

Please organise your work next time.

Moudie Alhoushan

Lab #1

What to hand in

For each of these question, take a screen shot and add attach it to your answer. Also, save your Wireshark lab file. We would use it later in the class.

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. What is the Internet address of your computer?
2. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
3. 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*.)
4. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)?
5. 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.

Don't forget to save your Wireshark Lab file.

① src: 192.168.1.182, Dst: 128.119.245.12

② ARP ✓
GQUIC ✓
TCP ✓
DNS ✓
TLSv1 ✓

requested for only 3.

③ 14:40:37.109495
14:40:37.131557

you didn't calculate

④

Please type.
Print
next time.

reshark · Packet 650 · Wi-Fi

Frame 650: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface 0
 Ethernet II, Src: IntelCor_c5:a0:c6 (00:e1:8c:c5:a0:c6), Dst: Verizon_a8:f8:d6 (48:5d:36:a8:f8:d6)
 Internet Protocol Version 4, Src: 192.168.1.182, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 57133, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
 Hypertext Transfer Protocol

```

0 48 5d 36 a8 f8 d6 00 e1 8c c5 a0 c6 08 00 45 00 HJ6.....E.
0 01 d3 63 8e 40 00 80 06 5d b4 c0 a8 01 b6 80 77 .c.@... ].....w
0 f5 0c df 2d 00 50 ad 2a 2a 2a 32 3b 31 72 50 18 ....P.* **2;1rp.
0 00 44 4d ab 00 00 47 45 54 20 2f 77 69 72 65 73 .DM...GE T /wires
0 68 61 72 6b 2d 6c 61 62 73 2f 69 6e 74 72 6f 2d hark-lab s/intro-
0 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.
0 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HTTP/1.1..H
0 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.cs.uma
0 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 ss.edu.. Connecti
0 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep -alive..
0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade- Insecure
0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 -Request s: 1..Us
0 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill
0 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W indows N
0 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; Win64; x
    
```

```

3 47 45 54 20 2f 77 69 72 65 73 .DM...GE T /wires
3 61 62 73 2f 69 6e 74 72 6f 2d hark-lab s/intro-
3 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.
    
```

-3E0F-4D64-858E-B50969B7A4B9_20180901185728_a11544.pcapng

Packets: 2017 · Displayed: 32 (1.6%) · Dropped: 0

Close

Help

search





Source Destination Protocol Length Info

192.168.1.182	192.168.8.101	TCP	66	[TCP Retransmission] 57132 → 3911 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=
192.168.1.182	192.168.1.1	DNS	77	Standard query 0xc8f4 A gaia.cs.umass.edu
192.168.1.182	8.18.25.18	TLSv1	395	Application Data
192.168.1.182	128.119.245.12	TCP	66	57133 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.182	128.119.245.12	TCP	66	57134 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.182	128.119.245.12	TCP	54	57133 → 80 [ACK] Seq=1 Ack=1 Win=17408 Len=0
192.168.1.182	128.119.245.12	HTTP	481	GET /wireshark-labs/intro-wireshark-file1.html HTTP/1.1
192.168.1.182	128.119.245.12	TCP	54	57134 → 80 [ACK] Seq=1 Ack=1 Win=17408 Len=0

on wire (3848 bits), 481 bytes captured (3848 bits) on interface 0

telCor_c5:a0:c6 (00:e1:8c:c5:a0:c6), Dst: Verizon_a8:f8:d6 (48:5d:36:a8:f8:d6)

rsion 4, Src: 192.168.1.182, Dst: 128.119.245.12

Protocol, Src Port: 57133, Dst Port: 80, Seq: 1, Ack: 1, Len: 427

protocol

```

5 00 e1 8c c5 a0 c6 08 00 45 00 H]6.....E.
3 80 06 5d b4 c0 a8 01 b6 80 77 ..c@... ].....w
3 ad 2a 2a 2a 32 3b 31 72 50 18 ....P.* **2;1rP.
3 47 45 54 20 2f 77 69 72 65 73 DM...GE T /wires
3 61 62 73 2f 69 6e 74 72 6f 2d hark-lab s/intro-
3 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.

```





Source	Destination	Protocol	Length	Info
192.168.1.182	128.119.245.12	HTTP	481	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
128.119.245.12	192.168.1.182	HTTP	492	HTTP/1.1 200 OK (text/html)
192.168.1.182	128.119.245.12	HTTP	452	GET /favicon.ico HTTP/1.1
128.119.245.12	192.168.1.182	HTTP	538	HTTP/1.1 404 Not Found (text/html)

s on wire (3848 bits), 481 bytes captured (3848 bits) on interface 0
telCor_c5:a0:c6 (00:e1:8c:c5:a0:c6), Dst: Verizon_a8:f8:d6 (48:5d:36:a8:f8:d6)
rsion 4, Src: 192.168.1.182, Dst: 128.119.245.12

Protocol, Src Port: 50138, Dst Port: 80, Seq: 1, Ack: 1, Len: 427

protocol

```

5 00 e1 8c c5 a0 c6 08 00 45 00 H]6.....E.
3 80 06 a0 6c c0 a8 01 b6 80 77 ..@...l....w
3 ca 75 ed 68 c2 dd 2e 64 50 18 .....P.u.h...dp.
3 47 45 54 20 2f 77 69 72 65 73 D[ ..GE T /wires
3 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-
3 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.

```



No.	Time	Source	Destination	Protocol	Length	Info
1239	14:40:37.109495	192.168.1.182	128.119.245.12	HTTP	481	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 1239: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface 0
Interface id: 0 (\Device\NPF_{32FF1456-3E0F-4D64-858E-B50969B7A4B9})
Encapsulation type: Ethernet (1)
Arrival Time: Aug 30, 2018 14:40:37.109495000 Eastern Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1535654437.109495000 seconds
[Time delta from previous captured frame: 0.000167000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 204.267339000 seconds]
Frame Number: 1239
Frame Length: 481 bytes (3848 bits)
Capture Length: 481 bytes (3848 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: IntelCor_c5:a0:c6 (00:e1:8c:c5:a0:c6), Dst: Verizon_a8:f8:d6 (48:5d:36:a8:f8:d6)
Internet Protocol Version 4, Src: 192.168.1.182, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50138, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
Source Port: 50138
Destination Port: 80
[Stream index: 21]
[TCP Segment Len: 427]
Sequence number: 1 (relative sequence number)
[Next sequence number: 428 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 68
[Calculated window size: 17408]
[Window size scaling factor: 256]
Checksum: 0x5b20 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (427 bytes)
Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
1244	14:40:37.131557	128.119.245.12	192.168.1.182	HTTP	492	HTTP/1.1 200 OK (text/html)

Frame 1244: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Interface id: 0 (\Device\NPF_{32FF1456-3E0F-4D64-858E-B50969B7A4B9})
Encapsulation type: Ethernet (1)
Arrival Time: Aug 30, 2018 14:40:37.131557000 Eastern Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1535654437.131557000 seconds
[Time delta from previous captured frame: 0.000897000 seconds]
[Time delta from previous displayed frame: 0.022062000 seconds]
[Time since reference or first frame: 204.289401000 seconds]
Frame Number: 1244
Frame Length: 492 bytes (3936 bits)
Capture Length: 492 bytes (3936 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Verizon_a8:f8:d6 (48:5d:36:a8:f8:d6), Dst: IntelCor_c5:a0:c6 (00:e1:8c:c5:a0:c6)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.182
Transmission Control Protocol, Src Port: 80, Dst Port: 50138, Seq: 1, Ack: 428, Len: 438
Source Port: 80
Destination Port: 50138
[Stream index: 21]
[TCP Segment Len: 438]
Sequence number: 1 (relative sequence number)
[Next sequence number: 439 (relative sequence number)]
Acknowledgment number: 428 (relative ack number)
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 237
[Calculated window size: 30336]
[Window size scaling factor: 128]
Checksum: 0x2e64 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (438 bytes)
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)