Lab 2 | lab4 | lab2

Command Prompt — My IP address

```
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : hsd1.va.comcast.net
   IPv6 Address. . . . . . . . . . . : 2601:140:8f00:8c0::ec7e
   IPv6 Address. . . . . . . . . . . : 2601:140:8f00:8c0:499a:f6d6:8fa8:97ca
   Temporary IPv6 Address. . . . . . : 2601:140:8f00:8c0:d5b1:b155:75f1:d952
   Link-local IPv6 Address . . . . . : fe80::499a:f6d6:8fa8:97ca%6
   IPv4 Address. . . . . . . . . . . : 10.0.0.170
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::d6ab:82ff:fe36:5e42%6
                                       10.0.0.1

Ethernet adapter Bluetooth Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Guamaral>
```

orks

section.

ark, and attach it to your
graded. A lab submission
ndicate the time and date

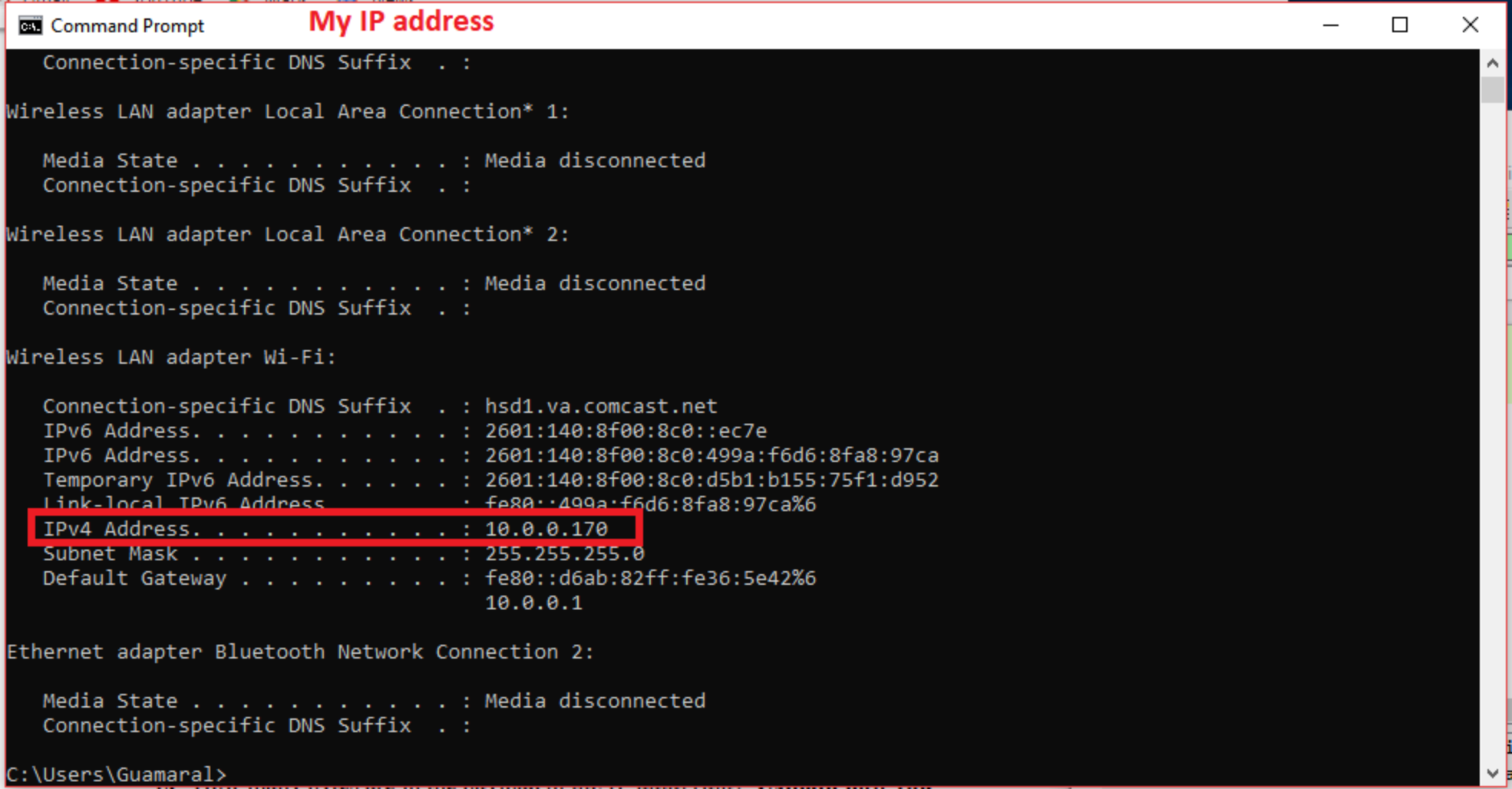
ss on the front page
ssage as the last page.

