Capstone Part III

By : Leonard Sterling

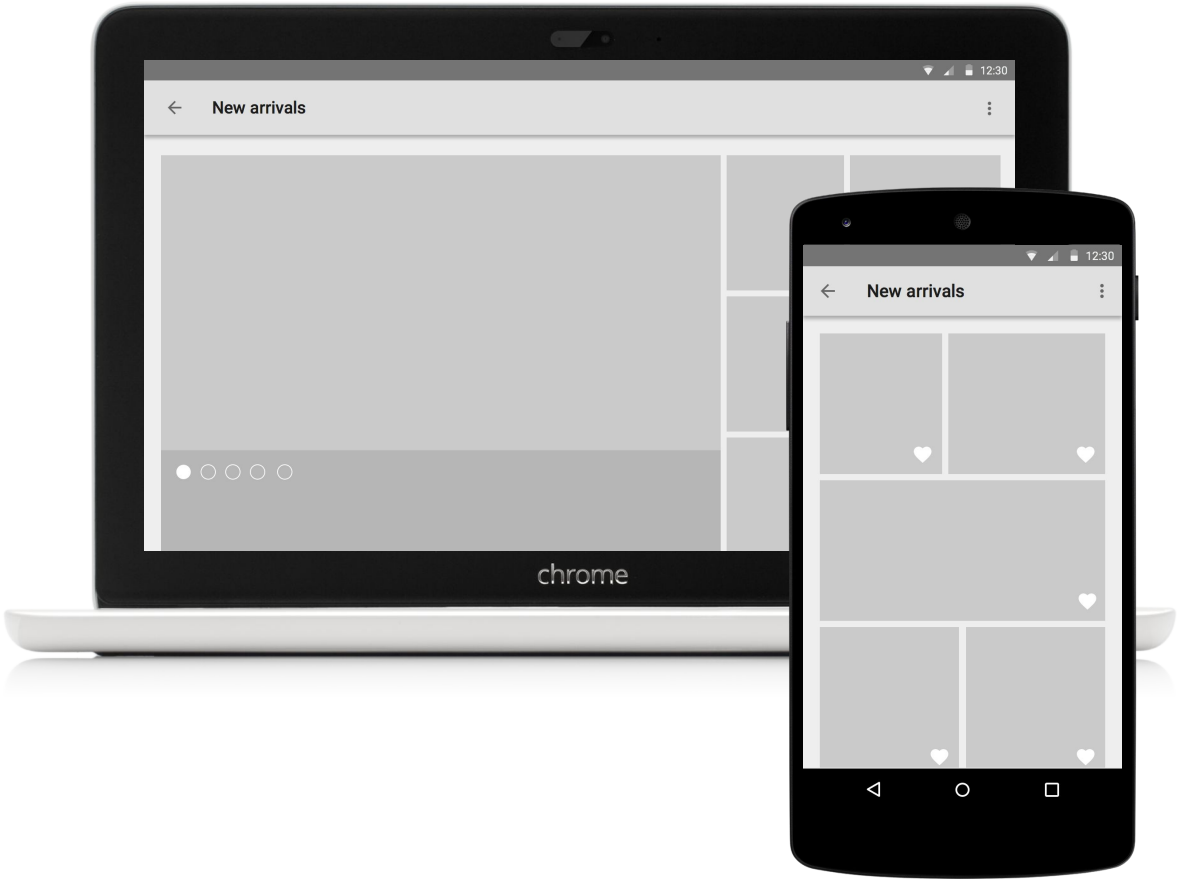
Overview: Network Analysis

Architecture

Network configuration

Performance monitoring

Security



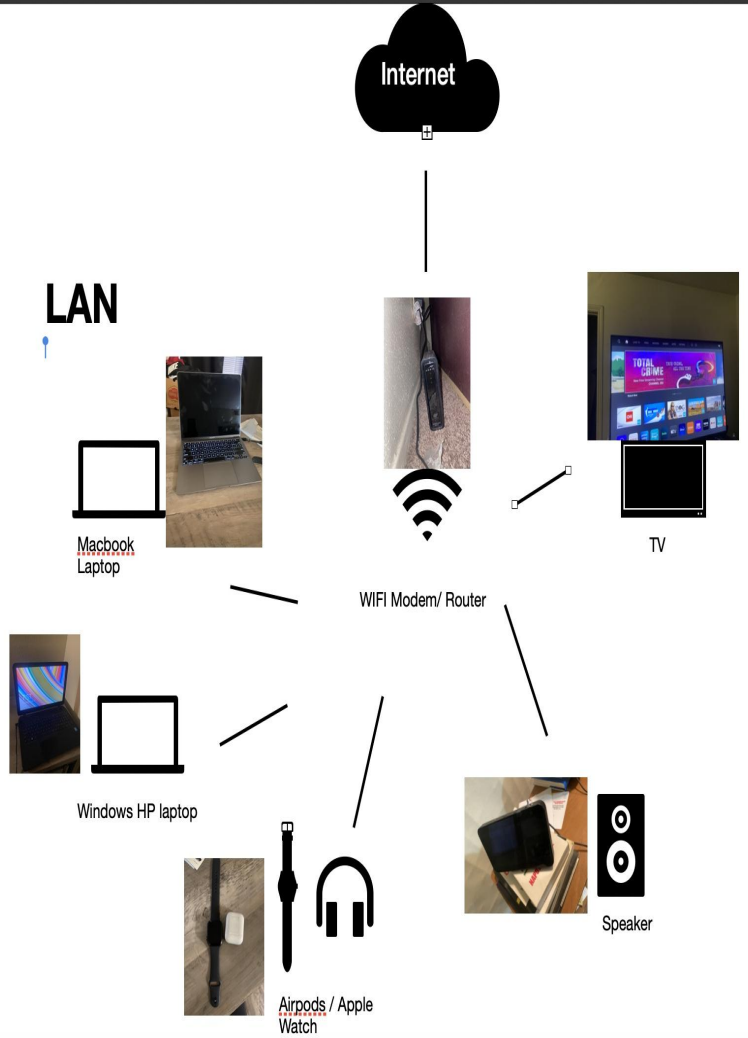
Architecture

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

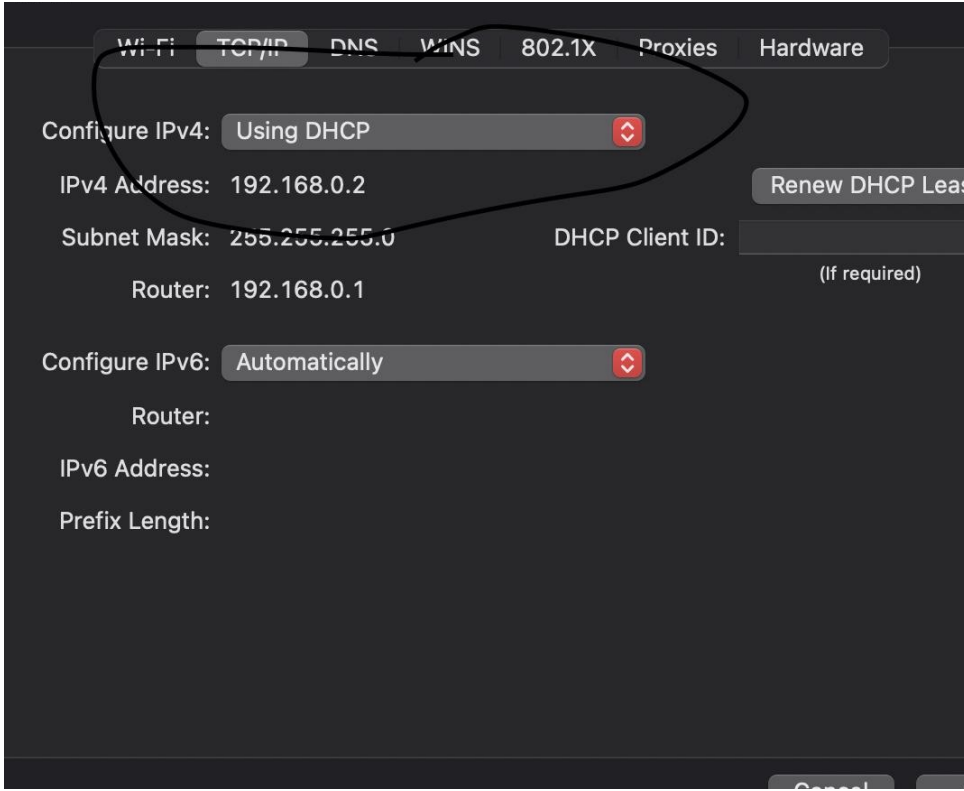
Apple Watch connects to the internet with a wireless connec:ons device same as a laptop. The smart tv connects to the internet using a wireless connec:ons as well has a built in wireless connec:on .the wireless Bluetooth speaker connects to the internet wireless with a built in component.



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

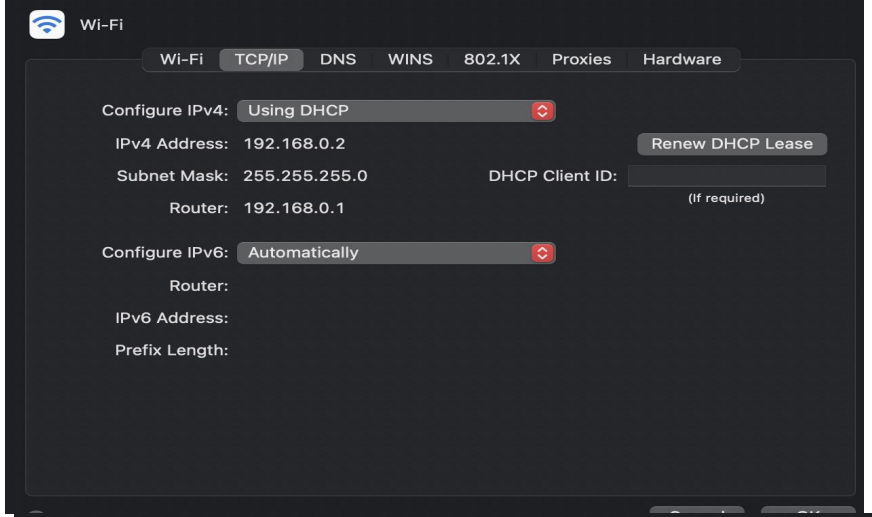
IP address 192.168.0.2

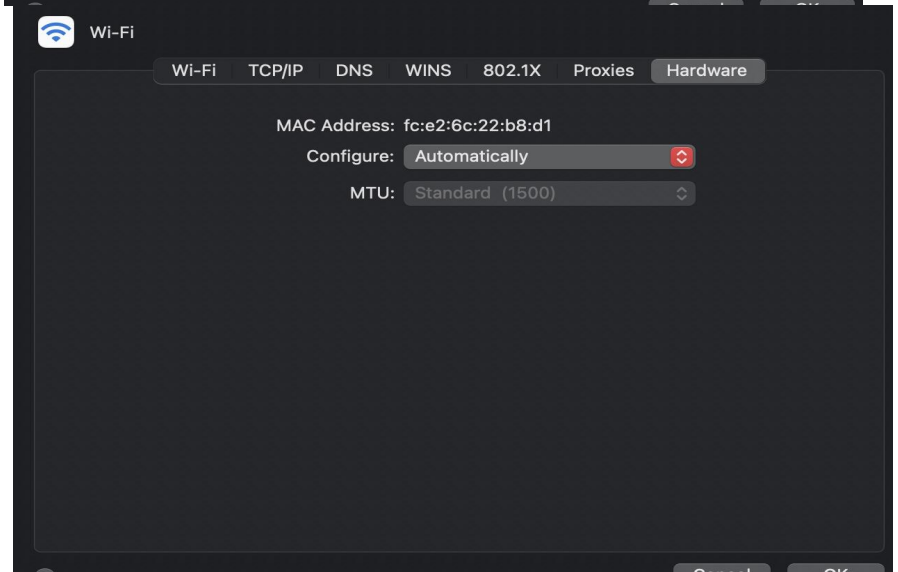
Subnet mask 255.255.255.0

Default gateway 192.168.0.1 (Router)

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

DNS informa:on 24.48.160.2 ,24.48.160.3
(Can be found in the DNS section)

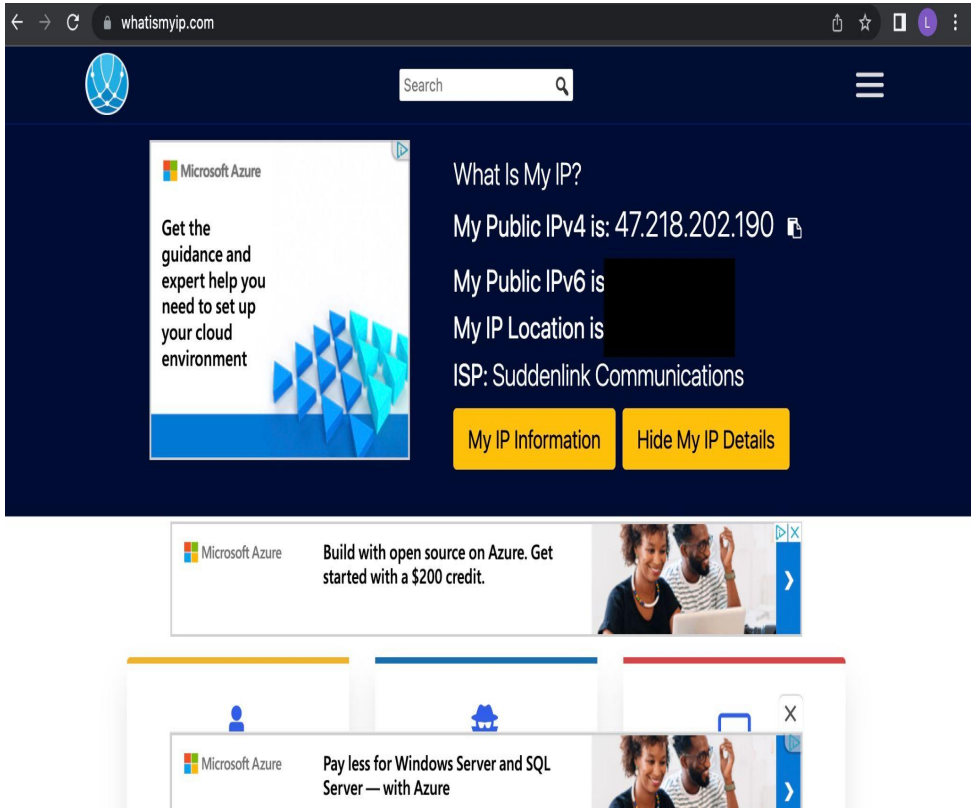




Network Configuration III

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.



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.

a similar tool complete the table to track your speeds.

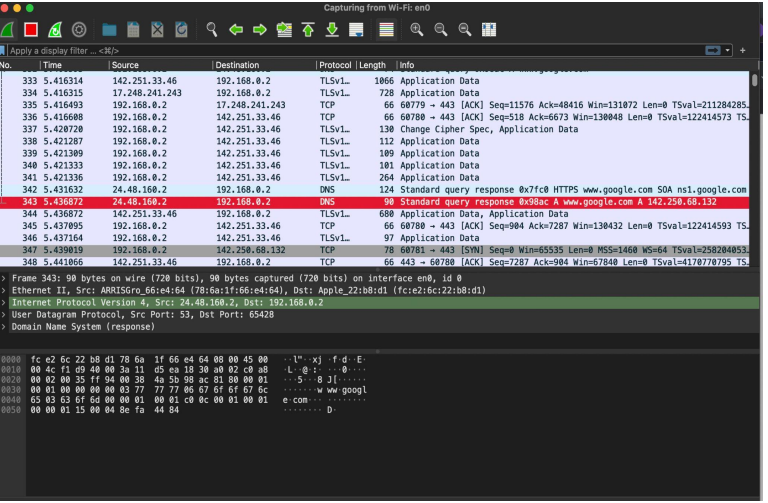
Test	Time Recorded	Upload Speed	Download Speed
Test 1	9:41 pm	11.95 mbps	7.43 mbps
Test 2	5:52 am	43.33mbps	90.24mbps
Test 3	4:59pm	36.69mbps	23.57mbps

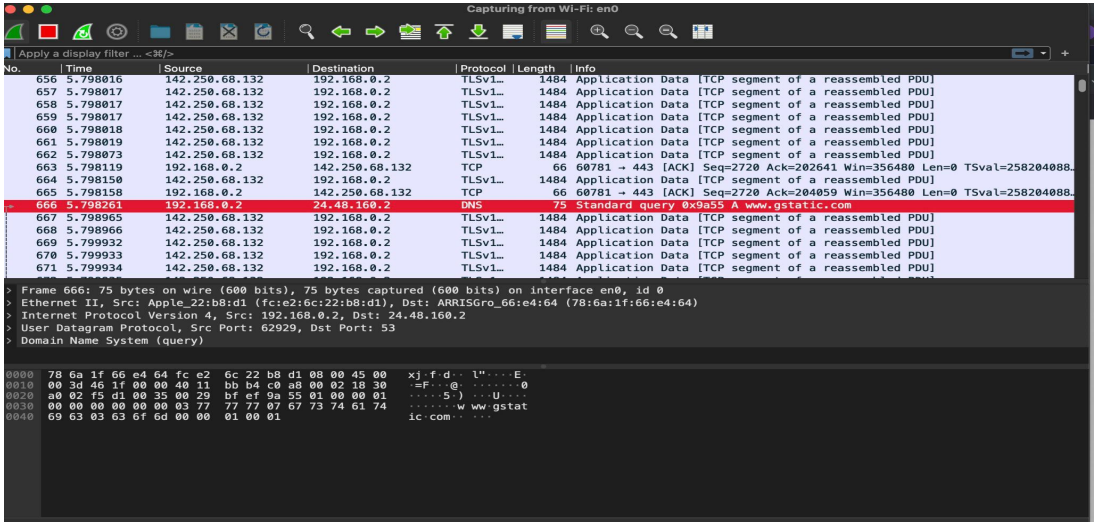
Bandwidth vs Throughput

When doing performance monitoring you need to know the difference between bandwidth and throughput. Bandwidth measures indirect related speed while throughout 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 a see the different sites that were visited at the time. Highlighted in red you can see the websites that were visited.

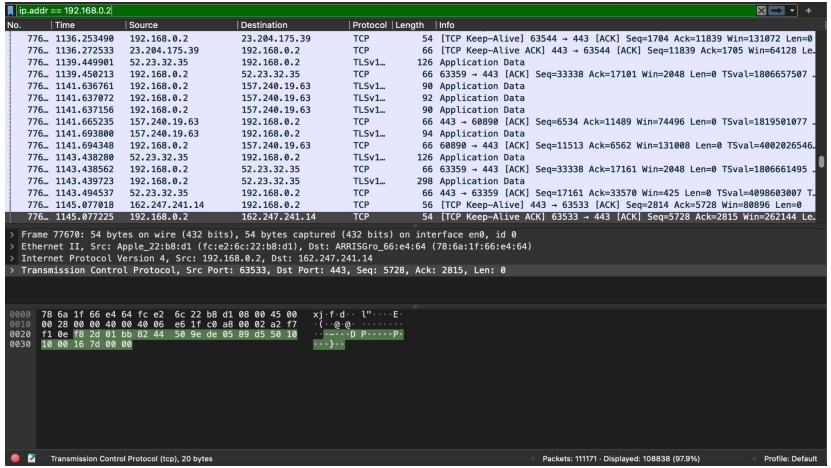


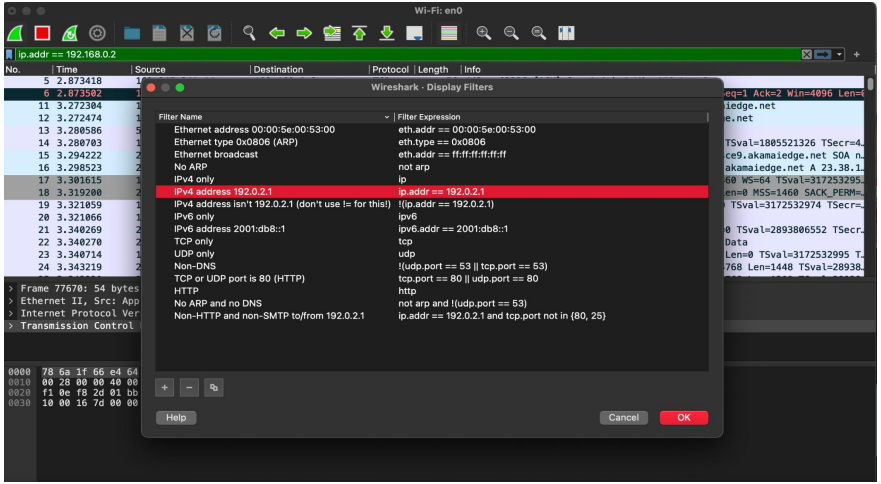


Network Capture II

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.

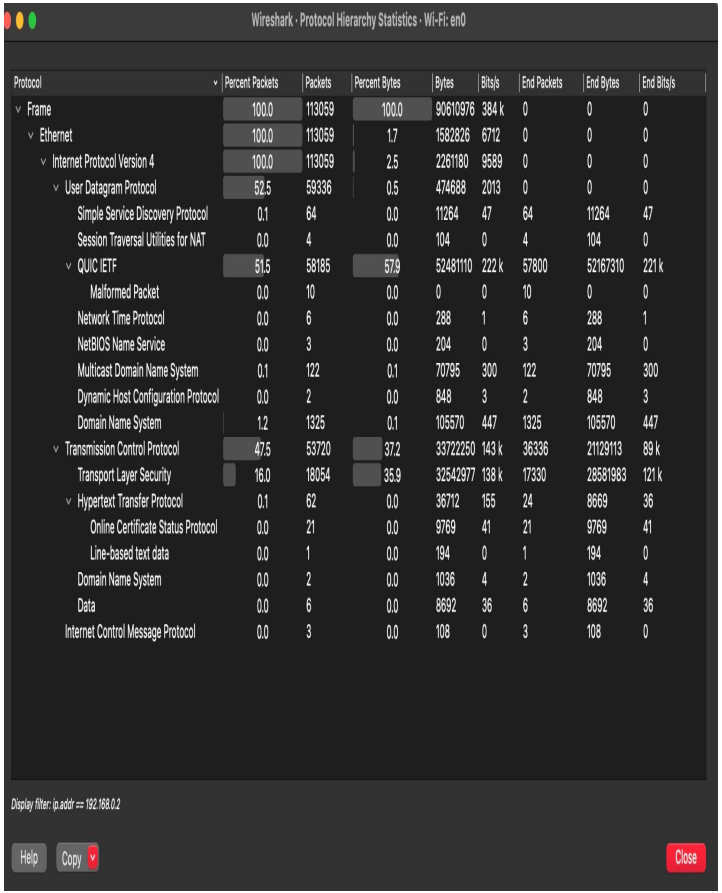
You can also go to statistics to capture filter to show only IPv4 only





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.

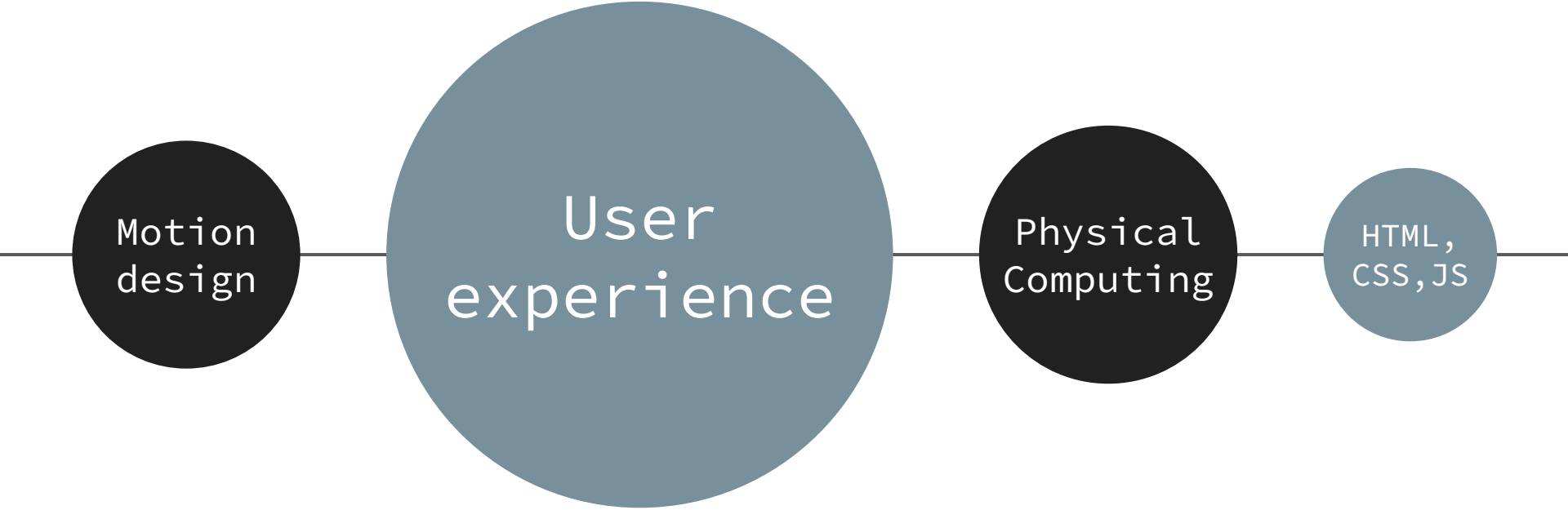


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	113059	100.0	90610976	384 k	0	0	0
Ethernet	100.0	113059	1.7	1582826	6712	0	0	0
Internet Protocol Version 4	100.0	113059	2.5	2261180	9589	0	0	0
User Datagram Protocol	52.5	59336	0.5	474688	2013	0	0	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	28581983	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

Your Name

Digital experience designer

Skills & expertise



Portfolio samples

Contact

Your Name
no_reply@example.com
www.example.com