Preparing Handshakes For Cracking

CAPTURED HANDSHAKES

Hcxdumptool

- .pcapng file

Aircrack-ng

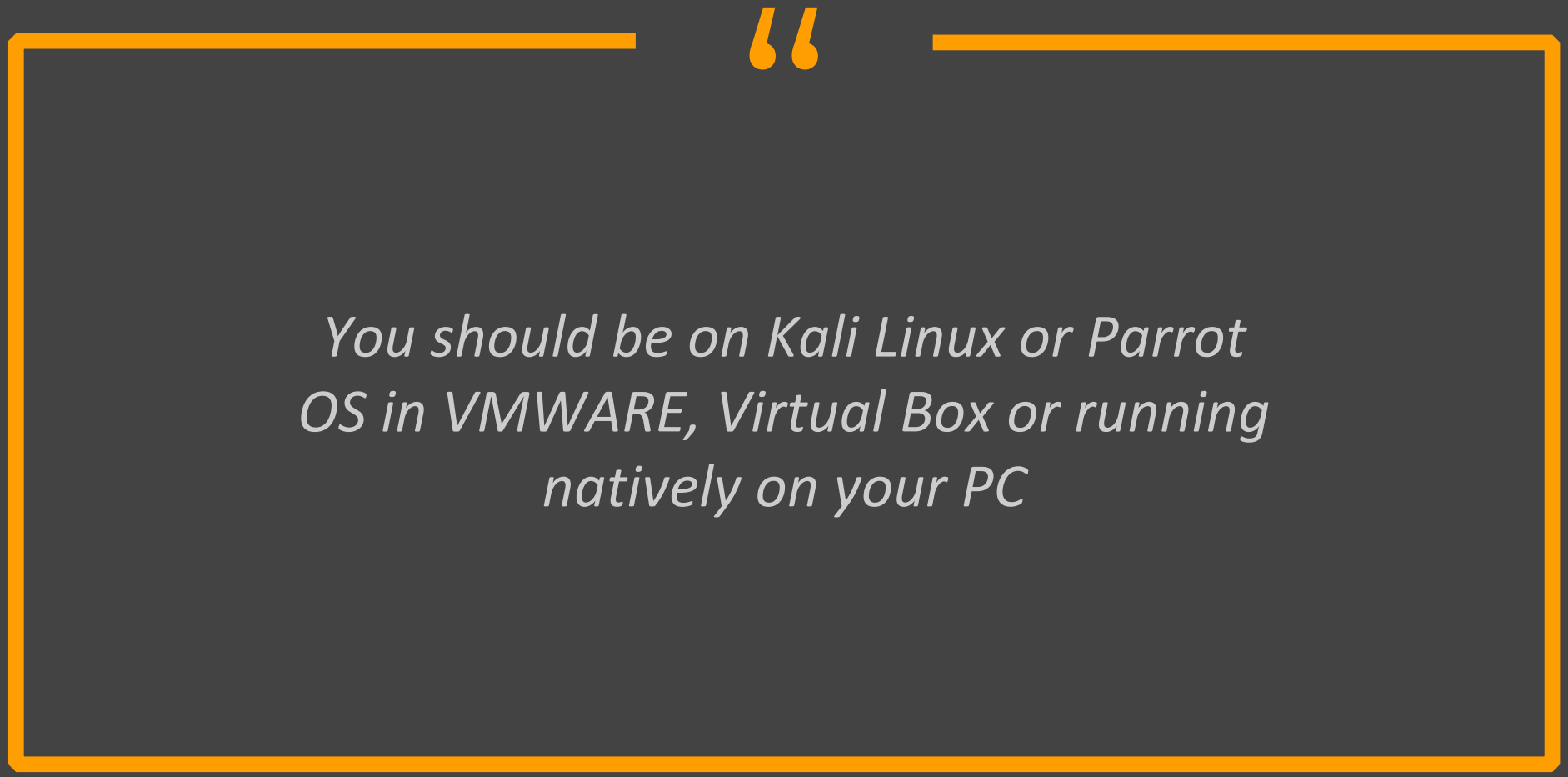
- .pcap file

.hc22000 file (for Hashcat)

Hashcat is a newer tool that can utilize GPU power to crack nearly all types of passwords. It supports multiple attacks like dictionary attacks and brute force attacks to crack more than 200 different types of passwords.

