

Capstone Part III

By : Leonard Sterling

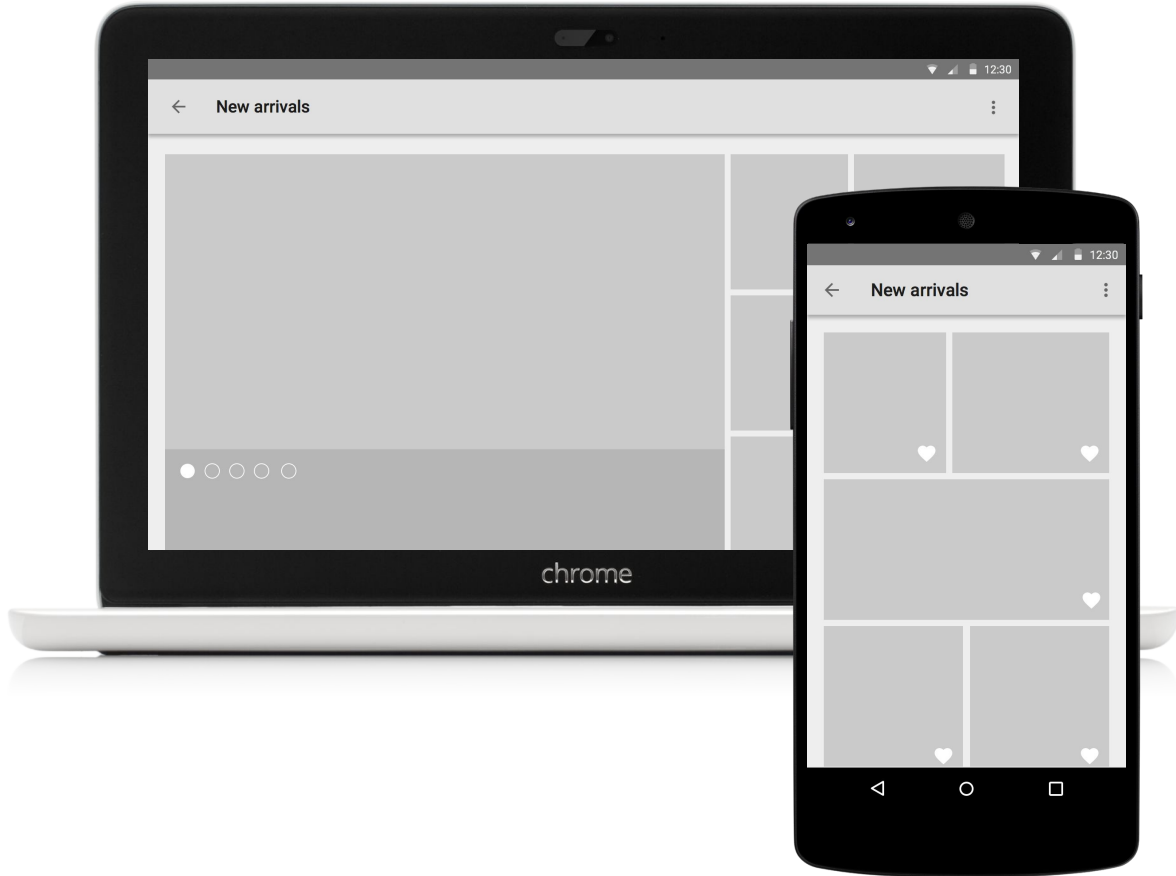
Overview: Network Analysis

Architecture

Network configuration

Performance monitoring

Security



Architecture

This is the topology on my network and the devices that are connected to it in the diagram these are devices that have internet access capabilities you have a Macbook air, Smart Tv , Router/Modem combo, Windows laptop , an Apple watch and airpods as well as an Amazon speaker.

.The Internet service provider is Suddenlink Communications and the hardware used for the internet to be access is the modem/router all in one combo that has a black coaxial cable that connects to the house to provide the network.

The Router/modem is one of two devices besides the smart tv can use wired connection in use in the diagram all the others devices are have wireless capabilities such as Macbook, Windows, smart tv apple watch

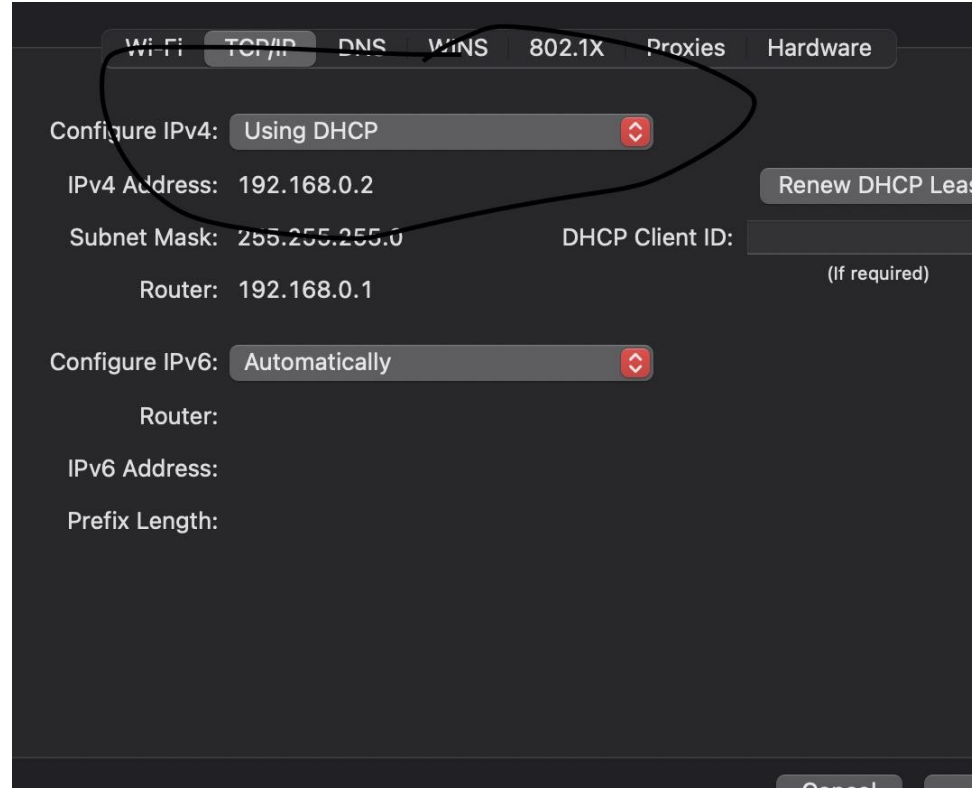
Apple Watch connects to the internet with a wireless connections device same as a laptop. The smart tv connects to the internet using a wireless connections as well has a built in wireless connection .the wireless Bluetooth speaker connects to the internet wireless with a built in component.



Network Configuration

With using the computer that I was operating with I was able to locate my network configuration settings. While doing this I identified within the network configuration settings my IP address, Subnet mask, default gateway, MAC address and the DNS Informations. The next slide will show screenshots of each

Also within my network you can tell my IP address is dynamic because static because DHCP is Enabled. Which mean it is automatically assign an IP address if it were static it would have to be put in Manually.



Network Configuration II

Within the image to the right you can see

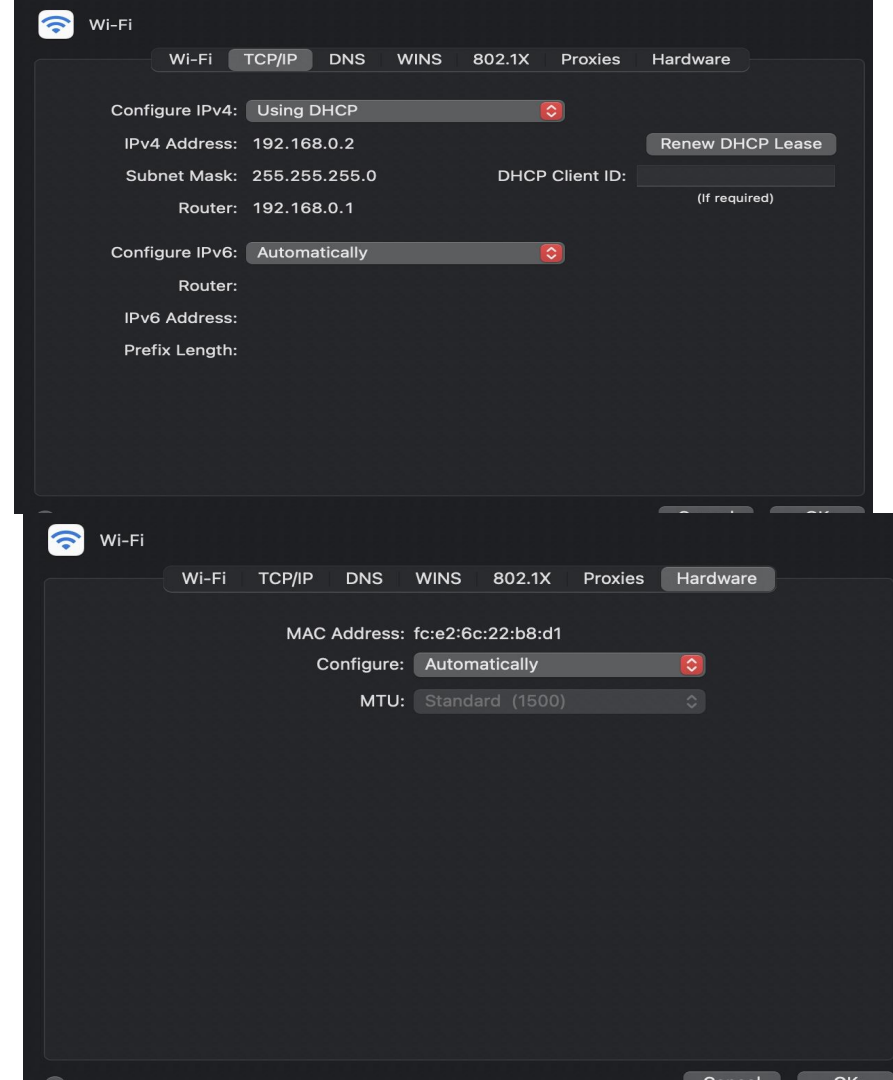
IP address 192.168.0.2

Subnet mask 255.255.255.0

Default gateway 192.168.0.1 (Router)

MAC address fc:e2:6c:22:b8:d1

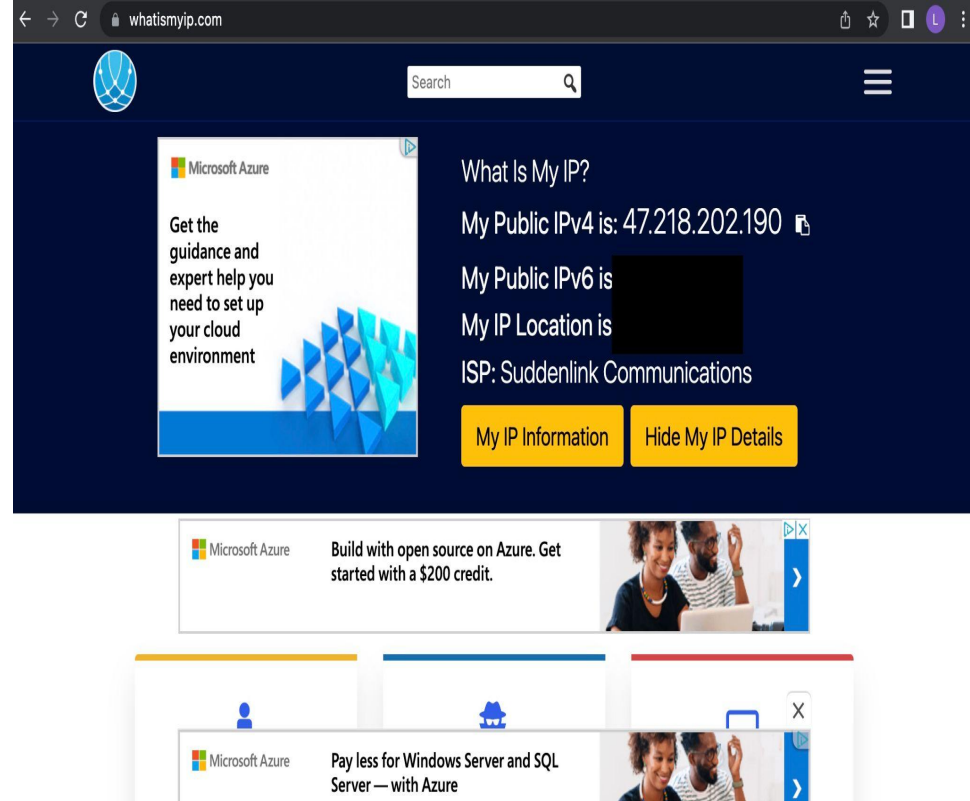
DNS information 24.48.160.2 ,24.48.160.3
(Can be found in the DNS section)



