**Malware Analysis:**

Malware, short for malicious software, refers to any program or file that is intentionally designed to harm a computer, network, or server. It can steal data, damage systems, or take control of your computer without your permission.

**Types:**

**Viruses -** A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system.

**Worms -** Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves.

**Trojan horse -** A [Trojan horse](https://www.geeksforgeeks.org/computer-networks/trojan-horse-in-information-security/) is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game.

**Ransomware** - [Ransomware](https://www.geeksforgeeks.org/computer-networks/difference-between-malware-and-ransomware/)encrypts data in the computer with a key that is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data.

**Adware** - It displays unwanted ads and pop-ups on the computer.

**Spyware** - Its purpose is to steal private information from a computer system for a third party.

**Rootkits -** A [rootkit](https://www.geeksforgeeks.org/computer-networks/what-is-a-rootkit/)modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly.

**Keyloggers -** Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

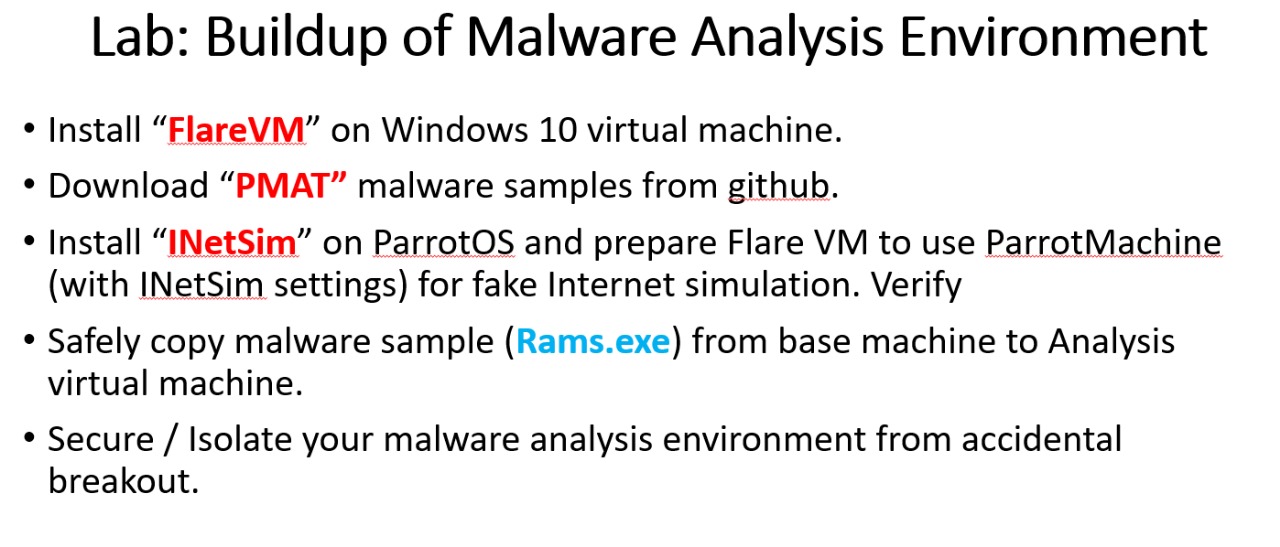
**What is Malware Analysis?**

**Malware Analysis** is the process of examining a suspicious file or URL to determine its functionality, origin and potential impact.

This involves understanding how malware works and identifying its behavior.

**Types of Malware Analysis:**

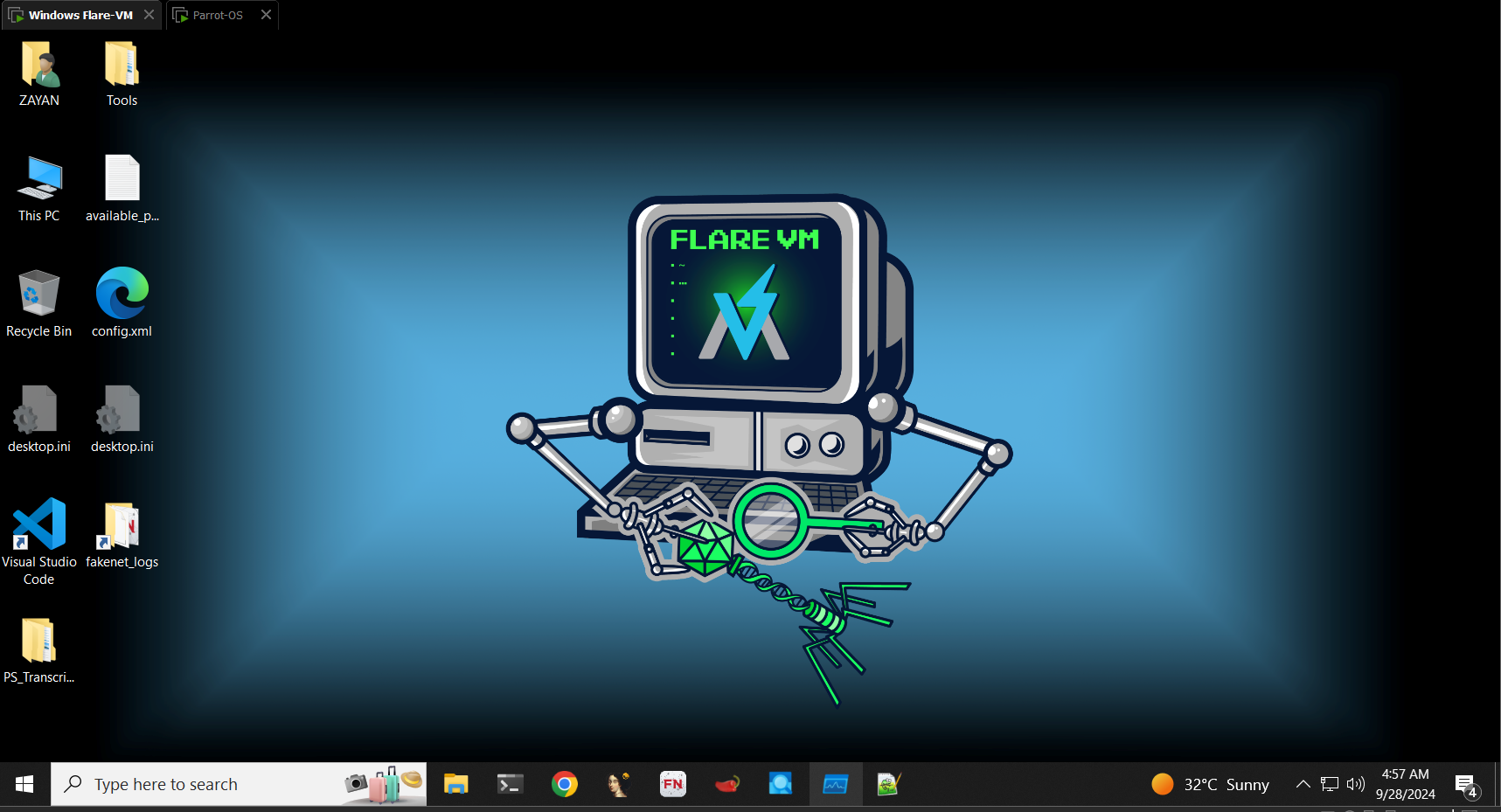
* Static Analysis
  + Analyze malware without executing it
* Dynamic Analysis
  + Analyze malware by executing its source code



**Installation of Flare-VM:**

1. Download Flare-VM from Github > Extract it >Run powershell as an administrator >Write this command **Set-ExecutionPolicy Unrestricted**
2. Navigate to the folder where flare-vm is **cd .. > cd .. > cd ZAYAN > cd Downloads > cd flare-vm main > .\install.ps1**

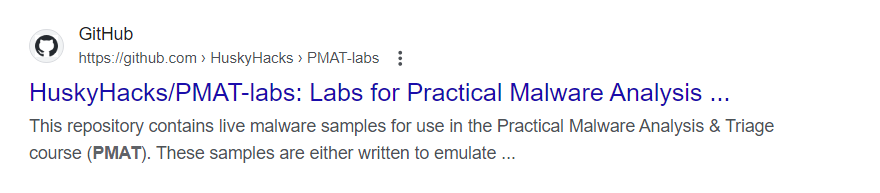
It will start installing VM.

****

It will look like this after installation.

**Installation of PMAT Labs:**

1. Search for pmat labs



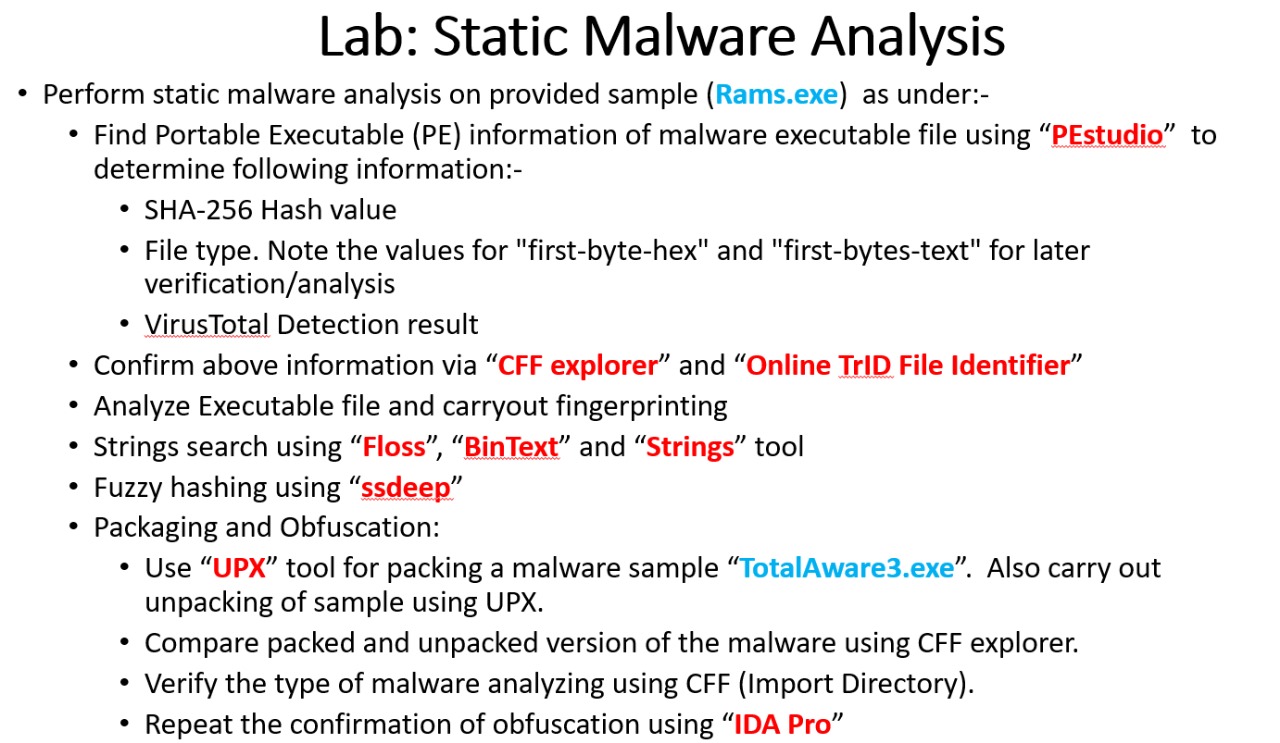
1. Search on github pmat –labs (Husky hacks )> click on souce code .zip > download suspicious file from the history > extract >



1. Inside Pmat there is a folder of pmat labs > clicks on labs to see its content.

Remember: Do not open any file

**Static Malware Analysis:**



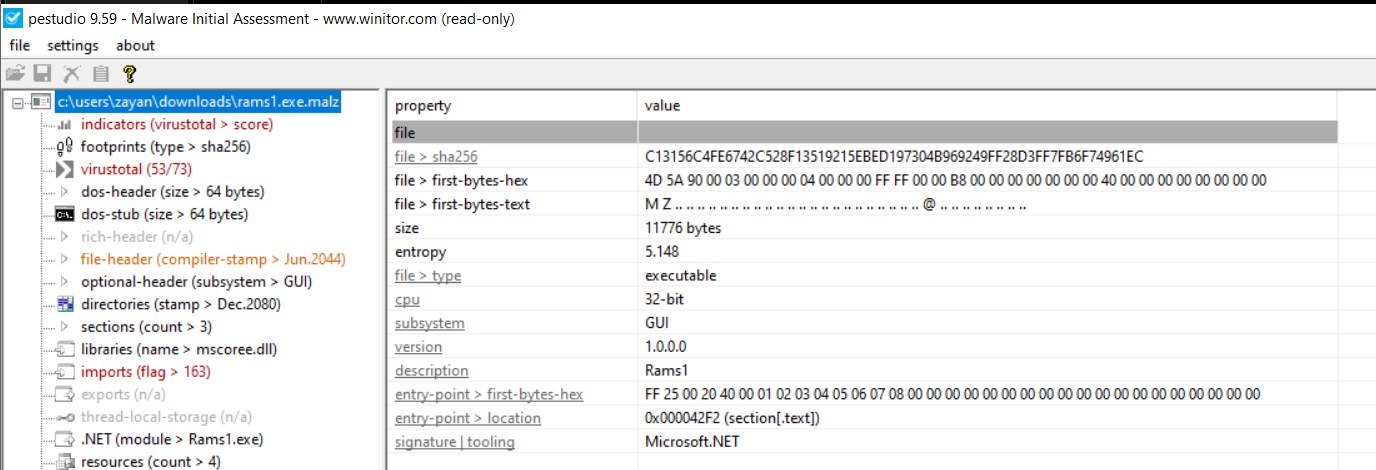
In Flare-VM > Tools > PE > pestudio > Run as an administrator

