

Lab 1

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

HTTP, TCP and UDP.

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.)**

Less than a tenth of a second (~ 0.8 seconds)

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

gaia.cs.umass.edu internet address: 128.119.245.12

my internet address: 192.168.1.11

4. **Screenshot the two HTTP messages (GET and OK) referred to in question 2 above. Make sure to include all pertinent information in the screenshot (Time field, Internet addresses, etc). Paste these screenshots into your lab report**

The image shows a Wireshark packet capture window titled "*Ethernet". The packet list at the top shows two packets: packet 143 is a GET request for "/wireshark-labs/INTRO-wireshark-file1.html" and packet 147 is an HTTP 304 Not Modified response. The packet details pane for packet 147 is expanded, showing the following structure:

- Frame 147: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0
- Ethernet II, Src: Actionte_8e:4a:8e (00:24:7b:8e:4a:8e), Dst: Micro-St_9d:2f:6a (30:9c:23:9d:2f:6a)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.11
 - 0100 ... = Version: 4
 - ... 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 279
 - Identification: 0xf58c (62860)
 - Flags: 0x4000, Don't fragment
 - Time to live: 45
 - Protocol: TCP (6)
 - Header checksum: 0x201d [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 128.119.245.12
 - Destination: 192.168.1.11
- Transmission Control Protocol, Src Port: 80, Dst Port: 49401, Seq: 1, Ack: 571, Len: 239
- Hypertext Transfer Protocol
 - HTTP/1.1 304 Not Modified\r\n
 - Date: Sun, 31 Mar 2019 22:56:15 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
 - Connection: Keep-Alive\r\n
 - Keep-Alive: timeout=5, max=100\r\n
 - ETag: "51-5855d99bbea46"\r\n
 - \r\n
 - [HTTP response 1/1]
 - [Time since request: 0.080000000 seconds]
 - [Request in frame: 143]
 - [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

The packet bytes pane at the bottom shows the raw data of the frame, starting with the Ethernet II header (30 9c 23 9d 2f 6a 00 24 7b 8e 4a 8e 08 00 45 00) and the IP header (01 17 f5 8c 40 00 2d 06 20 1d 80 77 f5 0c c0 a8).

Frame (frame), 293 bytes | Packets: 175 · Displayed: 2 (1.1%) · Dropped: 0 (0.0%) | Profile: Default

The image shows a Wireshark packet capture window titled "Ethernet". The packet list pane at the top shows two packets. Packet 143 is an HTTP GET request from 192.168.1.11 to 128.119.245.12. Packet 147 is the corresponding HTTP response from 128.119.245.12 to 192.168.1.11.

The packet details pane for packet 143 is expanded, showing the following structure:

- Frame 143: 624 bytes on wire (4992 bits), 624 bytes captured (4992 bits) on interface 0
- Ethernet II, Src: Micro-St_9d:2f:6a (30:9c:23:9d:2f:6a), Dst: Actionte_8e:4a:8e (00:24:7b:8e:4a:8e)
- Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
 - 0100 = Version: 4
 - ... 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 610
 - Identification: 0x643d (25661)
 - Flags: 0x4000, Don't fragment
 - Time to live: 128
 - Protocol: TCP (6)
 - Header checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.1.11
 - Destination: 128.119.245.12
- Transmission Control Protocol, Src Port: 49401, Dst Port: 80, Seq: 1, Ack: 1, Len: 570
- 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
 - Cache-Control: max-age=0\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/73.0.3683.86 Safari/537.36\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: en-US,en;q=0.9\r\n
 - If-None-Match: "51-5855d99bbea46"\r\n
 - If-Modified-Since: Sun, 31 Mar 2019 05:59:01 GMT\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: 147]

The packet bytes pane at the bottom shows the raw data of the frame, starting with the Ethernet II header (00 24 7b 8e 4a 8e 30 9c 23 9d 2f 6a 08 00 45 00) and the IP header (00 00 c0 a8 01 0b 80 77).

At the bottom of the window, the status bar indicates: "Frame (frame), 624 bytes" and "Packets: 175 · Displayed: 2 (1.1%) · Dropped: 0 (0.0%) | Profile: Default".