creenshot not,

5. How many bytes are in the payload *of the IP datagram*? **Explain how you determined the number of payload bytes.**

Type here to search

9:39 AM
3/18/2019


Command Prompt
My IP address
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : hsd1.va.comcast.net
IPv6 Address. . . . . : 2601:140:8f00:8c0::ec7e
IPv6 Address. . . . . : 2601:140:8f00:8c0:499a:f6d6:8fa8:97ca
Temporary IPv6 Address. . . . . : 2601:140:8f00:8c0:d5b1:b155:75f1:d952
Link-local IPv6 Address . . . . . : fe80::499a:f6d6:8fa8:97ca%6
IPv4 Address. . . . . : 10.0.0.170
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::d6ab:82ff:fe36:5e42%6
10.0.0.1
Ethernet adapter Bluetooth Network Connection 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\Guamaral>

Course Roster: 19/SP Technolog | lab4 | lab2

File | C:/Users/Guamaral/Downloads/lab4%20(2).pdf

Apps Gmail YouTube Maps News

IT 520-A – Enterprise Infrastructure & Networks

Instructions:

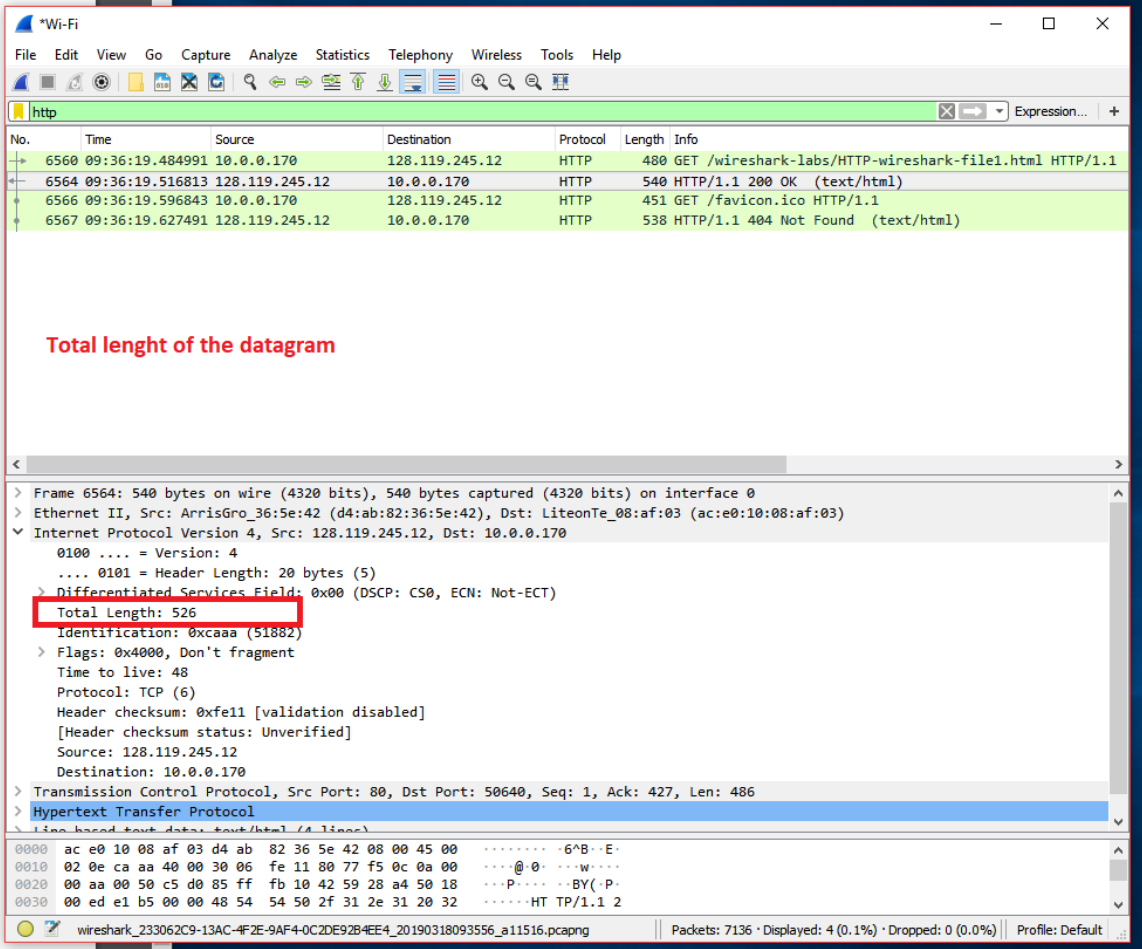
- Follow the instructions in Lab 2 and expand the IP detail section.
- Pay attention to the text in bold. I expect you to explain?

