Open WiFi Cookie 탈취

: 쿠키런

정보보안융합S/W 윤성준
이경문 교수님, 이병천 교수님

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

목차

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

주제선정 이유

- 비밀번호가 없는 Open Wifi 를 생각보다 쉽게 찾을 수 있다. (iptime,지하철 무료 wifi 등)

- http 통신을 하는 사이트를 어렵지 찾을 수 있다.

- 유선통신에 비해 무선통신은 패킷 스니핑이 상대적으로 쉽다.

- 일반 사람들은 보안통신을 하지 않는 Open Wifi에 대해서 대수롭지 않게 생각한다.

Cookie 란

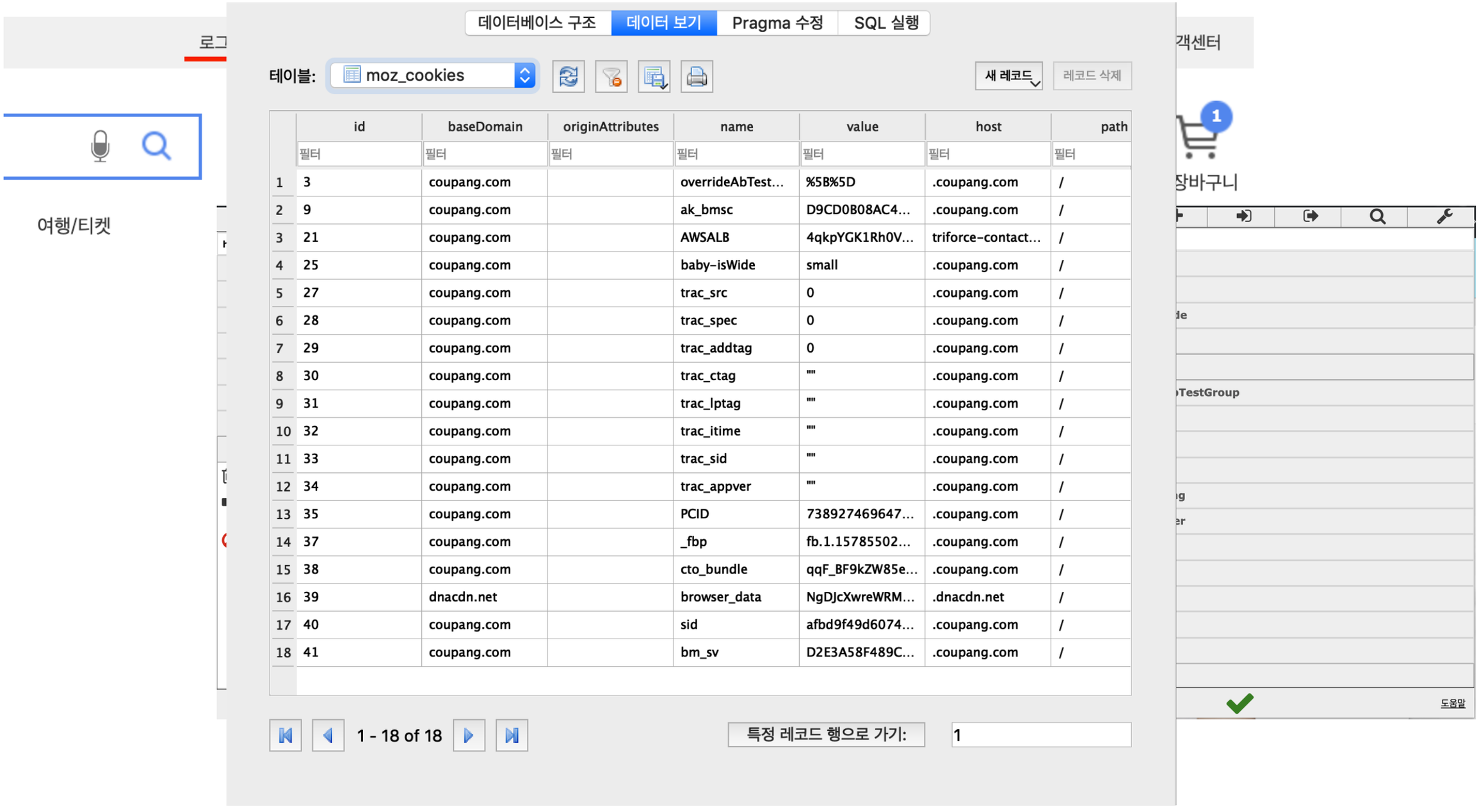
- 서버측에서 클라이언트 측에 상태 정보를 저장하고 추출할 수 있는 메커니즘.

