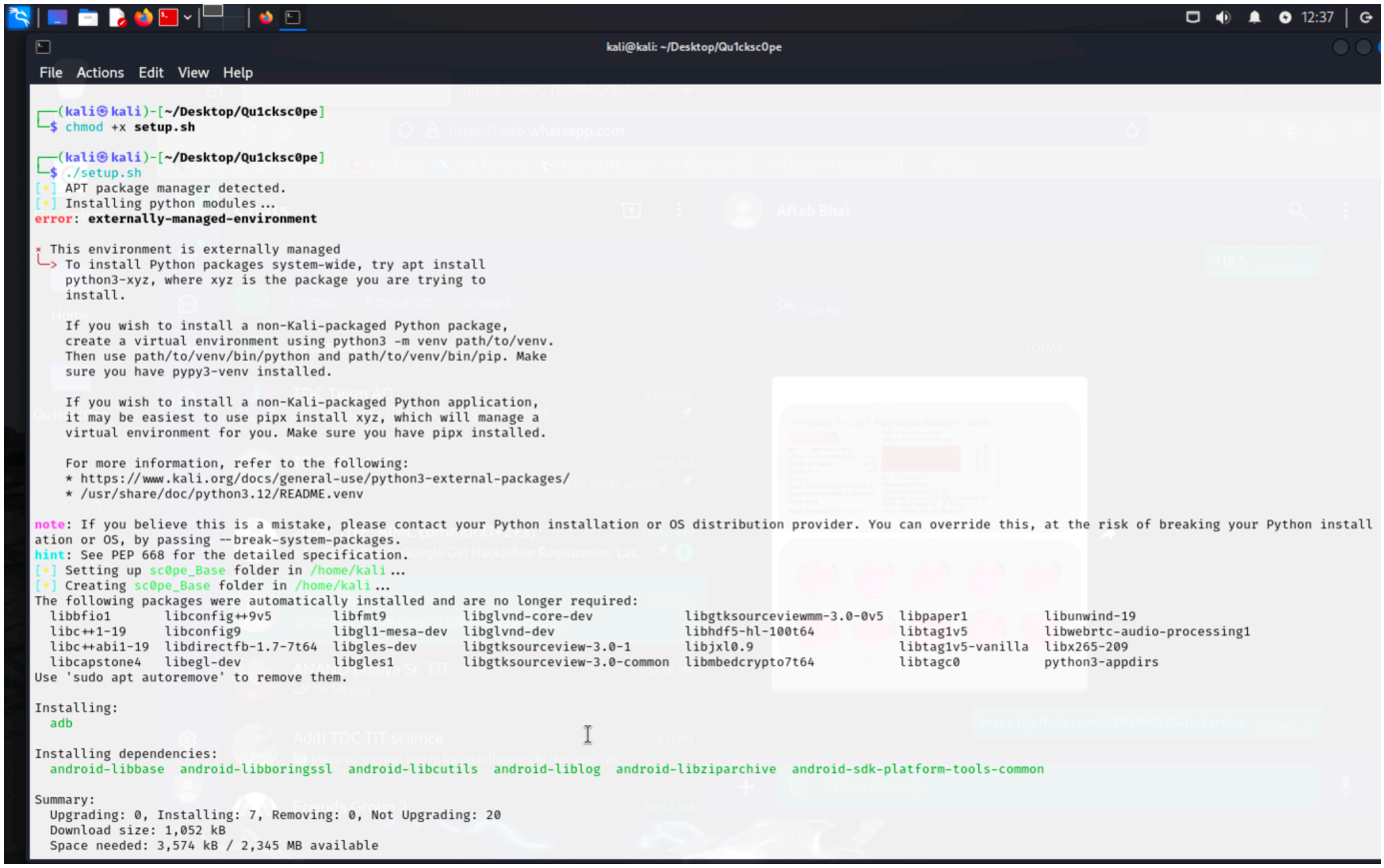
Hands-on Tasks (due by 6 feb 5:35pm)
(A) Malware Behavior Analysis

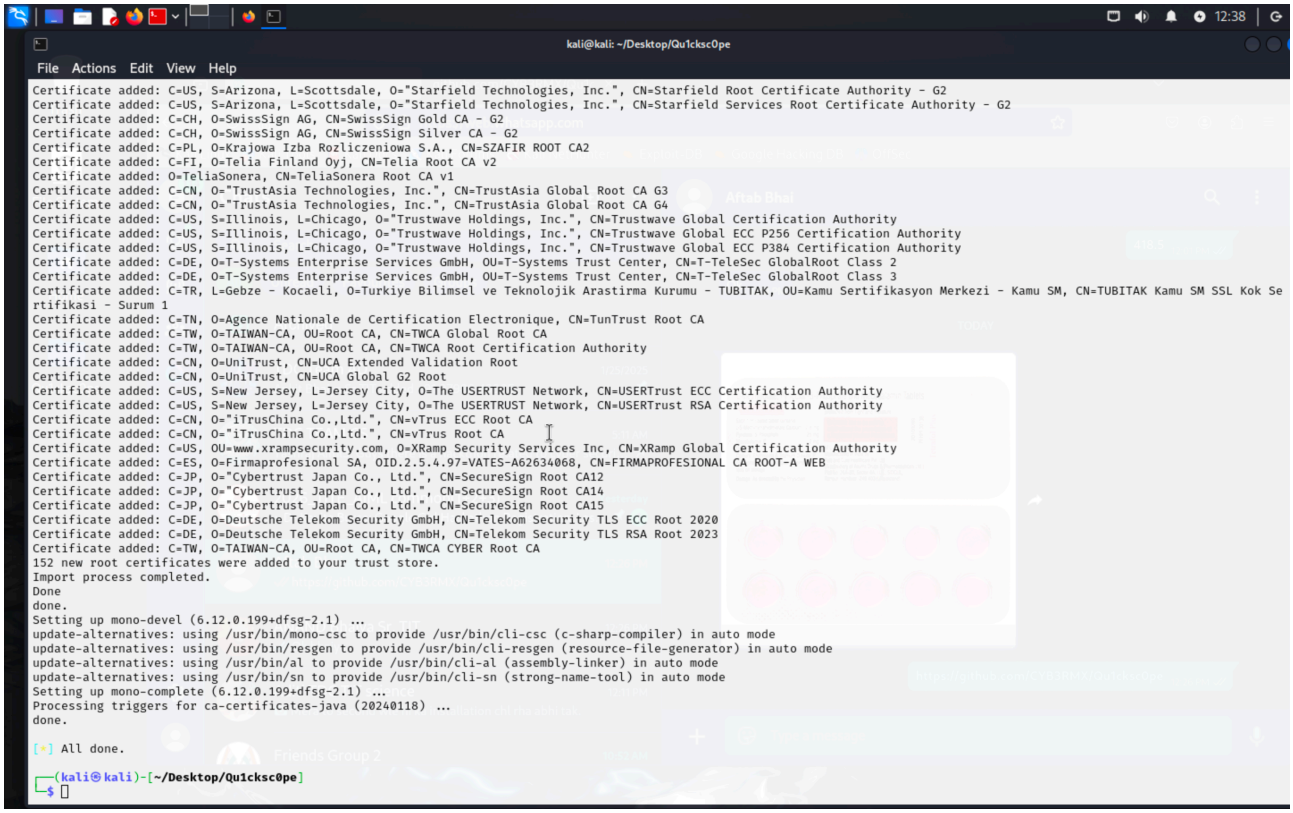
For this we use a tool Qu1cksc0pe: https://github.com/CYB3RMX/Qu1cksc0pe

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/CYB3RMX/Qu1cksc0pe
Cloning into 'Qu1cksc0pe' ...
remote: Enumerating objects: 4122, done.
remote: Counting objects: 100% (199/199), done.
remote: Compressing objects: 100% (106/106), done.
remote: Total 4122 (delta 122), reused 116 (delta 93), pack-reused 3923 (from 3)
Receiving objects: 100% (4122/4122), 109.87 MiB | 672.00 KiB/s, done.
Resolving deltas: 100% (2671/2671), done.
```

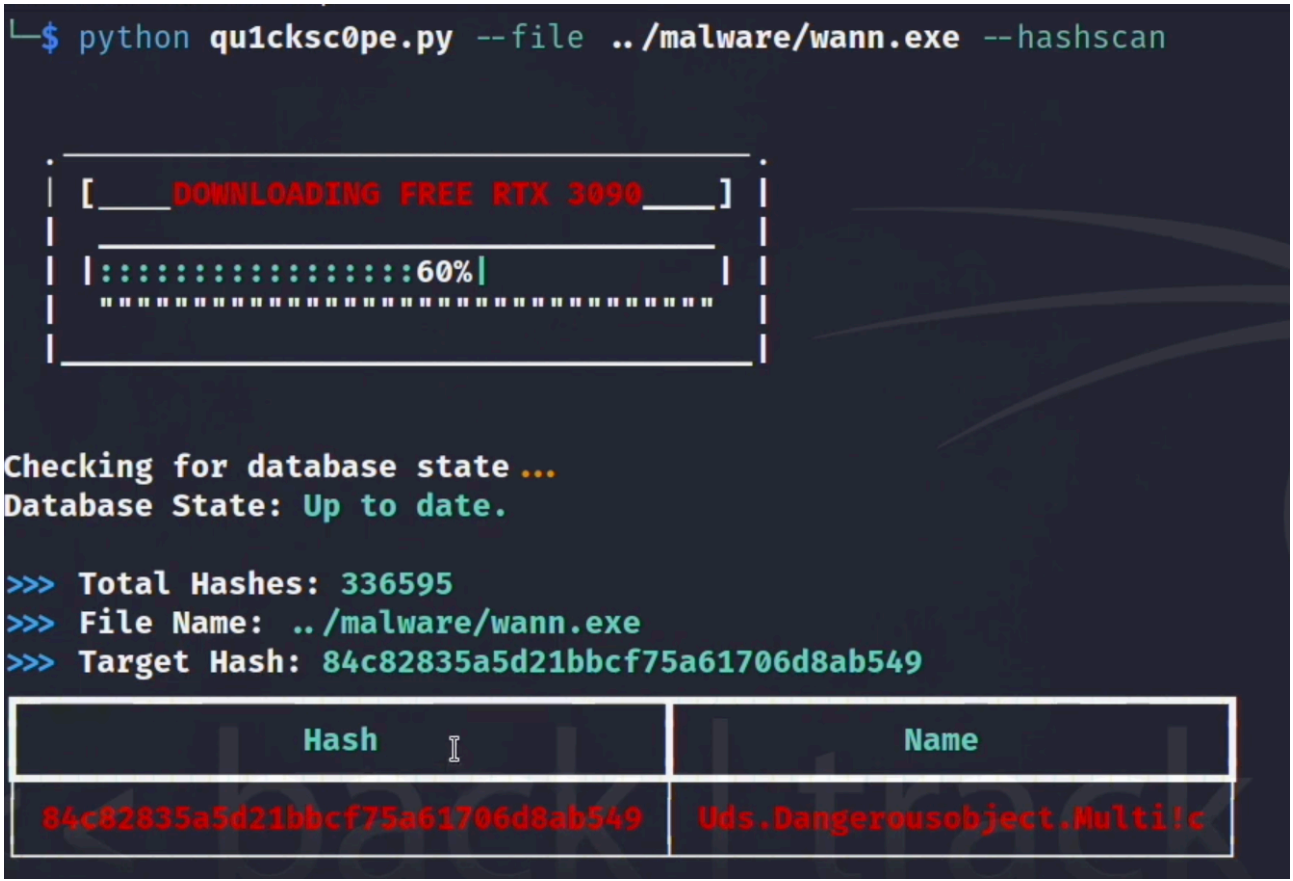
After installation we will setup this





After the setup we first
$ python quickscope.py —db_update
use this command to setup database

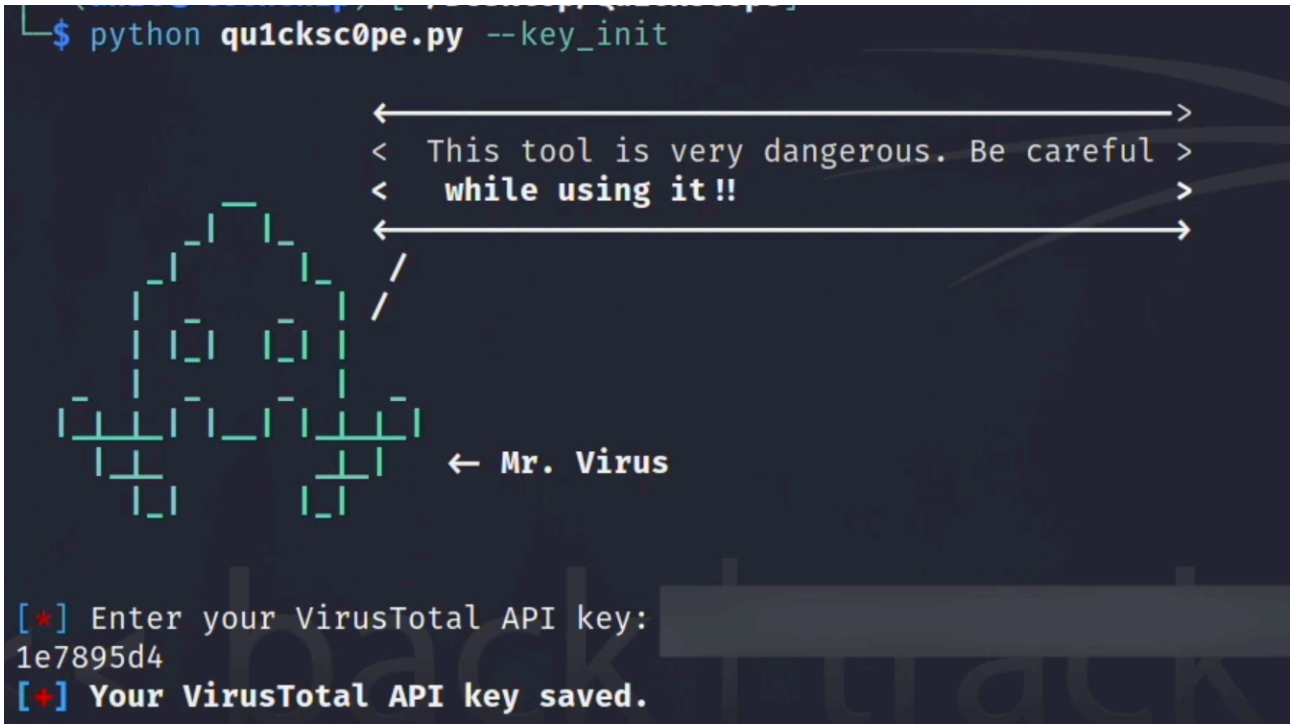
After database initialization we scan the malware



Here ../malware/warn.exe is the file location
And —hashscan is the tool which we are using

After scanning we conclude that one file is malicious which we can see in the image

For Identification of virus type we perform following steps
— > initialize api which we will get in the VirusTotal.com website



python quickscope.py --file .. /malware/see7. exe --sigcheck!

Using this command we can check which kind of file this is
this will give all the information about this file

python quickscope.py --file .. /malware/see7. exe —hashscan
Using this command we can scan whole file
this will give all the information about all the malicious files in this file

python quickscope.py --file .. /malware/see7. exe —analyze
This command analyzes the whole file

$ python quicksc0pe.py --file ../malware/infect.xls --doc
this command scans the whole document and analyzes that