ITIS 5250

Ruchira Pokhriyal

Lab 5

11/15/2018

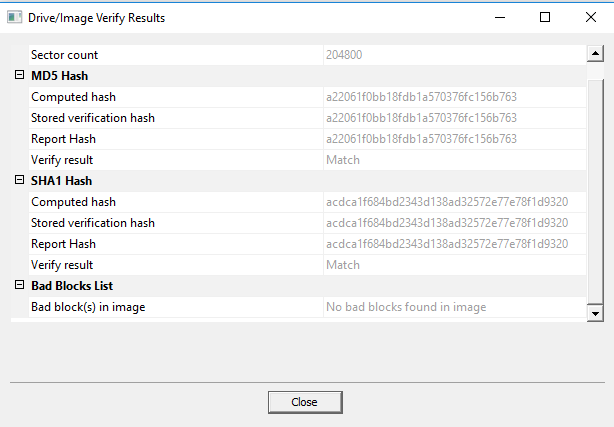
**Overview**

In this lab, I’m introduced to the basics of file recovery. For this purpose, I am given two images: ‘Carve.E01’ and ‘Deleted.E01’ to be verified using FTK Imager (Version 4.1.1.1). Then, I will be mounting one of the given images, and using HxD editor, I will be finding the name of a movie. Additionally, I will be correlating the jpeg files in both the provided images and will recover certain files using data carving (using FTK Version 6.3.0.186). Furthermore, I will be finding the oldest meta data date file.

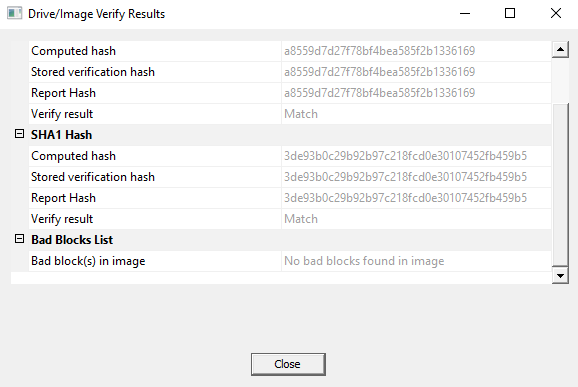
**Forensic Acquisition & Exam Preparation**

I accessed the images named **‘Carve.E01’** and **‘Deleted.E01’** along with their log files, from the server’s shared directory. I loaded these images using FTK Imager for hash verification and also used FTK for evidence processing.

**Hash Results for ‘Carve.E01’:**

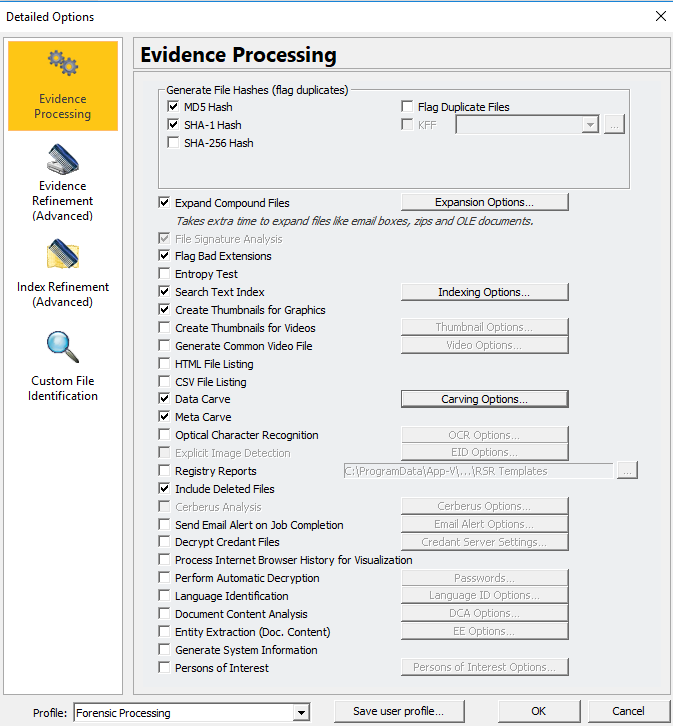
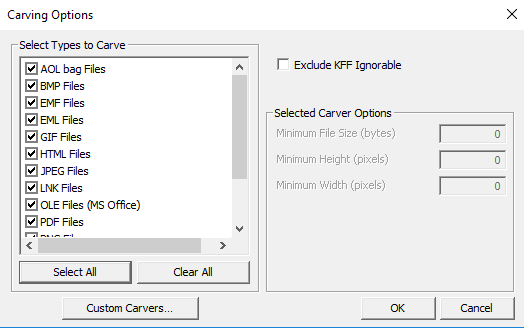


**Hash Results for ‘Deleted.E01’:**

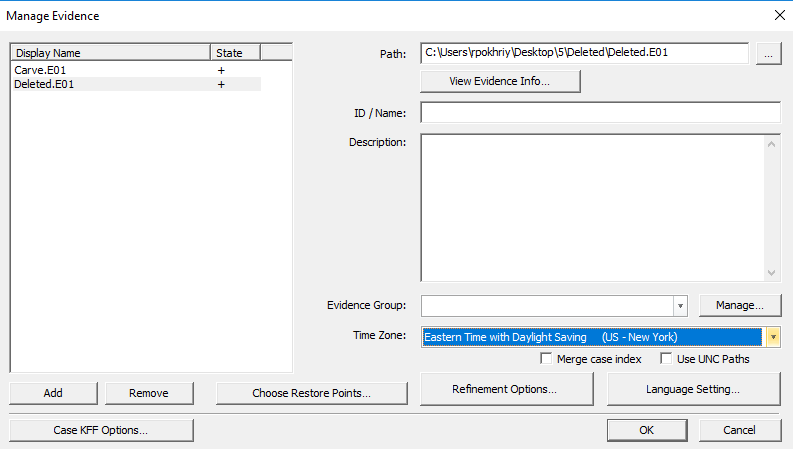


**Both, the computed and stored hash values match.**

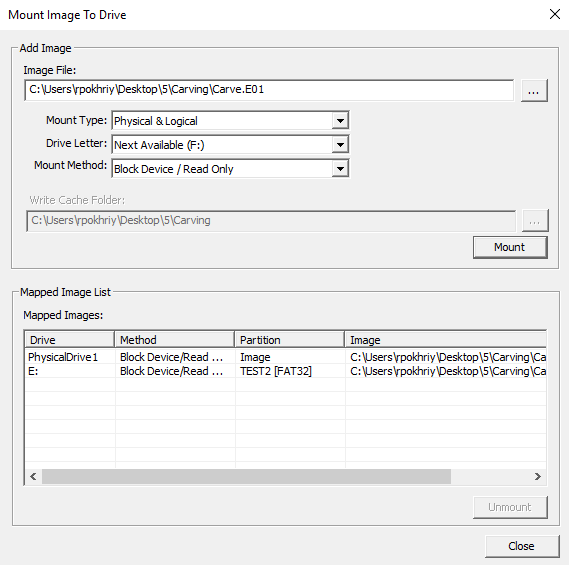
**Evidence Processing using FTK: Carving Options:**