Phase-1

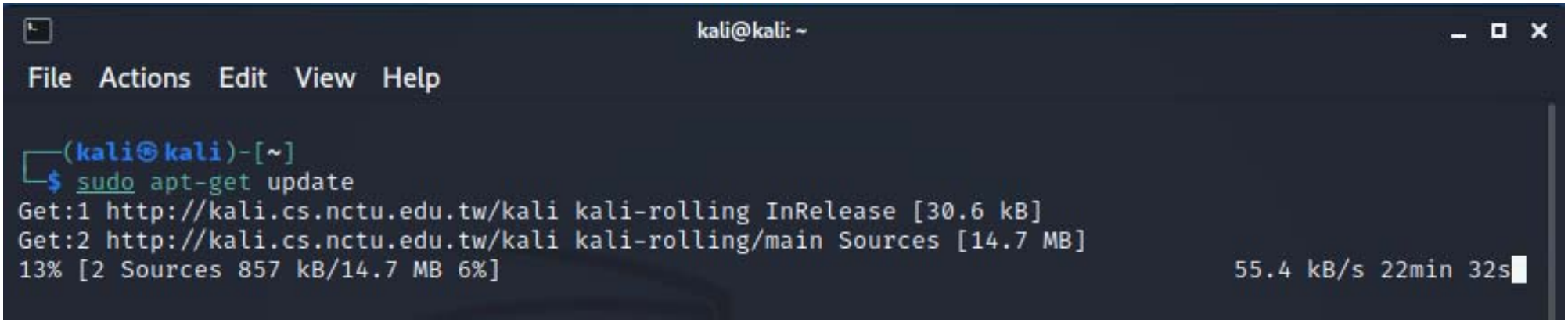
Convert Handshakes captured through Hcxdumptool



Step- 1

- Update the kali linux packages

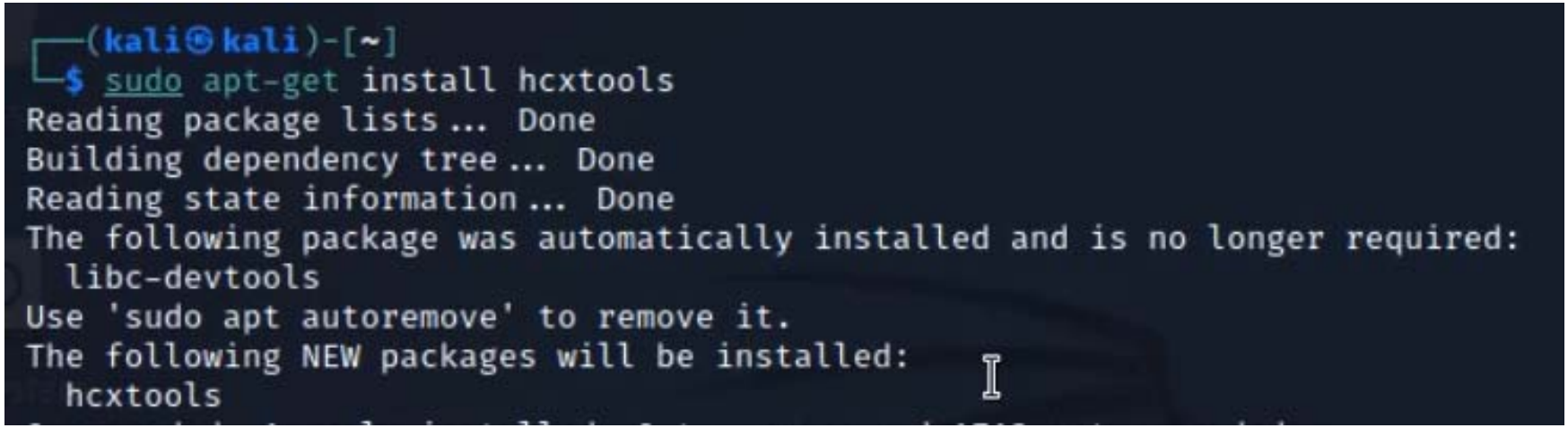
```
>sudo apt-get update
```



Step- 2

- Install the hcxpcapngtool

```
>sudo apt-get install hcxtools
```



Step- 3

- Convert the captured file with the tool

```
>hcxpcapngtool -o hash.hc22000 -E essidlist dumpfile.pcapng
```

