Lab 2: Secure Android Devices using Various Android Security Tools

Lab Scenario

Like personal computers, mobile devices store sensitive data and are susceptible to various threats. Therefore, they should be properly secured in order to prevent the compromise or loss of confidential data, lessen the risk of various threats such as viruses and Trojans, and mitigate other forms of abuse. Strict measures and security tools are vital to strengthening the security of these devices.

Android's growing popularity has led to increased security threats, ranging from typical malware to advanced phishing and identity theft techniques. As a professional ethical hacker or penetration tester, you should scan for any unsecured settings on the mobile device you are assessing, and then take appropriate action to secure them. You must do this before hackers exploit these vulnerabilities by; for example, downloading sensitive data, committing a crime using your Android device as a launchpad, and ultimately endangering your business.

There are various security tools available for scanning, detecting, and assessing the vulnerabilities and security status of Android devices. Many security software companies have launched their own apps, including several complete security suites with antitheft capabilities.

The tasks in this lab will assist you in performing a security assessment of a target Android device.

Lab Objectives

- Analyze a malicious app using online Android analyzers
- Secure Android devices from malicious apps using Malwarebytes Security

Overview of Android Security Tools

Android security tools reveal the security posture of particular Android platforms and devices. You can use them to find various ways to strengthen the security and robustness of your organization's mobile platforms. These tools automate the process of accurate Android platform security assessment.

Task 1: Analyze a Malicious App using Online Android Analyzers

Online Android analyzers allow you to scan Android APK packages and perform security analyses to detect vulnerabilities in particular apps. Some trusted online Android analyzers are Sixo Online APK Analyzer.

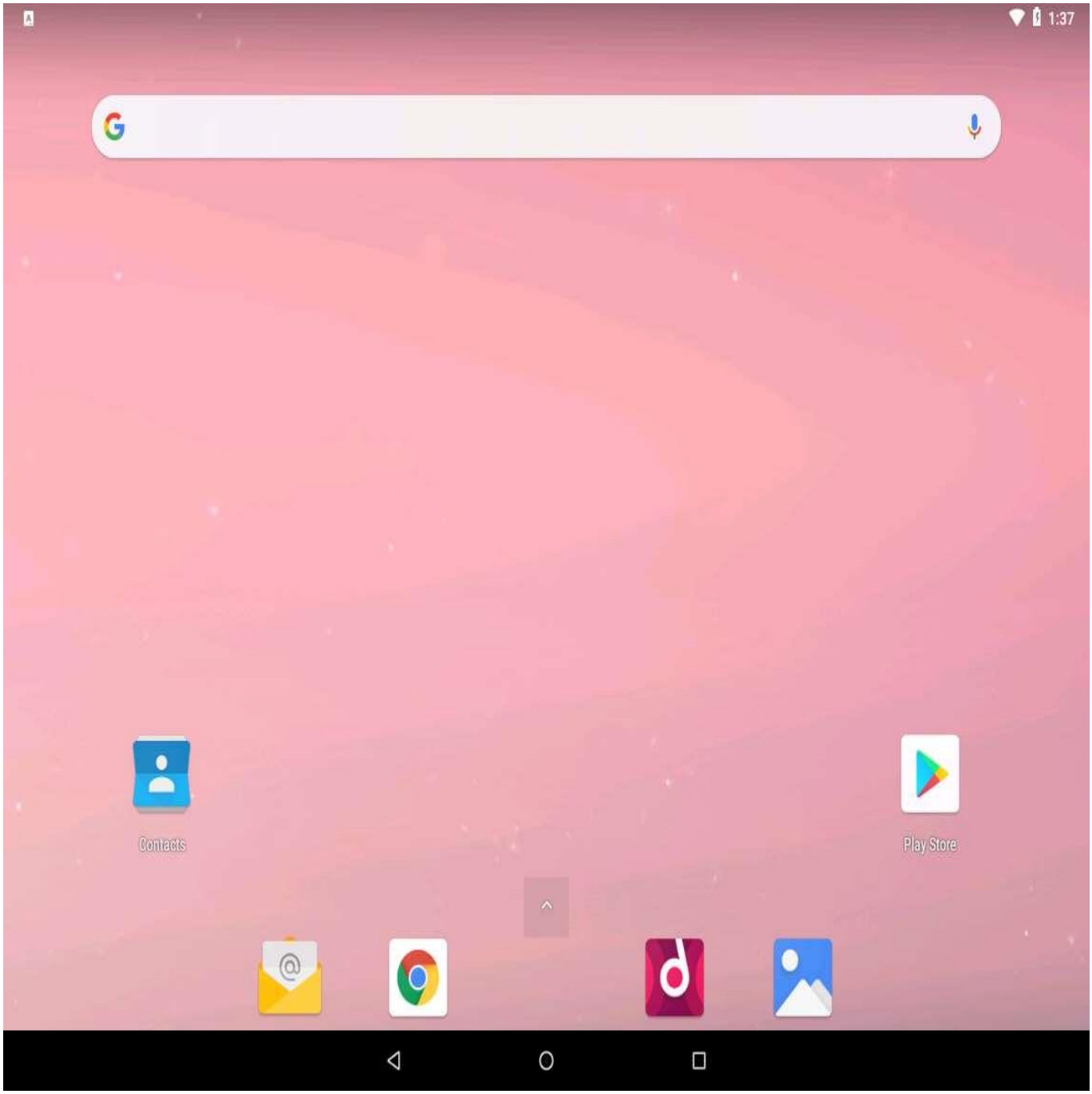
In this task, we will analyze a malicious app using various online Android analyzers.

In this lab, we will be analyzing the malicious file (**Backdoor.apk**), which we used in the previous lab to hack the target Android platform.

If the malicious file (**Backdoor.apk**) is missing then follow the steps given in Lab 1 Task 1 (**Hack an Android Device by Creating Binary Payloads using Parrot Security**) to re-create the file.

1. Click Android to switch to the **Android** machine, click the **Google Chrome** browser icon on the **Home screen** to launch Chrome.

   Restart the machine, if it non-responsive.

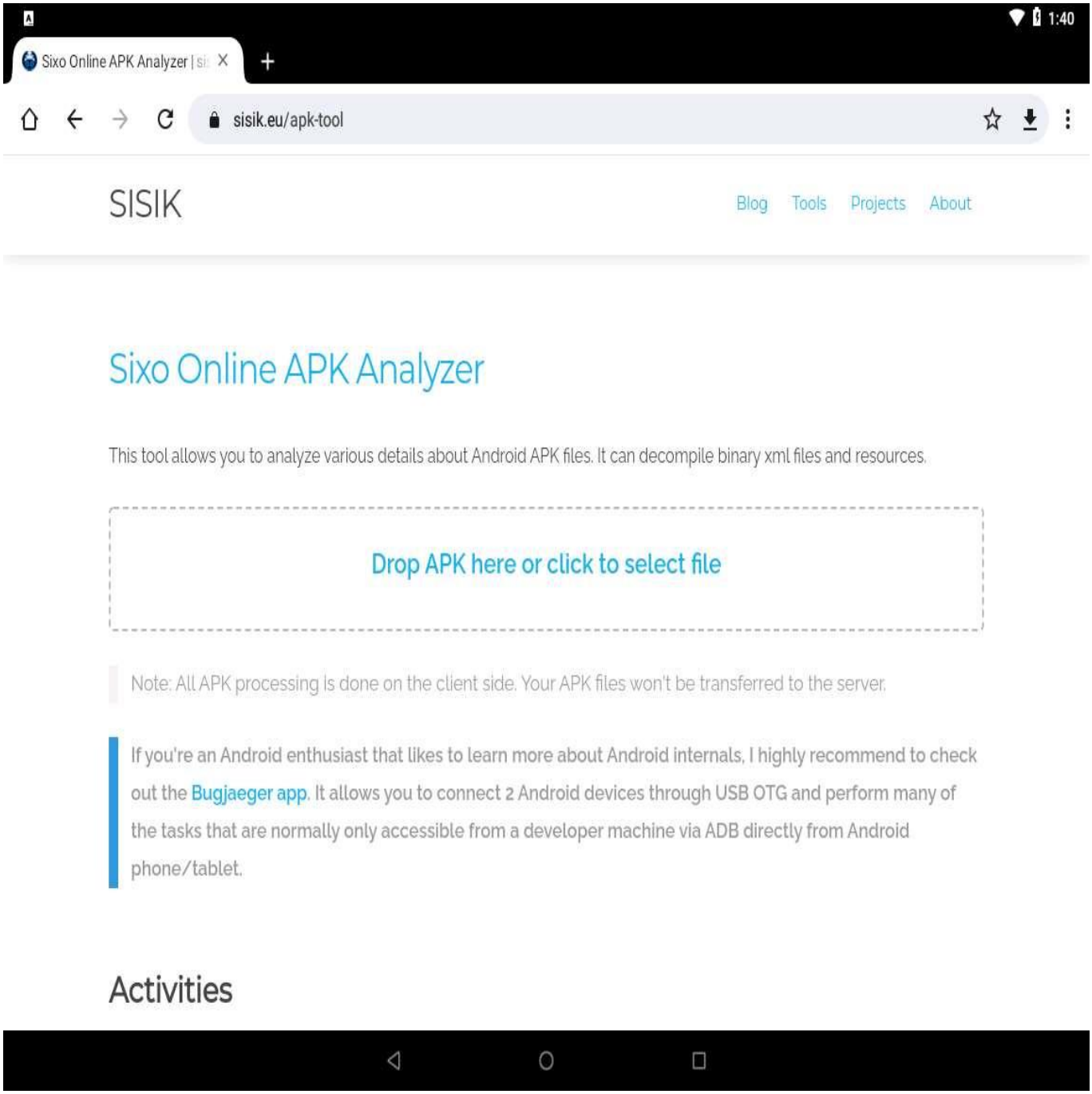


2. In **Chrome**, type **https://www.sisik.eu/apk-tool** in the address bar and press **Enter**.
3. The **Sixo Online APK Analyzer** webpage loads, as shown in the screenshot.

