Problem Statement:

To analyse my own spyware, that is a key-logger, captures screen and camera

Tools Used:

1. Windows McAfee
2. VirusTotal

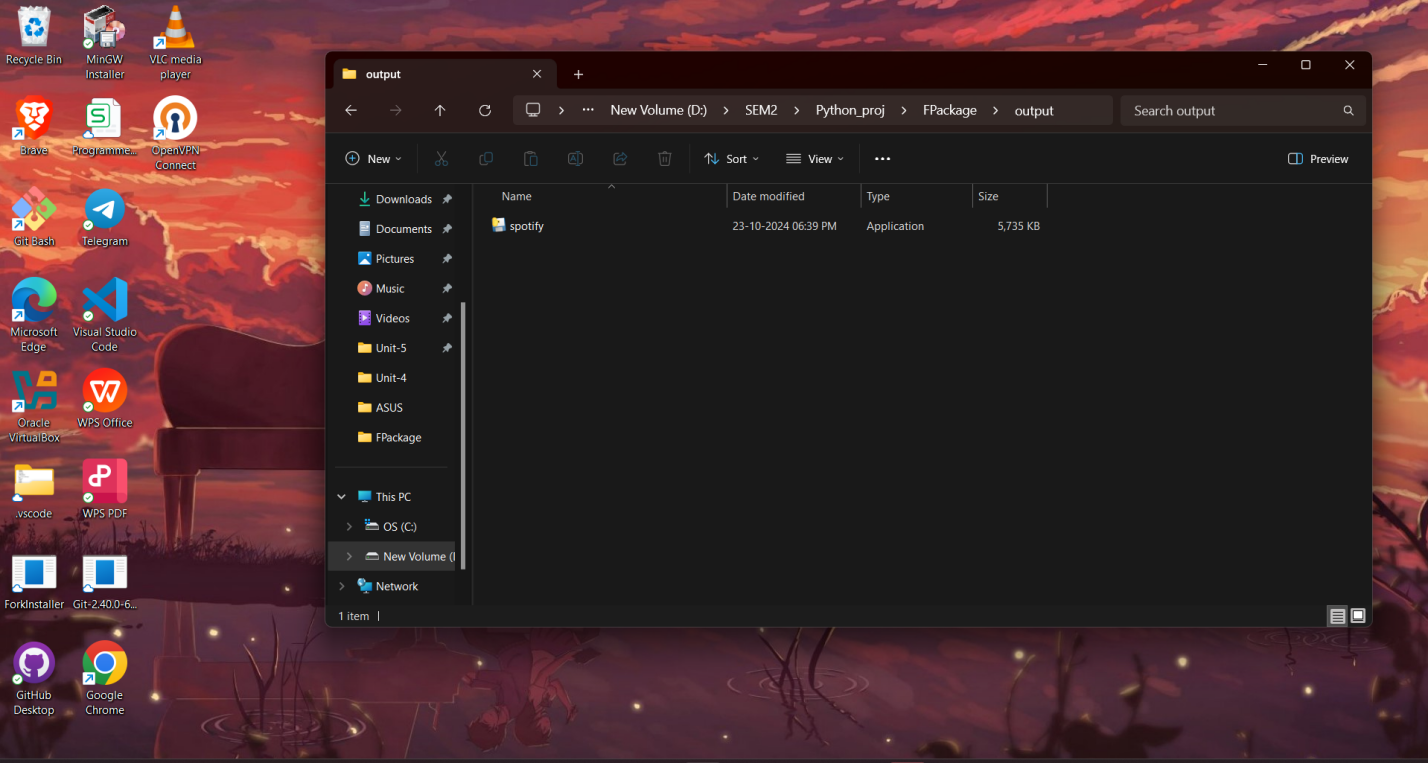
3. Ghidra

4. PEstudio

5. Wireshark

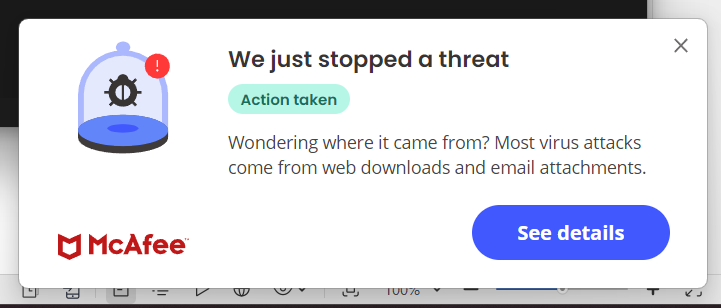
Analysis Done with screenshots:

