Abstract steps you should take to use Wireshark like an attacker:

1. Open wireshark as root
2. Monitor traffic on eth0
3. To save time find the IP address of metaspoitable via login to eth0 (hint: ifconfig)
4. Start the packet capture in Kali Linux
5. Execute an ARP attack to generate traffic for the victim
6. Use the filter in Wireshark to see the traffic from the victim's IP address (hint ip.dst == blah)
7. Generally: [protocol].[header/field][operator: +, ==,!=][value] Try to find packets from the server's source
8. Identify TCP packets trasmitted between server and Kali (hint right click one of the packets from metasploitable and go to Conversation Filter > TCP)
9. Write the filtering command for the above shortcut

Analyze packets collected by your firewall:

1. Enter option 8 in pfsense
2. Run tcpdump (you can exit tcpdump with CTRL+C)
3. Find out how to capture only tcp packets on port 443 (if you don't see any packets try refreshing the browser in Kali)
4. Make sure you understand the output of tcpdump in comparison to Wireshark :)

Exercise

Download 02-capture.pcap
Open the file in Wireshark and provide answers to:

1. What are the MAC and IP addresses of the victim's and attacker's machines?
2. What is the MAC address of the local network's router?