쉽게 시작하는
무선해킹

Who am I

한우영(@hanukoon)

010-9719-6521
hwymaster01@hanukoon.com
https://github.com/cokia
https://blog.hanukoon.com

- **자퇴생 -> 굳이 나이로 따지면 중3**
- Digital Forensic / Network / etc..
- **GoldenTime DApp Developer**
- **Team H4C / Anti-Root**
- 대구대학교 정보보호영재교육원 6기 고등전문B 과정
- 2017 TeamH4C 해킹캠프 발표자 (PowerShell 을 활용한 모의해킹)
- Codegate 2018 주니어 보안포럼 발표자 (윈도우 환경에서의 디지털 포렌식)

목차

01. Let’s Wireless!

01. Let’s Wireless - Protocol

RF : **Radio Frequency 의 약자**로 **1mm에서 100km 범위, 즉 진동수 3 KHz에서 300 GHz까지의 전자기파를 뜻한다.**

GPS : **Global Positioning System 의 약자로, 군용 및 민간용 목적으로** 사용되고 있다.보통 세 개 이상의 GPS 위성으로부터 송신된 신호를 수신하여 위성과 수신기의 위치를 결정한다. 그러나 시계가 완벽하지 않기에, 4개 이상의 위성에서 정보를 받아, **삼변측량법으로 위치를 구한다. 대역은 1575.42 Mhz (L1)**

01. Let’s Wireless - Protocol

BLE : **Bluetooth Low Energy 의 약자로 일반 블루투스 통신보다 저전력이며, 1:1 통신 이외에 1:n 통신을 지원하여 비컨과 같은곳에 활용된다.** (Bluetooth 4.0 이상 버전을 BLE 라 통칭하기도 한다)

WIFI : **전자기기들이 무선랜에 연결할 수 있게 하는 기술**로써, 주로 **2.4 기가헤르츠 및 5 기가헤르츠 대역에서 운용된다.**

ZigBee : **IOT 나 다양한 소형 디바이스에서 주로 활용하는 네트워크 프로토콜**로, 설정이 간단하고, 비용이 저렴하다는 장점이있다.

01. Let's Wireless - SDR

Software Defined Radio

HACKRF ONE

1 Mhz ~ 6 Ghz
300$
반이중 통신

저렴/반이중/간단하게?

BladeRF x40

300 Mhz ~ 3.8 Ghz
420$
전이중 통신

중저가/전이중/LTE,GPS,등등…

USRP B200/210

70 Mhz ~ 6 Ghz
1200$
전이중 통신

고가/전이중/개인이 쓰기엔 조금..?

01. Let’s Wireless - SDR

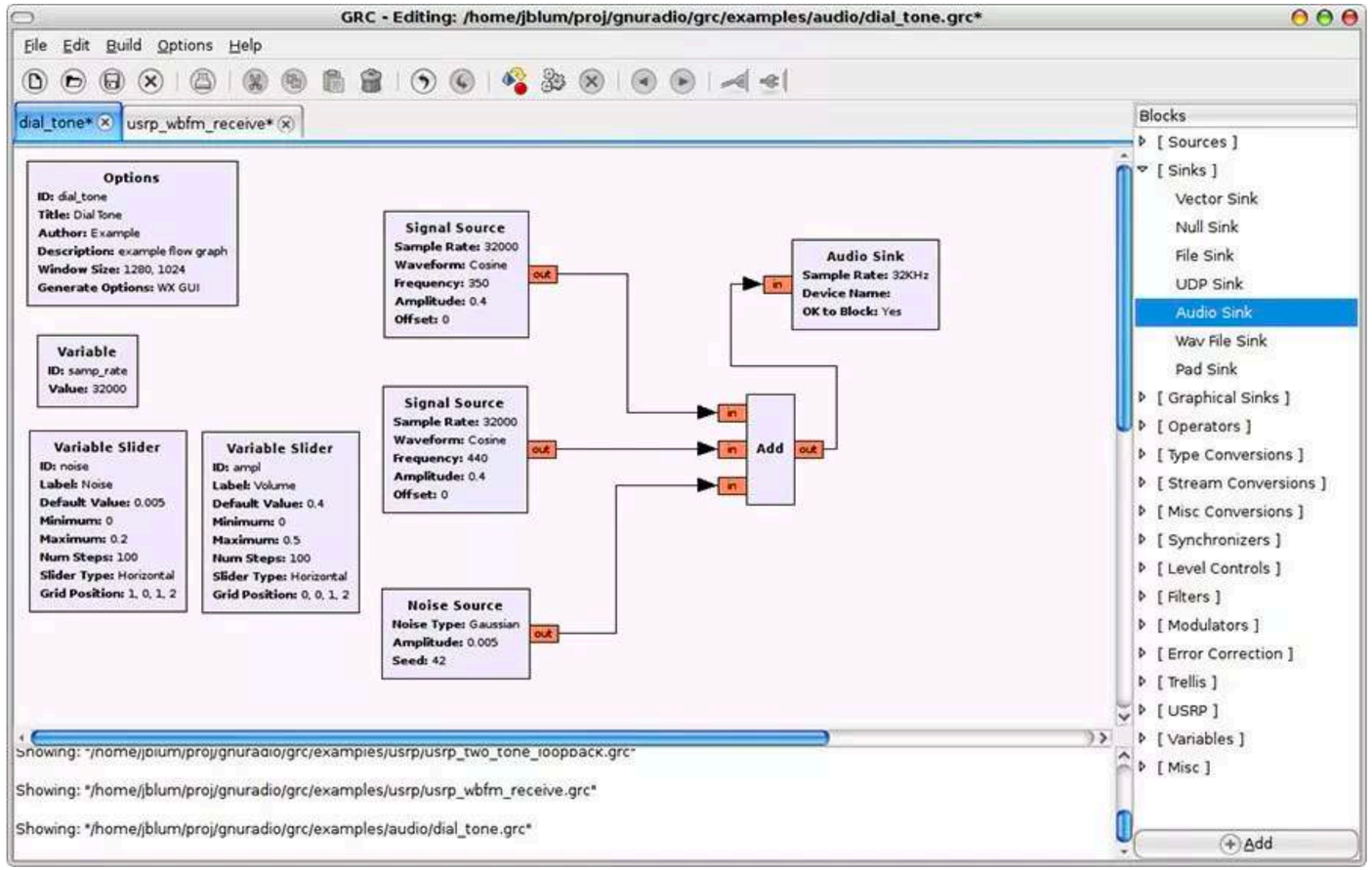
Software Defined Radio

RTL-SDR

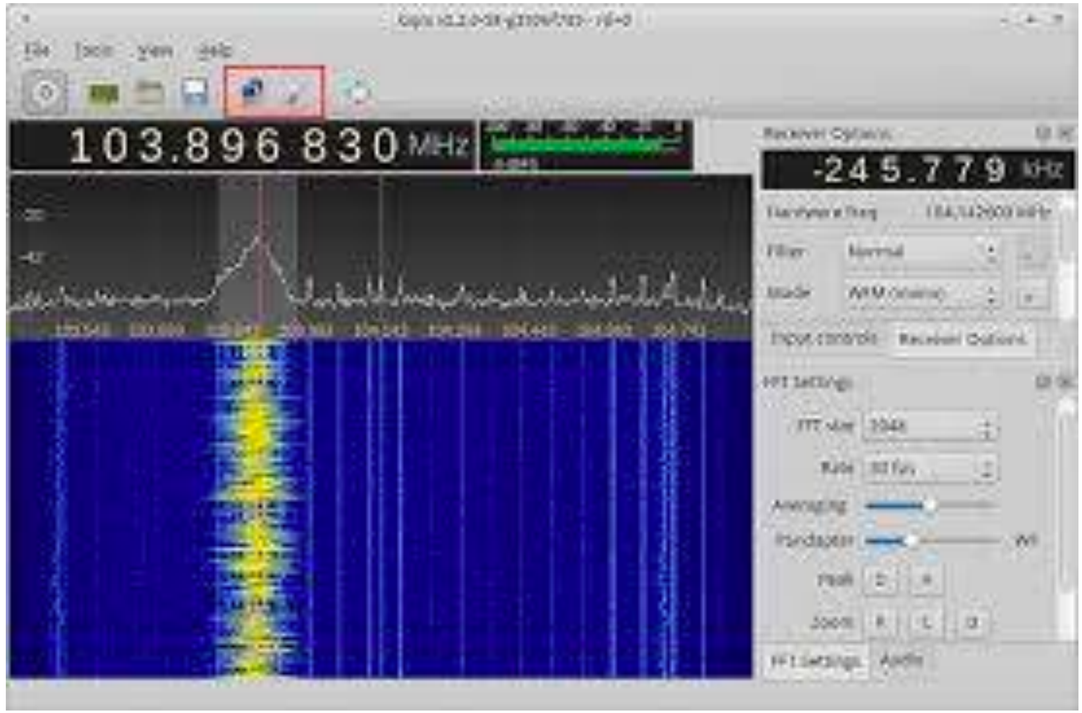
24Mhz ~1766MHz
15$
수신만 가능

초저렴/수신전용/

01. Let's Wireless - GQRX/GnuRadio



-gnuradio-



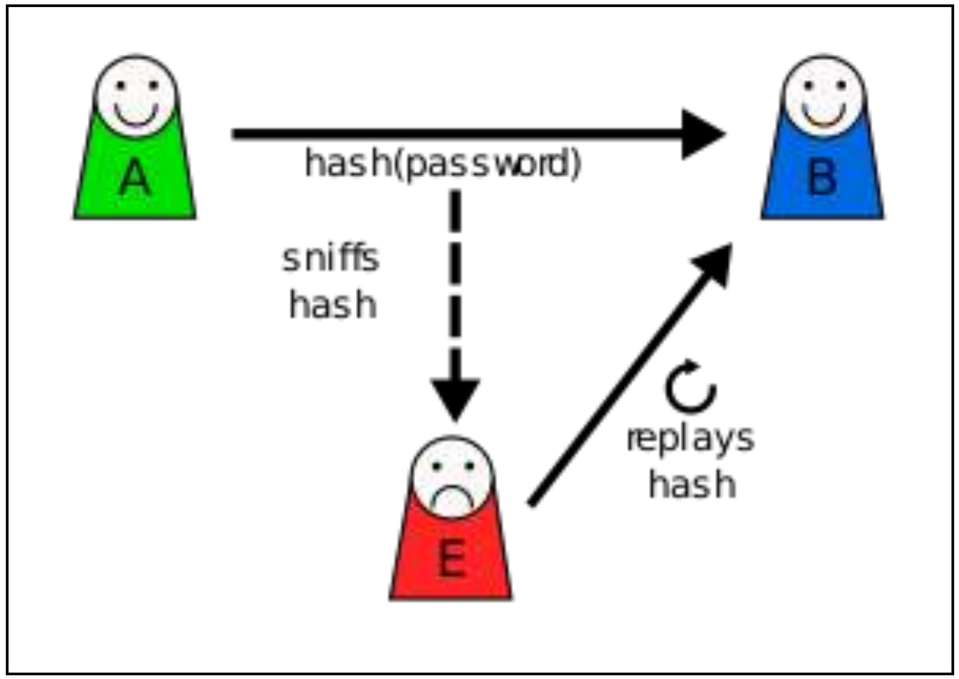
-gqrx-

02. Replay Attack

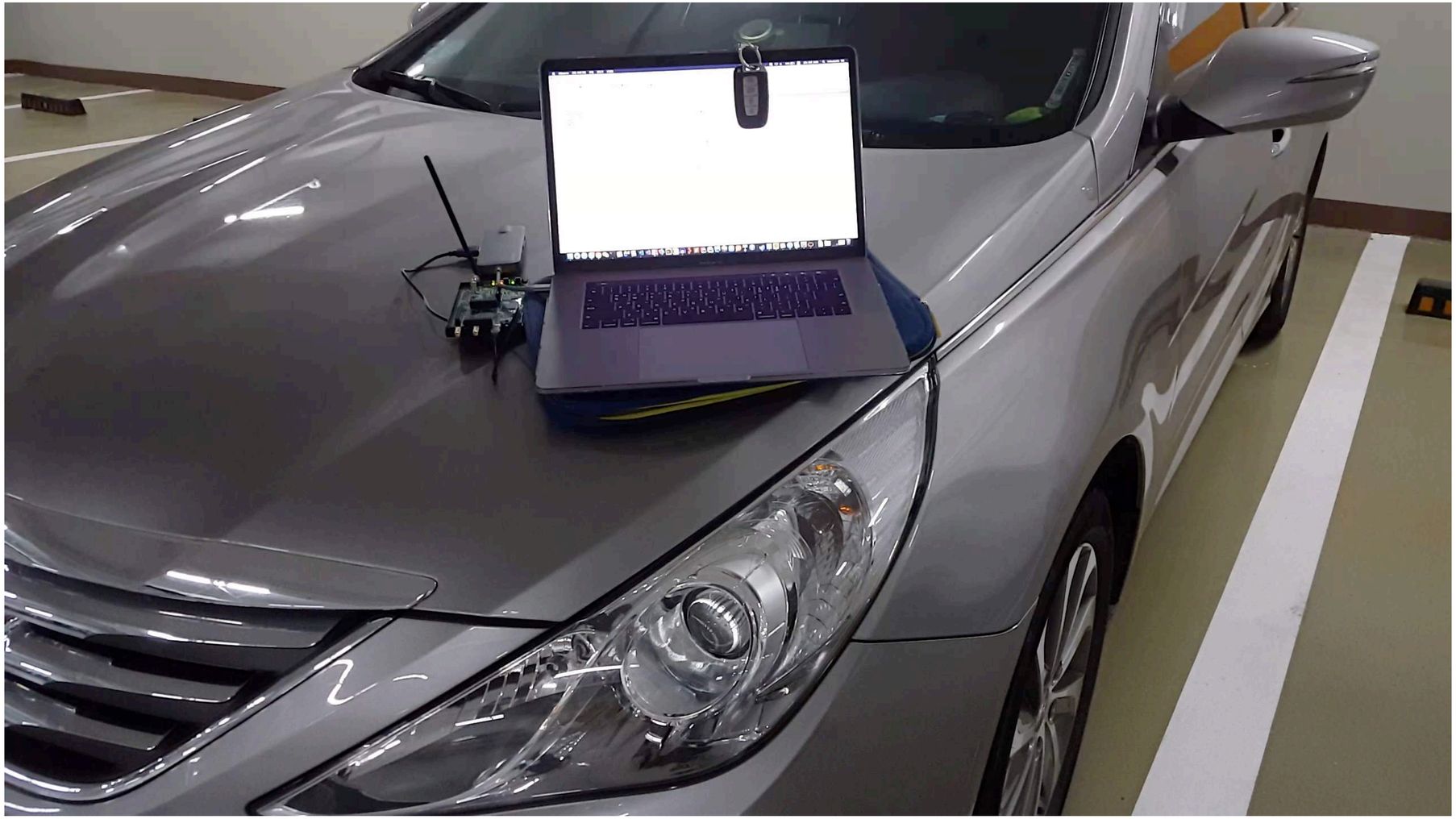
02. Smart Key - Replay Attack

Replay Attack

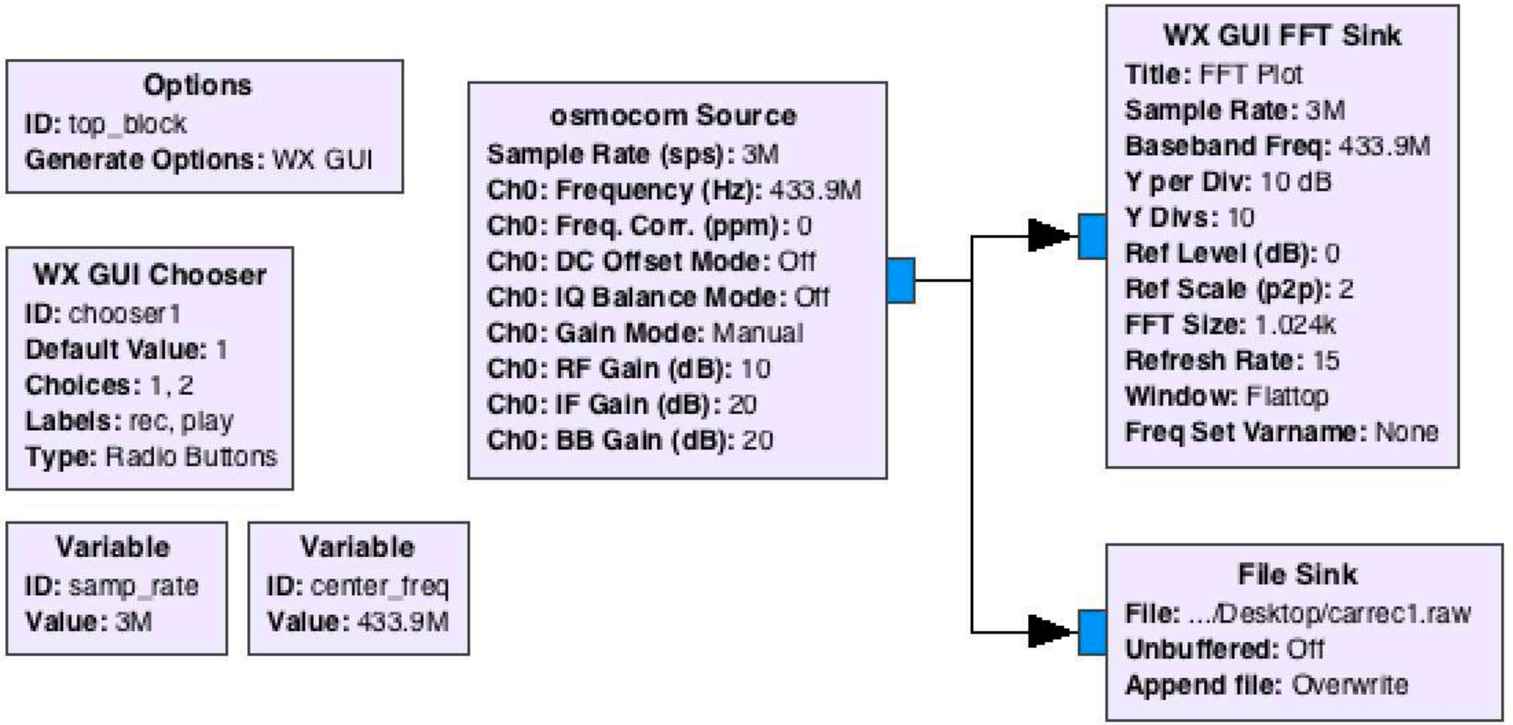
작동하는 장비의 송신기에서 방출되는 신호를 복제하여
수신기에 복제한 신호를 방출,
장비는 정상적인 RF신호로 감지하고 정상적으로 작동



