James W.

Access Methods and Data Hiding

Multimedia Data Hiding Lab

Table of Contents

Introduction

Investigating media on a PC, laptop or any other storage device with digital media is how criminals are arrested, prosecuted, and serving a prison sentence depending on the crime committed by the offender. Since 2011 there have been military personnel caught having inappropriate discussions with minors who were police officers, finding images of children being exploited on hard drives containing several terabytes of images and video. The substantial evidence is discovered on the confiscated media and other devices which is a growing concern worldwide with law enforcement stateside and in Europe.

The impact of computer forensics today is one of the crucial parts of an investigation due to the evidence ensuring a strong case which cannot be disputed. Retrieving images from a PC doesn't require several techniques. Extracting information from audio files such as mp3 or WAV files is going to be demonstrated in this experiment. Recovering data from a hidden to retrieve more information from the retrieved file will be displayed.

Tools Utilized

StegoAnalyst

StegoAnalyst is a useful tool when looking for the slightest anomaly in an image or an audio file. Investigators are provided many filters within the program to use to examine files in question while giving the end-user results that cannot be denied in a court of law. StegoAnalyst is ideal for individuals with advanced knowledge in forensic investigations.

Winhex

Winhex is a data carving tool which can recover data from an image or audio file that is suspected to have suspicious contents in the media through reviewing the binary code to seek out discover anything that isn't common in file formats.

TrueCrypt

Criminals have begun encrypting media to prevent law enforcement from conducting a forensic information. Information stored inside of a TrueCrypt container within a video file as laid out in this experiment, this denies the individuals involved in recovering the content quite difficult. TrueCrypt will be used to create a container to store information in without anyone knowing hidden data exists within the media.

Python script pyMP3.py

During the experiment, the python script pymp3.py will be used through Windows command prompt to retrieve if any, data within the music files. Music can carry a substantial amount of data within the files as long as the total value of the files does not exceed the overall size of the mp3 file.

File investigation

The examiner was provided with five mp3 files to investigate running the script via Windows command prompt. The examiner accomplished the same method with each of the mp3 files provided. The purpose of this experiment is to determine if each of the music files, in fact, contain any information. The mp3 file *EO.mp3* is the original mp3 file.

It was confirmed that data was extracted from each of the mp3 audio files to the images folder shown in Figure 1.

pymp3.py eo.mp3 > eoresult.txt

Figure 1 Original mp3 Data Extraction (EO)

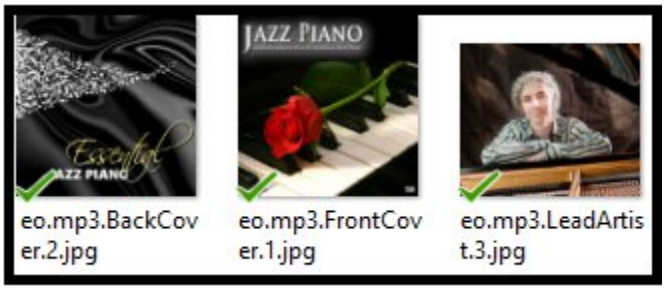


Figure 2 Original mp3 Images (EO)

Sending data out to a .txt file is more straightforward to review compared to viewing the output in the command prompt window.

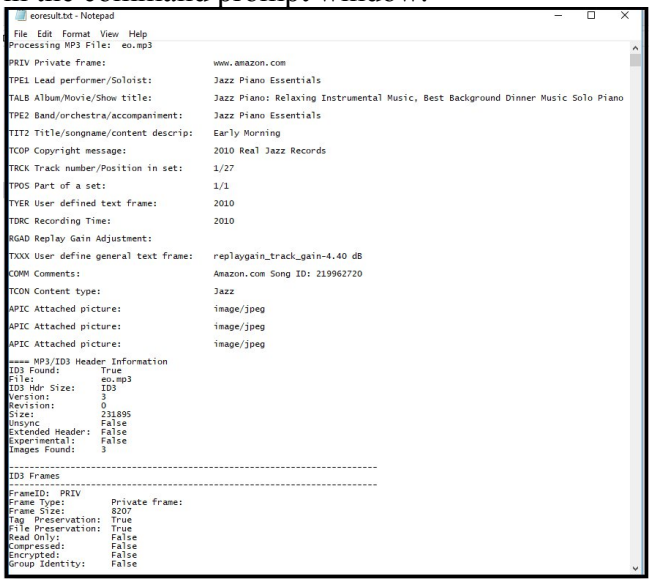


Figure 3 Original mp3 Output (EO)

pymp3.py ee.mp3 > eeresult.txt

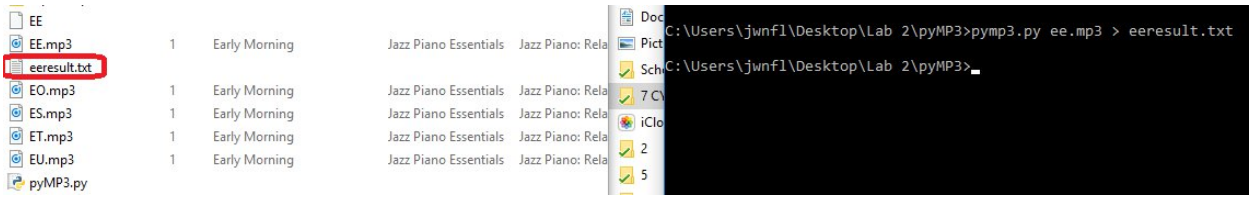


Figure 4 EE.mp3 Data Extraction

Figure 5 EE.mp3 Images

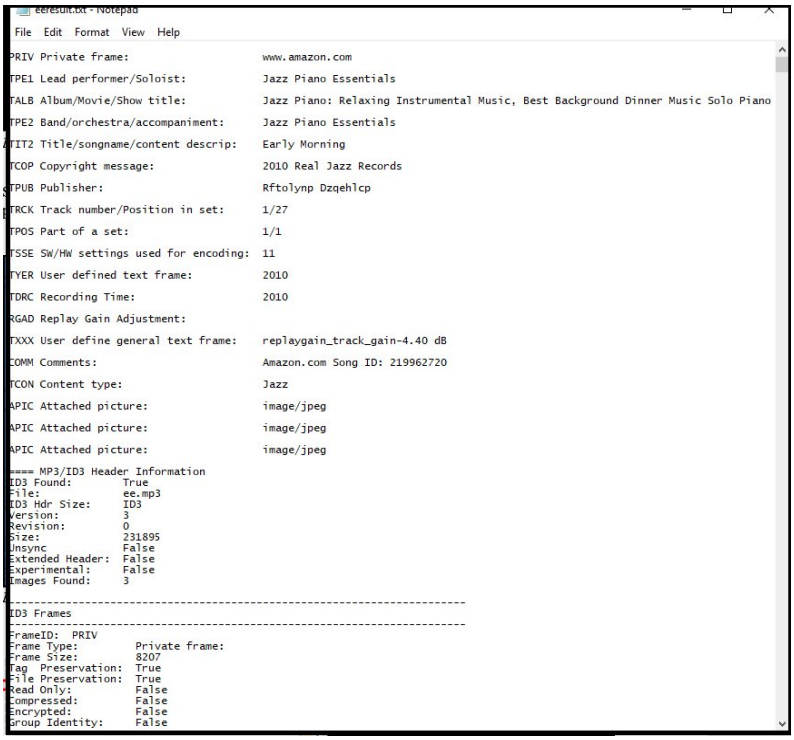


Figure 6 EE.mp3 Output

pymp3.py es.mp3 > esresult.txt

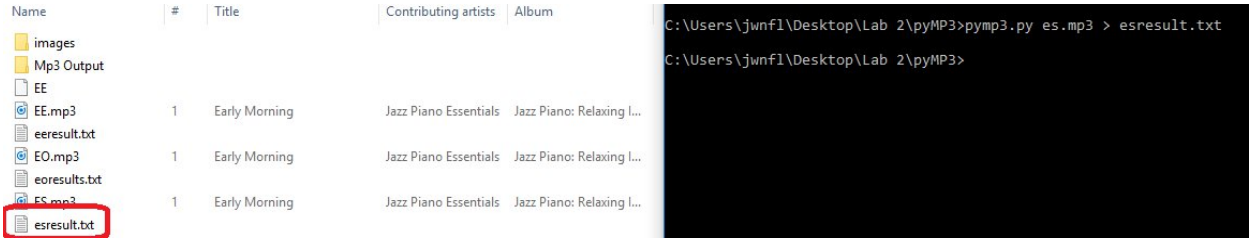


Figure 7 ES.mp3 Data Extraction

The examiner discovered ES.mp3 audio file contained an extra image.

Figure 8 ES.mp3 Images

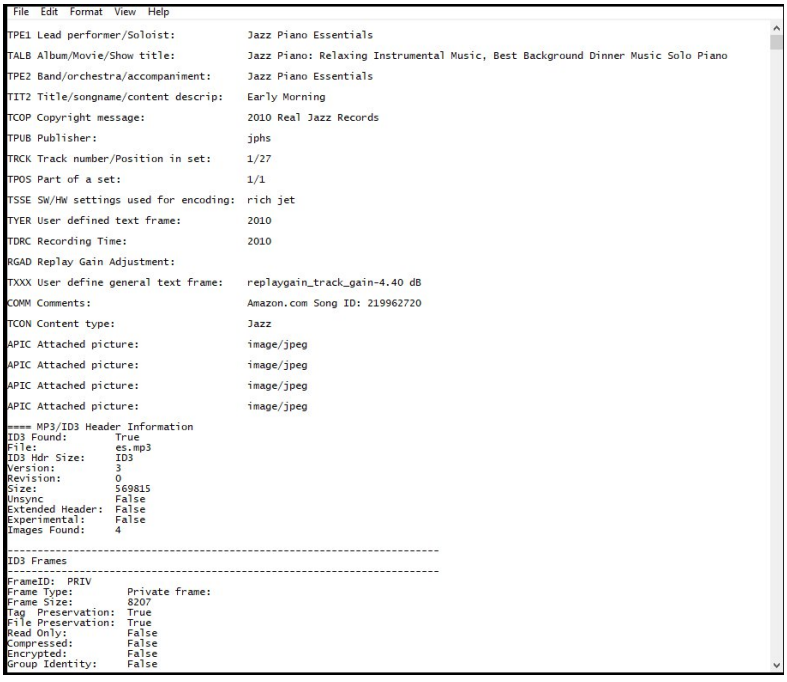


Figure 9 ES.mp3 Output

pymp3.py et.mp3 > etresult.txt

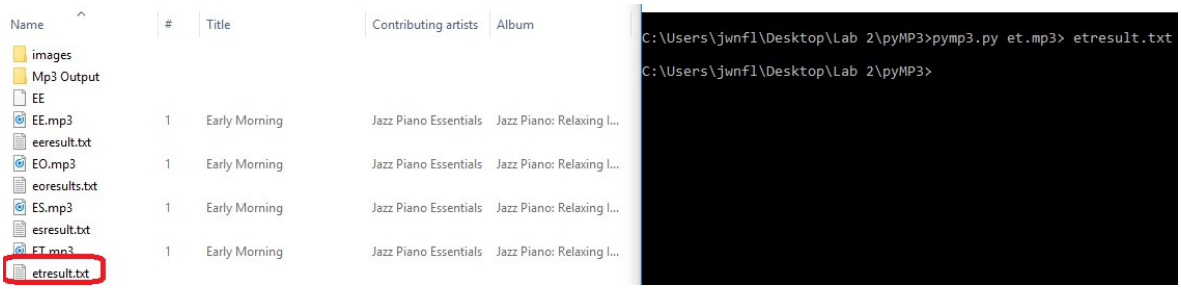


Figure 10 ET.mp3 Data Extraction

Figure 11 ET.mp3 Images

```
PRIV Private frame:                     www.amazon.com
TPE1 Lead performer/Soloist:            Jazz Piano Essentials
TALB Album/Movie/Show title:            Jazz Piano: Relaxing Instrumental Music, Best Background Dinner Music Solo Piano
TPE2 Band/orchestra/accompaniment:      Jazz Piano Essentials
TIT2 Title/songname/content descrip:    Early Morning
TCOP Copyright message:                 2010 Real Jazz Records
IPLS Involved people list:              Shawn McCreight
TPUB Publisher:                         Guidance Software
TRCK Track number/Position in set:      1/27
TPOS Part of a set:                     1/1
TYER User defined text frame:           2010
TDRC Recording Time:                    2010
RGAD Replay Gain Adjustment:
TXXX User define general text frame:    replaygain_track_gain-4.40 dB
COMM Comments:                          Amazon.com Song ID: 219962720
TCON Content type:                      Jazz
APIC Attached picture:                  image/jpeg
APIC Attached picture:                  image/jpeg
APIC Attached picture:                  image/jpeg

==== MP3/ID3 Header Information
ID3 Found:        True
File:             et.mp3
ID3 Hdr Size:     ID3
Version:          3
Revision:         0
Size:             231895
Unsync            False
Extended Header:  False
Experimental:     False
Images Found:     3

------------------------------------------------------------------------------
ID3 Frames
------------------------------------------------------------------------------
FrameID:  PRIV
Frame Type:          Private frame:
Frame Size:          8207
Tag  Preservation:   True
File Preservation:   True
Read Only:           False
Compressed:          False
Encrypted:           False
Group Identity:      False
```

