



RF 무선통신 해킹시연

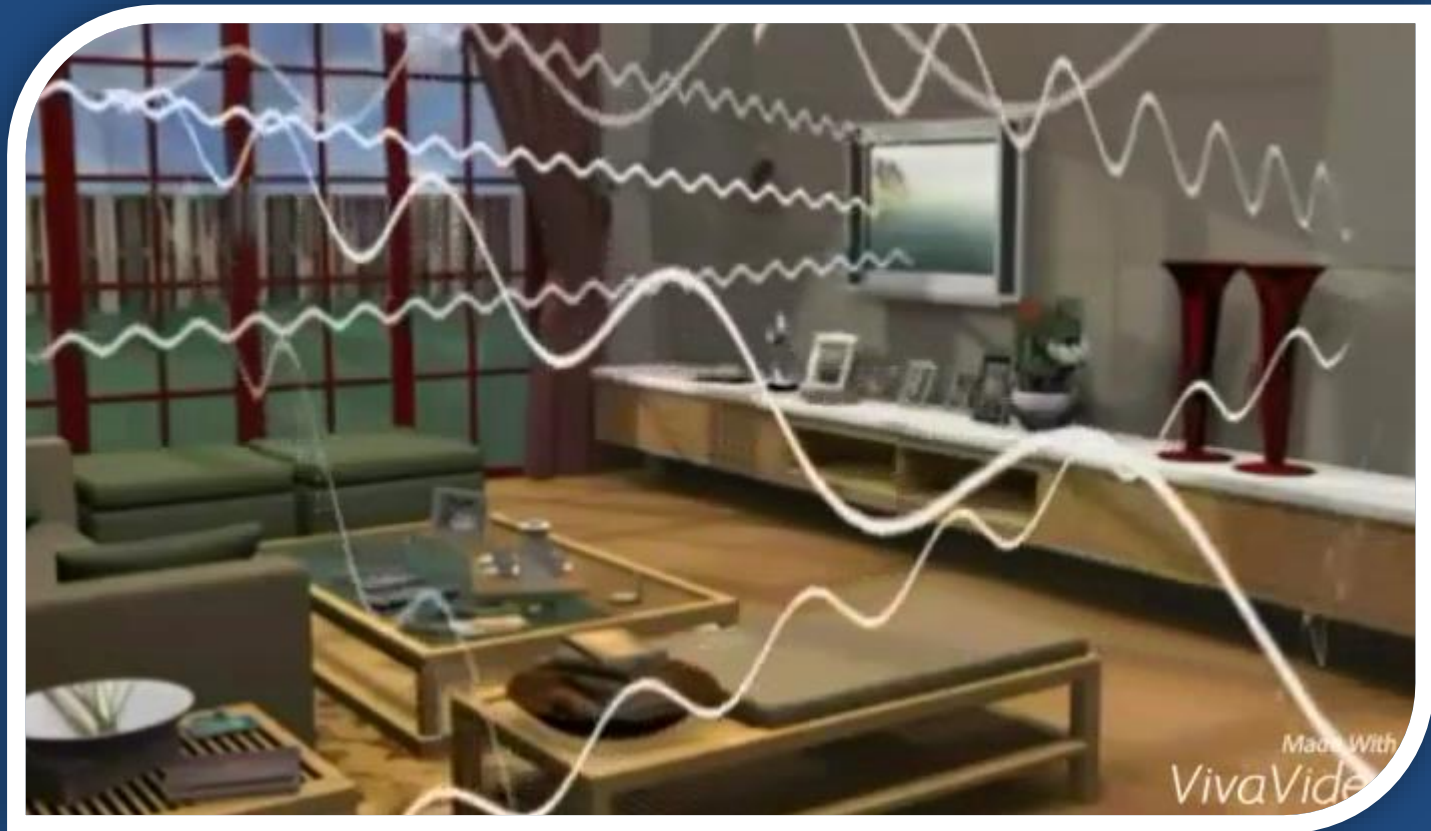
2015.10.26

cybermong@grayhash.com

주요 내용

- What is RF?
- RF Spectrum Analyzing
- **RF signal replay attack!**
- RF signal binary pattern analyzing

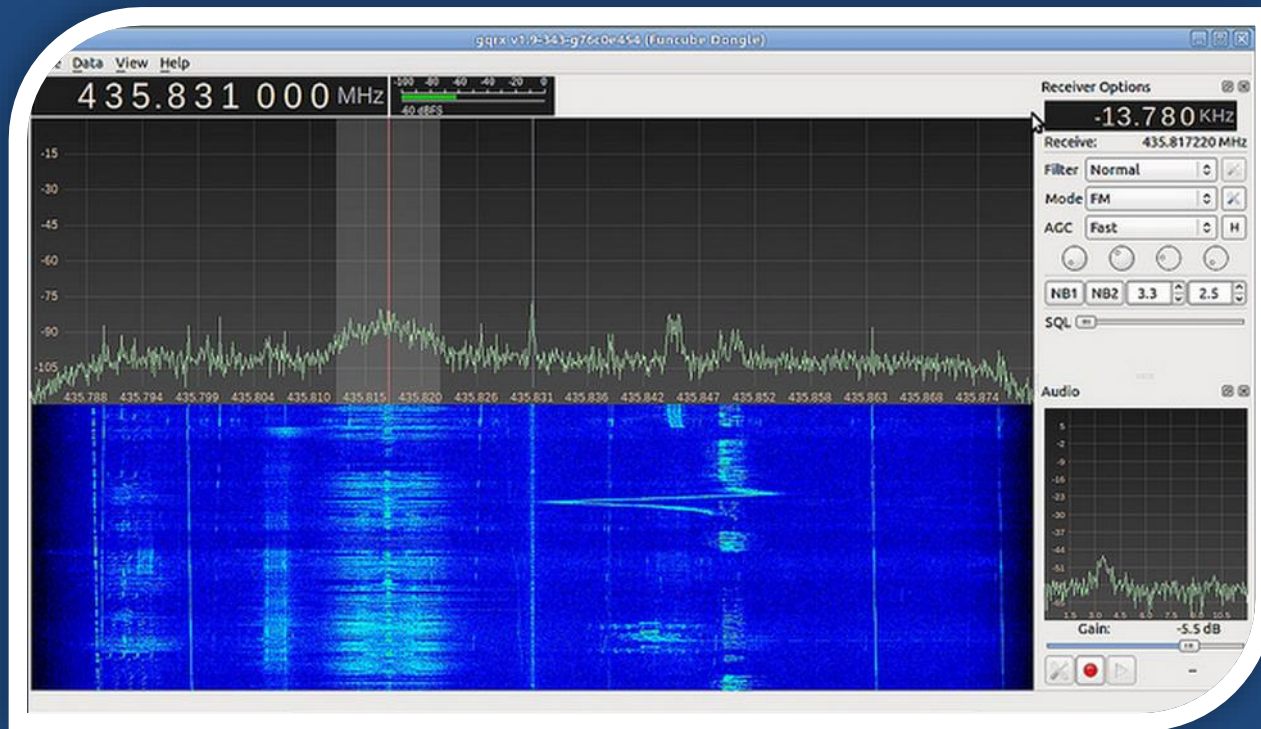
우리 주변의 무선 신호들



https://youtu.be/9WjSUpe_qfs

- WIFI, 휴대폰, 라디오, TV, GPS 등 우리 주변엔 수 많은 전자기파가 존재함

RF Spectrum Analyzing



- 관련 툴
 - GQRX
 - SDR#
 - GNU Radio
 - RF Analyzer (Android)

- 선택한 대역대의 무선 신호 강도를 Visualizing하게 보여줌

HackRF 소개

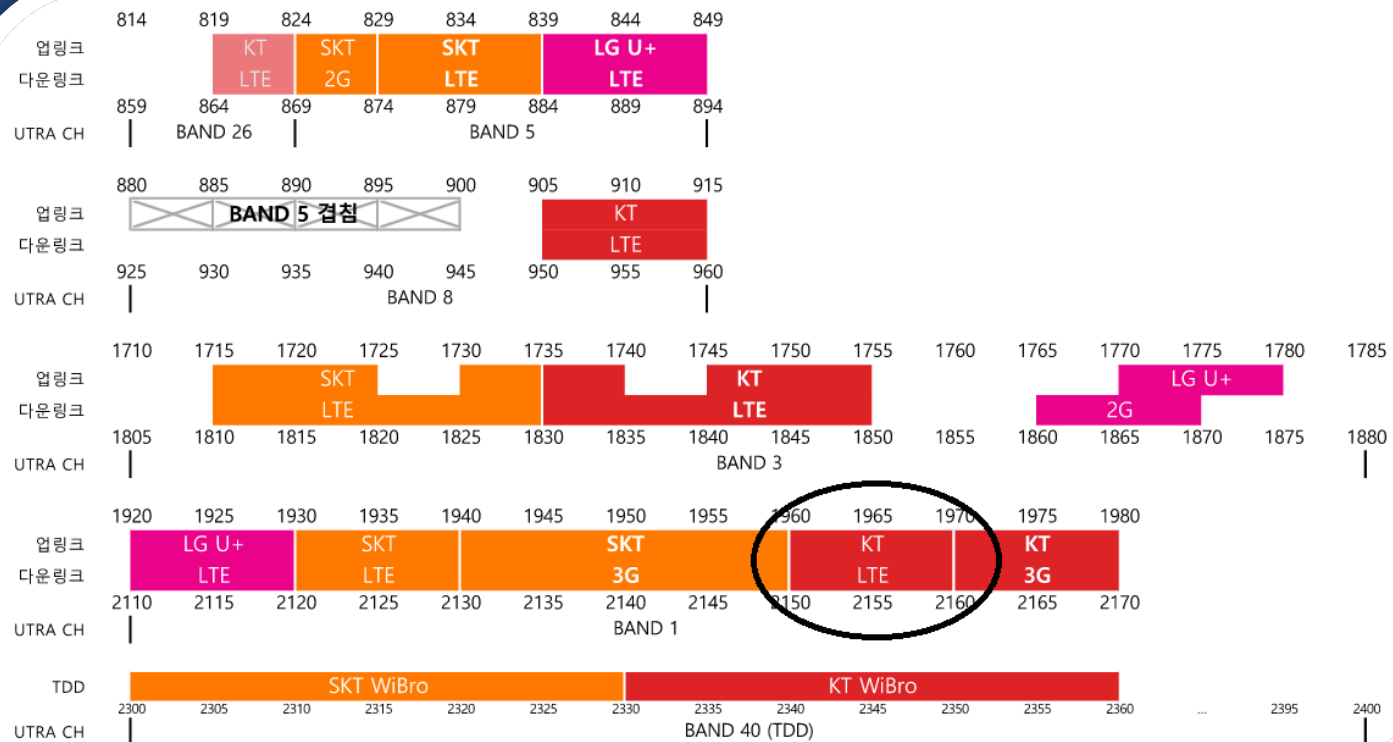


- 무선 신호 송수신 하드웨어 장비
- **1 MHz to 6 GHz** operating frequency
- **half-duplex** transceiver
- compatible with GNU Radio, SDR#, and more
- SMA female antenna connector
- Hi-Speed USB 2.0
- USB-powered
- open source hardware
- \$300
- 관련사이트
 - <https://greatscottgadgets.com/hackrf/>
 - <http://store.isource-asia.com/products/hackrf-one>
 - <https://www.kickstarter.com/projects/mossmann/hackrf-an-open-source-sdr-platform>

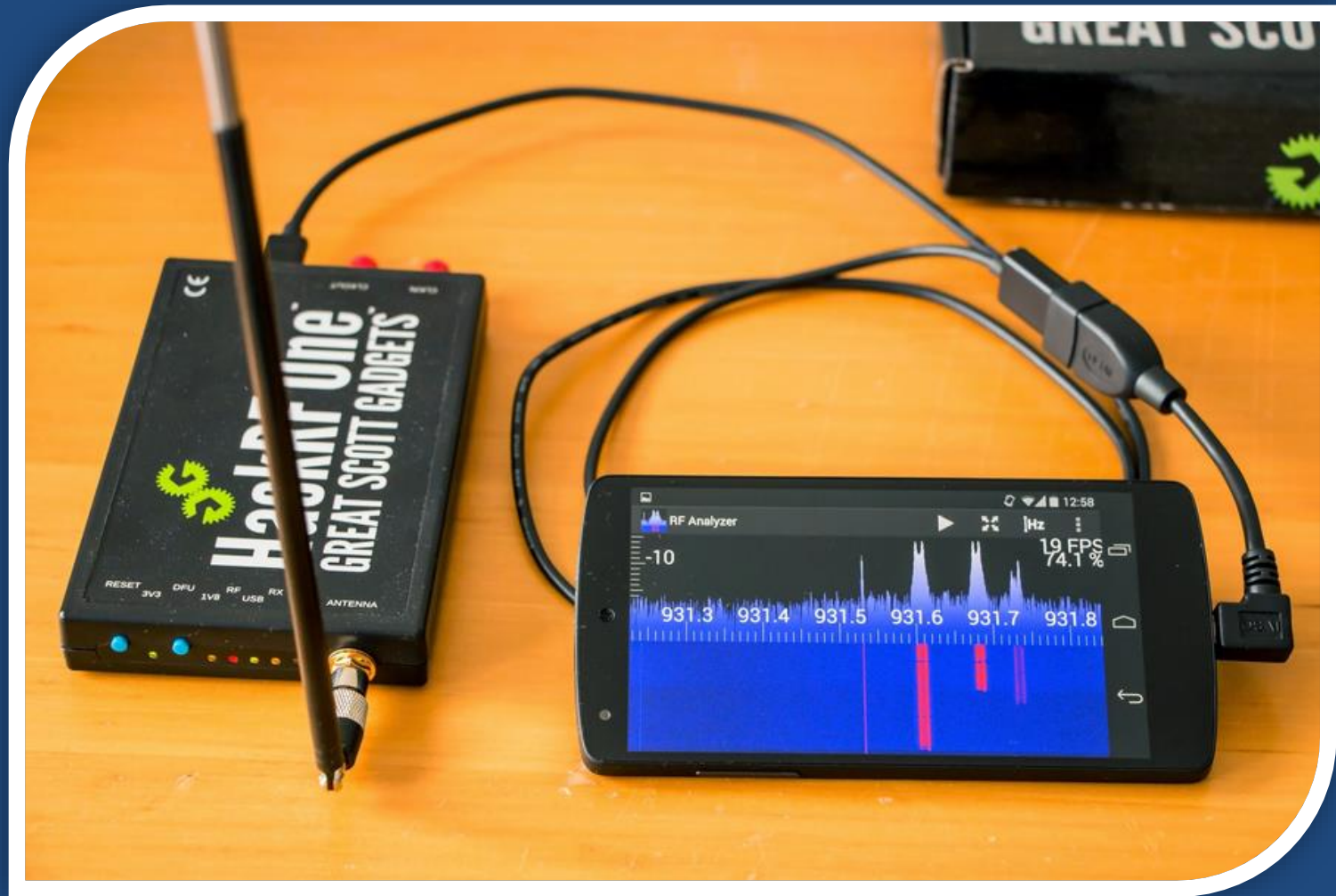
RF 스펙트럼 분석 시연

- FM 라디오 (89Mhz)
 - <https://youtu.be/w8aNrUW7JUc>
- 각종 리모컨 (315, 433, 915Mhz, 2.4Ghz)
 - <https://youtu.be/o5HqeJhzVjo>
- WIFI (2.4Ghz)
 - <https://youtu.be/49W7plgrRn0>
- 전자레인지 (2.45Ghz)
 - https://youtu.be/yu_Seu7cV74
- 휴대폰 통신 신호 (1970Mhz)
 - <https://youtu.be/NJ11KNb2Z4U>

휴대폰 통신 (예.KT-LTE)



Android RF Analyzer



무선 통신의 역사

- **에르스테드**

- 전기와 자기가 서로 연관되어 있음을 발견 (1820년)

- **마이클 패러데이**

- 자기장을 전기로 변화시킬 수 있음(전자기 유도현상)을 발견 (1831년)

- **맥스웰**

- 빛, 자기력, 전기력을 하나로 묶은 방정식 발견
- 전자기파의 존재 예언 (1873년)

- **헤르츠**

- 헤르츠 실험을 통해 전자기파의 존재와 성질을 규명 (1888년)
- 라디오 통신의 기초를 세움

- **마르코니**

- 무선전신기 발견 (1895년)
- 영국-프랑스간 무선통신 실험 성공 (1897년)
- 대서양을 건넌 무선통신 실험 성공 (1901년)

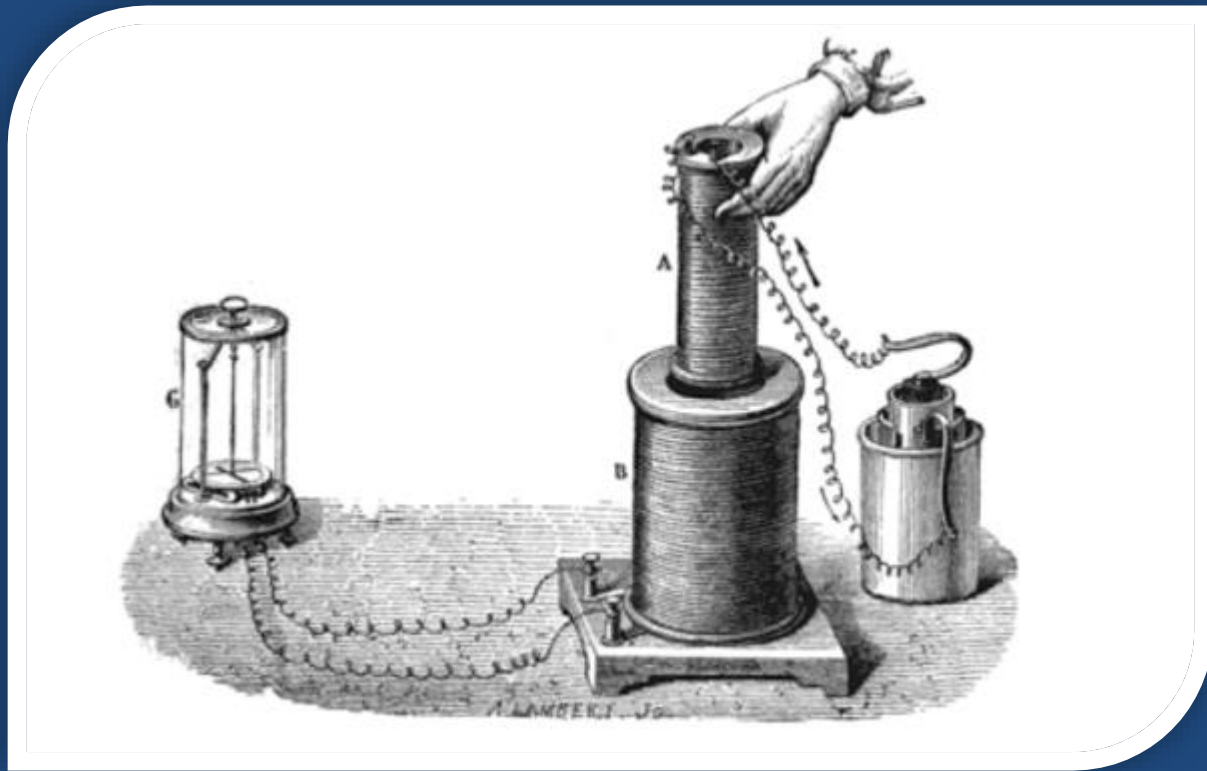
- **아인슈타인**

- 상대성 이론을 통해 전기와 자기가 왜 서로 관련이 있는지를 이론적으로 설명 (1915년)

에르스테드의 실험



패러데이의 전자기유도 실험



맥스웰 방정식

$$\begin{aligned}\vec{\nabla} \times \vec{H} &= \frac{1}{r^2 \sin \theta} \begin{vmatrix} \hat{a}_r & r \hat{a}_\theta & r \sin \theta \hat{a}_\phi \\ \frac{\partial}{\partial r} & \frac{\partial}{\partial \theta} & \frac{\partial}{\partial \phi} \\ 0 & 0 & r \sin \theta H_\phi \end{vmatrix} \\ &= 2 \frac{\hat{I} d\zeta}{4\pi} \beta_0^2 \cos \theta \left(-\frac{j}{\beta_0 r^2} + \frac{1}{\beta_0^2 r^3} \right) e^{-j\beta_0 r} \hat{a}_r \\ &\quad + \frac{\hat{I} d\zeta}{4\pi} \beta_0^2 \sin \theta \left(-\frac{j}{\beta_0 r} + \frac{j^2}{r} + \frac{1}{\beta_0^2 r^3} \right) e^{-j\beta_0 r} \hat{a}_\theta\end{aligned}$$

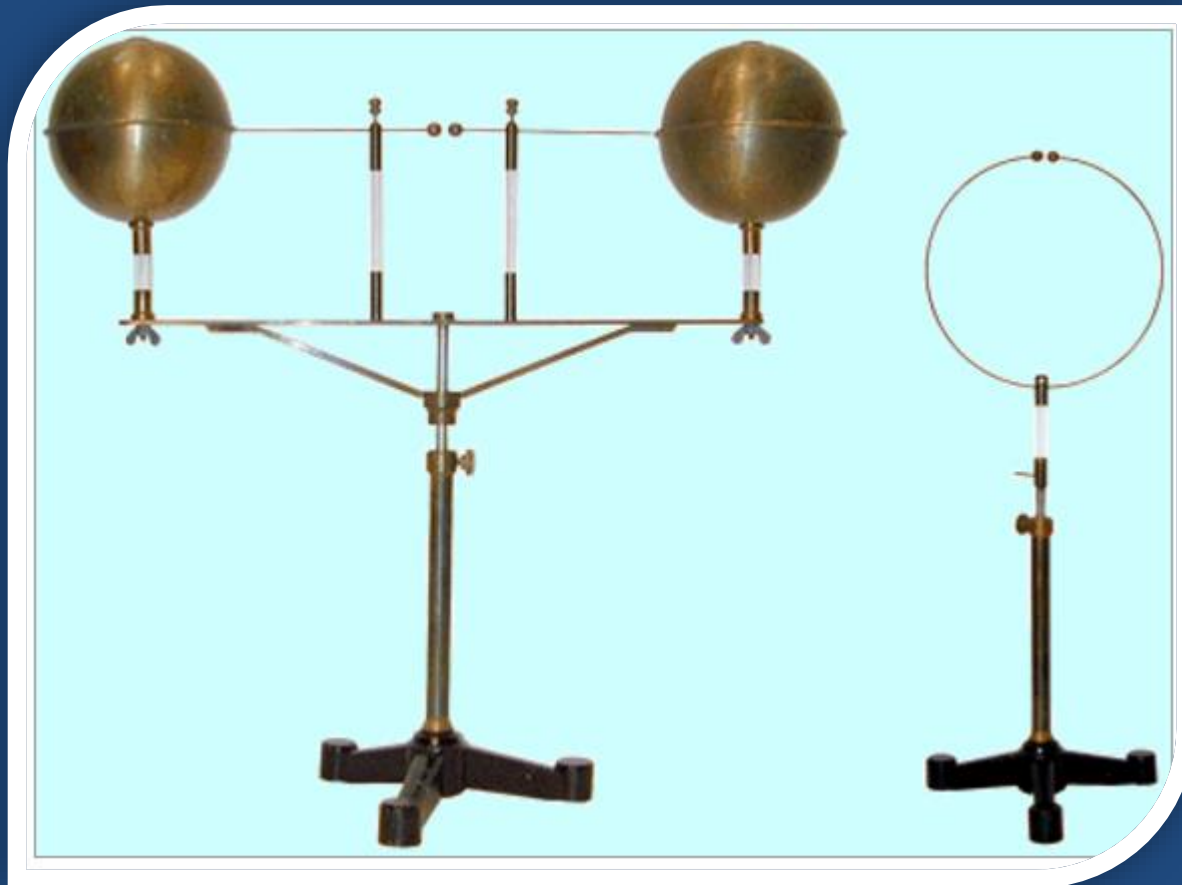
$$\begin{aligned}\vec{E} &= \frac{1}{j\omega \epsilon_0} \vec{\nabla} \times \vec{H} \\ &= 2 \frac{\hat{I} d\zeta}{4\pi} Z_0 \beta_0^2 \cos \theta \left(-\frac{1}{\beta_0^2 r^2} + \frac{1}{j \beta_0^3 r^3} \right) e^{-j\beta_0 r} \hat{a}_r \\ &\quad + \frac{\hat{I} d\zeta}{4\pi} Z_0 \beta_0^2 \sin \theta \left(-\frac{j}{\beta_0 r} + \frac{1}{\beta_0^2 r^2} + \frac{1}{j \beta_0^3 r^3} \right) e^{-j\beta_0 r} \hat{a}_\theta\end{aligned}$$

$$E_r = 2 \frac{\hat{I} d\zeta}{4\pi} Z_0 \beta_0^2 \cos \theta \left(-\frac{1}{\beta_0^2 r^2} + \frac{1}{j \beta_0^3 r^3} \right) e^{-j\beta_0 r}$$

$$E_\theta = \frac{\hat{I} d\zeta}{4\pi} Z_0 \beta_0^2 \sin \theta \left(-\frac{j}{\beta_0 r} + \frac{1}{\beta_0^2 r^2} + \frac{1}{j \beta_0^3 r^3} \right) e^{-j\beta_0 r}$$

