Mobile Application Security Assessment
Burp Suite

Table of Contents

Objective

In this lab experiment we will learn to use Burp Suite in mobile application environment to intercept the traffic by using man-in-the-middle attack and to detect SSL certificate validation errors.

Requirements

Android Emulator (any emulator of your choice Android X-86 or Genymotion), Linux VM (Kali or any Linux OS of your choice)

Report requirements

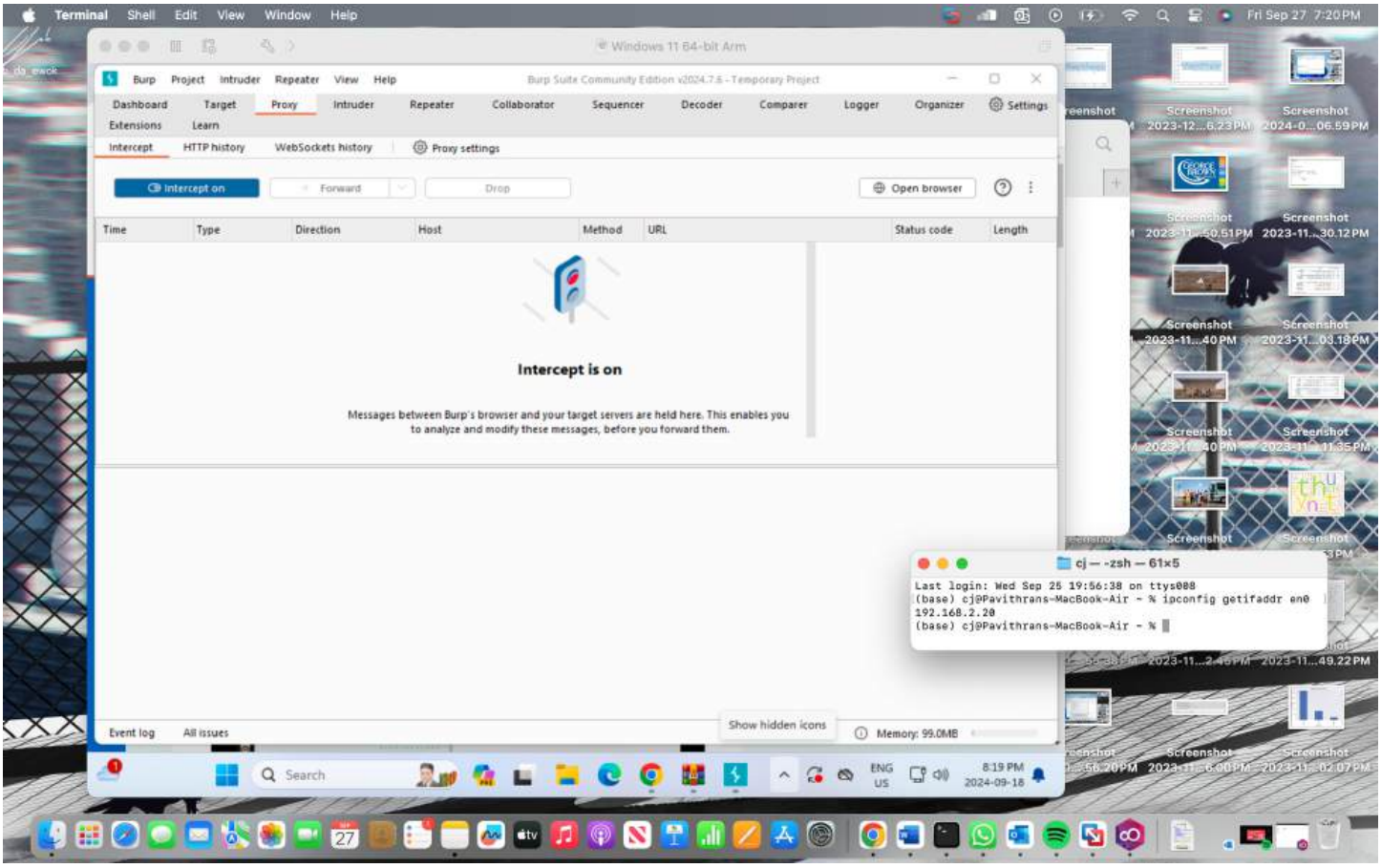
Follow the submission formatting guidelines and make sure to include significant screenshots, captions, and detailed explanation. The 2 screenshots in sections 7 and 16 (step 7 and step 16) are mandatory and shall indicate student's name and proof of completion.

Instruction

1. **Step 1: Installing Burp Suite**
    - Note: Burp Suite is already installed in Kali Linux. Therefore, of you are using Kali you do not need to install it again.

Burp is a very popular proxy, enabling you to view and alter network traffic. In a Web browser, go to https://portswigger.net/burp. In the "Community Edition" column, click Download", as shown below.

I'm using macbook Air M, so I have Windows 11 VM installed using VMWare Fusion. Installed burp suit there.
It shows interception on



2. Step 2: Starting Burp

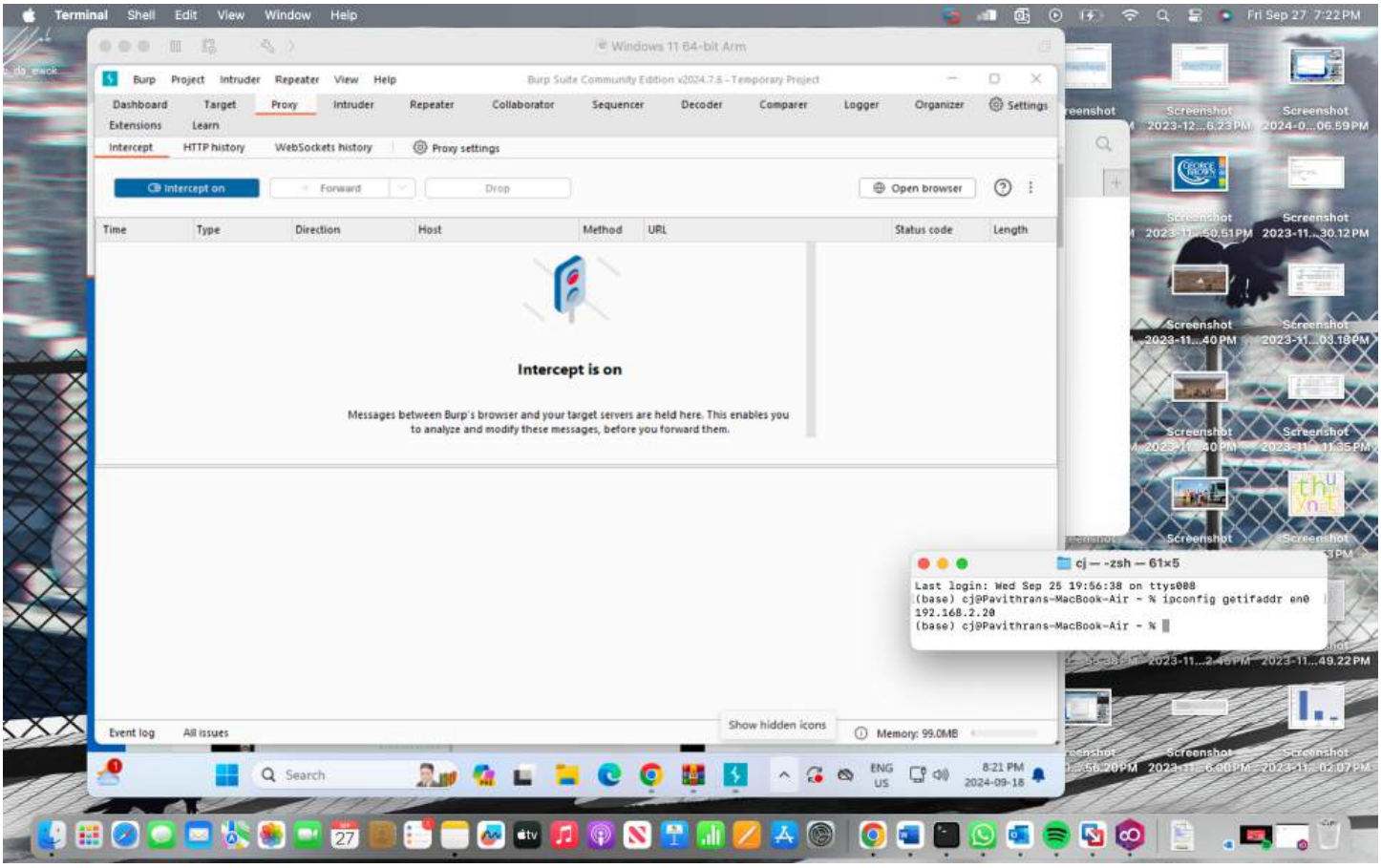
When Burp starts, the first window asks you to create a project. Accept the default option of "Temporary project" and click Next.

In the next page, click the Start Burp button.

The main Burp window opens, as shown below.

Click the Proxy tab. Click the Intercept sub-tab.

The third button says, "Intercept is on", as shown below.

