**Midterm Task**



**Submitted By**

Hammas Rashid

**Roll No**

SP21-BCS-011

**Submitted To**

Sir Farhan Aadil

**Subject**

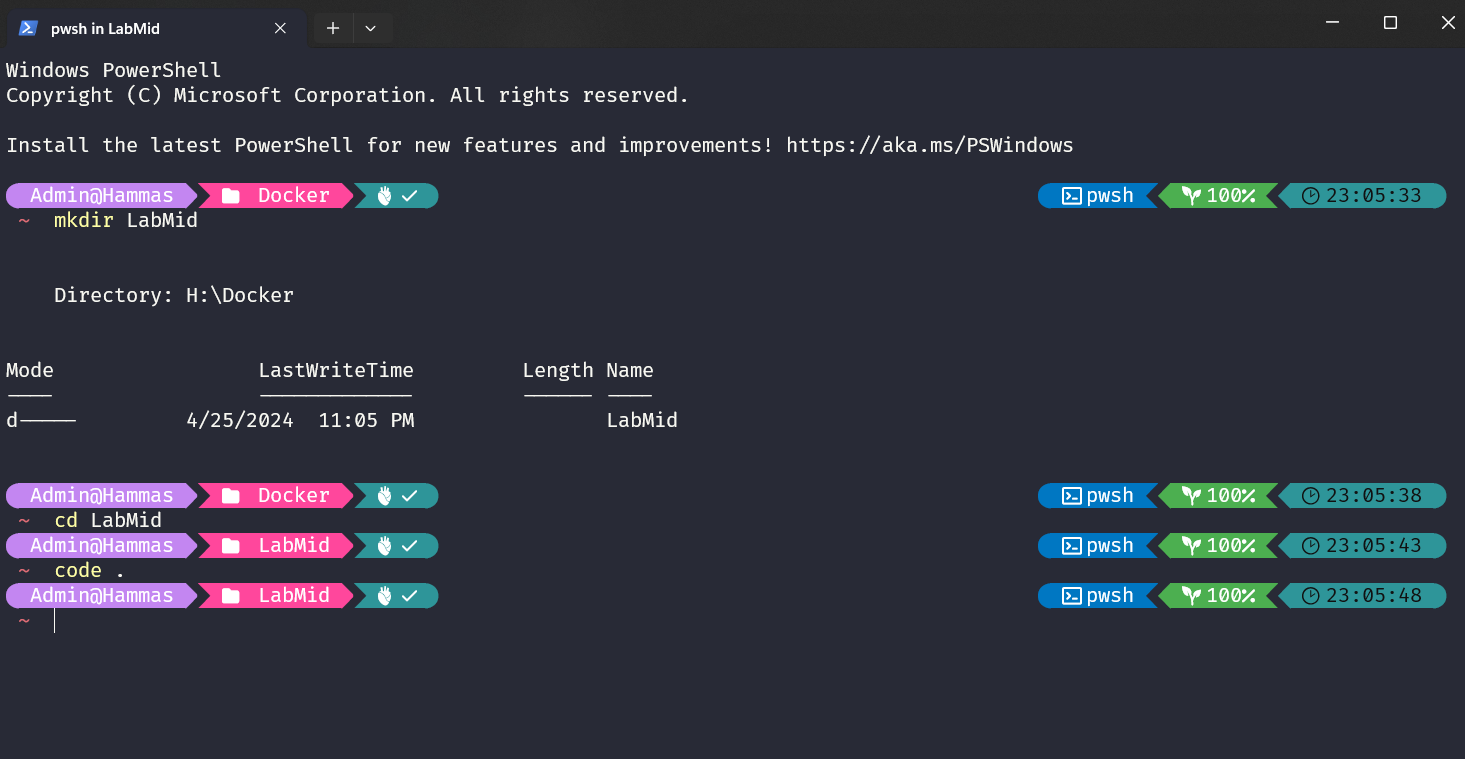
Topics of Computer Science

**Comsats Institute of Information Technology**

**Attock Campus**

**Running Network Analysis Tools:** Isolate network monitoring and analysis tools like Wireshark or tcpdump in containers for on-demand network traffic analysis.

