ITIS 5250

Sahil Bhirud – 801138029

Lab 4

**Overview:**

In this lab, I will be examining two forensic images viz. **Carve.E01** and **Deleted.E01**. I will be performing various operations and inspections on these image files using **FTK Imager Tool, HxD Editor and Autopsy**. I have been asked to find the presence of jpeg files related to USS North Carolina in both of the image files. I also have to the find the jpeg file with oldest file metadata.

**Forensic Acquisition and Exam Preparation:**

I downloaded the image files from canvas and verified their hash values. The software I used to verify the hash values is **FTK Imager**. For extracting and analysis of the image files, I used **HxD Editor** and **Autopsy.**

**Carve.E01:**

A screenshot of a social media post

Description automatically generated

**Deleted.E01:**

**A screenshot of a cell phone

Description automatically generated**

**Findings and Report (Forensic Analysis):**

Using FTK Imager, I mounted the Carve.E01 on the disk as a physical disk and found the Logical Drive **TEST2** mounted as **Drive F:**. I opened it and found a jpeg file of a movie poster named **searches**.

A screenshot of a social media post

Description automatically generated

Using HxD Editor, I found that it was a different movie from the one found in the drive. The movie poster found in HxD Editor was from **Venture Bros Season 6 Teaser**.

A screenshot of a social media post

Description automatically generated

Next, I used Autopsy to find jpegs related to USS North Carolina in both of the images.

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

The jpeg files I found in Carve.E01:

1. f0001368.jpg
2. f0002482.jpg
3. f0008662.jpg

match to the following jpeg files recovered in Deleted.E01:

1. 143136\_orig.jpg
2. U.S.S.\_North\_Carolina.jpg
3. USS\_North\_Carolina\_NYNY\_11306-6-46.jpg

To ensure that I was right, I also matched these files by their hash values.

1. f0001368.jpg and 143136\_orig.jpg have the hash value **0a9be6d24cb125399bd0ceb9ad09088f**.
2. f0002482.jpg and U.S.S.\_North\_Carolina.jpg have the hash value **4aabc32c7d87d77c4ea16fdc24083d77**.
3. f0008662.jpg and USS\_North\_Carolina\_NYNY\_11306-6-46.jpg have the hash value **2e1c30db7ae37aaabf5180465656062f**.

A screenshot of a social media post

Description automatically generated

A screenshot of a machine

Description automatically generated

* **From what movie is this poster?**

I found multiple movie posters in the **/img\_Carve.E01//$CarvedFiles/** directory. They are listed below:

1. Donovan’s Reef (f0000000.jpg)

A sign on a newspaper

Description automatically generated

1. The Shootist (f0000224.jpg)

A close up of text on a white background

Description automatically generated

1. The Venture Bros (f0020166.png)

A picture containing indoor, red, sitting, table

Description automatically generated

1. The Venture Bros – Shirt of the Week Club (f0020754.jpg)

A picture containing newspaper, food

Description automatically generated

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

After selecting Deleted.E01, I clicked on the Images/Video button on Autopsy and found the files in Recycle Bin. I also check the hash values for them and found them to be matching to the corresponding jpeg file in Carve.E01.

A screenshot of a video game

Description automatically generated

* **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 and f0002482.jpg which are basically the same image. The date is 2006/07/20.

A screenshot of a cell phone

Description automatically generated

**Conclusion:**

After carefully examining the image files, I have come to the following conclusions:

1. There are 3 jpeg files in **Deleted.E01** which matched to the ones in **Carve.E01**.
2. From the Carved folder in **Carve.E01**, I found 4 movie posters which were different than the one in the file system and out of those 2 of them were present in **Deleted.E01**.
3. The oldest metadata date associated with any of the files is 2006/07/20 which is of the file U.S.S.\_North\_Carolina.jpg and f0002482.jpg.