Tim ^.^

thE CLIENT  Cyber Insights

ARP POISONING PREVENTION

# Introduction

## Background

Technology is an integral part of everyone’s daily lives. Every device in the world with internet access is directly connected by some means, allowing for data transfer anywhere. For example, if I sent an Email (ancient technology, I know) to a friend, for that message to reach them, by definition, my device must be connected, to their device, otherwise the message would not have sent.

The internet has given us the incredible ability to interact with anyone and anything, anywhere else on the internet. However, because of the incredible power this provides, we rely extremely heavily on the internet, hence the first statement (Technology is an integral part of everyone’s daily lives).

## Connecting

There are several ways of connecting to the internet. This project will specifically focus on Wireless connections between devices and routers.

## Public Wi-Fi

Because of the relative safety of home networks, many are unaware of how dangerous public Wi-Fi can be compared. Because of this, people are less concerned about the sensitivity of the information being transmitted from their devices, making them vulnerable.

## ARP Spoofing

The goal of an ARP spoofing attack is to ensure all the data travelling between a device, or devices on a network and the router are intercepted. Depending on how the attacker chooses to do this, one device, or a whole network can be attacked.

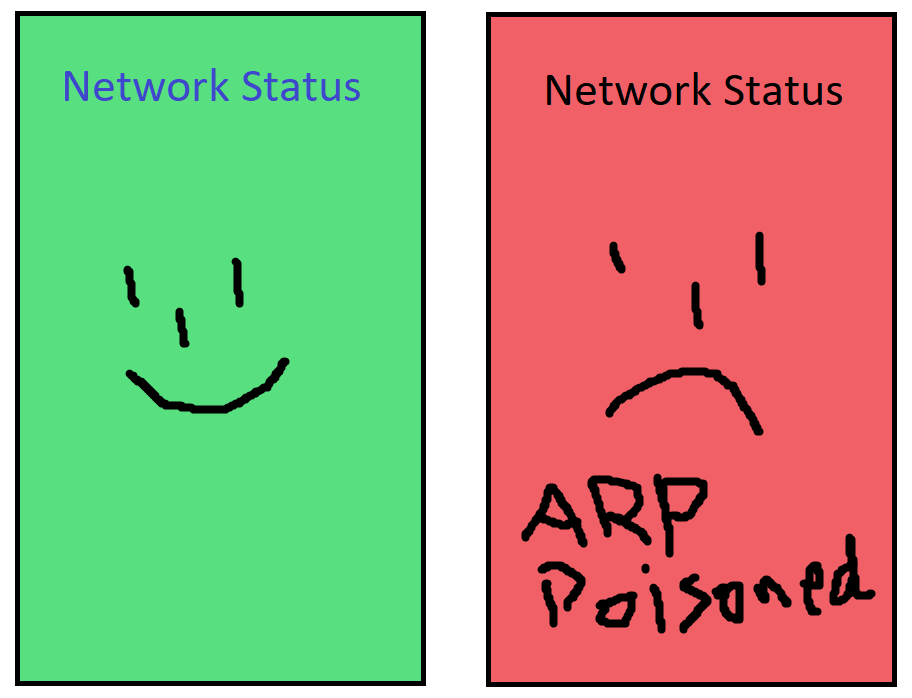
# My Project

The initial goal for my project was to build a tool for detecting ARP poisoning on a given network, the reason for this is that it’s very easy for an attacker to launch attacks on a network but very hard for the average person to detect or prevent being affected by these types of attack.

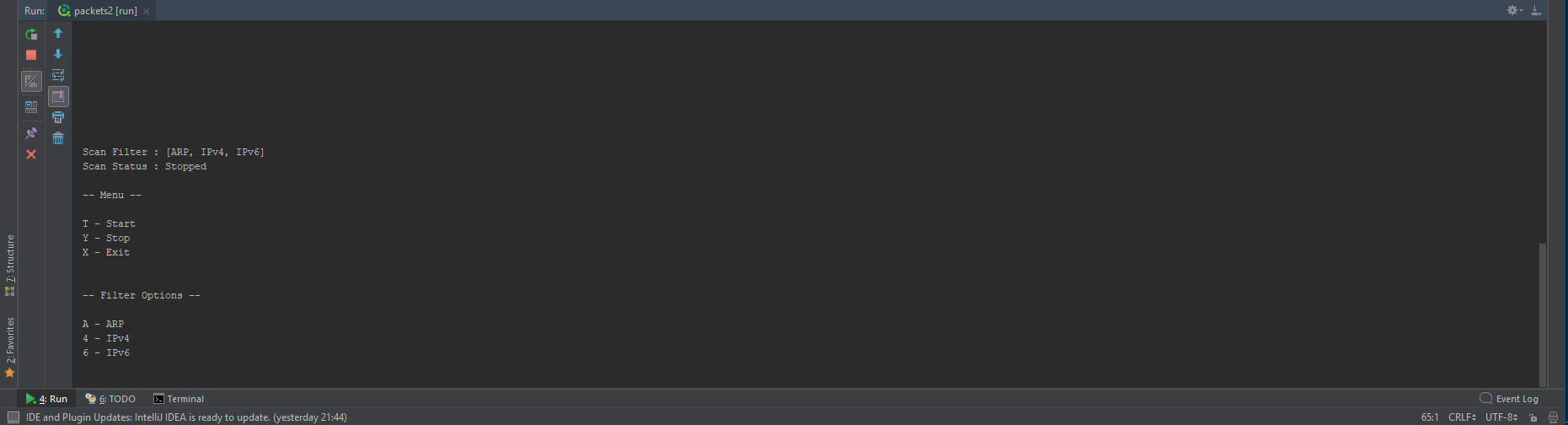
The tool was also going to be made for mobile as opposed to computer, the reason being that everyone uses apps, and has their phone on them all the time. It would be much easier to take a phone out and check a hotspot.

