SNIFFING VOIP CALLS USING A RASPBERRY PI

Table of Contents

1. Abstract

Voice over Internet Protocol (VoIP), is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.

Because of the bandwidth efficiency and low costs that VoIP technology can provide, businesses are migrating from traditional copper-wire telephone systems to VoIP systems to reduce their monthly phone costs. In 2008, 80% of all new Private branch exchange (PBX) lines installed internationally were VoIP[1].

The use of Voice Over Internet Protocol (VOIP) calls by criminals, have proved to be a hindrance in its investigations. The first use of VOIP calls was seen during the 26/11 terror attacks of 2008 and, since then, the practice has become alarmingly common among criminals, especially underworld elements who operate from outside the country[2].

This project aims at using the compactness and portability of raspberry pi for intercepting VoIP calls for investigative purposes.

2. Literature Review

As being an old concept, sufficient research is done on VoIP technology, security and forensics. Some of the relevant articles are cited here. Researcher Rakesh Arora have worked on understanding protocols and standards used in VoIP implementation[3] while Sohil Garg have worked on possible attacks on VoIP infrastructure[4]. Solutions have been proposed for the possible attacks vectors[5] by Santi Phithakkitnukoon, Enkh-Amgalan Baatarjav, Ram Dantu. Also efficient research has also been done on the forensic aspects of VoIP[6][7]. However, different researchers worked on enhancing security and forensics practice for VoIP attacks, no researcher has worked on sniffing VoIP call over a portable, robust, compact standalone device like a raspberry pi. This project focuses on the above mentioned untouched aspect in VoIP forensics.

3. Introduction

VoIP known as IP Telephony is the real-time transmission of voice signals to the Internet Protocol (IP) over the public Internet or a private data network. VoIP converts the voice signal from telephone into a digital signal that travels over the Internet. most important advantages of VoIP are that one can make a long distance phone call and bypass the toll charge. This integrated voice/data solution allows large organizations to carry voice applications over their existing data networks. Not only will this technological advancement have an impact on the large traditional telecommunications industry, it will alter the pricing and cost structures of traditional telephony (over a traditional public switched telephone network (PSTN - also known as a legacy networks). IP networks can carry 5 to 10 times the number of voice calls over the same bandwidth. However, through IP networks to transmit voice and other information, VoIP has inherited the security issues of Internet Protocol networks. As by default the Internet Protocol networks are not encrypted, the underlying VoIP calls are made in plain text. Though is a major security flaw, it is also a bone for a forensic expert as he can sniff and intercept the calls.

3.1 VoIP Packets

H.323

The procedures, elements and protocols specified by the H.323 standard that provides multimedia communication across packet-based networks. Multipoint multimedia or Point-to-point communication services is being provided by H.323 system when its four main elements Multipoint.

SIP

SIP (Session initiation protocol) is a communication protocol used for signalling and controlling multimedia communication sessions such as online gaming, instant messaging and various services. It is similar to web protocol HTTP since messages comprises of headers and a message body. SIP generally uses port 5060 as its default protocol for either TCP or UDP. SIP can be interpreted as the authorize protocol for voice, telephony and video over IP (VoIP) services.

Media Gateway Control Protocol

MGCP is a protocol for handling telephony and VoIP gateways from external network call control devices called Call Agents. The MGCP protocol assumes call control devices or Call

Agents, establish with each other to send commands to the they control. Call Agents also connect directly to IP Phones. The Media Gateways or IP Phones are run commands sent by the Call Agents. The figure shows the MGCP elements and call control actions.

RTP

RTP is using for real-time stream data transfer over the network. It allows data transfer to multiple destinations using IP and treated as primary protocol for audio/video transport within IP networks. RTP is used with a signalling protocol that assists in build-up connections across the network. The RTP protocol is useful for audio and video streaming. Two RTP sessions establishes for video streaming and each with different SSRC identifiers out of which one is useful for audio transmission whereas another for video transmission. Also, there is downside of RTP that it neither assures delivery of packets nor Quality of Service.

4. Lab Configuration

For the scope of this research, the following lab scenario is being considered:

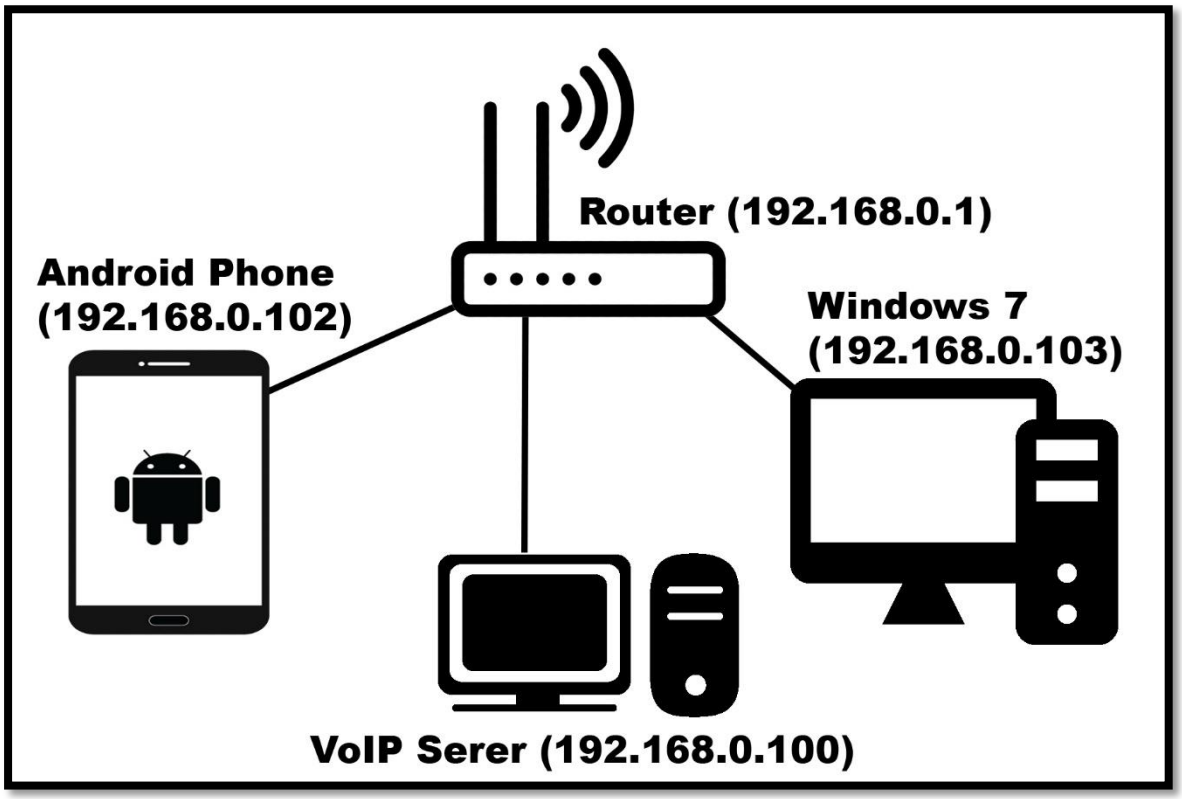

Figure 1 Lab Configuration

- Router

TP Link AC750 Wireless Router

Network Address: 192.168.0.1

- VoIP Server (Asterisk)

Network: 192.168.0.100

- Windows 7 Home System

Network Address: 192.168.0.103

Zoiper Softphone 1

- Android 5.1.1 device

Network Address: 192.168.0.102

Zoiper Softphone 2

4.1 Asterisk Configuration

Asterisk is an open source framework for building communications applications. It powers IP PBX systems, VoIP gateways, conference servers and other custom solutions. It is used by small businesses, large businesses, call centre carriers and government agencies, worldwide. Asterisk is free and open source.

Today, there are more than one million Asterisk-based communications systems in use, in more than 170 countries. Asterisk is used by almost the entire Fortune 1000 list of customers. [9]

Asterisk ISO can be downloaded from here .

Setup

Begin with creating a virtual machine 3 GB RAM, 50 GB Hard Disk space and 1 processor CPU.

Later, move inside Settings -> Storage -> Controller: IDE -> Add Asterisk ISO image.

Now, move inside network settings and set the adapter to “Bridge Adapter”.

Start the virtual machine, select option specified in screen shot.

Provide password for “Root” account.

Once configuration will be completed, the system will reboot. Once rebooted user will be greeted with following screen.

Here, account username is root. Password is one set in previous setting.

Look for the server IP Address.

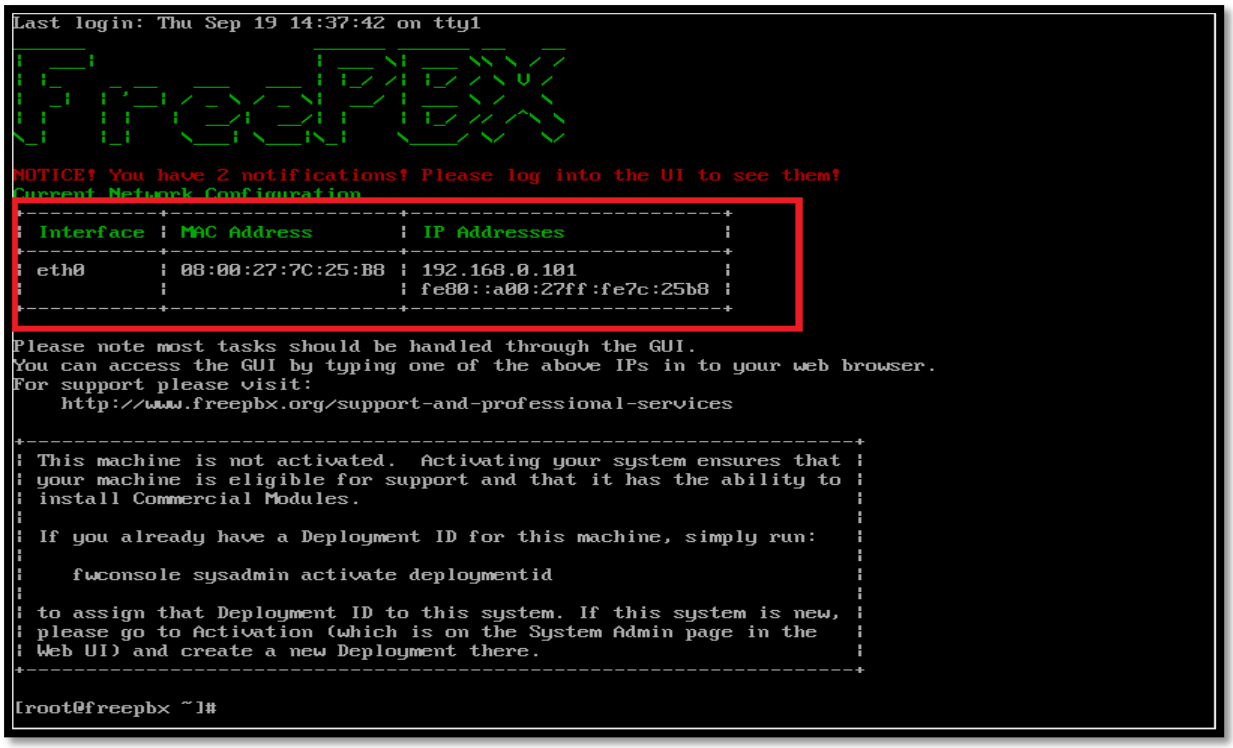

Figure 2 Server IP Address

Inside a web browser, traverse to the asterisk server IP address. User will be prompted to setup user account. Enter the required details.

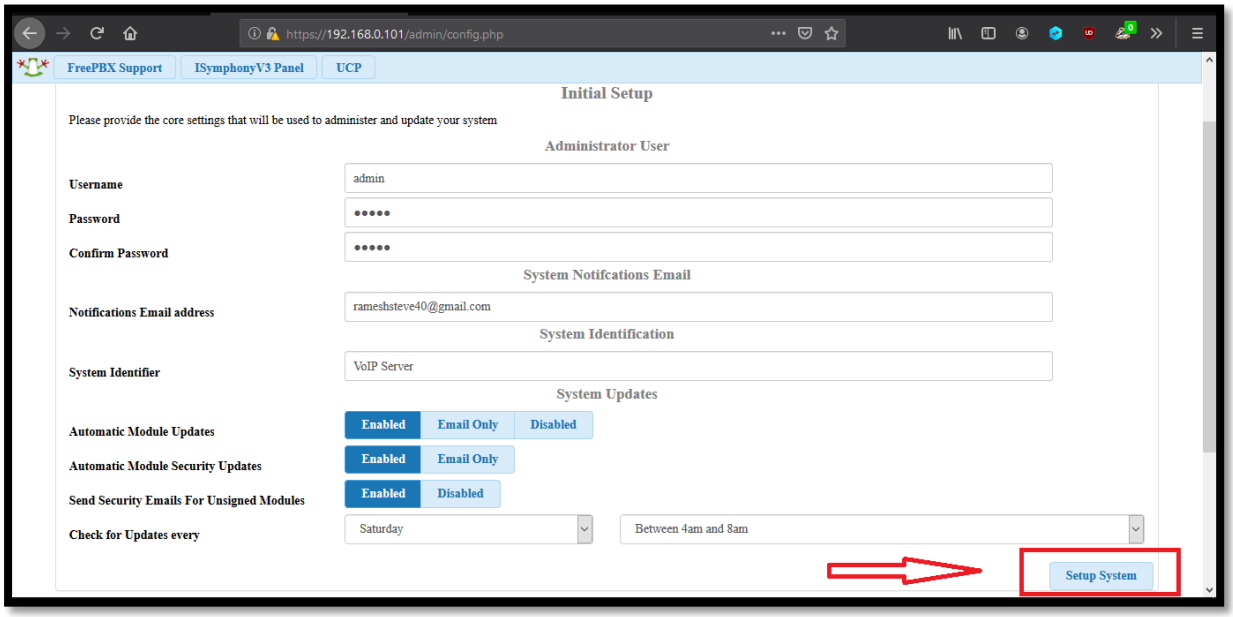

Figure 3 Setting User Account

After completing setup, move inside “FreePBX Administration”.

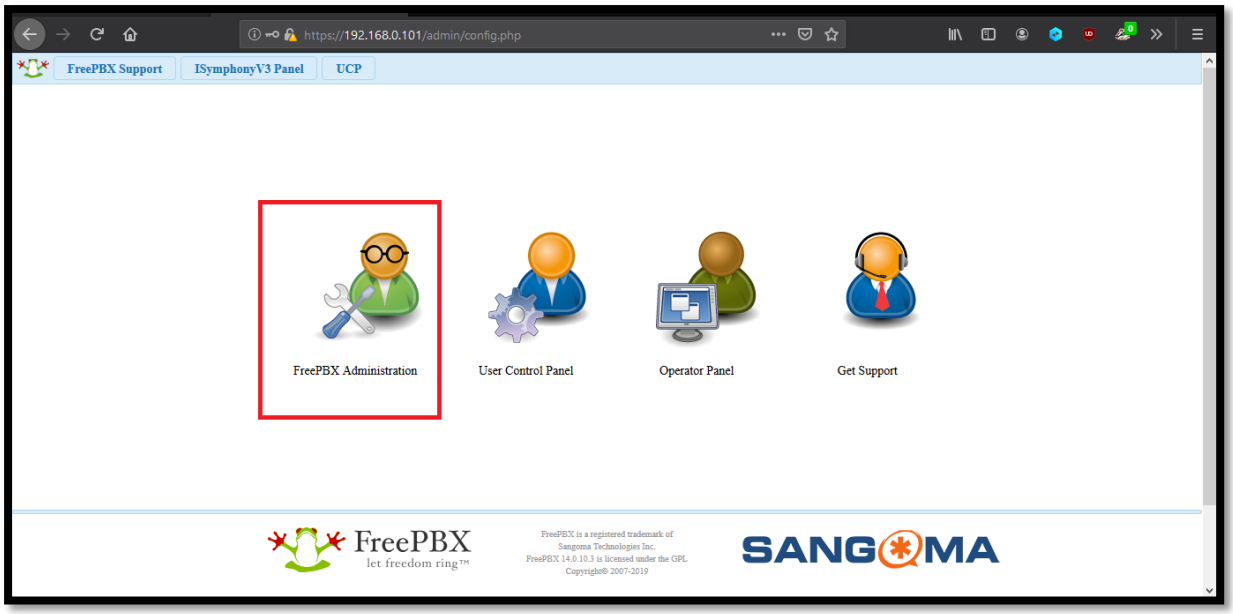

Figure 4 FreePBX Administration

Activate FreePBX.

User must provide an email address.

Select language and time zone and hit submit.

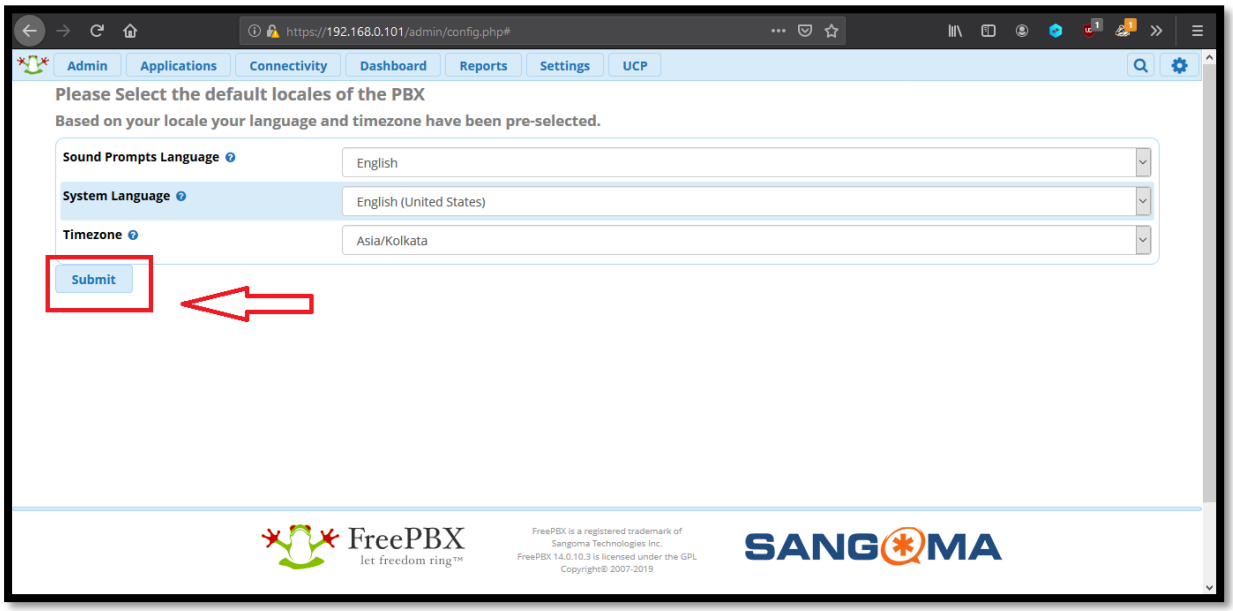

Figure 5 Language and Time Zone

In the next step, enable Sangoma Firewall.

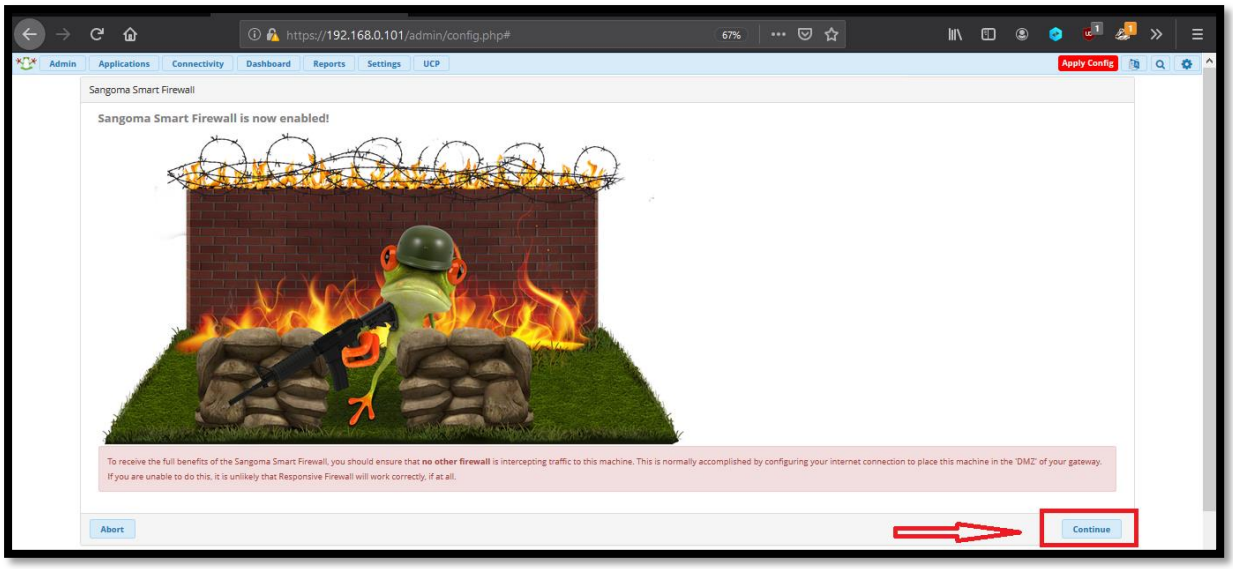

Figure 6 Setting Smart Firewall

Trust the underlying network.

Select “Yes” for automatically configuring asterisk IP settings.

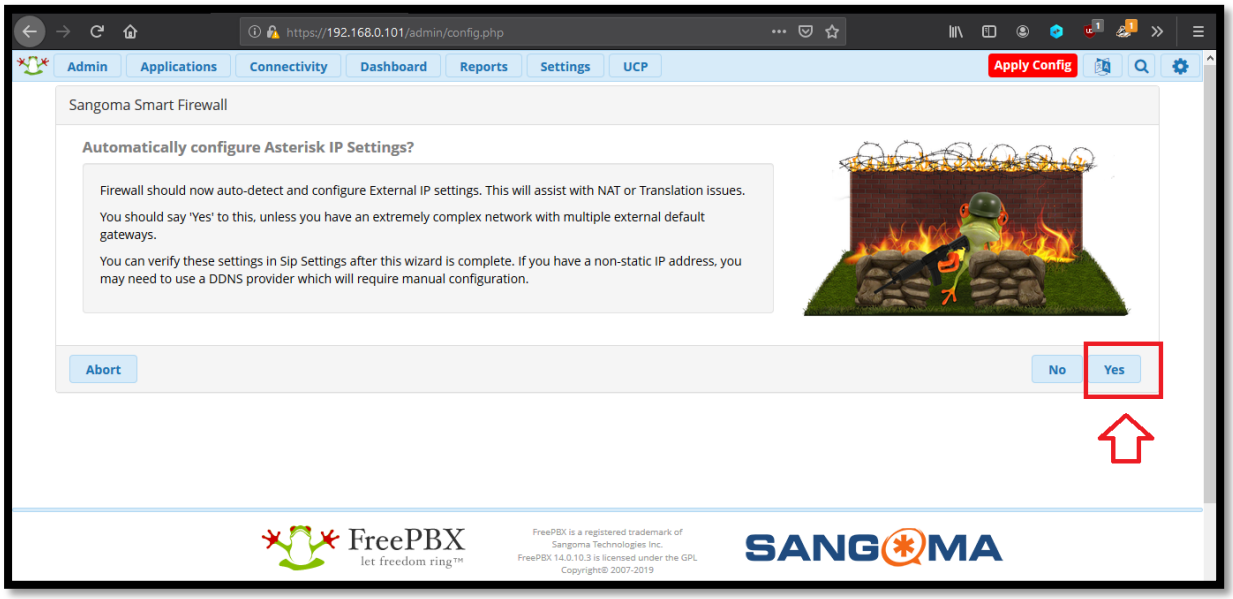

Figure 7 Automatically configuring IP Settings

User will be presented with a dashboard.

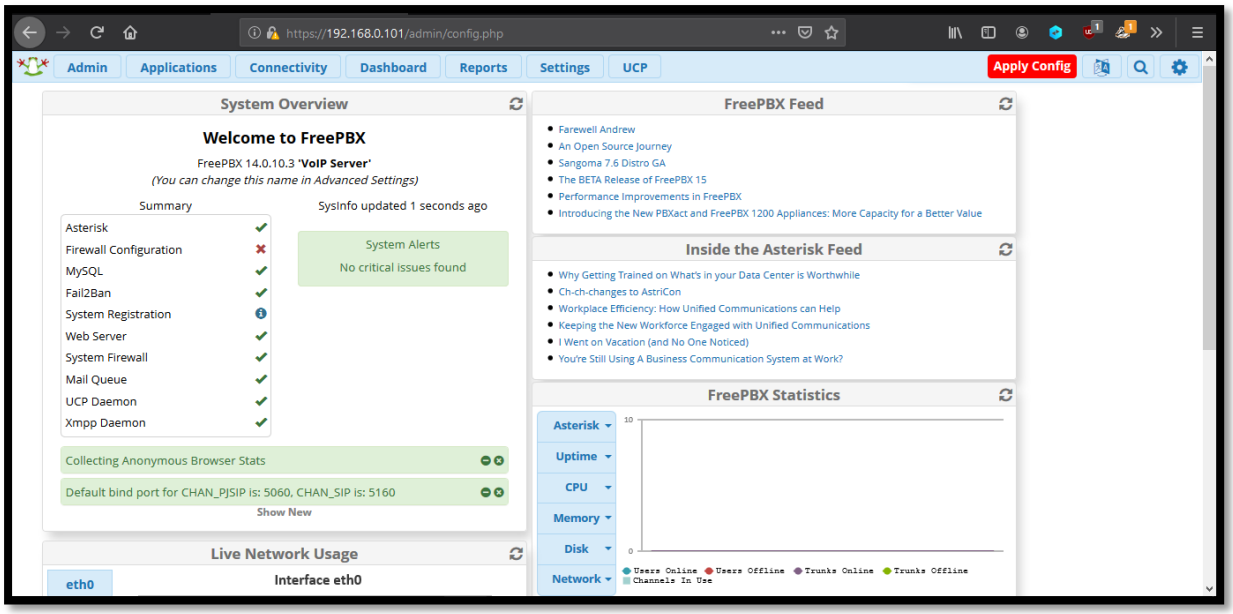

Figure 8 Asterisk Dashboard

Let's now add Extensions. Go to Applications -> Extensions.

