



# FM 라디오 전파 하이재킹

(with HackRF One)



중부대학교 SCP 정보보안 동아리  
2학년 부원 노무승

# 목 차

---

## 1. 환경 구축

1-1. HackRF One

1-2. GNU Radio

1-3. 환경 구축 (HackRF, GNU Radio, SDR#)

## 2. FM이란?

2-1. FM?

2-2. FM 라디오

## 3. FM 라디오 수신

## 4. FM 라디오 하이재킹

4-1. GNU Radio Design

4-2. 실습 영상



## 1. 환경 구축

## 1-1. HackRF One


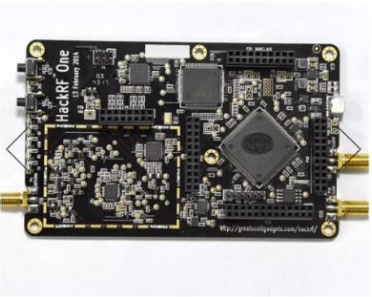


HackRF One은 1Mhz에서 6Ghz까지의 전파 송수신이 가능한 SDR(Software Defined Radio) 장치이다.

✓ 송신 기능이 있는 SDR 중 가격이 가장 저렴하다.

✓ 대신 반이중(Half-Duplex) 통신만 지원한다.

(Blade RF SDR은 전이중(Full-Duplex) 통신을 지원한다. 가격은 60만 원)





**HackRF One 기반 소프트웨어 정의 라디오  
(SDR based on HackRF One)**


판매가(VAT별도) **238,000원**

상품코드 P0000XKC

상품요약정보 HackRF One 기반 SDR 보드 입니다.

SNS 상품홍보  

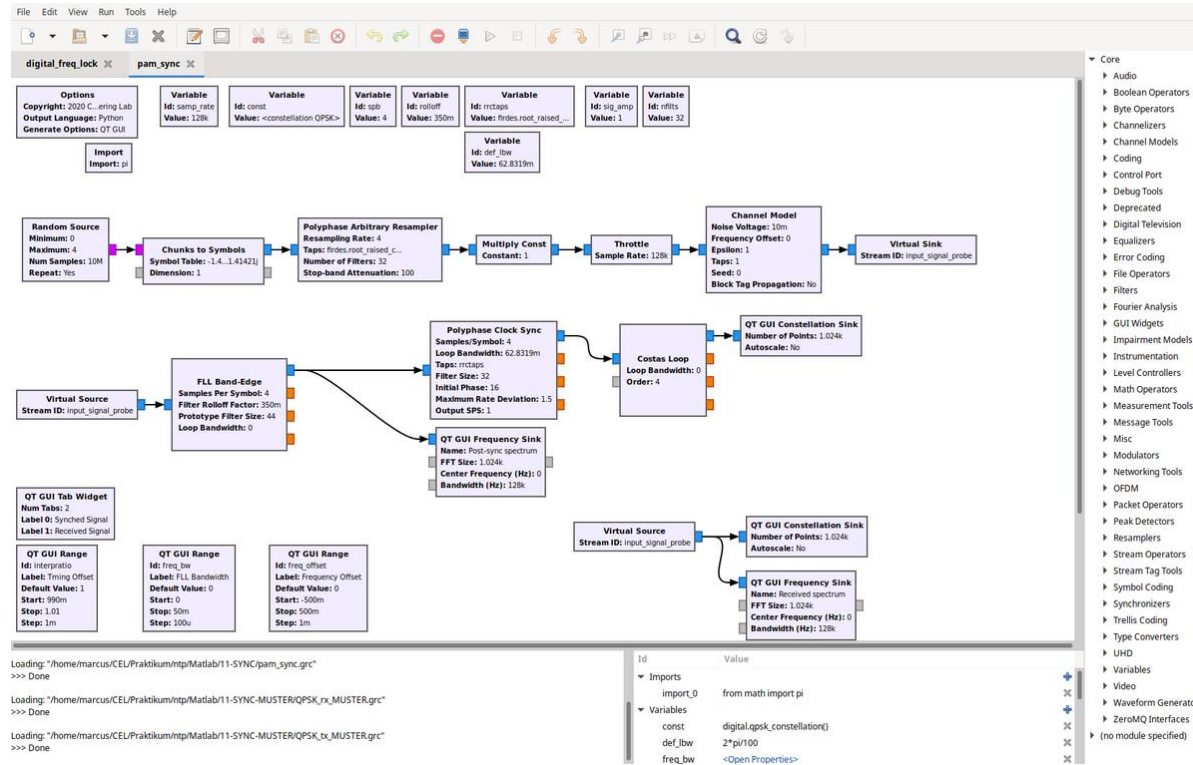
(최소주문수량 1개 이상)

 수량을 선택해주세요.

HackRF One 기반 소프트웨어 정의 라디오 (SDR based on HackRF One)  **238,000원**

총 상품금액(수량) : **238,000원** (1개)

# 1-2. GNU Radio



HackRF 도구로도 충분히 간단한 RF Replay Attack을 수행할 수 있지만,  
조금 더 자세한 작업을 하기 위해서는 GNU Radio라는 도구로 SDR을 컨트롤할 수 있다.