Figure 12 ET.mp3 Output

pymp3.py eu.mp3 > euresult.txt

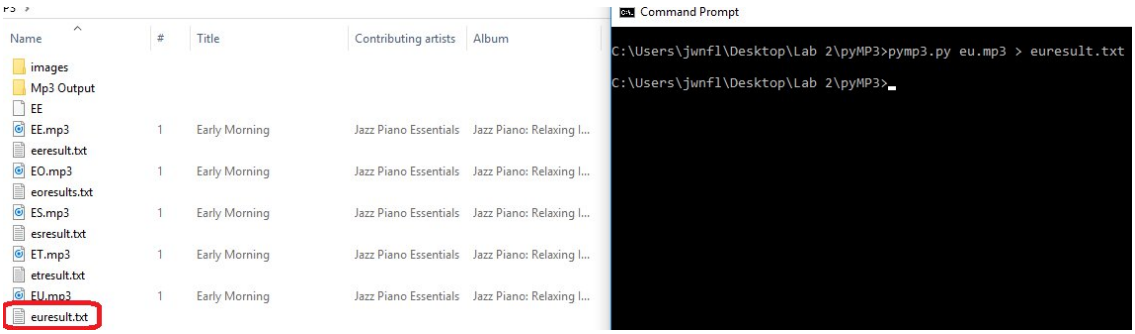


Figure 13 EU.mp3 Data Extraction

Figure 14 EU.mp3 Images

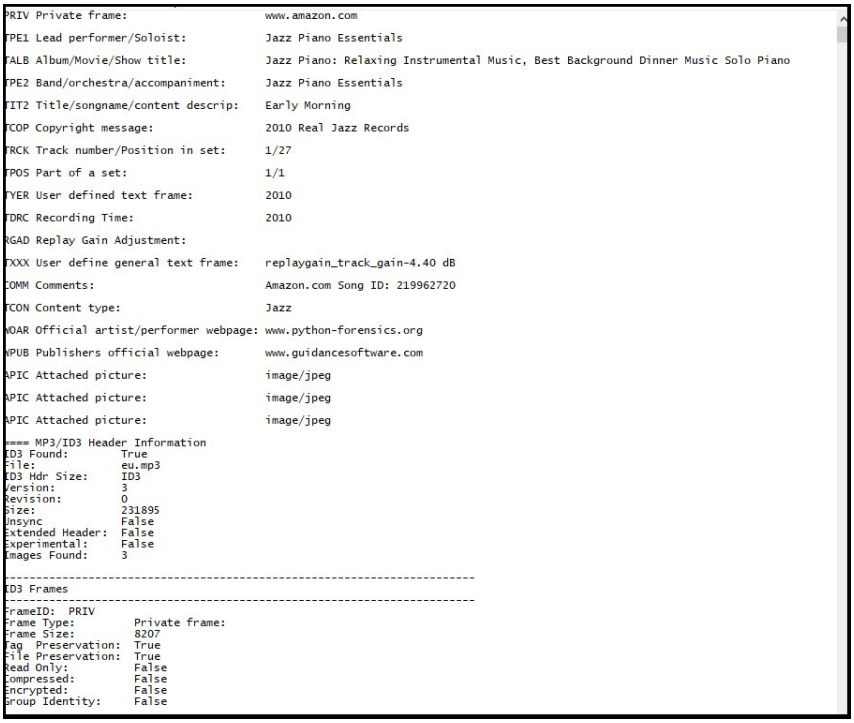


Figure 15 EU.mp3 Output

Image extractions

After the data was extracted from each of the mp3 files, images were embedded in all five of the files. The image folder displayed is where the images are located.

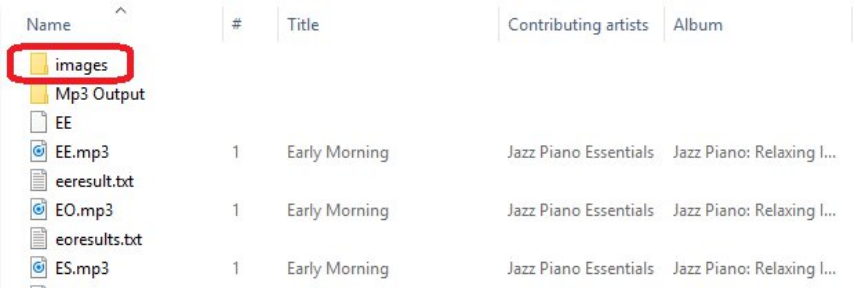


Figure 16 Location of Extracted Images

The images folder shows thirteen images total extracted from the mp3 files.

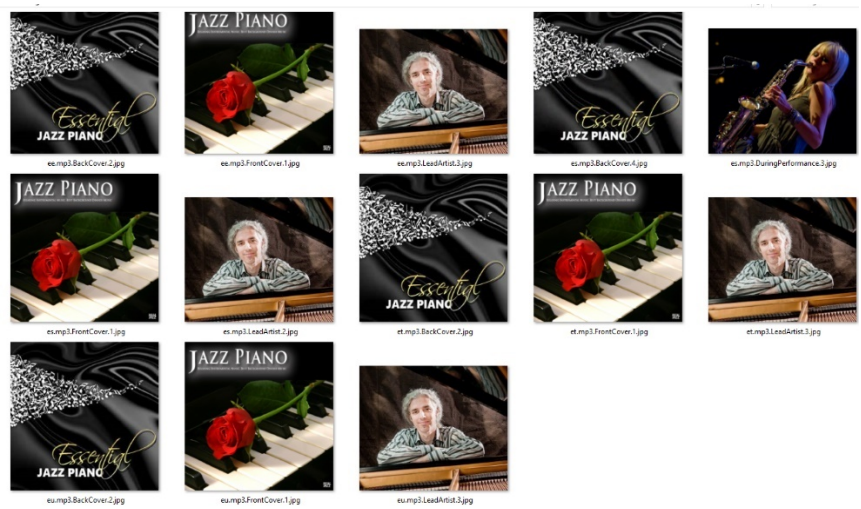


Figure 17 Extracted Images from mp3 files

Image Anomalies

StegAnalyst

The examiner reviews each of the obtained images with to see if there are any anomalies compared to the original images.

