Steps carried out for this process:

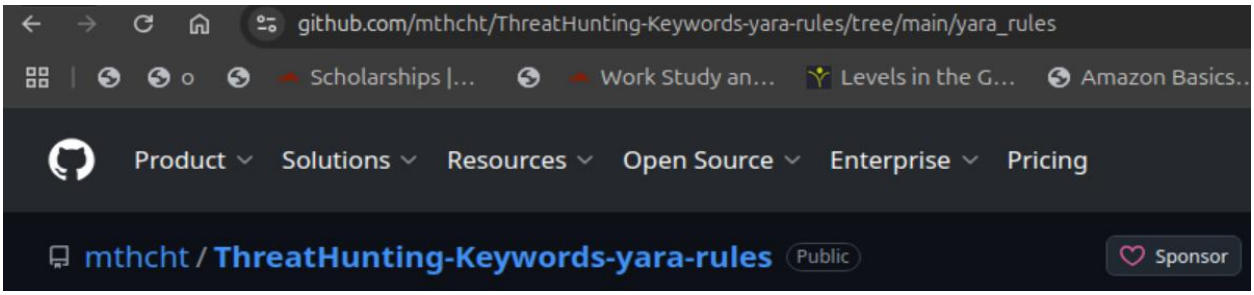
```
osboxes@monica:~/Practica_Malware$ sudo apt install python3.12-venv
```

```
osboxes@monica:~/Practica_Malware$ python3 -m venv venv
osboxes@monica:~/Practica_Malware$ source venv/bin/activate
(venv) osboxes@monica:~/Practica_Malware$ pip install requests yara-python
```

```
(venv) osboxes@monica:~/Practica_Malware$ ls
borrar_malware  malware  reglas_yara  reglas_yara_copia.py  reglas_yara.py  venv
(venv) osboxes@monica:~/Practica_Malware$
```

```
(venv) osboxes@monica:~/Practica_Malware$ ls
malware  reglas_yara  reglas_yara.py  venv
(venv) osboxes@monica:~/Practica_Malware$ python reglas_yara.py
```

.




```
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ python reglas_yara.py
```

```
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ ls
Cape  ReversingLabs  rules-compiled
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ mkdir Neo23x0
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ mkdir ThreatHunting
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ ls
Cape  Neo23x0  ReversingLabs  rules-compiled  ThreatHunting
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$
```

```
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ ls ~/Practica_Malware/reglas_yara/Cape/*.ya* | wc -l
97
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ ls ~/Practica_Malware/reglas_yara/ReversingLabs/*.ya* | wc -l
298
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ ls ~/Practica_Malware/reglas_yara/Neo23x0/*.ya* | wc -l
697
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ ls ~/Practica_Malware/reglas_yara/ThreatHunting/*.ya* | wc -l
130
```

Size of the compiled file before including only the YARA rules located in the Cape and ReversingLabs folders.

```
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ du -h rules-compiled
4.2M    rules-compiled
```

An initial manual execution of the program was performed to ensure that the Python script would function correctly when executed later.

```
(venv) osboxes@monica:~/Practica_Malware$ find reglas_yara -name "*.yar*"
reglas_yara/Neo23x0/exploit_cve_2018_0802.yar
reglas_yara/Neo23x0/apt_fidelis_phishing_plain_sight.yar
reglas_yara/Neo23x0/apt_pulsesecure.yar
```

```
(venv) osboxes@monica:~/Practica_Malware$ yarac reglas_yara/**/*.yar* reglas_yara/rules-compiled
```

```
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ du -h rules-compiled
19M     rules-compiled
```

Evidently, this difference in the size of the rules-compiled file serves as verification that the rules from the other two repositories were successfully incorporated. Next, I executed the YARA rule compilation script (which initially failed more than twice, though not due to syntax errors), during which the Cape and ReversingLabs folders were created and their YARA rules downloaded. Additionally, the Neo23x0 and ThreatHunting folders were added, along with their respective YARA rules

```
(venv) osboxes@monica:~/Practica_Malware$ python reglas_yara.py
```

```
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$ du -h rules-compiled
19M     rules-compiled
```

```
Cape  Neo23x0  ReversingLabs  rules-compiled  ThreatHunting
(venv) osboxes@monica:~/Practica_Malware/reglas_yara$
```

Up to this point, a collection of YARA rules from four repositories has been compiled, along with the rules-compiled file, which will be used for the purpose of detecting malware located in another subdirectory of this process.

Below are some screenshots of the various steps carried out, organized to lay the groundwork for achieving satisfactory results.

```
(venv) osboxes@monica:~/Practica_Malware/malware$ ls *.zip | wc -l
78
```

```
(venv) osboxes@monica:~/Practica_Malware/malware$ ls
VirusShare_01ec08e3ef7d262891318dbc646db535.zip  VirusShare_83c4df58416363dc3934996744c94bd7.zip
VirusShare_0ebe19e549781865af5659e40132094c.zip  VirusShare_86d3f3f29362283921a9277bdfb73648.zip
Google Chrome
8094385cdbc55a1a8b478881109200.zip  VirusShare_879a44649956c2c14557d1362436ebf4.zip
14fe92196204effcebf383b6c229fa20.zip  VirusShare_91752dde60ea456ed62c8c6b6ab257a3.zip
VirusShare_17fac44461415765c8ec7cc6edfecefa.zip  VirusShare_9309f7041527ed8a8bd00a1d8e14b167.zip
VirusShare_1a27fceaa8cf30b45e58957195768a4e.zip  VirusShare_9512f8fb0f54b27dc7f658f622c4e18c.zip
```

```
(venv) osboxes@monica:~/Practica_Malware$ unzip -P infected '/home/osboxes/Practica_Malware/malware/*.zip' -d /home/
osboxes/Practica_Malware/malware/
Archive:  /home/osboxes/Practica_Malware/malware/VirusShare_2719704cf61c3745abfb27eb71da148e.zip
  inflating: /home/osboxes/Practica_Malware/malware/7636a9a372ecbe65e84e5c16e626ab03929a0089d253d4dd391b915774dd67ef
```

```
(venv) osboxes@monica:~/Practica_Malware/malware$ ls
0b42fe12040accf3a276b7f5116719cb3f80dbc0b88ce0259b7f4a6634f6f043  VirusShare_01ec08e3ef7d262891318dbc646db535.zip
0bfc8b2637df250f70c58fd62d4c8bf00ca25e2a7390322e407e9f1916470825  VirusShare_0ebe19e549781865af5659e40132094c.zip
10e7ea5b7343919d7e08d966702e4393e386c2137602a4d7e14da011a13cf67b  VirusShare_118094385cdbc55a1a8b478881109200.zip
119f61f1905a8def5d38cb800af1e4bd478dbc98d679aa709cf4690a0df5f8d7  VirusShare_14fe92196204effcebf383b6c229fa20.zip
```

The following result shows how the escanear.py program finds some matches.

```
(venv) osboxes@monica:~/Practica_Malware$ python escanear.py
Match encontrado en /home/osboxes/Practica_Malware/malware/e940adf69acf6525fd8f05b54f289d0a85ff1c779086a8af9fcbb00c6
a39f547: [SUSP_ELF_LNX_UPX_Compressed_File]
Match encontrado en /home/osboxes/Practica_Malware/malware/666824d5b0f41724167572a0a3e7842e5daf129a9825c57fe90177e23
6eb1c01: [SUSP_Imphash_Mar23_3]
Match encontrado en /home/osboxes/Practica_Malware/malware/de323a65795ab0f493524810b1609b7a6a48aae6bffc8561fb2c18b70
6e2d186: [SUSP_ELF_LNX_UPX_Compressed_File]
Match encontrado en /home/osboxes/Practica_Malware/malware/e70cbe73cf82874ef820bd9d89163058dae6d237ad5ff4dcfae063522
55c8136: [SUSP_ELF_LNX_UPX_Compressed_File]
Match encontrado en /home/osboxes/Practica_Malware/malware/59e285d12ad8a15e05163e1fdfd6044a89baf7bf198639dc86b9ff407
47ecbfc: [SUSP_Imphash_Mar23_3]
Match encontrado en /home/osboxes/Practica_Malware/malware/6e12275e6e97816d64067be52eeb832289cb98179a3444214a7ab6be8
4b91df1: [SUSP_ELF_LNX_UPX_Compressed_File]
Match encontrado en /home/osboxes/Practica_Malware/malware/3a6ce58cbe810517f7b1d1e1a9c7c509e695a35a3d7cbc749f1930ff9
f197272: [SUSP_ELF_LNX_UPX_Compressed_File]
Match encontrado en /home/osboxes/Practica_Malware/malware/85c57b6512b9483301828f4a50d36e4c707454bd912ead9f287fa0cd2
a3e8cbc: [SUSP_ELF_LNX_UPX_Compressed_File]
```

"I would have liked to add a few hundred more YARA rules, as well as more malware, but the limited time available did not allow me to do so.