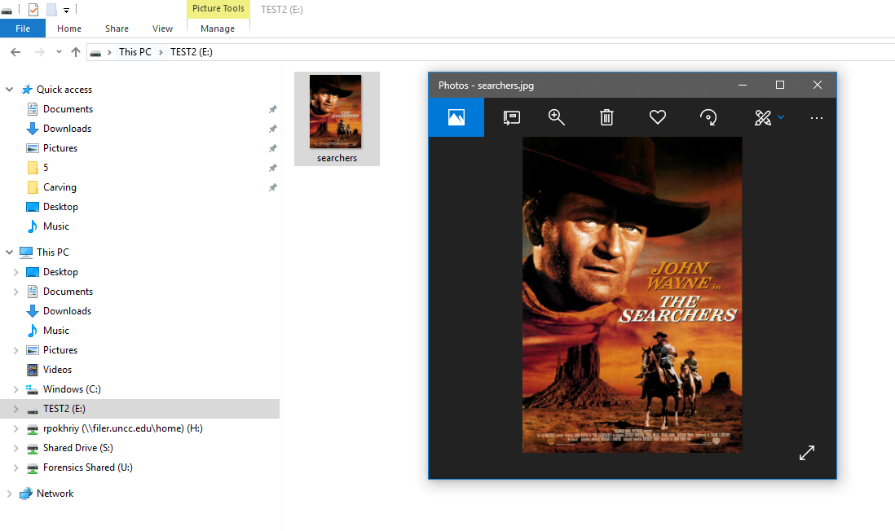
**Adding Images:**



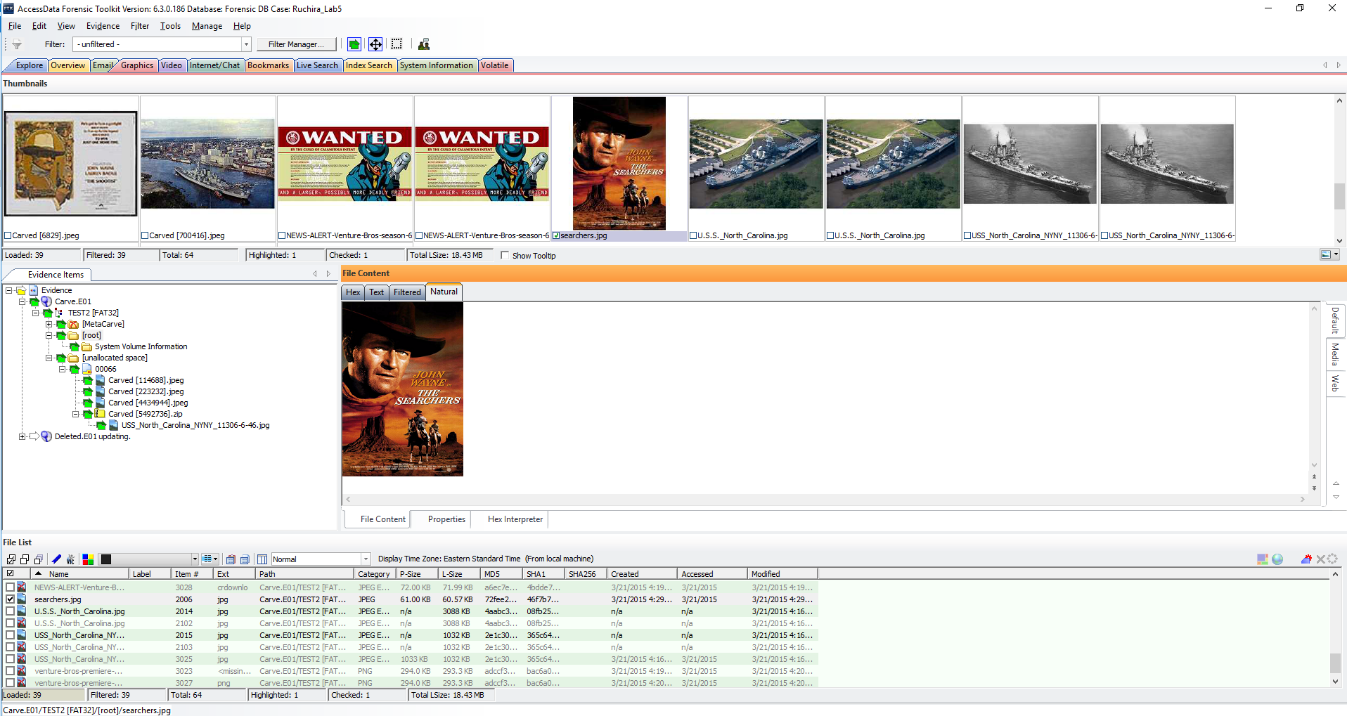
I then mounted the image **‘Carve.E01’** as a **physical** disk by loading it into ***FTK Imager*** and then right clicking on the image and finally selecting the option **‘Image Mounting’**.:



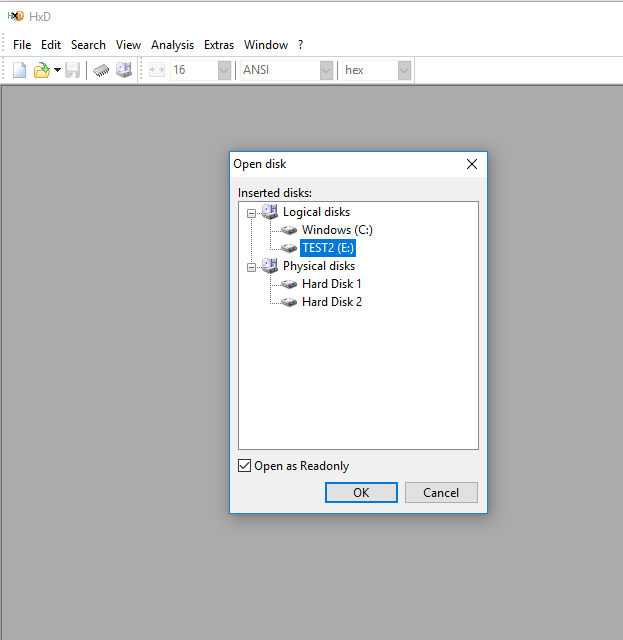
I was able to verify that the disk is mounted, by locating a new drive labeled **‘TEST2’**, in the file explorer. As shown below, this newly mounted drive contains a jpg file (a movie poster) named **“searchers”** for a movie called **‘The Searchers’** in it:



Upon further research, I also found the **“searchers.jpg”** under the path: *Carve.E01/TEST2 [FAT32]/[root]/searchers.jpg*:



Lastly, I opened the **HxD editor**, and through the **‘Extras’** tab, I selected the newly mounted physical disk: **‘TEST2(E:)’**

