

*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephoneie Wireless Outils Aide

http

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------|----------------|----------------|----------|--------|--|
| 60 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8fb7aa12ebcbc3... |
| 62 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X.. | 1186 | HTTP/1.1 200 OK |
| 76 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8fb7aa12ebcbc3... |
| 78 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X.. | 1186 | HTTP/1.1 200 OK |
| 94 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8fb7aa12ebcbc3... |
| 96 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X.. | 1186 | HTTP/1.1 200 OK |
| 212 | 0.000 | 192.168.1.10 | 128.119.245.12 | HTTP | 559 | GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 |
| 223 | 0.001 | 128.119.245.12 | 192.168.1.10 | HTTP | 540 | HTTP/1.1 200 OK (text/html) |
| 290 | 0.000 | 192.168.1.10 | 213.57.24.139 | HTTP | 178 | GET /ncsi.txt HTTP/1.1 |
| 292 | 0.000 | 213.57.24.139 | 192.168.1.10 | HTTP | 233 | HTTP/1.1 200 OK (text/plain) |

▼ Hypertext Transfer Protocol

 ▼ HTTP/1.1 200 OK\r\n

 ▼ [Expert Info (Chat/Sequence): **HTTP/1.1 200 OK\r\n**]

- [HTTP/1.1 200 OK\r\n]
- [Severity level: Chat]
- [Group: Sequence]

 Response Version: HTTP/1.1

 Status Code: 200

 [Status Code Description: OK]

 Response Phrase: OK

 Date: Thu, 12 Nov 2020 07:27:04 GMT\r\n

 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n

 Last-Modified: Thu, 12 Nov 2020 06:59:02 GMT\r\n

 ETag: "80-5b3e3726eb73"\r\n

 Accept-Ranges: bytes\r\n

 ▼ Content-Length: 128\r\n

 [Content length: 128]

| | | | |
|------|-------------------------|-------------------------|-------------------|
| 00c0 | 2e 31 36 2e 33 0d 0a 4c | 61 73 74 2d 4d 6f 64 69 | .16.3. L ast-Modi |
| 00d0 | 66 69 65 64 3a 20 54 68 | 75 2c 20 31 32 20 4e 6f | fied: Th u, 12 No |

HTTP Last Modified (http.last_modified), 46 byte(s)

Paquets: 332 · Affichés: 12 (3.6%) · Perdus: 0 (0.0%)

Profile: Default

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Answer: HTTP 1.1

The screenshot shows the Wireshark interface with the following details:

- Network Interface:** *Ethernet
- File Menu:** Fichier, Editer, Vue, Aller, Capture, Analyser, Statistiques, Téléphonie, Wireless, Outils, Aide
- Toolbar:** Includes icons for File, Edit, View, Capture, Analyse, Statistics, Telephone, Wireless, Tools, Help, and various search and selection tools.
- Selected Filter:** http
- List View (Table):** Shows a list of network packets with columns: No., Time, Source, Destination, Protocol, Length, and Info. The list includes several GET requests to 'http://192.168.1.10' and one to 'http://128.119.245.12'. The last packet selected is a GET request to 'http://wireshark-labs/HTTP-wireshark-file1.html' from port 128.119.245.12.
- Details View (Protocol Tree):** Expanded for the selected packet (index 212). It shows the Hypertext Transfer Protocol (HTTP) tree with the following details:
 - Request Line: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 - Headers:
 - Host: gaia.cs.umass.edu\r\n
 - Connection: keep-alive\r\n
 - DNT: 1\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/86.0.4240.193 Safari/537.36\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=0.9\r...
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
- Hex View:** Shows the raw hex dump of the selected packet, starting with 0030 and ending at 0070.
- Text View:** Shows the ASCII representation of the selected packet, identifying it as a Text item (text) with 56 byte(s).
- Bottom Status Bar:** Paquets: 332 · Affichés: 12 (3.6%) · Perdus: 0 (0.0%) · Profile: Default

2. What languages (if any) does your browser indicate that it can accept to the server?

Answer: fr-FR (FR French) and en-US (US English)

*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

http

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------|----------------|----------------|-----------|--------|--|
| 49 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8fb-7aa12ebcbc3b HTTP/... |
| 51 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X... | 1186 | HTTP/1.1 200 OK |
| 60 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8fb-7aa12ebcbc3b HTTP/... |
| 62 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X... | 1186 | HTTP/1.1 200 OK |
| 76 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8fb-7aa12ebcbc3b HTTP/... |
| 78 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X... | 1186 | HTTP/1.1 200 OK |
| 94 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8fb-7aa12ebcbc3b HTTP/... |
| 96 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X... | 1186 | HTTP/1.1 200 OK |
| 212 | 0.000 | 192.168.1.10 | 128.119.245.12 | HTTP | 559 | GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 |
| 223 | 0.001 | 128.119.245.12 | 192.168.1.10 | HTTP | 540 | HTTP/1.1 200 OK (text/html) |
| 290 | 0.000 | 192.168.1.10 | 213.57.24.139 | HTTP | 178 | GET /ncsi.txt HTTP/1.1 |
| 292 | 0.000 | 213.57.24.139 | 192.168.1.10 | HTTP | 233 | HTTP/1.1 200 OK (text/plain) |

```

> Frame 212: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-15334397F8C}, id 0
> Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55789, Dst Port: 80, Seq: 1, Ack: 1, Len: 505
< Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    DNT: 1\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/86.0.4240.193 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r...
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  \r\n
0030 04 02 44 9f 00 00 47 45 54 20 2f 77 69 72 65 73  --D--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

```

Text item (text), 56 byte(s) || Paquets: 332 · Affichés: 12 (3.6%) · Perdus: 0 (0.0%) || Profile: Default

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Answer: -My IP is 192.168.1.10 and gaia.cs.umass.edu server's IP is 128.119.245.12

*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephone Wireless Outils Aide

http

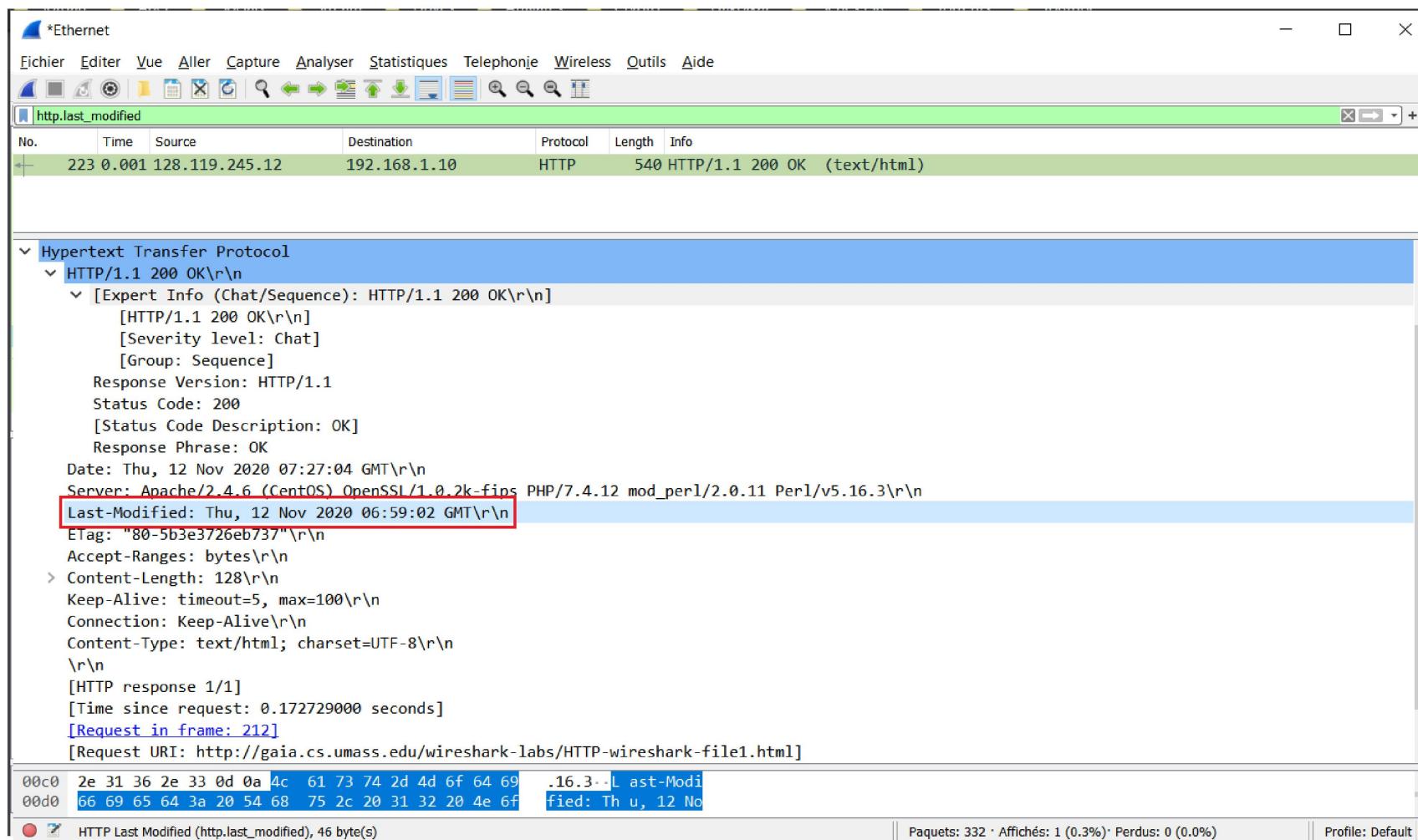
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------|----------------|----------------|-----------|--------|---|
| 49 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8bfb-7aa12ebcbc3b HTTP/... |
| 51 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X... | 1186 | HTTP/1.1 200 OK |
| 60 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8bfb-7aa12ebcbc3b HTTP/... |
| 62 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X... | 1186 | HTTP/1.1 200 OK |
| 76 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8bfb-7aa12ebcbc3b HTTP/... |
| 78 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X... | 1186 | HTTP/1.1 200 OK |
| 94 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8bfb-7aa12ebcbc3b HTTP/... |
| 96 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X... | 1186 | HTTP/1.1 200 OK |
| 212 | 0.000 | 192.168.1.10 | 128.119.245.12 | HTTP | 559 | GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 |
| 223 | 0.001 | 128.119.245.12 | 192.168.1.10 | HTTP | 540 | HTTP/1.1 200 OK (text/html) |
| 290 | 0.000 | 192.168.1.10 | 213.57.24.139 | HTTP | 178 | GET /ncsi.txt HTTP/1.1 |
| 292 | 0.000 | 213.57.24.139 | 192.168.1.10 | HTTP | 233 | HTTP/1.1 200 OK (text/plain) |

```
> Frame 212: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-153334397F8C}, id 0
> Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55789, Dst Port: 80, Seq: 1, Ack: 1, Len: 505
Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  DNT: 1\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/86.0.4240.193 Safari/537.36\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=0.9\r...
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
\r\n
0030  04 02 44 9f 00 00 47 45 54 20 2f 77 69 72 65 73  - - D - - 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
```