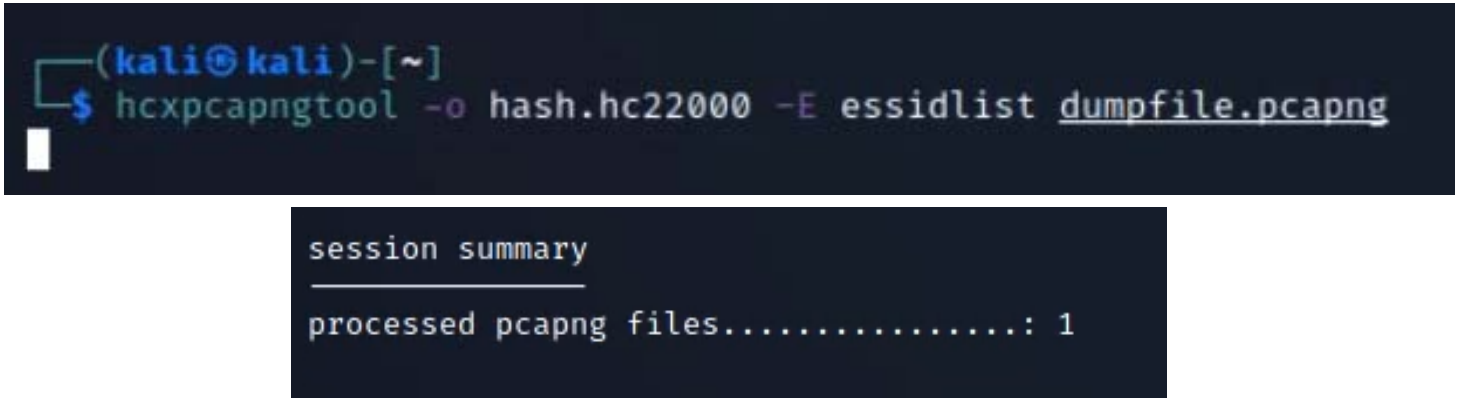
Here :

- -hash.hc22000 is the converted file
- Essid list will contain the list of SSIDs
- Dumpfile.pcapng is the source file

Step- 3

- Convert the captured file with the tool

```
>hcxpcapngtool -o hash.hc22000 -E essidlist dumpfile.pcapng
```



Step- 4

- Check the essidlist file for name of wifi networks

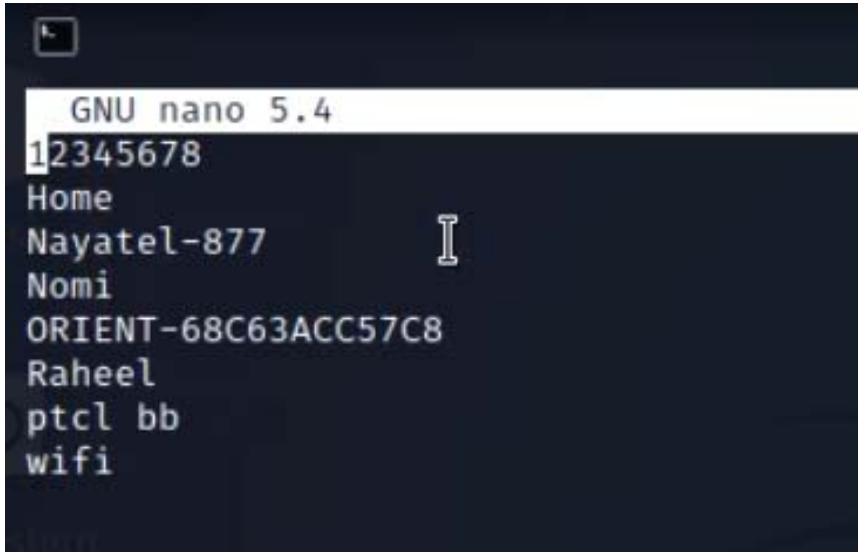
```
>nano essidlist
```

Sometimes wifi networks leak passwords and here we can see if there is some leaked password without even cracking something

Step- 4

- Check the essidlist file for name of wifi networks

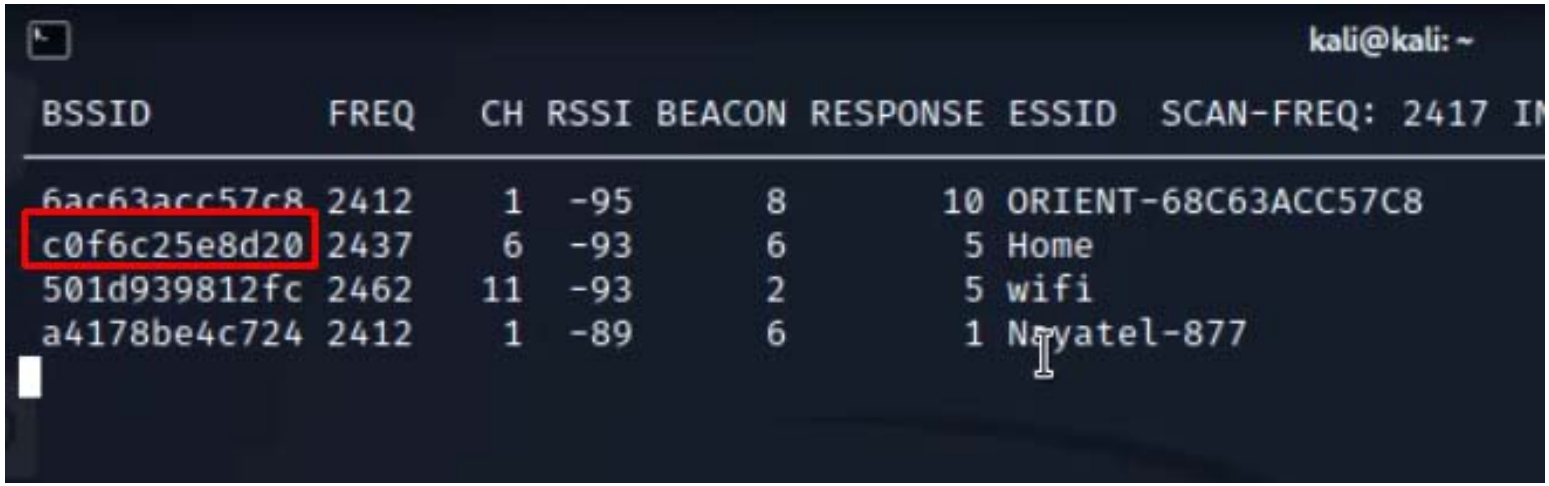
```
>nano essidlist
```



Step- 4

- Check the BSSID of our network

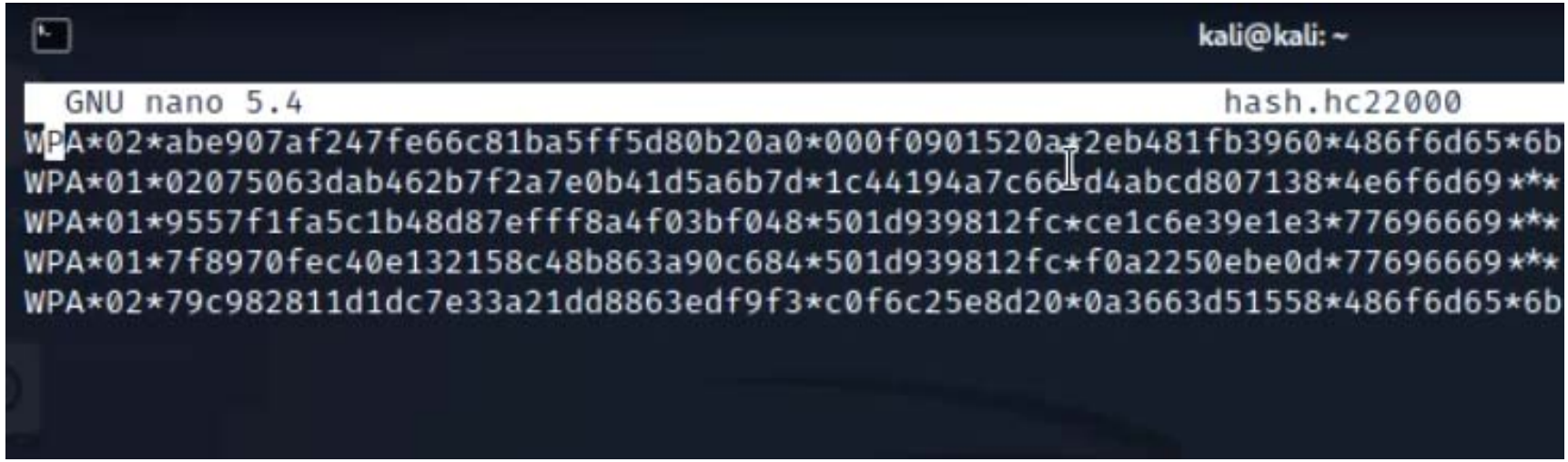
```
>sudo hcxdumptool -i wlan0 --do_rcascan
```