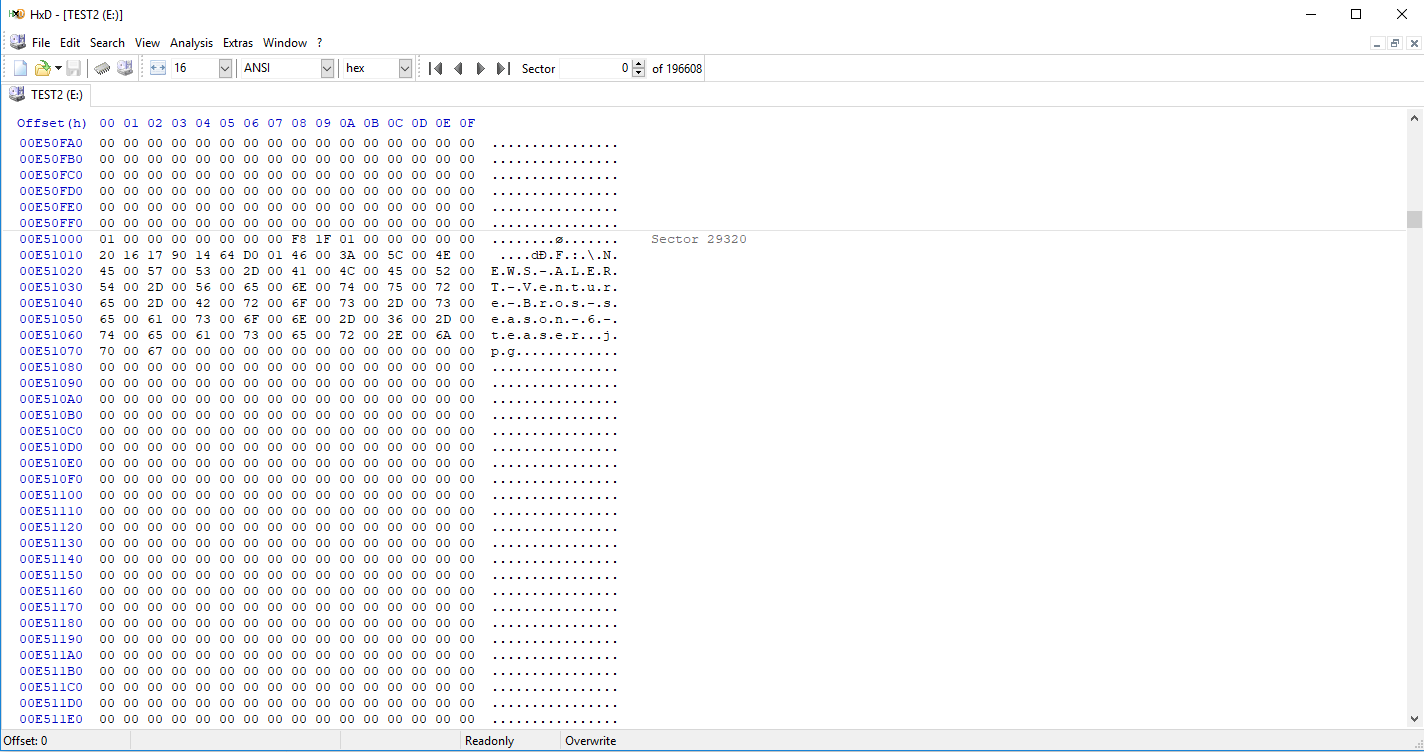


**Findings and Report (Forensic Analysis)**

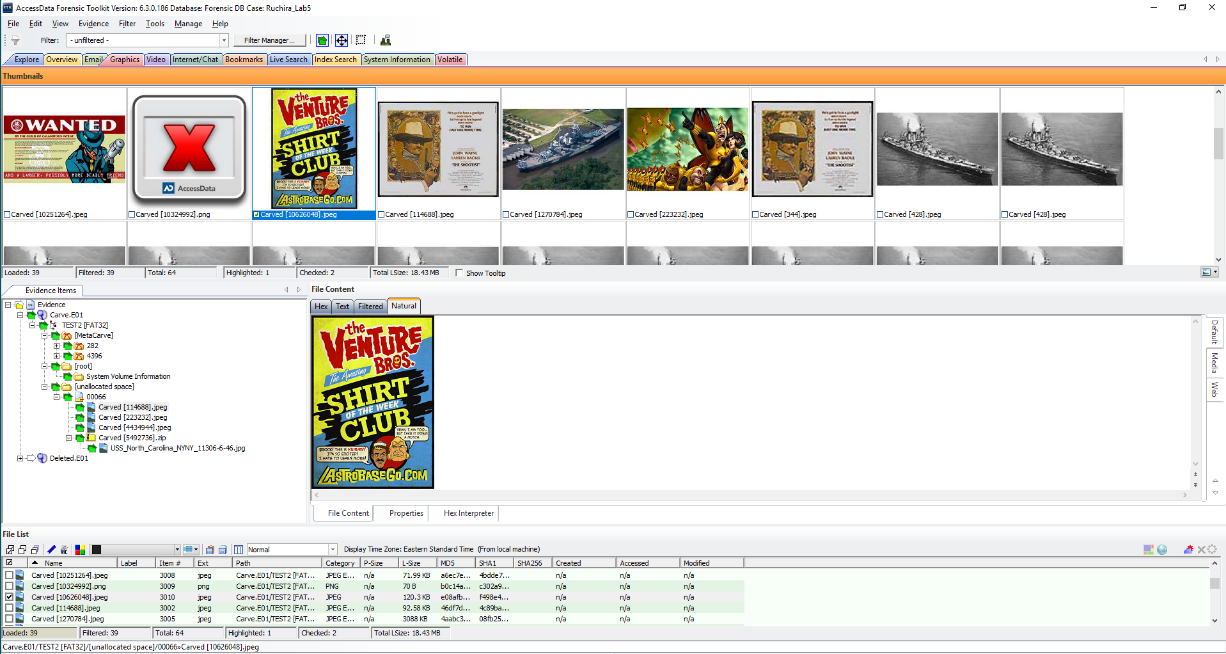
1. From what movie is this poster?

After selecting ‘TEST2(E:)’ drive in the HxD editor, I found a movie named ‘**Venture Bros**’

at **sector 29320**:



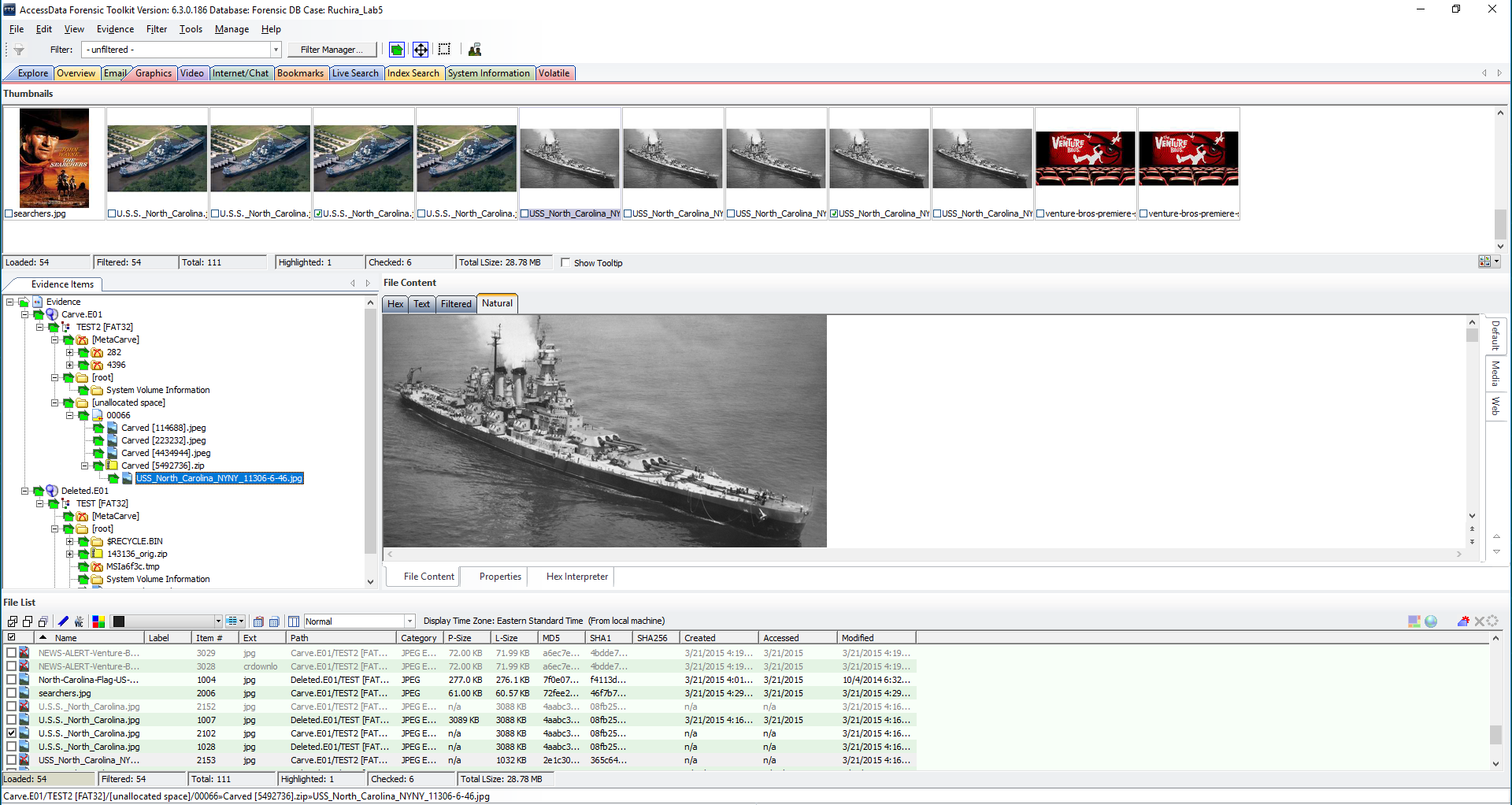
As shown below, the **‘Venture Bros’** movie poster was found under the path: **Carve.E01/Test2 [FAT32]/[unallocated space]/00066>>Carved [10626048].jpeg:**



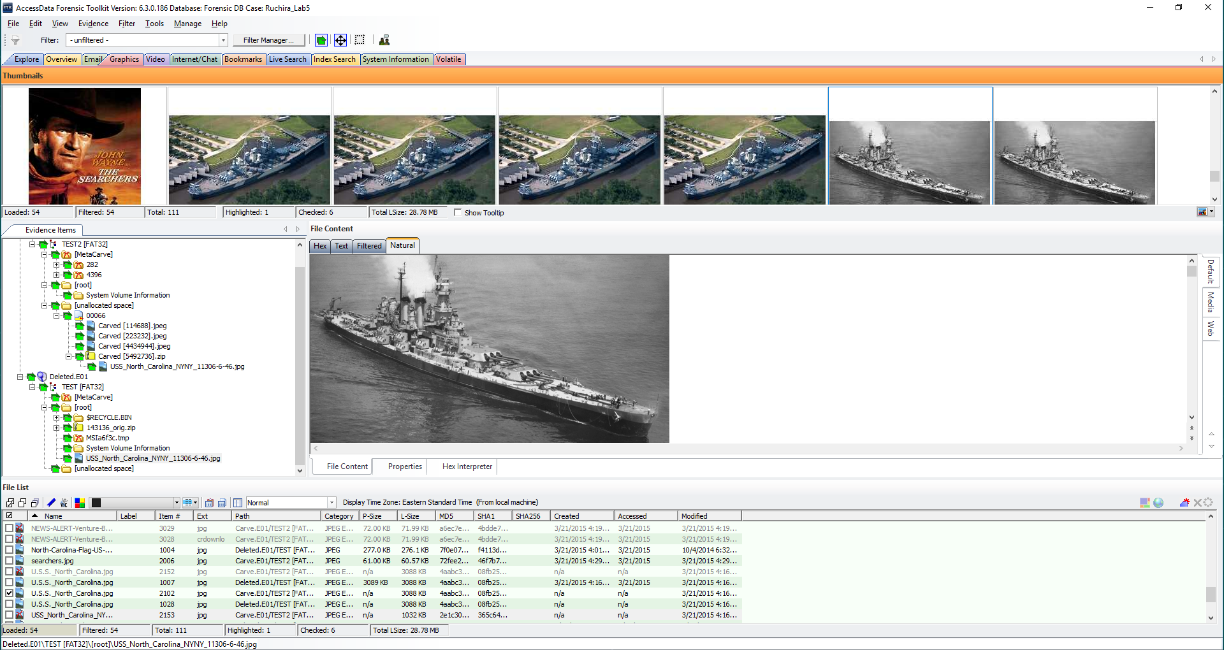
1. Attempt to match jpegs recovered in Carved.E01 that relate to the USS North Carolina from Deleted.E01.

As seen in the below screenshots, the file: ***USS\_North\_Carolina\_NNYY\_11306-6-46.jpg*** recovered in ‘Carve.E01’ matches with the one from ‘Deleted.E01’.

***USS\_North\_Carolina\_NNYY\_11306-6-46.jpg from the ‘Carve.E01’:***

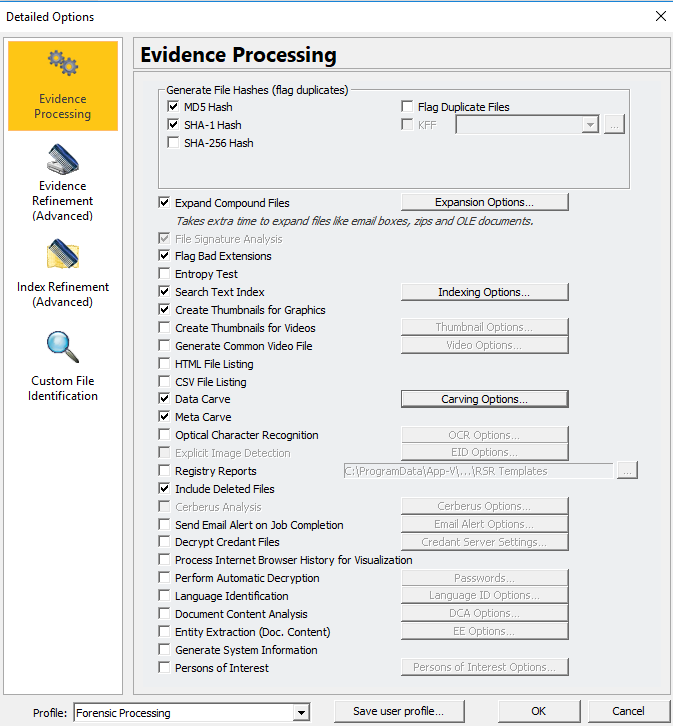


***USS\_North\_Carolina\_NNYY\_11306-6-46.jpg from the ‘Deleted.E01’:***

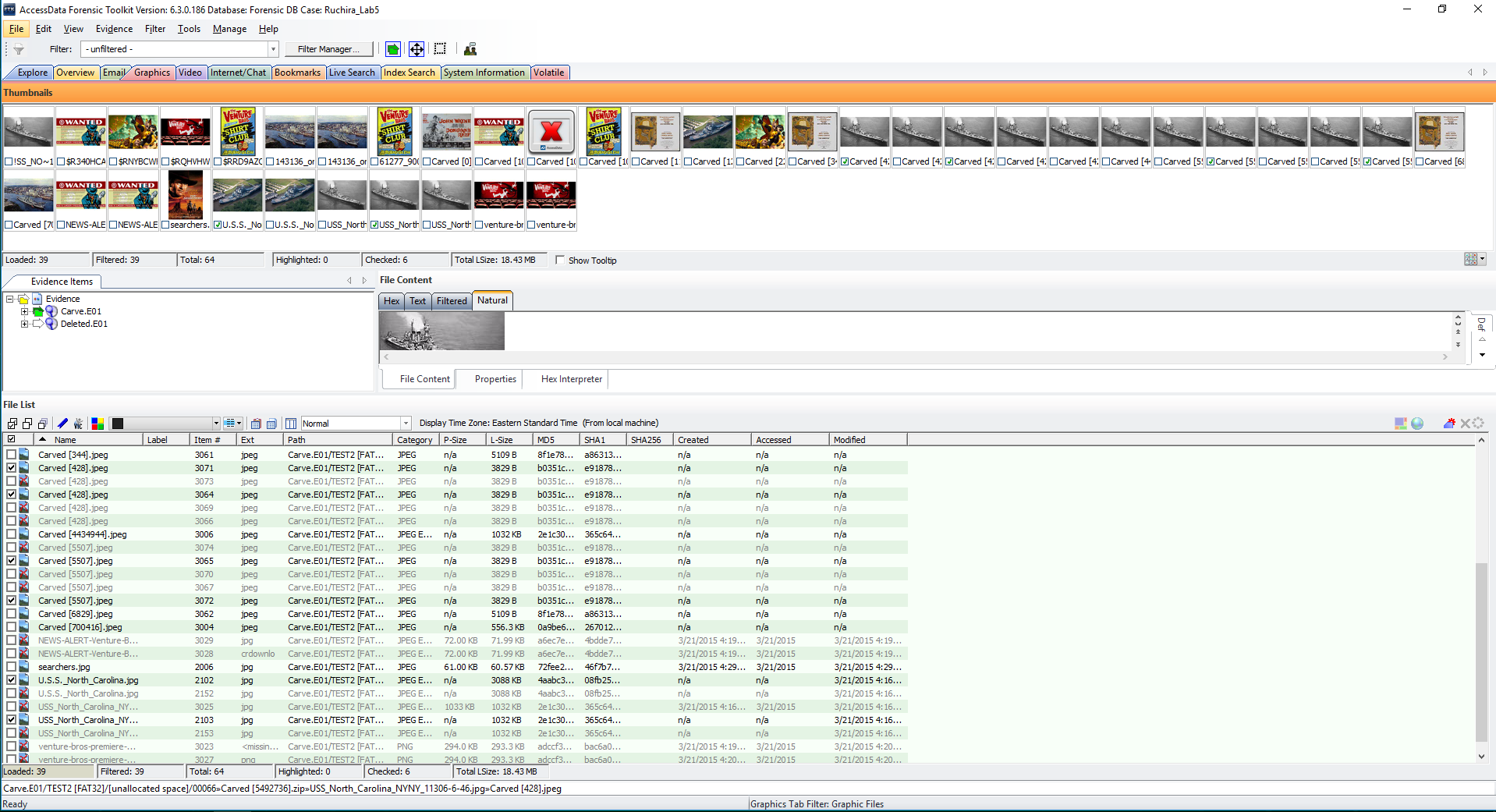


1. How did you find files in Deleted.E01 that are also found in ‘Carve.E01’?

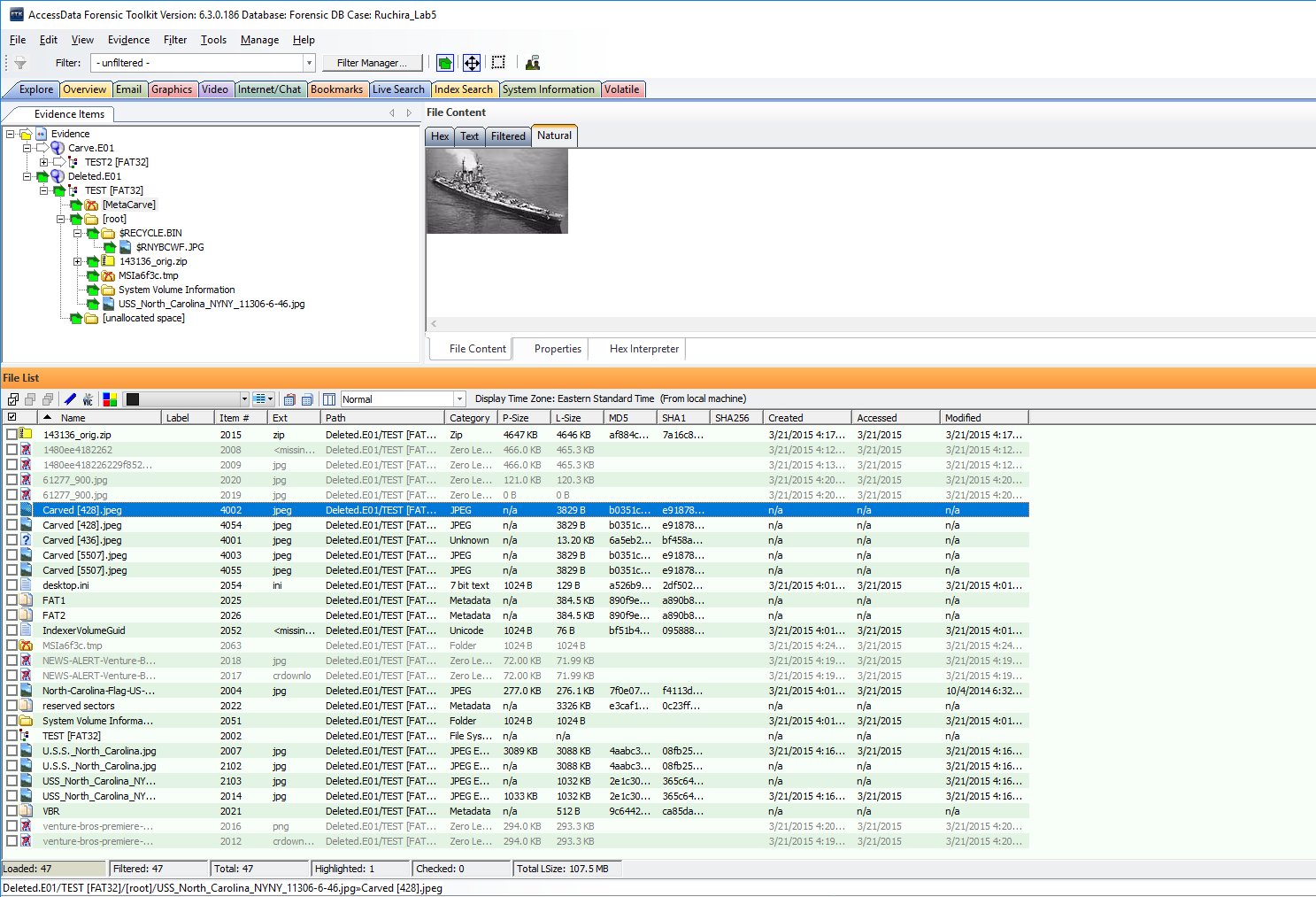
Performing the **Data Carving and Meta Carving** operations using FTK, enabled me to recover the files in ‘Deleted.E01’ which are also found in ‘Carve.E01’. I Opened the Deleted and Carved image files in FTK and under Evidence Items, explored TEST[FAT32] in both image files and finally, compared all the images in both of them.

