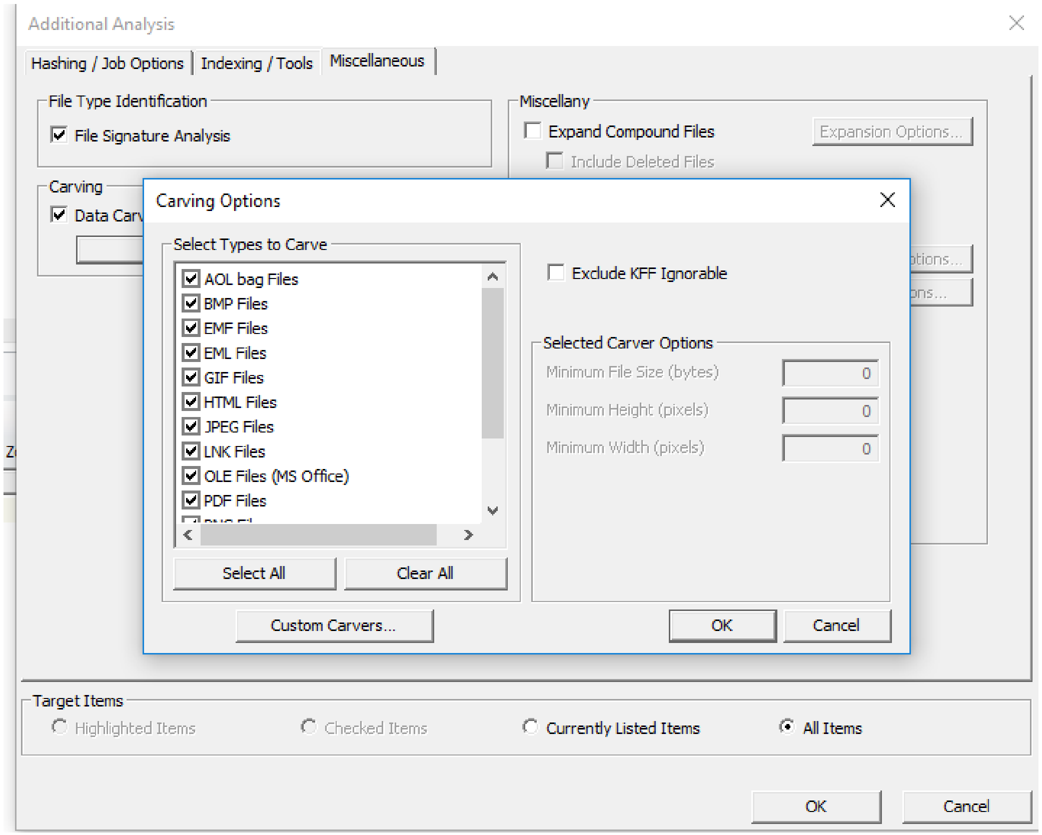


File Type Identification
☑ File Signature Analysis

Carving
☑ Data Carve

Miscellany
☐ Expand Compound Files
☐ Include Deleted Files
☑ Meta Carve
☐ Create Thumbnails for Graphics
☐ Create Thumbnails for Videos
☐ Create Common Video File
☐ Flag Bad Extensions
☐ HTML File Listing
☐ CSV File Listing
☐ Process File Slack Space
☐ Process Drive Free Space
☐ Don't Expand Embedded Graphics
☐ Process Internet Browser History for Visualization

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



Additional Analysis

Hashing / Job Options | Indexing / Tools | Miscellaneous

File Type Identification

☑ File Signature Analysis

Miscellany

□ Expand Compound Files

□ 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

□ Exclude KFF Ignorable

Selected Carver Options

Minimum File Size (bytes) 0

Minimum Height (pixels) 0

Minimum Width (pixels) 0

Target Items

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

(b) Attempt to match jpegs recovered in Carved.e01 that relate to the USS North Carolina from Deleted.e01

The JPEG files:

1. Carved[1270784]
2. Carved[4434944]

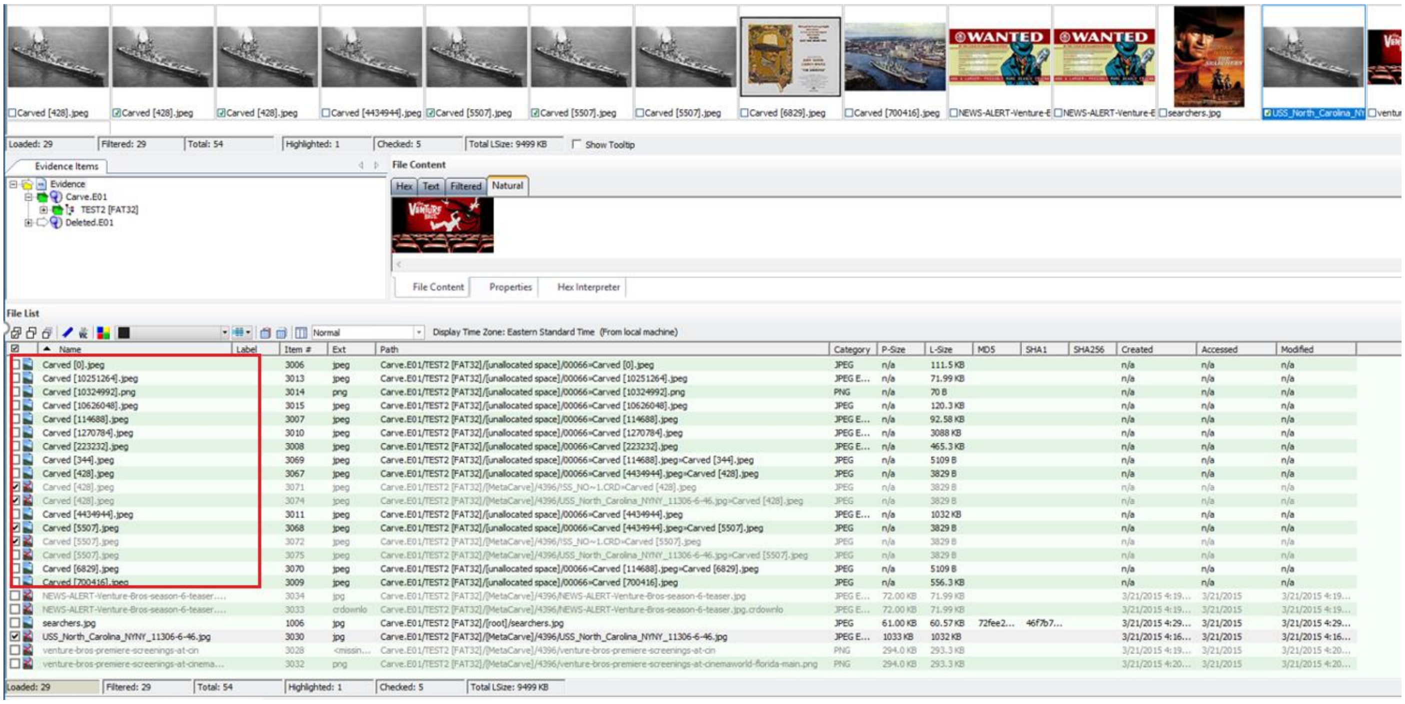
   recovered in ‘Carve.E01’ match to the JPEG files from “Deleted.E01” respectively.

1. U.S.S._North_Carolina
2. U.S.S._North_Carolina_NYNY_11306-6-46

I did the matching by hash values:

1. **Carved[1270784] -** 4aabc32c7d87d77c4ea16fdc24083d77
   U.S.S._North_Carolina - 4aabc32c7d87d77c4ea16fdc24083d77

2. **Carved [4434944] -** 2e1c30db7ae37aaabf5180465656062f
   U.S.S._North_Carolina_NYNY_11306-6-46 - 2e1c30db7ae37aaabf5180465656062f



Loaded: 29 | Filtered: 29 | Total: 54 | Highlighted: 1 | Checked: 5 | Total LSize: 9499 KB

