Week#11 – Starting from April 4 – 2016

PART #2

Analyse Transmission of a web request at byte level

1.Learning objectives:

Learn how to analyse a protocol at the byte level.

2. Test Scenario

Client(192.168.1.102) sends a HTTP request to get a file namely 'ethereal-labs/lab2-1.html' from the server Host: gaia.cs.umass.edu (128.119.245.12].

Trace file of this request is attached – http-trace-1.

3. What needs to be done ?

Open the file

Apply HTTP filter.

Select the first frame i.e3. Frame 10.

Click on it .

Ensure that you have enabled (in the Wireshark view)

- Packet details
- Packet bytes

The request message coming out of the host, comprising headers of all the layers , is represented in series of bytes as shown below:

Byte Count (hex)	**0**	
	1	
	2	
	…	
	A	
	B	
	…	
	F	
	10	
	…	
	…	
	1F	
	….	
	2FF	

In wireshark it is shown in PACKET BYTES window.

In this lab, you need to map different layers in to these bytes by inspecting **packet fields and packet bytes.**

Fill up the following :

Message level

	Total number of bits transmitted	
	Total number of bytes transmitted	

Link Layer [Ethernet]

1	Total number of bytes	
2	Destination MAC address	
	Byte count of start of Destination MAC address (Hex)	
3	Source MAC address	
	Byte count of start of Source MAC address (Hex)	

Network Layer [IP]

	Total number of bytes	
	Byte count – First field of IP Header (Hex)	
	Byte count – Last field of IP Header (Hex)	
	Byte count of start of Source IP address (Hex)	
	Source IP address (Hex)	
	Byte count of start of Destination IP address (Hex)	
	Destination IP address (Hex)	

Transport Layer [TCP]

	Total number of bytes	
	Byte count – First field of TCP Header (Hex)	
	Byte count – Last field of TCP Header (Hex)	
	Byte count of start of Source IP address (Hex)	
	Source Port (Hex)	
	Destination Port (Hex)	

Application Layer [HTTP]

	Byte count – First field of HTTP Header (Hex)	
	Byte count – Last field of HTTP Header (Hex)	