Worcester Polytechnic Institute
Department of Computer Science

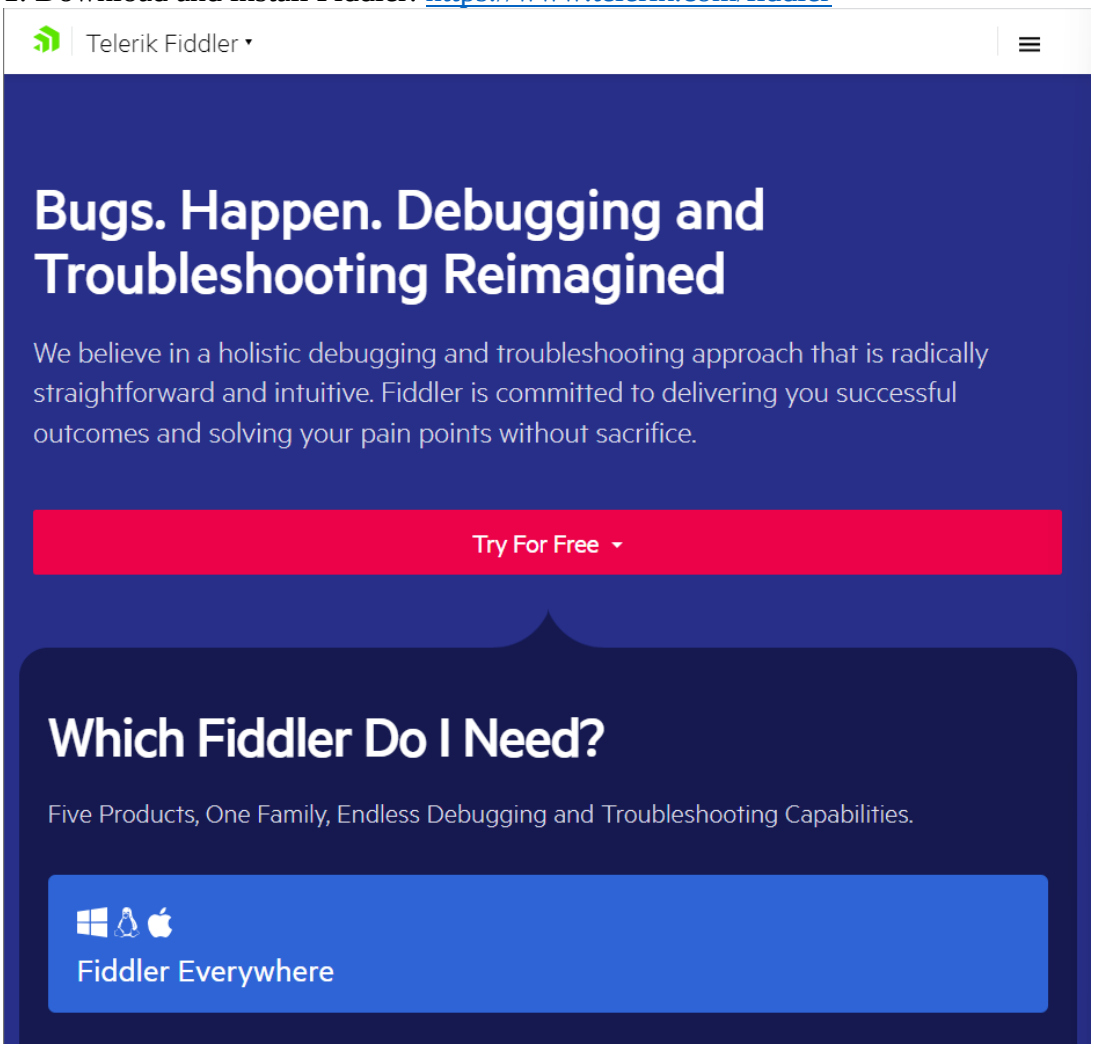
Module 1: Network Traffic Analysis

Objectives

- Use Fiddler to catch the traffic flow.
- Use Fiddler to decrypt the traffic and analyze user activities (such as login, sending messages).

Software Preparation

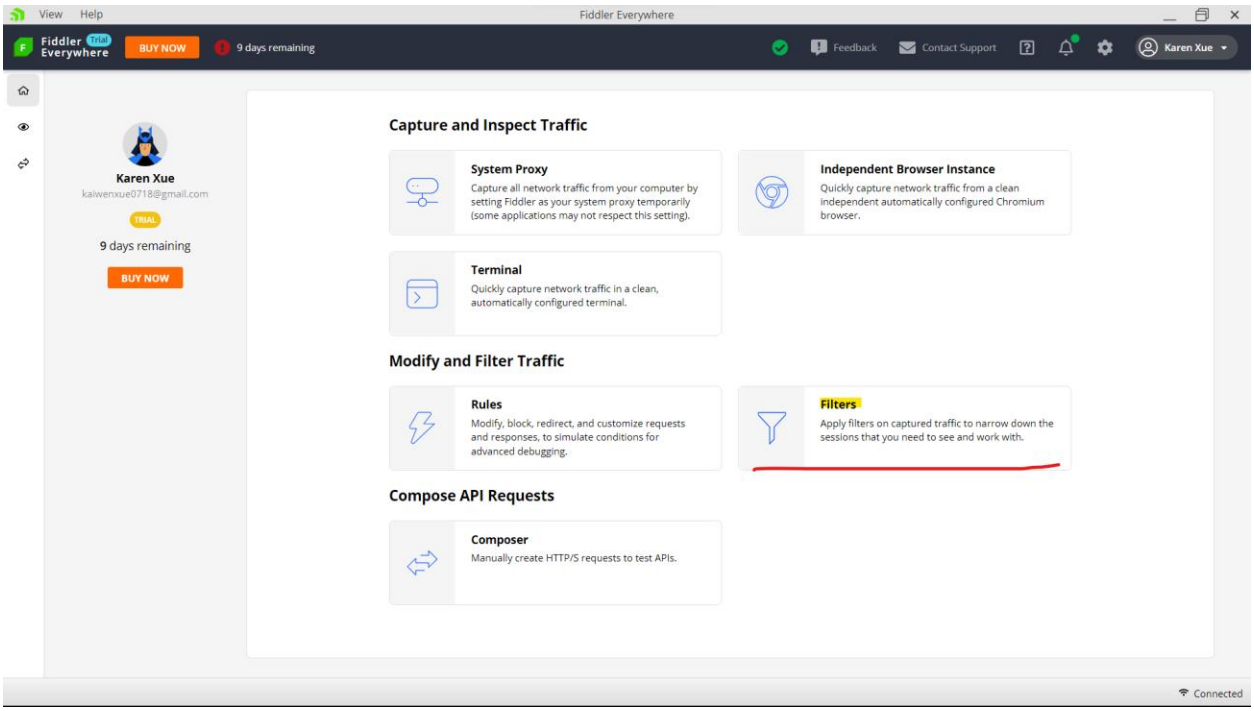
1. Download and install Fiddler: https://www.telerik.com/fiddler



