F20FO Lab 6

Imaging & Data Analysis

Chandrashekhar R (cr2007)

Contents

Lab 6.1: Hashing

Lab 6.1.1: Creating Hashes

Note the hashes and the filename

```
$ ./md5sum.sh
e72cad83bf69757f936d13d2055bcd3a  doc1.doc
99b8fb4f5836b07f974dd24530eb5f4d  doc2.doc
f80917e6587a040639b8c7a97009c6e1  doc3.doc
136903faf6ba51ae2361d9602d60a77d  doc4.doc
07ce25b776e7b7cf0b60fa6ec215bbb3  doc5.doc
28804e786cd28a70a777ff66019859bf  doc6.doc
07ce25b776e7b7cf0b60fa6ec215bbb3  doc7.doc
a2b132f425250972af1809819290b3ad  image1.jpg
4fd0247681673fcac997410b464eb9d0  image2.jpg
ccf34e7e1770f956166ac89e5af366aa  image3.jpg
9bafb511d5b8c5db01b071bdb5082f08  image4.jpg
```

Figure 1: A list of file hashes and the corresponding file names

---

Based on the above computer hashes, can you tell which of the files are exactly the same?

`doc5.doc` and **`doc7.doc`** contain the same computer hashes.

```
$ ./md5sum.sh
e72cad83bf69757f936d13d2055bcd3a  doc1.doc
99b8fb4f5836b07f974dd24530eb5f4d  doc2.doc
f80917e6587a040639b8c7a97009c6e1  doc3.doc
136903faf6ba51ae2361d9602d60a77d  doc4.doc
07ce25b776e7b7cf0b60fa6ec215bbb3  doc5.doc
28804e786cd28a70a777ff66019859bf  doc6.doc
07ce25b776e7b7cf0b60fa6ec215bbb3  doc7.doc
a2b132f425250972af1809819290b3ad  image1.jpg
4fd0247681673fcac997410b464eb9d0  image2.jpg
ccf34e7e1770f956166ac89e5af366aa  image3.jpg
9bafb511d5b8c5db01b071bdb5082f08  image4.jpg
a1e4283f69e0f65a423297dfc9c4d6fa  md5sum.sh
```

Figure 2: A list of file hashes with the same file hashes

Lab 6.1.2: Seeing the changes

Create a new text document.

In this file, type in "**Fundamentals of Digital Forensics AED 10.00**"

Save this file on your Desktop as **`price.txt`**, and close it.

Calculate the MD5 hash of this file.

Record this.

`e9ec0e0eaf23289e9e627586624e662b` | **price.txt**

Now make a copy of the file "**price.txt**" and call it "**copy of price.txt**". **DO NOT MODIFY** or **OPEN** this file.

Calculate the MD5 hash of this file.

Record this.

`e9ec0e0eaf23289e9e627586624e662b` | **copy of price.txt**

Now compare the hash values.

What can you learn from the hash of these two files? Why?

From the hash of these two values, we can learn that the contents within the 2 files are identical, since they produce the same MD5 hash.

Next, open the file price.txt you created earlier.

Change the statement "**Fundamentals of Digital Forensics AED 10.00**" to "**Fundamentals of Information Security AED 1000**"

Save the file (over-write it)

Just as before, calculate the hash of this edited file.

Compare the hash values to the ones you found before.

What can you see and why?

```
$ md5sum price.txt && md5sum "copy of price.txt"
3aa2d07bd2f61721b130d79b551dbfaf  price.txt
e9ec0e0eaf23289e9e627586624e662b  copy of price.txt
```

We can see the hash values for both the files changed. This is because both the `.txt` files have different values within them.

Lab 6.2: Digital Forensic Imaging and Analysis

Lab 6.2.1: Autopsy

What is the MD5 hash for the "Murder.E01 image?"

`e2c63db524627af7fdad7d7d4b7339e7`

Identify Device ID and the timeZone:

Device ID: `bf759dd7-22ff-40a4-9fdf-6b31fc52aade`

timeZone: Asia/Dubai

Click on Murder.E01, to expand it. What does the red X mean beside the Documents folder?

The red X indicates that the file was either deleted or unallocated. Autopsy highlights these files with a red cross to draw attention to them using forensic analysis.

What sort of evidence can you identify for Murder.EO1 by using Autopsy? Report your findings.

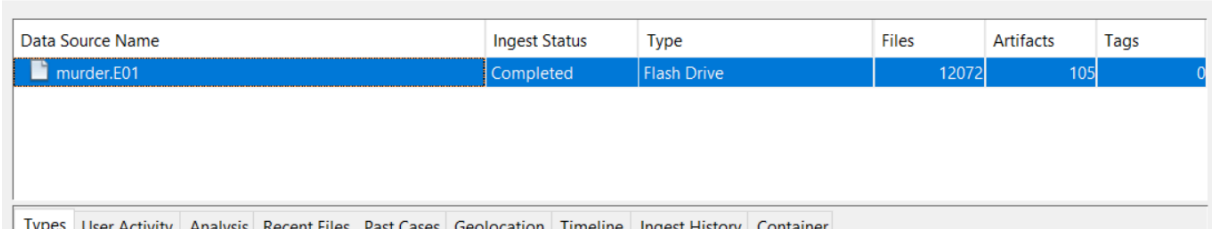
(Hint: Click on Murder.E01 look inside Documents, any related images or Documents. Also look at the visited sites). Record metadata details related to the evidence you found including MD5 hash for each evidence file.

Using Autopsy, many elements are revealed in the case of Murder.E01, including File Metadata, Deleted Files, File Hashes and Signatures, and Timeline Analysis. Examining the data, it's evident that the suspect engaged in frequent visits to online gun forums, conducted searches on shotgun operation, and accessed instructional materials aimed at novice gun users. Notably, an RTF file indicates the suspect booked a room on October 24, 2010, coinciding with the date of the murder. These findings strongly implicate the suspect as the perpetrator of the crime.

Lab 6.2.2.: FTK (Forensic ToolKit

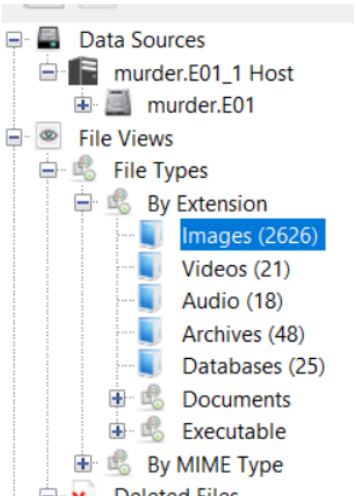
What is the total number of files processed in this evidence file (Murder.E01) by FTK?

After extracting the files from the evidence file, it shows that there are **12,072** files processed in this evidence file.



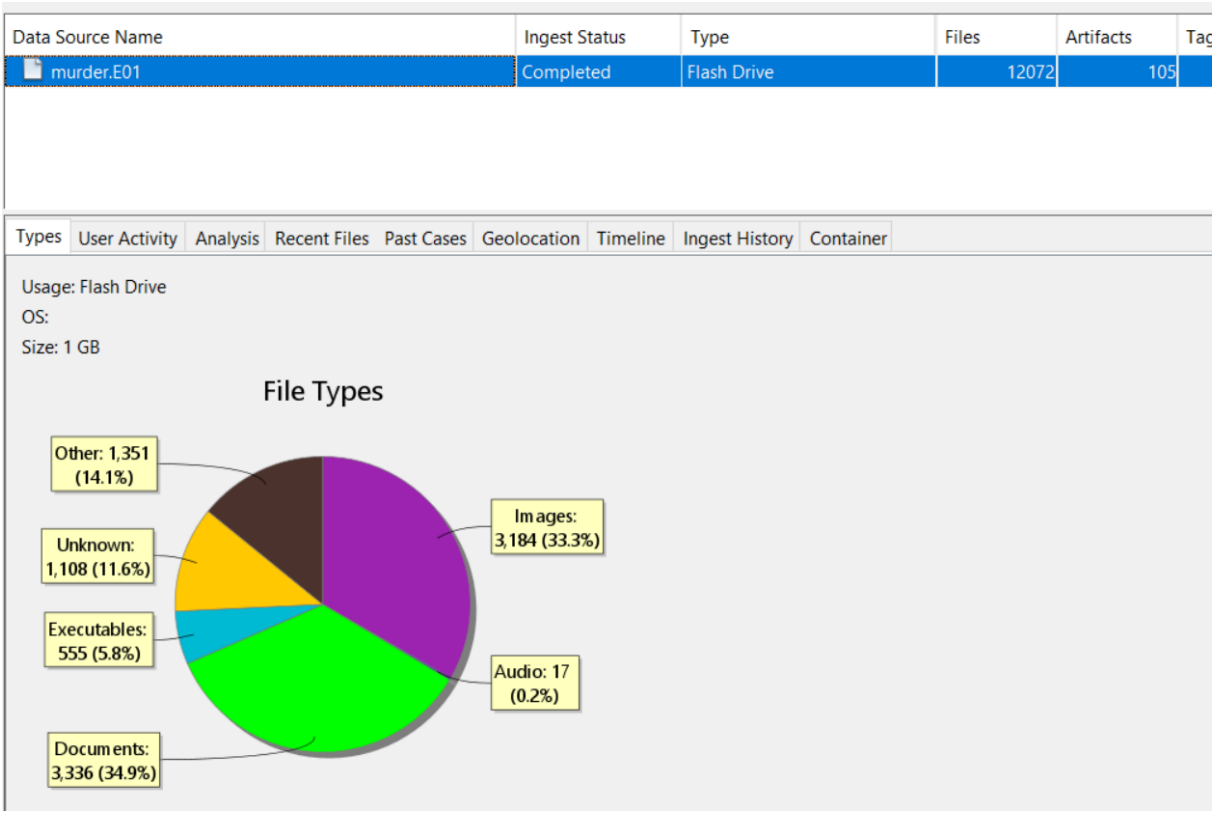
How many deleted files?

There are **6,115** deleted files in the evidence file.



How many graphic files?

There are **3,184** graphic files in the evidence file.



MAC Times

Do you notice anything? Do some of the graphics files have their modified date before creation and accessed dates? If yes, why do you think that happened? If all the dates correspond, you can write no as an answer.

Analysis of the suspect's accessed dates reveals manipulation. Examination of MAC times for recent graphic files indicates discrepancies, with access dates consistently set to one day prior to creation

and modification dates. Notably, the access time for these files consistently appears as 13:00, implying deliberate tampering by the suspect to conceal their activities.
