Portfolio 2 -

Matthew Faller

26/02/24

Contents:

[Task1: File Signature Investigations 2](#_Toc159860736)

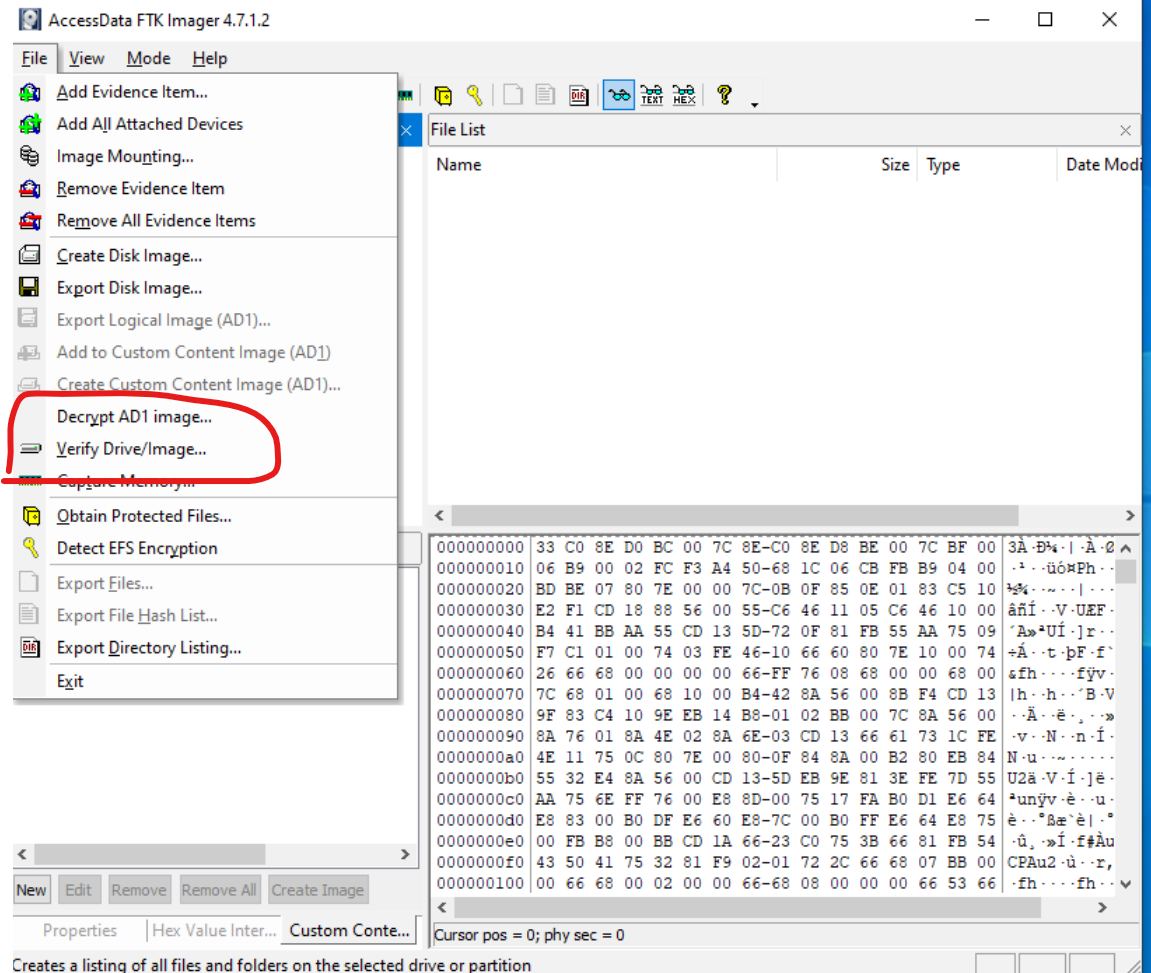
[Task 2: Analysing USB\_03.E01 Forensic Image with Autopsy 4](#_Toc159860737)

