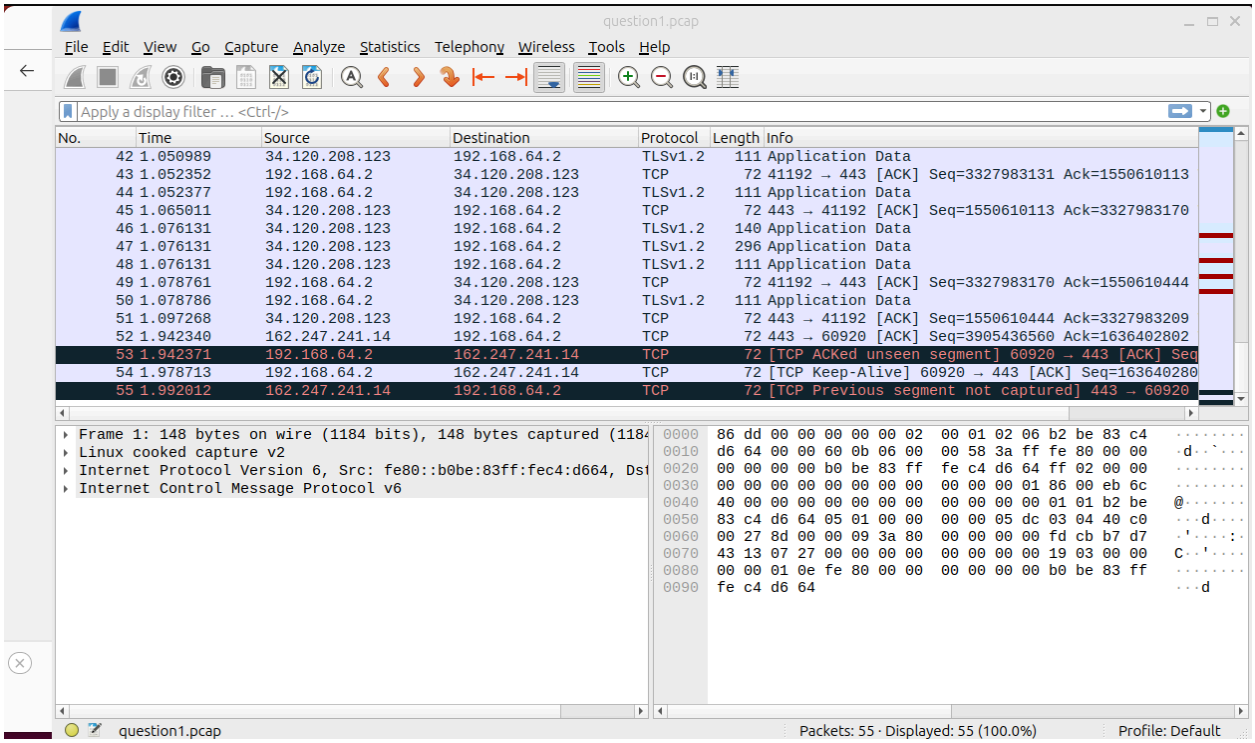
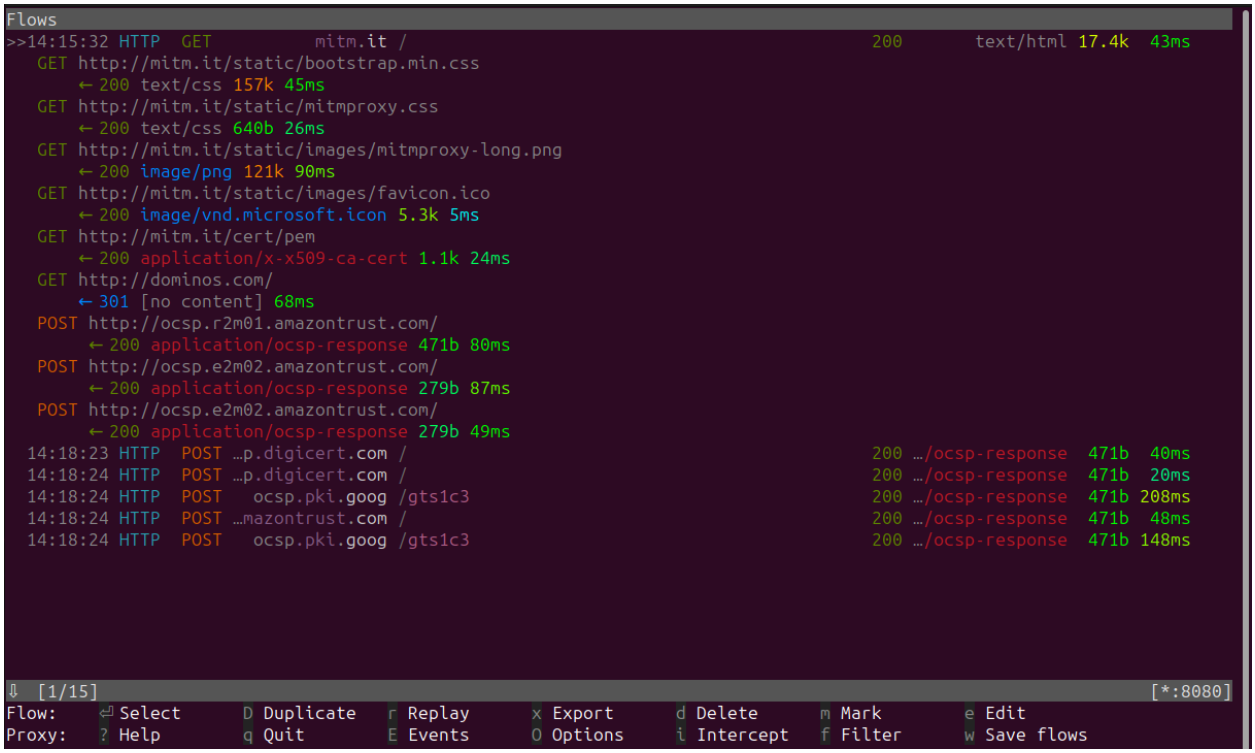
1. Tcpdump captures all the packets that the host sends and receives while the application is running and is able to give detailed information about the packets.
2. Tor Browser hides your IP address and browsing activity in order to allow users to stay anonymous when surfing the web.
3. Wireshark is a tool that allows you to analyze packets in a .pcap file, and lets you view detailed information of each packet.



4. MITMProxy is used to monitor http, https, etc. traffic and allows you to save the data so that you can analyze the information being sent back and forth when connected to a

server of that kind.



5. Scapy is a python library that allows you to directly interact with packets on a low level. For example being able to manipulate their information and send/receive individual packets.
6. The IP address of the vm im using is 146.187.0.44 and the physical location associated with it is in seattle washington.
7. I don’t have anything specific that I'm looking to learn about network security, but I’m just hoping to gain some real world skills and have a better understanding of how to recognize and mitigate cyber threats.
8. I really enjoy skiing and golfing