

**Wifi
Hacking**

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>

Home » Main Downloads

Download CommView for WiFi

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**. To enable the monitoring features of your wireless adapter, you will need to use a special driver that comes with this product.

Alternatively, you may want to consider using the **standard, non-wireless CommView edition** that will allow you to capture your own inbound and outbound wireless network packets, without capturing the traffic generated by other wireless stations.

If your card is not on the list, please click [here](#) for the technical information, or take advantage of our **special offer** and get a compatible adapter free of charge!

Featured offer

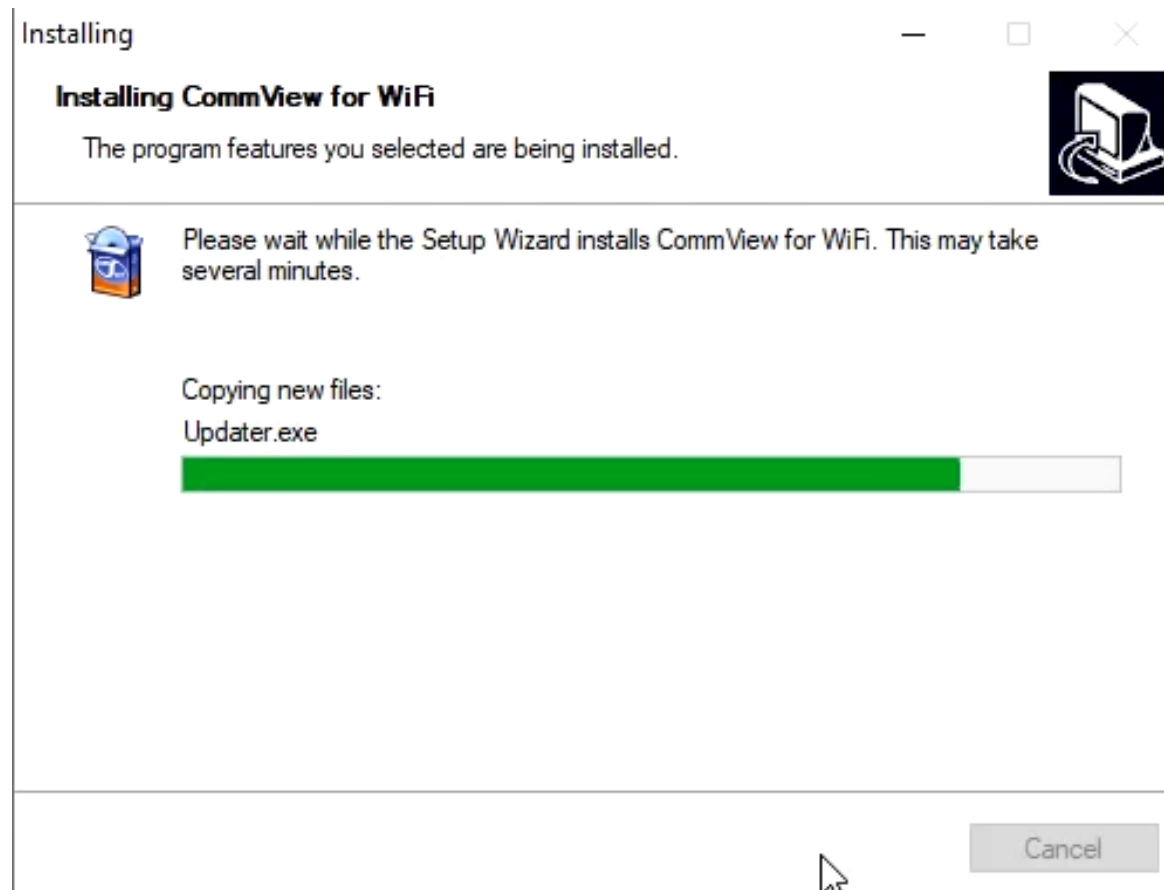
*Everything you need for site surveys
and spectrum analysis in a
super bundle!*



Download CommView for WiFi

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)

The following adapters that have not been tested, but that may be compatible, have been found on your computer:

- **Ralink RT3290 802.11bgn Wi-Fi Adapter**

Please make a selection from the following options and click "Next":

- I want to install the driver for my compatible adapter.
- I want to test my untested adapter that may be compatible.
- I have a compatible adapter, but I have not plugged it in yet. Tell me what to do after I plug in the compatible adapter.

Next >

Step- 3

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

The following adapters that have not been tested, but that may be compatible, have been found on your computer:

- **Ralink RT3290 802.11bgn Wi-Fi Adapter**

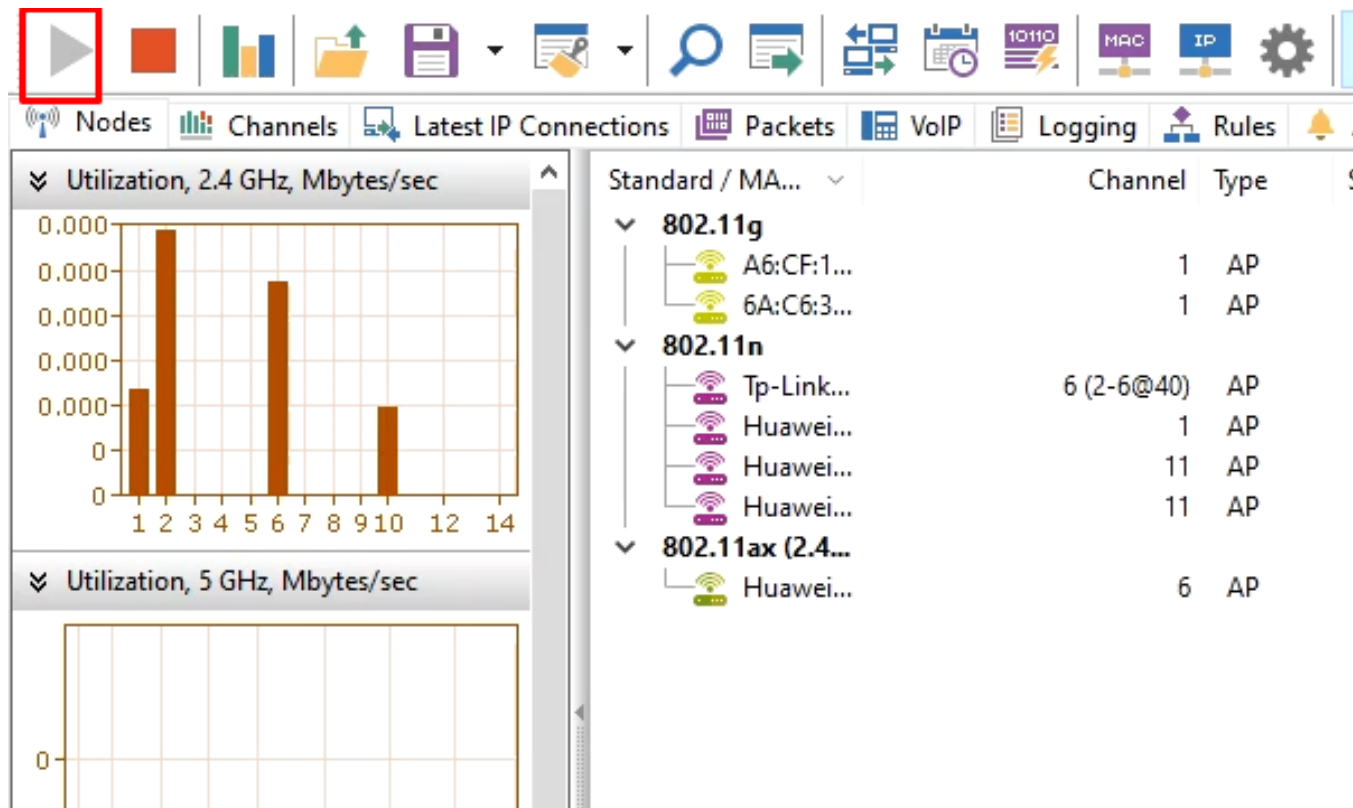
Please make a selection from the following options and click "Next":

- I want to install the driver for my compatible adapter.
- I want to test my untested adapter that may be compatible.
- I have a compatible adapter, but I have not plugged it in yet. Tell me what to do after I plug in the compatible adapter.

Next >

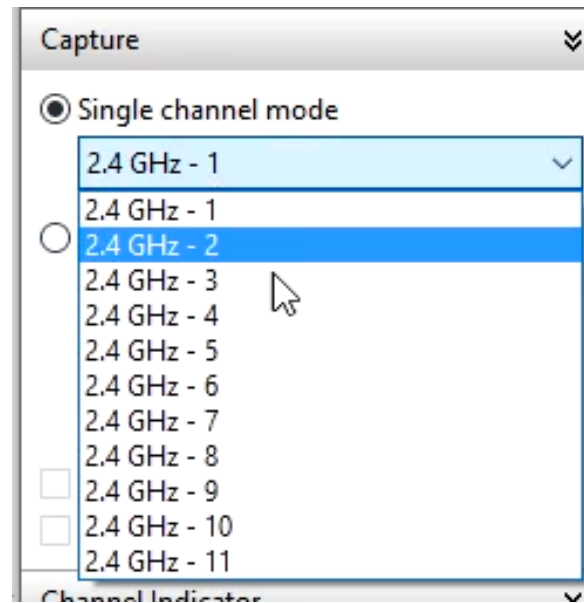
Step- 4

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



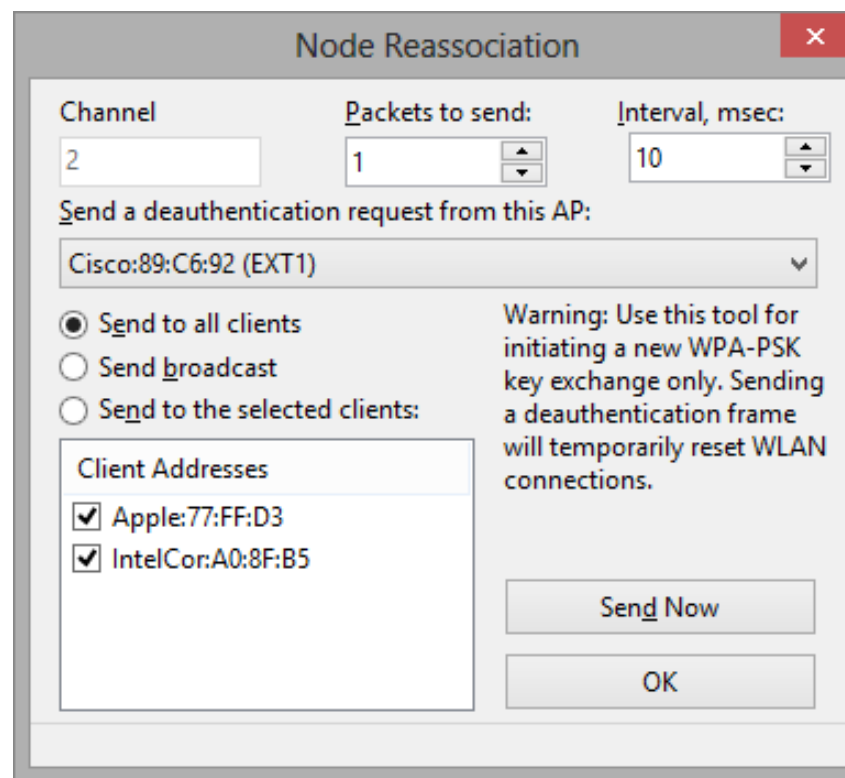
Step- 5

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



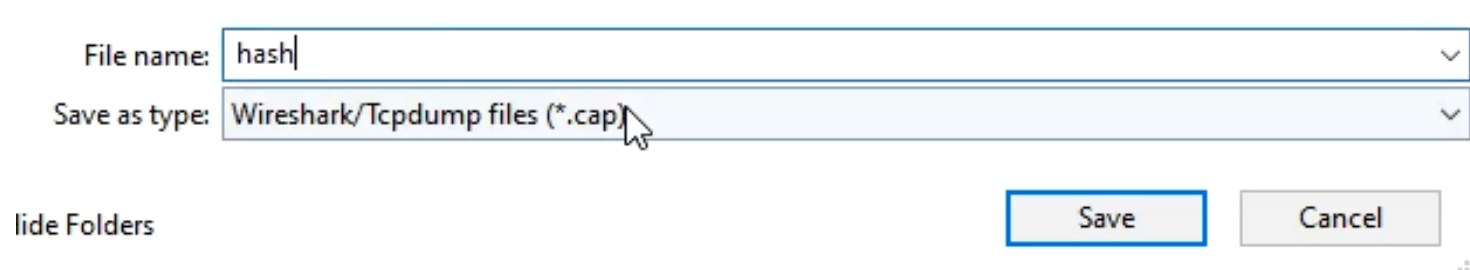
Step- 6

- ❖ 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

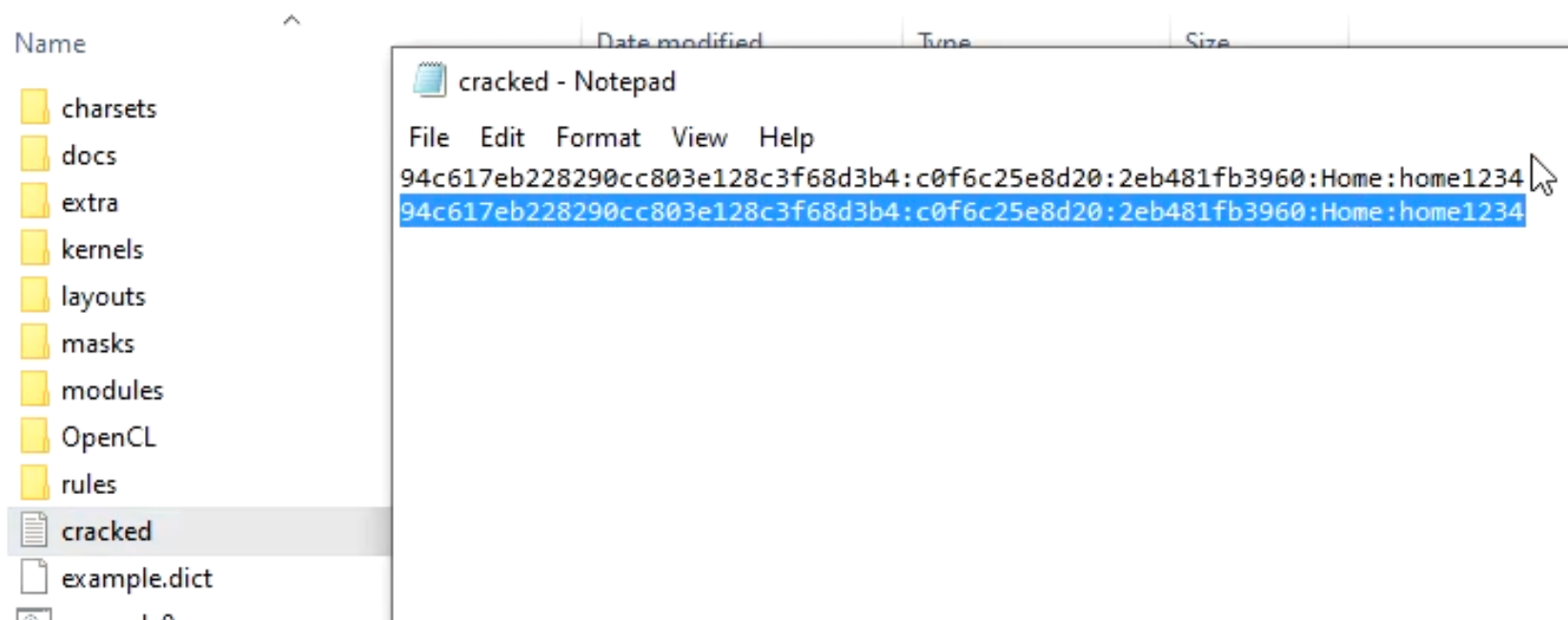
- ❖ Open the Power shell and then use the command to crack the handshake

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

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 22000 (WPB-PBKDF2-PMKID+EAPOL)
Hash.Target....: hash.hc22000
Time.Started...: Sun Aug 07 18:56:52 2022 (2 secs)
Time.Estimated...: Sun Aug 07 18:56:54 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#3.....: 18496 H/s (7.37ms) @ Accel:64 Loops:32 Thr:64 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 111883/14344384 (0.78%)
Rejected.....: 70923/111883 (63.39%)
Restore.Point...: 60488/14344384 (0.42%)
Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#3...: diamond6 -> greenbean1
```

Step- 10

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





DEMO



THANKS