

Lab – 2

Name: Ishan Aakash Patel

Student ID: 146151238

Course: CYT-230

Android & Burp Suite

I am using MobiSec (Linux) and Android x86 for this lab.

Note: I was half way there and I realized that I have to reinstall the android x86 in Read Write format.

Instruction

- Step 1: Install and run Burp Suite on Linux
- Step 2: Configure a proxy listener on the burp Suite
- Step 3: Adjusting Android Networking to Use the Burp Proxy
- Step 4: In the Android emulator browse a test http page (e.g., <http://testfire.net/>) and verify that that the http traffic is intercepted in the Burp Suite successfully.
- Step 5: In the Android emulator browse a secure https page (e.g., <https://senecapolytechnic.ca/>) and indicate that the Android emulator's browser generates an alert or warning.
- Step 6: Export the Burp Suite proxy's digital certificate and install it in the Android emulator.
- Step 7: In the Android emulator browse a secure https page (e.g., <https://senecapolytechnic.ca/>) and this time indicate that the Android emulator's browser does NOT generate any alerts or warnings.
- Step 8: Demonstrate and analyse the intercepted https traffic on the Burp Suite proxy.

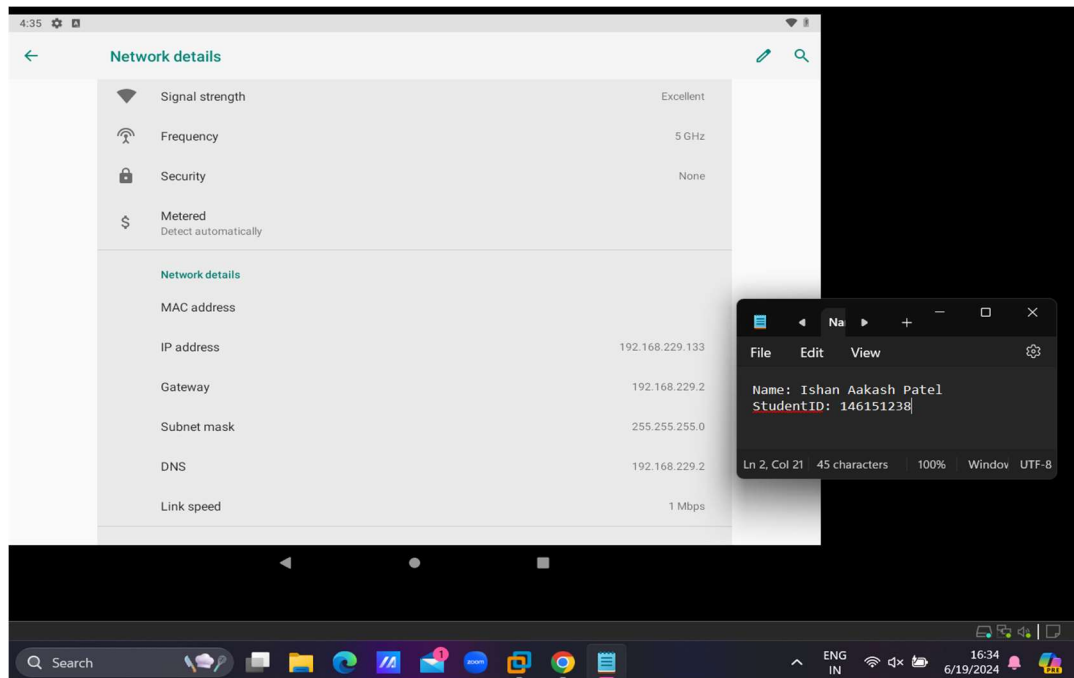


Figure 1 Android x86 IP: 192.168.229.133

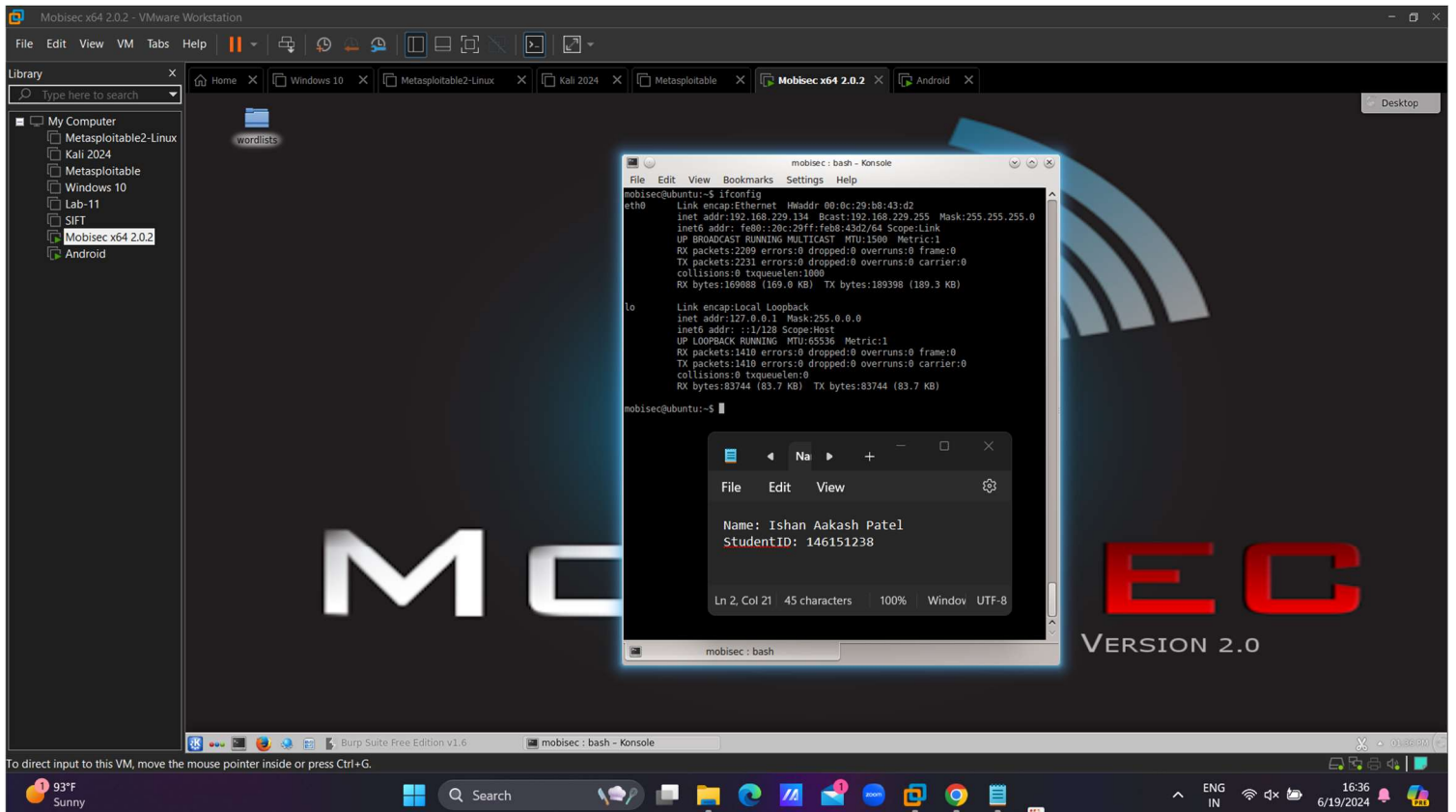


Figure 2 MobiSec IP: 192.168.229.134

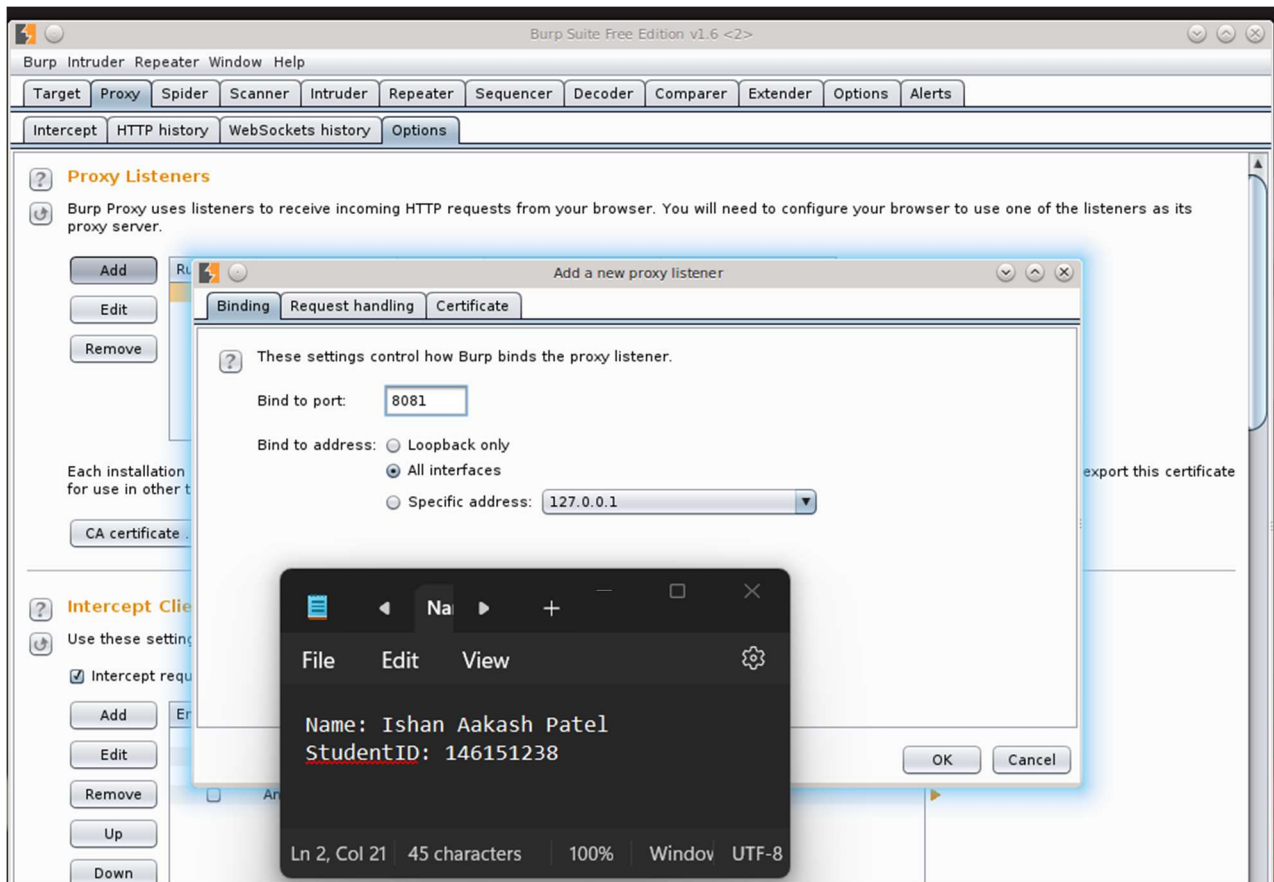


Figure 3 Burpsuite - Adding new Proxy

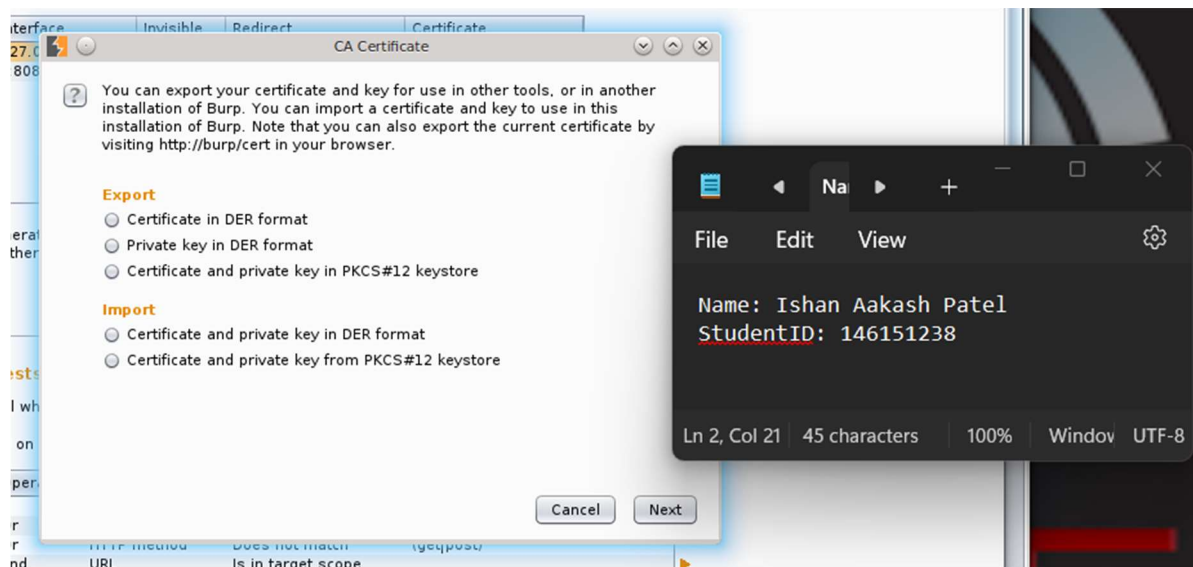


Figure 4 CA certificate (.DER format)

