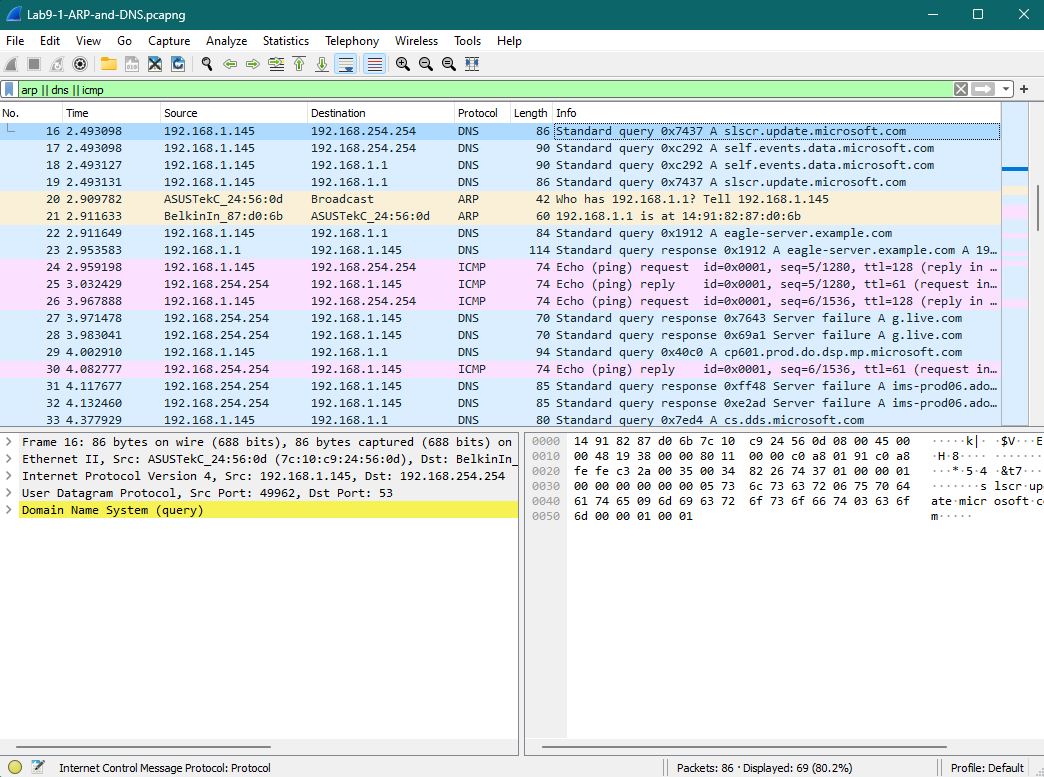
***Lab 9 answer sheet***

**Name: Nouraldin Hassan**

**Student number: 041054019**

Q1) Add a screenshot for Task 1 step 6 (showing the whole Wireshark window) and highlight the **APR** **request and the reply with the same color**, and the **DNS query and the reply with another colors**.



Also, answers these questions:

For the DNS QUERY  
source port: **192.168.1.145**destination port: **129.168.1.1**

For the DNS RESPONSE  
source port: **192.168.1.1**destination ports: **192.168.1.145**

How was the source port chosen on the client?

**It was chosen automatically. It is handled by the Transport Layer.**

How was the destination port chosen on the server?

**It was pre-determined by the server. It is associated with the service itself, i.e. DNS using port 53 and HTTP using port 80, both by default.**

What is the name of the DNS server that responded?

**Eagle Server.**

Q2) Screenshot for Task 2 step 5 (showing the whole Wireshark window) and **highlight the two http request frames**

A screenshot of a computer

Description automatically generated

*I don’t know why multiple HTTP requests happened like that. I cleared my cache multiple times prior to this capture*.  
*I also updated Wireshark to a newer version.*

Which layer 4 protocol is used for http?

**TCP is used for HTTP**

Which flags are set for each stage of the three way handshaking?

**SYN (Synchronize) is set first, where SYN is** **sent by the client to initiate a connection.**  
**SYN-ACK (Synchronize-Acknowledge) is set second, where SYN-ACK is sent by the server in response to the SYN flag.**  
**ACK (Acknowledge) is set third, where ACK is** **sent by the client to acknowledge the SYN-ACK flag from the server.**

What were the source and destination ports in the first web page request?

**Frame Number 447, SRC: 59981. DST: 80**

What were the source and destination ports of the acknowledged packet of the previous question? Was the acknowledgment sent by the layer 4 or the layer 7 protocol?

**Both SRC and DST ports are the same as given above, and acknowledgment was sent by the Layer 4 protocol.**

What were the source and destination ports in the second web page request?

**Frame Number 451, SRC: 59982. DST: 80.**

Did the client use the same source port as it did for the 1st web page?

**No, but generally the client would use the same source port as it did for the first web page request as it would reuse the same TCP connection for both requests­­[1].**

Is this the same layer 4 sessions, or a different one?

**Not entirely. The client and server could maintain the destination port, but not the source port nor the sequence and acknowledgement numbers**[1]**.**

Q3) Screenshot for Task 3 step 4 (showing the whole Wireshark window) and **highlight the DHCP Discover, Offer, Request and Acknowledgement**

A screenshot of a computer

Description automatically generated

*I updated Wireshark to a newer version.*

[1] “What Is Layer 7 Load Balancing?,” Benefits of layer 7 load balancing: Nginx Load balancer, <https://www.nginx.com/resources/glossary/layer-7-load-balancing/> (accessed Nov. 23, 2023).