

Luz Deloria
IT-520 – Lab1
09/06/2018

1. What is the Internet address of your computer?

What is the address?

Wireshark Screenshot showing network traffic:

- Frame 62: 17:19:09.255204 192.168.1.1 SSDP 239.255.255.250 Length: 217 Info: M-SEARCH * HTTP/1.1
- Frame 63: 17:19:09.693780 192.168.1.233 IGPv3 54 Memberlist Report / Join group 224.0.0.51 for any sources
- Frame 64: 17:19:09.988307 192.168.1.233 DNS 77 Standard query 0x8cc7 A galia.cs.umass.edu
- Frame 65: 17:19:10.001098 192.168.1.233 DNS 77 Standard query 0x8cc7 A galia.cs.umass.edu
- Frame 66: 17:19:10.000562 192.168.1.1 DNS 93 Standard query response 0x8cc7 A galia.cs.umass.edu A 128.119.245.12
- Frame 67: 17:19:10.012184 192.168.1.233 TCP 66 50943 → 80 [SYN] Seq=0 Win=54240 Len=0 MSS=1460 WS=265 SACK_PERM=1
- Frame 68: 17:19:10.012280 192.168.1.233 TCP 66 50944 → 80 [SYN] Seq=0 Win=54240 Len=0 MSS=1460 WS=265 SACK_PERM=1
- Frame 69: 17:19:10.030402 192.168.1.233 TCP 66 80 → 50943 [SYN, ACK] Seq=1 Ack=1 Win=28200 Len=0 MSS=1460 SACK_PERM=1 WS=128
- Frame 70: 17:19:10.031172 192.168.1.233 TCP 54 50943 → 80 [ACK] Seq=1 Ack=1 Win=5556 Len=0
- Frame 71: 17:19:10.031216 192.168.1.233 HTTP 566 GET /wireshark-labs/intro-wireshark-title1.html HTTP/1.1

Frame 64: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0

- > Ethernet II, Src: IntelCor_24:e1:0c (64:80:99:24:e1:0c), Dst: Verizon_ae:98:a6 (48:5d:36:aa:98:a6)
- > Internet Protocol Version 4, Src: 192.168.1.233, Dst: 192.168.1.1
- > User Datagram Protocol, Src Port: 57321, Dst Port: 53
- > Domain Name System (query)

Internet Protocol Version 4 (ip), 20 bytes

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|---|-----------------|-------------|----------|--------|------|
| 0000 | 48 5d 36 ae 98 a6 64 80 99 24 4e 0c 00 45 00 | HJ6 d SU E | | | | |
| 0010 | 00 3f 65 ca 00-00 80 11-00 a9 c0 a9 c0 a8 | ?e... P.... | | | | |
| 0020 | 01 01 df e9 00 35 00 2b 93 00 8c 67 01 00 00 01 | . 5 + | | | | |
| 0030 | 00 00 00 00 00 04 66 61 69 61 02 63 73 05 75 | mass edu | | | | |
| 0040 | 6d 61 73 73 03 65 64 75 00 00 01 00 01 | mass.edu | | | | |

(A) *Make sure you read the instructions next time.*

2. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

DNS ✓
 DNS
 DNS
 TCP ✓
 TCP
 TCP
 TCP
 HTTP ✓

X 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 packetlisting 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.)

Lab1_wireshark.pcapng

No. Time Source Destination Protocol Length Info

| | | | | | |
|----|-----------------|----------------|-----------------|-------|--|
| 62 | 17:19:09.256204 | 192.168.1.1 | 239.255.255.250 | SSDP | 217 M-SEARCH * HTTP/1.1 |
| 63 | 17:19:09.693780 | 192.168.1.233 | 224.0.0.22 | TGPv3 | 54 Membership Report / Join Group 224.0.0.251 for any sources |
| 64 | 17:19:09.988307 | 192.168.1.233 | 192.168.1.1 | DNS | 77 Standard query 0x8cc7 A gaia.cs.umass.edu |
| 65 | 17:19:10.008562 | 192.168.1.233 | 192.168.1.1 | DNS | 77 Standard query 0x8cc7 A galax.cs.umass.edu |
| 66 | 17:19:10.010584 | 192.168.1.233 | 192.168.1.233 | DNS | 93 Standard query 0x8cc7 A galax.cs.umass.edu |
| 67 | 17:19:10.010584 | 192.168.1.233 | 128.119.245.12 | TCP | 66 50943 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 Window=256 SACK_PERM=1 |
| 68 | 17:19:10.011200 | 192.168.1.233 | 128.119.245.12 | TCP | 66 50944 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 Window=256 SACK_PERM=1 |
| 69 | 17:19:10.030259 | 128.119.245.12 | 192.168.1.233 | TCP | 66 80 → 50943 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 Window=256 SACK_PERM=1 |
| 70 | 17:19:10.030402 | 192.168.1.233 | 128.119.245.12 | TCP | 54 50943 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 71 | 17:19:10.031172 | 192.168.1.233 | HTTP | | 566 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |

Now screenshot doesn't show the result.

Next time put a full screenshot and write down the protocols or highlight them.

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

What is the IP address?
Write in circle

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|----------------|-----------------|----------|--------|--|
| 62 | 17:19:09.256204 | 192.168.1.1 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 63 | 17:19:09.693780 | 192.168.1.233 | 224.0.0.122 | IGMPv3 | 54 | Membership Report / Join Group 224.0.0.251 for any sources |
| 64 | 17:19:09.988367 | 192.168.1.233 | 192.168.1.1 | DNS | 77 | Standard query 0x8cc7 A gaia.cs.umass.edu |
| 65 | 17:19:10.001099 | 192.168.1.233 | 192.168.1.1 | DNS | 77 | Standard query 0x8cc7 A gaia.cs.umass.edu |
| 66 | 17:19:10.008562 | 192.168.1.1 | 192.168.1.233 | DNS | 93 | Standard query response 0x8cc7 192.168.1.233 |
| 67 | 17:19:10.016184 | 192.168.1.233 | 128.119.245.12 | TCP | 65 | 50945 + 80 [SYN] Seq=0 Win=6240 Length=6240 MSS=1460 SACK_PERM=1 |
| 68 | 17:19:10.012200 | 192.168.1.233 | 128.119.245.12 | TCP | 66 | 50944 + 80 [SYN] Seq=0 Win=6240 Length=6240 MSS=1460 SACK_PERM=1 |
| 69 | 17:19:10.030259 | 128.119.245.12 | 192.168.1.1 | TCP | 66 | 80 + 80 [ACK] Seq=1 Win=5536 Length=0 |
| 70 | 17:19:10.030402 | 192.168.1.1 | 128.119.245.12 | TCP | 54 | 50943 + 80 [ACK] Seq=1 Ack=1 Win=5536 Length=0 |
| 71 | 17:19:10.031172 | 192.168.1.233 | 128.119.245.12 | HTTP | 566 | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |

- > Frame 65: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
- > Ethernet II, Src: Verizon_ae:98:a6 (48:5d:36:ae:98:a6), Dst: IntelCor_24:4e:0c (64:80:99:24:4e:0c)
- > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.233

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.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----------|--|--|---|---|--------|----------------------------------|
| 65 | 12.423474 | 192.168.1.233 | 192.168.1.1 | DNS | 77 | Standard query 0x8cc7 A gaia.cs. |
| Frame 65: | 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0 | Ethernet II, Src: IntelCor_24:4e:0c (64:80:99:24:4e:0c), Dst: verizon_ae:98:a6 (48:5d:36:ae:98:a6) | Internet Protocol Version 4, Src: 192.168.1.233, Dst: 192.168.1.1 | User Datagram Protocol, Src port: 57321, Dst port: 53 | | Domain Name System (query) |

It says Print Two

Get and OK. None of this is the OK
~~selected~~

C:\Users\Dominique Amor\Desktop\Lab1_Wireshark.pcapng 459 total packets, 459 shown

| No. | Time | Source | Destination | Protocol | Length | Info |
|----------------------------|--|---|---|---|--------|---|
| 65 | 12.423474 | 192.168.1.233 | 192.168.1.1 | DNS | 77 | Standard query 0x8cc7 A gaia.cs.umass.edu |
| Frame 65: | 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0 | Ethernet II, Src: IntelCor_24:4e:0c (64:80:99:24:4e:0c) | Dst: Verizon_ae:98:a6 (48:5d:36:ae:98:a6) | Internet Protocol Version 4, Src: 192.168.1.233, Dst: 192.168.1.1 | | User Datagram Protocol, Src Port: 57321, Dst Port: 53 |
| Domain Name System (query) | | | | | | |

9/16/18

WireShark Lab2 - HTTP

Luz Deloria

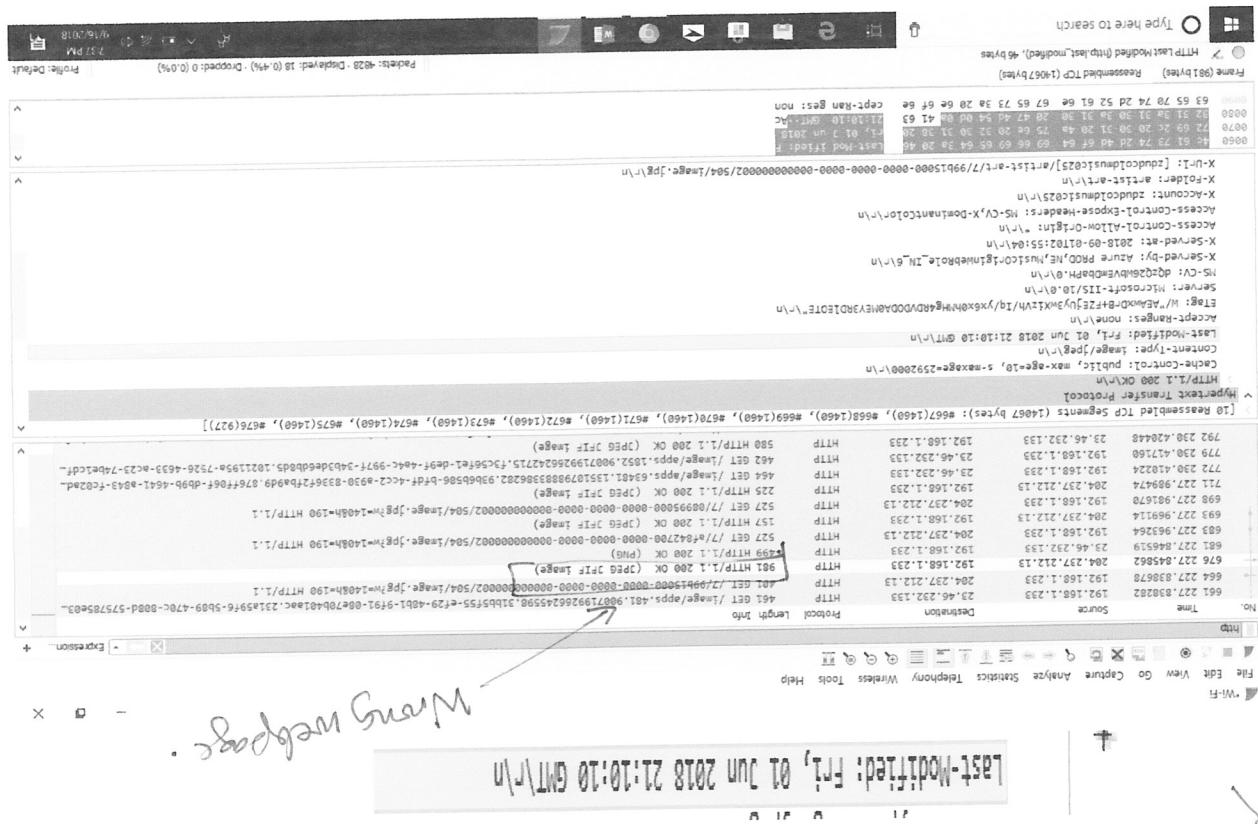
• 89

HTTP 1.1

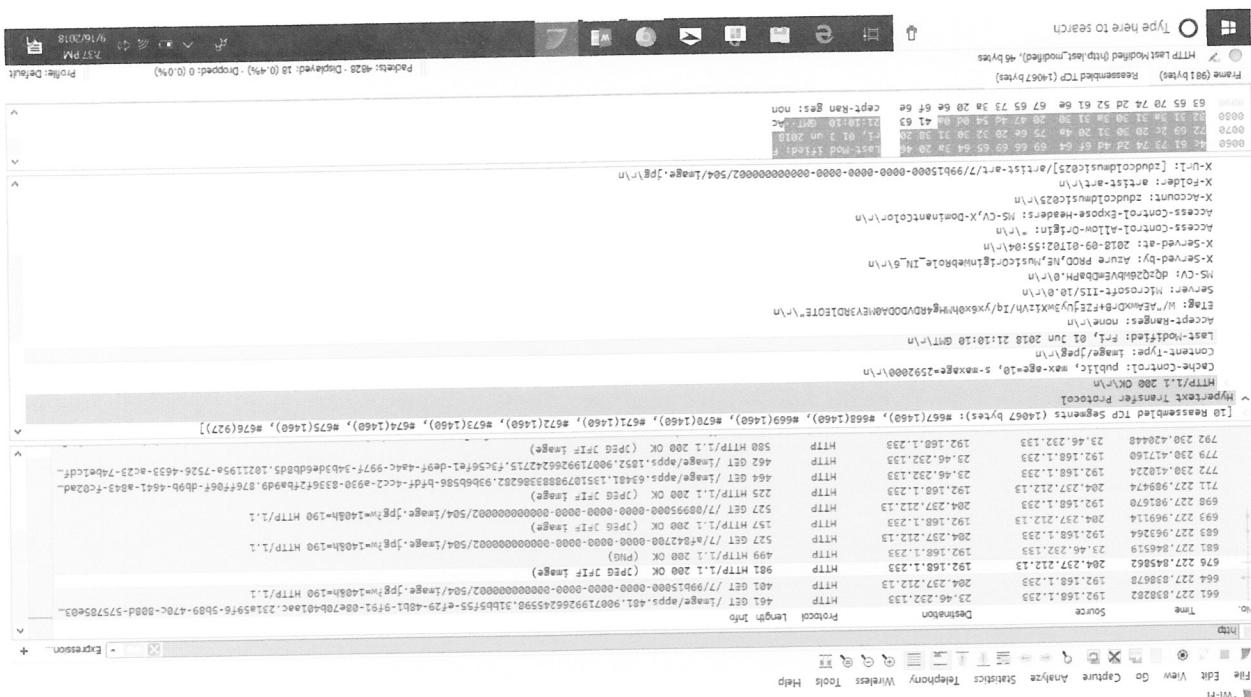
1. Is your browser running HTTP version 1.0 or 1.1?

Wings developed.
n 1.0 or 1.1?
Gumma
made sure you follow the instructions
I gave you earlier for the blowups
and
... somewhat well first.

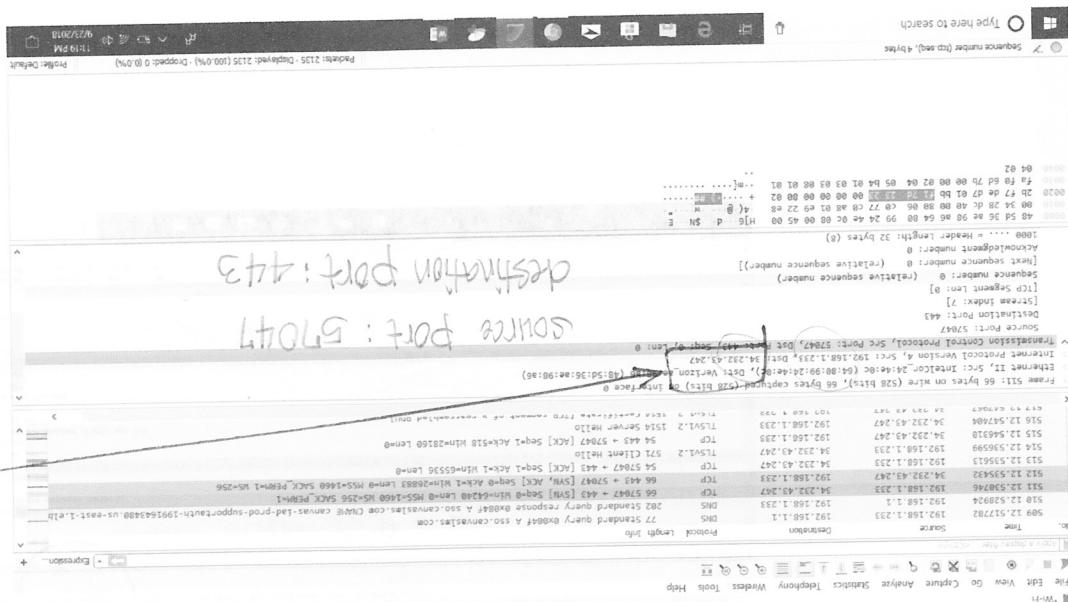
2. When was the HTML file that you are retrieving last modified at the server?



5. When was the HTML file that you are retrieving last modified at the server?



the number
number of the
TCP port



gala.cs.umass.edu?

1. What is the TCP port number used by your computer to communicate with

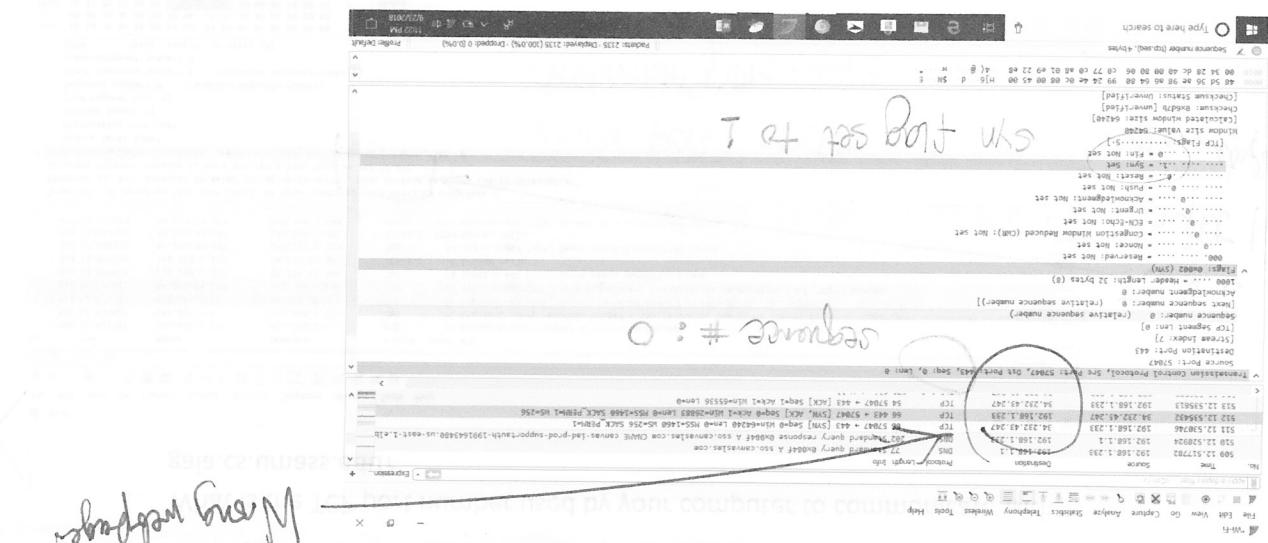
```
C:\Users\Dominiique Amore>
Wireless LAN adapter Wi-Fi:
Media State : Media disconnected
Connection-specific DNS Suffix : 
Link-Local IPv6 Address : fe80::dd04:6eed:1de:ff%3
Default Gateway : 192.168.1.1
Subnet Mask : 255.255.255.0
TIV4 Address : 192.168.1.233
Connection-specific DNS Suffix : fios-router.home
Wireless LAN adapter Local Area Connection* 2:
Media State : Media disconnected
Connection-specific DNS Suffix : 
Media State : Media disconnected
Wireless LAN adapter Local Area Connection* 1:
Media State : Media disconnected
Connection-specific DNS Suffix : 
Media State : Media disconnected
Wireless LAN adapter Wi-Fi:
Media State : Media disconnected
Connection-specific DNS Suffix : 
Media State : Media disconnected
IP address : 192.168.1.233
```

1

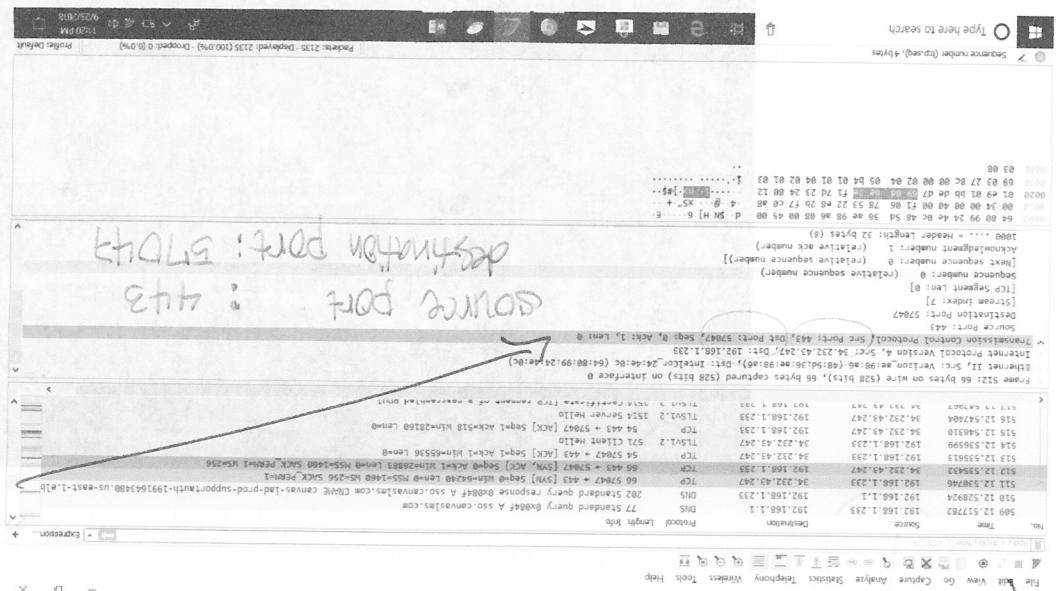
09/24/18
Wireshark lab 3 - TCP
Instructions of the scenario: Using the given demand, find the IP address

Luz Deloria

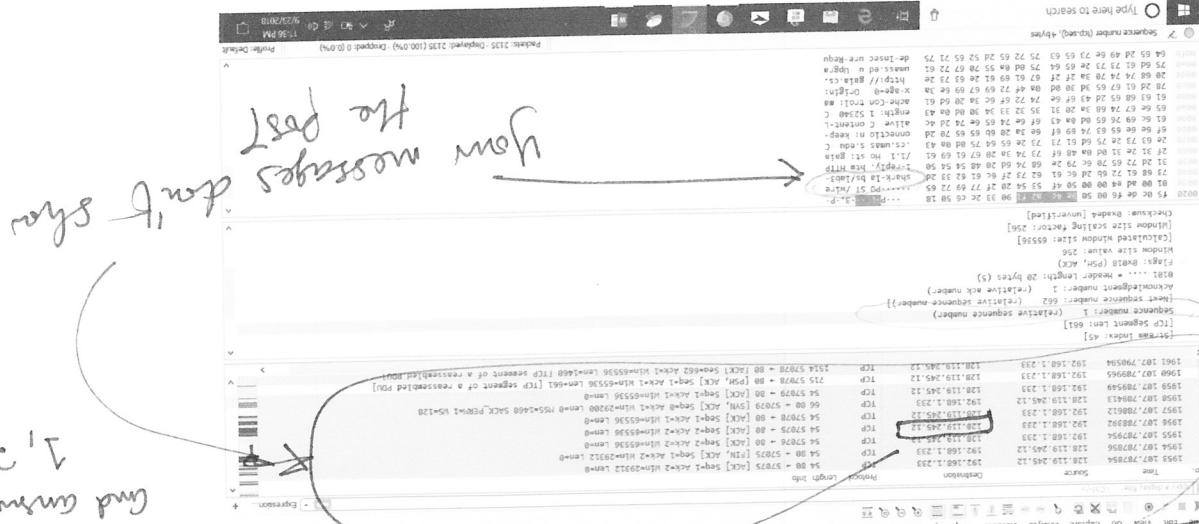
What is the TCP port number used by gai.cs.umass.edu to communicate with your computer?



3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between your computer and gai.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?



2. What is the TCP port number used by gai.cs.umass.edu to communicate with your computer?



- 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.
5. What is the sequence number of the TCP segment containing the HTTP POST command?



4. What is the sequence number of the SYNACK segment sent by gaias.cs.umass.edu to the client computer in reply to the SYN? - You must dig deep and find the ACK from

| No. | Time | Source | Destination | Protocol Length Info | HTTP/1.1 GET /favicon.ico | HTTP/1.1 435 3480 bytes captured (3480 bytes) | Frame 1792 Ethernet II, SRC: IntelCor-24:4e:0c (64:80:99:24:4e:0c), Dst: Verizon-ae:98:a6 (48:5d:36:ae:98:a6) on wire (3480 bits), 435 bytes captured (3480 bytes) on interface 0 | Ethernet III, SRC: IntelCor-24:4e:0c (64:80:99:24:4e:0c), Dst: Verizon-ae:98:a6 (48:5d:36:ae:98:a6) on interface 0 | Internet Protocol Version 4, SRC: 192.168.1.233, Dst: 128.119.245.12 | HyperText Transfer Protocol Transmission Control Protocol, Src Port: 57072, Dst Port: 80, Seq: 1, Len: 381 |
|------|-----------|---------------|----------------|----------------------|---------------------------|---|---|--|--|--|
| 1792 | 63.838901 | 192.168.1.233 | 128.119.245.12 | HTTP 435 | GET /favicon.ico | HTTP/1.1 435 3480 bytes captured (3480 bytes) | Frame 1792: 435 bytes on wire (3480 bits), 435 bytes captured (3480 bits) on interface 0 | Ethernet III, SRC: IntelCor-24:4e:0c (64:80:99:24:4e:0c), Dst: Verizon-ae:98:a6 (48:5d:36:ae:98:a6) on interface 0 | Internet Protocol Version 4, SRC: 192.168.1.233, Dst: 128.119.245.12 | HyperText Transfer Protocol Transmission Control Protocol, Src Port: 57072, Dst Port: 80, Seq: 1, Len: 381 |

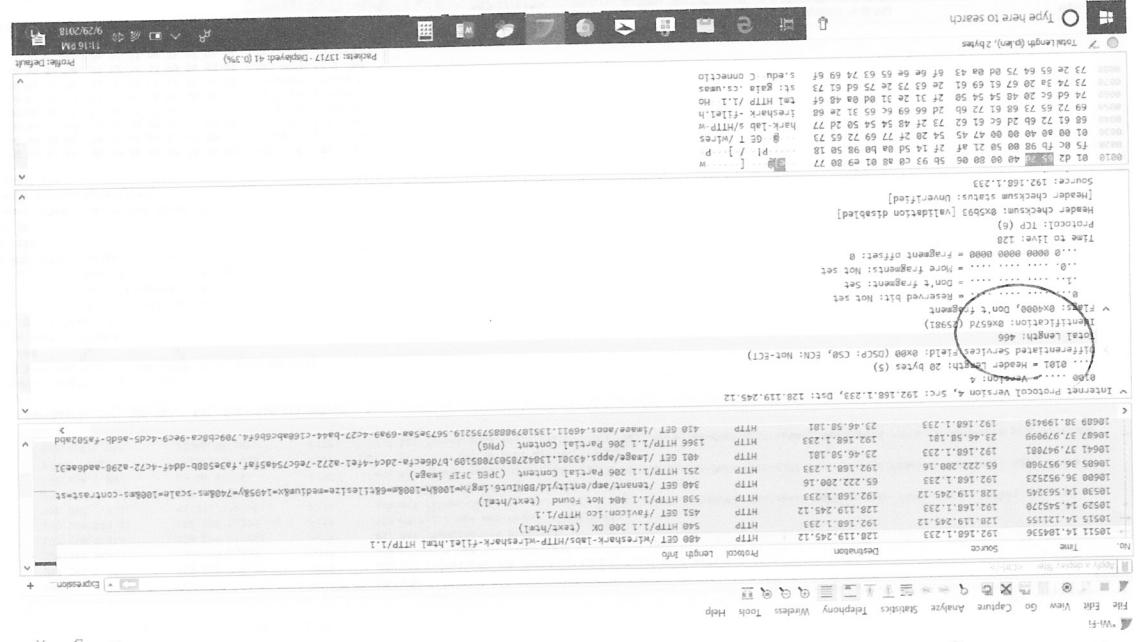
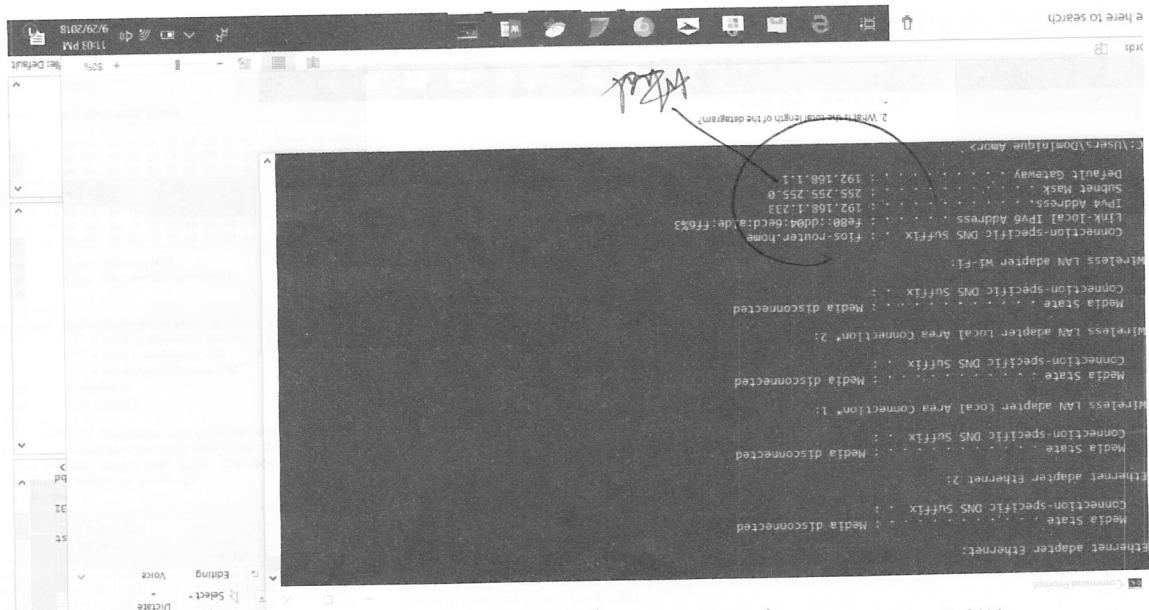
- Instructions:
- What is the TCP port number used by your computer to communicate with gaia.cs.umass.edu? What is the time and date on your computer? Indicate the time and date on your computer.
 - What is the TCP port number used by gaia.cs.umass.edu to communicate with your computer?
 - What is the 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 sequence number of the SYN segment that identifies the segment as a SYN segment?
 - 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.
 - What is the sequence number of the HTTP POST command containing the HTTP POST segment with a "POST" within its DATA field?

- Instructions:
- 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 steps you took to capture the traffic and the results of the analysis.
- Will NOT be graded if either of these two is missing. (You can refer to Lab 1 for 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
- Include a terminal screenshot showing the IP address on the front page
 - Pay attention to the SYN ACK packets.
 - Stop Wireshark packet capture and filter TCP packets.
 - Configure your browser to show the IP address of the front page.
 - Return 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 file named Alice.txt will be displayed in your browser window.
 - Return to your browser, press the "Upload Alice.txt file" button to upload the options here).
- OK on the Wireshark Packet Capture Options screen (we'll not need to select any 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 the "Upload Alice.txt file" button.
 - Use the Browse button in this form to enter the name of the file (full path name) somewhere on your computer containing Alice in Wonderland (or do so manually). Don't yet
 - Next go to <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file.html>.
- 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

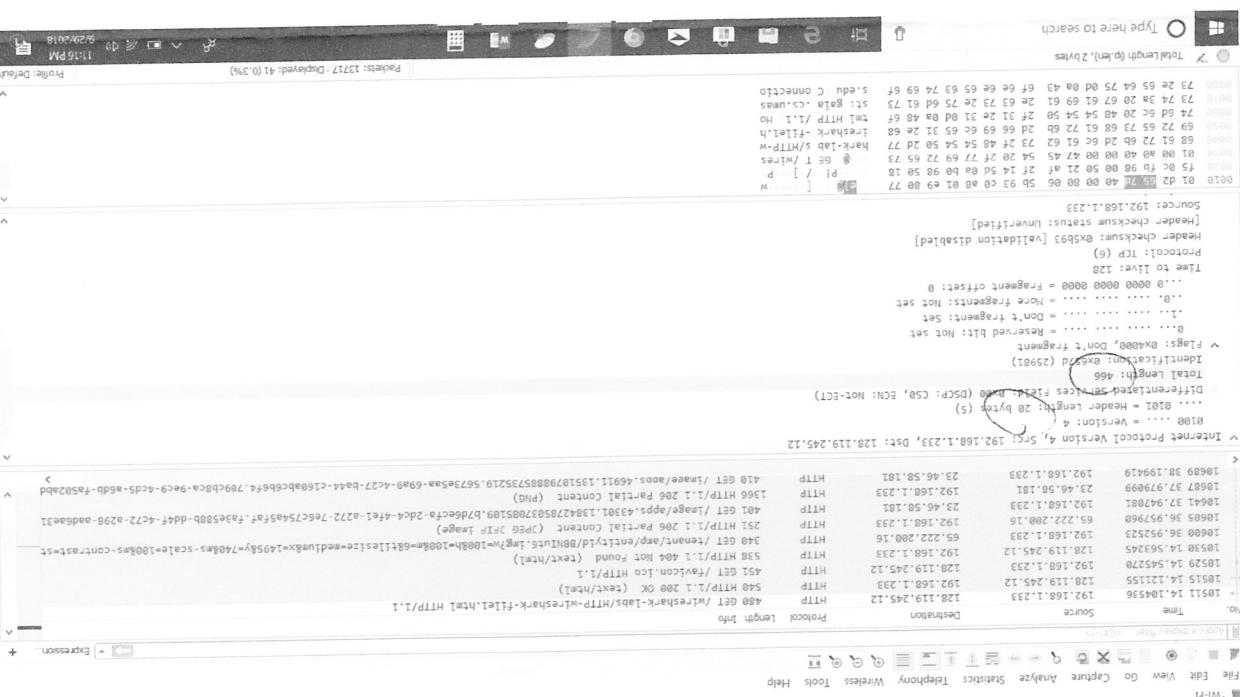
Due Date: 09/24/18 (Handed in at the beginning of class)
IT 520-A - Enterprise Infrastructure & Networks

Wireshark Lab 3 - TCP

1. What is the IP address of your computer? The IP address of my computer is 192.168.1.233



- The total length of the datagram is 466.



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

There are 20 bytes in the IP header, and 466 bytes total length, this gives 446 bytes in the payload of the IP datagram.

4

Luz Deloria
Lab 5- Traceroute

IT-520-A

❖ Maymount - Portal

← → G i file(c) 2018 Microsoft Corporation. All rights reserved.

Apps Compartir

C:\Users\Dominique Amor>www.webawards.com.au' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Dominique Amor>tracert www.webawards.com.au

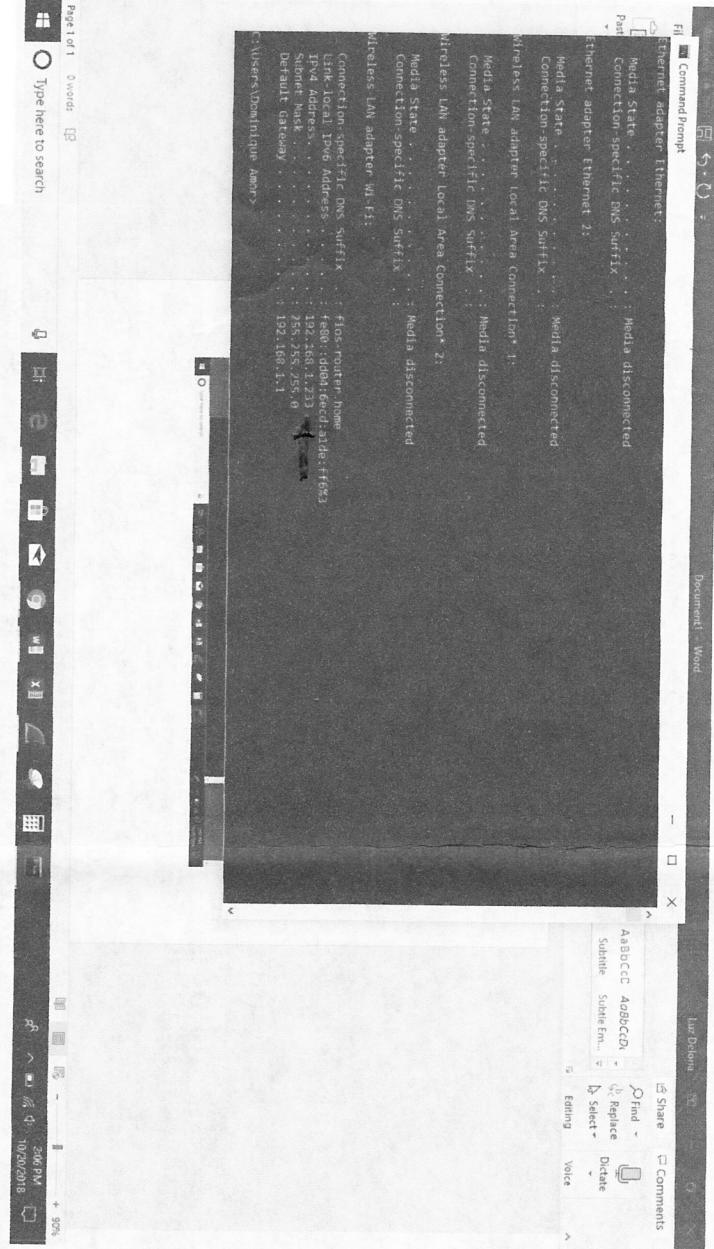
Tracing route to webawards.com.au [122.129.218.218]
over a maximum of 30 hops:

| Hop | MS | RTT | Router/Link |
|-----|-----|--------------|---|
| 1 | 6 | 2 ms | FIOS_Quantum_Gateway.fios-router.home [192.168.1.1] |
| 2 | 6 | 5 ms | 100-100.WASHDC-VFTTP-308.verizon-gni.net [108.54.59.1] |
| 3 | 9 | 5 ms | 12.ms.B3Z88.WASHDC-LCR-22.verizon-gni.net [130.81.217.82] |
| 4 | * | * | Request timed out. |
| 5 | 4 | 4 ms | 0.eet-7-1-2.BRI.IADS.ALTER.NET [140.222.226.15] |
| 6 | 5 | 5 ms | tbo.BR1.IA08.ALTER.NET [204.148.11.177] |
| 7 | 74 | 69 ms | et-0-0-53.GC3.lax2.ip4.gtt.net [218.254.230.254] |
| 8 | 67 | 67 ms | singapore-telecommunications-gw.ip4.gtt.net [46.33.80.34] |
| 9 | 67 | 66 ms | 203.208.172.173 |
| 10 | 218 | 215 ms | 203.208.177.130 |
| 11 | 228 | 229 ms | 230 ms |
| 12 | 237 | 235 ms | 59.154.18.146 |
| 13 | 234 | 229 ms | 232 ms |
| 14 | 235 | 233 ms | 161.43.103.42 |
| 15 | 234 | 233 ms | 235 ms |
| | | 210.56.92.11 | |
| | | 242 ms | 122.129.216.9 |
| | | 234 ms | myaccount5.mpcpanel.com [122.129.218.218] |

Trace complete.

C:\Users\Dominique Amor>

1. IP address: 192.168.1.233



1. IP address:

192.168.1.233

2. The IP address of the first IP from the traceroute result is: PRIVATE

The screenshot shows a Microsoft Word document with a "Traceroute" table. The table has two columns: "Source" and "Destination". The "Source" column lists the IP address 192.168.1.1. The "Destination" column lists the IP address 192.168.1.1. The table has 14 rows, representing a full round trip. The rows are numbered 1 through 14. The "Destination" column contains the same IP address 192.168.1.1 for all rows. The "Source" column shows various IP addresses along the path, including 192.168.1.1, 192.168.0.1, 192.168.255.255, 192.168.0.1-192.168.255.255, and 192.168.1.1 again at the end of the path.

The IPWHOIS Lookup tool finds contact information for the owner of a specified IP address.

Enter a host name or an IP address

192.168.1.1

Go ▶

Go ▶

The screenshot shows the IPWHOIS Lookup Tool interface. At the top, it says "WHOIS IP Lookup Tool". Below that, it says "The IPWHOIS Lookup tool finds contact information for the owner of a specified IP address." A search bar contains the IP address "192.168.1.1". The main content area displays the following contact information:

Source: WHOIS.arin.net
IP Address: 192.168.1.1
Name: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
Handle: NET-192-168-0-0-1
Registration Date: 3/15/94
Range: 0-192.168.255.255
Org: Internet Assigned Numbers Authority
Org Handle: IANA
Address: 12005 Waterfront Drive
Suite: 300
City: Los Angeles
State/Province: CA
Postal Code: 90292
Country: United States
Name Servers:

The screenshot shows a detailed WHOIS record for the IP address 192.168.1.1. The record includes the following fields:

Source: WHOIS.arin.net
IP Address: 192.168.1.1
Name: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
Handle: NET-192-168-0-0-1
Registration Date: 3/15/94
Range: 0-192.168.255.255
Org: Internet Assigned Numbers Authority
Org Handle: IANA
Address: 12005 Waterfront Drive
Suite: 300
City: Los Angeles
State/Province: CA
Postal Code: 90292
Country: United States
Name Servers:

The screenshot shows a detailed WHOIS record for the IP address 192.168.1.1. The record includes the following fields:

Source: WHOIS.arin.net
IP Address: 192.168.1.1
Name: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
Handle: NET-192-168-0-0-1
Registration Date: 3/15/94
Range: 0-192.168.255.255
Org: Internet Assigned Numbers Authority
Org Handle: IANA
Address: 12005 Waterfront Drive
Suite: 300
City: Los Angeles
State/Province: CA
Postal Code: 90292
Country: United States
Name Servers:

The screenshot shows a detailed WHOIS record for the IP address 192.168.1.1. The record includes the following fields:

Source: WHOIS.arin.net
IP Address: 192.168.1.1
Name: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
Handle: NET-192-168-0-0-1
Registration Date: 3/15/94
Range: 0-192.168.255.255
Org: Internet Assigned Numbers Authority
Org Handle: IANA
Address: 12005 Waterfront Drive
Suite: 300
City: Los Angeles
State/Province: CA
Postal Code: 90292
Country: United States
Name Servers:

3. IP address of the second IP from the traceroute result is: PUBLIC

The screenshot shows a Microsoft Word document with the title "Wieschak Lab 5 - TCP - Saved". The document contains a table of traceroute results and a screenshot of a web-based WHOIS lookup tool.

Traceroute Results:

| Sequence | IP Address | Latency |
|----------|-----------------|---------|
| 1 | 108.51.59.1 | 6 ms |
| 2 | 21.179.206.215 | 2 ms |
| 3 | 21.179.206.215 | 3 ms |
| 4 | 21.179.206.215 | 9 ms |
| 5 | 6.67.7.1 | 4 ms |
| 6 | 6.67.7.1 | 5 ms |
| 7 | 74.98.63.65 | 7 ms |
| 8 | 67.95.66.65 | 8 ms |
| 9 | 67.95.66.65 | 9 ms |
| 10 | 219.219.220.220 | 10 ms |
| 11 | 219.219.220.220 | 228 ms |
| 12 | 219.219.220.220 | 233 ms |
| 13 | 219.219.220.220 | 237 ms |
| 14 | 219.219.220.220 | 241 ms |
| 15 | 219.219.220.220 | 244 ms |
| 16 | 219.219.220.220 | 244 ms |
| 17 | 219.219.220.220 | 244 ms |

WHOIS IP Lookup Tool Screenshot:

The WHOIS tool interface includes fields for "Enter a host name or an IP address" and "108.51.59.1". Below the search bar are tabs for "DNS Traversal", "TraceRoute", "Vector Trace", and "WHOIS Lookup". The main pane displays the following information:

- Source: whois.arin.net
- IP Address: 108.51.59.1
- Name: VIS-SBLOCK
- Handle: NET-1A8-0-0-0-1
- Registration Date: 6/5/09
- Range: 108.0.0.0-108.51.255.255
- Org: NCI COMMUNICATIONS SERVICES, INC. d/b/a VERIZON BUSINESS
- Address: 22001 Loudoun County Pkwy
- City: Ashburn
- State/Province: VA
- Postal Code: 20147
- Country: United States
- Name Servers:

The bottom of the WHOIS tool window shows the URL <https://www.ultratools.com/tools/ipWhoisLookupResult>.

4

| Hop Count | IP address | Organization (IP Owner) | Location (US state)/Country |
|-----------|---------------|---|-----------------------------|
| 1 | 192.168.1.1 | Internet Assigned Numbers Authority | CA/USA |
| 2 | 108.51.59.1 | MCI Communications Services, Inc. d/b/a Verizon Business | Ashburn/VA |
| 3 | 130.81.217.82 | MCI Communications Services, Inc. d/b/a Verizon Business | Ashburn/VA |

It should be a complete table with all hosts

WHOIS IP Lookup Tool

The IPWHOIS Lookup tool finds contact information for the owner of a specified IP address.

130.81.217.82

Revised Tools DNS Trace DNS Traceroute TraceRoute VectorTrace Ping WHOIS Lookup

5. In your own words, explain everything you just did, and what route did your packet took from source to destination.

Out of the 30 hops, trace was complete in just 15 hops. From the packet source, which is my home router, the packet was transferred locally through a data link layer; then the next hop, it travelled internationally, Singapore → Australia, respectively.

How many US states did your packet go through? How many countries if any?

- The packets go through 2 US states; CA & VA.
- It travelled to 2 more countries- Singapore, Australia

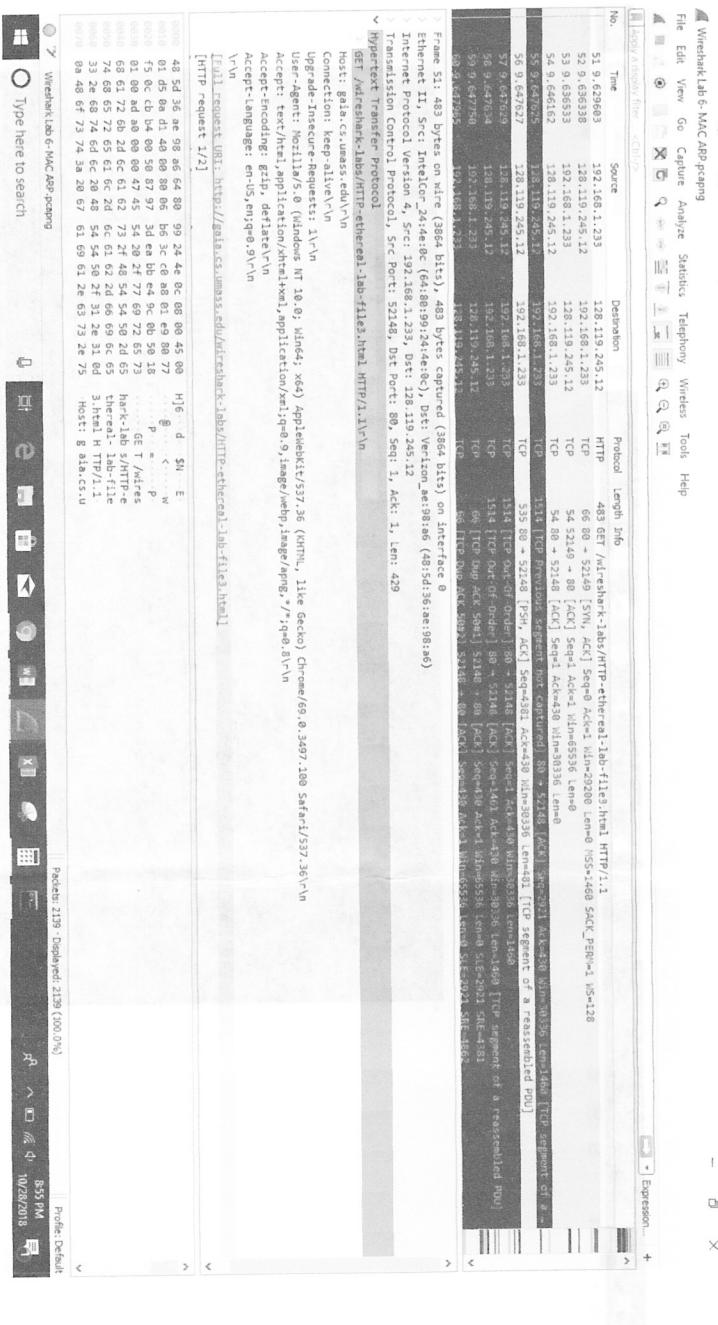
Instructions: •

Clear your browser history, and visit:

<http://gaia.cs.umass.edu/wireshark-labs/HTTPethereal-lab-file3.html>

(your browser should display the US Bill of Rights)

- Using Wireshark, capture the packets. Remember to start, then visit webpage, and then stop.
- We are going to analyze Ethernet frames.



- Take a screenshot of your IP address (this is not part of your grade)

Wireless Lab 6: MAC ARP answer

File Home Insert Design Layout References Mailings Review View Help Tell me what you want to do

Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 2:

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

Wireless LAN adapter Local Area Connection 1:

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

Wireless LAN adapter Wi-Fi:

- Connection-specific DNS Suffix : fios-router-home
- Link-local IPv6 Address : fe80::dfe84:6ec0:1de:ff6%3
- IPv4 Address : 192.168.1.233
- Subnet Mask : 255.255.255.0
- Default Gateway : 192.168.1.1

C:\Users\Dominique Amor\

SBCCC AebbcCcA Subtle Em... Select Editing Voice

Find Replace Dictate

Page 2 of 7 193 words □ (Ctrl) ▾

Type here to search

9:29 PM 10/26/2018 85%

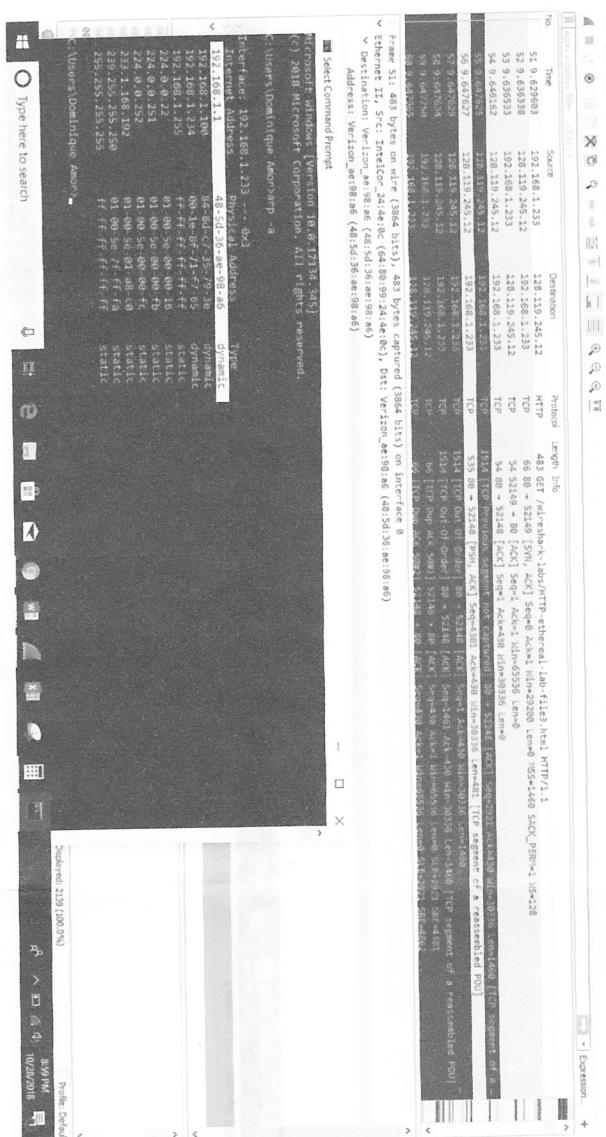
• Take a screenshot of your IP address (this is not part of your grade)

- * Please select the column for the question you would like to answer (you will see the file path below each question)
- * Go to https://umich.instructure.com/courses/13903/assignments/10000
- * Click "View Gradebook" (green button)
- * Click "View Gradebook" (green button)

THURSDAY
CSC 101
INTERVIEW

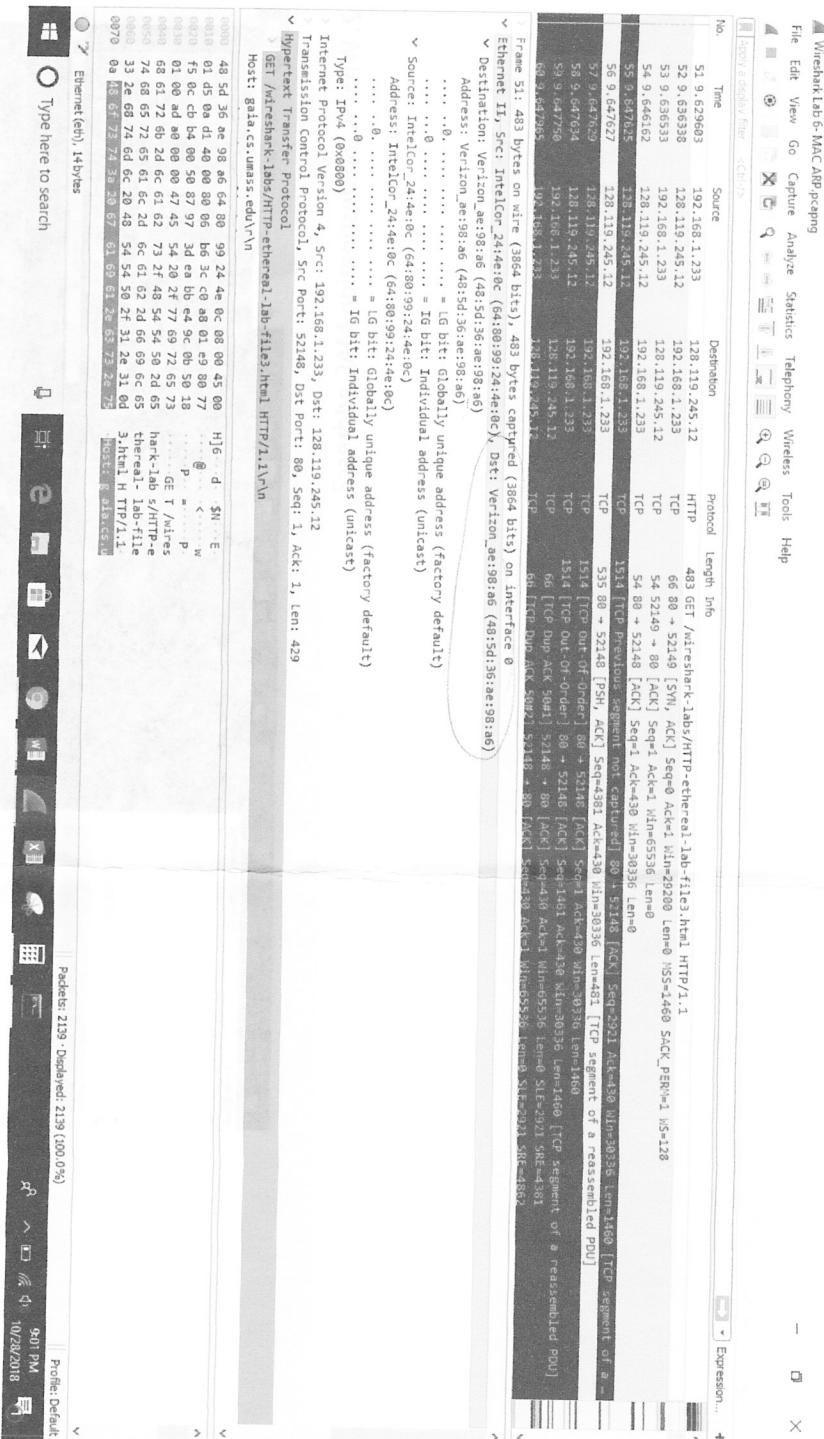
Questions:

1. What is the MAC address from your computer?



2. What is the destination MAC address?

(2)



3. What device has the MAC address shown in the destination? ✓✓✓✓✓

Wireshark Lab 6 - MAC ARP probing

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply as display filter: <Ctrl+L>

No. Time Source Destination Protocol Length Info

| | | | | | |
|----|----------|----------------|----------------|--|---|
| 51 | 9.629683 | 192.168.1.233 | 128.119.245.12 | HTTP | 483 GET /wiresnark-labs/HTTP-ethereum1-ipb-f1e3.html HTTP/1.1 |
| 52 | 9.636338 | 128.119.245.12 | TCP | 66 80 > 32149 [SYN, ACK] Seq=0 Ack=1 Win=2280 Len=0 SACK_PERM=1 NS=128 | |
| 53 | 9.636533 | 192.168.1.233 | TCP | 54 52149 > 80 [ACK] Seq=1 Ack=1 Win=5535 Len=0 | |
| 54 | 9.646162 | 128.119.245.12 | TCP | 54 80 > 32148 [ACK] Seq=1 Ack=430 Win=3036 Len=448 [TCP segment of a reassembled PDU] | |
| 55 | 9.646162 | 128.119.245.12 | TCP | 55 134 [TCP previous segment not contained] 80 > 32146 [ACK] Seq=293 Ack=430 Win=3036 Len=448 [TCP segment of a reassembled PDU] | |
| 56 | 9.647627 | 128.119.245.12 | TCP | 55 80 > 32148 [PSH, ACK] Seq=430 Ack=430 Win=3036 Len=448 [TCP segment of a reassembled PDU] | |
| 57 | 9.647639 | 128.119.245.12 | TCP | 55 154 [TCP out-of-order] 80 > 32148 [ACK] Seq=431 Ack=430 Win=3036 Len=448 [TCP segment of a reassembled PDU] | |
| 58 | 9.647639 | 128.119.245.12 | TCP | 55 154 [TCP out-of-order] 80 > 32148 [ACK] Seq=431 Ack=430 Win=3036 Len=448 [TCP segment of a reassembled PDU] | |
| 59 | 9.647756 | 192.168.1.233 | TCP | 56 155 [TCP out-of-order] 80 > 32148 [ACK] Seq=432 Ack=431 Win=5535 Len=448 [TCP segment of a reassembled PDU] | |
| 60 | 9.647756 | 128.119.245.12 | TCP | 56 155 [TCP out-of-order] 80 > 32148 [ACK] Seq=432 Ack=431 Win=5535 Len=448 [TCP segment of a reassembled PDU] | |

Frame 51: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface 0
Ethernet II, Src: IntelCor_24:4e:0c (64:80:90:24:4e:0c), Dst: Veriton_ae:98:a6 (48:5d:36:ae:98:a6)
Destination: Veriton_ae:98:a6 (48:5d:36:ae:98:a6)
Address: Veriton_ae:98:a6 (48:5d:36:ae:98:a6) = 16 bit: Globally unique address (factory default)
..... = 16 bit: Individual address (unicast)
..... = 16 bit: Individual address (unicast)
Source: IntelCor_24:4e:0c (64:80:90:24:4e:0c)
Address: IntelCor_24:4e:0c (64:80:90:24:4e:0c) = 16 bit: Globally unique address (factory default)
..... = 16 bit: Individual address (unicast)

Type: IPv4 (0x0800)
Internet Protocol Version 4, Src Port: 32148, Dst Port: 80, Seq: 1, Ack: 1, Len: 429
Transmission Control Protocol
HyperText Transfer Protocol
GET /wiresnark-labs/HTTP-ethereum1-ipb-f1e3.html HTTP/1.1\n\r
Host: gala.cs.unsw.edu.au

Destination Hardware Address (eth0), 6 bytes

Windows Type here to search

File Edit View Insert Tools Help

for next device

for destination (final)

Packets: 2139 - Displayed: 2139 (100.0%)

Profile: Default

9:05 PM 10/28/2018

4. Explain the relationship between the destination MAC address and the destination IP address.

→ MAC address is a UNIQUE address given to a machine while an IP address is used to identify a machine over the internet (public & private).
The ARP (Address Resolution Protocol) cache is the link between them. ARP's job is to map IP address to MAC address.

5. Using the terminal (cmd in Windows, Terminal in mac), run a command to display your full ARP list table. (Find out what the command is, and print a full screen shot of your result.)

→ **ipconfig /all** is a command to display your full ARP list table.

MW - a .

```

Windows PowerShell
Copyright (c) 2018 Microsoft Corporation. All rights reserved.

PS C:\Users\Dominique\OneDrive\Dropbox\juli

Part of the IP Configuration

Host Name : Dominique
Primary Dns Suffix : world
Node Type : Member Computer
IP Routing Enabled : No
WINS Proxy Enabled : No
DNS Suffix Search List : fios.router.home

Ethernet adapter Ethernet:

Media State : Media disconnected
Connection-specific DNS Suffix : Dominique
Description : Realtek PCIe GbE Family Controller
Physical Address : 08:11:32:AA:6D:3C
Link Enabled : Yes
Autoconfiguration Enabled : Yes

Ethernet adapter Ethernet 2:

Media State : Media disconnected
Connection-specific DNS Suffix : fios.router.home
Physical Address : 0A:00:00:00:00:00
Link Enabled : Yes
Autoconfiguration Enabled : Yes

Wireless LAN adapter Local Area Connection 1:

Media State : Media disconnected
Connection-specific DNS Suffix : Intel(R) Centrino(R) MAX 6216
Physical Address : 0A:00:00:2B:4F:00
Link Enabled : Yes
Autoconfiguration Enabled : Yes

Wireless LAN adapter Local Area Connection 2:

Media State : Media disconnected
Connection-specific DNS Suffix : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address : 06:00:00:24:41:0C
Link Enabled : Yes
Autoconfiguration Enabled : Yes

Windows PowerShell
Copyright (c) 2018 Microsoft Corporation. All rights reserved.

PS C:\Users\Dominique\OneDrive\Dropbox\juli

Public & private.

He command is, and

```

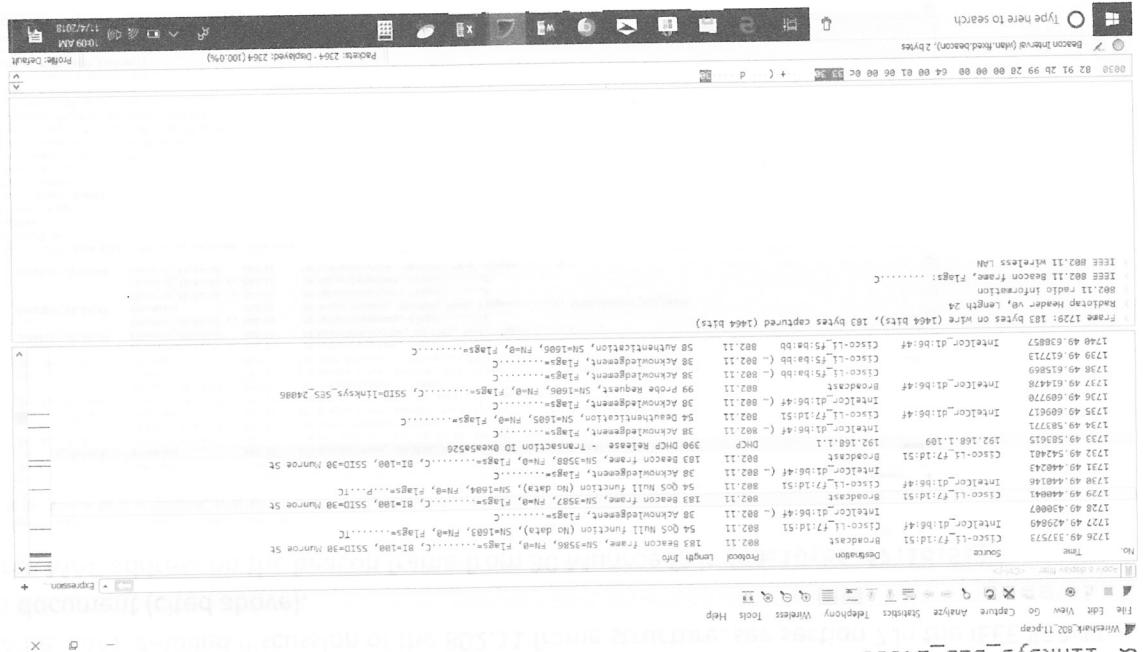
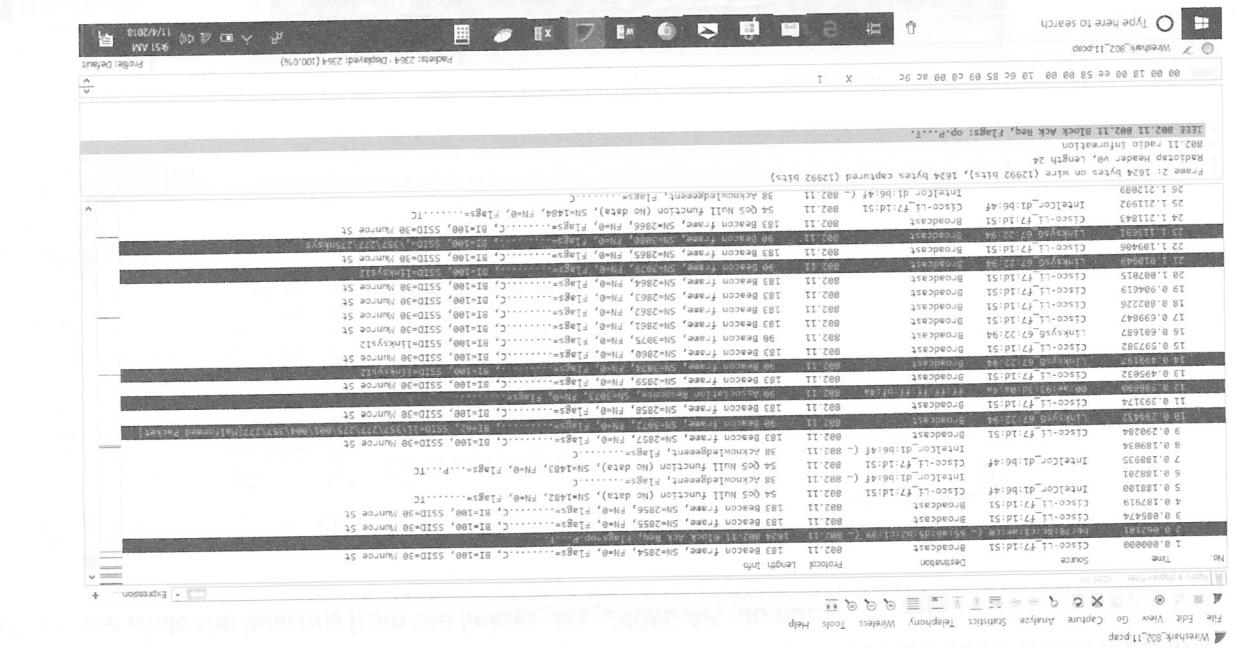
Luz Deloria

11/5/18

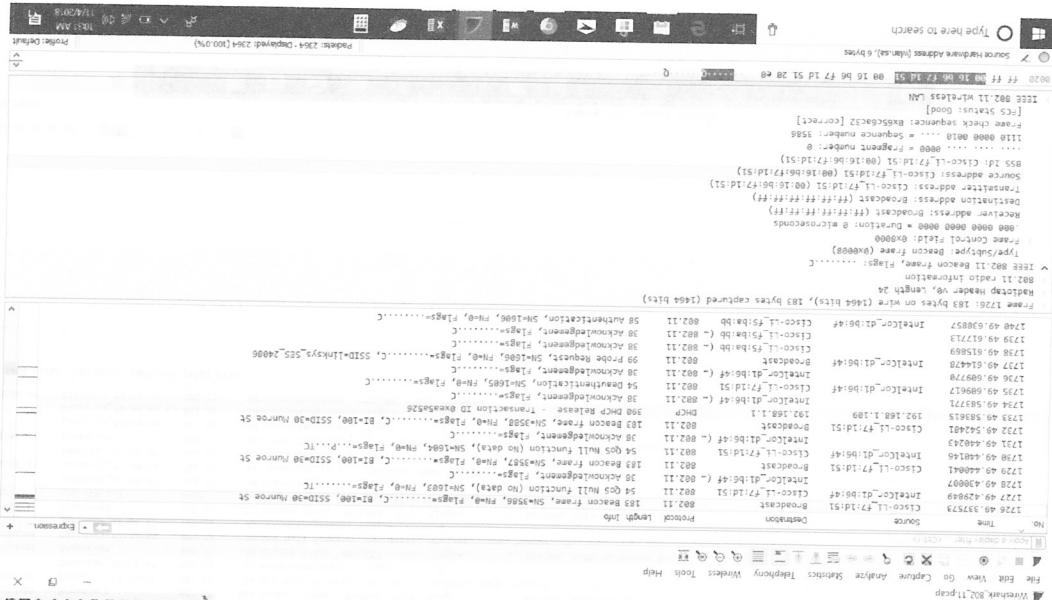
Luz

1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?
- The SSIDs of the two access points that are issuing most of the beacon frames in this trace are: 30 Munroe St

Questions:



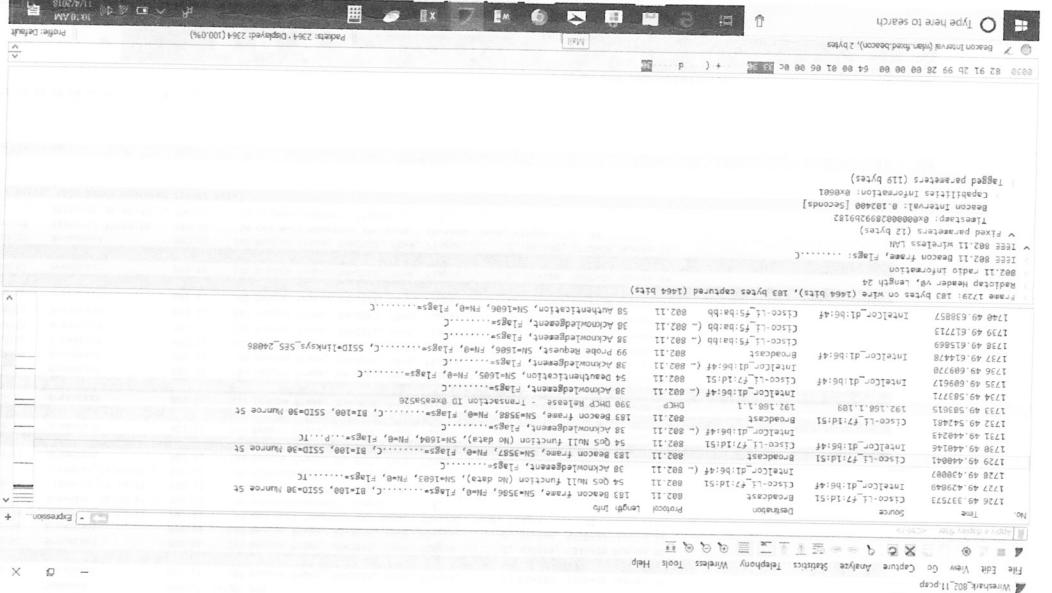
8. Linksys-SES-24086.



- The source MAC address on the beacon frame from 30 Munroe St is (00:16:b6:f7:1d:51)

Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).

3. What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St?



in the trace while the beacons from the linksys_ses_24086AP, do not.

LAN management frame as 0.102400 [Seconds]. In 30 Munroe St AP beacon frame shows regularity

- The beacon interval for both access points in reported in the beacon interval of the 802.11 wireless

containing in the beacon frame itself).

linksys_ses_24086 access point? From the 30 Munroe St, access point? (Hint: this interval of time is

2. What are the intervals of time between the transmissions of the beacon frames the

| No. | Time | Source | Destination | Protocol Length Info | Frame Info |
|----------------|------|-------------------|-------------|---|--|
| 1726 49.337573 | | Cisco-Li-f7:1d:51 | Broadcast | 802.11 183 Beacon frame, SN=3586, FN=0, Flags=..... | Frame 1726: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) Radiotap Header v0, Length/Type 802.11 Radio Information IEEE 802.11 Beacon frame, Flags:C IEEE 802.11 Beacon frame, Flags:C Type/Subtype: Beacon frame (0x0008) Frame Control Field: 0x8000 .000 0000 0000 = Duration: 0 microseconds Destination address: Broadcast (ff:ff:ff:ff:ff:ff) Receiver address: Broadcast (ff:ff:ff:ff:ff:ff) Source address: Cisco-Li-f7:1d:51 (00:16:b6:f7:1d:51) BSS ID: Cisco-Li-f7:1d:51 (00:16:b6:f7:1d:51) 0000 = Fragment number: 0 1110 0000 0010 = Sequence number: 3586 Frame check sequence: 0x65c6ac32 [correct] CTS Status: Good] IEEE 802.11 wireless LAN Fixed parameters (12 bytes) Timestamp: 0x0000002892aa0182 Beacon Interval: 0.102400 [Seconds] Capabilities Information: 0x0601 Tagged parameters (119 bytes) |

