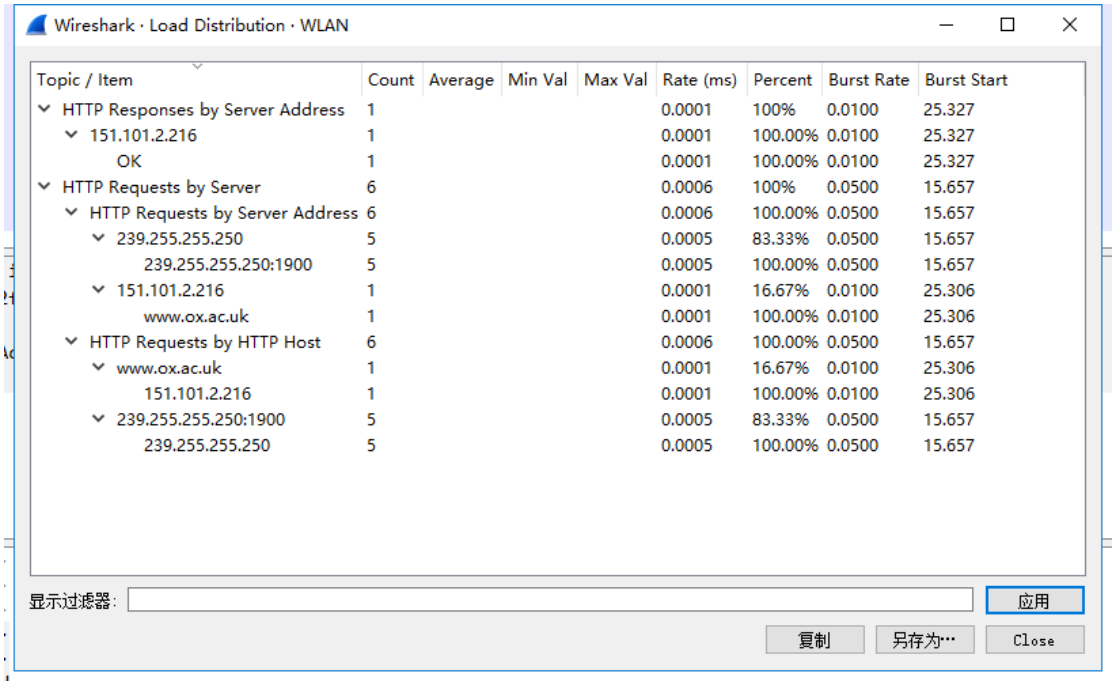
CS 352 - Summer 2021

Project 1 – Wireshark

Yuting Chen (yc1071)

Question 1



Wireshark · Load Distribution · WLAN

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Responses by Server Address	1				0.0001	100%	0.0100	25.327
151.101.2.216	1				0.0001	100.00%	0.0100	25.327
OK	1				0.0001	100.00%	0.0100	25.327
HTTP Requests by Server	6				0.0006	100%	0.0500	15.657
HTTP Requests by Server Address	6				0.0006	100.00%	0.0500	15.657
239.255.255.250	5				0.0005	83.33%	0.0500	15.657
239.255.255.250:1900	5				0.0005	100.00%	0.0500	15.657
151.101.2.216	1				0.0001	16.67%	0.0100	25.306
www.ox.ac.uk	1				0.0001	100.00%	0.0100	25.306
HTTP Requests by HTTP Host	6				0.0006	100.00%	0.0500	15.657
www.ox.ac.uk	1				0.0001	16.67%	0.0100	25.306
151.101.2.216	1				0.0001	100.00%	0.0100	25.306
239.255.255.250:1900	5				0.0005	83.33%	0.0500	15.657
239.255.255.250	5				0.0005	100.00%	0.0500	15.657

显示过滤器: 应用

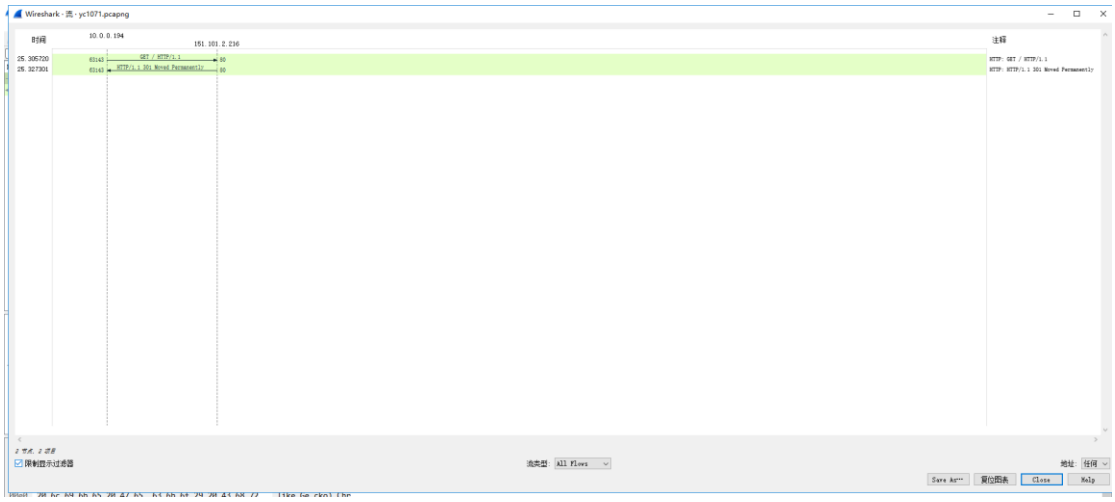
复制 另存为… Close

Question 2

2a. The Transmission Control Protocol(TCP) is used between my machine and the web server.

2b. HTTP is used to access websites, while TCP is a session establishment protocol between the client and the server. When the host requests a web page, it must ensure the reliability and integrity of the transmission, so HTTP will use TCP as its transport layer protocol.

2c.



Question 3

3a.

35	3.399442	142.250.176.195	10.0.0.194	TCP	56	443 → 60434 [ACK] Seq=3636 Ack=1597 Win=69632 Len=0
36	3.399442	142.250.176.195	10.0.0.194	TCP	56	443 → 60434 [ACK] Seq=3636 Ack=4457 Win=75264 Len=0
37	3.399442	142.250.176.195	10.0.0.194	TLSv1.3	85	Application Data
38	3.399442	142.250.176.195	10.0.0.194	TCP	56	443 → 60434 [ACK] Seq=3667 Ack=7317 Win=81152 Len=0
39	3.399442	142.250.176.195	10.0.0.194	TCP	56	443 → 60434 [ACK] Seq=3667 Ack=9360 Win=86784 Len=0
40	3.413201	142.250.176.195	10.0.0.194	TCP	56	443 → 60434 [ACK] Seq=3667 Ack=9391 Win=86784 Len=0
41	3.427587	142.250.176.195	10.0.0.194	TLSv1.3	970	Application Data
42	3.427587	142.250.176.195	10.0.0.194	TLSv1.3	1076	Application Data
43	3.427587	142.250.176.195	10.0.0.194	TLSv1.3	309	Application Data
44	3.427587	142.250.176.195	10.0.0.194	TLSv1.3	93	Application Data

3b.

Layer	Protocol
Network layer	IP
Fourth layer	TCP
Application Layer	HTTP

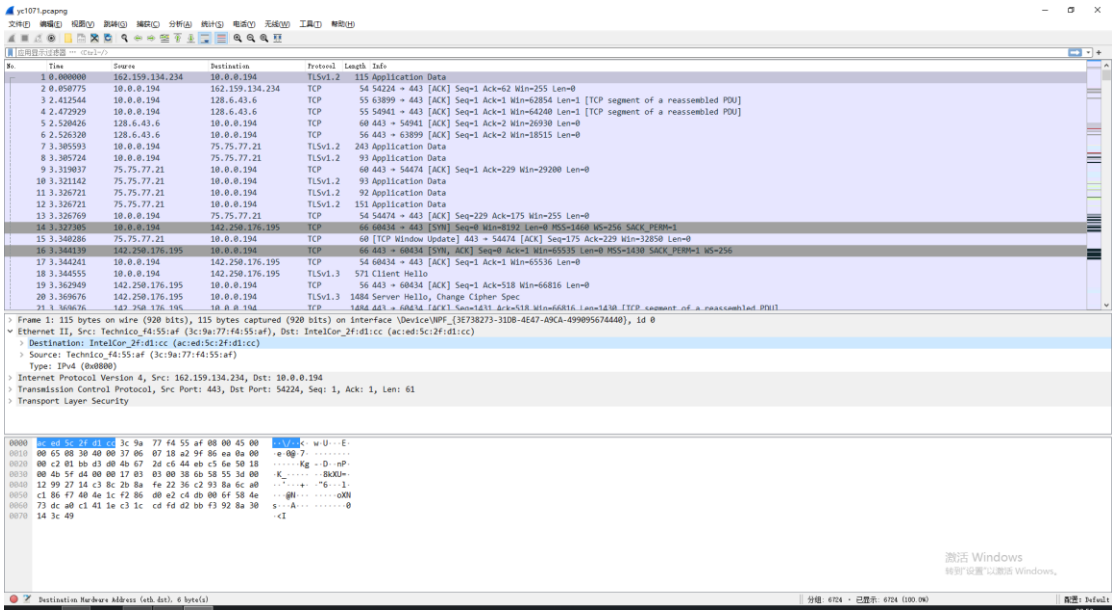
Question 4

4a.

```
Wireless LAN adapter Wi-Fi:
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . : hsd1.nj.comcast.net
   描述. . . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   物理地址. . . . . . . . . . . . . : AC-ED-5C-2F-D1-CC
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv4 地址 . . . . . . . . . . . . : 10.0.0.194(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2021年7月11日 14:19:28
   租约过期的时间  . . . . . . . . . : 2021年7月14日 17:54:46
   默认网关. . . . . . . . . . . . . : 10.0.0.1
   DHCP 服务器 . . . . . . . . . . . : 10.0.0.1
   DNS 服务器  . . . . . . . . . . . : 75.75.75.75
                                       75.75.76.76
   TCPIP 上的 NetBIOS . . . . . . . : 已启用
```

4b. Yes. I find the MAC address which is AC:ED:5C:2F:D1:CC for my machine in the trace.



4c. According to above screenshot, We can find that the 48-bit destination address is AC:ED:5C:2F:D1:CC. The address is not the ethernet address of www.ox.ac.uk.
It is address of my TP link router. A MAC address is the physical address of a device. It is not usually obtainable. A website can have mulitiple IP addresses when we hosted it at multiple locations. It can be for load balancing or redundancy. The website usually serve web pages based on the user location.

Question 5

5a.

```
C:\Users\Administrator>ping www.ox.ac.uk

正在 Ping www.ox.ac.uk [151.101.194.216] 具有 32 字节的数据:
来自 151.101.194.216 的回复: 字节=32 时间=16ms TTL=56
来自 151.101.194.216 的回复: 字节=32 时间=14ms TTL=56
来自 151.101.194.216 的回复: 字节=32 时间=14ms TTL=56
来自 151.101.194.216 的回复: 字节=32 时间=14ms TTL=56

151.101.194.216 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 14ms, 最长 = 16ms, 平均 = 14ms
Minimum        Maximum        Average
```

The time has given refers to the round-trip time taken for data to be transferred from a device to the server on the internet and back to sender.

106	21.191310	10.0.0.194	151.101.194.216	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 109)
109	21.207644	151.101.194.216	10.0.0.194	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=56 (request in 106)
116	22.195123	10.0.0.194	151.101.194.216	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 117)
117	22.209754	151.101.194.216	10.0.0.194	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=56 (request in 116)
120	23.197868	10.0.0.194	151.101.194.216	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 121)
121	23.212271	151.101.194.216	10.0.0.194	ICMP	74	Echo (ping) reply id=0x0001, seq=17/4352, ttl=56 (request in 120)
131	24.201152	10.0.0.194	151.101.194.216	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 132)
132	24.215834	151.101.194.216	10.0.0.194	ICMP	74	Echo (ping) reply id=0x0001, seq=18/4608, ttl=56 (request in 131)
153	32.868340	1.0.0.10	224.0.0.1	ICMP	56	Mobile IP Advertisement (Normal router advertisement)

5b.

```
C:\Users\Administrator>ping www.lincoln.ac.nz

正在 Ping www.lincoln.ac.nz [103.240.53.77] 具有 32 字节的数据:
来自 103.240.53.77 的回复: 字节=32 时间=400ms TTL=114
来自 103.240.53.77 的回复: 字节=32 时间=232ms TTL=114
来自 103.240.53.77 的回复: 字节=32 时间=233ms TTL=114
来自 103.240.53.77 的回复: 字节=32 时间=234ms TTL=114

103.240.53.77 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 232ms, 最长 = 400ms, 平均 = 274ms
Minimum        Maximum        Average
```

145	29.604966	10.0.0.194	103.240.53.77	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 146)
146	30.005678	103.240.53.77	10.0.0.194	ICMP	74	Echo (ping) reply id=0x0001, seq=19/4864, ttl=114 (request in 145)
147	30.611545	10.0.0.194	103.240.53.77	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 148)
148	30.843675	103.240.53.77	10.0.0.194	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=114 (request in 147)
156	31.617360	10.0.0.194	103.240.53.77	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 157)
157	31.850697	103.240.53.77	10.0.0.194	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=114 (request in 156)
163	32.623758	10.0.0.194	103.240.53.77	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (reply in 164)
164	32.858435	103.240.53.77	10.0.0.194	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=114 (request in 163)

Because the propagation delay in this case. Based on the formula of propagation delay, Propagation delay = distance between routers / propagation speed, the greater the distance, the longer the response round-trip time. I am in New jersey now. The distance between NJ and UK is much smaller than the distance between NJ and NZ, so the time in ms is greater when

compared to that in part a.