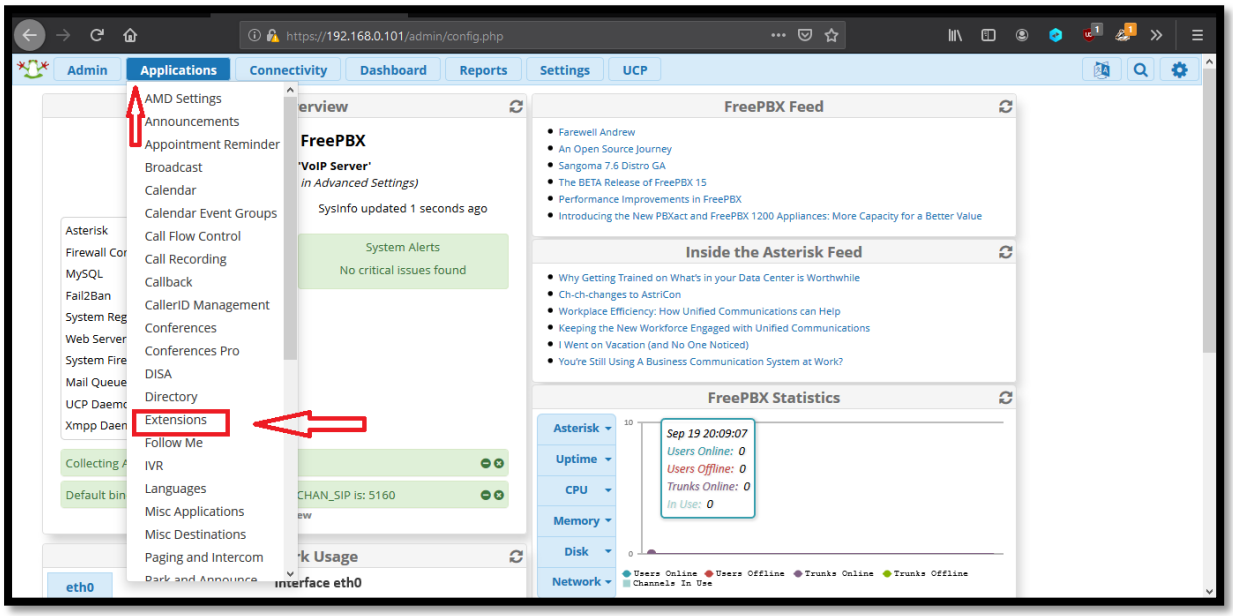

Figure 9 Adding Extensions

Under "Add Extensions", select "Add new CHAN_SIP Extension".

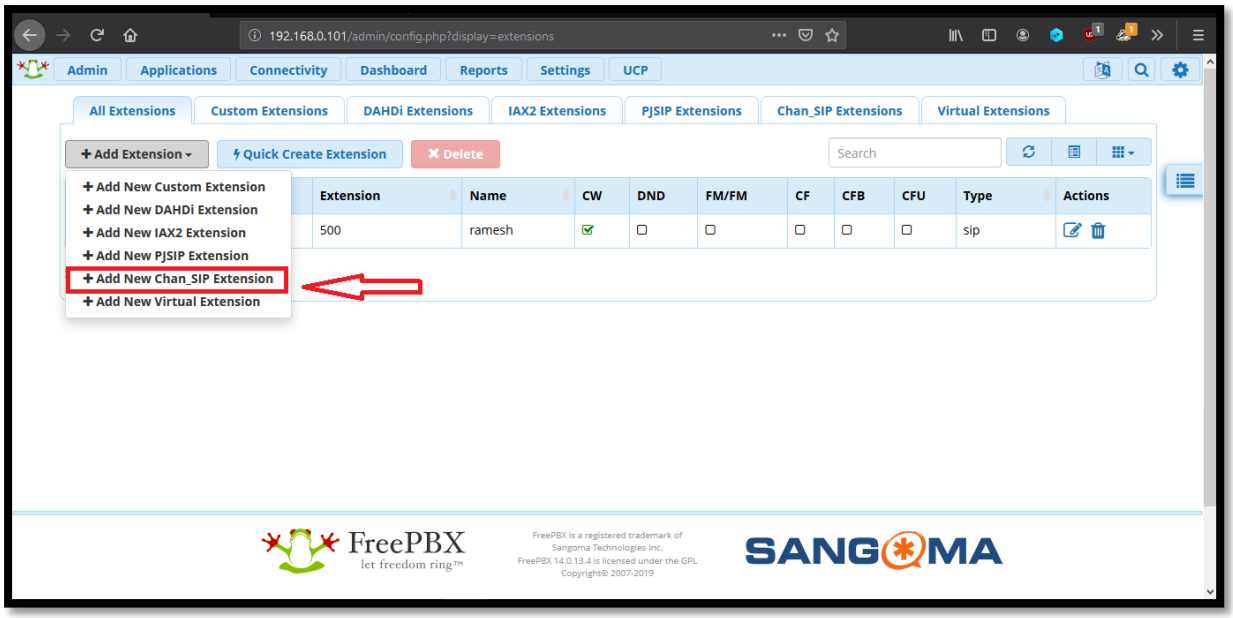

Figure 10 Chan-SIP Extension

Provide with details like, User Extension, Display Name and Secret.

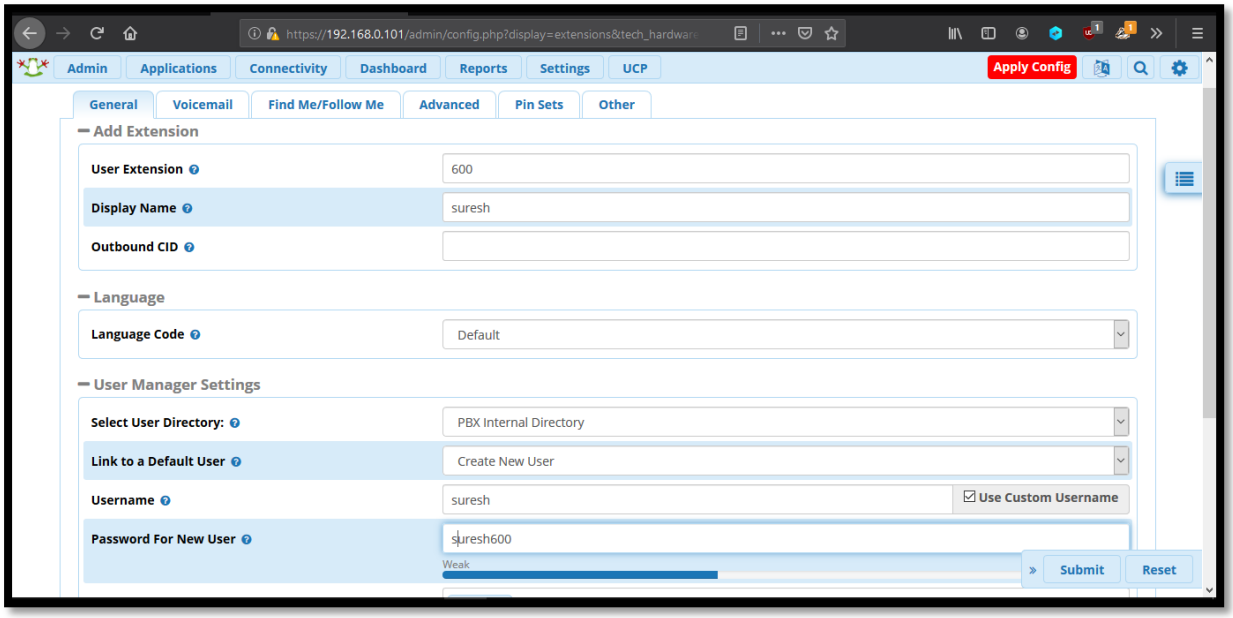

Figure 11 User Details

Similarly, create second Extension.

Inside, Applications -> Extensions, we can view the created Extensions.

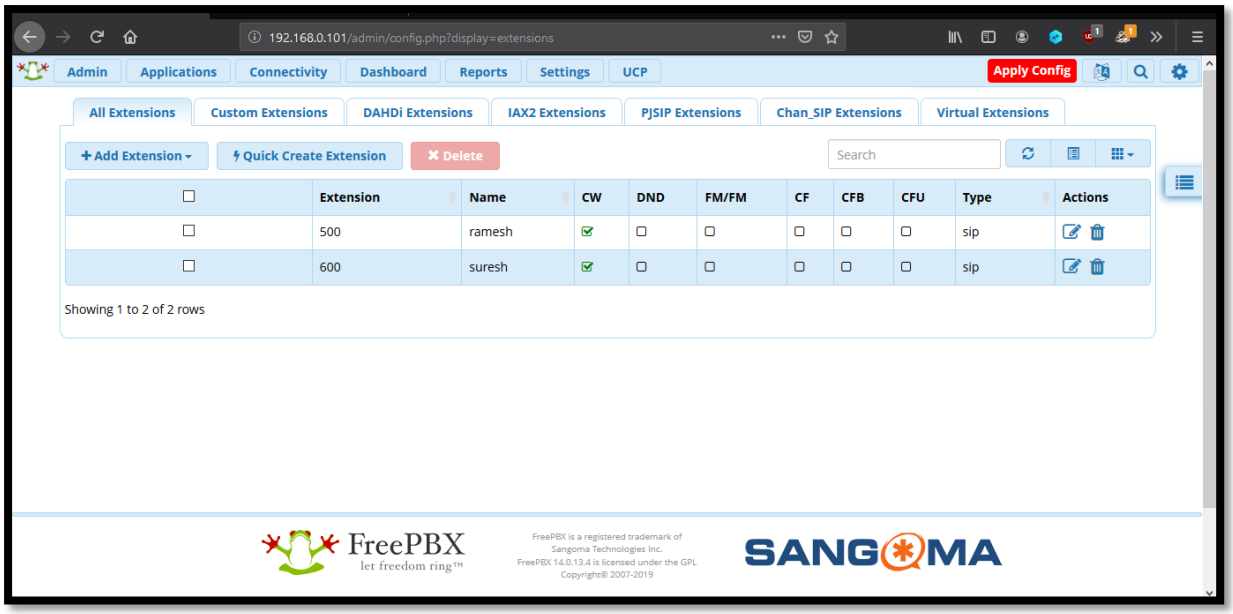

Figure 12 All Extensions

1.2 Configuring Zoiper Softphone

Zoiper is an on premise and cloud-based softphone solution that caters to service providers, call centres, VoIP integrators, mobile operators and businesses that require softphones independent of their service provider. [10]

Zoiper, the free softphone to make VoIP calls through your PBX or favourite SIP provider. Available for iPhone, Android, Windows Phone 8, Windows, Mac.

Zoiper can be downloaded from here .

The setup is demonstrated is on Windows 7 system.

Note: Here, we are considering the system to be on same network as that of VoIP server.

Install the downloaded Zoiper executable. After installation, launch the application. Provide with User Extension and password.

Note: Extension and password is the one added in Asterisk.

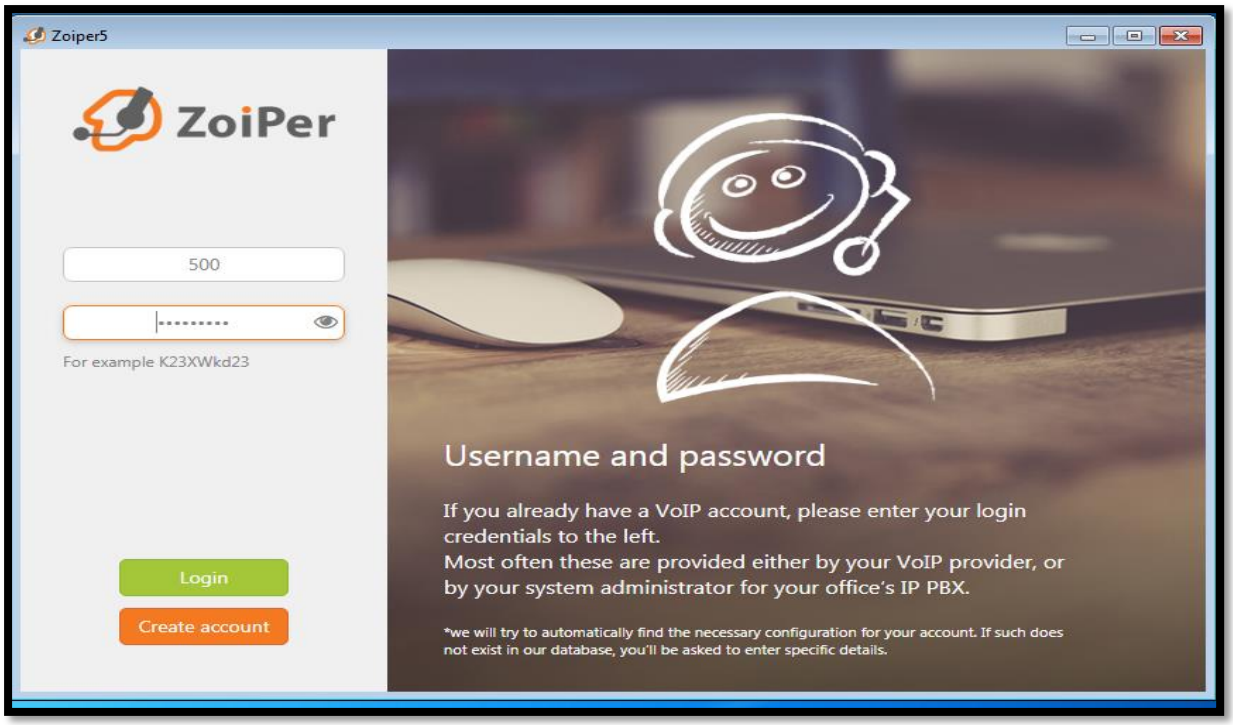

Figure 13 User Login

Provide the address of VoIP server along with port number.