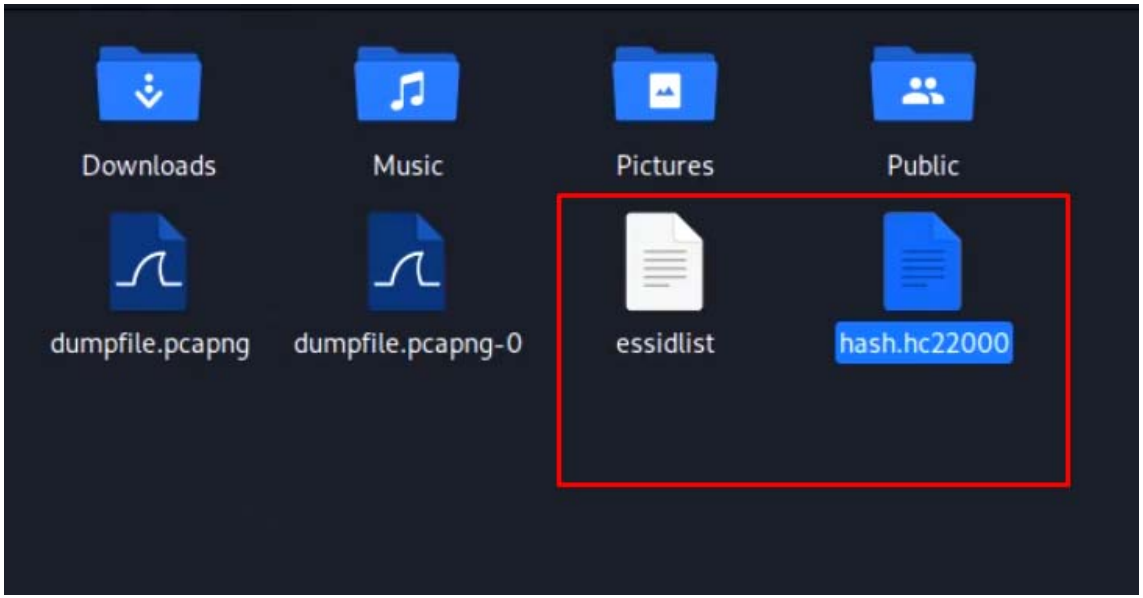
Step- 5

- Delete the excessive information and keep only the target network handshakes

```
>nano hash.hc22000
```



Now, we have our converted file hash.hc22000. Just copy it from Vmware machine to your main Windows Machine

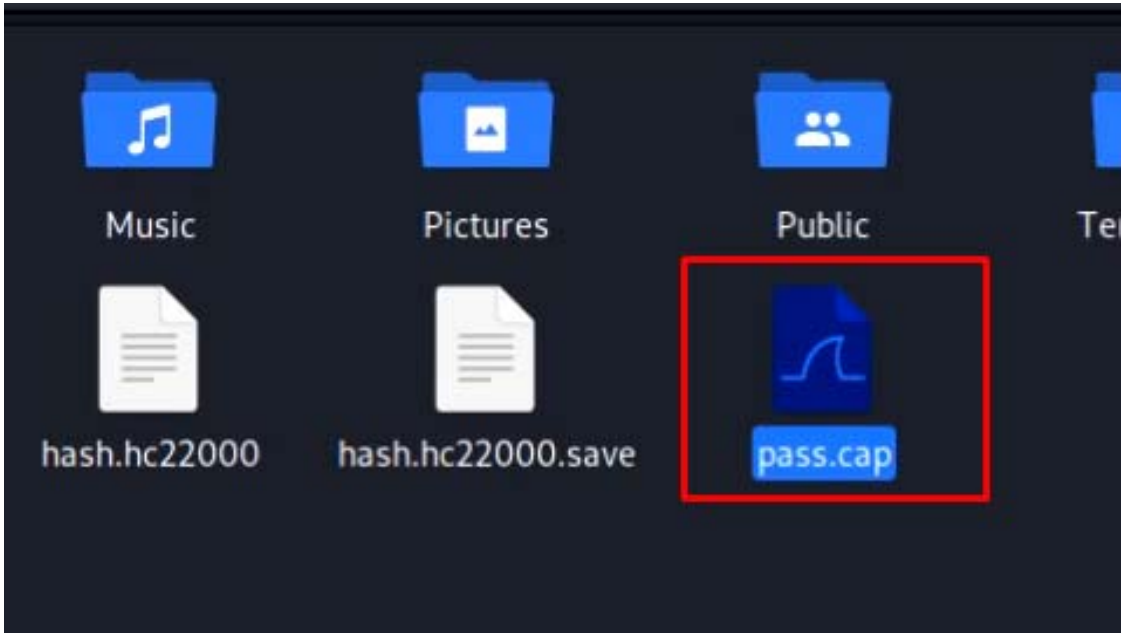


Phase-2

Convert Handshakes captured through Aircrack suite

Step- 1

- Copy the cap file from Vmware machine to Windows machine



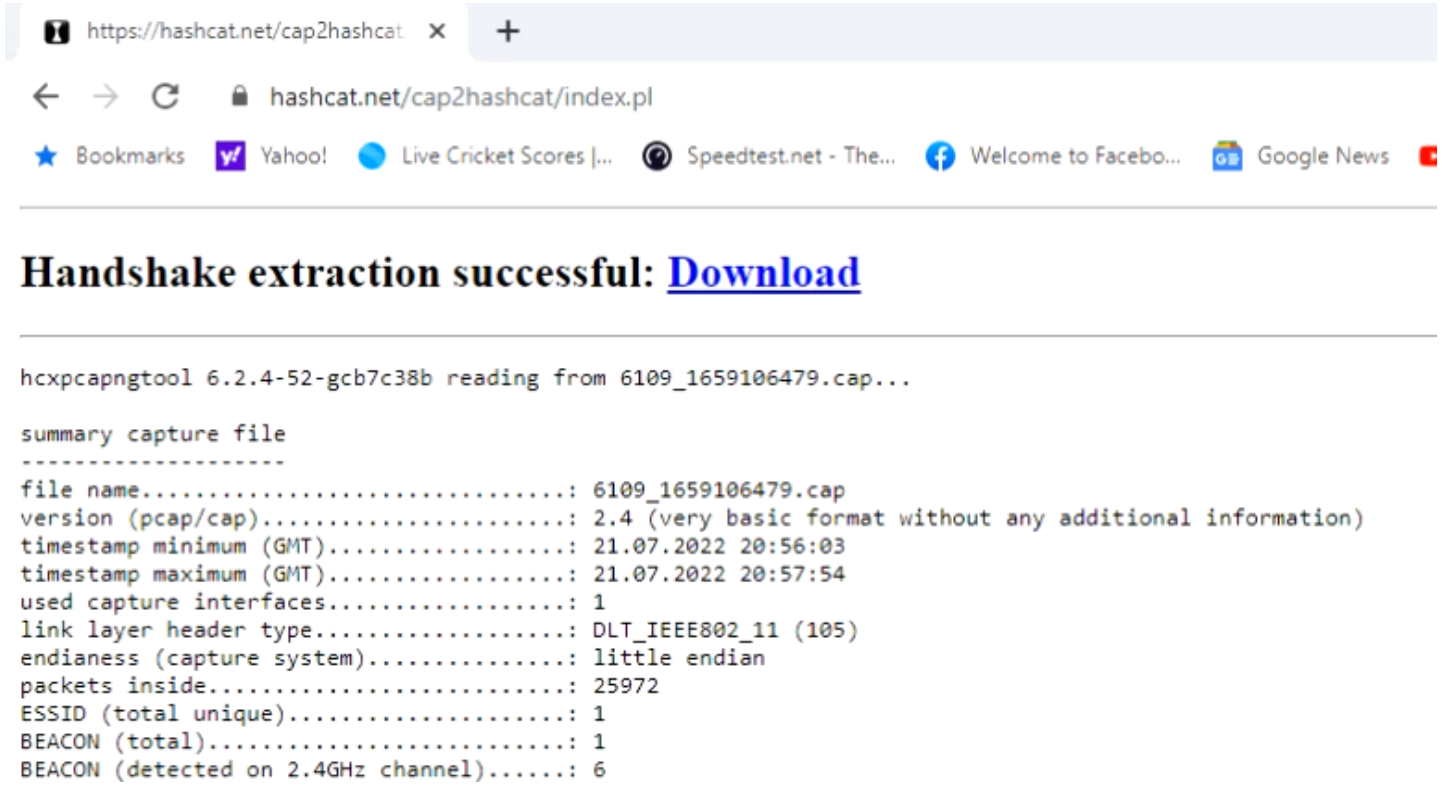
Step- 2

- Use the following official website from hashcat developers to convert the file to proper format(.hc2200)

https://hashcat.net/cap2hashcat/

Step- 3

- Download the converted file



DEMO

THANKS