ITIS 5250
Sneha Rangari
Lab 5
11/13/2018

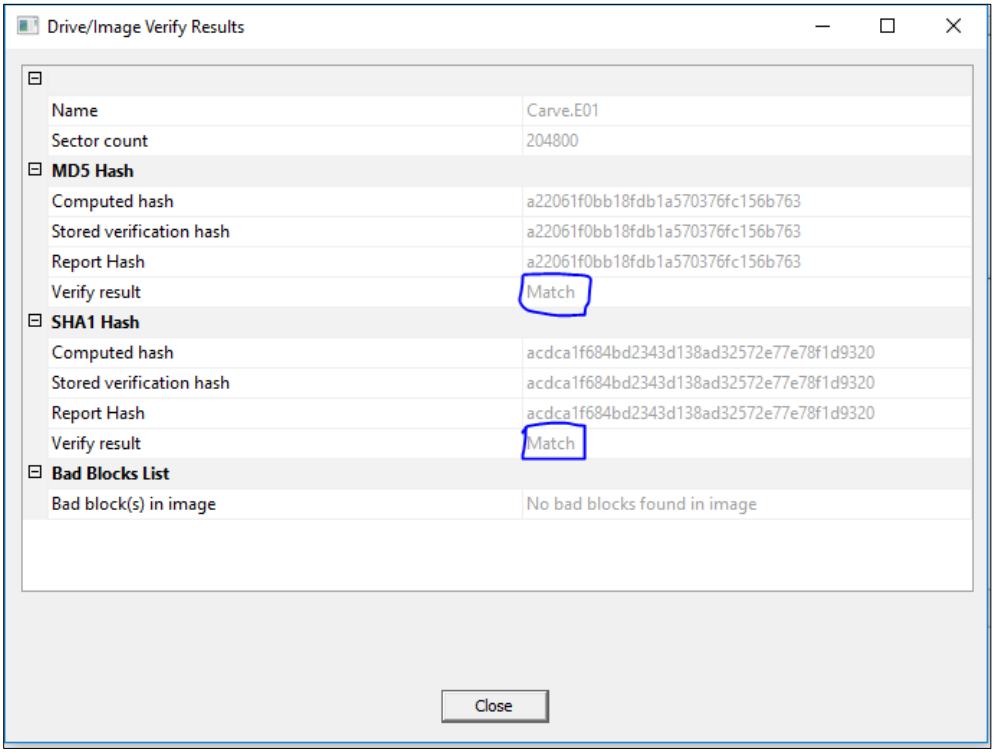
Overview:

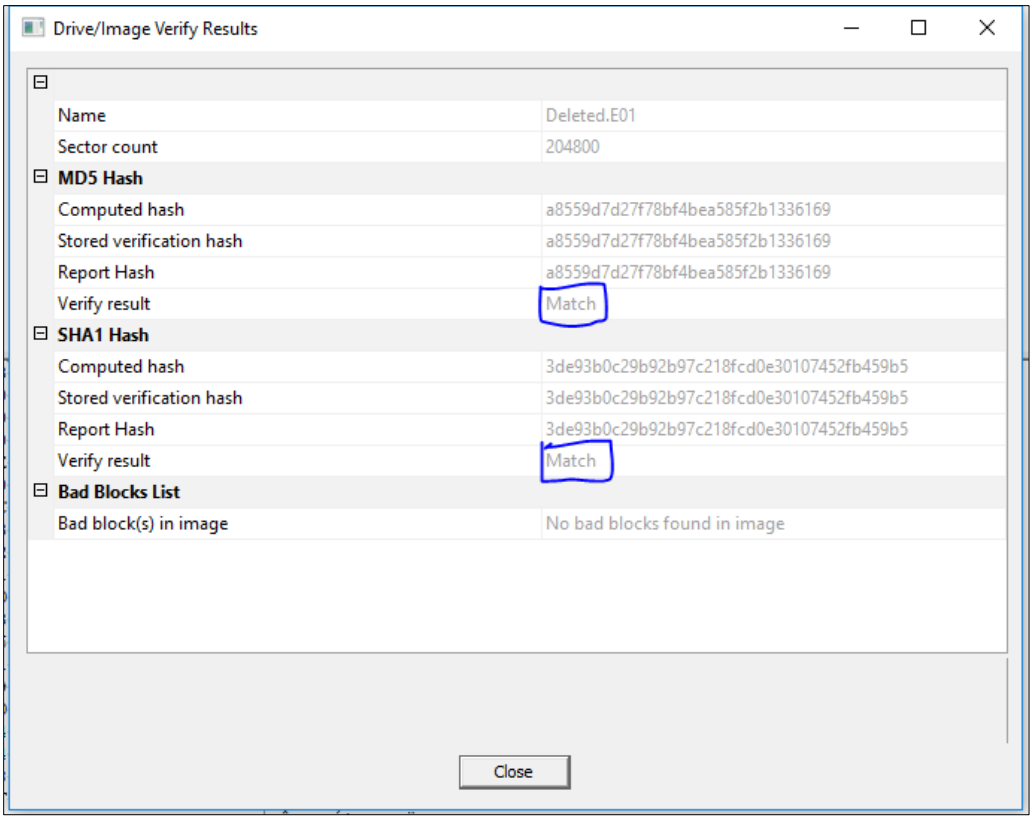
In this Lab, I have been given two files, namely “Carve.E01” and “Deleted.E01”. I have been asked to make use of the “FTK Tool” along with “FTK Imager Tool” and “HxD Editor” and to find the name of a movie poster and to compare the Jpeg files from the carved and deleted image files and find the oldest meta data date file.

Forensic Acquisition & Exam Preparation:

