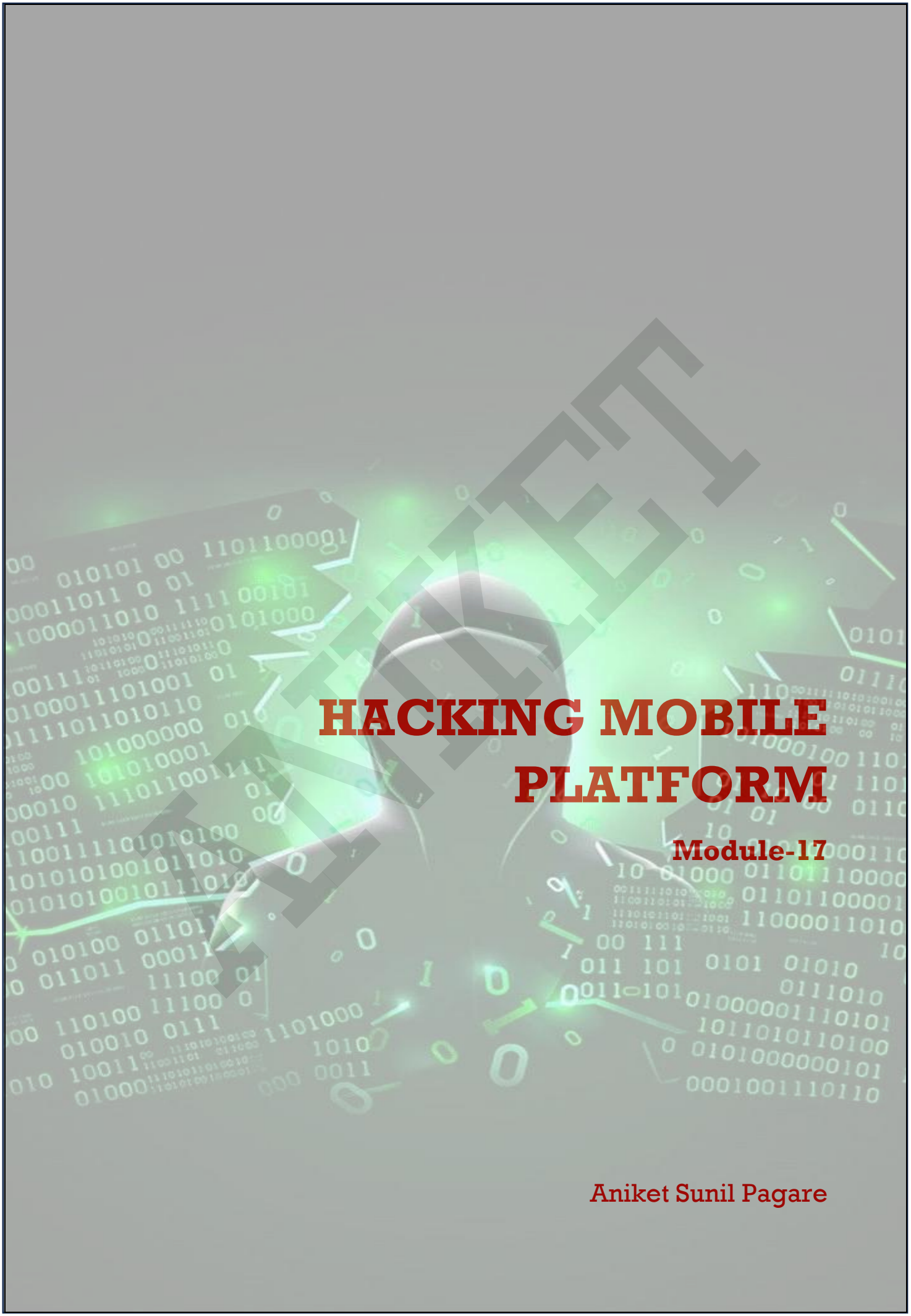


HACKING MOBILE PLATFORM

Module-17

Aniket Sunil Pagare

Table of Contents: Hacking Mobile Platform Module

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

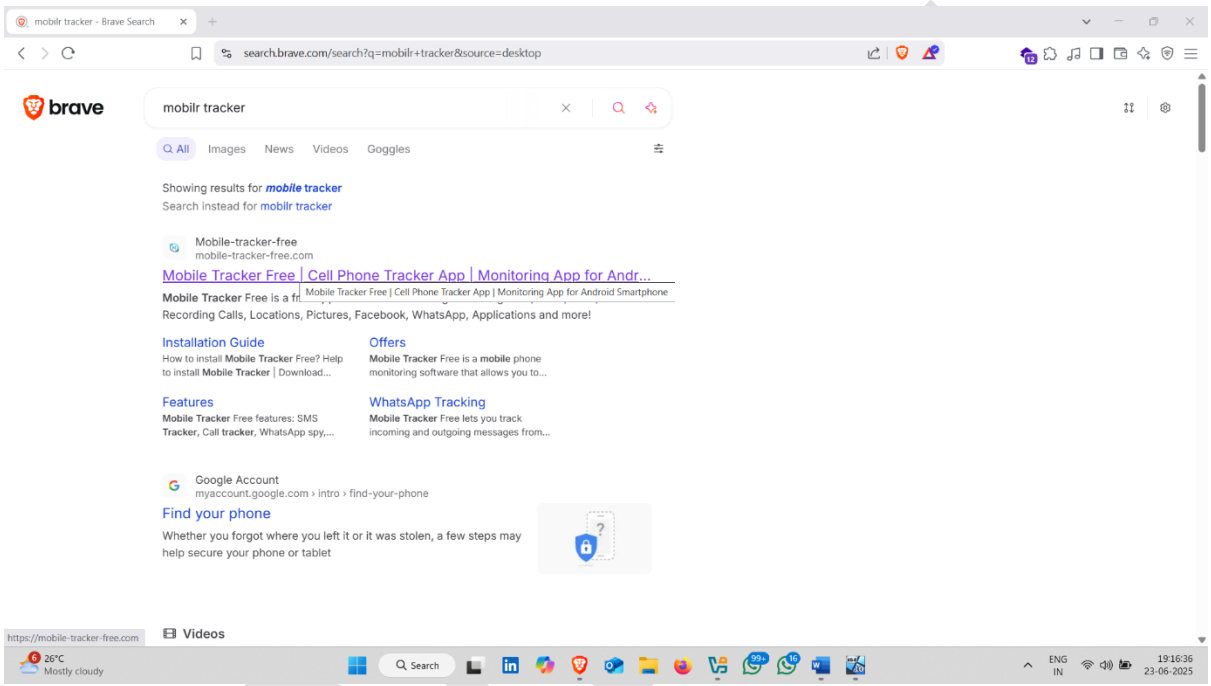
At present, smartphones are widely used for both business and personal purposes. Thus, they are a treasure trove for attackers looking to steal corporate or personal data. Security threats to mobile devices have increased with the growth of Internet connectivity, use of business and other applications, 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.

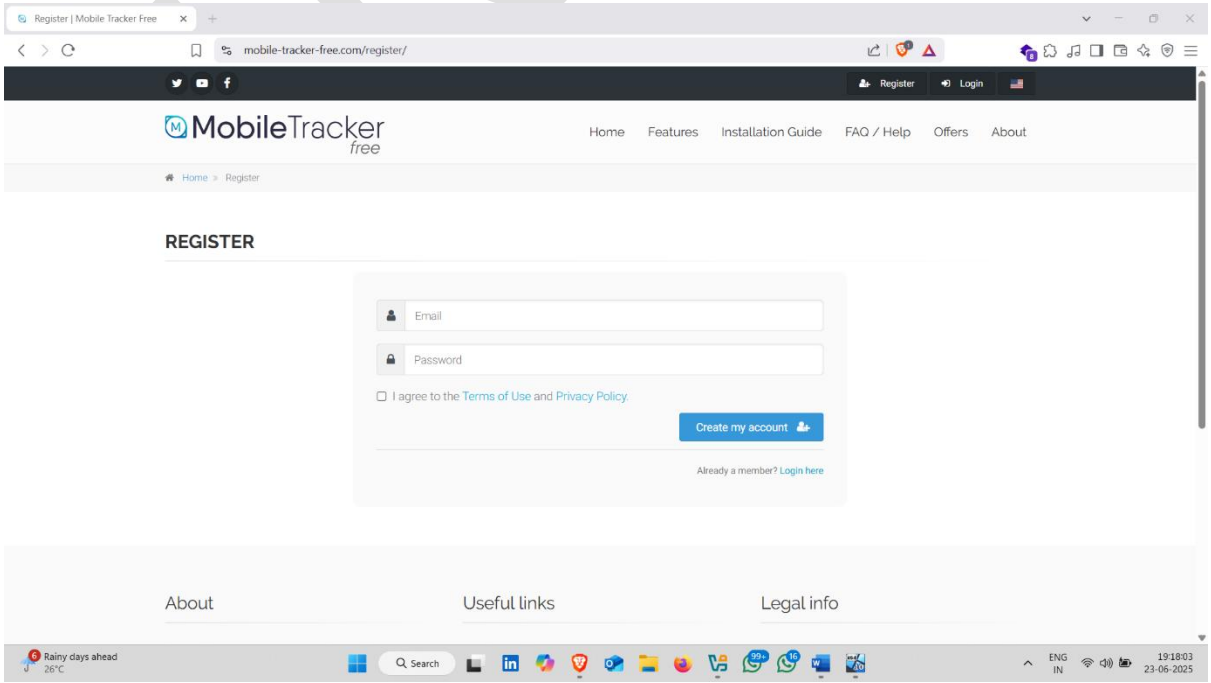
Android Hacking Using Mobile Tracker Website

How to use it -:

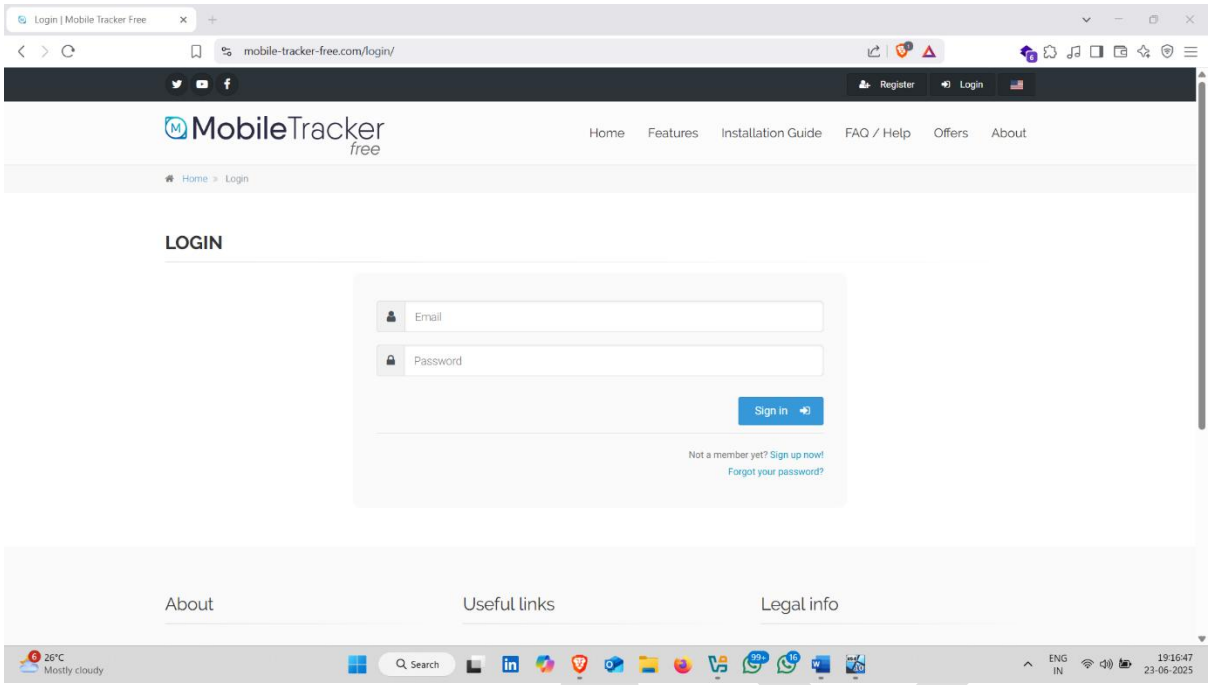
- Open Browser and search Mobile Tracker
- Click on First Official Website



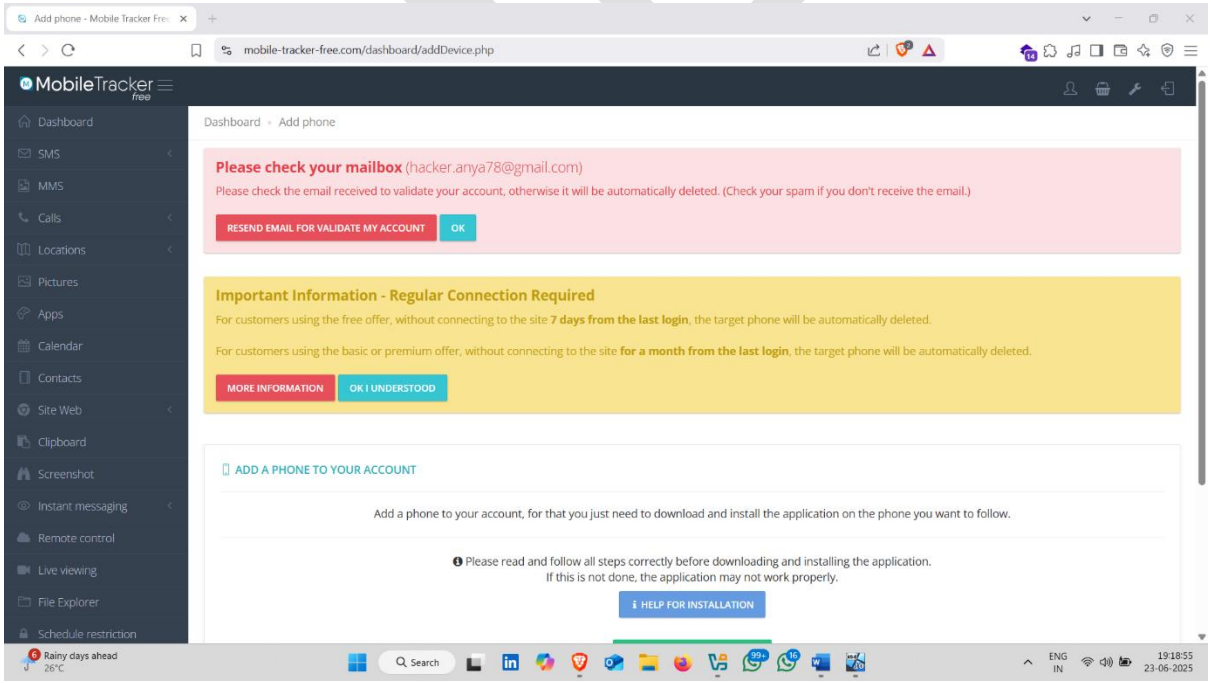
- **Now Register account**



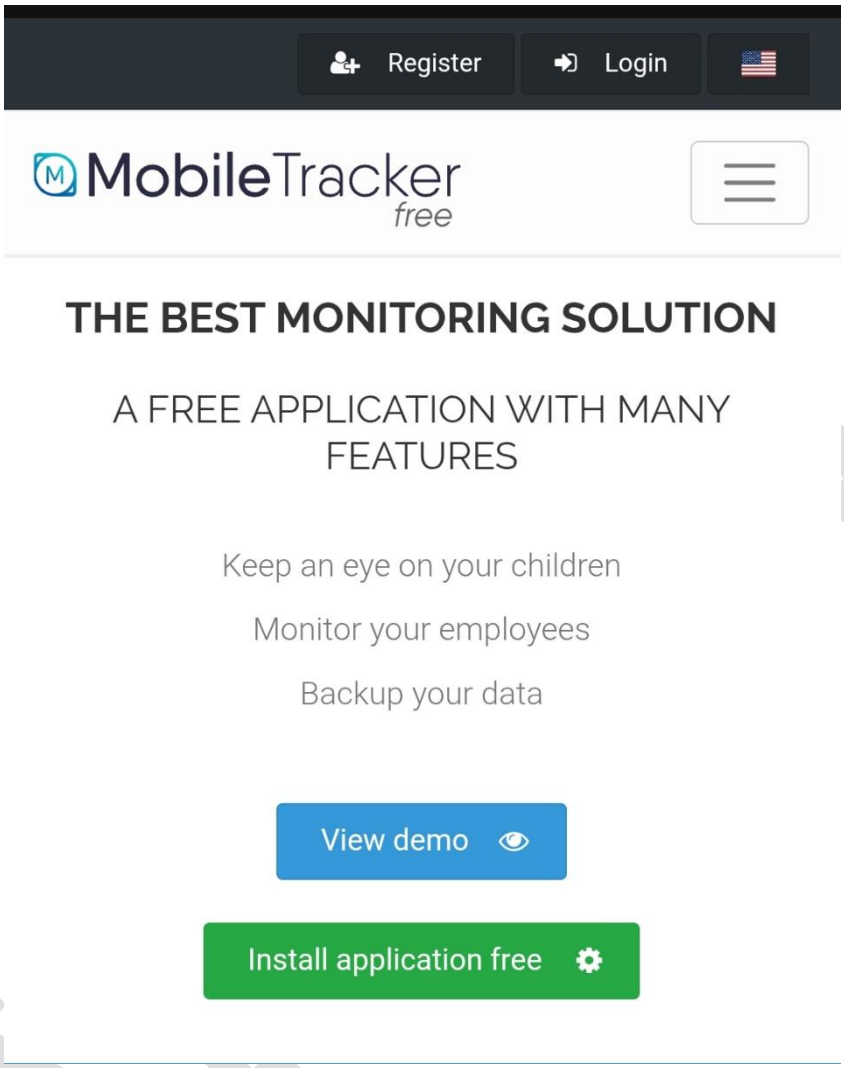
- After Register , **Login Your Account**



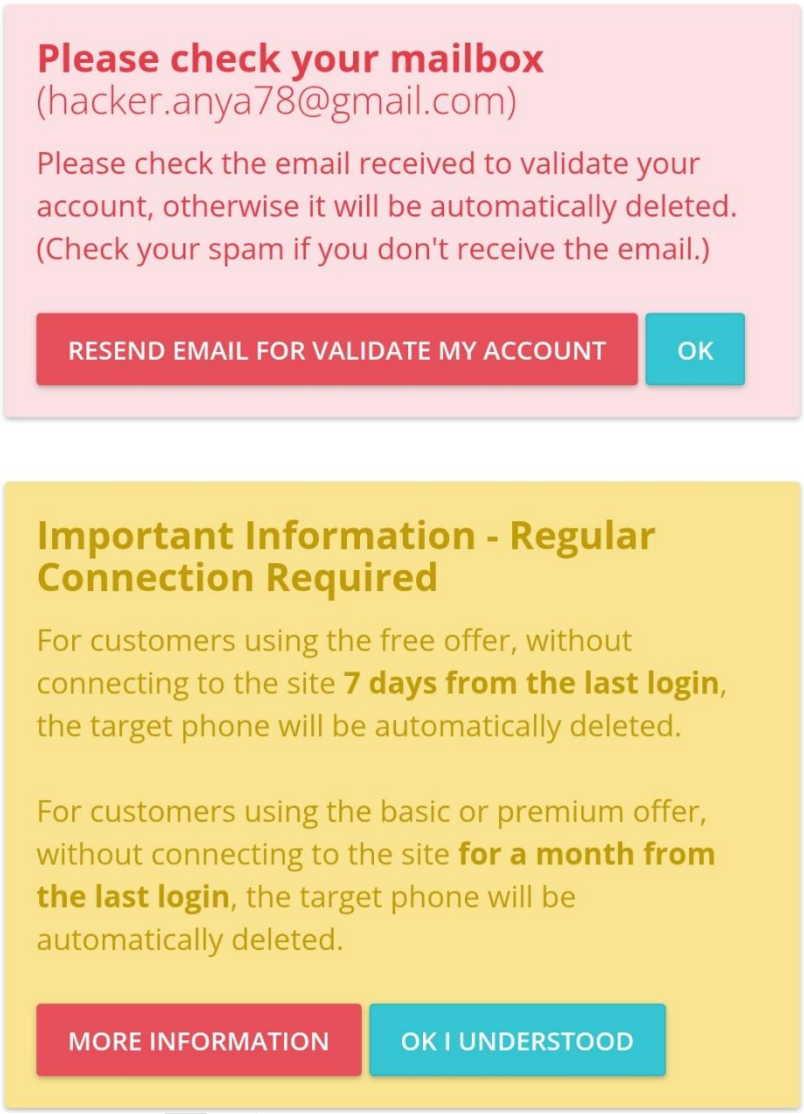
- **Login Successful** ✅ 👇



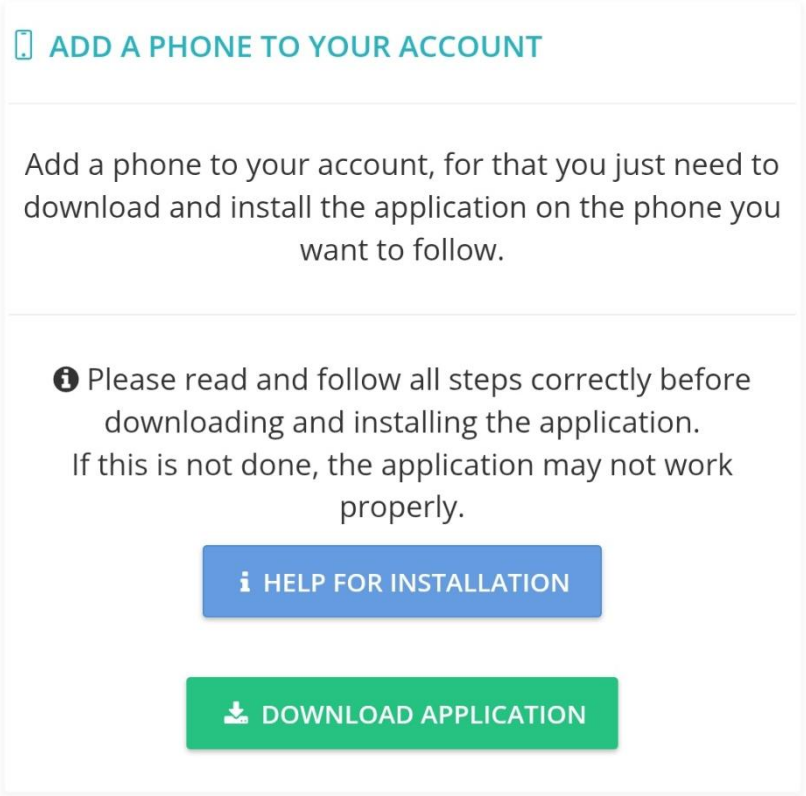
- **Now , open Mobile Tracker website on Victims phone**
- **And login using your mobile-tracker Website username and password**



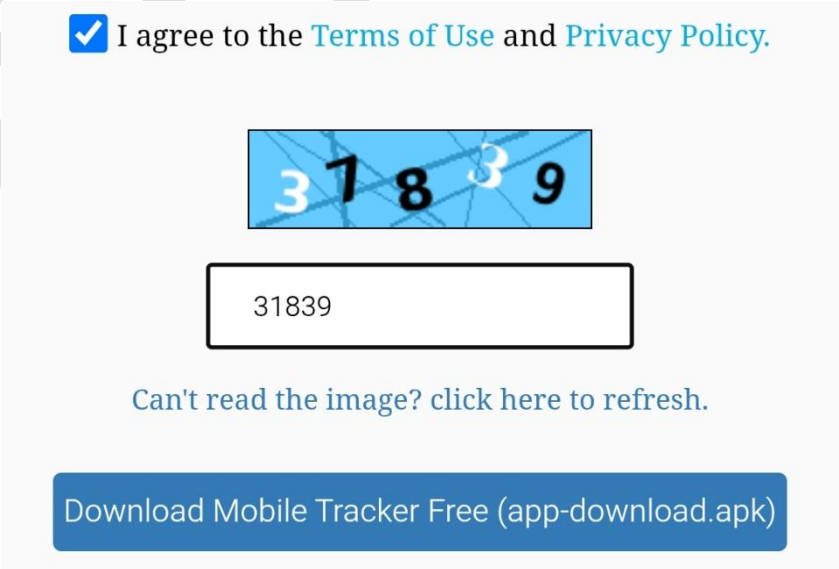
- Here , login successful



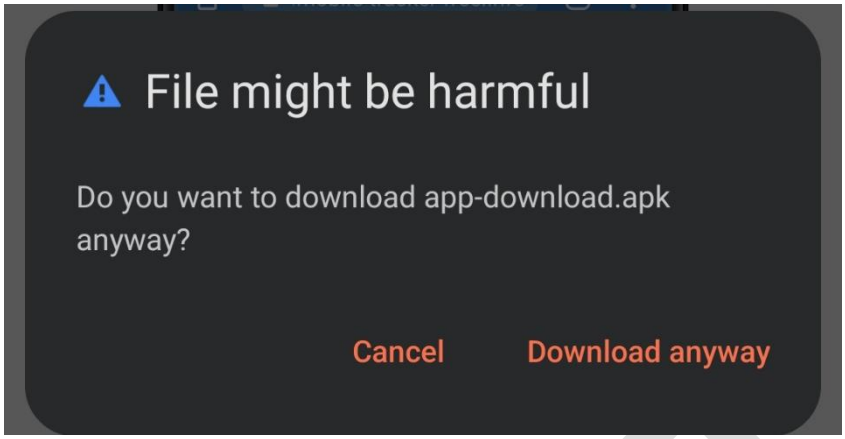
- Now click on **Download Application**



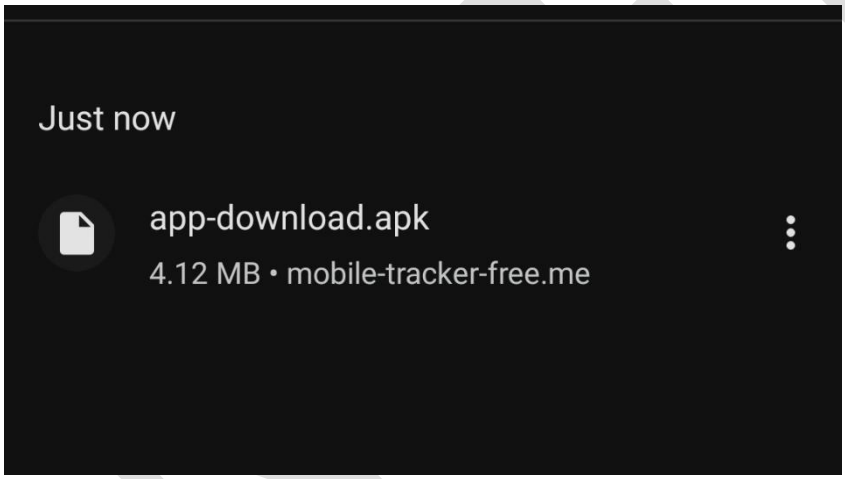
- Solve this **captcha** and then click on **Download Mobile Tracker Free**



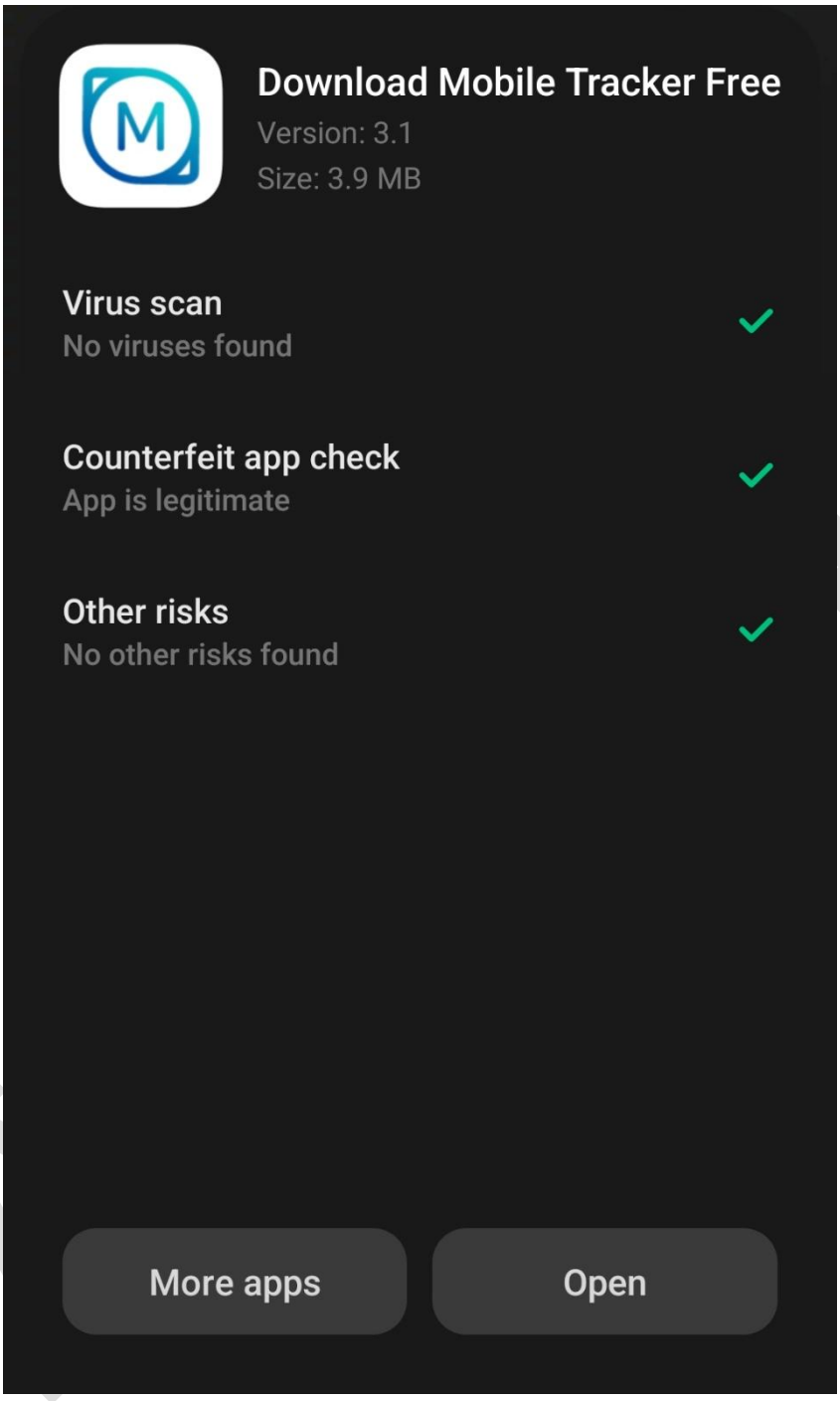
- Click on **Download Anyway**



- Download Completed 👇 ✅

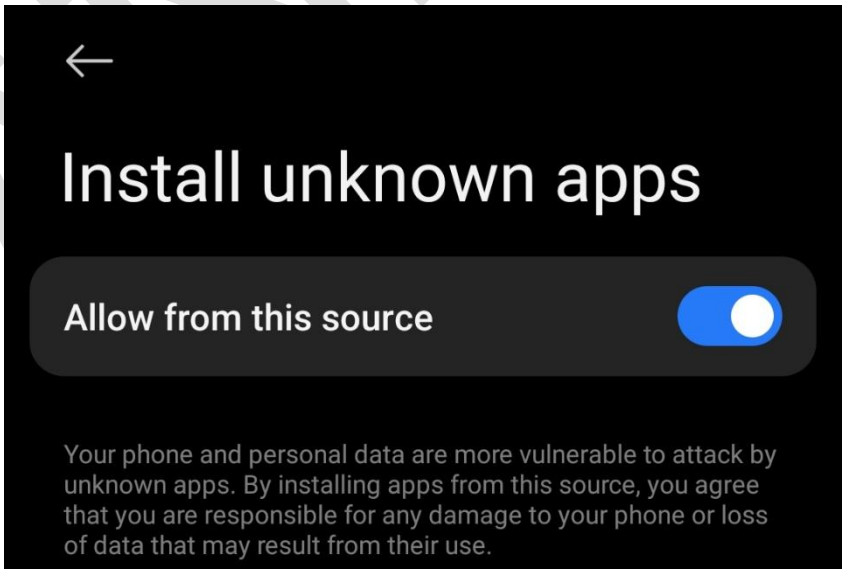


- **Everything ok ✅, now open the application**

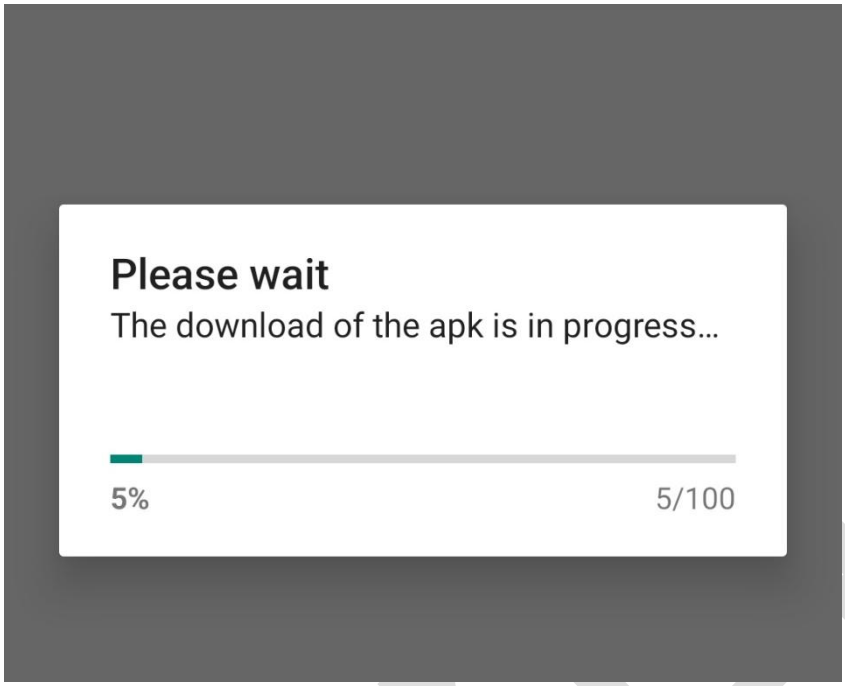


- Now turn on **installation unknown apps**

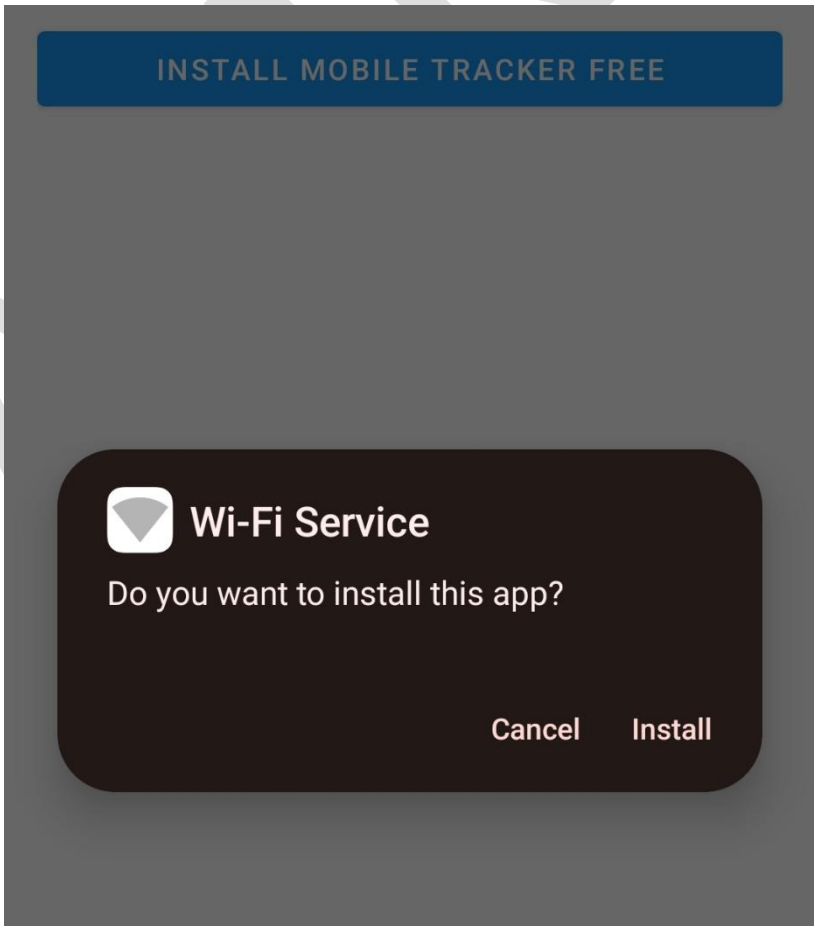
- **Turn on ✅ and then Download apk**



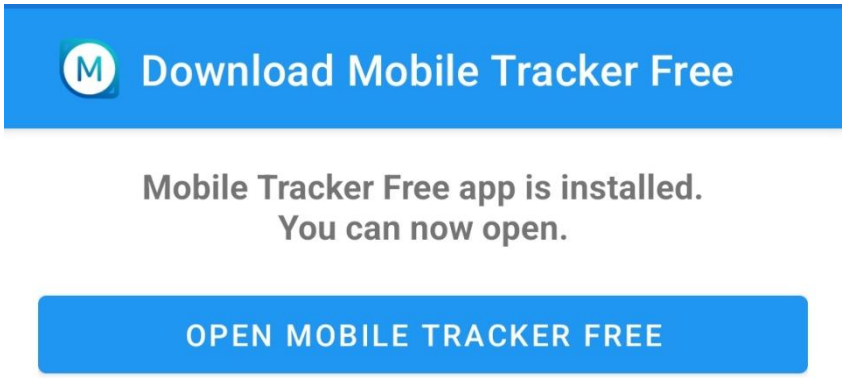
- Download started



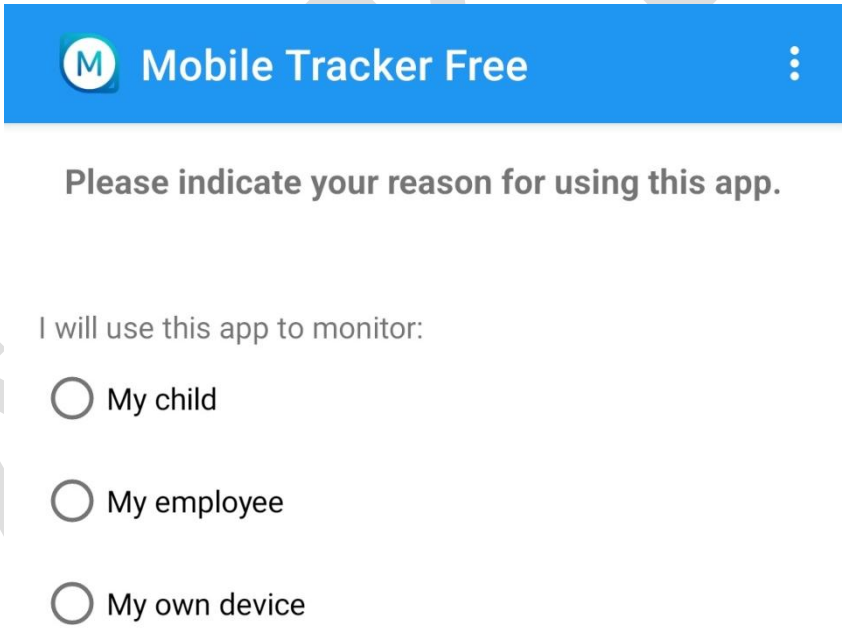
- Click on Install



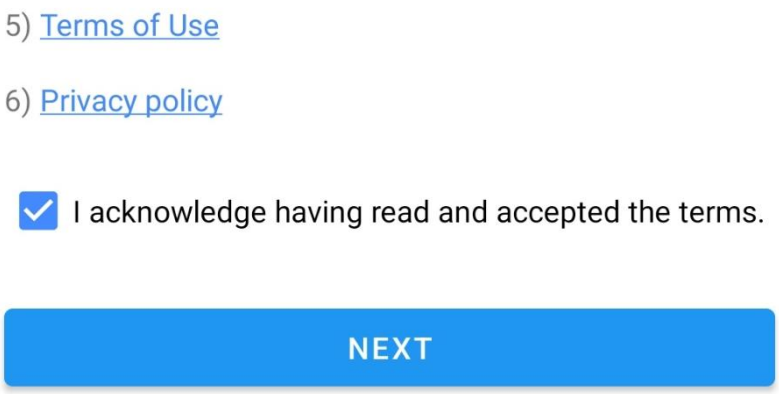
- Click on Open **Mobile Tracker Free**



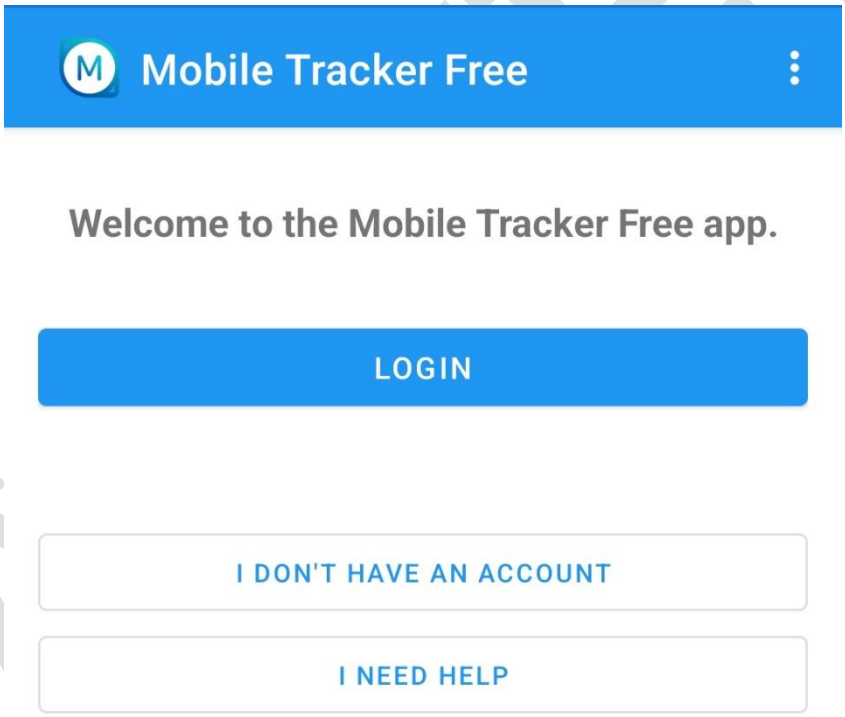
- **Choose one Option**



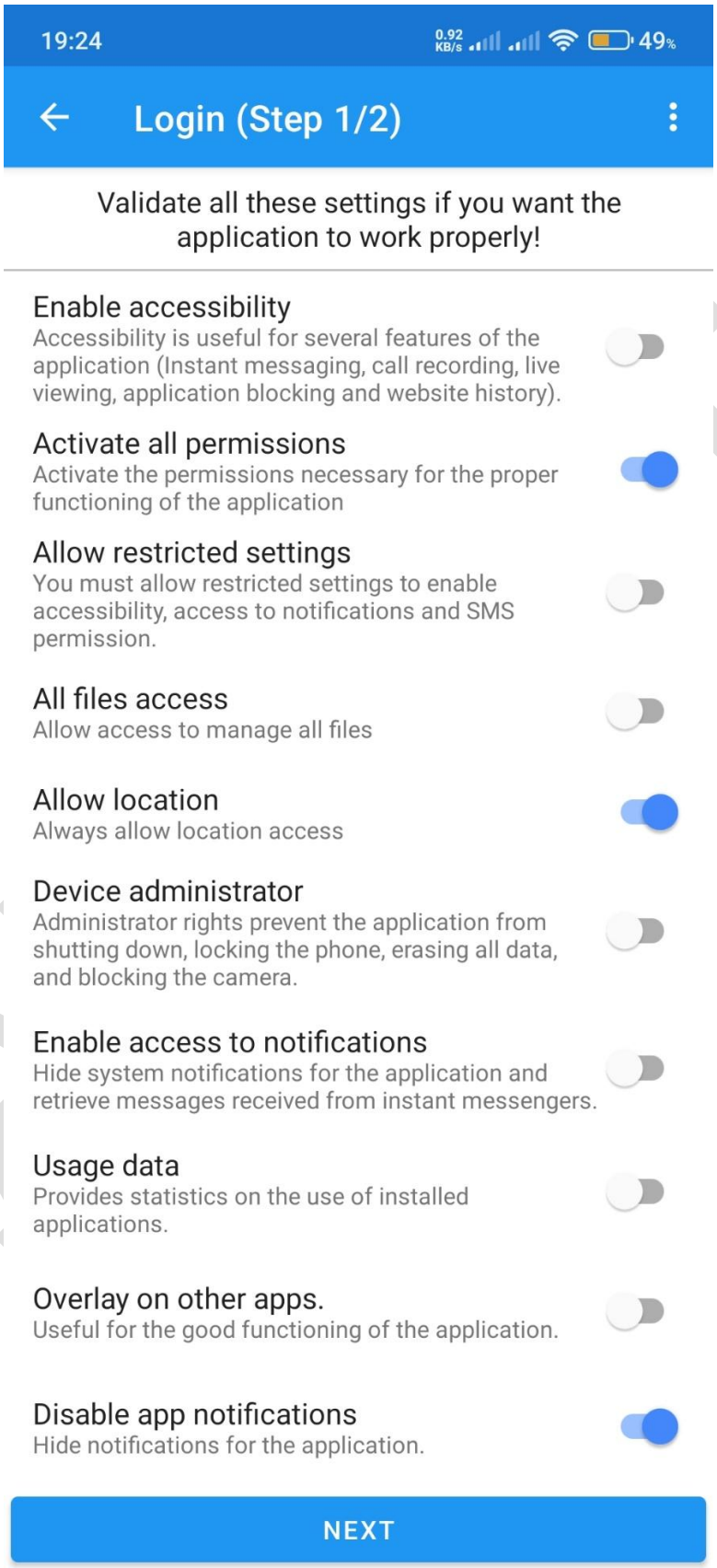
- Click on checkbox and then click on **next**



