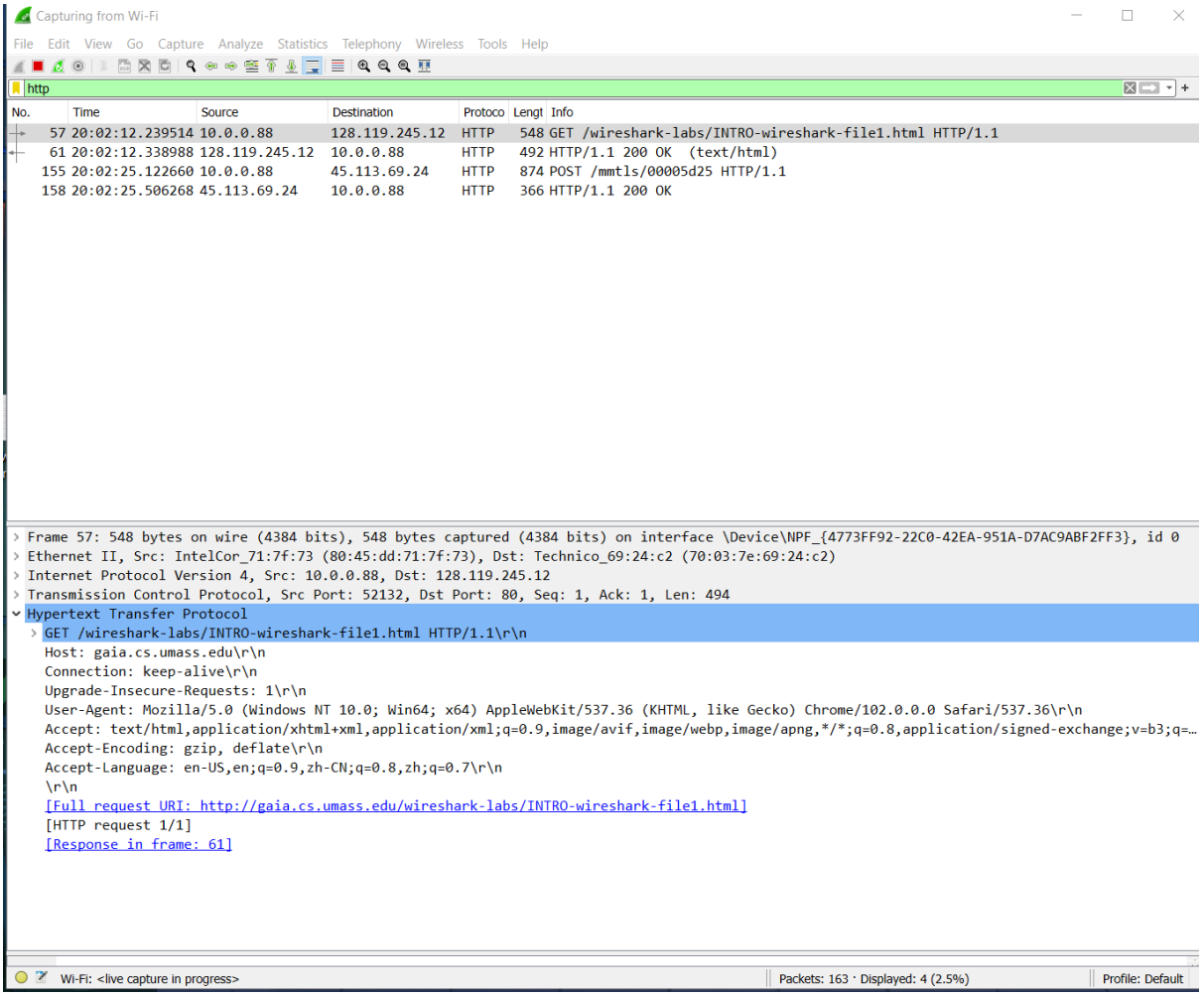
Yuhang Zhang
CS372
6/26/2022

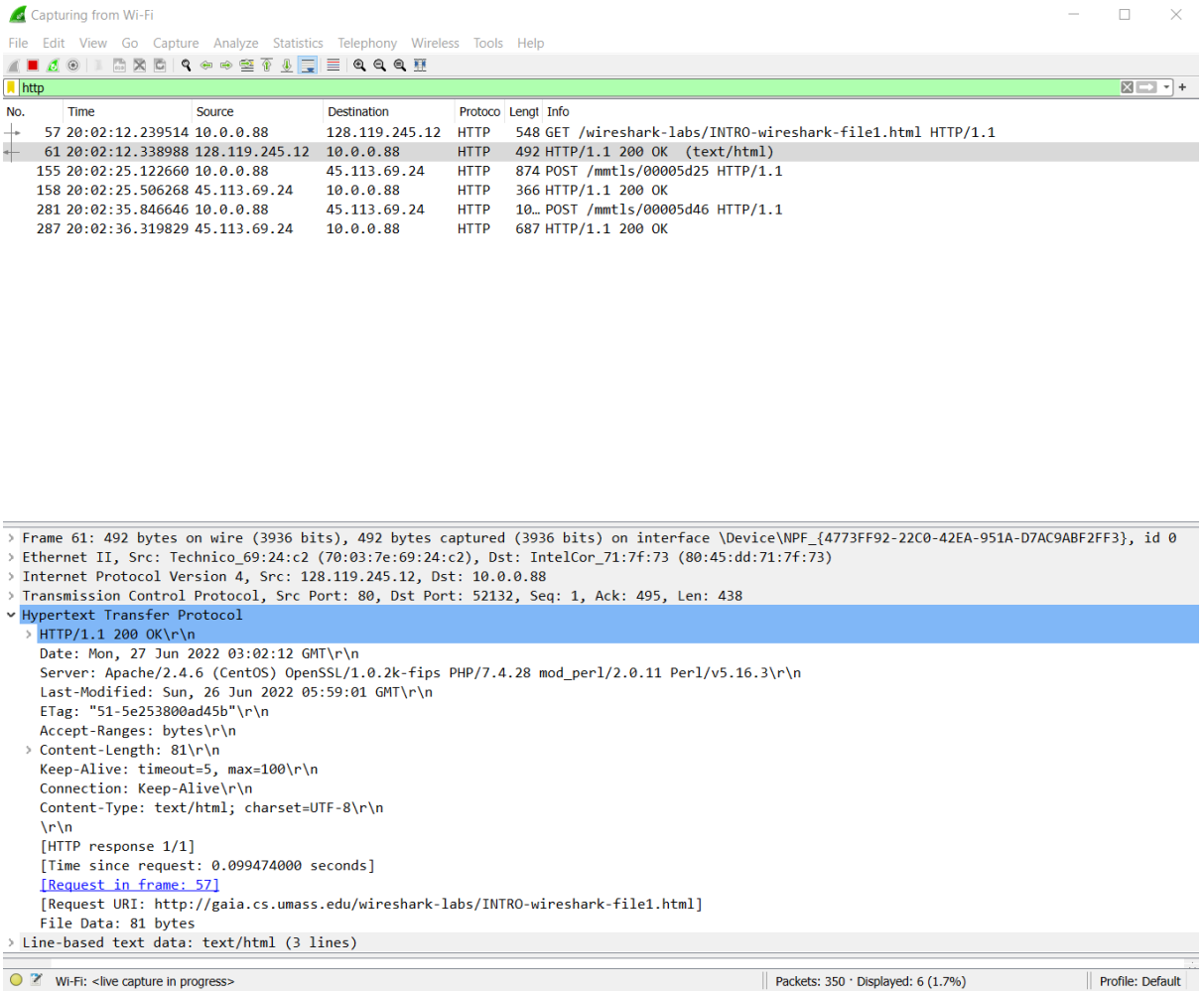
Lab 1

1. List 3 different protocols that appear in the protocol column in the unfiltered packet listing pane in step 7 above.
   HTTP
   TCP
   DNS

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 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.)
   0.099474s
3. What is the Internet Protocol (IP) address of the gaia.cs.umass.edu? What is the Internet Protocol (IP) address of your computer?
   gaia.cs.umass.edu: 128.119.245.12
   my computer: 10.0.0.88

4.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protoco Lengt Info
57 20:02:12.239514 10.0.0.88 128.119.245.12 HTTP 548 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
61 20:02:12.338988 128.119.245.12 10.0.0.88 HTTP 492 HTTP/1.1 200 OK (text/html)
155 20:02:25.122660 10.0.0.88 45.113.69.24 HTTP 874 POST /mmtls/00005d25 HTTP/1.1
158 20:02:25.506268 45.113.69.24 10.0.0.88 HTTP 366 HTTP/1.1 200 OK
Frame 57: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on interface \Device\NPF_{4773FF92-22C0-42EA-951A-D7AC9ABF2FF3}, id 0
Ethernet II, Src: IntelCor_71:7f:73 (80:45:dd:71:7f:73), Dst: Technico_69:24:c2 (70:03:7e:69:24:c2)
Internet Protocol Version 4, Src: 10.0.0.88, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52132, Dst Port: 80, Seq: 1, Ack: 1, Len: 494
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/102.0.0.0 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=…
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\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: 61]
Wi-Fi: <live capture in progress>
Packets: 163 · Displayed: 4 (2.5%)
Profile: Default


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protoco Lengt Info
57 20:02:12.239514 10.0.0.88 128.119.245.12 HTTP 548 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
61 20:02:12.338988 128.119.245.12 10.0.0.88 HTTP 492 HTTP/1.1 200 OK (text/html)
155 20:02:25.122660 10.0.0.88 45.113.69.24 HTTP 874 POST /mmtls/00005d25 HTTP/1.1
158 20:02:25.506268 45.113.69.24 10.0.0.88 HTTP 366 HTTP/1.1 200 OK
281 20:02:35.846646 10.0.0.88 45.113.69.24 HTTP 10… POST /mmtls/00005d46 HTTP/1.1
287 20:02:36.319829 45.113.69.24 10.0.0.88 HTTP 687 HTTP/1.1 200 OK
Frame 61: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{4773FF92-22C0-42EA-951A-D7AC9ABF2FF3}, id 0
Ethernet II, Src: Technico_69:24:c2 (70:03:7e:69:24:c2), Dst: IntelCor_71:7f:73 (80:45:dd:71:7f:73)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.88
Transmission Control Protocol, Src Port: 80, Dst Port: 52132, Seq: 1, Ack: 495, Len: 438
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Mon, 27 Jun 2022 03:02:12 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sun, 26 Jun 2022 05:59:01 GMT\r\n
ETag: "51-5e253800ad45b"\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: 0.099474000 seconds]
[Request in frame: 57]
[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)
Wi-Fi: <live capture in progress>
Packets: 350 · Displayed: 6 (1.7%)
Profile: Default