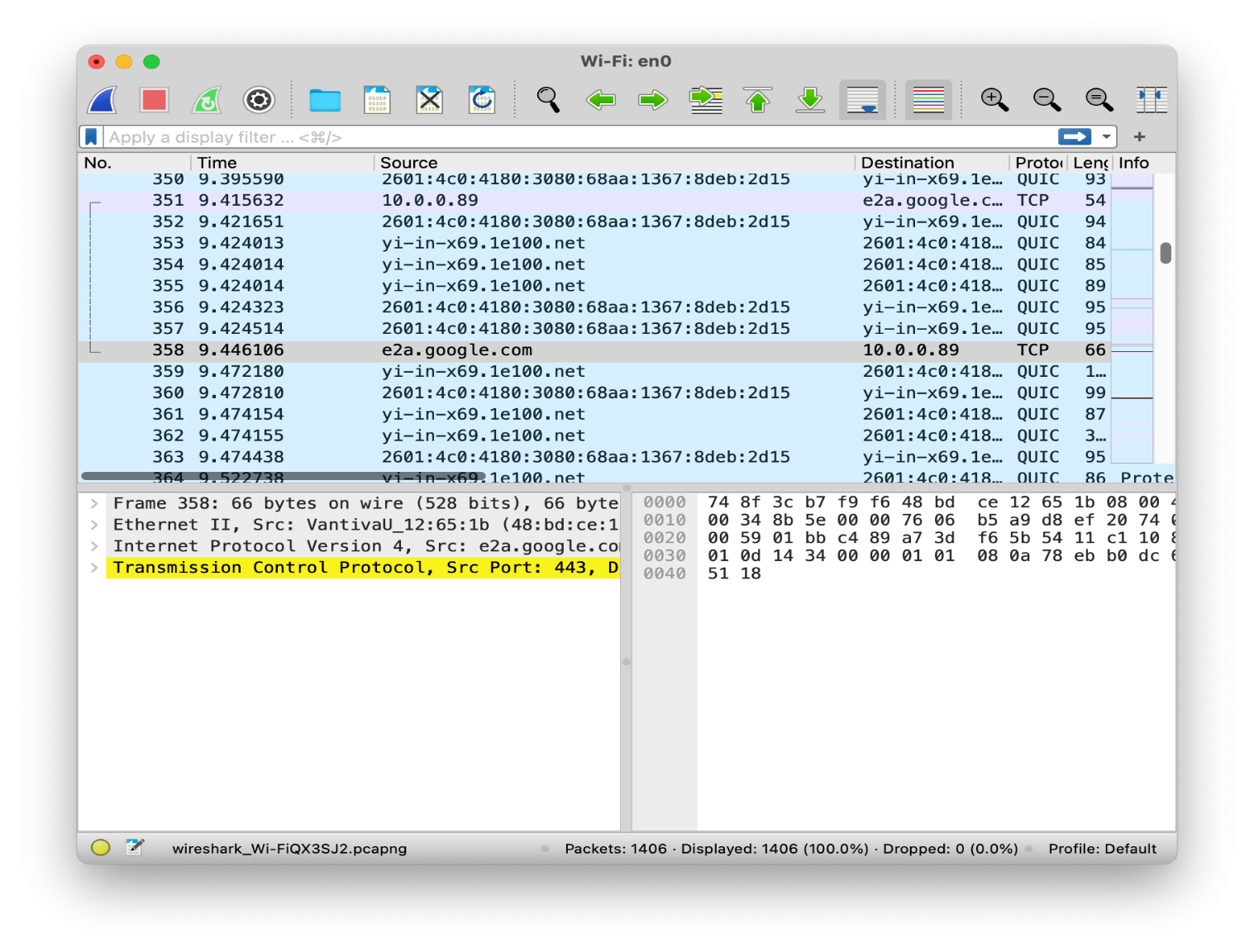
A screenshot of a computer

Description automatically generated



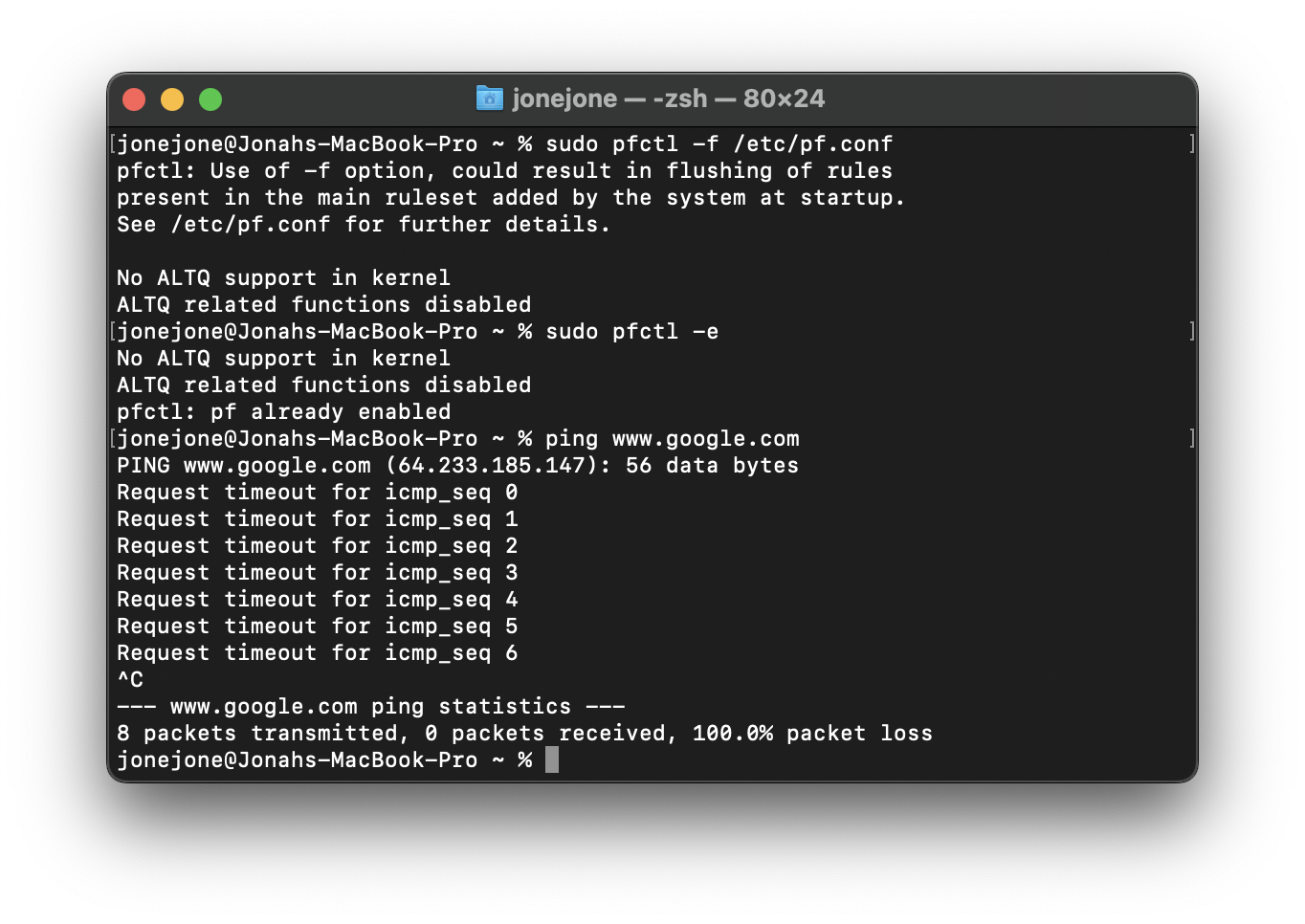
2.Requesting Google's main page

1. Network Interface Card - Capture Options

A screenshot of a computer

Description automatically generated

3. Hexadecimal packet contents

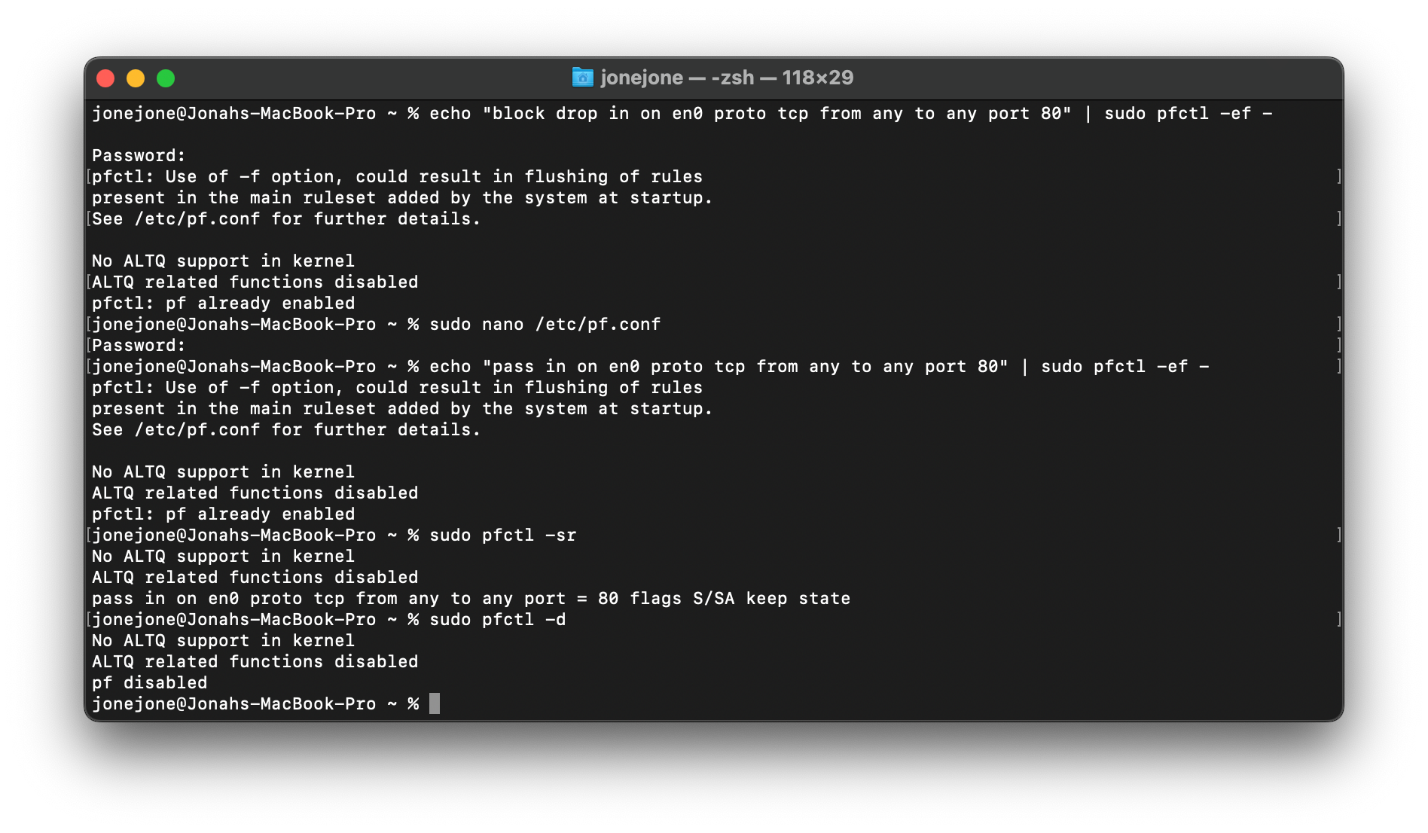
A screenshot of a computer

Description automatically generated

5. Pinging Google after blocking ICMP

4. Pinging Google Normally

A screenshot of a computer

Description automatically generated

6. Unsecure website blocked

7.Disabled rules

1. Why does your computer send so many packets? Why not send just one *big* packet?

Computers use packetization to break down data into smaller packets for more efficient transmission. This allows for better error recovery, retransmission of lost packets, and easier routing through networks with varying conditions.

1. What do SYN, ACK, FIN, GET mean?

* SYN (Synchronize): A TCP packet to initiate a connection.
* ACK (Acknowledgment): A TCP packet to acknowledge the receipt of data.
* FIN (Finish): A TCP packet to terminate a connection.
* GET: An HTTP method used in web requests to retrieve data from a specified resource.

1. Why do some packets have sequence numbers?

Sequence numbers help in reordering and reassembling packets at the destination, ensuring data integrity and proper reconstruction of the original message.

1. Why does your computer send packets to the webserver that you requested data from?

It does this to establish and maintain a communication channel, exchanging requests and responses to retrieve the requested data

1. What do the different colors in the Wireshark packet capture listing mean?

Colors in Wireshark indicate different types of traffic, such as green for TCP, blue for UDP, and pink for ICMP. This color-coded display helps users quickly identify and analyze the various packet types.

1. Why would your computer get packets that are addressed to another computer?

In a network, all packets are broadcasted, and network interfaces may accept packets addressed to other devices on the same network. However, the network stack filters out packets not intended for the specific device.

1. How many packets does your computer send/receive in a single mouse click when you visit a website?

It can range from dozens, to hundred to even thousands.

1. Could you organize or filter the traffic to make it easier to understand?

Yes, tools like Wireshark allow users to apply filters based on various criteria (e.g., IP address, protocol) to organize and focus on specific types of traffic, making analysis more manageable.

1. How could blocking all ICMP traffic protect you?

Blocking all ICMP traffic can prevent certain types of network reconnaissance and attacks, such as ping sweeps. However, it may also impact legitimate uses like network troubleshooting.

1. Could you still access some websites with your Port 80 rule enabled? Why?

Yes, because Port 80 is commonly used for HTTP traffic. Blocking it would prevent access to websites that rely on HTTP, but websites using HTTPS (Port 443) would still be accessible.

1. Why would you want to allow incoming (not outgoing) Port 443, but block incoming

Port 80?

Allowing incoming Port 443 (HTTPS) but blocking incoming Port 80 (HTTP) enhances security by encrypting data during transmission (HTTPS) while blocking potentially insecure non-encrypted traffic (HTTP).

1. Could malware rename itself in order to get through a firewall? Why would this work?

Yes, malware might use names or disguises that mimic legitimate processes or applications to bypass firewall rules. This can work if the firewall rules are based on specific names or characteristics rather than behavior analysis, allowing disguised malware to slip through undetected.