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

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
☐	Carved [0].jpeg		3006	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [0].jpeg	JPEG	n/a	111.5 KB				n/a	n/a	n/a
☐	Carved [10251264].jpeg		3013	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [10251264].jpeg	JPEG E…	n/a	71.99 KB				n/a	n/a	n/a
☐	Carved [10324992].png		3014	png	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [10324992].png	PNG	n/a	70 B				n/a	n/a	n/a
☐	Carved [10626048].jpeg		3015	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [10626048].jpeg	JPEG	n/a	120.3 KB				n/a	n/a	n/a
☐	Carved [114688].jpeg		3007	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [114688].jpeg	JPEG E…	n/a	92.58 KB				n/a	n/a	n/a
☐	Carved [1270784].jpeg		3010	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [1270784].jpeg	JPEG E…	n/a	3088 KB				n/a	n/a	n/a
☐	Carved [223232].jpeg		3008	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [223232].jpeg	JPEG E…	n/a	465.3 KB				n/a	n/a	n/a
☐	Carved [344].jpeg		3069	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [114688].jpeg»Carved [344].jpeg	JPEG	n/a	5109 B				n/a	n/a	n/a
☐	Carved [428].jpeg		3067	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [4434944].jpeg»Carved [428].jpeg	JPEG	n/a	3829 B				n/a	n/a	n/a
☑	Carved [428].jpeg		3071	jpeg	Carve.E01/TEST2 [FAT32]/[MetaCarve]/4396/!SS_NO~1.CRD»Carved [428].jpeg	JPEG	n/a	3829 B				n/a	n/a	n/a
☑	Carved [428].jpeg		3074	jpeg	Carve.E01/TEST2 [FAT32]/[MetaCarve]/4396/USS_North_Carolina_NYNY_11306-6-46.jpg»Carved [428].jpeg	JPEG	n/a	3829 B				n/a	n/a	n/a
☐	Carved [4434944].jpeg		3011	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [4434944].jpeg	JPEG E…	n/a	1032 KB				n/a	n/a	n/a
☑	Carved [5507].jpeg		3068	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [4434944].jpeg»Carved [5507].jpeg	JPEG	n/a	3829 B				n/a	n/a	n/a
☑	Carved [5507].jpeg		3072	jpeg	Carve.E01/TEST2 [FAT32]/[MetaCarve]/4396/!SS_NO~1.CRD»Carved [5507].jpeg	JPEG	n/a	3829 B				n/a	n/a	n/a
☐	Carved [5507].jpeg		3075	jpeg	Carve.E01/TEST2 [FAT32]/[MetaCarve]/4396/USS_North_Carolina_NYNY_11306-6-46.jpg»Carved [5507].jpeg	JPEG	n/a	3829 B				n/a	n/a	n/a
☐	Carved [6829].jpeg		3070	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [114688].jpeg»Carved [6829].jpeg	JPEG	n/a	5109 B				n/a	n/a	n/a
☐	Carved [700416].jpeg		3009	jpeg	Carve.E01/TEST2 [FAT32]/[unallocated space]/00066»Carved [700416].jpeg	JPEG	n/a	556.3 KB				n/a	n/a	n/a
☐	NEWS-ALERT-Venture-Bros-season-6-teaser.…		3034	jpg	Carve.E01/TEST2 [FAT32]/[MetaCarve]/4396/NEWS-ALERT-Venture-Bros-season-6-teaser.jpg	JPEG E…	72.00 KB	71.99 KB				3/21/2015 4:19…	3/21/2015	3/21/2015 4:19…
☐	NEWS-ALERT-Venture-Bros-season-6-teaser.…		3033	crdownlo	Carve.E01/TEST2 [FAT32]/[MetaCarve]/4396/NEWS-ALERT-Venture-Bros-season-6-teaser.jpg.crdownlo	JPEG E…	72.00 KB	71.99 KB				3/21/2015 4:19…	3/21/2015	3/21/2015 4:19…
☐	searchers.jpg		1006	jpg	Carve.E01/TEST2 [FAT32]/[root]/searchers.jpg	JPEG	61.00 KB	60.57 KB	72fee2…	46f7b7…		3/21/2015 4:29…	3/21/2015	3/21/2015 4:29…
☑	USS_North_Carolina_NYNY_11306-6-46.jpg		3030	jpg	Carve.E01/TEST2 [FAT32]/[MetaCarve]/4396/USS_North_Carolina_NYNY_11306-6-46.jpg	JPEG E…	1033 KB	1032 KB				3/21/2015 4:16…	3/21/2015	3/21/2015 4:16…
☐	venture-bros-premiere-screenings-at-cin		3028	<missin…	Carve.E01/TEST2 [FAT32]/[MetaCarve]/4396/venture-bros-premiere-screenings-at-cin	PNG	294.0 KB	293.3 KB				3/21/2015 4:19…	3/21/2015	3/21/2015 4:20…
☐	venture-bros-premiere-screenings-at-cinema…		3032	png	Carve.E01/TEST2 [FAT32]/[MetaCarve]/4396/venture-bros-premiere-screenings-at-cinemaworld-florida-main.png	PNG	294.0 KB	293.3 KB				3/21/2015 4:20…	3/21/2015	3/21/2015 4:20…

