

Introduction to Autopsy

Introduction

In this practical you will use Autopsy to examine a case

By the end of this lab you will be able to

- Use the basic functionalities within the Autopsy environment
- Use Autopsy to find various Windows artefacts

Autopsy can be downloaded from <https://www.autopsy.com/download/>

Task 1: Introduction to Autopsy

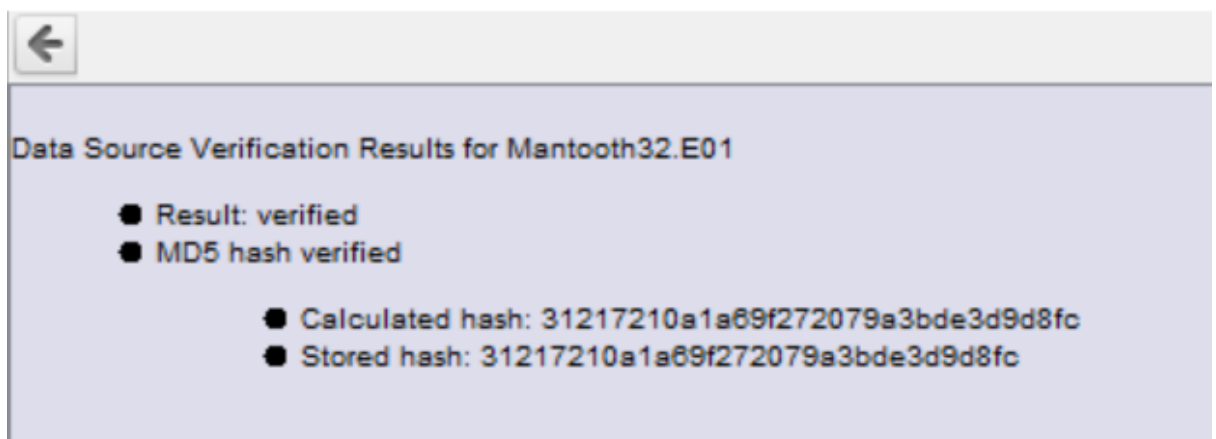
Scenario:

Wes Mantooth was found to be in possession of fraudulent checks. When Mantooth was questioned he stated that he had obtained the checks from an associate of his. Mantooth refused to give any further details to the people questioning him about his accomplice or accomplices were. When asked how Mantooth created the checks he said: "With a computer, you figure the rest out". Since Mantooth was living in Phoenix, his computer may be set to Mountain Time.

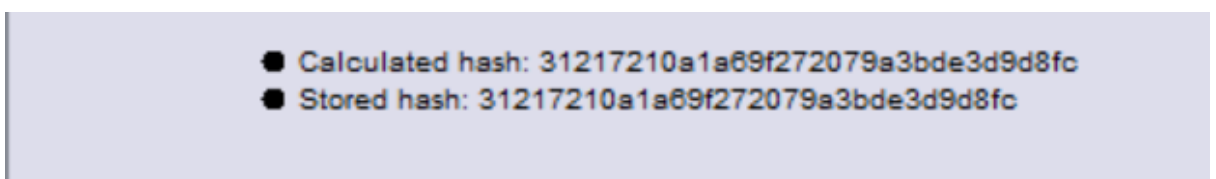
Create a new case by using the Mantooth.E01 image and answer the following questions

Gather basic information about the Image

1. Verify the image first; Via the "Data Source Integrity" module



2. What is the MD5 hash of the Mantooth image?



- Find additional information regarding the image, including sector size, total sector count, etc

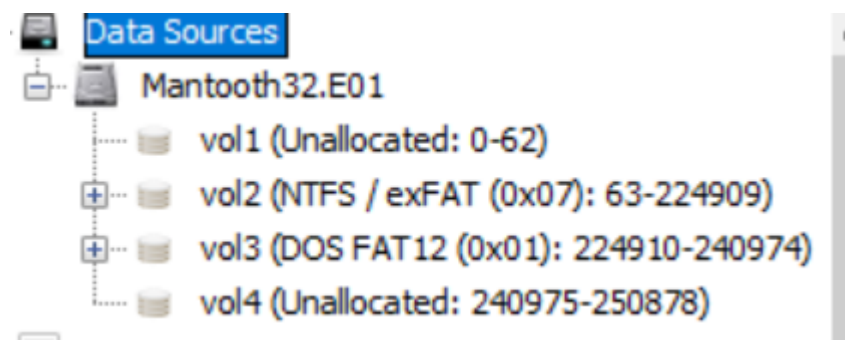
Data Sources						
Table Thumbnail						
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID	
Mantooth32.E01	Image	128450048	512	Europe/London	a8805c4c-e655-4ff7-8e28-d45096b4b7d4	

- How many partitions are on the evidence image and what are they?

```

0x00000180: 00 00 00 8B FC 1E 57 8B FS CB 00 00 00 00 00 00 .....W.....
0x00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000001a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000001b0: 00 00 00 00 00 00 00 00 34 28 9A 3B 00 00 80 01 .....4(.?....
0x000001c0: 01 00 07 FE 3F 0D 3F 00 00 00 4F 6E 03 00 00 00 ....?.?.On....
0x000001d0: 01 0E 01 FE 3F 0E 8E 6E 03 00 C1 3E 00 00 00 00 ....?.n...>...
0x000001e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000001f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA .....U.....

```

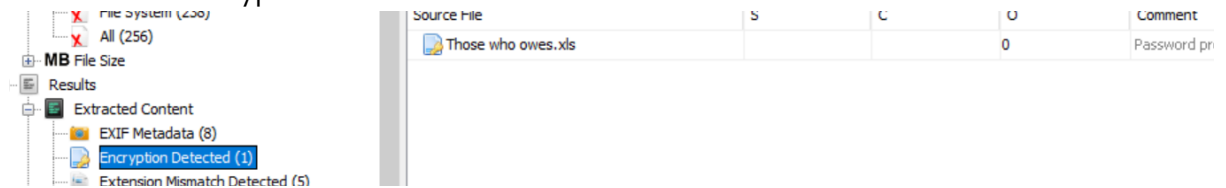


- Change the time zone to "Mountain time"

- Which photo was taken by an Olympus Optical device? add it to the bookmark

Extracted Content							
EXIF Metadata (8)	Autumn Leaves.jpg	0	2005-11-04 10:12:05 MST				Mantooth32.E01
Encryption Detected (1)	Dock.jpg	0	2005-06-22 13:17:19 MDT				Mantooth32.E01
Extension Mismatch Detected (5)	Humpback Whale.jpg	0	2005-11-30 06:20:37 MST				Mantooth32.E01
Operating System User Account (5)	Toco Toucan.jpg	0	2005-06-24 05:22:26 MDT				Mantooth32.E01
Recent Documents (86)	forsale.jpg	0	2005-11-14 04:10:56 MST	C730UZ	OLYMPUS OPTICAL CO.,LTD		Mantooth32.E01
Remote Drive (1)							
Web Cookies (50)							

7. Which file is encrypted?



8. What happened to HARDCOE.jpg and pfah603.jpg files?
they are ADS files

9. Go through the web search history; what are the three main search topics? which user performed the search?
check washing
atm card stealing
making meth

User Wes Mnatooth

10. list three IP addresses that can be found within the image
keyword lists -> IP addresses
24.8.181.100
65.54.246.207
66.196.96.95

11. list three email addresses from the given image
doolarhyde86@comcast.net
chkwasher@concast.net
skimmerman27@hotmail.com

12. go through various functions, including images/videos, timeline, and generate report.

Once you are familiar with the Autopsy Interface and its basic functionalities. Find evidences that are related to production of fraudulent check and accomplice of Mantooth