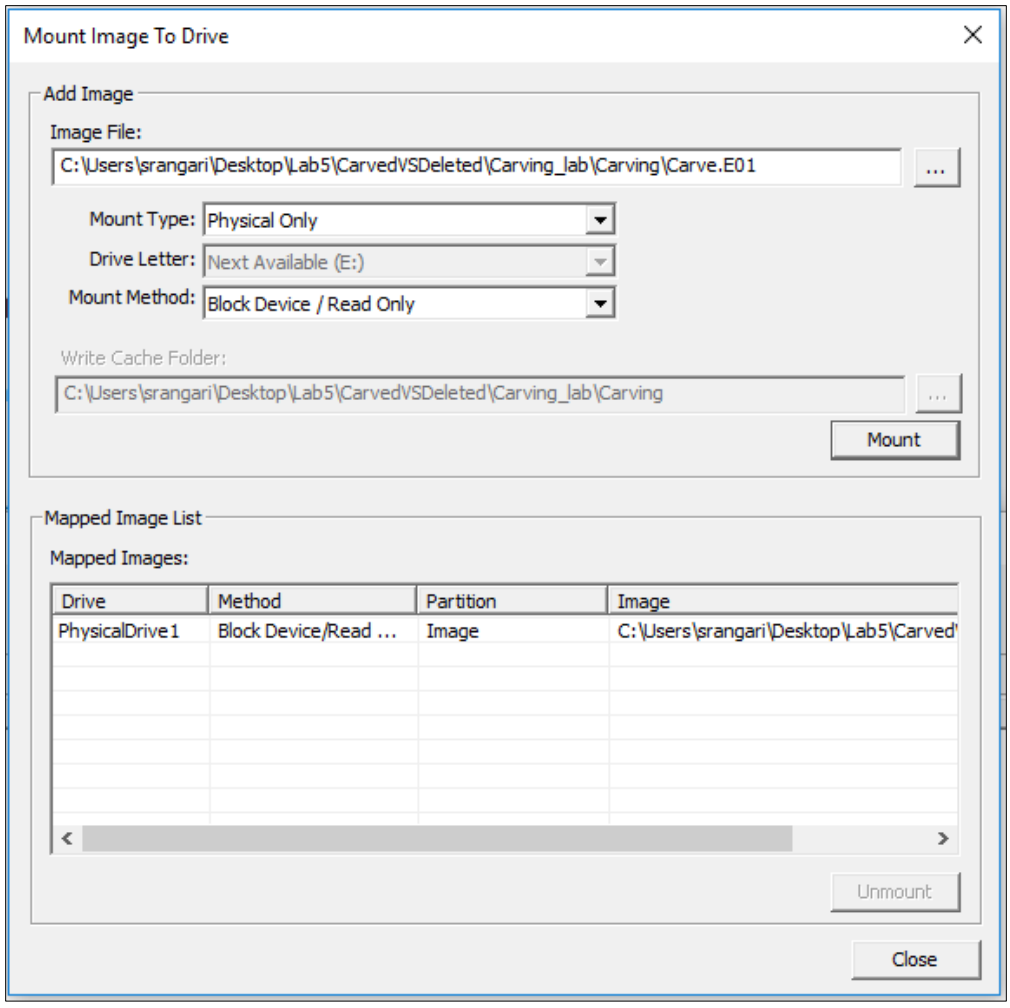
I accessed the Forensic images in the Shared Folder on the network from the Forensics Lab in Cone 169. I accessed images named “Carve.E01” and “Deleted.E01” and their log files. The software used for accessing & extracting information from the image is FTK Imager 4.1.1.1. The first step undertaken after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

Later, I loaded these two images using FTK Imager and verified their **integrity**.

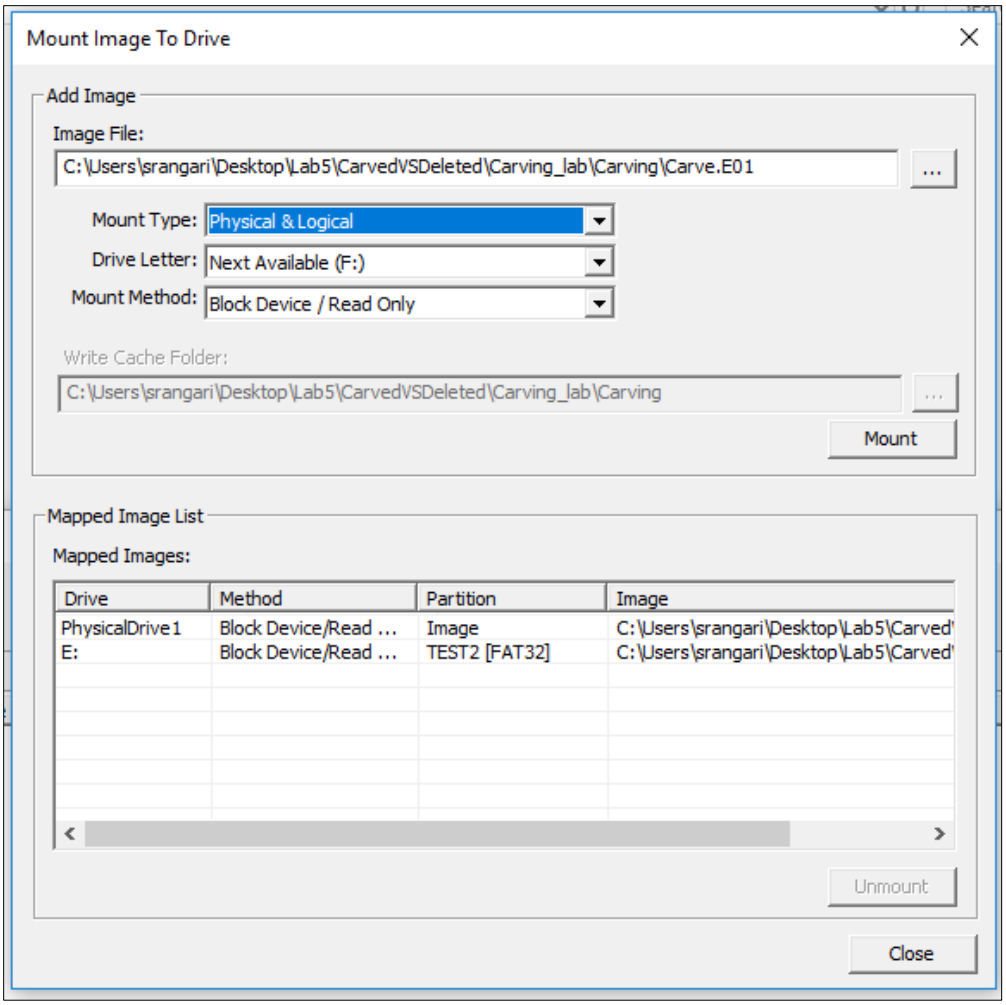


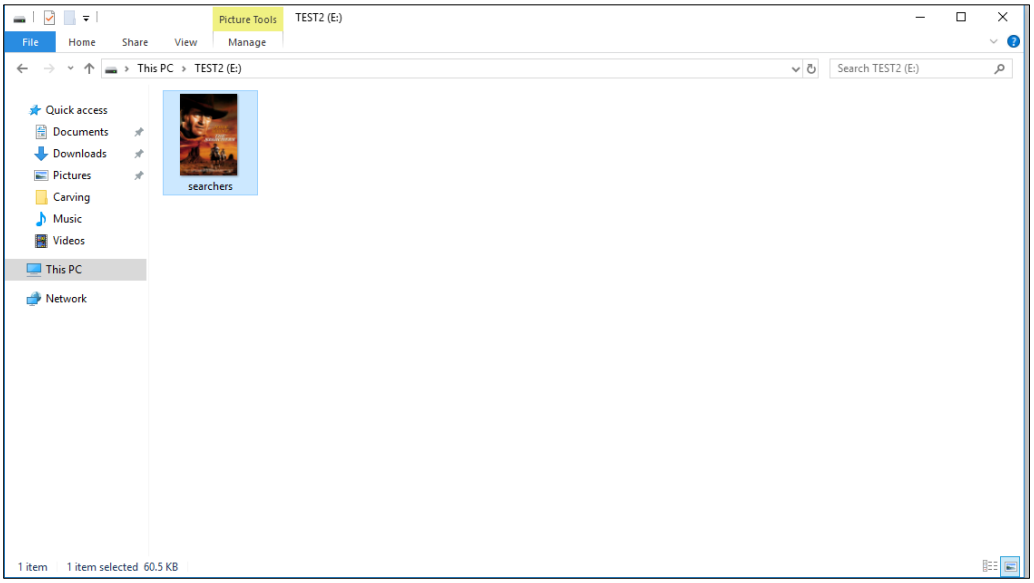


Later I opened the Image Carved.E01 with FTK Imager and right clicked on the image and selected “Image Mounting”. Thus I mounted ‘Carve.E01’ as a physical disk.