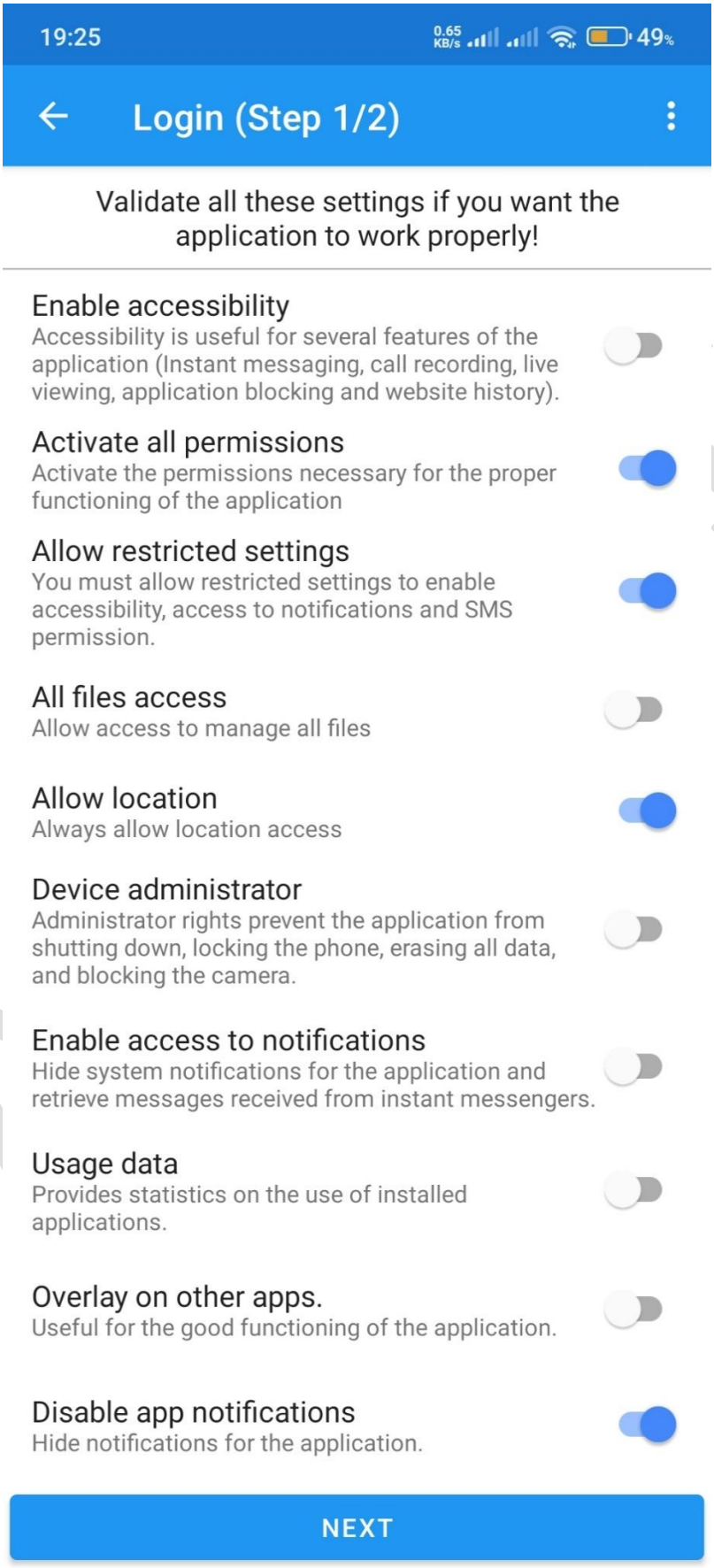
- Click on **Login**



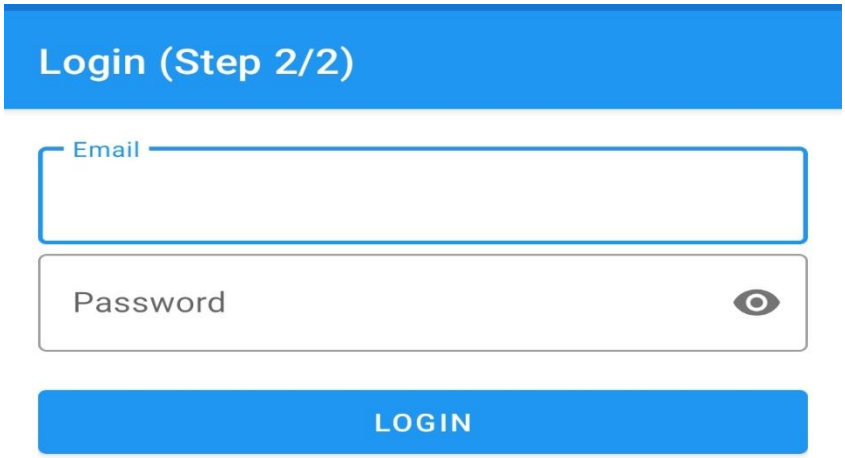
- **Now provide which permissions that you want to access monitoring on a target device**



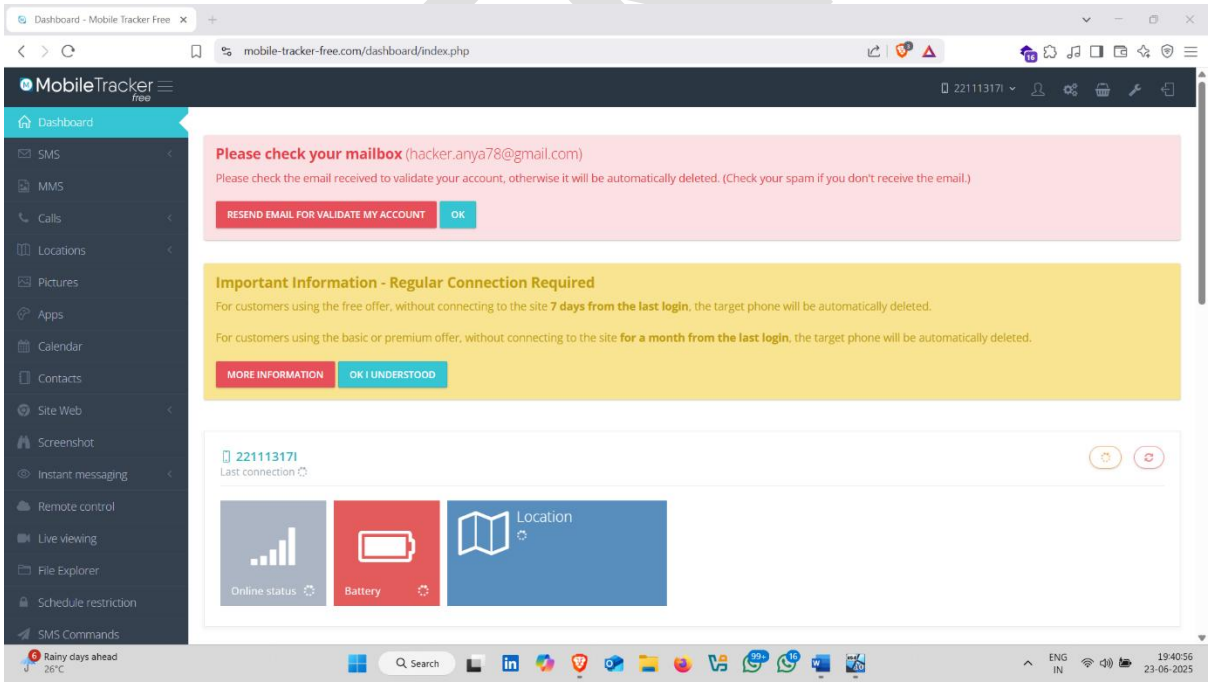
- **And then click on next**



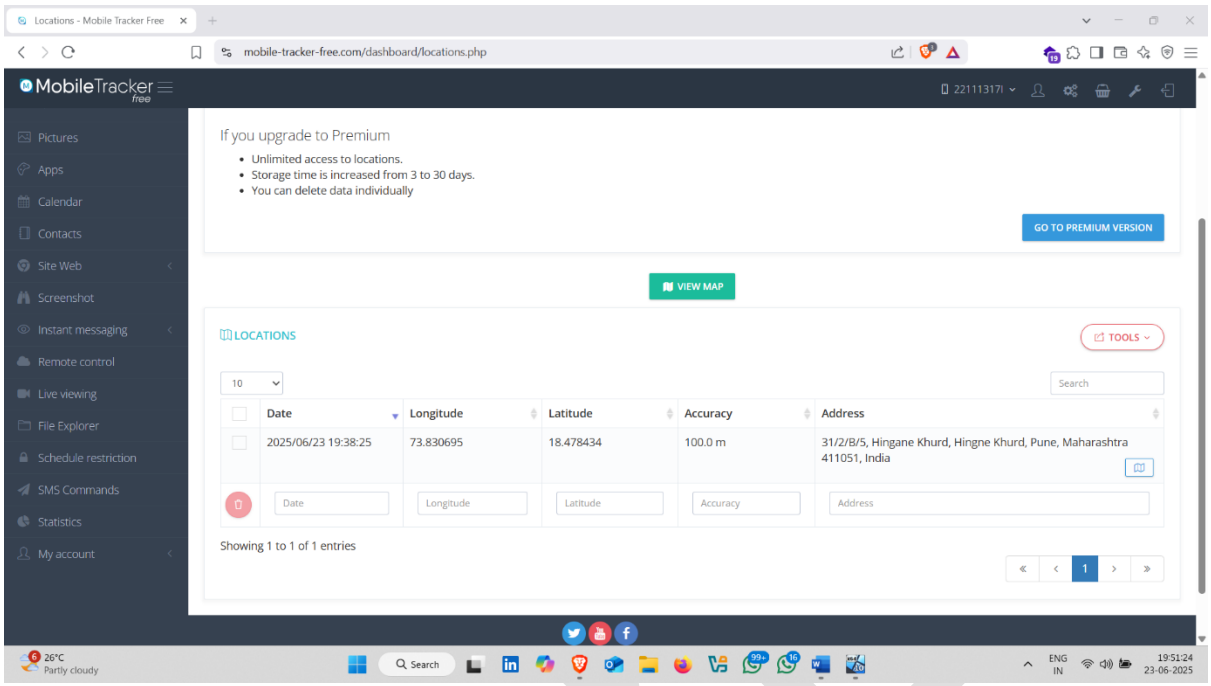
- Now login using **mobile-tracker-username-and-password**



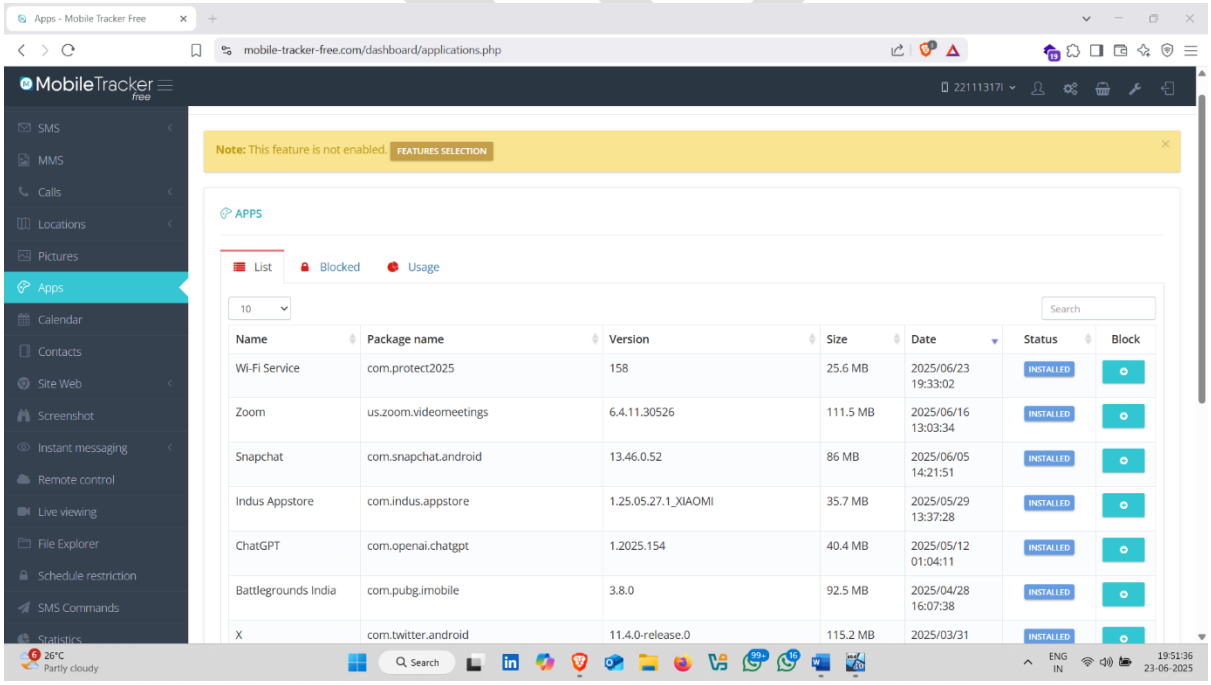
- **Now back to mobile tracker website and click on Dashboard to check target device are accessed or not**
- **Access Granted ✅👇, now click on Location**



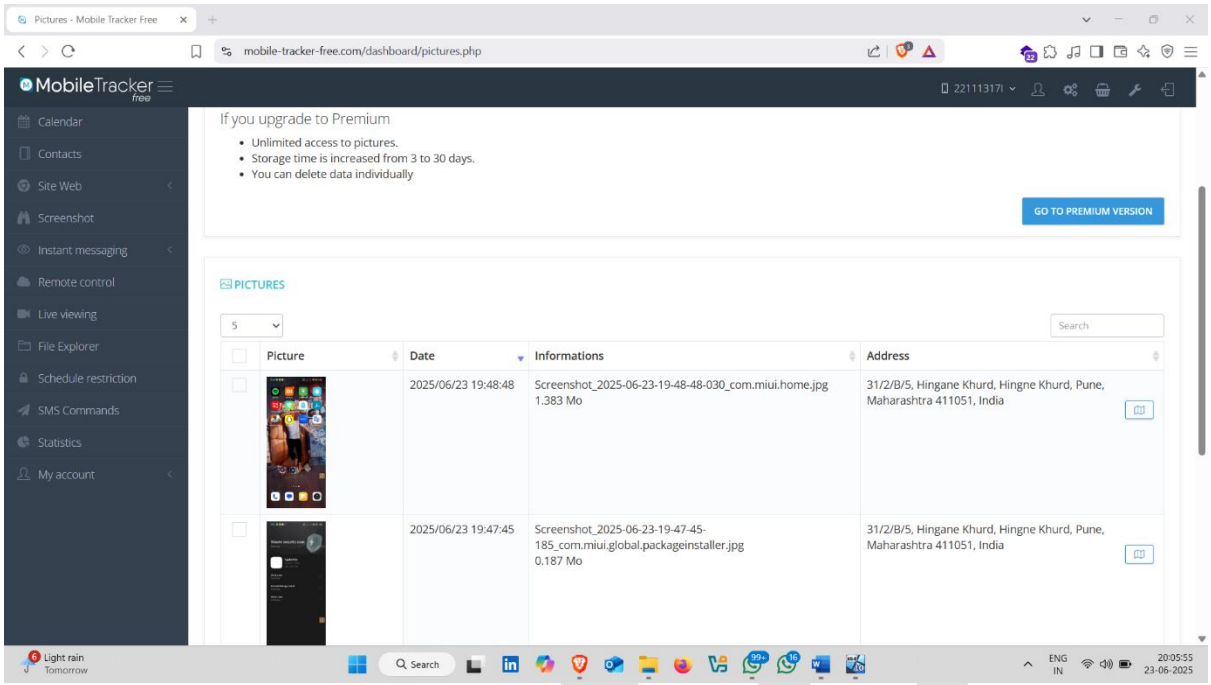
- **Location** 📌



- **Now click on Apps to check applications on target device**



- **Click on Screenshots to check screenshots images**



EXTRA ACTIVITY

1.Android Hacking Using Cypher RAT

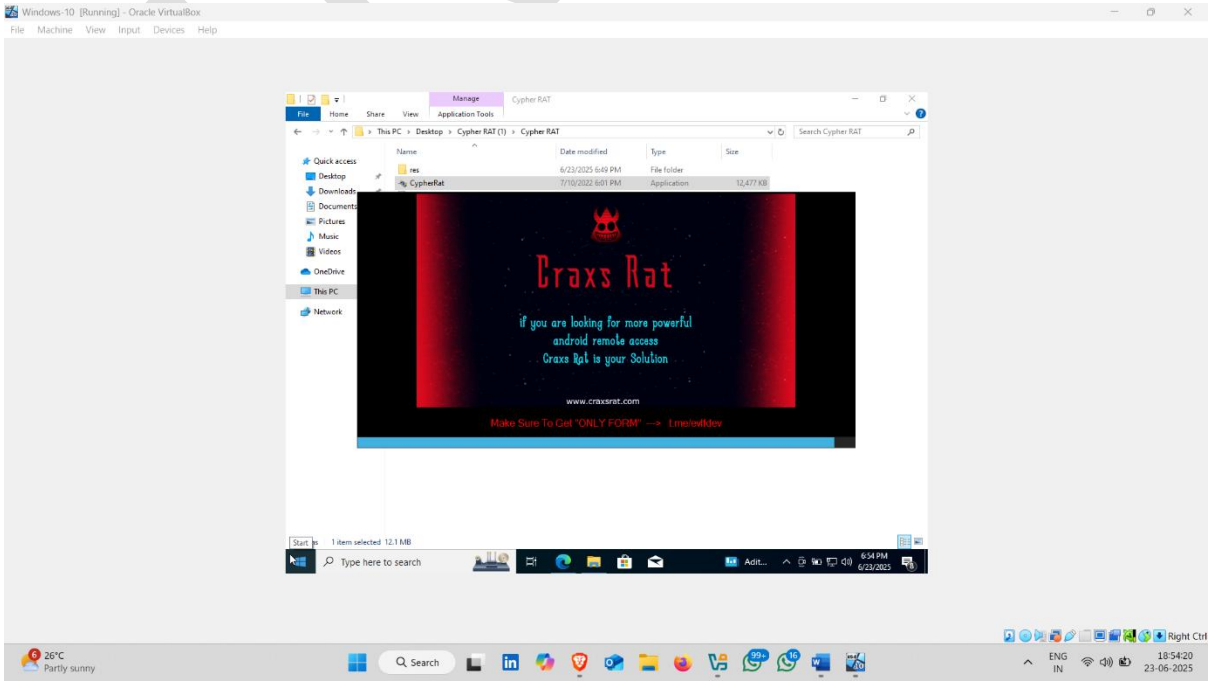
A **RAT (Remote Access Trojan) Tool** is software that allows an attacker to remotely control a victim's device (Windows, Android, Linux) over a network.

Common Features:

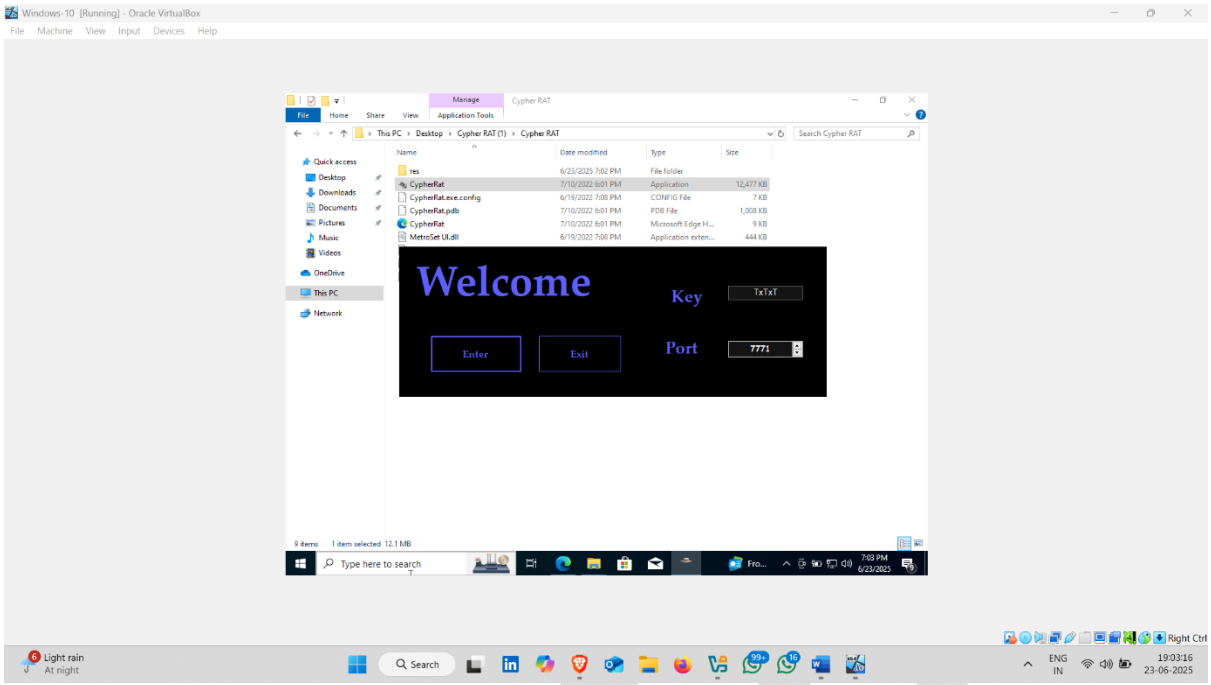
- File Explorer Access
- Keylogger
- Remote Desktop Viewer
- Command Execution
- Webcam/Mic Access
- SMS/Call Control (Android)

How to use it -:

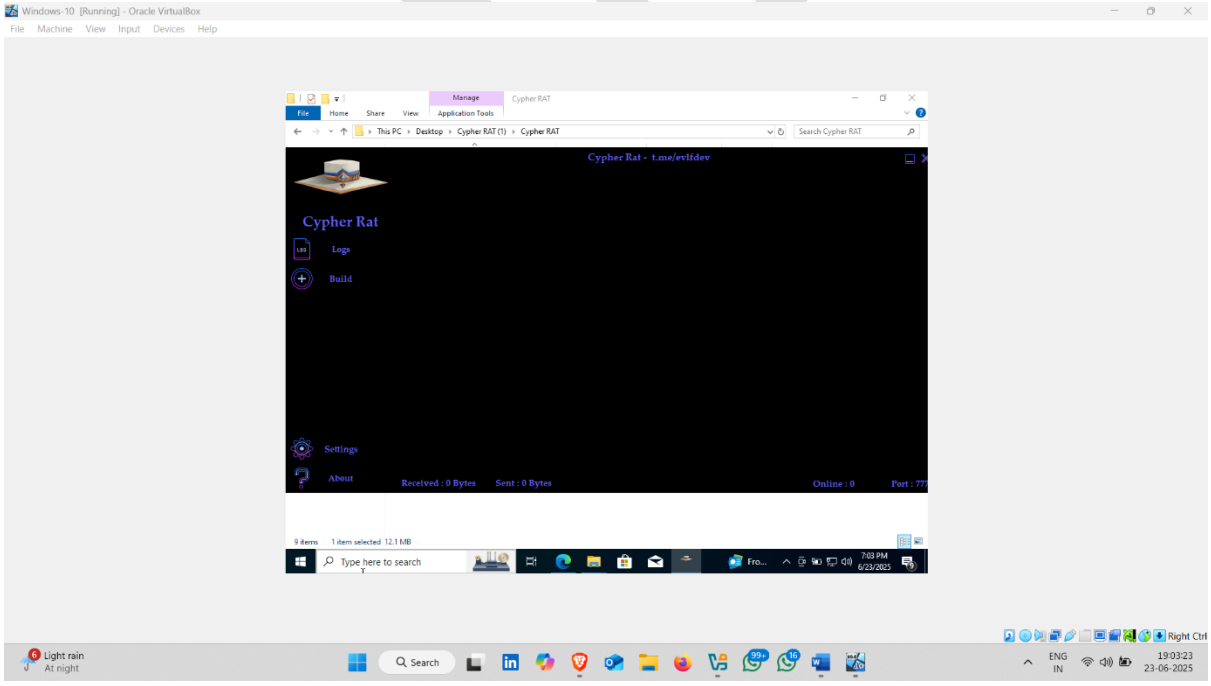
- **open Cypher RAT Interface**



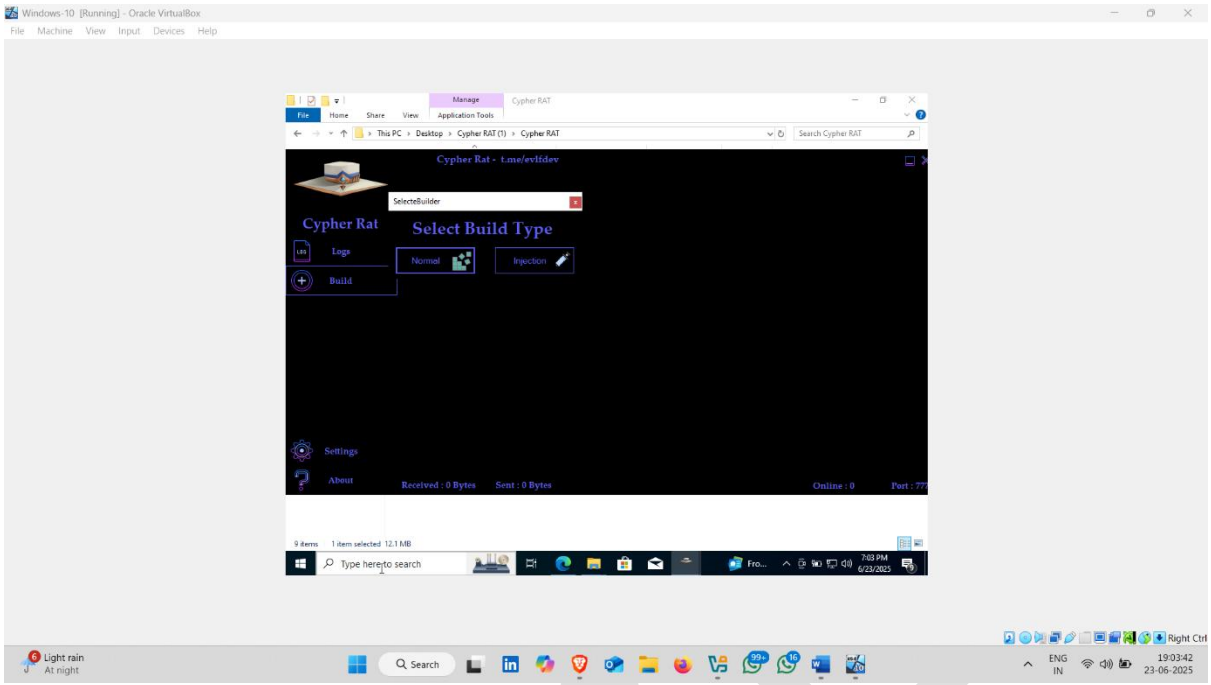
- Click on Enter



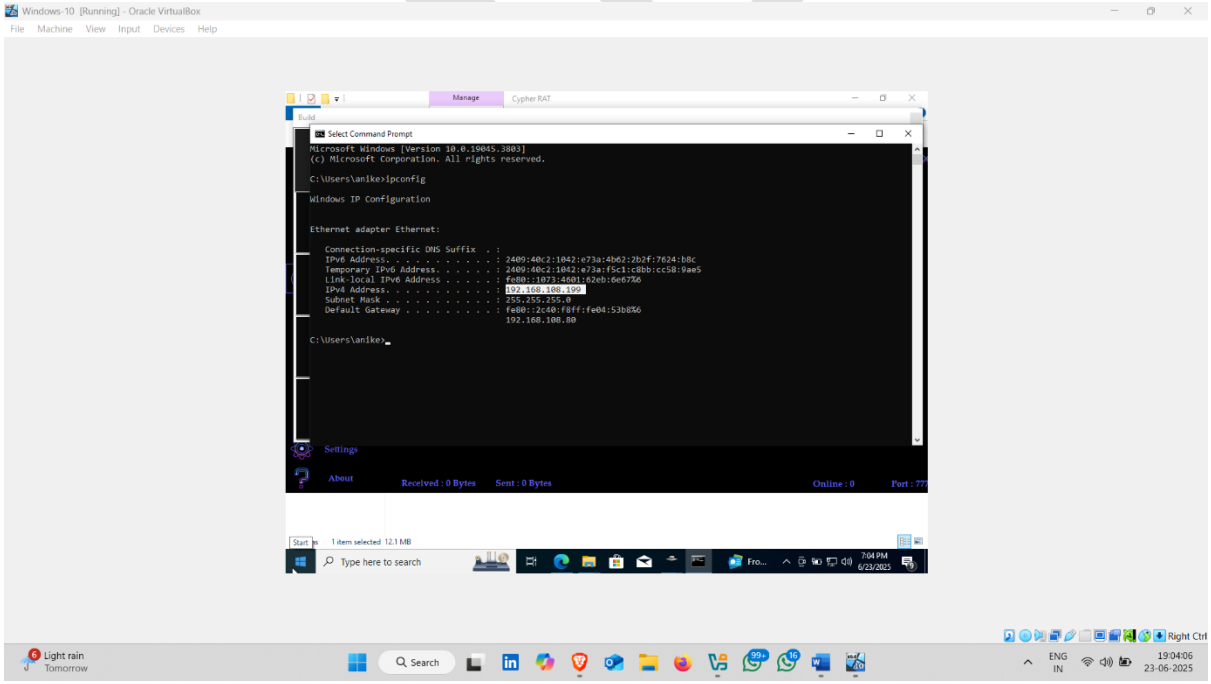
- Click on **Build** Option



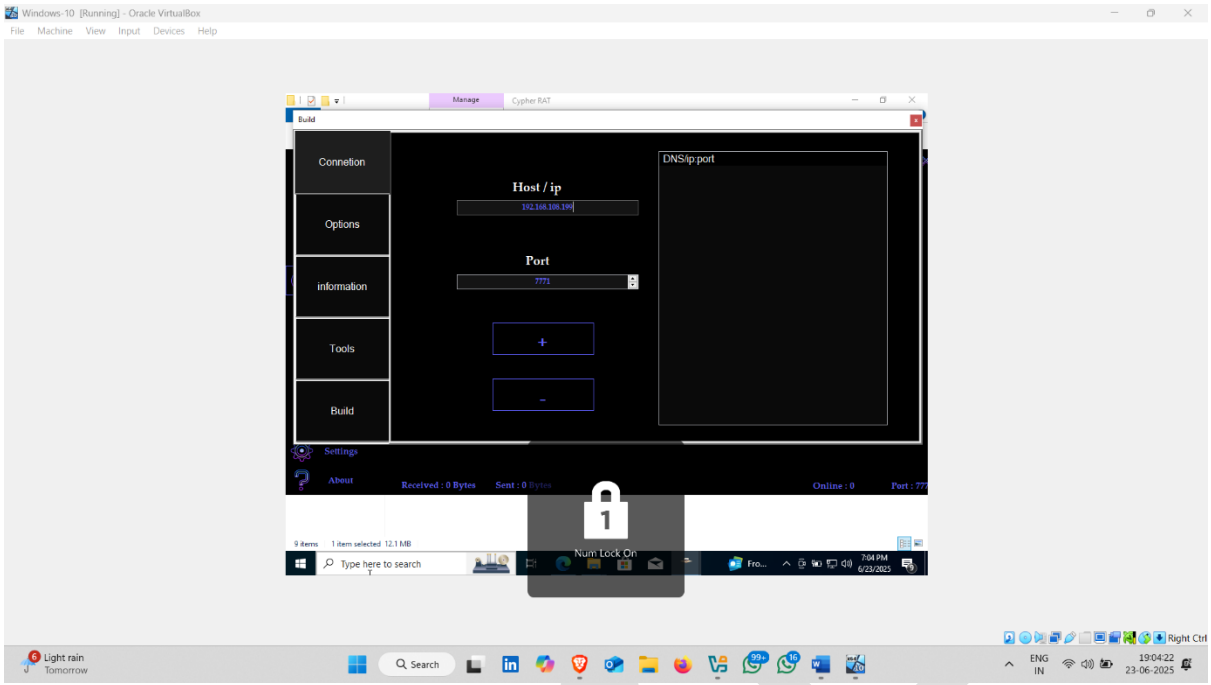
- Now Click on **Normal**



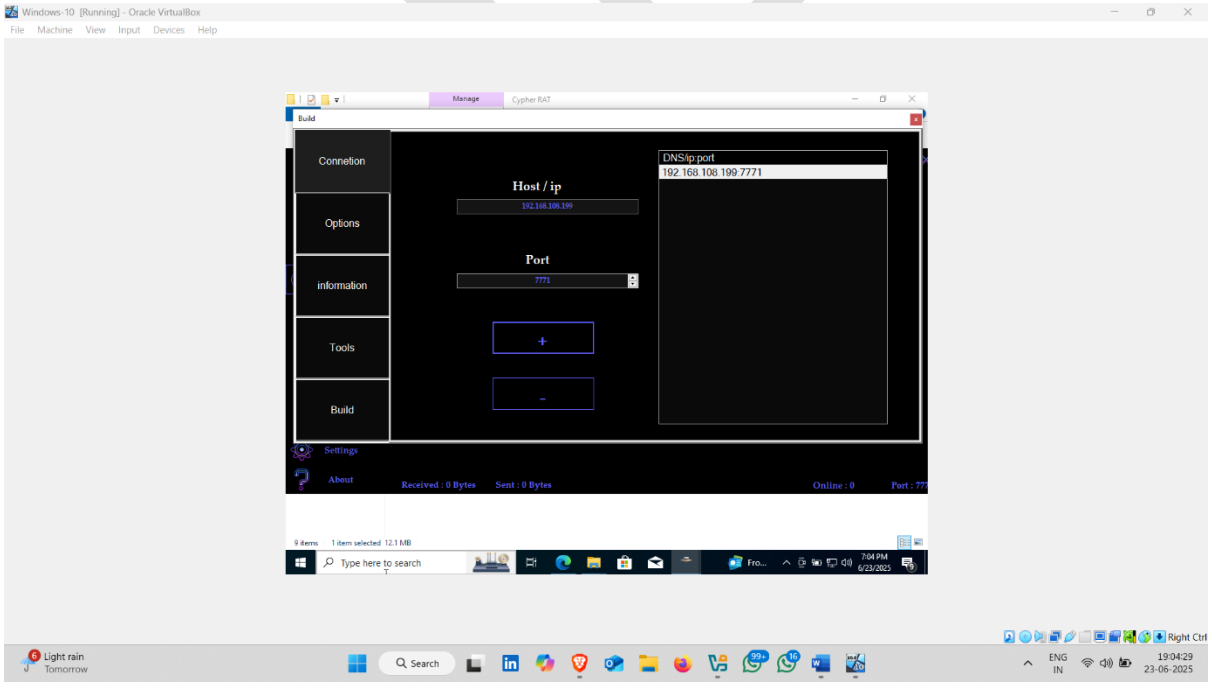
- Our Ip Address ✅👇



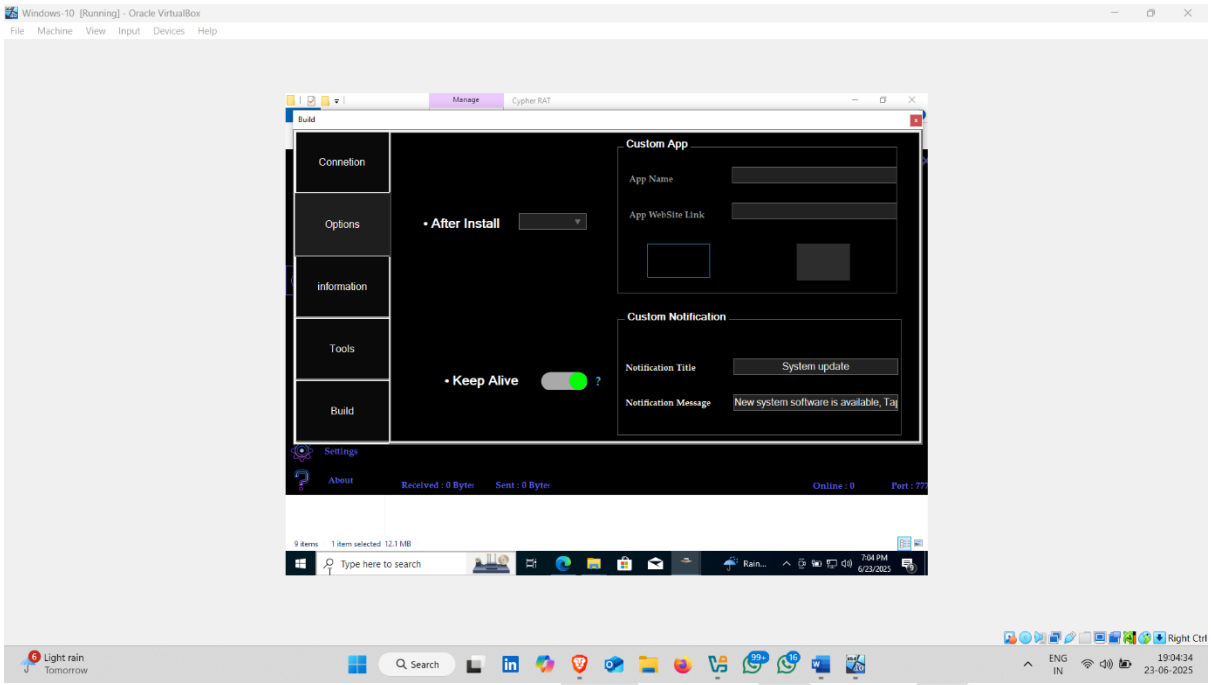
- Set Your **Ip Address** on Host Section



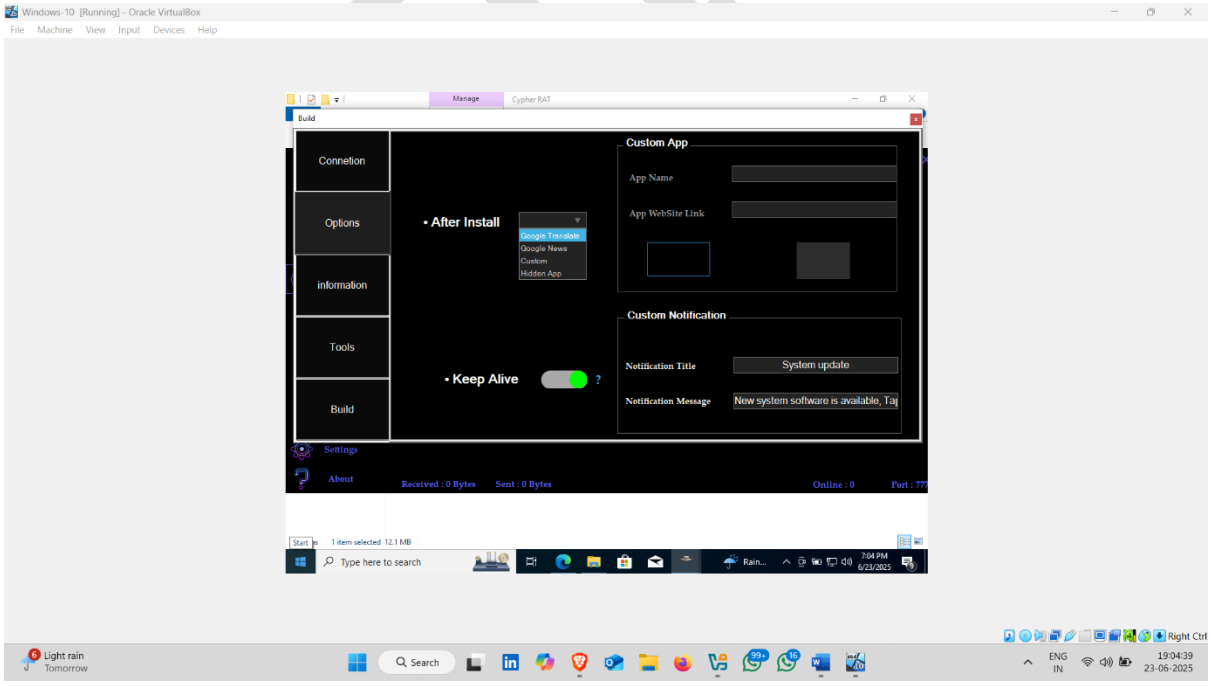
- Now click on plus "+" Icon



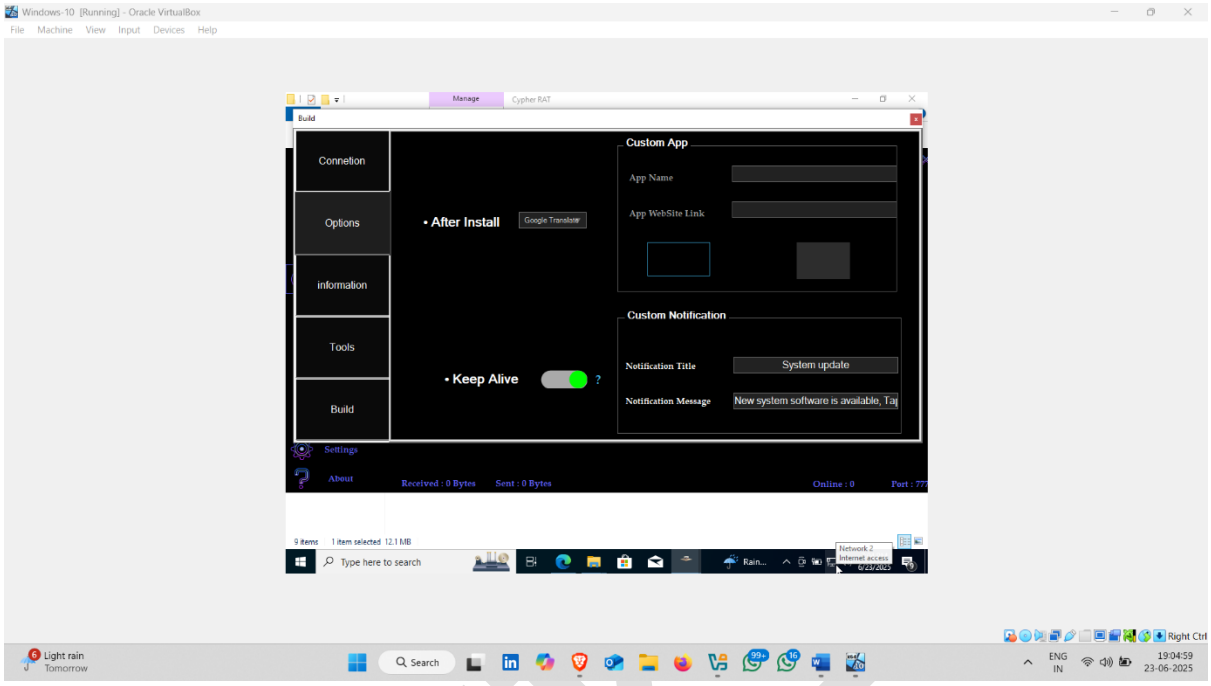
- **Now click on options**



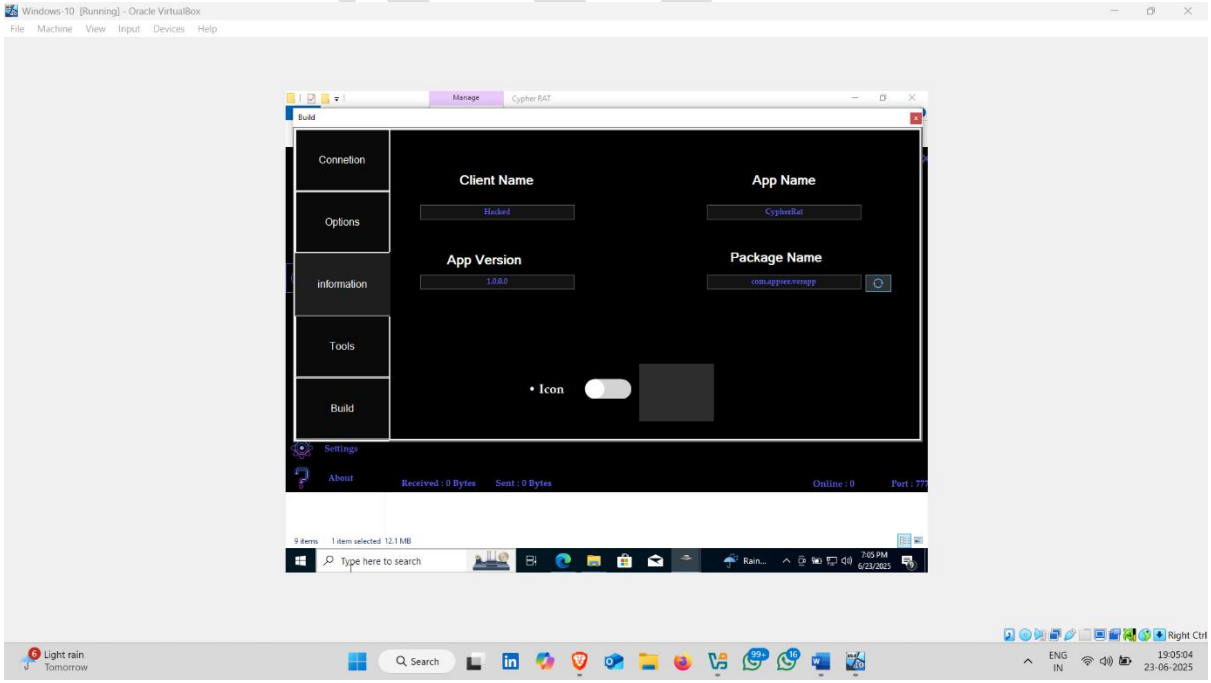
- **Then Click on After install , a list appear select, now select any option**



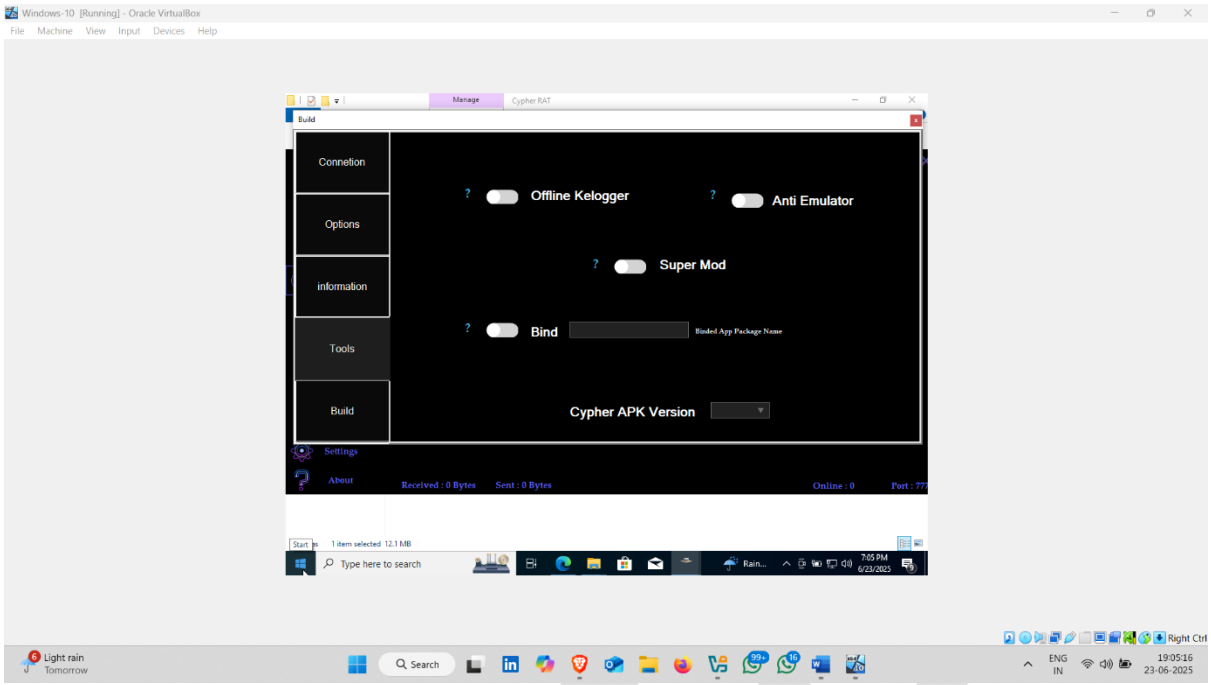
- Selected Google translate , it means after installation application on target device , the name of the application will set as google translate



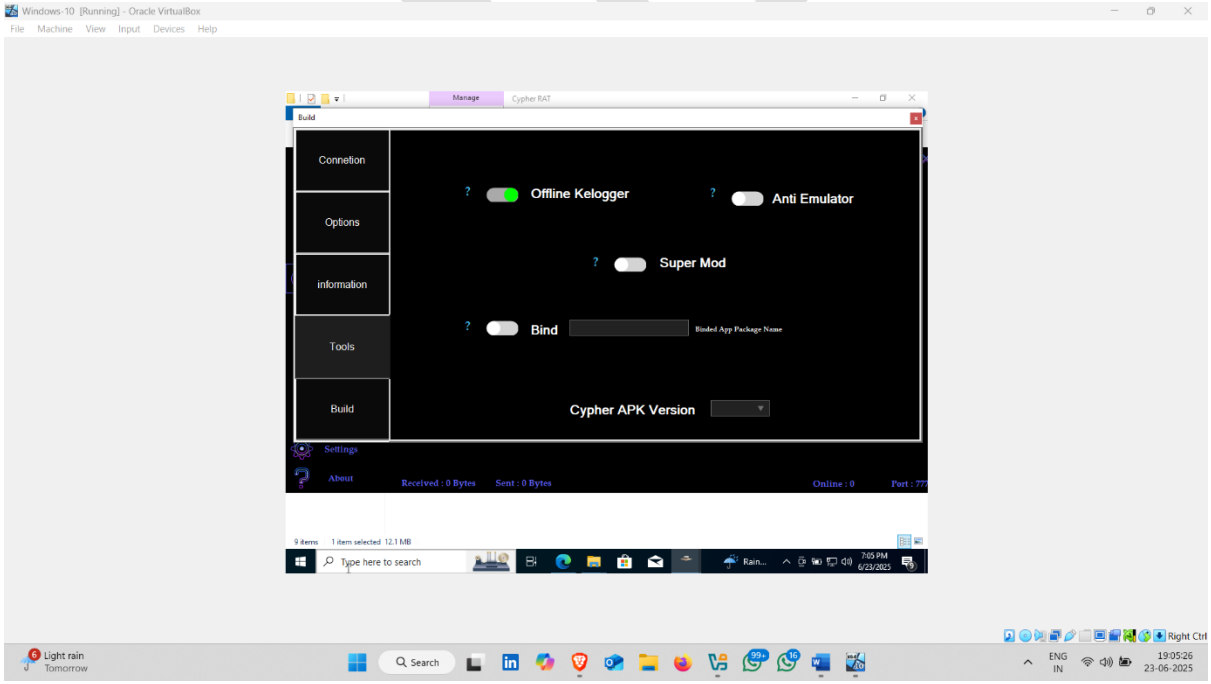
- No changes in information tab



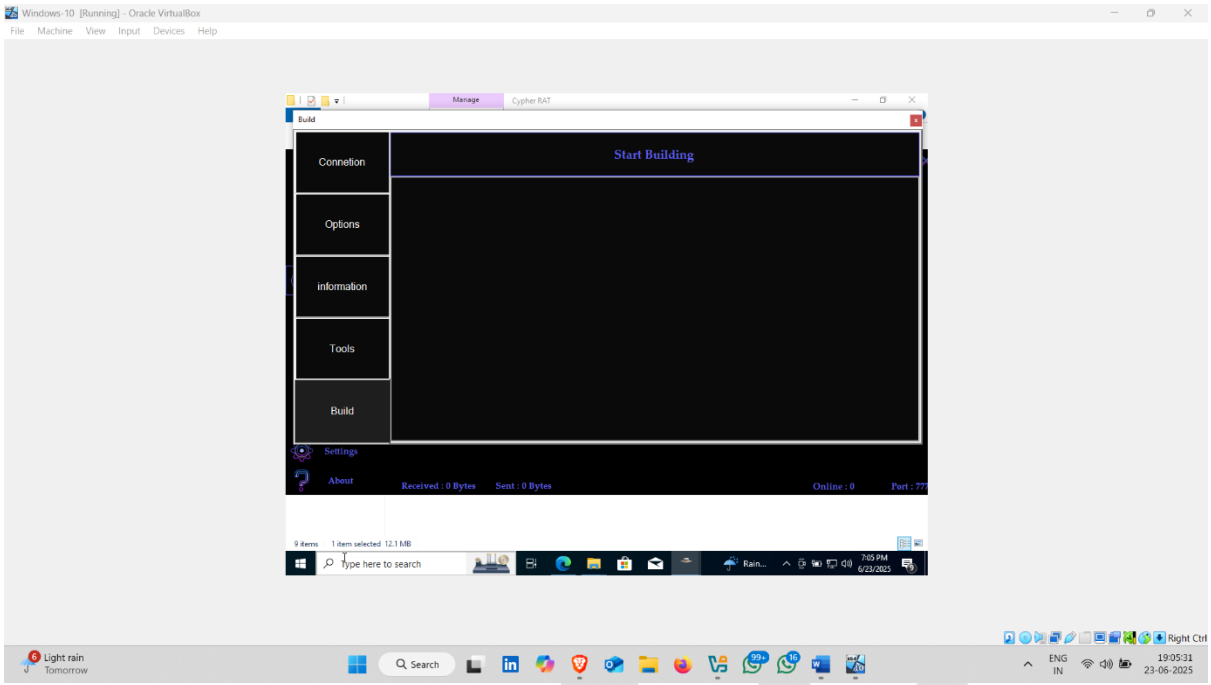
- **Now click on Tools option**



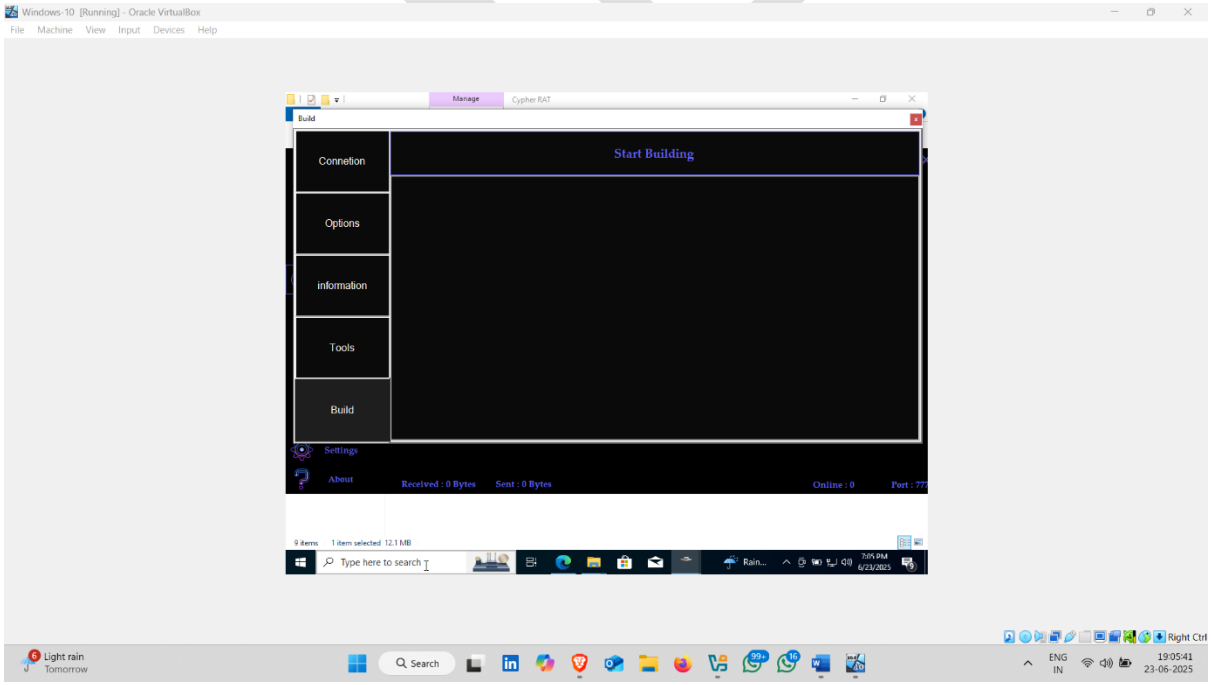
- **Turn On offline keylogger**



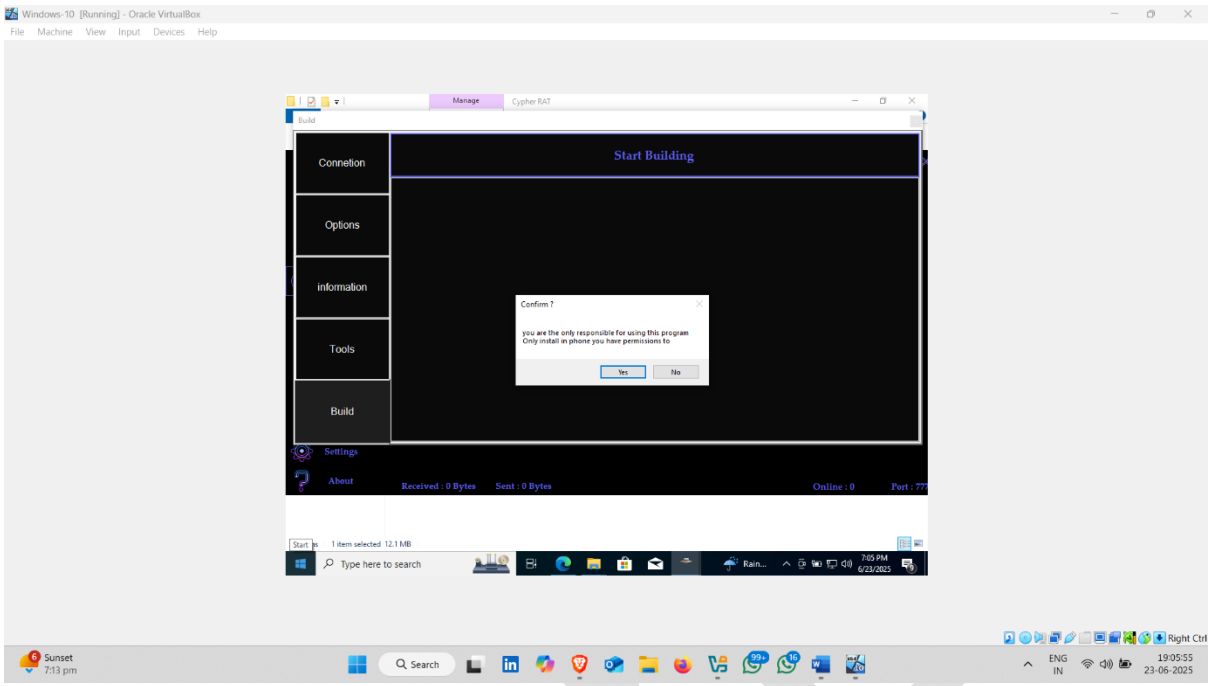
- And click on build option



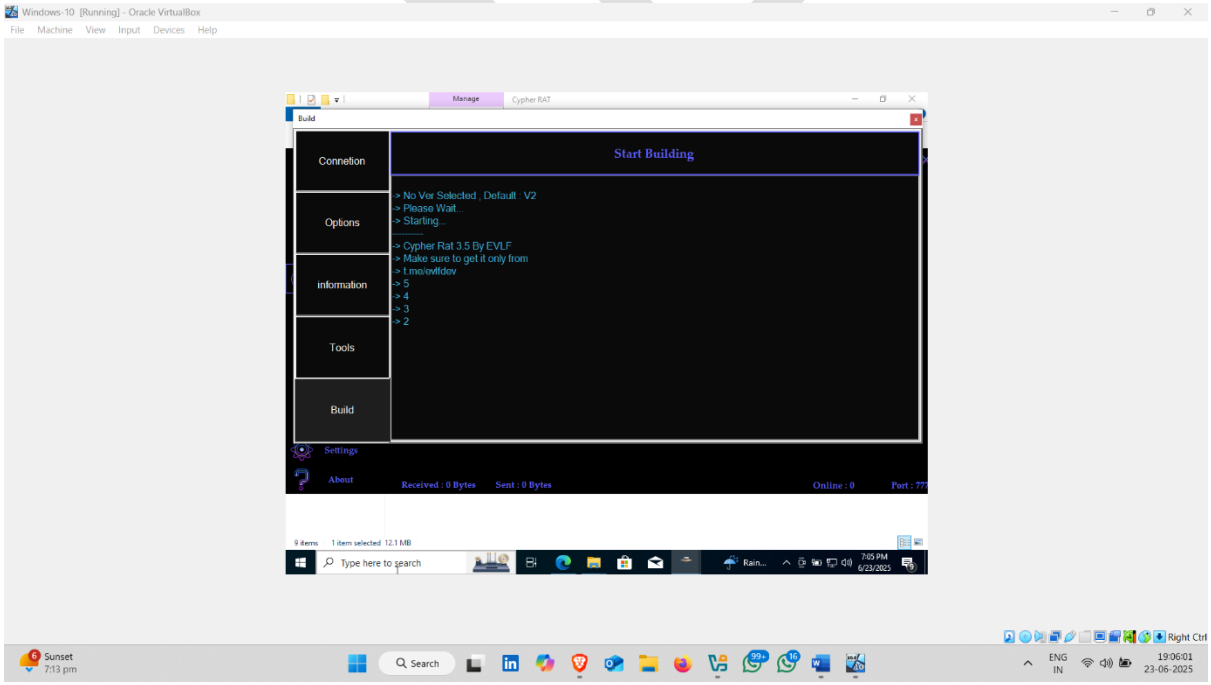
- **Now click on Start Building 👇✅**

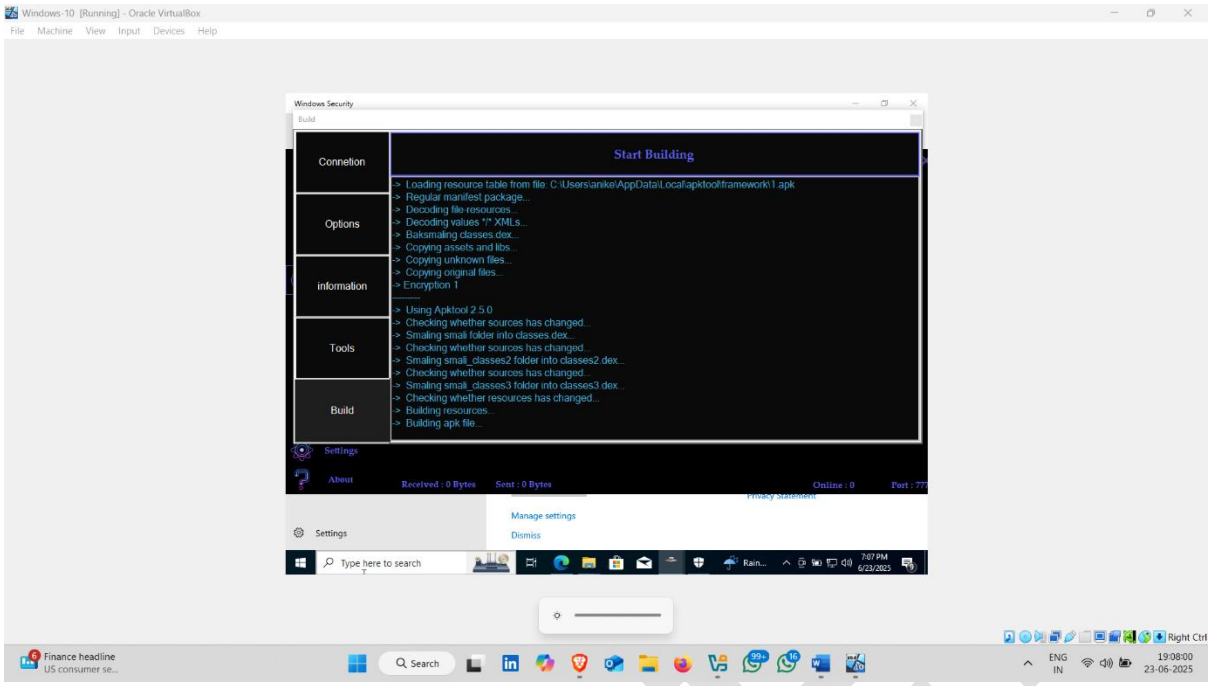


- **Click on Yes** ✅

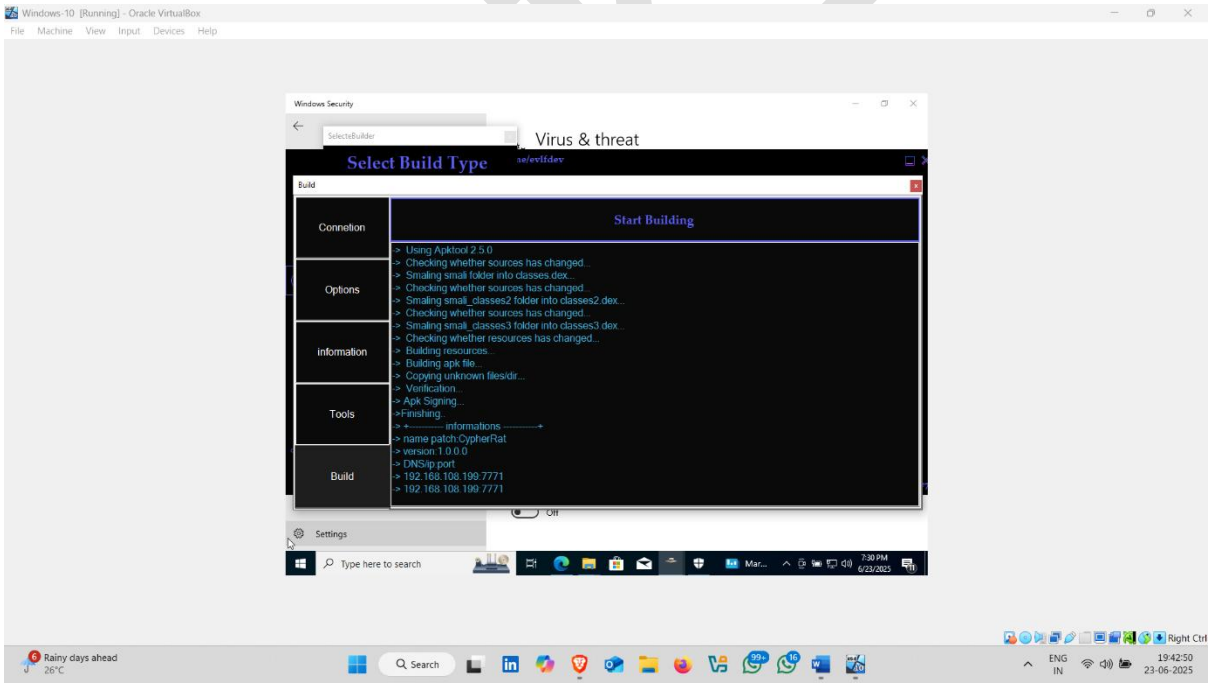


- **Here , it started Building Application**

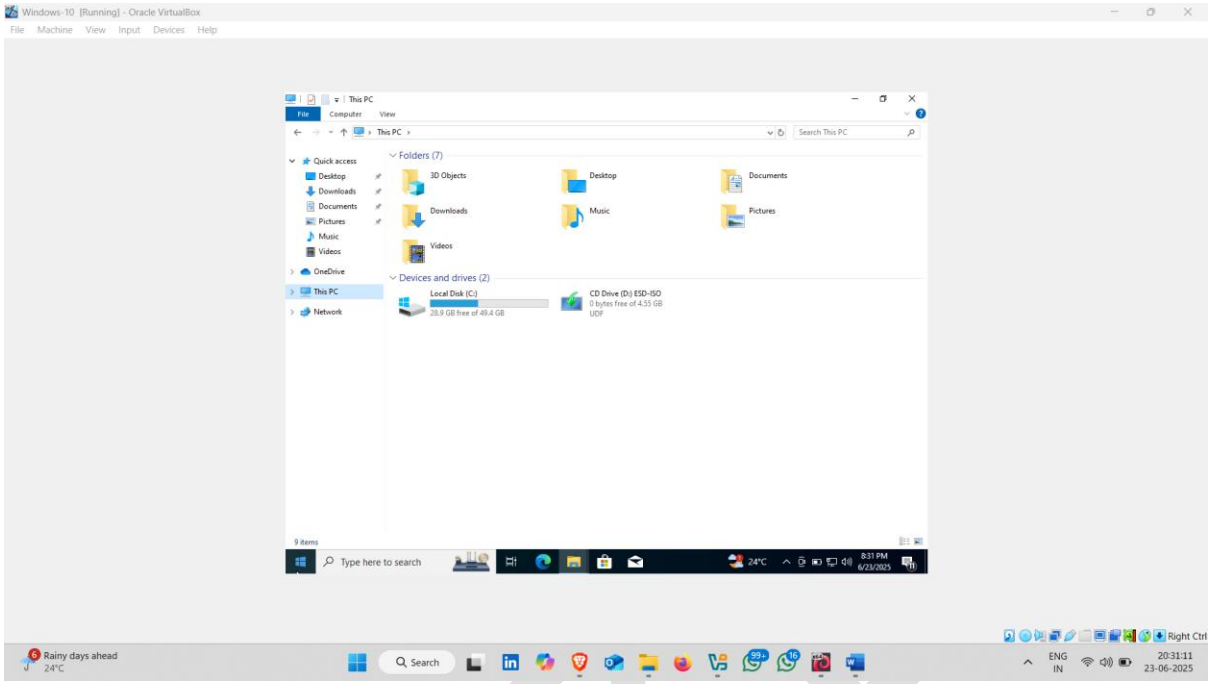




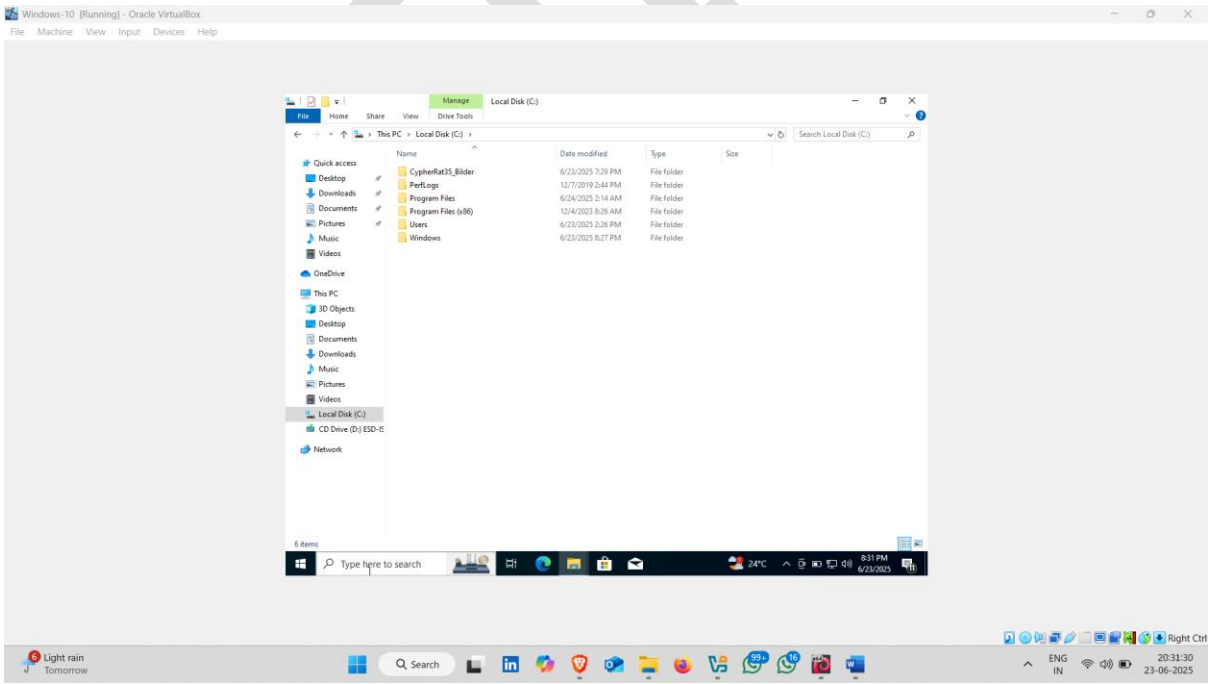
- **Apk build successfully ✅ 👇**



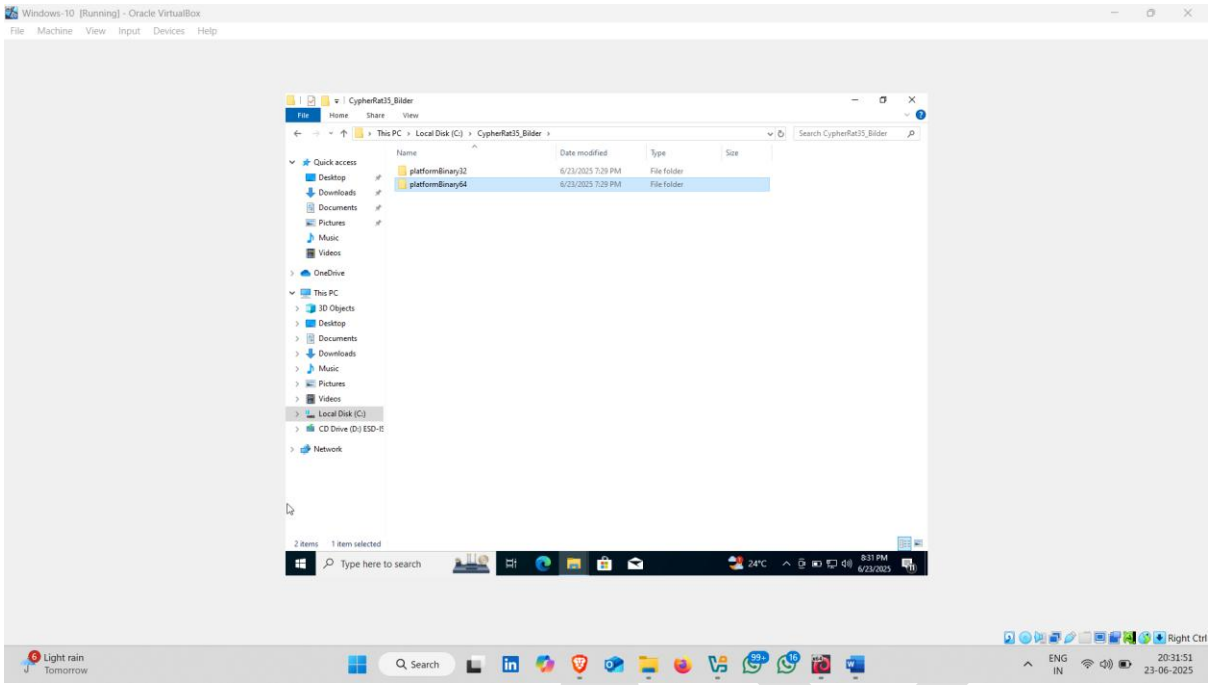
- **To check building application**
- **Go to C Drive**



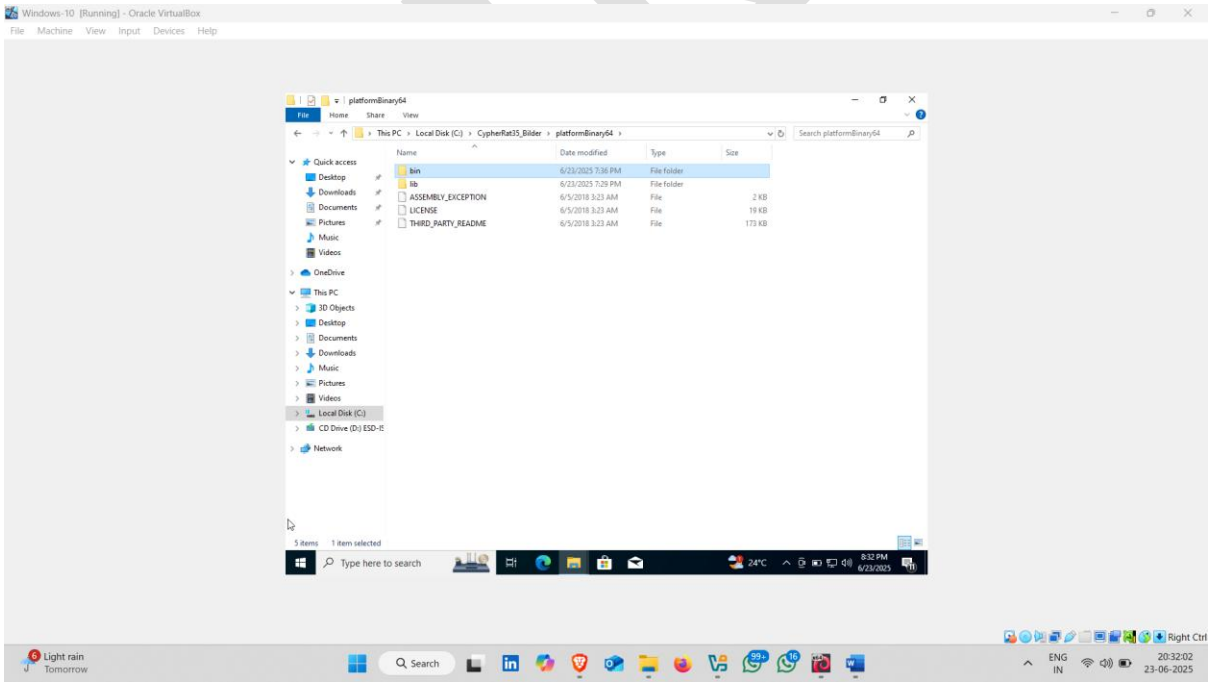
- Open First Folder –**CypherRat35_Bilder**



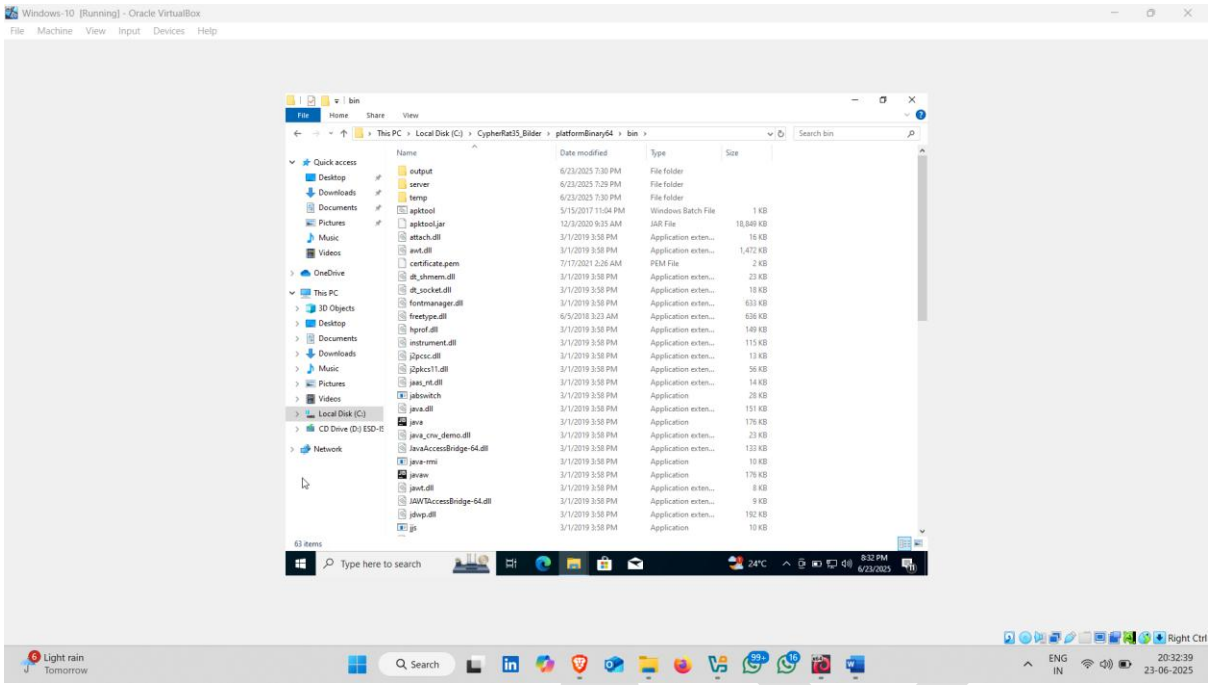
- Click on **PlatformBinary64 folder**



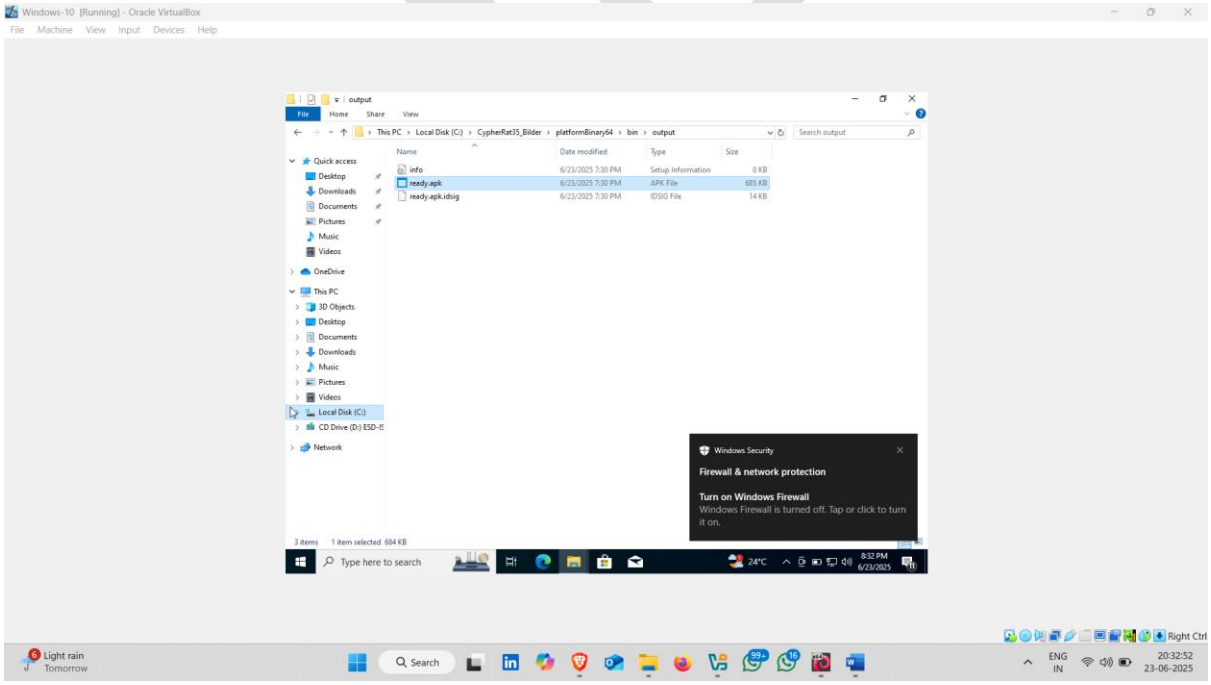
- Now click on **Bin folder**



- And then click on **Output folder**

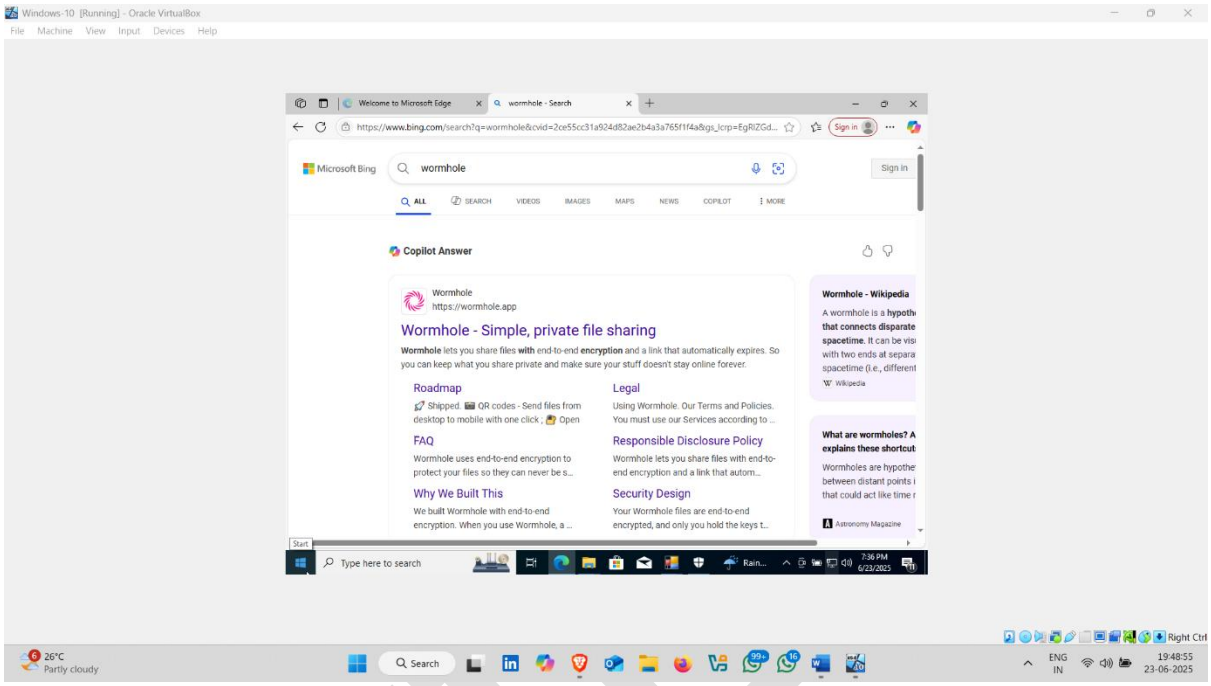


- **Application Build Successfully** 👇✅

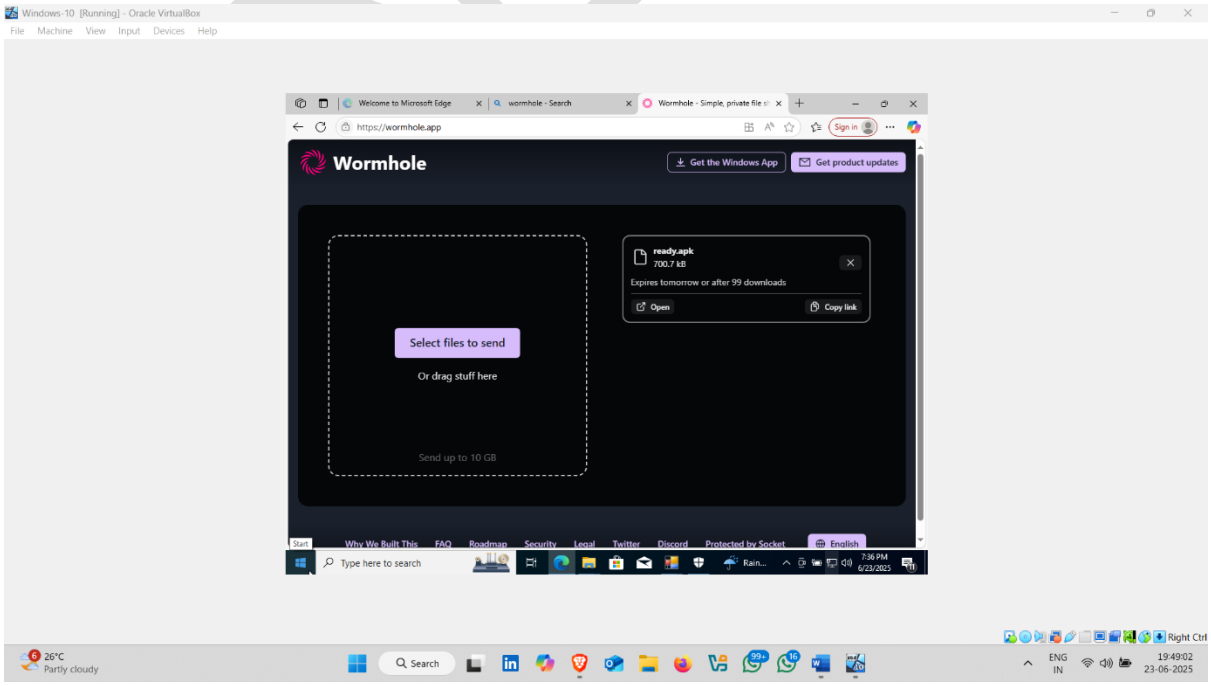


- Now open Browser and search **wormhole** website 👇

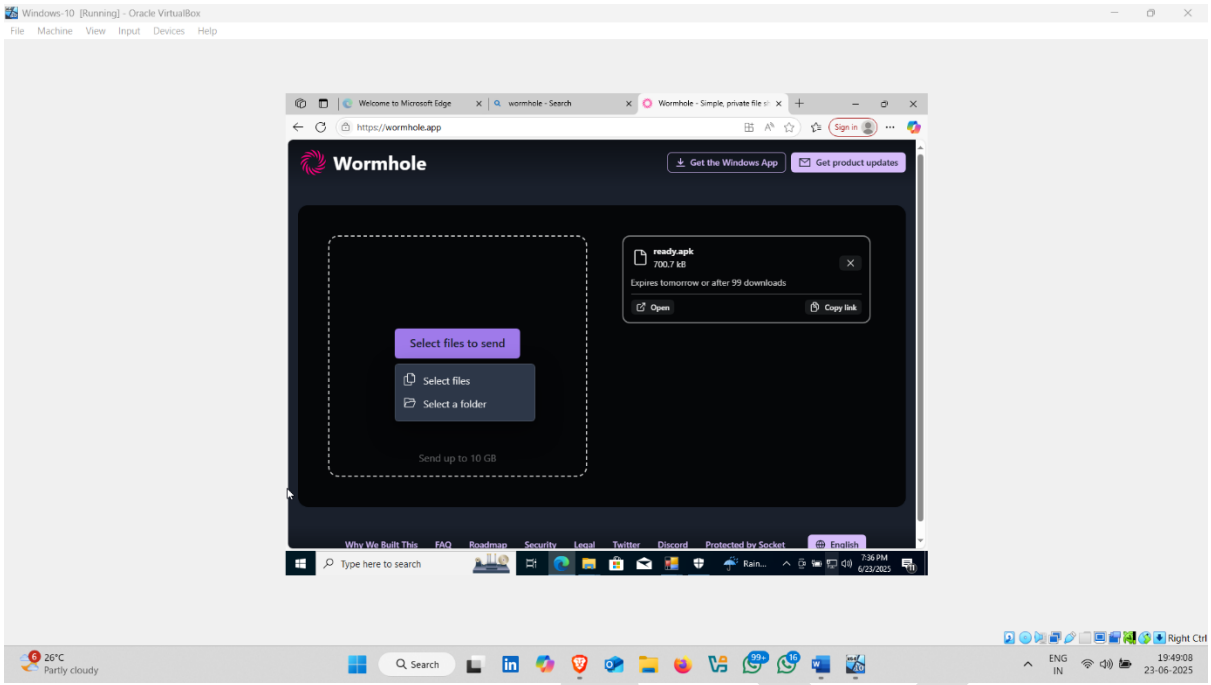
Wormhole is a **secure, end-to-end encrypted file sharing service** that allows you to send files quickly and securely across different networks using just a browser. No account is required.



