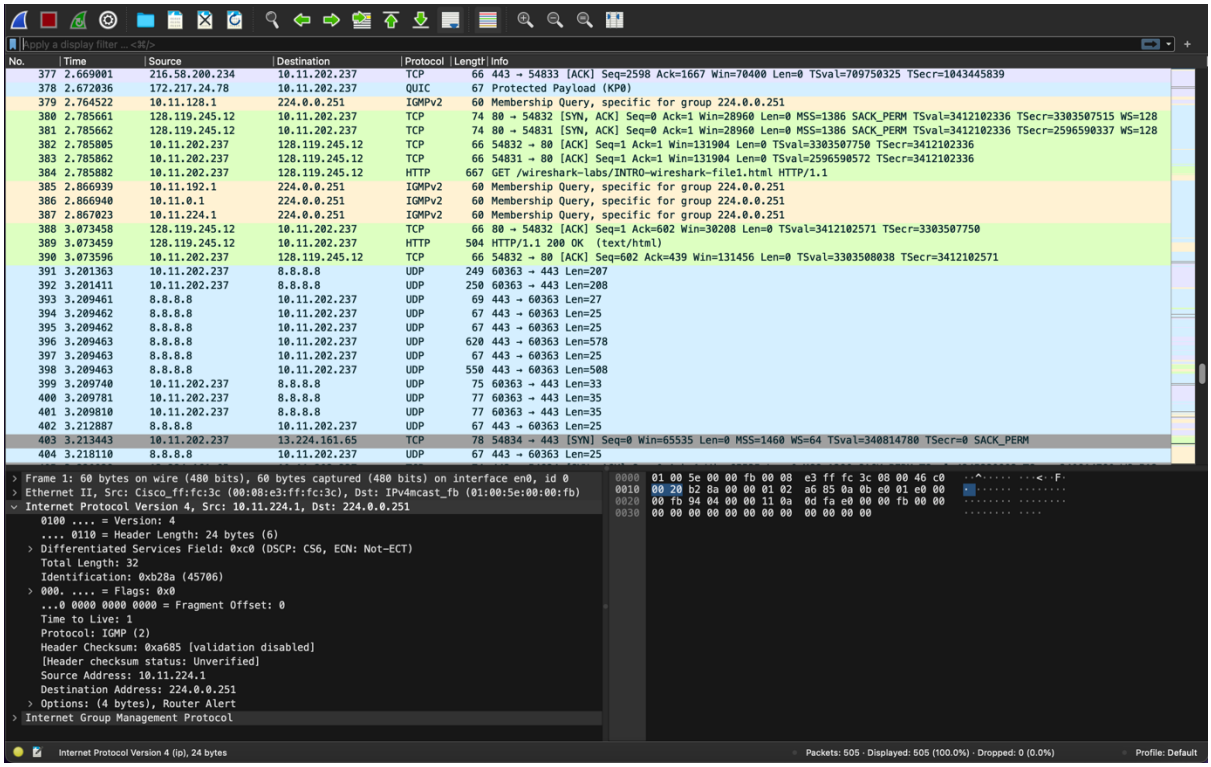
Lab 1 Wireshark Introduction

Lab Report

Guanlin Jiang (21093962D)

Q1:
According to the screenshot, the protocols in here are TCP, UDP, HTTP



Q2:
According to the screenshot, the time between the HTTP GET and HTTP OK is
3.073459 – 2.785882 = 0.287577 s

```
384 2.785882    10.11.202.237    128.119.245.12    HTTP    667 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
389 3.073459    128.119.245.12   10.11.202.237     HTTP    504 HTTP/1.1 200 OK  (text/html)
```

Q3:
According to the screenshot,
The gaia.cs.umass.edu IP is: 128.119.245.12
My computer is: 10.11.202.237

```
Internet Protocol Version 4, Src: 10.11.202.237, 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: 653
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xedee [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.11.202.237
    Destination Address: 128.119.245.12
```

Q4:
Here is HTTP GET message:

/var/folders/qm/z6p39g1918j8y92zw7mckm440000gn/T/wireshark_Wi-FiV8S5Y1.pcapng 505 total packets, 6 shown

```
No.     Time           Source                Destination           Protocol Length Info
    384 2.785882       10.11.202.237         128.119.245.12        HTTP     667    GET /
wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 384: 667 bytes on wire (5336 bits), 667 bytes captured (5336 bits) on interface en0, id 0
Ethernet II, Src: Apple_40:72:b8 (bc:d0:74:40:72:b8), Dst: IETF-VRRP-VRID_01 (00:00:5e:
00:01:01)
Internet Protocol Version 4, Src: 10.11.202.237, 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: 653
    Identification: 0x0000 (0)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xedee [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.11.202.237
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 54832, Dst Port: 80, Seq: 1, Ack: 1, Len: 601
Hypertext Transfer Protocol
```

Here is HTTP OK message:

/var/folders/qm/z6p39g1918j8y92zw7mckm440000gn/T/wireshark_Wi-FiV8S5Y1.pcapng 505 total packets, 6 shown

```
No.     Time           Source                Destination           Protocol Length Info
    389 3.073459       128.119.245.12        10.11.202.237         HTTP     504    HTTP/1.1 200
OK  (text/html)
Frame 389: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface en0, id 0
Ethernet II, Src: Cisco_ff:fc:34 (00:08:e3:ff:fc:34), Dst: Apple_40:72:b8 (bc:d0:74:40:72:b8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.11.202.237
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 490
    Identification: 0x0779 (1913)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 38
    Protocol: TCP (6)
    Header Checksum: 0x0119 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 10.11.202.237
Transmission Control Protocol, Src Port: 80, Dst Port: 54832, Seq: 1, Ack: 602, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```