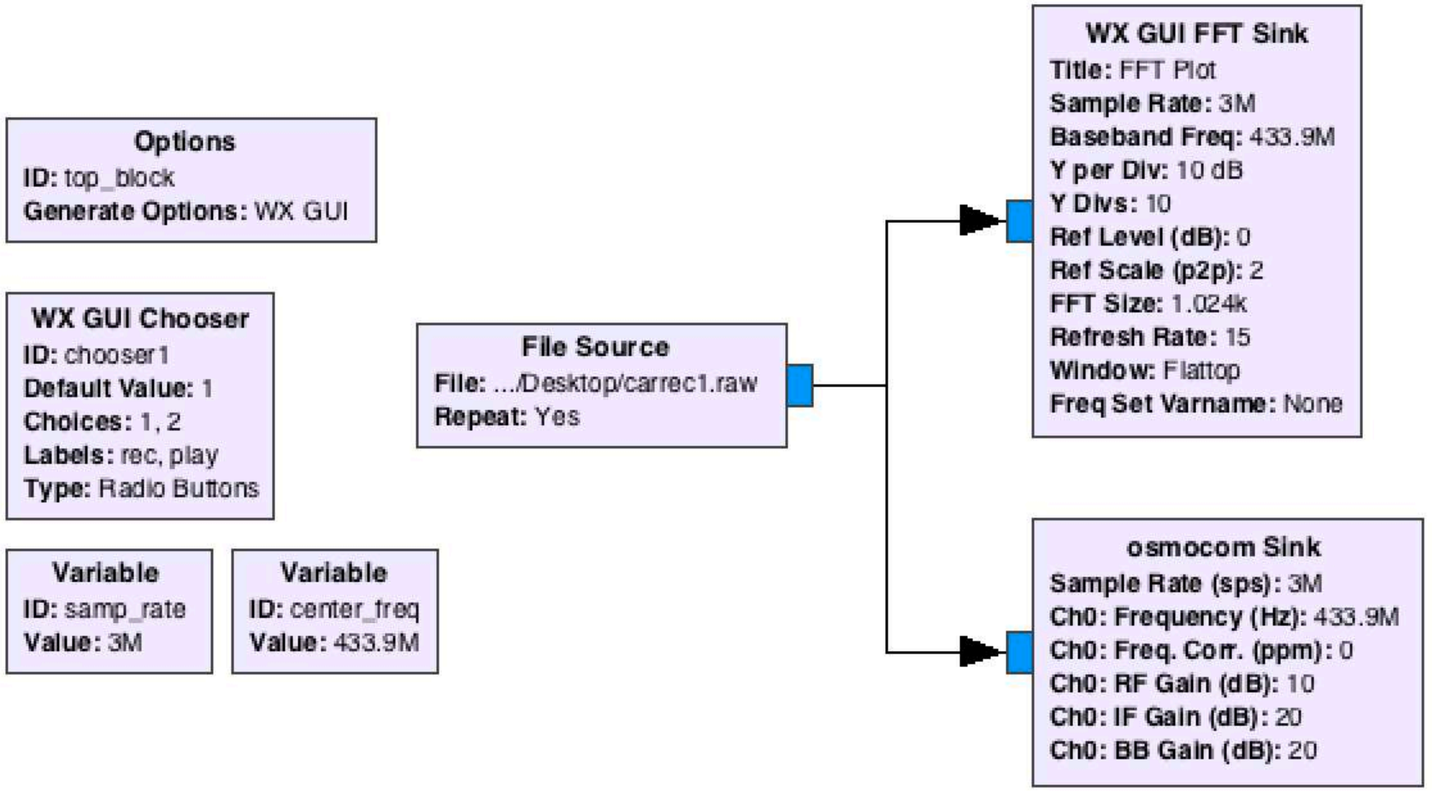
02. Smart Key - Replay Attack



02. Smart Key - Replay Attack



02. Smart Key - Replay Attack



02. Smart Key - Replay Attack

02. Smart Key - Replay Attack

1. **Replay attack 을 활용**해 차에 문을 연다
2. **OBD 나 CAN 포트를 통해** ECU 제어권을 탈취한다
3. **PROFIT!**

OBD : **O**n-**B**oard **D**iagnostics의 약자로, 차량 스스로가 자신을 진단하여
문제를 유발할 수 있는 부분에 대해서 운전자에게 경고하여 점검 및 정비를 받도록 유도할 수 있다.

ECU : **E**lectronic **C**ontrol **U**nit 의 약자로, 엔진의 내부적인 동작을 다양하게 제어하는
전자제어장치이다.

02. Smart Key - Replay Attack

03. Droooooone

03.Drooone

≠

~~??? : 서론 본론 결론 드론~~

03.Drooone - Jamming

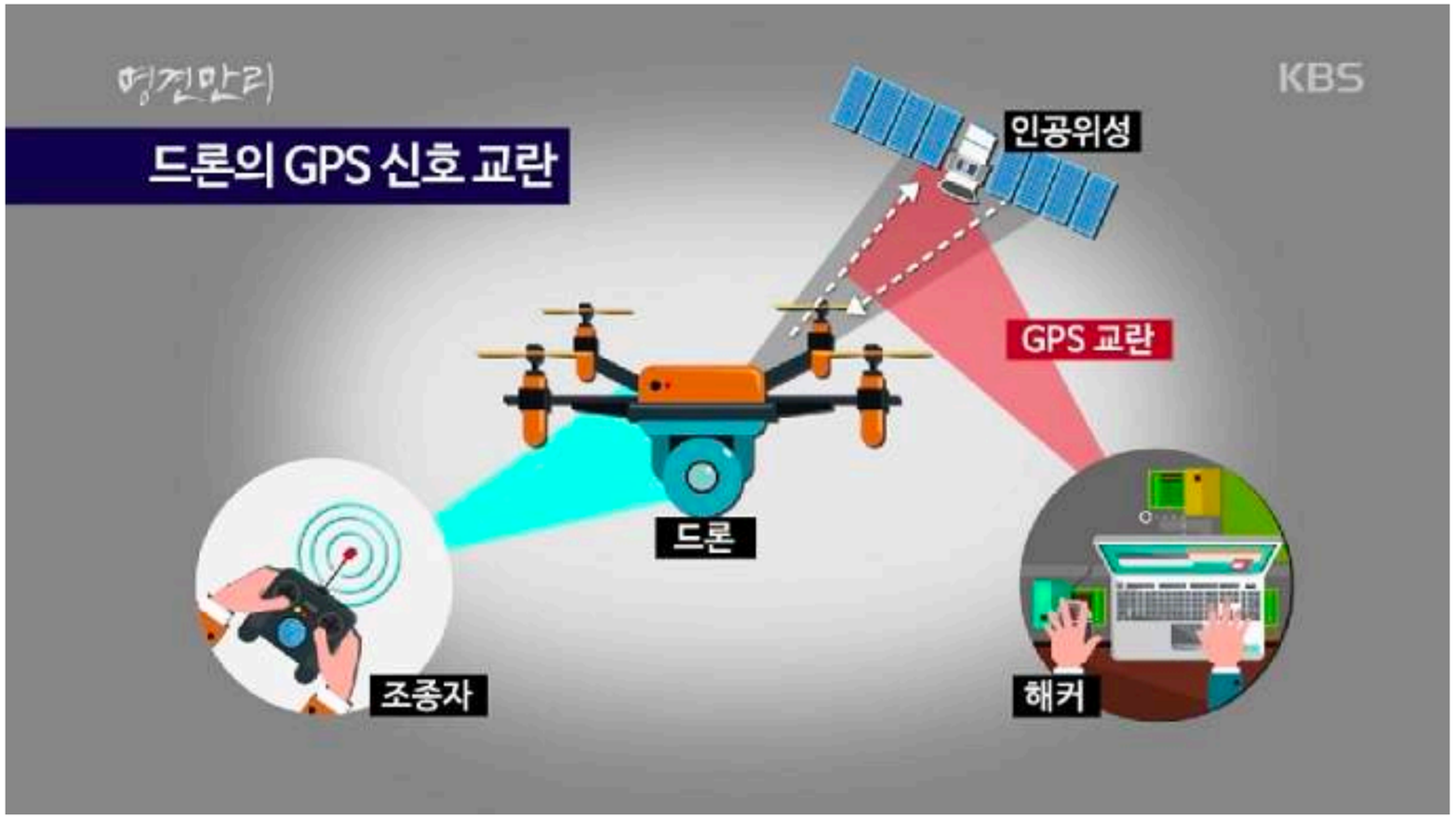
03.Drooone - GPS Spoofing

433MHz (433.05 ~ 434.79 MHz)
915MHz (Option 1 - 902 ~ 928MHz) (Option 2 - 915 ~ 928MHz)
(optional) GNSS L2 (1227 ~ 1251) & GNSS L1 (1575 ~ 1605)
2.4GHz ISM (2400 ~ 2483.5GHz)
5.8GHz ISM (5725 ~ 5850GHz)

03.Drooone - Jamming

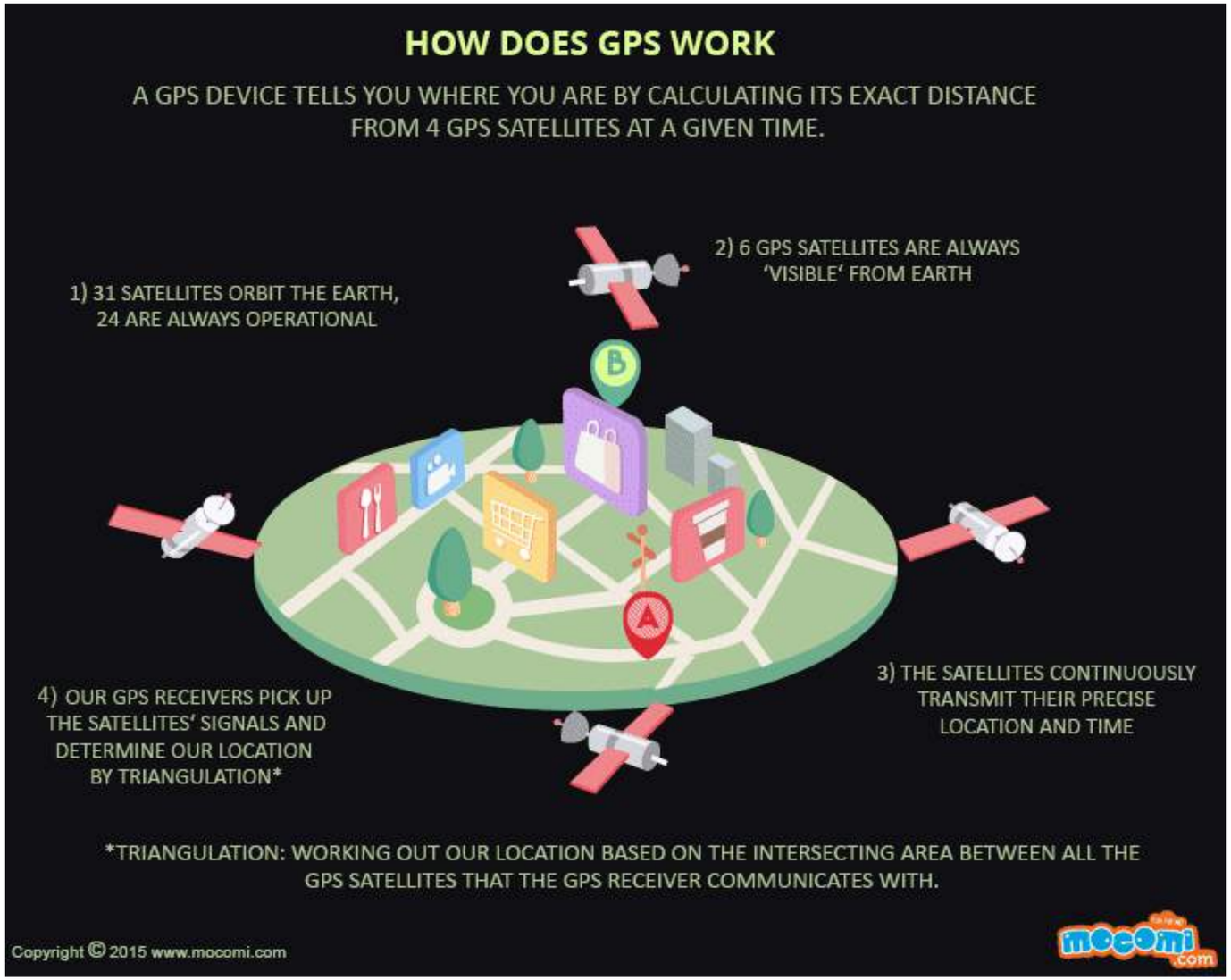
200 ~ 500$

03.Drooone - GPS Spoofing

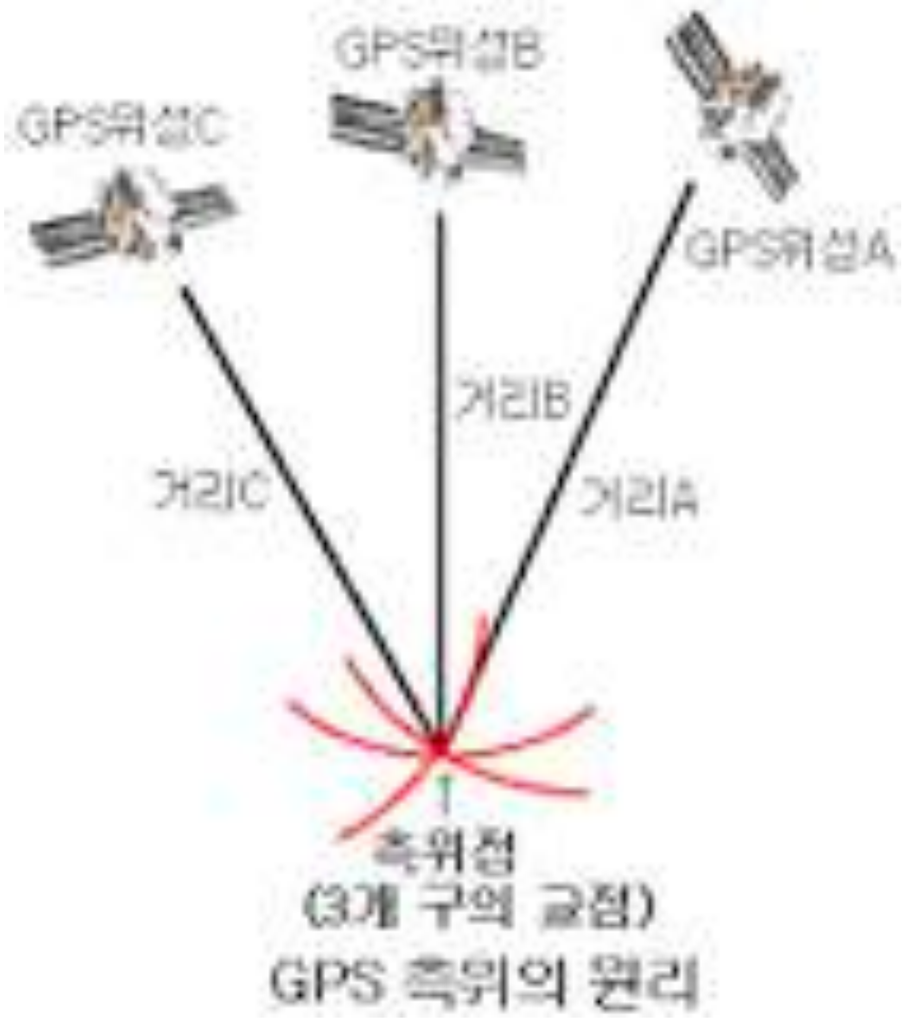


04. GeeePeeeS

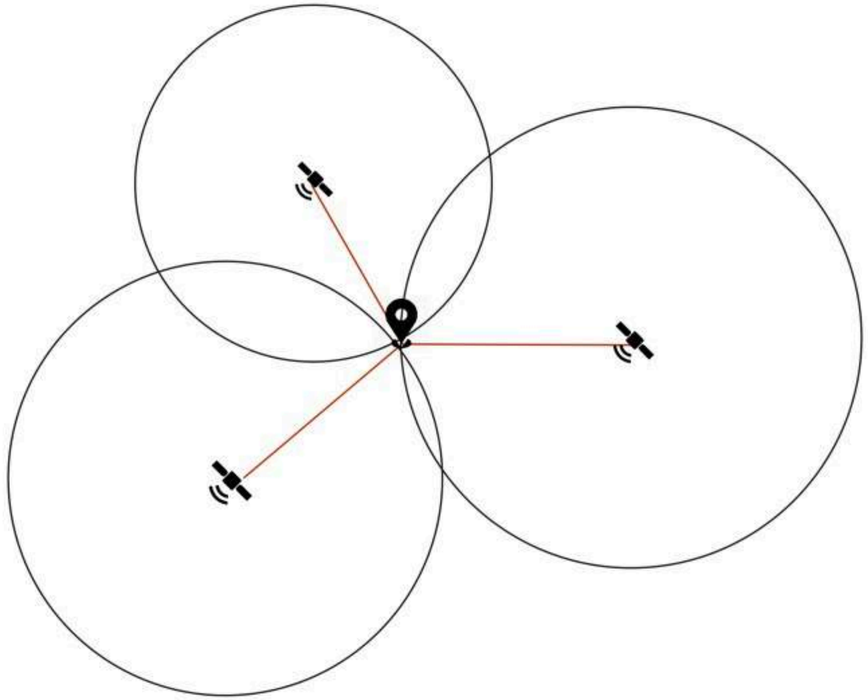
04.GPS - How is working?



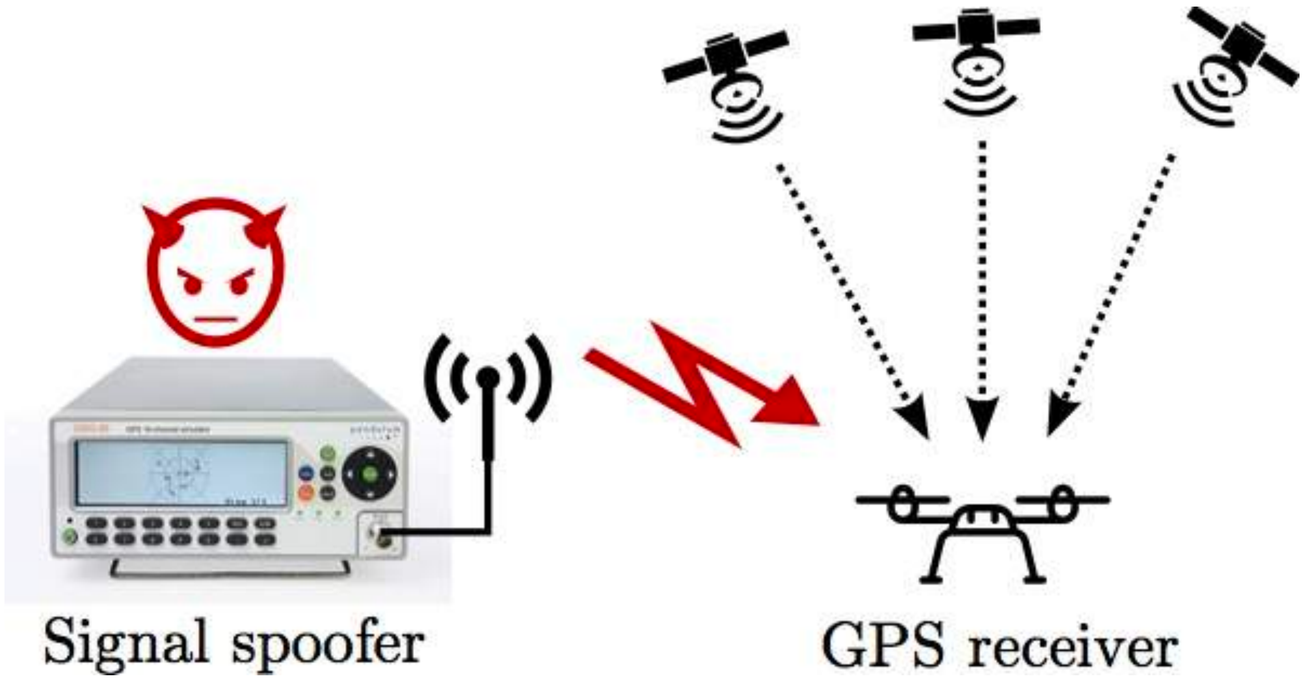
04.GPS - How is working?



GPS 측위의 원리



04.GPS - Let's Spoof!