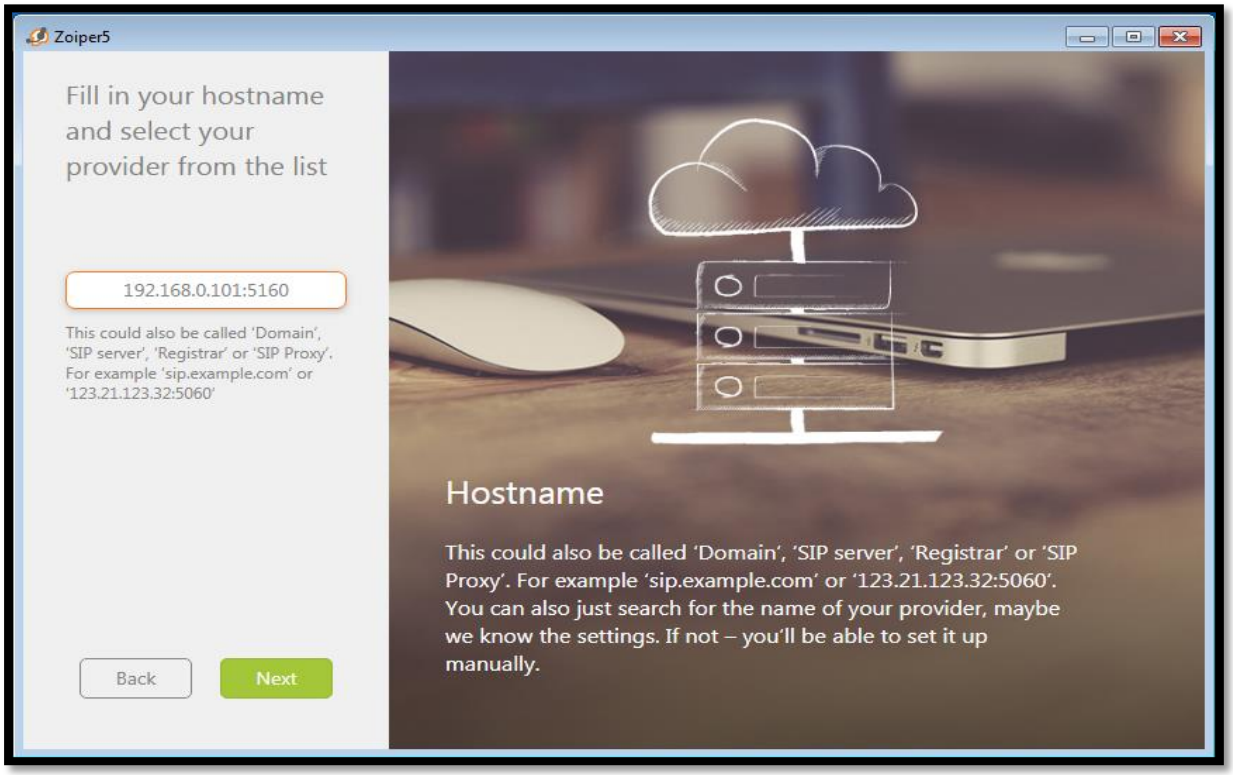

Figure 14 Providing hostname

User can choose to skip Proxy settings.

The softphone software will automatically check for possible configurations.

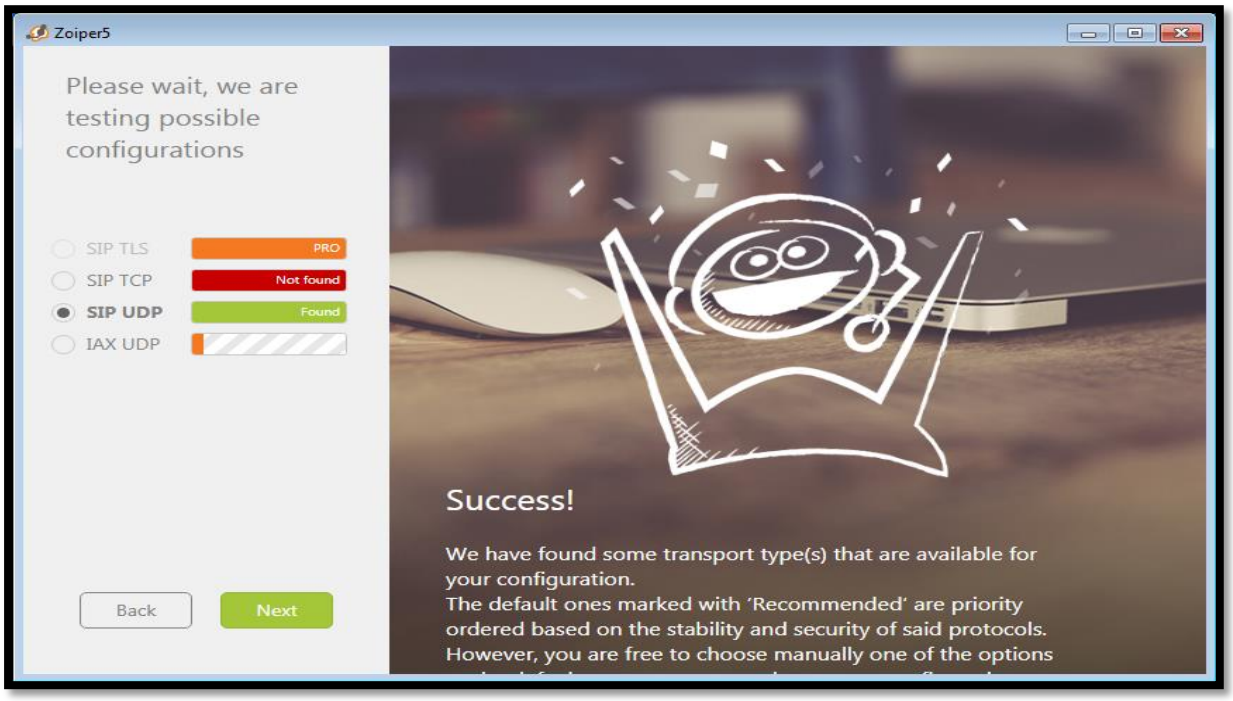

Figure 15 Automatic Network Configuration

Zoiper has been successfully configured.

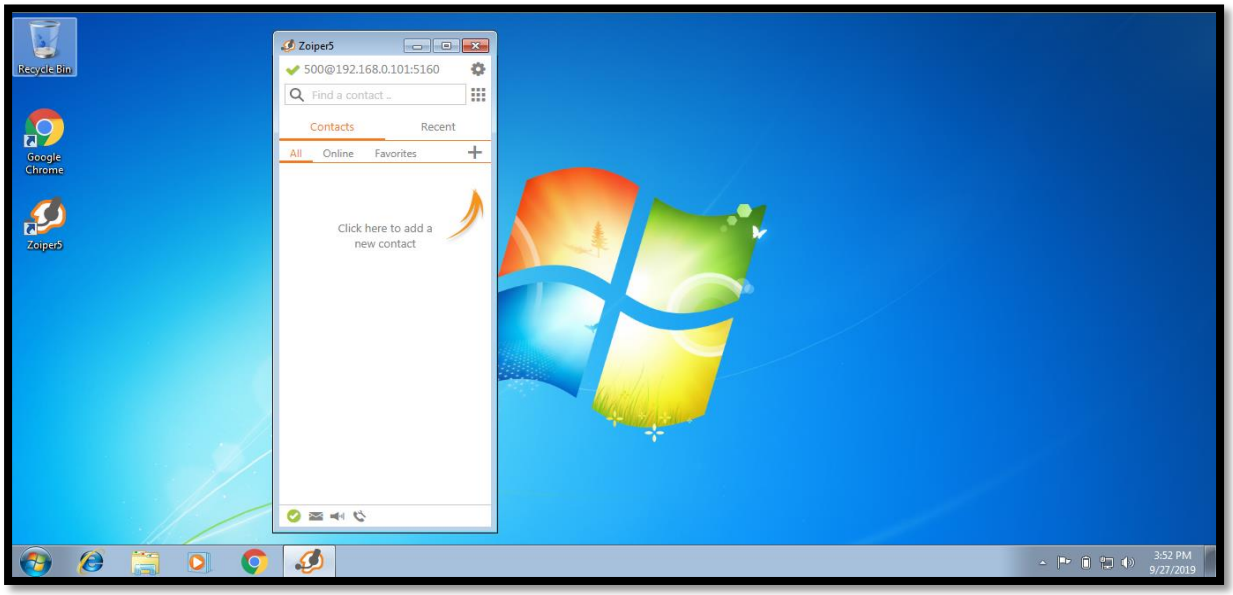

Figure 16 Zoiper Softphone

Following similar steps, configure Zoiper softphone inside android device.

5. Configuring Raspberry pi

For the scope of this project we will be working on Raspberry Pi Model 3.

The Raspberry Pi 3 Model B is the earliest model of the third-generation Raspberry Pi. It replaced the Raspberry Pi 2 Model B in February 2016. See also the Raspberry Pi 3 Model B+, the latest product in the Raspberry Pi 3 range. [11]

- Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
- 1GB RAM
- BCM43438 wireless LAN and Bluetooth Low Energy (BLE) on board
- 100 Base Ethernet
- 40-pin extended GPIO
- 4 USB 2 ports
- 4 Pole stereo output and composite video port
- Full size HDMI
- CSI camera port for connecting a Raspberry Pi camera
- DSI display port for connecting a Raspberry Pi touchscreen display
- Micro SD port for loading your operating system and storing data
- Upgraded switched Micro USB power source up to 2.5A

User must flash Kali Linux for ARM OS. Let's begin with downloading the kali image file from here.

Begin with formatting the SD Card, using SD card formatter.

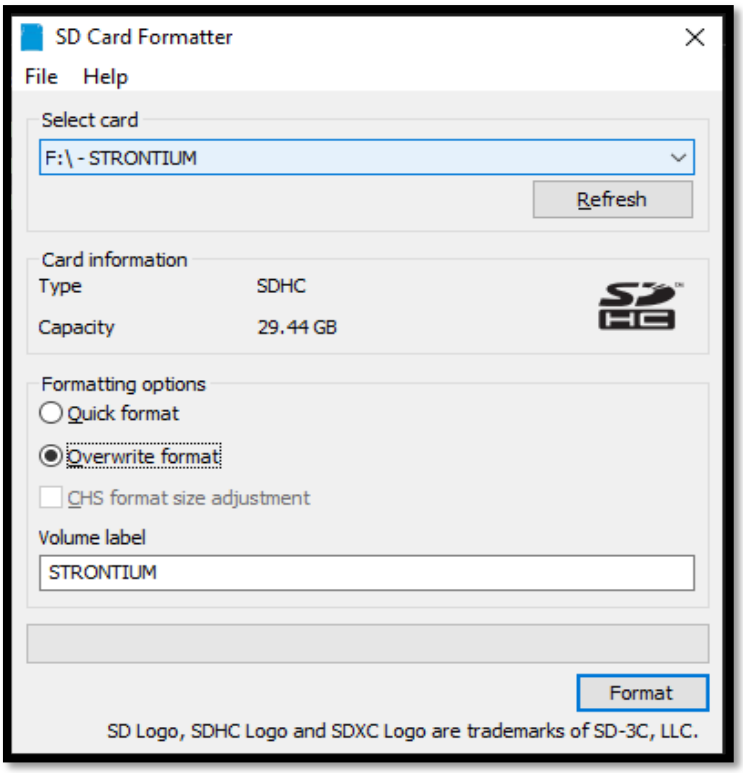

Figure 17 Formatting SD Card

After formatting the SD card, flash the image inside it. For that launch Balena Etcher software and follow the steps from the screen shot. Balena Etcher can be downloaded from https://www.balena.io/etcher/.

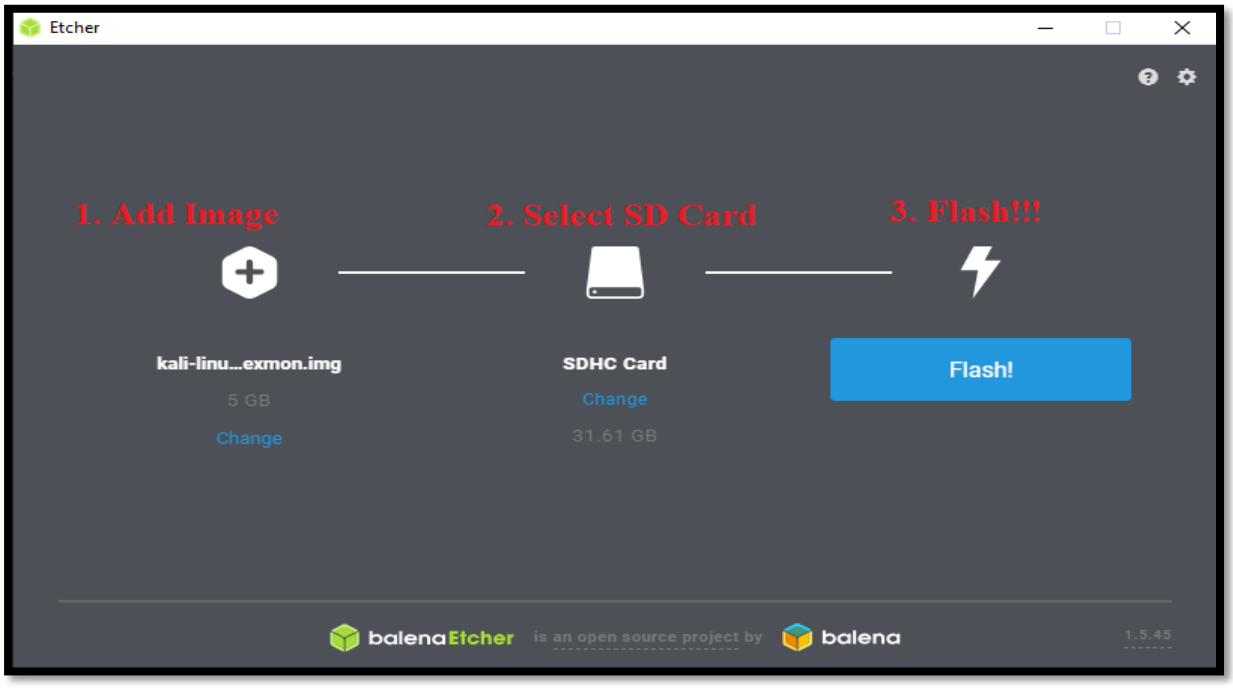

Figure 18 Flashing OS in SD Card

After flashing the SD card, insert SD card inside raspberry pi and power it on.

Now we will be connecting the raspberry pie with the network, so that latter we can SSH into the pie.

For that, inside your desktop go to Network Sharing centre and choose Wi-Fi.

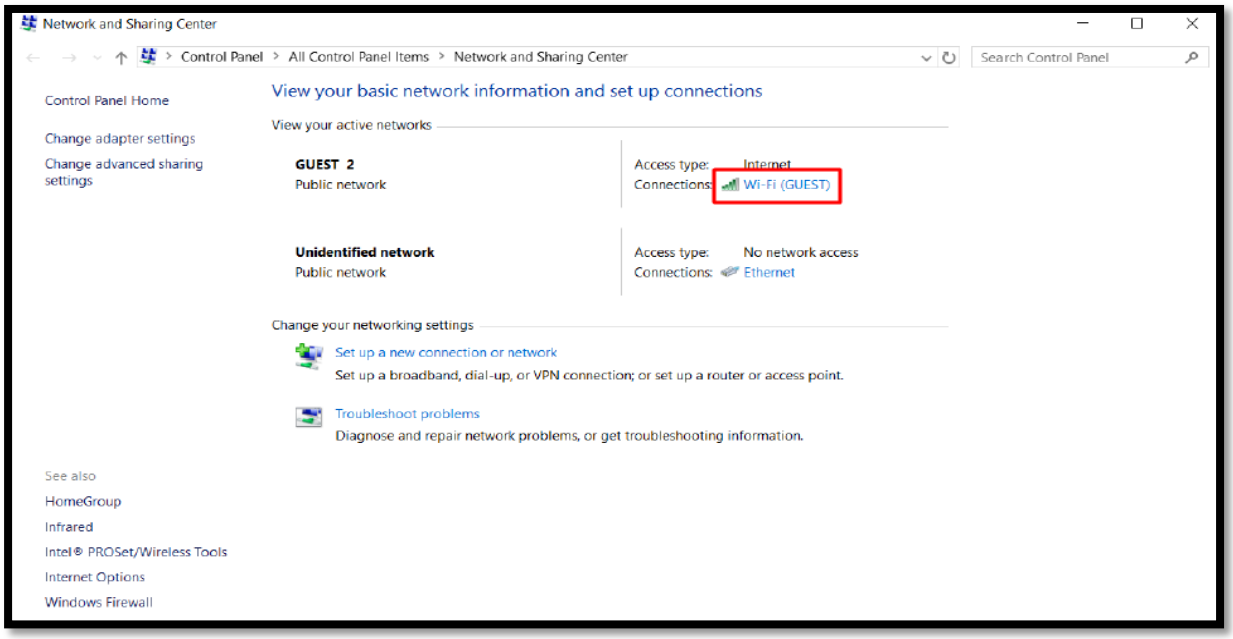

Figure 19 Network Sharing

Now, go to Properties -> Sharing and check the "Allow other network users to connect" checkbox. In "Home networking connection" choose Ethernet. Click "OK" to save the settings.

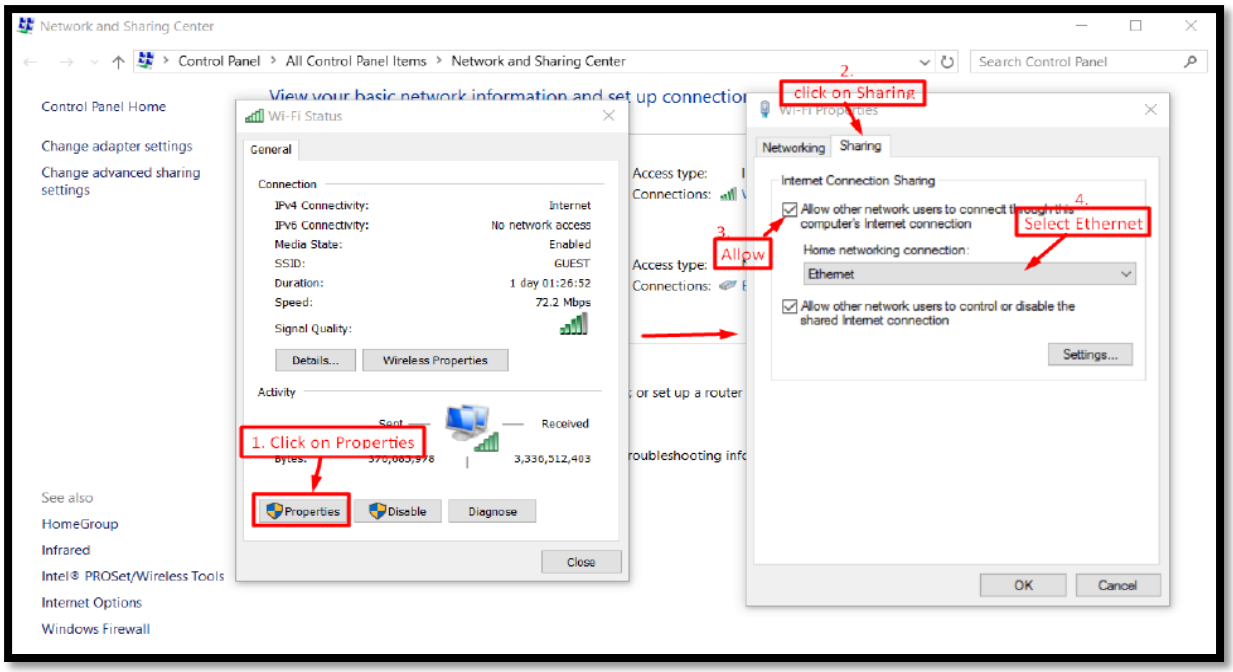

Figure 20 Allow network sharing for Ethernet

Now, move to Ethernet settings.

Now, go to “Details” and notice the IPv4 Address. Here, its 192.168.137.1 which will act as a gateway for our pi.

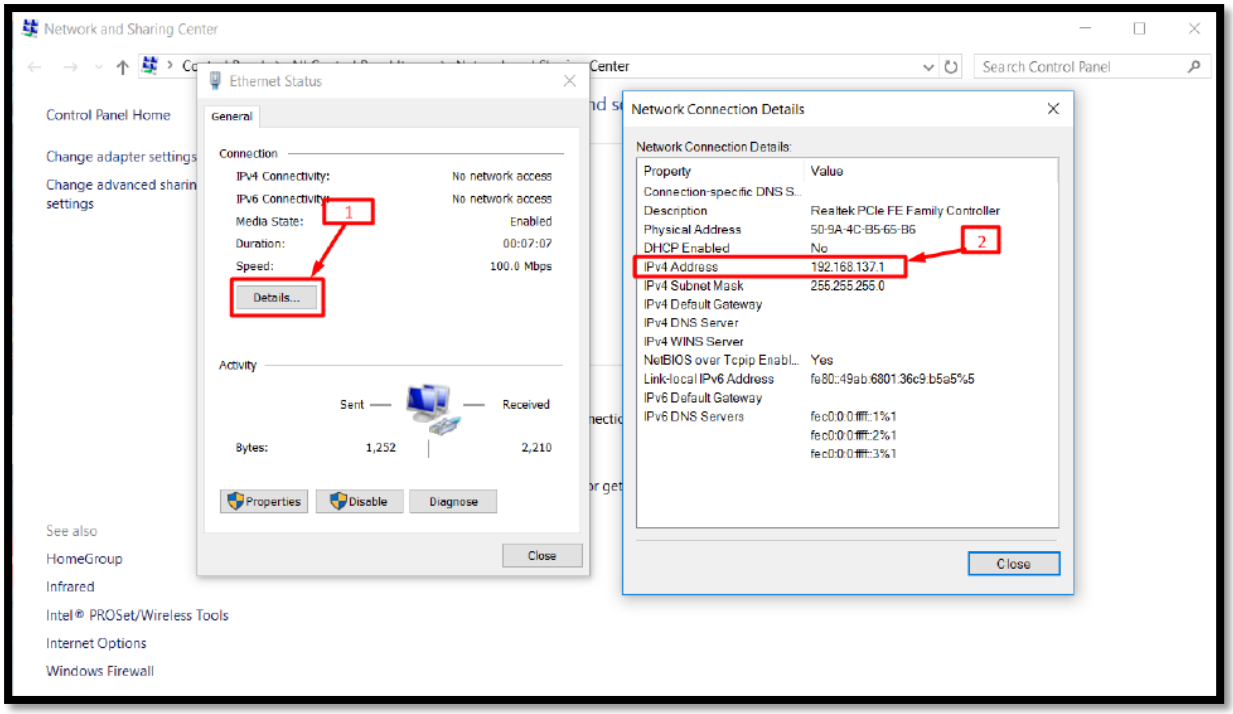

Figure 21 Checking Ethernet properties

Now for finding the IP address of raspberry pi, run advance in scanner on the IP range we found above (Ethernet settings).

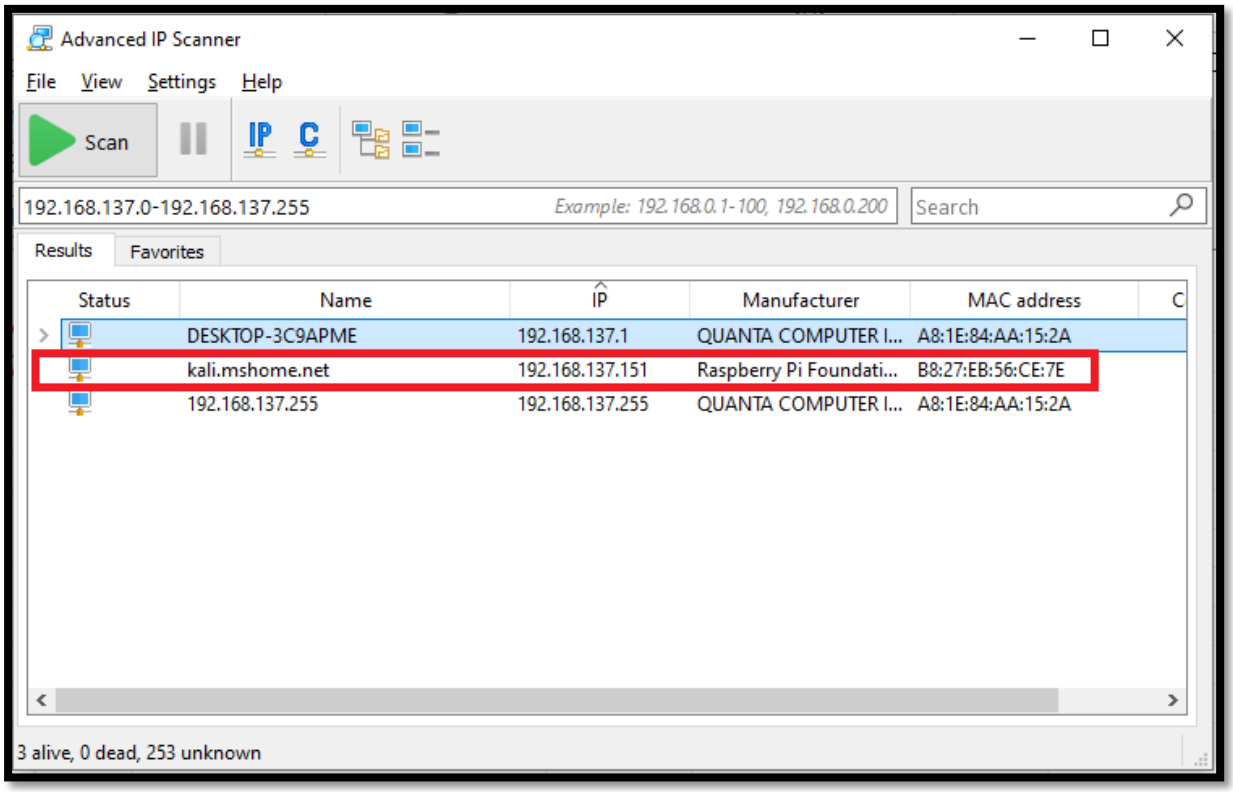

Figure 22 Advance IP Scanner

SSH into the raspberry pi by using SSH client of user's choice.

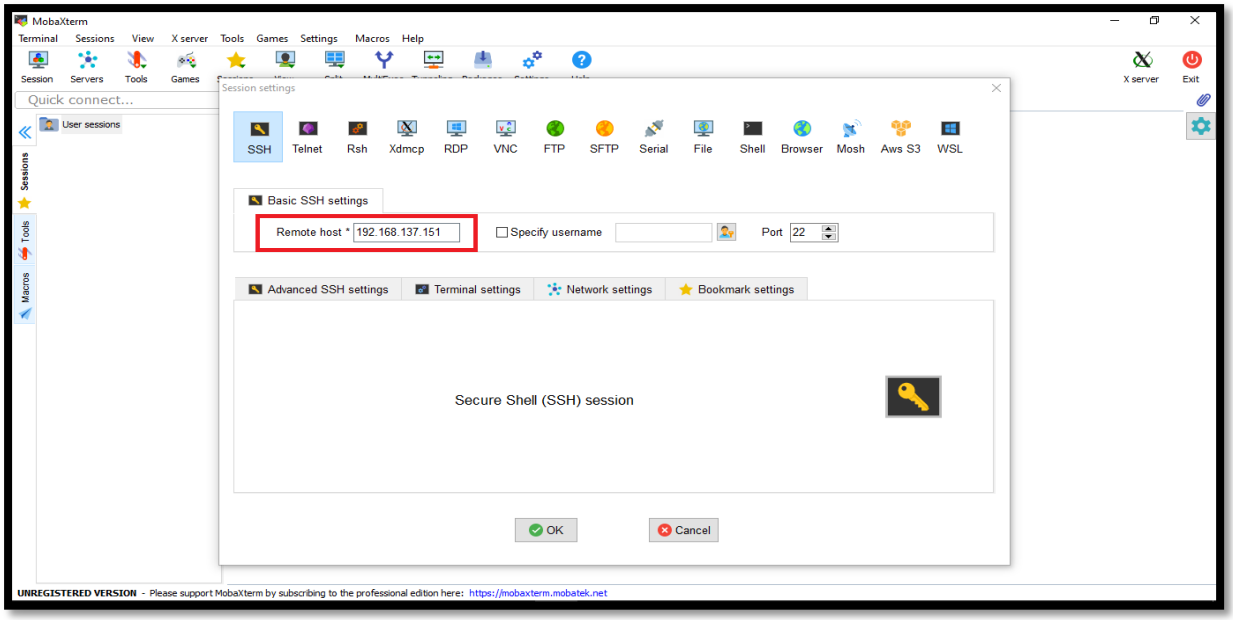

Figure 23 SSH Connection attempt

Proceed by entering login credentials. The default user for raspbian OS is “pi” and password is “raspbian”.

User will get a SSH terminal inside raspberry pi.

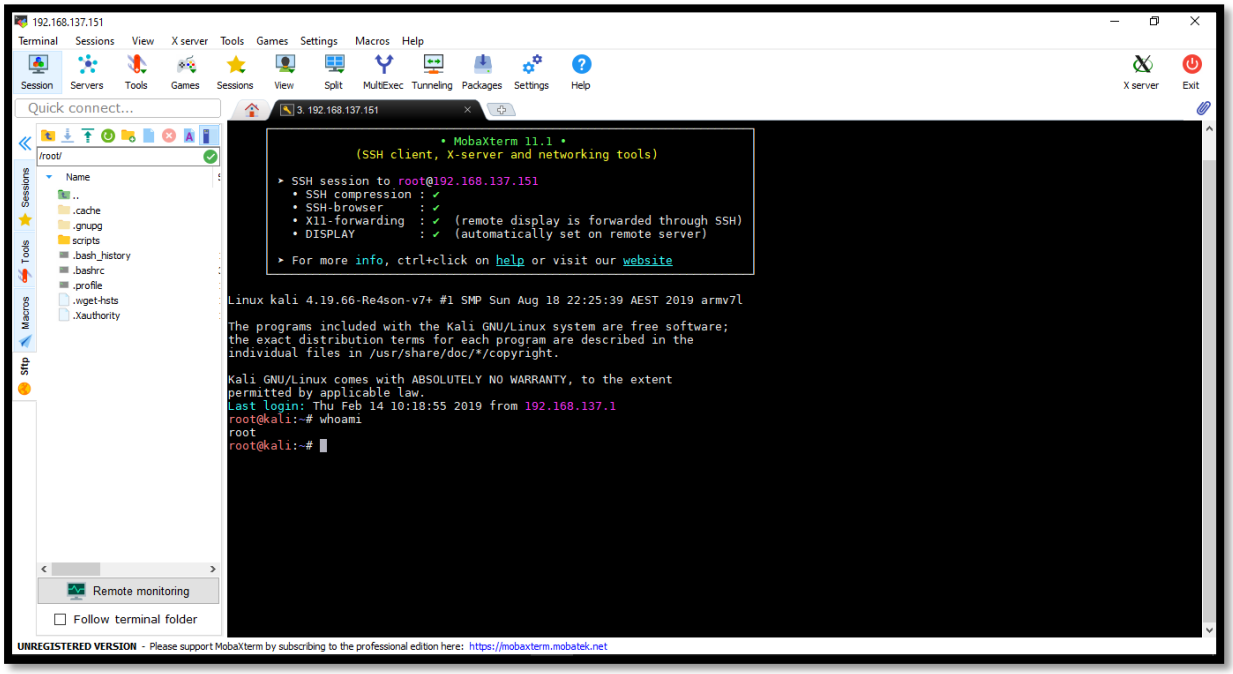

Figure 24 Raspberry pi terminal

Connect an additional USB Wi-Fi adapter to raspberry pi. After that user must configure the network settings. For that run the command:

$ nmtui

User will be prompted with a text menu. Move to “Edit Connection” -> “Add Connection” -> “Wi-Fi”. Provide details like SSID, Security Type, Password. Here static IP is configured.

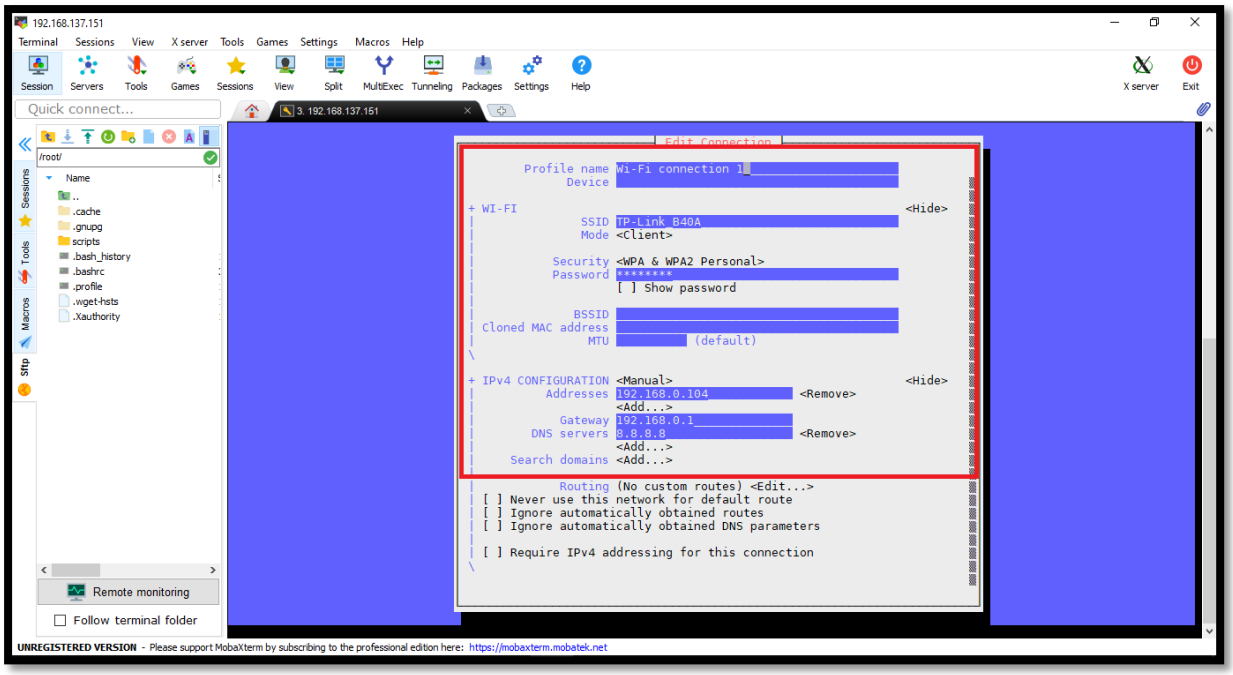

Figure 25 Configuring network settings

In similar manner, add another Wi-Fi connection.

Note: As static IP is set, the two Wi-Fi connections, even though have same SSID, must have different static IPs set.

Configure Wi-Fi adapter and USB Wi-Fi adapter with these connections respectively.

For checking network details, run the command:

$ ifconfig

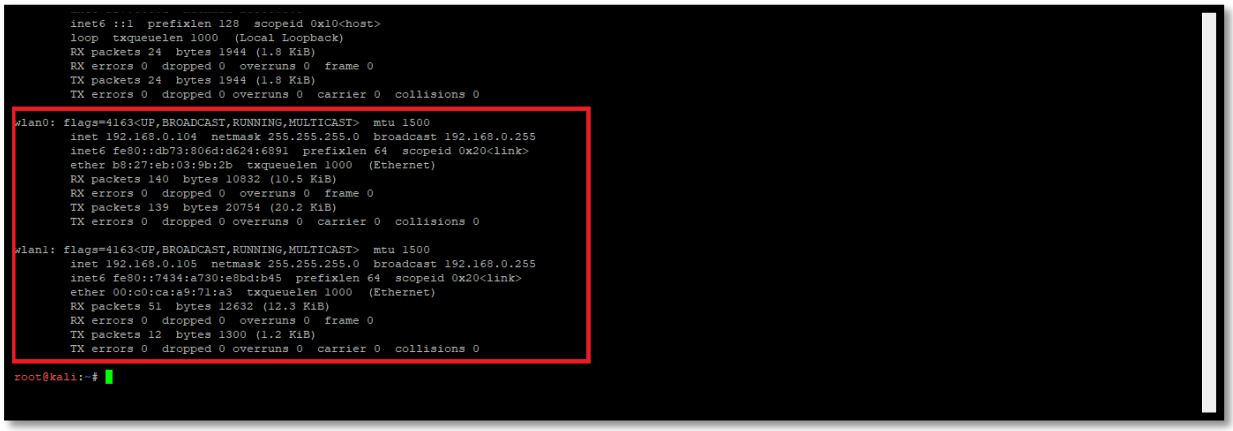

Figure 26 Network Details of Raspberry

5.1 Remote Log into Raspberry Pi's Full Operating System Using VNC Connect

VNC has been the best way to access any computer remotely on the same network. Recently, VNC Connect also came out to make it easy to access your Raspberry Pi from anywhere using a cloud connection. Once it's set up, you can access your Raspberry Pi's graphic interface from any other computer or smartphone using the VNC Viewer app.

VNC Connect comes packed in for free with the most recent versions of the Raspberry Pi operating system. [12]

VNC can be set up in few simple steps. Open up a terminal and run the following commands:

$ sudo apt-get update

$ sudo apt-get install realvnc-vnc-server realvnc-vnc-viewer

Once that's complete, type in

$ sudo raspi-config

and press Enter. Scroll down to VNC and set it to Enabled.

Once that's finished downloading, you can set up VNC Connect:

- Head to the RealVNC Raspberry Pi sign up page and enter your email address in the sign up box.
- Follow the on-screen instructions to finish setting up your account with a password.
- Back on your Raspberry Pi, click the VNC icon in the top-right corner of the screen to open VNC. Then click the status menu and select Licensing.
- Enter the email address and password you created in step one.
- When prompted, select "Direct and cloud connectivity." Your Raspberry Pi is now accessible online.
- Download the VNC Viewer application on the computer you want to control the Raspberry Pi from, like the laptop or smartphone you'll have when you travel.

Open the VNC Viewer application and enter the credentials you created in step one.

Your Raspberry Pi will pop up as an option automatically. Select it to open up the connection. When prompted, enter your Raspberry Pi's username and password (by default this is the username "pi" and "toor" raspberry). Within a few second it'll connect.

You're now able to log into your Raspberry Pi's graphic desktop from anywhere as long as your Raspberry Pi has internet access.

5.2 Installing Required Packages

The following packages need to be installed as the would be needed by our custom script.

Let's begin by install tcpdump.

Tcpdump is a common packet analyser that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software. [13]

$ sudo apt-get install tcpdump -y

Now user needs to install Ettercap. We will be using Ettercap text only version for ARP Spoofing.

Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. It can be used for computer network protocol analysis and security auditing. It runs on various Unix-like operating systems including Linux, Mac OS X, BSD and Solaris, and on Microsoft Windows. [14]

$ sudo apt-get install Ettercap-text-only -y

Next up, user needs to install python PyDrive library which will be useful for pushing files to the google drive.

PyDrive is a wrapper library of google-api-python-client that simplifies many common Google Drive API tasks. [15]

$ pip install PyDrive

6. Sniffing VoIP calls using custom script over a Raspberry pi

Inside our lab configuration, we are considering that there are two softphones i.e. an android phone and another setup on a windows system. The two softphone users are communication with each other through VoIP call. The scope of this project is to intercept and analyse this call for investigative purpose.

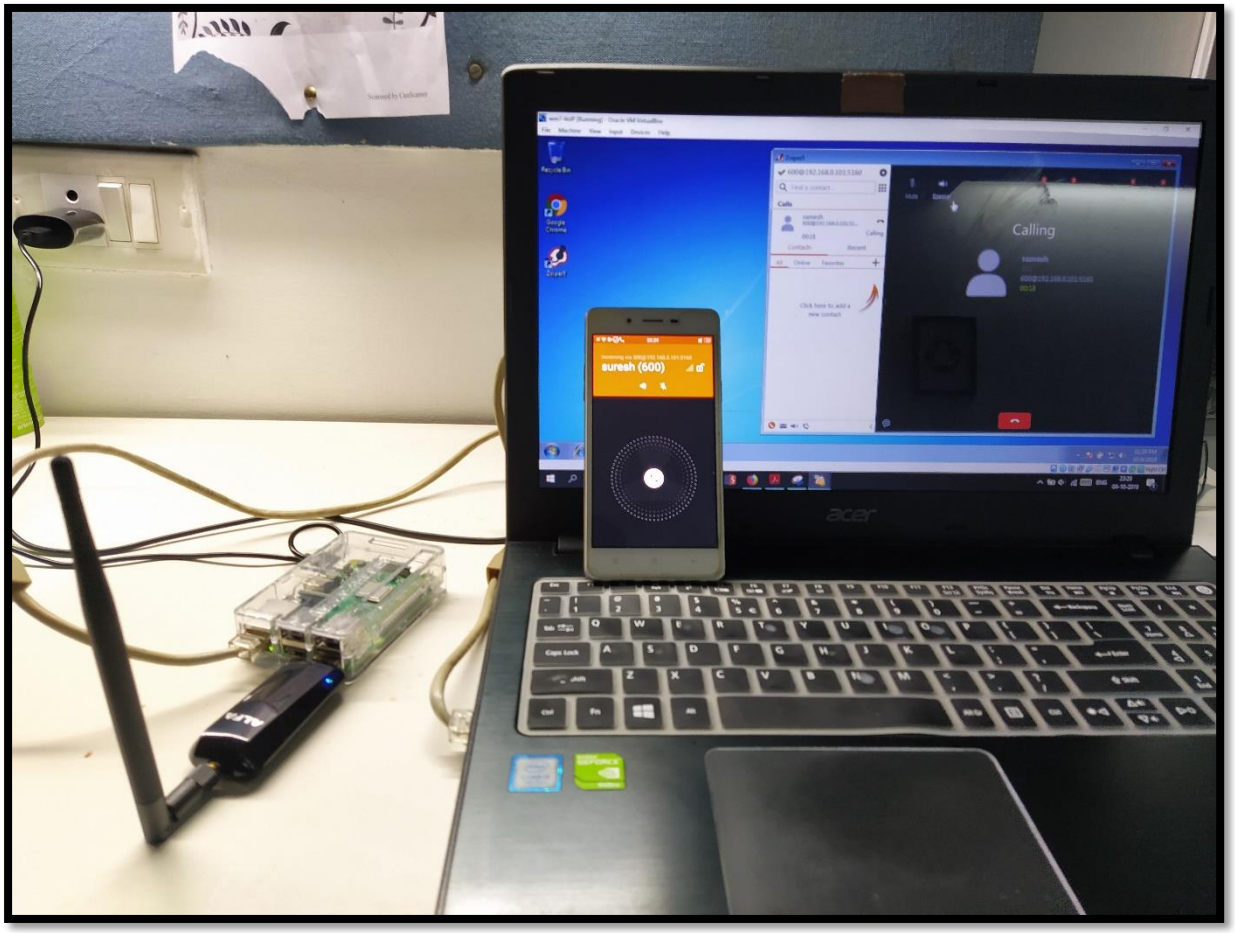

Figure 27 Picturing the scenario

We have setup a raspberry pi inside the same network of that of the two softphones. The investigator connects to this raspberry pi using VNC Connect cloud service through a remote location.

The first step is to find the IP address of softphone, for that the investigator needs to run a nmap scan.

Once the IP address is known, the investigator needs to proceed by calling the custom python script which we have named as “sip_exploitation.py”.

The scripts can be found at https://github.com/s3curityg33k/VoIP-Sniffer .

Sip_exploitation.py will ask for victim IP address. Enter the softphone IP address found through nmap scan.

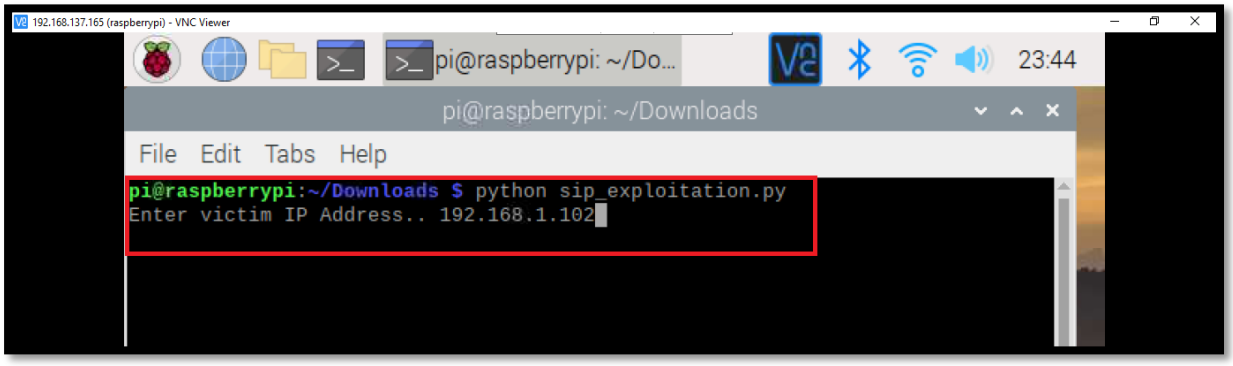

Figure 28 Running exploit script

The script will then try to perform an ARP spoof on the victim using Ettercap API.

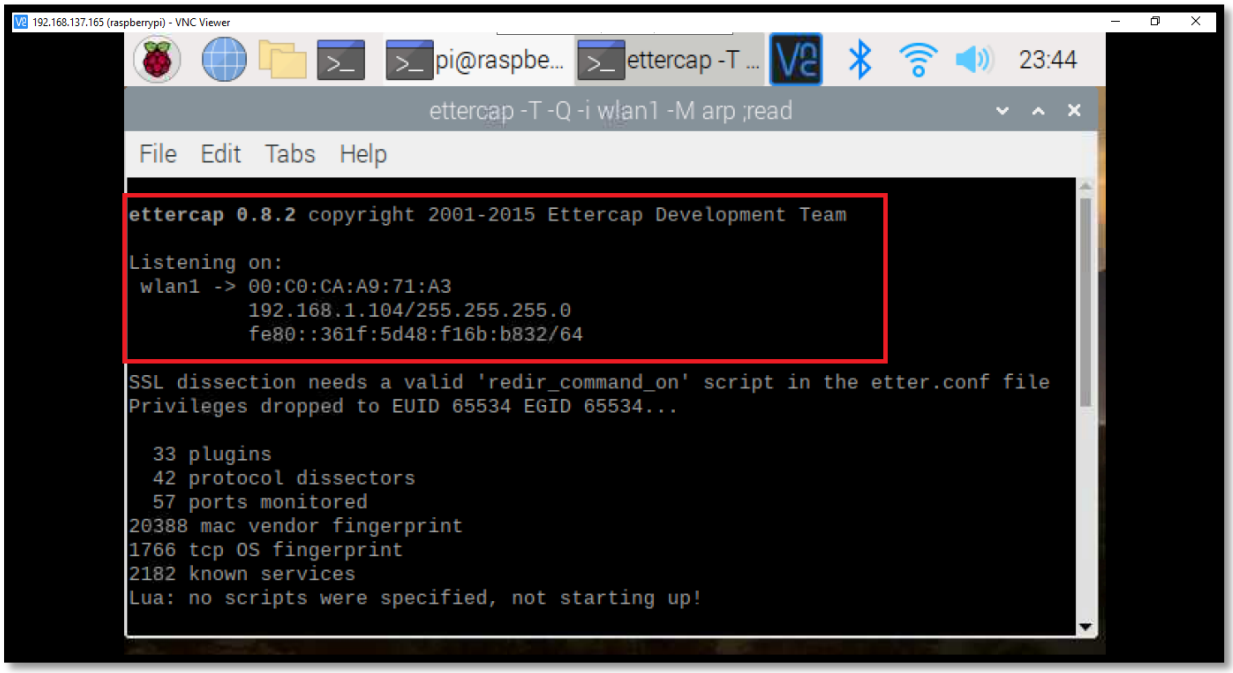

Figure 29 ARP poisoning

Consecutively, the script will also try to capture UDP packets belonging to the victim. Once the packet capture is completed the script will try to upload the pcap file on to google drive.

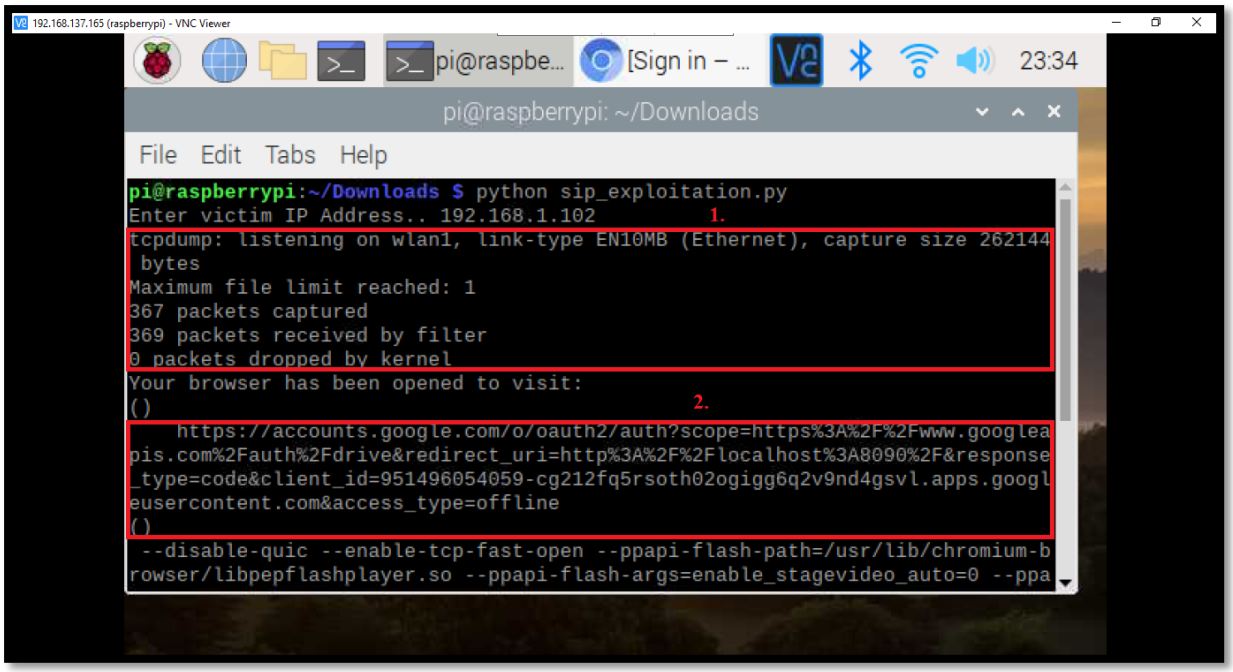

Figure 30 TCP dump

A web browser will be prompted asking to choose an account to which the script would be updated.

Note: Network congestion issues were seen when the script tried to upload the pcap on the drive. To avoid this, it is advisable to force shut the thread performing ARP spoofing once the packet capture is completed. For this press “Ctrl+C” on the terminal instance performing ARP spoofing.

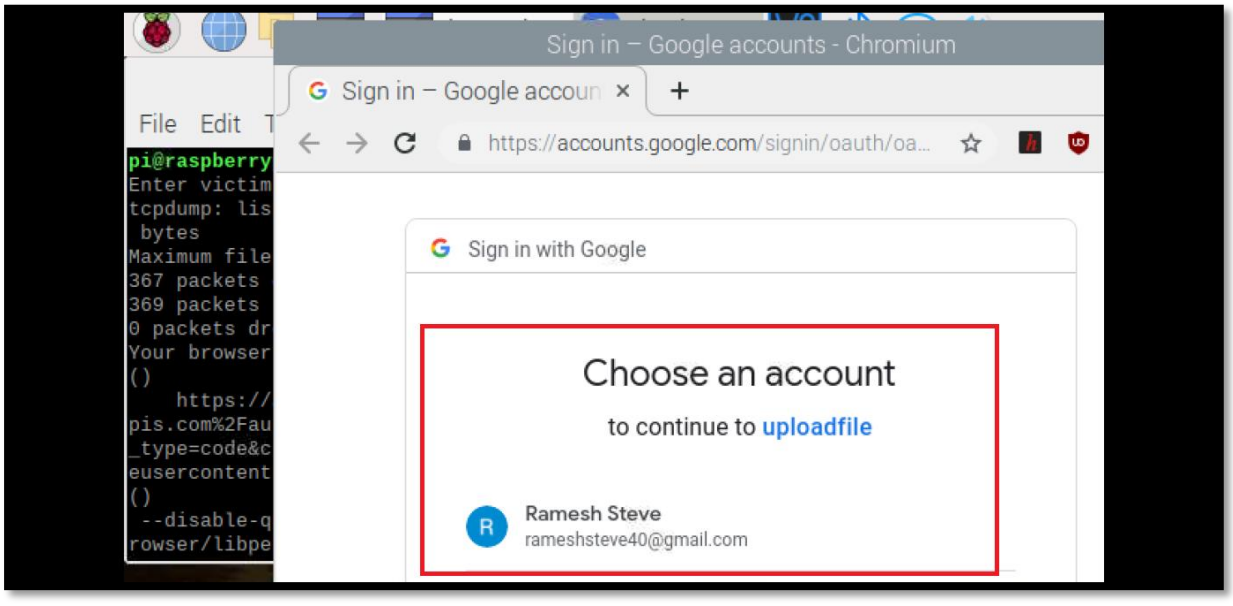

Figure 31 Drive account

After this, the packet capture file would be uploaded on the drive.

Now the investigator can try to listen to the VoIP conversation taken place between the two softphone users on his remote system.

For this, the investigator first needs to download the packet capture file from the drive.

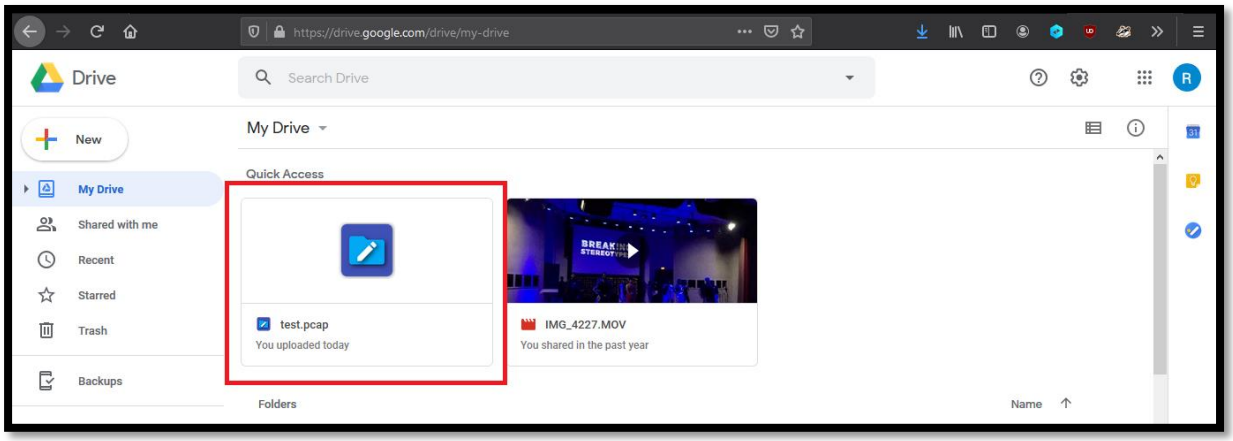

Figure 32 Uploaded packet capture

Open “test.pcap” inside wireshark.

For viewing all VoIP packets, apply the following filter “sip || rtp”.

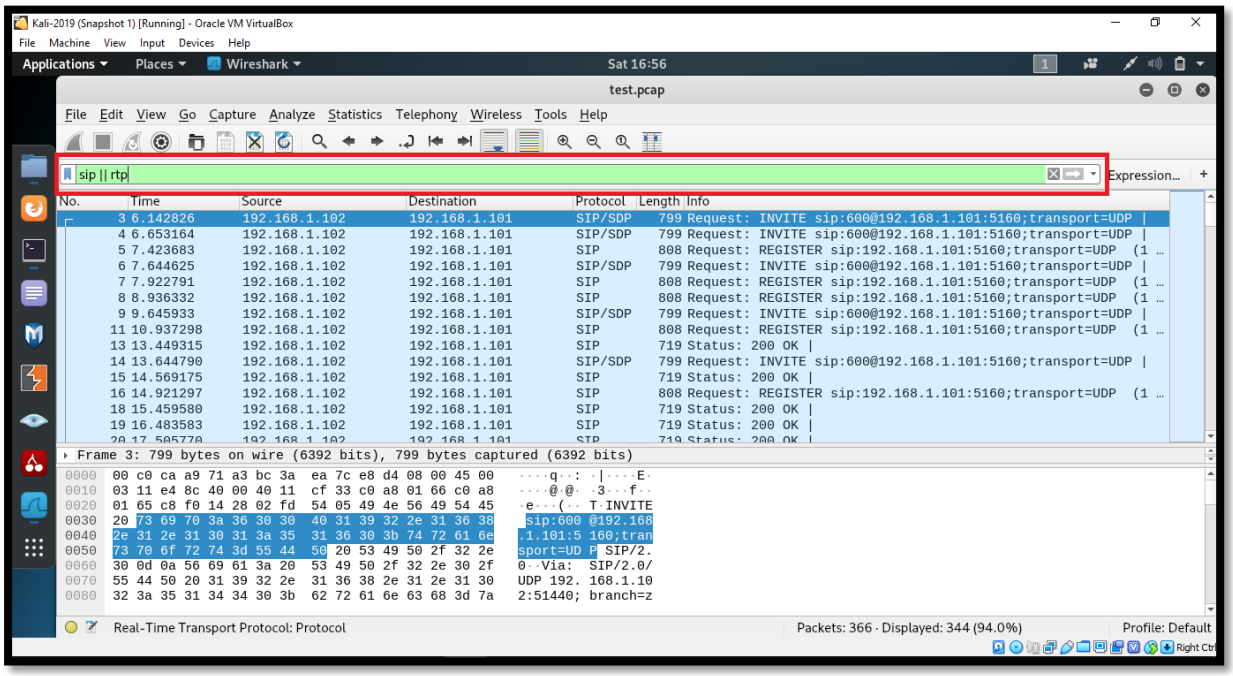

Figure 33 VoIP packets

For viewing the call packets, go to Telephony -> VoIP Calls

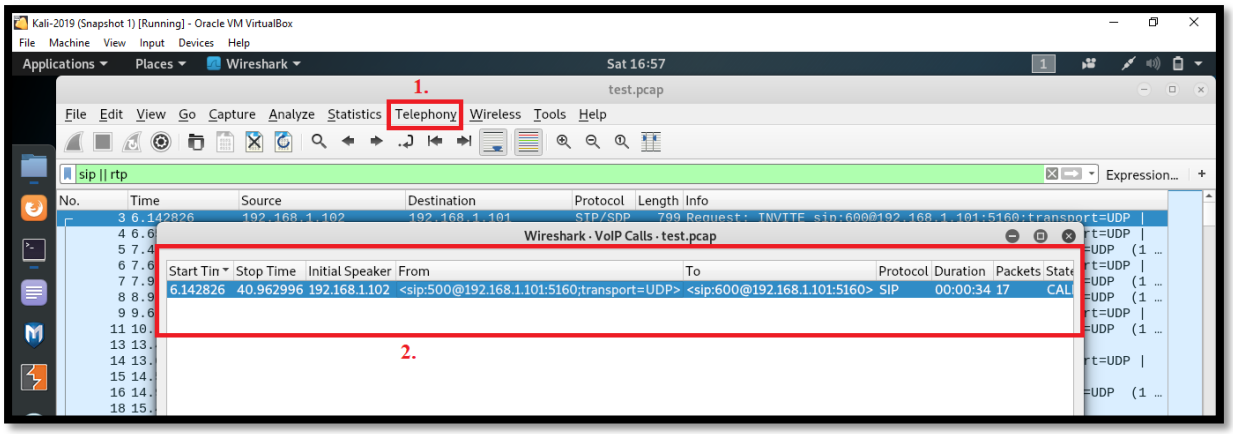

Figure 34 VoIP Conversation

Select the VoIP call and click on “Play Stream”.

Here, the investigator will be able to hear the conversation that took place between the two suspects.

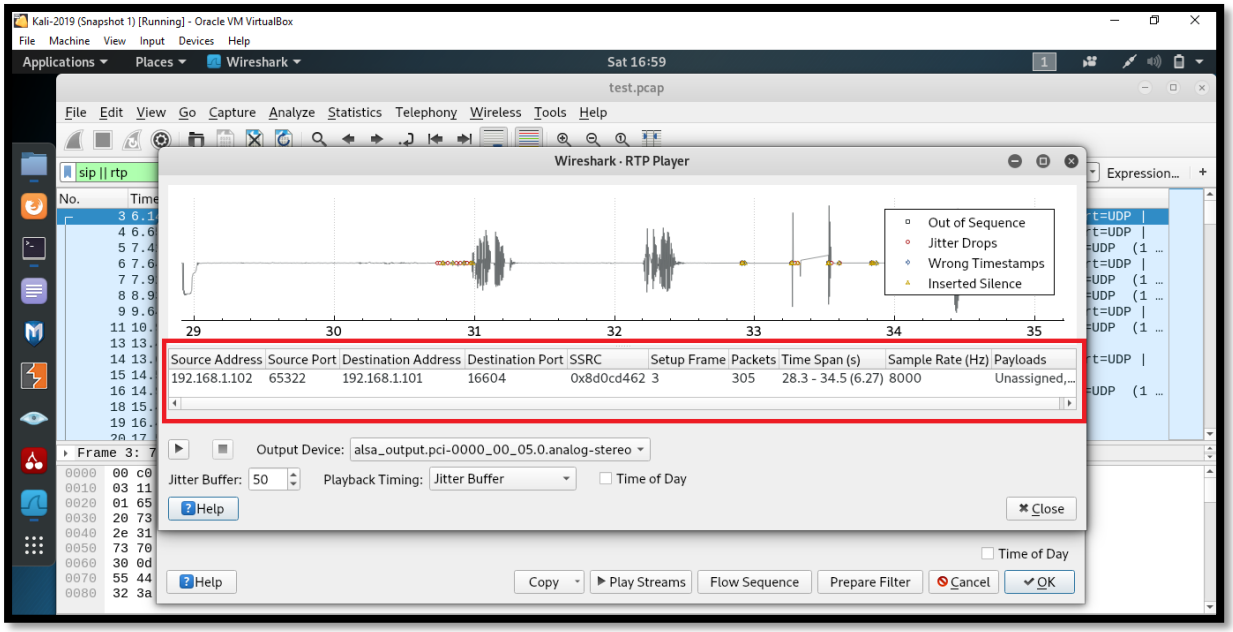

Figure 35 Playing VoIP call in RTP player

7. Conclusion

Outcome of this project work will assist forensic investigators in covertly sniffing and intercepting VoIP calls. This project will act as a basic guideline for the investigators and they can take help of findings of this project to speed up their investigation.

8. References

[1] Michael Dosch and Steve Church. "VoIP in the Broadcast Studio". Axia Audio. Archived from the original on October 7, 2011. Retrieved June 21, 2011.

[2] https://indianexpress.com/article/cities/mumbai/criminals-making-voip-calls-cops-seek-dot-help/

[3] Rakesh Arora. "Voice over IP: Protocols and Standards" dated November 23, 1999. http://www.cis.ohio-state.edu/~jain/cis788-99/voip_protocols/index.html

[4] Sohil Garg. "Enumerating and Breaking VoIP". https://www.exploit-db.com/docs/english/18136-paper-enumerating-and-breaking-voip.pdf

[5] Santi Phithakkitnukoon, Enkh-Amgalan Baatarjav, Ram Dantu. "VoIP Security – Attacks and Solutions" dated March 06, 2015. https://www.researchgate.net/publication/220449868

[6] Dharmin Suthar. "VoIP Penetration Testing and Forensics" dated April, 2018.

[7] Hardik Tandel, Dr. Parag Rughani. "Forensic Analysis of Asterisk-FreePBX based VoIP Server" dated June, 2018. https://www.researchgate.net/publication/326046523

[8] Yusuf Turk, Onur Demir, Sezer G¨oren. "Real Time Wireless Packet Monitoring with Raspberry Pi Sniffer". https://san.ee.ic.ac.uk/iscis2014/proceedings/27_turk.pdf

[9] https://www.asterisk.org/get-started

[10] https://www.softwareadvice.com/voip/zoiper-profile/

[11] https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

[12] https://lifehacker.com/how-to-control-a-raspberry-pi-remotely-from-anywhere-in-1792892937

[13] https://www.tcpdump.org/manpages/tcpdump.1.html

[14] https://en.wikipedia.org/wiki/Ettercap_(software)

[15] https://pythonhosted.org/PyDrive/