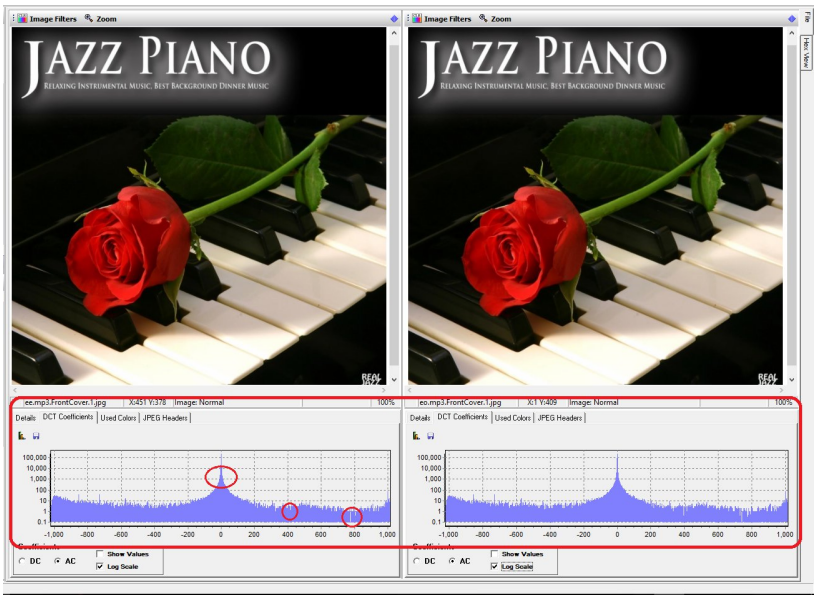


Figure 18 EE Front Cover

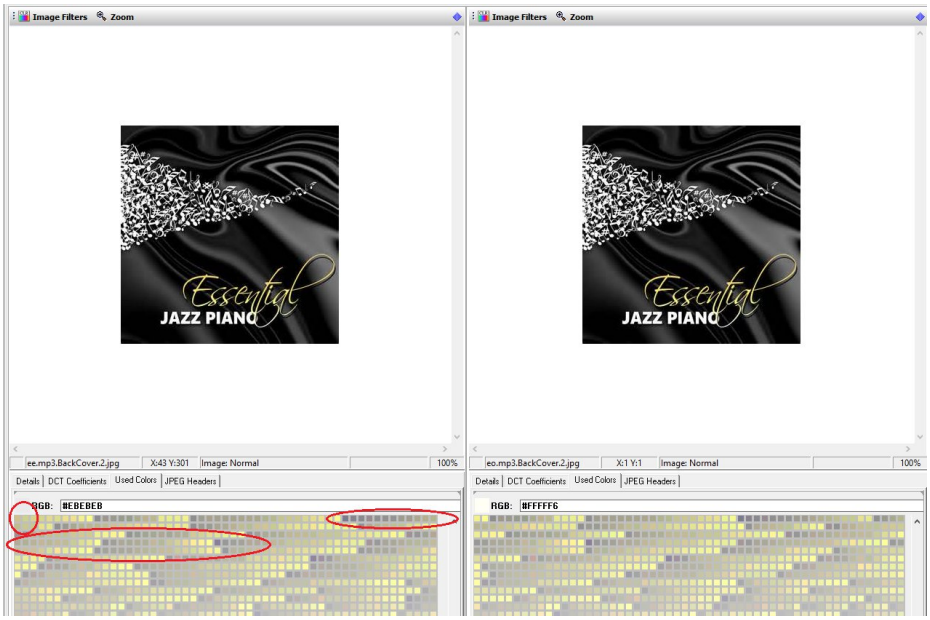


Figure 19 EE Back Cover

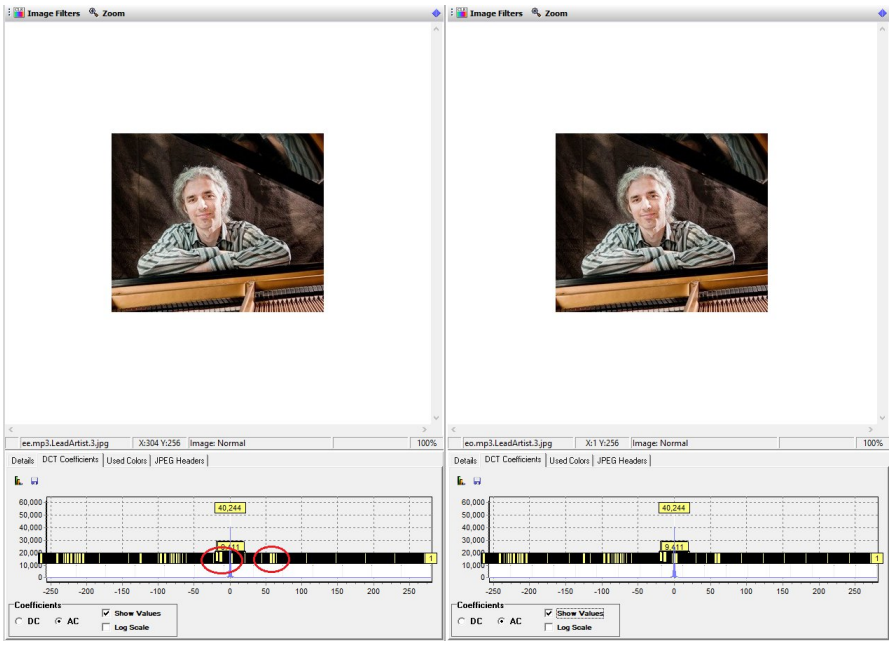


Figure 20 EE Lead Artist

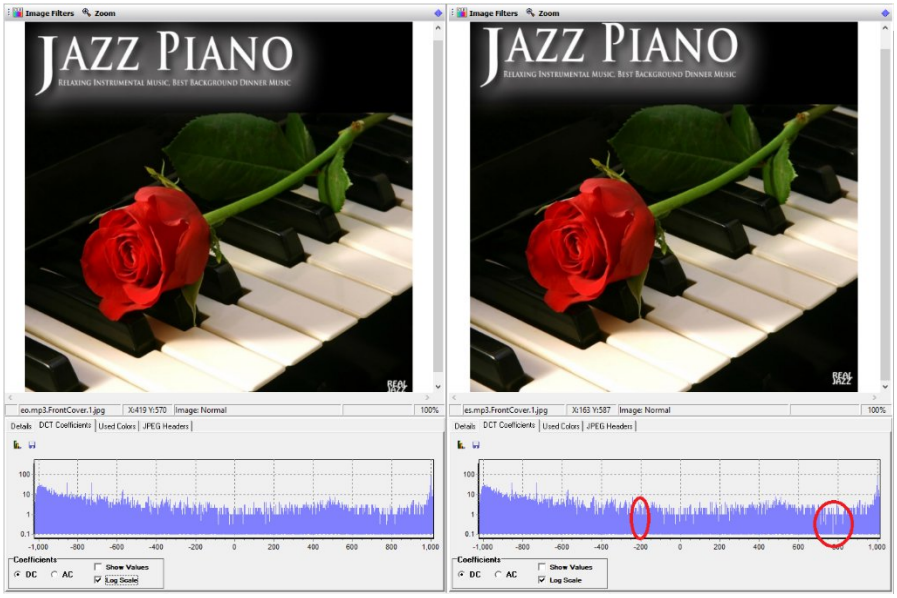


Figure 21 ES Front Cover DC Log Scale

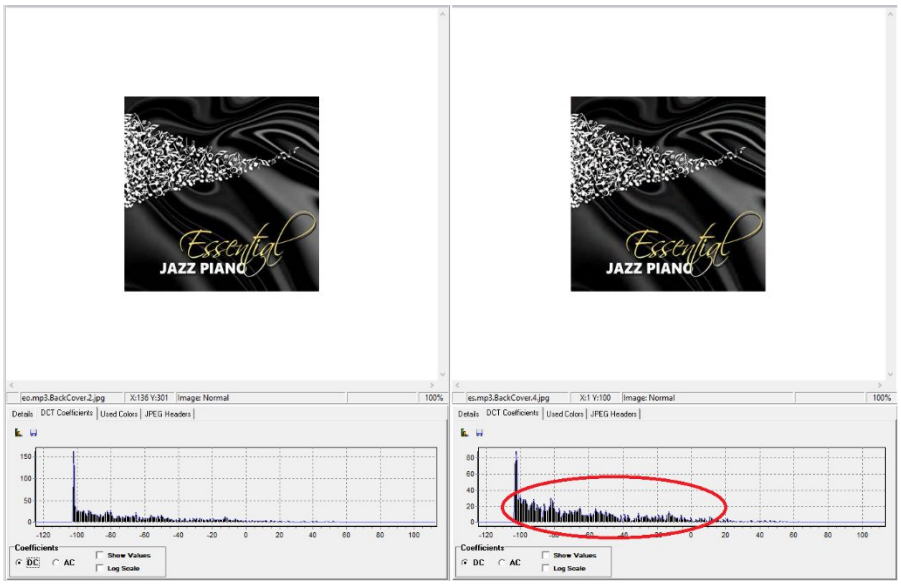


Figure 22 ES Back Cover DCT Coefficient Filter

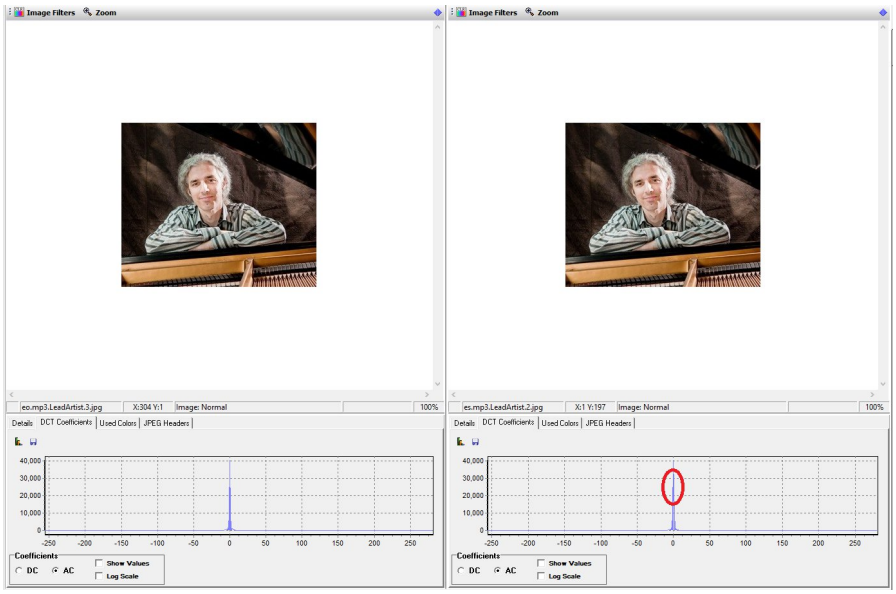


Figure 23 ES Lead Artist AC Coefficient Filter

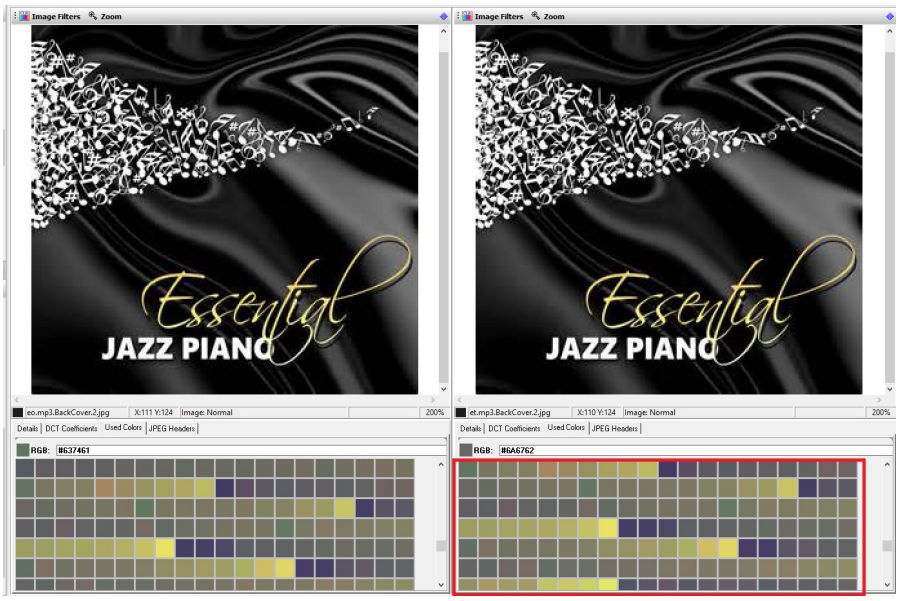


Figure 24 ET Back Cover Used Colors Filter

The examiner discovered that the images extracted have an image embedded within each file. The next step following utilizing StegoAnalyst is using Winhex to recover any images within the retrieved images from the mp3 files.

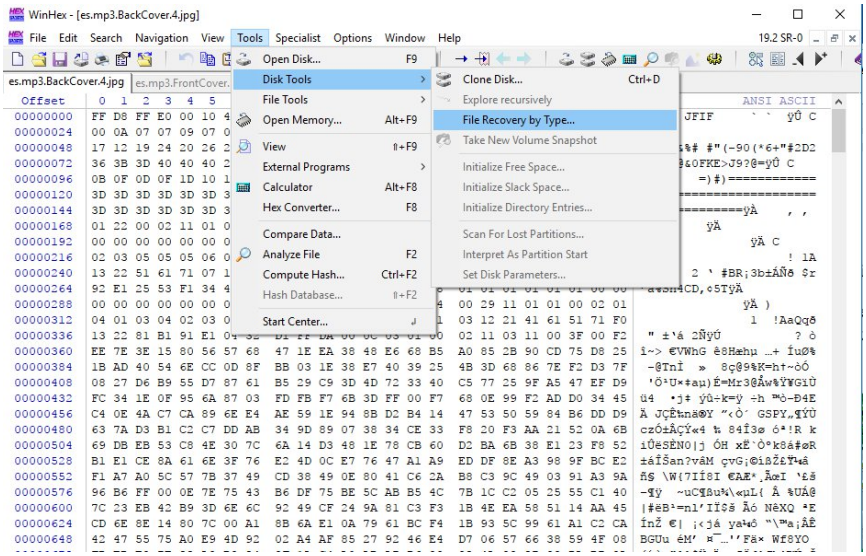


Figure 25 File Recovery

The examiner has options of what to look for each of the images opened in Winhex. The images extracted contained images embedded inside of the mp3 file which is why only the pictures folder is checked.

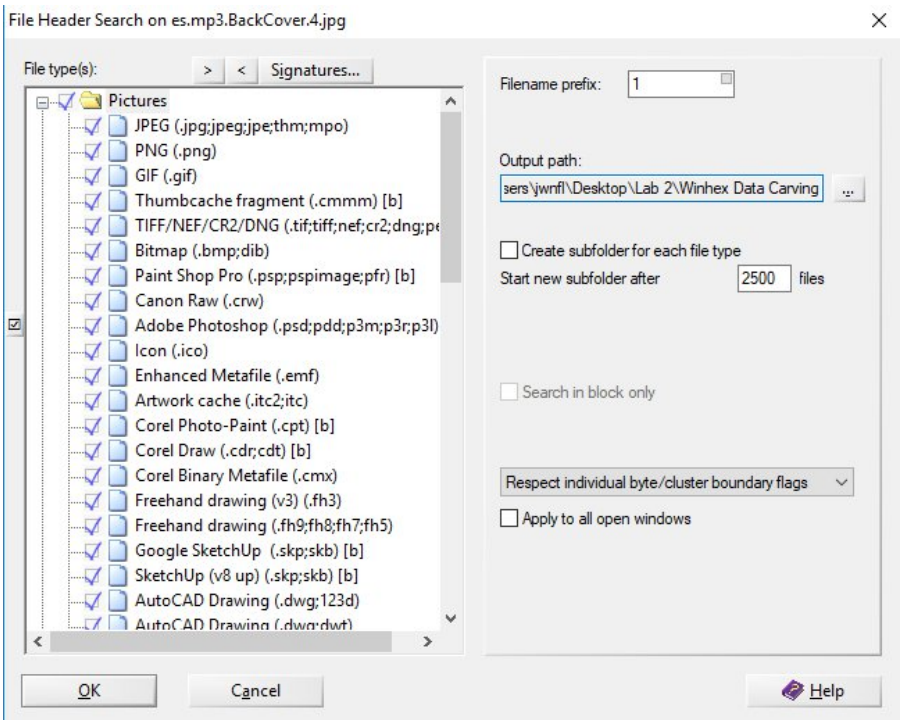


Figure 26 File Recovery Interface

The examiner will go to the folder where the extracted data was requested to be saved into.

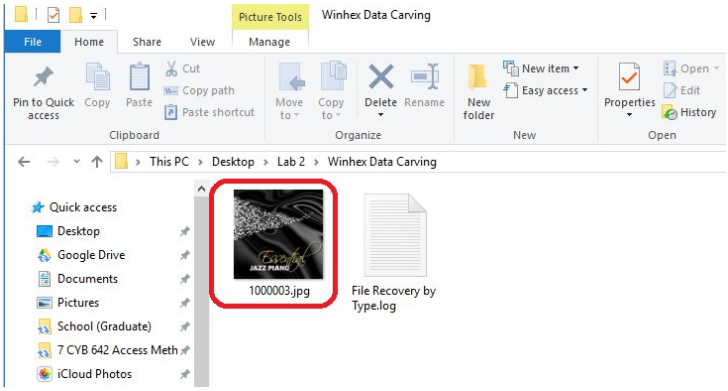


Figure 27 ES.mp3 Back-Cover Image Extraction

The examiner guessed correctly and there, in fact, was an image embedded inside of the back-cover file.

The examiner will now go through each of the images beyond the EO.mp3 file to search for more possibly hidden data.

Tools > Disk Tools > File Recovery by Type

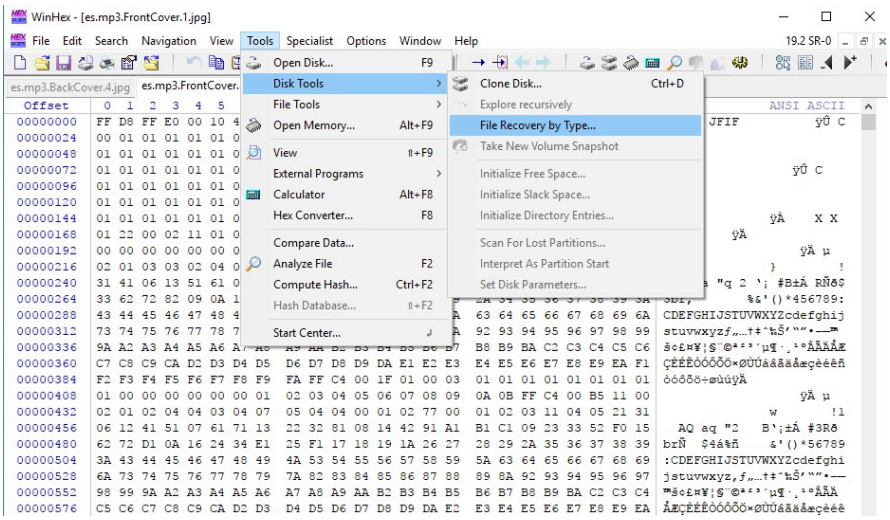


Figure 28 ES.mp3 Front Cover

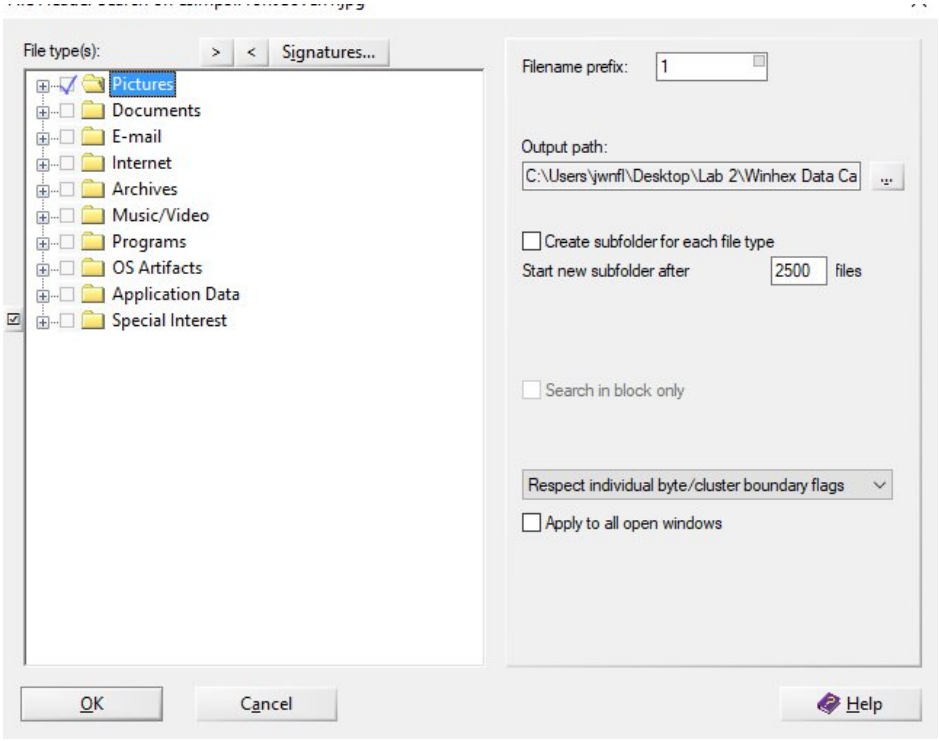


Figure 29 Data Type Options

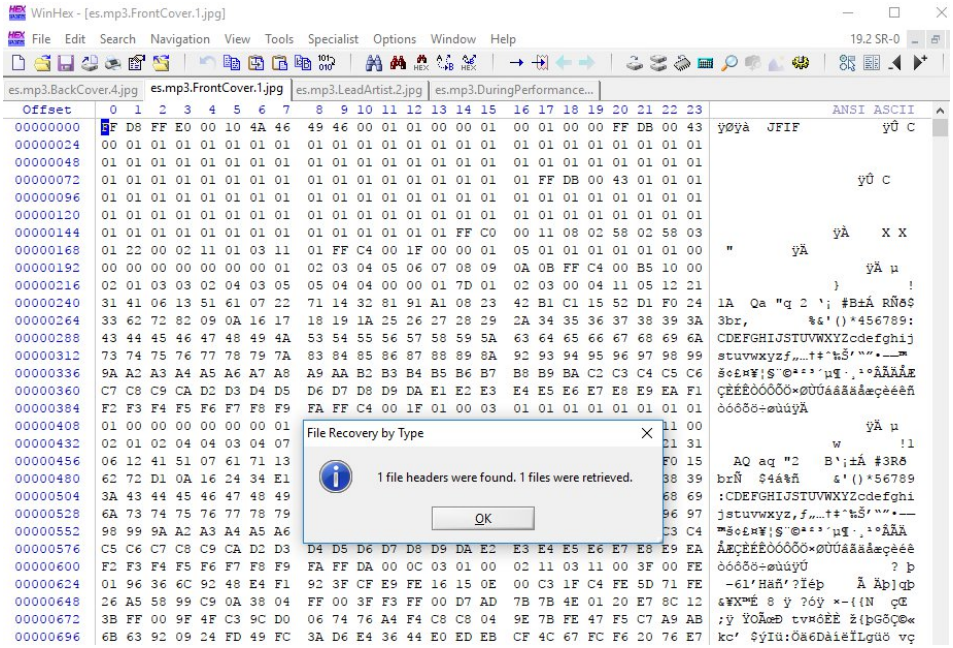


Figure 30 ES.mp3 Data Extraction

The examiner discovered that the front cover image file also contained an embedded inside of the file as well.

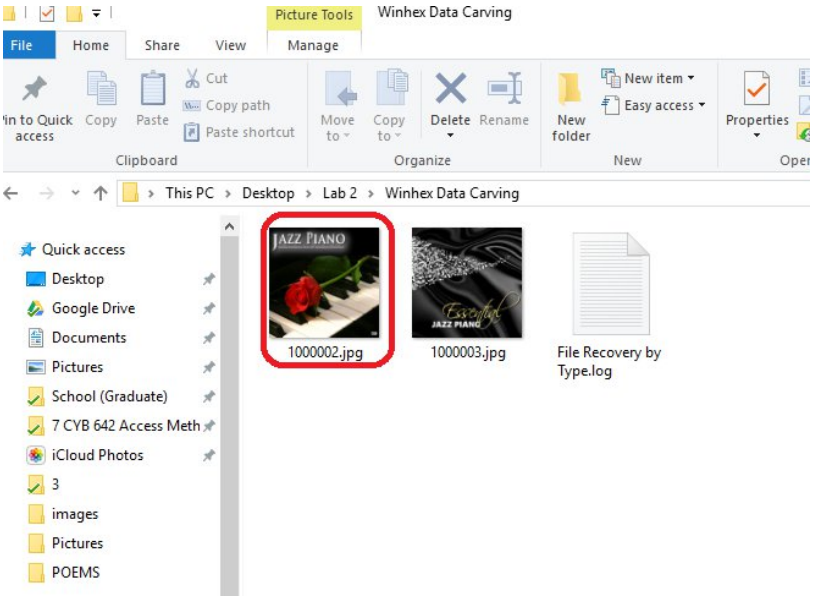


Figure 31 Front Cover Image Extraction

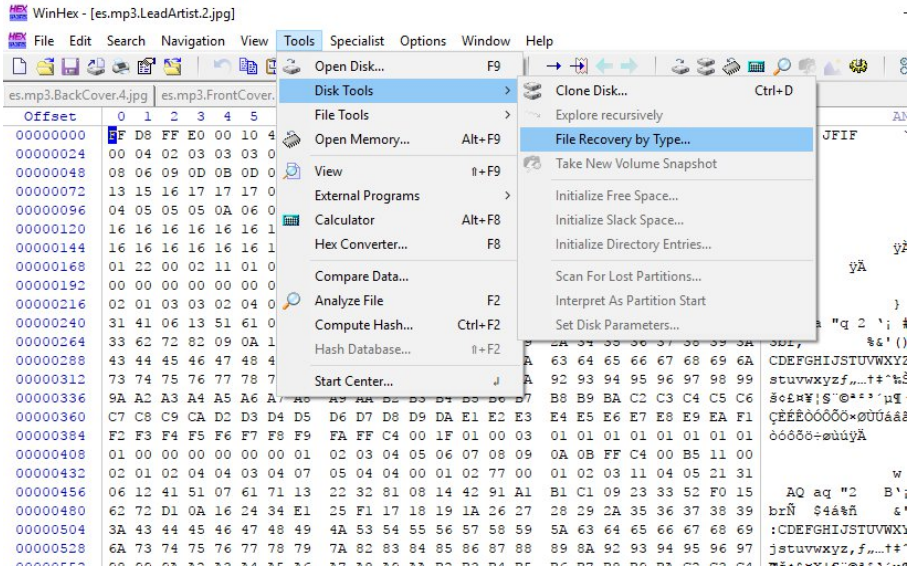


Figure 32 Lead Artist Image

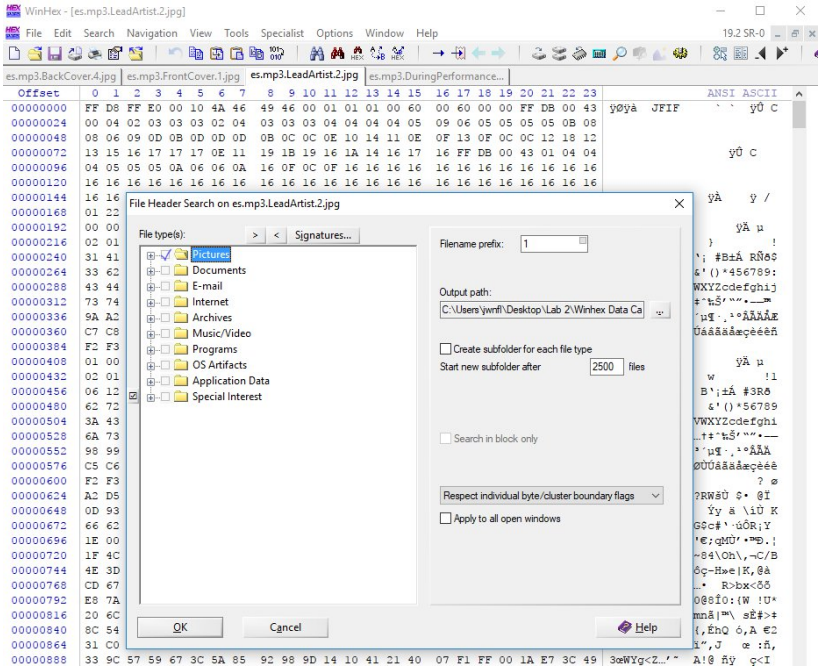


Figure 33 Lead Artist File Type

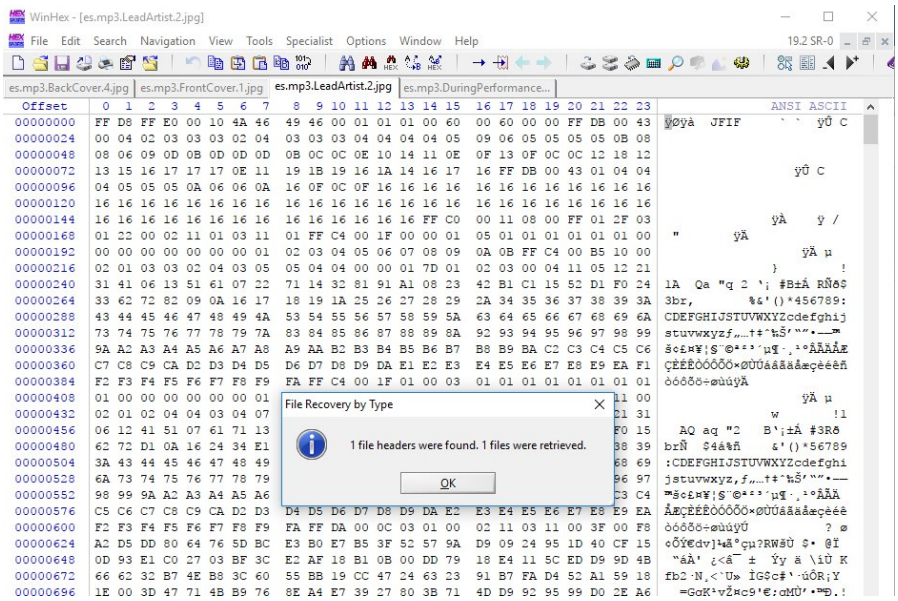


Figure 34 Lead Artist Image Extraction

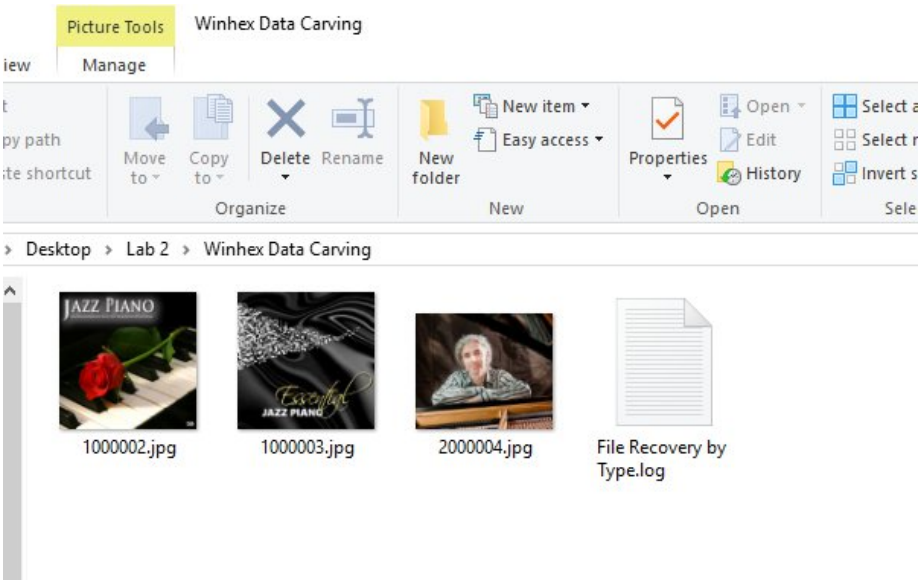


Figure 35 Lead Artist Image Extraction

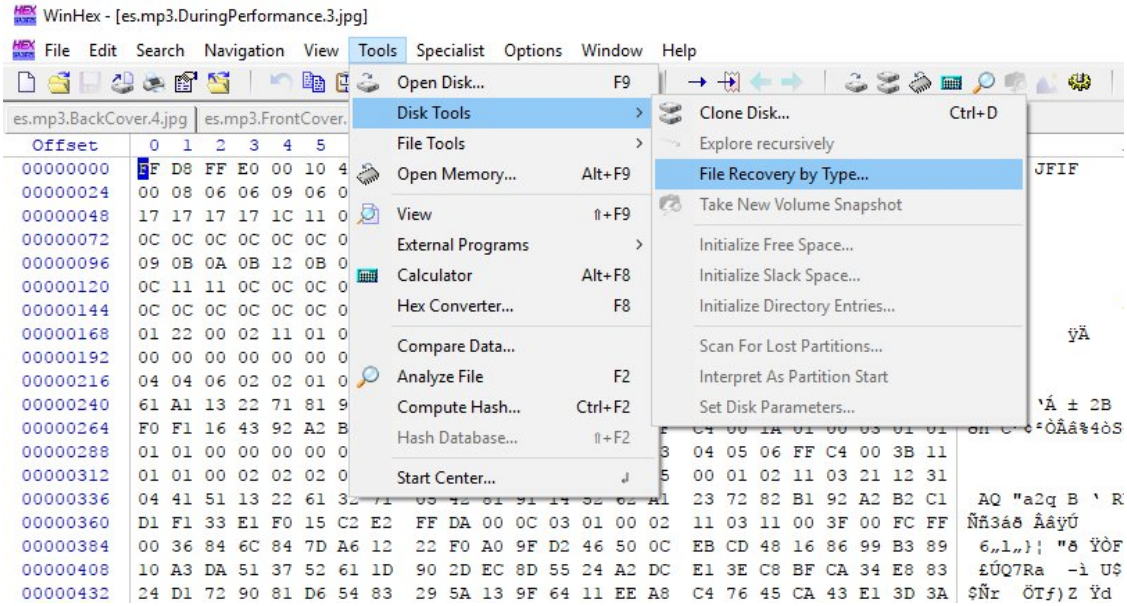


Figure 36 File Recovery

The examiner discovered the final image from the extracted images from the ES.mp3 files does not have any hidden images which conclude the image extraction process.

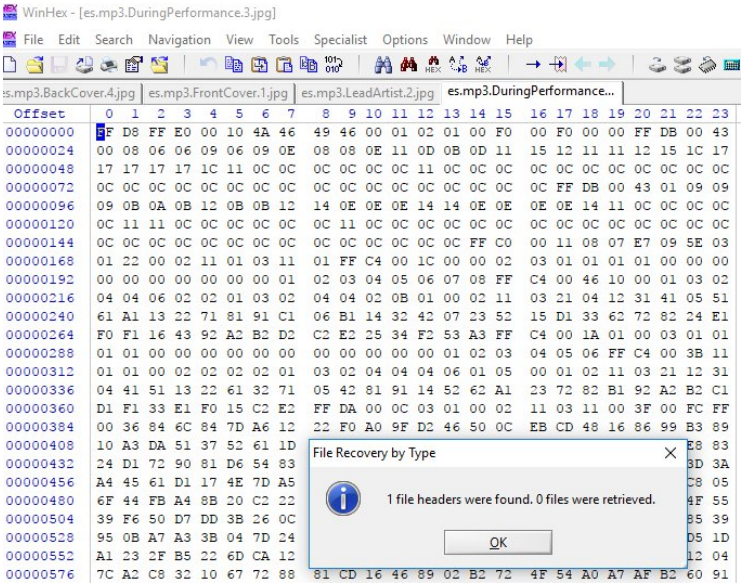


Figure 37 No Image Hidden

TrueCrypt

Volume Creation

Utilizing TrueCrypt to transfer data between two or more parties is ideal for individuals looking to send to each other private information hidden from everyone.

The examiner needs to select a file to create a container into. For this experiment, the examiner will use a short video.

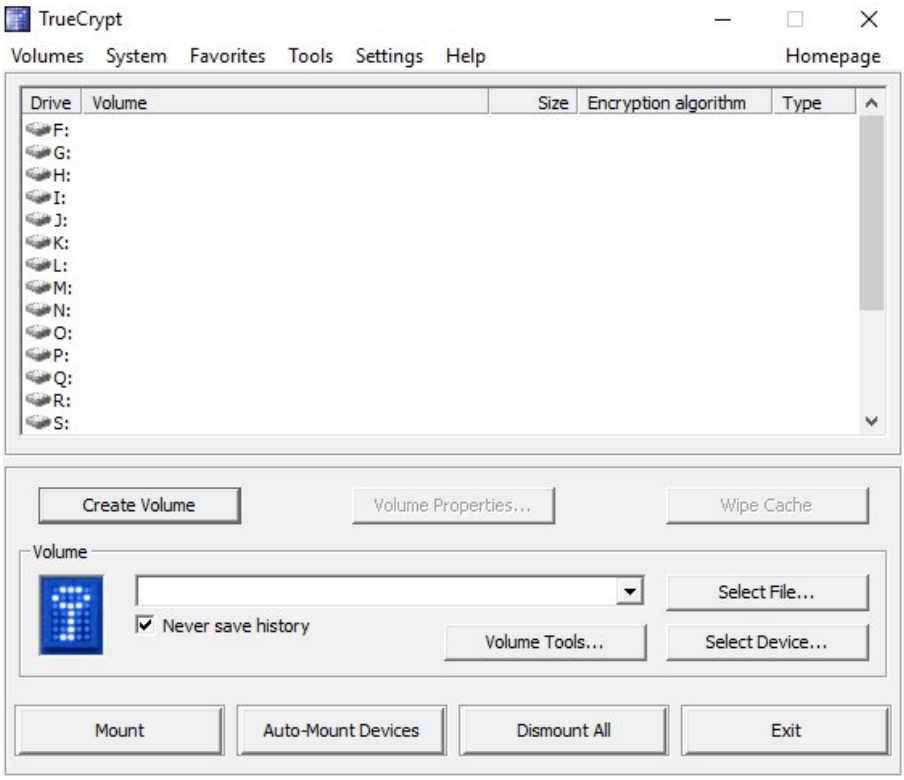


Figure 38 TrueCrypt Interface

Setting up the container needs to be an encrypted container to protect the data from any government entities to avoid detection. Once the appropriate option is selected, the examiner moves on to the next task.

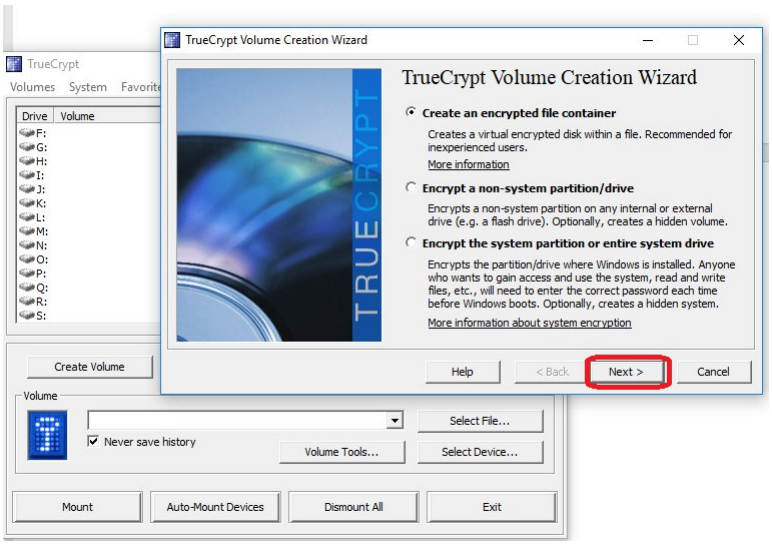


Figure 39 Volume Selection

The examiner selects the Hidden TrueCrypt volume which ensures the file with the information stored in the container can only be extracted using the appropriate password.

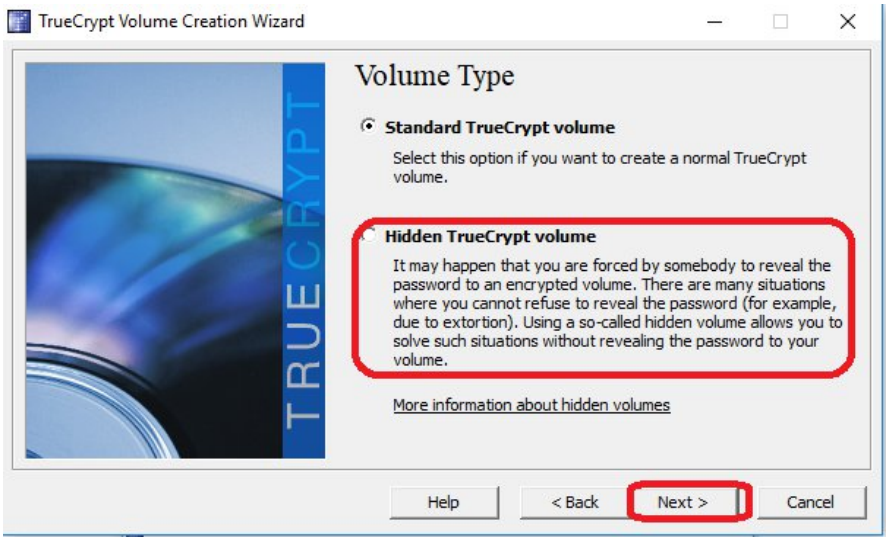


Figure 40 Hidden Volume Selection

Normal mode is selected since this experiment does not need the examiner to create a new hidden volume within a volume already created.

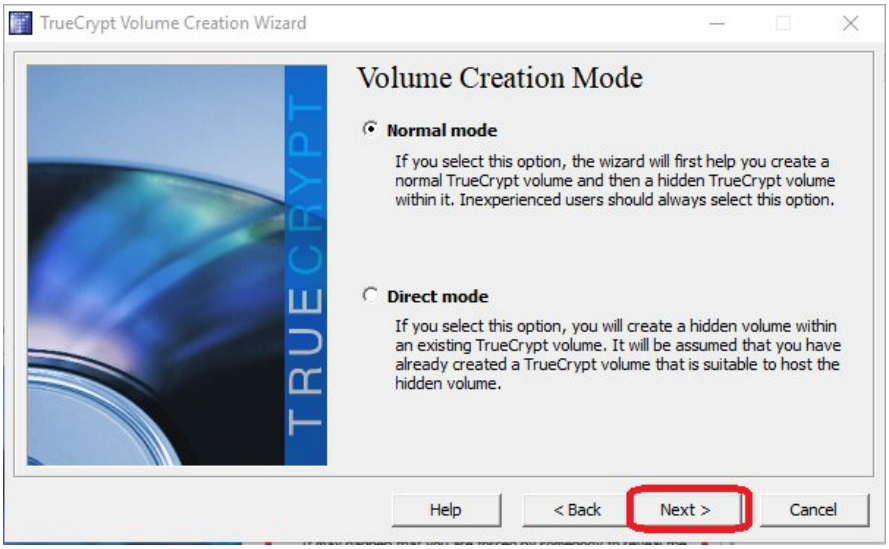


Figure 41 Normal Mode

The location to save the video file with the data collected within the file is selected in this step of the experiment.

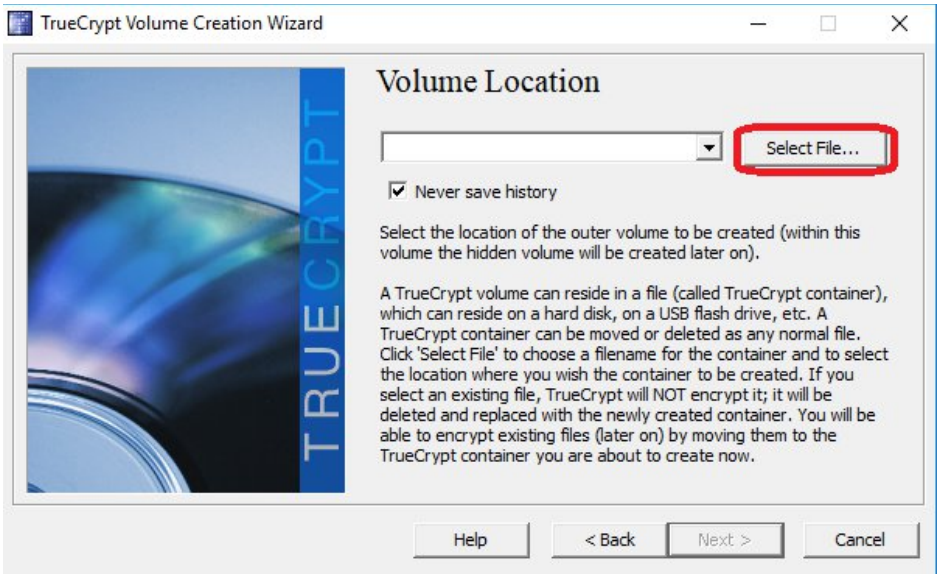


Figure 42 Location to Save File

The location the examiner saved the video is in the same folder the original file is saved to quickly find the encrypted video. Once the location of the data is selected, the examiner moves on to the next screen clicking on the following button.

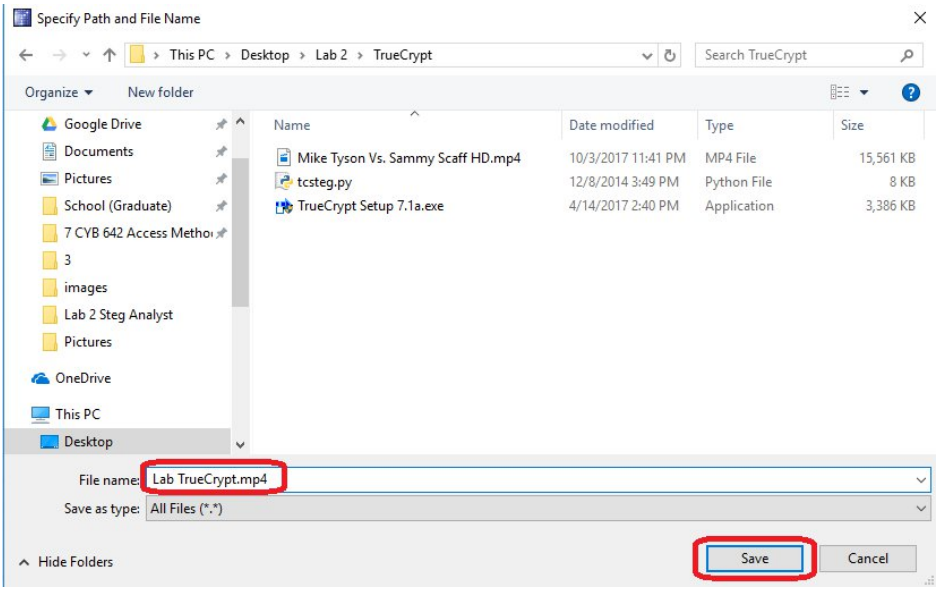


Figure 43 Saved Video Location

The examiner now moves forward with setting the passwords for the outer volume and inner volume.

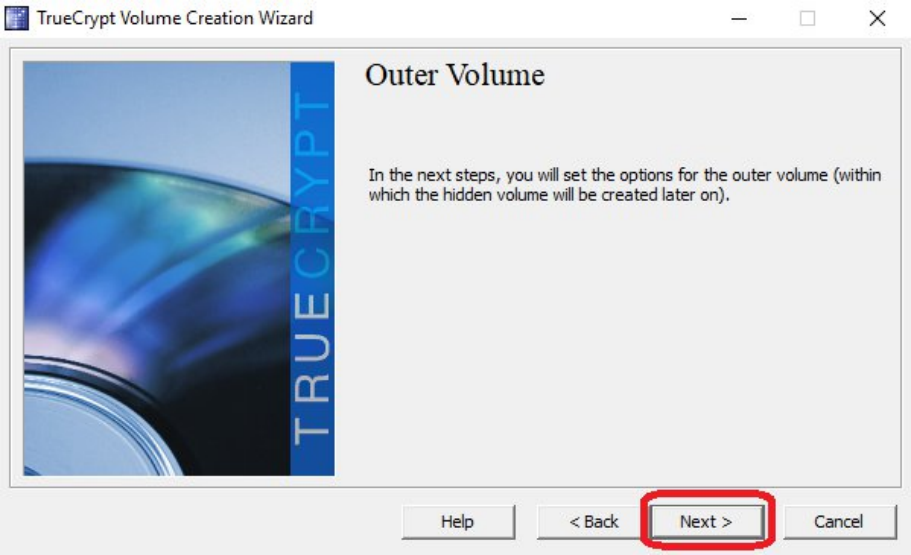


Figure 44 Outer Volume Creation

The outer volume encryption criteria configured for the volume is AES. The examiner is provided the option to rest the algorithm but moves along with the creation for this experiment.

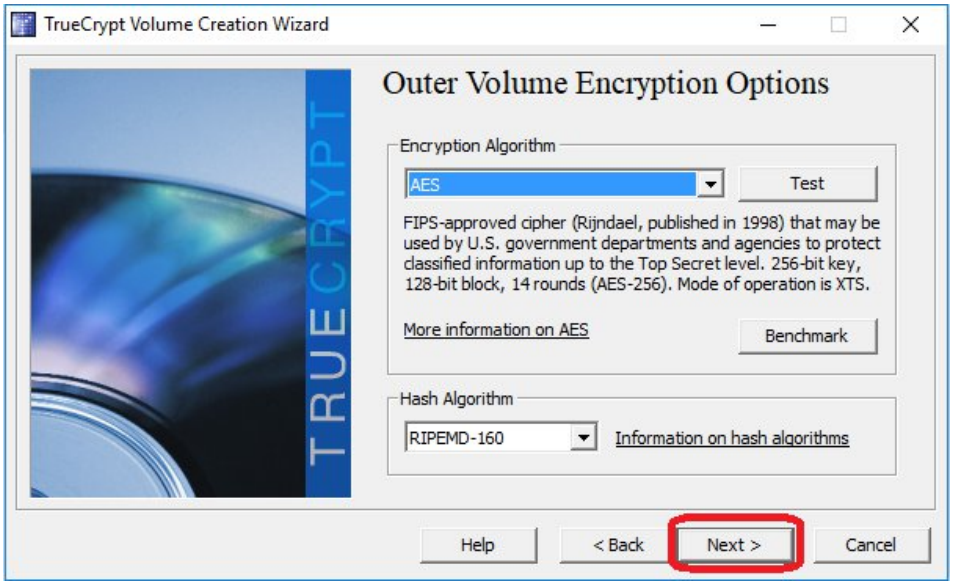


Figure 45 Encryption Type

The outer volume size limit is chosen for the video which is 10MB due to the video size being 15MB.

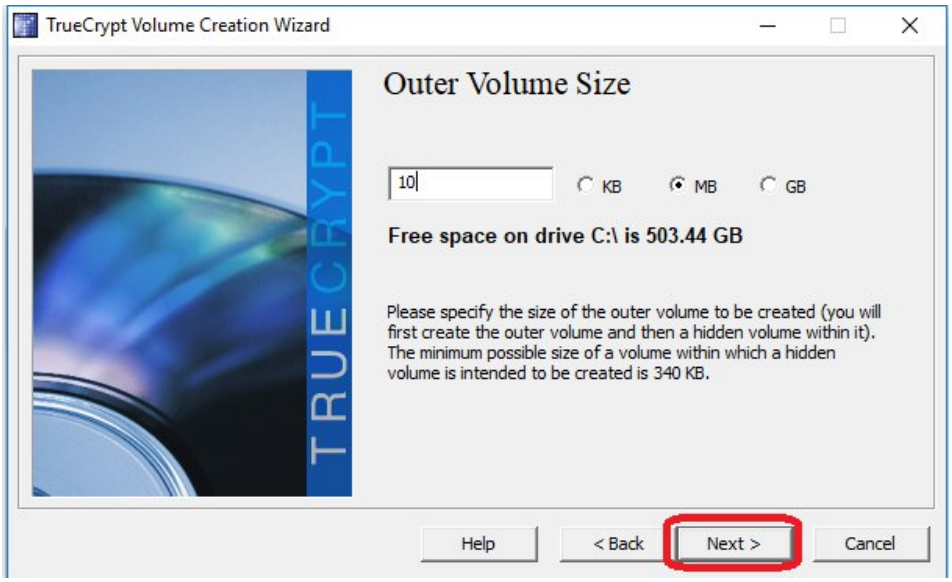


Figure 46 Container Size Configuration

Setting the password volume was set as “hello” for this experiment since the container isn’t created for other purposes.

Figure 47 Outer Container Password

The outside pool continually generates a new pool when the examiner moves the mouse around the screen. One the examiner clicks the format button, the pool and the header and master keys are set.

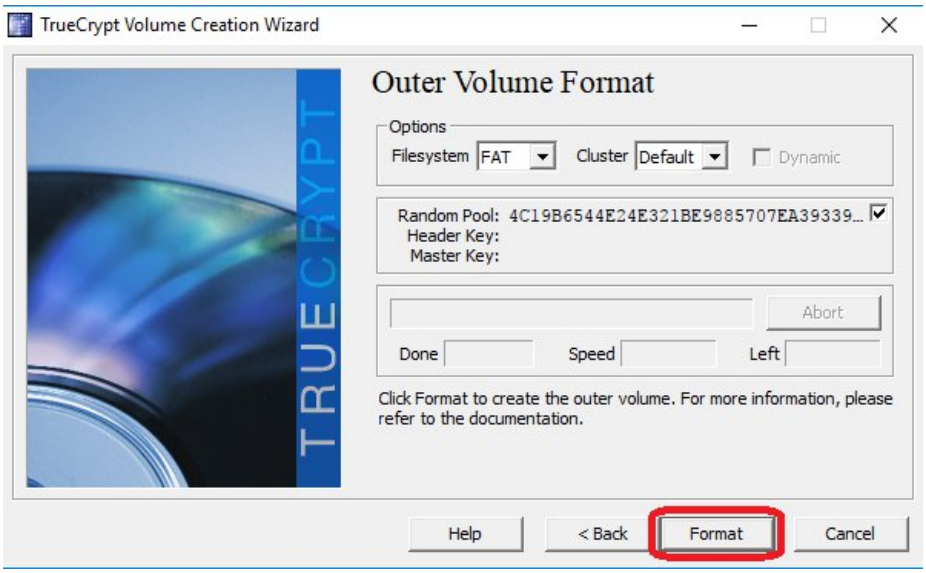


Figure 48 Outer Volume Format

The examiner successfully configured the outer volume and is now ready to create the hidden volume of the experiment.

Figure 49 Outer Volume Completed

The next step is moving forward to configure the hidden volume where the actual data is located that the suspect can hide the real data.

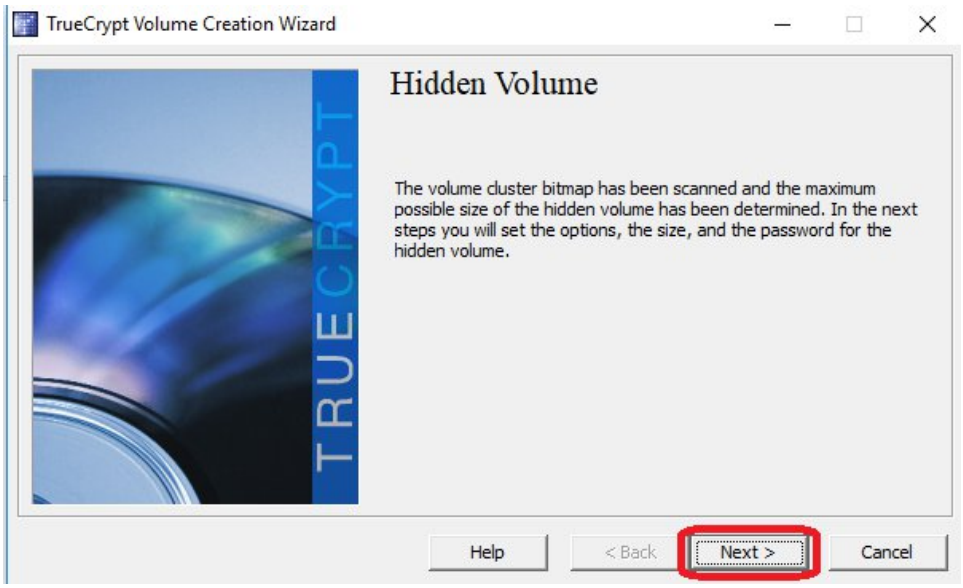


Figure 50 Hidden Volume

The examiner proceeds through the same process as the outer volume which makes the configuration of the hidden volume move along faster.

Figure 51 Hidden Volume Encryption

The size of the hidden volume is set during this step. During this phase the examiner is limited to the amount of space that can be allocated due to the size of the video.

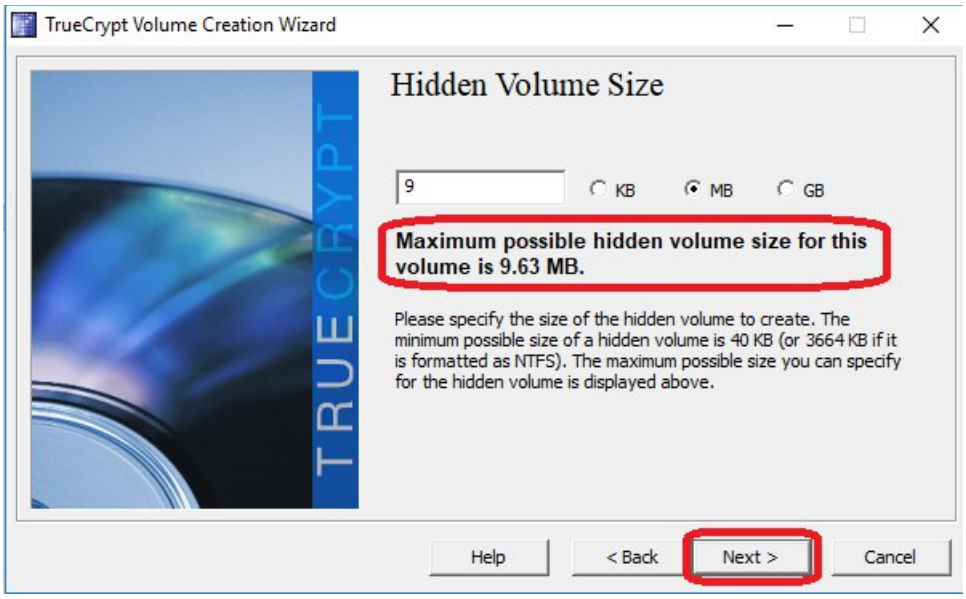


Figure 52 Hidden Volume Size Configuration

The hidden volume password is "cashmoney3." This passphrase is set very weak for this experiment.

Figure 53 Hidden Volume Password

Identical to the outer volume format, the random pool is randomly set and the header and master key are set to random numbers. The fields auto-populate once the format button is clicked.

