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

- Secure Android devices from malicious apps using AVG

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: Secure Android Devices from Malicious Apps using AVG

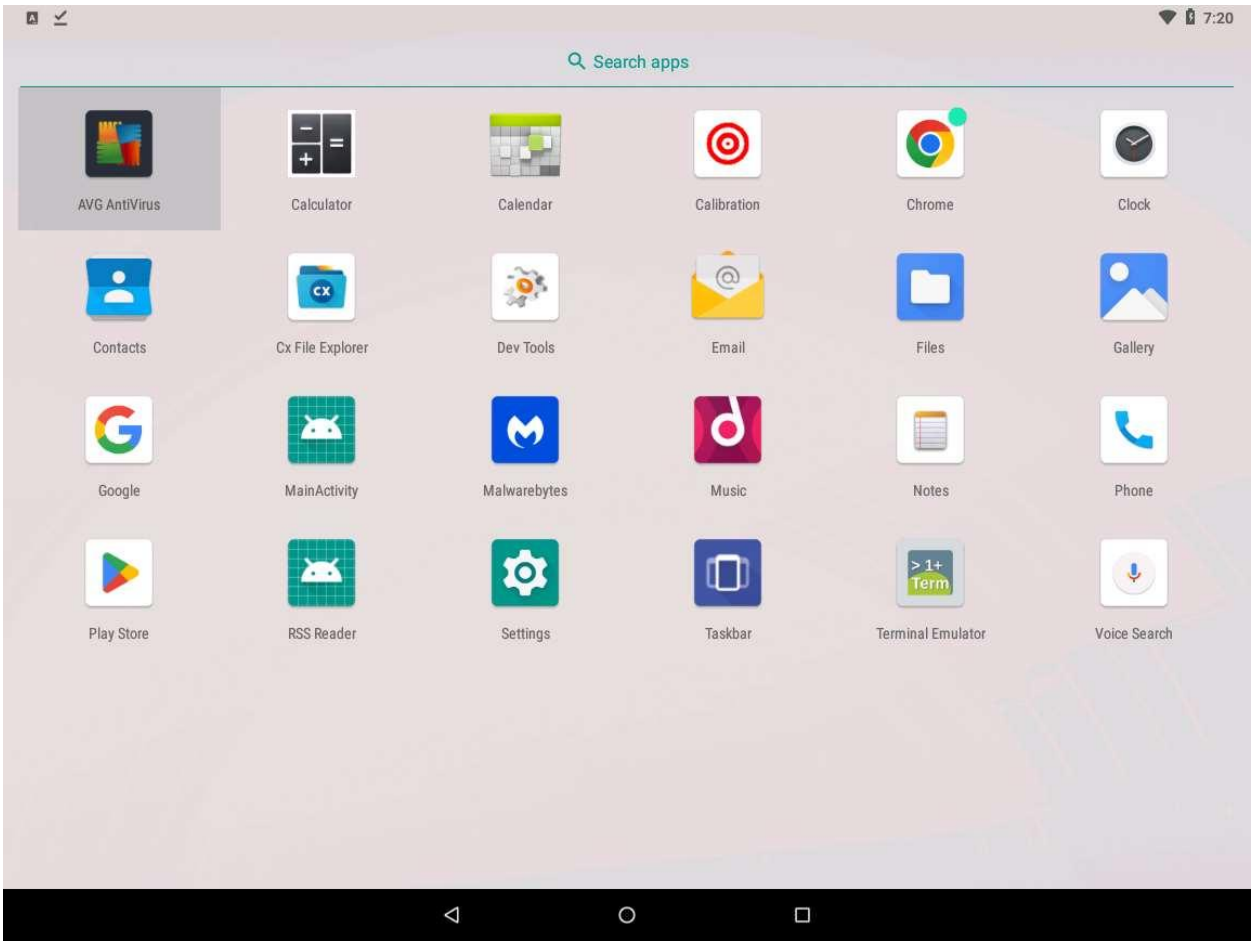
AVG AntiVirus is mobile security tool that provides protection against harmful viruses and malware. It also provides protection to your personal data afe with App Lock, Photo Vault, Wi-Fi Security Scan, Hack Alerts, Malware security, and App Permissions advisor.

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

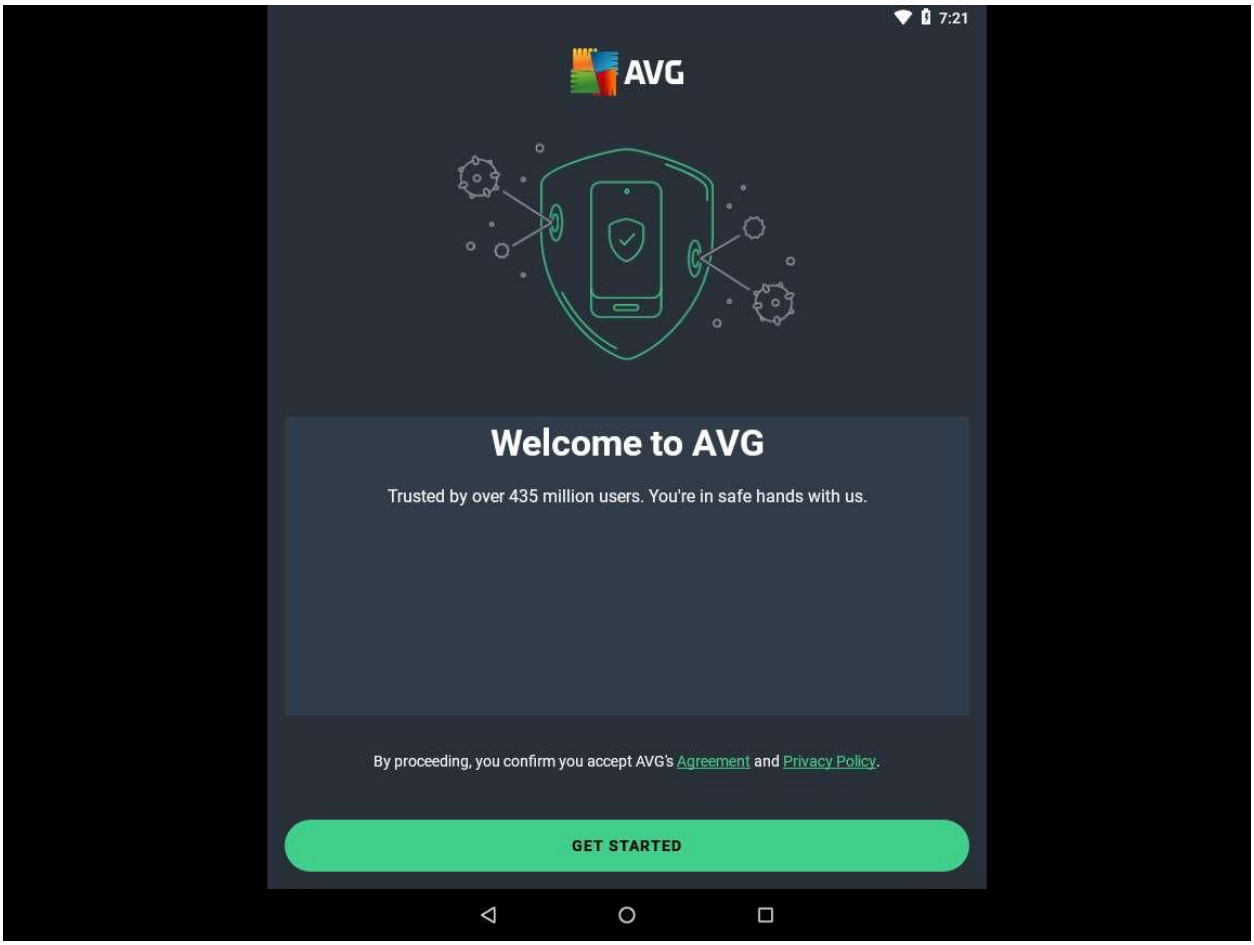
1. Click on Android to switch to **Android** machine, click **Commands** icon from the top section of the screen, click on **Power and Display** button and select **Reset/Reboot machine**.

