

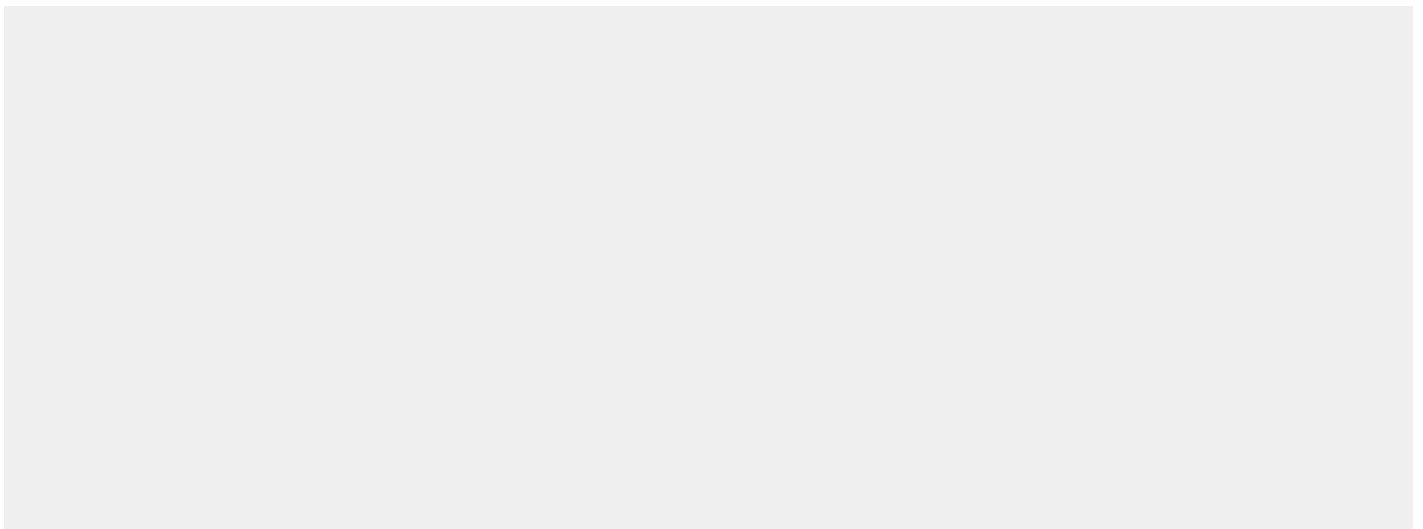
99: Validate Indications of Compromise: Analysis of PE File

Objective

- Use PESTudio to detect and identify signs of malicious activity in PE files

Scenario

Your organization's incident response team has asked you to look at a suspicious executable they found on an employee laptop in the finance office. Analyze the file and detect any malicious functions, suspicious strings, or symbols found in the file.




Detecting Evidence of Suspicious Symbols and Strings in Executables

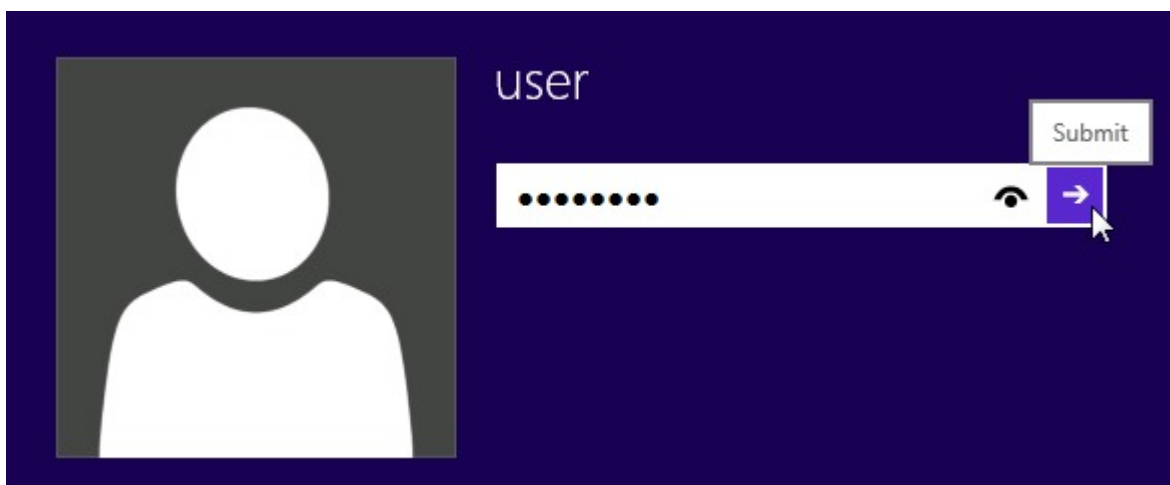
Scenario

It's important to be able to recognize some of the signs of malware, and as well the ways the creators of malware attempt to hide and thwart detection and analysis efforts. In order to properly detect and respond to an incident, you must be very familiar with the use of a variety of tools. These tools will help you detect various types of malware and to help formulate the appropriate response.

☐ 1. Login to Windows

Log in to the Windows 8 machine with the username **user** and the password **password**.

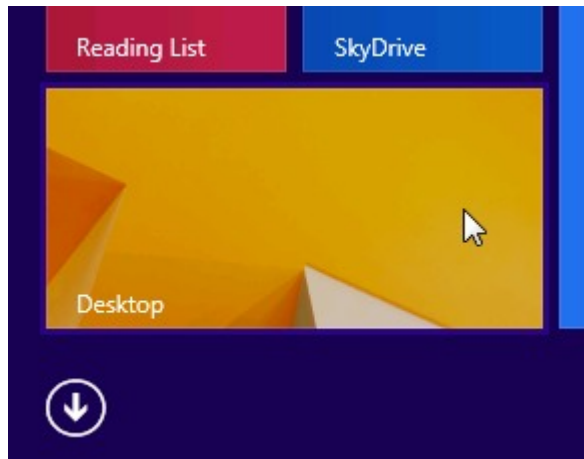
 Make sure to enter the credentials correctly, otherwise you cannot continue the lab.



☐ 2. Get to the Desktop

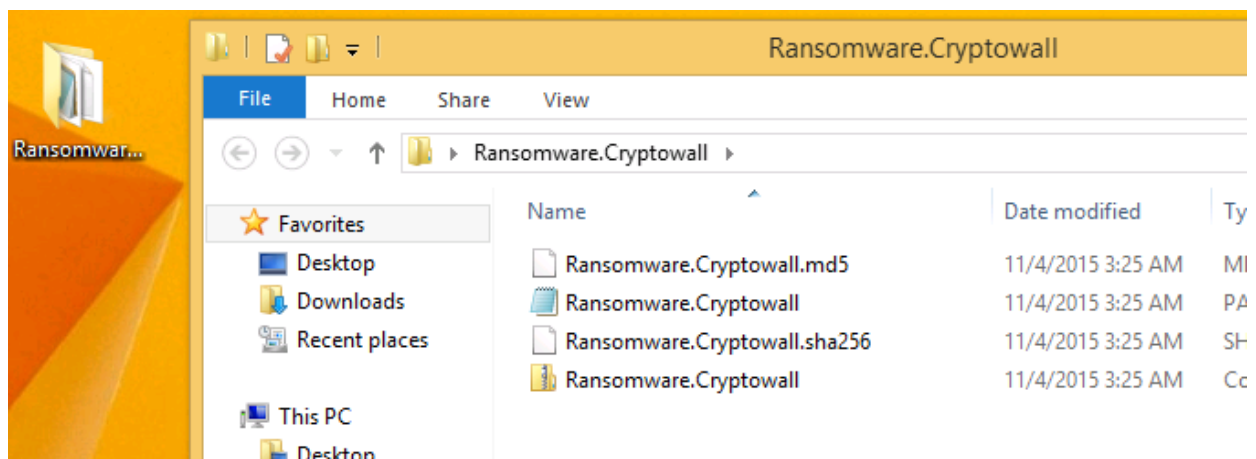
Click on the **Desktop** icon located in the lower left corner of the screen.

 If you receive a pop-up from Windows asking to update, click on No.



