ITIS 4250 / 5250

Lab # 4

10/25/2019

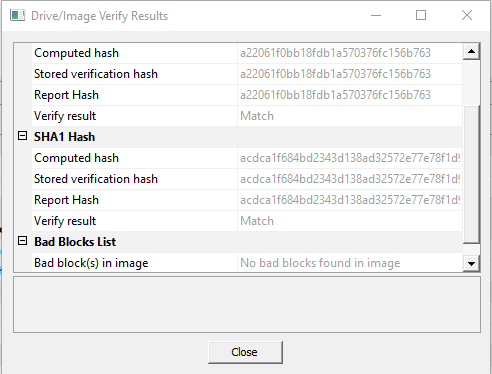
**Overview:**

This task involves the investigation, validation and analyzation 2 E01 files ‘Carve.E01 and ‘Deleted.E01 for this task. There was proper legal approval for this investigation.

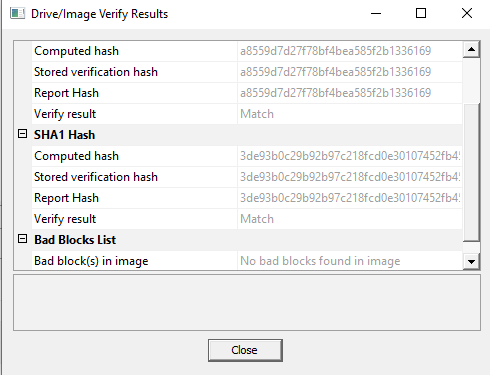
**Forensic Acquisition & Exam Preparation**

The first step was transferring the files ‘Carve.E01’, and ‘Deleted.E01’ from Canvas into a fresh folder on my work machine. My machine is a Lenovo Yoga 13 with 8gb of ddr4 ram along with an i5-8500. After transferring ‘Carve.E01’, and ‘Deleted.E01 on my machine I verified the hash to make sure the file hasn’t been tampered with

Carve.E01



Deleted.E01



**Findings and Report (Forensic Analysis)**

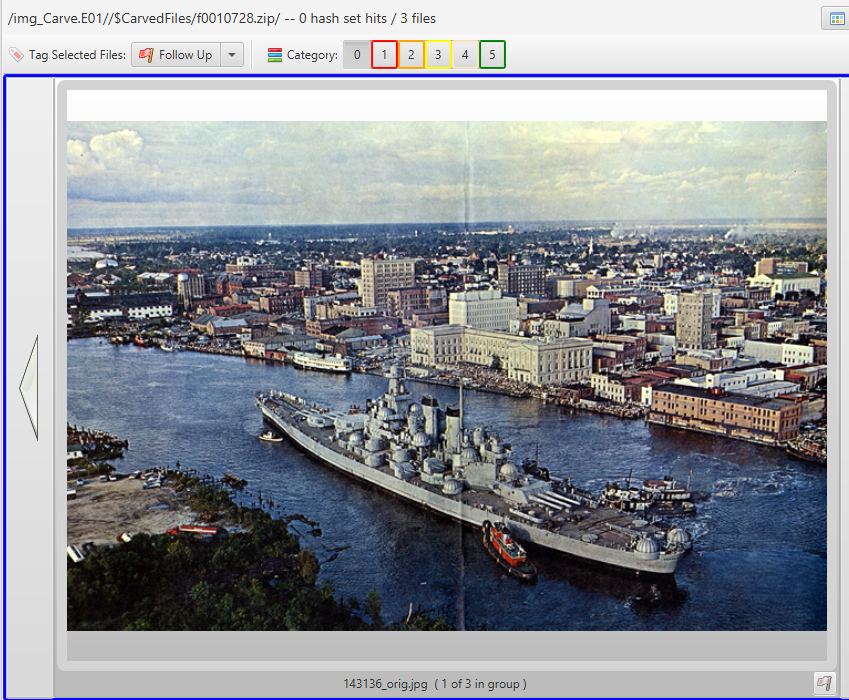
**Attempt to match jpegs recovered in Carved.e01 that relate to the USS North Carolina from Deleted.e01**

