

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 (a lengthy process). Some of the ingress modules do not run under Linux, these include "Yara" (runs rules checking files for malware) and "Plaso" which extracts information from the windows registry of the image.

1.1 Objectives

We are given the following objectives for the exercise, to get thoroughly around the disc image: "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?

1.2 Autopsy report

Autopsy has functionality to generate a report of the findings in various formats. I have published the report on github pages for reference in this report as:

- [1]: <https://kjwesthoff.github.io/252-Lab13-AutopsyReport/>

2 Image Ingestion

The file name indicates that the file is a Windows pc image. The image was subjected to the ingest modules from the default Autopsy 4.21 installation (See Case Summary section of [1]). The execution of various ingestion modules was a lengthy process (>24hrs. in this case). Autopsy can include custom ingestion modules that analyse the file hashes against known malware, in this case hashes were generated for all files (hence the lengthy ingest) and are thus ready for comparison against a database of known hashes (considered out of scope for this assignment). Luckily most of Autopsy's functionality is available while it analyzes the files, and various result sections are populated in the GUI as they become available.

3 Analysis Results

The Image holds two data sources; Windows Image.E01 and EvenMoreSecretStuff.vhd, the .vhd extension indicates that it is a Windows Virtual Hard Disc [2]

3.1 Assignment Objectives Results

Time Zone Both data sources indicate: "America/Los Angeles", and the images were acquired on Mar. 20, 2019 in the evening around 8pm, see Appendix A

Operating System Both the .E01 file name, the .vhd part and various artifacts indicate a Windows OS, the Autopsy report [1] indicated:

- OS: "Windows 10 Enterprise"
- product ID "00329-00000-00003-AA856"
- built for: "AMD64 architecture"
- with the business like computer name: "DESKTOP-0QT8017"

Event on January 1, 1980: January 1 1980 at midnight is the epoch (beginning of time) for MS-DOS¹. For unix systems it is January 1. 1970 (of course Microsoft had to have their own epoch). When computers get confused or are missing a time stamp they default to epoch. In this case it is apparently some google chrome files that is causing some confusion, see Appendix B

IP of "Suspect Drive" It appears that the machine was on a local network with IP address 10.0.1.5, when searching for IPv4 addresses it shows up second most after 6.0.0.0 (which I think is not an ip address in this context, but associated with version of "Microsoft-Windows-ServicingStack"), see Appendix D. The ip 10.0.1.5 shows up in files also containing the amd64 CPU architecture.

EvenMoreSecretStuff.vhd The .vhd extension suggests it is a "Virtual Hard Disc", the format is related to Microsoft Windows² and is used to host a separate hard drive on the file system with features such as its own partitions, file system etc. but, the .vhd files 'live' in a file on the host operating system [4]. The .vhd format is used when hosting a virtual machine on a windows pc. Autopsy identified it as an NTFS file system, accessing it shows "un-allocated Blocks" and it seems to be encrypted (Autopsy identified that "vol 2" is as encrypted using bitlocker), see Appendix C.

Do any of the suspicious items discovered look suspicious?

Other Suspicious Things I think the recent download (via chrome) and subsequent installation of teamviewer looks suspicious, it is often used by scammers to take control of a victims computer.

4 Conclusion

¹ I was about to write that it was when "Skynet became self-aware" but that was August 29, 1997 [3]

² Microsoft have released a specification and promised not to change it so others also can use the .vhd format [4]

References

- [1] Autopsy v 4.21. *Auto-generated report of Windows Image*. <https://kjwesthoff.github.io/252-Lab13-AutopsyReport/>. [Generated and published 27-November-2024]. 2024.
- [2] learn.microsoft.com. *Manage Virtual Hard Disks (VHD)*. <https://learn.microsoft.com/en-us/windows-server/storage/disk-management/manage-virtual-hard-disks>. [Online, accessed 27-November-2024]. 2024.
- [3] Wikipedia contributors. *Skynet (Terminator)* — *Wikipedia, The Free Encyclopedia*. [https://en.wikipedia.org/w/index.php?title=Skynet_\(Terminator\)&oldid=1259669280](https://en.wikipedia.org/w/index.php?title=Skynet_(Terminator)&oldid=1259669280). [Online; accessed 27-November-2024]. 2024.
- [4] Wikipedia contributors. *VHD (file format)* — *Wikipedia, The Free Encyclopedia*. [https://en.wikipedia.org/w/index.php?title=VHD_\(file_format\)&oldid=1249771178](https://en.wikipedia.org/w/index.php?title=VHD_(file_format)&oldid=1249771178). [Online; accessed 28-November-2024]. 2024.

