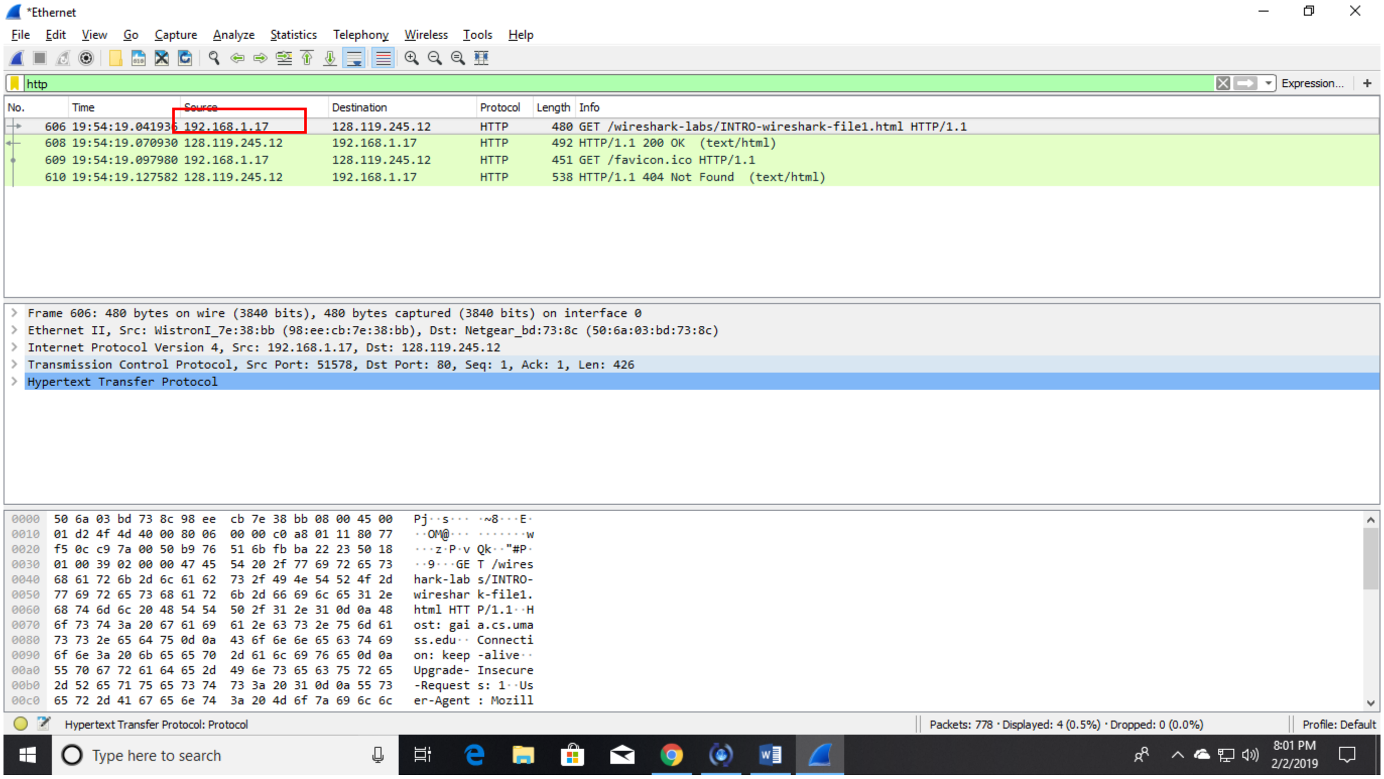
Wireshark lab 1 Getting Started

Jennifer Hurst


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
Type here to search
8:01 PM
2/2/2019

```
http
```

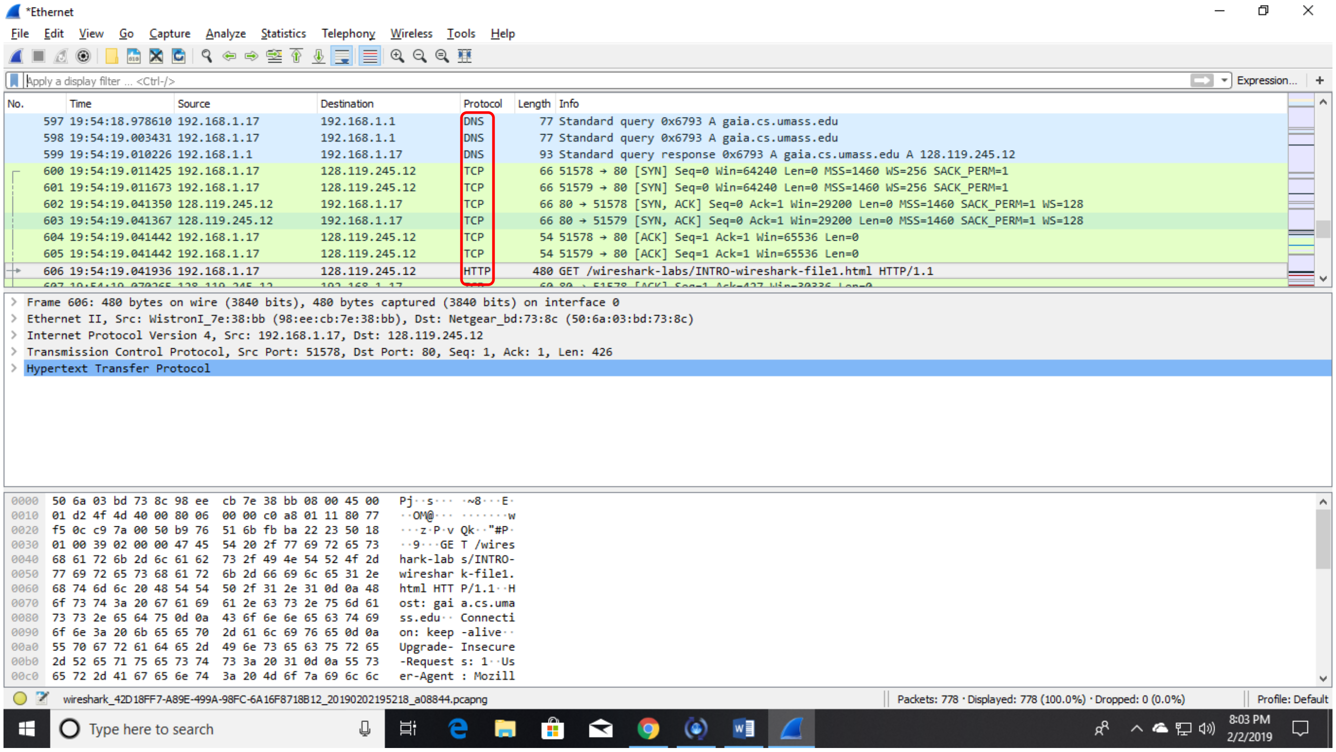
```
No.     Time             Source           Destination      Protocol  Length Info
    606 19:54:19.041936  192.168.1.17     128.119.245.12   HTTP       480 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    608 19:54:19.070930  128.119.245.12   192.168.1.17     HTTP       492 HTTP/1.1 200 OK  (text/html)
    609 19:54:19.097980  192.168.1.17     128.119.245.12   HTTP       451 GET /favicon.ico HTTP/1.1
    610 19:54:19.127582  128.119.245.12   192.168.1.17     HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 606: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
> Ethernet II, Src: WistronI_7e:38:bb (98:ee:cb:7e:38:bb), Dst: Netgear_bd:73:8c (50:6a:03:bd:73:8c)
> Internet Protocol Version 4, Src: 192.168.1.17, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51578, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
> Hypertext Transfer Protocol
```

```
0000  50 6a 03 bd 73 8c 98 ee  cb 7e 38 bb 08 00 45 00   Pj··s··· ·~8···E·
0010  01 d2 4f 4d 40 00 80 06  00 00 c0 a8 01 11 80 77   ··OM@··· ·······w
0020  f5 0c c9 7a 00 50 b9 76  51 6b fb ba 22 23 50 18   ···z·P·v Qk··"#P·
0030  01 00 39 02 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···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 55 73   -Request s: 1··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
```

```
Hypertext Transfer Protocol: Protocol    Packets: 778 · Displayed: 4 (0.5%) · Dropped: 0 (0.0%)    Profile: Default
```

1. What is the Internet address of your computer? The Internet Address of my computer is 192.167.1.17.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Type here to search
8:03 PM
2/2/2019

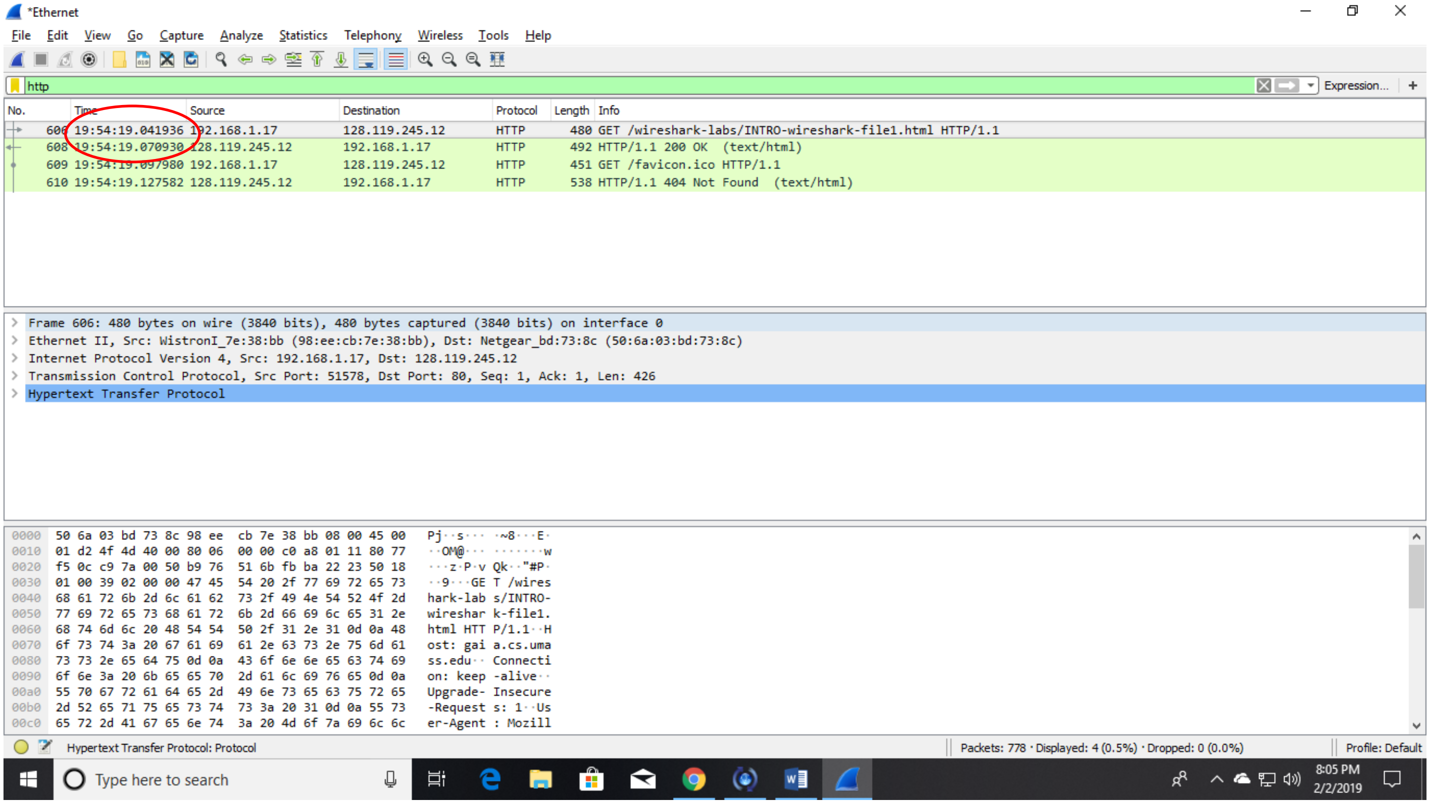
```
No.  Time            Source          Destination     Protocol Length Info
 597 19:54:18.978610 192.168.1.17    192.168.1.1     DNS      77 Standard query 0x6793 A gaia.cs.umass.edu
 598 19:54:19.003431 192.168.1.17    192.168.1.1     DNS      77 Standard query 0x6793 A gaia.cs.umass.edu
 599 19:54:19.010226 192.168.1.1     192.168.1.17    DNS      93 Standard query response 0x6793 A gaia.cs.umass.edu A 128.119.245.12
 600 19:54:19.011425 192.168.1.17    128.119.245.12  TCP      66 51578 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 601 19:54:19.011673 192.168.1.17    128.119.245.12  TCP      66 51579 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 602 19:54:19.041350 128.119.245.12  192.168.1.17    TCP      66 80 → 51578 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
 603 19:54:19.041367 128.119.245.12  192.168.1.17    TCP      66 80 → 51579 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
 604 19:54:19.041442 192.168.1.17    128.119.245.12  TCP      54 51578 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 605 19:54:19.041442 192.168.1.17    128.119.245.12  TCP      54 51579 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 606 19:54:19.041936 192.168.1.17    128.119.245.12  HTTP    480 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 607 19:54:19.070265 128.119.245.12  192.168.1.17    TCP      60 80 → 51578 [ACK] Seq=1 Ack=427 Win=30336 Len=0
```

```
> Frame 606: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
> Ethernet II, Src: WistronI_7e:38:bb (98:ee:cb:7e:38:bb), Dst: Netgear_bd:73:8c (50:6a:03:bd:73:8c)
> Internet Protocol Version 4, Src: 192.168.1.17, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51578, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
> Hypertext Transfer Protocol
```

```
0000  50 6a 03 bd 73 8c 98 ee  cb 7e 38 bb 08 00 45 00   Pj··s··· ·~8···E·
0010  01 d2 4f 4d 40 00 80 06  00 00 c0 a8 01 11 80 77   ··OM@··· ·······w
0020  f5 0c c9 7a 00 50 b9 76  51 6b fb ba 22 23 50 18   ···z·P·v Qk··"#P·
0030  01 00 39 02 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···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 55 73   -Request s: 1··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
```

```
wireshark_42D18FF7-A89E-499A-98FC-6A16F8718B12_20190202195218_a08844.pcapng | Packets: 778 · Displayed: 778 (100.0%) · Dropped: 0 (0.0%) | Profile: Default
```

2. List 3 different protocols that appear in the protocol column in the unfiltered packetlisting window in step 7 above. Three different protocols from the protocol column are DNS, TCP and HTTP.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Type here to search
8:05 PM
2/2/2019

```
http
```

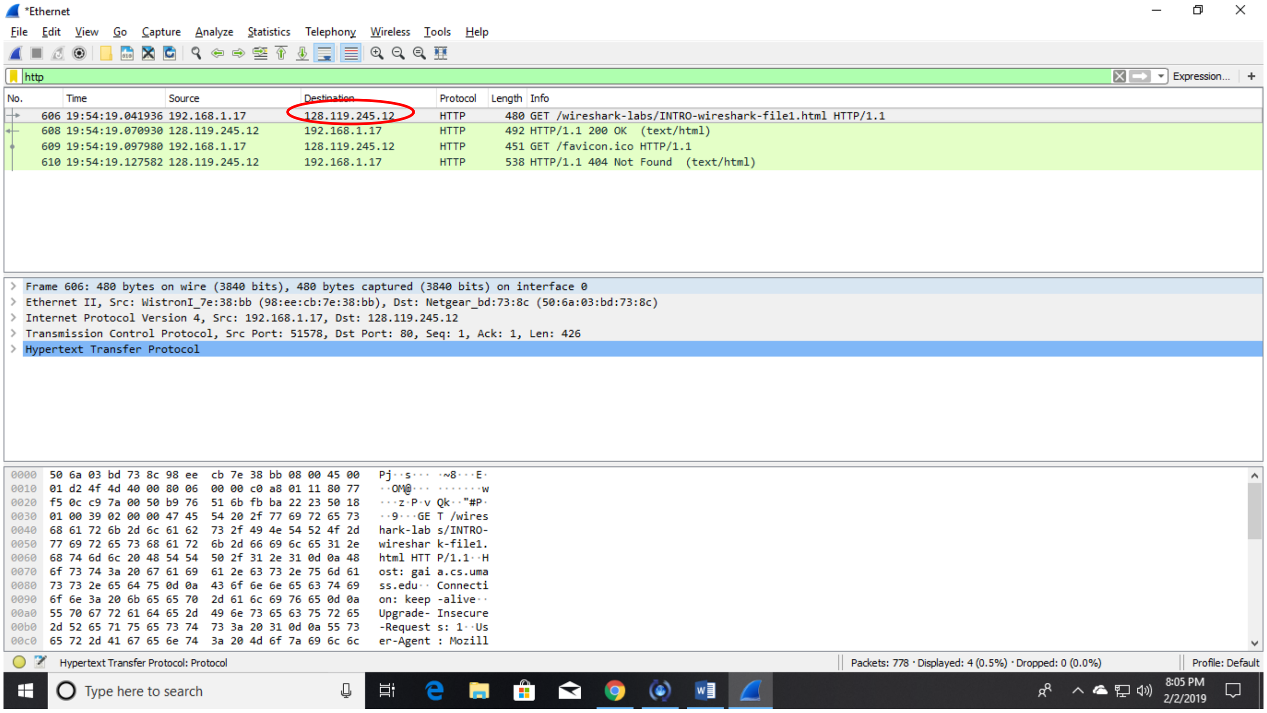
```
No.  Time            Source          Destination     Protocol Length Info
 606 19:54:19.041936 192.168.1.17    128.119.245.12  HTTP    480 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 608 19:54:19.070930 128.119.245.12  192.168.1.17    HTTP    492 HTTP/1.1 200 OK  (text/html)
 609 19:54:19.097980 192.168.1.17    128.119.245.12  HTTP    451 GET /favicon.ico HTTP/1.1
 610 19:54:19.127582 128.119.245.12  192.168.1.17    HTTP    538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 606: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
> Ethernet II, Src: WistronI_7e:38:bb (98:ee:cb:7e:38:bb), Dst: Netgear_bd:73:8c (50:6a:03:bd:73:8c)
> Internet Protocol Version 4, Src: 192.168.1.17, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51578, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
> Hypertext Transfer Protocol
```

```
0000  50 6a 03 bd 73 8c 98 ee  cb 7e 38 bb 08 00 45 00   Pj··s··· ·~8···E·
0010  01 d2 4f 4d 40 00 80 06  00 00 c0 a8 01 11 80 77   ··OM@··· ·······w
0020  f5 0c c9 7a 00 50 b9 76  51 6b fb ba 22 23 50 18   ···z·P·v Qk··"#P·
0030  01 00 39 02 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···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 55 73   -Request s: 1··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
```

```
Hypertext Transfer Protocol: Protocol | Packets: 778 · Displayed: 4 (0.5%) · Dropped: 0 (0.0%) | Profile: Default
```

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.) 1. It took .029 seconds from when HTTP GET was sent until HTTP OK was received.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+
Type here to search
8:05 PM
2/2/2019

http

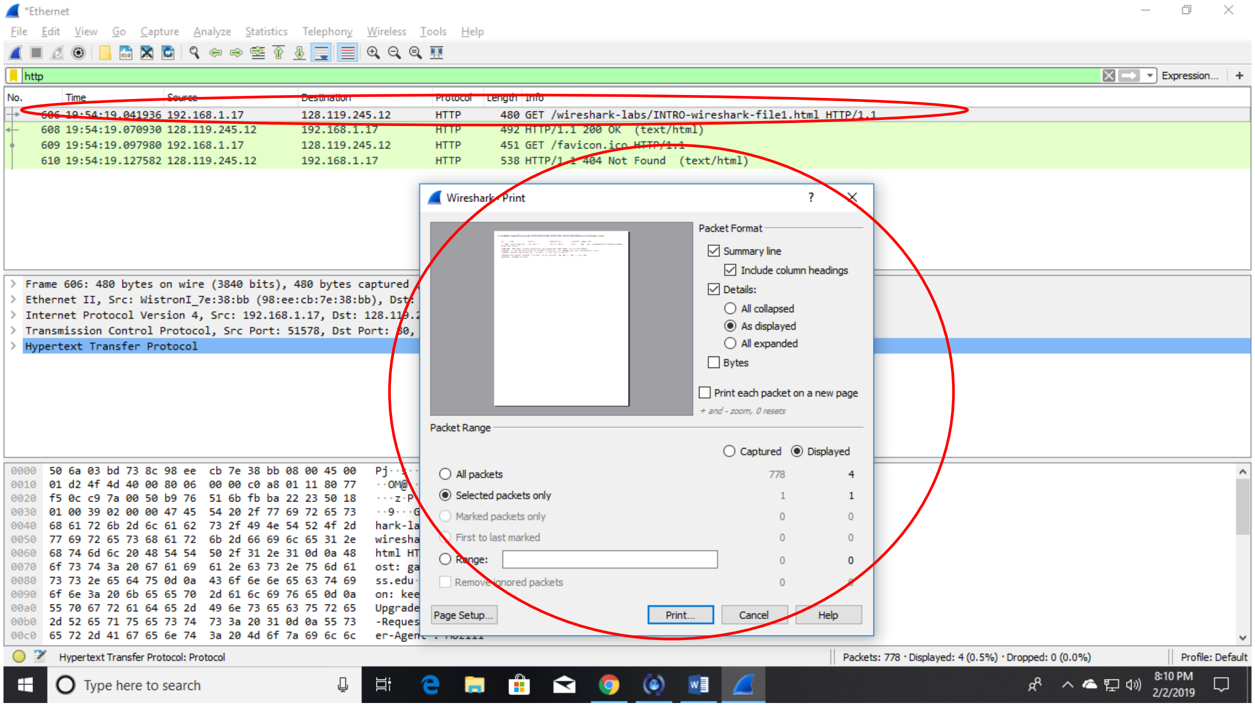
```
No.  Time            Source          Destination     Protocol Length Info
 606 19:54:19.041936 192.168.1.17    128.119.245.12  HTTP      480 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 608 19:54:19.070930 128.119.245.12  192.168.1.17    HTTP      492 HTTP/1.1 200 OK  (text/html)
 609 19:54:19.097980 192.168.1.17    128.119.245.12  HTTP      451 GET /favicon.ico HTTP/1.1
 610 19:54:19.127582 128.119.245.12  192.168.1.17    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 606: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
> Ethernet II, Src: WistronI_7e:38:bb (98:ee:cb:7e:38:bb), Dst: Netgear_bd:73:8c (50:6a:03:bd:73:8c)
> Internet Protocol Version 4, Src: 192.168.1.17, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51578, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
> Hypertext Transfer Protocol
```

```
0000  50 6a 03 bd 73 8c 98 ee  cb 7e 38 bb 08 00 45 00   Pj··s··· ·~8···E·
0010  01 d2 4f 4d 40 00 80 06  00 00 c0 a8 01 11 80 77   ··OM@··· ·······w
0020  f5 0c c9 7a 00 50 b9 76  51 6b fb ba 22 23 50 18   ···z·P·v Qk··"#P·
0030  01 00 39 02 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···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 55 73   -Request s: 1··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
```

Hypertext Transfer Protocol: Protocol | Packets: 778 · Displayed: 4 (0.5%) · 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)? The Internet address of gaia.cs.umass.edu 128.119.245.12.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

Filter: http

```
No.   Time              Source           Destination      Protocol  Length  Info
  606 19:54:19.041936 192.168.1.17     128.119.245.12   HTTP       480 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  608 19:54:19.070930 128.119.245.12   192.168.1.17     HTTP       492 HTTP/1.1 200 OK  (text/html)
  609 19:54:19.097980 192.168.1.17     128.119.245.12   HTTP       451 GET /favicon.ico HTTP/1.1
  610 19:54:19.127582 128.119.245.12   192.168.1.17     HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 606: 480 bytes on wire (3840 bits), 480 bytes captured
> Ethernet II, Src: WistronI_7e:38:bb (98:ee:cb:7e:38:bb), Dst:
> Internet Protocol Version 4, Src: 192.168.1.17, Dst: 128.119.2
> Transmission Control Protocol, Src Port: 51578, Dst Port: 80,
> Hypertext Transfer Protocol
```

```
0000  50 6a 03 bd 73 8c 98 ee  cb 7e 38 bb 08 00 45 00   Pj··s···
0010  01 d2 4f 4d 40 00 80 06  00 00 c0 a8 01 11 80 77   ··OM@···
0020  f5 0c c9 7a 00 50 b9 76  51 6b fb ba 22 23 50 18   ···z·P
0030  01 00 39 02 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···G
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-la
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wiresha
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HT
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: ga
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: kee
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Reques
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent: Mozill
```

Wireshark · Print

Packet Format
- ☑ Summary line
  - ☑ Include column headings
- ☑ Details:
  - ○ All collapsed
  - ● As displayed
  - ○ All expanded
- ☐ Bytes
- ☐ Print each packet on a new page

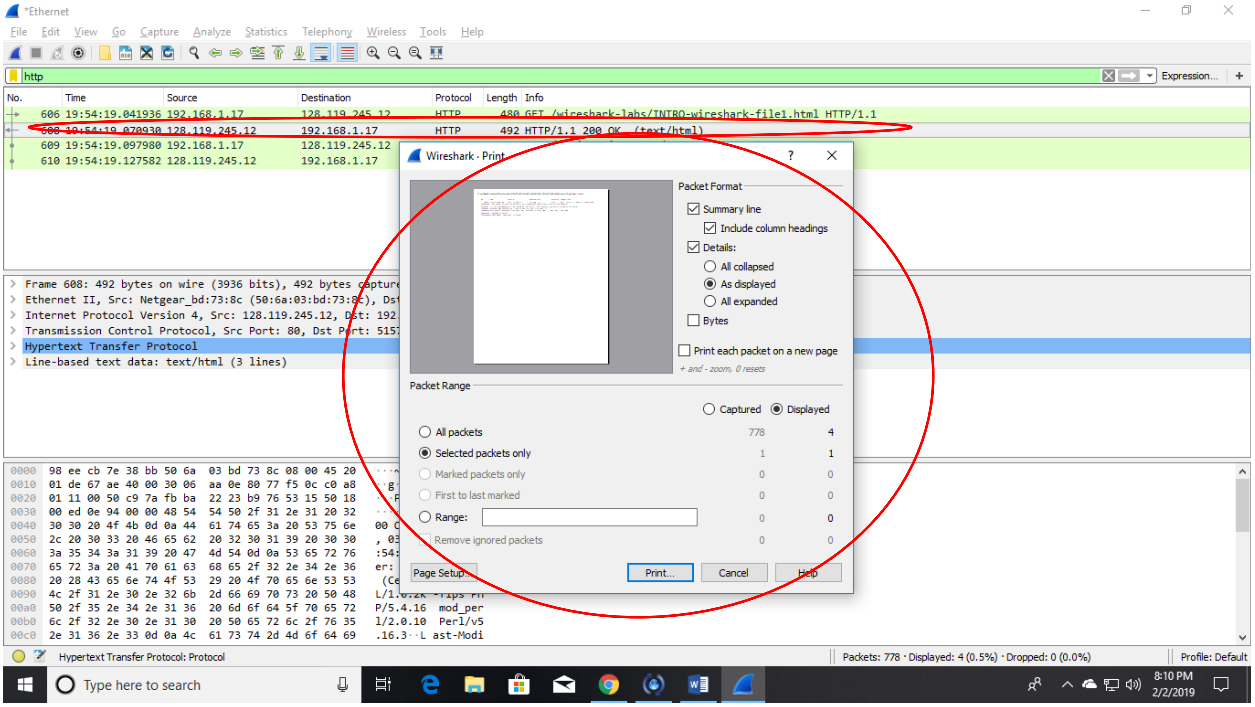
+ and - zoom, 0 resets

Packet Range

	Captured	Displayed
○ All packets	778	4
● Selected packets only	1	1
○ Marked packets only	0	0
○ First to last marked	0	0
○ Range:	0	0
☐ Remove ignored packets	0	0

Hypertext Transfer Protocol: Protocol | Packets: 778 · Displayed: 4 (0.5%) · Dropped: 0 (0.0%) | Profile: Default

Type here to search
8:10 PM
2/2/2019


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

Filter: http

```
No.   Time              Source           Destination      Protocol  Length  Info
  606 19:54:19.041936 192.168.1.17     128.119.245.12   HTTP       480 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  608 19:54:19.070930 128.119.245.12   192.168.1.17     HTTP       492 HTTP/1.1 200 OK  (text/html)
  609 19:54:19.097980 192.168.1.17     128.119.245.12
  610 19:54:19.127582 128.119.245.12   192.168.1.17
```

```
> Frame 608: 492 bytes on wire (3936 bits), 492 bytes capture
> Ethernet II, Src: Netgear_bd:73:8c (50:6a:03:bd:73:8c), Dst
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192
> Transmission Control Protocol, Src Port: 80, Dst Port: 5157
> Hypertext Transfer Protocol
> Line-based text data: text/html (3 lines)
```

```
0000  98 ee cb 7e 38 bb 50 6a  03 bd 73 8c 08 00 45 20   ···~
0010  01 de 67 ae 40 00 30 06  aa 0e 80 77 f5 0c c0 a8   ··g·
0020  01 11 00 50 c9 7a fb ba  22 23 b9 76 53 15 50 18   ···P
0030  00 ed 0e 94 00 00 48 54  54 50 2f 31 2e 31 20 32   ····
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 75 6e   00 O
0050  2c 20 30 33 20 46 65 62  20 32 30 31 39 20 30 30   , 03
0060  3a 35 34 3a 31 39 20 47  4d 54 0d 0a 53 65 72 76   :54:
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er:
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (Ce
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 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
00b0  6c 2f 32 2e 30 2e 31 30  20 50 65 72 6c 2f 76 35   l/2.0.10  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
```

Wireshark · Print

Packet Format
- ☑ Summary line
  - ☑ Include column headings
- ☑ Details:
  - ○ All collapsed
  - ● As displayed
  - ○ All expanded
- ☐ Bytes
- ☐ Print each packet on a new page

+ and - zoom, 0 resets

Packet Range

	Captured	Displayed
○ All packets	778	4
● Selected packets only	1	1
○ Marked packets only	0	0
○ First to last marked	0	0
○ Range:	0	0
☐ Remove ignored packets	0	0

Hypertext Transfer Protocol: Protocol | Packets: 778 · Displayed: 4 (0.5%) · Dropped: 0 (0.0%) | Profile: Default

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.

Do not crop out date and time, all of details tab needs to be there, highlight answer in screen shot.