## 1-3. 환경 구축 (우분투 20.04 - hackrf)

```
apt install -y hackrf libhackrf-dev libhackrf0
```

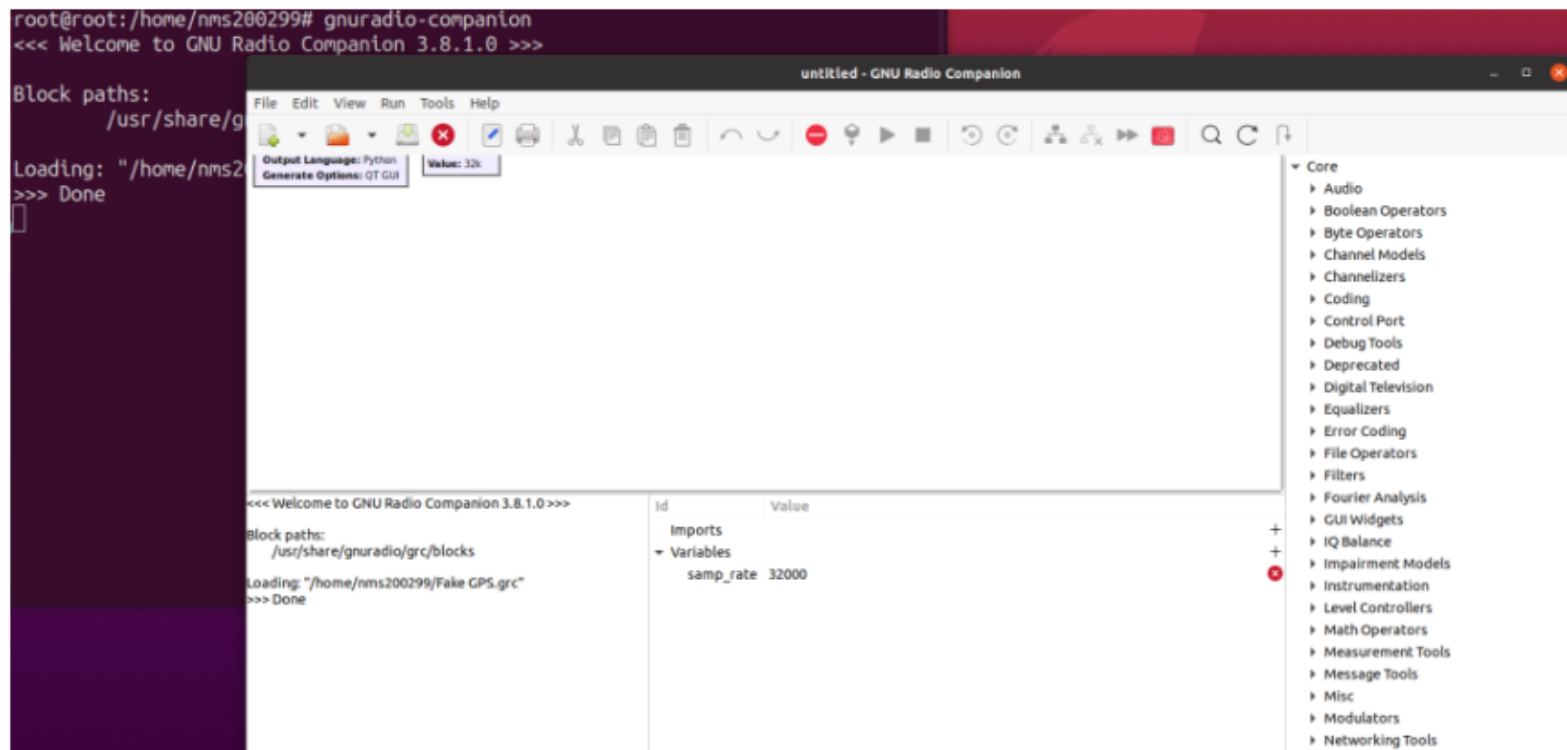


```
root@root:/home/nms200299# hackrf_info
hackrf_info version: unknown
libhackrf version: unknown (0.5)
Found HackRF
Index: 0
Serial number: 000000000000000000a27466e6296b310f
Board ID Number: 2 (HackRF One)
Firmware Version: 2015.07.2 (API:1.00)
Part ID Number: 0xa000cb3c 0x00774f68
```

'hackrf\_info' 명령

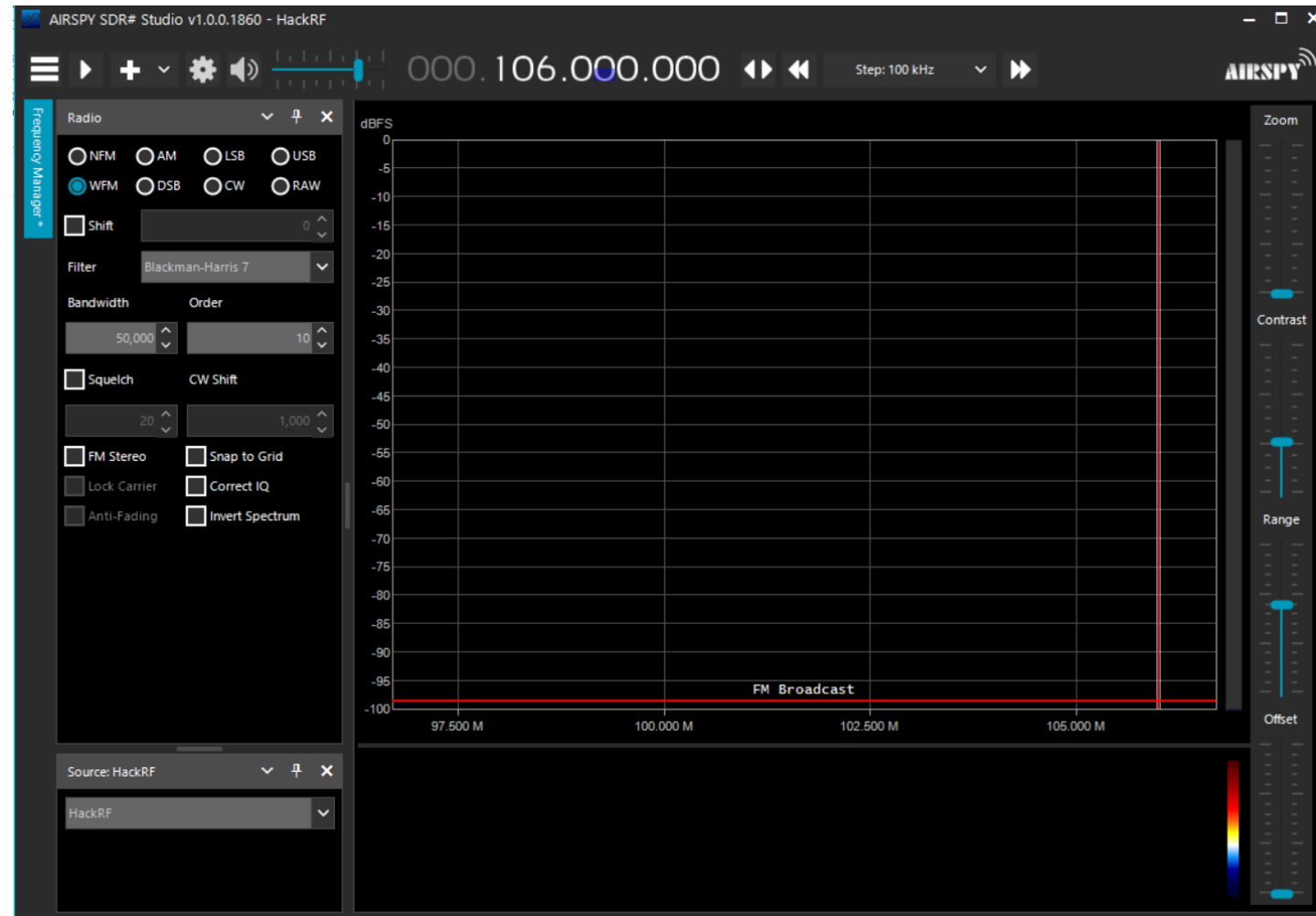
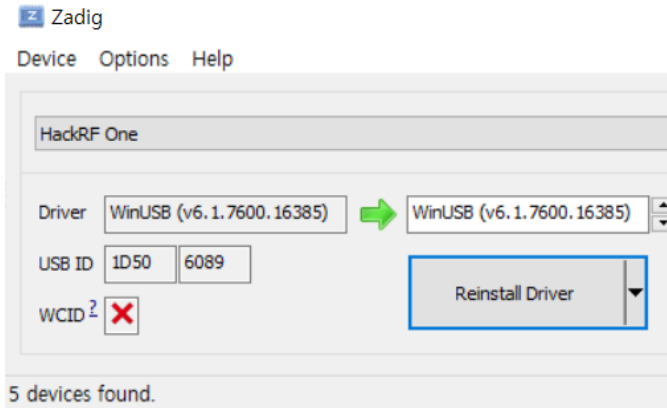
## 1-3. 환경 구축 (우분투 20.04 - GNU Radio)

```
apt install -y gnuradio gr-osmosdr
```



'gnuradio-companion' 명령

## 1-3. 환경 구축 (Windows 10 – SDR#)







## 2. FM이란?

## 2-1. FM이란?

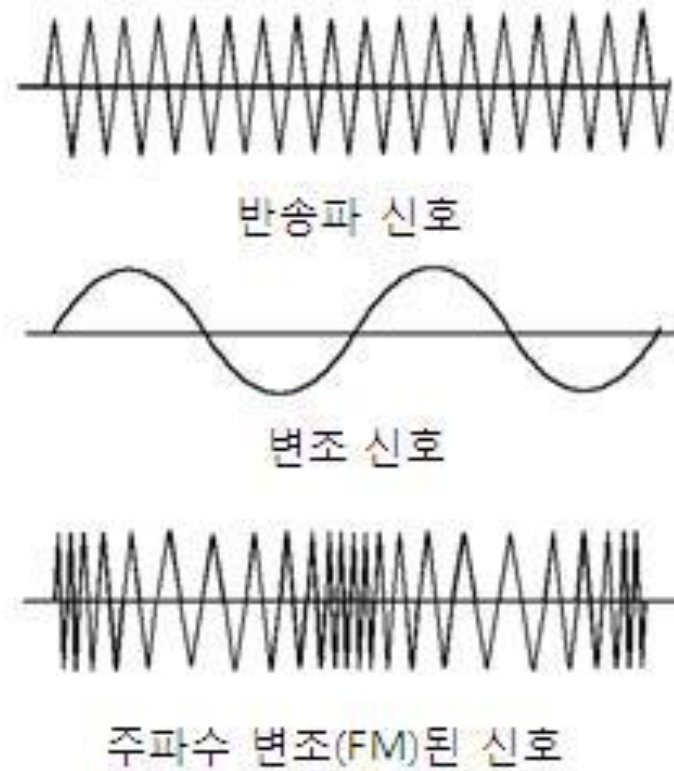
### 1. 주파수 변조 (Frequency Modulation, FM)

- 반송파의 순시주파수  $f_i(t)$ 를 원 신호  $m(t)$ 로 변조하는 방식
  - 반송파 주파수 주변에서 입력 신호에 따라 주파수를 순시적으로 변화시키며 변조

### 3. 주파수변조(FM)의 진폭변조(AM) 방식에 대한 장단점 비교

- 장점
  - 진폭변조(AM)에 비해 이득, 선택도, 감도가 우수
  - 저 전력 변조를 함으로써, 소비 전력이 AM 보다는 적음
  - 페이딩의 영향을 덜 받음
- 단점
  - 송수신기의 회로가 복잡함
  - 주파수대역폭(점유폭)이 넓음

## 2-1. FM이란?



## 2-2. FM 라디오

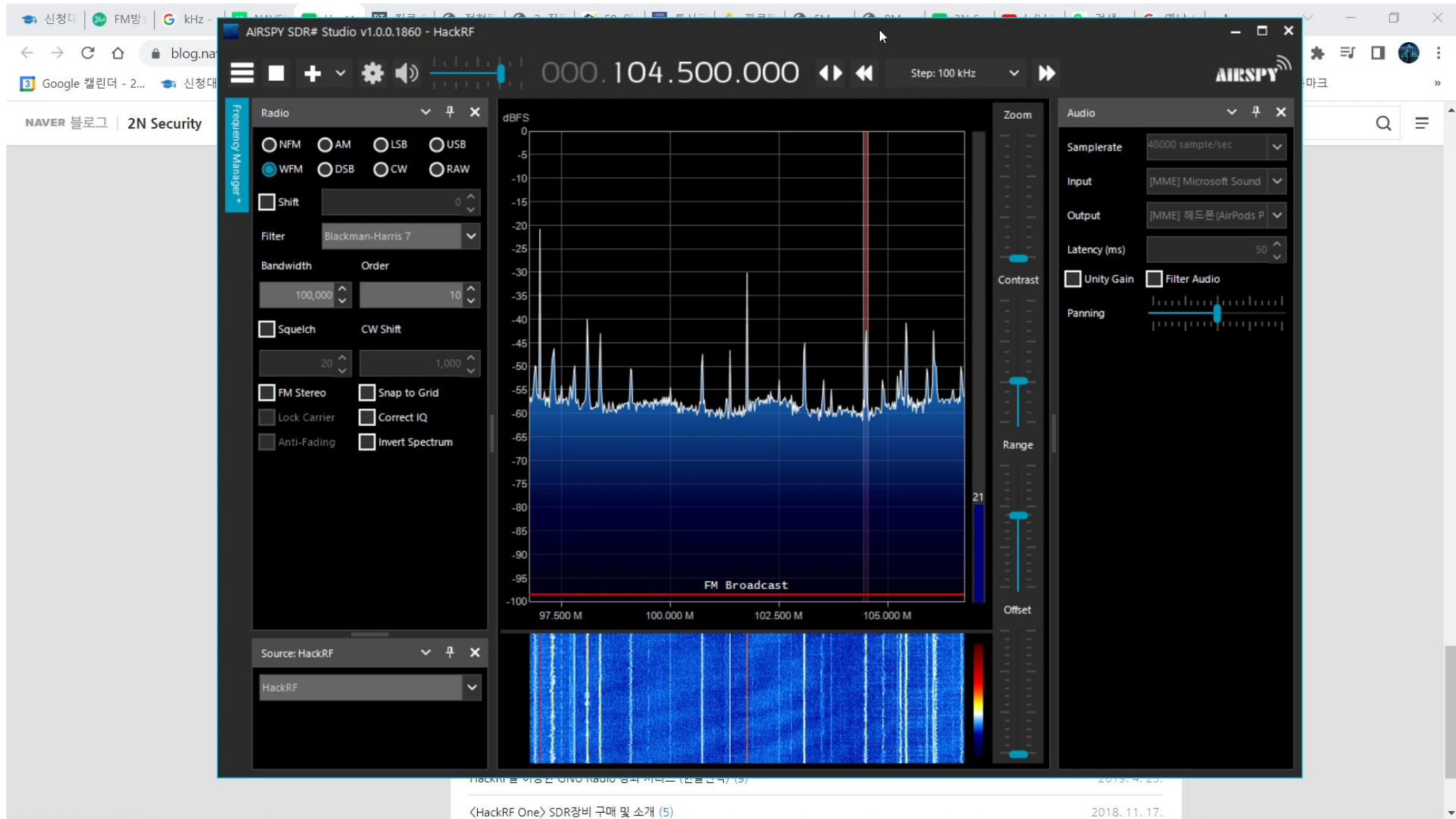


FM 변조 방식을 사용한 라디오로 국제 표준 주파수 대역은 87.5~108 MHz 대역이고, 현재 우리나라에서는 87.7 ~ 107.9 MHz 사이에서 200 kHz씩 나뉘어서 사용한다.



### 3. FM 라디오 수신

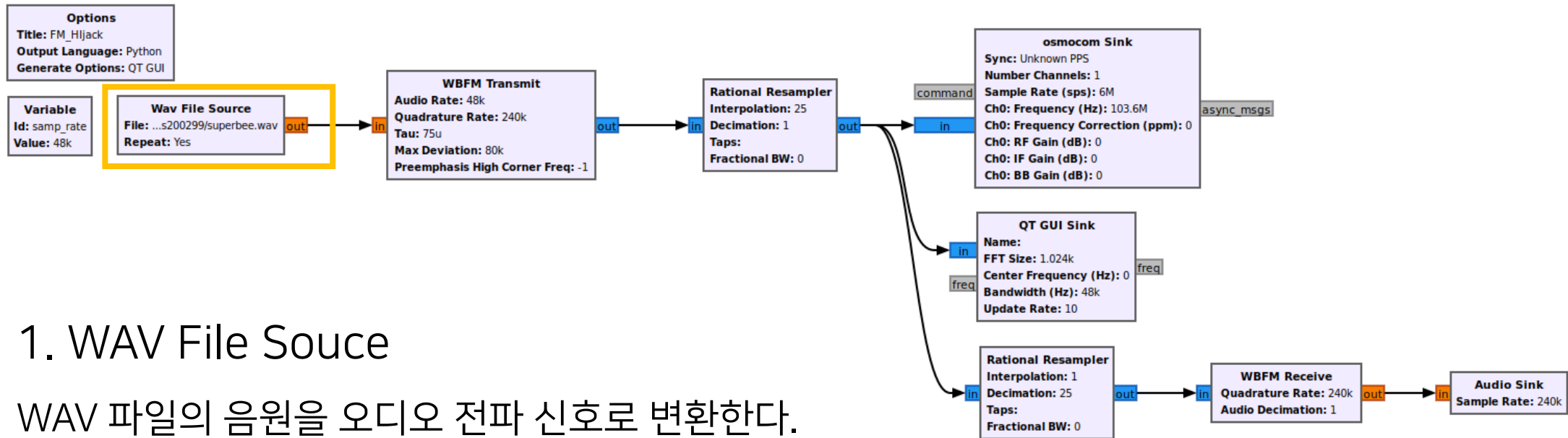
### 3. SDR#을 이용한 FM Radio 수신





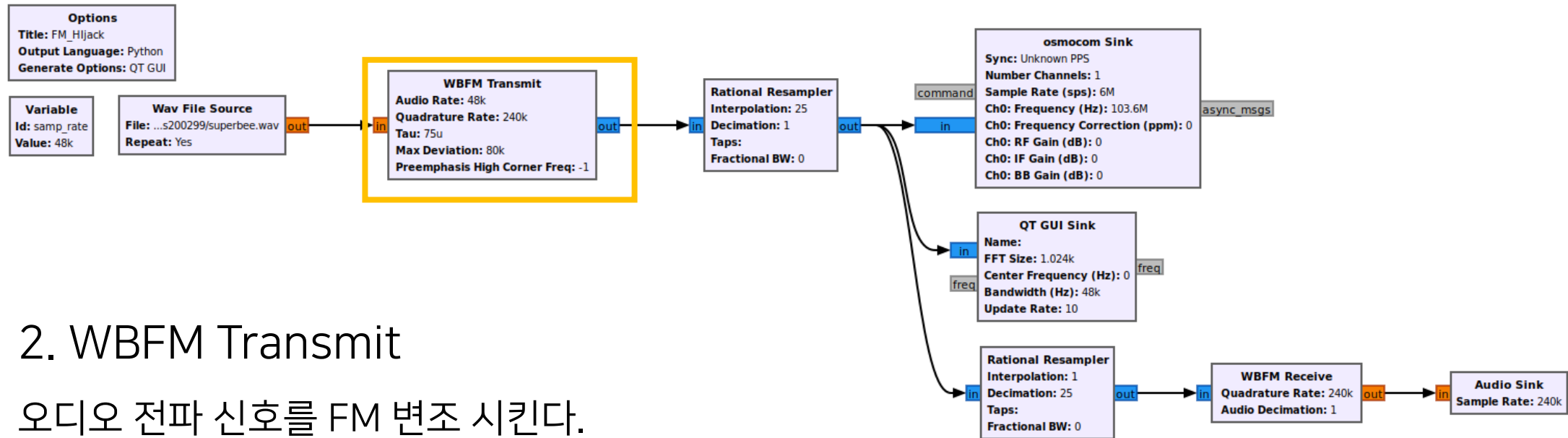
## 4. FM 라디오 하이재킹

# 4-1. GNU Radio Design





## 4-1. GNU Radio Design

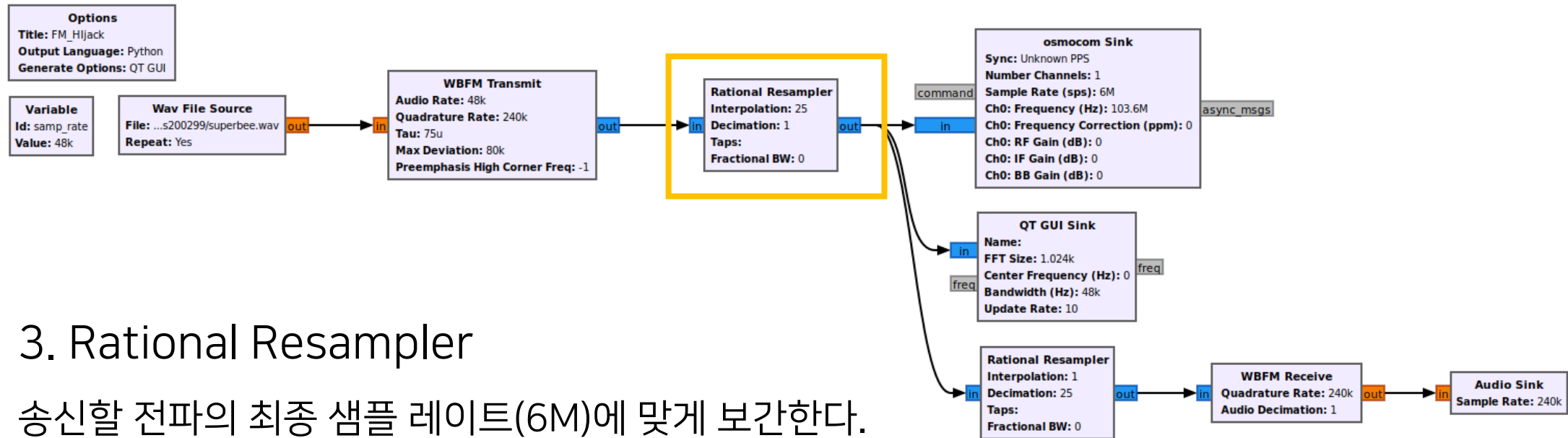


### 2. WBFM Transmit

오디오 전파 신호를 FM 변조 시킨다.

오디오의 샘플 레이트는 48k인데, 표준 편차(80k)를 감안하여  
FM 변조 후 샘플 레이트는 240k로 설정한다.

## 4-1. GNU Radio Design

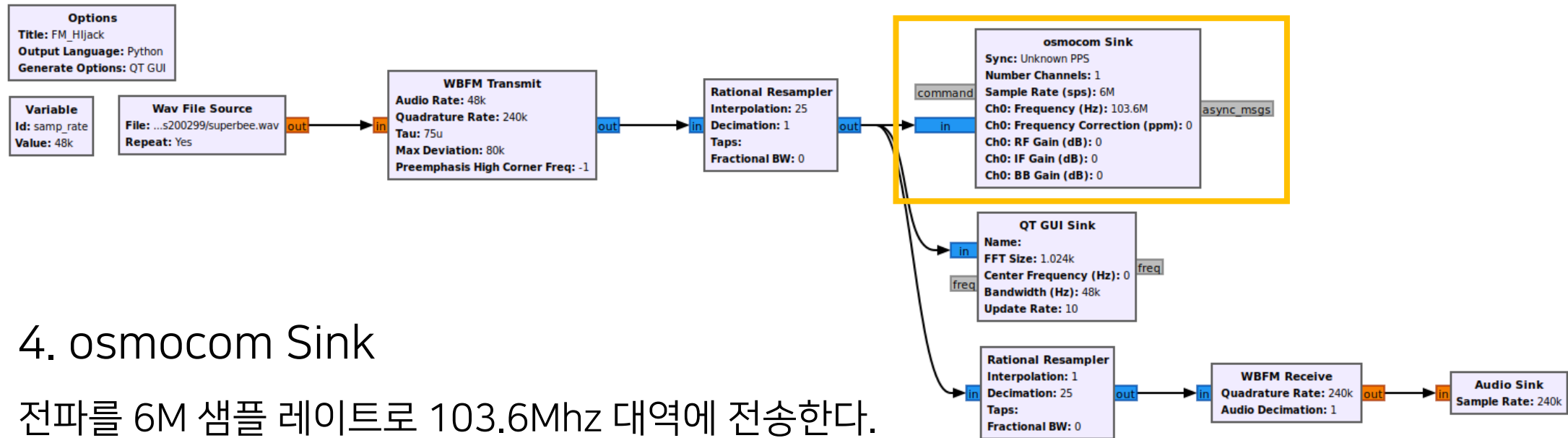


### 3. Rational Resampler

송신할 전파의 최종 샘플 레이트(6M)에 맞게 보간한다.

( $240k * 25 = 6M$ )

## 4-1. GNU Radio Design

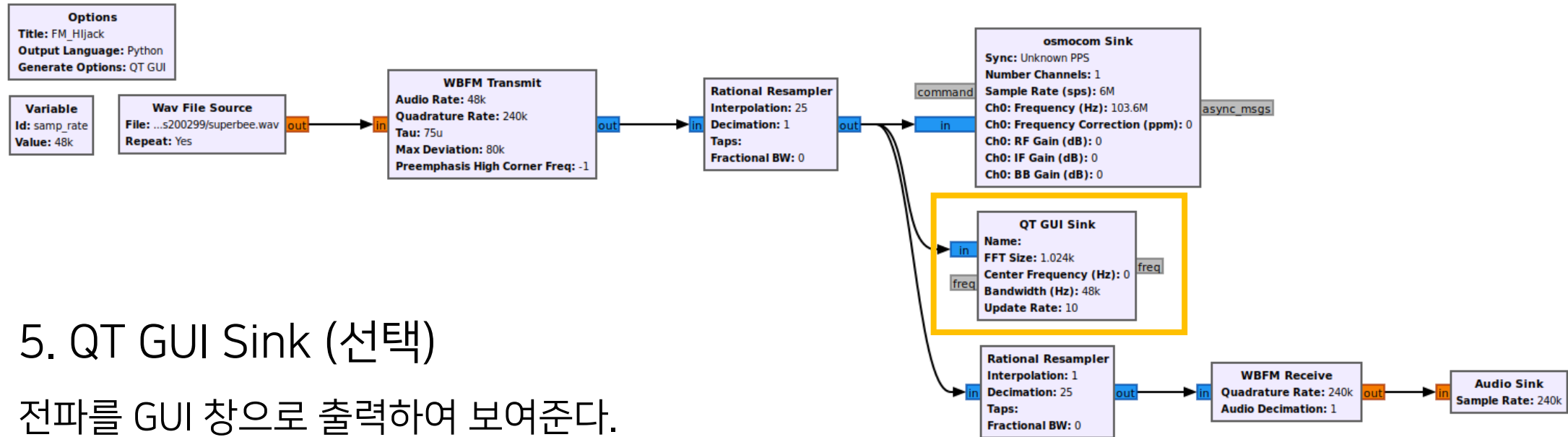


### 4. osmocom Sink

전파를 6M 샘플 레이트로 103.6Mhz 대역에 전송한다.

HackRF SDR을 통해 실제로 전파가 전송되는 부분이다.

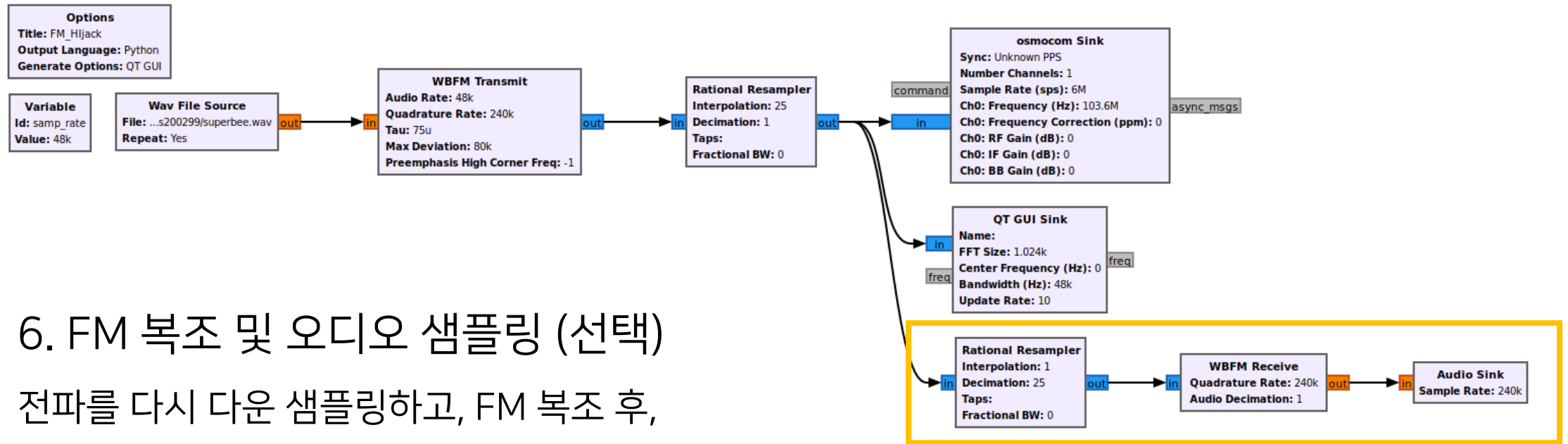
## 4-1. GNU Radio Design



### 5. QT GUI Sink (선택)

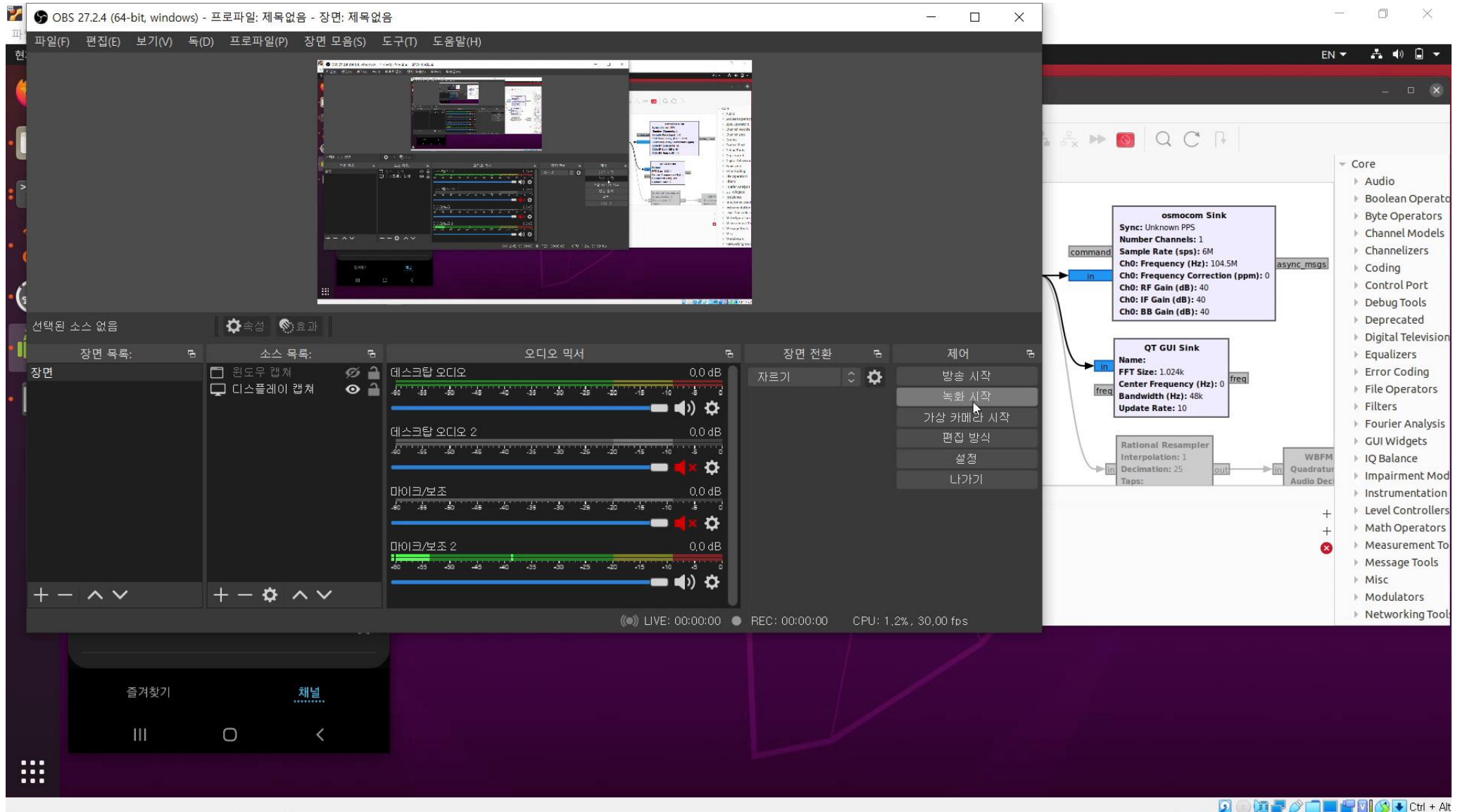
전파를 GUI 창으로 출력하여 보여준다.

## 4-1. GNU Radio Design



6. FM 복조 및 오디오 샘플링 (선택)  
전파를 다시 다운 샘플링하고, FM 복조 후,  
오디오를 샘플링하여 스피커에 출력한다.

## 4-2. 작동 영상





Q & A





감사합니다

