Internship Report for NullClass

Name: Mannava Sai Bhavana
Internship Duration: September 9, 2024 – October 9, 2024
Mentor/Organization: NullClass
Role: Cybersecurity Intern
NullClass Username: SAI BHAVANA MANNAVA

4. Activities and Tasks

Task 2: Configure Device Policies

Description:

This task involved guiding users through the process of configuring Android device policies. Device policies are crucial for ensuring that mobile devices operate within secure parameters, such as requiring a passcode, controlling Wi-Fi settings, and restricting applications. I walked users through each step of configuring these policies in a virtual Android device using Genymotion.

Prerequisites:

Before initiating the configuration process, I ensured the following prerequisites were met:

1. **Genymotion Setup**: A functioning Genymotion environment with an Android Virtual Device (AVD) running at least Android version 6.0.
2. **Android Studio**: Installed to facilitate the configuration and installation of necessary applications.
3. **Device Policy Controller (DPC) Application**: The "Test DPC" application was required to enable device policy management.

Steps:

1. Setting Up the Virtual Android Device in Genymotion
    - Launching Genymotion: I opened Genymotion and selected a virtual device compatible with the required Android version.
    - Starting the Device: By clicking the "Play" button, the device was launched successfully.
    - Enabling Developer Options:
        - I navigated to **Settings** > **About Phone** and tapped on **Build Number** seven times to activate Developer Mode.
        - I then accessed **Settings** > **Developer Options** and ensured that **USB Debugging** was enabled to facilitate further configurations.
2. Installing the Test DPC App

- Downloading the APK: I obtained the "Test DPC" APK file from a trusted source.
- Installing the APK: The APK was installed by dragging and dropping the file into the running Genymotion virtual device window, which automatically initiated the installation.

3. Configuring Device Admin for Test DPC
    - Launching Test DPC: After installation, I opened the Test DPC application.
    - Setting Up as Device Owner: I selected the option to **Set Up as Device Owner**, allowing Test DPC to manage device policies. This step was crucial for enabling administrative privileges.
4. Creating a Passcode Policy
    - Accessing Password Policies: I launched Test DPC and navigated to **Password Policies** from the main menu.
    - Configuring Password Quality:
        - I selected Set Password Quality and chose the desired complexity level (e.g., Alphanumeric).
        - Additional passcode rules such as minimum length and maximum failed attempts were set.
    - Applying the Policy: Upon applying the policy, the virtual device prompted me to establish a passcode that adhered to the specified requirements.
5. Configuring Wi-Fi Settings
    - Navigating Wi-Fi Configurations: Within Test DPC, I selected **Wi-Fi Configurations**.
    - Adding a Wi-Fi Network:
        - I clicked on Add Wi-Fi Network, entering the SSID (e.g., "MyWiFi") and selecting the appropriate security type (WPA/WPA2-Personal).
        - I entered the network password and saved the configuration.
    - Issue Encountered: Initially, the **Add Wi-Fi Network** option did not appear. To resolve this, I manually accessed the Wi-Fi settings using the ADB command:
      "adb shell am start -n com.android.settings/.wifi.WifiSettings "
      This command successfully opened the Wi-Fi settings, enabling me to add the network.
6. Setting Up App Restrictions
    - Navigating to Application Restrictions: I returned to the Test DPC main menu and selected **Application Restrictions**.
    - Restricting Apps:
        - I chose specific apps to restrict, such as Gallery, and configured their permissions to limit access.
7. Reviewing Configurations
    - Testing Configurations:
        - To verify the passcode policy, I locked the virtual device and attempted to unlock it using the newly set passcode.

- I also checked the Wi-Fi settings to confirm the network was correctly applied, ensuring it displayed "Connected" next to the SSID.
- I tested restricted apps to ensure that they were inaccessible as per the configured restrictions.

Troubleshooting Challenges Faced:

Throughout the configuration process, I encountered several issues:

a. **Blank Screen After Locking Device**: After accidentally clicking on the "Lock Now" option, I experienced a blank screen. To recover, I restarted the virtual device by navigating to **Settings** > **Developer Options** and using the **Reboot** option.
b. **Errors in Setting Device Owner**: Initially, I faced difficulties in establishing Test DPC as the device owner. I resolved this by executing the following commands in the ADB shell:
"adb shell dpm remove-active-admin com.afwsamples.testdpc/.DeviceAdminReceiver"
"adb uninstall com.afwsamples.testdpc"
"adb install path_to_test_dpc.apk"
"adb shell dpm set-device-owner com.afwsamples.testdpc/.DeviceAdminReceiver"
This sequence ensured that Test DPC was correctly set as the device owner.

The exercise of configuring device policies using Genymotion equipped me with practical skills in Android Device Management. I successfully set up passcode requirements, Wi-Fi configurations, and app restrictions while effectively troubleshooting various challenges. This experience will be invaluable for future endeavors in mobile device management and security.

9. Conclusion

This project allowed me to gain hands-on experience with mobile device management through virtualized Android environments. By configuring passcode policies, Wi-Fi settings, and app restrictions, I was able to simulate real-world scenarios where enterprises manage security policies for their devices.

The project enhanced my understanding of Android Device Policy Management and how organizations can enforce compliance standards. Additionally, troubleshooting the various issues helped me develop strong problem-solving skills, which are essential for managing complex technical tasks in a dynamic environment.

Overall, this task provided practical insights into mobile security management, and I gained valuable skills in configuring device policies, which will be beneficial for my future roles in cybersecurity and mobile device management.

10. Appendix

Task 2: Configure Device Policies

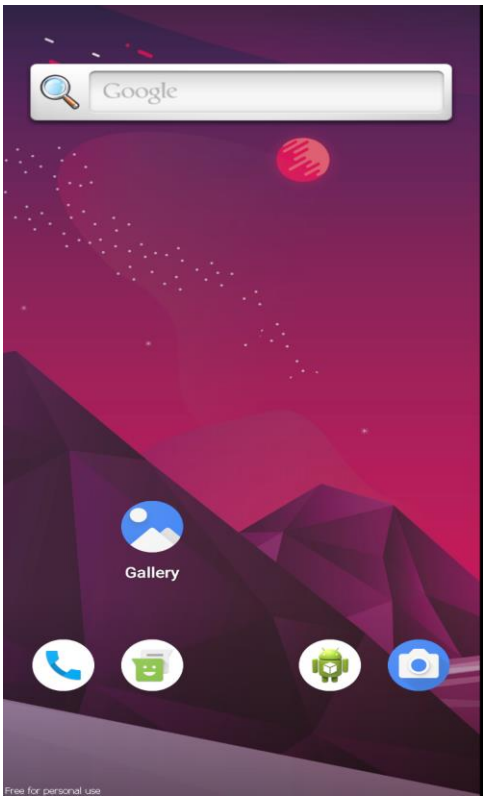

Figure 1: Virtual Android device in Genymotion

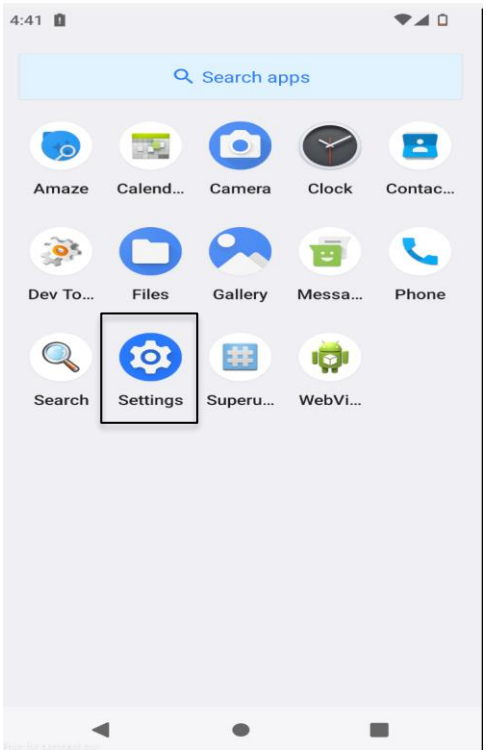

Figure 2: Open Settings

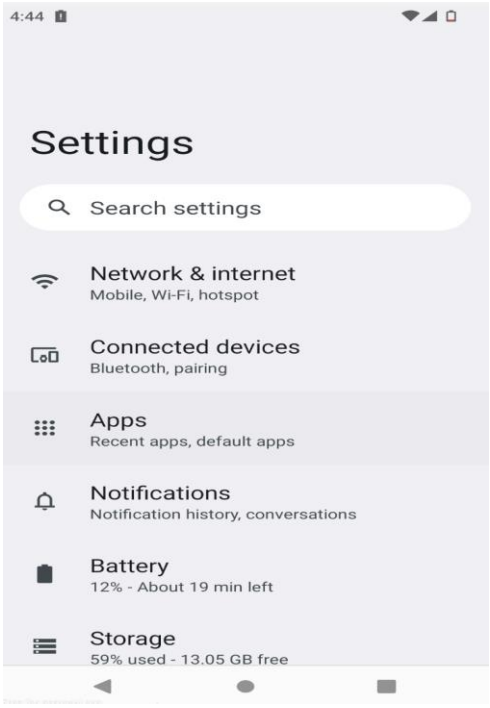

Figure 3: Settings options on device

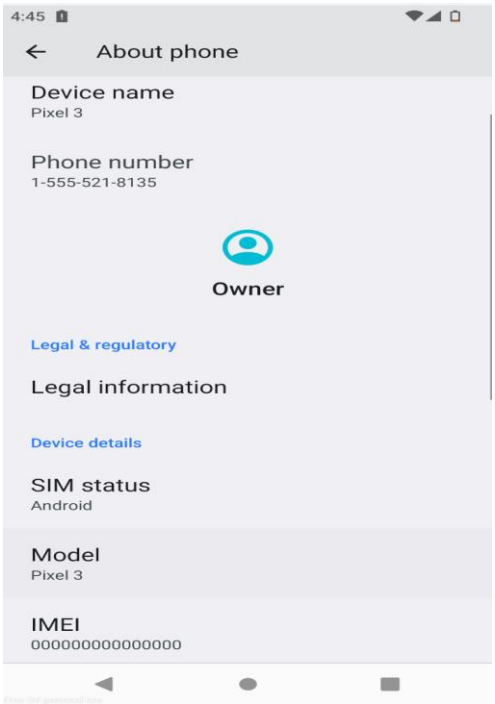

Figure 4: About Phone option in settings

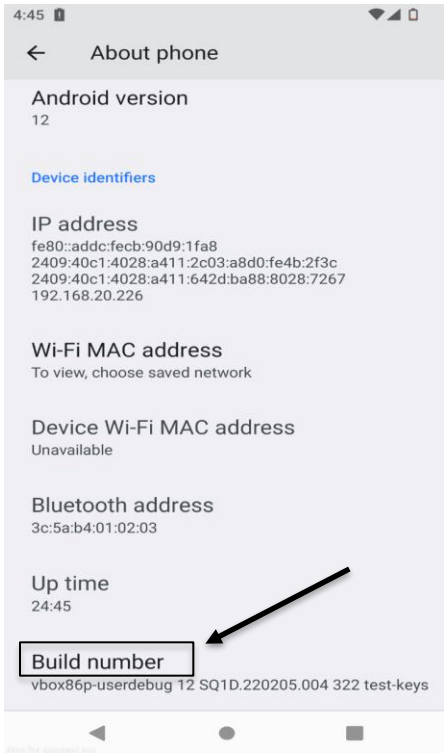

Figure 5: When we scroll down we will have this option.

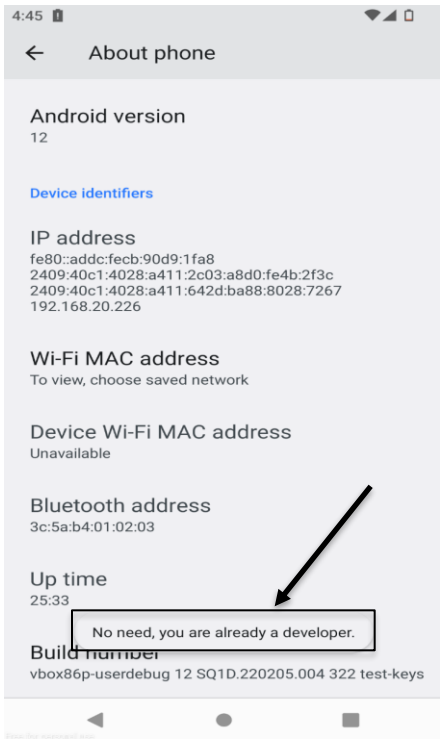

Figure 6: You need to click several times on the option to get that you are developer.

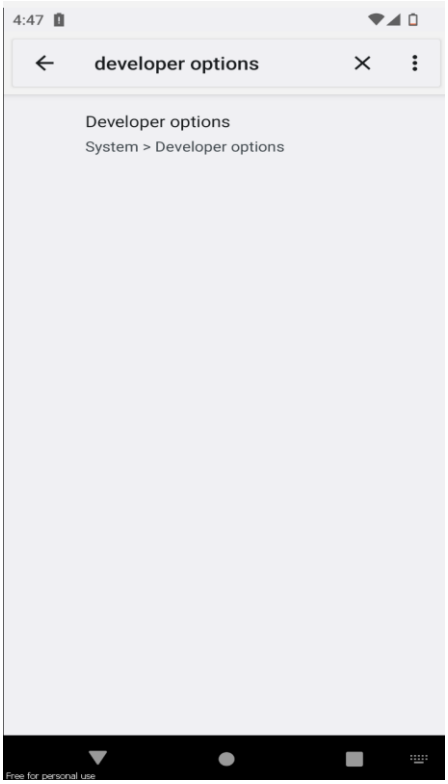

Figure 7: Now in phone settings search the above developer options

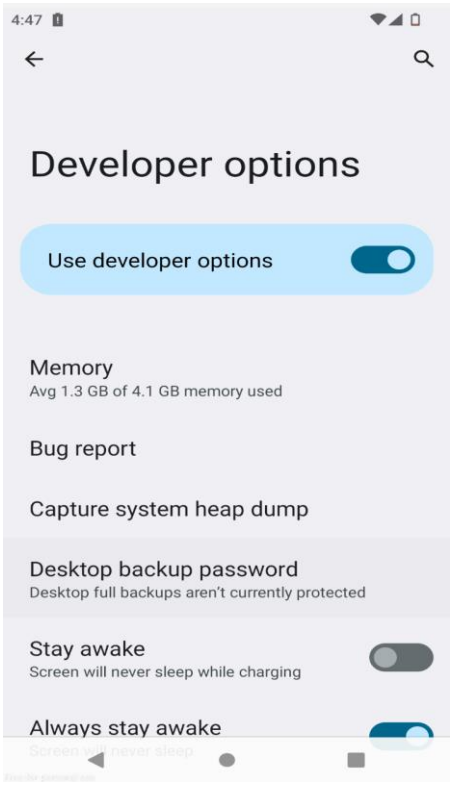

Figure 8: When you click that Developer options you willl get these few more options.

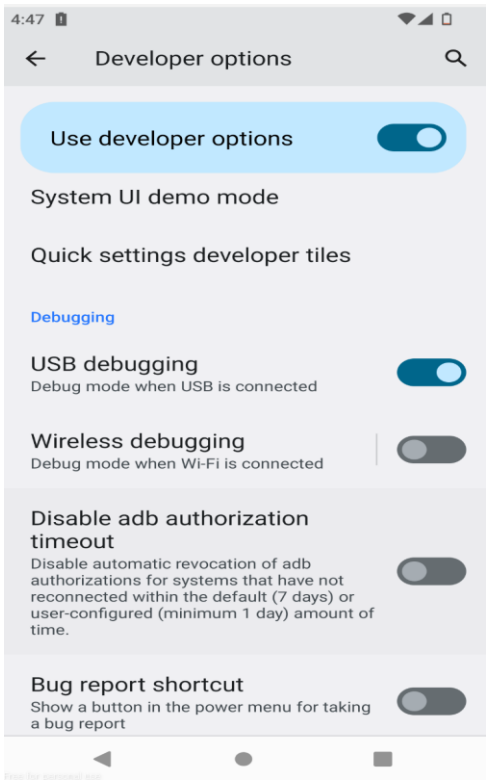

Figure 9: Enable USB debugging

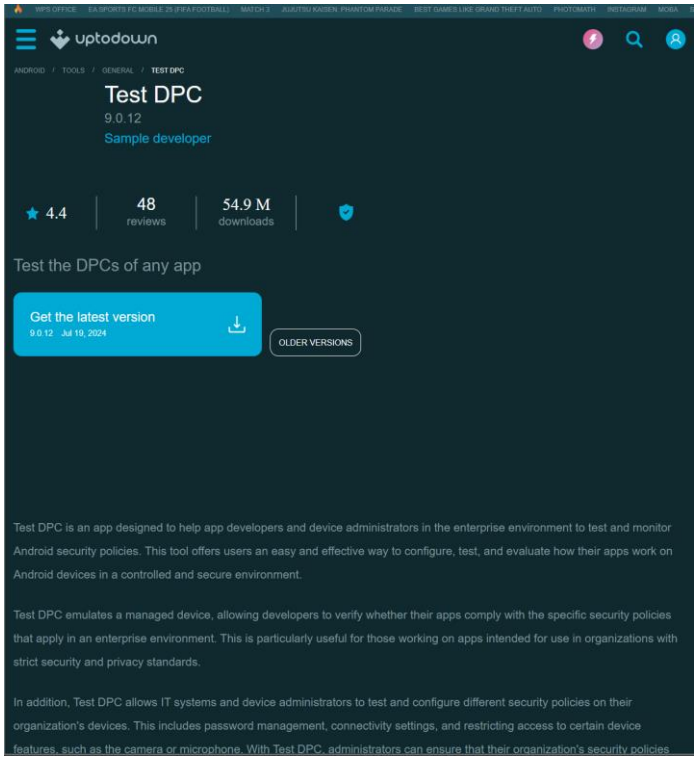

Figure 10: Download this TestDPC.apk file

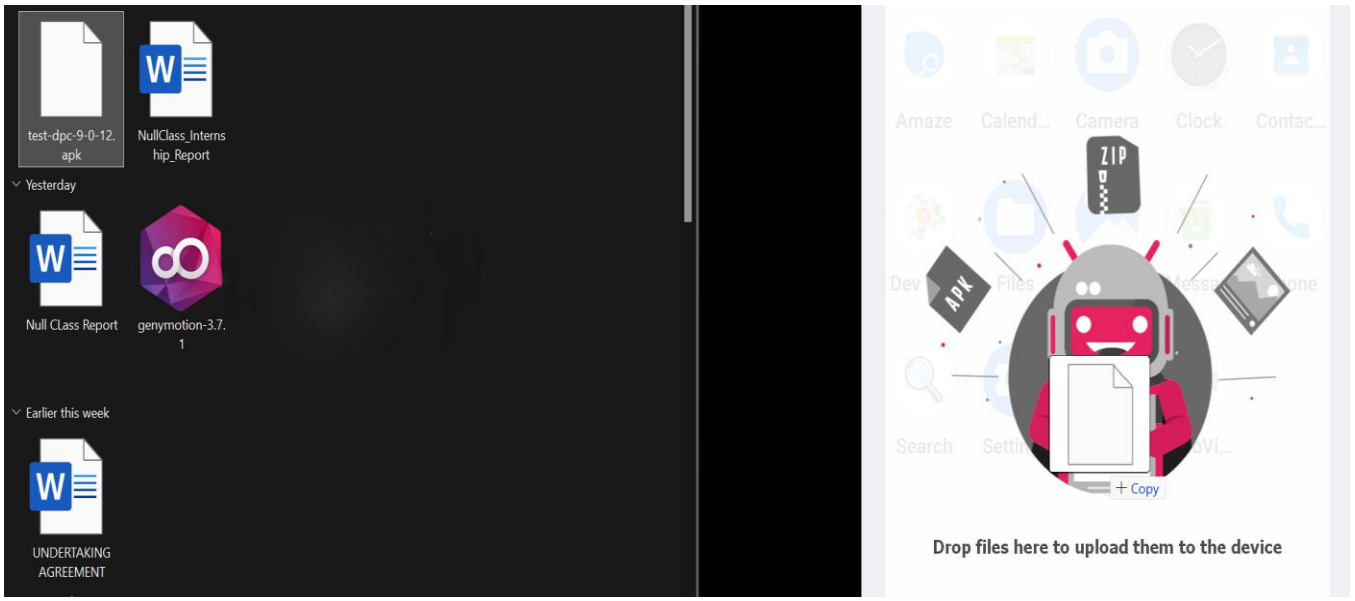

Figure 11: Now Drag and drop the apk file into the virtual device

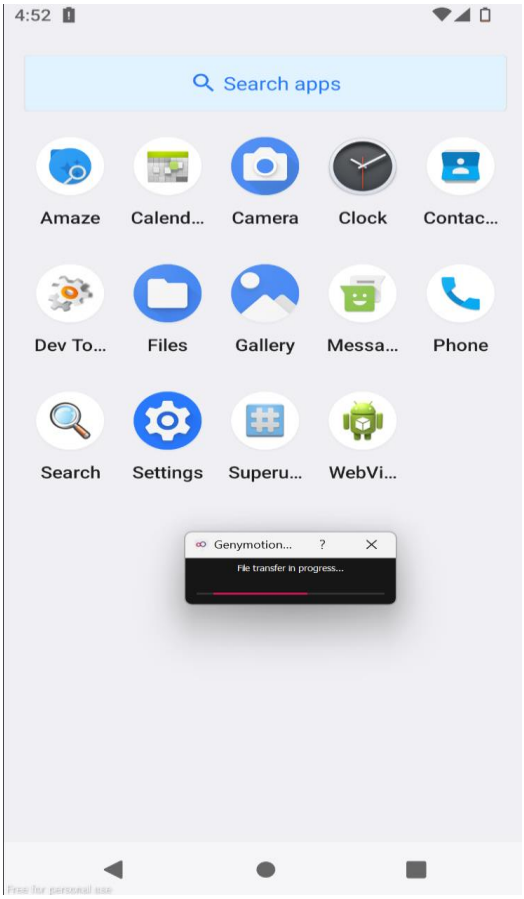

Figure 12: The File transfer is in progress

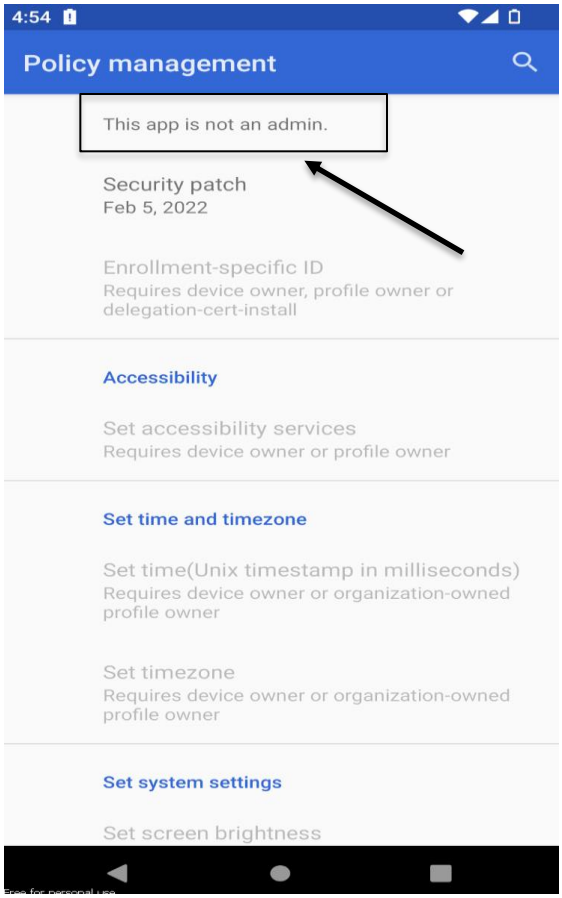

Figure 13: After Completion of transfer when we open the app we will get like highlighted

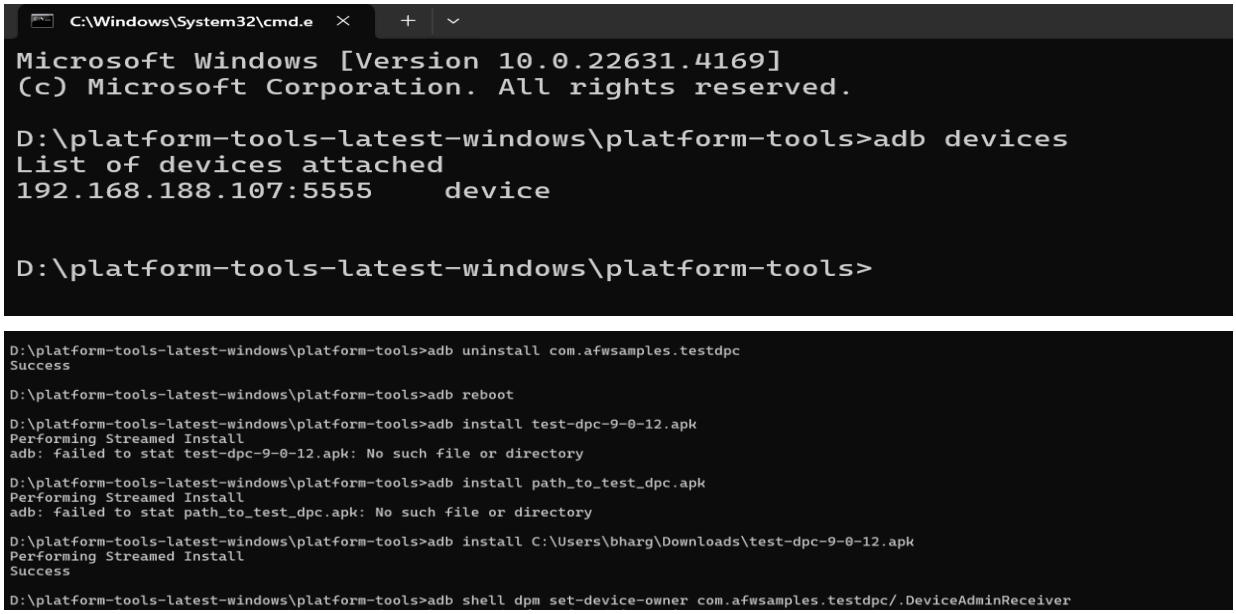

Figure 14: In first pic we have seen that device is connected or not via adb . The second pic is to troubleshoot the first issue that is showed in Fig 13

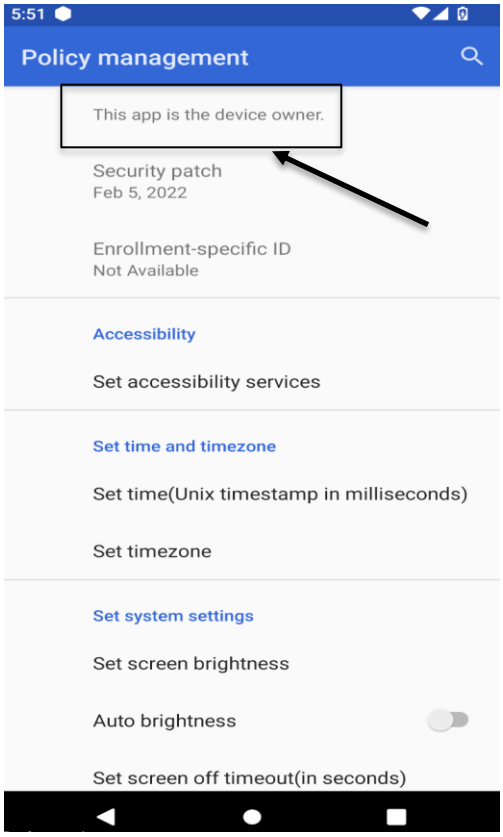

Figure 15: After troubleshooting it showed like this.

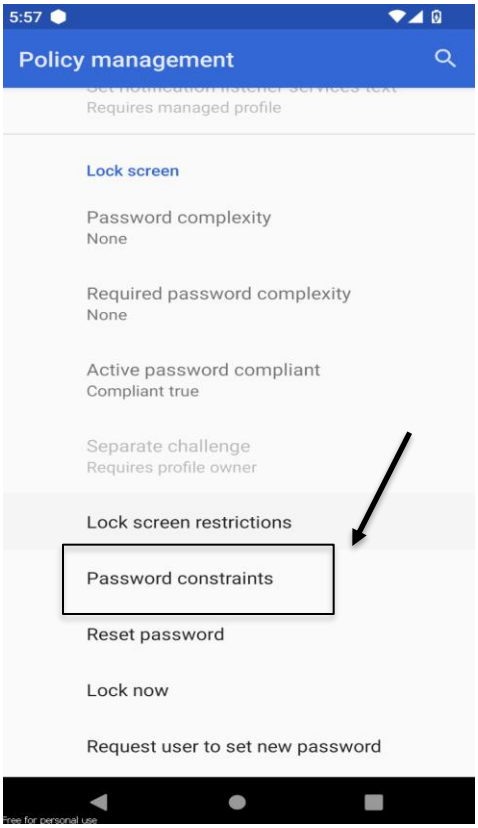

Figure 16: We are going to change the password policies.

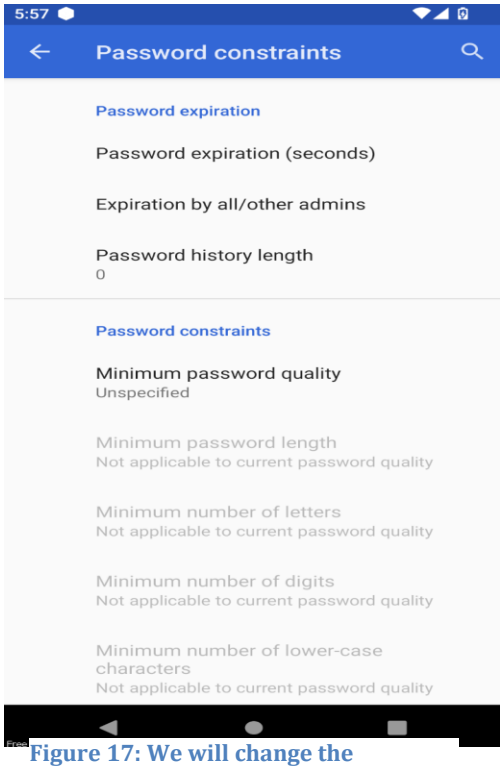

Figure 17: We will change the Password constraints.

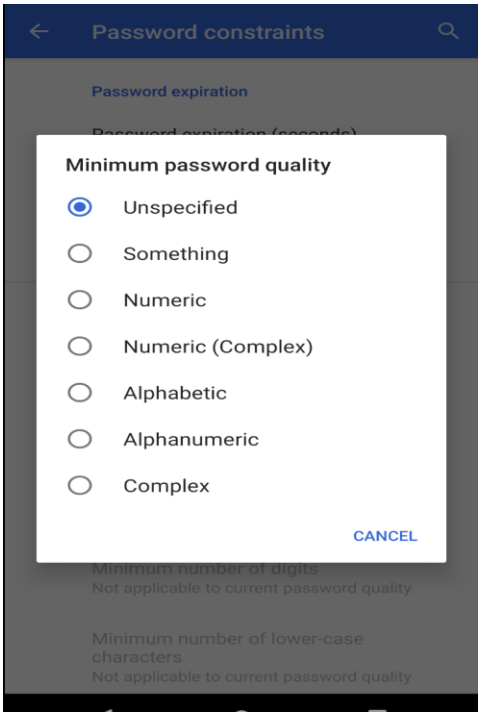

Figure 18: We need to select password quality type which you prefer.

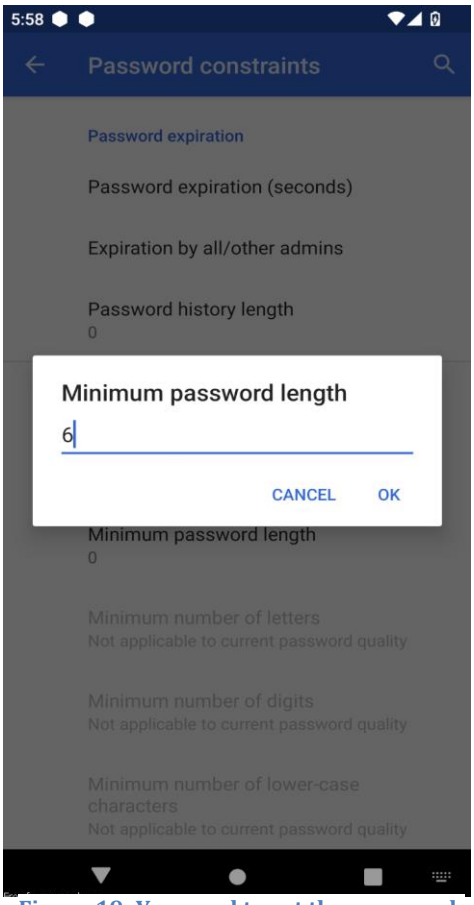

Figure 19: You need to set the password length.

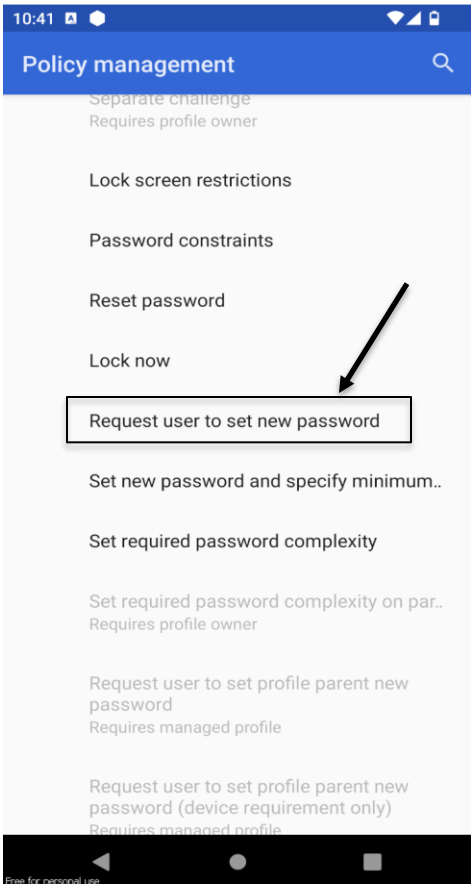

Figure 20: Now select this option.

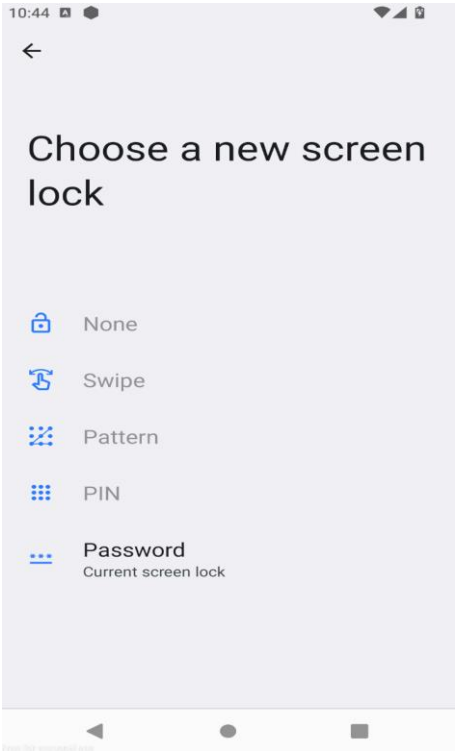

Figure 21: After you select your constraints one option will only be enabled to choose.

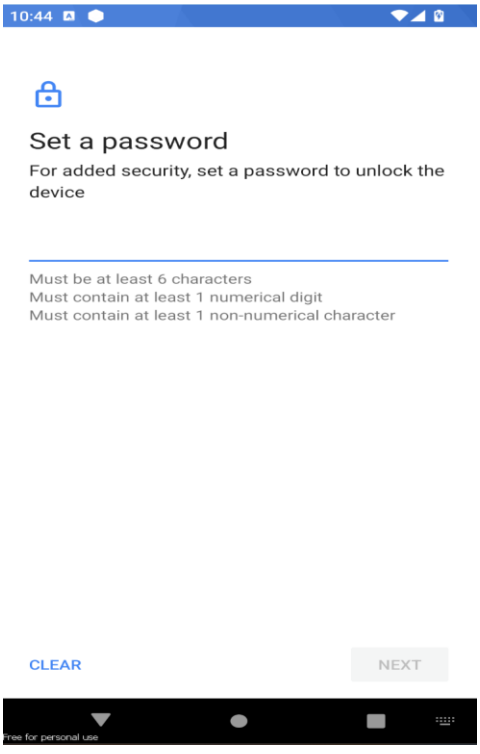

Figure 22: Now Set Your Password to meet the requirements that you chose.

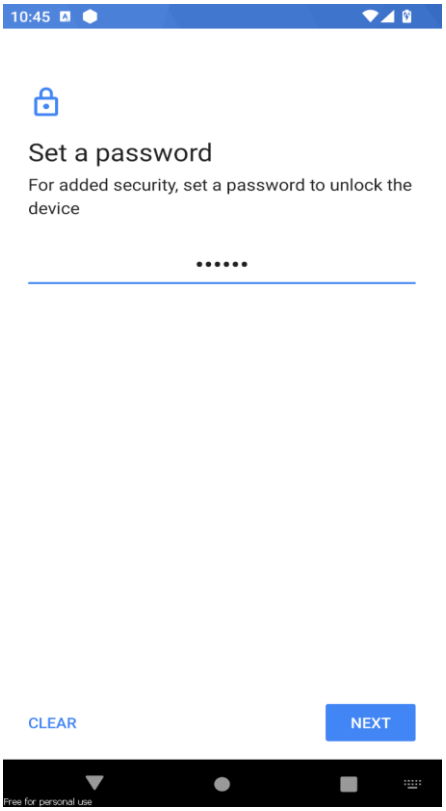

Figure 23: Now you need to reset the password.

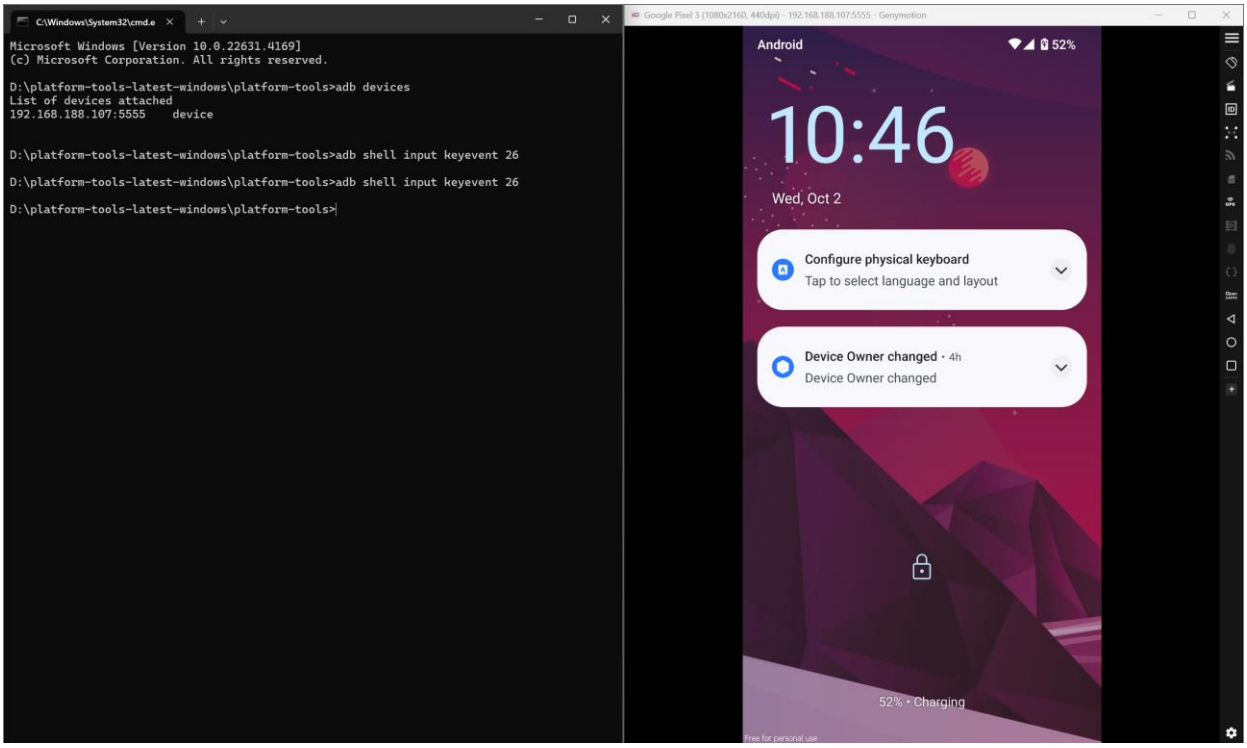

Figure 24: By using the commands in the command prompt you can lock the device.

Figure 25: Unlock the screen by using the password you choose.

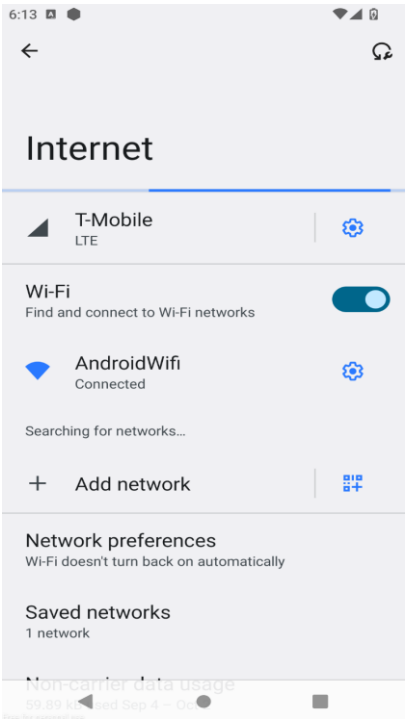

Figure 26: Now we need to set the Wi-Fi settings.

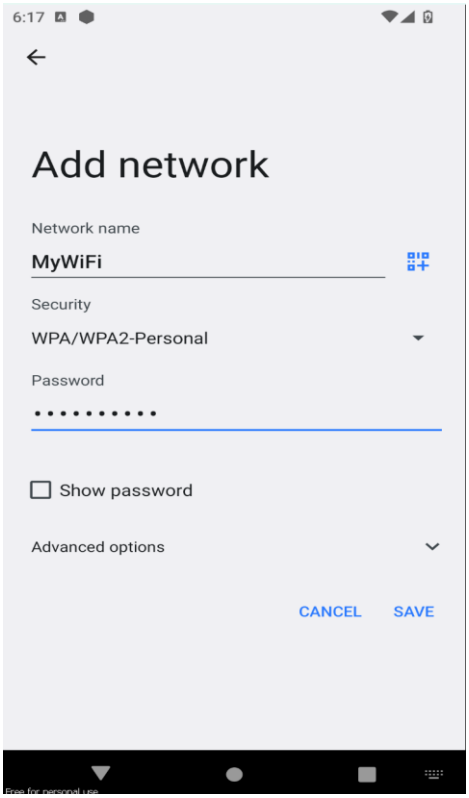

Figure 27: Here we are adding the network with name and password and connecting the device with that wifi network we added

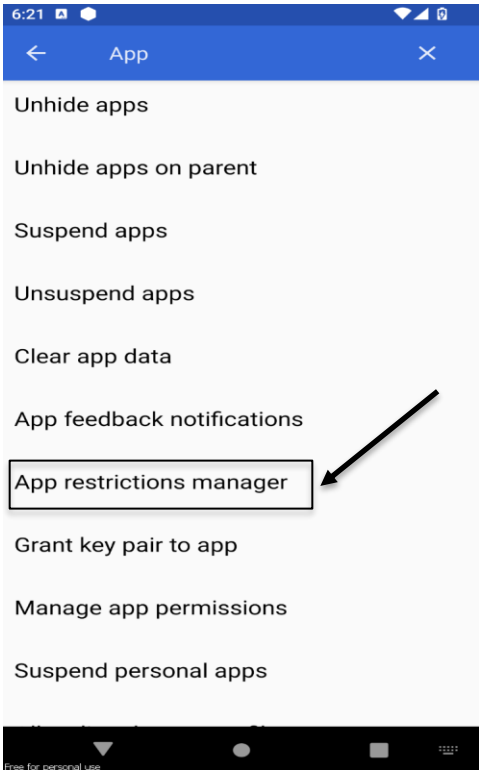

Figure 28: Here we are going for the next step that is restricting applications.

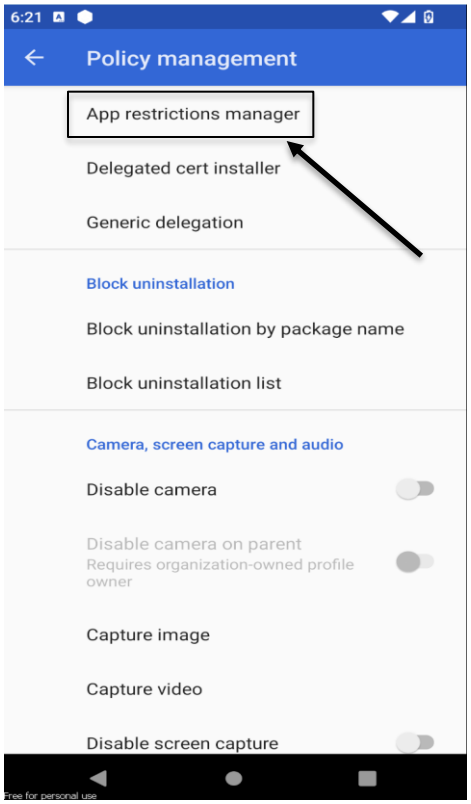

Figure 29: We need to select that option to restrict the apps.

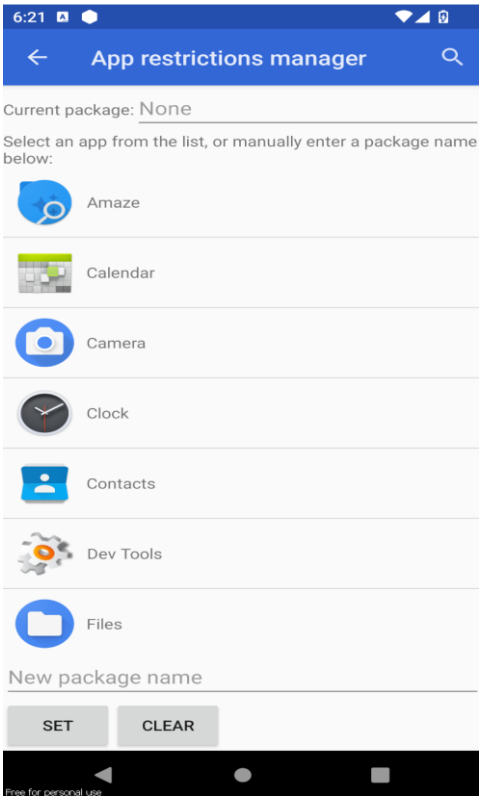

Figure 30: Here we need to select the app that we wanted to restrict.

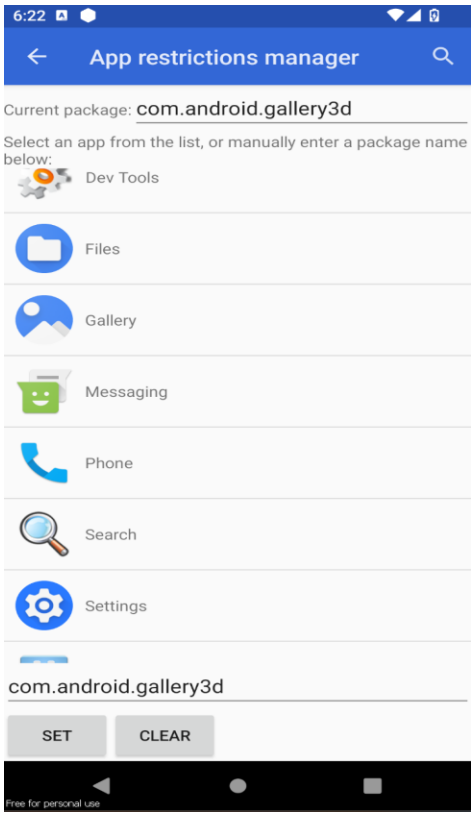

Figure 30.1: Here i have selected the gallery option and clicked on "set" option.

Figure 30.2: I tried to open the gallery but the application was not opening and it is not showing any warning like stuff to paste for the proof.