SCS2205 – Computer Networks I

21002241 – R.B. Wimalasena

Wireshark Tutorial

Start Wireshark using the terminal/command prompt and start capturing packets

```
C:\Users\Rusara>start wireshark

C:\Users\Rusara>

 ** (wireshark:3288) 00:48:17.191632 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:3288) 00:48:17.400586 [Capture MESSAGE] -- Capture started
 ** (wireshark:3288) 00:48:17.400956 [Capture MESSAGE] -- File: "C:\Users\Rusara\AppData\Local\Temp\wireshark_Wi-FiD3ZIA2.pcapng"
```

Capture packets on Wireshark while browsing different websites

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
7849	159.679539	192.168.1.9	8.8.8.8	TCP	66	[TCP Retransmission] 60026 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7850	159.679545	192.168.1.9	8.8.8.8	TCP	66	[TCP Retransmission] 60025 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7851	159.680599	2620:1ec:c11::200	2402:d000:813c:1c71…	TCP	74	443 → 60056 [ACK] Seq=5473 Ack=743 Win=4194304 Len=0
7852	159.680987	2620:1ec:c11::200	2402:d000:813c:1c71…	TLSv1.2	416	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
7853	159.681221	2620:1ec:c11::200	2402:d000:813c:1c71…	TLSv1.2	143	Application Data
7854	159.681237	2402:d000:813c:1c71…	2620:1ec:c11::200	TCP	74	60056 → 443 [ACK] Seq=743 Ack=5884 Win=65280 Len=0
7855	159.692208	2600:140f:4::17da:f…	2402:d000:813c:1c71…	TCP	74	443 → 60058 [ACK] Seq=265 Ack=677 Win=64256 Len=0
7856	159.692362	2600:140f:4::17da:f…	2402:d000:813c:1c71…	TLSv1.3	345	Application Data
7857	159.742168	2402:d000:813c:1c71…	2600:140f:4::17da:f…	TCP	74	60058 → 443 [ACK] Seq=677 Ack=536 Win=65792 Len=0
7858	159.788621	2402:d000:813c:1c71…	64:ff9b::681a:d06	TCP	75	[TCP Keep-Alive] 59634 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1
7859	159.793426	64:ff9b::681a:d06	2402:d000:813c:1c71…	TCP	86	[TCP Keep-Alive ACK] 443 → 59634 [ACK] Seq=1 Ack=2 Win=8 Len=0 SLE=1 SRE=2
7860	159.855032	fe80::1	ff05::c	SSDP	189	M-SEARCH * HTTP/1.1
7861	159.928631	192.168.1.9	8.8.8.8	TCP	66	[TCP Retransmission] 60031 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7862	160.037078	2402:d000:813c:1c71…	2620:1ec:12::239	TCP	75	[TCP Keep-Alive] 59981 → 443 [ACK] Seq=750 Ack=4570 Win=65792 Len=1
7863	160.085576	2620:1ec:12::239	2402:d000:813c:1c71…	TCP	86	[TCP Keep-Alive ACK] 443 → 59981 [ACK] Seq=4570 Ack=751 Win=4194048 Len=0 SLE=750 SRE=751
7864	160.117391	fe80::1	ff05::c	SSDP	189	M-SEARCH * HTTP/1.1
7865	160.370676	2600:140f:4::17da:f…	2402:d000:813c:1c71…	TLSv1.3	113	Application Data
7866	160.370810	2600:140f:4::17da:f…	2402:d000:813c:1c71…	TLSv1.3	98	Application Data
7867	160.370836	2402:d000:813c:1c71…	2600:140f:4::17da:f…	TCP	74	60020 → 443 [ACK] Seq=676 Ack=599 Win=65536 Len=0
7868	160.371528	2600:140f:4::17da:f…	2402:d000:813c:1c71…	TLSv1.3	113	Application Data

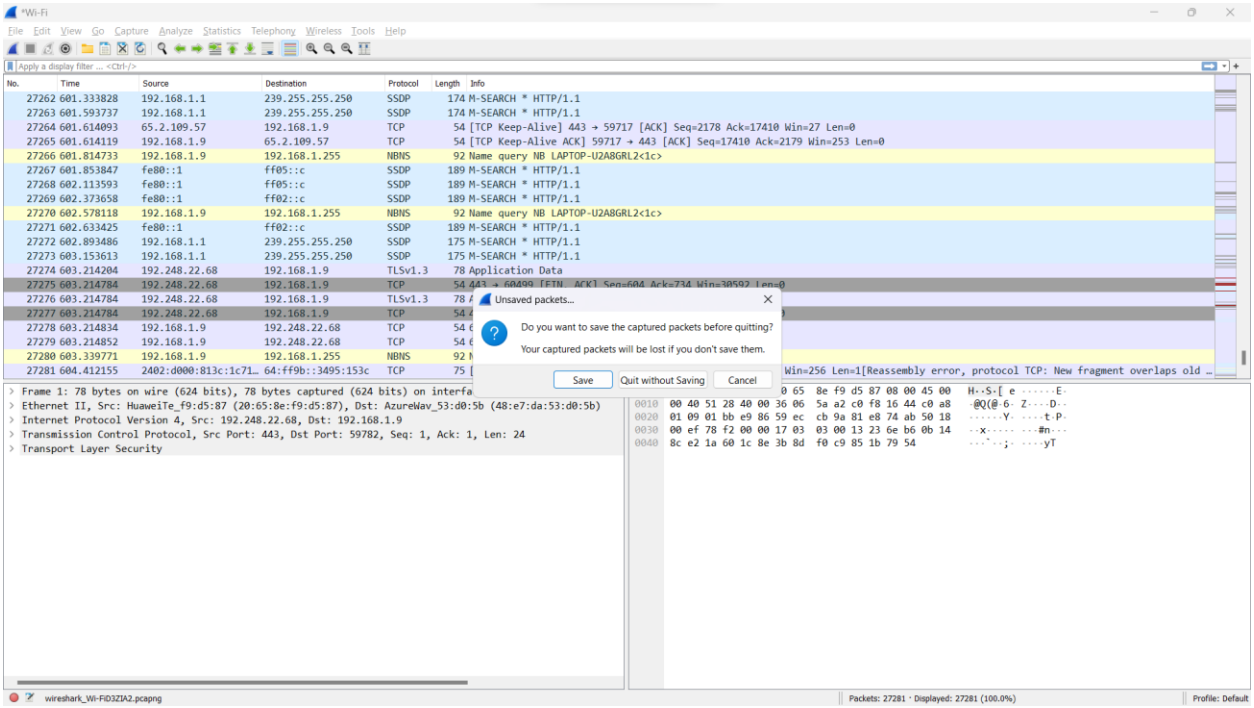
Capturing packets on Wireshark pinging from terminal/command prompt to 8.8.8.8

8784	276.206232	192.168.1.9	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 8785)
8785	276.255695	8.8.8.8	192.168.1.9	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=54 (request in 8784)
8786	277.211899	192.168.1.9	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 8787)
8787	277.257211	8.8.8.8	192.168.1.9	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=54 (request in 8786)
8788	278.228348	192.168.1.9	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 8789)
8789	278.273673	8.8.8.8	192.168.1.9	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=54 (request in 8788)
8790	279.243012	192.168.1.9	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 8791)
8791	279.327716	8.8.8.8	192.168.1.9	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=54 (request in 8790)

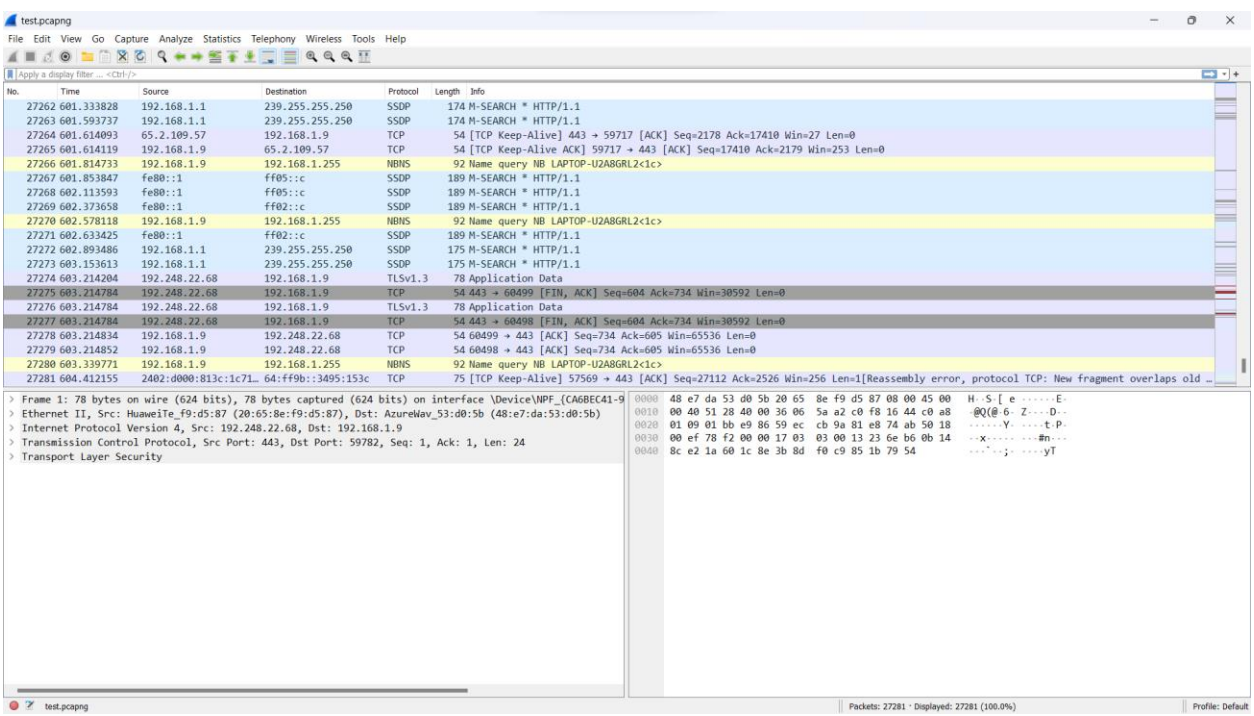
Navigate to https://ucsc.cmb.ac.lk/ and https://ugvle.ucsc.cmb.ac.lk/ using the web browser

26034	548.554590	192.168.1.9	40.126.16.166	TCP	54	60480 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
26035	548.555238	192.168.1.9	40.126.16.166	TLSv1.2	283	Client Hello
26036	548.667217	40.126.16.166	192.168.1.9	TCP	1466	443 → 60480 [ACK] Seq=1 Ack=230 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
26037	548.667653	40.126.16.166	192.168.1.9	TCP	1466	443 → 60480 [ACK] Seq=1413 Ack=230 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
26038	548.667672	192.168.1.9	40.126.16.166	TCP	54	60480 → 443 [ACK] Seq=230 Ack=2825 Win=66304 Len=0
26039	548.668030	40.126.16.166	192.168.1.9	TLSv1.2	1183	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
26040	548.670660	192.168.1.9	40.126.16.166	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
26041	548.774917	40.126.16.166	192.168.1.9	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
26042	548.775576	192.168.1.9	40.126.16.166	TLSv1.2	353	Application Data
26043	548.775633	192.168.1.9	40.126.16.166	TCP	1466	60480 → 443 [ACK] Seq=687 Ack=4005 Win=65024 Len=1412 [TCP segment of a reassembled PDU]
26044	548.775633	192.168.1.9	40.126.16.166	TCP	1466	60480 → 443 [ACK] Seq=2099 Ack=4005 Win=65024 Len=1412 [TCP segment of a reassembled PDU]
26045	548.775633	192.168.1.9	40.126.16.166	TCP	1466	60480 → 443 [ACK] Seq=3511 Ack=4005 Win=65024 Len=1412 [TCP segment of a reassembled PDU]
26046	548.775633	192.168.1.9	40.126.16.166	TCP	1466	60480 → 443 [ACK] Seq=4923 Ack=4005 Win=65024 Len=1412 [TCP segment of a reassembled PDU]
26047	548.775633	192.168.1.9	40.126.16.166	TLSv1.2	1446	Application Data
26048	548.880840	40.126.16.166	192.168.1.9	TCP	56	443 → 60480 [ACK] Seq=4005 Ack=7727 Win=4194816 Len=0
26049	548.957949	2402:d000:813c:1c71…	2404:6800:4003:c01:…	TCP	75	[TCP Keep-Alive] 60180 → 443 [ACK] Seq=1765 Ack=12793 Win=65536 Len=1
26050	548.996940	2404:6800:4003:c01:…	2402:d000:813c:1c71…	TCP	86	[TCP Keep-Alive ACK] 443 → 60180 [ACK] Seq=12793 Ack=1766 Win=67840 Len=0 SLE=1765 SRE=1766
26051	549.047938	40.126.16.166	192.168.1.9	TCP	1466	443 → 60480 [ACK] Seq=4005 Ack=7727 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
26052	549.048047	40.126.16.166	192.168.1.9	TCP	1466	443 → 60480 [ACK] Seq=5417 Ack=7727 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]

Stop capturing packets in Wireshark and save the captured packets to a pcap file for later use

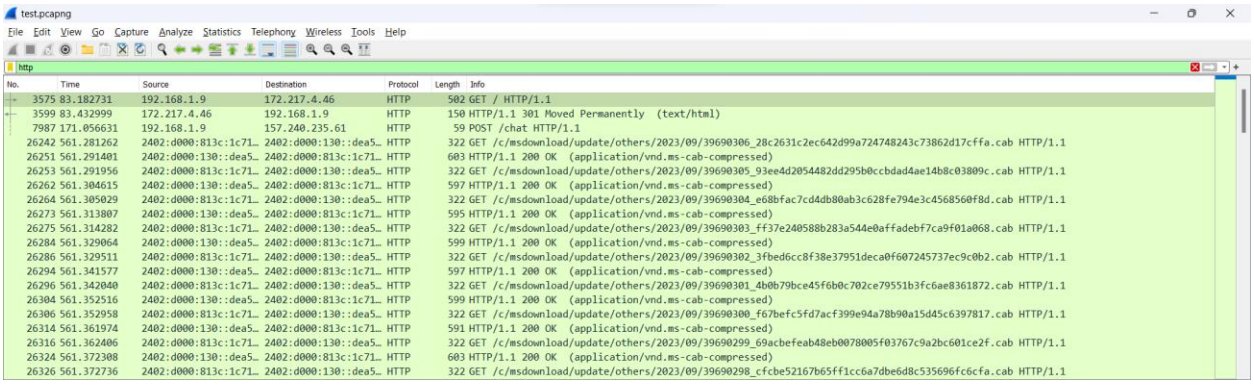


Open the saved pcap file from Wireshark (test.pcapng)

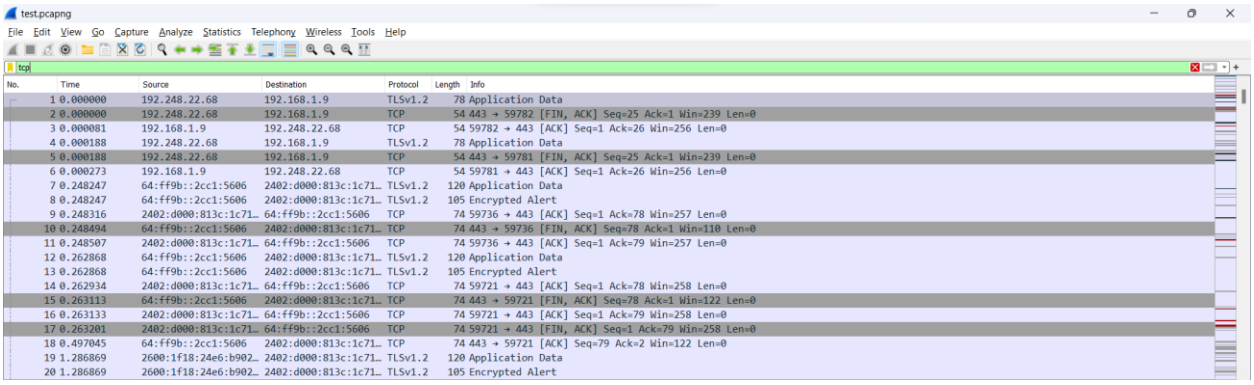


Check whether the packets exist under following protocols

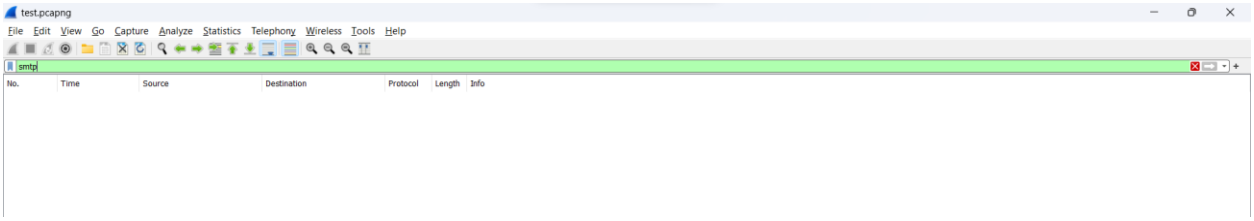
HTTP



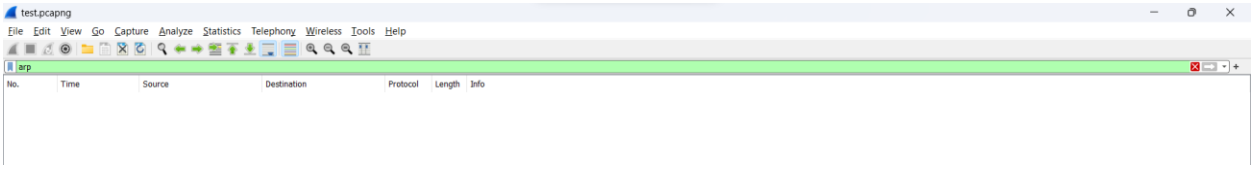
TCP



SMTP



ARP



Identify sender and target's MAC and IP addresses

```
> Ethernet II, Src: HuaweiTe_f9:d5:87 (20:65:8e:f9:d5:87), Dst: AzureWav_53:d0:5b (48:e7:da:53:d0:5b)
> Internet Protocol Version 4, Src: 192.248.22.68, Dst: 192.168.1.9
```

Identify requests and responses to those requests

8784	276.206232	192.168.1.9	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 8785)
8785	276.255695	8.8.8.8	192.168.1.9	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=54 (request in 8784)
8786	277.211899	192.168.1.9	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 8787)
8787	277.257211	8.8.8.8	192.168.1.9	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=54 (request in 8786)
8788	278.228348	192.168.1.9	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 8789)
8789	278.273673	8.8.8.8	192.168.1.9	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=54 (request in 8788)
8790	279.243012	192.168.1.9	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 8791)
8791	279.327716	8.8.8.8	192.168.1.9	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=54 (request in 8790)

Finding packets originated from a particular IP address.ip.src== 192.248.22.56

ip.src==192.248.22.56

No.	Time	Source	Destination	Protocol	Length	Info
2759	50.154436	192.248.22.56	192.168.1.9	TCP	66	80 → 60734 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
2761	50.154750	192.248.22.56	192.168.1.9	TCP	66	80 → 60735 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
2763	50.157157	192.248.22.56	192.168.1.9	TCP	66	443 → 60736 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
2766	50.169844	192.248.22.56	192.168.1.9	TCP	54	443 → 60736 [ACK] Seq=1 Ack=576 Win=30464 Len=0
2767	50.174449	192.248.22.56	192.168.1.9	TLSv1.3	1466	Server Hello, Change Cipher Spec, Application Data
2768	50.175018	192.248.22.56	192.168.1.9	TCP	1466	443 → 60736 [ACK] Seq=1413 Ack=576 Win=30464 Len=1412 [TCP segment of a reassembled PDU]
2770	50.175925	192.248.22.56	192.168.1.9	TLSv1.3	662	Application Data, Application Data, Application Data
2774	50.184324	192.248.22.56	192.168.1.9	TCP	54	443 → 60736 [FIN, ACK] Seq=3433 Ack=606 Win=30464 Len=0
2776	50.184558	192.248.22.56	192.168.1.9	TCP	56	443 → 60736 [ACK] Seq=3434 Ack=607 Win=30464 Len=0
2785	50.192099	192.248.22.56	192.168.1.9	TCP	54	80 → 60734 [ACK] Seq=1 Ack=441 Win=30336 Len=0
2786	50.196479	192.248.22.56	192.168.1.9	HTTP	765	HTTP/1.1 303 See Other (text/html)
4029	55.198806	192.248.22.56	192.168.1.9	TCP	54	80 → 60734 [FIN, ACK] Seq=712 Ack=441 Win=30336 Len=0
14309	76.565078	192.248.22.56	192.168.1.9	TCP	54	80 → 60735 [FIN, ACK] Seq=1 Ack=2 Win=29312 Len=0
14311	76.565365	192.248.22.56	192.168.1.9	TCP	54	80 → 60734 [ACK] Seq=713 Ack=442 Win=30336 Len=0

Finding packets headed to a particular IP address.ip.dst== 192.248.22.125

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst==192.248.22.125

No.	Time	Source	Destination	Protocol	Length	Info

Finding packets exchanged from or to a particular IP address. ip.addr==192.168.100.2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.100.2

No.	Time	Source	Destination	Protocol	Length	Info

Finding packets headed to a particular IP address and to a particular TCP port. ip.dst==192.248.22.56 && tcp.port==80

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst_host==192.248.22.56&&tcp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
1435	17.917946	192.168.1.9	192.248.22.56	TCP	66	61147 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1436	17.918109	192.168.1.9	192.248.22.56	TCP	66	61148 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1438	17.929996	192.168.1.9	192.248.22.56	TCP	54	61148 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
1439	17.930238	192.168.1.9	192.248.22.56	HTTP	503	GET / HTTP/1.1
1441	17.930658	192.168.1.9	192.248.22.56	TCP	54	61147 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
1461	17.989130	192.168.1.9	192.248.22.56	TCP	54	61148 → 80 [ACK] Seq=450 Ack=712 Win=65536 Len=0
1816	22.947574	192.168.1.9	192.248.22.56	TCP	54	61148 → 80 [ACK] Seq=450 Ack=713 Win=65536 Len=0
1842	24.862947	192.168.1.9	192.248.22.56	TCP	54	61148 → 80 [FIN, ACK] Seq=450 Ack=713 Win=65536 Len=0
2092	49.884679	192.168.1.9	192.248.22.56	TCP	66	[TCP Dup ACK 1441#1] 61147 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0 SLE=0 SRE=1