

# Lab 1 :

## Part one :

### Task one : capturing HTTP TRAFFIC

Capturing from شبكة 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
9952	16.562487	151.248.104.57	172.20.10.2	TCP	1454	443 → 50506 [PSH, ACK] Seq=1401 Ack=1722 Win=64128 Len=1400 [TCP PDU reassembled in 9953]
9953	16.562487	151.248.104.57	172.20.10.2	TLSv1.3	1288	Application Data, Application Data, Application Data
9954	16.562487	151.248.104.57	172.20.10.2	QUIC	1292	Protected Payload (KP0)
9955	16.562800	172.20.10.2	151.248.104.57	TCP	54	50506 → 443 [ACK] Seq=1722 Ack=2801 Win=131328 Len=0
9956	16.563272	172.20.10.2	151.248.104.57	QUIC	73	Protected Payload (KP0), DCID=03561fa4f2018723
9957	16.568178	172.20.10.2	151.248.104.57	TLSv1.3	134	Change Cipher Spec, Application Data
9958	16.572620	151.248.104.57	172.20.10.2	QUIC	1292	Protected Payload (KP0)
9959	16.572620	162.125.69.18	172.20.10.2	TCP	1454	443 → 50501 [ACK] Seq=4015 Ack=750 Win=66560 Len=1400 [TCP PDU reassembled in 9960]
9960	16.572620	162.125.69.18	172.20.10.2	TLSv1.3	613	Application Data
9961	16.572620	151.248.104.57	172.20.10.2	QUIC	1292	Protected Payload (KP0)
9962	16.572620	151.248.104.57	172.20.10.2	QUIC	1292	Protected Payload (KP0)
9963	16.572620	151.248.104.57	172.20.10.2	TCP	66	443 → 50507 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1384 SACK_PERM WS=128
9964	16.572840	172.20.10.2	162.125.69.18	TCP	54	50501 → 443 [ACK] Seq=750 Ack=5974 Win=262144 Len=0

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF...  
> Ethernet II, Src: 3a:53:9c:9c:5a:64 (3a:53:9c:9c:5a:64), Dst: Intel\_5b:15:9e (40:ec:95:5b:15:9e)  
> Internet Protocol Version 4, Src: 13.107.6.254, Dst: 172.20.10.2  
> Transmission Control Protocol, Src Port: 443, Dst Port: 50458, Seq: 1, Ack: 1, Len: 0

Bytes 52-53: Urgent Pointer (tcp.urgent\_pointer)

Packets: 9964

Profile: Default

### Task 2: Filter HTTP packets and analyze them

\*شبكة Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
26077	25.074137	2001:16a2:c052:f8c9...	2001:41a8:44:3::5c7...	HTTP	360	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?636abf5d3abe97a2 HTTP/1.1
26083	25.167289	2001:41a8:44:3::5c7...	2001:16a2:c052:f8c9...	HTTP	340	HTTP/1.1 304 Not Modified
26084	25.174185	2001:16a2:c052:f8c9...	2001:41a8:44:3::5c7...	HTTP	355	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?3a0665aaa503a2ee HTTP/1.1
26086	25.261510	2001:41a8:44:3::5c7...	2001:16a2:c052:f8c9...	HTTP	341	HTTP/1.1 304 Not Modified
31943	34.410253	2001:16a2:c052:f8c9...	2001:16a2:c052:f8c9...	HTTP	474	GET /MFEwTzBNMESwSTAJBgUrDgMCGgUABBRr2bwARTxMtEy9aspRAZg5QFhagQQUgrWPZfOn89x6JI3r%2F2ztWk1... HTTP/1.1
31945	34.454250	2600:1416:e000:1ba...	2001:16a2:c052:f8c9...	HTTP	433	HTTP/1.1 304 Not Modified
31961	34.562199	2001:16a2:c052:f8c9...	2600:1416:e000:1ae...	HTTP	301	GET / HTTP/1.1
31963	34.601189	2600:1416:e000:1ae...	2001:16a2:c052:f8c9...	HTTP	337	HTTP/1.1 304 Not Modified
31964	34.611497	2001:16a2:c052:f8c9...	2600:1416:e000:1ba...	HTTP	470	GET /MFEwTzBNMESwSTAJBgUrDgMCGgUABBRr2bwARTxMtEy9aspRAZg5QFhagQQUgrWPZfOn89x6JI3r%2F2ztWk1... HTTP/1.1
31968	34.657588	2600:1416:e000:1ba...	2001:16a2:c052:f8c9...	HTTP	433	HTTP/1.1 304 Not Modified
31969	34.665904	2001:16a2:c052:f8c9...	2600:1416:e000:1ba...	HTTP	474	GET /MFEwTzBNMESwSTAJBgUrDgMCGgUABBRr2bwARTxMtEy9aspRAZg5QFhagQQUgrWPZfOn89x6JI3r%2F2ztWk1... HTTP/1.1
31978	34.709989	2600:1416:e000:1ba...	2001:16a2:c052:f8c9...	HTTP	433	HTTP/1.1 304 Not Modified
31992	34.864542	2001:16a2:c052:f8c9...	2a00:1450:4006:800...	HTTP	274	GET /r/r1.crl HTTP/1.1
31999	34.983950	2a00:1450:4006:800...	2001:16a2:c052:f8c9...	HTTP	297	HTTP/1.1 304 Not Modified

> Frame 31943: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface...  
> Ethernet II, Src: Intel\_5b:15:9e (40:ec:95:5b:15:9e), Dst: 3a:53:9c:9c:5a:64 (3a:53:9c:9c:5a:64)  
> Internet Protocol Version 6, Src: 2001:16a2:c052:f8c9:8ef:c711:fe6:7c11, Dst: 2600:1416:e000:1ba...  
> Transmission Control Protocol, Src Port: 64890, Dst Port: 80, Seq: 1, Ack: 1, Len: 406  
> Hypertext Transfer Protocol

Hypertext Transfer Protocol: Protocol

Packets: 115939 · Displayed: 26 (0.0%) · Dropped: 0 (0.0%)

Profile: Default

## Task 1: Filter TCP packets

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, and Capture. The main window is titled "Wireshark - Follow TCP Stream (tcp.stream eq 63) - شبكة Wi-Fi". The left sidebar shows the packet list with 10 packets, and the packet details pane for packet 6 (Frame 30696: 66 bytes on wire (528 bytes captured) on interface 0, Ethernet II, Src: 3a:53:9, Internet Protocol Version 4, Destination: 10.0.0.1, Transmission Control Protocol, Seq: 30696, Win: 0, Len: 0). The packet bytes pane shows the raw data of the TCP stream, which is a GET request to a Microsoft server. The data is displayed in hexadecimal and ASCII. The ASCII view shows the following text:

```

.....f.jj..MN..H.Ji`N..b....S...o..$.+.0./.$#.(.
.....= <5./.....%#. watson.events.data.microsoft.com.....
.....#.....h2.http/1.1.....
.....A...U..f.ji6...KChw>I(/;...z.pDOWNGRD. WS...!.`9HF.9..*S.i...h...j.ni.0..
.....S.p...0...0...r.....3.....a^.....0
.....*H..
.....0~1.0 ..U....US1.0...U...
Washington1.0...U....Redmond1.0...U.
..Microsoft Corporation1(0&..U....Microsoft Secure Server CA 20110..
240613185711Z.
250613185711Z0t1.0 ..U....US1.0 ..U....WA1.0...U....Redmond1.0...U.
..Microsoft1.0
..U....WSE1$0".U....*.events.data.microsoft.com0.."0
.....*H..
.....0..
.....O...@.....%F..d.VO.W...
D...naG(.n.n.nP.Z...C.q.x."G." <p...EhbF.2.|.Y..c...[3X.k].(.{...$O.-:k..."-...s..
.....X.F...=..a.R...H.j...7...Y..fn.K%.)..y...T9..f@...*. [a0.H.t.S.&.....j.T...G...Kj...r..Y..RrBz.....
!.)...#.7J.U...&..s$.jm.....0...0...U....0...U...0...+.....0...U....0...U....W).>
p..r.3.$*...j$.0...U....0.....*.events.data.microsoft.com..events.data.microsoft.com..umwatsonc.telemetry.mi
crosoft.com..lkmwatsonc.telemetry.microsoft.com..watson.telemetry.microsoft.com..watson.microsoft.com..oca.teleme
try.microsoft.com..oca.microsoft.com..*.events.data.microsoft.us..events.data.microsoft.us..umwatsonc.telemetry.
microsoft.us..kmmwatsonc.telemetry.microsoft.us..watson.telemetry.microsoft.us..watson.microsoft.us..oca.telemetry.
y.microsoft.us..oca.microsoft.us0...U.#...0...6V.eI.[./<.B.PM..3..0S..U...L00H.F.D.Bhttp://www.microsoft.com/pki
ops/crl/MicSecSerCA2011_2011-10-18.crl0'..+.....T0R0P..+.....0..Dhttp://www.microsoft.com/pkiops/certs/MicSec
SerCA2011_2011-10-18.crt0...U.....0.0
.....*H..
.....A.....V.Pc.W..U..8^..y..j..nR%..5...1..$a(v.....'05..h...$. F.x...s...>.....3.R..
~.....)
...C...1.8.S.<.....1
...Js{.z&

```

The bottom status bar shows the current filter is "tcp.stream eq 63", and the packet list shows 10 packets. The packet details pane shows the details of packet 6, which is a GET request to a Microsoft server.



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

Wireshark interface showing a packet capture of a TCP stream (eq 63). The packet list shows a sequence of packets including SYN, ACK, and data segments. The packet details pane shows the selected packet (1566) with its structure and flags.

No.	Time	Source	Destination	Protocol	Length	Info
1260...	85.362900	172.20.10.3	2.16.149.28	TCP	66	59529 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1263...	85.473159	2.16.149.28	172.20.10.3	TCP	66	443 → 59529 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=128
1263...	85.473421	172.20.10.3	2.16.149.28	TCP	54	59529 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
1263...	85.474800	172.20.10.3	2.16.149.28	TLV1.2	359	Client Hello (SNI=stream-production.avcdn.net)
1271...	85.844917	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1281...	86.233232	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1297...	86.896547	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1317...	88.239058	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1355...	90.888571	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1400...	95.316748	172.20.10.3	2.16.149.28	TLV1.2	61	Alert (Level: Warning, Description: Close Notify)
1400...	95.316941	172.20.10.3	2.16.149.28	TCP	54	59529 → 443 [FIN, ACK] Seq=313 Ack=1 Win=131584 Len=0
1413...	96.187534	172.20.10.3	2.16.149.28	TCP	366	[TCP Retransmission] 59529 → 443 [FIN, PSH, ACK] Seq=1 Ack=1 Win=131584 Len=312
1566...	106.792066	172.20.10.3	2.16.149.28	TCP	54	59529 → 443 [RST, ACK] Seq=314 Ack=1 Win=0 Len=0

Packet details for packet 1566:

- [Stream index: 63]
- [Stream Packet Number: 1]
- [Conversation completeness: Complete, WITH\_DATA (63)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 1391919707
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1000 ... = Header Length: 32 bytes (8)
- Flags: 0x002 (SYN)
- Window: 64240
- [Calculated window size: 64240]
- Checksum: 0x4d6a [unverified]

Packet bytes (hex): 0000 3a 53 9c 9c 5a 64 40 ec 99 5b 15 9e 08 00 45 00 :S...Zd...E...  
0010 00 34 bb 52 40 00 00 06 00 00 ac 14 0a 03 02 10 :4...3...  
0020 95 1c e8 89 01 bb 52 f7 02 5b 00 00 00 00 02 :...R...  
0030 fa f0 4d 6a 00 00 02 04 05 b4 01 03 03 08 01 01 :...Mj...  
0040 04 02 ..

Wireshark interface showing a packet capture of a TCP stream (eq 63). The packet list shows a sequence of packets including SYN, ACK, and data segments. The packet details pane shows the selected packet (1566) with its structure and flags.

No.	Time	Source	Destination	Protocol	Length	Info
1260...	85.362900	172.20.10.3	2.16.149.28	TCP	66	59529 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1263...	85.473159	2.16.149.28	172.20.10.3	TCP	66	443 → 59529 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=128
1263...	85.473421	172.20.10.3	2.16.149.28	TCP	54	59529 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
1263...	85.474800	172.20.10.3	2.16.149.28	TLV1.2	359	Client Hello (SNI=stream-production.avcdn.net)
1271...	85.844917	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1281...	86.233232	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1297...	86.896547	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1317...	88.239058	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1355...	90.888571	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1400...	95.316748	172.20.10.3	2.16.149.28	TLV1.2	61	Alert (Level: Warning, Description: Close Notify)
1400...	95.316941	172.20.10.3	2.16.149.28	TCP	54	59529 → 443 [FIN, ACK] Seq=313 Ack=1 Win=131584 Len=0
1413...	96.187534	172.20.10.3	2.16.149.28	TCP	366	[TCP Retransmission] 59529 → 443 [FIN, PSH, ACK] Seq=1 Ack=1 Win=131584 Len=312
1566...	106.792066	172.20.10.3	2.16.149.28	TCP	54	59529 → 443 [RST, ACK] Seq=314 Ack=1 Win=0 Len=0

Packet details for packet 1566:

- [Stream index: 63]
- [Stream Packet Number: 2]
- [Conversation completeness: Complete, WITH\_DATA (63)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 887942787
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 1391919708
- 1000 ... = Header Length: 32 bytes (8)
- Flags: 0x012 (SYN, ACK)
- Window: 64240
- [Calculated window size: 64240]

Packet bytes (hex): 0000 40 ec 99 5b 15 9e 3a 53 9c 9c 5a 64 08 00 45 00 @...[...S...Zd...E...  
0010 00 34 00 00 00 00 33 06 3a 81 02 10 95 1c ac 14 :4...3...  
0020 0a 03 01 bb e8 89 34 ec ee 83 52 f7 02 5c 80 12 :...4...R...  
0030 fa f0 c4 00 00 00 02 04 05 78 01 01 04 02 01 03 :...x...  
0040 03 07 ..

Wireshark interface showing a packet capture of a TCP stream (eq 63). The packet list shows a sequence of packets including SYN, ACK, and data segments. The packet details pane shows the selected packet (1566) with its structure and flags.

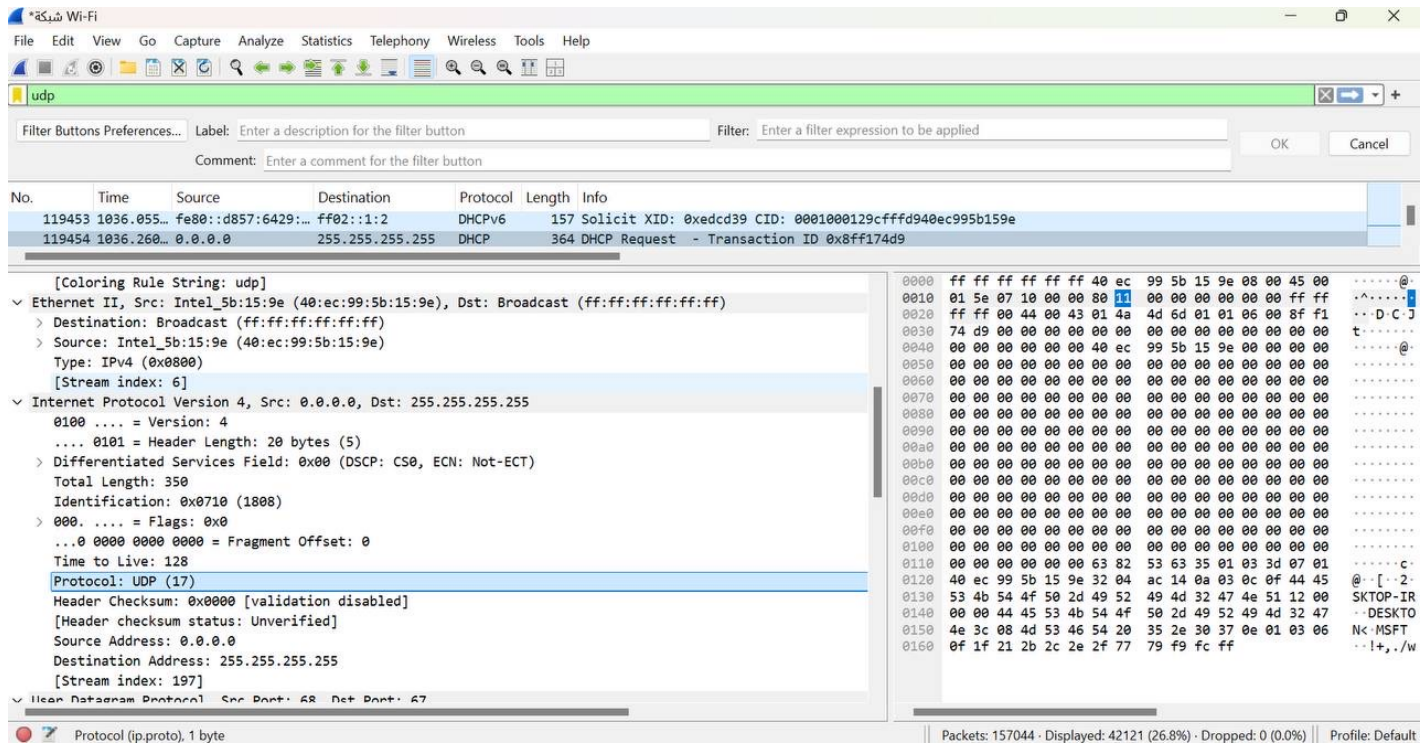
No.	Time	Source	Destination	Protocol	Length	Info
1260...	85.362900	172.20.10.3	2.16.149.28	TCP	66	59529 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1263...	85.473159	2.16.149.28	172.20.10.3	TCP	66	443 → 59529 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=128
1263...	85.473421	172.20.10.3	2.16.149.28	TCP	54	59529 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
1263...	85.474800	172.20.10.3	2.16.149.28	TLV1.2	359	Client Hello (SNI=stream-production.avcdn.net)
1271...	85.844917	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1281...	86.233232	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1297...	86.896547	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1317...	88.239058	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1355...	90.888571	172.20.10.3	2.16.149.28	TCP	359	[TCP Retransmission] 59529 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=305
1400...	95.316748	172.20.10.3	2.16.149.28	TLV1.2	61	Alert (Level: Warning, Description: Close Notify)
1400...	95.316941	172.20.10.3	2.16.149.28	TCP	54	59529 → 443 [FIN, ACK] Seq=313 Ack=1 Win=131584 Len=0
1413...	96.187534	172.20.10.3	2.16.149.28	TCP	366	[TCP Retransmission] 59529 → 443 [FIN, PSH, ACK] Seq=1 Ack=1 Win=131584 Len=312
1566...	106.792066	172.20.10.3	2.16.149.28	TCP	54	59529 → 443 [RST, ACK] Seq=314 Ack=1 Win=0 Len=0

Packet details for packet 1566:

- [Stream index: 63]
- [Stream Packet Number: 3]
- [Conversation completeness: Complete, WITH\_DATA (63)]
- [TCP Segment Len: 0]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 1391919708
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 887942788
- 0101 ... = Header Length: 20 bytes (5)
- Flags: 0x010 (ACK)
- Window: 514
- [Calculated window size: 131584]
- [Window size scaling factor: 256]

Packet bytes (hex): 0000 3a 53 9c 9c 5a 64 40 ec 99 5b 15 9e 08 00 45 00 :S...Zd...E...  
0010 00 28 bb 53 40 00 00 06 00 00 ac 14 0a 03 02 10 :...S...  
0020 95 1c e8 89 01 bb 52 f7 02 5c 34 ec ee 84 50 10 :...4...P...  
0030 02 02 4d 5e 00 00 :...M...

## Task 2: Filter and analysis UDP packets



### Part 4 :

## Reliability and Connection Establishment

### Use TCP:

Reasons: Ensures a reliable connection with a three-way handshake and retransmissions, suitable for web browsing and email.

### Use UDP:

Reasons: Faster, no connection setup, but less reliable. Ideal for live streaming and gaming.

## Data Integrity and Ordering

### Use TCP:

Reasons: Ensures data integrity and correct order with sequence numbers, perfect for file downloads and banking.

### Use UDP:

Reasons: No guarantee of order or integrity. Faster but less

accurate, suitable for live broadcasts and online gaming.

## Task 2: Use Cases and Performance of TCP and UDP

### TCP    UDP

#### Use Cases

- Web browsing (HTTP/HTTPS) - Real-time applications (VoIP, video streaming)
- Email (SMTP, IMAP, POP3) - Online gaming
- File transfer (FTP, SFTP)    - DNS queries
- Remote administration (SSH) - Broadcasting/multicasting (e.g., live video)

#### Performance

- Reliable, ensures data delivery    - Fast, minimal latency
- Higher overhead due to connection setup, error checking, and flow control    - Low overhead, no connection setup
- Suitable for applications where data accuracy is crucial-  
Suitable for time-sensitive applications where some data loss is tolerable