****

**University of Wollongong**

School of Computing and Information Technology

Faculty of Engineering & Information Sciences

Bachelor of Computer Science (Digital System Security)

SIM Session 2, 2019

**CSCI321 – Project**

Preliminary User Manual

|  |  |
| --- | --- |
| **Project Topic:** | Android Network Sniffer |
| **Submitted To:** | Mr. Premarajan P |
| **Submitted By:** | Kan Kar Jun Alvin (5709659)  Liao Weisheng Wilson (6212591)  Nyein Soe (5710959) |
| **Group:** | SSP19/2B |
| **Date:** | 28/8/2019 |

**Contents**

1. [Introduction](#Introduction) 3
2. [Application Overview](#ApplicationOverview) 3
3. [Process to use the program](#Processtousetheprogram) 4

3.1. Start-up Screen and Gathering Resources 4

3.2. Function menu 5

3.3. Sniffing function 7

3.3.1. Device Scan 7

3.3.2. Packet Scan 14

3.4. Network Tool 17

3.5. Help Function 18

1. [Error handling on user side](#ErrorHandling) 20
2. [Team Members Profiles](#Profile) \ 20
3. [Guide on rooting an android device](#guide) 21
4. **Introduction**

The main objective of this document is made mainly for the target users so that they know all the related topics on the program that we have implemented. This can also act as a guideline for the users to get familiarized with the program itself. But of course, the current program being implemented is only at its preliminary stage, in other words, a prototype, and hence, this document will only cover what is being implemented and may not cover everything for the time being.

The purpose of this document includes:

* Assisting the users on the usage of the program and thus, making it easy for them to understand.
* Answering some of the basic queries and or doubts of the prototype program.

1. **Application Overview**

In order to use Pocket Sonar, the code implementation is only functional after using a compatible android device, preferably Samsung Note 2 [Section 6]. Before installing the application, itself, one needs to make sure that the device is rooted properly as mentioned previously and the full procedure on how to root an android device can be found Appendix A. It is recommended to only install the application once the rooting process has been successful.

The main reason why rooting is required is to unlock the bootloader in the device itself which will provide access to the user to install necessary custom firmware and at the same time allowing them to run commands with elevated function.

In addition, the minimum firmware requirements of a device for our application to work properly is Android 7.1.1 and the base device that we have used to test out the application is Samsung note2 4G, N7105.

Also, the android device will need to be installed with an armeabi, which is actually an ARM architecture that all the CPUS of the Android devices have. This works in a way that the codes are linked to the application. In other words, ARM is a type of instruction set for CPUs usually based on mobile devices.

The installation (APK) file can be found from our website as mentioned below and further guidance on the overall installation process can be found as well.

Website: [**android-network-sniffer.webnode.com**](http://android-network-sniffer.webnode.com/).

1. **Process to use the program**

**3.1. *Start-up screen and Gathering Resources***

Once the rooting of the android device and installation as mentioned in the previous section [Section 6] has been done successfully, the user will be now able to open up the application without any error. Once opened, the application will start off with a splash screen and at this page, the application itself will gather all the required resources needed for sniffing and all other functions that will be featured in the overall program.



Figure 3.1.1. Start-Up Screen

**3.2. *Function menu***

After the start-up menu and gathering all required resources, the application will continue to the next page which will be the function menu. The user interface will be like as shown in the figure below and we will be going through what each of the icon represents and brief explanation on its relative function features.

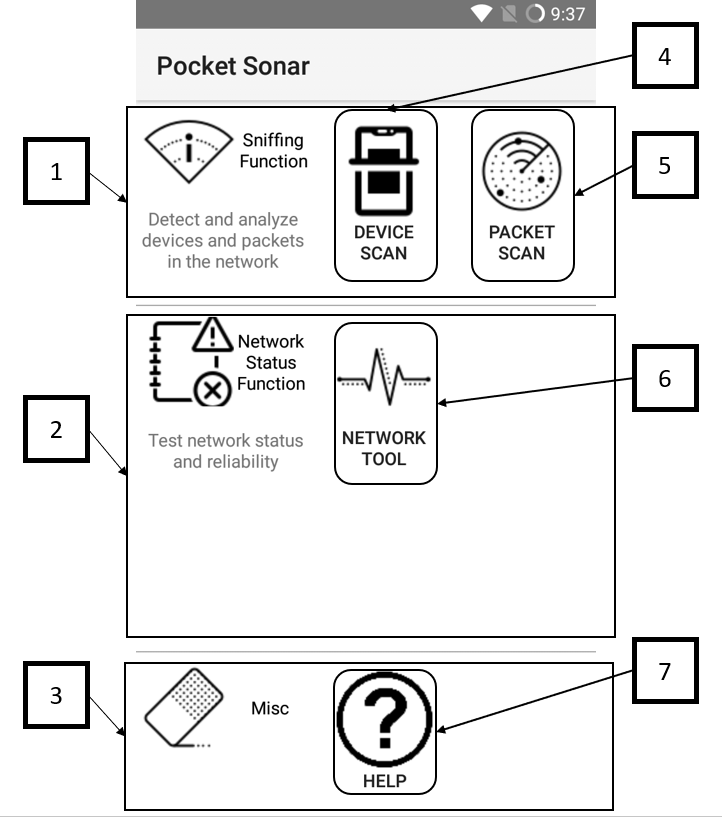


Figure 3.2.1. Function Menu

|  |  |  |
| --- | --- | --- |
| **No.** | **UI name** | **Description** |
| **1** | Sniffing Function | In this part of the menu, we are implementing our main function, which is the network analysis. There are two sub functions, namely Device Scan and Packet Scan. |
| **2** | Network Status Function | This part of the sub function is to provide some general test of the network connectivity. |
| **3** | Miscellaneous | This part will provide some additional general information for the user. |
| **4** | Device Scan | This is where the application will perform two sub functions. One to scan the IP which has been defined by the user and the other is to scan the port which will then bring the user to a certain website where he/she will be able to review and analyze all the associated services, port vulnerabilities, etc. |
| **5** | Packet Scan | There are actually two main features in this part of the application. The first part includes performing the sniff function on the DNS packets and display out the log. At the same time, this feature will create a PCAP file filled with all the sniffed files so that the user will be able to utilize these files for future analysis. |
| **6** | Network Tool | The main feature of the Network Tool function is to detect network devices leading to the connection of the application and its targeted address so that the user will be able to analyze and take immediate action on the anomalies and preventing further damage. |
| **7** | Help | This function provides general help for the user where brief description of the functions will be provided and at the same time, information on how to use the functions. |

**3.3. *Sniffing Function***

**3.3.1. *Device Scan***

In this sub function, there are two modes, scanning all IPs in subnet or one single IP and scanning Port for 1 device. The user interface for this function is as shown below.

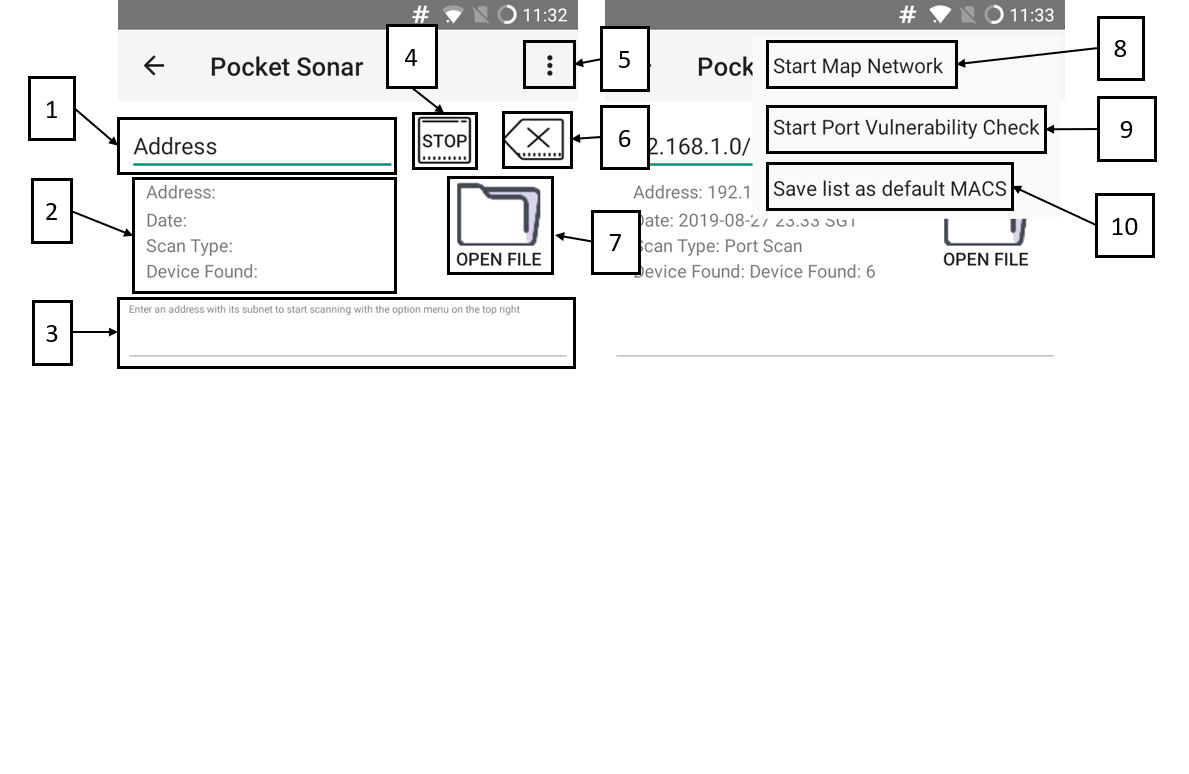


Figure 3.3.1.1. UI for Device Scan

|  |  |  |
| --- | --- | --- |
| **No.** | **UI name** | **Description** |
| **1** | Address Input | The user will be required to key in the IP address which he/she wishes to perform the scan. |
| **2** | General Information after scan | When the user starts the scan process, this interface will provide general information such as address, date, scan type, etc. |
| **3** | Brief Instruction/Display Log | This part provides basic instruction for the user on how to use the application. At the same time, this will be taken over by log display based on the scan data. |
| **4** | Stop Scan |  |
| **5** | Drop Down Menu | After the required address has been keyed in, the user can start either scanning of the IP or Port depending on whichever he/she chooses in the 3-dotted drop-down menu |
| **6** | Clear Log | To clear up all the log display |
| **7** | Open File | After each scan, the files will be saved under the device internal storage. The user will be able to open back these saved files at any time he/she wishes to do so. |
| **8** | Start Map Network | So as seen in the figure above, “Start Map Network” is for scanning based on IP definition. |
| **9** | Start Port Vulnerability | “Start Port Vulnerability Check” is for Port scanning so that the user will be able to analyze all associated services and port vulnerabilities. |
| **10** | Save list as default MACs | “Save list as default MACS” is for the users to perform comparison with for the future analysis. |

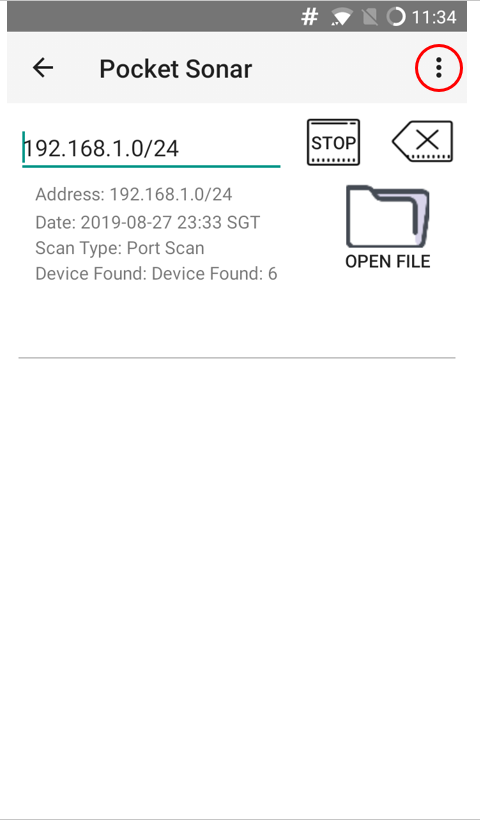


Figure 3.3.1.2. Device Scan User Input

After the required address has been keyed in, the user can start either scanning of the IP or Port depending on whichever he/she chooses in the 3-dotted drop-down menu as seen at the right top corner circled in red.

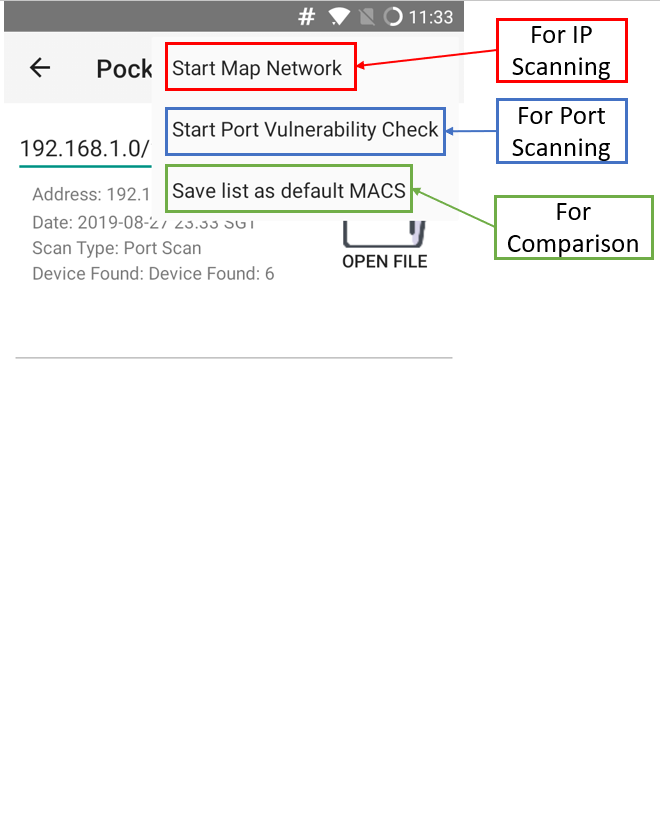


Figure 3.3.1.3. Scan Types and Options

So as seen in the figure above, “Start Map Network” is for IP scanning, “Start Port Vulnerability Check” is for Port scanning and “Save list as default MACS” is for the users to perform comparison with for the future analysis.

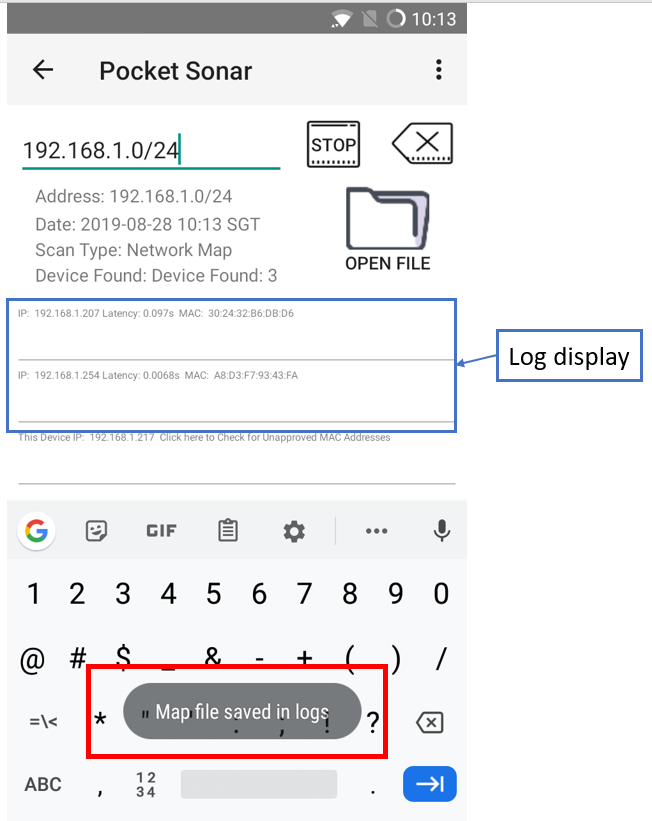


Figure 3.3.1.4. Log display

The log display is as shown in the blue box and after each

*Device Scan*, the logs will be then saved internally under “download” folder in the mobile device itself so that the users can use these history files as comparison for future analysis. The log will be saved in a format such as IP address, device name, latency and MAC information.

The process is still the same for Port scanning, where the user will have to key in the IP address. But for this case, instead of putting a range input (e.g. 192.168.1.0/24), the user will have to be specific with the address. For instance, he should specifically put “192.168.1.207” so that the application will focus on scanning the specific port and display out the log. Once the log has been displayed, the user will be able to click on it, which will then bring the user to the respective webpage where all the relevant TCP services associated with the port will be shown. This is how the user can make decision whether the ports are valid or not. Refer to the figure below.

