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). of the image.

1.1 Objectives

We are given the following objective 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 here:

- [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). 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. 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

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-DOS[1]. For unix systems it is January 1. 1970 (of course Microsoft had to have their own epoch). When computers

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

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" I found this a bit difficult, first tactics was to regex search for all IPv4-like numbers on the image and sort them by occurrence. The idea being that the host would receive an IP on the same subnet and that this would be logged in many places. The IP address 10.0.1.5, shows up second most after 6.0.0.0 (This is not an ip address, but associated with version of "Microsoft-Windows-ServicingStack"), see Appendix D, figure 7. However, after talking about it with peers from the class, another approach was to search for DHCP allocations of IP's to the host, This proved un-conclusive on my analysis, but an OSInt search of the internet recommended to look at the reports generated by Autopsy using "Regripper", and the information is found under "/Windows/System32/config/SYSTEM" which holds information of the NIC[2] at the time of image capture.

The IP is: 64.44.141.76, see figure 1

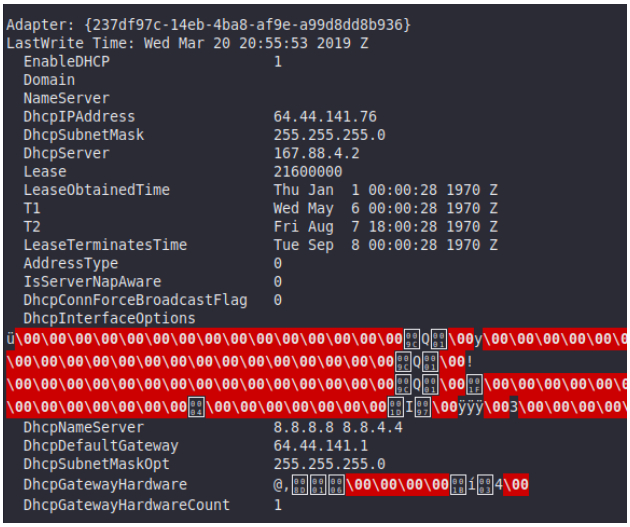

Figure 1: *Host IP at time of image capture, found in the network card information of the Windows registry obtained in Autopsy by the "Regripper" module*

EvenMoreSecretStuff.vhd The .vhd extension suggests it is a "Virtual Hard Disc", the format is related to Microsoft Windows[3] 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.

[2] Network Interface Card (from back when it was a self contained hardware)
[3] Microsof have relased a specification and promised not to change it so others also can use the .vhd format [4]

Do any of the suspicious items discovered look suspicious? Selma Bouvier[4] Has a link to some virtual hard discs (.vhd) on her desktop with "Super Secret" in the filename one of them flagged by Autopsy see Figure 2, the file is empty, the other file is the encrypted MoreSecretStuff.vhd previously found by Autopsy.

