University of Utah
School of Computing
CS 6967: Security Operations

Lab 13 Response Outline

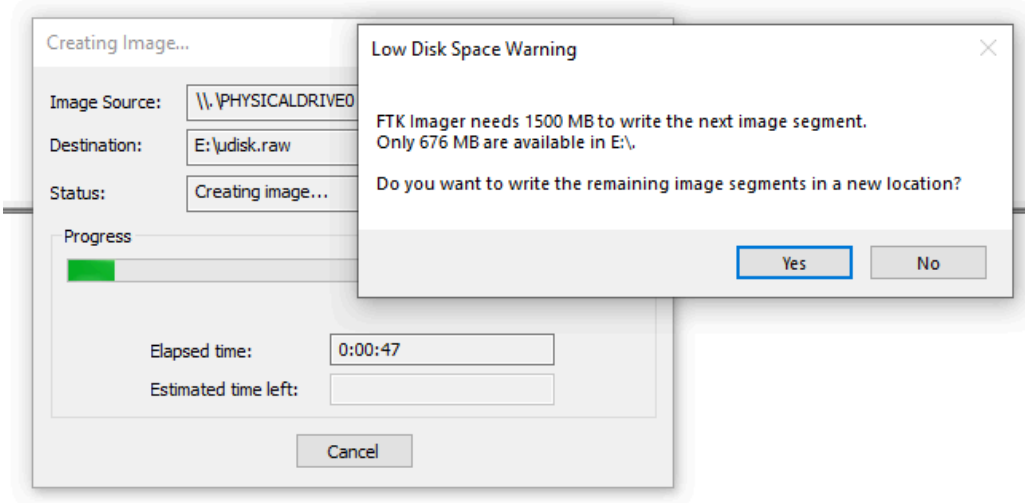
Lab 13: Threat Hunting with Disk Data

Test 1: Capture a Disk Dump

Summary of test experience:

This test requires us to dump a disk of a Windows machine. I used FTK imager to do this. But I couldn't finish this due to insufficient space. It usually requires a lot of space to capture a disk dump.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

The above screenshot shows that I was with a warning sign at the end of the process of capturing the C:\ drive of the disk to E:\ drive.

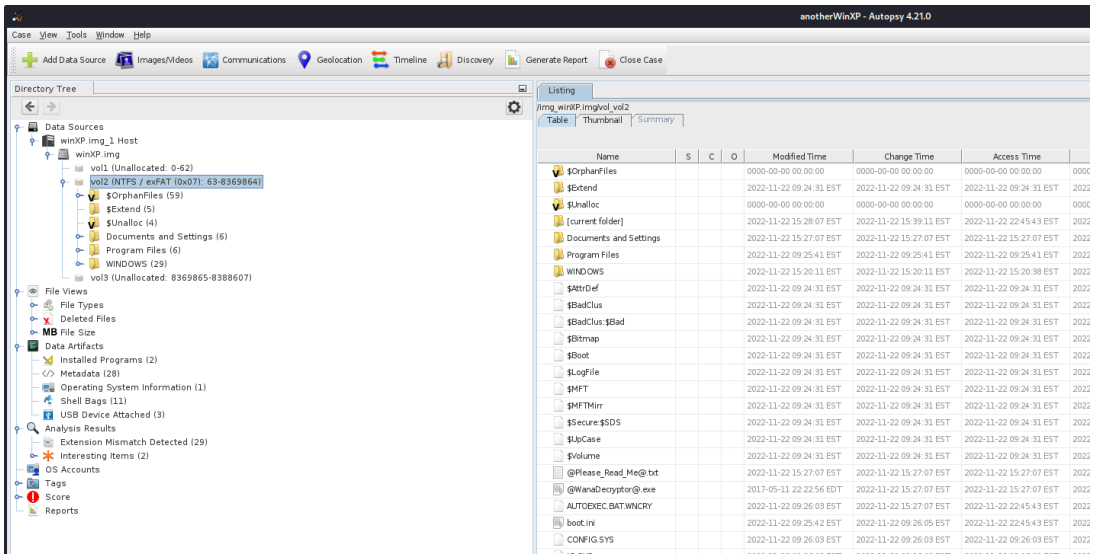
Test 2: Load the Disk Dump Into Autopsy

Summary of test experience:

In this test, the goal was to load the provided disk dump into Autopsy. However, I had a hard time installing the Austopsy, mainly because the instructions on the official documentation were

deprecated. Then, I figured out the required modifications and eventually installed Autopsy successfully. Finally, after configuring it, I could load the disk dump.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

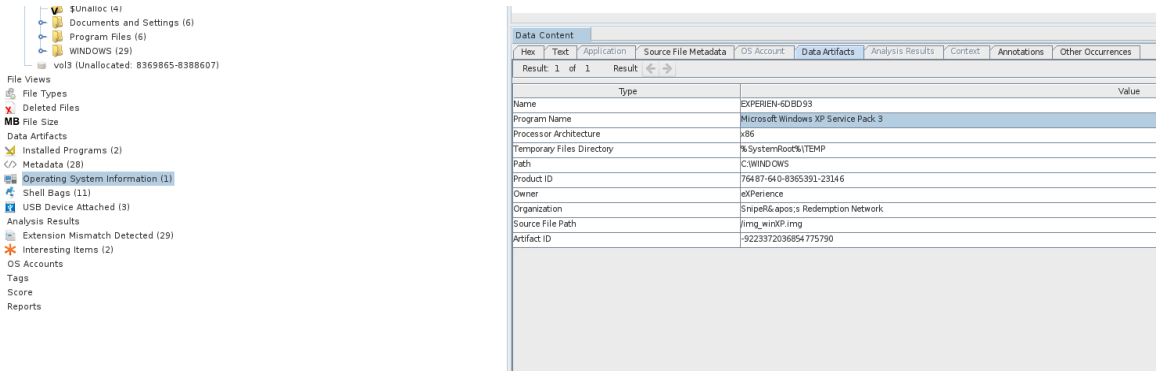
From the above screenshot, we can view the tree view of the file system on the left and the list view on the right.