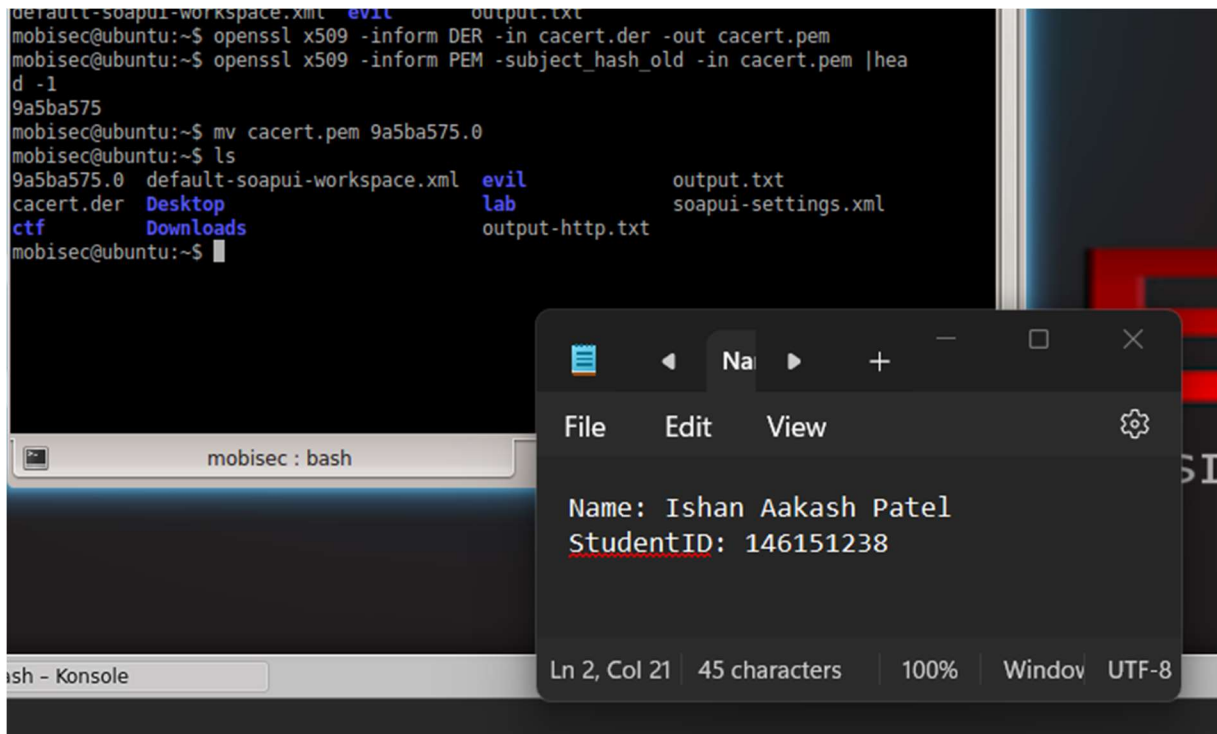


Figure 5 Converting the certificate in .PEM using openssl

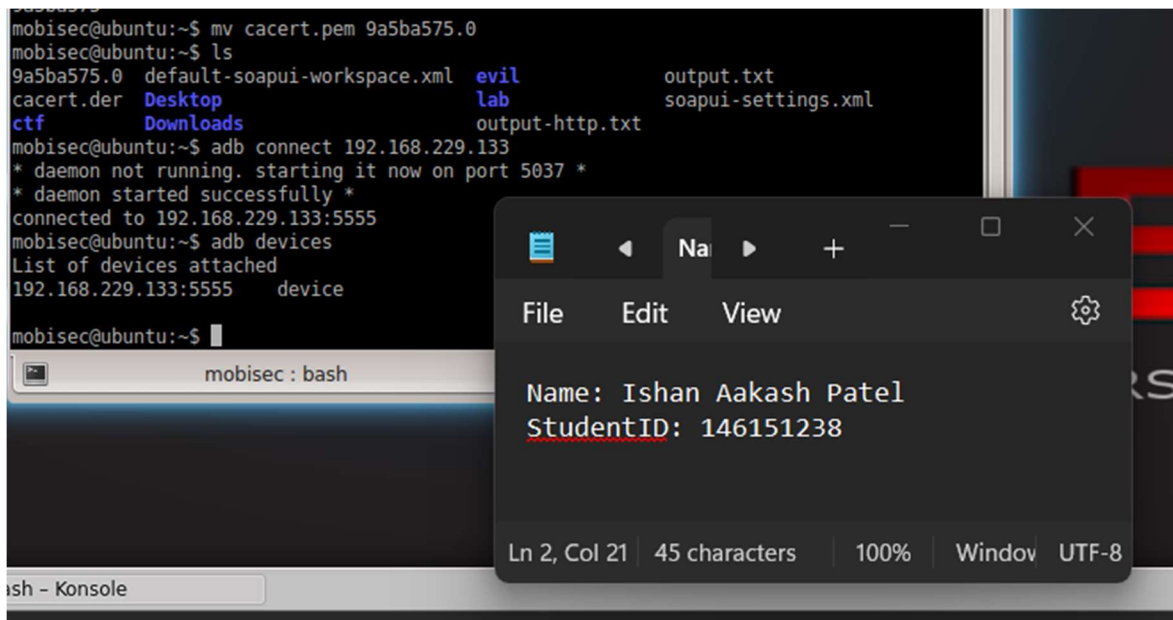


Figure 6 Connect with android x86 using adb tool

