

EXPERIMENT NO-9

CN-C32-2103167

Aim:-

Use Wireshark to understand the operation of TCP/IP layers:

- Ethernet layer: Frame header / Frame Sized.
- Data Link Layer: - MAC address; ARP.
(IP & MAC addressing)
- Network Layer: IP Packet.
- Transport layer: TCP Reset, TCP, handshake segments etc.

Application Layer: - DHCP, FTP, HTTP. header format.

Theory:-

Wireshark is a popular, open source network protocol analysis used for capturing and inspecting packets on a network. It is a powerful tool for network administrators, security professionals and students.

The objective of this experiment is to use Wireshark, a network protocol analysis, to capture and analyze network traffic to understand the operation of various layers of TCP/IP protocol suite.

1.) Ethernet layer.

This layer deals with frames, which are packets of data at the ethernet layer. One can observe the size of ethernet frames. One can observe the size of ethernet frames. One can observe the size of ethernet frames. Ethernet frames have headers containing information like source & destination MAC address.

2.) Data link layer

The data link layer deals with MAC addresses. Wireshark will show you the MAC addresses of the addresses of the devices communicating in network. Users can capture ARP packet to see how devices map IP addresses to MAC addresses.


3.) Network Layer

This layer involves a lot of processes. It involves IP packets. Wireshark displays IP headers with information like source & destination IP address. ~~Source~~ ICMP packet can be captured to observe network troubleshooting, messages, like ping request & replies.

Transport layers :-

CN - C32 - 2103/64

User can see which ports are used by application (eg:- web browsers, email, clients) for communication. By capturing TCP traffic, you can see three-way handshake process, which is how two devices establish a connect.

CP Tools


Source	No.	Time	Destination	Protocol	Length	Info
192.168.31.10	266	12.719752	204.79.197.203	TCP	54	49700 → 443 [ACK] Seq=518 Ack=2881 Win=132352 Len=0
204.79.197.203	267	12.719826	192.168.31.10	TCP	1494	443 → 49700 [ACK] Seq=2881 Ack=518 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
204.79.197.203	268	12.719957	192.168.31.10	TCP	1494	443 → 49700 [ACK] Seq=4321 Ack=518 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
192.168.31.10	269	12.719984	204.79.197.203	TCP	54	49700 → 443 [ACK] Seq=518 Ack=5761 Win=132352 Len=0
204.79.197.203	270	12.719991	192.168.31.10	TLSv1.2	251	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
192.168.31.10	271	12.765667	204.79.197.203	TCP	54	49700 → 443 [ACK] Seq=518 Ack=5958 Win=132096 Len=0
192.168.31.10	272	12.769267	203.212.24.46	DNS	71	Standard query 0xdeeb A ntp.msn.com
203.212.24.46	273	12.771620	192.168.31.10	DNS	146	Standard query response 0xdeeb A ntp.msn.com CNAME www.msn.com A 0003.a-msedge.net CNAME a-0003.a-msedge.net A 204.79.197.203
192.168.31.10	274	12.775409	204.79.197.203	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
192.168.31.10	275	12.776889	204.79.197.203	TLSv1.2	153	Application Data
192.168.31.10	276	12.777086	204.79.197.203	TLSv1.2	2099	Application Data
204.79.197.203	277	12.777365	192.168.31.10	TCP	60	443 → 49700 [ACK] Seq=5958 Ack=676 Win=4193792 Len=0
204.79.197.203	278	12.778875	192.168.31.10	TLSv1.2	396	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
204.79.197.203	279	12.778875	192.168.31.10	TLSv1.2	123	Application Data
192.168.31.10	280	12.778912	204.79.197.203	TCP	54	49700 → 443 [ACK] Seq=2820 Ack=6369 Win=131840 Len=0
204.79.197.203	281	12.778926	192.168.31.10	TCP	60	443 → 49700 [ACK] Seq=6369 Ack=775 Win=4193792 Len=0
192.168.31.10	282	12.779039	204.79.197.203	TLSv1.2	92	Application Data
204.79.197.203	283	12.779451	192.168.31.10	TLSv1.2	92	Application Data
204.79.197.203	284	12.779451	192.168.31.10	TCP	60	443 → 49700 [ACK] Seq=6407 Ack=2820 Win=4194048 Len=0
204.79.197.203	285	12.780927	192.168.31.10	TCP	60	443 → 49700 [ACK] Seq=6407 Ack=2858 Win=4194048 Len=0
192.168.31.10	286	12.828175	204.79.197.203	TCP	54	49700 → 443 [ACK] Seq=2858 Ack=6407 Win=131584 Len=0
204.79.197.203	288	12.926652	192.168.31.10	TCP	1494	443 → 49700 [ACK] Seq=6407 Ack=2858 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
204.79.197.203	289	12.926731	192.168.31.10	TCP	1494	443 → 49700 [ACK] Seq=7847 Ack=2858 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
192.168.31.10	290	12.926744	204.79.197.203	TCP	54	49700 → 443 [ACK] Seq=2858 Ack=9287 Win=132352 Len=0
204.79.197.203	291	12.926857	192.168.31.10	TCP	1494	443 → 49700 [ACK] Seq=9287 Ack=2858 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
204.79.197.203	292	12.927009	192.168.31.10	TCP	1494	443 → 49700 [ACK] Seq=10727 Ack=2858 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
192.168.31.10	293	12.927021	204.79.197.203	TCP	54	49700 → 443 [ACK] Seq=2858 Ack=12167 Win=132352 Len=0
204.79.197.203	294	12.927101	192.168.31.10	TCP	1494	443 → 49700 [ACK] Seq=12167 Ack=2858 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]