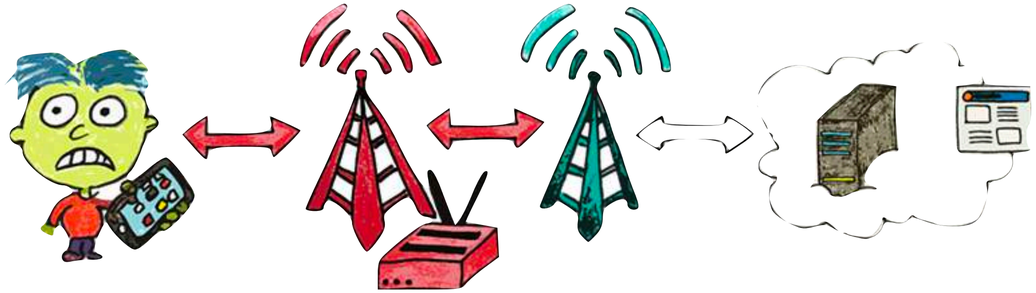


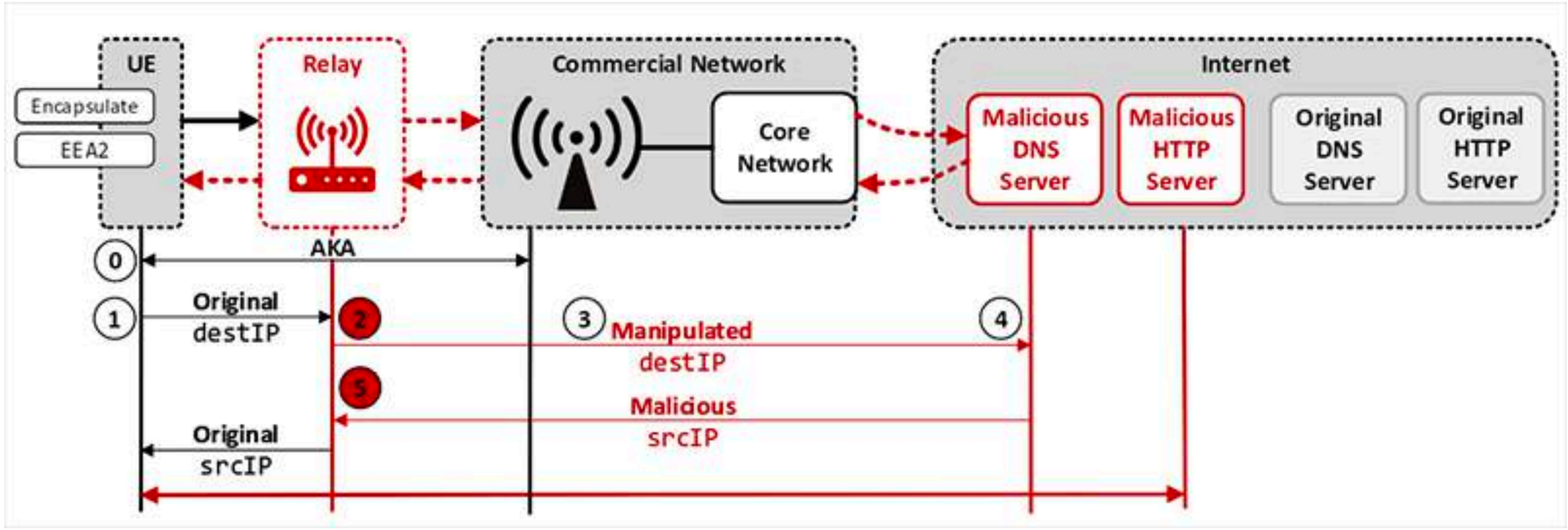
- 1575.42 MHz(L1),
- 1227.60 MHz(L2)

04.GPS - Let's Spoof!