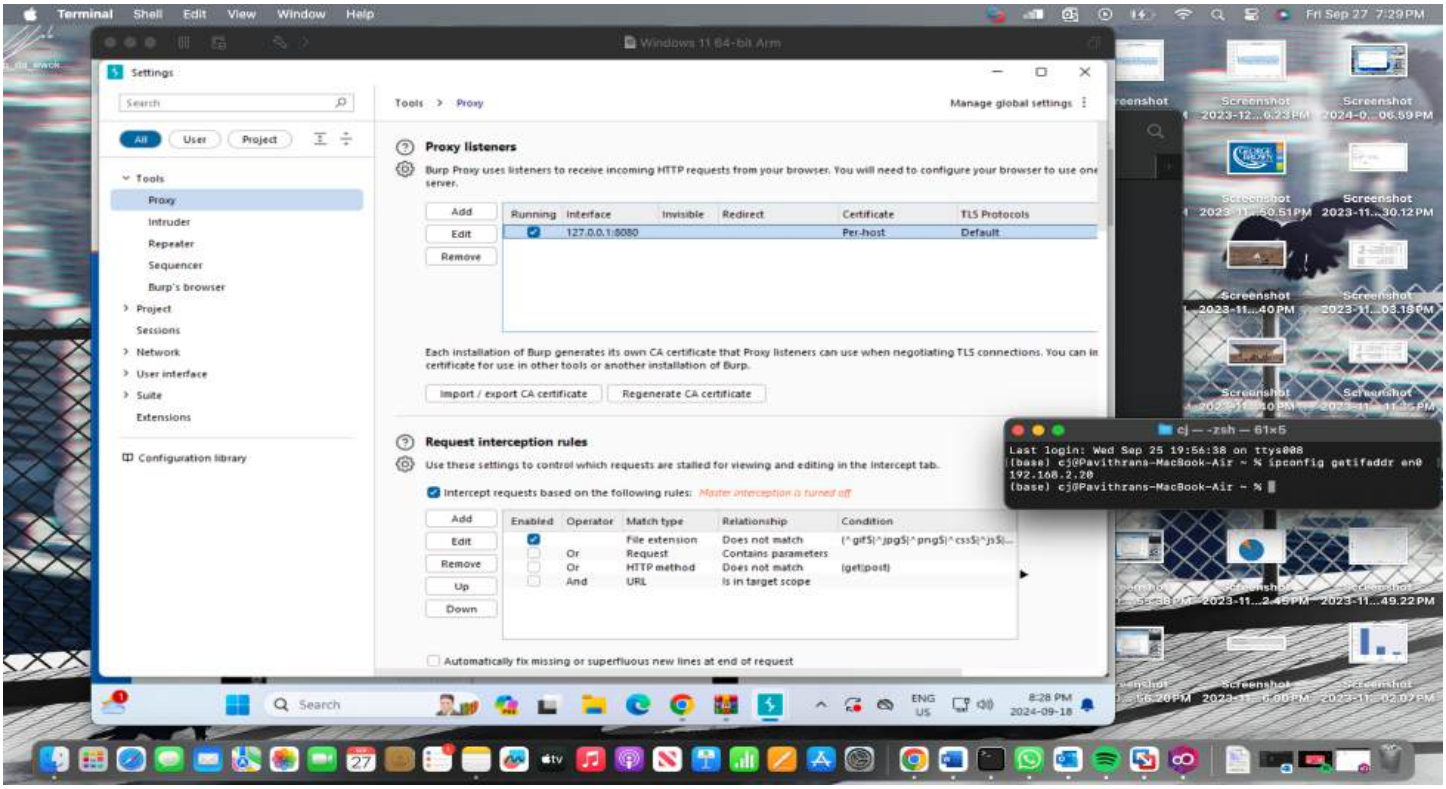


3. Step 3: Configuring Burp

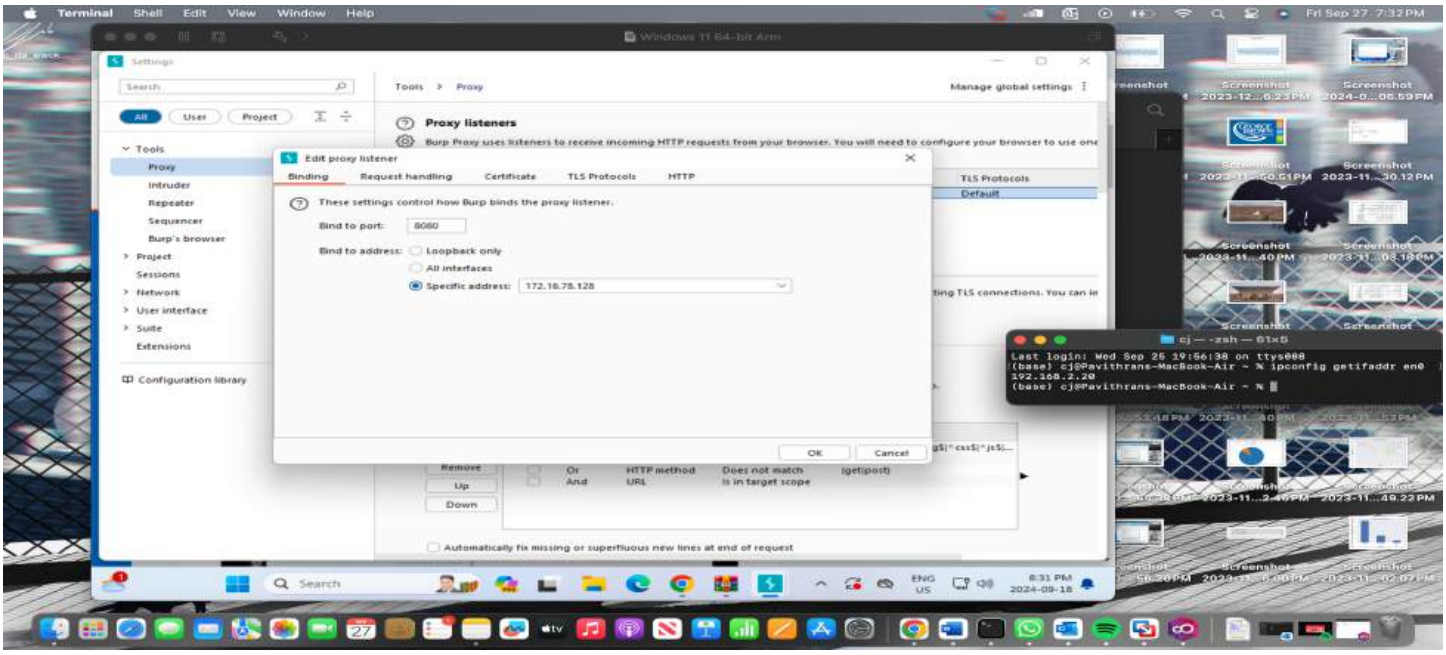
In Burp, click the "Intercept is on" button. It changes to "Intercept is off".

On the Proxy tab, click the Options sub-tab.

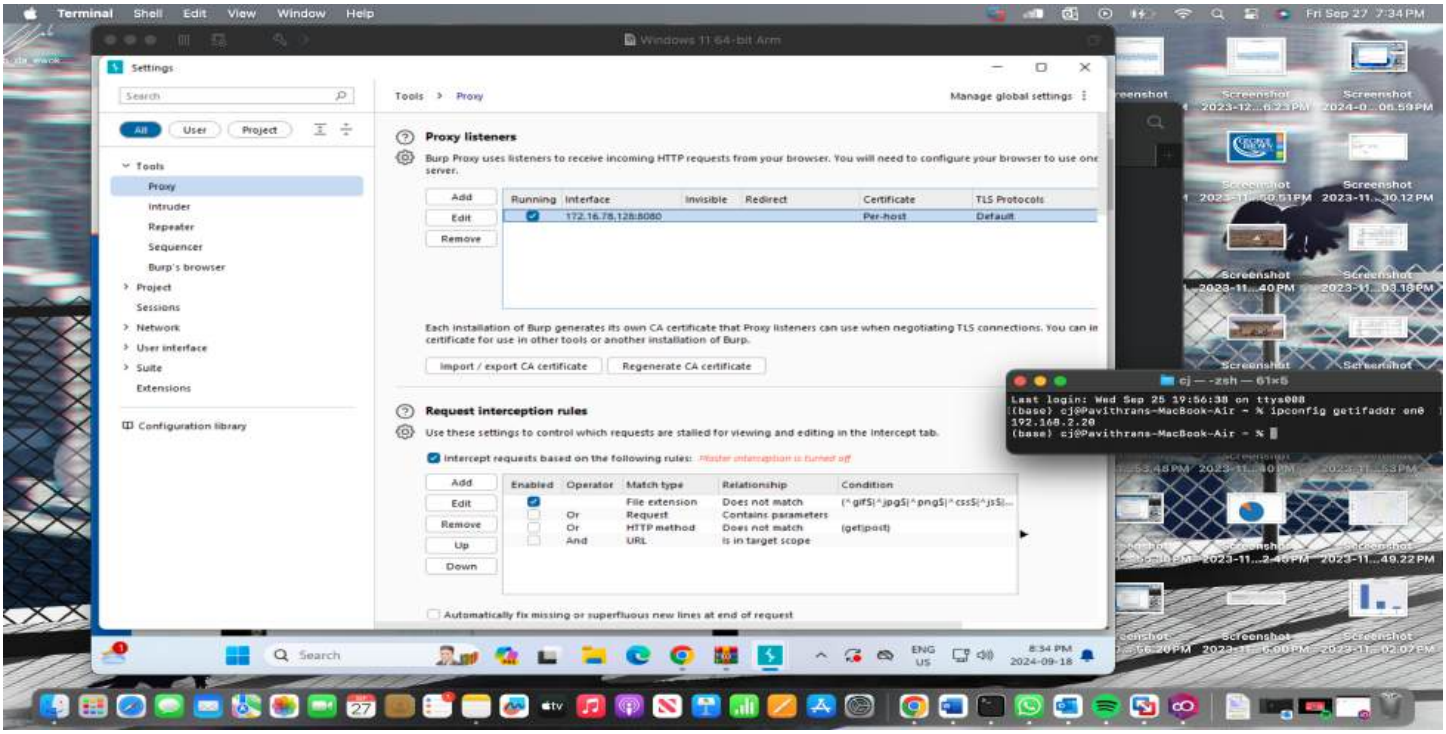
In the central box, click the Interface address to highlight it, as shown below.



On the left side, click the Edit button.
In the "Edit proxy listener" box, click the "Specific address" button, and select your computer's IP address that is used to connect to the Internet, as shown below.



Click OK.
Burp shows a proxy listener on your IP address and port 8080, as shown below.
Make a note of this address--you will need it below.



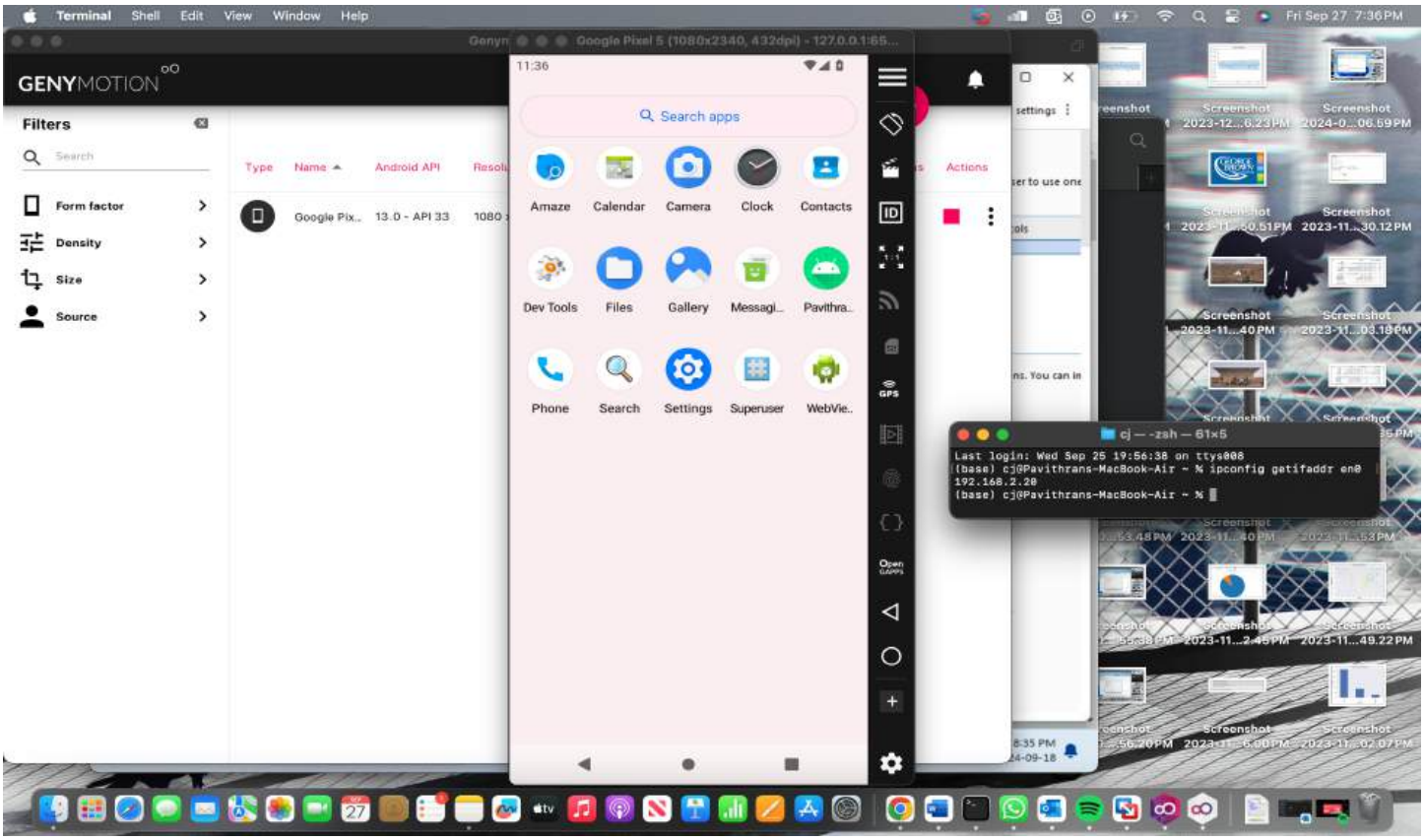
Burp is configured by turning the interception off and selecting the ip and port.

4. Step 4: Adjusting Android Networking to Use the Burp Proxy

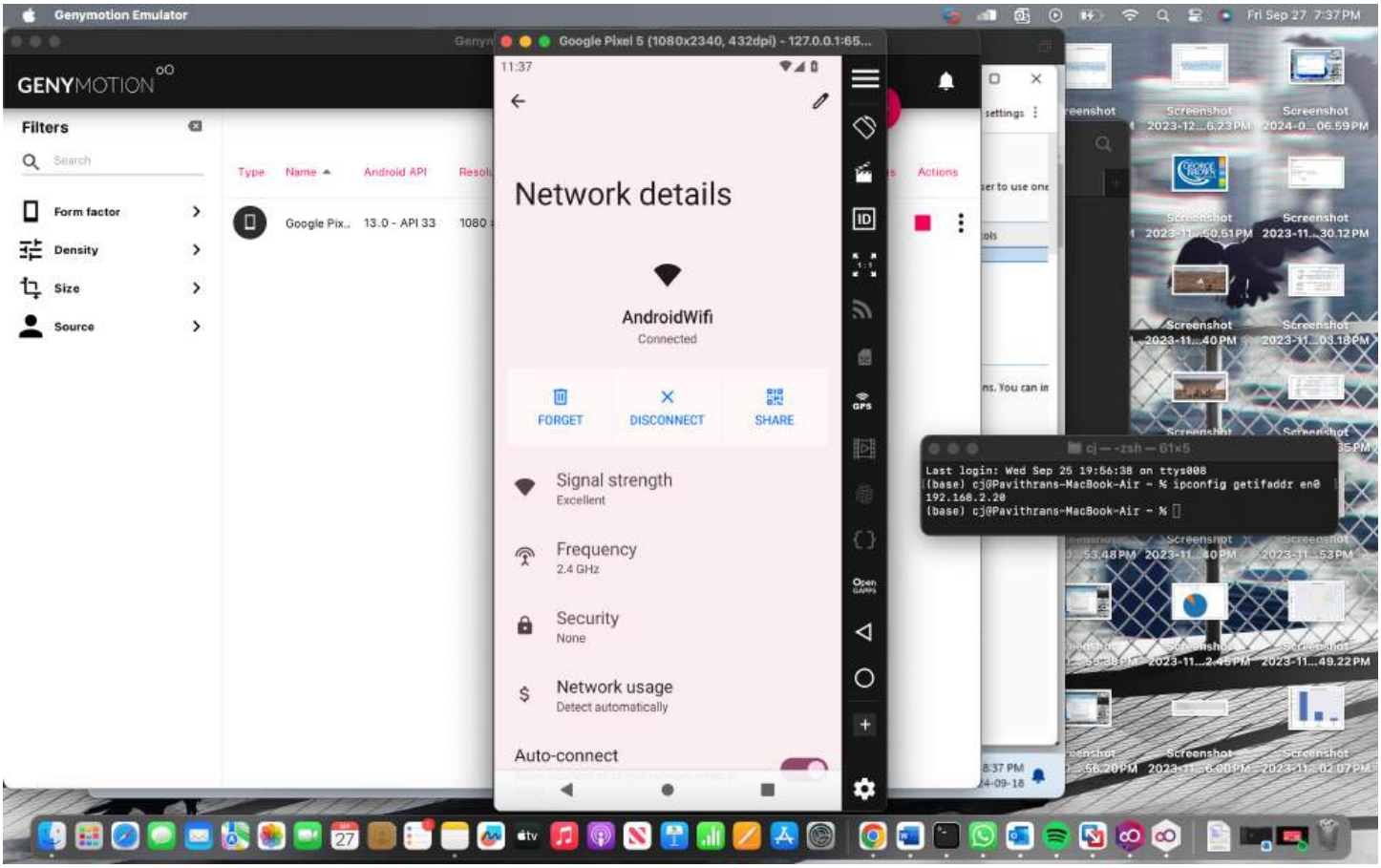
Launch your Android emulator (i.e. Genymotion, Android X-86, etc.)

From the Android home screen, click and drag up to show all apps.

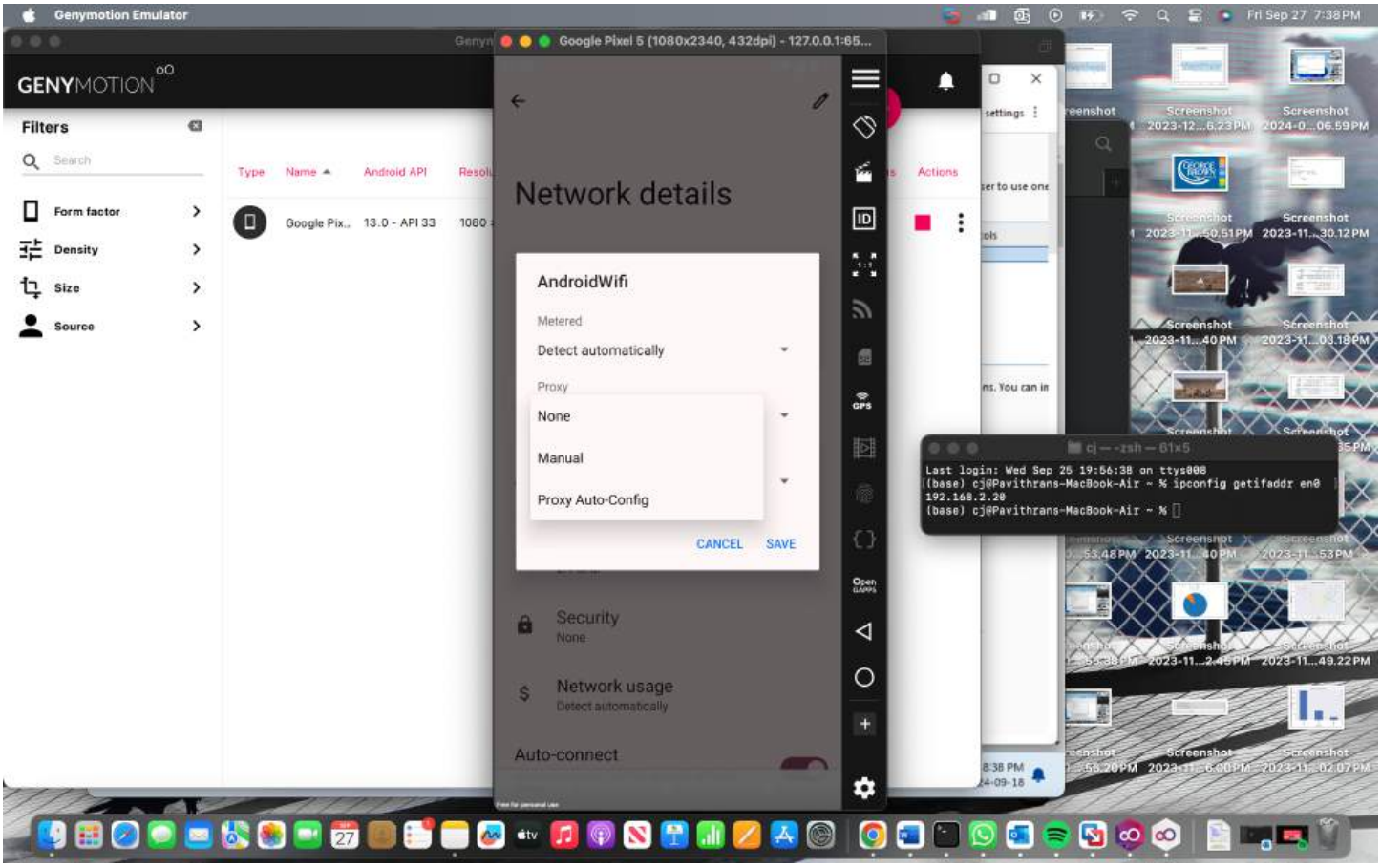
Click Settings, which is outlined in green in the image below.



In Settings, click "Network & internet".
Click Wi-Fi.
Click AndroidWiFi.
Click Advanced.
In the "Network details" screen, at the top right, click the Pencil icon, outlined in green in the image below.

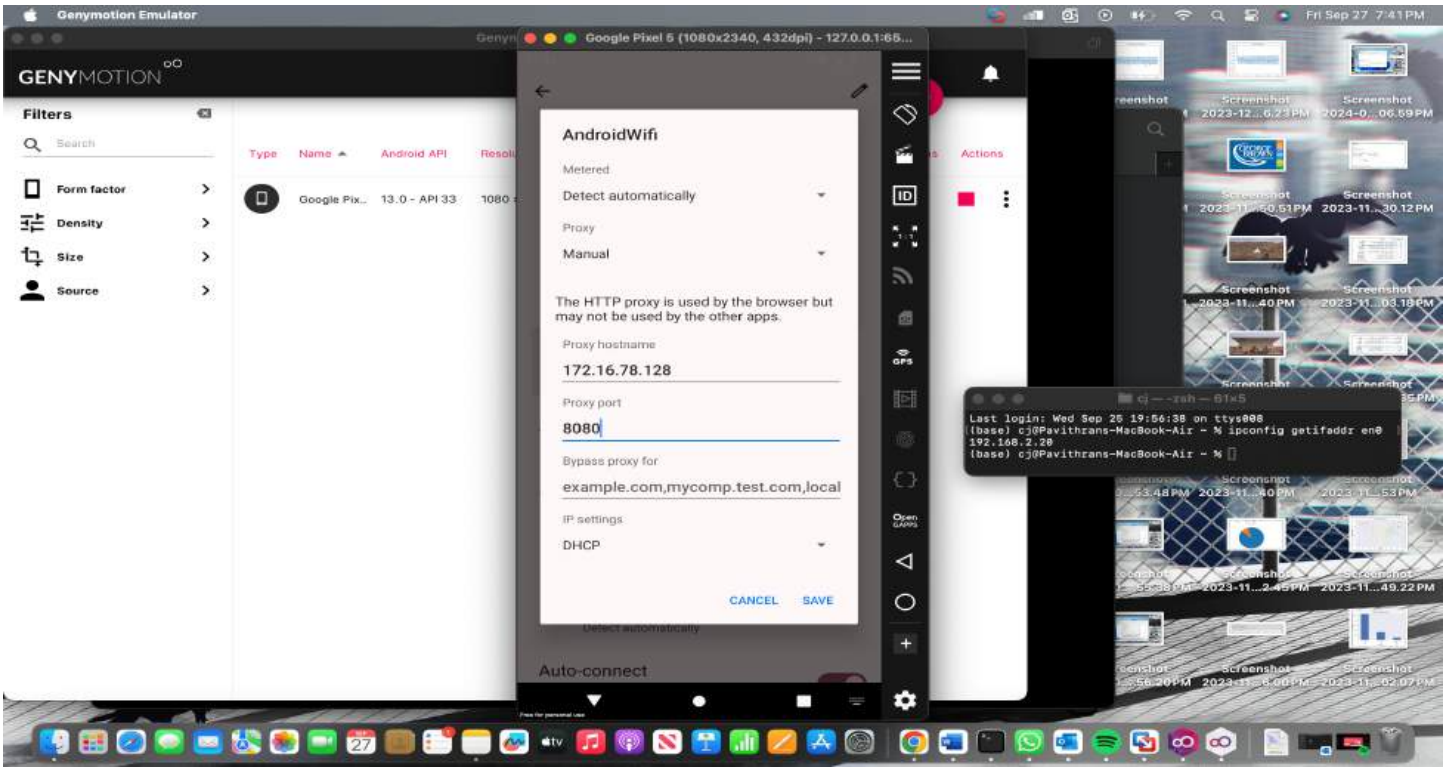


In the "AndroidWifi" box, in the "Advanced options" row, click the down-arrow.
In the "Proxy" field, click the down-arrow.
Click Manual, which is outlined in green in the image below.



Here we change from manual to customize, here we give the port and ip from out burp that we configured

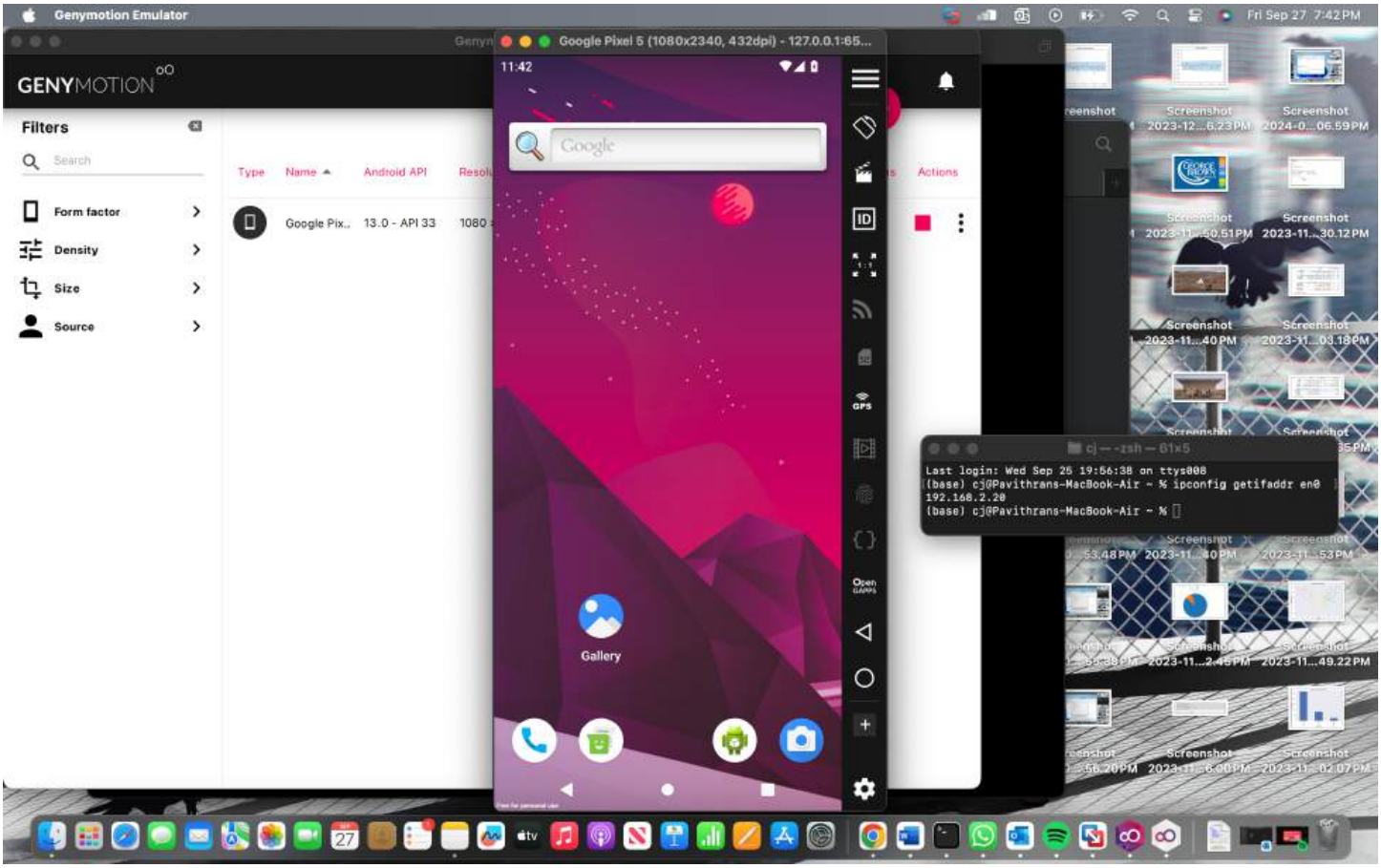
Enter the IP address and port number of the Burp proxy listener, as shown below.



