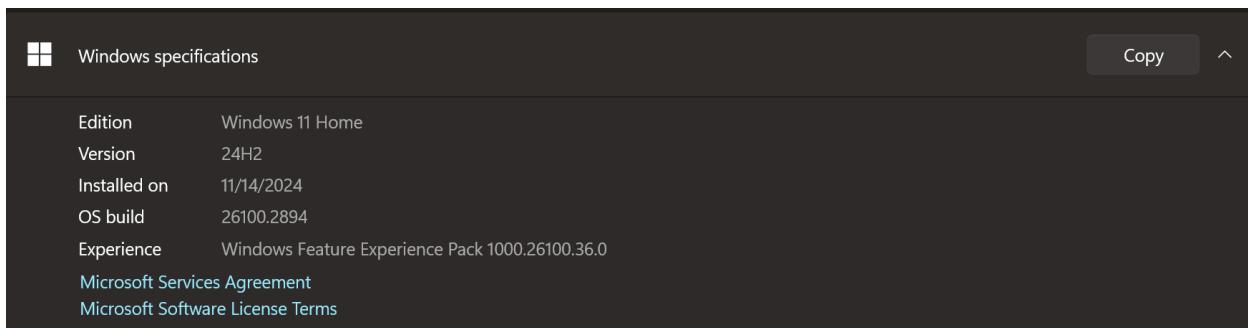


Malware Protection Test – (36 points)

The purpose of this assignment is for you to test two malware / end-point protections of your choice using a test file known as “eicar”. The “eicar” file is harmless to your computer, but malware protections know to flag the file as malicious for testing purposes.

Download the “eicar-test-smb.zip” from Canvas and answer the following questions. Provide screenshots to support your answers.

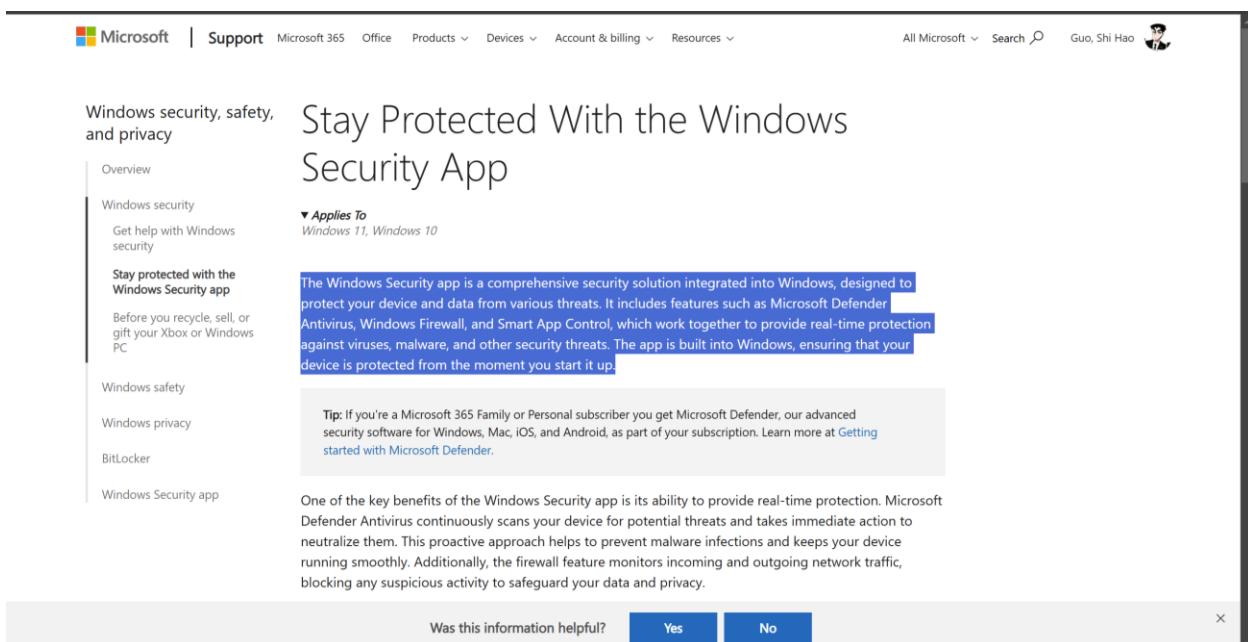
1. What type / OS version are you running? Microsoft Windows 11 Home (24H2).



A screenshot of a Windows specification page. It shows the following details:

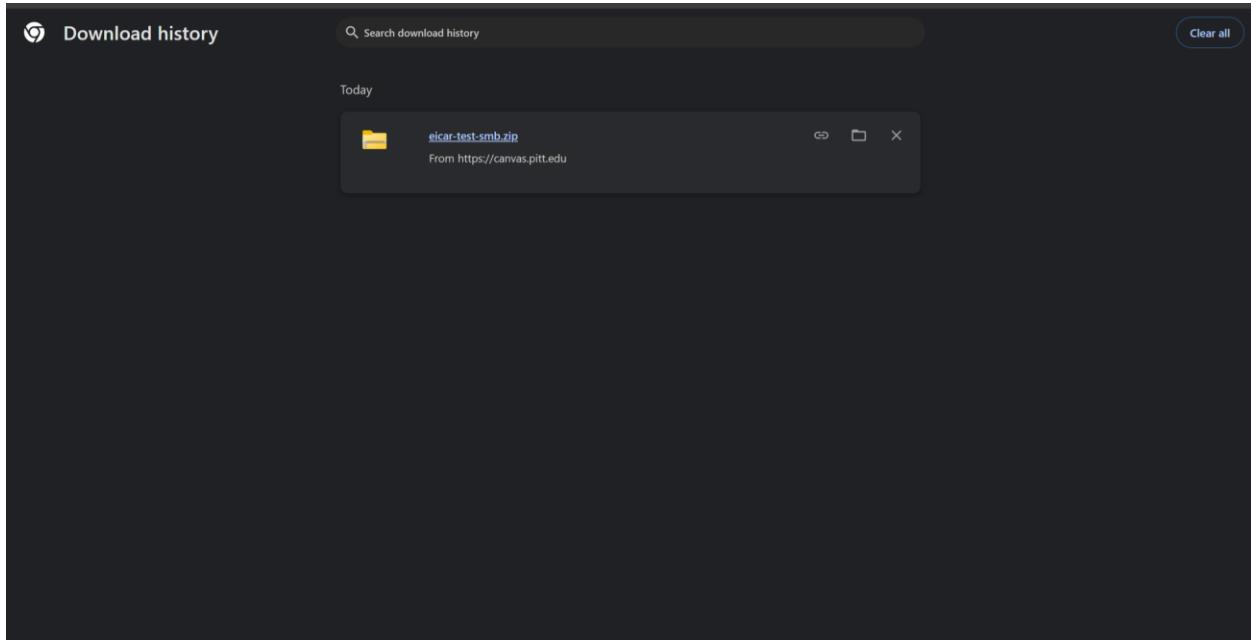
| | |
|----------------------------------|---|
| Edition | Windows 11 Home |
| Version | 24H2 |
| Installed on | 11/14/2024 |
| OS build | 26100.2894 |
| Experience | Windows Feature Experience Pack 1000.26100.36.0 |
| Microsoft Services Agreement | |
| Microsoft Software License Terms | |

2. What malware / end-point protection are you running for your test? Microsoft Windows Security App (Microsoft Defender Antivirus).