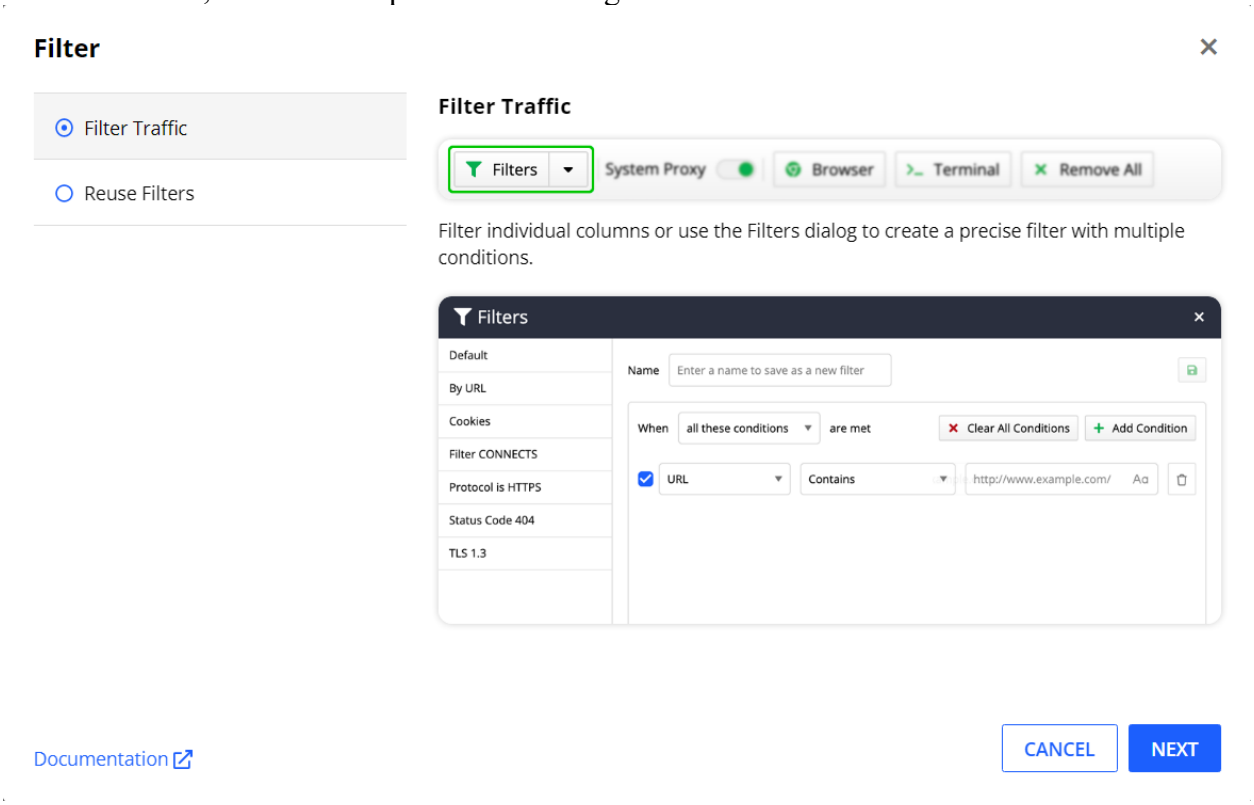
Please note: The Fiddler free trial only lasts for 10 days.

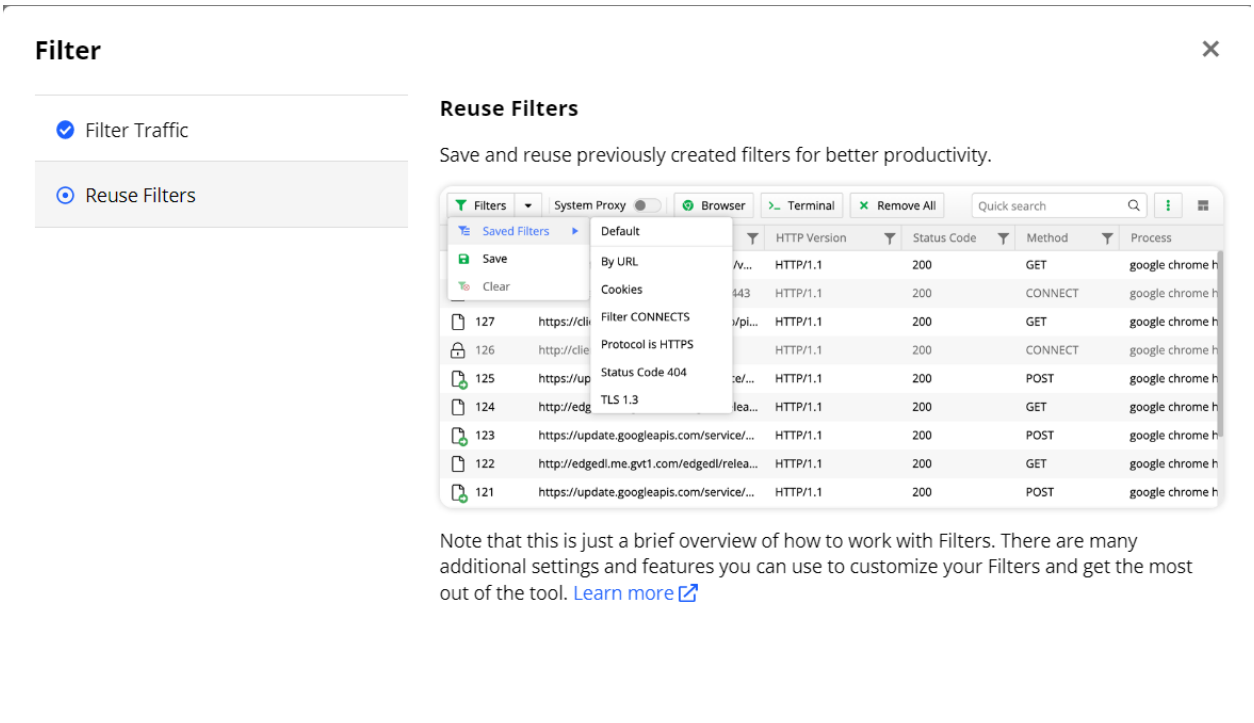
Part1. Use Fiddler to catch traffic flow.

2. Open Fiddler, then choose “Filters”.

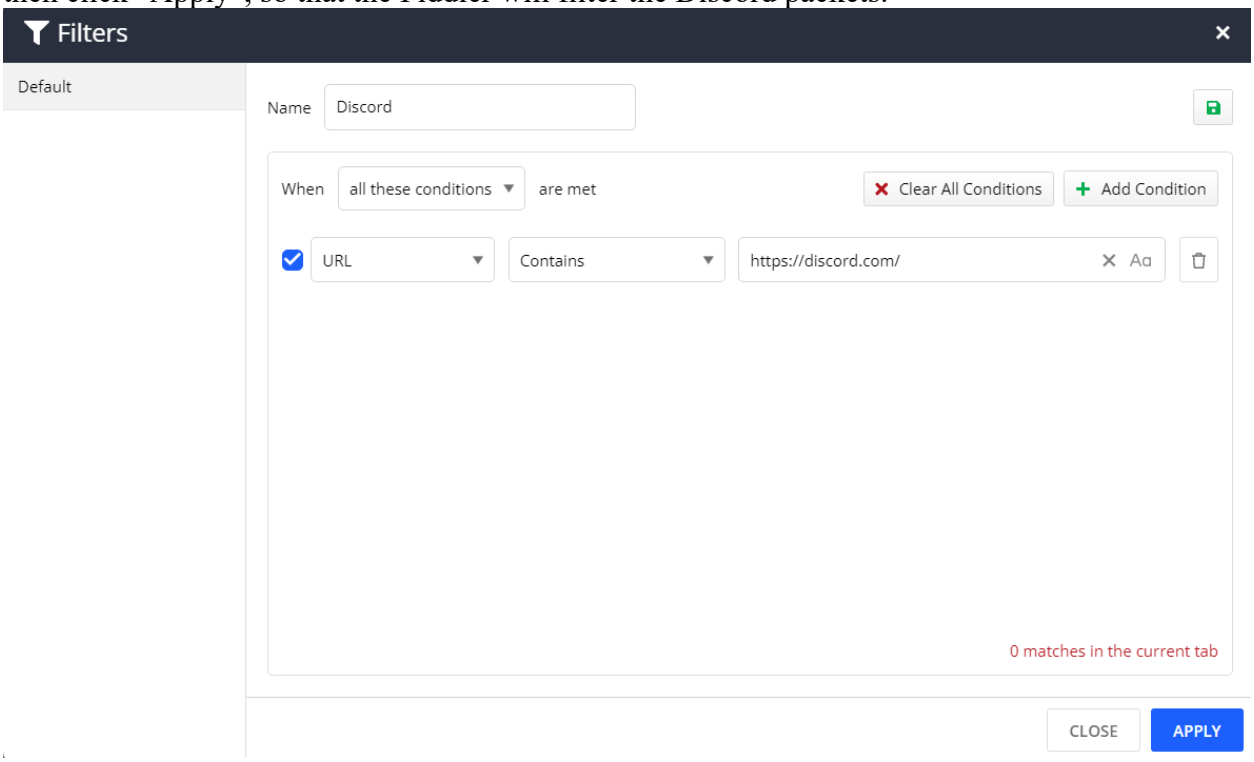


3. Click “Next”, then click “Open Filters Dialog”.

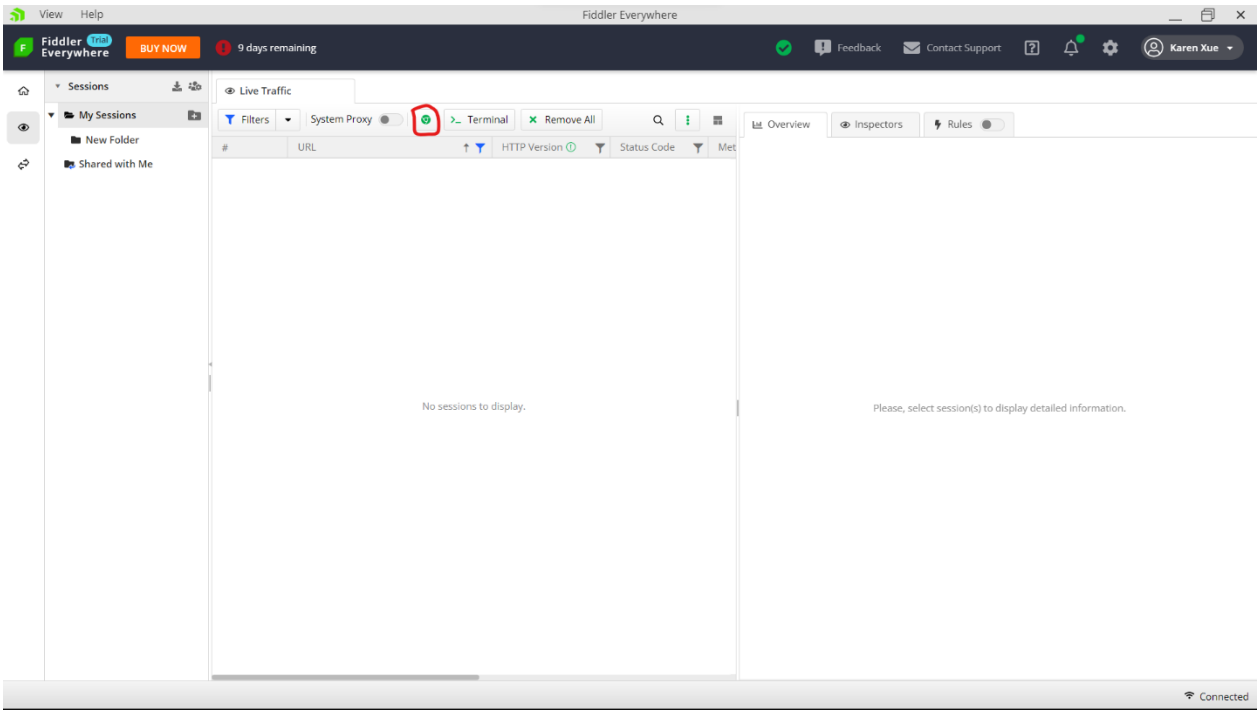




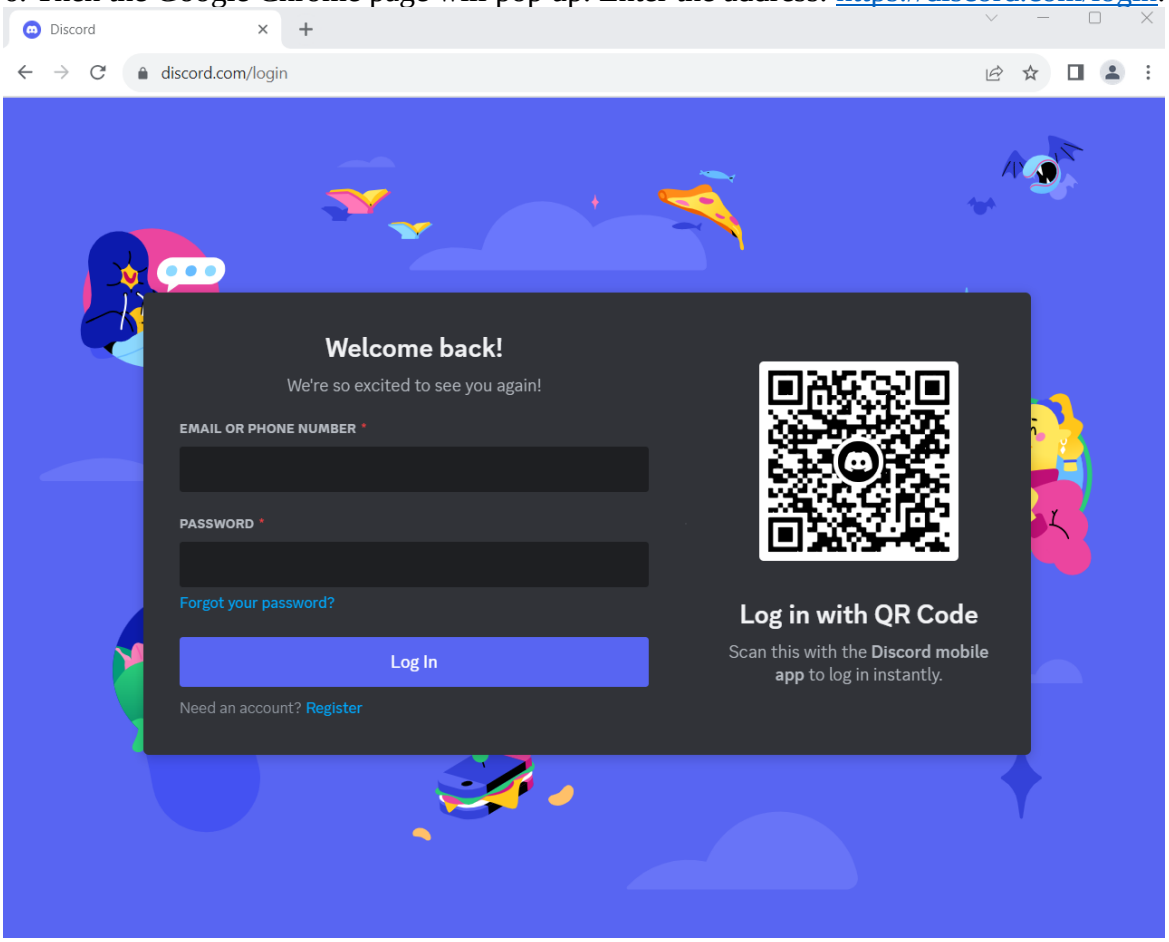
4. Name this filter as “Discord”, and for the URL, enter the address https://discord.com/, and then click “Apply”, so that the Fiddler will filter the Discord packets.



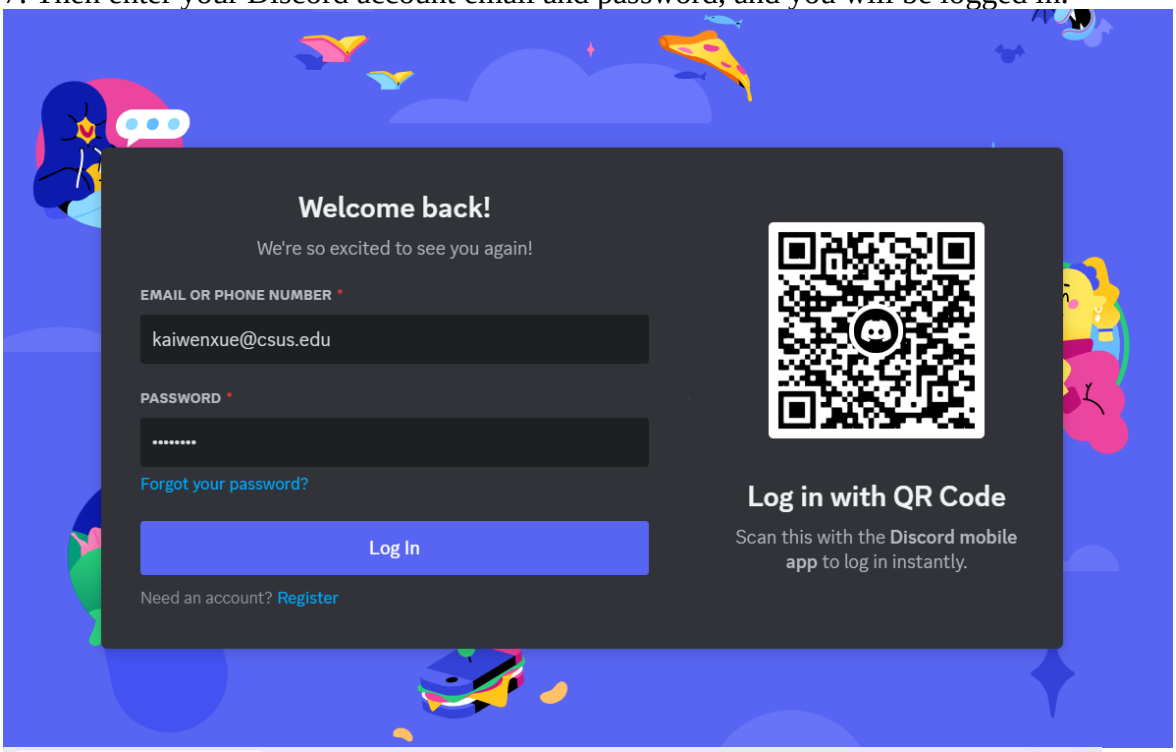
5. After opening the panel, click the Google Chrome icon. As shown on the screenshot.

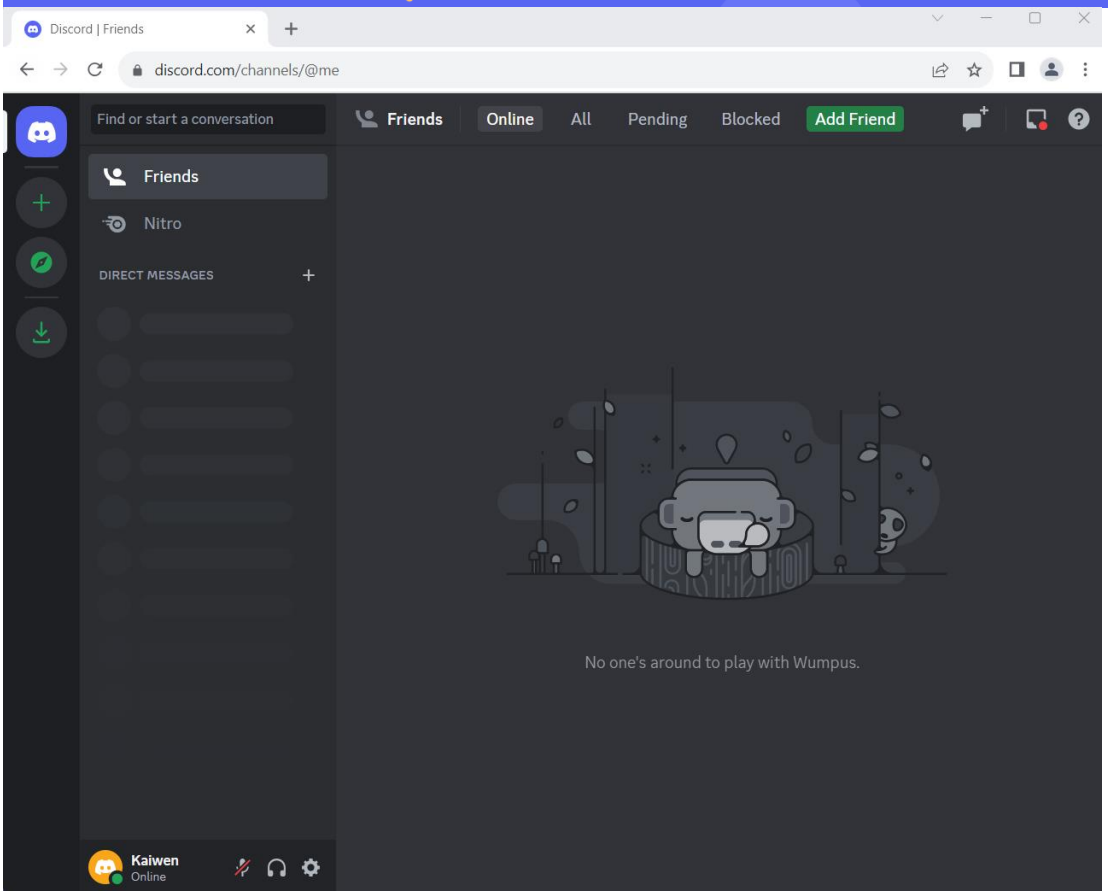


6. Then the Google Chrome page will pop up. Enter the address: https://discord.com/login.

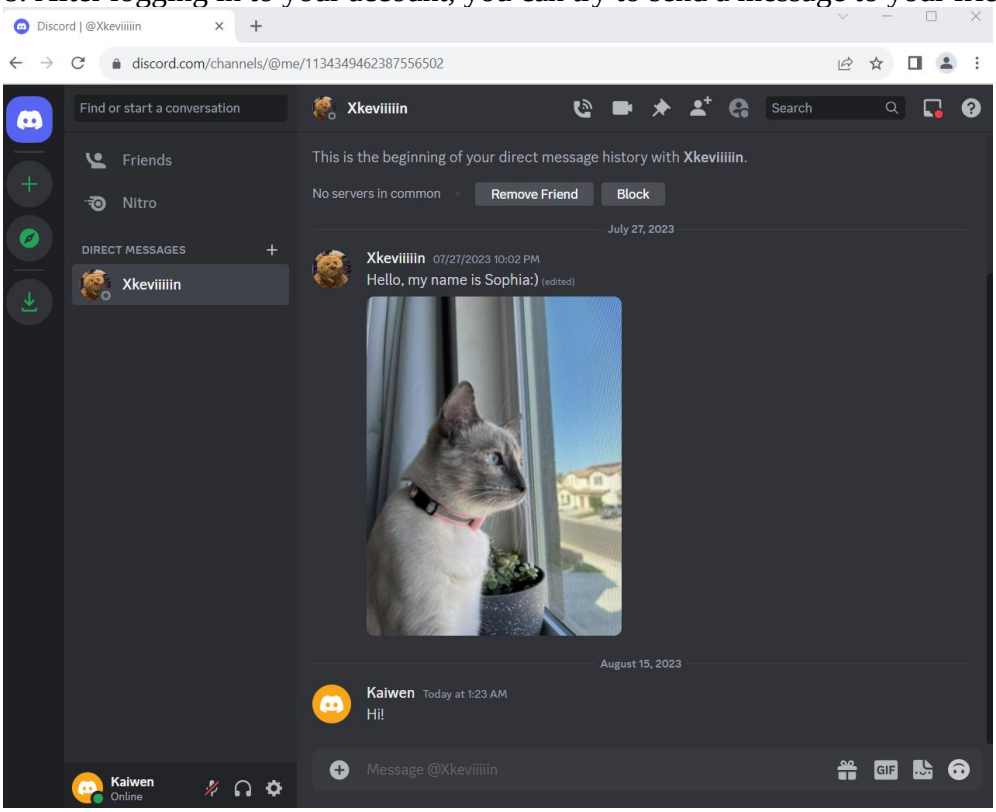


7. Then enter your Discord account email and password, and you will be logged in.

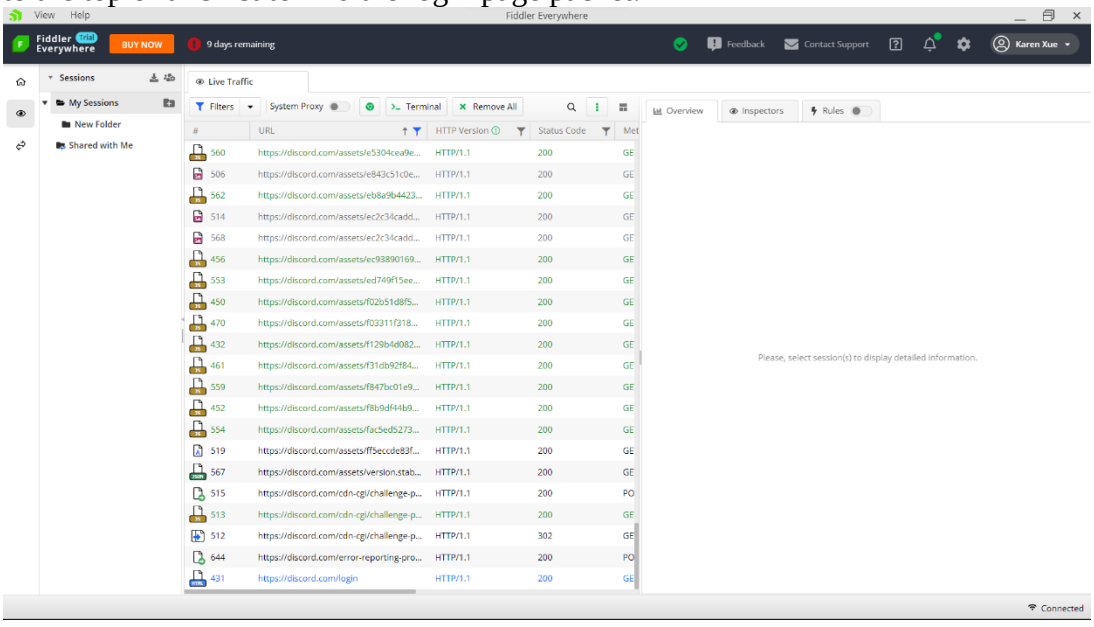


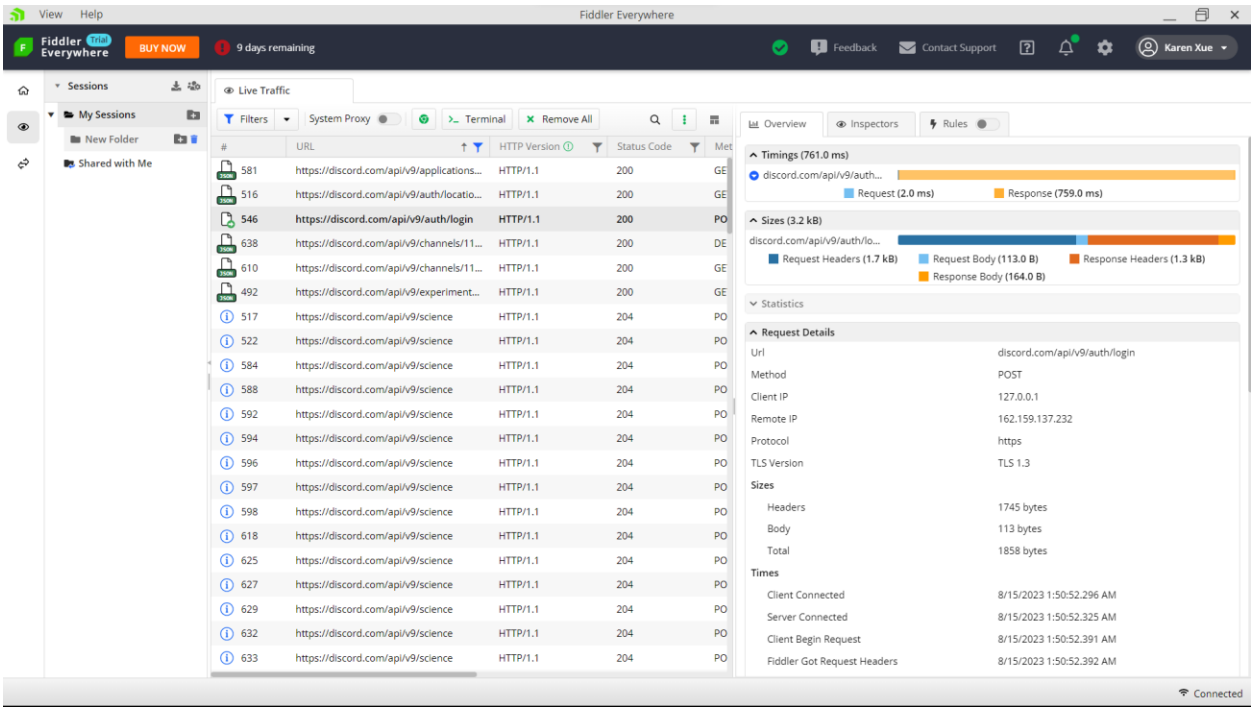


8. After logging in to your account, you can try to send a message to your friend.

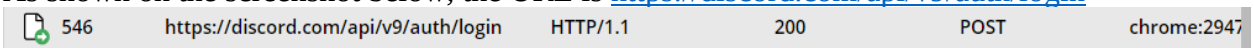


9. Go back to Fiddler, there are many packets as shown on the screenshot. You need to go back to the top of this list to find the login page packet.

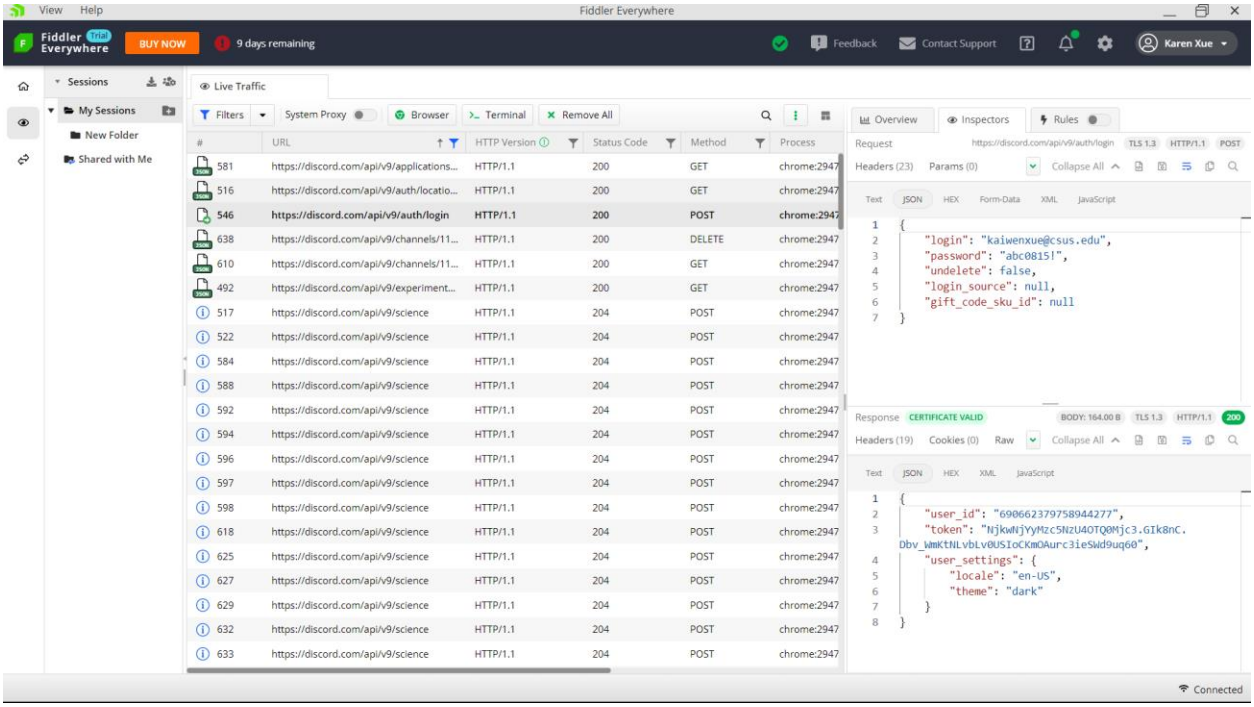


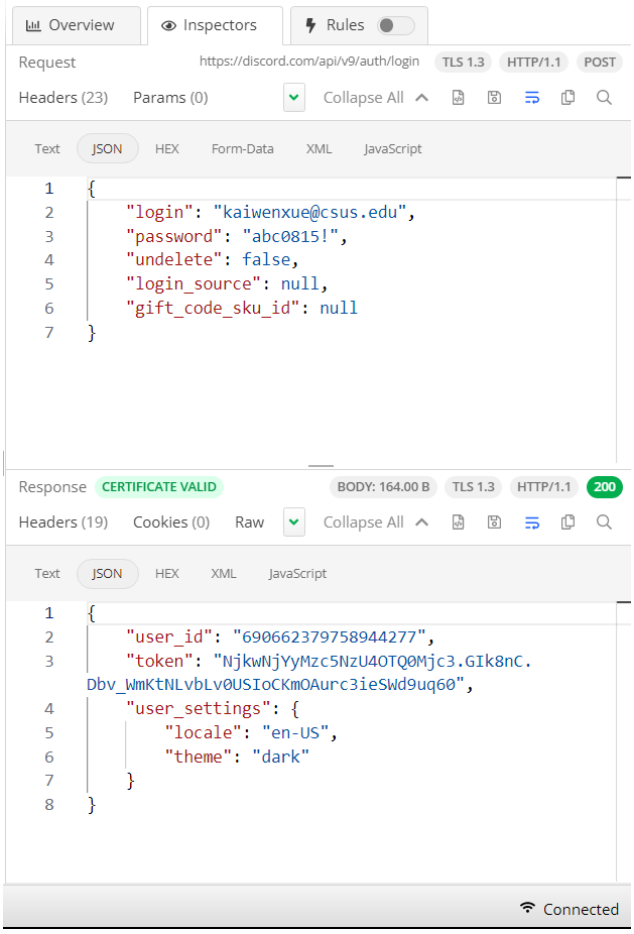


As shown on the screenshot below, the URL is https://discord.com/api/v9/auth/login

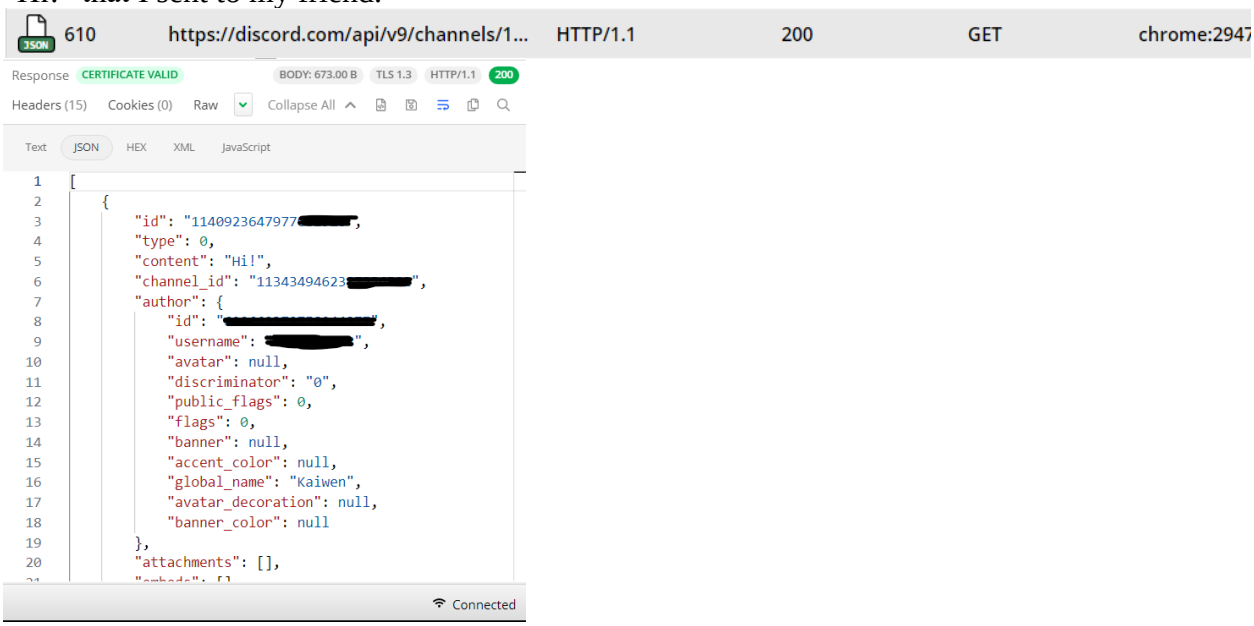


10. And then on the right window, choose the “Inspectors”, and you can see the login information.





11. And then find some packets with the “GET” method and click these packets to view the information. As shown in the screenshot, you can see the chat that you sent on step 8.
For example, for this lab, the packet contains the message is packet 610. And the message is the “Hi!” that I sent to my friend.



12. After analyzing the packets, you can click the “Remove All” to close all the packets and close Fiddler.