Text item (text), 56 byte(s) || Paquets: 332 · Affichés: 12 (3.6%) · Perdus: 0 (0.0%) || Profile: Default

4. What is the status code returned from the server to your browser?

Answer: 200 OK



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

Answer : Using "http.last_modified" filter we can see that the last modified was on Thu, 12 Nov 2020 at 06:59:02 GMT

*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephone Wireless Outils Aide

http

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------|----------------|----------------|-----------|--------|---|
| 60 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8fb-7aa12ebcbc3... |
| 62 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X... | 1186 | HTTP/1.1 200 OK |
| 76 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8fb-7aa12ebcbc3... |
| 78 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X... | 1186 | HTTP/1.1 200 OK |
| 94 | 0.000 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8fb-7aa12ebcbc3... |
| 96 | 0.000 | 192.168.1.10 | 192.168.1.1 | HTTP/X... | 1186 | HTTP/1.1 200 OK |
| 212 | 0.000 | 192.168.1.10 | 128.119.245.12 | HTTP | 559 | GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 |
| 223 | 0.001 | 128.119.245.12 | 192.168.1.10 | HTTP | 540 | HTTP/1.1 200 OK (text/html) |
| 290 | 0.000 | 192.168.1.10 | 213.57.24.139 | HTTP | 178 | GET /ncsi.txt HTTP/1.1 |
| 292 | 0.000 | 213.57.24.139 | 192.168.1.10 | HTTP | 233 | HTTP/1.1 200 OK (text/plain) |

[HTTP/1.1 200 OK\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Thu, 12 Nov 2020 07:27:04 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Thu, 12 Nov 2020 06:59:02 GMT\r\nETag: "80-5b3e3726eb737"\r\nAccept-Ranges: bytes\r\nContent-Length: 128\r\n[Content length: 128]
Keep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n

00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..L ast-Modi
00d0 66 69 65 64 3a 20 54 68 75 2c 20 31 32 20 4e 6f fied: Th u, 12 No

HTTP Last Modified (http.last_modified), 46 byte(s)

Paquets: 332 · Affichés: 12 (3.6%) · Perdus: 0 (0.0%)

Profile: Default

6. How many bytes of content are being returned to your browser?

Answer: 128 bytes

Ethernet :

| | | |
|------|---|--------------------|
| 0000 | 8c 16 45 e0 0d 35 30 24 78 c0 4d 74 08 00 45 00 | ..E..50\$ x.Mt..E. |
| 0010 | 02 0e 72 58 40 00 2b 06 a4 5b 80 77 f5 0c c0 a8 | ..rX@+..[w.... |
| 0020 | 01 0a 00 50 d9 ed a9 9c 8f ed 62 4e dd 79 50 18 | ..P.....bn.yP. |
| 0030 | 00 ed 4a 75 00 00 48 54 54 50 2f 31 2e 31 20 32 | ..Ju..HT TP/1.1 2 |
| 0040 | 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 | 00 OK..D ate: Thu |

Internet:

| | | |
|------|--|--------------------|
| 0000 | 8c 16 45 e0 0d 35 30 24 78 c0 4d 74 08 00 45 00 | ..E..50\$ x.Mt..E. |
| 0010 | 02 0e 72 58 40 00 2b 06 a4 5b 80 77 f5 0c c0 a8 | ..rX@+..[w.... |
| 0020 | 01 0a 00 50 d9 ed a9 9c 8f ed 62 4e dd 79 50 18 | ..P.....bn.yP. |
| 0030 | 00 ed 4a 75 00 00 48 54 54 50 2f 31 2e 31 20 32 | ..Ju..HT TP/1.1 2 |
| 0040 | 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 | 00 OK..D ate: Thu |
| 0050 | 2e 22 31 22 22 22 1e ff 7e 2e 22 22 22 22 22 22 22 | 12 Nov 2020 07 |

Transmission:

| | | |
|------|--|-------------------|
| 0020 | 01 0a 00 50 d9 ed a9 9c 8f ed 62 4e dd 79 50 18 | ..P.....bn.yP. |
| 0030 | 00 ed 4a 75 00 00 48 54 54 50 2f 31 2e 31 20 32 | ..Ju..HT TP/1.1 2 |
| 0040 | 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 | 00 OK..D ate: Thu |
| 0050 | 2c 20 31 32 20 4e 6f 76 20 32 30 32 30 20 30 37 | , 12 Nov 2020 07 |
| 0060 | 2e 22 22 22 22 22 22 1e ff 7e 2e 22 22 22 22 22 22 | 27.04.6 MT...Serv |

Application:

```

0150 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63
0160 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65
0170 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20
0180 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73
0190 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d
01a0 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f
01b0 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e
01c0 6c 6f 61 64 65 64 20 74 68 65 20 66 69 6c 65 20
01d0 0a 68 74 74 70 3a 2f 67 61 69 61 2e 63 73 2e
01e0 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68
01f0 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69
0200 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74
0210 6d 6c 21 0a 3c 2f 68 74 6d 6c 3e 0a

```

HTTP:

```

0000 8c 16 45 e0 0d 35 30 24 78 c0 4d 74 08 00 45 00 ..E..50$ x.Mt..E.
0010 02 0e 72 58 40 00 2b 06 a4 5b 80 77 f5 0c c0 a8 ..rX@+..[w....
0020 01 0a 00 50 d9 ed a9 9c 8f ed 62 4e dd 79 50 18 ..P.....bn.yP.
0030 00 ed 4a 75 00 00 48 54 54 50 2f 31 2e 31 20 32 ..Ju..HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 00 OK..D ate: Thu
0050 2e 22 22 22 22 22 22 1e ff 7e 2e 22 22 22 22 22 22 , 12 Nov 2020 07
0060 3a 32 37 3a 30 34 20 47 4d 54 0d 0a 53 65 72 76 :27.04 G MT...Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 0d 66 69 70 73 20 50 48
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 0d 6d 6f 64 5f 70 65 72
0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 0d 6f 64 5f 70 65 72
00a0 50 2f 37 2e 34 2e 31 32 20 6d 6f 64 5f 70 65 72 0d 6f 64 5f 70 65 72
00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 0d 6f 64 5f 70 65 72
00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 0d 6f 64 5f 70 65 72
00d0 66 69 65 64 3a 20 54 68 75 2c 20 31 32 20 4e 6f 0d 6f 64 5f 70 65 72
00e0 76 20 32 30 32 30 20 30 36 3a 35 39 3a 30 32 20 0d 6f 64 5f 70 65 72
00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 35 0d 6f 64 5f 70 65 72
0100 62 33 65 33 37 32 36 65 62 37 33 37 22 0d 0a 41 0d 6f 64 5f 70 65 72
0110 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 0d 6f 64 5f 70 65 72
0120 74 65 73 0d 0a 43 6f 6e 74 65 74 2d 4c 65 6e 0d 6f 64 5f 70 65 72
0130 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 0d 6f 64 5f 70 65 72
0140 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 0d 6f 64 5f 70 65 72
0150 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 0d 6f 64 5f 70 65 72
0160 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 6f 64 5f 70 65 72
0170 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 0d 6f 64 5f 70 65 72
0180 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 0d 6f 64 5f 70 65 72
0190 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 0d 6f 64 5f 70 65 72
01a0 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f 0d 6f 64 5f 70 65 72
01b0 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e 0d 6f 64 5f 70 65 72
01c0 6c 6f 61 64 65 64 20 74 68 65 20 66 69 6c 65 20 0d 6f 64 5f 70 65 72
01d0 0a 68 74 74 70 3a 2f 67 61 69 61 2e 63 73 2e 0d 6f 64 5f 70 65 72
01e0 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68 0d 6f 64 5f 70 65 72
01f0 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 0d 6f 64 5f 70 65 72
0200 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 0d 6f 64 5f 70 65 72
0210 6d 6c 21 0a 3c 2f 68 74 6d 6c 3e 0a

```

max=100 ..Connection: Keep-Alive
..Content-Type: text/html; charset=UTF-8
l>Congratulations. You've downloaded the file
http://galaxy.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
m!..</html>

7. By inspecting the raw data in the packet content window, do you see any headers

within the data that are not displayed in the packet-listing window? If so, name one.

Answer: No, everything appears on the packet-listing window (everything is covered)

8. 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?

Answer: No

The screenshot shows a Wireshark interface with the following details:

- Network Interface:** *Ethernet
- File Menu:** Fichier, Editer, Vue, Aller, Capture, Analyser, Statistiques, Téléphonie, Wireless, Outils, Aide
- Selected Protocol:** http
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info
- Table Data:** Shows 10 rows of network traffic, mostly HTTP requests from 192.168.1.10 to 128.119.245.12. Row 80 shows a GET request for /wireshark-labs/HTTP-wireshark-file2.html.
- Protocol Details:** A expanded section for the selected row (HTTP) shows:
 - Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.10
 - Transmission Control Protocol, Src Port: 80, Dst Port: 56402, Seq: 1, Ack: 506, Len: 730
 - Hypertext Transfer Protocol
- Line-based text data:** A expanded section for the selected row (text/html) shows the content of the file lab2-2.html, which includes text about file modification and browser behavior.
- Hex View:** Shows the raw hex and ASCII data for the selected packet.
- Bottom Status Bar:** Paquets: 431 · Affichés: 8 (1.9%) · Perdus: 0 (0.0%) · Profile: Default

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer: Yes it did. We can tell by reading the file on the Line-based text data protocol

*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

http

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------|----------------|----------------|----------|--------|--|
| 80 | 0.000 | 192.168.1.10 | 128.119.245.12 | HTTP | 559 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 112 | 0.003 | 128.119.245.12 | 192.168.1.10 | HTTP | 784 | HTTP/1.1 200 OK (text/html) |
| 126 | 0.014 | 192.168.1.10 | 128.119.245.12 | HTTP | 491 | GET /favicon.ico HTTP/1.1 |
| 131 | 0.011 | 128.119.245.12 | 192.168.1.10 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |
| 182 | 0.000 | 192.168.1.10 | 213.57.24.194 | HTTP | 178 | GET /ncsi.txt HTTP/1.1 |
| 184 | 0.000 | 213.57.24.194 | 192.168.1.10 | HTTP | 233 | HTTP/1.1 200 OK (text/plain) |
| 189 | 0.096 | 192.168.1.10 | 128.119.245.12 | HTTP | 671 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 190 | 0.164 | 128.119.245.12 | 192.168.1.10 | HTTP | 293 | HTTP/1.1 304 Not Modified |

```
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
DNT: 1\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/86.0.4240.193 Safari/537.36\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=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
If-None-Match: "173-5b3e3726ab7f"\r\n
If-Modified-Since: Thu, 12 Nov 2020 06:59:02 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
0000 30 24 78 c0 4d 74 8c 16 45 e0 0d 35 08 00 45 00 0$xE-Mt..E..5..E..
0010 02 91 f2 40 40 00 80 06 ce ef c0 a8 01 0a 80 77 ...@@... .....w
0020 f5 0c dc 52 00 50 38 18 bf 41 f6 5d 59 2b 50 18 ...R.PB..A.]Y+P..
```

Expert Info (_ws.expert) || Paquets: 431 · Affichés: 8 (1.9%) · Perdus: 0 (0.0%) || Profile: Default

10. 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?

