

**CSCI321 – Project (Android Packet Sniffer)**

User Document

Table of Contents

[1. Document Overview 3](#_Toc523152638)

[2. Application Overview 3](#_Toc523152639)

[3. Appendix A – Nexmon Supported Devices 8](#_Toc523152640)

[4. Appendix B – Root Instructions for Nexus 5 8](#_Toc523152641)

[5. Appendix C – Comparison Report Format 8](#_Toc523152642)

Group Member List

|  |  |
| --- | --- |
| Name | Student ID |
| Soh Yu Xuan | 5498636 |
| Timothy Chin | 5498399 |
| Kenneth Huang | 5498442 |
| Kendrick Tan | 5026556 |

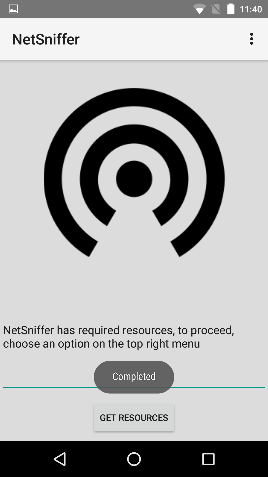
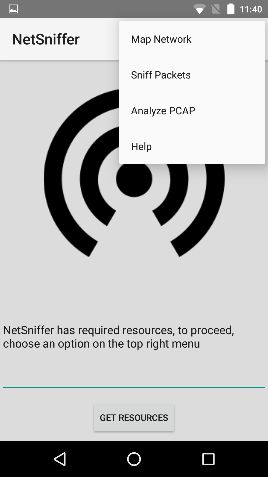
# **1.** **Document Overview**

This document will contain details and instructions on how to set up and use the NetSniffer application. Constraints and limitations will also be detailed depending on device and external factors. The application will be split into 2 different versions, one with support from Nexmon (i.e Nexus 5) and another without support (i.e LG G4) albeit with limited functionality in comparison.

# **2. Application Overview**

**2.1 Application Overview**

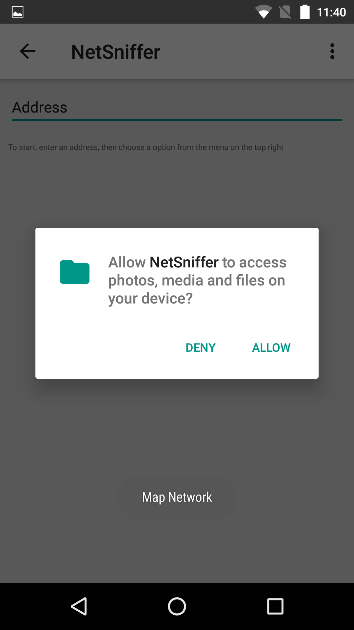
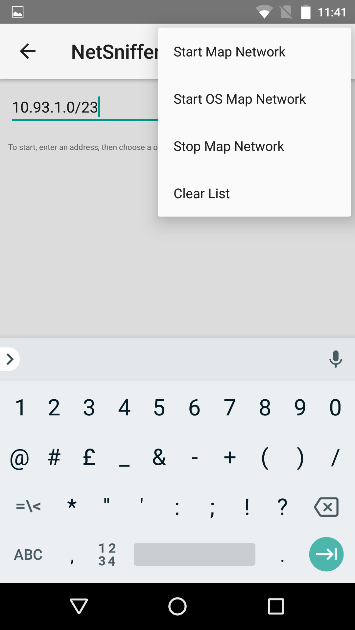
NetSniffer will have full functionality with a Nexmon compatible device [Appendix A]. Before installation of the application, please ensure that device has SU permissions. Instructions to root the Nexus 5 device are included in [Appendix B], results may vary and require other solutions depending on device. Once device has SU permissions, SuperSU should be installed with a file manager of your choice, to manage given SU permissions. Please enable default “Grant” permissions for NetSniffer to work properly. Once complete, set “Install from Unknown Sources” to allow installation of NetSniffer, connect your device to your PC and drag the NetSniffer APK file to any location of your choice. Navigate to that location on your file manager and click NetSniffer to install.

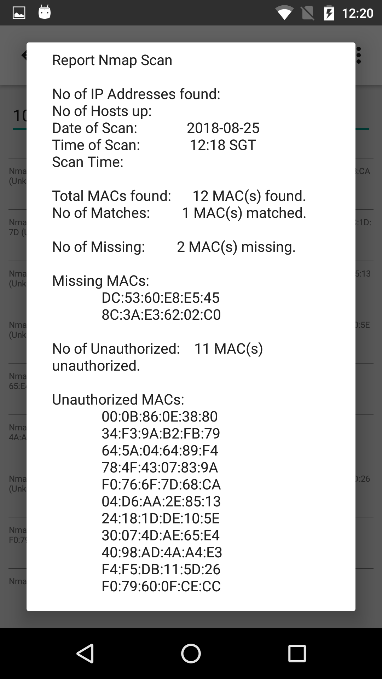
Once the installation of NetSniffer is complete, click “open” and the main screen of NetSniffer will appear. If this is the first installation of NetSniffer, there will be a prompt that indicates that NetSniffer does not have its required resources. Click on the button for NetSniffer to inject required resources into device memory. (NetSniffer will not be able to Map or Sniff without required resources) Once the required resources are injected, the prompt will change and you can start using the functionalities of NetSniffer by choosing an option on the top right menu.

**2.2 Functionality – Map Network**

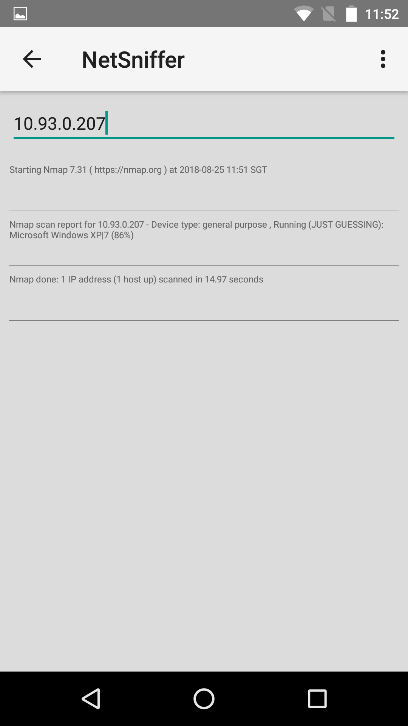
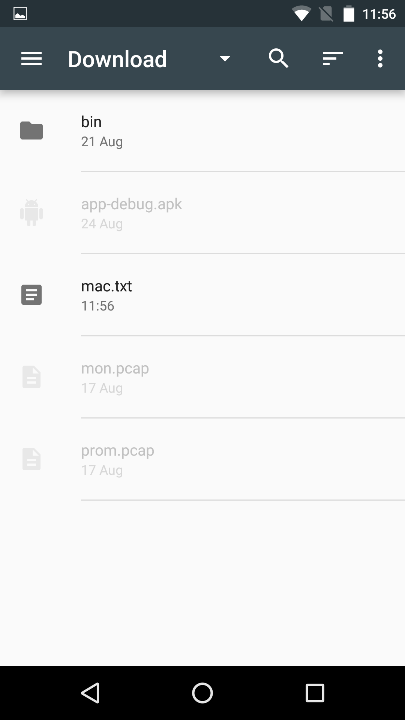
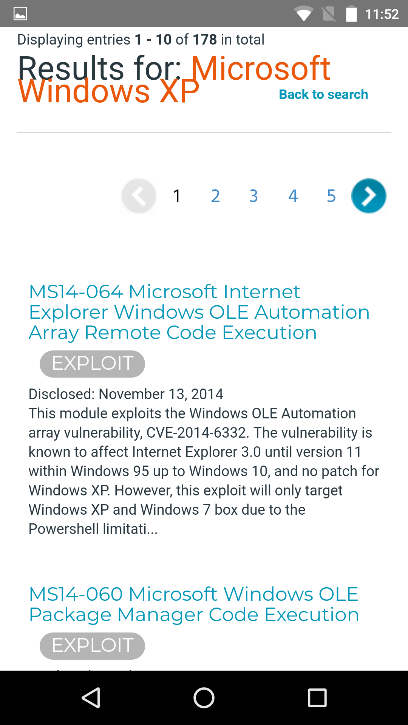
In the Map Network activity, there are two main options, Start Map Network and Start OS Map Network. First fill in the address to be mapped, either a singular device (i.e. 192.168.1.1) or a network (10.93.0.0/23) then start the mapping in the top right menu.

With the normal map, pings are sent out to addresses given, if replies are returned, device results are displayed. After the scan, if a list item with device details are clicked, MAC address is copied (if available – for adding as filters for Sniff). If the last view is clicked, the user is given a choice to input an external text document, with MAC addresses in each line [Appendix C] and NetSniffer will generate a report based on given details (Devices missing / devices found etc).

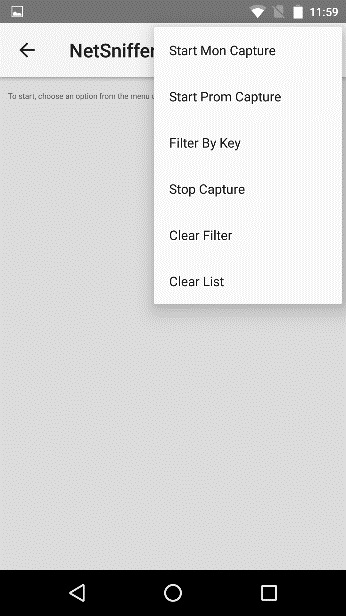
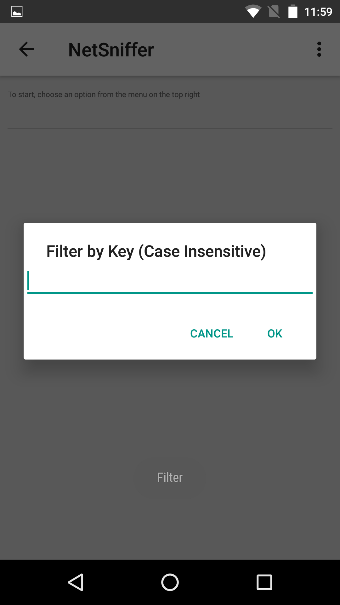
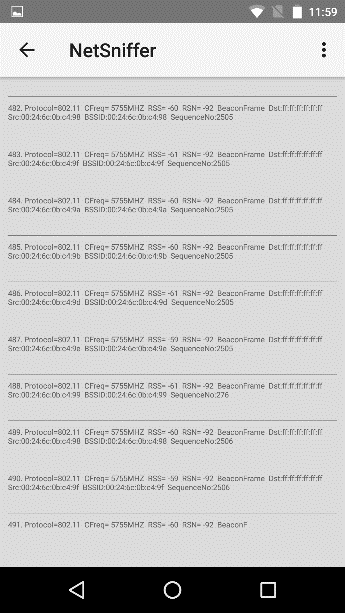
With the OS map, it takes longer to complete a scan. Accuracy of OS returned may vary. If a list item with device details are clicked, NetSniffer executes a search for vulnerabilities on the online database, Rapid7.

In the case whereby a scan takes too long or the input address is incorrect, the user may choose to Stop Scan, otherwise, the application stops the scan automatically once complete.

