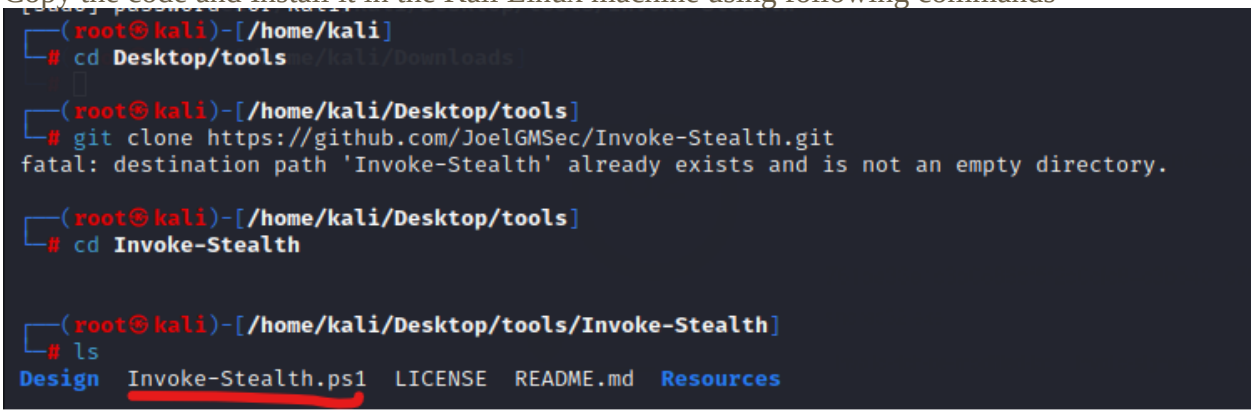
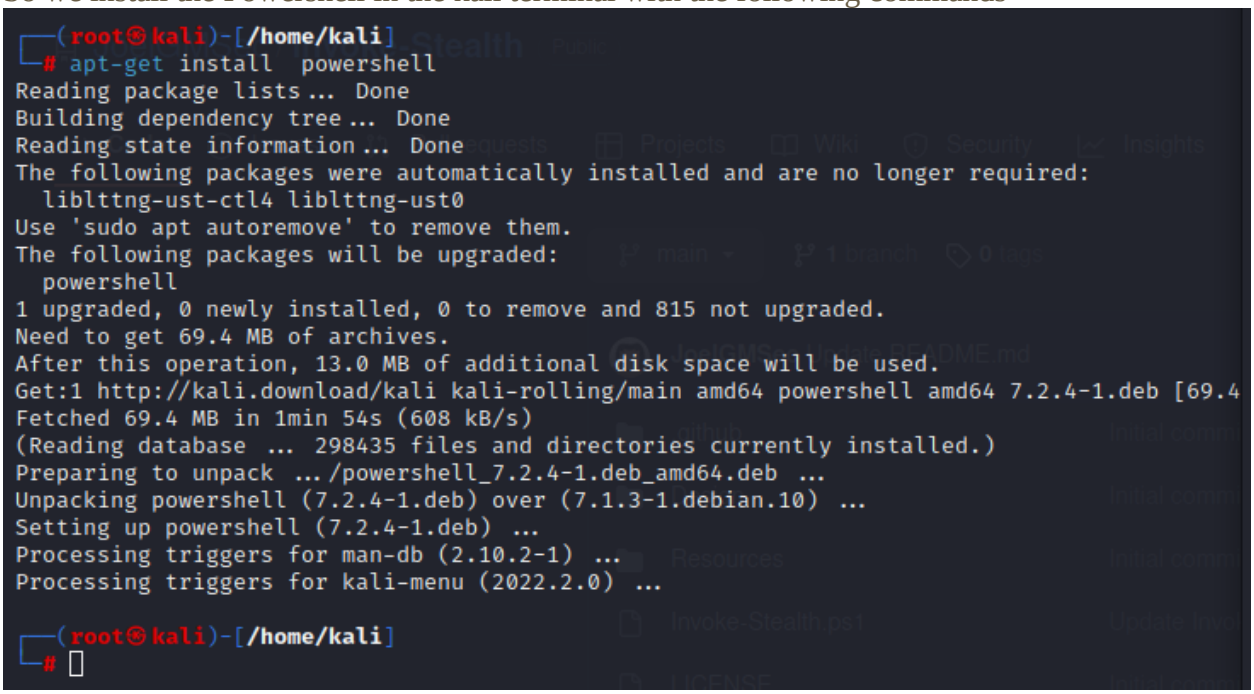
Now we are Changing the 340s.exe's content by using tool called "**Invoke Stealth**".Invoke Stealth Changes the file signature and then contents of the malware file without corrupting the malicious code so that malware can be undetectable by the most of the antivirus engines

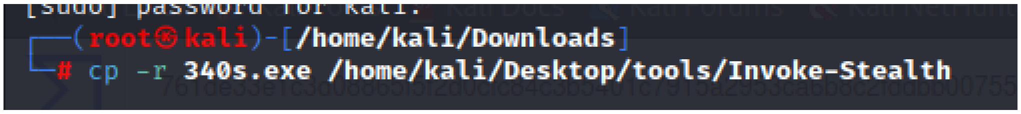
Go to github in your kali linux machine and in the browser search for the Invoke Stealth in the Github
Copy the code and Install it in the Kali Linux machine using following commands



From the above picture we can see that there is a file called Invoke-stealth.ps1 this is a powershell file which is a terminal in windows.
So to run this file we need Powershell.
Since we are on the Kali linux we only have the kali terminal
So we install the Powershell in the kali terminal with the following commands



Now we have Powershell in the Kali terminal
Now move the malware file 340s.exe(malware file which needs to be undetected) to the directory where this invoke-stealth is there.

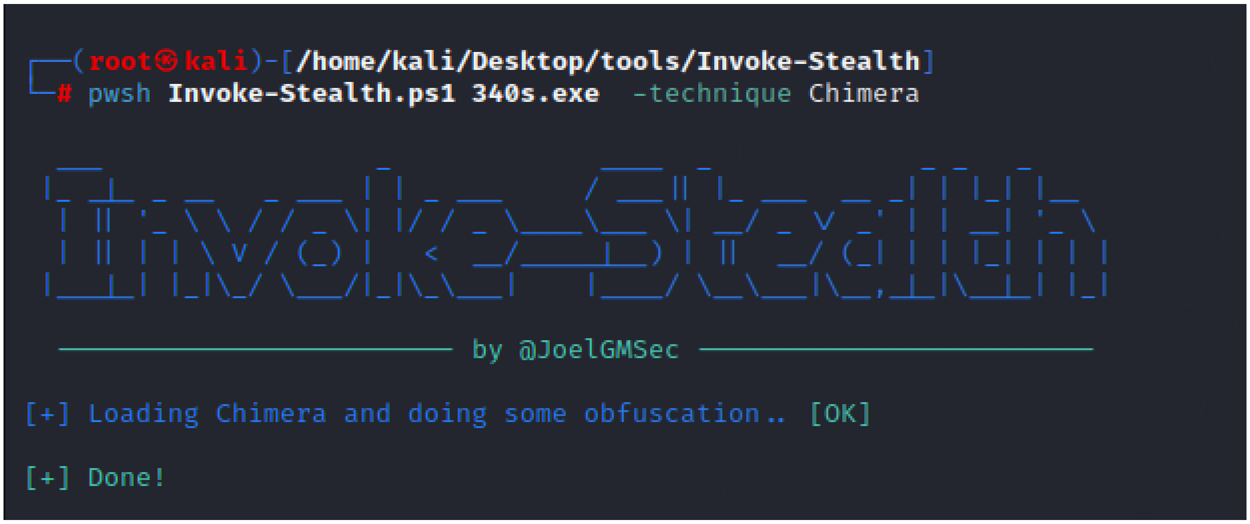


```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Downloads]
└─# cp -r 340s.exe /home/kali/Desktop/tools/Invoke-Stealth
```

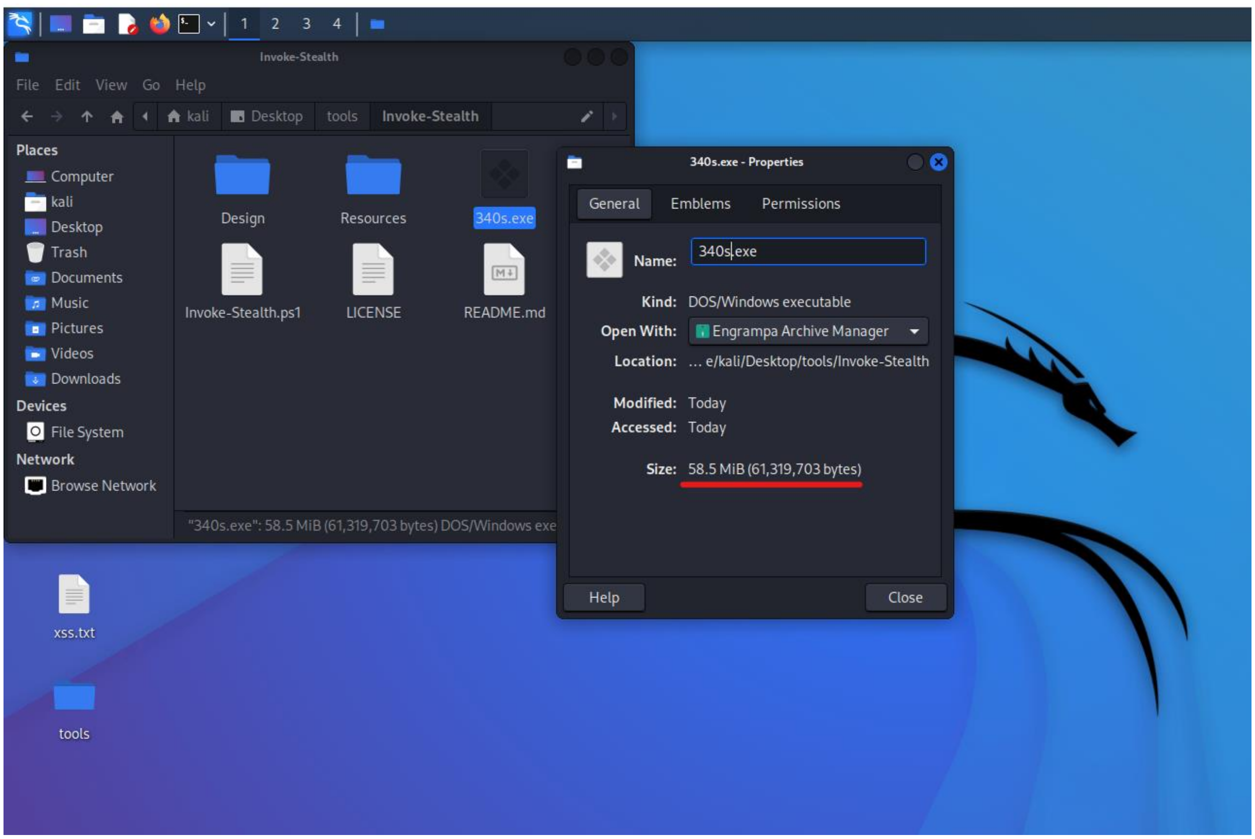
Now run the following command
This gives the information like how to use it and its techniques

```
┌──(root㉿kali)-[/home/kali/Desktop/tools/Invoke-Stealth]
└─# pwsh Invoke-Stealth.ps1

  ──────────────────────── by @JoelGMSec ────────────────────────

  Error: No input file!

  Info:  This tool helps you to automate the obfuscation process of
         any script written in PowerShell with different techniques

  Usage: .\Invoke-Stealth.ps1 script.ps1 -technique Chimera
          - You can use as single or separated by commas -

  Techniques:
        · Chimera: Substitute strings and concatenate variables
        · BetterXencrypt: Compresses and encrypts with random iterations
        · PyFuscation: Obfuscate functions, variables and parameters
        · PSObfuscation: Convert content to bytes and compress with Gzip
        · ReverseB64: Encode with base64 and reverse it to avoid detections
        · All: Sequentially executes all techniques described above

  Warning: The output script will exponentially multiply the original size
           Chimera & PyFuscation need dependencies to work properly in Windows
```

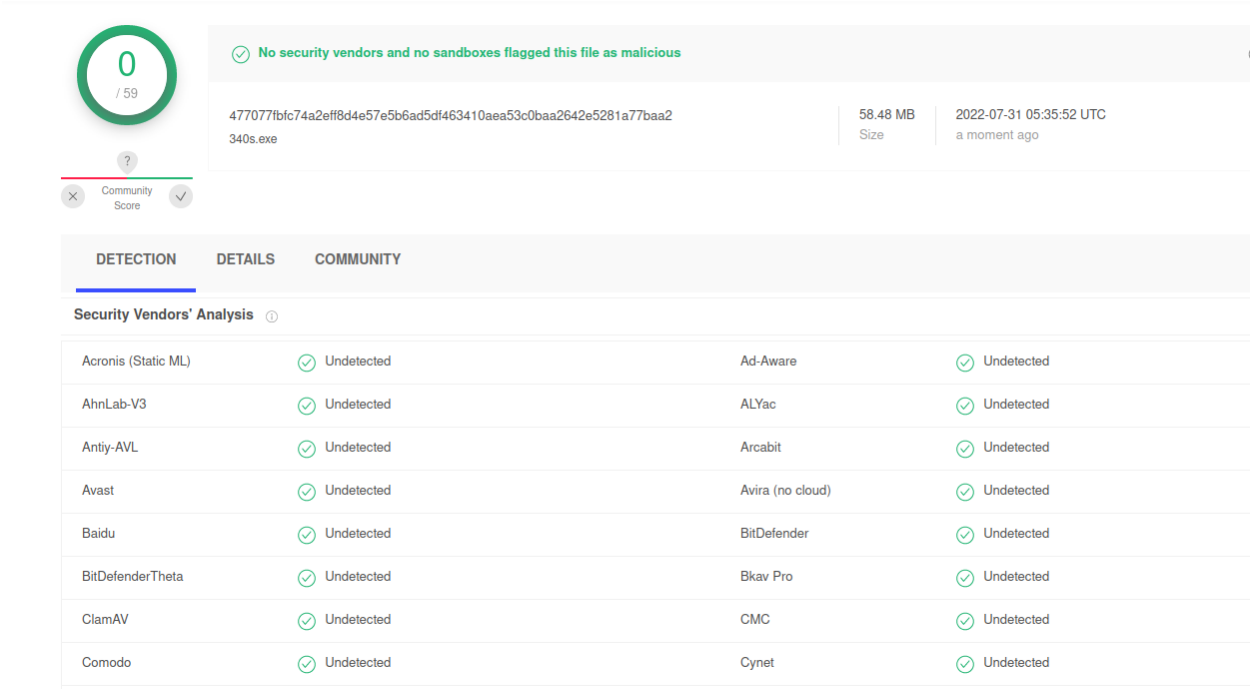
Now to change the signature and the contents of our malware file use the following commands
By doing so, the file size of our 340s.exe increases largely because invoke-stealth adds lots of other content to our 340s.exe file to change its signature,so that most of the antivirus engines cant detect the malicious content in our malware file.The commands for doing it is



Now lets check the size of the 340s.exe file which we used invoke-stealth on



After using the invoke-stealth on the 340s.exe, its size increased from 349KB to 58.5 MB
Lets check this new 340s.exe file in the VirusTotal and see how many of the antivirus engines detect malware content in our malware file



Surprisingly, our malware file 340s.exe came out5 clean and none of then antivirus engines out of 59 engines detected our malware file 340s.exe as malicious file.

This is possible because of changing the file signature and the contents of our malware file 340s.exe without corrupting the malicious content of the file.The file 340s.exe can we used as a malware without being detected by the any antivirus engines.