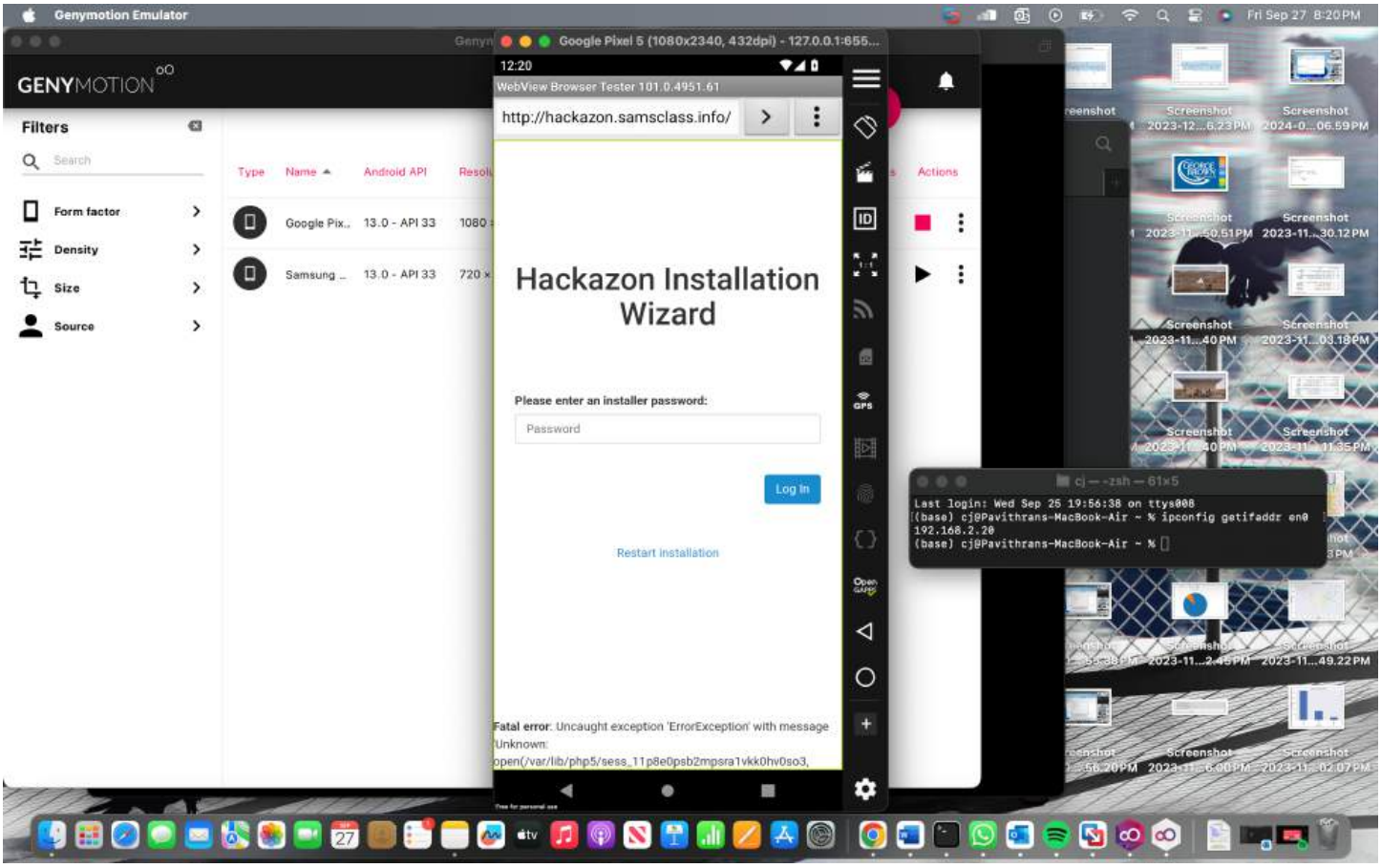
On your Android device, click SAVE.
At the bottom center of the device, click the round Home button.

5. Step 5: Testing the Proxy

From the Android home page, on the lower right, click the Browser, outlined in green in the image below.



In the Browser, go to http://hackazon.samsclass.info/ or http://testfire.net/login.jsp or preferably create your own http based login web page using XAMPP or any other web server (http://<ip address of your own http login website>) and then continue the next steps. This lab manual continues with hackazon for demonstration, but you don't need to use it.
A "Hackazon" shopping site opens, as shown below.

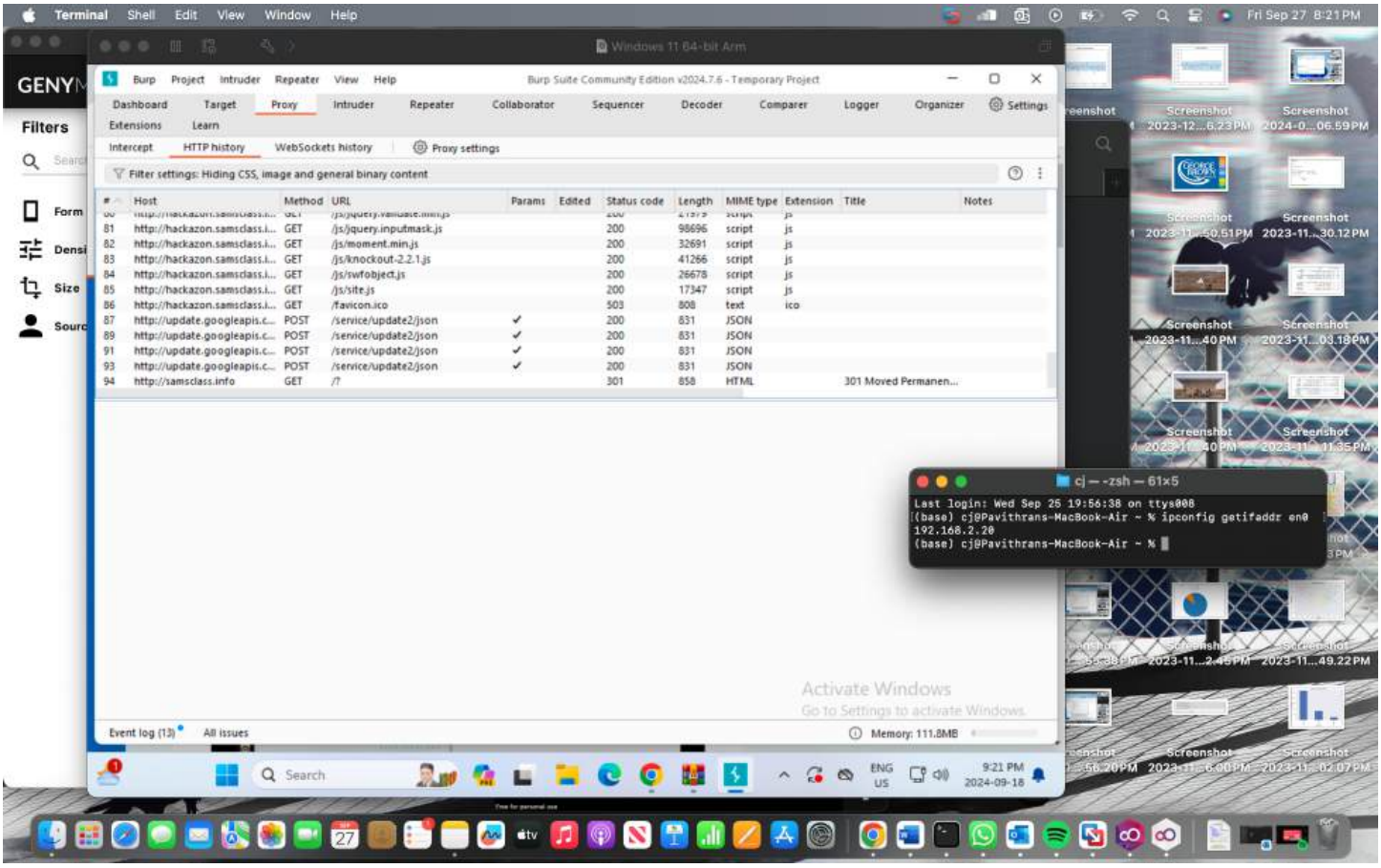


We test the proxy by the browser following the steps above and I used the hackzone website for this step.

6. Step 6: Viewing Traffic in Burp

In Burp, on the Proxy tab, click the "HTTP history" sub-tab.

Scroll down and find traffic to hackazon.samsclass.info as shown below.

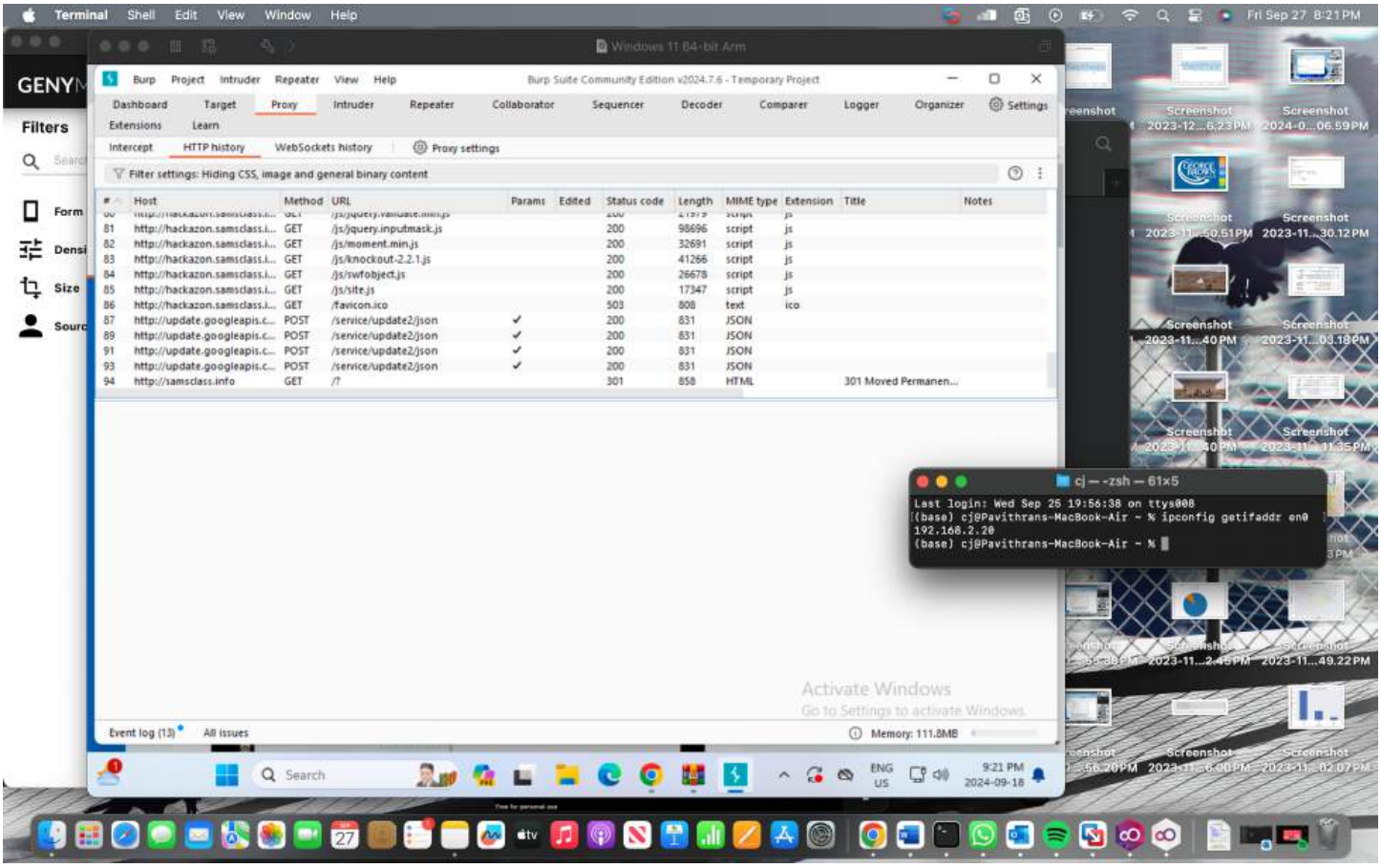


Here I can view the traffic that I visited hackzone website on our burpsuit

7. Step 7: Saving a Screen Image

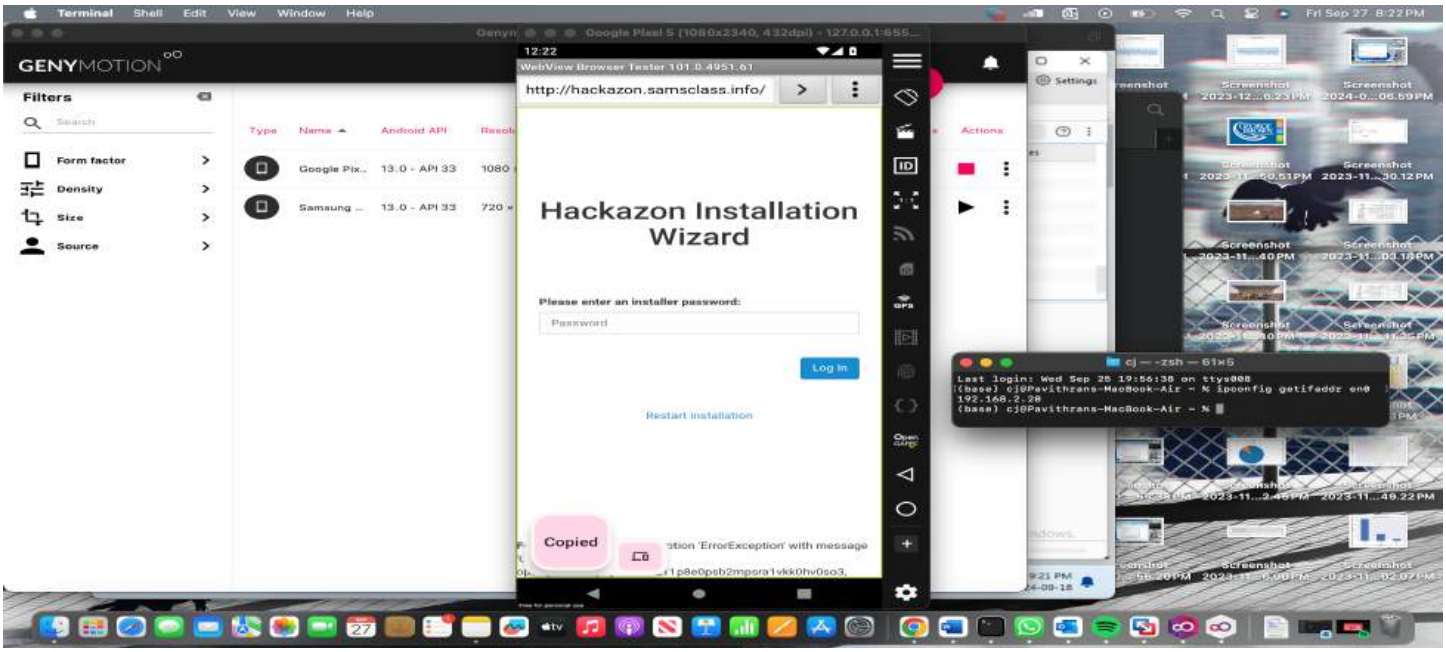
In addition to your previous screenshots and explanations, at this step make sure you can see hackazon.samsclass.info or any other http site of your choice in Burp, as shown above.
This screenshot is mandatory in addition to other significant screenshots.

Here I can view the traffic that I visited hackzone website on our burp suit, it gives all the details listed on the screenshot.



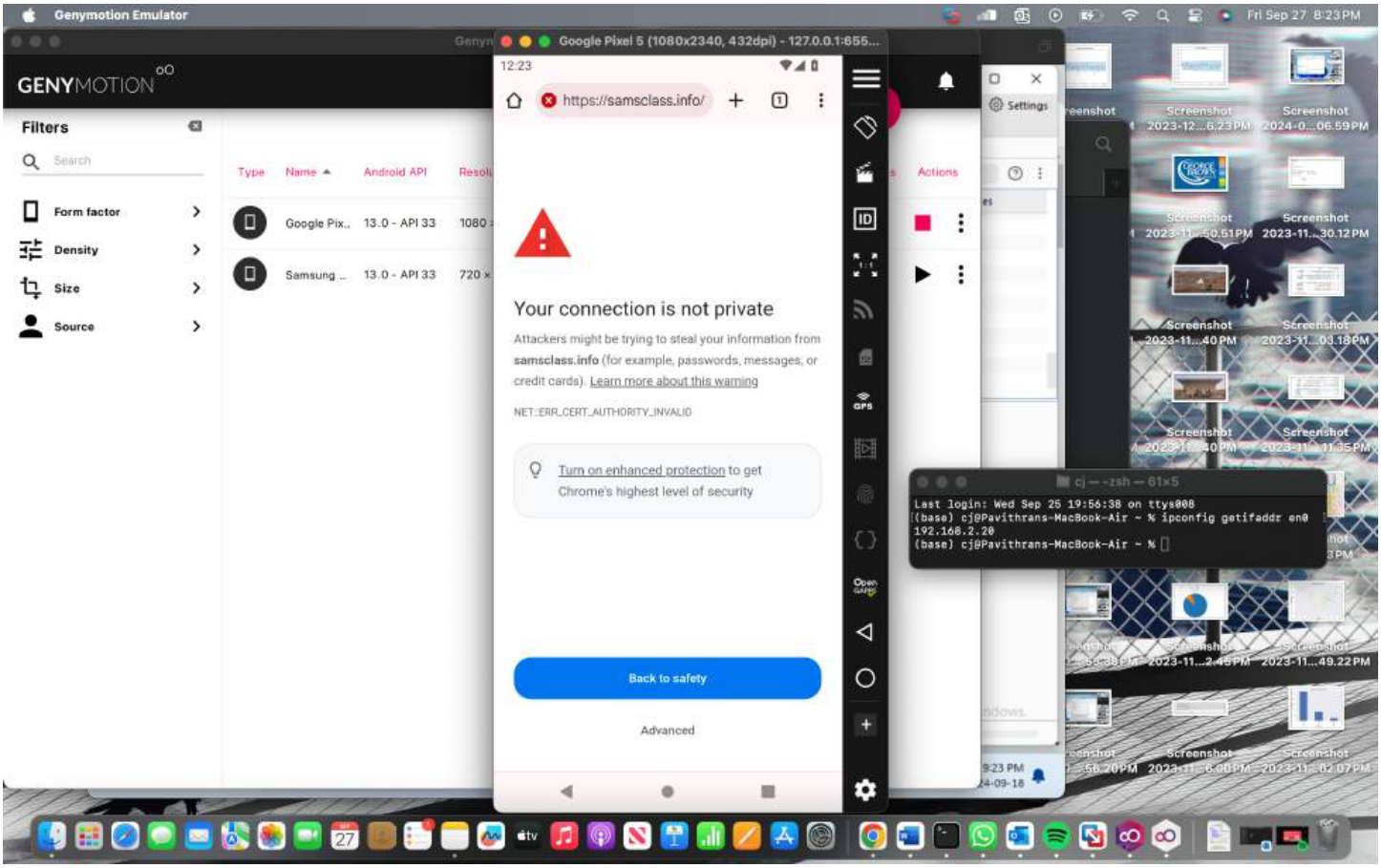
8. Step 8: Opening a Secure Page

In the Android device, in the Browser, and go to https://samsclass.info or your locally created https site. The browser does nothing, as shown below. It's a lousy browser, which is why we installed Chrome.



9. Step 9: Opening a Secure Page in Chrome

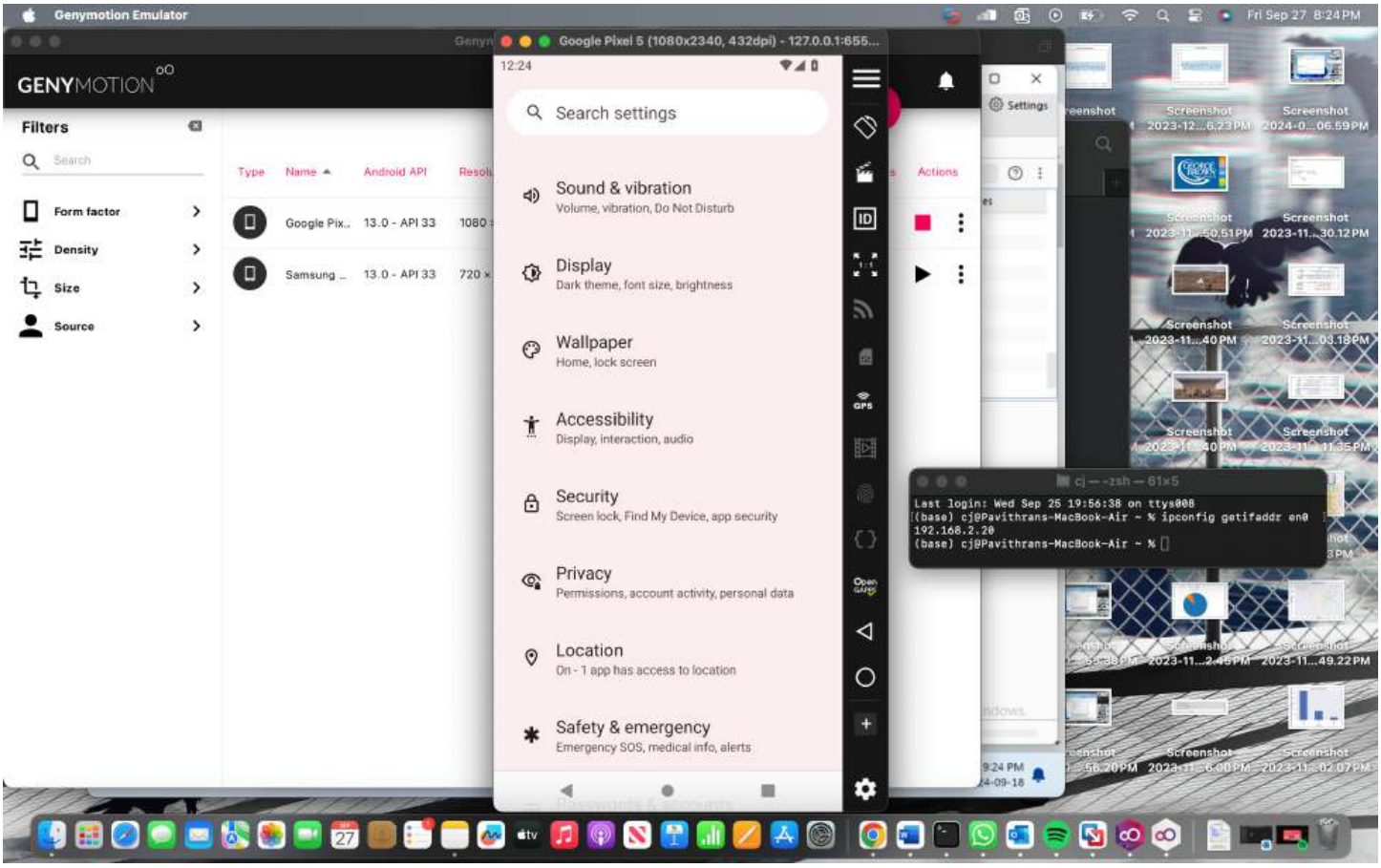
If using your own https login page accept the certificate warning. If using hackazon then at the bottom center of the device, click the Home button. Open Chrome.
When you see the "Sign in to Chrome" page, click "NO THANKS".
In Chrome, go to https://samsclass.info
A warning message appears, saying "Your connection is not private", as shown below. Notice the specific error shown: NET:ERR_CERT_AUTHORITY_INVALID. This happens because Burp is performing a man-in-the-middle attack with a self-signed certificate.



