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:

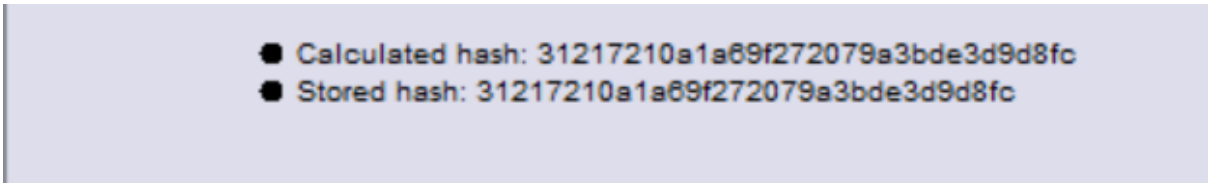
Wes Mantooth was found to be in possession of fraudulent checks. When Mantooth was questioned he stated that he had obtained the checks from an associate of his. Mantooth refused to give any further details to the people questioning him about his accomplice or accomplices were. When asked how Mantooth 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

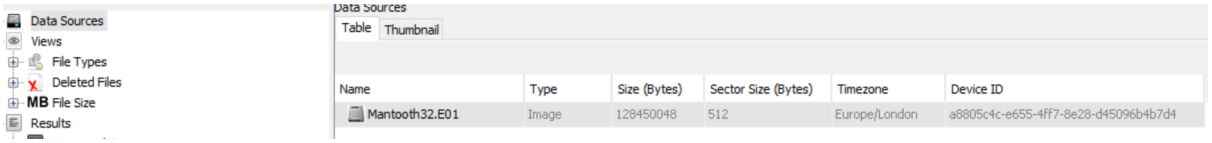
Gather basic information about the Image

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

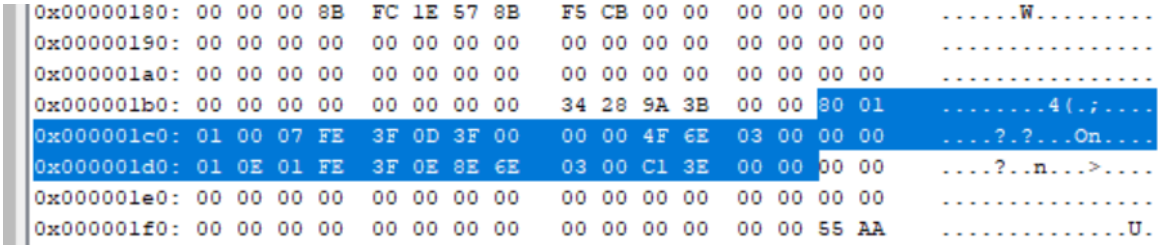
2. What is the MD5 hash of the Mantooth image?

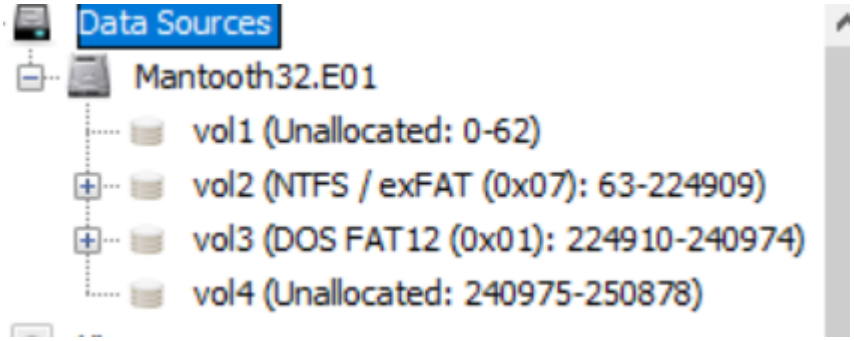


3. Find additional information regarding the image, including sector size, total sector count, etc

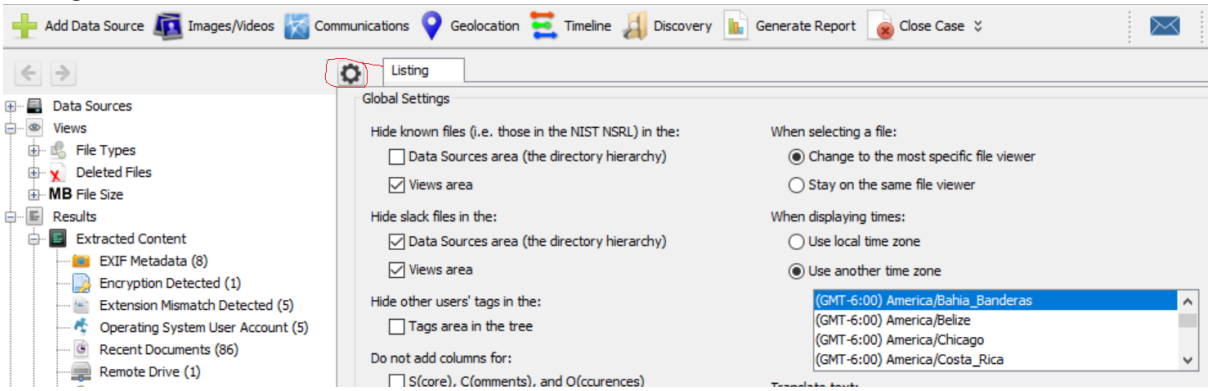


4. How many partitions are on the evidence image and what are they?

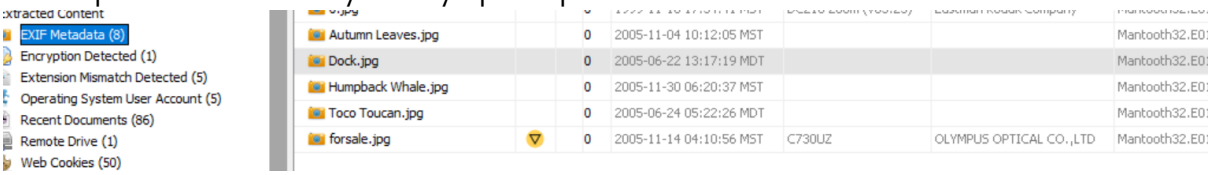




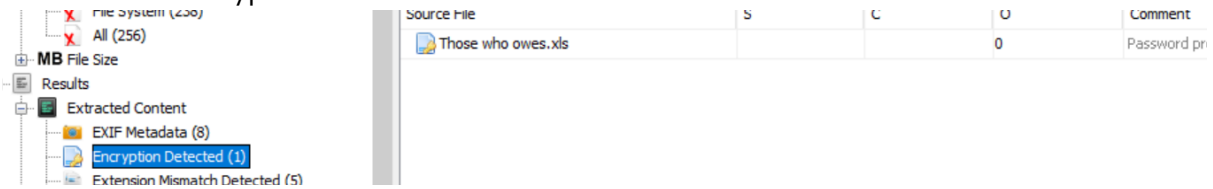
5. Change the time zone to "Mountain time"



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



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