☐ 3. **Detect Evidence of Packing in Executables**

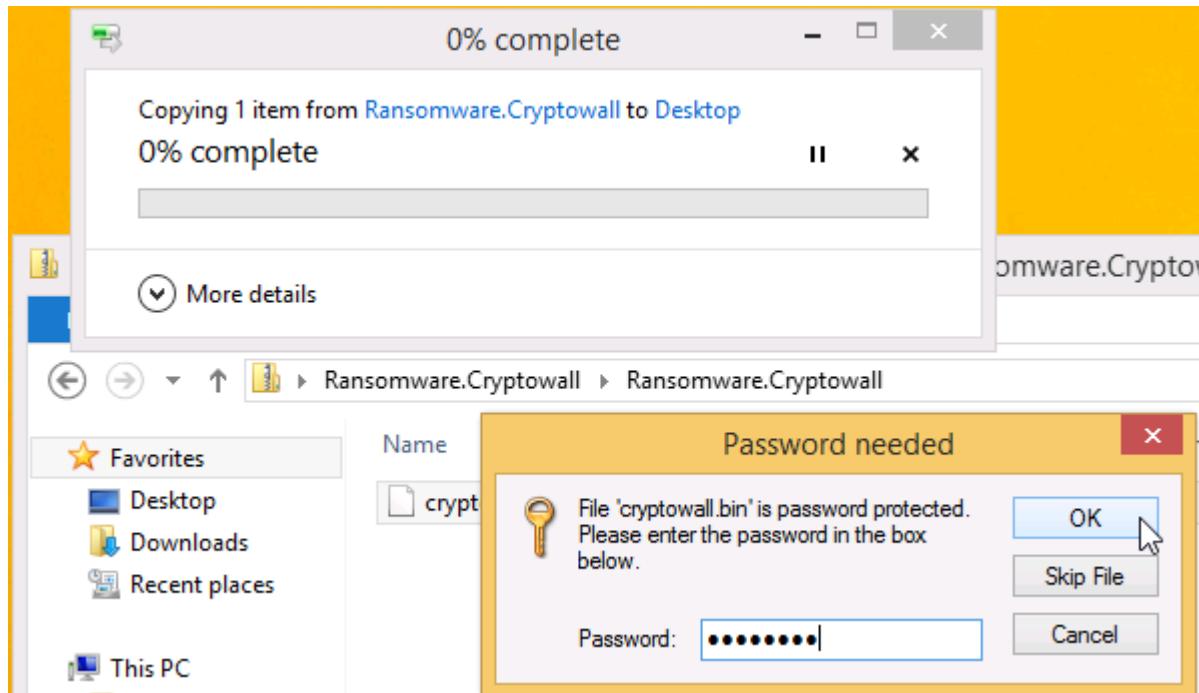
Open the **Ransomware.Cryptowall** folder located on the desktop and then open up **Ransomware.Cryptowall.zip**.



Switch to Win 8.1

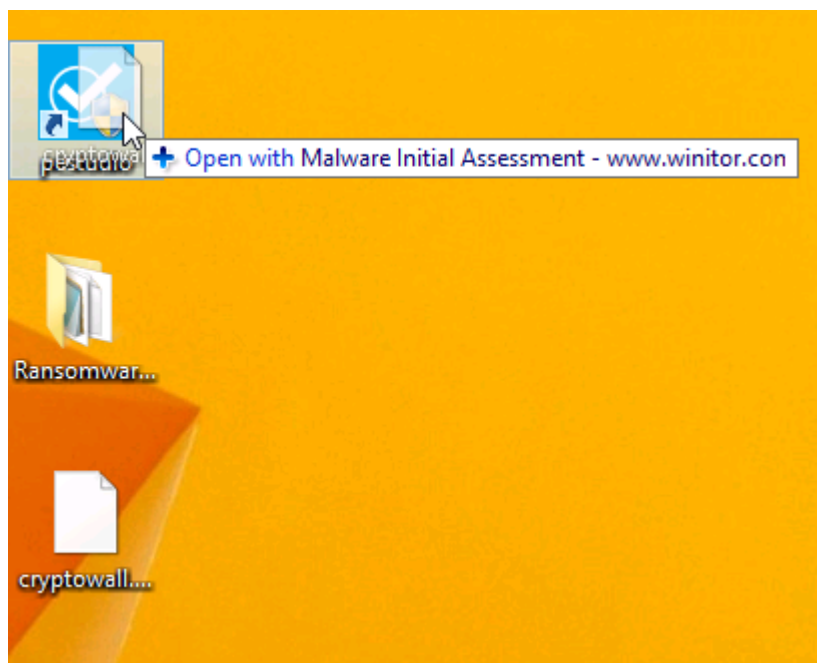
☐ 4. **Detect Evidence of Packing in Executables**

Next, drag the **cryptowall.bin** file to the desktop. The file password is **infected**.