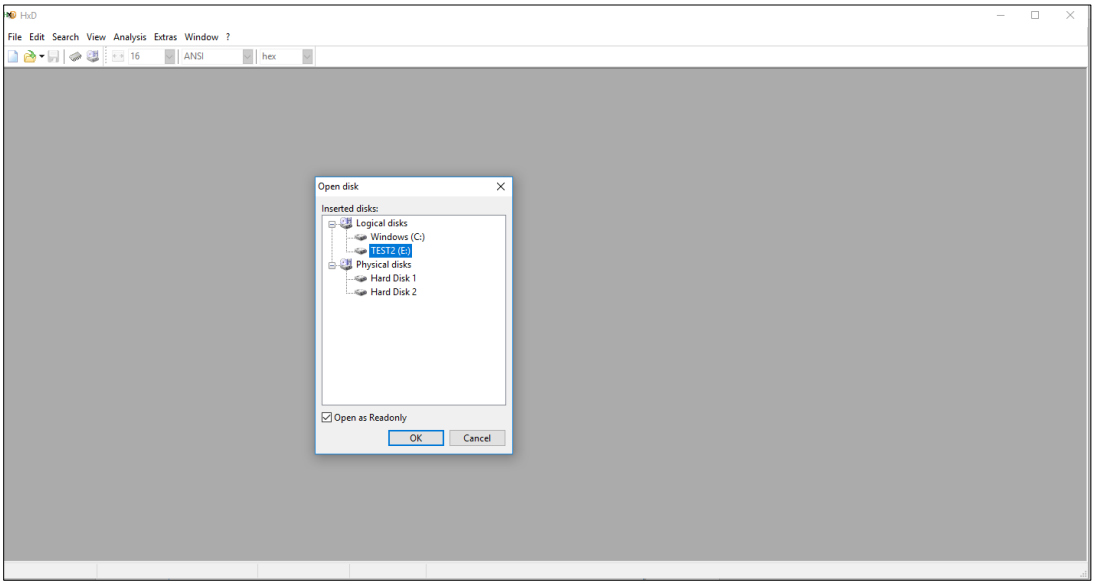


I verified the disk is mounted by locating a new drive in file explorer labeled “TEST2”. I browsed this drive to see a movie poster in the filesystem.


Mount Image To Drive
Add Image
Image File:
C:\Users\srangari\Desktop\Lab5\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\srangari\Desktop\Lab5\CarvedVSDeleted\Carving_lab\Carving
...
Mount
Mapped Image List
Mapped Images:
Drive
Method
Partition
Image
PhysicalDrive1
Block Device/Read ...
Image
C:\Users\srangari\Desktop\Lab5\Carved'
E:
Block Device/Read ...
TEST2 [FAT32]
C:\Users\srangari\Desktop\Lab5\Carved'
Unmount
Close


Picture Tools
TEST2 (E:)
File
Home
Share
View
Manage
This PC
TEST2 (E:)
Search TEST2 (E:)
Quick access
Documents
Downloads
Pictures
Carving
Music
Videos
This PC
Network
searchers
1 item
1 item selected 60.5 KB

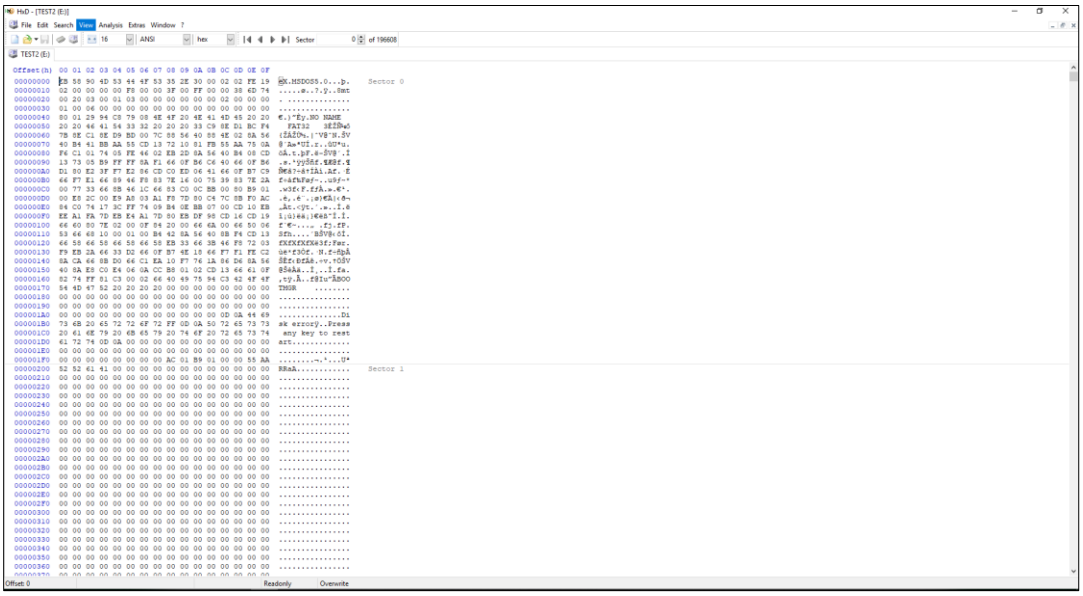
Lastly, I opened HxD (As Administrator), from the menu, opened Extras and opened Disk. Selected the physical disk matching the newly mounted image.

