



## Lab 1

Packet Analysis at Application layer by using Wireshark Software

### Objective:

1. To introduce student with Wireshark software tool for packet analyzer.
2. To analyze protocol used in application layer such as *http* and *icmp*.

Name : NG JING ER

Section: 09

Date: 20/11/2020

Checked By: Dr Ahmad Fariz Ali



Mark

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

- TCP
- DNS
- ICMPv6

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

54.460699s

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)?

128.119.245.12

What is the Internet address of your computer?

192.168.0.194

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

```
Users\USER\AppData\Local\Temp\wireshark-Wi-Fi\YMPFU0.pcapng 888 total packets, 35 shown

No.    Time                Source                Destination            Protocol Length Info
 66 16:38:22.222697    192.168.0.194        128.119.245.12        HTTP      621    GET /wireshark-labs/INTRO-wireshark-file1.html H1
1.1
Frame 66: 621 bytes on wire (4968 bits), 621 bytes captured (4968 bits) on interface \Device\NPF_{A885E52D-B399-49E1-9911-667672292919},
id 0
Ethernet II, Src: IntelCor_3c:1d:fb (d8:f2:ca:3c:1d:fb), Dst: zte_02:2d:8b (d4:72:26:02:2d:8b)
Internet Protocol Version 4, Src: 192.168.0.194, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 23593, Dst Port: 80, Seq: 1, Ack: 1, Len: 567
Hypertext Transfer Protocol
No.    Time                Source                Destination            Protocol Length Info
 350 16:39:17.092571    211.159.235.216      192.168.0.194        HTTP      193    HTTP/1.1 200 OK
Frame 350: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface \Device\NPF_{A885E52D-B399-49E1-9911-667672292919},
id 0
Ethernet II, Src: zte_02:2d:8b (d4:72:26:02:2d:8b), Dst: IntelCor_3c:1d:fb (d8:f2:ca:3c:1d:fb)
Internet Protocol Version 4, Src: 211.159.235.216, Dst: 192.168.0.194
Transmission Control Protocol, Src Port: 80, Dst Port: 23600, Seq: 140, Ack: 957, Len: 139
Hypertext Transfer Protocol
```