

ENTERPRISE INFRASTRUCTURE AND NETWORK

IT520

LAB#1

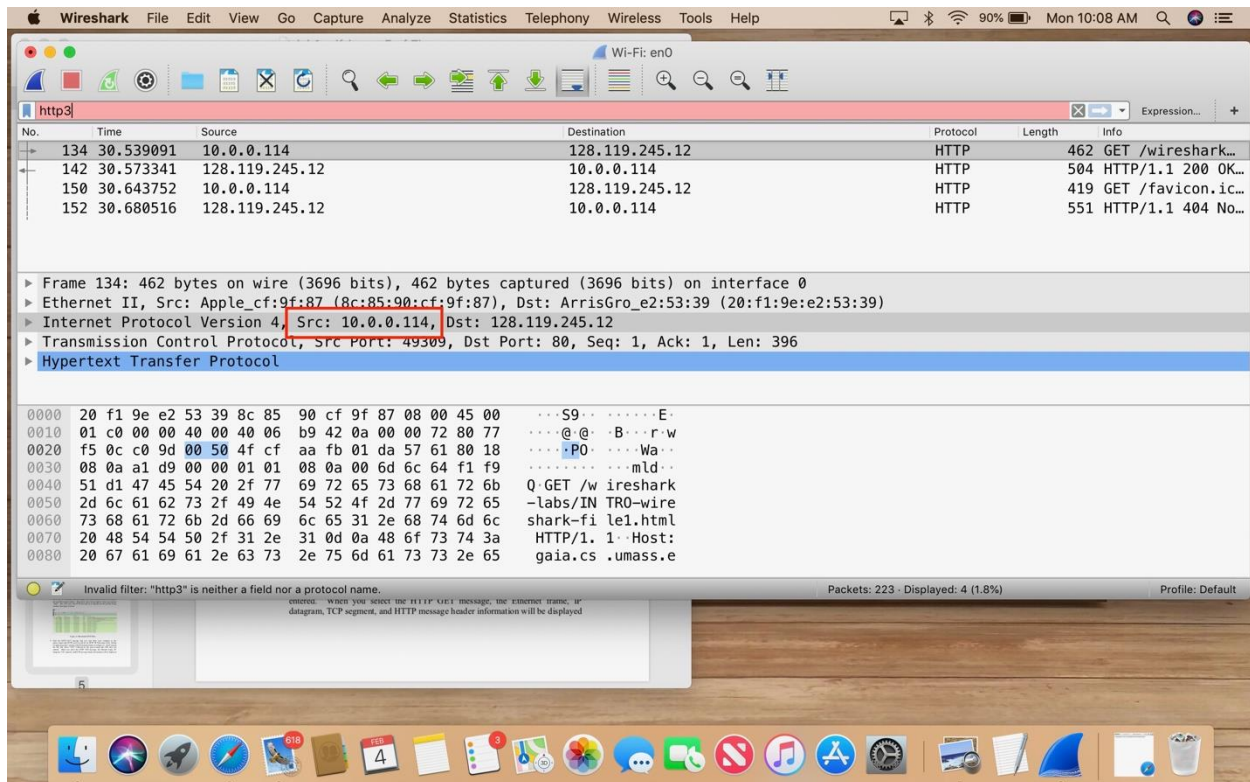
OHUOD ALTHIYABI

Due to: Feb/04/2019

Questions 1:

- What is the Internet address of your computer?

10.0.0.114



Question 2:

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

Protocols:

TCP

TLSv1.2

DNS

No.	Time	Source	Destination	Protocol	Length	Info
118	30.485321	2601:140:8100:1832:6480:1e10:d746:2a11	2620:149:a41:302::7	TLSv1.2	1204	Application Data
119	30.485412	2601:140:8100:1832:6480:1e10:d746:2a11	2620:149:a41:302::7	TLSv1.2	530	Application Data
120	30.485703	2601:140:8100:1832:6480:1e10:d746:2a11	2620:149:a41:302::7	TLSv1.2	116	Application Data
121	30.498959	2620:149:a41:302::7	2601:140:8100:1832:6480:1e10:d746:2a11	TCP	86	443 → 49307 [ACK.
122	30.498963	2620:149:a41:302::7	2601:140:8100:1832:6480:1e10:d746:2a11	TCP	86	443 → 49307 [ACK.
123	30.499159	2620:149:a41:302::7	2601:140:8100:1832:6480:1e10:d746:2a11	TLSv1.2	116	Application Data
124	30.499218	2601:140:8100:1832:6480:1e10:d746:2a11	2620:149:a41:302::7	TCP	86	49307 → 443 [ACK.
125	30.500371	2620:149:a41:305::e	2601:140:8100:1832:6480:1e10:d746:2a11	TLSv1.2	137	Change Cipher Sp.
126	30.500444	2601:140:8100:1832:6480:1e10:d746:2a11	2620:149:a41:305::e	TCP	86	49308 → 443 [ACK.
127	30.505446	2001:558:feed::1	2601:140:8100:1832:6480:1e10:d746:2a11	DNS	150	Standard query r.
128	30.507292	2001:558:feed::1	2601:140:8100:1832:6480:1e10:d746:2a11	DNS	113	Standard query r.

Frame 105: 968 bytes on wire (7744 bits), 968 bytes captured (7744 bits) on interface 0
Ethernet II, Src: ArrisGro_e2:53:39 (20:f1:9e:e2:53:39), Dst: Apple_cf:9f:87 (8c:85:90:cf:9f:87)
Internet Protocol Version 6, Src: 2620:149:a41:305::e, Dst: 2601:140:8100:1832:6480:1e10:d746:2a11
Transmission Control Protocol, Src Port: 443, Dst Port: 49308, Seq: 8569, Ack: 518, Len: 882
[3 Reassembled TCP Segments (3391 bytes): #101(1428), #104(1428), #105(535)]
Secure Sockets Layer
Secure Sockets Layer

0000 8c 85 90 cf 9f 87 20 f1 9e e2 53 39 86 dd 62 01S9..b.
0010 df a0 03 92 06 35 26 20 01 49 0a 41 03 05 00 005&..I A..
0020 00 00 00 00 00 0e 26 01 01 40 81 00 18 32 64 80&...@...2d..
0030 1e 10 d7 46 2a 11 01 bb c0 9c 79 ee 67 3a 2b adF*...y:g+..
0040 c6 e5 80 18 03 9e 36 ad 00 00 01 01 08 0a 10 036.....
0050 20 fc 00 6d 6c 00 46 92 2e 4f ca f1 87 43 c1 16 ...mL.F...0...C..
0060 95 57 2d 50 ef 89 2d 80 7a 57 ad f2 ee 5f 6b d2 W-P...zW...k..
0070 00 8d b9 14 f8 14 15 35 d9 c0 46 a3 7b 72 c8 915...F{r..
0080 bf c9 55 2b cd d0 97 3e 9c 26 64 cc df ce 83 19 ..U+...&d.....
0090 71 ca 4e e6 d4 d5 7b a9 19 cd 55 de c8 ec d2 5e q.N...{-U....^..
00a0 38 53 e5 5c 4f 8c 2d fe 50 23 36 fc 66 e6 cb 8e 8S\0...P#6.f...
00b0 a4 39 19 00 b7 95 02 39 91 0b 0e fe 38 2e d1 1d 9...9...8...
00c0 05 9a f6 4d 3e 6f 0f 07 1d af 2c 1e 8f 60 39 e2 ...M>o...,'9..

Frame (968 bytes) Reassembled TCP (3391 bytes)
Internet Protocol Version 6 (IPv6), 40 bytes
Packets: 223 · Displayed: 223 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Question3:

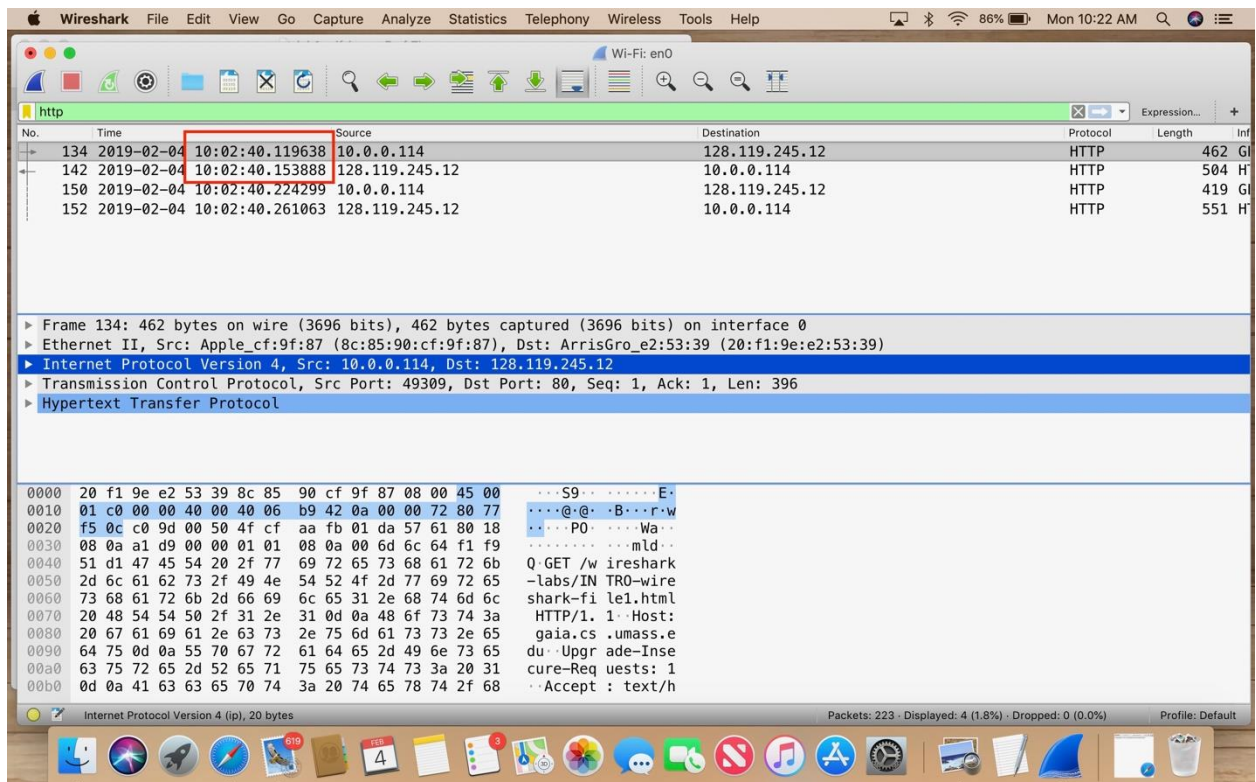
- How long did it take from when the HTTP GET message was sent until the HTTP

OK reply was received? (By default, the value of the Time column in the packet- listing 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*.)

Time:

10:02:40.119638

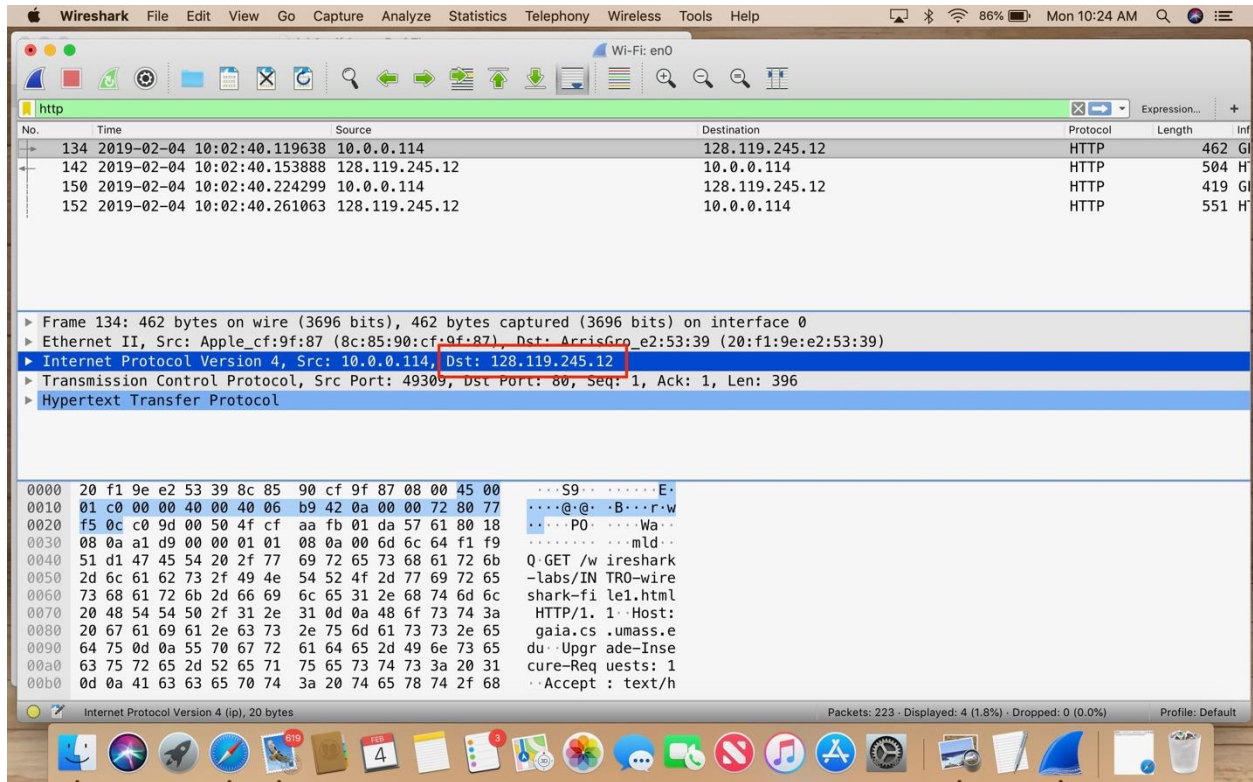
10:02:40.153888



Question4:

- What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)?

128.119.245.12



Question 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.

I attached the printed file to the lap.