If a cookie notification pop-up appears, click **Got it!**

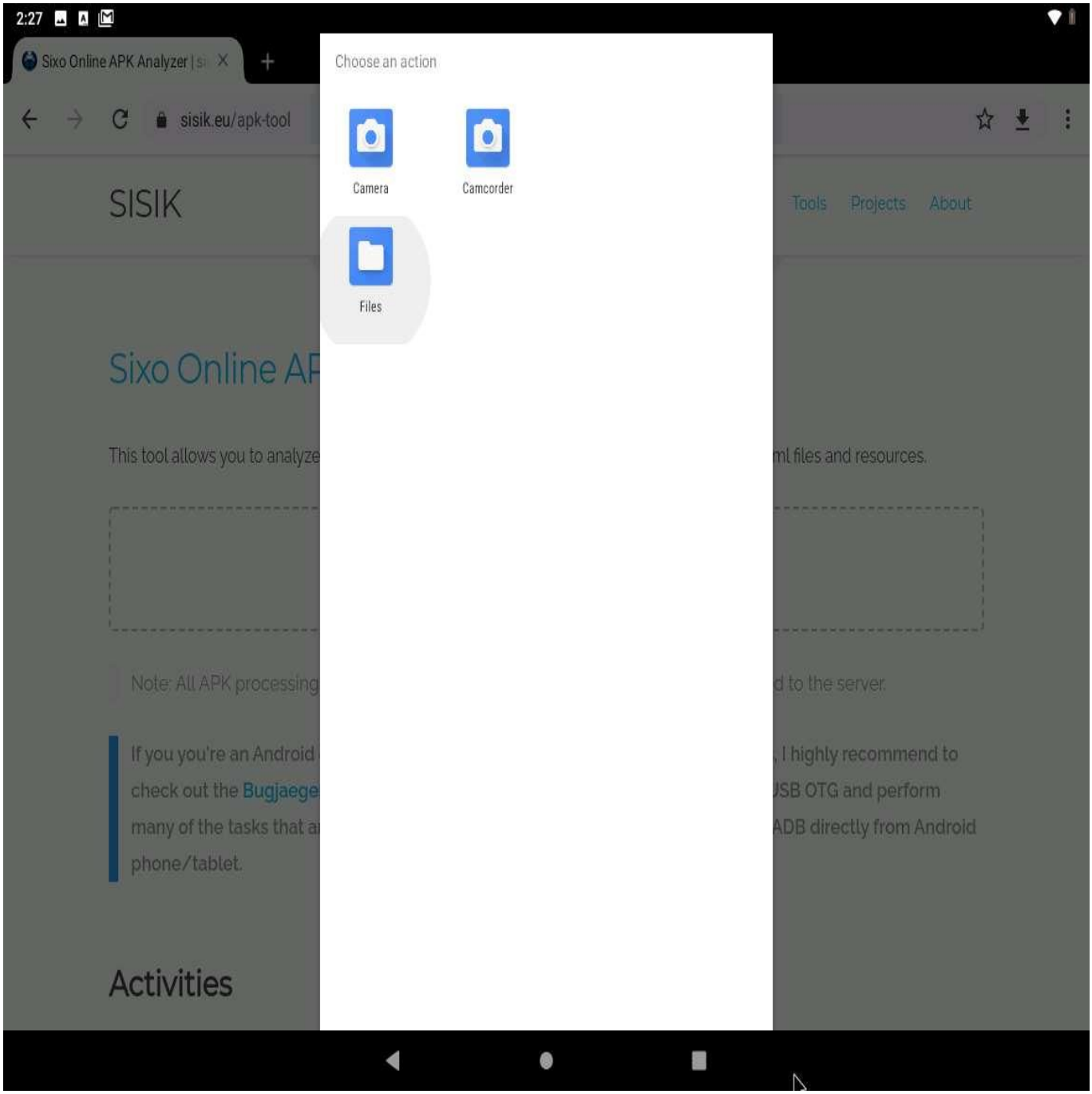
4. Click the **Drop APK here or click to select file** field to upload an APK file from the device.

Sixo Online APK Analyzer allows you to analyze various details about Android APK files. It can decompile binary XML files and resources.



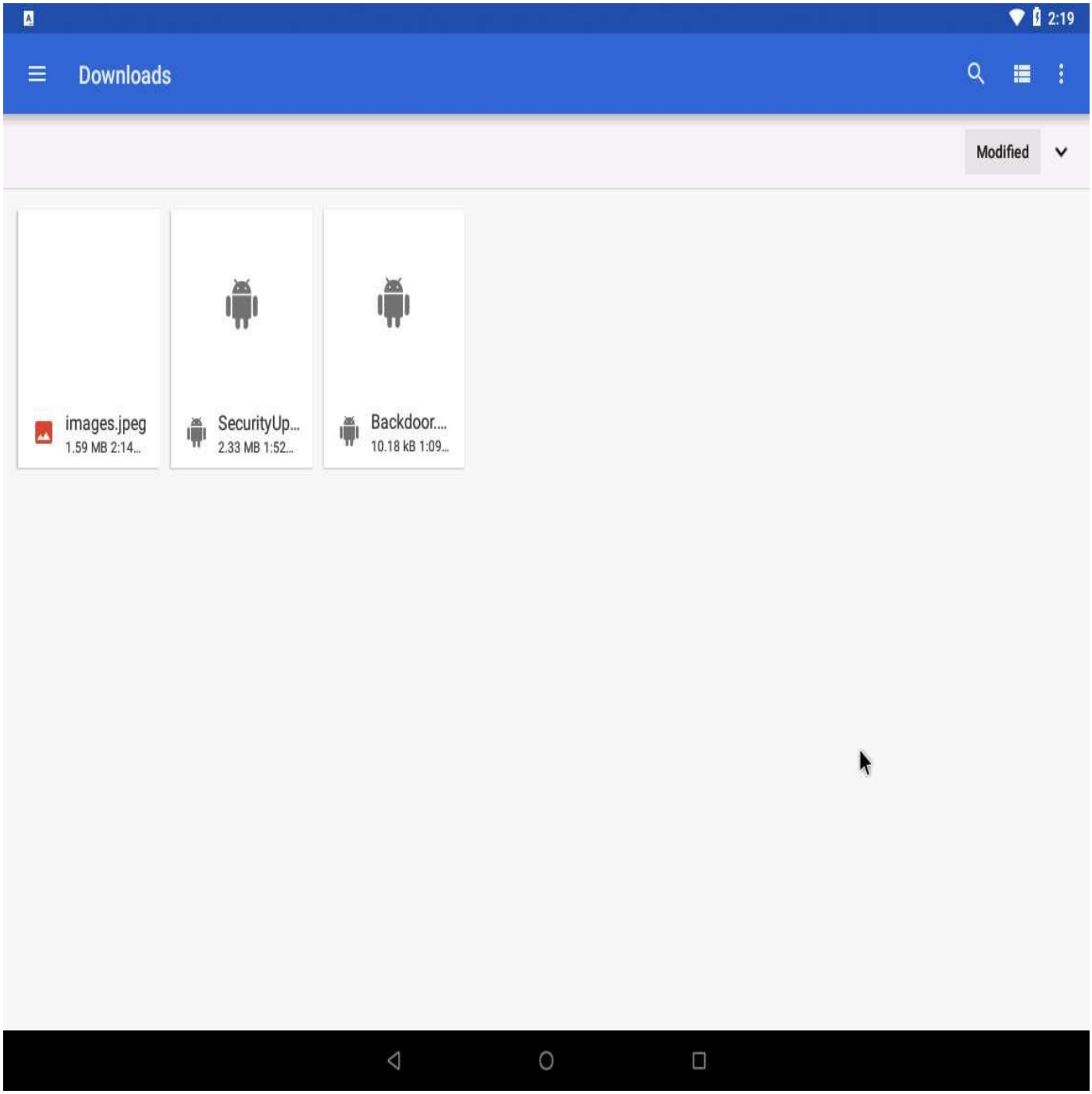
5. In the **Choose an action** pop-up, click **Files**.

If Chrome pop-up appears, click **ALLOW**.

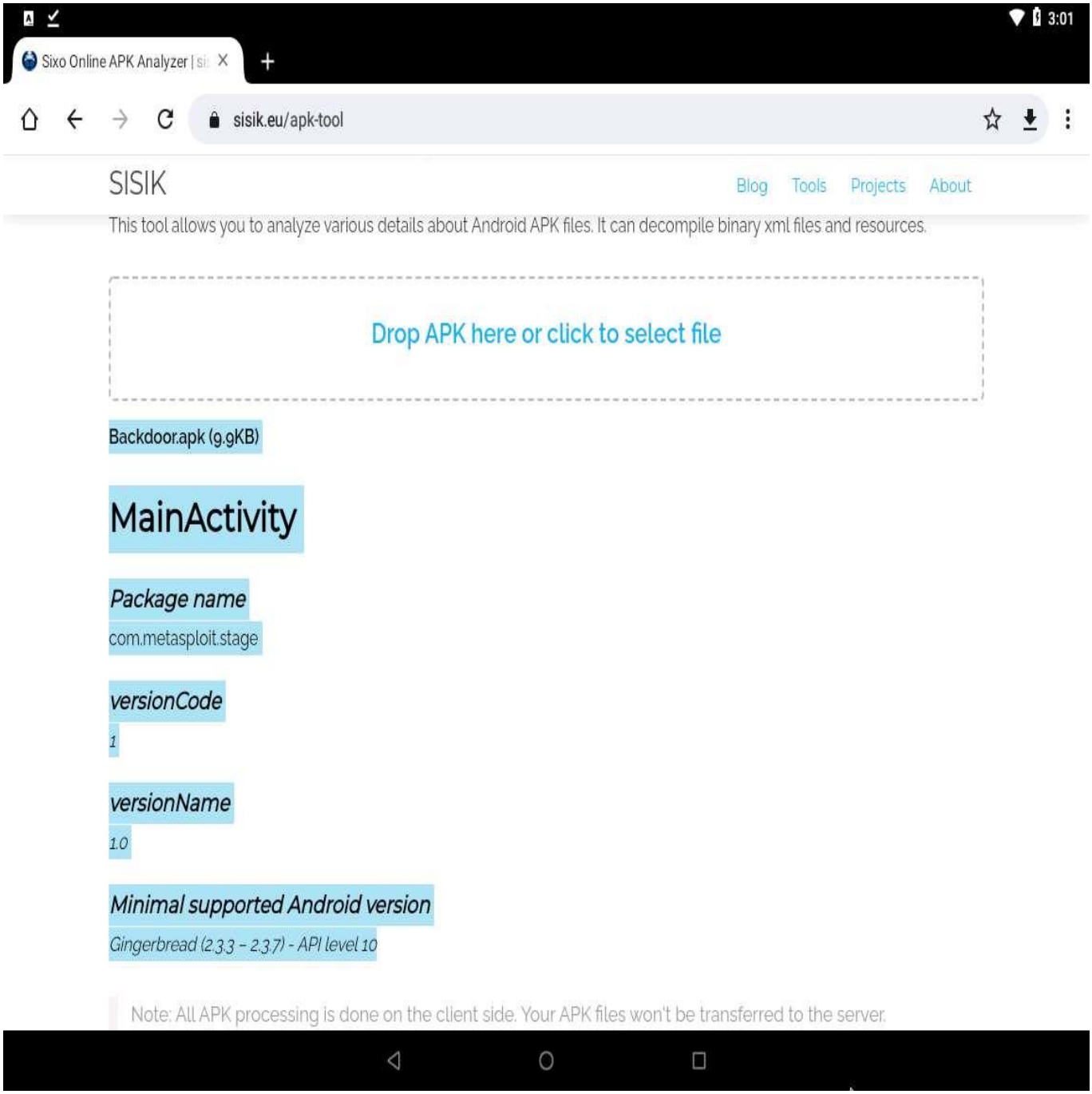


6. ☐ The **Downloads** screen appears; double-click the **Backdoor.apk** file.