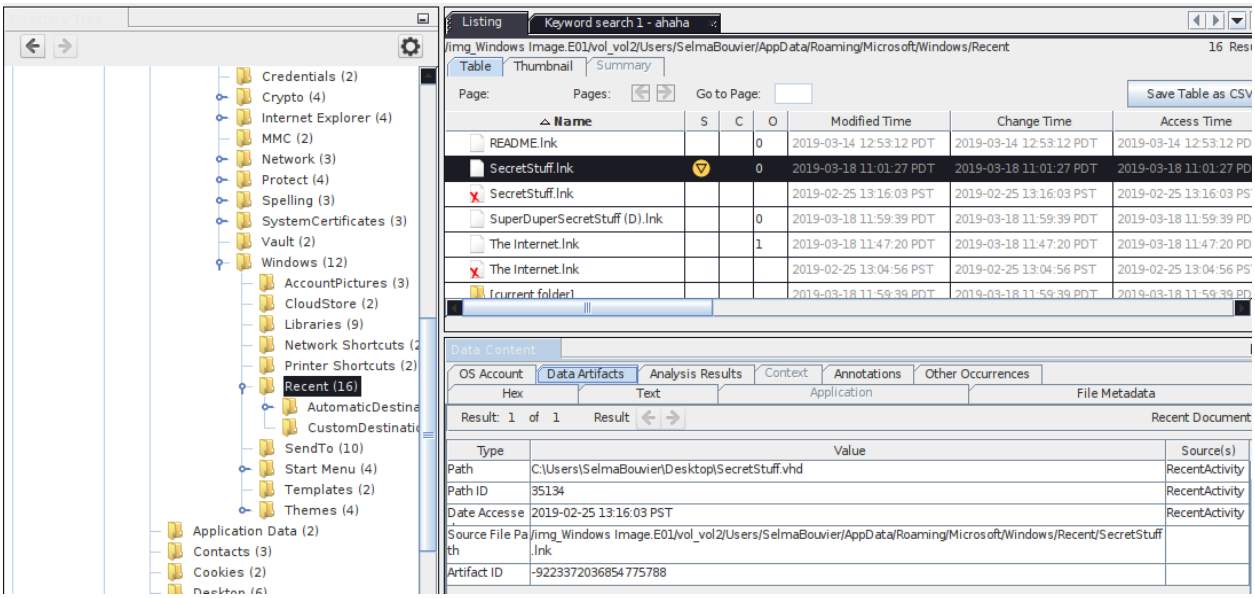

Figure 2: *The "Selma Bouvier" user has some interesting things on her desktop*

Poking some more Around Selma Bouvier's data revals a Readme.txt with a link to a Simpsons episode, where Homer gets hod of an "auto dialer" ST-5000. An .exe file named ST-5000 is also present in the profile's OneDrive under "Magnetic4nsics" I think she has been up to some auto dialing scam.

Other Suspicious Things I think the recent download (via chrome) and subsequent installation and execution of teamviewer in February and March of 2019 looks suspicious, see details in Appendix E TeamViewer is often used by scammers to take control of a victims computer.

4 Conclusion

The disc image was ingested and analyzed using Autopsy, Ingestion is a lengthy process depending on which Autopsy analysis modules are run on the image. In general the exercise gave a good tour of Autopsy.

[4] One of Marge Simpsons chain smoking sisters

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`. [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`. [Online; accessed 28-November-2024]. 2024.