- (*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.

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

Questions:

1. What is the IP address of your computer? – **Wireshark screenshot not, Terminal**
2. What is the total length of the datagram?
3. Has this IP datagram been fragmented?
4. How many bytes are in the IP header?
5. How many bytes are in the payload *of the IP datagram*? **Explain how you determined the number of payload bytes.**



Type here to search

9:50 AM
3/18/2019

Course Roster: 19/SP Technolog | lab4 | lab2

File | C:/Users/Guamaral/Downloads/lab4%20(2).pdf

Apps Gmail YouTube Maps News

lab4 1 / 1

Instructions:

- Follow the instructions in Lab 2 and expand the IP detail section.
- Pay attention to the text in bold. I expect you to explain?

- (*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.

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

Questions:

1. What is the IP address of your computer? – **Wireshark screenshot not, Terminal**
2. What is the total length of the datagram?
3. Has this IP datagram been fragmented?
4. How many bytes are in the IP header?
5. How many bytes are in the payload *of the IP datagram*? **Explain how you determined the number of payload bytes.**

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http Expression...

No.	Time	Source	Destination	Protocol	Length	Info
6560	09:36:19.484991	10.0.0.170	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
6564	09:36:19.516813	128.119.245.12	10.0.0.170	HTTP	540	HTTP/1.1 200 OK (text/html)
6566	09:36:19.596843	10.0.0.170	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
6567	09:36:19.627491	128.119.245.12	10.0.0.170	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Has this IP datagram fragmented?

```
> Ethernet II, Src: ArrisGro_36:5e:42 (d4:ab:82:36:5e:42), Dst: LiteonTe_08:af:03 (ac:e0:10:08:af:03)
v Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.170
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 526
    Identification: 0xcaaa (51882)
  > Flags: 0x4000, Don't fragment
    Time to live: 48
    Protocol: TCP (6)
    Header checksum: 0xfe11 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 10.0.0.170
> Transmission Control Protocol, Src Port: 80, Dst Port: 50640, Seq: 1, Ack: 427, Len: 486
> Hypertext Transfer Protocol
> Line-based text data: text/html (4 lines)
```

```
0000  ac e0 10 08 af 03 d4 ab  82 36 5e 42 08 00 45 00   ........ .6^B..E.
0010  02 0e ca aa 40 00 30 06  fe 11 80 77 f5 0c 0a 00   ....@.0. ...w....
0020  00 aa 00 50 c5 d0 85 ff  fb 10 42 59 28 a4 50 18   ...P.... ..BY(.P.
0030  00 ed e1 b5 00 00 48 54  54 50 2f 31 2e 31 20 32   ......HT TP/1.1 2
```

wireshark_233062C9-13AC-4F2E-9AF4-0C2DE92B4EE4_20190318093556_a11516.pcapng | Packets: 7136 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

Type here to search

9:53 AM
3/18/2019

Course Roster: 19/SP Technolog | lab4 | lab2

File | C:/Users/Guamaral/Downloads/lab4%20(2).pdf

Apps Gmail YouTube Maps News

IT 520-A – Enterprise Infrastructure & Networks

Instructions:

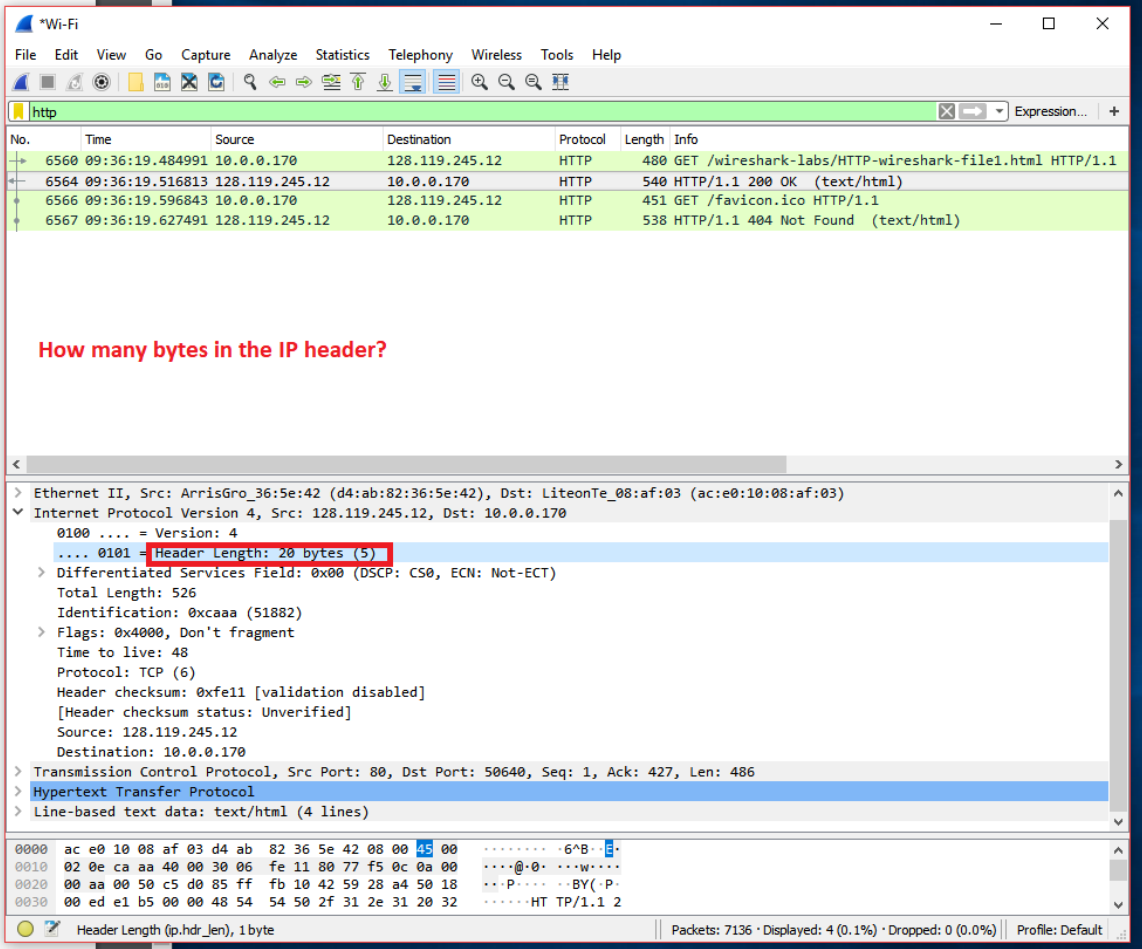
- Follow the instructions in Lab 2 and expand the IP detail section.
- Pay attention to the text in bold. I expect you to explain?

- (*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.

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

Questions:

1. What is the IP address of your computer? – **Wireshark screenshot not, Terminal**
2. What is the total length of the datagram?
3. Has this IP datagram been fragmented?
4. How many bytes are in the IP header?
5. How many bytes are in the payload *of the IP datagram*? **Explain how you determined the number of payload bytes.**



Type here to search

9:55 AM
3/18/2019

Course Roster: 19/SP Technolog | lab4 | lab2

File | C:/Users/Guamaral/Downloads/lab4%20(2).pdf

Apps Gmail YouTube Maps News

lab4 1 / 1

Instructions:

- Follow the instructions in Lab 2 and expand the IP detail section.
- Pay attention to the text in bold. I expect you to explain?

- (*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.

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

Questions:

1. What is the IP address of your computer? – **Wireshark screenshot not, Terminal**
2. What is the total length of the datagram?
3. Has this IP datagram been fragmented?
4. How many bytes are in the IP header?
5. How many bytes are in the payload *of the IP datagram*? **Explain how you determined the number of payload bytes.**

Total length 526
Header lenght (20)
Payload bytes = 506

506 bytes are in the payload of the IP datagram

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http Expression...

No.	Time	Source	Destination	Protocol	Length	Info
6560	09:36:19.484991	10.0.0.170	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
6564	09:36:19.516813	128.119.245.12	10.0.0.170	HTTP	540	HTTP/1.1 200 OK (text/html)
6566	09:36:19.596843	10.0.0.170	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
6567	09:36:19.627491	128.119.245.12	10.0.0.170	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
> Ethernet II, Src: ArrisGro_36:5e:42 (d4:ab:82:36:5e:42), Dst: LiteonTe_08:af:03 (ac:e0:10:08:af:03)
v Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.170
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 526
    Identification: 0xcaaa (51882)
  > Flags: 0x4000, Don't fragment
    Time to live: 48
    Protocol: TCP (6)
    Header checksum: 0xfe11 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 10.0.0.170
> Transmission Control Protocol, Src Port: 80, Dst Port: 50640, Seq: 1, Ack: 427, Len: 486
> Hypertext Transfer Protocol
> Line-based text data: text/html (4 lines)
```

```
0010  02 0e ca aa 40 00 30 06  fe 11 80 77 f5 0c 0a 00   ····@·0· ···w····
0020  00 aa 00 50 c5 d0 85 ff  fb 10 42 59 28 a4 50 18   ···P···· ··BY(·P·
0030  00 ed e1 b5 00 00 48 54  54 50 2f 31 2e 31 20 32   ·····HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D ate: Mon
```

Total Length (ip.len), 2 bytes | Packets: 7136 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

Type here to search

9:56 AM
3/18/2019

Course Roster: 19/SP Technolog | lab4 | lab2

File | C:/Users/Guamaral/Downloads/lab2%20(2).pdf

Apps Gmail YouTube Maps News

Instructions:

1. Part 1: Start up your web browser.
2. Start up the Wireshark packet sniffer, as described in the Introductory lab (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
3. Wait a bit more than one minute (we'll see why shortly), and then begin Wireshark packet capture.
4. Enter the following to your browser: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
5. Stop Wireshark packet capture.

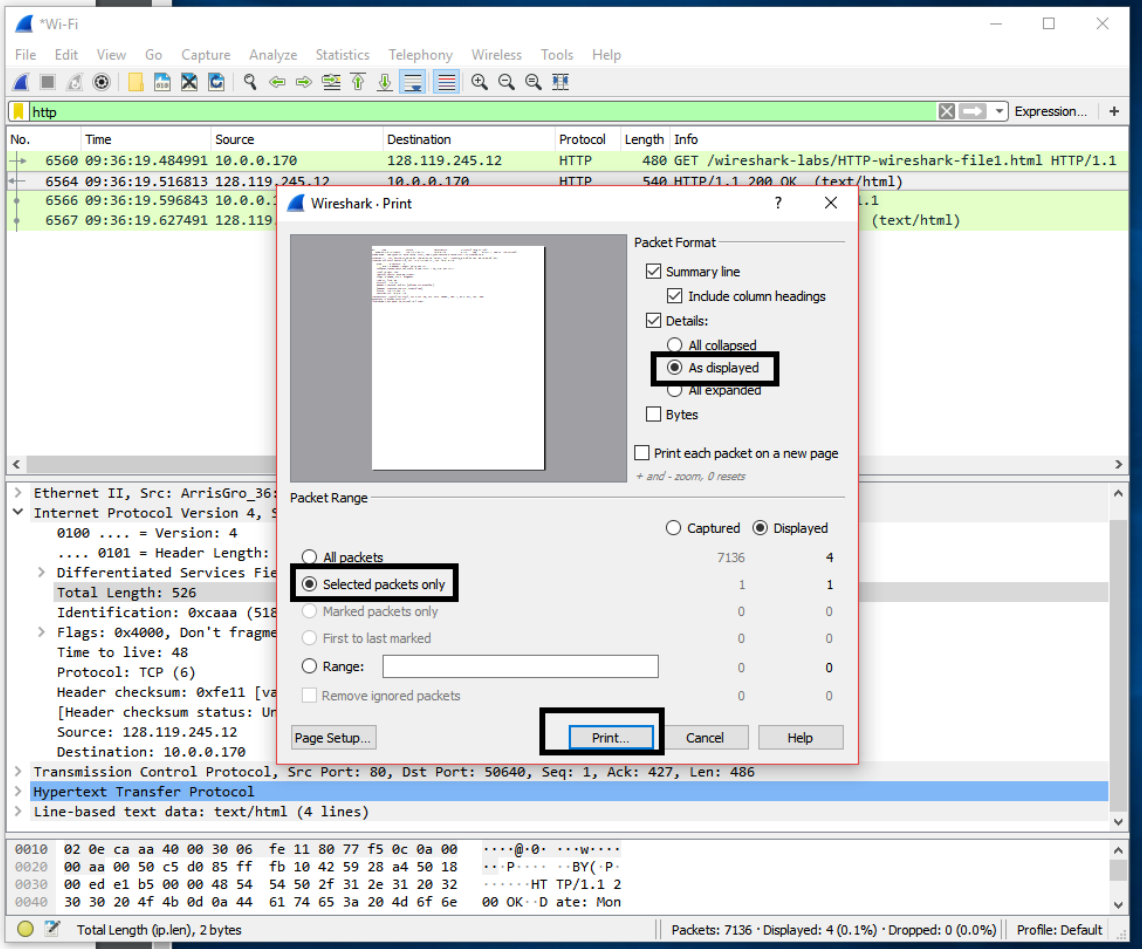
- (*For each of these questions, take a screenshot of Wireshark, and attach it to your answer*) - Questions without Full Screenshot will not be graded. A lab submission template is available on canvas. Your screenshot should indicate the time and date on your computer.
- Include a terminal screenshot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

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

Questions:

1. Is your browser running HTTP version 1.0 or 1.1?
2. When was the HTML file that you are retrieving last modified at the server?
3. What is the IP address of the gaia.cs.umass.edu server?
4. What languages does your browser indicate that it can accept to the server?
5. When was the HTML file that you are retrieving created at the server?

Don't forget to save your Wireshark Lab file.



Type here to search

9:58 AM
3/18/2019