# SECURITY+ V4 LAB SERIES

# Lab 19: Working with Android

**Document Version: 2023-02-27**

| Material in this Lab Aligns to the Following | |
|---|---|
| CompTIA Security+ (SY0-601)<br>Exam Objectives | 3.5: Given a scenario, implement mobile solutions |
| All-In-One CompTIA Security+ Sixth Edition<br>ISBN-13: 978-1260464009<br>Chapters | 21: Secure Mobile Solutions |

# Contents

## Introduction

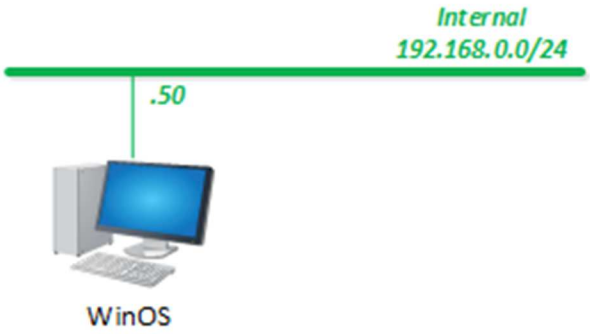
In this lab, you will use Android Studio and Android Virtual Device Manager to operate a virtual Android phone. You will then use command line tools to debug the virtual Android device.

## Objective

In this lab, you will perform the following tasks:

- Learn basic Android device security settings

## Lab Topology



## Lab Settings

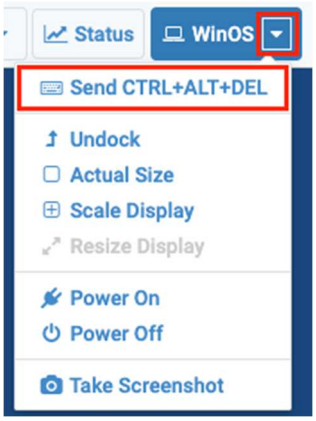
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

| **Virtual Machine** | **IP Address** | **Account** (if needed) | **Password** (if needed) |
|---|---|---|---|
| WinOS | `192.168.0.50` | `Administrator` | `NDGlabpass123!` |

# 1 Android Security

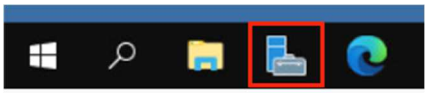
## 1.1 Start the Android Virtual Machine

1. Launch the **WinOS** virtual machine to access the graphical login screen. While on the splash screen, focus on the *NETLAB+* tabs. Click the dropdown menu for the *WinOS* tab and click on **Send CTRL+ALT+DEL**.

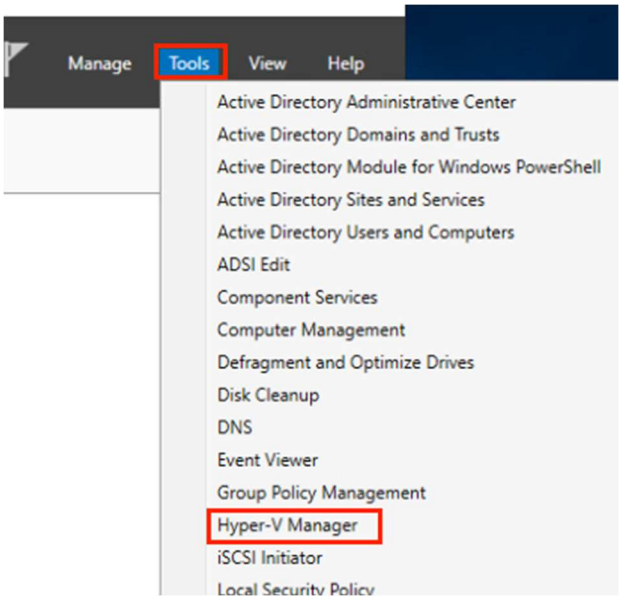



2. Log in as `Administrator` using the password `NDGlabpass123!`.

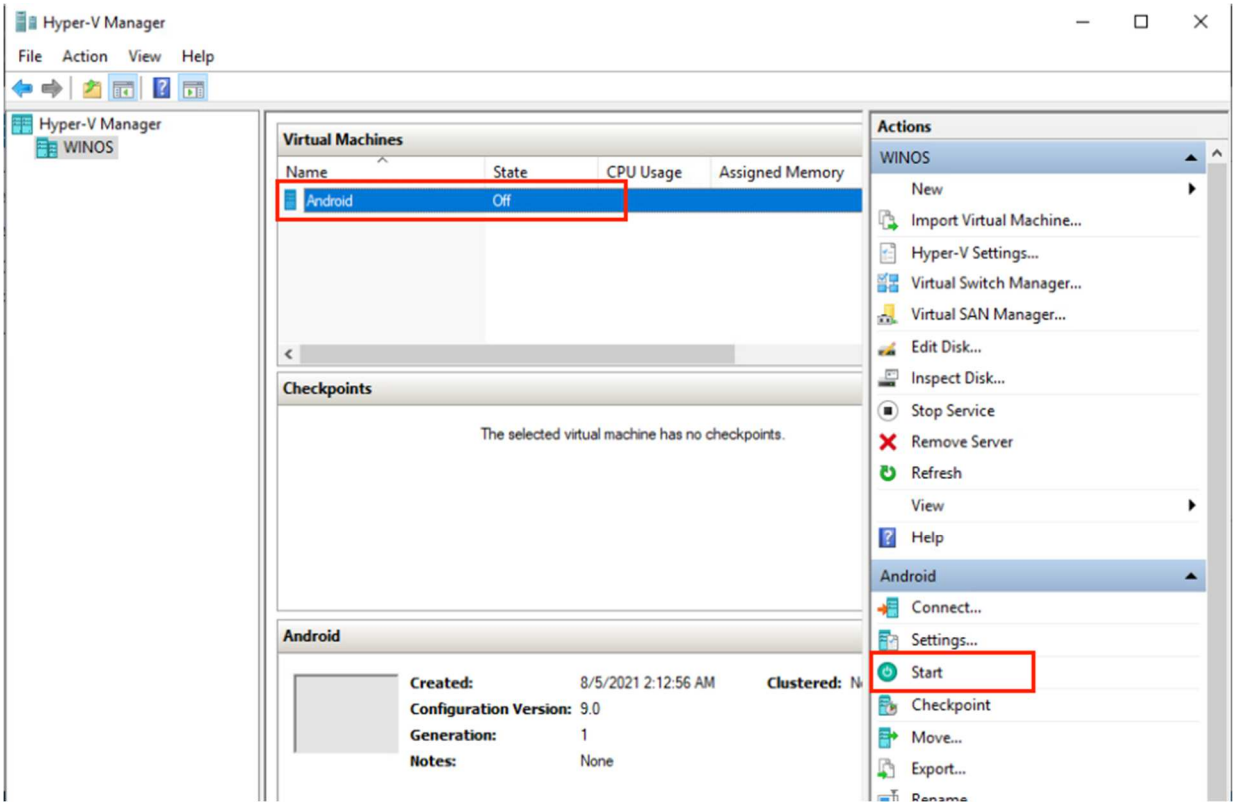
3. Once logged in, click the **Server Manager** icon to launch it.



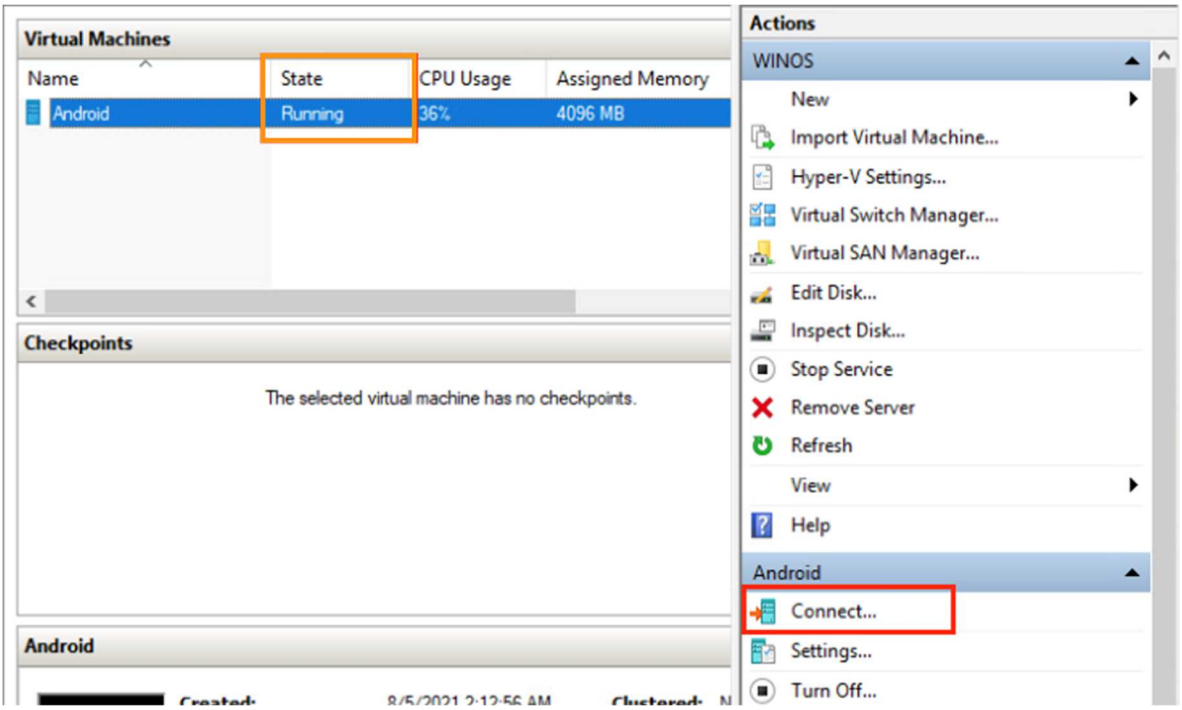
4. In the *Server Manager* window, click **Tools**, then **Hyper-V Manager**.



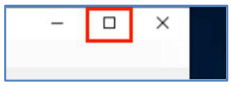

5. The *Hyper-V Manager* window will appear, click on **Android** (notice the *Status* shows as *Off*), then to the right pane, click **Start.**

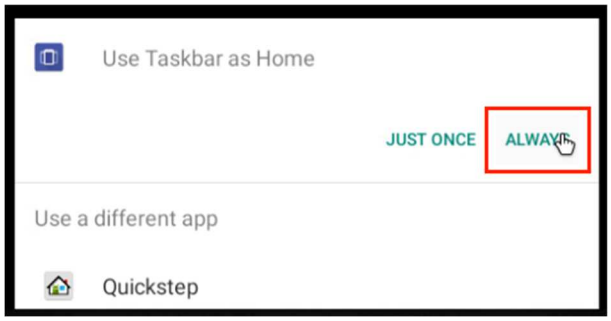


6. After the last step, the Status should change to Running. In the right pane again, click **Connect…** to connect to the Android Virtual Machine's graphic interface.