Answer: Yes. It says: IF-MODIFIED-SINCE: Thu, 12 Nov 2020 06:59:02 GMT

The screenshot shows the Wireshark interface with the following details:

- Network Interface:** *Ethernet
- File Menu:** Fichier, Editer, Vue, Aller, Capture, Analyser, Statistiques, Téléphonie, Sans fil, Outils, Aide
- Toolbar:** Various icons for file operations, search, and analysis.
- Selected Filter:** http
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info
- Table Data:**

| | | | | | |
|-----------|----------------|----------------|------|-----|--|
| 89 0.000 | 192.168.1.10 | 128.119.245.12 | HTTP | 559 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 112 0.003 | 128.119.245.12 | 192.168.1.10 | HTTP | 784 | HTTP/1.1 200 OK (text/html) |
| 126 0.014 | 192.168.1.10 | 128.119.245.12 | HTTP | 491 | GET /favicon.ico HTTP/1.1 |
| 131 0.011 | 128.119.245.12 | 192.168.1.10 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |
| 182 0.000 | 192.168.1.10 | 213.57.24.194 | HTTP | 178 | GET /ncsi.txt HTTP/1.1 |
| 184 0.000 | 213.57.24.194 | 192.168.1.10 | HTTP | 233 | HTTP/1.1 200 OK (text/plain) |
| 189 0.096 | 192.168.1.10 | 128.119.245.12 | HTTP | 671 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 190 0.164 | 128.119.245.12 | 192.168.1.10 | HTTP | 293 | HTTP/1.1 304 Not Modified |
- Selected Row:** The last row (No. 190) is highlighted with a red border.
- Details View:**

```
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
DNT: 1\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/86.0.4240.193 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
If None Match: "e173_5b3e3726cab7f"\r\n
If-Modified-Since: Thu, 12 Nov 2020 06:59:02 GMT\r\n
\r\n
[Full request URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```
- Hex View:**

| | | |
|------|---|--------------------|
| 0000 | 30 24 78 c0 4d 74 8c 16 45 e0 0d 35 08 00 45 00 | 05x-Mt... E..S..E. |
| 0010 | 02 91 f2 40 40 00 80 06 ce ef c0 a8 01 0a 80 77 |@.....w |
| 0020 | f5 0c dc 52 00 50 38 18 bf 41 f6 5d 59 2b 50 18 | ..R-PB..A.]Y+P.. |
- Statistics:** Paquets: 431 - Affichés: 8 (1.9%) - Perdus: 0 (0.0%)
- Profile:** Default

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Answer: The response from the server is HTTP/1.1 304 Not Modified Response.

The server didn't explicitly return the contents of the file since it already was stored in cache. It means our web browser (Chrome) performed an object caching and thus performed a conditional GET, which resulted in finding the object already stored in cache.

The screenshot shows a Wireshark capture of an HTTP session. The packet list pane displays four entries:

- Packet 36: GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
- Packet 90: HTTP/1.1 200 OK (text/html)
- Packet 115: GET /favicon.ico HTTP/1.1
- Packet 118: HTTP/1.1 404 Not Found (text/html)

The details pane shows the expanded HTTP response for packet 90, which includes the following headers:

```

> Frame 90: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-153334397F8C}, id 0
> Ethernet II, Src: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74), Dst: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 54450, Seq: 4381, Ack: 506, Len: 481
  [4 Reassembled TCP Segments (4861 bytes): #86(1460), #87(1460), #88(1460), #90(481)]
    [Frame: 86, payload: 0-1459 (1460 bytes)]
    [Frame: 87, payload: 1460-2919 (1460 bytes)]
    [Frame: 88, payload: 2920-4379 (1460 bytes)]
    [Frame: 90, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205361742c203134204e6f762032...]
  Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      Date: Sat, 14 Nov 2020 21:54:40 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Sat, 14 Nov 2020 06:59:02 GMT\r\n
      ETag: "1194-5b40bae1a0877"\r\n
      Accept-Ranges: bytes\r\n
    > Content-Length: 4500\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=UTF-8\r\n
      \r\n
      [HTTP response 1/2]

```

The bytes pane at the bottom shows the raw hex and ASCII data for the selected frame.

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Answer: Ignoring the favicon the browser sent only one request. The packet containing the GET message for the Bill or Rights is packet 36

The screenshot shows a Wireshark capture window titled '*Ethernet'. The menu bar includes 'Fichier', 'Editer', 'Vue', 'Aller', 'Capture', 'Analyser', 'Statistiques', 'Téléphonie', 'Wireless', 'Outils', and 'Aide'. The toolbar contains icons for file operations, capture, analysis, and statistics. A green bar at the top indicates the current filter is 'http'. The main pane displays a list of network packets. The second packet from the top (highlighted with a red box) is selected, showing details: No. 90, Time 0.000, Source 128.119.245.12, Destination 192.168.1.10, Protocol HTTP, Length 535, Info: HTTP/1.1 200 OK (text/html). The packet list also includes: 36 0.000 192.168.1.10 128.119.245.12 HTTP 559 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1; 115 0.003 192.168.1.10 128.119.245.12 HTTP 491 GET /favicon.ico HTTP/1.1; 118 0.006 128.119.245.12 192.168.1.10 HTTP 538 HTTP/1.1 404 Not Found (text/html). Below the packet list, the 'Http' analysis pane shows: [4 Reassembled TCP Segments (4861 bytes): #86(1460), #87(1460), #88(1460), #90(481)], Hypertext Transfer Protocol, Line-based text data: text/html (98 lines). The response body for packet 90 is displayed, starting with the title 'THE BILL OF RIGHTS' and containing several paragraphs of text. A large red box highlights the entire response body. At the bottom, the hex and ASCII panes show the raw data for the selected frame.

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer: Packet 90

14. What is the status code and phrase in the response?

Answer: HTTP/1.1 200 OK (text/html)

*Ethernet

Eichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

http

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------|----------------|----------------|----------|--------|--|
| 36 | 0.000 | 192.168.1.10 | 128.119.245.12 | HTTP | 559 | GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| 90 | 0.000 | 128.119.245.12 | 192.168.1.10 | HTTP | 535 | HTTP/1.1 200 OK (text/html) |
| 115 | 0.003 | 192.168.1.10 | 128.119.245.12 | HTTP | 491 | GET /favicon.ico HTTP/1.1 |
| 118 | 0.006 | 128.119.245.12 | 192.168.1.10 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

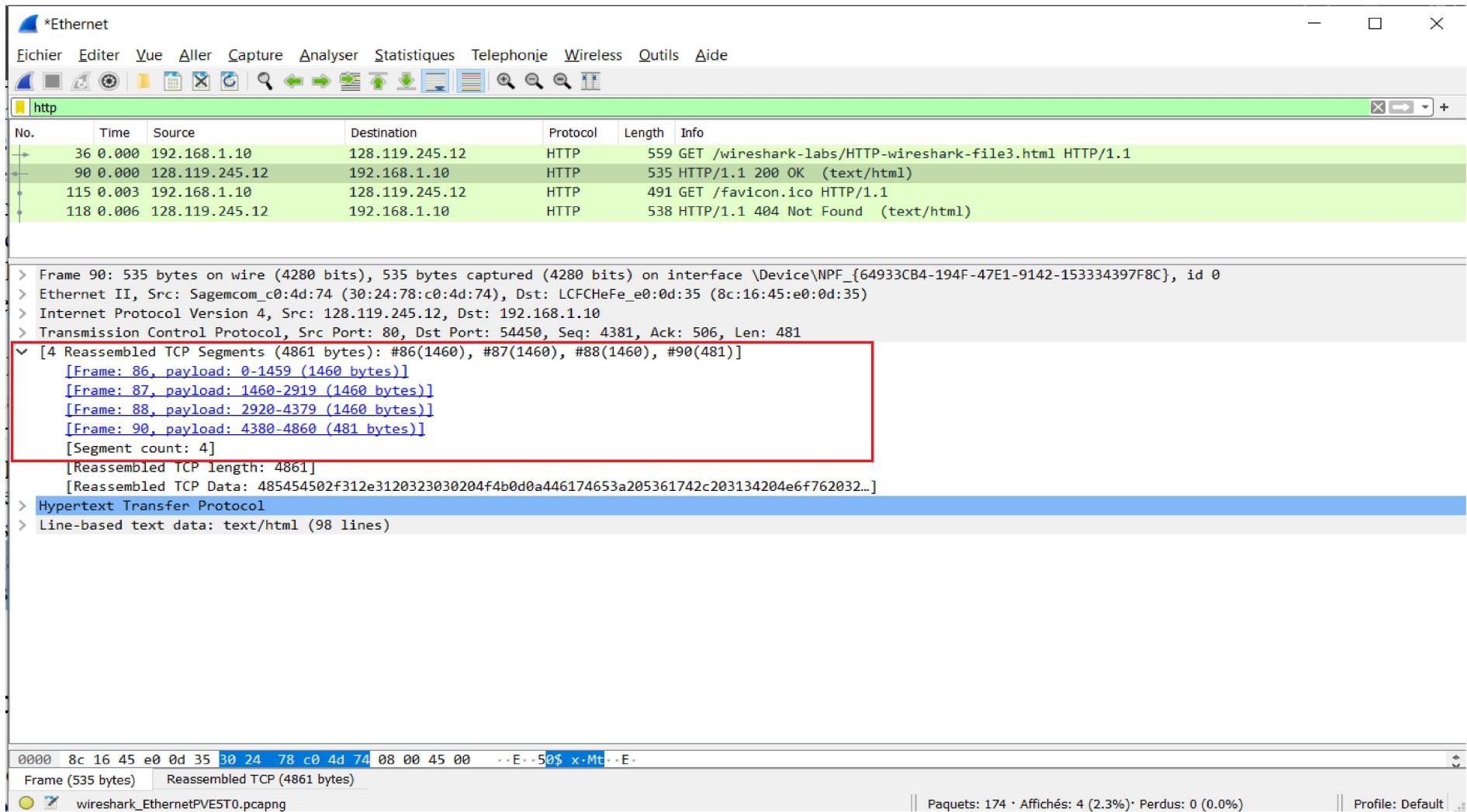
> Frame 90: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-153334397F8C}, id 0
> Ethernet II, Src: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74), Dst: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 54450, Seq: 4381, Ack: 506, Len: 481

↳ [4 Reassembled TCP Segments (4861 bytes): #86(1460), #87(1460), #88(1460), #90(481)]
[Frame: 86, payload: 0-1459 (1460 bytes)]
[Frame: 87, payload: 1460-2919 (1460 bytes)]
[Frame: 88, payload: 2920-4379 (1460 bytes)]
[Frame: 90, payload: 4380-4860 (481 bytes)]
[Segment count: 4]
[Reassembled TCP length: 4861]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205361742c203134204e6f762032...]

↳ Hypertext Transfer Protocol
↳ Line-based text data: text/html (98 lines)

0000 8c 16 45 e0 0d 35 30 24 78 c0 4d 74 08 00 45 00 ..E..50\$ x-Mt..E.
Frame (535 bytes) Reassembled TCP (4861 bytes)

Paquets: 174 · Affichés: 4 (2.3%) · Perdus: 0 (0.0%) Profile: Default



15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Answer: 4 segments

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------|----------------|----------------|----------|--------|--|
| 38 | 0.000 | 192.168.1.10 | 128.119.245.12 | HTTP | 559 | GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 74 | 0.000 | 128.119.245.12 | 192.168.1.10 | HTTP | 1127 | HTTP/1.1 200 OK (text/html) |
| 86 | 0.097 | 192.168.1.10 | 128.119.245.12 | HTTP | 491 | GET /pearson.png HTTP/1.1 |
| 90 | 0.000 | 192.168.1.10 | 128.119.245.12 | HTTP | 465 | GET /~kurose/cover_5th_ed.jpg HTTP/1.1 |
| 93 | 0.000 | 128.119.245.12 | 192.168.1.10 | HTTP | 745 | HTTP/1.1 200 OK (PNG) |
| 186 | 0.000 | 128.119.245.12 | 192.168.1.10 | HTTP | 632 | HTTP/1.1 200 OK (JPEG JFIF image) |
| 188 | 0.006 | 192.168.1.10 | 128.119.245.12 | HTTP | 491 | GET /favicon.ico HTTP/1.1 |
| 191 | 0.014 | 128.119.245.12 | 192.168.1.10 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

```
> Frame 38: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-153334397F8C}, id 0
> Ethernet II, Src: LCFChFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54874, Dst Port: 80, Seq: 1, Ack: 1, Len: 505
> Hypertext Transfer Protocol
```

Paquets: 214 · Affichés: 8 (3.7%) | Profile: Default

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Answer: Ignoring the favicon, the browser sent 3 HTTP GET requests (in red)
Internet addresses are in blue.

| http | | | | | | |
|-------------|----------|----------------|----------------------------------|---------------------------|-----------|--|
| Titre: Time | | | Type: Time (format as specified) | Fields: Enter a field ... | événement | OK Annuler |
| No. | Time | Source | Destination | Protocol | Length | Info |
| 38 | 0.000535 | 192.168.1.10 | 128.119.245.12 | HTTP | 559 | GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 74 | 0.000771 | 128.119.245.12 | 192.168.1.10 | HTTP | 1127 | HTTP/1.1 200 OK (text/html) |
| 86 | 0.097043 | 192.168.1.10 | 128.119.245.12 | HTTP | 491 | GET /pearson.png HTTP/1.1 |
| 90 | 0.000459 | 192.168.1.10 | 128.119.245.12 | HTTP | 465 | GET /~kurose/cover_5th_ed.jpg HTTP/1.1 |
| 93 | 0.000000 | 128.119.245.12 | 192.168.1.10 | HTTP | 745 | HTTP/1.1 200 OK (PNG) |
| 186 | 0.000000 | 128.119.245.12 | 192.168.1.10 | HTTP | 632 | HTTP/1.1 200 OK (JPEG JFIF image) |
| 188 | 0.006348 | 192.168.1.10 | 128.119.245.12 | HTTP | 491 | GET /favicon.ico HTTP/1.1 |
| 191 | 0.014683 | 128.119.245.12 | 192.168.1.10 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

> Frame 86: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-153334397F8C}, id 0
 > Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
 > Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.245.12
 > Transmission Control Protocol, Src Port: 54874, Dst Port: 80, Seq: 506, Ack: 1074, Len: 437
 > Hypertext Transfer Protocol

| http | | | | | | |
|-------------|----------|----------------|----------------------------------|---------------------------|-----------|--|
| Titre: Time | | | Type: Time (format as specified) | Fields: Enter a field ... | événement | OK Annuler |
| No. | Time | Source | Destination | Protocol | Length | Info |
| 38 | 0.000535 | 192.168.1.10 | 128.119.245.12 | HTTP | 559 | GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 74 | 0.000771 | 128.119.245.12 | 192.168.1.10 | HTTP | 1127 | HTTP/1.1 200 OK (text/html) |
| 86 | 0.097043 | 192.168.1.10 | 128.119.245.12 | HTTP | 491 | GET /pearson.png HTTP/1.1 |
| 90 | 0.000459 | 192.168.1.10 | 128.119.245.12 | HTTP | 465 | GET /~kurose/cover_5th_ed.jpg HTTP/1.1 |
| 93 | 0.000000 | 128.119.245.12 | 192.168.1.10 | HTTP | 745 | HTTP/1.1 200 OK (PNG) |
| 186 | 0.000000 | 128.119.245.12 | 192.168.1.10 | HTTP | 632 | HTTP/1.1 200 OK (JPEG JFIF image) |
| 188 | 0.006348 | 192.168.1.10 | 128.119.245.12 | HTTP | 491 | GET /favicon.ico HTTP/1.1 |
| 191 | 0.014683 | 128.119.245.12 | 192.168.1.10 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

> Frame 90: 465 bytes on wire (3720 bits), 465 bytes captured (3720 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-153334397F8C}, id 0
 > Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
 > Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.245.12
 > Transmission Control Protocol, Src Port: 54878, Dst Port: 80, Seq: 1, Ack: 1, Len: 411
 > Hypertext Transfer Protocol

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Answer: : By checking the TCP ports(54874 and 54878) we can see that the 2 images were transmitted over two different TCP connections. Therefore they were downloaded serially.

*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Téléphonie Wireless Outils Aide

http

Titre: Time Type: Time (format as specified) Fields: Enter a field ... événement

No. Time Source Destination Protocol Length Info

| | | | | | | |
|-----|----------|----------------|----------------|----------|------|--|
| 40 | 0.000549 | 192.168.1.10 | 128.119.245.12 | HTTP | 575 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 84 | 0.001729 | 128.119.245.12 | 192.168.1.10 | HTTP | 771 | HTTP/1.1 401 Unauthorized (text/html) |
| 138 | 0.000512 | 192.168.1.10 | 213.57.24.194 | HTTP | 178 | GET /ncsi.txt HTTP/1.1 |
| 143 | 0.000105 | 213.57.24.194 | 192.168.1.10 | HTTP | 233 | HTTP/1.1 200 OK (text/plain) |
| 534 | 0.000459 | 192.168.1.10 | 213.57.24.194 | HTTP | 178 | GET /ncsi.txt HTTP/1.1 |
| 536 | 0.000953 | 213.57.24.194 | 192.168.1.10 | HTTP | 233 | HTTP/1.1 200 OK (text/plain) |
| 551 | 0.000540 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8fb-7aa12ebcbc3b HTTP/1.1 |
| 553 | 0.000043 | 192.168.1.10 | 192.168.1.1 | HTTP/XML | 1186 | HTTP/1.1 200 OK |
| 562 | 0.003126 | 192.168.1.10 | 128.119.245.12 | HTTP | 660 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 567 | 0.001310 | 128.119.245.12 | 192.168.1.10 | HTTP | 544 | HTTP/1.1 200 OK (text/html) |
| 569 | 0.185708 | 192.168.1.10 | 128.119.245.12 | HTTP | 550 | GET /favicon.ico HTTP/1.1 |
| 570 | 0.164726 | 128.119.245.12 | 192.168.1.10 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

```

> Frame 84: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-153334397F8C}, id 0
> Ethernet II, Src: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74), Dst: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 55518, Seq: 1, Ack: 522, Len: 717
> Hypertext Transfer Protocol
<-- Line-based text data: text/html (12 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n        <title>401 Unauthorized</title>\n    </head><body>\n        <h1>Unauthorized</h1>\n        <p>This server could not verify that you\n    </body>\n</html>

```

Paquets: 581 · Affichés: 12 (2.1%) · Perdus: 0 (0.0%) Profile: Default

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Answer: HTTP/1 401 Unauthorized (text/html)

*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

http

| Titre | Time | Type: | Time (format as specified) | Fields: | Enter a field ... | événement | OK | Annuler |
|-------|----------|----------------|----------------------------|----------|-------------------|---|----|---------|
| No. | Time | Source | Destination | Protocol | Length | Info | | |
| 40 | 0.000549 | 192.168.1.10 | 128.119.245.12 | HTTP | 575 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 | | |
| 84 | 0.001729 | 128.119.245.12 | 192.168.1.10 | HTTP | 771 | HTTP/1.1 401 Unauthorized (text/html) | | |
| 138 | 0.000512 | 192.168.1.10 | 213.57.24.194 | HTTP | 178 | GET /ncsi.txt HTTP/1.1 | | |
| 143 | 0.000105 | 213.57.24.194 | 192.168.1.10 | HTTP | 233 | HTTP/1.1 200 OK (text/plain) | | |
| 534 | 0.000459 | 192.168.1.10 | 213.57.24.194 | HTTP | 178 | GET /ncsi.txt HTTP/1.1 | | |
| 536 | 0.000953 | 213.57.24.194 | 192.168.1.10 | HTTP | 233 | HTTP/1.1 200 OK (text/plain) | | |
| 551 | 0.000540 | 192.168.1.1 | 192.168.1.10 | HTTP | 311 | GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab51-4578-8bfb-7aa12ebcbc3b HTTP/1.1 | | |
| 553 | 0.000043 | 192.168.1.10 | 192.168.1.1 | HTTP/XML | 1186 | HTTP/1.1 200 OK | | |
| 562 | 0.003126 | 192.168.1.10 | 128.119.245.12 | HTTP | 660 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 | | |
| 567 | 0.001310 | 128.119.245.12 | 192.168.1.10 | HTTP | 544 | HTTP/1.1 200 OK (text/html) | | |
| 569 | 0.185708 | 192.168.1.10 | 128.119.245.12 | HTTP | 550 | GET /favicon.ico HTTP/1.1 | | |
| 570 | 0.164726 | 128.119.245.12 | 192.168.1.10 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) | | |

```

> Transmission Control Protocol, Src Port: 55519, Dst Port: 80, Seq: 1, Ack: 1, Len: 606
< Hypertext Transfer Protocol
  < GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      Cache-Control: max-age=0\r\n
    > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      DNT: 1\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/86.0.4240.193 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
```

wireshark_Ethernet5BT9T0.pcapng Paquets: 581 · Affichés: 12 (2.1%) · Perdus: 0 (0.0%) Profile: Default

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer: Authorization : Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms= (wireshark-students:network in Base64 encryption)