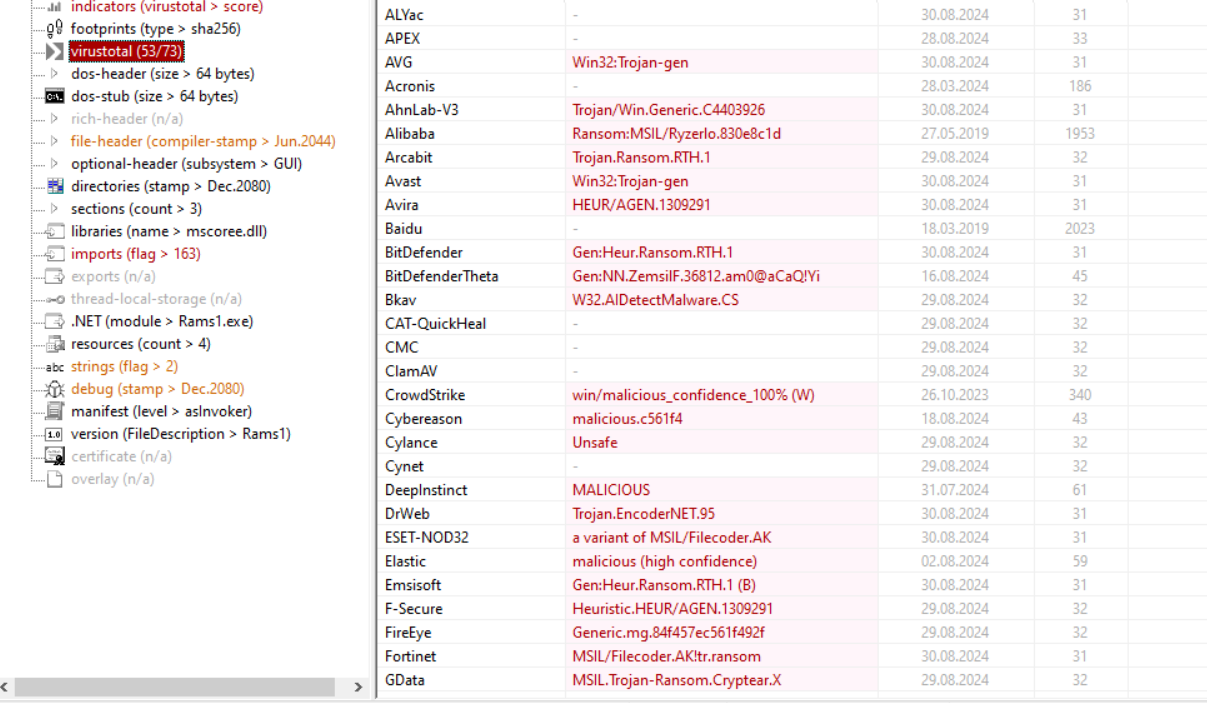
Put malware in this tool.

If we put malware in **pestudio**, it will extract information from it like type of hash, first byte hex, first byte text etc.

**First byte hex** will help us to identify which type of file it is. 4D 5A means it is .exe file

Look for **entropy** value to determine severity and randomness of this malware.

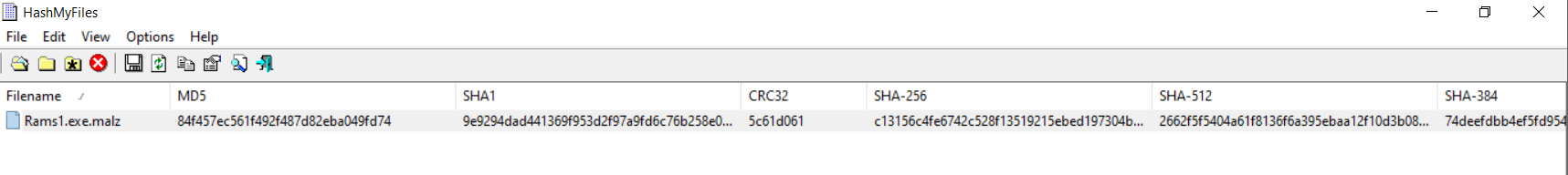




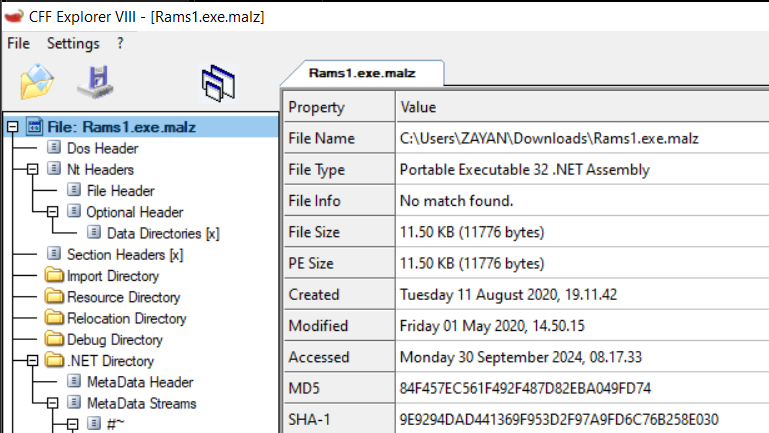
**Virus-total** telling us that 53 out of 73 components tell us that it’s a malware.

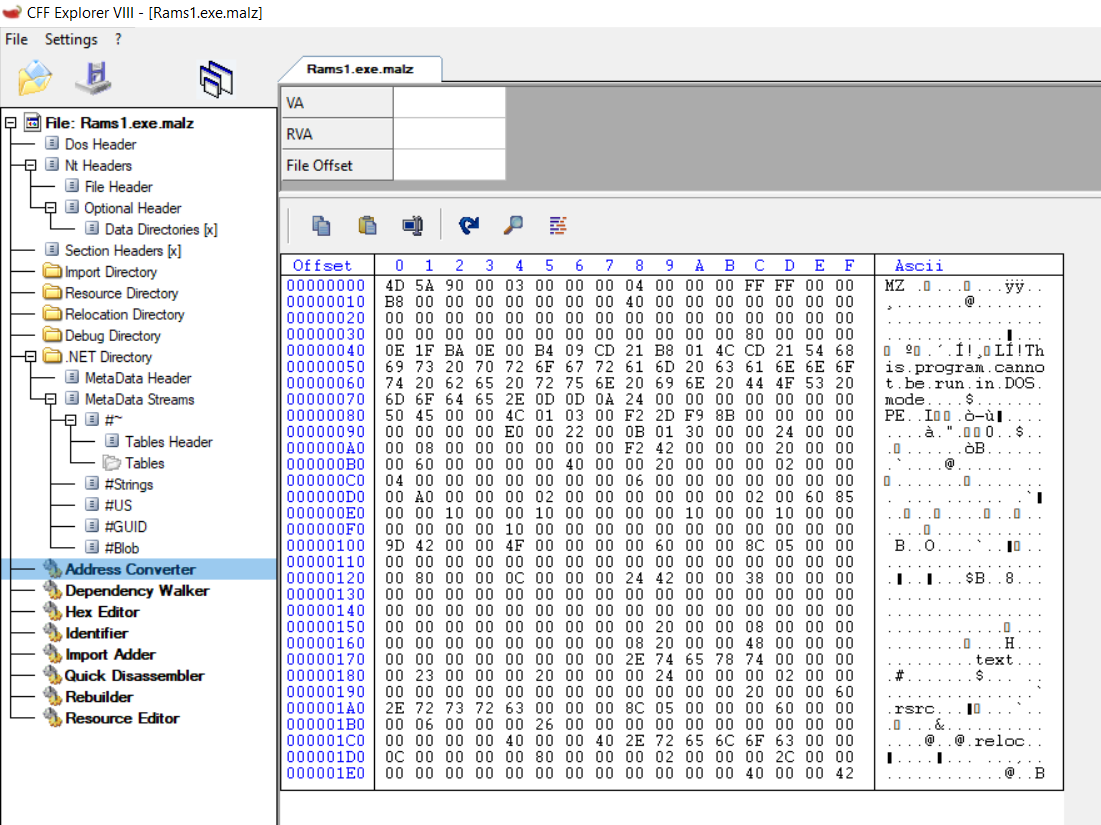
In Flare-VM, right click on malware file and in drop-down click **HashmyFile** to find about different hashes of this malware.