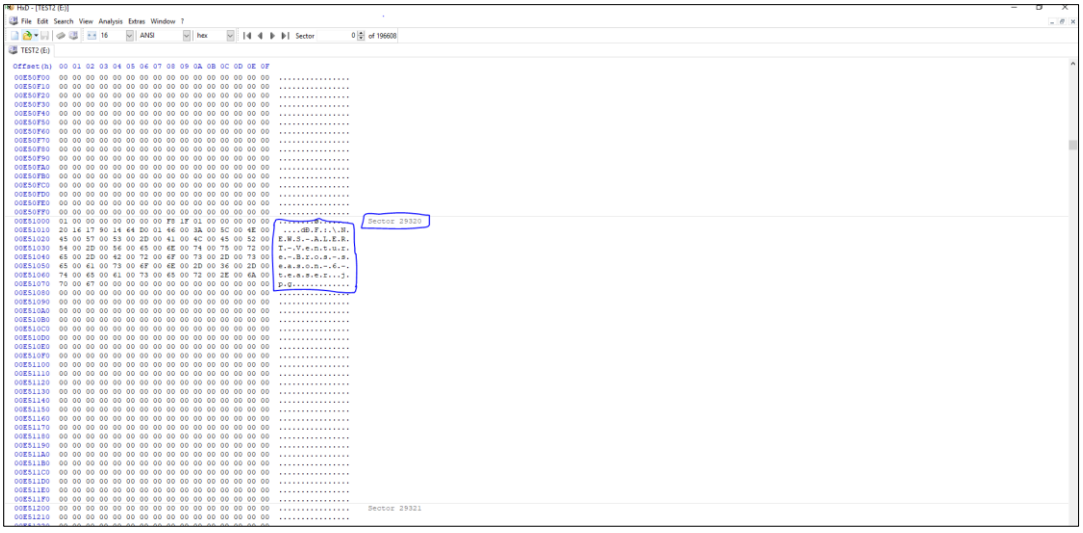


Findings & Report (Forensic Analysis)

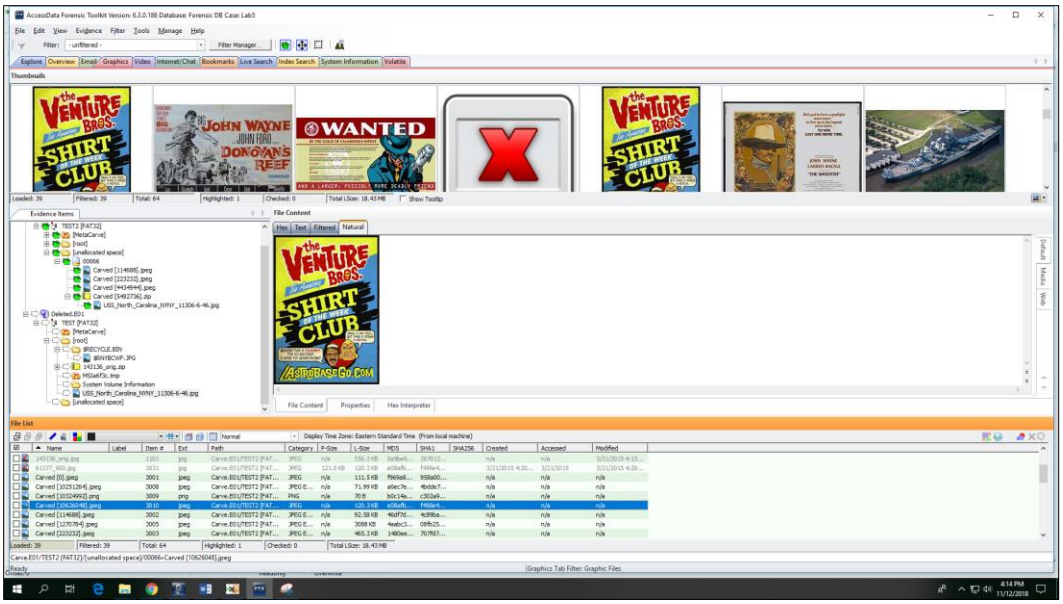
From what different movie is the poster from the newly mounted drive?

In HxD editor, after selecting ‘TEST2(E:)’ drive, at sector 29320, I found a movie named ‘**Venture Bros**’ which is name of different movie.





Movie Poster:

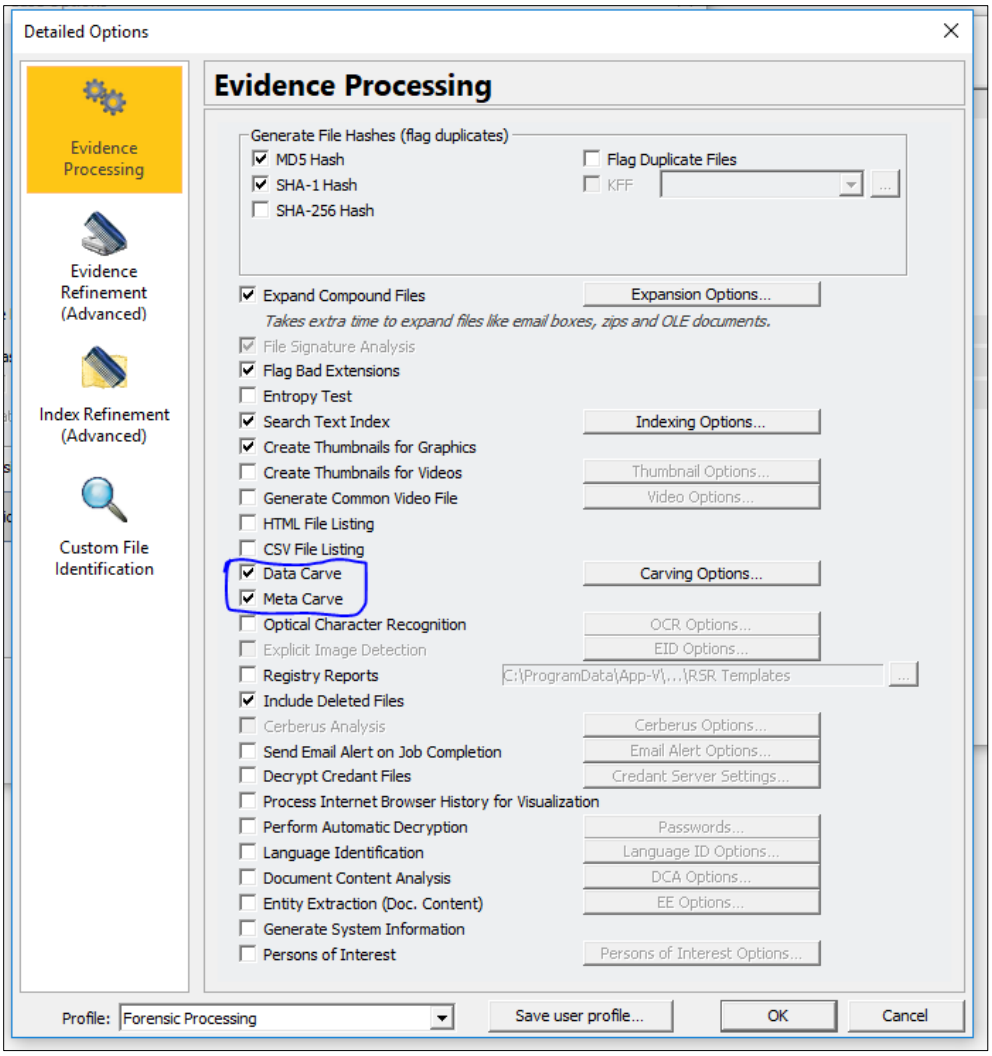


How did you find files in Deleted.E01 that are also found in 'Carve.E01'?