$$E_\phi = 0$$

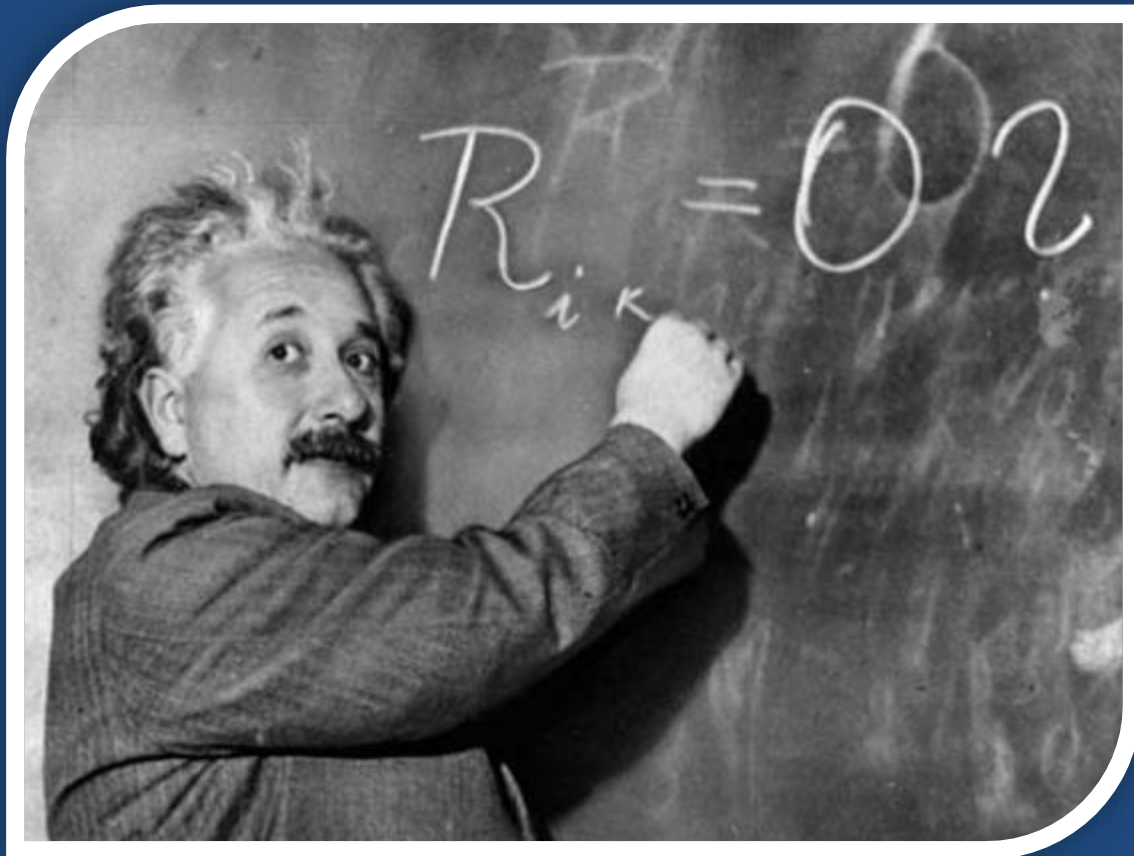
헤르츠 실험



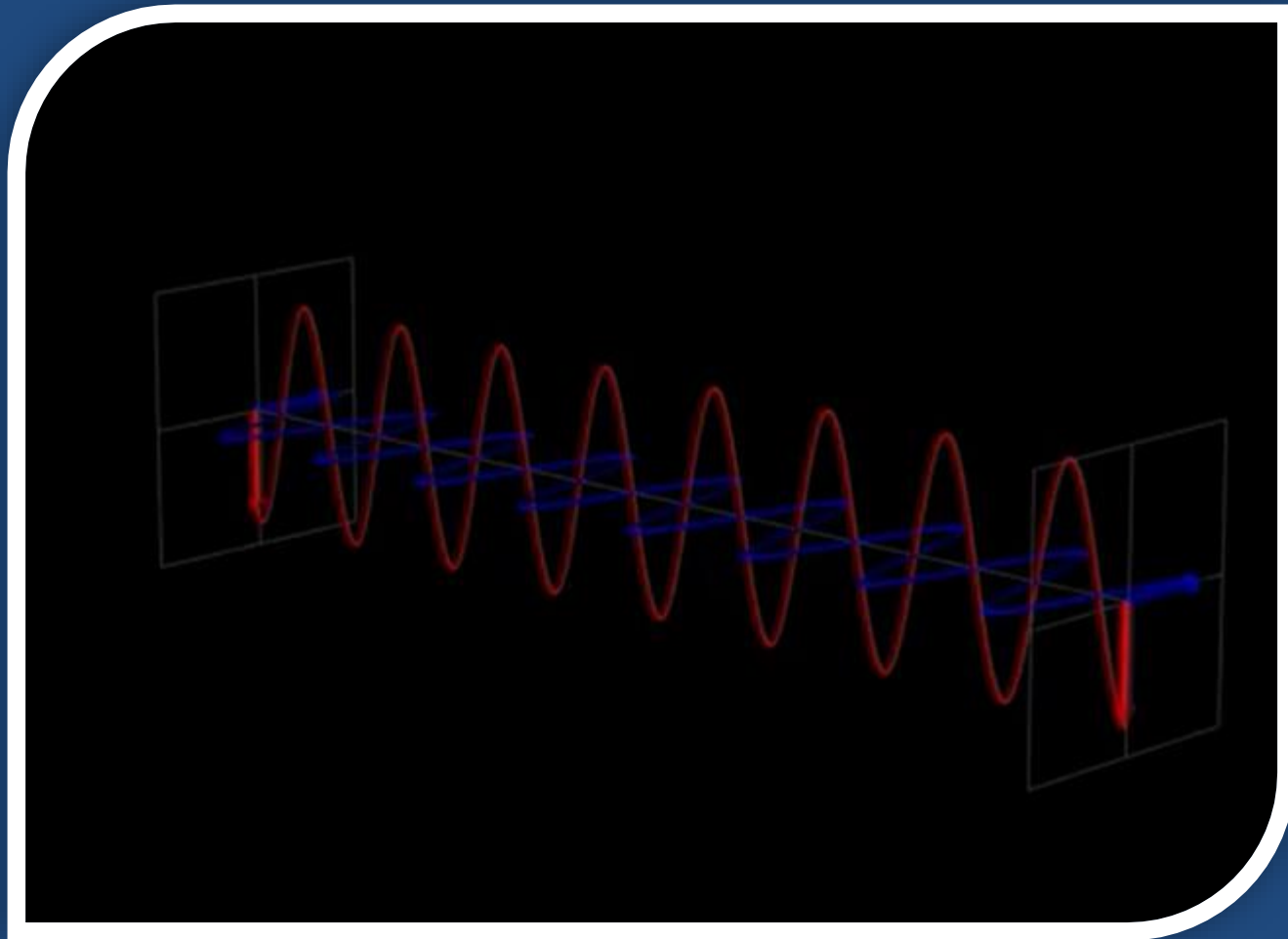
마르코니의 무선전신기



아인슈타인



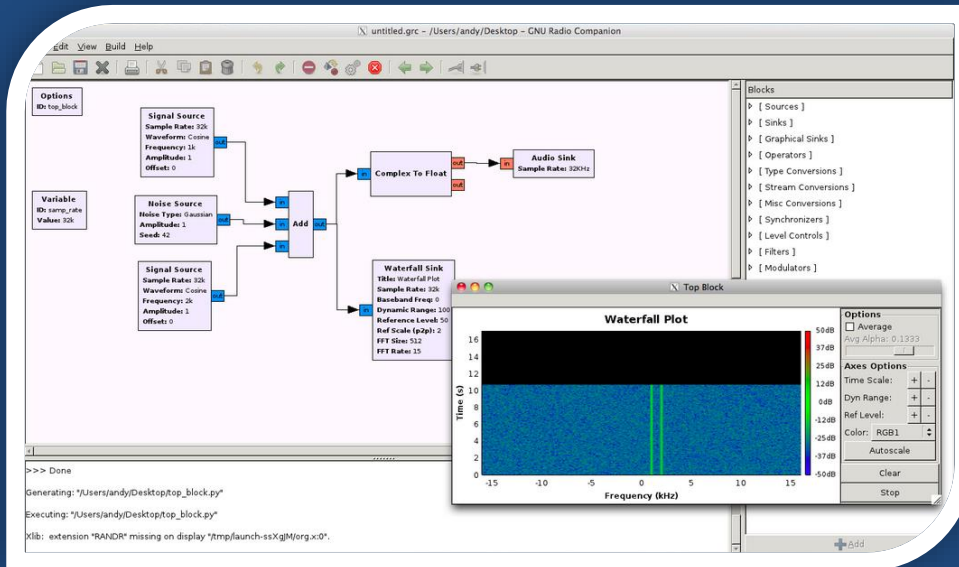
전자기파의 원리



<https://youtu.be/KlfpHLpqtIA>

RF Signal Replay Attack

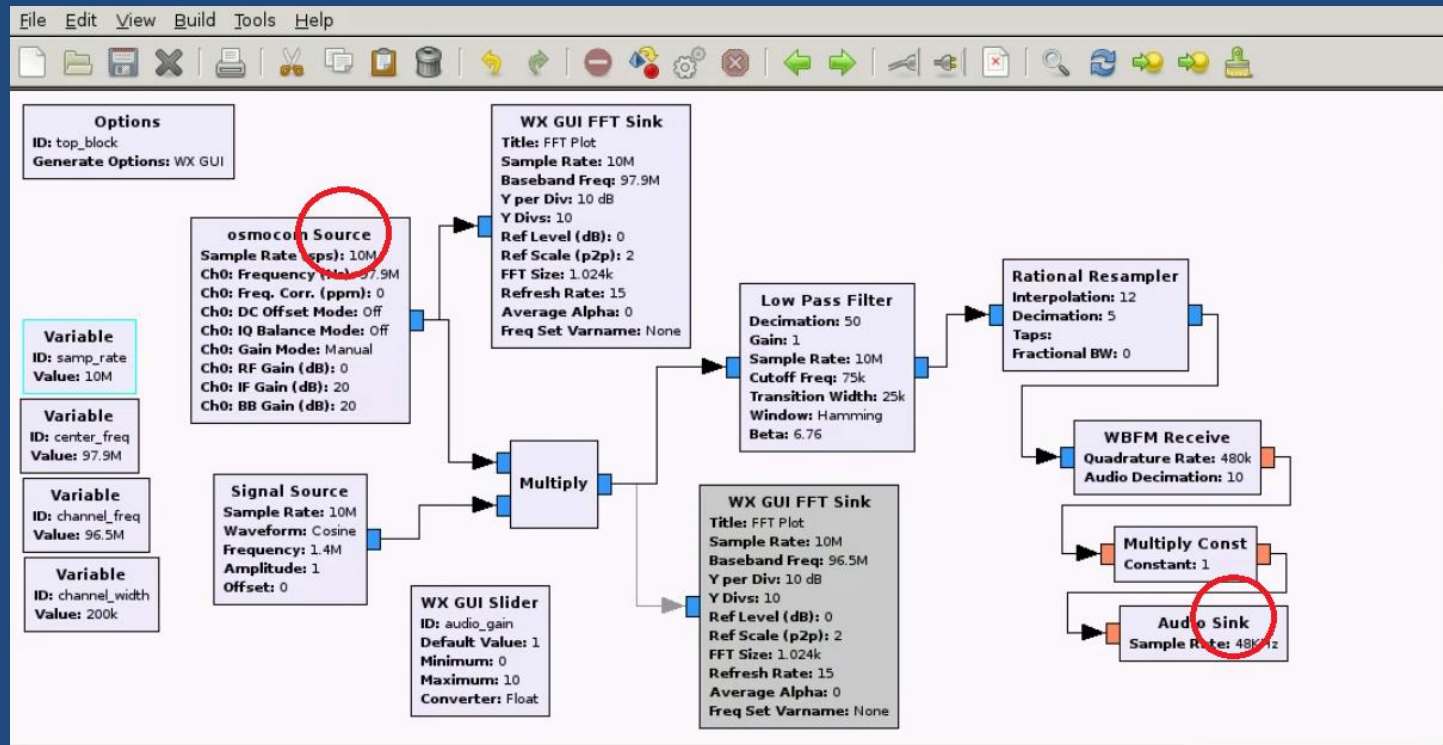
GNU Radio 소개



- 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/>

GNU Radio 사용 방법

- Block의 이해 : 다양한 기능들을 Block이라는 모듈 단위로 제공
- Source와 Sink의 이해 : Source = 데이터의 근원지, Sink = 목적지
- Osmocom의 이해 : HackRF가 사용하는 Device Driver



Pentoo Linux 소개

- 무선 해킹에 최적화된 Linux 배포본

```
* driver = snd-ens1371...
* VideoCard: nVidia Corporation|NV18DDR [GeForce 256 DDR]... [ ok ]
* Starting Bluetooth... [ ok ]
*   Starting hcid... [ ok ]
*   Starting sdpd... [ ok ]
*   Starting rfcomm... [ ok ]
* Starting portmap... [ ok ]
* Starting famd... [ ok ]
* Mounting network filesystems... [ ok ]
* Starting local... [ ok ]
* Setting Console frame buffer images... [ ok ]

Last login: Thu Feb 17 23:49:33 on vc/2

This is pentoo livecd by Michael Zanetta (mzanetta@pentoo.ch)

      .a$bb
    ..a$bb..  .ca$b..  .a$b..  a$bb$a$bb$a$bb..  .a$b..  .a$b..
  .a$bb$a$bb..  a$bb(a$bb..  a$bb$a$bb..  Q$bb$a$bb..  a$bb..  a$bb..
  $$$$ ( )$$$a$bb$a$bbP"  a$bbQ$bb..  $$$..  $$$P' 999 9$P' $$$
  .a$bb$a$bbP Q$bb$a$bb..  a$bbP Q$bb..  $$$..  $$$..  a$bb..a$bb..
  a$bb$a$bbP' "a$bb$a$bb Q$bb Q$bb $$$ Q$bb$a$bbP' Q$bb$a$bbP
  $$$P'          """""""" """" """" Q$bbP ""Q$bbP"" ""Q$bbP""
  "Q$bbP"

Welcome to Pentoo on Gentoo linux...

First type ifconfig -a to see if your network card has been detected.
You can type net-setup eth0 to setup your network interface.

You are jailed in the root user so no need to try sudo or su.

If you are connected to the internet and have loaded the nessus plugins in ram or on
the usb stick, just type nessus-update-plugins to have the up-to-date -7 days plugins.

pentoo root # █
```

Pentoo LiveCD
powered by gentoo™

Mac + HackRF

1. Xquartz(X11) 설치.

- <http://xquartz.macosforge.org/landing/>

2. MACPORTS 설치.

- <https://guide.macports.org/chunked/installing.shell.html>

3. 터미널 작업.

- > `sudo port self`
- > `xcode-select --install`
- > `sudo port install gnuradio`
- > `sudo port install gr-osmosdr`

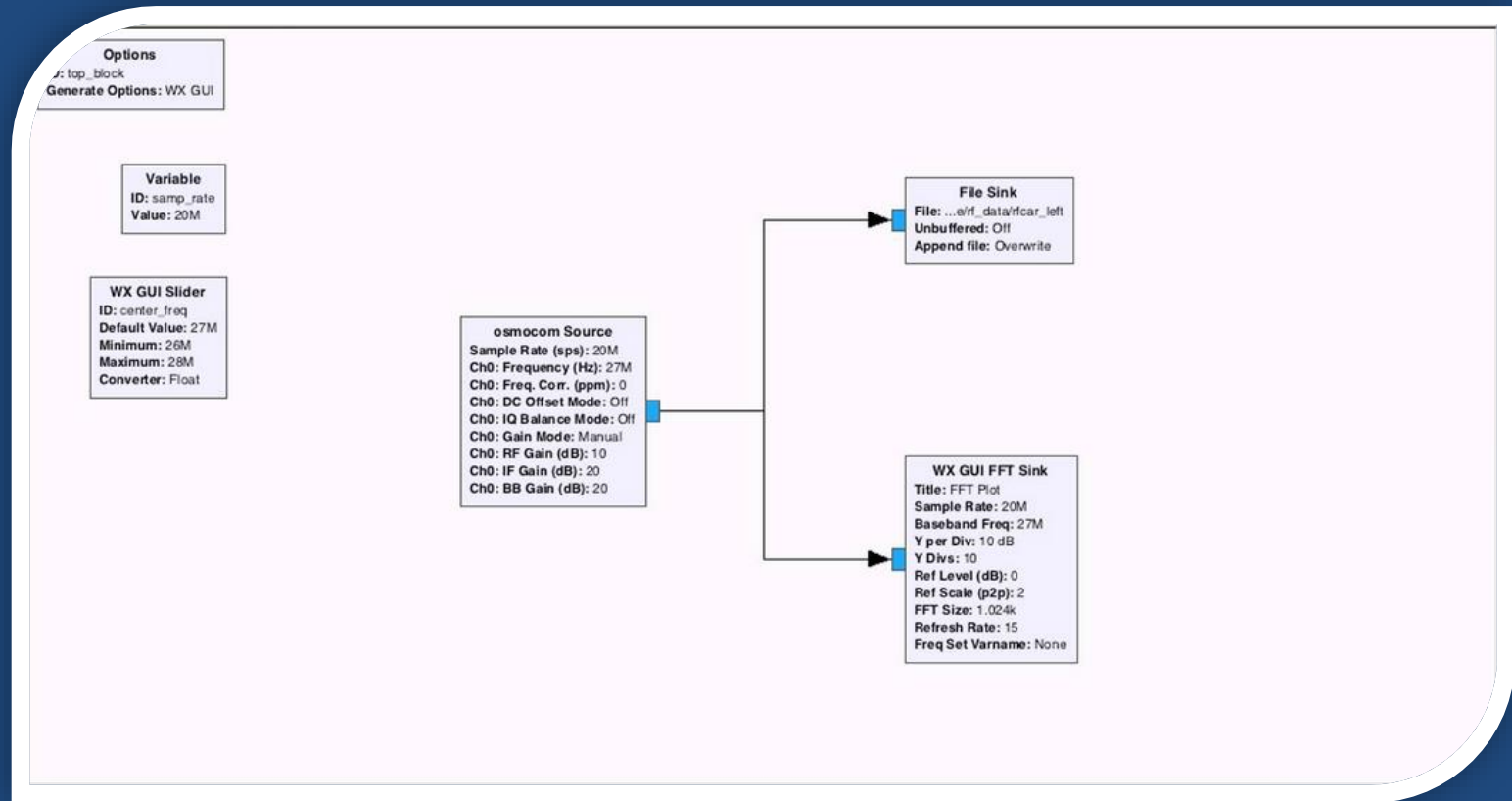
// 바탕화면에 바로가기 생성.

- `ln -s /opt/local/bin/gnuradio-companion ~/Desktop/`

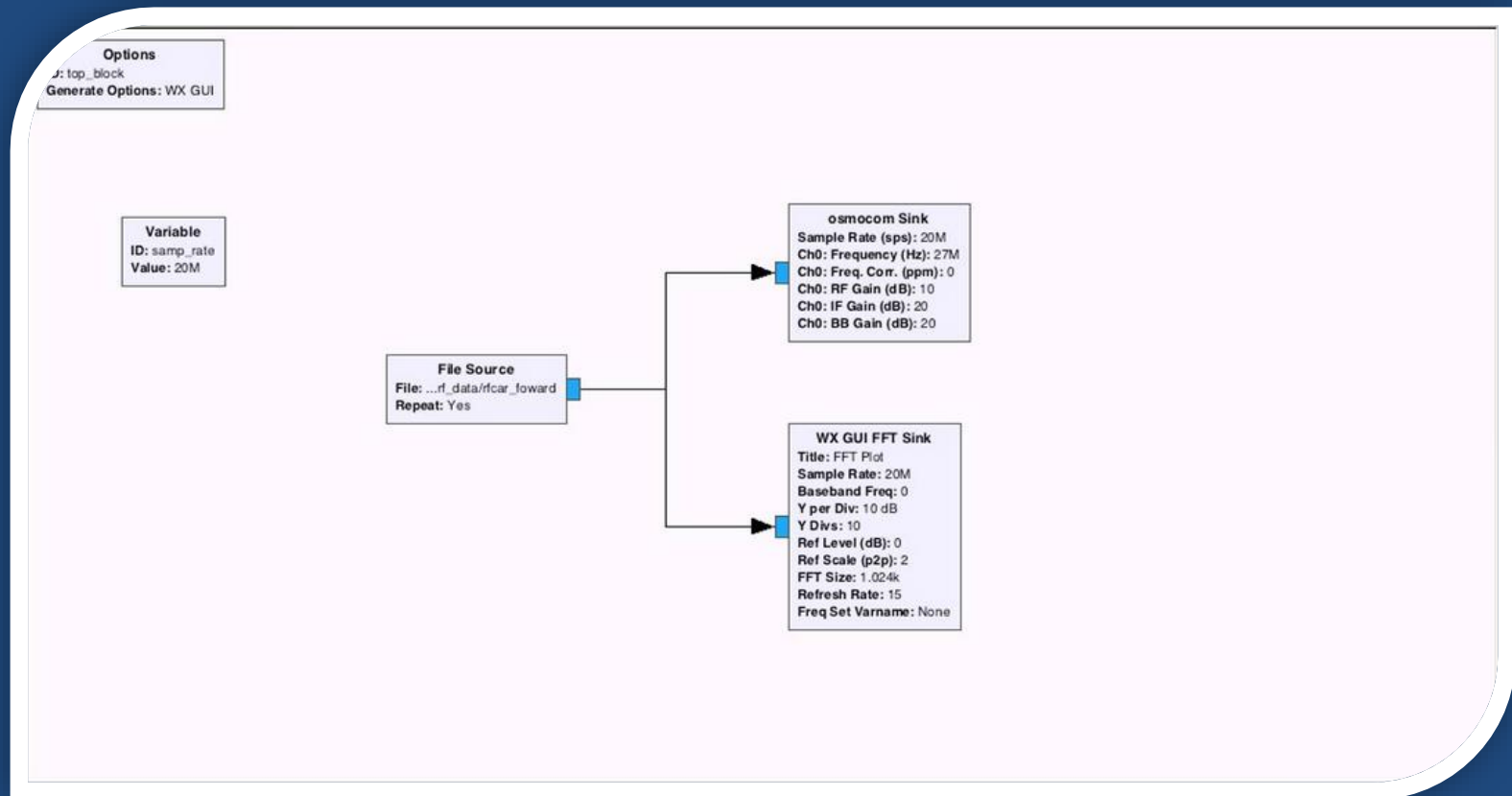
RF 신호 replay attack

- GNU Radio를 이용한 무선신호 Recording
 - RF signal Source -> File Sink
- Recording 된 신호 재생
 - File Source 선택
 - Osmocom Sink로 출력

RF 신호 Record



RF 신호 Replay



Replay Attack 시연

- RC카
- 자동차 리모컨
- 차량 차단기
- 드론
- 도어락

RF카 무선 해킹 시연



주파수 대역 알아내기

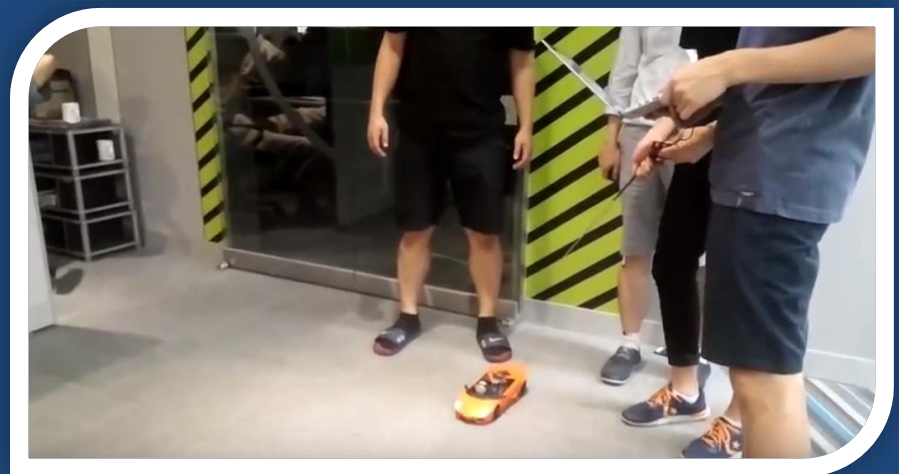


RF카 무선해킹 시연 영상



<https://youtu.be/M1YYRAGeuRE>

<https://youtu.be/rC3cKMXD7VQ>



자동차 리모컨 무선 해킹 시연



RF 주파수(Frequency)

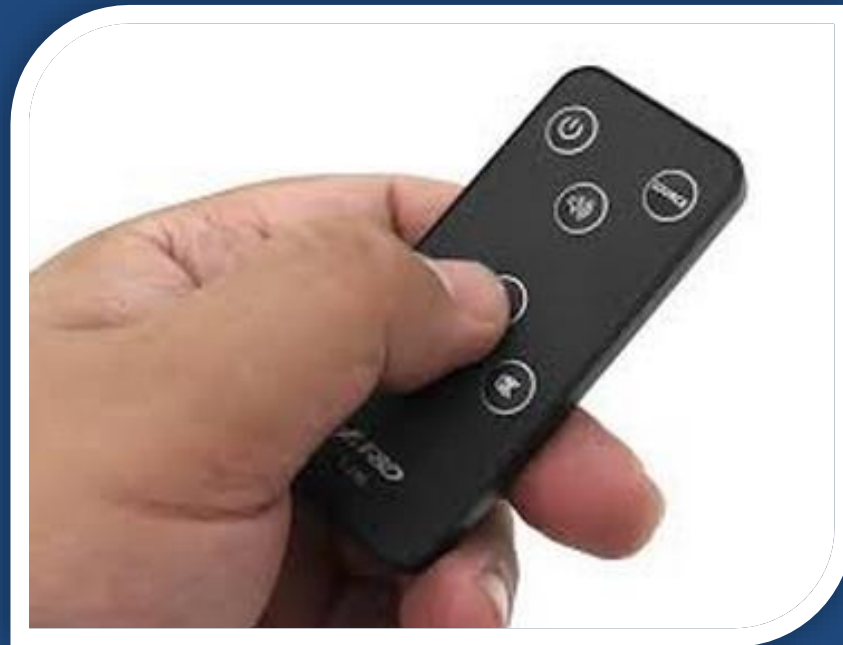
무서운 전파법

- 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]

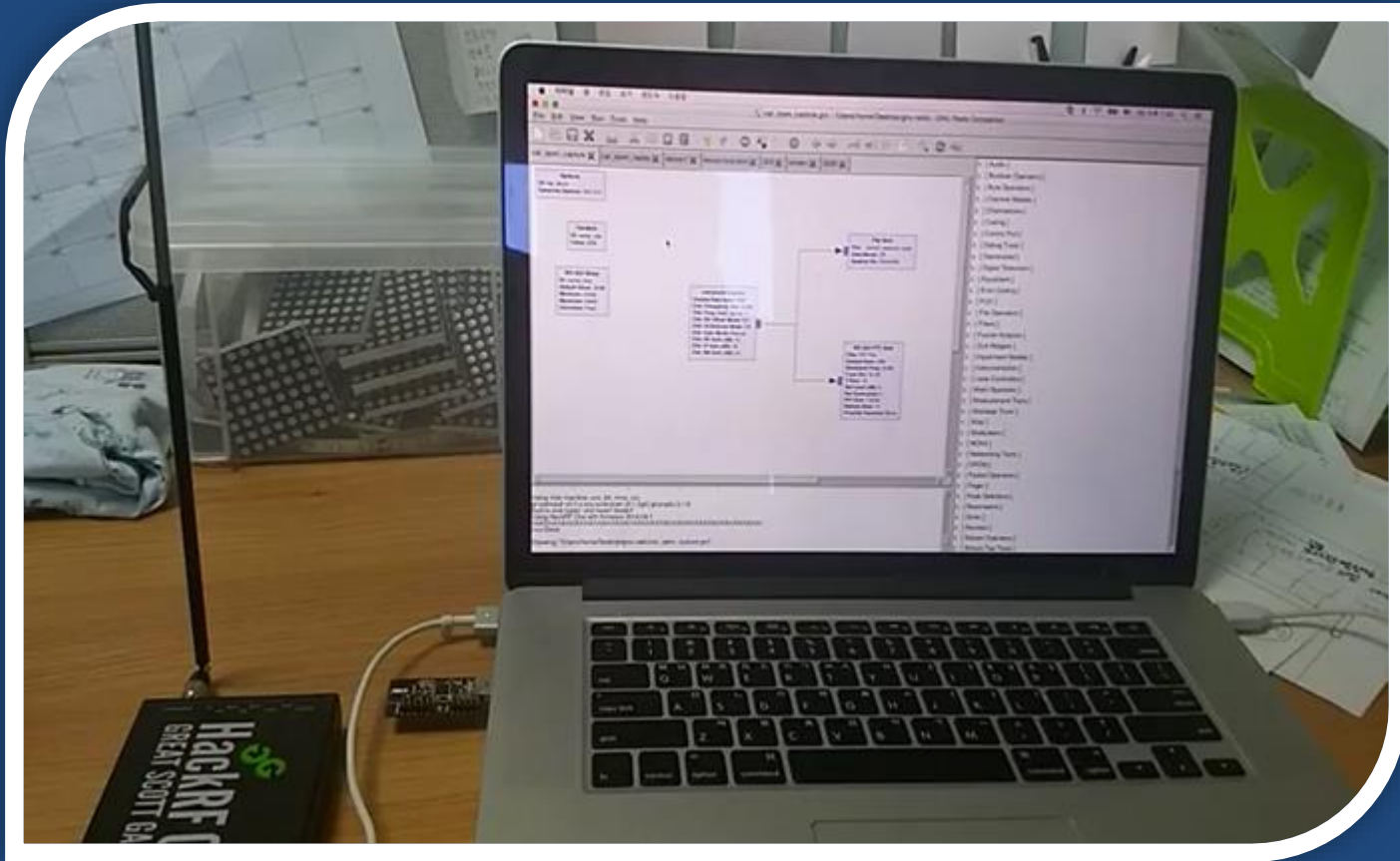
Frequency range		Bandwidth	Center frequency	Availability	Licensed users
6.765 MHz	6.795 MHz	30 kHz	6.780 MHz	Subject to local acceptance	Fixed & Mobile services
13.553 MHz	13.567 MHz	14 kHz	13.560 MHz	Worldwide	Fixed & Mobile services
26.957 MHz	27.283 MHz	326 kHz	27.120 MHz	Worldwide	Citizens band radio ^[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

주파수 대역 알아내기



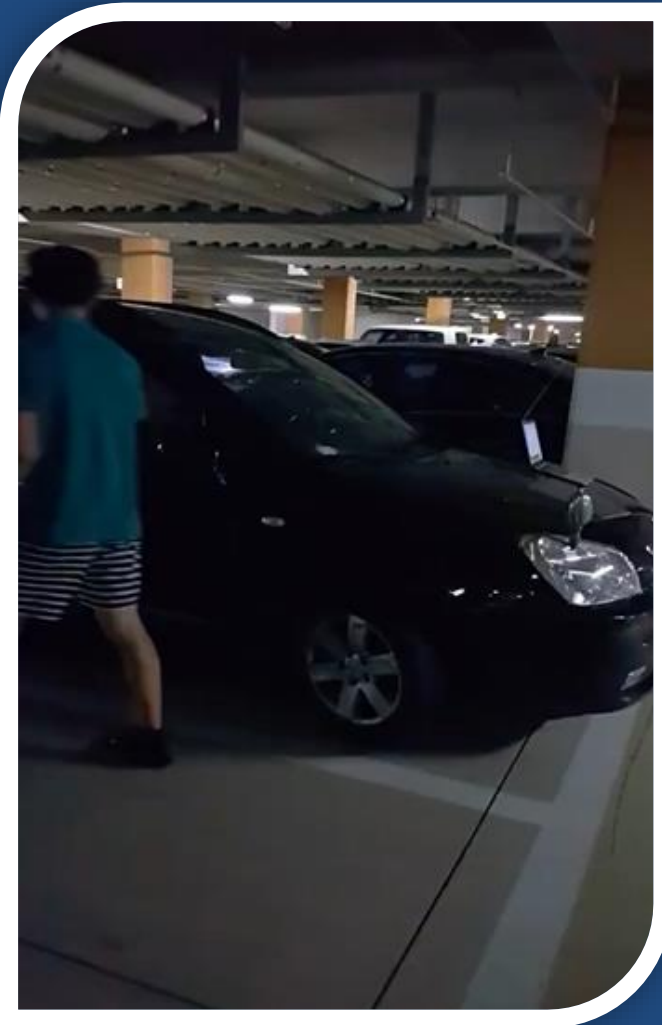
<https://youtu.be/H6wHU1Fo5QQ>

무선 신호 캡처하기



<https://youtu.be/u9T4-Bzlxxk>

열려라 참깨!

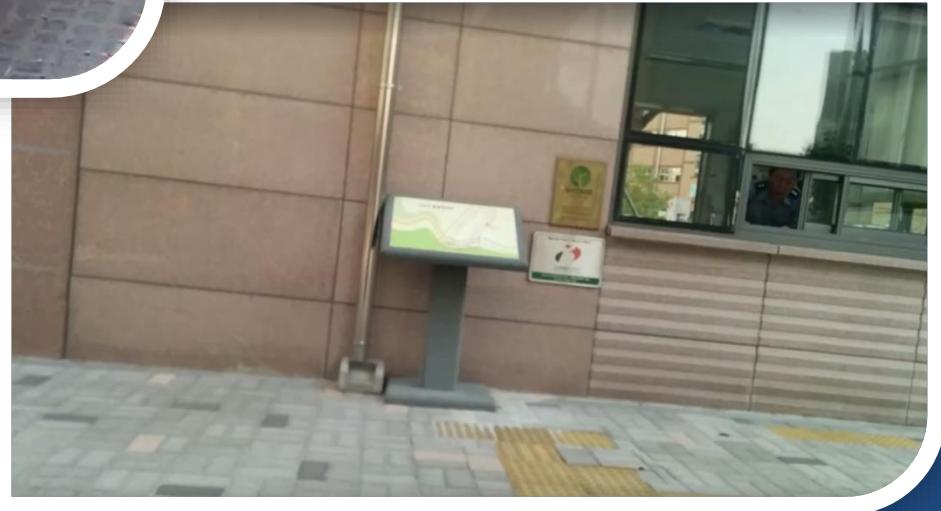
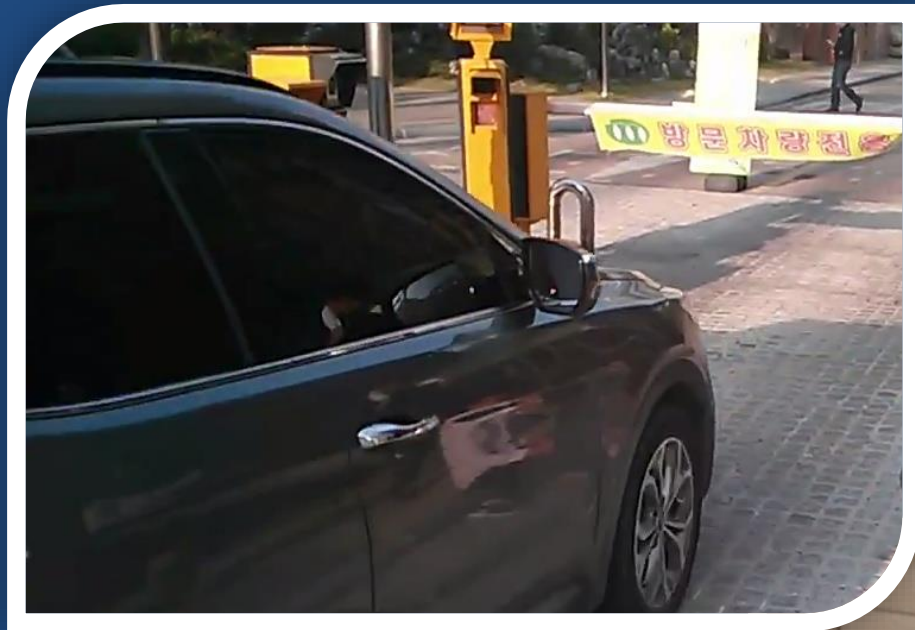


<https://youtu.be/i6-yqsW2mKc>

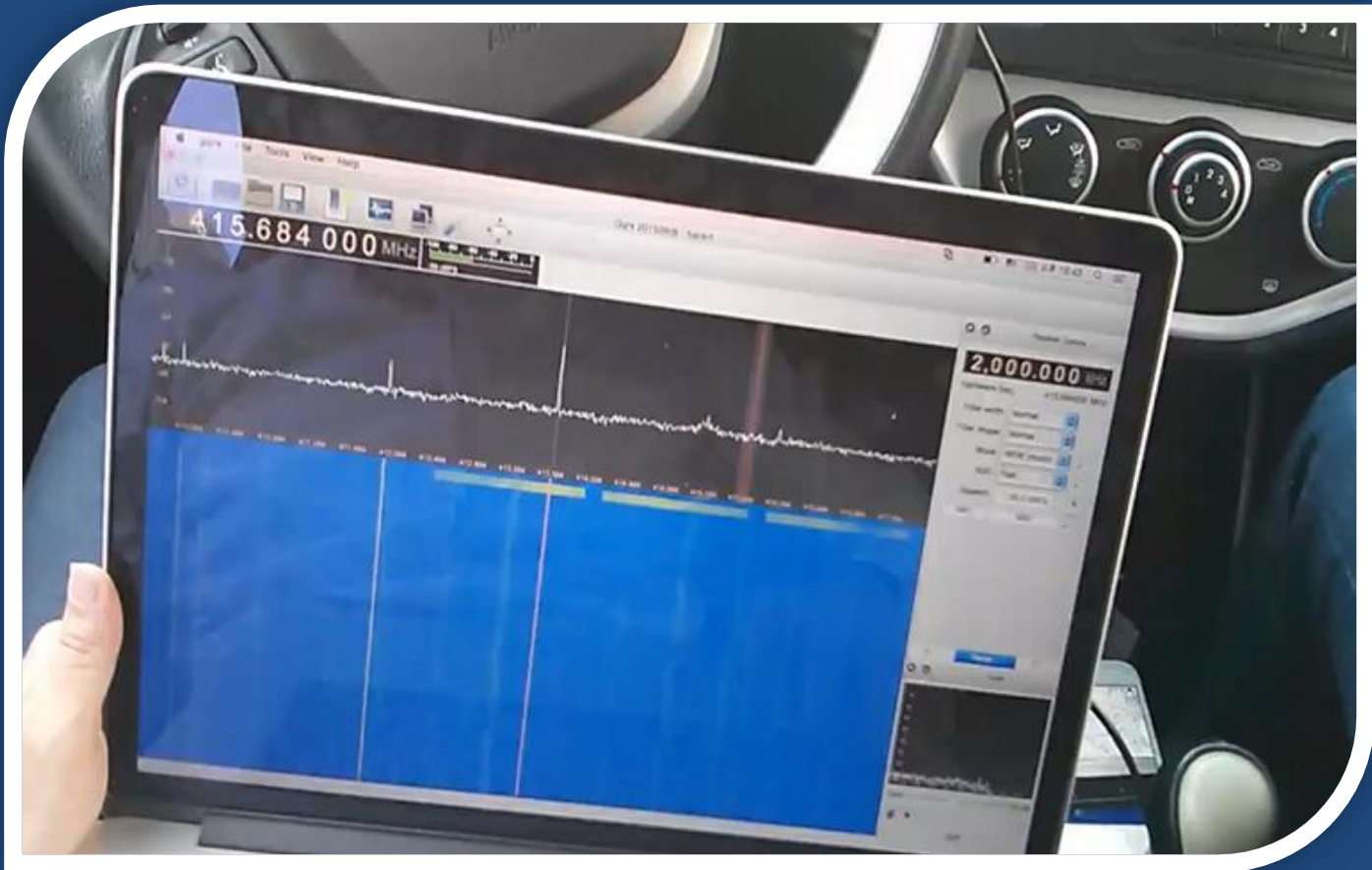
차량 차단기 무선 해킹 시연



It works with RF too!



RF 주파수 알아내기



<https://youtu.be/MxHvFyShFuM>

1~3차 시도

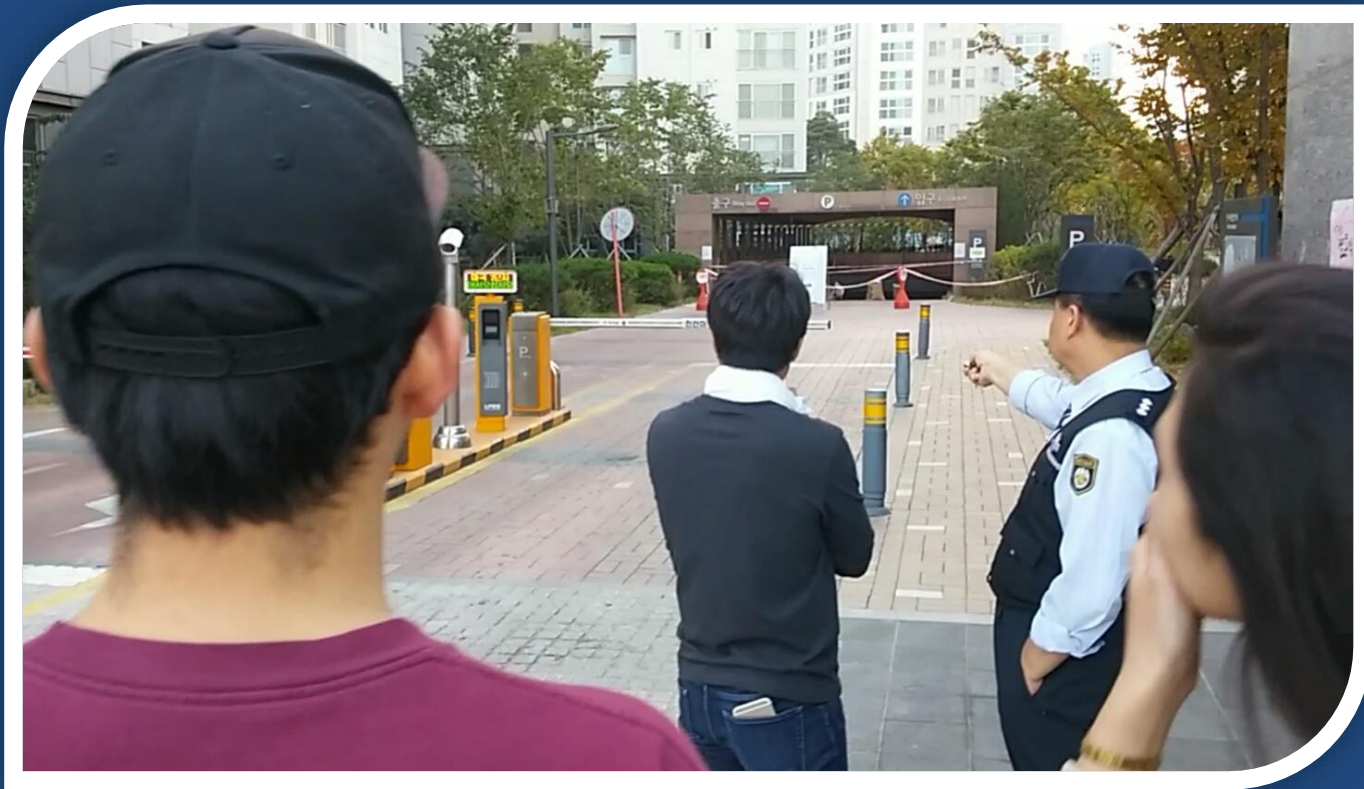
- 1차 시도 – 실패..
 - https://youtu.be/QdE_3Kh6f_4
- 2차 시도 – 실패..
 - <https://youtu.be/XNDQWUahdfE>
- 3차 시도 – 실패 + Ban.. OTL
 - <https://youtu.be/CYLe2wf1O8A>

경비아저씨는 우리편!

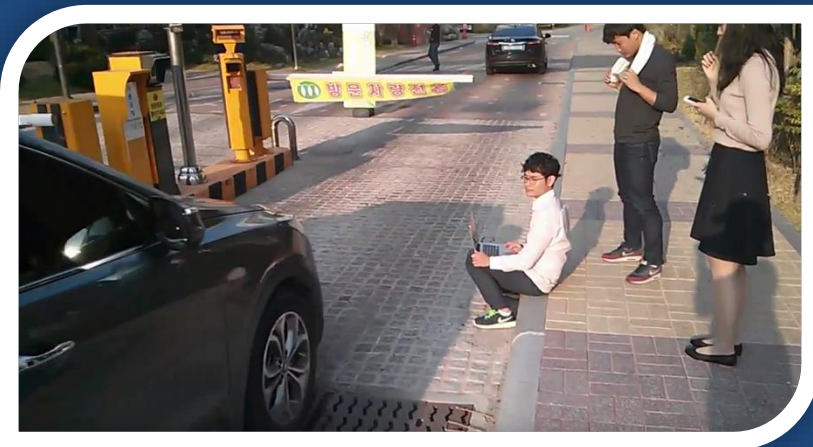
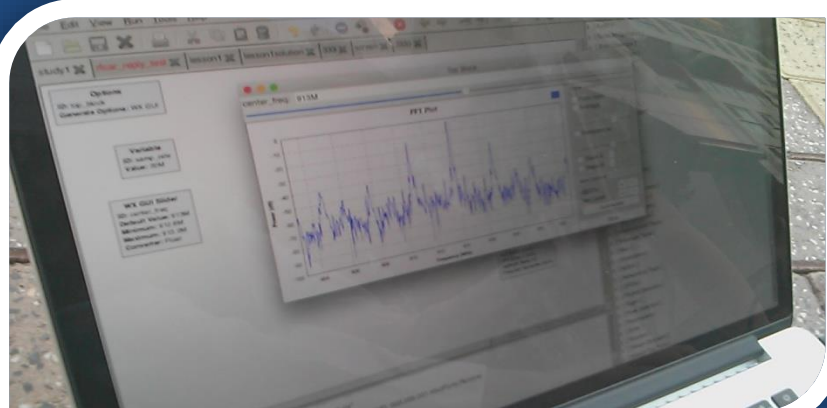


<https://youtu.be/V3v-OnJmXms>

경비아저씨는 우리편!



삽질.. 또 삽질..



성공!!

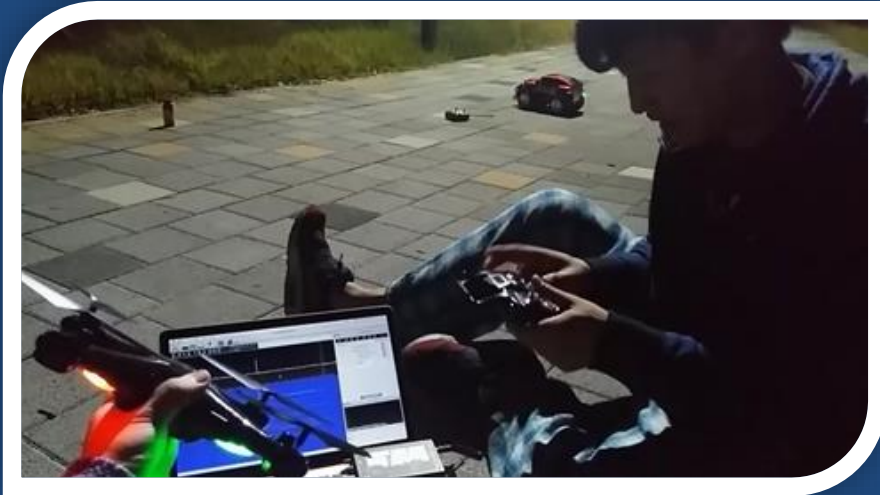


<https://youtu.be/xT5masLZ2el>

Drone 무선 해킹 시연

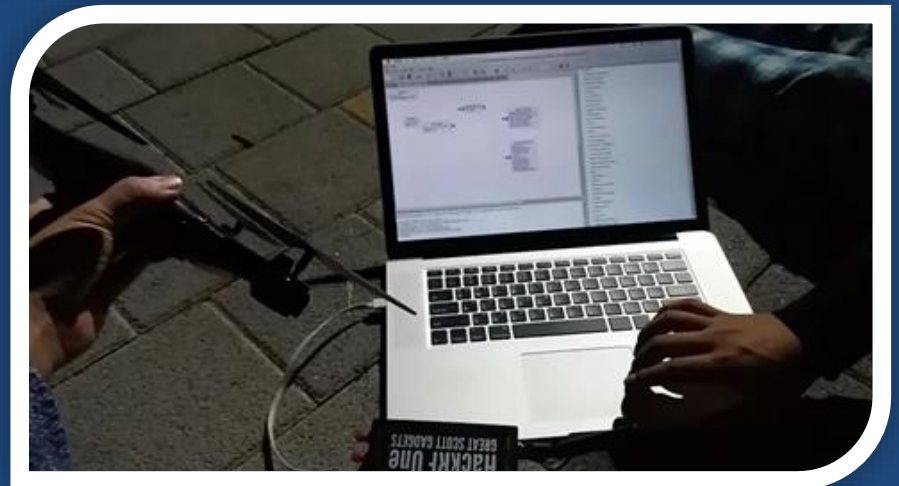


드론 주파수 알아내기

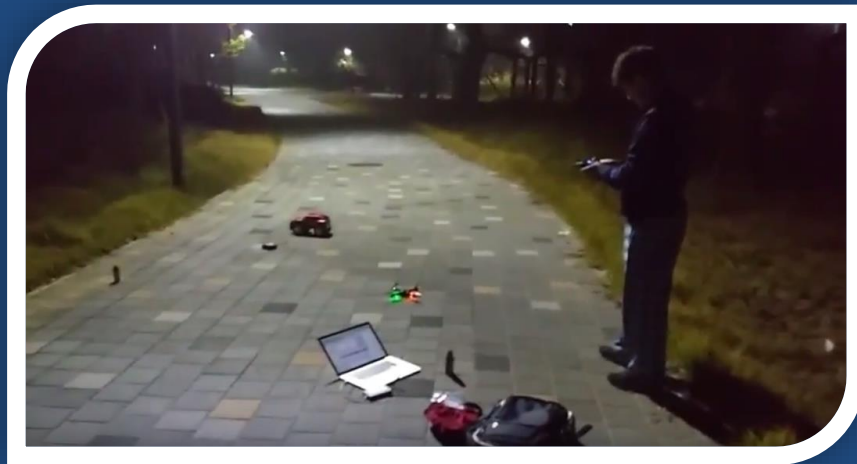


<https://youtu.be/Er5gdhGf9RA>

<https://youtu.be/1rwOkiUx1WI>

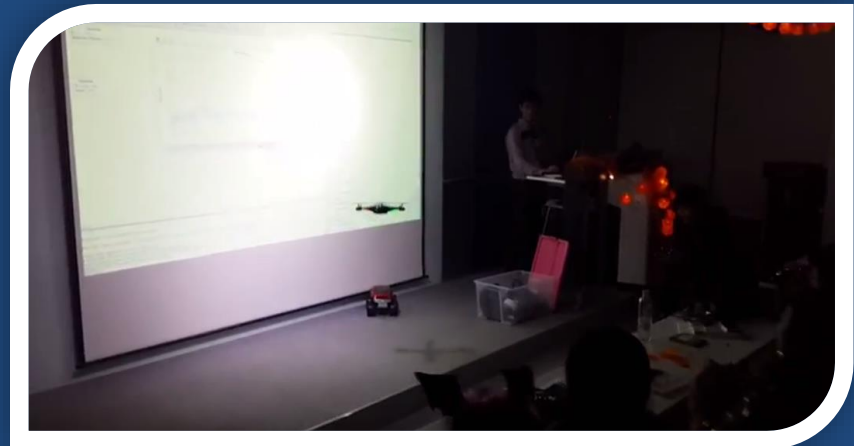


드론 무선해킹 시연 영상

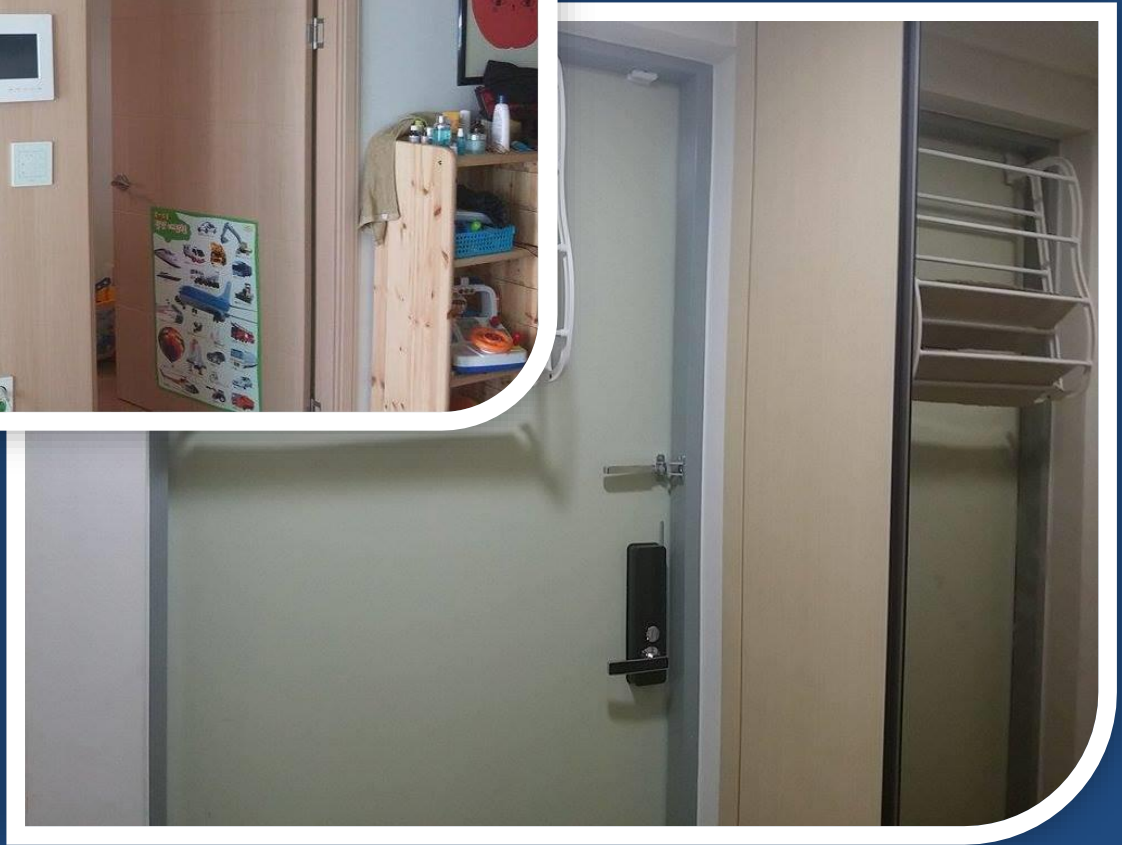
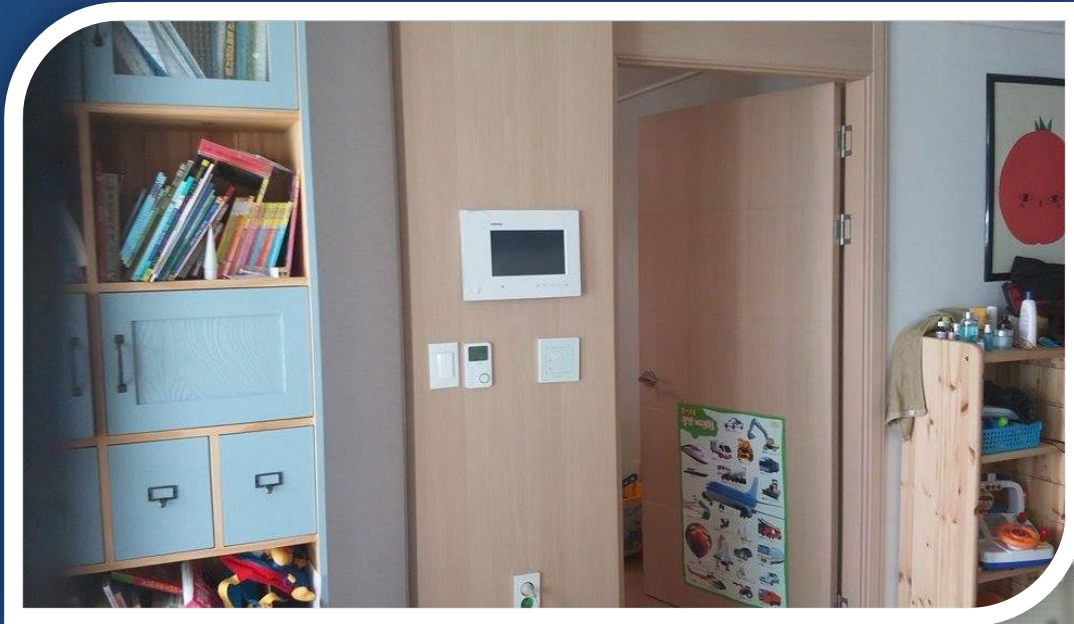


<https://youtu.be/u4BsxkilgIE>

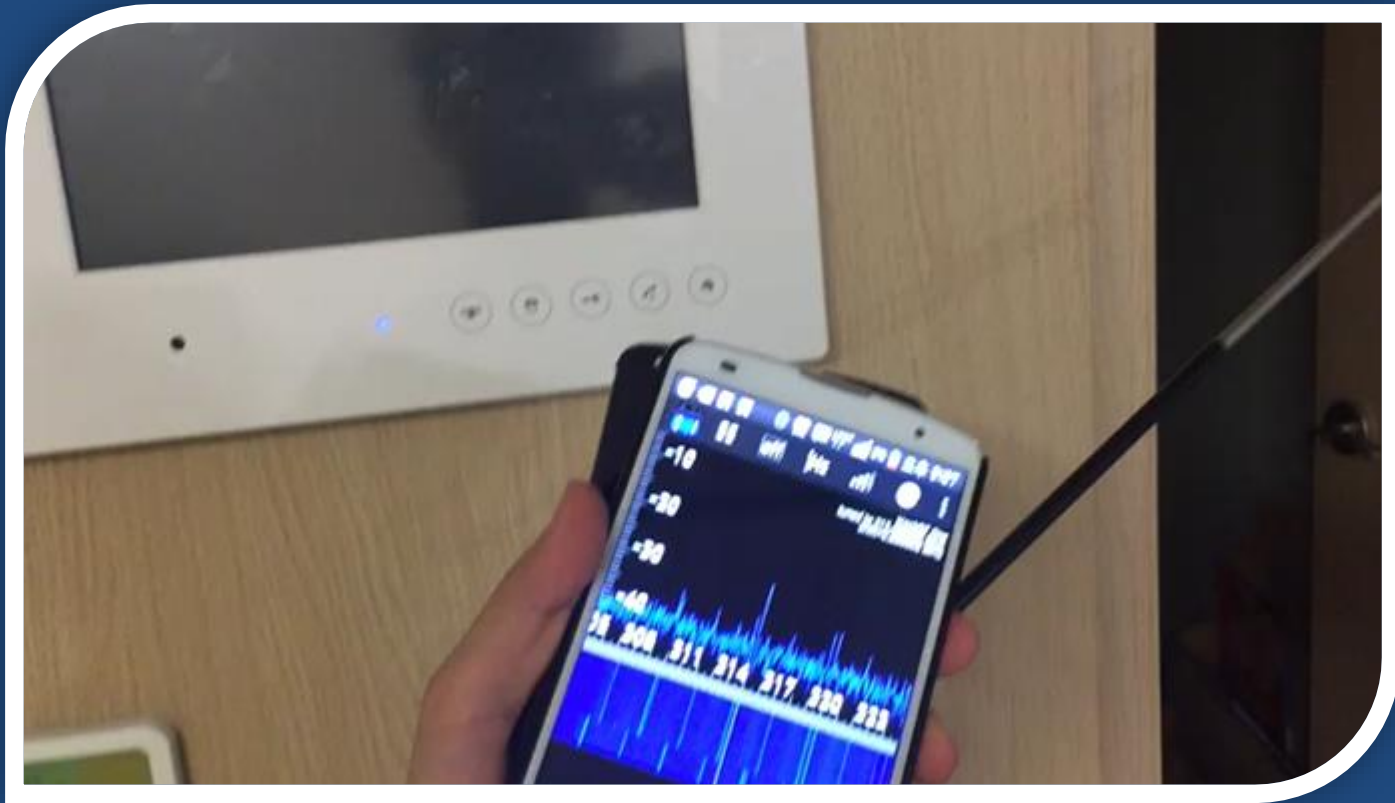
<https://youtu.be/1nE0TrR9AjA>



도어락 무선 해킹 시연

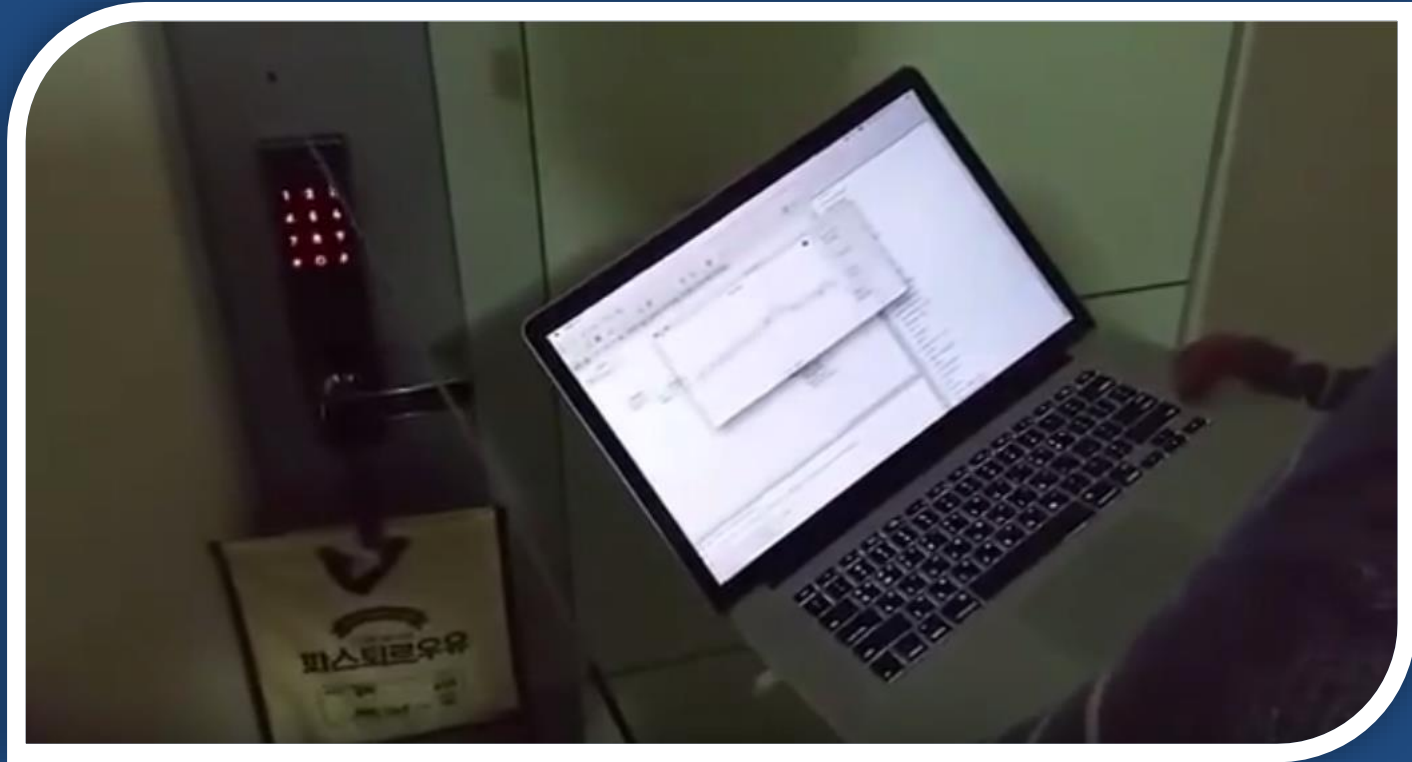


도어락 주파수 알아내기



<https://youtu.be/4NW5m3PHCTg>

열려라 참깨!!



<https://youtu.be/zfoUI6Z5RBo>

RF 주파수 알아내기 팁



RF 주파수 알아내기 팁

EQUIPMENT 주/차/관/제/설/비

- ▶ 주차설비제안
- ▶ LPR시스템
- ▶ RF시스템
- ▶ 리모콘시스템
- ▶ 시스템 비교
- ▶ 제품소개

리모콘시스템 REMOTE SYSTEM



설치비 절감과 관리 효율성 실현

.. 리모콘을 이용한 출입차량 제어

- ▶ 고정 이용객의 출입 편리성 확보
- ▶ 경제적인 설치 비용(설치비 가장 저렴)
- ▶ 개별 리모콘 코드 관리
- ▶ 모든 출입차량의 이용 자료 검색 기능
- ▶ 고정차량의 무정차 실현



송신기

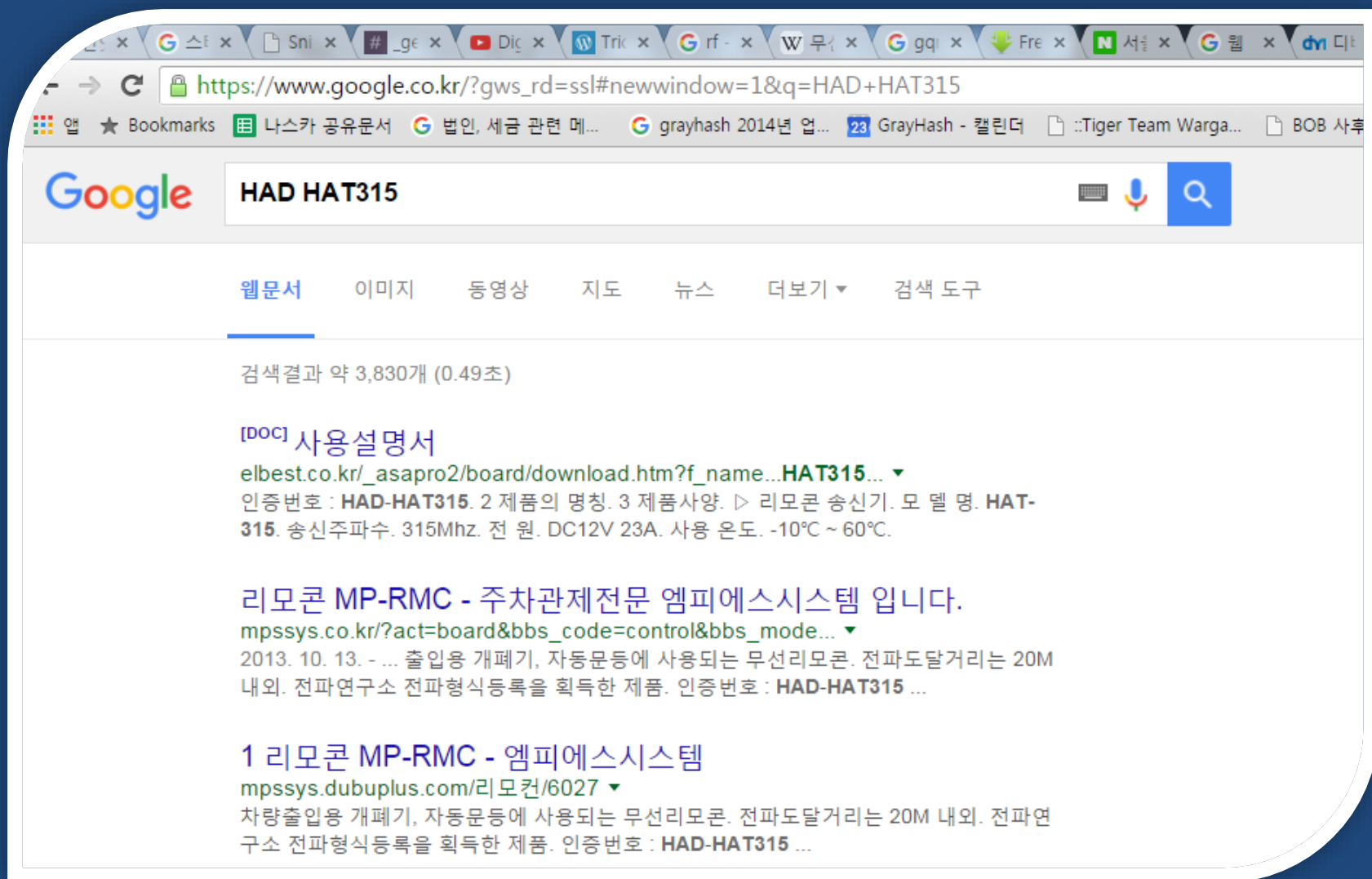
MODEL - SPS2CD (외부차량 진입통제용)



개요: 아파트,오피스텔,공장,학교,빌딩 등
주차장에 진입하는 차량 중 외부차량을 통제 하기 위하여
REMOCON을 사용하여 차단기를 열고 닫을 수 있습니다.

사 양 : 송신 주파수----- 304 MHz (단일채널)
사 용 전 원----- DC 12V (알카라인 전지)
송수신 거리----- 직선거리 10m MAX
송수신 방식----- 데이터 코드 송신
크 기----- 32× 62× 13mm

RF 주파수 알아내기 팁



The screenshot shows a Google search interface with the query "HAD HAT315". The search results are displayed under the "웹문서" (Web Documents) tab. The first result is from elbest.co.kr, titled "[DOC] 사용설명서" (User Manual), which describes the HAD-HAT315 remote control. The second result is from mpssys.co.kr, titled "리모콘 MP-RMC - 주차관제전문 엠피에스시스템 입니다." (Remote Control MP-RMC - Parking Management Specialist EMS System), which also describes the HAD-HAT315 remote control. The third result is from mpssys.dubuplus.com, titled "1 리모콘 MP-RMC - 엠피에스시스템" (1 Remote Control MP-RMC - EMS System), which also describes the HAD-HAT315 remote control.

Google HAD HAT315

웹문서 이미지 동영상 지도 뉴스 더보기 ▾ 검색 도구

검색결과 약 3,830개 (0.49초)

[DOC] 사용설명서
elbest.co.kr/_asapro2/board/download.htm?f_name...HAD315... ▾
인증번호 : HAD-HAT315. 2 제품의 명칭. 3 제품사양. ▷ 리모콘 송신기. 모 델 명. HAT-315. 송신주파수. 315Mhz. 전 원. DC12V 23A. 사용 온도. -10°C ~ 60°C.

리모콘 MP-RMC - 주차관제전문 엠피에스시스템 입니다.
mpssys.co.kr/?act=board&bbs_code=control&bbs_mode... ▾
2013. 10. 13. - ... 출입용 개폐기, 자동문등에 사용되는 무선리모콘. 전파도달거리는 20M 내외. 전파연구소 전파형식등록을 획득한 제품. 인증번호 : HAD-HAT315 ...

1 리모콘 MP-RMC - 엠피에스시스템
mpssys.dubuplus.com/리모컨/6027 ▾
차량출입용 개폐기, 자동문등에 사용되는 무선리모콘. 전파도달거리는 20M 내외. 전파연구소 전파형식등록을 획득한 제품. 인증번호 : HAD-HAT315 ...

RF 주파수 알아내기 팁

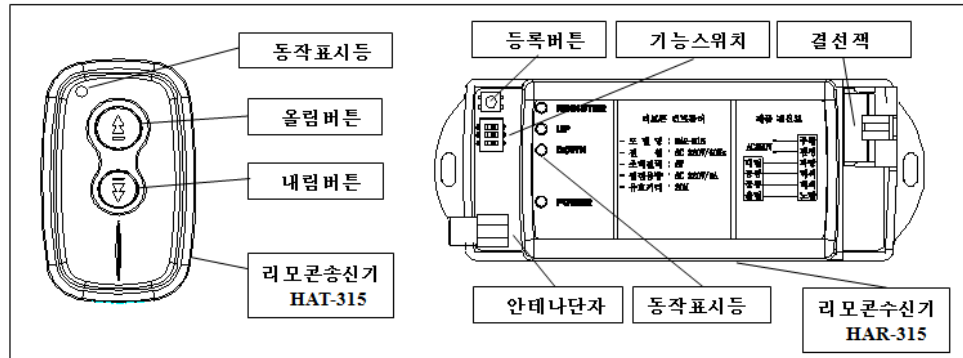
무선 리모콘 송/수신기

먼저 저희 제품을 구입하여 주셔서 대단히 감사드립니다.
기기를 사용하기에 앞서 사용설명서를 충분히 숙지하신 후 설치해 주시기를 부탁드립니다.

1 본기기에 대하여

- 본 제품은 차량출입용 개폐기, 자동문등에 사용되는 무선리모콘입니다.
- 본 제품의 전파도달거리는 20M 내외입니다.
- 본 제품은 전파연구소 전파형식등록을 획득한 제품입니다. 인증번호 : HAD-HAT315

2 제품의 명칭




3 제품사양

▶ 리모콘 송신기

모 델 명	HAT-315	송신 주파수	315Mhz
전 원	DC12V 23A	사용 온도	-10℃ ~ 60℃
변 조 방식	ASK	도달 거리	20M 내외

RF 주파수 알아내기 팁



국립전파연구원
NATIONAL RADIO RESEARCH AGENCY

사이트맵 ENGLISH

Q 검색

정부3.0 정보공개


업무마당

알림마당

자료실

연구원안내

메뉴전체보기



업무마당

적합성평가현황검색

Home 업무마당 적합성평가제도 적합성평가현황검색

적합성평가를 받은 기기, 모델명, 상호, 인증/등록 연월일 등을 검색하실 수 있습니다.
인증/등록 연월일 조건검색은 필수사항이며, 10년이나 20년 단위로 하셔도 상관없습니다.
페이지 전환이 안될시 메뉴모음 > 도구 > 호환성보기 체크후 다시 검색해보시기 바랍니다.
시스템 관련문의 : 061-338-4922

적합성평가제도

- 적합성평가제도개요
- 신규적합성평가현황
- 적합성평가현황검색
- 부적합방송통신기자재현황
- 지정시험기관개요
- 지정시험기관현황
- MRA안내

방송통신기술기준

방송통신국가표준

전자파흡수율


전자파적합표준시험

우주전자환경

국제협력업무

전파특성지도

검색할 내용을 입력해 주시기 바랍니다.



분 류 (Category) 전제

인증/등록 연월일 (Date of Certification / Registration) 1주일 1개월 3개월 1년 5년 (예) 20100322 ~ 20131018

상 호 (Applicant)

기 기 명 칭 (Equipment Name) (예) 무선설비의 기기

모 델 명 (Model Number) (예) HSC-T80

인증/등록 번호 (Certification / Registration No.) (예) R-LARN-00-0210

제 조 자 (Manufacturer)

제 조 국 가 (Country of Origin) (예) 한국

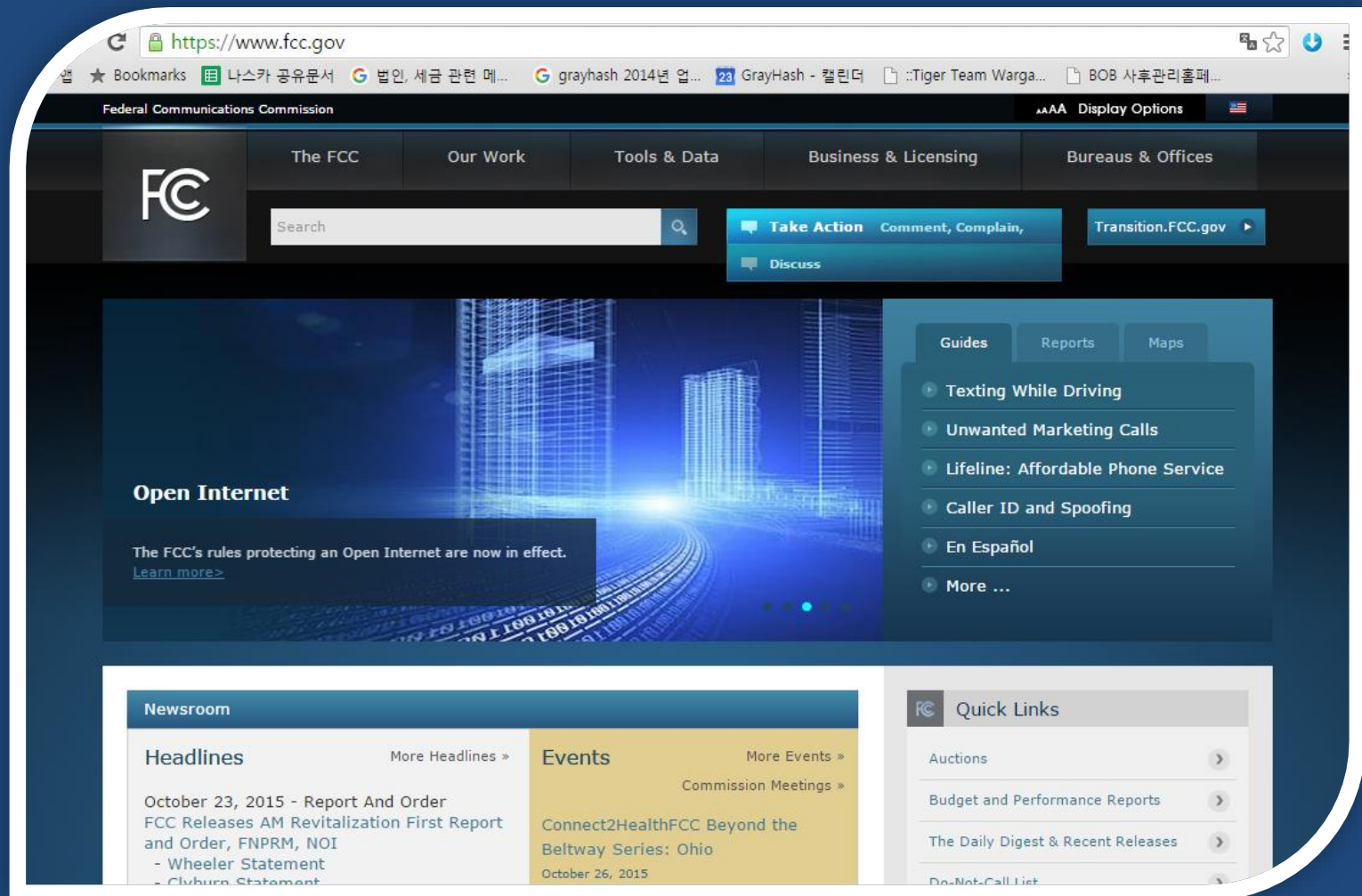
신청자 식별부호 조회

검색

엑셀

CSV

RF 주파수 알아내기 팁



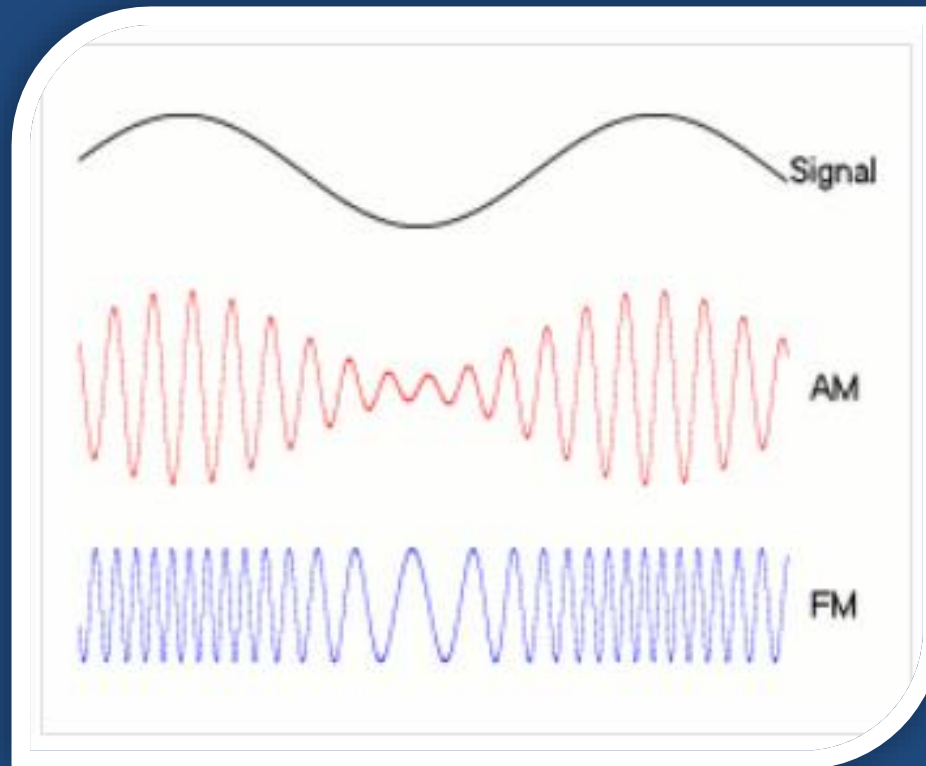
Replay Attack 시의 팁

- Sample Rate 값이 적절해야 한다.
 - 32Khz : X
 - 20Mhz : O
 - 50Mhz : X
- 신호가 약할 경우 Multiply Const Block을 이용하여 증폭시킨다.
 - 1 -> 2 -> 3

RF Signal Modulation

Modulation

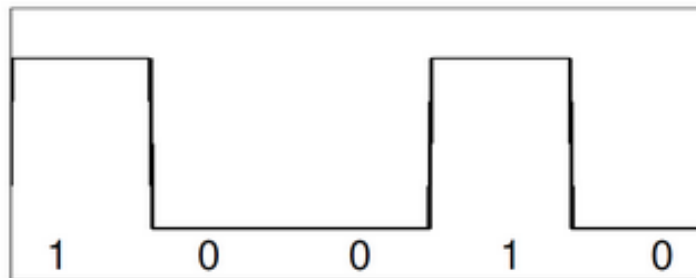
- ASK, FSK 모듈레이션



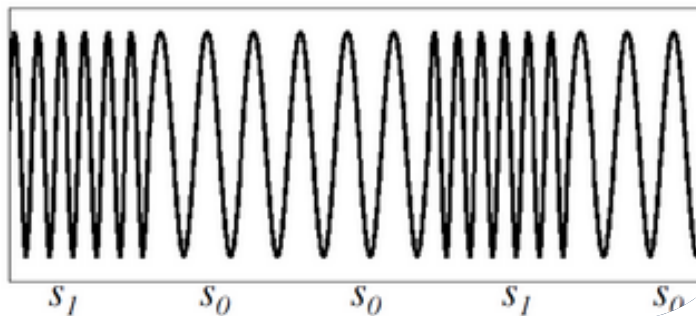
FSK 예시

* Frequency-Shift Keying

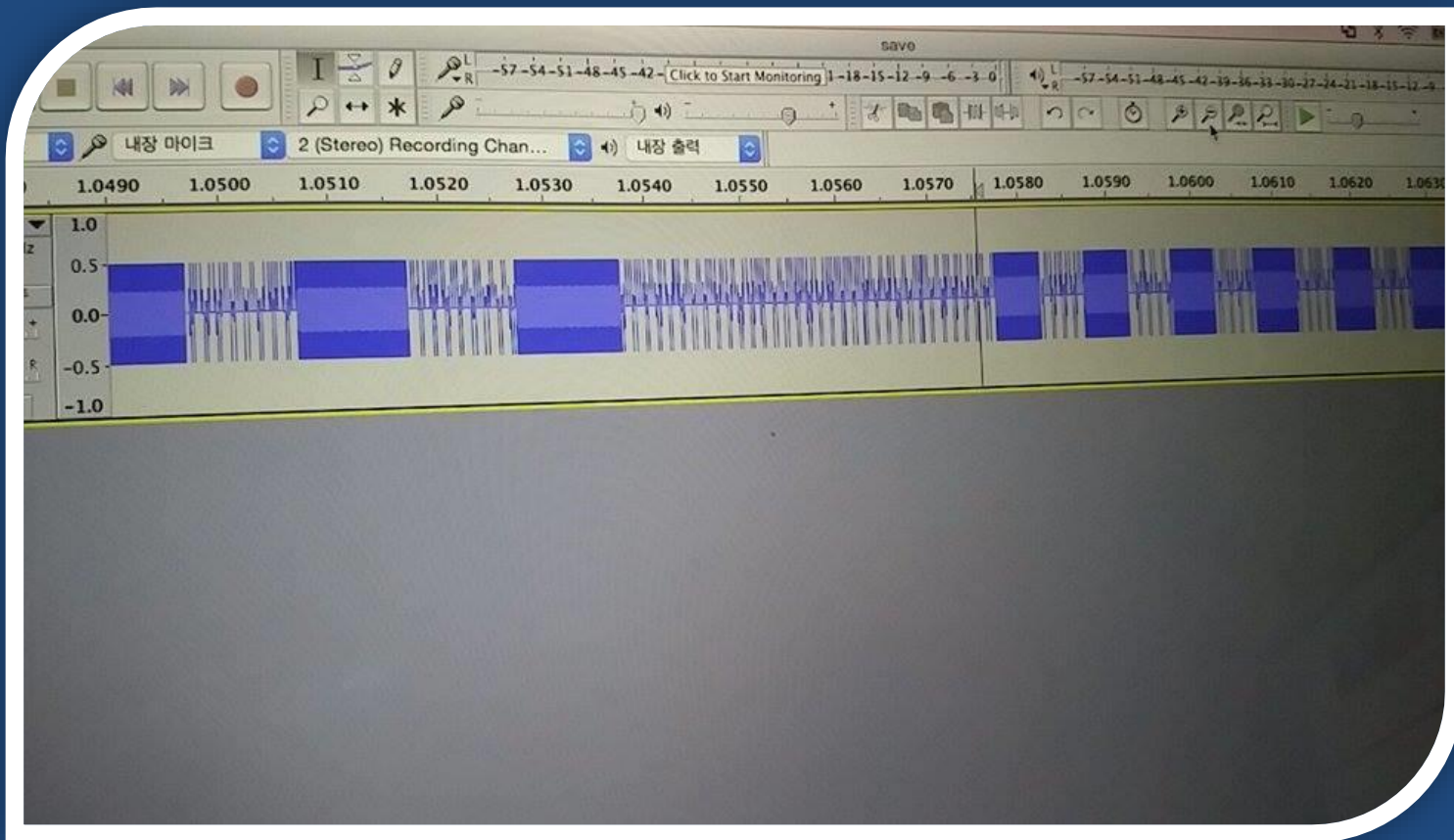
Baseband data:



FSK modulated signal:

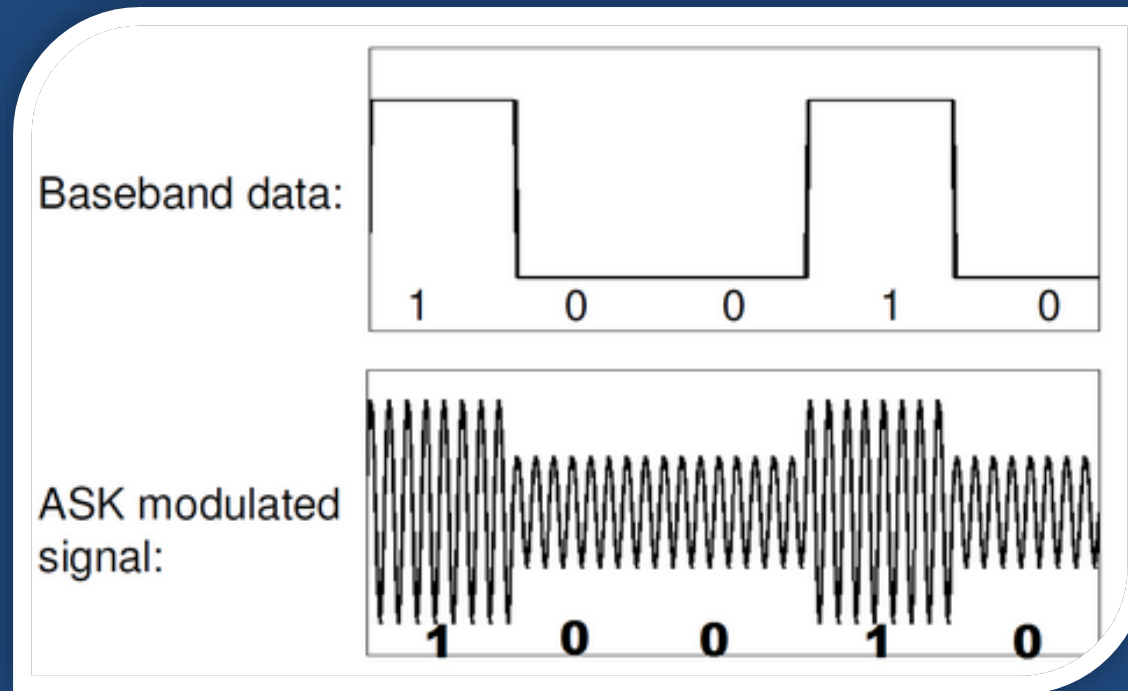


FSK Modulation



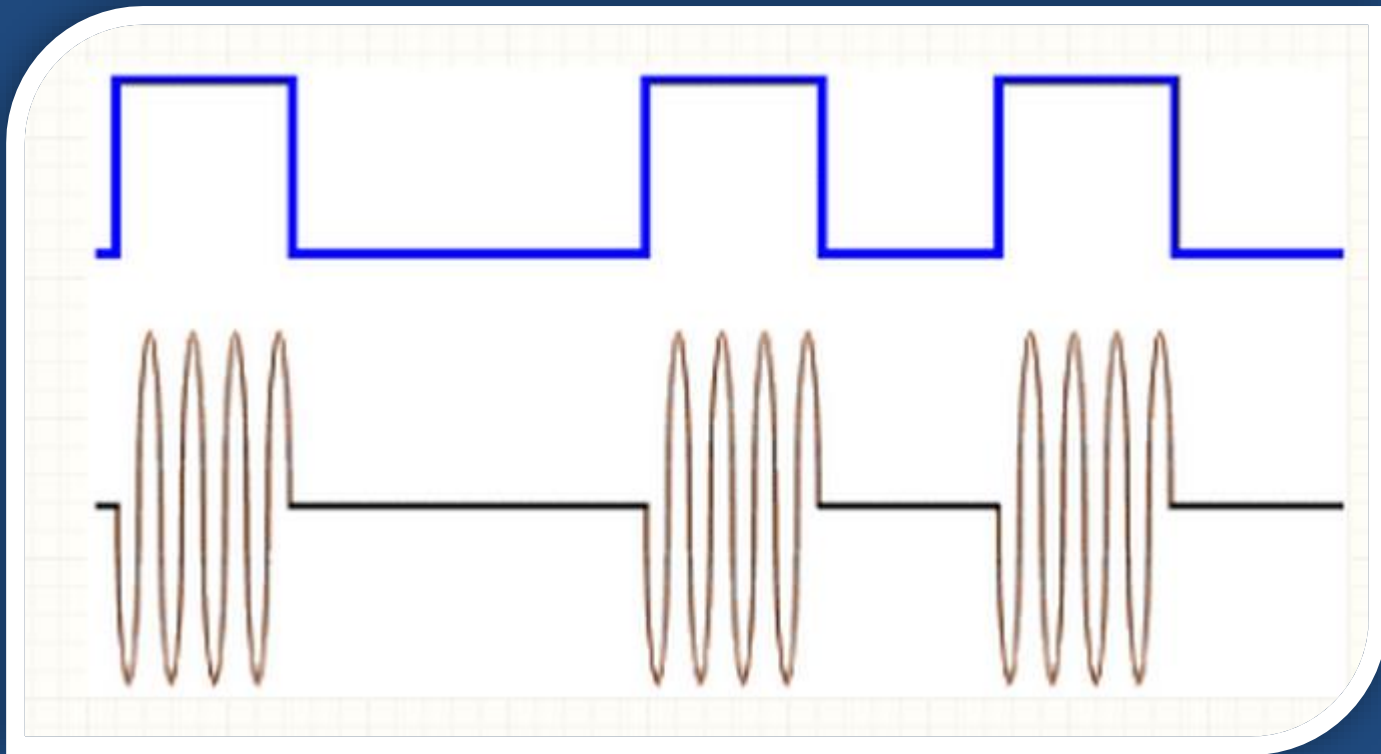
ASK 예시

- Amplitude-Shift Keying

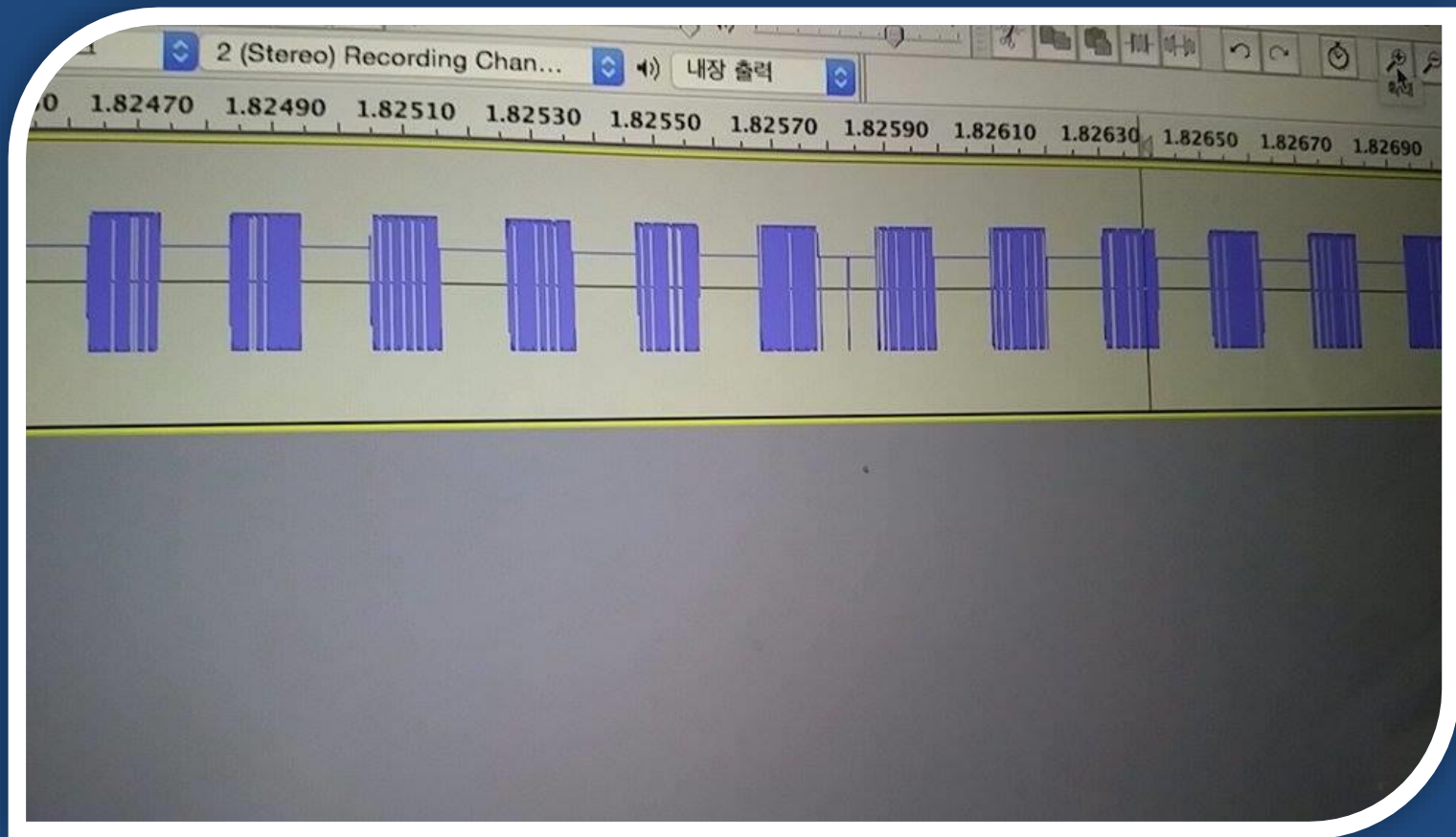


ASK-OOK 예시

* ON-OFF Keying



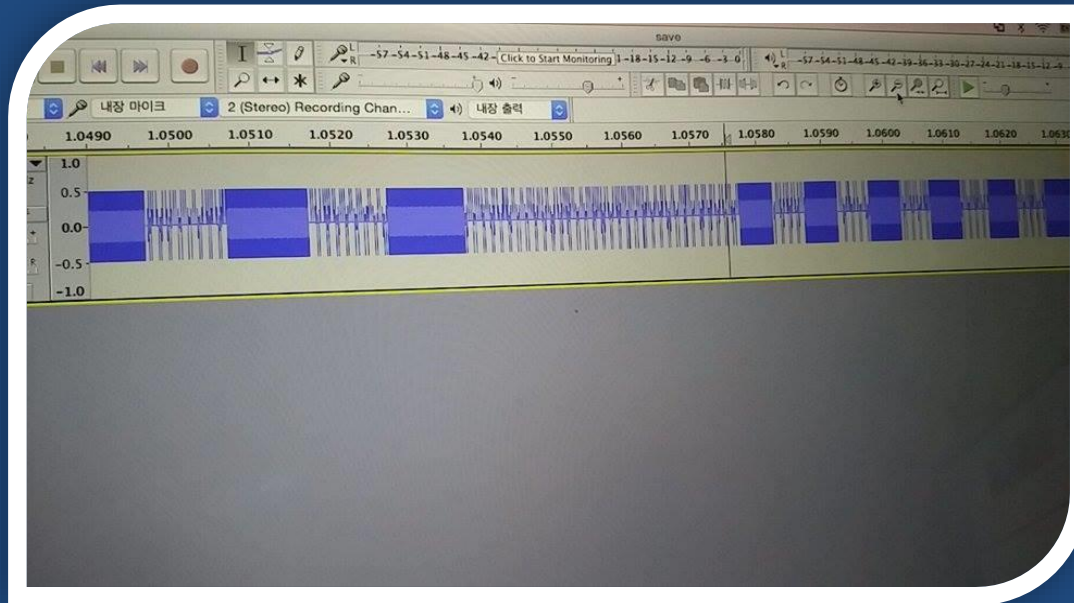
ASK-OOK Modulation



Binary Pattern 분석

Binary Pattern 분석의 필요성

- 단순 replay attack이 아닌, 무선신호의 Bit 해석 및 조작을 통한 정교한 공격 가능
 - Ex> RC카의 전진/후진/좌/우회전 패킷 포맷 분석

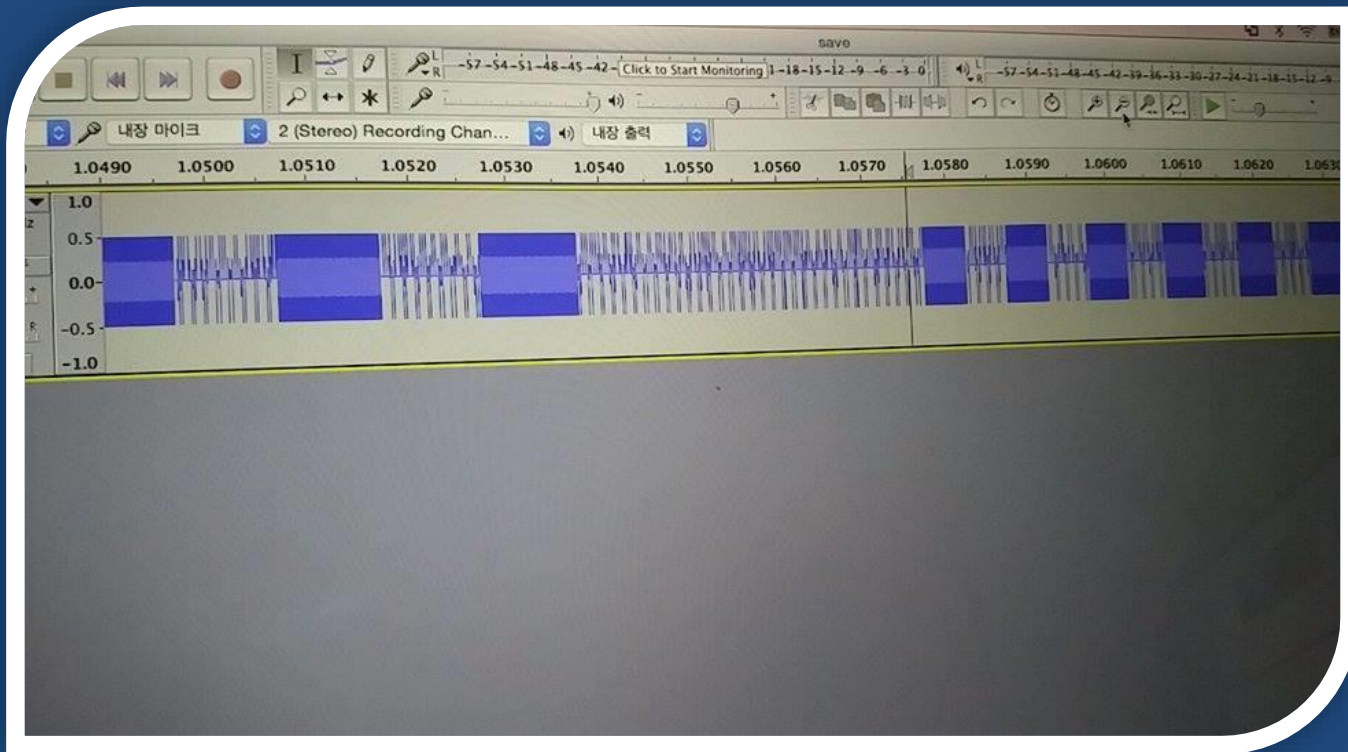


관련 도구들

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

Wav 캡처

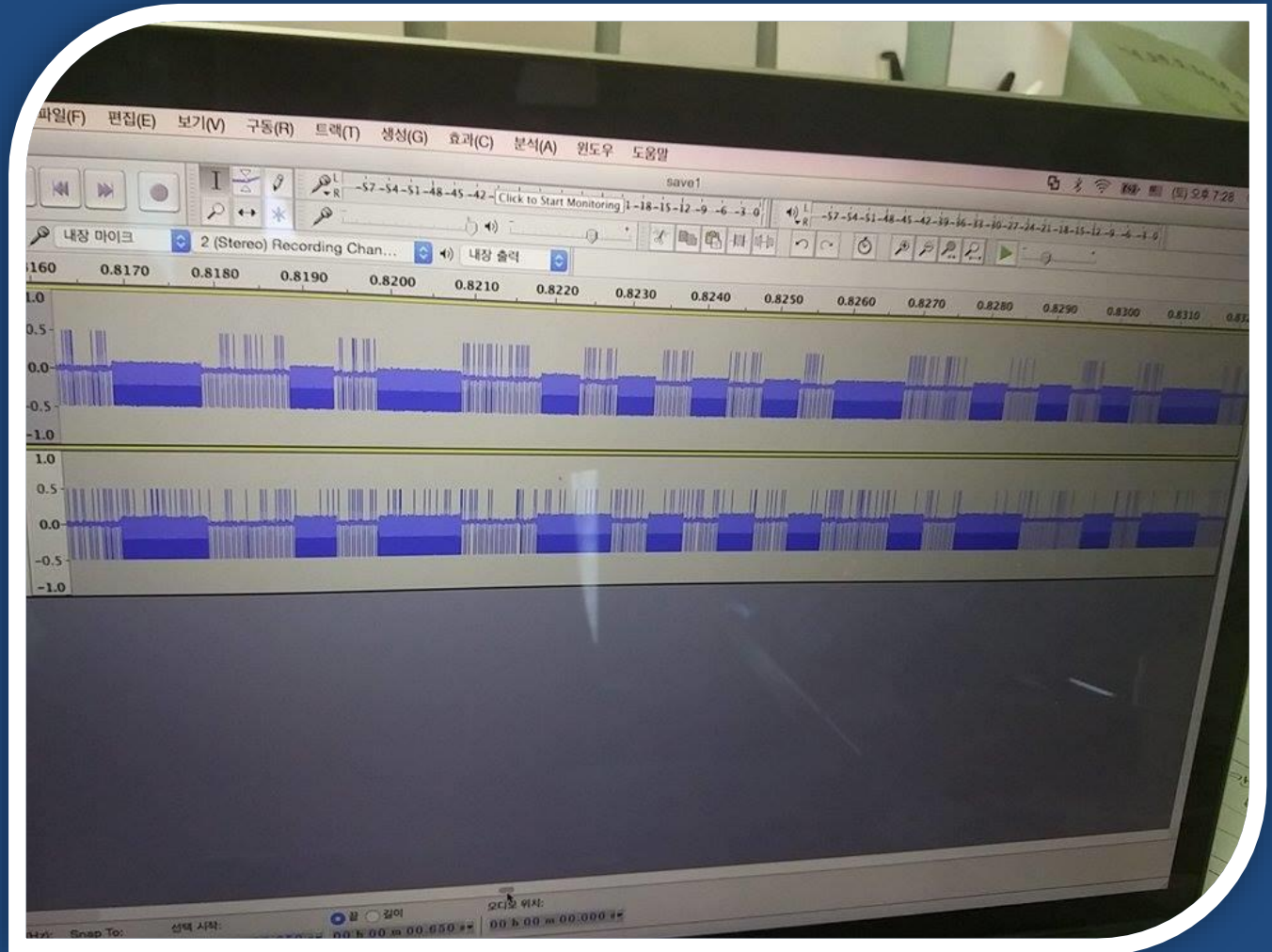
- `# hackrf_fm -f 433000000 -s 2000000 | sox -t raw -r 2000000 -e signed-integer -b 16 -c 1 -V1 - save.wav`



두 개의 신호 비교

차문 Open →

차문 Close →



RF 패킷의 구조 (nRF24L01 예)

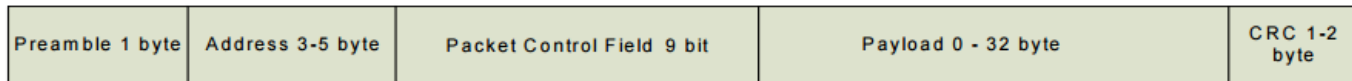


Figure 4. An Enhanced ShockBurst™ packet with payload (0-32 bytes)

7.3.1 Preamble

The preamble is a bit sequence used to detect 0 and 1 levels in the receiver. The preamble is one byte long and is either 01010101 or 10101010. If the first bit in the address is 1 the preamble is automatically set to 10101010 and if the first bit is 0 the preamble is automatically set to 01010101. This is done to ensure there are enough transitions in the preamble to stabilize the receiver.

7.3.2 Address

This is the address for the receiver. An address ensures that the correct packet are detected by the receiver. The address field can be configured to be 3, 4 or, 5 bytes long with the `AW` register.

Note: Addresses where the level shifts only one time (that is, 000FFFFFFF) can often be detected in noise and can give a false detection, which may give a raised Packet-Error-Rate. Addresses as a continuation of the preamble (hi-low toggling) raises the Packet-Error-Rate.

nRF24L01 Spec

- Radio X Worldwide 2.4GHz ISM band operation
- 126 RF channels
- GFSK modulation
- Up to 2Mbps on air data rate
- 1.9 to 3.6V supply range

-Datasheet

http://www.nordicsemi.com/eng/content/download/2730/34105/file/nRF24L01_Product_Specification_v2_0.pdf



CC1111 Spec

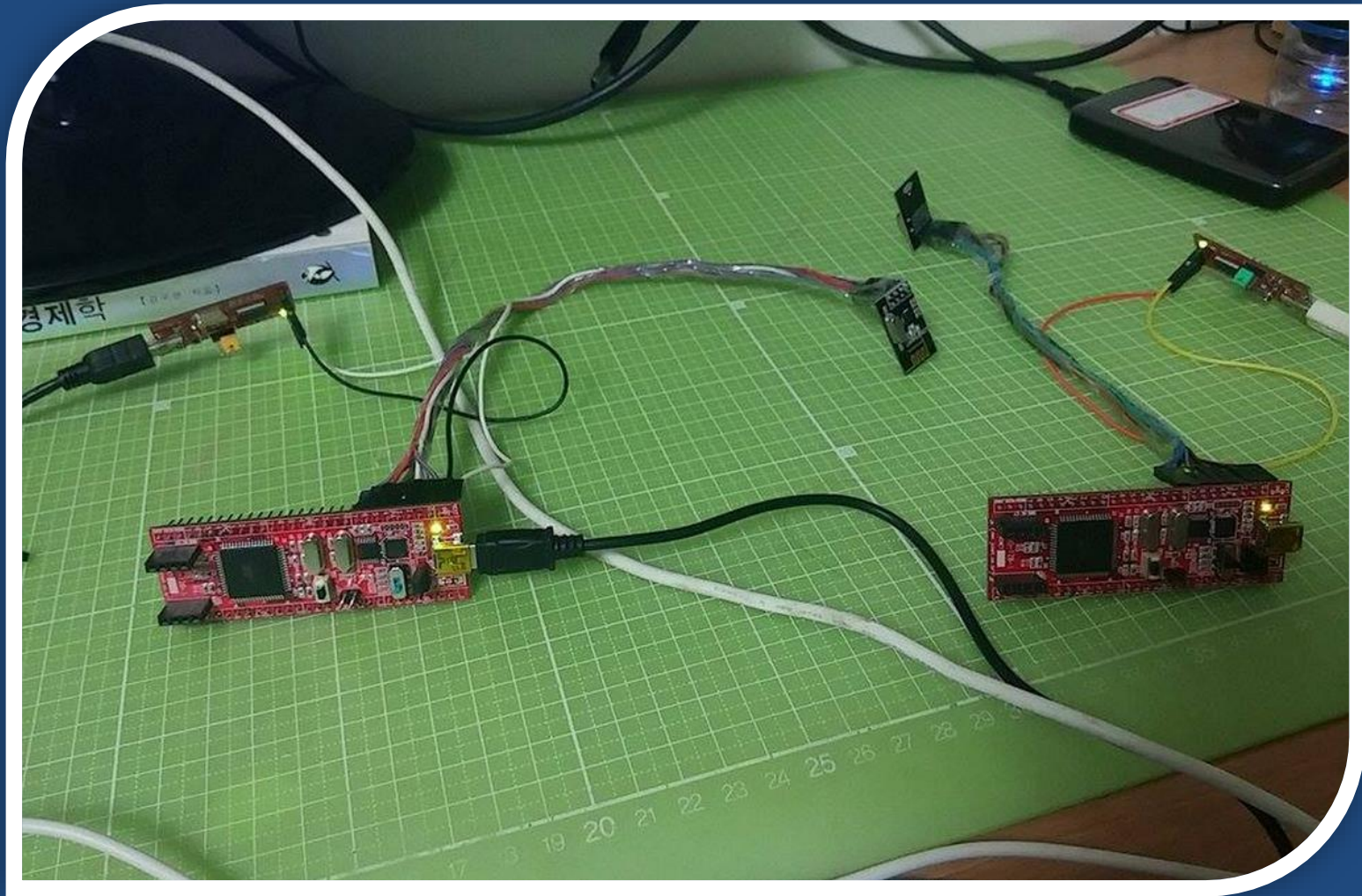
- 1기가 이하의 주파수
- 315/433/868/915MHz ISM/SRD bands
- FSK, ASK modulation
- Up to 500Kbps on air data rate
- 3.6V supply range

-Datasheet

<http://www.ti.com/product/cc1110-cc1111>



RF 통신 개발



결론

- HackRF와 같은 무선 송수신기와 GNU Radio와 같은 SDR 툴을 이용하면 다양하고 흥미로운 무선 해킹 연구가 가능
- 수 많은 무선통신 장비들이 기본적인 Signal replay attack에 조차 취약한 상황
- 무선 레벨에서의 보안성 강화가 시급히 필요한 시점

감사합니다!

