Appendix K: Mobile Device Penetration Testing Methodology

Objective

The labs in this module are designed to make you familiar with pen testing methodology to audit a wireless network infrastructure consisting of mobile devices by creating a malicious apk file and executing it.

Scenario

By finding a secure spot in the vicinity of a building, hackers can exploit a wireless signal and gain entry into an organization's internal network. Starting from the SSID of the wireless network to its strength in different areas of its radius, everything is critical to wireless security. Password for the wireless signal, encryption methodology and protocols used, devices interacting with the network are all potential weak points for the hackers to exploit. As a wireless penetration tester, you have to ensure that all the vulnerable points of a network are either secured or strengthened. You also have to identify the users who can easily be enticed to click on links or execute the malicious files you built.

Exercise 1: Gaining Complete Access to an Android Device Using SpyNote

Scenario

SpyNote is a client/server application developed in Java Android for the client side and in Java/Swing for the Server side. The goal of the application is to provide the control of the Android system remotely and retrieve information from it.

Personnel working in an organization might carry their mobile devices to the workplace and use them to access enterprise data and systems. Hence, it is evident that mobile devices contain sensitive information related to organizations. This might open doors for attackers to perform attacks and get control over the personnel' devices and access them to gain sensible information related to the organizations. This might reveal information related to the policies of the organization, payrolls of its personnel, HR policies, quotations signed by clients, and so on.

Being a penetration tester or an information security auditor, you should have knowledge of how to develop a malicious apk file and merge it with a genuine apk file. When this file is shared with an employee in an organization and he/she installs it, the apk gives complete access to the pentester.

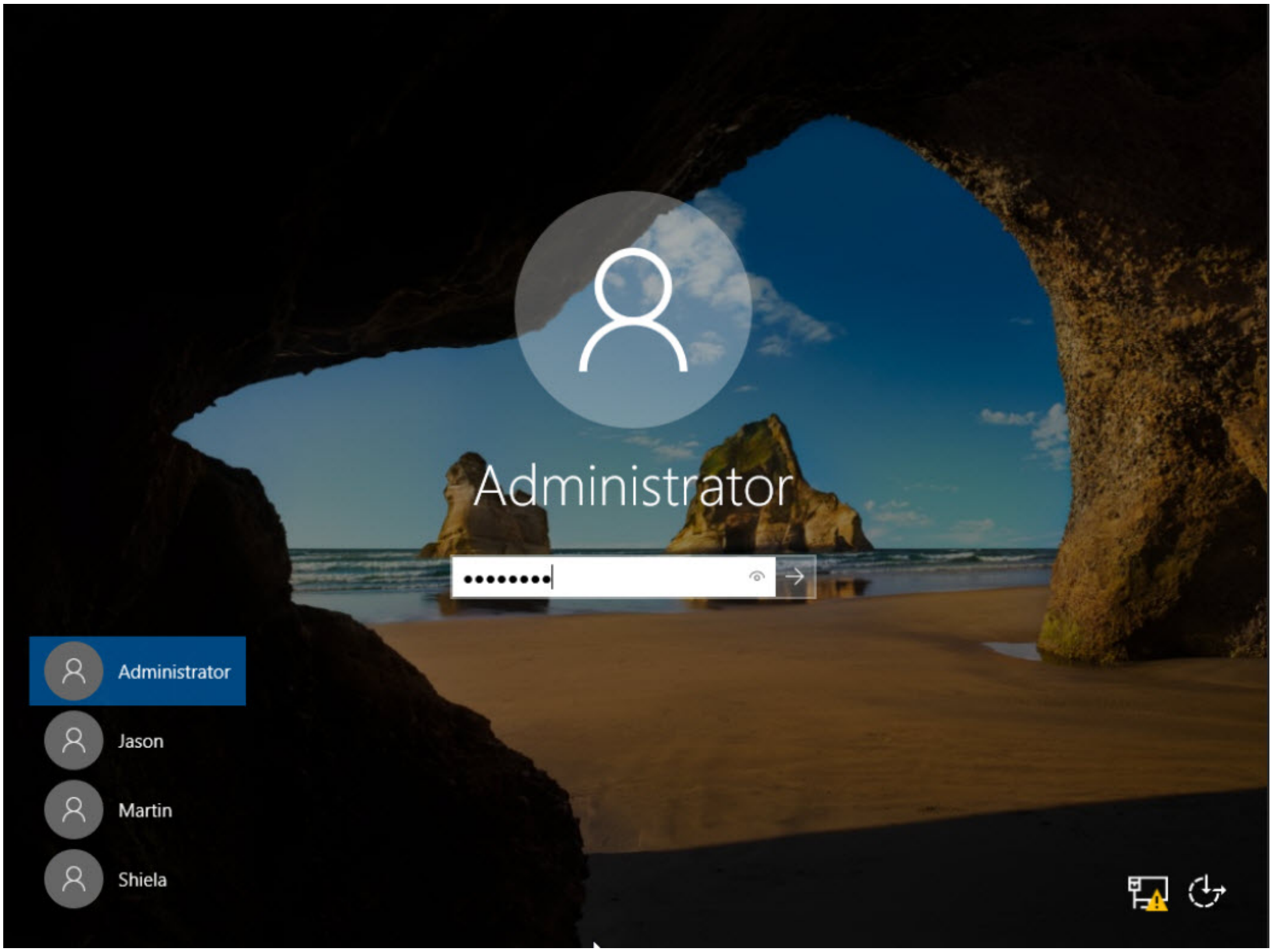
In this lab, you will learn how to gain remote access to a device by using a remote access Trojan.

Lab Duration: **40** Minutes

1. In the **CPENT Appendix K Windows Server 2019** machine, click **Ctrl+Alt+Del**.

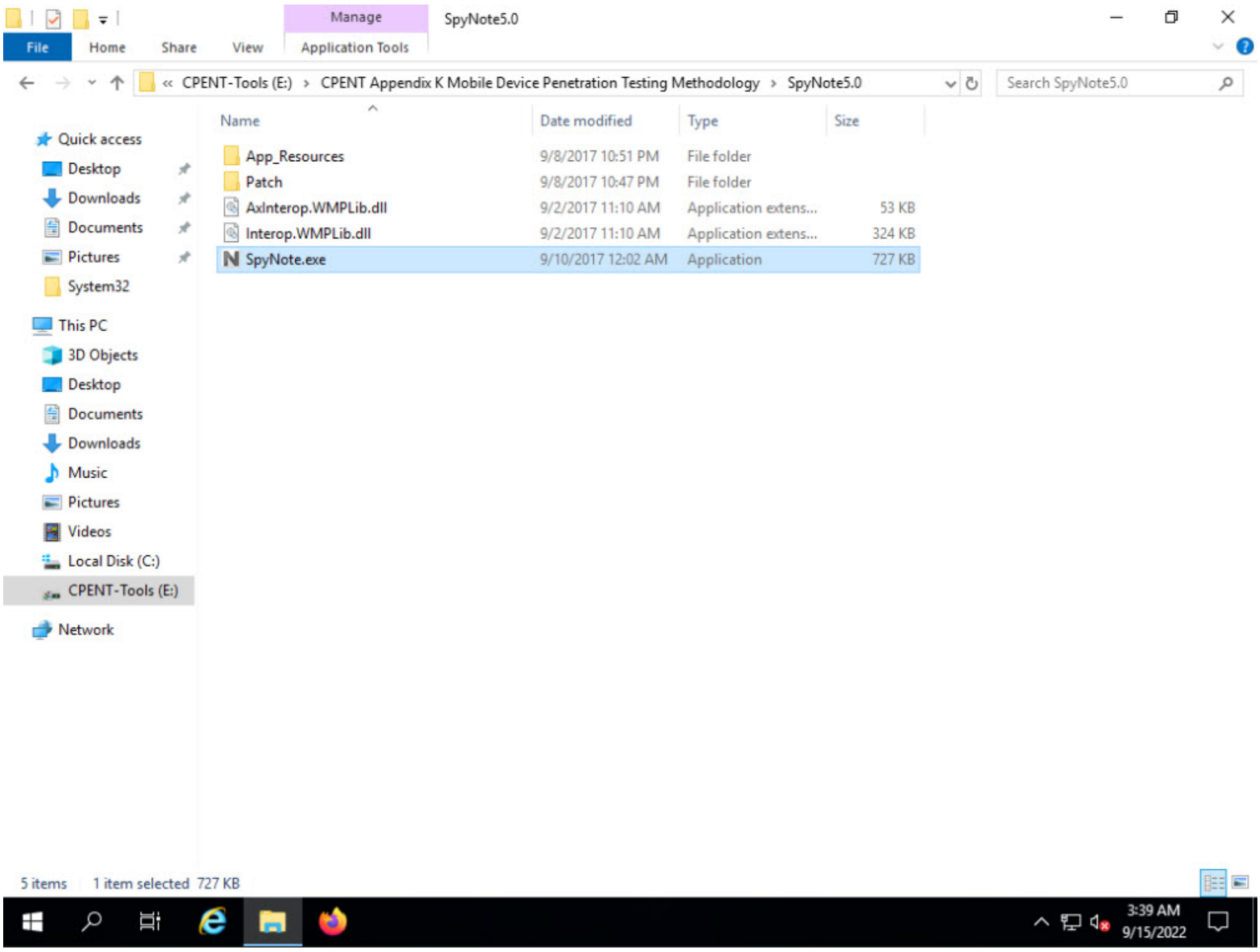
2. In the password field, type **Pa$$w0rd** and press **Enter**.

Note: You can also use the **Type Password** option from the **Commands** menu to enter the password.

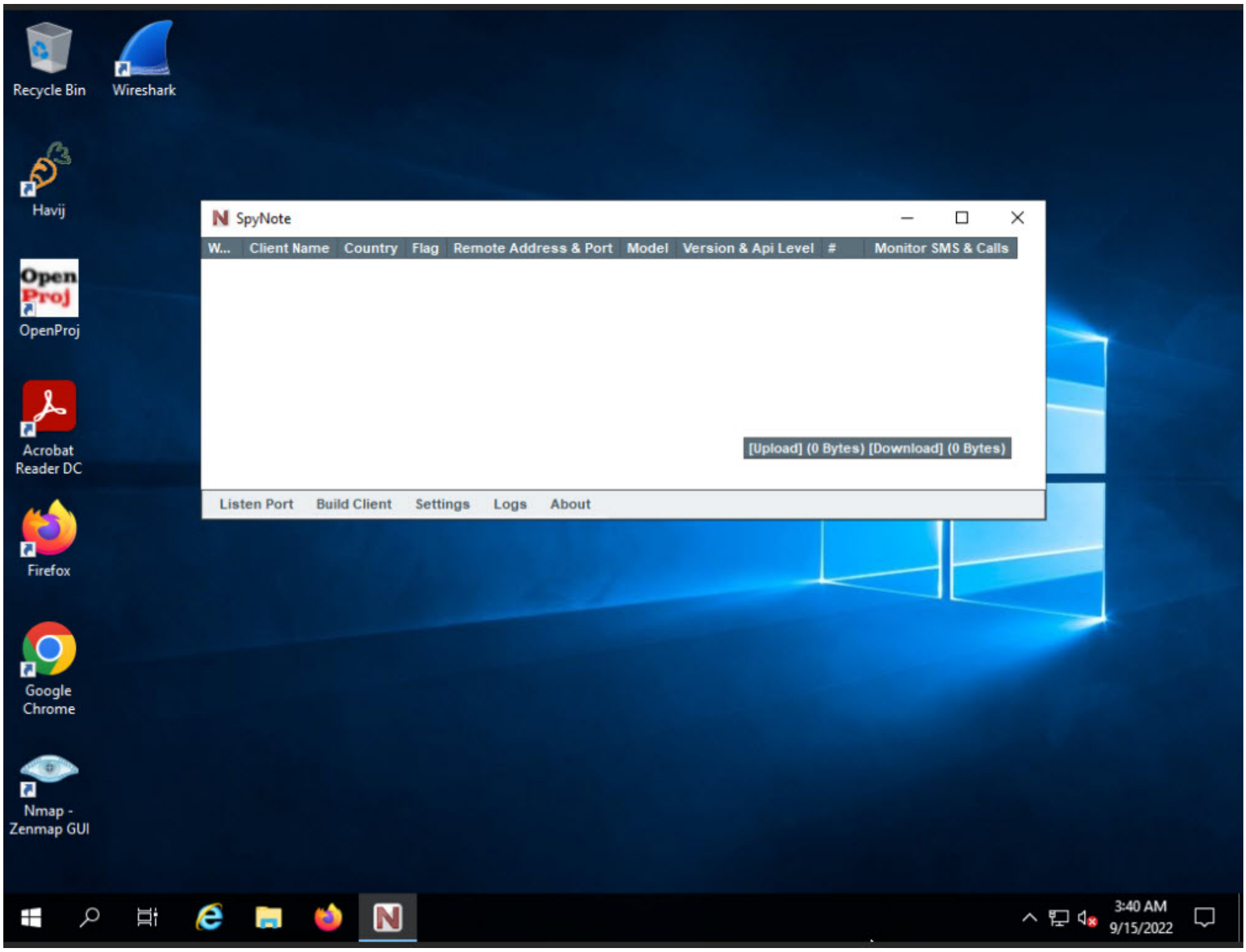


3. Navigate to **E:\CPENT Appendix K Mobile Device Penetration Testing Methodology\SpyNote5.0**, and double-click **SpyNote.exe**.

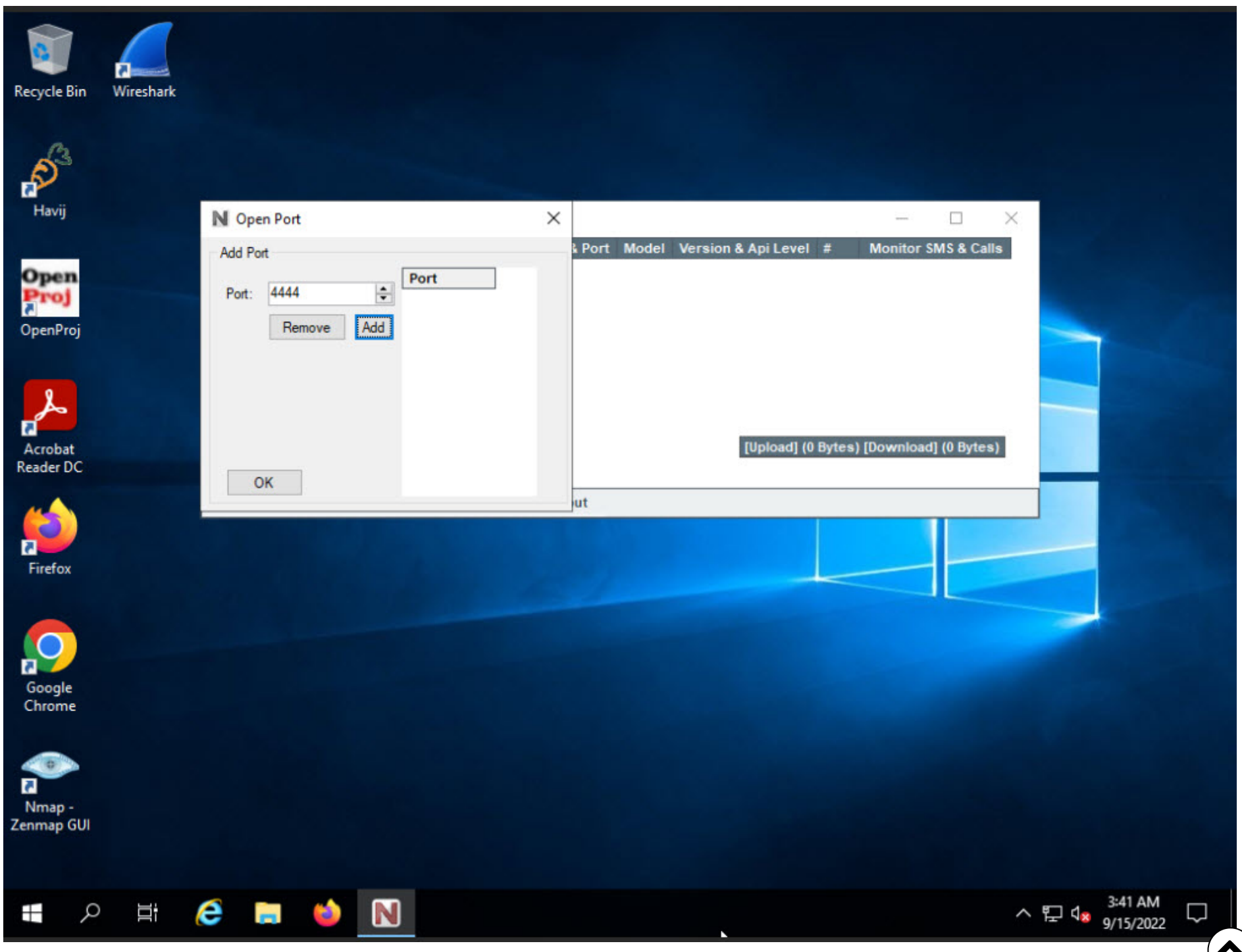
Note: If an **Open File - Security Warning** pop-up appears, click **Run**.



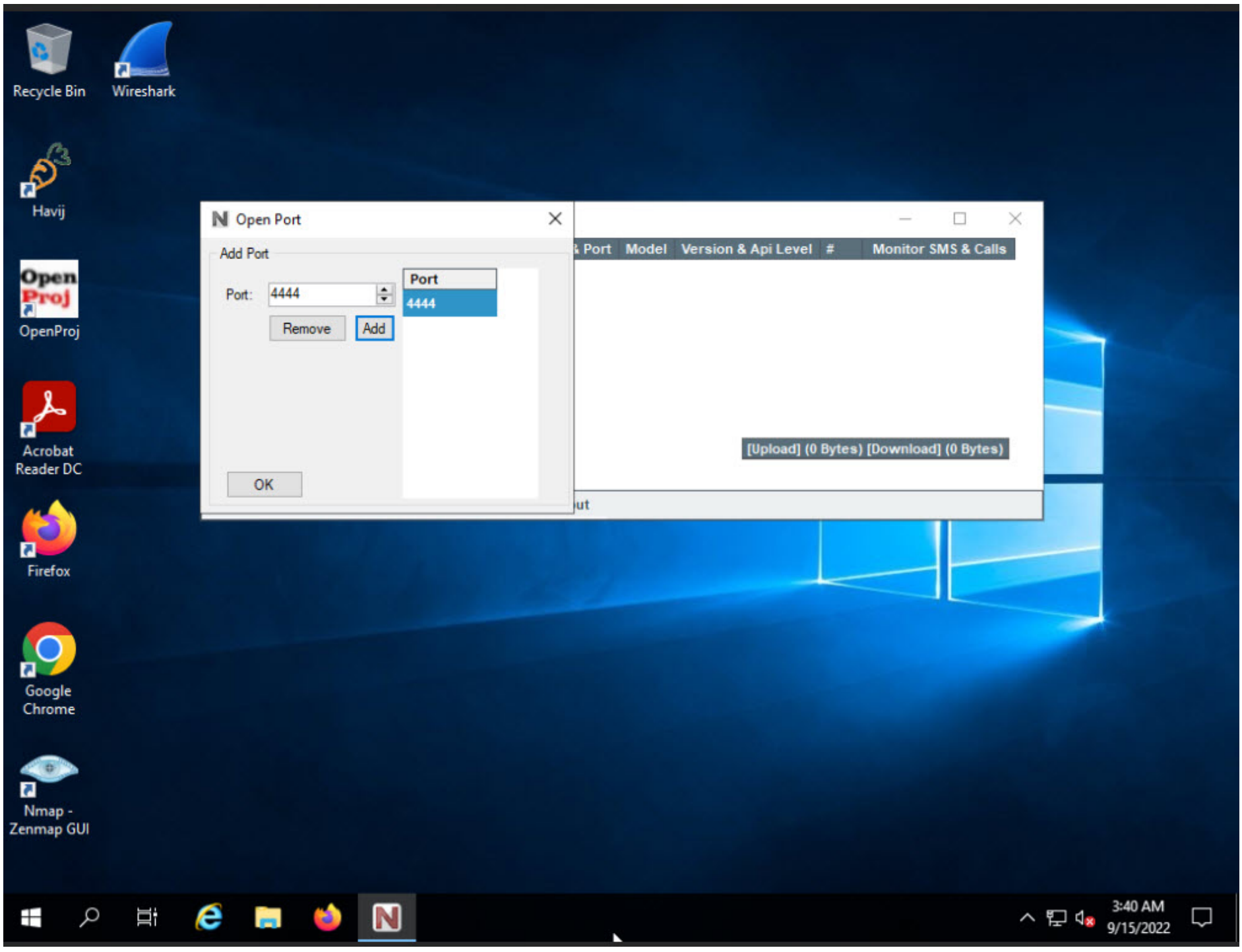
4. **SpyNote** listener window appears. You need to configure a port on which you want SpyNote to listen. To perform this, click **Listen Port** option in the lower left corner of the Listener window.



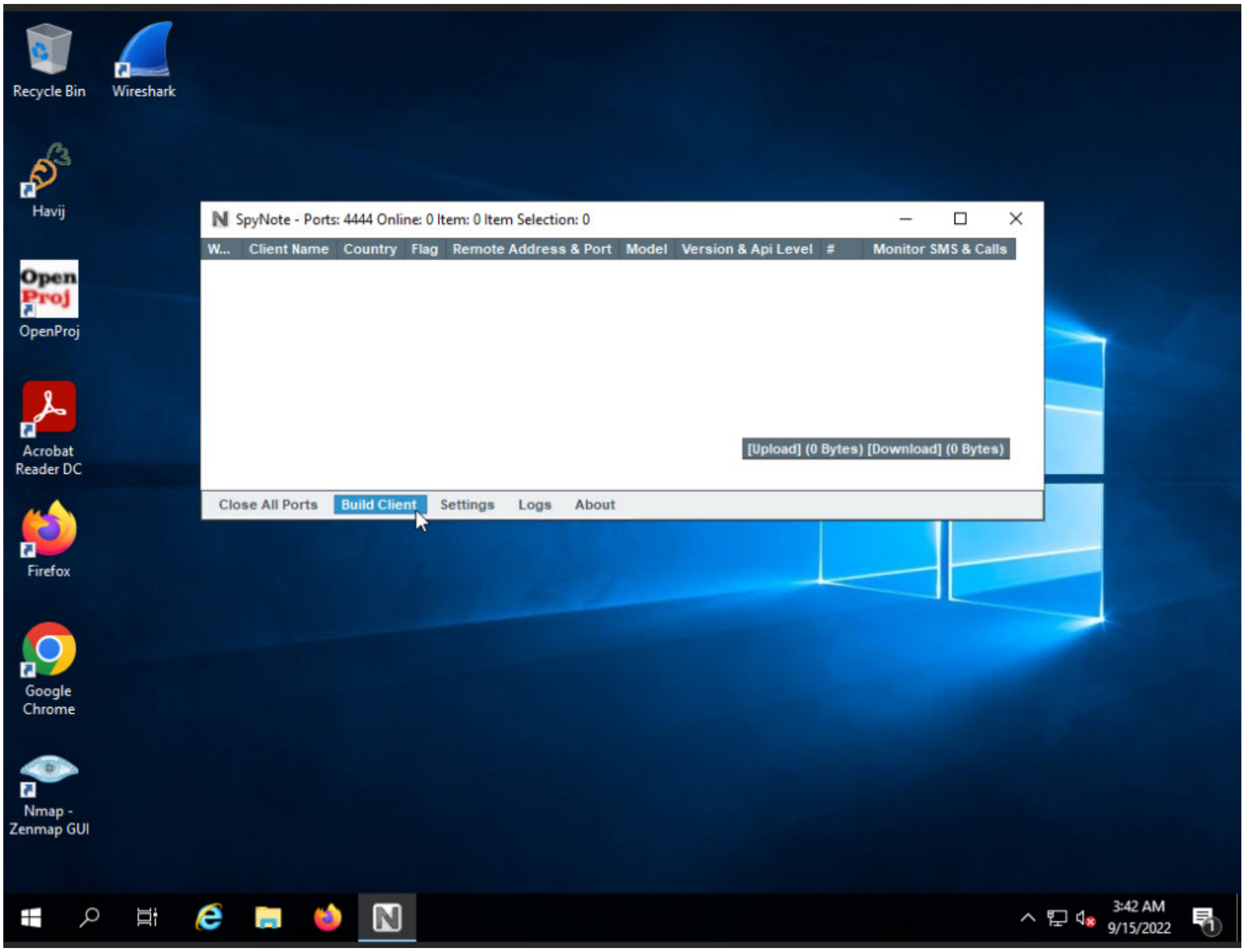
5. **Open Port** window appears. In this lab, we will be configuring SpyNote to listen on port **4444**. To perform this, type **4444** in the **Port** field and click **Add**.



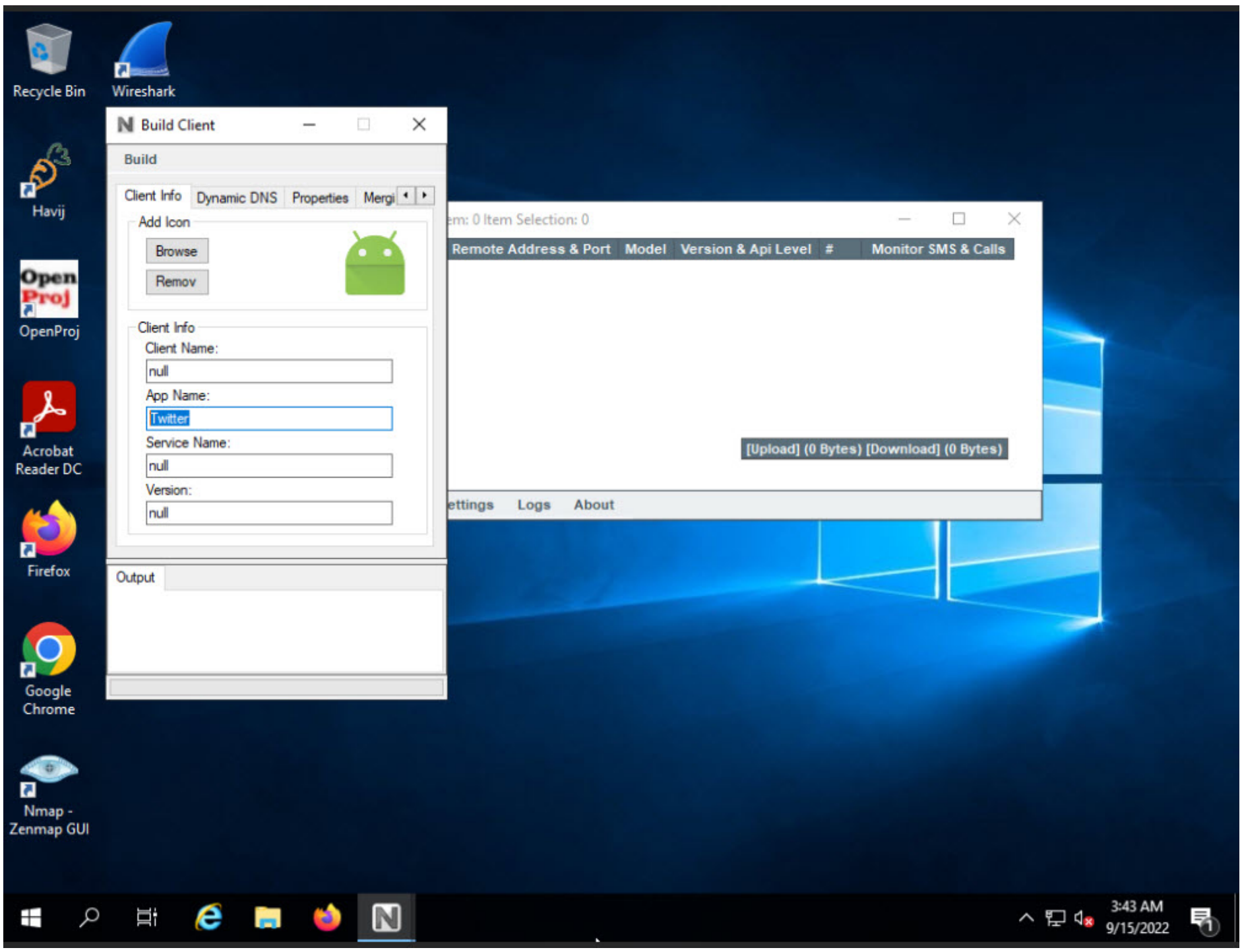
6. You will observe that the port has been added. Click **Ok** to close the window.



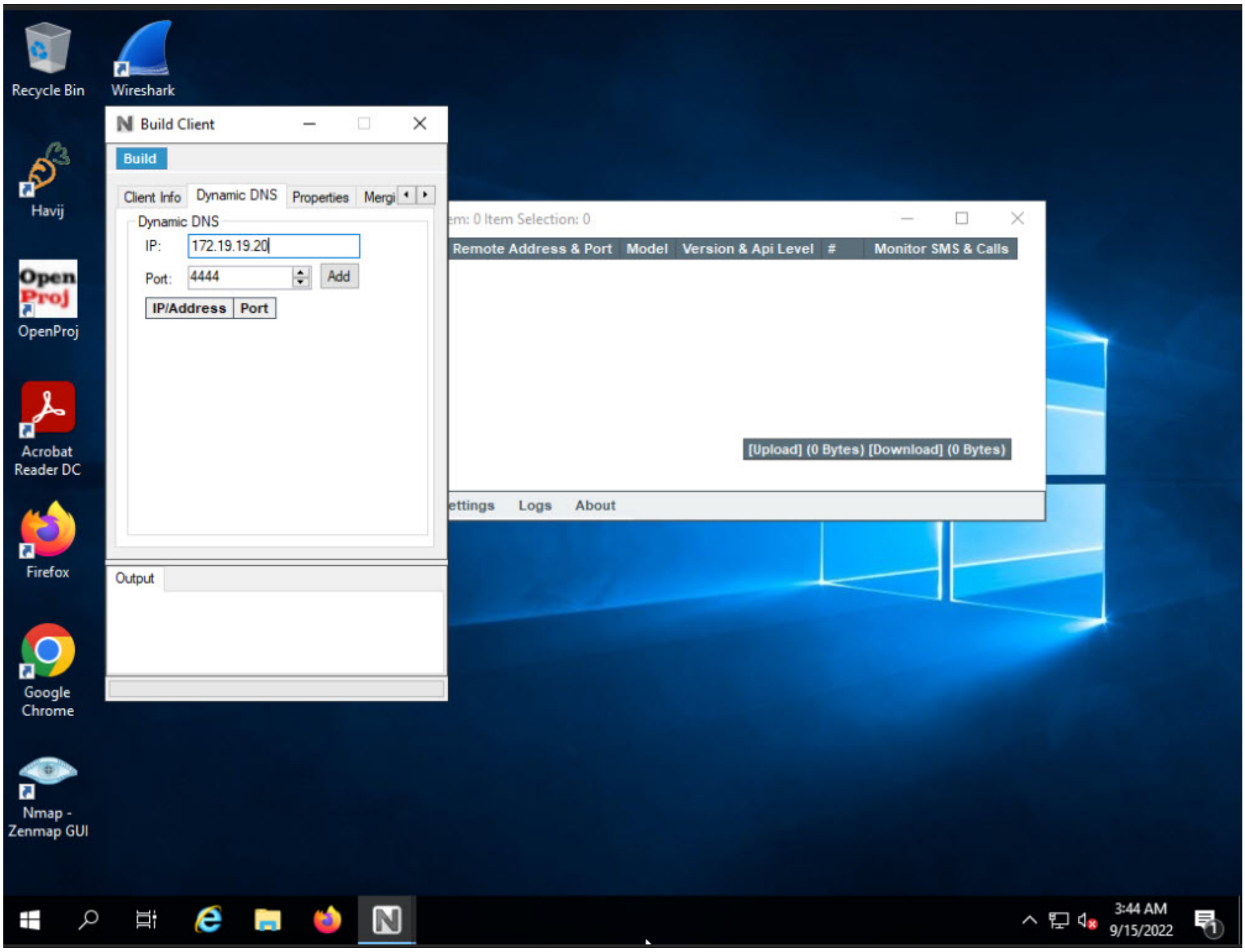
7. Click **Build Client** option in the lower section of the listener window to launch the Build Client.



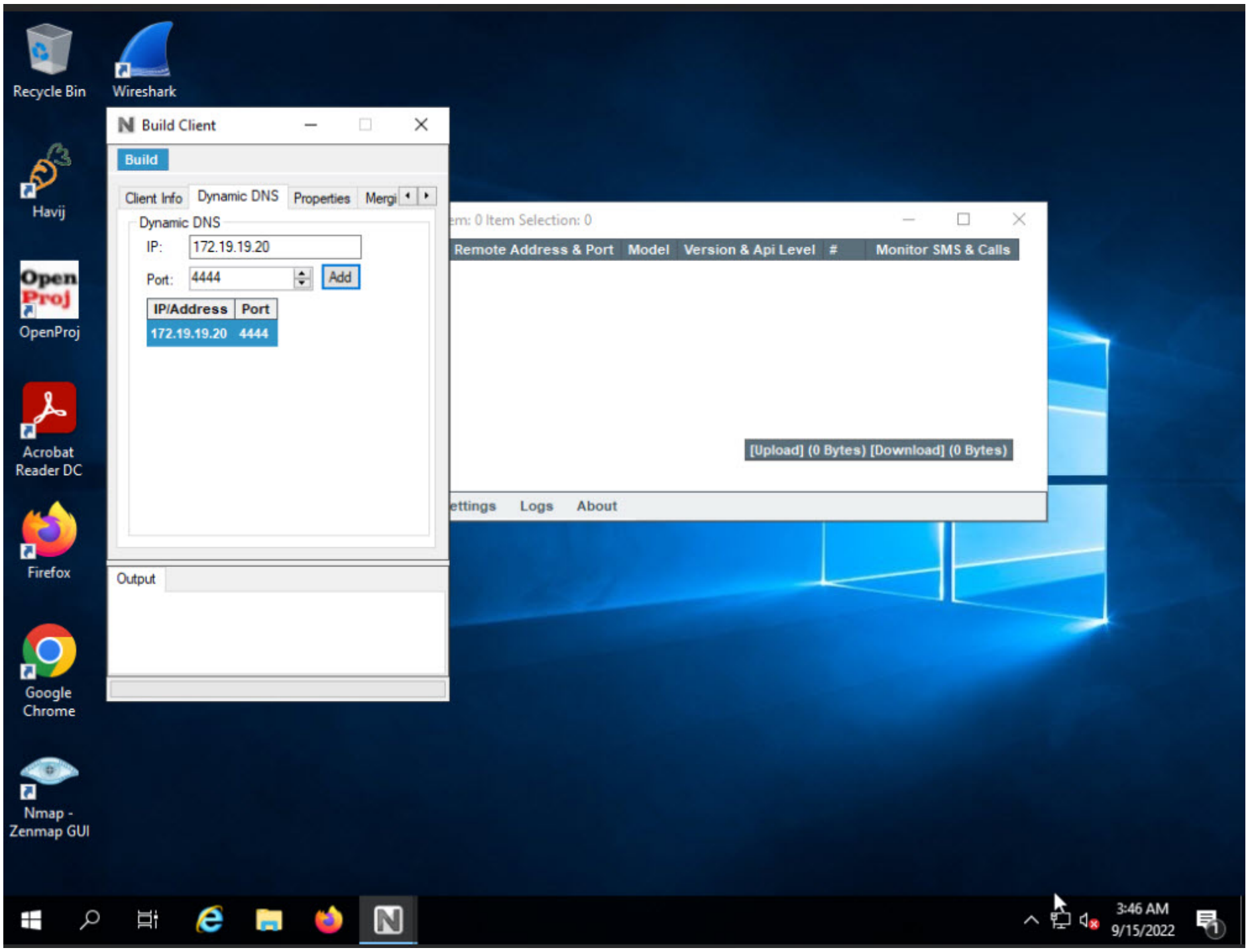
8. **Build Client** window appears displaying the **Client Info** section. Enter the **App Name** as **Twitter** and click **Dynamic DNS** tab.



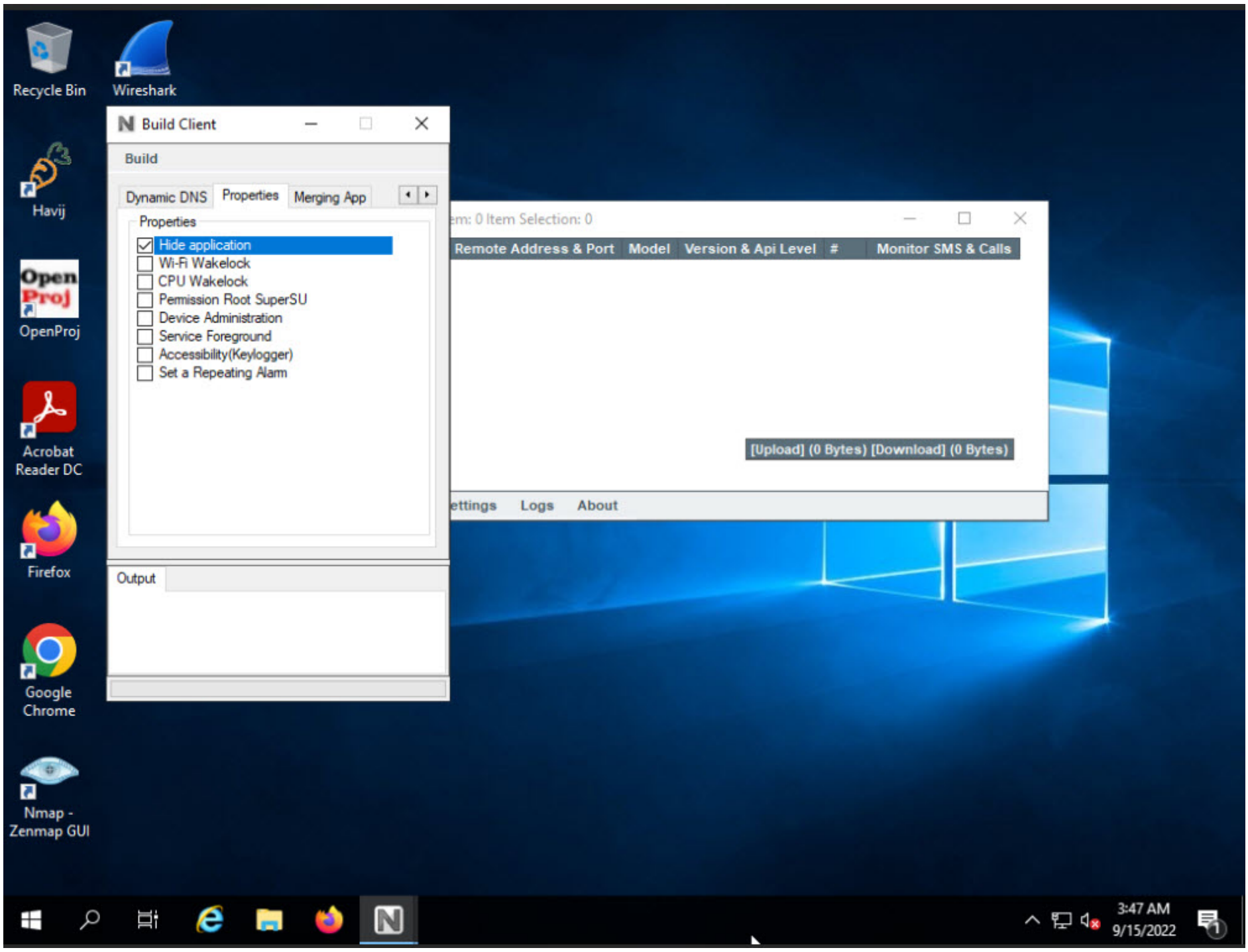
9. Dynamic DNS section appears, enter the IP address of **Windows Server 2019** in the **IP** field. The IP address to enter is **172.19.19.20**. Type **4444** in the **Port** field and click **Add**. By doing so, we are configuring the client to connect to **172.19.19.20** on port **4444**..



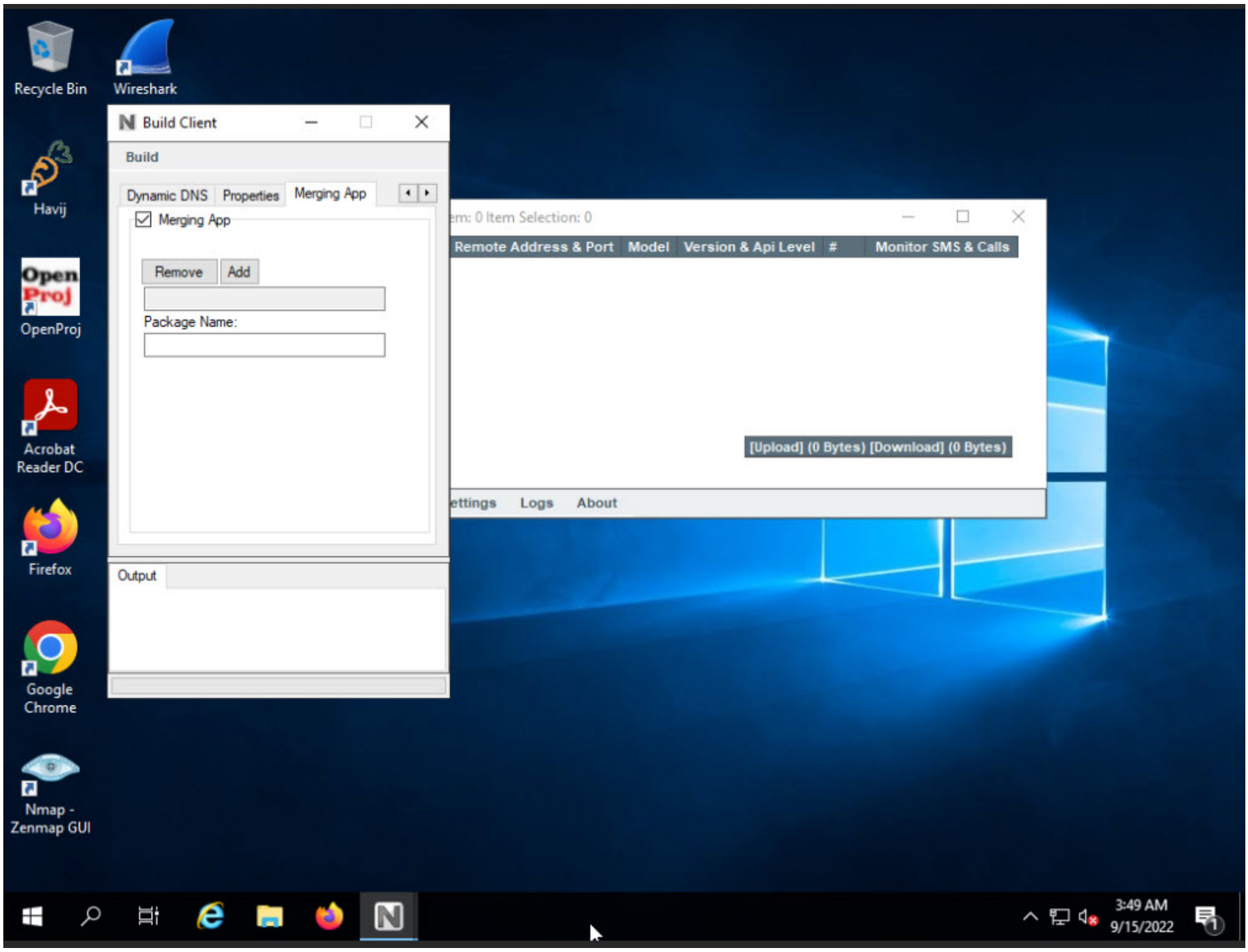
10. The IP Address and Port are added to the client. Click on **Properties** tab.



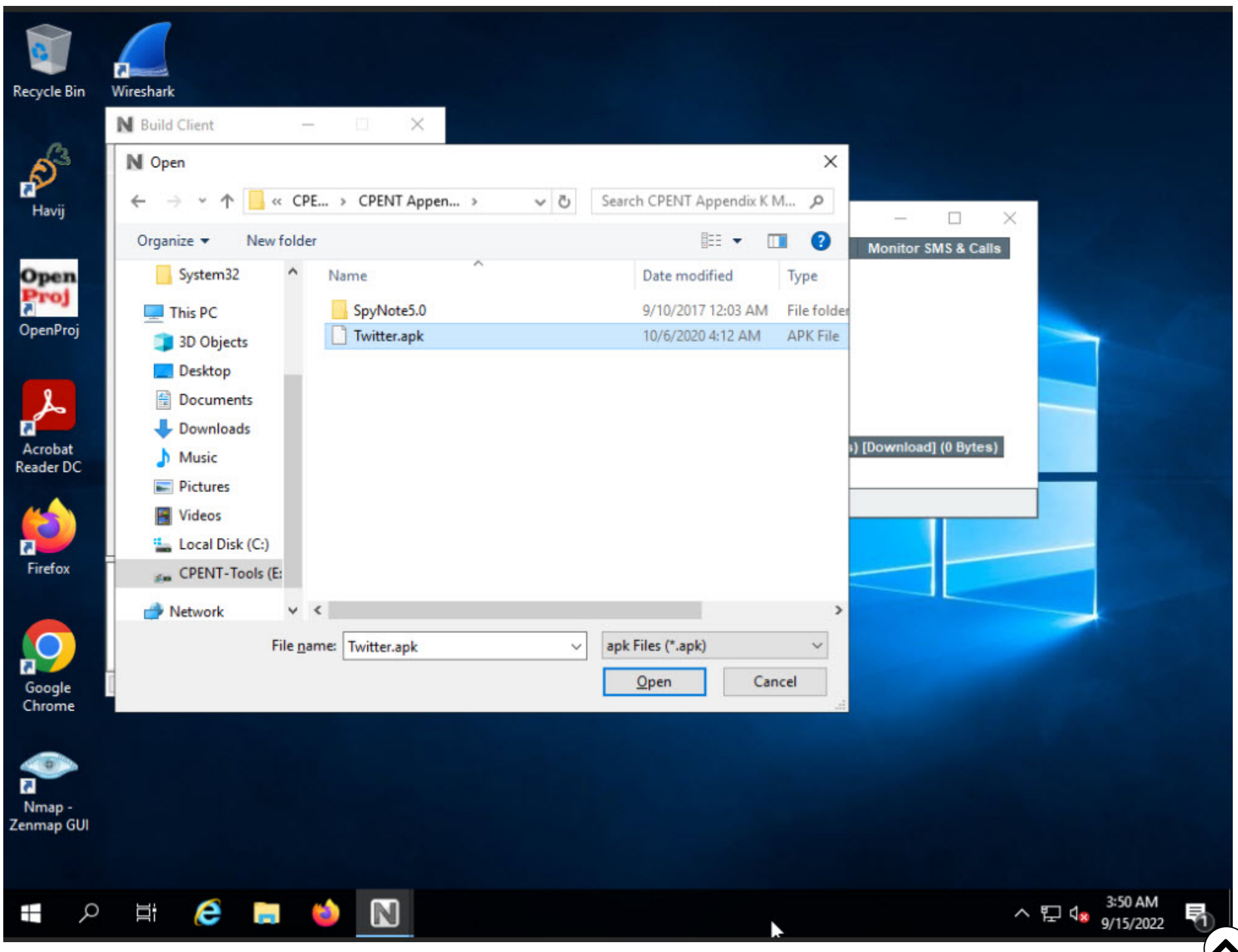
11. We will be configuring the client in such a way that it gets hidden upon installation. To perform this, check **Hide application** option, and uncheck the other options as we are not focusing on keylogging, device administration, and so on in this lab. Once you check the option, click on the **Merging App** tab.



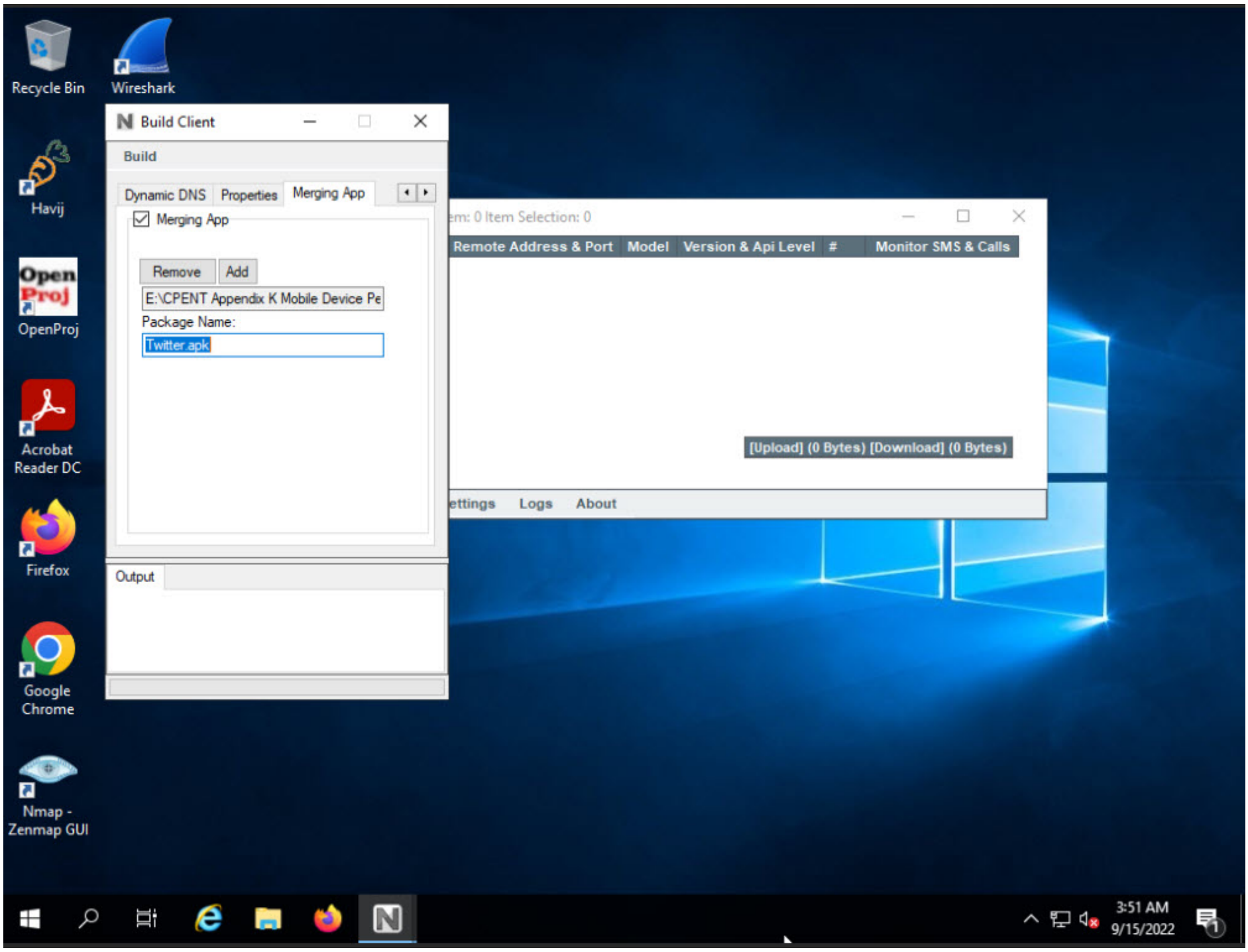
12. We will be merging the malicious apk with Twitter app. So, when a person installs the app, the original Twitter app is installed and displayed in the applications menu, while the malicious app gets hidden and runs in the background. To merge with the Twitter app, check **Merging App**, and click **Add.**



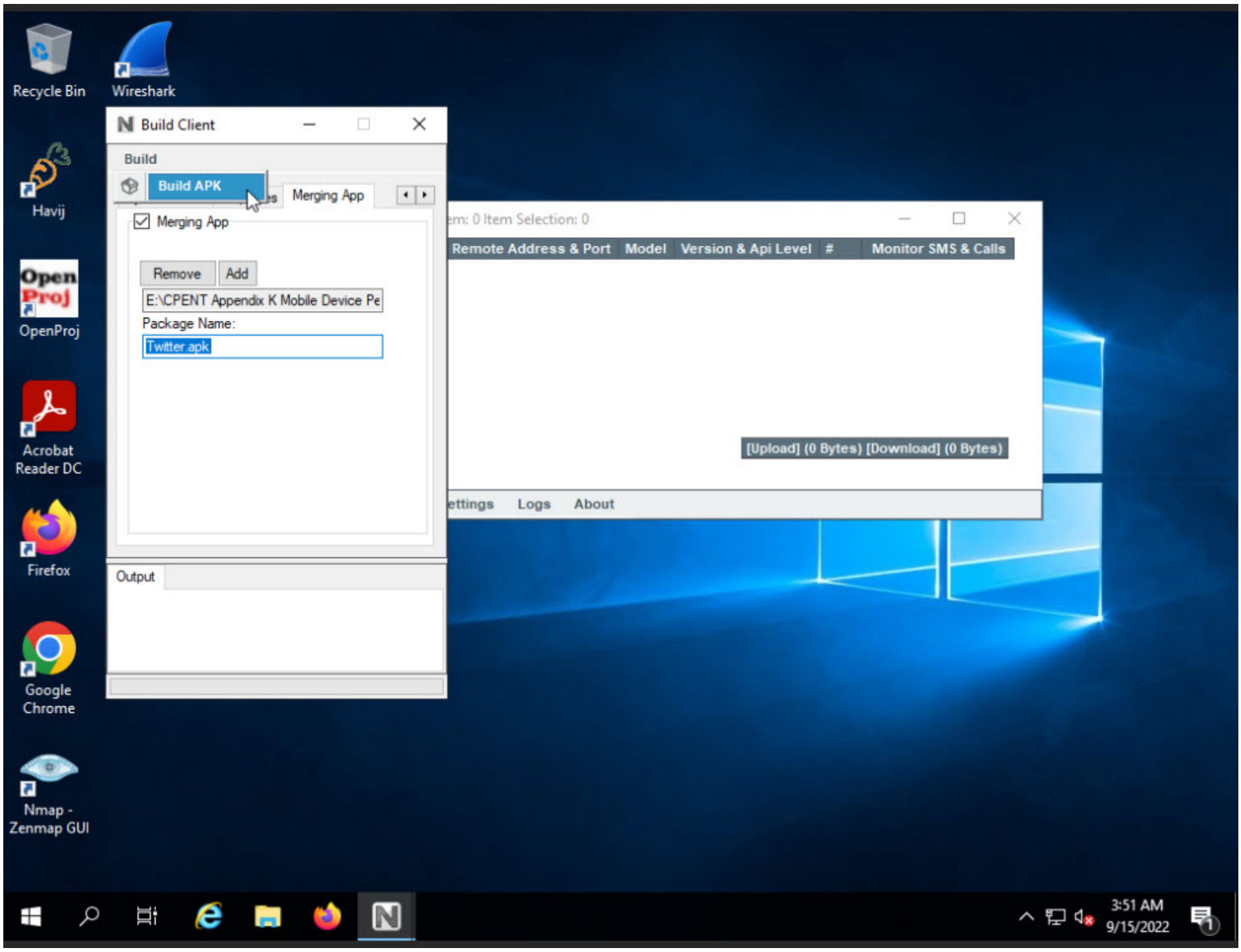
13. **Open** window appears, navigate to **E:\CPENT Appendix K Mobile Device Penetration Testing Methodology** and select **Twitter.apk** and click **Open**.



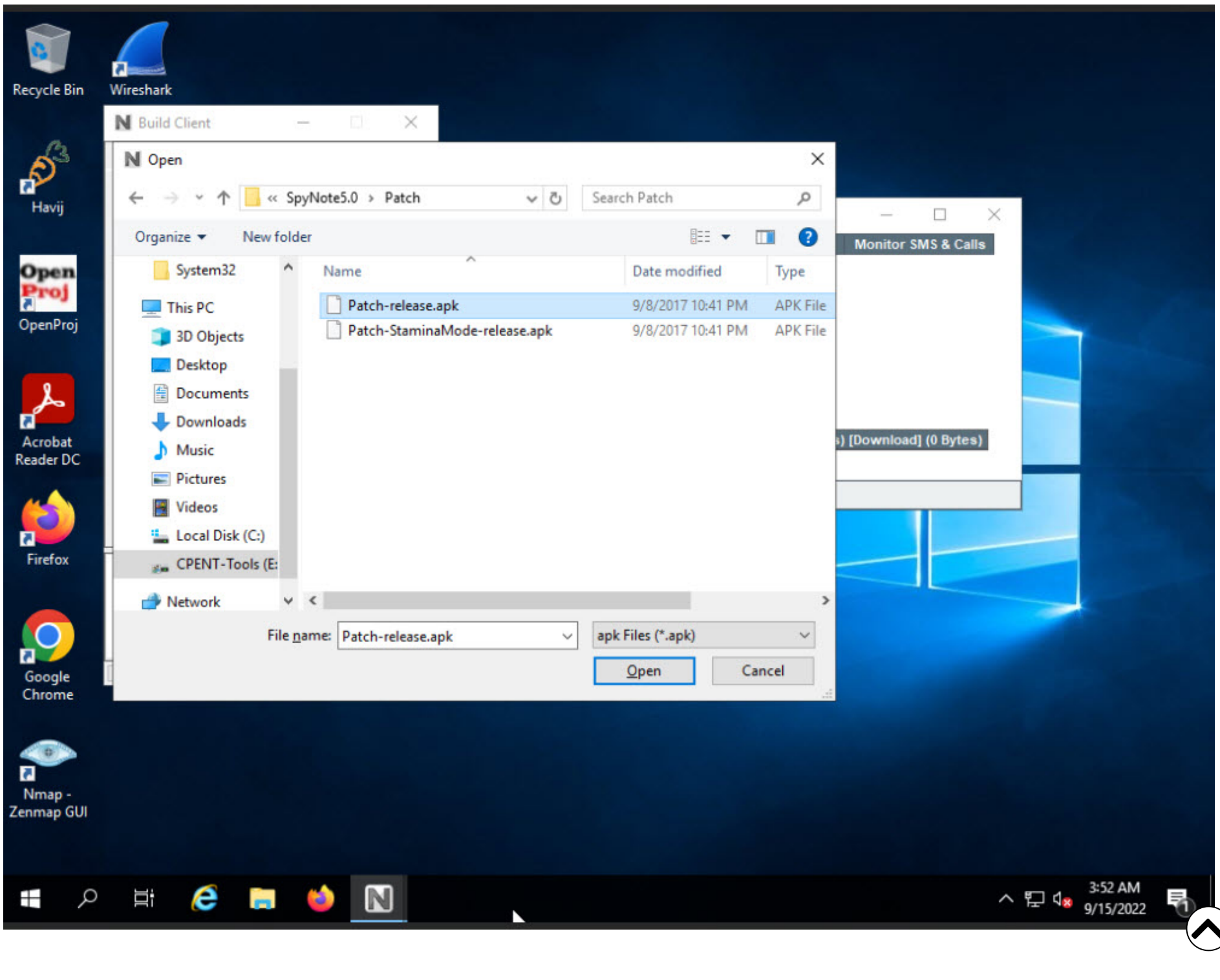
14. The Twitter apk has been added to the Merging App section. Enter the **Package Name** as **Twitter.apk**.



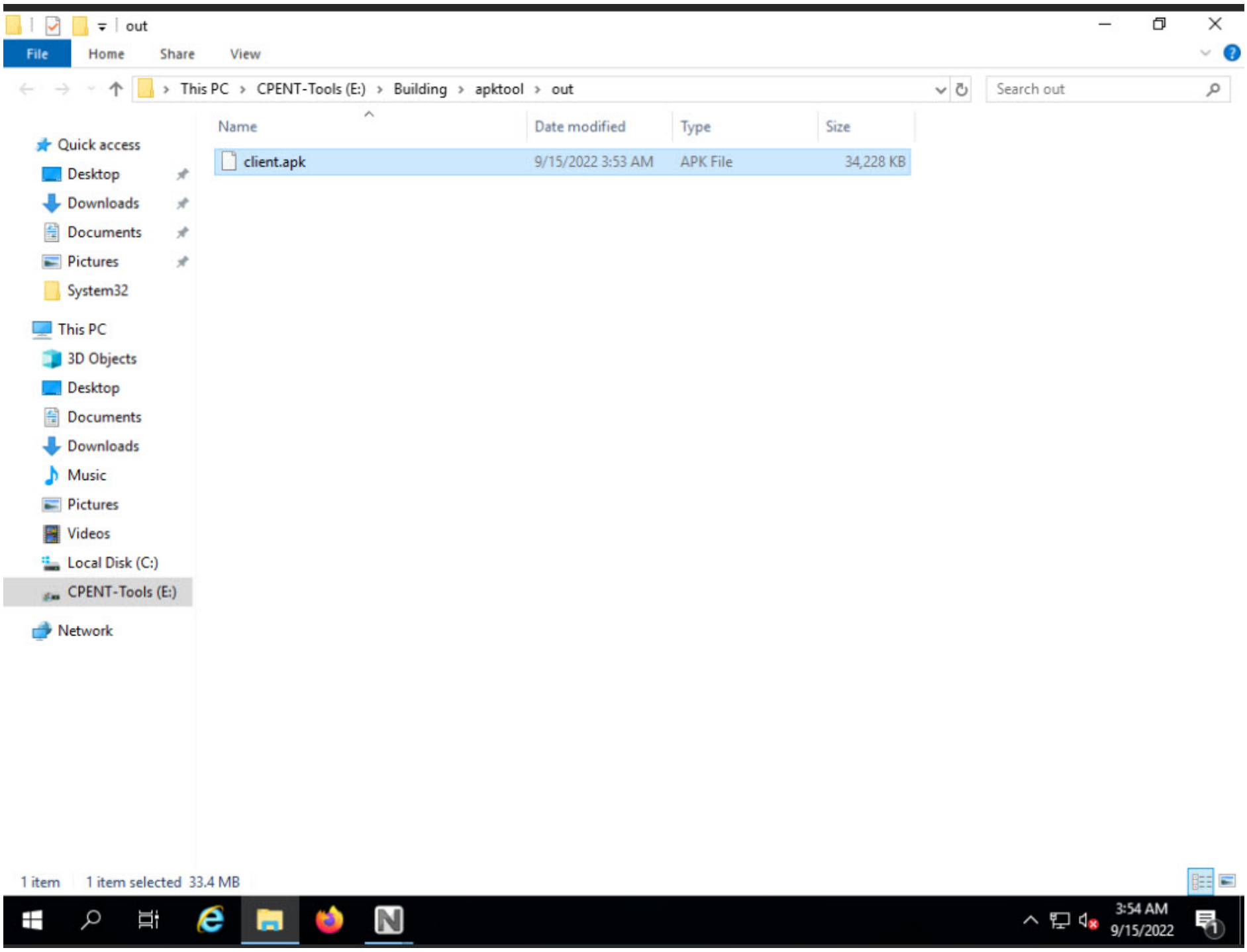
15. Now, click on **Build** button in the top left corner of the **Build Client** window and click **Build APK**.



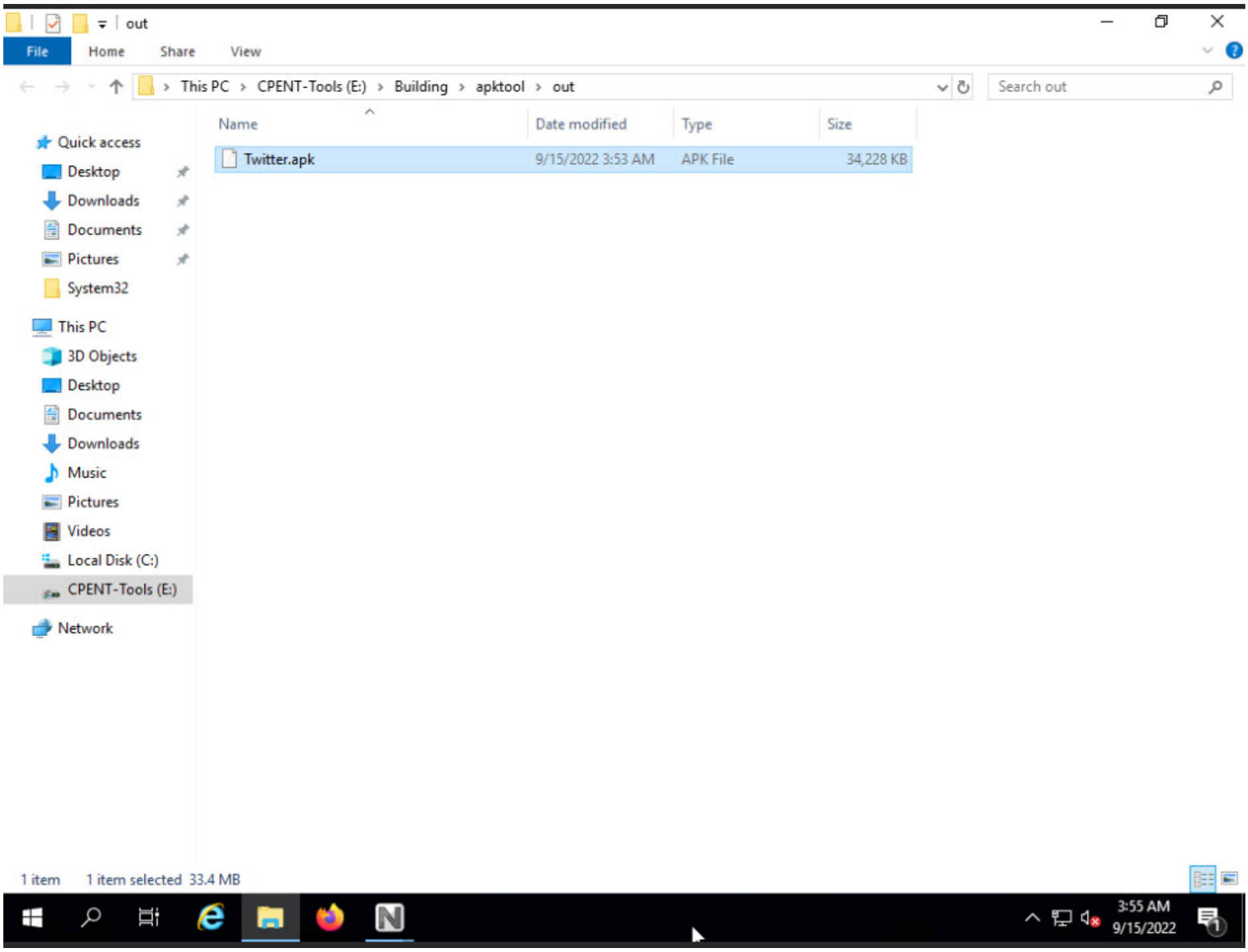
16. **Open** window appears, navigate to **E:\CPENT Appendix K Mobile Device Penetration Testing Methodology\SpyNote5.0\Patch**, select **Patch-release.apk** and click **Open**.



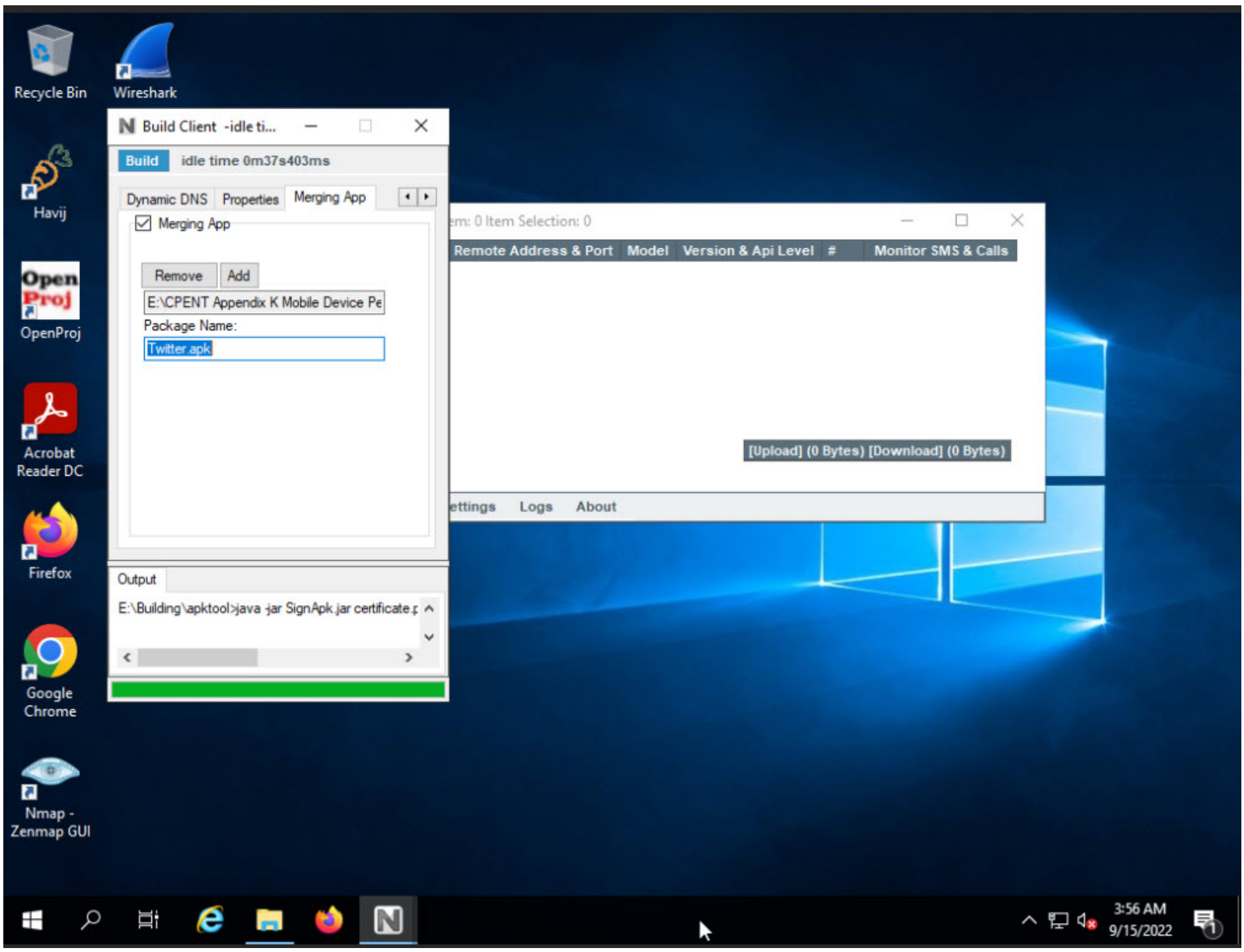
17. SpyNote takes some time to build the client. Once the client is created, the client folder opens as shown in the screenshot.



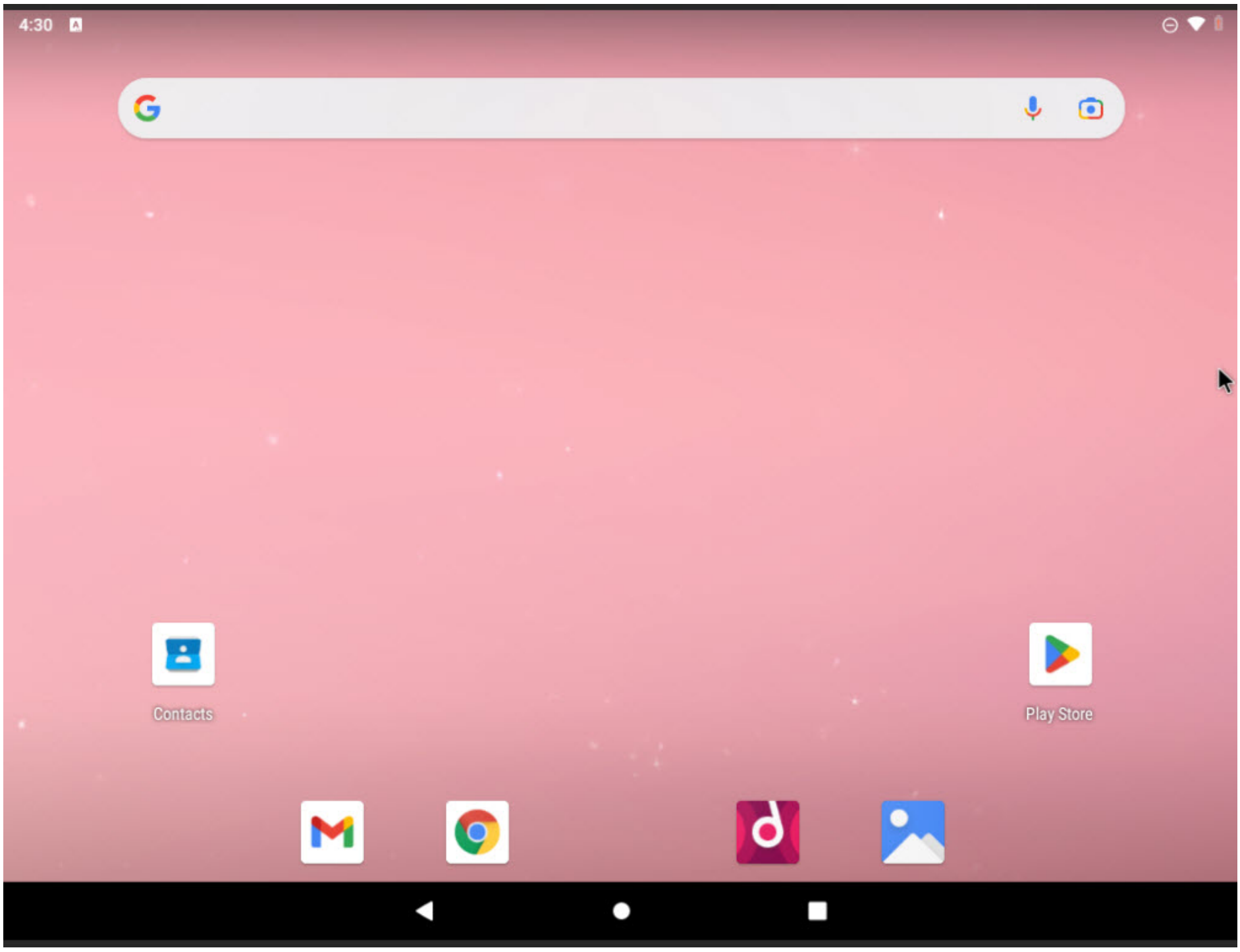
18. In order to make the client look more realistic, we shall rename the file to **Twitter.apk** as shown in the screenshot below. Minimize the File Explorer window.