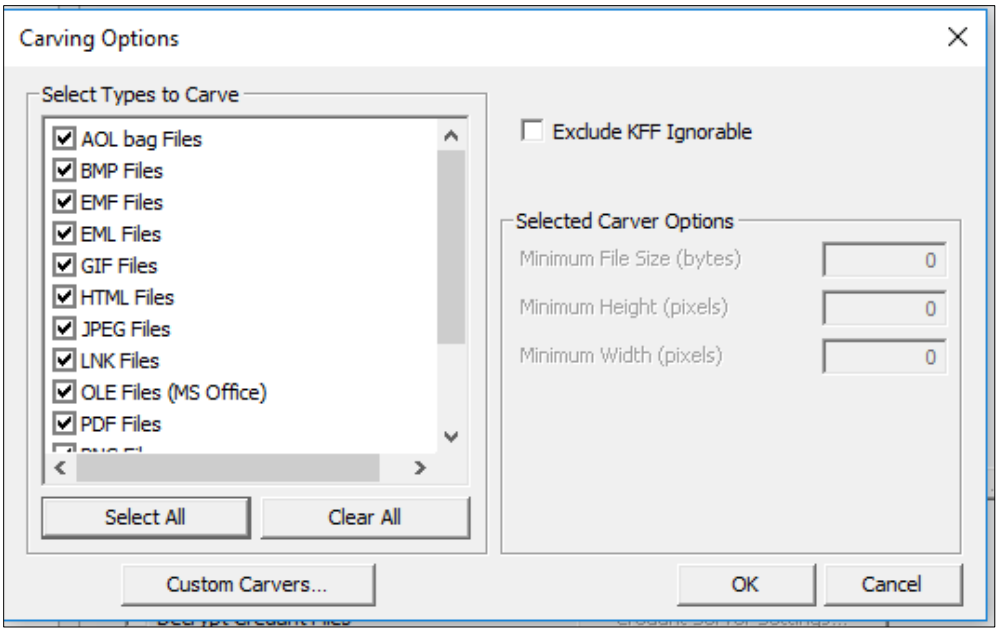
In the FTK, I **performed carving** where I was able to recover files in 'Deleted.E01'.

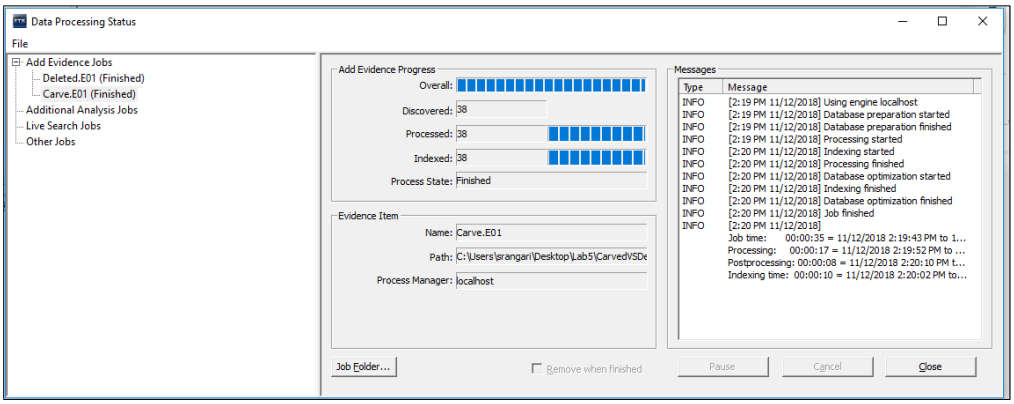
Firstly, I customized processing profile by adding options:

- Data Carve
- Meta Carve



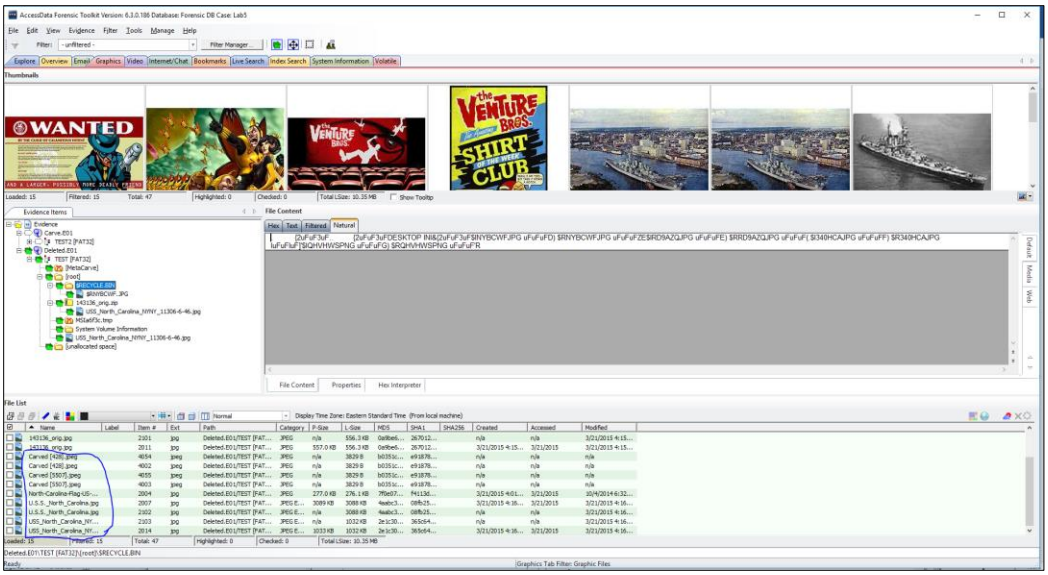
In Carving options, I selected all types to Carve.



