CS3516 - Lab 1

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

2. **How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?**
   0.041683 seconds (41.683 ms)

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?**
   The IP address of gaia.cs.umass.edu is 128.119.245.12 and the IP address of my computer is 10.0.1.36.

4. **Print the two HTTP messages (GET and OK) referred to in question 2 above.**
   GET:

   > C:\Users\Przemek\Desktop\session.pcapng 67 total packets, 67 shown   48
   > 19:22:25.405215   10.0.1.36   128.119.245.12   HTTP   489   GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 Frame 48: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface 0 Ethernet II, Src: Giga-Byt_20:0f:b1 (e0:d5:5e:20:0f:b1), Dst: Apple_0c:91:8d (90:72:40:0c:91:8d) Internet Protocol Version 4, Src: 10.0.1.36, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 58283, Dst Port: 80, Seq: 1, Ack: 1, Len: 435 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   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36\r\n   Upgrade-Insecure-Requests: 1\r\n   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n   DNT: 1\r\n   Accept-Encoding: gzip, deflate\r\n   Accept-Language: en-US,en;q=0.8\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: 50

   OK:

   > C:\Users\Przemek\Desktop\session.pcapng 67 total packets, 67 shown   50
   > 19:22:25.446898   128.119.245.12   10.0.1.36   HTTP   492   HTTP/1.1 200 OK (text/html) Frame 50: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0 Ethernet II, Src: Apple_0c:91:8d (90:72:40:0c:91:8d), Dst: Giga-Byt_20:0f:b1 (e0:d5:5e:20:0f:b1) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.1.36 Transmission Control Protocol, Src Port: 80, Dst Port: 58283, Seq: 1, Ack: 436, Len: 438 Hypertext Transfer Protocol   HTTP/1.1 200 OK\r\n   Date: Sat, 28 Oct 2017 23:22:25 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: Sat, 28 Oct 2017 05:59:01 GMT\r\n   ETag: "51-55c951a1b7ac2"\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:

0.041683000 seconds]   [Request in frame: 48]   File Data: 81 bytes Line-based text data: text/html