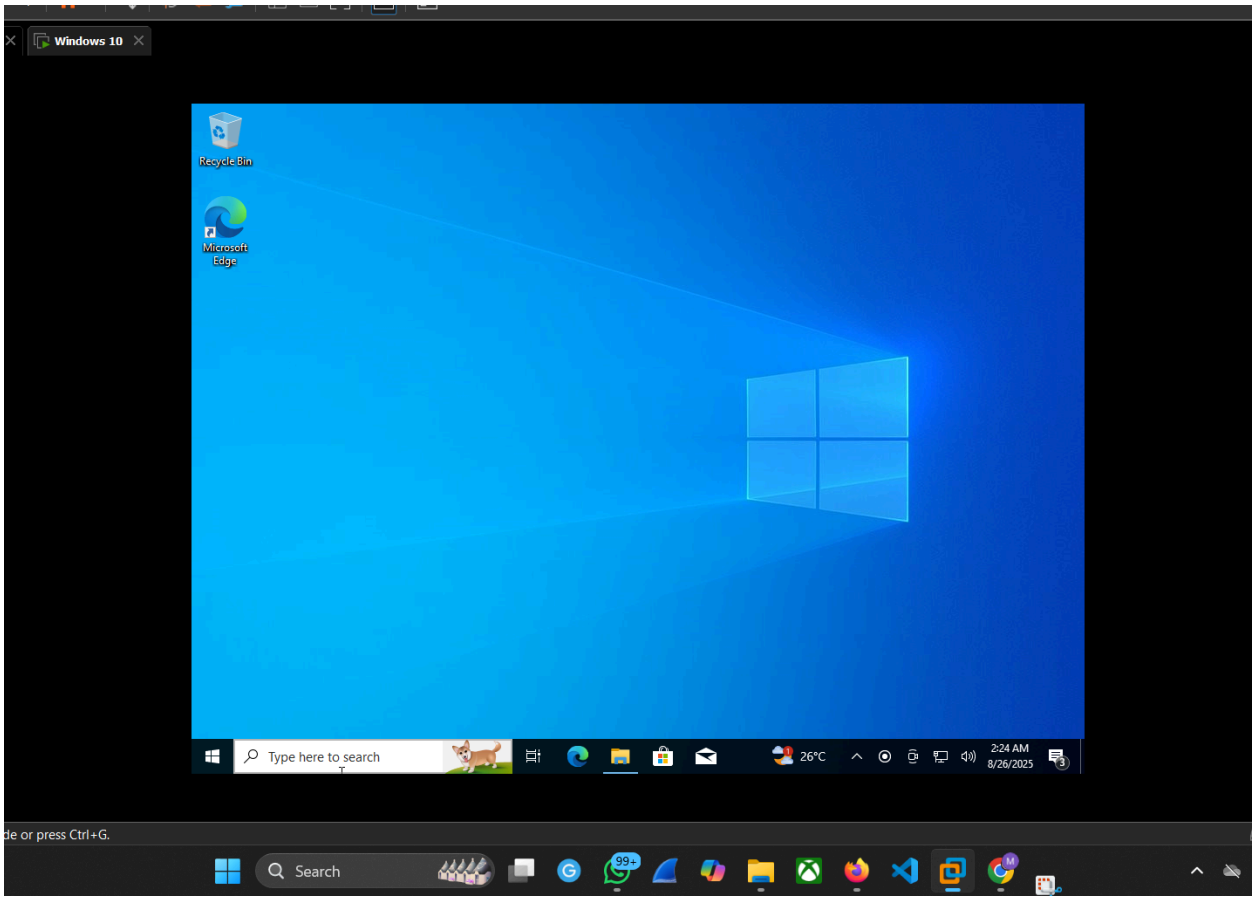
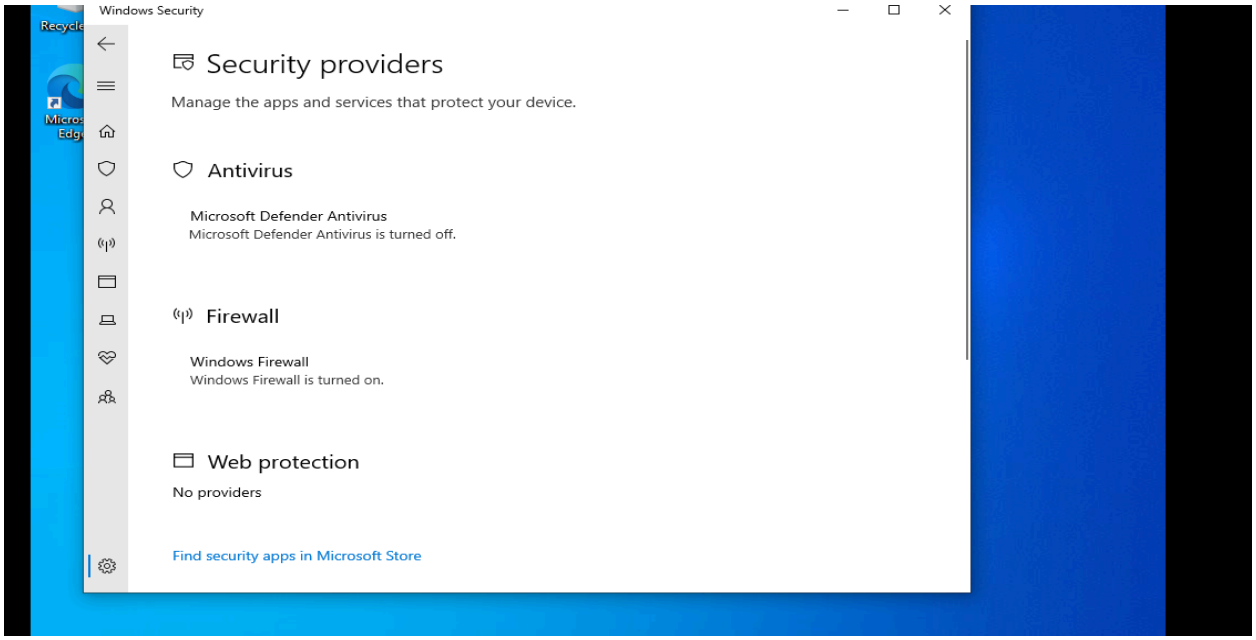
1.Installing windows 10 pro in VMware to set up flare vm

