

Exercises :

1. [Follow the instructions in this pdf tutorial.](#) Use Wireshark. Monitor the wireless interface instead of the Ethernet interface.

There are hundreds of filters available in Wireshark. Which three filters in the list might be the most useful to a network administrator? Explain.

- IP address filter
- Protocol filter
- Port filter

These filters provide network administrators with the ability to pinpoint relevant traffic quickly, facilitating effective network monitoring, troubleshooting, and security analysis. By leveraging these filters, administrators can gain insights into network behaviour, detect anomalies, and respond promptly to potential threats or performance issues.

tcp.port==80						
No.	Time	Source	Destination	Protocol	Length	Info
859	17:02:55	192.168.0.119	88.221.83.24	TCP	66	62450 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
861	17:02:55	88.221.83.24	192.168.0.119	TCP	66	80 → 62450 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
862	17:02:55	192.168.0.119	88.221.83.24	TCP	54	62450 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
863	17:02:55	192.168.0.119	88.221.83.24	HTTP	331	GET /appinfo/443030/sha/52654ce9696618c29975a6002c5495b2bb3ac389.txt.gz HTTP/1.1
864	17:02:55	88.221.83.24	192.168.0.119	TCP	56	80 → 62450 [ACK] Seq=1 Ack=278 Win=64128 Len=0
865	17:02:55	88.221.83.24	192.168.0.119	TCP	1514	80 → 62450 [ACK] Seq=1 Ack=278 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
866	17:02:55	88.221.83.24	192.168.0.119	TCP	1514	80 → 62450 [ACK] Seq=1461 Ack=278 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
867	17:02:55	88.221.83.24	192.168.0.119	HTTP	479	HTTP/1.1 200 OK (application/gzip)
868	17:02:55	192.168.0.119	88.221.83.24	TCP	54	62450 → 80 [ACK] Seq=278 Ack=3346 Win=131328 Len=0
2522	17:03:25	192.168.0.119	88.221.83.24	TCP	54	62450 → 80 [FIN, ACK] Seq=278 Ack=3346 Win=131328 Len=0
2523	17:03:26	88.221.83.24	192.168.0.119	TCP	54	80 → 62450 [FIN, ACK] Seq=3346 Ack=279 Win=64128 Len=0
2524	17:03:26	192.168.0.119	88.221.83.24	TCP	54	62450 → 80 [ACK] Seq=279 Ack=3347 Win=131328 Len=0