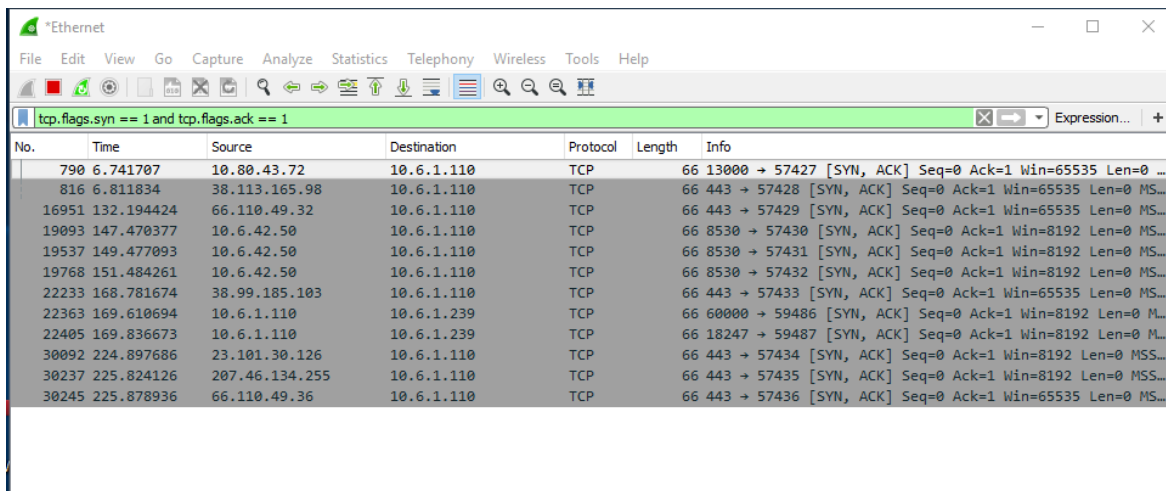


Wireshark Packet Project

- You will use Wireshark to display the network packets and place them into a word document **along with the specific command used to filter the results.**
- This information will be “print screened” and “cropped” onto a word document

Example:



The screenshot shows the Wireshark interface with a packet capture filter applied: `tcp.flags.syn == 1 and tcp.flags.ack == 1`. The packet list pane displays the following data:

No.	Time	Source	Destination	Protocol	Length	Info
790	6.741707	10.80.43.72	10.6.1.110	TCP	66	13000 → 57427 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 ...
816	6.811834	38.113.165.98	10.6.1.110	TCP	66	443 → 57428 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS...
16951	132.194424	66.110.49.32	10.6.1.110	TCP	66	443 → 57429 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS...
19093	147.470377	10.6.42.50	10.6.1.110	TCP	66	8530 → 57430 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS...
19537	149.477093	10.6.42.50	10.6.1.110	TCP	66	8530 → 57431 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS...
19768	151.484261	10.6.42.50	10.6.1.110	TCP	66	8530 → 57432 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS...
22233	168.781674	38.99.185.103	10.6.1.110	TCP	66	443 → 57433 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS...
22363	169.610694	10.6.1.110	10.6.1.239	TCP	66	60000 → 59486 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 M...
22405	169.836673	10.6.1.110	10.6.1.239	TCP	66	18247 → 59487 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 M...
30092	224.897686	23.101.30.126	10.6.1.110	TCP	66	443 → 57434 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS...
30237	225.824126	207.46.134.255	10.6.1.110	TCP	66	443 → 57435 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS...
30245	225.878936	66.110.49.36	10.6.1.110	TCP	66	443 → 57436 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS...

1. Filter TCP packets from your default gateway at port 80:
2. Filter SYN Flags only:
3. Filter SYN and ACK flags only:
4. Filter all packets that are not from your IP address:
5. Filter all packets that are from source TCP port 80 or 443:
6. Identify at least 4 Websites from the network traffic: