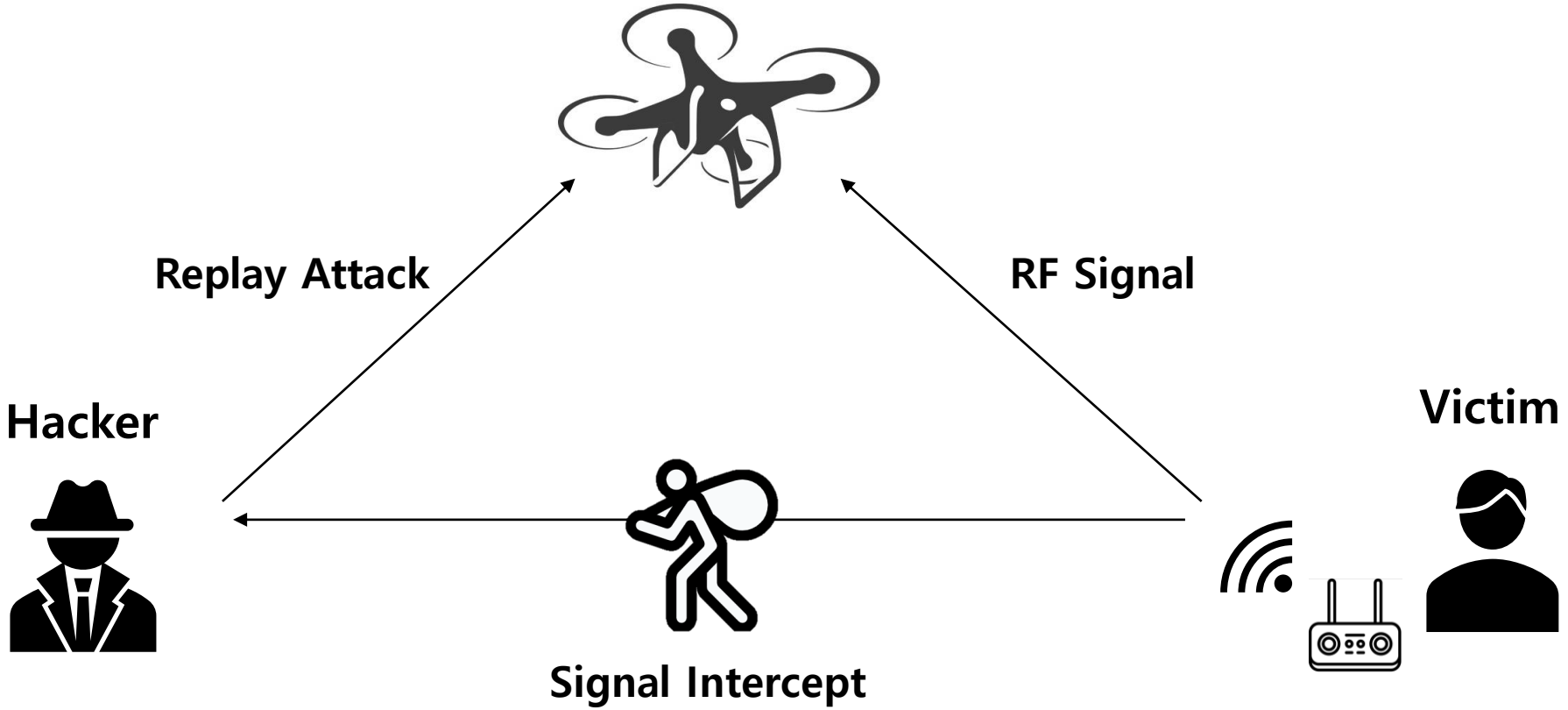
Drone Hacking

CONTENTS

Part 1.

Drone Hacking 개요

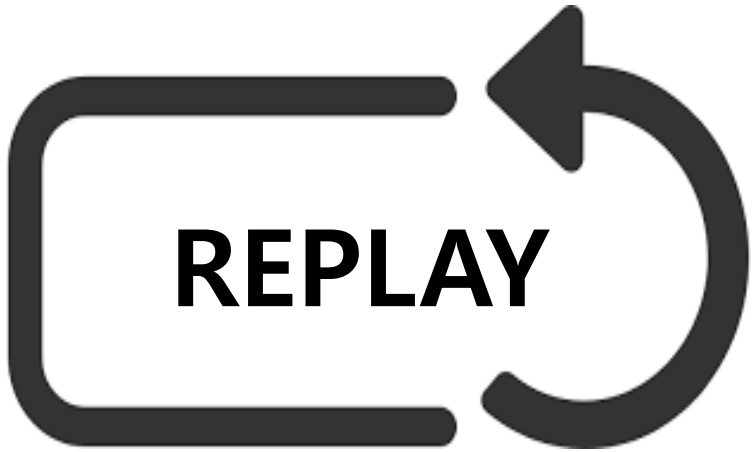
01. Drone Hacking 개요



01. Replay Attack

REPLAY ATTACK이란?

Replay Attack이란 악성 해커가 네트워크를 통해 유효한 데이터 전송을 가로 챈 후 반복하는 사이버 공격입니다.
원래 데이터 의 유효성으로 인해 네트워크의 보안 프로토콜은 해커의 공격을 유효한 데이터인 전송인 것처럼 여기게 됩니다.



Part 2.

Hacking 환경 구축

02. Drone Hacking 환경 구축

HackRF One

HackRF One

10Mhz에서 6Ghz까지의 라디오 신호 송수신이 가능한 SDR(Software Defined Radio) 장치이다. SDR이란 주파수 범위나 변조 방식, 무선 출력 등 주요 무선 특성이 소프트웨어적으로 변경할 수 있는 무선 송수신 장치를 말한다.

Antenna

Antenna 장치로 이 부분에 Antenna를 직접 연결하여 신호를 출력 혹은 입력 받는다.

02. Drone Hacking 환경 구축

GQRX, GNU Radio, Kali linux

Part 3.

Hacking 실습

03. Hacking 실습

HackRF, GQRX, GNU Radio 설치

HackRF 설치

먼저 Kali Linux에 HackRF를 설치해주어야 한다. HackRF를 설치 후 info 명령어를 이용하여 장비의 Serial Number 및 Version과 같은 정보를 파악할 수 있다.

```
root@kali:~# apt-get install hackrf
```

```
root@kali:~# hackrf_info
hackrf_info version: unknown
libhackrf version: unknown (0.5)
Found HackRF
Index: 0
Serial number: 0000000000000000087c867dc2a997a5f
Board ID Number: 2 (HackRF One)
Firmware Version: 2018.01.1 (API:1.02)
Part ID Number: 0xa000cb3c 0x0058434e
```

03. Hacking 실습

HackRF, GQRX, GNU Radio 설치

GQRX 설치

Kali Linux에 GQRX 역시 설치해주어야 한다. GQRX 설치 명령어는 다음과 같다. 설치가 끝난 후 터미널에서 gqrx를 입력하면 프로그램이 실행되는 것을 확인해 볼 수 있다.

```
root@kali:~# apt-get install gqrx-sdr
```

```
root@kali:~# gqrx
Controlport disabled
No user supplied config file. Using "default.conf"
gr-osmosdr 0.1.4 (0.1.4) gnuradio 3.8.0.0
built-in source types: file osmosdr fcd rtl rtl_tcp
ace airspy airspyhf soapy redpitaya freesrp
gr::log :WARN: file_source0 - file size is not a mul
FM demod gain: 3.05577
Resampling audio 96000 -> 48000
IQ DCR alpha: 1.04166e-05
Using audio backend: auto
BookmarksFile is /root/.config/gqrx/bookmarks.csv
[INFO] [UHD] linux; GNU C++ version 9.2.1 20190909;
```

03. Hacking 실습

HackRF, GQRX, GNU Radio 설치

GNU Radio 설치

마지막으로 GNU Radio를 설치해야 한다. GNU Radio를 설치하는 명령어는 다음과 같으며, 설치 후 추가로 osmocom 블록을 설치해주어야 한다. GNU Radio의 실행 명령어는 gnuradio-companion이다.

```
root@kali:~# apt-get install gnuradio
```

```
root@kali:~# apt-get install gr-osmosdr
```

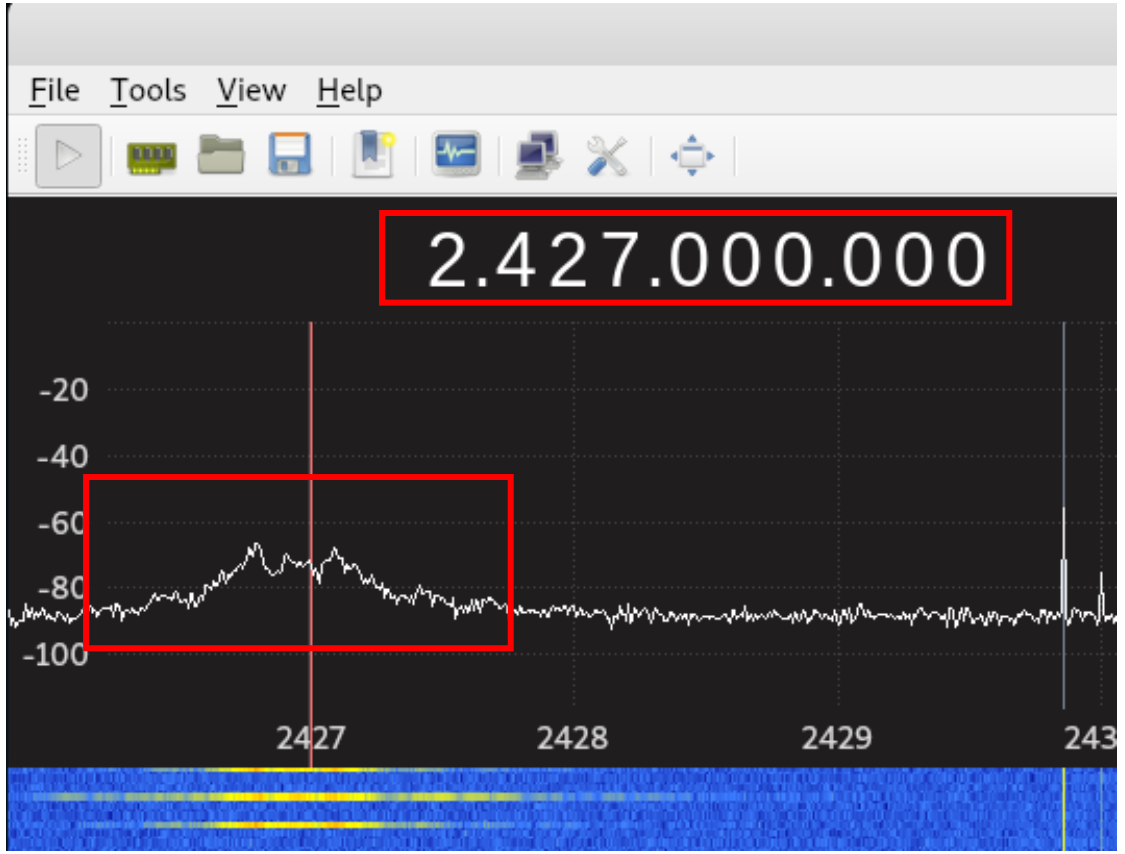
```
root@kali:~# gnuradio-companion
/usr/lib/python3/dist-packages/markupsafe/__init
ing or importing the ABCs from 'collections' ins
s deprecated, and in 3.8 it will stop working
  from collections import Mapping
/usr/lib/python3/dist-packages/yaml/constructor.
g or importing the ABCs from 'collections' inste
deprecated, and in 3.8 it will stop working
  if not isinstance(key, collections.Hashable):
<<< Welcome to GNU Radio Companion 3.8.0.0 >>>

Block paths:
        /usr/share/gnuradio/grc/blocks
```

03. Hacking 실습

GQRX를 이용한 주파수 대역 확인

주파수 대역 확인

먼저 우리는 드론의 주파수 대역을 알아야 한다. 주파수 대역을 모른다면 GNU Radio를 이용하여 통신 시스템을 제작할 때 정확한 드론의 주파수를 잡을 수가 없다.
GQRX를 이용한다면 우리는 드론의 정확한 주파수 대역을 확인할 수 있다.



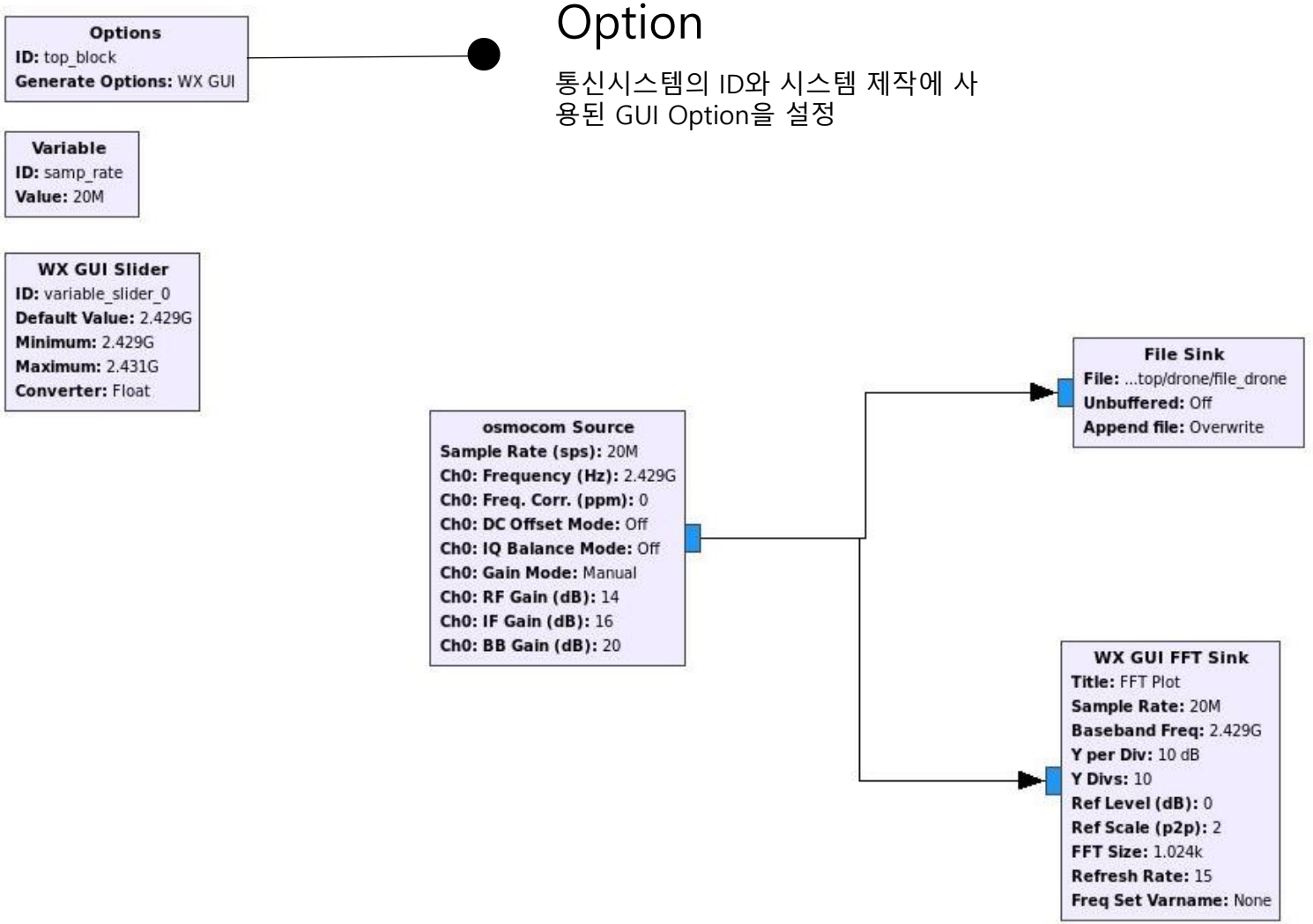
03. Hacking 실습

GNU Radio를 이용한 무선 통신시스템 제작

Record

Replay

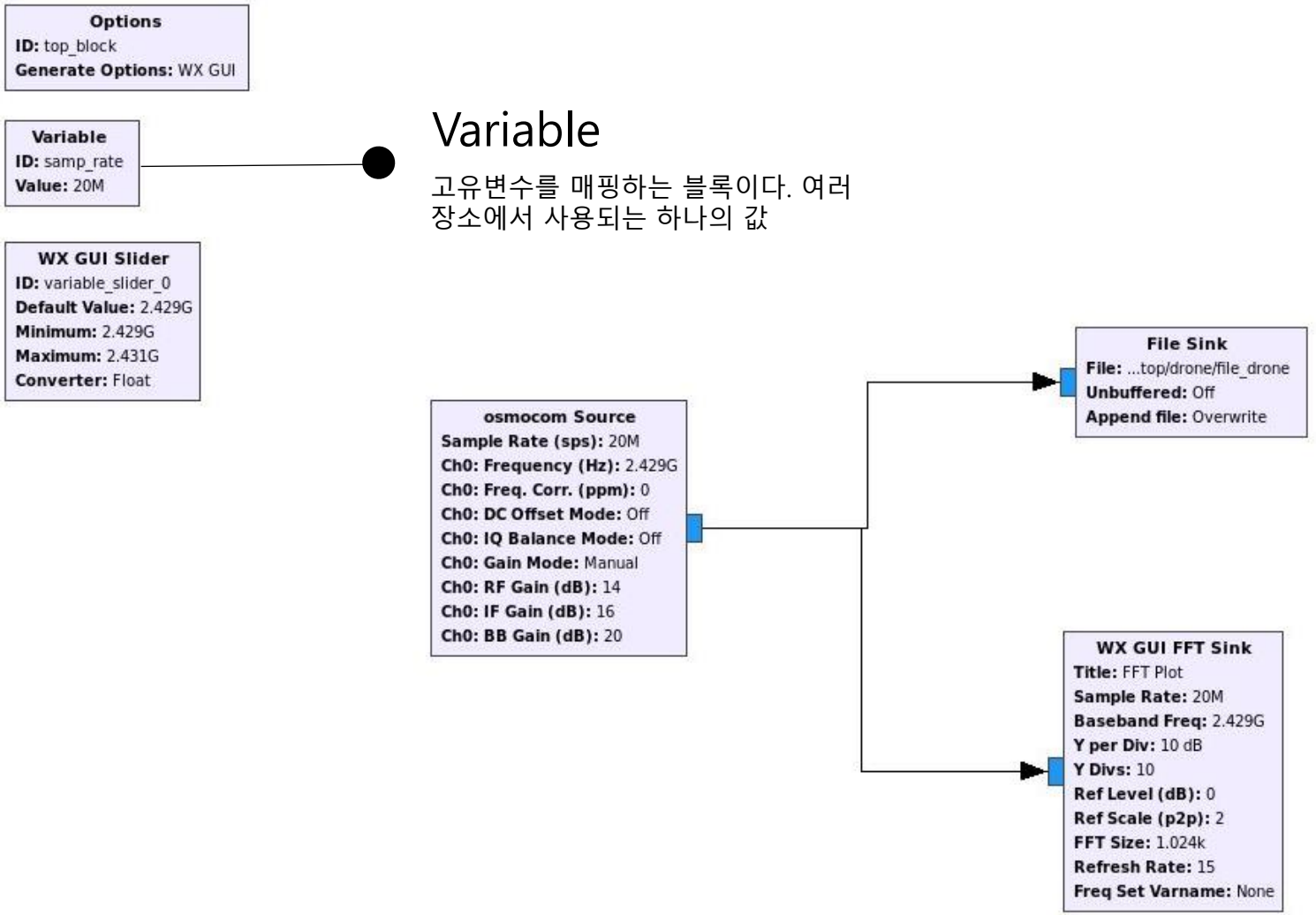
03. Record File



Option

통신시스템의 ID와 시스템 제작에 사용된 GUI Option을 설정

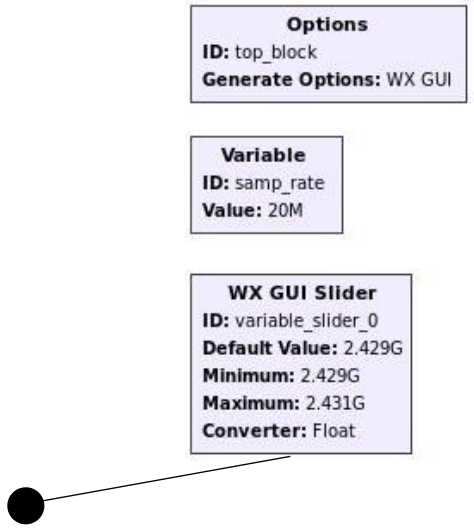
03. Record File



Variable

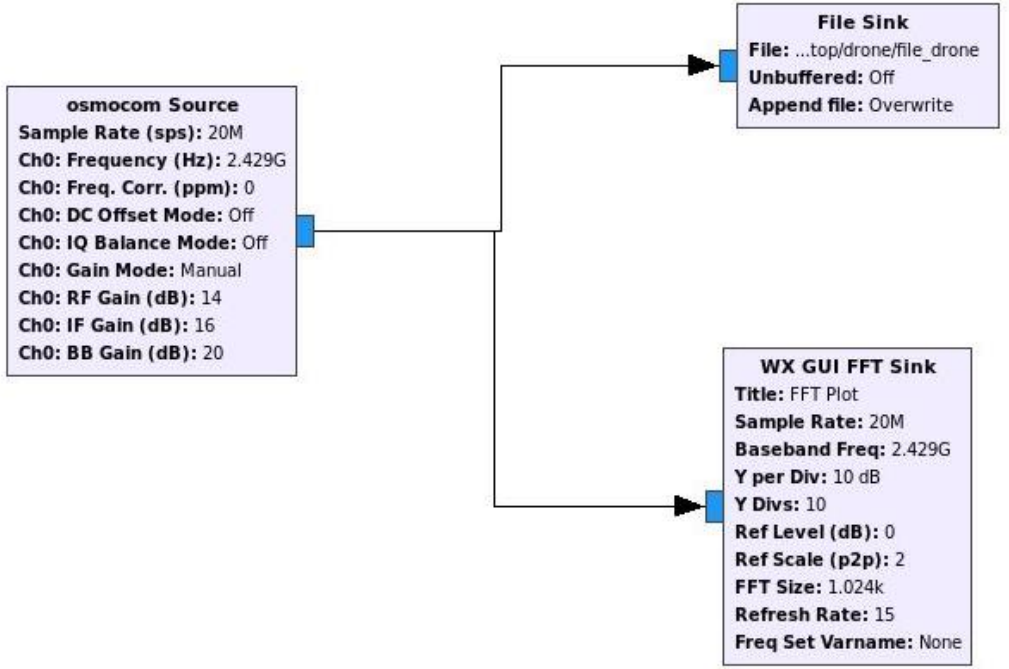
고유변수를 매핑하는 블록이다. 여러 장소에서 사용되는 하나의 값

03. Record File

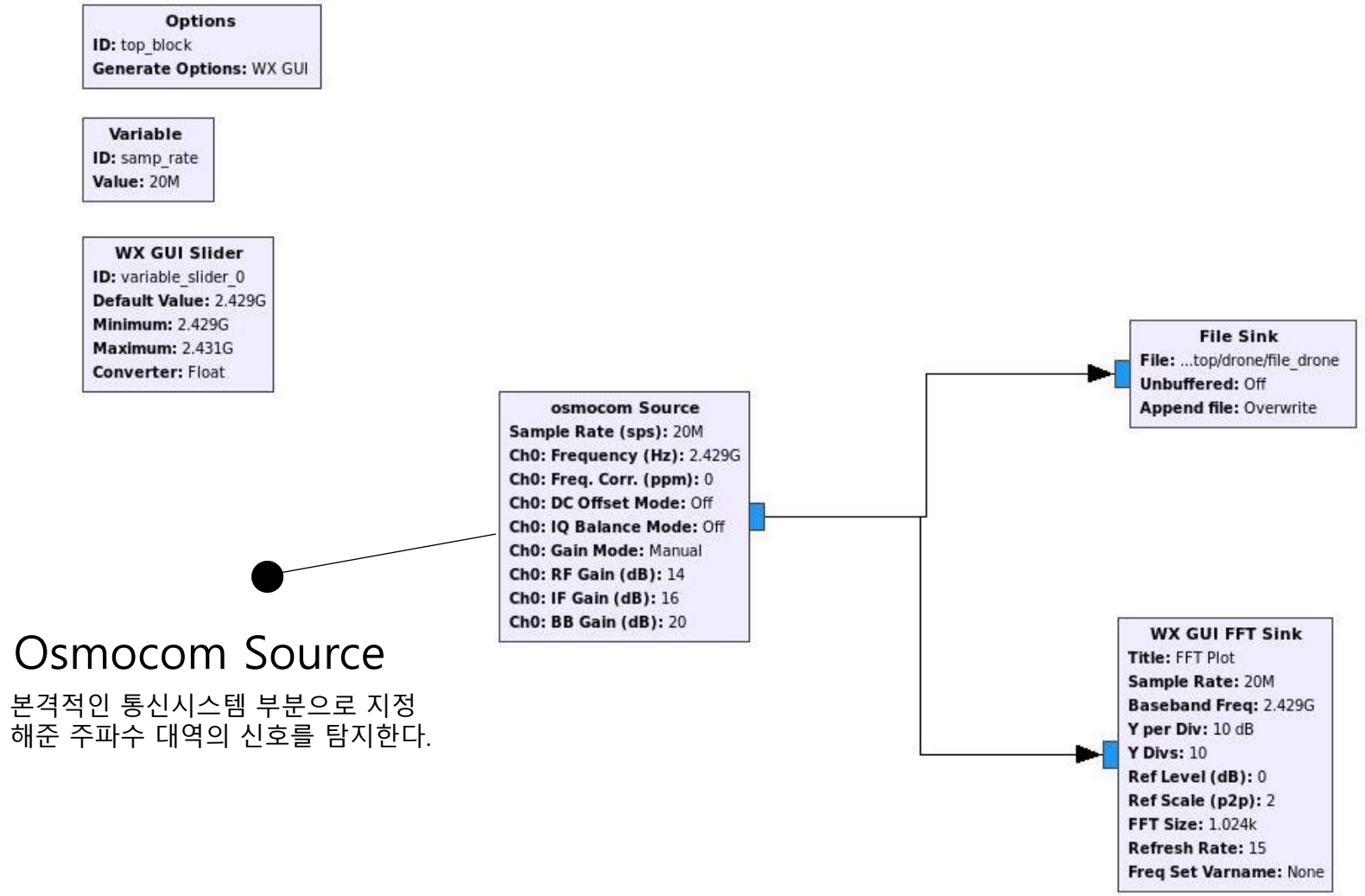


WX GUI Slider

Record 하고 싶은 주파수 대역을 위해 최대값과 최소값을 정하는 블록



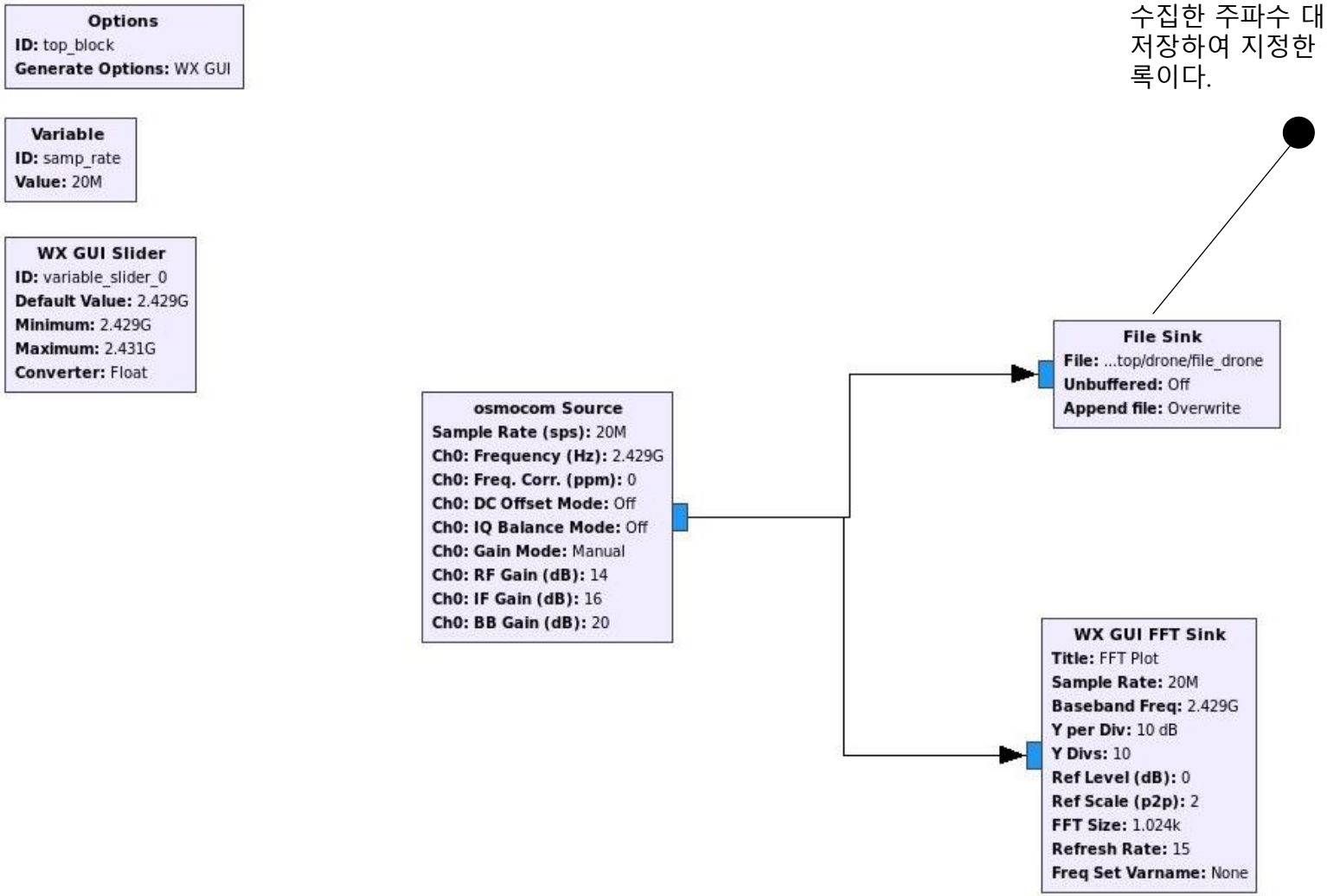
03. Record File



Osmocom Source

본격적인 통신시스템 부분으로 지정
해준 주파수 대역의 신호를 탐지한다.

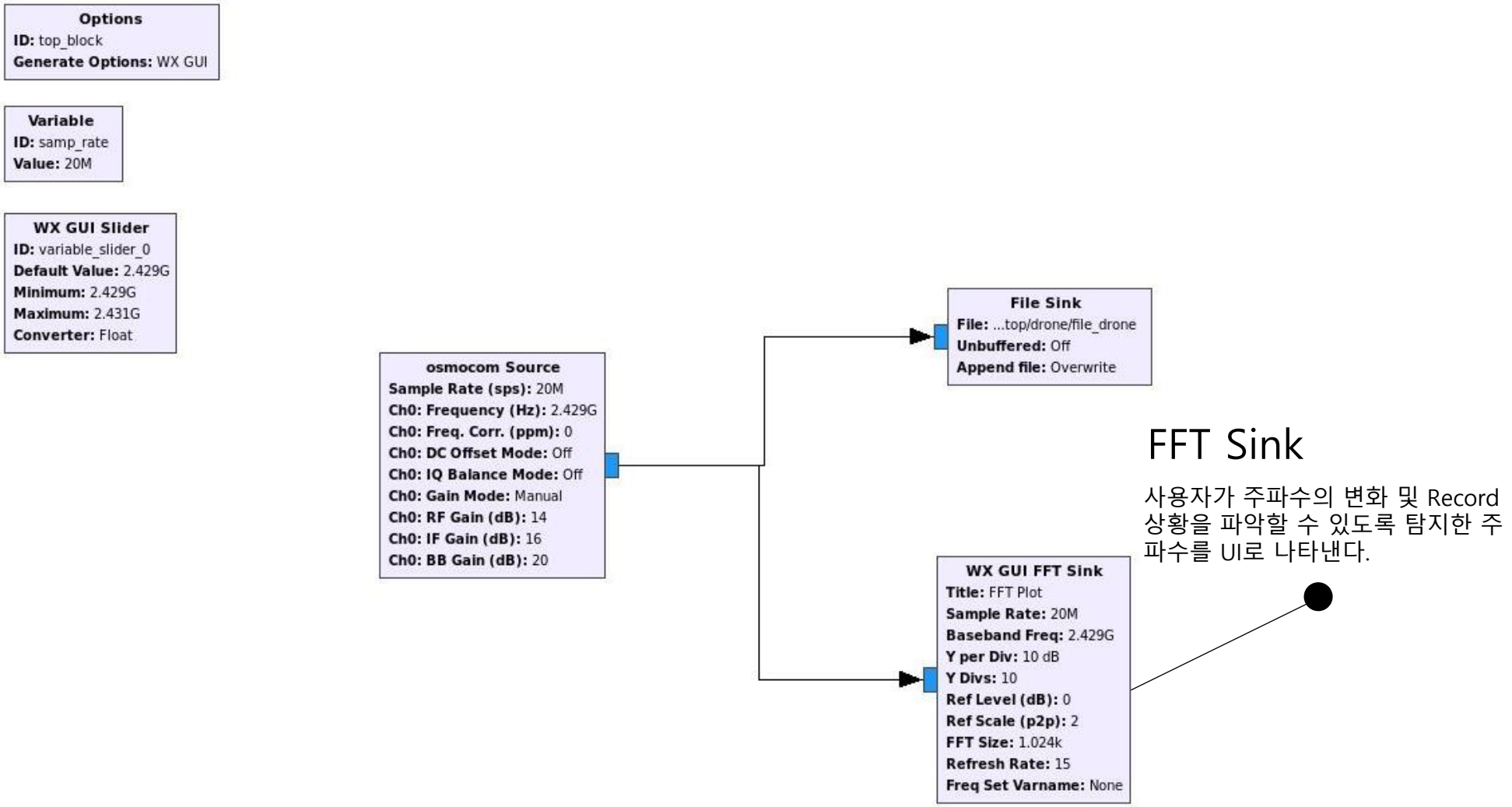
03. Record File



File Sink

수집한 주파수 대역의 신호를 파일로 저장하여 지정한 경로로 저장하는 블록이다.

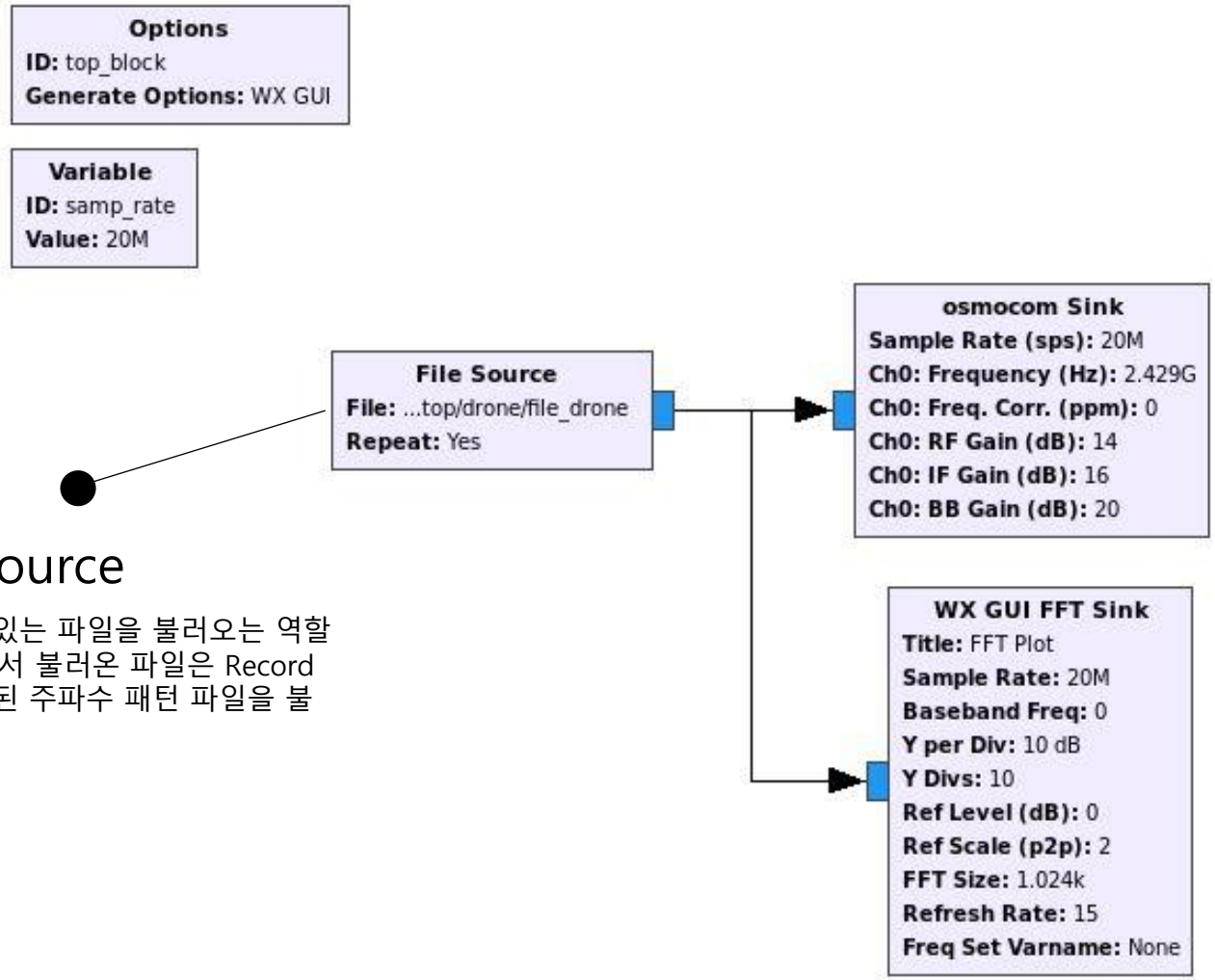
03. Record File



FFT Sink

사용자가 주파수의 변화 및 Record 상황을 파악할 수 있도록 탐지한 주파수를 UI로 나타낸다.

03. Replay File



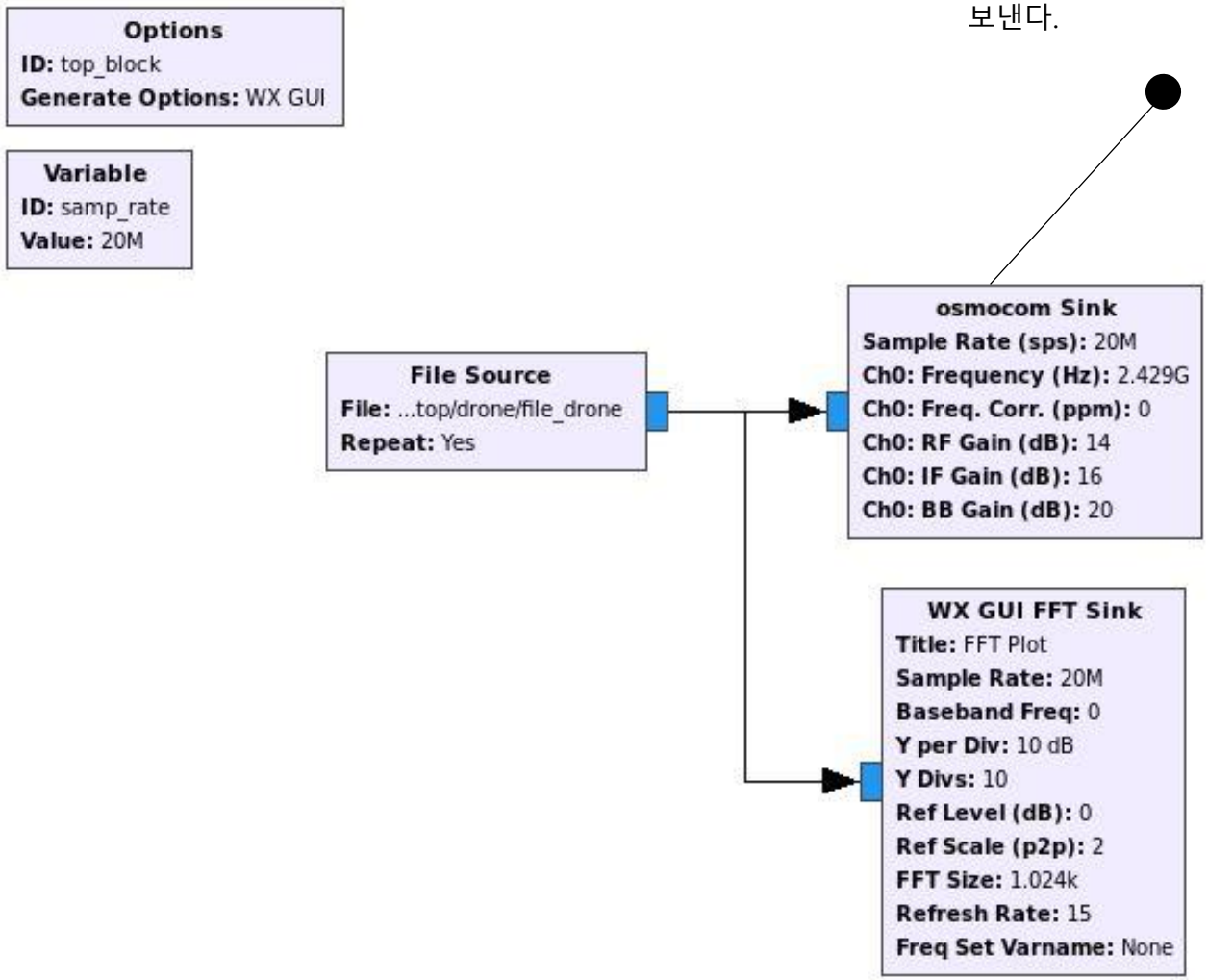
File Source

저장되어 있는 파일을 불러오는 역할이다. 여기서 불러온 파일은 Record에서 저장된 주파수 패턴 파일을 불러온다

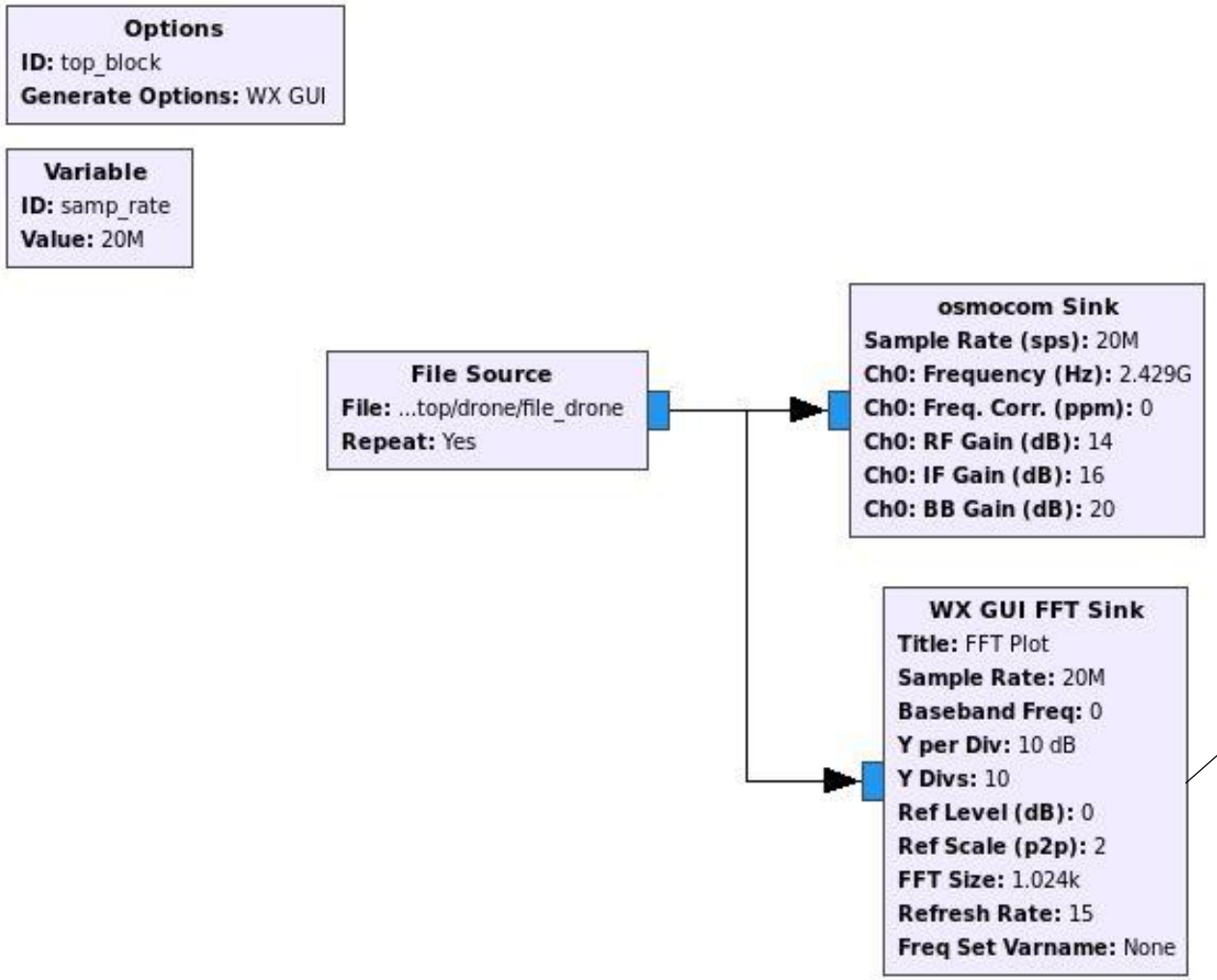
03. Replay File

Osmocom Sink

불러온 파일에서 주파수를 가공해 HackRFOne 장비를 이용해 주파수를 보낸다.



03. Replay File



FFT Sink

사용자가 주파수의 변화 및 Replay 상황을 파악할 수 있도록 탐지한 주파수를 UI로 나타낸다.

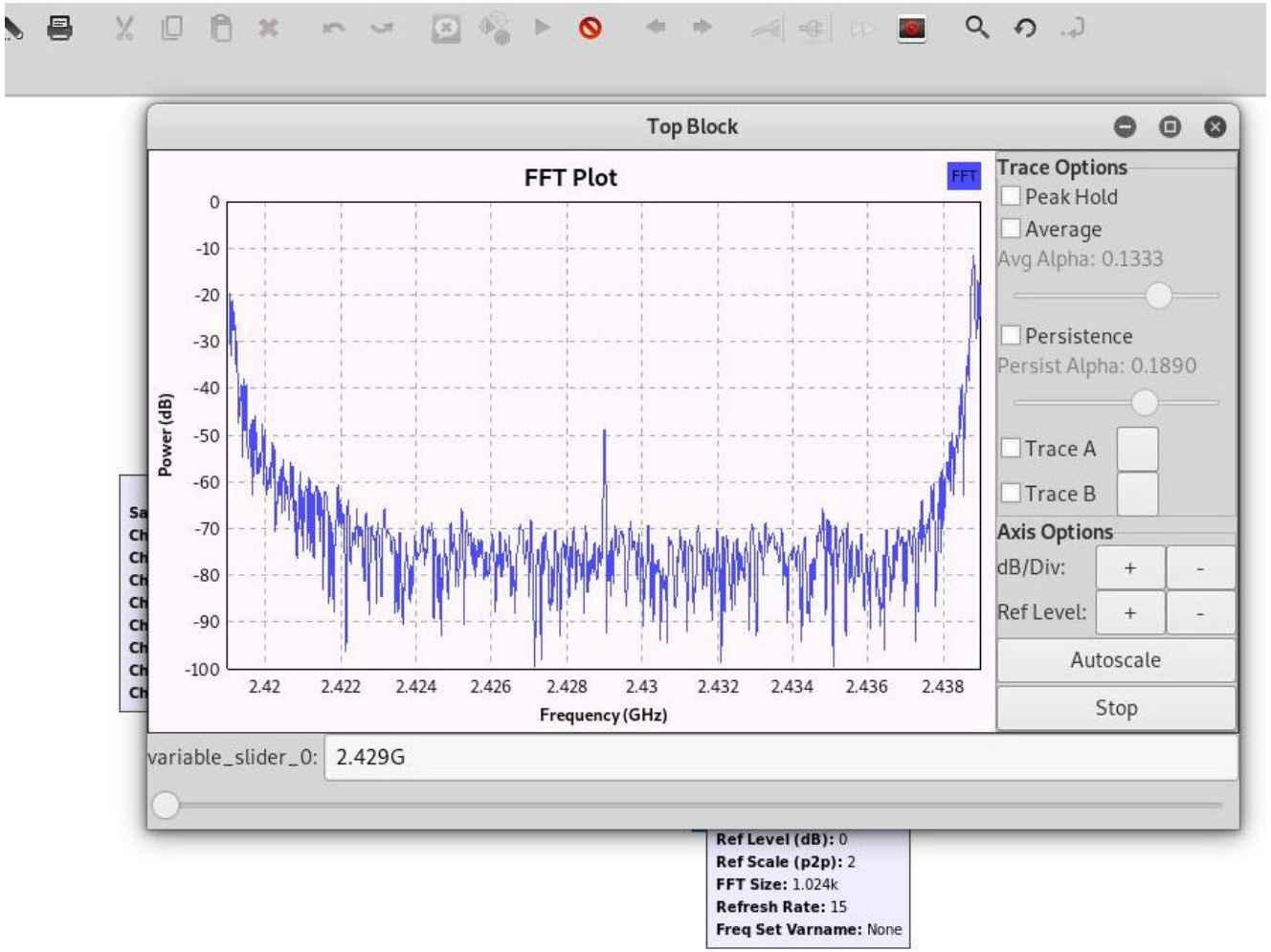
03. Hacking 실습

Record File을 이용한 주파수 탈취

Record File 실행

Record File을 만든 후 실행시키면 다음과 같은 UI가 나타난다. 이때 드론을 조종한다면 FFT Plot의 그래프가 요동치는 현상을 확인할 수 있다.

적당한 시간이 지난 후 오른쪽 하단에 Stop을 누르면 Record가 끝난다.

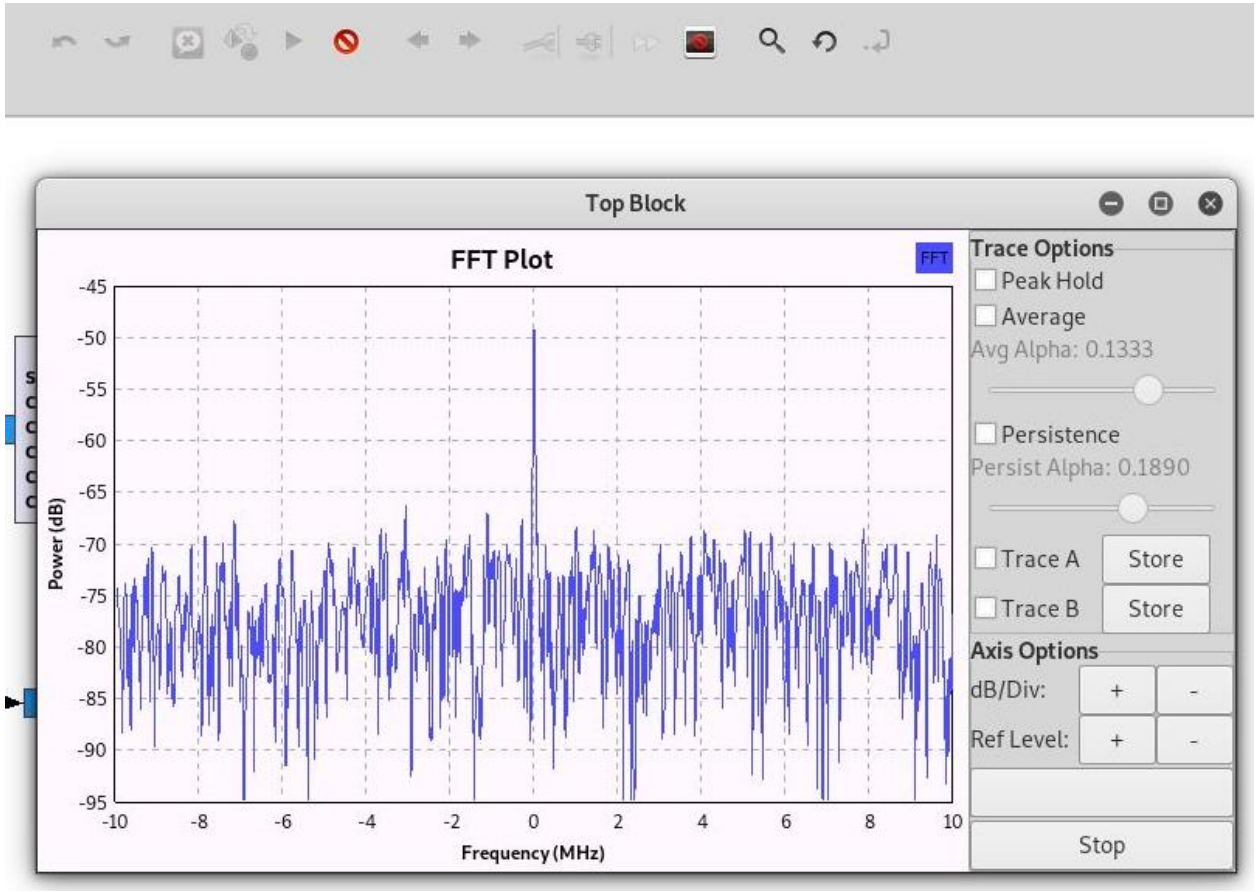


03. Hacking 실습

Replay File을 이용한 드론 조작

Replay File 실행

Record를 진행한 후 Replay File을 실행시키면 다음과 같은 UI가 나타난다. 이후 Record된 주파수로 인해 드론이 자기 멋대로 움직이는 현상을 확인할 수 있다. 오른쪽 하단에 Stop을 누르면 더 이상 주파수를 보내지 않는다.



Part 4.

Drone Hacking 대응방법

04. Drone 활용 사례

Drone의 다양한 활용 사례

04. Drone 활용 사례

Drone 시장의 성장 규모

성장하는 드론 시장

왼쪽의 그래프는 전 세계 드론 시장의 규모 전망을 나타낸다. 정부는 드론 시장이 앞으로 5년간 50% 이상 성장할 것이라고 예측하였으며, 많은 기업 혹은 정부들이 드론 사업에 투자할 것이라고 발표하였다.

드론은 민간 사업, 군사 사업, 농업 등 활용 분야가 매우 다양하여 계속 성장할 가능성이 매우 큰 시장이라고 할 수 있다.

04. Drone 활용 사례

Hacking에 취약한 Drone

Spoofing

2011년 12월 이란은 이란 영공을 정찰하던 미국 공군 최첨단 드론을 GPS 조작으로 탈취했다고 밝혔다. 이란은 드론의 GPS 연결을 차단하고 자동 비행 모드로 전환하길 기다렸다가 다시 암호화되지 않은 GPS 주파수를 찾도록 조작했다.

Jamming

2012년 5월 인천 송도에서 시험 비행하던 중이던 무인항공기가 추락해 외국인 원격조종사 1명이 숨지고 한국인 2명이 다쳤다. 원인은 북한의 전파 교란으로 GPS 수신 불능으로 인한 추락으로 추정하고 있다.

Hijacking

2016 팩섹(PacSec)에서 레저용 드론들을 마구잡이로 해킹해 마음대로 조종하는 상황을 시연한 적이 있다. 드론을 포함해 원격조종기로 움직이는 어떤 기기라도 통신 프로토콜을 장악해 해킹하는 '이카루스(Icarus)'시스템을 공개했다.

Drone Hacking 대응방안

- GPS 송수신기 상호 인증을 이용하면 신호에 대한 무결성을 증명할 수 있다.
- 데이터 암호화를 이용하여 주파수 탈취를 막을 수 있다.
- SecureOS 및 역공학 차단을 이용한다면 물리적 위협 역시 방어가 가능하다.

THANK YOU