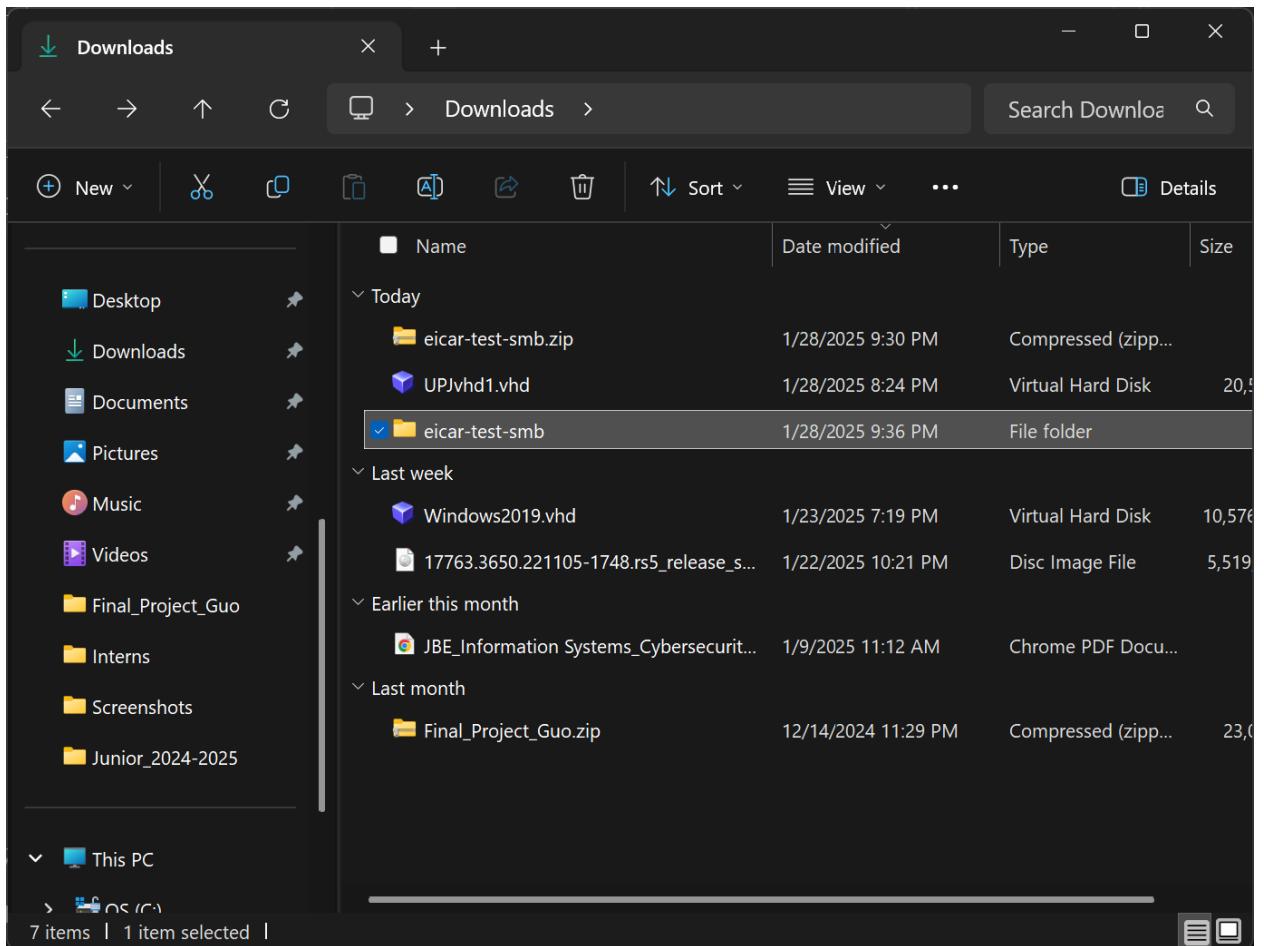


A screenshot of the Microsoft Windows Security app page. The main heading is "Stay Protected With the Windows Security App". Below it, a section titled "Applies To" specifies "Windows 11, Windows 10". A detailed description states: "The Windows Security app is a comprehensive security solution integrated into Windows, designed to protect your device and data from various threats. It includes features such as Microsoft Defender Antivirus, Windows Firewall, and Smart App Control, which work together to provide real-time protection against viruses, malware, and other security threats. The app is built into Windows, ensuring that your device is protected from the moment you start it up." A tip box notes: "Tip: If you're a Microsoft 365 Family or Personal subscriber you get Microsoft Defender, our advanced security software for Windows, Mac, iOS, and Android, as part of your subscription. Learn more at Getting started with Microsoft Defender." Another section highlights: "One of the key benefits of the Windows Security app is its ability to provide real-time protection. Microsoft Defender Antivirus continuously scans your device for potential threats and takes immediate action to neutralize them. This proactive approach helps to prevent malware infections and keeps your device running smoothly. Additionally, the firewall feature monitors incoming and outgoing network traffic, blocking any suspicious activity to safeguard your data and privacy." At the bottom, a poll asks "Was this information helpful?" with "Yes" and "No" buttons.

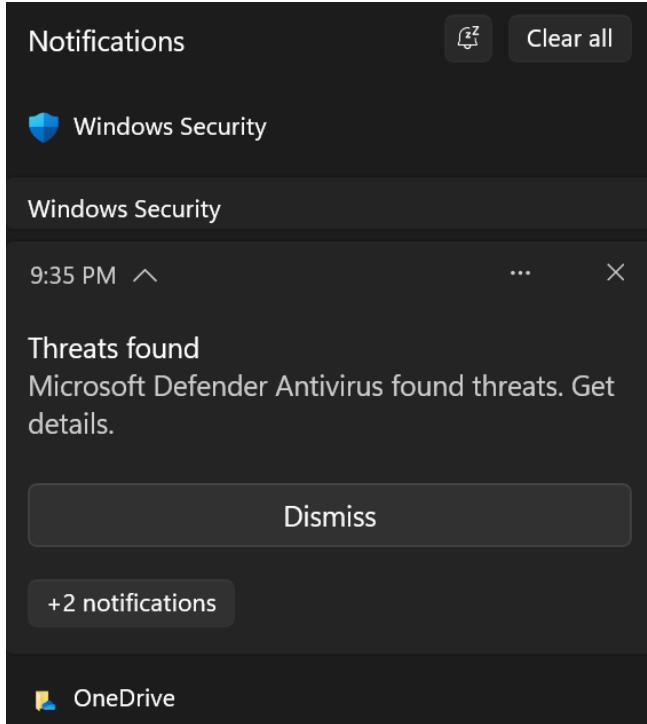
3. Download the “eicar-test-smb.zip” to your computer. Did your malware protection detect a malicious file as soon as you downloaded the file to your computer? No, my malware protection does not detect the file as malicious when I downloaded it.



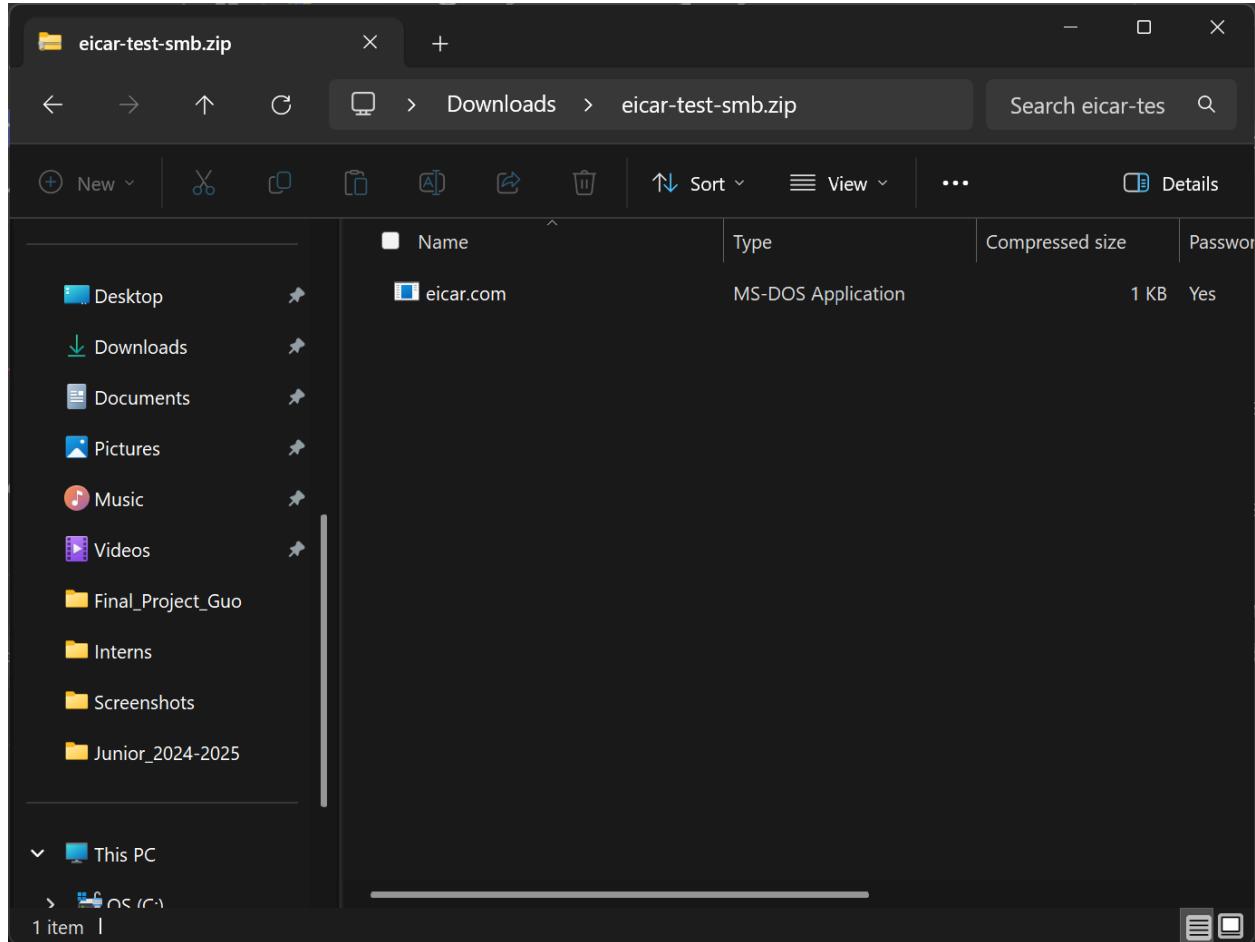
4. Unzip the “eicar-test-smb.zip” using the password “f11-11”