1

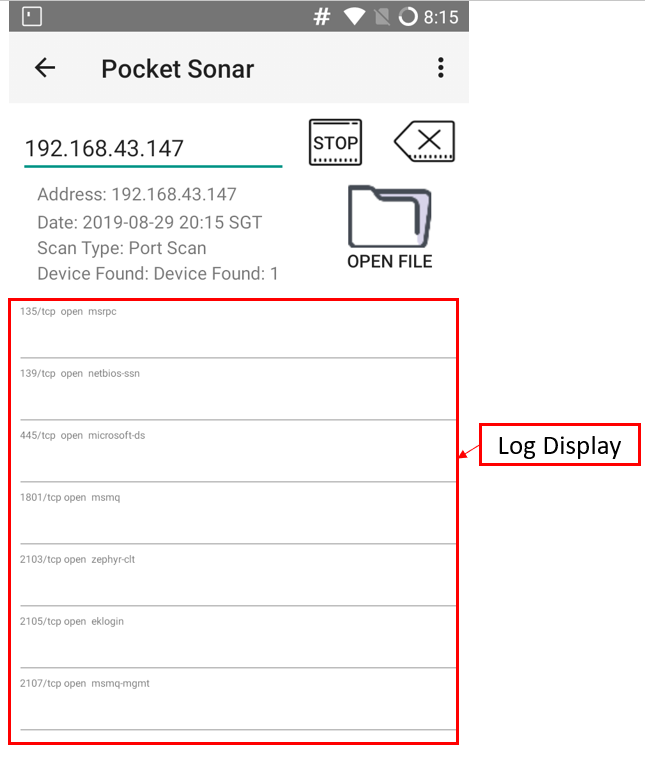


Figure 3.3.1.5. UI for Port Scan\_1

So as mentioned previously, if the user key in a valid address and press “Start Port Vulnerability Check” as shown in figure 3.3.1.3, the application will scan and display the output log. The user will then be able to click on either one of the data and by doing so, the application will prompt a website providing all the necessary detailed information of the respective port that has been scanned. The UI display is as shown below.

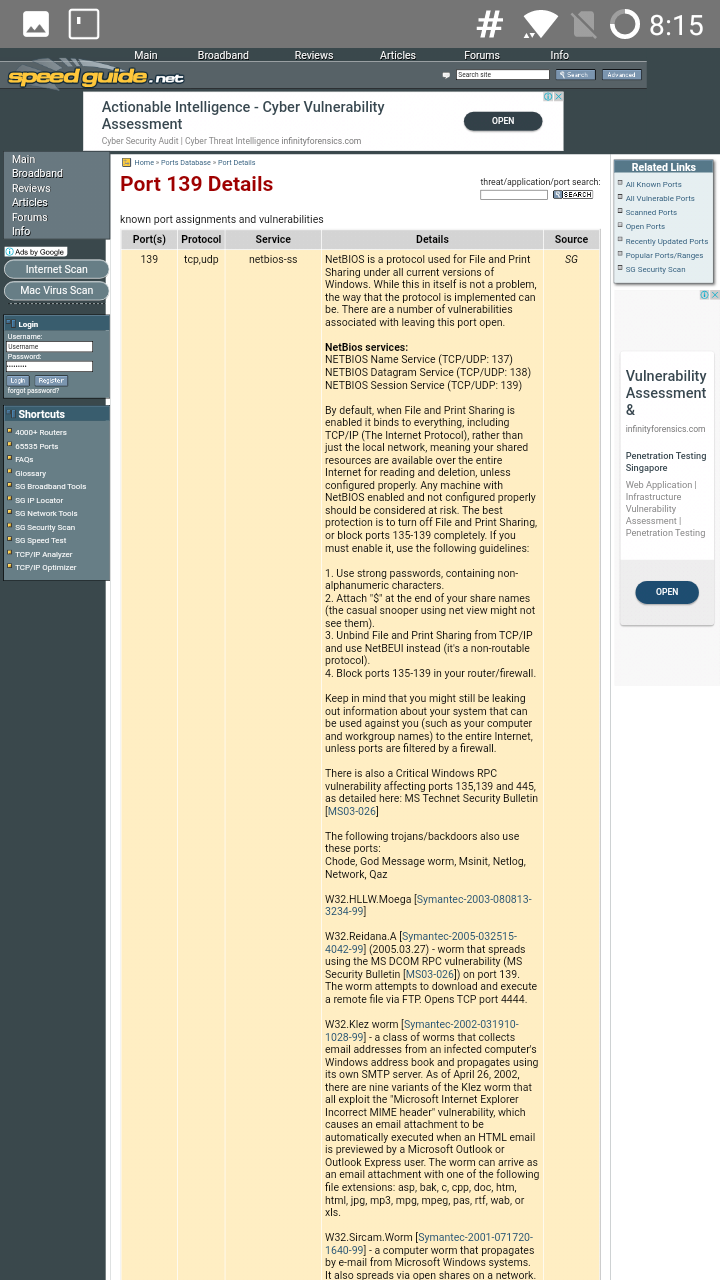


Figure 3.3.1.6. UI for Port Scan\_2

**3.3.2. *Packet Scan***

This part of the sub function is to sniff out all the packets for the connected network and display them out so that the user will be able to perform analysis on this. The interface is as shown below.

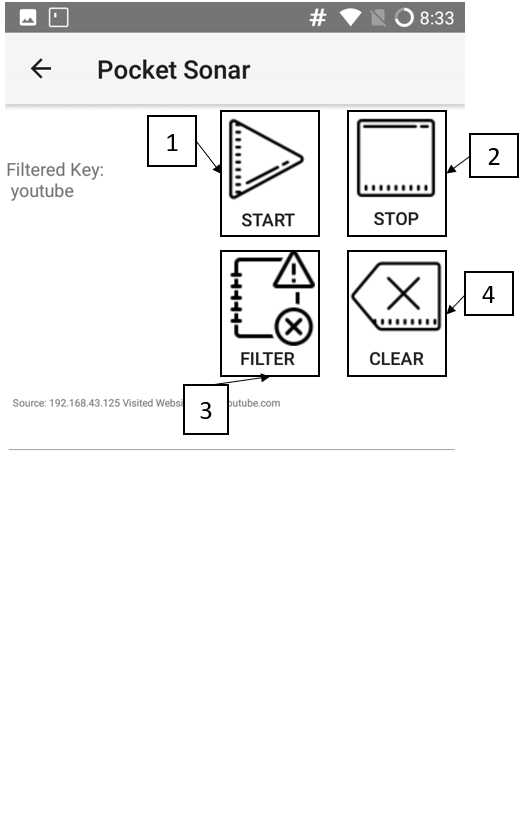


Figure 3.3.2.1. UI for Sniffing Packets

|  |  |  |
| --- | --- | --- |
| **No.** | **UI name** | **Description** |
| **1** | Start Sniffing | Start the sniffing process |
| **2** | Stop Sniffing | Stop the sniffing process |
| **3** | Filter Configuration | Filter the over sniffing process by keyword such as “Facebook”, “Google”, etc., so that only the packets associated with that keyword will be displayed |
| **4** | Clear Log | Clear the log display |

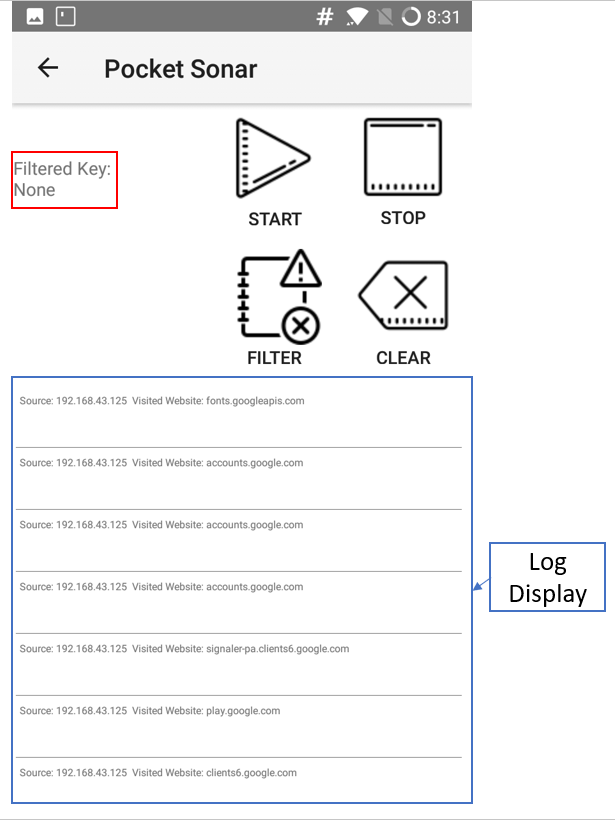


Figure 3.3.2.2. UI for Sniffing\_2

As you can see, for this type of sniffing, no filter configuration is set as shown in the red box and thus, all available packets on this network will be sniffed. Throughout the scanning process, the user will be able to press the stop button at any time to terminate the sniffing process.

