Student Name : _____

Group : _____

Date : _____

LAB 3: SNIFFING AND ANALYSING NETWORK PACKETS

EXERCISE 3A: PACKETS CAPTURING

List the sequence of all relevant network packets sent and received by your laboratory PC from the time your Rfc865UdpClient initiated a request to the DNS server to resolve the QoD server name till it received the quote of the day. Fill in the MAC and IP address of the packets where appropriate/available.

Packet	Source MAC	Source IP	Dest. MAC	Dest. IP	Purpose of Packet
1.					DNS request
2.					
...					
Last.	QOTD server		Your QotdClient		Quote of the day reply

What is the IP address of DNS server? [_____]
What is the IP address of the QoD server? [_____]
What is the MAC address of the router? [_____]

EXERCISE 3B: DATA ENCAPSULATION

Complete Captured Data (please fill in ONLY 8 bytes in a row, in hexadecimal)	

EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

What type of upper layer data is the captured ethernet frame carrying?
How do you know?

Determine the following from the captured data in Exercise 3B:

Destination Address	
Source Address	
Protocol	
Frame Data (8 bytes in a row, in hexadecimal)	

EXERCISE 3D: NETWORK PDU - IP DATAGRAM

What type of upper layer data is the captured IP packet carrying? How do you know?

Does the captured IP header have the field: Options + Padding? How do you know?

Determine the following from the Frame Data field in Exercise 3C:

Version	
Total Length	
Identification	
Flags (interpret the meanings)	
Fragment Offset	
Protocol	
Source Address	
Destination Address	
Packet Data (8 bytes in a row, in hexadecimal)	

EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

Determine the following from the Packet Data field in Exercise 3D:

Source Port	
Destination Port	
Length	
Data	

(8 bytes in a row, in hexadecimal)	

EXERCISE 3F: APPLICATION PDU

Interpret the application layer data from the Data field in Exercise 3E:

Message	

Is this the message that you have sent?