CSCE 4753 Computer Networks – Wireshark Introduction

Name: Robert Goss
ID: 010837761

20 points
4 questions (some of them are required screenshot)

Instructions

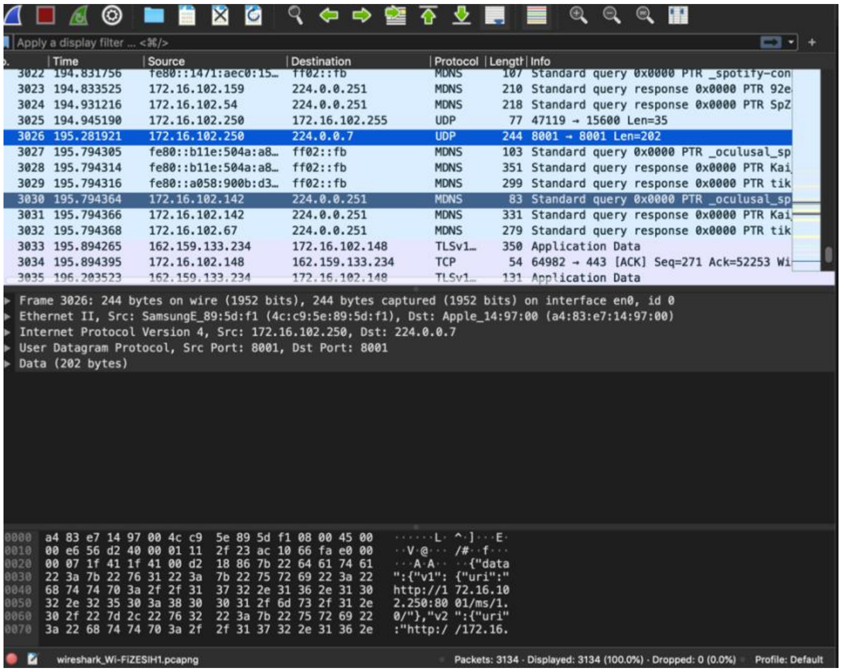
- Type your work, print it to a *single* PDF, and upload it to Blackboard before the due date and time. It is strongly suggested to use the given document.
- Show all of your work. Without proper justification and details of steps, correct answers alone may not carry full credit.
- -2 points if you do not insert your name and ID at the top of the document.
- -5 points if it is not typed or legible. On this homework, you may scan it with something like the app CamScanner but just make sure it is a legible PDF.
- -5 points if it is not a PDF file.
- -5 points if it is not a single PDF file. Submit one PDF file. Do not submit zip files containing one or more files.
- -5 points if you present the worked problems out of order. In other words, please present the problems in the order assigned, 1, 2, 3, …

What to hand in

The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

1. (5 pts.) List 5 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above. **Please attached a screenshot in your report**.

   -UDP, TCP, MDNS, SSDP, QUIC



```
o.   Time        Source                 Destination        Protocol  Length Info
3022 194.831756  fe80::1471:aec0:15…    ff02::fb           MDNS       107 Standard query 0x0000 PTR _spotify-con
3023 194.833525  172.16.102.159         224.0.0.251        MDNS       210 Standard query response 0x0000 PTR 92e
3024 194.931216  172.16.102.54          224.0.0.251        MDNS       218 Standard query response 0x0000 PTR SpZ
3025 194.945190  172.16.102.250         172.16.102.255     UDP         77 47119 → 15600 Len=35
3026 195.281921  172.16.102.250         224.0.0.7          UDP        244 8001 → 8001 Len=202
3027 195.794305  fe80::b11e:504a:a8…    ff02::fb           MDNS       103 Standard query 0x0000 PTR _oculusal_sp
3028 195.794314  fe80::b11e:504a:a8…    ff02::fb           MDNS       351 Standard query response 0x0000 PTR Kai
3029 195.794316  fe80::a058:900b:d3…    ff02::fb           MDNS       299 Standard query response 0x0000 PTR tik
3030 195.794364  172.16.102.142         224.0.0.251        MDNS        83 Standard query 0x0000 PTR _oculusal_sp
3031 195.794366  172.16.102.142         224.0.0.251        MDNS       331 Standard query response 0x0000 PTR Kai
3032 195.794368  172.16.102.67          224.0.0.251        MDNS       279 Standard query response 0x0000 PTR tik
3033 195.894265  162.159.133.234        172.16.102.148     TLSv1…     350 Application Data
3034 195.894395  172.16.102.148         162.159.133.234    TCP         54 64982 → 443 [ACK] Seq=271 Ack=52253 Wi
3035 196.203523  162.159.133.234        172.16.102.148     TLSv1…     131 Application Data
```

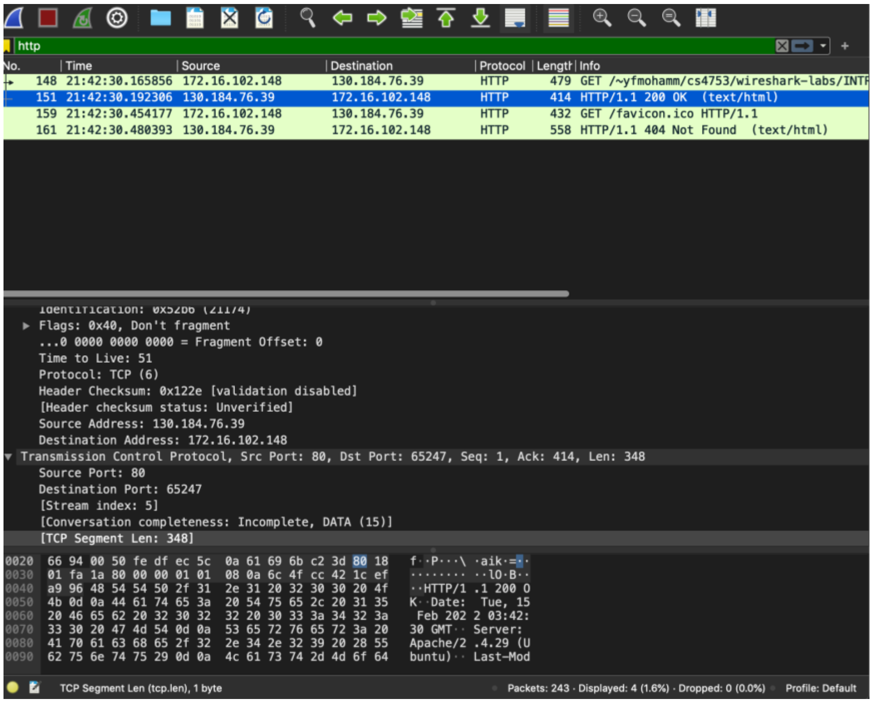
```
▶ Frame 3026: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits) on interface en0, id 0
▶ Ethernet II, Src: SamsungE_89:5d:f1 (4c:c9:5e:89:5d:f1), Dst: Apple_14:97:00 (a4:83:e7:14:97:00)
▶ Internet Protocol Version 4, Src: 172.16.102.250, Dst: 224.0.0.7
▶ User Datagram Protocol, Src Port: 8001, Dst Port: 8001
▶ Data (202 bytes)
```

```
0000  a4 83 e7 14 97 00 4c c9  5e 89 5d f1 08 00 45 00   ······L· ^·]···E·
0010  00 e6 56 d2 40 00 01 11  2f 23 ac 10 66 fa e0 00   ··V·@··· /#··f···
0020  00 07 1f 41 1f 41 00 d2  18 86 7b 22 64 61 74 61   ···A·A·· ··{"data
0030  22 3a 7b 22 76 31 22 3a  7b 22 75 72 69 22 3a 22   ":{"v1": {"uri":"
0040  68 74 74 70 3a 2f 2f 31  37 32 2e 31 36 2e 31 30   http://1 72.16.10
0050  32 2e 32 35 30 3a 38 30  30 31 2f 6d 73 2f 31 2e   2.250:80 01/ms/1.
0060  30 2f 22 7d 2c 22 76 32  22 3a 7b 22 75 72 69 22   0/"},"v2 ":{"uri"
0070  3a 22 68 74 74 70 3a 2f  2f 31 37 32 2e 31 36 2e   :"http:/ /172.16.
```

```
wireshark_Wi-FIZESIH1.pcapng          Packets: 3134 · Displayed: 3134 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

2. (5 pts.) 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*.) **Please attached a screenshot in your report**.

0.192306s – 0.165856s = 0.026450s



```
http
```

```
No.   Time             Source           Destination      Protocol  Length Info
  148 21:42:30.165856  172.16.102.148   130.184.76.39    HTTP       479 GET /~yfmohamm/cs4753/wireshark-labs/INTR
  151 21:42:30.192306  130.184.76.39    172.16.102.148   HTTP       414 HTTP/1.1 200 OK  (text/html)
  159 21:42:30.454177  172.16.102.148   130.184.76.39    HTTP       432 GET /favicon.ico HTTP/1.1
  161 21:42:30.480393  130.184.76.39    172.16.102.148   HTTP       558 HTTP/1.1 404 Not Found  (text/html)
```

```
    Identification: 0x52b6 (21174)
  ▶ Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 51
    Protocol: TCP (6)
    Header Checksum: 0x122e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 130.184.76.39
    Destination Address: 172.16.102.148
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 65247, Seq: 1, Ack: 414, Len: 348
    Source Port: 80
    Destination Port: 65247
    [Stream index: 5]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 348]
```

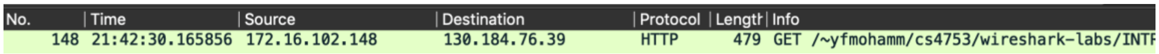
```
0020  66 94 00 50 fe df ec 5c  0a 61 69 6b c2 3d 80 18   f··P···\ ·aik·=··
0030  01 fa 1a 80 00 00 01 01  08 0a 6c 4f cc 42 1c ef   ········ ··lO·B··
0040  a9 96 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   ··HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 54 75 65 2c 20 31 35   K··Date:  Tue, 15
0060  20 46 65 62 20 32 30 32  32 20 30 33 3a 34 32 3a    Feb 202 2 03:42:
0070  33 30 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   30 GMT·· Server:
0080  41 70 61 63 68 65 2f 32  2e 34 2e 32 39 20 28 55   Apache/2 .4.29 (U
0090  62 75 6e 74 75 29 0d 0a  4c 61 73 74 2d 4d 6f 64   buntu)·· Last-Mod
```

```
TCP Segment Len (tcp.len), 1 byte          Packets: 243 · Displayed: 4 (1.6%) · Dropped: 0 (0.0%)   Profile: Default
```

3. (5 pts.) What is the Internet address of the ***csce.uark.edu***? What is the Internet address of your computer? **Please attached a screenshot in your report.**

   csce.uark.edu: 130.184.76.39

   My Computer: 172.16.102.148



No.	Time	Source	Destination	Protocol	Length	Info
148	21:42:30.165856	172.16.102.148	130.184.76.39	HTTP	479	GET /~yfmohamm/cs4753/wireshark-labs/INTR

4. (5 pts.) 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.

```
/var/folders/xx/wb15mcws2b3g36zb4mvlldr80000gn/T/wireshark_Wi-FiCKBEH1.pcapng 243 total
packets, 4 shown

No.     Time              Source              Destination           Protocol Length Info
    148 21:42:30.165856   172.16.102.148      130.184.76.39         HTTP     479    GET /
~yfmohamm/cs4753/wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 148: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface en0, id 0
Ethernet II, Src: Apple_14:97:00 (a4:83:e7:14:97:00), Dst: Routerbo_74:9c:fe (d4:ca:6d:74:9c:fe)
    Destination: Routerbo_74:9c:fe (d4:ca:6d:74:9c:fe)
    Source: Apple_14:97:00 (a4:83:e7:14:97:00)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.102.148, Dst: 130.184.76.39
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))
    Total Length: 465
    Identification: 0x0000 (0)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x57a1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.102.148
    Destination Address: 130.184.76.39
Transmission Control Protocol, Src Port: 65247, Dst Port: 80, Seq: 1, Ack: 1, Len: 413
    Source Port: 65247
    Destination Port: 80
    [Stream index: 5]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 413]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1768669344
    [Next Sequence Number: 414    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3965454945
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
    Window: 2058
    [Calculated window size: 131712]
    [Window size scaling factor: 64]
    Checksum: 0xe473 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (413 bytes)
Hypertext Transfer Protocol
    GET /~yfmohamm/cs4753/wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: csce.uark.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/605.1.15 (KHTML,
like
Gecko) Version/14.1.2 Safari/605.1.15\r\n
   Accept-Language: en-us\r\n
   Accept-Encoding: gzip, deflate\r\n
   Connection: keep-alive\r\n

\r\n

   [Full request URI: http://csce.uark.edu/~yfmohamm/cs4753/wireshark-labs/INTRO-wireshark-
file1.html]
   [HTTP request 1/1]
   [Response in frame: 151]
No.     Time              Source                Destination           Protocol Length Info

/var/folders/xx/wb15mcws2b3g36zb4mvlldr80000gn/T/wireshark_Wi-FiCKBEH1.pcapng 243 total
packets, 4 shown

   151 21:42:30.192306    130.184.76.39         172.16.102.148        HTTP     414    HTTP/1.1
200 OK  (text/html)
Frame 151: 414 bytes on wire (3312 bits), 414 bytes captured (3312 bits) on interface en0, id 0
Ethernet II, Src: Routerbo_74:9c:fe (d4:ca:6d:74:9c:fe), Dst: Apple_14:97:00 (a4:83:e7:14:97:00)
   Destination: Apple_14:97:00 (a4:83:e7:14:97:00)
   Source: Routerbo_74:9c:fe (d4:ca:6d:74:9c:fe)
   Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 130.184.76.39, Dst: 172.16.102.148
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 400
   Identification: 0x52b6 (21174)
   Flags: 0x40, Don't fragment
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 51
   Protocol: TCP (6)
   Header Checksum: 0x122e [validation disabled]
   [Header checksum status: Unverified]
```

```
    Source Address: 130.184.76.39
    Destination Address: 172.16.102.148
Transmission Control Protocol, Src Port: 80, Dst Port: 65247, Seq: 1, Ack: 414, Len: 348
    Source Port: 80
    Destination Port: 65247
    [Stream index: 5]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 348]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3965454945
    [Next Sequence Number: 349    (relative sequence number)]
    Acknowledgment Number: 414    (relative ack number)
    Acknowledgment number (raw): 1768669757
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
    Window: 506
    [Calculated window size: 64768]
    [Window size scaling factor: 128]
    Checksum: 0x1a80 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (348 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 15 Feb 2022 03:42:30 GMT\r\n
    Server: Apache/2.4.29 (Ubuntu)\r\n
    Last-Modified: Thu, 28 Jan 2021 15:25:10 GMT\r\n
    ETag: "41-5b9f77e4efb71"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 65\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.026450000 seconds]
    [Request in frame: 148]
    [Request URI: http://csce.uark.edu/~yfmohamm/cs4753/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 65 bytes
Line-based text data: text/html (1 lines)
```