

1. What is the Internet address of your computer?

192.168.0.3

Wireless Network Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
79	13:58:16.311874	2607:f8b0:4000:80f::...	2600:8806:6101:e600::...	TLSv1.2	358	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
80	13:58:16.312420	2607:f8b0:4000:80f::...	2600:8806:6101:e600::...	TLSv1.2	143	Application Data
81	13:58:16.312476	2600:8806:6101:e600::...	2607:f8b0:4000:80f::...	TCP	74	59326 → 443 [ACK] Seq=611 Ack=3320 Win=65760 Len=0
82	13:58:16.440490	2600:8806:6101:e600::...	2607:f8b0:4000:811::...	TCP	74	59323 → 443 [ACK] Seq=611 Ack=2845 Win=66236 Len=0
83	13:58:16.449472	2600:8806:6101:e600::...	2607:f8b0:4003:c07::...	TCP	74	59325 → 5228 [ACK] Seq=611 Ack=3860 Win=66640 Len=0
84	13:58:16.452528	192.168.0.1	192.168.0.3	TCP	74	4651 → 2869 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 WS=1 TSval=153297739 TSecr=0
85	13:58:16.452640	192.168.0.3	192.168.0.1	TCP	74	2869 → 4651 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 TSval=43187280 TSecr=153297739
86	13:58:16.468479	192.168.0.1	192.168.0.3	TCP	66	4651 → 2869 [ACK] Seq=1 Ack=1 Win=17376 Len=0 TSval=153297739 TSecr=43187280
87	13:58:16.468480	192.168.0.1	192.168.0.3	HTTP/X.	587	NOTIFY /upnp/eventing/wzfdfoilz HTTP/1.1
88	13:58:16.471280	192.168.0.3	192.168.0.1	HTTP	191	HTTP/1.1 200 OK
89	13:58:16.476146	192.168.0.1	192.168.0.3	TCP	66	4651 → 2869 [ACK] Seq=522 Ack=127 Win=17351 Len=0 TSval=153297741 TSecr=43187280

▶ Frame 88: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface 0  
 ▶ Ethernet II, Src: MonHaiPr\_26:b5:f1 (38:59:f9:26:b5:f1), Dst: Netgear\_de:1d:73 (3c:37:86:de:1d:73)  
 ▶ Internet Protocol Version 4, Src: 192.168.0.3, Dst: 192.168.0.1  
 ▶ Transmission Control Protocol, Src Port: 2869, Dst Port: 4651, Seq: 1, Ack: 522, Len: 125  
 ▶ Hypertext Transfer Protocol

```

0000  3c 37 86 de 1d 73 38 59 f9 26 b5 f1 08 00 45 00  <7...sBY-&....E.
0010  00 b1 23 c3 40 00 80 06 55 2f c0 a0 00 03 c0 a8  .#.@...U/.....
0020  00 01 0b 35 12 2b 93 99 6e e8 50 55 35 1d 80 19  ...5+...n-PUS...
0030  01 04 9b f6 00 00 01 01 08 0a 02 92 fc 52 09 23  .....R.#
0040  23 4b 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f  #KHTTP/1.1 200 0
0050  4b 0d 0a 53 65 72 76 65 72 3a 20 4d 69 63 72 6f  K..Serve r: Micro
0060  73 6f 66 74 2d 48 54 54 50 41 50 49 2f 32 2e 30  soft-HTTP PAPI/2.0
0070  0d 0a 44 61 74 65 3a 20 53 75 6e 2c 20 30 33 20  .Date: Sun, 03
0080  46 65 62 20 32 30 31 39 20 31 38 3a 35 38 3a 31  Feb 2019 18:58:1
0090  36 20 47 4d 54 0d 0a 43 6f 6e 6e 65 63 74 69 6f  6 GMT..C onnectio
00a0  6e 3a 20 63 6c 6f 73 65 0d 0a 43 6f 6e 74 65 6e  n: close ..Conten
00b0  74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 0d 0a    t-Length: 0....
  
```

wireshark\_6D8C6C4E-7F69-4A94-83C7-1D7587D59643\_20190203135804\_a03448.pcapng

Packets: 730 · Displayed: 730 (100.0%) · Dropped: 0 (0.0%) Profile: Default

2:00 PM 2/3/2019

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

## TCP – SSDP - DNS

Wireshark packet capture window showing network traffic. The packet list pane displays several packets, with three highlighted: 138 (TCP), 141 (SSDP), and 144 (DNS). The packet details pane shows the structure of packet 147, which is a DNS query. The packet bytes pane shows the raw data of packet 147.

No.	Time	Source	Destination	Protocol	Length	Info
138	13:58:16.765453	2607:f8b0:4000:80f::...	2600:8806:6101:e600::...	TCP	74	443 → 59324 [ACK] Seq=4490 Ack=1055 Win=29440 Len=0
139	13:58:16.793565	2607:f8b0:4000:811::...	2600:8806:6101:e600::...	TCP	74	443 → 59323 [ACK] Seq=3607 Ack=1772 Win=30464 Len=0
140	13:58:16.849501	2600:8806:6101:e600::...	2607:f8b0:4003:c07::...	TCP	74	59325 → 5228 [ACK] Seq=793 Ack=4142 Win=66356 Len=0
141	13:58:16.978369	192.168.0.3	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
142	13:58:16.990428	2600:8806:6101:e600::...	2001:578:3f::30	DNS	99	Standard query 0x66d4 A clients2.google.com
143	13:58:17.000486	2001:578:3f::30	2600:8806:6101:e600::...	DNS	139	Standard query response 0x66d4 A clients2.google.com CNAME clients.l.google.com A 172.217.12.46
144	13:58:17.000919	2600:8806:6101:e600::...	2001:578:3f::30	DNS	99	Standard query 0x7d24 AAAA clients2.google.com
145	13:58:17.012493	2001:578:3f::30	2600:8806:6101:e600::...	DNS	151	Standard query response 0x7d24 AAAA clients2.google.com CNAME clients.l.google.com AAAA 2607:f8b0:4000:81...
146	13:58:17.013106	2600:8806:6101:e600::...	2607:f8b0:4000:815::...	TCP	86	59327 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=4 SACK_PERM=1
147	13:58:17.056588	2600:8806:6101:e600::...	2001:578:3f::30	DNS	98	Standard query 0x23bd A auth.grammarly.com

Frame 147: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

- Ethernet II, Src: HonHaiPr\_26:b5:f1 (38:59:f9:26:b5:f1), Dst: Netgear\_de:1d:73 (3c:37:86:de:1d:73)
- Internet Protocol Version 6, Src: 2600:8806:6101:e600:802d:531f:916e:c267, Dst: 2001:578:3f::30
- User Datagram Protocol, Src Port: 55020, Dst Port: 53
- Domain Name System (query)

0000 3c 37 86 de 1d 73 38 59 f9 26 b5 f1 86 dd 60 00 <7...s8Y &....`

0010 00 00 00 2c 11 40 26 00 88 06 61 01 e6 00 80 2d ..., @&...a....

0020 53 1f 91 6e c2 67 20 01 05 78 00 3f 00 00 00 00 S...n g...x?...`

0030 00 00 00 00 00 30 d6 ec 00 35 00 2c ed a0 23 bd .....0...5,...#

0040 01 00 00 01 00 00 00 00 00 00 04 61 75 74 68 09 .....auth...

0050 67 72 61 6d 6d 61 72 6c 79 03 63 6f 6d 00 00 01 grammarly.com...

0060 00 01 ..

wireshark\_608c6c4e-7f69-4a94-83c7-1d7587d59643\_20190203135804\_a03448.pcapng

Packets: 730 • Displayed: 730 (100.0%) • Dropped: 0 (0.0%)

Profile: Default

2:05 PM  
2/3/2019

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 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*.)

The duration = 0.520986 - 0.494326 = 0.26660 second

The screenshot shows the Wireshark interface with a packet capture on a wireless network connection. The packet list pane displays several packets, with packet 540 selected. This packet is an HTTP GET request from 192.168.0.3 to 128.119.245.12 for the resource /wireshark-labs/INTRO-wireshark-file1.html. The packet details pane shows the structure of the frame, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates that 730 packets were captured, with 6 displayed and 0 dropped.

No.	Time	Source	Destination	Protocol	Length	Info
87	13:58:16.468480	192.168.0.1	192.168.0.3	HTTP/X..	587	NOTIFY /upnp/eventing/wzfnfz HTTP/1.1
88	13:58:16.471280	192.168.0.3	192.168.0.1	HTTP	191	HTTP/1.1 200 OK
540	13:58:20.494326	192.168.0.3	128.119.245.12	HTTP	479	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
543	13:58:20.520986	128.119.245.12	192.168.0.3	HTTP	492	HTTP/1.1 200 OK (text/html)
548	13:58:21.325768	192.168.0.3	128.119.245.12	HTTP	450	GET /favicon.ico HTTP/1.1
549	13:58:21.376677	128.119.245.12	192.168.0.3	HTTP	538	HTTP/1.1 404 Not Found (text/html)

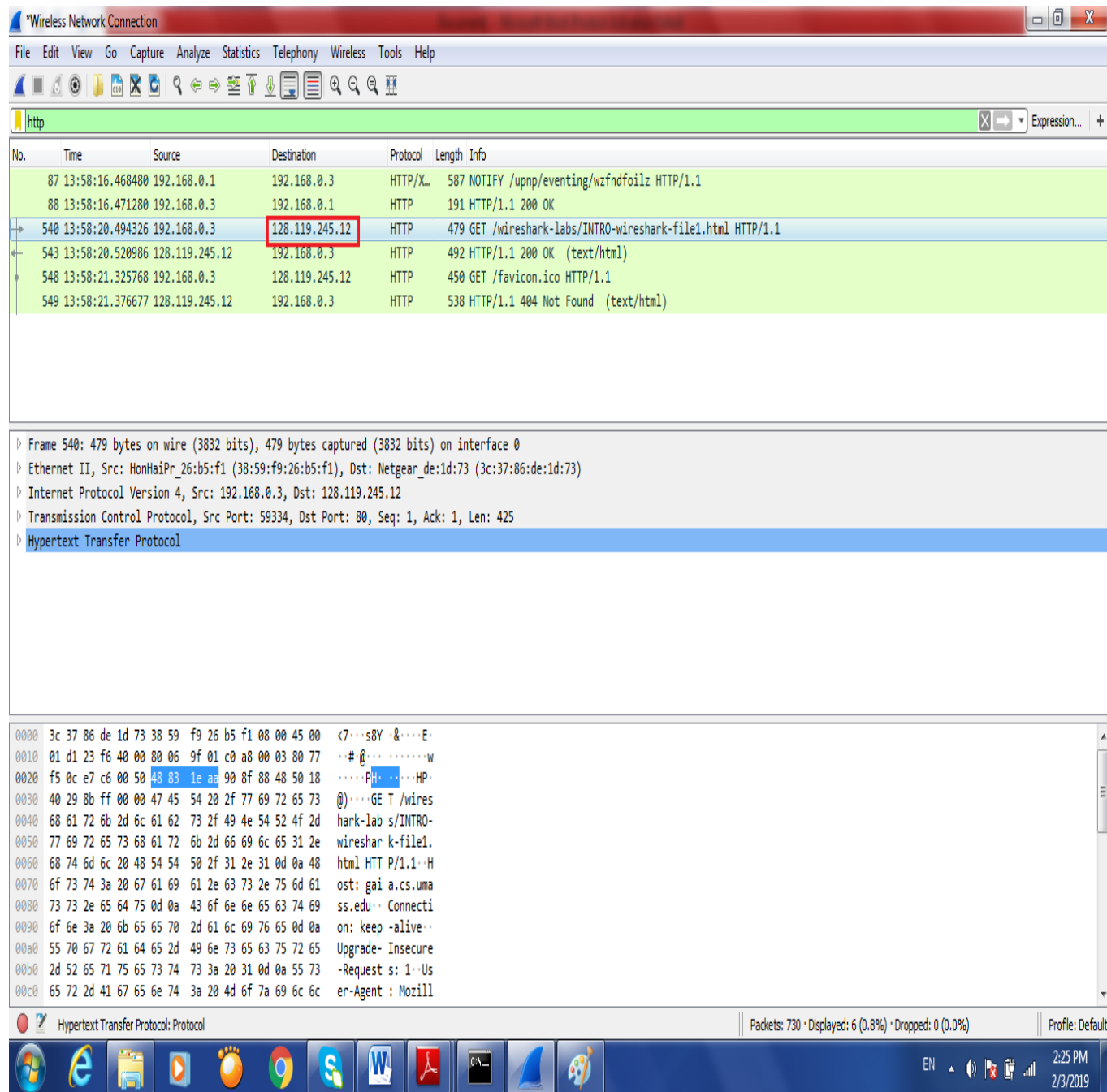
Frame 540: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0  
 Ethernet II, Src: HonHaiPr\_26:b5:f1 (38:59:f9:26:b5:f1), Dst: Netgear\_de:1d:73 (3c:37:86:de:1d:73)  
 Internet Protocol Version 4, Src: 192.168.0.3, Dst: 128.119.245.12  
 Transmission Control Protocol, Src Port: 59334, Dst Port: 80, Seq: 1, Ack: 1, Len: 425  
 Hypertext Transfer Protocol

0000 3c 37 86 de 1d 73 38 59 f9 26 b5 f1 00 00 45 00 <7...s8Y -&...E.  
 0010 01 d1 23 f6 40 00 00 06 9f 01 c0 a8 00 03 80 77 ..#@... ..W  
 0020 f5 0c e7 c6 00 50 48 83 1e aa 90 8f 88 48 50 18 .....PH... ..HP  
 0030 40 29 8b ff 00 00 47 45 54 20 2f 77 69 72 65 73 @)....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 htm] HTTP/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: 730 · Displayed: 6 (0.8%) · Dropped: 0 (0.0%)  
 Profile: Default

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

128.119.245.12



The image shows a Wireshark network traffic capture window titled "Wireless Network Connection". The main display area shows a list of captured packets. Packet 540 is selected, showing an HTTP GET request to 128.119.245.12. The packet details pane below shows the structure of the frame: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

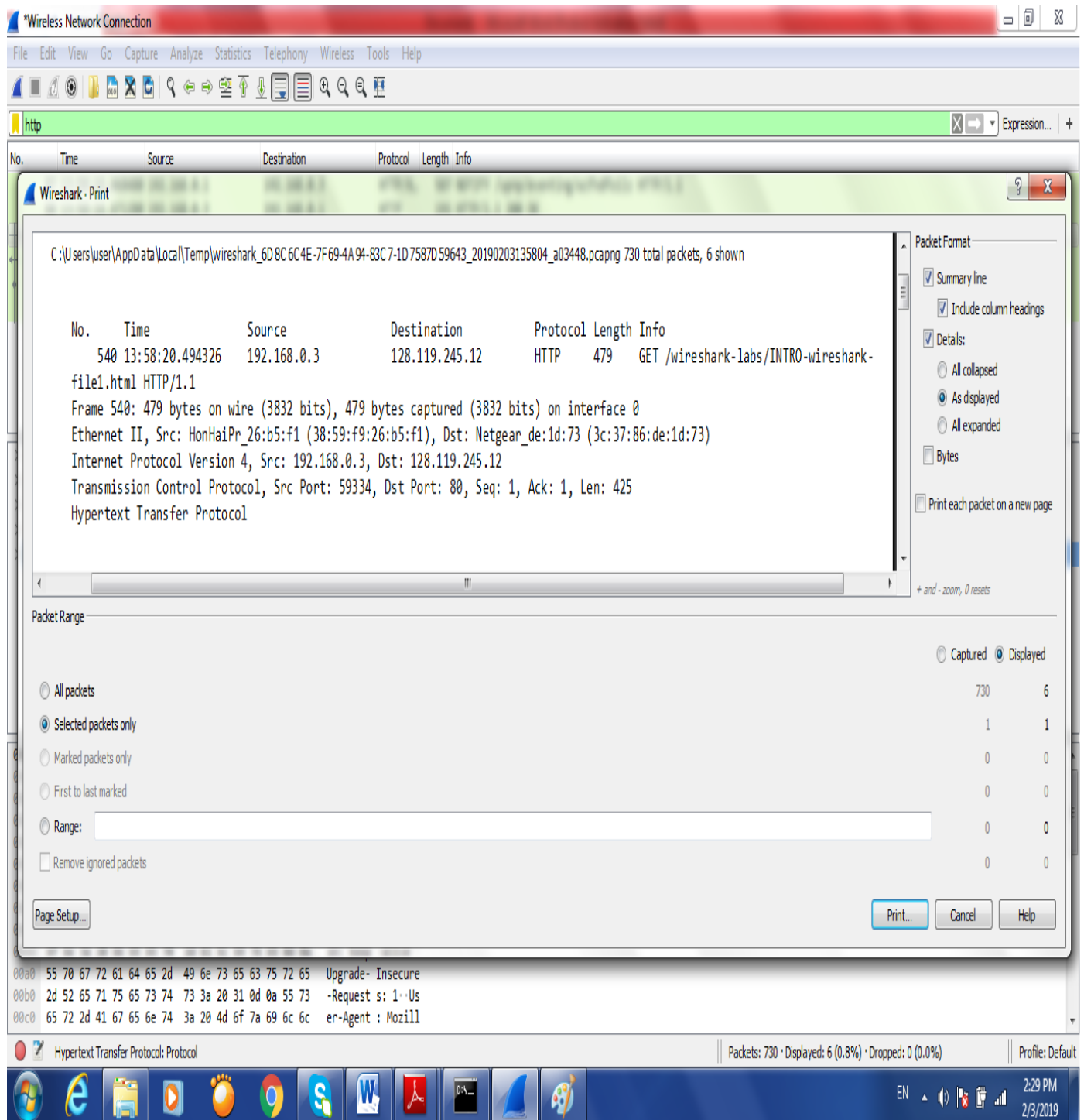
No.	Time	Source	Destination	Protocol	Length	Info
87	13:58:16.468480	192.168.0.1	192.168.0.3	HTTP/XML	587	NOTIFY /upnp/eventing/wzfdnfoilz HTTP/1.1
88	13:58:16.471280	192.168.0.3	192.168.0.1	HTTP	191	HTTP/1.1 200 OK
540	13:58:20.494326	192.168.0.3	128.119.245.12	HTTP	479	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
543	13:58:20.520986	128.119.245.12	192.168.0.3	HTTP	492	HTTP/1.1 200 OK (text/html)
548	13:58:21.325768	192.168.0.3	128.119.245.12	HTTP	450	GET /favicon.ico HTTP/1.1
549	13:58:21.376677	128.119.245.12	192.168.0.3	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 540: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0  
Ethernet II, Src: HonHaiPr\_26:b5:f1 (38:59:f9:26:b5:f1), Dst: Netgear\_de:1d:73 (3c:37:86:de:1d:73)  
Internet Protocol Version 4, Src: 192.168.0.3, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 59334, Dst Port: 80, Seq: 1, Ack: 1, Len: 425  
Hypertext Transfer Protocol

0000 3c 37 86 de 1d 73 38 59 f9 26 b5 f1 08 00 45 00 <?...s8Y...&....E.  
0010 01 d1 23 f6 40 00 00 06 9f 01 c0 a8 00 03 80 77 ..#:@.....w  
0020 f5 0c e7 c6 00 50 48 83 1e aa 90 8f 88 48 50 18 ....PH....HP.  
0030 40 29 8b ff 00 00 47 45 54 20 2f 77 69 72 65 73 @)....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: 730 • Displayed: 6 (0.8%) • 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.







Wireshark - Print

C:\Users\User\AppData\Local\Temp\Wireshark\_6D8C6C4E-7F69-4A94-83C7-1D7587D59643\_20190203135804\_a03448.pcapng 730 total packets, 6 shown

No.	Time	Source	Destination	Protocol	Length	Info
543	13:58:20.520986	128.119.245.12	192.168.0.3	HTTP	492	HTTP/1.1 200 OK (text/html)

Frame 543: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0  
Ethernet II, Src: Netgear\_de:1d:73 (3c:37:86:de:1d:73), Dst: HonHaiPr\_26:b5:f1 (38:59:f9:26:b5:f1)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.3  
Transmission Control Protocol, Src Port: 80, Dst Port: 59334, Seq: 1, Ack: 426, Len: 438  
Hypertext Transfer Protocol  
Line-based text data: text/html (3 lines)

Packet Range

☐ All packets 730 6  
☒ Selected packets only 1 1  
☐ Marked packets only 0 0  
☐ First to last marked 0 0  
☐ Range: 0 0  
☐ Remove ignored packets 0 0

Page Setup... Print... Cancel Help

Hypertext Transfer Protocol: Protocol

Packets: 730 · Displayed: 6 (0.8%) · Dropped: 0 (0.0%) Profile: Default

2:34 PM 2/3/2019



\*Wireless Network Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
87	13:58:16.468480	192.168.0.1	192.168.0.3	HTTP/XML	587	NOTIFY /upnp/eventing/wzfnfz HTTP/1.1
88	13:58:16.471280	192.168.0.3	192.168.0.1	HTTP	191	HTTP/1.1 200 OK
540	13:58:20.494326	192.168.0.3	128.119.245.12	HTTP	479	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
543	13:58:20.520986	128.119.245.12	192.168.0.3	HTTP	492	HTTP/1.1 200 OK (text/html)
548	13:58:21.325768	192.168.0.3	128.119.245.12	HTTP	450	GET /favicon.ico HTTP/1.1
549	13:58:21.376677	128.119.245.12	192.168.0.3	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.3

Transmission Control Protocol, Src Port: 80, Dst Port: 59334, Seq: 1, Ack: 426, Len: 438

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sun, 03 Feb 2019 18:58:20 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod\_perl/2.0.10 Perl/v5.16.3\r\n

Last-Modified: Sun, 03 Feb 2019 06:59:01 GMT\r\n

ETag: "51-580f7e9333493"\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

0000 38 59 f9 26 b5 f1 3c 37 86 de 1d 73 08 00 45 00 8Y&...<7 ...s..E

0010 01 de 31 f5 40 00 fc 06 14 f5 80 77 f5 0c c0 a8 ..1.@... ..w....

0020 00 03 00 50 e7 c6 90 8f 88 48 48 83 20 53 50 18 ...P.... ..H. SP

0030 00 ed 8e 85 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 53 75 6e 00 OK..D ate: Sun

0050 2c 20 30 33 20 46 65 62 20 32 30 31 39 20 31 38 , 03 Feb 2019 18

0060 3a 35 38 3a 32 30 20 47 4d 54 0d 0a 53 65 72 76 :58:20 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 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

Hypertext Transfer Protocol: Protocol

Packets: 730 · Displayed: 6 (0.8%) · Dropped: 0 (0.0%)

Profile: Default

2:38 PM 2/3/2019