> Frame 221: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0
 > Ethernet II, Src: Micro-St_c2:99:72 (d8:bb:c1:c2:99:72), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
 > Internet Protocol Version 4, Src: 192.168.31.10, Dst: 224.0.0.22
 > Internet Group Management Protocol

The image shows a Wireshark packet capture of IGMPv3 traffic. The packet list pane displays five packets, with the 70th packet selected. The packet details pane shows the structure of the selected packet, which is an IGMPv3 Membership Report. The report includes a checksum, status, and three group records, all of which have been changed to 'Exclude Mode'.

Source	No.	Time	Destination	Protocol	Length	Info
169.254.190.1	202270	35.653162	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.251 for any sources
169.254.190.1	202271	35.653162	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
169.254.190.1	202290	35.655593	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources
169.254.190.1	205508	36.156458	224.0.0.22	IGMPv3	70	Membership Report / Join group 224.0.0.252 for any sources / Join group 224.0.0.251 for any sources / Join group 239.255.255.250
192.168.31.11	234053	40.552535	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
192.168.31.11	234104	40.561403	224.0.0.22	IGMPv3	60	Membership Report / Leave group 239.255.255.250

> Frame 205508: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0
 > Ethernet II, Src: Micro-St_e4:ef:8f (d8:bb:c1:e4:ef:8f), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
 > Internet Protocol Version 4, Src: 169.254.190.1, Dst: 224.0.0.22
 > Internet Group Management Protocol
 [IGMP Version: 3]
 Type: Membership Report (0x22)
 Reserved: 00
 Checksum: 0x2009 [correct]
 [Checksum Status: Good]
 Reserved: 0000
 Num Group Records: 3
 > Group Record : 224.0.0.252 Change To Exclude Mode
 > Group Record : 224.0.0.251 Change To Exclude Mode
 > Group Record : 239.255.255.250 Change To Exclude Mode

Wireshark packet capture showing ICMP Echo (ping) requests. The capture shows six packets, all of which are 'Destination unreachable (Port unreachable)'.

Source	No.	Time	Destination	Protocol	Length	Info
192.168.31.10	1136	6.937252	203.212.24.46	ICMP	204	Destination unreachable (Port unreachable)
192.168.31.10	2406	11.541414	203.212.24.46	ICMP	169	Destination unreachable (Port unreachable)
192.168.31.10	4004	13.003202	203.212.24.46	ICMP	176	Destination unreachable (Port unreachable)
192.168.31.10	4385	13.926884	203.212.24.46	ICMP	239	Destination unreachable (Port unreachable)
192.168.31.10	165592	31.196969	203.212.24.46	ICMP	347	Destination unreachable (Port unreachable)
192.168.31.10	289892	66.235611	203.212.24.46	ICMP	180	Destination unreachable (Port unreachable)

Details for packet 6 (165592):