Meanwhile, if we set the filter configuration with a certain keywork, for instance YouTube, then only the packets related that keyword will be sniffed and displayed as shown below.

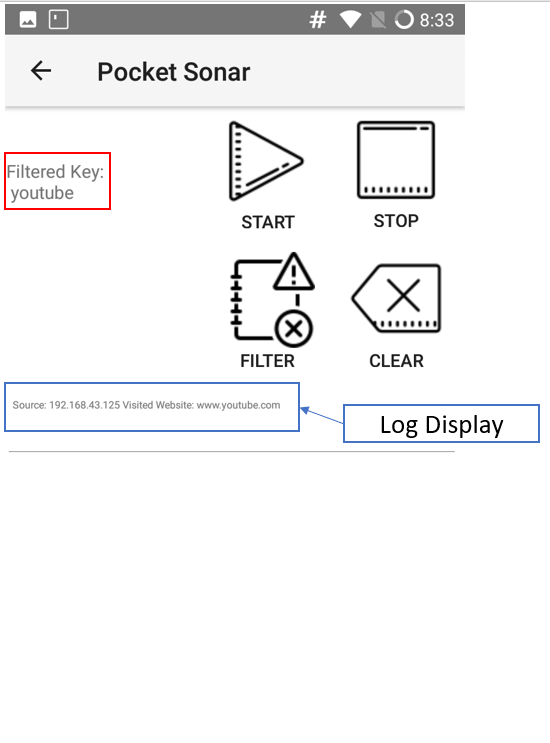


Figure 3.3.2.3. UI for Sniffing\_3

**3.4. *Network Tool***

**3.5. *Help Function***

This function provides general help for the user where brief description of the functions will be provided and at the same time, information on how to use the functions. In addition, some other information such as application version will be displayed as well.

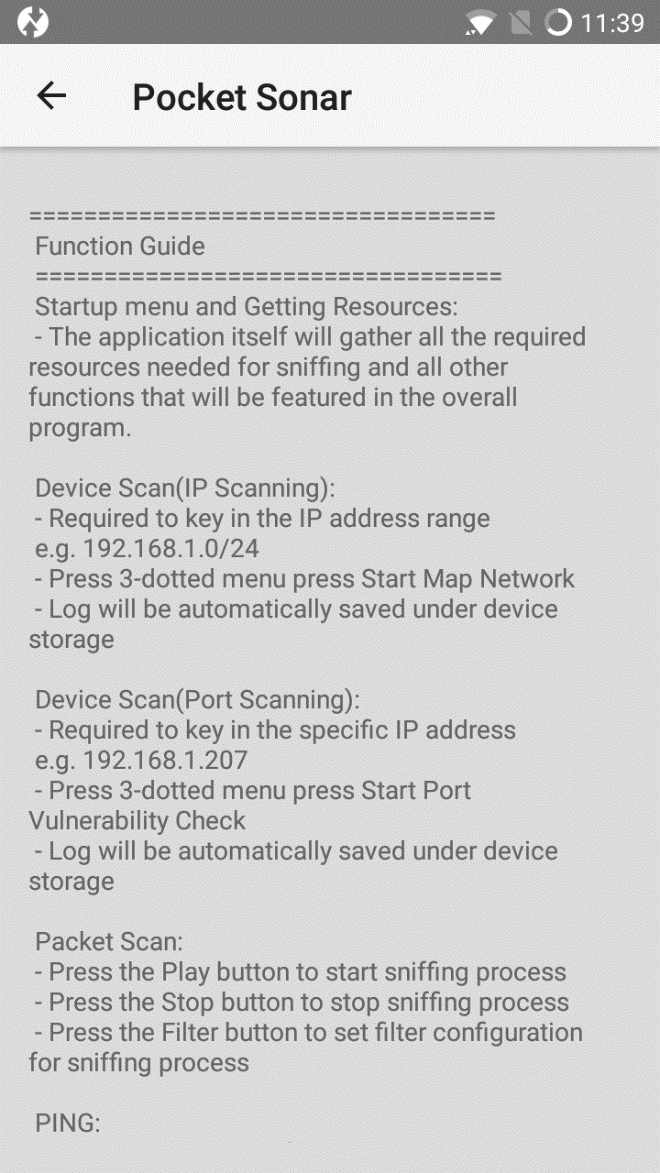
****

Figure 3.5.1. UI for Help(Instruction)

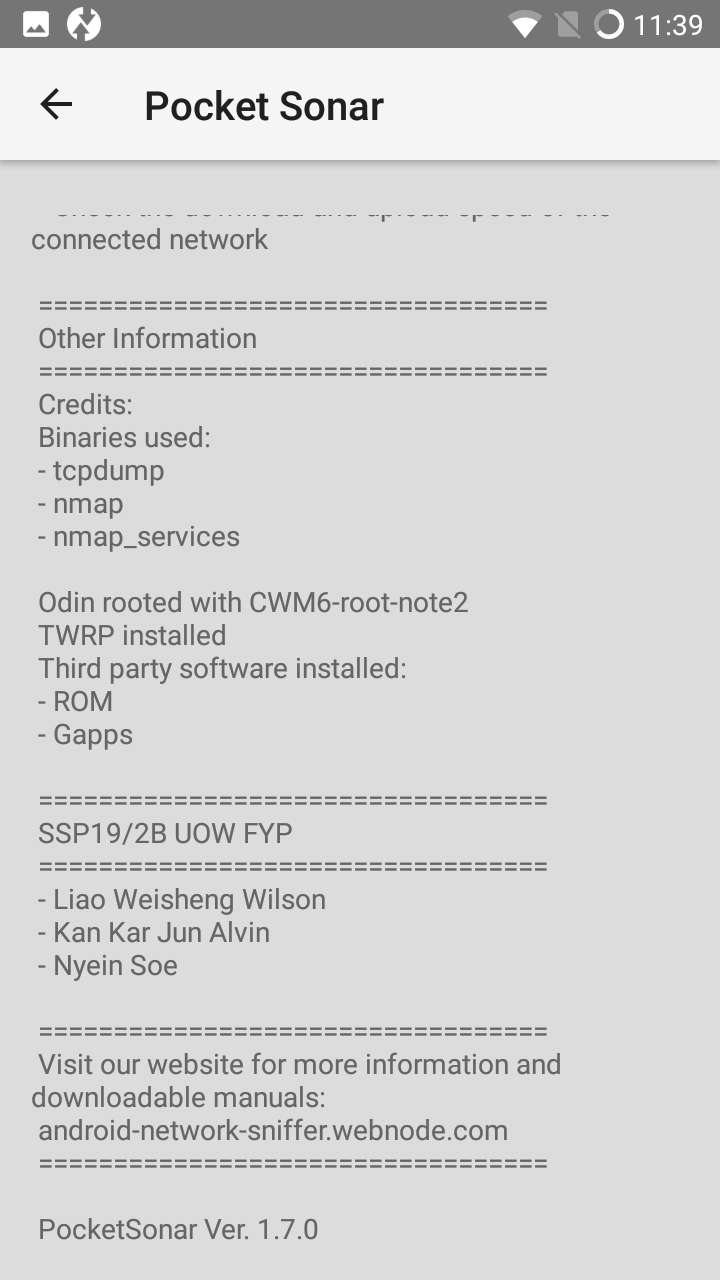


Figure 3.5.2. UI for Help(Application Information)

1. **Error handling on user side**

If the users encounter any error or problem using our program, they can directly email us or even call us, providing the details of their errors or problems they are facing, and our team will try out best to get back to you with possible solutions as soon as possible.

In addition, the installation procedure and steps on how to utilize the application will be found on our main website as mentioned previously.

