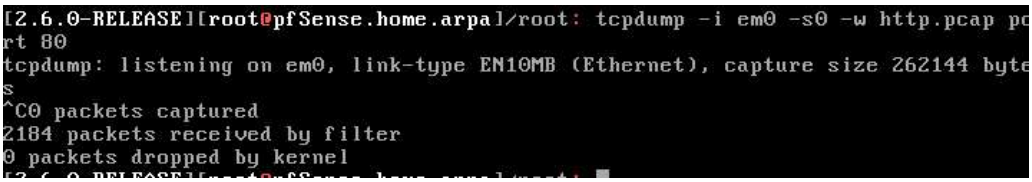
This project explores how to capture and analyze network traffic on a pfSense firewall using Wireshark and tcpdump. The goal is to gain insight into the traffic passing through the firewall and identify any potential security issues or suspicious activity.

To start with go to Wireshark

After it has been running for a few minutes go to the website of your choice

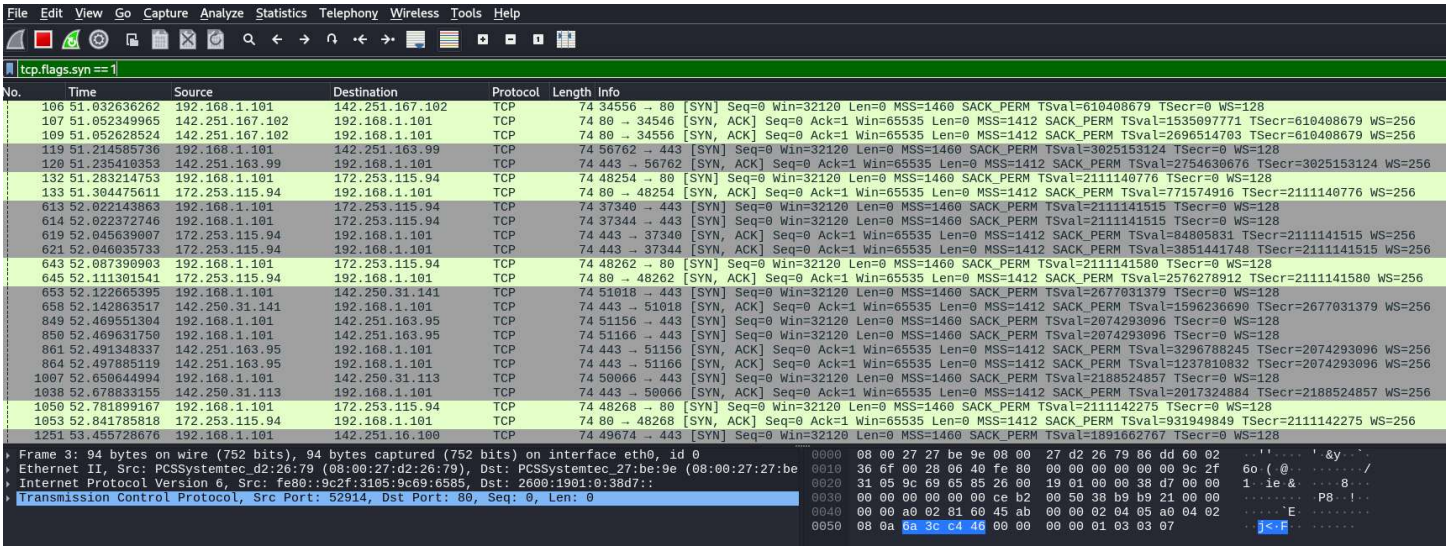
On the pfSense firewall, access the shell by selecting option 8

In the shell, run the following tcpdump command to capture all HTTP traffic on the em0 interface and save it to a file named http.pcap: “tcpdump -i em0 -s0 -w http.pcap port 80”

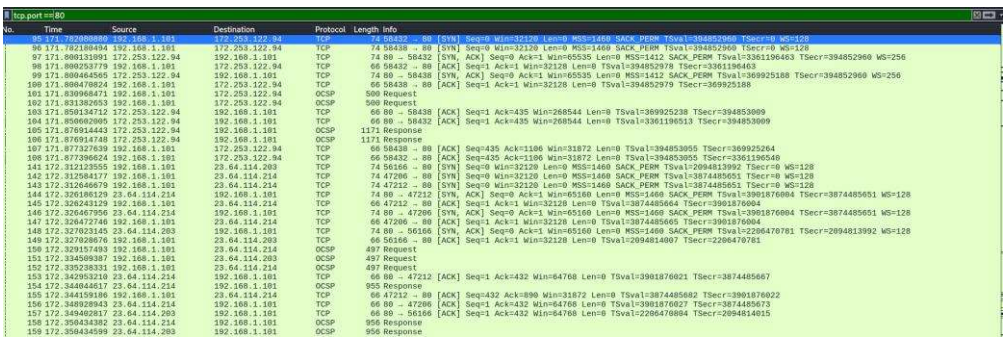


In Wireshark, you can apply the following filters to view specific traffic:

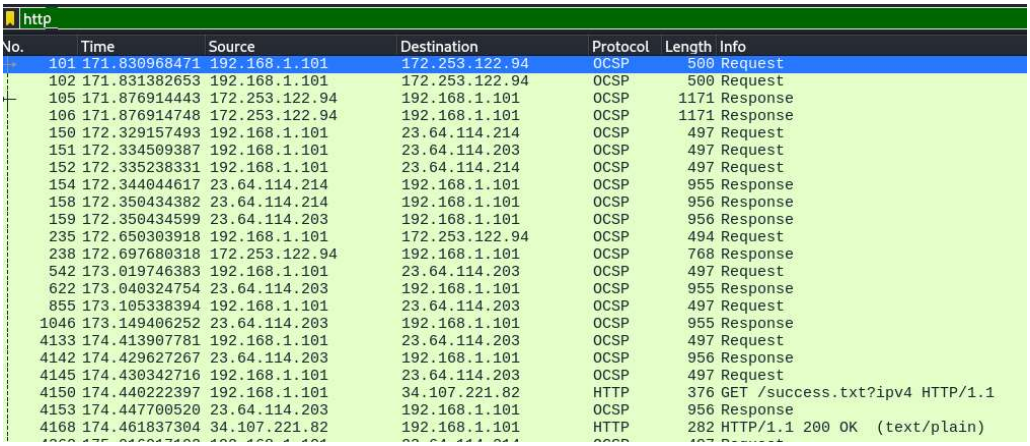
`ip.dst == 192.168.1.101` to see traffic to a specific IP address



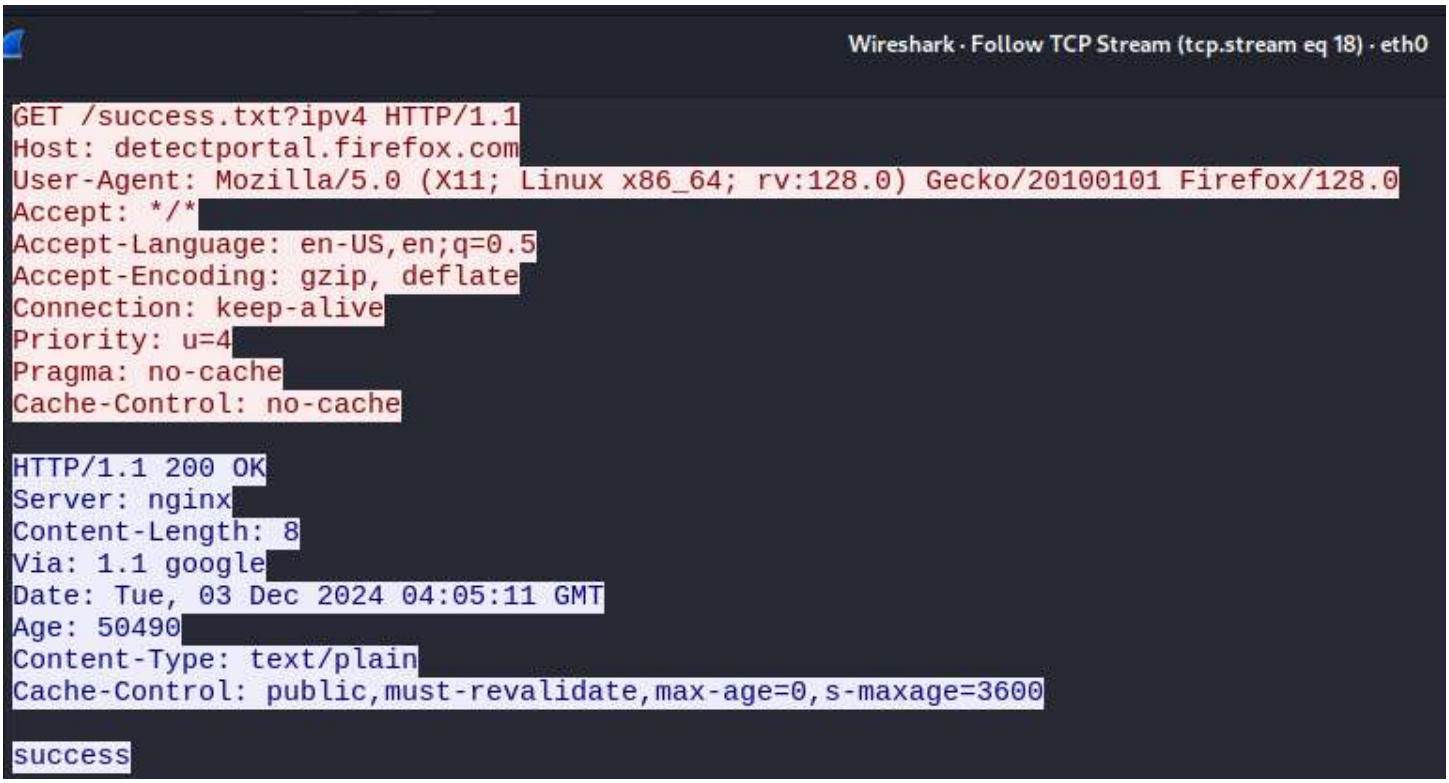
tcp.port == 80 to see only HTTP traffic



http to see HTTP protocol-specific information



Following the TCP stream by right-clicking on a packet and select "Follow" > "TCP Stream"



In this project, you can see how to capture and analyze network traffic on a pfSense firewall using Wireshark and tcpdump. By applying various filters and techniques, you can identify suspicious activity and investigate potential security issues within your network. This knowledge can be valuable for maintaining the security and integrity of your network infrastructure.