**Software Requirements**

**Specification**

**for**

**<Android Network Sniffer>**

**Version 1.0**

**Prepared by**

**< Soh Yu Xuan, Timothy Chin, Kenneth Huang, Kendrick Tan >**

**<22 June 2018>**

# Table of Contents

[Table of Contents ii](#_Toc5834)

[Revision History ii](#_Toc5835)

[1. Introduction 1](#_Toc5836)

[1.1 Purpose 1](#_Toc5837)

[1.2 Document Conventions 1](#_Toc5838)

[1.3 Intended Audience and Reading Suggestions 1](#_Toc5839)

[1.4 Project Scope 1](#_Toc5840)

[1.5 References 1](#_Toc5841)

[2. Overall Description 2](#_Toc5842)

[2.1 Product Perspective 2](#_Toc5843)

[2.2 Product Features 2](#_Toc5844)

[2.3 User Classes and Characteristics 2](#_Toc5845)

[2.4 Operating Environment 2](#_Toc5846)

[2.5 Design and Implementation Constraints 2](#_Toc5847)

[2.6 User Documentation 2](#_Toc5848)

[2.7 Assumptions and Dependencies 3](#_Toc5849)

[3. System Features 3](#_Toc5850)

[3.1 System Feature 1 3](#_Toc5851)

[3.2 System Feature 2 (and so on) 4](#_Toc5852)

[4. External Interface Requirements 4](#_Toc5853)

[4.1 User Interfaces 4](#_Toc5854)

[4.2 Hardware Interfaces 4](#_Toc5855)

[4.3 Software Interfaces 4](#_Toc5856)

[4.4 Communications Interfaces 4](#_Toc5857)

[5. Other Nonfunctional Requirements 5](#_Toc5858)

[5.1 Performance Requirements 5](#_Toc5859)

[5.2 Safety Requirements 5](#_Toc5860)

[5.3 Security Requirements 5](#_Toc5861)

[5.4 Software Quality Attributes 5](#_Toc5862)

[6. Other Requirements 5](#_Toc5863)

[Appendix A: Glossary 5](#_Toc5864)

[Appendix B: Analysis Models 6](#_Toc5865)

[Appendix C: Issues List 6](#_Toc5866)

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Date** | **Reason For Changes** | **Version** |
| Kendrick Tan | 02/07 | Correction of certain description and explanation | 1.1 |
|  |  |  |  |

# 1. Introduction

## 1.1 Purpose

This document describes the requirement specification for the Android Network Sniffer application “NetSniffer” that captures packets through the use of existing packet capturing technologies. It presents a means of viewing packets that are currently in a network and possibly provide some information on the packets. It will explain the Features of the system, Interface, what the system can do, what are the possible constraints and limitation when using the Network Sniffer, possible additional features of the Network Sniffer compared to currently known Android Network Sniffer. The document is intended for developers and users of the system.

## 1.2 Document Conventions

This document follows the basic SRS convention methodology and also based on templates that are online in which to draft this document

## 1.3 Intended Audience and Reading Suggestions

This document is intended for developers, project managers, users, testers and documentation writers. The SRS below contains information regarding the project, scope of the project, references used in writing the SRS, testers who if possible solve any issues that the current developers may have faced, and also for users who wish to understand what the project created was about. It is suggested when reading to have knowledge with regards to Networking, Android, Android Programming, Java, C Programming, as they will provide an easier understanding.

## 1.4 Project Scope

The android network sniffer application where the application should be able to capture packets and view them. However, there may be certain limitations and constraints that may be imposed on due to the requirements which will be further explained in the later sections

Objectives are to have the ability to perform real time capturing and viewing of packet data and save the data into a file which can be viewed later, additional features such as filtering of traffic, viewing

## 1.5 References

# *<https://krazytech.com/projects/sample-software-requirements-specificationsrs-report-airline-database>*

<https://aakashtechsupportdocs.readthedocs.io/en/latest/prodpersp.html>

# 2. Overall Description

## 2.1 Product Perspective

The application is solitary consisting single mobile application. The mobile application will be used to capture and view packets, also to save packet information in text files on the mobile device. The mobile application will need to be rooted for this application to work. By default network card for mobile phone manufacturers disable the ability to change the mode of the network card. Rooting the phone allows the ability to change the mode of the network card that allows the capturing of packets. This is a network/data centric application that requires some storage space. It also utilizes text files and storage locations on the mobile device. Storage locations such as "/sdcard/Download/".

