



MODULE_4 LAP 3

Amani Almutairi
IT-120B

- 1. What is the Internet address of your computer?

Source Address: 192.168.1.176

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
64	2.816549	192.168.1.176	17.253.21.203	HTTP	387	GET /ocsp03-apsrsa1
67	2.832752	17.253.21.203	192.168.1.176	OCSP	887	Response
1708	7.980483	192.168.1.176	172.217.7.227	HTTP	371	GET /gts1o1core/MFcv
1710	7.989222	172.217.7.227	192.168.1.176	OCSP	780	Response
1970	8.342046	192.168.1.176	172.217.13.227	HTTP	369	GET /gts1o1core/MFcv
1973	8.357253	172.217.13.227	192.168.1.176	OCSP	780	Response

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 355
Identification: 0x0000 (0)
> Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xbc80 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.176
Destination Address: 172.217.13.227
> Transmission Control Protocol, Src Port: 50879, Dst Port: 80, Seq: 1, Ack: 1, Len: 303
> Hypertext Transfer Protocol

0010 01 63 00 00 40 00 06 bc 80 c0 a8 01 b0 ac d9 ·c·@·@· ·····
0020 0d e3 c6 bf 00 50 22 b7 63 61 30 96 39 40 80 18 ·····P"· ca0·9@·
0030 08 0c d3 18 00 00 01 01 08 0a 2d be 16 f9 99 14 ·····
0040 32 ae 47 45 54 20 2f 67 74 73 31 6f 31 63 6f 72 2·GET /g ts1o1cor
0050 65 2f 4d 46 63 77 56 61 41 44 41 67 45 41 4d 45 e/MFcvVa ADaGEAME
0060 34 77 54 44 42 4b 4d 41 6b 47 42 53 73 4f 41 77 4wTDBKMA kGBSS0Aw

Source Address (ip.src), 4 bytes Packets: 3688 · Displayed: 6 (0.2%) · Dropped: 0 (0.0%) · Profile: Default

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

HTTP –TCP - DNS

aaa.pcapng

Apply a display filter ...<=>

No.	Time	Source	Destination	Protocol	Length	Info
418	9.538751	192.168.1.176	92.242.140.21	TCP	66	58941 → 80 [FIN, ACK] Seq=226 Ack=227
419	9.541315	192.168.1.1	192.168.1.176	DNS	84	Standard query response 0x0426 A yy
420	9.542573	192.168.1.176	92.242.140.21	TCP	78	58943 → 80 [SYN] Seq=0 Win=65535 Len=0
421	9.575543	92.242.140.21	192.168.1.176	TCP	66	80 → 58941 [ACK] Seq=223 Ack=227 Win=0
422	9.575552	92.242.140.21	192.168.1.176	TCP	74	80 → 58942 [SYN, ACK] Seq=0 Ack=1 Win=0
423	9.575554	92.242.140.21	192.168.1.176	TCP	74	80 → 58943 [SYN, ACK] Seq=0 Ack=1 Win=0
424	9.575766	192.168.1.176	92.242.140.21	TCP	66	58942 → 80 [ACK] Seq=1 Ack=1 Win=1
425	9.575766	192.168.1.176	92.242.140.21	TCP	66	58943 → 80 [ACK] Seq=1 Ack=1 Win=1
426	9.576109	192.168.1.176	92.242.140.21	HTTP	290	HEAD / HTTP/1.1
427	9.576273	192.168.1.176	92.242.140.21	HTTP	291	HEAD / HTTP/1.1

> Frame 427: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface en0, id 0

> Ethernet II, Src: Apple_6c:a6:c3 (08:f8:bc:6c:a6:c3), Dst: Arcadyan_4e:ef:3f (b8:f8:53:4e:ef:3f)

> Internet Protocol Version 4, Src: 192.168.1.176, Dst: 92.242.140.21

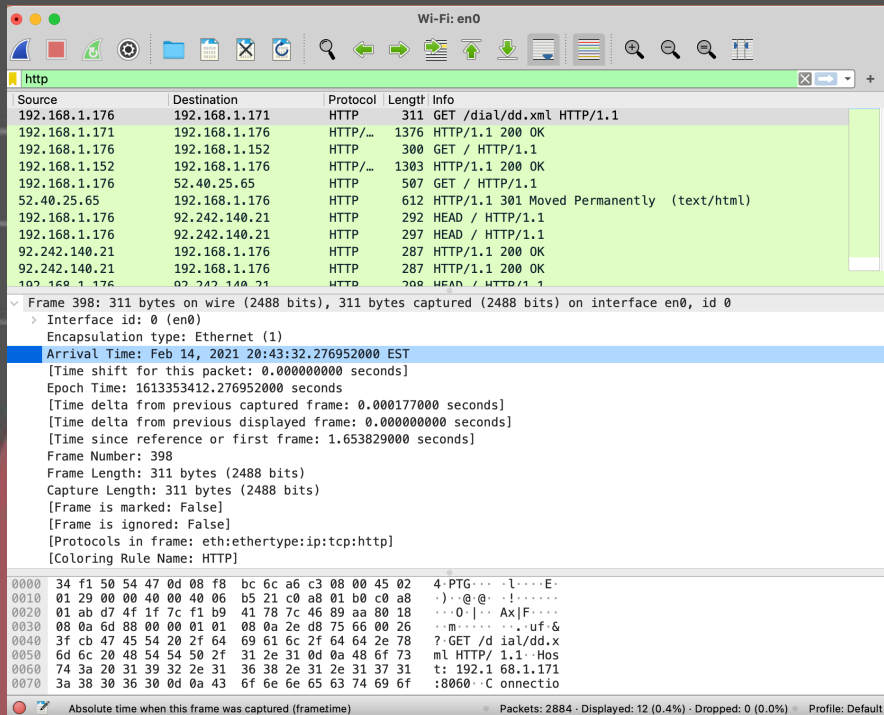
> Transmission Control Protocol, Src Port: 58943, Dst Port: 80, Seq: 1, Ack: 1, Len: 225

> Hypertext Transfer Protocol

Frame is ignored by the dissectors (frame.ignored)

Packets: 1911 · Displayed: 1911 (100.0%) · Profile: Default

```
0000 b8 f8 53 4e ef 3f 08 f8 bc 6c a6 c3 08 00 45 00 ..SN.?..l...E.
0010 01 15 00 00 40 00 40 06 8e 83 c0 a8 01 b0 5c f2 ....@.@.....\
0020 8c 15 e6 3f 00 50 fc df e1 f1 b4 83 01 72 80 18 ...?P.....
0030 08 0a b4 c6 00 00 01 01 08 0a 3c 84 f2 90 9b 01 .....<.....
0040 56 c8 48 45 41 44 20 2f 20 48 54 54 50 2f 31 2e V-HEAD / HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 79 79 69 79 6a 61 77 1..Host: yyijaw
0060 72 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b r..Conne ction: k
0070 65 65 70 2d 61 6c 69 76 65 0d 0a 55 73 65 72 2d eep-aliv e..User-
```

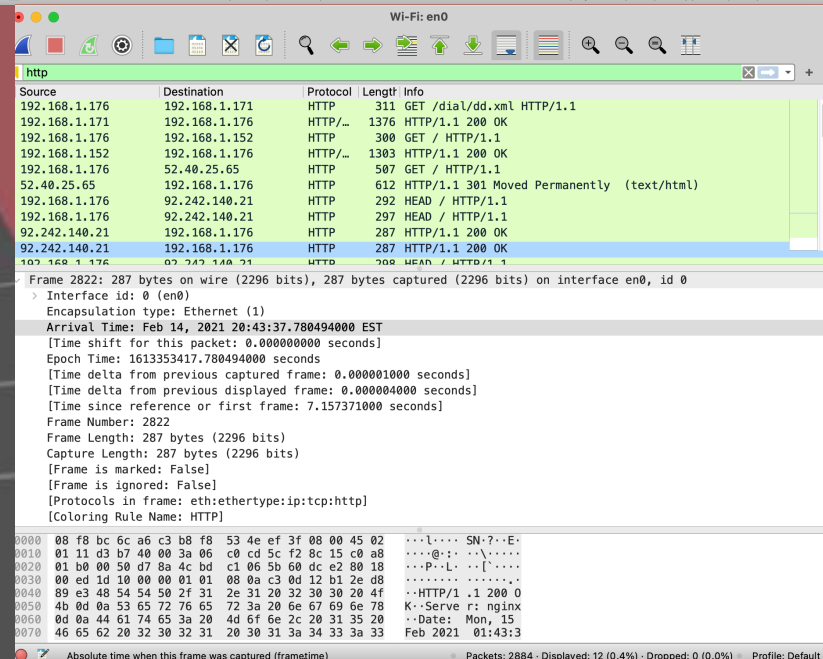


3. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

Arrival time of GET is: Feb 14, 2021 20:43:32.276952000

Arrival Time of HTTP OK is: Feb 14, 2021 20:43:33.684128000

Destination: Apple_6c:a6:c3 (08:f8:bc:6c:a6:c3)



Wi-Fi: en0

http

Source	Destination	Protocol	Length	Info
192.168.1.176	192.168.1.171	HTTP	311	GET /dial/dd.xml HTTP/1.1
192.168.1.171	192.168.1.176	HTTP/...	1376	HTTP/1.1 200 OK
192.168.1.176	192.168.1.152	HTTP	300	GET / HTTP/1.1
192.168.1.152	192.168.1.176	HTTP/...	1303	HTTP/1.1 200 OK
192.168.1.176	52.40.25.65	HTTP	507	GET / HTTP/1.1
52.40.25.65	192.168.1.176	HTTP	612	HTTP/1.1 301 Moved Permanently (text/html)
192.168.1.176	92.242.140.21	HTTP	292	HEAD / HTTP/1.1
192.168.1.176	92.242.140.21	HTTP	297	HEAD / HTTP/1.1
92.242.140.21	192.168.1.176	HTTP	287	HTTP/1.1 200 OK
92.242.140.21	192.168.1.176	HTTP	287	HTTP/1.1 200 OK
192.168.1.176	92.242.140.21	HTTP	208	HEAD / HTTP/1.1

> Frame 398: 311 bytes on wire (2488 bits), 311 bytes captured (2488 bits) on interface en0, id 0

> Ethernet II, Src: Apple_6c:a6:c3 (08:f8:bc:6c:a6:c3), Dst: HuiZhouG_54:47:0d (34:f1:50:54:47:0d)

> Internet Protocol Version 4, Src: 192.168.1.176, Dst: 192.168.1.171

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))

Total Length: 297

Identification: 0x0000 (0)

> Flags: 0x40, Don't fragment

Fragment Offset: 0

Time to Live: 64

Protocol: TCP (6)

Header Checksum: 0xb521 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.176

Destination Address: 192.168.1.171

0010 01 29 00 00 40 00 40 06 b5 21 c0 a8 01 b0 c0 a8 .) .@ .@ .!

0020 01 ab d7 4f 1f 7c f1 b9 41 78 7c 46 89 aa 80 18 . . 0 . | . . Ax | F . . .

0030 08 0a 6d 88 00 00 01 01 08 0a 2e d8 75 66 00 26 . . m u f . &

0040 3f cb 47 45 54 20 2f 64 69 61 6c 2f 64 64 2e 78 ? . GET / d i a l / d d . x

0050 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 m l H T T P / 1 . 1 . H o s

0060 74 3a 20 31 39 32 2e 31 36 38 2e 31 2e 31 37 31 t : 1 9 2 . 1 6 8 . 1 . 1 7 1

0070 3a 38 30 36 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f : 8 0 6 0 . C o n n e c t i o


0080 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n : k e e p - a l i v e . U

Source Address (in src) 4 bytes

Packets: 2884 - Displayed: 12 (0.4%) - Dropped: 0 (0.0%) - Profile: Default

4. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)?

Source Address: 192.168.1.176

- 
- 5. 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.