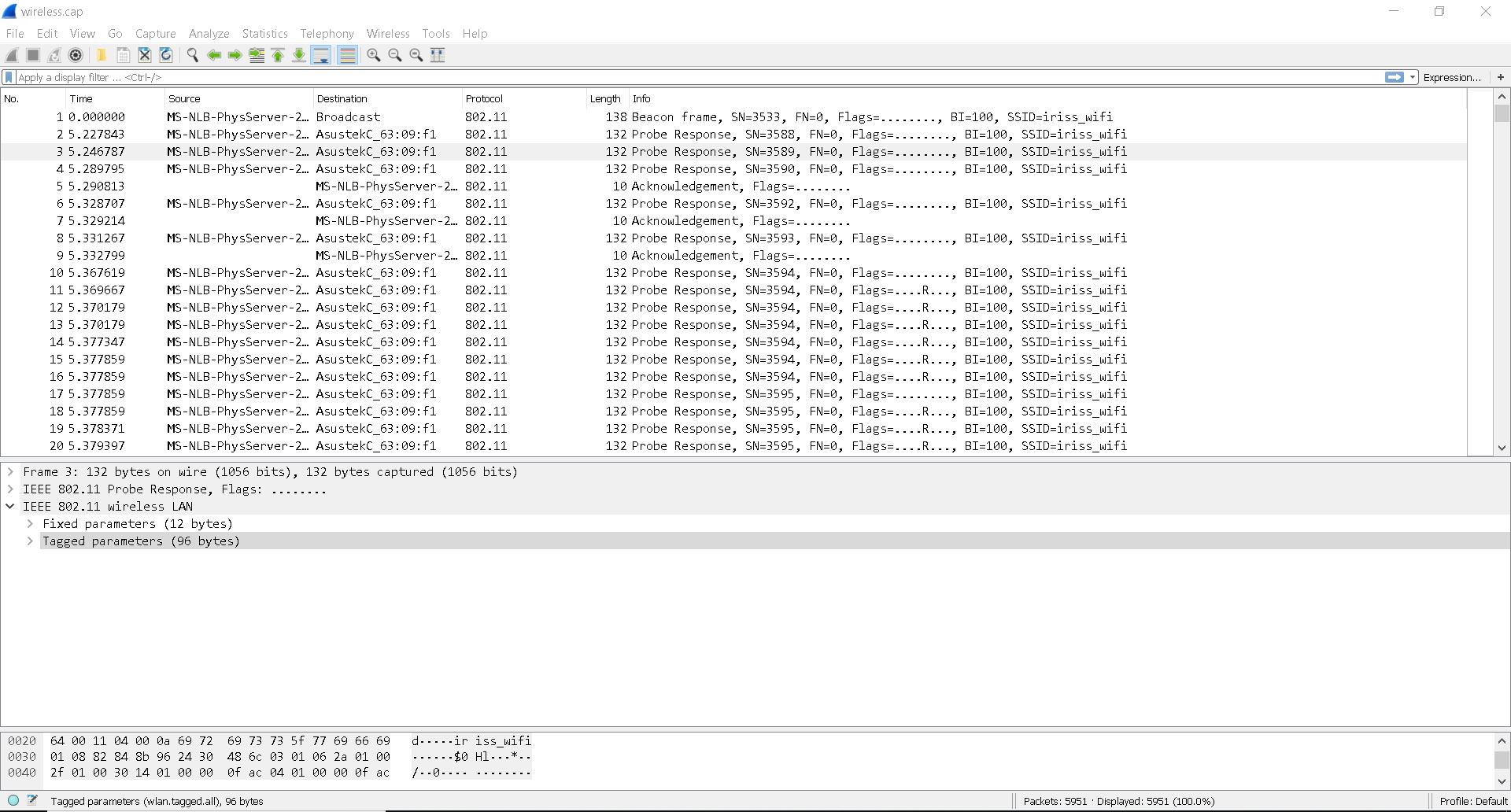
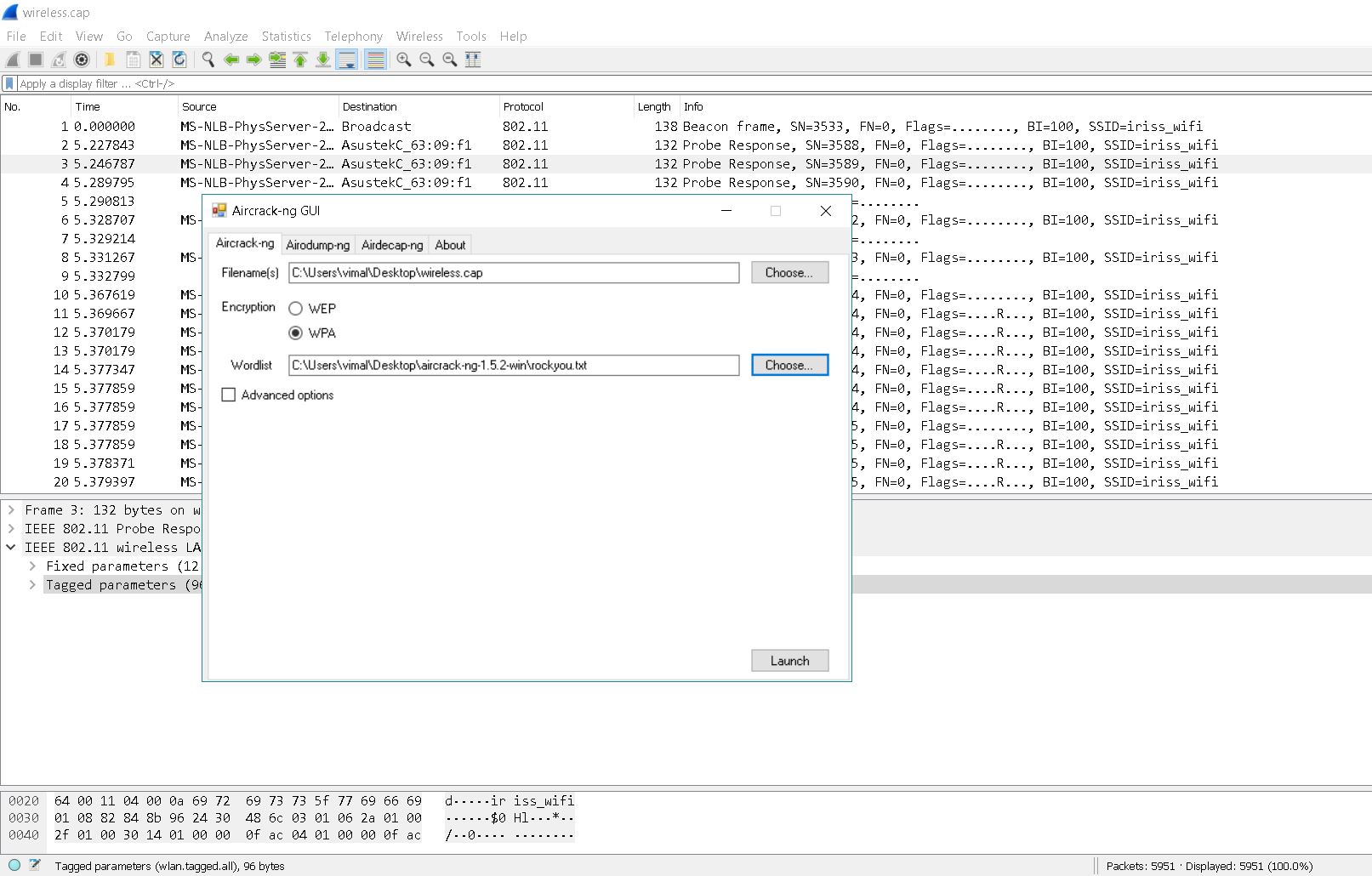
**Lab 5 Wireless Encryption**

“You have been presented with a packet capture of some encrypted wireless network traffic. Your task is to decode the packet capture and discover the secret message hidden within the pcap. Evidence File - Wireless.cap

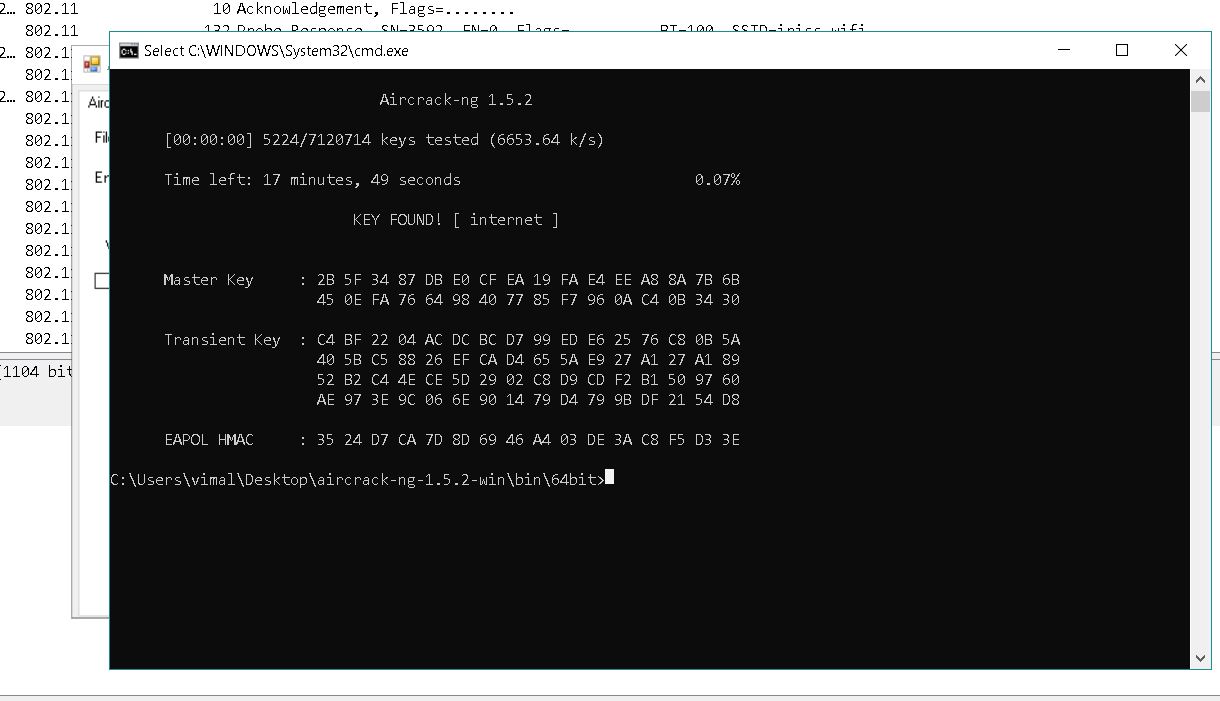
* Open wireless.cap packet capture file using Wireshark.
* The packet capture shows the traffic of wireless network having protocol 802.11 and have SSID=iriss\_wifi



* Run aircrack-ng in windows. Depending upon the system 32bit or 64bit launch or start aircrack-ng.exe

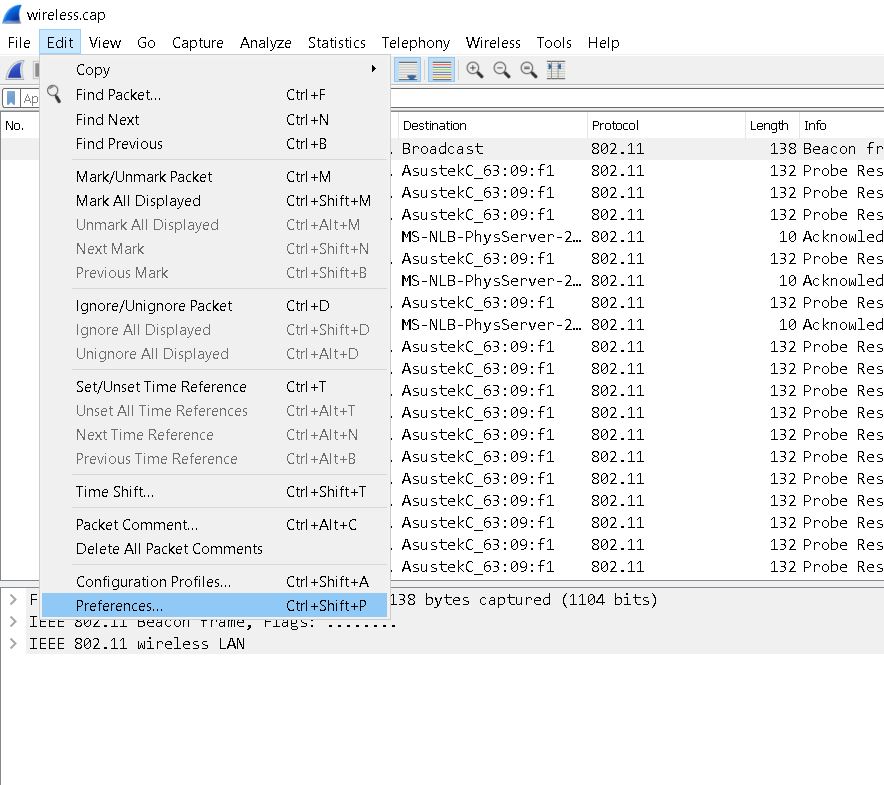


* Choose WPA(wireless protected access) from encryption and provide the path wireless network capture wireless.cap file.
* For cracking encryption download ‘rockyou’ wordlist.txt file from <https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt> Aircrack-ng will use this wordlist for decrypting the hidden message in file. Secret Password will be cracked by aircrack-ng by applying several combinations from the wordlist. There are various wordlist we an use.



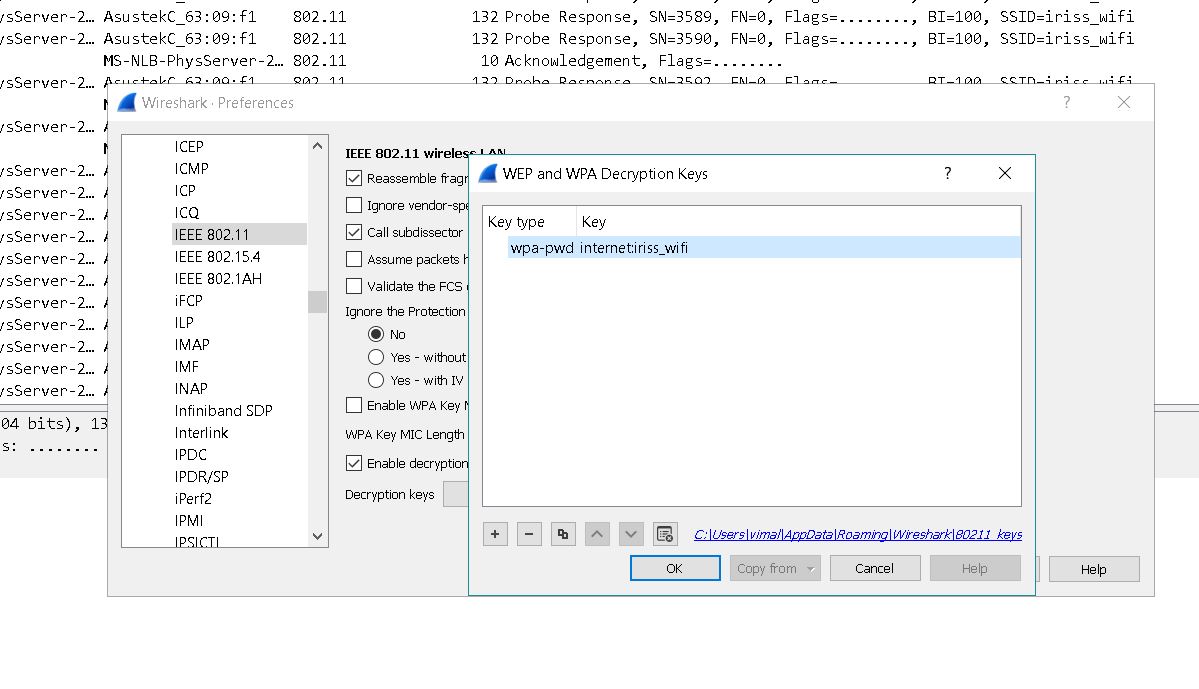
After running aircrack-ng wordlist with capture file. Go to wireshark for filtering and viewing decrypted message.

Edit🡪Preferences



From Protocols🡪select IEEE 802.11🡪click edit decryption keys and

add key🡪wpa-pwd🡪internet:iriss\_wifi



Ensure Enable decryption checkbox is checked and click OK.

* To see the decrypted message from wireless network traffic filter irc and follow tcp stream by right clicking on irc packet. Irc or Internet Relay Chat is an application layer protocol that facilitates in text communication. It is based on a client/server networking model.

From the tcp stream of irc packet you will be able to see in text information. Scroll the page to find the decrypted secret message.

