Hacking Wifi Networks on Windows

CommView for Wifi is a tool for monitoring wireless 802.11 a/b/g/n/ac/ax networks. To use this product, you must have a compatible wireless adapter

CommView for Wifi is not free ($500 approx)

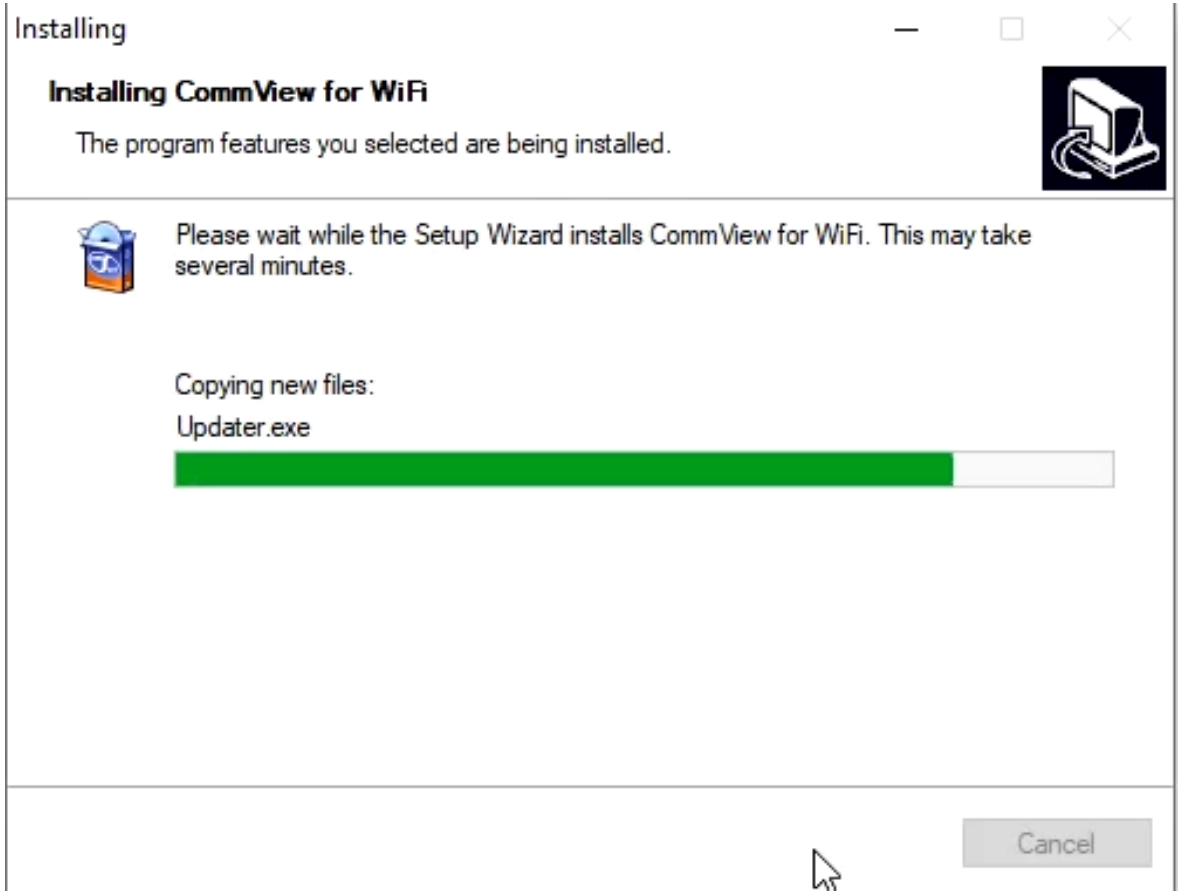
Step- 1

