|  |  |  |
| --- | --- | --- |
|  | | |
|  | | |
| Answer Sheet | | |
| Assignment - A05 | | |
| A Day in The Life of a Webpage Request | | |
| Name | : | Alvaro Austin |
| Student ID | : | 2106752180 |

|  |
| --- |
| **Notes:**   1. All answers you provide must be supported with relevant screenshots in the space provided. You can also highlight the part of the screenshot where it supports your answer. 2. Make sure before submitting a report, all screenshots and answers can be read by the assessment team properly. |

|  |
| --- |
| **Client PC Network Configuration:** |
| **Server PC Network Configuration:** |

# [10 points] The Protocols

|  |  |  |
| --- | --- | --- |
| **Layer** | **Protocol** | **Frame Number** |
| **Application Layer** | DNS | 58 |
| **Application Layer Screenshot:** | | |
| **Transport Layer** | Transmission Control Protocol (TCP) | 65 |
| **Transport Layer Screenshot** | | |
| **Network Layer** | Internet Protocol (IP) | 65 |
| **Network Layer Screenshot:** | | |
| **Link Layer** | Ethernet | 65 |
| **Link Layer Screenshot:** | | |

# [20 points] The First Step

1. **[2 points]** Based on your observation, which frame is the ﬁrst frame related to the communication between the client machine and the server machine?

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  The first frame that is related to communication between the client machine and the server machine is frame 58. This indicates the start of the communication, when the client try to access the web of a4.jarkom.csui. DNS is an application layer protocol that is used to mapped an IP Address to specific domain name. In this case, the DNS server (10.1.0.2), finds the server which was 10.0.0.27 and told the client about this information. |

1. **[2 points]** What protocol is primarily being used in the frame (and is identiﬁed by Wireshark as that protocol)?

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  Protocol that is primarily being used in the frame is the application layer protocol, the Domain Name System Protocol. |

1. **[5 points]** What function does the communication done with this frame (and its counterpart) serve as part of the communication between the client and server machines?

|  |
| --- |
| **Screenshot:**  Frame 58:    Frame 61: |
| **Explanation:**  The role of this frame is to translate the domain name using DNS protocol to get the desired IP that mapped to the domain name. As you can see in the screenshot above, the first frame that was related to the communication between the client and the server is frame 58, in which, DNS protocol, has 1 question. The question is related to the IP Address of a4.jarkom.csui.Then, in frame 61, DNS gave their answer, which highlighted in blue color in the screenshot above.  From the highlights, you can see that when the client access a4.jarkom.csui, DNS protocol translate that domain name using DNS protocol, then returns the IP address once it’s found. |

1. **[2 points]** Who is the sender of the frame? The answer options are “Client”, “Server”, and “DNS Server”. However, you need to elaborate on how you deduce who the sender is based on existing information.

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  The sender of the frame is the client. The client in this case is the Client A4 with IP of 10.0.0.26. I can deduce this because the first frame has the source IP address of the client. |

1. **[2 points]** Who is the recipient of the frame? The answer options are “Client”, “Server”, and “DNS Server”. However, you need to elaborate on how you deduce who the recipient is based on existing information.

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  The recipient of the frame 58 is the DNS Server. DNS Server acts as the local DNS server to map the domain name to find the desired IP address. The reason I chose this, is because the destination of the frame is towards the IP address of DNS Server. |

1. **[2 points]** Based on your observation, which frame is the response for the frame that you identiﬁed in the ﬁrst number?

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  The frame that was the response of my request is frame 61. This is because the response above were sent by DNS server back to the client for the answers. As you can see in the above screenshots, there were also answers. You can see in the first number screenshot, there is “Response in: 61”. |

1. **[5 points]** What is the information that is contained in the response that fulﬁlls the function of this communication? Please be speciﬁc regarding the information type.

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  The information that is contained in the response is the type, which was, A record, towards address 10.0.0.27 (Server). This response basically meant that, a4.jarkom.csui is mapped to IP address of 10.0.0.27, from then on, the client will know that when they sent request to a4.jarkom.csui, it will automatically refer to IP 10.0.0.27 until TTL is expired. |

# [20 points] The Second Step

1. **[2 points]** Based on your observation, which frame is the next frame, after the first step and its response, related to the communication between the client machine and the server machine?

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  The frame that is the next frame is frame 63. This frame is right after the last frame of DNS protocol frames related to communication between the client and the server. |

1. **[5 points]** What protocol is primarily being used in the frame (and is identified by Wireshark as that protocol)?

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  Protocol that is primarily used in the frame is Address Resolution Protocol (ARP). ARP is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN). |

1. **[2 points]** What function does the communication done with this frame (and its counterpart) serve as part of the communication between the client and server machines?

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  This ARP protocol is used to find the MAC address of a PC. This MAC address is used to uniquely identify PC’s related. The MAC address is then used for each PC to communicate with each other. This frame is basically broadcast to all PC, to find the mac address of the PC that has the IP address of 10.0.0.27. |

1. **[2 points]** Who is the sender of the frame? The answer options are “Client”, “Server”, and “DNS Server”. However, you need to elaborate on how you deduce who the sender is based on existing information.

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  The sender of the frame is the client. The reason for this, is because Wistron\_22::cb:8a (sender) is the MAC Address of the client. Hence the client, is the sender of the frame. This information is backed because from the detail, you can see that Sender IP Address is 10.0.0.26, which is the client. |

1. **[2 points]** Why is the sender address format different between the first and second step?

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  The sender address format in second step is the MAC address of the sender of first step (Client’s MAC address). So these two is different because MAC address identify physical address of a device (Client), and IP address identify the device (client) globally. |

1. **[2 points]** Based on your observation, which frame is the response for the frame that you identified in the first number?

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  The frame that gives the response for previous frame is **frame 64.** |

1. **[5 points]** What is the information that is contained in the response that fulfills the function of this communication? Please be specific regarding the information type.

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  As you can see in the screenshot above, the reason that the response fulfills the function of this communication is because the response replied back to the initial sender (client). This happened because when previously, the client ask for server’s MAC Address (initially, MAC address for server is 00:00:00:00:00:00). Then, as you can see from the screenshot, the server sent back a reply with the sender MAC address of 00:26:2d:14:4a:67. Hence, ARP is fulfilled because the ARP request has been replied with the information of server’s MAC Address. |

# [8 points] HTTP and Its Transport

1. **[3 points]** Look for a frame that has information about the HTTP request to the domain that has been loaded. What transport layer protocol supports the selected frame?

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  Transport layer protocol that supported it’s selected frame is Transmission Control Protocol (TCP). This can be found in the details of the request, above Hypertext Transfer Protocol. |

1. **[5 points]** Does the HTTP protocol include information regarding the origin and destination of the request? Explain specifically the type of information it contains, for example MAC Address, FQDN, and others!

|  |
| --- |
| **Screenshot:**  **Origin: -**  **Information Regarding Destination of the Request in HTTP Protocol:**    **MAC Address:**    **FQDN:**    **IP Address of Source and Destination:** |
| **Explanation:**  Partially, yes and no. HTTP protocol doesn’t include the origin of the request, but they do include the destination of request in form of FQDN. Meanwhile, Network layer does show the source and destination IP address but network layer is not considered HTTP protocol.  The HTTP protocol itself does not include information about MAC addresses. MAC addresses are part of the lower-level network protocols, such as Ethernet, which operate at the data link layer of the networking stack. MAC addresses are used for communication between devices within a local network.  Basically, MAC Address and source address doesn’t directly visible on HTTP protocol, but in other protocol in HTTP request, it has the supporting data there. |

# [15 points] TCP Connection Life Cycle

1. **[10 points]** Identify all frames that form the mechanism for establishing and disbanding the TCP connection in the web page request! Fill in the following table based on the information that you obtain from the identification (add additional rows as needed)!

|  |  |  |
| --- | --- | --- |
| **Frame Number** | **TCP Flag** | **Role** |
| 65 | SYN | The client initiates the TCP connection by sending a SYN packet (synchronize) to the server. |
| 66 | SYN, ACK | The server responds with a SYN-ACK packet (synchronize-acknowledge) to acknowledge the client's request and establish the connection. |
| 67 | ACK | The client sends an ACK packet (acknowledge) to confirm the server's response and complete the three-way handshake. |
| 97 | FIN, ACK | The client sends a FIN packet, indicating its intention to terminate the connection. |
| 98 | ACK | The server acknowledges the receipt of the client's FIN packet. |
| 100 | FIN, ACK | The server also sends a FIN packet, indicating its intention to terminate the connection. |
| 101 | ACK | The client acknowledges the receipt of the server's FIN packet, and the connection is fully terminated. |

1. **[5 points]** Does the TCP include information regarding the origin and destination of the request? Explain specifically the type of information loaded, for example MAC Address, FQDN, and others!

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  TCP doesn’t gives information about the origin and destination of the request. But, they did give information about source and destination port of the request. |

# [7 points] The Network Layer

1. **[2 points]** What is the network layer protocol used by the frame that you have selected? Please be specific in the protocol name!

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  Network layer protocol that is used by the frame is Internet Protocol (IP). |

1. **[5 points]** Does the Network Layer include information regarding the origin and destination of the request? Explain specifically the type of information loaded, for example MAC Address, FQDN, and others!

|  |
| --- |
| **Screenshot:** |
| **Explanation:**  Yes. They give the information regarding the origin and destination of the request. Although, they didn’t specify the information about MAC, FQDN, Port, etc. In the screenshot above, you can see that, there is origin and destination IP address of the request. |

# [20 Points] Synthesis

Based on your observations on this task, create a 150-300 word long narrative, explaining how a web page request can occur and cover all the steps taken, starting from the initial connection that you identified in the second part until the TCP connection is closed after the response is received. Resize the table or add more pages as needed.

|  |
| --- |
| Based on the observation above, when a **client** (**IP: 10.0.0.26**) tried to access a webpage, in this case (a4.jarkom.csui), they needed to see the content in the server (if there is any). In order to see the content on the server, we need to use the domain name to find the correct IP address that was mapped to that particular domain name. So when the client access the domain name (a4.jarkom.csui), they perform a DNS protocol that happened on application layer to **DNS Server (10.1.0.2)** available. This DNS server will perform query that mapped the domain name to find the correct IP address. Once the DNS finds it, they will return the IP address of the **server (10.0.0.27)** to the client.  After that, ARP is performed by the client to find the physical (MAC) address of the server because they were located in the local network. After the server replies back, then the communication can be started. The client then starts a new TCP connection to the server with the sign of **SYN bit to 1**. Afterwards, the server responds back with a packet of SYN-ACK that acknowledges the client request and establishes the connection. Client sends an ACK packet and confirms the server response and completes the three way handshake. Here, the client will send requests to the server and the server will respond back. When the client finishes the request, they send a FIN-ACK to close the connection. Then the server replied back with ACK to acknowledge the FIN packet. Although in my case, there were still packets to be acknowledged, hence the need to have a FIN-ACK packet by the server to terminate the session and an ACK packet replied by the client. |

# 