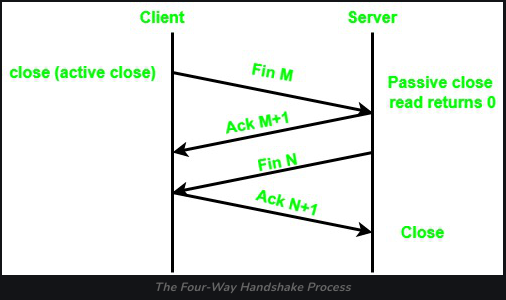
Key terms   
-SSID: tên mạng mà bạn thấy khi thử và kết nối   
-ESSID: một SSID \*may\* nhiều điểm truy cấp (AP) như công ty hay mạng lớn. Đối với Aircrack thì họ thường chỉ đối tượng đang tấn công.

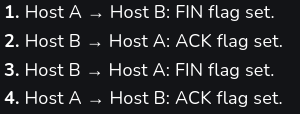
-BSSID: điểm truy cập địa chỉ MAC

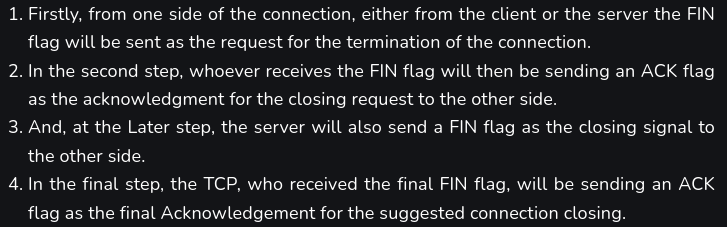
-WPA2-PSK: Mạng Wifi mà bạn kết nối bằng cách cung cấp mật khẩu giống nhau cho mọi người

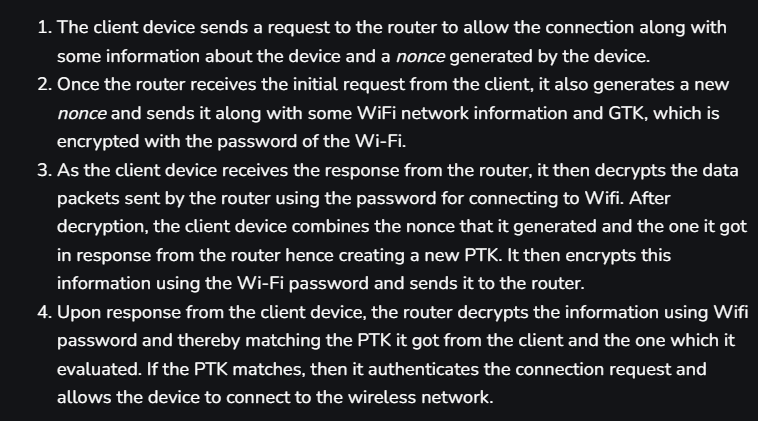
-WPA2-EAP: Mạng Wifi mà bạn xác thực bằng cách cung cấp username và password, khi nó đc gửi cho RADIUS server

-RADIUS: 1 server xác thực clients, không chỉ cho wifi  
  
-Cốt lõi của WPA(2) được xác thực bằng 4 way handshake



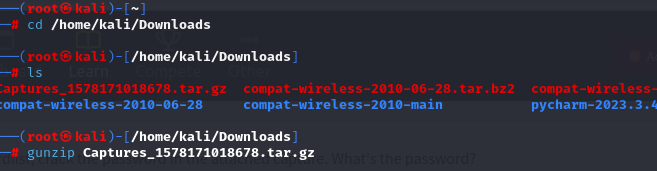


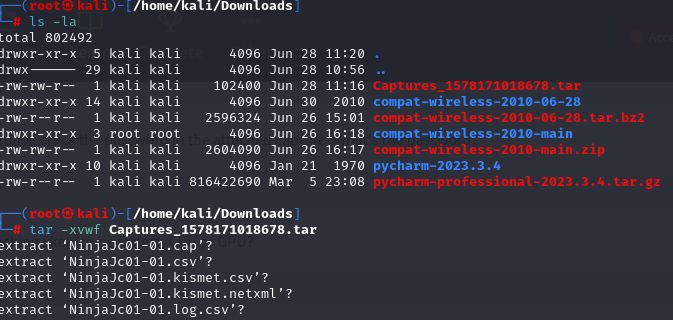


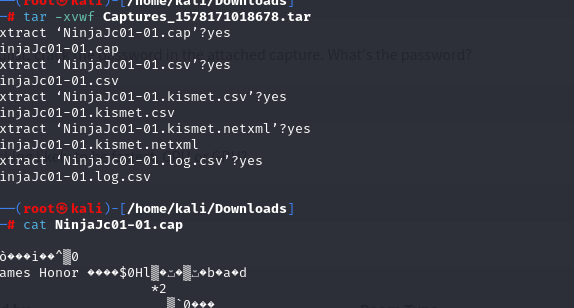


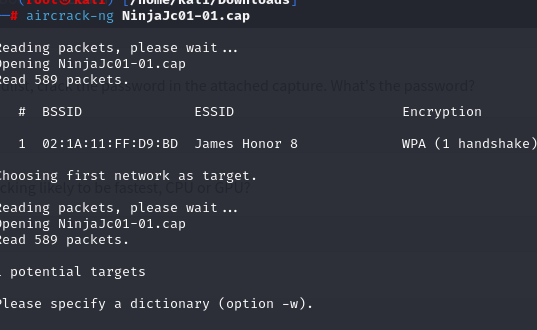
-A nonce is a random number that is only used once by an authentication protocol in a particular communication.



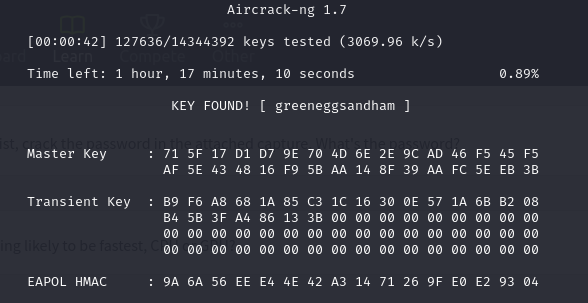


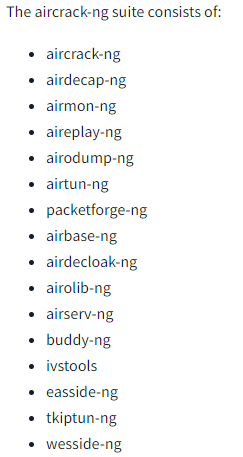


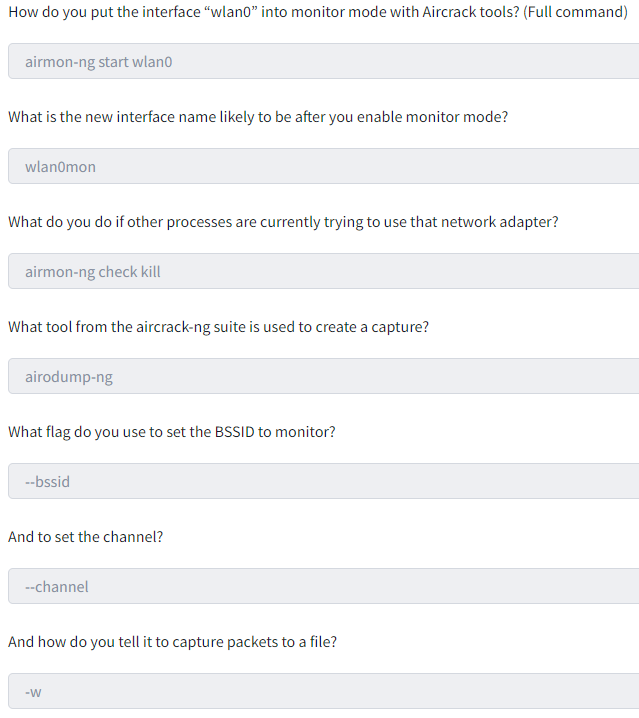




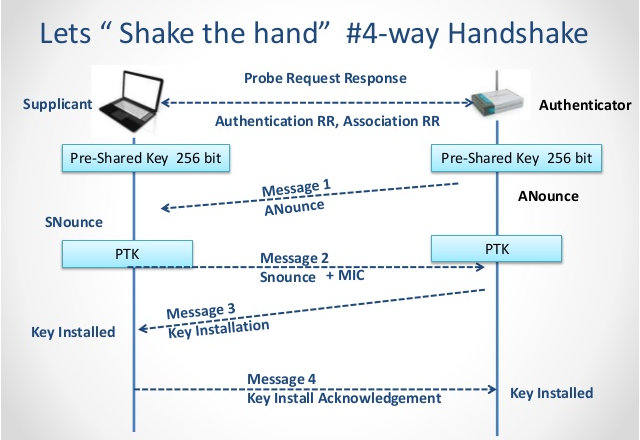


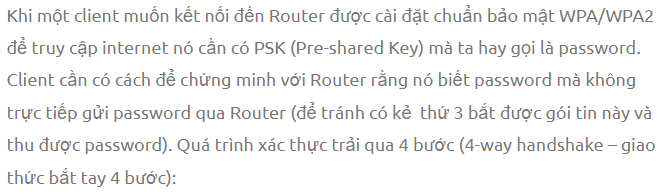
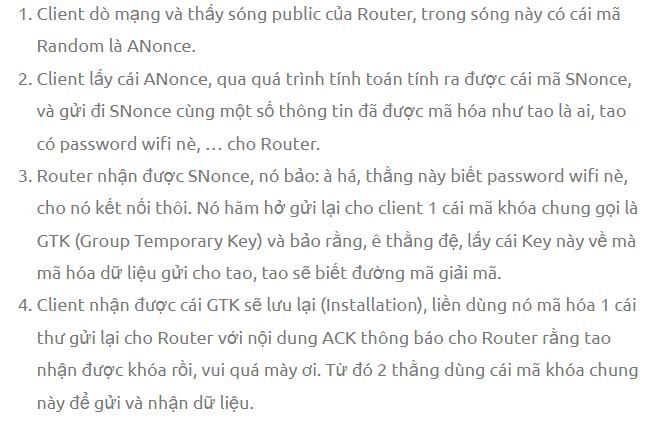
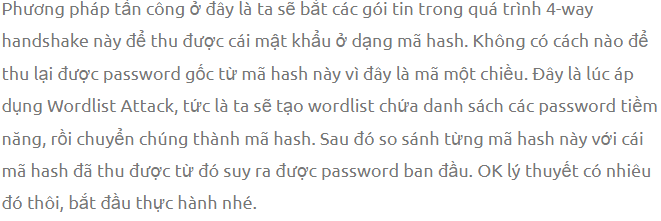






Adapter : Atheros – Ar9271

* Tool hack wifi: aircrack , airgeddon, wifiphisher
* Tool crack password và tạo wordlists: hashcat, cupp, bopscrk, cewl, crunch
* <https://www.hackingarticles.in/wordlists-for-pentester/>
* B1: Dùng aircrack or airgeddon để bắt handshake của bssid với bộ phát wifi
* B2: Nếu password không nằm trong các wordlists mặc định thì dùng social engineering (càng nhiều thông tin về đối tượng càng tốt nhưng đừng nhiều quá vì quét lâu lắm hihi) và các tool để tạo 1 wordlists mới
* B3: Nếu wordlists mới ko có password thì dùng các rule của hashcat hoặc john để chạy như best64.rule khả năng cao sẽ crack được password

wifiphiser:

https://www.hackingarticles.in/wifi-exploitation-wifiphisher/  
https://www.tecninf.it/attack-on-a-public-wifi-network/