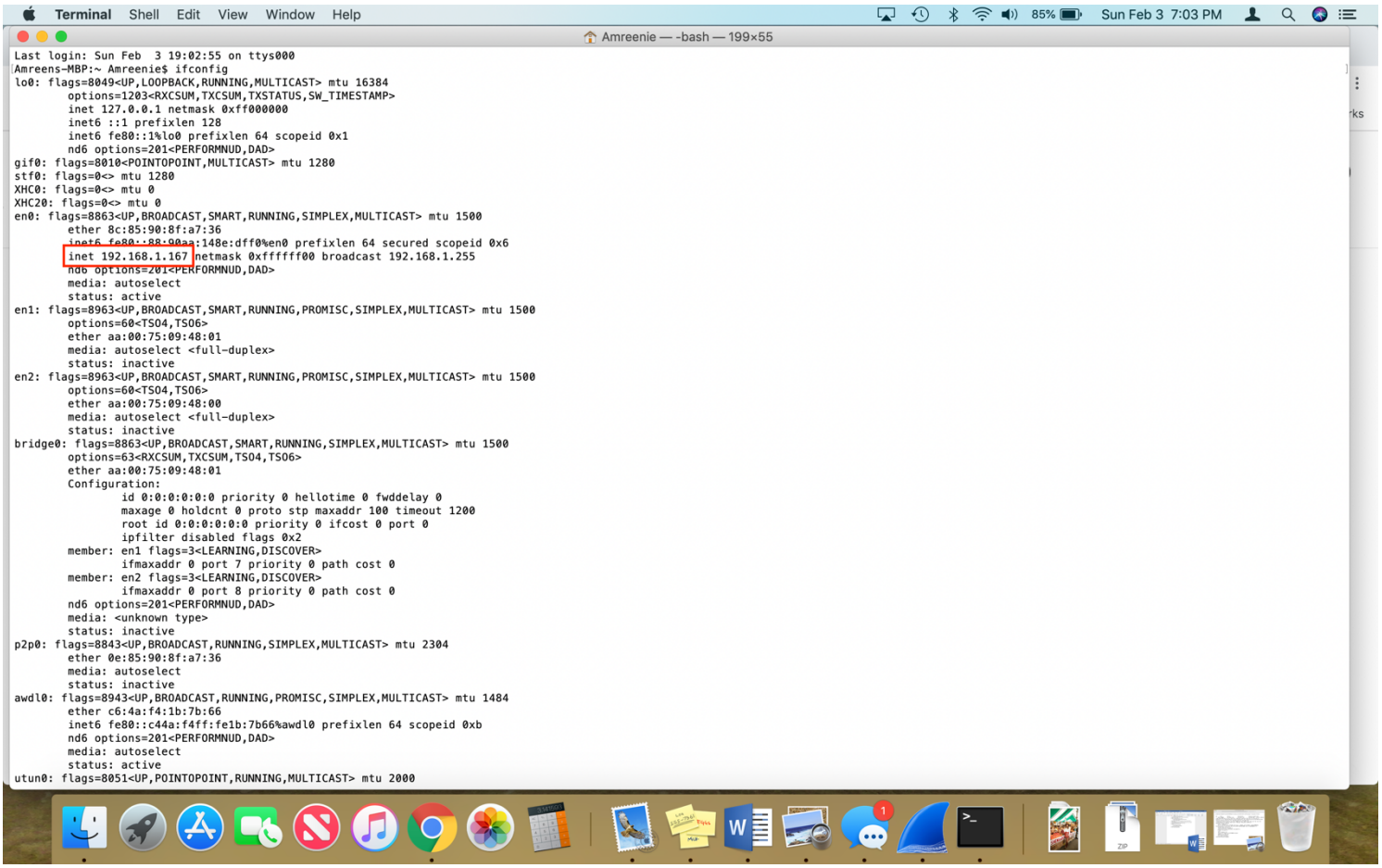
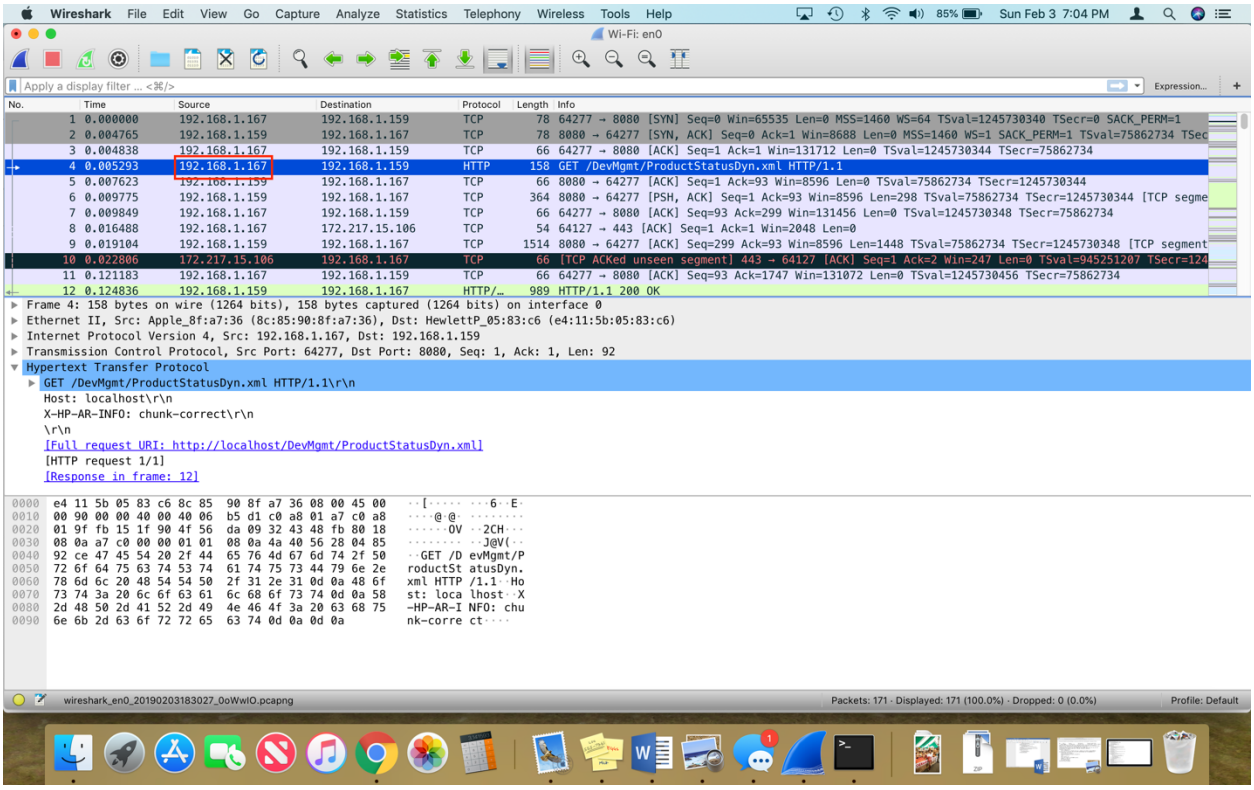
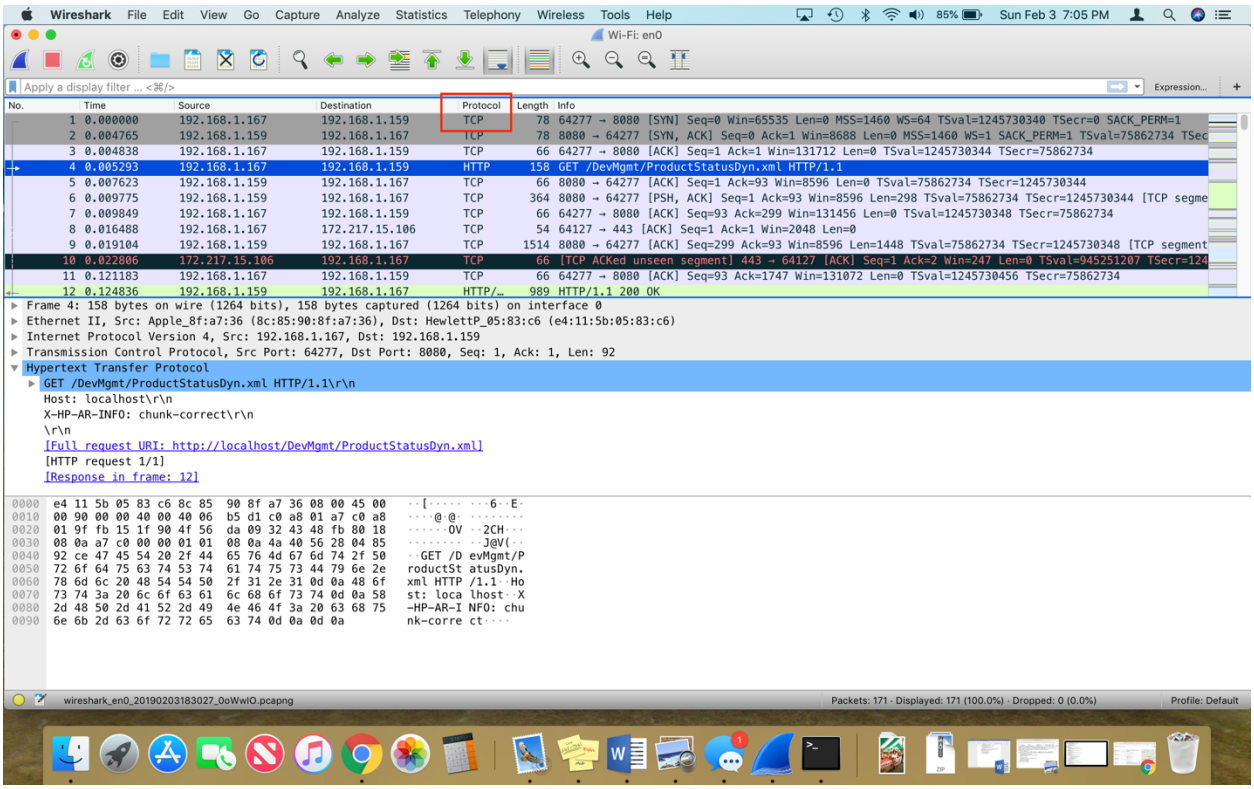

Terminal Shell Edit View Window Help
85%
Sun Feb 3 7:03 PM
Amreenie — -bash — 199×55
Last login: Sun Feb 3 19:02:55 on ttys000
Amreens-MBP:~ Amreenie$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
inet 127.0.0.1 netmask 0xff000000
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC0: flags=0<> mtu 0
XHC20: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether 8c:85:90:8f:a7:36
inet6 fe80::88:90aa:148e:dff0%en0 prefixlen 64 secured scopeid 0x6
inet 192.168.1.167 netmask 0xffffff00 broadcast 192.168.1.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
options=60<TSO4,TSO6>
ether aa:00:75:09:48:01
media: autoselect <full-duplex>
status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
options=60<TSO4,TSO6>
ether aa:00:75:09:48:00
media: autoselect <full-duplex>
status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=63<RXCSUM,TXCSUM,TSO4,TSO6>
ether aa:00:75:09:48:01
Configuration:
id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
ipfilter disabled flags 0x2
member: en1 flags=3<LEARNING,DISCOVER>
ifmaxaddr 0 port 7 priority 0 path cost 0
member: en2 flags=3<LEARNING,DISCOVER>
ifmaxaddr 0 port 8 priority 0 path cost 0
nd6 options=201<PERFORMNUD,DAD>
media: <unknown type>
status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
ether 0e:85:90:8f:a7:36
media: autoselect
status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
ether c6:4a:f4:1b:7b:66
inet6 fe80::c44a:f4ff:fe1b:7b66%awdl0 prefixlen 64 scopeid 0xb
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000

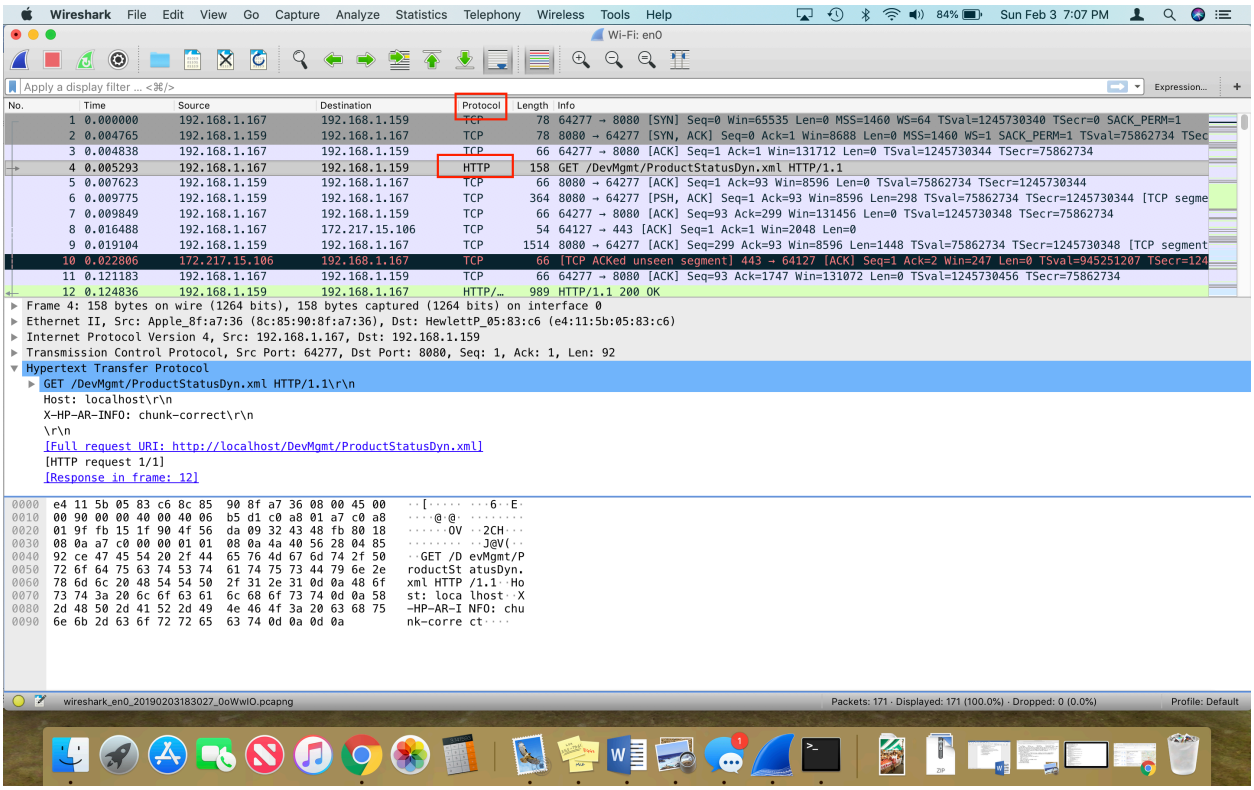
1. What is the internet address of your computer? 192.168.1.167

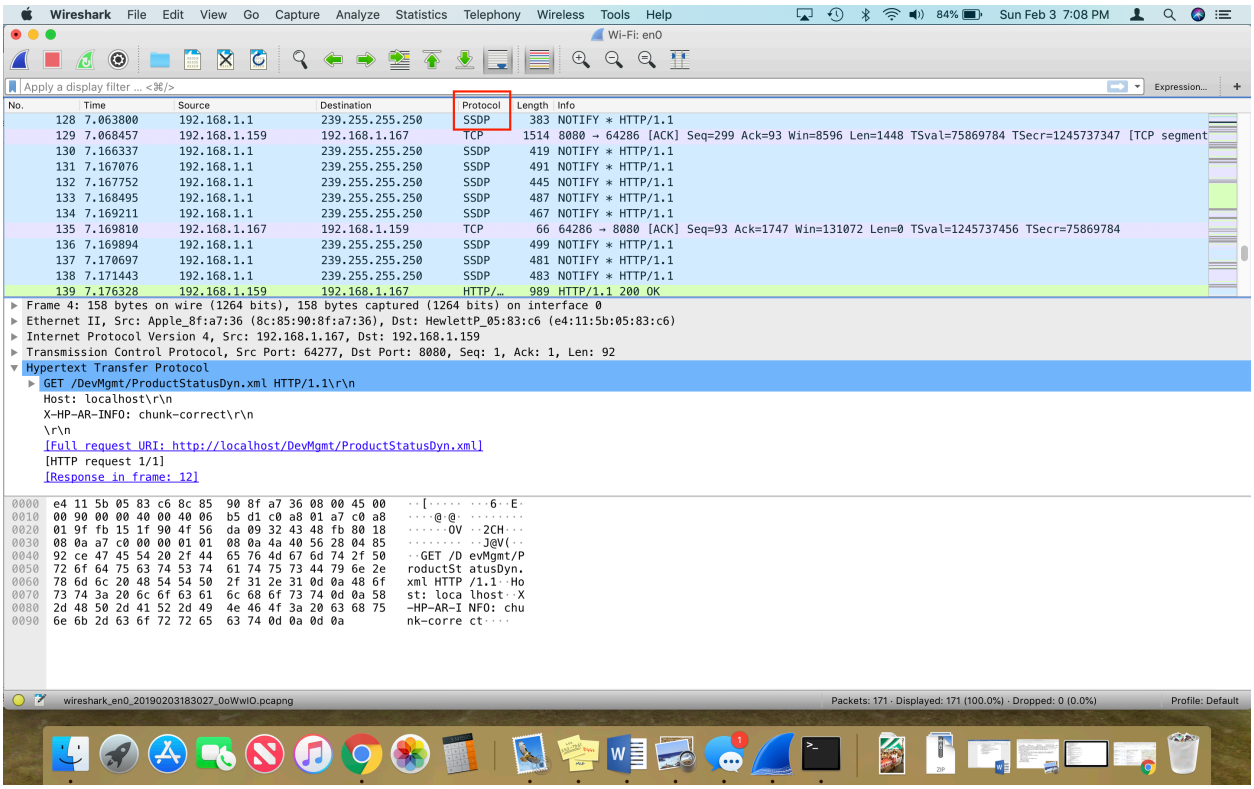


2. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window.

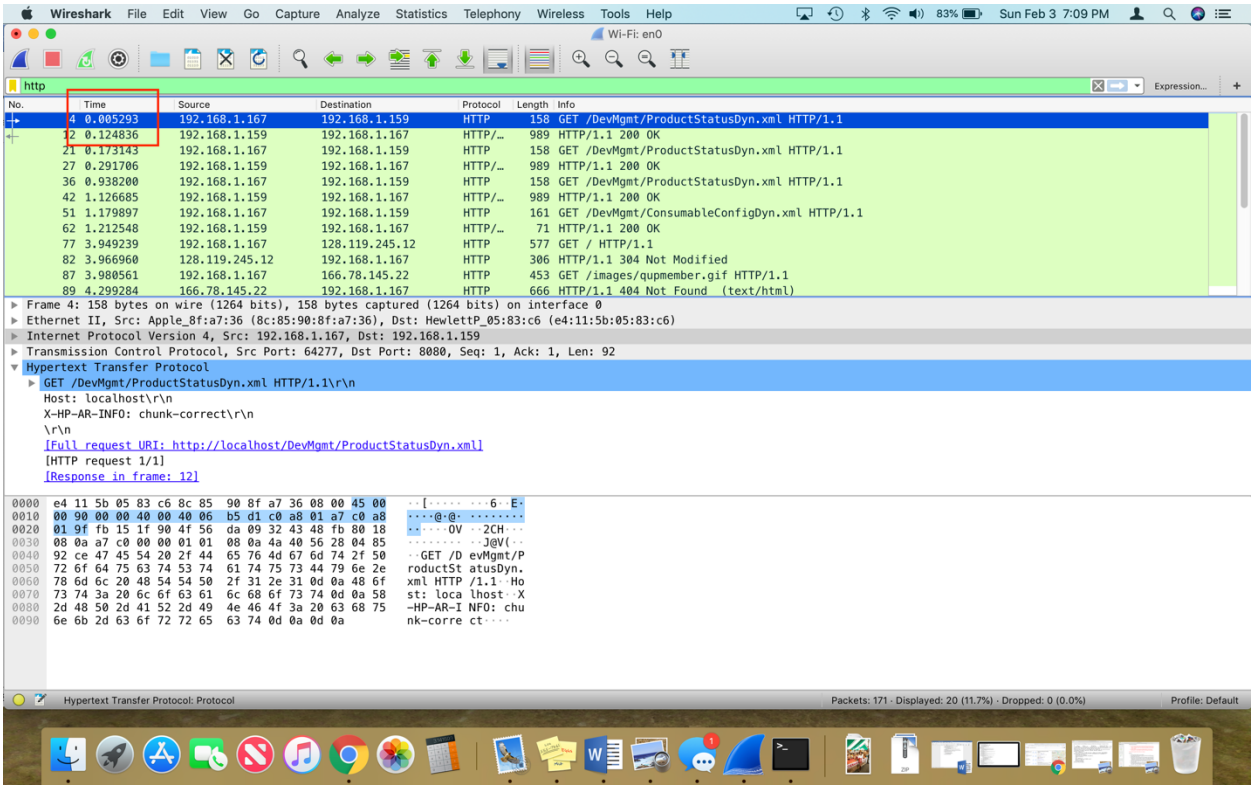
HTTP – screenshot 1
TCP – screenshot 2
SSDP – screenshot 3


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Sun Feb 3 7:05 PM
Wi-Fi: en0
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.167 192.168.1.159 TCP 78 64277 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1245730340 TSecr=0 SACK_PERM=1
2 0.004765 192.168.1.159 192.168.1.167 TCP 78 8080 → 64277 [SYN, ACK] Seq=0 Ack=1 Win=8688 Len=0 MSS=1460 WS=1 SACK_PERM=1 TSval=75862734 TSec
3 0.004838 192.168.1.167 192.168.1.159 TCP 66 64277 → 8080 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=1245730344 TSecr=75862734
4 0.005293 192.168.1.167 192.168.1.159 HTTP 158 GET /DevMgmt/ProductStatusDyn.xml HTTP/1.1
5 0.007623 192.168.1.159 192.168.1.167 TCP 66 8080 → 64277 [ACK] Seq=1 Ack=93 Win=8596 Len=0 TSval=75862734 TSecr=1245730344
6 0.009775 192.168.1.159 192.168.1.167 TCP 364 8080 → 64277 [PSH, ACK] Seq=1 Ack=93 Win=8596 Len=298 TSval=75862734 TSecr=1245730344 [TCP segme
7 0.009849 192.168.1.167 192.168.1.159 TCP 66 64277 → 8080 [ACK] Seq=93 Ack=299 Win=131456 Len=0 TSval=1245730348 TSecr=75862734
8 0.016488 192.168.1.167 172.217.15.106 TCP 54 64127 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
9 0.019104 192.168.1.159 192.168.1.167 TCP 1514 8080 → 64277 [ACK] Seq=299 Ack=93 Win=8596 Len=1448 TSval=75862734 TSecr=1245730348 [TCP segment
10 0.022806 172.217.15.106 192.168.1.167 TCP 66 [TCP ACKed unseen segment] 443 → 64127 [ACK] Seq=1 Ack=2 Win=247 Len=0 TSval=945251207 TSecr=124
11 0.121183 192.168.1.167 192.168.1.159 TCP 66 64277 → 8080 [ACK] Seq=93 Ack=1747 Win=131072 Len=0 TSval=1245730456 TSecr=75862734
12 0.124836 192.168.1.159 192.168.1.167 HTTP/… 989 HTTP/1.1 200 OK
Frame 4: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0
Ethernet II, Src: Apple_8f:a7:36 (8c:85:90:8f:a7:36), Dst: HewlettP_05:83:c6 (e4:11:5b:05:83:c6)
Internet Protocol Version 4, Src: 192.168.1.167, Dst: 192.168.1.159
Transmission Control Protocol, Src Port: 64277, Dst Port: 8080, Seq: 1, Ack: 1, Len: 92
Hypertext Transfer Protocol
GET /DevMgmt/ProductStatusDyn.xml HTTP/1.1\r\n
Host: localhost\r\n
X-HP-AR-INFO: chunk-correct\r\n
\r\n
[Full request URI: http://localhost/DevMgmt/ProductStatusDyn.xml]
[HTTP request 1/1]
[Response in frame: 12]
0000 e4 11 5b 05 83 c6 8c 85 90 8f a7 36 08 00 45 00 ··[····· ···6··E·
0010 00 90 00 00 40 00 40 06 b5 d1 c0 a8 01 a7 c0 a8 ····@·@· ········
0020 01 9f fb 15 1f 90 4f 56 da 09 32 43 48 fb 80 18 ·····OV ··2CH···
0030 08 0a a7 c0 00 00 01 01 08 0a 4a 40 56 28 04 85 ·····J@V(··
0040 92 ce 47 45 54 20 2f 44 65 76 4d 67 6d 74 2f 50 ··GET /D evMgmt/P
0050 72 6f 64 75 63 74 53 74 61 74 75 73 44 79 6e 2e roductSt atusDyn.
0060 78 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f xml HTTP /1.1··Ho
0070 73 74 3a 20 6c 6f 63 61 6c 68 6f 73 74 0d 0a 58 st: loca lhost··X
0080 2d 48 50 2d 41 52 2d 49 4e 46 4f 3a 20 63 68 75 -HP-AR-I NFO: chu
0090 6e 6b 2d 63 6f 72 72 65 63 74 0d 0a 0d 0a nk-corre ct····
wireshark_en0_20190203183027_0oWwIO.pcapng
Packets: 171 · Displayed: 171 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

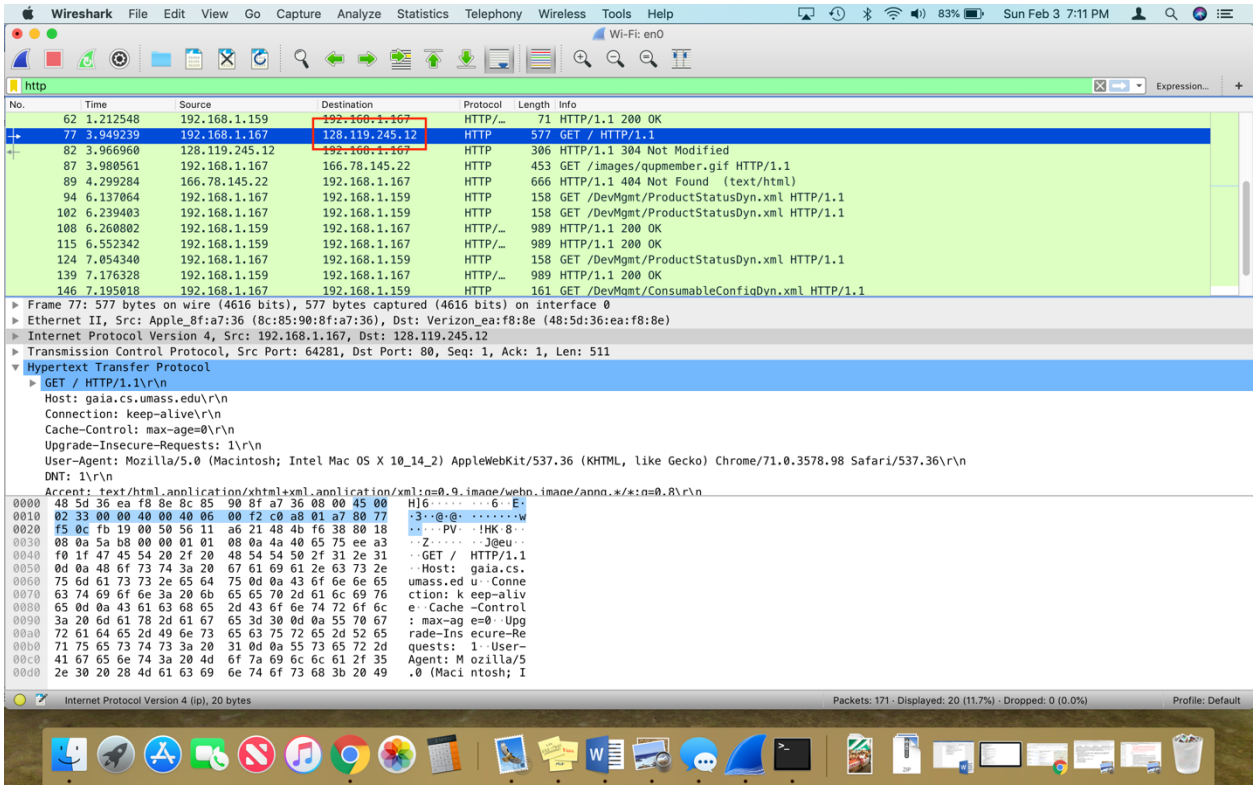

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Sun Feb 3 7:07 PM
Wi-Fi: en0
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.167 192.168.1.159 TCP 78 64277 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1245730340 TSecr=0 SACK_PERM=1
2 0.004765 192.168.1.159 192.168.1.167 TCP 78 8080 → 64277 [SYN, ACK] Seq=0 Ack=1 Win=8688 Len=0 MSS=1460 WS=1 SACK_PERM=1 TSval=75862734 TSec
3 0.004838 192.168.1.167 192.168.1.159 TCP 66 64277 → 8080 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=1245730344 TSecr=75862734
4 0.005293 192.168.1.167 192.168.1.159 HTTP 158 GET /DevMgmt/ProductStatusDyn.xml HTTP/1.1
5 0.007623 192.168.1.159 192.168.1.167 TCP 66 8080 → 64277 [ACK] Seq=1 Ack=93 Win=8596 Len=0 TSval=75862734 TSecr=1245730344
6 0.009775 192.168.1.159 192.168.1.167 TCP 364 8080 → 64277 [PSH, ACK] Seq=1 Ack=93 Win=8596 Len=298 TSval=75862734 TSecr=1245730344 [TCP segme
7 0.009849 192.168.1.167 192.168.1.159 TCP 66 64277 → 8080 [ACK] Seq=93 Ack=299 Win=131456 Len=0 TSval=1245730348 TSecr=75862734
8 0.016488 192.168.1.167 172.217.15.106 TCP 54 64127 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
9 0.019104 192.168.1.159 192.168.1.167 TCP 1514 8080 → 64277 [ACK] Seq=299 Ack=93 Win=8596 Len=1448 TSval=75862734 TSecr=1245730348 [TCP segment
10 0.022806 172.217.15.106 192.168.1.167 TCP 66 [TCP ACKed unseen segment] 443 → 64127 [ACK] Seq=1 Ack=2 Win=247 Len=0 TSval=945251207 TSecr=124
11 0.121183 192.168.1.167 192.168.1.159 TCP 66 64277 → 8080 [ACK] Seq=93 Ack=1747 Win=131072 Len=0 TSval=1245730456 TSecr=75862734
12 0.124836 192.168.1.159 192.168.1.167 HTTP/… 989 HTTP/1.1 200 OK
Frame 4: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0
Ethernet II, Src: Apple_8f:a7:36 (8c:85:90:8f:a7:36), Dst: HewlettP_05:83:c6 (e4:11:5b:05:83:c6)
Internet Protocol Version 4, Src: 192.168.1.167, Dst: 192.168.1.159
Transmission Control Protocol, Src Port: 64277, Dst Port: 8080, Seq: 1, Ack: 1, Len: 92
Hypertext Transfer Protocol
GET /DevMgmt/ProductStatusDyn.xml HTTP/1.1\r\n
Host: localhost\r\n
X-HP-AR-INFO: chunk-correct\r\n
\r\n
[Full request URI: http://localhost/DevMgmt/ProductStatusDyn.xml]
[HTTP request 1/1]
[Response in frame: 12]
0000 e4 11 5b 05 83 c6 8c 85 90 8f a7 36 08 00 45 00 ··[····· ···6··E·
0010 00 90 00 00 40 00 40 06 b5 d1 c0 a8 01 a7 c0 a8 ····@·@· ········
0020 01 9f fb 15 1f 90 4f 56 da 09 32 43 48 fb 80 18 ·····OV ··2CH···
0030 08 0a a7 c0 00 00 01 01 08 0a 4a 40 56 28 04 85 ·····J@V(··
0040 92 ce 47 45 54 20 2f 44 65 76 4d 67 6d 74 2f 50 ··GET /D evMgmt/P
0050 72 6f 64 75 63 74 53 74 61 74 75 73 44 79 6e 2e roductSt atusDyn.
0060 78 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f xml HTTP /1.1··Ho
0070 73 74 3a 20 6c 6f 63 61 6c 68 6f 73 74 0d 0a 58 st: loca lhost··X
0080 2d 48 50 2d 41 52 2d 49 4e 46 4f 3a 20 63 68 75 -HP-AR-I NFO: chu
0090 6e 6b 2d 63 6f 72 72 65 63 74 0d 0a 0d 0a nk-corre ct····
wireshark_en0_20190203183027_0oWwIO.pcapng
Packets: 171 · Displayed: 171 (100.0%) · Dropped: 0 (0.0%)
Profile: Default



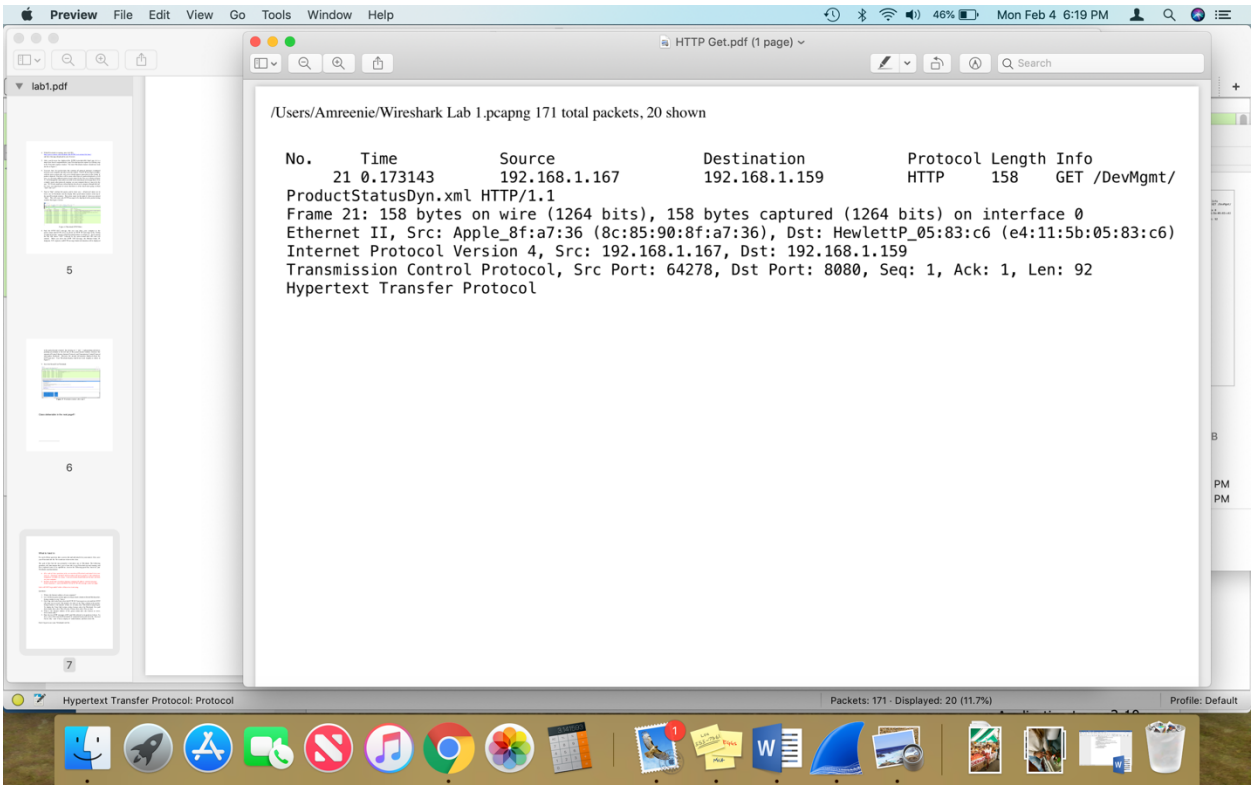
3. How long did it take from when the HTTP GET message was sent until the HTTP OK message was received? .119543 seconds

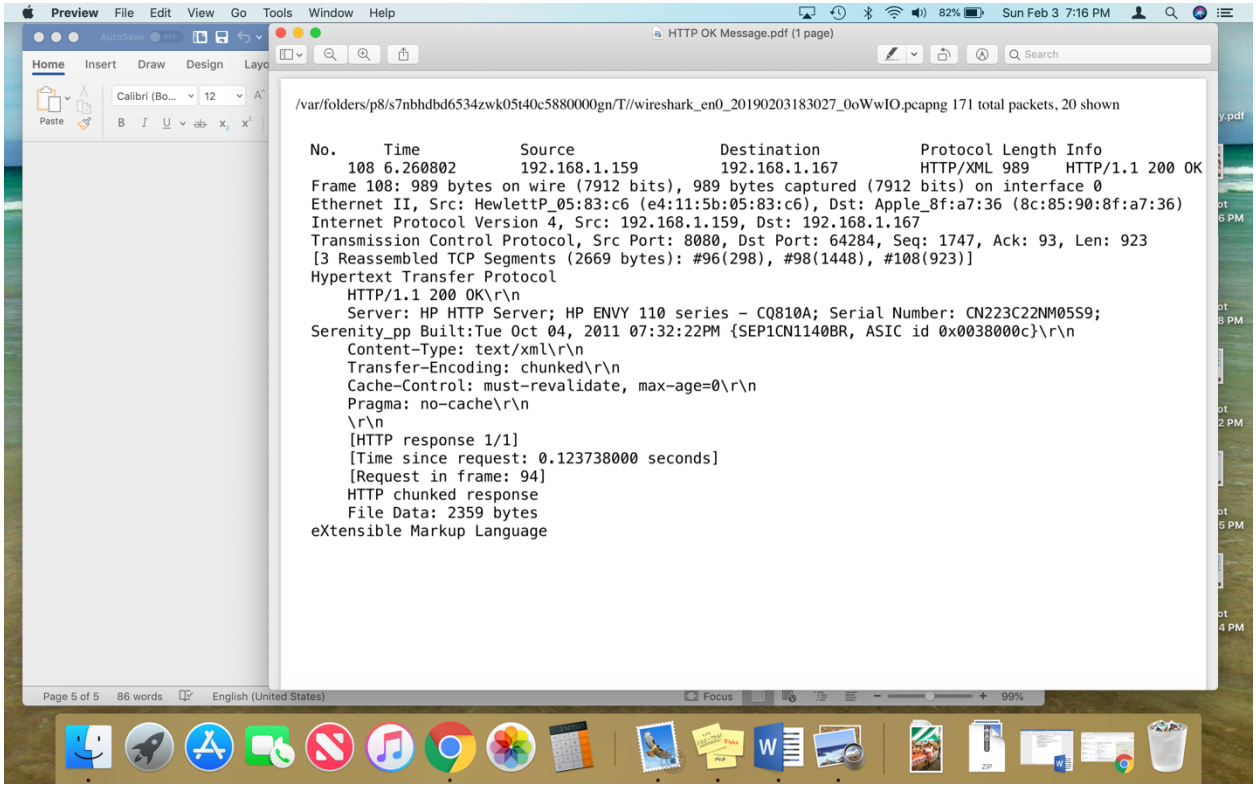


4. What is the internet address of the website: gaia.cs.umass.edu? 128.119.245.12



5. Print the HTTP messages referred to in question 2 above. Attached in a separate PDF file and screenshotted below.


Preview File Edit View Go Tools Window Help
Mon Feb 4 6:19 PM
HTTP Get.pdf (1 page)
lab1.pdf
/Users/Amreenie/Wireshark Lab 1.pcapng 171 total packets, 20 shown
No. Time Source Destination Protocol Length Info
21 0.173143 192.168.1.167 192.168.1.159 HTTP 158 GET /DevMgmt/ProductStatusDyn.xml HTTP/1.1
Frame 21: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0
Ethernet II, Src: Apple_8f:a7:36 (8c:85:90:8f:a7:36), Dst: HewlettP_05:83:c6 (e4:11:5b:05:83:c6)
Internet Protocol Version 4, Src: 192.168.1.167, Dst: 192.168.1.159
Transmission Control Protocol, Src Port: 64278, Dst Port: 8080, Seq: 1, Ack: 1, Len: 92
Hypertext Transfer Protocol
Hypertext Transfer Protocol: Protocol
Packets: 171 · Displayed: 20 (11.7%)
Profile: Default


Preview File Edit View Go Tools Window Help
Sun Feb 3 7:16 PM
HTTP OK Message.pdf (1 page)
/var/folders/p8/s7nbhdbd6534zwk05t40c5880000gn/T//wireshark_en0_20190203183027_0oWwIO.pcapng 171 total packets, 20 shown
No. Time Source Destination Protocol Length Info
108 6.260802 192.168.1.159 192.168.1.167 HTTP/XML 989 HTTP/1.1 200 OK
Frame 108: 989 bytes on wire (7912 bits), 989 bytes captured (7912 bits) on interface 0
Ethernet II, Src: HewlettP_05:83:c6 (e4:11:5b:05:83:c6), Dst: Apple_8f:a7:36 (8c:85:90:8f:a7:36)
Internet Protocol Version 4, Src: 192.168.1.159, Dst: 192.168.1.167
Transmission Control Protocol, Src Port: 8080, Dst Port: 64284, Seq: 1747, Ack: 93, Len: 923
[3 Reassembled TCP Segments (2669 bytes): #96(298), #98(1448), #108(923)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Server: HP HTTP Server; HP ENVY 110 series - CQ810A; Serial Number: CN223C22NM05S9;
Serenity_pp Built:Tue Oct 04, 2011 07:32:22PM {SEP1CN1140BR, ASIC id 0x0038000c}\r\n
Content-Type: text/xml\r\n
Transfer-Encoding: chunked\r\n
Cache-Control: must-revalidate, max-age=0\r\n
Pragma: no-cache\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.123738000 seconds]
[Request in frame: 94]
HTTP chunked response
File Data: 2359 bytes
eXtensible Markup Language
Page 5 of 5
86 words
English (United States)
Focus
99%