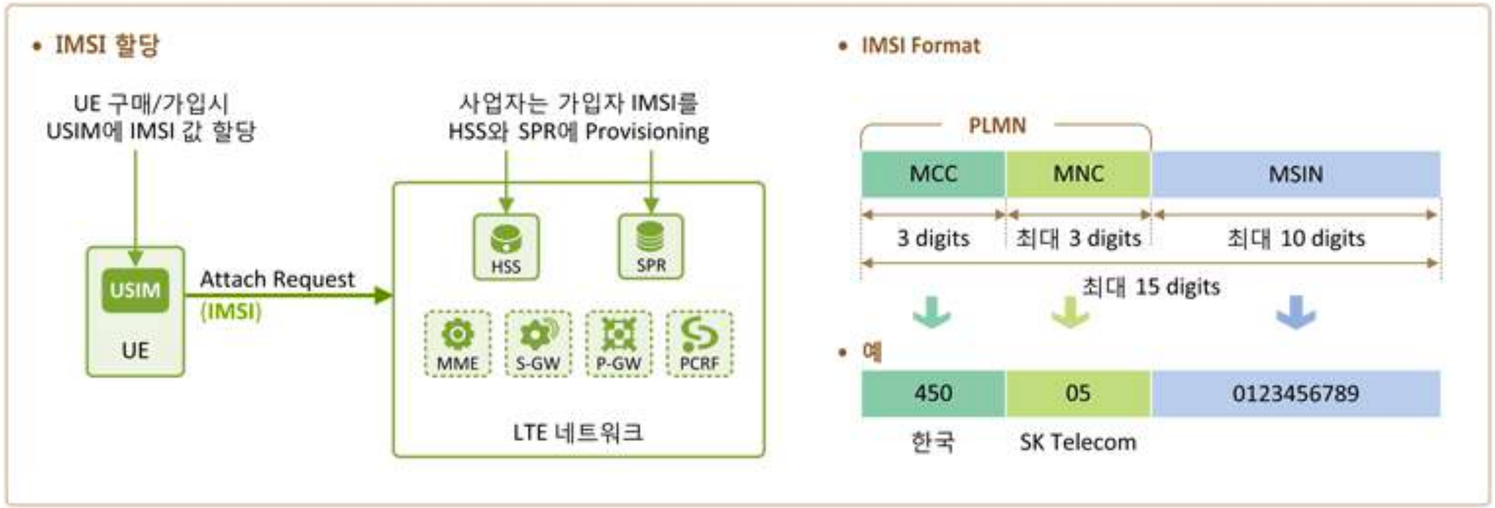
05. LTE

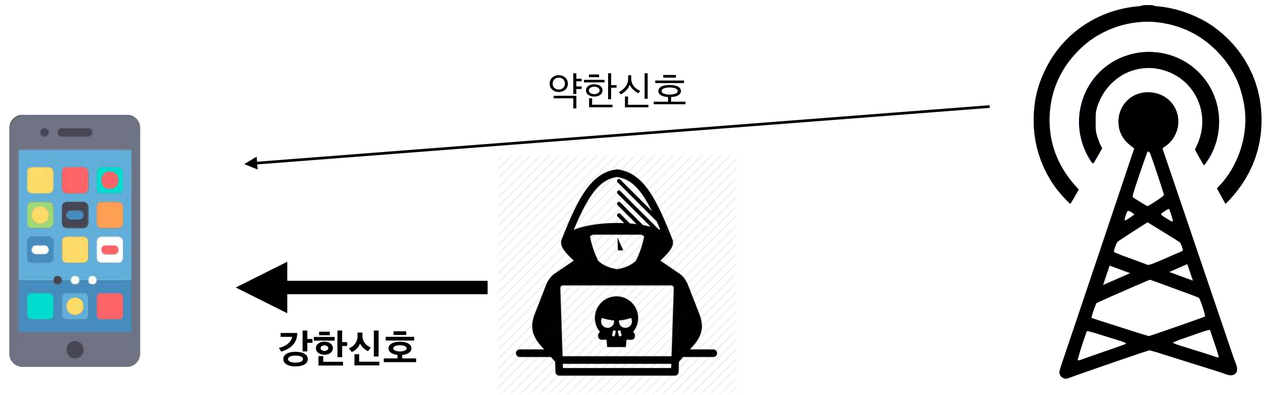
05. LTE - aLTEr




UE
Encapsulate
EEA2
Relay
Commercial Network
Core Network
Internet
Malicious DNS Server
Malicious HTTP Server
Original DNS Server
Original HTTP Server
0
AKA
1
Original destIP
2
3
Manipulated destIP
4
5
Malicious srcIP
Original srcIP

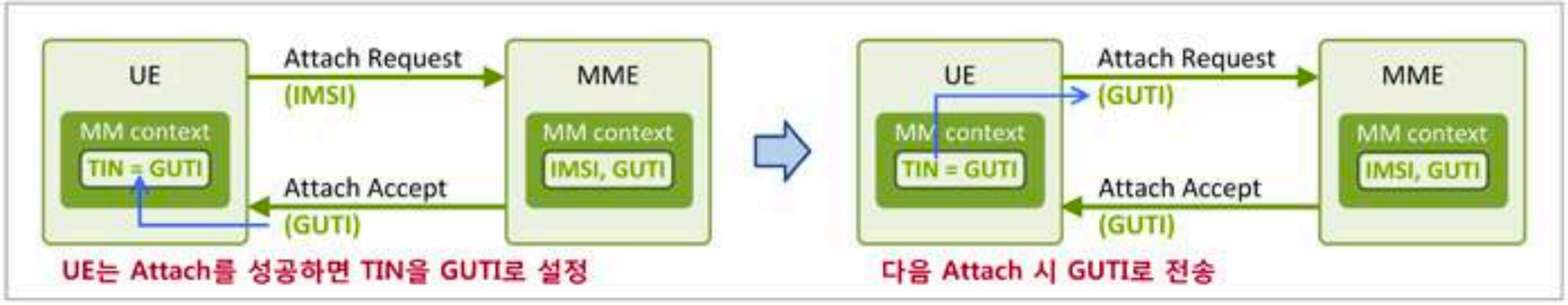
05. LTE - IMSI / GTUI



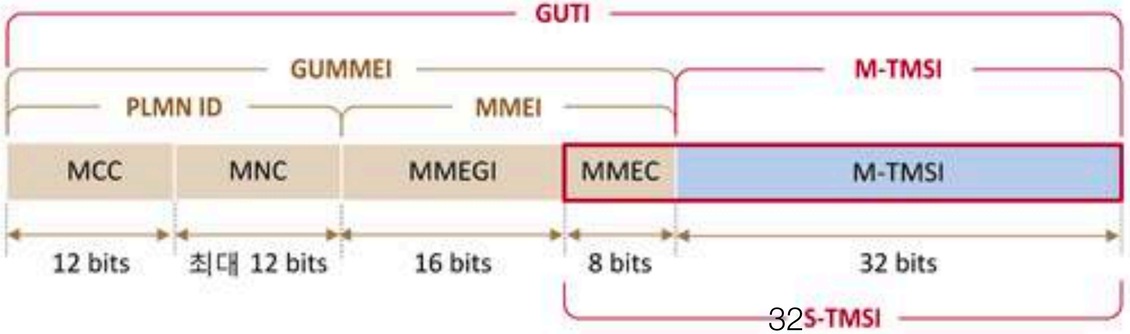


05. LTE - IMSI / GTUI

- GUTI 설정



- GUTI Format



06. 무서운 전파법

ISM 대역

Frequency range		Bandwidth	Center frequency	Availability
6.765 MHz	6.795 MHz	30 kHz	6.780 MHz	Subject to local acceptance
13.553 MHz	13.567 MHz	14 kHz	13.560 MHz	
26.957 MHz	27.283 MHz	326 kHz	27.120 MHz	
40.660 MHz	40.700 MHz	40 kHz	40.680 MHz	
433.050 MHz	434.790 MHz	1.84 MHz	433.920 MHz	Region 1 only and subject to local acceptance
902.000 MHz	928.000 MHz	26 MHz	915.000 MHz	Region 2 only
2.400 GHz	2.500 GHz	100 MHz	2.450 GHz	
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz	
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz	
61.000 GHz	61.500 GHz	500 MHz	61.250 GHz	Subject to local acceptance
122.000 GHz	123.000 GHz	1 GHz	122.500 GHz	Subject to local acceptance
244.000 GHz	246.000 GHz	2 GHz	245.000 GHz	Subject to local acceptance

TMI

→ 중앙전파관리소 민원부
→ 과기부 민원부
→ 방송통신위원회 (전자파시험관 없어짐)
→ 중앙전파관리소 민원부(다시 원점으로;;)
→ 부산전파관리소 검사관리계
→ 서울전파관리소 검사관리계
→ 서울전파관리소 실험국 허가 관리 업무 담당자 (3시 40분에 퇴근;;)
→ (다음날)서울전파관리소 실험국 허가 관리 업무 담당자

- 무선국 개설에만 **최소 6개월;;;**
- **개인이 “사유지” 내 에서 범위를 조절하여(제한적으로) 연구**하는건 문제가없음
- 일반적으로 3mw (6dbi) 를 넘지않으면, 단속에 잡히진 않음. 그러나 **실험국 개설을 권장**
- **국내에서 개인이 LTE/GSM 과 같은 면허대역을 사용해서 전파를 송출하는것은 “무조건” 불법**
- **전파인증을 받은 장치라면 무선국 개설을 할 필요 없음 (SDR은 전파인증 받은 제품이 없..)**

결론

1. 신호 **수신 방법을 알면 송신도 가능**
2. 신호를 **송신하는건 어렵지 않음**
3. 소형 장비의 **신호 대부분은 매우 단순,취약**
4. 연구할때 **꼭 전파법 조심하자**

Q&A

hwymaster01@hanukoon.com

참고자료

- BalCCon2k17 - Nikola Rasovic - Mobile phone surveillance with BladeRF
- hitb2018 - Forcing Targeted LTE Cellphone into Unsafe Network
- DEF CON 23 - Lin Huang and Qing Yang - Low cost GPS simulator: GPS spoofing by SDR
- stealth-cell-tower - juliaoliver
- 3GPP Reference
- RTL-SDR Website
- gps-sim-sdr