NETWORK ARCHITECTURE 1

HOME WORK -4

SUBMITTED BY

JASWANTH KRISHNA AAVULA

16133295

1. Consider the network shown below. Suppose AS3 and AS2 are running OSPF for their intra-AS routing protocol. Suppose AS1 and AS4 are running RIP for their intra-AS routing protocol. Suppose eBGP and iBGP are used for the inter-AS routing protocol. Initially suppose there is no physical link between AS2 and AS4.
2. Router 3c learns about prefix x from which routing protocol: OSPF, RIP, eBGP or iBGP?

Ans: Router 3c learns about prefix x from eBGP routing protocol. Router 3c uses inter-AS routing protocol to know about the destination x which is connected to 4a of AS4.

1. Router 3a learns about prefix x from which routing protocol?

Ans: It learns through iBGP inter routing protocol

1. Router 1c learns about prefix x from which routing protocol?

Ans: It learns through eBGP, inter-AS routing protocol

1. Router 1d learns about prefix x from which routing protocol?

Ans: It learns through iBGP inter routing protocol.

1. (a) Show the operation of Dijkstra’s (Link State) algorithm for computing the shortest path from C to all destinations.

Sol: NODES D(A) D(B) D(D) D(E)

C 1,C 4,C 1,C ∞

CD 1,C 4,C 4,D

CDA 4,C 4,D

CDAB 4,D

CDABE

B

A

E

D

C

Fig: Shortest Path

FORWARDING TABLE:

|  |  |
| --- | --- |
| DESTINATION | LINK |
| A | (C,A) |
| B | (C,B) |
| D | (C,D) |
| E | (C,D) |

(b) Show the distance table that would be computed by the distance vector algorithm in C. You don’t have to show all the steps of the distance vector algorithm.

Ans:

The formula used for computation of path using Distance vector algorithm is

dc(E) = min { c(C,B) + dB(E), c(C,D) + dD(E),c(C,A) + dA(E) }

|  |  |  |  |
| --- | --- | --- | --- |
| From c | Via A | Via B | Via D |
| To A | 1 | 9 | 3 |
| To B | 6 | 4 | 6 |
| To D | 3 | 9 | 1 |
| To E | 6 | 5 | 4 |

The algorithm selects the minimum value in every column. So the minimum distance from

C to A Via A is 1

C to B Via B is 4

C to D Via D is 1

C to E Via C is 4.

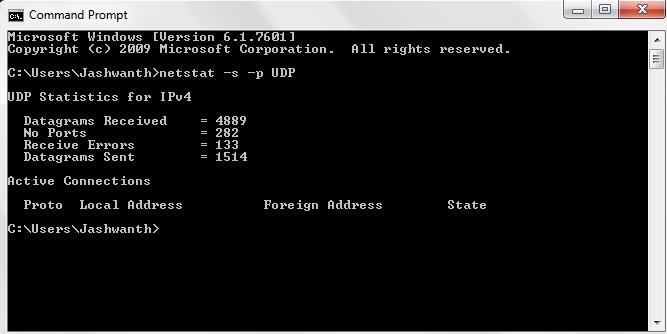
**LABORATORY HOMEWORK:**

1. Use netstat on your local host to find current UDP sessions and TCP connections.How many of them do you find and what port numbers are used?

Sol:

UDP:

UDP connections found = 0



TCP:

TCP connections found = 75

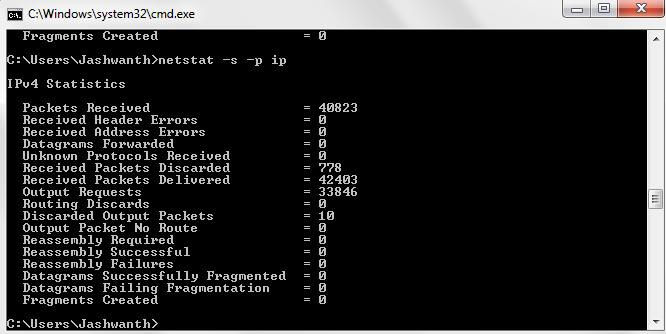
Port numbers = 2869, 5357, 12080, 27015, 49183, 49184, 49188, 49190, 49191, 49209, 49212, 49225, 49229, 49233, 49236, 49249, 49251, 49822, 49939, 50032, 50081, 50084, 50122, 50126, 50128, 50130, 50132, 50135, 50231, 50235, 50240, 50251, 50262, 50264, 52001, 49158, 49213, 49250, 49252, 49357, 49358, 49382, 49383, 50046, 50225, 50226, 50227. 50228, 50229, 50230, 50232, 50233, 50234, 50239, 50241, 50242, 50244, 50247, 50254, 50256, 50263, 50265, 50266.



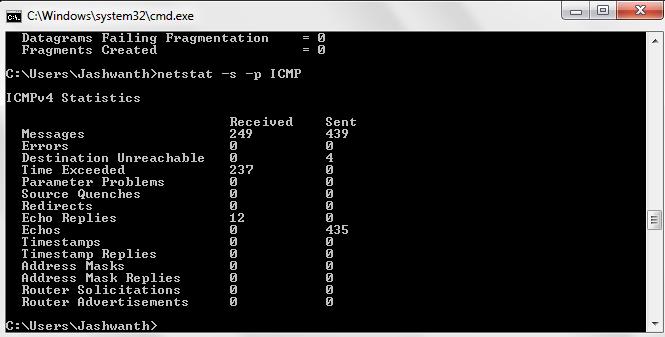
1. Find out per-protocol (IP, ICMP, TCP and UDP) statistics (using –s option).Then try ping or traceroute to a well-known server (eg. www.google.com). Now check per-protocol (IP, ICMP, TCP and UDP) statistics again. Summarize your findings.

Sol:

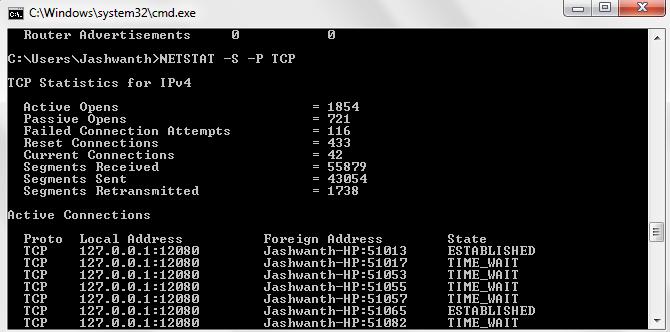
***IP statistics:***

******

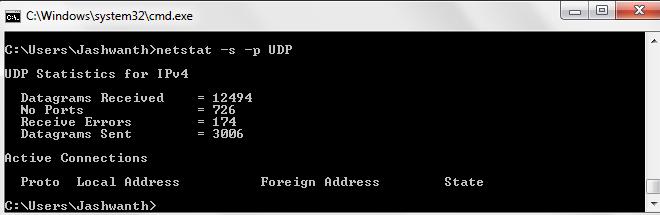
***ICMP STATISTICS:***

******

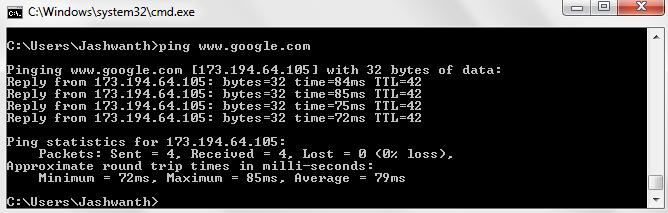
***TCP STATISTICS:***

******

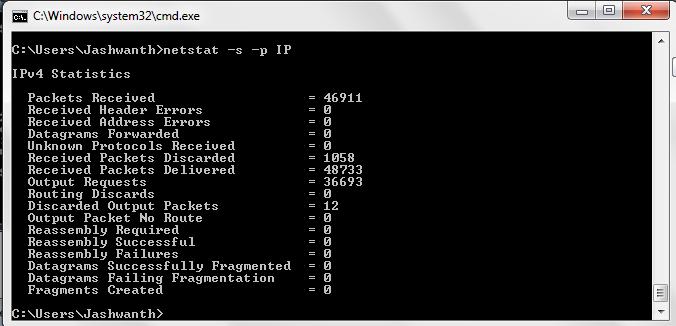
***UDP STATISTICS:***

******

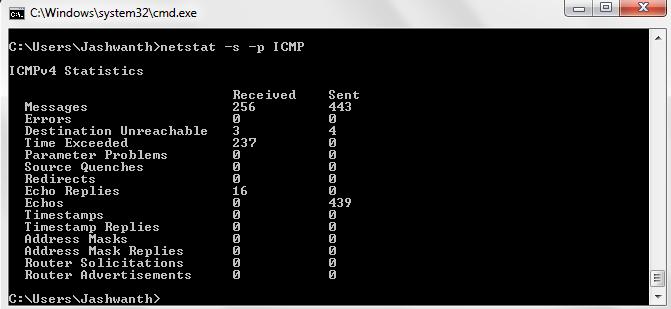
***PING TO*** [***www.google.com***](http://www.google.com)

******

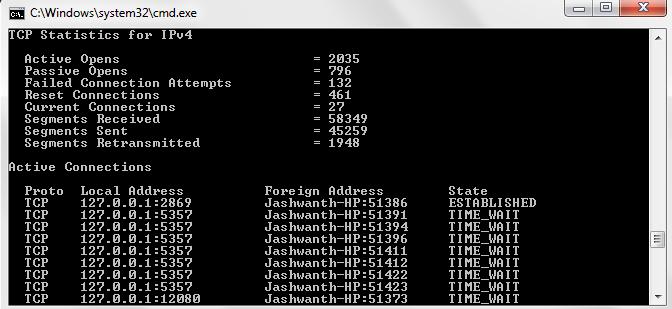
***IP STATISTICS AFTER USING PING:***

******

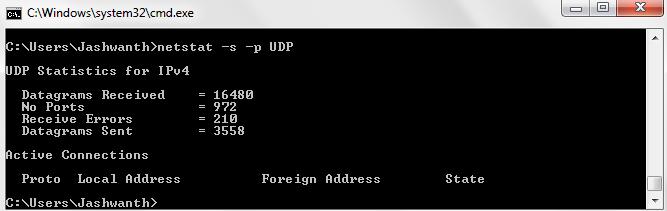
***ICMP STATISTICS AFTER USING PING:***

******

***TCP STATISTICS AFTER USING PING:***

******

***UDP STATISTICS AFTER USING PING:***

******

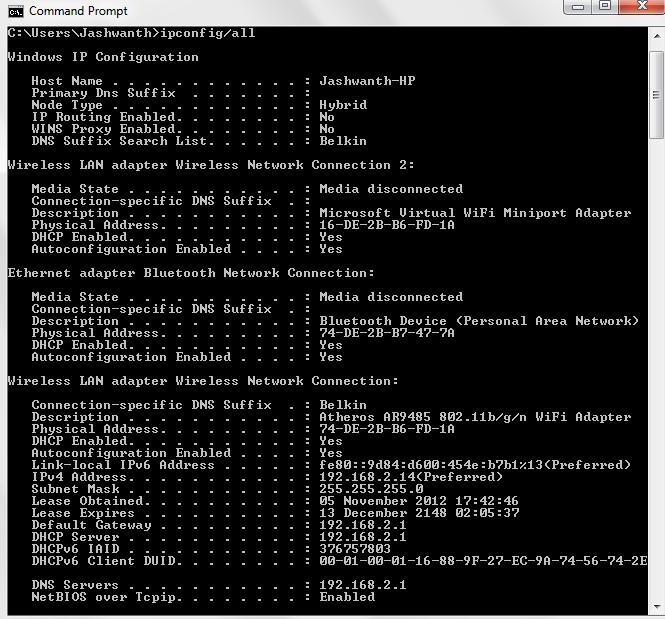
To summarise the findings when we send a request to [www.google.com](http://www.google.com) using ping then different parameters like number of packets sent, packets discarded, connections established would increase when compared to the values that are calculated prior to using ping command.

1. What are the Physical and IP addresses of the host?

Ans:

Physical address:74-DE-2B-B6-FD-1A

Ip Address: 192.168.2.14



1. How many bits are for the subnet mask? What is the subnet (not subnet mask) of the host?

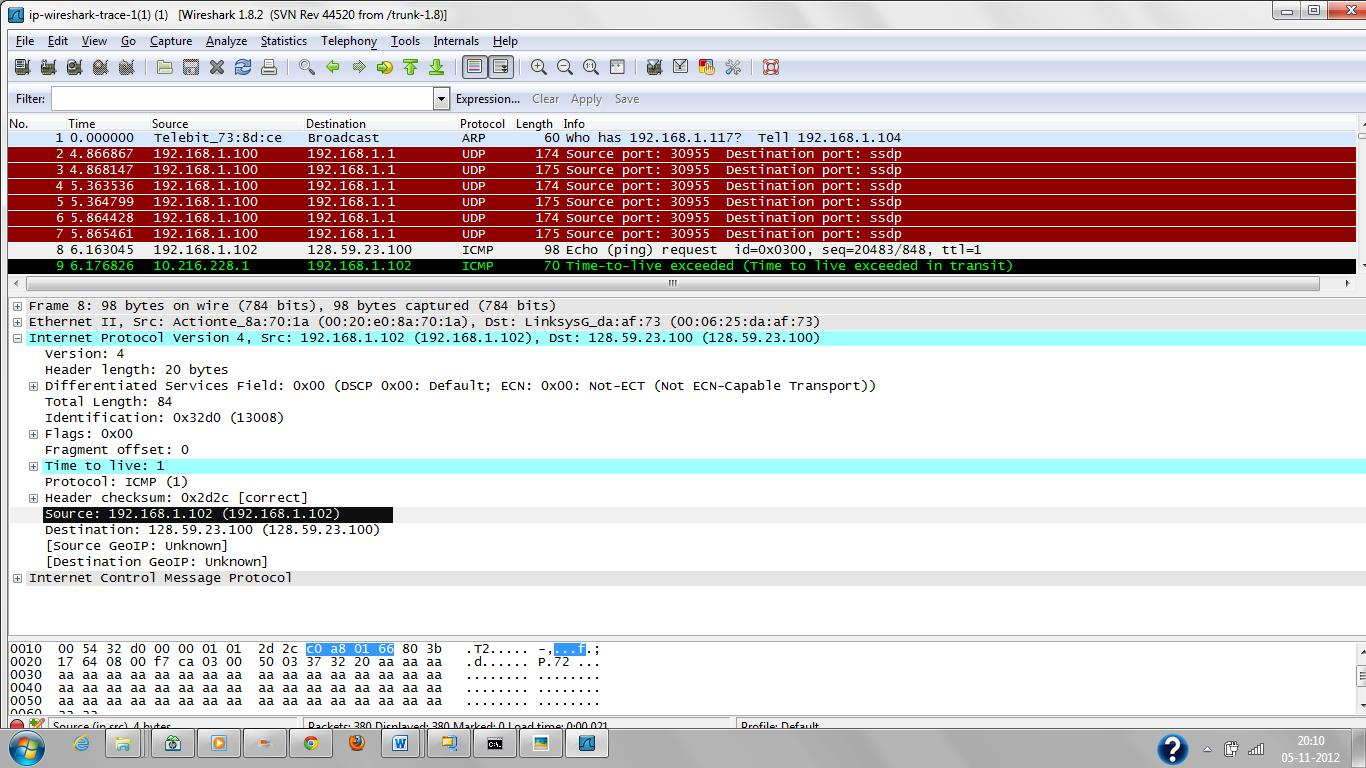
Ans: There are 32 bits in the subnet mask. Subnet of the host is 192.168.2.0

**PART-2 (WIRESHARK)**

1. Select the first ICMP Echo Request message sent by the computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of the user's computer?

Sol:

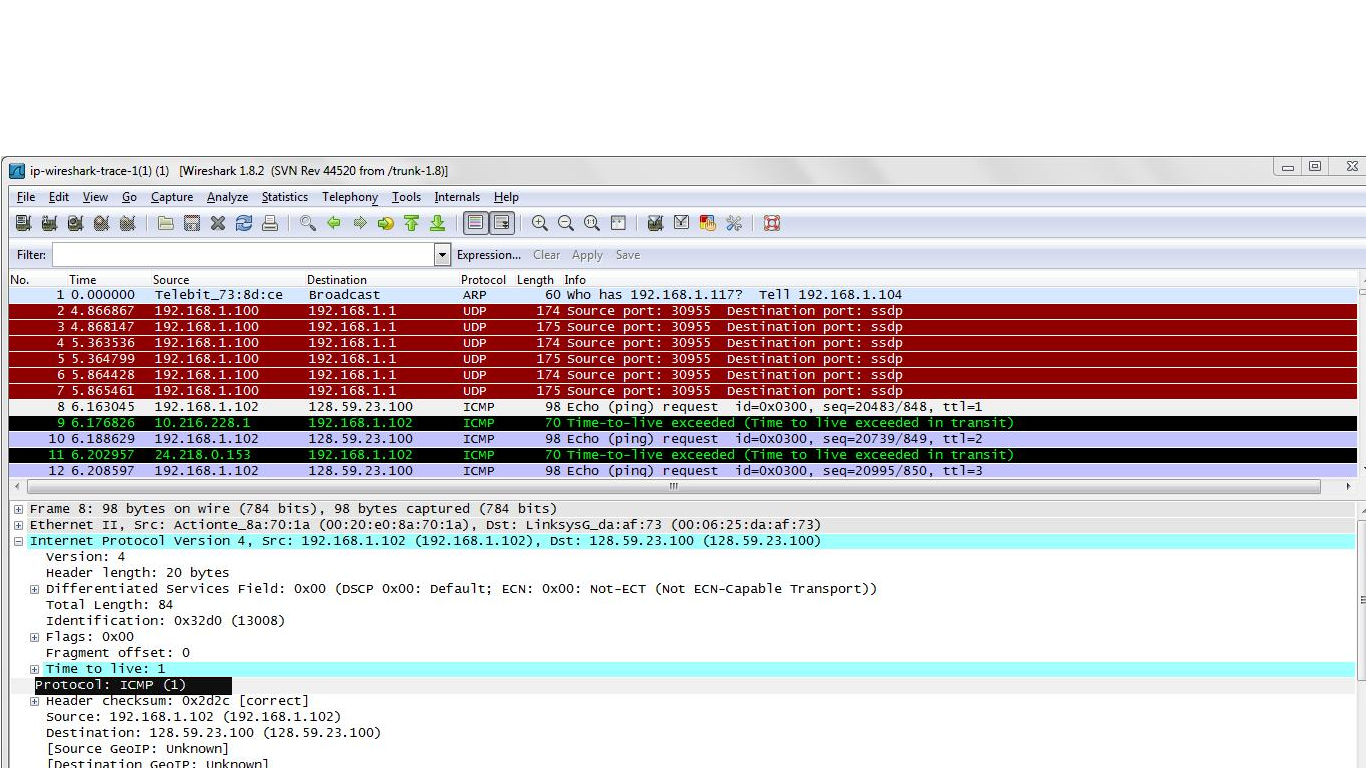
IP Address of user computer: 192.168.1.102



2. Within the IP packet header, what is the value in the upper layer protocol field?

Ans:

The value in the upper layer protocol field is 1.

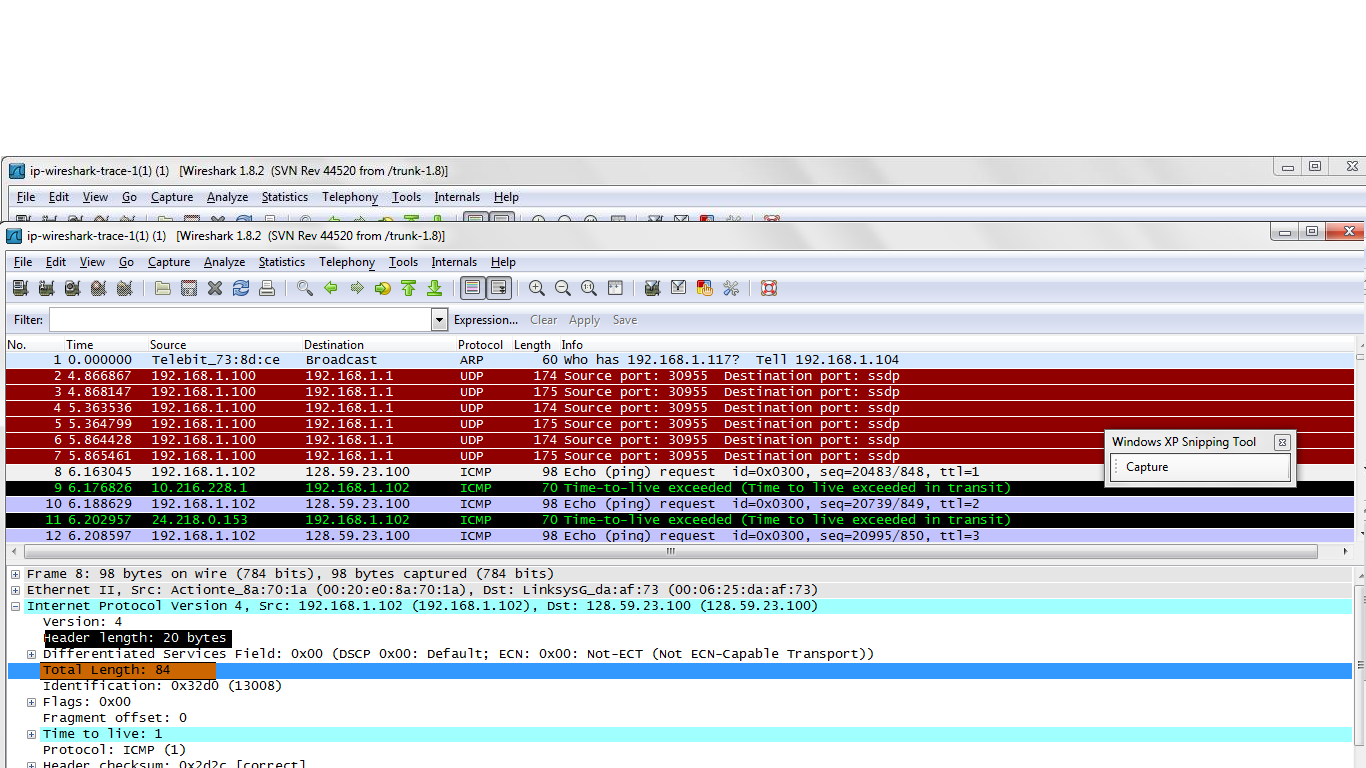


3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Ans:

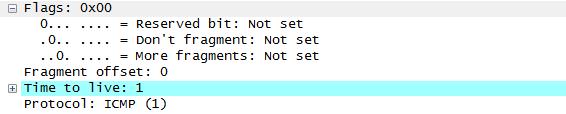
There are 20 bytes in IP header.

Number of bytes in the payload of IP datagram = 84-20 = 64 bytes.



4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

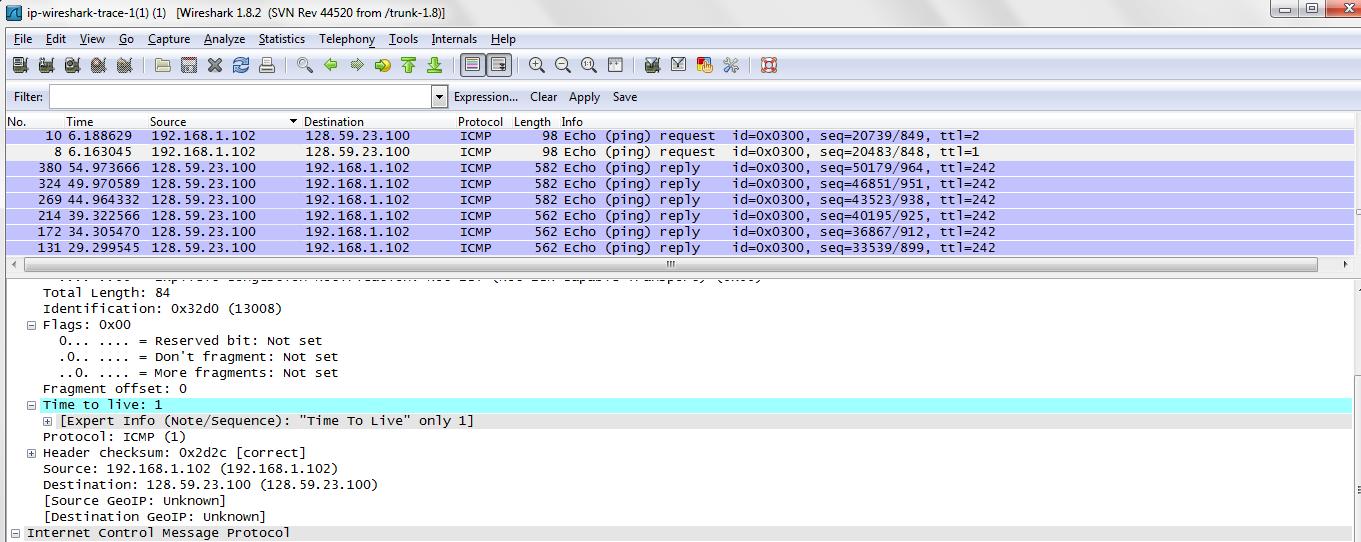
Ans: The datagram has not been fragmented. As the flag bits are 0X00 it can be determined that datagram has not been fragmented.



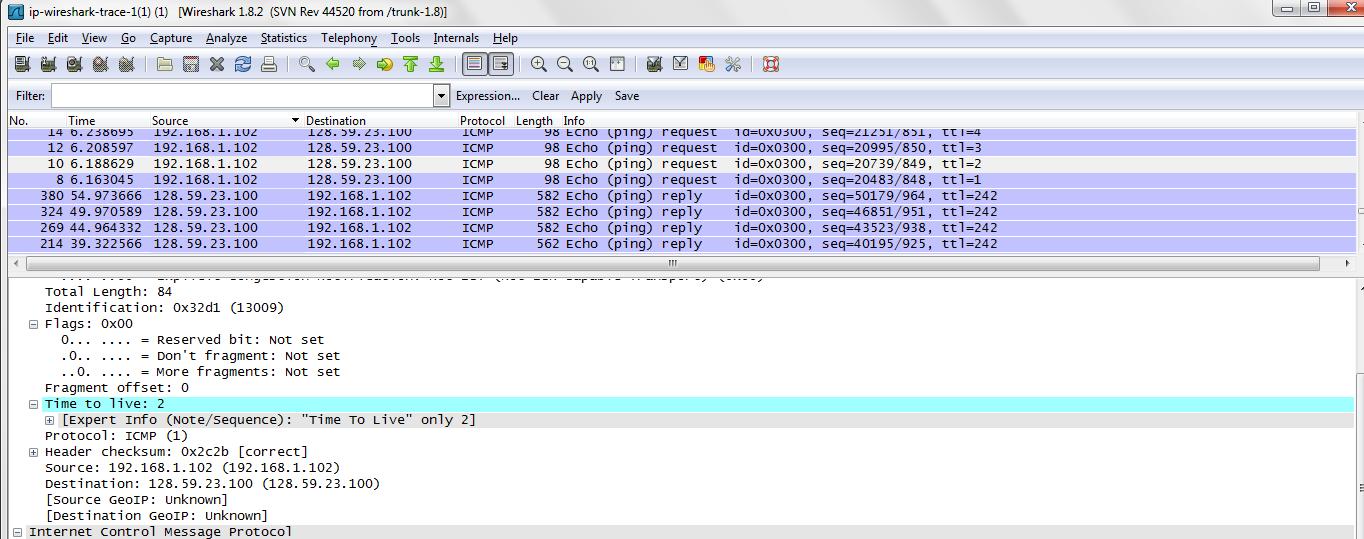
5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by the computer?

Ans:

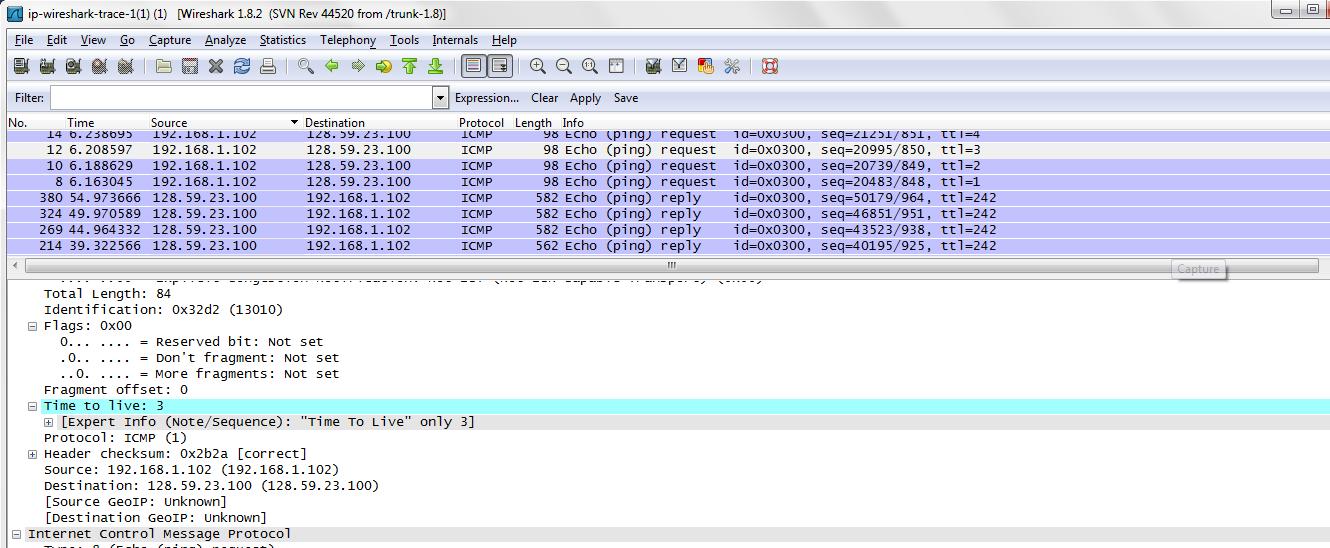
Datagram No 8



Datagram 10



Datgram 12



The fields in the IP datagram that change from one datagram to the next within this series of ICMP messages are Identification, Checksum and Time To Live.

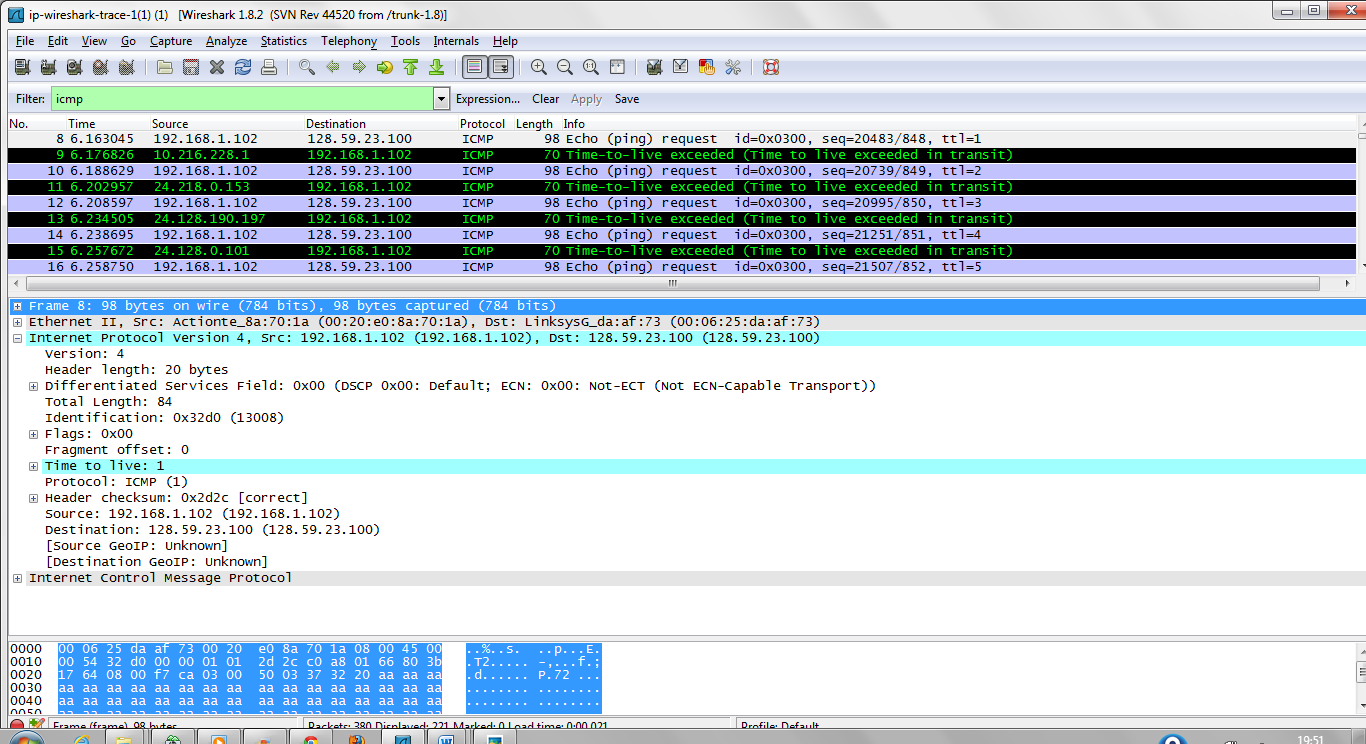
6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

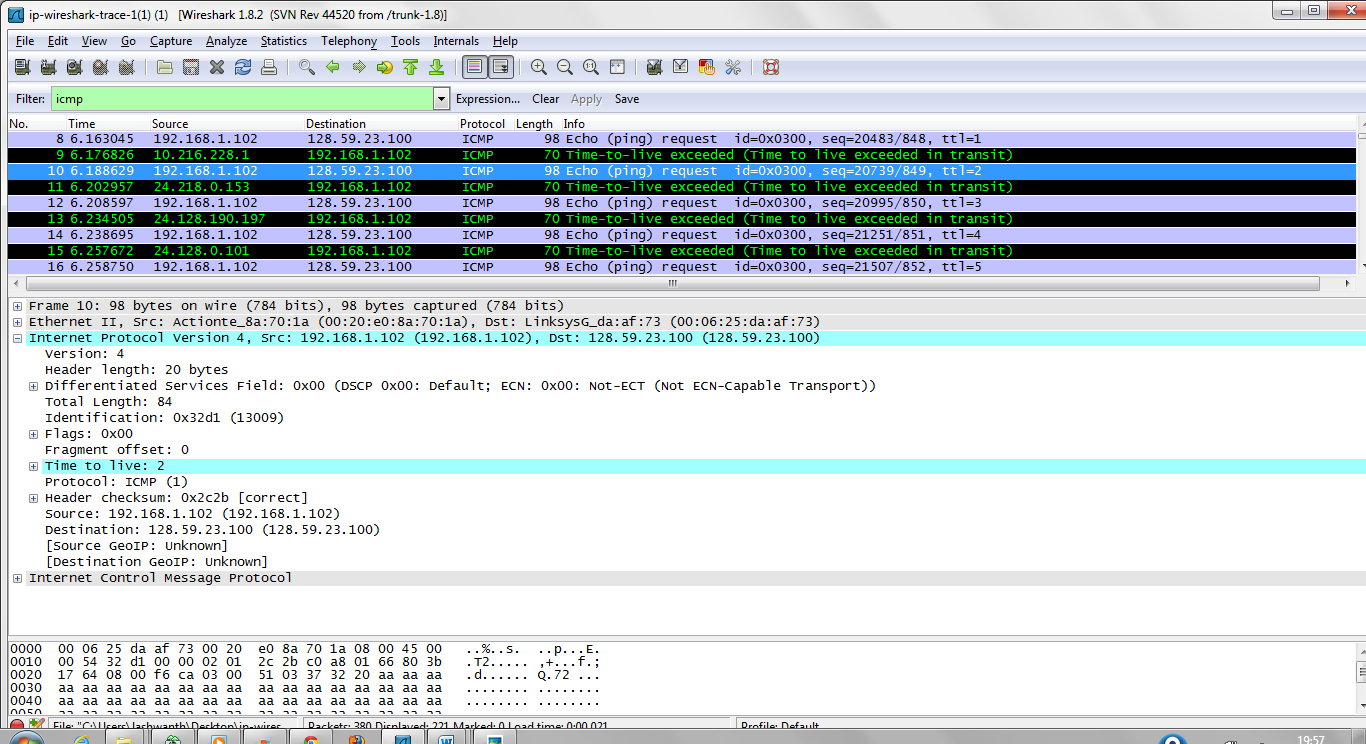
Ans:

As the webpage being accessed is same the fields like version, header length, flags, fragment offset, total length, source address, and destination address field stay constant.

The fields like identification, time to live, header checksum fields change because each packet has unique identification and factors like time to live and checksum are generated for individual elements.

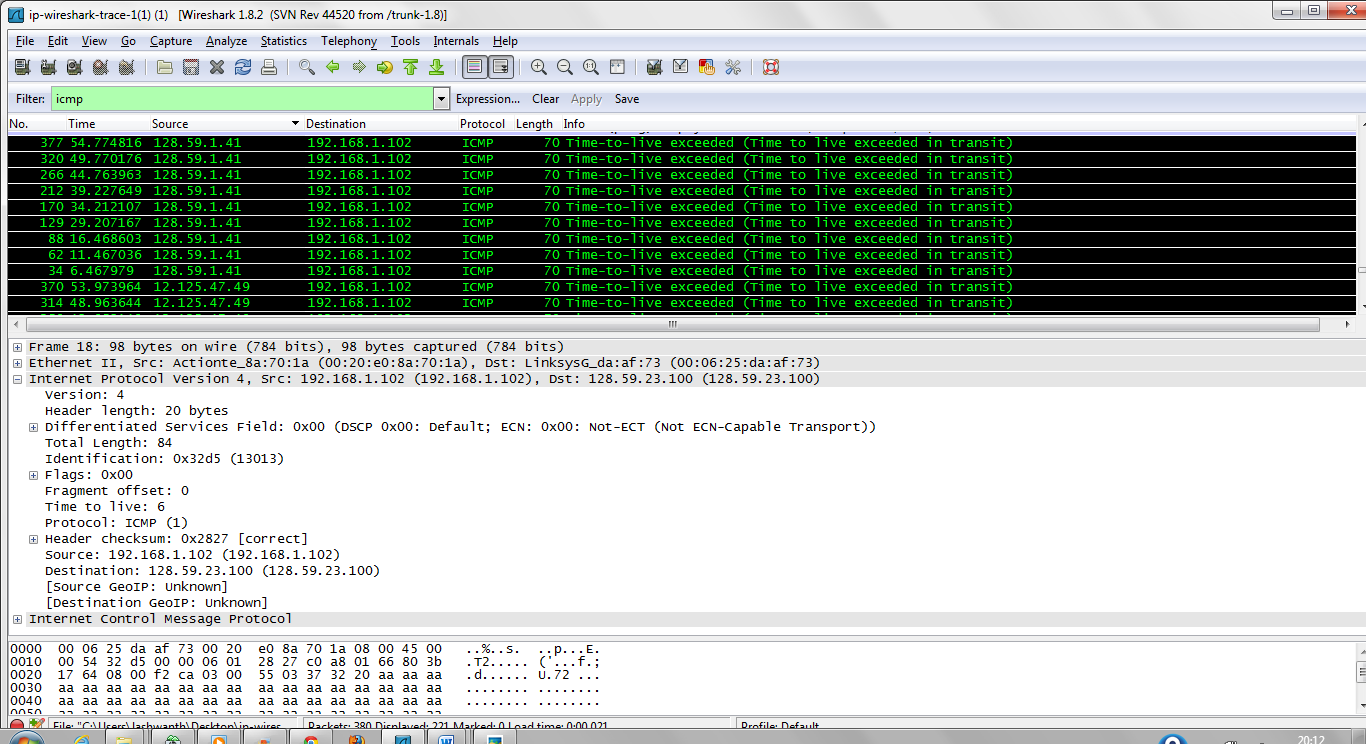
These changes can be identified by examining the following snapshots.





7. Describe the pattern you see in the values in the Identification field of the IP datagram Next (with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to the computer by the nearest (first hop) router.

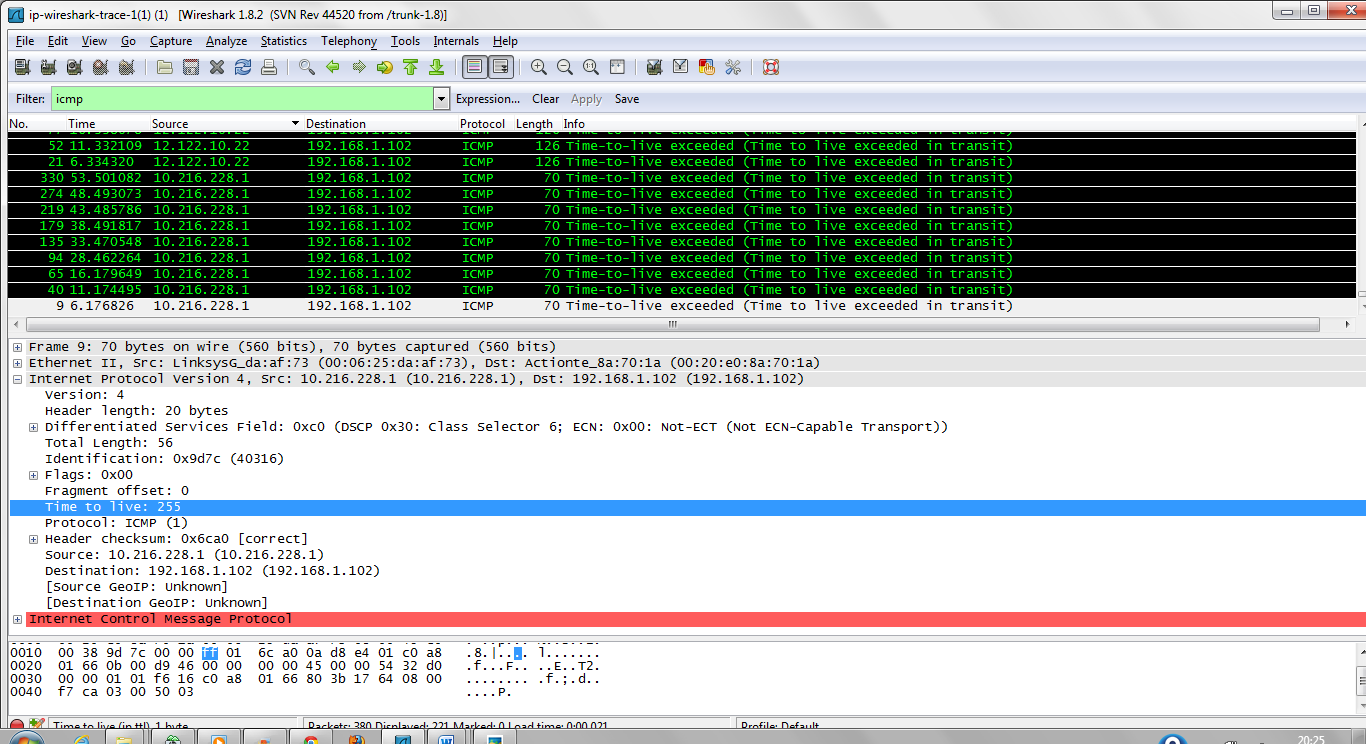
Ans: It can be inferred that in the Identification field of the IP datagram the value is increased by 1

.

8. What is the value in the Identification field and the TTL field?

Ans: Value in Identification Field = 0x9d7c

Time to live = 225



9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to the computer by the nearest (first hop) router? Why?

Ans: Identification field value changes and TTL field remains unchanged for all the ICMP-TTL exceeded replies sent to the computer because no datagram is sent to router. If datagram is sent to router then TTL might have changed.

