



Lab 1:
Packet Analysis at Application Layer Using Wireshark

Name : NUR ALEEYA SYAKILA BINTI MUHAMAD
SUBIAN

Matric No. : A19EC0127

Name : NURUL ALIS ALIA BINTI MOHAMAD
ZAMRI

Matric No. : A19EC0141

Section/Group : 01-06B

Marks:

PART B: HTTP Trace

B.1 1) the version of http that the server running is version 1.1

No.	Time	Source	Destination	Protocol	Length	Info
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

2) the ip address of the client computer is 192.168.1.102

No.	Time	Source	Destination	Protocol	Length	Info
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

3) the ip address of the e gaia.cs.umass.edu server is 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

4) 73 bytes and 1071 bytes

```
Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
    ETag: "1bfed-49-79d5bf00"\r\n
    Accept-Ranges: bytes\r\n
    > Content-Length: 73\r\n
```

```
Hypertext Transfer Protocol
  > HTTP/1.1 404 Not Found\r\n
    Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Vary: accept-language\r\n
    Accept-Ranges: bytes\r\n
    > Content-Length: 1071\r\n
```

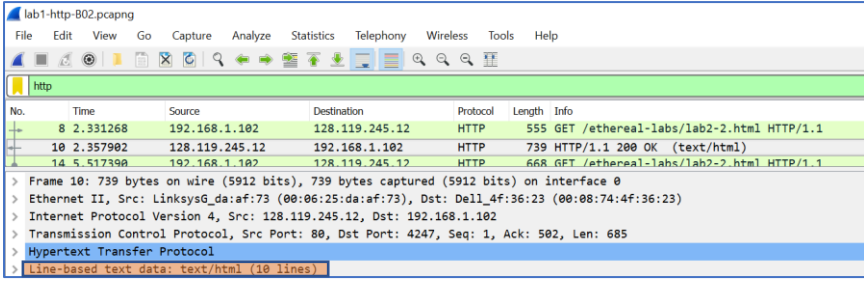
5) the status code returned is 200 OK and 404 Not Found

No.	Time	Source	Destination	Protocol	Length	Info
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

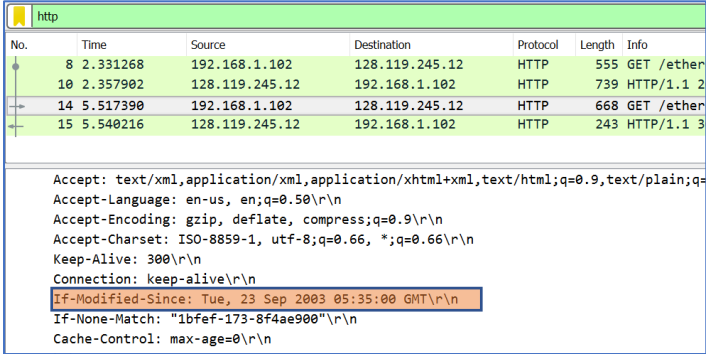
B.2

1) No, “IF-MODIFIED-SINCE” is in the second HTTP GET

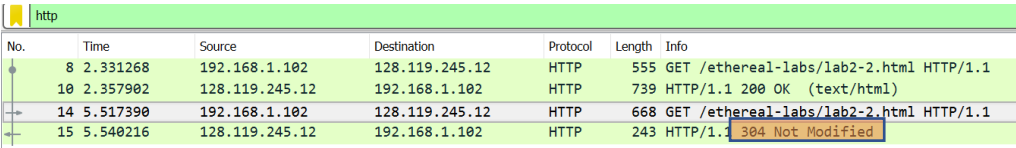
2) Yes, we can see the contents in the “Line-based text data” field.



3) Yes, what follows “IF-MODIFIED-SINCE” is Tue, 23 Sep 2003 05:35:00 GMT

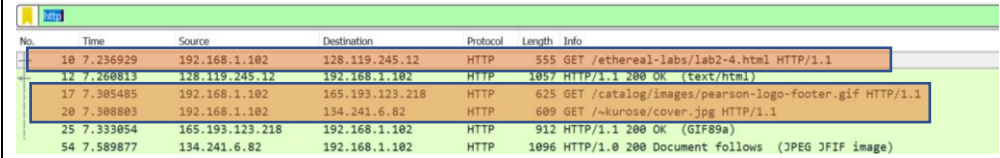


4) The status code is 304 Not Modified. The server did not return the contents of the file since the browser’s cache has up-to-date cached version. There is no modification made after the If-Modified-Since date and time.



B.3

1) There is 3 HTTP GET request messages from the client browser



2)	<p>FIRST HTTP GET : 128.119.245.12</p> <p>SECOND HTTP GET : 165.193.123.218</p> <p>THIRD HTTP GET : 134.241.6.82</p> <table border="1"> <thead> <tr> <th>No.</th> <th>Time</th> <th>Source</th> <th>Destination</th> <th>Protocol</th> <th>Length</th> <th>Info</th> </tr> </thead> <tbody> <tr> <td>10</td> <td>7.236929</td> <td>192.168.1.102</td> <td>128.119.245.12</td> <td>HTTP</td> <td>555</td> <td>GET /ethereal-labs/lab2-4.html HTTP/1.1</td> </tr> <tr> <td>12</td> <td>7.260813</td> <td>128.119.245.12</td> <td>192.168.1.102</td> <td>HTTP</td> <td>1057</td> <td>HTTP/1.1 200 OK (text/html)</td> </tr> <tr> <td>17</td> <td>7.305485</td> <td>192.168.1.102</td> <td>165.193.123.218</td> <td>HTTP</td> <td>625</td> <td>GET /catalog/images/pearson-logo-footer.gif HTTP/1.1</td> </tr> <tr> <td>20</td> <td>7.308803</td> <td>192.168.1.102</td> <td>134.241.6.82</td> <td>HTTP</td> <td>609</td> <td>GET ~/kurose/cover.jpg HTTP/1.1</td> </tr> <tr> <td>25</td> <td>7.333054</td> <td>165.193.123.218</td> <td>192.168.1.102</td> <td>HTTP</td> <td>912</td> <td>HTTP/1.1 200 OK (GIF89a)</td> </tr> <tr> <td>54</td> <td>7.589877</td> <td>134.241.6.82</td> <td>192.168.1.102</td> <td>HTTP</td> <td>1096</td> <td>HTTP/1.0 200 Document follows (JPEG JFIF image)</td> </tr> </tbody> </table>	No.	Time	Source	Destination	Protocol	Length	Info	10	7.236929	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-4.html HTTP/1.1	12	7.260813	128.119.245.12	192.168.1.102	HTTP	1057	HTTP/1.1 200 OK (text/html)	17	7.305485	192.168.1.102	165.193.123.218	HTTP	625	GET /catalog/images/pearson-logo-footer.gif HTTP/1.1	20	7.308803	192.168.1.102	134.241.6.82	HTTP	609	GET ~/kurose/cover.jpg HTTP/1.1	25	7.333054	165.193.123.218	192.168.1.102	HTTP	912	HTTP/1.1 200 OK (GIF89a)	54	7.589877	134.241.6.82	192.168.1.102	HTTP	1096	HTTP/1.0 200 Document follows (JPEG JFIF image)
No.	Time	Source	Destination	Protocol	Length	Info																																												
10	7.236929	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-4.html HTTP/1.1																																												
12	7.260813	128.119.245.12	192.168.1.102	HTTP	1057	HTTP/1.1 200 OK (text/html)																																												
17	7.305485	192.168.1.102	165.193.123.218	HTTP	625	GET /catalog/images/pearson-logo-footer.gif HTTP/1.1																																												
20	7.308803	192.168.1.102	134.241.6.82	HTTP	609	GET ~/kurose/cover.jpg HTTP/1.1																																												
25	7.333054	165.193.123.218	192.168.1.102	HTTP	912	HTTP/1.1 200 OK (GIF89a)																																												
54	7.589877	134.241.6.82	192.168.1.102	HTTP	1096	HTTP/1.0 200 Document follows (JPEG JFIF image)																																												
3)	<p>3357 bytes</p> <ul style="list-style-type: none"> ✓ Hypertext Transfer Protocol <ul style="list-style-type: none"> > HTTP/1.1 200 OK\r\n Server: Netscape-Enterprise/3.6 SP3\r\n Date: Sun, 21 Sep 2003 06:00:35 GMT\r\n Content-type: image/gif\r\n Etag: "6fc149-d1d-3ef0b3f8"\r\n Last-modified: Wed, 18 Jun 2003 18:48:24 GMT\r\n > Content-length: 3357\r\n 																																																	
4)	<p>15642 bytes</p> <ul style="list-style-type: none"> ✓ Hypertext Transfer Protocol <ul style="list-style-type: none"> > HTTP/1.0 200 Document follows\r\n Date: Tue, 23 Sep 2003 05:38:44 GMT\r\n Server: NCSA/1.5.2\r\n Last-modified: Tue, 23 Sep 2003 04:56:38 GMT\r\n Content-type: image/jpeg\r\n > Content-length: 15642\r\n 																																																	

PART C: DNS Trace

C.1	<p>1) The IP addresses are 2001:e68:2:38c::356e, 2001:e68:2:389::356e and 184.28.141.249.</p> <pre> Command Prompt - nslookup Microsoft Windows [Version 10.0.19041.630] (c) 2020 Microsoft Corporation. All rights reserved. C:\Users\Dell Inspiron>nslookup Default Server: cdns01v6.tm.net.my Address: 2001:e68::b:68 > www.microsoft.com Server: cdns01v6.tm.net.my Address: 2001:e68::b:68 Non-authoritative answer: Name: e13678.dspb.akamaiedge.net Addresses: 2001:e68:2:38c::356e 2001:e68:2:389::356e 184.28.141.249 Aliases: www.microsoft.com www.microsoft.com-c-3.edgekey.net www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net </pre>
-----	--

2)

```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.19041.630]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Dell Inspiron>nslookup
Default Server: cdns01v6.tm.net.my
Address: 2001:e68::b:68

> www.microsoft.com
Server: cdns01v6.tm.net.my
Address: 2001:e68::b:68

Non-authoritative answer:
Name: e13678.dspb.akamaiedge.net
Addresses: 2001:e68:2:38c::356e
           2001:e68:2:389::356e
           184.28.141.249
Aliases: www.microsoft.com
         www.microsoft.com-c-3.edgekey.net
         www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net
```

C.3

1)

UDP

Wireshark capture of a DNS query packet. The packet list shows a standard query from 128.238.38.160 to 128.238.29.23. The packet details pane shows the User Datagram Protocol (UDP) source port as 3163 and destination port as 53. The Domain Name System (query) section is expanded.

Wireshark capture of a DNS response packet. The packet list shows a standard query response from 128.238.29.23 to 128.238.38.160. The packet details pane shows the User Datagram Protocol (UDP) source port as 53 and destination port as 3163. The Domain Name System (response) section is expanded.

2)

Destination port for DNS query message: 53

Wireshark packet details for the DNS query message. The User Datagram Protocol (UDP) section shows the destination port as 53. The Domain Name System (query) section is expanded.

Source port of DNS response message: 53

Wireshark packet details for the DNS response message. The User Datagram Protocol (UDP) section shows the source port as 53. The Domain Name System (response) section is expanded.

3) To IP address 128.238.29.23

The image shows a Wireshark capture of a DNS transaction. The packet list pane shows two packets:

No.	Time	Source	Destination	Protocol	Length	Info
8	3.075845	128.238.38.160	128.238.29.23	DNS	72	Standard query 0x006e A www.ietf.org
9	3.076689	128.238.29.23	128.238.38.160	DNS	104	Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51

4) It's a type A standard query and it does not contain any answers.

The image shows the details pane for a DNS query packet. The tree view is expanded to show the following information:

- Domain Name System (query)
 - Transaction ID: 0x006e
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
- Queries
 - www.ietf.org: type A, class IN

5) There are 2 answers provided. The answers contain the name of the host, the type of address, class, the time to live, the data length and the IP address.

The image shows the details pane for a DNS response packet. The tree view is expanded to show the following information:

- Domain Name System (response)
 - Transaction ID: 0x006e
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 2
 - Authority RRs: 0
 - Additional RRs: 0
- Answers
 - www.ietf.org: type A, class IN, addr 132.151.6.75
 - Name: www.ietf.org
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 1678
 - Data length: 4
 - Address: 132.151.6.75
 - www.ietf.org: type A, class IN, addr 65.246.255.51
 - Name: www.ietf.org
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 1678
 - Data length: 4
 - Address: 65.246.255.51

6) The first SYN packet was sent to 132.151.6.75 which corresponds to the first IP address provided in the DNS response message.

The image shows the details and packet list panes for a SYN packet. The details pane shows:

- Answers
 - www.ietf.org: type A, class IN, addr 132.151.6.75

The packet list pane shows:

No.	Time	Source	Destination	Protocol	Length	Info
10	3.078479	128.238.38.160	132.151.6.75	TCP	62	3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1

7) No

8) Destination port for the DNS query message: 53

The image shows the details pane for a User Datagram Protocol (UDP) packet. The tree view is expanded to show the following information:

- User Datagram Protocol, Src Port: 3742, Dst Port: 53
 - Source Port: 3742
 - Destination Port: 53
 - Length: 37

Source port for the DNS response message: 53

```
▼ User Datagram Protocol, Src Port: 53, Dst Port: 3742
  Source Port: 53
  Destination Port: 3742
  Length: 162
```

9) The DNS query message is sent to IP address 128.238.29.22 which is not the IP address of my default local DNS server as it can be seen in the screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
15	4.951232	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
16	4.951638	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
17	4.952571	128.238.38.160	128.238.29.22	DNS	80	Standard query 0x0002 A www.mit.edu.poly.edu
18	4.952953	128.238.29.22	128.238.38.160	DNS	139	Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
19	4.953172	128.238.38.160	128.238.29.22	DNS	71	Standard query 0x0003 A www.mit.edu
20	4.969929	128.238.29.22	128.238.38.160	DNS	196	Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu ...

```
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Wireless-AC 9462
Physical Address. . . . . : DC-71-96-0A-0D-20
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:e68:5401:64bf:79f8:65f6:f454:4e4d(Preferred)
Temporary IPv6 Address. . . . . : 2001:e68:5401:64bf:1971:1f5e:825:d0de(Preferred)
Link-local IPv6 Address . . . . . : fe80::79f8:65f6:f454:4e4d%17(Preferred)
IPv4 Address. . . . . : 192.168.0.192(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, 16 November, 2020 9:28:57 PM
Lease Expires . . . . . : Tuesday, 17 November, 2020 3:16:11 AM
Default Gateway . . . . . : fe80::36e8:94ff:fe8e:fa14%17
192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 299659670
DHCPv6 Client DUID . . . . . : 00-01-00-01-26-D2-B1-22-DC-71-96-0A-0D-20
DNS Servers . . . . . : 2001:e68::b:68
2001:e68::b:69
192.168.0.1
```

10) It's a type A standard query and it does not contain any answers.

```
▼ Domain Name System (query)
  Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
  > www.mit.edu: type A, class IN
```

11) There are 1 answer provided. The answer contain the name of the host, the type of address, class, the time to live, the data length and the IP address.

```
▼ Domain Name System (response)
  Transaction ID: 0x0003
  > Flags: 0x8500 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 3
  Additional RRs: 3
  > Queries
  ▼ Answers
  ▼ www.mit.edu: type A, class IN, addr 18.7.22.83
    Name: www.mit.edu
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 60
    Data length: 4
    Address: 18.7.22.83
```