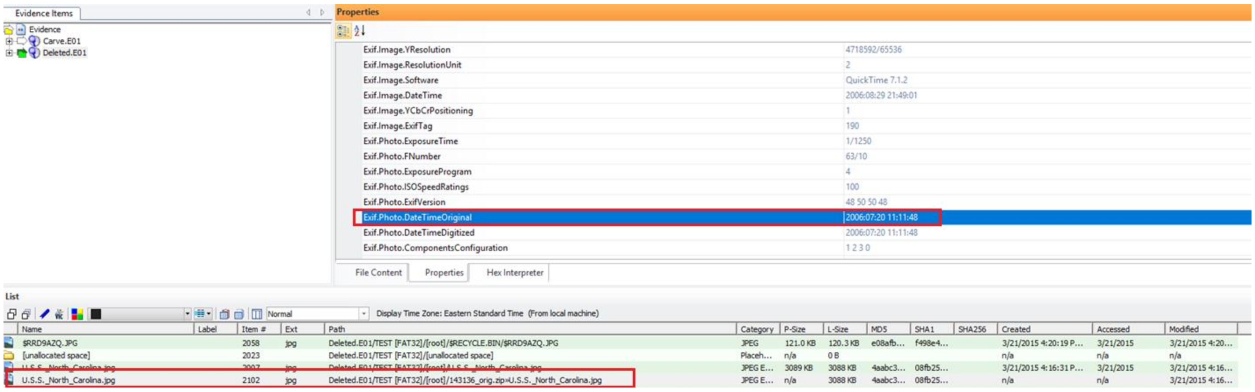
Loaded: 29 | Filtered: 29 | Total: 54 | Highlighted: 1 | Checked: 5 | Total LSize: 9499 KB

(c) How did you find files in Deleted that are also found in Carved?

After loading the images into FTK, I performed "Data Carving" and "Meta Carving" and recovered files in Carve.E01. Then using the "Graphics" tab, I checked the images and attempted to match them visually. After, matching the size of the image and further using hash values to watch, I matched the images mentioned in the question above.

(d) What is the oldest meta data date you were able to find associated with any of these files?

The oldest Meta data date amongst all the files in both the forensic images is that of U.S.S._North_Carolina.jpg. The date is 2006/07/20.



Properties

Exif.Image.YResolution	4718592/65536
Exif.Image.ResolutionUnit	2
Exif.Image.Software	QuickTime 7.1.2
Exif.Image.DateTime	2006:08:29 21:49:01
Exif.Image.YCbCrPositioning	1
Exif.Image.ExifTag	190
Exif.Photo.ExposureTime	1/1250
Exif.Photo.FNumber	63/10
Exif.Photo.ExposureProgram	4
Exif.Photo.ISOSpeedRatings	100
Exif.Photo.ExifVersion	48 50 50 48
Exif.Photo.DateTimeOriginal	2006:07:20 11:11:48
Exif.Photo.DateTimeDigitized	2006:07:20 11:11:48
Exif.Photo.ComponentsConfiguration	1 2 3 0

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

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
$RRD9AZQ.JPG		2058	jpg	Deleted.E01/TEST [FAT32]/[root]/$RECYCLE.BIN/$RRD9AZQ.JPG	JPEG	121.0 KB	120.3 KB	e08afb…	f498e4…		3/21/2015 4:20:19 P…	3/21/2015	3/21/2015 4:20…
[unallocated space]		2023		Deleted.E01/TEST [FAT32]/[unallocated space]	Placeh…	n/a	0 B				n/a	n/a	n/a
U.S.S._North_Carolina.jpg		2097	jpg	Deleted.E01/TEST [FAT32]/[root]/U.S.S._North_Carolina.jpg	JPEG E…	3089 KB	3088 KB	4aabc3…	08fb25…		3/21/2015 4:16:31 P…	3/21/2015	3/21/2015 4:16…
U.S.S._North_Carolina.jpg		2102	jpg	Deleted.E01/TEST [FAT32]/[root]/143136_orig.zip»U.S.S._North_Carolina.jpg	JPEG E…	n/a	3088 KB	4aabc3…	08fb25…		n/a	n/a	3/21/2015 4:16…

Conclusion:

I successfully completed the forensic operations on the given images “Carve.E01” and “Deleted.E01”. After performing all the given tasks, my findings are as follows:

(a) The name of the movie poster on Carved.E01 is “Venture Bros”.
(b) I was able to match 2 images from “Carved.E01” to 2 images from “Deleted.E01”
(c) After performing file carving, I matched the images visually and from file size. After that, hash matching helped me match the images.
(d) The oldest meta data date associated with any of the files is 2006/07/20 that of U.S.S._North_Carolina.jpg