- Frame 165592: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0
- Ethernet II, Src: Micro-St_c2:99:72 (d8:bb:c1:c2:99:72), Dst: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19)
- Internet Protocol Version 4, Src: 192.168.31.10, Dst: 203.212.24.46
- Internet Control Message Protocol
 - Type: 3 (Destination unreachable)
 - Code: 3 (Port unreachable)
 - Checksum: 0xc1e0 [correct]
 - [Checksum Status: Good]
 - Unused: 00000000
- Internet Protocol Version 4, Src: 203.212.24.46, Dst: 192.168.31.10
- User Datagram Protocol, Src Port: 53, Dst Port: 53854
- Domain Name System (response)

4. Address Resolution Protocol (ARP)

File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help

arp

Source	No.	Time	Destination	Protocol	Length	Info
9c:53:22:05:6a:19	264869	45.548152	Broadcast	ARP	60	Who has 192.168.31.37? Tell 192.168.31.1
Micro-St_e4:ef:8f	265469	45.650649	Broadcast	ARP	60	ARP Announcement for 192.168.31.11
Micro-St_c2:99:72	265644	45.678832	Micro-St_c2:9a:72	ARP	42	Who has 192.168.31.21? Tell 192.168.31.10
Micro-St_c2:9a:72	268408	46.126503	Micro-St_c2:99:72	ARP	60	192.168.31.21 is at d8:bb:c1:c2:9a:72
9c:53:22:05:6a:19	268744	46.182324	Broadcast	ARP	60	Who has 192.168.31.5? Tell 192.168.31.1
Dell_a5:05:b6	276786	47.419387	Broadcast	ARP	60	Who has 192.168.31.1? Tell 192.168.31.37
Dell_a5:05:b6	277230	47.491097	Broadcast	ARP	60	Who has 192.168.31.37? (ARP Probe)
Dell_a5:05:b6	278451	47.679929	Broadcast	ARP	60	Who has 192.168.31.1? Tell 192.168.31.37
Dell_a5:05:b6	283428	48.491127	Broadcast	ARP	60	Who has 192.168.31.37? (ARP Probe)
Dell_a5:05:b6	288875	49.490832	Broadcast	ARP	60	Who has 192.168.31.37? (ARP Probe)

> Frame 276786: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0

> Ethernet II, Src: Dell_a5:05:b6 (54:bf:64:a5:05:b6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: Dell_a5:05:b6 (54:bf:64:a5:05:b6)

Sender IP address: 192.168.31.37

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.31.1

```

0000  ff ff ff ff ff ff 54 bf  64 a5 05 b6 08 06 00 01  .....T: d:.....
0010  08 00 06 04 00 01 54 bf  64 a5 05 b6 c0 a8 1f 25  .....T: d:.....%
0020  00 00 00 00 00 00 c0 a8  1f 01 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....

```

Address Resolution Protocol: Protocol
Packets: 298488 · Displayed: 122 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

5. Dynamic Host Configuration Protocol (DHCP)

[illegible]

6. Domain Name System (DNS)

Source	No.	Time	Destination	Protocol	Length	Info
203.212.24.46	4788	14.792727	192.168.31.10	DNS	273	Standard query response 0x7e0a A speedtest.bigventuresmedia.com.prod.hosts.ooklaserver.net CNAME speedtest.bigventuresmedia.com
192.168.31.10	4961	17.714059	203.212.24.46	DNS	82	Standard query 0x93fa A ipv6-api.speedtest.net
192.168.31.10	4962	17.714155	203.212.24.46	DNS	82	Standard query 0xd6bc HTTPS ipv6-api.speedtest.net
203.212.24.46	4963	17.718900	192.168.31.10	DNS	169	Standard query response 0xd6bc HTTPS ipv6-api.speedtest.net SOA ns-1643.awsdns-13.co.uk
203.212.24.46	4965	17.730163	192.168.31.10	DNS	169	Standard query response 0x93fa A ipv6-api.speedtest.net SOA ns-1643.awsdns-13.co.uk
192.168.31.10	4966	17.730744	203.212.24.46	DNS	82	Standard query 0xc7f4 A ipv6-api.speedtest.net
203.212.24.46	4967	17.732393	192.168.31.10	DNS	169	Standard query response 0xc7f4 A ipv6-api.speedtest.net SOA ns-1643.awsdns-13.co.uk
192.168.31.10	32845	20.498282	203.212.24.46	DNS	83	Standard query 0x2fbb A ctldl.windowsupdate.com
203.212.24.46	33034	20.513474	192.168.31.10	DNS	242	Standard query response 0x2fbb A ctldl.windowsupdate.com CNAME wu-bg-shim.trafficmanager.net CNAME download.windowsupdate.com
192.168.31.10	61693	22.811315	203.212.24.46	DNS	79	Standard query 0x714e A download.lenovo.com

> Frame 4967: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0

> Ethernet II, Src: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19), Dst: Micro-St_c2:99:72 (d8:bb:c1:c2:99:72)

> Internet Protocol Version 4, Src: 203.212.24.46, Dst: 192.168.31.10

> User Datagram Protocol, Src Port: 53, Dst Port: 53854

> Domain Name System (response)

Transaction ID: 0xc7f4

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 0

> Queries

> Authoritative nameservers

[Request in: 4966]

[Time: 0.001649000 seconds]

7. Hypertext Transfer Protocol (HTTP)

Source	No.	Time	Destination	Protocol	Length	Info
192.168.31.10	298069	98.556072	192.168.31.1	HTTP/X	363	POST /ifc HTTP/1.1
192.168.31.1	298104	98.558649	192.168.31.10	HTTP/X	406	HTTP/1.1 200 OK
192.168.31.10	298165	98.562941	192.168.31.1	HTTP/X	367	POST /ifc HTTP/1.1
192.168.31.1	298217	98.567233	192.168.31.10	HTTP/X	422	HTTP/1.1 200 OK
14.104.35.123	298410	98.582406	192.168.31.10	HTTP	1084	HTTP/1.1 206 Partial Content
192.168.31.10	298415	98.584567	192.168.31.1	HTTP/X	363	POST /ifc HTTP/1.1

> Frame 298410: 1084 bytes on wire (8672 bits), 1084 bytes captured (8672 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0

> Ethernet II, Src: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19), Dst: Micro-St_c2:99:72 (d8:bb:c1:c2:99:72)

> Internet Protocol Version 4, Src: 14.104.35.123, Dst: 192.168.31.10

> Transmission Control Protocol, Src Port: 80, Dst Port: 51270, Seq: 5419490, Ack: 6104, Len: 1030

> [247 Reassembled TCP Segments (355270 bytes): #298017(1440), #298018(1440), #298019(1440), #298020(1440), #298021(1440), #298022(1440), #298023(1440), #298025(1440), #298027(1440), #298028(1440), #298029(1440), #298030(1440), #298031(1440), #298032(1440), #298033(1440), #298034(1440), #298035(1440), #298036(1440), #298037(1440), #298038(1440), #298039(1440), #298040(1440), #298041(1440), #298042(1440), #298043(1440), #298044(1440), #298045(1440), #298046(1440), #298047(1440), #298048(1440), #298049(1440), #298050(1440), #298051(1440), #298052(1440), #298053(1440), #298054(1440), #298055(1440), #298056(1440), #298057(1440), #298058(1440), #298059(1440), #298060(1440), #298061(1440), #298062(1440), #298063(1440), #298064(1440), #298065(1440), #298066(1440), #298067(1440), #298068(1440), #298069(1440), #298070(1440), #298071(1440), #298072(1440), #298073(1440), #298074(1440), #298075(1440), #298076(1440), #298077(1440), #298078(1440), #298079(1440), #298080(1440), #298081(1440), #298082(1440), #298083(1440), #298084(1440), #298085(1440), #298086(1440), #298087(1440), #298088(1440), #298089(1440), #298090(1440), #298091(1440), #298092(1440), #298093(1440), #298094(1440), #298095(1440), #298096(1440), #298097(1440), #298098(1440), #298099(1440), #298100(1440), #298101(1440), #298102(1440), #298103(1440), #298104(1440), #298105(1440), #298106(1440), #298107(1440), #298108(1440), #298109(1440), #298110(1440), #298111(1440), #298112(1440), #298113(1440), #298114(1440), #298115(1440), #298116(1440), #298117(1440), #298118(1440), #298119(1440), #298120(1440), #298121(1440), #298122(1440), #298123(1440), #298124(1440), #298125(1440), #298126(1440), #298127(1440), #298128(1440), #298129(1440), #298130(1440), #298131(1440), #298132(1440), #298133(1440), #298134(1440), #298135(1440), #298136(1440), #298137(1440), #298138(1440), #298139(1440), #298140(1440), #298141(1440), #298142(1440), #298143(1440), #298144(1440), #298145(1440), #298146(1440), #298147(1440), #298148(1440), #298149(1440), #298150(1440), #298151(1440), #298152(1440), #298153(1440), #298154(1440), #298155(1440), #298156(1440), #298157(1440), #298158(1440), #298159(1440), #298160(1440), #298161(1440), #298162(1440), #298163(1440), #298164(1440), #298165(1440), #298166(1440), #298167(1440), #298168(1440), #298169(1440), #298170(1440), #298171(1440), #298172(1440), #298173(1440), #298174(1440), #298175(1440), #298176(1440), #298177(1440), #298178(1440), #298179(1440), #298180(1440), #298181(1440), #298182(1440), #298183(1440), #298184(1440), #298185(1440), #298186(1440), #298187(1440), #298188(1440), #298189(1440), #298190(1440), #298191(1440), #298192(1440), #298193(1440), #298194(1440), #298195(1440), #298196(1440), #298197(1440), #298198(1440), #298199(1440), #298200(1440), #298201(1440), #298202(1440), #298203(1440), #298204(1440), #298205(1440), #298206(1440), #298207(1440), #298208(1440), #298209(1440), #298210(1440), #298211(1440), #298212(1440), #298213(1440), #298214(1440), #298215(1440), #298216(1440), #298217(1440), #298218(1440), #298219(1440), #298220(1440), #298221(1440), #298222(1440), #298223(1440), #298224(1440), #298225(1440), #298226(1440), #298227(1440), #298228(1440), #298229(1440), #298230(1440), #298231(1440), #298232(1440), #298233(1440), #298234(1440), #298235(1440), #298236(1440), #298237(1440), #298238(1440), #298239(1440), #298240(1440), #298241(1440), #298242(1440), #298243(1440), #298244(1440), #298245(1440), #298246(1440), #298247(1440), #298248(1440), #298249(1440), #298250(1440), #298251(1440), #298252(1440), #298253(1440), #298254(1440), #298255(1440), #298256(1440), #298257(1440), #298258(1440), #298259(1440), #298260(1440), #298261(1440), #298262(1440), #298263(1440), #298264(1440), #298265(1440), #298266(1440), #298267(1440), #298268(1440), #298269(1440), #298270(1440), #298271(1440), #298272(1440), #298273(1440), #298274(1440), #298275(1440), #298276(1440), #298277(1440), #298278(1440), #298279(1440), #298280(1440), #298281(1440), #298282(1440), #298283(1440), #298284(1440), #298285(1440), #298286(1440), #298287(1440), #298288(1440), #298289(1440), #298290(1440), #298291(1440), #298292(1440), #298293(1440), #298294(1440), #298295(1440), #298296(1440), #298297(1440), #298298(1440), #298299(1440), #298300(1440), #298301(1440), #298302(1440), #298303(1440), #298304(1440), #298305(1440), #298306(1440), #298307(1440), #298308(1440), #298309(1440), #298310(1440), #298311(1440), #298312(1440), #298313(1440), #298314(1440), #298315(1440), #298316(1440), #298317(1440), #298318(1440), #298319(1440), #298320(1440), #298321(1440), #298322(1440), #298323(1440), #298324(1440), #298325(1440), #298326(1440), #298327(1440), #298328(1440), #298329(1440), #298330(1440), #298331(1440), #298332(1440), #298333(1440), #298334(1440), #298335(1440), #298336(1440), #298337(1440), #298338(1440), #298339(1440), #298340(1440), #298341(1440), #298342(1440), #298343(1440), #298344(1440), #298345(1440), #298346(1440), #298347(1440), #298348(1440), #298349(1440), #298350(1440), #298351(1440), #298352(1440), #298353(1440), #298354(1440), #298355(1440), #298356(1440), #298357(1440), #298358(1440), #298359(1440), #298360(1440), #298361(1440), #298362(1440), #298363(1440), #298364(1440), #298365(1440), #298366(1440), #298367(1440), #298368(1440), #298369(1440), #298370(1440), #298371(1440), #298372(1440), #298373(1440), #298374(1440), #298375(1440), #298376(1440), #298377(1440), #298378(1440), #298379(1440), #298380(1440), #298381(1440), #298382(1440), #298383(1440), #298384(1440), #298385(1440), #298386(1440), #298387(1440), #298388(1440), #298389(1440), #298390(1440), #298391(1440), #298392(1440), #298393(1440), #298394(1440), #298395(1440), #298396(1440), #298397(1440), #298398(1440), #298399(1440), #298400(1440), #298401(1440), #298402(1440), #298403(1440), #298404(1440), #298405(1440), #298406(1440), #298407(1440), #298408(1440), #298409(1440), #298410(1440), #298411(1440), #298412(1440), #298413(1440), #298414(1440), #298415(1440), #298416(1440), #298417(1440), #298418(1440), #298419(1440), #298420(1440), #298421(1440), #298422(1440), #298423(1440), #298424(1440), #298425(1440), #298426(1440), #298427(1440), #298428(1440), #298429(1440), #298430(1440), #298431(1440), #298432(1440), #298433(1440), #298434(1440), #298435(1440), #298436(1440), #298437(1440), #298438(1440), #298439(1440), #298440(1440), #298441(1440), #298442(1440), #298443(1440), #298444(1440), #298445(1440), #298446(1440), #298447(1440), #298448(1440), #298449(1440), #298450(1440), #298451(1440), #298452(1440), #298453(1440), #298454(1440), #298455(1440), #298456(1440), #298457(1440), #298458(1440), #298459(1440), #298460(1440), #298461(1440), #298462(1440), #298463(1440), #298464(1440), #298465(1440), #298466(1440), #298467(1440), #298468(1440), #298469(1440), #298470(1440), #298471(1440), #298472(1440), #298473(1440), #298474(1440), #298475(1440), #298476(1440), #298477(1440), #298478(1440), #298479(1440), #298480(1440), #298481(1440), #298482(1440), #298483(1440), #298484(1440), #298485(1440), #298486(1440), #298487(1440), #298488(1440), #298489(1440), #298490(1440), #298491(1440), #298492(1440), #298493(1440), #298494(1440), #298495(1440), #298496(1440), #298497(1440), #298498(1440), #298499(1440), #298500(1440), #298501(1440), #298502(1440), #298503(1440), #298504(1440), #298505(1440), #298506(1440), #298507(1440), #298508(1440), #298509(1440), #298510(1440), #298511(1440), #298512(1440), #298513(1440), #298514(1440), #298515(1440), #298516(1440), #298517(1440), #298518(1440), #298519(1440), #298520(1440), #298521(1440), #298522(1440), #298523(1440), #298524(1440), #298525(1440), #298526(1440), #298527(1440), #298528(1440), #298529(1440), #298530(1440), #298531(1440), #298532(1440), #298533(1440), #298534(1440), #298535(1440), #298536(1440), #298537(1440), #298538(1440), #298539(1440), #298540(1440), #298541(1440), #298542(1440), #298543(1440), #298544(1440), #298545(1440), #298546(1440), #298547(1440), #298548(1440), #298549(1440), #298550(1440), #298551(1440), #298552(1440), #298553(1440), #298554(1440), #298555(1440), #298556(1440), #298557(1440), #298558(1440), #298559(1440), #298560(1440), #298561(1440), #298562(1440), #298563(1440), #298564(1440), #298565(1440), #298566(1440), #298567(1440), #298568(1440), #298569(1440), #298570(1440), #298571(1440), #298572(1440), #298573(1440), #298574(1440), #298575(1440), #298576(1440), #298577(1440), #298578(1440), #298579(1440), #298580(1440), #298581(1440), #298582(1440), #298583(1440), #298584(1440), #298585(1440), #298586(1440), #298587(1440), #298588(1440), #298589(1440), #298590(1440), #298591(1440), #298592(1440), #298593(1440), #298594(1440), #298595(1440), #298596(1440), #298597(1440), #298598(1440), #298599(1440), #298600(1440), #298601(1440), #298602(1440), #298603(1440), #298604(1440), #298605(1440), #298606(1440), #298607(1440), #298608(1440), #298609(1440), #298610(1440), #298611(1440), #298612(1440), #298613(1440), #298614(1440), #298615(1440), #298616(1440), #298617(1440), #298618(1440), #298619(1440), #298620(1440), #298621(1440), #298622(1440), #298623(1440), #298624(1440), #298625(1440), #298626(1440), #298627(1440), #298628(1440), #298629(1440), #298630(1440), #298631(1440), #298632(1440), #298633(1440), #298634(1440), #298635(1440), #298636(1440), #298637(1440), #298638(1440), #298639(1440), #298640(1440), #298641(1440), #298642(1440), #298643(1440), #298644(1440), #298645(1440), #298646(1440), #298647(1440), #298648(1440), #298649(1440), #298650(1440), #298651(1440), #298652(1440), #298653(1440), #298654(1440), #298655(1440), #298656(1440), #298657(1440), #298658(1440), #298659(1440), #298660(1440), #298661(1440), #298662(1440), #298663(1440), #298664(1440), #298665(1440), #298666(1440), #298667(1440), #298668(1440), #298669(1440), #298670(1440), #298671(1440), #298672(1440), #298673(1440), #298674(1440), #298675(1440), #298676(1440), #298677(1440), #298678(1440), #298679(1440), #298680(1440), #298681(1440), #298682(1440), #298683(1440), #298684(1440), #298685(1440), #298686(1440), #298687(1440), #298688(1440), #298689(1440), #298690(1440), #298691(1440), #298692(1440), #298693(1440), #298694(1440), #298695(1440), #298696(1440), #298697(1440), #298698(1440), #298699(1440), #298700(1440), #298701(1440), #298702(1440), #298703(1440), #298704(1440), #298705(1440), #298706(1440), #298707(1440), #298708(1440), #298709(1440), #298710(1440), #298711(1440), #298712(1440), #298713(1440), #298714(1440), #298715(1440), #298716(1440), #298717(1440), #298718(1440), #298719(1440), #298720(1440), #298721(1440), #298722(1440), #298723(1440), #298724(1440), #298725(1440), #298726(1440), #298727(1440), #298728(1440), #298729(1440), #298730(1440), #298731(1440), #298732(1440), #298733(1440), #298734(1440), #298735(1440), #298736(1440), #298737(1440), #298738(1440), #298739(1440), #298740(1440), #298741(1440), #298742(1440), #298743(1440), #298744(1440), #298745(1440), #298746(1440), #298747(1440), #298748(1440), #298749(1440), #298750(1440), #298751(1440), #298752(1440), #298753(1440), #298754(1440), #298755(1440), #298756(1440), #298757(1440), #298758(1440), #298759(1440), #298760(1440), #298761(1440), #298762(1440), #298763(1440), #298764(1440), #298765(1440), #298766(1440), #298767(1440), #298768(1440), #298769(1440), #298770(1440), #298771(1440), #298772(1440), #298773(1440), #298774(1440), #298775(1440), #298776(1440), #2

8. Transmission Control Protocol (TCP)

Wireshark packet capture showing TCP traffic. The packet list displays several TCP segments, with packet 33816 selected. The packet details pane shows the structure of the TCP segment, including source and destination ports, sequence and acknowledgment numbers, and flags.

Packet 33816 details:

- Source Port: 57571
- Destination Port: 80
- [Stream index: 0]
- [Conversation completeness: Incomplete (12)]
- [TCP Segment Len: 0]
- Sequence Number: 2671 (relative sequence number)
- Sequence Number (raw): 1178984078
- [Next Sequence Number: 2671 (relative sequence number)]
- Acknowledgment Number: 7039441 (relative ack number)
- Acknowledgment number (raw): 3066583598
- 1000 = Header Length: 32 bytes (8)
- Flags: 0x010 (ACK)
- Window: 481
- [Calculated window size: 481]
- [Window size scaling factor: -1 (unknown)]
- Checksum: 0x6ccb [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- Options: 0x00 (No-Operation (NOP), No-Operation (NOP), Timestamps)
- [Timestamps]
- [SEQ/ACK analysis]

9. User Datagram Protocol (UDP)

Wireshark packet capture showing UDP traffic. The packet list displays several UDP segments, with packet 485 selected. The packet details pane shows the structure of the UDP segment, including source and destination ports, length, and checksum.

Packet 485 details:

- Source Port: 58779
- Destination Port: 53
- Length: 52
- Checksum: 0xc3fd [unverified]
- [Checksum Status: Unverified]
- [Stream index: 3]
- [Timestamps]
- UDP payload (44 bytes)
- Domain Name System (query)