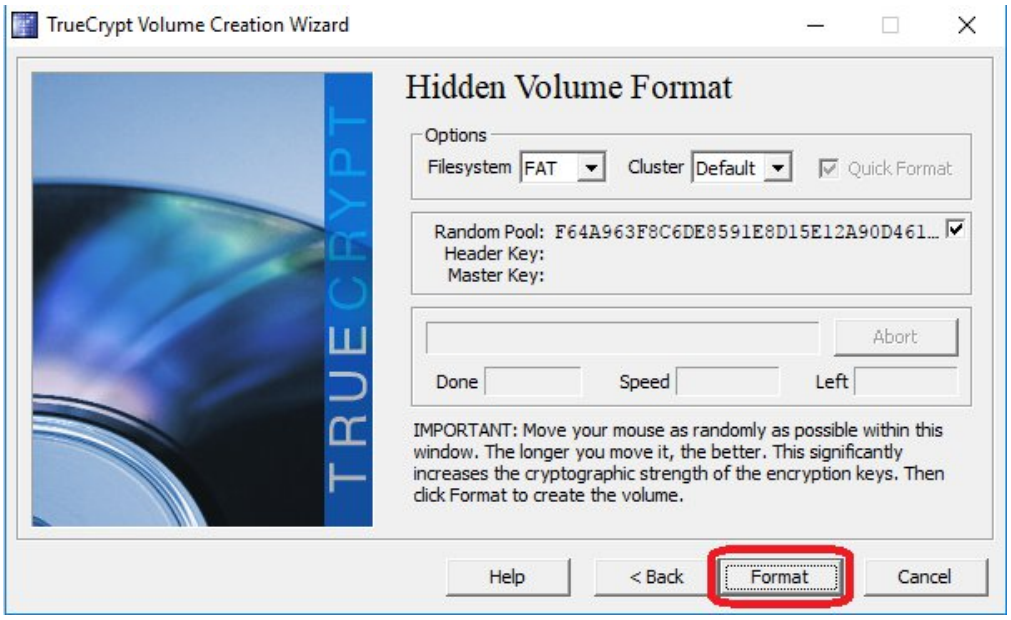


Figure 54 Hidden Volume Format

The examiner successfully created the hidden volume. Now the container can be embedded into the video selected. Figure 56 displays the last step in the creation of the secret volume.

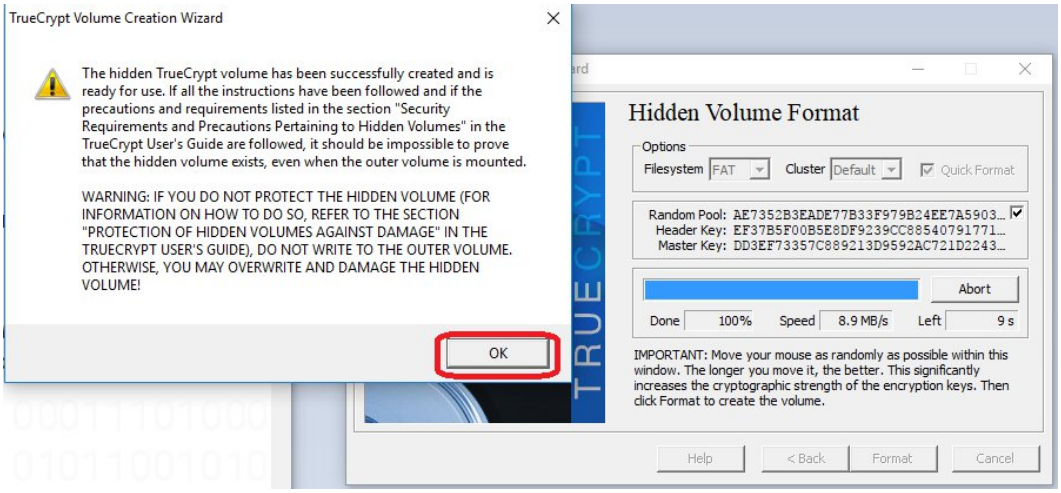


Figure 55 Hidden Volume Configuration Completed

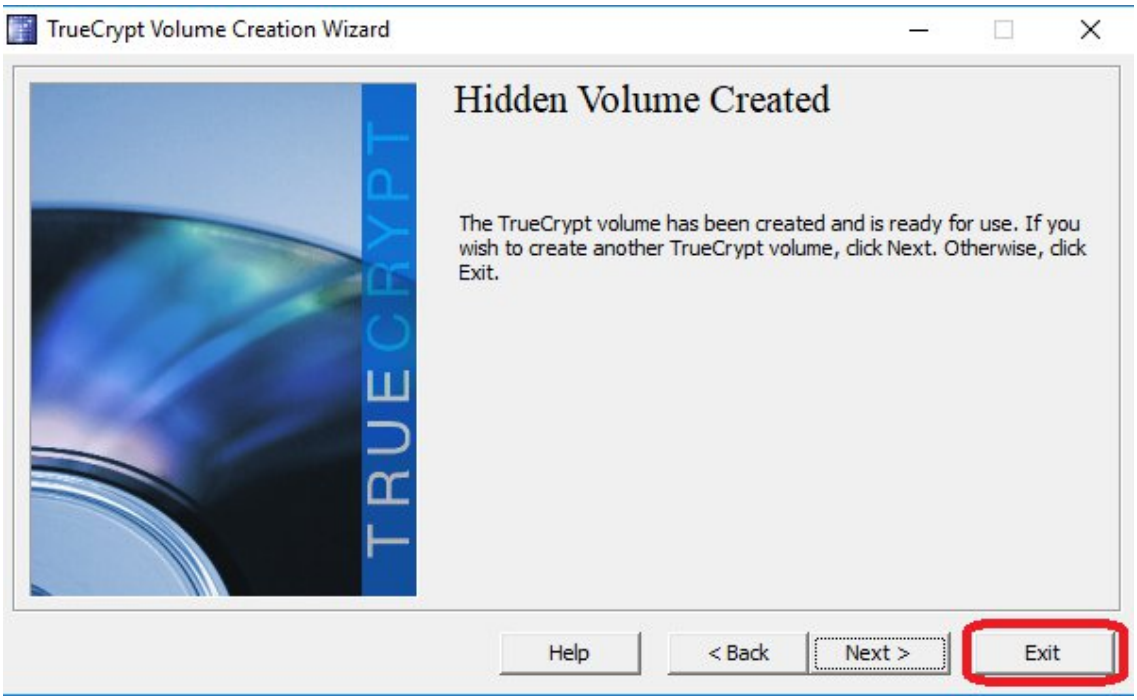


Figure 56 Hidden Container

The examiner now navigates to the command prompt to complete the experiment by embedding the container in the video.

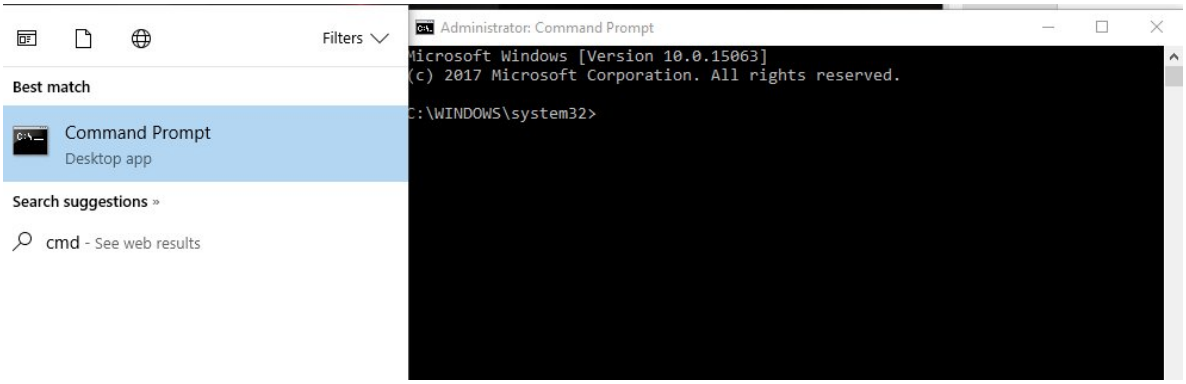


Figure 57 Command Prompt

The figure below shows the container created where the Tyson.mp4 video will be copied to for this experiment.

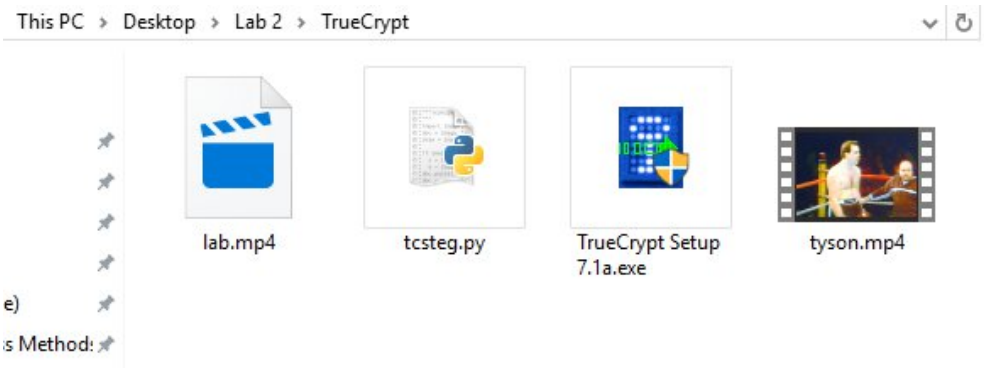


Figure 58 Before Copying Tyson.mp4

The command prompt screen shows the command needed to copy the Tyson.mp4 video to the lab container to complete embedding the container.

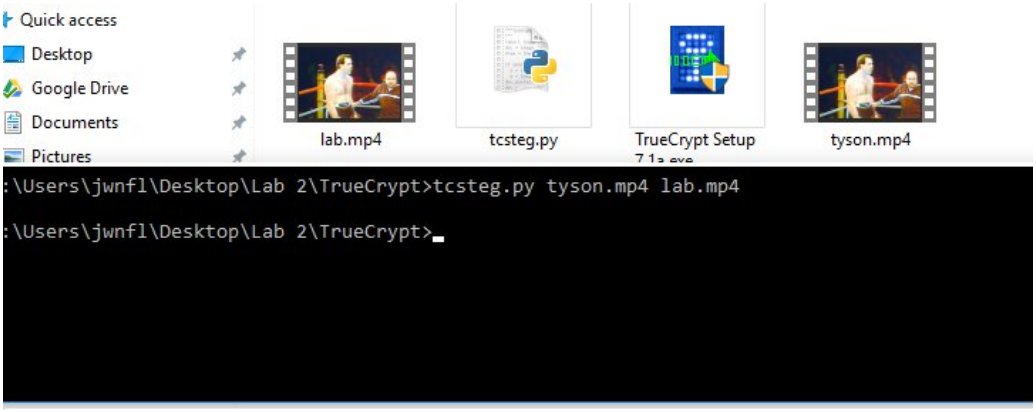


Figure 59 Container Embedded

The examiner has opened TrueCrypt to test if the video and container both are fully operational. The volume with the video needs to be mounted to check the video.

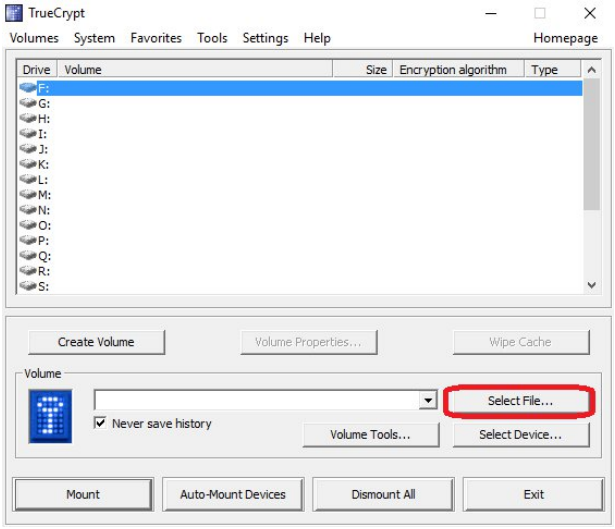


Figure 60 TrueCrypt Mounting

The video lab4.mp4 is selected to test the video and container.

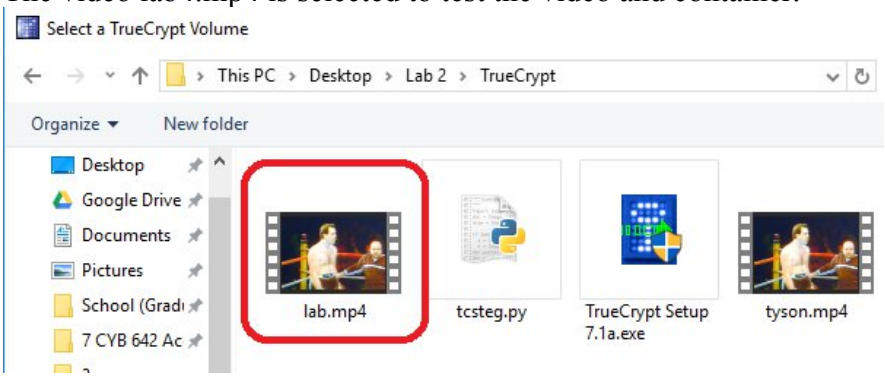
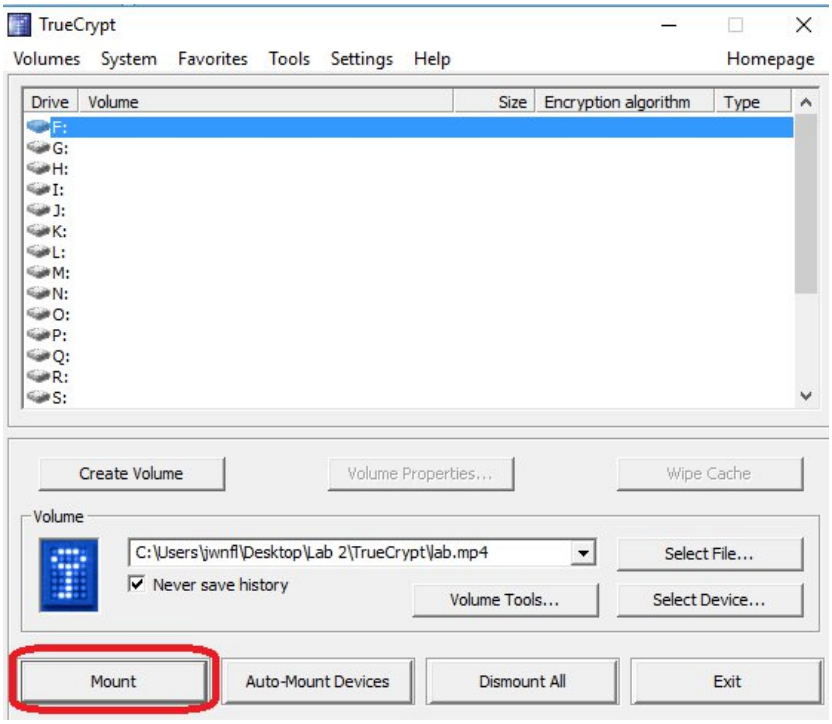


Figure 61 Video Select Window

The file is selected and now needs to be mounted to the computer as another hard drive. The created drive selected is F.



Upon mounting the file, the examiner now needs to enter the password for the hidden volume to access the contents within the container.

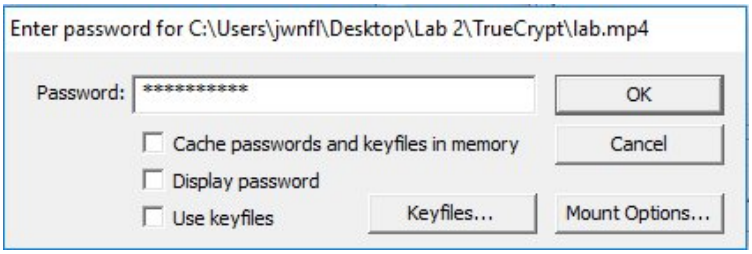


Figure 62 Encryption Authentication

The password was entered correctly which shows the mounted volume. The container is now ready to be viewed to ensure the file was configured correctly.

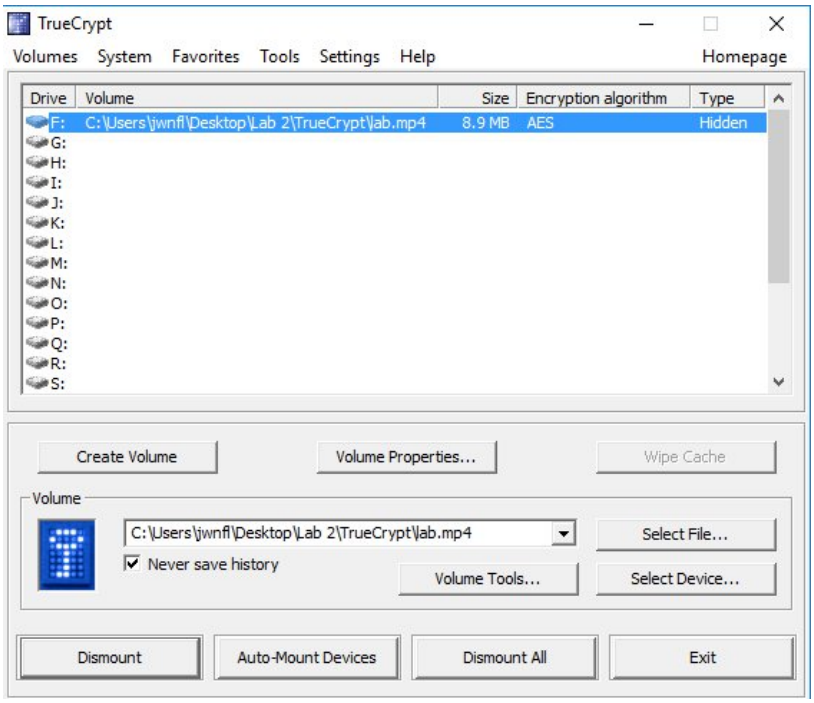


Figure 63 Mounted Volume

Figure 64 shows the counted drive which the examiner selected to mount the container to for viewing.

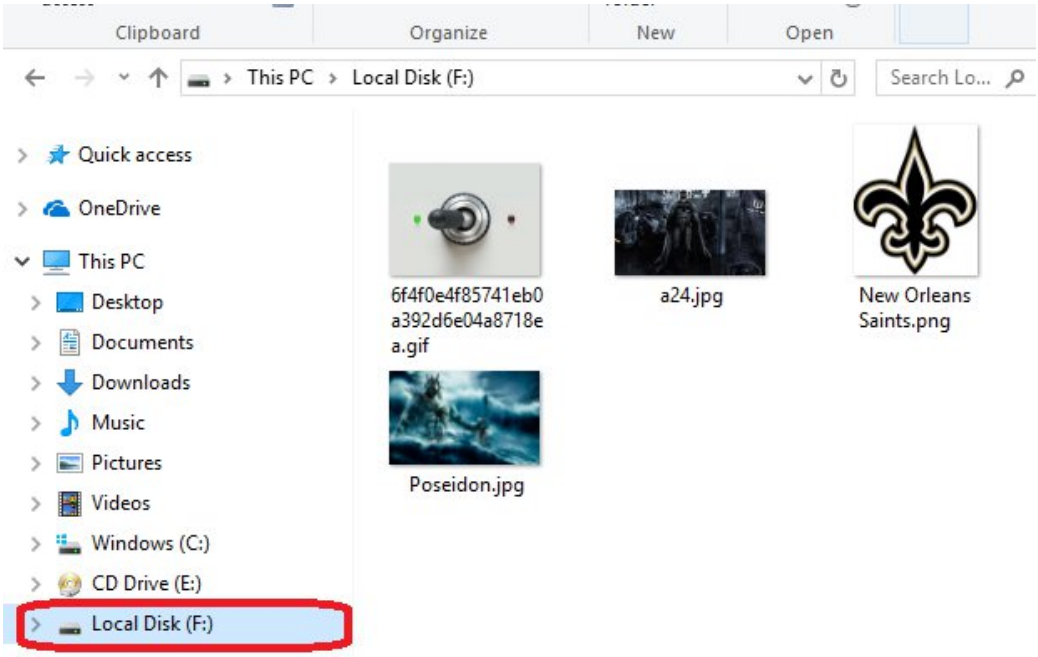


Figure 64 Mounted Drive F:

Lab.mp4 is selected to for testing. The examiner completed the process correctly which shouldn't create any issues.

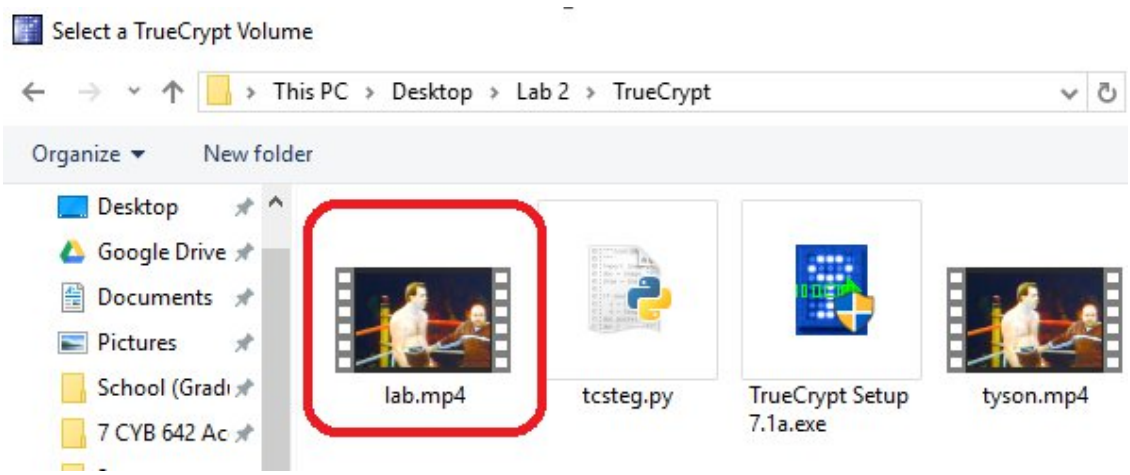


Figure 65 Test Phase

The video plays without any issues. The examiner now will move on to the outer volume to ensure it works as well.

Figure 66 Video

The examiner needs to dismount the drive to avoid detection of any activities out of the ordinary happening.

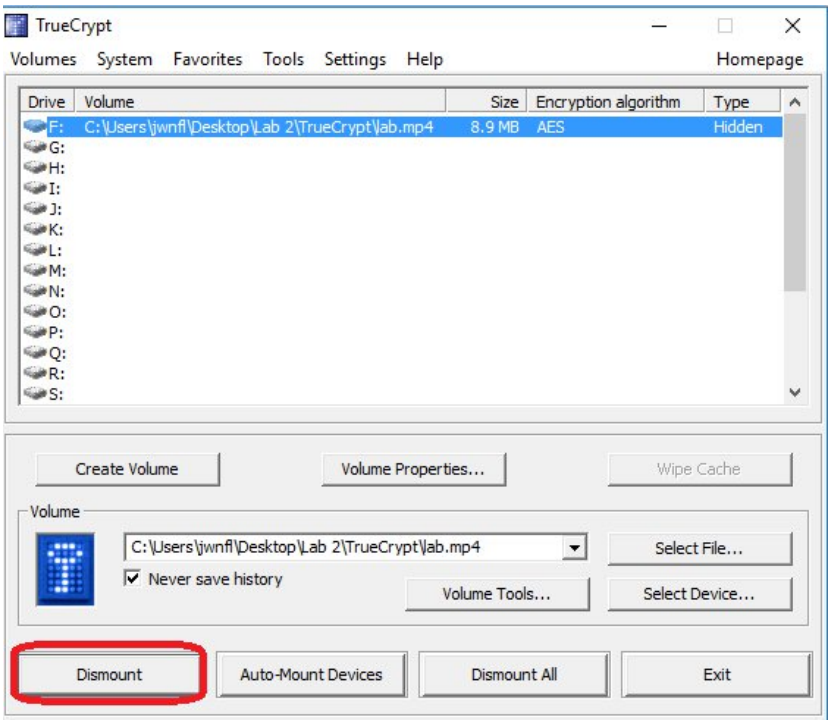


Figure 67 Dismount

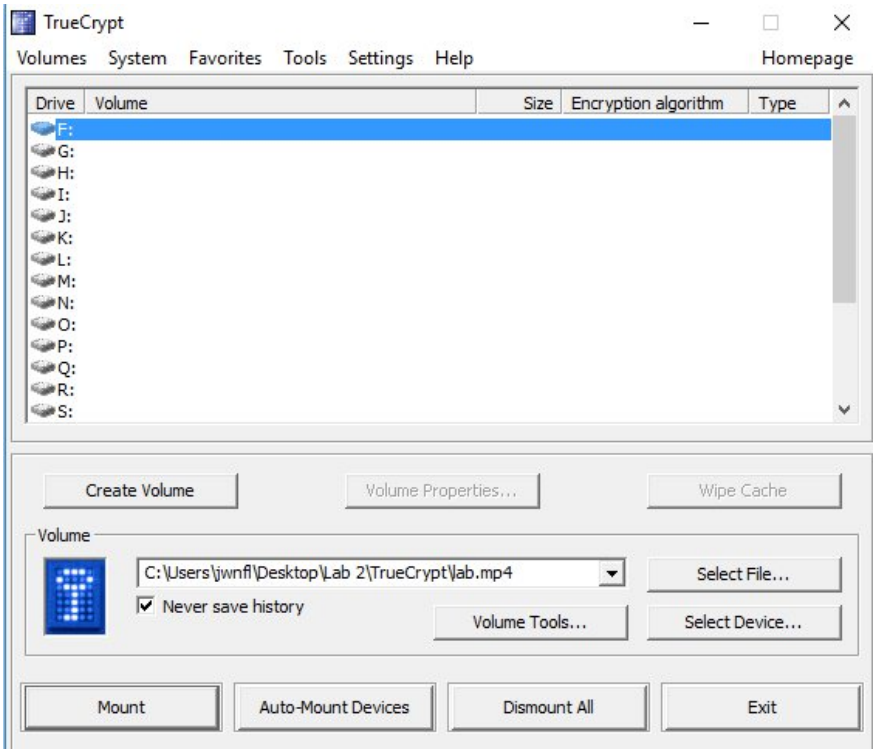


Figure 68 Dismounted Volume

Conclusion

During this experiment, there were many things that the examiner learned throughout the process. The sophistication of methods of hiding information regardless of the size can be hidden inside of pixels of an image. The color shifts are minimal however the human eye can't notice the difference. Using StegoAnalyst is the only method discovered throughout the experiment providing the examiner the tools required to discover the subtle modifications to the colors of the pixels of the images. Altering the image pixels in the manner displayed in the experiment provides the criminals an advantage of sending to their network gigabytes or more of information contained inside of an image.

Placing encrypted containers within video files is another method which can cause problems with law enforcement due to them unknowingly having information in their possession that they are not aware has more incriminating information within the files. However, if someone is suspected of containing images such as the files mentioned in the experiment, they can also investigate further through using other programs. One of the major hurdles for law enforcement is decrypting the containers. Today, if the individual has created a complex password, this creates a bigger problem.

While technology continues to evolve, the methods of the criminals also become more sophisticated. Entities that deal with digital forensics need to be current with regard to training and the methods of the individuals committing the computer crimes. Digital forensics is still continuing to advance which will be a significant advantage to local, state, and federal law enforcement once the technology surpasses criminal methods.