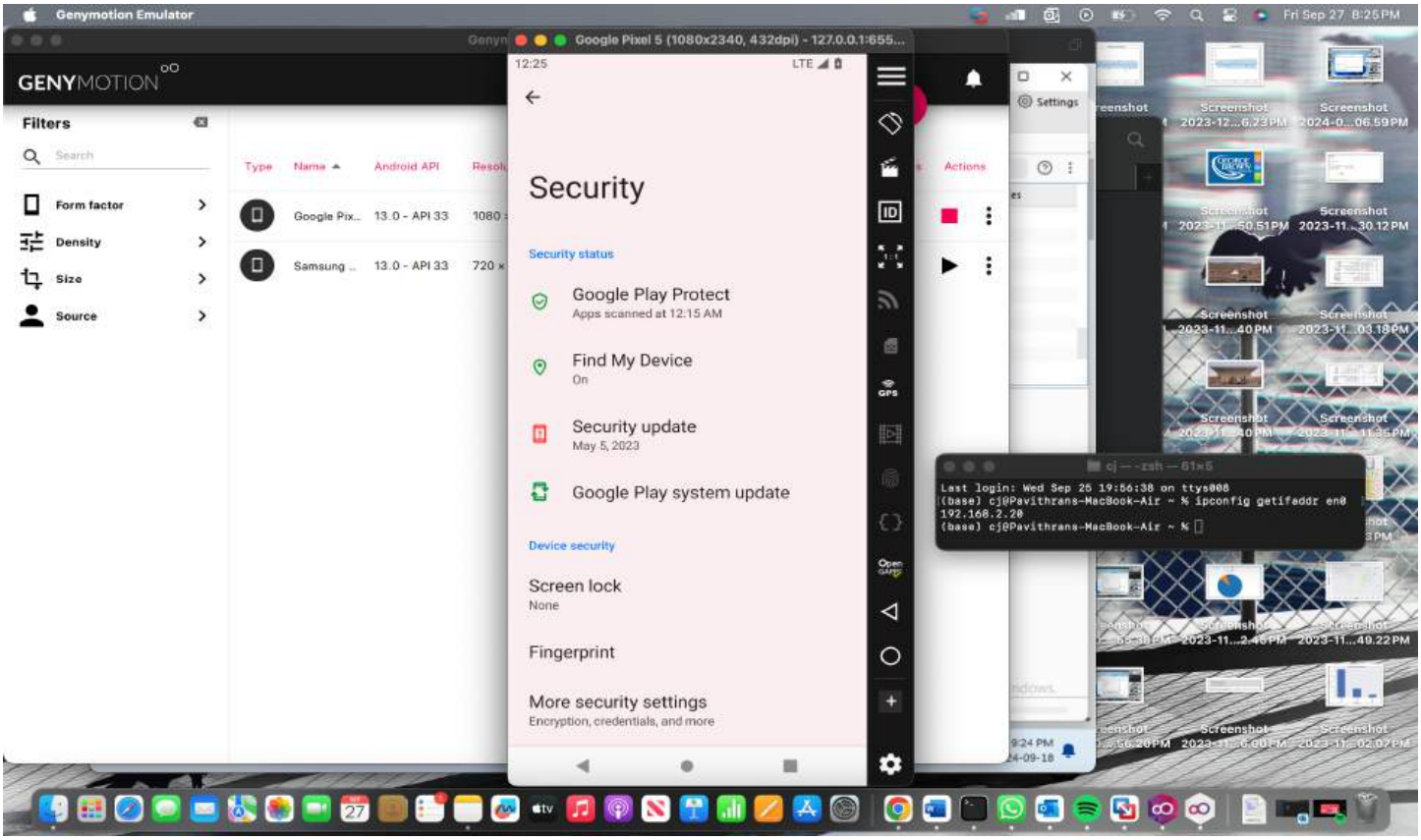
When I tried using chrome I'm getting the error to load the hackzone website as expected

10. Step 10: Setting a PIN

Android won't let us import a certificate until the device has a PIN configured, so we'll do that first.
At the bottom center of the device, click the Home button. Open Settings.
Scroll down and click "Security & location", as shown below.



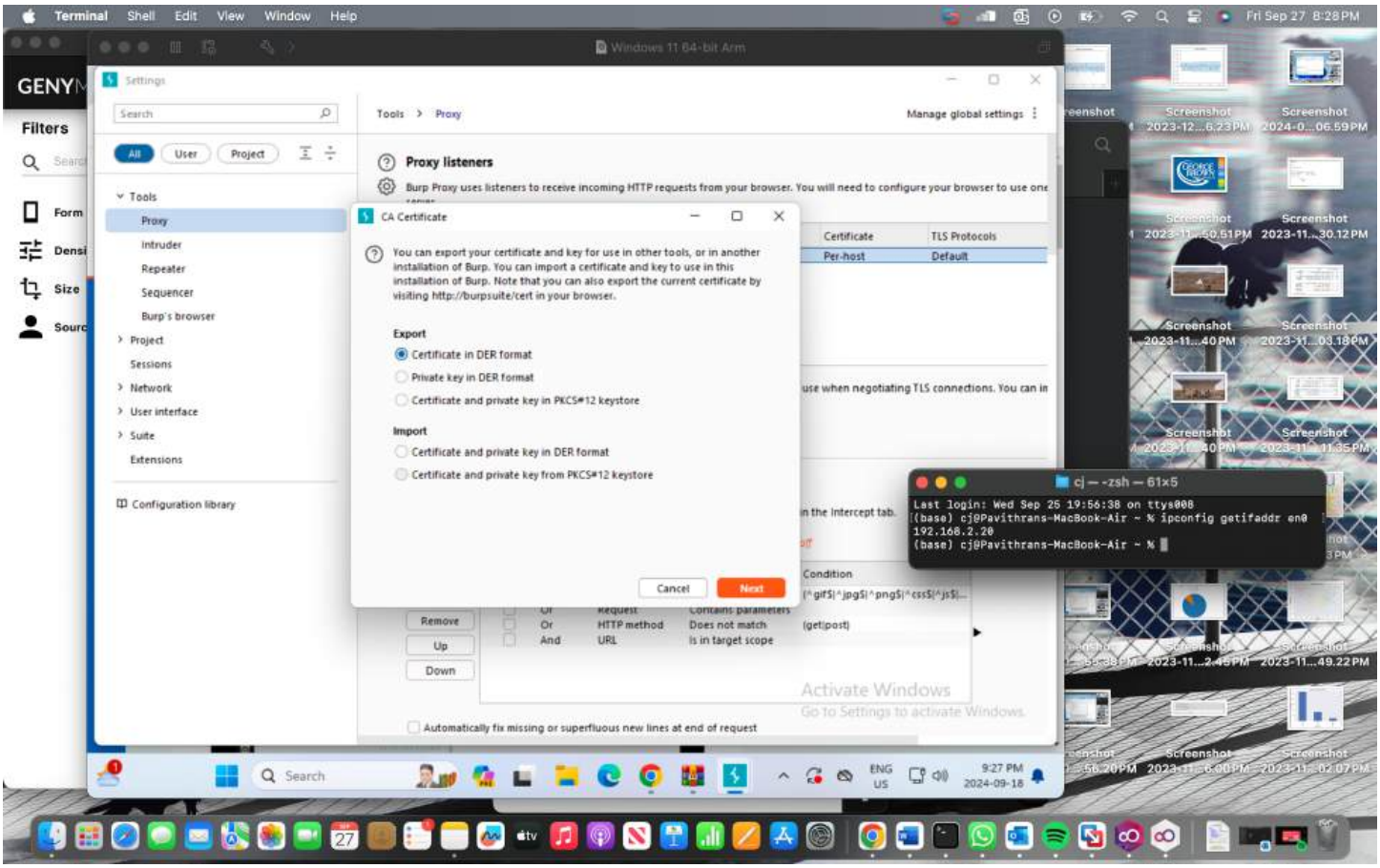
In the "Security & location" screen, click "Screen lock", as shown below.



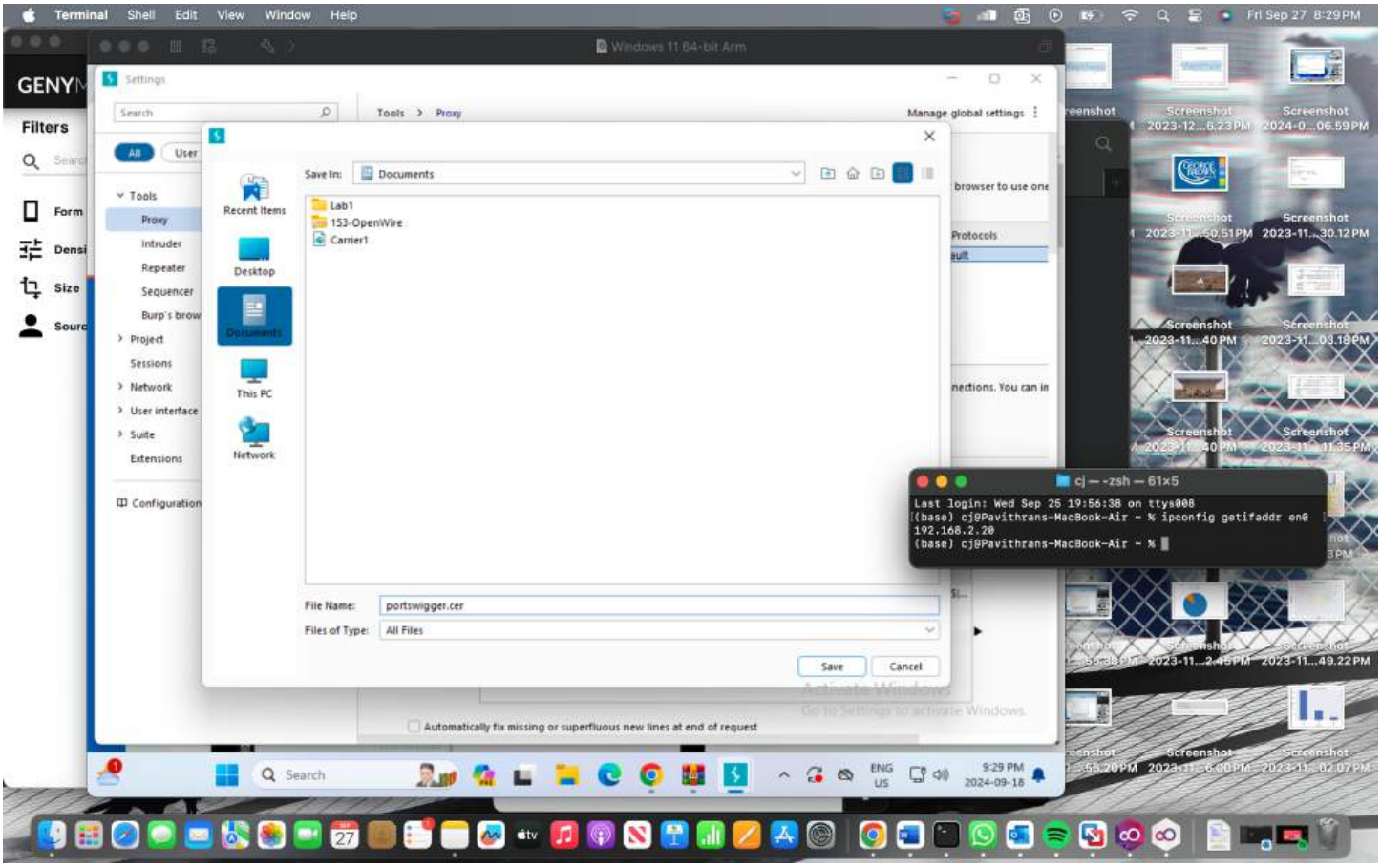
In the "Choose screen lock" screen, click PIN.
Enter a simple PIN you can remember, such as 1234, twice. Click DONE.

11. Step 11: Exporting the PortSwigger CA Certificate from Burp

This is HTTPS working as it should, warning you that you do not have a secure connection to the end site. Burp is intercepting the traffic.
We want to add PortSwigger as a trusted certificate authority to get rid of these messages.
In Burp, click the Proxy tab.
Click the Options sub-tab.
Click the "Import /export CA certificate..." button.
In the "CA Certificate" box, in the Export setion, click the "Certificate in DER format" button, as shown below.