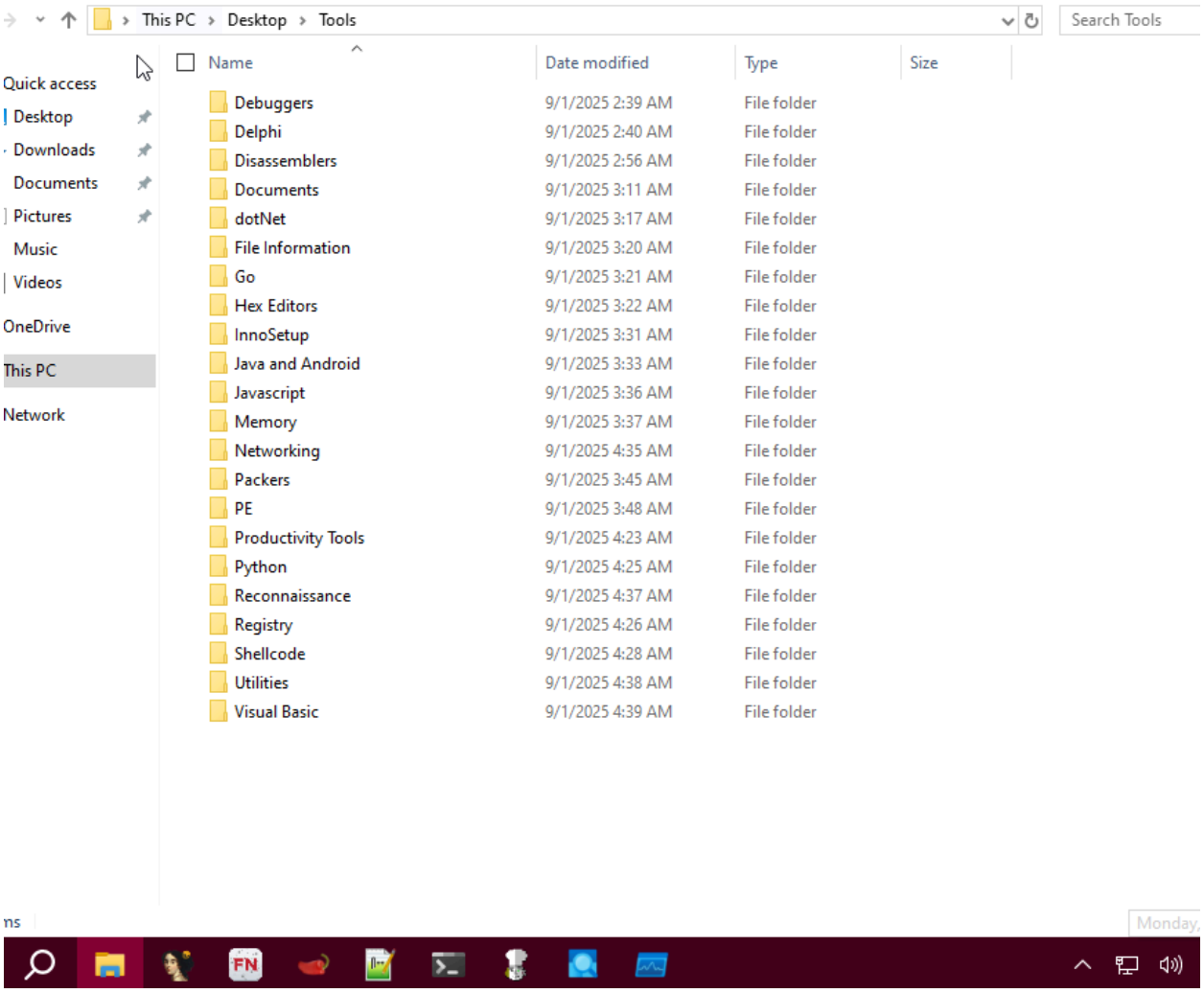


Setting up windows 10 pro by Disabling automatic updates and Windows Defender for a controlled malware analysis environment

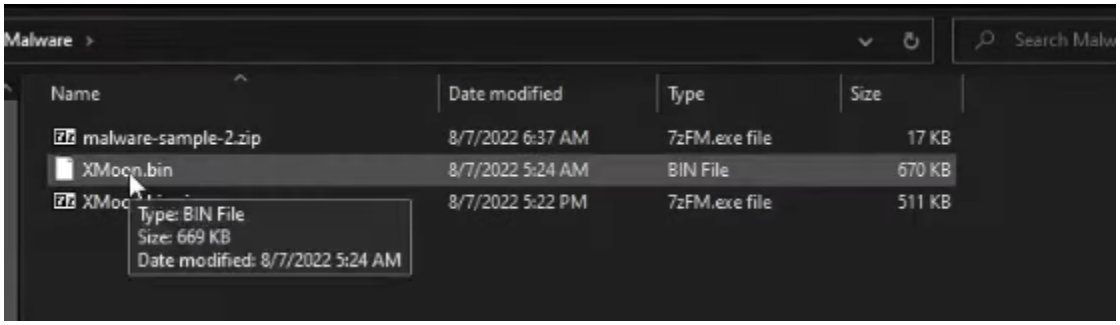


2.0 Installing flare VM and setup

All the tools that needed for Malware Analysis

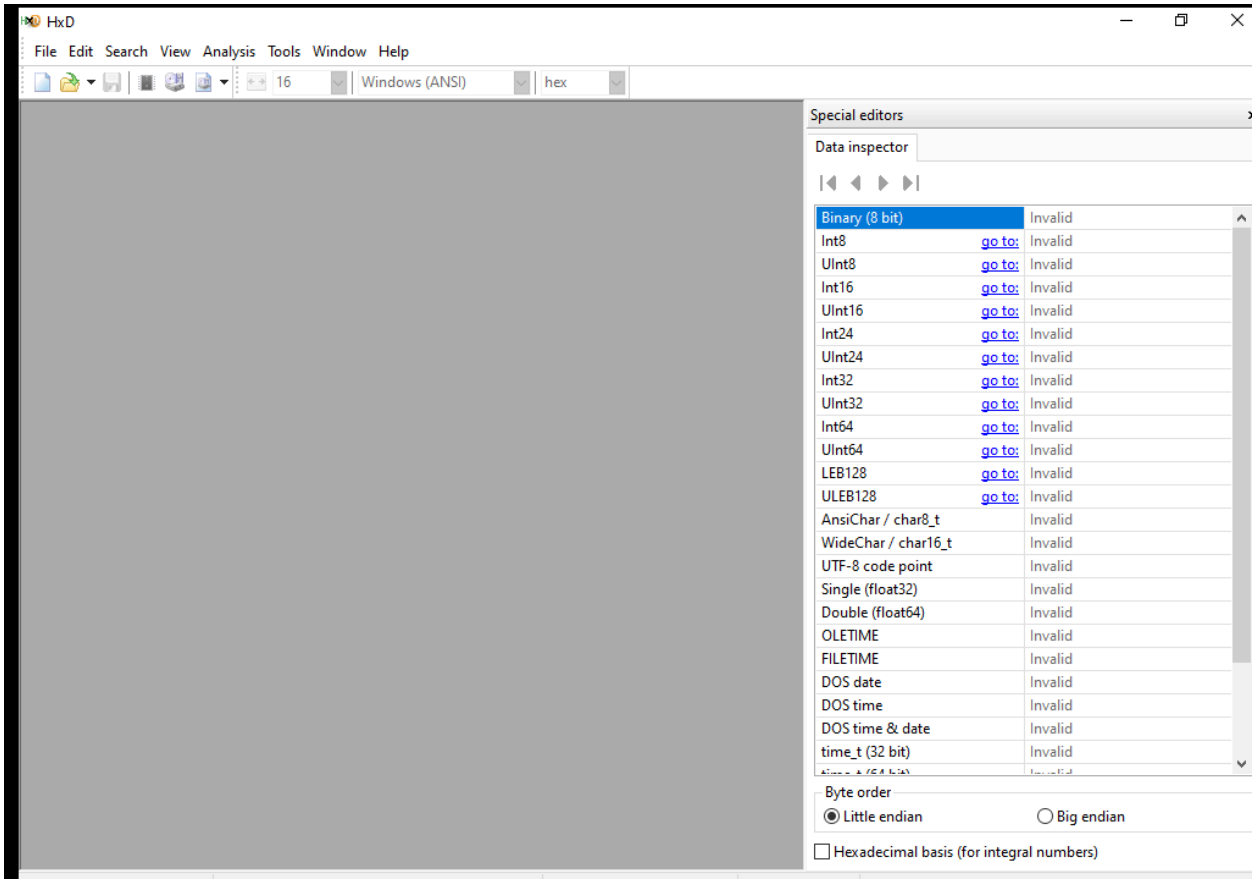


2.1 Taking two malware file samples :

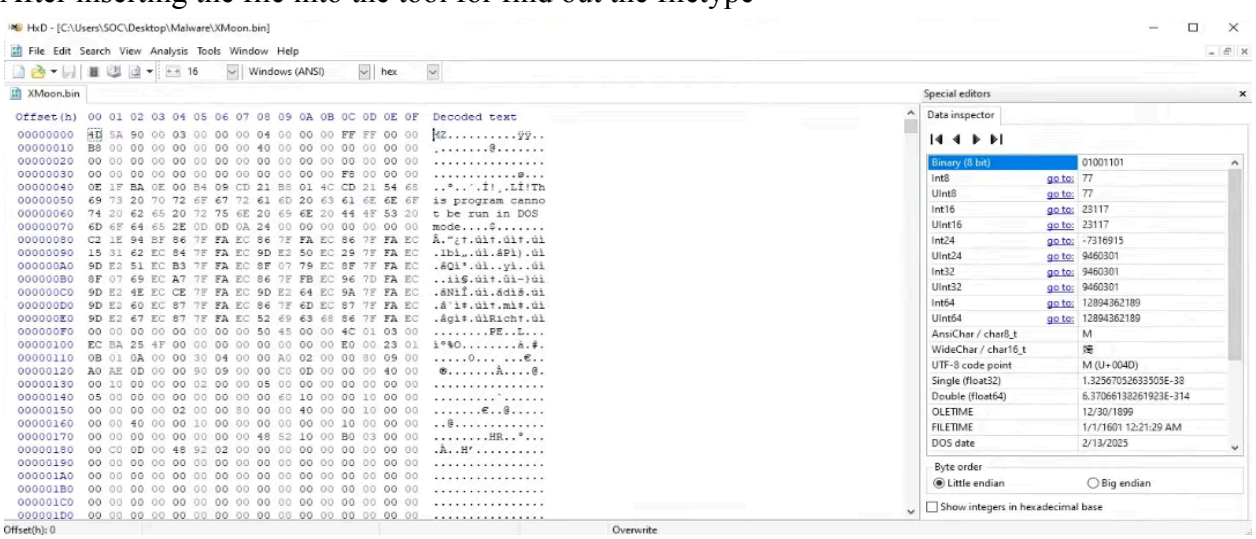


3.0 Filetype of the Malware :

To see the filetype we will use HxD tool



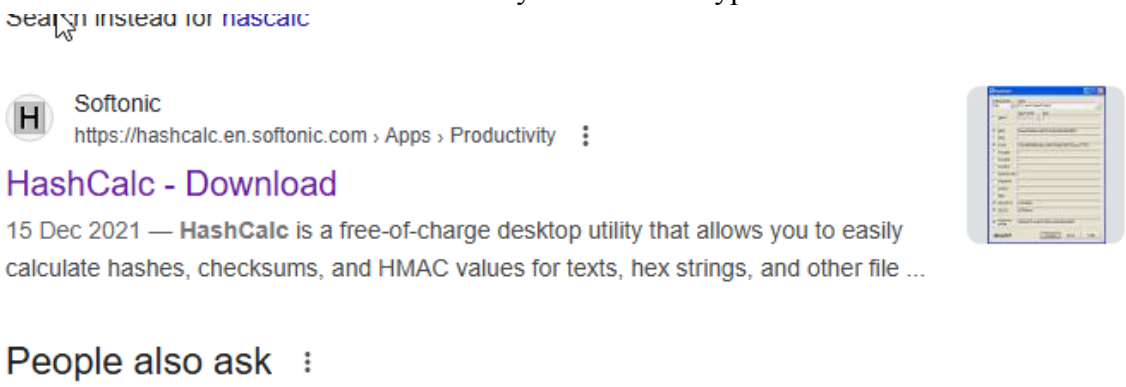
After inserting the file into the tool for find out the filetype



We can see the signature 4D 5A which is an executable file which may contain malware , it can be an image file , so we can use that tool to find the signature and see if it's an executable file .

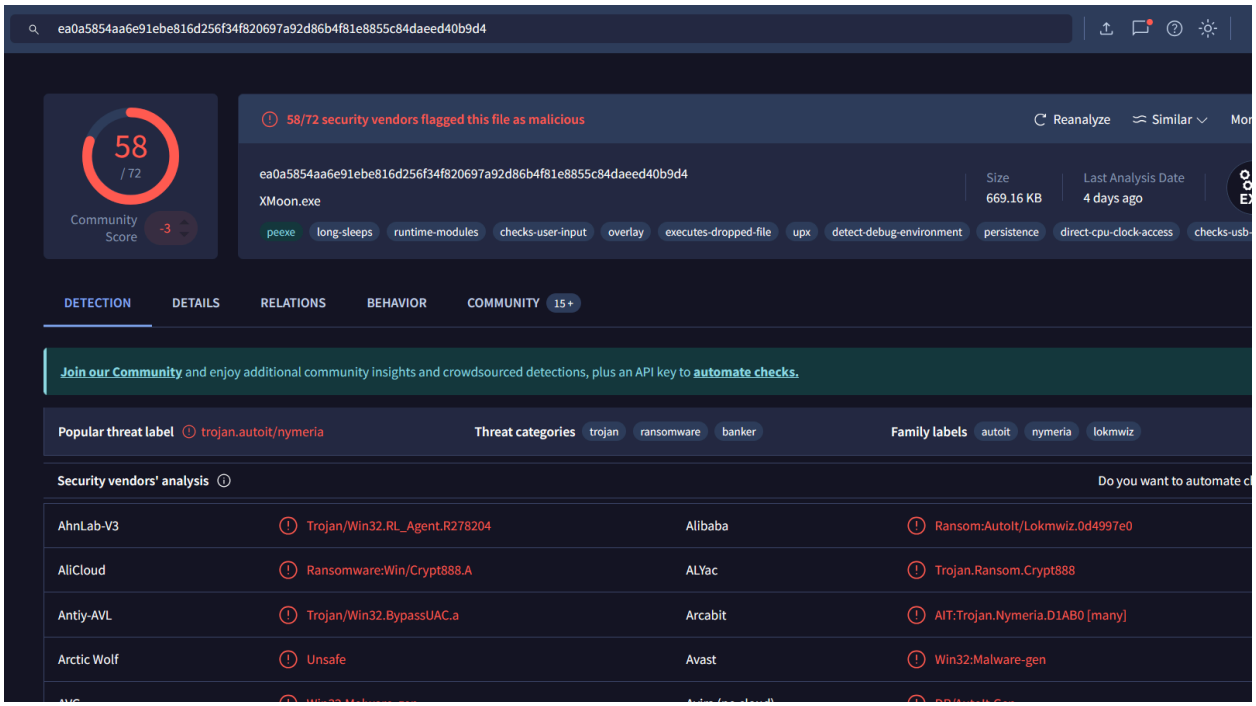
3.0 Fingerprinting the malware :

We will use the hascalc software for identify the malware type



3.1 Using Virustotal

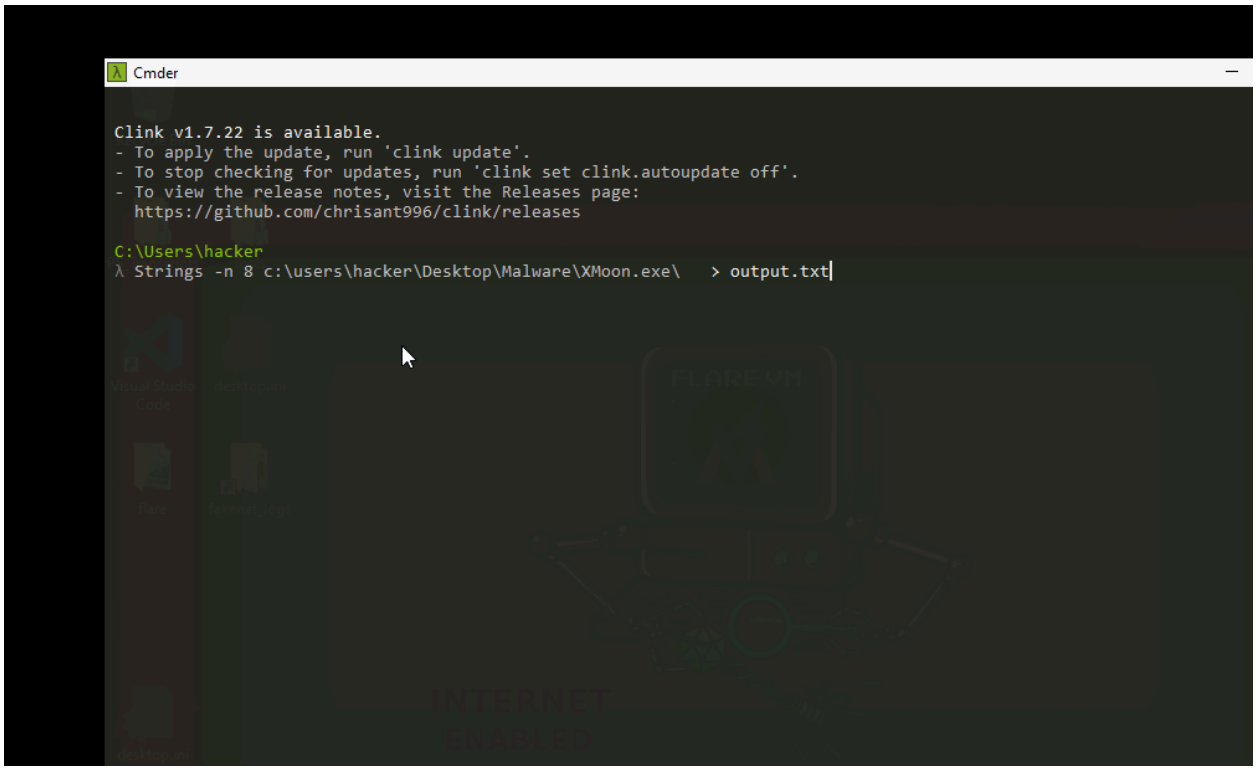
After getting the hash number of the malwere file as *ea0a5854aa6e91ebe816d256f34f820697a92d86b4f81e8855c84daeed40b9d4* and inserting the hasnumber into the virustotal software we find out that its a trojan malware



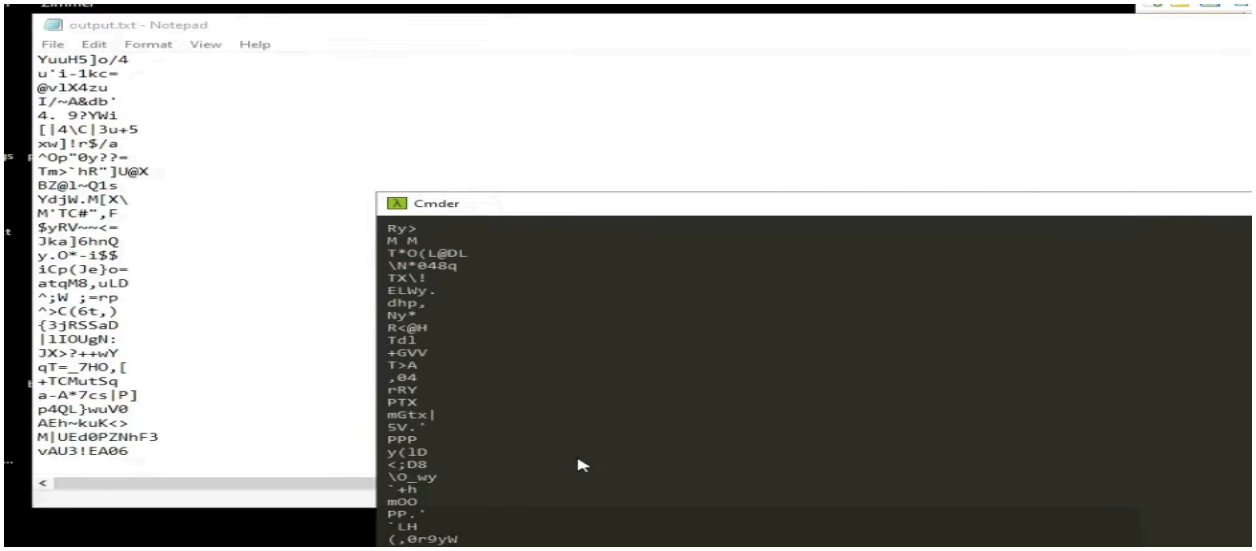
4.0 Strings

Now we will go through the malware file to know that what's inside the file the urls, the ip , windows API

Run this command in cmd tool to find out the string in output.txt



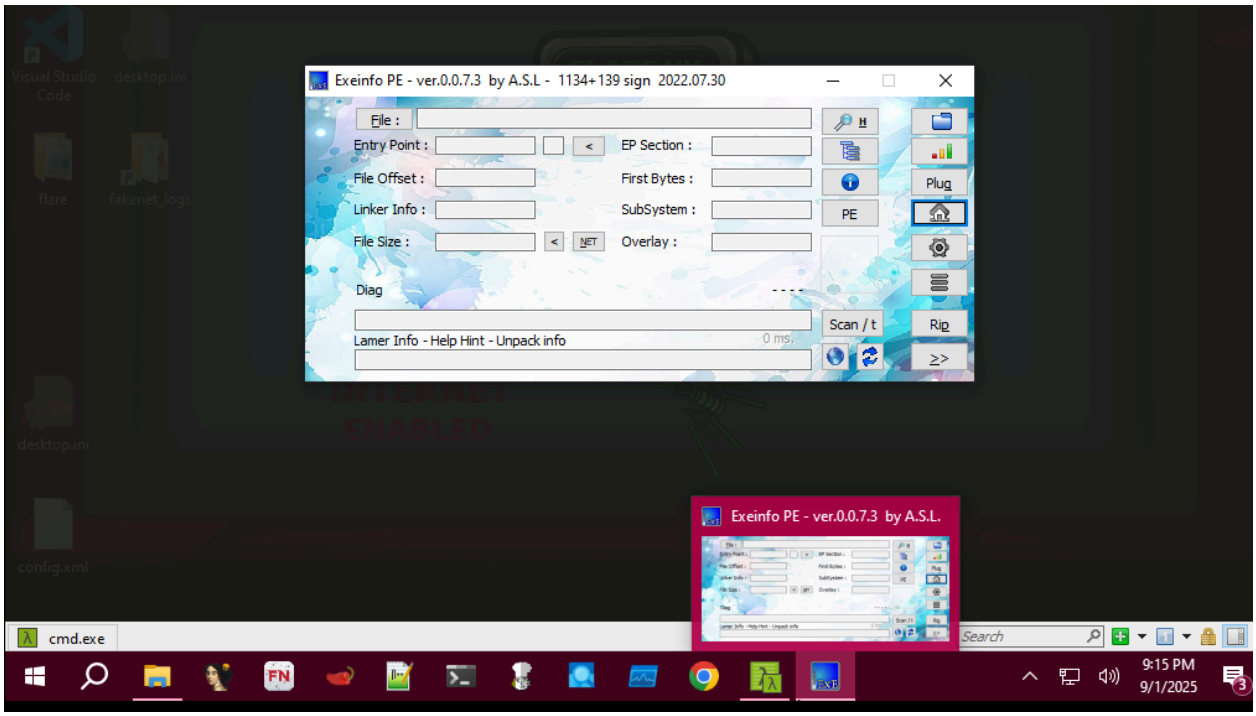
Then we will find out the output where the string of ip address, api will be included

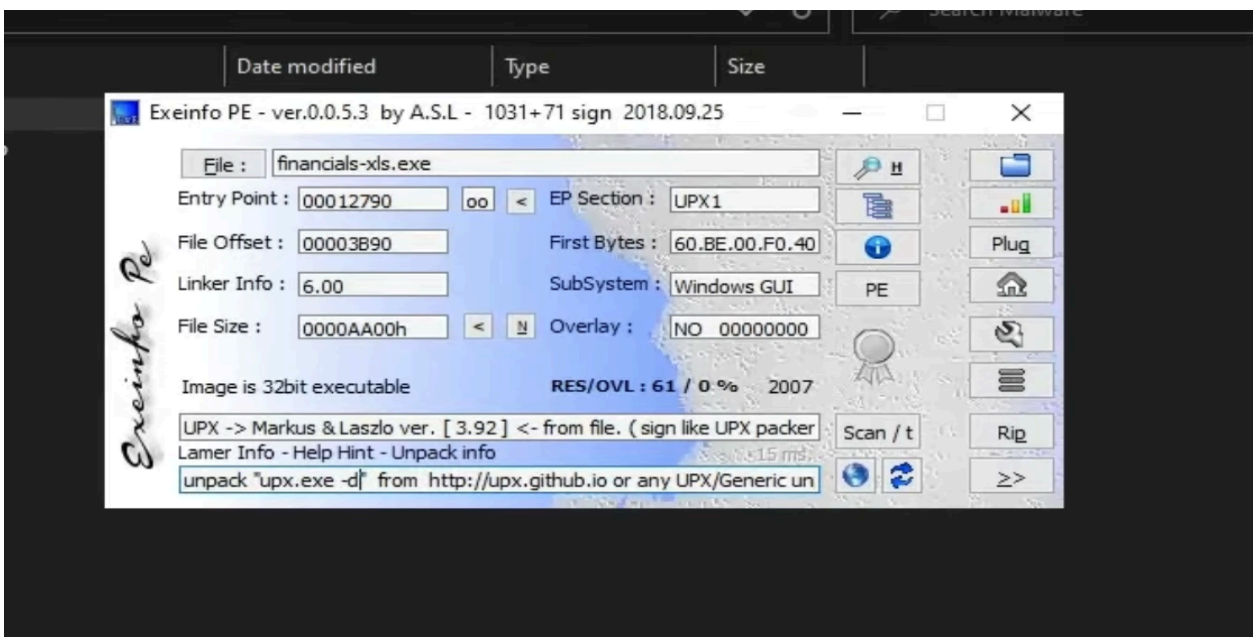


5.0 Packing

In malware analysis, packing is a technique used by attackers to obfuscate malware code by compressing or encrypting it to evade detection by antivirus software and hinder analysis.

So we gonna check it now with **exeinfo tool**





From here we know that what packing technique the attacker used , its using UPX to hide itself , from the tool we also know that how to decode the pack as Lamer info

Now we gonna unpack it using the command

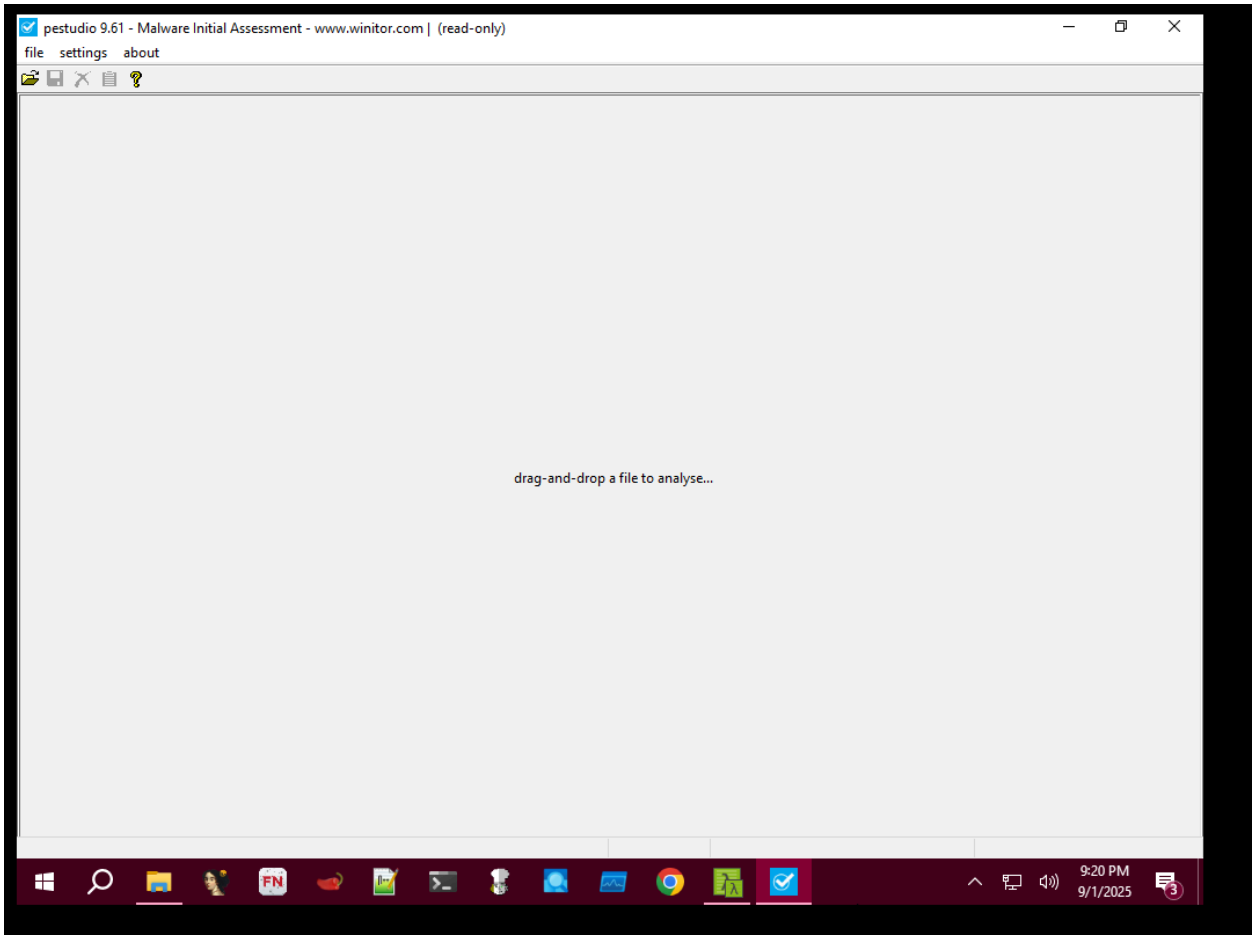
```
λ upx -d -o UnpackedMalware.exe financials-xls.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     57344 <-     43520   75.89%    win32/pe     UnpackedMalware.exe

Unpacked 1 file.
```

6.0 Pestudio

PeStudio is used for the static analysis of Windows executable files (like .exe, .dll) to identify potential malware and suspicious artifacts without actually running the file, its like all in one



Let's use the tool by dropping the malware file here