- Download Commview for Wifi from official website

> https://www.tamos.com/download/main/ca.php

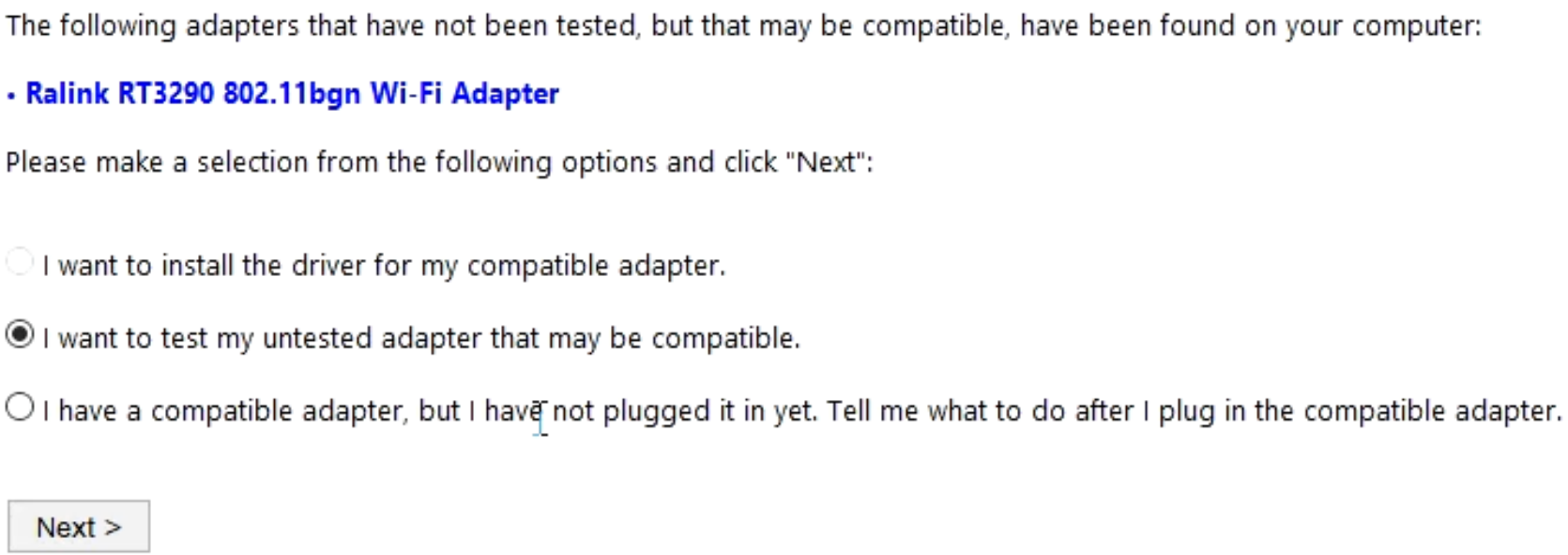
Step- 2

- Now extract the downloaded file and install it by running the setup



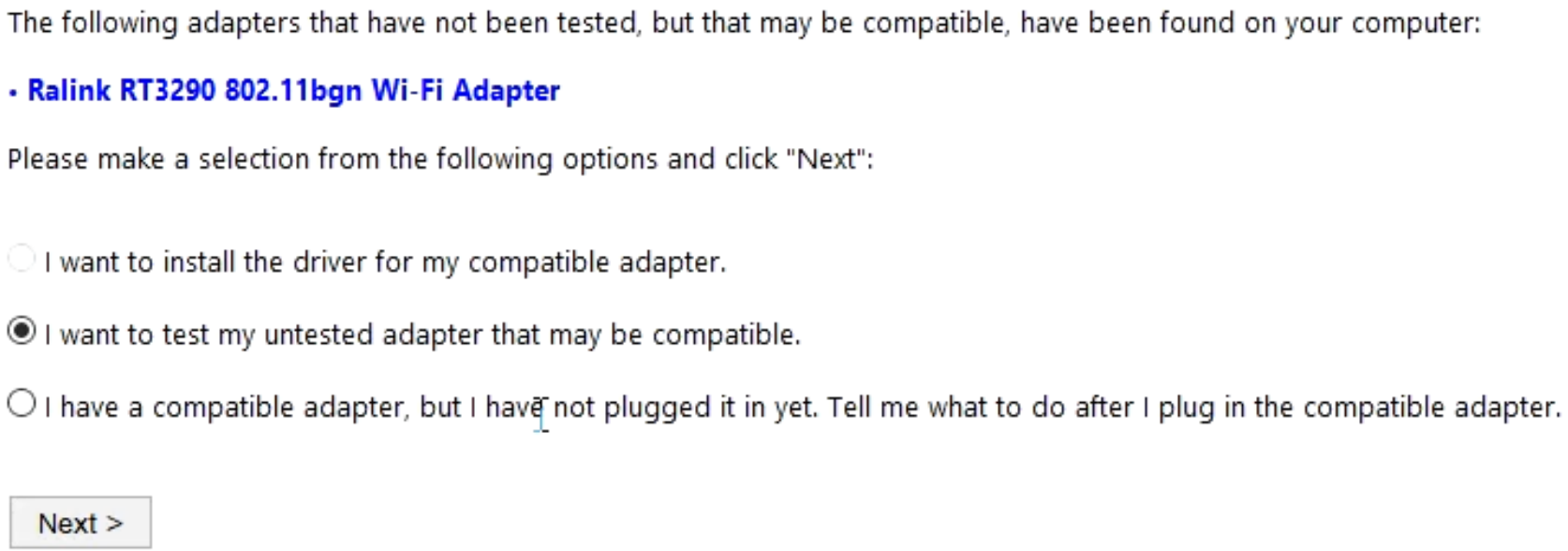
Step- 3

- Once installed, the Driver configuration page will appear. You must have a compatible wireless adapter for comm view for wifi (the list is on official website)



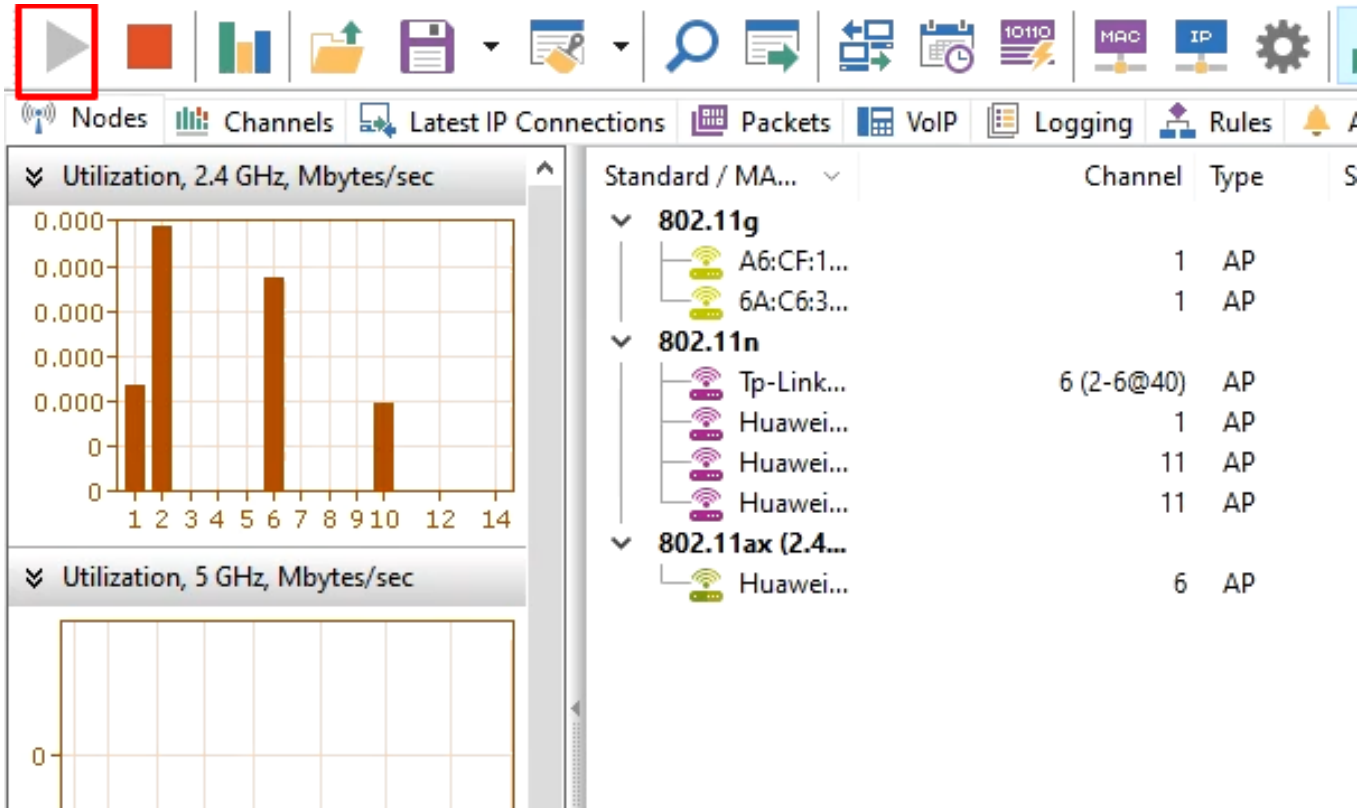
Step- 3

- Select the adapter and complete the driver configuration guide, Comm view will exit and restart



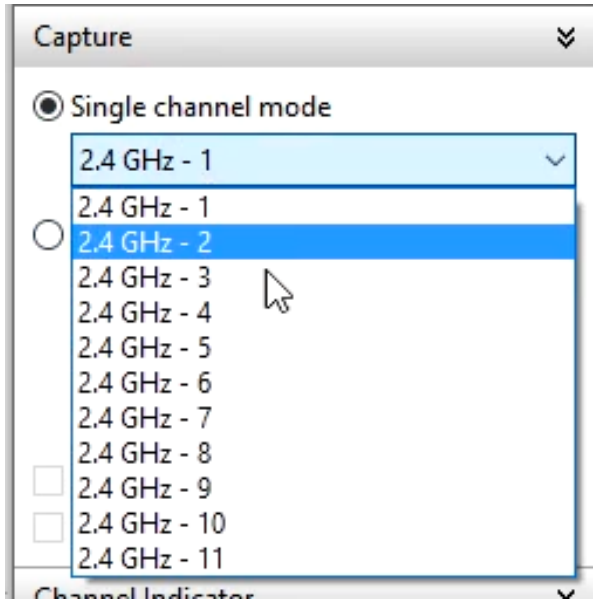
Step- 4

- Once the commview starts, press the play button to scan for available networks



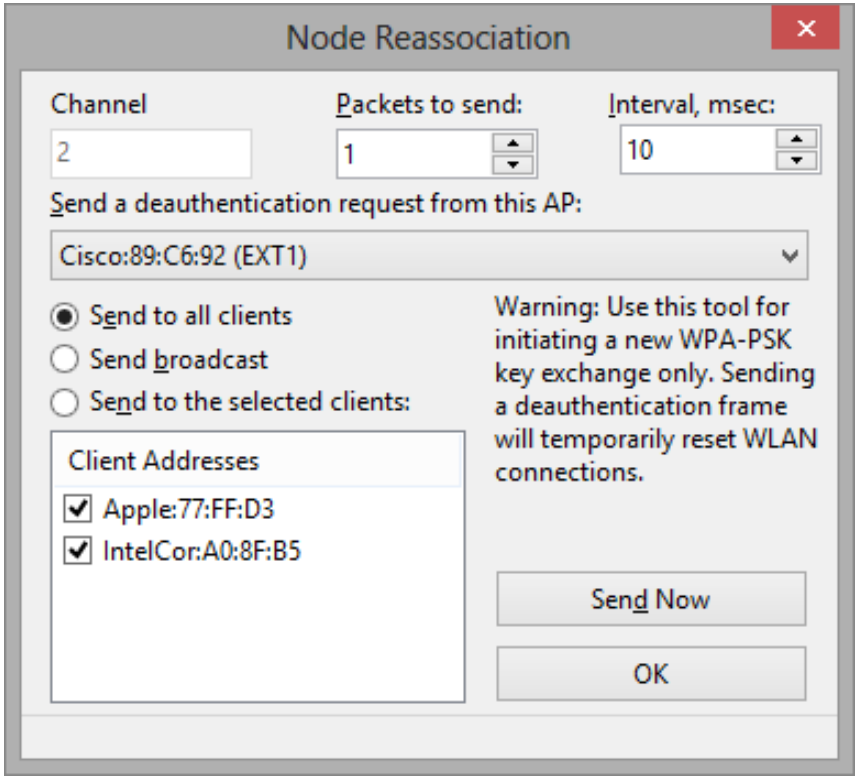
Step- 5

- Note the channel number, stop the capture and on the right hand pane select the target channel and start capture again



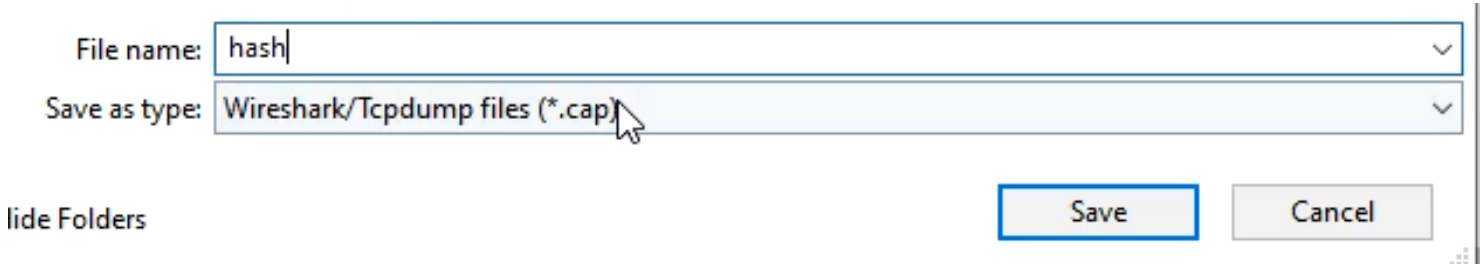
Step- 6

- If your wifi cards support injection, go to tools and perform node reassociation attack



Step- 7

- Let commview run for a few minutes and then stop the capture and save the capture as cap file



Step- 8

- Convert the cap file to hashcat format file from the following website and paste the converted file in hashcat folder

https://hashcat.net/cap2hashcat/

Step- 9

- You must have hashcat and RockYou dictionary already available from the “cracking with Hashcat tutorial”

https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

https://hashcat.net/hashcat/

Step- 10

- Open the Power shell and then use the command to crack the handshake

```
.\Hashcat.exe -m 22000 -a 0 -o cracked.txt hash.hc22000 rockyou.txt
```

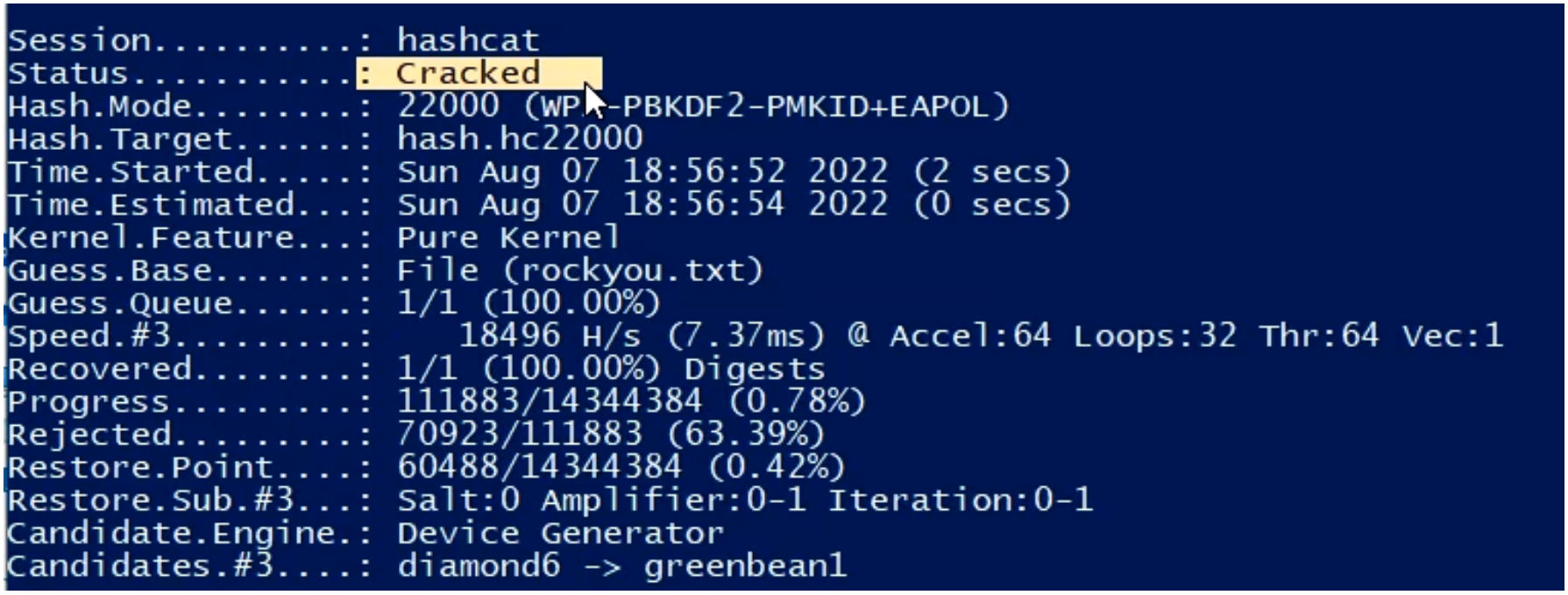
Here :

- 22000 tells the hashcat that its wifi password to be cracked
- Cracked.txt will store cracked passwords
- Hash.hc22000 is the source file
- Rockyou.txt is the dictionary file

Step- 10

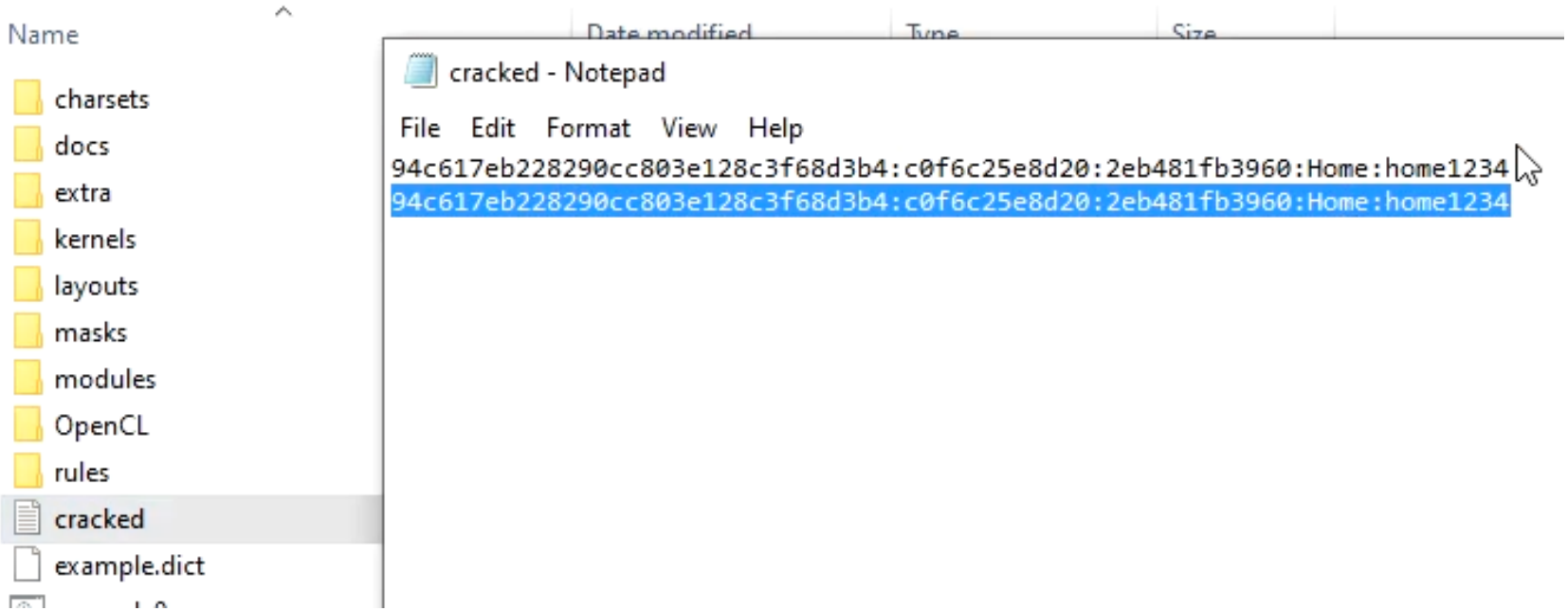
- Open the Power shell and then use the command to crack the handshake

```
.\Hashcat.exe -m 22000 -a 0 -o cracked.txt hash.hc22000 rockyou.txt
```



Step- 10

- You can check the password by opening cracked.txt file in hashcat folder



DEMO

THANKS