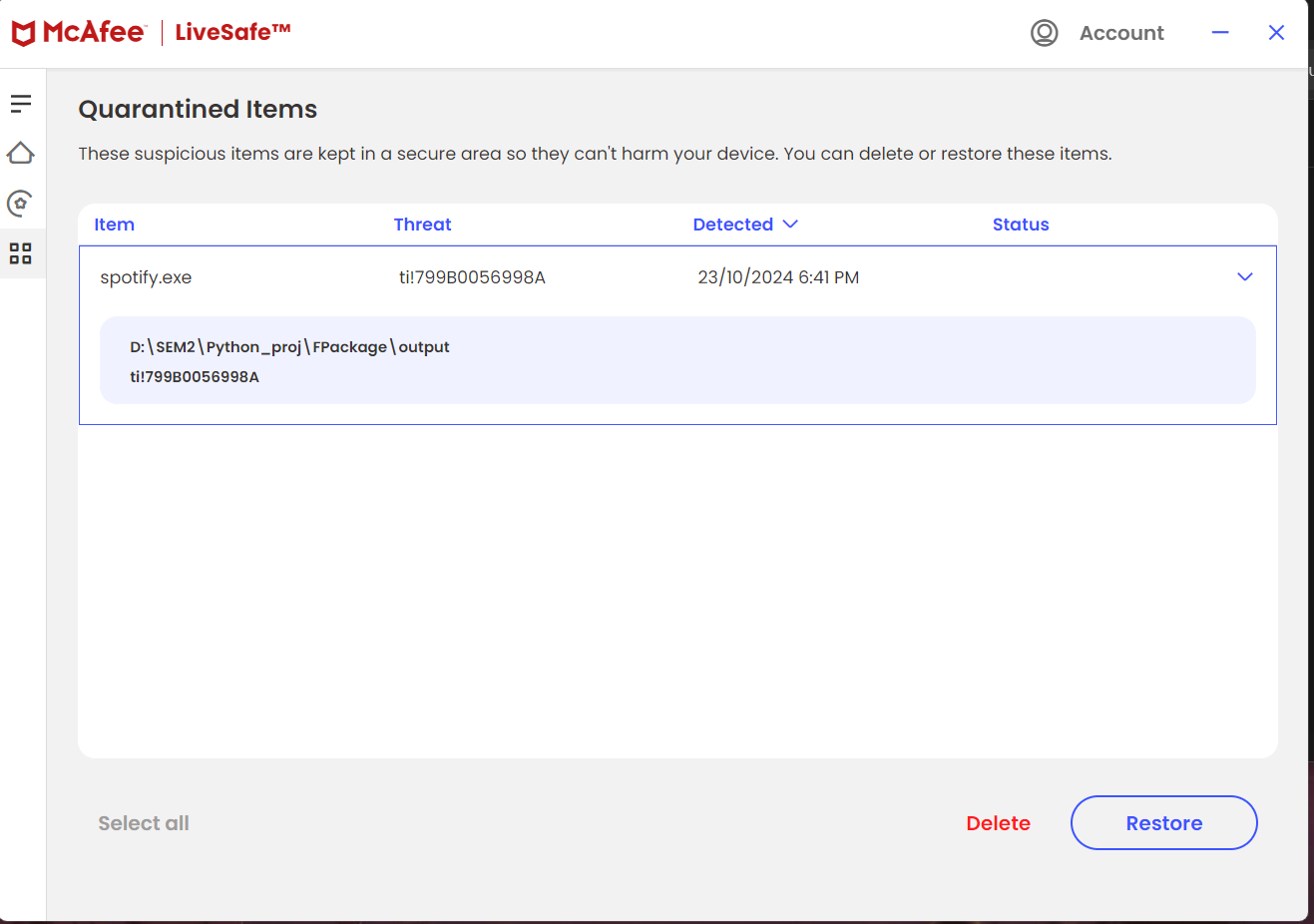
1. First I make sure that my malware file is active



This is the malicious .exe file.