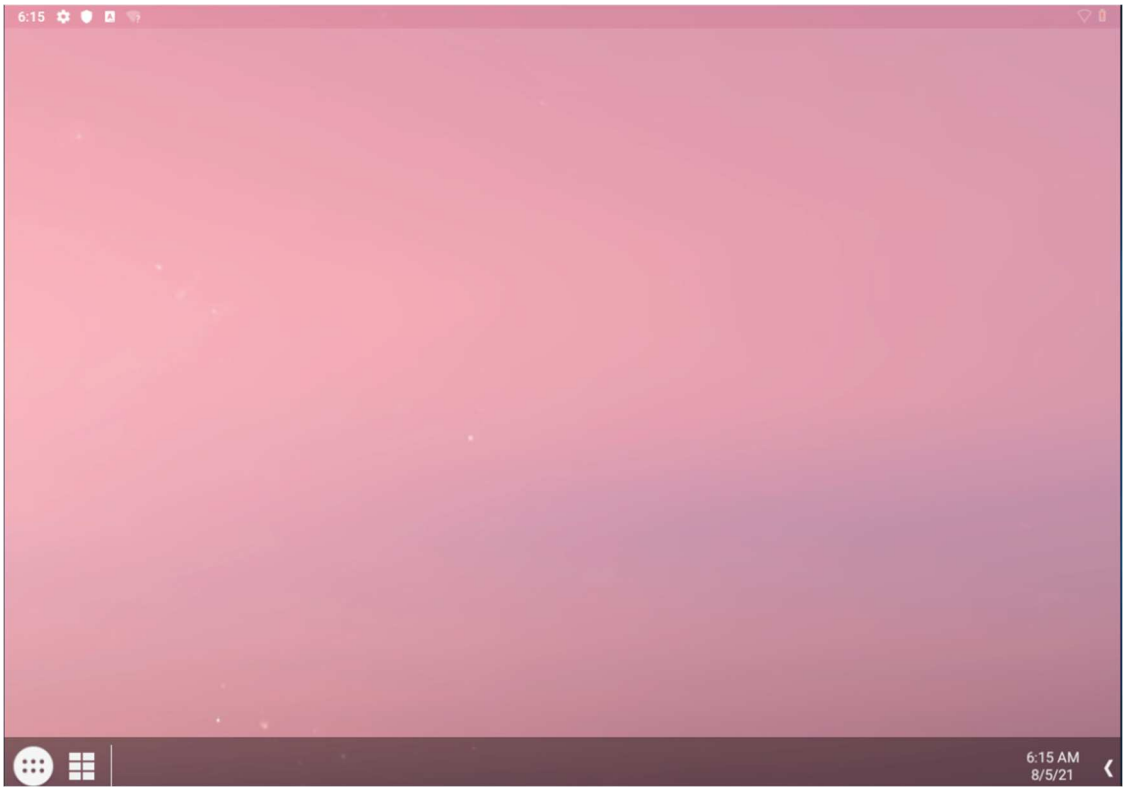



7. A screen with the word *Android* will appear, click on the **maximize** button at the top-right corner of the virtual machine window. Wait until the Android logo disappears and prompts you for options as shown below, click the **ALWAYS.**





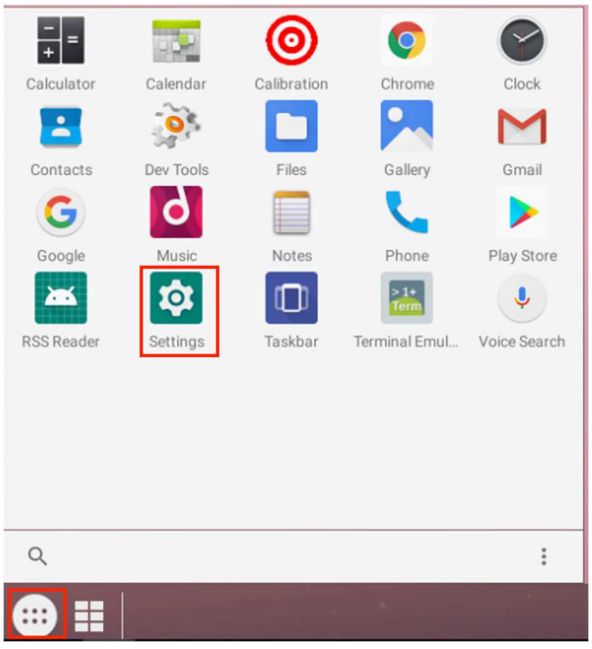
8. The Android desktop with a pink background will be displayed. Leave the window open and continue to the next step.




## 1.2 Security Settings Checkup on Android OS

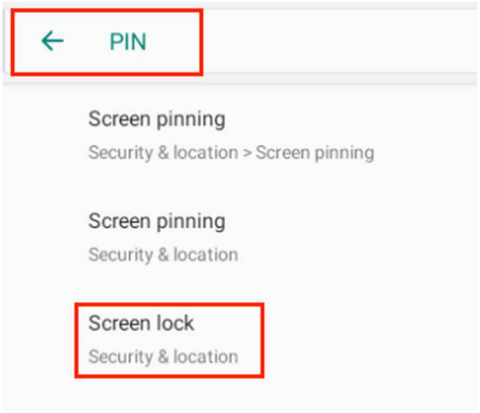
### 1.2.1 Screen Lock

1. Click the lower-left **Applications** button, then click **Settings**.

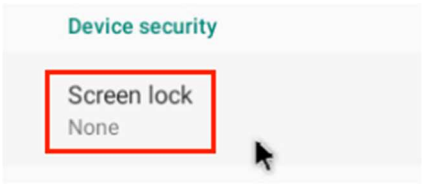


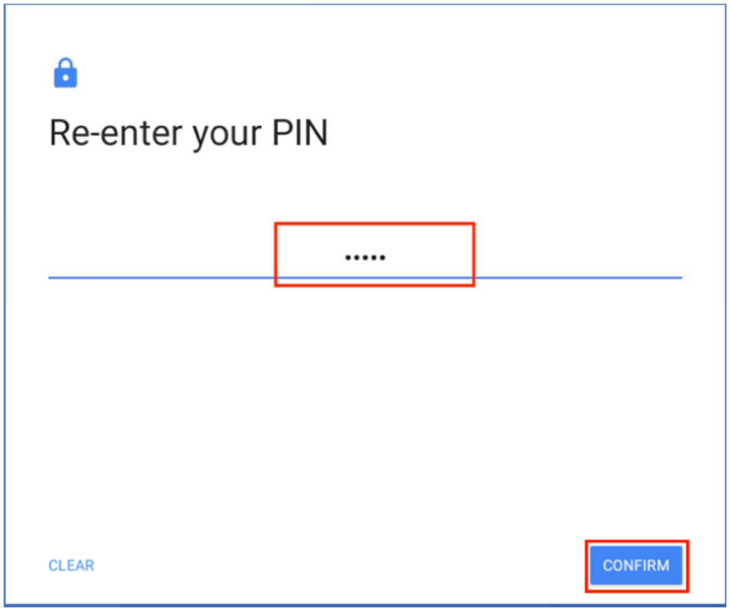
2. Click In the search bar, type `PIN`, then select the **Screen lock.**