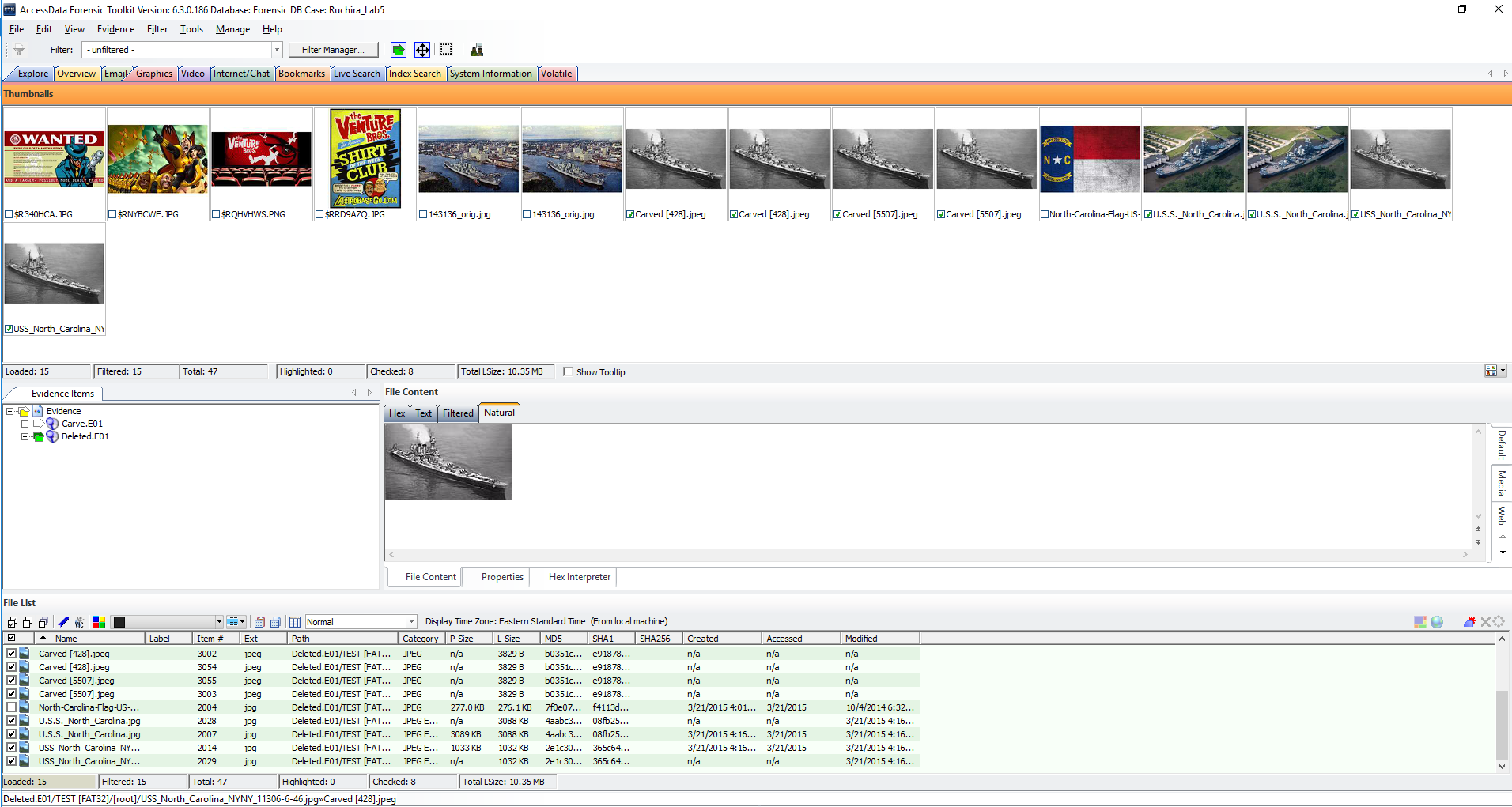


**Files found in ‘Carve.E01’:**



**Files found in ‘Deleted.E01’ which are also found in ‘Carve.E01’:**



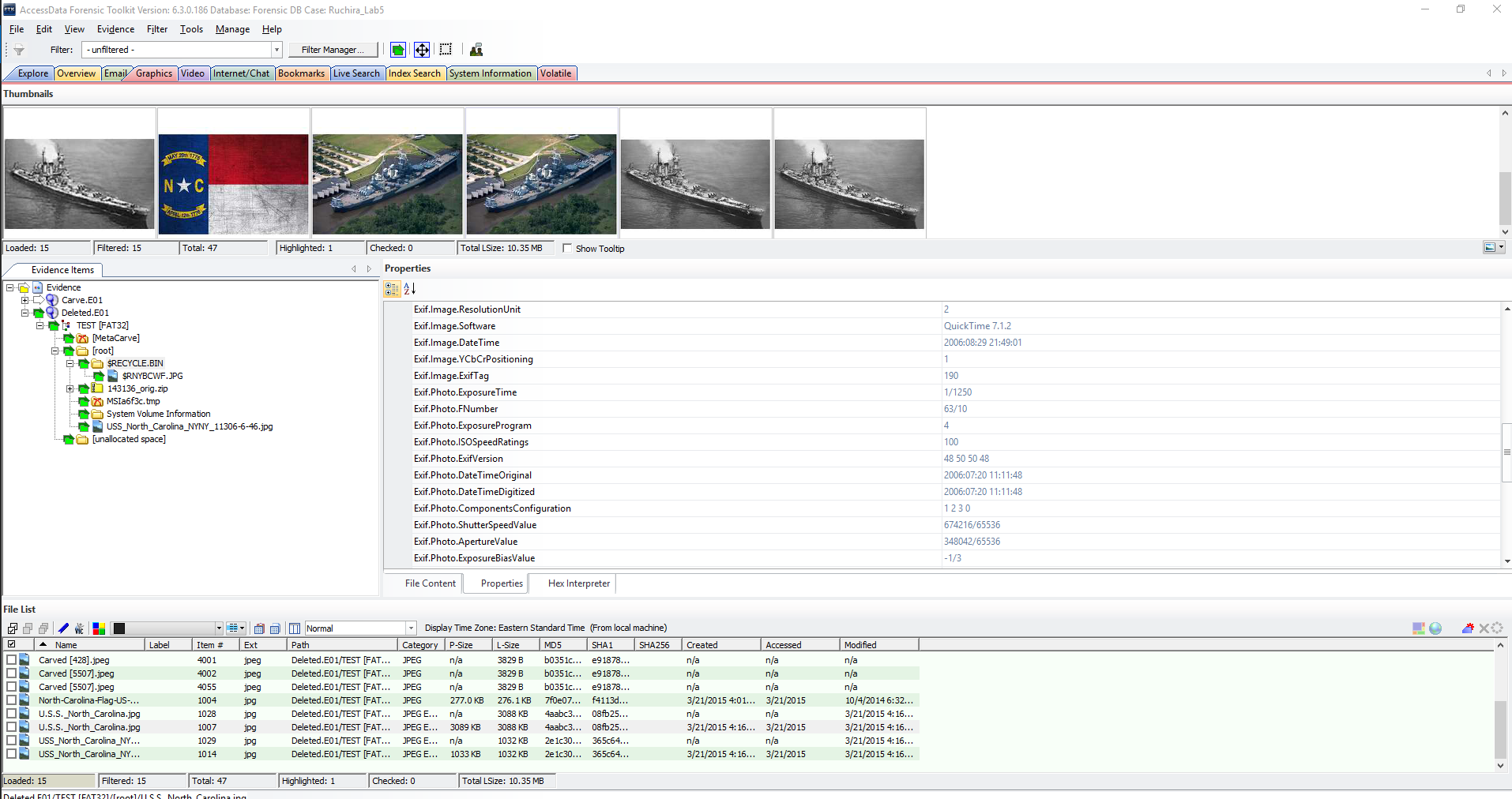


1. What is the oldest meta date you were able to find associated with any of these files?

The oldest meta data date associated with all these files in both the images is **2006/07/20** of **USS\_North\_Carolina.jpg,** as shown below:

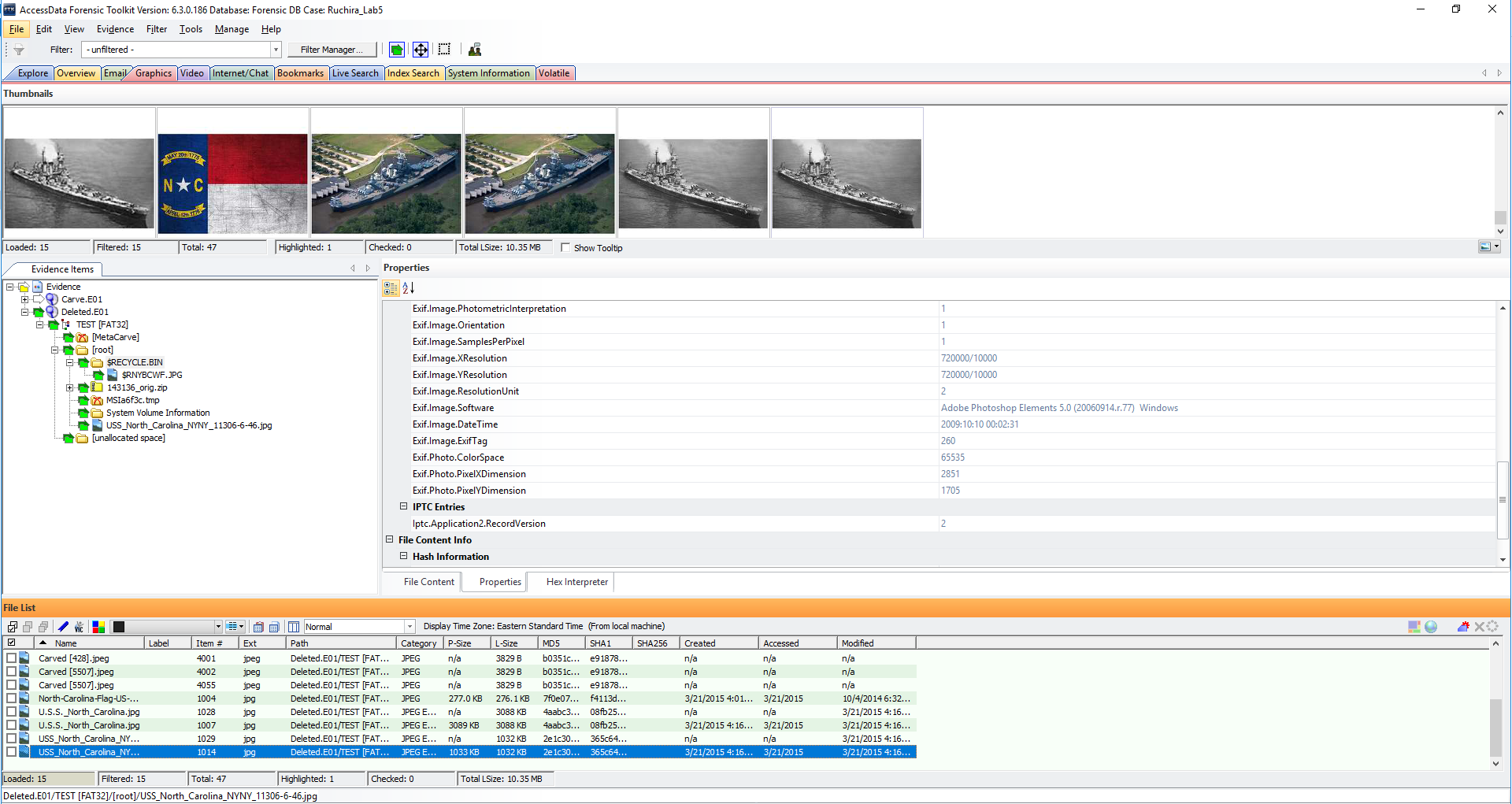
**From Deleted Image File:**

***USS\_North\_Carolina.jpg (2006/07/20)***

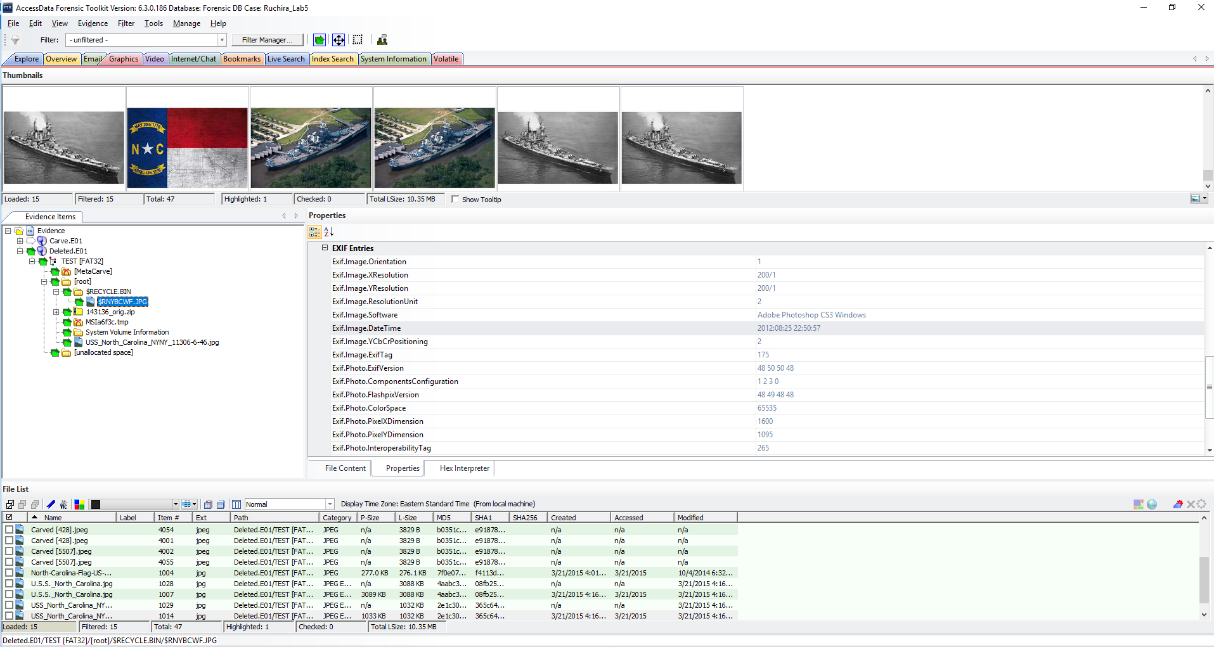


**Other Meta Data Date Details:**

***USS\_North\_Carolina\_NYNY11306-6-46.jpg (2009/10/10)***

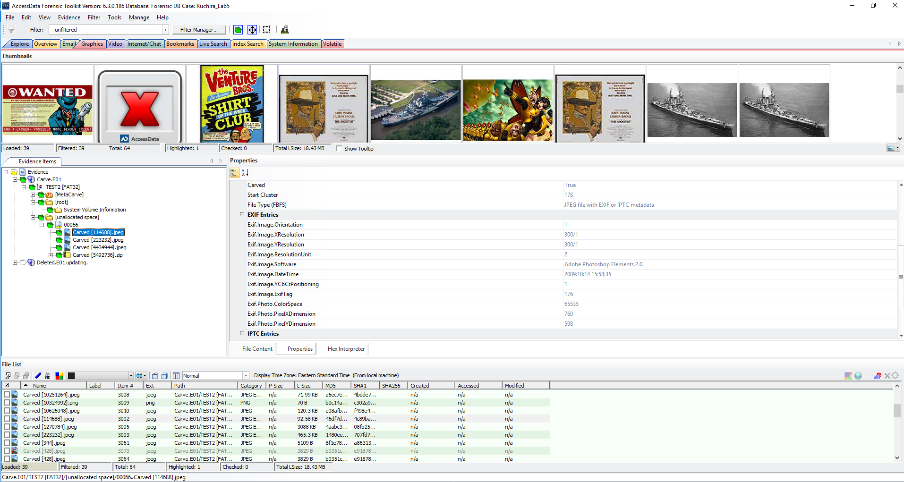


***$RNYBCWF.JPG (2012/08/25)***

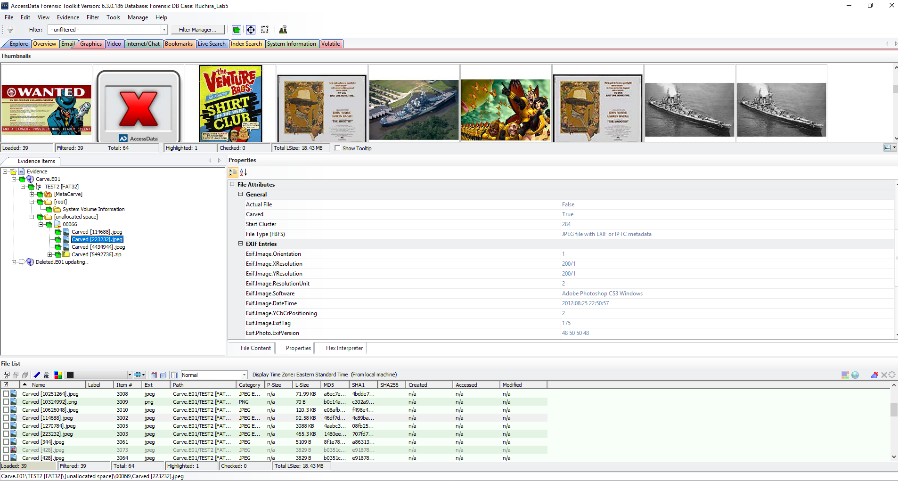


**From carved image file:**

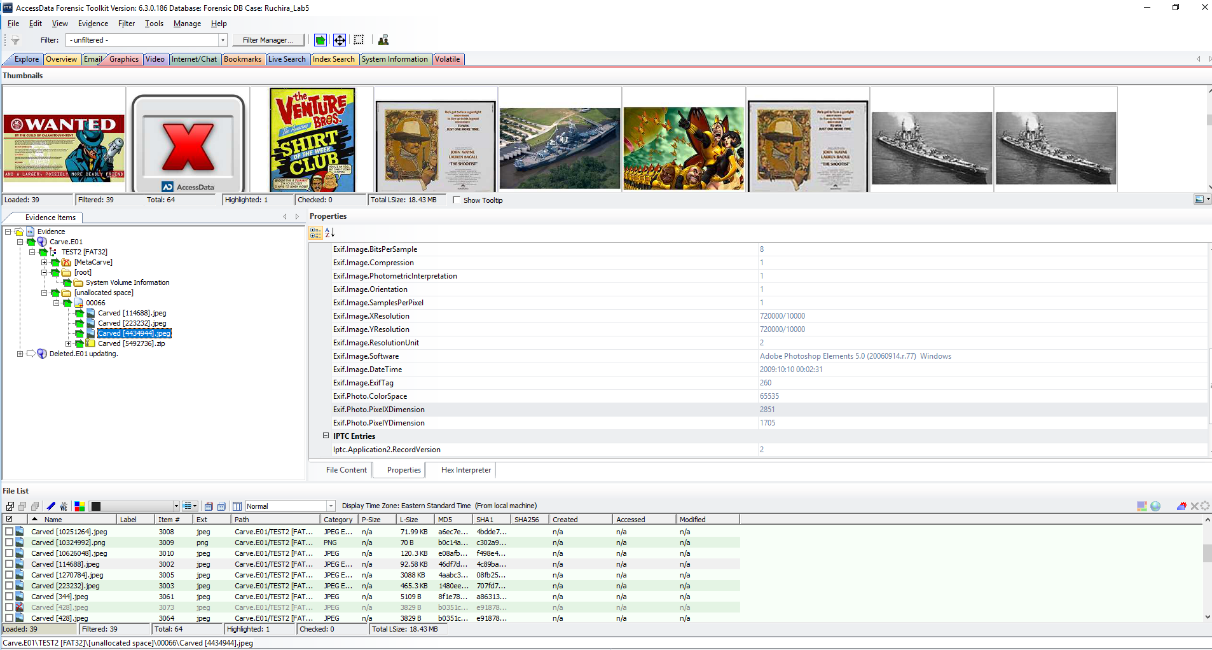
***Carved [114688].jpeg (2009/10/14)***



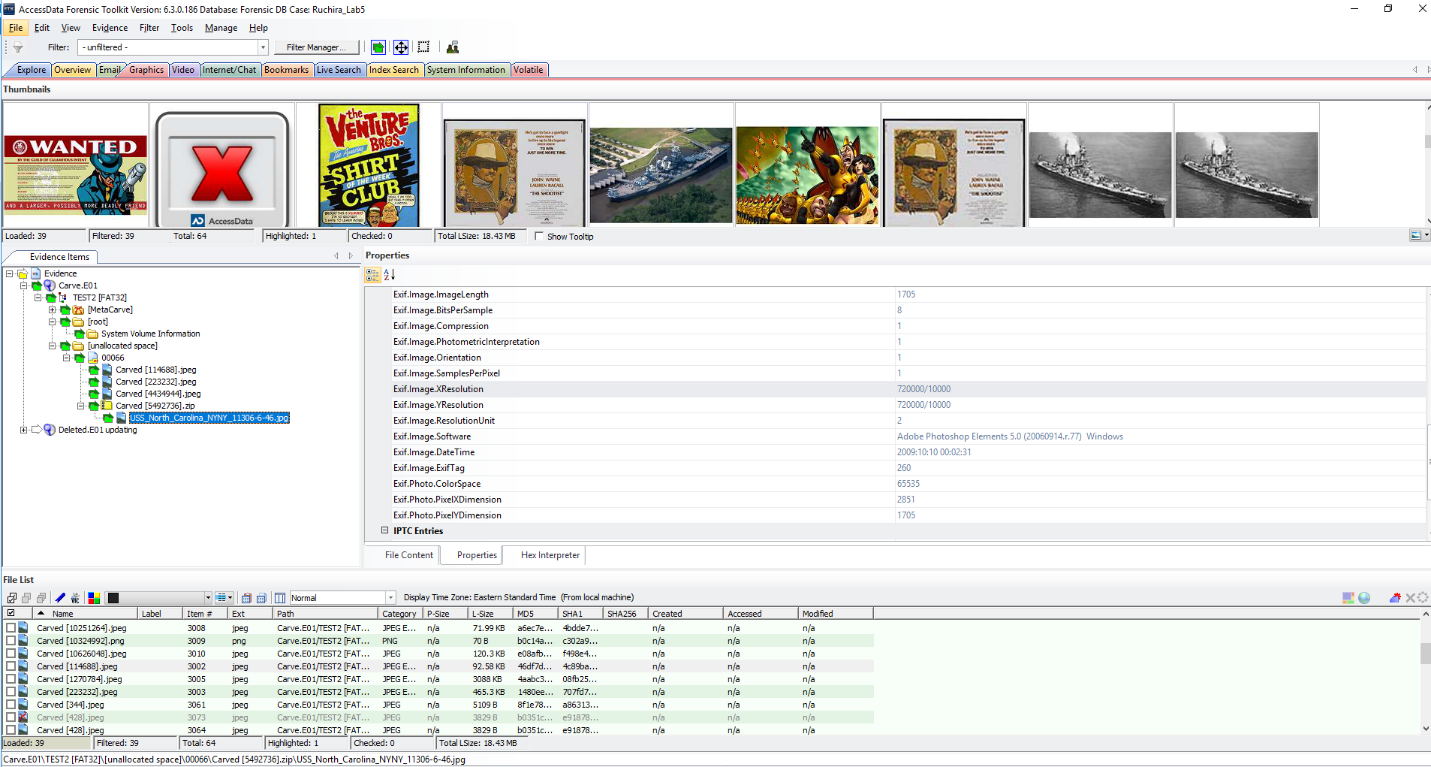
***Carved [223232].jpeg (2012/08/25)***



***Carved [4434944].jpeg (2009/10/10)***



***USS\_North\_Carolina\_NYNY11306-6-46.jpg (2009/10/10)***



**Conclusion**

I performed **Image Mounting** where I found a movie named **“The searchers”** which is different from the one found in HxD, **“Venture Bros”**. Furthermore, I performed Meta and Data Carving on the given images and tried to relate the jpegs in ‘Carve.E01’ to that of ‘USS North Carolina’ in ‘Deleted.E01’. Finally, I found the oldest meta data date associated with these files.