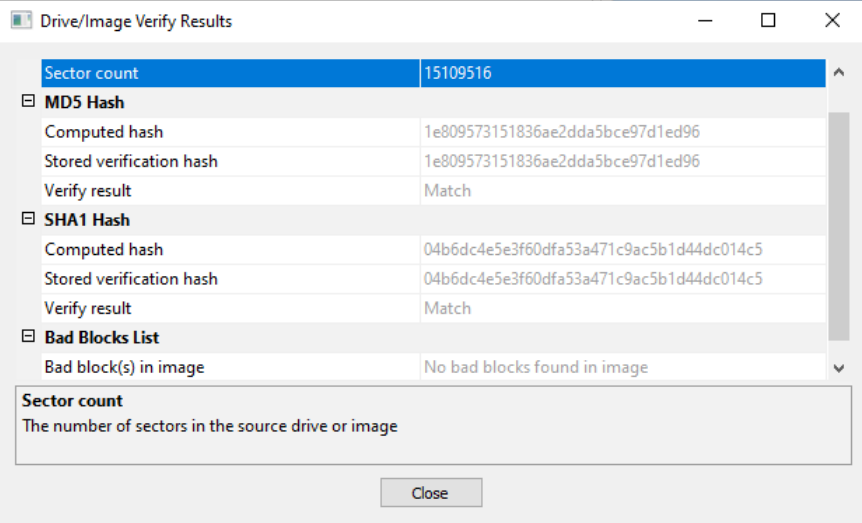
[Task 3: Analysing USB\_03.E01 Forensic Image 9](#_Toc159860738)

[Task 4: File structure investigation 12](#_Toc159860739)

# Task1: File Signature Investigations

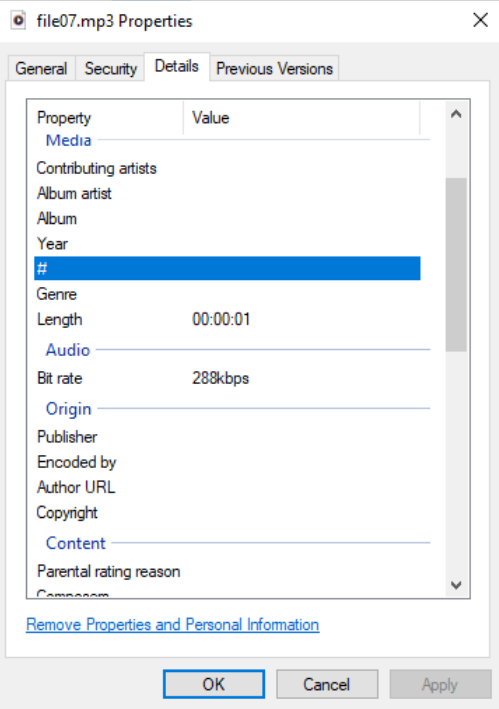
1. The screenshots show how you can confirm that the image hash downloaded matches the image hash of the original image





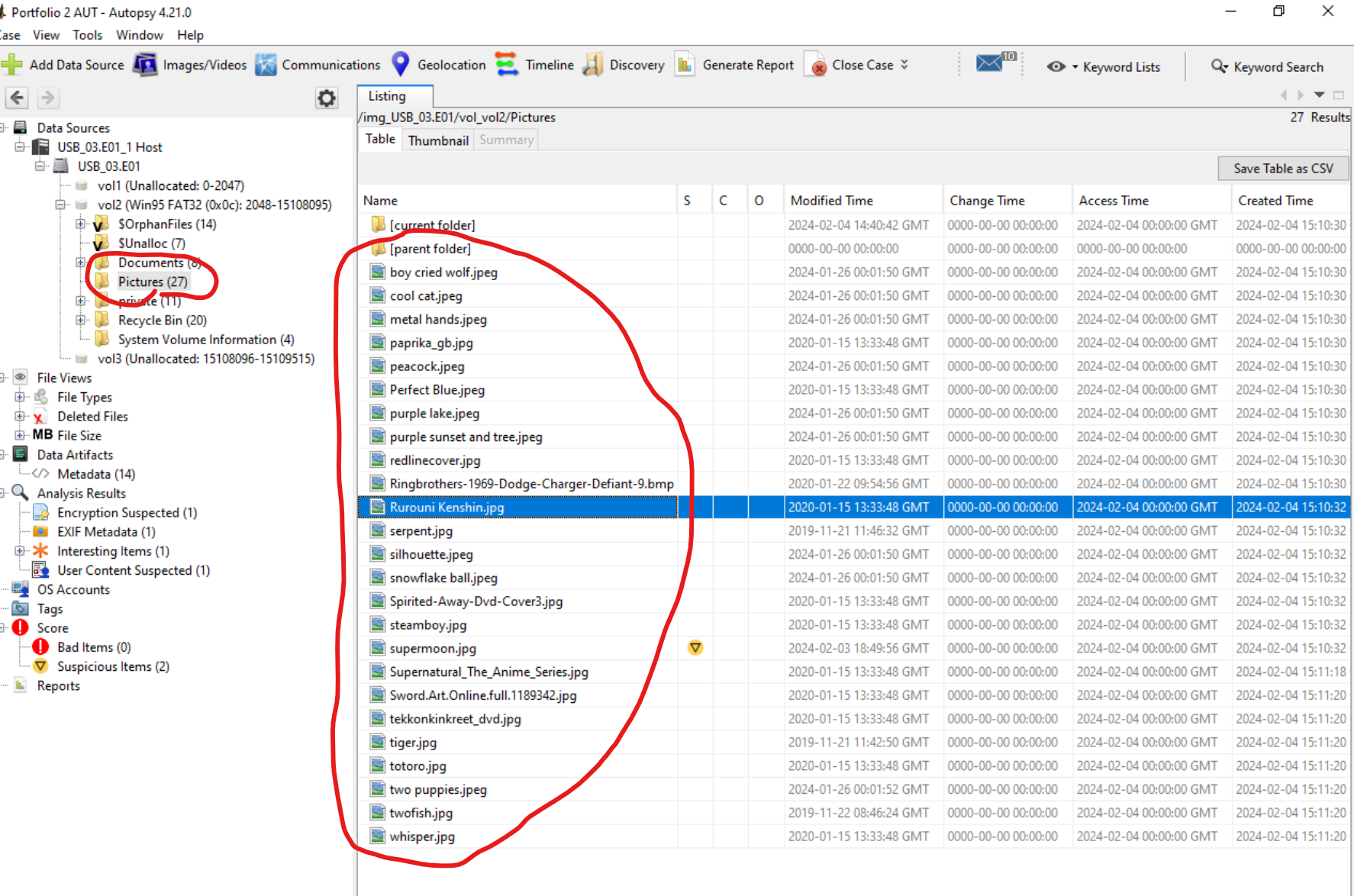
1. Below is the file extension of each file along with the file signature and sizes.

* File01 – Extension = PDF, Signature = 25 50 44 46, Size = 126 KB
* File02 – Extension = ZIP, Signature = 50 4B 03 04, Size = 13,214 KB
* File03 – Extension = TXT, Signature = No signature for a text file, Size = 3 KB
* File04 – Extension = HTML, Signature = 3C 21 44 4F 43 44 49 40, Size = 79 KB
* File05 – Extension = 7Zip, Signature = 37 7A BC AF 27 1C, Size = 1,643 KB
* File06 – Extension = GIF, Signature = 47 49 46 38 39 61, Size = 1,688 KB
* File07– Extension = MP3, Signature = FF FB, Size = 53 KB