1. **Team Members Profiles**

|  |  |
| --- | --- |
| **Name** | **Email Address** |
| NYEIN SOE | [soe018@mymail.sim.edu.sg](mailto:soe018@mymail.sim.edu.sg) |
| LIAO WEISHENG WILSON | [wwliao001@mymail.sim.edu.sg](mailto:wwliao001@mymail.sim.edu.sg) |
| KAN KAR JUN ALVIN | [kjakan001@mymail.sim.edu.sg](mailto:kjakan001@mymail.sim.edu.sg) |

1. **Guide on rooting android device before installing the application**

Basically, rooting a device enables the user to install custom ROMs, exclusive features from other devices and many other customizations.

As mentioned, for our program to work on an android device (preferably Samsung Galaxy Note2), the device must go through a rooting process using a Windows computer and this appendix will provide the necessary guidance on how any user can be able to root the mobile device.

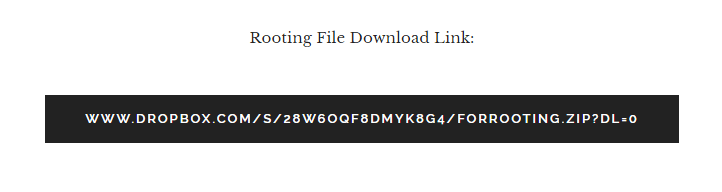
**Alternately, all the necessary files that are needed for the process can be downloaded through our website as well.**

Website: [**android-network-sniffer.webnode.com**](http://android-network-sniffer.webnode.com/).

**Step 1:**

As mentioned, since rooting is required, we have provided all the required resources that can be downloaded from our website as mentioned below. Alternately, if the provided download link is not working for some unforeseen reason, then the user may follow the instructions provided from step 2 onwards.

<https://android-network-sniffer.webnode.com/downloads/>



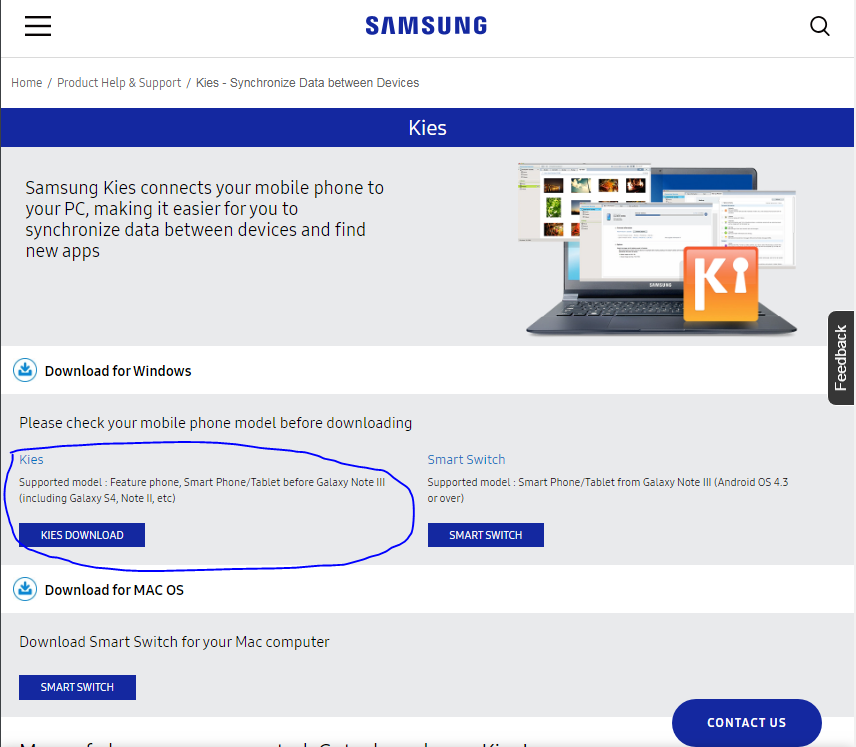
**Step 2:**

Before starting the rooting process on the mobile device, the user is required to download and install some necessary software, ODIN which will help perform the rooting process and SAMSUNG KIES which will provide easier synchronization data between the mobile device and the PC.

Alternately, all the required resources can be downloaded from the following links provided the download link in Step 1 cannot be opened.

The link below will provide the installation file for SAMSUNG KIES.

<https://www.samsung.com/sg/support/kies/>

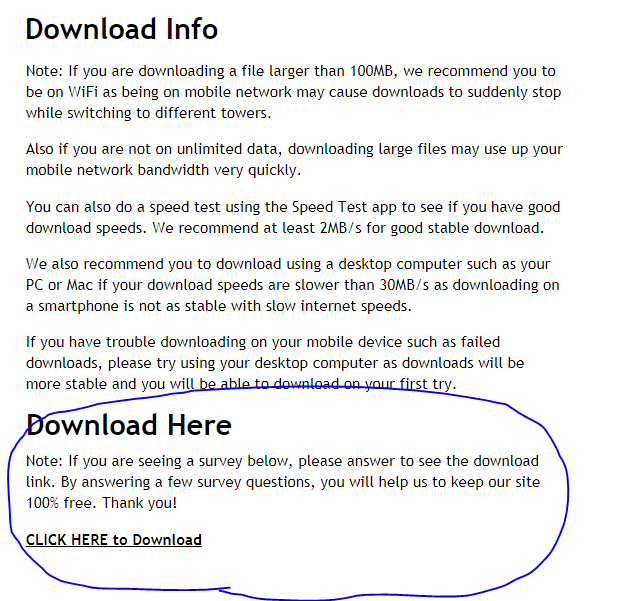


Simply click the download link and once the download is completed, simply click the installation file (.exe) and it will automatically install inside the PC.

From another link mentioned below, you will be able to get the ODIN file.

<http://downloadandroidrom.com/file/GalaxyNote2/rooting/GalaxyNote2Root.zip>

Once you have reached the webpage, scroll down until you see the download link as mentioned in the figure and simply click on it to start the download.



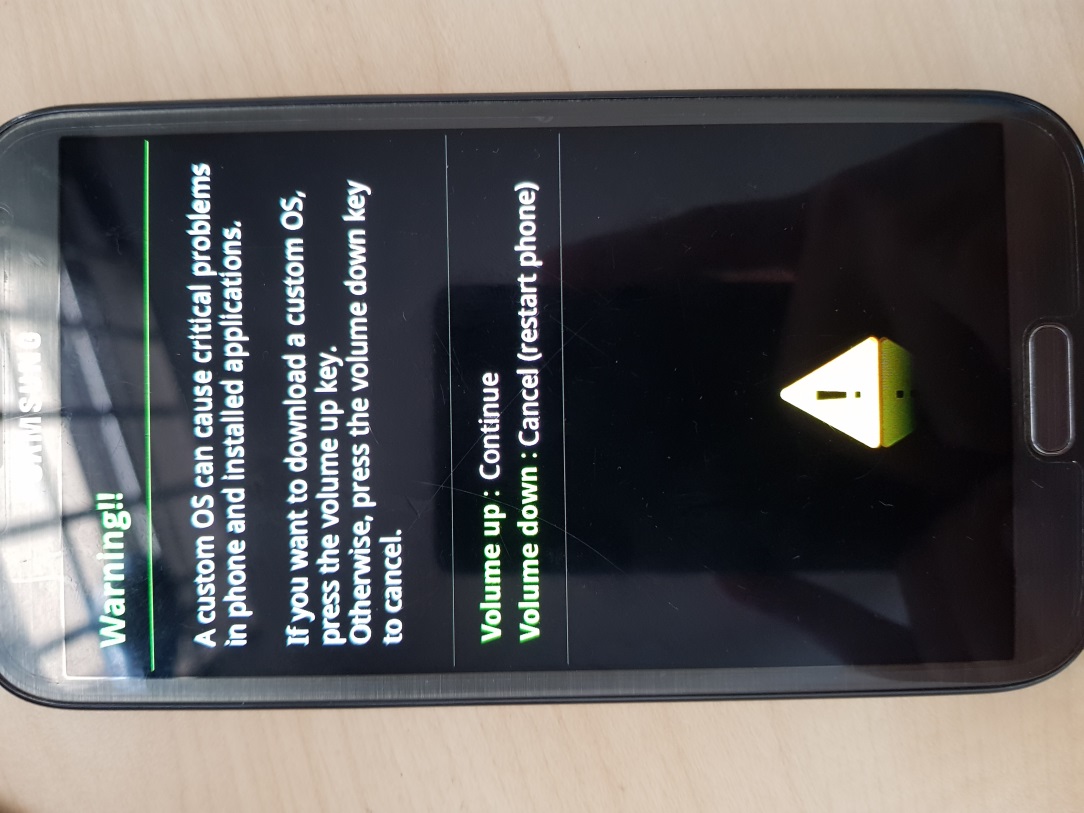
After downloading the zipped file, extract or unzip it and you will be able to see “odin3 v1.85.exe” application file.

**Step 3:**

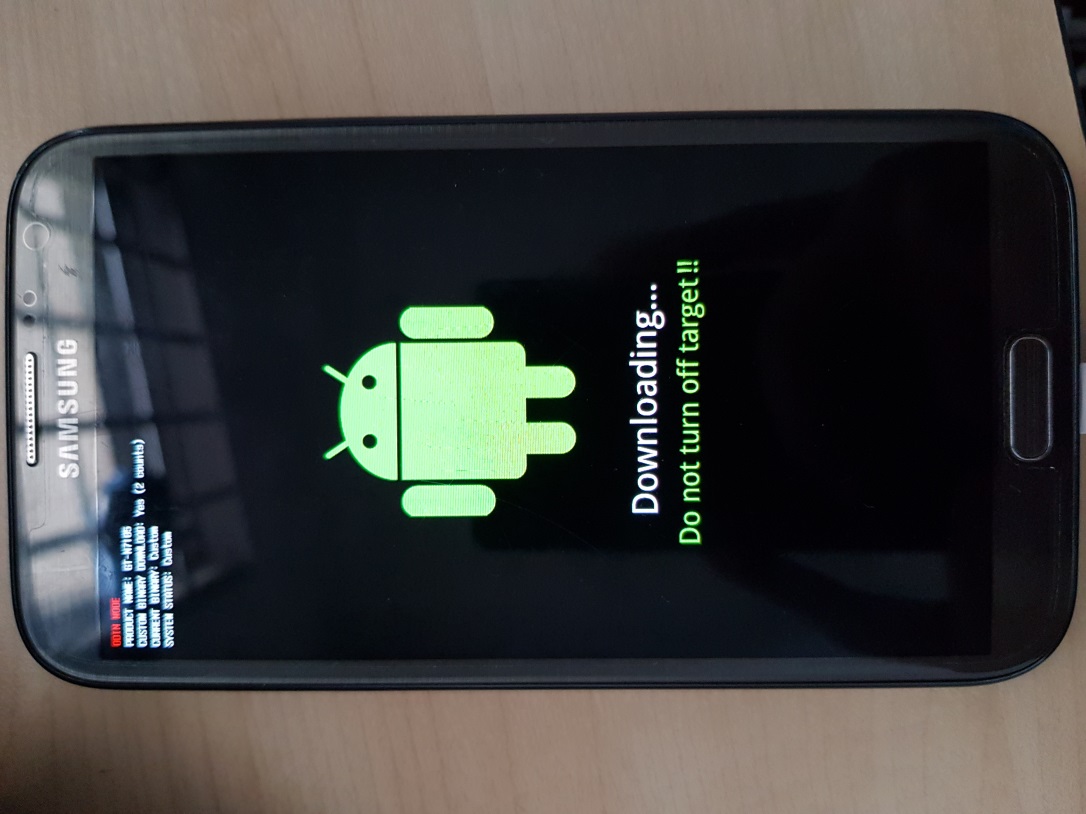
In this step, we will prepare the android mobile device so that it will be in a ready state to root.

First of, power off the device and make sure it is not plugged in to the computer.

Afterwards, **press and hold** the “**Volume Down Button + Home button + Power button”** until the screen as shown below can be seen.



As seen in the figure above, press the **“Volume Up Button”** to continue. This will then put your device in download mode as shown below.

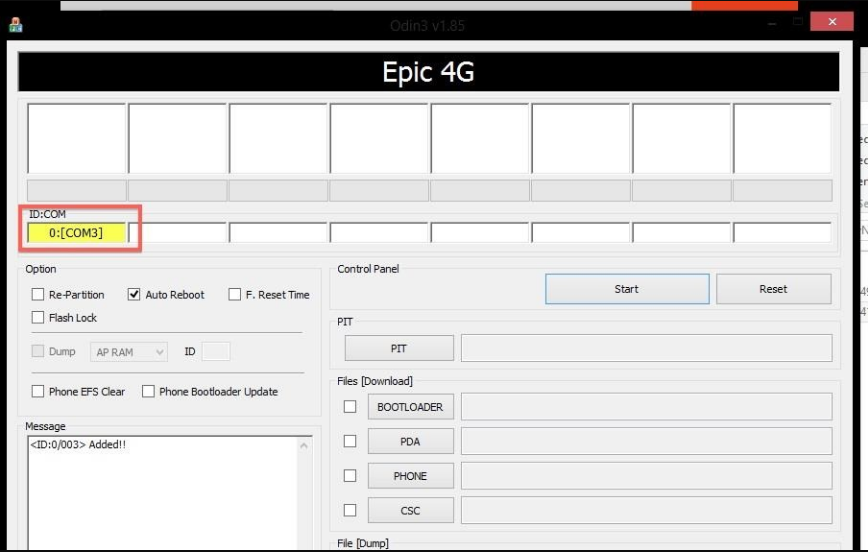


Once it has successfully entered downloading mode, you can then plug in the mobile device to your computer via USB cable.

**Step 4:**

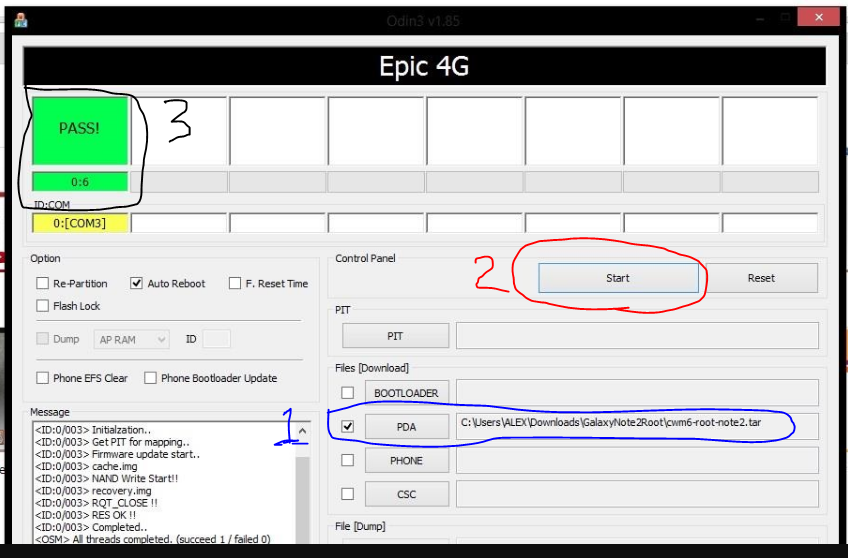
Since we have already installed ODIN program in step 1, open the program and make sure the android device is already connected to the computer as mentioned in step 2.

Once opened, you will be able to see a **yellow ID:COM** box with some random numbers in it as shown below. If you are not able to see this for some reason, you can check whether the **SAMSUNG KIES** is properly installed and another thing you can do is by unplugging the android device and plugging back in.

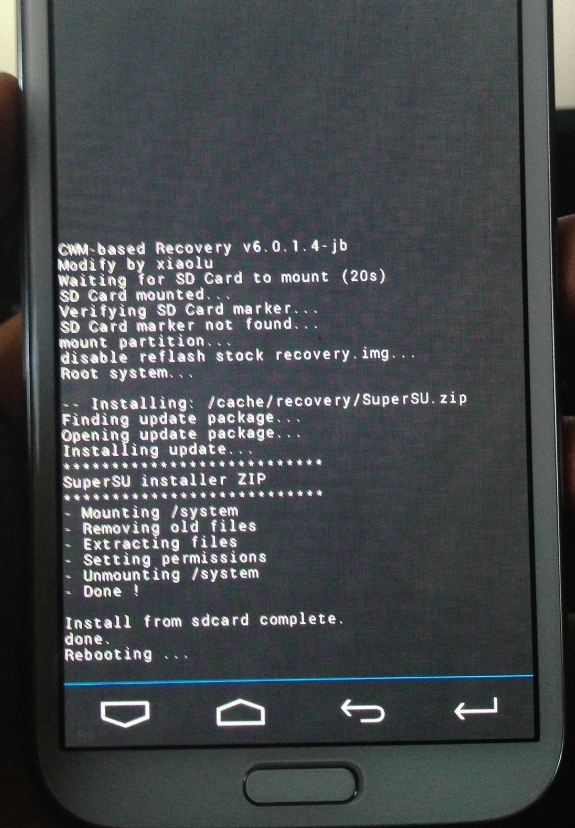


Previously when we have downloaded the zipped file for ODIN installation process as mentioned in step 1, the zipped file should include **“cwm6-root-note2.tar”** file. Afterwards without changing any other settings in the ODIN program, simply click on the **“PDA”** button under **“Files [Download]” [1]** as shown below and navigate to the folder where the “.tar” file has been saved previously. Select the file and click **“Start” [2]**.

Now ODIN will perform the automatic installation on the mobile device and if it is successful, you will be able to see the green **“PASS!”** box in the program **[3].**



When it finishes, your device will boot into **ClockworkMod (CWM) Recovery** one time in order to install the **SuperUser** app and its binaries. Then, reboot again.



After everything has been installed, the device will automatically reboot and the rooting process is done.

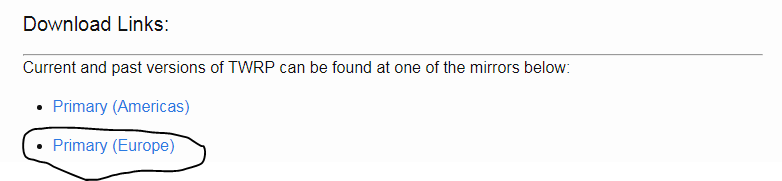
**Step 5:**

In this step, we will be guiding you on how to install TWRP (TeamWin Recovery Project) and this application is an open source software custom recovery for rooted Android devices. It is also helpful to install third party firmware and backup the system which in our case, we will be using this TWRP to install some additional third-party firmware, namely custom ROMs and Gapps.

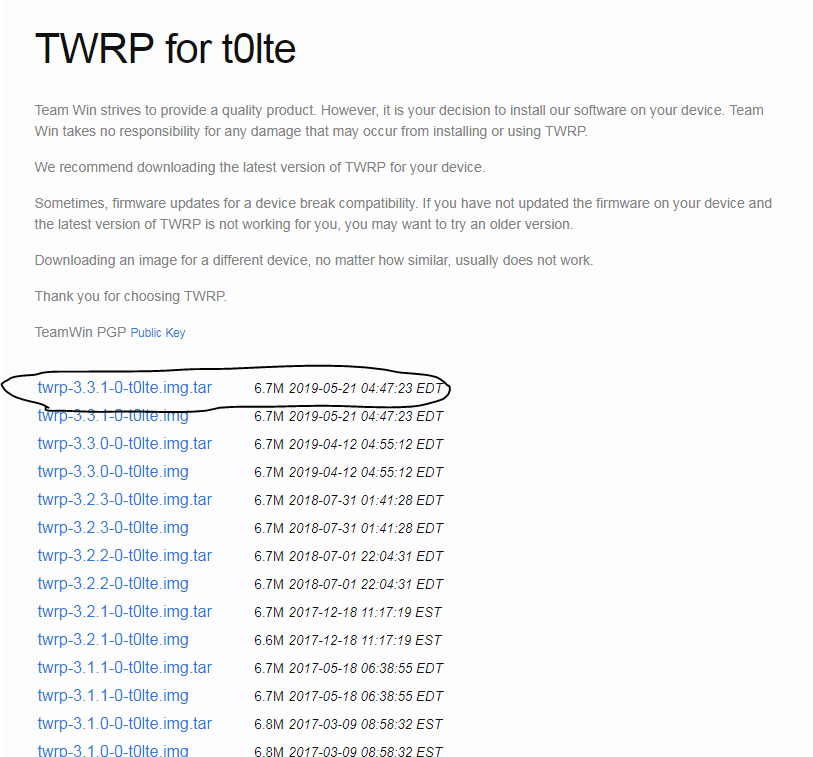
The user will be able to download the TWRP application from the following link.

<https://twrp.me/samsung/samsunggalaxynote2n7105.html>

Once you have reached the webpage, it is recommended to install by downloading under **“Primary (Europe)”** as shown below.



After clicking the link as mentioned above, we are required to download the latest .tar file as shown below.



After the .tar file has been downloaded, we will then use ODIN program to install into our mobile device and the steps are exactly the same as mentioned in Step 2 and Step 3.

First off, power off the phone and set it to “Downloading state” [See step 2].

Once it has been set to this state, you can plug in the device to your computer via USB cable and open up the ODIN program. Here, the steps are very similar to those in step 3.

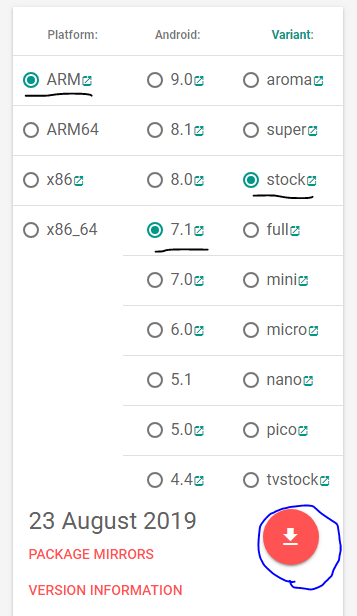
But for this case, after clicking “**PDA”**, you are required to navigate to the folder where you have saved the twrp.tar file. Once the pathway has been set, simply click the “**START**” button and the twrp will then be installed in the rooted android device.

**Step 6:**

After successfully installing TWRP app on the rooted device, we will then move on to install some custom third party firmware so that the device will be compatible to use our sniffing application.

First, we have to download the zip file for Gapps and the link is as shown below. Please note that the platform, android model and variant should be selected correctly and download as shown. Otherwise, there might be some problems when installing the main application.

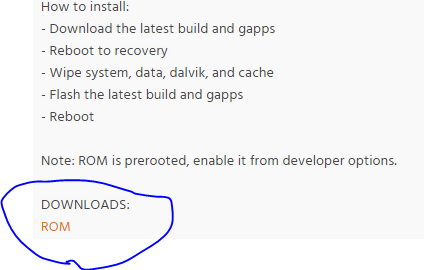
<https://opengapps.org/>



Next, we will download the required ROM and the link is as given below.

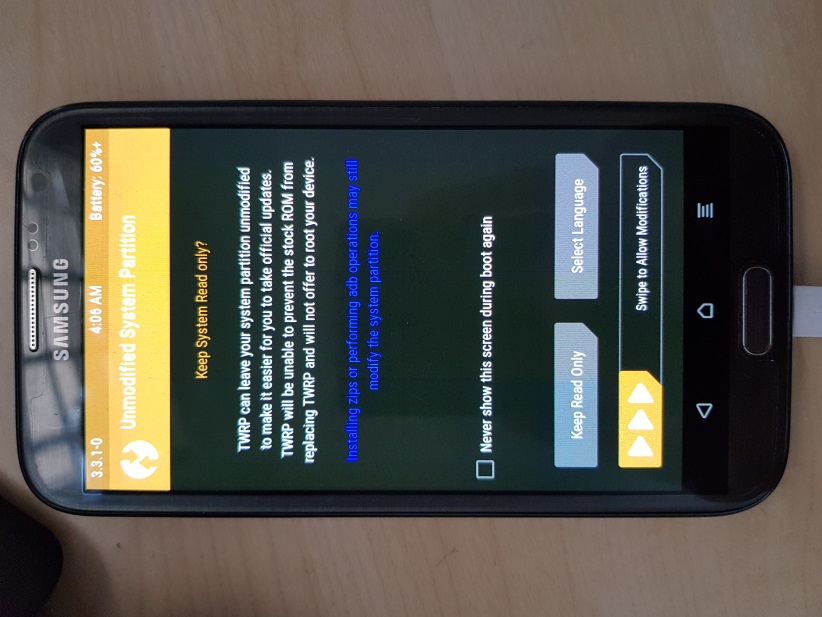
<https://forum.xda-developers.com/galaxy-note-2/development-n7105/crdroid-unoffical-build-t0lte-t3721152>

Simply go to Downloads section and click on “ROM” and download the respective zipped file depending on the device model.

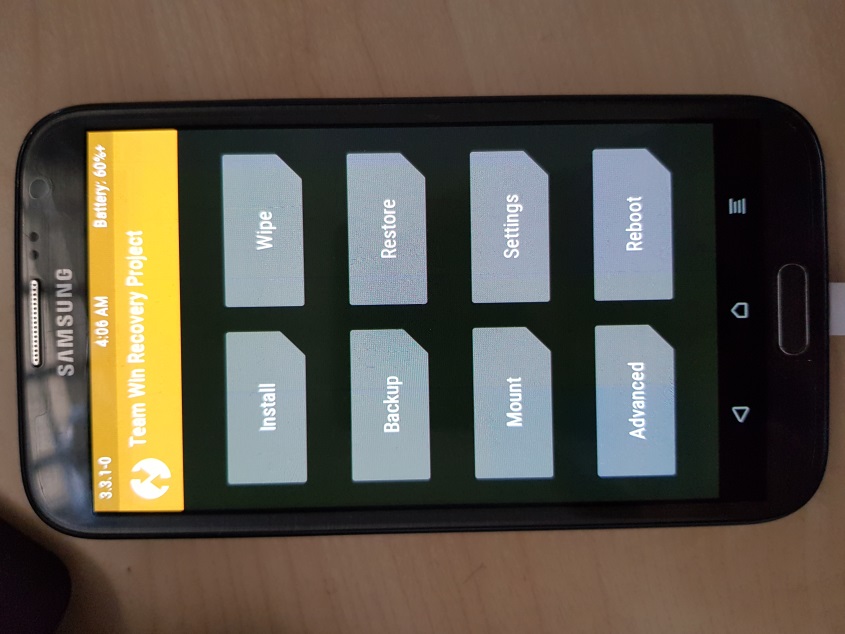


After downloading the required two zipped files, Gapps and ROMs, you can just simply transfer (copy/paste) it over to one of the folders under the android mobile device. Please also note that the directory of the folder that you have copied over the files must be remembered. After the files have been copied over, you can unplug the phone and power off.

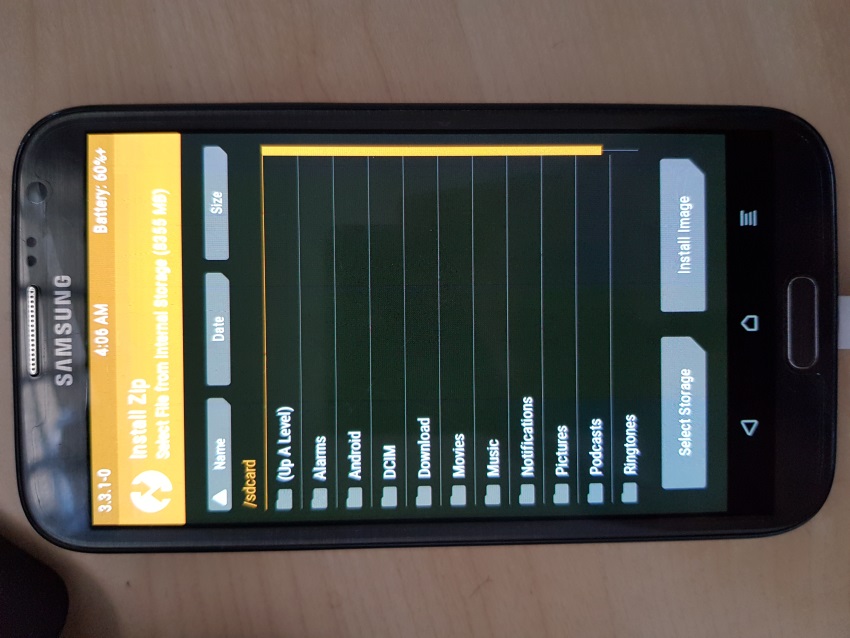
From this point on, we will put the phone under recovery mode. In order to do this, you have to press and hold **“Volume up button + Home button + Power button”.** When doing so, the phone will look like powering up normally but when the you see this happening, **DO NOT** let go of the button but continue pressing. The screen will then black out and power up again. Only then, the user should let go of the three buttons. If done properly, they will reach the recovery page as shown below.

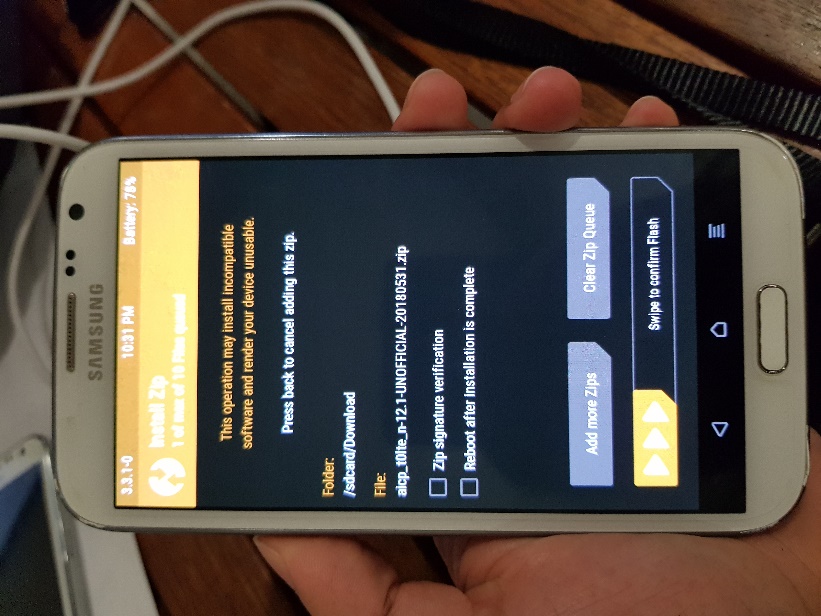


Once you have reached the page as shown above, simply swipe as mentioned to go to the setting page.



Now that we are in the setting page, first thing we need to do is to press “**Install”.** After pressing, it will take you to the next page as shown below. This is where you have to navigate to the folder where you have transferred the zipped files for Gapp and ROM. Once you are in the directory, simply select the zipped file and press “**Select Storage”** followed by “**install Image**” as shown. It is recommended to install ROM first then followed by Gapps.

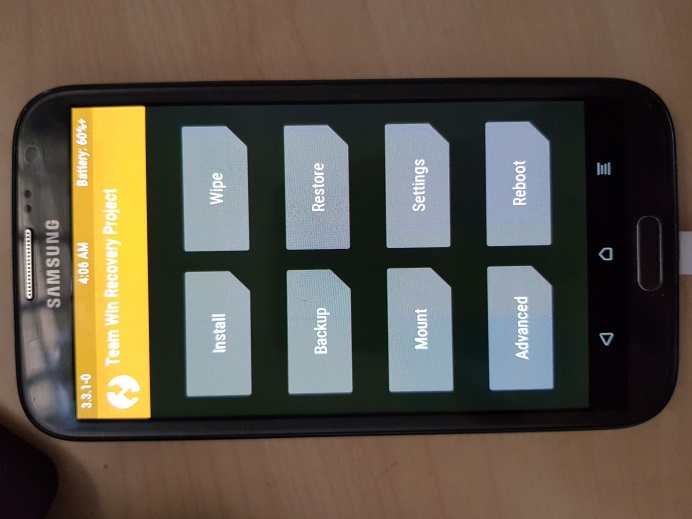




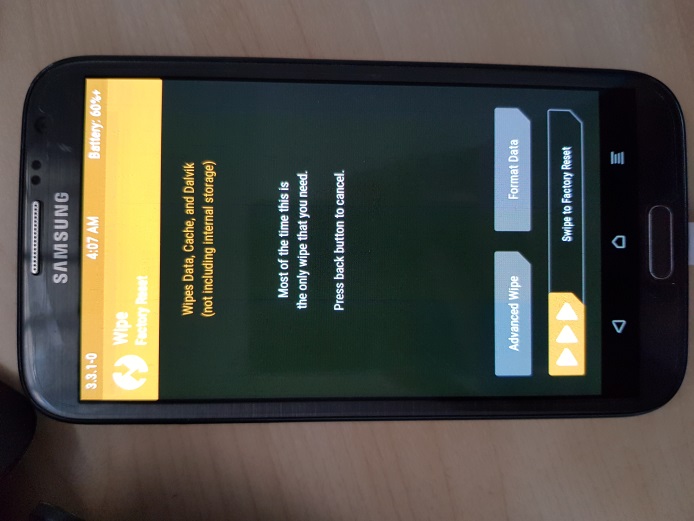
You can select multiple zip files then swipe as shown above to start the flash process. Then you will be able to see the below installation process.



After installing everything, go back to the home page by pressing the home button. Then press “Wipe” this time.



This will take you to the page as shown below.



From here on, simply swipe the bar below and this will reboot the mobile device. This is the final step for all the rooting process and now your device is finally ready to install the main Network Sniffing application (PocketSonar).