

Ex0- WireSharkIntro

Q1- As you can see, at the image below there are 3 different protocols,

1.TCP.

2.HTTP.

3.DNS.

The image shows a Wireshark packet capture interface. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (packet 10), which is an HTTP GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------------|-----------------|----------|--------|-----------------------------------------------------------------------------------|
| 1 | 0.000000 | 192.168.1.156 | 128.119.245.12 | TCP | 60 | Seq=487 Win=0 Len=0 [RST] 52031 → 80 60 |
| 2 | 0.000000 | 192.168.1.156 | 128.119.245.12 | TCP | 60 | Seq=2 Ack=2 Win=29312 Len=0 [ACK] 52032 → 80 60 |
| 3 | 0.000000 | 192.168.1.156 | 128.119.245.12 | TCP | 66 | Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 [SYN, ACK] 52037 → 80 66 |
| 4 | 0.000000 | 192.168.1.156 | 128.119.245.12 | TCP | 54 | Seq=1 Ack=1 Win=131328 Len=0 [ACK] 80 → 52037 54 |
| 5 | 0.000000 | 128.119.245.12 | 192.168.1.156 | HTTP | 662 | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 662 |
| 6 | 0.000000 | 192.168.1.156 | 128.119.245.12 | TCP | 66 | Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 [SYN, ACK] 52036 → 80 66 |
| 7 | 0.000000 | 128.119.245.12 | 192.168.1.156 | TCP | 54 | Seq=1 Ack=1 Win=131328 Len=0 [ACK] 80 → 52036 54 |
| 8 | 0.000000 | 192.168.1.156 | 128.119.245.12 | TCP | 60 | Seq=1 Ack=609 Win=30464 Len=0 [ACK] 52037 → 80 60 |
| 9 | 0.000000 | 192.168.1.156 | 128.119.245.12 | HTTP | 293 | HTTP/1.1 304 Not Modified 293 |
| 10 | 0.000000 | 192.168.1.1 | 192.168.1.156 | DNS | 70 | Standard query 0xcddc A google.com 70 |
| 11 | 0.000000 | 192.168.1.156 | 192.168.1.1 | DNS | 86 | Standard query response 0xcddc A google.com A 142.250.185.206 86 |
| 12 | 0.000000 | 192.168.1.156 | 128.119.245.12 | TCP | 54 | Seq=609 Ack=240 Win=131072 Len=0 [ACK] 80 → 52037 54 |
| 13 | 0.000000 | 142.250.185.206 | 192.168.1.156 | TCP | 66 | Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 [SYN] 443 → 52038 66 |
| 14 | 0.000000 | 192.168.1.156 | 142.250.185.206 | TCP | 66 | Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256 [SYN, ACK] 52038 → 443 66 |
| 15 | 0.000000 | 192.168.1.156 | 142.250.185.206 | TCP | 54 | Seq=1 Ack=1 Win=131328 Len=0 [ACK] 443 → 52038 54 |

Packet 10 Details:

- Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.156
- Transmission Control Protocol, Src Port: 80, Dst Port: 52013, Seq: 1, Ack: 609, Len: 239
- Hypertext Transfer Protocol

Raw Data:

```
0000  3c 58 c2 a8 1d d4 35 1d 51 4c bb 08 00 45 a0  <X....5..QL...E.
0010  01 17 dd 00 40 00 26 06 3e 78 80 77 f5 0c c0 a8  ...@.&..>x-w....
0020  01 9c 00 50 cb 2d 2a 00 0b 6a 7e 71 d3 3f 50 18  ...P-.-. .j~q?P.
0030  00 ee 2e 2f 00 00 48 54 54 50 2f 31 2e 31 20 33  .../..HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d  04 Not Modified.
0050  0a 44 61 74 65 3a 20 54 68 75 2c 20 30 34 20 4e  .Date: T hu, 04 N
0060  6f 76 20 32 30 32 31 20 31 35 3a 35 33 3a 32 36  ov 2021 15:53:26
0070  20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70  GMT--Se rver: Ap
```

Q2- As you can see in the image below, the time of the GET request took 5.471426 and the OK respond took 5.689781 , it means that all the request took 0.218355 sec.

| | | Info | Length | Protocol | Destination | Source | Time | .No |
|--|--|------------------------------------------------|-------------------------------|----------|----------------|----------------|------------|-----|
| | | GET /wireshark-labs/INTRO-wireshark-file1.html | HTTP/1.1 662 | HTTP | 128.119.245.12 | 192.168.1.156 | 5.47142632 | |
| | | | HTTP/1.1 304 Not Modified 293 | HTTP | 192.168.1.156 | 128.119.245.12 | 5.68978138 | |

Q3- As you can see in the image below, the IP address of gaia.cd.umass.edu is 128.119.245.12.
My IP address id 192.168.1.156.

| | | Info | Length | Protocol | Destination | Source | Time | .No |
|--|--|------------------------------------------------|-------------------------------|----------|----------------|----------------|------------|-----|
| | | GET /wireshark-labs/INTRO-wireshark-file1.html | HTTP/1.1 662 | HTTP | 128.119.245.12 | 192.168.1.156 | 5.47142632 | |
| | | | HTTP/1.1 304 Not Modified 293 | HTTP | 192.168.1.156 | 128.119.245.12 | 5.68978138 | |

Q4- As you can see in the image below, if we would like to print our OK and GET requests, we can do so.

```

38 5.689781 128.119.245.12 192.168.1.156 HTTP 293 HTTP/1.1 304 Not Modified
Frame 38: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
Interface id: 0 (\Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA})
Encapsulation type: Ethernet (1)
Arrival Time: Nov 4, 2021 17:53:26.994234000 Jerusalem Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1636041206.994234000 seconds
[Time delta from previous captured frame: 0.000859000 seconds]
[Time delta from previous displayed frame: 0.218355000 seconds]
[Time since reference or first frame: 5.689781000 seconds]
Frame Number: 38
Frame Length: 293 bytes (2344 bits)
Capture Length: 293 bytes (2344 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.156
Transmission Control Protocol, Src Port: 80, Dst Port: 52013, Seq: 1, Ack: 609, Len: 239
Hypertext Transfer Protocol

```

Part 2-

Q1- As you can see in the image below, my browser use HTTP 1.1.

The image shows a Wireshark packet capture window titled "Capturing from Wi-Fi". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The main display area is divided into three panes. The top pane shows a list of captured packets, with the first four packets highlighted in green. The middle pane shows the details of the selected packet (Frame 229), and the bottom pane shows the raw packet data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--------------------------------------------------------|
| 229 | 3.486956 | 192.168.1.156 | 128.119.245.12 | HTTP | 550 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 246 | 3.680718 | 128.119.245.12 | 192.168.1.156 | HTTP | 784 | HTTP/1.1 200 OK (text/html) |
| 250 | 3.755343 | 192.168.1.156 | 128.119.245.12 | HTTP | 496 | GET /favicon.ico HTTP/1.1 |
| 252 | 3.948994 | 128.119.245.12 | 192.168.1.156 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

Frame 229: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d), Dst: Technico_51:4c:bb (d4:35:1d:51:4c:bb)
> Internet Protocol Version 4, Src: 192.168.1.156, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52175, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
> Hypertext Transfer Protocol

0000 d4 35 1d 51 4c bb 3c 58 c2 a8 a8 1d 08 00 45 00 -5 QL<XE-
0010 02 18 3c 45 40 00 80 06 00 00 c0 a8 01 9c 80 77 -<<E@-...w
0020 f5 0c cb cf 00 50 58 1b 11 8f 10 9c 6a 1c 50 18PX....j.P-
0030 02 01 39 d3 00 00 47 45 54 20 2f 77 69 72 65 73 --9...GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68 ireshark -file2.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1--Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas

Wi-Fi: <live capture in progress> | Packets: 303 · Displayed: 4 (1.3%) | Profile: Default

Q2- As you can see in the image below, I have marked the language which our WireShark work with, and as we can see, its English.

Wireshark interface showing a capture of HTTP traffic. The packet list shows a GET request from 192.168.1.155 to 128.119.245.12. The packet details show the HTTP request with 'Accept-Language: en-US,en;q=0.5' highlighted in blue. The packet bytes show the raw data with 'Accept-Language: en-US,en;q=0.5' highlighted in blue.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--------------------------------------------------------|
| 453 | 53.352985 | 192.168.1.155 | 128.119.245.12 | HTTP | 443 | GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 |
| 456 | 53.559069 | 128.119.245.12 | 192.168.1.155 | HTTP | 540 | HTTP/1.1 200 OK (text/html) |
| 458 | 53.619044 | 192.168.1.155 | 128.119.245.12 | HTTP | 400 | GET /favicon.ico HTTP/1.1 |
| 460 | 53.865464 | 128.119.245.12 | 192.168.1.155 | HTTP | 539 | HTTP/1.1 404 Not Found (text/html) |

Frame 453: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
Ethernet II, Src: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d), Dst: Technico_51:4c:bb (d4:35:1d:51:4c:bb)
Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58786, Dst Port: 80, Seq: 1, Ack: 1, Len: 389
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 456]

0140 0d 0a 41 63 65 70 74 2d 4c 61 6e 67 75 61 67 --Accept-Language
0150 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e e: en-US ,en;q=0.
0160 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 s: Accept-Encodi
0170 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 ng: gzip , deflat
0180 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b e: Conne ction: k
0190 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 eep-aliv e: Upgra
01a0 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ

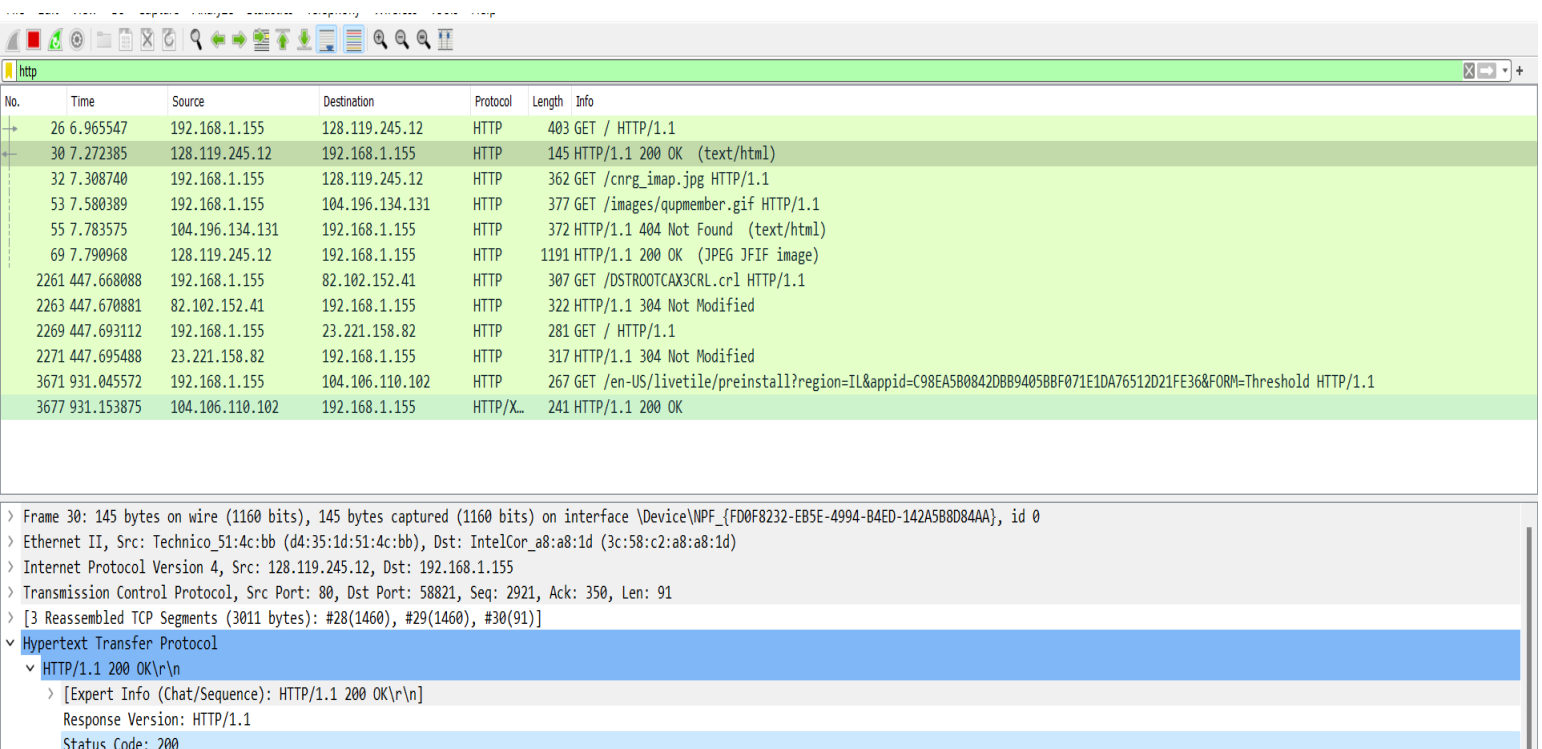
HTTP Accept Language (http.accept_language), 33 bytes | Packets: 949 · Displayed: 4 (0.4%) | Profile: Default

**Q3- As you can see in the image below, the source IP (which is my computer IP) is 192.168.1.155.
And gaia.cs.umass.edu's IP is 128.119.245.12.**

Wireshark interface showing a capture of HTTP traffic. The packet list shows a GET request from 192.168.1.155 to 128.119.245.12. The packet details show the HTTP request with 'Accept-Language: en-US,en;q=0.5' highlighted in blue.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|-----------------------------|
| 26 | 6.965547 | 192.168.1.155 | 128.119.245.12 | HTTP | 403 | GET / HTTP/1.1 |
| 30 | 7.272385 | 128.119.245.12 | 192.168.1.155 | HTTP | 145 | HTTP/1.1 200 OK (text/html) |

Q4- As you can see in the image below, the status code is 200 (which I marked below).

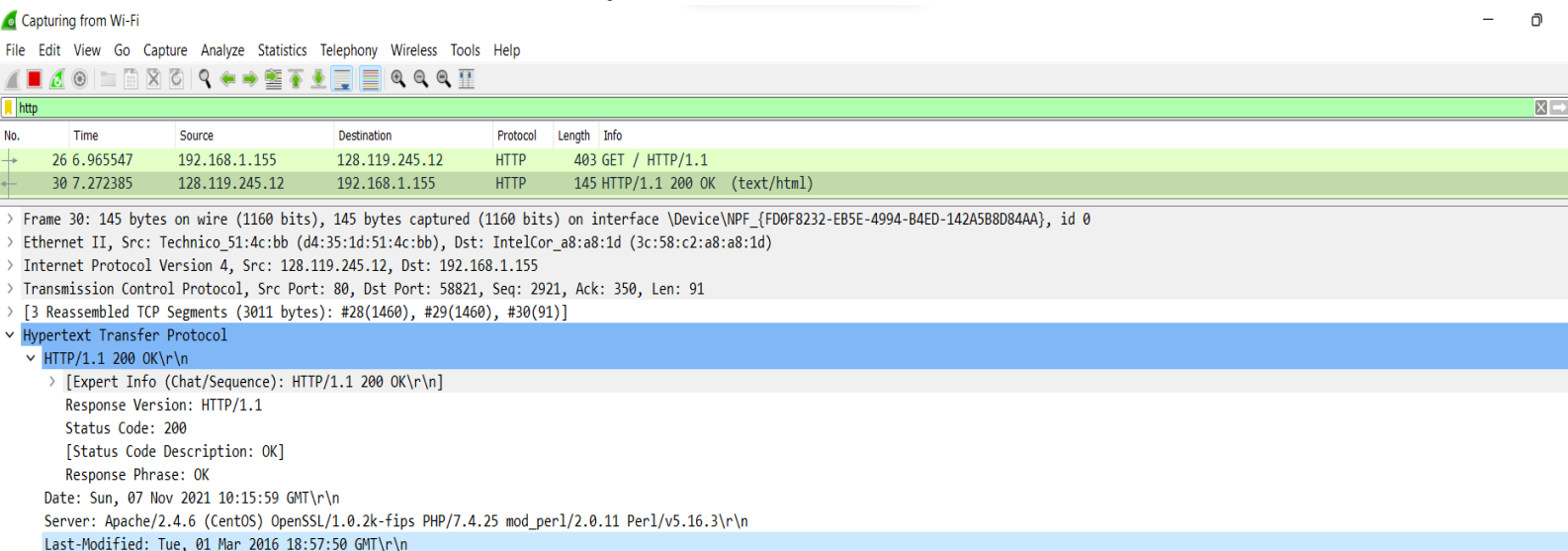


The image shows a Wireshark packet capture of an HTTP transaction. The packet list pane displays several packets, with packet 30 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded, showing the status code 200.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|-----------------|-----------------|----------|--------|-----------------------------------------------------------------------------------------------------------------|
| 26 | 6.965547 | 192.168.1.155 | 128.119.245.12 | HTTP | 403 | GET / HTTP/1.1 |
| 30 | 7.272385 | 128.119.245.12 | 192.168.1.155 | HTTP | 145 | HTTP/1.1 200 OK (text/html) |
| 32 | 7.308740 | 192.168.1.155 | 128.119.245.12 | HTTP | 362 | GET /cnrg_imap.jpg HTTP/1.1 |
| 53 | 7.580389 | 192.168.1.155 | 104.196.134.131 | HTTP | 377 | GET /images/qupmember.gif HTTP/1.1 |
| 55 | 7.783575 | 104.196.134.131 | 192.168.1.155 | HTTP | 372 | HTTP/1.1 404 Not Found (text/html) |
| 69 | 7.790968 | 128.119.245.12 | 192.168.1.155 | HTTP | 1191 | HTTP/1.1 200 OK (JPEG JFIF image) |
| 2261 | 447.668088 | 192.168.1.155 | 82.102.152.41 | HTTP | 307 | GET /DSTROOTCAX3CRL.crl HTTP/1.1 |
| 2263 | 447.670881 | 82.102.152.41 | 192.168.1.155 | HTTP | 322 | HTTP/1.1 304 Not Modified |
| 2269 | 447.693112 | 192.168.1.155 | 23.221.158.82 | HTTP | 281 | GET / HTTP/1.1 |
| 2271 | 447.695488 | 23.221.158.82 | 192.168.1.155 | HTTP | 317 | HTTP/1.1 304 Not Modified |
| 3671 | 931.045572 | 192.168.1.155 | 104.106.110.102 | HTTP | 267 | GET /en-US/livetile/preinstall?region=IL&appid=C98EA580842D8B94058BF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1 |
| 3677 | 931.153875 | 104.106.110.102 | 192.168.1.155 | HTTP/X. | 241 | HTTP/1.1 200 OK |

Frame 30: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A588D84AA}, id 0
Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
Transmission Control Protocol, Src Port: 80, Dst Port: 58821, Seq: 2921, Ack: 350, Len: 91
[3 Reassembled TCP Segments (3011 bytes): #28(1460), #29(1460), #30(91)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200

Q5- As you can see in the image below, every html file has a date which show when it was last modified, in our case, the html file was last modified in Tuesday, 01 March 2016 18:57:50.



The image shows a Wireshark packet capture of an HTTP transaction, similar to the one above. The packet list pane displays several packets, with packet 30 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded, showing the status code 200 and various headers including Date, Server, and Last-Modified.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|-----------------------------|
| 26 | 6.965547 | 192.168.1.155 | 128.119.245.12 | HTTP | 403 | GET / HTTP/1.1 |
| 30 | 7.272385 | 128.119.245.12 | 192.168.1.155 | HTTP | 145 | HTTP/1.1 200 OK (text/html) |

Frame 30: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A588D84AA}, id 0
Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
Transmission Control Protocol, Src Port: 80, Dst Port: 58821, Seq: 2921, Ack: 350, Len: 91
[3 Reassembled TCP Segments (3011 bytes): #28(1460), #29(1460), #30(91)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Sun, 07 Nov 2021 10:15:59 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Tue, 01 Mar 2016 18:57:50 GMT\r\n

Q6- As you can see in the image below, the number of bite, which returned from my browser, are 2651.

| http | | | | | | |
|------|----------|----------------|----------------|----------|--------|-----------------------------|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 26 | 6.965547 | 192.168.1.155 | 128.119.245.12 | HTTP | 403 | GET / HTTP/1.1 |
| 30 | 7.272385 | 128.119.245.12 | 192.168.1.155 | HTTP | 145 | HTTP/1.1 200 OK (text/html) |

> Frame 30: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0

> Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155

> Transmission Control Protocol, Src Port: 80, Dst Port: 58821, Seq: 2921, Ack: 350, Len: 91

> [3 Reassembled TCP Segments (3011 bytes): #28(1460), #29(1460), #30(91)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]Response Version: HTTP/1.1Status Code: 200[Status Code Description: OK]Response Phrase: OKDate: Sun, 07 Nov 2021 10:15:59 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Tue, 01 Mar 2016 18:57:50 GMT\r\nEtag: "a5b-52d015789ee9e"\r\nAccept-Ranges: bytes\r\nContent-Length: 2651\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/1][Time since request: 0.306838000 seconds][Request in frame: 26][Request URI: http://gaia.cs.umass.edu/]File Data: 2651 bytes

Q7- As you can see in the image below there are exactly the same number of content file and file data, so the answer is: No, there is no data which not display.

| http | | | | | | |
|------|----------|----------------|----------------|----------|--------|-----------------------------|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 26 | 6.965547 | 192.168.1.155 | 128.119.245.12 | HTTP | 403 | GET / HTTP/1.1 |
| 30 | 7.272385 | 128.119.245.12 | 192.168.1.155 | HTTP | 145 | HTTP/1.1 200 OK (text/html) |

> Frame 30: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0

> Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155

> Transmission Control Protocol, Src Port: 80, Dst Port: 58821, Seq: 2921, Ack: 350, Len: 91

> [3 Reassembled TCP Segments (3011 bytes): #28(1460), #29(1460), #30(91)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]Response Version: HTTP/1.1Status Code: 200[Status Code Description: OK]Response Phrase: OKDate: Sun, 07 Nov 2021 10:15:59 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Tue, 01 Mar 2016 18:57:50 GMT\r\nEtag: "a5b-52d015789ee9e"\r\nAccept-Ranges: bytes\r\nContent-Length: 2651\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/1][Time since request: 0.306838000 seconds][Request in frame: 26][Request URI: http://gaia.cs.umass.edu/]File Data: 2651 bytes

Q8- No, we cannot see the Last Modified information in GET requests.

Q9- As you can see in the image below, the html content in our inspecting is exactly like the browser content.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--------------------------------------------------------|
| 10 | 0.716630 | 34.107.221.82 | 192.168.1.155 | HTTP | 273 | HTTP/1.1 200 OK (text/plain) |
| 26 | 2.916294 | 192.168.1.155 | 128.119.245.12 | HTTP | 443 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 31 | 3.114445 | 128.119.245.12 | 192.168.1.155 | HTTP | 784 | HTTP/1.1 200 OK (text/html) |
| 36 | 3.171067 | 192.168.1.155 | 128.119.245.12 | HTTP | 400 | GET /favicon.ico HTTP/1.1 |
| 43 | 3.379000 | 128.119.245.12 | 192.168.1.155 | HTTP | 539 | HTTP/1.1 404 Not Found (text/html) |

> Frame 31: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
> Transmission Control Protocol, Src Port: 80, Dst Port: 58984, Seq: 1, Ack: 390, Len: 730
> Hypertext Transfer Protocol
v Line-based text data: text/html (10 lines)
\n<html>\n\n\nCongratulations again! Now you've downloaded the file lab2-2.html.
\nThis file's last modification date will not change. <p>\nThus if you download this multiple times on your browser, a complete copy
\nwill only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\nfield in your browser's HTTP GET request to the server.\n\n</html>\n

Q10- Yes, As we can see in the second get request, now we can see the "IF-Modified-Since", and the date is Sunday, 07 November, 2021 06:59:01.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--------------------------------------------------------|
| 10 | 3.123942 | 192.168.1.155 | 128.119.245.12 | HTTP | 555 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 12 | 3.338219 | 128.119.245.12 | 192.168.1.155 | HTTP | 294 | HTTP/1.1 304 Not Modified |

> Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d), Dst: Technico_51:4c:bb (d4:35:1d:51:4c:bb)
> Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59034, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
> Hypertext Transfer Protocol
v GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nIf-Modified-Since: Sun, 07 Nov 2021 06:59:01 GMT\r\nIf-None-Match: "173-5d02d6946d99"\r\nCache-Control: max-age=0\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 12]

Q11- The HTTP status code which return is 304, and the phrase contents which returned in "Not Modified".

Right now we see that the contents which return is not the file content, the reason for that is that the status code is "Not Modified", all of the details we got from the website at the first time we visit in is already saved in my computer. In addition, we see that this packet is much smaller than the first time we visit this website.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--------------------------------------------------------|
| 20 | 4.480640 | 192.168.1.155 | 128.119.245.12 | HTTP | 555 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 22 | 4.682332 | 128.119.245.12 | 192.168.1.155 | HTTP | 294 | HTTP/1.1 304 Not Modified |

> Frame 22: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A588D84AA}, id 0
> Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
> Transmission Control Protocol, Src Port: 80, Dst Port: 59068, Seq: 1, Ack: 502, Len: 240

▼ Hypertext Transfer Protocol

▼ HTTP/1.1 304 Not Modified\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]

Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
Date: Sun, 07 Nov 2021 11:27:02 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\nConnection: Keep-Alive\r\nKeep-Alive: timeout=5, max=100\r\nETag: "173-5d02d6946d99"\r\n\r\n\r\n[HTTP response 1/1]
[Time since request: 0.201692000 seconds]
[\[Request in frame: 20\]](#)
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

Q12- There is only one GET request for Bill or Rights and the number of packet is 32.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|-----------------------------------------------------------------------------------------|
| 22 | 11.876831 | 192.168.1.155 | 74.125.133.188 | TCP | 55 | 50847 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1 |
| 23 | 11.939164 | 74.125.133.188 | 192.168.1.155 | TCP | 66 | 5228 → 50847 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2 |
| 27 | 14.020022 | 192.168.1.155 | 128.119.245.12 | TCP | 66 | 59220 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 28 | 14.021321 | 192.168.1.155 | 128.119.245.12 | TCP | 66 | 59221 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 30 | 14.214447 | 128.119.245.12 | 192.168.1.155 | TCP | 66 | 80 → 59220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 31 | 14.214520 | 192.168.1.155 | 128.119.245.12 | TCP | 54 | 59220 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 32 | 14.214830 | 192.168.1.155 | 128.119.245.12 | HTTP | 443 | GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| 33 | 14.229809 | 128.119.245.12 | 192.168.1.155 | TCP | 66 | 80 → 59221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 34 | 14.229867 | 192.168.1.155 | 128.119.245.12 | TCP | 54 | 59221 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 36 | 14.408929 | 128.119.245.12 | 192.168.1.155 | TCP | 60 | 80 → 59220 [ACK] Seq=1 Ack=390 Win=30336 Len=0 |
| 37 | 14.409308 | 128.119.245.12 | 192.168.1.155 | TCP | 1514 | 80 → 59220 [ACK] Seq=1 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU] |
| 38 | 14.411037 | 128.119.245.12 | 192.168.1.155 | TCP | 1514 | 80 → 59220 [ACK] Seq=1461 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU] |
| 39 | 14.411037 | 128.119.245.12 | 192.168.1.155 | TCP | 1514 | 80 → 59220 [ACK] Seq=2921 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU] |
| 40 | 14.411037 | 128.119.245.12 | 192.168.1.155 | HTTP | 535 | HTTP/1.1 200 OK (text/html) |
| 41 | 14.411135 | 192.168.1.155 | 128.119.245.12 | TCP | 54 | 59220 → 80 [ACK] Seq=390 Ack=4862 Win=131328 Len=0 |

Q13- As you can see in the image below, it contain the message "OK", the number of packet is 40.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|-----------------------------------------------------------------------------------------|
| 22 | 11.876831 | 192.168.1.155 | 74.125.133.188 | TCP | 55 | 50847 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1 |
| 23 | 11.939164 | 74.125.133.188 | 192.168.1.155 | TCP | 66 | 5228 → 50847 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2 |
| 27 | 14.020022 | 192.168.1.155 | 128.119.245.12 | TCP | 66 | 59220 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 28 | 14.021321 | 192.168.1.155 | 128.119.245.12 | TCP | 66 | 59221 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 30 | 14.214447 | 128.119.245.12 | 192.168.1.155 | TCP | 66 | 80 → 59220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 31 | 14.214520 | 192.168.1.155 | 128.119.245.12 | TCP | 54 | 59220 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 32 | 14.214830 | 192.168.1.155 | 128.119.245.12 | HTTP | 443 | GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| 33 | 14.229809 | 128.119.245.12 | 192.168.1.155 | TCP | 66 | 80 → 59221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 34 | 14.229867 | 192.168.1.155 | 128.119.245.12 | TCP | 54 | 59221 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 36 | 14.408929 | 128.119.245.12 | 192.168.1.155 | TCP | 60 | 80 → 59220 [ACK] Seq=1 Ack=390 Win=30336 Len=0 |
| 37 | 14.409308 | 128.119.245.12 | 192.168.1.155 | TCP | 1514 | 80 → 59220 [ACK] Seq=1 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU] |
| 38 | 14.411037 | 128.119.245.12 | 192.168.1.155 | TCP | 1514 | 80 → 59220 [ACK] Seq=1461 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU] |
| 39 | 14.411037 | 128.119.245.12 | 192.168.1.155 | TCP | 1514 | 80 → 59220 [ACK] Seq=2921 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU] |
| 40 | 14.411037 | 128.119.245.12 | 192.168.1.155 | HTTP | 535 | HTTP/1.1 200 OK (text/html) |

> Frame 40: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
> Transmission Control Protocol, Src Port: 80, Dst Port: 59220, Seq: 4381, Ack: 390, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #37(1460), #38(1460), #39(1460), #40(481)]
v Hypertext Transfer Protocol
v HTTP/1.1 200 OK\r\n

Q14- As we can see in the image below the status code is 200, and the response phrase is "OK".

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|-----------------------------------------------------------------------------------------|
| 22 | 11.876831 | 192.168.1.155 | 74.125.133.188 | TCP | 55 | 50847 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1 |
| 23 | 11.939164 | 74.125.133.188 | 192.168.1.155 | TCP | 66 | 5228 → 50847 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2 |
| 27 | 14.020022 | 192.168.1.155 | 128.119.245.12 | TCP | 66 | 59220 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 28 | 14.021321 | 192.168.1.155 | 128.119.245.12 | TCP | 66 | 59221 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 30 | 14.214447 | 128.119.245.12 | 192.168.1.155 | TCP | 66 | 80 → 59220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 31 | 14.214520 | 192.168.1.155 | 128.119.245.12 | TCP | 54 | 59220 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 32 | 14.214830 | 192.168.1.155 | 128.119.245.12 | HTTP | 443 | GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| 33 | 14.229809 | 128.119.245.12 | 192.168.1.155 | TCP | 66 | 80 → 59221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 34 | 14.229867 | 192.168.1.155 | 128.119.245.12 | TCP | 54 | 59221 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 36 | 14.408929 | 128.119.245.12 | 192.168.1.155 | TCP | 60 | 80 → 59220 [ACK] Seq=1 Ack=390 Win=30336 Len=0 |
| 37 | 14.409308 | 128.119.245.12 | 192.168.1.155 | TCP | 1514 | 80 → 59220 [ACK] Seq=1 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU] |
| 38 | 14.411037 | 128.119.245.12 | 192.168.1.155 | TCP | 1514 | 80 → 59220 [ACK] Seq=1461 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU] |
| 39 | 14.411037 | 128.119.245.12 | 192.168.1.155 | TCP | 1514 | 80 → 59220 [ACK] Seq=2921 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU] |
| 40 | 14.411037 | 128.119.245.12 | 192.168.1.155 | HTTP | 535 | HTTP/1.1 200 OK (text/html) |

> Frame 40: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
> Transmission Control Protocol, Src Port: 80, Dst Port: 59220, Seq: 4381, Ack: 390, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #37(1460), #38(1460), #39(1460), #40(481)]
v Hypertext Transfer Protocol
v HTTP/1.1 200 OK\r\n

Q15- As we can see in the image below , there are 4 TCP response, the size of 3 of them is 1460 bytes and the last one is 471 bytes.

0

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--------------------------------------------------------|
| 32 | 14.214830 | 192.168.1.155 | 128.119.245.12 | HTTP | 443 | GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| 40 | 14.411037 | 128.119.245.12 | 192.168.1.155 | HTTP | 535 | HTTP/1.1 200 OK (text/html) |
| 50 | 14.477161 | 192.168.1.155 | 128.119.245.12 | HTTP | 400 | GET /favicon.ico HTTP/1.1 |
| 56 | 14.686122 | 128.119.245.12 | 192.168.1.155 | HTTP | 539 | HTTP/1.1 404 Not Found (text/html) |

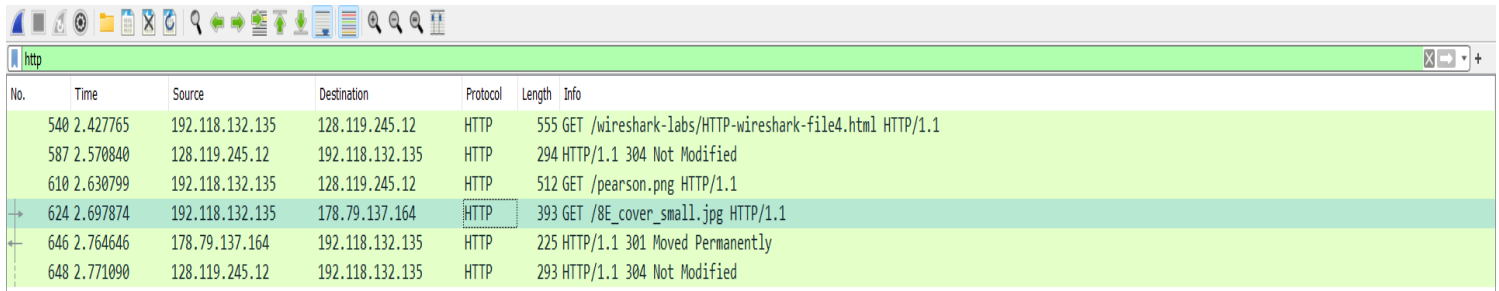
| |
|-------------------------------------------------------------------------------------------------------------------------------------------------|
| > Frame 40: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0 |
| > Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d) |
| > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155 |
| > Transmission Control Protocol, Src Port: 80, Dst Port: 59220, Seq: 4381, Ack: 390, Len: 481 |
| > [4 Reassembled TCP Segments (4861 bytes): #37(1460), #38(1460), #39(1460), #40(481)] |
| [Frame: 37, payload: 0-1459 (1460 bytes)] |
| [Frame: 38, payload: 1460-2919 (1460 bytes)] |
| [Frame: 39, payload: 2920-4379 (1460 bytes)] |
| [Frame: 40, payload: 4380-4860 (481 bytes)] |
| [Segment count: 4] |
| [Reassembled TCP Length: 4861] |
| [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c203037204e6f762032...] |
| > Hypertext Transfer Protocol |
| > Line-based text data: text/html (98 lines) |

Q16- As you can see in the image below, there are 3 GET requests messages.

**Two of them sent to IP 128.119.245.12 (gaia's website),
the other one sent to IP 178.79.137.164 (the cover book's website).**

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------------|-----------------|----------|--------|--------------------------------------------------------|
| 540 | 2.427765 | 192.118.132.135 | 128.119.245.12 | HTTP | 555 | GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 587 | 2.570840 | 128.119.245.12 | 192.118.132.135 | HTTP | 294 | HTTP/1.1 304 Not Modified |
| 610 | 2.630799 | 192.118.132.135 | 128.119.245.12 | HTTP | 512 | GET /pearson.png HTTP/1.1 |
| 624 | 2.697874 | 192.118.132.135 | 178.79.137.164 | HTTP | 393 | GET /8E_cover_small.jpg HTTP/1.1 |
| 646 | 2.764646 | 178.79.137.164 | 192.118.132.135 | HTTP | 225 | HTTP/1.1 301 Moved Permanently |
| 648 | 2.771090 | 128.119.245.12 | 192.118.132.135 | HTTP | 293 | HTTP/1.1 304 Not Modified |

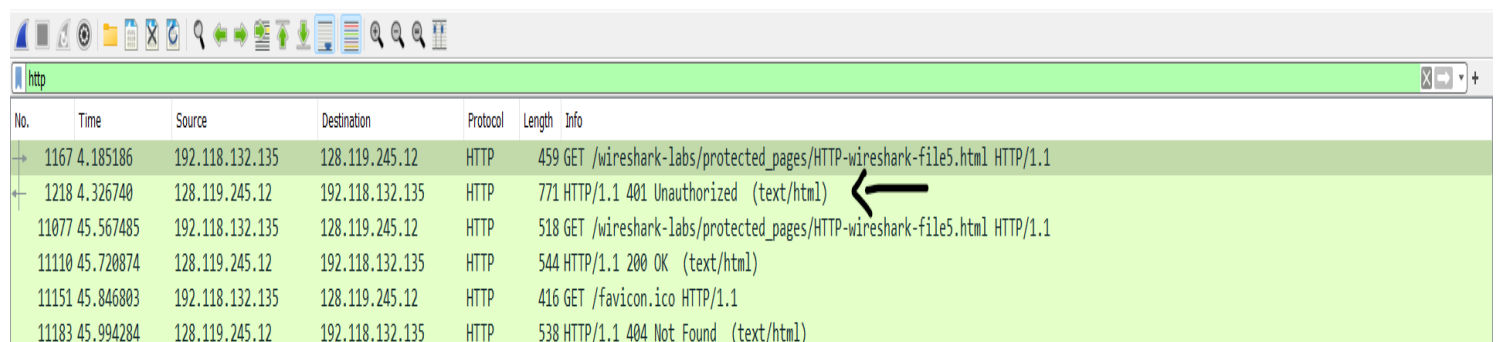
Q17- As we can see in the image below, every GET requests for each of the images is standing independently and serially, and as we can see, every GET request is closed and have different TCP connections.



The image shows a Wireshark packet capture of HTTP traffic. The packet list pane displays several GET requests. The selected packet (No. 624) is a GET request for /8E_cover_small.jpg, which is highlighted in green. The packet details pane shows the HTTP request structure.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------------|-----------------|----------|--------|--------------------------------------------------------|
| 540 | 2.427765 | 192.118.132.135 | 128.119.245.12 | HTTP | 555 | GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 587 | 2.570840 | 128.119.245.12 | 192.118.132.135 | HTTP | 294 | HTTP/1.1 304 Not Modified |
| 610 | 2.630799 | 192.118.132.135 | 128.119.245.12 | HTTP | 512 | GET /pearson.png HTTP/1.1 |
| 624 | 2.697874 | 192.118.132.135 | 178.79.137.164 | HTTP | 393 | GET /8E_cover_small.jpg HTTP/1.1 |
| 646 | 2.764646 | 178.79.137.164 | 192.118.132.135 | HTTP | 225 | HTTP/1.1 301 Moved Permanently |
| 648 | 2.771090 | 128.119.245.12 | 192.118.132.135 | HTTP | 293 | HTTP/1.1 304 Not Modified |

Q18- As we can see in the image below, the status code is 401. And the phrase is "Unauthorized".



The image shows a Wireshark packet capture of HTTP traffic. The packet list pane displays several HTTP requests and responses. The selected packet (No. 1218) is an HTTP 401 Unauthorized response, which is highlighted in green. A black arrow points to the status code '401' in the 'Info' column. The packet details pane shows the HTTP response structure.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|-----------|-----------------|-----------------|----------|--------|------------------------------------------------------------------------|
| 1167 | 4.185186 | 192.118.132.135 | 128.119.245.12 | HTTP | 459 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 1218 | 4.326740 | 128.119.245.12 | 192.118.132.135 | HTTP | 771 | HTTP/1.1 401 Unauthorized (text/html) |
| 11077 | 45.567485 | 192.118.132.135 | 128.119.245.12 | HTTP | 518 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 11110 | 45.720874 | 128.119.245.12 | 192.118.132.135 | HTTP | 544 | HTTP/1.1 200 OK (text/html) |
| 11151 | 45.846803 | 192.118.132.135 | 128.119.245.12 | HTTP | 416 | GET /favicon.ico HTTP/1.1 |
| 11183 | 45.994284 | 128.119.245.12 | 192.118.132.135 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

Q19- As you can see in the image below, the new field which added is the "Authorization" field

| | | | | | | | | |
|---|-------|-----------|-----------------|-----------------|------|-----|------------------------------------------------------------------------|---|
| → | 11077 | 45.567485 | 192.118.132.135 | 128.119.245.12 | HTTP | 518 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 | ← |
| ← | 11110 | 45.720874 | 128.119.245.12 | 192.118.132.135 | HTTP | 544 | HTTP/1.1 200 OK (text/html) | |
| → | 11151 | 45.846803 | 192.118.132.135 | 128.119.245.12 | HTTP | 416 | GET /favicon.ico HTTP/1.1 | |
| | 11183 | 45.994284 | 128.119.245.12 | 192.118.132.135 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) | |

> Frame 11077: 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
 > Ethernet II, Src: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d), Dst: PaloAlto_35:ea:30 (84:d4:12:35:ea:30)
 > Internet Protocol Version 4, Src: 192.118.132.135, Dst: 128.119.245.12
 > Transmission Control Protocol, Src Port: 59806, Dst Port: 80, Seq: 1, Ack: 1, Len: 464
 > Hypertext Transfer Protocol
 > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
 Host: gaia.cs.umass.edu\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\r\n
 Upgrade-Insecure-Requests: 1\r\n
 < Authorization: Basic d2lyZXNoYXJrLXN0dWRLbnRzOm5ldHdvcm0=\r\n
 Credentials: wireshark-students:network\r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
 [HTTP request 1/2]
 [Response in frame: 11110]
 [Next request in frame: 11151]