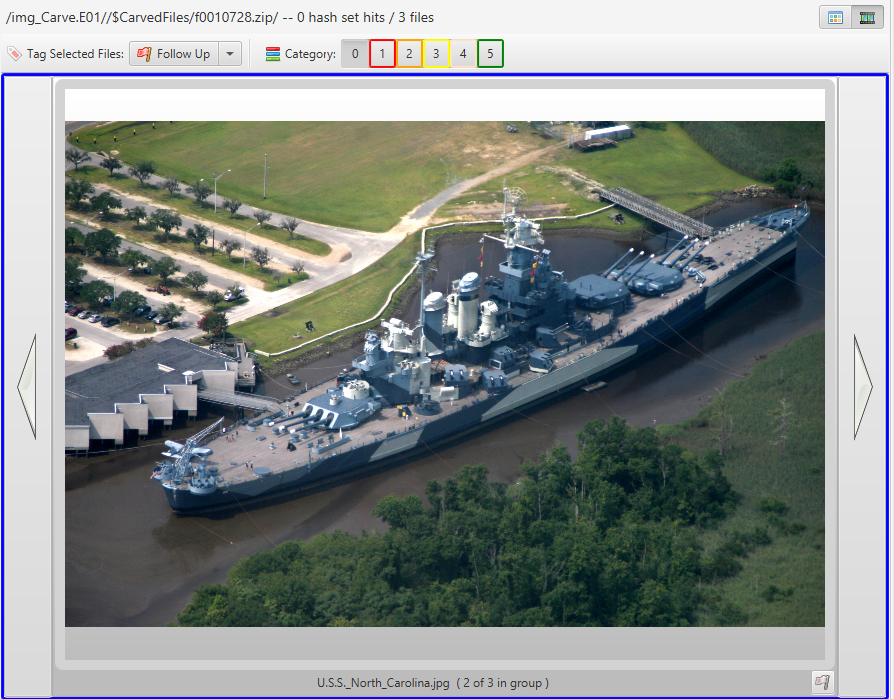
I found multiple files in ‘Carve.E01’ that are related to the USS North Carolina from Deleted.E01. This was done by loading the image into autopsy and opening the image viewer. After going into the Image Viewer I was able to view the carved files that Autopsy was able to fin and within that I was able to find 3 pictures of ships that are closely related to the USS North Carolina from Deleted.E01.