3. It will take us to the *Screen lock* configuration location; notice it says *None* now. Click on the **Screen lock**.



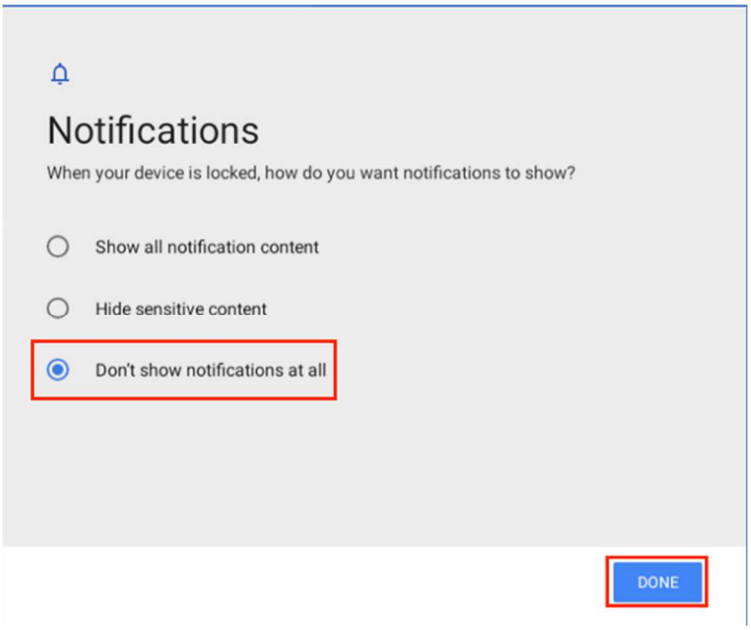

4. Click to choose the **PIN** option; we will set a 5-digit PIN. Type **89757,** click **NEXT**, type **89757** again, then click the **CONFIRM.**



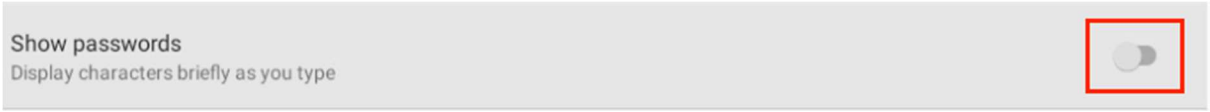

Please Note

On your device, you will want to set a PIN at least of 8 digits in length. For the demonstration purpose, we are using a 5-digit PIN instead.

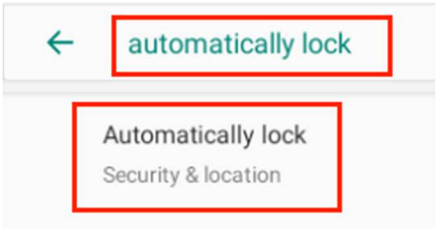
5. At the next screen, when asked whether we want to show notification while the screen is locked, we will choose **Don't show notification at all** and click **DONE**.



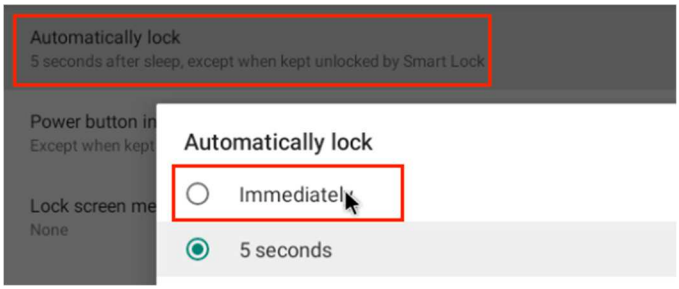

6. Now the *Screen lock* should show as *PIN protected*. Scroll down a little bit and click to **turn off** the *Show passwords* option.




7. Click the magnifying glass at the top-right corner, and type `automatically lock`.

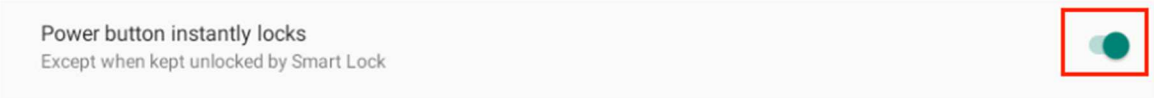



8. Click on the search result *Automatically lock***.** On the new screen, click on the **Automatically lock**, and select **Immediately.**

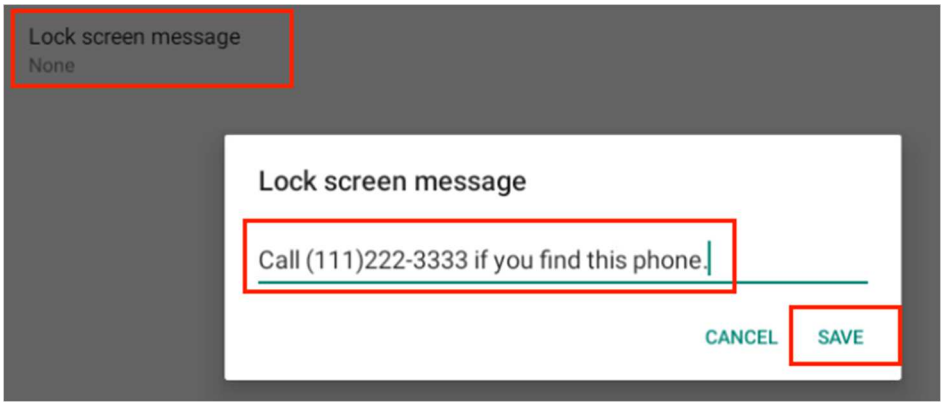


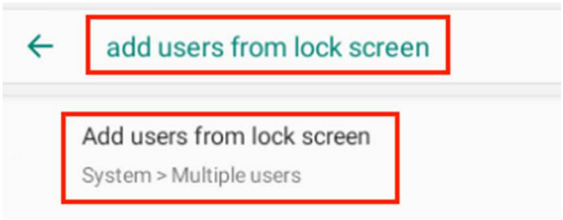
9. Then, make sure the *Power button instantly locks* switch is set to **ON** (Flipped to the right side)




10. Click the **Lock screen message**. Add a message to help find your phone when it is lost. Click **SAVE**.



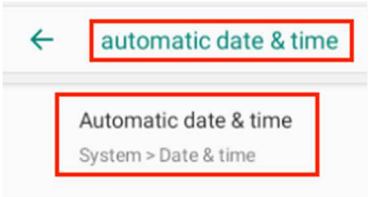

11. Click the magnifying glass, type `add users from lock screen` and click on the search result.



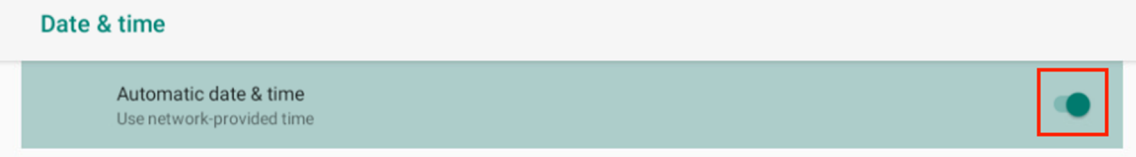

12. On the new screen, make sure the option switch is **turned off** (flipped to the left side)


### 1.2.2 Network Settings

1. Click the magnifying glass, type `automatic date & time`, click the search result.

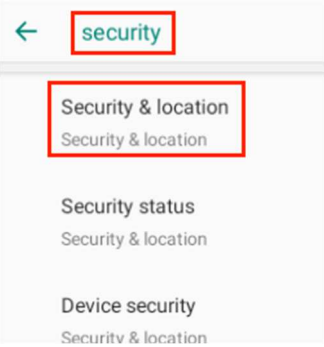


2. On the new screen, make sure the *Automatic date & time* switch is **turned on** (flipped to the right side)

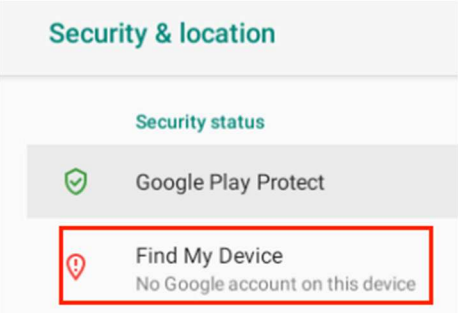



Maintaining the correct on your device will help the Forensics people record the events accurately.

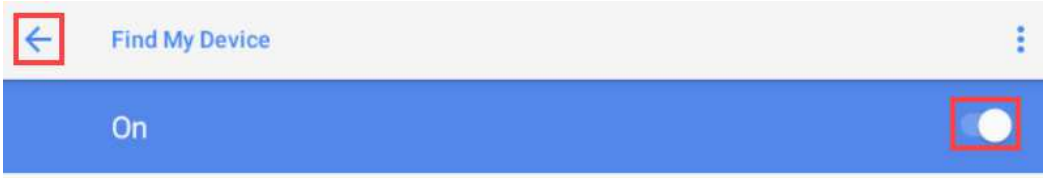
3. Click the magnifying glass, type `security`, then click **Security & location** from the search results.