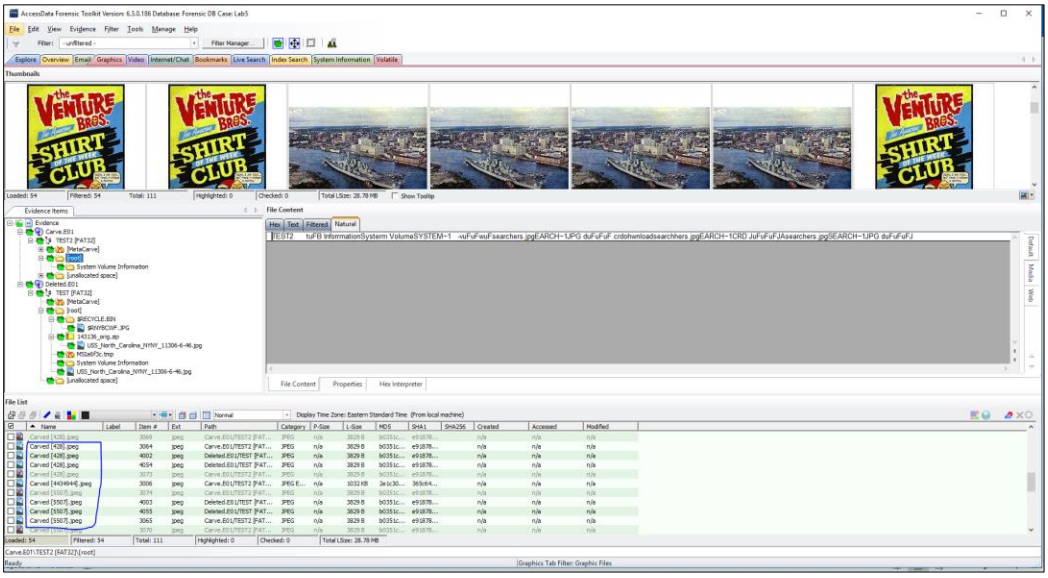


Later I explored the TESTFAT32 folder and checked all the images in the both deleted image file and carved image file and compared all the images.

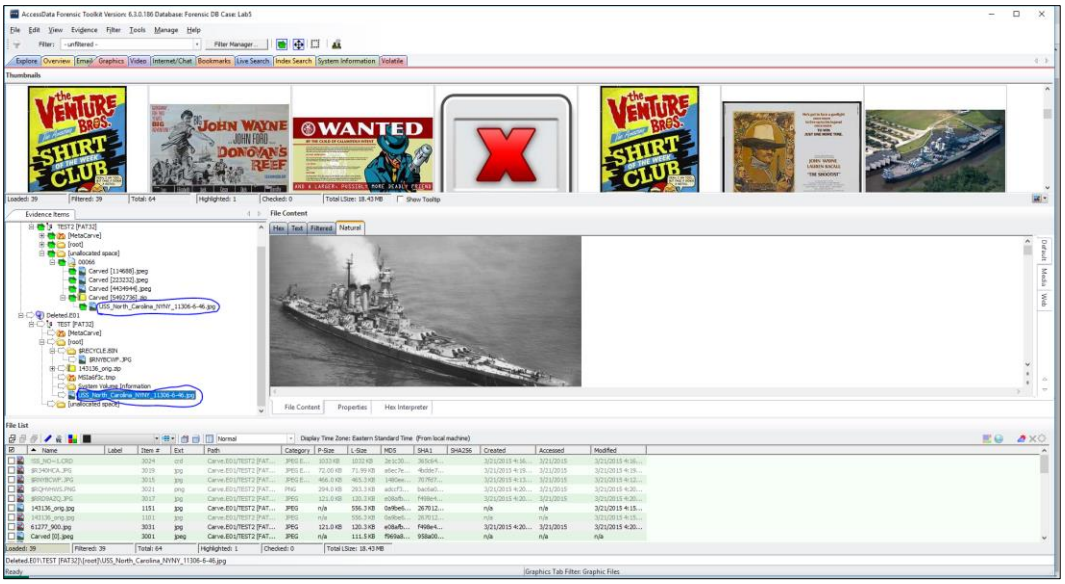
From Deleted.E01 file:

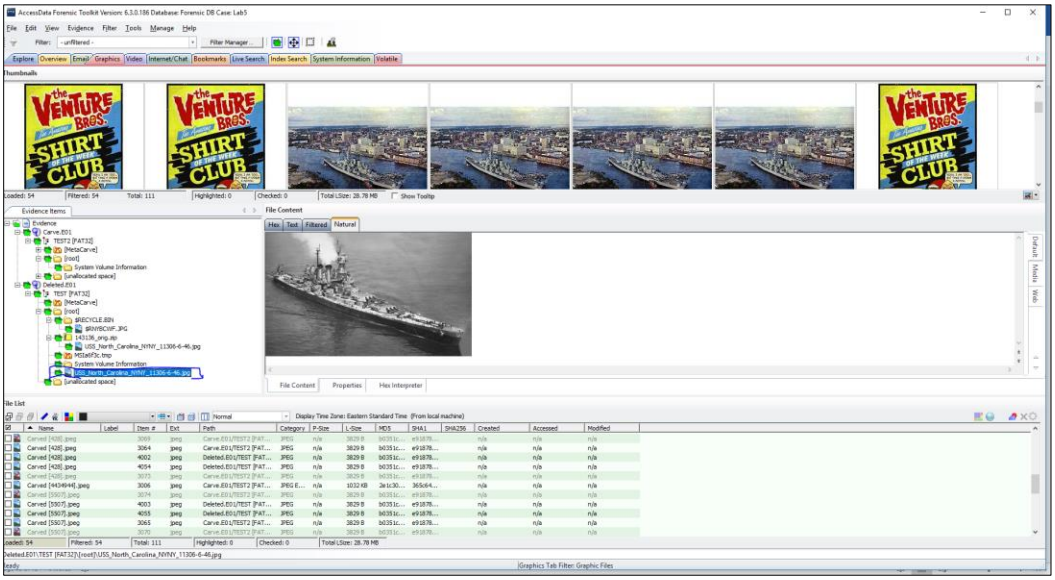


From Carve.E01 File:



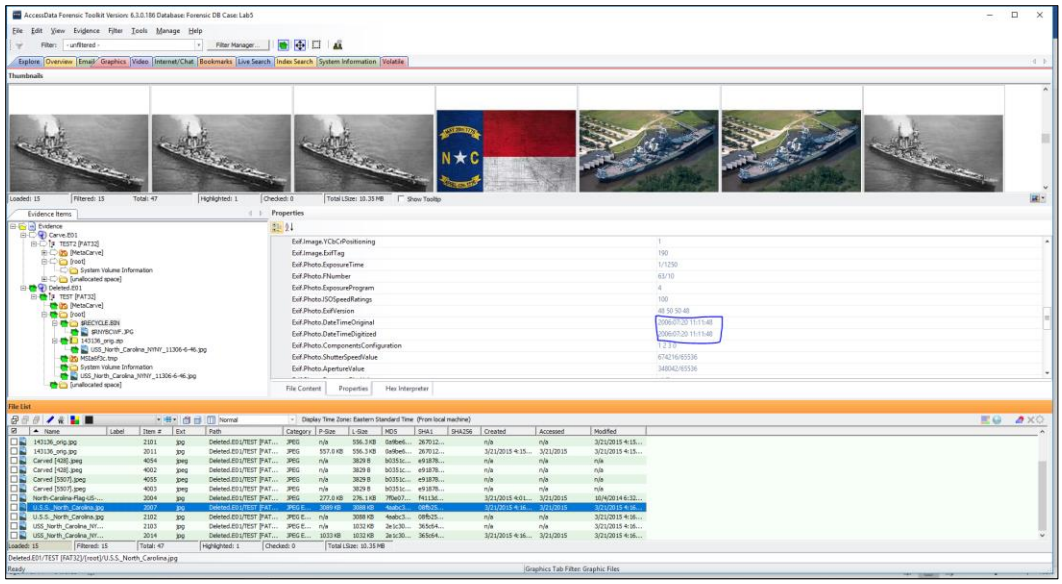
The following are the jpegs that are **recovered** in ‘Carve.E01’ that **relate** to the USS North Carolina from’Deleted.E01’.



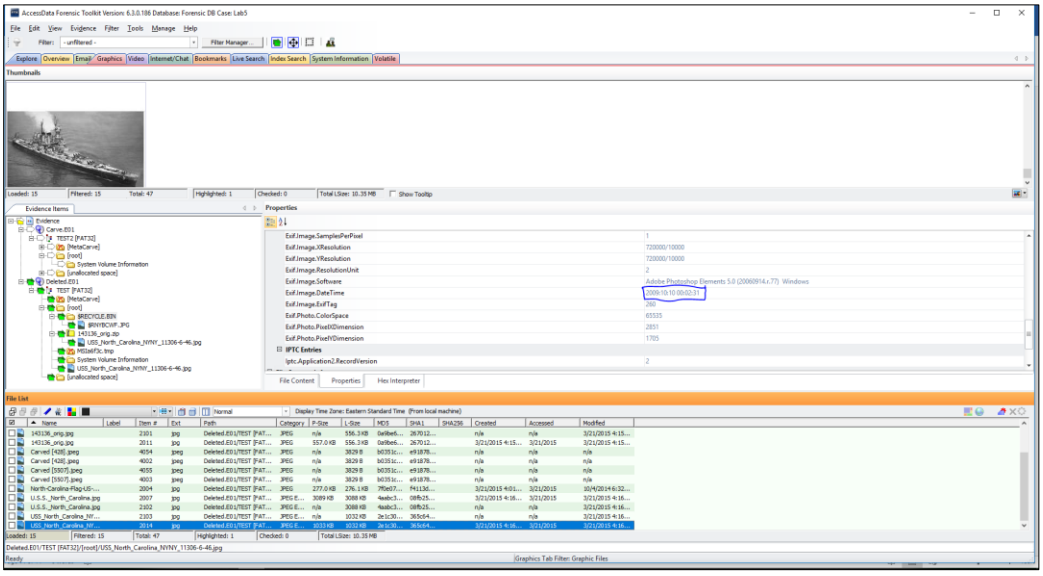


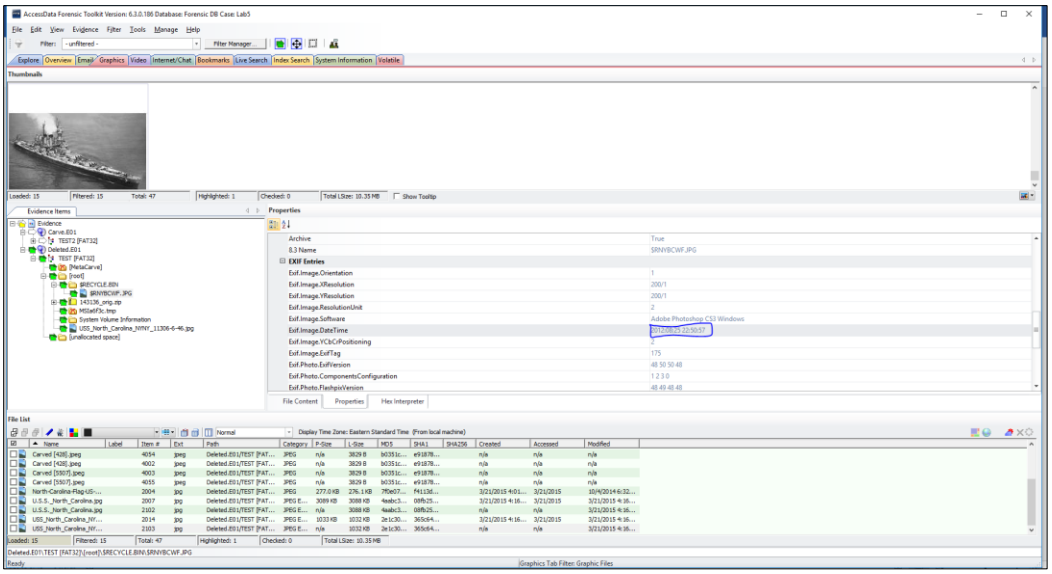
What is the oldest meta date you were able to find associated with any of these files?

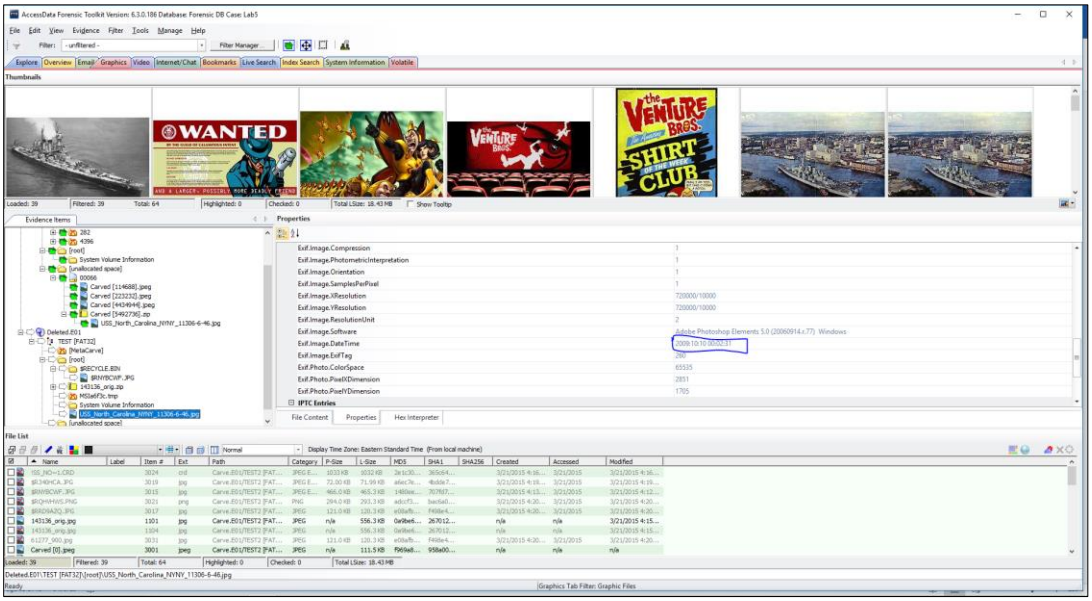
The oldest meta date amongst all these files in both the images is **2006/07/20** of USS_North_Carolina.jpg as shown.