**Step #01:** Creating a working directory.



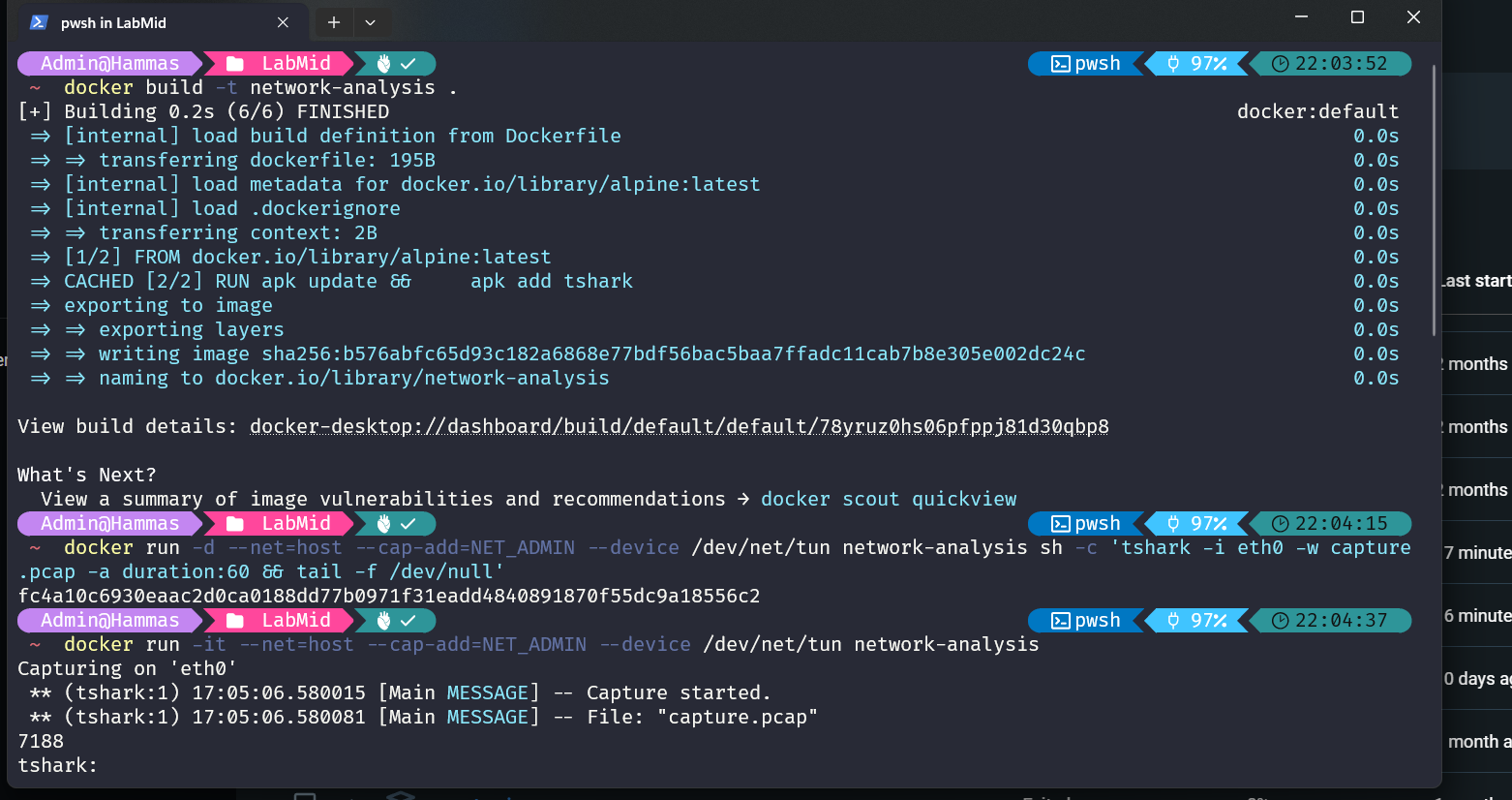
**Step #02:** Creating the *Dockerfile* and downloading *alinpe* imageandinstalling *wireshark,tshark and tcpdump*.

