NAME: Chidinma B. Aniekwena

BUFF ID: 1108372

COURSE: Current Issues in Cybersecurity

WEEK 3: Assignment

ASSIGNMENT TOPIC: Wireless/Phishing

1. WHAT DID I DO

I did a download and installation of WireShark on my Mac by goggling Wireshark for Mac.

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

One could think of a network packet analyzer as a measuring device for examining what’s happening inside a network cable, just like an electrician uses a voltmeter for examining what’s happening inside an electric cable (but at a higher level, of course).

The features of WireShark are the following;

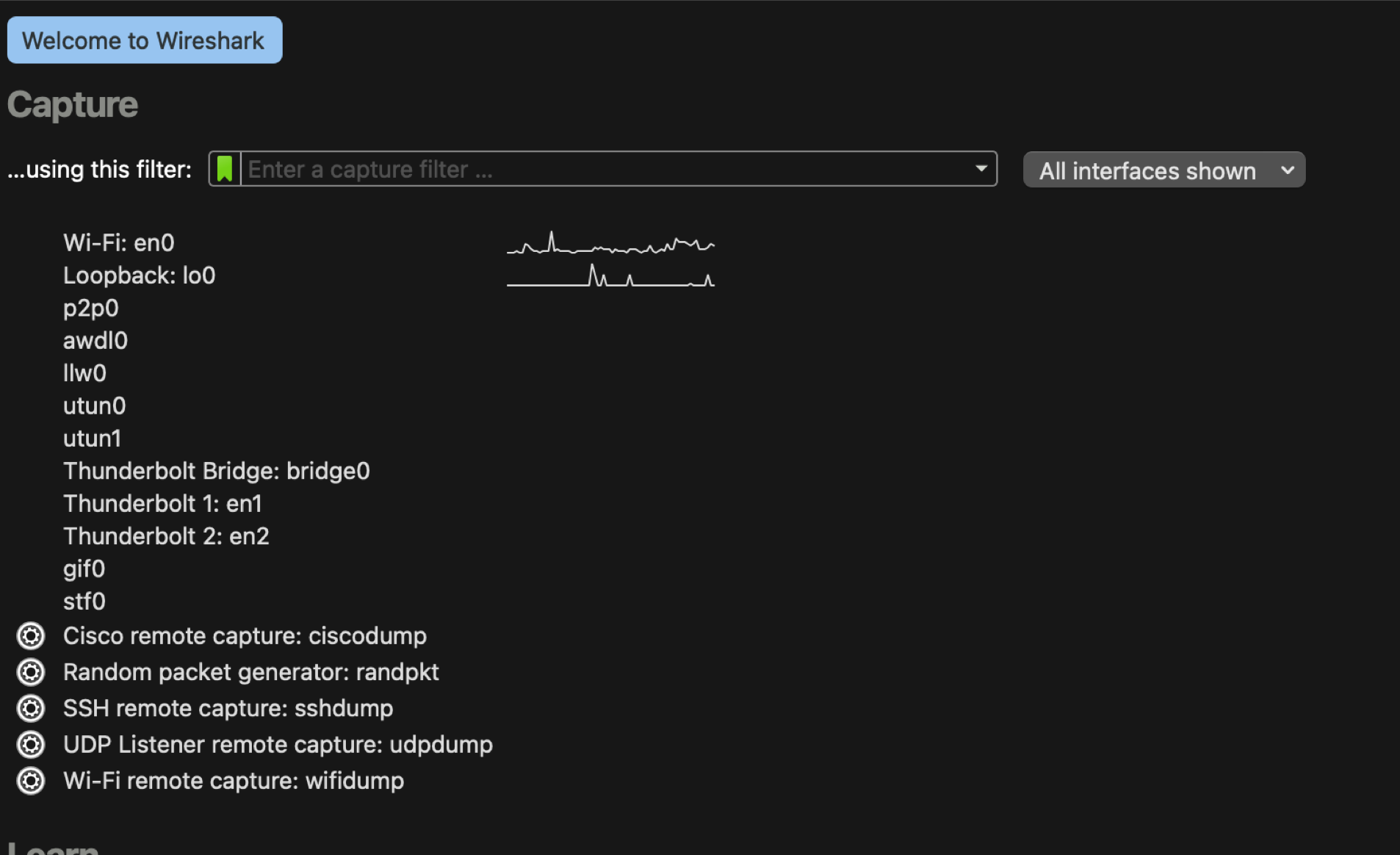
* Available for UNIX and Windows.
* Capture live packet data from a network interface.
* Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
* Import packets from text files containing hex dumps of packet data.
* Display packets with very detailed protocol information.
* Save packet data captured.
* Export some or all packets in a number of capture file formats.
* Filter packets on many criteria.
* Search for packets on many criteria.
* Colorize packet display based on filters.
* Create various statistics.
* …​and a lot more!

Some of the intentions or purpose of using WireShark is that;

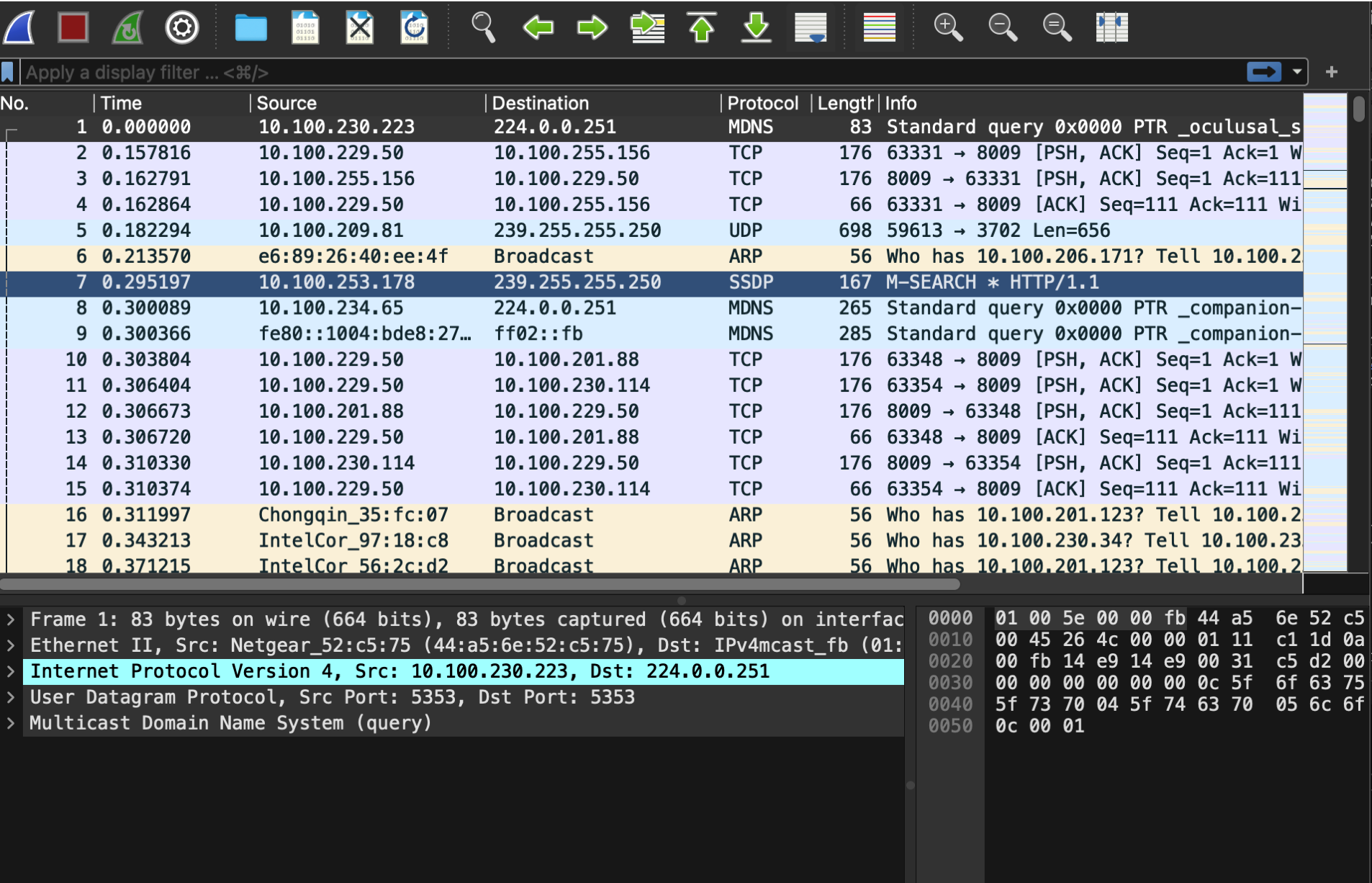
* Network administrators use it to troubleshoot network problems
* Network security engineers use it to examine security problems
* QA engineers use it to verify network applications
* Developers use it to debug protocol implementations
* People use it to learn network protocol internals

As shown below the WireShark application featured all wired, wireless and external capture interface on my network passing forth and back on my computer.

The Wi-Fi: en0 has a lot of traffic because my computer is connected to the apartment’s wifi. Other interfaces was also displayed like loopback:lo0, p2p0, awdl0 etc, though their data will be encrypted. I know it is illegal to capture other people’s data and use it for malicious purpose. As a study case it can see a lot of traffic from other peoples’ computers in order to understand what type of feedwork tray packages is going through our network.



On clicking on the Wi-Fi: en0, which is the network on my computer, it automatically entered capturing mode. The application started capturing all the network traffic that is going through and from my computer. I stopped the capturing and looked at the pages that has been captured. See below for screen display of the captured pages and details shown.



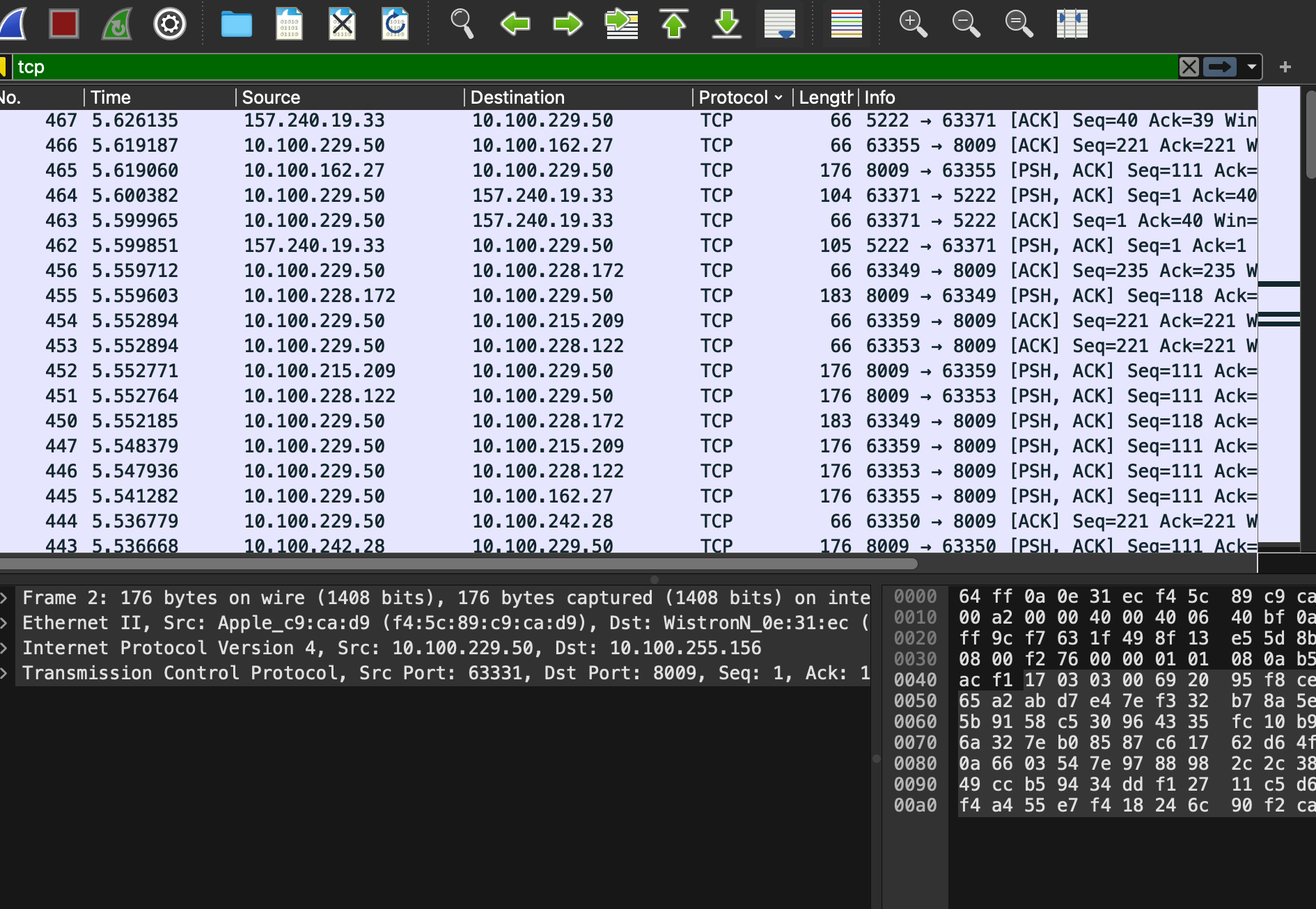
1. WHAT WERE MY RESULTS

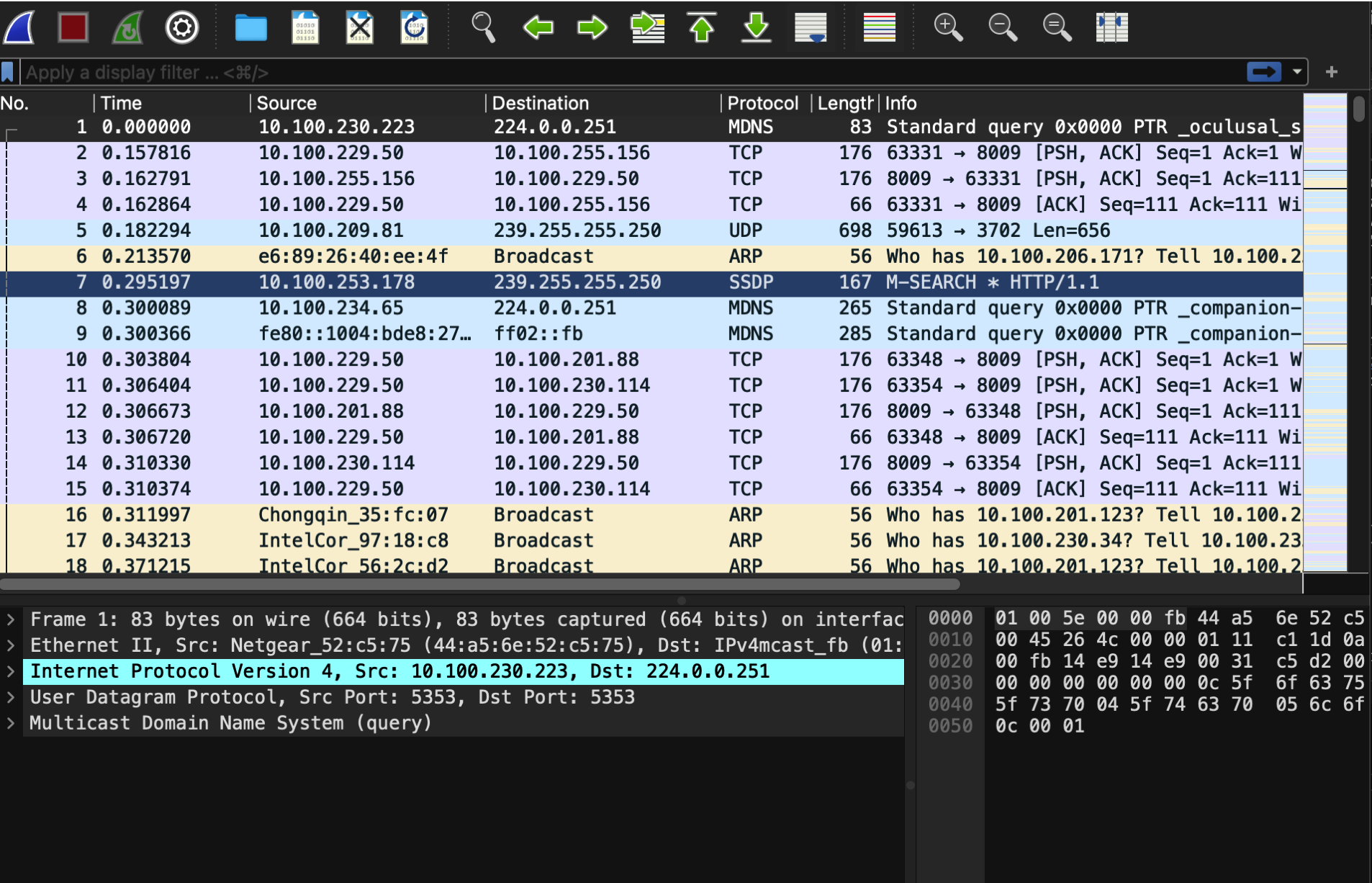
The results showed the number of the packages, the time for each package, the device IP source and the IP destination, the protocol, the length of the package and additional information. WireShark also captured a lot of traffic because all my application on the computer is running at the background and sending information back and forth. Notwithstanding am not doing anything on my browser, my computer is still communicating a lot with the wireless network. I see all the traffic from all devices on the wifi network, which happens to be a lot.

I did a filtering to see a specific protocol (TCP) and (UDP) it displayed only TCP and UDP protocol information respectively. TCP is connection-oriented while UDP is connectionless

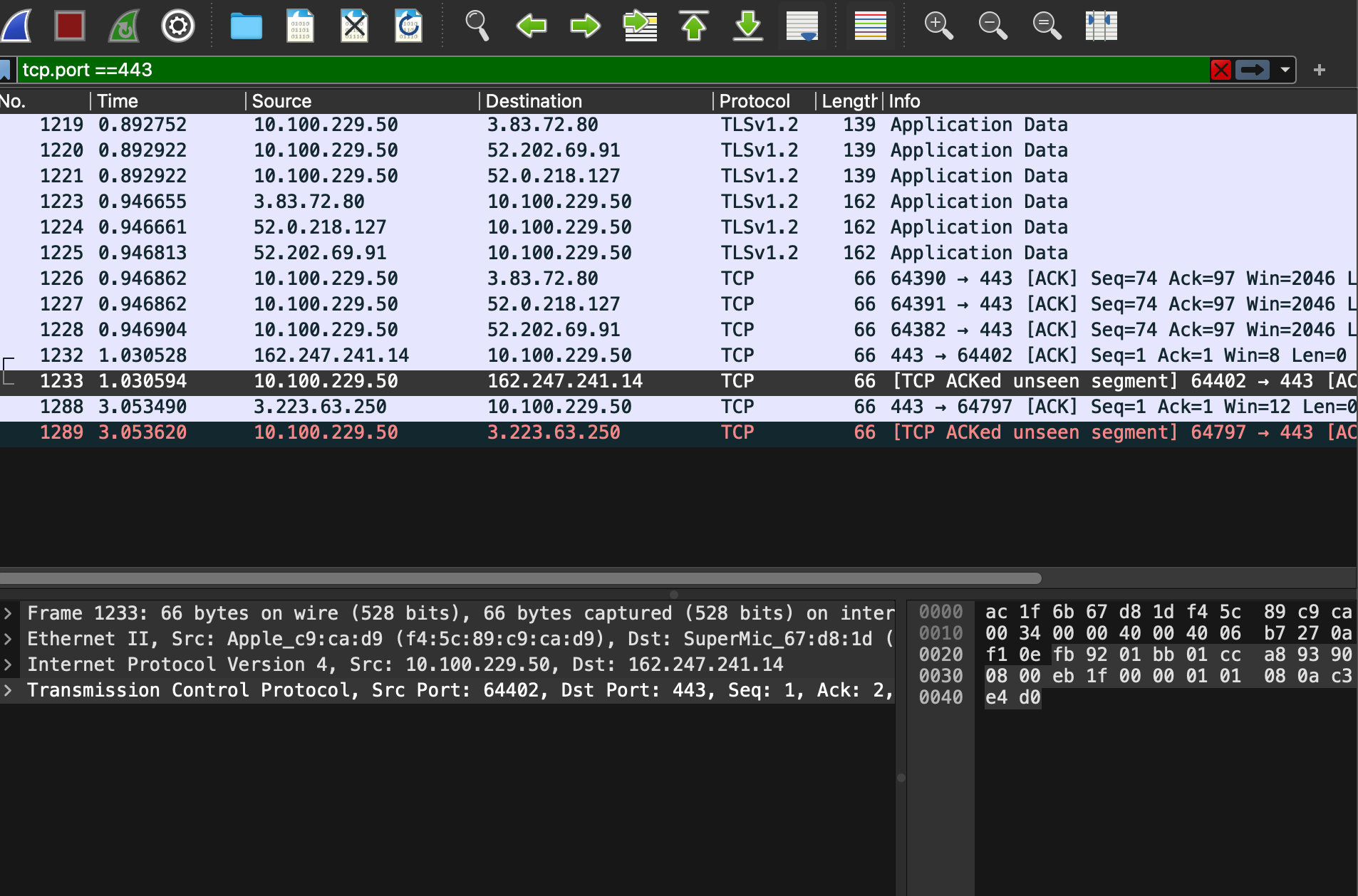
The connection is established via a three-way handshake. The client sends a synchronization request, the server sends back an acknowledgment, and the client returns a synchronization acknowledgment in response.

TCP - used for traffic that you need all the data for. i.e HTML, pictures, etc. UDP - used for traffic that doesn't suffer much if a packet is dropped, i.e. video & voice streaming, some data channels of online games, etc.

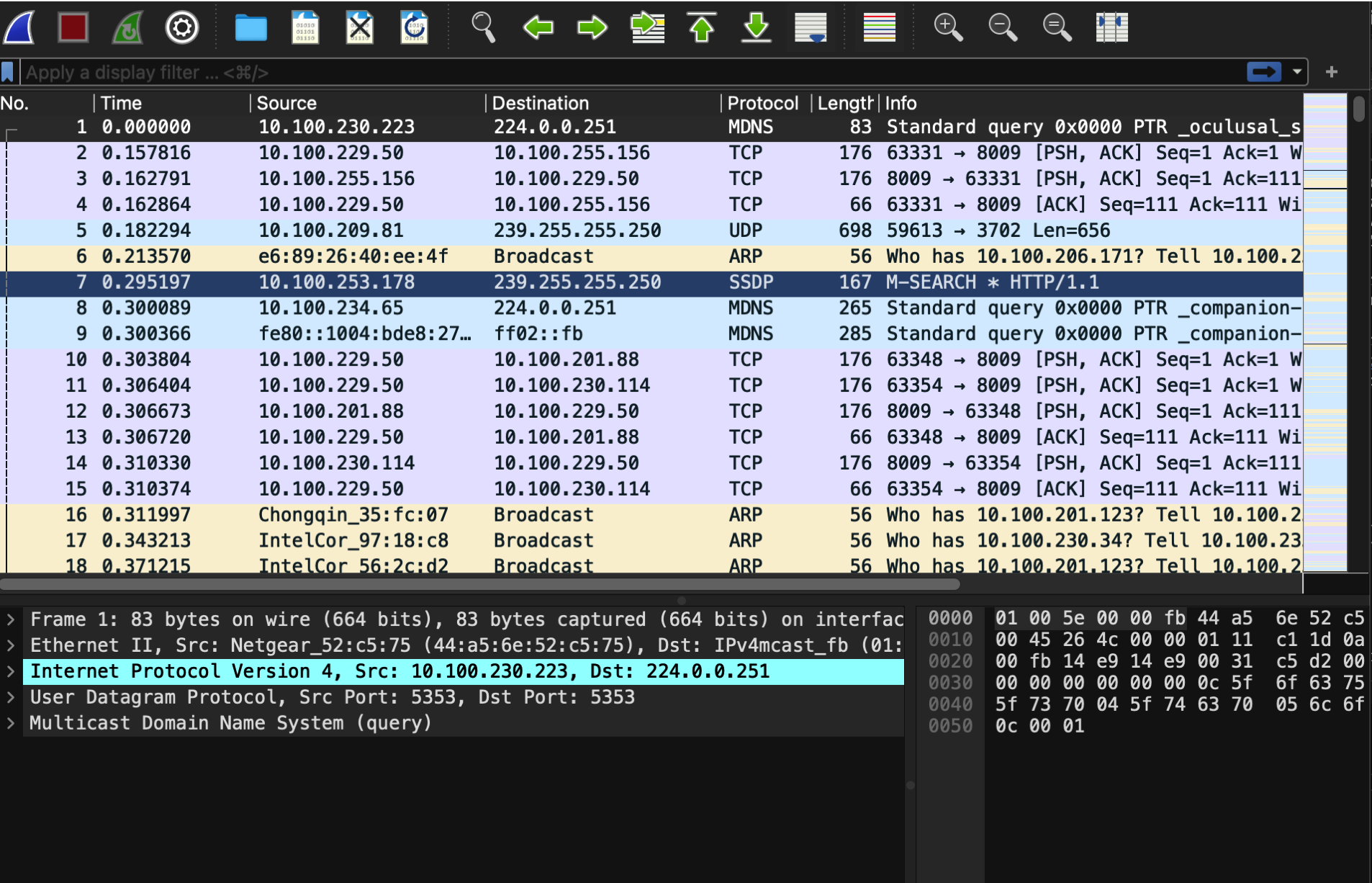




I filtered the packets to show the TCP port 443. Normally all web traffic is screened under port 443. It also showed that my computer IP address 10.100.229.50 is the source IP transmitting to IP address 162.247.241.14. on destination port 443 and the source port is 64402. The time of the package and the time stamps was also displayed.



I also checked all the packages that my device sent to the IP, I typed ip.addr == 10.100.229.50 and clicked Enter, then a lot of packages going back and forth my device.



1. WHAT DID I LEARN

I learnt how to discover all other networks in my neighbourhood, identify the IP address that is the source and destination. Notwithstanding am not doing anything on my browser, my computer is still communicating a lot with the wireless network. I see all the traffic from all devices on the wifi network, which happens to be a lot.

To be able to check an exact port and know which IP address is the source and destination and also what IP address is giving out information from my computer.