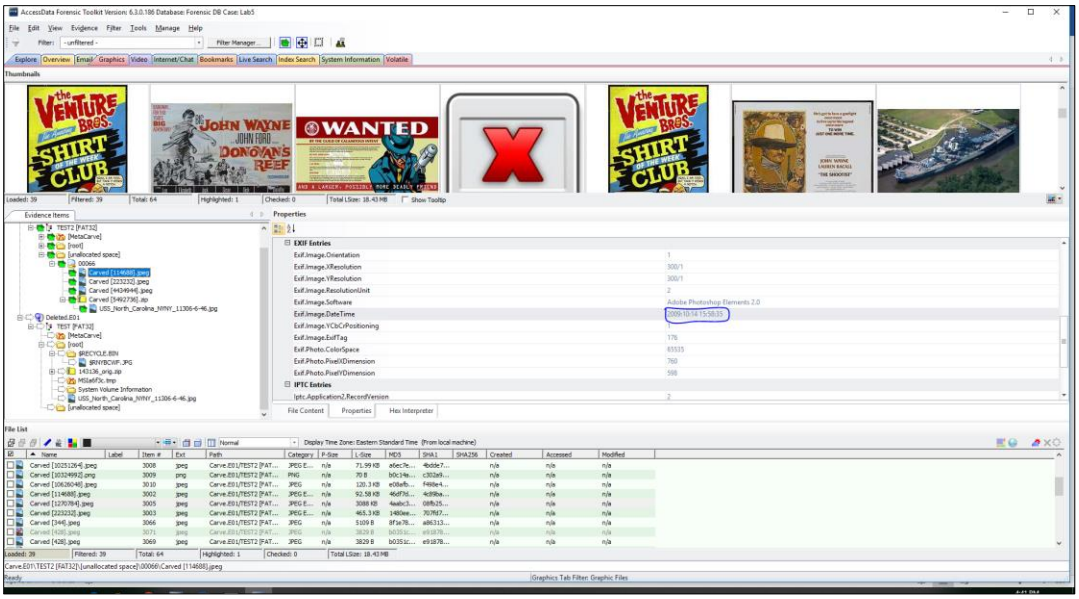
From Deleted.E01 File:

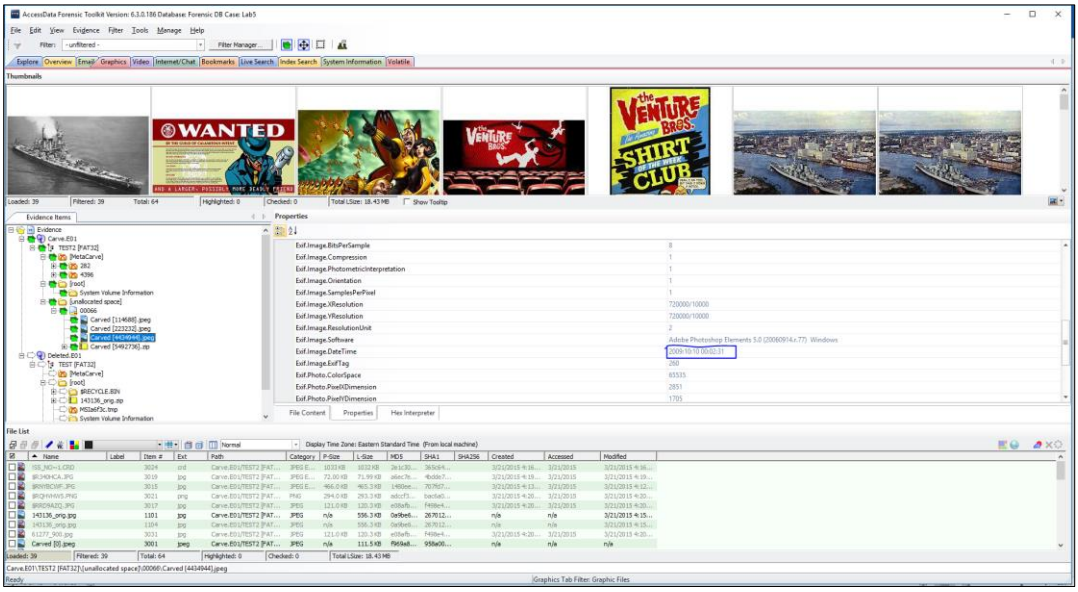


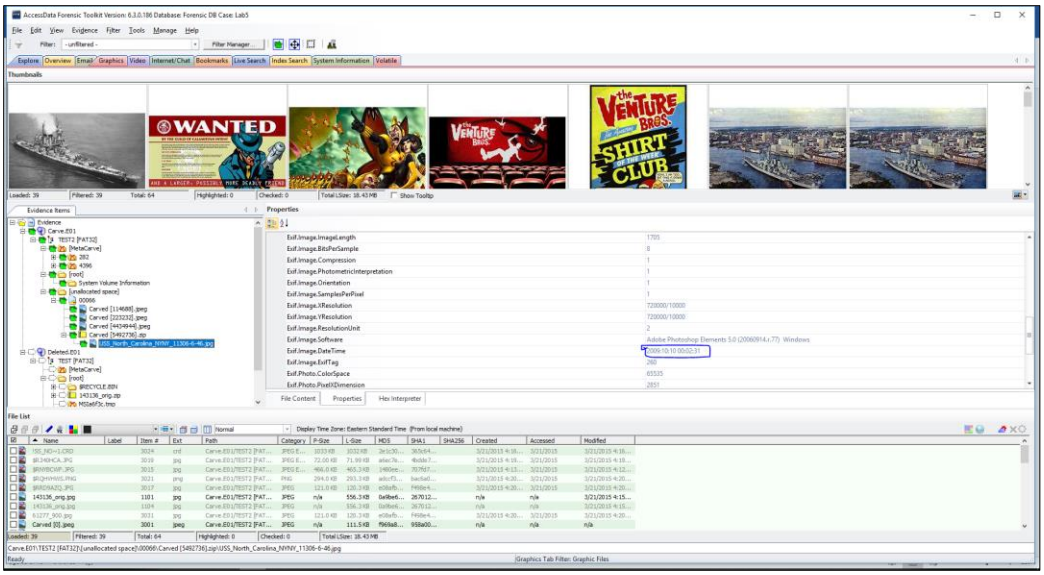




From Carve.E01 File:







Conclusion

After obtaining and verifying the forensic images, I performed operation using FTK Imager Tool to verify the integrity. In this lab I used HxD Editor which is used to open and edit the raw contents of disk drives, as well as display and edit the memory used by running processes.

The information I found was as follows:

1) Using HxD editor, after selecting 'TEST2(E:)' drive, at sector 29320, I found a movie named '**Venture Bros**'.
2) Performed carving on these images and tried to relate jpegs in 'Carve.E01' to that of 'USS North Carolina' in 'Deleted.E01'
3) Found out the oldest meta date amongst all these files which is **2006/07/20** for USS_North_Carolina.jpg

Thus I examined the provided images and found out information relating in both the images.