# USER GUIDE

## WiCC – Wifi Cracking Camp

Wireless pentesting tool with functionalities such as password cracking (in WEP and WPA/WPA2 networks), DoS attacks, client de-authentication, and data decryption.

This user guide is for version 1.0

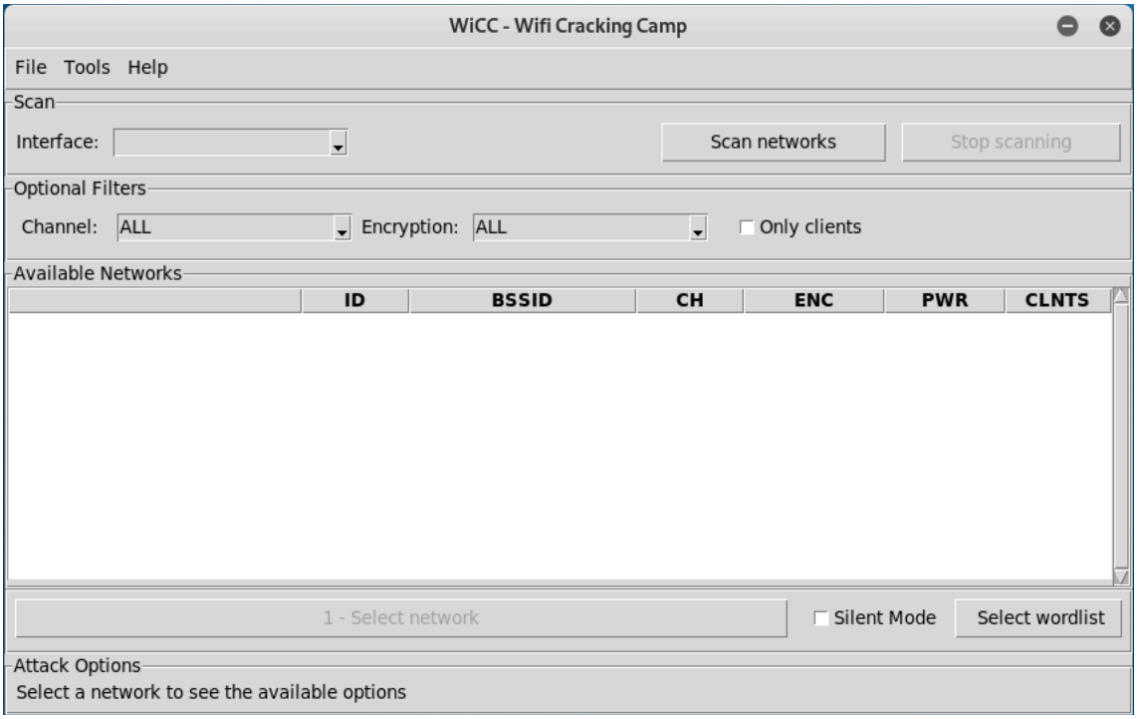
# Tabla de contenido

## 1. Simple attack

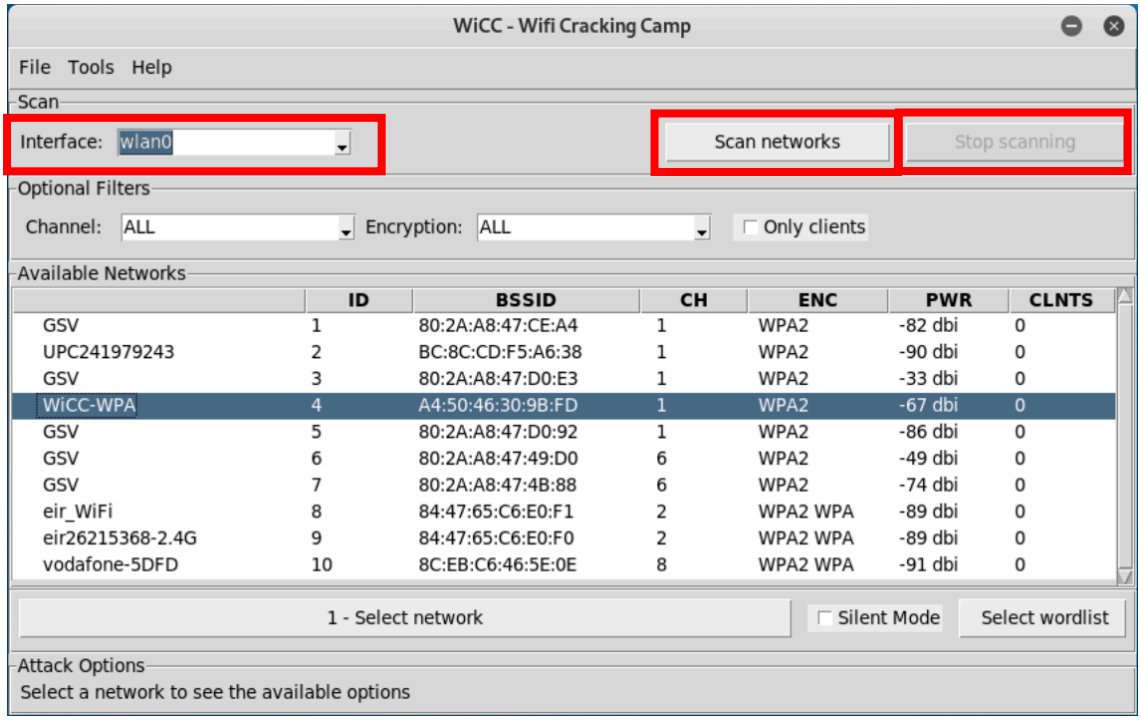
The application must be start on the terminal, to do it go to the application directory and execute the following command:

*$ sudo python3 WiCC.py [options]*

When the application starts shows a splash window and after a couple of seconds the main window will start. In this window are the minimum required features to execute an attack against a network.



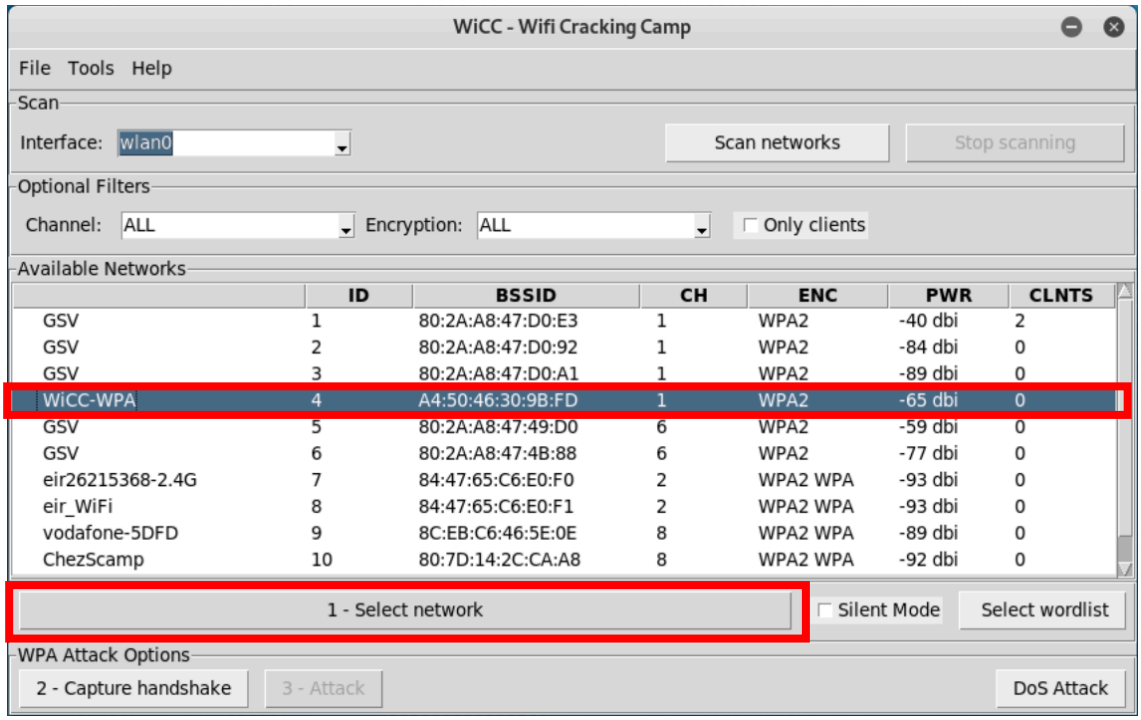

The first thing to do is to choose an interface from the list. In this list are all wireless interfaces detected by the application. After selecting one, the next step is to scan the available networks by clicking on the *Scan networks* button. The application remain scanning until the *Stop scanning* button is pressed, and all detected networks are added (in live mode) to the list. During the scan all buttons will be disabled except the *Stop scanning* button.



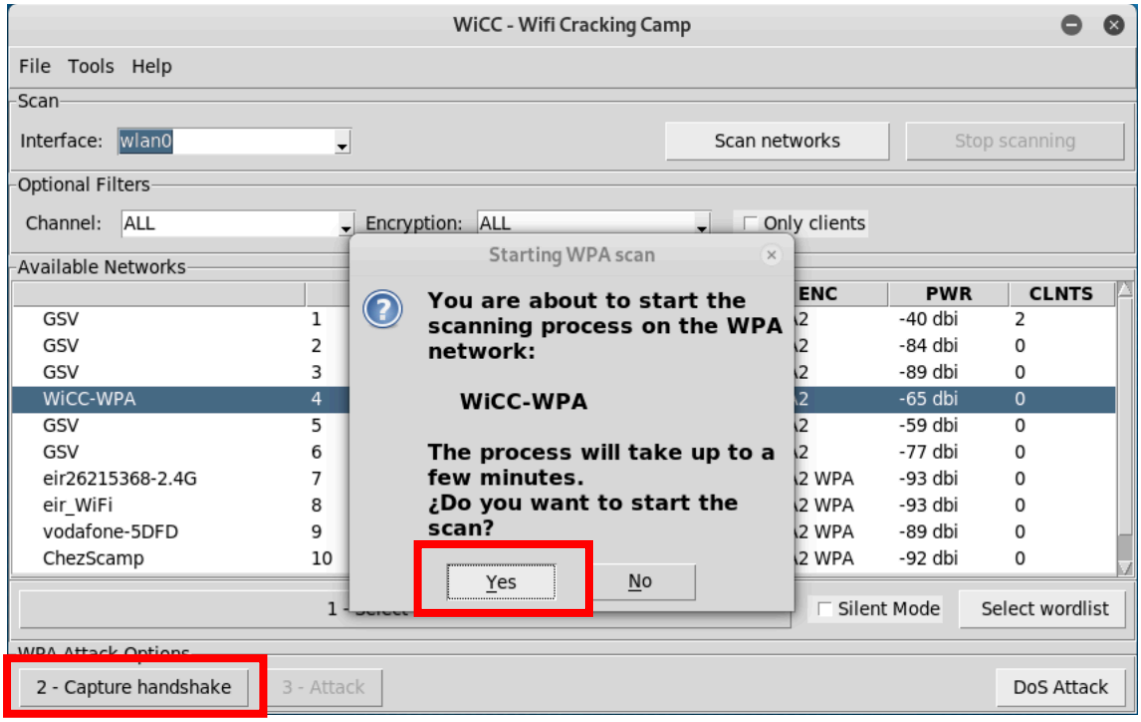

After stopping the scan is time to select the network to attack. To do this you have to click on the network and then click on *Select network* button. After that the *Attack Options* frame will show the available options to attack the network. These options will be different for WEP and WPA/WPA2 encryption types.

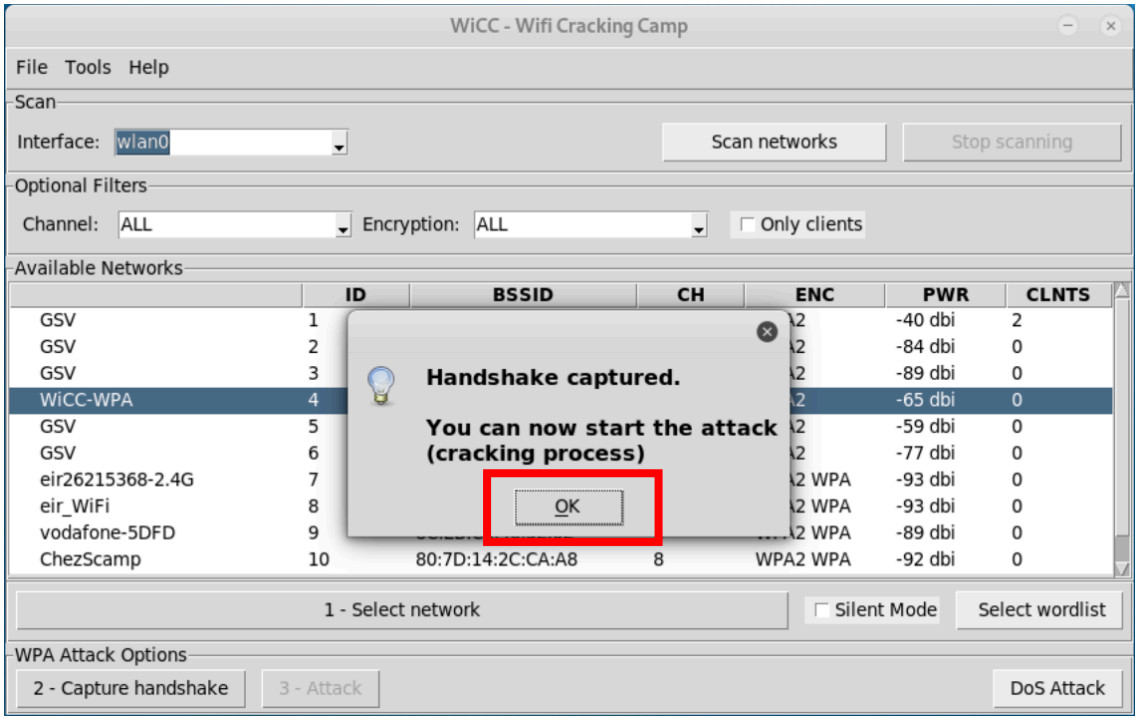
For this test we have a couple of networks (WEP and WPA2) expressly created to perforform the tests: WiCC-WPA and WiCC_WEP.

- WPA

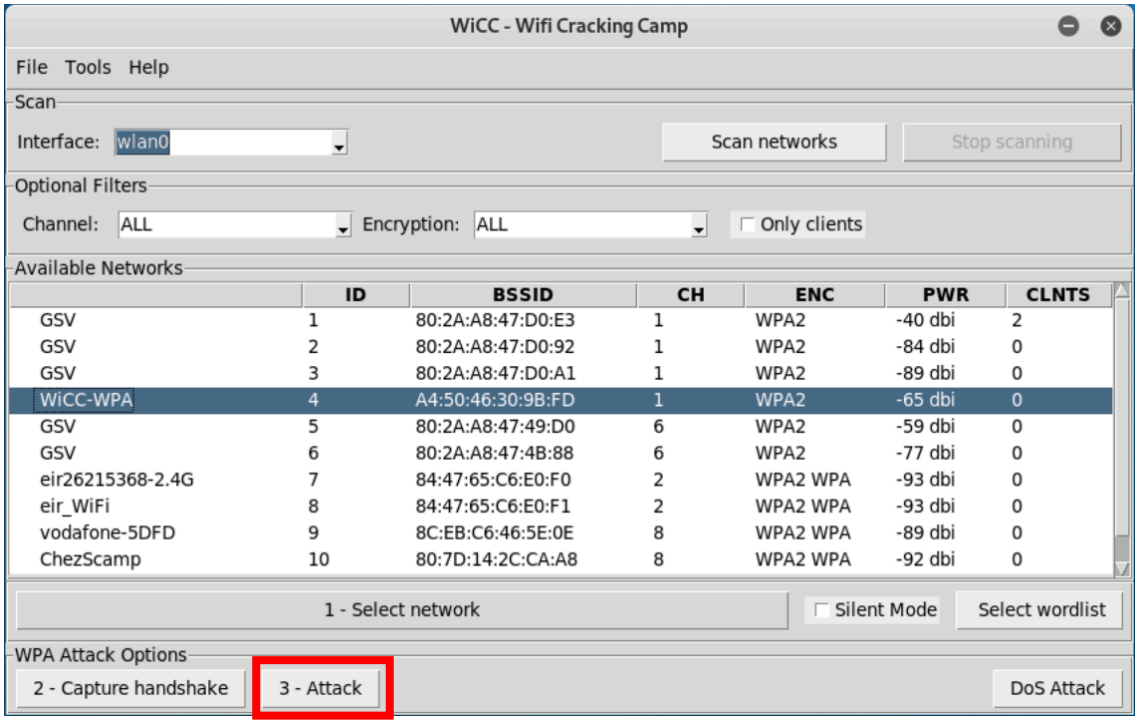


For the WPA/WPA2 networks the options are scan and attack. It is a two steps process, the *Capture handshake* button captures the handshake and the *Attack* button cracks the handshake file using a wordlist. By default the selected list is *rockyou.txt* which is included in the application resources.
To start the scan, press the *Capture handshake* button, until this button is pressed the resting buttons will remain disabled. The application gives feedback each time a process has finished.
The process starts when the pop-up's *Yes* button is pressed, at the end will show another pop-up with a success or failure message.

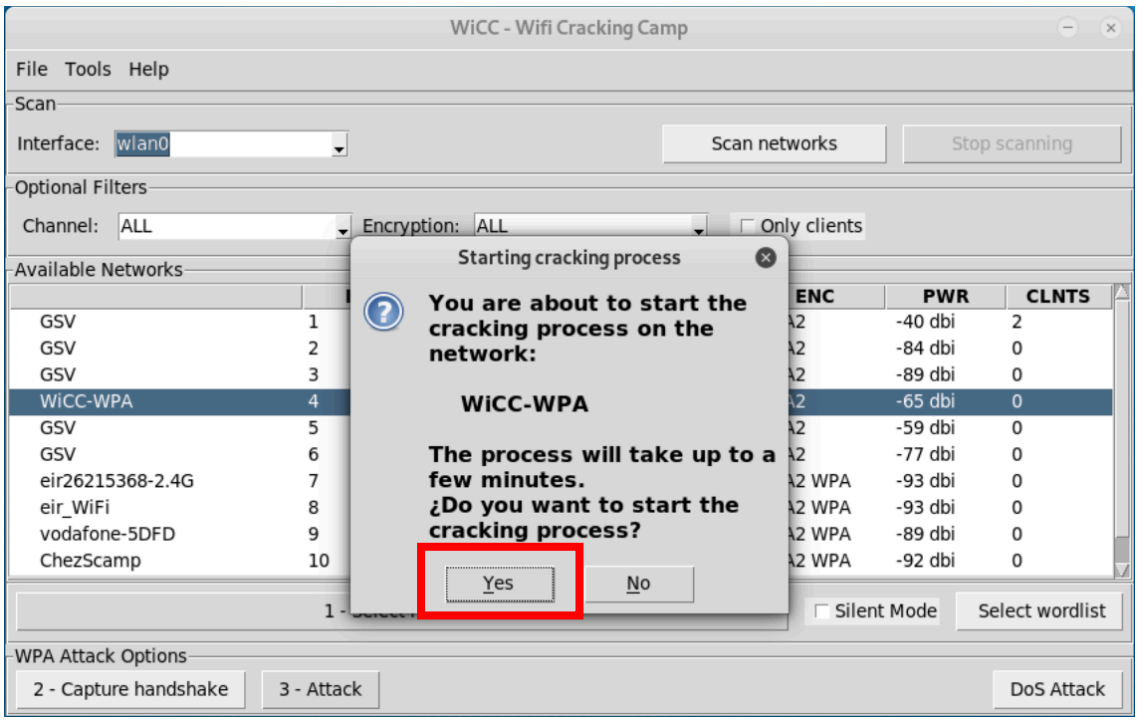




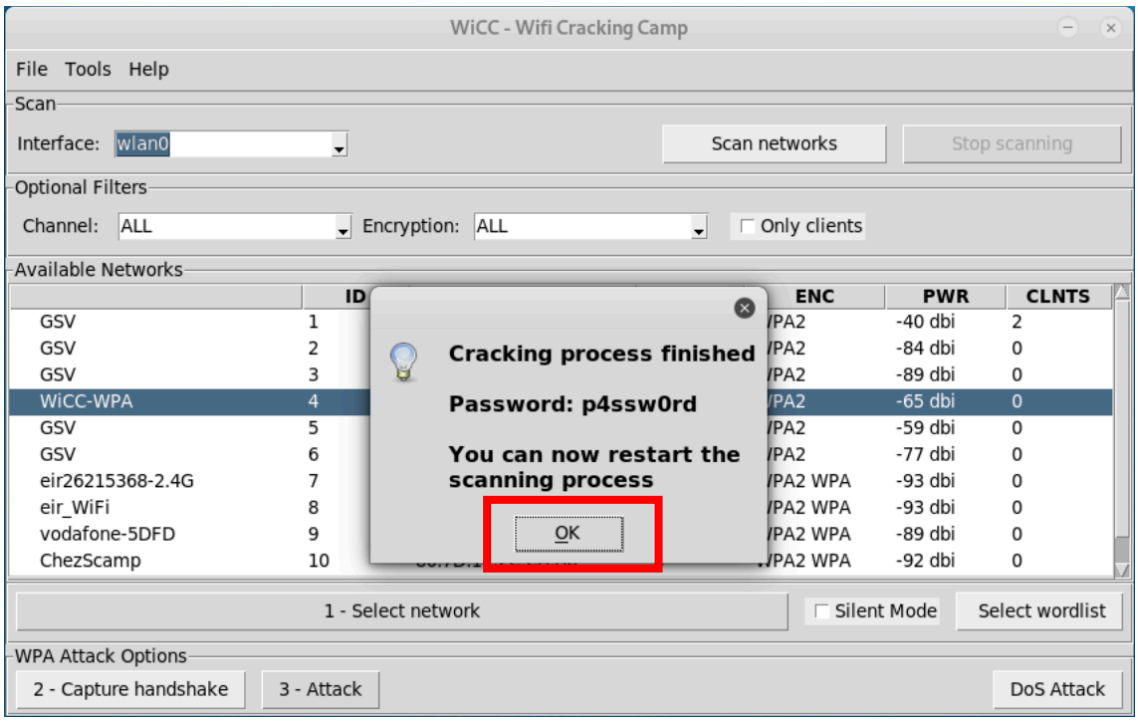

After clicking on de *OK* button in the pop-up window, the *Attack* will be enabled .Click on the button to start the process. Another pop-up will appear after that.



Click *Yes* to continue and start the cracking process.

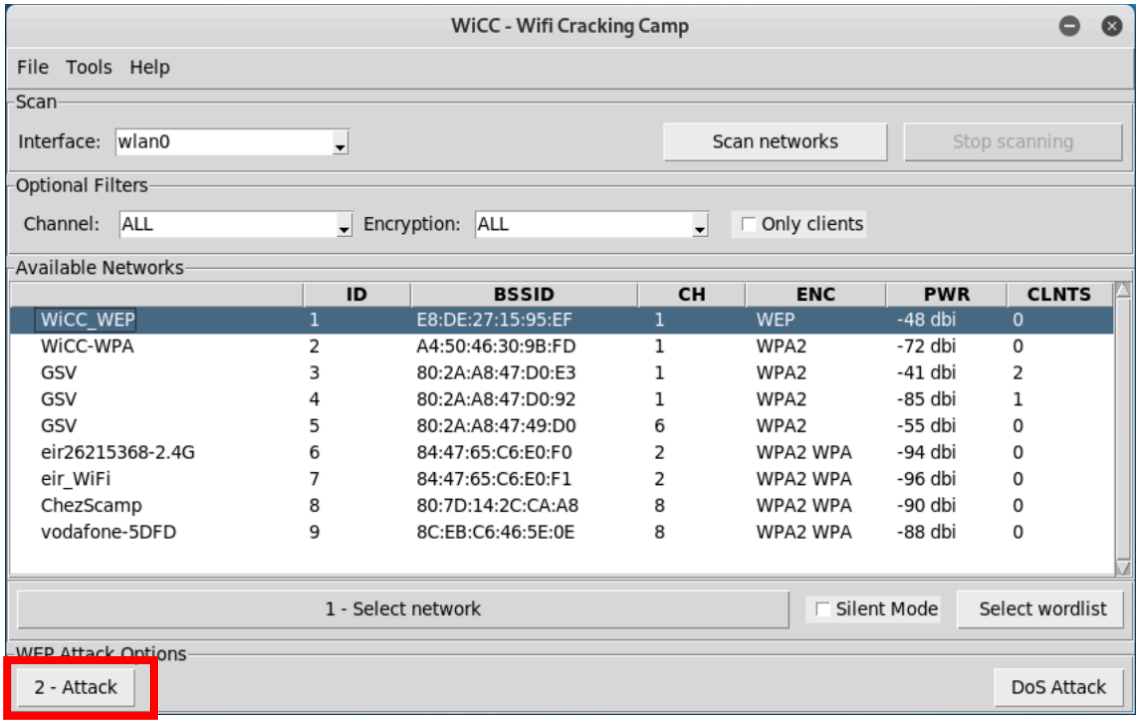



When the process finishes, the cracked password is shown in another pop and stored in the *crackednetworks* file in the *savefiles* folder. Press *OK* to return to the main window.



- WEP

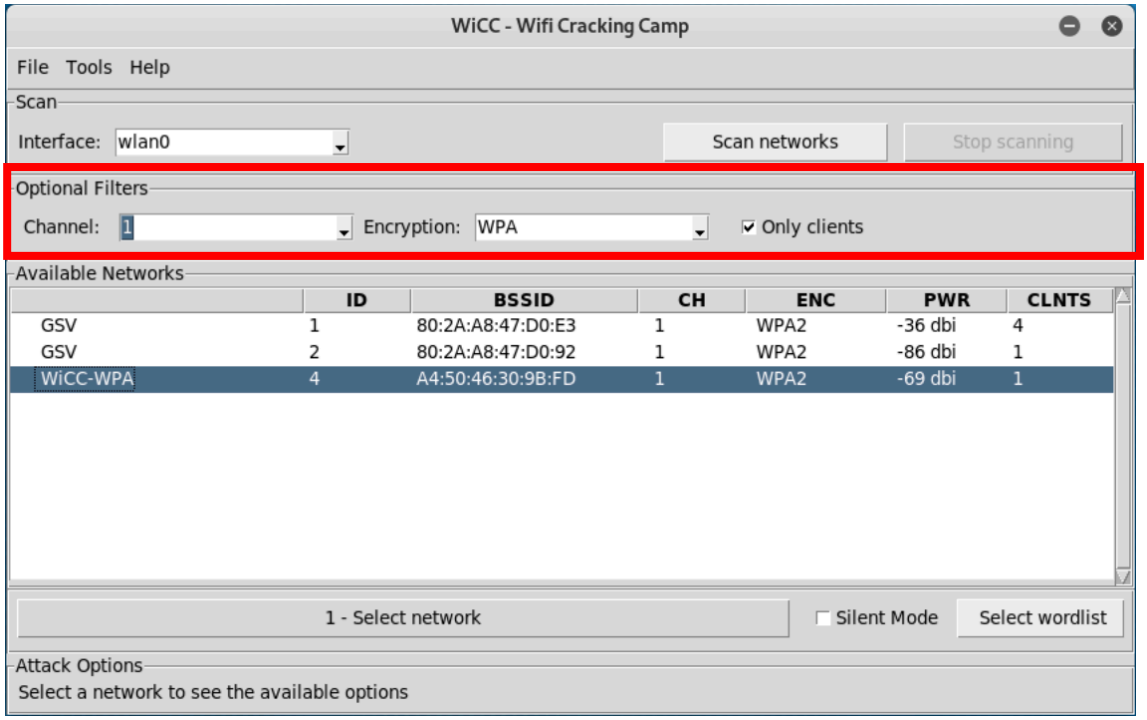
The WEP attack options are simpler than the WPA/WPA2 ones. This section only have an *Attack* and *Stop attack* buttons. The *Attack* button will execute the whole attack. The *Stop* button will only be enabled during the attacking process. The password will be also added to the *crackednetworks.txt* file.




## 2. Filters and options

To be more productive, the application include some filters to speed up the scan. These options permits to show networks only in a desired channel, with a desired encryption, and remove the networks without clients. All this stuff is on the *Filters* frame.

By default this filters are not activated, so in a normal scan will appear all founded networks.



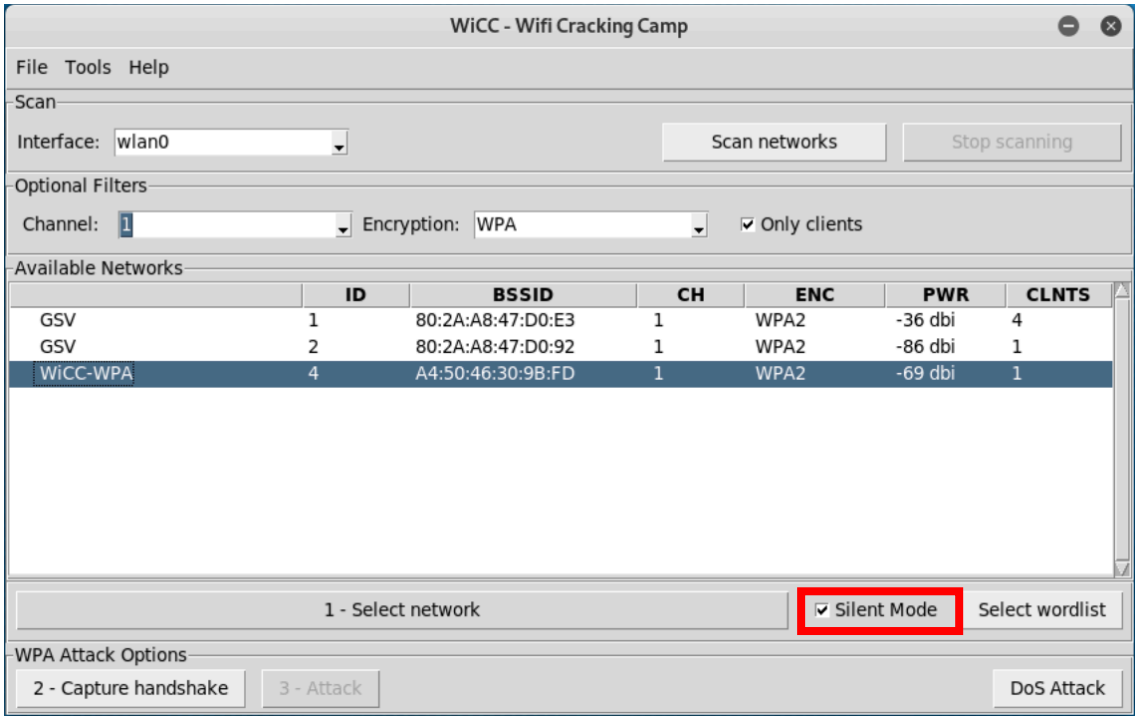

## 3. Silent mode

By default when attacking a network the application interacts with the networks.

- In the case of WEP performs a fake authentication, packet injection, and ARP Replay.
- In the WPA/WPA2 the application deauthenticates clients to increase the velocity during the handshake capture.

Performing this, the victim can detect the attack and interrupt it.

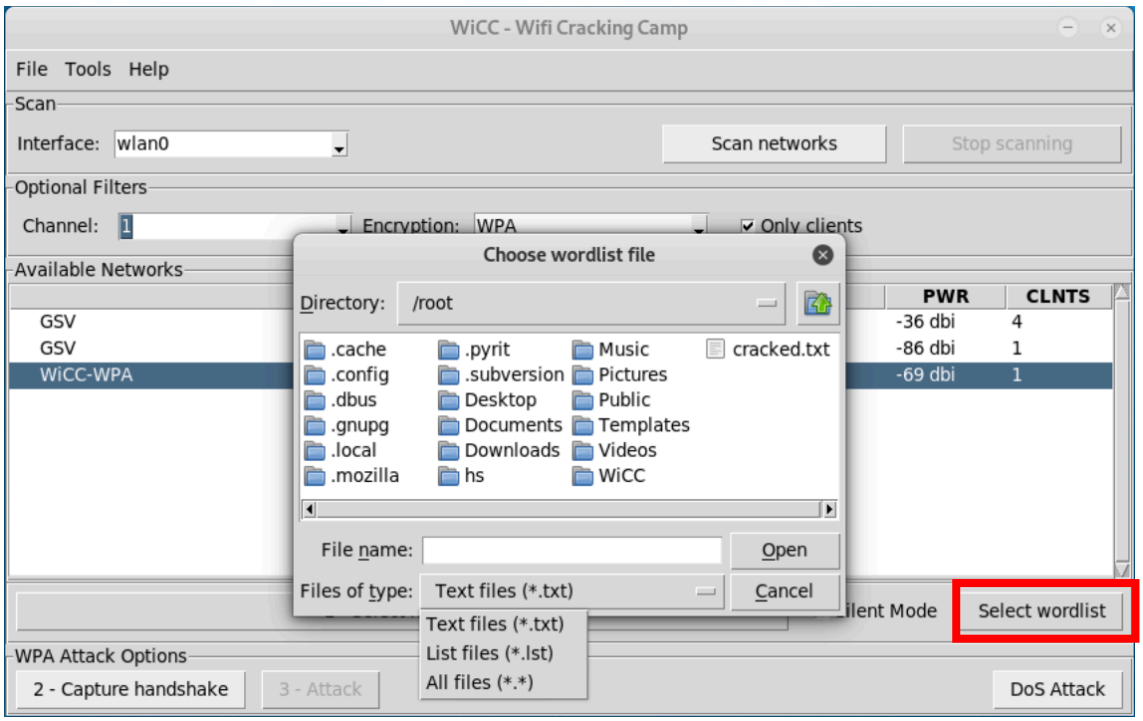
Activating the *Silent mode* option, the application will be invisible by avoiding all direct interaction with the AP. This mode will make the scan slower.




## 4. Custom wordlist

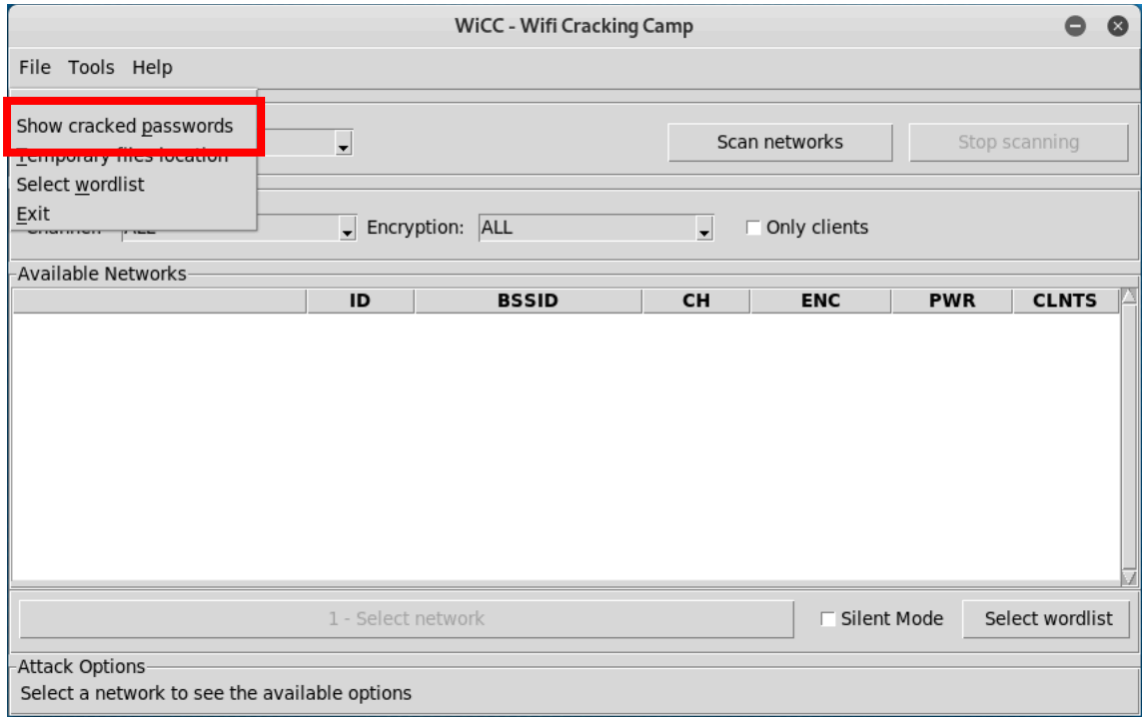
As mentioned before, the applications uses *rockyou.txt* as default wordlist. With this option one can select a custom wordlist to perform the WPA/WPA2 attack. The file must be selected before clicking on *Attack*.

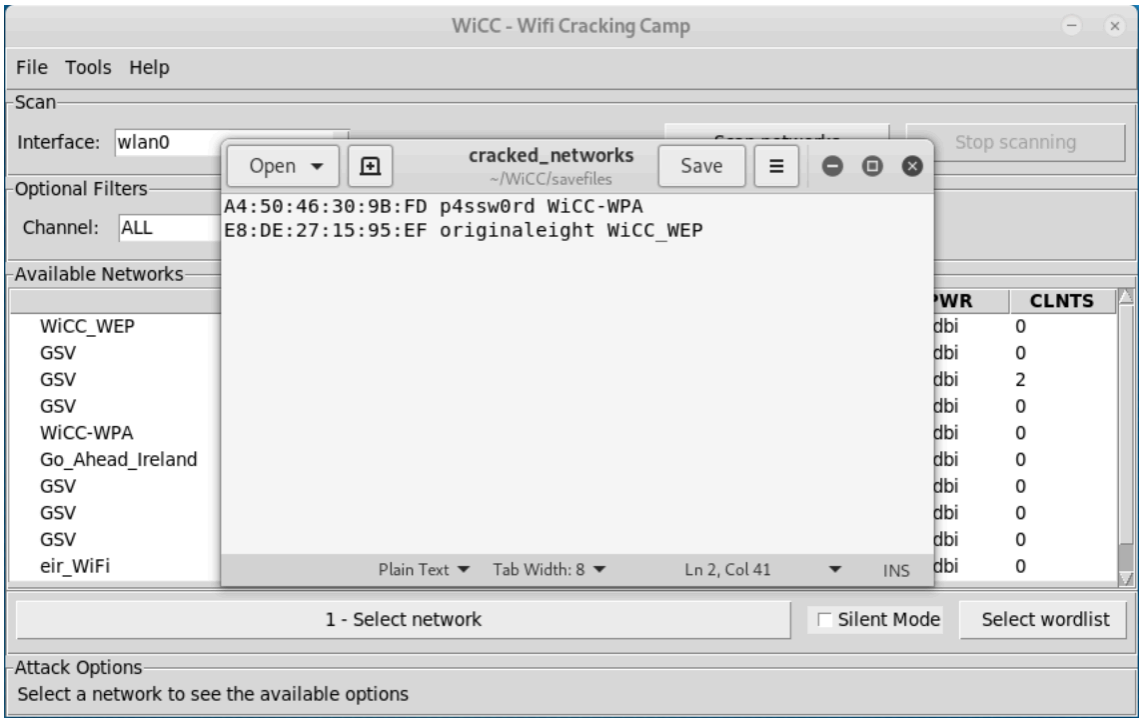
Clicking on *Select wordlist* button will appear a file explorer window to select the wordlist. This wordlist will remain set even dough changing the network.



## 5. Show cracked passwords

To see the cracked passwords just click on the *Show cracked passwords* button on the *File* menu. This will open the text file where the passwords are stored (bssid, password, essid).

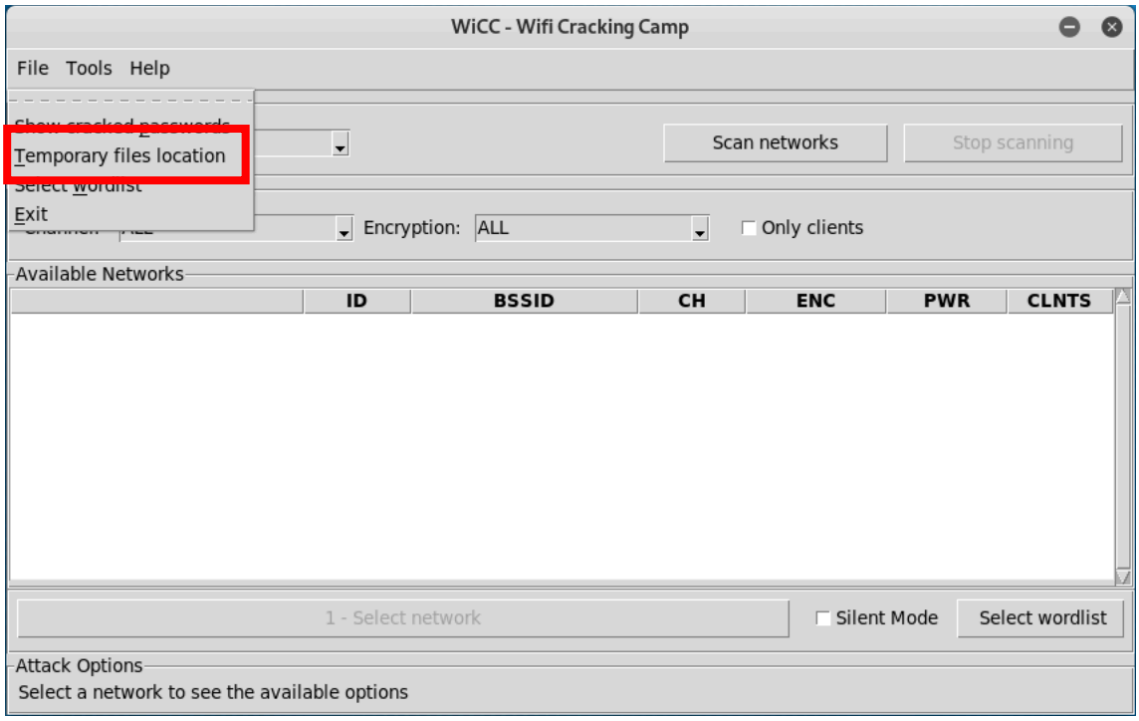


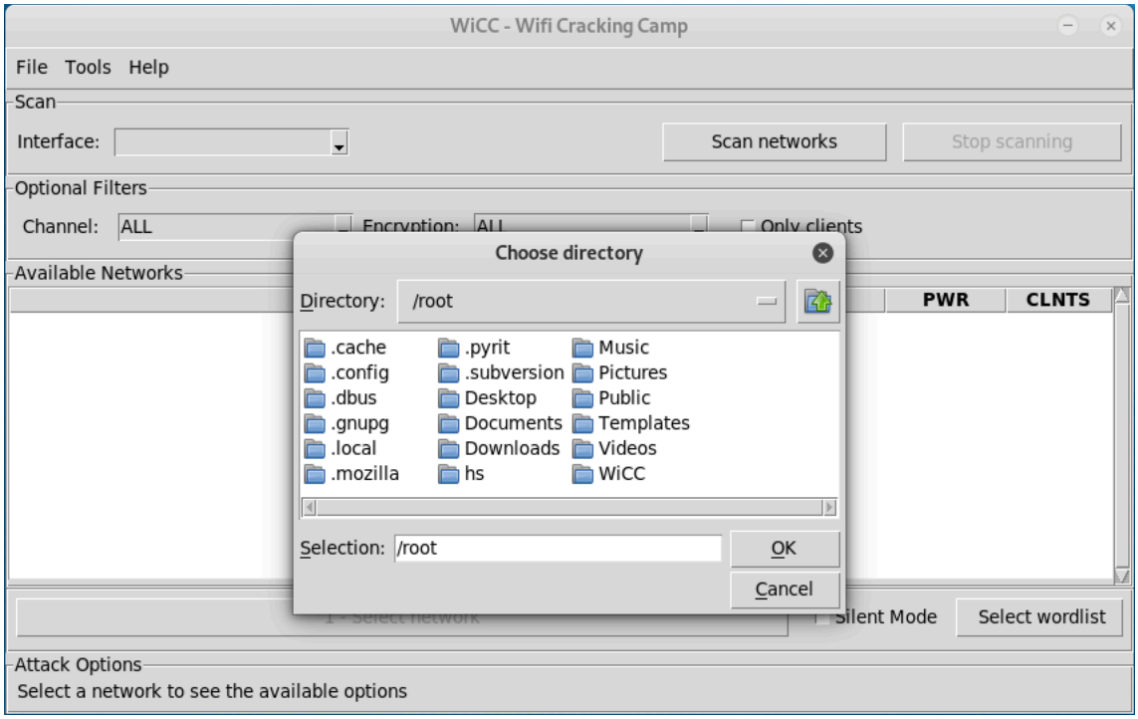



## 6. Temporary files location

All the files generated by the application (except *crackednetworks.txt*) are send to system temp directory and will be deleted on the system startup. For those who want to keep the capture files, there is an option to change the directory where this file are going to be saved.

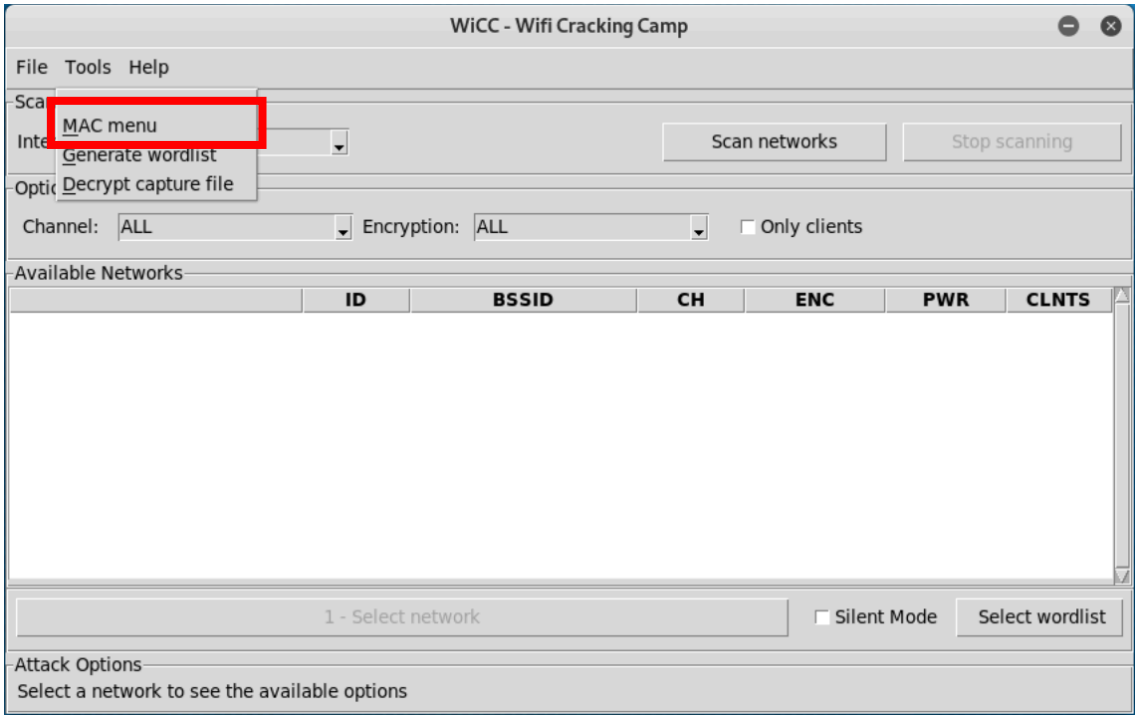
To do this click on the *File* tab on the top menu bar and then click on the *Temporary files location* button. This will open an explorer window to choose a directory. All files will now be saved on this directory until the application's closing.



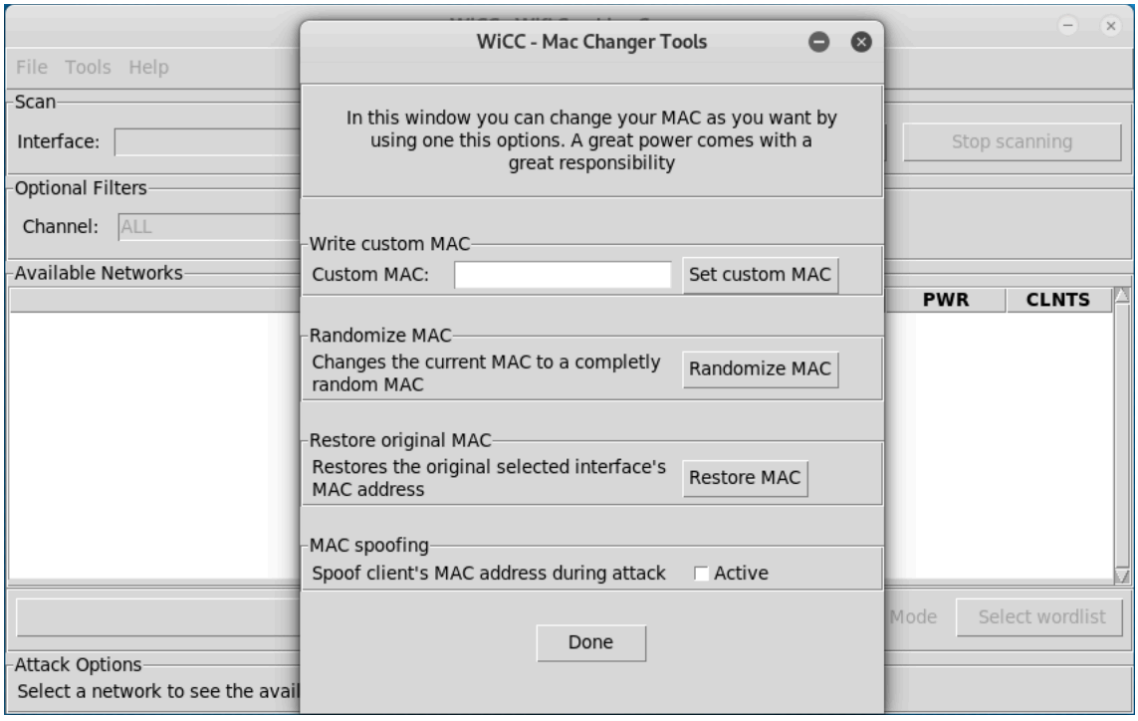



## 7. MAC menu

With this tool one can change the interface's MAC address by setting a custom address, randomizing it, or resetting to the original one. Also includes an option to activate MAC spoofing.

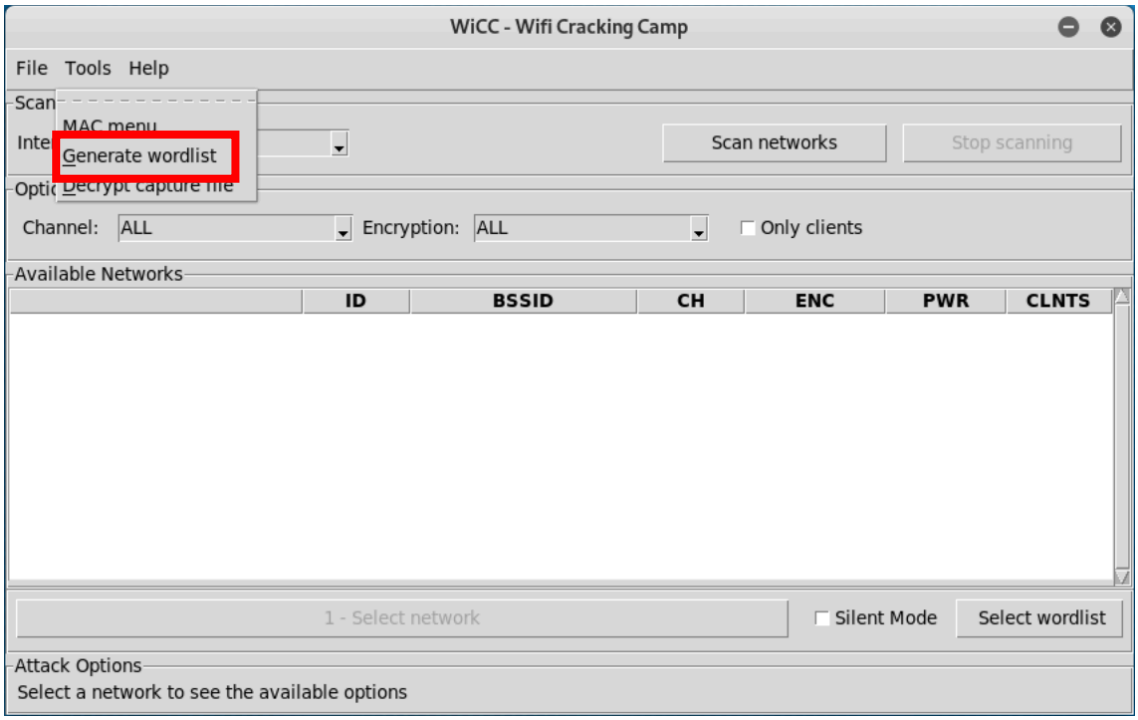


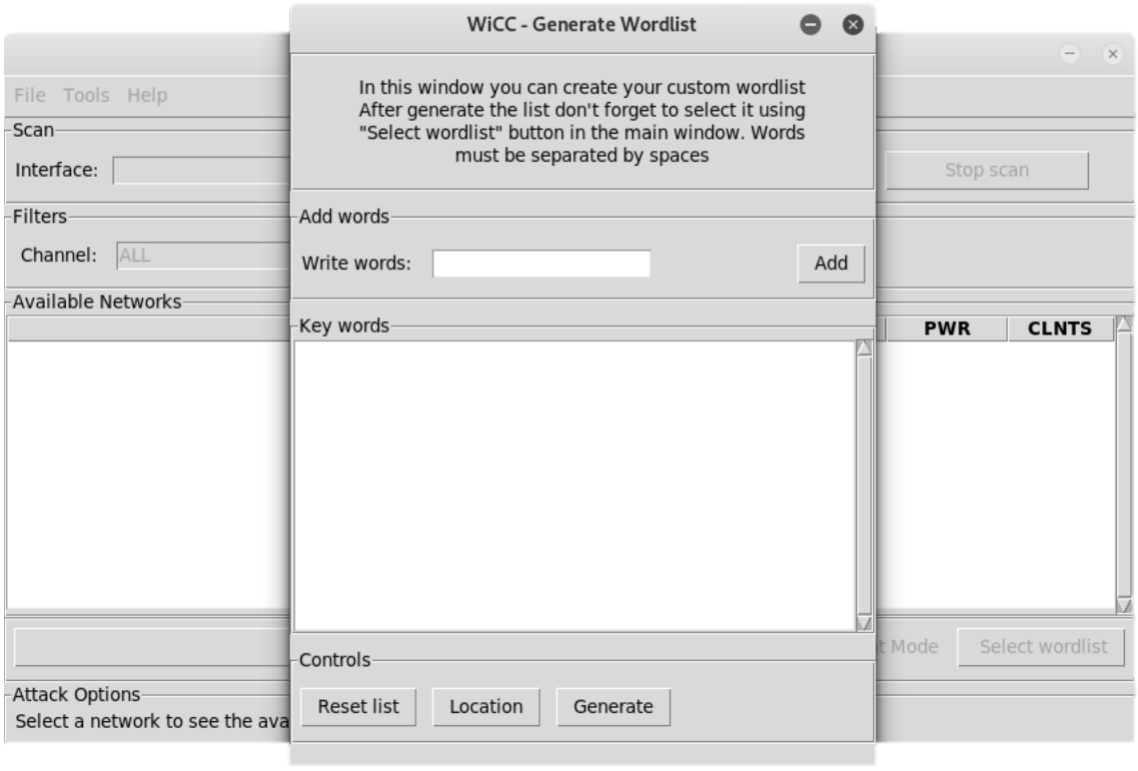

This tool is on the *Tools* tab from the top bar menu. It will open a new window to perform all these actions.



## 8. Wordlist generator

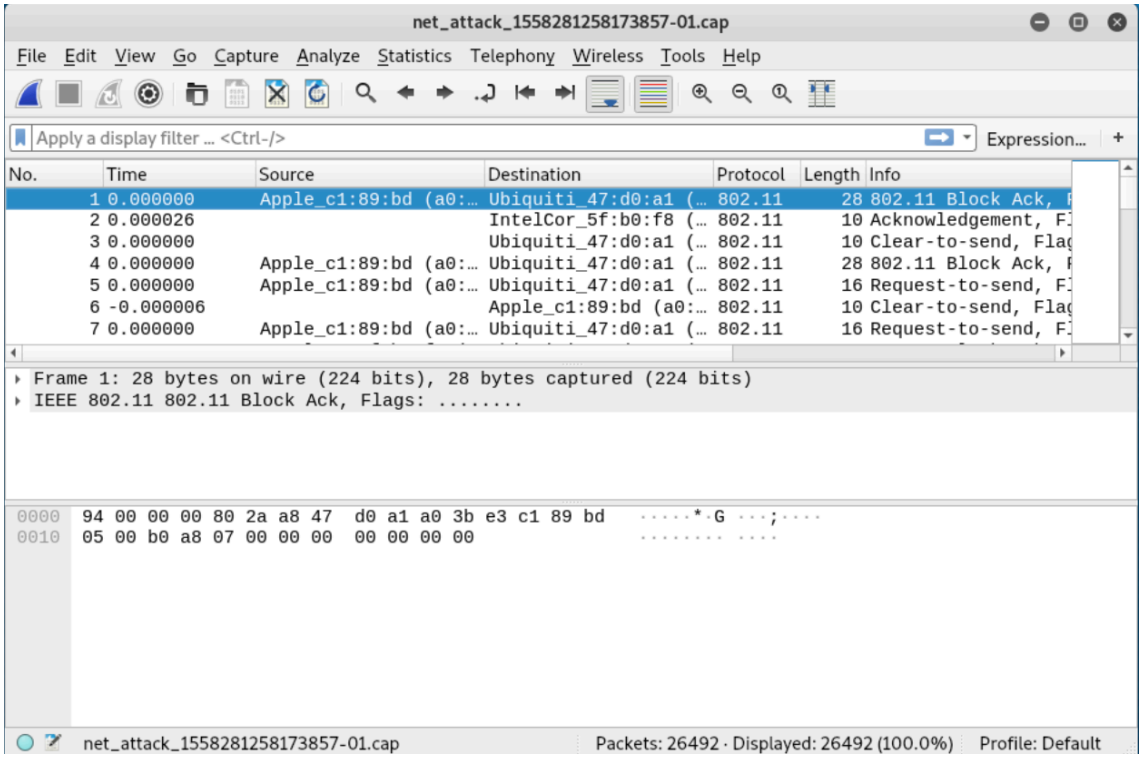
With this tool you can create your custom wordlist. Write the words in the *Add words* frame and click on add. After that click on *Location* to select where the file is going to be generated and then click on *Generate*.
The tool will perform all possible permutations with the added words. Depending on how many words are in the list the amount of time can be considerably big.
This tool is in the *Tools* tab from the top bar menu.



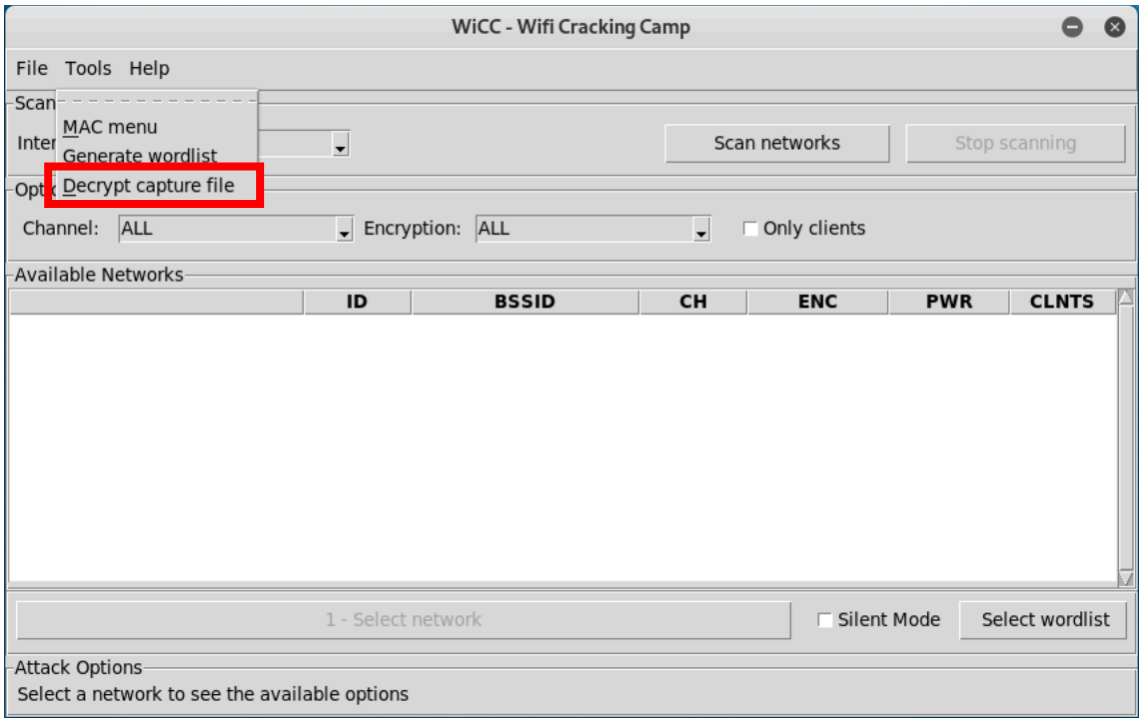



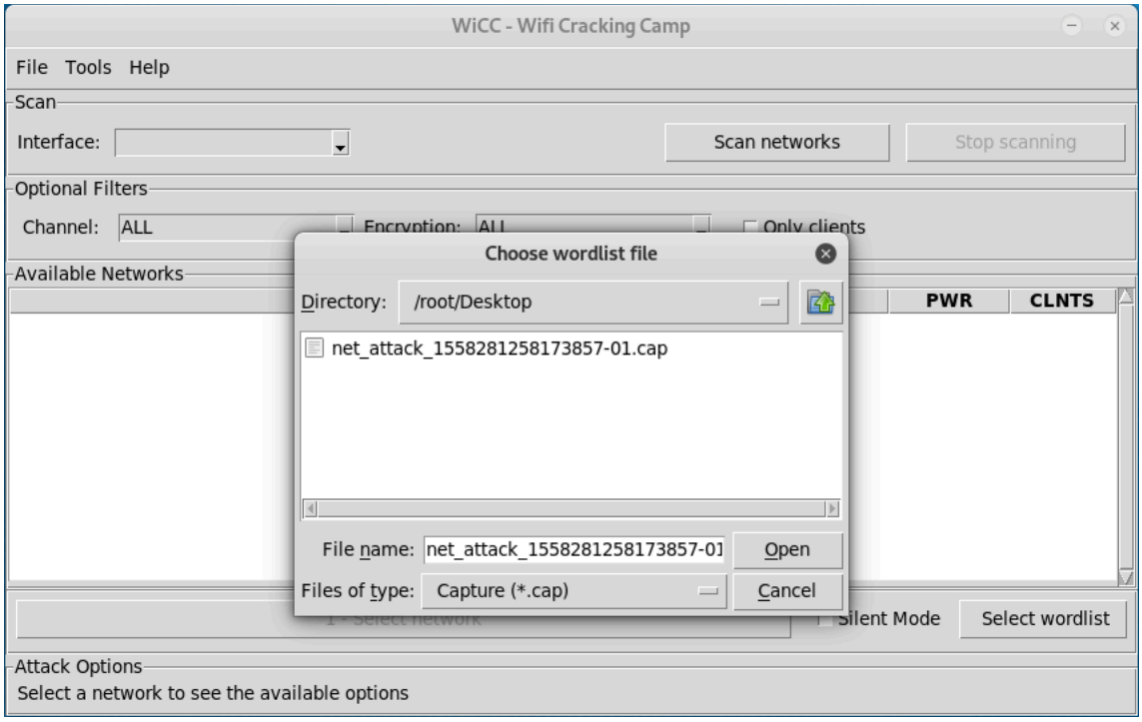
## 9. Decrypt capture file

Captured packets from a wireless connection are always encrypted (if it's not an open network) and is needed to decrypt that capture to see the packets.

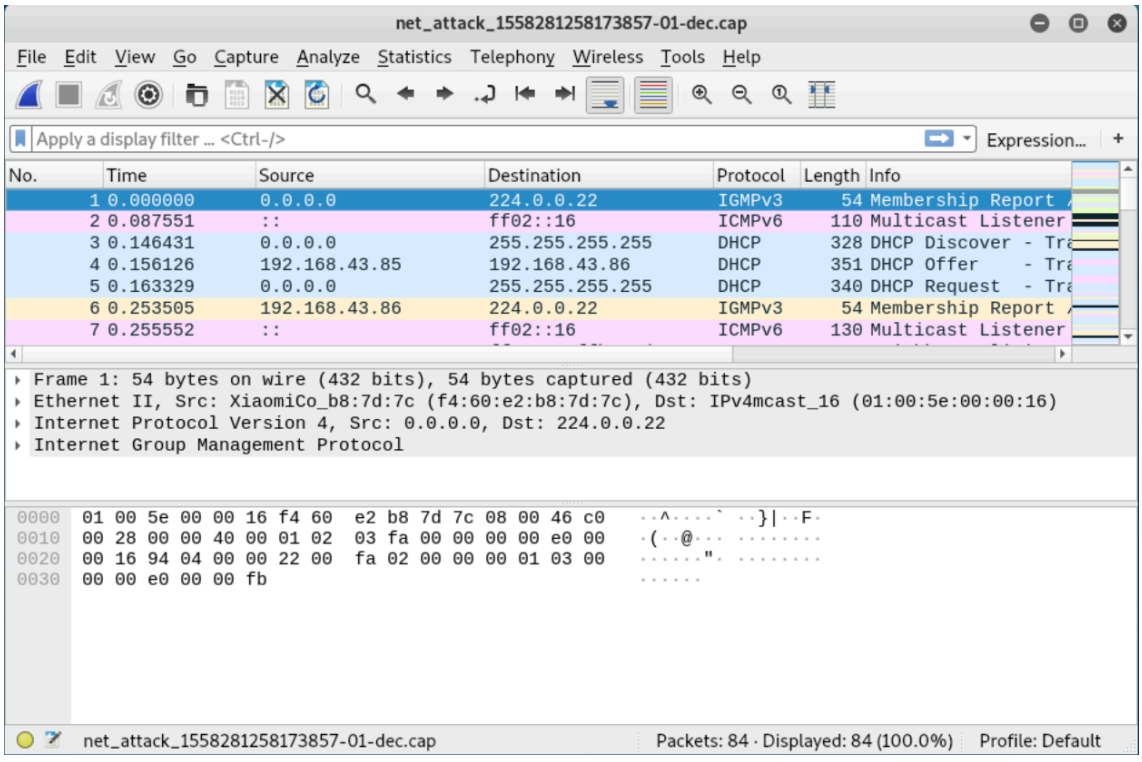



To decrypt a capture file of one of the networks we have cracked, just select the *Decrypt capture file* on the *Tools* tab, select the file, click *Open* and wait (the tool will do the rest for you).



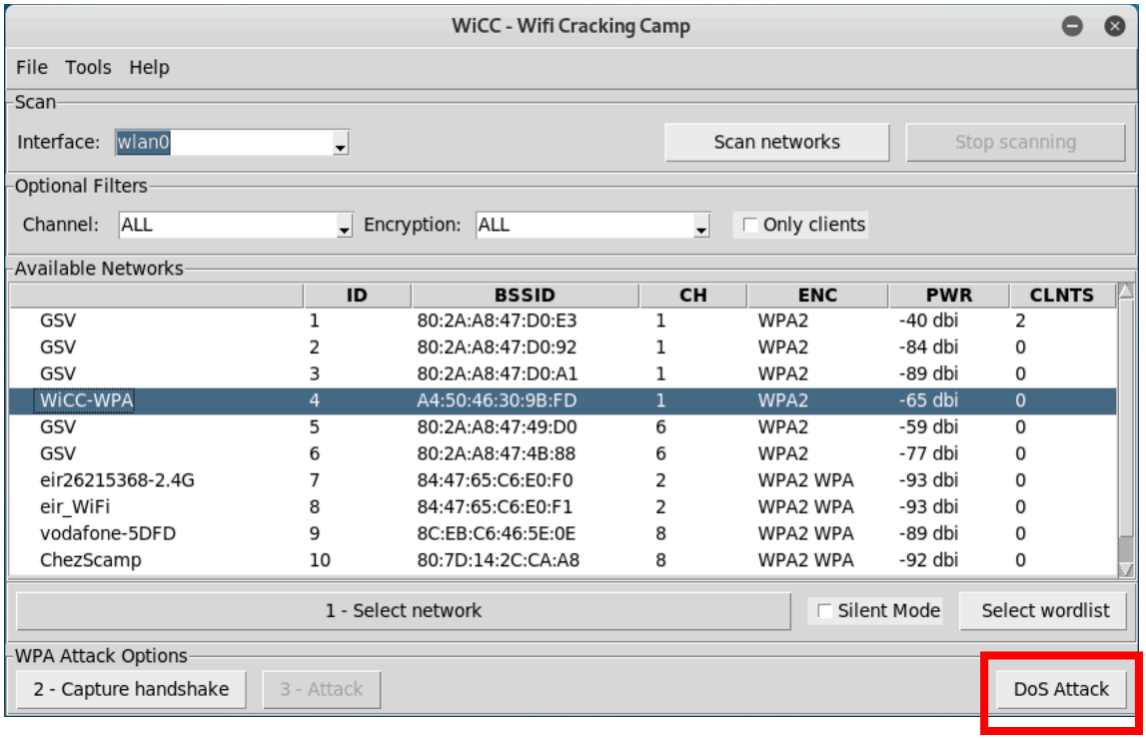


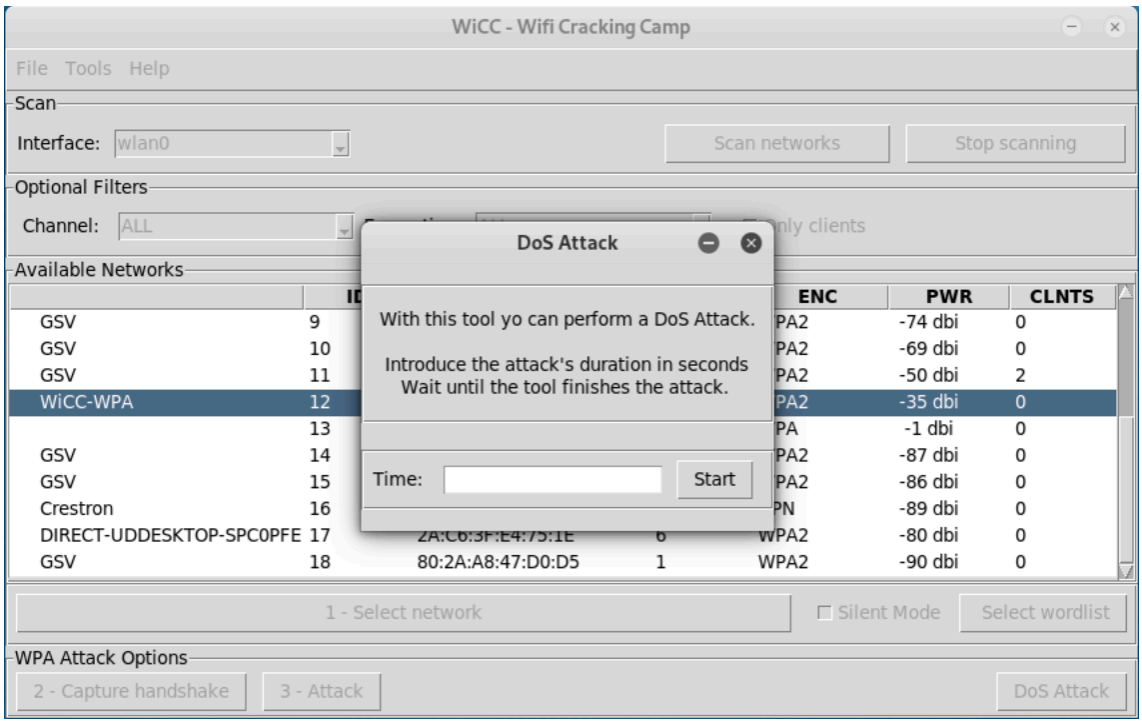

When the application finishes, will show a pop-up saying “File decrypted”. It will crete a new file in the same directory as the selected one with the same name plus “-dec” appended to the end. Just open the file and the packets from that network will be decrypted. Sometimes the capture files are corrupt, when this happens the decrypted file will be empty.



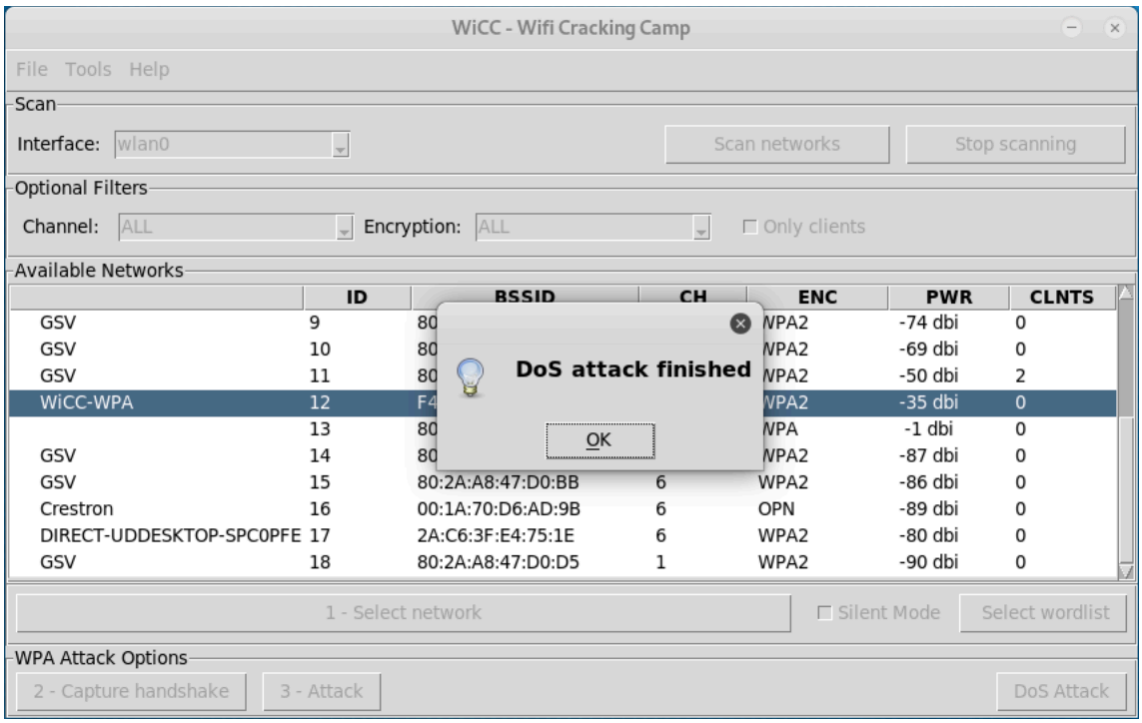
## 10. DoS attack

To perform a DoS attack on a network make a scan first and the select any network. On the right side of the *Attack Options* panel will appear the *DoS Attack* button. This button opens the DoS attack window.



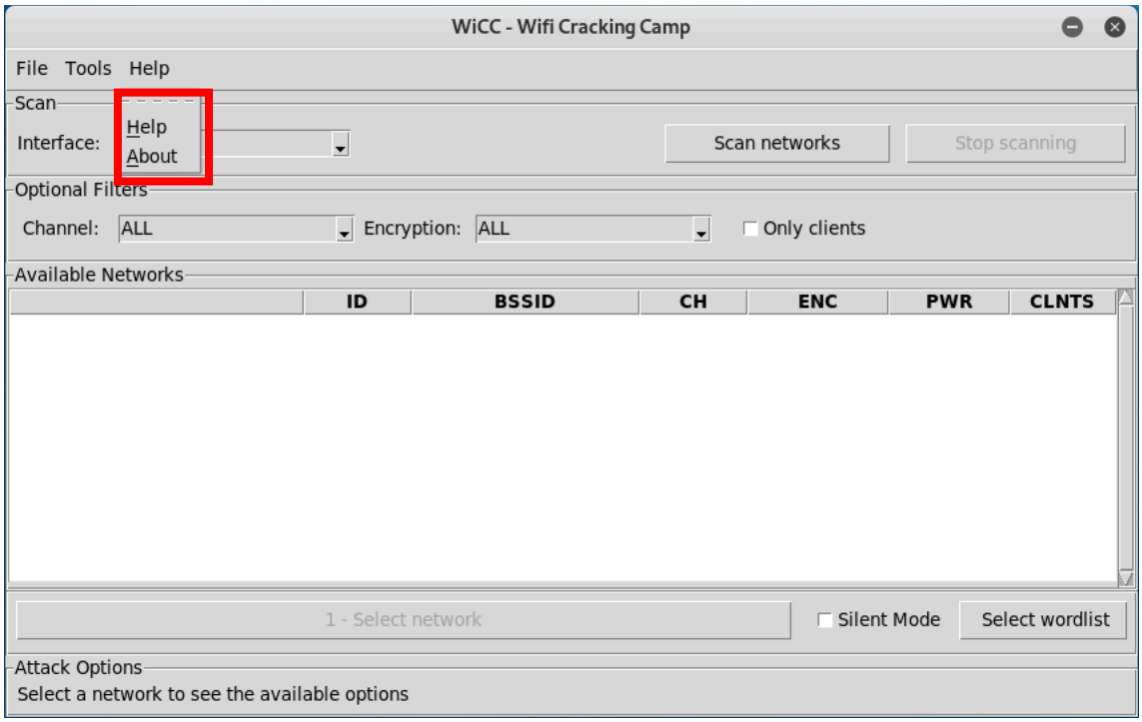



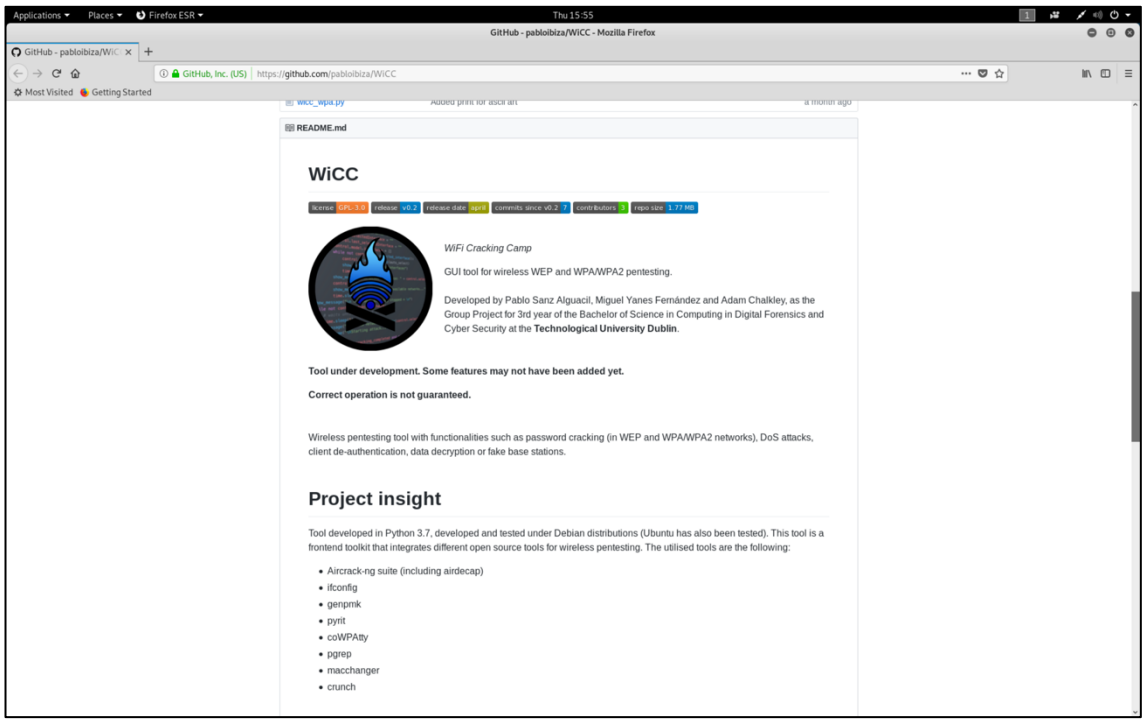
On this window introduce the duration of the attack in seconds and press start. When the attack finishes will appear a pop-up window saying “DoS attack finished”.




## 11. Help and About

In the *Help* tab from the top bar menu are the *Help* and *About* buttons. The help button opens the project Github’s page where the application’s functioning is explained.






The About button shows a new window with a brief description of the application and the coders names.


On this window introduce the duration of the attack in seconds and press start. When the attack finishes will appear a pop-up window saying “DoS attack finished”.