Wireshark Laboratories

Laboratory #1 (IP)

In this lab, we will examine the content of the IP header. Firstly, we need to prepare the Wireshark to capture packets from the right network interface as follows:

1. Open Wireshark and start capture from the right network interface.
2. Enable the internet connection in your PC.
3. Open your web browser and browsing any websites for a few seconds.
4. Stop the Wireshark.

Secondly, double click on any packet and open the "Internet Protocol version 4" field. ***Figure 1*** shows the content of the IP header.

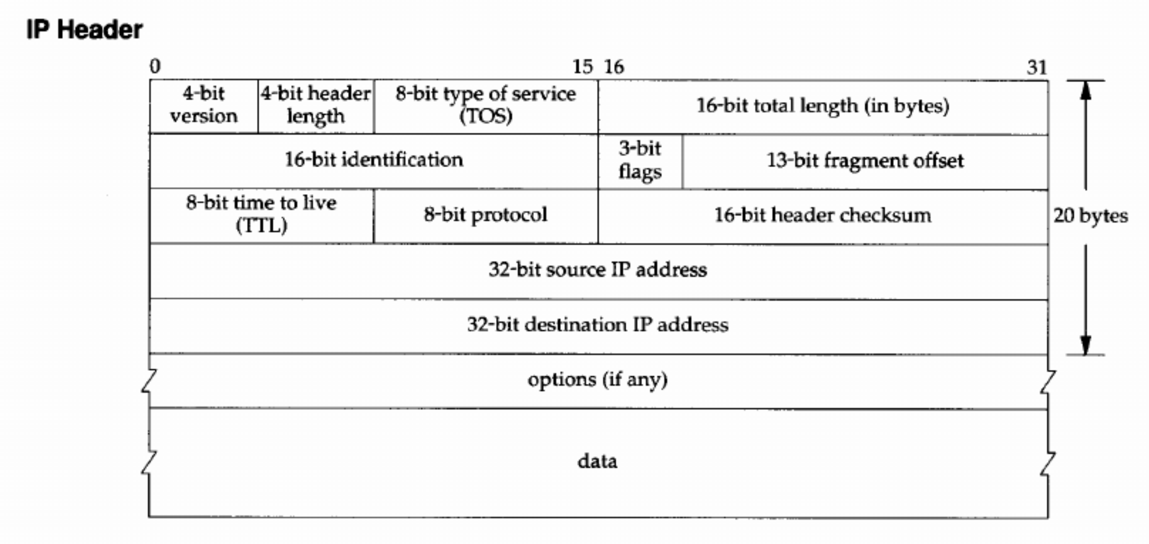


Figure 1: IP Header

Finally, try to answer any question such as the following:

1. What is the IP address of your computer?

2. Within the IP packet header, what is the value in the upper layer protocol field?
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.
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
5. What is the value in the Identification field and the TTL field?

There are many filters that can be used the IP packets such as the following:

- ip.addr = *.*.*.* //display all packets that contain that IP address.
- ip.src = *.*.*.* //display all packets with source IP equal to *.*.*.*
- ip.dst = *.*.*.* //display all packets with destination IP equal to *.*.*.*

Laboratory #2 (UDP and DNS)

In this lab, we will examine the content of both UDP and DNS packets. Firstly, we need to prepare the Wireshark to capture packets from the right network interface as follows:

1. Open Wireshark and start capture from the right network interface.
2. Enable the internet connection in your PC.
3. Open your web browser and browsing any websites for a few seconds.
4. Stop the Wireshark.

Secondly, types "dns" in the filter bar to display all DNS packets. Then, double click on any packet and open the "Domain Name System" field. ***Figure 2*** and ***Figure 3*** show the content of the UDP header and the DNS packet respectively.

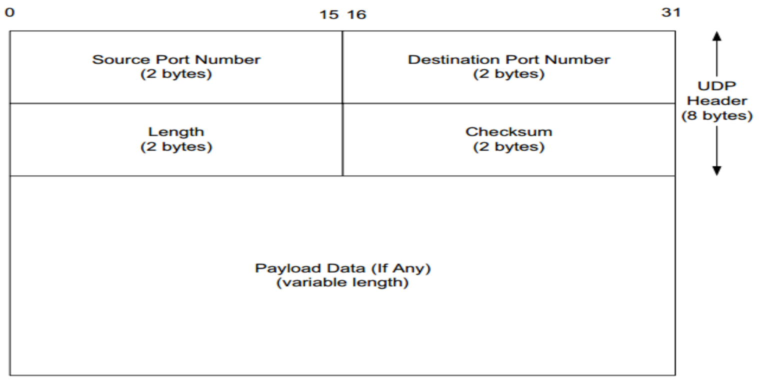


Figure 2: UDP Header

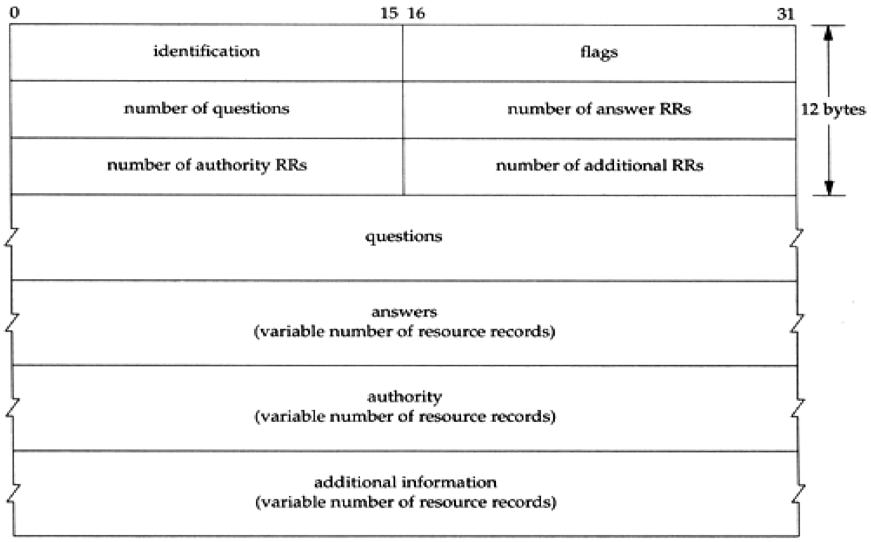


Figure 3: DNS Packet

There are many filters that can be used the IP packets such as the following:

- dns //display all DNS packets.
- udp //display all UDP packets.
- udp.srcport = * //display all UDP packets with source port equal to *.
- udp.dstport = * //display all UDP packets with source port equal to *.
- udp.port = * //display all UDP packets with source or destination port equal to *.
- udp.length = * //display all UDP packets with length equal to *.

Finally, try to answer any question such as the following:

1. how many fields there are in the UDP header?
2. From the packet content field, determine the length (in bytes) of each of the UDP header fields.
3. The value in the Length field is the length of what?
4. What is the maximum number of bytes that can be included in a UDP payload.
5. What is the source port number?
6. What is the destination port number?
7. What is the largest possible source port number?
8. What is the protocol number for UDP?
9. The DNS query and response messages. Are then sent over UDP or TCP?
10. What is the source port for the DNS query message? What is the destination port of DNS response message?
11. From and To what IP addresses are the DNS query message sent?
12. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
13. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
14. What is the IP address of the DNS server?

Laboratory #3 (DHCP)

In this lab, we will examine the content of the DHCP packets. Firstly, we need to prepare the Wireshark to capture packets from the right network interface as follows:

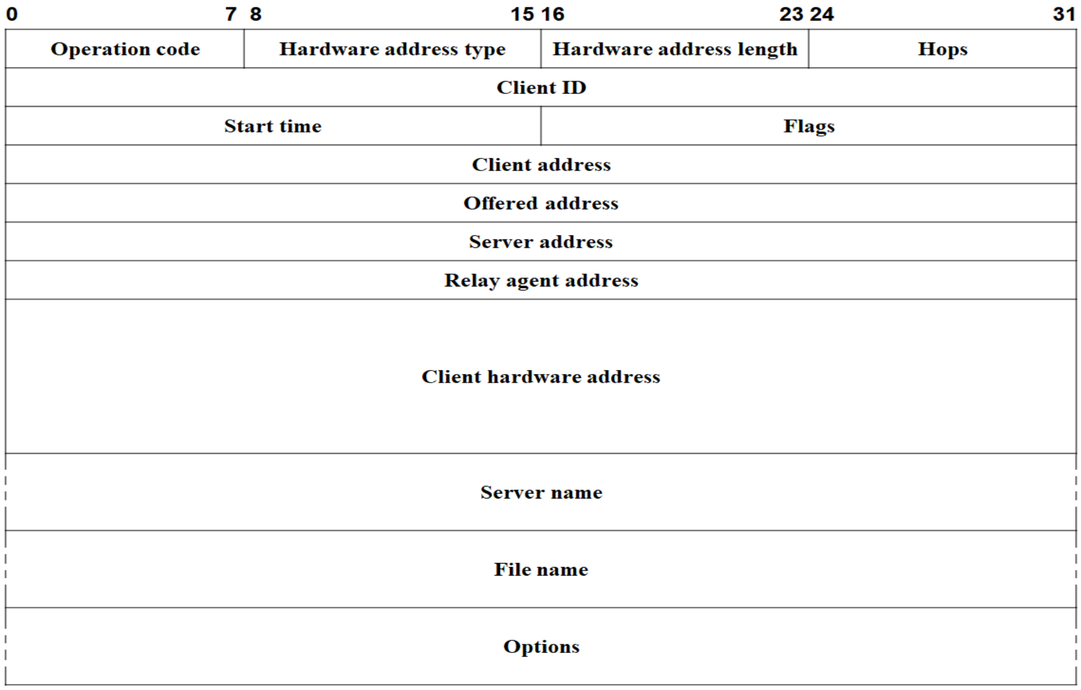
1. Open Wireshark and start capture from the right network interface.
2. Enable the internet connection in your PC.
3. Open your web browser and browsing any websites for a few seconds.

4. Stop the Wireshark.

Secondly, types “dhcp” in the filter bar to display all DHCP packets. Then, double click on any packet and open the “Dynamic Host Configuration Protocol”. ***Figure 4*** shows the content of the DHCP packet.

Finally, try to answer any question such as the following:

1. What is Message type?
2. Are DHCP messages sent over UDP or TCP?
3. What is the link-layer (physical) address of your host?
4. What is the source port address?
5. What is the destination port address?
6. What are the source IP and destination IP addresses in the DHCP Discover message?
7. What are the source IP and destination IP addresses in the DHCP Offer message?
8. What is the content of the client IP address in the DHCP Offer message?
9. What are the source IP and destination IP addresses in the DHCP Request message?
10. What are the source IP and destination IP addresses in the DHCP Inform message?
11. What are the source IP and destination IP addresses in the DHCP Ack message?
12. What values in the DHCP discover message differentiate this message from the DHCP request message?
13. What is the value of the Transaction-ID?
14. What is the IP address of the DHCP server?
15. What IP address is the DHCP server offering to your host in the DHCP Offer message?
16. What is the purpose of the lease time? How long is the lease time in your experiment?



0 7	8 15	16 23	24 31
Operation code	Hardware address type	Hardware address length	Hops
Client ID			
Start time		Flags	
Client address			
Offered address			
Server address			
Relay agent address			
Client hardware address			
Server name			
File name			
Options			

Figure 4: DHCP Packet

Laboratory #4 (TCP and HTTP)

In this lab, we will examine the content of the TCP header and HTTP packets. Firstly, we need to prepare the Wireshark to capture packets from the right network interface as follows:

1. Open Wireshark and start capture from the right network interface.
2. Enable the internet connection in your PC.
3. Open your web browser and browsing any websites for a few seconds.
4. Stop the Wireshark.

Secondly, types "http" in the filter bar to display all HTTP packets. Then, double click on any packet and open the "Hypertext Transfer Protocol". ***Figure 5*** shows the content of the TCP header.

Finally, try to answer any question such as the following:

1. What is the request Method?
2. What is the request URI?
3. What is the request Version?
4. What is content of the host field?
5. What is content of the connection field?
6. What languages does your browser indicate that it can accept to the server?
7. What is the status code returned from the server to your browser?
8. How many bytes of content are being returned to your browser?
9. What are the source and destination port numbers?
10. What are the sequence and acknowledgement numbers?
11. What is the TCP header length?
12. How many bytes are in the TCP payload?
13. How many TCP segments are sent?

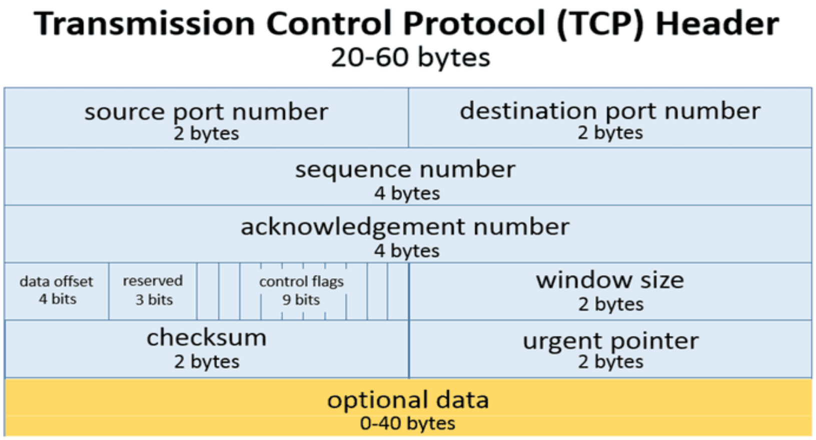


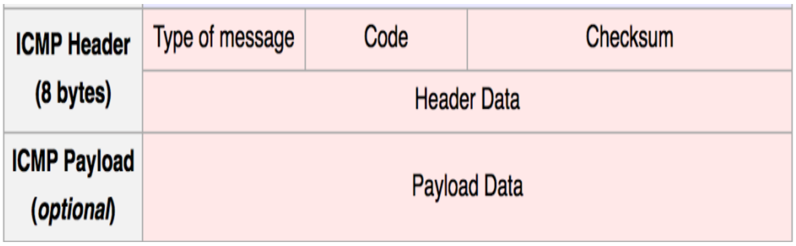
Figure 5: TCP Header

Laboratory #5 (ICMP)

In this lab, we will examine the content of the ICMP packets. Firstly, we need to prepare the Wireshark to capture packets from the right network interface as follows:

1. Open the VMware and start the operating system.
2. Get the IP address of the VMware guest.
3. Open Wireshark and start capture from the right network interface.
4. Open the CMD in your main operating system and execute the following commands:
   a. Ping -n 2 VM_IP // VM_IP is the IP address of the VMware guest.
   b. Ping -n 2 -l 1500 VM_IP
5. Stop the Wireshark.

Secondly, types "icmp" in the filter bar to display all ICMP packets. Then, double click on any packet and open the "Internet Control Message Protocol". ***Figure 6*** shows the content of the ICMP packet.



ICMP Header **(8 bytes)**	Type of message	Code	Checksum
	Header Data		
ICMP Payload ***(optional)***	Payload Data		

Figure 6: ICMP Packet

Finally, try to answer any question such as the following:

1. What is the type of the ICMP packet?
2. What is the source and destination IP addresses?
3. Why is it that an ICMP packet does not have source and destination port numbers?
4. What is length (in Bytes) of the checksum, sequence number and identifier fields?

5. What is the length of the data field?
6. What is value of the TTL field?
7. What information in the IP header indicates that the packet been fragmented?
8. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet length in ***ping*** to be 1500. Has that message been fragmented across more than one IP packet? If yes, how many fragments were created from the original packer? And how many bytes in each fragment?
9. What fields change in the IP header among the fragments?

Laboratory #6 (Wireshark Statistics)

In this lab, we will examine the network statistics of the captured packets. Firstly, we need to prepare the Wireshark to capture packets from the right network interface as follows:

1. Open Wireshark and start capture from the right network interface.
2. Enable the internet connection in your PC.
3. Open your web browser and browsing any websites for a few seconds.
4. Stop the Wireshark.

Secondly, from the statistics tab in the Wireshark, answer the following questions:

1. What is the capture time of the first and last packets?
2. From which interface the Wireshark capture the packets?
3. How many packets and bytes have been captured?
4. How many packets and bytes have been captured per second?
5. How many frames have been captured?
6. How many IPv4 packets and its percentage?
7. How many IPv6 packets and its percentage?

8. How many ICMP packets and its percentage?
9. How many UDP and TCP packets and its percentage?
10. How many packets have been sent during the conversation between Host_A and Host_B? and how many sent by Host_A? and how many sent by Host_B?
11. How many packets have been sent during the conversation between MAC_A and MAC_B? and how many sent by MAC_A? and how many sent by MAC_B?
12. How many UDP packets have been sent during the conversation between Host_A:port_A and Host_B:port_B? and how many sent by Host_A:port_A? and how many sent by Host_B:port_B?
13. How many TCP packets have been sent during the conversation between Host_A:port_A and Host_B:port_B? and how many sent by Host_A:port_A? and how many sent by Host_B:port_B?
14. How many packets have been sent by Host_A?
15. How many packets have been Received by Host_A?
16. How many packets have been sent and received by Host_A?
17. How many packets have been sent by Host_A:port_B?
18. How many packets have been Received by Host_A:port_B?
19. How many packets have been sent and received by Host_A:port_B?
20. How many frames have been sent by MAC_A?
21. How many packets have been Received by MAC_A?
22. How many packets have been sent and received by MAC_A?
23. How many packets have length between 160-319?
24. What is the length of the smallest captured packet?
25. What is the length of the largest captured packet?
26. How many DHCP packets?
27. How many DHCP request packets?
28. How many DHCP Inform packets?
29. How many DHCP ACK packets?
30. How many DNS packets?
31. How many DNS query packets?

32. How many DNS response packets?
33. How many HTTP packets?
34. How many HTTP request packets?
35. How many HTTP request packets using Get method?
36. How many HTTP response packets?
37. How many succeeded response HTTP packets?