Appendices

A Image MetaData

Data Content	
Hex	Text
Application	File Metadata
OS Account	Data Artifacts
Metadata	
Name:	/img_Windows Image.E01
Type:	E01
Size:	53687091200
MD5:	c0d0eaf2c981cd247bf600b46e6487c3
SHA1:	a20c2f43a80ddcad35b958b701a6cdd4b67e535c
SHA-256:	Not calculated
Sector Size:	512
Time Zone:	America/Los_Angeles
Acquisition Details:	Description: Desktop
:	Case Number: MUS-CTF
:	Examiner Name: Powers
:	Acquired Date: Wed Mar 20 21:29:33 2019
:	System Date: Wed Mar 20 21:29:33 2019
:	Acquiry Operating System: Win 201x
:	Acquiry Software Version: ADI3.1.1.8
Device ID:	5285eca3-ba0b-40c5-8b2d-f00352e13c85
Internal ID:	1
Local Path:	/home/kj/Desktop/Lab12/img/Windows Image.E01

Figure 1: Meta data for the Windows image.E01 Data source

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Metadata									
Name:	/img_EvenMoreSecretStuff.vhd								
Type:	VHD								
Size:	5368709120								
MD5:	7adc399e0930127d8cb2b7884ff2526b								
SHA1:	9e35ed1a3b7424401a18530372dce545137ced05								
SHA-256:	08768181eb8a031e24fb04fb88814471070ccd7fac036a19c5d50cc42d6247d6								
Sector Size:	512								
Time Zone:	America/Los_Angeles								
Acquisition Details:	Unknown								
Device ID:	5285eca3-ba0b-40c5-8b2d-f00352e13c85								
Internal ID:	465654								
Local Path:	/home/kj/Documents/Courses/MICS/252 SecOps/Assignments/HandsOnLab12/analyses/Lab13/ModuleOutput/Virtual Machine Extractor/Windows Image.E01_1_2024_11_25_21_24_29/1/EvenMoreSecretStuff.vhd								