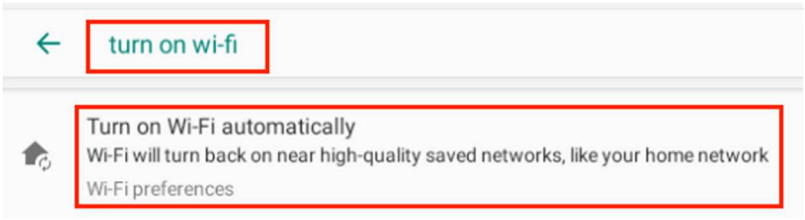

4. On the new screen, click **Find My Device** when the Google account is logged in.



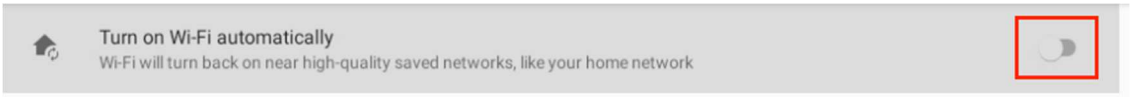

5. Ensure that the *Find My Device* feature is turned **On**. Then, click the **back** button.



6. Click the magnifying glass, type `turn on wi-fi automatically` and click the search result.



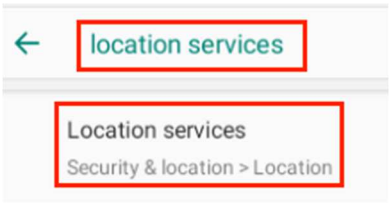

7. On the new screen, turn off the **Turn on Wi-Fi automatically** switch.



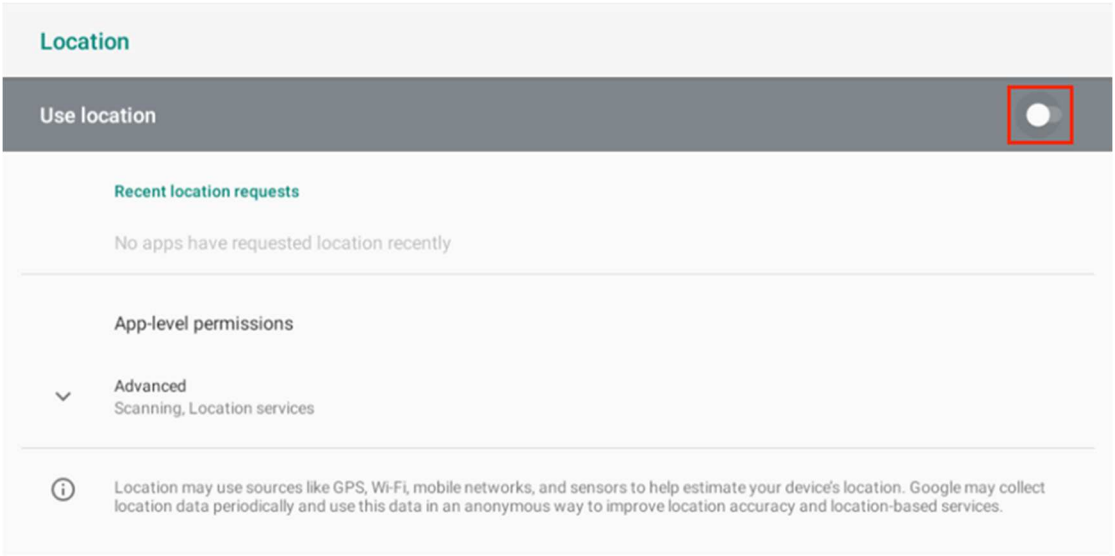

This could be a dilemma between convenience and security. The phone will automatically connect to known networks, if attacker spoofed a known network, the phone would connect to it. For security purposes, it is better to always turn off the Wi-Fi network when not near a trusted Wi-Fi network.

### 1.2.3 Privacy Settings

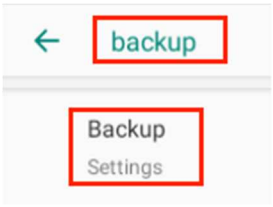
1. Click the magnifying glass, type `location services`, click the search result.



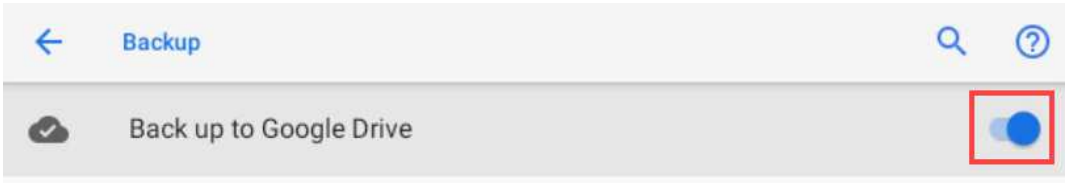
2. On the new screen, turn off the **Use location** switch.



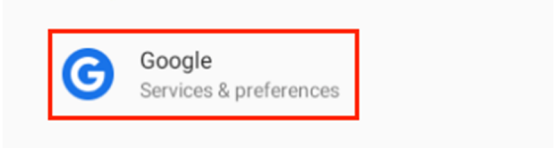

3. Click the magnifying glass, type **backup** and click the search result.



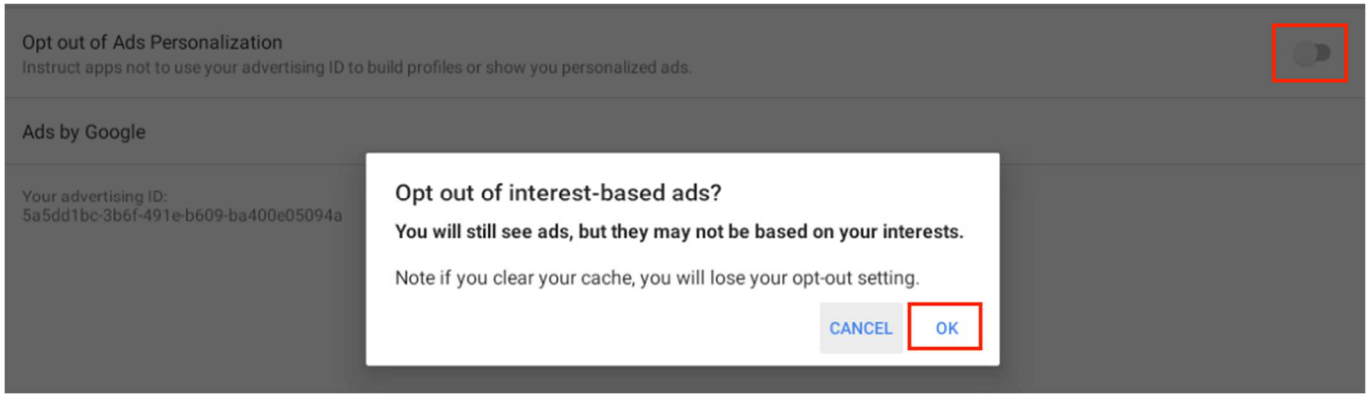

4. On the new screen, turn on the **Back up to Google Drive** switch.




5. Click the **X** button to exit the *Settings* window and start a new *Settings* window (or click the left arrow at the bottom of the screen multiple times to go back to the main setting screen). On the main screen, scroll down until you see the *Google* icon. Click the **Google** button.

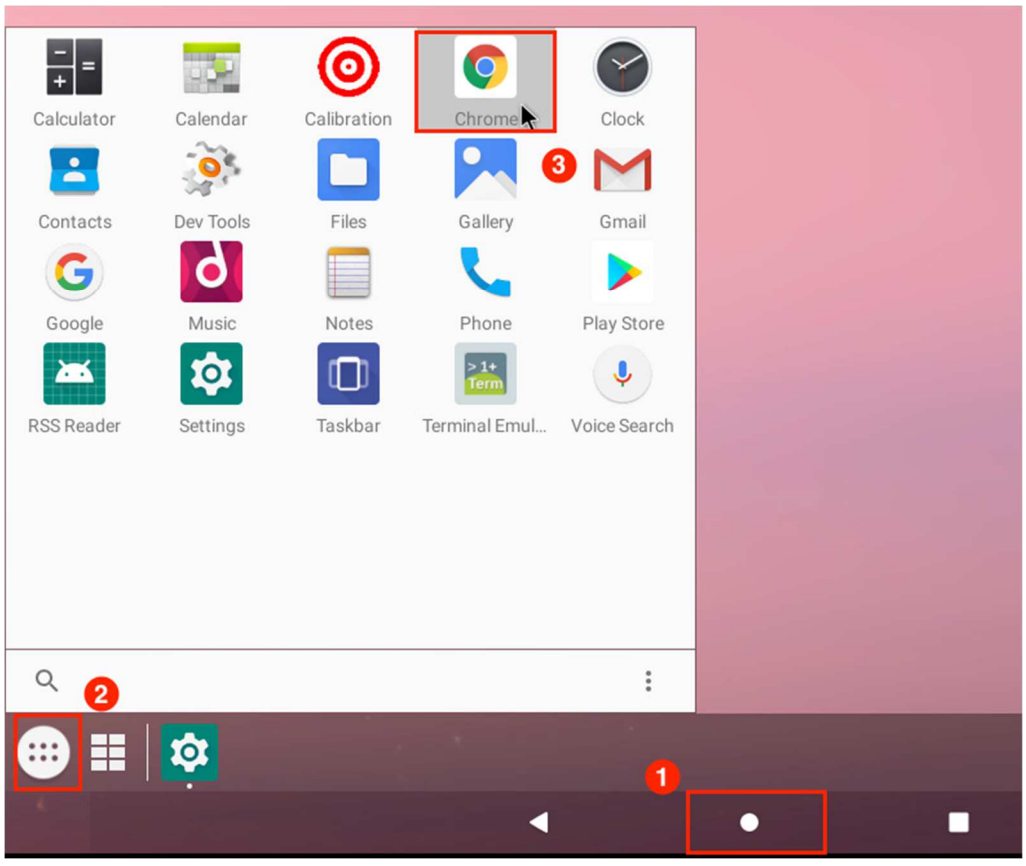


6. On the new screen, click the **Ads,** then turn on the *Opt out of Ads Personalization* switch; on the pop-up screen, click **OK.**

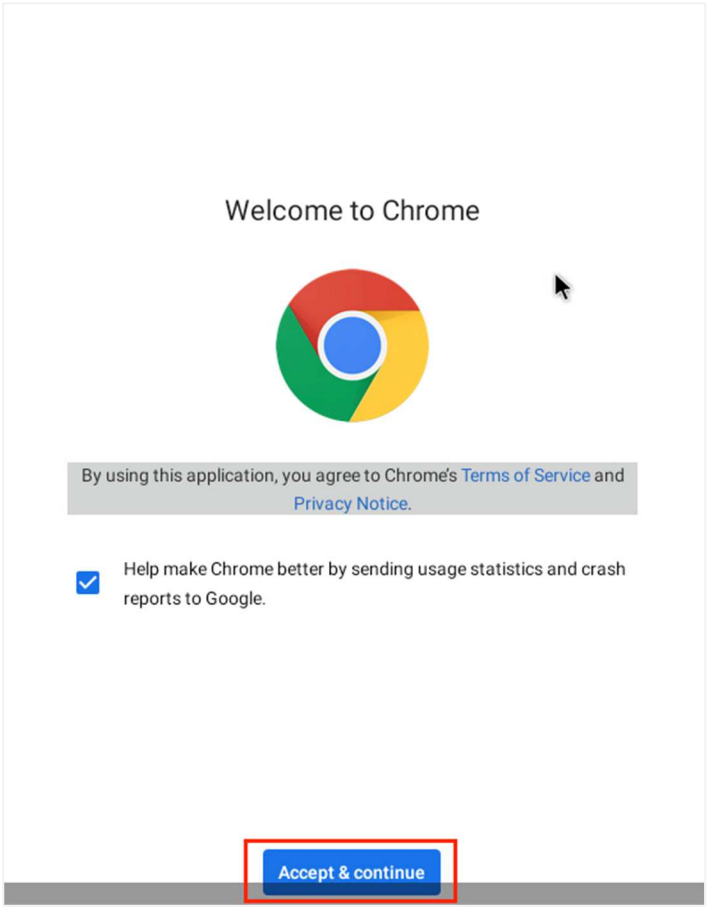



### 1.2.4 Android Chrome Browser Settings

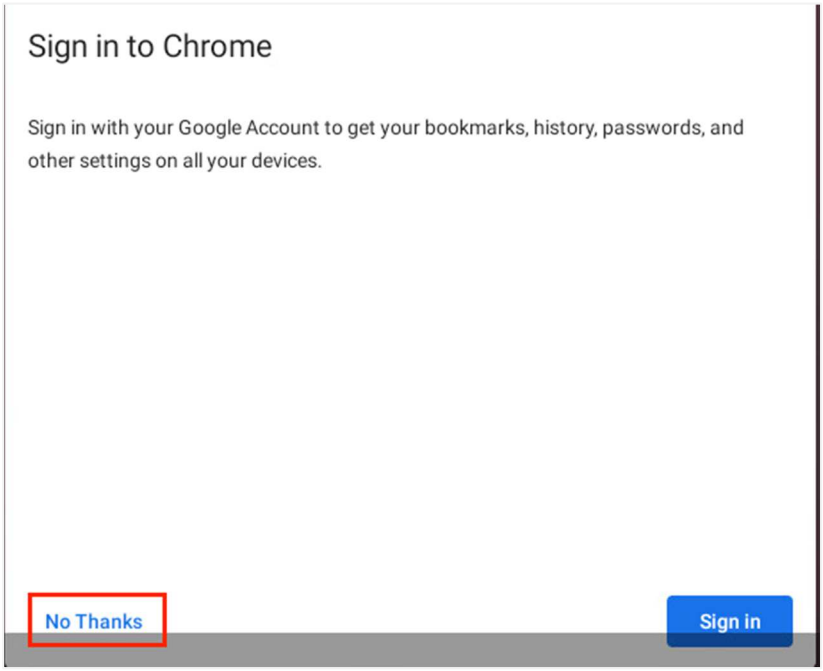
1. Click the **round dot** at the bottom of the screen to go back to the desktop. Then, click the **Applications** button. At last, click to start **Chrome**.



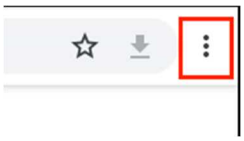
2. In the *Welcome* window, click **Accept & continue**. The usage statistics and crash reports may help Google improve the security of Chrome. We are going to leave it checked.




3. On the *Sign in* screen, click **No Thanks** since the virtual machine does not have internet access.

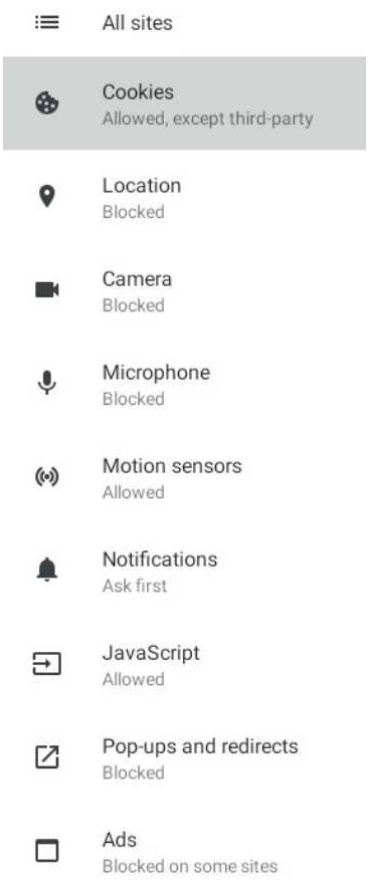


4. The *Chrome* browser will open. Let's go to the top-right corner of the screen, click the **menu** button.

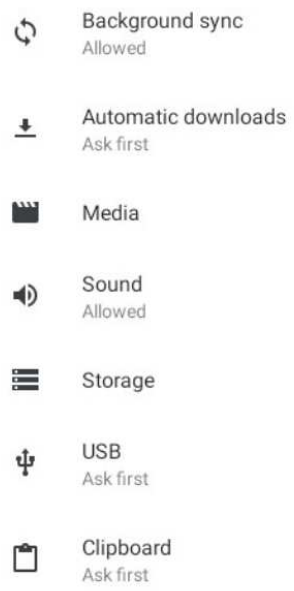


5. Then navigate to **Settings > Site settings > Cookies**, then check to **Block third-party cookies.**

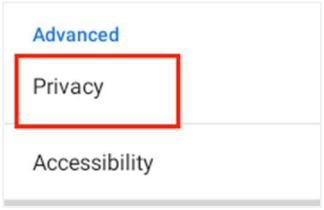

6. Click the **left arrow** to go back, verify the others are matching the settings shown in the screenshot below:



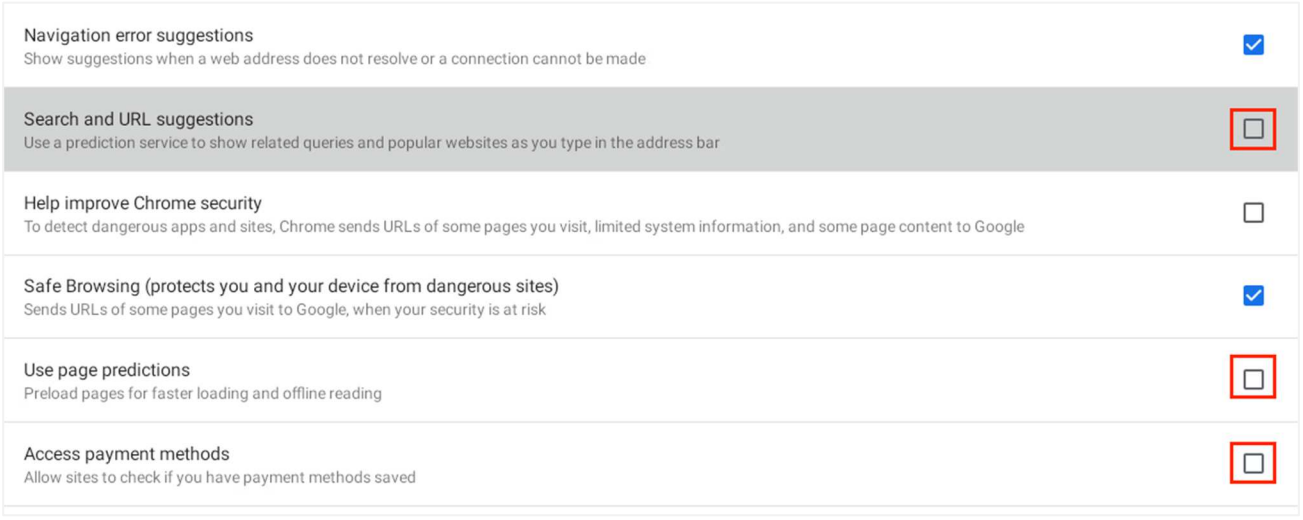

  




7. Click the **left arrow** once again. In the *Advanced* section, click **Privacy.**

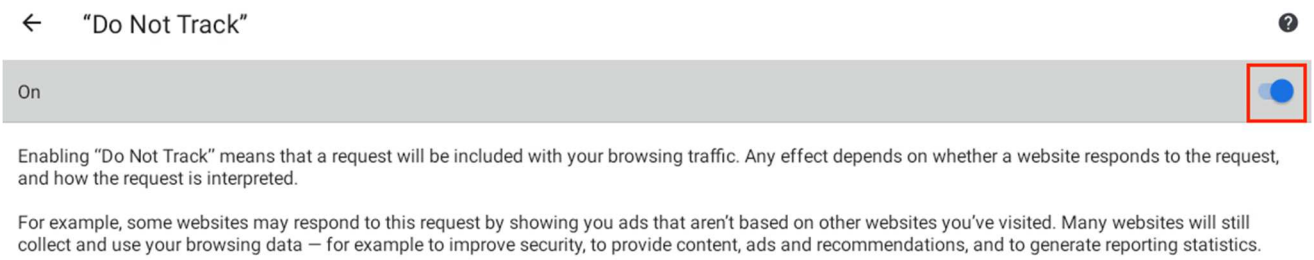



8. On the new screen, uncheck the **Search and URL suggestions, Use page predictions,** and **Access payment methods.**



9. Click **Do Not Track** and turn on the switch.




10. The security, privacy, and basic settings mentioned in this lab are general settings. The Android operating system can adjust the settings for different apps. You will want to check them each time when you install new apps and understand what privileges they need and why they need them.

11. The lab is now complete; you may end the reservation.