Appendices

A Image MetaData

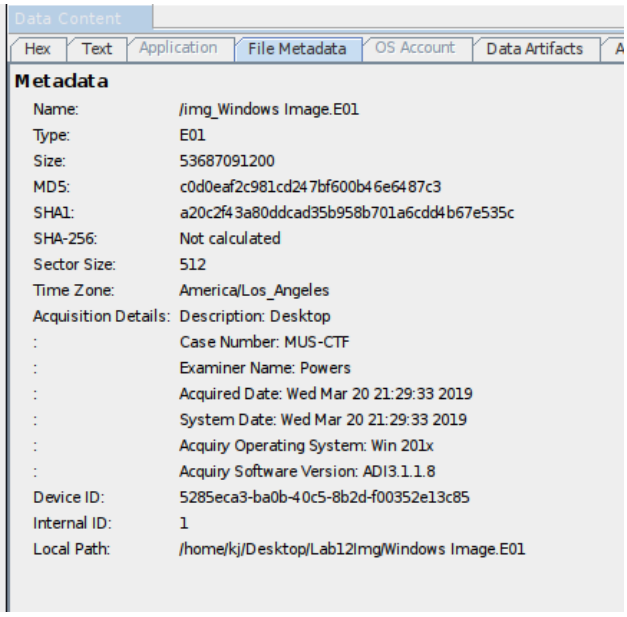

Figure 3: *Meta data for the Windows image.E01 Data source*

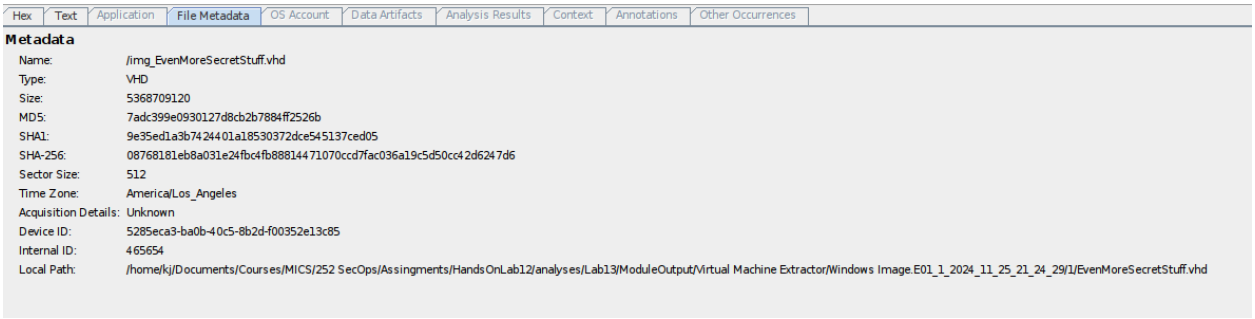

Figure 4: *Meta data for the "EvenMoreSecretStuff" Data source*

B January 1. 1980

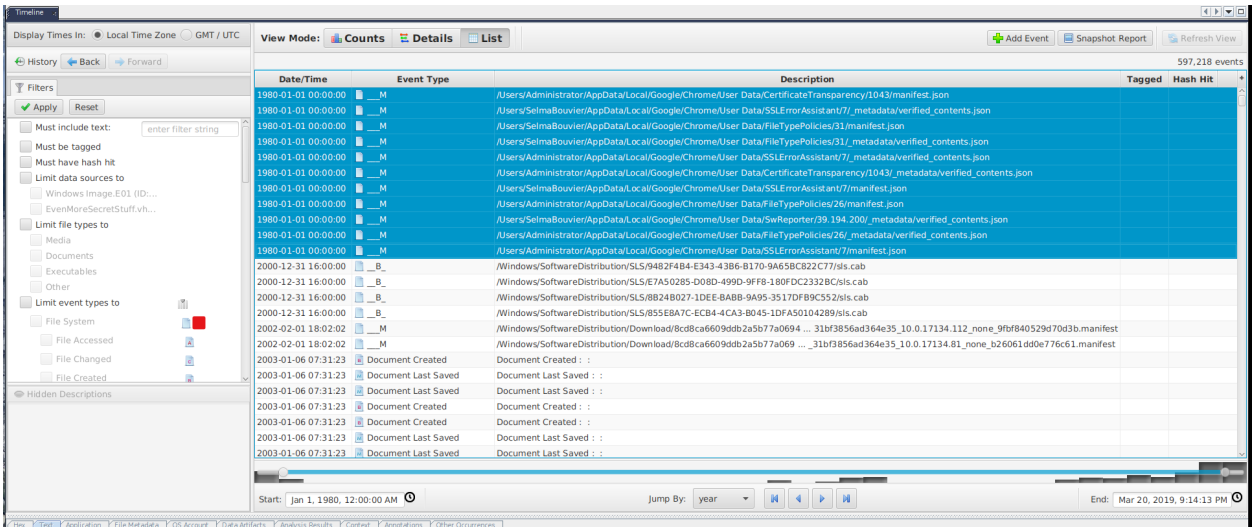

Figure 5: *Timeline results for January 1. 1980*

C VHD file encrypted

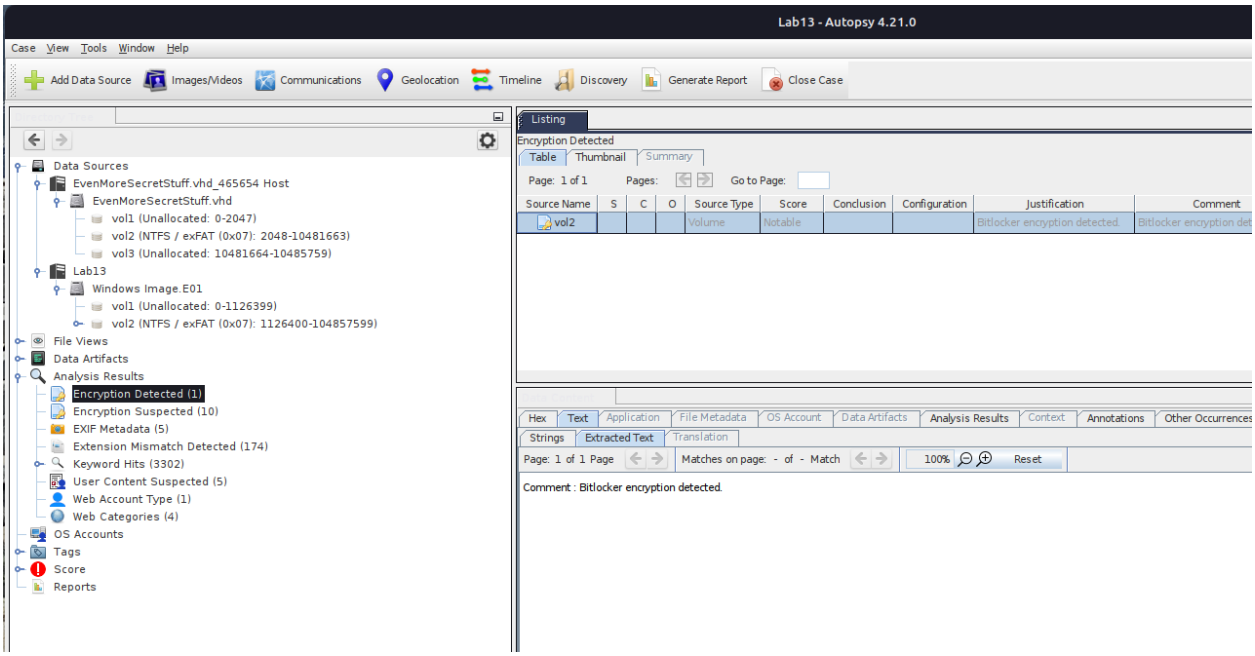

Figure 6: *The "EvenMoreSecretStuff" virtual drive, seems encrypted using bitlocker*

