Wireless Security Lab 7 Revised with SDR Edition

Wireless Device Management

Weight: 1.15% Marks: /78

Student Name:

Student ID: Date:

# Introduction

In this lab, there are two sections. In the first you will focus on security protocols and denial of service identification. In the second part, you will setup the Nooelec SDR radio, tune to an FM station and others.

Your task is to

1. watch the links below and answer the questions.
2. Perform the tasks related to SDRs

# Equipment

* Nooelec SDR radio,
* Windows Laptop with USB to run SDR software. There are links below for the Airspy SDR monitoring software. Alternatives can be found on these links:

<http://www.hdsdr.de/>

<https://github.com/AlexandreRouma/SDRPlusPlus> (betaware)

<http://www.sm5bsz.com/linuxdsp/linrad.htm> (Linux Radio)

<https://gqrx.dk/>

<https://github.com/cjcliffe/CubicSDR>

# Lab Setup

Before you begin the lab activities, set up a laptop with the following parameters:

* SDR monitoring software installed
* Connect the SDR and filter and antenna to laptop

**Activity 1 (10 points)**

Detecting WiFi Jamming with Wireshark

<https://null-byte.wonderhowto.com/how-to/detect-script-kiddie-wi-fi-jamming-with-wireshark-0186138/>

Questions:

1. In Kali, what two methods do we use to locate the network card interface?
2. What commands do we use to set up monitor mode?
3. How do we set up a capture for management frames only in WireShark?

**Link Two (10 points)**

Cracking WPA using PMKID Hashcat

<https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-passwords-using-new-pmkid-hashcat-attack-0189379/>

Questions:

1. What was the old way of cracking WPA2?

2.What are the 2 downsides of the old methodology?

3. What does RSN IE stand for?

4. Do you need to have connected devices on the target network to perform the attack?

5. What are the three components of the Hashcat attack tool?

6. What happens when you can not get the password?

# Activity 2: Software defined Radio Operation (58 points)

Verify that the SDR is functioning by accessing the SDR interface. Show that the unit is receiving signal

(Insert screenshots to verify)

**An Introductory Project for Software Defined Radio**

Credit – All about circuits [Christi Durham](https://www.allaboutcircuits.com/author/christi-durham)

**Learn how to listen to frequencies on the air with nothing more than a USB dongle: first FM radio, then voice signals.**

There are two parts to this project. First, we’ll listen to FM radio stations: stations that you can get from tuning your car radio, for example. This will allow us to get acquainted with the software and get through the setup of the software-defined radio (SDR).

The second part of this project is a little more involved, but in the end we will be able to decrypt common live radio chatter. These frequencies are more dependent on your area—including highway departments, fire districts, and police dispatch. This is intended only for educational purposes and should not be used in any other activities.

Heads up before we get started: This tutorial is focused on the Windows operating system.