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

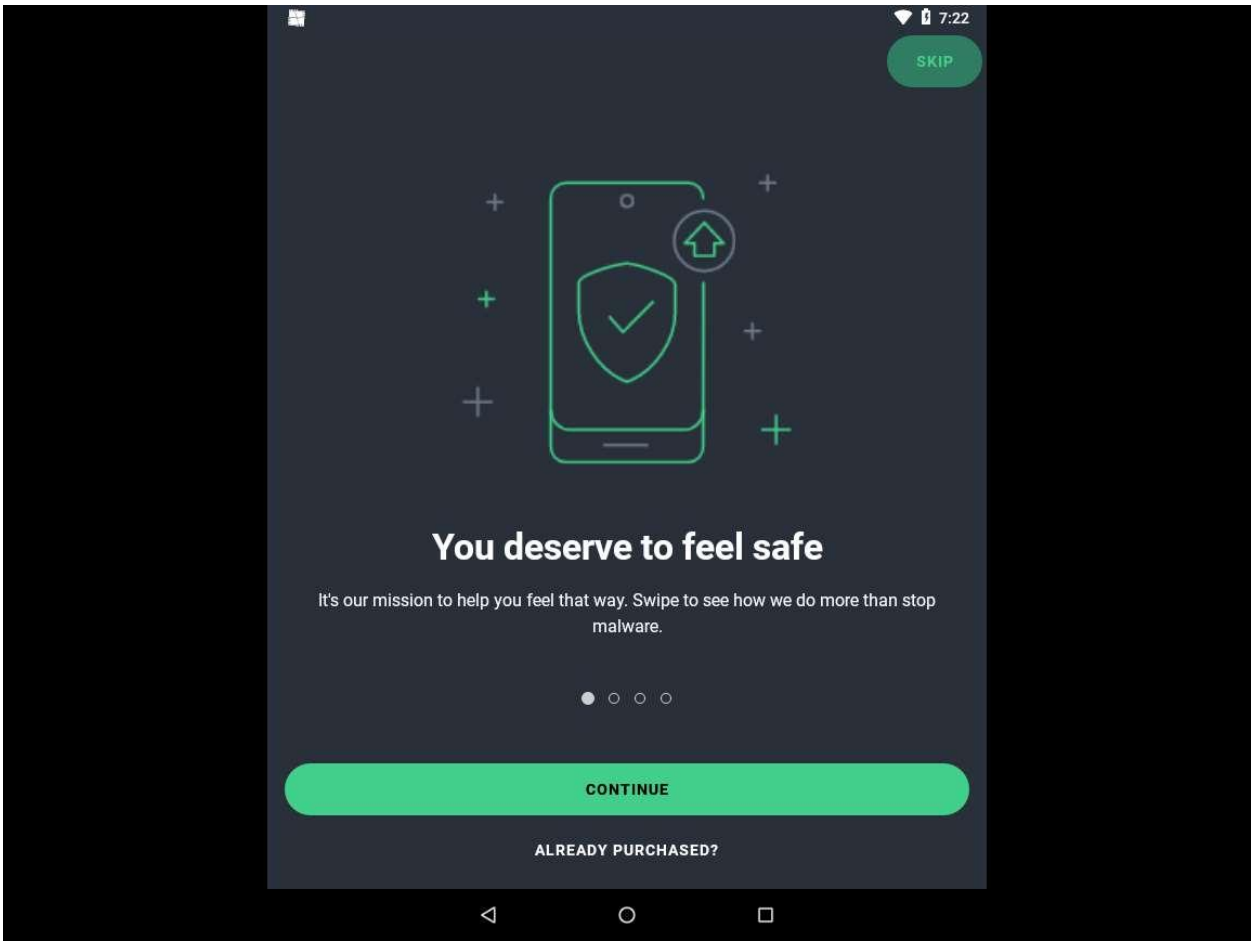
2. After the machine reboots, swipe-up the home screen, which will show all apps. Click on the **AVG AntiVirus** app.



3. **AVG AntiVirus** initializes. A **Welcome to AVG** message appears; click the **GET STARTED** button to proceed.



