SECR1213 NETWORK COMMUNICATION

Lab 1:
Packet Analysis at Application Layer Using Wireshark

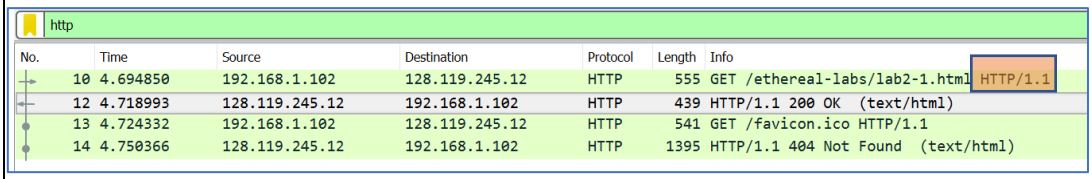
Name	:	NUR ALEEYA SYAKILA BINTI MUHAMAD SUBIAN
Matric No.	:	A19EC0127
Name	:	NURUL ALIS ALIA BINTI MOHAMAD ZAMRI
Matric No.	:	A19EC0141
Section/Group	:	01-06B

Marks:

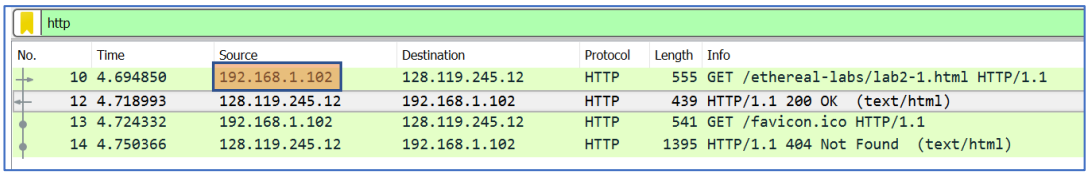
PART B: HTTP Trace

B.1

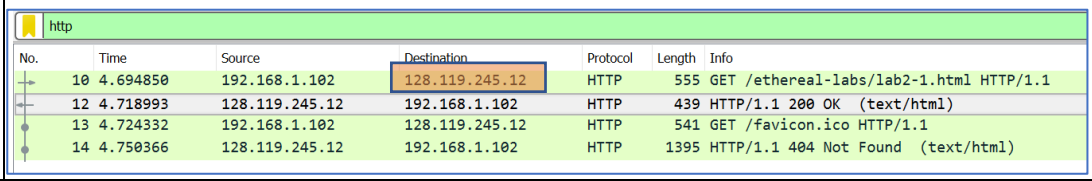
1) the version of http that the server running is version 1.1



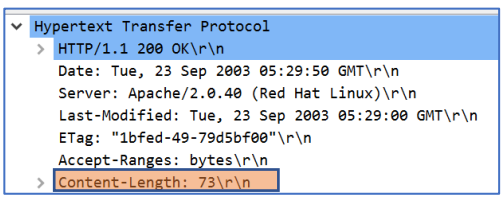
2) the ip address of the client computer is 192.168.1.102

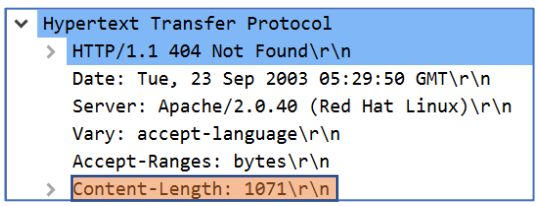


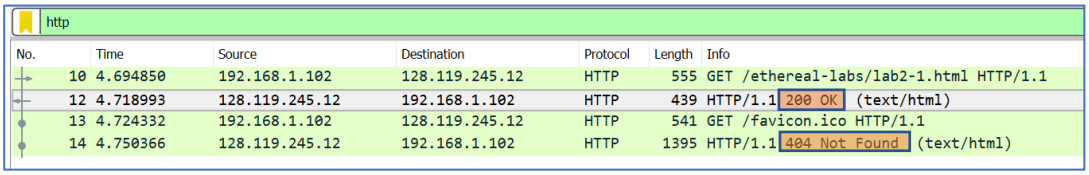
3) the ip address of the e gaia.cs.umass.edu server is 128.119.245.12

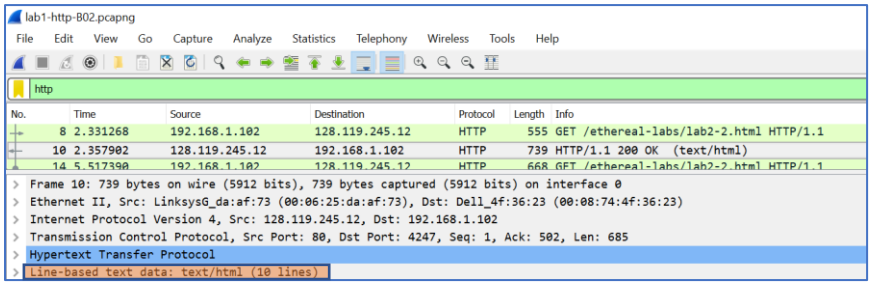
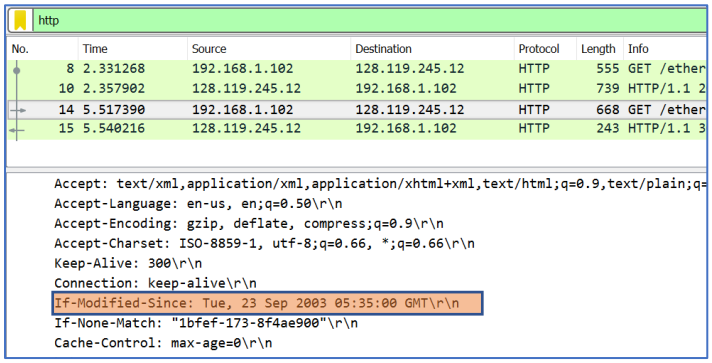
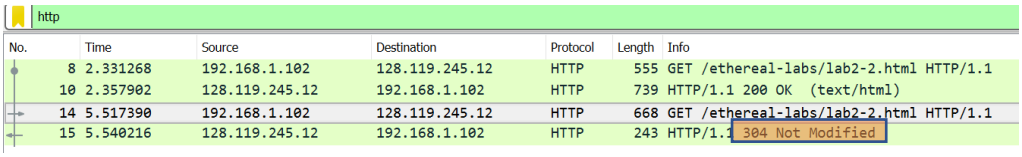


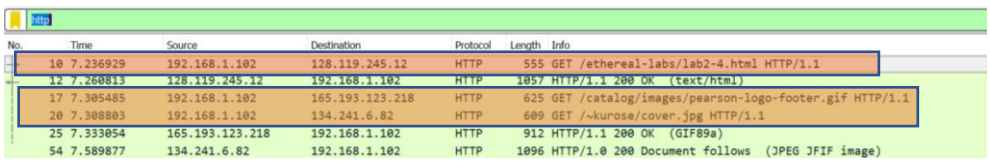
4) 73 bytes and 1071 bytes

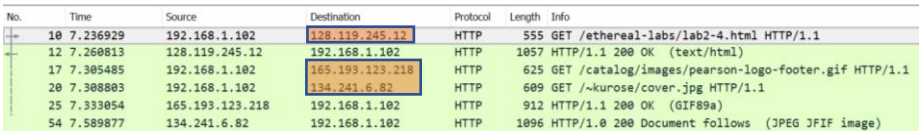
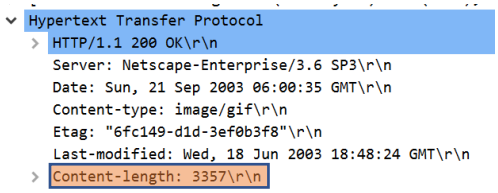
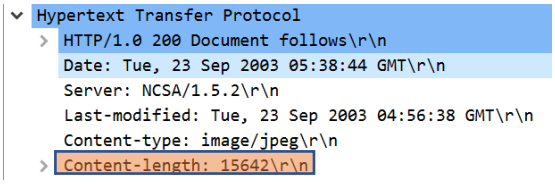


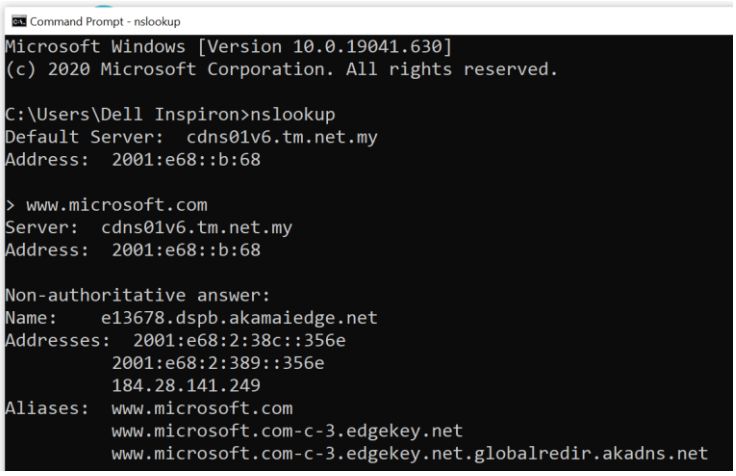


	5)	the status code returned is 200 OK and 404 Not Found  http No. Time Source Destination Protocol Length Info 10 4.694850 192.168.1.102 128.119.245.12 HTTP 555 GET /ethereal-labs/lab2-1.html HTTP/1.1 12 4.718993 128.119.245.12 192.168.1.102 HTTP 439 HTTP/1.1 200 OK (text/html) 13 4.724332 192.168.1.102 128.119.245.12 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.  lab1-http-B02.pcapng File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help http No. Time Source Destination Protocol Length Info 8 2.331268 192.168.1.102 128.119.245.12 HTTP 555 GET /ethereal-labs/lab2-2.html HTTP/1.1 10 2.357902 128.119.245.12 192.168.1.102 HTTP 739 HTTP/1.1 200 OK (text/html) Frame 10: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits) on interface 0 Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102 Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 1, Ack: 502, Len: 685 Hypertext Transfer Protocol Line-based text data: text/html (10 lines)
	3)	Yes, what follows “IF-MODIFIED-SINCE” is Tue, 23 Sep 2003 05:35:00 GMT  http No. Time Source Destination Protocol Length Info 8 2.331268 192.168.1.102 128.119.245.12 HTTP 555 GET /ether 10 2.357902 128.119.245.12 192.168.1.102 HTTP 739 HTTP/1.1 2 14 5.517390 192.168.1.102 128.119.245.12 HTTP 668 GET /ether 15 5.540216 128.119.245.12 192.168.1.102 HTTP 243 HTTP/1.1 3 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q= Accept-Language: en-us, en;q=0.50\r\n Accept-Encoding: gzip, deflate, compress;q=0.9\r\n Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n Keep-Alive: 300\r\n Connection: keep-alive\r\n If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n If-None-Match: "1bfef-173-8f4ae900"\r\n Cache-Control: max-age=0\r\n
	4)	The status code is 304 Not Modified. The server did not returns 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.  http No. Time Source Destination Protocol Length Info 8 2.331268 192.168.1.102 128.119.245.12 HTTP 555 GET /ethereal-labs/lab2-2.html HTTP/1.1 10 2.357902 128.119.245.12 192.168.1.102 HTTP 739 HTTP/1.1 200 OK (text/html) 14 5.517390 192.168.1.102 128.119.245.12 HTTP 668 GET /ethereal-labs/lab2-2.html HTTP/1.1 15 5.540216 128.119.245.12 192.168.1.102 HTTP 243 HTTP/1.1 304 Not Modified

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

	2)	FIRST HTTP GET : 128.119.245.12 SECOND HTTP GET : 165.193.123.218 THIRD HTTP GET : 134.241.6.82 
	3)	3357 bytes 
	4)	15642 bytes 

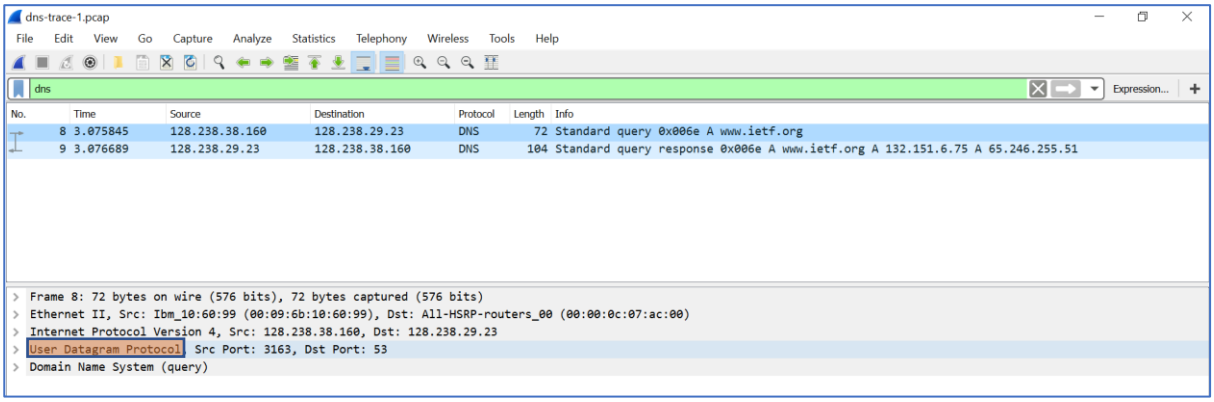
PART C: DNS Trace		
C.1	1)	The IP addresses are 2001:e68:2:38c::356e, 2001:e68:2:389::356e and 184.28.141.249. 

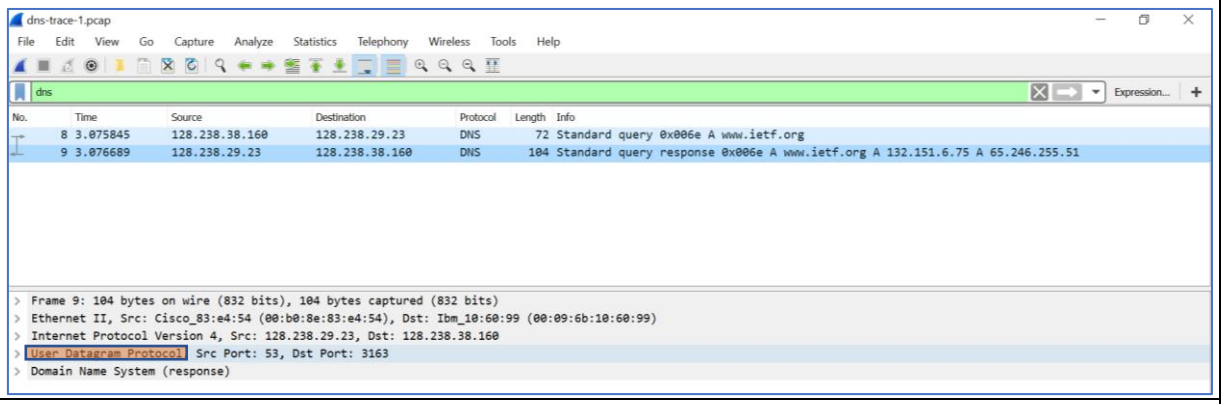
2)

```
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)

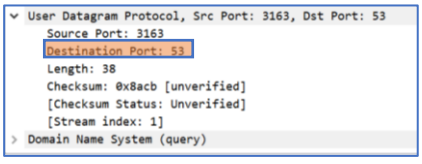
UDP



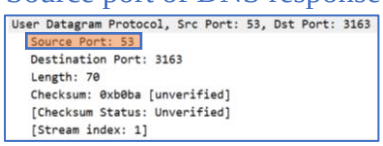


2)

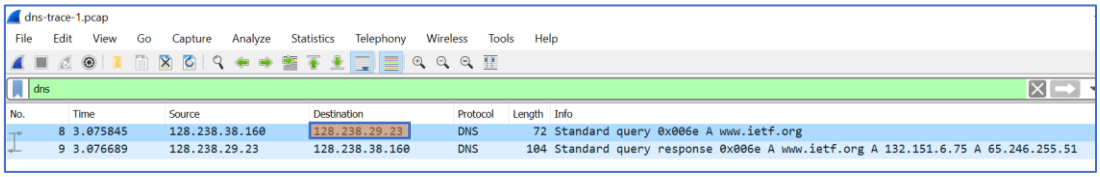
Destination port for DNS query message: 53



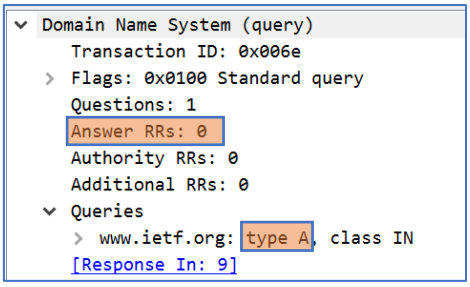
Source port of DNS response message: 53



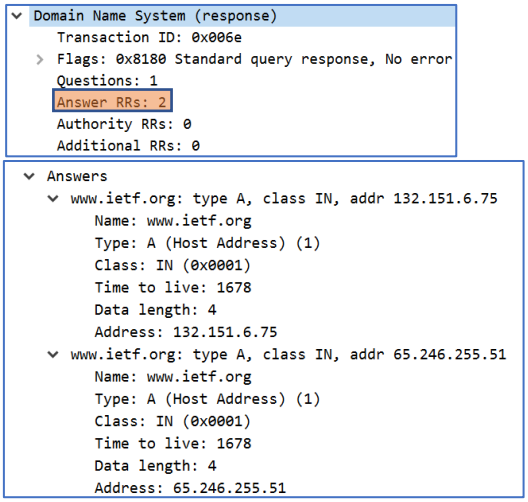
3) To IP address 128.238.29.23



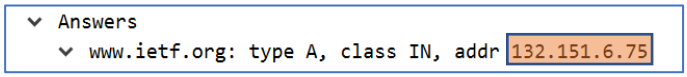
4) It's a type A standard query and it does not contain any answers.

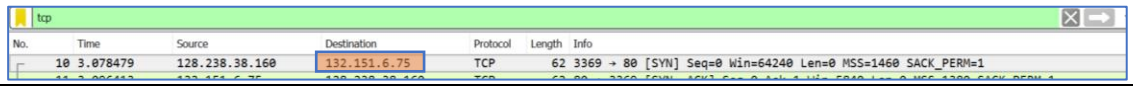


5) There are 2 answers provided. The answers contain the name of the host, the type of address, class, the time to live, the data length and the IP address.



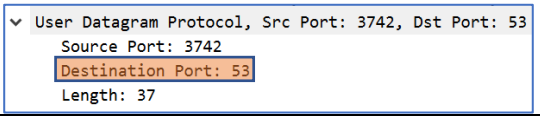
6) The first SYN packet was sent to 132.151.6.75 which corresponds to the first IP address provided in the DNS response message.



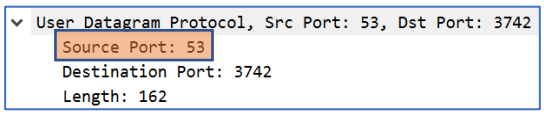


7) No

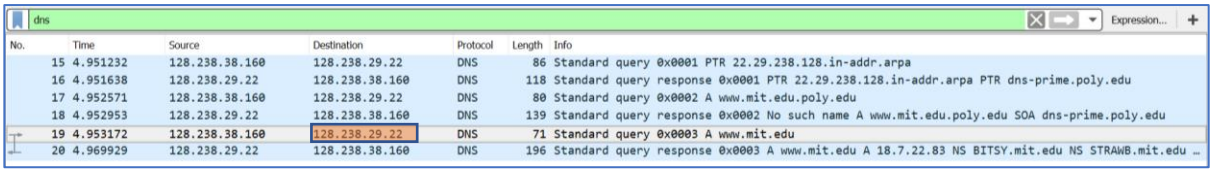
8) Destination port for the DNS query message: 53

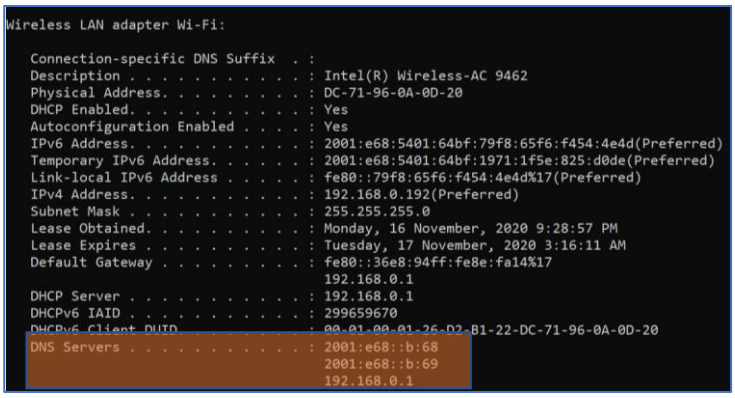


Source port for the DNS response message: 53

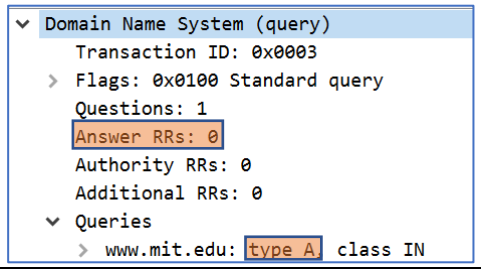


9) The DNS query message is sent to IP address 128.238.29.22 which is not the IP address of my default local DNS server as it can be seen in the screenshot below.





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



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.