A screenshot of a computer

Description automatically generated

I take duration of 60 seconds, so it will capture packets of 60 seconds only.

**Step #03:** Building image and then run 2 containers of that image.

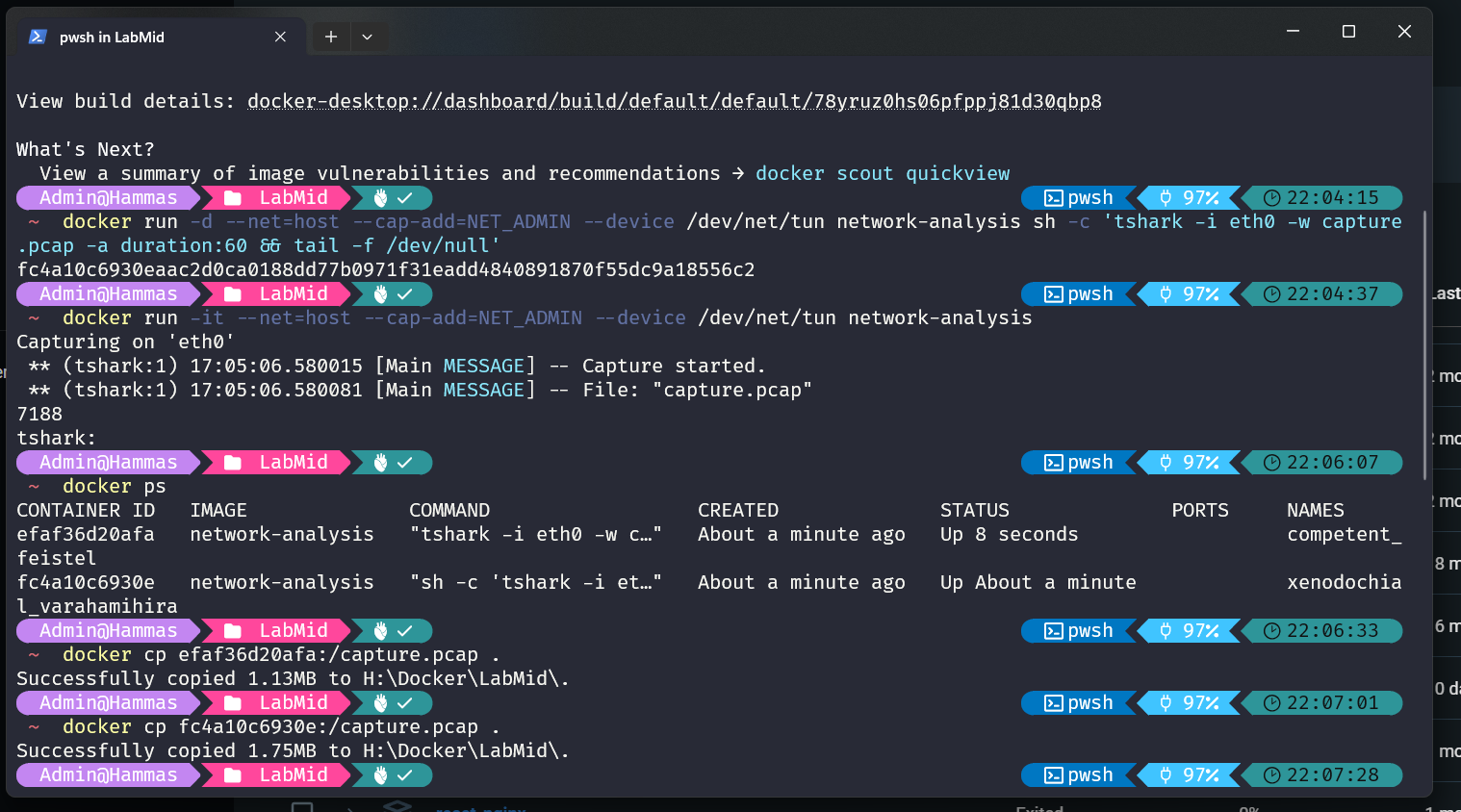


**Step #04:** Running containers are showing in Docker Desktop.

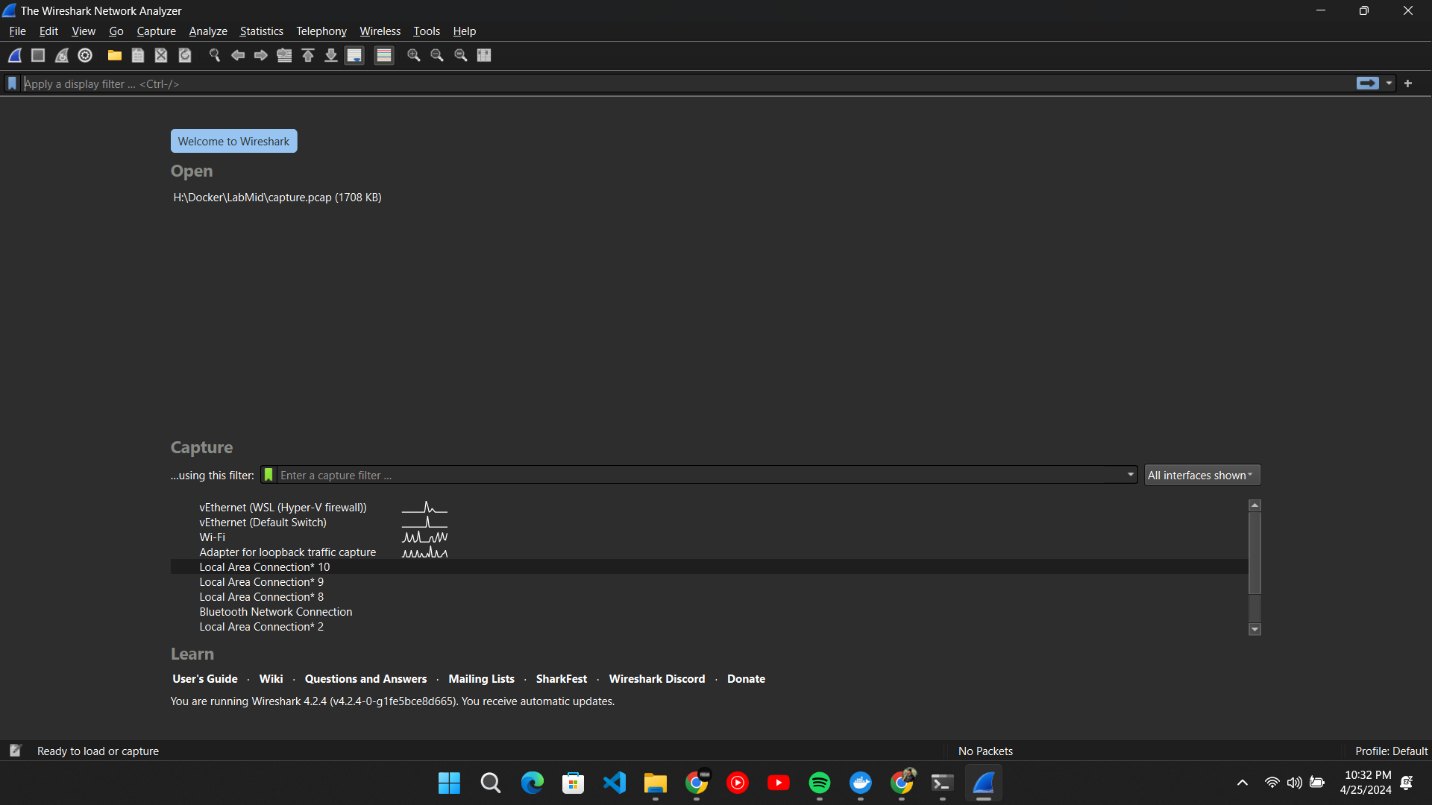
A screenshot of a computer

Description automatically generated

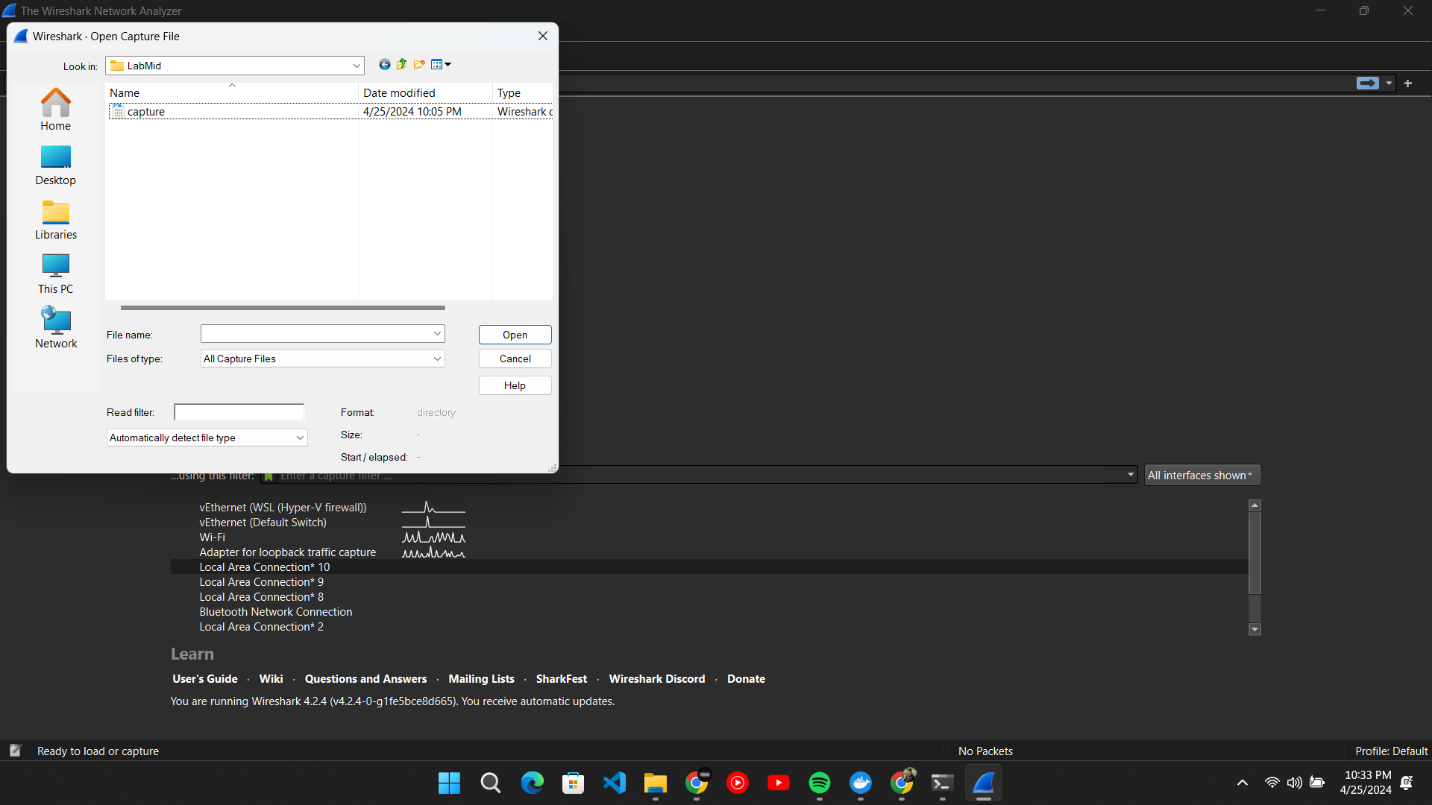
**Step #05:** Copy the capture.pacp file from the container to the path in my Dockerfile directory.



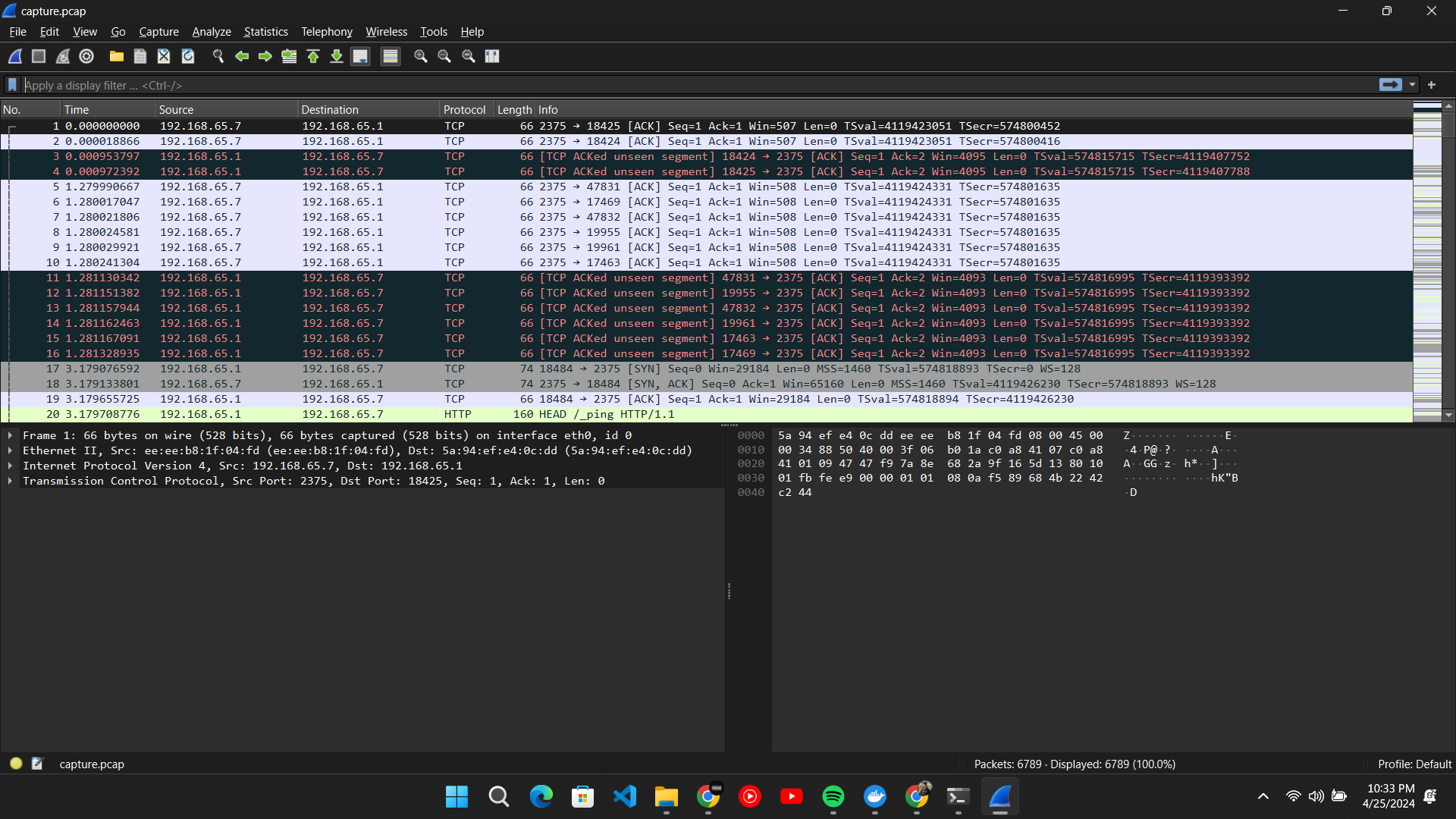
**Step #06:** Opens the Wireshark Desktop App.



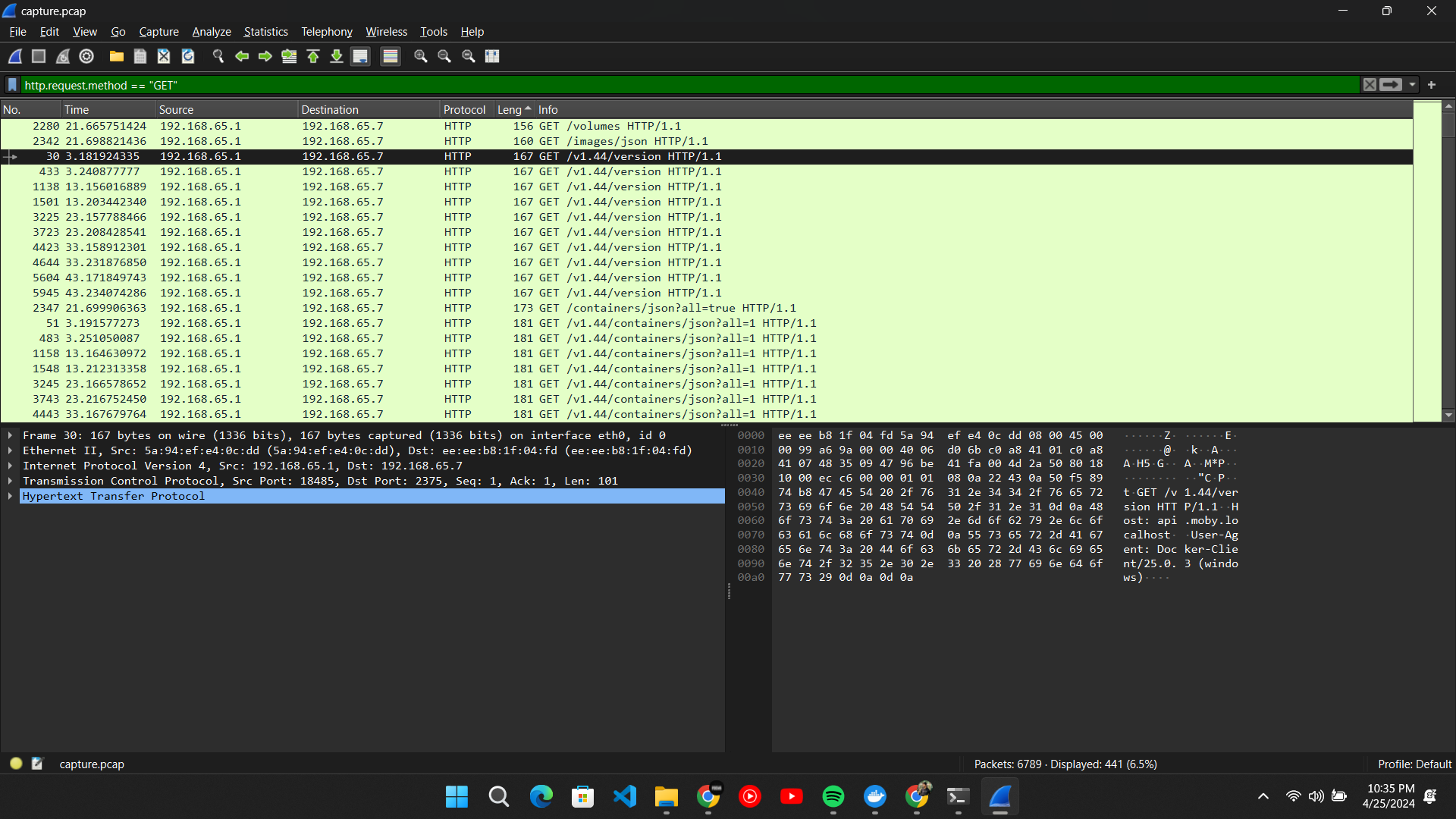
**Step #07:** Opens the saved capture.pacp file in wireshark to analyze.



**Step #08:** Displays all the captured packets.



**Step #09:** Filter all those packets where protocol is HTTP and http method is GET.



**Step #10:** Filter all those packets where protocol is HTTP and http method is POST.