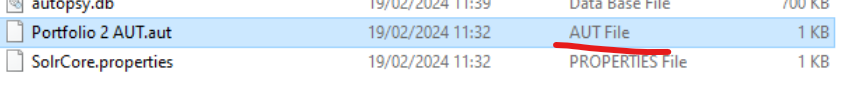
1. The first 3 bytes of file 7 are ‘FF FB 90’ the FF FB means that the file is an mp3 file and the 90 is just apart of the file.
2. To check the bit rate of file 7 I went into the properties of the file   
   
3. The bit rate binary setting is 288,000 bits per second. I found this by looking at the screenshot from the previous question

# Task 2: Analysing USB\_03.E01 Forensic Image with Autopsy

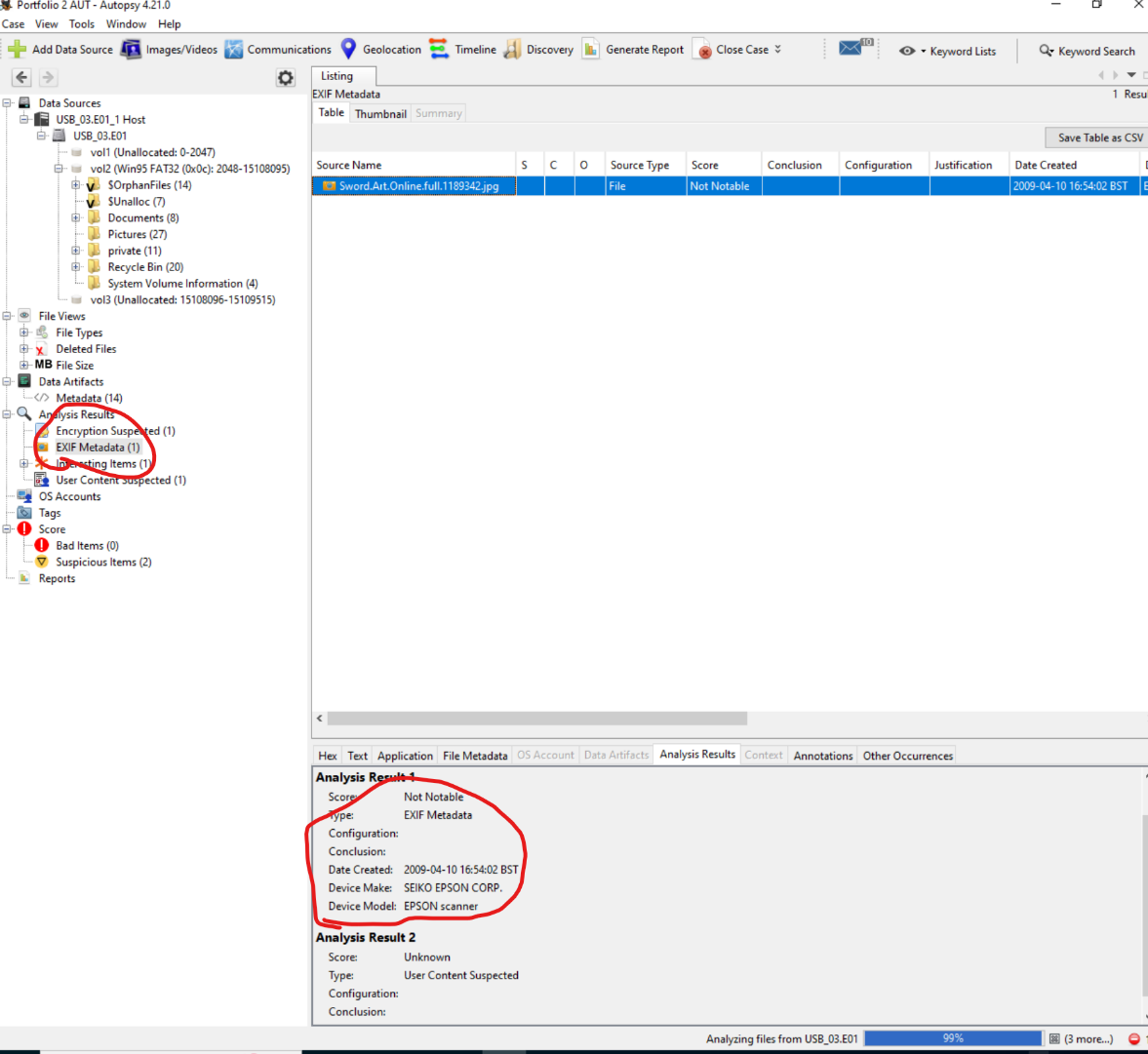
1. Autopsy claims to have found 27 .jpeg or .bmp image files alone with one suspicious image as you can see in the screenshot below