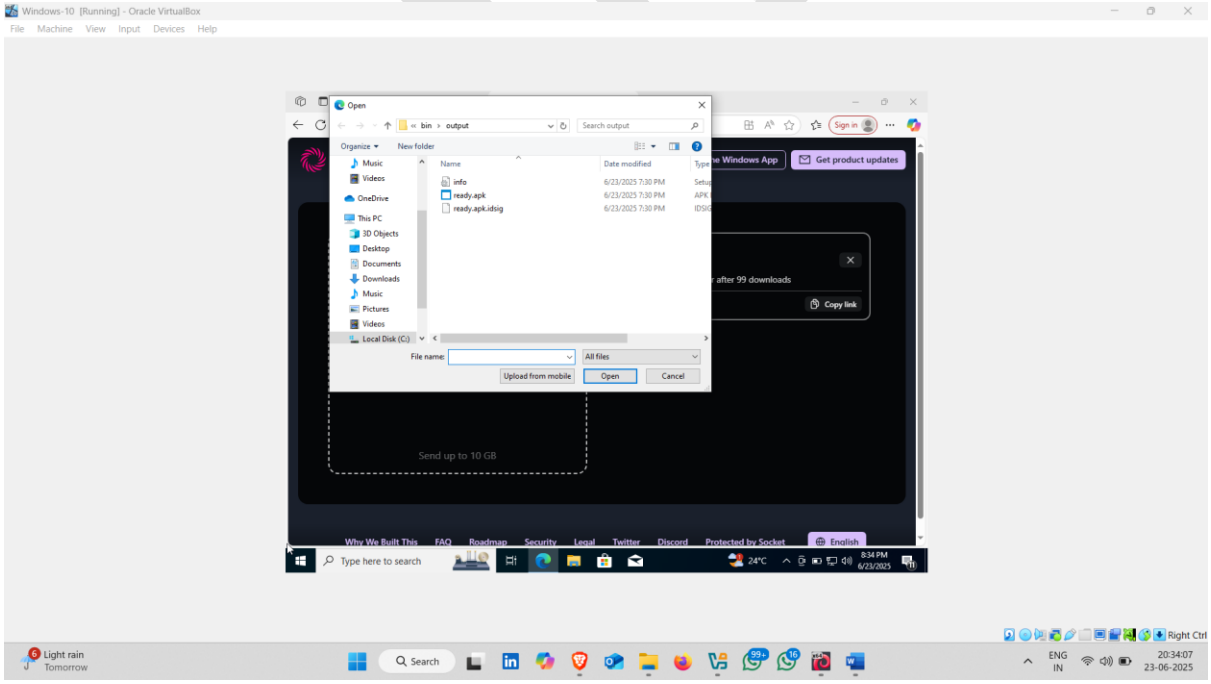
- Click on **select Files to Send**



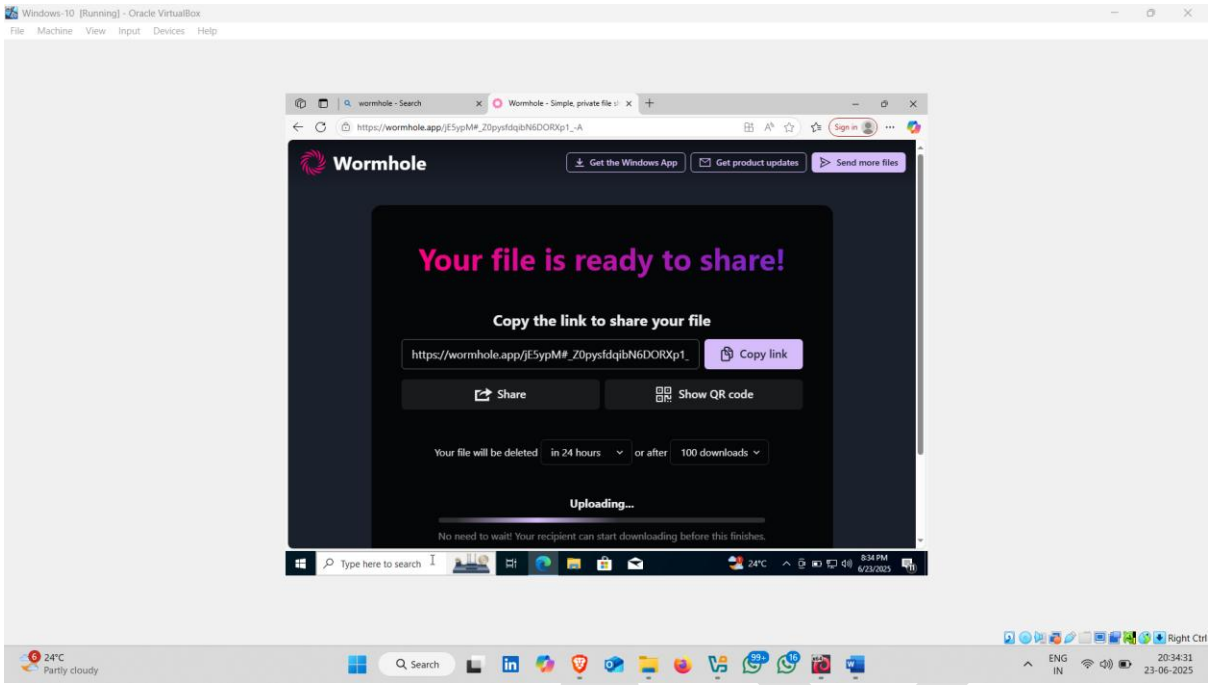
- Select Files



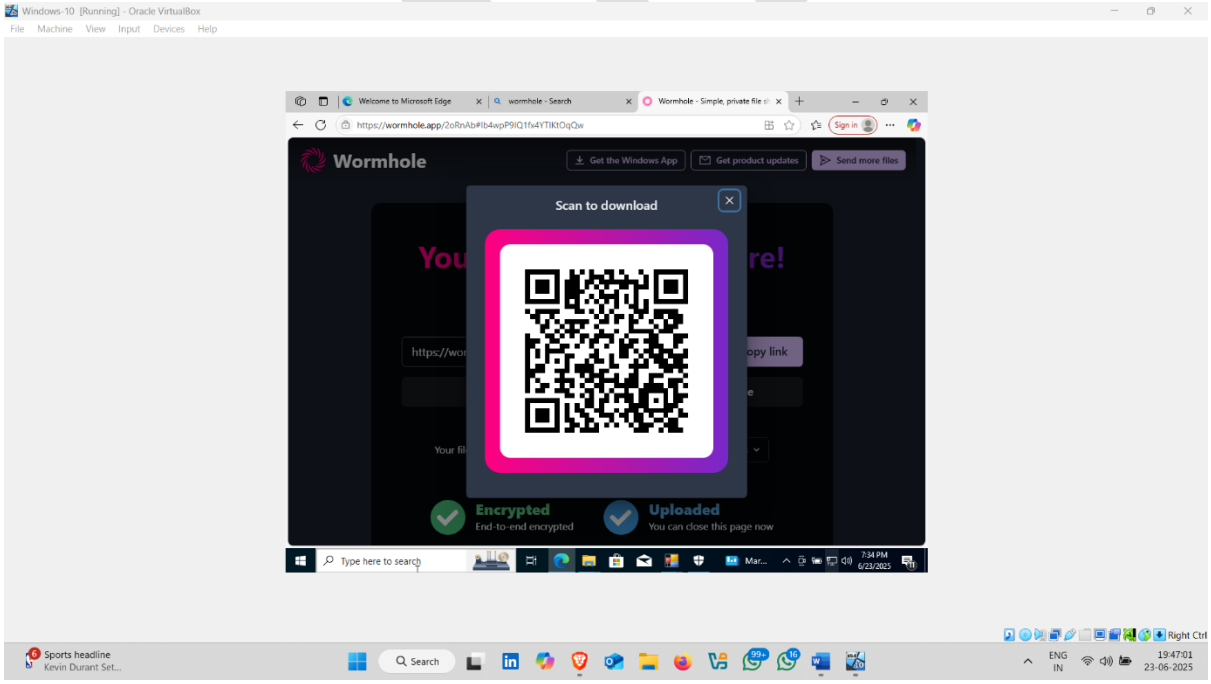
- Now **select application** and then click on **open**



- Here , its many way to share application to victim

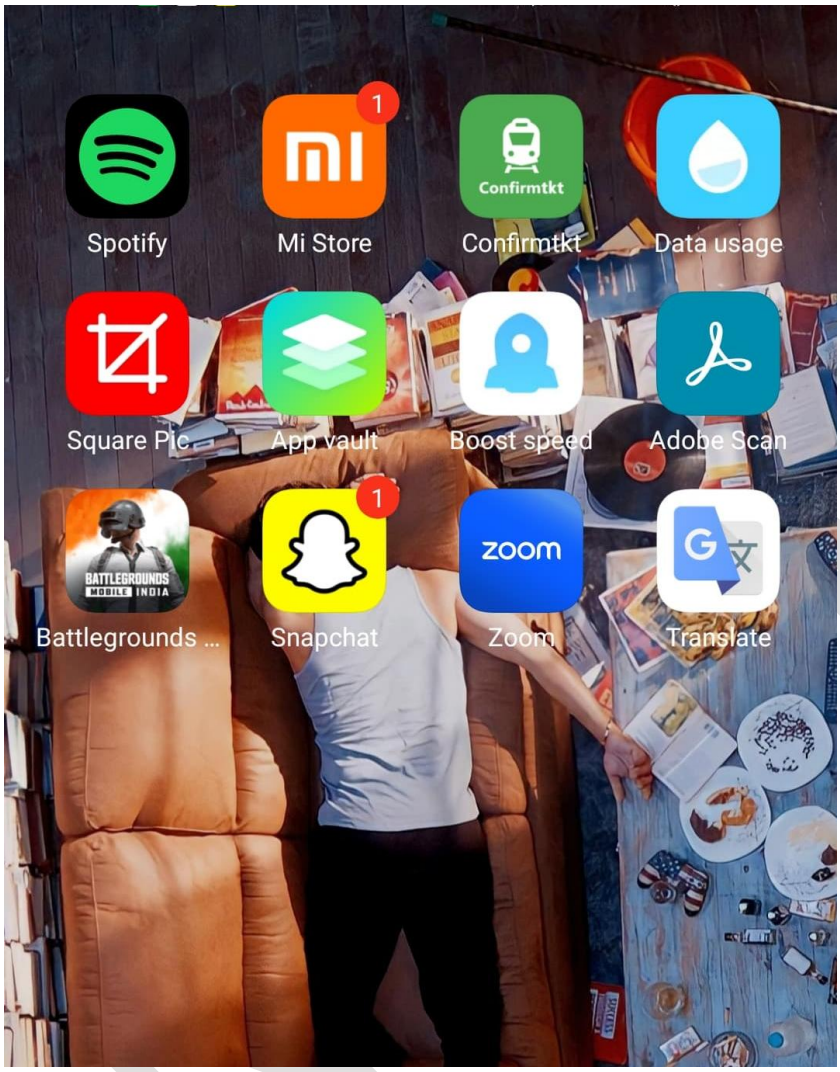


- **QR Code**

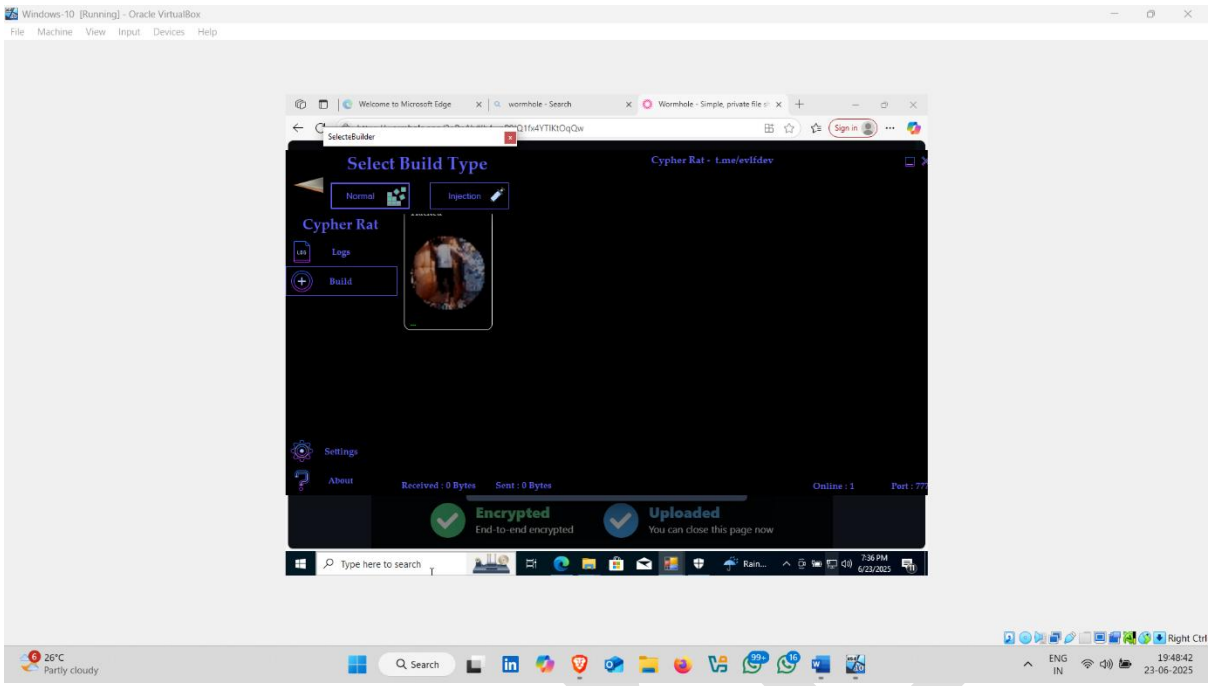


- **Started installing 👇**

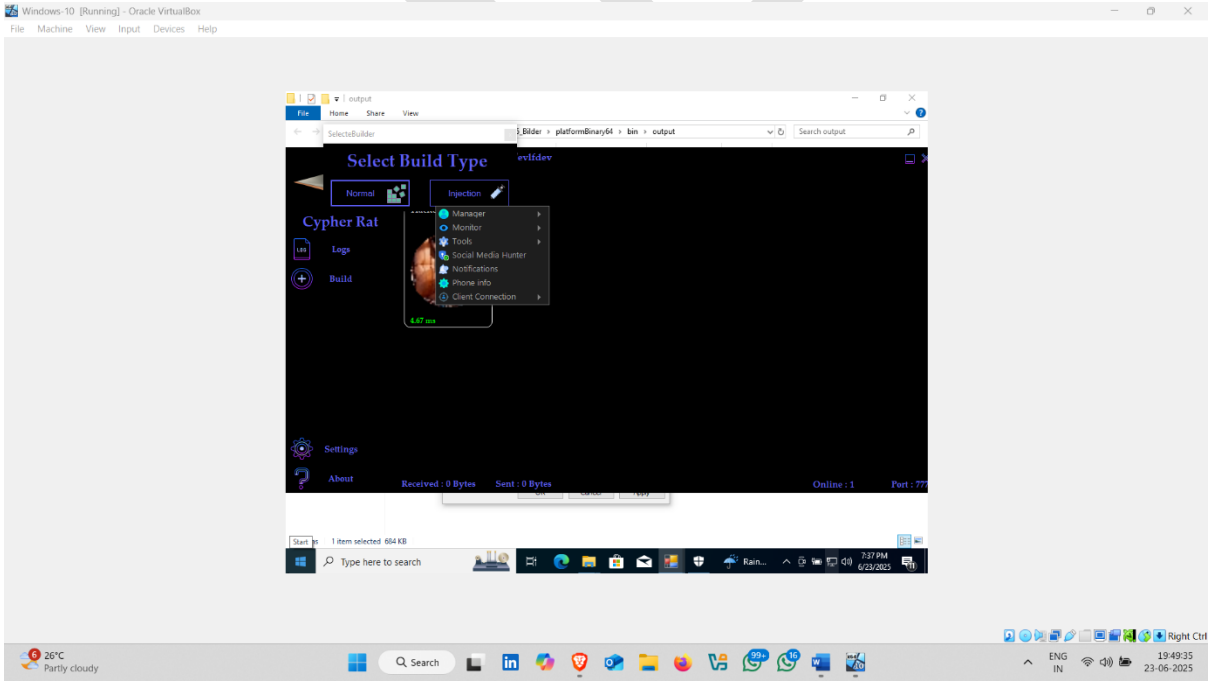
- Google Translate👇✅



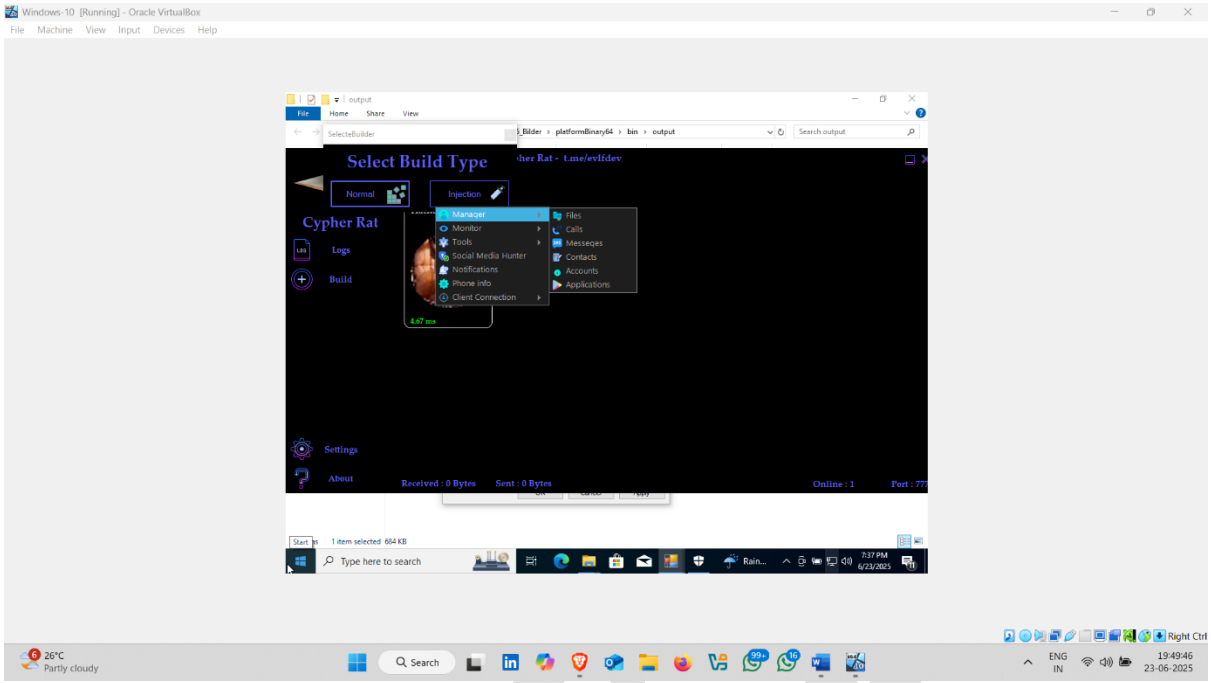
- Gaining Access ✅ 👇



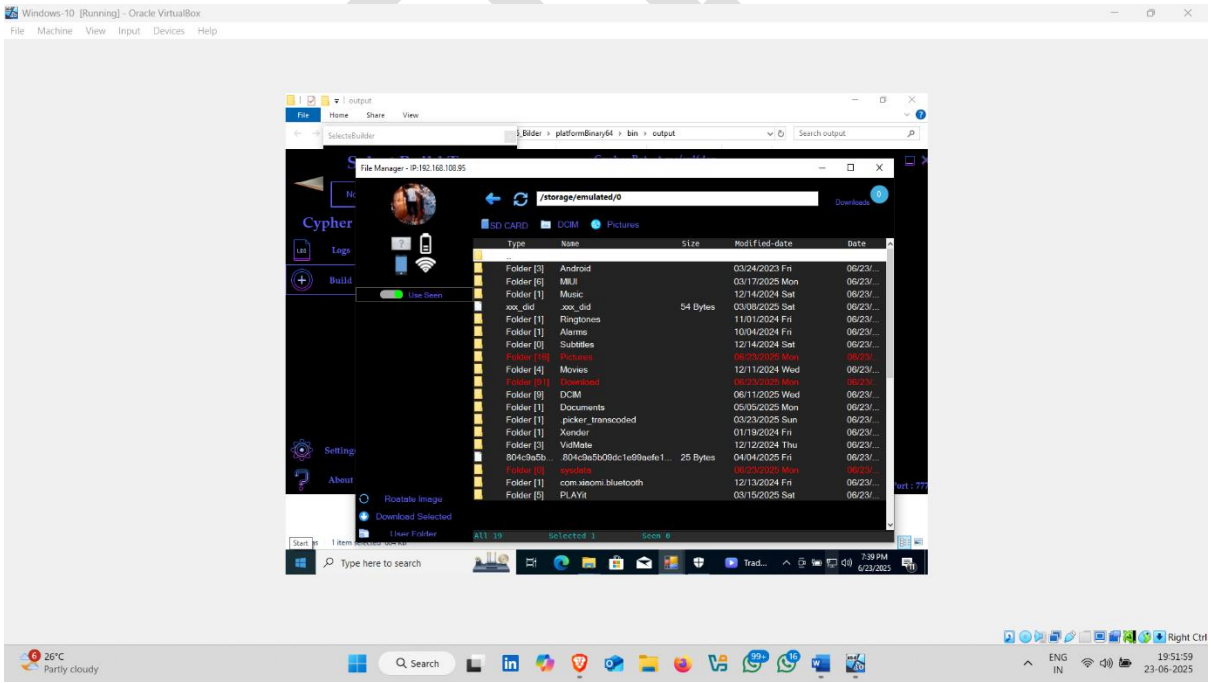
- **Now Click on device , options are appear**



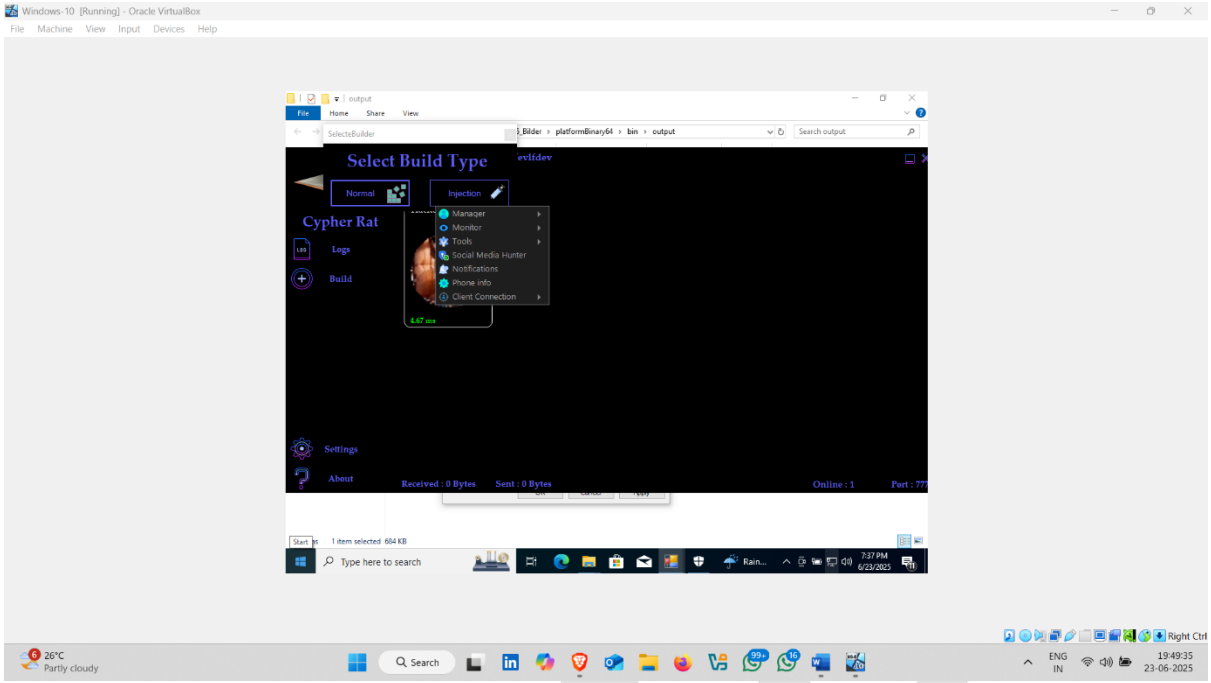
- Now click on **manager and then Files** – to view all files/folder on victims device



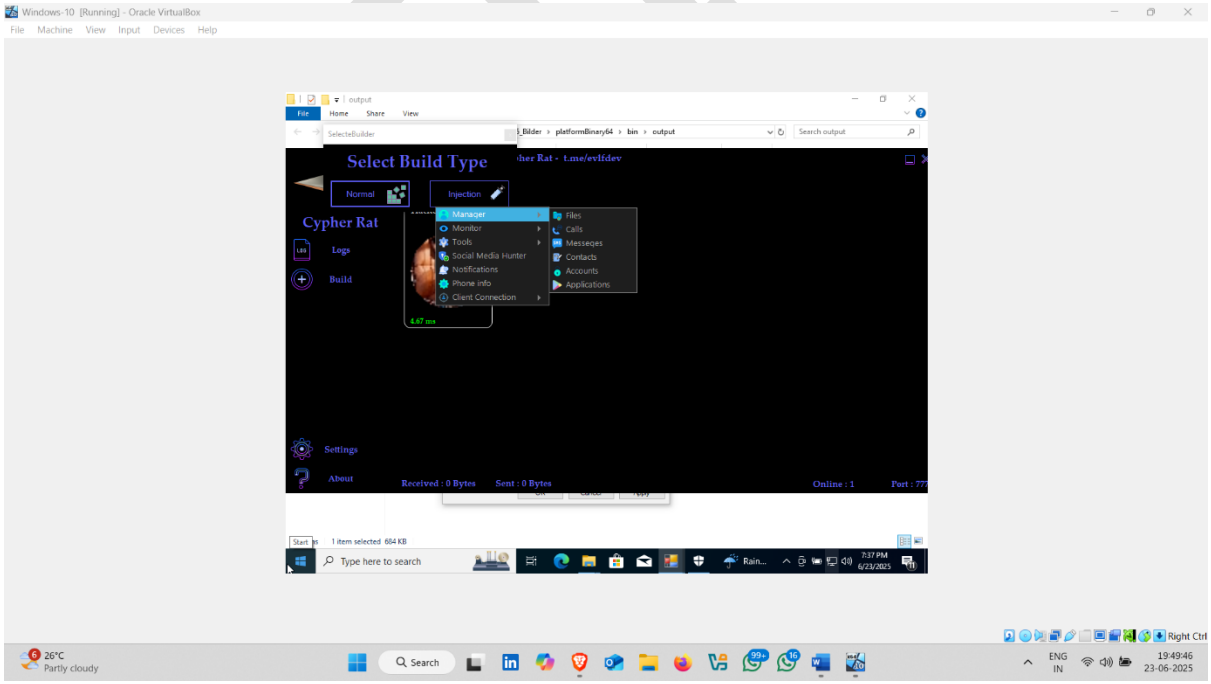
- **All files and folder** 👇✅



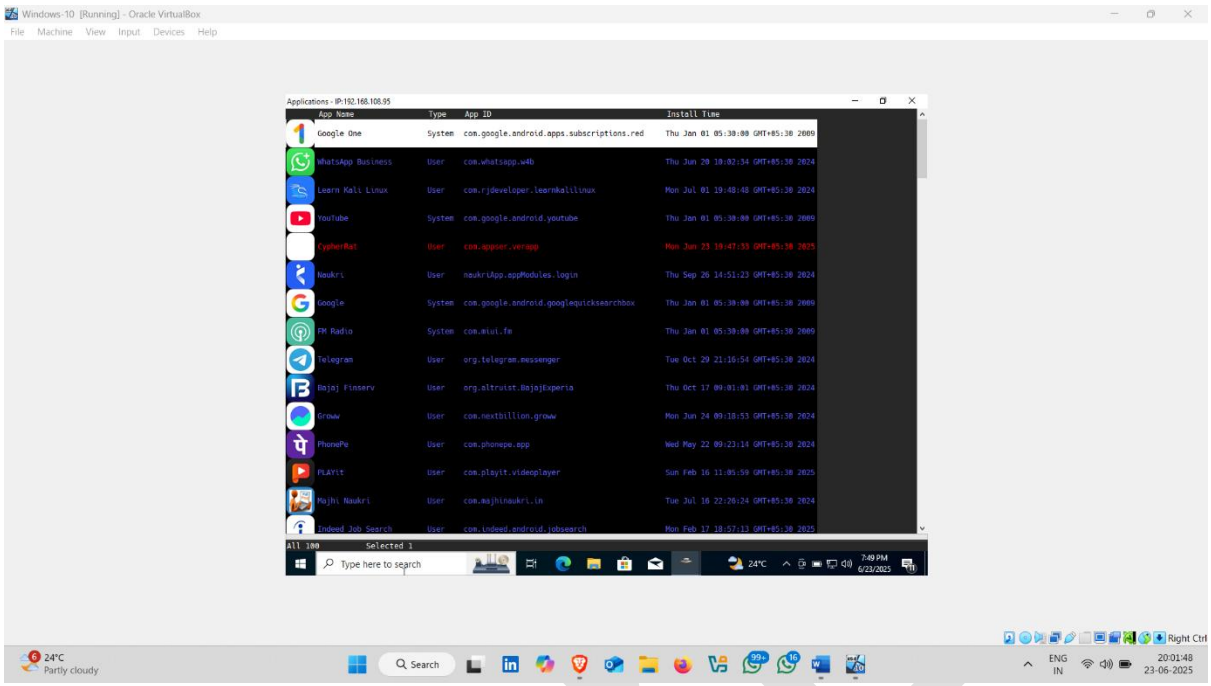
- **Now , once again click on manager**



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



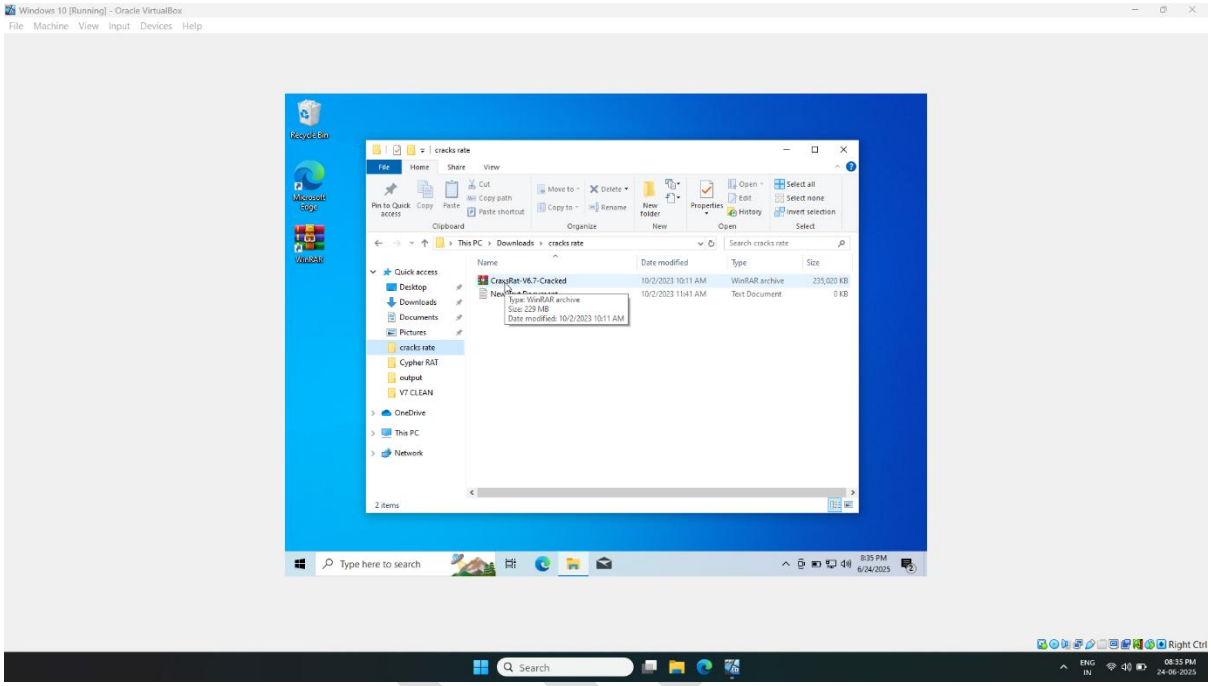
- **Installed apps ✅ 👇**



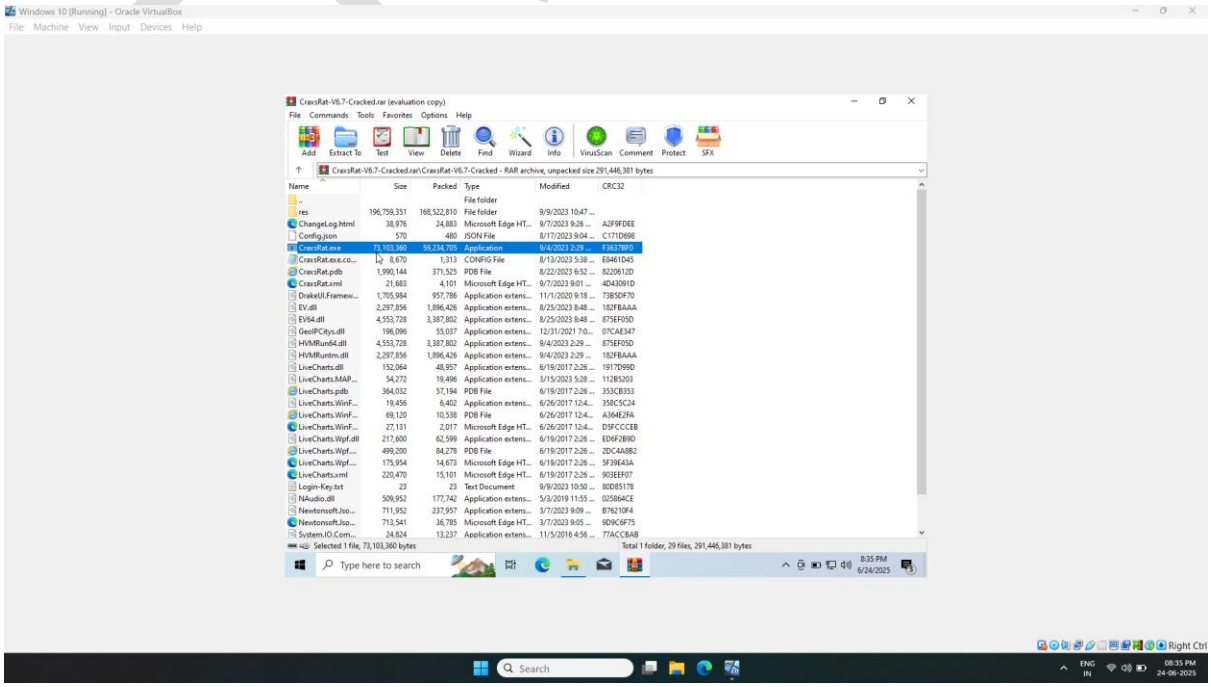
2.Android Hacking Using Craxs RAT

How to use it -:

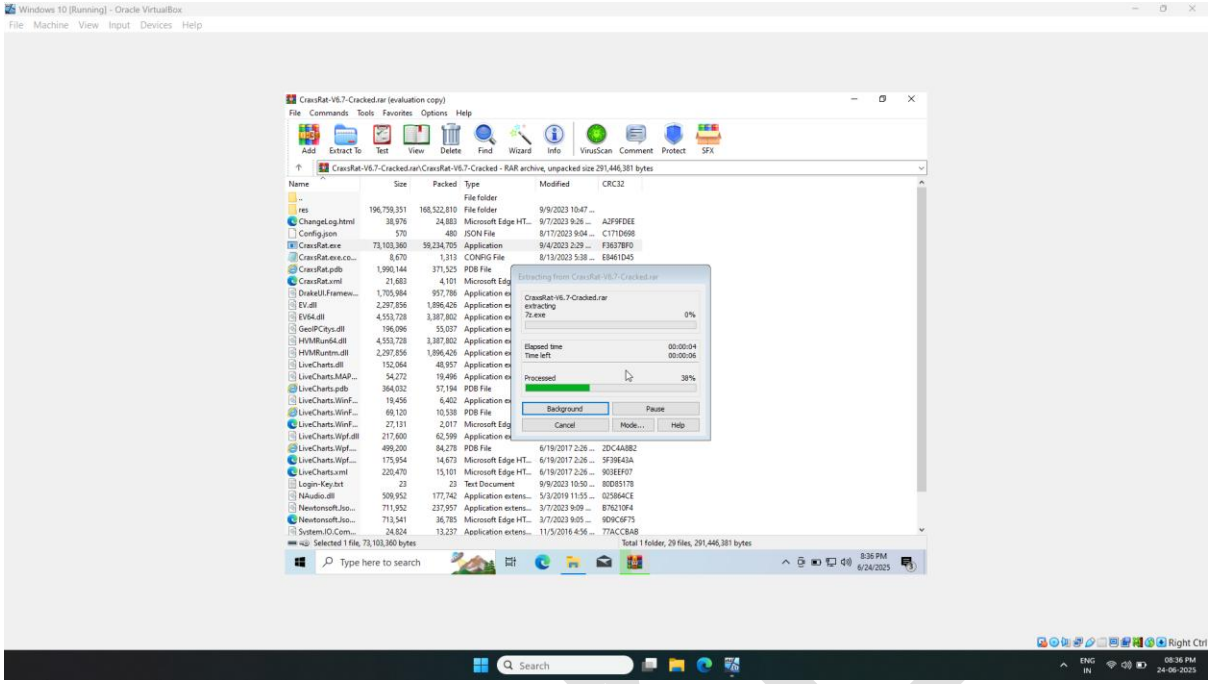
- Open Craxs RAT rar File



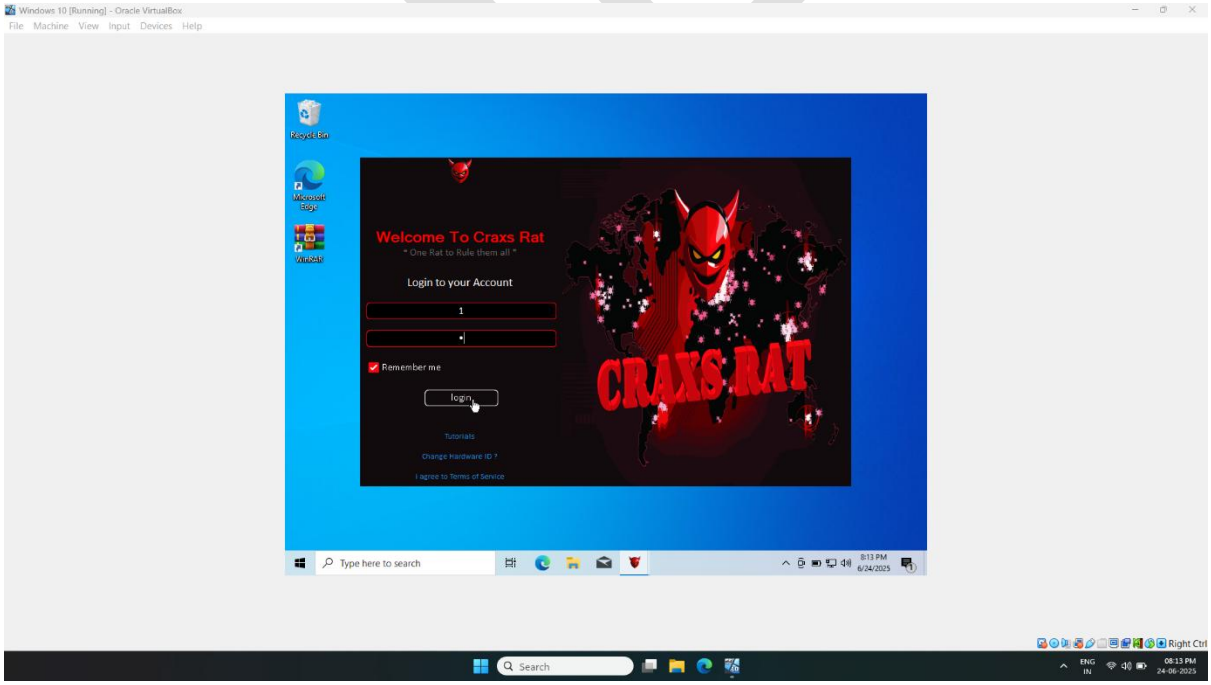
- **Run This .exe File**



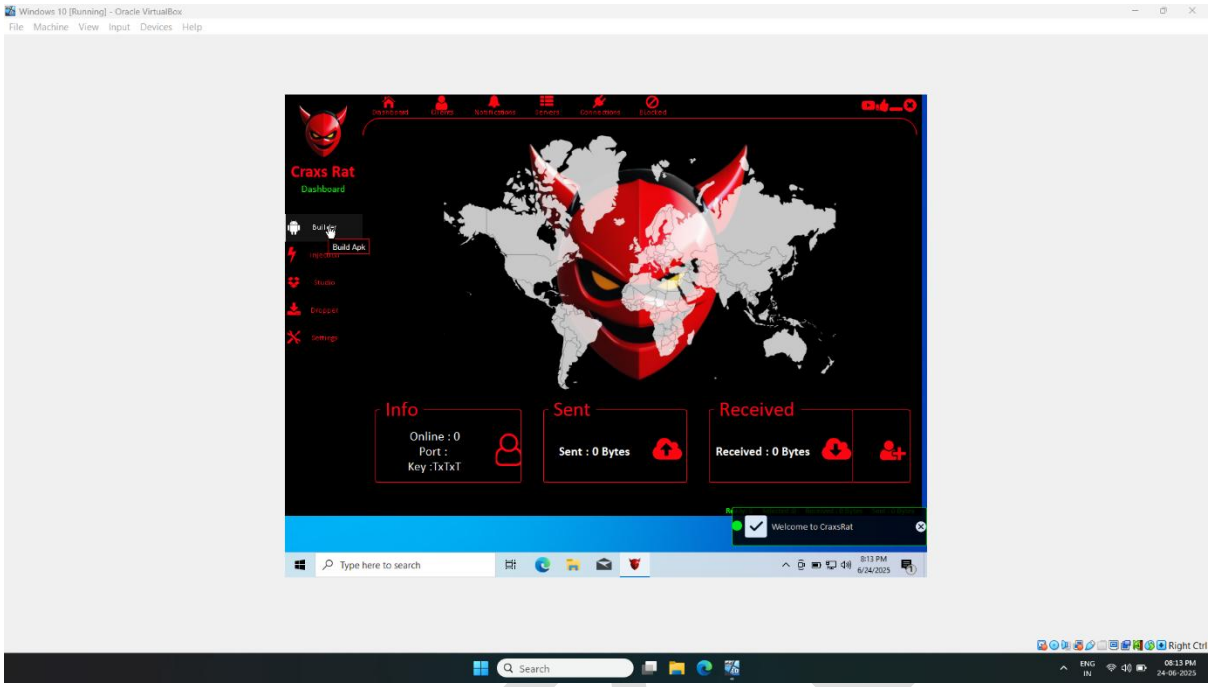
- 👇



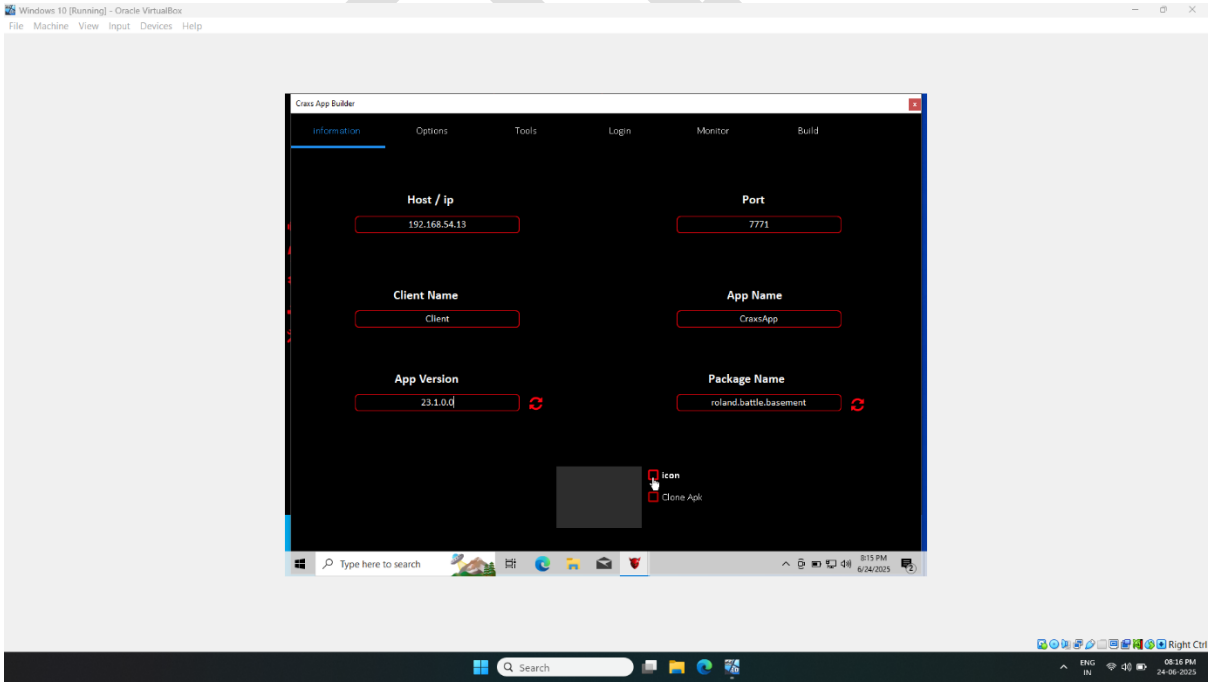
- Type 1 on both username and password and then click on login



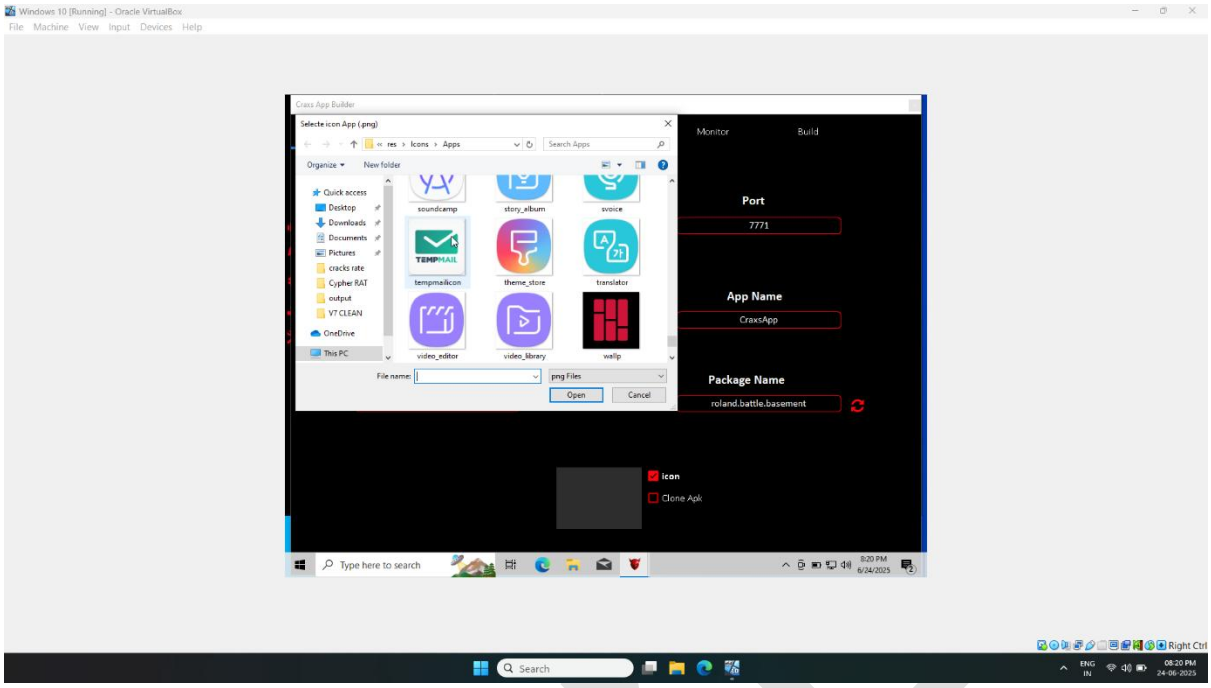
- Craxs Rat Interface 👇 ✅
- Click on **Builder**



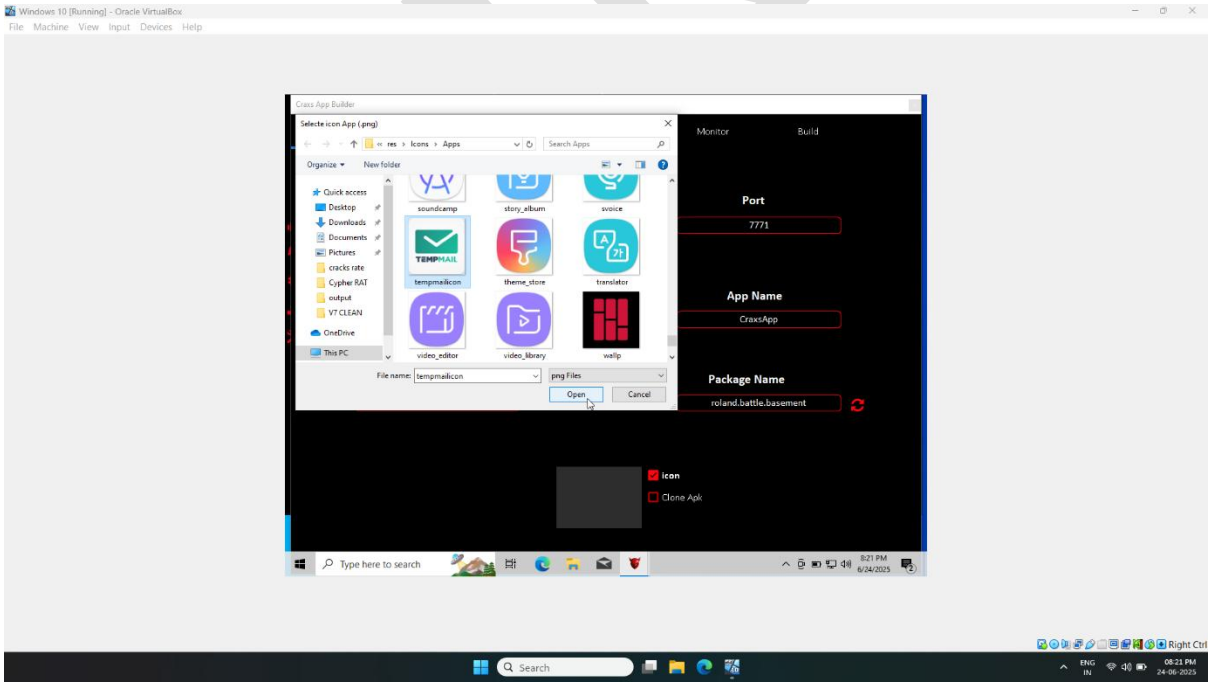
- Now set your ip address and select icon checkbox



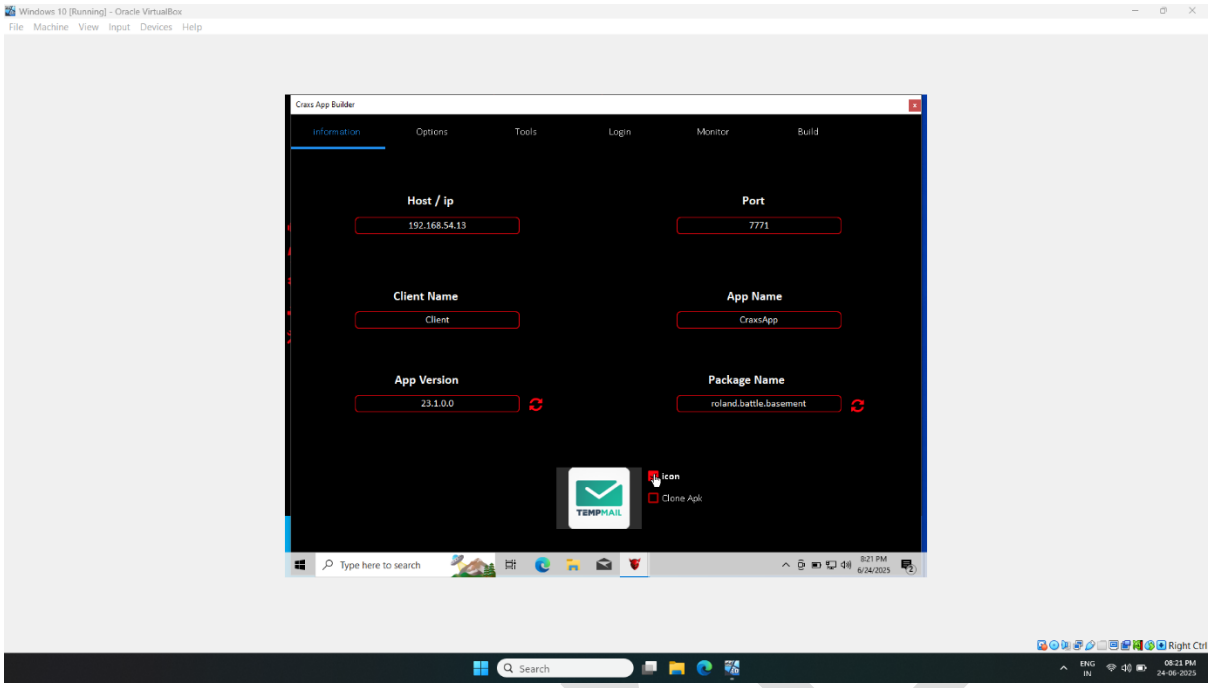
- Select Image for your application



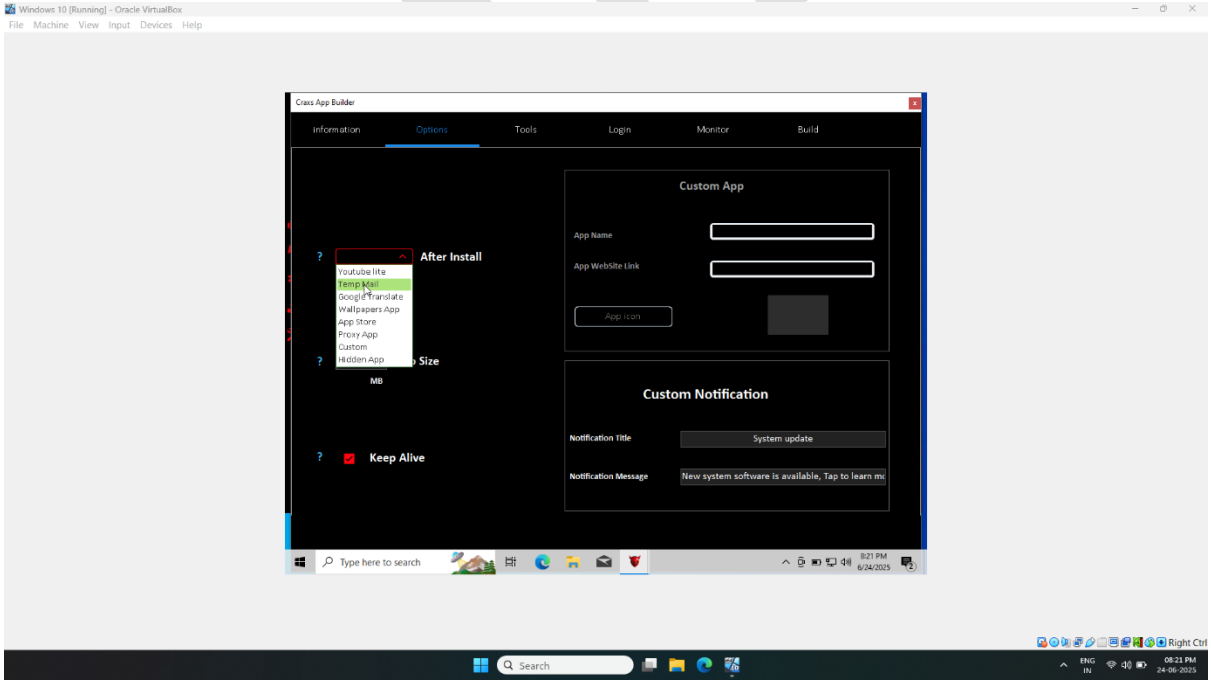
- Icon Selected , now click on **open**



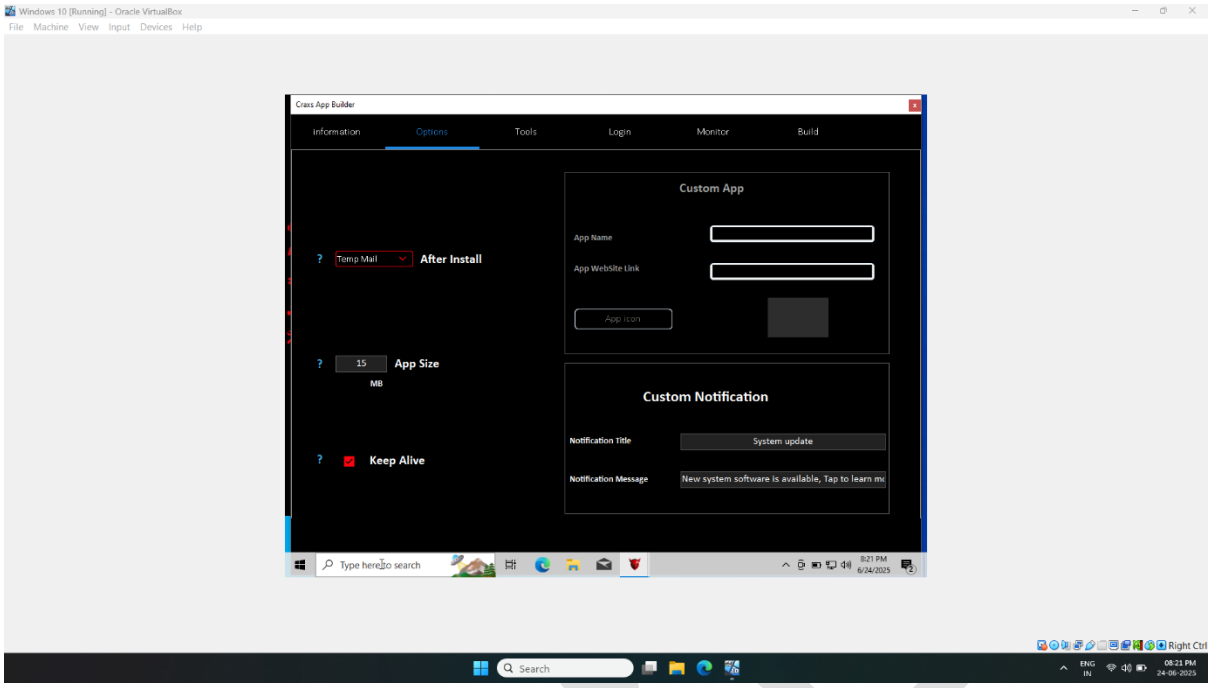
- Now click on **options** tab



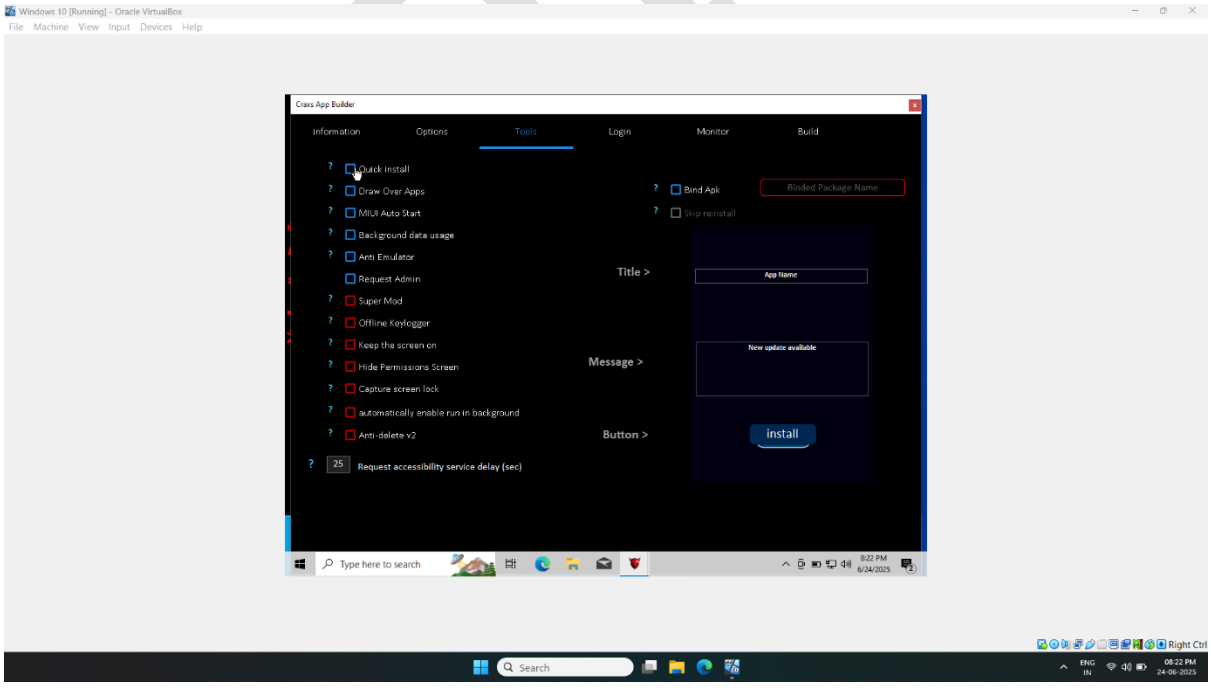
- Select application name after installed on target device



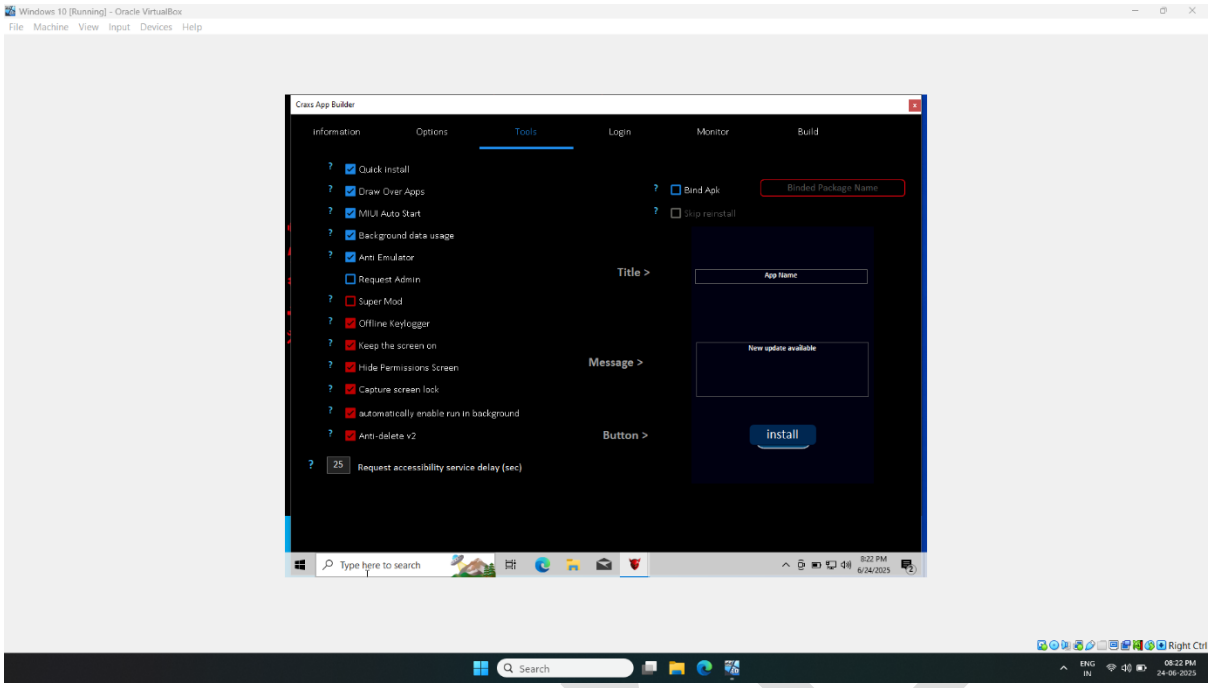
- Name selected and then click on **tools** tab



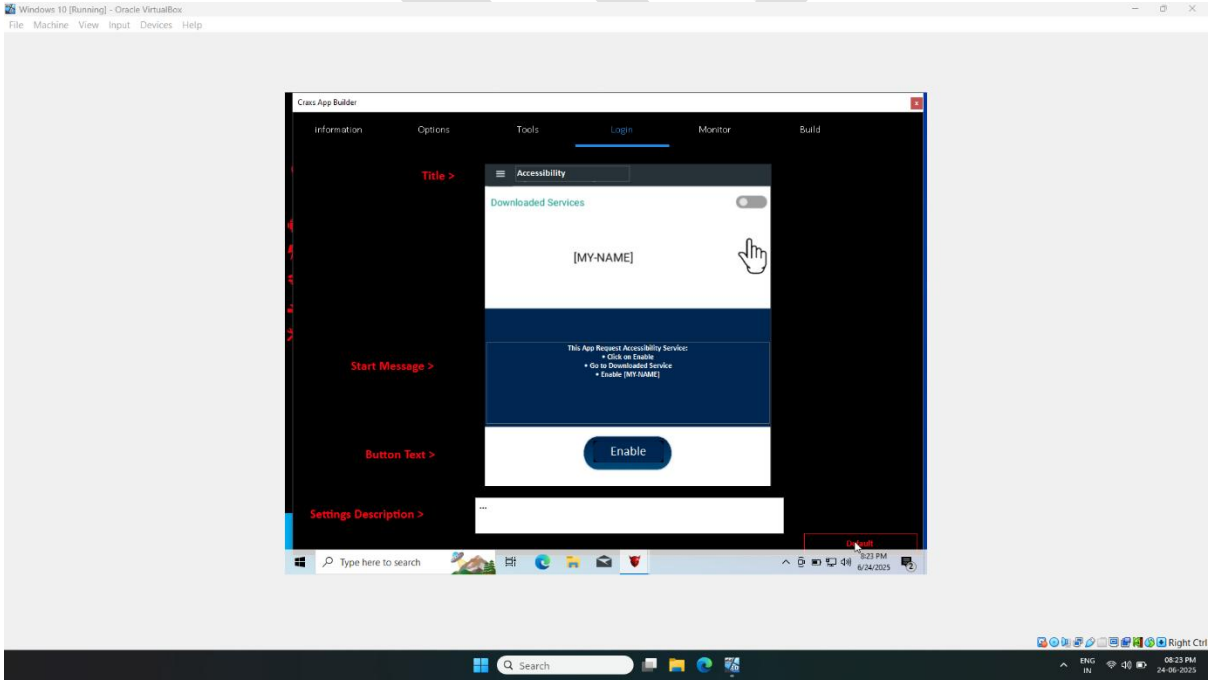
- Now select checkboxes for what access you want on target device



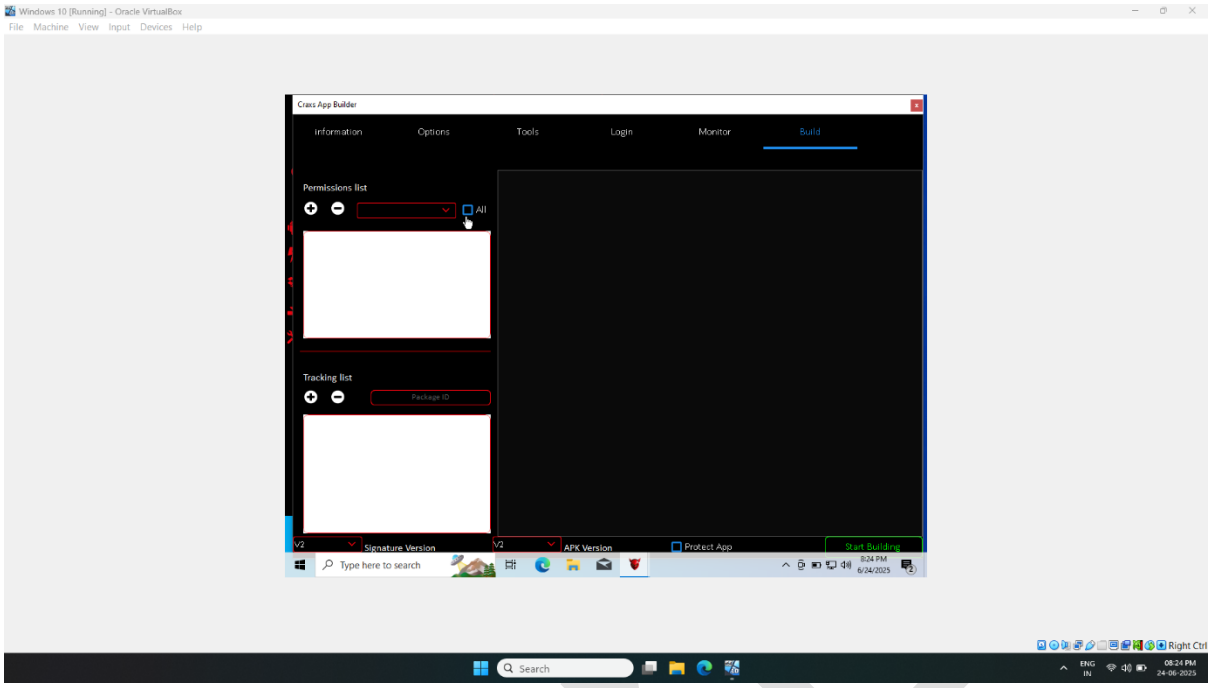
- All set now click on **login** tab



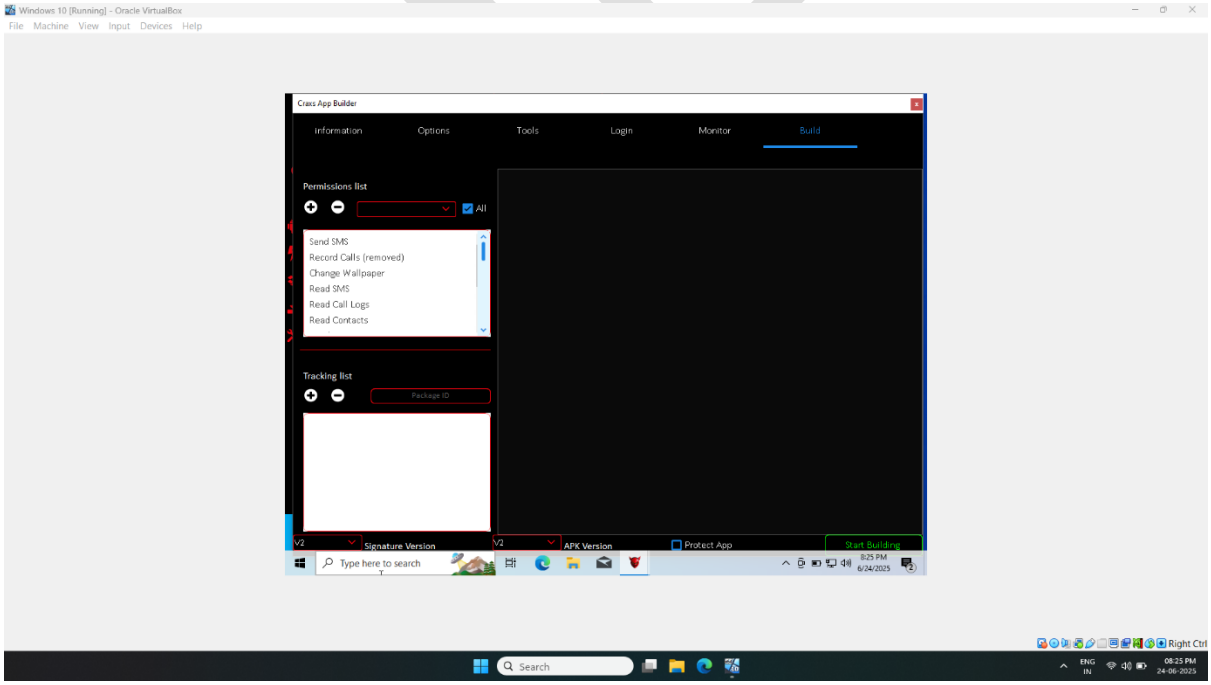
- Click on **Enable**



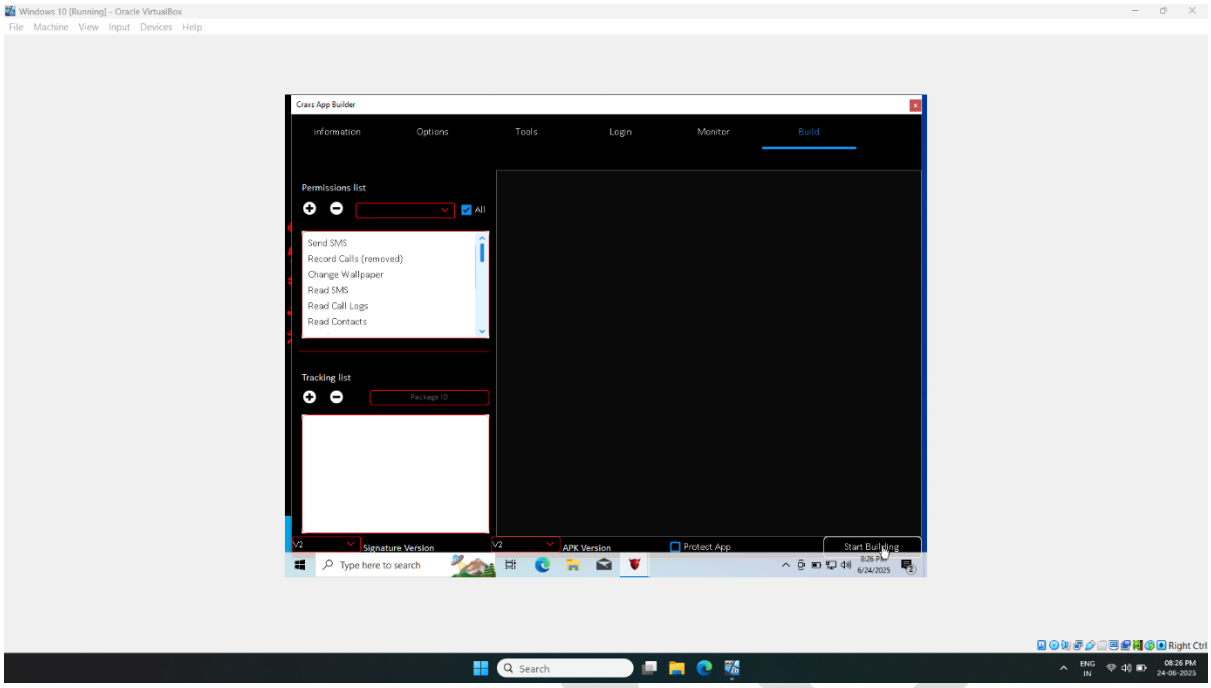
- Now click on **build** tab and then click checkbox "**all**"



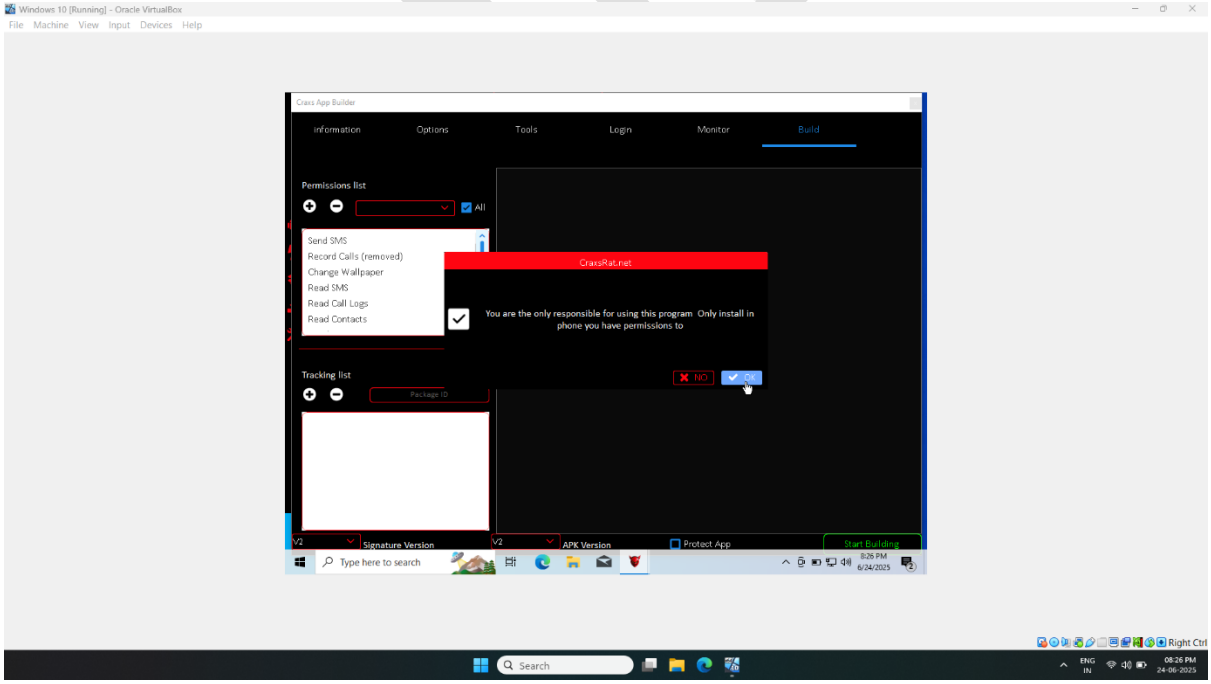
- All set ✅ 👇



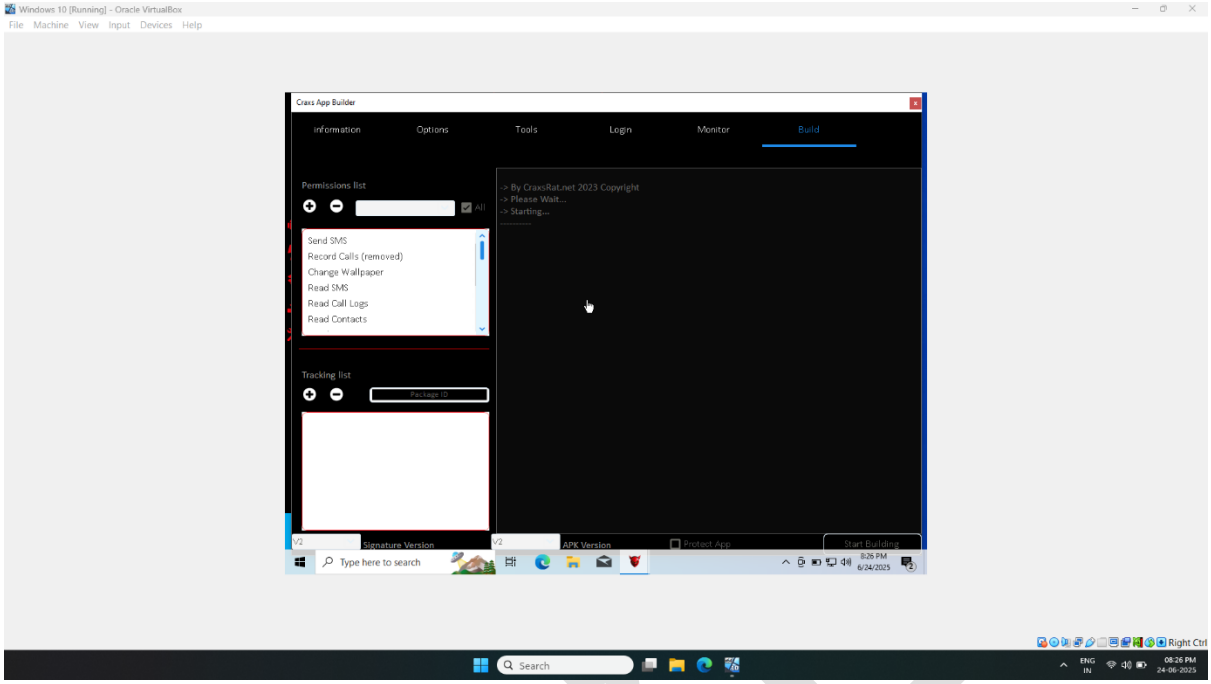
- Click on **start Building**



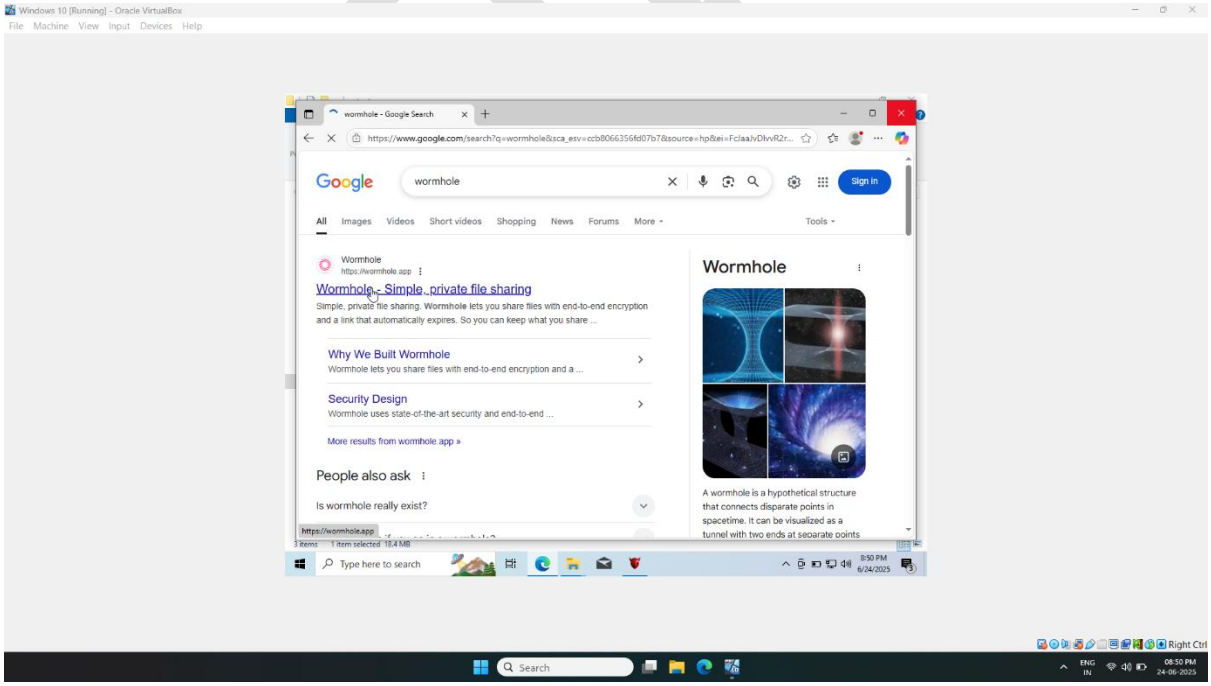
- Click on **ok**



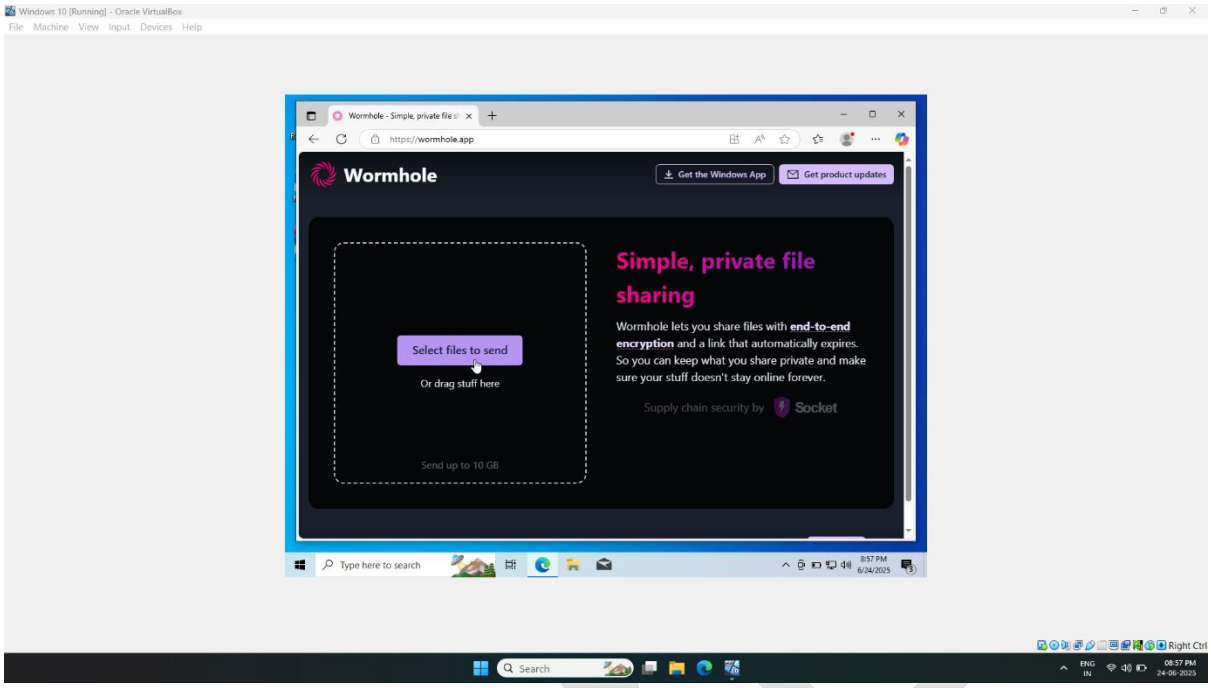
- Started Building Application 👇 ✅



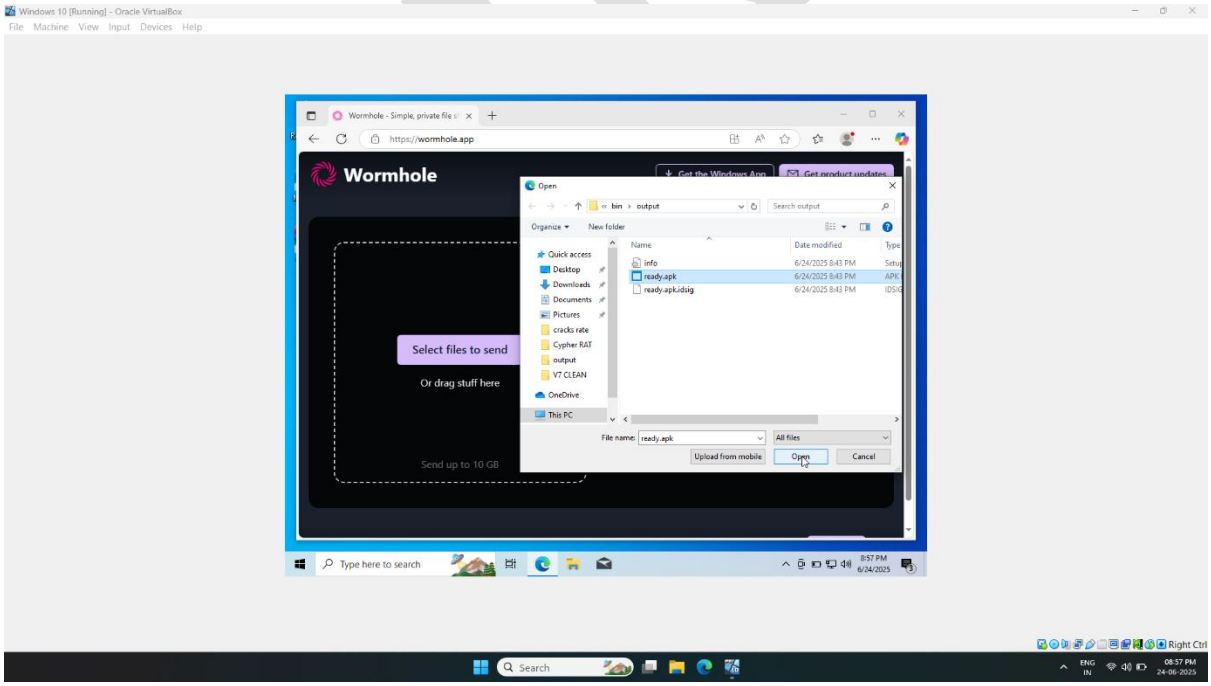
- Now open browser , search wormhole website
- Open First Website



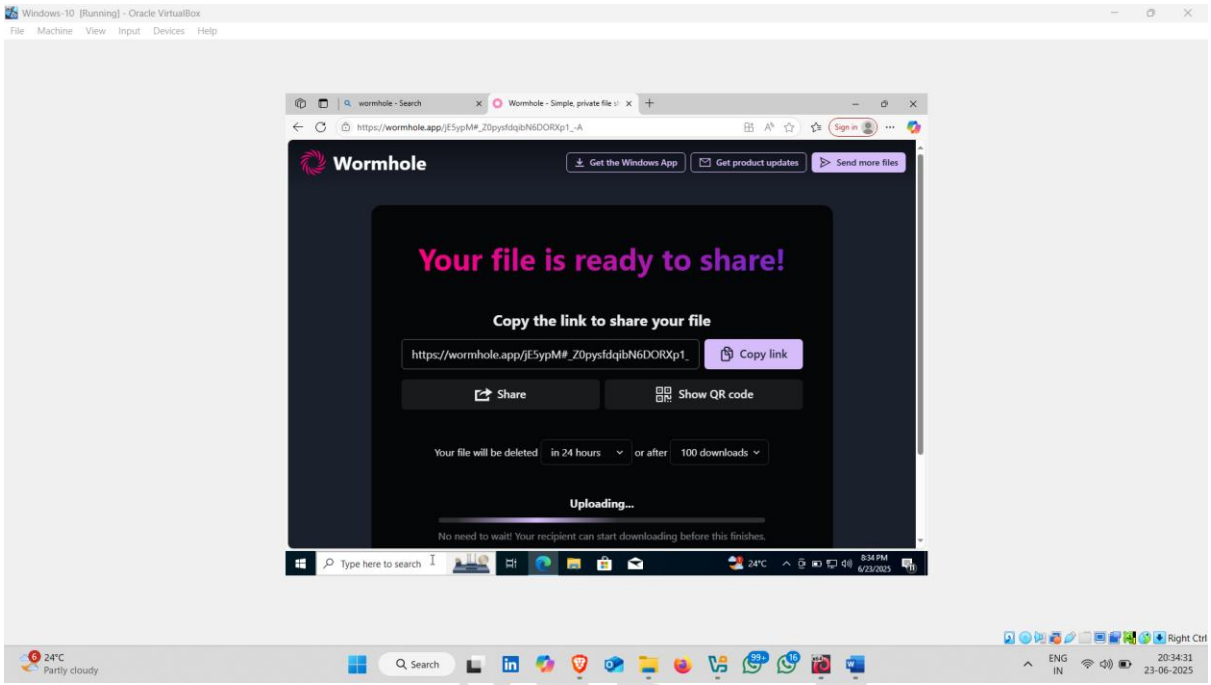
- Click on **select Files to send**



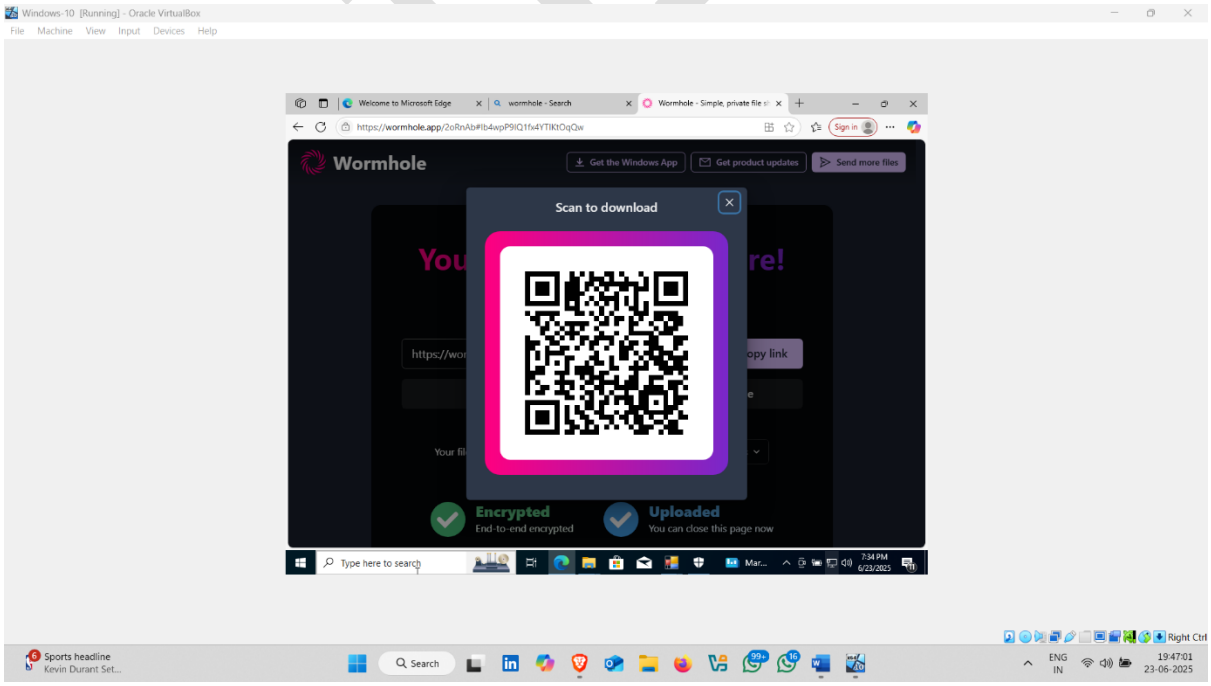
- Select apk file and click on open



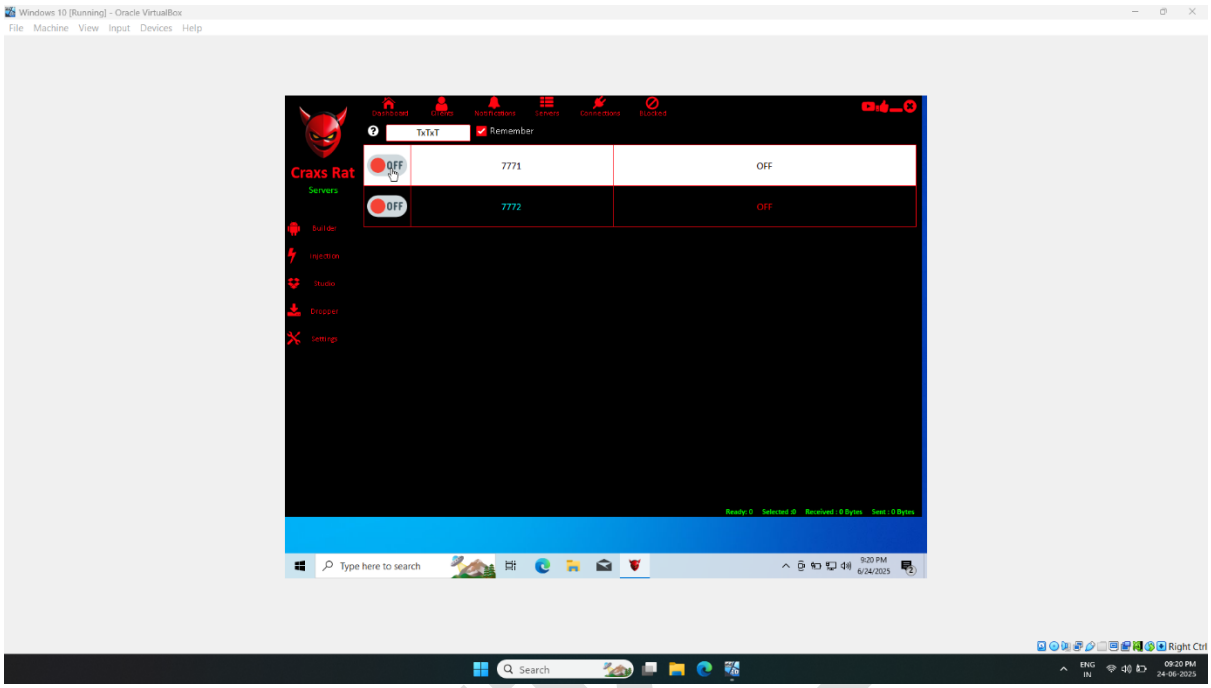
- Link created ✅ 👇
- Now you can share link or qr code to the target to download our malicious apk file