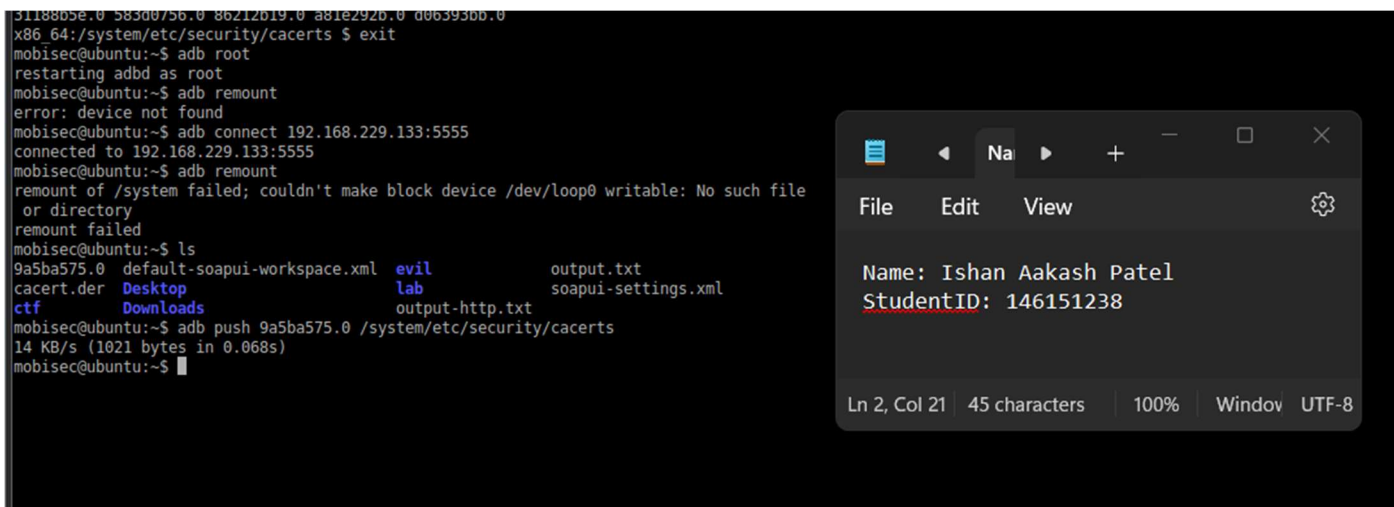


Figure 8 Using push command move the certificate to android

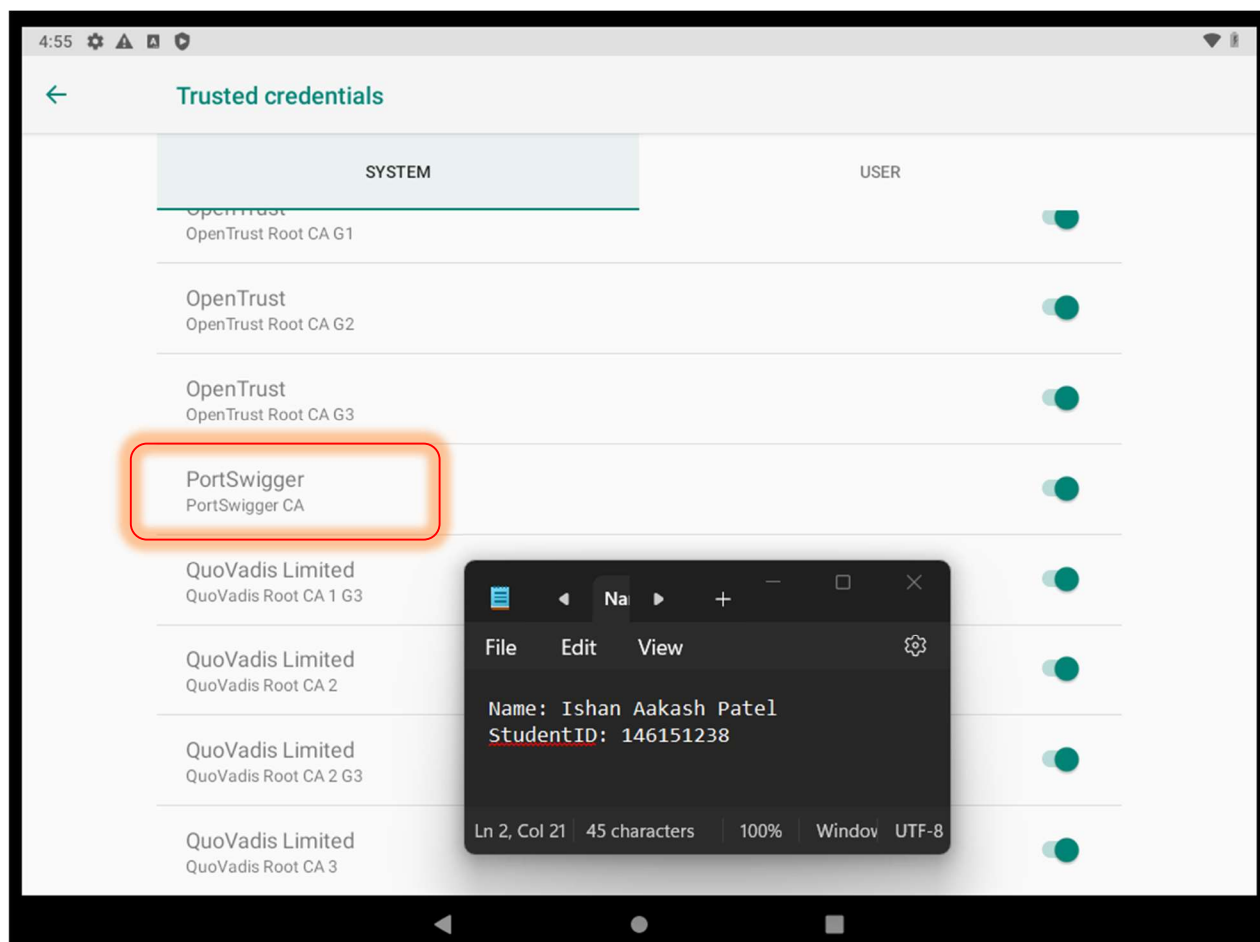


Figure 7.1 Burpsuite certificate installed successfully

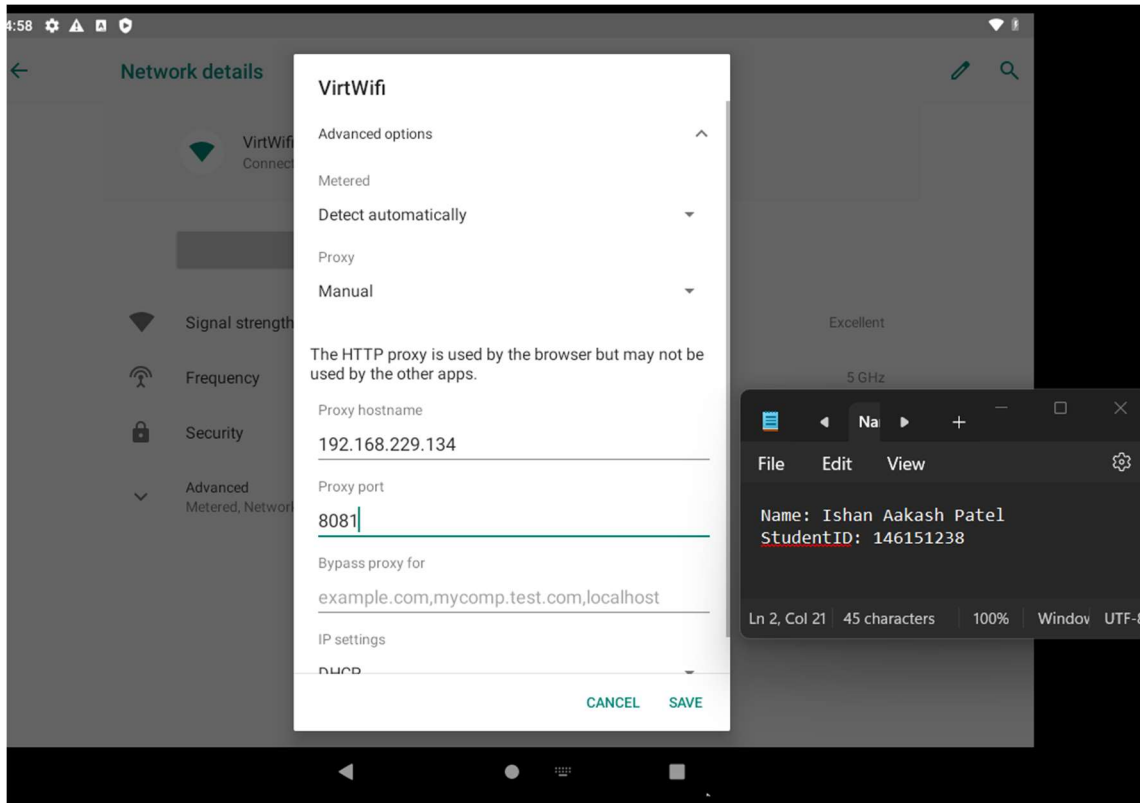