Figure 2: Meta data for the "EvenMoreSecretStuff" Data source

B January 1. 1980

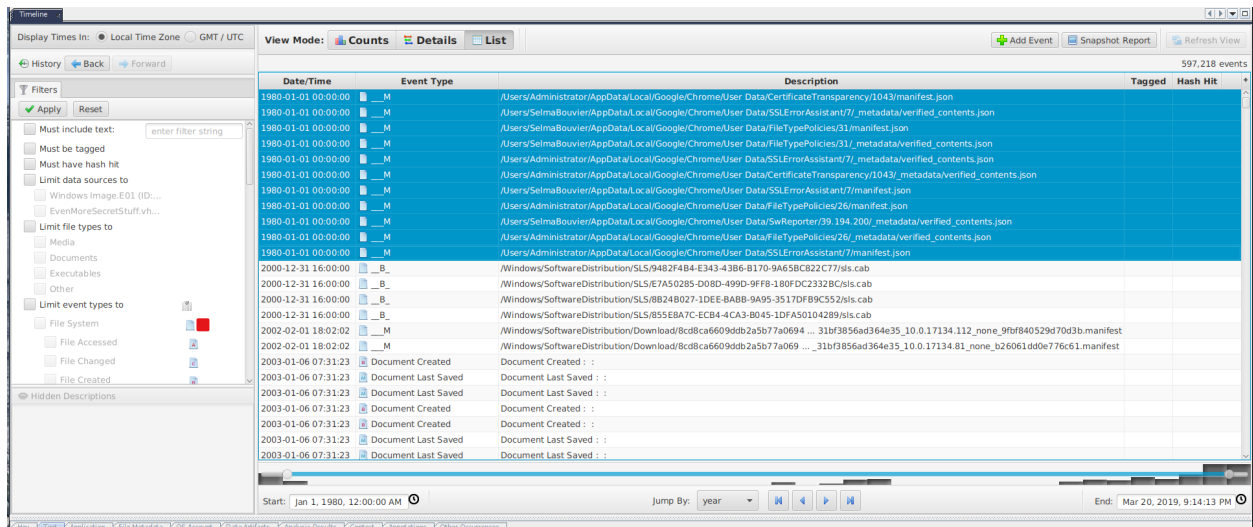


Figure 3: Timeline results for January 1. 1980

C VHD file encrypted

The screenshot shows the Autopsy 4.21.0 interface. On the left, the 'Data Sources' tree shows the 'EvenMoreSecretStuff.vhd' file. The 'Analysis Results' pane on the right shows 'Encryption Detected (1)' under 'Data Artifacts'. The 'Encryption Detected' table lists the following entry:

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment
vol2				Volume	Notable			Bitlocker encryption detected	Bitlocker encryption detected

The 'Strings' pane at the bottom shows 'Comment : Bitlocker encryption detected'.

Figure 4: The "EvenMoreSecretStuff" virtual drive, seems encrypted using bitlocker

D IP Hits

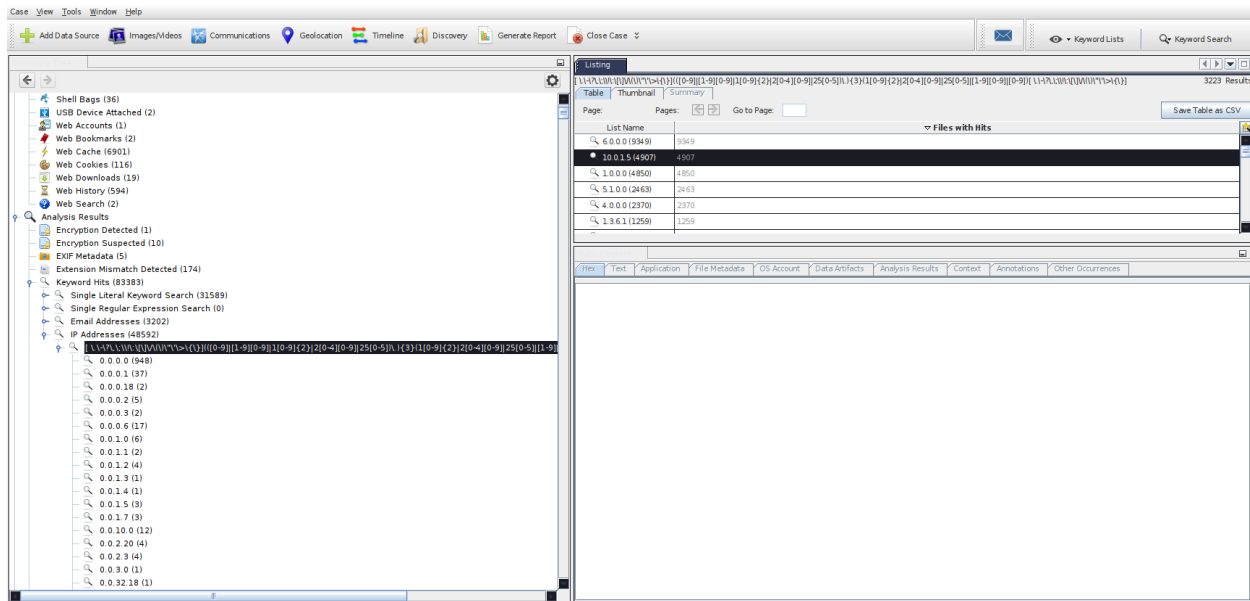


Figure 5: Hits searching for ip v.4 addresses, the 6.0.0.0 hit is associated with the version of a windows subsystem and it not an IP in this context