Test 3: Identify the OS Information

Summary of test experience:

Here, from the data artifacts, we needed to extract OS information.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

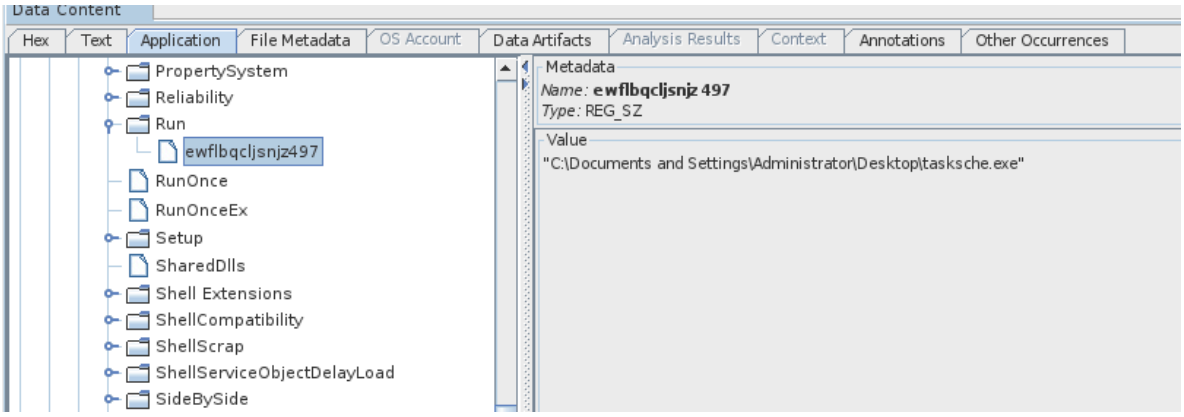
The above screenshot shows that the OS is ‘Microsoft Windows XP Service Pack 3.”

Test 4: Identify the Ransomware Program

Summary of test experience:

This test asks to find the Ransomware Program from the file system. For this, I searched for unusual exe file names on the hive files, which store all the registry information when the OS is started or a user logs on.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

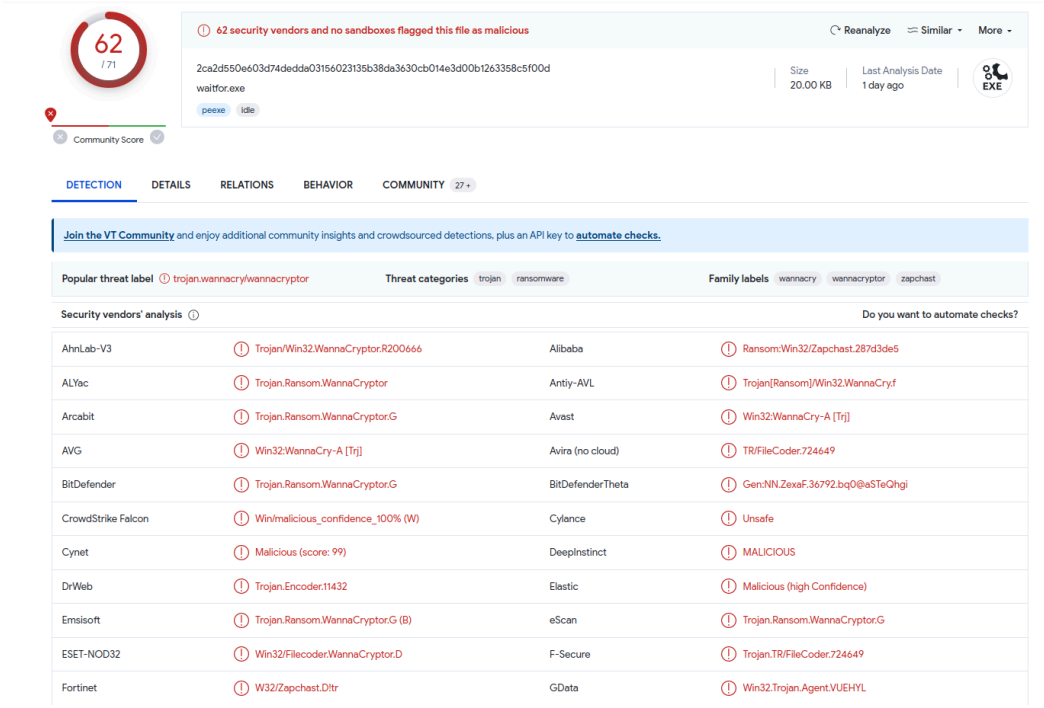
From the above image, it can be seen that a suspicious program named “tasksche.exe” was executed, hinting that it might be a ransomware program.

Test 5: Get Details of the Ransomware Program

Summary of test experience:

In this final test, we must find the details of the Ransomware Program. Suppose you have the hash of a ransomware program. In that case, you can find the details from VirusTotal, which is a database of ransomware programs and provide necessary information by scanning its website based on the search query. So, I collected the hash file of that ransomware program and uploaded it on VirusTotal to get the details about the malicious program.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

From the above screenshot, it's seen that 62 security vendors marked this file as 'wannacry' ransomware.