Network Configuration III

A way that you can find a public ip address is by going to <https://www.whatismyip.com/> in the image to my right you can see my public IP address is 47.218.202.190

Also the way a public and a private network is used on a network is a public IP address on a network identifies you to a wider range so any information that you are searching for can find you. Private IP address can connect securely to any other device within the network.



The screenshot shows the website [whatismyip.com](https://www.whatismyip.com/) in a browser. The page has a dark blue header with a search bar and a menu icon. Below the header, there is a Microsoft Azure advertisement on the left and a main content area on the right. The main content area displays the following information:

- What Is My IP?
- My Public IPv4 is: 47.218.202.190
- My Public IPv6 is: [Redacted]
- My IP Location is: [Redacted]
- ISP: Suddenlink Communications

At the bottom of the main content area, there are two yellow buttons: "My IP Information" and "Hide My IP Details". Below the main content area, there is another Microsoft Azure advertisement with the text "Build with open source on Azure. Get started with a \$200 credit." and a photo of two people. At the very bottom, there is a third Microsoft Azure advertisement with the text "Pay less for Windows Server and SQL Server — with Azure" and a photo of two people.

Performance Monitoring

In the image on the right i ran speed test on my network at different times of the day to see the difference in speeds. I was able to do this by going to www.speedtest.net

As you can see the network is fastest in the earliest morning (5:52am) and is slowest late night (9:41pm) I think its faster in the morning because less people is on the network and slower in the evening because more people are on the network.

As you can see the network is fastest in the earliest morning (5:52am) and is slowest late night (9:41pm) I think its faster in the morning because less people is on the network and slower in the evening because more people are on the network.

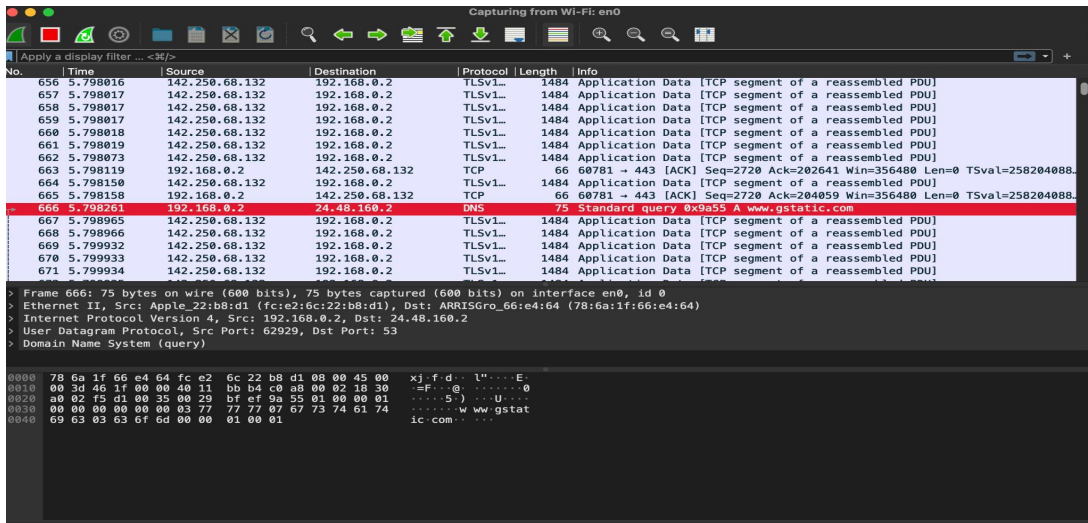
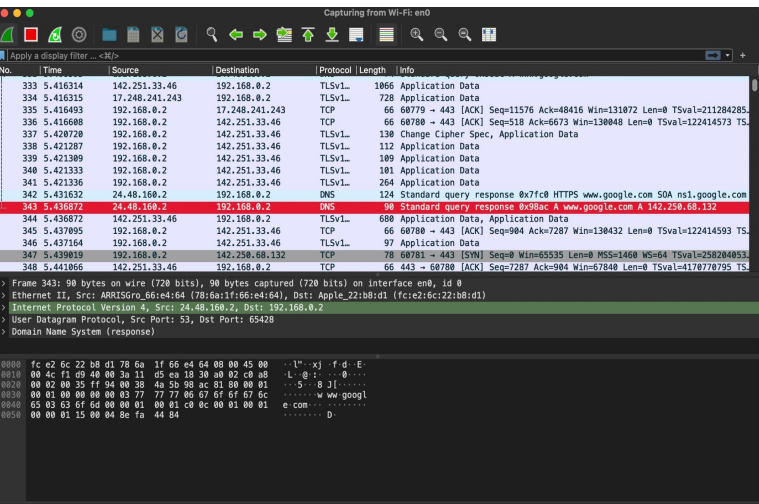
Test	Time Recorded	Upload Speed	Download Speed
Test 1	9:41 pm	11.95 mbps	7.43 mbps
Test 2	5:52 am	43.33mbps	90.24mbps
Test 3	4:59pm	36.69mbps	23.57mbps

Bandwidth vs Throughput

When doing performance monitoring you need to know the difference between bandwidth and throughput. Bandwidth measures indirect related speed while throughput measures speed. They both are similar but they measure different aspects of networks. Throughput measures the amount of data traveling successfully while bandwidth measure how much data could be transferred.

Network Capture

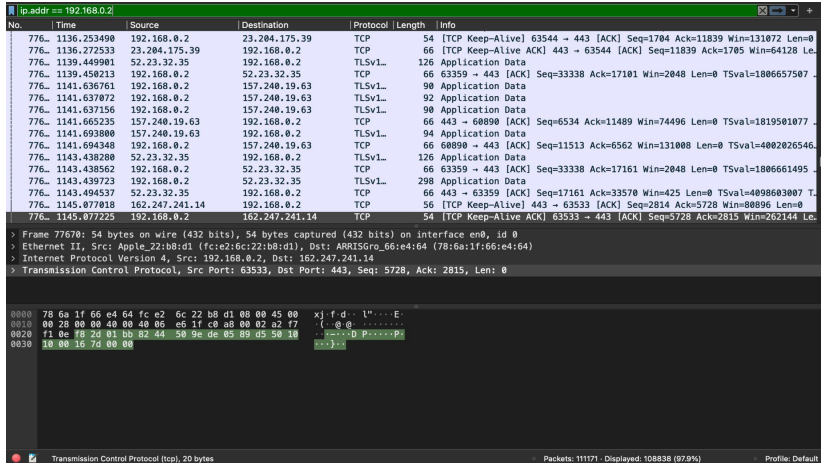
I used Wireshark to capture at least 60 seconds of network traffic. While doing this I was able to go in and see the different sites that were visited at the time. Highlighted in red you can see the websites that were visited.



Network Capture II

In this example i was able to use filter `ip.addr == 192.168.0.2` to show all the captures on my network also an analyst might use this filter to see or show any packets to or from an ip address basically monitoring information from the IP.