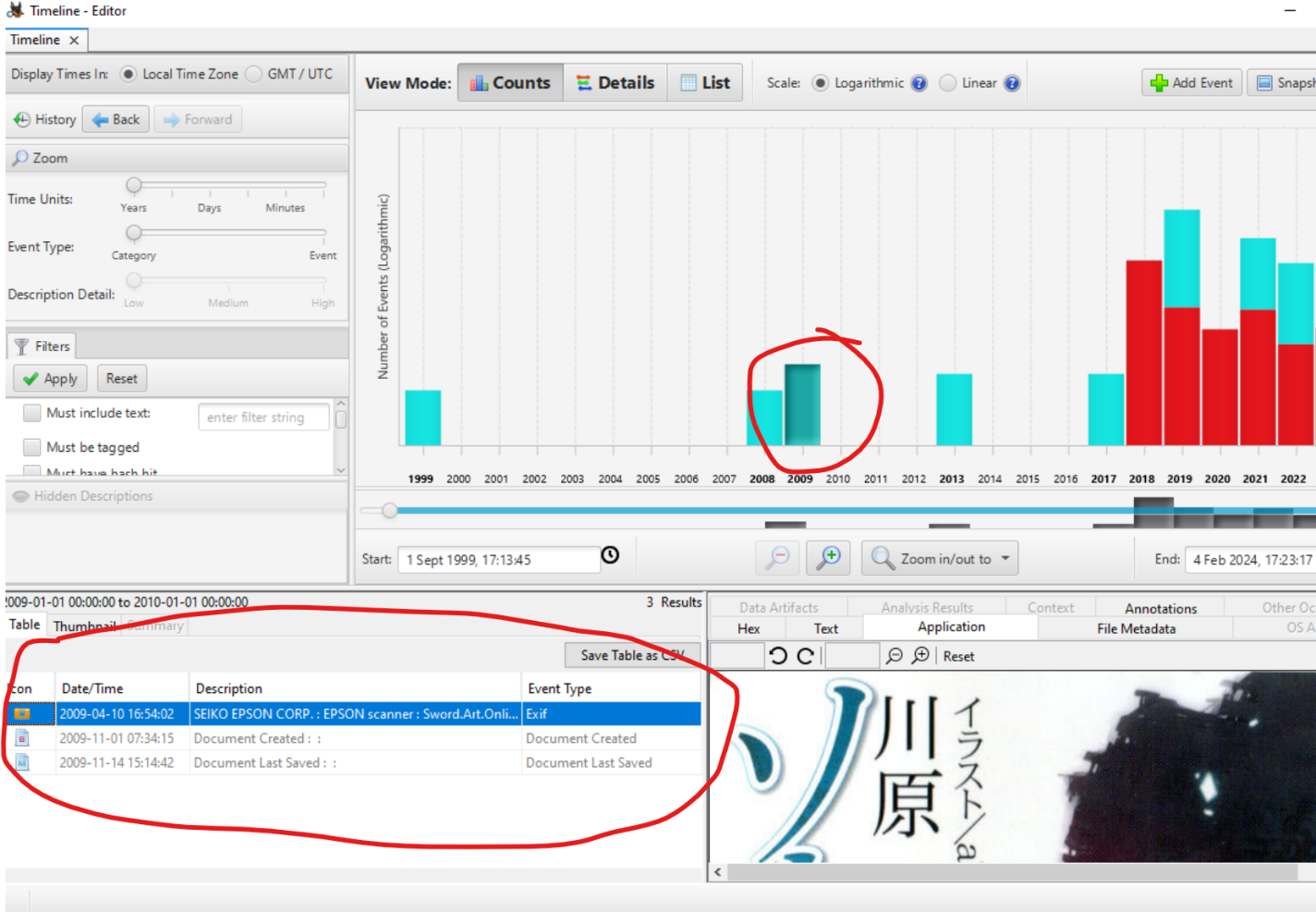
1. The file extension for autopsy case files is .aut which you can see in the screenshot

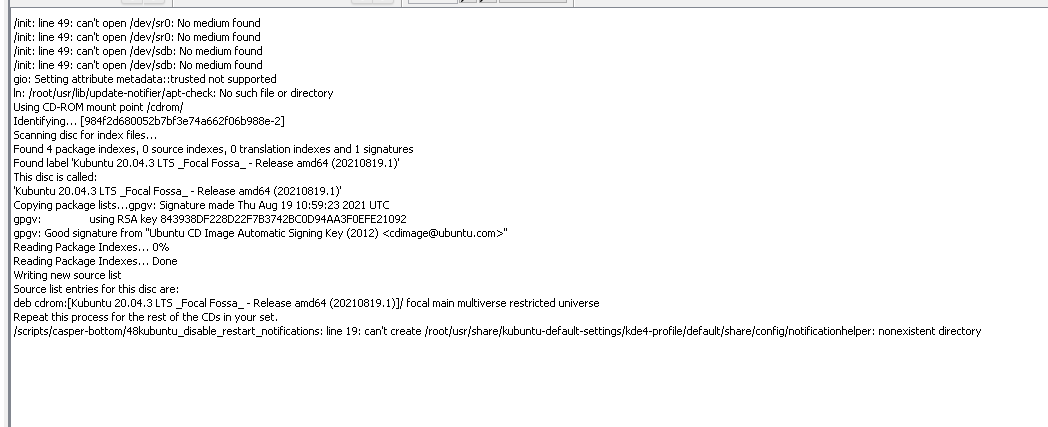
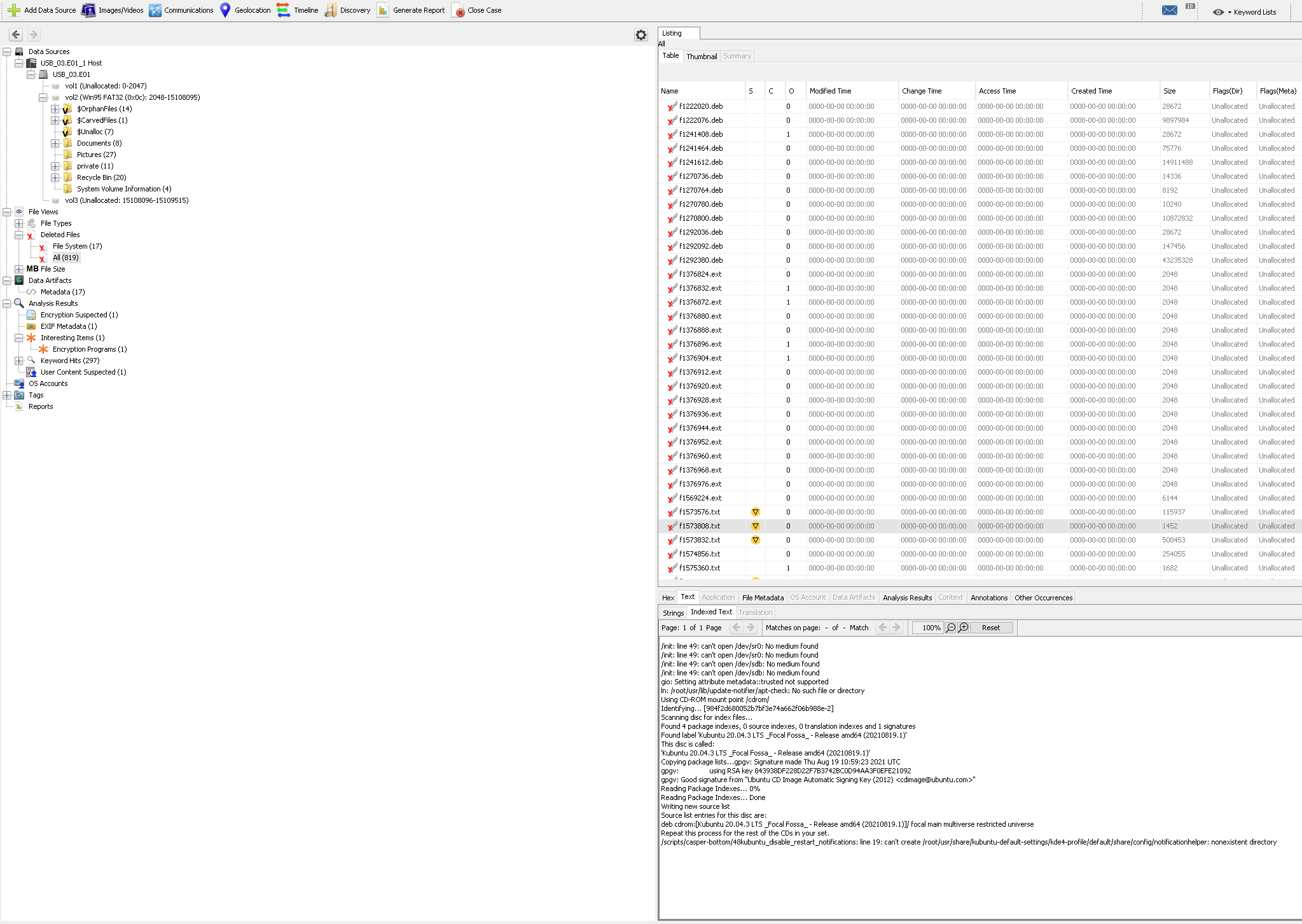