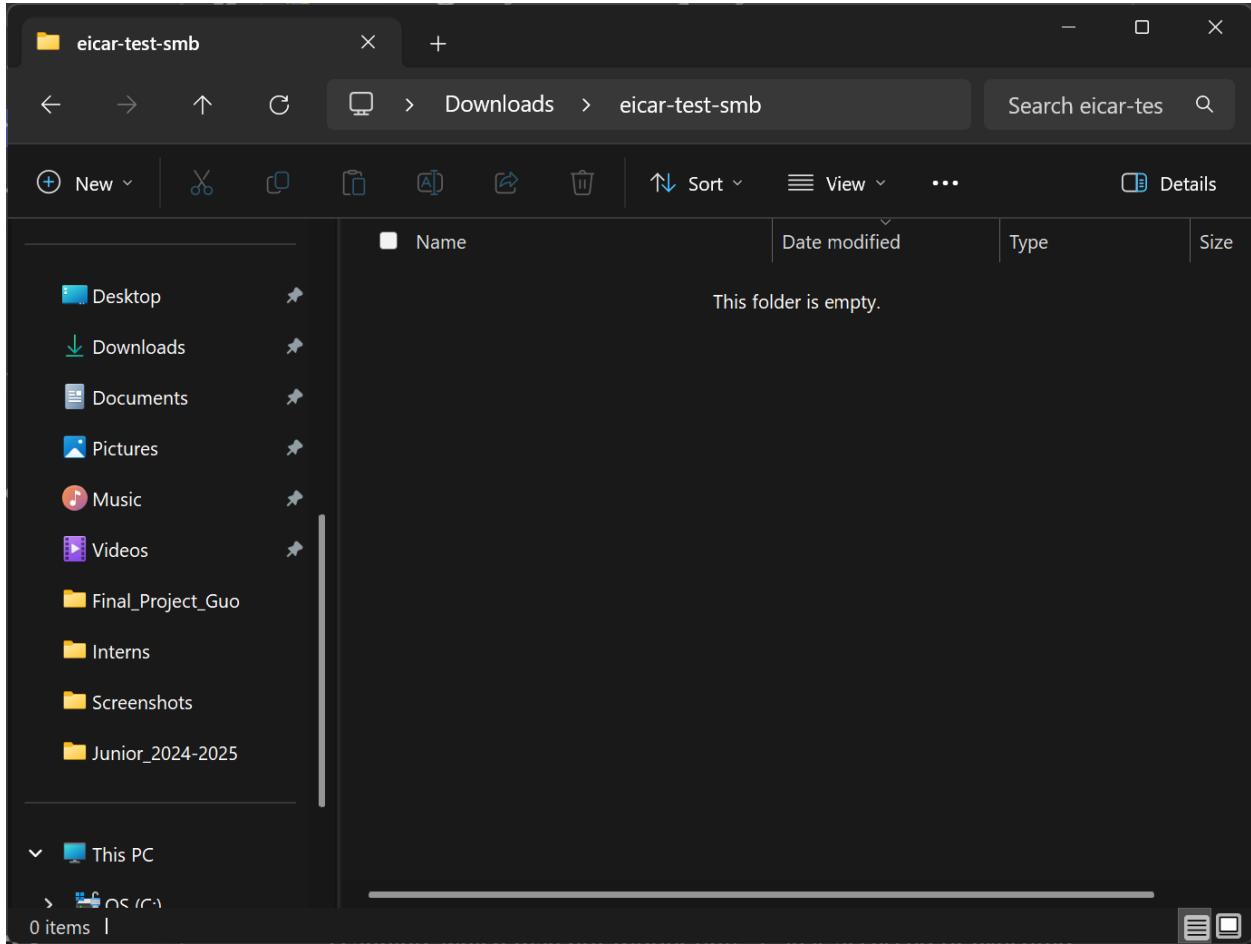


5. Did your malware / end-point protection detect “eicar” file as malware? Yes, it did.

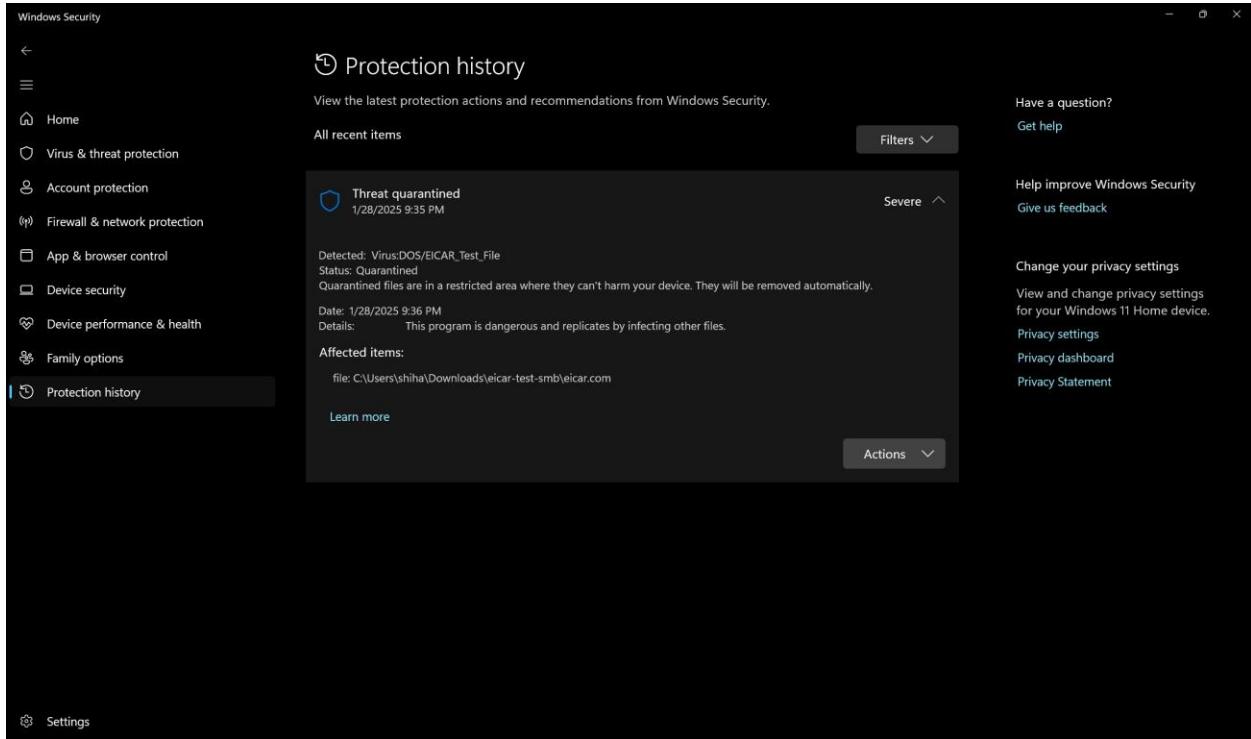


6. Why did your malware / end-point protection not detect the file as malware for step 3, but did after you unzipped the file? The most likely reason is because this specific ZIP file is password-protected, the antivirus cannot inspect its content until password is entered and file is extracted.
7. Did your malware automatically delete or quarantine the eicar file once it was detected? If so, which one? Yes, it automatically deleted the “eicar.com” application after I extracted the file.





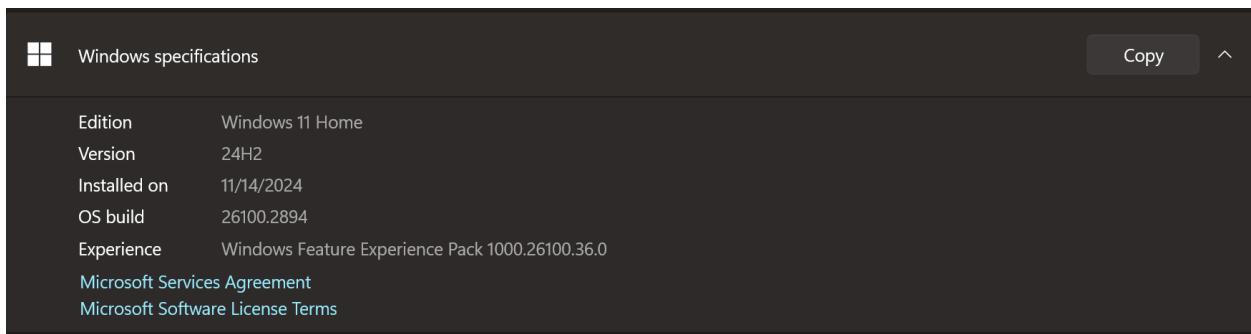
8. Were you given a choice on what type of action your malware protection would perform to the file? Nope, it did not prompt me with any choice, it just notified me that the file is malicious and deleted the file.
9. Does your malware protection show a history of detection / actions taken? Yes, it does show me a history of detection and operation.



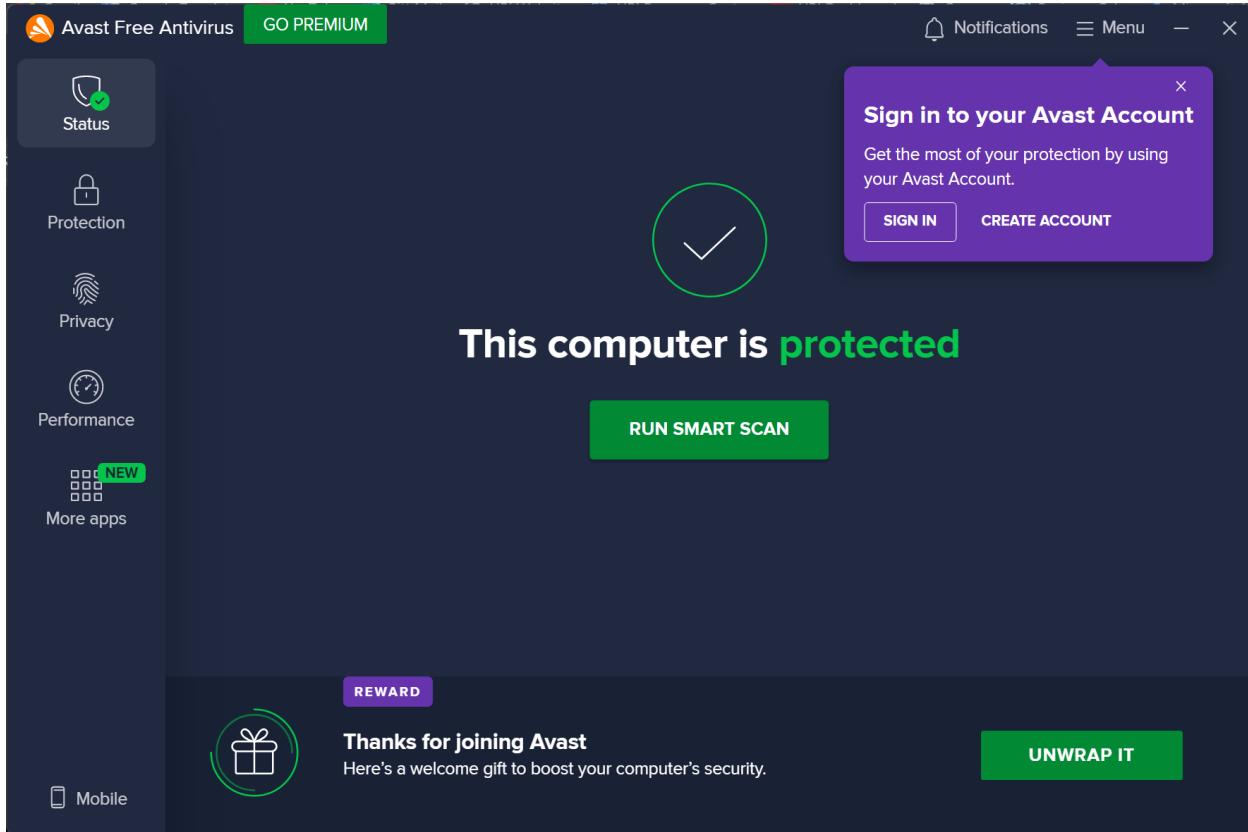
10. Repeat steps 1-9 again testing with a second malware / end-point protection.

Note: You can test within a VM using a hypervisor or the cloud and/or just use a different computer.

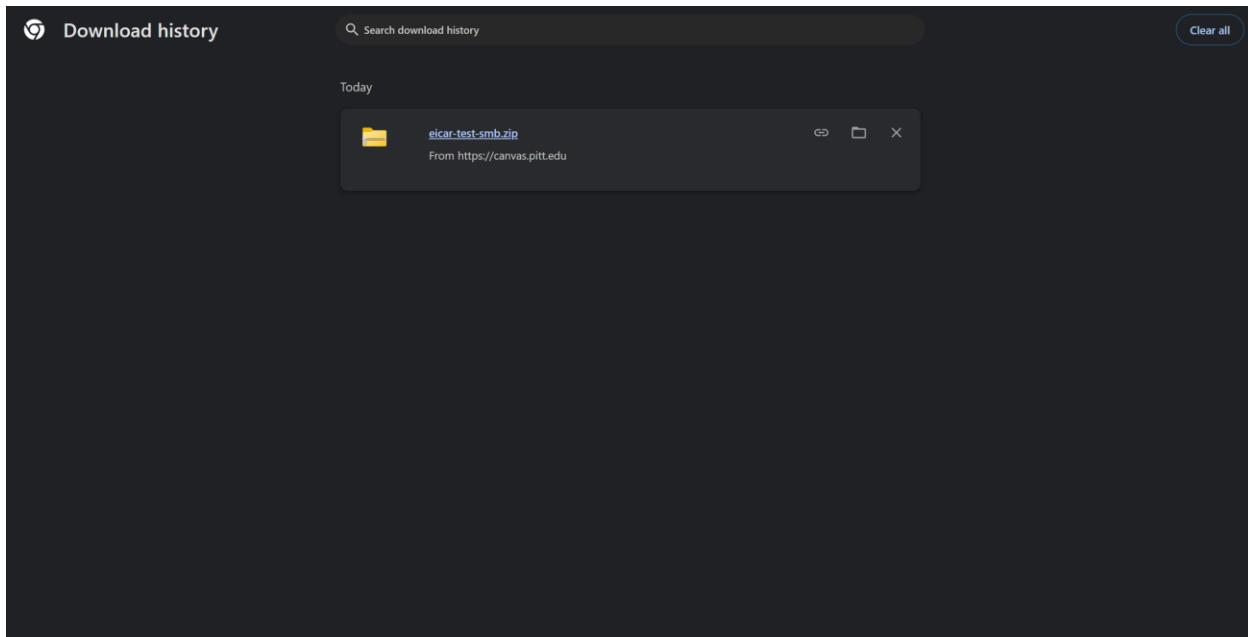
11. What type / OS version are you running? Microsoft Windows 11 Home (24H2).



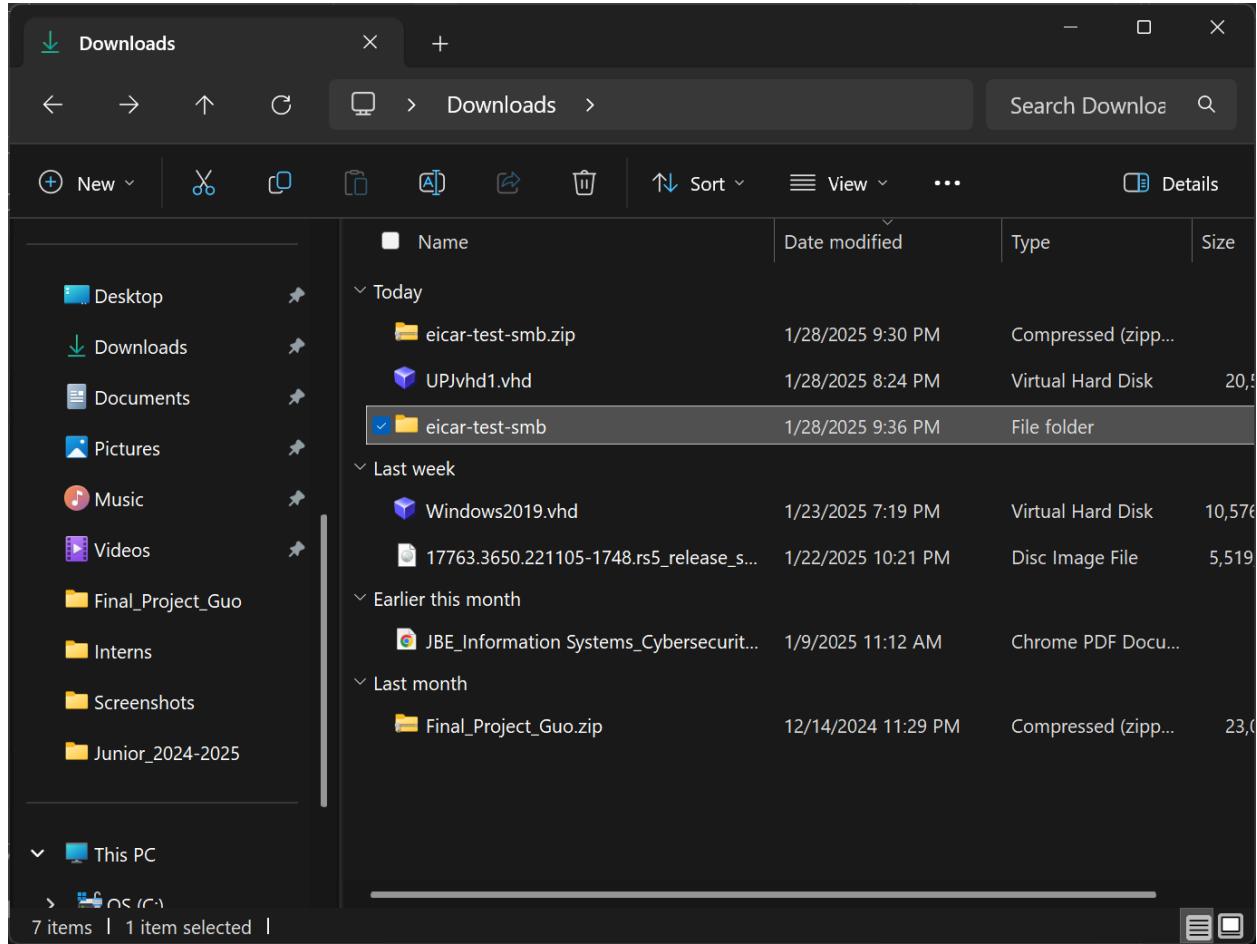
12. What malware / end-point protection are you running for your test? Avast Free Antivirus



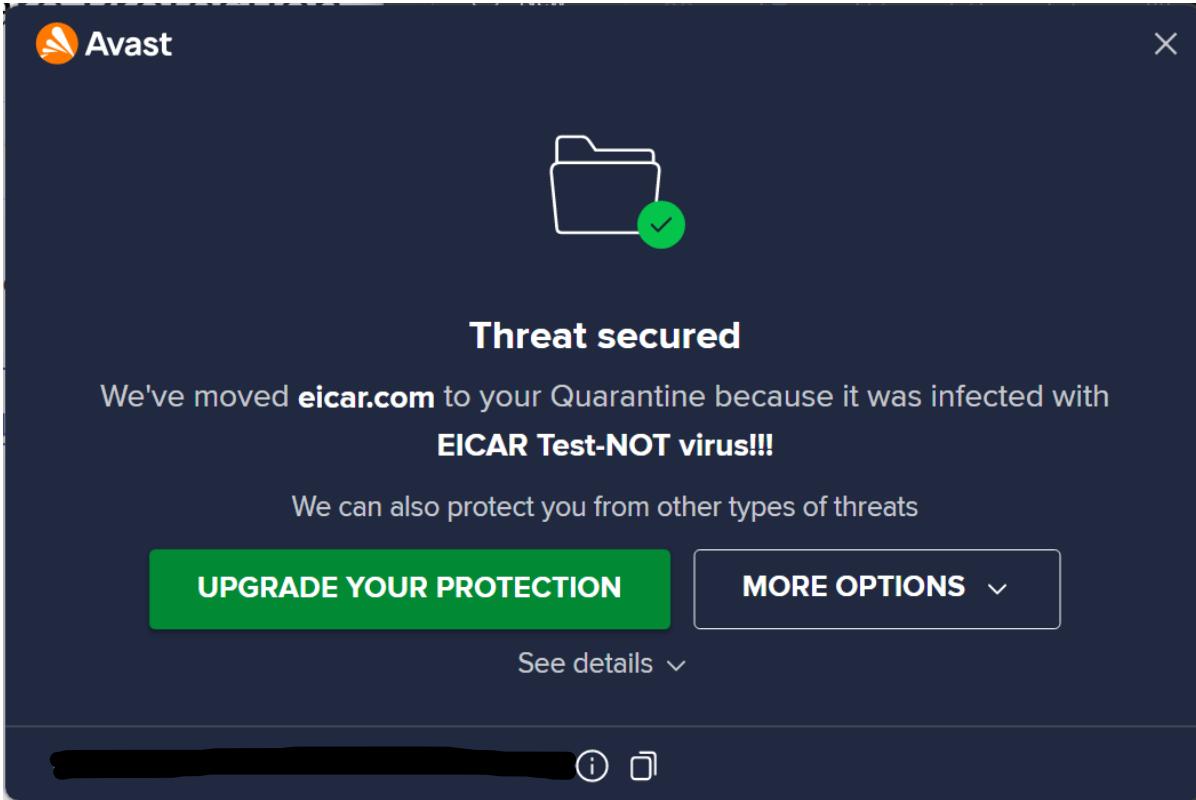
13. Download the “eicar-test-smb.zip” to your computer. Did your malware protection detect a malicious file as soon as you downloaded the file to your computer? No, my malware protection does not detect the file as malicious when I downloaded it.



14. Unzip the “eicar-test-smb.zip” using the password “f11-11”

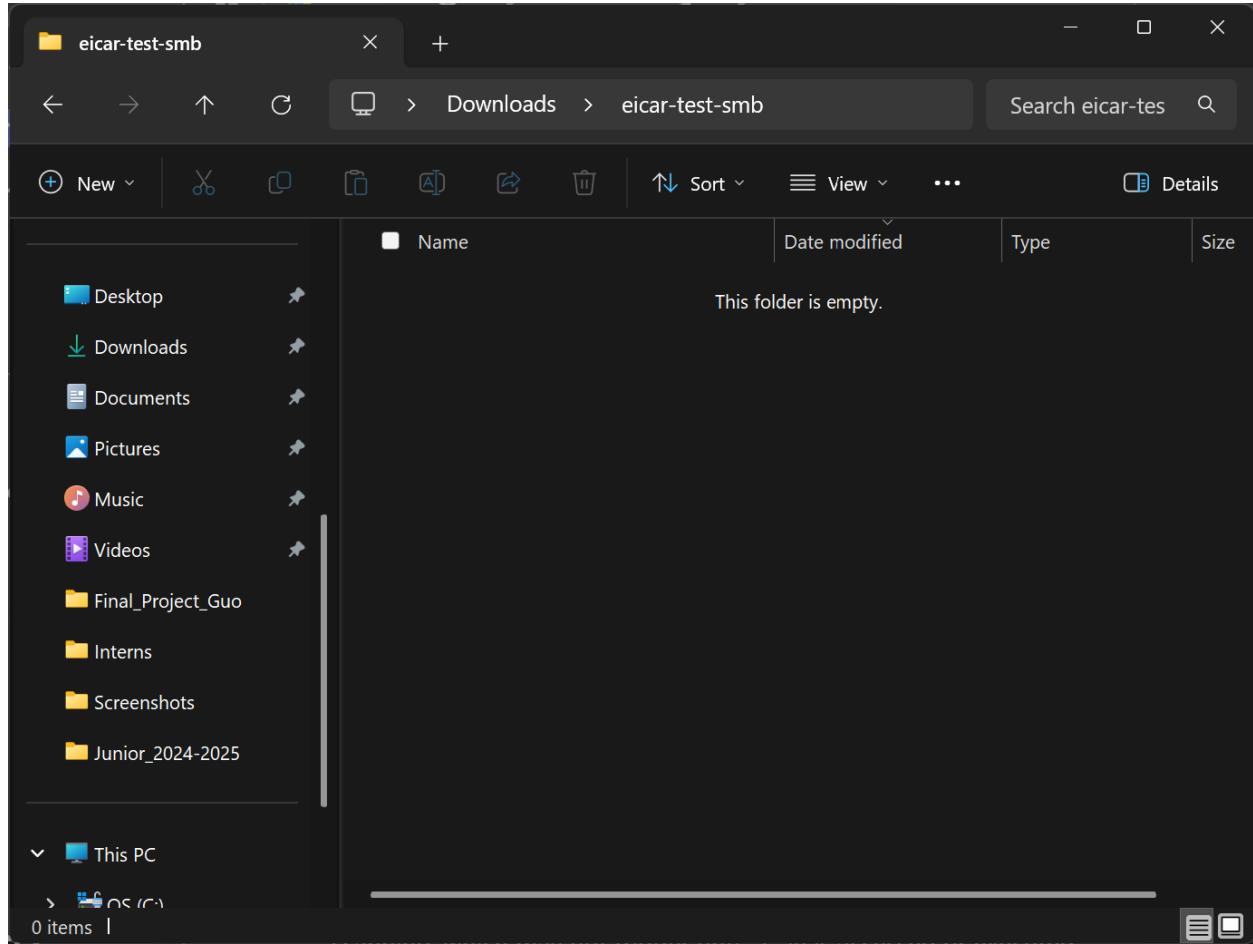


15. Did your malware / end-point protection detect “eicar” file as malware? Yes, it did.

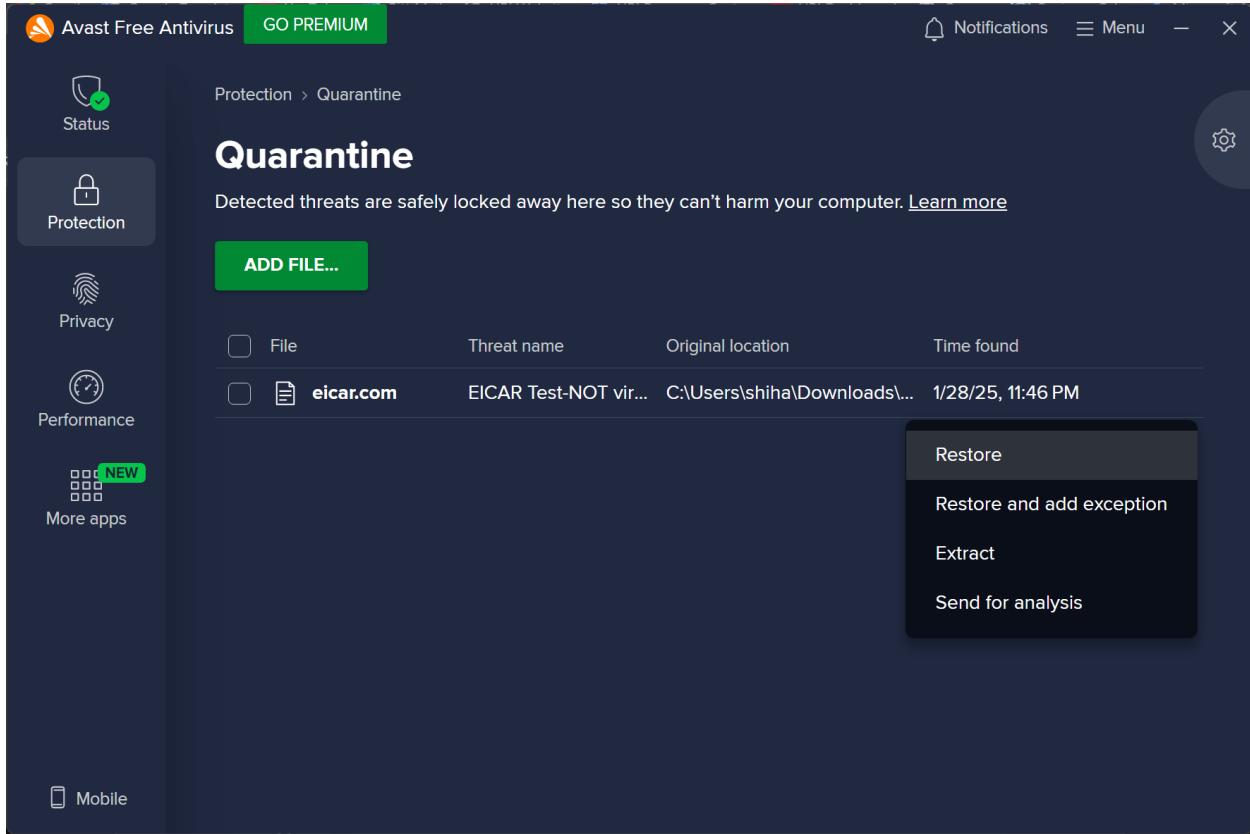


16. Why did your malware / end-point protection not detect the file as malware for step 3, but did after you unzipped the file? The most likely reason is because this specific ZIP file is password-protected, the antivirus cannot inspect its content until password is entered and file is extracted.

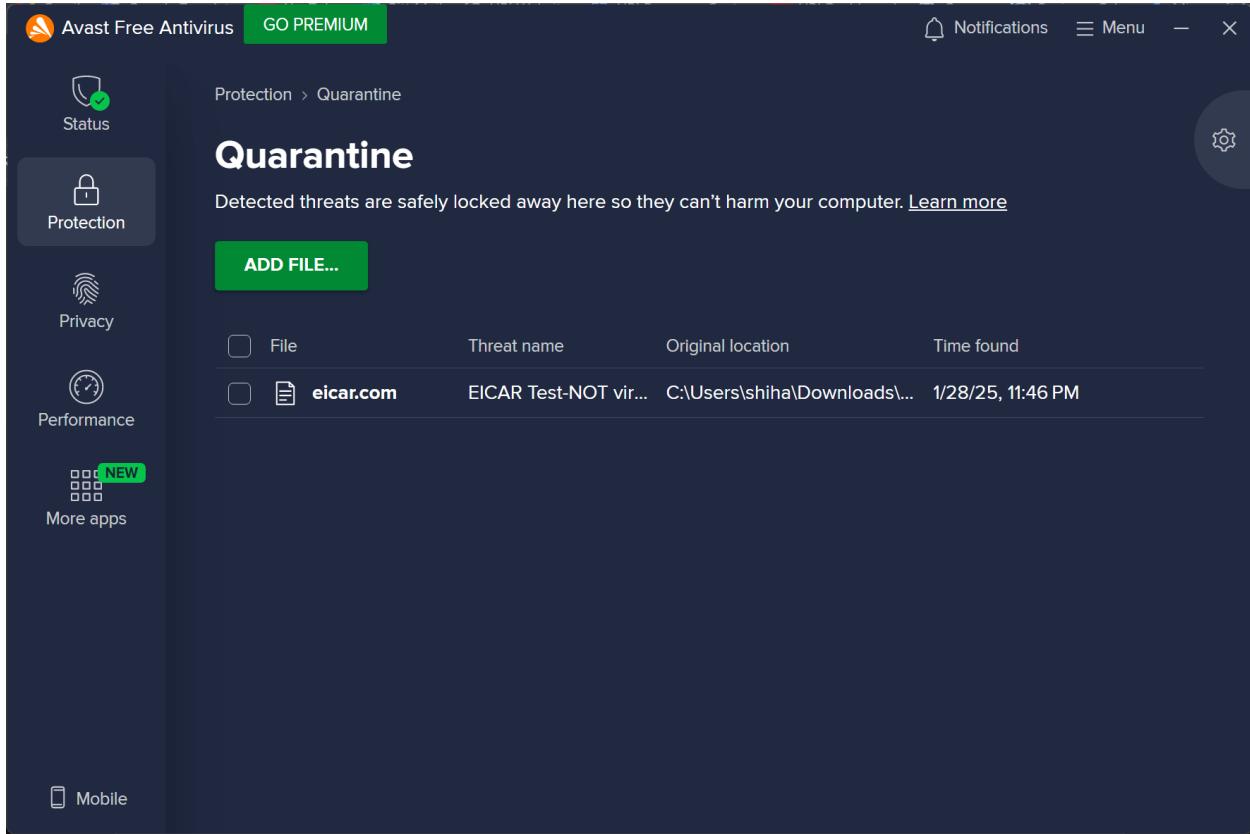
17. Did your malware automatically delete or quarantine the eicar file once it was detected? If so, which one? Yes, it automatically quarantines the “eicar.com” application after I extracted the file.



18. Were you given a choice on what type of action your malware protection would perform to the file? Nope, it did not prompt me with any choice, it just notified me, just like Microsoft Defender, that the file is malicious and deleted the file. But I can go into quarantine and restore the file or operate other actions.



19. Does your malware protection show a history of detection / actions taken? Yes, it does show me a history of detection and operation.



Be sure to include screenshots to support each of your answers!