와이어리스 네뚜와크

와이파이 연결은 되는데 비밀번호를 까먹으셨다구요?
그런 당신을 위해 준비했읍니다!

2018/08/16

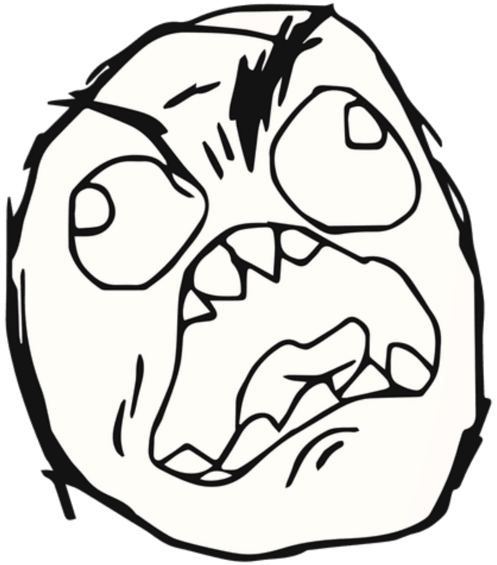
정재훈

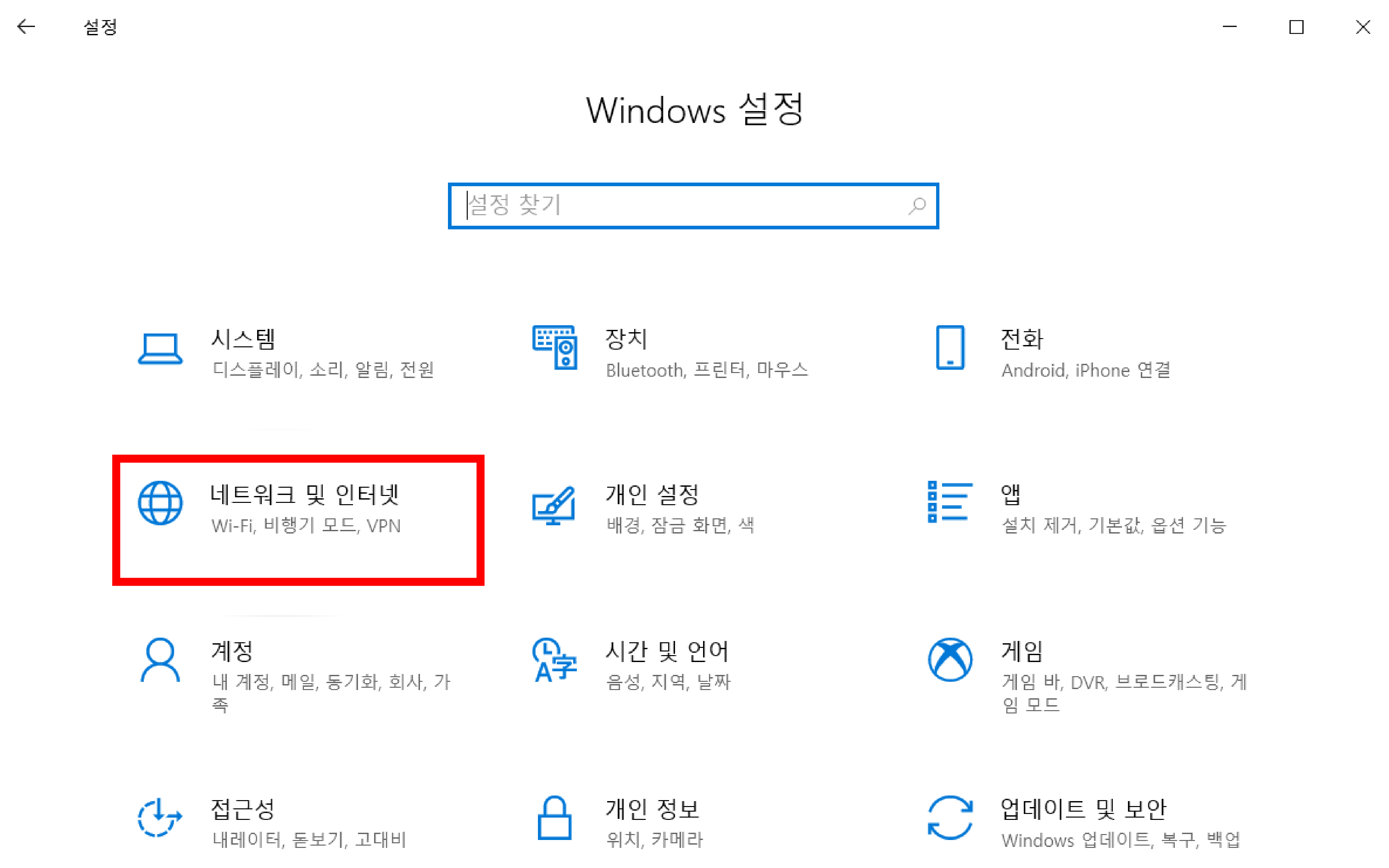
team S.C.P

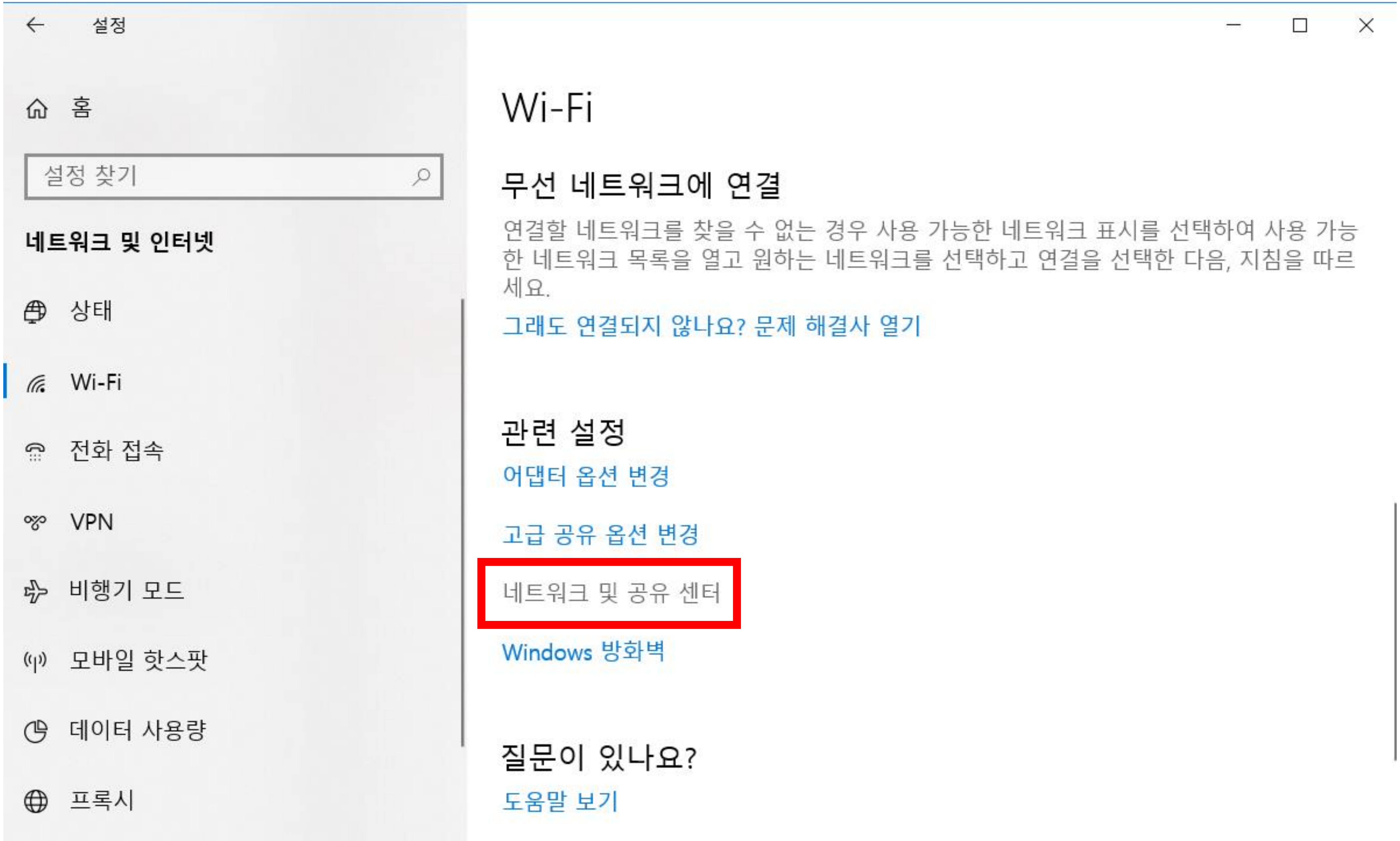
목차

- 비밀번호 찾기 (평범쓰 버전)
- 비밀번호 찾기 (고오급 버전)
- 802.11 네트워크 연결과정
- 패킷캡쳐 꿀팁
- 해본거

문제의 발단




설정
Windows 설정
설정 찾기
시스템
디스플레이, 소리, 알림, 전원
장치
Bluetooth, 프린터, 마우스
전화
Android, iPhone 연결
네트워크 및 인터넷
Wi-Fi, 비행기 모드, VPN
개인 설정
배경, 잠금 화면, 색
앱
설치 제거, 기본값, 옵션 기능
계정
내 계정, 메일, 동기화, 회사, 가족
시간 및 언어
음성, 지역, 날짜
게임
게임 바, DVR, 브로드캐스팅, 게임 모드
접근성
내레이터, 돋보기, 고대비
개인 정보
위치, 카메라
업데이트 및 보안
Windows 업데이트, 복구, 백업



Wi-Fi

무선 네트워크에 연결

연결할 네트워크를 찾을 수 없는 경우 사용 가능한 네트워크 표시를 선택하여 사용 가능한 네트워크 목록을 열고 원하는 네트워크를 선택하고 연결을 선택한 다음, 지침을 따르세요.