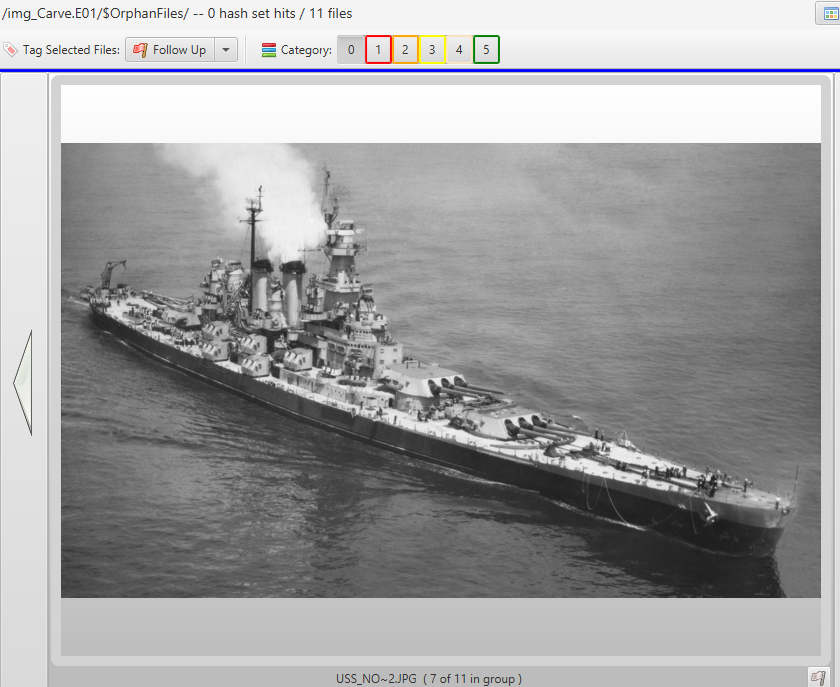
USS North Carolina from Deleted.e01



Ships found on Carve.E01

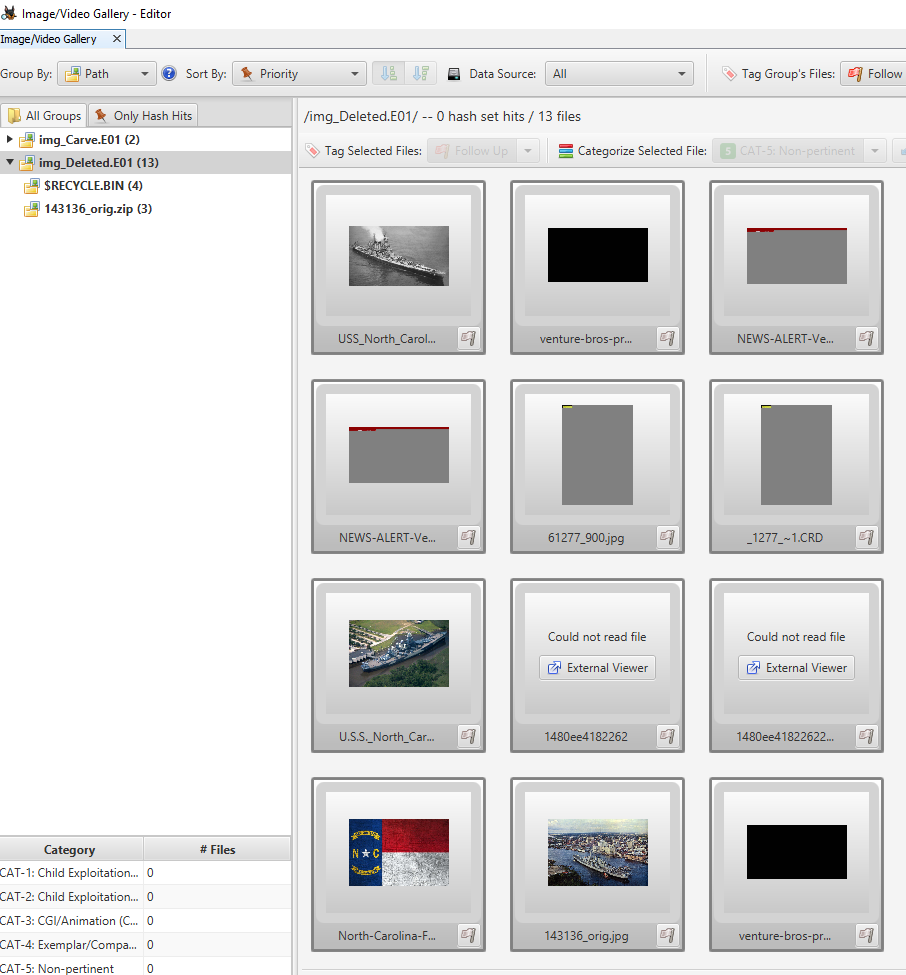






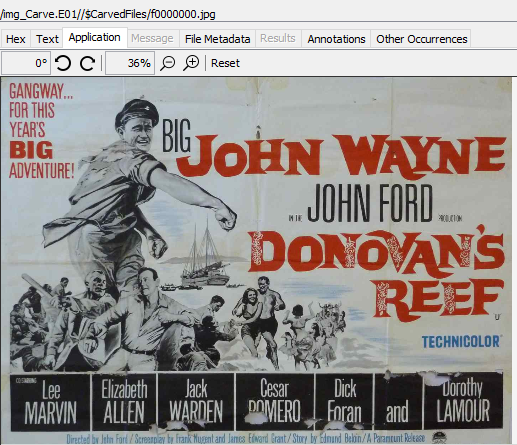
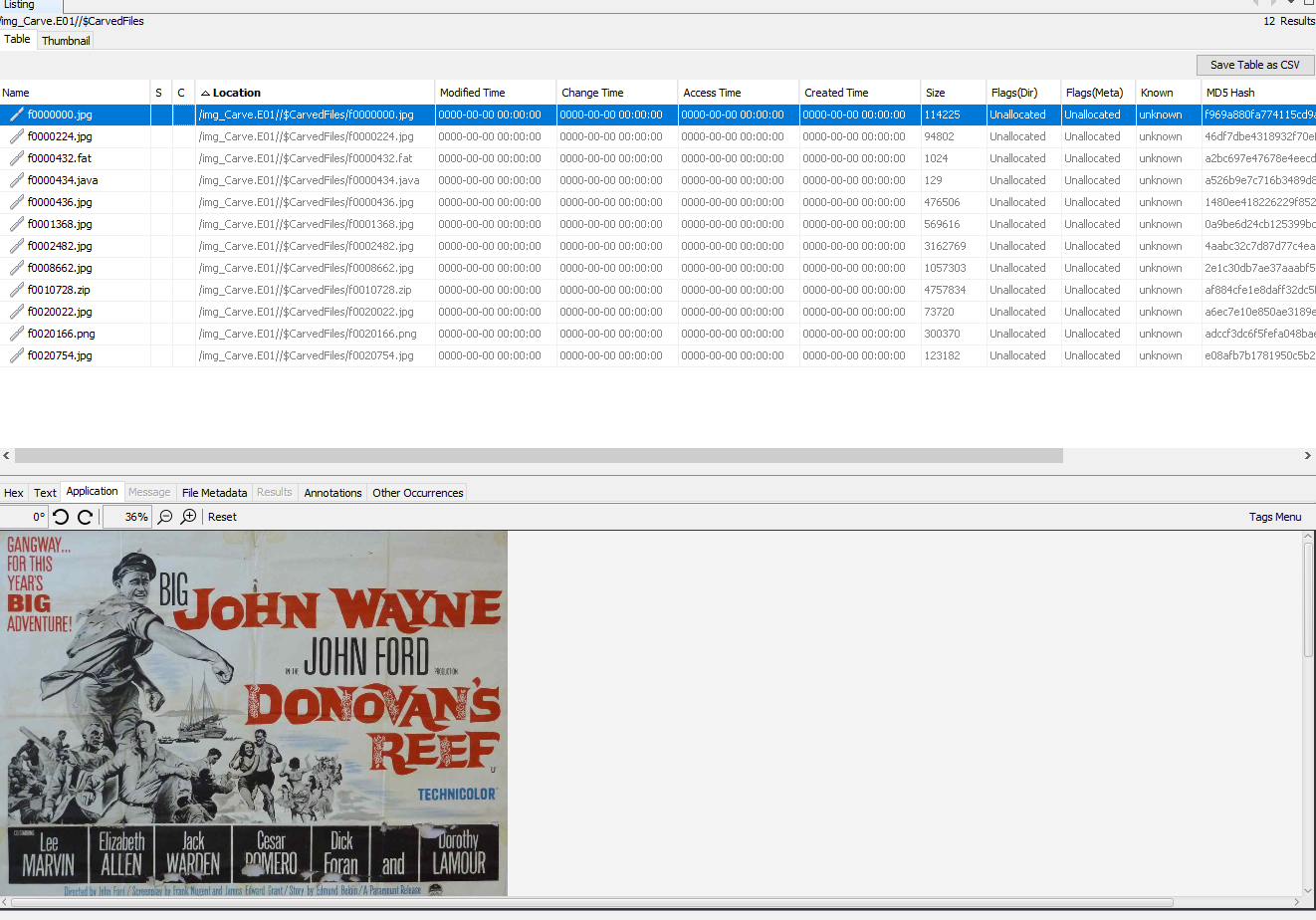
**How did you find files in Deleted that are also found in Carved?**

I was able to find files in Deleted that are also found in Carved by opening the image viewer and then investigating the images that autopsy was able to manually carve.