You can also go to statistics to capture filter to show only IPv4 only

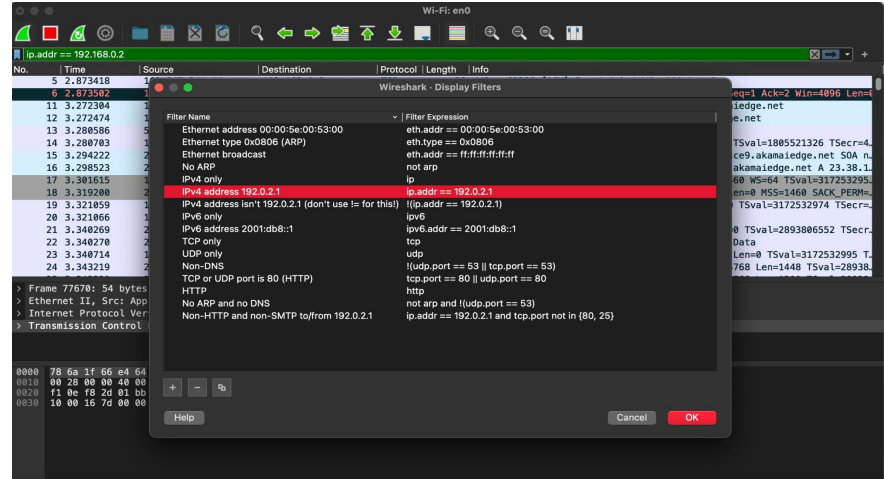


No.	Time	Source	Destination	Protocol	Length	Info
776.	1136.253490	192.168.0.2	23.204.175.39	TCP	54	[TCP Keep-Alive] 63544 → 443 [ACK] Seq=1704 Ack=11839 Win=131072 Len=0
776.	1136.272533	23.204.175.39	192.168.0.2	TCP	66	[TCP Keep-Alive ACK] 443 → 63544 [ACK] Seq=11839 Ack=1705 Win=64128 Len=0
776.	1139.449901	52.23.32.35	192.168.0.2	TLSv1.	126	Application Data
776.	1139.450213	192.168.0.2	52.23.32.35	TCP	66	63359 → 443 [ACK] Seq=33338 Ack=17101 Win=2048 Len=0 TSval=1806657507
776.	1141.636761	192.168.0.2	157.240.19.63	TLSv1.	90	Application Data
776.	1141.637072	192.168.0.2	157.240.19.63	TLSv1.	92	Application Data
776.	1141.637156	192.168.0.2	157.240.19.63	TLSv1.	90	Application Data
776.	1141.665235	157.240.19.63	192.168.0.2	TCP	66	443 → 60890 [ACK] Seq=6534 Ack=11489 Win=74496 Len=0 TSval=1819501077
776.	1141.693800	157.240.19.63	192.168.0.2	TLSv1.	94	Application Data
776.	1141.694348	192.168.0.2	157.240.19.63	TCP	66	60890 → 443 [ACK] Seq=11513 Ack=6562 Win=131008 Len=0 TSval=4002026546
776.	1143.438208	52.23.32.35	192.168.0.2	TLSv1.	126	Application Data
776.	1143.438562	192.168.0.2	52.23.32.35	TCP	66	63359 → 443 [ACK] Seq=33338 Ack=17161 Win=2048 Len=0 TSval=1806661495
776.	1143.439723	192.168.0.2	52.23.32.35	TLSv1.	298	Application Data
776.	1143.494537	52.23.32.35	192.168.0.2	TCP	66	443 → 63359 [ACK] Seq=17161 Ack=33570 Win=425 Len=0 TSval=4098603007
776.	1145.077018	162.247.241.14	192.168.0.2	TCP	56	[TCP Keep-Alive] 443 → 63333 [ACK] Seq=5720 Ack=2615 Win=202114 Len=0

Frame 77678: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: Apple 22:8b:d1 (fc:e2:6c:22:8b:d1), Dst: ARRISGro_66:e4:64 (78:6a:1f:66:e4:64)
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 162.247.241.14
Transmission Control Protocol, Src Port: 63333, Dst Port: 443, Seq: 5720, Ack: 2615, Len: 0

0000 78 6a 1f 66 e4 64 fc e2 6c 22 8b d1 00 00 45 00 x f d i l E
0010 00 20 00 00 40 00 06 e6 1f c0 a8 00 02 a2 77 (. @ @
0020 f1 0e f8 2d 01 bb 82 44 50 9e de 85 89 d5 50 10D P.....P
0030 30 00 16 7d 00 00 (.....)