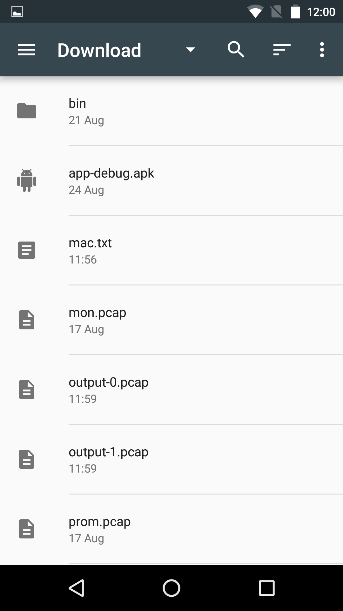
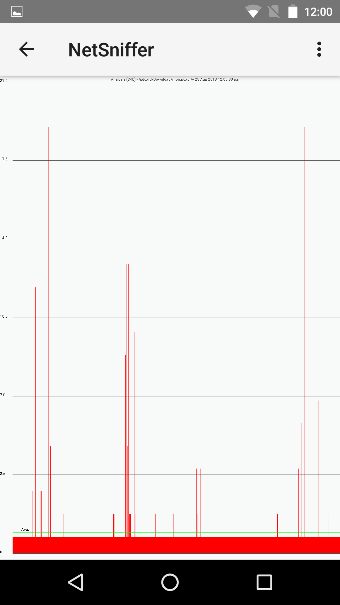
**2.3 Functionality – Sniff Packets**

There are two main options in Sniff Packets. The user may choose to sniff in monitor or promiscuous mode. The user may choose to include a filter (which filters display output only). Both modes generate a PCAP file (output-X.pcap, starting from 0 per session) which may be used in Analyze PCAP or read through wireshark or other PCAP analyzers on PC. For non-supported devices, Monitor mode will not be available.

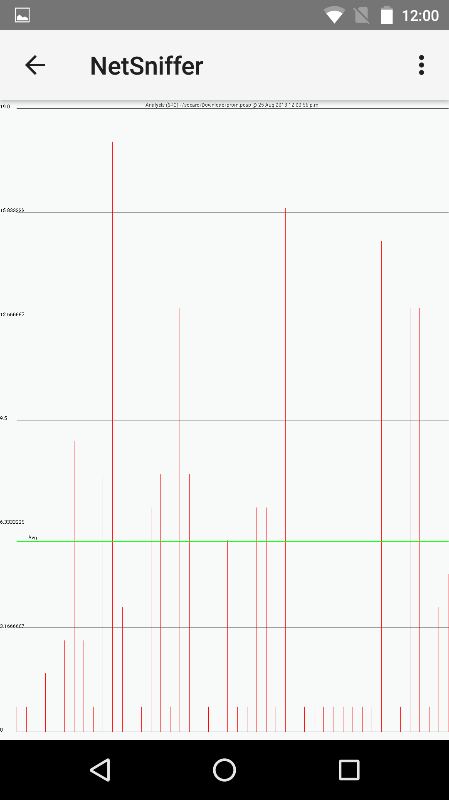
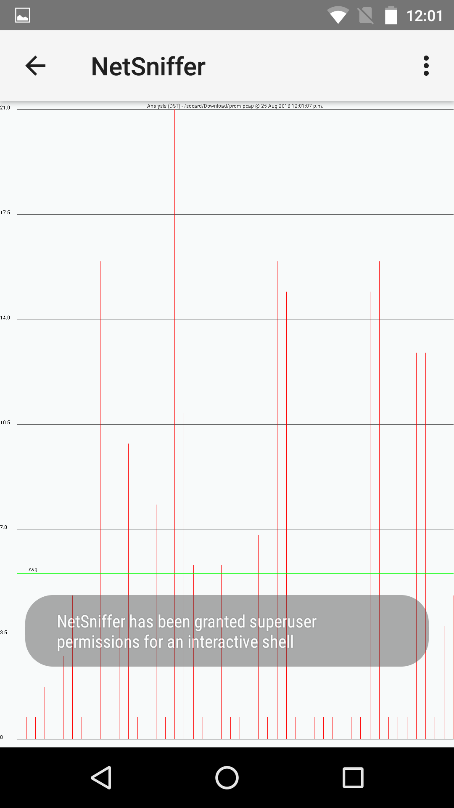
   

**2.4 Functionality – Analyze PCAP**

Depending on the type of PCAP data (Monitor / Promiscuous), the two options will interpret data and draw a graph depending on different things. For monitor mode, SRC mode will draw a graph depending on each radiotap header (type + timestamp), with multiple occurrences pulling the graph up higher. DST mode will display one line, the total amount of packets captured in the selected PCAP file.

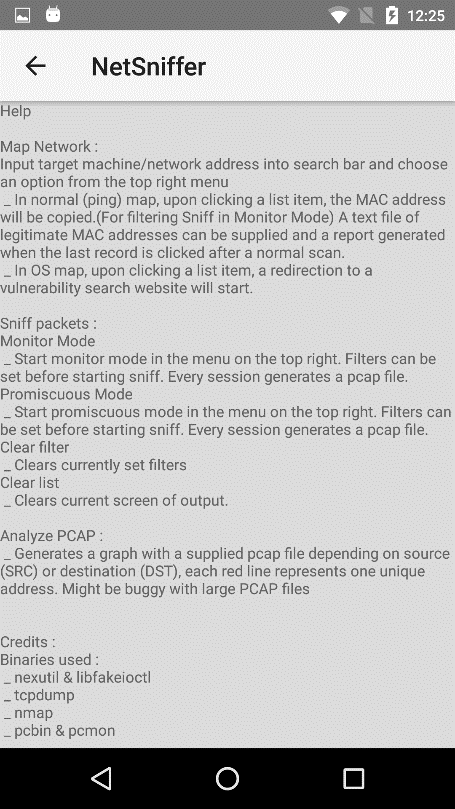
   

For Promiscuous mode, SRC mode will draw a graph, with each line representing each Source IP and the number of packets with that IP in the source. DST mode will draw a graph, with each line representing each Destination IP and the number of packets with that IP in the destination.

**2.5 Help**

A short section is included locally in the application, under Help. If there are any queries with normal operation of the application, it should be included in the Help page.



**2.6 Output of application**

All output generated by NetSniffer will be saved in /sdcard/Download/. Erroneous text files may be generated and output in the same Download folder. Otherwise, each time a user sniffs for packets, a PCAP file will be generated. Repeated sessions of Sniff will overwrite PCAP files if they exist.

# **3. Appendix A – Nexmon Supported Devices**

Android 4.0 (Ice Cream Sandwich) -> 6.0 (Marshmallow)

Chipset Qualcomm MSM8974 Snapdragon

List of Possible Devices

* Google Nexus 5
* Samsung Galaxy Note 3
* Samsung Galaxy S2
* Nexus One
* Raspberry Pi 3 and Zero w
* Huawei P9
* Galaxy J7 2017
* Nexus 6
* Nexus 6P
* Samsung Galaxy S7

# 4. **Appendix B – Root Instructions for Nexus 5**

<https://forum.xda-developers.com/google-nexus-5/orig-development/nexus-5-cf-auto-root-t2507211>

CF-Root is the root for “rooting beginners”

What’s installed

* SuperSU Binary and APK

Installation and usage

* Download the ZIP file
* Extract the ZIP file
* Boot your device in bootloader/fastboot mode. Usually this can be done by turning your deice off then holding VolUp + VolDown + Power to turn it on
* Connect your device to your computer using USB

Windows

Run root-windows.bat

Linux

Chmod +x root-linux.sh

Run root-linux.sh

Mac OS X

Chmod +x root-mac.sh

Run root-mach.sh

Follow the on-screen instructions – watch both the computer and device

If your device has not been unlocked before, this procedure will wipe all your data

# **5. Appendix C – Comparison Report Format**

Sample mac.txt comparison file

XX:XX:XX:XX:XX:XX

XX:XX:XX:XX:XX:XX