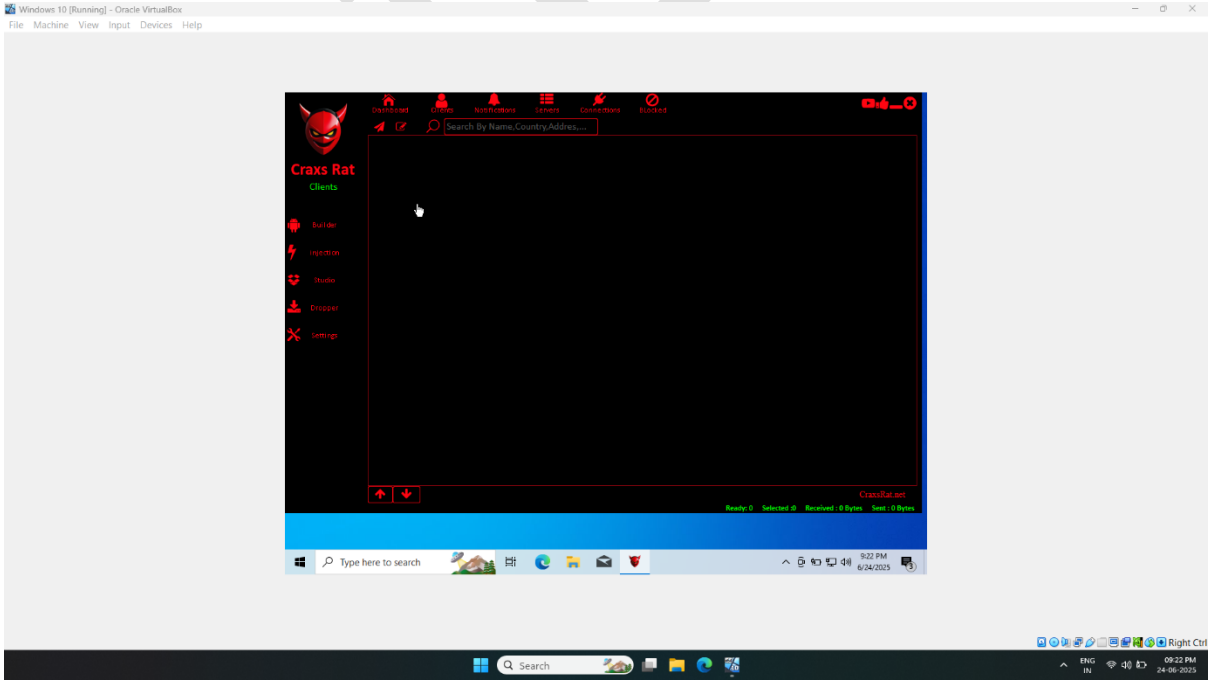
- QR Code



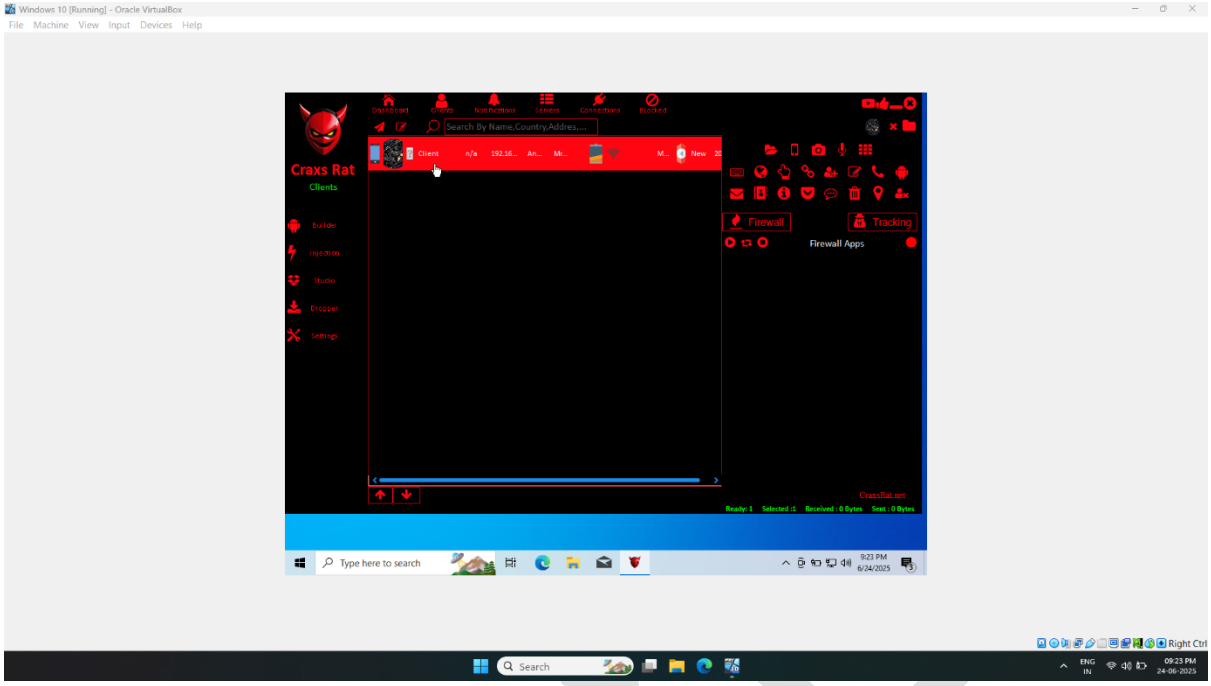
- After installation and permission given on the target application back to craxs RAT
- **Turn on listener port**



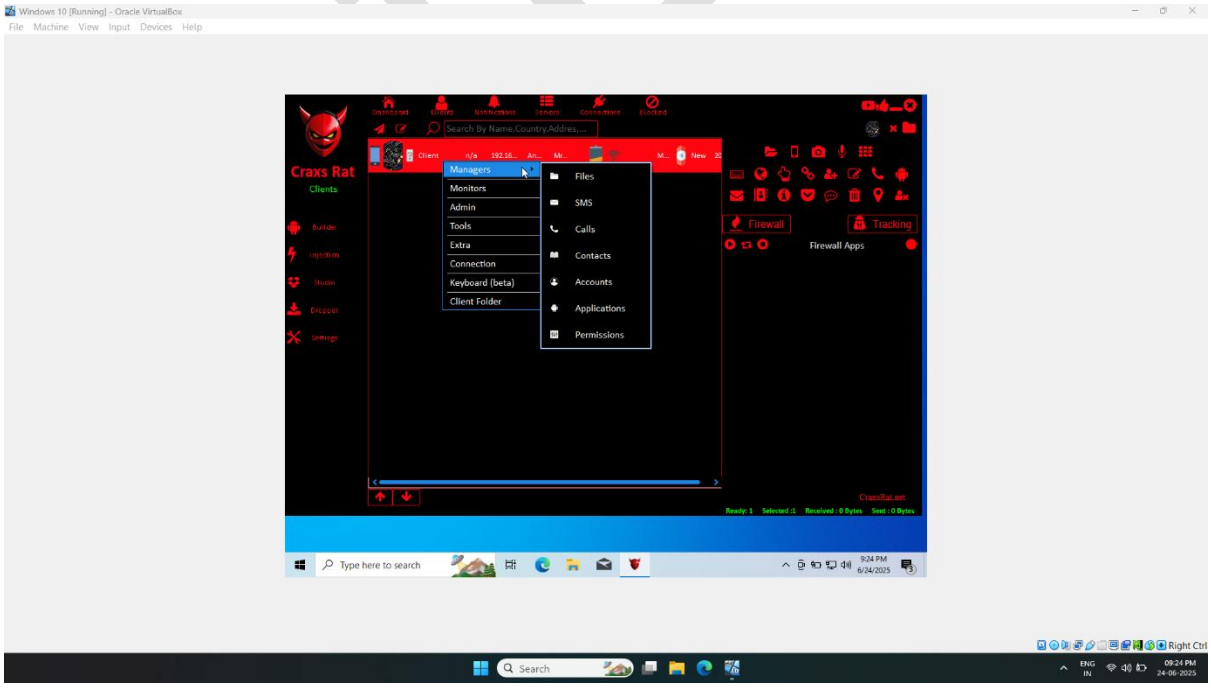
- Wait for Connection



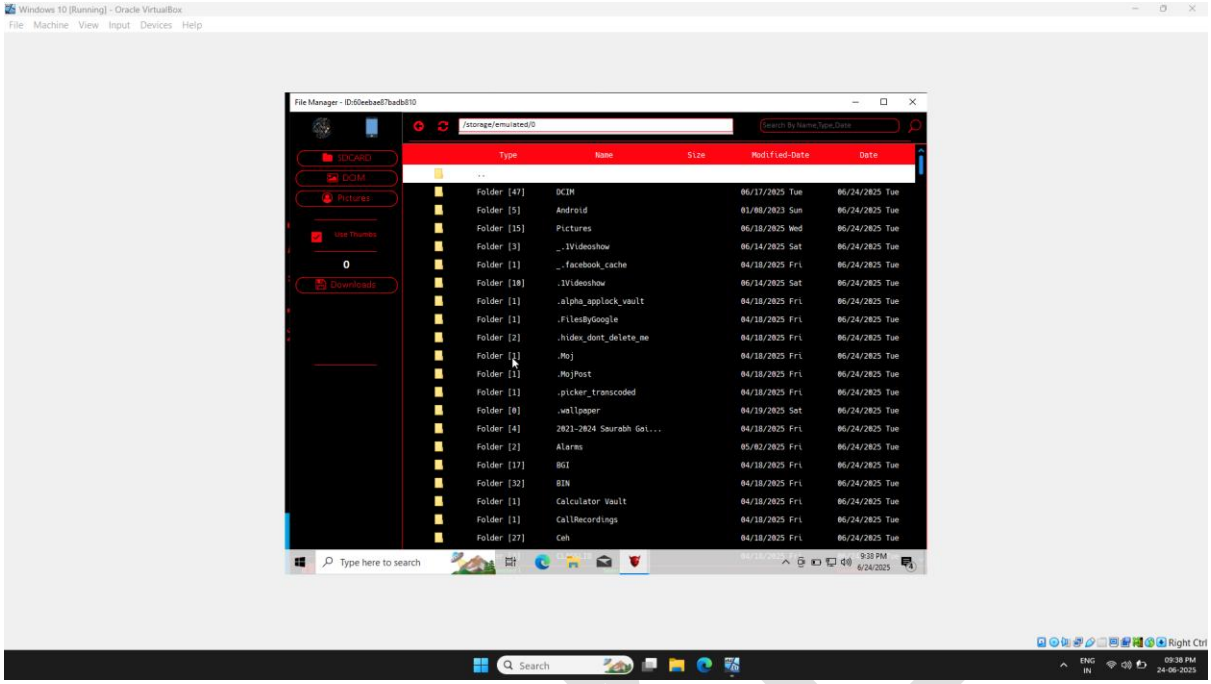
- Gaining access of target device



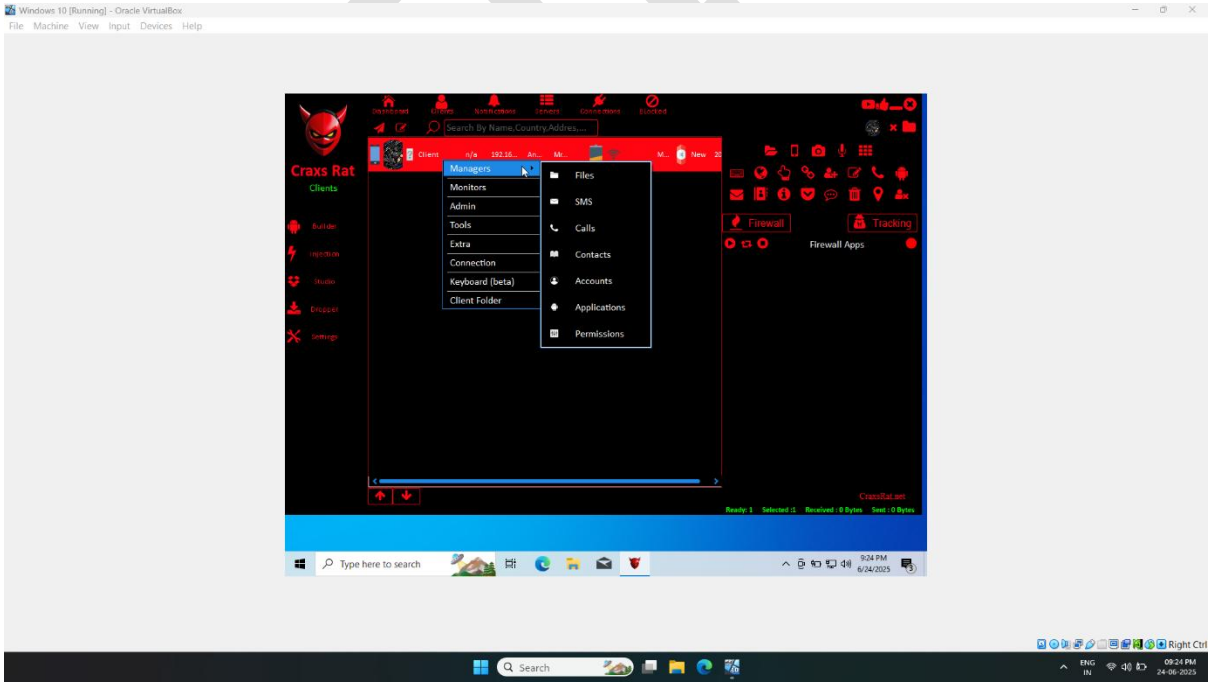
- **Now click on target device , list appear then click on managers and then click on files – to view files and folder on target device**



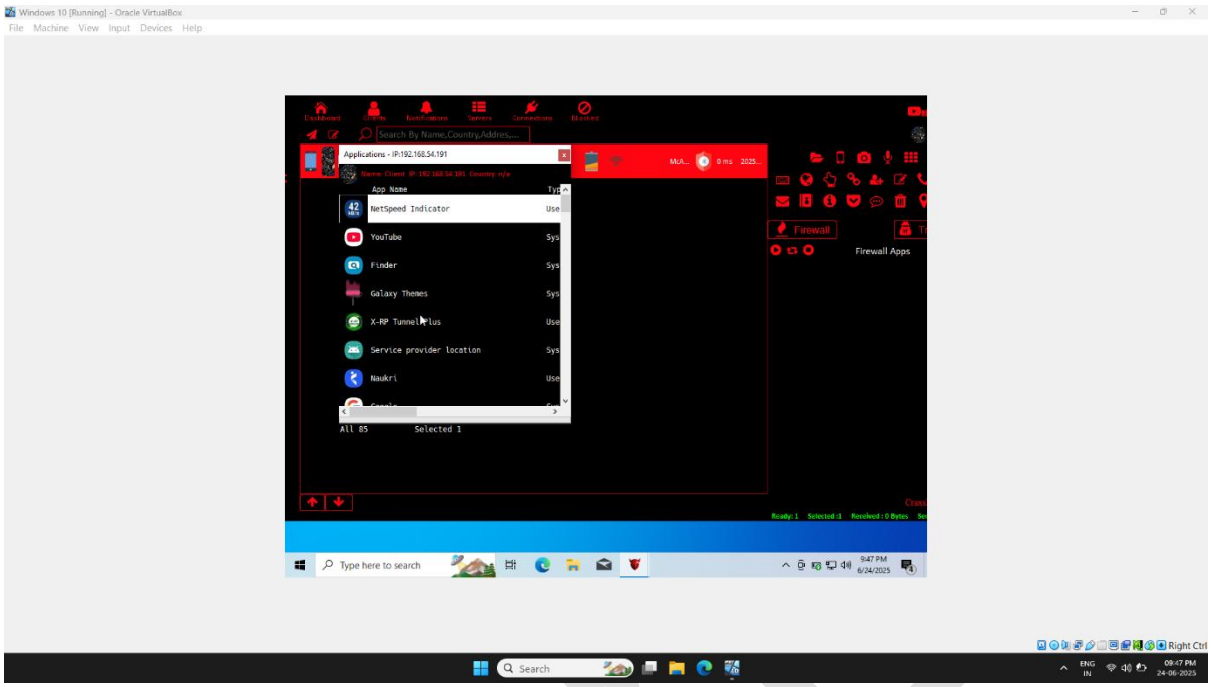
- Target device files and folders 👇 ✅



- **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):**

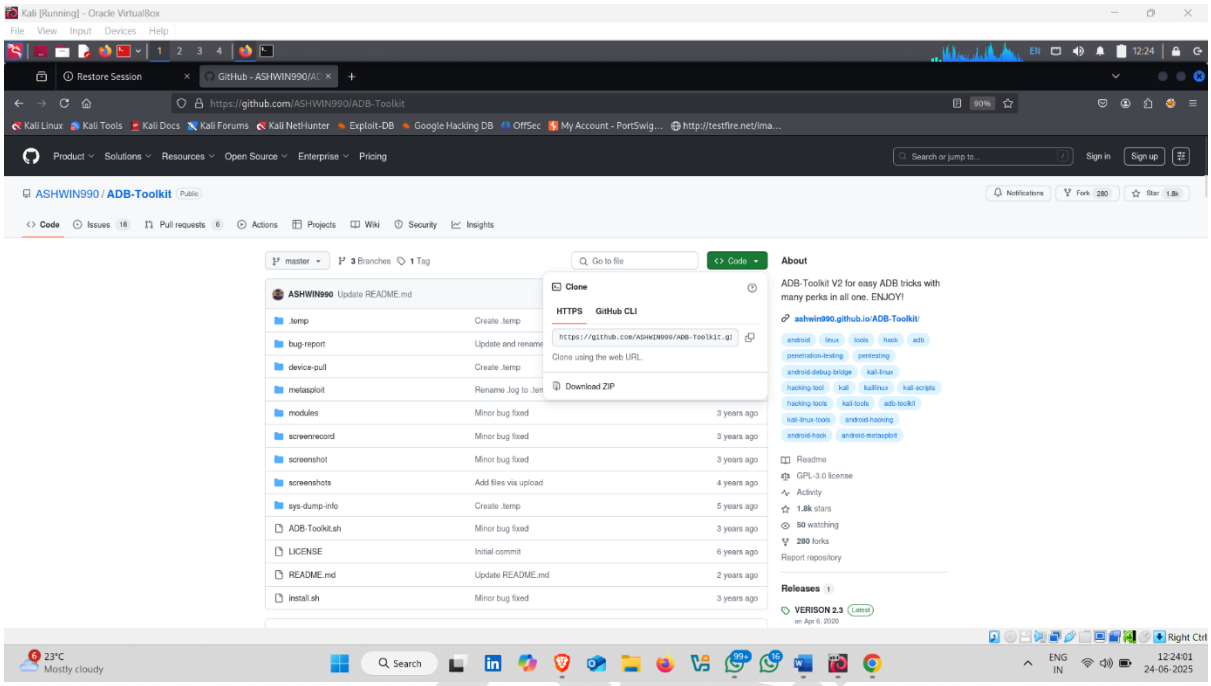
- **Kali Linux or any Linux OS**
- **ADB installed (sudo apt install adb)**
- **ADB-Toolkit installed**
- **USB cable for connection**
- **(Optional) Wireless ADB setup if targeting over network**

⚙️ **Software Requirements:**

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

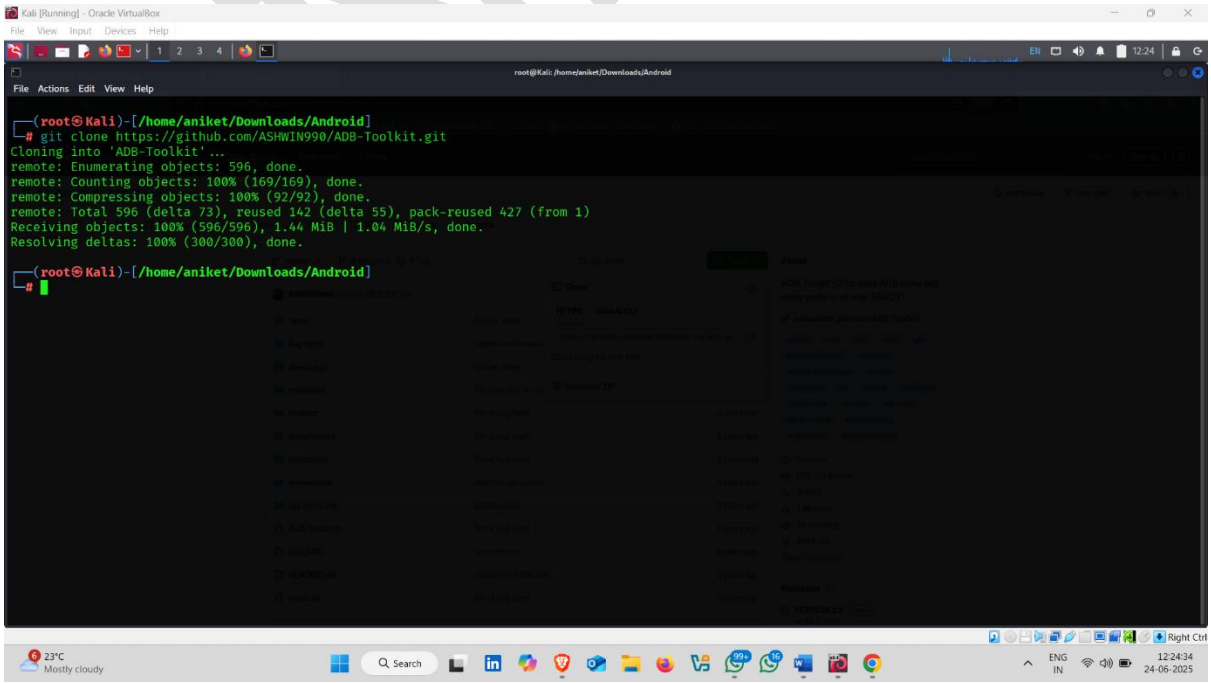
How to use it -:

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

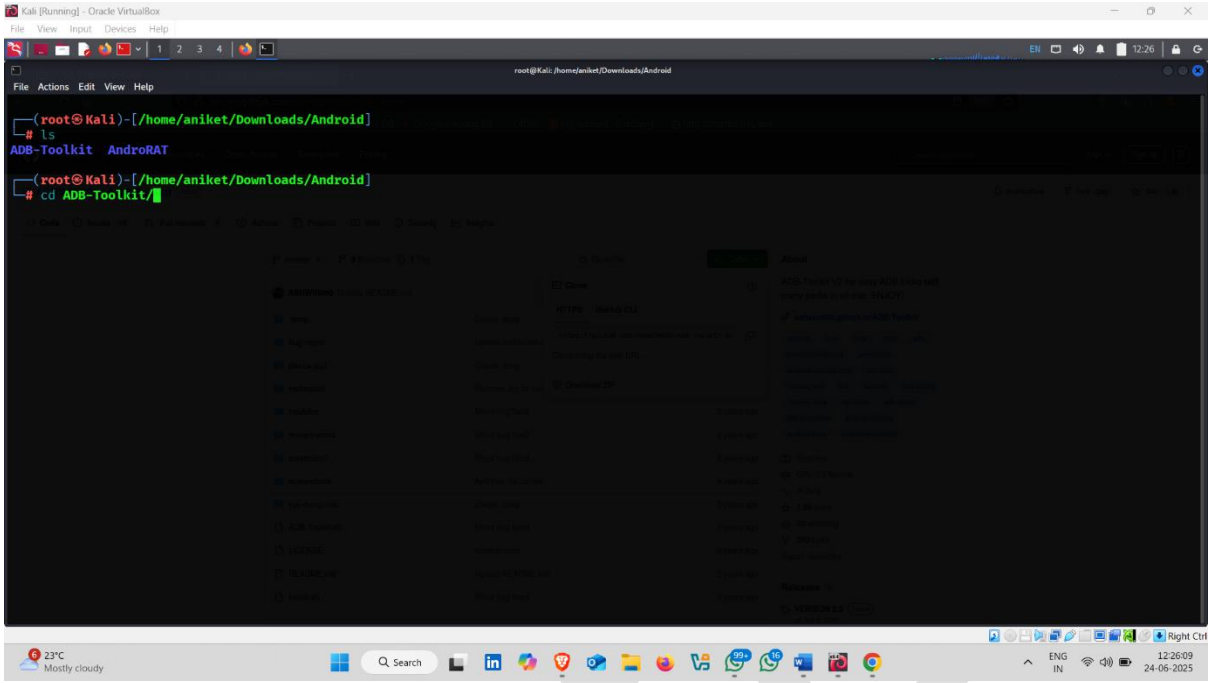


- Open Kali linux terminal and type following command

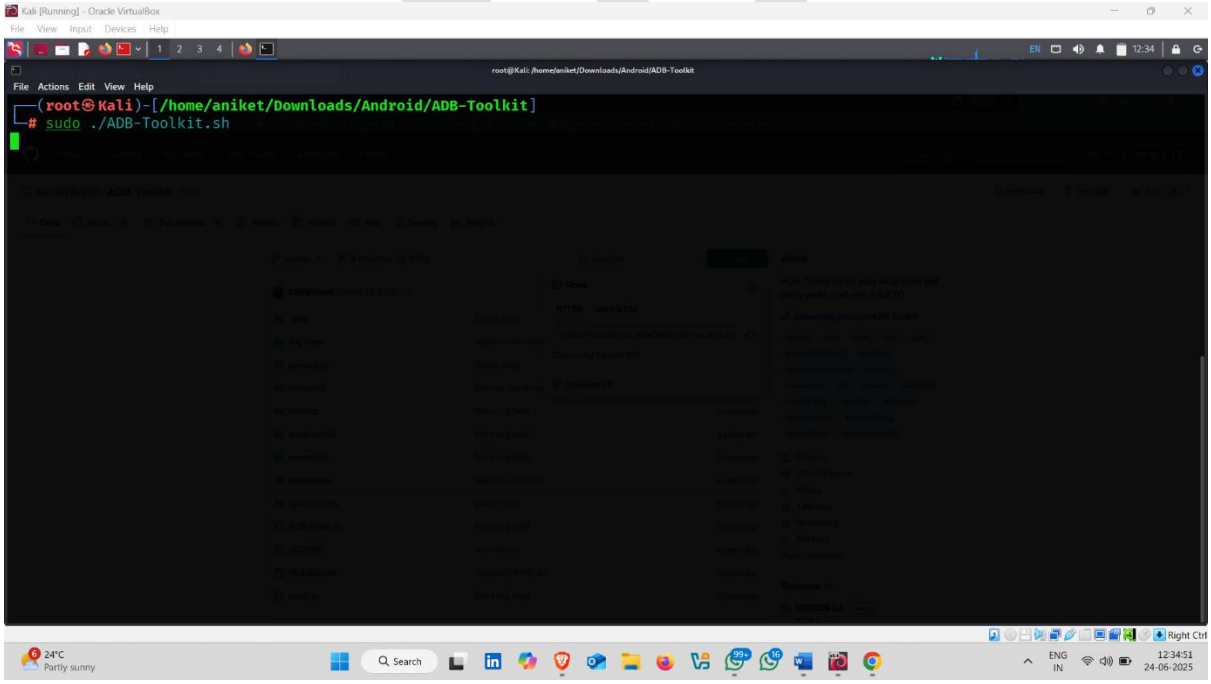
Command -: **Git clone < ADB-Tool-Kit URL>**



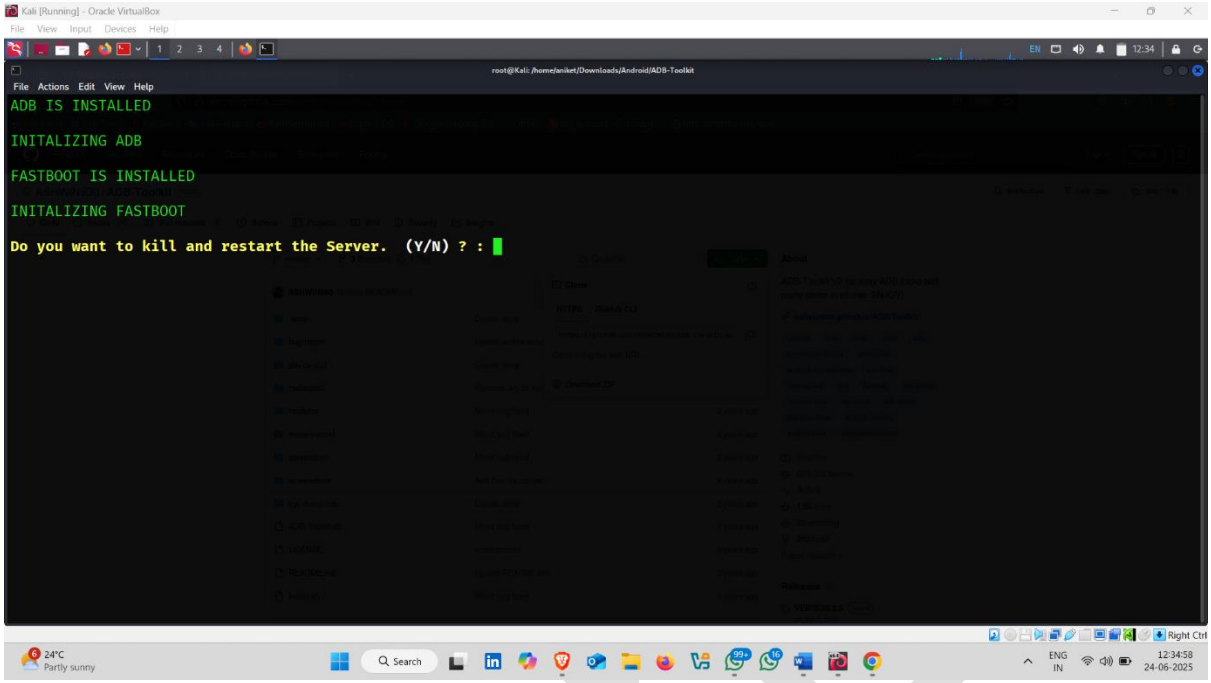
- **Now Go to ADB-Tool-Kit Directory**



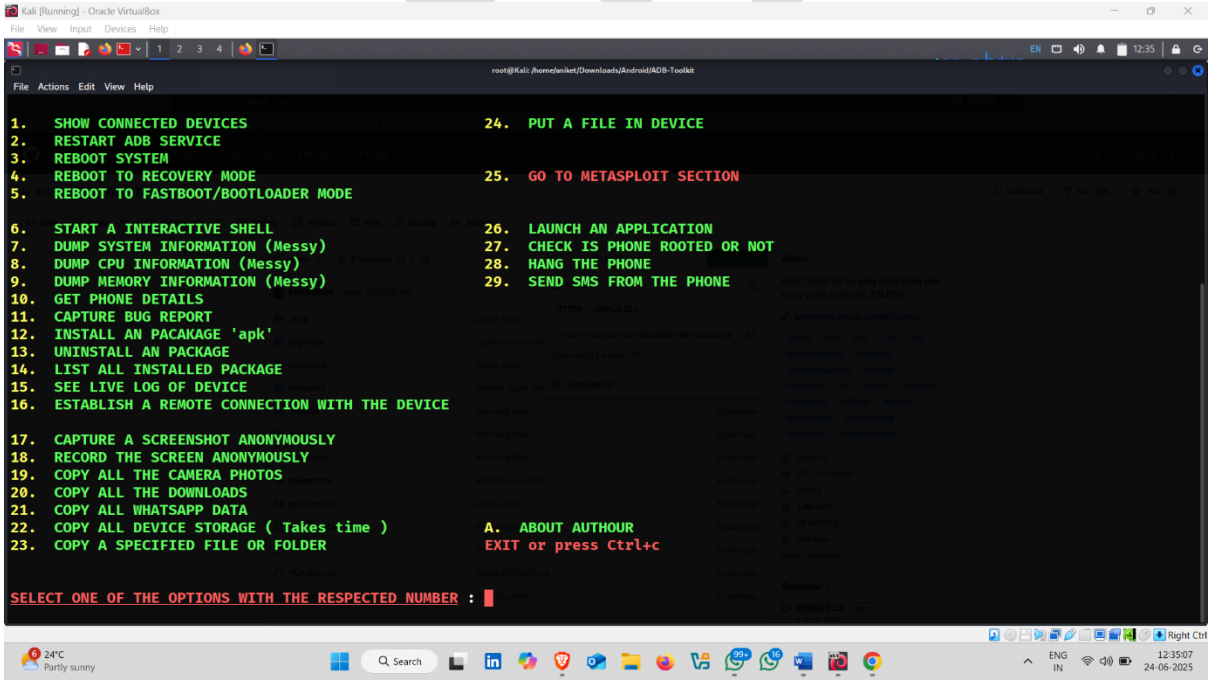
- Type following command to start ADB-Tool-Kit



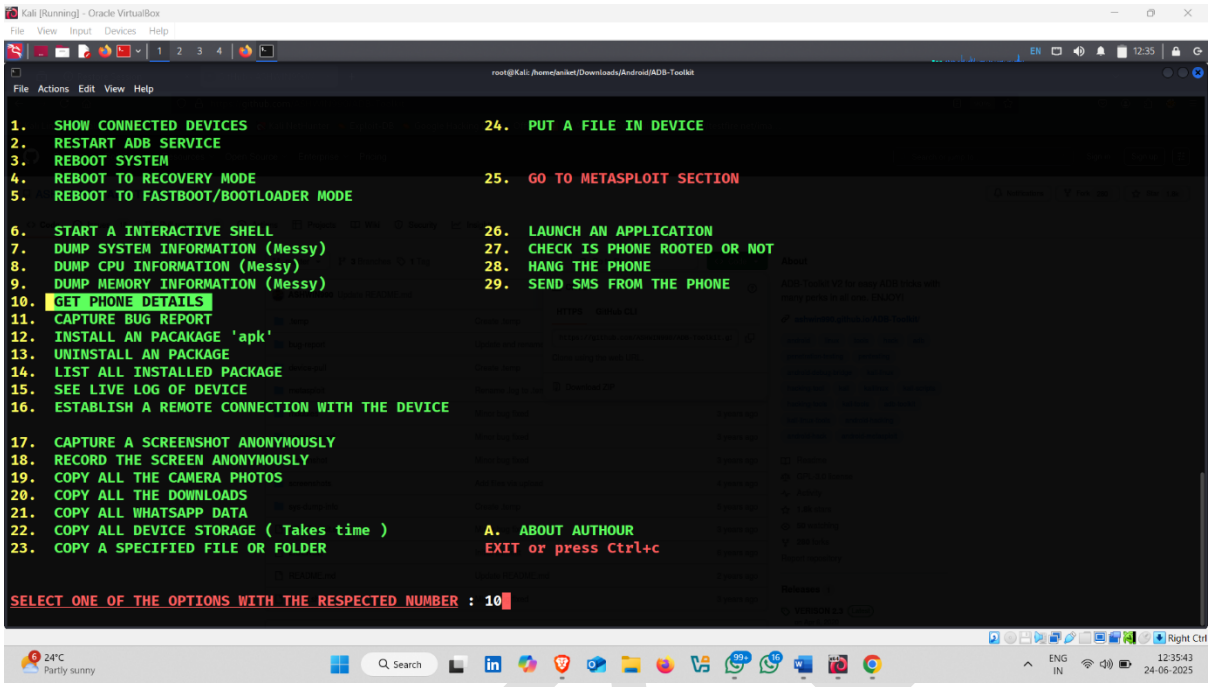
- Type **yes** ✅



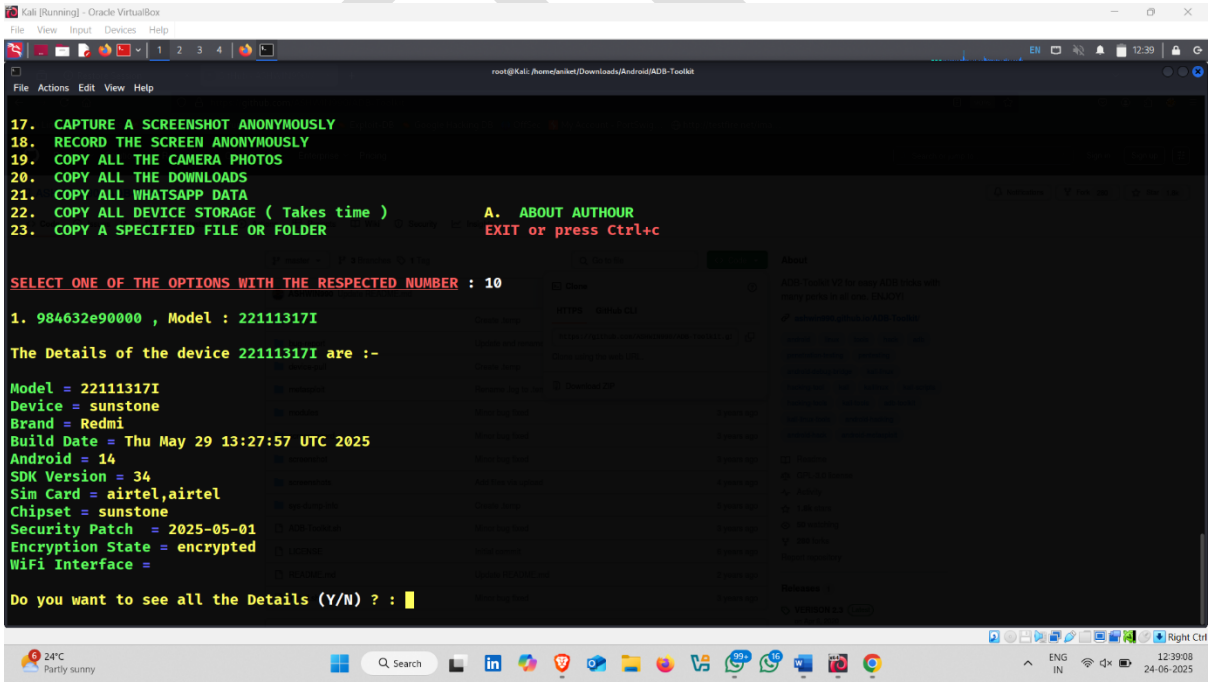
- ADB-Tool-kit Start



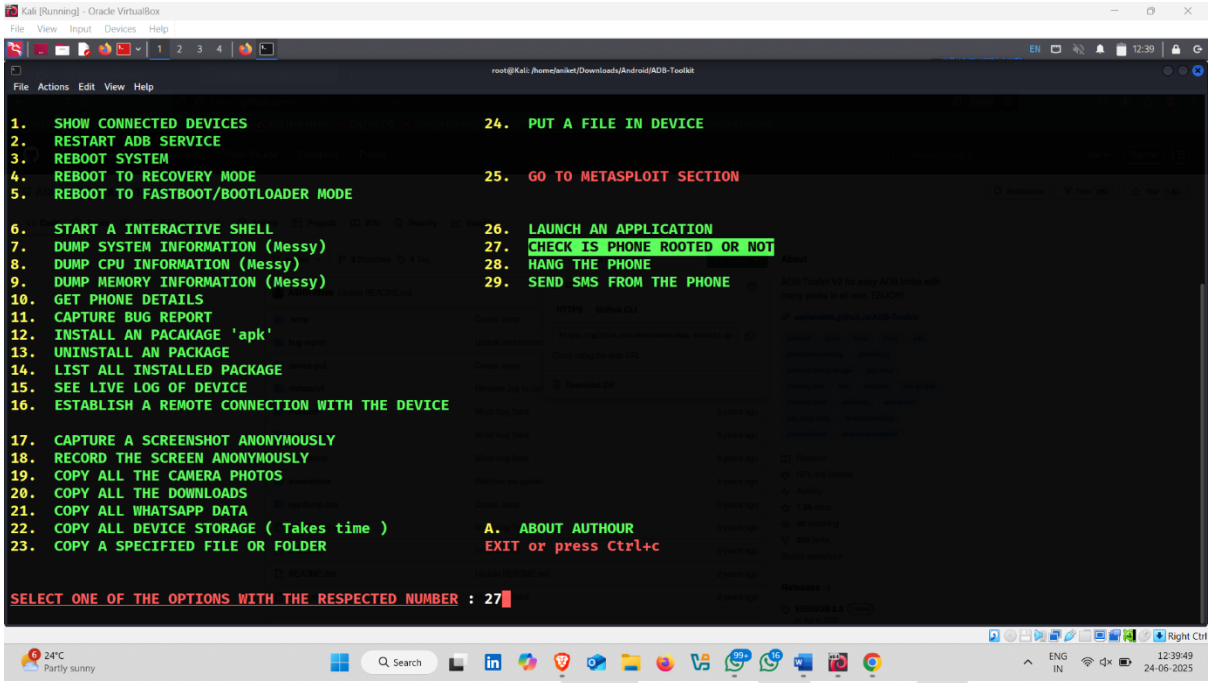
- Now , you can used any command that given below 👇
- 10—**to get phone details**



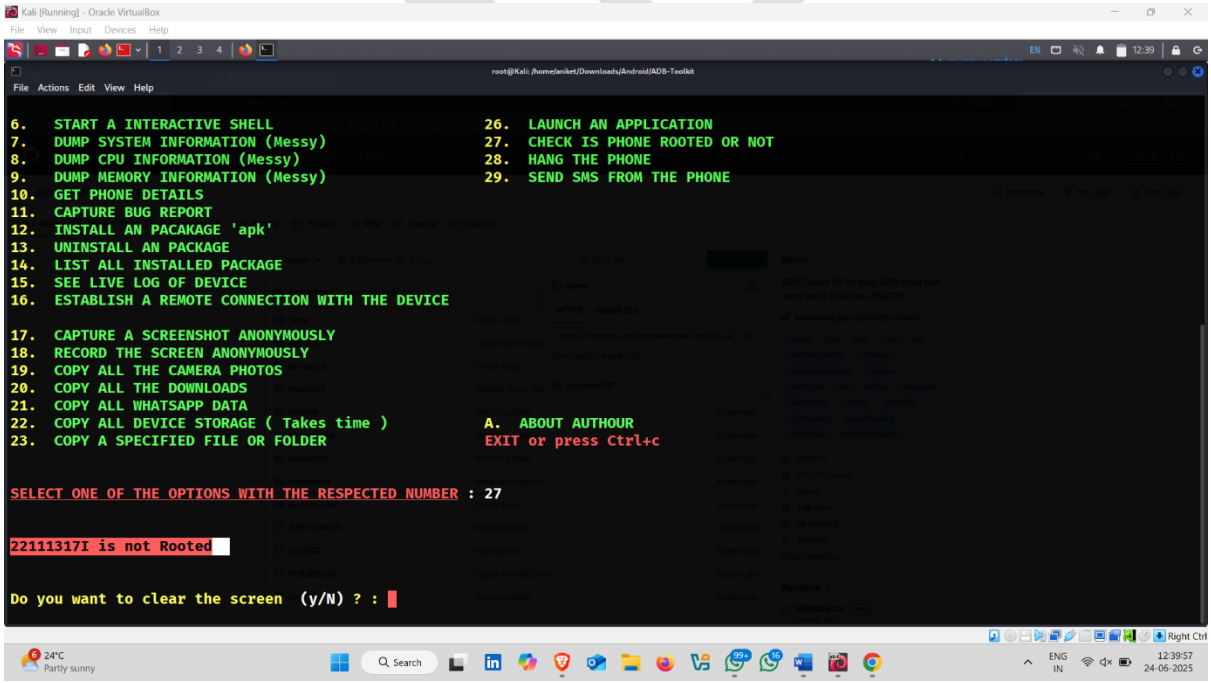
- Details ✅ 👇



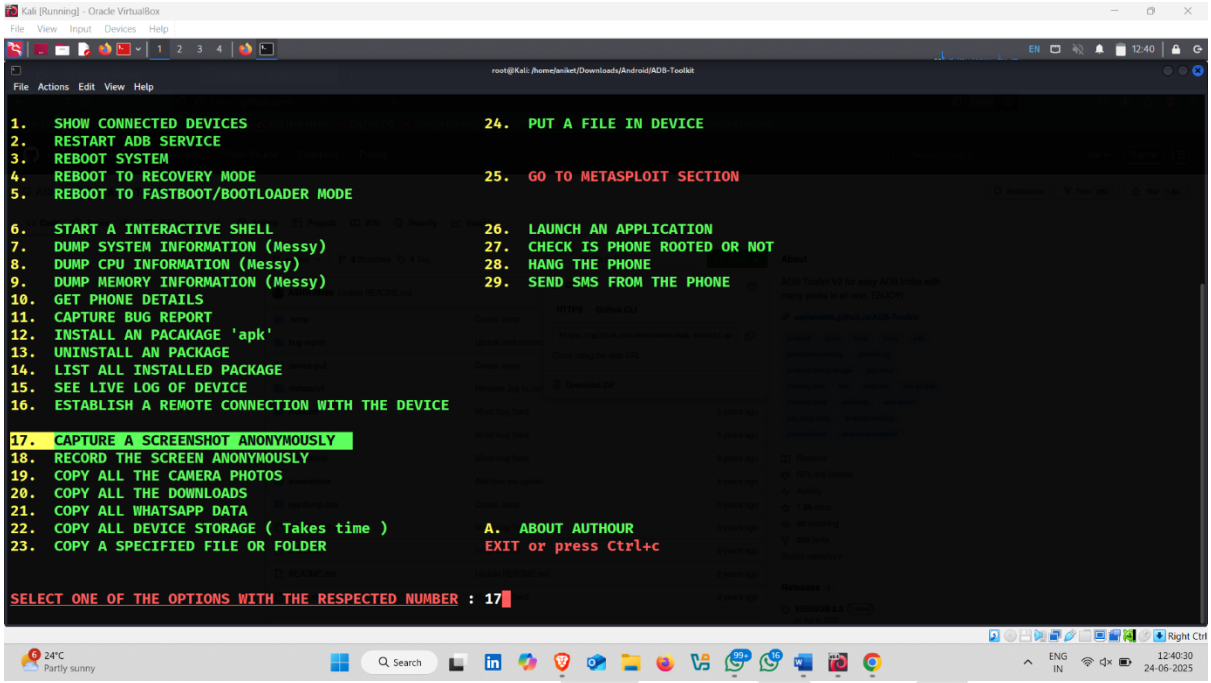
- 27 – **To check phone is rooted or not**



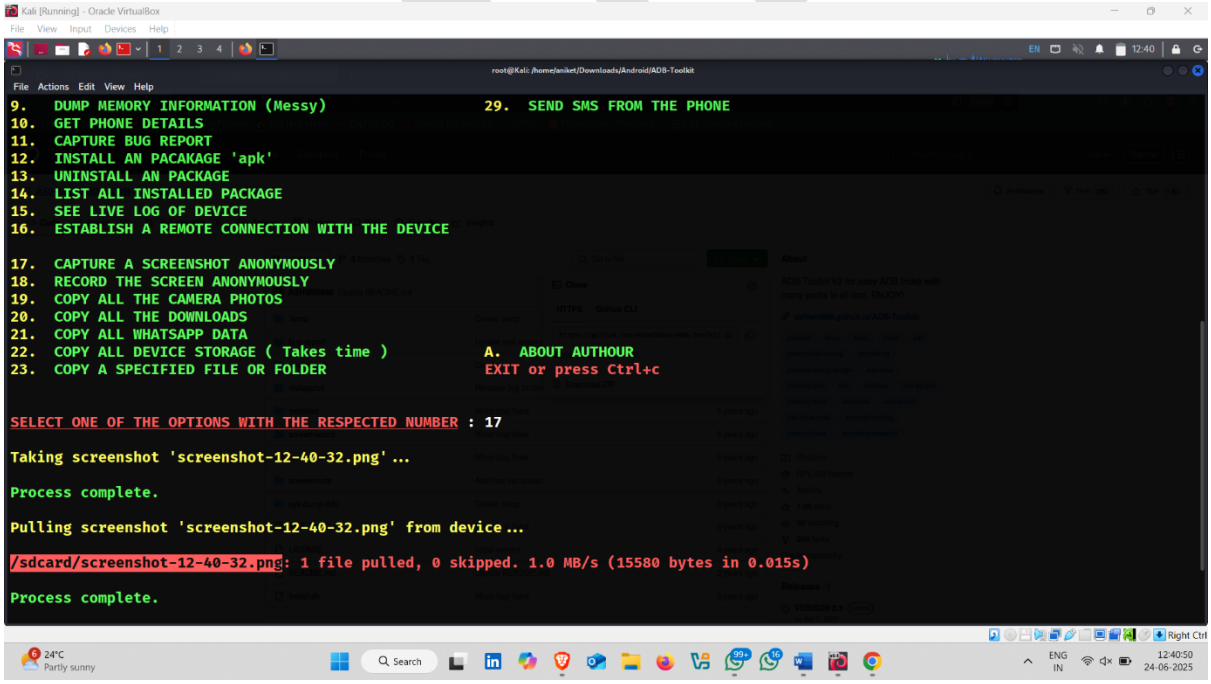
- **The Device is not a root** 👇



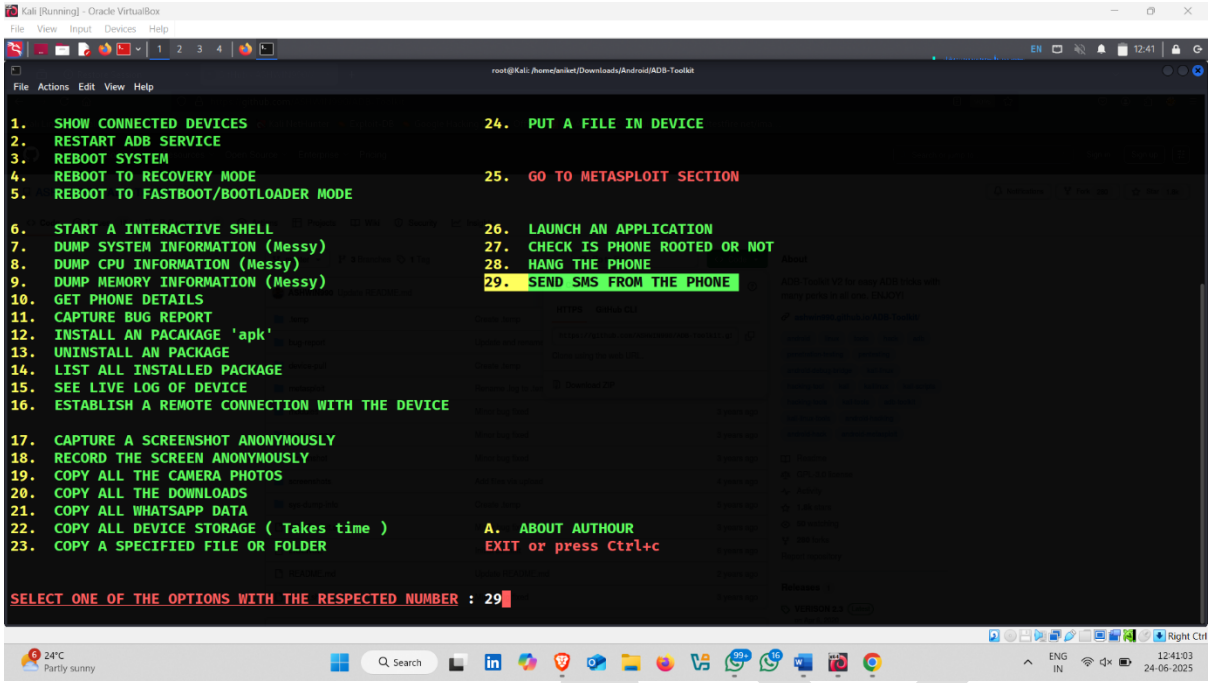
- 17 – **Capture a Screenshot anonymously**



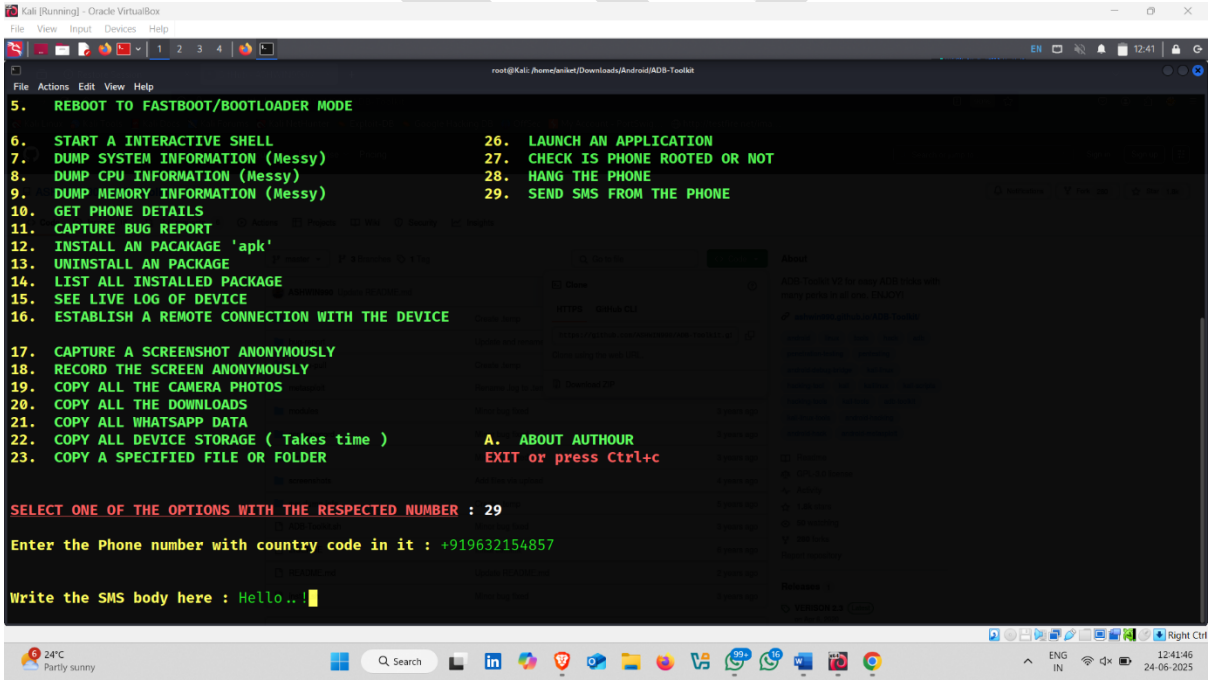
- **Screenshot captured**



- 29 – **Send SMS From The Phone**

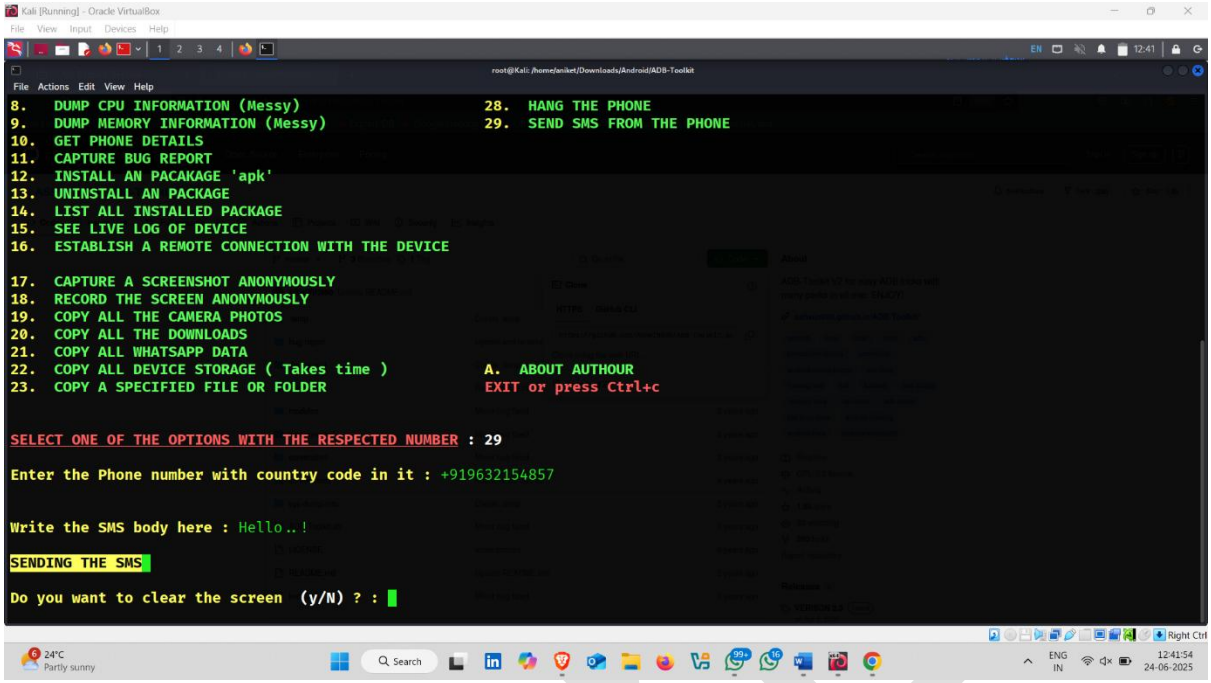


- **Enter mobile number with country code and type message**



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

- SMS Sending 👇 ✅



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.

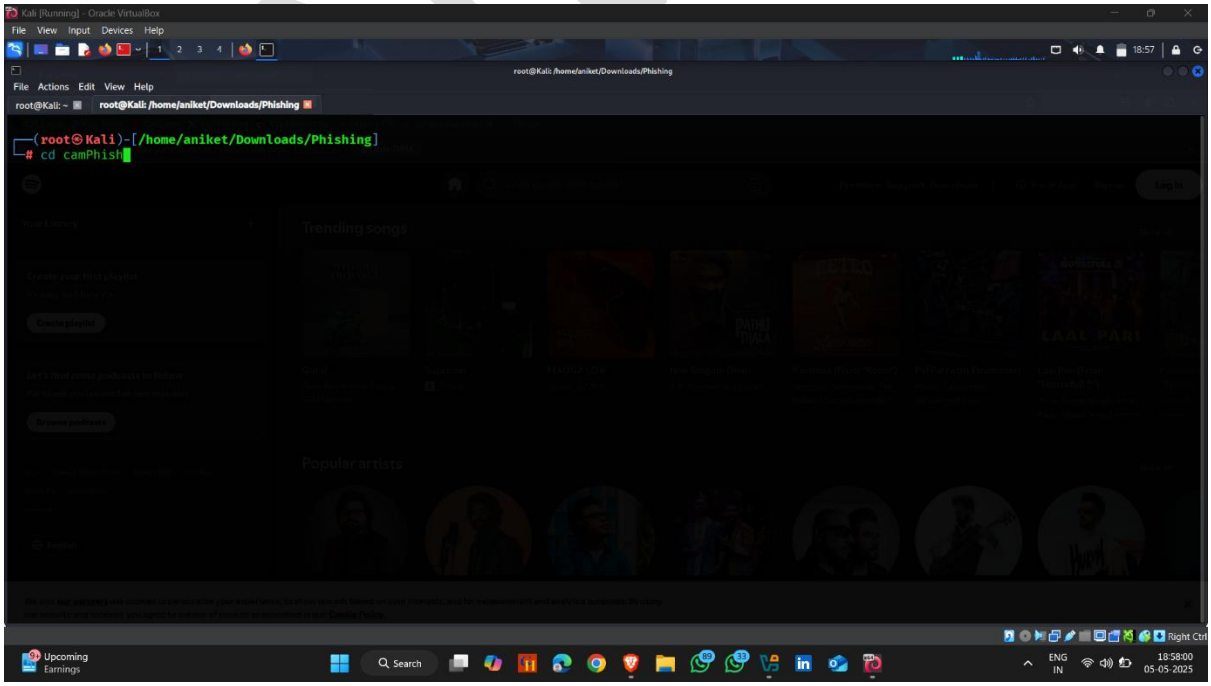
links.

🎭 Main Purpose of CamPhish:

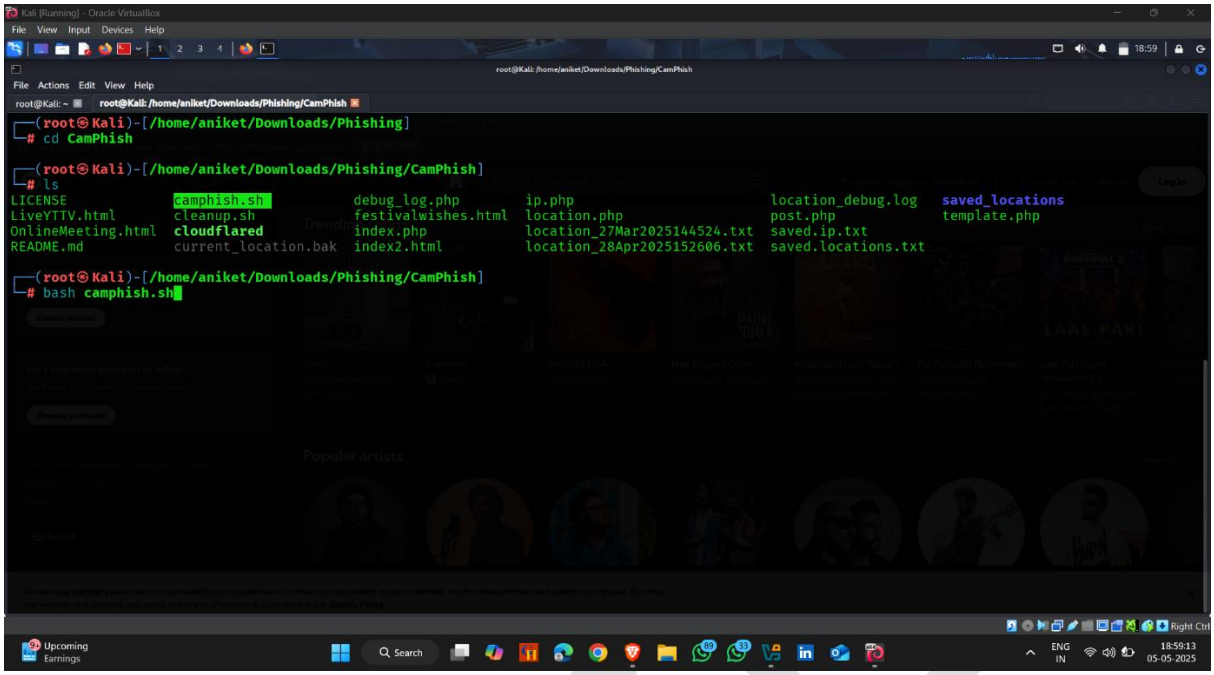
- 🎯 **Capture webcam pictures remotely.**
- 🎯 **Phish the victim using a fake website.**
- 🎯 **Demonstrate social engineering and phishing techniques.**

How to use it -:

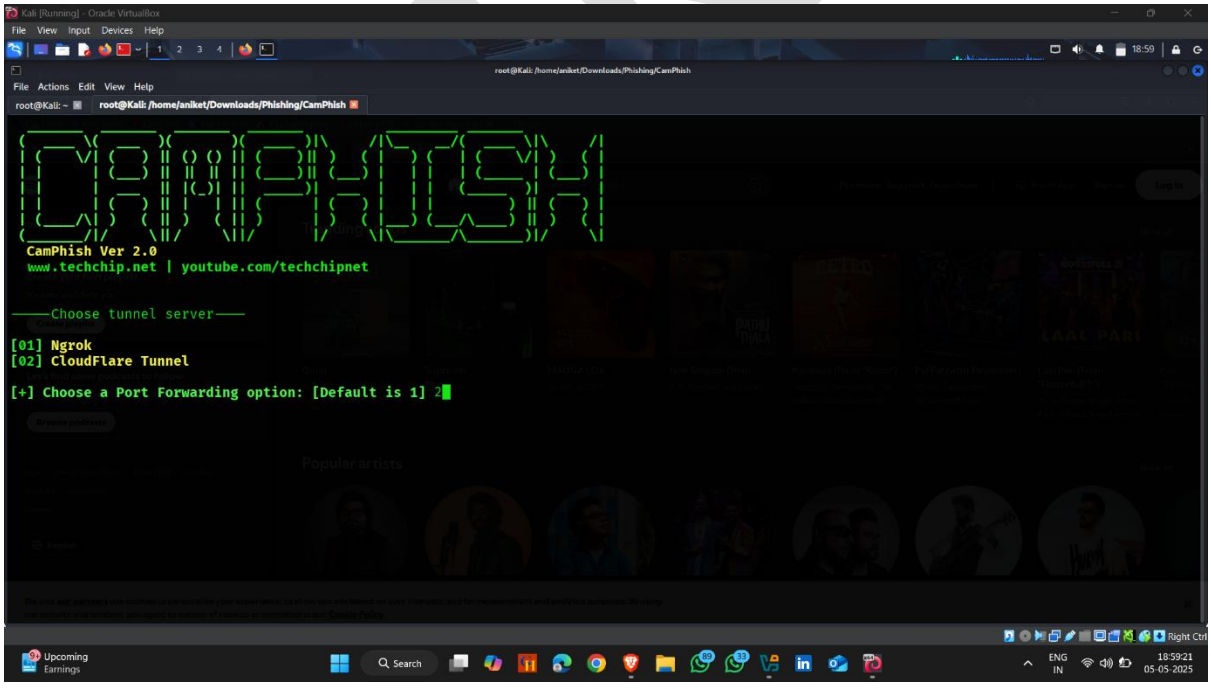
- Open kali linux terminal go to the camphish directory



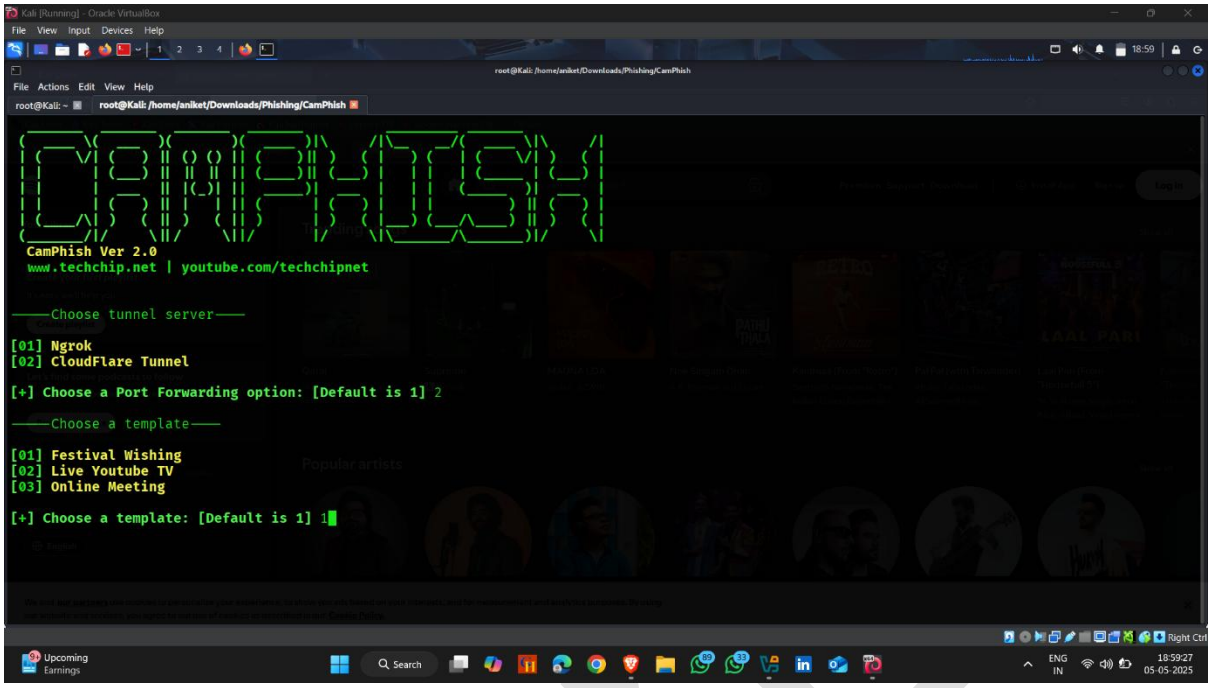
- Type command –**bash camphish**



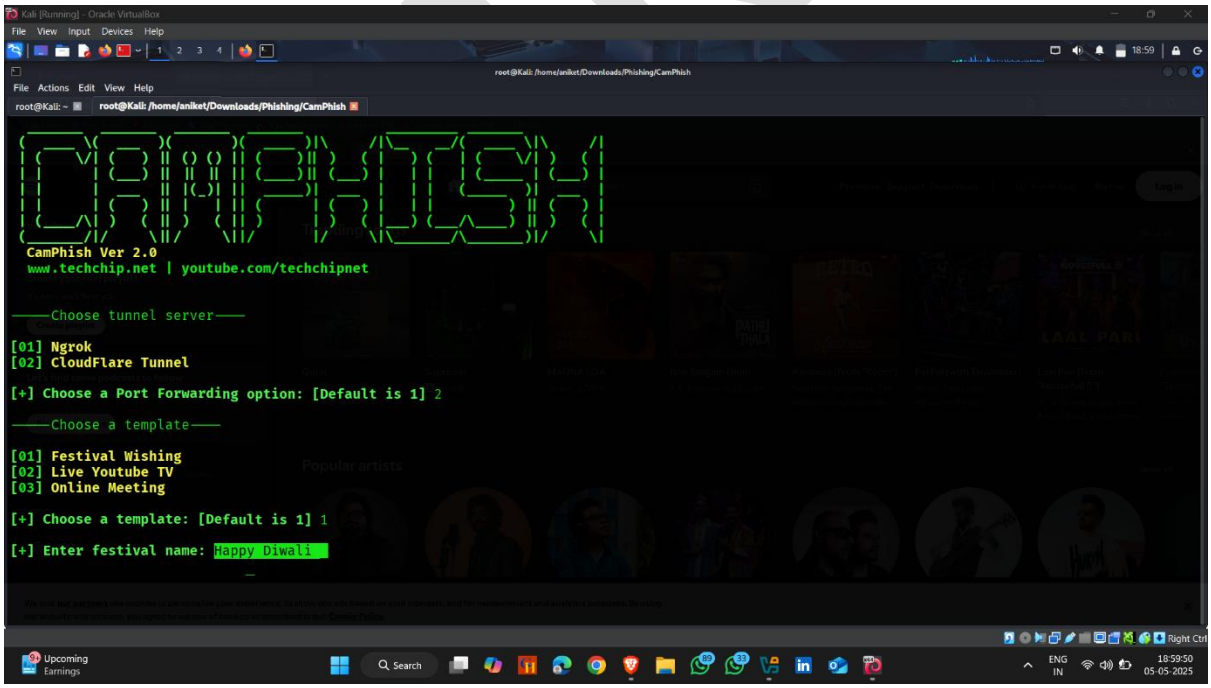
- Select Server – cloudflare tunnel



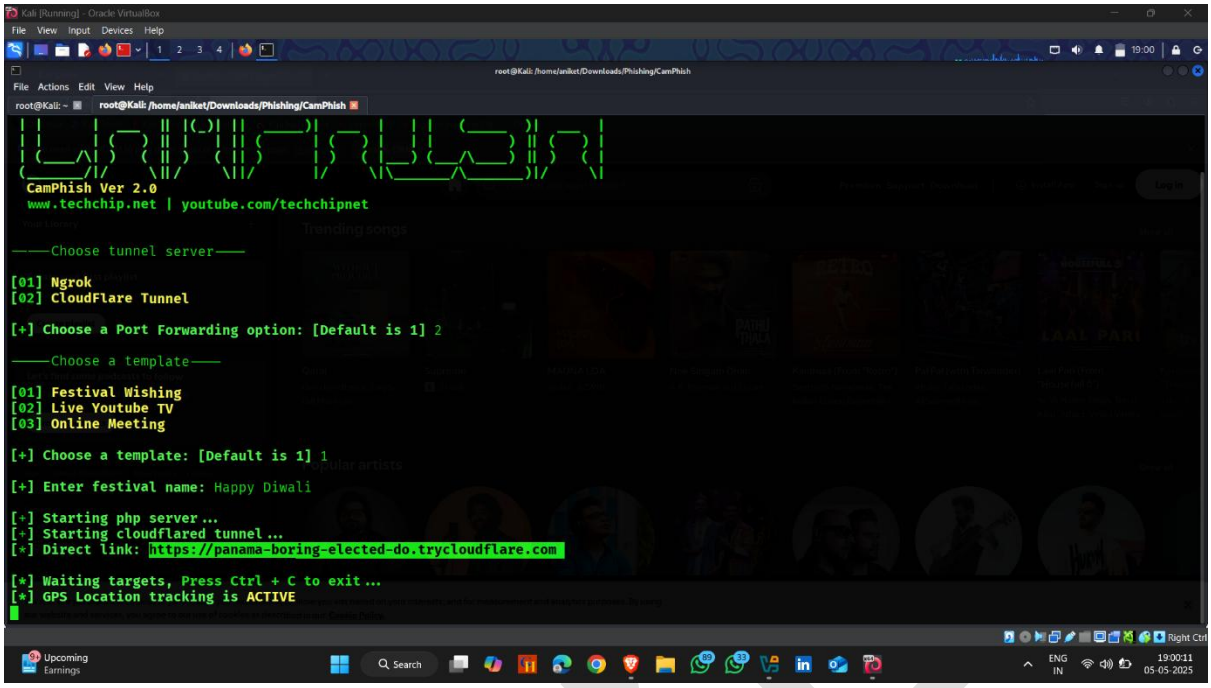
- Select 1



- **Enter Message**

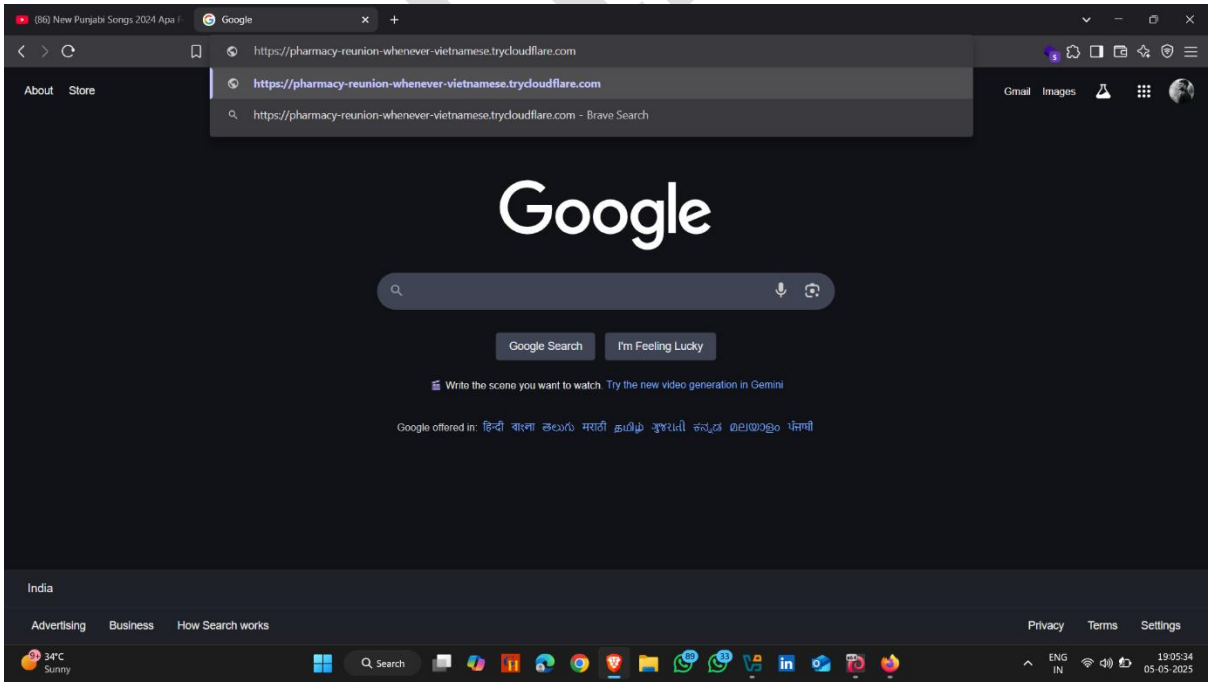


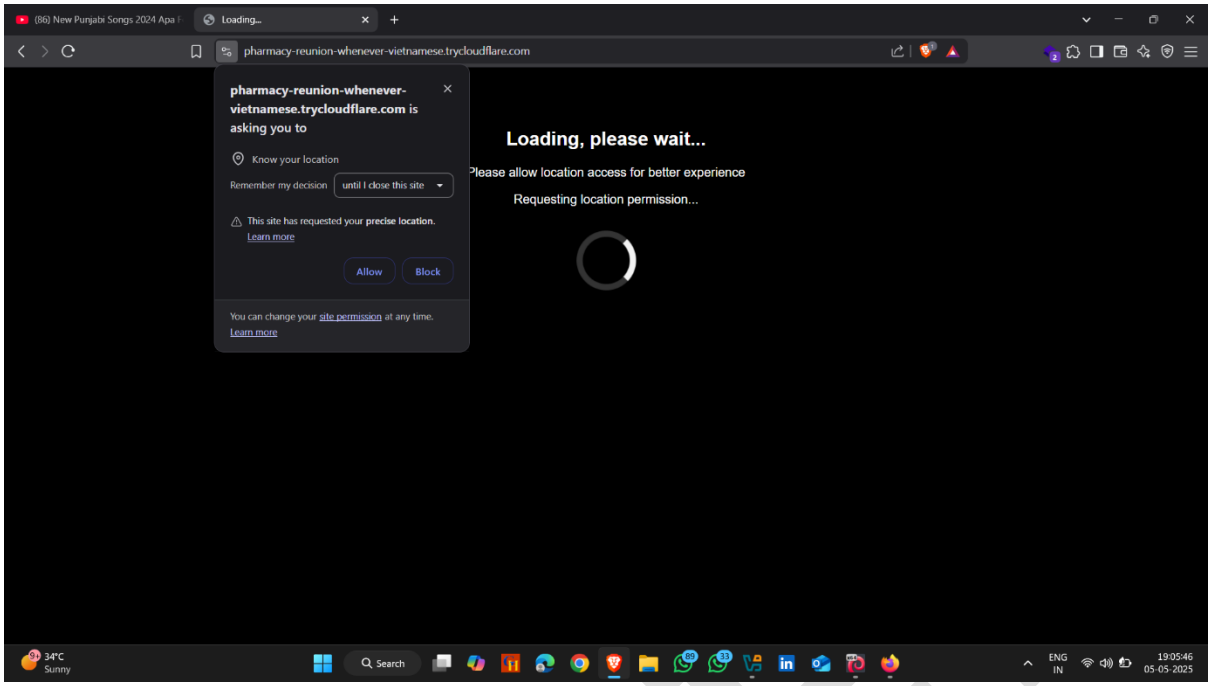
- Link Generated



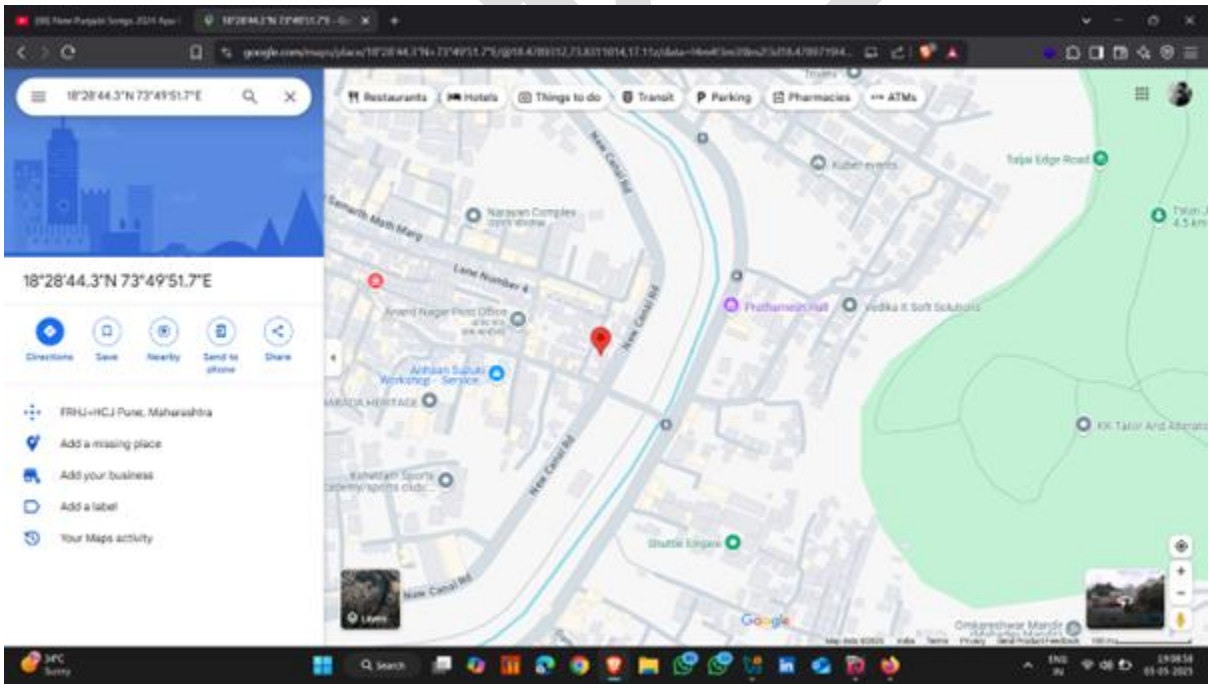
Note -: Im using my own browser for just demonstrate , you directly send this link to the target to access their camera

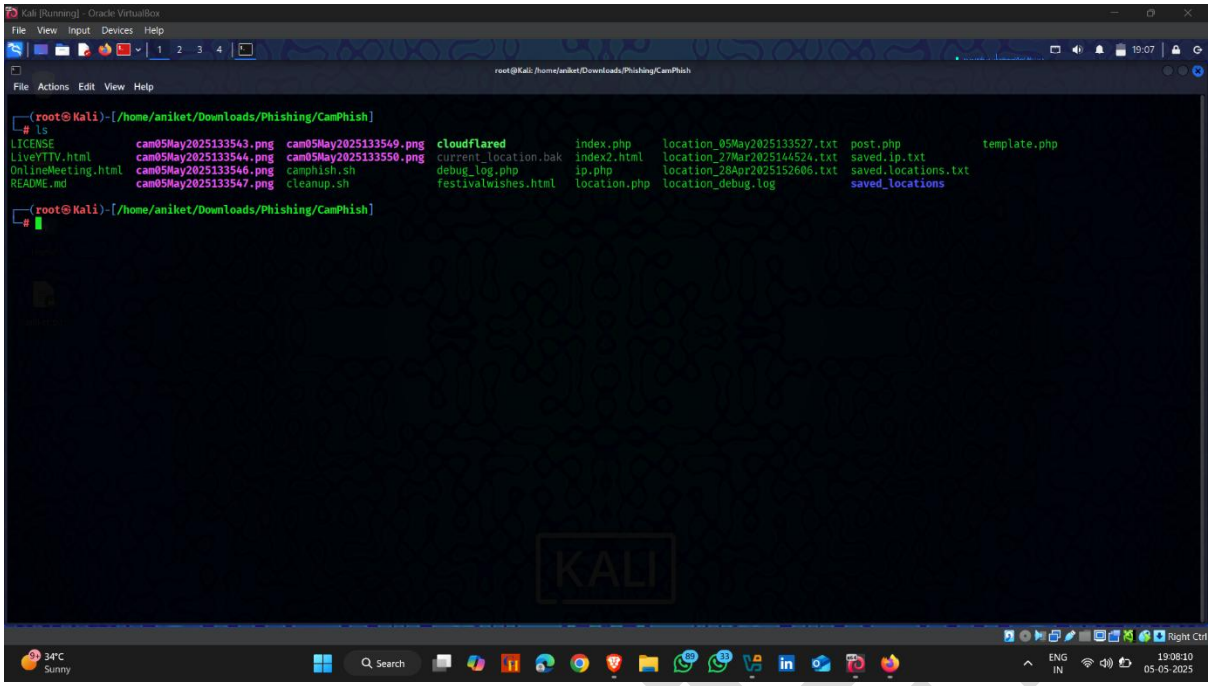
- Paste link on Browser





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




Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali: /home/aniket/Downloads/Phishing/CamPhish
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
LiveYTTV.html cam05May2025133544.png cam05May2025133550.png current_location.bak index2.html location_27Mar2025144524.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
(root㉿Kali)-[/home/aniket/Downloads/Phishing/CamPhish]
#
KALI
34°C Sunny
Search
ENG IN
19:08:10 05-05-2025

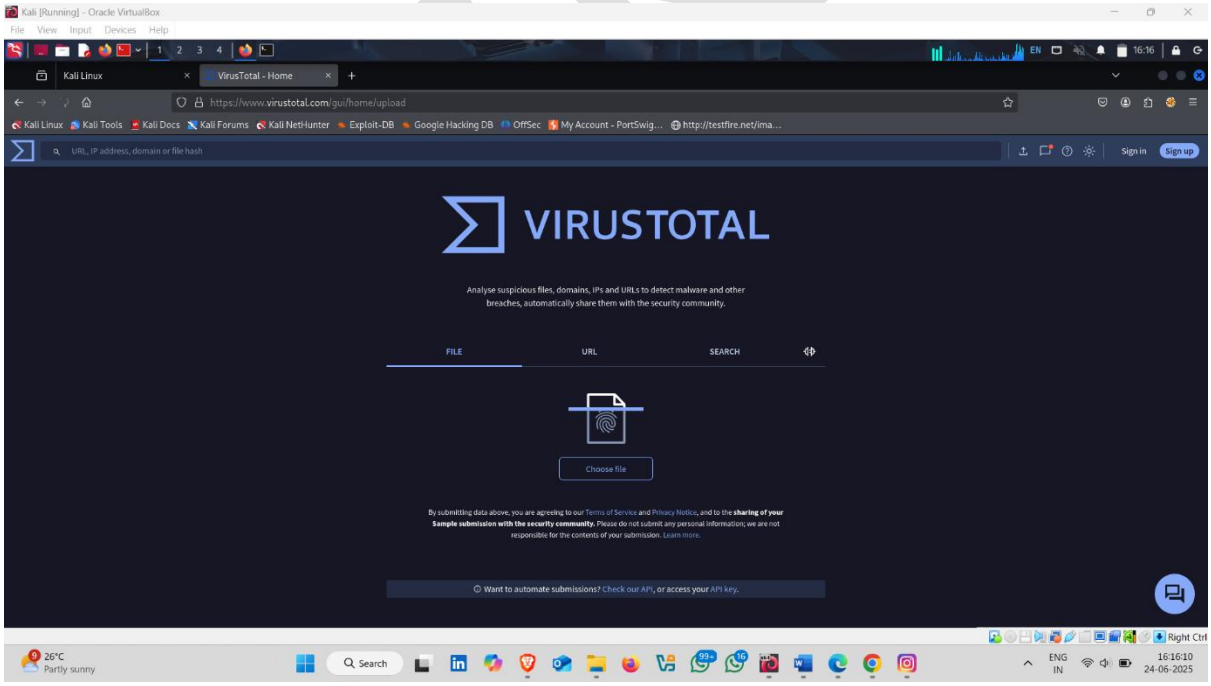
APK Security Analysis Using Online Tools

1.Perform Application Security Analysis Using Virus Total

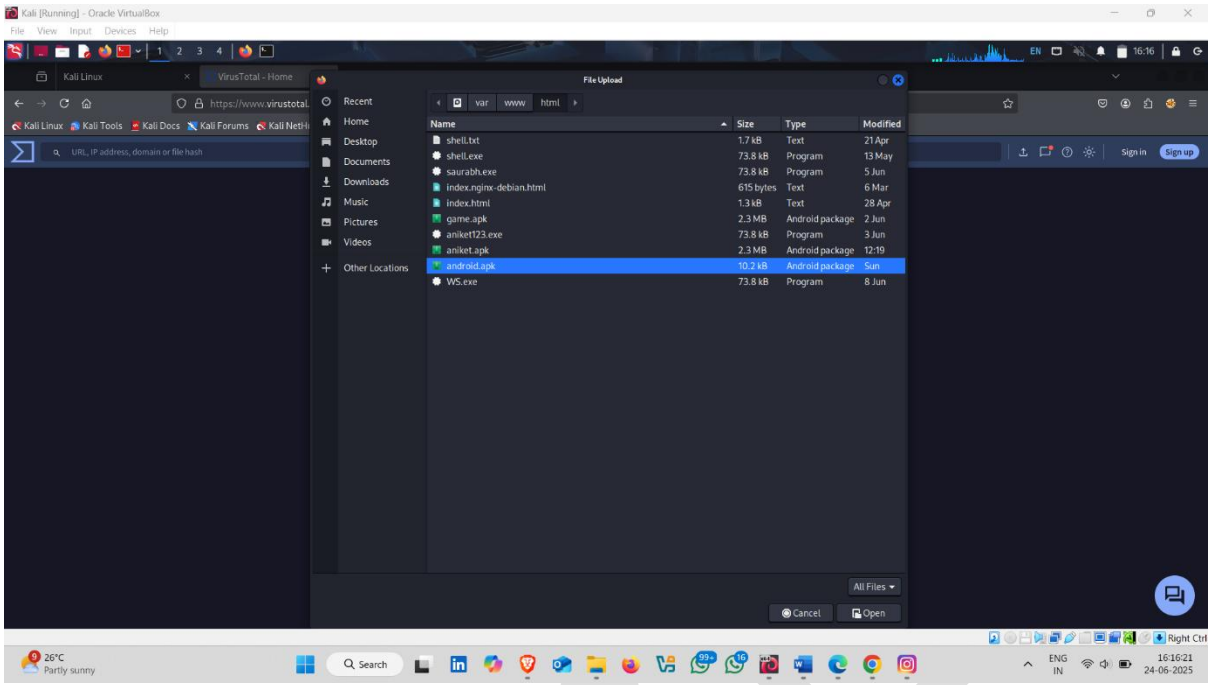
VirusTotal is a **free online malware scanning and analysis platform** that allows users to upload files, including APKs, executables, documents, and URLs, to check them against **multiple antivirus engines and security tools simultaneously.**

How to use it -:

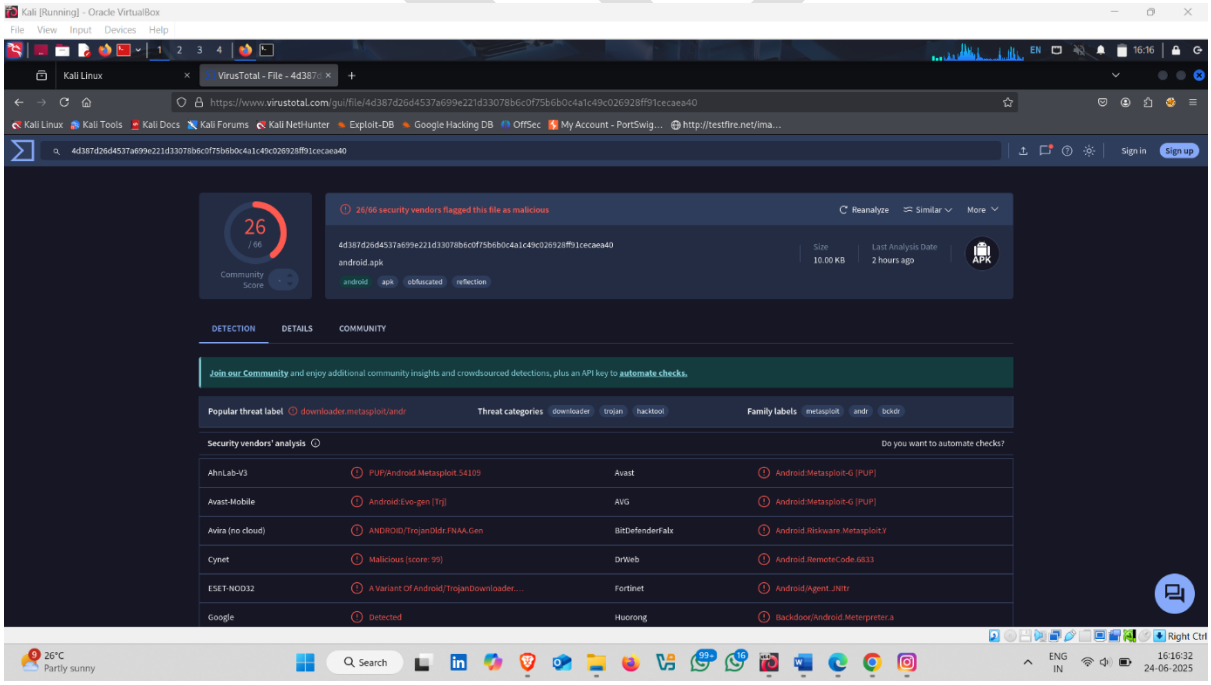
- Open Virus total on Browser and choose Apk that you want to scan



- Select Application and then click on open



- Malware Scanned ✅👇

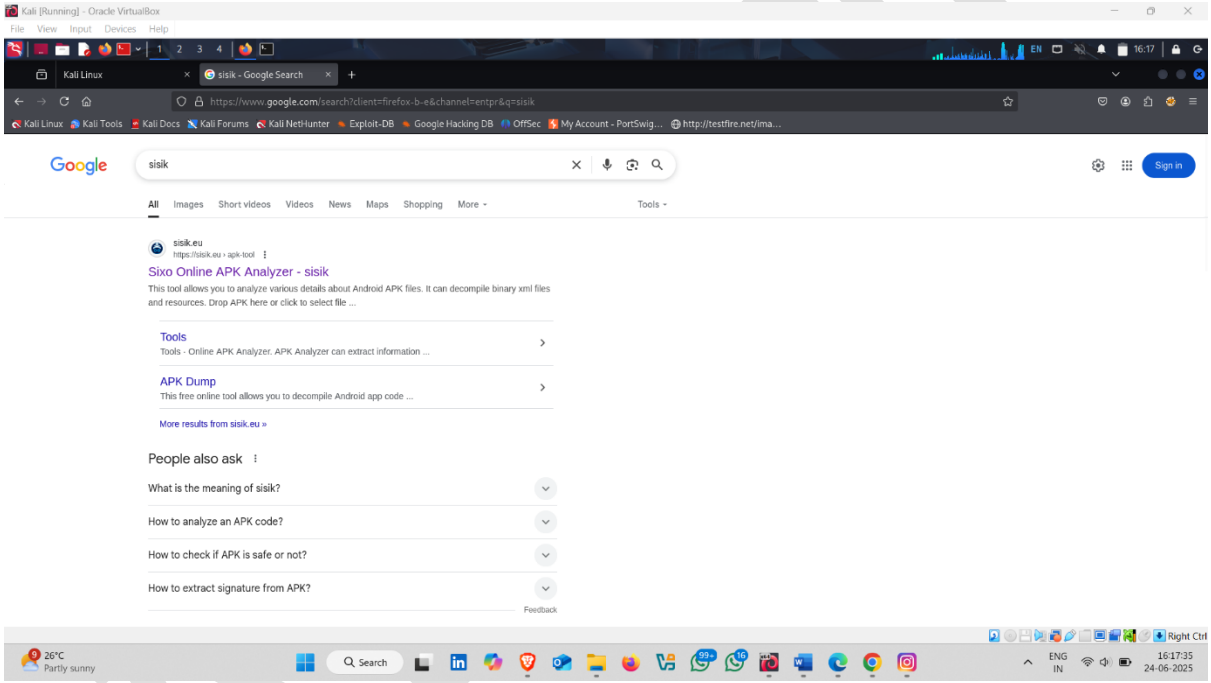


2.Perform Application Security Analysis Using Sisik Online APK Analyzer

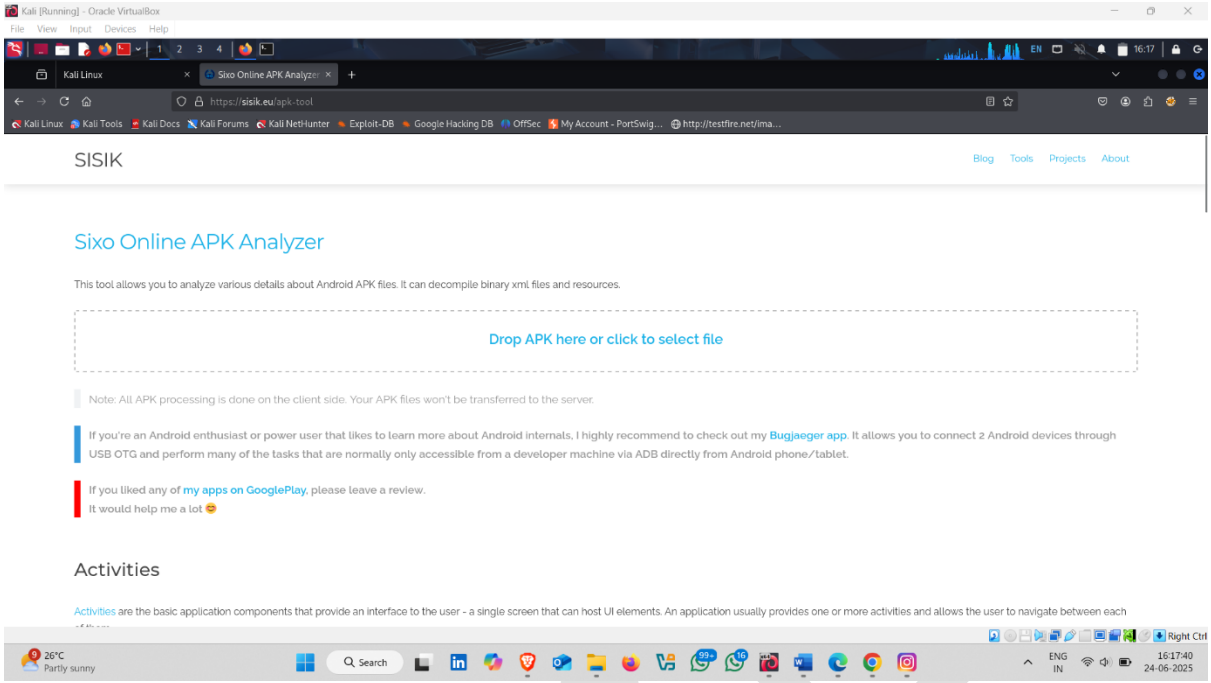
Sisik APK Analyzer is a **free, web-based APK analysis tool** that helps you inspect the internal structure, manifest file, permissions, and components of an Android application (APK file) without installing any software.

How to use it –:

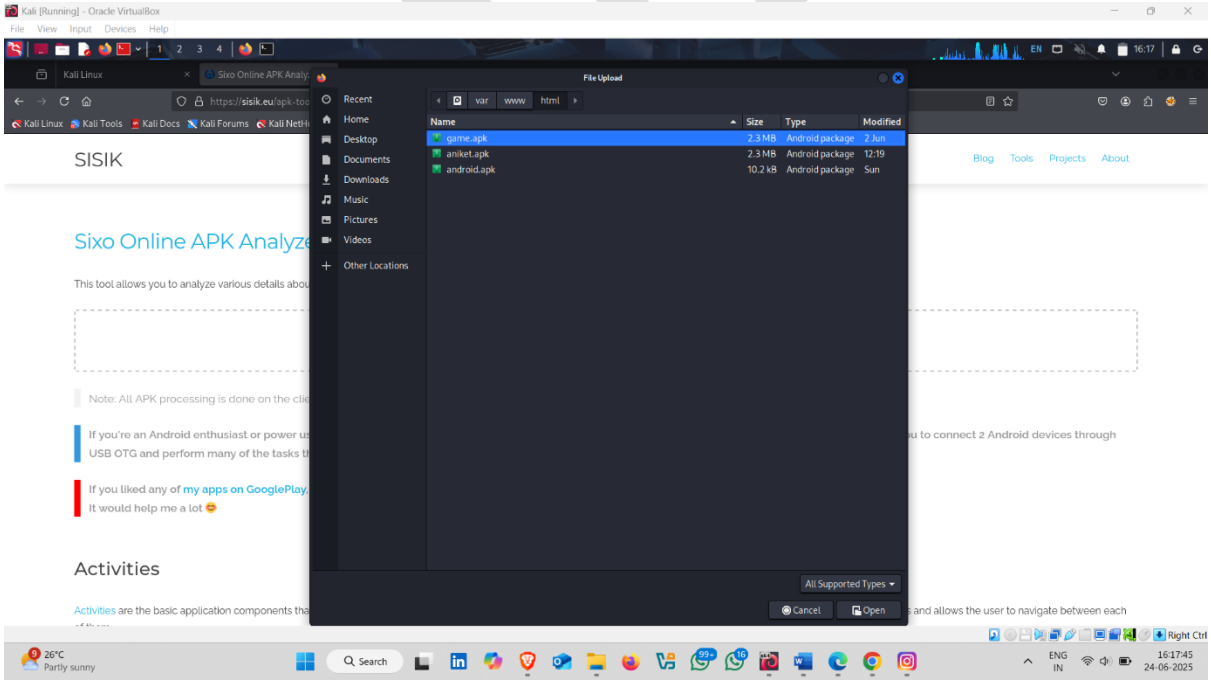
- Open Browser and search sisk online APK Analyzer
- Click on first website



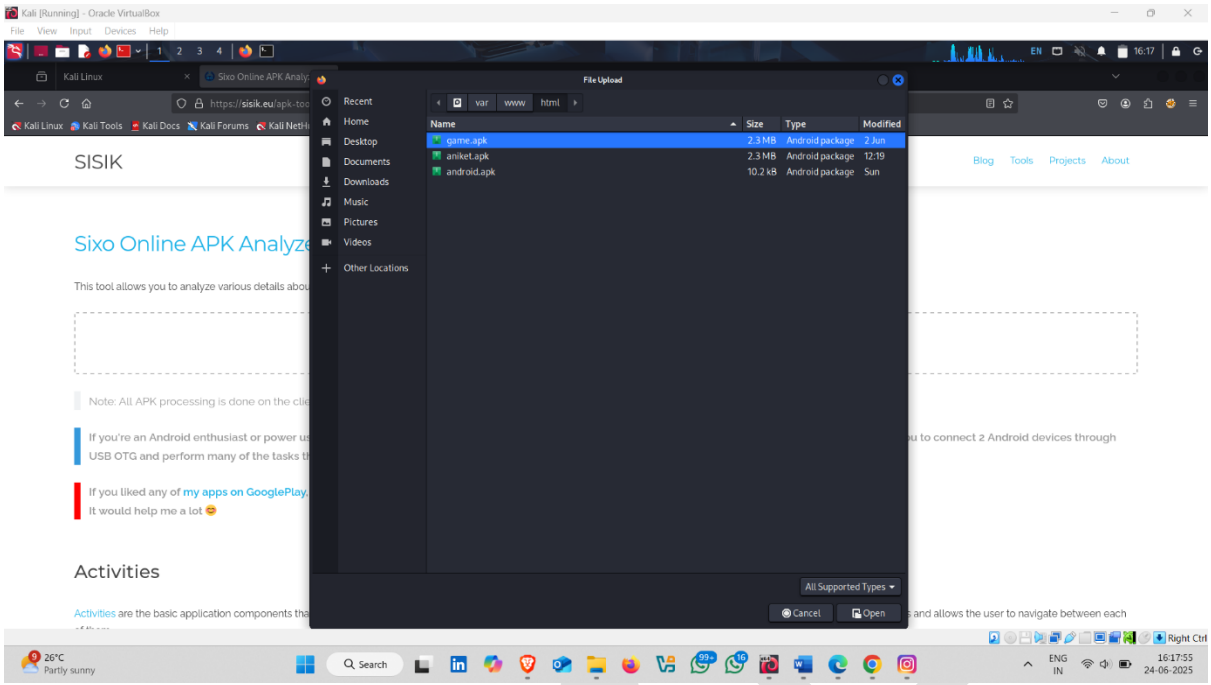
- Click on select file to select the application



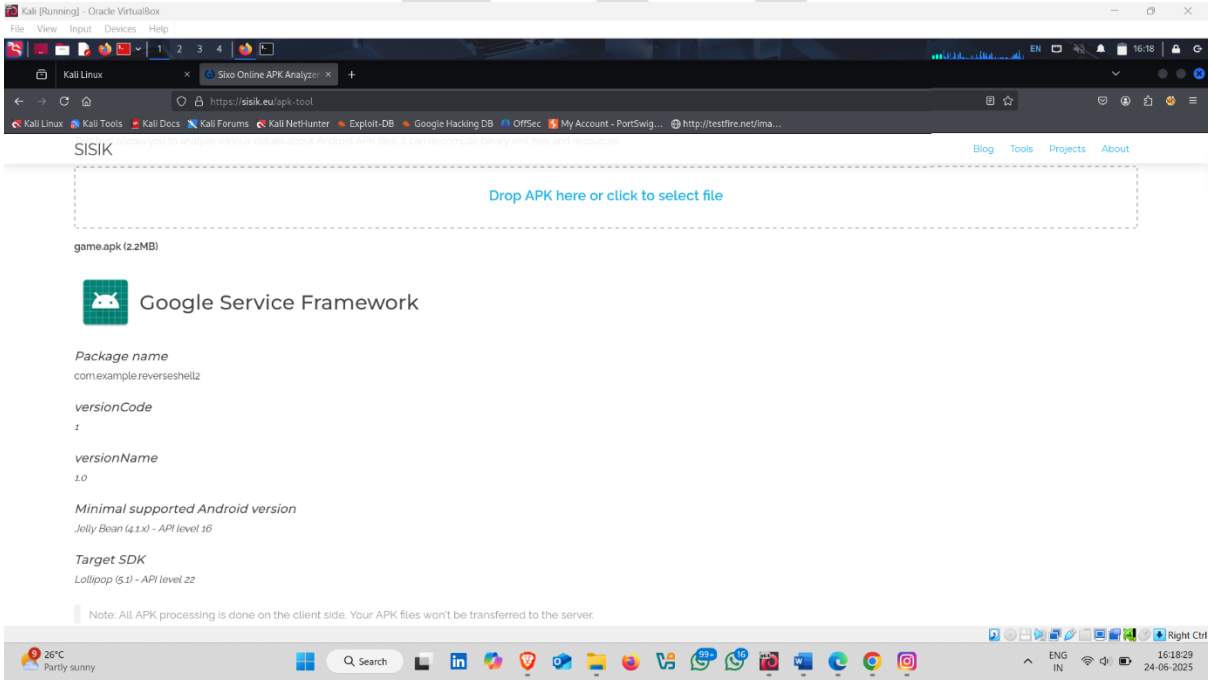
- Select application



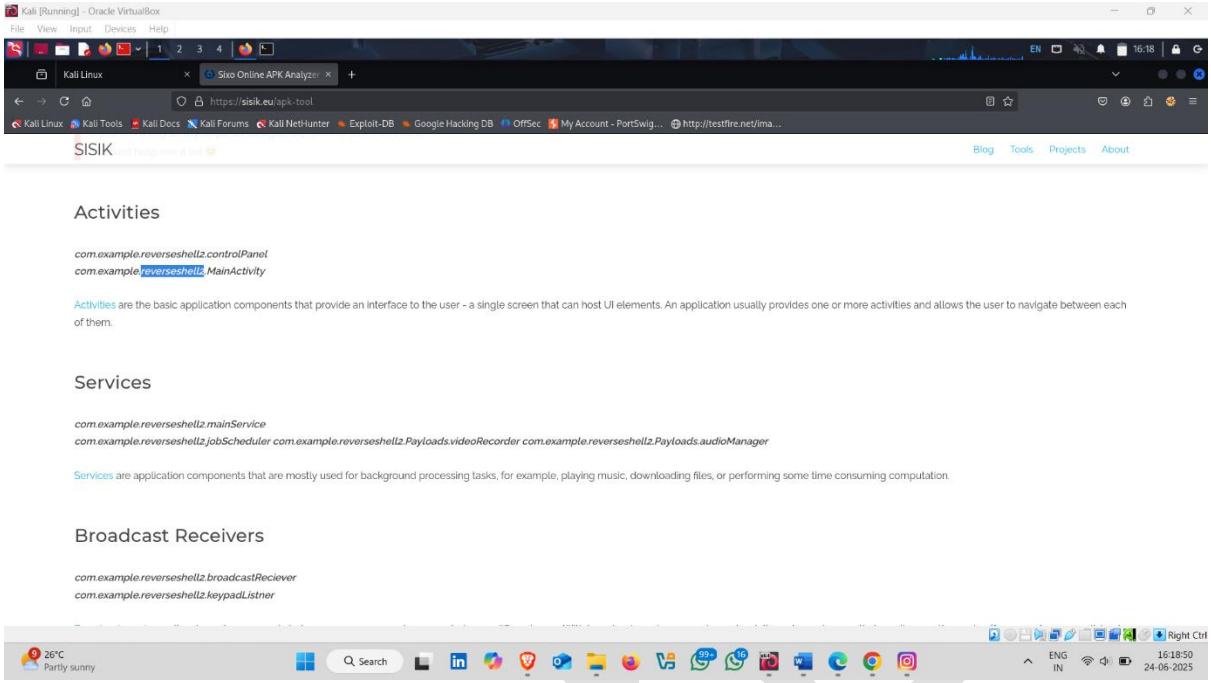
- then click on open



- it analyze the application



- main activity – reverse shell 👇



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.

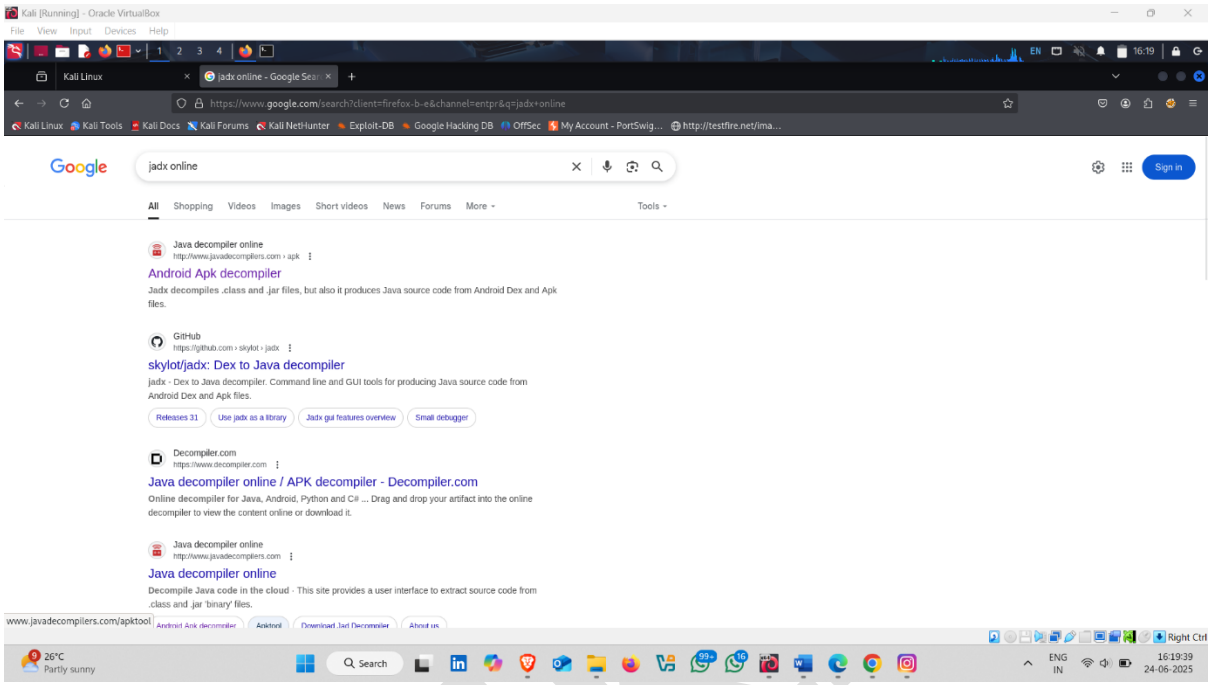
🔍 Why It Is Used in Application Scanning?

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

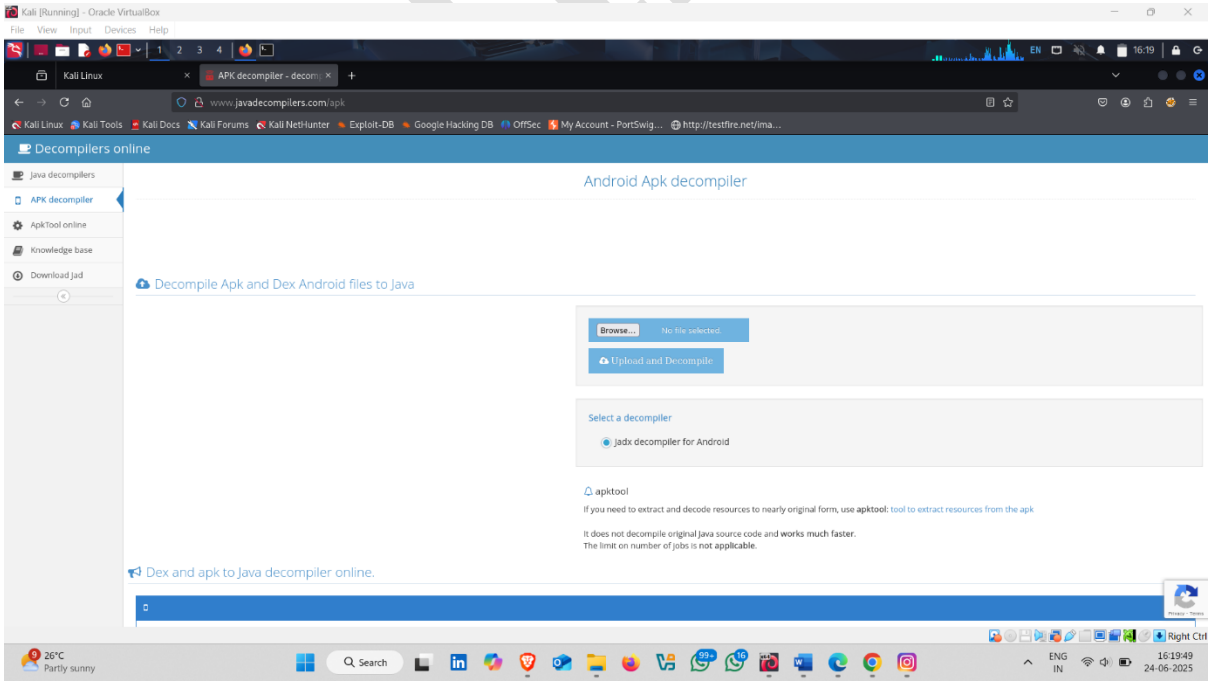
- 🕵️ **Inspect app logic and workflows.**
- 🔍 **Find security flaws, hardcoded credentials, API keys, and encryption keys.**
- 📜 **Understand app permissions, functions, and communication patterns.**
- 🚨 **Identify vulnerabilities like exposed tokens, insecure API calls, or weak encryption.**
- 🔐 **Check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

How to use it -:

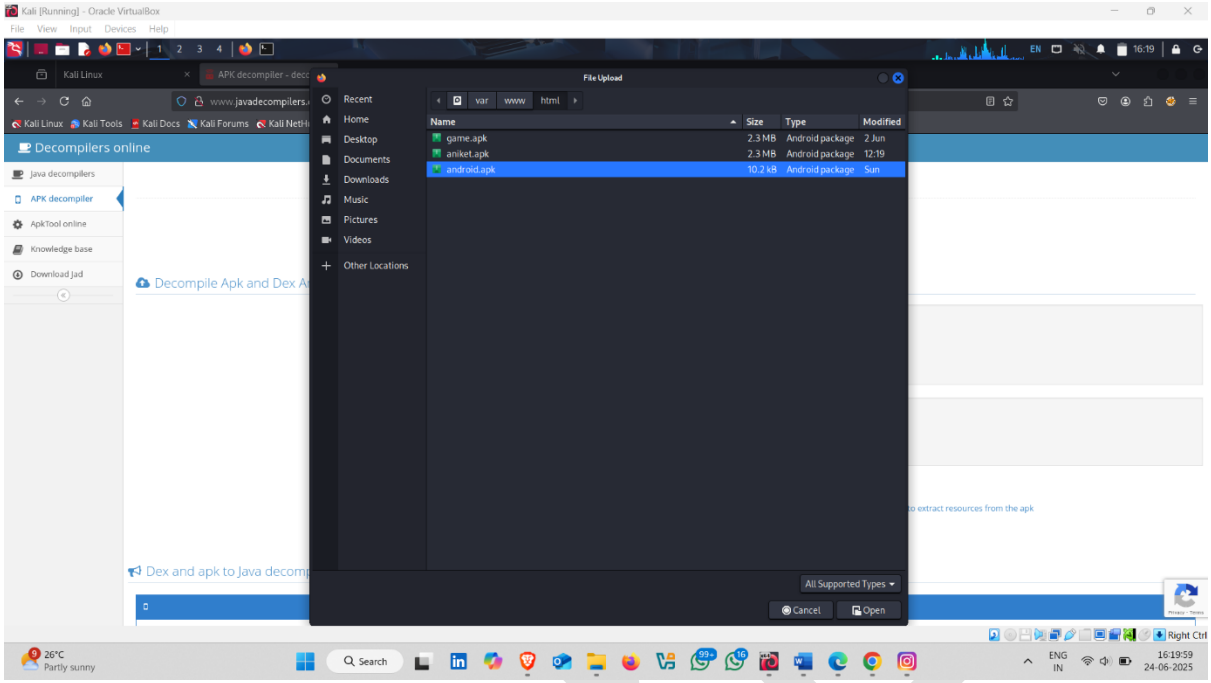
- Open Browser and search jadx online
- Click on first website



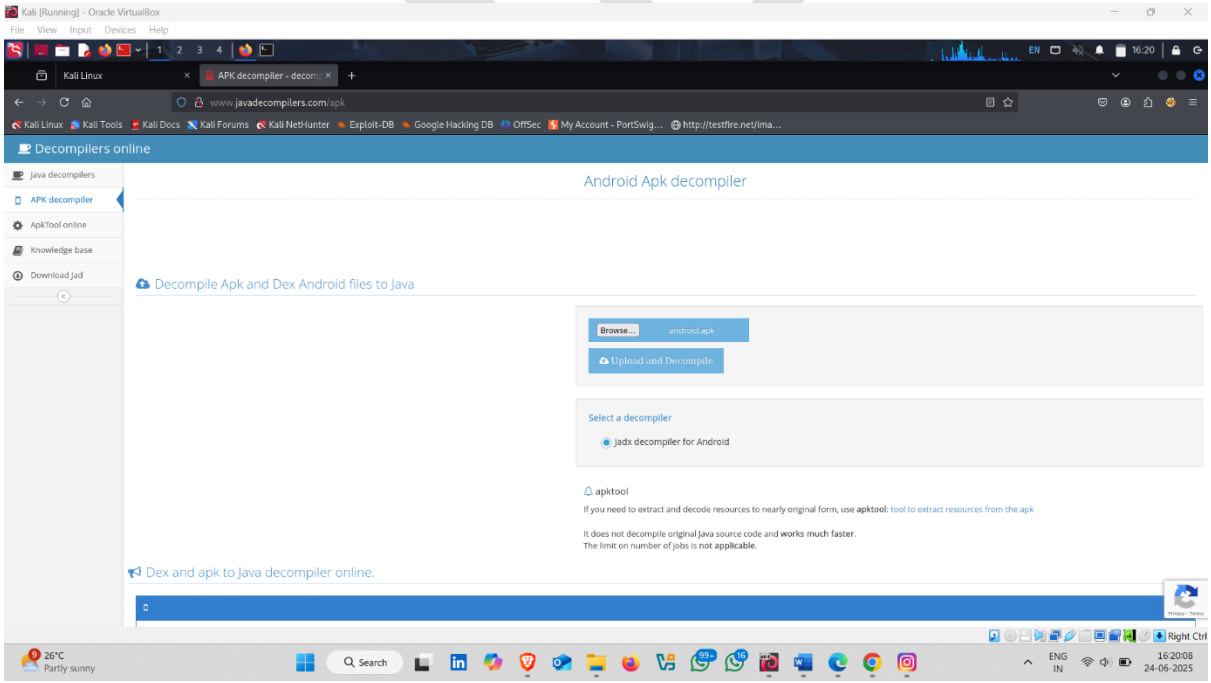
- Click on Browse to select the application



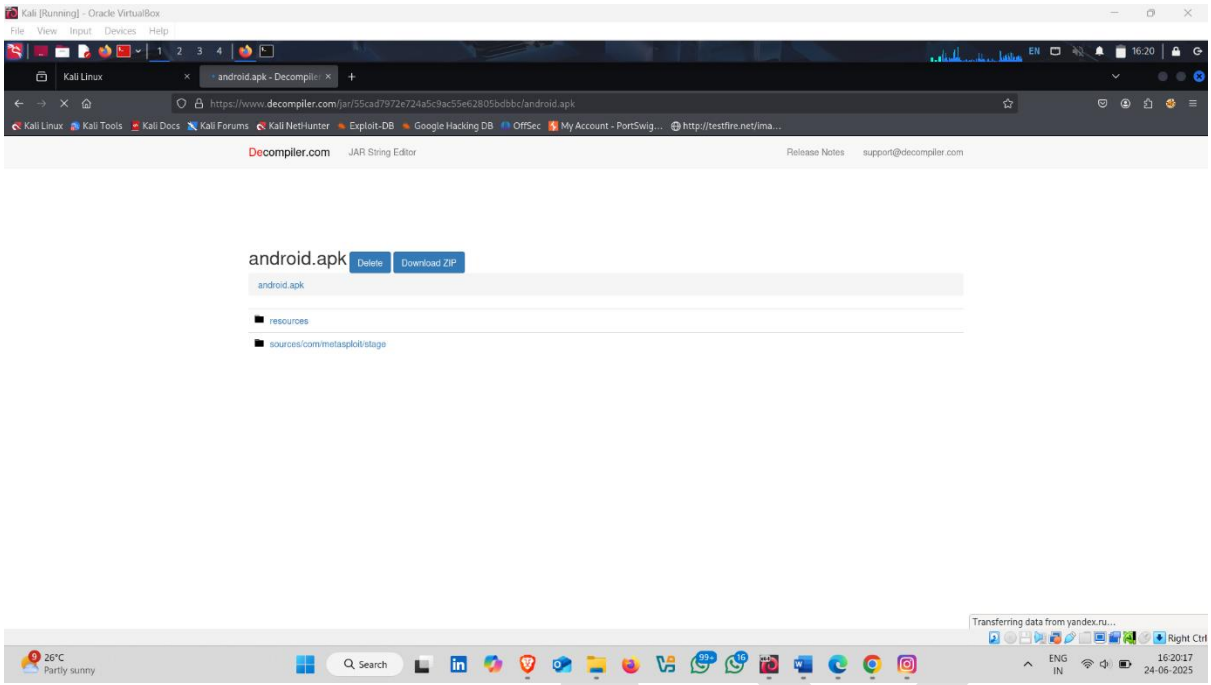
- Select application 👇



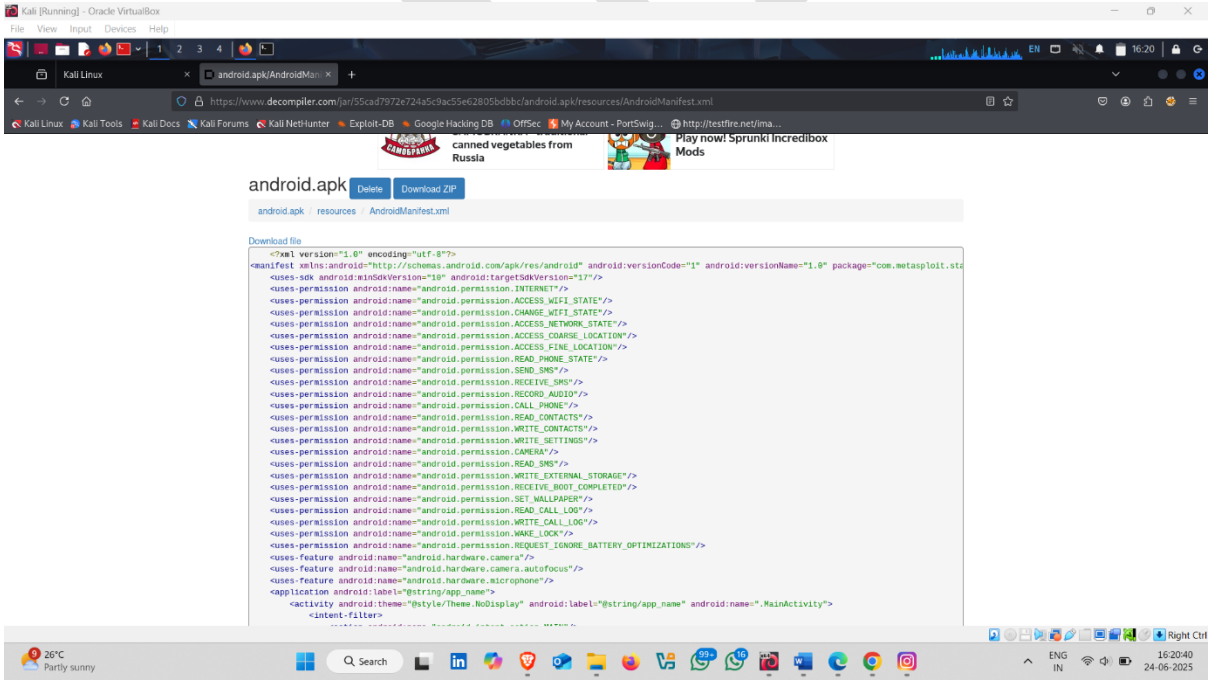
- Now click on upload and decompile option



- 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:

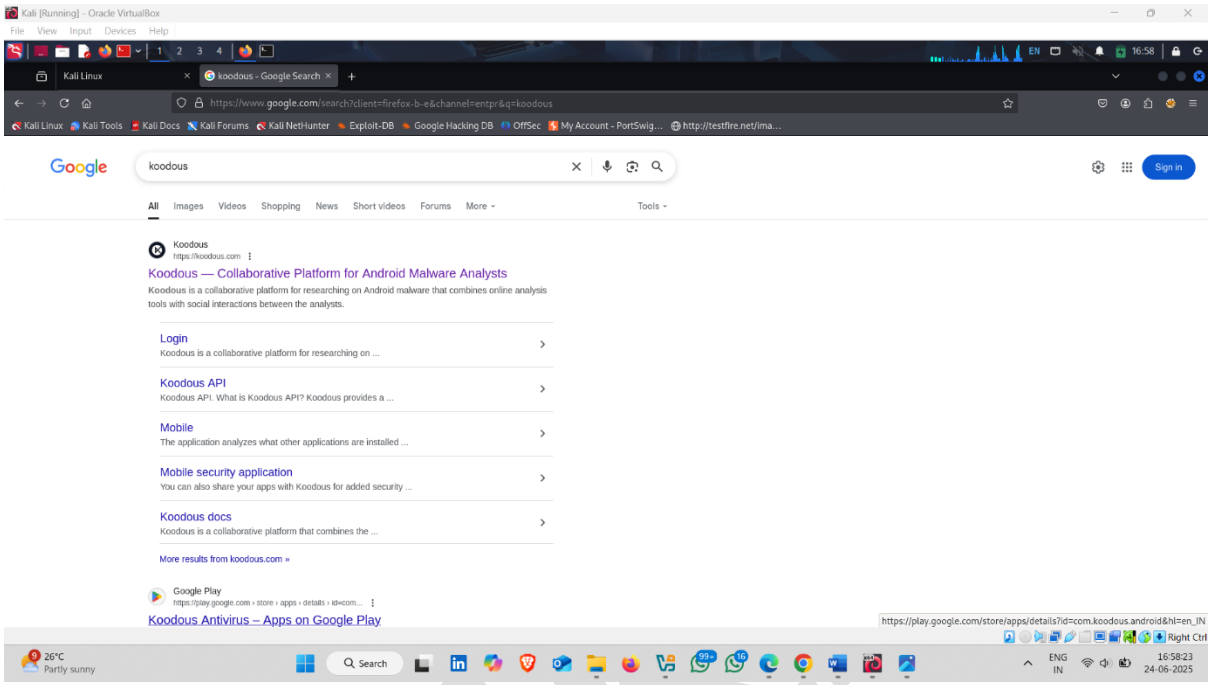
- Malware analysts
- Penetration testers
- Android security researchers
- Bug bounty hunters

🔍 **Main Purpose of Koodous:**

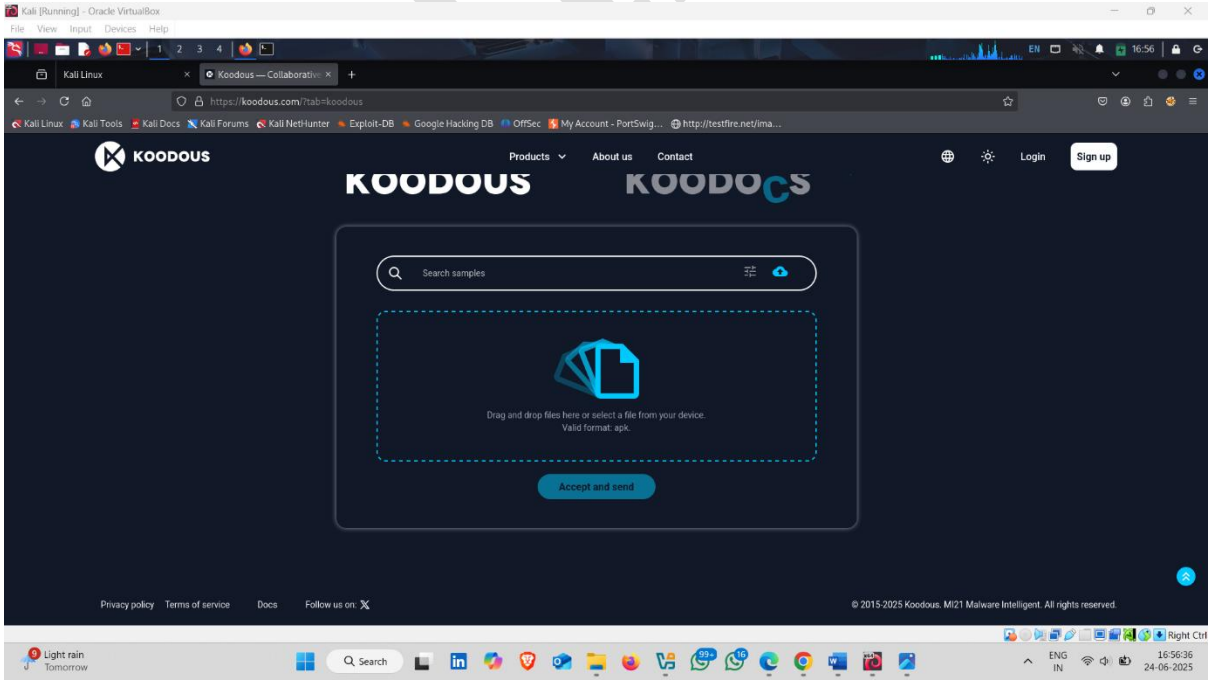
- 📁 **Analyze Android APKs for malware and security risks.**
- 🔍 **Review behavior, permissions, and suspicious code.**
- 🗂️ **Access a massive database of already-scanned APKs.**
- 🤝 **Allow security researchers to contribute rules and threat intelligence.**

How to use it -:

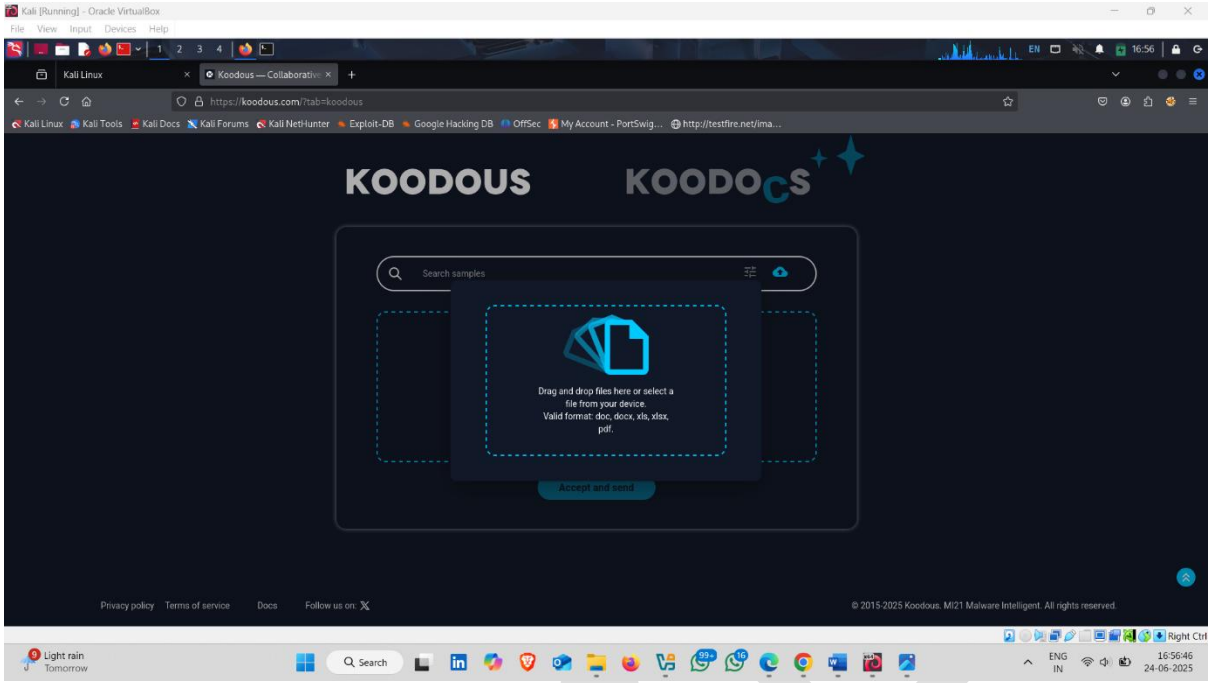
- Open browser and search koodous
- Click on first official website



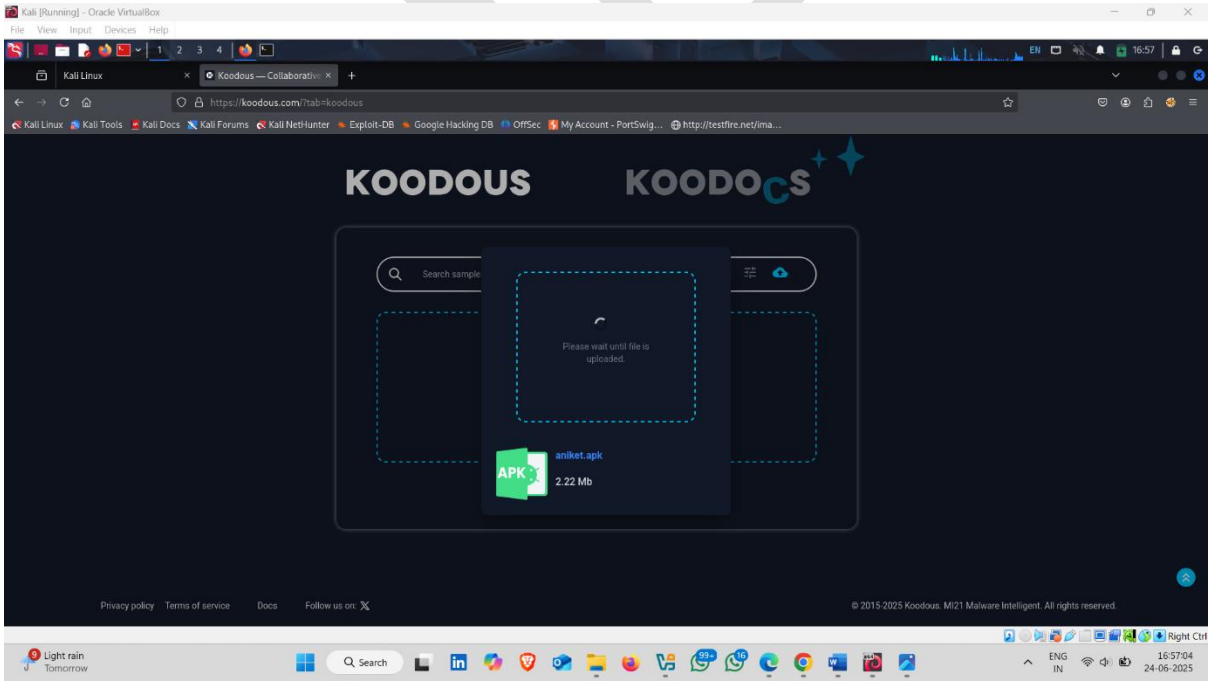
- Click on cloud “ ☁ ” option to upload application



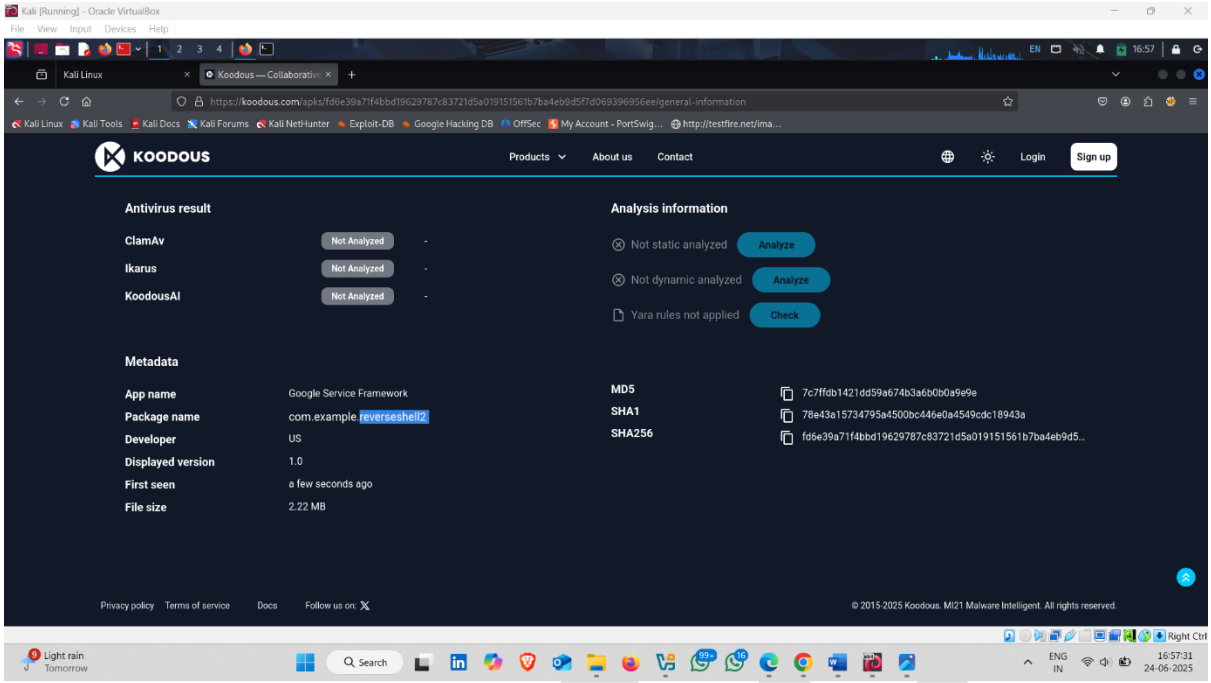
- Click on this pop-up and then select application



- Uploading process start 👇



- Here , meta data and hashesh about application



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)

✅