☐ 5. Analyze Malicious Binary with PEstudio

Drag and drop the **cryptowall.bin** file from the desktop onto the PEstudio shortcut on the Desktop. Click **Yes** on the User Account Control pop-up window. The PEstudio tool will open and analyze the file.




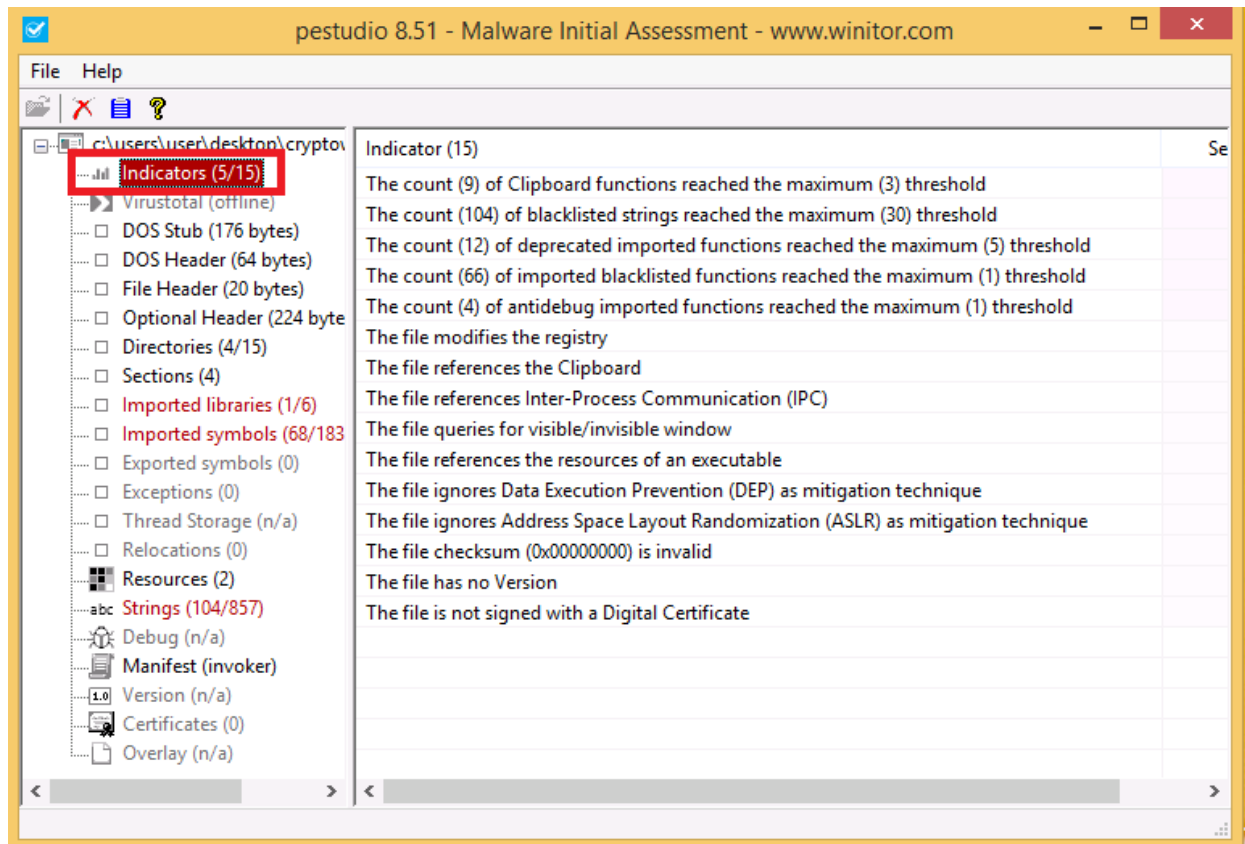
Switch to  Win 8.1

☐ 6. Review Indicators

On the left side of the PEstudio program, you will see a list of clickable data types. Based on the results of the analysis performed by PEstudio these groups will be populated with further details.

Click on the **Indicators** link and review the list of indicators. These indicators are various items that PEstudio has assessed to be signs of malicious. We see evidence of blacklisted strings and functions, anti-debugging activity, and excessive memory management functions.


 Indicators are represented as human-readable results based on the things observed in the analyzed file. Each item is further grouped into categories according to the assessed severity. Indicators show the potential for malicious behavior as well as any anomalies discovered.

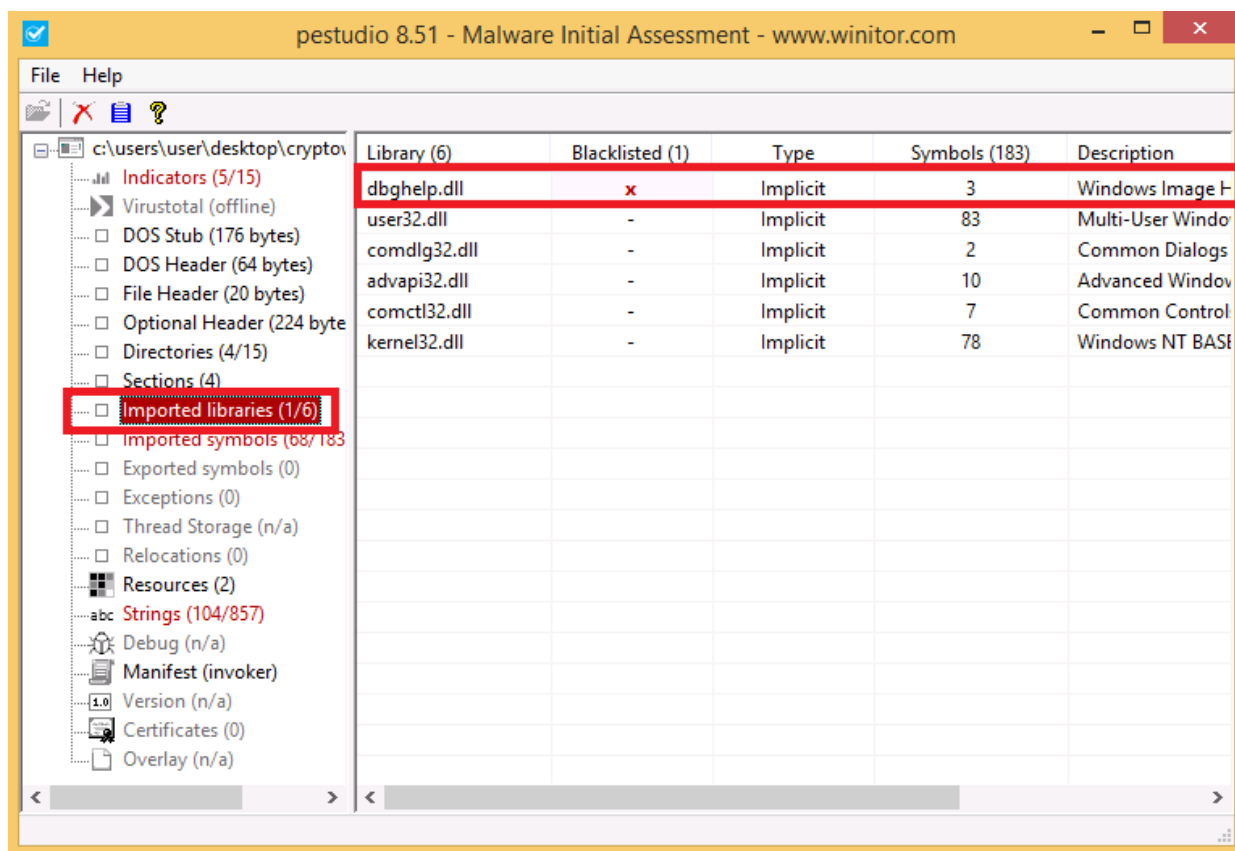


Switch to  Win 8.1

☐ 7. Review Imported Libraries

Click on the **Imported libraries** detail. This contains a list of DLL files that the analyzed file calls at the start of execution. Note the inclusion of **dbghlp.dll**... it is a blacklisted DLL and is considered an indicator that the file may be malicious.

 All executables must interact with the operating system in order to perform its programmed activity. For this to be possible, a certain amount of libraries must be used. PESTUDIO retrieves the libraries and the functions used by the image.



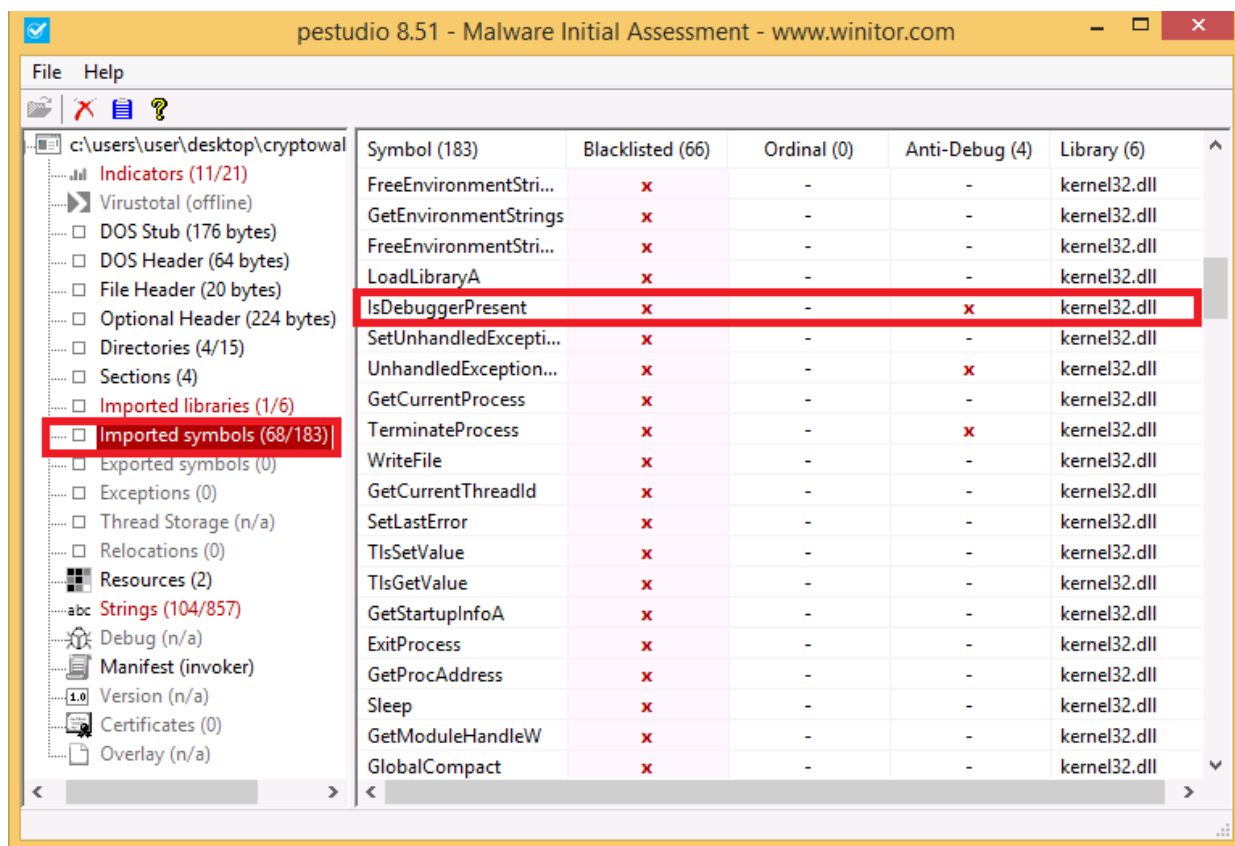
Switch to Win 8.1

☐ 8. Review Imported Symbols

Click on the **Imported symbols** entry and look at the blacklisted items. Think about how some of these items could be used by malware.

Look at the item highlighted in the screenshot. The file calls a function that is used to check for the presence of a running debugger. Why do you think malware would want to see if a debugger was present?