If you find yourself in a folder called **Recent**, navigate to the **Downloads** folder by clicking on the ellipse icon in the top-left corner.

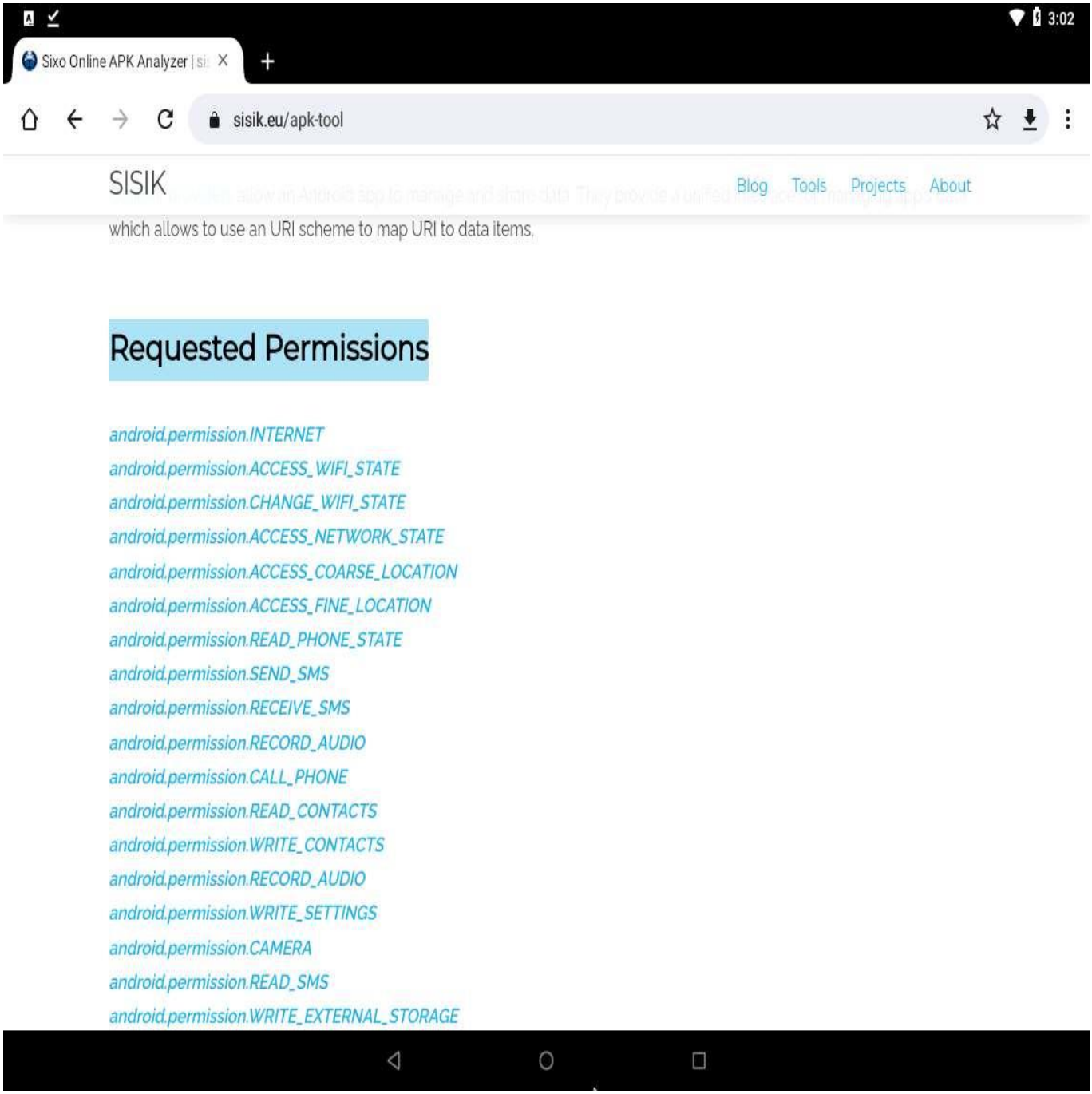


7. ☐ The browser window reappears with the information about the uploaded file (**Backdoor.apk**), as shown in the screenshot.



8. Scroll down to the **Requested Permissions** section to view information regarding the app's requested permissions.

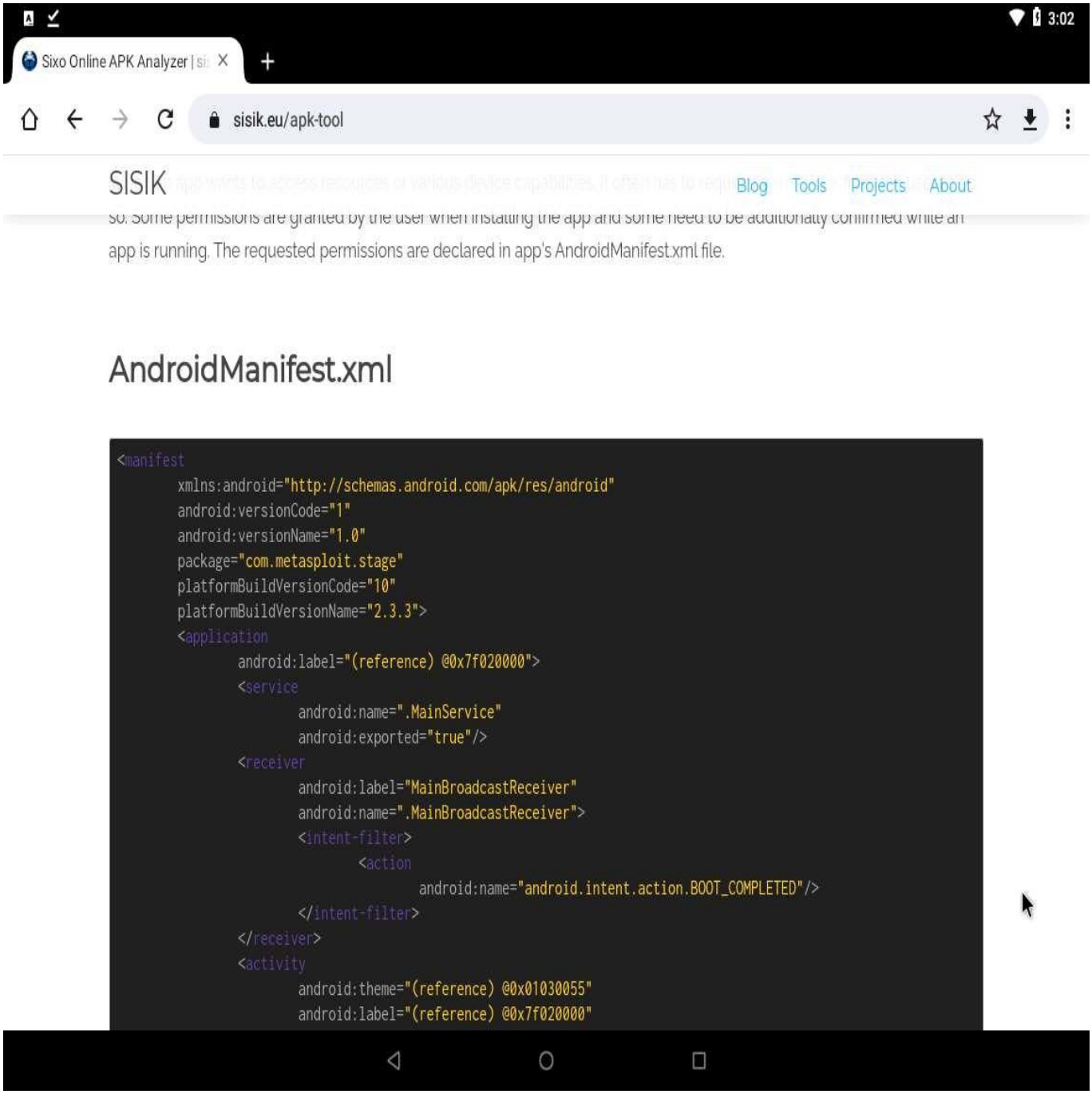
When an app wants to access resources or various device capabilities, it typically must request permission from the user to do so. Some permissions are granted by the user when installing the app and some need to be confirmed later while the app is running. The requested permissions are declared in the app's AndroidManifest.xml file.



9. ☐ Scroll down to the **AndroidManifest.xml** section, which consists of essential information about the APK file.

The manifest file contains important information about the app that is used by development tools, the Android system, and app stores. It contains the app's package name, version information, declarations of app components, requested permissions, and other important data. It is serialized into a binary XML format and bundled inside the app's APK file.

more...



10. ☐ You can also scroll down to view information about the app's **APK Signature**, **App Source Code**, etc.
11. ☐ This concludes the demonstration of analyzing a malicious app using online Android analyzers.
12. ☐ You can also use other online Android analyzers such as **SandDroid** (http://sanddroid.xjtu.edu.cn), and **Apktool** (http://www.javadecompilers.com), to analyze malicious applications.
13. ☐ Close all open windows and document all the acquired information.
14. ☐ You can also use other Android vulnerability scanners such as **X-Ray 2.0** (https://duo.com), **Vulners Scanner** (https://play.google.com), **Shellshock Scanner - Zimperium** (https://play.google.com), **Yaazhini** (https://www.vegabird.com), and **Quick Android Review Kit (QARK)** (https://github.com) to analyze malicious apps for vulnerabilities.
15. ☐ Close all open windows and document all the acquired information.

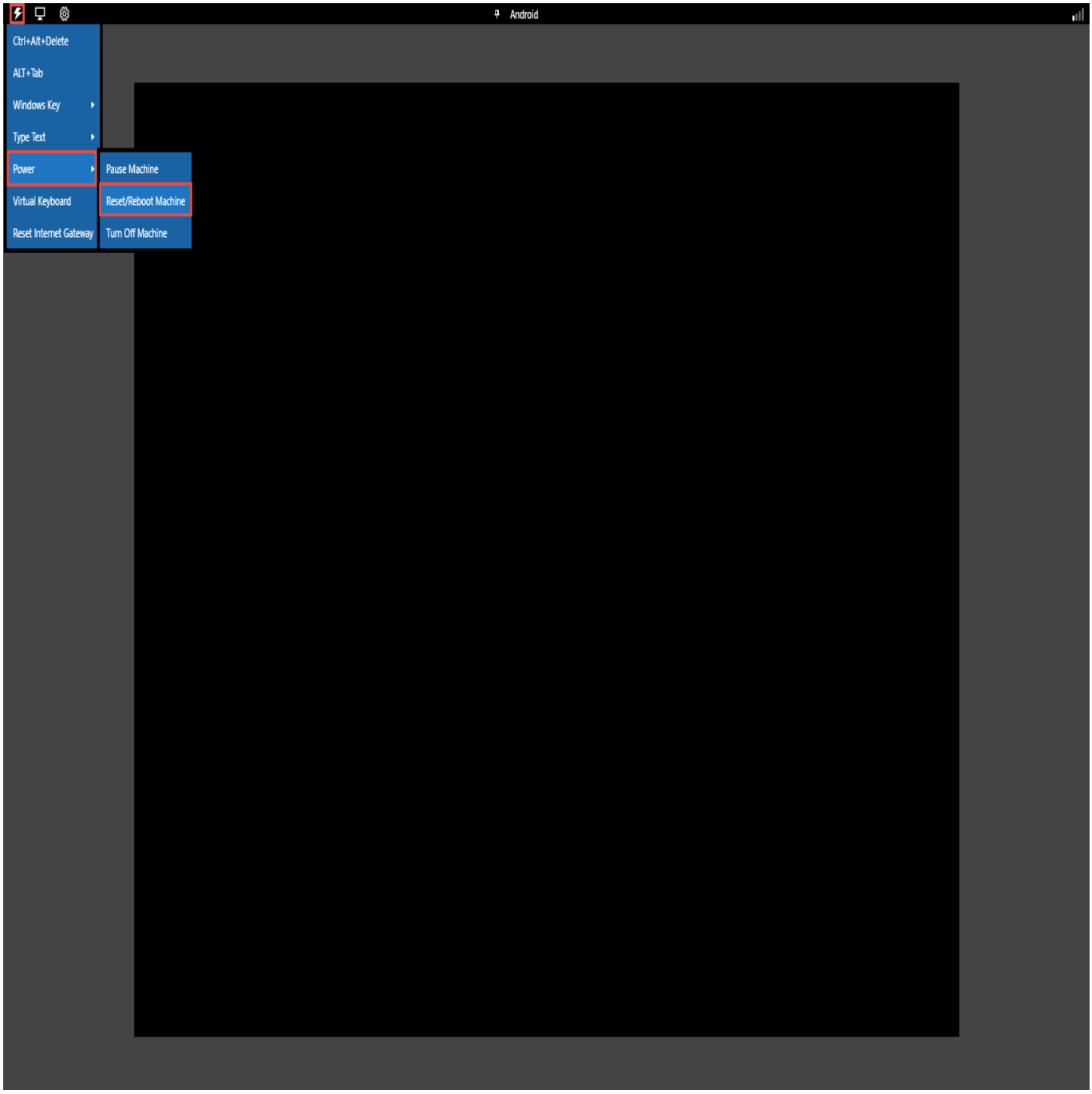
Task 2: Secure Android Devices from Malicious Apps using Malwarebytes Security

Malwarebytes is an antimalware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It blocks, detects, and removes adware and malware; conducts privacy audits for all apps; and ensures safer browsing.

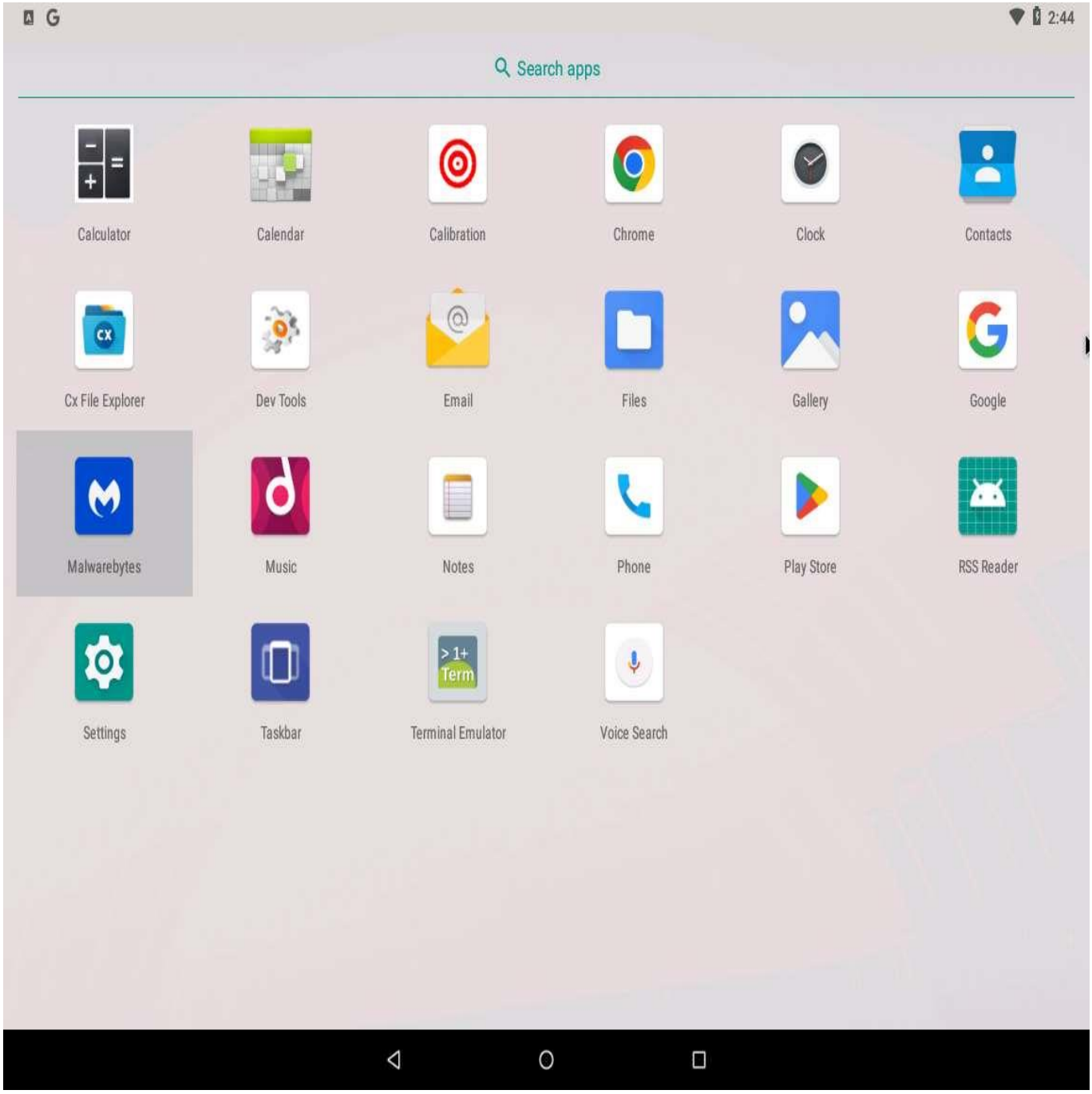
In this task, we will secure an Android device from malicious applications using Malwarebytes Security.

1. In the **Android** machine, click **Commands** icon from the top-left corner of the screen, navigate to **Power** --> **Reset/Reboot machine**.

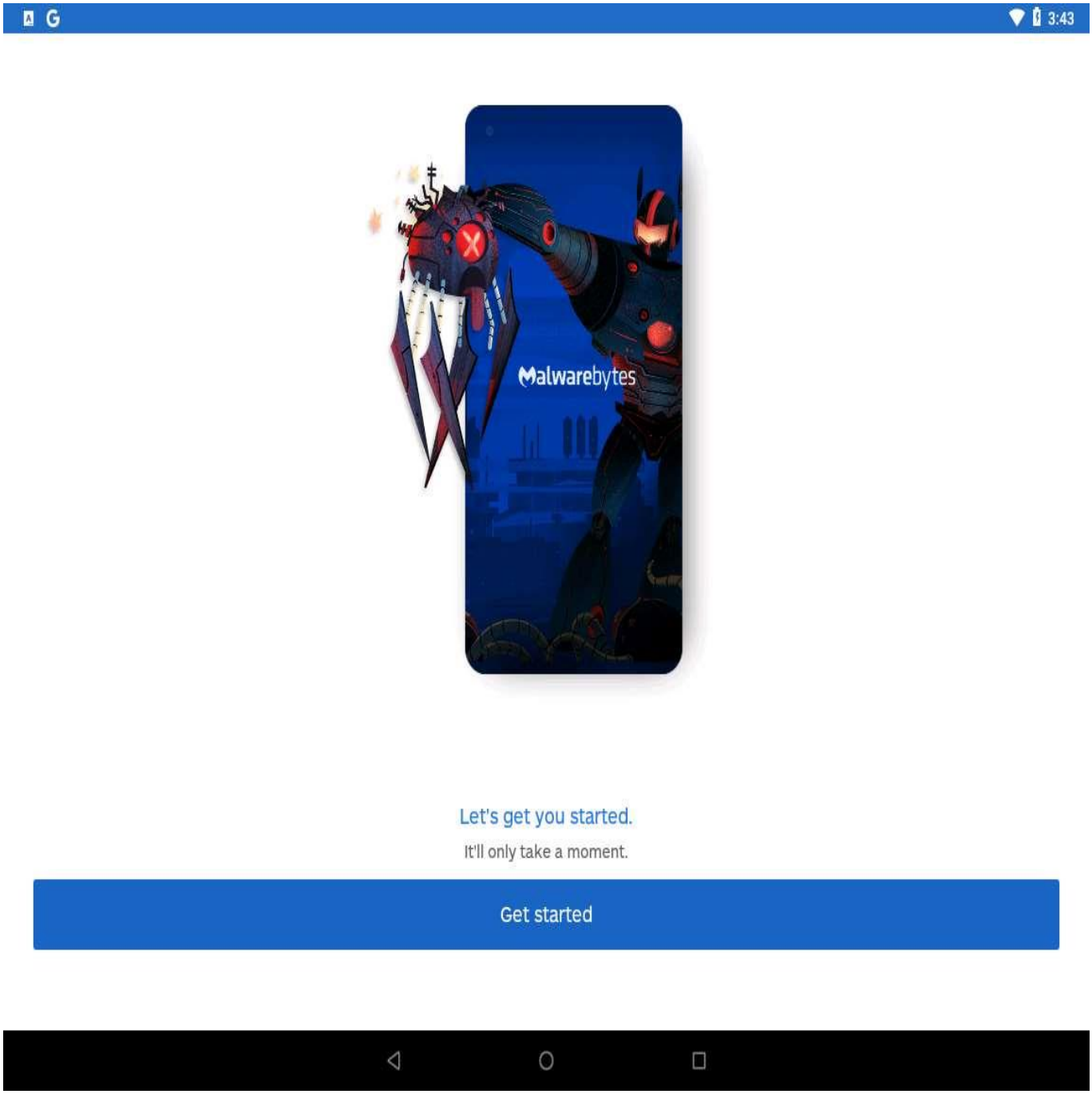
   If **Reset/Reboot machine** pop-up appears, click **Yes** to proceed.



