Hands On Lab: Unit 13

MICS-252, Fall 2024

Digital Forensics II

Image Analysis

Prepared by: Karl-Johan Westhoff

email: kjwesthoff@berkeley.edu

UC Berkeley School of Information

MICS Course 252 Fall 2024 (Kristy Westphal)

1 Introduction

We are given an Encase .E01 image: "Windows Image.E01" with a size of 10.6 GB. The image was ingested into Autopsy version 4.21. We are given the following objectives for the exercise, to get tour around the disc image.

1.1 Objectives

Attempt to answer the following questions:

- What time zone is the image set in?
- What Operating System is the suspect drive using?
- What event happened on January 1, 1980?
- What is the IP address of the suspect drive?
- What is the EvenMoreSecretStuff.vhd (and can you see what is in it?)
- Do any of the suspicious items discovered look suspicious to you?
- Anything else that you found that you want to highlight?

2 Image Ingestion

The file name indicates that the file is a Windows pc image.

3 Conclusion

Appendices