4. Click **SKIP** present on the top-right corner of the window.

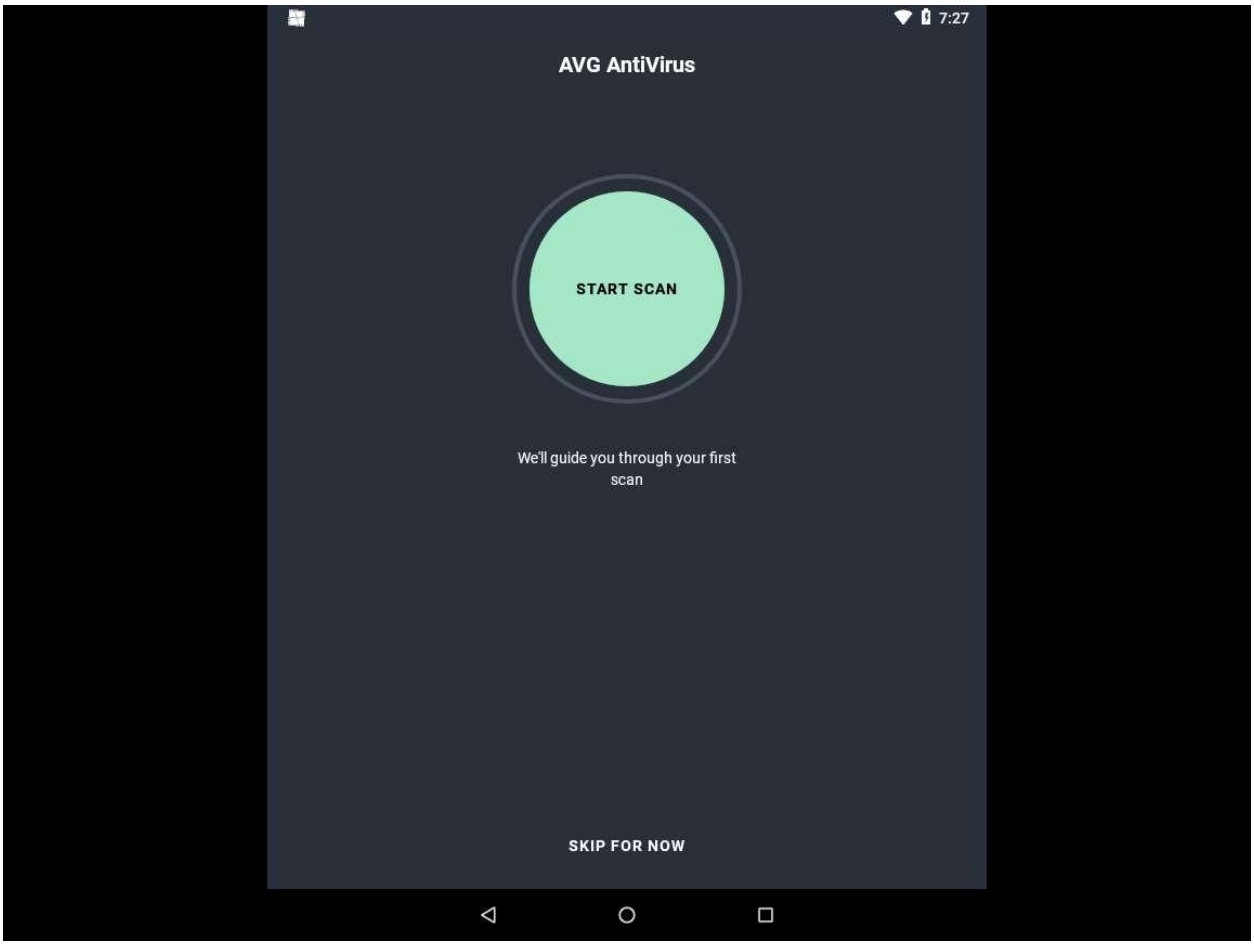


5. A window appears, asking to Upgrade to Ultimate plan; click on the **Click on Continue with Ads | Consent**.
6. The **AVG AntiVirus** screen loads; click the **START SCAN** button.

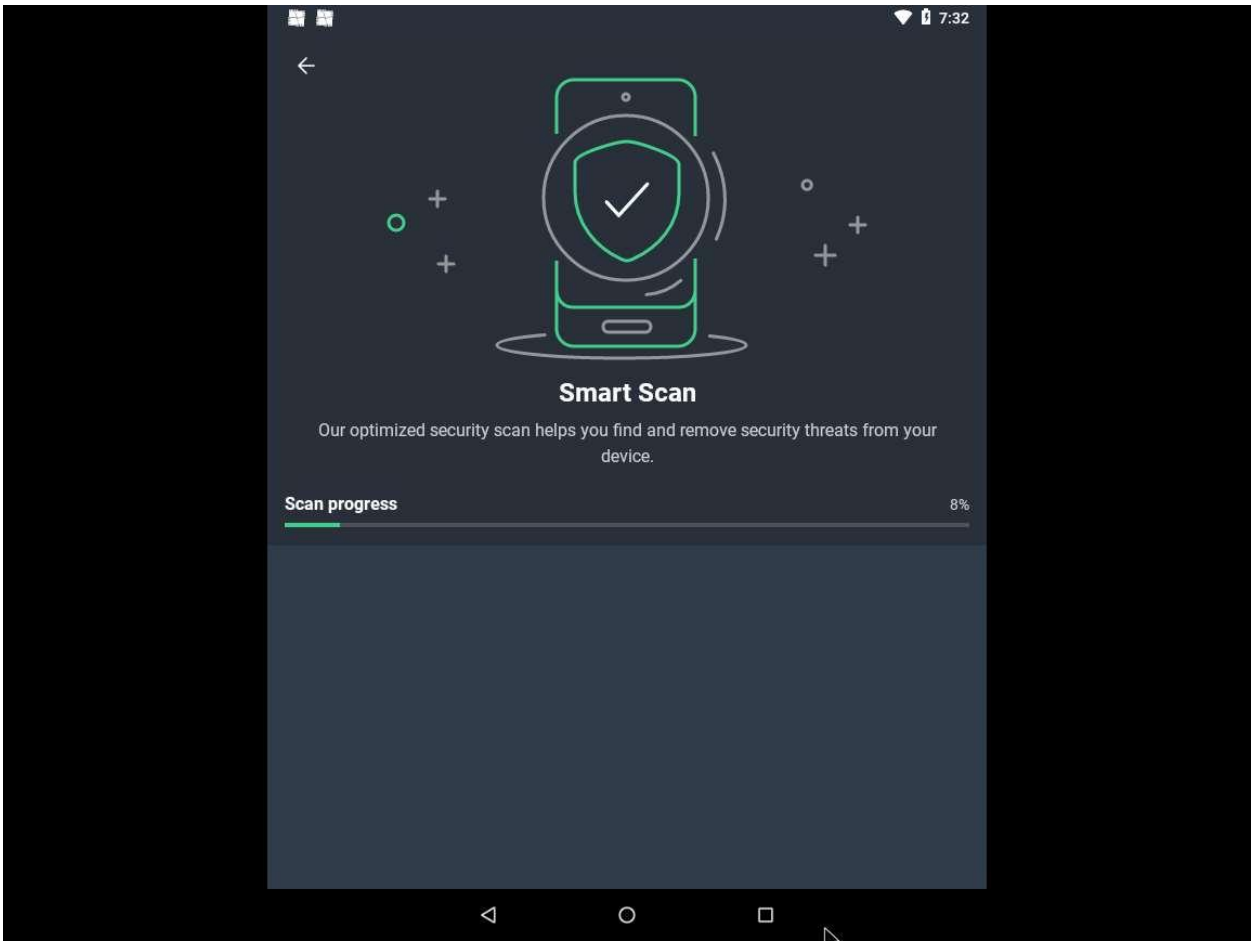
If **You are protected with AVG** pop-up appears, click on **Continue with Ads**.

If **Permission required** pop-up appears, click **OK**.

If system pop-up appears asking for permission to **Allow AVG AntiVirus to access photos, media and files**, click **Allow**.



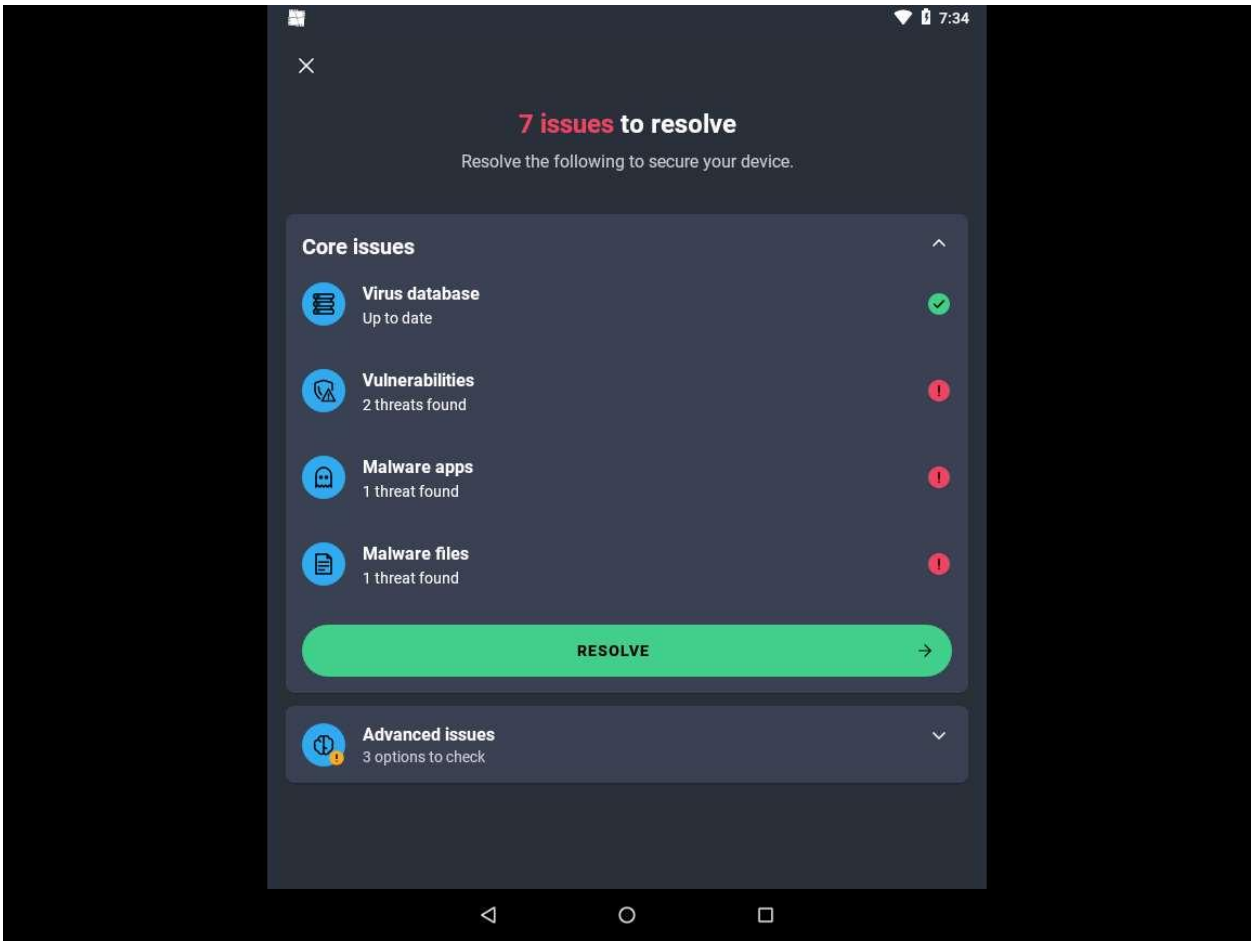
7. **AVG AntiVirus** begins a security scan, as shown in screenshot.



