무선 패킷 수집 방법 - 환경 구축

- 환경
  - Kali Linux, iptime n150UA NIC
- 외장 WLAN카드를 Monitor 모드로 변환

```
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

```
root@kali:~# ifconfig wlan0 down
root@kali:~# iwconfig wlan0 mode monitor
root@kali:~# ifconfig wlan0 up
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

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:off
```

무선 패킷 수집 방법 - 환경 구축

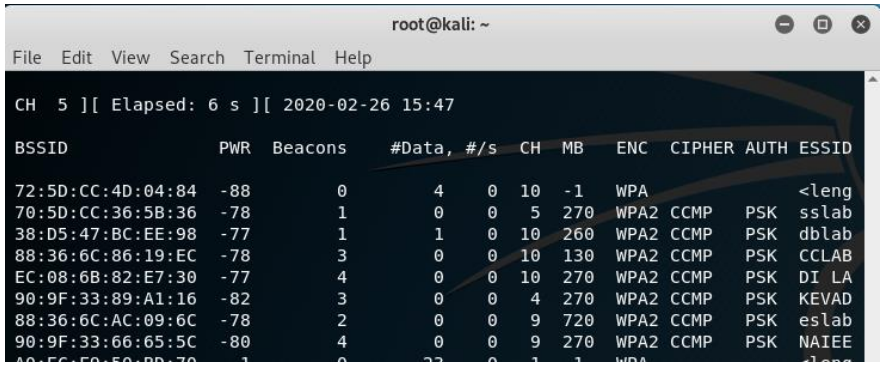
- Monitor Mode인 NIC는 1번 채널만 Listen

Source	Destination	Protocol	Length	Signal strength (dBm)	Duration	Tag	Tag	SSID	Channel
Apple_85:db:b7	Cisco_50:bd:70	802.11	48	-59dBm	32µs				1
	Broadcom_08:db:b7 (…	802.11	34	-59dBm	40µs				1
Fn-LinkT_6e:67:58 (…	AsustekC_c1:fb:68 (…	802.11	40	-87dBm	320µs				1
	Broadcom_08:db:b7 (…	802.11	34	-59dBm	40µs				1
Fn-LinkT_6e:67:58 (…	AsustekC_c1:fb:68 (…	802.11	40	-87dBm	320µs				1
	Fn-LinkT_6e:67:58 (…	802.11	34	-73dBm	272µs				1
Apple_85:db:b7	Cisco_50:bd:70	802.11	48	-57dBm	32µs				1
Apple_85:db:b7	Cisco_50:bd:70	802.11	48	-57dBm	32µs				1
Apple_85:db:b7	Cisco_50:bd:70	802.11	48	-55dBm	210µs				1
Apple_85:db:b7	Cisco_50:bd:70	802.11	48	-57dBm	32µs				1
Fn-LinkT_6e:67:58 (…	AsustekC_c1:fb:68 (…	802.11	40	-89dBm	320µs				1
EfmNetwo_23:e6:d8	Broadcast	802.11	279	-63dBm	2232µs	✓	✓	SDLab	1
AsustekC_c1:fb:68 (…	Fn-LinkT_6e:67:58 (…	802.11	44	-71dBm	352µs				1
	Fn-LinkT_6e:67:58 (…	802.11	34	-73dBm	272µs				1
Mercury_c5:40:59	Broadcast	802.11	267	-77dBm	2136µs	✓	✓	U+Net405B	1

- 전체 채널 탐색을 위해 Airodump-ng 사용

무선 패킷 수집 방법 - 환경 구축

- Monitor Mode인 NIC는 1번 채널만 Listen
- 전체 채널 탐색을 위해 Airodump-ng 사용
  - airodump-ng wlan0
  - 터미널을 닫지 않은 상태로 wireshark 실행 시 모든 채널의 패킷 캡처 가능



Source	Destination	Protocol	Length	Signal strength (dBm)	Duration	Tag	Tag	SSID	Channel
EfmNetwo_1f:1f:d4	Broadcast	802.11	279	-75dBm	2232µs	✓	✓	sslab	6
TendaTec_36:60:00	Broadcast	802.11	216	-73dBm	1728µs	✓	✓	cse_5603	6
EfmNetwo_1f:1f:d4	Broadcast	802.11	279	-77dBm	2232µs	✓	✓	sslab	12
EfmNetwo_1f:1f:d4	Broadcast	802.11	279	-77dBm	2232µs	✓	✓	sslab	12
Netgear_7f:3f:4d	Broadcast	802.11	331	-89dBm	2648µs	✓	✓	CCLAB2	12
Mercury_c5:40:58	Broadcast	802.11	277	-79dBm	2216µs	✓	✓		12
Mercury_c5:40:58	Broadcast	802.11	277	-79dBm	2216µs	✓	✓		12
SamsungE_75:86:c5	Broadcast	802.11	100	-83dBm	800µs	✓	✓	iptime	12
EfmNetwo_23:e6:d8	Broadcast	802.11	279	-63dBm	2232µs	✓	✓	SDLab	1
Mercury_c5:40:59	Broadcast	802.11	267	-79dBm	2136µs	✓	✓	U+Net405B	1
Mercury_c5:40:58	Broadcast	802.11	277	-79dBm	2216µs	✓	✓		1

무선 패킷 수집 방법

- 자동화를 위해서 Wireshark보다 Tshark 사용 권장
  - 필터링 옵션을 이용하여 다양한 802.11 무선 패킷 중 Beacon frame과 Probe request만을 수집하여 불필요한 데이터를 제거
  - tshark -i <인터페이스명> -w <경로> -f 'wlan type mgt and subtype probe-req' -a duration:<수집할시간(초)>

```
root@kali:~/Desktop# tshark -i wlan0mon -w ~/Desktop/data/data.pcapng
-f 'wlan type mgt and (subtype beacon or subtype probe-req)' -a durati
on:86400
Running as user "root" and group "root". This could be dangerous.
Capturing on 'wlan0mon'
125
```