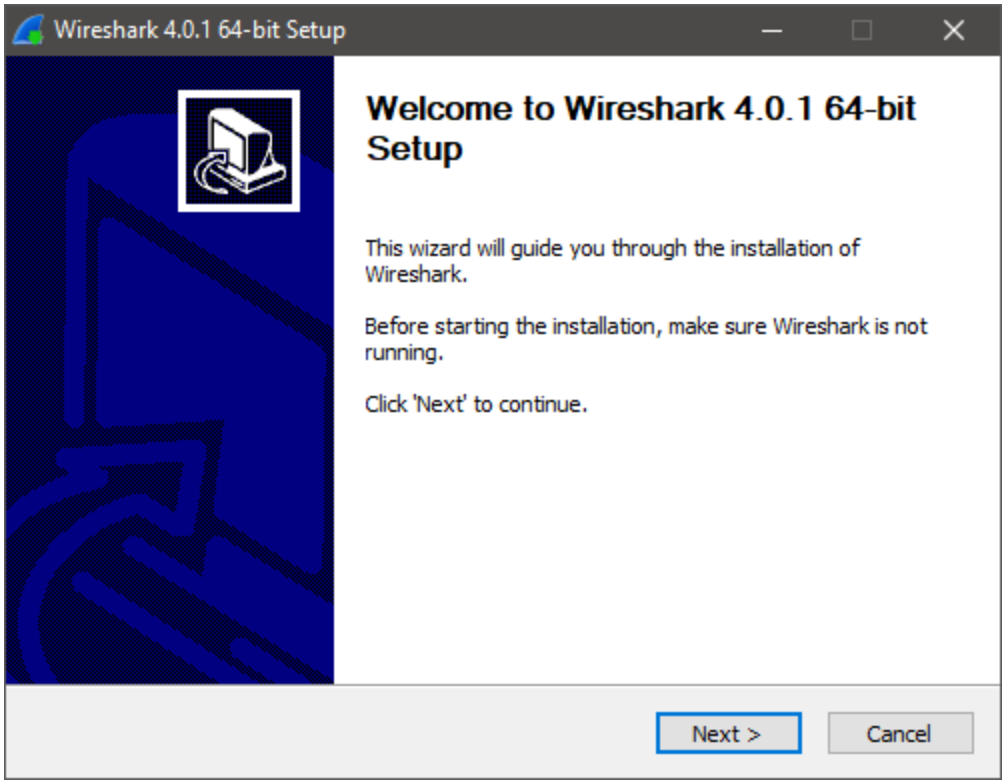
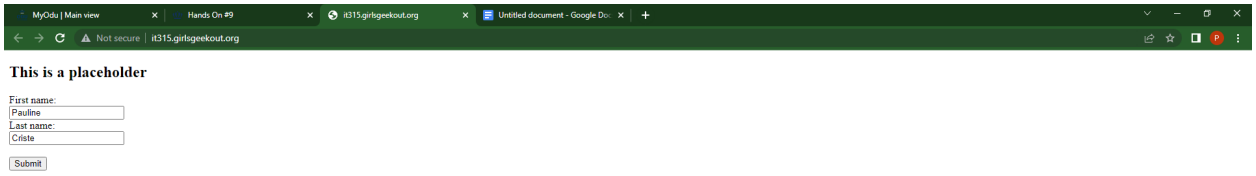
Pauline Criste

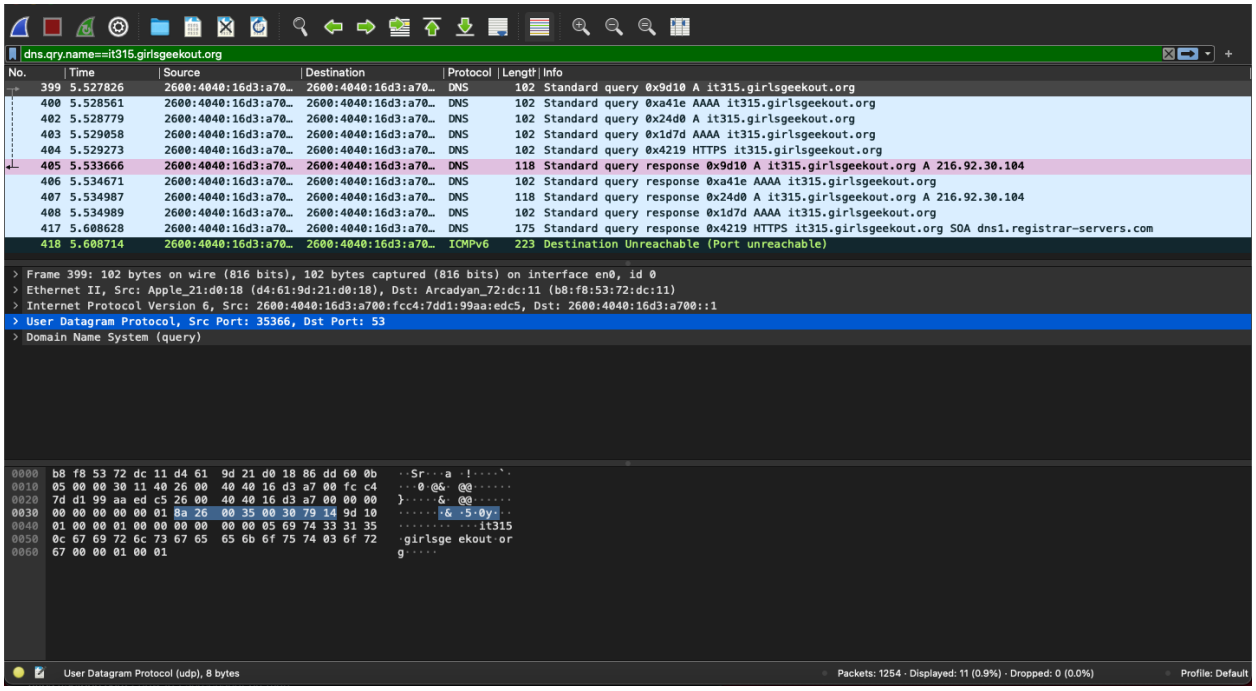


Above is the installer for Wireshark

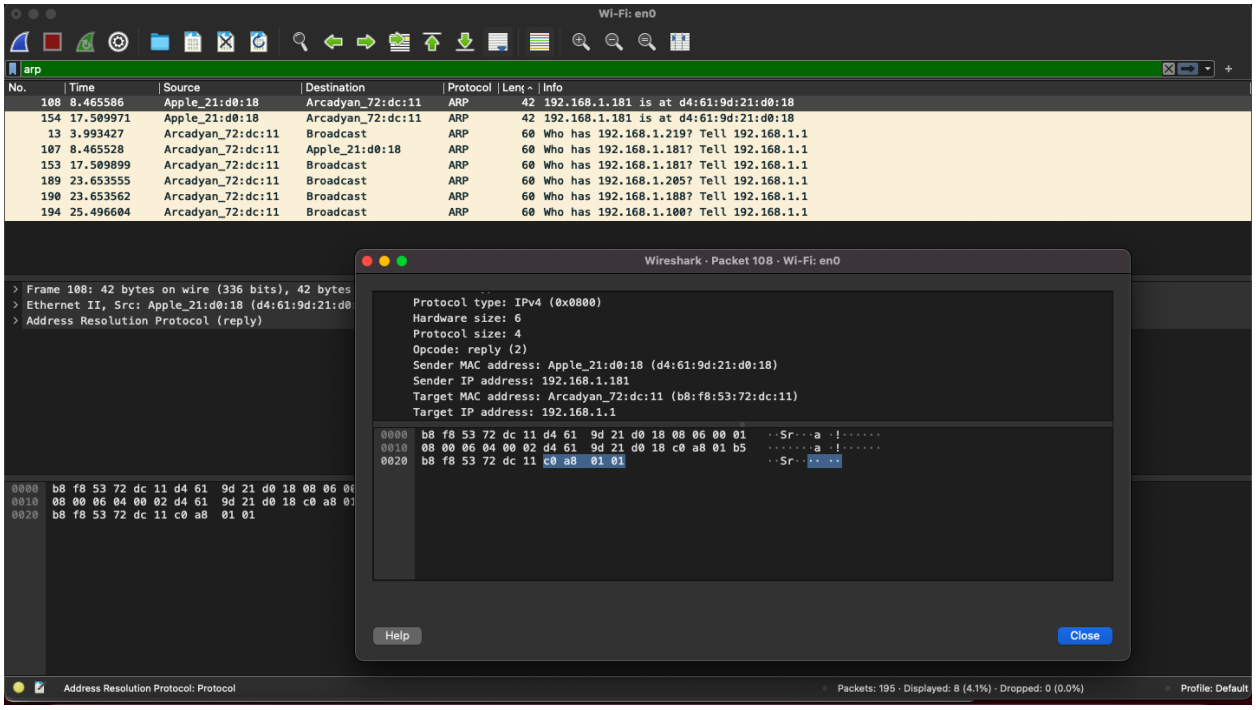


This is the website to input our first and last name. We will capture the traffic on this website.

Pauline Criste

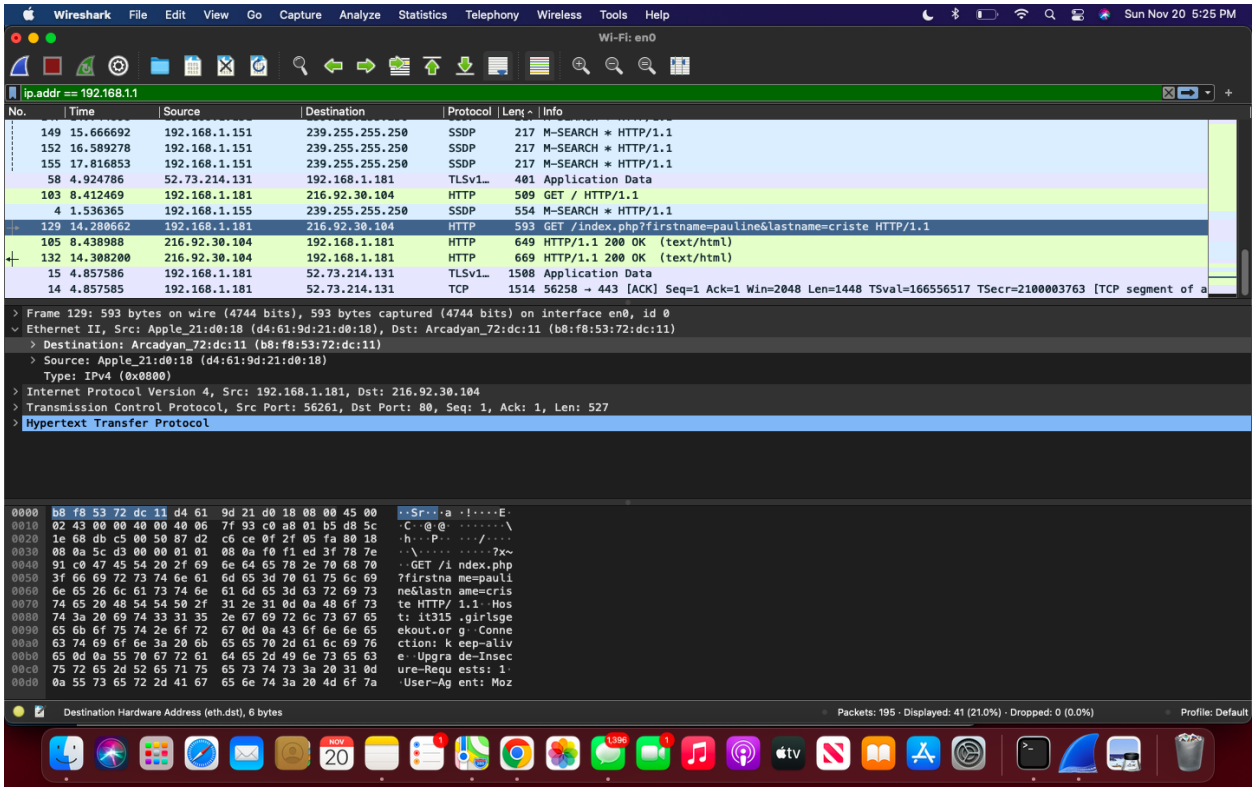


1. I entered on the capture filter dns.qry.name==it315.girlsgeekout.org and it displayed all traffic sent through the website

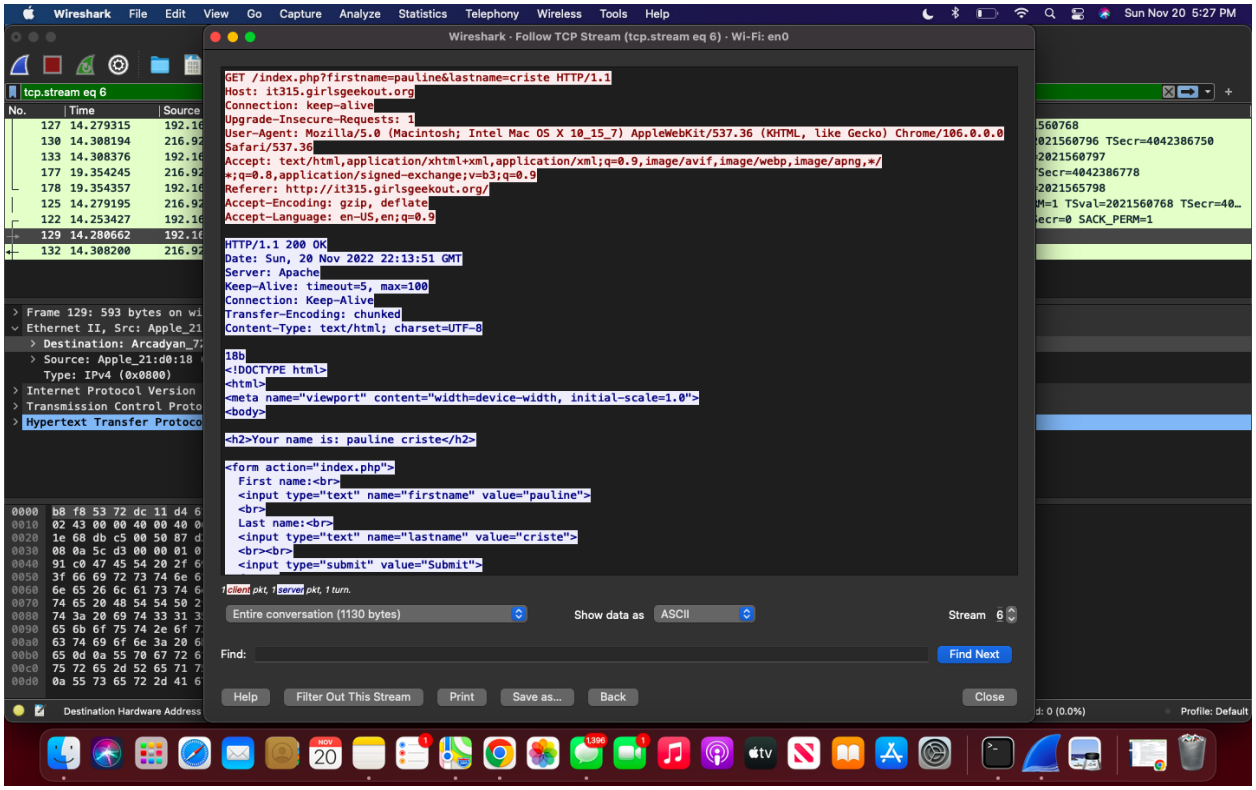


I looked at the information from the DNS packet to see the source and destination. My wireshark was not working properly on Windows so I used my Macbook that has wireshark in it as well. It says that I am the sender (Apple) and the target is

it315.girlsgeekout.org. I used the arp as a filter and it I clicked on where is says source apple, sender arcadyan_72:dc:31 and matched the information from the DNS packet.



2. The ip address that was provided from the ARP for it315.girlsgeekout.org is 192.168.1.1 and so I filtered ip.addr==192.168.1.1 and it displayed packets that included that information. It then includes the GET command under HTTP which has my first and last name.



3. When I right clicked on the GET command with my name on it, went to follow, and clicked on TCP stream, it displayed this information. It contained information about the website and the data that was entered in it. It also says the connection is keep-alive

4. Sniffing this traffic, I was able to capture the information that I input on the website. This means that the website is not encrypted and anyone can access the information that was being entered in the website. It is important to encrypt the network traffic because it is harder to capture rather than plain text.