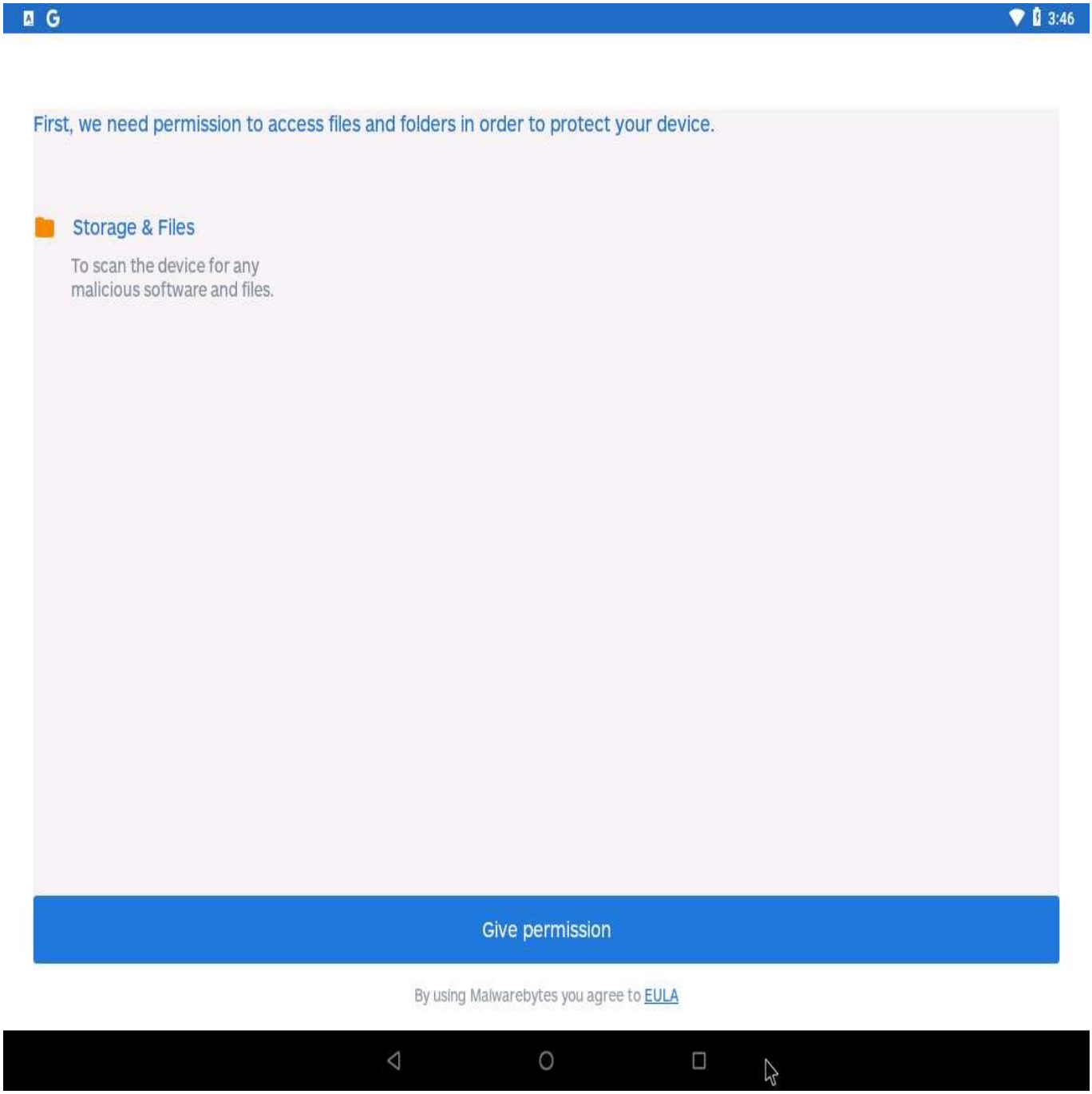
2. ☐ After the machine reboots, swipe-up the home screen, which will show all apps. Click on the **Malwarebytes** app.



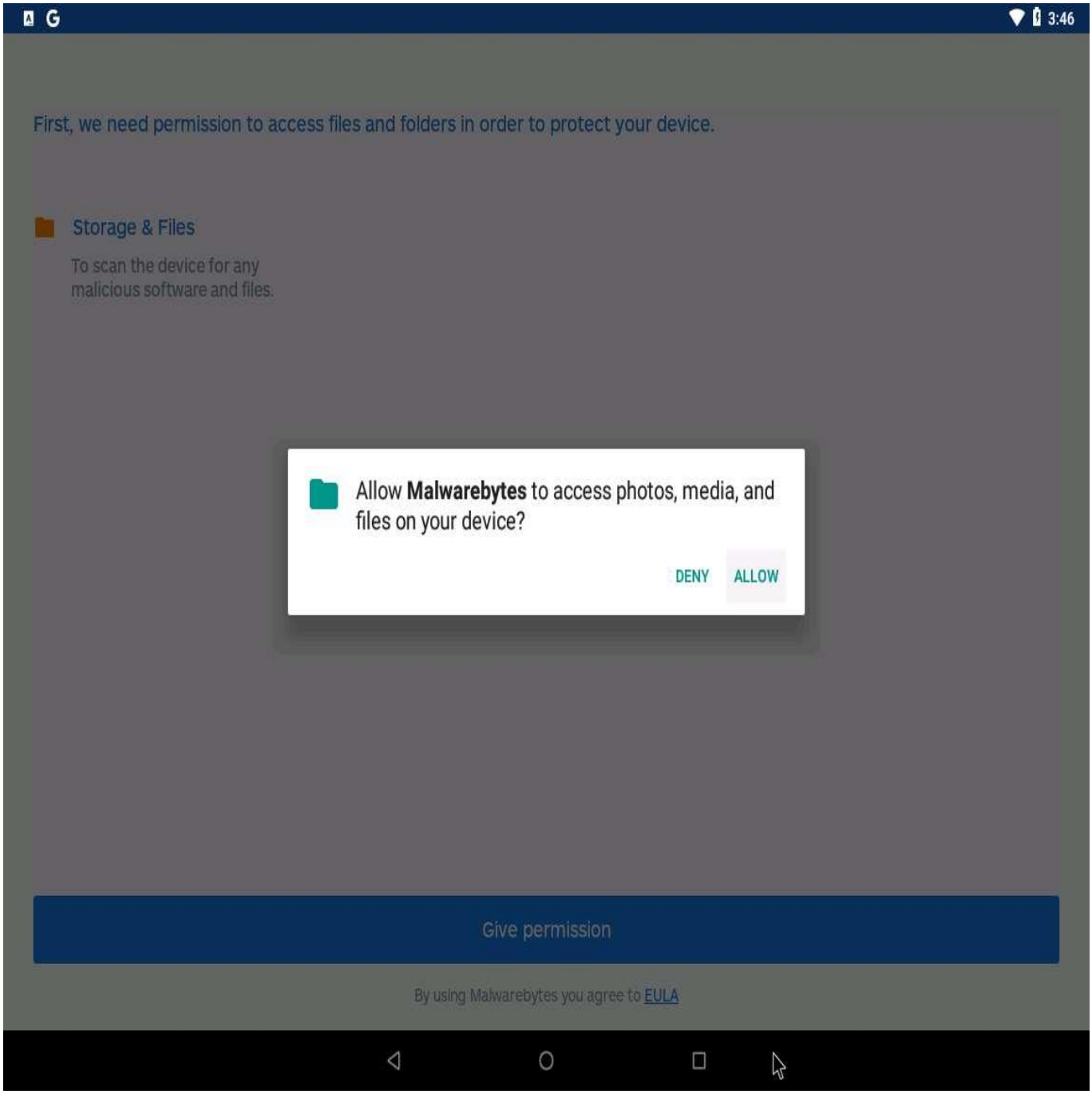
3. ☐ **Malwarebytes Security** initializes. A **Let's get you started** message appears; click the **Get started** button to proceed.



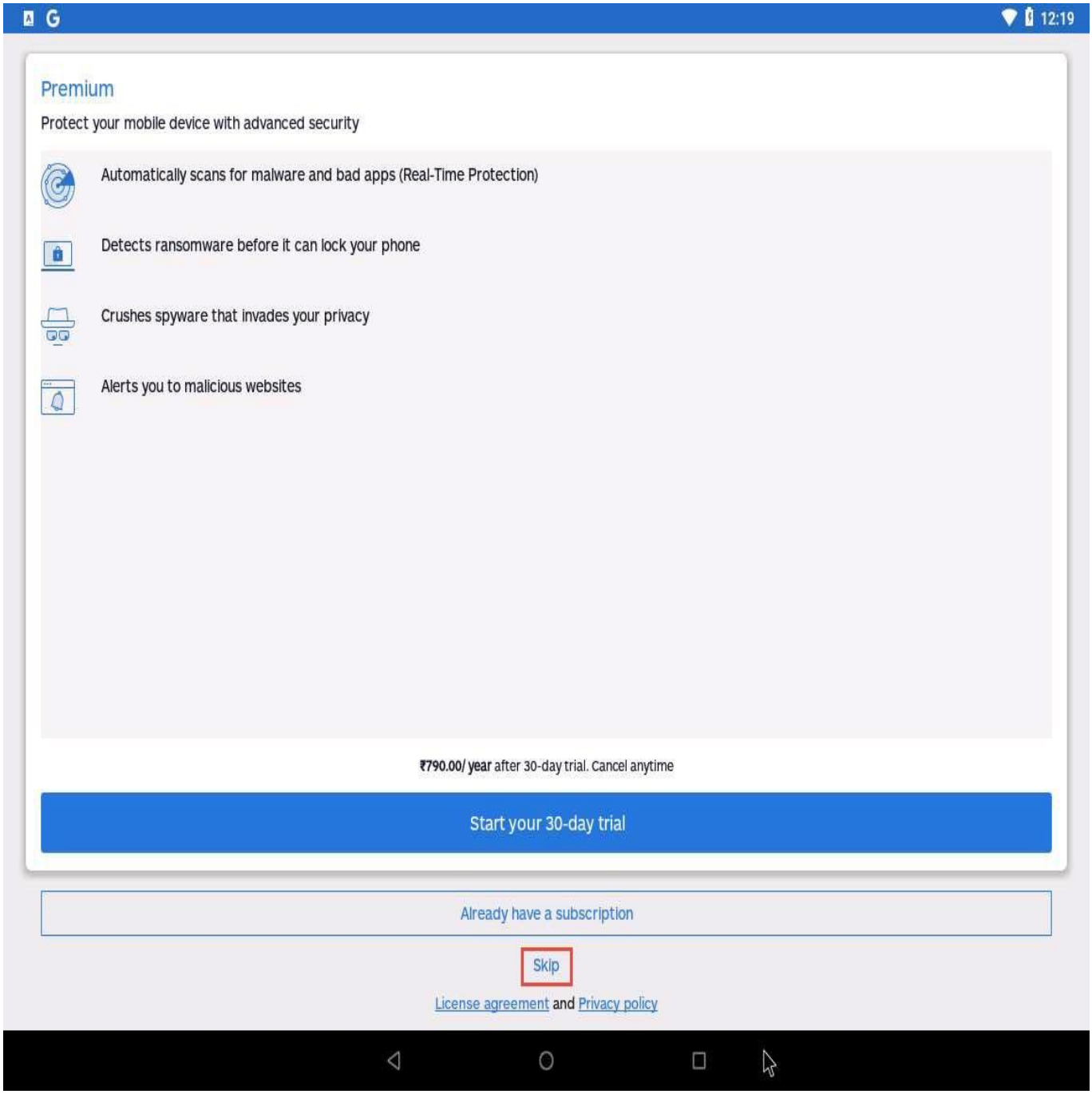
4. ☐ In the permissions window, click **Give permission**.



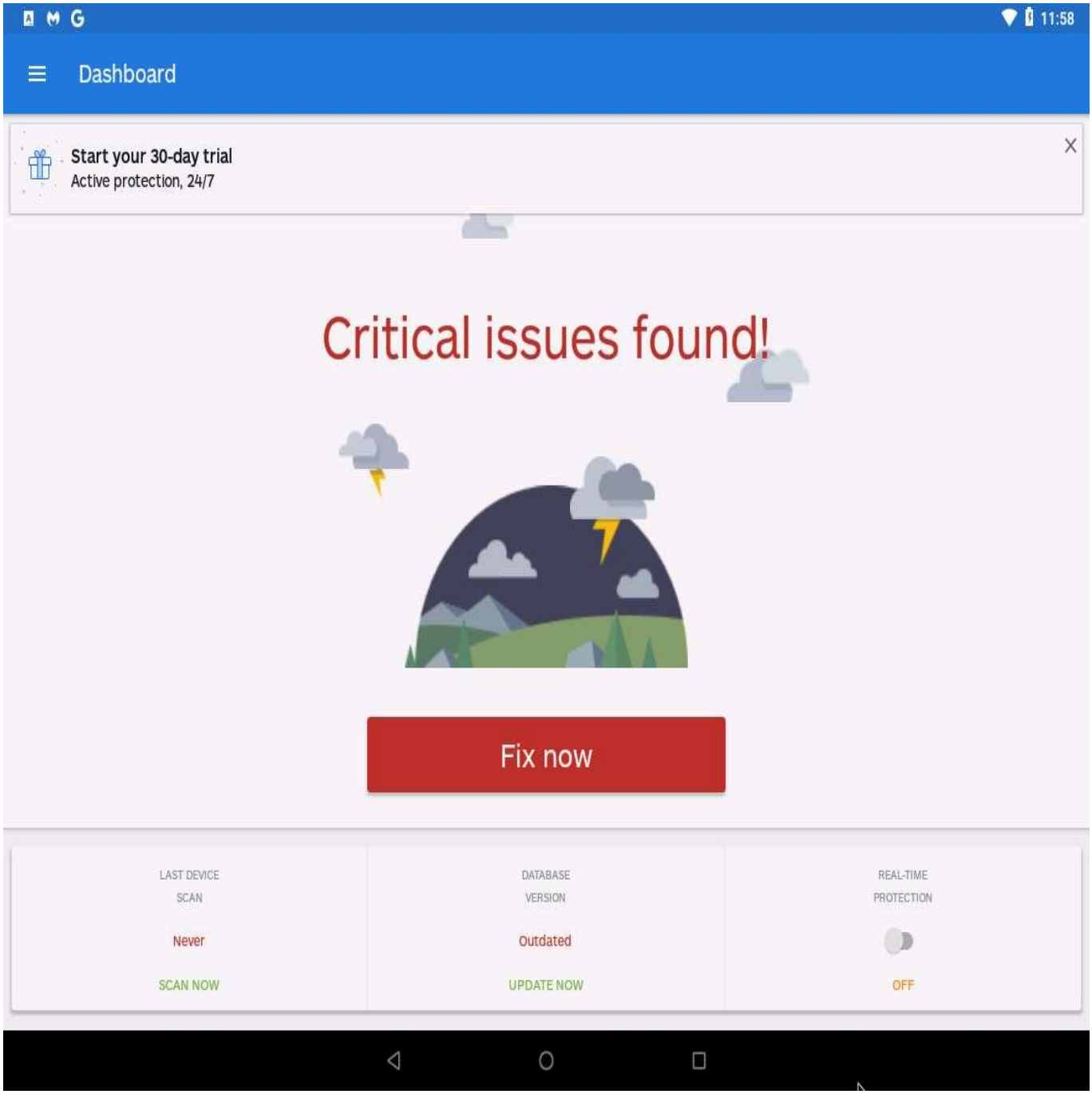
5. ☐ A system pop-up appears, asking for permission; click **ALLOW**.



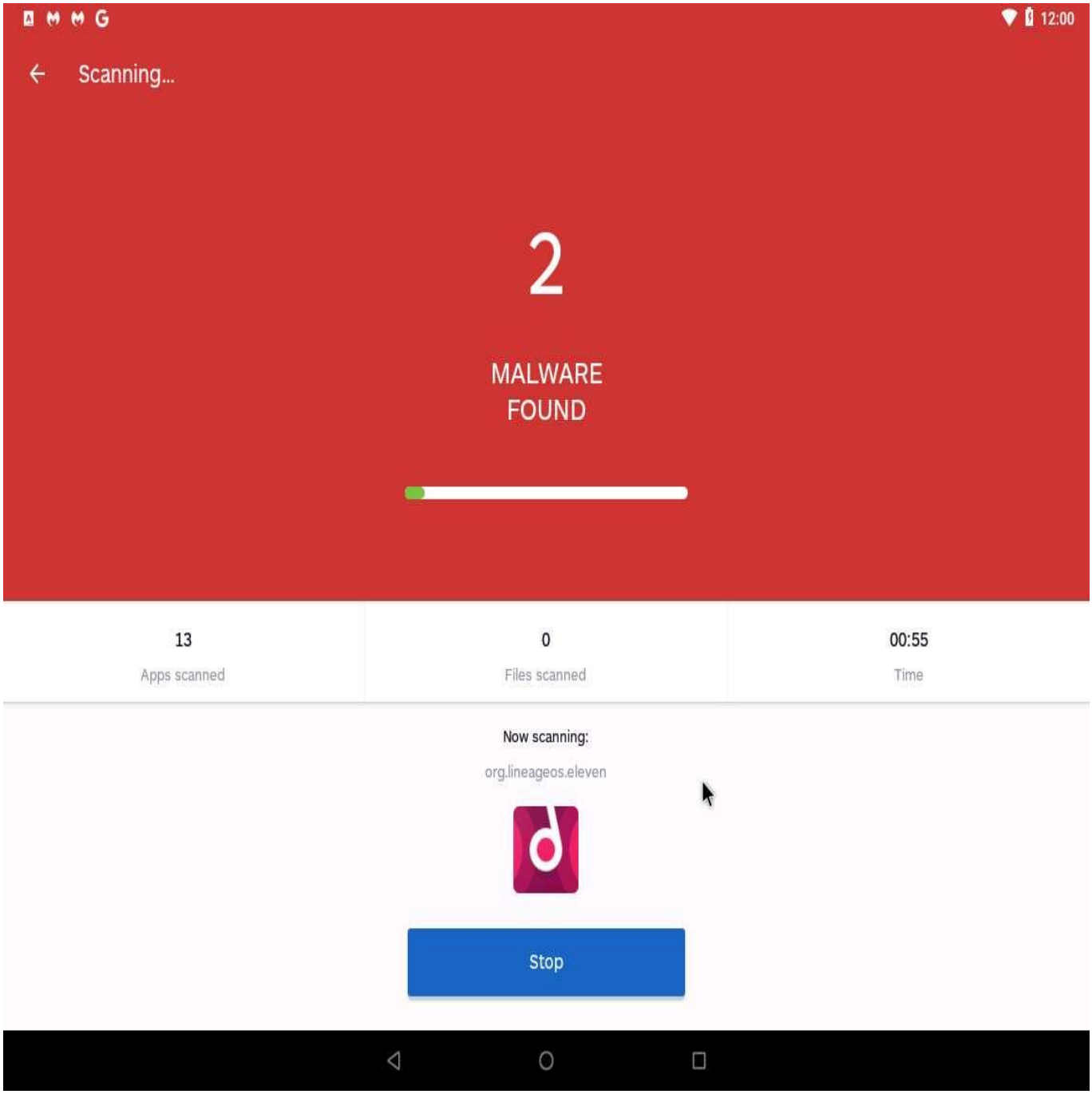
6. Click the **skip** button under **Already have a subscription** as shown in screenshot.