IsDebuggerPresent is a function available in the kernel32.dll library. This function is often used by malware to frustrate and confuse the reverse engineering process because it will take different paths in the program's flow when the malware is analyzed in a user-mode debugger such as OllyDbg.

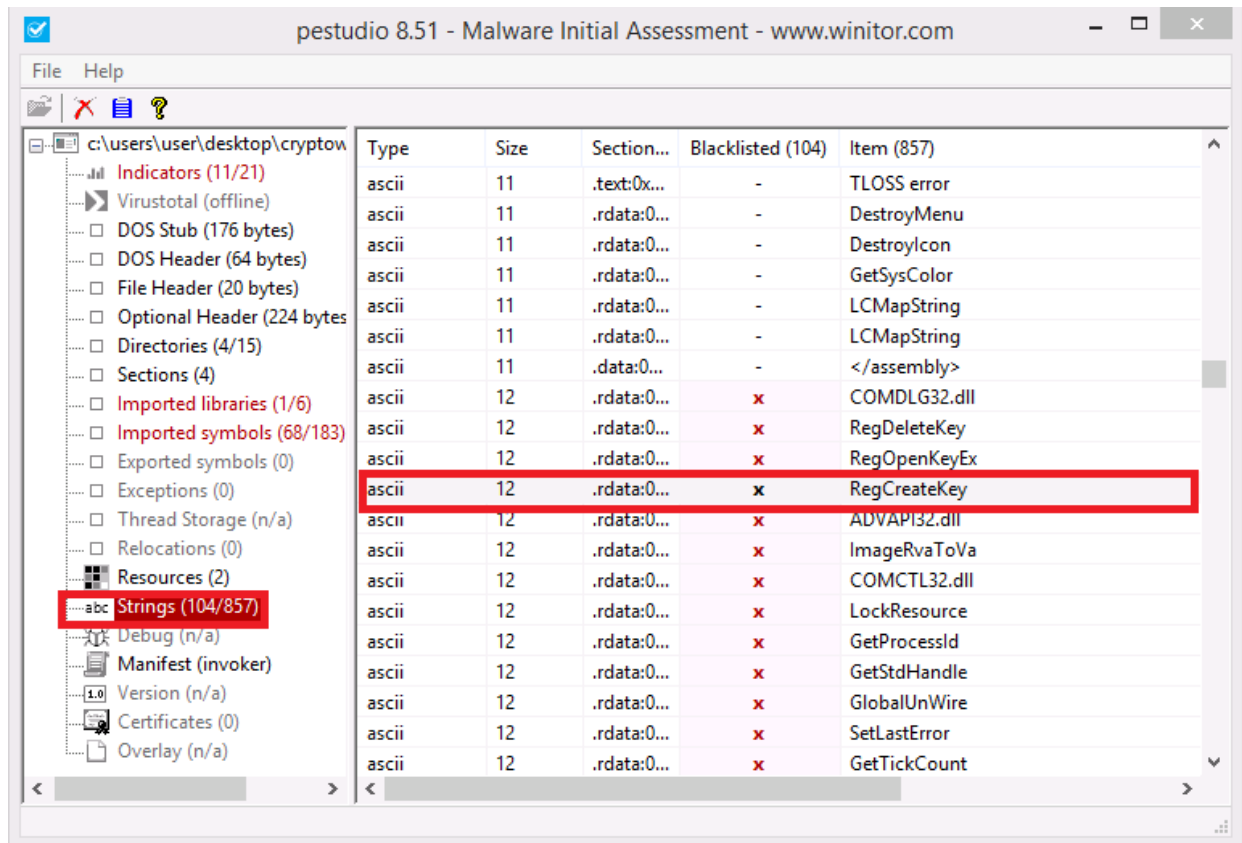


Switch to Win 8.1

☐ 9. Review Strings

Click on Strings and scroll through the list of strings PESTudio found in the executable. Some of them are blacklisted because they are frequently found in malware and are associated with various functions that malware use.

Scroll down and look at the **RegCreateKey** string. What do you think this is used for?