Figure 8 Set the Proxy in WIFI settings

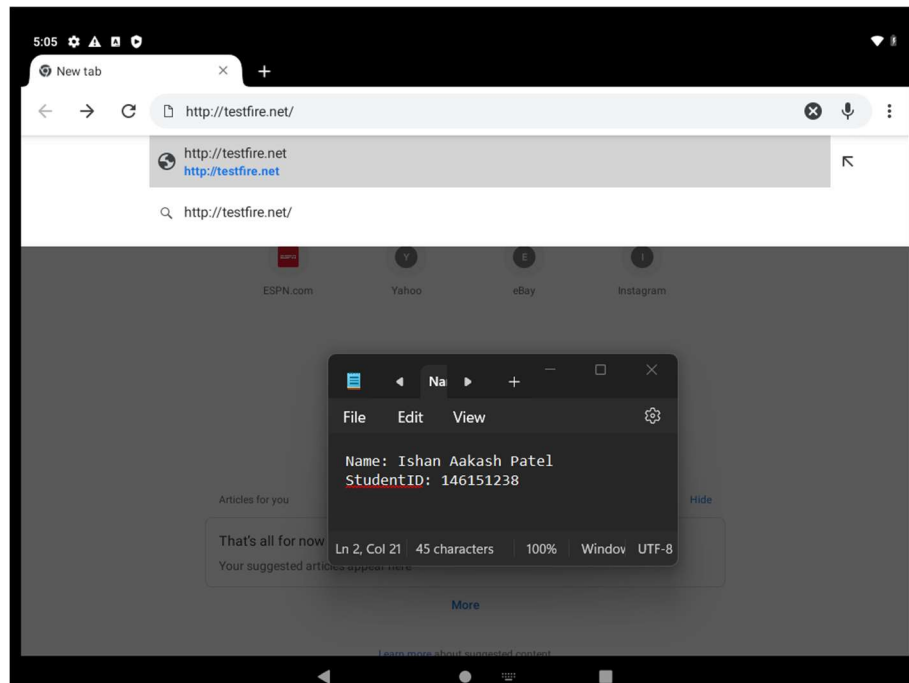


Figure 9 testing http traffic

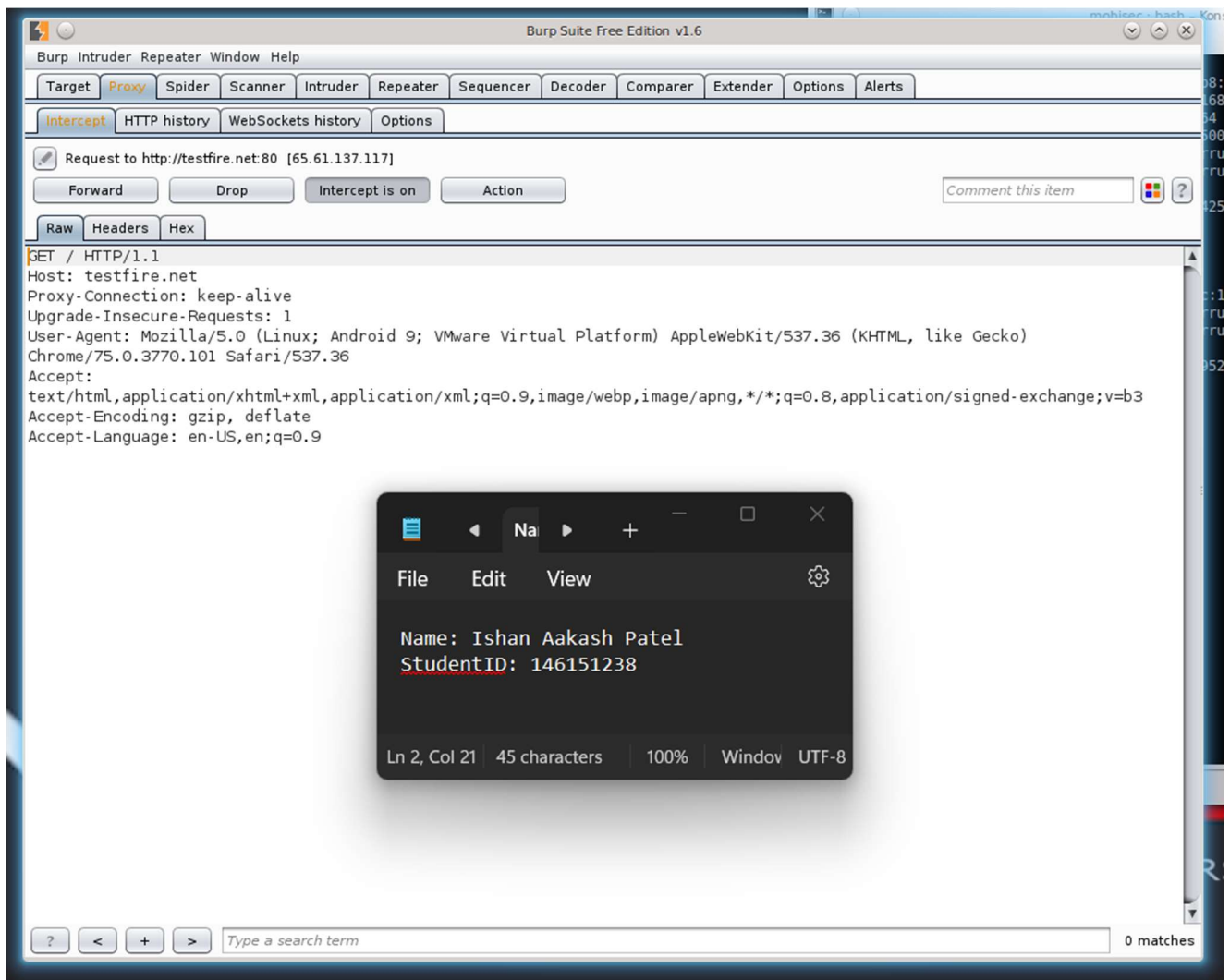
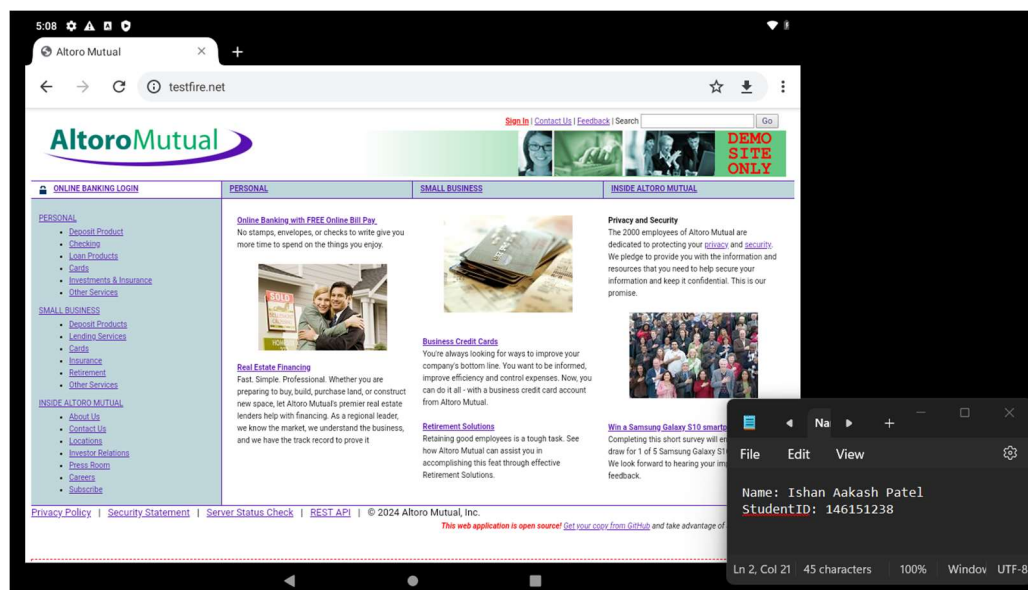


Figure 10 http request successfully intercepted



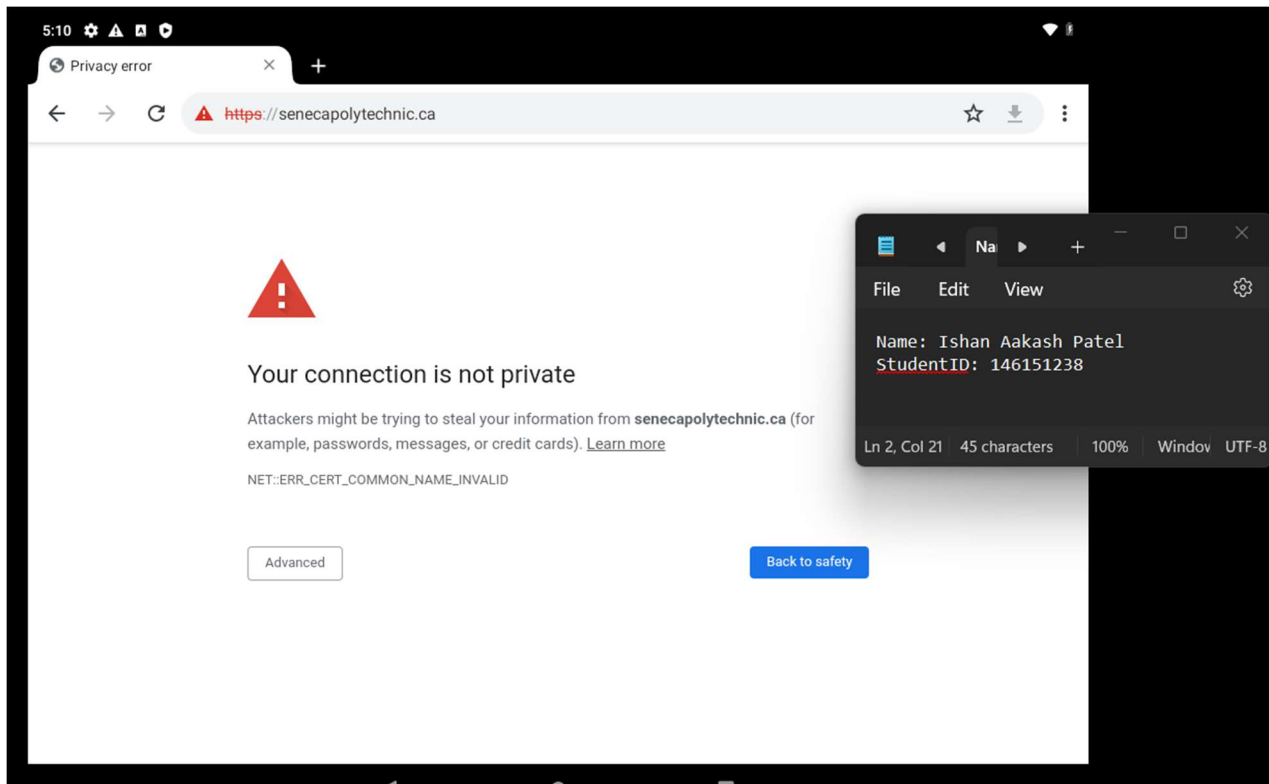
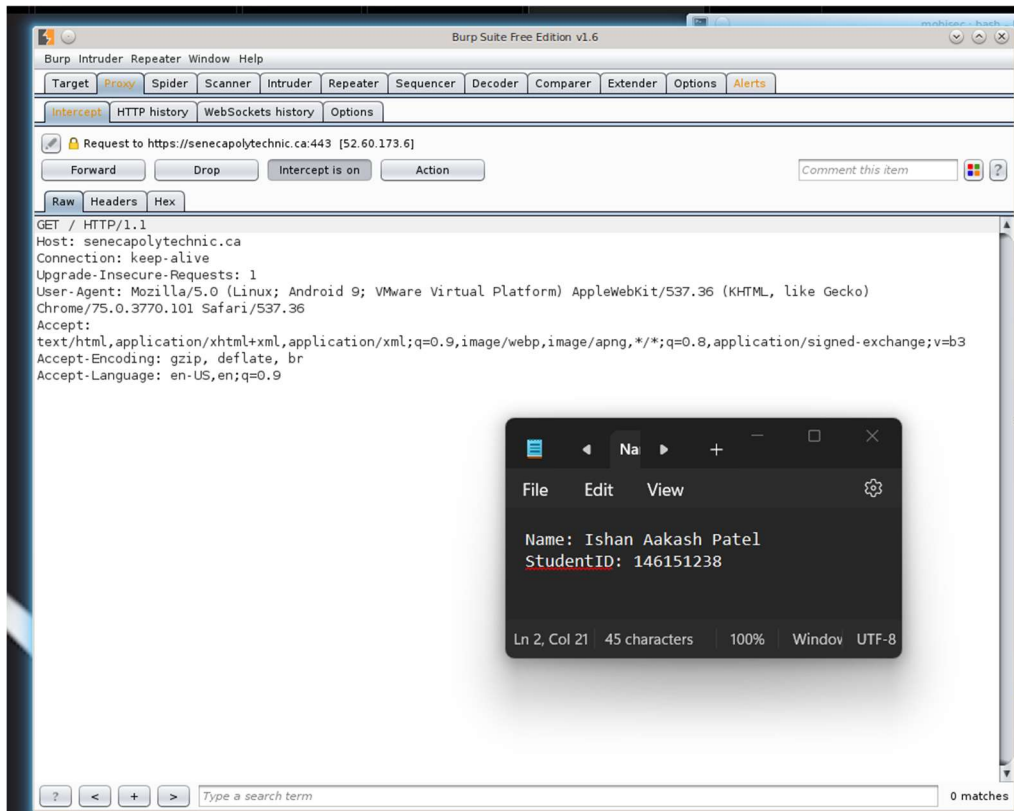


Figure 11 Warning for https request



https request

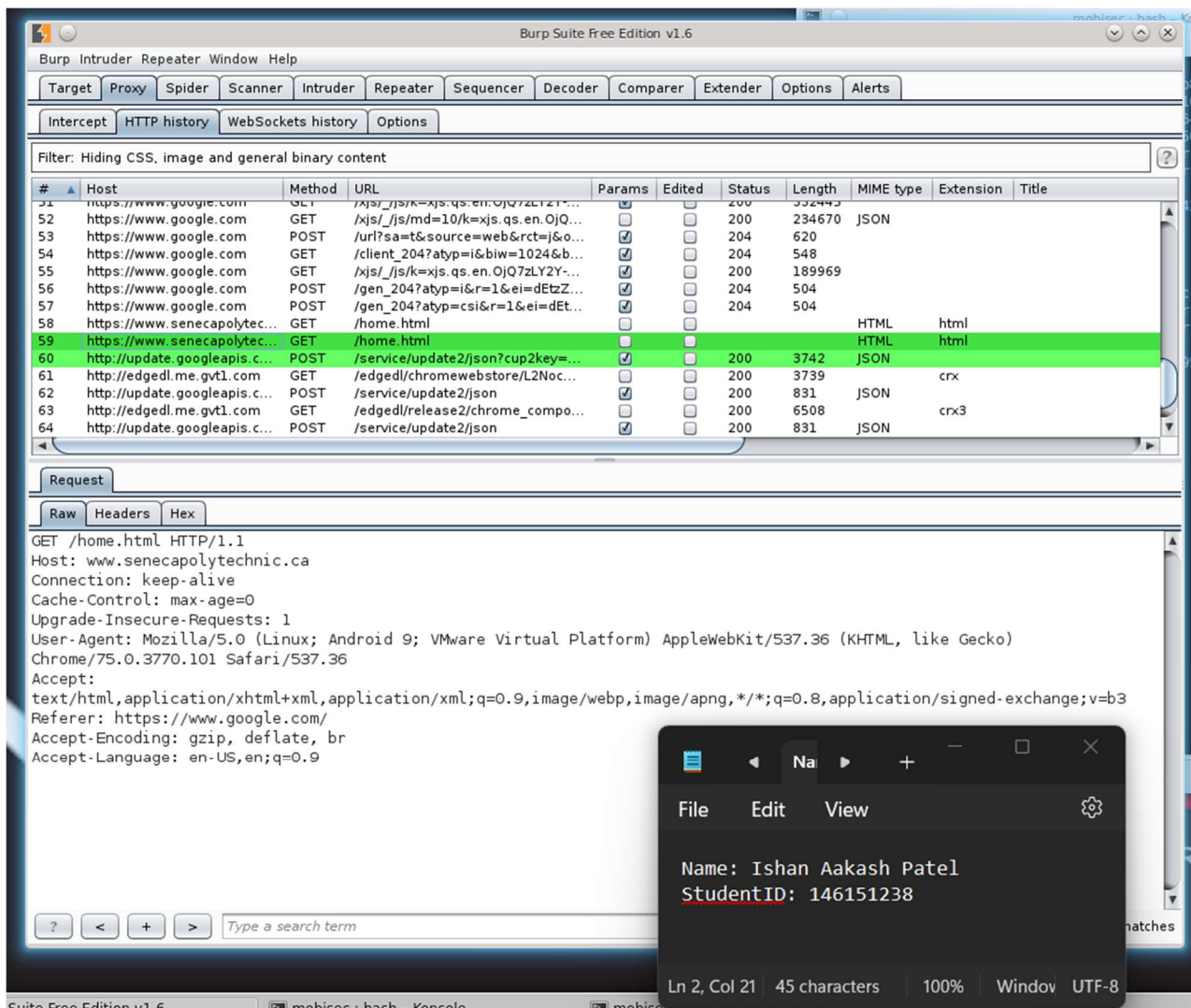


Figure 12 https traffic

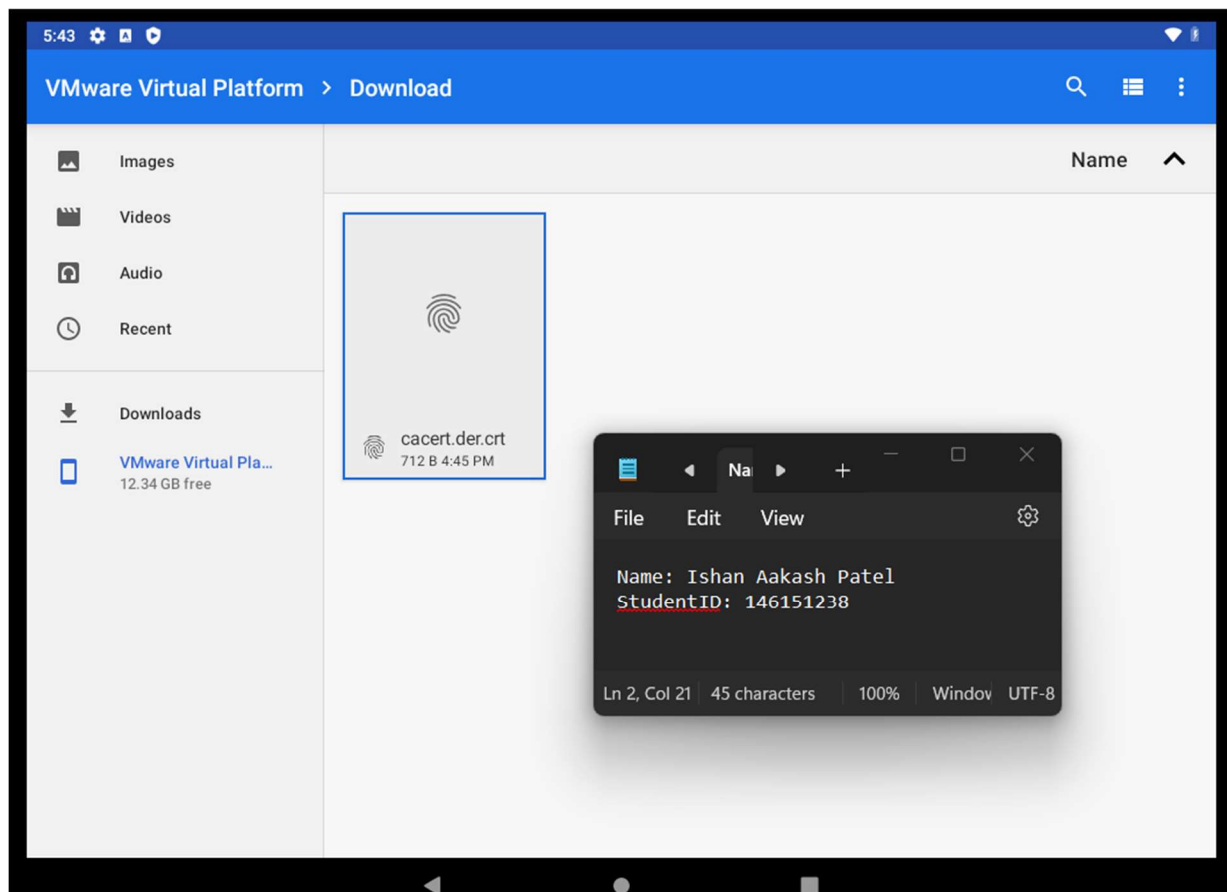


Figure 13 Installing the CA certificate to avoid the warning for https

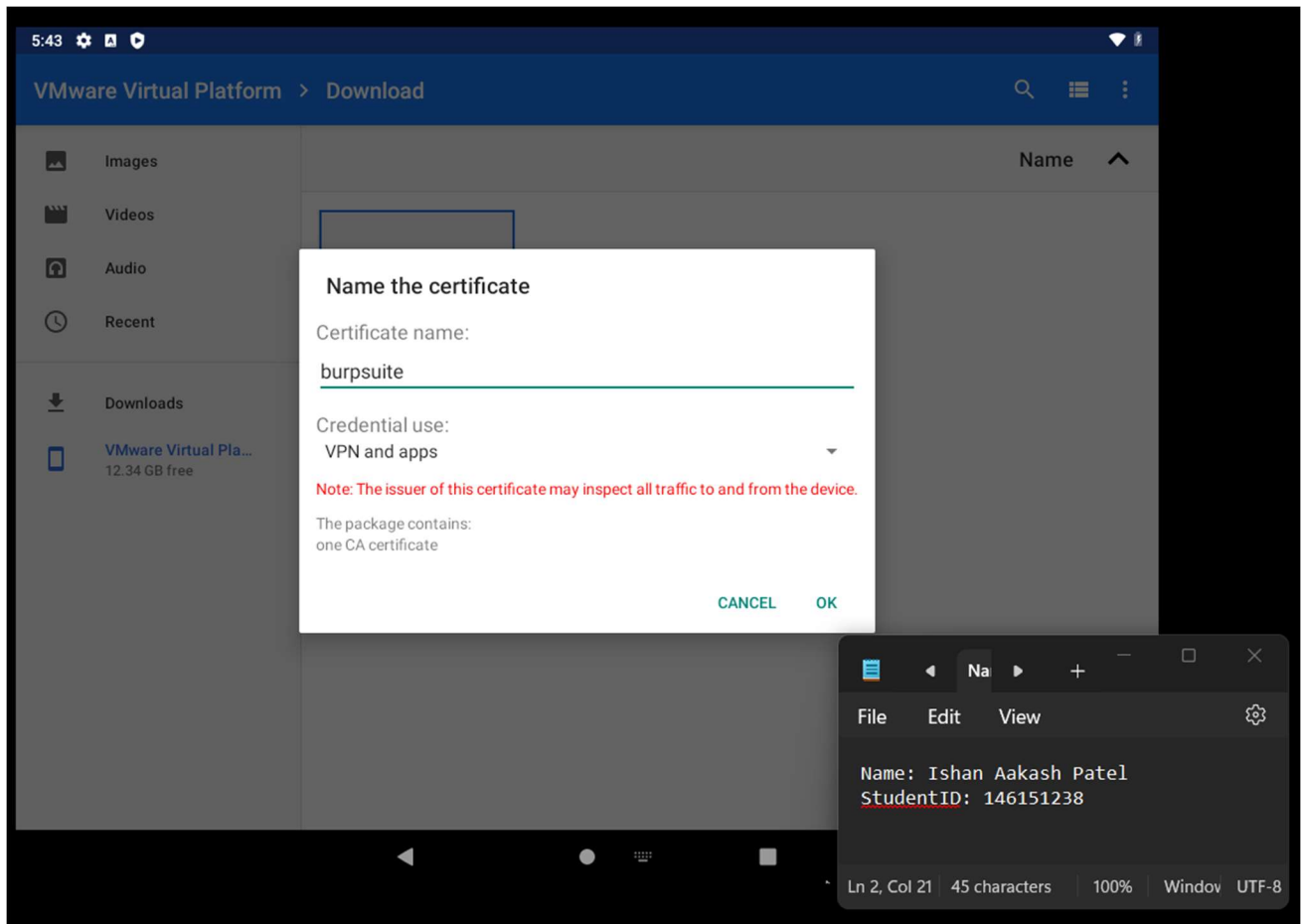


Figure 14 Installing the certificate

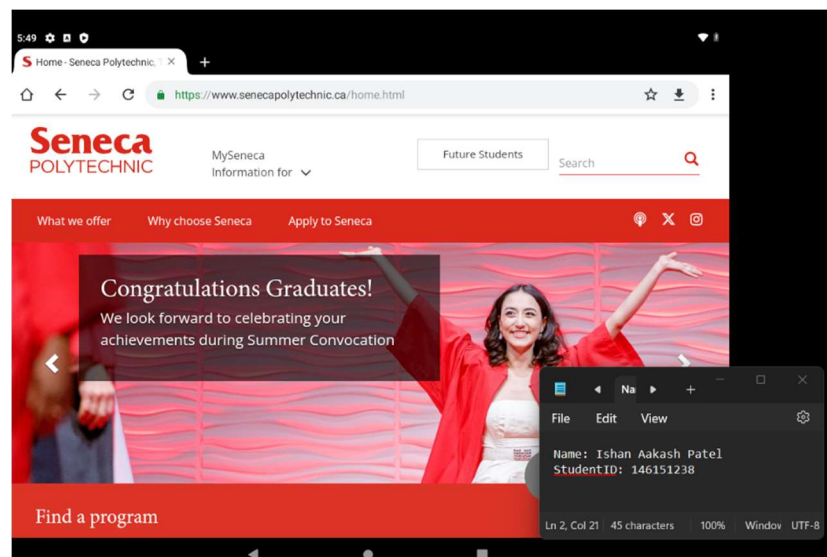


Figure 15 Warning removed

Figure 16 displays a screenshot of the Burp Suite Free Edition v1.6 interface, showing a list of HTTP requests and the details of a selected request.

The top section shows the Burp Suite Free Edition v1.6 window with various tabs (Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Options, Alerts) and a Filter: Hiding CSS, image and general binary content.

The main table lists HTTP requests. The selected request (row 24) is:

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
24	https://m.youtube.com	POST	/youtubei/v1/feedback?prettyPrint=...			200	1204			

