

Faisal Alwayli

Lab 1

IT-520

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.

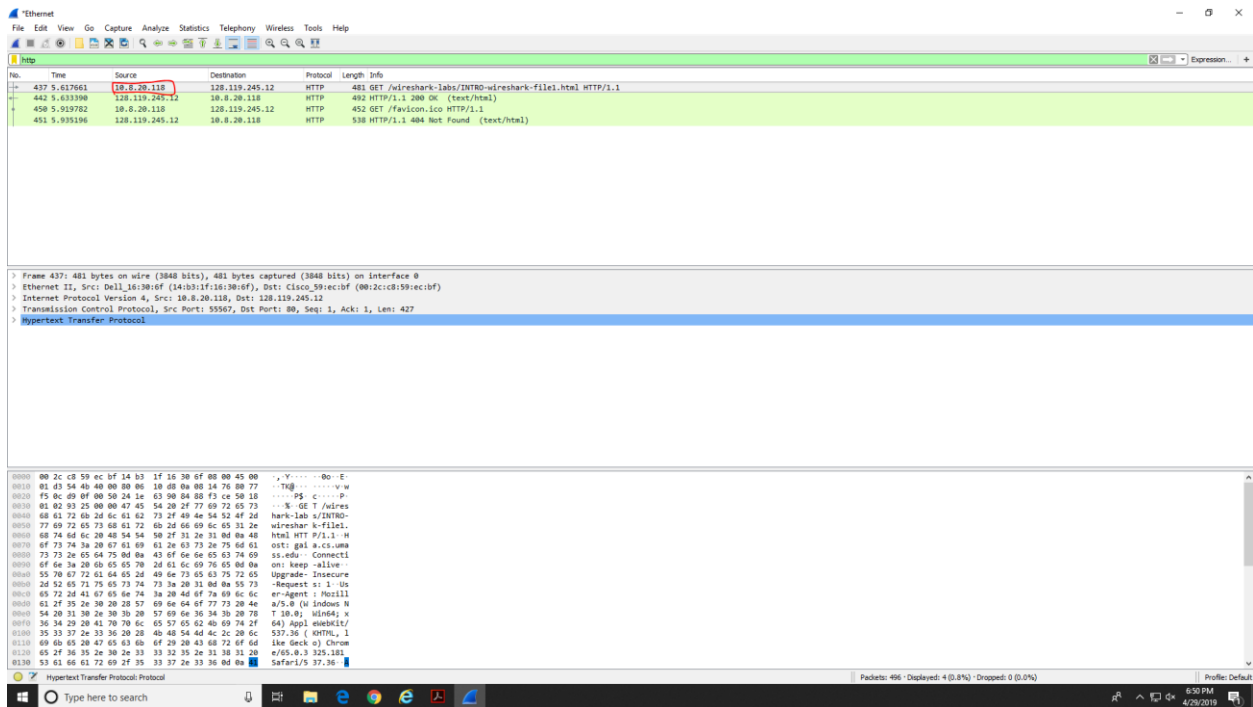
The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

- (For each of these questions, take a screenshot of Wireshark, and attach it to your answer) - Questions without Full Screenshot will not be graded. A lab submission template is available on canvas. Your screenshot should indicate the time and date on your computer.
- Include a terminal screenshot showing computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.

Labs will NOT be graded if either of these two is missing.

Questions:

1. What is the Internet address of your computer?



- List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
 - http
 - tcp
 - arp
- 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.)

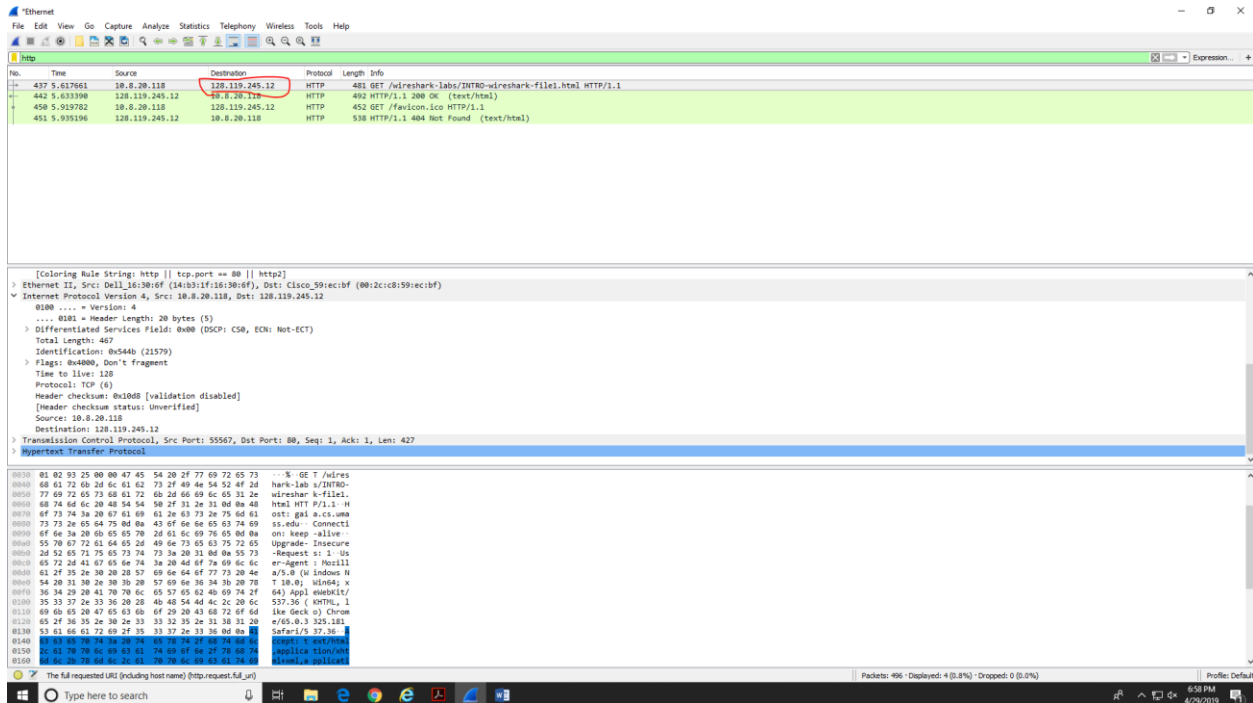
Wireshark packet capture showing an HTTP GET request to /INTRO-wireshark-File1.html. The packet list shows three HTTP packets. The packet details pane shows the structure of the HTTP request, including the GET method, the URL, and the User-Agent string. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
437	5.613661	10.8.20.118	128.119.245.12	HTTP	481	GET /wireshark-labs/INTRO-wireshark-File1.html HTTP/1.1
438	5.613390	128.119.245.12	10.8.20.118	HTTP	492	HTTP/1.1 200 OK (text/html)
439	5.701972	10.8.20.118	128.119.245.12	HTTP	452	GET /Textbook-Intro-Intro-...
451	5.935106	128.119.245.12	10.8.20.118	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 437: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on Interface 0
> Ethernet II, Src: Dell_14_3816ff (14:3b:b1:16:38:1f), Dst: Cisco_99:ec:b1 (08:00:0c:28:ec:b1)
> Internet Protocol Version 4, Src: 10.8.20.118, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55567, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
> Hypertext Transfer Protocol

0000 00 2c c8 59 ec bf 14 b3 1f 16 30 0f 00 00 45 00 .Y.....0oE:
0010 01 43 54 4b 40 00 00 06 10 d8 0a 00 14 76 00 77 ..TQ.....v w
0020 f5 8c 49 0f 00 50 24 1e 63 90 04 00 f5 ce 50 18 ..PS.....P
0030 01 02 93 25 00 00 47 45 54 20 2f 7f 69 72 65 73 ..%GE T/wires
0040 68 61 72 65 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-
0050 77 69 72 65 73 68 61 72 6b 2d 46 69 6e 65 31 2a wireshar k-File1.
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 00 0a 40 html HT P/1.1: H
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 out: gal a.cs-um
0080 73 73 2e 65 64 75 0d 0a 43 0f 6e 6e 65 63 74 69 ss.edu: Connecti
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep-alive:
00a0 35 78 67 73 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade: Insecure
00b0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 -Request si: 1: Us
00c0 65 72 2d 41 67 65 6e 7a 20 4d 6f 7a 69 6c 6c en-Agent: Mozilla
00d0 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (i ndows N
00e0 54 20 31 30 2e 30 30 20 57 69 6e 36 36 30 20 78 T 10.0; Win64; x
00f0 36 34 28 20 41 70 70 6c 65 57 65 62 40 69 74 2f 6a) Appl etics/1
0100 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 527.36 (KHTML, 1
0110 69 6b 65 20 47 65 63 6f 6f 20 20 43 68 72 6f 6d lse deck o) Chrom
0120 65 2f 36 35 2e 30 2e 33 33 32 35 2e 31 30 31 20 e/65.0.3 25.185
0130 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a Safari/5 37.36

4. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)?



- 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

