Creating and Analyzing APK Backdoors: A Comprehensive Guide Using AhMyth

Prepared by

THOMAS A

Intern at

EXTION INFOTECH

May 28, 2024

Table of Contents

Introduction

Stepping into the cybersecurity domain, I delve into the intricate world of mobile security using AhMyth, an open-source remote access tool (RAT) designed to illustrate potential vulnerabilities in Android devices.

As an intern at Extion Infotech, my mission is clear: create and analyze backdoors using AhMyth, investigate their mechanisms, and understand the implications of such vulnerabilities. This project provides me with a unique opportunity to enhance my cybersecurity skills, focusing on the identification and mitigation of mobile threats.

With the support of Extion Infotech and access to essential tools like Ngrok and Genymotion, I navigate the complexities of mobile security, equipped with the knowledge and resources necessary for this endeavor. Together, we embark on a journey to uncover the intricacies of mobile device exploitation, driven by a passion for cybersecurity, a commitment to ethical practices, and an eagerness to learn.

Understanding AhMyth

AhMyth is an open-source RAT designed to remotely control Android devices. It comprises two main components:

1. **AhMyth Server**: The control interface for managing infected devices.
2. **AhMyth Client**: The payload (APK) that is installed on the target device.

Requirements

Before starting, ensure you have the following:

- A computer with Windows, Linux, or macOS.
- Java Development Kit (JDK) installed.
- An Android device or Genymotion emulator for testing.
- Ngrok installed for tunneling.
- AhMyth RAT downloaded from the official GitHub repository (https://github.com/AhMyth/AhMyth-Android-RAT).

Comprehensive Walkthrough

Step 1: Setting Up AhMyth

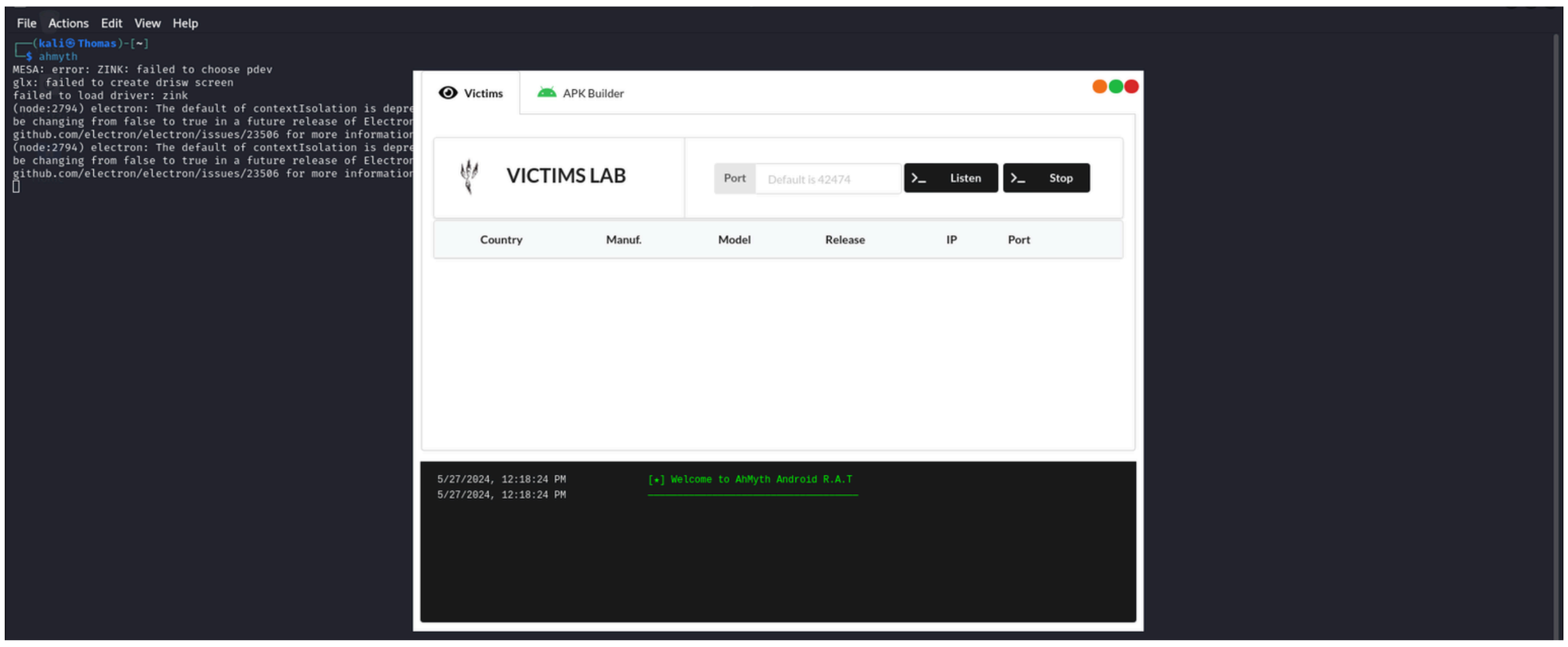
1. Download AhMyth:
    - Visit the AhMyth GitHub repository and download the ZIP file.
2. Extract AhMyth:
    - Extract the downloaded ZIP file to a preferred directory on your computer.

Step 2: Launching the AhMyth Server

1. Open Command Line Interface (CLI):
    - Navigate to the directory where you extracted AhMyth.
2. Start AhMyth Server:
    - Execute the following command to execute Ahmyth server,

```
java -jar AhMyth.jar
```

3. Access AhMyth GUI:
    - The AhMyth graphical user interface (GUI) should now be visible.

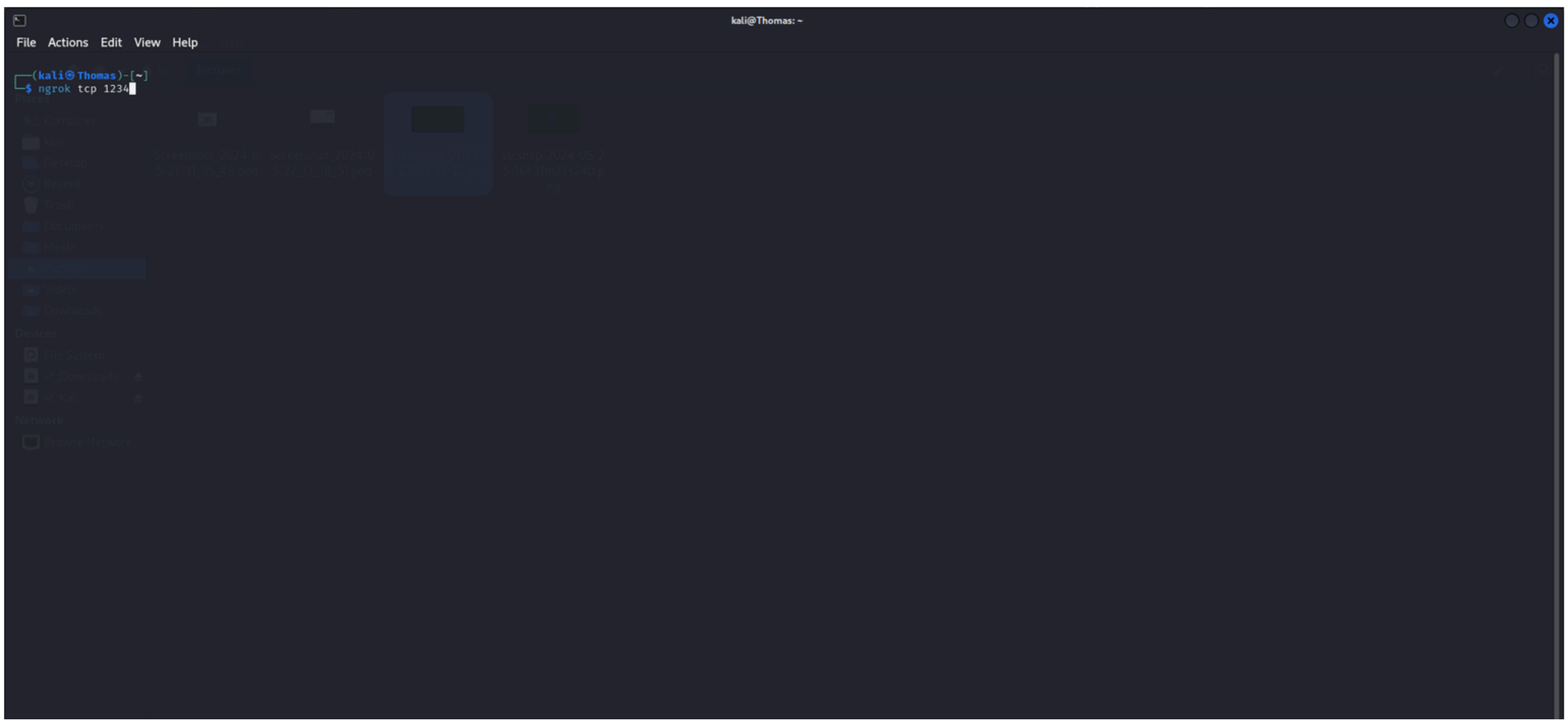


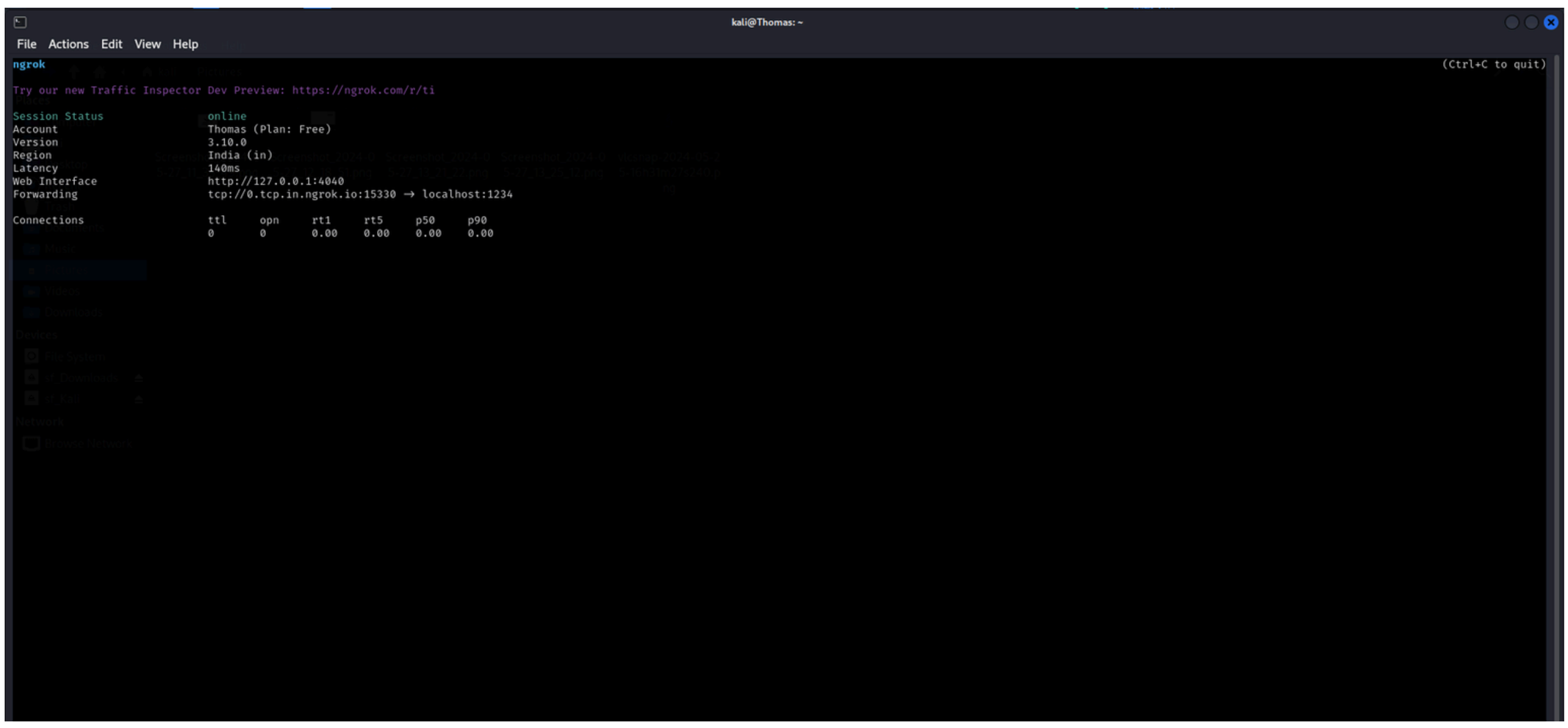
Step 3: Configuring Ngrok for Tunneling

Ngrok is essential for exposing the local server to the internet securely.

1. Download and Install Ngrok:
    - Visit Ngrok's website and download Ngrok.
    - Follow the installation instructions provided on the website.
2. Start Ngrok:
    - Open a terminal or command prompt and navigate to the Ngrok installation directory.
    - Run the following command to start a tunnel on port 1234 (or any desired port):

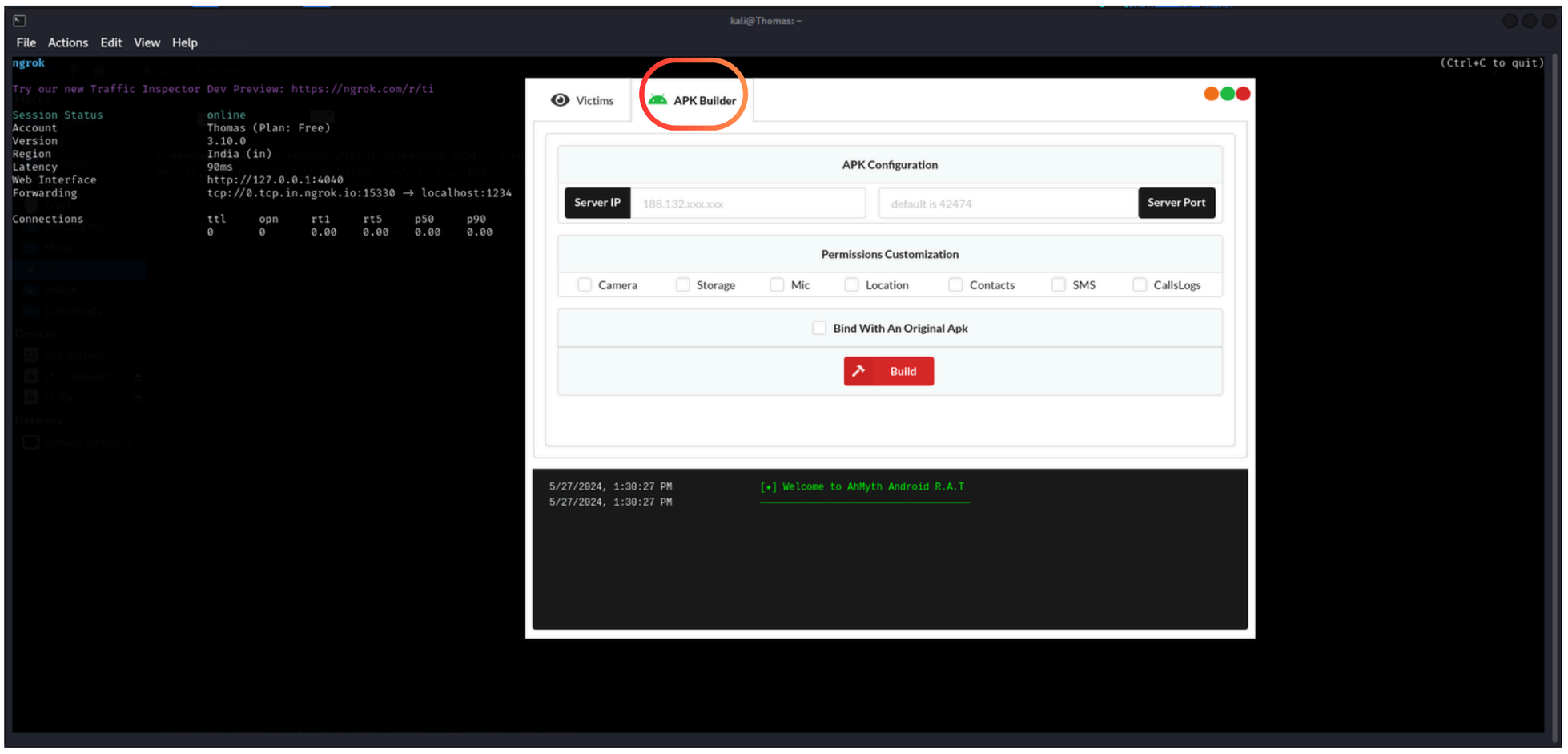
```
./ngrok tcp 1234
```





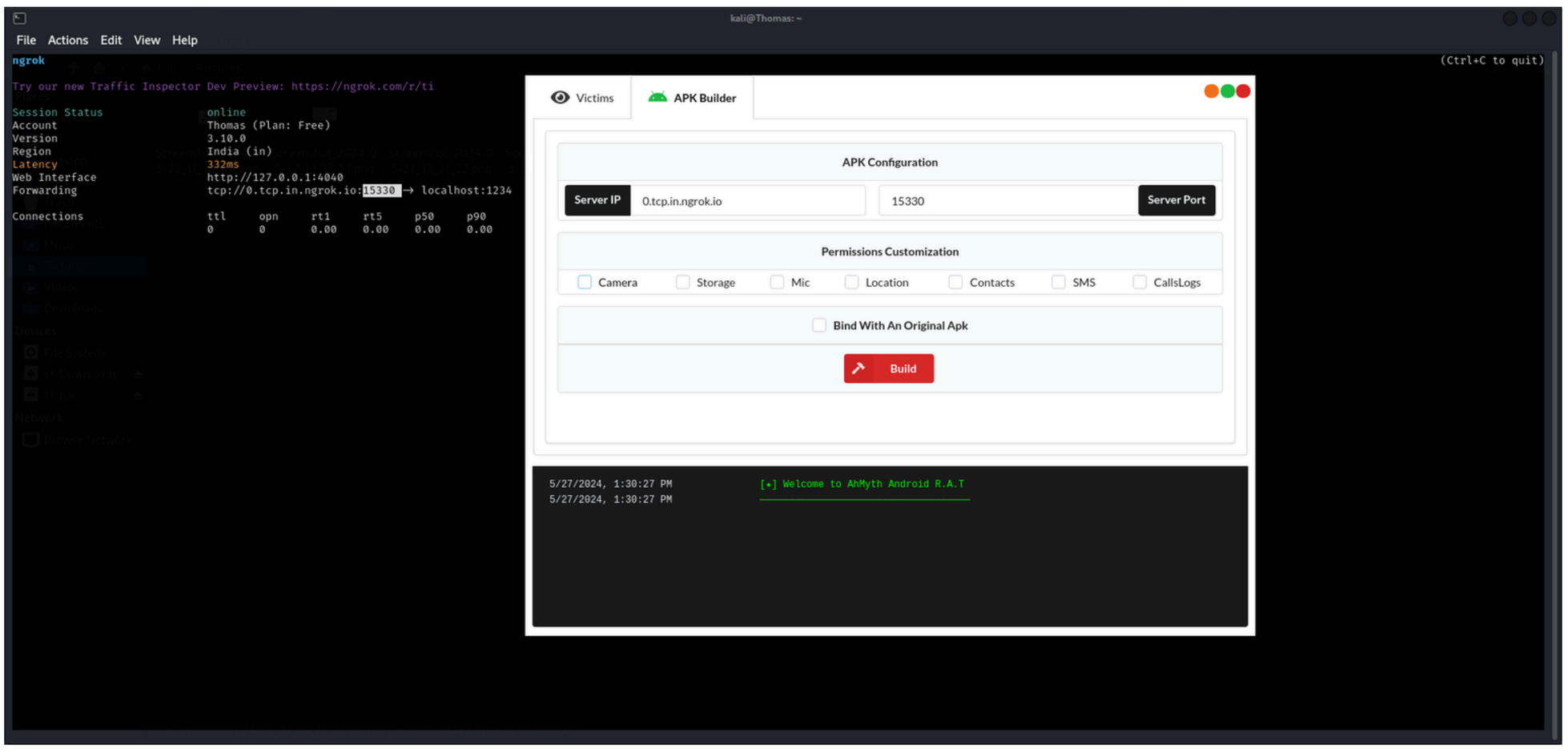
Step 4: Building the Malicious APK

1. Navigate to the APK Builder Tab:
    - In the AhMyth interface, select the “APK Builder” tab.



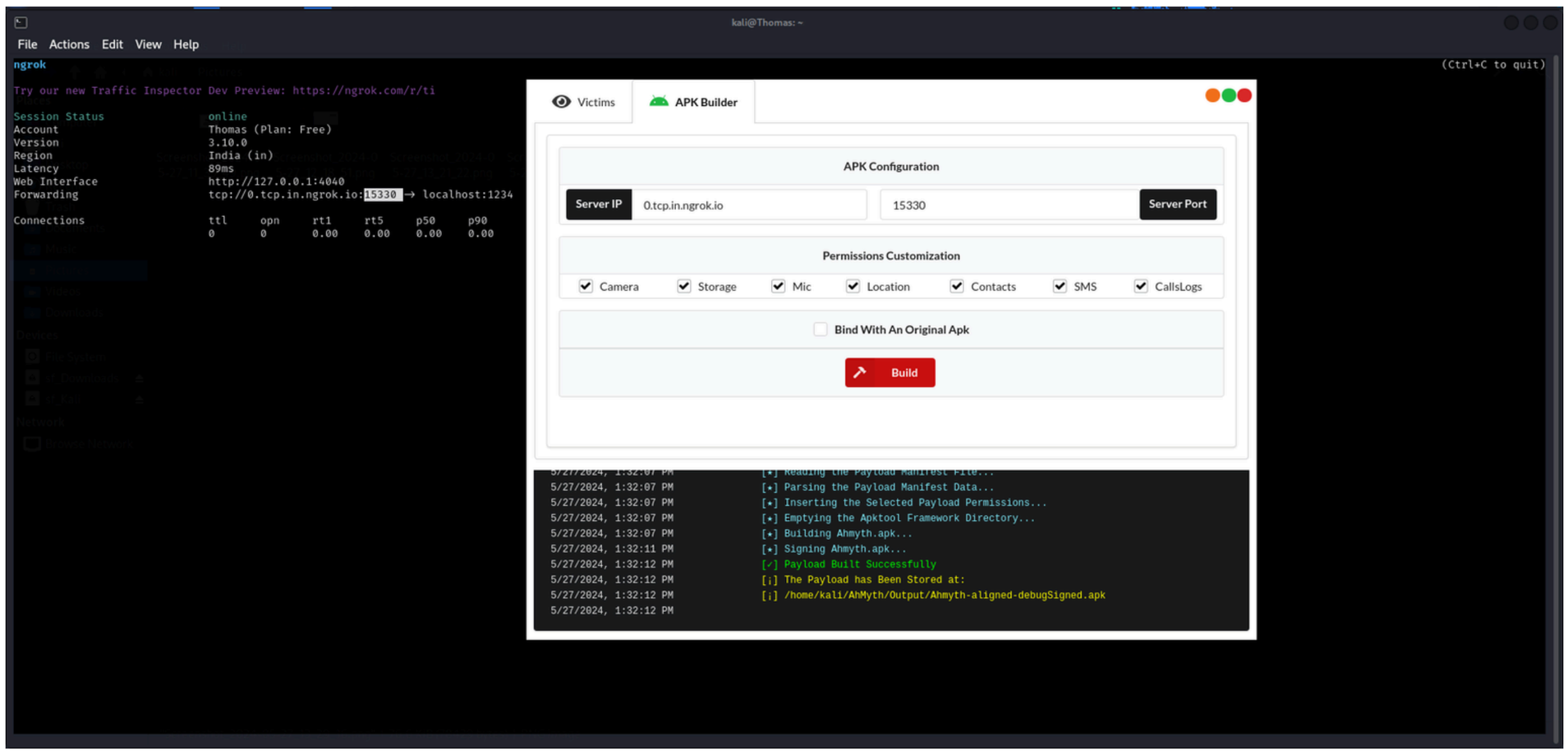
2.Input Configuration Details:

- IP Address: Enter the forwarding address provided by Ngrok (e.g.,0.tcp.ngrok.io).
- Port: Enter the port number provided by Ngrok



3.Generate the APK:

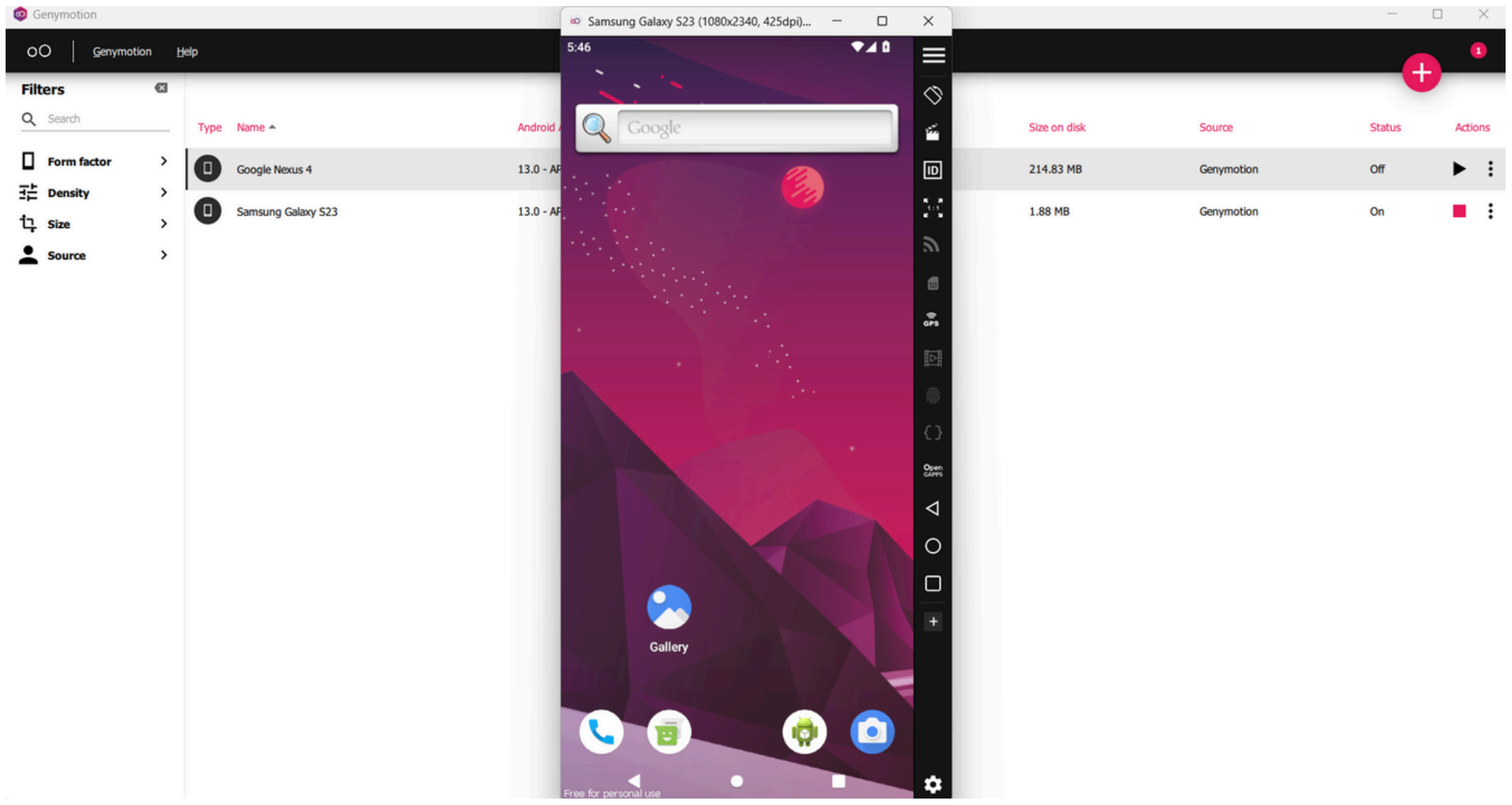
- Click on “Build APK” to create the malicious APK file.
- The APK file will be saved to the specified directory.



Step 5: Setting Up Genymotion Emulator (Victim Device)

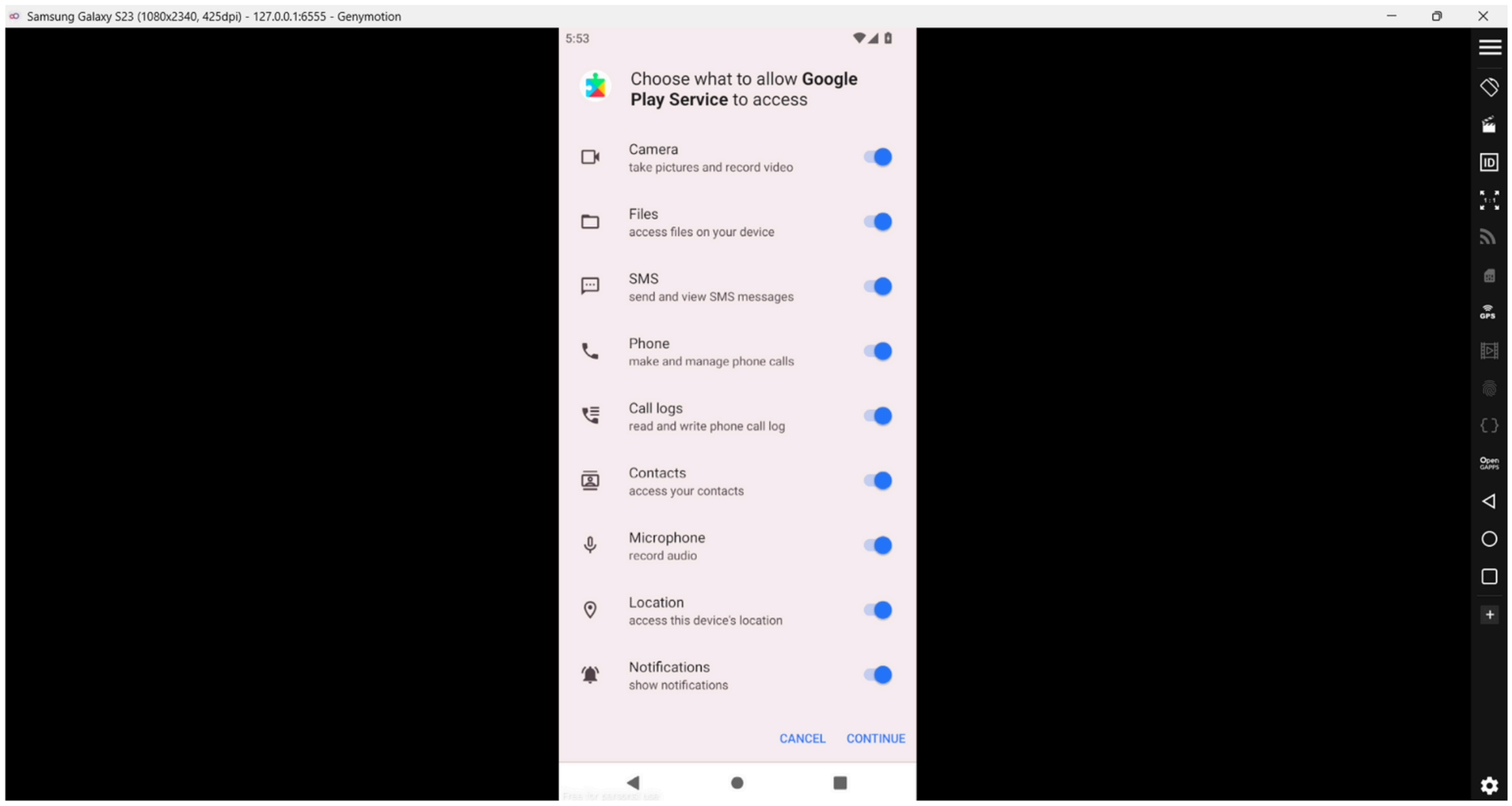
Genymotion is a popular Android emulator that can simulate a target device.

1. Download and Install Genymotion:
   - Visit Genymotion's website and download the emulator.
   - Follow the installation instructions provided on the website.
2. Create a Virtual Device:
   - Open Genymotion and create a new virtual device with your desired Android version.
   - Start the virtual device.



Step 6: Distributing and Installing the APK

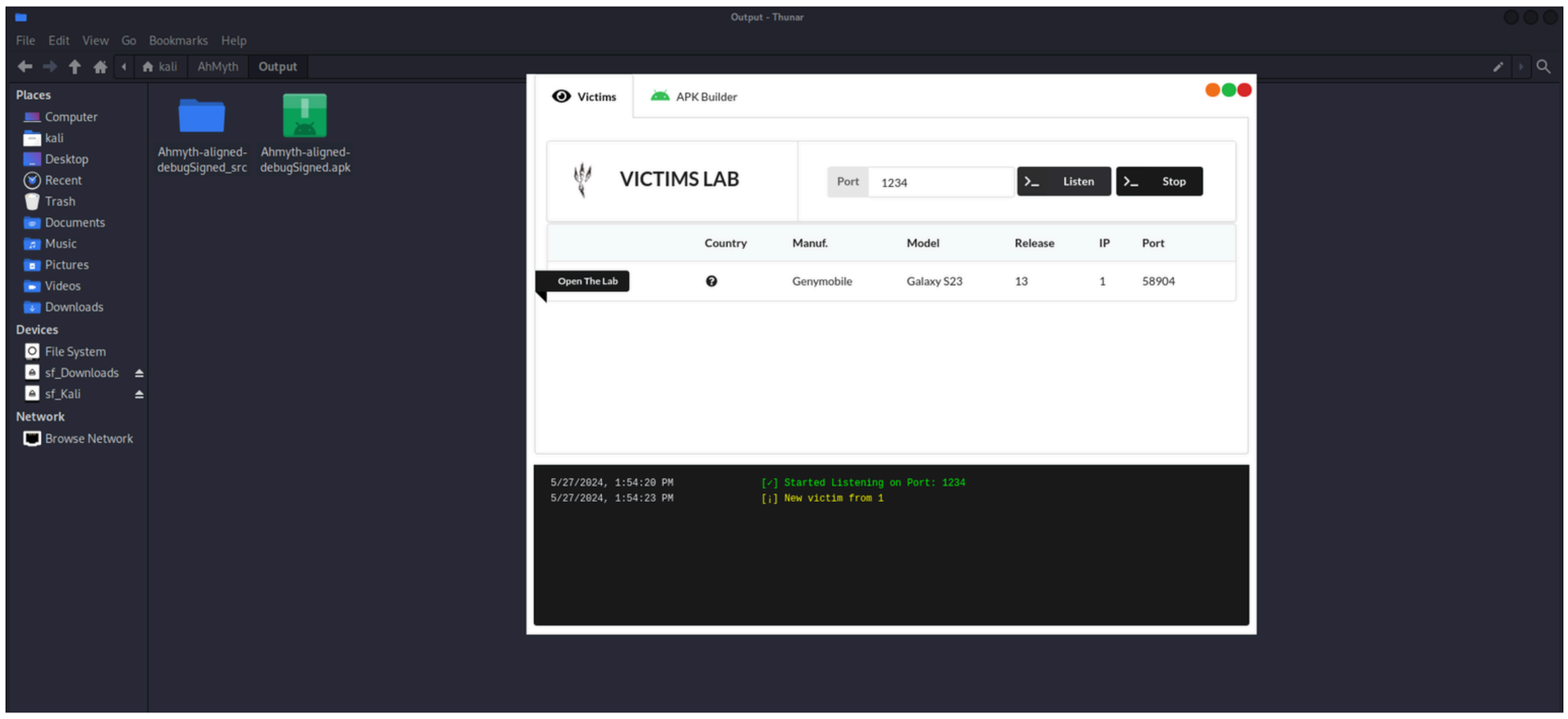
1. Install the APK on Target Device:
    - Transfer the generated APK to the Genymotion emulator
    - Install the APK and grant any necessary permissions requested during installation.



Step 7: Connecting to the Target Device

With the APK installed and the target device online, you can connect to it using the AhMyth server.

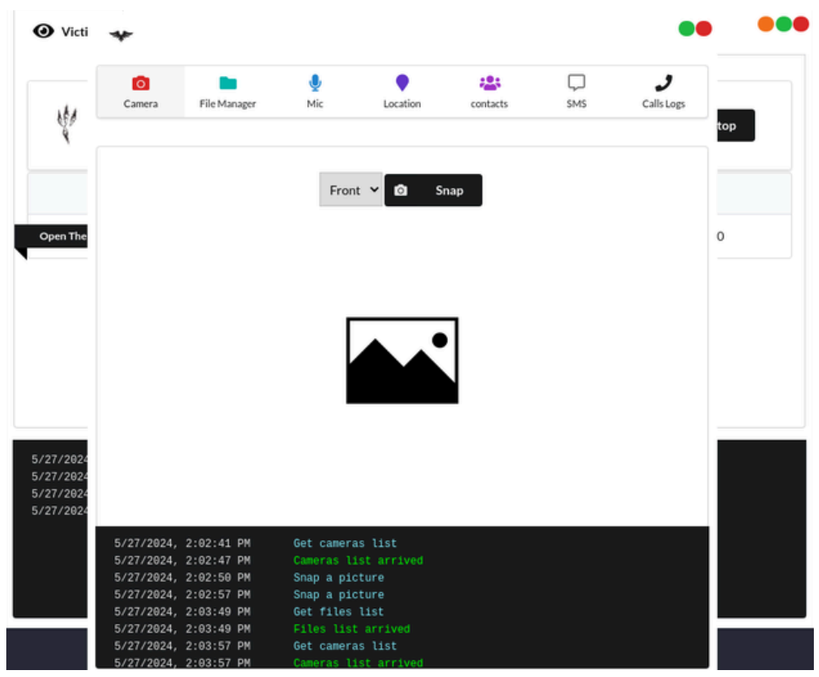
1. Open the AhMyth Interface:
    - Return to the AhMyth server interface.
2. Identify the Target Device:
    - The infected device should appear in the “Victims” tab once it’s online.
3. Establish a Remote Session:
    - Select the device and initiate a remote session