You can also check it with **CFF Explorer**



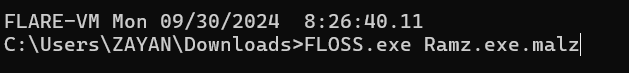


We have used multiple tools inside Flare-VM for surety of information because it is not best practice to rely on just 1 tool.

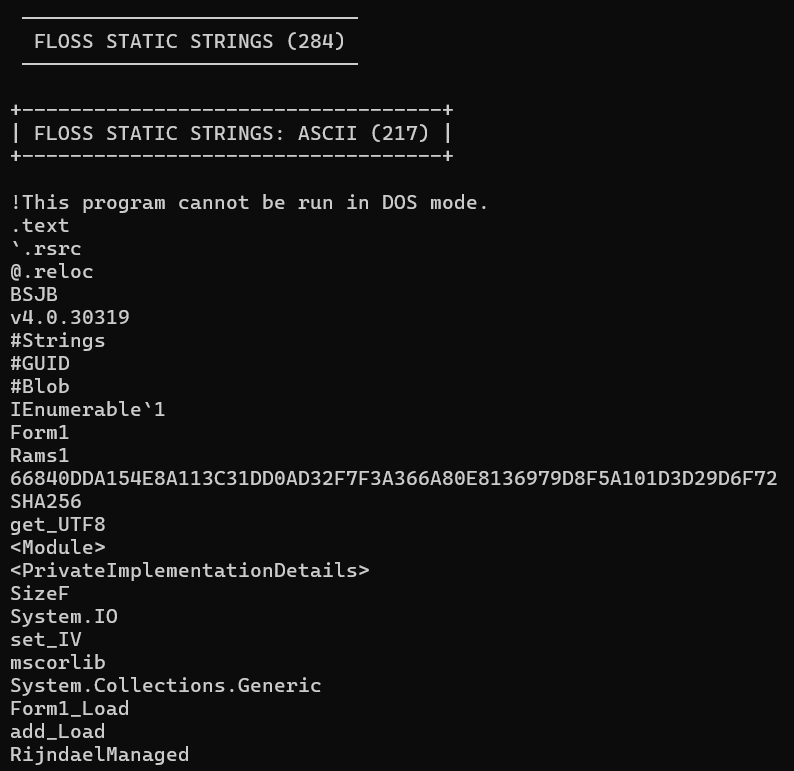
C > Program Data > Chocolatey > bin (Here you can find all .exe files)

Open terminal here in Flare-VM FLOSS.exe followed by malware name.

e.g: FLOSS.exe Ramz.exe



This tool extracts all the strings from malware. **Strings** are text or characters inside malware code. They help us to identify what this malware is doing whether it is creating backdoor to some site or which commands this malware is executing.



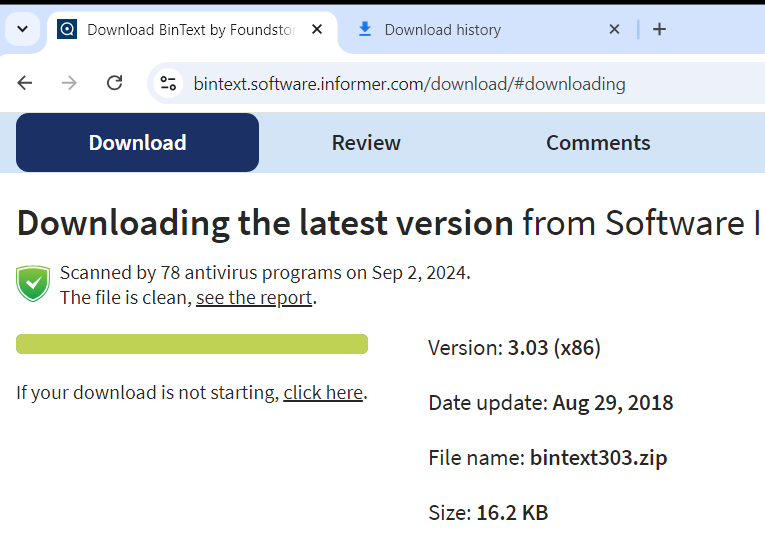


If we read this, we can see it is redirecting our machine to some onion site and also telling us our files have been encrypted. From this, we know this is a ransomware.

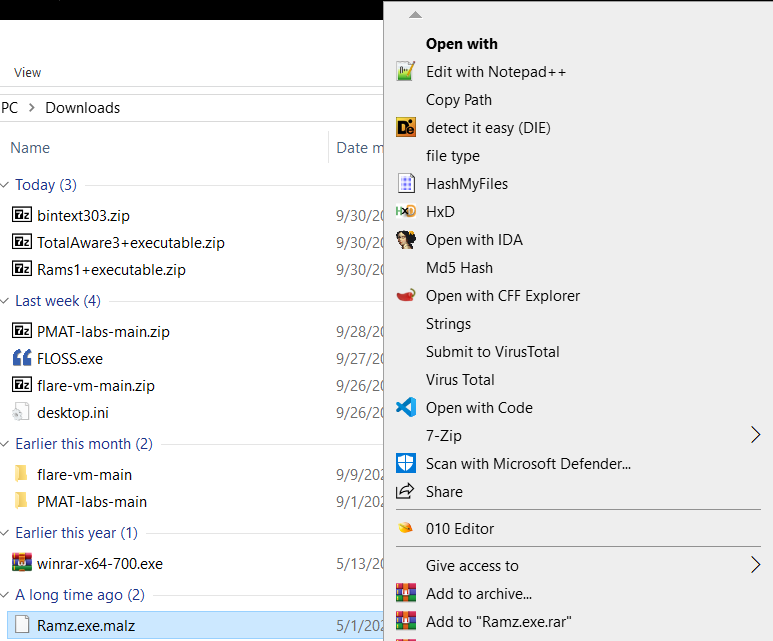
**Strings extracted from pestudio:**



Download **bintext** tool. It is also for extracting strings. It is GUI based tool.



We can also find strings using built-in tool in Flare-VM. Just right click on sample and click on strings.





Packing of sample using **UPX** **Tool:**

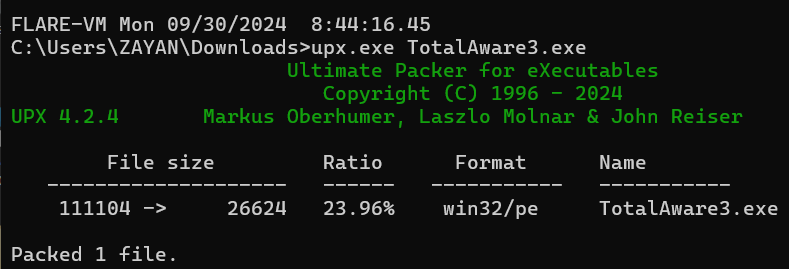
Open terminal in Flare-VM > upx.exe (It will open help section like what you can do with this tool)

For packing, use the following command:

**upx.exe TotalAware3.exe**

For unpacking, use this:

**upx.exe -d TotalAware3.exe**

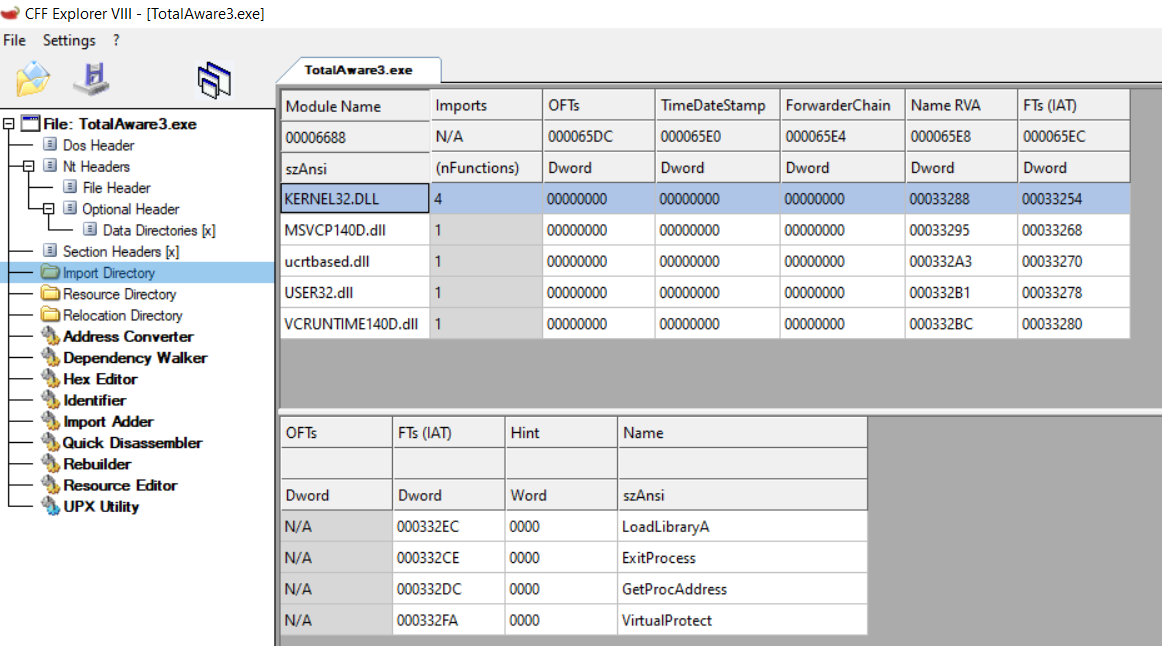




Open this sample with **CFF Explorer**, you’ll find info like UPX. This means this file is packed.

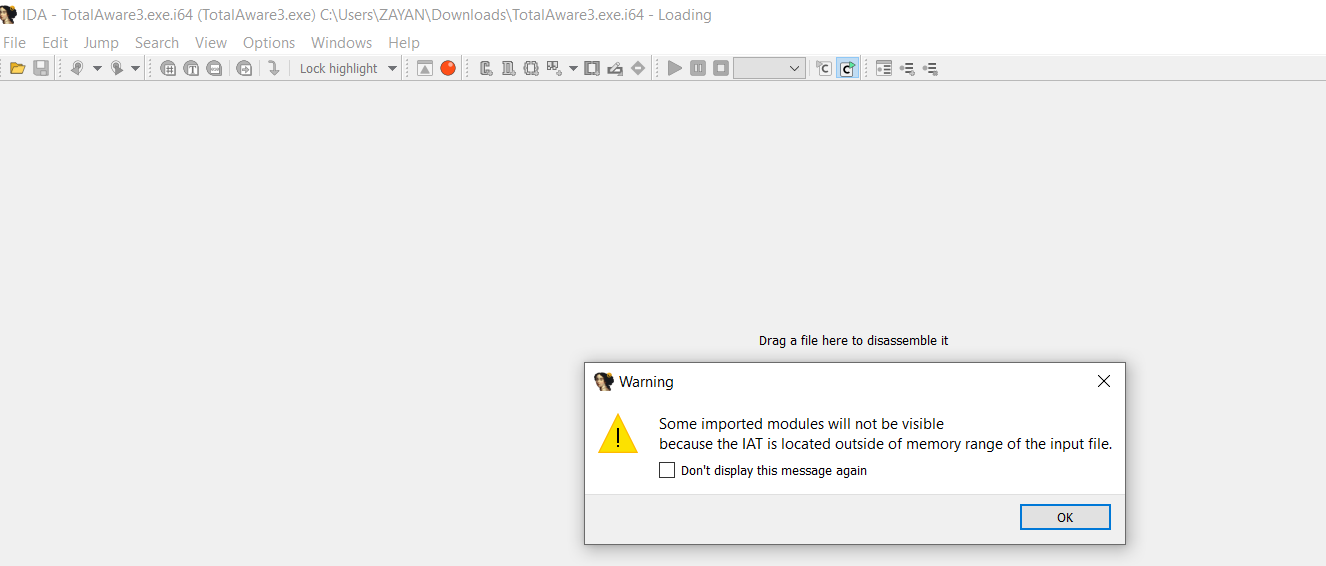


Also, the kernel processes are more like 23 or 24 but it is showing only 4. This is also a sign that this is a packed file.

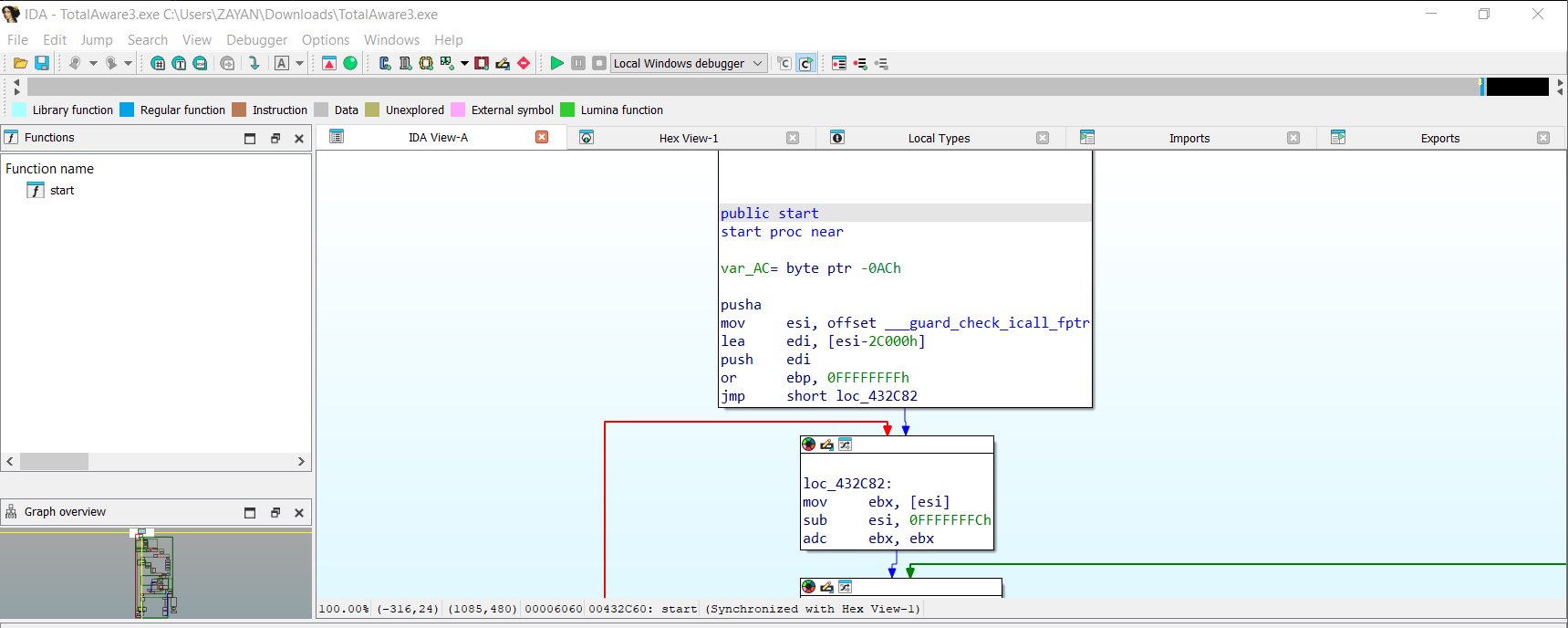


Similarly, open this unpacked file, it will tell you its executable file.

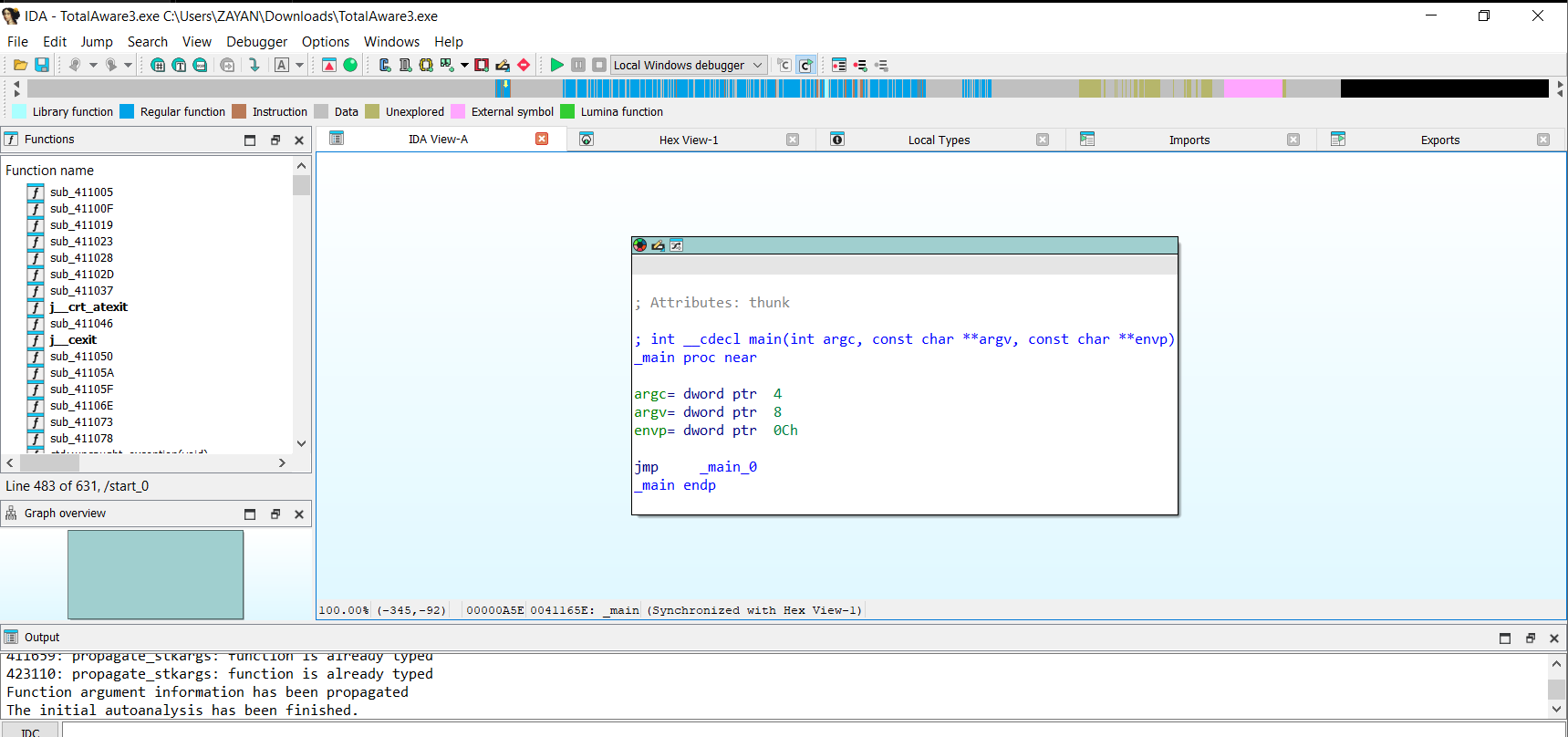
In **IDA tool**, when we open malware which will be packed, it’ll show us message like some contents are not visible. It will then indicate that the malware is obfuscated.



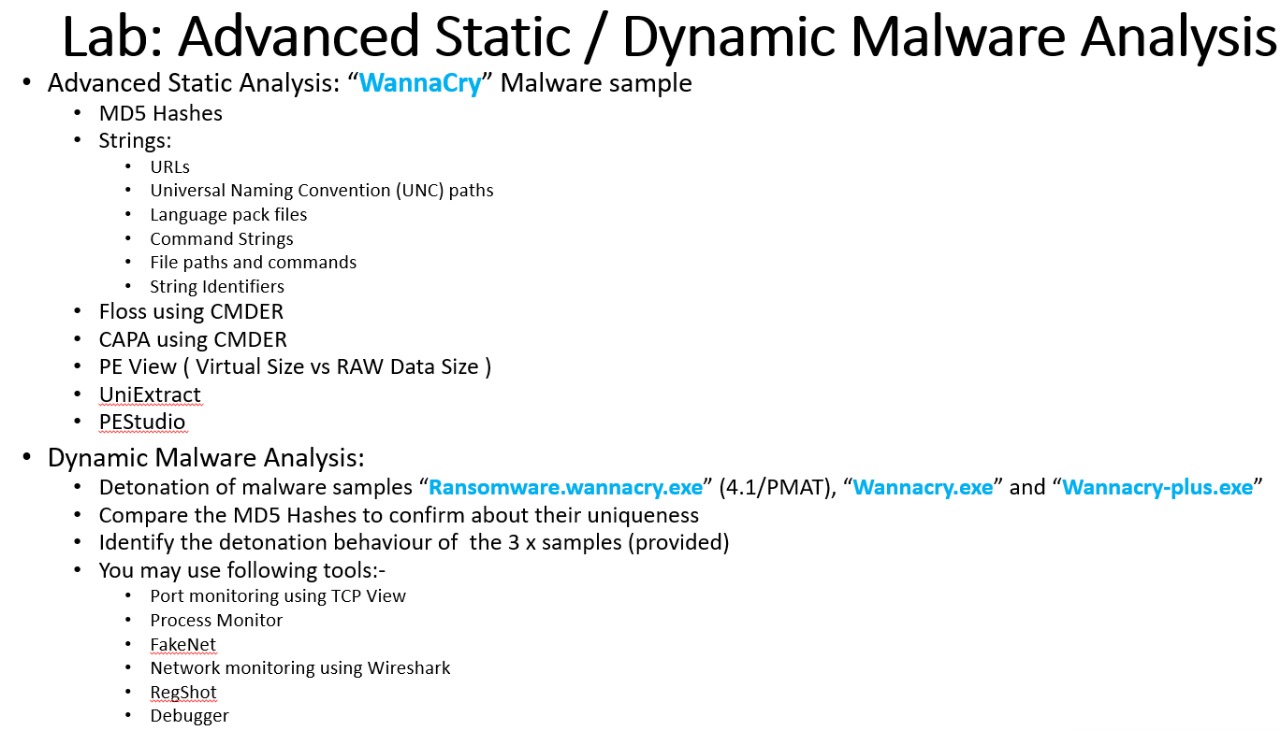
If file is packed, the color of bar will be black and grey.