7. ☐ The **Your device has issues!** screen loads; click the **SCAN NOW** button under LAST DEVICE SCAN



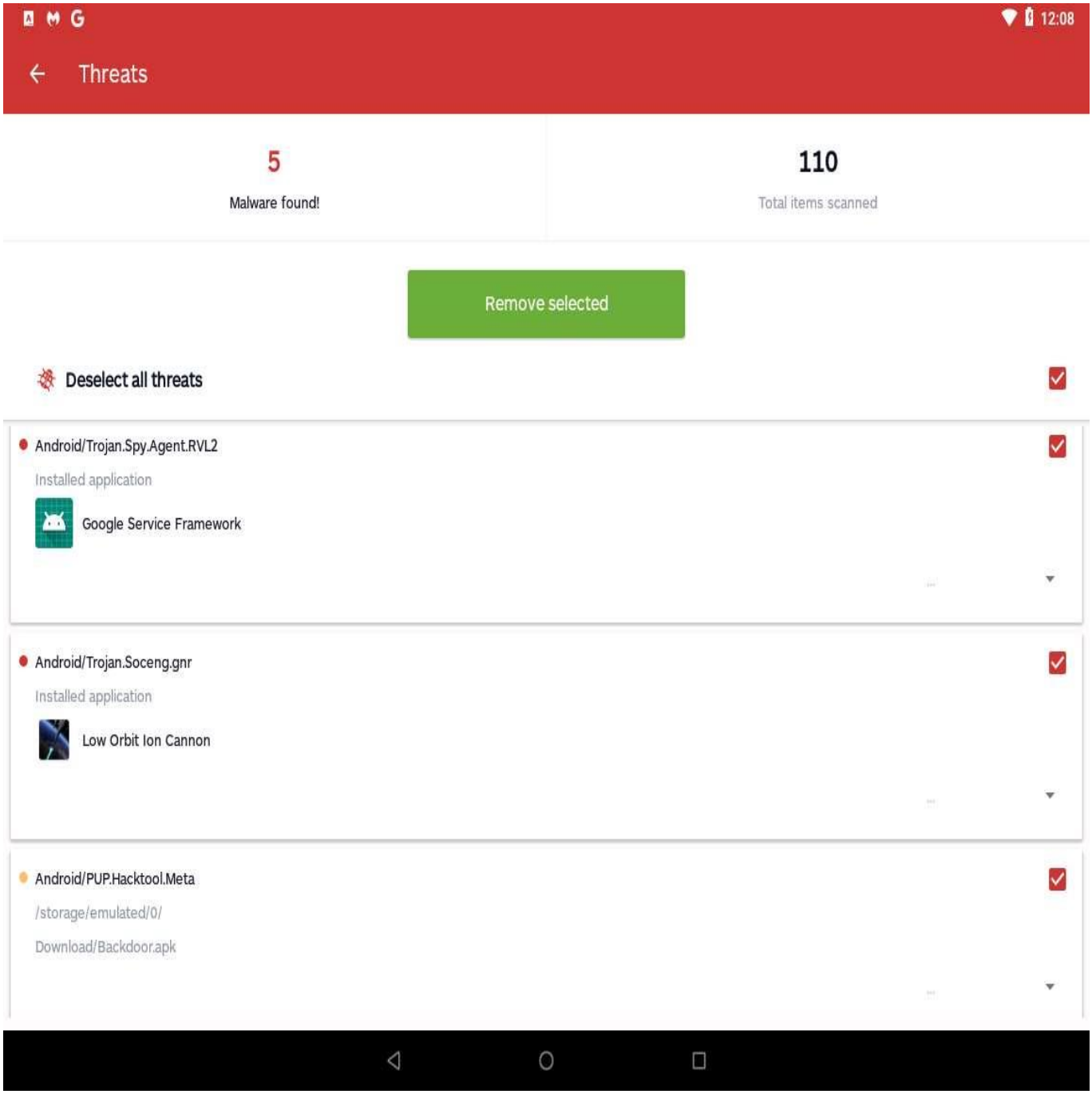
8. **Malwarebytes security** begins a security scan, as shown in screenshot



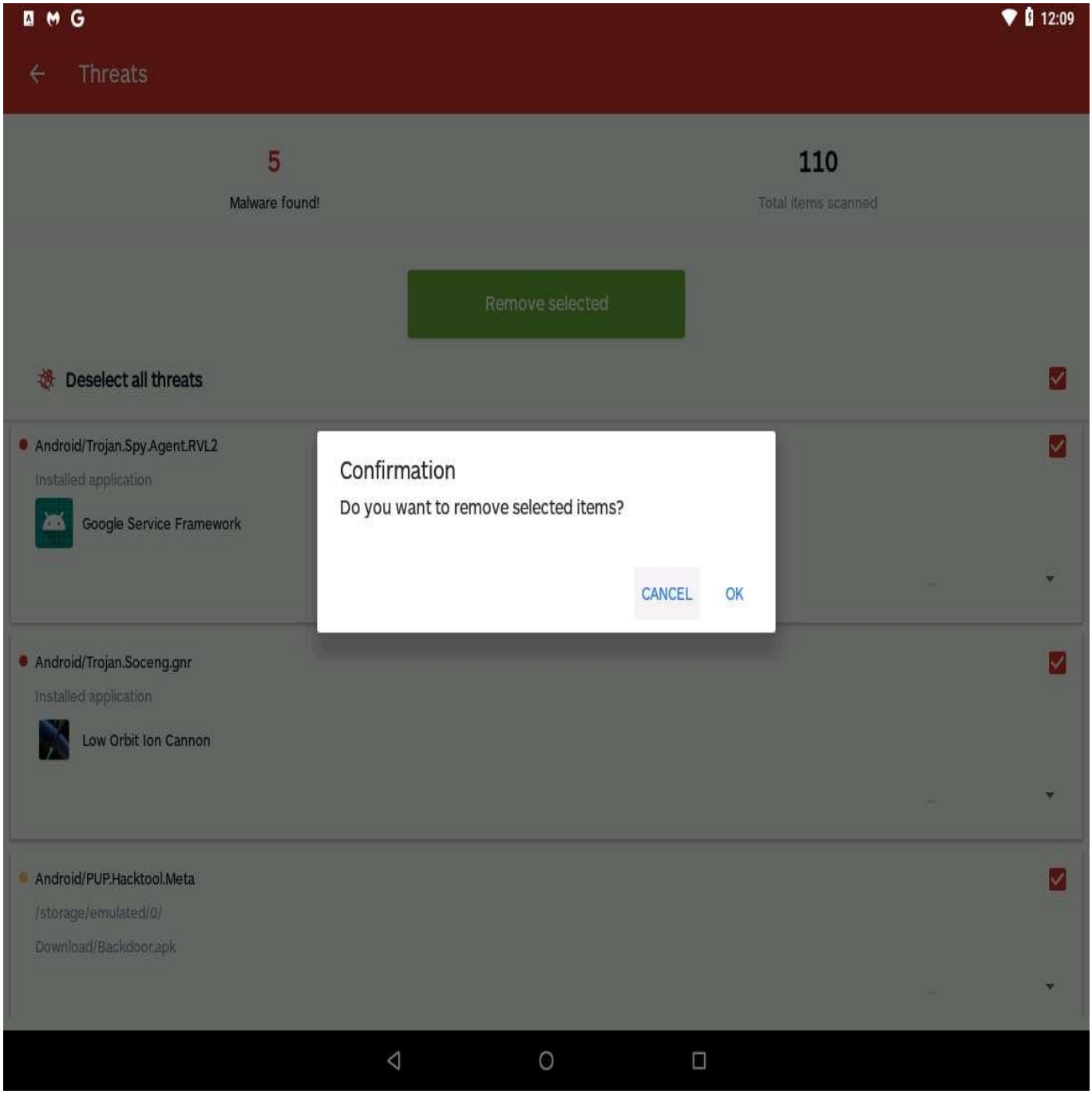
9. A **Threats** screen appears. This will show you all the malware (if any) found on your device.

The number of malware found might differ when you perform the lab.