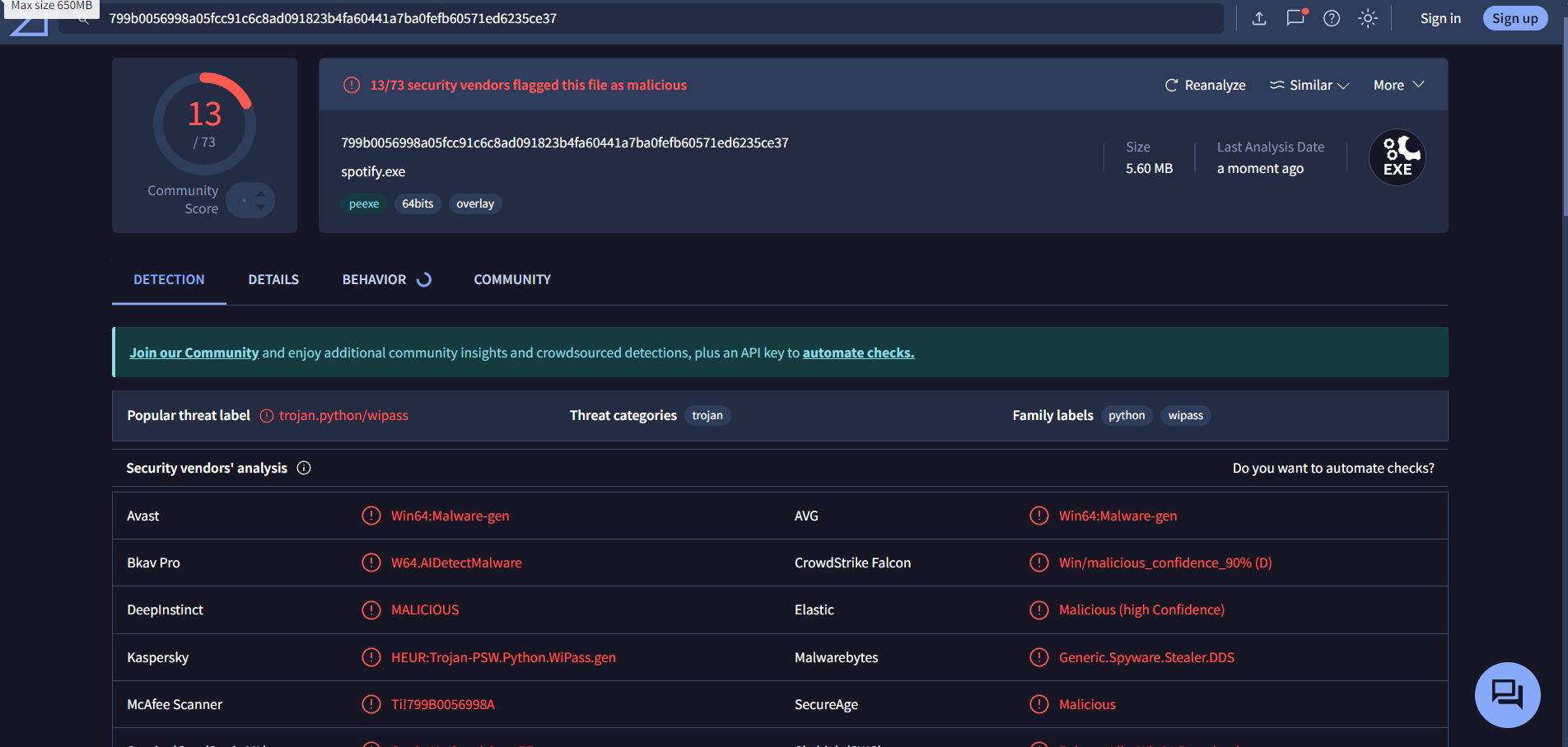
We run it. But our system’s inbuilt virus software quarantines it.



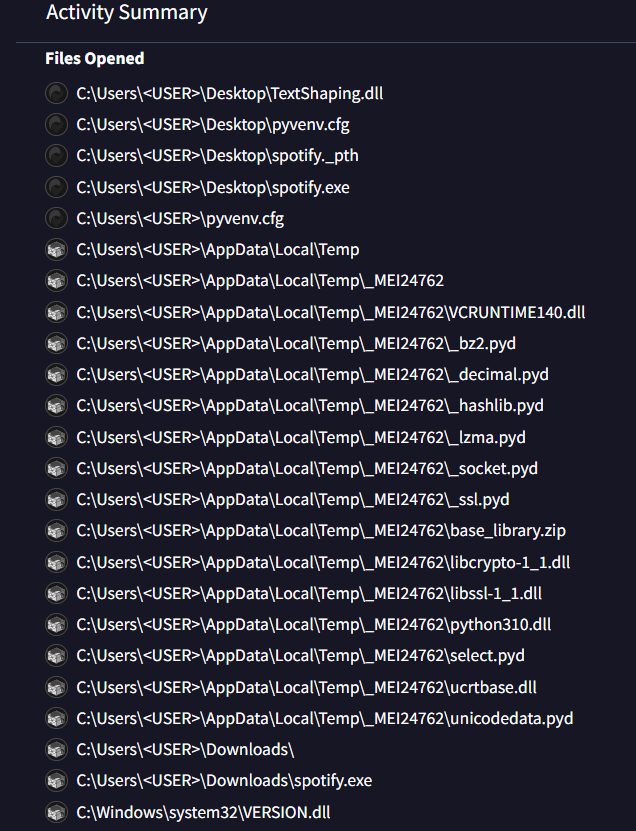


So we restore the file and turn off the virus detector

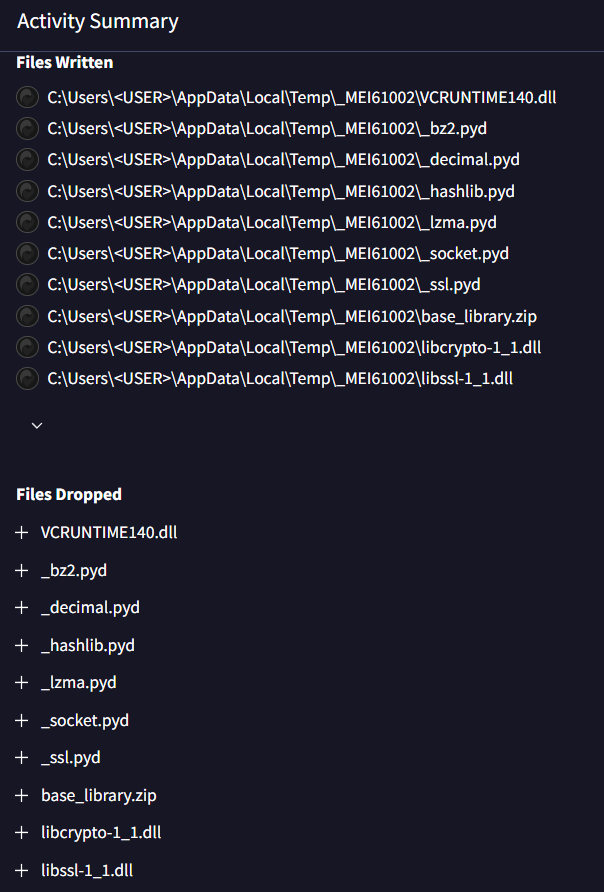
1. We upload the malware file to VirusTotal



We can see that out of 73 antivirus software of VirusTotal 13 of the reported the spotify.exe as malware.



[Turn to next page]



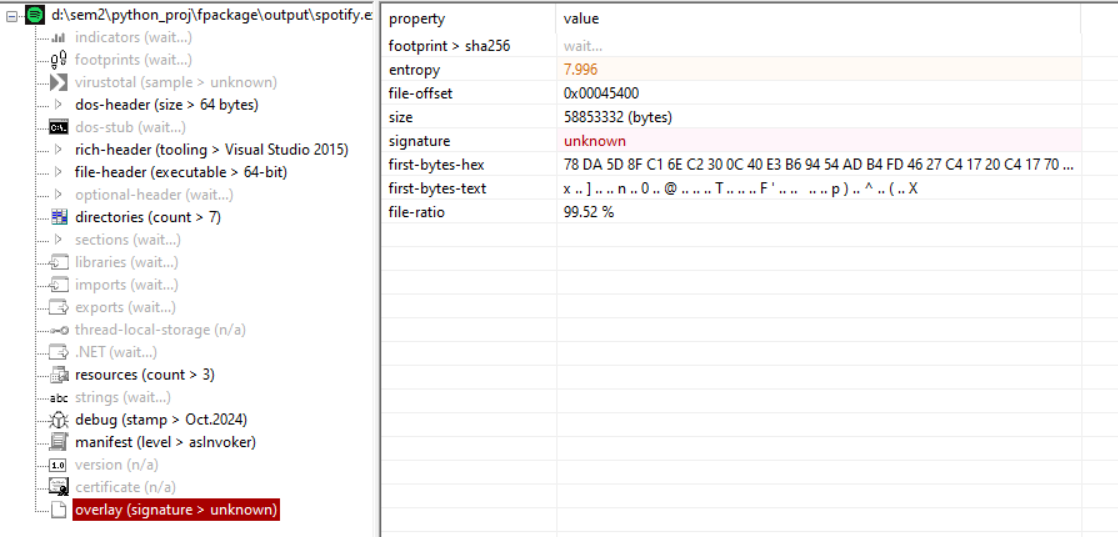
We can see that the temp folder is being used for logging purpose.



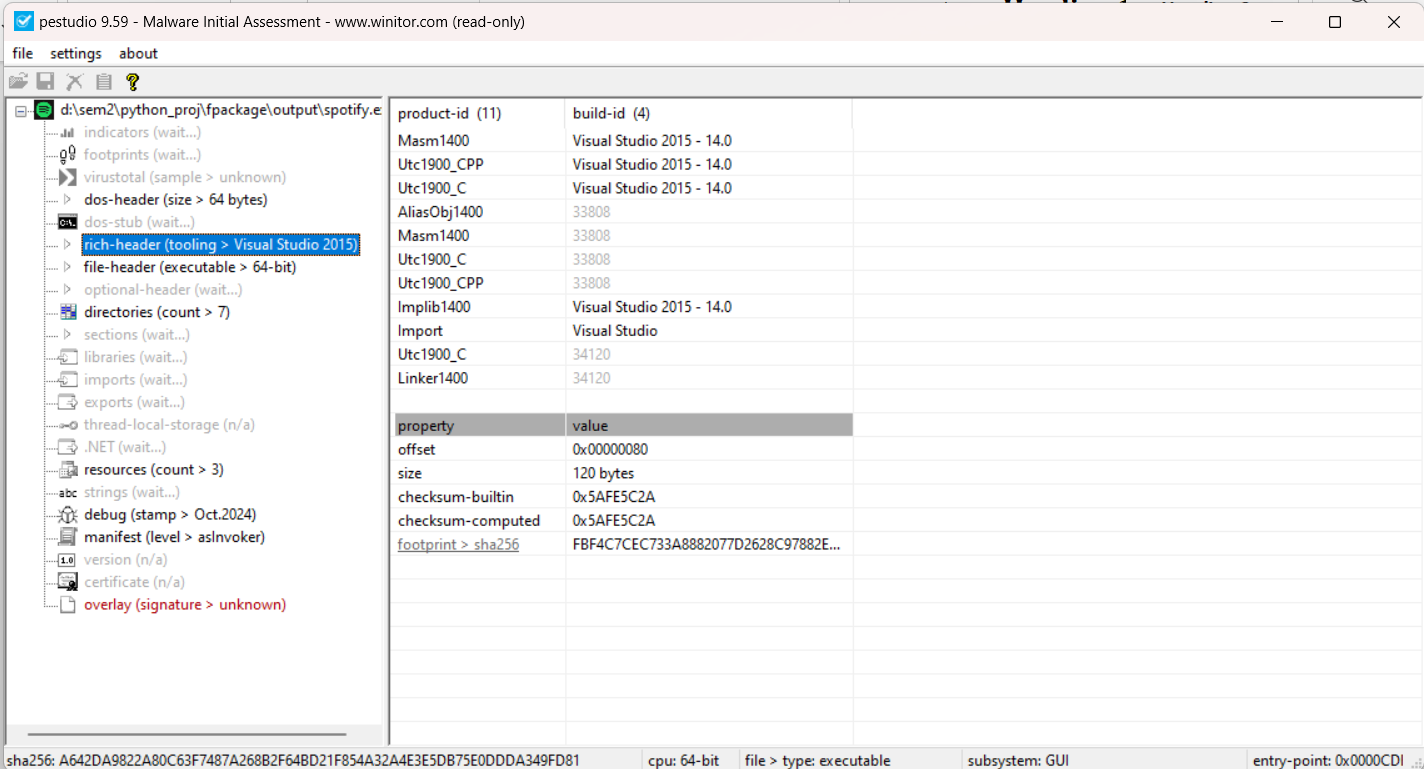
Sigma Rules detect that the source code is python and its attempting a side loading attack

1. Next we upload the file to PEstudio

We check for validness of signature

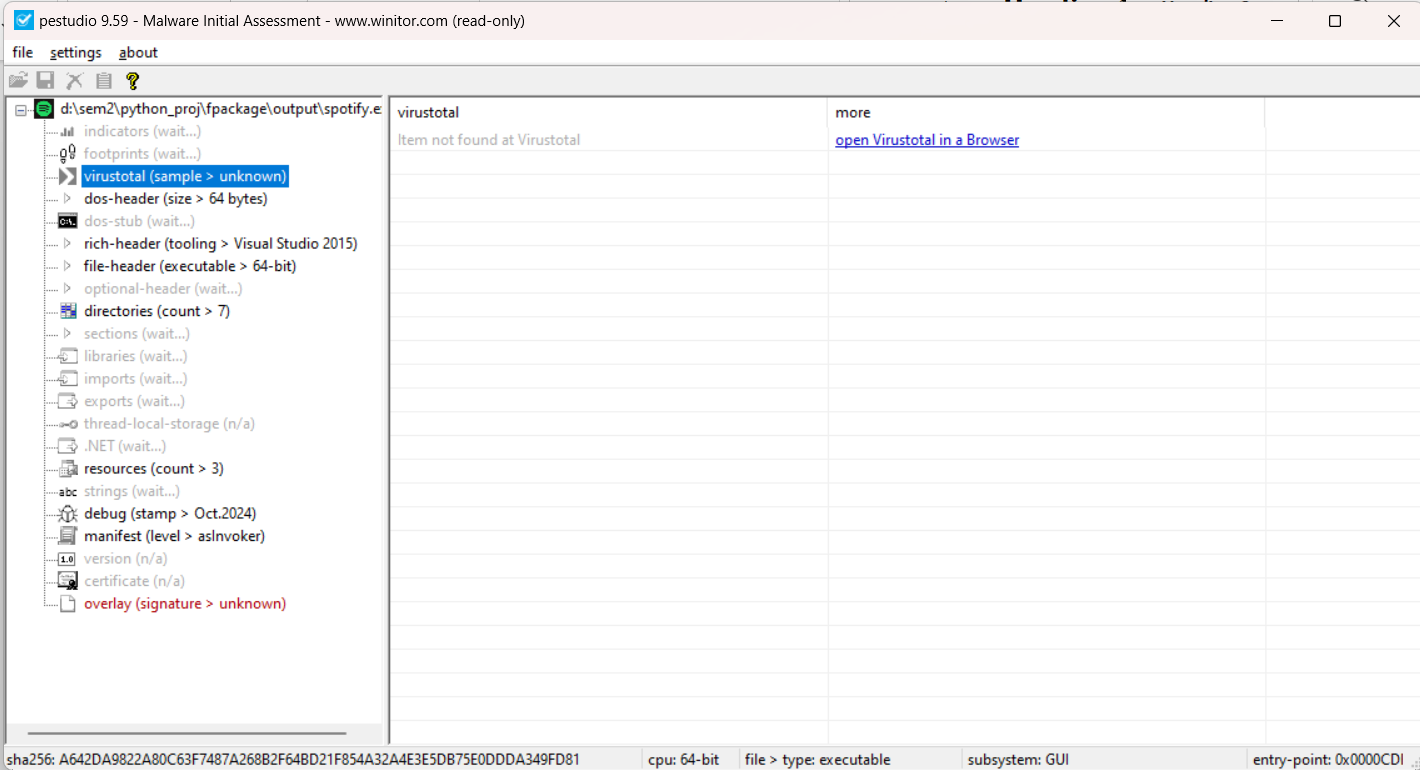


Signature is unknown. So possibly a malware or spyware

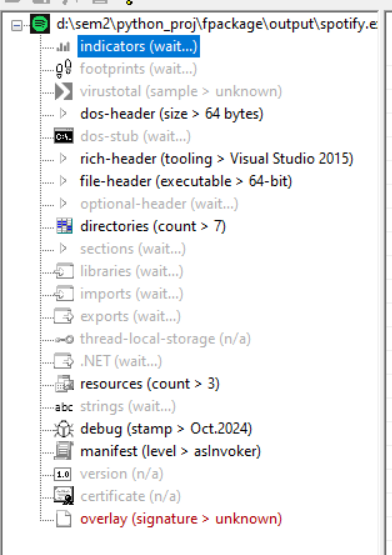


We can see that the software was written in Visual studio code and compiler there.

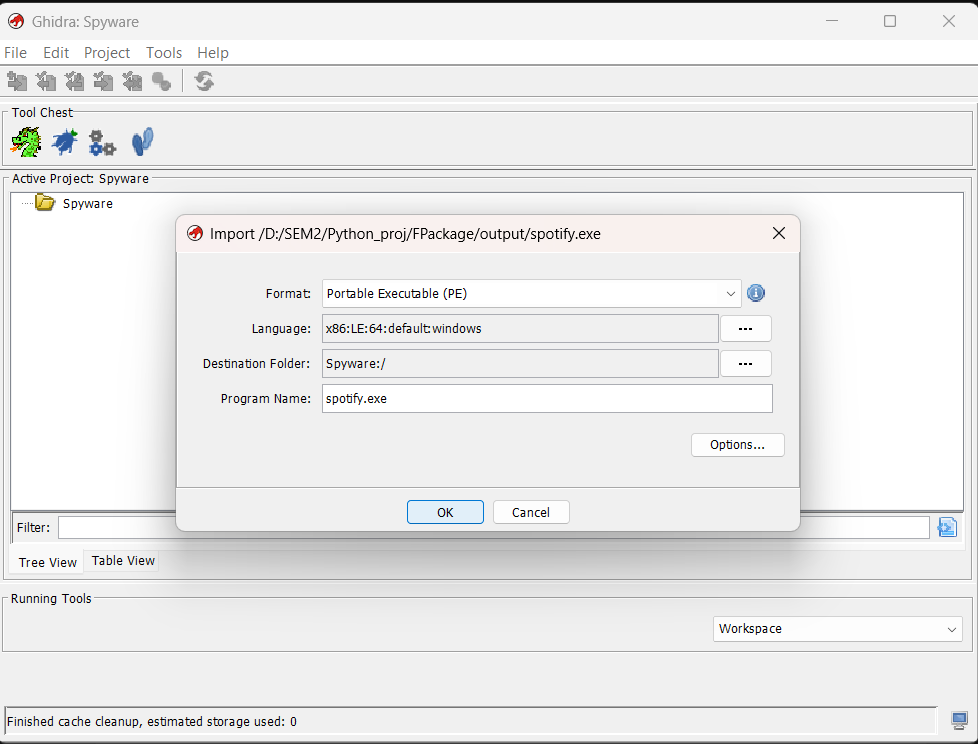
Since its own code it cannot be found in VirusTotal



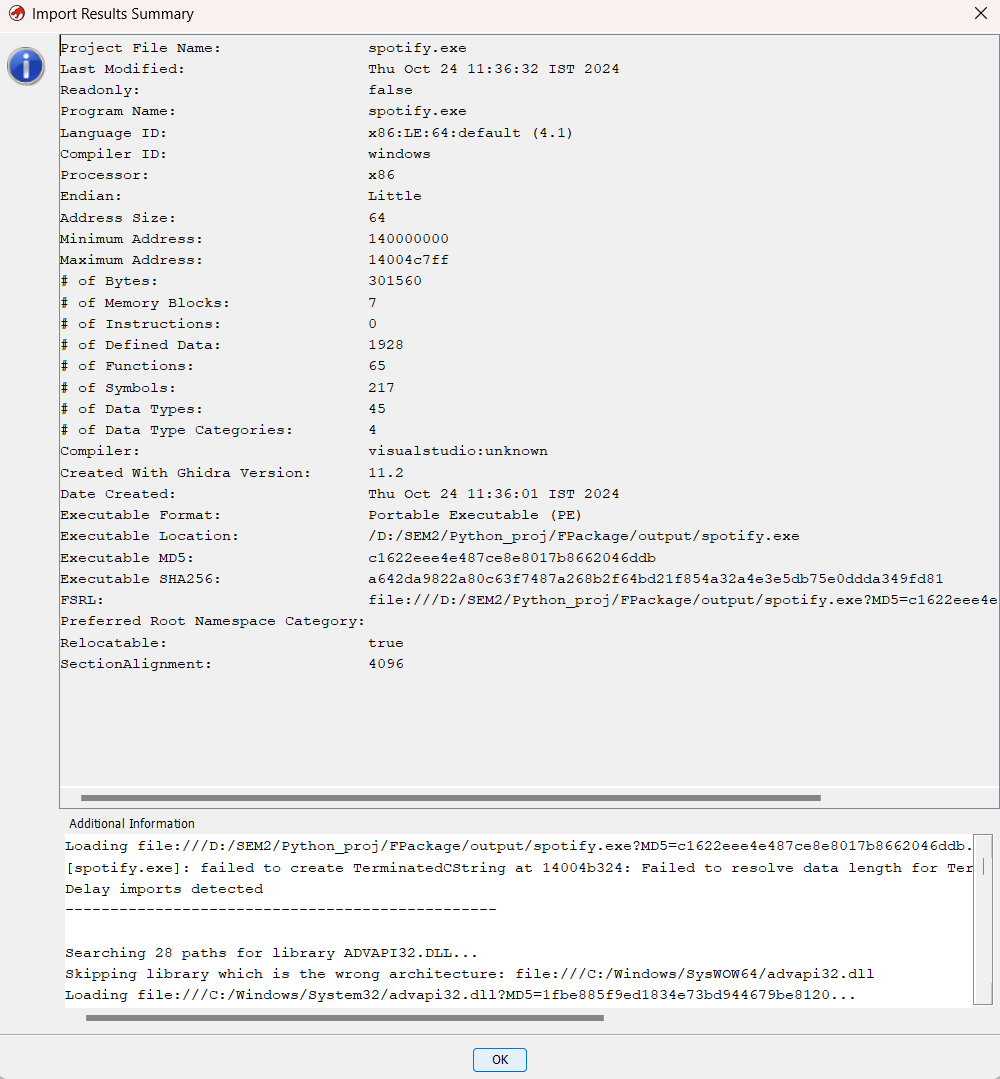
Also the version and certificate are unknown



1. Next we create a project in ghidra and import our file

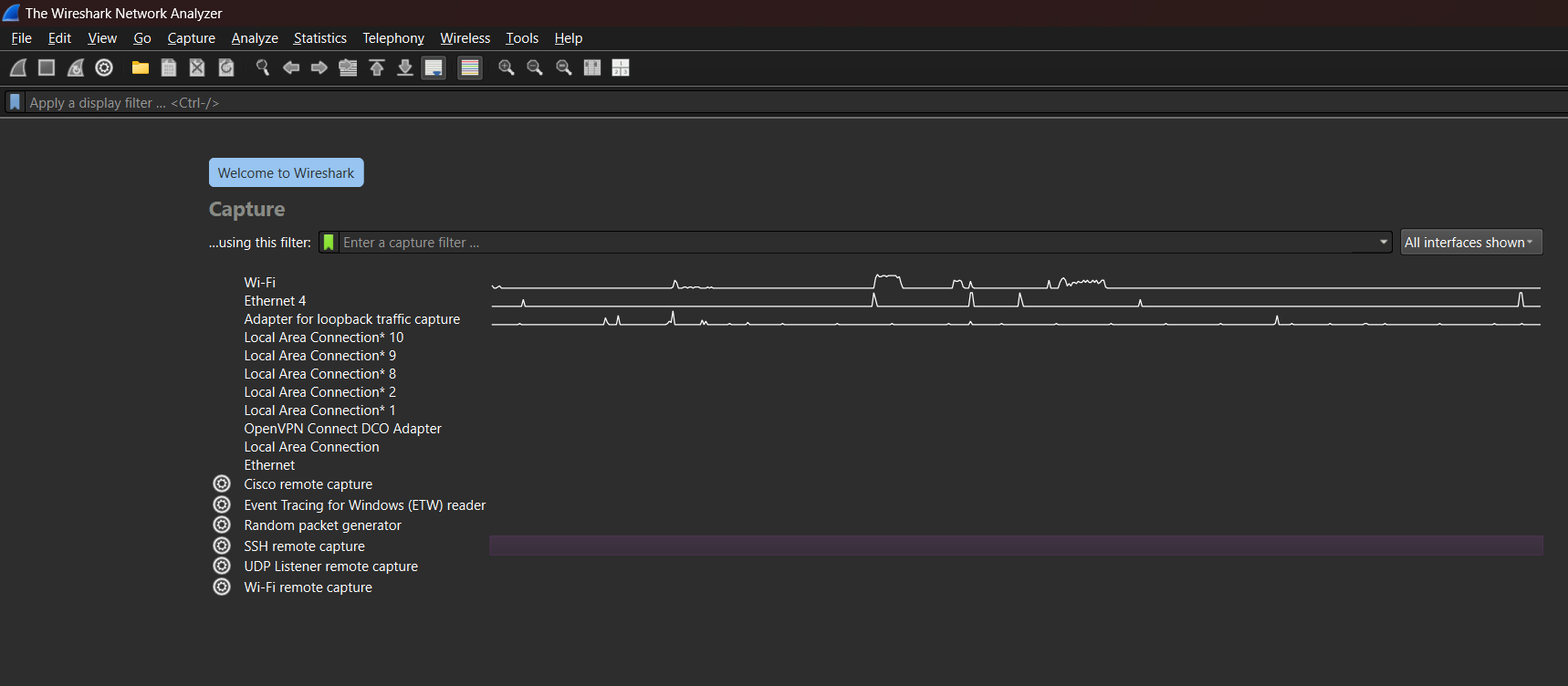


We get import summary after this:

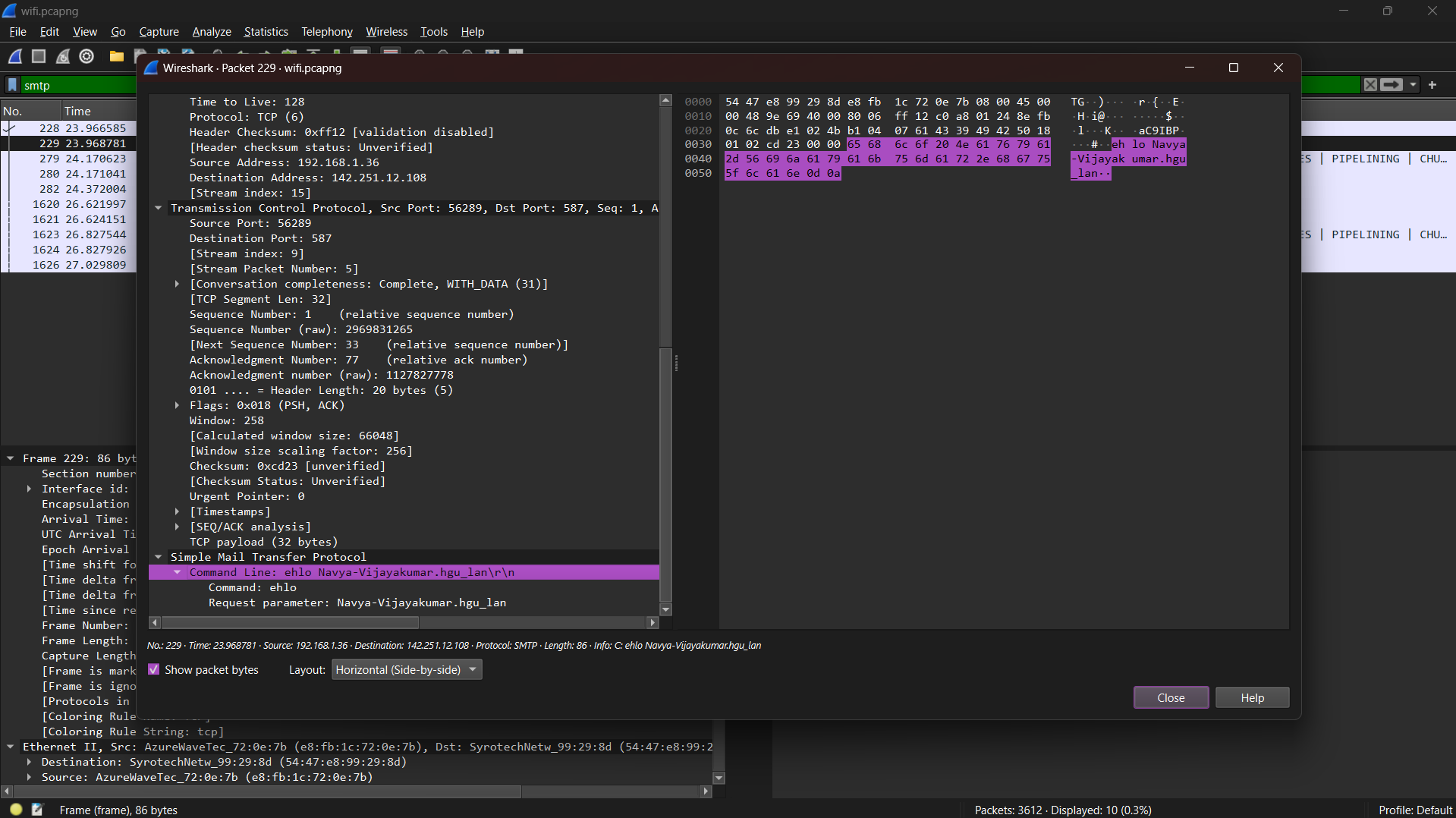


The malicious code was analyzed and left unpredictable in ghidra.

1. Wireshark is used to analyse the data packet sent by the spyware



We then run the spyware and start the capture filters of the WiFi



We can see that the mail has been sent through the command line of our windows

Action Taken with screen shot (If any) based on analysis: