Youser Alalusi

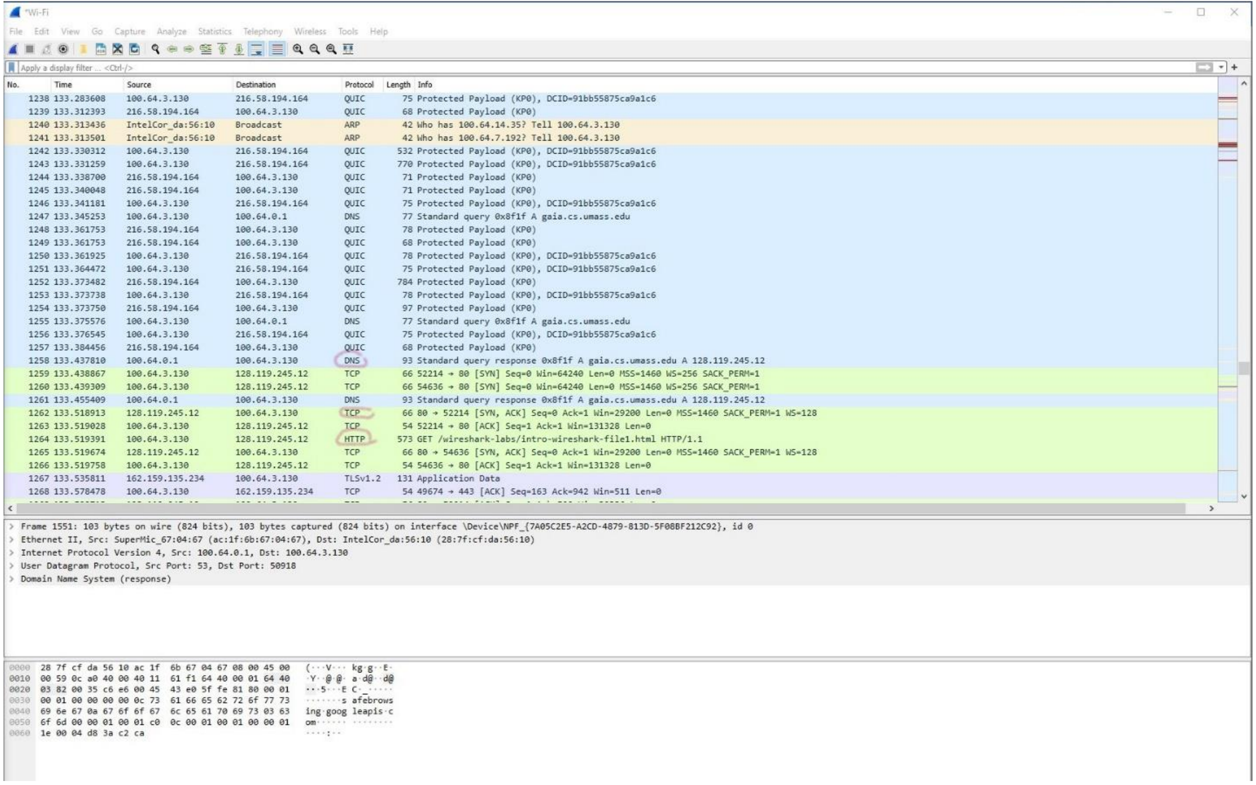
CSUS, College of Engineering and Computer Science
Department of Computer Science
CSC/CPE 138 – Computer Network and Internet

Lab 1 - Wireshark – Introduction

What to hand in

The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

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


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source            Destination       Protocol Length Info
 1238 133.283608  100.64.3.130      216.58.194.164    QUIC       75 Protected Payload (KP0), DCID=91bb55875ca9a1c6
 1239 133.312393  216.58.194.164    100.64.3.130      QUIC       68 Protected Payload (KP0)
 1240 133.313436  IntelCor_da:56:10 Broadcast         ARP        42 Who has 100.64.14.35? Tell 100.64.3.130
 1241 133.313501  IntelCor_da:56:10 Broadcast         ARP        42 Who has 100.64.7.192? Tell 100.64.3.130
 1242 133.330312  100.64.3.130      216.58.194.164    QUIC      532 Protected Payload (KP0), DCID=91bb55875ca9a1c6
 1243 133.331259  100.64.3.130      216.58.194.164    QUIC      770 Protected Payload (KP0), DCID=91bb55875ca9a1c6
 1244 133.338700  216.58.194.164    100.64.3.130      QUIC       71 Protected Payload (KP0)
 1245 133.340048  216.58.194.164    100.64.3.130      QUIC       71 Protected Payload (KP0)
 1246 133.341181  100.64.3.130      216.58.194.164    QUIC       75 Protected Payload (KP0), DCID=91bb55875ca9a1c6
 1247 133.345253  100.64.3.130      100.64.0.1        DNS        77 Standard query 0x8f1f A gaia.cs.umass.edu
 1248 133.361753  216.58.194.164    100.64.3.130      QUIC       78 Protected Payload (KP0)
 1249 133.361753  216.58.194.164    100.64.3.130      QUIC       68 Protected Payload (KP0)
 1250 133.361925  100.64.3.130      216.58.194.164    QUIC       78 Protected Payload (KP0), DCID=91bb55875ca9a1c6
 1251 133.364472  100.64.3.130      216.58.194.164    QUIC       75 Protected Payload (KP0), DCID=91bb55875ca9a1c6
 1252 133.373482  216.58.194.164    100.64.3.130      QUIC      784 Protected Payload (KP0)
 1253 133.373738  100.64.3.130      216.58.194.164    QUIC       78 Protected Payload (KP0), DCID=91bb55875ca9a1c6
 1254 133.373750  216.58.194.164    100.64.3.130      QUIC       97 Protected Payload (KP0)
 1255 133.375576  100.64.3.130      100.64.0.1        DNS        77 Standard query 0x8f1f A gaia.cs.umass.edu
 1256 133.376545  100.64.3.130      216.58.194.164    QUIC       75 Protected Payload (KP0), DCID=91bb55875ca9a1c6
 1257 133.384456  216.58.194.164    100.64.3.130      QUIC       68 Protected Payload (KP0)
 1258 133.437810  100.64.0.1        100.64.3.130      DNS        93 Standard query response 0x8f1f A gaia.cs.umass.edu A 128.119.245.12
 1259 133.438867  100.64.3.130      128.119.245.12    TCP        66 52214 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1260 133.439309  100.64.3.130      128.119.245.12    TCP        66 54636 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1261 133.455409  100.64.0.1        100.64.3.130      DNS        93 Standard query response 0x8f1f A gaia.cs.umass.edu A 128.119.245.12
 1262 133.518913  128.119.245.12    100.64.3.130      TCP        66 80 → 52214 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
 1263 133.519028  100.64.3.130      128.119.245.12    TCP        54 52214 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 1264 133.519391  100.64.3.130      128.119.245.12    HTTP      573 GET /wireshark-labs/intro-wireshark-file1.html HTTP/1.1
 1265 133.519674  128.119.245.12    100.64.3.130      TCP        66 80 → 54636 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
 1266 133.519758  100.64.3.130      128.119.245.12    TCP        54 54636 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 1267 133.535811  162.159.135.234   100.64.3.130      TLSv1.2   131 Application Data
 1268 133.578478  100.64.3.130      162.159.135.234   TCP        54 49674 → 443 [ACK] Seq=163 Ack=942 Win=511 Len=0
```

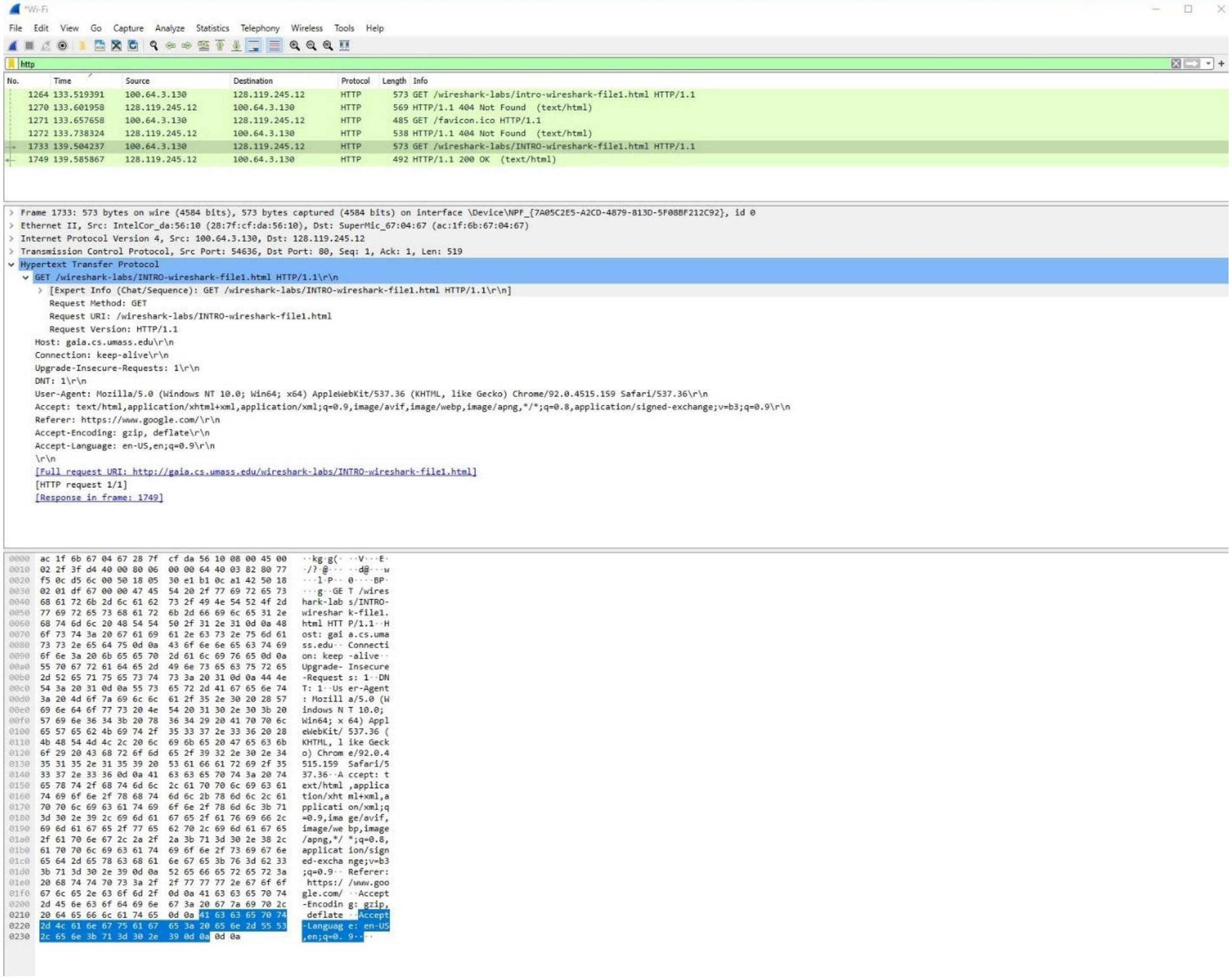
```
> Frame 1551: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{7A05C2E5-A2CD-4879-813D-5F08BF212C92}, id 0
> Ethernet II, Src: SuperMic_67:04:67 (ac:1f:6b:67:04:67), Dst: IntelCor_da:56:10 (28:7f:cf:da:56:10)
> Internet Protocol Version 4, Src: 100.64.0.1, Dst: 100.64.3.130
> User Datagram Protocol, Src Port: 53, Dst Port: 50918
> Domain Name System (response)
```

```
0000  28 7f cf da 56 10 ac 1f  6b 67 04 67 08 00 45 00   (···V··· kg·g··E·
0010  00 59 0c a0 40 00 40 11  61 f1 64 40 00 01 64 40   ·Y··@·@· a·d@··d@
0020  03 82 00 35 c6 e6 00 45  43 e0 5f fe 81 80 00 01   ···5···E C·_·····
0030  00 01 00 00 00 00 0c 73  61 66 65 62 72 6f 77 73   ·······s afebrows
0040  69 6e 67 0a 67 6f 6f 67  6c 65 61 70 69 73 03 63   ing·goog leapis·c
0050  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 01   om······ ········
0060  1e 00 04 d8 3a c2 ca                               ····:··
```

- DNS
- TCP
- HTTP

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 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*.)



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.    Time        Source          Destination     Protocol  Length Info
  1264 133.519391  100.64.3.130    128.119.245.12  HTTP      573 GET /wireshark-labs/intro-wireshark-file1.html HTTP/1.1
  1270 133.601958  128.119.245.12  100.64.3.130    HTTP      569 HTTP/1.1 404 Not Found  (text/html)
  1271 133.657658  100.64.3.130    128.119.245.12  HTTP      485 GET /favicon.ico HTTP/1.1
  1272 133.738324  128.119.245.12  100.64.3.130    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
  1733 139.504237  100.64.3.130    128.119.245.12  HTTP      573 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  1749 139.585867  128.119.245.12  100.64.3.130    HTTP      492 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 1733: 573 bytes on wire (4584 bits), 573 bytes captured (4584 bits) on interface \Device\NPF_{7A05C2E5-A2CD-4879-813D-5F08BF212C92}, id 0
> Ethernet II, Src: IntelCor_da:56:10 (28:7f:cf:da:56:10), Dst: SuperMic_67:04:67 (ac:1f:6b:67:04:67)
> Internet Protocol Version 4, Src: 100.64.3.130, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54636, Dst Port: 80, Seq: 1, Ack: 1, Len: 519
v Hypertext Transfer Protocol
  v GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/INTRO-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    DNT: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 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=0.9\r\n
    Referer: https://www.google.com/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\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: 1749]
```

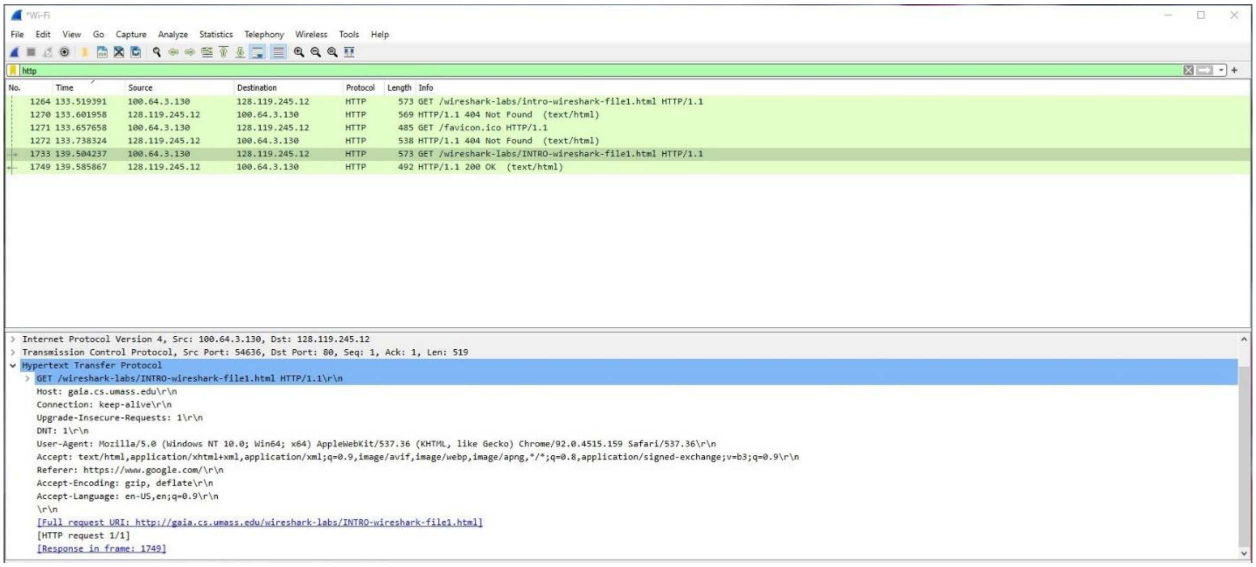
```
0000  ac 1f 6b 67 04 67 28 7f  cf da 56 10 08 00 45 00   ··kg·g(· ··V···E·
0010  02 2f 3f d4 40 00 80 06  00 00 64 40 03 82 80 77   ·/?·@··· ··d@···w
0020  f5 0c d5 6c 00 50 18 05  30 e1 b1 0c a1 42 50 18   ···l·P·· 0····BP·
0030  02 01 df 67 00 00 47 45  54 20 2f 77 69 72 65 73   ···g··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·· Connecti
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 44 4e   -Request s: 1··DN
00c0  54 3a 20 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   T: 1··Us er-Agent
00d0  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 57   : Mozill a/5.0 (W
00e0  69 6e 64 6f 77 73 20 4e  54 20 31 30 2e 30 3b 20   indows N T 10.0; 
00f0  57 69 6e 36 34 3b 20 78  36 34 29 20 41 70 70 6c   Win64; x 64) Appl
0100  65 57 65 62 4b 69 74 2f  35 33 37 2e 33 36 20 28   eWebKit/ 537.36 (
0110  4b 48 54 4d 4c 2c 20 6c  69 6b 65 20 47 65 63 6b   KHTML, l ike Geck
0120  6f 29 20 43 68 72 6f 6d  65 2f 39 32 2e 30 2e 34   o) Chrom e/92.0.4
0130  35 31 35 2e 31 35 39 20  53 61 66 61 72 69 2f 35   515.159  Safari/5
0140  33 37 2e 33 36 0d 0a 41  63 63 65 70 74 3a 20 74   37.36··A ccept: t
0150  65 78 74 2f 68 74 6d 6c  2c 61 70 70 6c 69 63 61   ext/html ,applica
0160  74 69 6f 6e 2f 78 68 74  6d 6c 2b 78 6d 6c 2c 61   tion/xht ml+xml,a
0170  70 70 6c 69 63 61 74 69  6f 6e 2f 78 6d 6c 3b 71   pplicati on/xml;q
0180  3d 30 2e 39 2c 69 6d 61  67 65 2f 61 76 69 66 2c   =0.9,ima ge/avif,
0190  69 6d 61 67 65 2f 77 65  62 70 2c 69 6d 61 67 65   image/we bp,image
01a0  2f 61 70 6e 67 2c 2a 2f  2a 3b 71 3d 30 2e 38 2c   /apng,*/ *;q=0.8,
01b0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 73 69 67 6e   applicat ion/sign
01c0  65 64 2d 65 78 63 68 61  6e 67 65 3b 76 3d 62 33   ed-excha nge;v=b3
01d0  3b 71 3d 30 2e 39 0d 0a  52 65 66 65 72 65 72 3a   ;q=0.9·· Referer:
01e0  20 68 74 74 70 73 3a 2f  2f 77 77 77 2e 67 6f 6f    https:/ /www.goo
01f0  67 6c 65 2e 63 6f 6d 2f  0d 0a 41 63 63 65 70 74   gle.com/ ··Accept
0200  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
0210  20 64 65 66 6c 61 74 65  0d 0a 41 63 63 65 70 74    deflate ··Accept
0220  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 55 53   -Languag e: en-US
0230  2c 65 6e 3b 71 3d 30 2e  39 0d 0a 0d 0a            ,en;q=0. 9····
```

- 139.585867 - 139.504237 = **0.08163 seconds** for the HTTP GET request to be received by the server and the OK message to be sent back to my computer.

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?
    - Internet address of the gaia.cs.umass.edu: 128.119.245.12
    - Internet address of my computer: 100.64.3.130
4. 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.

Youser Alalusi

Get:

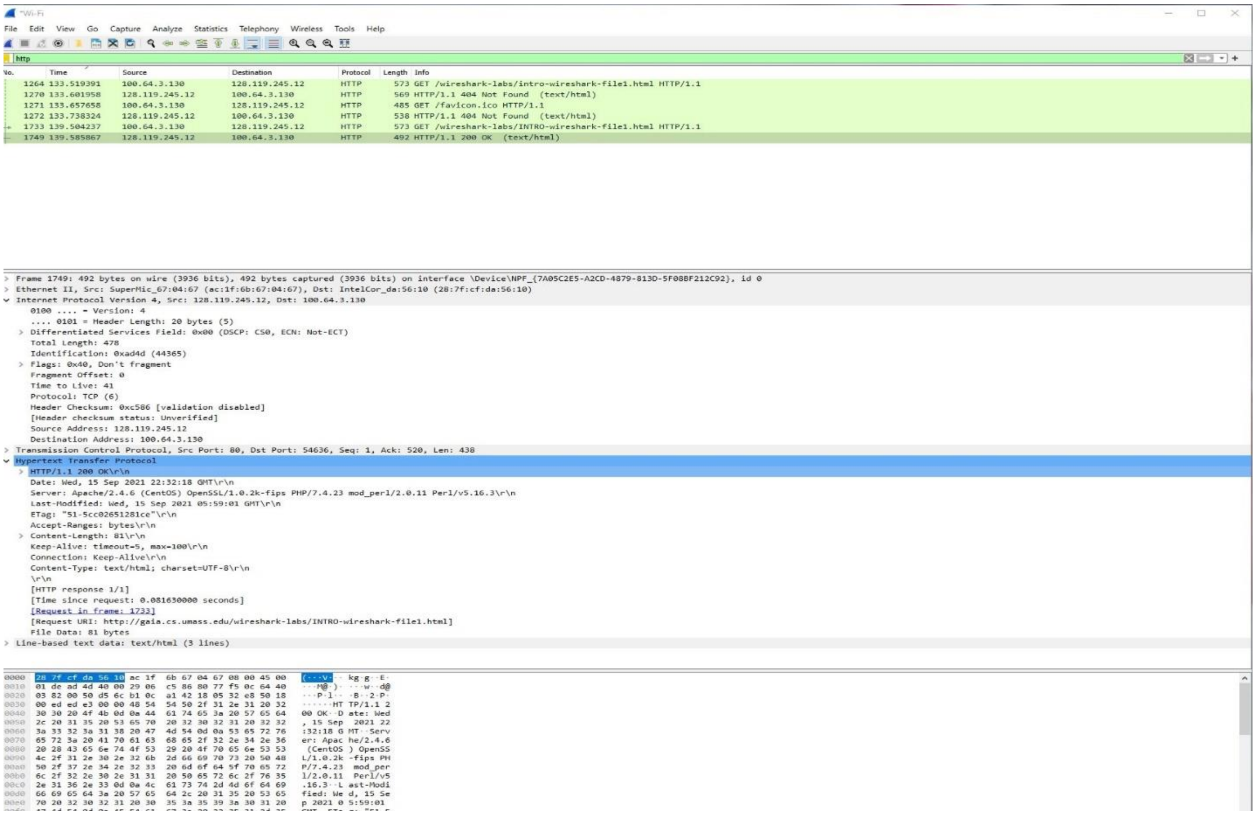

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.   Time        Source          Destination     Protocol Length Info
 1264 133.519391  100.64.3.130    128.119.245.12  HTTP     573 GET /wireshark-labs/intro-wireshark-file1.html HTTP/1.1
 1270 133.601958  128.119.245.12  100.64.3.130    HTTP     569 HTTP/1.1 404 Not Found  (text/html)
 1271 133.657658  100.64.3.130    128.119.245.12  HTTP     485 GET /favicon.ico HTTP/1.1
 1272 133.738324  128.119.245.12  100.64.3.130    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
 1733 139.504237  100.64.3.130    128.119.245.12  HTTP     573 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 1749 139.585867  128.119.245.12  100.64.3.130    HTTP     492 HTTP/1.1 200 OK  (text/html)
```

```
> Internet Protocol Version 4, Src: 100.64.3.130, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54636, Dst Port: 80, Seq: 1, Ack: 1, Len: 519
v 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
    DNT: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 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=0.9\r\n
    Referer: https://www.google.com/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\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: 1749]
```

OK:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.   Time        Source          Destination     Protocol Length Info
 1264 133.519391  100.64.3.130    128.119.245.12  HTTP     573 GET /wireshark-labs/intro-wireshark-file1.html HTTP/1.1
 1270 133.601958  128.119.245.12  100.64.3.130    HTTP     569 HTTP/1.1 404 Not Found  (text/html)
 1271 133.657658  100.64.3.130    128.119.245.12  HTTP     485 GET /favicon.ico HTTP/1.1
 1272 133.738324  128.119.245.12  100.64.3.130    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
 1733 139.504237  100.64.3.130    128.119.245.12  HTTP     573 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 1749 139.585867  128.119.245.12  100.64.3.130    HTTP     492 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 1749: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{7A05C2E5-A2CD-4879-813D-5F08BF212C92}, id 0
> Ethernet II, Src: SuperMic_67:04:67 (ac:1f:6b:67:04:67), Dst: IntelCor_da:56:10 (28:7f:cf:da:56:10)
v Internet Protocol Version 4, Src: 128.119.245.12, Dst: 100.64.3.130
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 478
    Identification: 0xad4d (44365)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 41
    Protocol: TCP (6)
    Header Checksum: 0xc586 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 100.64.3.130
> Transmission Control Protocol, Src Port: 80, Dst Port: 54636, Seq: 1, Ack: 520, Len: 438
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 15 Sep 2021 22:32:18 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.23 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 15 Sep 2021 05:59:01 GMT\r\n
    ETag: "51-5cc02651281ce"\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: 0.081630000 seconds]
    [Request in frame: 1733]
    [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)
```

```
0000  28 7f cf da 56 10 ac 1f  6b 67 04 67 08 00 45 00   (···V··· kg·g··E·
0010  01 de ad 4d 40 00 29 06  c5 86 80 77 f5 0c 64 40   ···M@·)· ···w··d@
0020  03 82 00 50 d5 6c b1 0c  a1 42 18 05 32 e8 50 18   ···P·l·· ·B··2·P·
0030  00 ed ed e3 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 57 65 64   00 OK··D ate: Wed
0050  2c 20 31 35 20 53 65 70  20 32 30 32 31 20 32 32   , 15 Sep  2021 22
0060  3a 33 32 3a 31 38 20 47  4d 54 0d 0a 53 65 72 76   :32:18 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 37 2e 34 2e 32 33  20 6d 6f 64 5f 70 65 72   P/7.4.23  mod_per
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 57 65  64 2c 20 31 35 20 53 65   fied: We d, 15 Se
00e0  70 20 32 30 32 31 20 30  35 3a 35 39 3a 30 31 20   p 2021 0 5:59:01
```