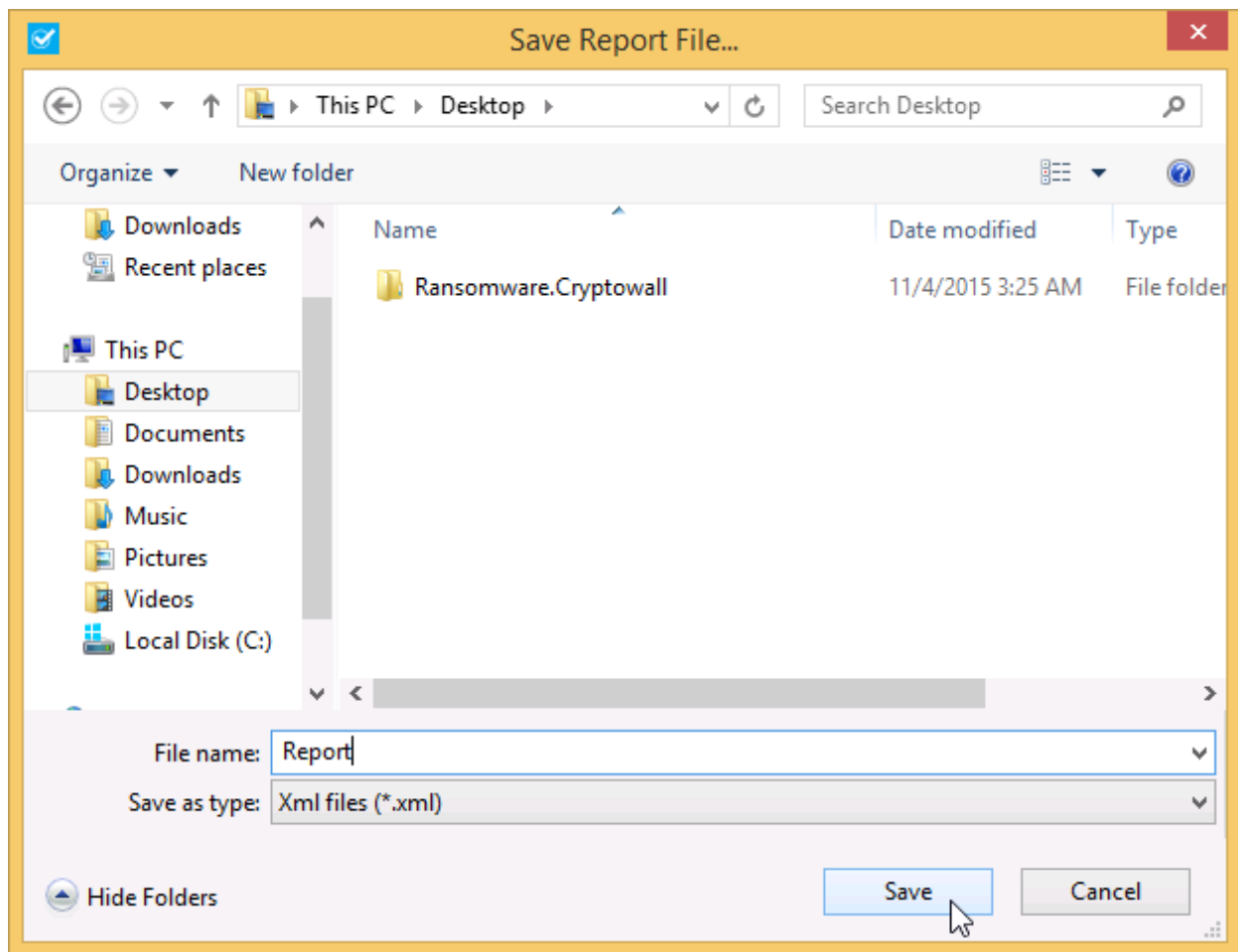
Switch to Win 8.1

☐ 10. Create a Report

The final step is to document your work for use later. Click **File** -> **Create Report** -> **Save to Desktop** and name it.

Find the file on the Desktop and then right-click on it and open it with **Internet Explorer**. This XML file is very useful and contains all the information from PEstudio's analysis. This file can be used by other programs as well.

PEstudio allows investigators to analyze unknown and suspicious executable files, many of those files will need to have reports written about them. For this purpose, PEstudio produces an XML report that documents all of the automated analysis findings. The goal of having an XML-formatted report is to allow the report to be utilized by other third-party analysis tools.



Switch to  Win 8.1

Congratulations. You have successfully completed this lab.