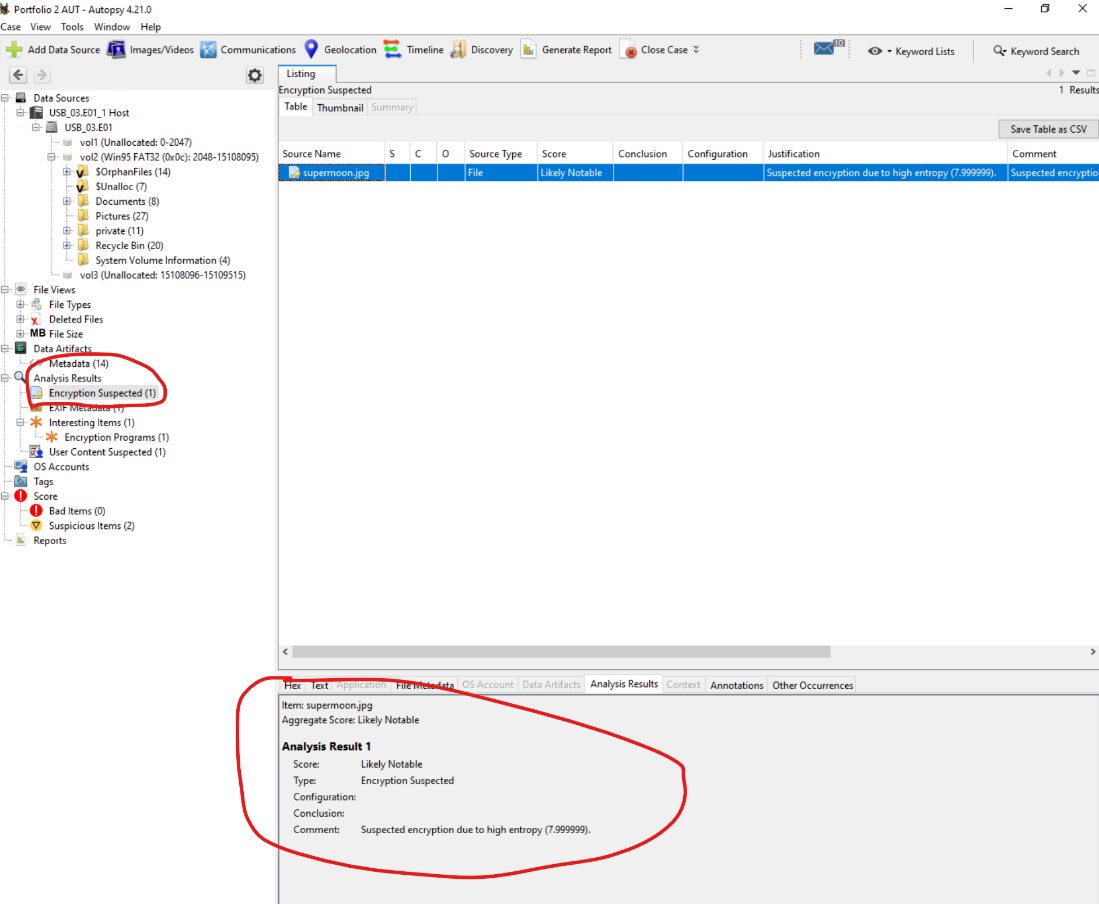
1. The device model for the jpeg file is shown below. I found the device model by looking at the EXIF metadata which contains the device model which is an EPSON scanner for this image.



1. There were 3 events in the year 2009 with a document being created and saved along with an EXIF event. I found the timeline by clicking the tools drop down menu and selecting timeline and it generated me a timeline of the number of events over the years



1. I found this file in the deleted files and it shows that there is a hidden linux system of kunbuntu 2019 
2. The possibly encrypted file is a file called supermoon.jpg as the file size is abnormally large for an image file compared to the others so it is likely that there is another file hidden inside



# Task 3: Analysing USB\_03.E01 Forensic Image

1. The file that got me into the VeraCrypt container ( container was stored in file supermoon.jpg ) was - Twofish\_encryption.pdf
2. The hash result from that file was - cbca79cfd838aaae8b21f3df724fde090de17cb276dd82d78adfb48d984a36ae
3. I found 3 files inside the container you can see their sizes and names in the screenshot below

A screenshot of a computer

Description automatically generated

1. There are 22 collectors in the income.xlsx fileA screenshot of a spreadsheet

   Description automatically generated
2. There are 8 movie titles in the second file as you can see in the screenshot below. I found this file by mounting the veracrypt container and then scanning it with autopsy to look inside the recycling bin and that’s where I found $RJKF6BP.xlsx along with some others.

A screenshot of a computer

Description automatically generated

1. Based on my investigation I can’t find any evidence of a crime committed in the image or the veracrypt contents.

# Task 4: File structure investigation

**47 49 46 38 39 61 0B 02 88 01 F5 00 00 70 70 70 50 50 50 22 22 22 A4 A4 A4 C3 C3 C3 CB CB CB D3 D3 D3 DB DB**

**Width:**

Bytes 18-21: 50 22 22 22 (in little-endian format)

50h = 80 dec

22h = 34 dec

80 \*34 \* 34 \* 34 = 3144320

After converting the hex to decimal = 3144320 pixels of width

**Height:**

Bytes 22-25: A4 A4 A4 C3 (in little-endian format)

A4h = 164 dec

C3 = 195 dec

164 \* 164 \* 164 \* 195 = 860134080

After converting the hex to decimal = 860134080 pixels of height