Transmission Control Protocol (tcp), 20 bytes
Packets: 111171 - Displayed: 106838 (97.9%)
Profile: Default



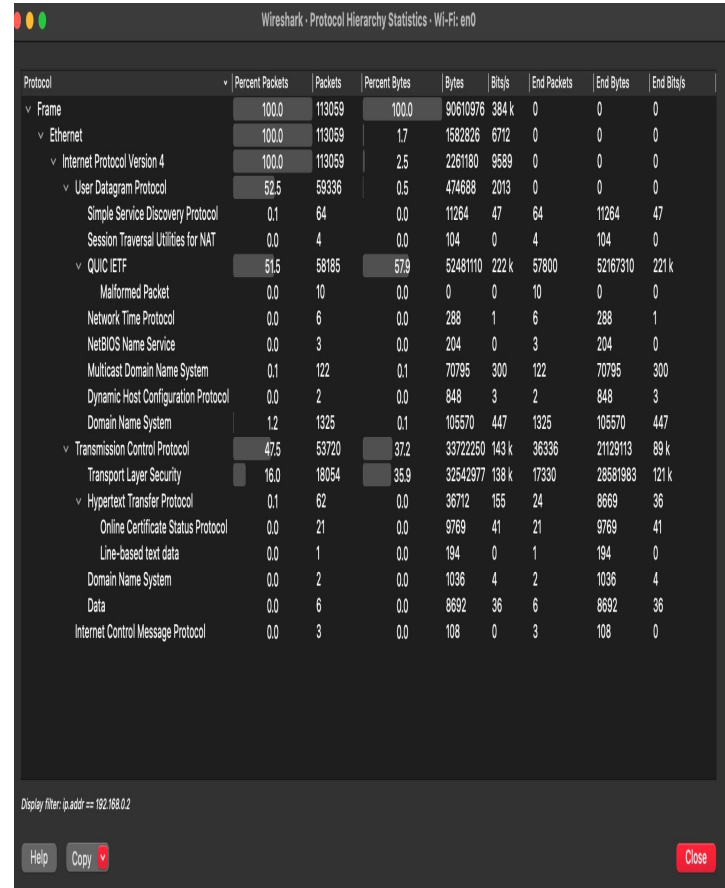
No.	Time	Source	Destination	Protocol	Length	Info
5	2.873418					
12	3.272384					
12	3.272474					
13	3.288586					
14	3.288783					
15	3.294222					
16	3.298523					
17	3.301615					
18	3.319200					
19	3.321859					
20	3.321866					
21	3.340269					
22	3.340270					
23	3.340714					
24	3.343219					

Filter Name: Filter Expression
Ethernet address 00:00:5e:00:53:00 eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP) eth.type == 0x0806
Ethernet broadcast eth.addr == ff:ff:ff:ff:ff:ff
No ARP not arp
IPv4 only ip
IPv4 address 192.0.2.1 ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this) !ip.addr == 192.0.2.1
IPv6 only ip6
IPv6 address 2001:db8::1 ip6.addr == 2001:db8::1
TCP only tcp
UDP only udp
Huds port == 53 || tcp.port == 53
TCP or UDP port is 80 (HTTP) tcp.port == 80 || udp.port == 80
HTTP http
No ARP and no DNS not arp and !udp.port == 53
Non-HTTP and non-SMTP to/from 192.0.2.1 ip.addr == 192.0.2.1 and tcp.port not in (80, 25)

Help Cancel OK

Network Capture III

In Wireshark i was able to use the protocol hierarchy option within the statistics to list the top 5 protocols on the network during capture the top 5 include **Internet Protocol Ver.4** - used to deliver datagrams between such hosts. **User Datagram Protocol**- used to establish latency and loss tolerating connections between applications. **QUIC IETF** - an encrypted connection oriented that operates on the OSI layer 4. **Transmission Control P**- establishes and maintain a network conversation by data exchange. **Hypertext Transfer P** - sets rules for transferring files such as images, sound and video.

A screenshot of the Wireshark Protocol Hierarchy Statistics window. The window title is 'Wireshark - Protocol Hierarchy Statistics - Wi-Fi: en0'. It displays a table of network protocols and their statistics. The table has columns for Protocol, Percent Packets, Packets, Percent Bytes, Bytes, Bits/s, End Packets, End Bytes, and End Bits/s. The protocols are listed in a tree view on the left, with expandable icons. The data is sorted by Percent Packets in descending order.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	113059	100.0	90610976	384 k	0	0	0
Ethernet	100.0	113059	1.7	1582826	6712	0	0	0
Internet Protocol Version 4	100.0	113059	2.5	2261180	9589	0	0	0
User Datagram Protocol	52.5	59336	0.5	474688	2013	0	0	0
Simple Service Discovery Protocol	0.1	64	0.0	11264	47	64	11264	47
Session Traversal Utilities for NAT	0.0	4	0.0	104	0	4	104	0
QUIC IETF	51.5	58185	57.9	52481110	222 k	57800	52167310	221 k
Malformed Packet	0.0	10	0.0	0	0	10	0	0
Network Time Protocol	0.0	6	0.0	288	1	6	288	1
NetBIOS Name Service	0.0	3	0.0	204	0	3	204	0
Multicast Domain Name System	0.1	122	0.1	70795	300	122	70795	300
Dynamic Host Configuration Protocol	0.0	2	0.0	848	3	2	848	3
Domain Name System	1.2	1325	0.1	105570	447	1325	105570	447
Transmission Control Protocol	47.5	53720	37.2	33722250	143 k	36336	21129113	89 k
Transport Layer Security	16.0	18054	35.9	32542977	138 k	17330	28591983	121 k
Hypertext Transfer Protocol	0.1	62	0.0	36712	155	24	8669	36
Online Certificate Status Protocol	0.0	21	0.0	9769	41	21	9769	41
Line-based text data	0.0	1	0.0	194	0	1	194	0
Domain Name System	0.0	2	0.0	1036	4	2	1036	4
Data	0.0	6	0.0	8692	36	6	8692	36
Internet Control Message Protocol	0.0	3	0.0	108	0	3	108	0

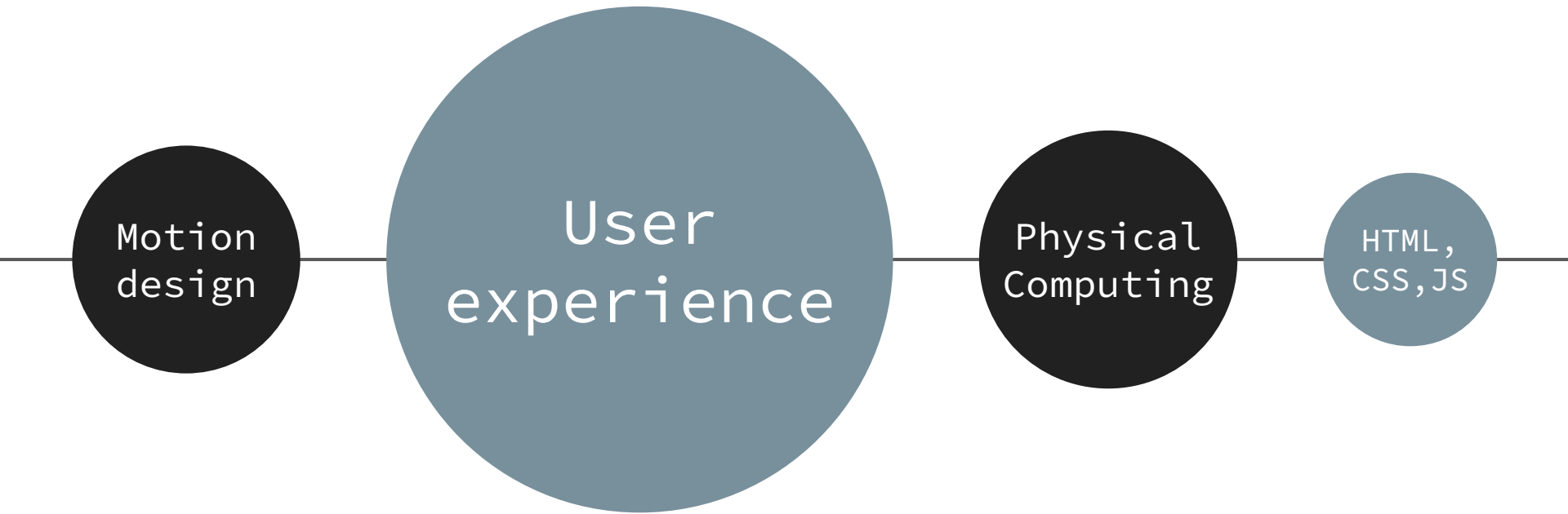
Display filter: ip.addr == 192.168.0.2

Help Copy Close

Your Name

Digital experience designer

Skills & expertise



Portfolio samples

Contact

Your Name

no_reply@example.com

www.example.com