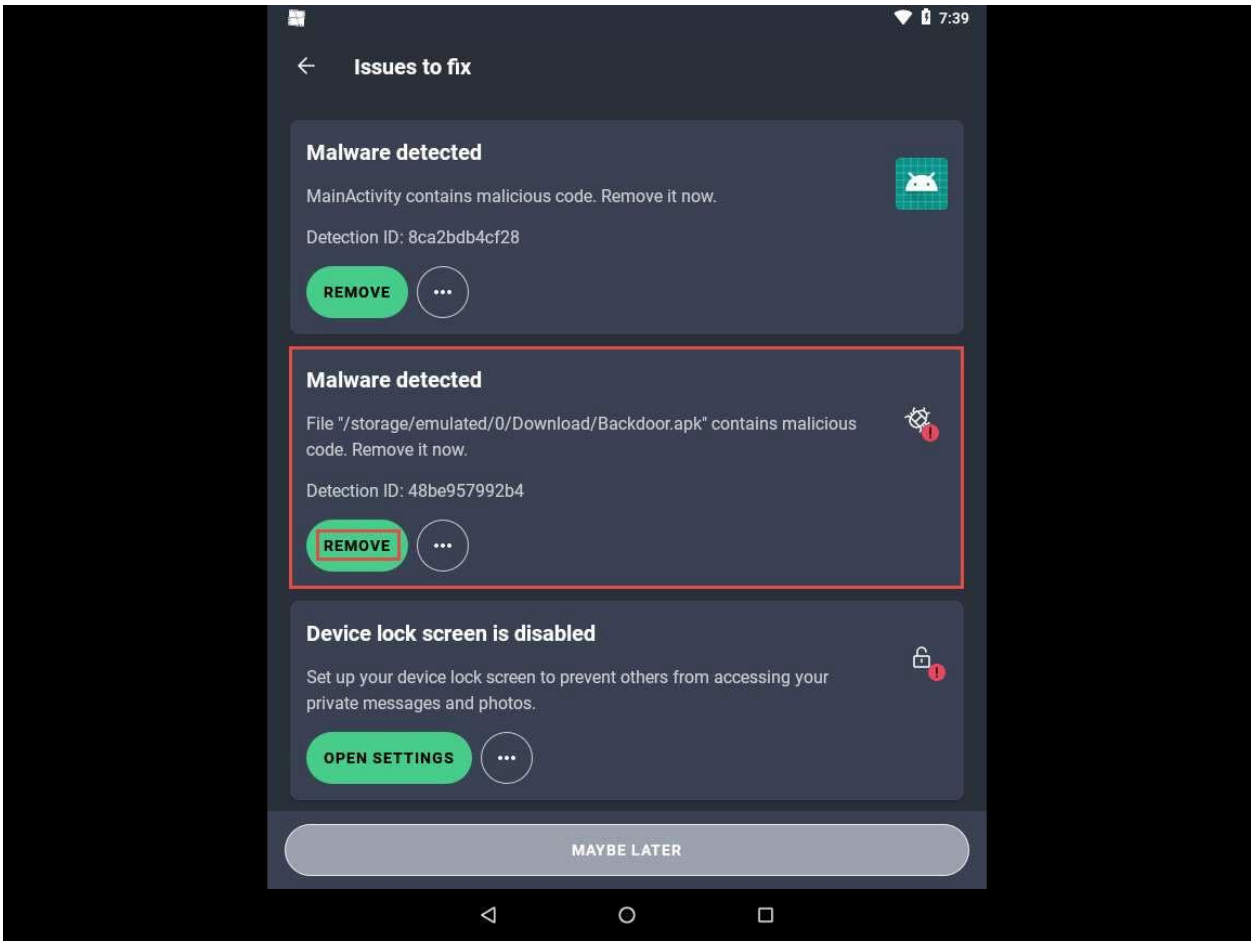
8. A **Threats** screen appears. This will show you all the malware (if any) found on your device.

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

9. Click the **RESOLVE** button to remove the detected malware from your device.

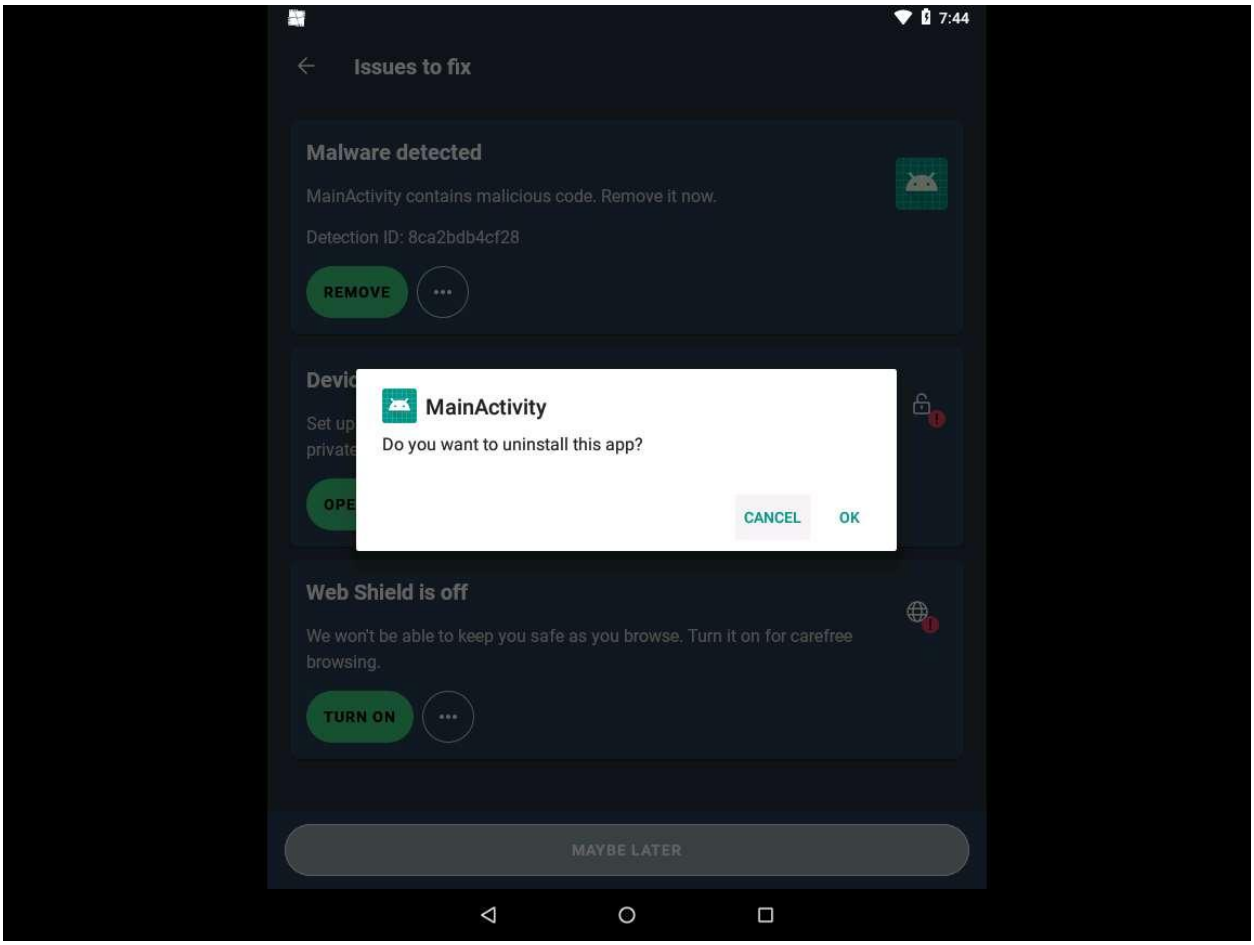


10. The **Issues to fix** window appears showing a list of malwares detected. The scan has detected malware in file **"/storage/emulated/0/Download/Backdoor.apk"**, to resolve this issue click on **REMOVE**.



11. Similarly, click on **REMOVE** under Malware Detected section to remove the respective malware.

If **MainActivity** pop-up appears, click **OK** to uninstall the app.



12. After removing the malware, you may encounter remaining alerts. Simply click on the ellipsis and select **Ignore** to dismiss them.
13. After completing the process, **Scan finished** window appears, click on **"X"** present on top-left corner of the window to close the window.
14. This concludes the demonstration of how to secure Android devices from malicious apps using AVG.
15. You can use other mobile antivirus and anti-spyware tools such as **Certo: Anti Spyware & Security** (https://play.google.com), **Anti Spy Detector - Spyware** (https://play.google.com), **iAmNotified - Anti Spy System** (https://iamnotified.com), **Anti Spy** (https://www.protectstar.com), and **Secury - Anti Spy Security** (https://apps.apple.com) to secure mobile devices from malicious apps.
16. Close all open windows and document all the acquired information.

Question 17.2.1.1

In Android machine, use AVG AntiVirus tool to scan the Android Device for malware and resolve the detected malware files. Which screen in the AVG antivirus tool shows the list of malware and malicious files that are found after the scan?