The bottom section shows the details of the selected request (POST /youtubei/v1/feedback?prettyPrint=false HTTP/1.1). The request body is:

```
POST /youtubei/v1/feedback?prettyPrint=false HTTP/1.1
Host: m.youtube.com
Connection: keep-alive
Content-Length: 2923
Origin: https://m.youtube.com
X-YouTube-Bootstrap-Logged-In: false
User-Agent: Mozilla/5.0 (Linux; Android 9; VMware Virtual Platform) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/75.0.3770.101 Safari/537.36
Content-Type: application/json
X-YouTube-Client-Name: 2
X-YouTube-Client-Version: 2.20240617.09.00
X-Goog-Visitor-Id: CgtEVEE3eHZmWldYcyjQqc2zBjIKCgJDQRIEGgAgbg%3D%3D
Accept: */*
X-Client-Data: CK6lyQEihLbJAQiitskBCkmdygEI4qjKAQiXrcoBCM2tygEI97TKAQiOusoB
Referer: https://m.youtube.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: YSC=dNSM140DOIY; VISITOR_INFO1_LIVE=DTA7xvfZWxs; VISITOR_PRIVACY_METADATA=CgJDQRIEGgAgbg%3D%3D
PREF=tz=America.New_York
```

A small window in the bottom right corner displays the name "Name: Ishan Aakash Patel" and the "StudentID: 146151238".

Figure 16 Other https requests