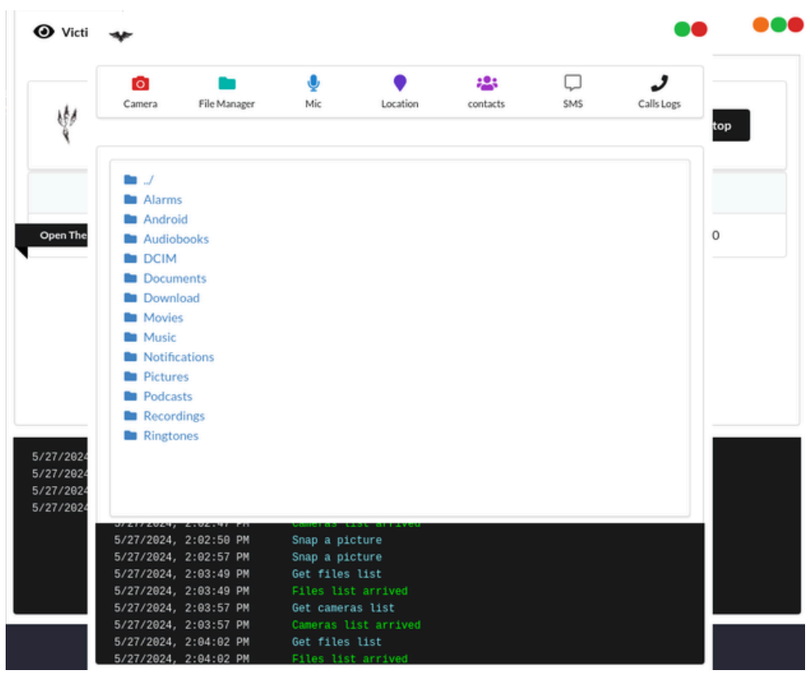


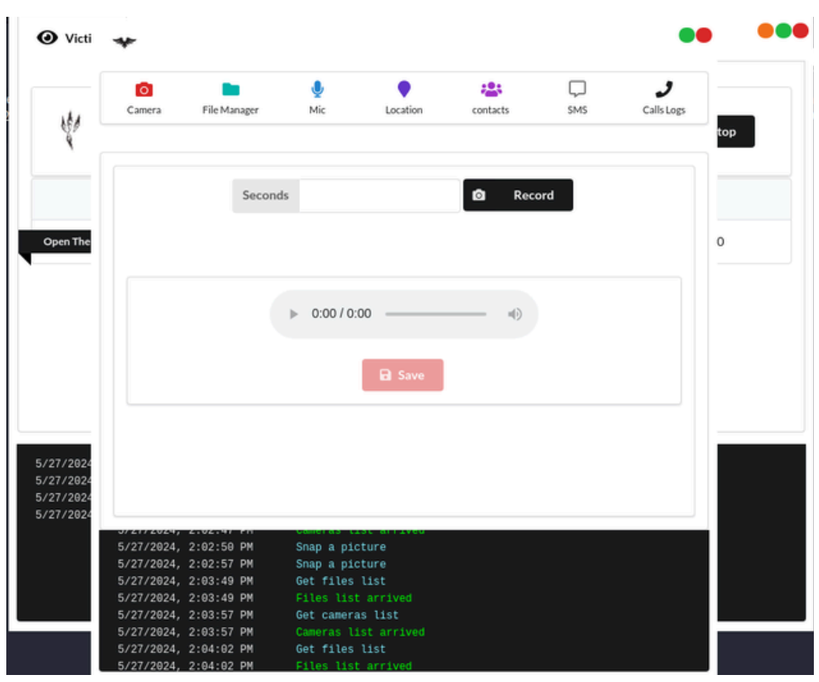
Step 8: Exploring AhMyth's Capabilities

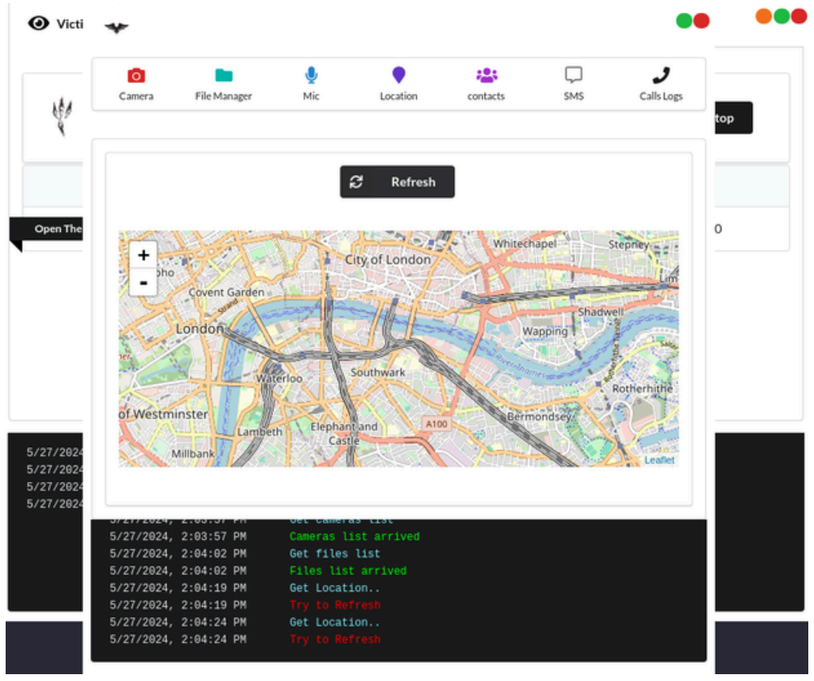
Once connected, you can demonstrate various features of AhMyth.

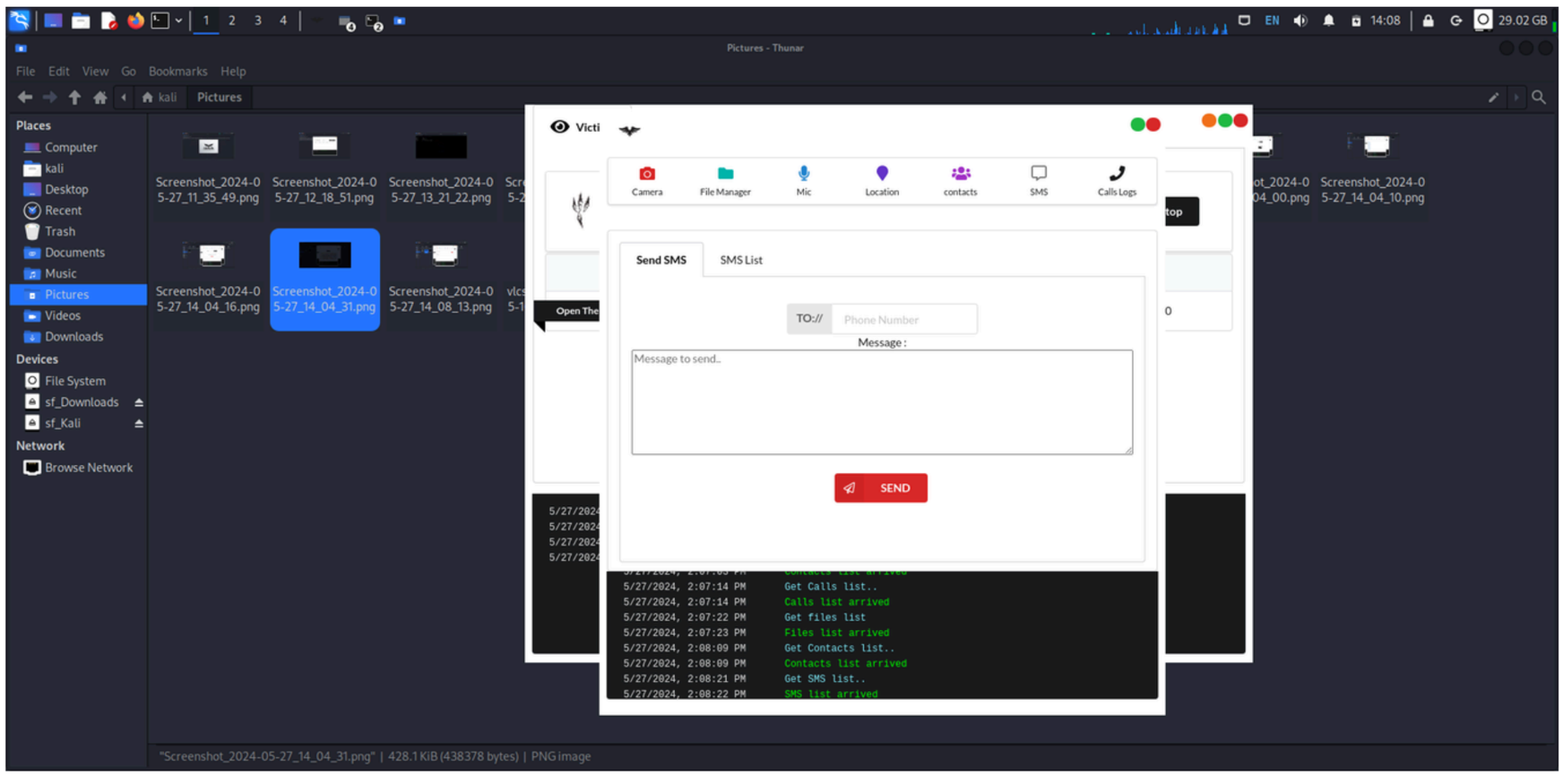
1. File Management:
    - Access and manage files on the infected device.
2. SMS and Call Logs:
    - Read SMS messages and view call logs.
3. Location Tracking:
    - Track the device’s location.
4. Remote Control:
    - Execute commands, take pictures, record audio, etc.

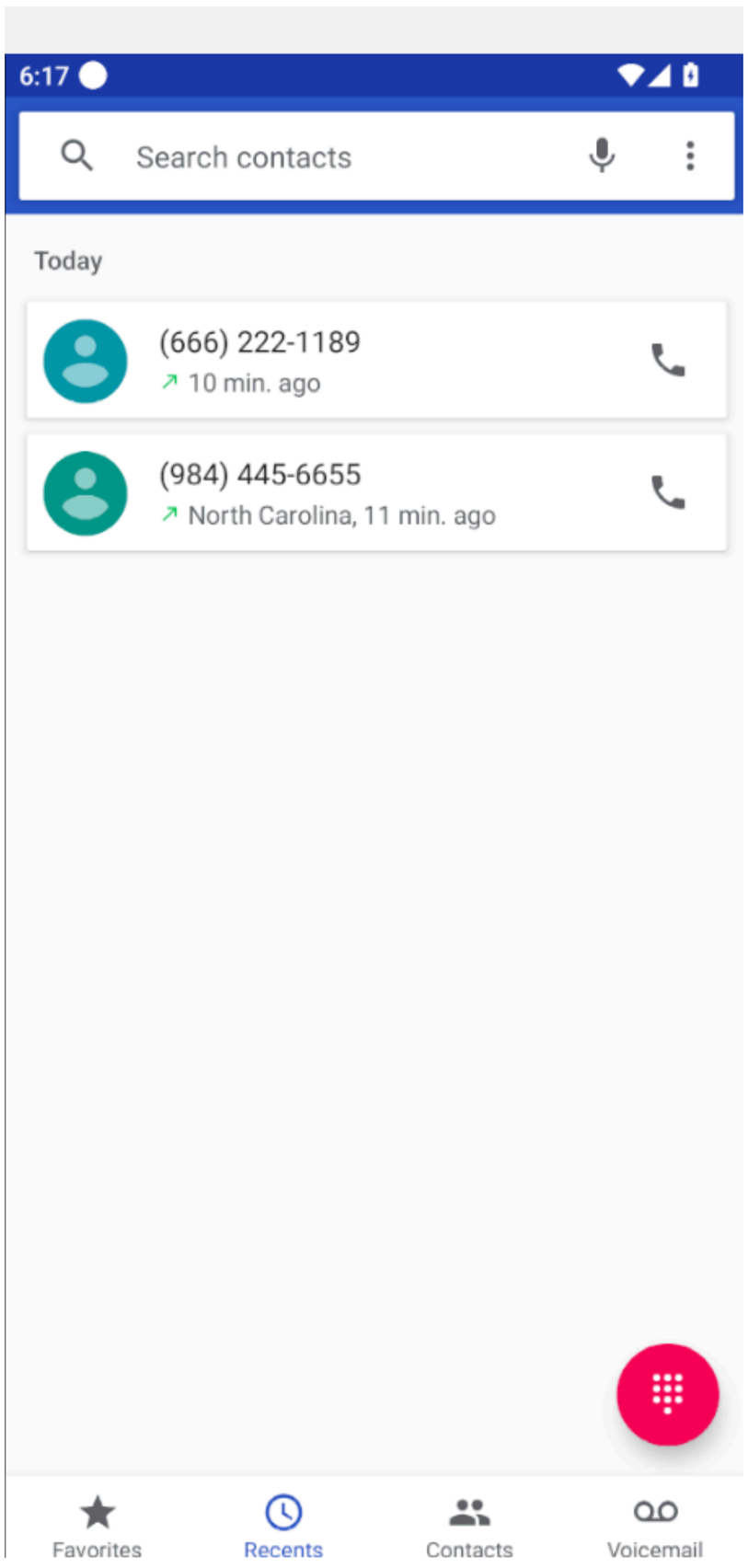


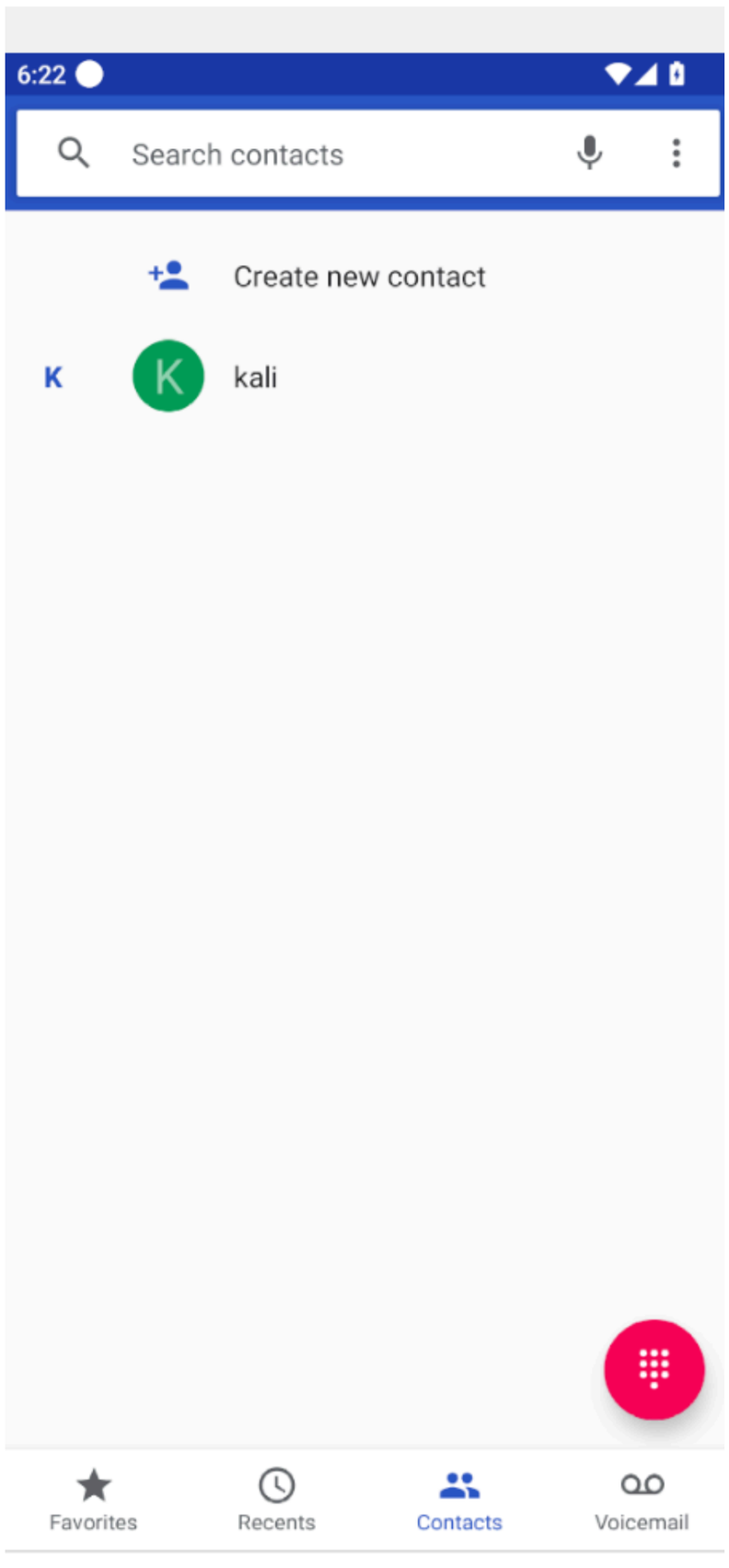


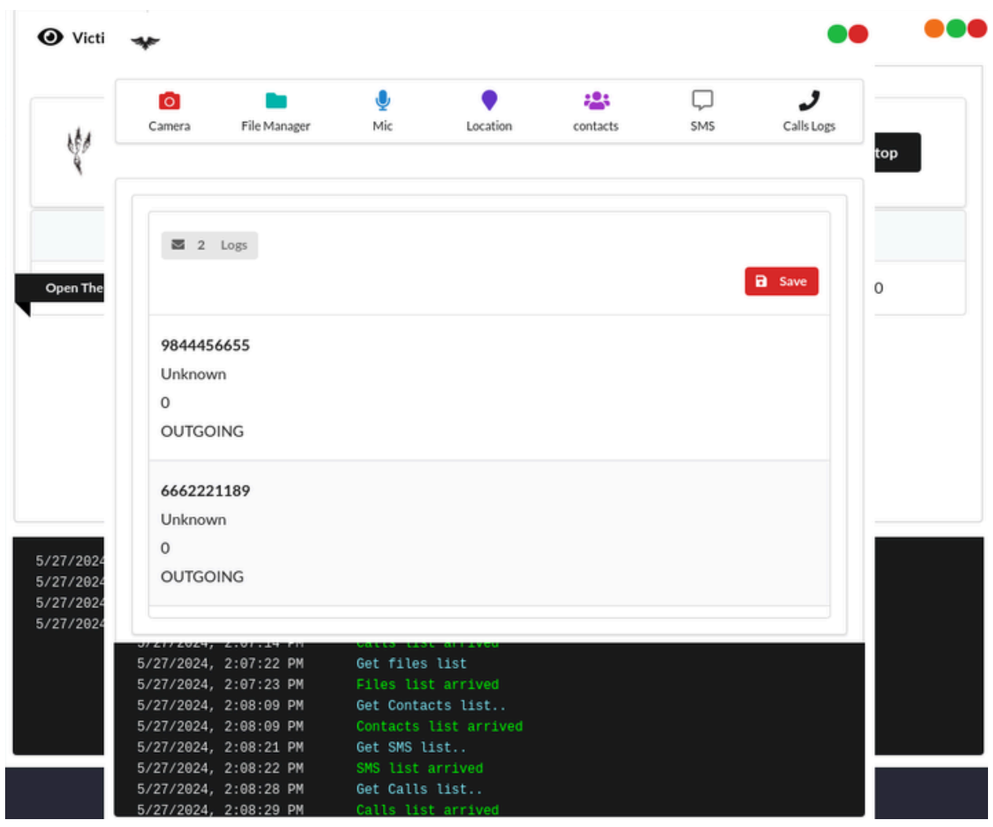


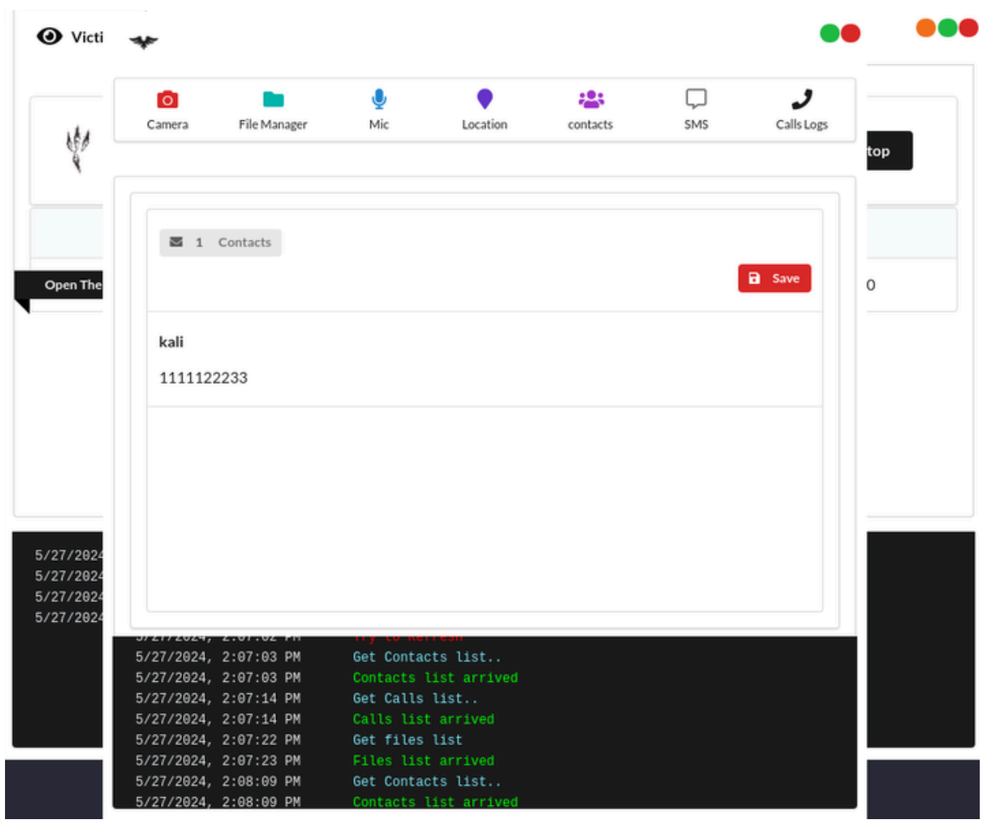





6:17
Search contacts
Today
(666) 222-1189
10 min. ago
(984) 445-6655
North Carolina, 11 min. ago
Favorites
Recents
Contacts
Voicemail


6:22
Search contacts
Create new contact
K
kali
Favorites
Recents
Contacts
Voicemail


Victi
Camera
File Manager
Mic
Location
contacts
SMS
Calls Logs
2 Logs
Save
9844456655
Unknown
0
OUTGOING
6662221189
Unknown
0
OUTGOING
5/27/2024, 2:07:22 PM Get files list
5/27/2024, 2:07:23 PM Files list arrived
5/27/2024, 2:08:09 PM Get Contacts list..
5/27/2024, 2:08:09 PM Contacts list arrived
5/27/2024, 2:08:21 PM Get SMS list..
5/27/2024, 2:08:22 PM SMS list arrived
5/27/2024, 2:08:28 PM Get Calls list..
5/27/2024, 2:08:29 PM Calls list arrived


Victi
Camera
File Manager
Mic
Location
contacts
SMS
Calls Logs
1 Contacts
Save
kali
1111122233
5/27/2024, 2:07:03 PM Get Contacts list..
5/27/2024, 2:07:03 PM Contacts list arrived
5/27/2024, 2:07:14 PM Get Calls list..
5/27/2024, 2:07:14 PM Calls list arrived
5/27/2024, 2:07:22 PM Get files list
5/27/2024, 2:07:23 PM Files list arrived
5/27/2024, 2:08:09 PM Get Contacts list..
5/27/2024, 2:08:09 PM Contacts list arrived

Defense and Mitigation Strategies

Understanding how to protect against such intrusions is crucial. Effective defense mechanisms and strategies can significantly reduce the risk of unauthorized access and potential data breaches. Educating peoples on the following essential practices to enhance security:

1.Application Verification

- Install Apps from Trusted Sources: Emphasize the importance of downloading and installing apps only from official app stores such as Google Play Store for Android devices. Third-party app stores or direct downloads from unknown sources can host malicious applications that pose significant security risks.
- Check Developer Credentials: Before installing an app, verify the developer's credibility by checking their ratings, reviews, and other apps they have developed. Reputable developers are less likely to distribute malicious software.

2.Permissions Management

- Regularly Review App Permissions: Educate students on the importance of periodically reviewing the permissions granted to installed apps. Excessive or unnecessary permissions can be a red flag indicating potential malicious intent.
- Limit Permissions to Necessity: Encourage the principle of least privilege by only granting permissions that are essential for the app's functionality. For example, a simple game app should not need access to contacts, camera, or microphone.

3.Antivirus Software

- Use Reputable Antivirus Solutions: Install and maintain reliable antivirus software on devices. These programs can detect, quarantine, and remove malware, including backdoors, thereby providing an additional layer of security.
- Regular Scans and Updates: Schedule regular scans and ensure that the antivirus software is always up to date. Antivirus databases need to be updated frequently to recognize and mitigate new threats.

4.Security Updates

- Keep the OS and Apps Updated: Security vulnerabilities in the operating system and applications are often exploited by attackers. Regularly updating the OS and apps ensures that the latest security patches are applied, minimizing the risk of exploitation.
- Enable Automatic Updates: Where possible, enable automatic updates to ensure that security patches are applied promptly without requiring manual intervention.

Conclusion

- This comprehensive guide has outlined the process of creating and deploying a backdoor using tools like AhMyth and Ngrok. By exploring these methods, individuals can gain a deeper understanding of how such intrusions are executed, which is critical for developing effective cybersecurity measures. It is essential to emphasize the ethical and legal implications of using these tools, ensuring they are employed responsibly to enhance security rather than exploit vulnerabilities.
- During my internship at Extion Infotech, I have gained valuable insights into ethical hacking practices and the importance of adhering to legal guidelines in the pursuit of a more secure digital environment. The support and resources provided by Extion Infotech have been instrumental in enhancing my understanding and skills in cybersecurity.

References

- AhMyth GitHub Repository: https://github.com/AhMyth/AhMyth-Android-RAT
- Ngrok: https://ngrok.com/
- Genymotion: https://www.genymotion.com/