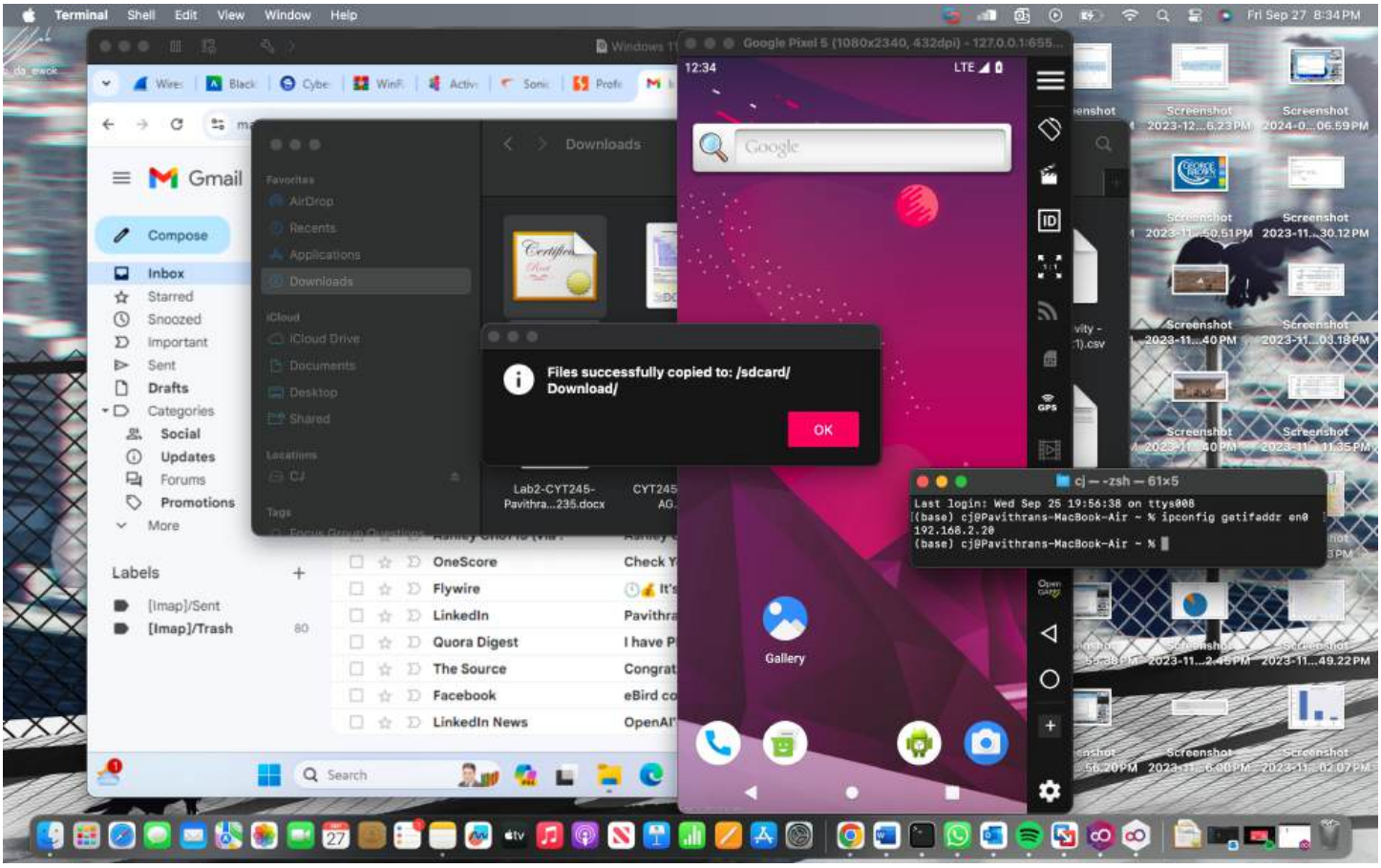
Click Next.
On the next page, click the "Select file..." button. Navigate to a folder you can find, such as your Desktop.
Give the file a name of portswigger.cer, as shown below.



Click Save.
Click Next. Click Close.
Followed all the steps to download the certificate.

12. Step 12: Installing the PortSwigger CA Certificate into Android

Drag the portswigger.cer file from your host system and drop it on the Android home page.
A message appears, saying "Files successfully copied to sdcard/Download", as shown below.

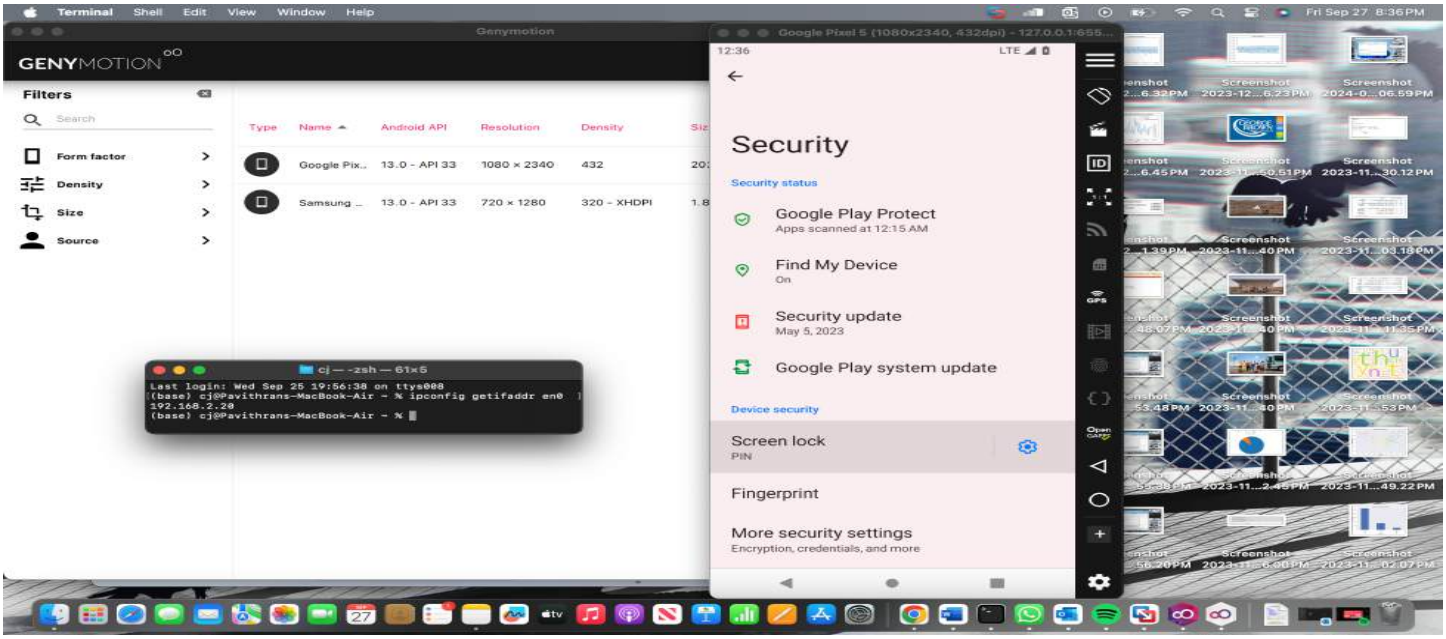


Click OK.

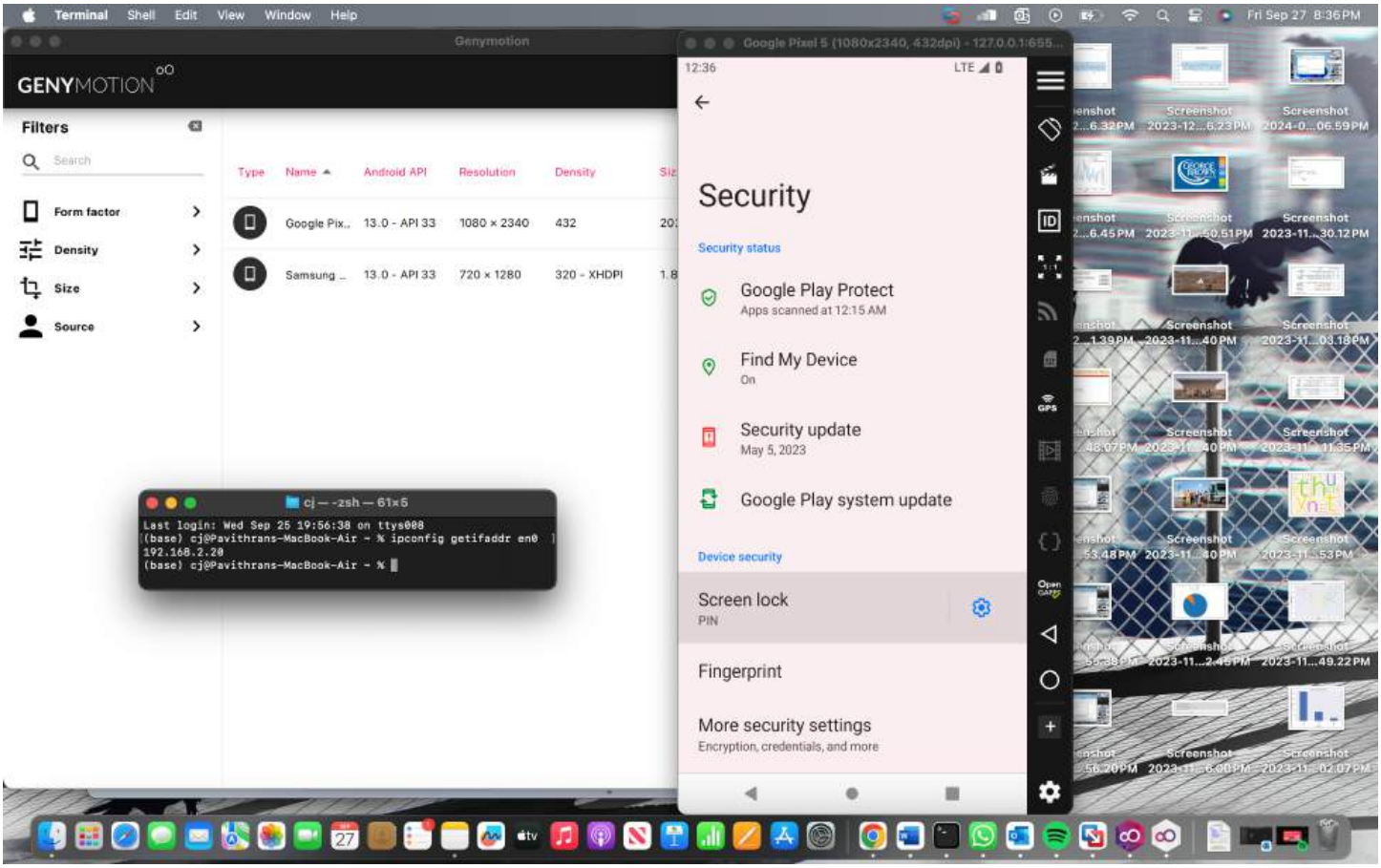
I emailed the certificate so that I can download it on my local system and drop it on my android screen

13. Step 13: Importing the Portswigger Certificate

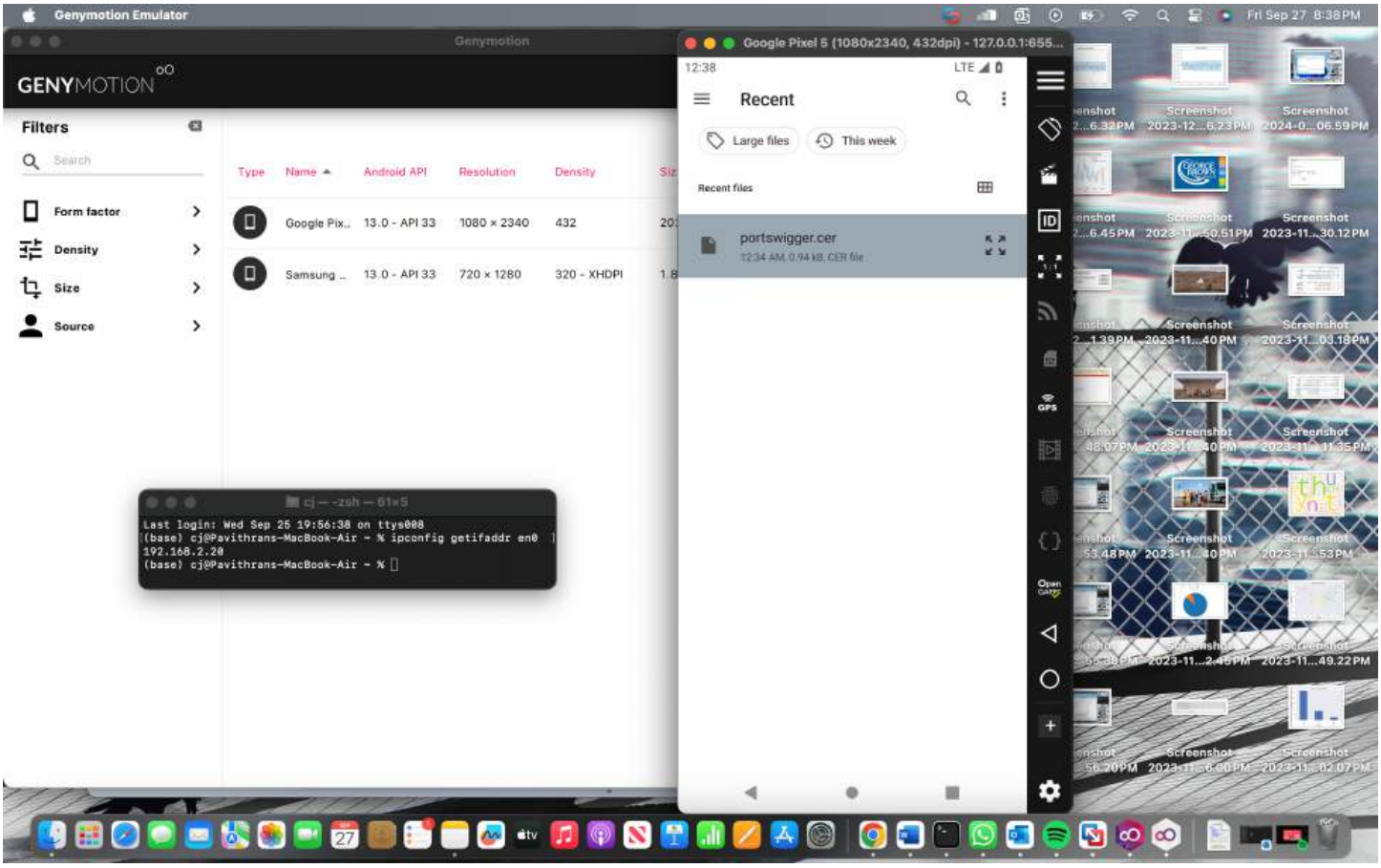
On your Android device, in the "Security & location" screen, click Advanced, as shown below.