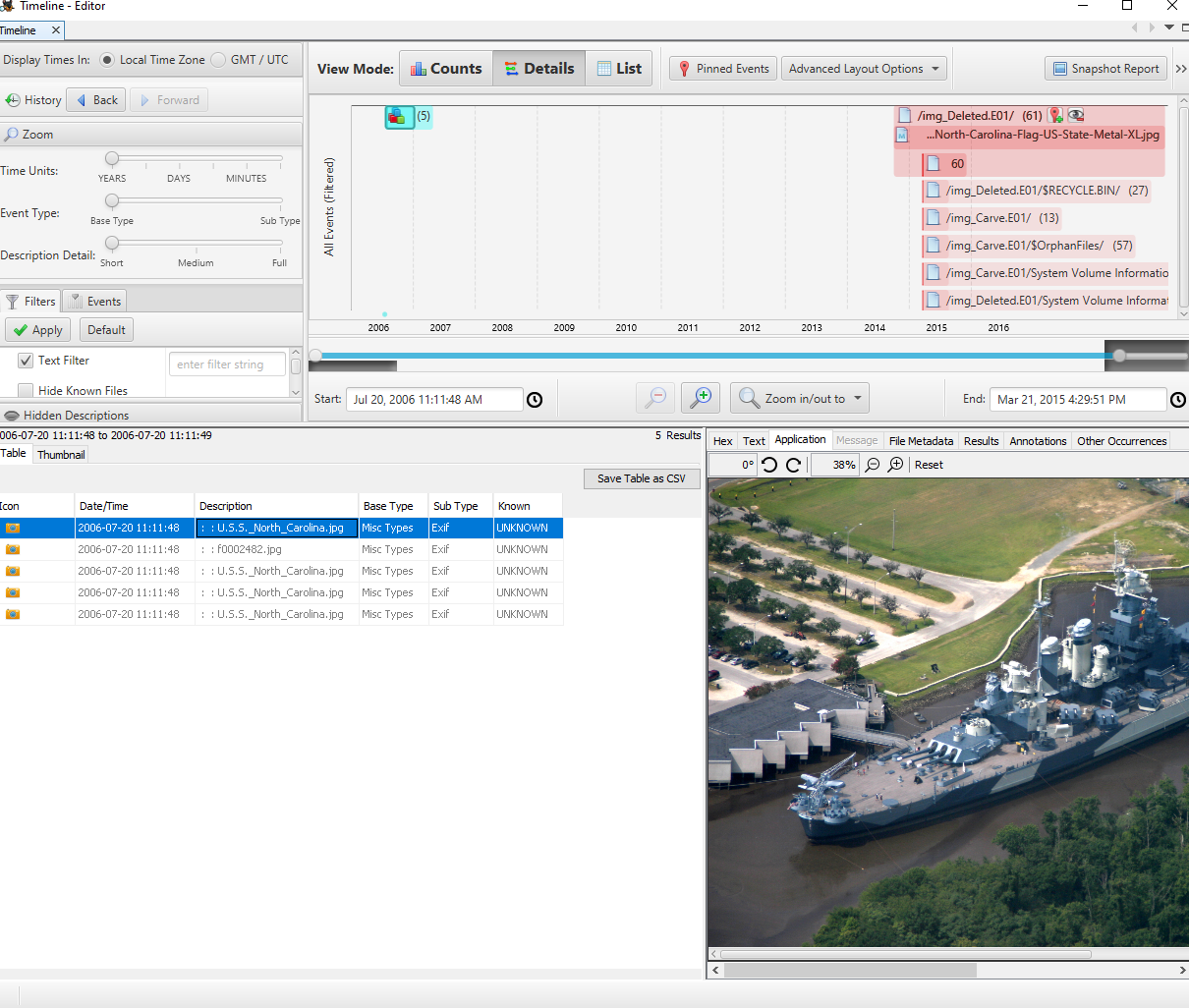
**Find a movie poster that is different from the ones that were still available in the file system From what movie is this Poster.**

I found other poster within the data source drop down in autopsy. This poster is Donovan’s Reef which is different than The Searchers which was originally found.

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

The Oldest meta data date I was able to find was on the images of the USS North Carolina which is from 7/20/2006. I found this by going into the timeline section of autopsy and viewing the oldest data on the drive.



**Conclusion:**

After investigating both images I was able to find jpg images that were not apparent when the image was merely mounted. Through this I was able to find different movie posters than The Searchers. I was also able to find other images including ships as well as figure out what the oldest meta-data is on the drive.