- 클라이언트의 매 요청마다 웹 브라우저로부터 서버에게 전송되는 정보패킷의 일종이다.

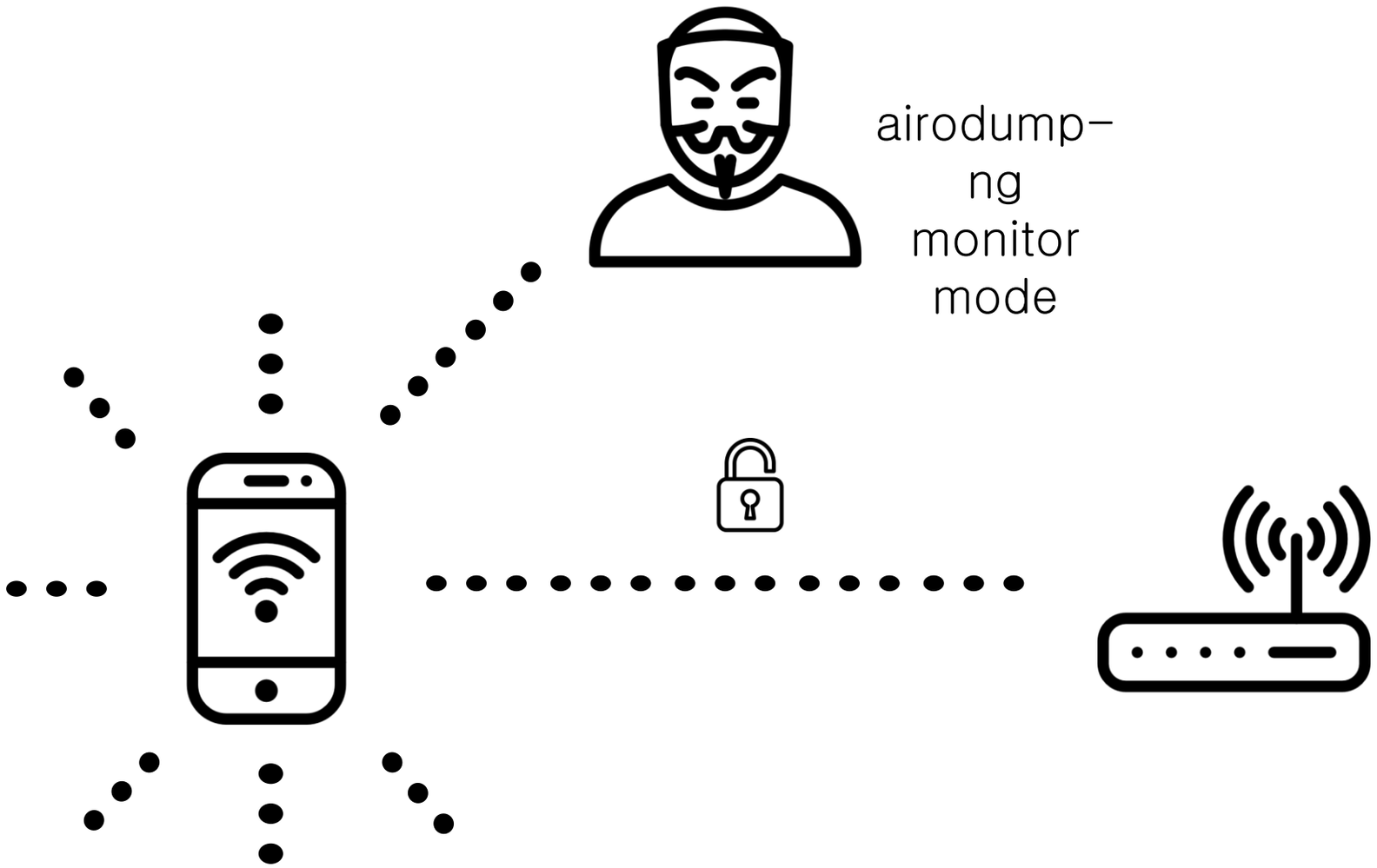
- HTTP에서 클라이언트의 상태 정보를 클라이언트의 하드 디스크에 저장하였다가 필요시 정보를 참조하거나 재 사용할수 있다.
ex) 방문했던 사이트를 다시 방문할 때 아이디와 비밀번호가 자동입력되는 현상

- Web 상에서 사용자 식별,사용자 정보 유지에 도움이 된다.

Cookie 란


로그
객센터
여행/티켓
장바구니
데이터베이스 구조
데이터 보기
Pragma 수정
SQL 실행
테이블:
moz_cookies
새 레코드
레코드 삭제
id
baseDomain
originAttributes
name
value
host
path
필터
1 3 coupang.com overrideAbTest... %5B%5D .coupang.com /
2 9 coupang.com ak_bmsc D9CD0B08AC4... .coupang.com /
3 21 coupang.com AWSALB 4qkpYGK1Rh0V... triforce-contact... /
4 25 coupang.com baby-isWide small .coupang.com /
5 27 coupang.com trac_src 0 .coupang.com /
6 28 coupang.com trac_spec 0 .coupang.com /
7 29 coupang.com trac_addtag 0 .coupang.com /
8 30 coupang.com trac_ctag "" .coupang.com /
9 31 coupang.com trac_lptag "" .coupang.com /
10 32 coupang.com trac_itime "" .coupang.com /
11 33 coupang.com trac_sid "" .coupang.com /
12 34 coupang.com trac_appver "" .coupang.com /
13 35 coupang.com PCID 738927469647... .coupang.com /
14 37 coupang.com _fbp fb.1.15785502... .coupang.com /
15 38 coupang.com cto_bundle qqF_BF9kZW85e... .coupang.com /
16 39 dnacdn.net browser_data NgDJcXwreWRM... .dnacdn.net /
17 40 coupang.com sid afbd9f49d6074... .coupang.com /
18 41 coupang.com bm_sv D2E3A58F489C... .coupang.com /
1 - 18 of 18
특정 레코드 행으로 가기:
1
TestGroup
도움말

구현 방법



Monitor Mode

- 모니터 모드란 쉽게 말해 무선랜 패킷을 볼 수 있는 모드이다.

- 기본적으로는 Managed mode 이다. (나에게만 오는 패킷만 받음)

- 모니터 모드를 하기 위해서는 모니터 모드를 지원하는 어댑터가 있어야 한다.

AWUS036NH

Monitor Mode

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUN
        inet 192.168.123.102  net
        inet6 fe80::20c:29ff:fee7
        ether 00:0c:29:e7:91:69
        RX packets 95  bytes 186
        RX errors 0  dropped 0
        TX packets 65  bytes 567
        TX errors 0  dropped 0 ov

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback
        RX packets 18  bytes 1038 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  fr
        TX packets 18  bytes 1038 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether c2:dc:91:9d:ee:33  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
```

```
root@kali:~# iwconfig wlan0
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

```
root@kali:~# iwconfig wlan0 mode monitor
root@kali:~# iwconfig wlan0
wlan0     IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off
```

ifconfig wlan0 down
iwconfig wlan0 mode monitor
ifconfig wlan0 up

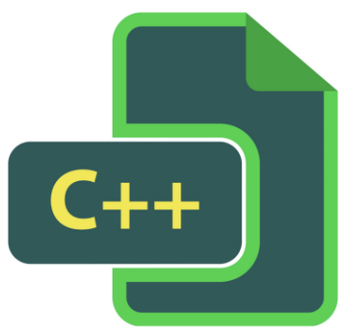
AP 정보 수집 및 채널 설정

```
CH  1 ][ Elapsed: 0 s ][ 2019-10-29 22:40

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

08:5D:DD:79:FF:07  -29        2        2    0  10  130  WPA2 CCMP   PSK  U+NetFF08
88:36:6C:FA:BC:FA  -16        3        0    0   1  135  OPN                  jun
```

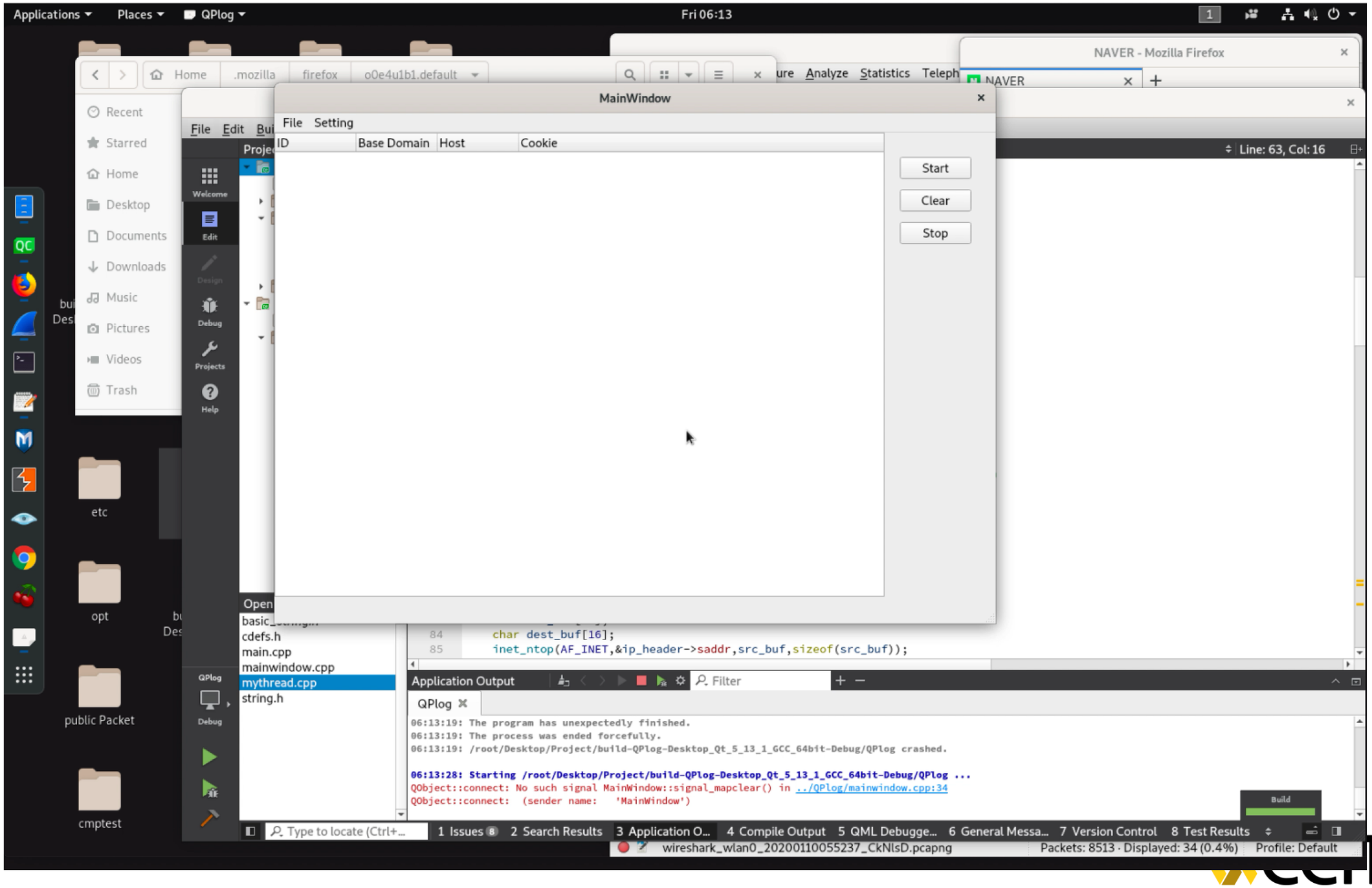
WiFi에 대한 정보 수집
airodump-ng wlan0

스니핑을 위한 네트워크 인터페이스 채널 설정(주파수 맞추기)
iwconfig wlan0 channel 1

개발 환경



데모 영상


Applications
Places
QPlog
Fri 06:13
MainWindow
File Setting
ID
Base Domain
Host
Cookie
Start
Clear
Stop
NAVER - Mozilla Firefox
NAVER
Line: 63, Col: 16
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
etc
opt
public Packet
cmptest
Welcome
Edit
Design
Debug
Projects
Help
cdefs.h
main.cpp
mainwindow.cpp
mythread.cpp
string.h
char dest_buf[16];
inet_ntop(AF_INET,&ip_header->saddr,src_buf,sizeof(src_buf));
Application Output
QPlog
06:13:19: The program has unexpectedly finished.
06:13:19: The process was ended forcefully.
06:13:19: /root/Desktop/Project/build-QPlog-Desktop_Qt_5_13_1_GCC_64bit-Debug/QPlog crashed.
06:13:28: Starting /root/Desktop/Project/build-QPlog-Desktop_Qt_5_13_1_GCC_64bit-Debug/QPlog ...
QObject::connect: No such signal MainWindow::signal_mapclear() in ../QPlog/mainwindow.cpp:34
QObject::connect: (sender name: 'MainWindow')
Build
Type to locate (Ctrl+...
1 Issues 2 Search Results 3 Application O... 4 Compile Output 5 QML Debugge... 6 General Messa... 7 Version Control 8 Test Results
wireshark_wlan0_20200110055237_CkNlsD.pcapng
Packets: 8513 · Displayed: 34 (0.4%)
Profile: Default

감사합니다

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY