

S471 – Web Technologies (Laboratory)



Lab 1 The Internet Protocols

Lab Activities:

Part 1: Capturing HTTP Traffic.

Task 1: Start Wireshark and capture packets.

No.	Time	Source	Destination	Protocol	Length	Info
1213..	168.164868	2a00:1450:4006:806::	2001:16a2:c053:ec16::	QUIC	85	Protected Payload (KP0)
1213..	168.165723	2001:16a2:c053:ec16::	2a00:1450:4006:806::	QUIC	97	Protected Payload (KP0), DCID=ee550f3ba8ef4b60
1213..	168.178756	fe80::a84a:28ff:fee::	fe80::2308:8666:1ec::	DNS	403	Standard query response 0x7129 A d1.delivery.mp.microsoft.com CNAME d1.delivery.mp.microsoft.com.delivery.microso...
1213..	168.180295	2001:16a2:c053:ec16::	2001:16a6:c002::3	TCP	86	13200 → 80 [SYN] Seq=0 Win=65330 Len=0 MSS=1390 WS=256 SACK_PERM
1213..	168.252856	2a00:1450:4006:806::	2001:16a2:c053:ec16::	QUIC	182	Protected Payload (KP0)
1213..	168.277315	2a00:1450:4006:806::	2001:16a2:c053:ec16::	QUIC	87	Protected Payload (KP0)
1213..	168.279977	172.20.10.2	95.161.76.101	TCP	66	[TCP Retransmission] 13196 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	168.280006	2001:16a2:c053:ec16::	2a00:1450:4006:806::	QUIC	94	Protected Payload (KP0), DCID=ee550f3ba8ef4b60
1213..	168.488559	172.20.10.2	85.195.179.37	TCP	66	13201 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	168.562461	172.20.10.2	85.195.179.37	TCP	66	[TCP Retransmission] 13148 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	168.595482	172.20.10.2	85.195.179.37	TCP	66	[TCP Retransmission] 13151 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	168.595533	172.20.10.2	149.154.167.41	TCP	66	[TCP Retransmission] 13193 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	168.595553	172.20.10.2	149.154.167.41	TCP	66	[TCP Retransmission] 13194 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	168.985326	64:ff9b:13694:b381::	2001:16a2:c053:ec16::	TLvSv1.2	509	Application Data
1213..	169.029809	2001:16a2:c053:ec16::	64:ff9b:13694:b381::	TCP	74	12416 → 443 [ACK] Seq=1 Ack=39104 Win=510 Len=0
1213..	169.078874	2001:16a2:c053:ec16::	2603:1040:a06:6::	TLvSv1.2	117	Application Data
1213..	169.294859	172.20.10.2	95.161.76.101	TCP	66	13202 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	169.298168	2603:1040:a06:6::	2001:16a2:c053:ec16::	TLvSv1.2	248	Application Data
1213..	169.341545	2001:16a2:c053:ec16::	2603:1040:a06:6::	TCP	74	6451 → 443 [ACK] Seq=710 Ack=4124 Win=511 Len=0
1213..	169.406143	172.20.10.2	85.195.179.37	TCP	66	[TCP Retransmission] 13201 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	169.581305	172.20.10.2	149.154.167.41	TCP	66	13203 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	169.583756	172.20.10.2	149.154.167.41	TCP	66	13204 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	170.041302	172.20.10.2	149.154.167.91	TCP	66	[TCP Retransmission] 13185 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	170.041400	172.20.10.2	149.154.167.91	TCP	66	[TCP Retransmission] 13186 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	170.295279	172.20.10.2	95.161.76.101	TCP	66	[TCP Retransmission] 13202 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	170.572762	172.20.10.2	149.154.175.100	TCP	66	13205 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	170.575046	2001:16a2:c053:ec16::	2a06:98c1:52::4	TCP	86	13206 → 443 [SYN] Seq=0 Win=65330 Len=0 MSS=1390 WS=256 SACK_PERM
1213..	170.576621	172.20.10.2	149.154.175.100	TCP	66	13207 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1213..	170.650934	2a06:98c1:52::4	2001:16a2:c053:ec16::	TCP	86	443 → 13206 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM WS=8192
1213..	170.651053	2001:16a2:c053:ec16::	2a06:98c1:52::4	TCP	74	13206 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
1213..	170.654079	2001:16a2:c053:ec16::	2a06:98c1:52::4	TLvSv1.3	591	Client Hello (SNI=mozilla.cloudflare-dns.com)
1213..	170.751837	2a06:98c1:52::4	2001:16a2:c053:ec16::	TCP	74	443 → 13206 [ACK] Seq=1 Ack=518 Win=73728 Len=0
1213..	170.755874	2a06:98c1:52::4	2001:16a2:c053:ec16::	TLvSv1.3	1434	Server Hello, Change Cipher Spec
1213..	170.755874	2a06:98c1:52::4	2001:16a2:c053:ec16::	TCP	1434	443 → 13206 [ACK] Seq=1 Ack=518 Win=73728 Len=1360 [TCP segment of a reassembled PDU]
1213..	170.755874	2a06:98c1:52::4	2001:16a2:c053:ec16::	TLvSv1.3	222	Application Data
1213..	170.756085	2001:16a2:c053:ec16::	2a06:98c1:52::4	TCP	74	13206 → 443 [ACK] Seq=518 Ack=2869 Win=131840 Len=0
1213..	170.763982	2001:16a2:c053:ec16::	2a06:98c1:52::4	TLvSv1.3	154	Change Cipher Spec, Application Data
1213..	170.863336	2a06:98c1:52::4	2001:16a2:c053:ec16::	TCP	74	443 → 13206 [ACK] Seq=2869 Ack=598 Win=73728 Len=0
1213..	170.863371	2001:16a2:c053:ec16::	2a06:98c1:52::4	TLvSv1.3	565	Application Data
1213..	170.945856	2a06:98c1:52::4	2001:16a2:c053:ec16::	TCP	74	443 → 13206 [ACK] Seq=2869 Ack=1089 Win=73728 Len=0
1213..	170.949678	2a06:98c1:52::4	2001:16a2:c053:ec16::	TLvSv1.3	1427	Application Data, Application Data
1213..	170.951333	2001:16a2:c053:ec16::	2a06:98c1:52::4	TCP	74	13206 → 443 [FIN, ACK] Seq=1089 Ack=1222 Win=130560 Len=0

Task 2: Filter HTTP packets and analyze them.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

h: http

No.	Time	Source	Destination	Protocol	Length	Info
61	4.509739	10.90.46.37	34.223.124.45	HTTP	641	GET /online/ HTTP/1.1
6	6.974264	34.223.124.45	10.90.46.37	HTTP	214	HTTP/1.1 200 OK (text/html)
1538	82.135994	149.154.167.91	10.90.46.37	HTTP	357	HTTP/1.1 200 OK

> Frame 61: 641 bytes on wire (5128 bits), 641 bytes captured (5128 bits) on interface \Device\NPF{FDC08268-EFB4-48...}

Ethernet II, Src: Intel_71:67:f9 (f4:b3:01:71:67:f9), Dst: Fortinet_Sd.fc:8a (e0:23:ff:5d:fc:8a)

Internet Protocol Version 4, Src: 10.90.46.37, Dst: 34.223.124.45

Transmission Control Protocol, Src Port: 3960, Dst Port: 80, Seq: 1, Ack: 1, Len: 587

Hypertext Transfer Protocol

GET /online/ HTTP/1.1

[Expert Info (Chat/Sequence): GET /online/ HTTP/1.1]

Request Method: GET

Request URI: /online/

Request Version: HTTP/1.1

Host: silverwonderousshiningsong.neverssl.com

Connection: keep-alive

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Accept-Encoding: gzip, deflate

Accept-Language: en-US;q=0.9,ar;q=0.8

If-None-Match: "8be-5a28b29291e10-gzip"

If-Modified-Since: Wed, 29 Jun 2022 00:23:22 GMT

[Full request URI: http://silverwonderousshiningsong.neverssl.com/online/]

[HTTP request 1/1]

[Response in frame: 85]

0000 e0 23 ff 5d fc 8a f4 b3 01 71 67 f9 08 00 45 00 #]qg...E

0010 02 73 47 a2 40 00 80 06 00 00 8a 5a 2e 25 22 df s0 @ - ...Z.M

0020 7c 2d 0f 78 00 50 f0 fe 11 c5 ff 6c 9f 63 50 18 [- x P - ...l-cP

0030 01 03 d9 f0 00 00 47 45 54 20 2f 6f 6e 6c 69 6eGE T /onlin

0040 65 2f 20 48 54 50 2f 31 2e 31 0d 0a 48 6f 73 e / HTTP/ 1.1 -Hos

0050 74 3a 20 73 69 6c 76 65 72 77 6f 6e 64 65 72 6f t: silve rwondero

0060 75 73 73 68 69 6e 69 6e 67 73 6f 6e 67 2e 6e 65 ushlinxngsong-ne

0070 76 65 72 73 73 6c 2e 63 6f 6d 0d 0a 43 6f 6e 6e verssl.c om: Conn

0080 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 6e action: keep-all

0090 76 65 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f ve--Cach e-Contro

00a0 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 0a 55 70 1: max-a ge=0- Up

00b0 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 grade-In secure-R

00c0 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 7.36 (KH TML, lIk

00d0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f e -Agent: Mozilla/

00e0 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (Win dows NT

00f0 31 30 2e 30 3b 20 57 69 6e 66 36 34 3b 20 78 36 34 10.0; Win 64; x64

0100 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33) AppleWebKit/53

0110 37 2a 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 60 7.36 (KH TML, lIk

0120 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f e e Gecko) Chrome/

0130 31 33 31 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 131.0.0.0 Safa

0140 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 3a /537.36 - Accept:

0150 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 text/ht ml,appli

0160 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 20 78 6d 6c cation/xhtml=xml

0170 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c ,applic tion/xml

0180 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 69 q=0.9, i mage/avi

0190 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61 f,image/ webp,ima

01a0 67 65 2f 61 70 70 6c 6f 2c 2a 2f 2a 3b 71 3d 30 2e ge/apng, /*;q=0.

01b0 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 69 8,applic tion/si

01c0 67 6e 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 3d gned-exc hange;v

01d0 62 33 3b 71 3d 30 2e 37 0d 0a 41 63 63 65 70 74 b3;q=0.7 -Accept

Part 2: Analyzing TCP/IP Traffic.

Task 1: Filter TCP packets

tcp.stream eq 3

No.	Time	Source	Destination	Protocol	Length	Info
52	4.210952	10.90.46.37	34.223.124.45	TCP	66	3960 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
59	4.509141	34.223.124.45	10.90.46.37	TCP	60	80 → 3960 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1386 SACK_PERM WS=128
60	4.509272	10.90.46.37	34.223.124.45	TCP	54	3960 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
61	4.509739	10.90.46.37	34.223.124.45	HTTP	641	GET /online/ HTTP/1.1
65	4.832752	34.223.124.45	10.90.46.37	TCP	1440	80 → 3960 [ACK] Seq=1 Ack=588 Win=28160 Len=1386 [TCP segment of a reassembled PDU]
66	4.853666	34.223.124.45	10.90.46.37	TCP	60	80 → 3960 [ACK] Seq=1 Ack=588 Win=28160 Len=0
67	4.853744	10.90.46.37	34.223.124.45	TCP	54	3960 → 80 [ACK] Seq=588 Ack=1387 Win=66304 Len=0
85	6.974264	34.223.124.45	10.90.46.37	HTTP	214	HTTP/1.1 200 OK (text/html)
86	7.019541	10.90.46.37	34.223.124.45	TCP	54	3960 → 80 [ACK] Seq=588 Ack=1547 Win=66304 Len=0
121	9.840486	34.223.124.45	10.90.46.37	TCP	60	80 → 3960 [FIN, ACK] Seq=1547 Ack=588 Win=28160 Len=0
122	9.840554	10.90.46.37	34.223.124.45	TCP	54	3960 → 80 [ACK] Seq=588 Ack=1548 Win=66304 Len=0
313	17.567278	10.90.46.37	34.223.124.45	TCP	54	3960 → 80 [FIN, ACK] Seq=588 Ack=1548 Win=66304 Len=0
338	17.826416	34.223.124.45	10.90.46.37	TCP	60	80 → 3960 [ACK] Seq=1548 Ack=589 Win=28160 Len=0

Wireshark · Follow TCP Stream (tcp.stream eq 3) - شبكة Wi-Fi

Host: silverwonderousshiningsong.neverss1.com

Connection: keep-alive

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9,ar;q=0.8

If-None-Match: "8be-5e28b29291e10-gzip"

If-Modified-Since: Wed, 29 Jun 2022 00:23:22 GMT

HTTP/1.1 200 OK

Date: Sun, 02 Feb 2025 09:01:35 GMT

Server: Apache/2.4.62 ()

Upgrade: h2,h2c

Connection: Upgrade, Keep-Alive

Last-Modified: Wed, 29 Jun 2022 00:23:22 GMT

ETag: "8be-5e28b29291e10-gzip"

Accept-Ranges: bytes

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 1173

Keep-Alive: timeout=5, max=100

Content-Type: text/html; charset=UTF-8

Task 2: Analyze TCP handshake and investigate Data Transfer and Termination

tcp.stream eq 3

No.	Time	Source	Destination	Protocol	Length	Info
52	4.210952	10.90.46.37	34.223.124.45	TCP	66	3960 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
59	4.509141	34.223.124.45	10.90.46.37	TCP	60	80 → 3960 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1386 SACK_PERM WS=128
60	4.509272	10.90.46.37	34.223.124.45	TCP	54	3960 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
61	4.509739	10.90.46.37	34.223.124.45	HTTP	641	GET /online/ HTTP/1.1
65	4.832752	34.223.124.45	10.90.46.37	TCP	1440	80 → 3960 [ACK] Seq=1 Ack=588 Win=28160 Len=1386 [TCP segment of a reassembled PDU]
66	4.853666	34.223.124.45	10.90.46.37	TCP	60	80 → 3960 [ACK] Seq=1 Ack=588 Win=28160 Len=0
67	4.853744	10.90.46.37	34.223.124.45	TCP	54	3960 → 80 [ACK] Seq=588 Ack=1387 Win=66304 Len=0
85	6.974264	34.223.124.45	10.90.46.37	HTTP	214	HTTP/1.1 200 OK (text/html)
86	7.019541	10.90.46.37	34.223.124.45	TCP	54	3960 → 80 [ACK] Seq=588 Ack=1547 Win=66304 Len=0
121	9.840486	34.223.124.45	10.90.46.37	TCP	60	80 → 3960 [FIN, ACK] Seq=1547 Ack=588 Win=28160 Len=0
122	9.840554	10.90.46.37	34.223.124.45	TCP	54	3960 → 80 [ACK] Seq=588 Ack=1548 Win=66304 Len=0
313	17.567278	10.90.46.37	34.223.124.45	TCP	54	3960 → 80 [FIN, ACK] Seq=588 Ack=1548 Win=66304 Len=0
338	17.826416	34.223.124.45	10.90.46.37	TCP	60	80 → 3960 [ACK] Seq=1548 Ack=589 Win=28160 Len=0

Frame 121: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface Device\NPF_{FDC0826B-EFB4-4802-0000-000000000000} (eth0) on interface Device\NPF_{FDC0826B-EFB4-4802-0000-000000000000}

Ethernet II, Src: Fortinet_Sd-fc:8a (e0:23:ff:5d:fc:8a), Dst: Intel_71:67:f9 (f4:b3:01:71:67:f9)

Internet Protocol Version 4, Src: 34.223.124.45, Dst: 10.90.46.37

Transmission Control Protocol, Src Port: 80, Dst Port: 3960, Seq: 1547, Ack: 588, Len: 0

Source Port: 80

Destination Port: 3960

[Stream index: 3]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 1547 (relative sequence number)

Sequence Number (raw): 4285310317

[Next Sequence Number: 1548 (relative sequence number)]

Acknowledgment Number: 588 (relative ack number)

Acknowledgment number (raw): 4043183632

0101 = Header Length: 20 bytes (5)

Flags: 0x011 (FIN, ACK)

Window: 220

[Calculated window size: 28160]

[Window size scaling factor: 128]

Checksum: 0x1bbb [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

Part 3: Capturing and Analyzing UDP Traffic

Task 1: Generate UDP traffic and capture packets

Task 2: Filter and analysis UDP Packets

The image shows a Wireshark packet capture of UDP traffic. The packet list on the left shows a series of packets, including a DNS query and response, and several UDP packets. The packet details pane on the right shows the structure of a UDP packet, including source and destination ports, length, and checksum. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

Part 4: Comparing TCP and UDP by filling in the following tables. Save your work (e.g., in an MS Word document), and upload it to your online git repo.

Task 1: Fill in the following table and provide reasons.

	TCP or UDP	Reasons
Reliability and Connection Establishment	TCP	it sets up a connection before sending data. It makes sure all data is received and will resend if anything is lost.
Data Integrity and Ordering	TCP	It keeps data in the right order and checks for errors, so nothing gets mixed up. UDP does not do this.

Task 2: Identify the use Cases and Performance of TCP and UDP.

	TCP	UDP
Use cases	Best for things that need all data to be correct, like websites (HTTP/HTTPS), emails, and file downloads.	Best for fast communication where some data loss is okay, like video calls, online games, and live streaming.
Performance	Slower because it checks for errors and resends lost data.	Faster because it doesn't check for errors or resend lost data

Shahd Alsuhaibani