**SAN JOSE STATE UNIVERSITY**

**Charles W. Davidson College of Engineering**

**DEPARTMENT OF COMPUTER ENGINEERING**

**CMPE-208 Computer network architecture and protocols**



**By**

**Group #01**

**Jeevan Venkataramana (011917477)**

**Pavan Haravu Ramesh (011875318)**

**Roopashree Munegowda (012235834)**

**Sai** **Sri Vaishnavi Chittoori (012415130)**

**Submitted to**

**Prof. Shai Silberman**

**Department of computer Engineering**

**SAN JOSE STATE UNIVERSITY**

**Objectives**

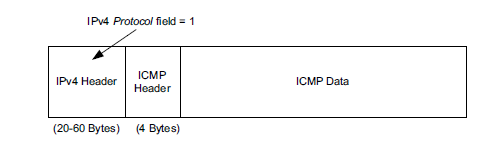
* To understand the operation and implementation of the ICMP protocol
* To understand how the network component, get the configuration in the network
* To study the different type of the ICMP messages used for error reporting and the detecting the correct configuration or the routing path required to transmit the data.

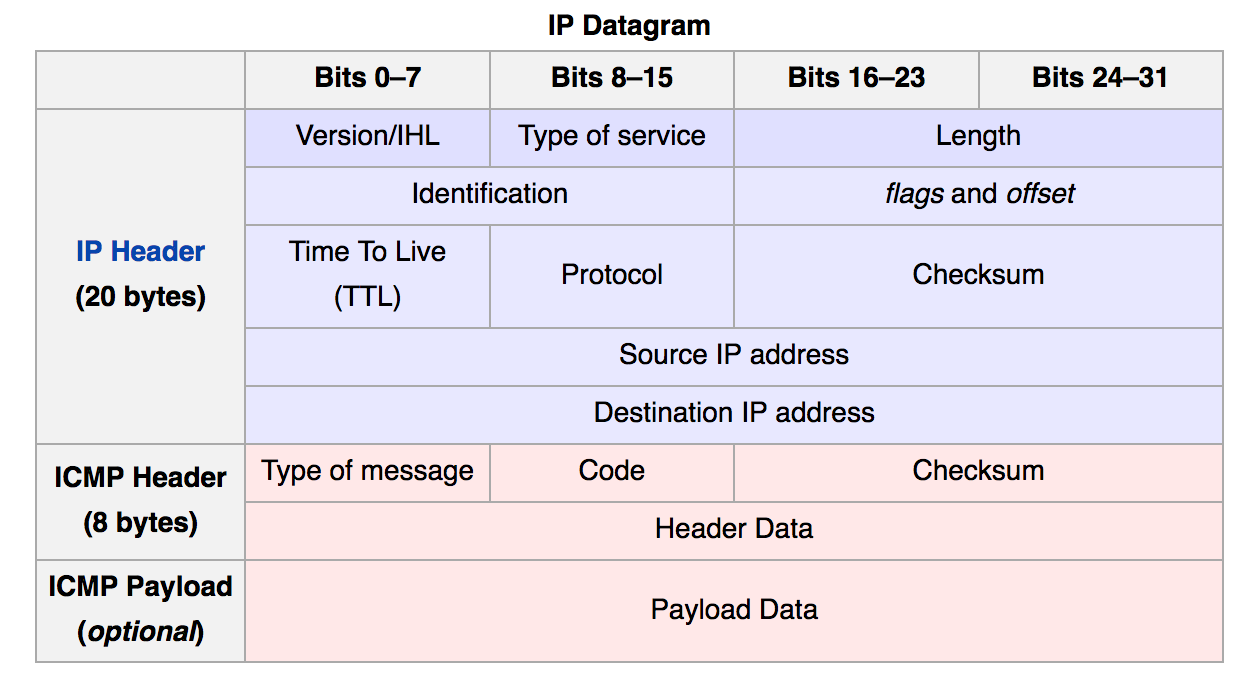
**Introduction**

ICMP stands for internet control message protocol. It is basically an error reporting protocol and is used for delivery of error messages across the network. It is a part of IP protocol suite and is used for diagnostic or control purposes generated in response to errors which occur during IP operation across the network. The error messages will be directed to the sender to inform about the error. This is basically done by sending the header of the IP packet with the payload which failed to reach its destination. It is also used to troubleshoot the network by using commands such as ping and traceroute. Ping is used to test the reachability of a host on the network and also gives us the round-trip time for a particular destination, traceroute on the other hand helps in identifying the route path and transit delays across the network. ICMP messages are sent in situations where a destination host is unreachable or there is a better path to forward the traffic for a destination. There is no assurance that a datagram or a control message will be delivered, some datagrams may be undelivered without the report of their loss. For the IPV6, a version of ICMP called ICMV6 will be used.

**ICMP Packet Format**

ICMP packet is encapsulated in IP datagram. The description of various fields of ICMP packet is are described as below.



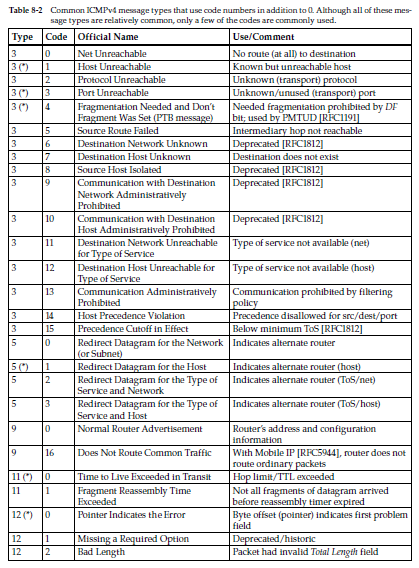


ICMP header is totally of 8 bytes. The4 bytes of the ICMP message defines the Type of the ICMP message, and the code of the specific ICMP message being used and 2 bytes of checksum. The detail description of the ICMP messages fields are defined below.

Type of message: Type of message defines the which type of the ICMP message is being transmitted. There are many ICMP message types and the most commonly used message types are defined below.

Code: Code field will be used to define the subtype of the ICMP messages. The details of the codes for a ICMP message type is given below.

Checksum: It is generally used for the error checking of the ICMP datagram and is calculated from ICMP header and data. This should be cleared to zero before generating the checksum.



Header Data: It includes the first eight bytes of the data from the ipv4 packet that caused the error in addition to the copy of entire ipv4 header.

Payload Data: It contains the data specific to the message type indicated by the type and code fields. This field has been exploited for various attack purposes such as ping of death, large or fragmented packets for DOS attacks.

**ICMP Messages**

There are 2 types of ICMP messages, error messages or query/information messages. The error messages will be used to inform the sender what went wrong about the IP datagram that it sent and the query or the information messages will be used to get the network components used to transmit the data or to get the diagnostic information of the network components.

**ICMP Error messages**

The distinction between the ICMP error message class and the ICMP information message class should be clearly defined since the restrictions that are imposed on the ICMP error messages will not be applicable to the ICMP information messages. The ICMP error message generated will consists of the offended IPV4 datagram and the payload the specific IP datagram.

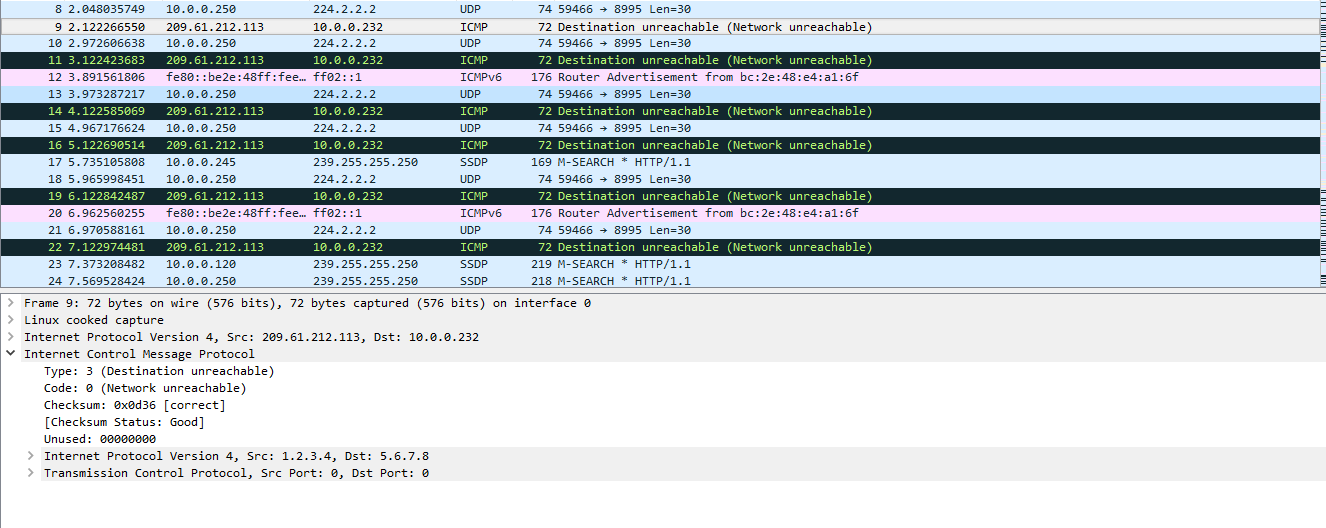
Some restrictions imposed on the generation of the ICMP error messages are like generating ICMP error message for another received ICMP error message, an ICMP error message for a datagram destined for multicast or broadcast address, an ICMP error message for an link layer broadcast address, generation of ICMP error messages for only the first fragment of the data etc.

The sender is restricted to generate only to generate specific number of ICMP messages by defining the bucket. The bucket will be refilled with the token periodically to send the ICMP messages in future. This is used to restrict the sender in generating the unnecessary traffic in the network.

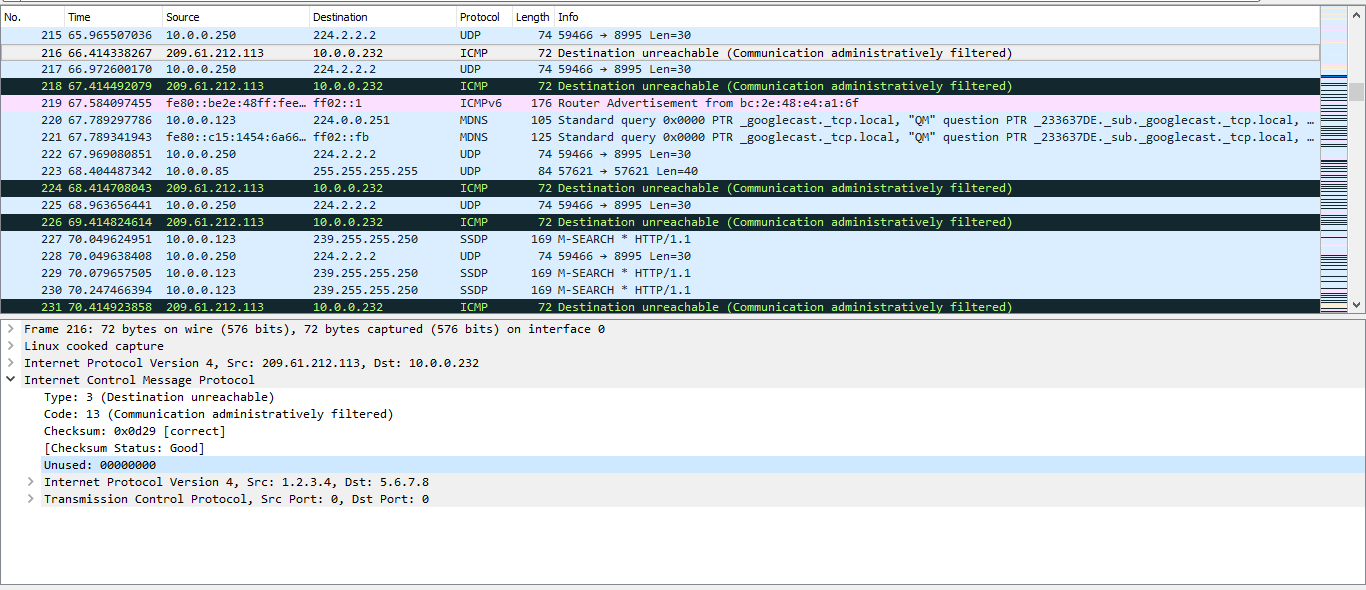
Error Message type – Destination Unreachable (Type 3)

This will error message will be used for indicating the sender that the sent datagram could not be delivered to the destination for a specific reason. The reason will be defined in terms of the code mentioned in the ICMP Destination Unreachable message. There are around 16 codes defined for the ICMP message type and the few are implemented below.

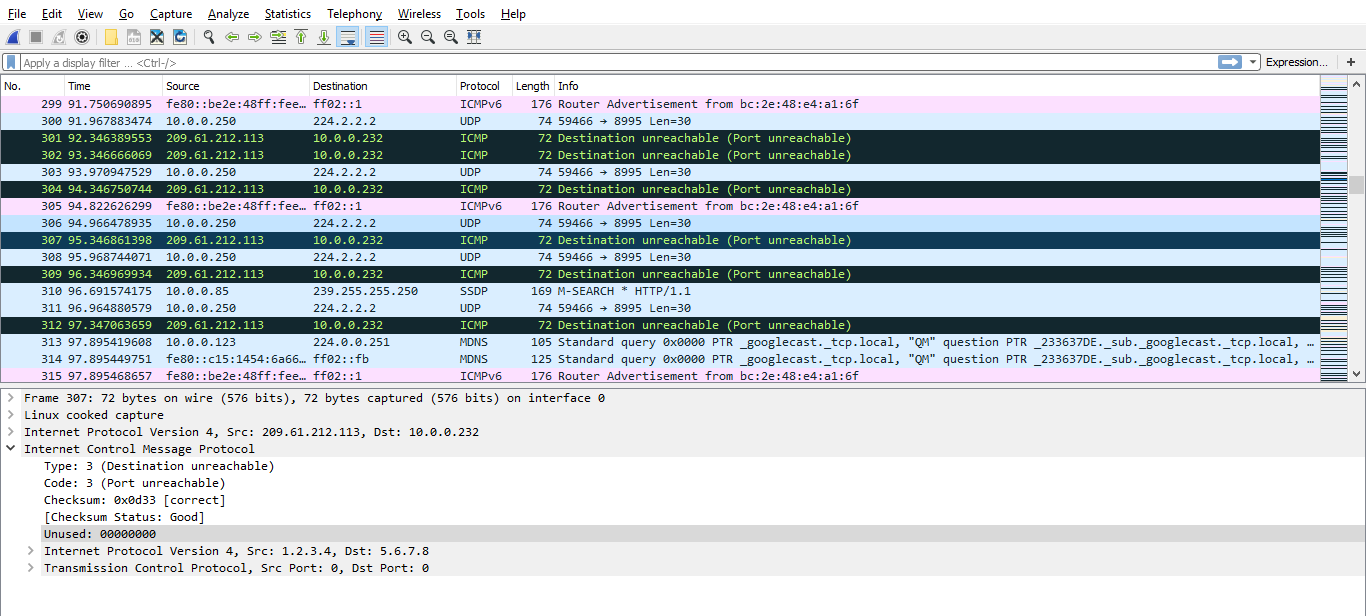
Host Unreachable (Code 1) - This type of error message will be generated when the host try to send the information to another host but for some reason the host is not reachable or the host does not exist in the network.



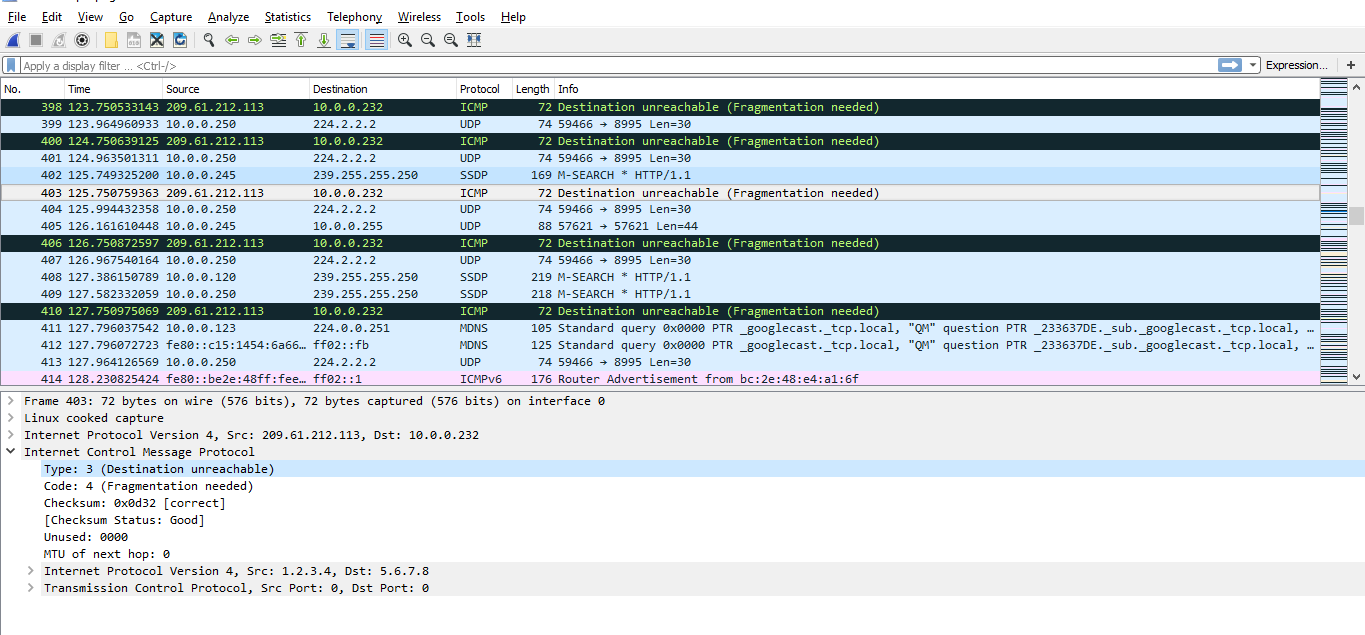
Communication Administratively Filtered (Code 13) – This type of the error message will be generated when the host trying to establish communication with a destination host but the firewall at the destination drops the packet if it fails to comply with the operation policy enforced. It is possible for the destination host to configure the firewall in such a way that it does not require to send these ICMP messages to the sender if the traffic sent by the sender does not comply with the operation policies.



Port Unreachable (Code 3) – This ICMP error message will be generated when the packet sent by the user destined for a specific port number at the destination side is not active. This occurs mostly in conjunction with UDP since there will be no connection establishment between the hosts before exchanging the information between them.

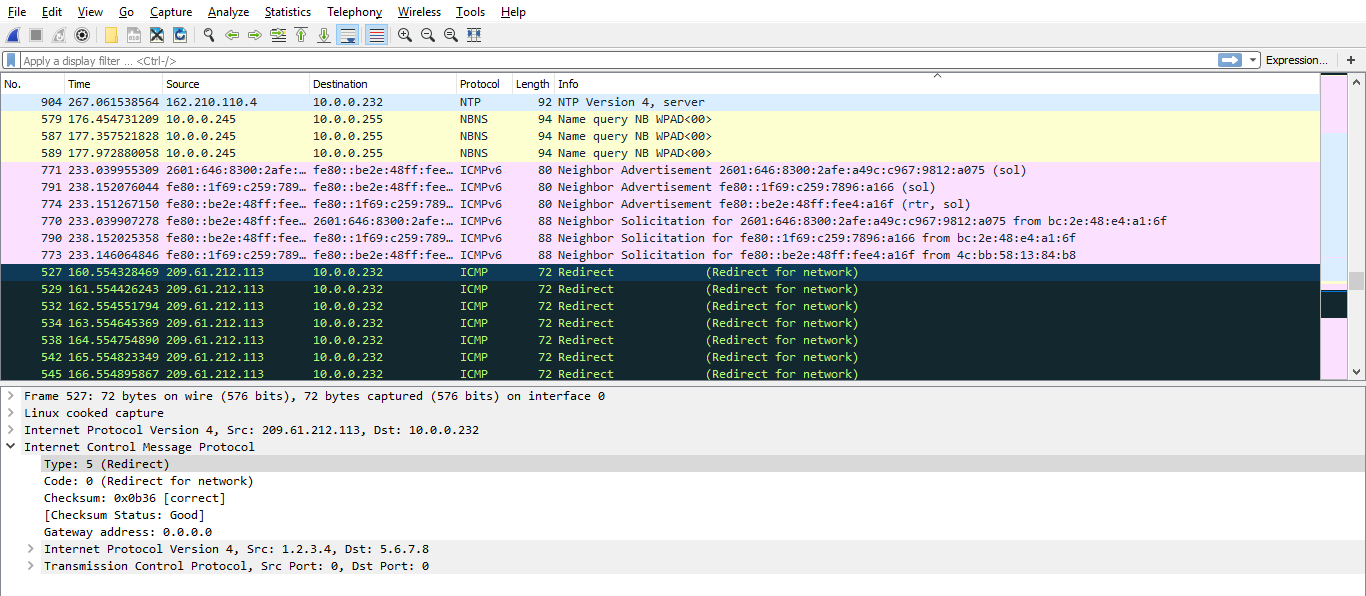


Fragmentation Needed (Code 4) – This type of the ICMP message will be generated when the fragmentation of the datagram sent by the sender requires the fragmentation at the router side to send to the next network component in the topology. This ICMP error message will be used for determining the MTU between the hosts in the network. This process is called as the MTU discovery.



ICMP Redirect Message Type (Type 5)

This type of ICMP message will be generated when data sent by the host is reached to the wrong router or when the router finds that there is more efficient path the datagram to reach the destination. At that time the router sends this type of error message and forwards the packet to the next hop. On getting this ICMP message, the host updates its routing table and sends the other datagram that it wants to send according to the updated routing table entry. This message type helps the attacker to masquerade as an router and make the host to send the information to it.

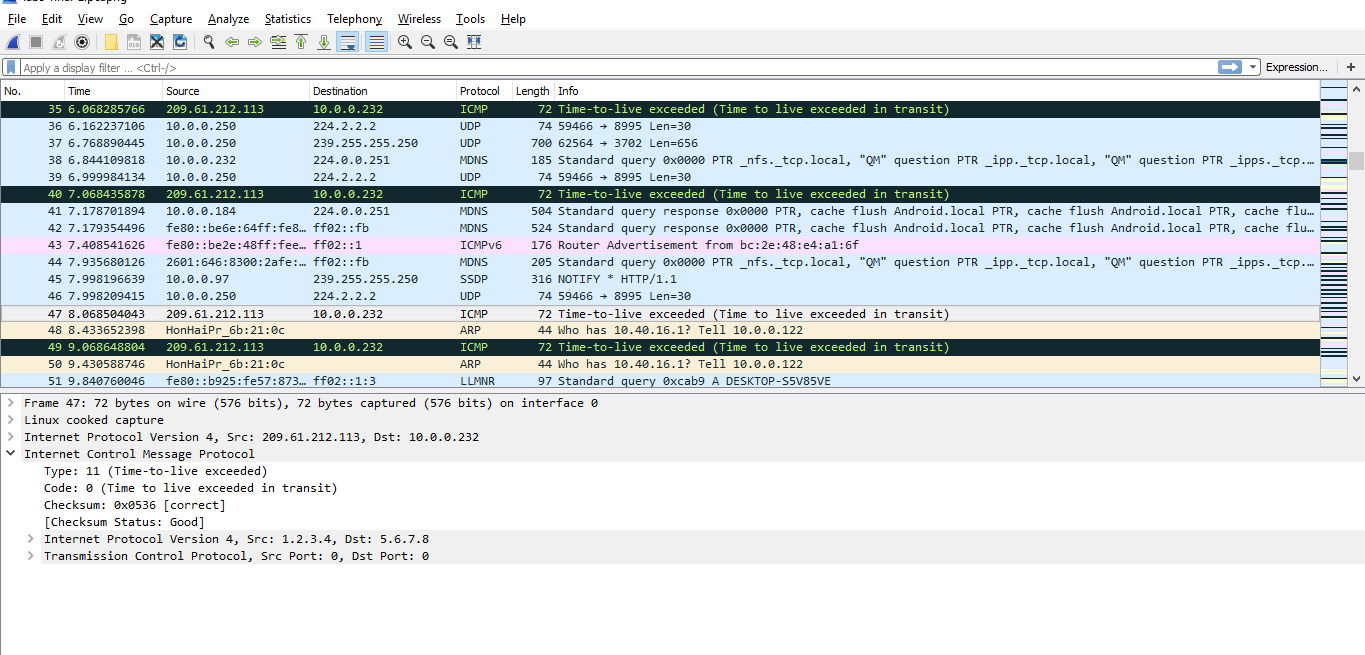


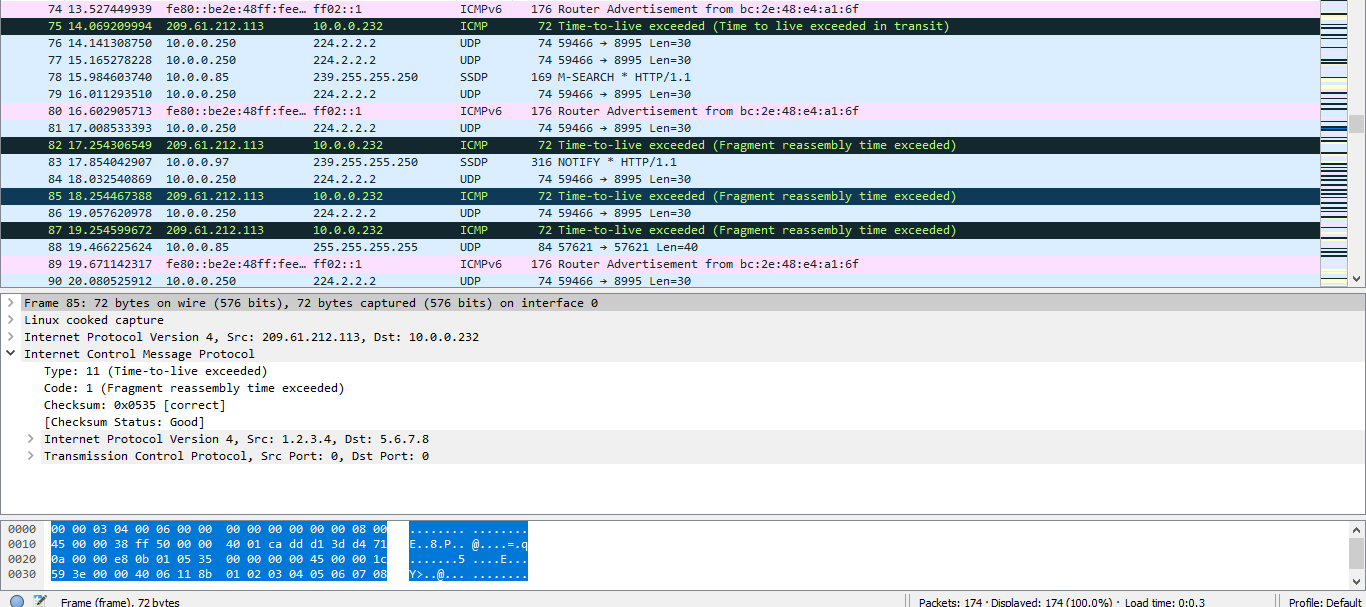
Note in the above packet details that the code of the Redirect Message Type is 0.

ICMP Time Exceeded Message type

Time to live exceeded in transit (Code 0) - When a host sends a packet, a field called TTL (Time Limit filed in IPv4) will be updated. This field defines for how many hops the sent datagram be existed in the network. When the datagram reaches to a router, then the TTL value will be decremented by 1 and sends to next router. When the router founds that the TTL field of the sent datagram is 1 then it decrements the TTL value and sends the ICMP message of Time Exceeded to the host. The next router drops the packet.

Fragment Reassembly Time Exceeded (Code 1) - This type of ICMP error message will be generated by the destination host when all the fragments related to the data send by the user has not reached in specific amount of time to destination





**Query/ Information Message**

ICMP Information messages will be used to get the configuration and the information related to the network components and the hosts. There are 3 types of the ICMP information messages.

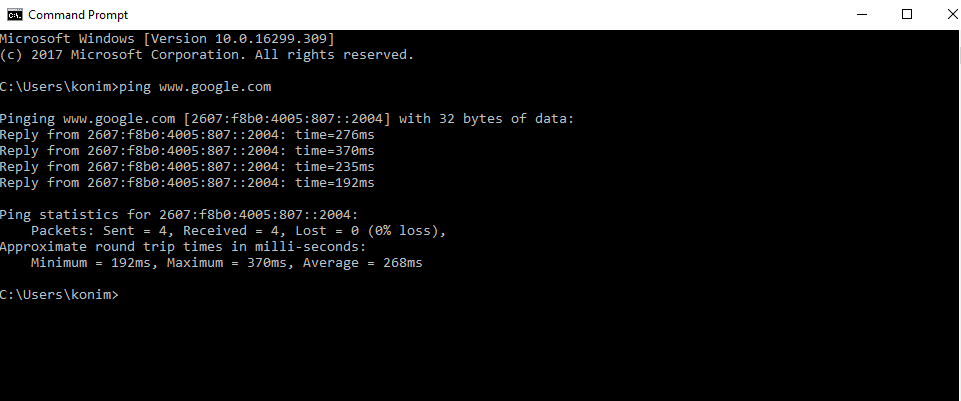
* Address Mask Request/Reply (Type 17/18)
* Time stamp Request/Reply (Type 13/14)
* Information Request/Reply (Type 15/16)

The first 2 types of the information ICMP message types are replaced with the more secured protocol called DHCP. The only used information ICMP messages are Information Request/ Reply type. It includes Echo request/reply, Router solicitation and the Router advertisement.

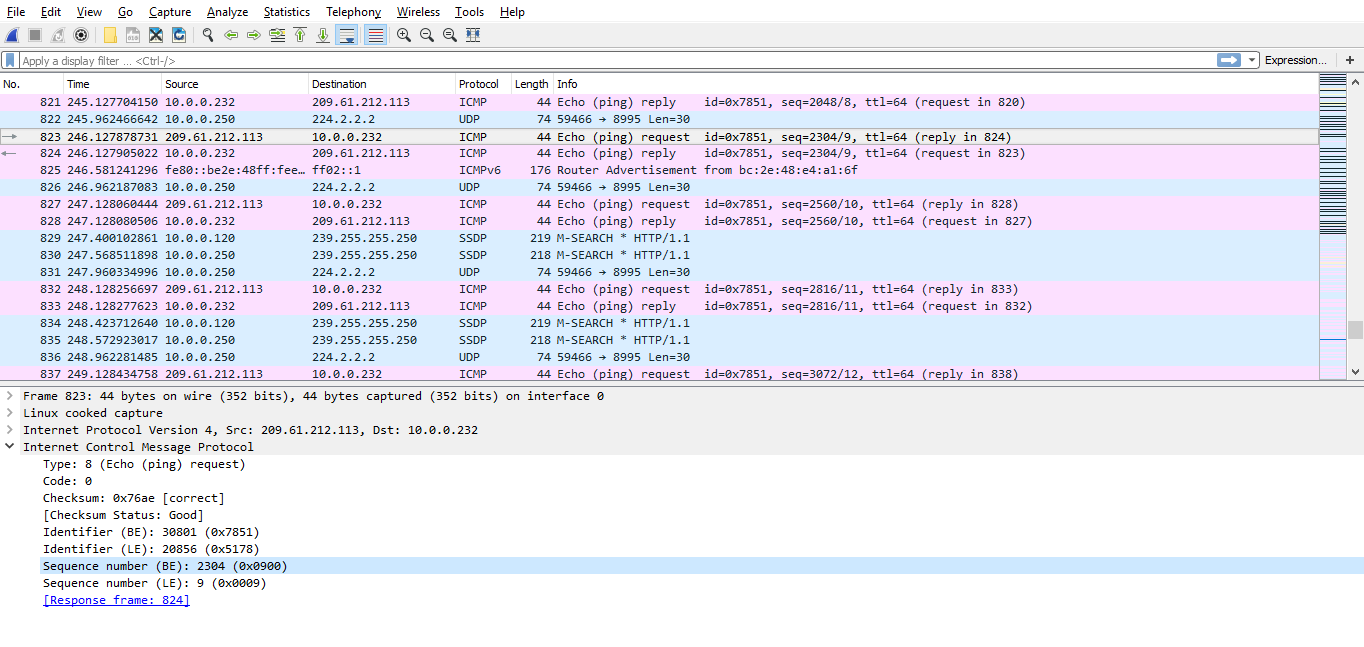
Echo Request (Type 8) and Echo reply (Type 0)

Echo Request and Echo Reply ICMP messages will be used to check whether a host is reachable or not. It is always not true that if the ICMP echo reply for a host is generated for an Echo Reply since some of the host configured with the firewall might not reply to the echo requests and also some of the echo request messages might not be transferred to the host present far if the TTL is set to the low value.

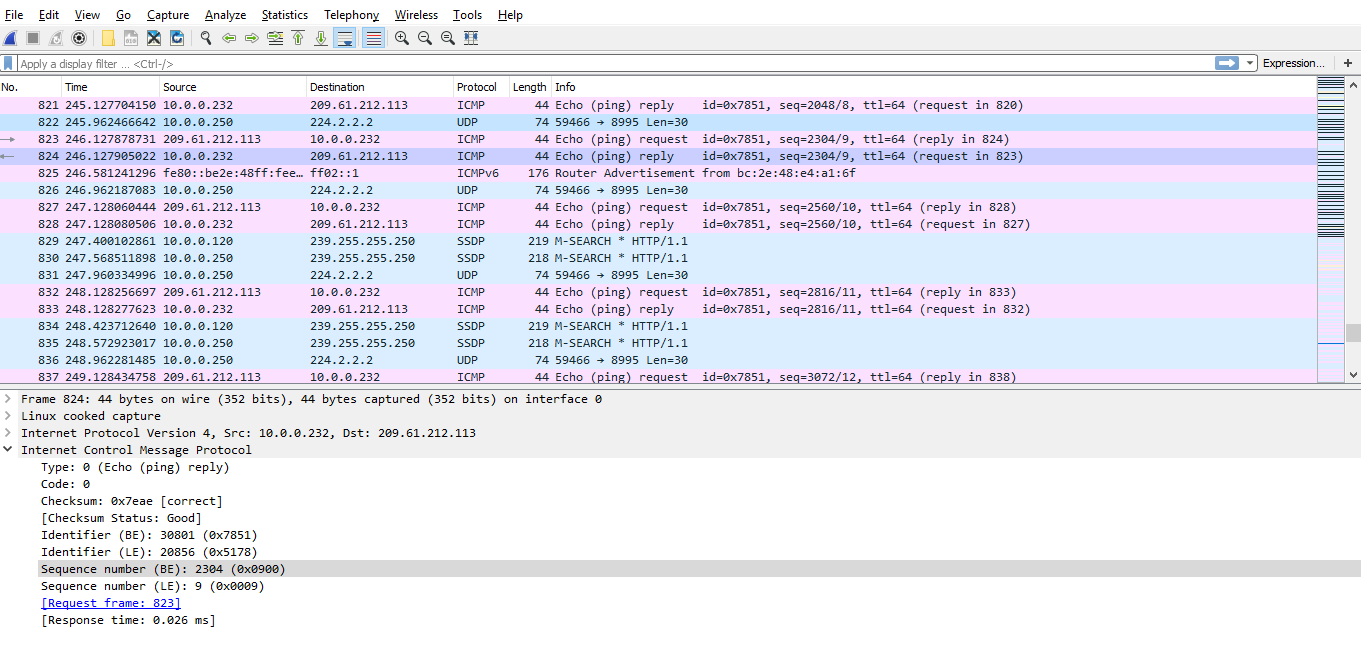
When a host sends ICMP request message, the message contains the sequence number and the time stamp. When that echo request reaches to the destination, the destination hosts replies with the Echo Reply message with the sequence number of the echo request message and the time stamp at which the request message is received. This helps the user to check what time it takes to send the packet to the destination and to receive the response. This is used to calculate the RTT (Round Trip Time) measurement.



Echo Request (Type 8)



Echo Reply (Type 0)

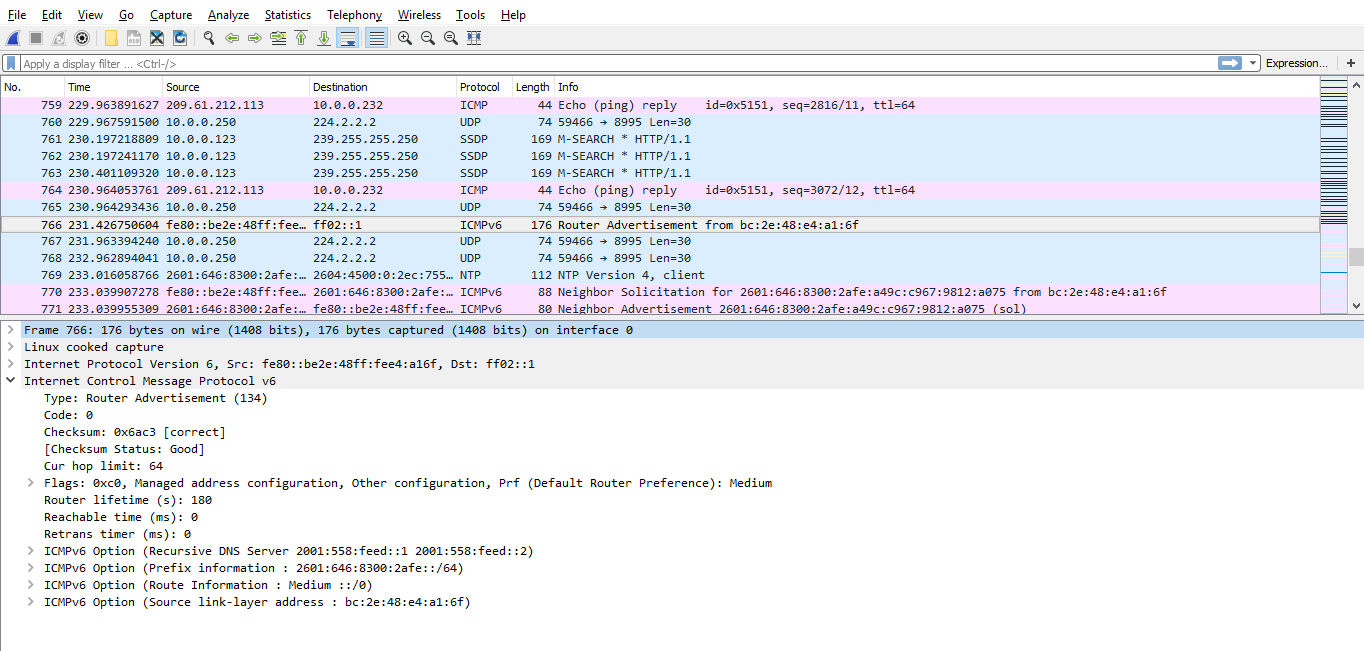


Router Advertisement and solicitation

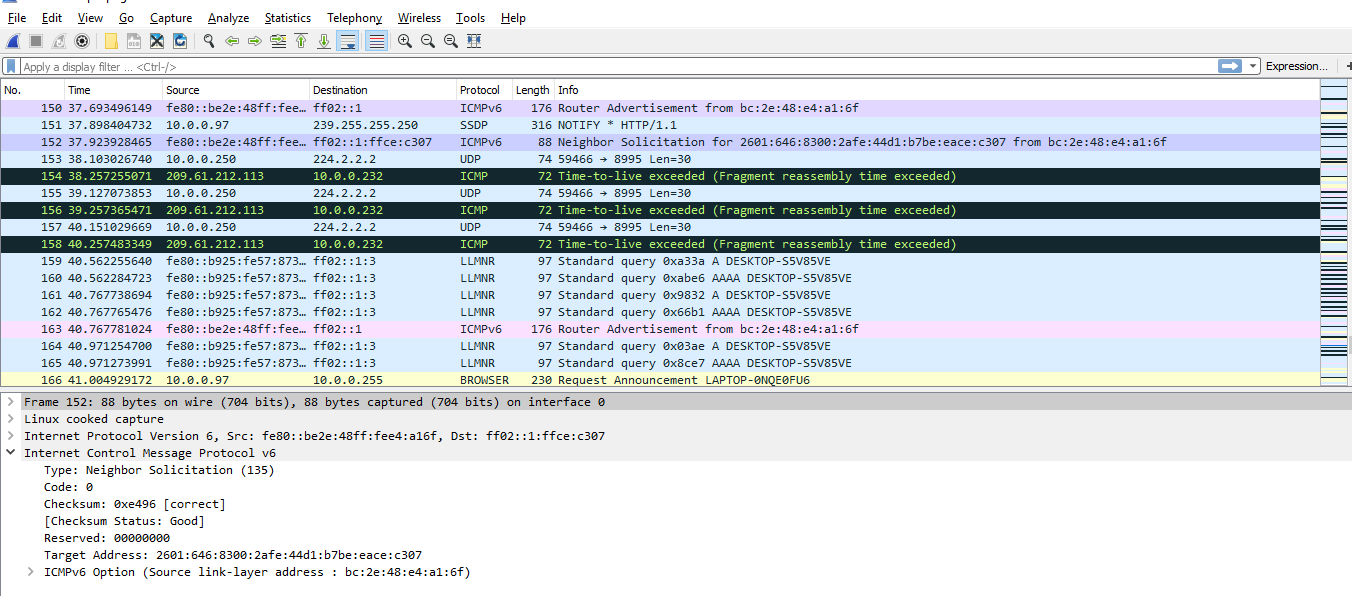
The ICMP router discovery messages are called "Router Advertisements" and "Router Solicitations". Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses

of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if (and only if) no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

Router Advertisement



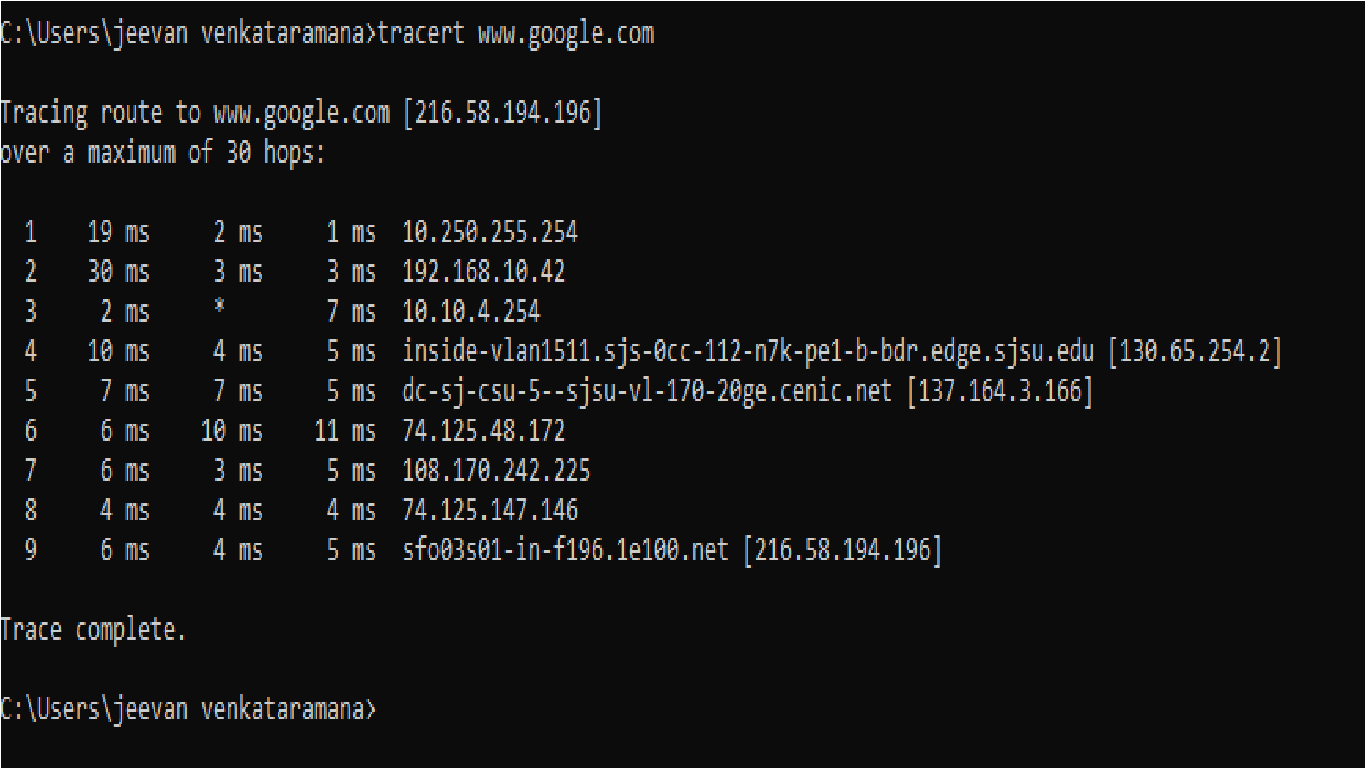
Router Solicitation Or Neighbor solicitation



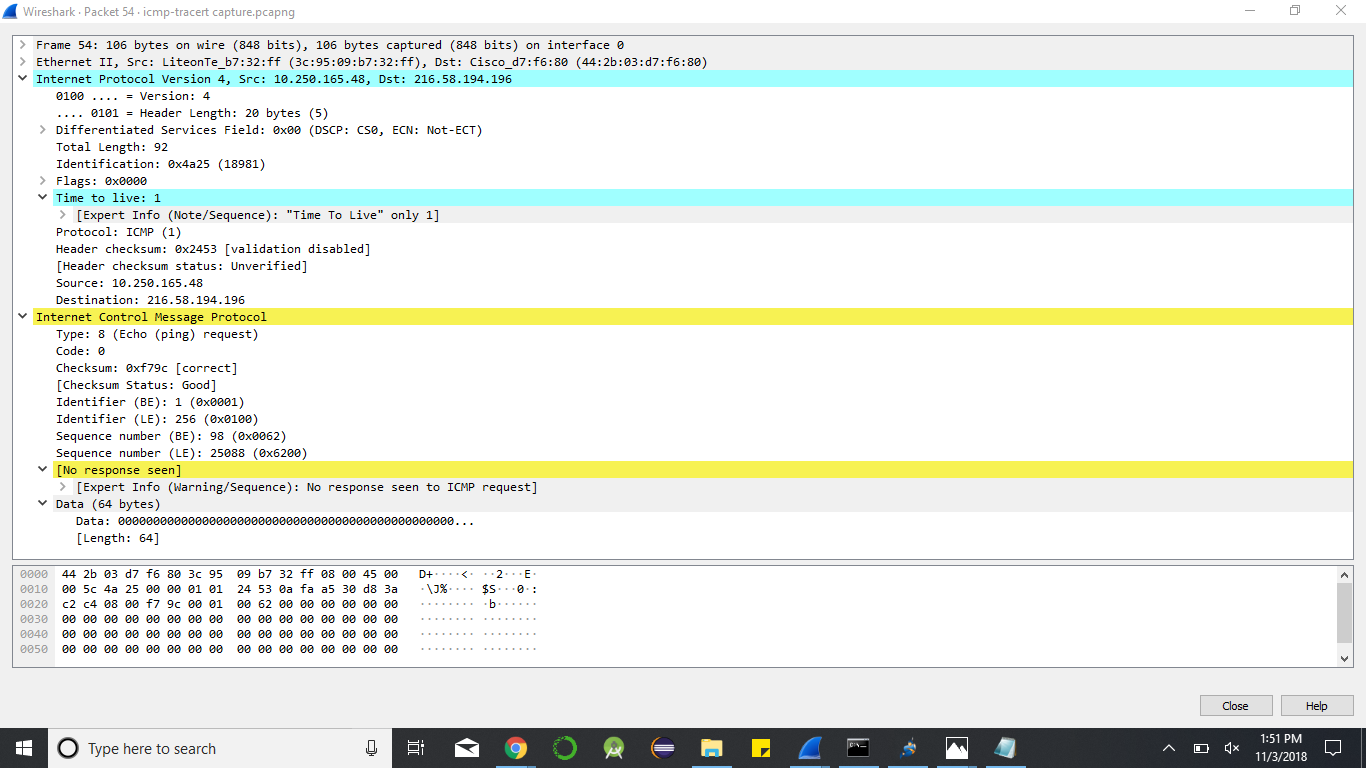
Traceroute Command

To determine the path taken by packets to reach the destination. For a normal ICMP message the hop count is by default set to 30. The hop count decrements on the packet as it passes a router. In the case of traceroute command the time to live is set to 1. This is an indication for the router to respond to the ICMP packet. This message lets the source know the packet traverses that particular router as a hop.

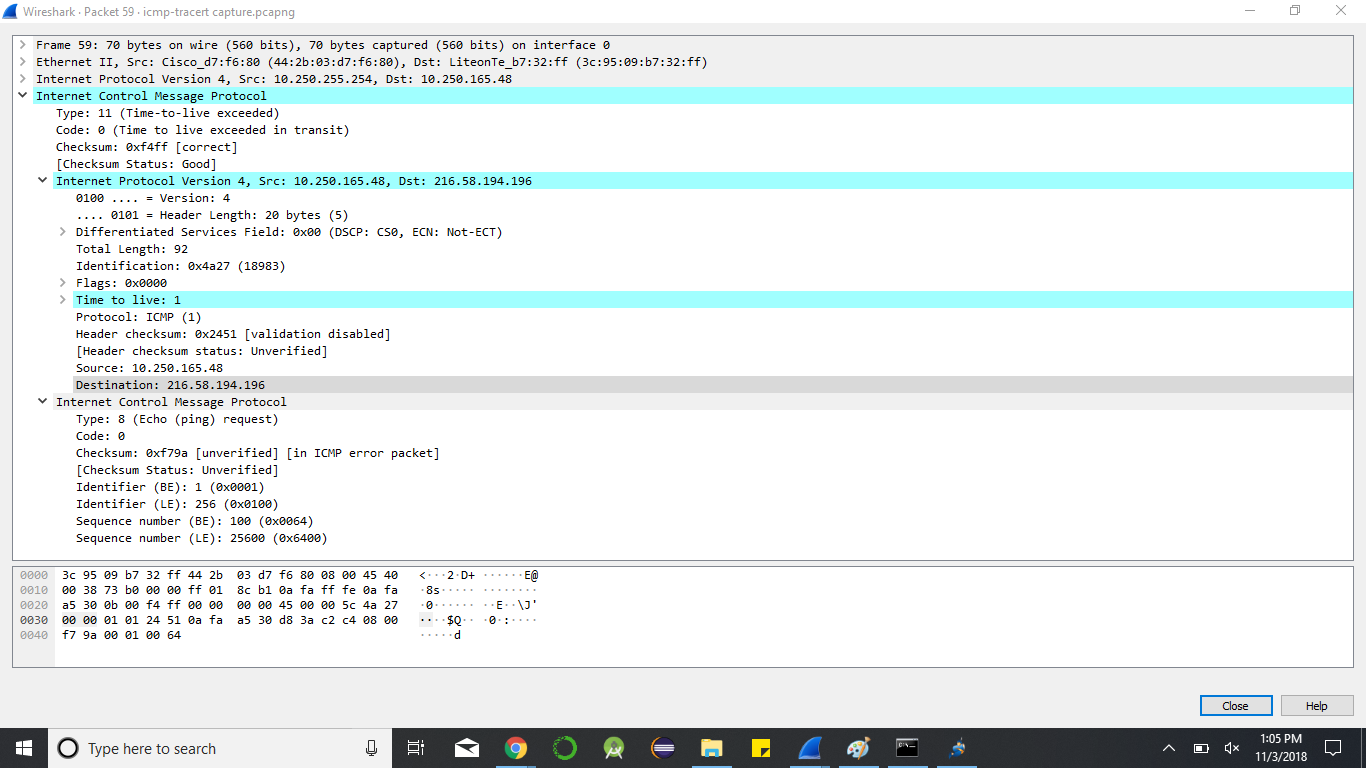
We have analyzed by pinging [www.google.com](http://www.google.com) through our host machine. The following were the observations. The IP address of our host machine is 10.250.165.48



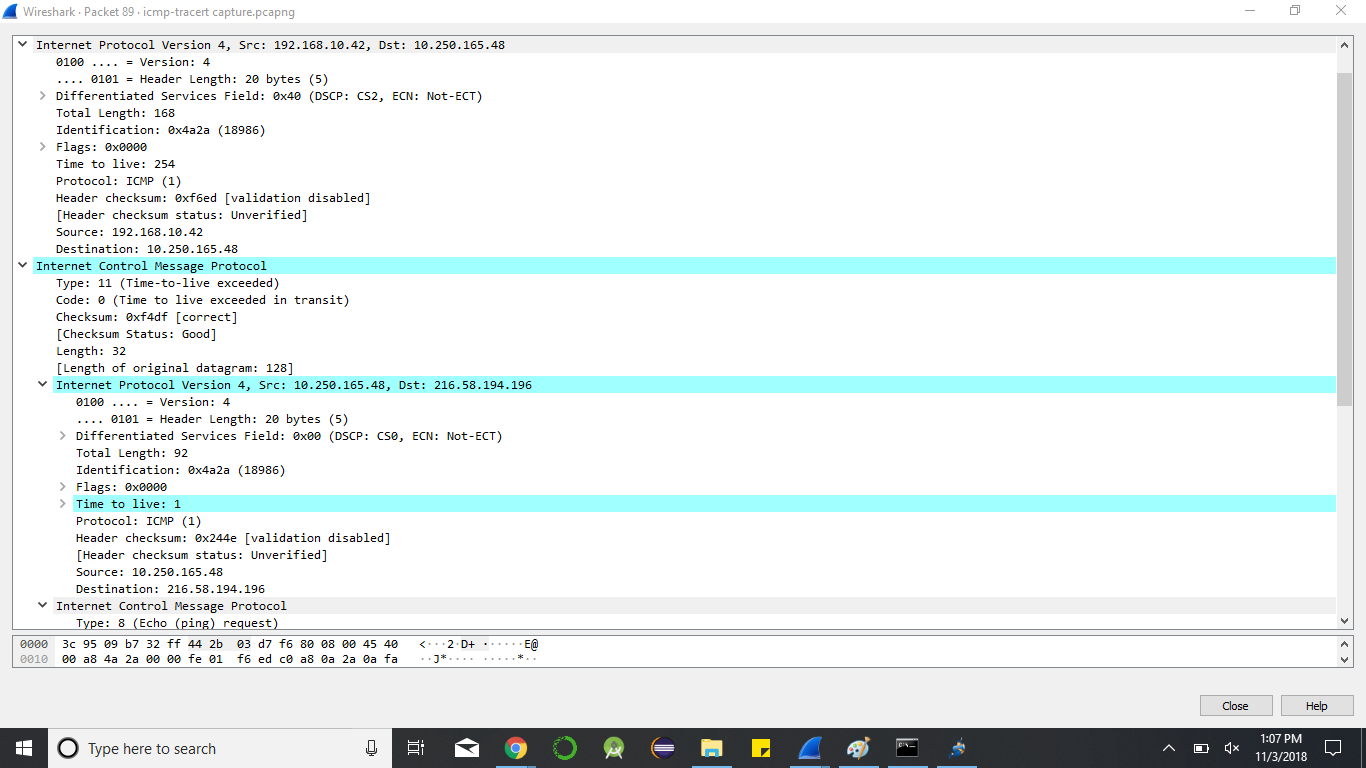
The above results show the path taken by packets to reach the datacenter of Google which is located at San Francisco



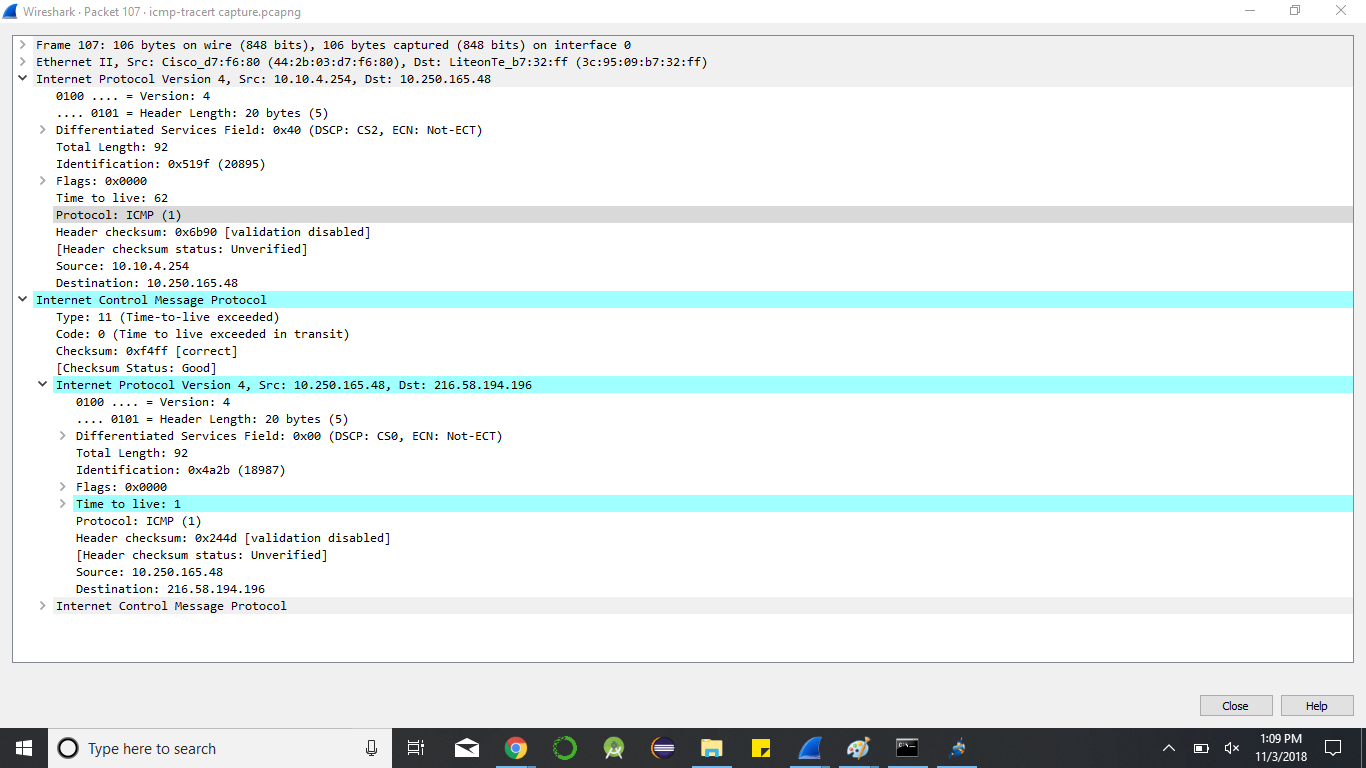
The above capture is the ping request from host machine to Google. The Time to live is set 1. The IP address in the destination field is set to 216.58.194.196 which is the IP address of Google. This address was recognized since the host machine already had an entry for the DNS name in its cache.

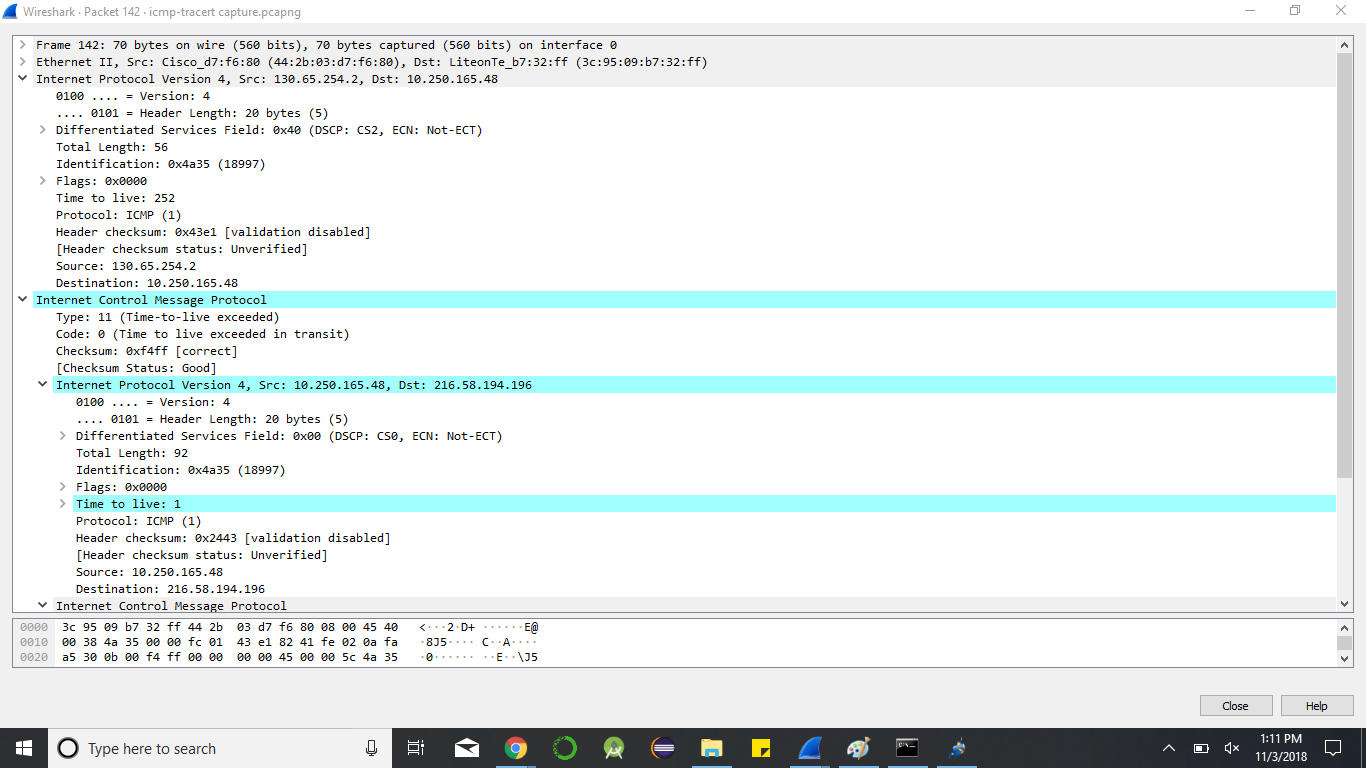


The above capture is a reply from the default gateway. Since the IP address specified in the destination field is out of the private network. The router having the interface to the public network will respond. The response contains the router IP address which helps the host machine to determine the first hop of the packet on its way to the destination. The type field is set to 11 by replying router to indicate the time to live has exceeded. Since the request had 1 in its ttl field.

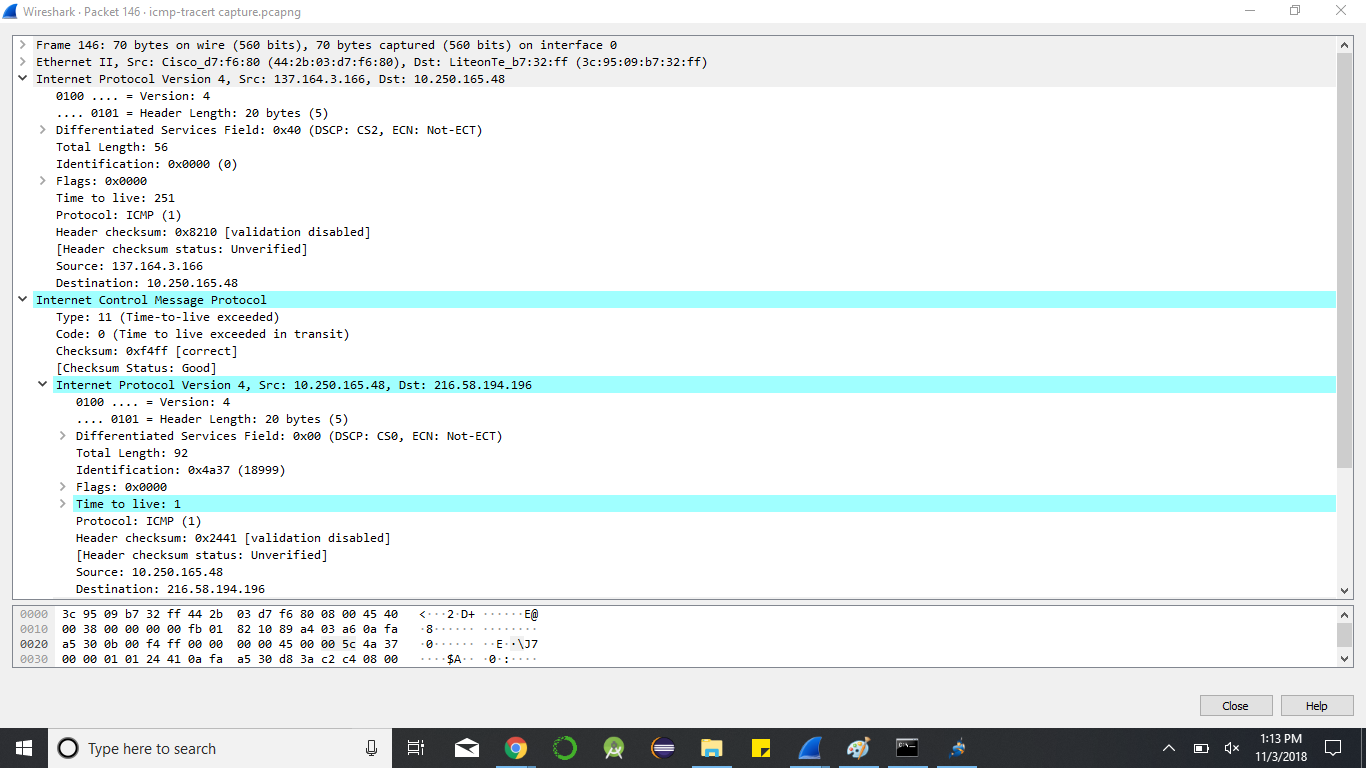


The above capture is a reply from the next hop router on the path to the destination. The ICMP message protocol contains IP address of the host and the IP address of the destination it is trying to reach. Every reply contains this information by default. The host recognizes the replying router’s IP address from the address specified in the network layer.

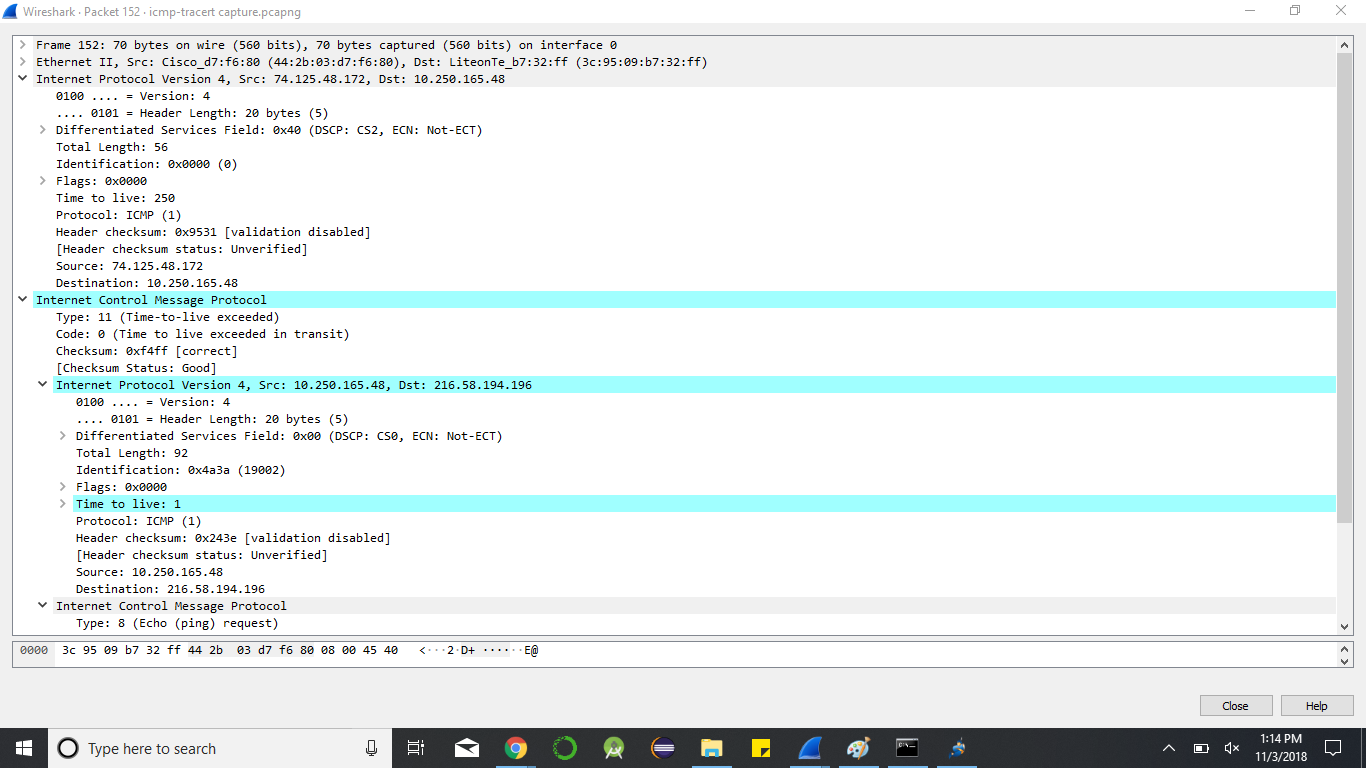


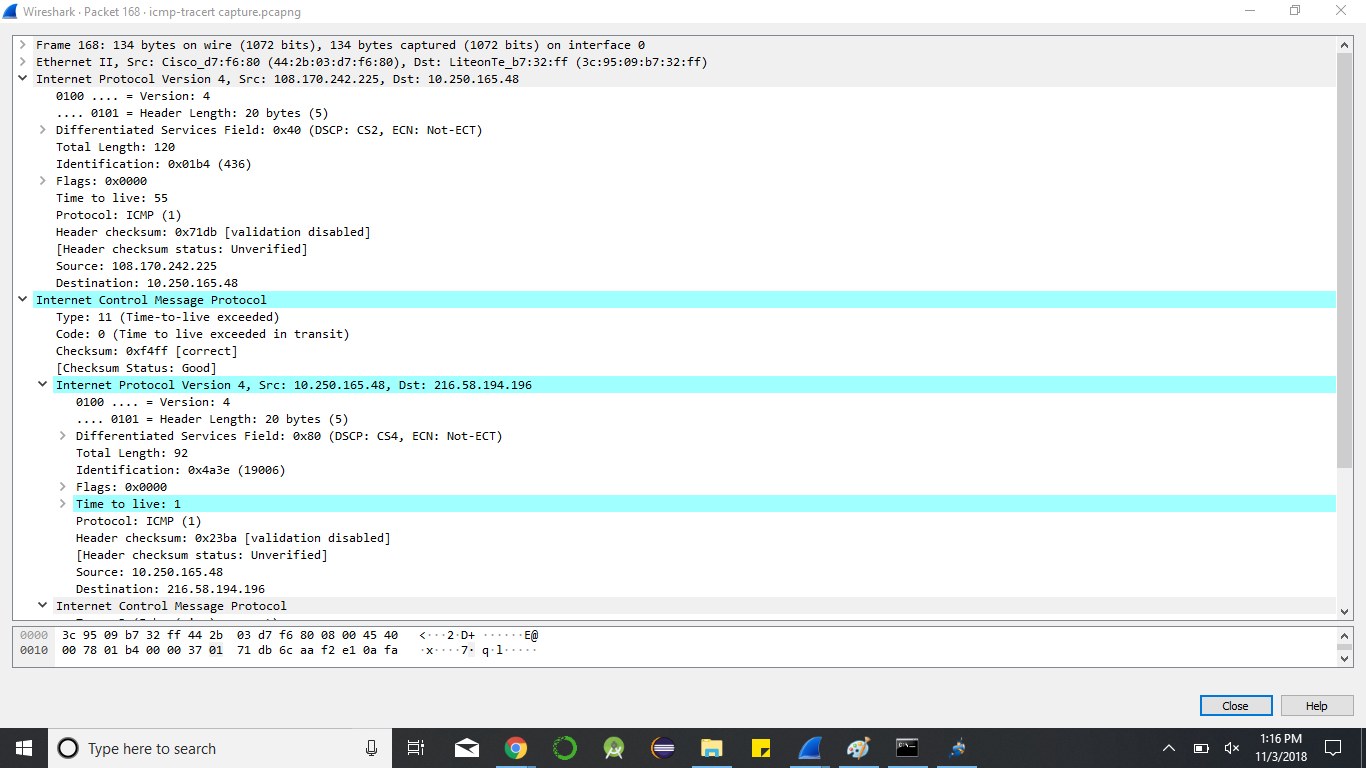


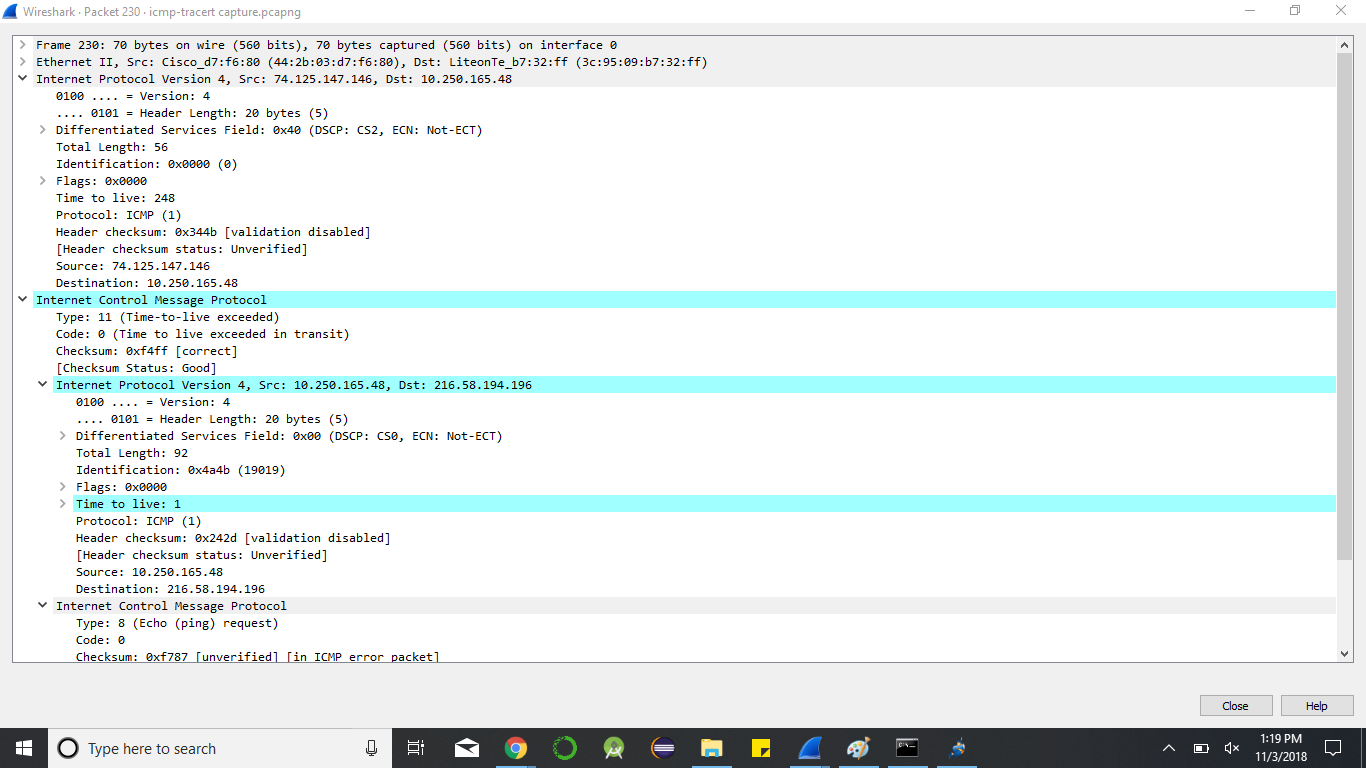
The above capture is the gateway IP address leaving the university network. The next address would be the ISP IP address

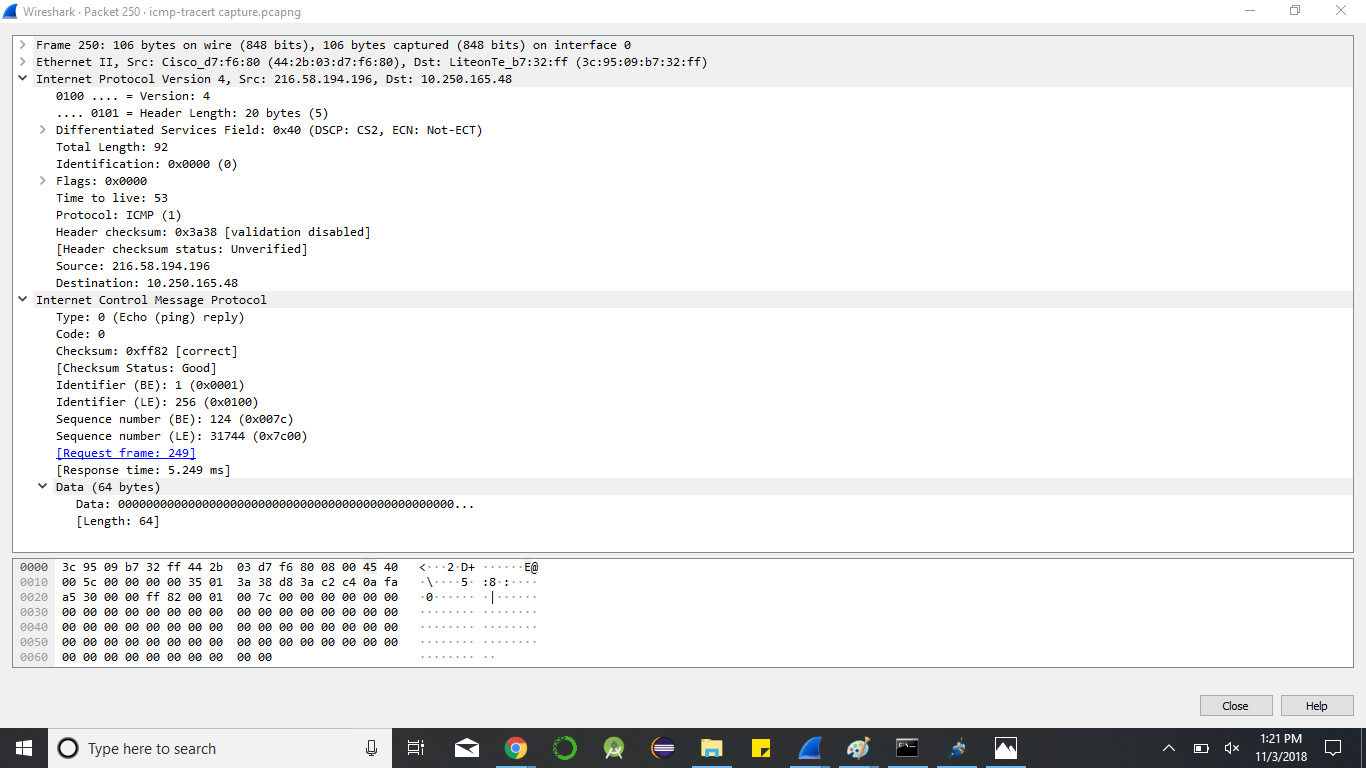


The following three captures are the reply from the root server, TLD server and name server.









The above capture is the reply from the destination.

**ICMP Tunnel**

ICMP tunnel uses a mechanism to send arbitrary data inside an ICMP echo packet. The source sends the data inside an ICMP request packet which the receiver replies by sending its data in the reply packet. Thus, all the communication takes place using the ICMP request/reply packets. This is basically used to bypass the firewall rules and can be used as a means of encrypted communication between the users. The network administrators can only identify such activities by using network log and extensive analysis of the packets.

**Attacks involving ICMP**

The different types of attacks involving ICMP are:

Floods: A large amount of traffic is induced for denial of service attacks on one or more systems. Bombs: A specifically designed message to make the IP or ICMP processing collapse or dangle.

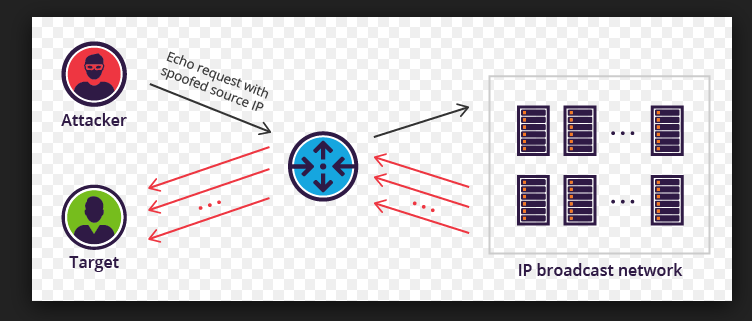
Information disclosure attacks: These attacks are not detrimental by themselves but are used with other attacks to get undetected.

Ping of death attack: ICMP request/reply packets are framed in an order that when they are reassembled the packet size exceeds the ipv4 maximum packet size i.e. 64KB, thus used as a form of dos attack.

Teardrop Attack: The value in the fragment offset field of an ipv4 header is changed to make an intuition about errors in the ipv4 fragment reassembly routes.

ICMP redirect attacks: The ICMP redirect capability may be used to redirect packets to a scrupulous system which can tamper the packet and would result in man-in-the-middle attack.

The Smurf Attack: It is a type of distributed denial-of-service attack in which a numerous amount of ICMP packets are broadcast across the network with the victim’s spoofed source IP address, the reply of which is sent by most of the systems available across the network, suppose the network has large number of users then this large number of replies will flood the victim’s system which may lead to crashing of the host system. To prevent this the router could be configured with no IP directed-broadcast on the interface configuration mode.



**Conclusion**

The Internet Control Message Passing protocol is used as the error reporting and information conveying protocol for IP. We have discussed the different message types of ICMP and their operations and gone through the packets of each type in wireshark. We concluded this the attacks that can be done using the ICMP protocol and discussed why the ICMP message packets will be dropped at some servers or host because of the firewall configuration.

**Reference:**

TCP Illustrated Volume 1, Second edition, The Protocols by Kevin R. Fall and W. Richard Steven.

<https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol>

<https://searchnetworking.techtarget.com/definition/ICMP>

<http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/icmp.html>

<http://www.networksorcery.com/enp/protocol/icmp/msg10.htm>

<https://www.google.com/search?biw=1366&bih=613&tbm=isch&sa=1&ei=vL7KWsCkKc7atQWnwJqQAQ&q=smurf+attack&oq=Smurf+&gs_l=psy-ab.3.0.0i67k1j0l9.10477.12852.0.13800.7.6.0.1.1.0.105.452.4j1.6.0....0...1c.1.64.psy-ab..0.6.456.0...71.0_4Wlm8YQi0#imgrc=ePbAcP4306iUGM>: