

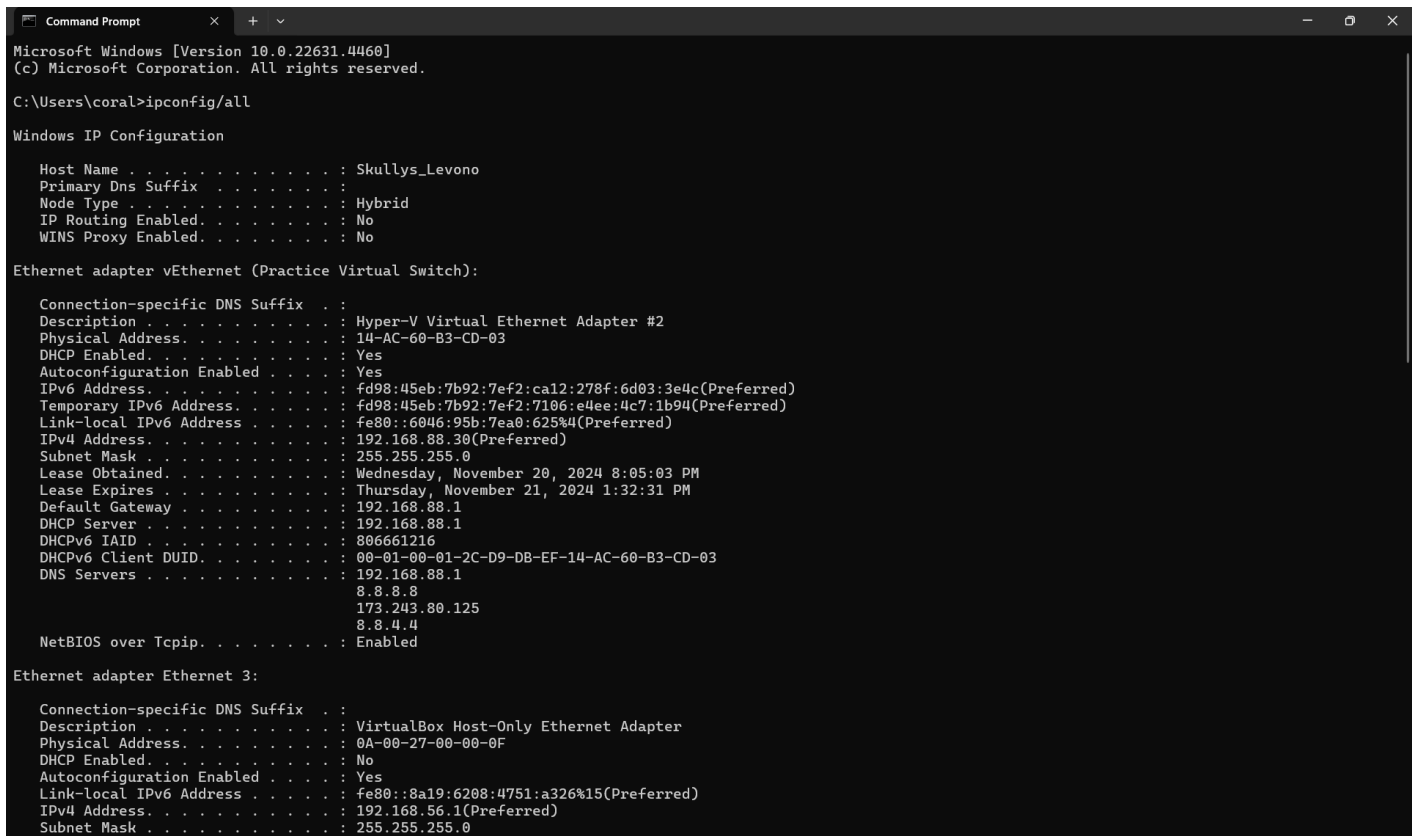
**Homework 2**

**Name: Coral S. Schmidt Montilla**

**ID#: 148830**

***Completely answer all of the following questions.***

1. Open Windows' Command Prompt and type ipconfig /all (in Linux/Unix/Mac type ifconfig). Provide a screenshot that shows the result of executing the command for the network interface in use during the exercise. This screenshot will show your computer's IP address, default gateway, and local DNS servers. *1 point*



```
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\coral>ipconfig/all

Windows IP Configuration

Host Name . . . . . : Skullys_Levono
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter vEthernet (Practice Virtual Switch):

Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter #2
Physical Address. . . . . : 14-AC-60-B3-CD-03
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : fd98:45eb:7b92:7ef2:ca12:278f:6d03:3e4c(Preferred)
Temporary IPv6 Address. . . . . : fd98:45eb:7b92:7ef2:7106:e4ee:4c7:1b94(Preferred)
Link-local IPv6 Address . . . . . : fe80::6046:95b:7ea0:625%4(Preferred)
IPv4 Address. . . . . : 192.168.88.30(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, November 20, 2024 8:05:03 PM
Lease Expires . . . . . : Thursday, November 21, 2024 1:32:31 PM
Default Gateway . . . . . : 192.168.88.1
DHCP Server . . . . . : 192.168.88.1
DHCPv6 IAID . . . . . : 806661216
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-D9-DB-EF-14-AC-60-B3-CD-03
DNS Servers . . . . . : 192.168.88.1
                        8.8.8.8
                        173.243.80.125
                        8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet 3:

Connection-specific DNS Suffix . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-0F
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8a19:6208:4751:a326%15(Preferred)
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

**Polytechnic University of Puerto Rico**  
**Electrical and Computer Engineering & Computer Science Department**  
**COE 4330, Section 80 – Computer Networks**

---

```
Command Prompt
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 1074397223
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-D9-DB-EF-14-AC-60-B3-CD-03
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 16-AC-60-B3-ED-23
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 16-AC-60-B3-FD-33
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::28a3:11e8:92b3:92f7%5(Preferred)
IPv4 Address. . . . . : 192.168.137.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 14-AC-60-B3-CD-04
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter vEthernet (Default Switch):

Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter
Physical Address. . . . . : 00-15-5D-35-2C-00
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::d935:21df:e5f4:563e%52(Preferred)
IPv4 Address. . . . . : 172.29.64.1(Preferred)
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
```

```
Command Prompt
IPv4 Address. . . . . : 192.168.137.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 14-AC-60-B3-CD-04
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter vEthernet (Default Switch):

Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter
Physical Address. . . . . : 00-15-5D-35-2C-00
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::d935:21df:e5f4:563e%52(Preferred)
IPv4 Address. . . . . : 172.29.64.1(Preferred)
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 872420701
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-D9-DB-EF-14-AC-60-B3-CD-03
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\coral>
```

**Polytechnic University of Puerto Rico**  
**Electrical and Computer Engineering & Computer Science Department**  
**COE 4330, Section 80 – Computer Networks**

---

2. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running? Include Wireshark screenshots to justify your answers. *2 points*

As you can see from the screenshots below the version of HTTP ran by my browser and server is **HTTP/1.1**.

The first screenshot shows a packet capture of an HTTP GET request. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
4228	51.209256	192.168.88.30	34.223.124.45	HTTP	504	GET / HTTP/1.1
4260	51.332644	34.223.124.45	192.168.88.30	HTTP	867	HTTP/1.1 200 OK (text/html)

The packet details pane for the selected packet (4228) shows the following structure:

- Frame 4228: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface \Device\NPF\_{CD880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0
- Ethernet II, Src: CloudNetwork\_b3:cd:03 (14:ac:60:b3:cd:03), Dst: Routerboardc\_99:fb:5a (18:fd:74:99:fb:5a)
- Internet Protocol Version 4, Src: 192.168.88.30, Dst: 34.223.124.45
- Transmission Control Protocol, Src Port: 53977, Dst Port: 80, Seq: 1, Ack: 1, Len: 450
- Hypertext Transfer Protocol
  - GET / HTTP/1.1\r\n
  - Host: neverssl.com\r\n
  - Connection: keep-alive\r\n
  - Upgrade-Insecure-Requests: 1\r\n
  - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0\r\n
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
  - Accept-Encoding: gzip, deflate\r\n
  - Accept-Language: en-US,en;q=0.9,es;q=0.8\r\n
  - \r\n
  - [Response in frame: 4260]
  - [Full request URI: http://neverssl.com/]

The second screenshot shows a packet capture of an HTTP 200 OK response. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
4228	51.209256	192.168.88.30	34.223.124.45	HTTP	504	GET / HTTP/1.1
4260	51.332644	34.223.124.45	192.168.88.30	HTTP	867	HTTP/1.1 200 OK (text/html)

The packet details pane for the selected packet (4260) shows the following structure:

- Frame 4260: 867 bytes on wire (6936 bits), 867 bytes captured (6936 bits) on interface \Device\NPF\_{CD880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0
- Ethernet II, Src: Routerboardc\_99:fb:5a (18:fd:74:99:fb:5a), Dst: CloudNetwork\_b3:cd:03 (14:ac:60:b3:cd:03)
- Internet Protocol Version 4, Src: 34.223.124.45, Dst: 192.168.88.30
- Transmission Control Protocol, Src Port: 80, Dst Port: 53977, Seq: 1461, Ack: 451, Len: 813
- [2 Reassembled TCP Segments (2273 bytes): #4259 (1460), #4260 (813)]
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
  - Date: Thu, 21 Nov 2024 17:34:46 GMT\r\n
  - Server: Apache/2.4.62 (Ubuntu)\r\n
  - Upgrade: h2,h2c\r\n
  - Connection: Upgrade, Keep-Alive\r\n
  - Last-Modified: Wed, 29 Jun 2022 00:23:33 GMT\r\n
  - ETag: "f79-5e28b29d38e93-gzip"\r\n
  - Accept-Ranges: bytes\r\n
  - Vary: Accept-Encoding\r\n
  - Content-Encoding: gzip\r\n
  - Content-Length: 1980\r\n
  - Keep-Alive: timeout=5, max=100\r\n
  - \r\n

**Polytechnic University of Puerto Rico**  
**Electrical and Computer Engineering & Computer Science Department**  
**COE 4330, Section 80 – Computer Networks**

---

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server? Include Wireshark screenshots to justify your answers. *2 points*

As shown in the screenshot bellow the IP address of my computer is **192.168.88.30** and the servers IP address is **128.119.245.12**.

The screenshot displays the Wireshark interface with a packet capture of a TCP connection. The packet list shows a SYN packet (2841) and an ACK packet (2868). The packet details pane shows the structure of the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol headers. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
2841	34.628115	192.168.88.30	128.119.245.12	TCP	66	54195 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2860	34.675829	192.168.88.30	128.119.245.12	TCP	66	54196 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2863	34.678408	192.168.88.30	128.119.245.12	TCP	66	54197 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2866	34.710573	128.119.245.12	192.168.88.30	TCP	66	80 → 54195 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
2867	34.710914	192.168.88.30	128.119.245.12	TCP	54	54195 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
2868	34.711377	192.168.88.30	128.119.245.12	HTTP	509	GET / HTTP/1.1
2870	34.728126	128.119.245.12	192.168.88.30	TCP	60	80 → 54195 [ACK] Seq=1 Ack=456 Win=43302 Len=0

Frame 2841: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{CD880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0

Ethernet II, Src: CloudNetwork\_b3:cd:03 (14:ac:60:b3:cd:03), Dst: Routerboard\_99:fb:5a (18:fd:74:99:fb:5a)

Internet Protocol Version 4, Src: 192.168.88.30, Dst: 128.119.245.12

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 52
- Identification: 0x97e3 (38883)
- > 010, .... = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0xd495 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.88.30
- Destination Address: 128.119.245.12
- [Stream index: 82]

> Transmission Control Protocol, Src Port: 54195, Dst Port: 80, Seq: 0, Len: 0

0000 18 fd 74 99 fb 5a 14 ac 60 b3 cd 03 08 00 45 00 ...t...  
0010 00 34 97 e3 40 00 00 06 d4 95 c0 a8 58 1e 80 77 ...4...  
0020 f5 0c d3 b3 00 50 72 2d 66 c4 00 00 00 00 02 ...Pr...  
0030 fa f0 38 df 00 00 02 04 05 b4 01 03 03 08 01 01 ...8...  
0040 04 02 ..

wireshark\_Wi-FiCOGX2.pcapng | Packets: 3929 - Displayed: 76 (1.9%) - Dropped: 0 (0.0%) | Profile: Default

**Polytechnic University of Puerto Rico**  
**Electrical and Computer Engineering & Computer Science Department**  
**COE 4330, Section 80 – Computer Networks**

---

4. What is the status code returned from the server to your browser? Include a Wireshark screenshot to justify your answer. *1 point*

As shown by the screenshot below the status code returned from the server to my browser is **200**  
**OK.**

The screenshot shows a Wireshark capture of an HTTP response. The packet list pane on the left shows several packets, with packet 2903 selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP 200 OK response. The packet bytes pane on the right shows the raw data of the packet, which is a 145-byte HTML document. The status bar at the bottom indicates that the response is Boolean.

No.	Time	Source	Destination	Protocol	Length	Info
2390	23.207562	192.168.88.19	192.168.88.30	HTTP/XML	1253	HTTP/1.1 200 OK
2405	23.331121	192.168.88.19	192.168.88.30	HTTP	98	HTTP/1.1 404 Not Found
2903	34.804762	128.119.245.12	192.168.88.30	HTTP	145	HTTP/1.1 200 OK (text/html)
3002	35.013955	128.119.245.12	192.168.88.30	HTTP	1190	HTTP/1.1 200 OK (JPEG JFIF image)
3020	35.325955	165.160.13.20	192.168.88.30	HTTP	230	HTTP/1.1 301 Moved Permanently
3493	39.203889	128.119.245.12	192.168.88.30	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 2903: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF\_{CD880491-6C77-45EE-81FC-2C...}

Ethernet II, Src: HewlettPacka\_23:0b:02 (48:b4:c3:23:0b:02), Dst: CloudNetwork\_b3:cd:03 (14:ac:60:b3:cd:03)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.88.30

Transmission Control Protocol, Src Port: 80, Dst Port: 54195, Seq: 2921, Ack: 456, Len: 91

[3 Reassembled TCP Segments (3011 bytes): #2901(1460), #2902(1460), #2903(91)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Thu, 21 Nov 2024 17:50:01 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Tue, 01 Mar 2016 18:57:50 GMT\r\n

Etag: "a5b-52d015789ee9e"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 2651\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

[Request in frame: 2868]

[Time since request: 0.093385000 seconds]

[Request URI: /]

[Full request URI: <http://gaia.cs.umass.edu/>]

File Data: 2651 bytes

Line-based text data: text/html (68 lines)

Frame (145 bytes) Reassembled TCP (3011 bytes)

Packets: 3929 · Displayed: 6 (0.2%) · Dropped: 0 (0.0%)

Profile: Default

**Polytechnic University of Puerto Rico**  
**Electrical and Computer Engineering & Computer Science Department**  
**COE 4330, Section 80 – Computer Networks**

---

5. When was the HTML file that you are retrieving last modified at the server? Include a Wireshark screenshot to justify your answer. *1 point*

As shown in the screenshot the HTML file that I am retrieving was last modified at the server on

**Tue, 01 Mar 2016 18:57:50 GMT\r\n.**

The screenshot shows the Wireshark interface with a packet list on the left and packet details on the right. The selected packet is an HTTP response (Frame 2903).

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
2390	23.207562	192.168.88.19	192.168.88.30	HTTP/XML	1253	HTTP/1.1 200 OK
2405	23.331121	192.168.88.19	192.168.88.30	HTTP	98	HTTP/1.1 404 Not Found
2903	34.804762	128.119.245.12	192.168.88.30	HTTP	145	HTTP/1.1 200 OK (text/html)
3002	35.013955	128.119.245.12	192.168.88.30	HTTP	1190	HTTP/1.1 200 OK (JPEG JFIF image)
3020	35.325955	165.160.13.20	192.168.88.30	HTTP	230	HTTP/1.1 301 Moved Permanently
3493	39.203889	128.119.245.12	192.168.88.30	HTTP	538	HTTP/1.1 404 Not Found (text/html)

**Packet Details:**

- Frame 2903: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF\_{CD880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0
- Ethernet II, Src: HewlettPacka\_23:0b:02 (48:b4:c3:23:0b:02), Dst: CloudNetwork\_b3:cd:03 (14:ac:60:b3:cd:03)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.88.30
- Transmission Control Protocol, Src Port: 80, Dst Port: 54195, Seq: 2921, Ack: 456, Len: 91
- [3 Reassembled TCP Segments (3011 bytes): #2901(1460), #2902(1460), #2903(91)]
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
  - Date: Thu, 21 Nov 2024 17:50:01 GMT\r\n
  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\n
  - Last-Modified: Tue, 01 Mar 2016 18:57:50 GMT\r\n
  - ETag: "a5b-52d015789ee9e"\r\n
  - Accept-Ranges: bytes\r\n
  - Content-Length: 2651\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
  - [Request in frame: 2868]
  - [Time since request: 0.093385000 seconds]
  - [Request URI: /]
  - [Full request URI: http://gaia.cs.umass.edu/]
  - File Data: 2651 bytes
- Line-based text data: text/html (68 lines)

**Packet Bytes:**

0000 14 ac 60 b3 cd 03 48 b4 c3 23 0b 02 08 00 45 00 ...H-  
0010 00 83 68 46 40 00 2a 06 59 e4 80 77 f5 0c c0 a8 ...hF@\*  
0020 58 1e 00 50 d3 b3 4d c2 d5 d9 72 2d 68 8c 50 18 X..P..H-  
0030 01 53 82 a5 00 00 66 3d 22 2f 6e 65 74 77 6f 72 S...fz  
0040 6b 73 2f 72 65 73 6f 75 72 63 65 73 2f 69 6e 64 ks/resou  
0050 65 78 2e 68 74 6d 6c 22 3e 20 0a 52 45 53 4f 55 ex.html"  
0060 52 43 45 53 3c 2f 61 3e 20 0a 3c 70 3e 0a 0a 3c RCES</a>  
0070 2f 66 6f 6e 74 3e 0a 3c 2f 63 65 6e 74 65 72 3e /font><  
0080 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e </body><  
0090 0a

Frame (145 bytes) Reassembled TCP (3011 bytes)

Packets: 3020 - Disassembled: 6 (0.2%) - Reassembled: 0 (0.0%) Profile: Default

**Polytechnic University of Puerto Rico**  
**Electrical and Computer Engineering & Computer Science Department**  
**COE 4330, Section 80 – Computer Networks**

---

6. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET? If so, write down the field’s value. Include a Wireshark screenshot to justify your answer. *1 point*

As shown in the screenshot bellow **there is no IF-MODIFIED-SINCE** line in the HTTP GET.

The screenshot shows the Wireshark interface with a filter set to `http.request.method == "GET"`. The packet list displays several HTTP GET requests. The selected packet (No. 2868) is an HTTP GET request to `/` from `192.168.88.30` to `128.119.245.12`. The packet details pane shows the structure of the request, including the Request Method (GET), Request URI (/), Request Version (HTTP/1.1), Host (gaia.cs.umass.edu), Connection (keep-alive), Upgrade-Insecure-Requests (1), User-Agent (Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0), Accept (text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7), Accept-Encoding (gzip, deflate), and Accept-Language (en-US,en;q=0.9,es;q=0.8). The packet bytes pane shows the raw data of the request, including the GET / HTTP/1.1 line and the Host: gaia.cs.umass.edu header.

No.	Time	Source	Destination	Protocol	Length	Info
2386	23.160223	192.168.88.30	192.168.88.19	HTTP	238	GET /ssdp/device-desc.xml HTTP/1.1
2398	23.288602	192.168.88.30	192.168.88.19	HTTP	247	GET /apps/com.spotify.Spotify.TVv2 HTTP/1.1
2868	34.711377	192.168.88.30	128.119.245.12	HTTP	509	GET / HTTP/1.1
2910	34.826282	192.168.88.30	128.119.245.12	HTTP	457	GET /cnrg_imap.jpg HTTP/1.1
3018	35.120429	192.168.88.30	165.160.13.20	HTTP	472	GET /images/qupmember.gif HTTP/1.1
3450	38.811525	192.168.88.30	128.119.245.12	HTTP	455	GET /favicon.ico HTTP/1.1

Frame 2868: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface \Device\NPF\_{CD880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0  
> Ethernet II, Src: CloudNetwork\_b3:cd:03 (14:ac:60:b3:cd:03), Dst: Routerboardc\_99:fb:5a (18:fd:74:99:fb:5a)  
> Internet Protocol Version 4, Src: 192.168.88.30, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 54195, Dst Port: 80, Seq: 1, Ack: 455  
▼ Hypertext Transfer Protocol  
 GET / HTTP/1.1\r\n Request Method: GET  
 Request URI: /\n Request Version: HTTP/1.1  
Host: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9,es;q=0.8\r\n\r\n[Response in frame: 2903]  
[Full request URI: http://gaia.cs.umass.edu/]

**Polytechnic University of Puerto Rico**  
**Electrical and Computer Engineering & Computer Science Department**  
**COE 4330, Section 80 – Computer Networks**

---

7. Inspect the contents of the server response. Did the server explicitly return the contents of the file?  
How can you tell? Include a Wireshark screenshot to justify your answer. *1 point*

As you can see from the screenshot below **the server explicitly returned the contents of the file**. This is shown by the **Response Code: 200 OK** and the **Content-Length** field, which specifies the size of the returned file. The **Content-Type** field also indicates the file type.

The screenshot shows a Wireshark capture of an HTTP response. The packet list pane at the top shows four packets. Packet 1967 is an HTTP 200 OK response from 192.229.211.108 to 192.168.88.30. The packet details pane shows the following structure:

- Frame 1967: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface \Device\NPF\_{CD880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0
- Ethernet II, Src: HewlettPacka\_22:97:12 (48:b4:c3:22:97:12), Dst: CloudNetwork\_b3:cd:03 (14:ac:60:b3:cd:03)
- Internet Protocol Version 4, Src: 192.229.211.108, Dst: 192.168.88.30
- Transmission Control Protocol, Src Port: 80, Dst Port: 51221, Seq: 1461, Ack: 302, Len: 43
- [2 Reassembled TCP Segments (1503 bytes): #1966(1468), #1967(43)]
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
    - Response Version: HTTP/1.1
    - Status Code: 200
      - [Status Code Description: OK]
    - Response Phrase: OK
    - Accept-Ranges: bytes\r\n
    - Age: 90925\r\n
    - cache-control: max-age=172800, public\r\n
    - Content-Type: application/pkix-cert\r\n
    - Date: Thu, 21 Nov 2024 20:31:29 GMT\r\n
    - Etag: "5a28641a-48f"\r\n
    - expires: Sat, 23 Nov 2024 20:31:29 GMT\r\n
    - last-modified: Wed, 06 Dec 2017 21:41:46 GMT\r\n
    - Server: ECacc (mid/874E)\r\n
    - X-Cache: HIT\r\n
  - Content-Length: 1167\r\n
    - [Content length: 1167]
  - \r\n
  - [Request in frame: 1726]
  - [Time since request: 0.314512000 seconds]
  - [Request URI: /ThawteTLRSACAG1.crt]
  - [Full request URI: http://cacerts.thawte.com/ThawteTLRSACAG1.crt]
  - File Data: 1167 bytes
- PKIX CERT File Format

The packet bytes pane on the right shows the raw data of the response, starting with 0000 14 ac 60 b3 cd 03 48 b4 c3 22 97 12.



**Polytechnic University of Puerto Rico**  
**Electrical and Computer Engineering & Computer Science Department**  
**COE 4330, Section 80 – Computer Networks**

---

8. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header? Include a Wireshark screenshot to justify your answer. *1 point*

As you can see from the screenshot below the **If-Modified-Since** line is present in the second HTTP GET request. The date shown is **Thu, 25 Jul 2024 14:48:00 GMT\r\n**.