The mobile application also has some restrictions such that it has to be connected to a wifi access point to capture packets.

## 2.2 Product Features

The main features of our product includes:

* Network Sniffing: To be able to start & stop network sniffing
* To be able to provide real time viewing of sniffed data
* To be able to save the sniffed data into a file
* To be able to read from the saved file
* To be able to filter packet type captured

## 2.3 User Classes and Characteristics

The type of User classes for our product would be mostly IT users, developers.

IT Users: users that work in the field of IT such as System Administrators, who constantly have work involving Network such as Monitoring of Network Traffic for anomaly, or even regular data collection of network traffic to improve the system such as avoiding overhead. IT users would be the type of users that most frequently use Android Network Sniffers

Developers: Users that wish to develop a similar type of Application may want to user our product as reference or possibly create a more improved version of ours as the technology improves

## 2.4 Operating Environment

The device of our product choice must support Android Studio, programming language will mostly be done in Java, with the exceptions of binaries done in C using the Pcap library.

Hardware of the device must have a chipset that allows NIC promiscuous mode. Device also needs to be rooted.

## 2.5 Design and Implementation Constraints

Because of the platform in which our product is on which is Android there will be limitation and constraints compared to the Personal Computer type of Network Sniffer.

When designing our product, the constraints are as follows:

* Network Cards/Wifi Chips for mobile devices are manufactured in such a way that they are not allowed to change their mode.(Why root is needed)
* Not all wifi chips support promiscuous/monitor mode, resulting in some phones unable to capture packets. (Only certain wifi chips support packet capture)
* The device must be rooted which is to give Super User Access to the phone. However, it is to be noted that rooting a phone would be similar to what would be known as Jail Breaking an iPhone.
* Phone being rooted and requiring the network card means only 1 person test app at a time. (Inconvenience, cannot use emulator to fully test app)
* Device being rooted results in super user privileges given to applications that should not have the permissions. This requires something to manage the SU privileges.
* The inability to give the app SU results in the need to spawn processes that have SU permission.
* The inability to give the sniff app SU also means that code cannot be used in to sniff. (must use process -> binary)
* Limited resources on mobile devices.
* Have to be coded in Android environment, Java or C.

## 2.6 User Documentation

Other than the product of an Android Network Sniffer there will also be a Technical Documentation that elaborate clearly the entire technical aspect of the product

Other than the Technical Document there will also be a User Documentation to allow ease of use for the users who will be using our application

## 2.7 Assumptions and Dependencies

Assumptions -> users are using devices that are rooted, Android Marshmellow 5.0 and above, wi-fi card must be able to support promiscuous mode.

Dependencies -> C compile Binaries

# 

# 3. System Features

Below list our system features of the product and all possible features available

## 3.1 Network Sniffing Feature

Users should be able to start and stop the network sniffing of the application

#### 3.1.1 Description and Priority

This Feature is considered the core of our entire product where by the user is able to start and stop sniffing of network and once the High Priority

#### 3.1.2 Stimulus/Response Sequences

User Starts the Network Sniffing and the device will display on screen and can Stop

User Starts the network sniffing and the device will save it to a file in the downloads folder once the sniffing is stopped and can be viewed using wireshark

#### 3.1.3 Functional Requirements

Start and Stop Sniffing of Packets

Can save the sniffing to a file which can be retrieved later for viewing

## 3.2 System Feature 2 (and so on)

# 4. External Interface Requirements

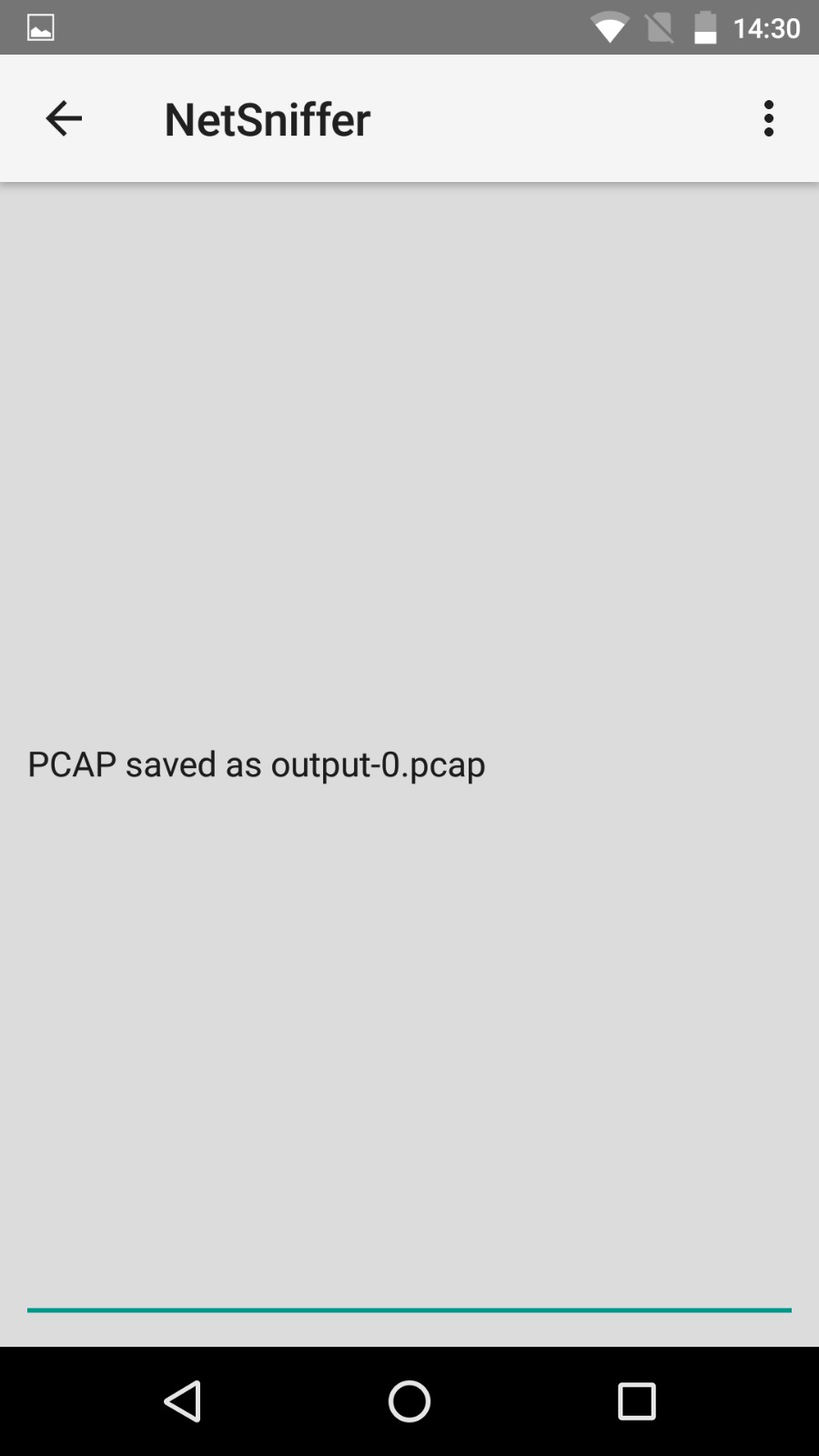
## 4.1 User Interfaces

## C:\Users\Kendrick\AppData\Local\Microsoft\Windows\INetCacheContent.Word\WhatsApp Image 2018-07-02 at 2.34.34 PM.JPEG

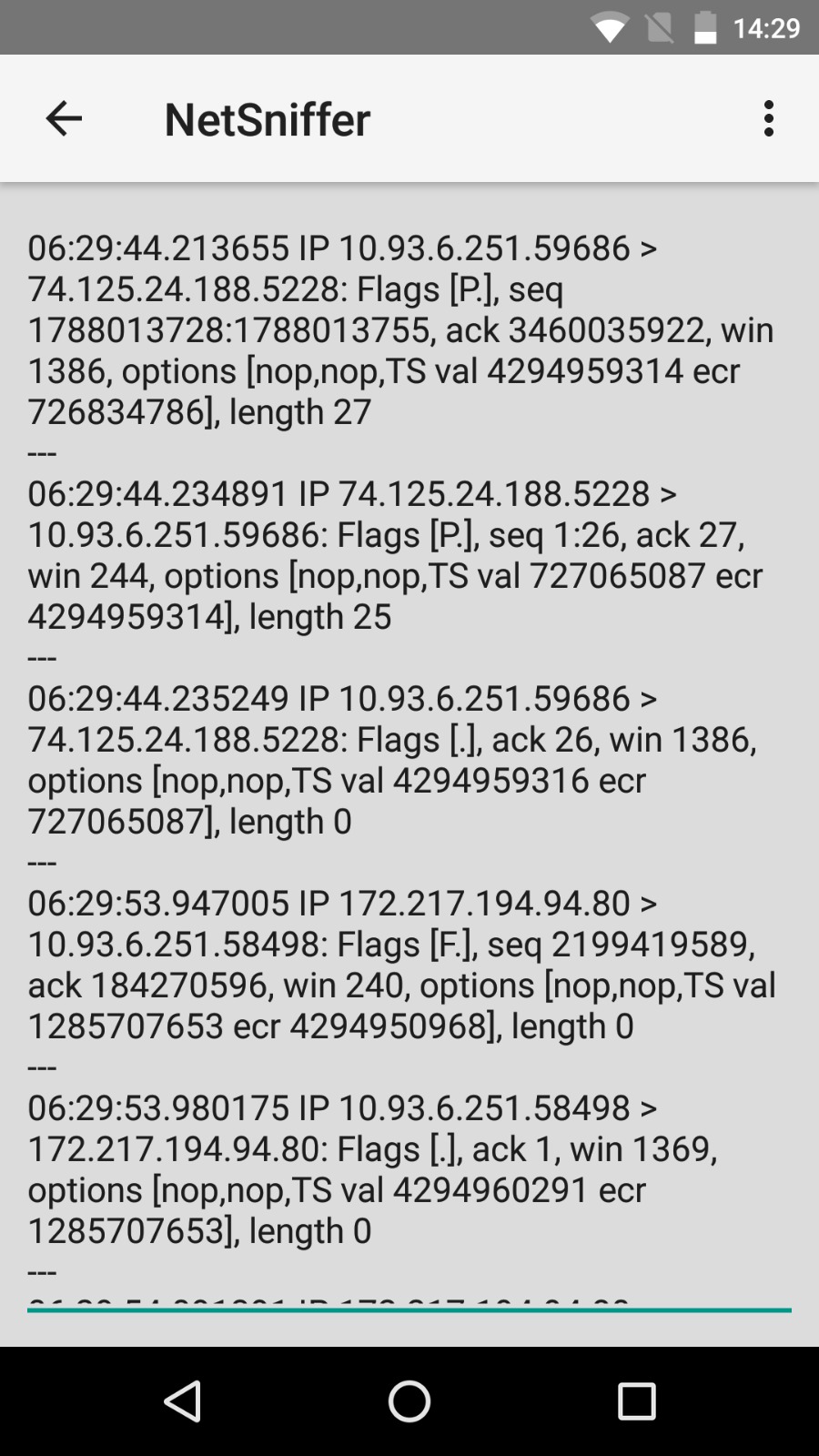
Main Screen of the Application



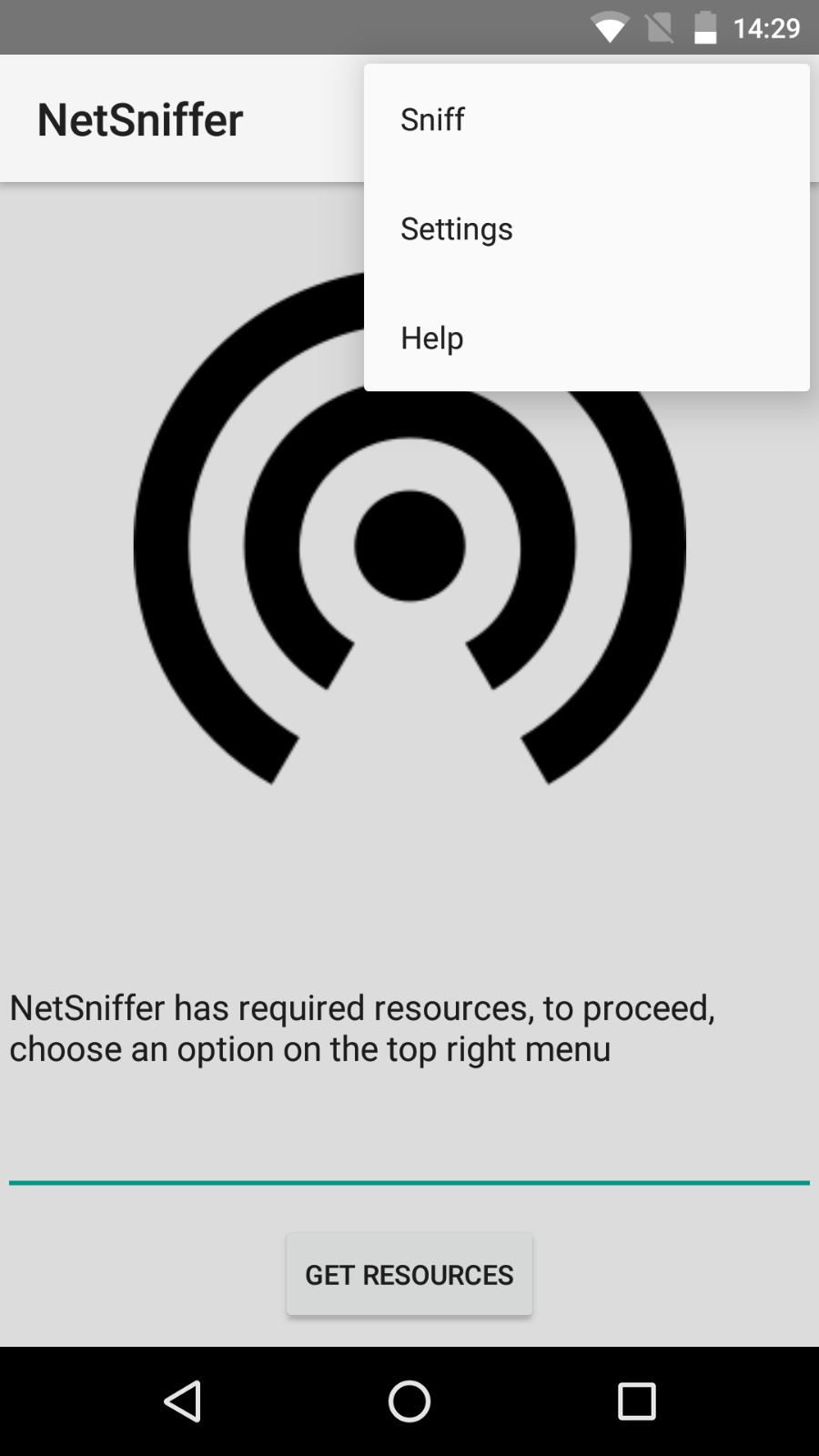
## *User start sniffing PCAP*



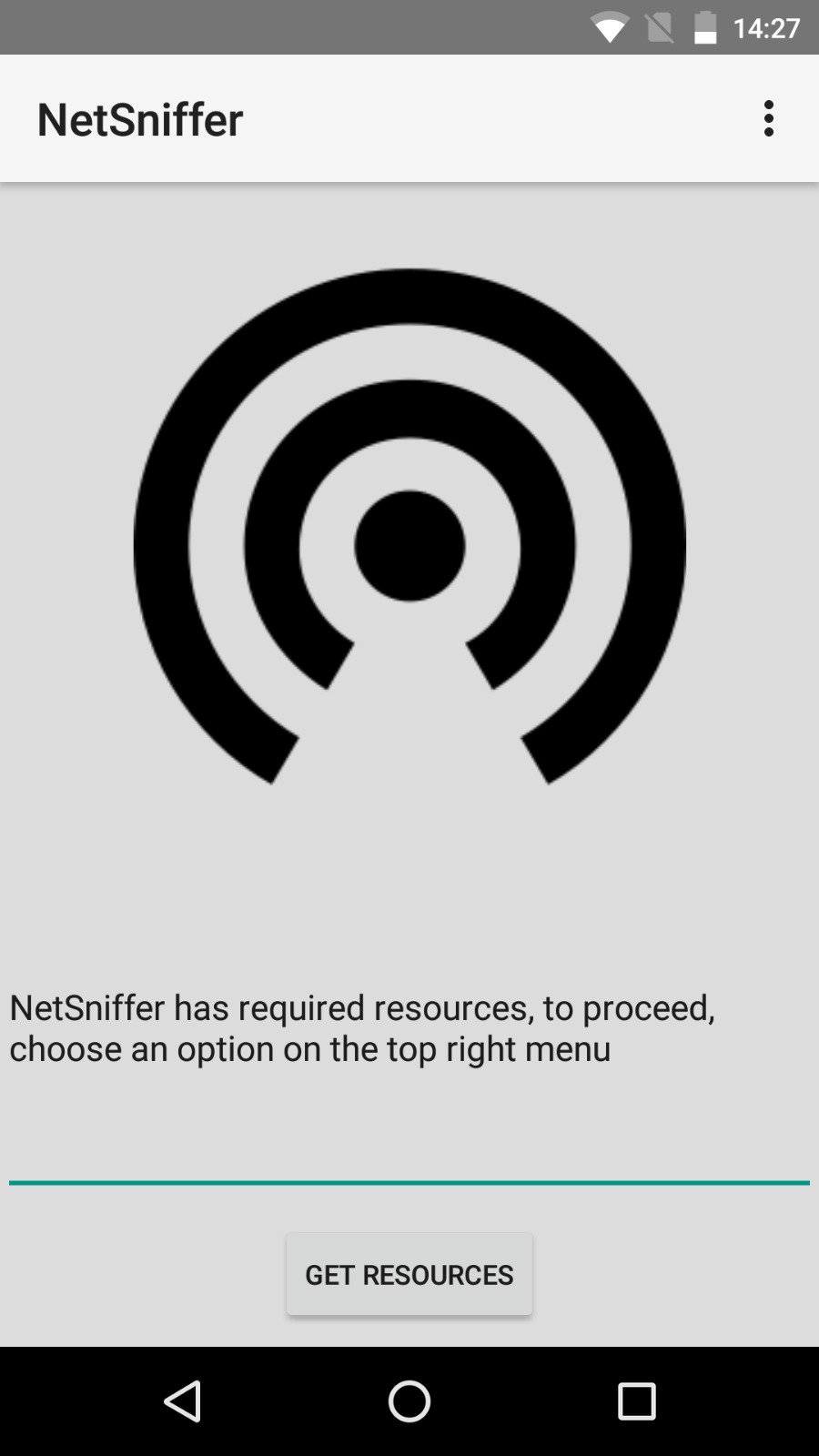
Saving the Sniffed data into a file



Prototype version Real time display of sniffing, with delay of 3s and updates after every 1s



Menu of our Application where user can Select to sniff



Application Main Page which is displayed to the user when they launch the application

## 4.2 Hardware Interfaces

Devices used must have chipset that allows Monitor mode, device also needs to have root access. After Sniffing of the network the file will be saved in a Pcap format that can only be run by applications that can read this particular format.

Example of chipset BCM 4325,4329,4330, 4335,4339.

Nexus 5 device for our project uses BCM 4339.

## 4.3 Software Interfaces

Prototype version -> TCP Binary for ARM devices

* Stored in assets
* Extracted to Internal Storage (app)
  + /data/data/com.example.yuxuan.netsniffer/tcpdump
* Main Activity checks if exists
* Sniff Activity
  + Creates process (threads)
  + Queries Binary and Output to a text file
  + Updates UI

# 5. Other Nonfunctional Requirements

## 5.1 Performance Requirements

Wi-Fi card Range that is device specific as different devices uses different Wi-Fi cards and even if the Wi-Fi cards are compatible they may have different ranges to do the sniffing

## 5.2 Safety Requirements

Rooting the phone is one of the requirements of the device however it is to be noted that when rooting the phone there will be some effects that the user must be aware of

Disadvantages when Rooting phone

* Rooting immediately voids your phone’s warranty
* Rooting have a risk of “bricking” the phone: Device might become dead and unusable
* Poor performance: when additional features that need to be added might cause the device to lose performance speed and features
* Viruses: custom programs used might make changes to software codes which might have a chance of introducing virus

## 5.3 Security Requirements

There is a security issue when using the phone in which if the device is rooted. There will be an increase in risk of viruses because rooted device allows for special permissions that allow additional customization of the device. For example, places that were not allowed to be modified can now be accessed. This causes vulnerabilities as things that shouldn’t be changed are now open.

There is now a need to manage the Super User permission on the device. “SuperSu” android application in this case was used to manage permissions.

## 5.4 Software Quality Attributes

<Specify any additional quality characteristics for the product that will be important to either the customers or the developers. Some to consider are: adaptability, availability, correctness, flexibility, interoperability, maintainability, portability, reliability, reusability, robustness, testability, and usability. Write these to be specific, quantitative, and verifiable when possible. At the least, clarify the relative preferences for various attributes, such as ease of use over ease of learning.>

# 6. Other Requirements

NIL

# Appendix A: Glossary

IT: Information Technology

Pcap: a type of file extension similar to .txt .html

# Appendix B: Analysis Models

<Optionally, include any pertinent analysis models, such as data flow diagrams, class diagrams, state-transition diagrams, or entity-relationship diagrams.>

# Appendix C: Issues List

1. Output from runOnUiThread should be formatted in some way for user friendliness
   1. Working on adapter with ListView(dynamic) in help activity