**Required Hardware and Software for Part One**

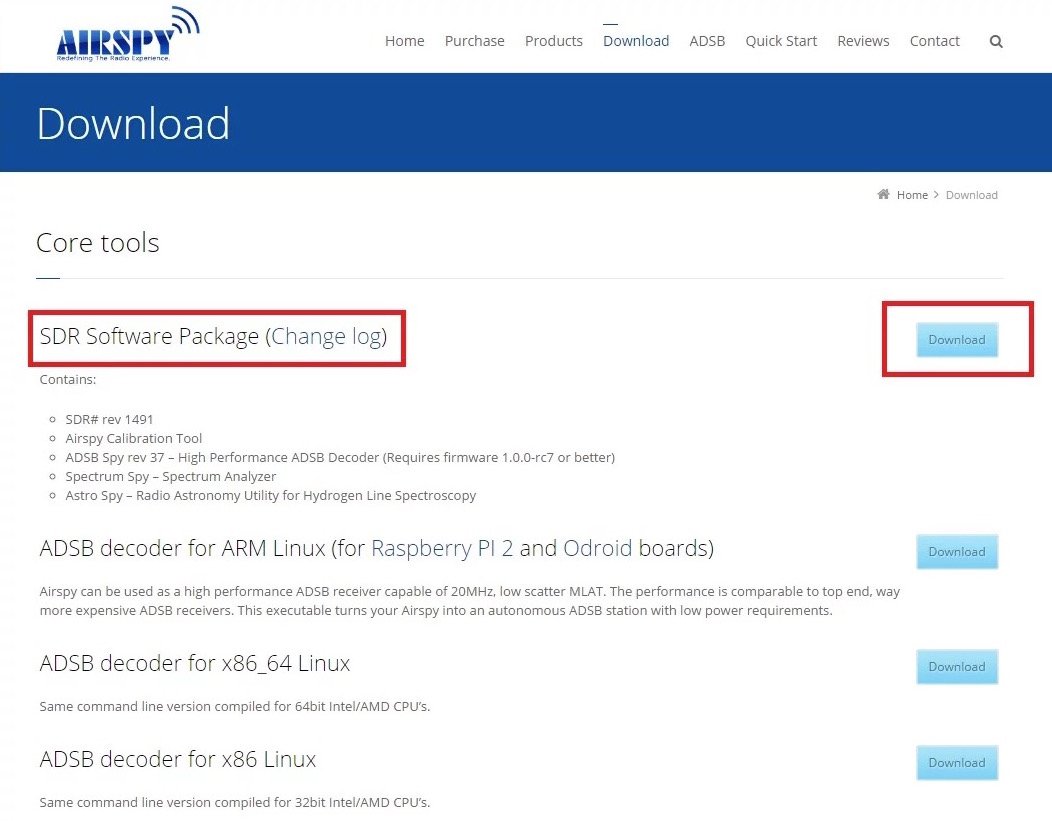
* RTL-SDR R820T2  (~$25)
* SDR Sharp (free software available at <http://airspy.com/download/>)
* Zadig USB Driver Installer (free software available at <http://zadig.akeo.ie/>)

**Recreating the FM Radio**

Once you’ve plugged in your SDR dongle, wait for Windows to stop trying to automatically install drivers for the device. Make sure you’ve screwed in the antenna that came with the dongle. Without it, you won’t be able to pick up anything!

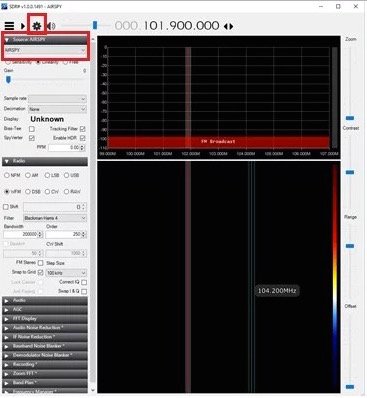
The simplest way to obtain the drivers for your dongle will be to use [Zadig](http://zadig.akeo.ie/" \t "_blank), which should automatically detect the proper drivers for your system. Make sure “List All Devices” is on under the Options menu, then select the RTL2838 in the dropdown menu. Zadig will select the driver you need and all you have to do is click the “Install” button.

Once you've got your drivers sorted out, it's time to download the [SDR Software Package](http://airspy.com/download/). It should be at the top of the page.



***The SDRSharp download page at*** [***Airspy.com***](http://airspy.com/)

Unzip the file you downloaded and save it in a memorable directory (you will have to navigate to this folder again in order to open the program). No further installation is required! Go ahead and open the SDRSharp application

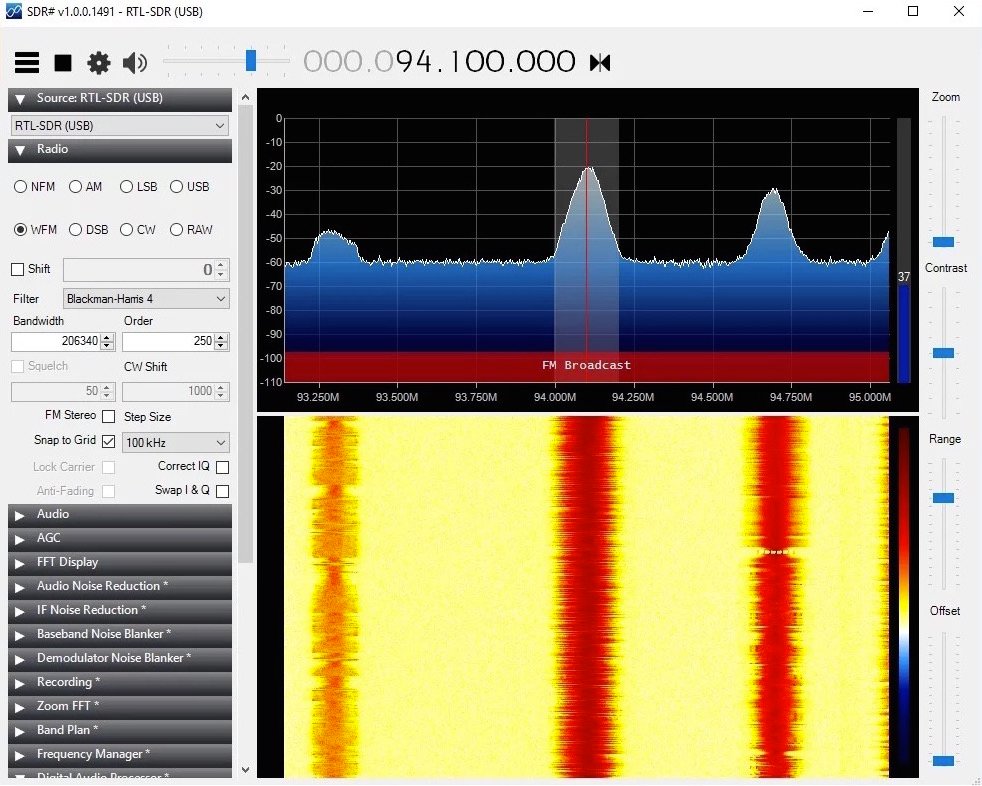


***Screenshot of our first use of SDRSharp***

Upon first opening the application, it will look something like mine above. Most importantly, the default source is set to AIRSPY. In order to use the USB dongle, it’s necessary to change the dropdown (highlighted in the picture) and select “RTL-SDR (USB)”.

Next, click on the gear highlighted in red in the picture. This will bring you to a settings menu. Ensure that the correct device is in the drop-down menu. Then, select the highest available sample rate—without this, your signals will be lower resolution and you’ll pick up more noise.

Finally, increase the RF gain by moving the arrow to the right. It makes a big difference in the clarity of the signals you receive.



***Listening to FM radio in SDRSharp***

In my example screenshot above, you see clear peaks in the top window and a much darker spectrum reading where my cursor is. Each peak symbolizes one station’s signal. If you are getting poor signal quality, you can adjust your bandwidth setting. Hint: Try to get it to match the width of the signal. A smaller bandwidth should work, but if it’s much larger than the signal then you’ll get a lot of extra noise.

That concludes this part of this project! If you had problems with any part of these settings, feel free to leave a comment or see if it’s been covered here: [http://www.rtl-sdr.com/rtl-sdr-quick-start-guide/](https://www.rtl-sdr.com/rtl-sdr-quick-start-guide/)

If you want to explore more frequencies you can pick up with the SDR, I strongly recommend the Frequency Manager Suite add-on to SDRSharp. It includes features that greatly improve the user friendliness of SDRSharp with features like typing in the frequency you’d like to go to (instead of scrolling), as well as scanning frequencies to check for signals and scheduling. You can find the Frequency Manager Suite here: <http://www.freqmgrsuite.com/>

# Activity 2: SDR Tuning

Attach screenshots of tuning to the 3 different voice signals in these frequencies:

1. CFVP broadcasts at a power of 100 watts on 6.03 MHz in the 49m shortwave band.

Screengrab 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Frequency** | **License** | **Type** | **Tone** | **Alpha Tag** | **Description** | **Mode** | **Tag** |
| **413.86250** | XJM271 | RM | 196.6 PL | CAN-TF2 OPS | Calgary Area CAN-TF2 Ops |  |  |

Screengrab 2

# 3)Weatheradio Canada: Alberta network 162.400 Mhz

Screengrab 3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **463.61250** | VOC446 | RM | CC 12 TG 899 SL 2 | SAIT Cleaners | Southern Alberta Institute of Technology - Cleaners |