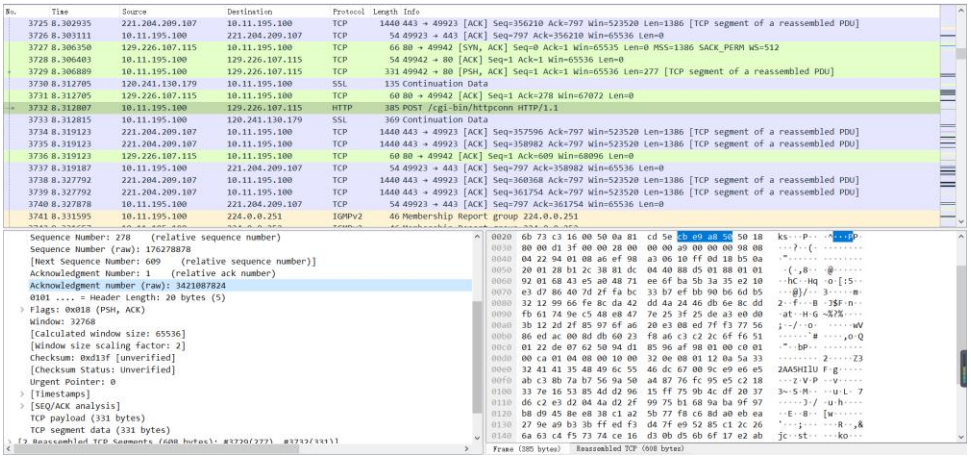
Lab Report

Lab 1 Wireshark Introduction

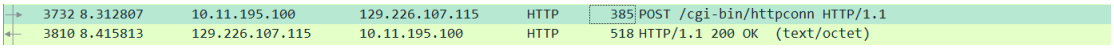
ZHOU Siyu

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

   TCP, SSL, HTTP

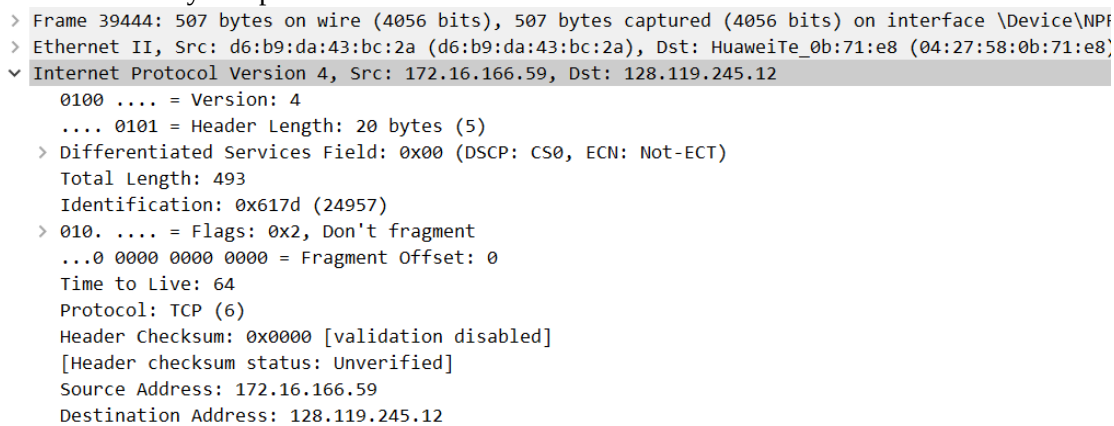


2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?



   8.415813 - 8.312807 = 0.103006 s

3. What is the IP address of gaia.cs.umass.edu? What is the IP address of your computer?
   IP address of gaia.cs.umass.edu: 128.119.245.12
   IP address of my computer: 172.119.245.12



4. Print the above two HTTP messages (GET and OK) by selecting Print from the menu Wireshark File, and selecting the “Selected Packet Only” and “Print as displayed” radial buttons, and then clicking OK.

Here is GET message:

```
C:\Users\zoezh\AppData\Local\Temp\wireshark_WLANVKZSY1.pcapng 96206 总分组数,206 已显示

No.     Time           Source                Destination           Protocol Length Info
  39444 664.959852     172.16.166.59         128.119.245.12        HTTP     507    GET / HTTP/1.1
Frame 39444: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits) on interface \Device\NPF_{93EBE42A-
FB37-4581-A7C7-17CF555DBAE1}, id 0
Ethernet II, Src: d6:b9:da:43:bc:2a (d6:b9:da:43:bc:2a), Dst: HuaweiTe_0b:71:e8 (04:27:58:0b:71:e8)
Internet Protocol Version 4, Src: 172.16.166.59, 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: 493
    Identification: 0x617d (24957)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.166.59
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 60872, Dst Port: 80, Seq: 1, Ack: 1, Len: 453
Hypertext Transfer Protocol
    GET / HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\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/109.0.0.0
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
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-US;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/]
    [HTTP request 1/2]
    [Response in frame: 39466]
    [Next request in frame: 39468]
```

Here is OK message:

```
C:\Users\zoezh\AppData\Local\Temp\wireshark_WLANVKZSY1.pcapng 128966 总分组数,264 已显示

No.     Time           Source                Destination           Protocol Length Info
  39466 665.193184     128.119.245.12        172.16.166.59         HTTP     145    HTTP/1.1 200 OK  (text/html)
Frame 39466: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{93EBE42A-
FB37-4581-A7C7-17CF555DBAE1}, id 0
Ethernet II, Src: HuaweiTe_0b:71:e8 (04:27:58:0b:71:e8), Dst: d6:b9:da:43:bc:2a (d6:b9:da:43:bc:2a)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.166.59
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 131
    Identification: 0xc261 (49761)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 39
    Protocol: TCP (6)
    Header Checksum: 0xc943 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 172.16.166.59
Transmission Control Protocol, Src Port: 80, Dst Port: 60872, Seq: 2921, Ack: 454, Len: 91
[3 Reassembled TCP Segments (3011 bytes): #39464(1460), #39465(1460), #39466(91)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 17 Jan 2023 14:59:04 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 01 Mar 2016 18:57:50 GMT\r\n
    ETag: "a5b-52d015789ee9e"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 2651\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 1/2]
    [Time since request: 0.233332000 seconds]
    [Request in frame: 39444]
    [Next request in frame: 39468]
    [Next response in frame: 39588]
    [Request URI: http://gaia.cs.umass.edu/cnrg_imap.jpg]
    File Data: 2651 bytes
Line-based text data: text/html (68 lines)
```