# Design

This is a basic concept design for the app I had in mind. A simple app which can relay as much information as possible with the least confusion/complication.

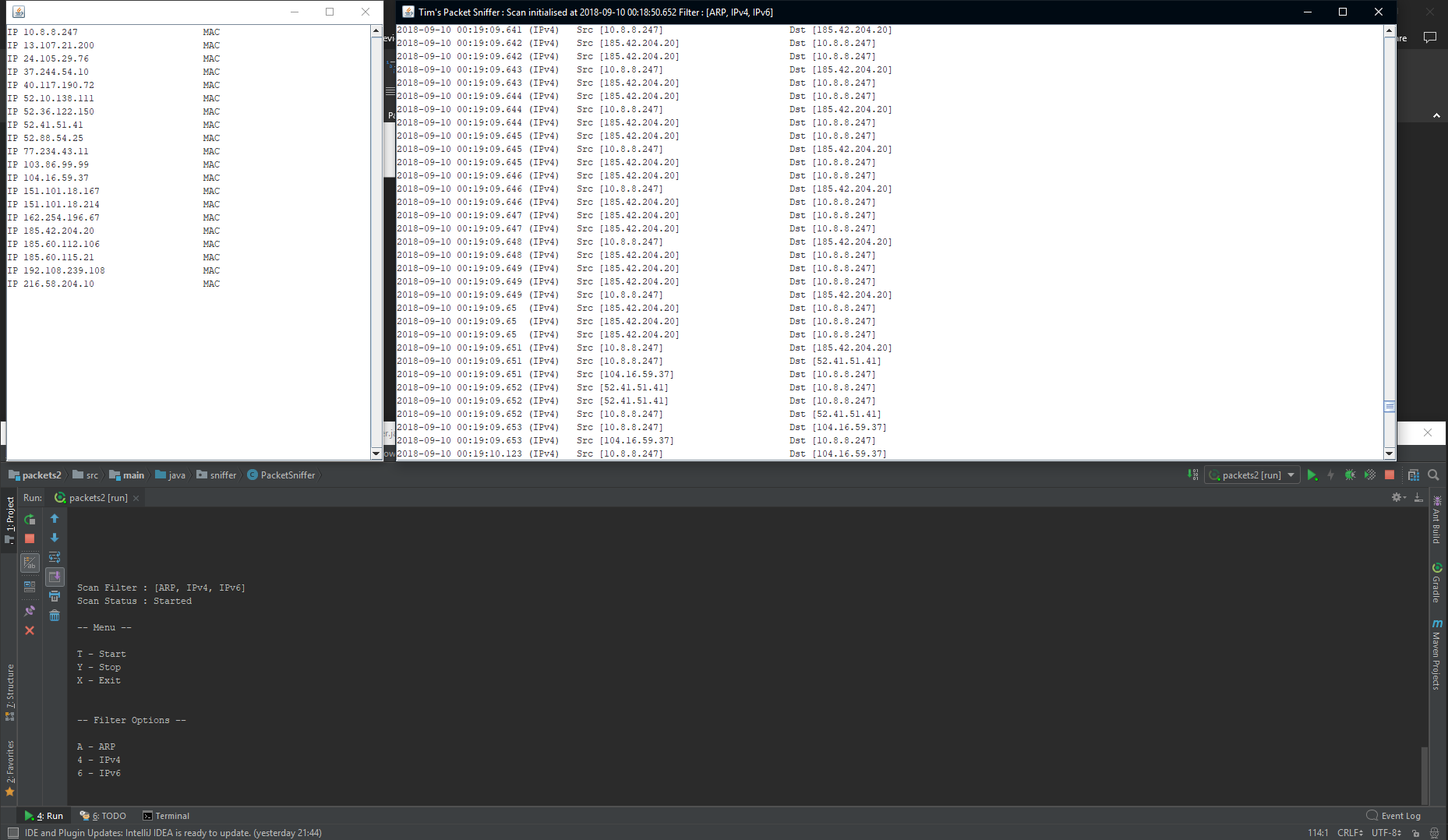


# Usage

The program should either be built in Intellij or run at a command line. The user will see the following screen:

|  |  |
| --- | --- |
| T | Start the scan |
| Y | Stop the scan |
| X | Exit the program |
| 4 | Toggle monitoring of IPv4 packets |
| 6 | Toggle monitoring of IPv6 packets |
| A | Toggle monitoring of ARP packets |

