***Lab Title:*** *Analysis of UDP in Wireshark*

***Name: Mujtaba Shahid Faizi***

***Regn No: 131818***

***Current IP address: 10.99.31.81***

***Objective of this lab:***

*In this lab, we will analyze the behavior of UDP in detail, determining the number of fields in UDP header, the value in the UDP header fields, and maximum number of bytes in UDP payload, source & destination port numbers etc.*

***Instructions:***

* *Read carefully before starting the lab.*
* *These exercises are to be done individually.*
* *You are supposed to provide the answers to the questions listed at the end of this document (substantiate your answers with screen shots of your Wireshark captures) and upload the completed report to your course’s LMS site.*
* *Avoid plagiarism by copying from the Internet or from your peers. You may refer to source/ text but you must paraphrase the original work.*

***Background:***

1. ***Introduction to UDP:***

UDP (User Datagram Protocol) is a simple transport layer protocol for client/server network applications based on [Internet Protocol (IP)](http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm). UDP is the main alternative to TCP and one of the oldest network protocols in existence, introduced in 1980. UDP is often used in videoconferencing applications or computer games specially tuned for real-time performance. To achieve higher performance, the protocol allows individual packets to be dropped (with no retries) and UDP packets to be received in a different order than they were sent as dictated by the application.

1. ***UDP Datagrams:***

UDP network traffic is organized in the form of datagrams. A datagram comprises one message unit. The first eight (8) bytes of a datagram contain header information and the remaining bytes contain message data.

A UDP datagram header consists of four (4) fields of two bytes each: Source port number, Destination port number, Datagram size and checksum

* 1. **UDP port number:** UDP [port numbers](http://compnetworking.about.com/od/networkprotocols/f/port-numbers.htm) allow different applications to maintain their own channels for data similar to TCP. UDP port headers are two bytes long.
  2. **Datagram size:** The UDP datagram size is a count of the total number of bytes contained in header and data sections. As the header length is a fixed size, this field effectively tracks the length of the variable-sized data portion (sometimes called payload). The size of datagrams varies depending on the operating environment but has a maximum of 65535 bytes.
  3. **Checksum**: UDP checksums protect message data from tampering. The checksum value represents an encoding of the datagram data calculated first by the sender and later by the receiver. Should an individual datagram be tampered with or get corrupted during transmission, the UDP protocol detects a checksum calculation mismatch. In UDP, check-summing is optional as opposed to TCP where checksums are mandatory.

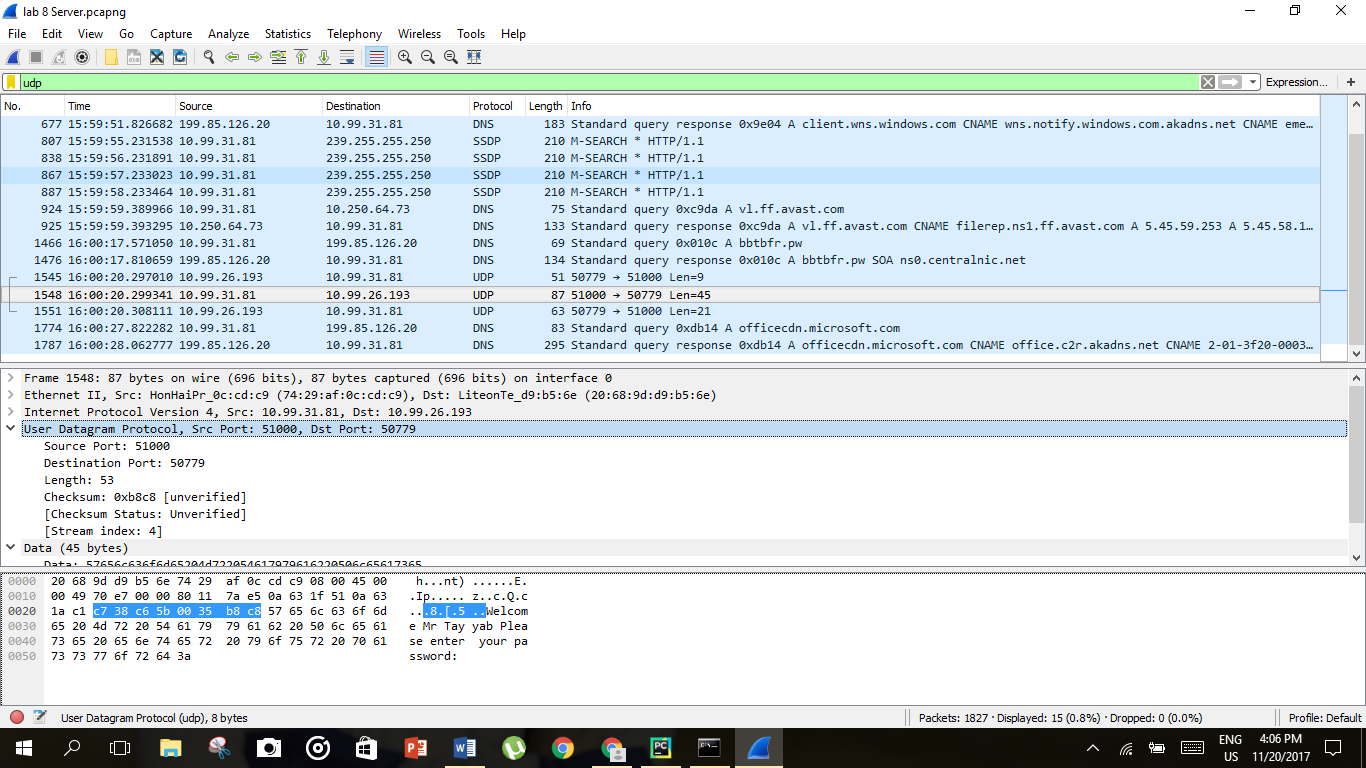
***Steps for performing this lab:***

*Do the following:*

1. ***Download*** *files UDPCient.py and UDPServer.py from your LMS site.*
2. ***Edit*** *these files. In UDPClient.py The serverIP address; use one of your neighbor and the message; as your name. In UDPServer.py use your own IP address*
3. ***Start up the Wireshark software.***
4. ***Begin packet capture,*** *select the Capture pull down menu and select Options.*
5. ***Selecting the network interface on which packets would be captured:*** *You can use most of the default values in this window. The network interfaces (i.e., the physical connections) that your computer has to the network will be shown in the Interface pull down menu at the top of the Capture Options window. Click Start. Packet capture will now begin*
6. ***Run your UDPServer and UDPClient.***
7. ***Stopping the capture and inspecting captured packets:*** *After you have received a welcome message, stop Wireshark packet capture*
8. ***Filtering:*** *Filter the UDP packets.*
9. ***Details of a packet:*** *Select the UDP messages shown in the packet-listing window and analyze by looking into the detail of packets pane and answer the questions given at the end of this document.*
10. ***Obtaining credit for this lab:*** *Now, please proceed to the questions section to answer the questions. You must note down your answers, along with screen shots in this file itself. Please note that you must upload this file (after duly filling in the answers) through the appropriate link at your LMS to obtain credit. Please clarify with your instructor/ lab engineer if you have any queries.*

***Questions:***

1. *Select one UDP packet and determine the* ***Source IP, Source port No, Destination IP and Destination port No*** *of that UDP packet.*





*SourceIP:10.99.31.81  
DestIP:10.99.26.193  
SourcePort:51000  
Dest Port:50779*

1. *Select one UDP packet and determine how many* ***fields*** *are there in the UDP header. List* ***the name of these fields*** *and write the length in bytes of each field.*

*6 fields:*

*Source port*

*Destination port*

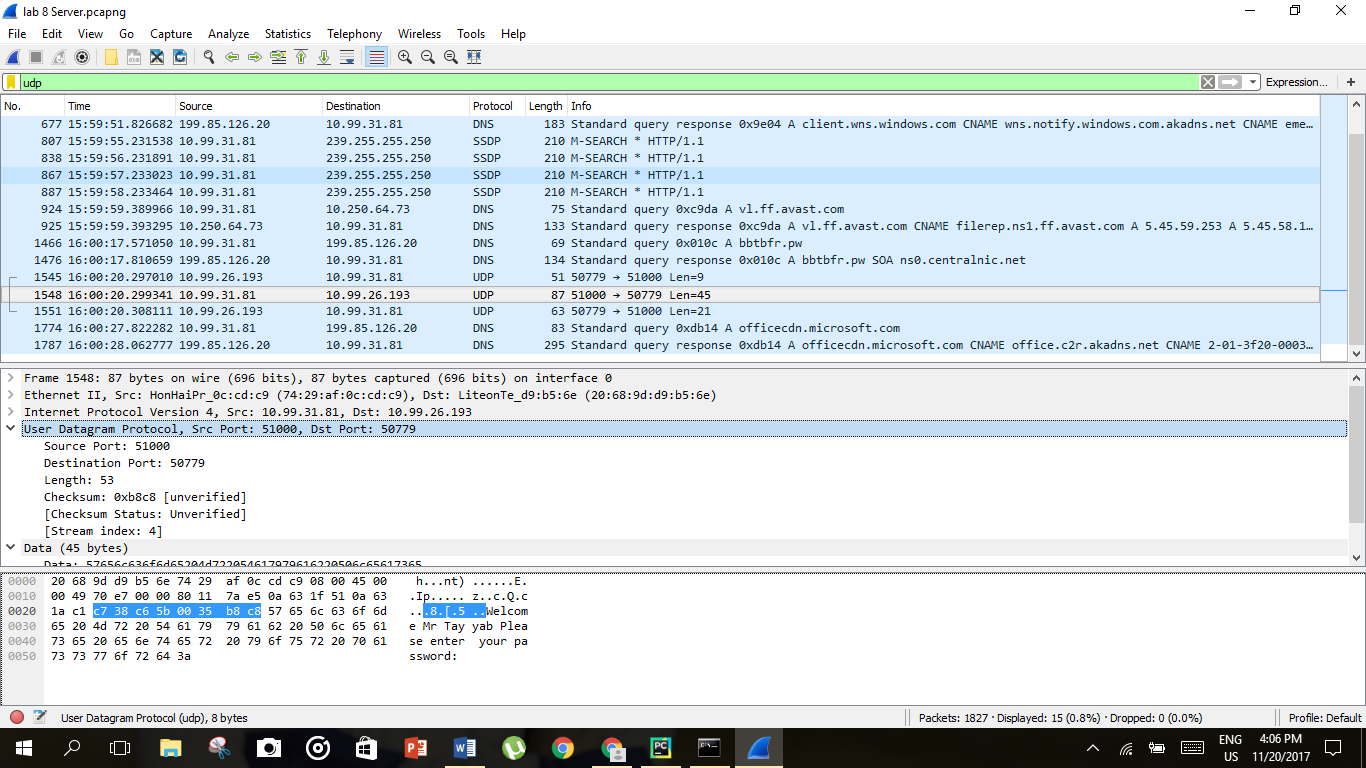
*Length*

*Checksum*

*Checksum status*

*Stream index*

*Each field has 2 bytes.*





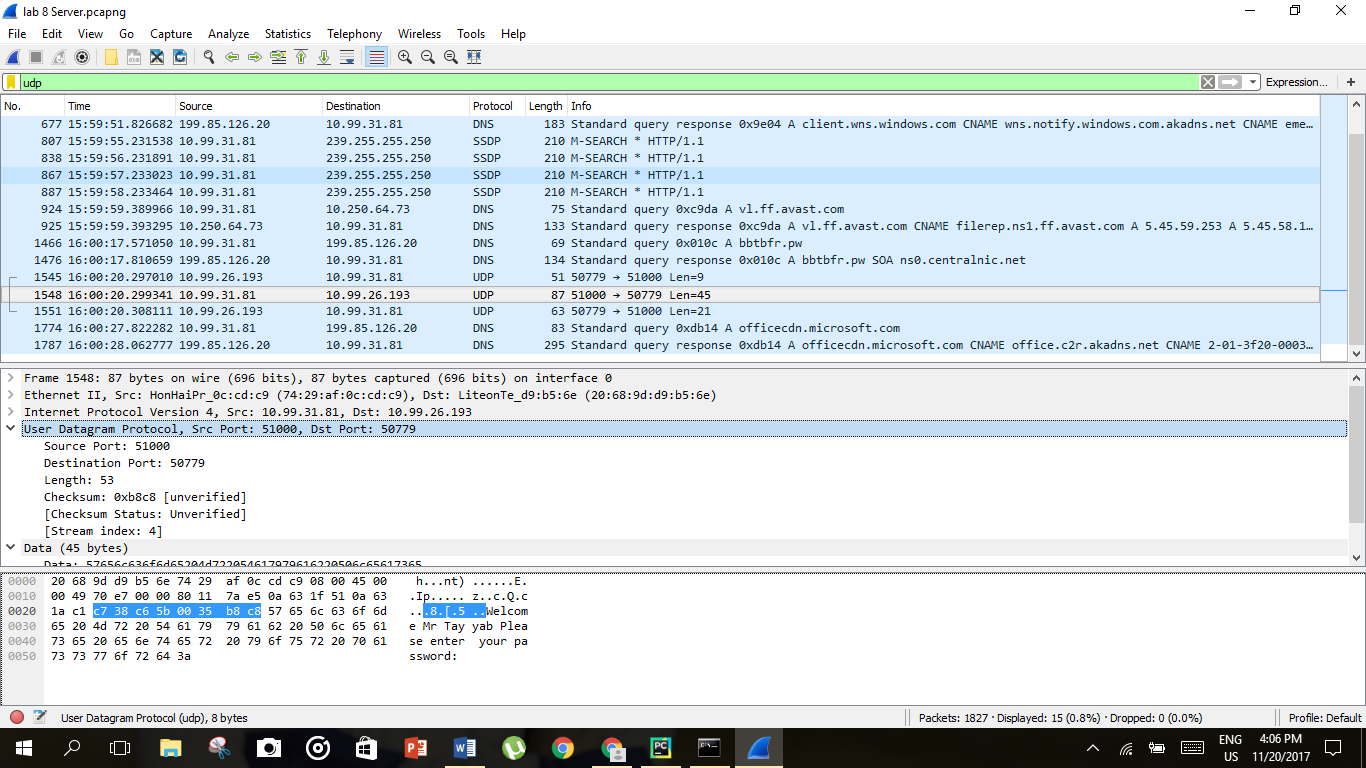
1. ***Examine the pair of UDP packets*** *in which your host sends the first packet and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.*

*One port number is manually assigned while the other port number is checked in the packet’s header.*

1. *Analyze the UDP packet and answer that the* ***value in the Length field*** *is the length of what? Verify your claim with your captured UDP packet.*

*Length:53*

*UDP header and UDP data*





*Data:45+Header:8=53bytes*

1. *What is the* ***maximum number of bytes*** *that can be included in a UDP payload? Why this is the maximum?*

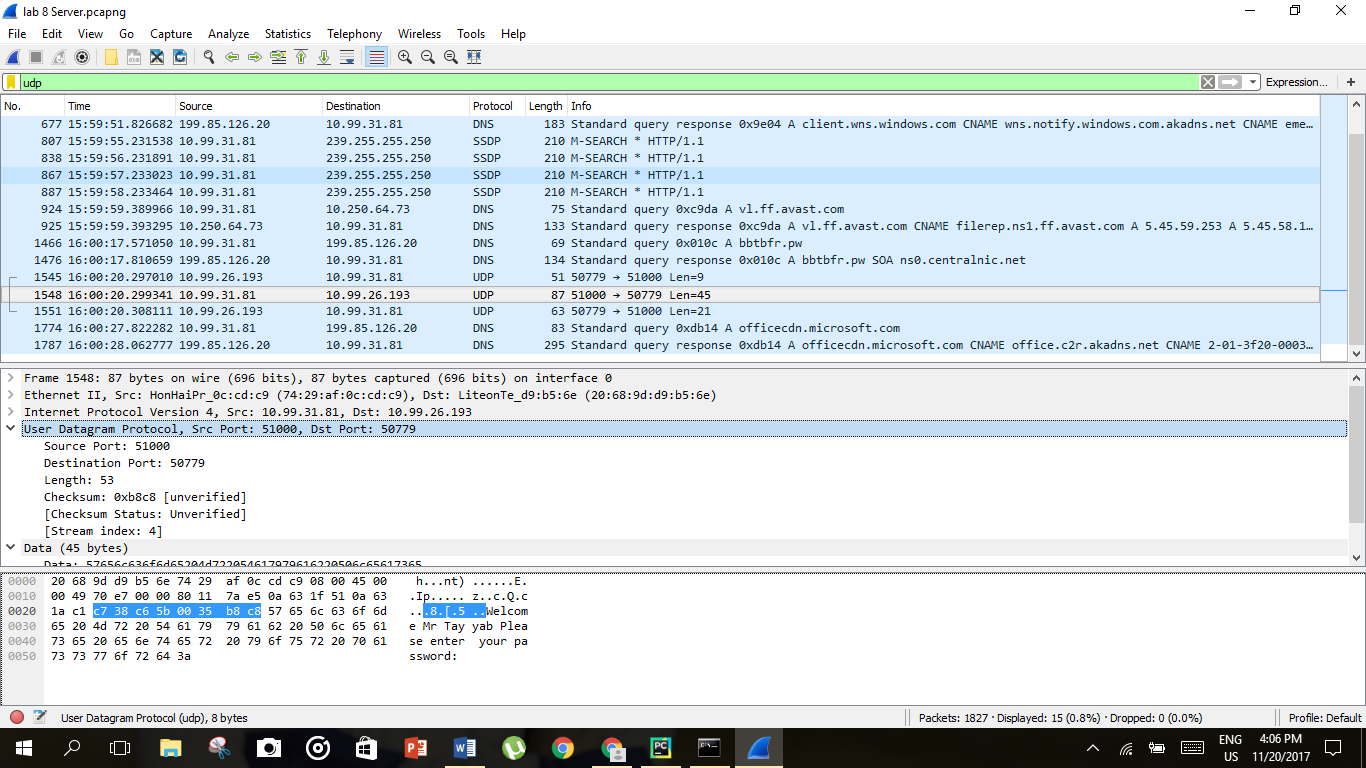
*655527 bytes*

*Due to the theoretical limit of ipv4 packet size*

1. *How much* ***data*** *has been sent from Client to the server and from the server to the client?*

*Client to server: 2 packets: 21 and 9 bytes*

*Server to client: 1 packet of 45 bytes*

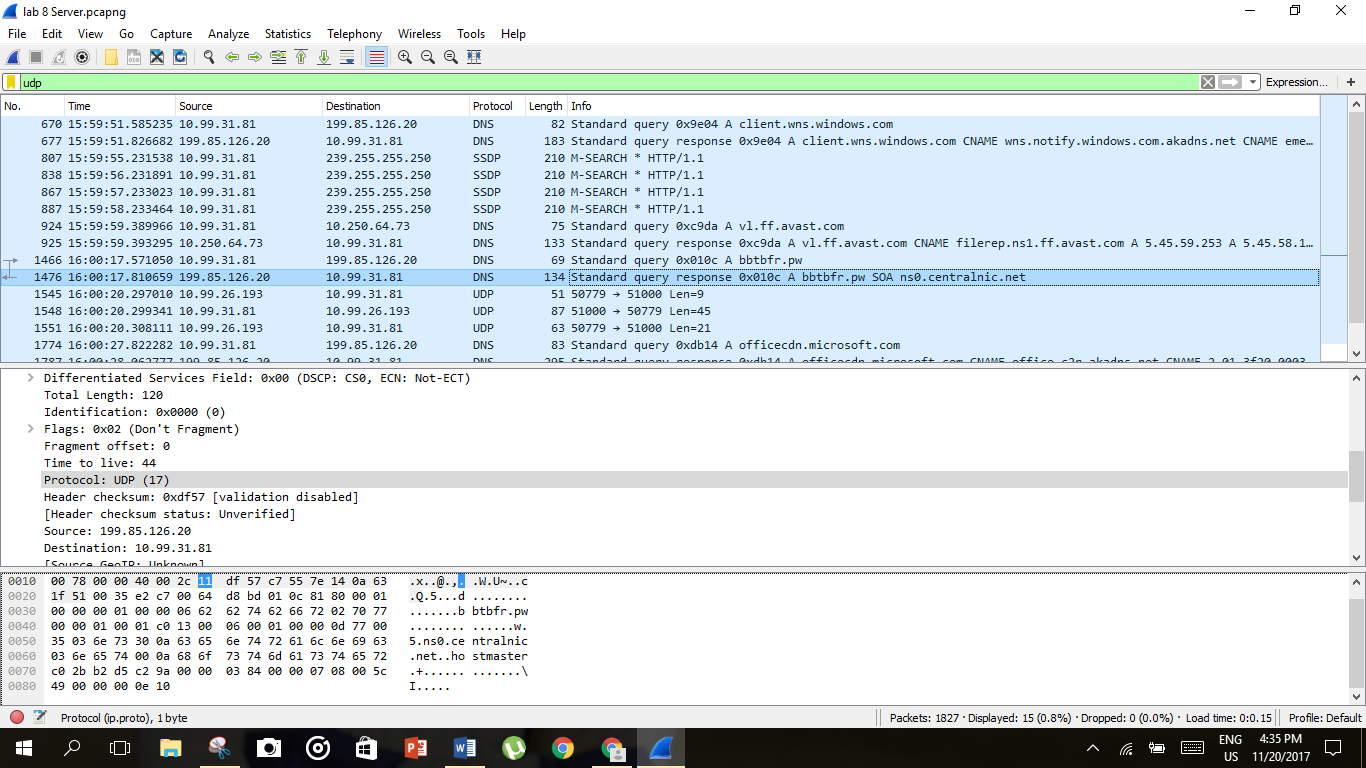




1. *What is the* ***protocol number for UDP****? Give your answer in both hexadecimal and decimal notation.*

*Decimal: 17*

*Hexadecimal:11*





1. *Compare the* ***checksum values*** *in the UDP segment header sent from client to server and from the server to the client. Are they same or they differ? If the payload of each packet is same, would the checksum change?*

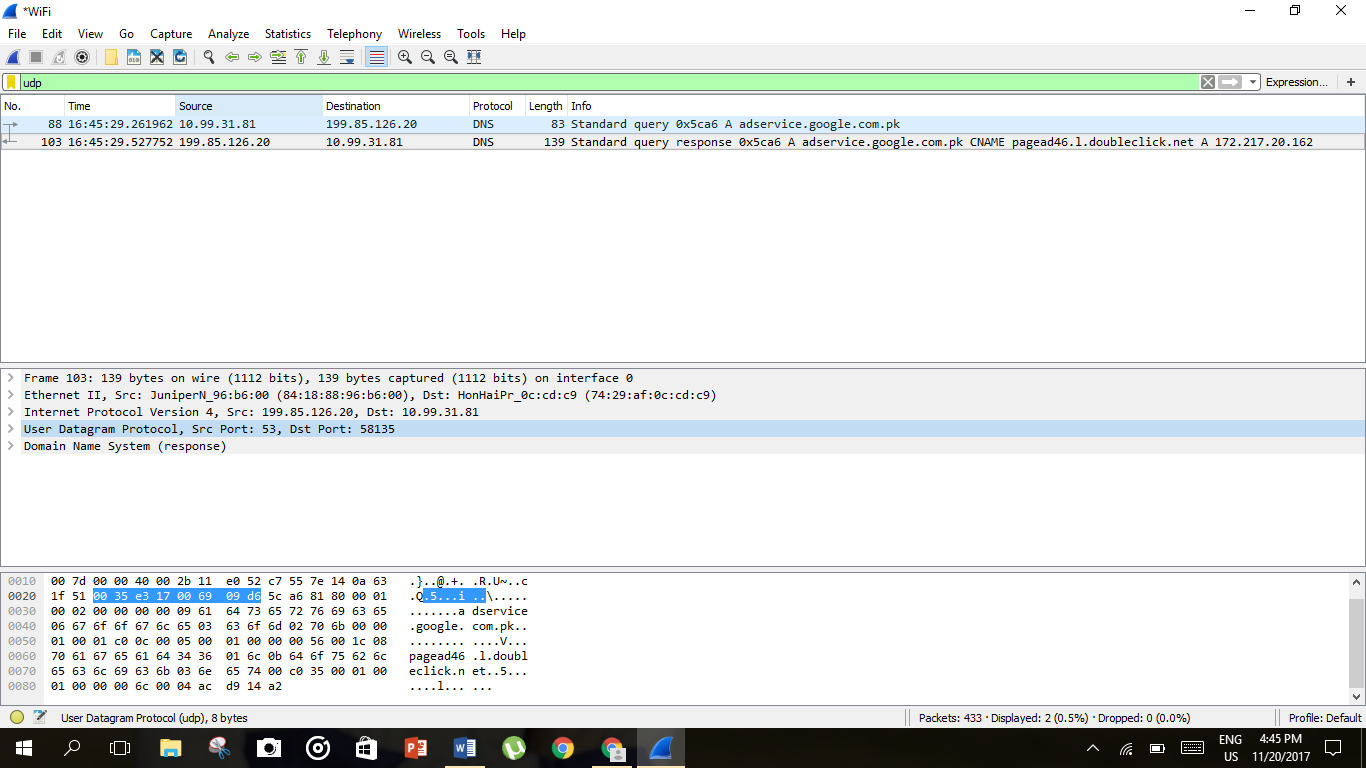
*They are different.*

*If the payload is same, checksum would change*

1. *Which fields are included in calculating the UDP checksum?*

*Information in IP header, UDP header and data is used to calculate the UDP checksum.*

1. *Run any application you know of that uses UDP at the transport layer. Capture the interaction using wireshark and verify that the application is indeed running on UDP.*





*DNS query*