If it is not, bar will be of rainbow color



**Static & Dynamic Malware Analysis:**



1. Go to the browser > Search Zoo malware > malware > binaries > Download Wanna Cry and Wanna Cry plus Ransomware

We can also find this sample in our Flare-VM

Pmat labs > labs > 4.1 > 3rd sample is Wanna Cry Ransomware

1. Put these 3 samples in 1 folder and find their hashes and strings and compare them if they are same or different.

**Remember:** Default universal password for malware samples is **infected**

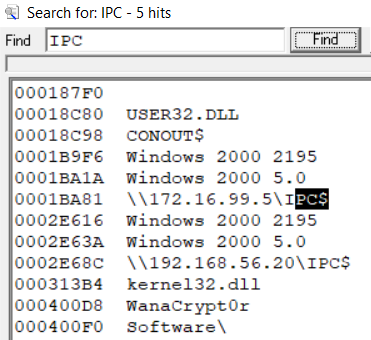
1. Find strings using **floss** in **cmder** tool.

In cmder, go to the directory where floss is and type FLOSS.exe followed by sample path.

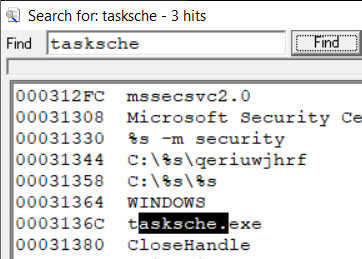
e.g: FLOSS.exe C:\users\ZAYAN\Desktop\WannaCry\Ransomware.wannacry > mydata.txt

It will find strings and save them into txt file. If you want to read the file just type **more mydata.txt**

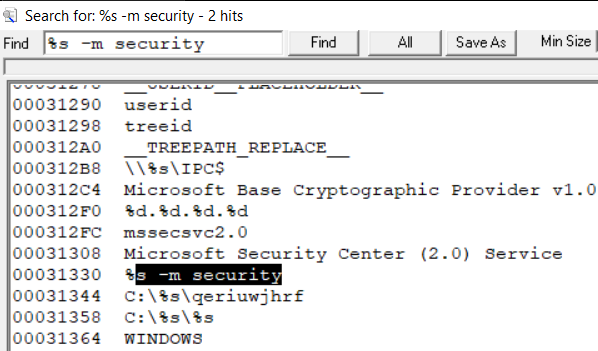
1. Find **IPC** in strings, you’ll find IP. It is indicating that it is trying to access common sharing so that it can spread through sharing. Anyone who shares or take file will get infected. What’s the purpose of .exe file accessing sharing resources? It indicates that it wants itself to spread.



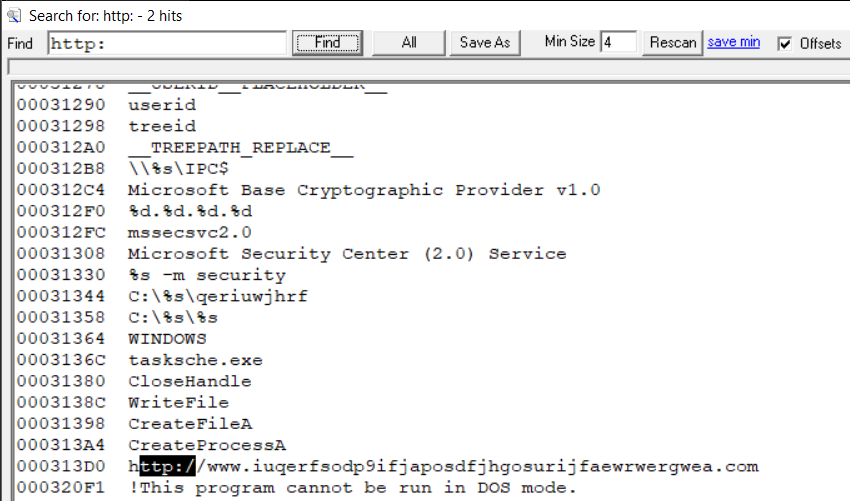
1. Find **tasksche**, this means that it will schedule tasks so it can make itself persistent.



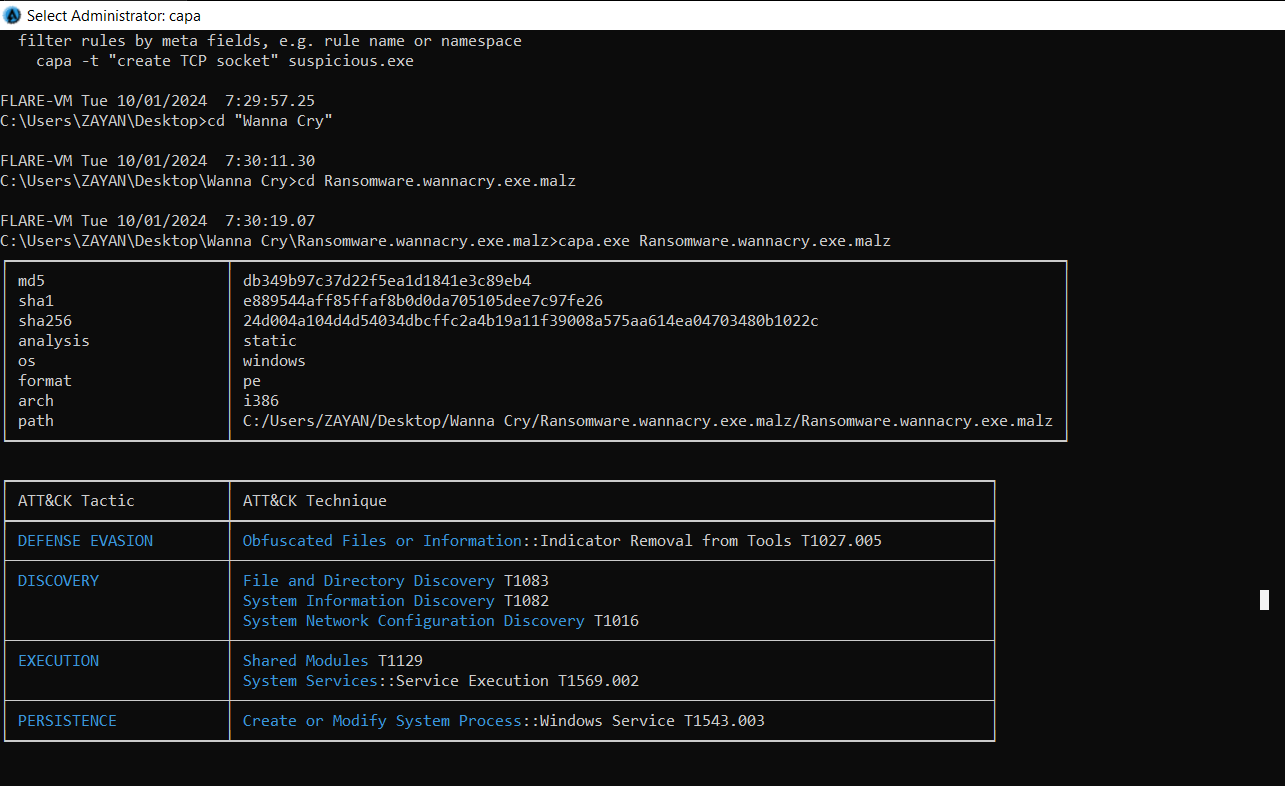
If you find **%s** symbol, it indicates it is placeholder like the result of execution of some command will be pasted here.



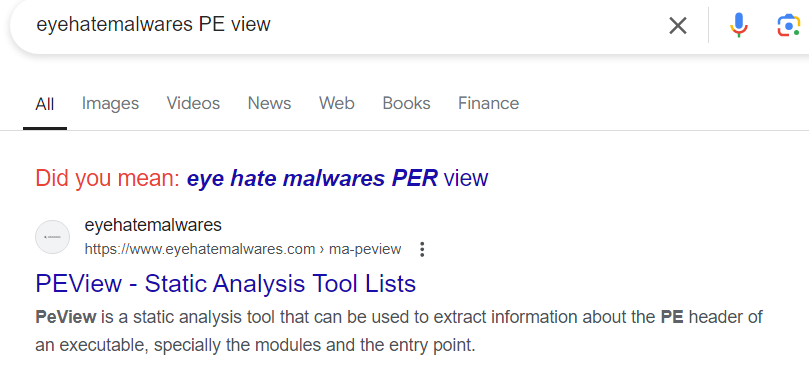
You can see unusual URL here. This surely means it is redirecting traffic to some kind of malware



**CAPA:**

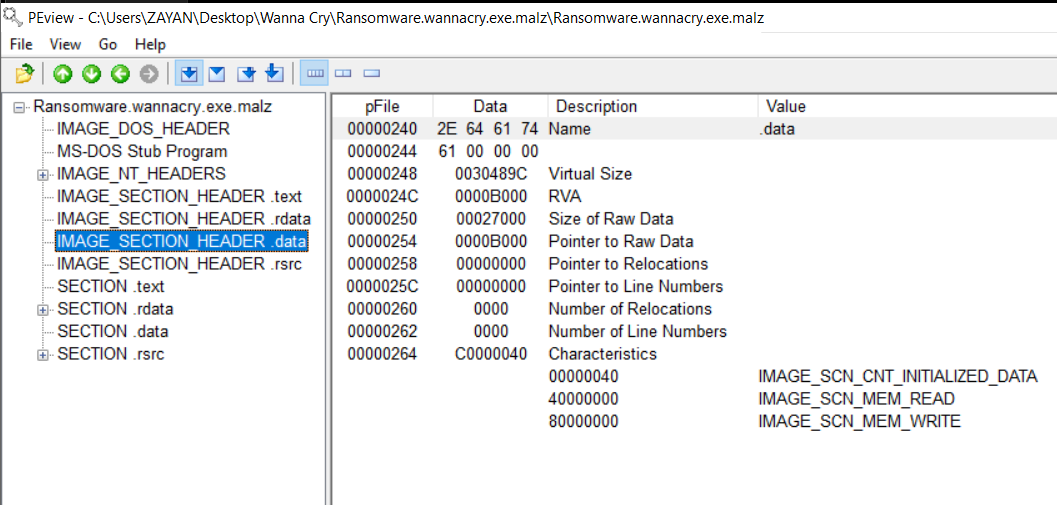


Eyehatemalwares PE view site to download **PE tool**.



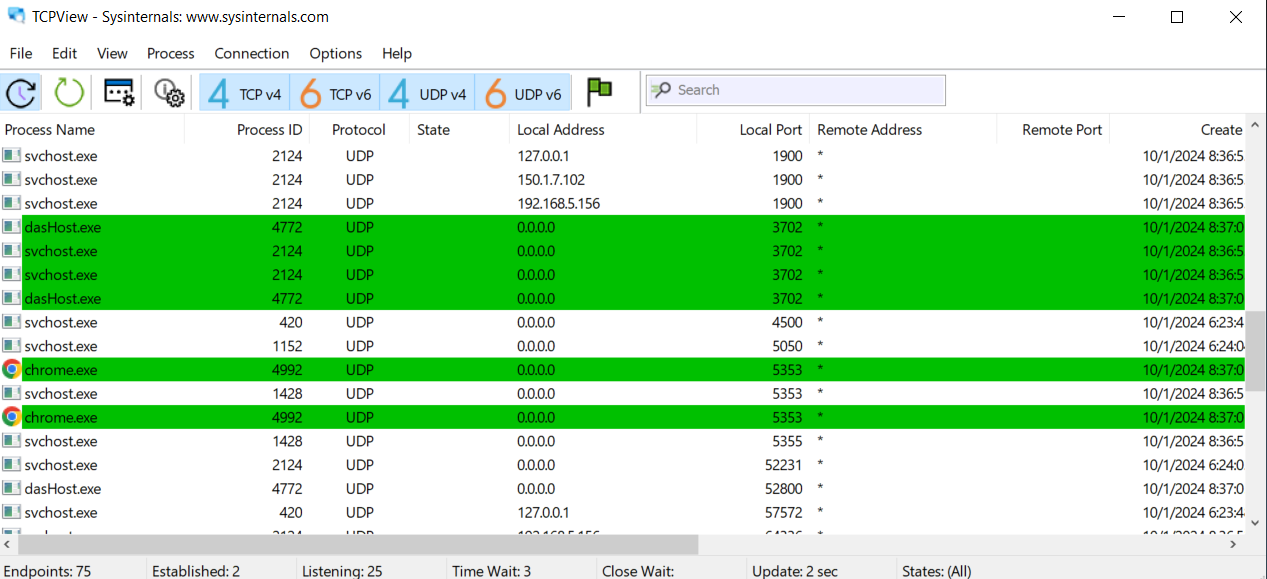
1. Right click on Download Tool button > Save link as
2. Open Malware in **PE** tool

If Virtual size is more than Raw Data size, it means that file/sample is packed. When it executes, its functionality will increase.



Now we are going to do **Dynamic Analysis:**

1. Open the tool **tcpview**



Green color indicates that system is running fine.

1. Run the Ransomware and look again in **tcpview**, color will change to red.

Also use **Fakenet** to check if this malware is sending http requests or trying to establish a backdoor connection.

1. Open the tool **Regshot** > Click on 1st shot to take a shot



1. Run the malware and then take 2nd shot >Compare the both shots and see what changes in registry files and keys, malware has made.