10. Click the **Remove selected** button to remove the detected malware from your device.

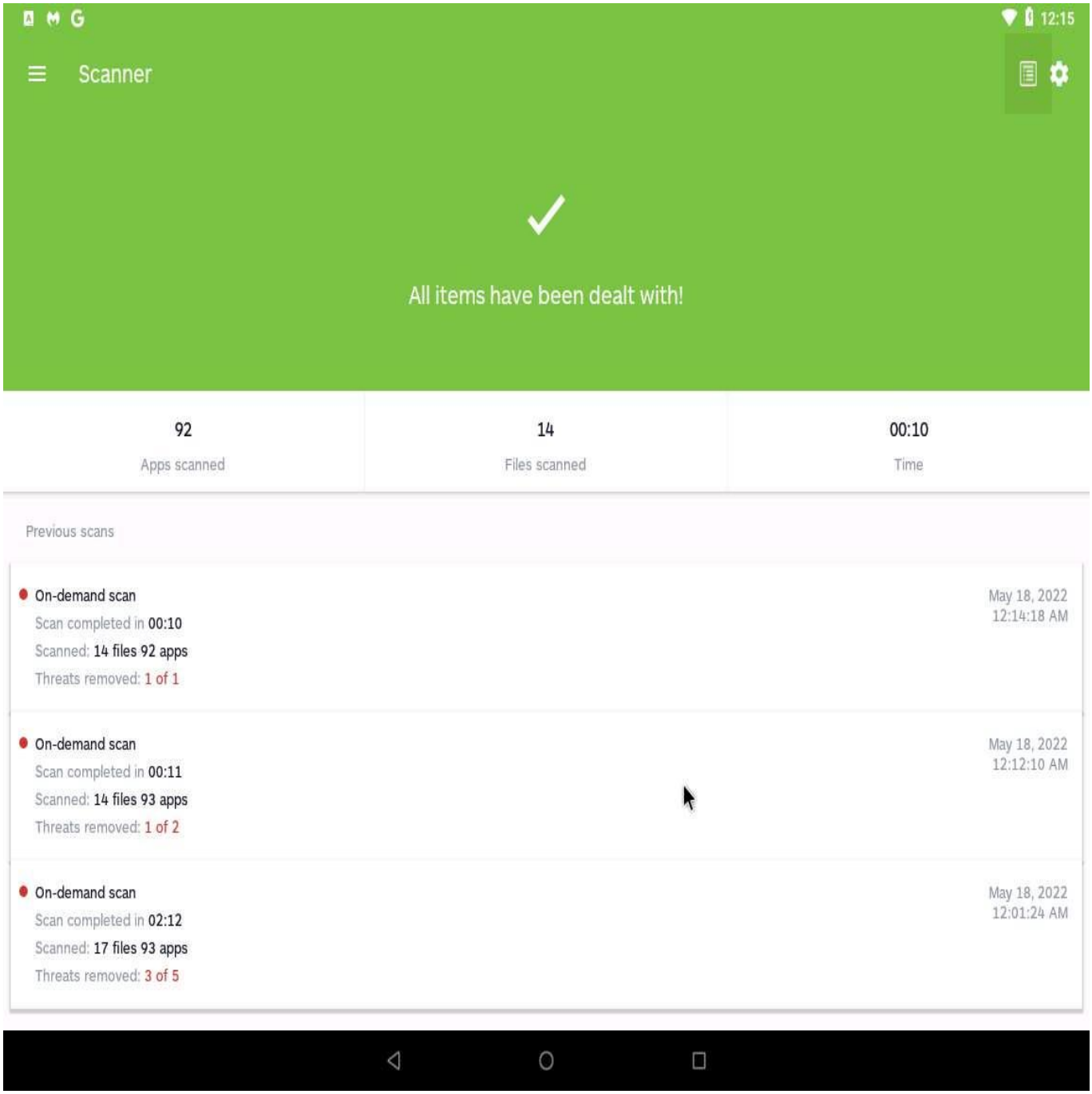


11. A **confirmation** pop-up appears; click **OK** to confirm the removal of the malware.

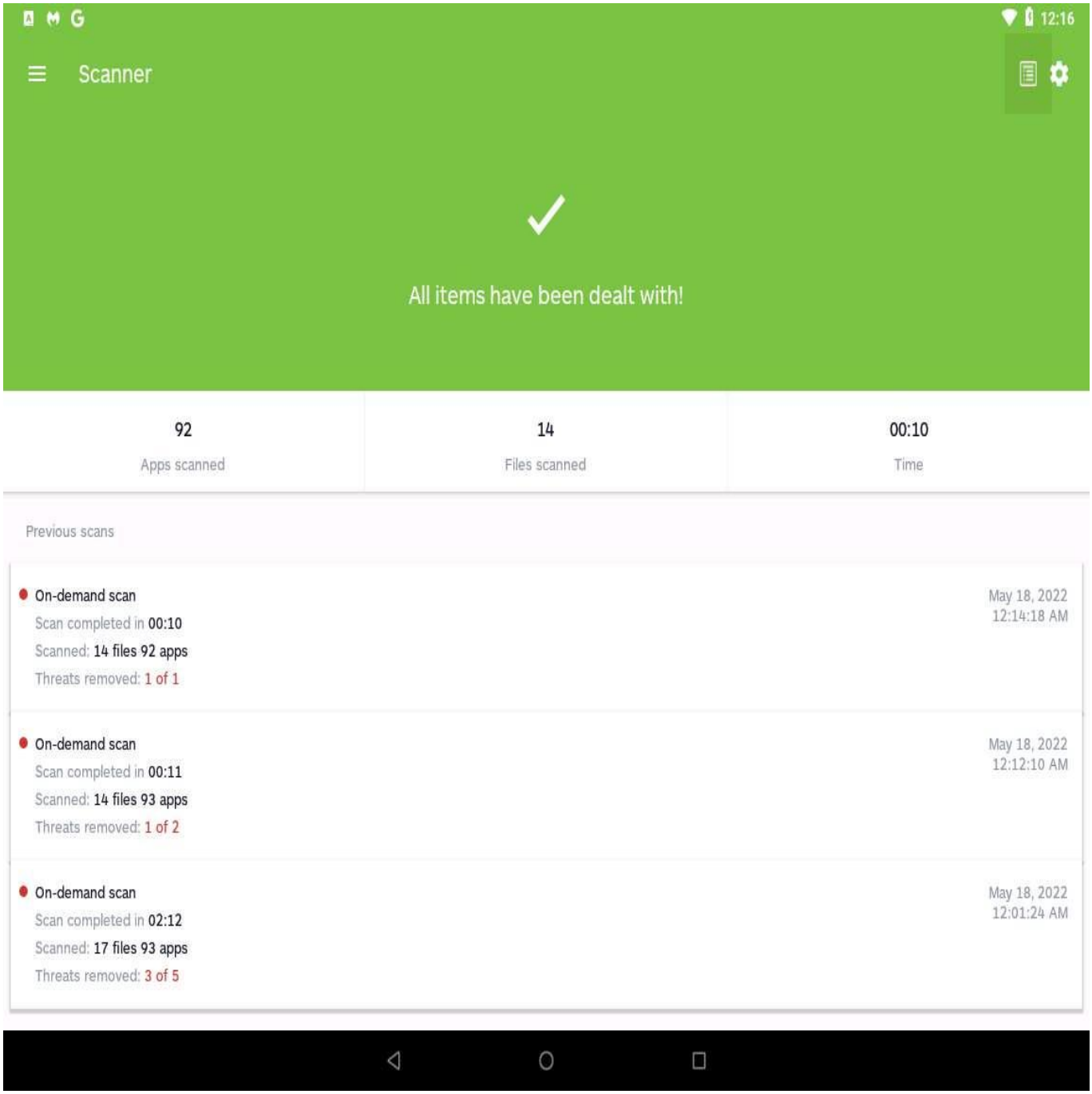


12. ☐ The Malwarebytes **Scanner** screen appears, notifying you that **All items have been dealt with!**.

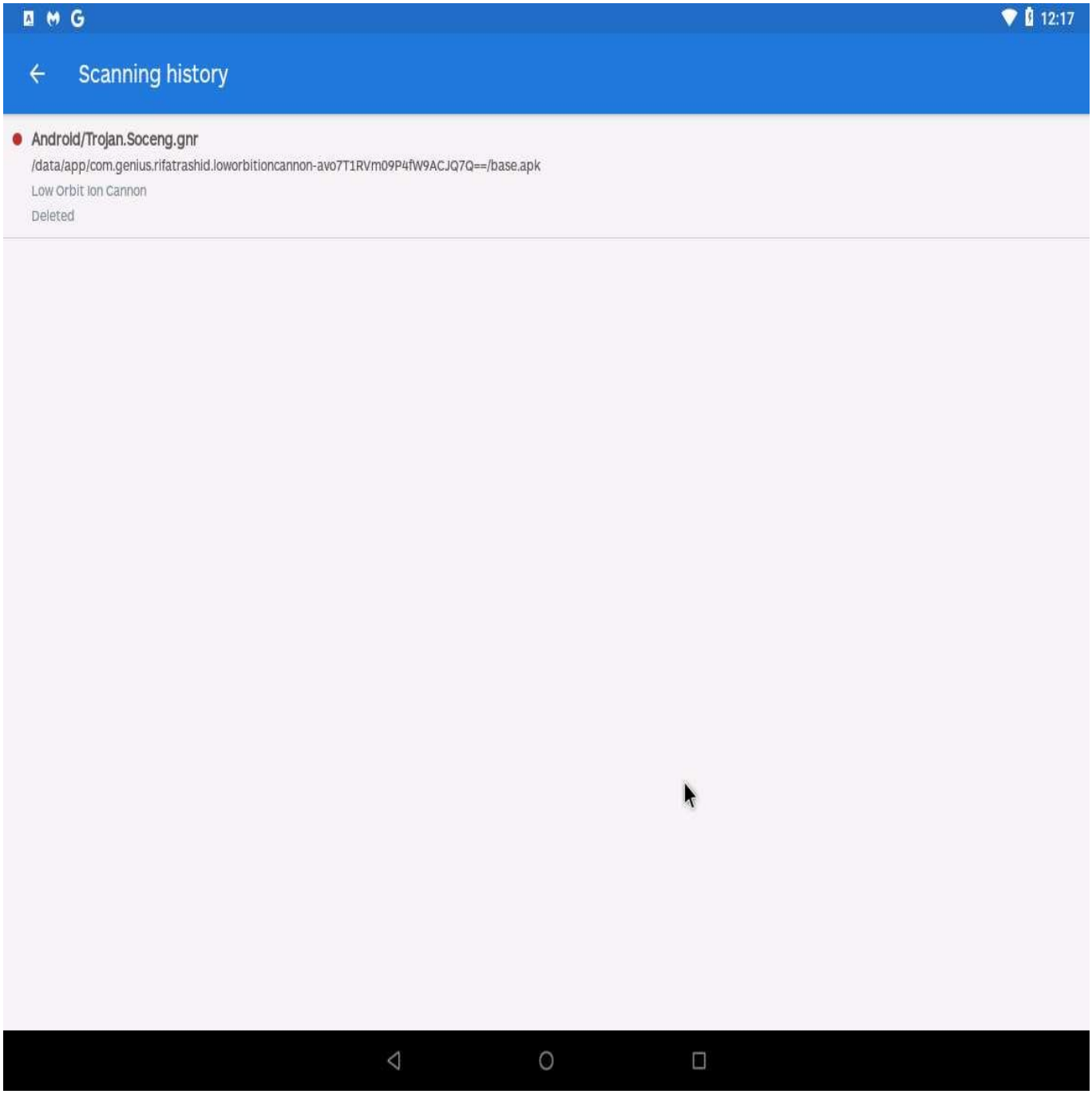
If **Share the love** pop-up appears, click **NOT NOW** to proceed.



13. ☐ Click **On-demand scan** in the lower section of the **Scanner** window under **Previous scans** to view details of the scan.



14. ☐ The **Scanning history** screen appears, displaying the deleted malicious file, as shown in the screenshot.



15. ☐ This concludes the demonstration of how to secure Android devices from malicious apps using Malwarebytes Security.
16. ☐ You can use other mobile antivirus and anti-spyware tools such as **AntiSpy Mobile** (https://antispymobile.com), **Spyware Detector - Spy Scanner** (https://play.google.com), **iAmNotified - Anti Spy System** (https://iamnotified.com), and **Privacy Scanner (AntiSpy) Free** (https://play.google.com) to secure mobile devices from malicious apps.
17. ☐ Close all open windows and document all the acquired information.