19. Now, close the **Build Client** window.

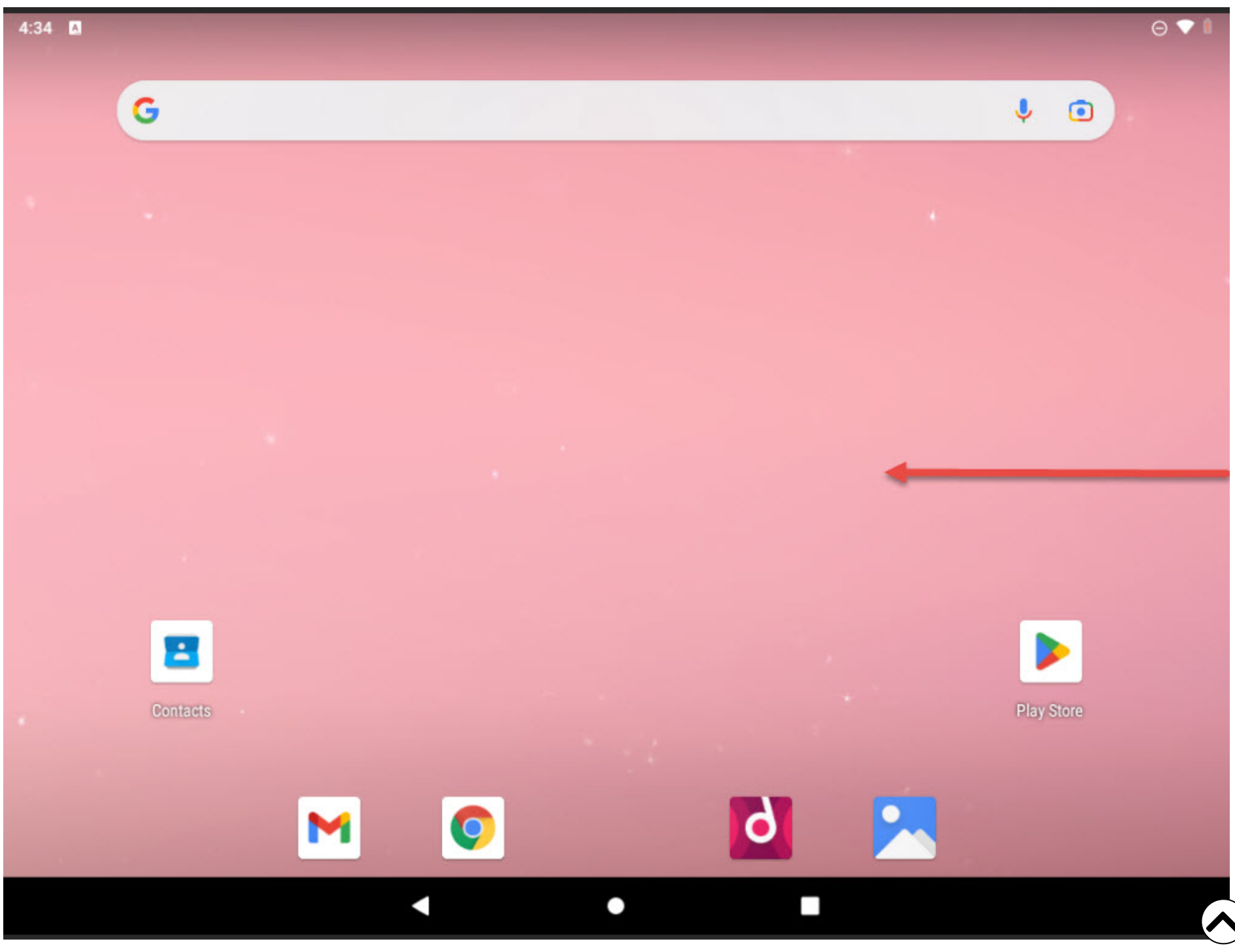


20. Now, select **target_CPENT Appendix K Android** machine. Android home screen appears.

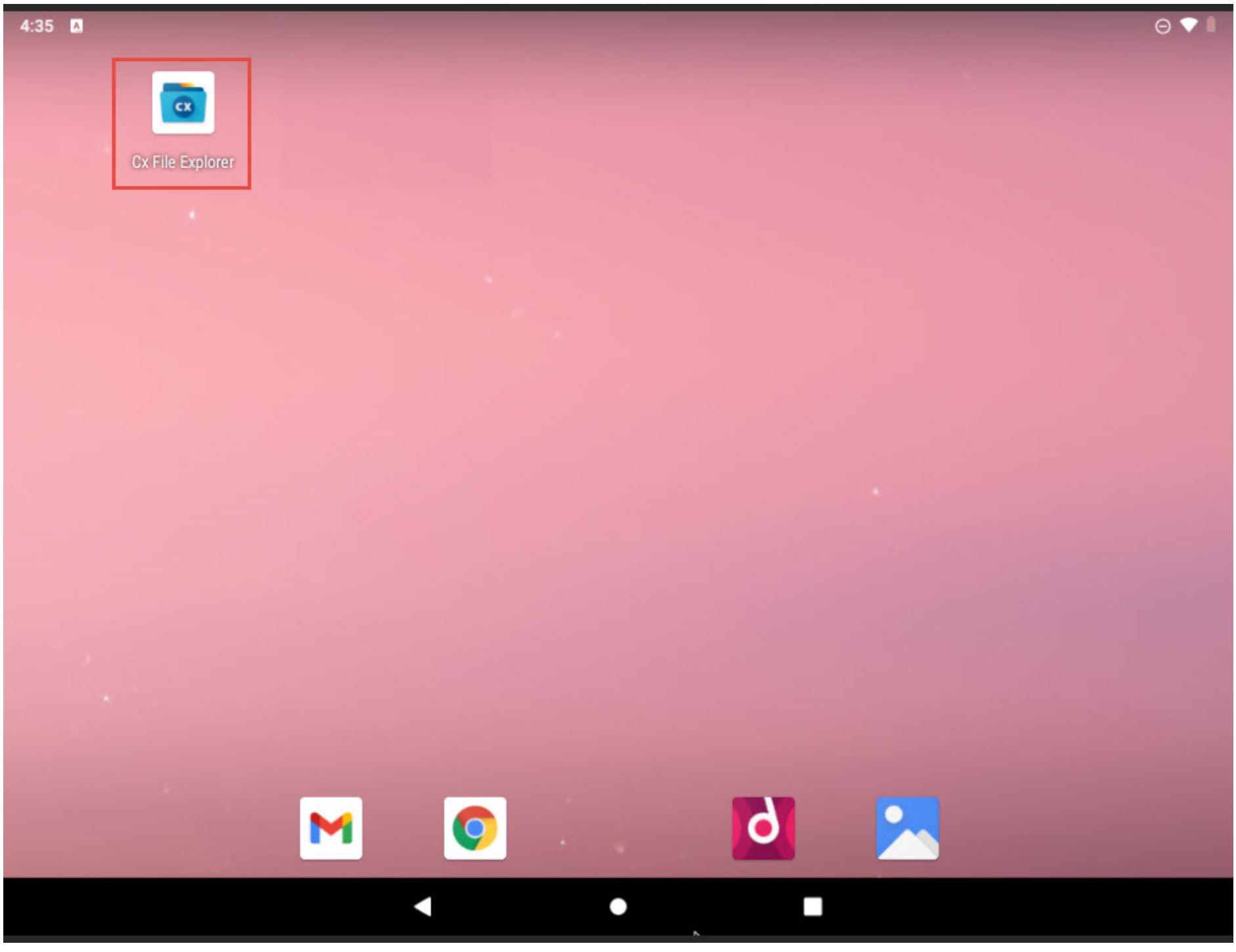


21. In this lab, we will be allowing installation of apps from unknown sources on the device.

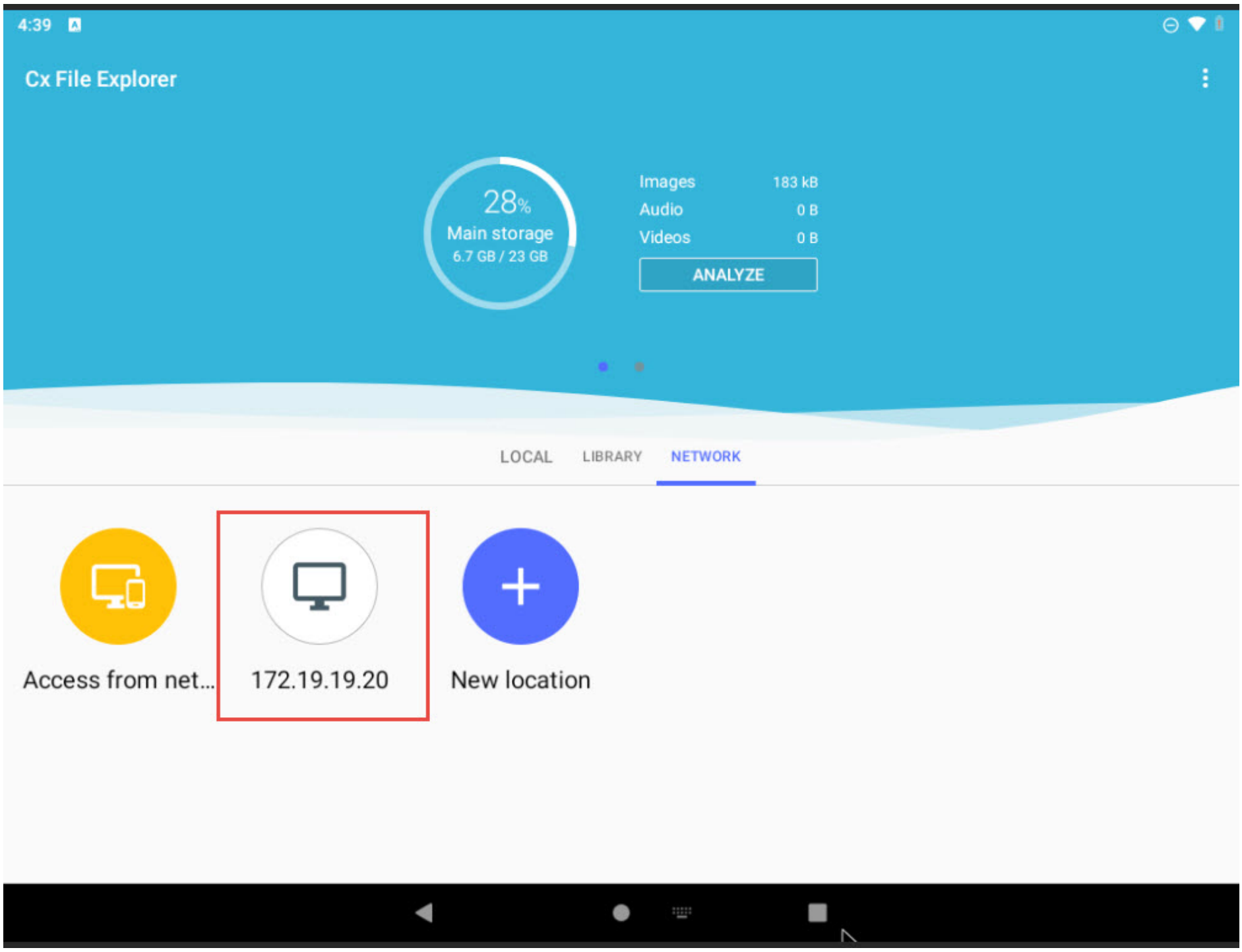
22. On the **Home Screen**, swipe from right to left to navigate to the second page of the **Home screen**.



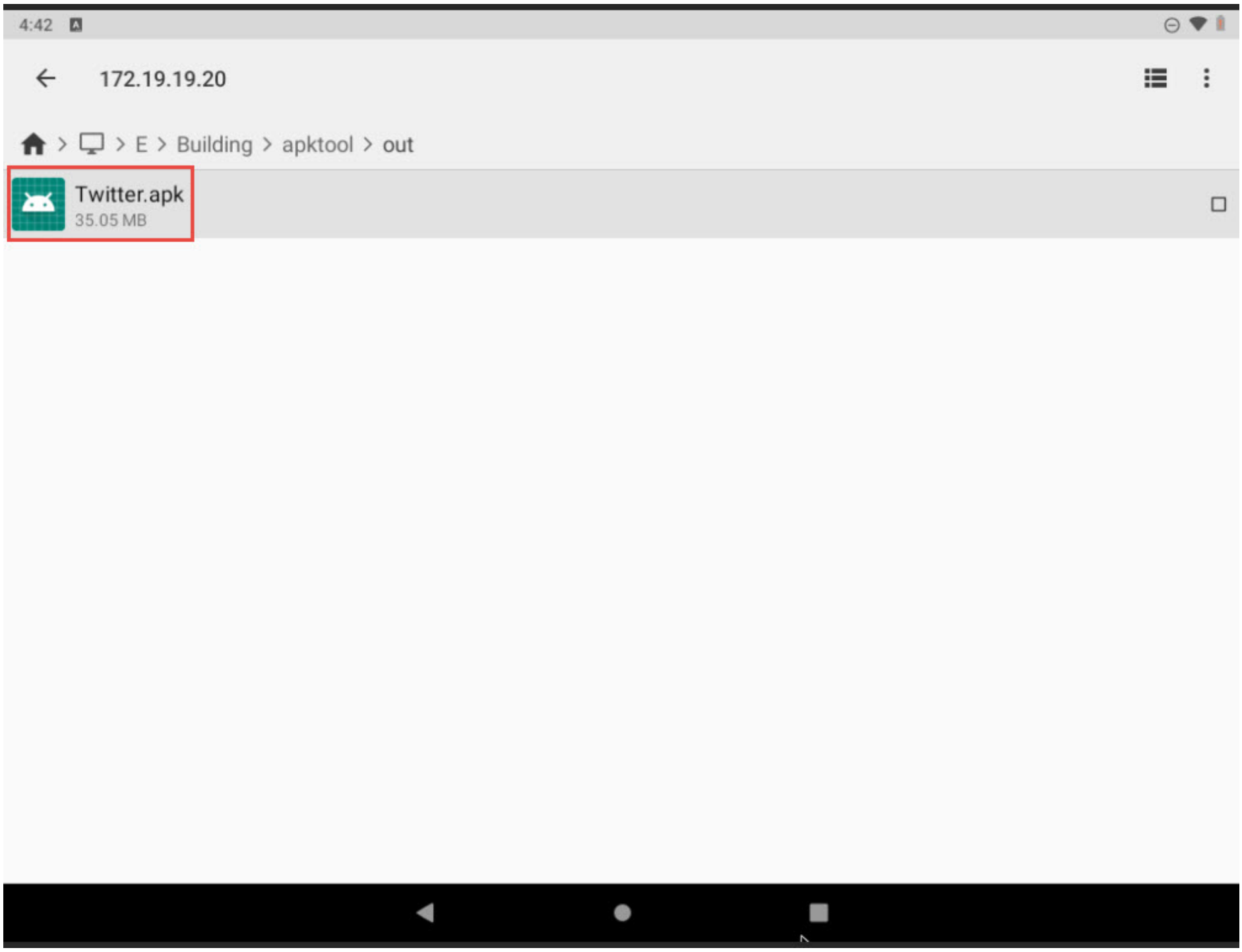
23. On the second page of the **Home screen**, click the **Cx File Explorer** app.



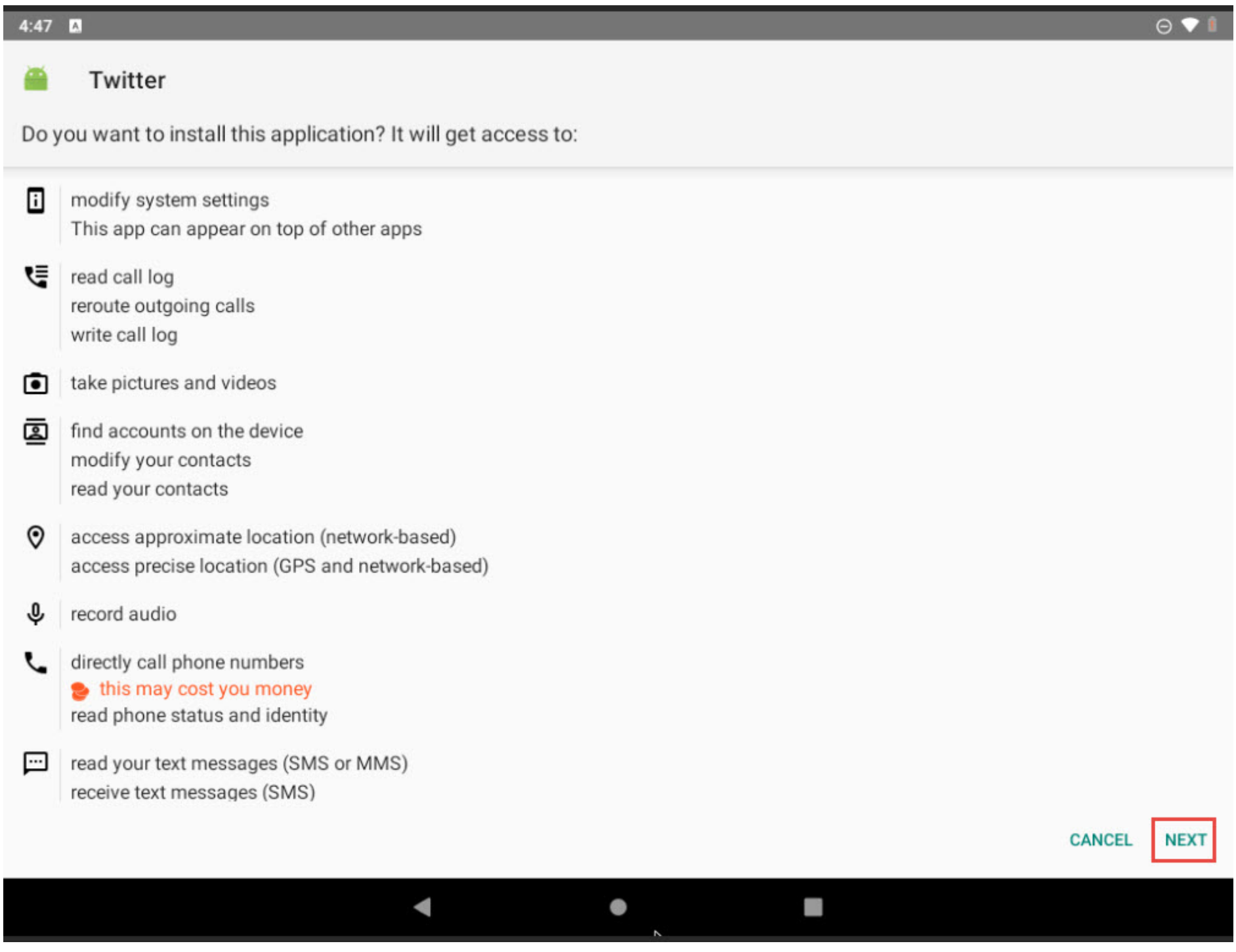
24. **Cx File Explorer** app appears; select **172.19.19.20** under the **Network** tab.



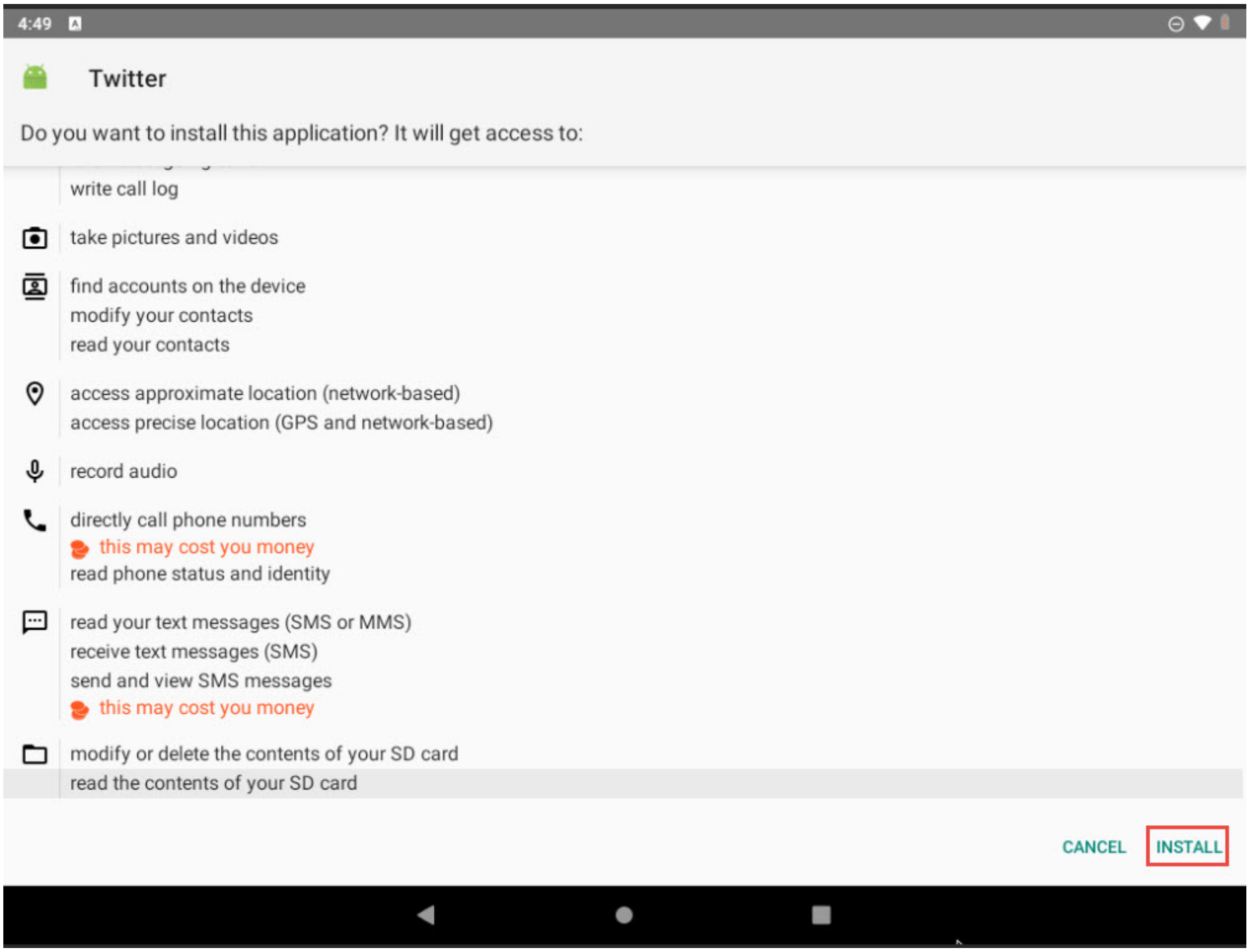
25. Now, navigate to **E > Building > apktool > out**. You need to install the malicious apk file in the emulator. In real-time, an attacker creates a malicious apk file and shares it with the victim through Email or any other means. We install the apk file directly by sharing the file through shared folder. Click **Twitter.apk**.



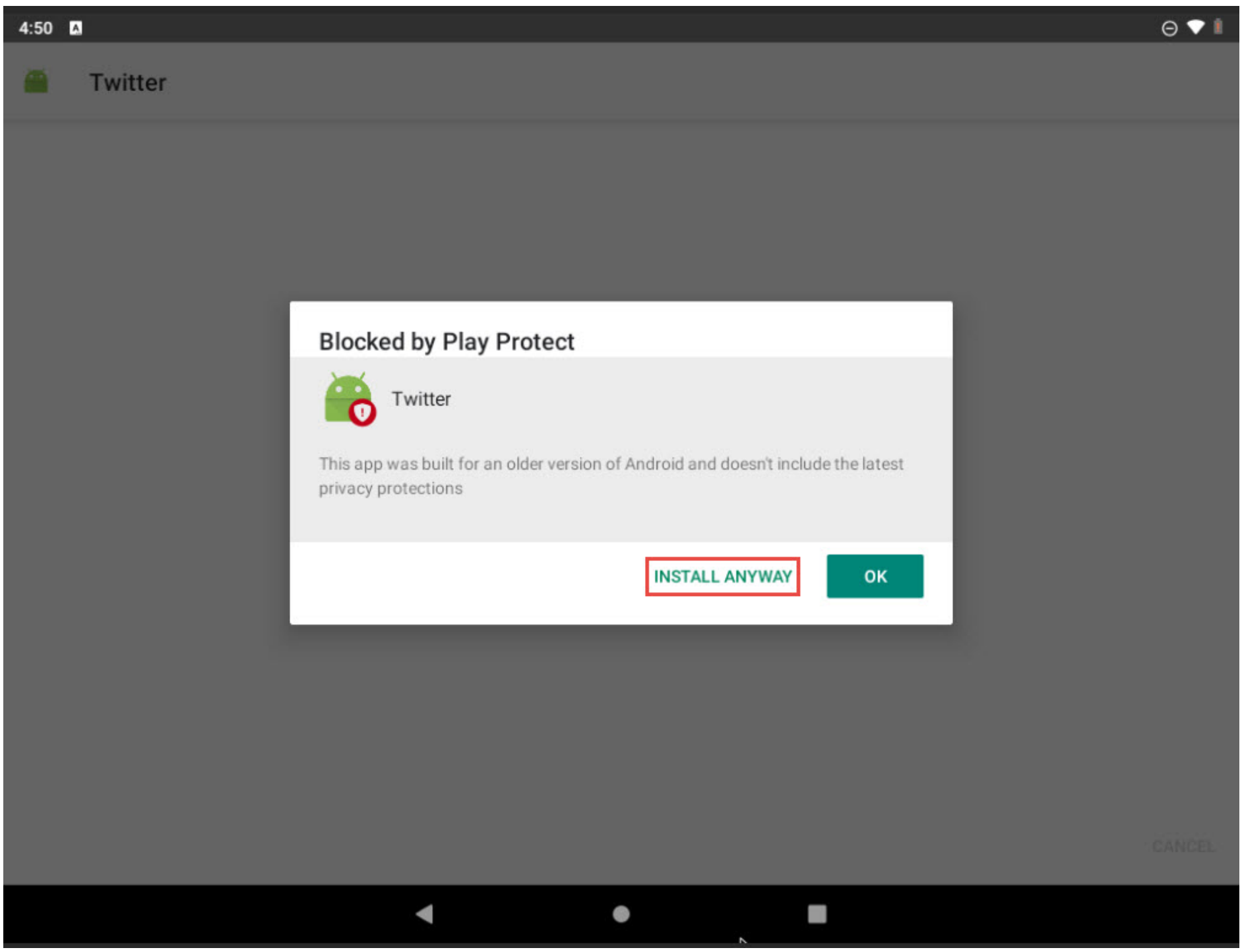
26. A **Do you want to install this application?** screen appears, click **NEXT**.



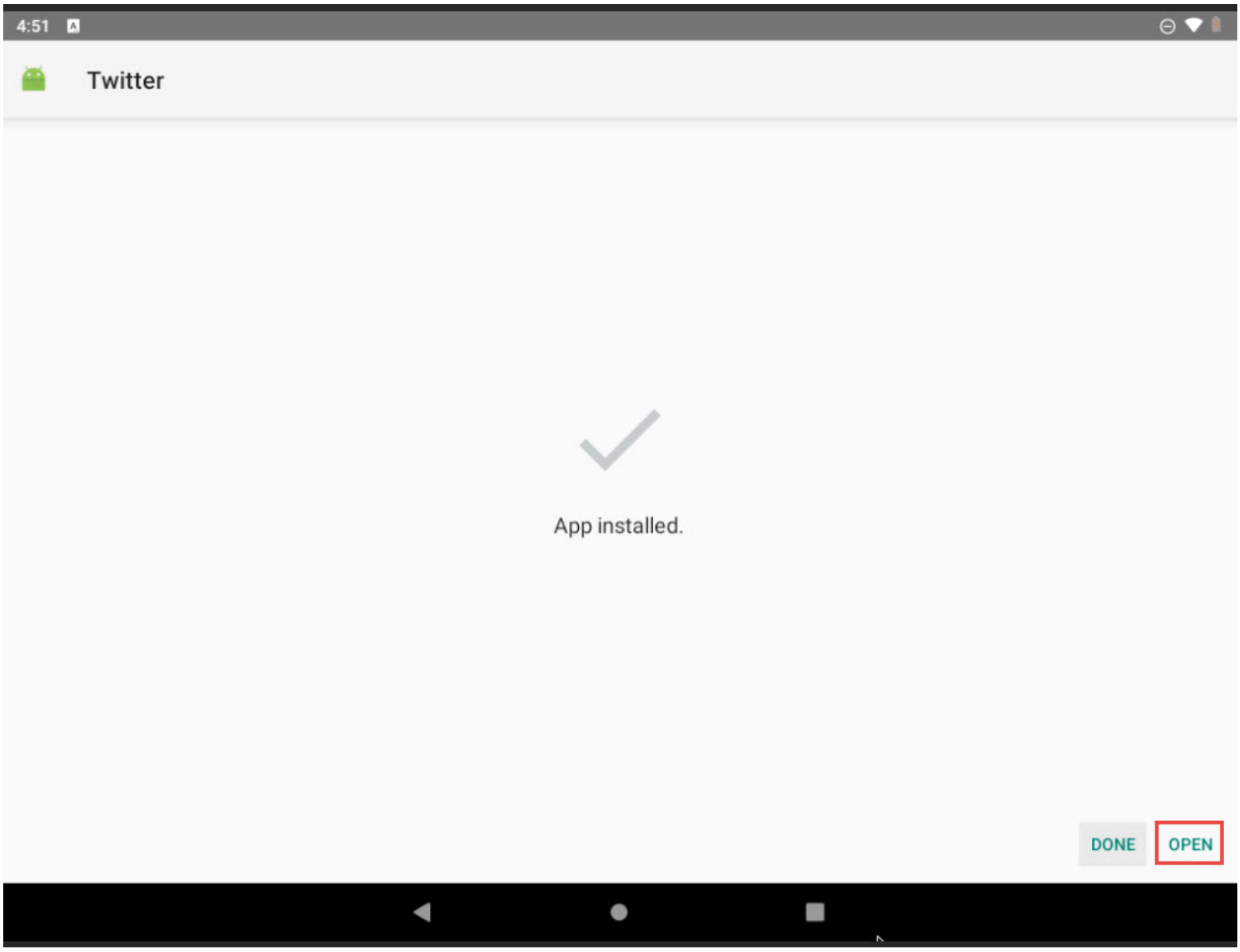
27. In the next screen, click **INSTALL**.



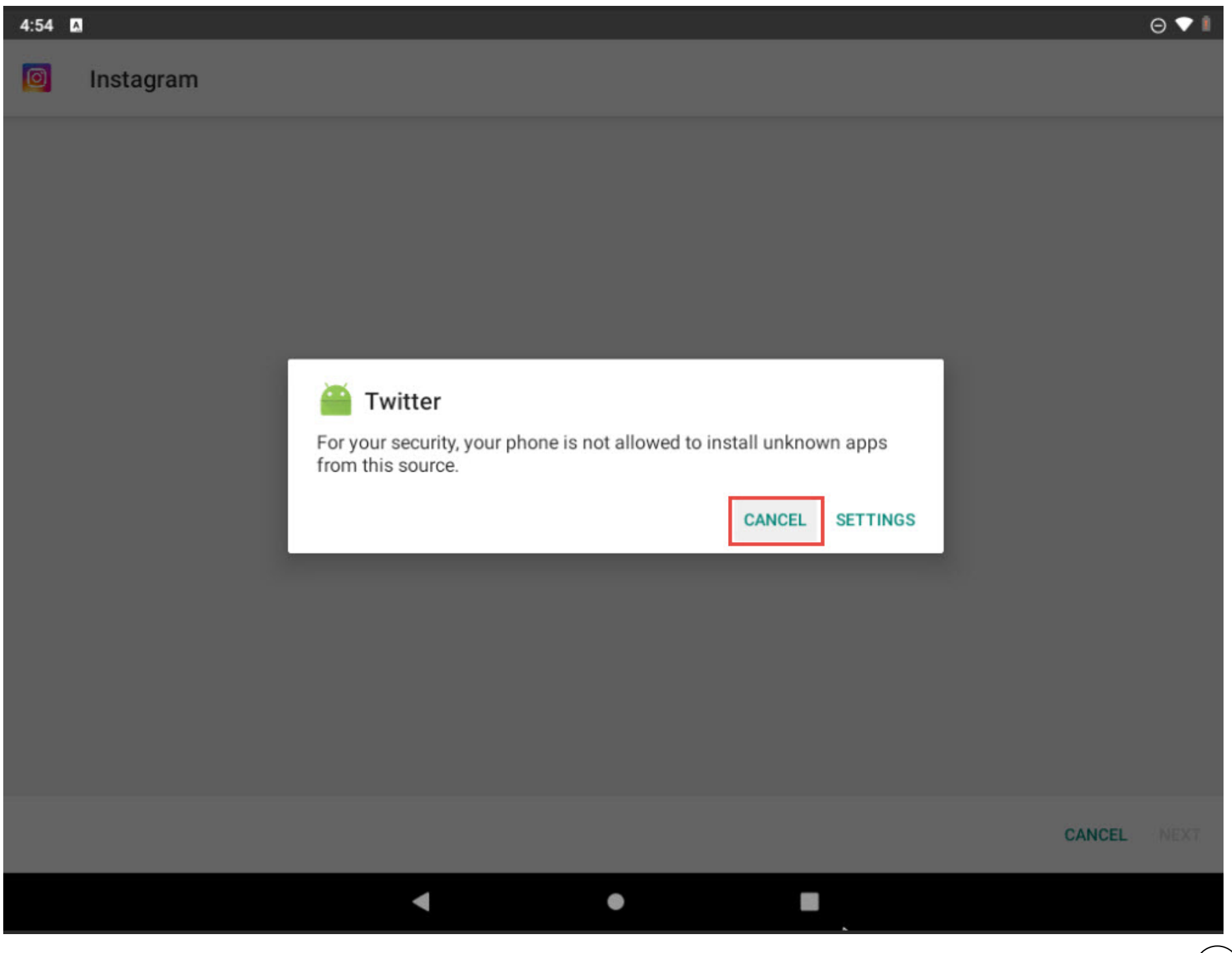
28. A **Blocked by Play Protect** screen appears, click **INSTALL ANYWAY**.



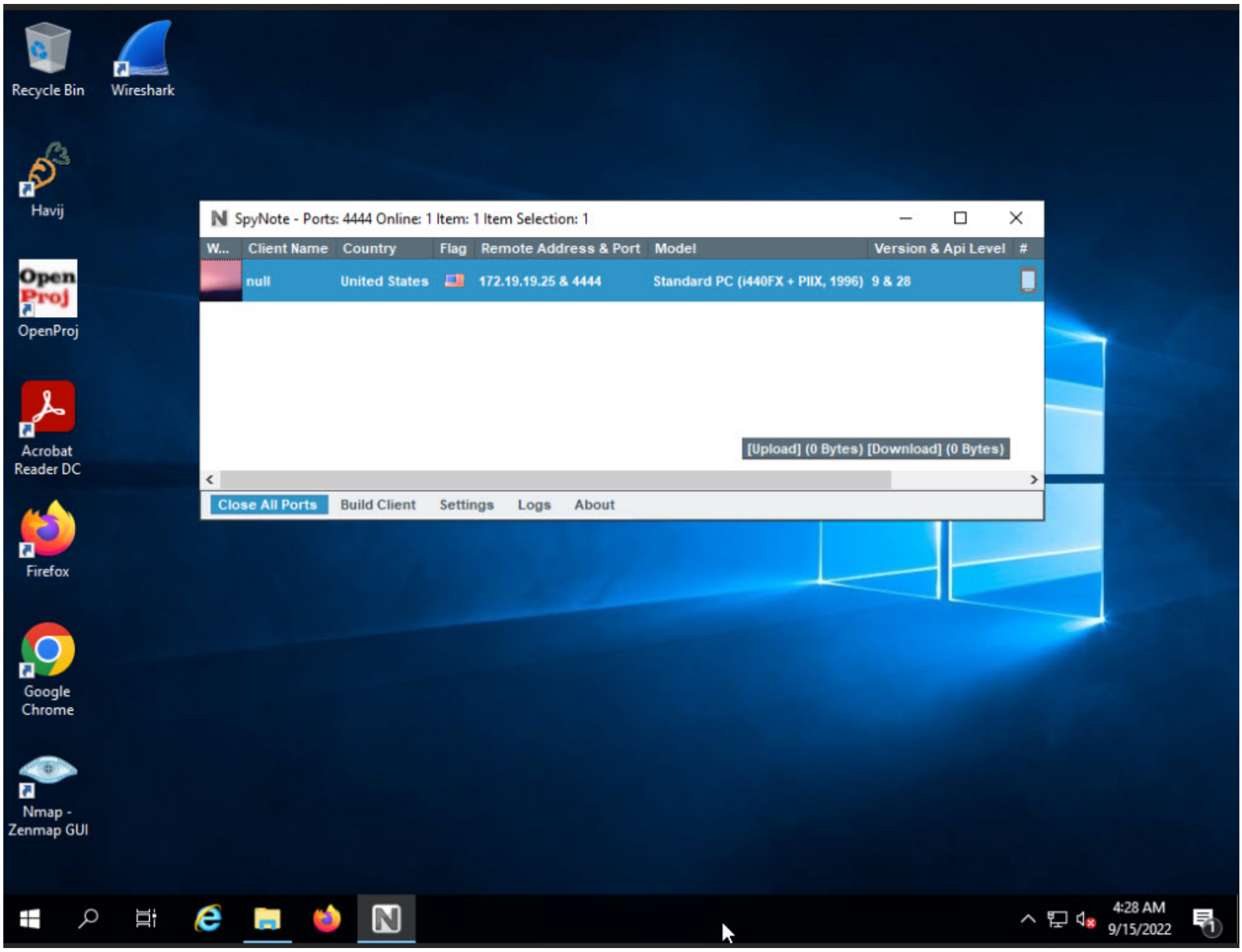
29. After the app installs, **App installed** notification appears, click **OPEN**.



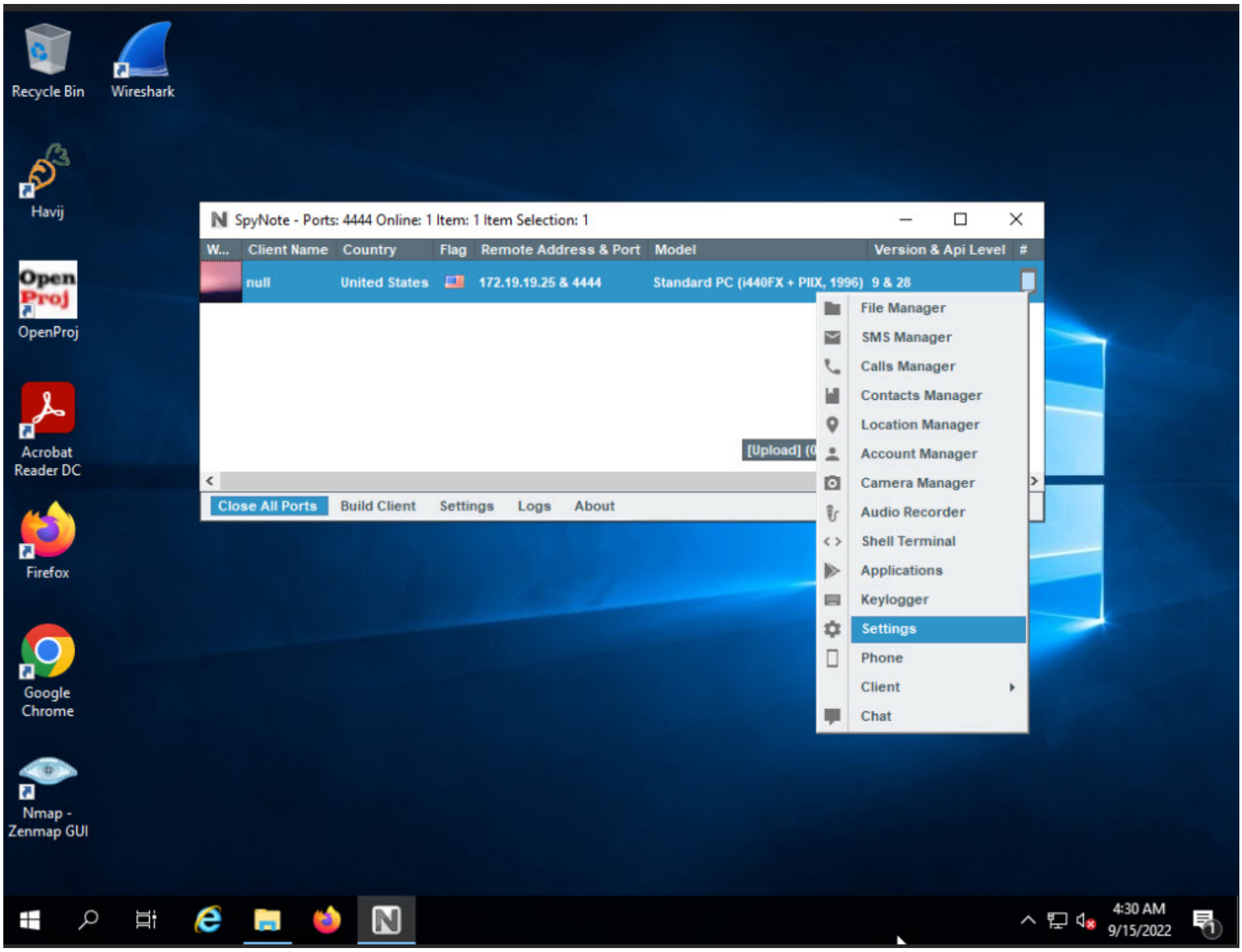
30. In the **Twitter** dialog box, click **CANCEL** and ignore any alerts in the Android machine .



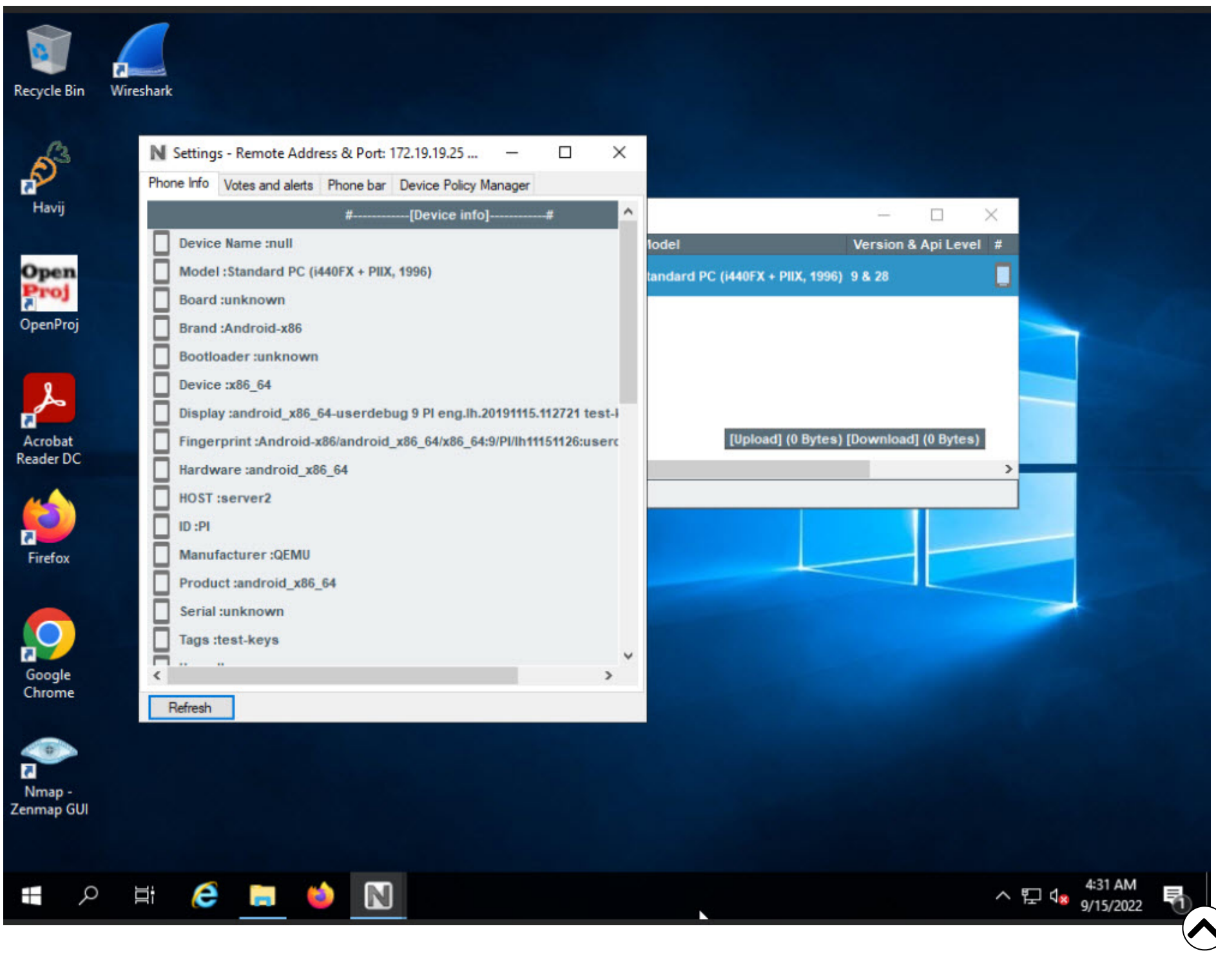
31. Now, select **CPENT Appendix K Windows Server 2019** machine and you can observe that the SpyNote Client has established a connection and displays the details of the victim device, as shown in the screenshot.



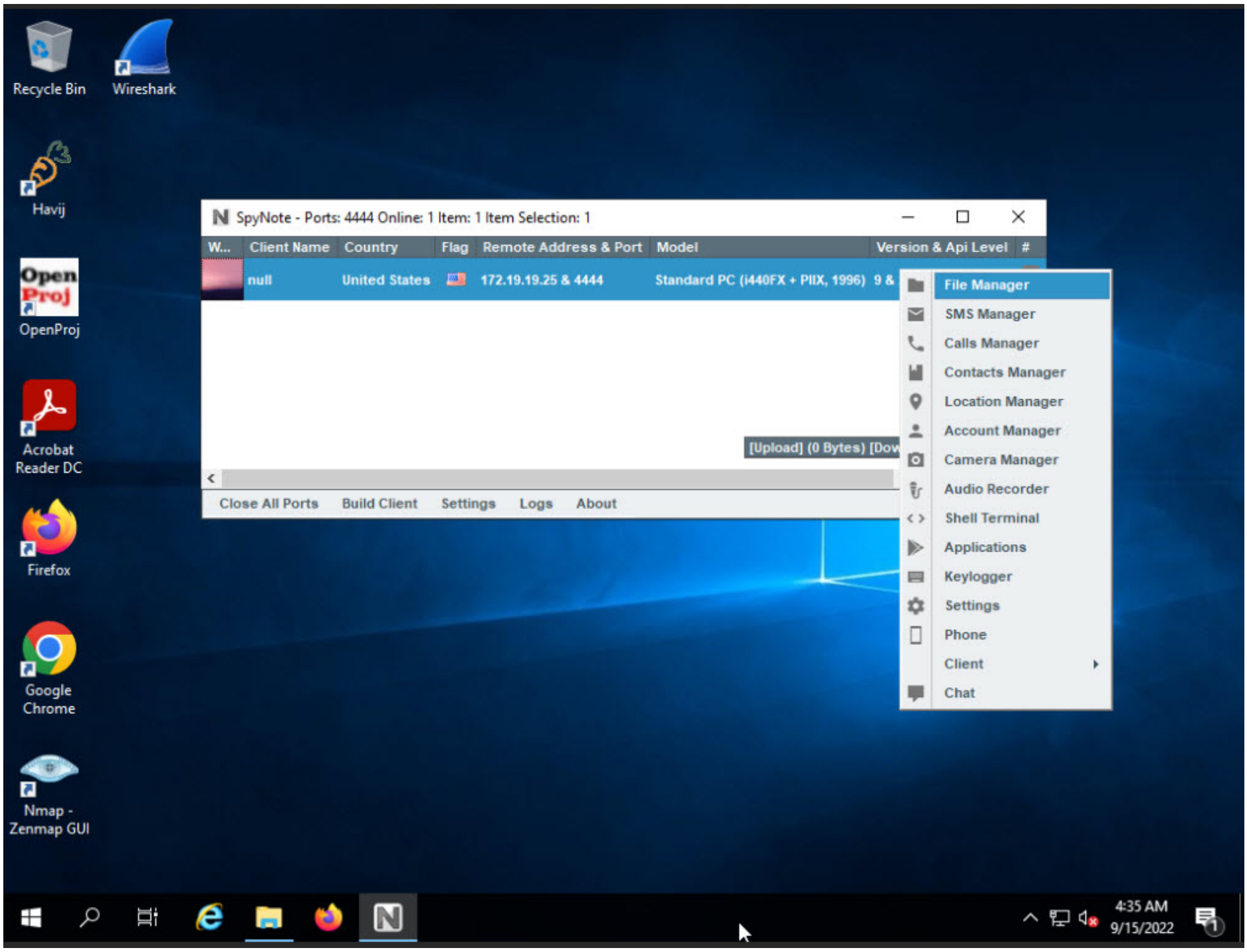
32. Right-click on the device connection and click on **Settings** to view the device information.



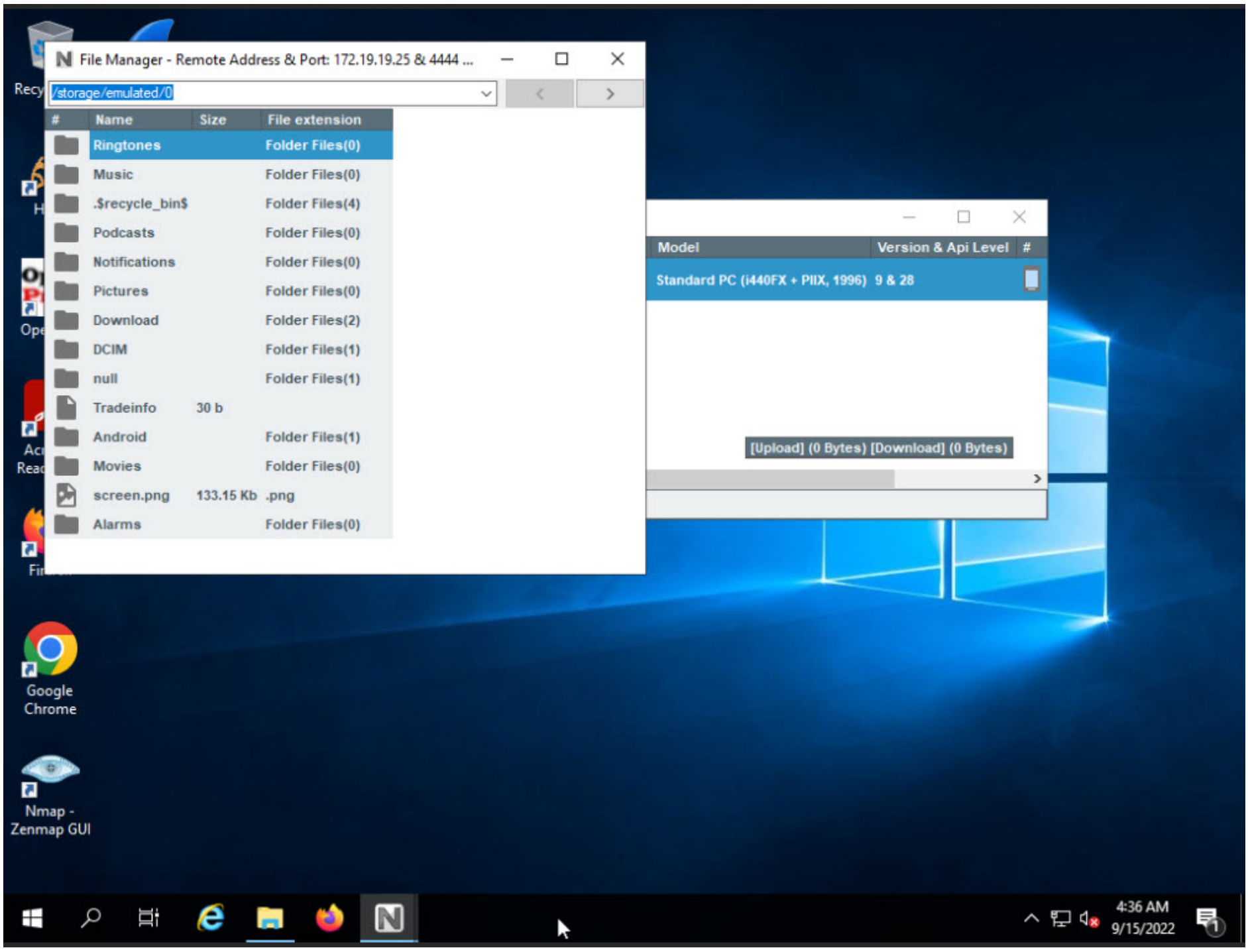
33. **Settings** window appears displaying the device information in the **Phone Info** tab. Scroll down the window to view detailed information. Once you are done viewing the information, close the **Settings** window.



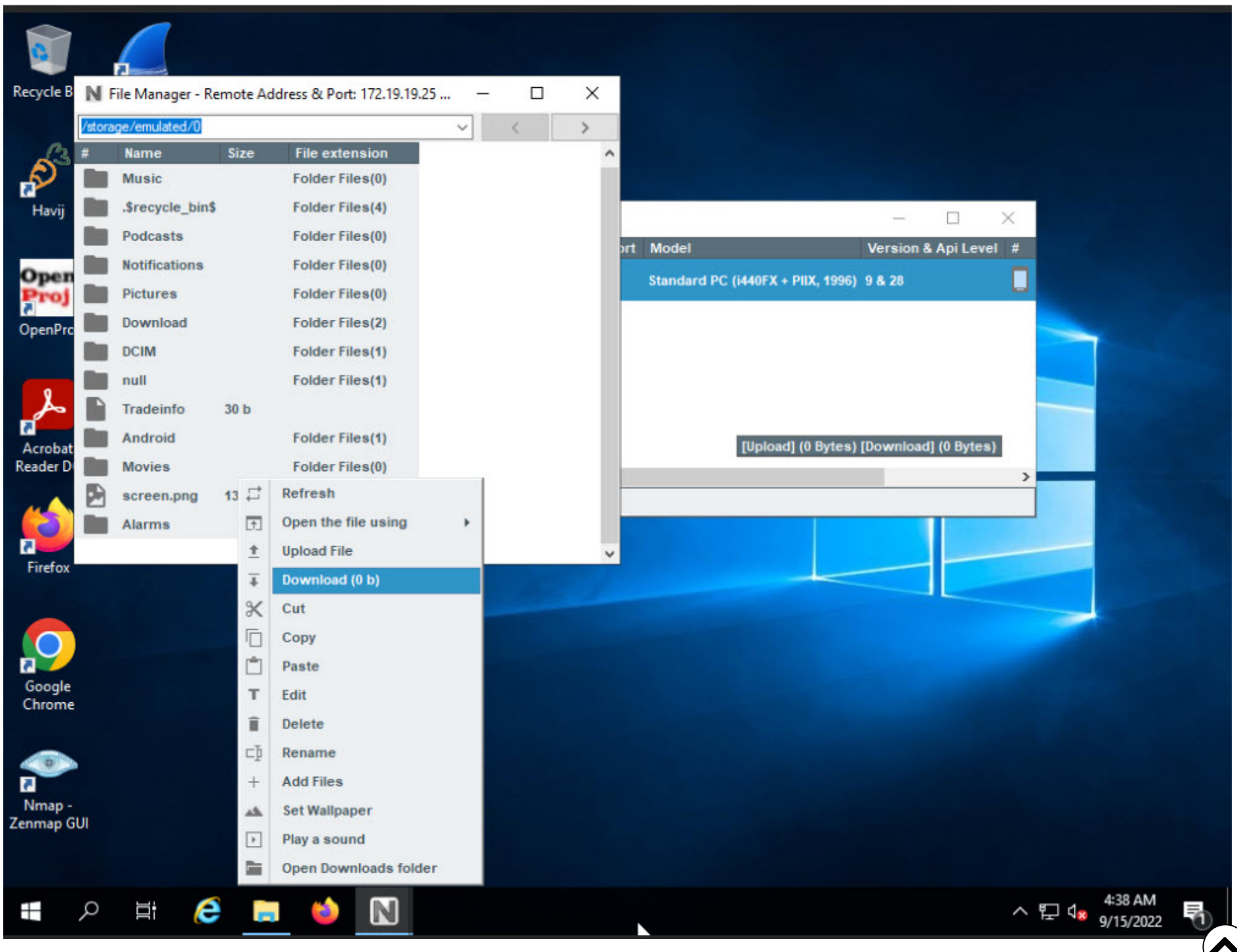
34. Right-click on the device connection and click on **File Manager** to view the file manager in the emulator.



35. **File Manager** window appears displaying the contents of **/storage/emulated/0** location.



36. If you want to download a file, right-click on the desired file and click **Download**. This downloads the file to the local machine. Close the File Manager window.



37. In the same way, you may use other features of SpyNote and explore the contents of the emulator.

In this lab, you have learned how to gain remote access to a mobile device (emulator) using **SpyNote**.
