

Tirth V Patel (200435378)

Ramanpreet Singh (200384219)

ENSE 472

Lab: 2

Phase 1:

769	4125.8169807	127.0.0.1	127.0.0.1	TCP	66	37464 → 1234	[ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=181865734 TSecr=181865734
770	4125.8172948	127.0.0.1	127.0.0.1	TCP	107	1234 → 37464	[PSH, ACK] Seq=1 Ack=1 Win=65536 Len=41 TSval=181865734 TSecr=181865734
771	4125.8173682	127.0.0.1	127.0.0.1	TCP	66	37464 → 1234	[ACK] Seq=1 Ack=42 Win=65536 Len=0 TSval=181865734 TSecr=181865734
772	4127.3624842	127.0.0.1	127.0.0.1	TCP	71	37464 → 1234	[PSH, ACK] Seq=1 Ack=42 Win=65536 Len=5 TSval=181868079 TSecr=181865734
773	4127.3624986	127.0.0.1	127.0.0.1	TCP	66	1234 → 37464	[ACK] Seq=42 Ack=6 Win=65536 Len=0 TSval=181868079 TSecr=181868079
774	4127.3655172	127.0.0.1	127.0.0.1	TCP	118	1234 → 37464	[PSH, ACK] Seq=42 Ack=6 Win=65536 Len=52 TSval=181868082 TSecr=181868079
775	4127.3655218	127.0.0.1	127.0.0.1	TCP	66	37464 → 1234	[ACK] Seq=6 Ack=94 Win=65536 Len=0 TSval=181868082 TSecr=181868082
776	4130.2273188	127.0.0.1	127.0.0.1	TCP	74	37478 → 1234	[SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=181870944 TSecr=0 WS=128
777	4130.2273266	127.0.0.1	127.0.0.1	TCP	74	1234 → 37478	[SYN, ACK] Seq=9 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=181870944 TSecr=181870944 WS=128
778	4130.2273266	127.0.0.1	127.0.0.1	TCP	66	37478 → 1234	[ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=181870944 TSecr=181870944
779	4130.2275253	127.0.0.1	127.0.0.1	TCP	107	1234 → 37478	[PSH, ACK] Seq=1 Ack=1 Win=65536 Len=41 TSval=181870944 TSecr=181870944
780	4130.2275928	127.0.0.1	127.0.0.1	TCP	66	37478 → 1234	[ACK] Seq=1 Ack=42 Win=65536 Len=0 TSval=181870944 TSecr=181870944
781	4131.9684902	127.0.0.1	127.0.0.1	TCP	72	37478 → 1234	[PSH, ACK] Seq=1 Ack=42 Win=65536 Len=0 TSval=181872685 TSecr=181870944
782	4131.9685133	127.0.0.1	127.0.0.1	TCP	66	1234 → 37478	[ACK] Seq=42 Ack=7 Win=65536 Len=0 TSval=181872685 TSecr=181872685
783	4131.9795015	127.0.0.1	127.0.0.1	TCP	119	1234 → 37478	[PSH, ACK] Seq=42 Ack=7 Win=65536 Len=53 TSval=181872696 TSecr=181872685
784	4131.9795055	127.0.0.1	127.0.0.1	TCP	66	37478 → 1234	[ACK] Seq=7 Ack=95 Win=65536 Len=0 TSval=181872696 TSecr=181872696
785	4131.9795323	127.0.0.1	127.0.0.1	TCP	95	1234 → 37464	[PSH, ACK] Seq=94 Ack=6 Win=65536 Len=29 TSval=181872696 TSecr=181868082
786	4131.9795406	127.0.0.1	127.0.0.1	TCP	66	37464 → 1234	[ACK] Seq=6 Ack=123 Win=65536 Len=0 TSval=181872696 TSecr=181872696
787	4136.0983858	127.0.0.1	127.0.0.1	TCP	70	37464 → 1234	[PSH, ACK] Seq=6 Ack=123 Win=65536 Len=4 TSval=181876815 TSecr=181872696
788	4136.0985654	127.0.0.1	127.0.0.1	TCP	79	1234 → 37478	[PSH, ACK] Seq=95 Ack=7 Win=65536 Len=13 TSval=181876815 TSecr=181872696
789	4136.0985740	127.0.0.1	127.0.0.1	TCP	66	37478 → 1234	[ACK] Seq=7 Ack=108 Win=65536 Len=0 TSval=181876815 TSecr=181876815
790	4136.1389065	127.0.0.1	127.0.0.1	TCP	66	1234 → 37464	[ACK] Seq=123 Ack=10 Win=65536 Len=0 TSval=181876815 TSecr=181876815
791	4142.3208148	127.0.0.1	127.0.0.1	TCP	87	37478 → 1234	[PSH, ACK] Seq=7 Ack=108 Win=65536 Len=21 TSval=181883037 TSecr=181876815
792	4142.3210271	127.0.0.1	127.0.0.1	TCP	97	1234 → 37464	[PSH, ACK] Seq=123 Ack=10 Win=65536 Len=31 TSval=181883038 TSecr=181876815
793	4142.3210395	127.0.0.1	127.0.0.1	TCP	66	37464 → 1234	[ACK] Seq=10 Ack=154 Win=65536 Len=0 TSval=181883038 TSecr=181883038
794	4142.3630330	127.0.0.1	127.0.0.1	TCP	66	1234 → 37478	[ACK] Seq=108 Ack=20 Win=65536 Len=0 TSval=181883038 TSecr=181883037
795	4148.5942077	127.0.0.1	127.0.0.1	TCP	84	37464 → 1234	[PSH, ACK] Seq=10 Ack=154 Win=65536 Len=18 TSval=181889311 TSecr=181883038
796	4148.5942217	127.0.0.1	127.0.0.1	TCP	66	1234 → 37464	[ACK] Seq=154 Ack=28 Win=65536 Len=0 TSval=181889311 TSecr=181889311
797	4148.5943922	127.0.0.1	127.0.0.1	TCP	93	1234 → 37478	[PSH, ACK] Seq=108 Ack=28 Win=65536 Len=27 TSval=181889311 TSecr=181883037
798	4148.5944065	127.0.0.1	127.0.0.1	TCP	66	37478 → 1234	[ACK] Seq=28 Ack=135 Win=65536 Len=0 TSval=181889311 TSecr=181889311

This capture shows the TCP 3-way handshake between the server and the client.

Packets **776-778** represent the handshake sequence:

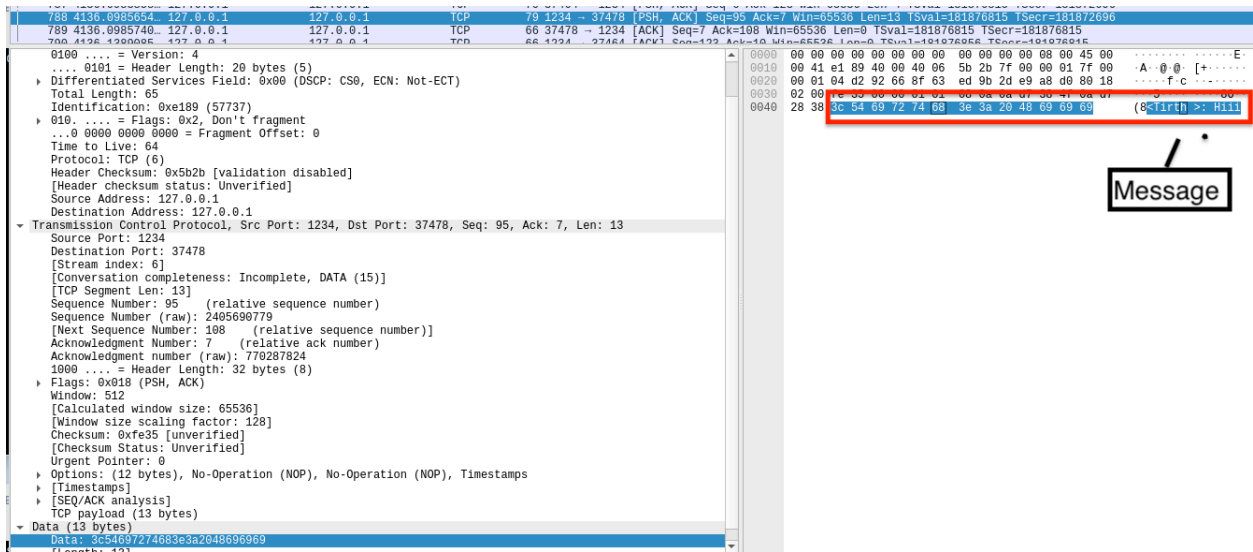
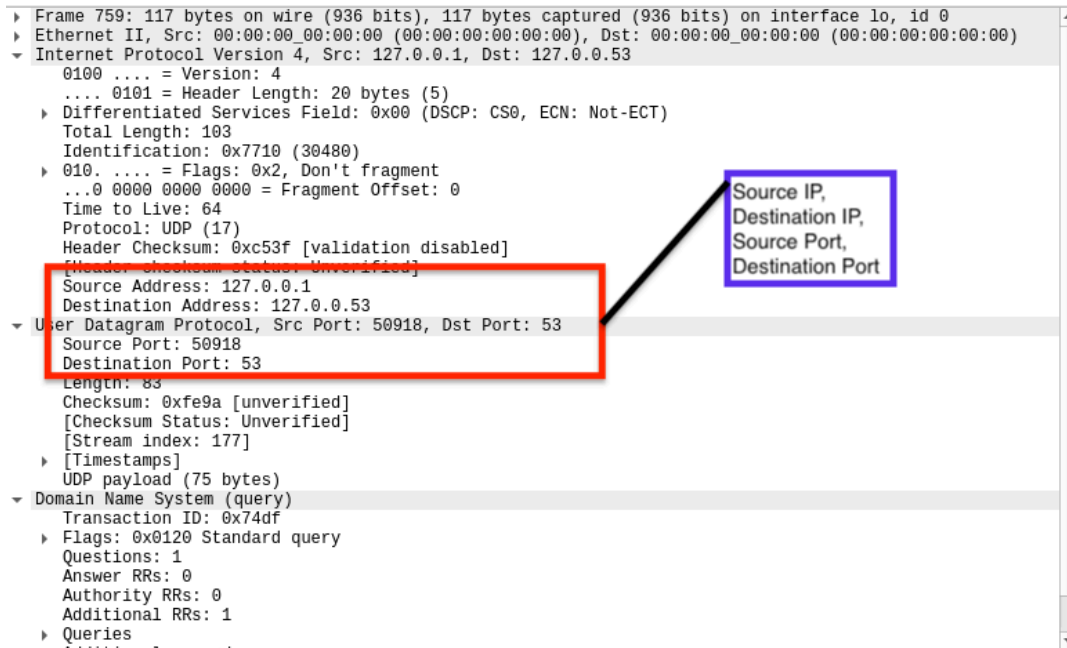
- SYN packet from the client to initiate the connection.
- SYN-ACK from the server acknowledging the request.
- ACK from the client to confirm the connection.

The packets traveled in a sequential manner:

1. Initial SYN request from client to server.
2. Server responds with SYN-ACK.
3. Client sends ACK to complete the connection.
4. Message is sent from the client to the server.
5. Server sends an ACK to confirm receipt.

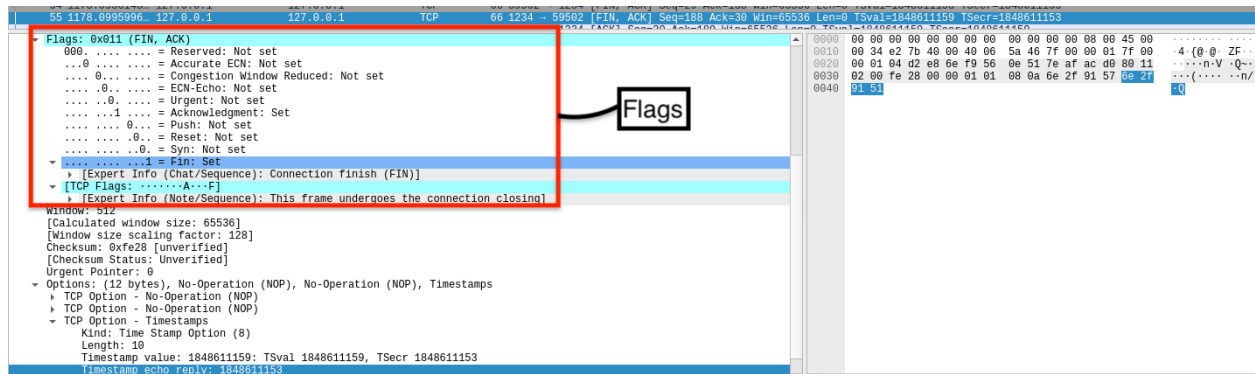
This image below shows detailed information for a specific packet:

- Source IP: 127.0.0.1 (localhost).
- Destination IP: 127.0.0.53 (localhost).
- Source Port: 50918
- Destination Port: 53



This capture illustrates the message payload being sent from one client to another.

- The message content **Tirth > Hiii** is visible in the TCP payload section.
- This transmission uses the **PSH, ACK** flags, meaning data is being pushed from the sender to the receiver, and an acknowledgment is sent back to confirm receipt.
- The messages are not secure. The content of the message is visible in the TCP payload, as shown in the image above. Since the message is transmitted in plain text and not encrypted, anyone with access to the network can intercept and read the messages.



The image above shows a TCP segment with the FIN and ACK flags set, indicating the sender is initiating a graceful connection termination. The FIN flag signals that no more data will be sent, while the ACK flag confirms receipt of previous data, marking the beginning of the TCP connection closure process.

Phase 2:

420	1257.3918540..	127.0.0.1	127.0.0.1	TCP	74	59786 - 1234	[SYN, ACK] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=1049040941 TSecr=0 WS=128
421	1257.3918547..	127.0.0.1	127.0.0.1	TCP	74	1234 - 59786	[SYN, ACK] Seq=0 Ack=1 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=1049040941 TSecr=1049040941
422	1257.3918720..	127.0.0.1	127.0.0.1	TCP	66	59786 - 1234	[ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1049040941 TSecr=1049040941
423	1257.3981068..	127.0.0.1	127.0.0.1	TLSv1.3	359	Client Hello	
424	1257.3981208..	127.0.0.1	127.0.0.1	TCP	66	1234 - 59786	[ACK] Seq=1 Ack=294 Win=65280 Len=0 TSval=1049040947 TSecr=1049040947
425	1257.3995649..	127.0.0.1	127.0.0.1	TLSv1.3	1539	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application D..	
426	1257.3995889..	127.0.0.1	127.0.0.1	TCP	66	59786 - 1234	[ACK] Seq=294 Ack=1474 Win=64128 Len=0 TSval=1049040949 TSecr=1049040949
427	1257.4001837..	127.0.0.1	127.0.0.1	TLSv1.3	146	Change Cipher Spec, Application Data	
428	1257.4003874..	127.0.0.1	127.0.0.1	TLSv1.3	639	Application Data, Application Data, Application Data	
429	1257.4396895..	127.0.0.1	127.0.0.1	TCP	66	59786 - 1234	[ACK] Seq=374 Ack=2047 Win=65536 Len=0 TSval=1049040989 TSecr=1049040949
430	1262.1800458..	127.0.0.1	127.0.0.1	TLSv1.3	93	Application Data	
431	1262.1803261..	127.0.0.1	127.0.0.1	TLSv1.3	140	Application Data	
432	1262.1803335..	127.0.0.1	127.0.0.1	TCP	66	59786 - 1234	[ACK] Seq=401 Ack=2121 Win=65536 Len=0 TSval=1049045729 TSecr=1049045729
433	1298.3538932..	127.0.0.1	127.0.0.1	TCP	74	32812 - 1234	[SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=1049081903 TSecr=0 WS=128
434	1298.3539016..	127.0.0.1	127.0.0.1	TCP	74	1234 - 32812	[SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=1049081903 TSecr=1049081903
435	1298.3539089..	127.0.0.1	127.0.0.1	TCP	66	32812 - 1234	[ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1049081903 TSecr=1049081903
436	1298.3553298..	127.0.0.1	127.0.0.1	TLSv1.3	359	Client Hello	
437	1298.3553359..	127.0.0.1	127.0.0.1	TCP	66	1234 - 32812	[ACK] Seq=1 Ack=294 Win=65280 Len=0 TSval=1049081904 TSecr=1049081904
438	1298.3562851..	127.0.0.1	127.0.0.1	TLSv1.3	1539	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application D..	
439	1298.3563046..	127.0.0.1	127.0.0.1	TCP	66	32812 - 1234	[ACK] Seq=294 Ack=1474 Win=64128 Len=0 TSval=1049081905 TSecr=1049081905
440	1298.3568397..	127.0.0.1	127.0.0.1	TLSv1.3	146	Change Cipher Spec, Application Data	
441	1298.3569926..	127.0.0.1	127.0.0.1	TLSv1.3	639	Application Data, Application Data, Application Data	
442	1298.3960821..	127.0.0.1	127.0.0.1	TCP	66	32812 - 1234	[ACK] Seq=374 Ack=2047 Win=65536 Len=0 TSval=1049081945 TSecr=1049081906
443	1311.7618497..	127.0.0.1	127.0.0.1	TLSv1.3	94	Application Data	
444	1311.7667067..	127.0.0.1	127.0.0.1	TLSv1.3	141	Application Data	
445	1311.7667117..	127.0.0.1	127.0.0.1	TCP	66	32812 - 1234	[ACK] Seq=402 Ack=2122 Win=65536 Len=0 TSval=1049095316 TSecr=1049095316
446	1311.7667327..	127.0.0.1	127.0.0.1	TLSv1.3	117	Application Data	
447	1311.7667396..	127.0.0.1	127.0.0.1	TCP	66	59786 - 1234	[ACK] Seq=401 Ack=2172 Win=65536 Len=0 TSval=1049095316 TSecr=1049095316
448	1317.2282739..	127.0.0.53	127.0.0.53	DNS	82	Standard query 0x3c32 A www.meta.ai OPT	
449	1317.2306901..	127.0.0.1	127.0.0.53	DNS	82	Standard query response 0x3c3f AAAA www.meta.ai OPT	
450	1317.2581305..	127.0.0.53	127.0.0.1	DNS	134	Standard query response 0x3c32 A www.meta.ai CNAME star.c10r.facebook.com A 31.13.80.8 OPT	
451	1317.2604893..	127.0.0.53	127.0.0.1	DNS	146	Standard query response 0x3c3f AAAA www.meta.ai CNAME star.c10r.facebook.com AAAA 2a03:2880:f00e:a:fa..	
452	1326.1476224..	127.0.0.1	127.0.0.1	TLSv1.3	101	Application Data	
453	1326.1478423..	127.0.0.1	127.0.0.1	TLSv1.3	110	Application Data	
454	1326.1478490..	127.0.0.1	127.0.0.1	TCP	66	32812 - 1234	[ACK] Seq=402 Ack=2166 Win=65536 Len=0 TSval=1049109697 TSecr=1049109697
455	1326.1876746..	127.0.0.1	127.0.0.1	TCP	66	1234 - 59786	[ACK] Seq=2172 Ack=436 Win=65536 Len=0 TSval=1049109737 TSecr=1049109697
456	1340.7702470..	127.0.0.1	127.0.0.1	TLSv1.3	105	Application Data	
457	1340.7705217..	127.0.0.1	127.0.0.1	TLSv1.3	115	Application Data	
458	1340.7705335..	127.0.0.1	127.0.0.1	TCP	66	59786 - 1234	[ACK] Seq=436 Ack=2221 Win=65536 Len=0 TSval=1049124319 TSecr=1049124319
459	1340.8116332..	127.0.0.1	127.0.0.1	TCP	66	1234 - 32812	[ACK] Seq=2166 Ack=441 Win=65536 Len=0 TSval=1049124361 TSecr=1049124319
460	1346.4356604..	127.0.0.1	127.0.0.1	TLSv1.3	99	Application Data	
461	1346.4356747..	127.0.0.1	127.0.0.1	TCP	66	1234 - 59786	[ACK] Seq=2221 Ack=469 Win=65536 Len=0 TSval=1049129985 TSecr=1049129985
462	1346.4359675..	127.0.0.1	127.0.0.1	TLSv1.3	108	Application Data	
463	1346.4359756..	127.0.0.1	127.0.0.1	TCP	66	32812 - 1234	[ACK] Seq=441 Ack=2208 Win=65536 Len=0 TSval=1049129985 TSecr=1049129985
464	1350.1297024..	127.0.0.1	127.0.0.1	TLSv1.3	92	Application Data	
465	1350.1297121..	127.0.0.1	127.0.0.1	TCP	66	1234 - 32812	[ACK] Seq=2208 Ack=467 Win=65536 Len=0 TSval=1049133679 TSecr=1049133679
466	1350.1299030..	127.0.0.1	127.0.0.1	TLSv1.3	102	Application Data	
467	1350.1299100..	127.0.0.1	127.0.0.1	TCP	66	59786 - 1234	[ACK] Seq=469 Ack=2257 Win=65536 Len=0 TSval=1049133679 TSecr=1049133679

This image shows packet transfers captured between a client and a server, specifically related to the TCP and TLS handshake process.

Order of Packet Transfer:

1. The client sends a SYN request to establish a connection with the server. **TCP SYN** (Packet 420)
2. The server responds with a **SYN-ACK** to acknowledge the client's SYN request. **TCP SYN-ACK** (Packet 421)
3. The client sends back an **ACK** packet to confirm receipt of the server's SYN-ACK. **TCP ACK** (Packet 422)
4. The client initiates the TLS handshake with a **Client Hello message**, which indicates supported versions of TLS (TLS 1.3). **TLS Client Hello** (Packet 423)
5. The server responds with a **Server Hello message**. **TLS Server Hello** (Packet 425)
6. The server sends a Change Cipher Spec message to indicate **encrypted communication**.

This image below shows detailed information for a specific packet:

- Source IP: 127.0.0.1 (localhost).
- Destination IP: 127.0.0.1 (localhost).
- Source Port: 59786
- Destination Port: 1234

The image displays a Wireshark packet capture of a network traffic. The packet list on the left shows a series of packets, with packet 422 selected. The packet details pane on the right shows the structure of the selected packet, which is a TCP ACK packet. The packet is from source IP 127.0.0.1 (localhost) to destination IP 127.0.0.1 (localhost). The source port is 59786 and the destination port is 1234. The packet length is 293 bytes. The details pane shows the TCP segment and the TLS Client Hello message. The TLS Client Hello message is a TLSv1.3 record layer, content type handshake, version 1.0 (0x0301). The packet is captured on the interface eth0.

No.	Time	Source	Destination	Protocol	Length	Info
422	1257.3918720	127.0.0.1	127.0.0.1	TCP	66	59786 → 1234 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1049040941 TSecr=1049040941
423	1257.3981968	127.0.0.1	127.0.0.1	TLSv1.3	359	Client Hello
424	1257.3981208	127.0.0.1	127.0.0.1	TCP	66	1234 → 59786 [ACK] Seq=1 Ack=294 Win=65280 Len=0 TSval=1049040947 TSecr=1049040947
425	1257.3995640	127.0.0.1	127.0.0.1	TLSv1.3	1539	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data
426	1257.3995889	127.0.0.1	127.0.0.1	TCP	66	59786 → 1234 [ACK] Seq=294 Ack=1474 Win=64128 Len=0 TSval=1049040949 TSecr=1049040949
427	1257.4001837	127.0.0.1	127.0.0.1	TLSv1.3	146	Change Cipher Spec, Application Data
428	1257.4003674	127.0.0.1	127.0.0.1	TLSv1.3	639	Application Data, Application Data, Application Data
429	1257.4396895	127.0.0.1	127.0.0.1	TCP	66	59786 → 1234 [ACK] Seq=374 Ack=2047 Win=65536 Len=0 TSval=1049040989 TSecr=1049040949
430	1262.1800458	127.0.0.1	127.0.0.1	TLSv1.3	93	Application Data

Total Length: 345
Identification: 0x471b (18203)
010 = Flags: 0x2, Don't Fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xf481 [validation disabled]
Header Checksum: 0xf481 [validation disabled]
Source Address: 127.0.0.1
Destination Address: 127.0.0.1
Transmission Control Protocol, Src Port: 59786, Dst Port: 1234, Seq: 1, Ack: 1, Len: 293
Source Port: 59786
Destination Port: 1234
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 293]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 348932992
[Next Sequence Number: 294 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment Number (raw): 1130870092
1000 = Header Length: 32 bytes (8)
Flags: 0x010 (PSH, ACK)
Window: 512
[Calculated window size: 65536]
[Window size scaling factor: 128]
Checksum: 0xffff [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
TCP payload (293 bytes)
Transport Layer Security
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Handshake Protocol: Client Hello

The images above show that we can't see the actual messages being sent. The data is encrypted, as you can tell from the label "Encrypted Application Data" in the capture. The hex values shown in the packet don't show any readable content, which means the messages are securely encrypted and protected. The **PSH** and **ACK** flags are set, indicating that the data is being pushed to the application and acknowledging the receipt of previous data.

From an end-user perspective, there would be no noticeable difference in terms of interaction with the application. The user interface and general behavior would remain the same.

Phase 3:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	UDP	47	38902 → 1234 Len=5
2	0.000177535	127.0.0.1	127.0.0.1	ADwin ...	94	
3	10.915412778	127.0.0.1	127.0.0.1	UDP	48	35626 → 1234 Len=6
4	10.915562345	127.0.0.1	127.0.0.1	UDP	95	1234 → 35626 Len=53
5	10.915582054	127.0.0.1	127.0.0.1	UDP	71	1234 → 38902 Len=29
6	26.589519913	127.0.0.1	127.0.0.1	UDP	53	38902 → 1234 Len=11
7	26.589692383	127.0.0.1	127.0.0.1	UDP	62	1234 → 35626 Len=20
8	31.693728913	127.0.0.1	127.0.0.1	UDP	51	35626 → 1234 Len=9
9	31.693868894	127.0.0.1	127.0.0.1	UDP	61	1234 → 38902 Len=19
10	53.706330050	127.0.0.1	127.0.0.1	UDP	55	38902 → 1234 Len=13
11	53.706483142	127.0.0.1	127.0.0.1	ADwin ...	64	
12	59.131594770	127.0.0.1	127.0.0.1	UDP	51	35626 → 1234 Len=9
13	59.131753002	127.0.0.1	127.0.0.1	UDP	61	1234 → 38902 Len=19
14	66.496581141	127.0.0.1	127.0.0.1	UDP	44	38902 → 1234 Len=2
15	66.496771495	127.0.0.1	127.0.0.1	UDP	67	1234 → 35626 Len=25

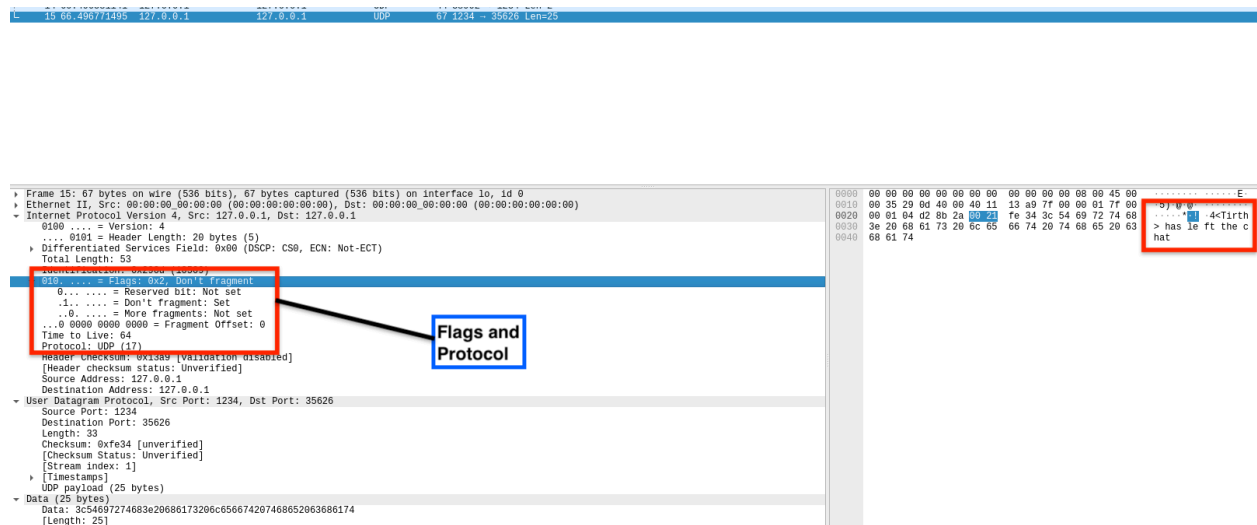
The above image shows the sequence of UDP packets exchanged between the client and the server.

Order of Packet Transfer for UDP:

1. The client sends the first **UDP datagram** to the server. Since UDP is connectionless, this is sent without any prior handshake.(Packet 1)
2. After the initial message, subsequent UDP packets contain the chat messages sent by the client to the server and vice versa. (Packet3, Packet 7 and packets 11-15).
3. The client sends a message indicating that the user has left the chat, marking the end of communication.(Packet 15)

The protocol used is **UDP (User Datagram Protocol)**, which is connectionless and does not guarantee message delivery.

These messages are not secure. The reason is that the messages are transmitted in plain text without any encryption. Anyone capturing these packets can easily view the content, as shown above the name "**Tirth**" is clearly readable.



This image shows the "**Don't Fragment**" flag in the UDP packet. It means that the message should be sent in one piece without being split into smaller parts. UDP is simpler and doesn't have extra flags for things like starting or ending a connection.