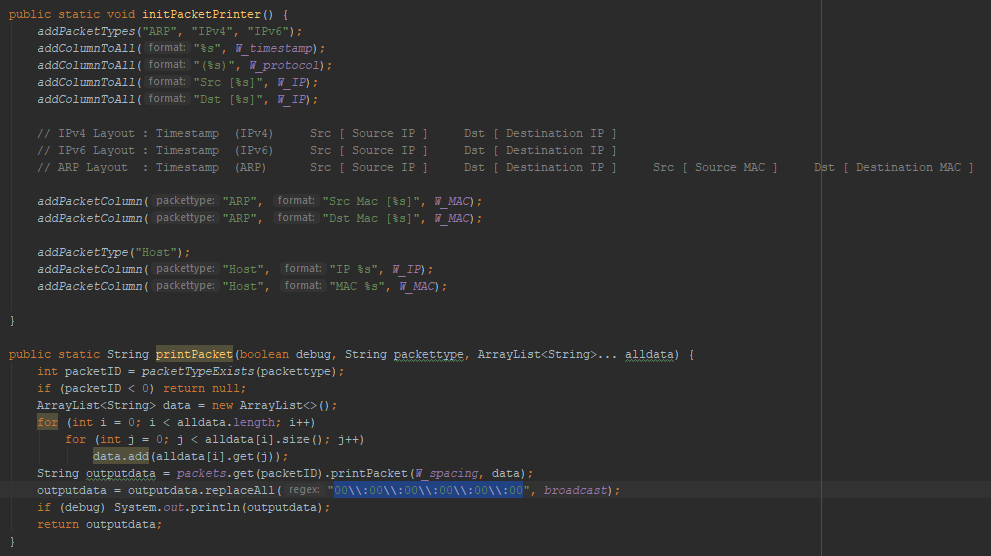
Once the user presses T to start the program displays this



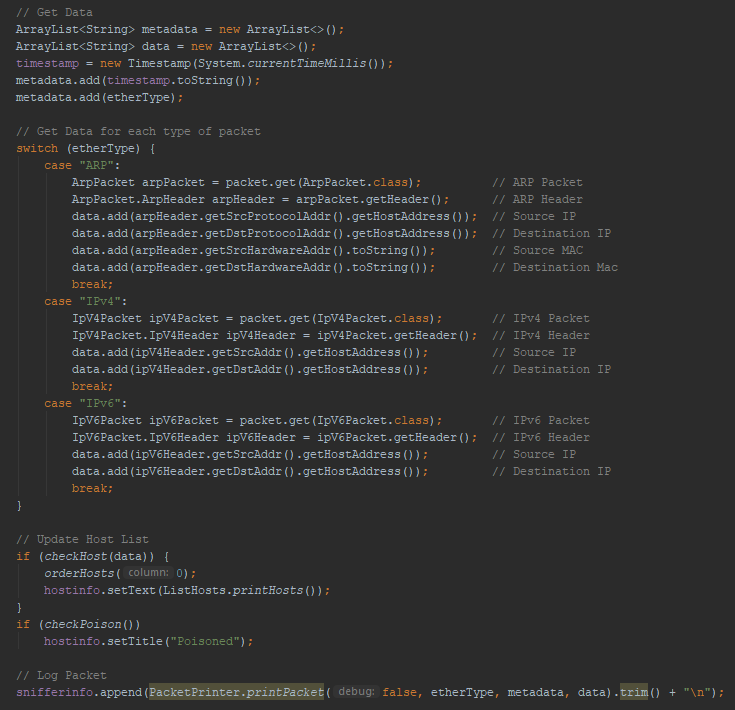
The desktop I tested on is connecting to a VPN, through an Ethernet cable through my laptop, through WiFi, as such the network is a little strange, I don’t get ARP packets as there isn’t really any kind of network my PC sees (there have been demonstrations in other locations).

# Data Structure

The data structure I built for this project was one of my favourite parts about it as it is modular and highly customisable, self-formatting and easy to use.



First the data is collected in this function, where it’s split into metadata and data. There would potentially be much more data which could be collected and used for other windows, but for now this is fine.



The data is then passed through an infinite overloads function which takes multiple ArrayList<String>.

# Detect ARP Poisoning

The project is coded so that the host window will pop up saying the network is poisoned if it detects the same IP address for 2 MAC addresses.

