Malware Analysis

Part I Dataset and Resources

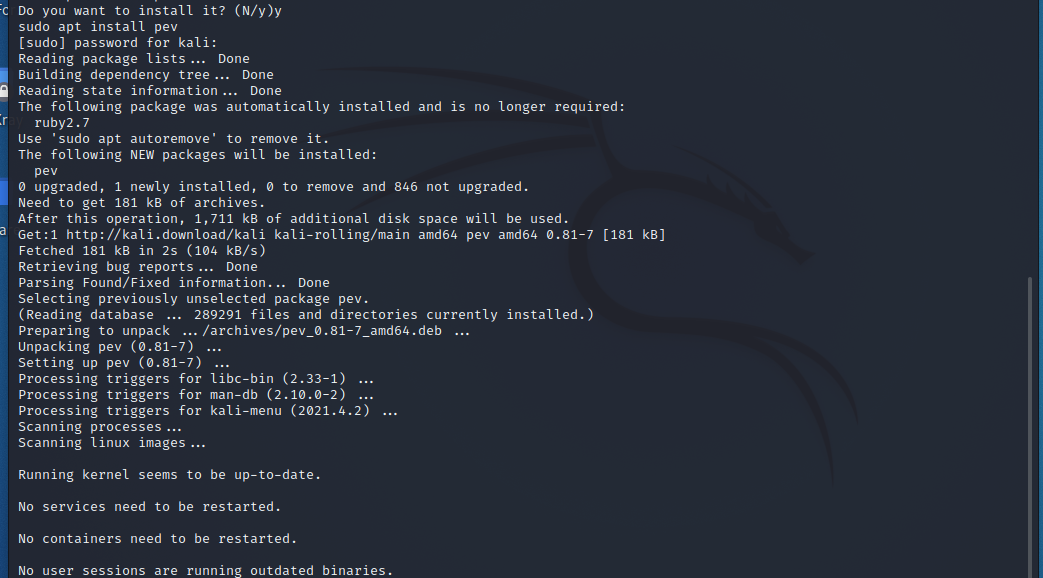
Ok so we have a **zip** folder that is going to be used in this lab for **Malware Analysis**. Download the file from the specific **URL** and unzipping it.

Part II Malicious Software

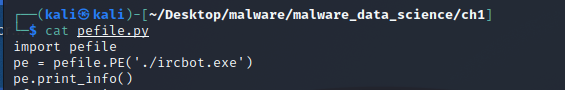
* There are two types of malware analysis:
* **Static analysis**: Static analysis is performed by analyzing a program file’s code, graphical images, strings, and other in-file stored information.
* **Dynamic analysis**: Dynamic analysis consist of the running the malware in a safe and isolate environment to analyze its behavior.
* Most common types of malwares:
* **Virus:** A program that can replicate itself and needs user interaction to activate it.
* **Trojan Horse:** A program that appears to be a legitimate software but is hiding a malicious payload in it.
* **Computer Worm:** It copies itself without the need of user interaction and spreads over the network.
* **Rootkits**: Software’s that gains administrator level access and are cable to do anything.
* **Botnets:** Number of devices (Network) compromised is called botnet. A single command from an attacker order all of these devices to perform the same task.
* **Adware:** Software that only spams advertisement on user’s screen.
* **Spyware:** A program that captures user’s information without his/her knowledge.
* **Ransomware:** A malware that encrypts device’s data. Attacker asks for ransom to decrypt the data.

Part III Portable Executable File Format

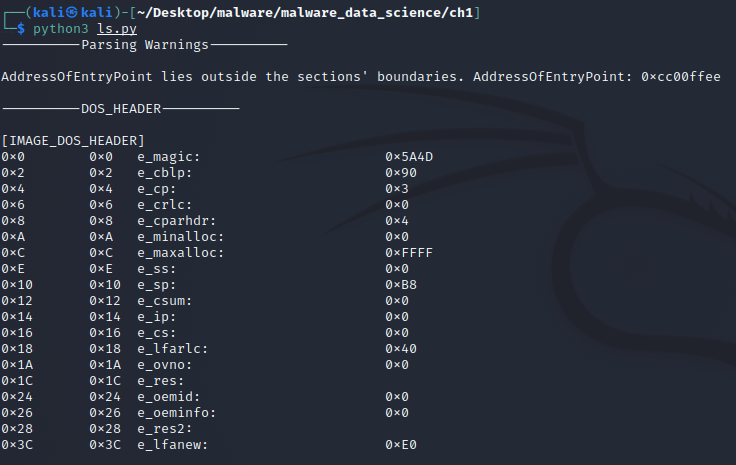
**PE-file** format is used by windows. An understanding of file structure for static malware analysis is necessary. PE format includes information to instruct the operating system on how to load the program in to the memory, in addition to several sections that contain executable’s actual data.



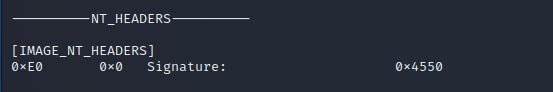
Here we have written a simple python script to import **pefile** library and now we are going to examine **ircbot.exe** program



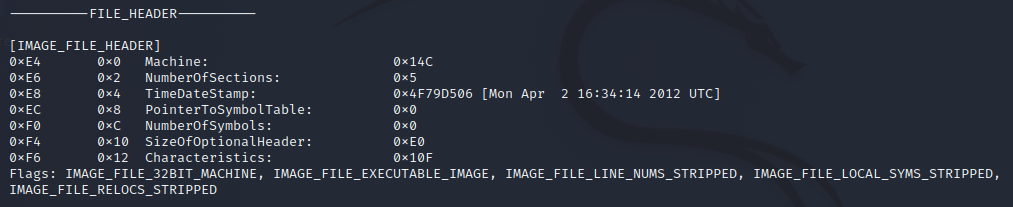
Analyzing **DOS-HEADER** file, it is present for compatibility reasons.



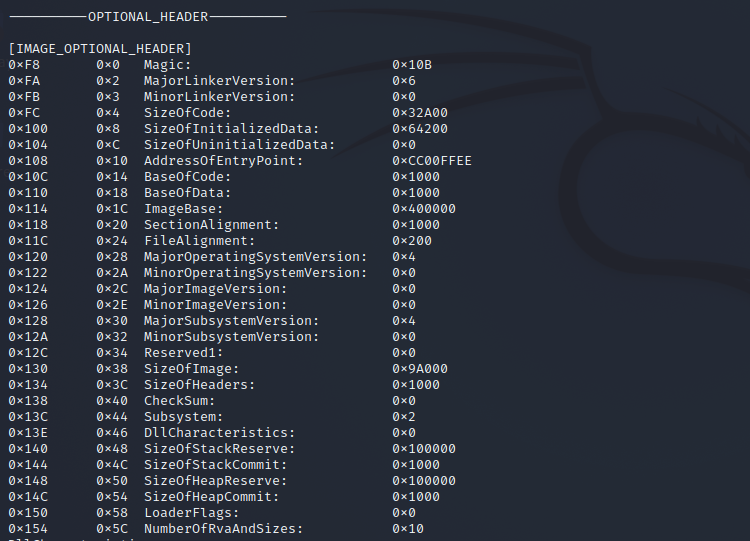
Analyzing **NT-HEADERS**, here we have a signature of 0x4550



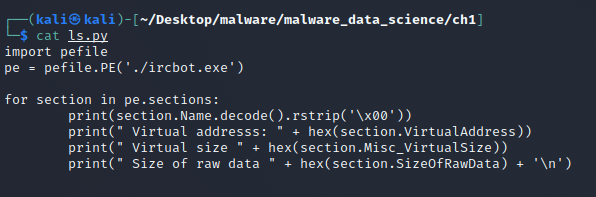
Analyzing **FILE-HEADER**, it contains information about the number of sections.

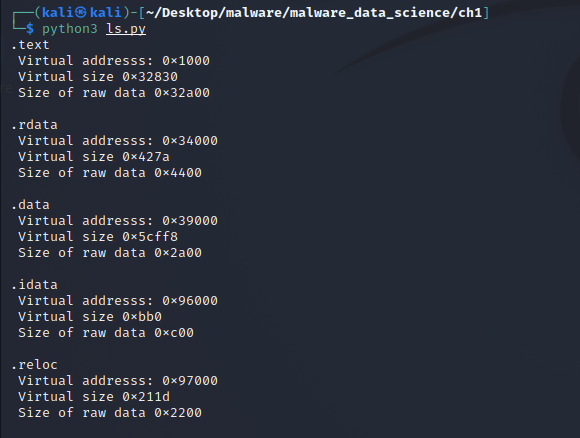


Analyzing **OPTIONAL-HEADER**, it contains very important information including program’s entry point in the PE file.

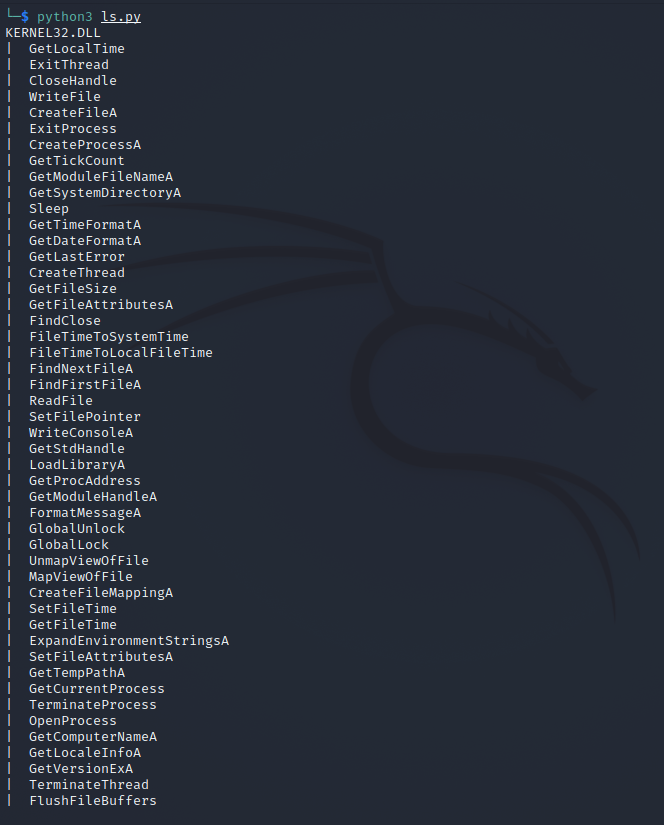


Ok so now we wrote another script that is going to extract information about sections.

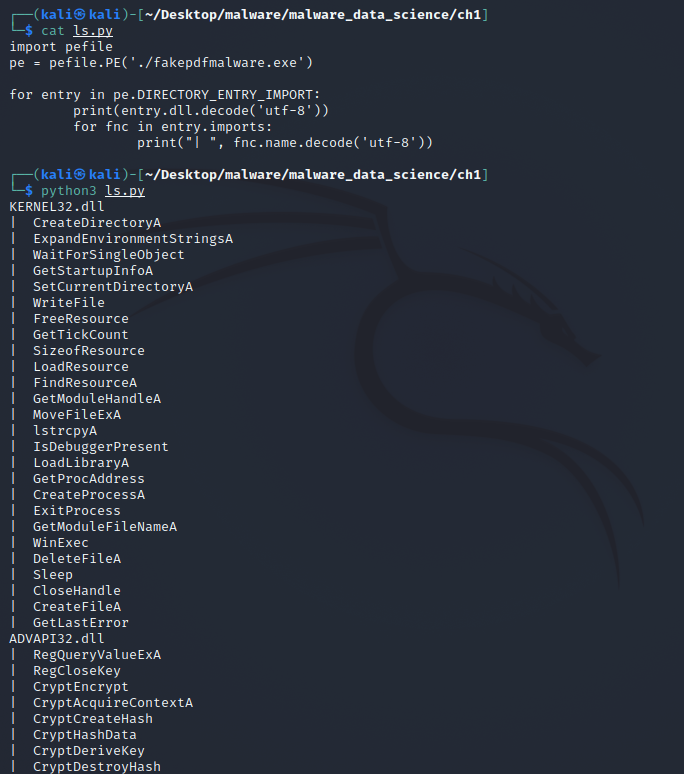


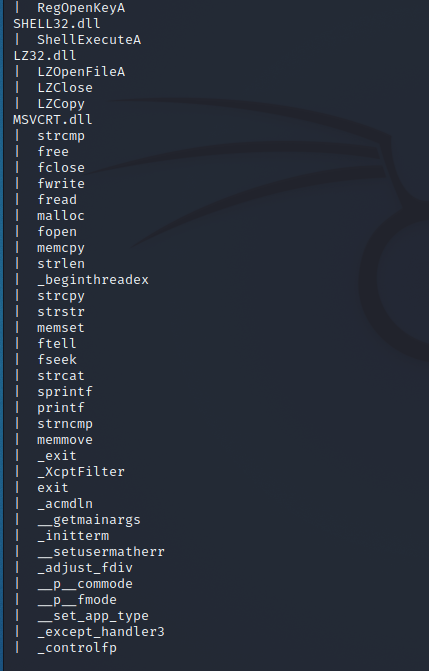


Another script that is going to extract list of DLL that a binary will load.



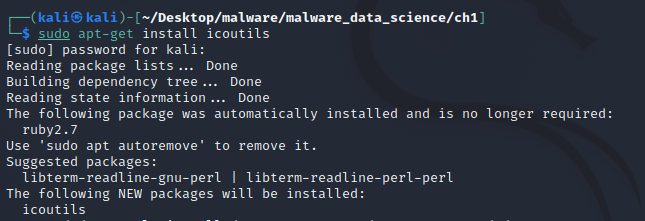


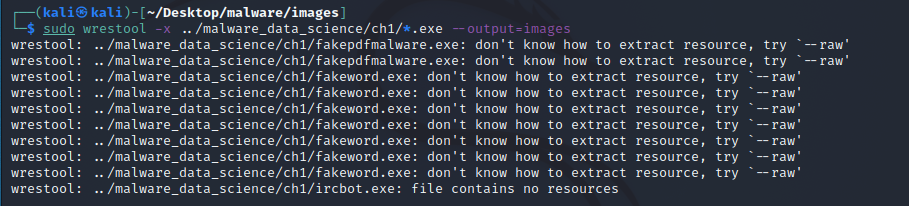




STEP 7

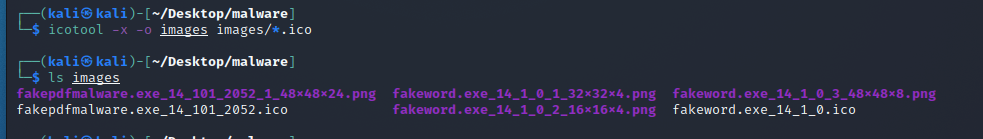
Malware always trick users by masquerading themselves as Word or PDF documents. In this step we will get executable images using the tool **icoutils**.





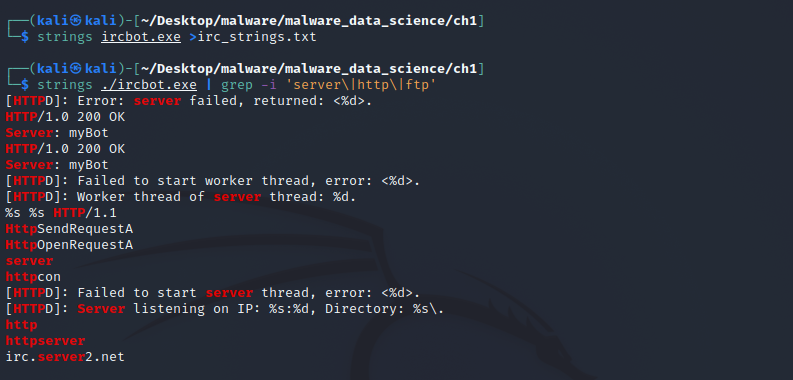


Here we have extracted png images



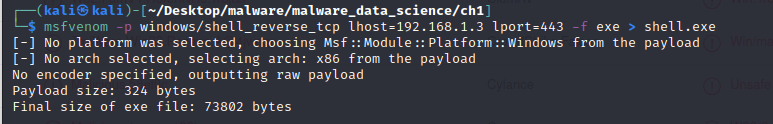
Part IV Examining Malware Strings

**Strings** are printable characters within a program binary. It is important to analyze the strings of a suspicious software to extract important information such HTTP connections.

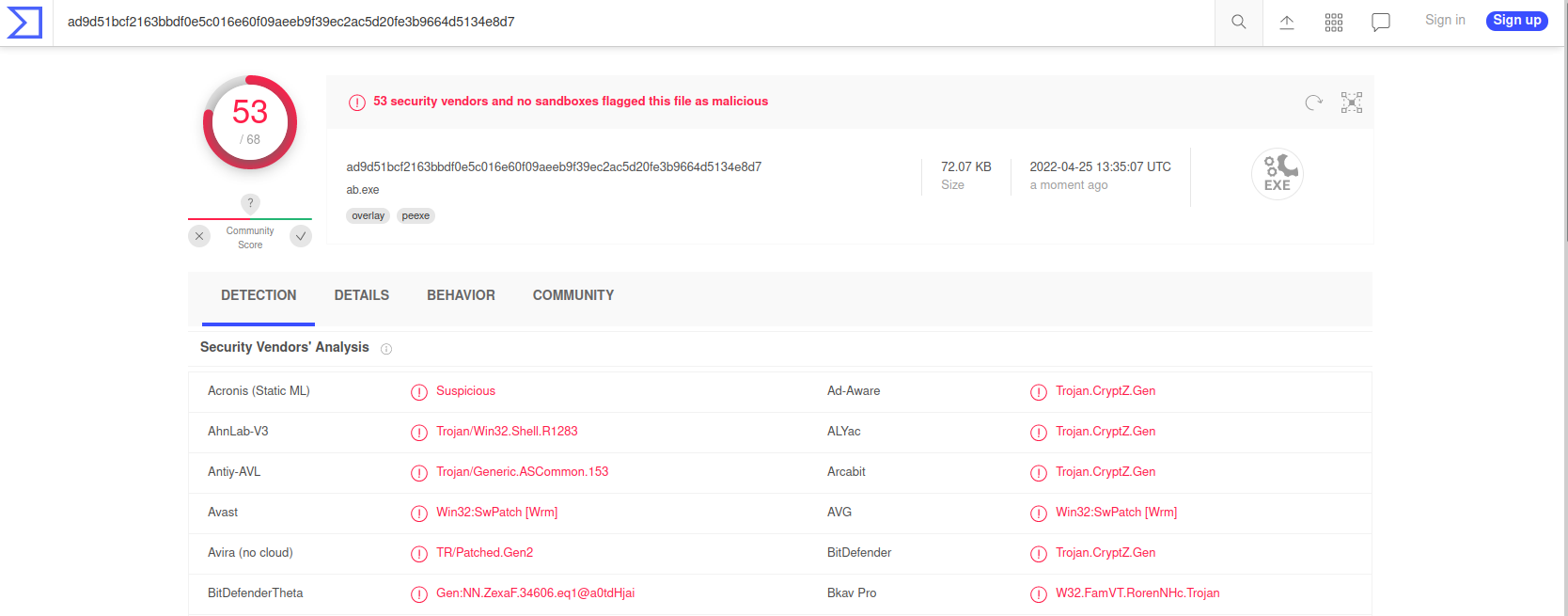


Part V Dynamic Malware Analysis

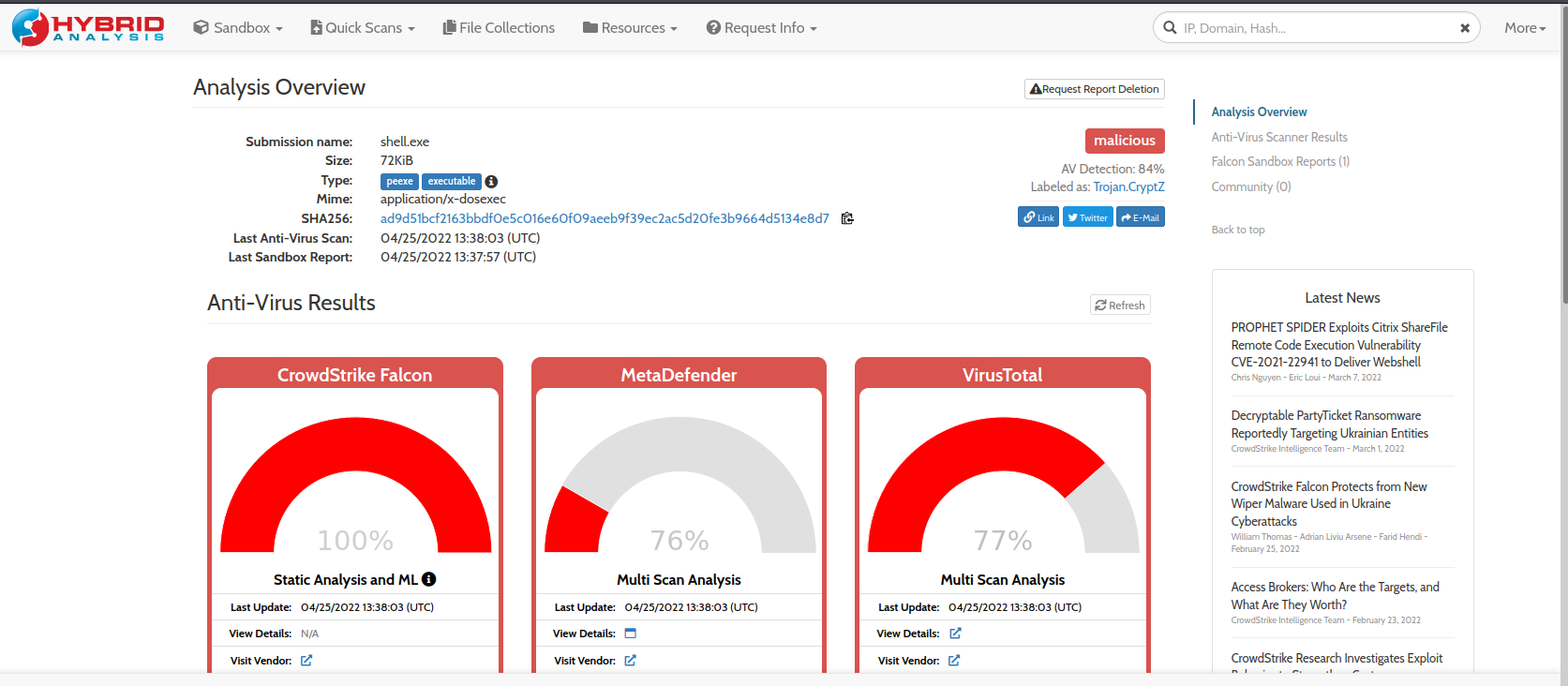
Ok so we are going to generate a virus using **msfvenom** and then we are going to analyses the result using two platforms **virus-total** and **hybrid-analysis.**



Virus-total Report



Hybrid-analysis Report



SUMMARY

This lab was all about learning **Malware Analysis** from analyzing malware detected files using pefile to using Virus-Total and Hybrid-analysis as a discovery tool. In the First part, we learned how to analyze **headers** of the vulnerable program using pe-file, we used python scripting to achieve it. In the Second part, we learned about examining the malware file using **strings**. In the Third part, we performed **Dynamic Malware Analysis** to generate a report of a vulnerable program using **Virus-Total** and **Hybrid-Analysis**.