Click "Encryption & credentials".
Click "Install from SD card", as shown below.



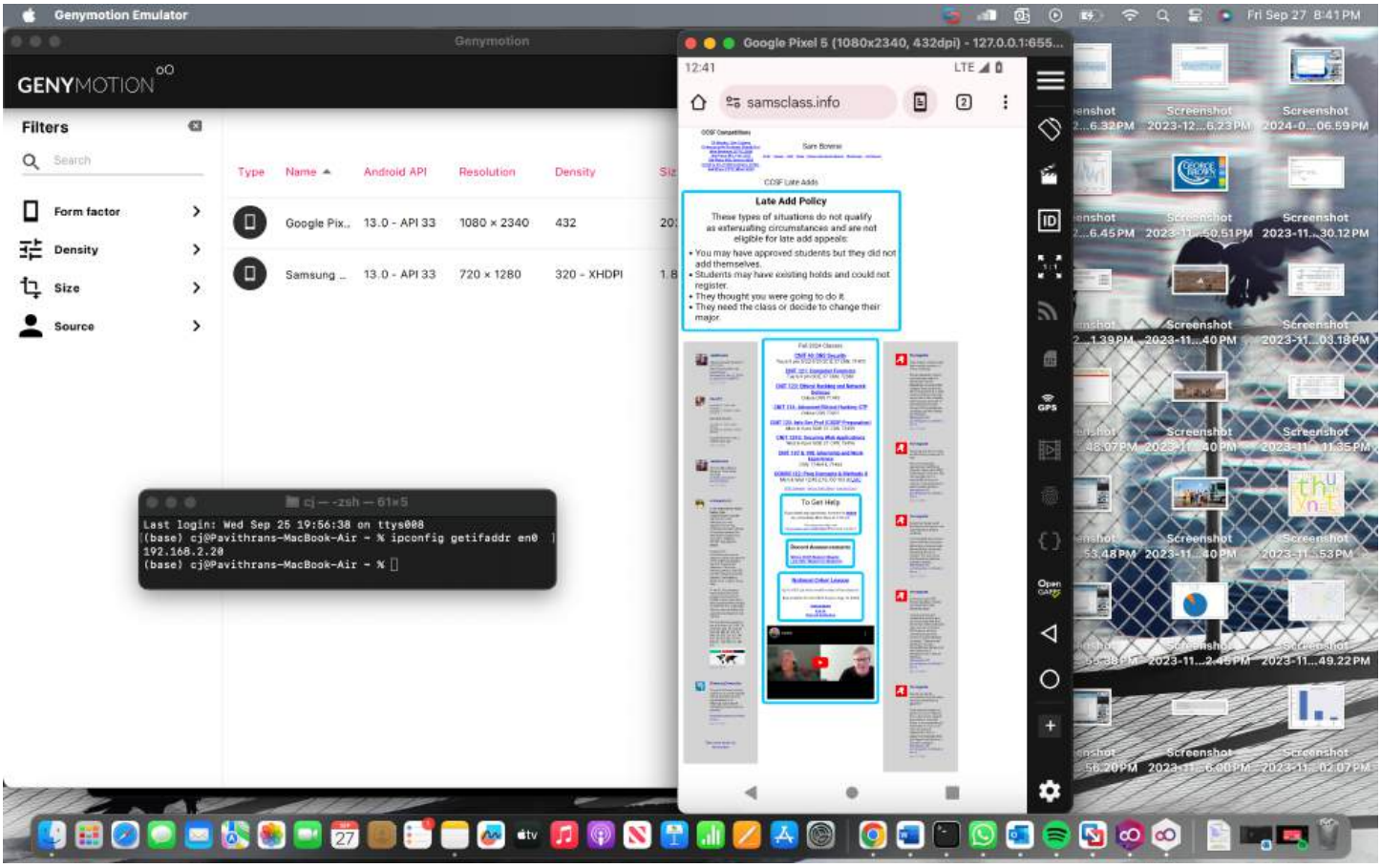
In the next screen, at the top left, click the three-bar icon. Click Downloads.
In the Downloads window, click portswigger.cer, as shown below.



Enter your PIN.
Enter a name of portswigger, as shown below, and click OK.

14. Step 14: Opening a Secure Page Again

In Android, launch Chrome. Go to
https://samsclass.info The page opens, as shown below.

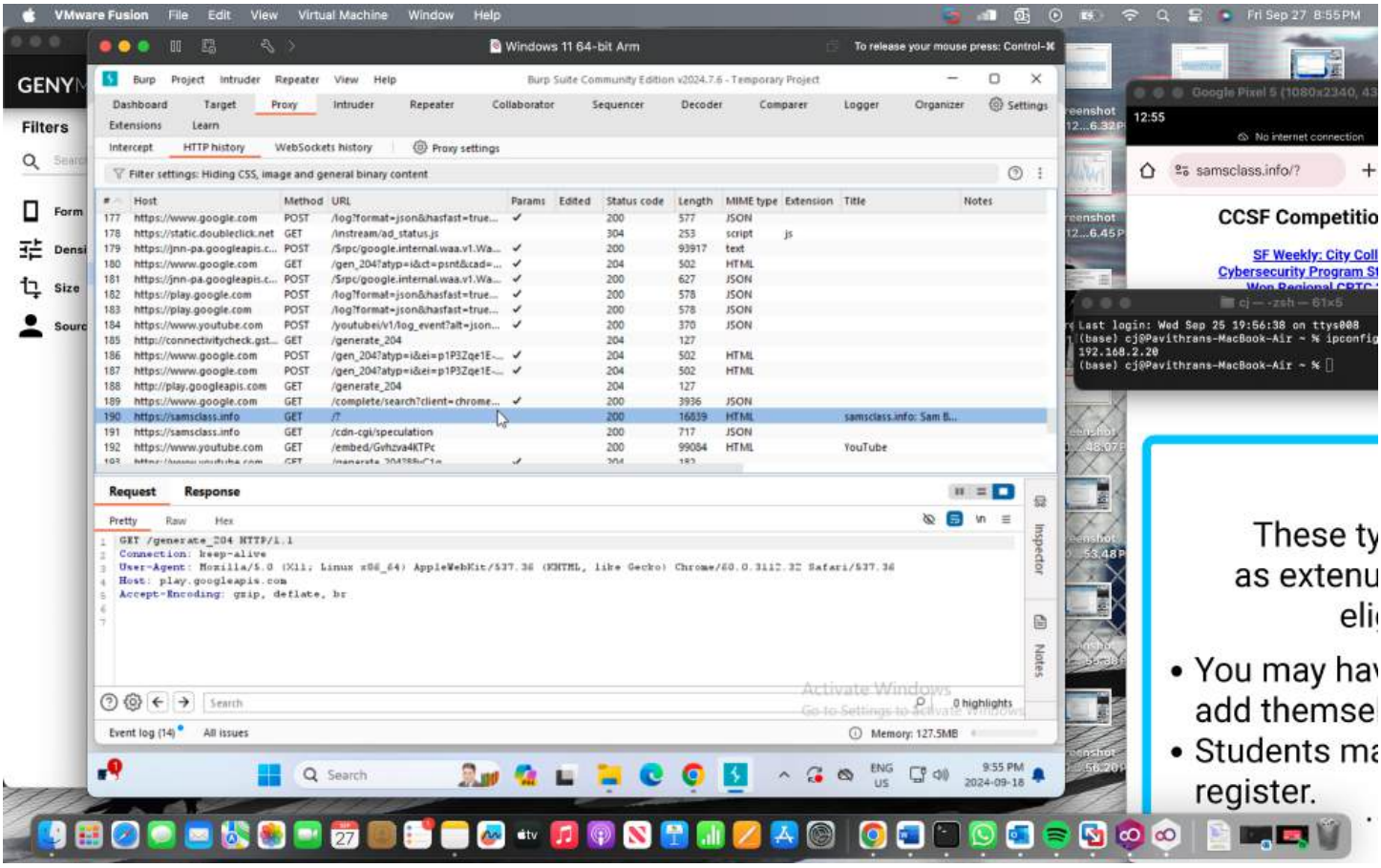


Now im able to open the website on my chroam

15. Step 15: Viewing HTTPS Requests in Burp

In Burp, on the Proxy tab, click the "HTTP history" sub-tab.

Find the line that shows the https://samsclass.info page loading, as shown below.

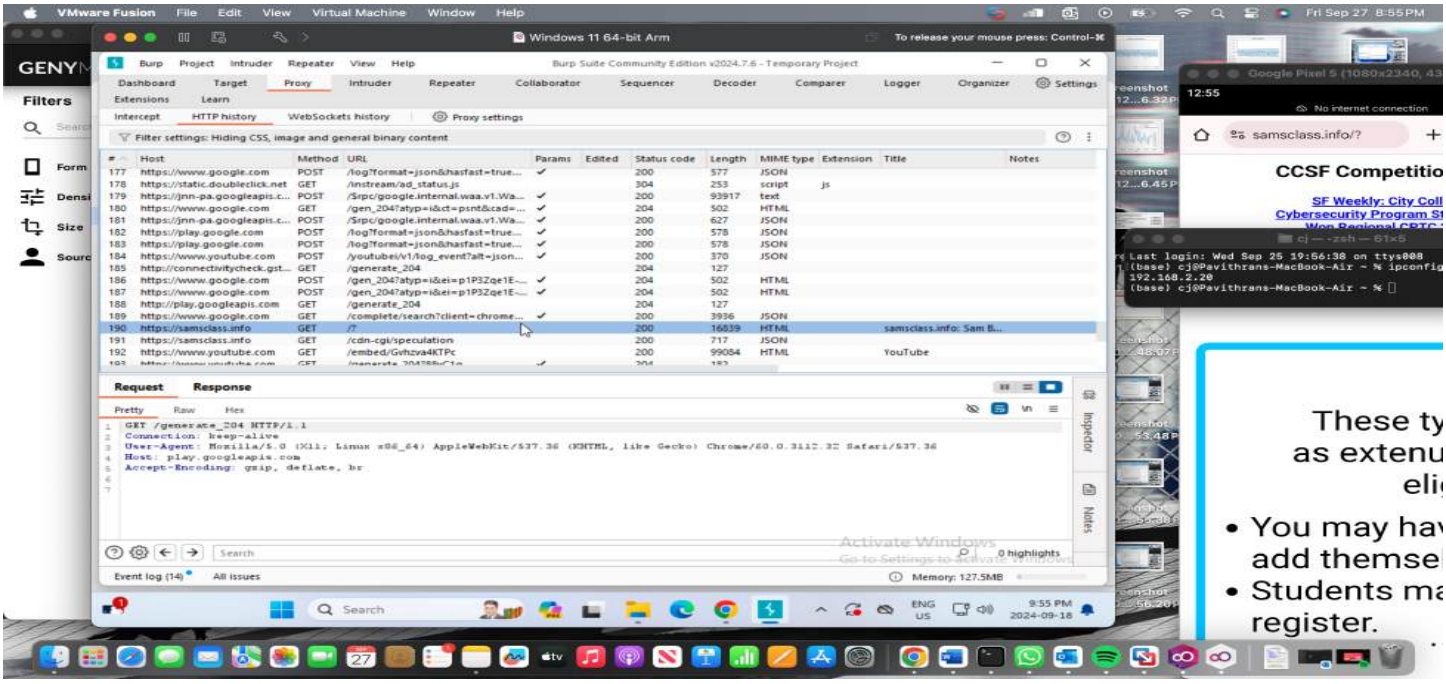


We can see that the website is loaded on our burpsuit.

16. Step 16: Saving a Screen Image

In addition to previous screenshots and explanations, make sure you can see an https:// connection in Burp, as shown above or your own https site.

This screenshot is mandatory in addition to other significant screenshots.



17. Step 17: Adjusting Android to Bypass the Proxy

While Burp is useful, most of the time you want to bypass it so you can get to Google Play.
From the Android home screen, click the circle at the bottom center.
Open Settings.
In Settings, click "Network & internet".
Click Wi-Fi.
Click AndroidWiFi.
Click Advanced.
In the "Network details" screen, at the top right, click the Pencil icon.
In the "Proxy" field, click the down-arrow.
Click None.
Then click Save.