D IP Hits

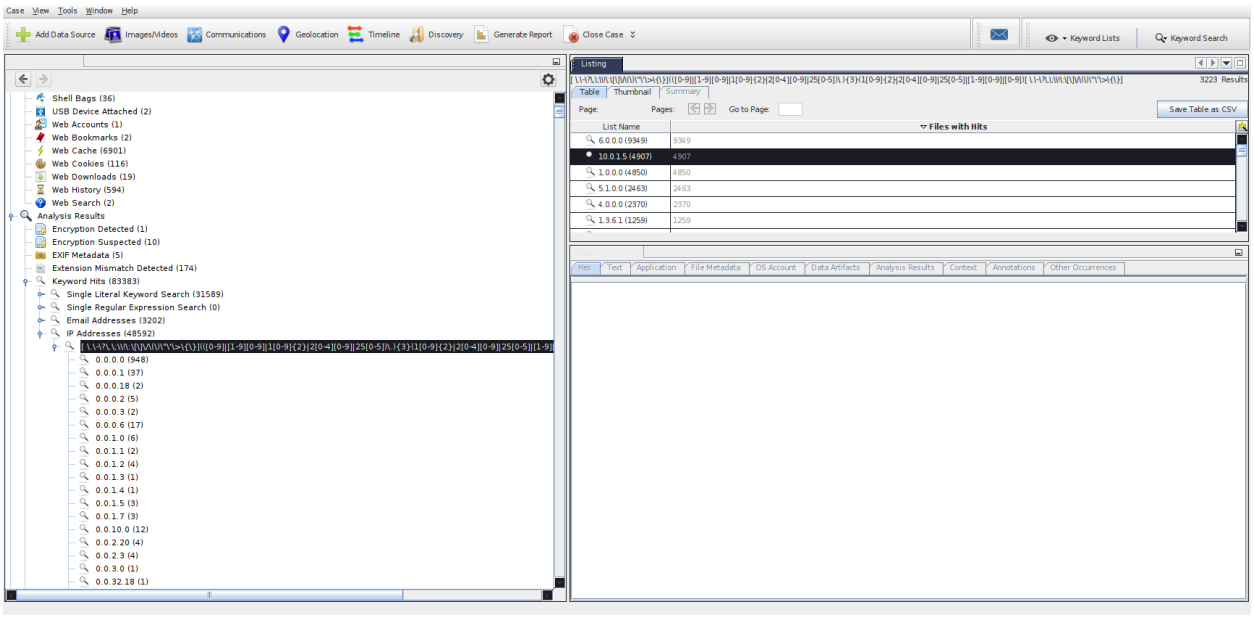

Figure 7: *Hits searching for ip v.4 addresses, the 6.0.0.0 hit is associated with the version of a windows subsystem and it not an IP in this context*