그래도 연결되지 않나요? 문제 해결사 열기

관련 설정

어댑터 옵션 변경

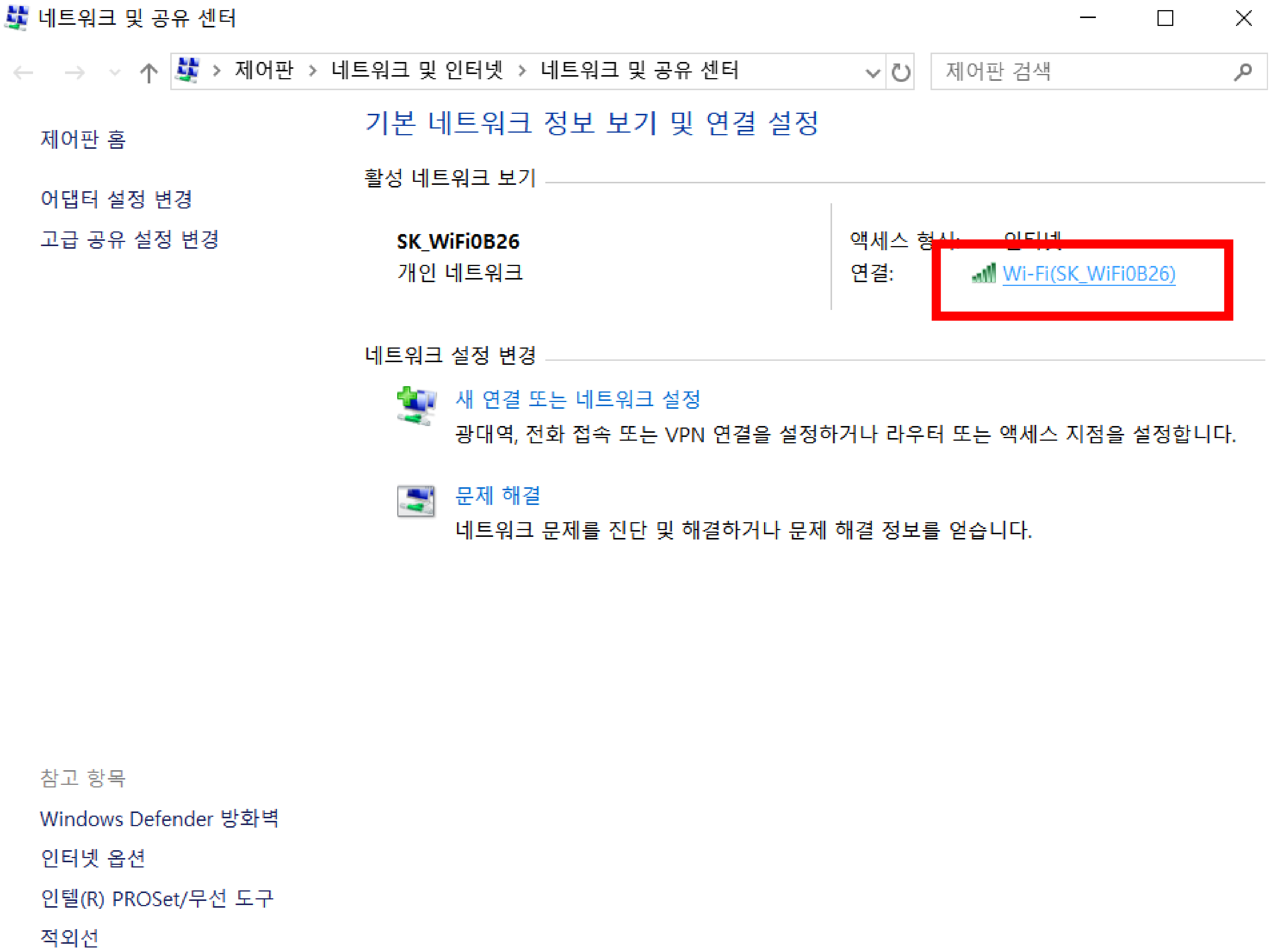
고급 공유 옵션 변경

네트워크 및 공유 센터

Windows 방화벽

질문이 있나요?

도움말 보기



기본 네트워크 정보 보기 및 연결 설정

활성 네트워크 보기

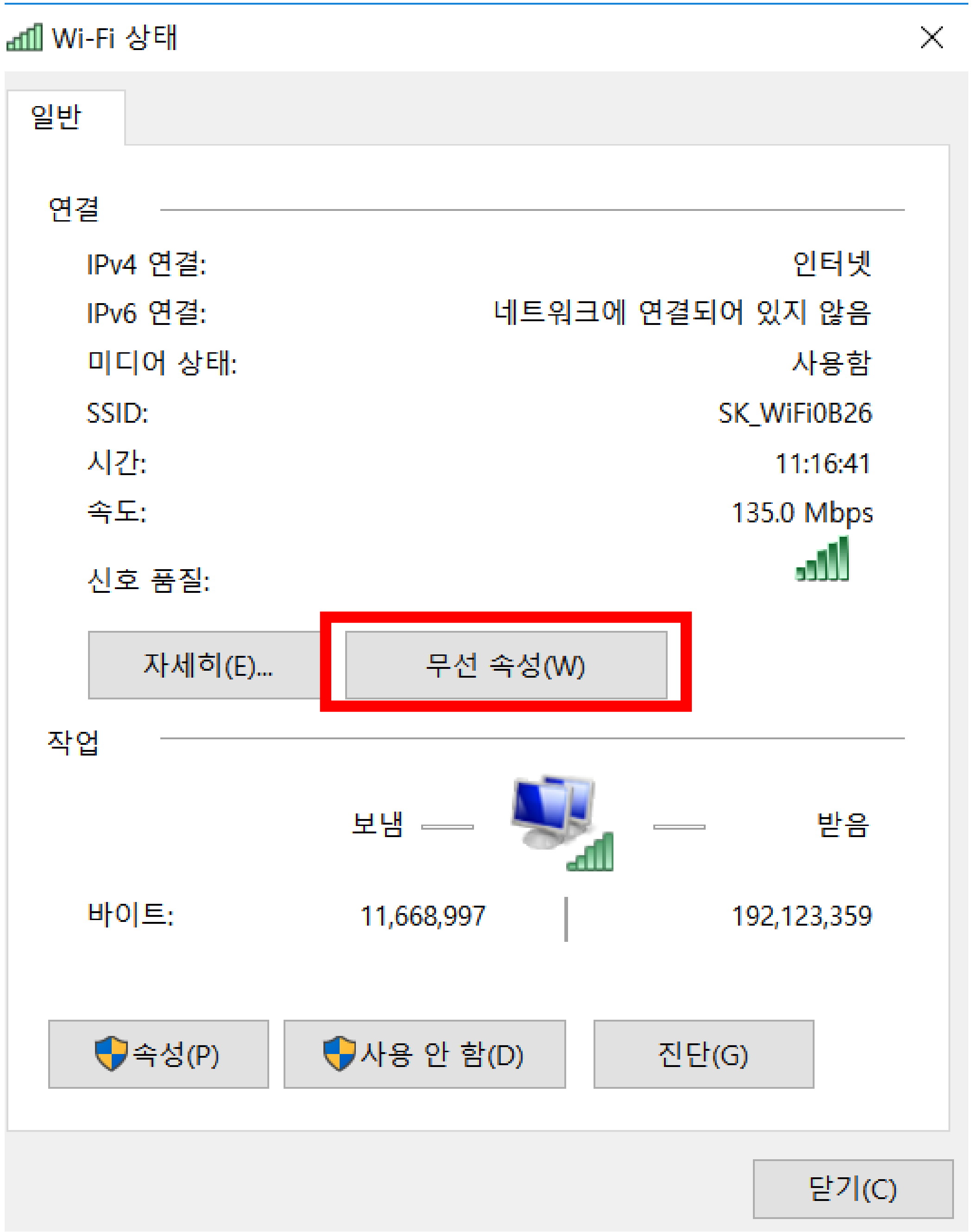
SK_WiFi0B26
개인 네트워크

액세스 형식: 인터넷
연결: Wi-Fi(SK_WiFi0B26)

네트워크 설정 변경

새 연결 또는 네트워크 설정
광대역, 전화 접속 또는 VPN 연결을 설정하거나 라우터 또는 액세스 지점을 설정합니다.

문제 해결
네트워크 문제를 진단 및 해결하거나 문제 해결 정보를 얻습니다.



Wi-Fi 상태

일반

연결

IPv4 연결: 인터넷

IPv6 연결: 네트워크에 연결되어 있지 않음

미디어 상태: 사용함

SSID: SK_WiFi0B26

시간: 11:16:41

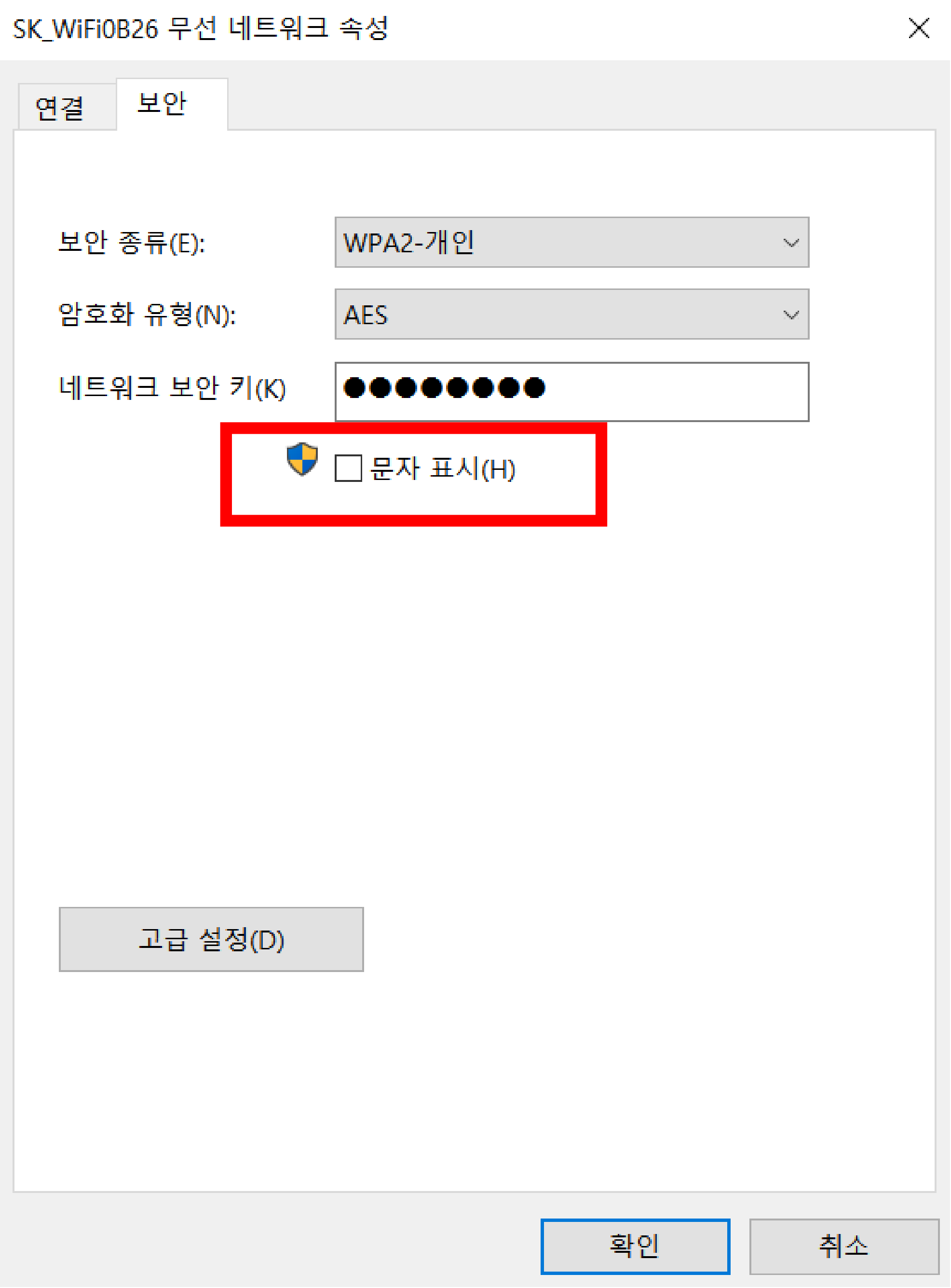
속도: 135.0 Mbps

신호 품질:

작업

보냄 — 받음

바이트: 11,668,997 | 192,123,359



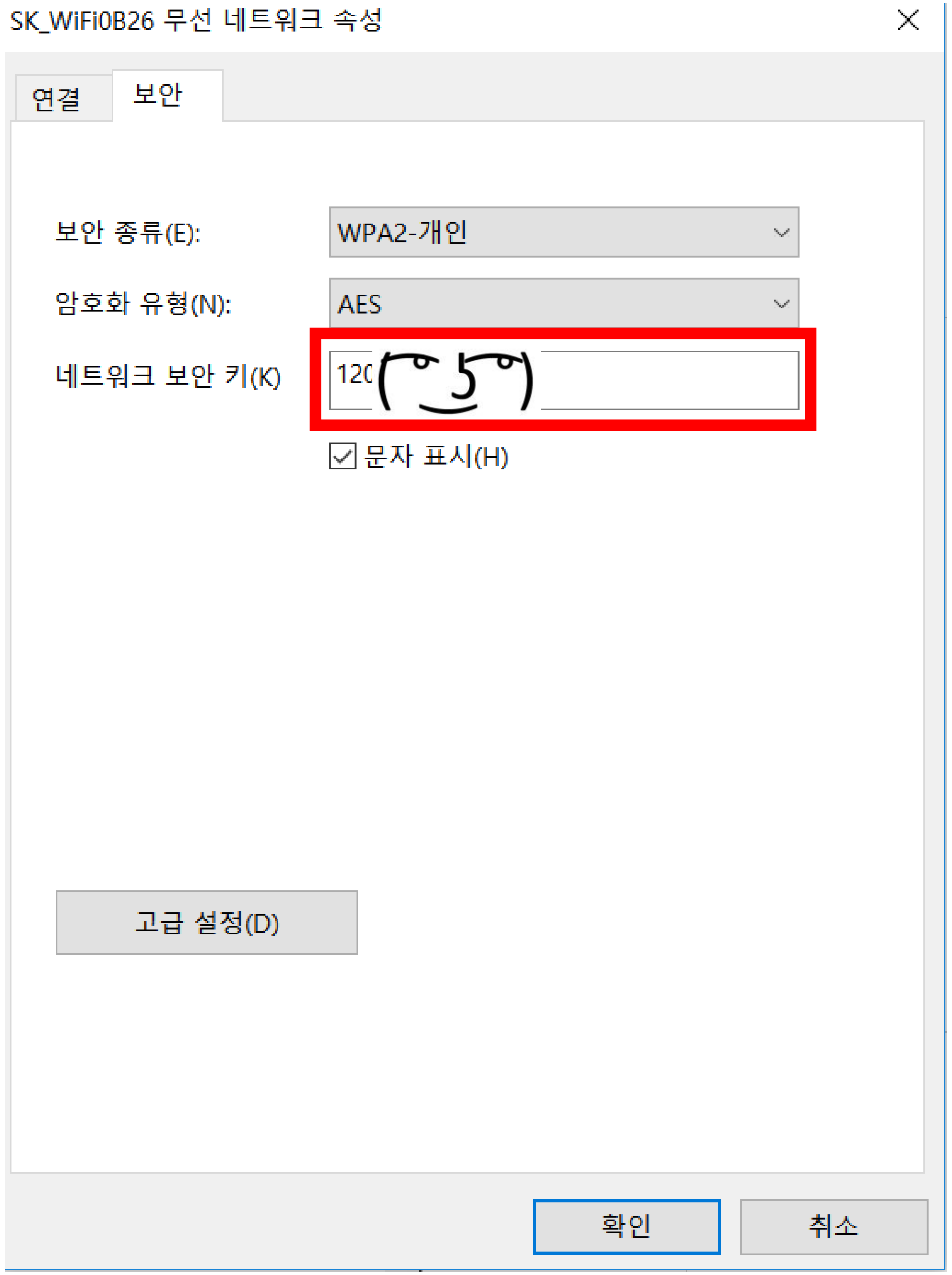
SK_WiFi0B26 무선 네트워크 속성

보안 종류(E): WPA2-개인

암호화 유형(N): AES

네트워크 보안 키(K) ●●●●●●●●

□ 문자 표시(H)



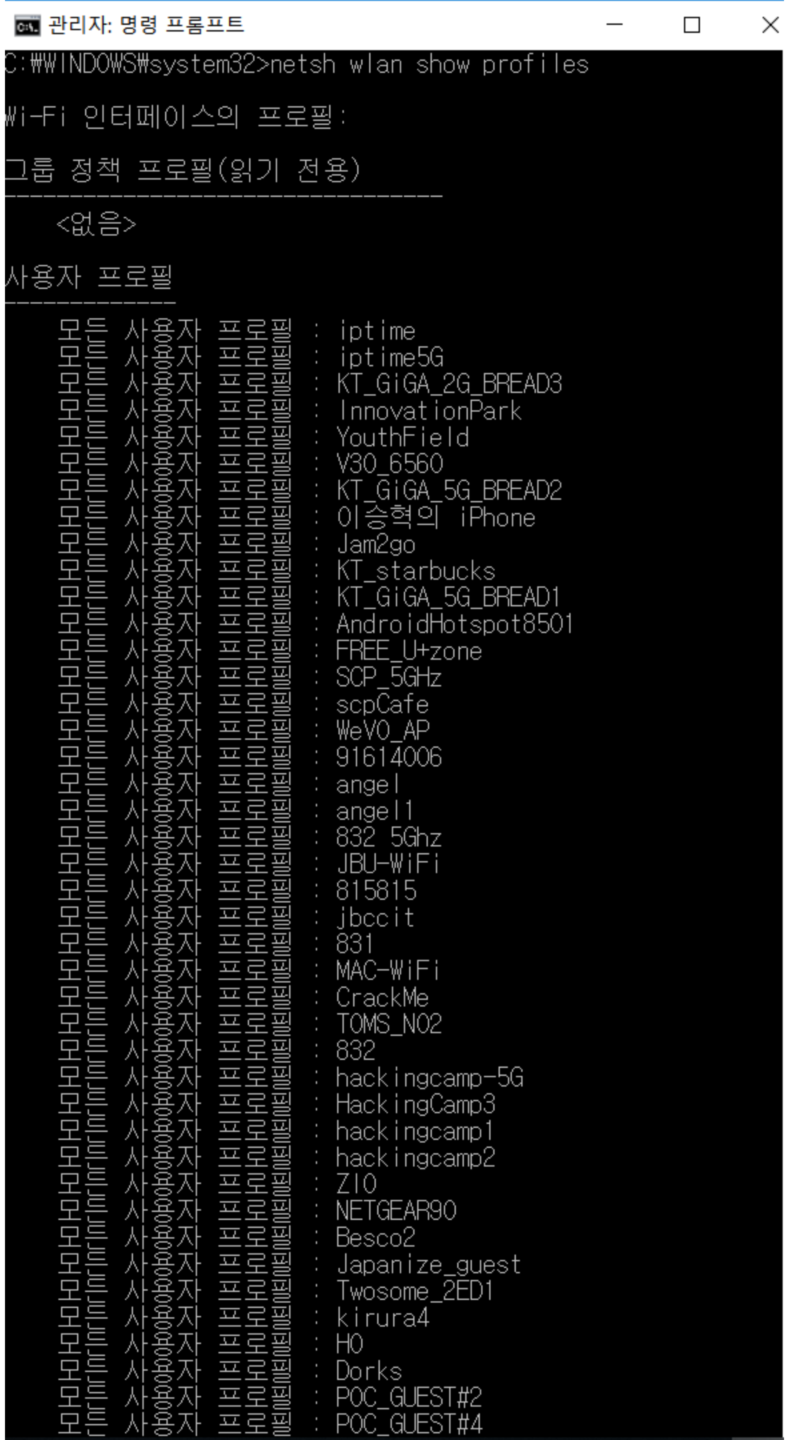
SK_WiFi0B26 무선 네트워크 속성

보안 종류(E): WPA2-개인

암호화 유형(N): AES

네트워크 보안 키(K) 120(͡° ͜ʖ ͡°)

☑ 문자 표시(H)



