Lab_1b_Wireshark_Intro_v8.0

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

Answer:

2838	51.331400885	157.240.199.17	192.168.30.111	TLSv1.2	348	Application Data
2839	51.331448238	192.168.30.111	157.240.199.17	TCP	68	53986 → 443 [ACK] Seq=1070 Ack=1942 Win=4782 Len=0 TSval=1959…
2840	51.333024825	192.168.30.111	157.240.199.17	TLSv1.2	110	Application Data
2841	51.363889389	157.240.199.17	192.168.30.111	TCP	68	443 → 53986 [ACK] Seq=1942 Ack=1112 Win=691 Len=0 TSval=31836…
2842	51.365093700	192.168.30.111	74.125.250.80	UDP	102	41785 → 19305 Len=58
2843	51.365914421	157.240.199.17	192.168.30.111	TLSv1.2	112	Application Data
2844	51.365934466	192.168.30.111	157.240.199.17	TCP	68	53986 → 443 [ACK] Seq=1112 Ack=1986 Win=4782 Len=0 TSval=1959…
2845	51.383186296	192.168.30.111	74.125.250.80	UDP	102	41785 → 19305 Len=58
2846	51.410796313	74.125.250.80	192.168.30.111	UDP	117	19305 → 41785 Len=73
2847	51.432210235	74.125.250.80	192.168.30.111	UDP	83	19305 → 41785 Len=39
2848	51.432428556	192.168.30.111	74.125.250.80	UDP	102	41785 → 19305 Len=58
2849	51.455713248	192.168.30.111	74.125.250.80	UDP	82	41785 → 19305 Len=38
2850	51.461035580	74.125.250.80	192.168.30.111	UDP	87	19305 → 41785 Len=43
2851	51.505832078	192.168.30.111	74.125.250.80	UDP	82	41785 → 19305 Len=38

Câu 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 packet listing 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.)

Answer:

7030	14.055252565	192.168.30.111	128.119.245.12	HTTP	500	GET / HTTP/1.1
7223	14.311105884	128.119.245.12	192.168.30.111	HTTP	3077	HTTP/1.1 200 OK (text/html)

HTTP GET

```
Frame 7030: 500 bytes on wire (4000 bits), 500 bytes captured (4000 bits) on interface wlo1, id 0
  Interface id: 0 (wlo1)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 25, 2021 01:51:50.771491878 +07
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1632509510.771491878 seconds
  [Time delta from previous captured frame: 0.000153800 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 14.055252565 seconds]
  Frame Number: 7030
  Frame Length: 500 bytes (4000 bits)
  Capture Length: 500 bytes (4000 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```

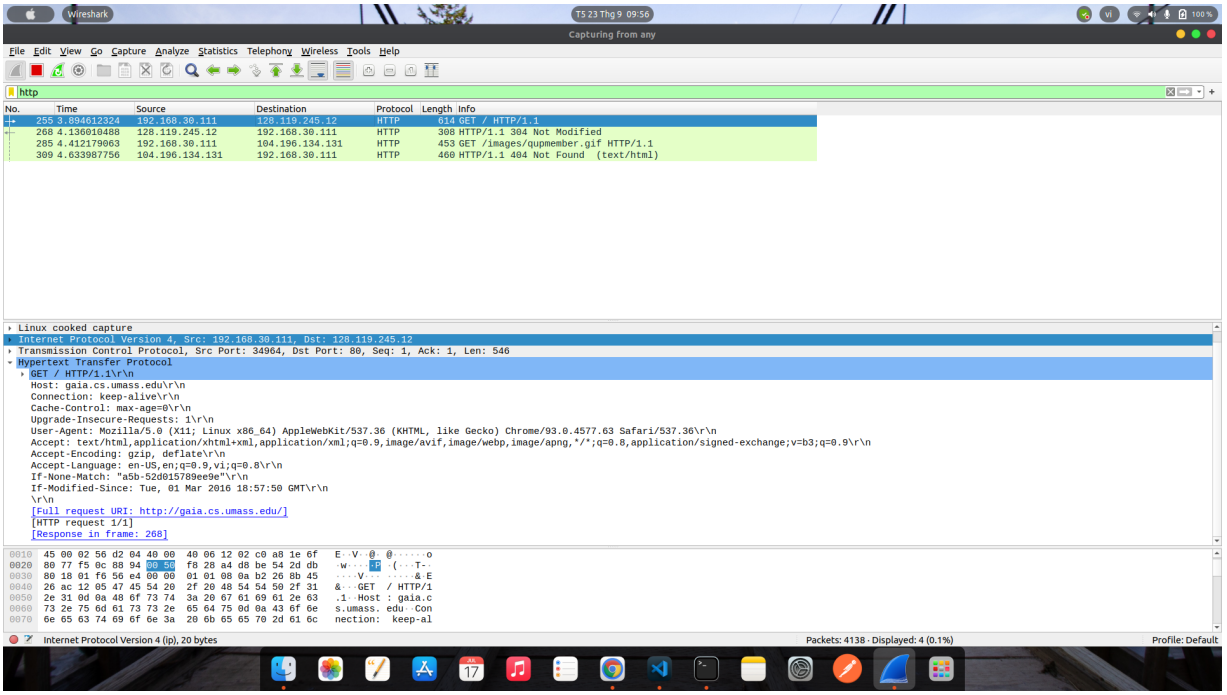
HTTP OK

```
Frame 7223: 3077 bytes on wire (24616 bits), 3077 bytes captured (24616 bits) on interface wlo1, id 0
  Interface id: 0 (wlo1)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 25, 2021 01:51:51.027345197 +07
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1632509511.027345197 seconds
  [Time delta from previous captured frame: 0.000000551 seconds]
  [Time delta from previous displayed frame: 0.255853319 seconds]
  [Time since reference or first frame: 14.311105884 seconds]
  Frame Number: 7223
  Frame Length: 3077 bytes (24616 bits)
  Capture Length: 3077 bytes (24616 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```

Time =1.027345197-0.771491878 = 0.255853319(s)

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

Answer:



- Internet address of the gaia.cs.umass.edu: 128.119.245.12
- Internet address of my computer: 192.168.30.111

Câu 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

HTTP GET

/tmp/wireshark_wlo1_20210925015136_k8OITR.pcapng 203403 total packets, 10 shown

```
No.     Time           Source                Destination           Protocol Length Info
   7030 14.055252565   192.168.30.111        128.119.245.12        HTTP     500    GET / HTTP/1.1
Frame 7030: 500 bytes on wire (4000 bits), 500 bytes captured (4000 bits) on interface wlo1, id 0
    Interface id: 0 (wlo1)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 25, 2021 01:51:50.771491878 +07
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1632509510.771491878 seconds
    [Time delta from previous captured frame: 0.000153800 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 14.055252565 seconds]
    Frame Number: 7030
    Frame Length: 500 bytes (4000 bits)
    Capture Length: 500 bytes (4000 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: IntelCor_97:c3:86 (d0:c6:37:97:c3:86), Dst: Tp-LinkT_e2:32:12 (7c:8b:ca:e2:32:12)
Internet Protocol Version 4, Src: 192.168.30.111, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 39490, Dst Port: 80, Seq: 1, Ack: 1, Len: 434
Hypertext Transfer Protocol
    GET / HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63
Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,vi;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/]
    [HTTP request 1/3]
    [Response in frame: 7223]
    [Next request in frame: 7268]
```

HTTP OK

/tmp/wireshark_wlo1_20210925015136_k8OITR.pcapng 260747 total packets, 10 shown

```
No.     Time           Source                Destination           Protocol Length Info
   7223 14.311105884   128.119.245.12        192.168.30.111        HTTP     3077   HTTP/1.1 200 OK  (text/
html)
Frame 7223: 3077 bytes on wire (24616 bits), 3077 bytes captured (24616 bits) on interface wlo1, id 0
    Interface id: 0 (wlo1)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 25, 2021 01:51:51.027345197 +07
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1632509511.027345197 seconds
    [Time delta from previous captured frame: 0.000000551 seconds]
    [Time delta from previous displayed frame: 0.255853319 seconds]
    [Time since reference or first frame: 14.311105884 seconds]
    Frame Number: 7223
    Frame Length: 3077 bytes (24616 bits)
    Capture Length: 3077 bytes (24616 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Tp-LinkT_e2:32:12 (7c:8b:ca:e2:32:12), Dst: IntelCor_97:c3:86 (d0:c6:37:97:c3:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.30.111
Transmission Control Protocol, Src Port: 80, Dst Port: 39490, Seq: 1, Ack: 435, Len: 3011
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Fri, 24 Sep 2021 18:51:50 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 01 Mar 2016 18:57:50 GMT\r\n
    ETag: "a5b-52d015789ee9e"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 2651\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/3]
    [Time since request: 0.255853319 seconds]
    [Request in frame: 7030]
    [Next request in frame: 7268]
    [Next response in frame: 7543]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 2651 bytes
Line-based text data: text/html (68 lines)
```