**Department of Electronics & Communication Engineering**Computer Communication Networks Laboratory   
Worksheet-5

|  |  |  |  |
| --- | --- | --- | --- |
| **Name:** | | | |
| **Semester:** 5 | **Section:** | **SRN:** | **Date:** |

**Lab 5: Analyse the TCP fragmentation when downloading large files from a web-server using Wireshark**

1. Draw the TCP segment structure and briefly explain the functions of each of the flag bits, along with their full forms (URG, ACK, SYN, etc.)

2. How many TCP segments were required to download the requested object? Note down each of their frame numbers and length in bytes.  
3. Fill in the following table:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Request/Response** | **Source IP Address** | **Destination IP Address** | **Source Port No** | **Destination Port No** |
| GET Request | 192.168.45.145 | 128.119.245.12 | 55940 | 80 |
| Response | 128.119.245.12 | 192.168.45.145 | 80 | 55940 |

4. Briefly explain the TCP connection establishment process with a relevant timing diagram.

5. Using Wireshark, answer the following questions and thus verify whether the TCP connection establishment process is taking place as explained above:

i) Who initiated the TCP connection? What was their port number? (Hint: Search for the first packet exchanged between the 2 port numbers mentioned in Q3, and check whether it was sent from the client or the server).

ii) For each of the 3 packets mentioned in the timing diagram above (Q4), note down the following values:  
  
(Note: You can switch between relative and absolute numbers by right clicking on the packet, going to Protocol Preferences -> TCP and then checking/unchecking the ‘Relative sequence numbers’ option.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Frame Number** | **Flags Set  (SYN, FIN, ACK, etc.)** | **Relative Sequence No** | **Relative Ack No** | **Absolute Sequence No** | **Absolute Ack No** |
| 4615 | SYN | 0 | 0 | 1722001088 | 0 |
| 4617 | SYN,ACK | 0 | 1 | 3363488991 | 1722001089 |
| 17597 | ACK | 597 | 243 | 1722001685 | 3363489234 |

6. Briefly explain the TCP connection termination/teardown process with a relevant timing diagram.

7. Using Wireshark, answer the following questions and thus verify whether the TCP connection termination process is taking place as explained above:

i) Who initiated the termination of the TCP connection? What was their port number? (Hint: Search for the first FIN packet exchanged between the 2 port numbers mentioned in Q3, and check whether it was sent from the client or the server).

ii) For each of the 4 packets mentioned in the timing diagram above (Q6), note down the following values:  
  
(Note:   
1. You can switch to relative numbers by right clicking on the packet, going to Protocol Preferences -> TCP and then checking the ‘Relative sequence numbers’ option.  
2. If in case any 2 packets were combined while being sent, copy the same values for both rows.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Frame Number** | **Flags Set  (SYN, FIN, ACK, etc.)** | **Relative Sequence No** | **Relative Ack No** | **Source Port No** | **Destination Port No** |
|  |  |  |  | 42758 | 80 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |