CS359 - Computer Network Lab

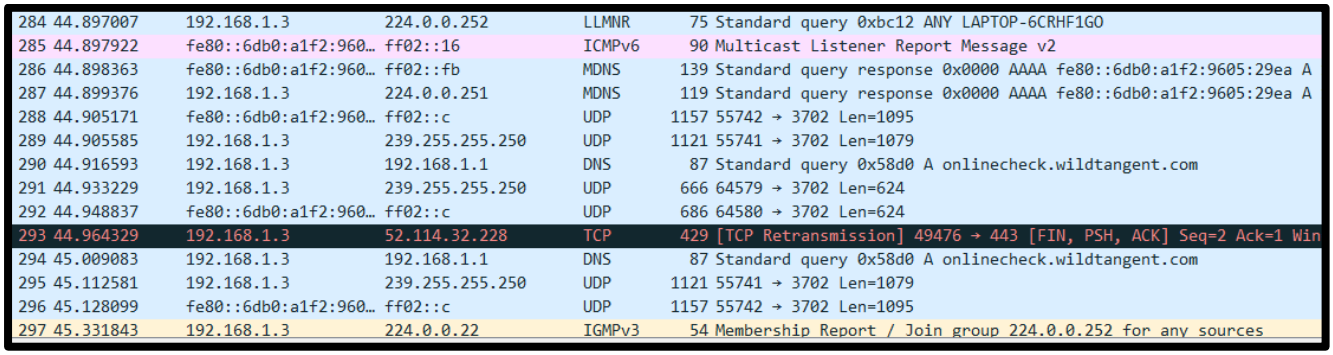
Lab 1a: Wireshark Intro

Tarusi Mittal 1901CS65

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

Ans: 3 different protocols captured are:

- DNS: DNS, or the Domain Name System, translates human readable domain names to machine readable IP addresses
- UDP: User Datagram Protocol (UDP) – a communications protocol that facilitates the exchange of messages between computing devices in a network. It's an alternative to the transmission control protocol (TCP).
- TCP: The Transmission Control Protocol (TCP) is a transport protocol that is used on top of IP to ensure reliable transmission of packets.

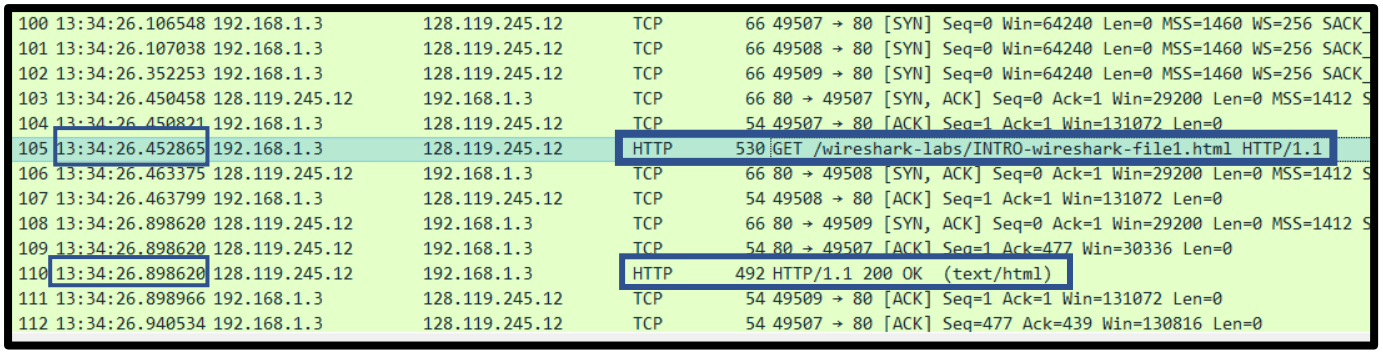


284 44.897007	192.168.1.3	224.0.0.252	LLMNR	75	Standard query 0xbc12 ANY LAPTOP-6CRHF1GO
285 44.897922	fe80::6db0:a1f2:960…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
286 44.898363	fe80::6db0:a1f2:960…	ff02::fb	MDNS	139	Standard query response 0x0000 AAAA fe80::6db0:a1f2:9605:29ea A
287 44.899376	192.168.1.3	224.0.0.251	MDNS	119	Standard query response 0x0000 AAAA fe80::6db0:a1f2:9605:29ea A
288 44.905171	fe80::6db0:a1f2:960…	ff02::c	UDP	1157	55742 → 3702 Len=1095
289 44.905585	192.168.1.3	239.255.255.250	UDP	1121	55741 → 3702 Len=1079
290 44.916593	192.168.1.3	192.168.1.1	DNS	87	Standard query 0x58d0 A onlinecheck.wildtangent.com
291 44.933229	192.168.1.3	239.255.255.250	UDP	666	64579 → 3702 Len=624
292 44.948837	fe80::6db0:a1f2:960…	ff02::c	UDP	686	64580 → 3702 Len=624
293 44.964329	192.168.1.3	52.114.32.228	TCP	429	[TCP Retransmission] 49476 → 443 [FIN, PSH, ACK] Seq=2 Ack=1 Win
294 45.009083	192.168.1.3	192.168.1.1	DNS	87	Standard query 0x58d0 A onlinecheck.wildtangent.com
295 45.112581	192.168.1.3	239.255.255.250	UDP	1121	55741 → 3702 Len=1079
296 45.128099	fe80::6db0:a1f2:960…	ff02::c	UDP	1157	55742 → 3702 Len=1095
297 45.331843	192.168.1.3	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources

Question 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*.)

Ans:

Time when HTTP Get request was sent: 13:34:26.452865
Time when HTTP OK reply was received: 13:34:26.898620
Time Taken = 0.445755 seconds



```
100 13:34:26.106548 192.168.1.3      128.119.245.12      TCP      66 49507 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_
101 13:34:26.107038 192.168.1.3      128.119.245.12      TCP      66 49508 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_
102 13:34:26.352253 192.168.1.3      128.119.245.12      TCP      66 49509 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_
103 13:34:26.450458 128.119.245.12   192.168.1.3         TCP      66 80 → 49507 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 S
104 13:34:26.450821 192.168.1.3      128.119.245.12      TCP      54 49507 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
105 13:34:26.452865 192.168.1.3      128.119.245.12      HTTP    530 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
106 13:34:26.463375 128.119.245.12   192.168.1.3         TCP      66 80 → 49508 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 S
107 13:34:26.463799 192.168.1.3      128.119.245.12      TCP      54 49508 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
108 13:34:26.898620 128.119.245.12   192.168.1.3         TCP      66 80 → 49509 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 S
109 13:34:26.898620 128.119.245.12   192.168.1.3         TCP      54 80 → 49507 [ACK] Seq=1 Ack=477 Win=30336 Len=0
110 13:34:26.898620 128.119.245.12   192.168.1.3         HTTP    492 HTTP/1.1 200 OK  (text/html)
111 13:34:26.898966 192.168.1.3      128.119.245.12      TCP      54 49509 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
112 13:34:26.940534 192.168.1.3      128.119.245.12      TCP      54 49507 → 80 [ACK] Seq=477 Ack=439 Win=130816 Len=0
```

Question 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?

Ans:

IP address of gaia.cs.umass.edu : 128.119.245.12

IP address of my computer : 192.168.1.3

Question 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.

Ans:

```
No.     Time              Source                Destination           Protocol Length Info
    105 13:34:26.452865   192.168.1.3           128.119.245.12        HTTP     530    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 105: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface \Device\NPF_{DDB895CF-AA09-4620-
A3F9-31FCA682551A}, id 0
Ethernet II, Src: IntelCor_39:95:40 (58:a0:23:39:95:40), Dst: HuaweiTe_2e:bf:ce (6c:eb:b6:2e:bf:ce)
Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49507, Dst Port: 80, Seq: 1, Ack: 1, Len: 476
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 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\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 110]
```

```
No.     Time               Source                Destination           Protocol Length Info
    110 13:34:26.898620    128.119.245.12        192.168.1.3           HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 110: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{DDB895CF-AA09-4620-
A3F9-31FCA682551A}, id 0
Ethernet II, Src: HuaweiTe_2e:bf:ce (6c:eb:b6:2e:bf:ce), Dst: IntelCor_39:95:40 (58:a0:23:39:95:40)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.3
Transmission Control Protocol, Src Port: 80, Dst Port: 49507, Seq: 1, Ack: 477, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 24 Jan 2022 08:04:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 24 Jan 2022 06:59:02 GMT\r\n
    ETag: "51-5d64e80e7f43e"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\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 1/1]
    [Time since request: 0.445755000 seconds]
    [Request in frame: 105]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X