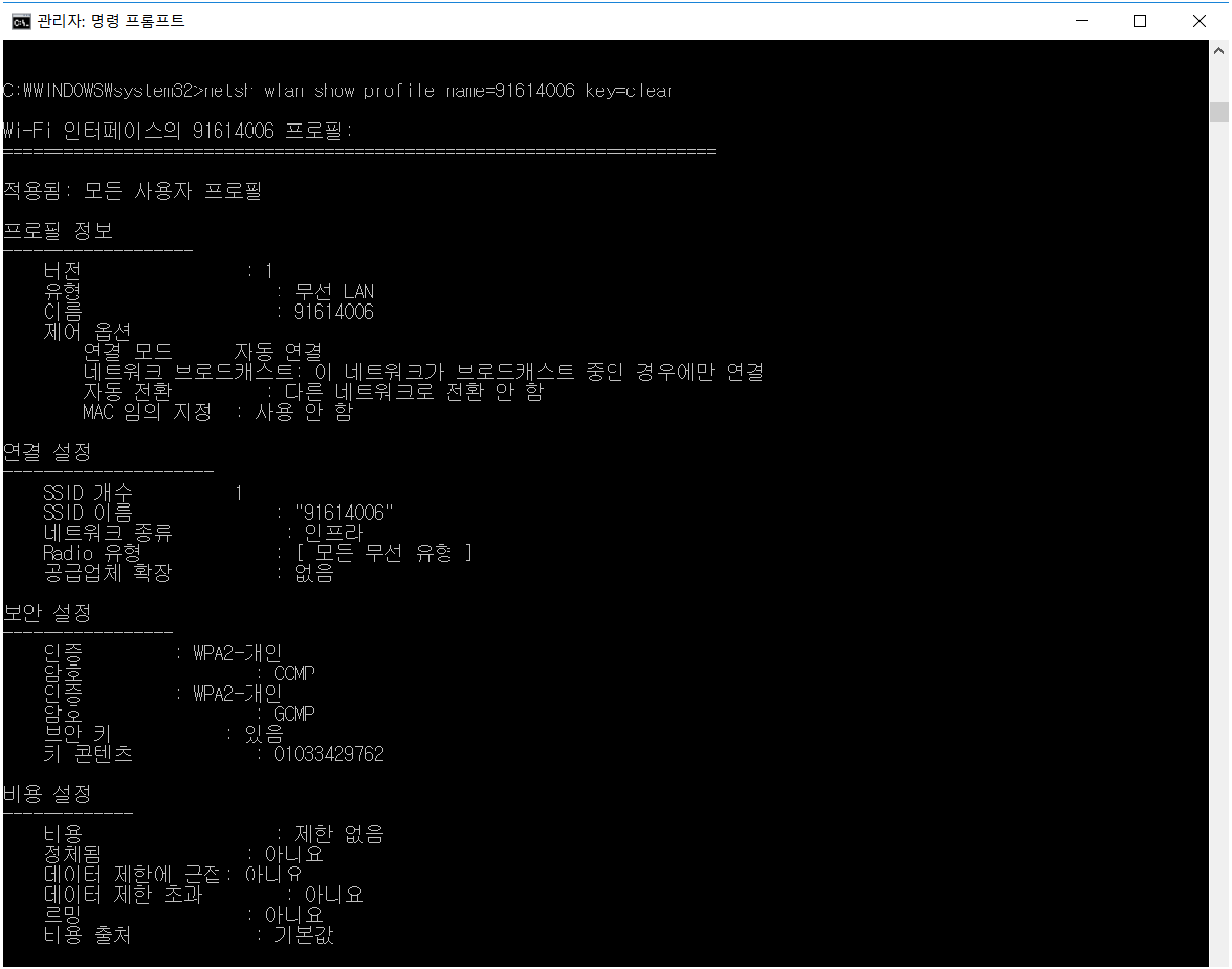
```
C:\WINDOWS\system32>netsh wlan show profiles

Wi-Fi 인터페이스의 프로필:

그룹 정책 프로필(읽기 전용)
---------------------------------
    <없음>

사용자 프로필
-------------
    모든 사용자 프로필 : iptime
    모든 사용자 프로필 : iptime5G
    모든 사용자 프로필 : KT_GiGA_2G_BREAD3
    모든 사용자 프로필 : InnovationPark
    모든 사용자 프로필 : YouthField
    모든 사용자 프로필 : V30_6560
    모든 사용자 프로필 : KT_GiGA_5G_BREAD2
    모든 사용자 프로필 : 이승혁의 iPhone
    모든 사용자 프로필 : Jam2go
    모든 사용자 프로필 : KT_starbucks
    모든 사용자 프로필 : KT_GiGA_5G_BREAD1
    모든 사용자 프로필 : AndroidHotspot8501
    모든 사용자 프로필 : FREE_U+zone
    모든 사용자 프로필 : SCP_5GHz
    모든 사용자 프로필 : scpCafe
    모든 사용자 프로필 : WeVO_AP
    모든 사용자 프로필 : 91614006
    모든 사용자 프로필 : angel
    모든 사용자 프로필 : angel1
    모든 사용자 프로필 : 832 5Ghz
    모든 사용자 프로필 : JBU-WiFi
    모든 사용자 프로필 : 815815
    모든 사용자 프로필 : jbccit
    모든 사용자 프로필 : 831
    모든 사용자 프로필 : MAC-WiFi
    모든 사용자 프로필 : CrackMe
    모든 사용자 프로필 : TOMS_NO2
    모든 사용자 프로필 : 832
    모든 사용자 프로필 : hackingcamp-5G
    모든 사용자 프로필 : HackingCamp3
    모든 사용자 프로필 : hackingcamp1
    모든 사용자 프로필 : hackingcamp2
    모든 사용자 프로필 : ZIO
    모든 사용자 프로필 : NETGEAR90
    모든 사용자 프로필 : Besco2
    모든 사용자 프로필 : Japanize_guest
    모든 사용자 프로필 : Twosome_2ED1
    모든 사용자 프로필 : kirura4
    모든 사용자 프로필 : HO
    모든 사용자 프로필 : Dorks
    모든 사용자 프로필 : POC_GUEST#2
    모든 사용자 프로필 : POC_GUEST#4
```

Windows

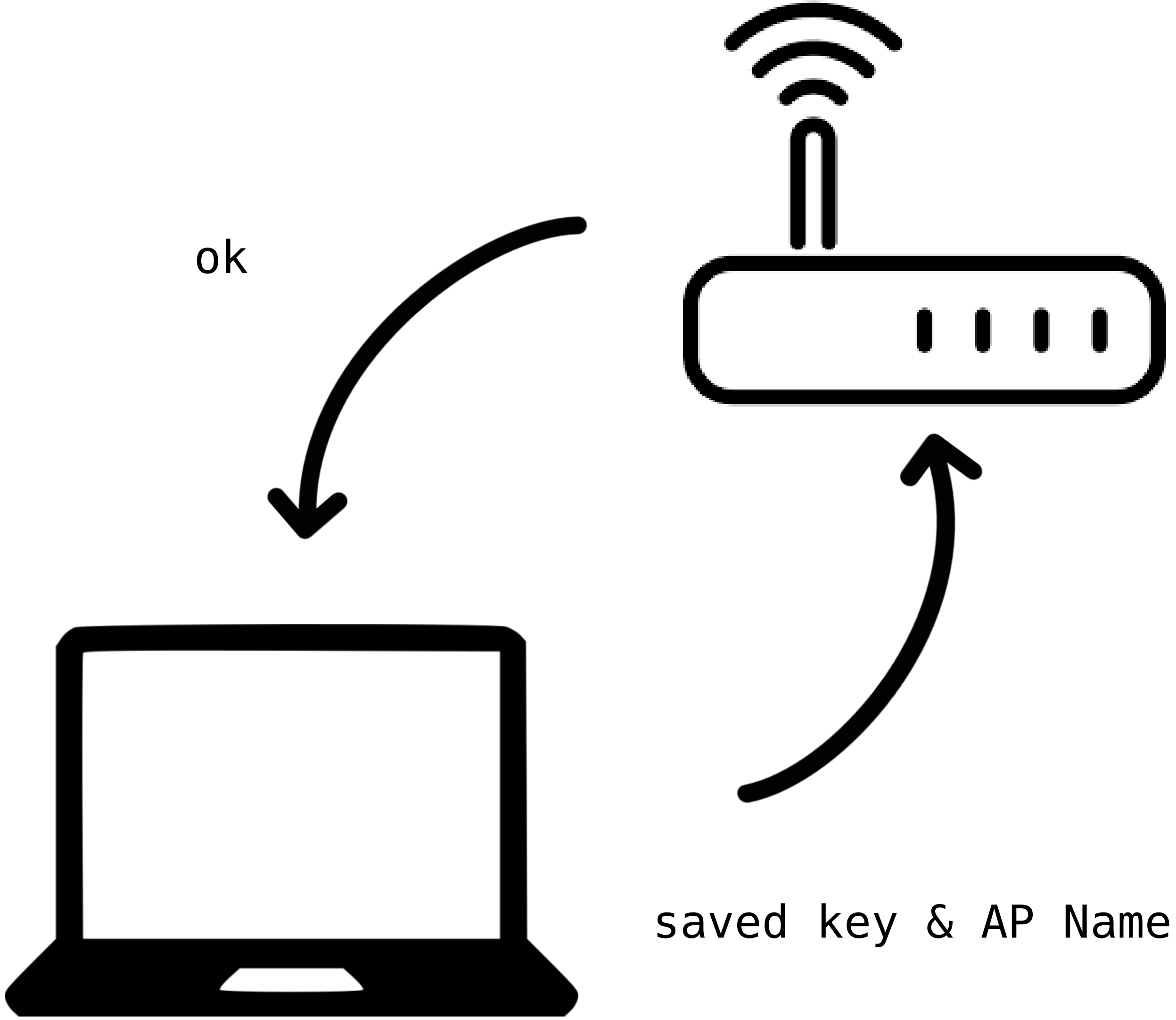
- ➢ netsh wlan show profiles
- ➢ netsh wlan show profile name="AP_name" key=clear

MAC

- ➢ security find-generic-password -wa AP_name



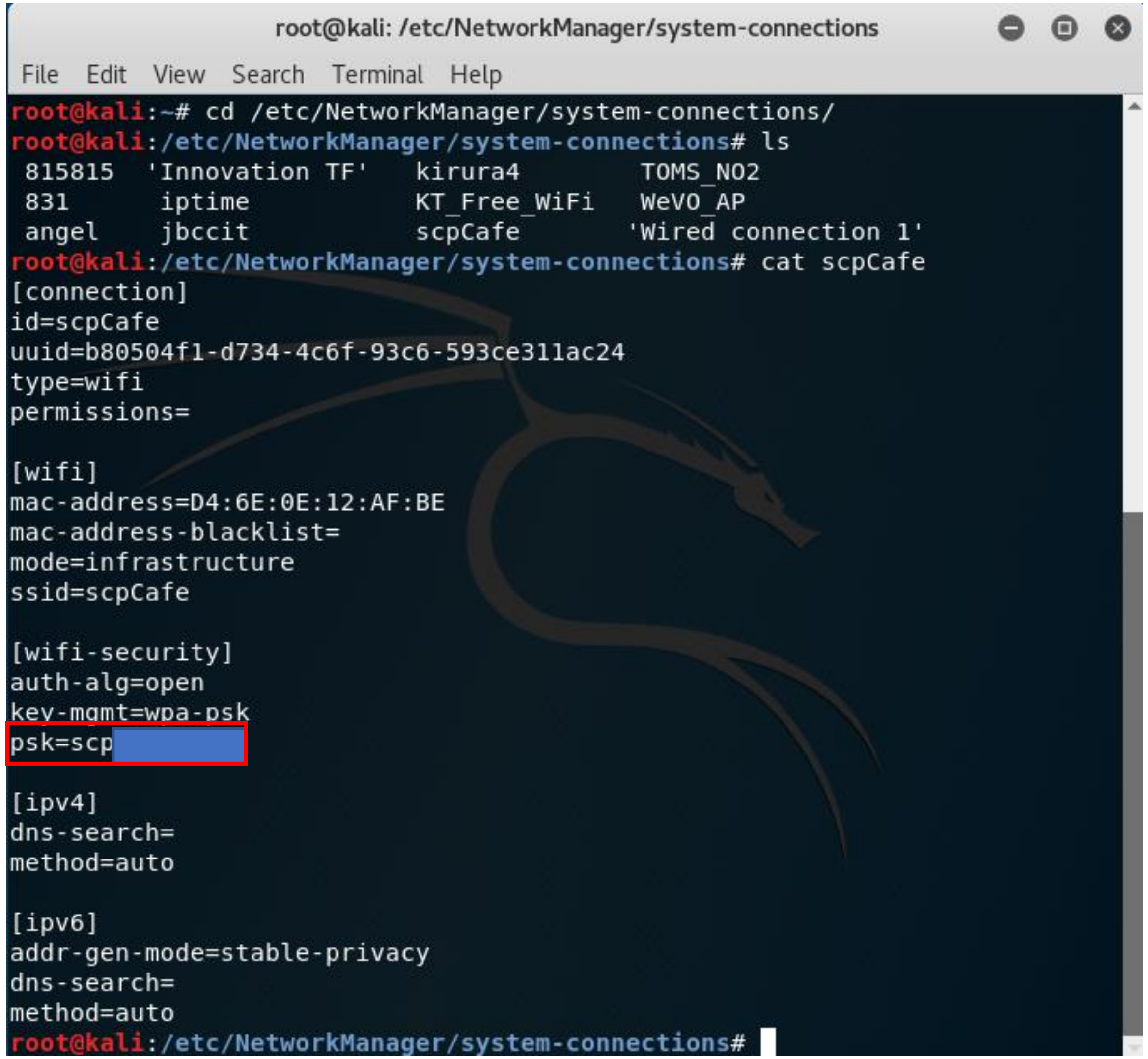
```
C:₩WINDOWS₩system32>netsh wlan show profile name=91614006 key=clear

Wi-Fi 인터페이스의 91614006 프로필:
=======================================================================

적용됨: 모든 사용자 프로필

프로필 정보
-------------------
    버전                   : 1
    유형                   : 무선 LAN
    이름                   : 91614006
    제어 옵션              :
        연결 모드          : 자동 연결
        네트워크 브로드캐스트: 이 네트워크가 브로드캐스트 중인 경우에만 연결
        자동 전환          : 다른 네트워크로 전환 안 함
        MAC 임의 지정      : 사용 안 함

연결 설정
---------------------
    SSID 개수              : 1
    SSID 이름              : "91614006"
    네트워크 종류          : 인프라
    Radio 유형             : [ 모든 무선 유형 ]
    공급업체 확장          : 없음

보안 설정
-----------------
    인증                   : WPA2-개인
    암호                   : CCMP
    인증                   : WPA2-개인
    암호                   : GCMP
    보안 키                : 있음
    키 콘텐츠              : 01033429762

비용 설정
-------------
    비용                   : 제한 없음
    정체됨                 : 아니요
    데이터 제한에 근접: 아니요
    데이터 제한 초과       : 아니요
    로밍                   : 아니요
    비용 출처              : 기본값
```



ok

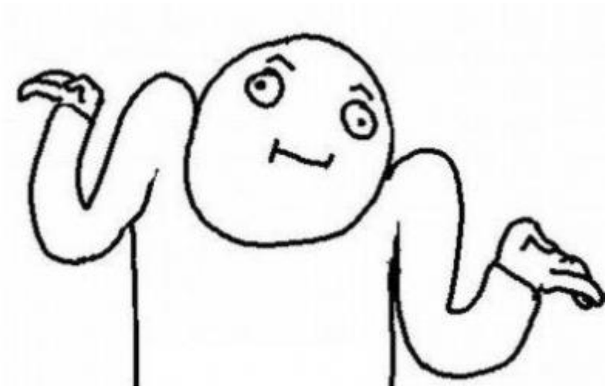
saved key & AP Name

in Linux(kali)


root@kali: /etc/NetworkManager/system-connections
File Edit View Search Terminal Help

```
root@kali:~# cd /etc/NetworkManager/system-connections/
root@kali:/etc/NetworkManager/system-connections# ls
 815815  'Innovation TF'   kirura4       TOMS_NO2
 831      iptime           KT_Free_WiFi  WeVO_AP
 angel    jbccit           scpCafe      'Wired connection 1'
root@kali:/etc/NetworkManager/system-connections# cat scpCafe
[connection]
id=scpCafe
uuid=b80504f1-d734-4c6f-93c6-593ce311ac24
type=wifi
permissions=

[wifi]
mac-address=D4:6E:0E:12:AF:BE
mac-address-blacklist=
mode=infrastructure
ssid=scpCafe

[wifi-security]
auth-alg=open
key-mgmt=wpa-psk
psk=scp[redacted]

[ipv4]
dns-search=
method=auto

[ipv6]
addr-gen-mode=stable-privacy
dns-search=
method=auto
root@kali:/etc/NetworkManager/system-connections# 
```

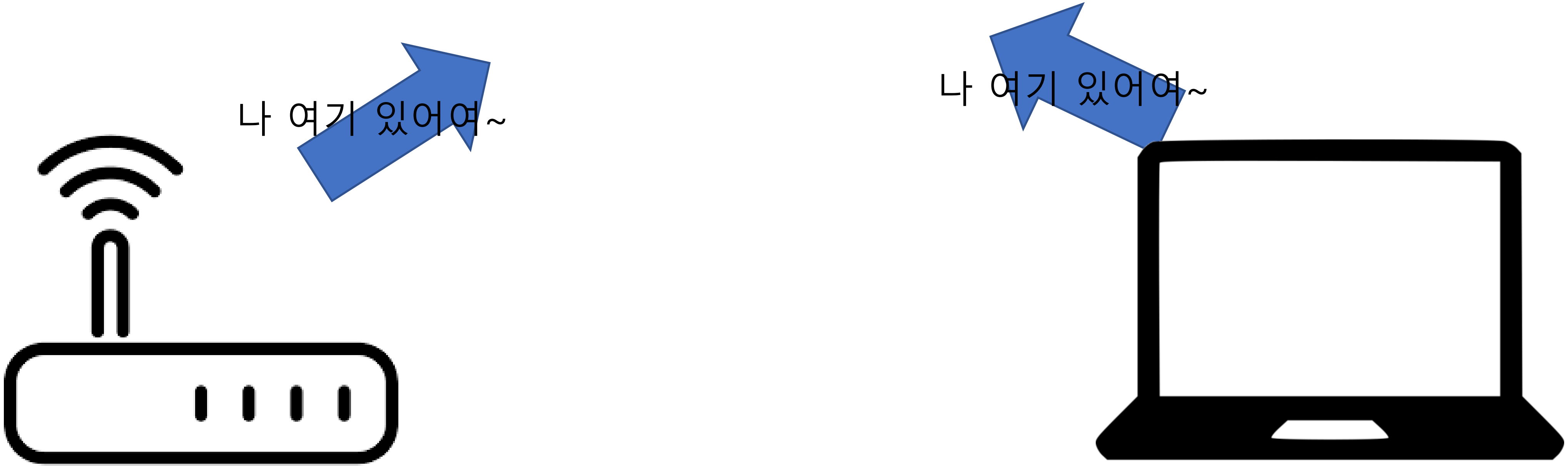
where?



saved key & AP Name

공유기와 장치가 서로 확인하는 방법

AP Station

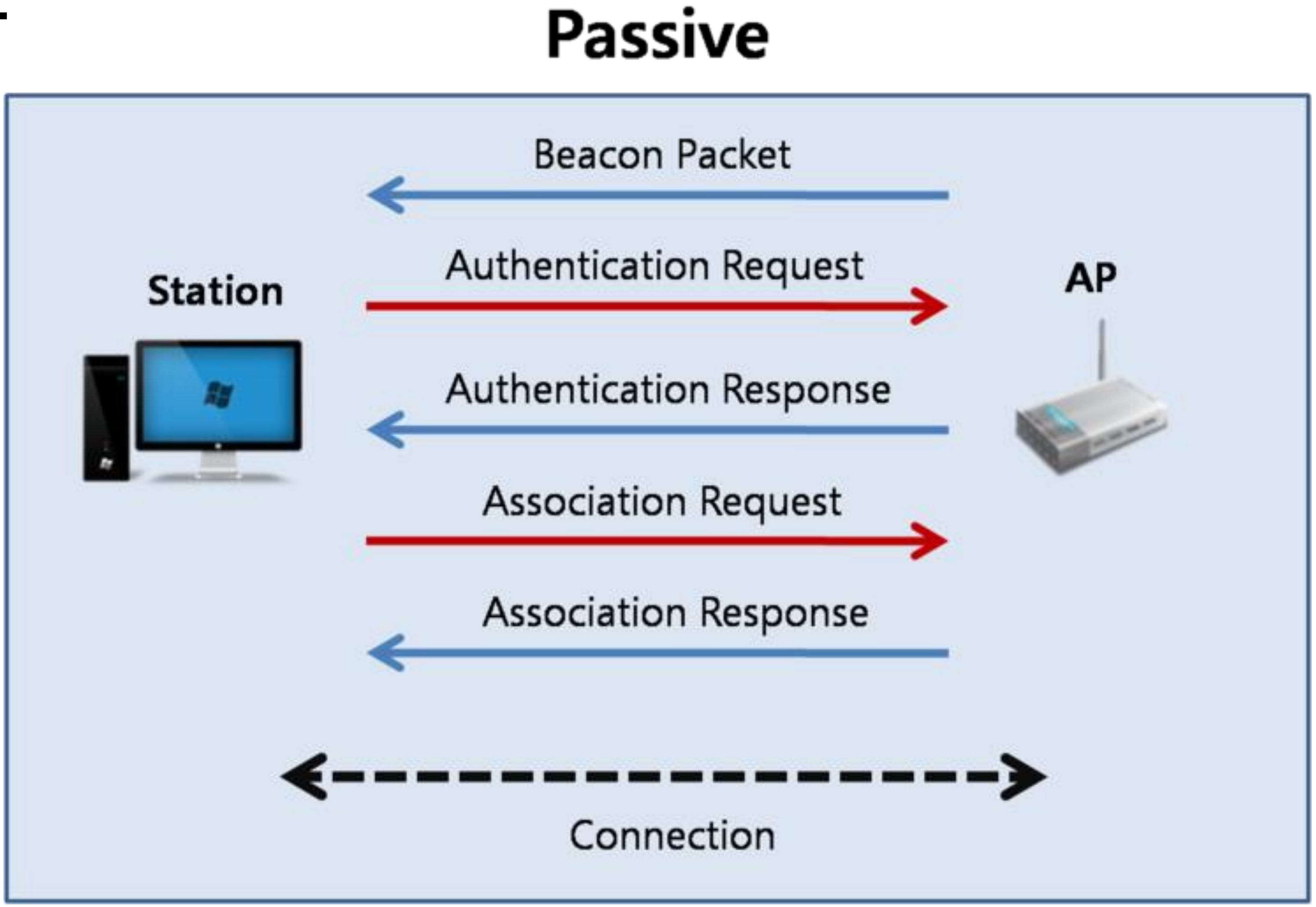


나 여기 있어여~

나 여기 있어여~

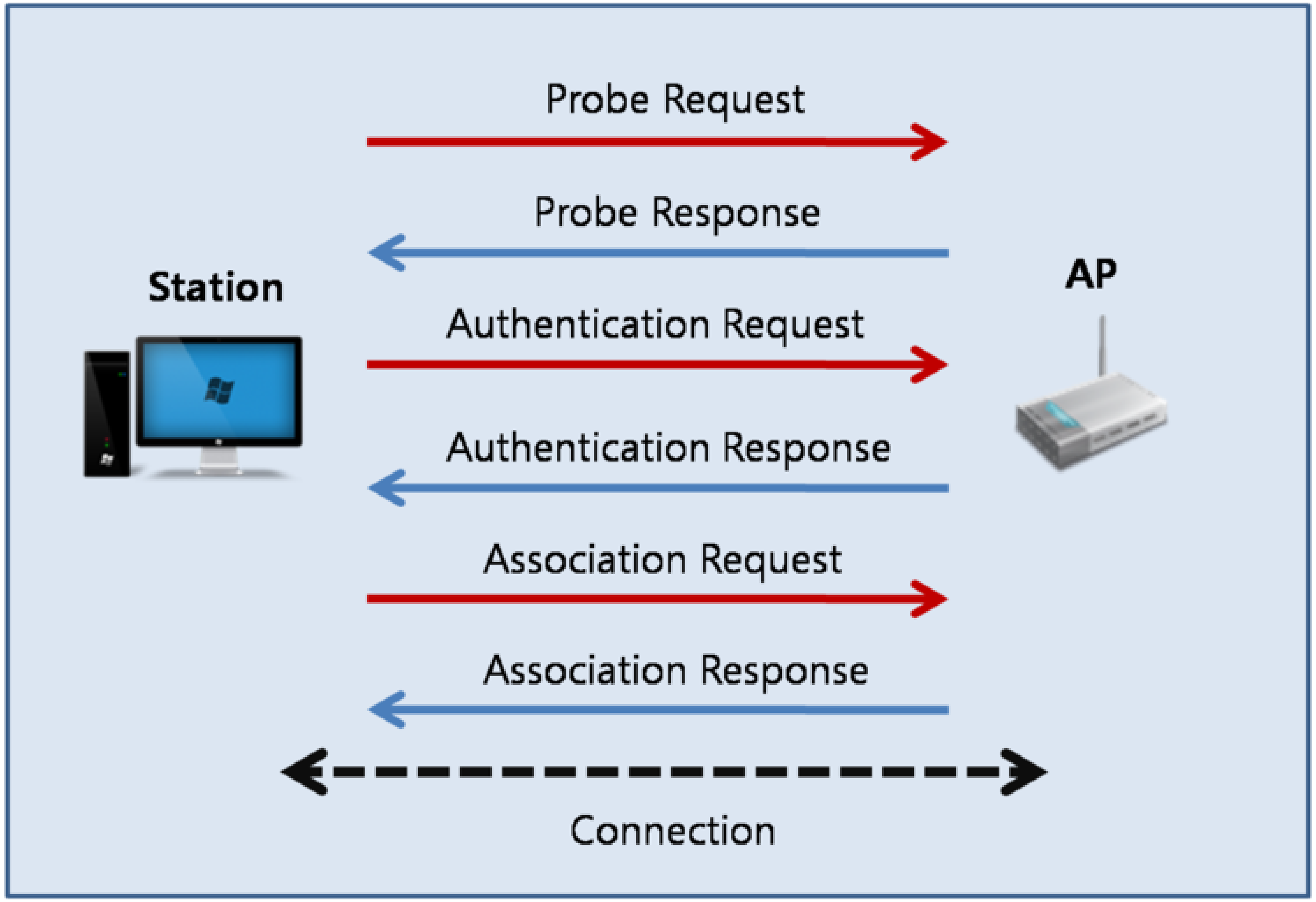
802.11 의 결합 방식

패시브


Passive
Beacon Packet
Station
Authentication Request
AP
Authentication Response
Association Request
Association Response
Connection

액티브

Active



Probe Request

Probe Response

Station

AP

Authentication Request

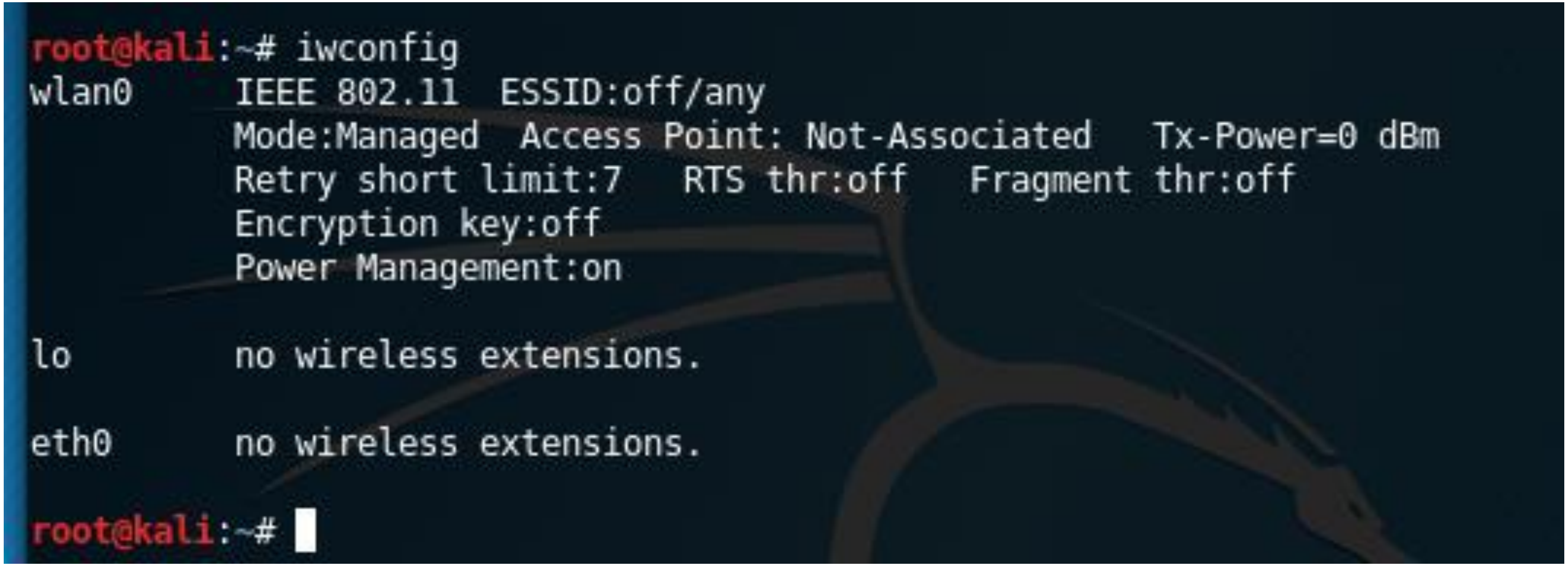
Authentication Response

Association Request

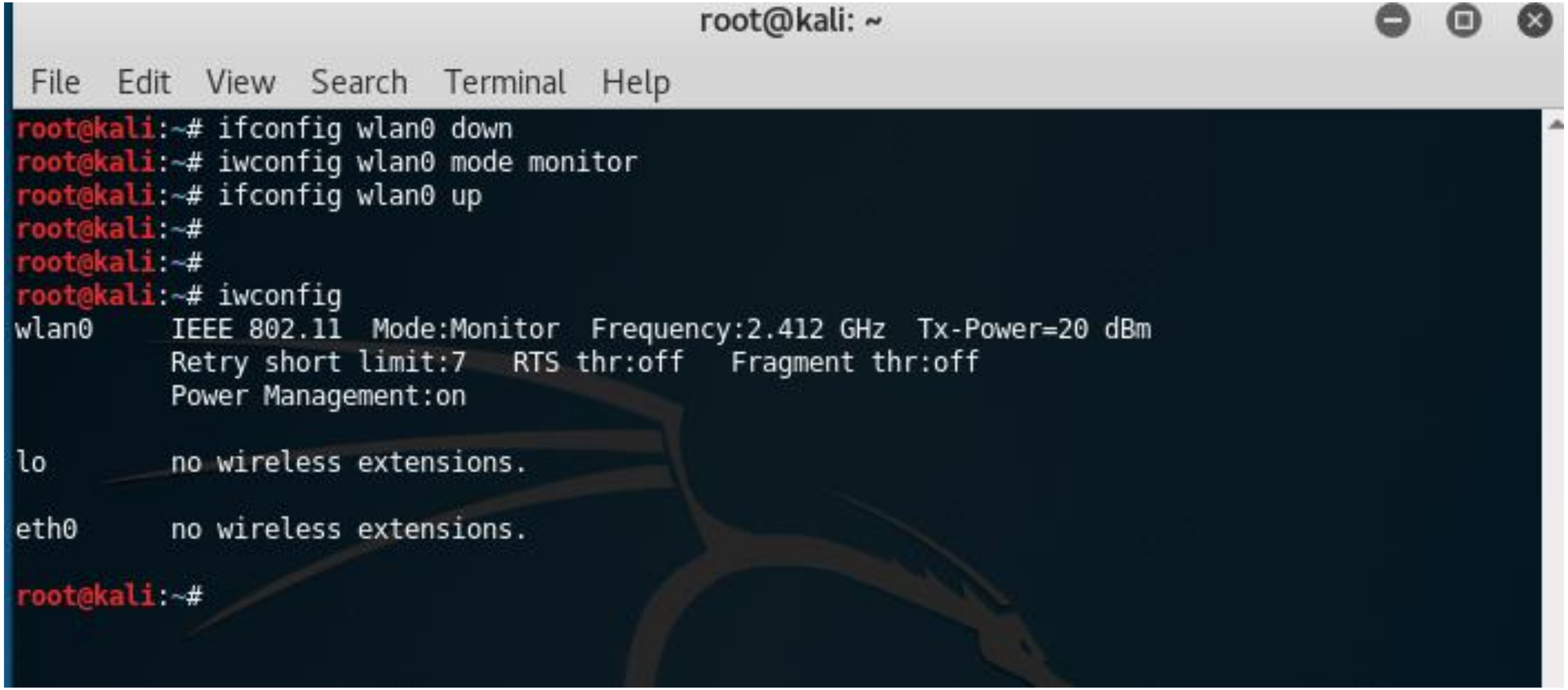
Association Response

Connection

패킷 캡쳐 (monitor mode)

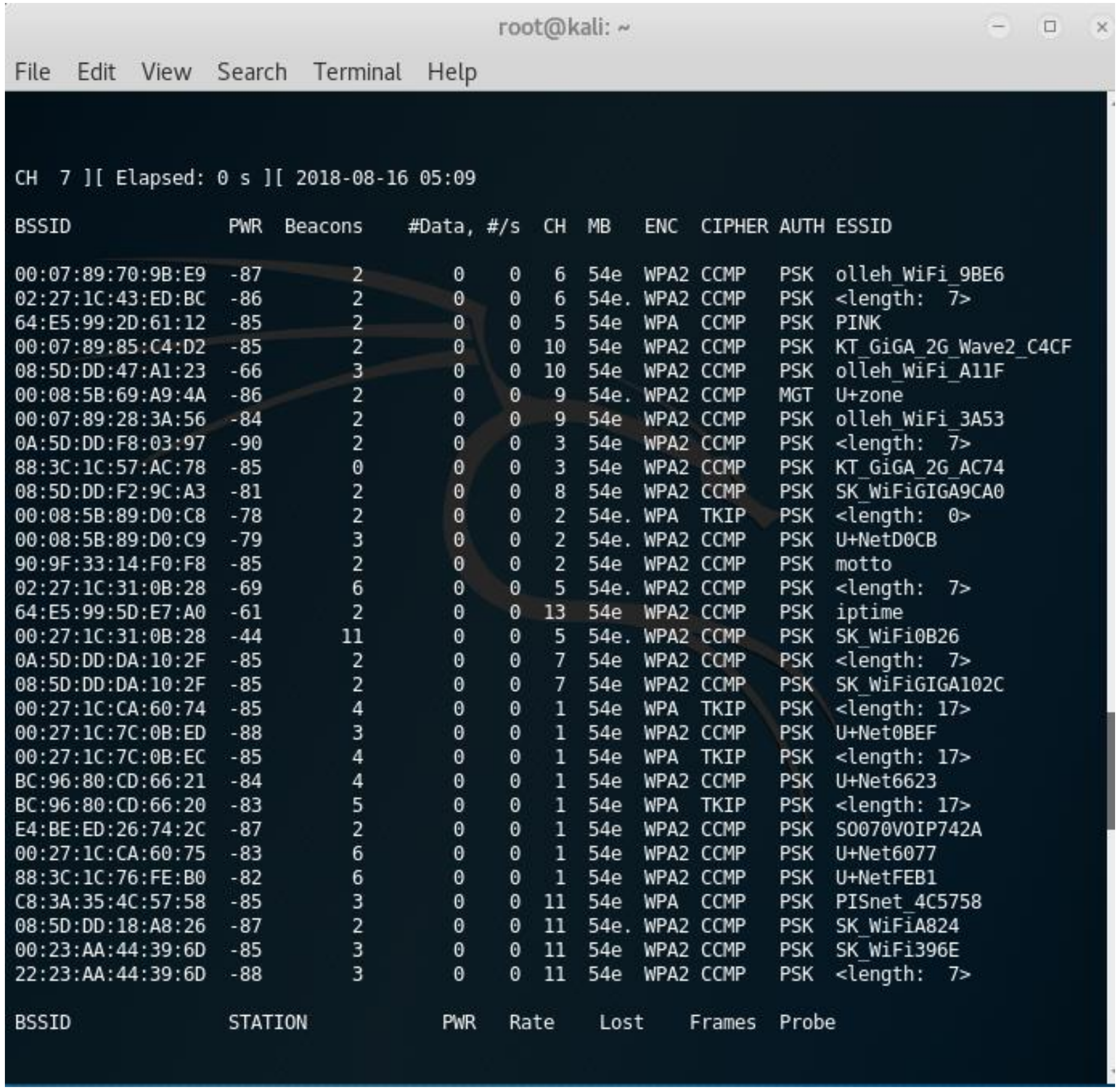


```
root@kali:~# iwconfig
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

lo        no wireless extensions.

eth0      no wireless extensions.

root@kali:~# 
```



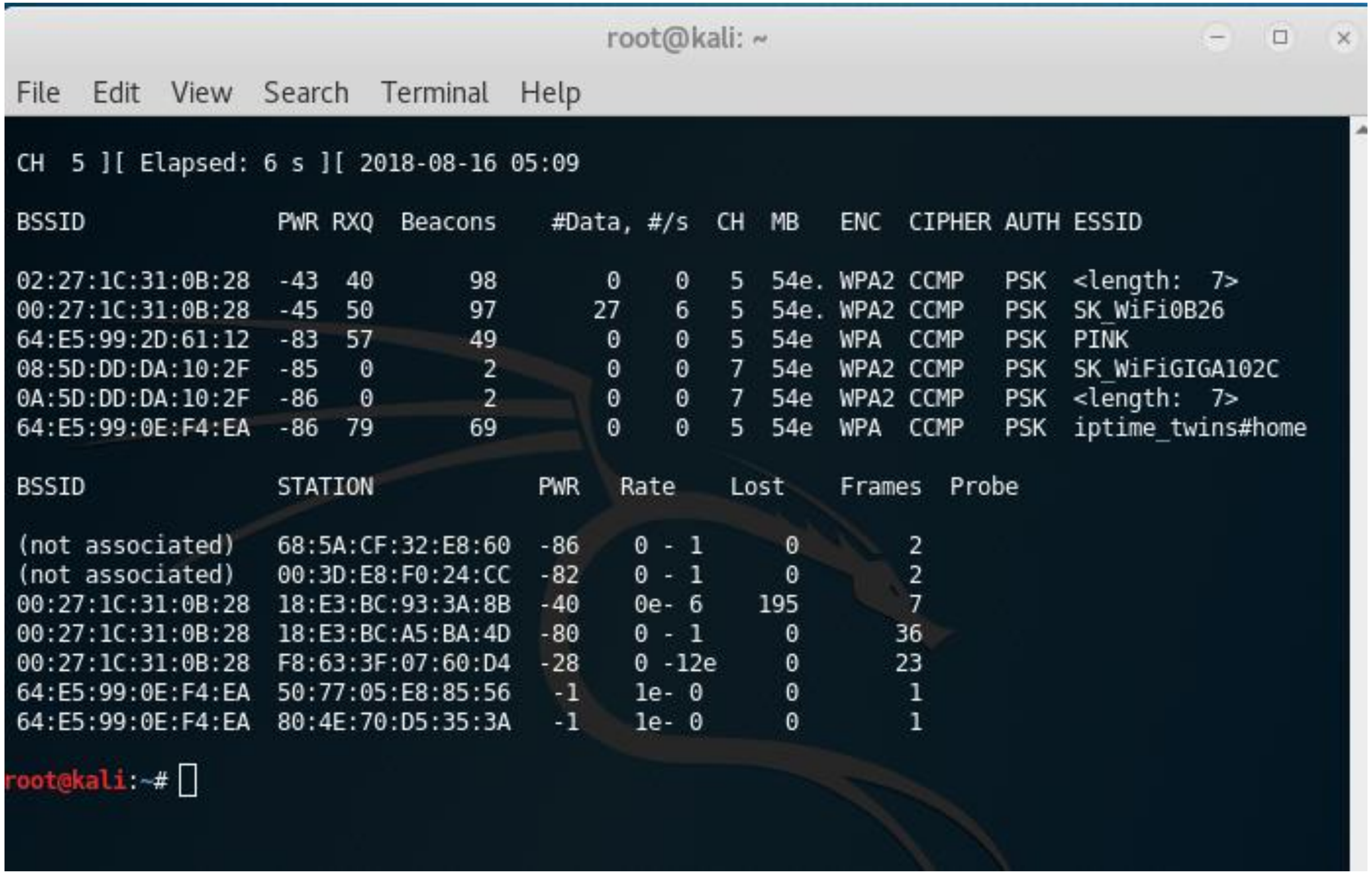
```
root@kali:~# ifconfig wlan0 down
root@kali:~# iwconfig wlan0 mode monitor
root@kali:~# ifconfig wlan0 up
root@kali:~#
root@kali:~#
root@kali:~# iwconfig
wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

lo        no wireless extensions.

eth0      no wireless extensions.

root@kali:~#
```

```
# airodump-ng wlan0
```

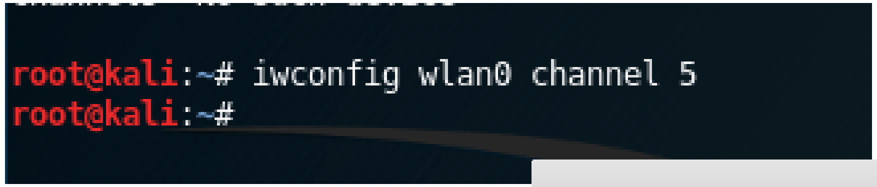


```
CH  7 ][ Elapsed: 0 s ][ 2018-08-16 05:09

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:07:89:70:9B:E9  -87        2        0    0   6  54e  WPA2 CCMP   PSK  olleh_WiFi_9BE6
02:27:1C:43:ED:BC  -86        2        0    0   6  54e. WPA2 CCMP   PSK  <length:  7>
64:E5:99:2D:61:12  -85        2        0    0   5  54e  WPA  CCMP   PSK  PINK
00:07:89:85:C4:D2  -85        2        0    0  10  54e  WPA2 CCMP   PSK  KT_GiGA_2G_Wave2_C4CF
08:5D:DD:47:A1:23  -66        3        0    0  10  54e  WPA2 CCMP   PSK  olleh_WiFi_A11F
00:08:5B:69:A9:4A  -86        2        0    0   9  54e. WPA2 CCMP   MGT  U+zone
00:07:89:28:3A:56  -84        2        0    0   9  54e  WPA2 CCMP   PSK  olleh_WiFi_3A53
0A:5D:DD:F8:03:97  -90        2        0    0   3  54e  WPA2 CCMP   PSK  <length:  7>
88:3C:1C:57:AC:78  -85        0        0    0   3  54e  WPA2 CCMP   PSK  KT_GiGA_2G_AC74
08:5D:DD:F2:9C:A3  -81        2        0    0   8  54e  WPA2 CCMP   PSK  SK_WiFiGIGA9CA0
00:08:5B:89:D0:C8  -78        2        0    0   2  54e. WPA  TKIP   PSK  <length:  0>
00:08:5B:89:D0:C9  -79        3        0    0   2  54e. WPA2 CCMP   PSK  U+NetD0CB
90:9F:33:14:F0:F8  -85        2        0    0   2  54e  WPA2 CCMP   PSK  motto
02:27:1C:31:0B:28  -69        6        0    0   5  54e. WPA2 CCMP   PSK  <length:  7>
64:E5:99:5D:E7:A0  -61        2        0    0  13  54e  WPA2 CCMP   PSK  iptime
00:27:1C:31:0B:28  -44       11        0    0   5  54e. WPA2 CCMP   PSK  SK_WiFi0B26
0A:5D:DD:DA:10:2F  -85        2        0    0   7  54e  WPA2 CCMP   PSK  <length:  7>
08:5D:DD:DA:10:2F  -85        2        0    0   7  54e  WPA2 CCMP   PSK  SK_WiFiGIGA102C
00:27:1C:CA:60:74  -85        4        0    0   1  54e  WPA  TKIP   PSK  <length: 17>
00:27:1C:7C:0B:ED  -88        3        0    0   1  54e  WPA2 CCMP   PSK  U+Net0BEF
00:27:1C:7C:0B:EC  -85        4        0    0   1  54e  WPA  TKIP   PSK  <length: 17>
BC:96:80:CD:66:21  -84        4        0    0   1  54e  WPA2 CCMP   PSK  U+Net6623
BC:96:80:CD:66:20  -83        5        0    0   1  54e  WPA  TKIP   PSK  <length: 17>
E4:BE:ED:26:74:2C  -87        2        0    0   1  54e  WPA2 CCMP   PSK  SO070VOIP742A
00:27:1C:CA:60:75  -83        6        0    0   1  54e  WPA2 CCMP   PSK  U+Net6077
88:3C:1C:76:FE:B0  -82        6        0    0   1  54e  WPA2 CCMP   PSK  U+NetFEB1
C8:3A:35:4C:57:58  -85        3        0    0  11  54e  WPA  CCMP   PSK  PISnet_4C5758
08:5D:DD:18:A8:26  -87        2        0    0  11  54e. WPA2 CCMP   PSK  SK_WiFiA824
00:23:AA:44:39:6D  -85        3        0    0  11  54e  WPA2 CCMP   PSK  SK_WiFi396E
22:23:AA:44:39:6D  -88        3        0    0  11  54e  WPA2 CCMP   PSK  <length:  7>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

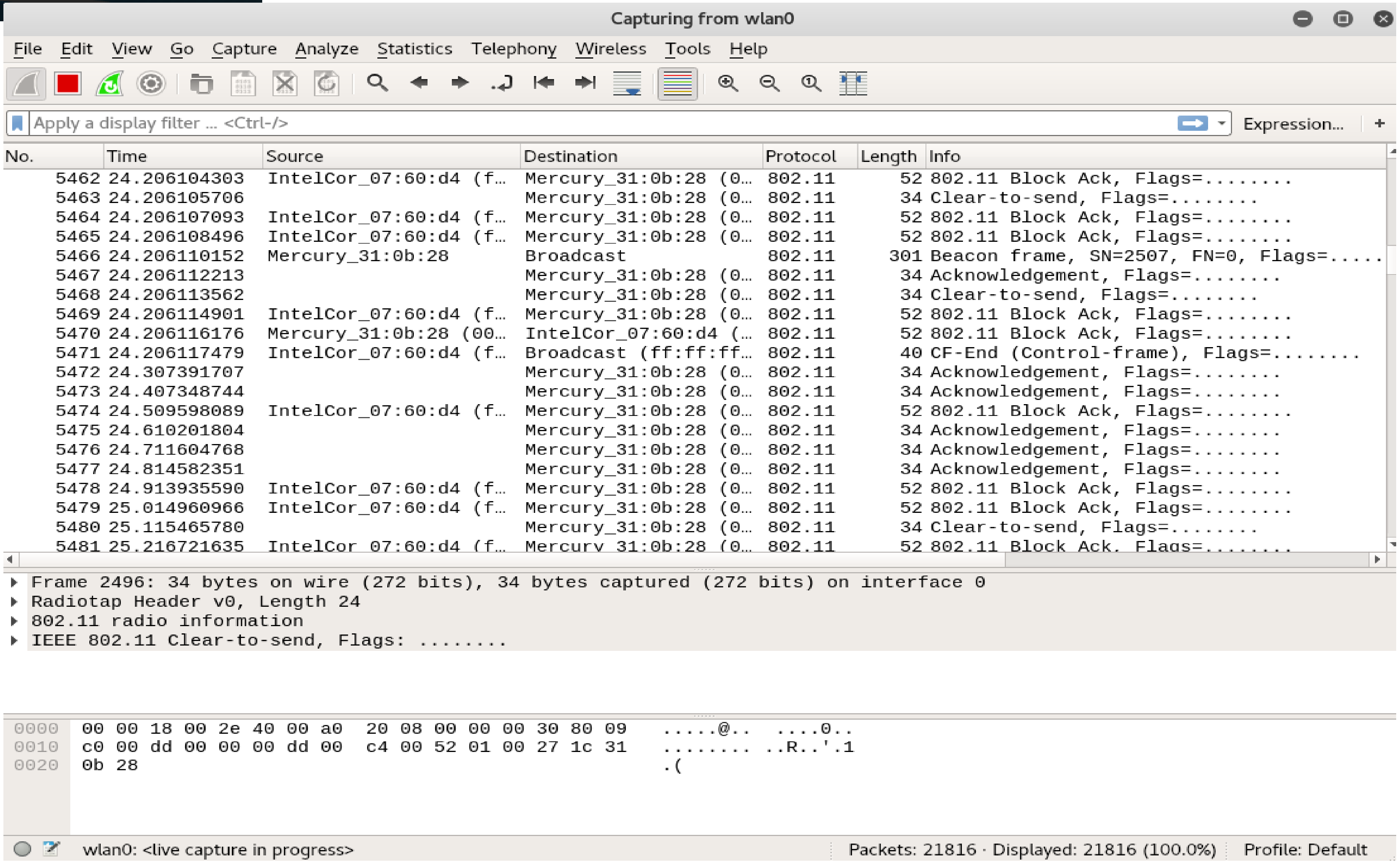
```
# airodump-ng wlan0 –c 5
```



```
CH  5 ][ Elapsed: 6 s ][ 2018-08-16 05:09

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:27:1C:31:0B:28  -43  40       98        0    0   5  54e. WPA2 CCMP   PSK  <length:  7>
00:27:1C:31:0B:28  -45  50       97       27    6   5  54e. WPA2 CCMP   PSK  SK_WiFi0B26
64:E5:99:2D:61:12  -83  57       49        0    0   5  54e  WPA  CCMP   PSK  PINK
08:5D:DD:DA:10:2F  -85   0        2        0    0   7  54e  WPA2 CCMP   PSK  SK_WiFiGIGA102C
0A:5D:DD:DA:10:2F  -86   0        2        0    0   7  54e  WPA2 CCMP   PSK  <length:  7>
64:E5:99:0E:F4:EA  -86  79       69        0    0   5  54e  WPA  CCMP   PSK  iptime_twins#home

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   68:5A:CF:32:E8:60  -86    0 - 1      0        2
(not associated)   00:3D:E8:F0:24:CC  -82    0 - 1      0        2
00:27:1C:31:0B:28  18:E3:BC:93:3A:8B  -40    0e- 6    195        7
00:27:1C:31:0B:28  18:E3:BC:A5:BA:4D  -80    0 - 1      0       36
00:27:1C:31:0B:28  F8:63:3F:07:60:D4  -28    0 -12e     0       23
64:E5:99:0E:F4:EA  50:77:05:E8:85:56   -1    1e- 0      0        1
64:E5:99:0E:F4:EA  80:4E:70:D5:35:3A   -1    1e- 0      0        1

root@kali:~# 
```



```
root@kali:~# iwconfig wlan0 channel 5
root@kali:~#
```



Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.  Time            Source                   Destination              Protocol  Length Info
 5462 24.206104303 IntelCor_07:60:d4 (f…  Mercury_31:0b:28 (0…  802.11     52 802.11 Block Ack, Flags=........
 5463 24.206105706                        Mercury_31:0b:28 (0…  802.11     34 Clear-to-send, Flags=........
 5464 24.206107093 IntelCor_07:60:d4 (f…  Mercury_31:0b:28 (0…  802.11     52 802.11 Block Ack, Flags=........
 5465 24.206108496 IntelCor_07:60:d4 (f…  Mercury_31:0b:28 (0…  802.11     52 802.11 Block Ack, Flags=........
 5466 24.206110152 Mercury_31:0b:28       Broadcast             802.11    301 Beacon frame, SN=2507, FN=0, Flags=.....
 5467 24.206112213                        Mercury_31:0b:28 (0…  802.11     34 Acknowledgement, Flags=........
 5468 24.206113562                        Mercury_31:0b:28 (0…  802.11     34 Clear-to-send, Flags=........
 5469 24.206114901 IntelCor_07:60:d4 (f…  Mercury_31:0b:28 (0…  802.11     52 802.11 Block Ack, Flags=........
 5470 24.206116176 Mercury_31:0b:28 (00…  IntelCor_07:60:d4 (…  802.11     52 802.11 Block Ack, Flags=........
 5471 24.206117479 IntelCor_07:60:d4 (f…  Broadcast (ff:ff:ff…  802.11     40 CF-End (Control-frame), Flags=........
 5472 24.307391707                        Mercury_31:0b:28 (0…  802.11     34 Acknowledgement, Flags=........
 5473 24.407348744                        Mercury_31:0b:28 (0…  802.11     34 Acknowledgement, Flags=........
 5474 24.509598089 IntelCor_07:60:d4 (f…  Mercury_31:0b:28 (0…  802.11     52 802.11 Block Ack, Flags=........
 5475 24.610201804                        Mercury_31:0b:28 (0…  802.11     34 Acknowledgement, Flags=........
 5476 24.711604768                        Mercury_31:0b:28 (0…  802.11     34 Acknowledgement, Flags=........
 5477 24.814582351                        Mercury_31:0b:28 (0…  802.11     34 Acknowledgement, Flags=........
 5478 24.913935590 IntelCor_07:60:d4 (f…  Mercury_31:0b:28 (0…  802.11     52 802.11 Block Ack, Flags=........
 5479 25.014960966 IntelCor_07:60:d4 (f…  Mercury_31:0b:28 (0…  802.11     52 802.11 Block Ack, Flags=........
 5480 25.115465780                        Mercury_31:0b:28 (0…  802.11     34 Clear-to-send, Flags=........
 5481 25.216721635 IntelCor_07:60:d4 (f…  Mercury_31:0b:28 (0…  802.11     52 802.11 Block Ack, Flags=........
```

```
▸ Frame 2496: 34 bytes on wire (272 bits), 34 bytes captured (272 bits) on interface 0
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▸ IEEE 802.11 Clear-to-send, Flags: ........
```

```
0000  00 00 18 00 2e 40 00 a0  20 08 00 00 00 30 80 09   .....@..  ....0..
0010  c0 00 dd 00 00 00 dd 00  c4 00 52 01 00 27 1c 31   ........ ..R..'.1
0020  0b 28                                              .(
```

```
wlan0: <live capture in progress>        Packets: 21816 · Displayed: 21816 (100.0%)     Profile: Default
```