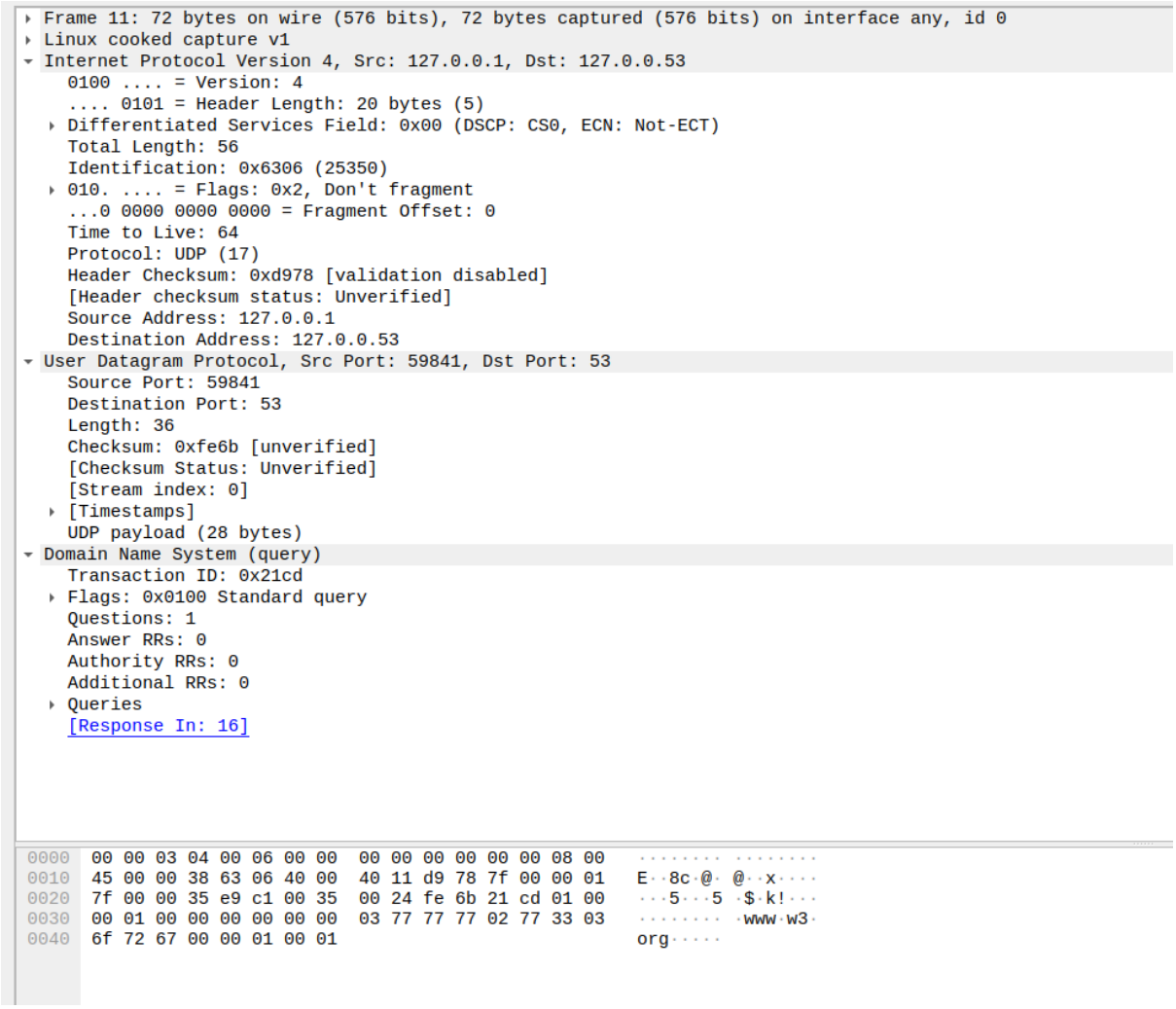
LAB 3
WIRESHARK

NAME-KUSHALA SARADA A V
210905189
ROLL NUMBER 33

2. Analyzing UDP datagrams using Wireshark:
• Start your web browser and clear the browser's cache memory, but do not access any website yet.
• Open Wireshark and start capturing.
• Go back to your web browser and retrieve any file from a website. Wireshark starts capturing packets.
• After enough packets have been captured, stop Wireshark, and save the captured file.
•
Using the captured file, analyze TCP & UDP packets captured
.Note: DNS uses UDP for name resolution & HTTP uses TCP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Routerbo_3c:11:e5		ARP	62	Who has 10.70.2.14? Tell 10.70.0.2
2	0.000000412	Routerbo_3c:11:e5		ARP	62	Who has 10.70.2.14? Tell 10.70.0.2
3	2.560571889	142.250.183.67	10.70.1.93	TLSv1.2	141	Application Data
4	2.561035483	10.70.1.93	142.250.183.67	TCP	68	42116 → 443 [FIN, ACK] Seq=1 Ack=74 Win=501 Len=0 TSval=2288054789 TSecr=188284695
5	2.599069828	142.250.183.67	10.70.1.93	TCP	68	443 → 42116 [FIN, ACK] Seq=74 Ack=2 Win=301 Len=0 TSval=188284821 TSecr=2288054789
6	2.599115200	10.70.1.93	142.250.183.67	TCP	68	42116 → 443 [ACK] Seq=2 Ack=75 Win=501 Len=0 TSval=2288054827 TSecr=188284821
7	2.739485427	142.250.183.67	10.70.1.93	TLSv1.2	141	Application Data
8	2.739812650	10.70.1.93	142.250.183.67	TCP	68	51388 → 443 [FIN, ACK] Seq=1 Ack=74 Win=501 Len=0 TSval=2288054967 TSecr=2174806903
9	2.875139222	142.250.183.67	10.70.1.93	TCP	68	443 → 51388 [FIN, ACK] Seq=74 Ack=2 Win=271 Len=0 TSval=2174807041 TSecr=2288054967
10	2.875175583	10.70.1.93	142.250.183.67	TCP	68	51388 → 443 [ACK] Seq=2 Ack=75 Win=501 Len=0 TSval=2288055103 TSecr=2174807041
11	2.999577224	127.0.0.1	127.0.0.53	DNS	72	Standard query 0x21cd A www.w3.org
12	2.999661673	127.0.0.1	127.0.0.53	DNS	72	Standard query 0x878e HTTPS www.w3.org
13	2.999869230	10.70.1.93	4.2.2.2	DNS	72	Standard query 0x89f5 A www.w3.org
14	3.000090065	10.70.1.93	4.2.2.2	DNS	72	Standard query 0xfbae HTTPS www.w3.org
15	3.074388604	4.2.2.2	10.70.1.93	DNS	563	Standard query response 0x89f5 A www.w3.org CNAME www.w3.org.cdn.cloudflare.net A 104.18.22.19 A 104.18.23.19 NS l.root-servers.ne
16	3.074923704	127.0.0.53	127.0.0.1	DNS	147	Standard query response 0x21cd A www.w3.org CNAME www.w3.org.cdn.cloudflare.net A 104.18.23.19 A 104.18.22.19
17	3.097706370	10.70.1.93	104.18.23.19	QUIC	1294	Initial, DCID=55a99a66ea94e05f, PKN: 1, PADDING, CRYPTO, PADDING, CRYPTO, CRYPTO, CRYPTO, PADDING, PING, PING, CRYPTO, PADDING, CR
18	3.101997082	4.2.2.2	10.70.1.93	DNS	636	Standard query response 0xfbae HTTPS www.w3.org CNAME www.w3.org.cdn.cloudflare.net HTTPS NS d.root-servers.net NS a.root-servers..
19	3.102520647	127.0.0.53	127.0.0.1	DNS	188	Standard query response 0x878e HTTPS www.w3.org CNAME www.w3.org.cdn.cloudflare.net HTTPS
20	3.102540025	127.0.0.1	127.0.0.53	ICMP	216	Destination unreachable (Port unreachable)
21	3.141176524	10.70.1.93	142.250.192.68	UDP	990	52591 → 443 Len=946
22	3.141703277	10.70.1.93	142.250.192.68	UDP	487	52591 → 443 Len=443
23	3.147069249	10.70.1.93	142.251.42.10	UDP	210	37734 → 443 Len=166
24	3.158441949	104.18.23.19	10.70.1.93	QUIC	1244	Protected Payload (KP0)
25	3.163781115	104.18.23.19	10.70.1.93	QUIC	1244	Protected Payload (KP0)
26	3.168411095	10.70.1.93	104.18.23.19	QUIC	1294	Initial, DCID=01aad016d88e6938b3a84e165e8e7e962d1c885a, PKN: 2, ACK, PADDING
27	3.173789128	104.18.23.19	10.70.1.93	QUIC	1244	Handshake, SCID=01aad016d88e6938b3a84e165e8e7e962d1c885a
28	3.173789364	104.18.23.19	10.70.1.93	QUIC	813	Handshake, SCID=01aad016d88e6938b3a84e165e8e7e962d1c885a
29	3.174319530	10.70.1.93	104.18.23.19	QUIC	97	Handshake, DCID=01aad016d88e6938b3a84e165e8e7e962d1c885a
30	3.187931579	142.251.42.10	10.70.1.93	UDP	71	443 → 37734 Len=27
31	3.190275853	142.250.192.68	10.70.1.93	UDP	76	443 → 52591 Len=32
32	3.191091232	142.250.192.68	10.70.1.93	UDP	76	443 → 52591 Len=32
33	3.197139471	10.70.1.93	104.18.23.19	QUIC	129	Handshake, DCID=01aad016d88e6938b3a84e165e8e7e962d1c885a
34	3.197332961	10.70.1.93	104.18.23.19	QUIC	126	Protected Payload (KP0), DCID=01aad016d88e6938b3a84e165e8e7e962d1c885a
35	3.209081664	10.70.1.93	142.250.192.68	UDP	77	52591 → 443 Len=33
36	3.216263108	10.70.1.93	142.251.42.10	UDP	77	37734 → 443 Len=33
37	3.222502662	104.18.23.19	10.70.1.93	QUIC	577	Protected Payload (KP0)
38	3.248970936	10.70.1.93	104.18.23.19	QUIC	89	Protected Payload (KP0), DCID=01aad016d88e6938b3a84e165e8e7e962d1c885a
39	3.283397065	104.18.23.19	10.70.1.93	QUIC	68	Protected Payload (KP0)
40	3.283397226	104.18.23.19	10.70.1.93	QUIC	68	Protected Payload (KP0)
41	3.283397275	104.18.23.19	10.70.1.93	QUIC	93	Protected Payload (KP0)
42	3.283565618	10.70.1.93	104.18.23.19	QUIC	89	Protected Payload (KP0), DCID=01aad016d88e6938b3a84e165e8e7e962d1c885a
43	3.283606550	10.70.1.93	104.18.23.19	QUIC	91	Protected Payload (KP0), DCID=01aad016d88e6938b3a84e165e8e7e962d1c885a
44	3.286198185	142.250.192.68	10.70.1.93	UDP	295	443 → 52591 Len=251

A.
In the packet list pane, select the first DNS packet. In the packet detail pane, select the User Datagram Protocol. The UDP hexdump will be highlighted in the packet byte lane. Using the hexdump, Answer the following:
a. the source port number.
b. the destination port number.
c. the total length of the user datagram.
d. the length of the data.
e. whether the packet is directed from a client to a server or vice versa.
f. the application-layer protocol.
g. whether a checksum is calculated for this packet or not.



A)59841
B)53
C)Total Length: 56
D)Length: 36
E)The packet is directed from a client to a server.
F)DNS
G)[Checksum Status: Unverified]

B. What are the source and destination IP addresses in the DNS query message? What are those
addresses in the response message? What is the relationship between the two?

In the DNS query:
- Source IP: 127.0.0.1
- Destination IP: 127.0.0.53

In the DNS response:
- Source IP: 127.0.0.53
- Destination IP: 127.0.0.1

The relationship: Query from client (127.0.0.1) to local DNS resolver (127.0.0.53), response from resolver to client.

C. What are the source and destination port numbers in the query message? What are those addresses in the response message? What is the relationship between the two? Which port number is a well-known port number?

In the DNS query:
- Source Port: 59841
- Destination Port: 53 (Well-known port for DNS)

In the DNS response:
- Source Port: 53
- Destination Port: 59841

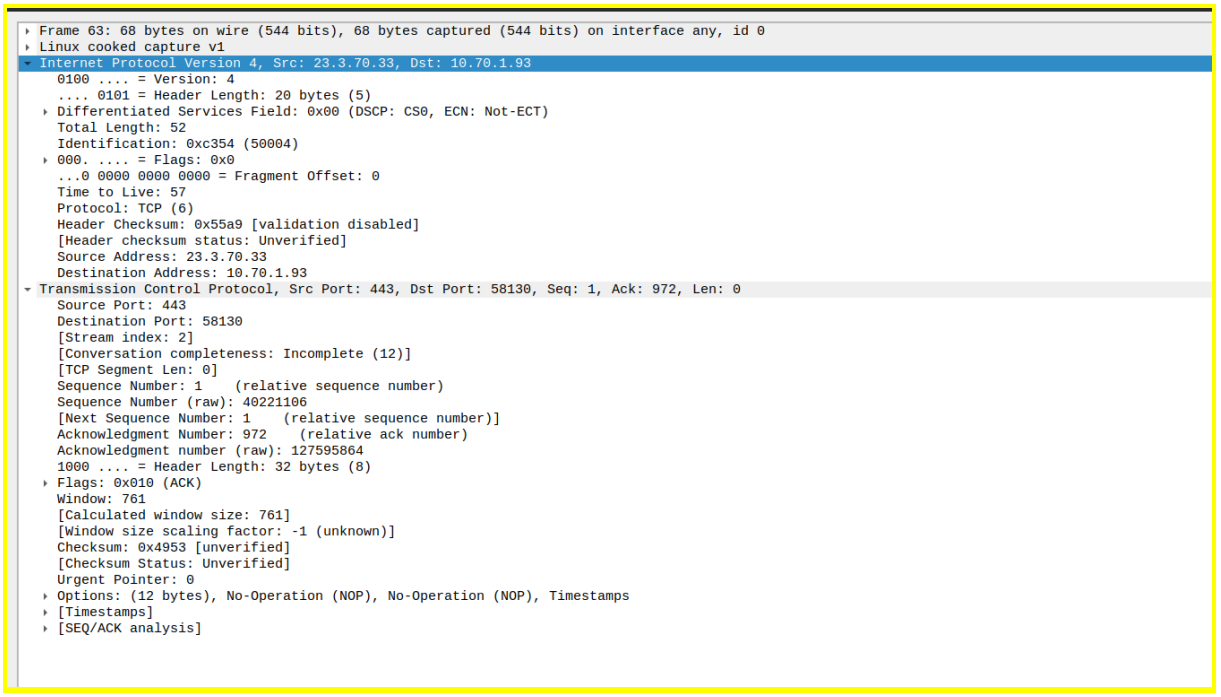
The relationship: The client (source port 59841) queries the DNS server (destination port 53), and the DNS server responds to the client's query.

The well-known port number is 53, which is used for DNS communication.

D. What is the length of the first packet? How many bytes of payload are carried by the first packet?

The length of the first packet is 72 bytes. The payload carried by the first packet is 28 bytes.

2b. Analyzing TCP packets using Wireshark:
Start your web browser and clear the browser's cache memory, but do not access any website yet.
■ Open Wireshark and start capturing.
■ Go back to your web browser and retrieve any file from a website. Wireshark starts capturing
packets.
■ After enough packets have been captured, stop Wireshark and save the captured file.
■ Using the captured file, select only those packets that use the service of TCP. For this purpose,
type tcp (lowercase) in the filter field and press Apply. The packet list pane of the Wireshark window should now display a bunch of packets.



Part I: Connection-Establishment Phase
Identify the TCP packets used for connection establishment. Note that the last packet used for
connection establish may have the application-layer as the source protocol.

Questions
Using the captured information, answer the following question in your lab report about packets
used for connection establishment.
1. What are the socket addresses for each packet?

The source socket address for the packet is 23.3.70.33:443, and the destination socket address is 10.70.1.93:58130.

2. What flags are set in each packet?
Flags: 0x010 (ACK)

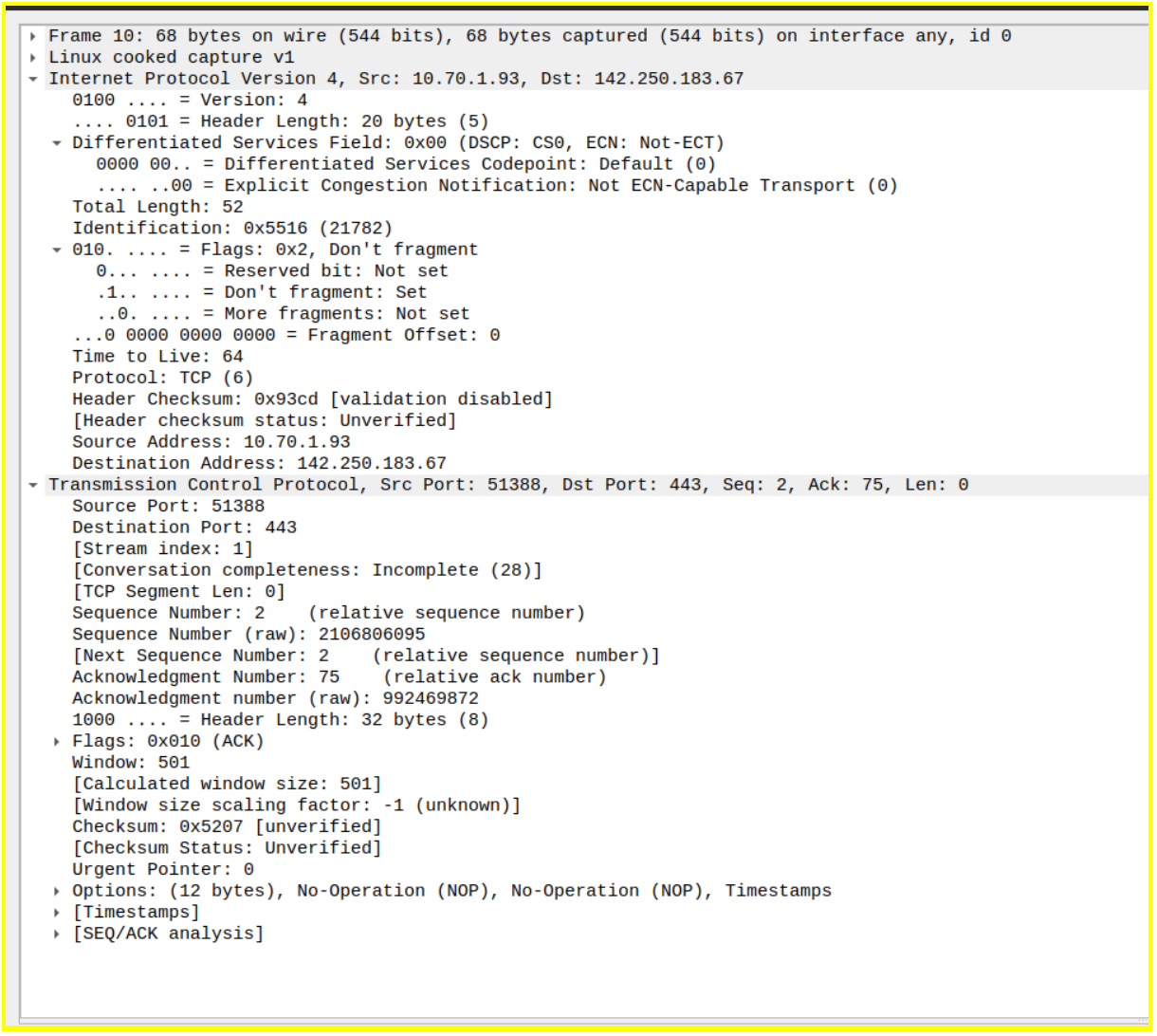
3. What are the sequence number and acknowledgment number of each packet?

1) Sequence Number: 1 (Relative sequence number: 40221106)
2) Acknowledgment Number: 972 (Relative acknowledgment number: 127595864)

4. What are the window size of each packet?

window size:761

Part II: Data-Transfer Phase
The data-transfer phase starts with an HTTP GET request message and ends with an HTTP OK
message.
Questions
Using the captured information, answer the following question in your lab report about packets
used for data transfer.



1. What TCP flags are set in the first data-transfer packet (HTTP GET message)?

The TCP flag set in the first data-transfer packet (HTTP GET message) is the ACK (Acknowledgment) flag.

2. How many bytes are transmitted in this packet?

3. How often does the receiver generate an acknowledgment? To which acknowledgment rule
(defined in Page 200 in the textbook) does your answer correspond to?

The receiver generates an acknowledgment for every two received packets. This corresponds to the "Delayed ACK" acknowledgment rule defined on Page 200 of the textbook.

4. How many bytes are transmitted in each packet? How are the sequence and acknowledgment
numbers related to number of bytes transmitted?

Each packet has 68 bytes. The sequence number marks the first byte's position, and the acknowledgment number indicates the next expected byte. The difference between them equals the bytes transmitted.

5. What are the original window sizes that are set by the client and the server? Are these numbers
expected? How do they change as more segments are received by the client?

Original window sizes: Client - 761, Server - 501. They reflect buffer space. Change as more data received due to flow control.

6. Explain how the window size is used in flow control?

The window size in TCP flow control indicates the amount of data a sender can transmit before waiting for acknowledgment. It prevents overwhelming the receiver. Sender adjusts based on acknowledgments and dynamic window updates, optimizing data transfer.

7. What is the purpose of the HTTP OK message in the data transfer phase?
The HTTP OK (200 OK) message is a response from the server to confirm that the requested resource has been successfully received and is available. It indicates that the data transfer phase can proceed as intended.