Moudie Alhousainan

Wireshark Lab 3 - TCP

IT 520-A – Enterprise Infrastructure & Networks
Due Date: 09/24/18 (Handed in at the beginning of class)

Instructions:

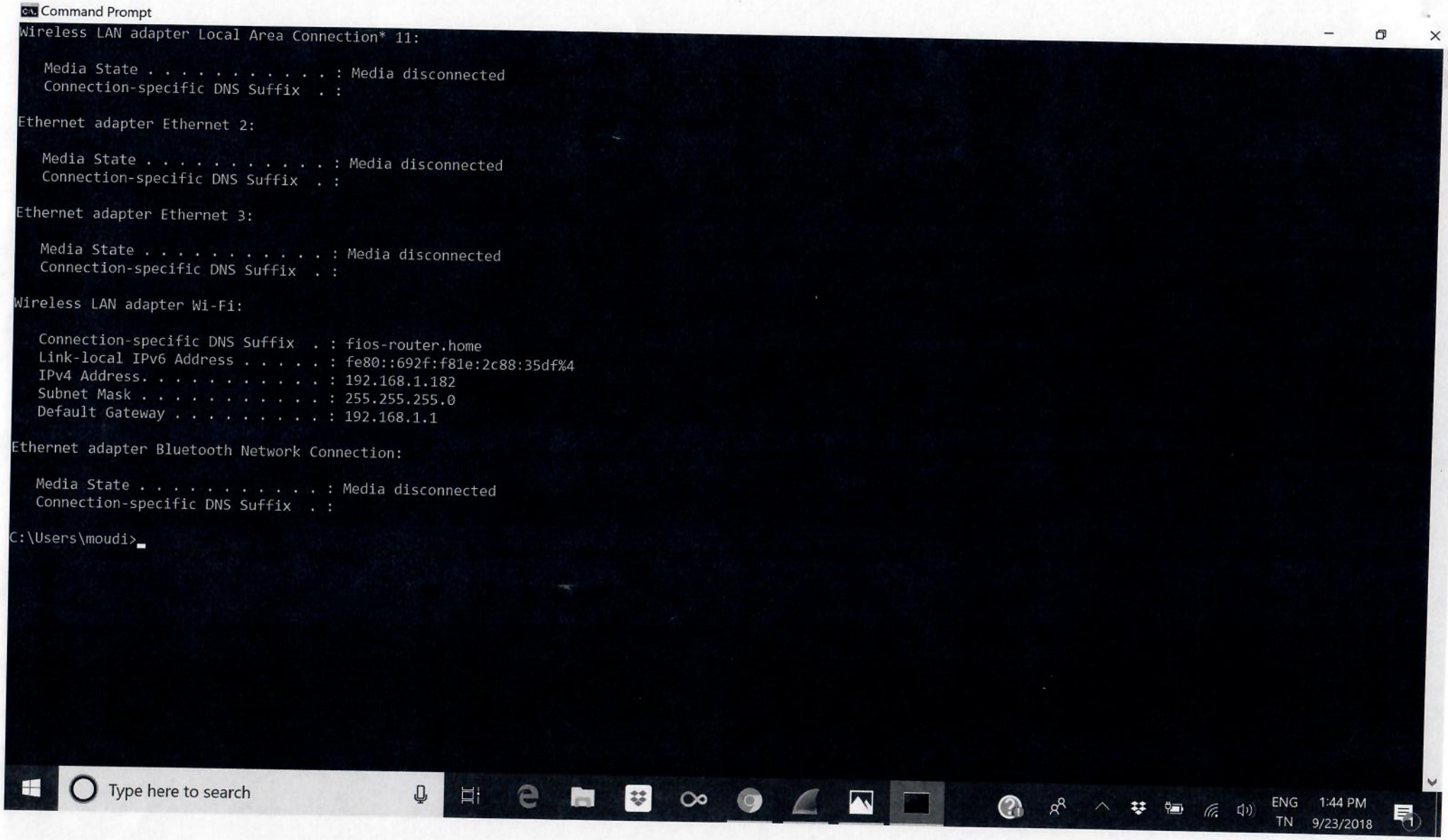
- Start up your web browser. Go the http://gaia.cs.umass.edu/wireshark-labs/alice.txt and retrieve an ASCII copy of *Alice in Wonderland.* Save this file somewhere on your computer.
- Next go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.
- Use the *Browse* button in this form to enter the name of the file (full path name) on your computer containing *Alice in Wonderland* (or do so manually). Don't yet press the "*Upload alice.txt file*" button.
- Now start up Wireshark and begin packet capture *(Capture->Start)* and then press *OK* on the Wireshark Packet Capture Options screen (we'll not need to select any options here).
- Returning to your browser, press the "*Upload alice.txt file*" button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.
- Stop Wireshark packet capture and filter tcp packets.
- Pay attention to the SYN ACK packets.
- 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. (You can refer to Lab 1 for instructions on how to PRINT

Questions:

(*For each of these questions, take a screenshot of Wireshark, and attach it to your answer*) - Questions without Full Screenshot will not be graded. Your screenshot should indicate the time and date on your computer.

1. What is the TCP port number used by your computer to communicate with gaia.cs.umass.edu?
2. What is the TCP port number used by gaia.cs.umass.edu to communicate with your computer?
3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between your computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?
4. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? - You must dig deep and find the ACK from gaia.cs.umass.edu.
5. What is the sequence number of the TCP segment containing the HTTP POST command? Note: that to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

Moudie Alhou jinan



Q # 1

lab3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
2	22:51:16.648469	192.168.1.182	192.168.8.101	TCP	66	60695 → 3911 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
30	22:51:25.026891	192.168.1.182	192.168.1.1	TCP	66	60696 → 58589 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
31	22:51:25.034382	192.168.1.1	192.168.1.182	TCP	66	58589 → 60696 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=32
32	22:51:25.034494	192.168.1.182	192.168.1.1	TCP	54	60696 → 58589 [ACK] Seq=1 Ack=1 Win=65536 Len=0
33	22:51:25.034673	192.168.1.182	192.168.1.1	HTTP	251	GET /rootDesc.xml HTTP/1.1
34	22:51:25.042622	192.168.1.1	192.168.1.182	TCP	60	58589 → 60696 [ACK] Seq=1 Ack=198 Win=15680 Len=0
35	22:51:25.043547	192.168.1.1	192.168.1.182	TCP	1514	58589 → 60696 [ACK] Seq=1 Ack=198 Win=15680 Len=1460 [TCP segment of a reassembled PDU]
36	22:51:25.043764	192.168.1.1	192.168.1.182	HTTP/...	1375	HTTP/1.1 200 OK
37	22:51:25.043764	192.168.1.1	192.168.1.182	TCP	60	58589 → 60696 [FIN, ACK] Seq=2782 Ack=198 Win=15680 Len=0
38	22:51:25.043816	192.168.1.182	192.168.1.1	TCP	54	60696 → 58589 [ACK] Seq=198 Ack=2783 Win=65536 Len=0
39	22:51:25.043940	192.168.1.182	192.168.1.1	TCP	54	60696 → 58589 [FIN, ACK] Seq=198 Ack=2783 Win=65536 Len=0
40	22:51:25.049460	192.168.1.1	192.168.1.182	TCP	60	58589 → 60696 [ACK] Seq=2783 Ack=199 Win=15680 Len=0
62	22:51:37.202140	192.168.1.182	128.119.245.12	TCP	55	60688 → 80 [ACK] Seq=1 Ack=1 Win=253 Len=1

Expression...

```
> Frame 30: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 192.168.1.1
v Transmission Control Protocol, Src Port: 60696, Dst Port: 58589, Seq: 0, Len: 0
    Source Port: 60696
    Destination Port: 58589
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 64240
```

This destination is not gaia.cs.umass.edu.

```
0000  48 5d 36 a8 f8 d6 00 e1  8c c5 a0 c6 08 00 45 00   H]6·····  ·····E·
```

Ready to load or capture

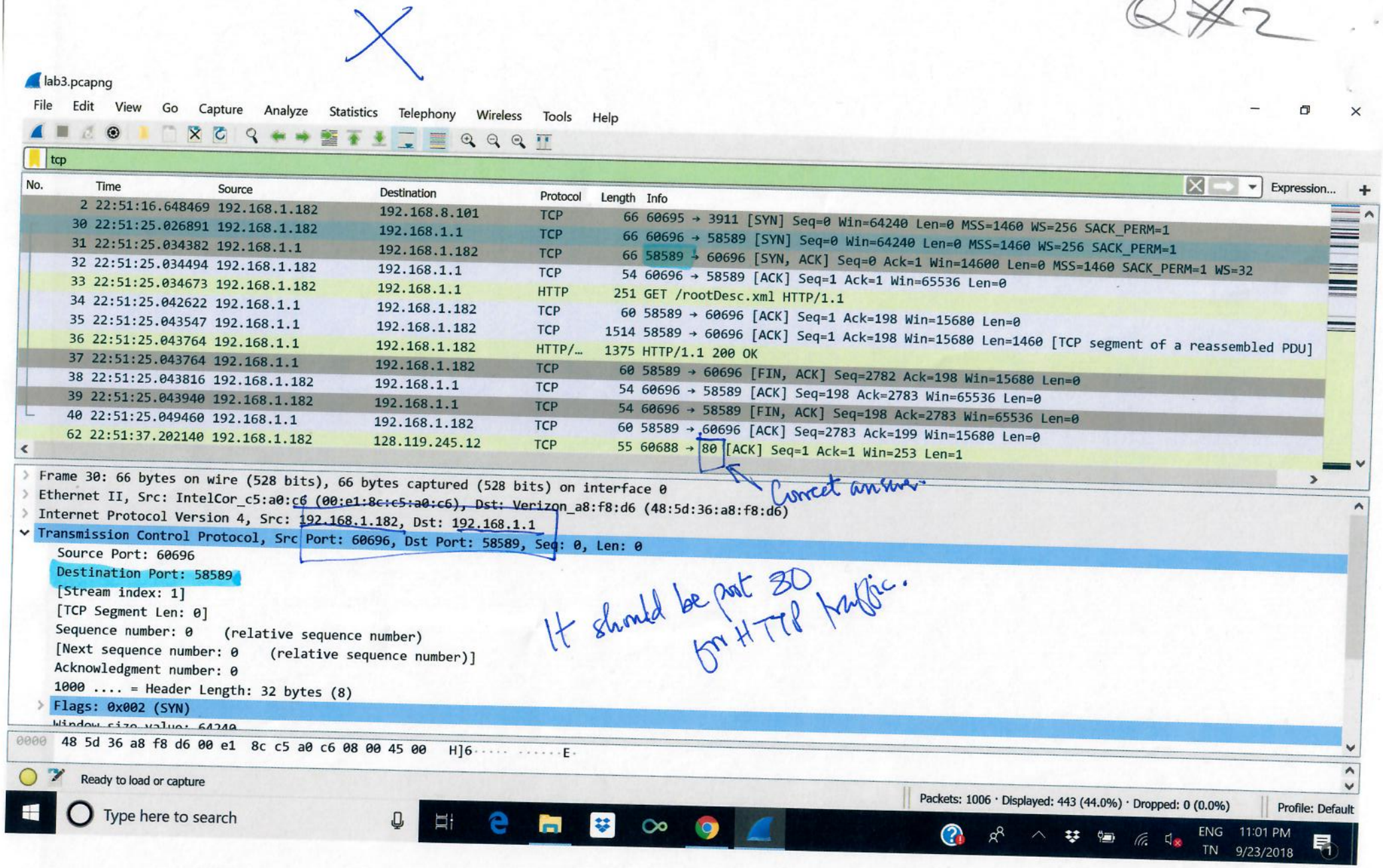
Packets: 1006 · Displayed: 443 (44.0%) · Dropped: 0 (0.0%)

Profile: Default

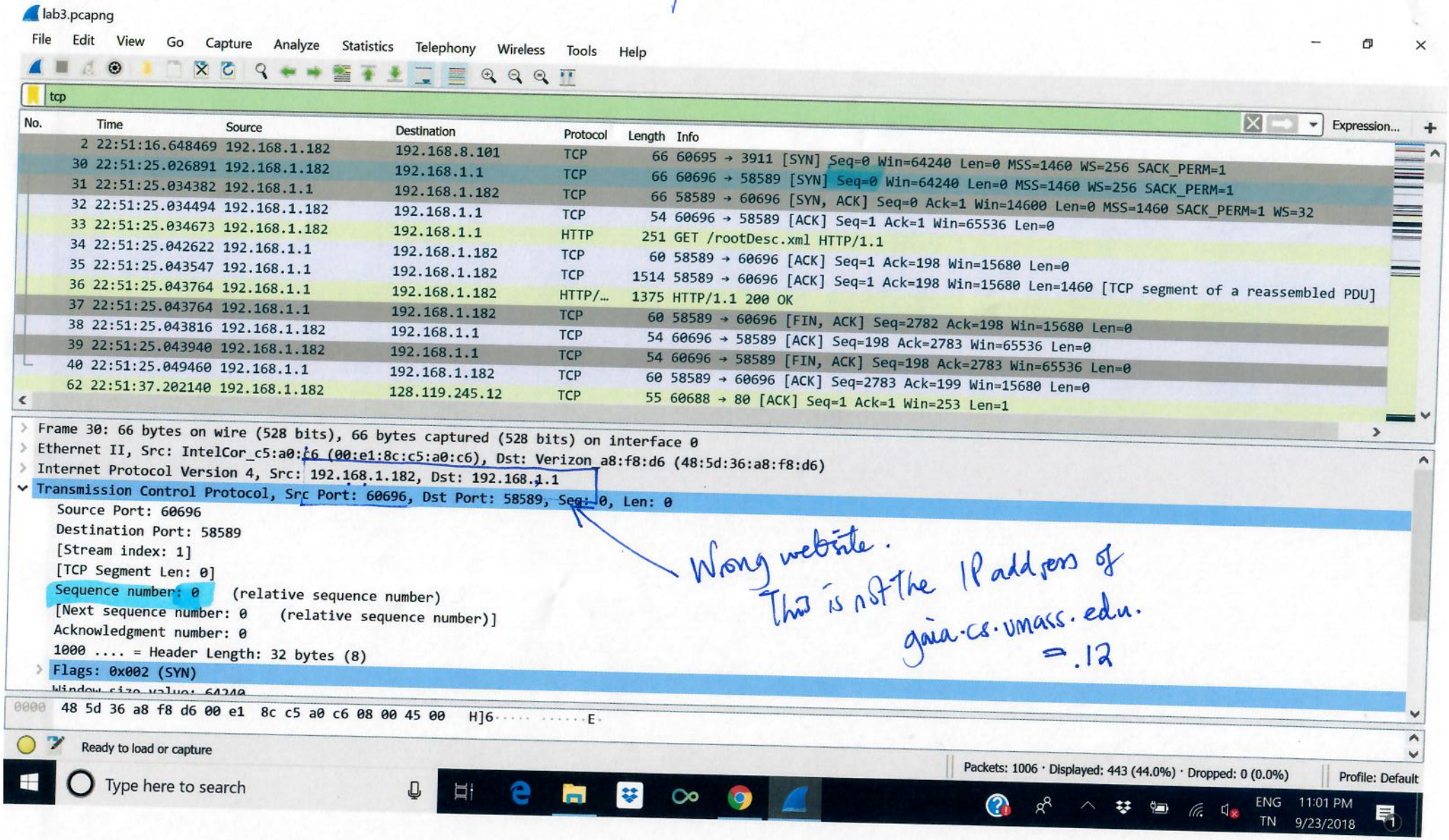
Type here to search

ENG TN 11:01 PM 9/23/2018

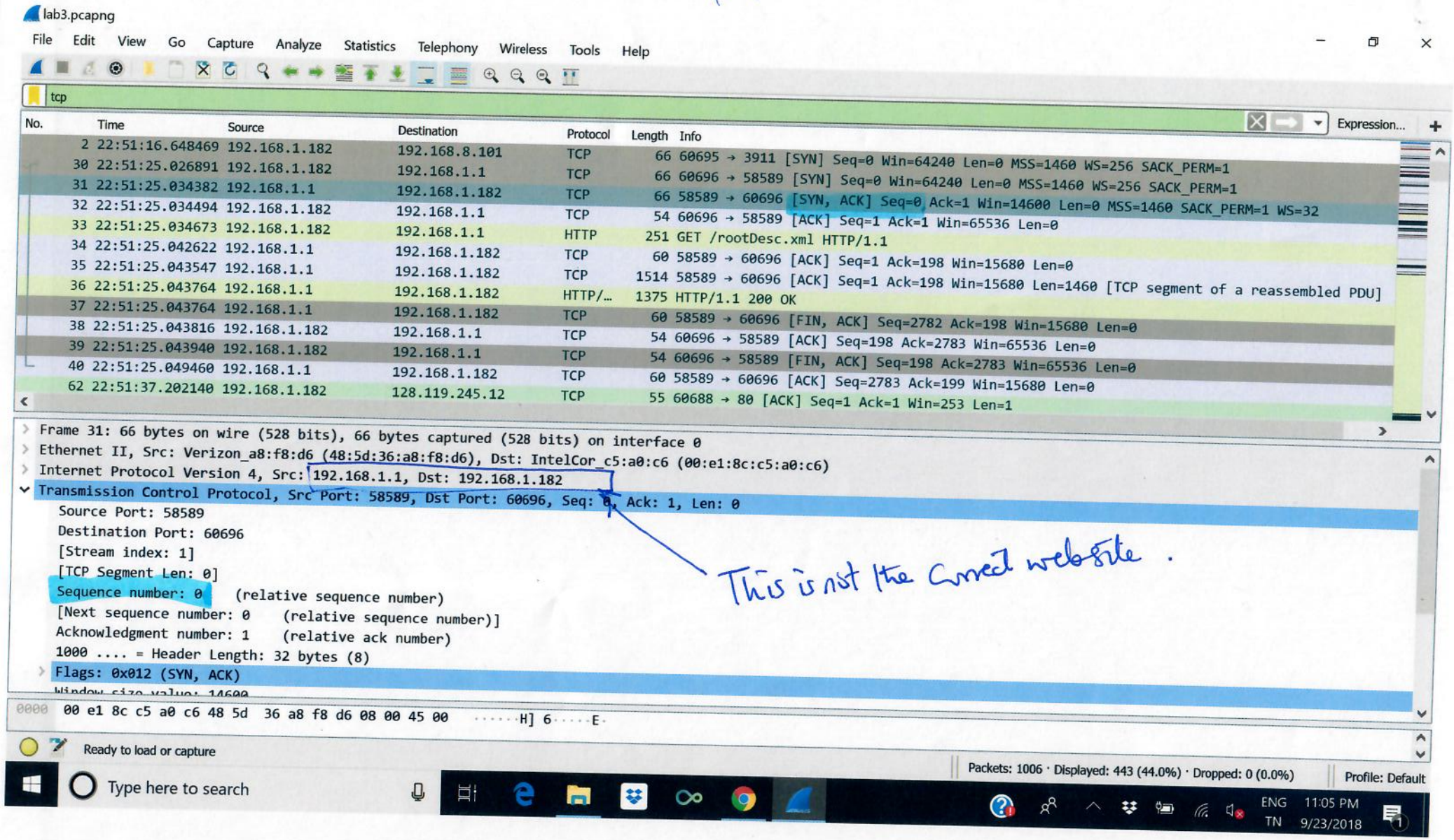
Q#2


lab3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
2 22:51:16.648469 192.168.1.182 192.168.8.101 TCP 66 60695 → 3911 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
30 22:51:25.026891 192.168.1.182 192.168.1.1 TCP 66 60696 → 58589 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
31 22:51:25.034382 192.168.1.1 192.168.1.182 TCP 66 58589 → 60696 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=32
32 22:51:25.034494 192.168.1.182 192.168.1.1 TCP 54 60696 → 58589 [ACK] Seq=1 Ack=1 Win=65536 Len=0
33 22:51:25.034673 192.168.1.182 192.168.1.1 HTTP 251 GET /rootDesc.xml HTTP/1.1
34 22:51:25.042622 192.168.1.1 192.168.1.182 TCP 60 58589 → 60696 [ACK] Seq=1 Ack=198 Win=15680 Len=0
35 22:51:25.043547 192.168.1.1 192.168.1.182 TCP 1514 58589 → 60696 [ACK] Seq=1 Ack=198 Win=15680 Len=1460 [TCP segment of a reassembled PDU]
36 22:51:25.043764 192.168.1.1 192.168.1.182 HTTP/... 1375 HTTP/1.1 200 OK
37 22:51:25.043764 192.168.1.1 192.168.1.182 TCP 60 58589 → 60696 [FIN, ACK] Seq=2782 Ack=198 Win=15680 Len=0
38 22:51:25.043816 192.168.1.182 192.168.1.1 TCP 54 60696 → 58589 [ACK] Seq=198 Ack=2783 Win=65536 Len=0
39 22:51:25.043940 192.168.1.182 192.168.1.1 TCP 54 60696 → 58589 [FIN, ACK] Seq=198 Ack=2783 Win=65536 Len=0
40 22:51:25.049460 192.168.1.1 192.168.1.182 TCP 60 58589 → 60696 [ACK] Seq=2783 Ack=199 Win=15680 Len=0
62 22:51:37.202140 192.168.1.182 128.119.245.12 TCP 55 60688 → 80 [ACK] Seq=1 Ack=1 Win=253 Len=1
Expression...
Correct answer.
Frame 30: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 192.168.1.1
Transmission Control Protocol, Src Port: 60696, Dst Port: 58589, Seq: 0, Len: 0
Source Port: 60696
Destination Port: 58589
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
0000 48 5d 36 a8 f8 d6 00 e1 8c c5 a0 c6 08 00 45 00 H]6 .... E.
It should be port 80 for HTTP traffic.
Ready to load or capture
Packets: 1006 · Displayed: 443 (44.0%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
ENG TN 11:01 PM 9/23/2018

Q #3

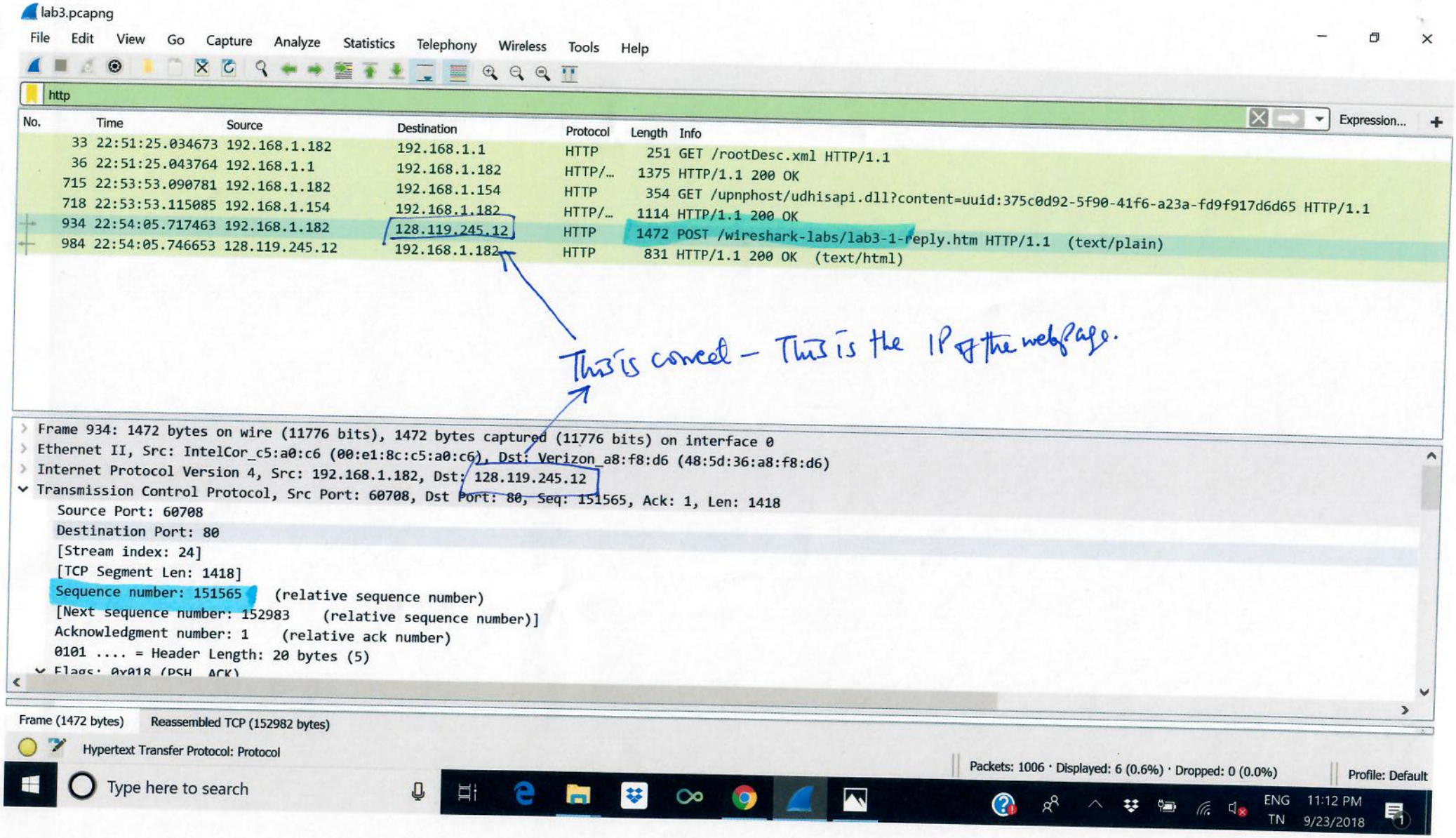


Wrong website.
This is not the IP address of gaia.cs.umass.edu.
= .12



This is not the Correct website.

Q#5


lab3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
33 22:51:25.034673 192.168.1.182 192.168.1.1 HTTP 251 GET /rootDesc.xml HTTP/1.1
36 22:51:25.043764 192.168.1.1 192.168.1.182 HTTP/... 1375 HTTP/1.1 200 OK
715 22:53:53.090781 192.168.1.182 192.168.1.154 HTTP 354 GET /upnphost/udhisapi.dll?content=uuid:375c0d92-5f90-41f6-a23a-fd9f917d6d65 HTTP/1.1
718 22:53:53.115085 192.168.1.154 192.168.1.182 HTTP/... 1114 HTTP/1.1 200 OK
934 22:54:05.717463 192.168.1.182 128.119.245.12 HTTP 1472 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
984 22:54:05.746653 128.119.245.12 192.168.1.182 HTTP 831 HTTP/1.1 200 OK (text/html)
Expression...
This is correct – This is the IP of the webpage.
Frame 934: 1472 bytes on wire (11776 bits), 1472 bytes captured (11776 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: 60708, Dst Port: 80, Seq: 151565, Ack: 1, Len: 1418
Source Port: 60708
Destination Port: 80
[Stream index: 24]
[TCP Segment Len: 1418]
Sequence number: 151565 (relative sequence number)
[Next sequence number: 152983 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Frame (1472 bytes)
Reassembled TCP (152982 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 1006 · Displayed: 6 (0.6%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
ENG TN 11:12 PM 9/23/2018

C:\Users\moudi\Documents\Network\lab3.pcapng 1006 total packets, 6 shown

Correct IP.

```
No.     Time                 Source                Destination           Protocol Length Info
    934 22:54:05.717463      192.168.1.182         128.119.245.12        HTTP     1472   POST /wireshark-labs/lab3-1-reply.htm HTTP/
1.1  (text/plain)
Frame 934: 1472 bytes on wire (11776 bits), 1472 bytes captured (11776 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: 60708, Dst Port: 80, Seq: 151565, Ack: 1, Len: 1418
    Source Port: 60708
    Destination Port: 80
    [Stream index: 24]
    [TCP Segment Len: 1418]
    Sequence number: 151565    (relative sequence number)
    [Next sequence number: 152983    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: .......AP...]
    Window size value: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
    Checksum: 0xb4a1 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.022808000 seconds]
        [Bytes in flight: 75740]
        [Bytes sent since last PSH flag: 4338]
    [Timestamps]
    TCP payload (1418 bytes)
    TCP segment data (1418 bytes)
[107 Reassembled TCP Segments (152982 bytes): #772(661), #773(1460), #774(1460), #775(1460), #776(1460), #777(1460), #778(1460),
#779(1460), #780(1460), #781(1460), #785(1460), #787(1460), #788(1460), #790(1460), #791(1460), #793(1460), #79]
Hypertext Transfer Protocol
    POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Content-Length: 152321\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryl4TsKLQ9uBqnBBkH\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/
537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/lab3-1-reply.htm]
    [HTTP request 1/1]
    [Response in frame: 984]
    File Data: 152321 bytes
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundaryl4TsKLQ9uBqnBBkH"
```

C:\Users\moudi\Documents\Network\lab3.pcapng 1006 total packets, 6 shown

```
No.     Time                 Source                Destination           Protocol Length Info
    984 22:54:05.746653      128.119.245.12        192.168.1.182         HTTP     831    HTTP/1.1 200 OK  (text/html)
Frame 984: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface 0
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: 60708, Seq: 1, Ack: 152983, Len: 777
    Source Port: 80
    Destination Port: 60708
    [Stream index: 24]
    [TCP Segment Len: 777]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 778    (relative sequence number)]
    Acknowledgment number: 152983    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: .......AP...]
    Window size value: 2093
    [Calculated window size: 267904]
    [Window size scaling factor: 128]
    Checksum: 0xccfd [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.022808000 seconds]
        [Bytes in flight: 777]
        [Bytes sent since last PSH flag: 777]
    [Timestamps]
    TCP payload (777 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 24 Sep 2018 02:54:06 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sat, 23 Oct 2010 11:38:58 GMT\r\n
    ETag: "1a2-4934734677880"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 418\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.029190000 seconds]
    [Request in frame: 934]
    File Data: 418 bytes
Line-based text data: text/html (11 lines)
```