E TeamViewer

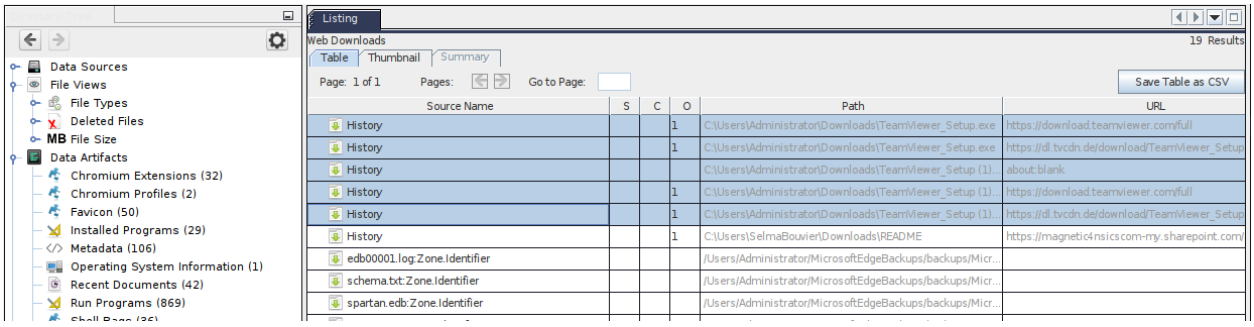

Figure 8: *TeamViewer was downloaded on January 25 2019 at 12:39pm*

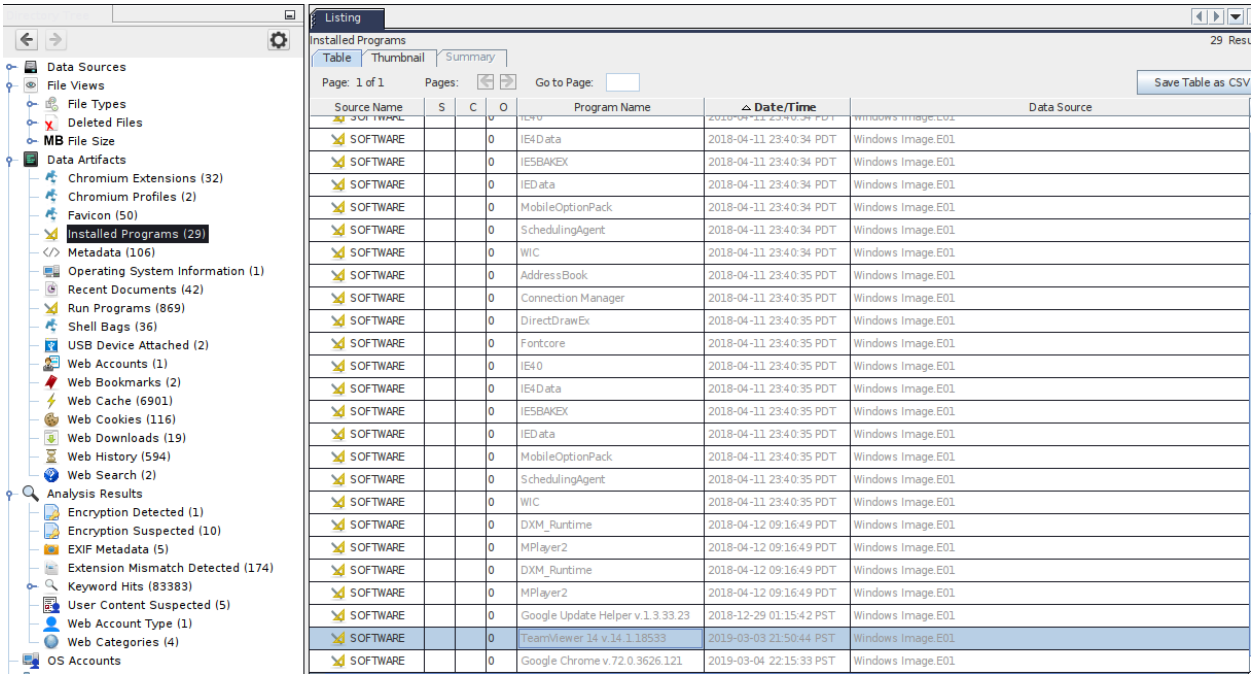

Figure 9: *TeamViewer was installed on February 3rd 2019 at at 9:50pm*

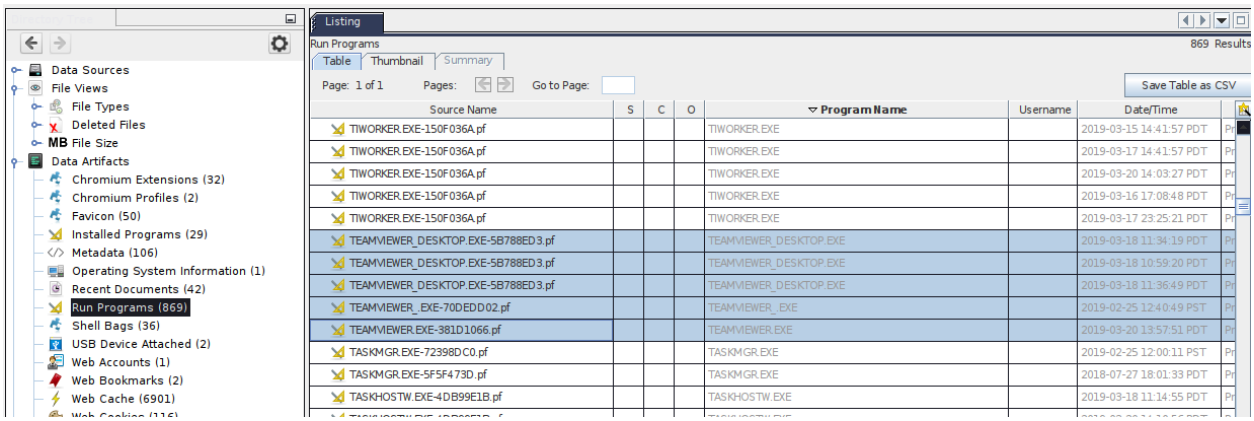

Figure 10: *TeamViewer was last run on February 20rd 2019 at at 1:57pm*