

Networks

Lab2 - HTTP protocol

Lab goal:

- 1 - Explore HTTP protocol
- 2 - Explore Persistent and Non-Persistent HTTP connection
- 3 - Compare HTTP vs HTTPS connection

TCP/IP stack

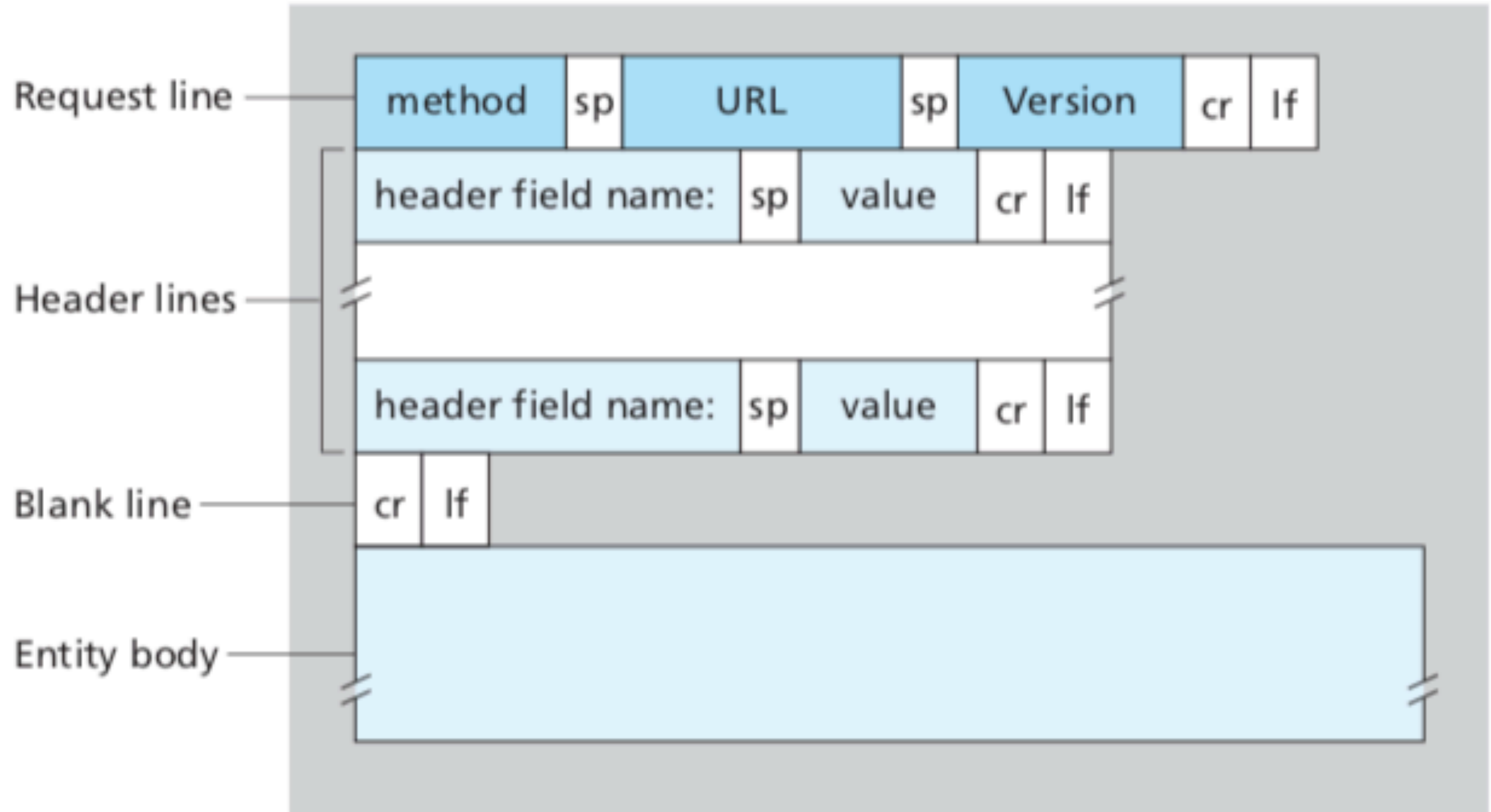


HTTP

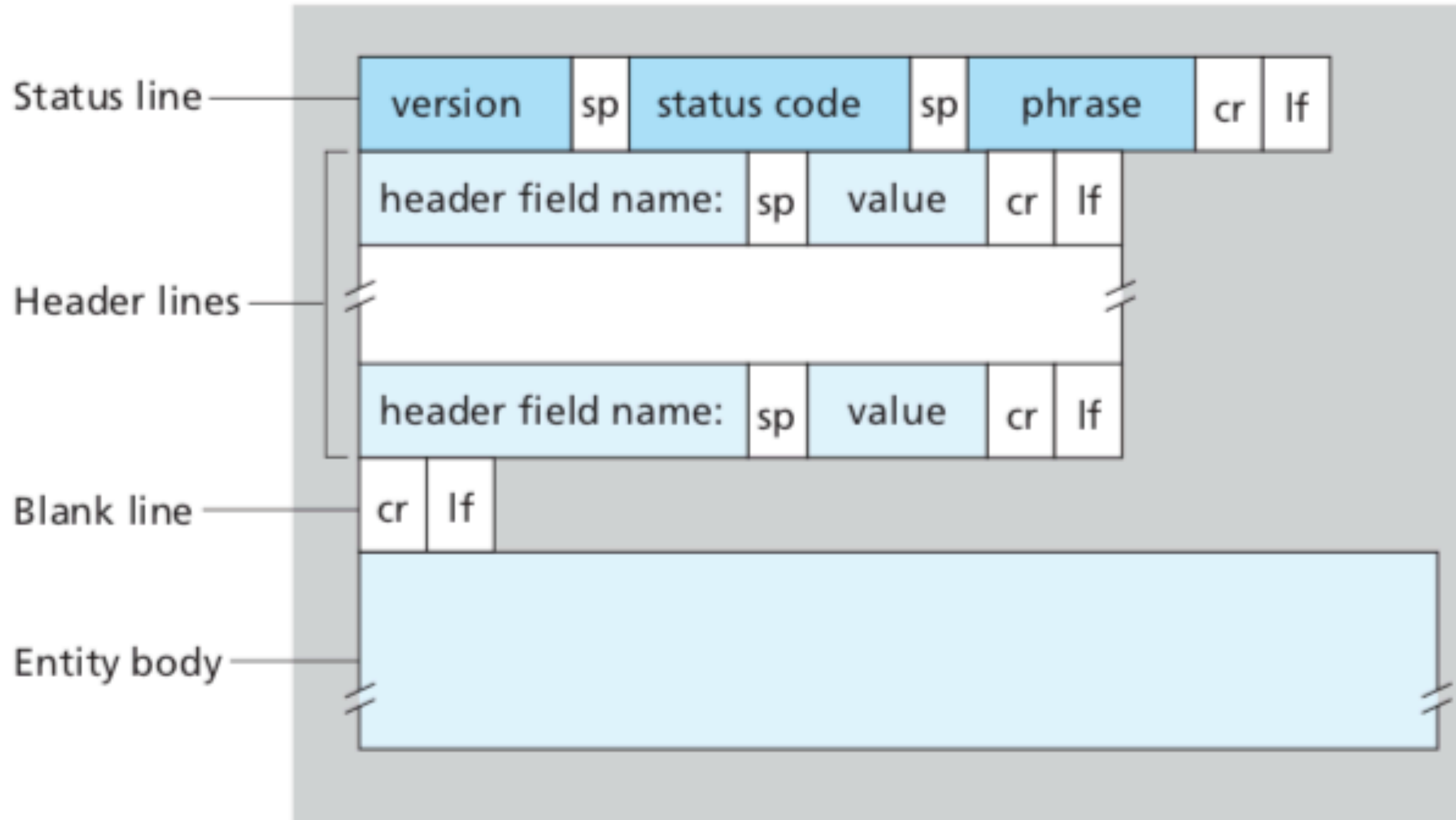
DNS

TCP

General format of an HTTP request message

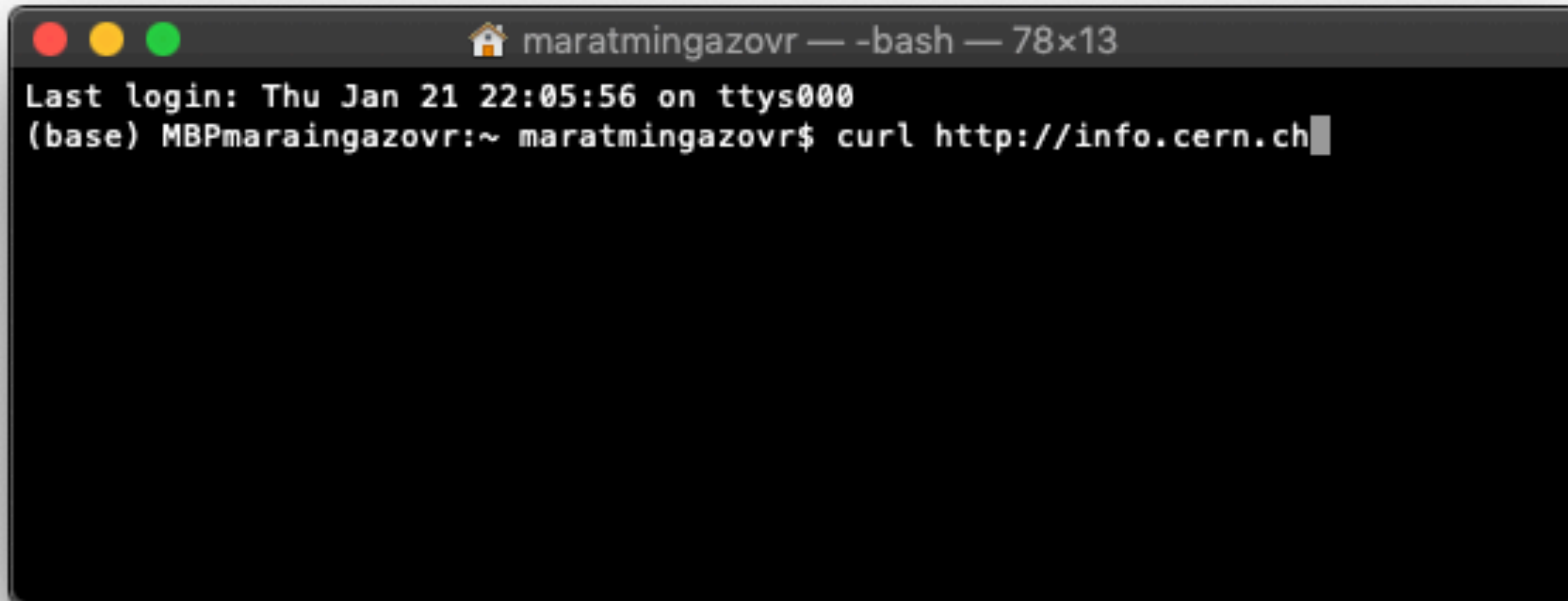


General format of an HTTP response message



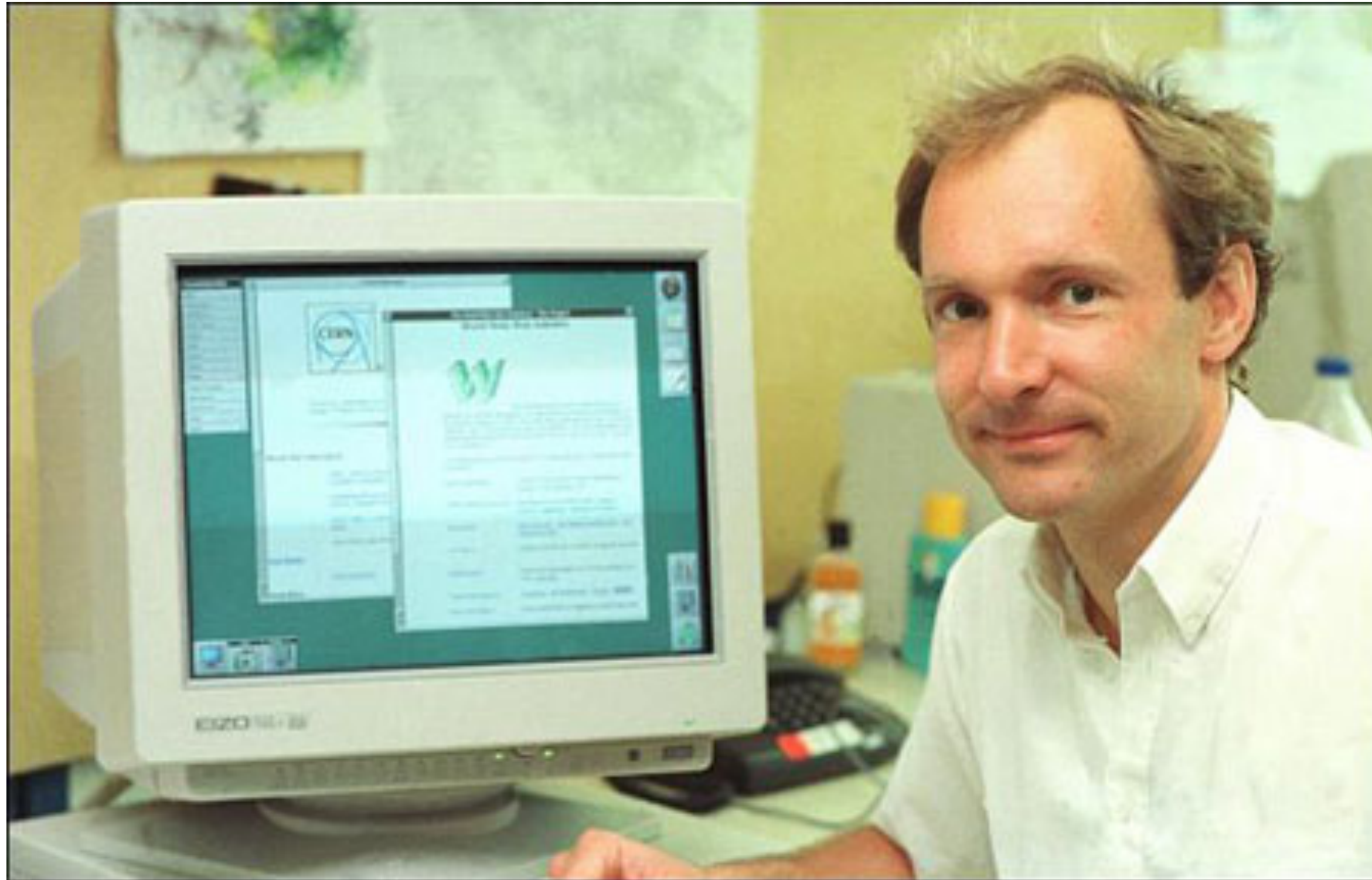
Task 1. Open the terminal and send GET request to info.cern.ch
Analyze what happened on the network

- 1 - You can use different tools to send GET request. For example **CURL**
- 2 - To send a **GET** request, type **curl http://info.cern.ch**

A screenshot of a macOS terminal window. The title bar shows a home icon, the username 'maratmingazovr', and the shell '-bash' with a window size of '78x13'. The terminal content shows the last login time as 'Thu Jan 21 22:05:56 on ttys000' and the current command prompt '(base) MBPmaratmingazovr:~ maratmingazovr\$' followed by the command 'curl http://info.cern.ch' with a cursor at the end.

```
maratmingazovr — -bash — 78x13
Last login: Thu Jan 21 22:05:56 on ttys000
(base) MBPmaratmingazovr:~ maratmingazovr$ curl http://info.cern.ch
```


What is info.cern.ch web-site?



Tim Berners-Lee

is an English computer scientist best known as the inventor of the World Wide Web.

Berners-Lee published the first web site, which described the project itself, **on 20 December 1990;**

it was available to the Internet from the CERN network.

info.cern.ch was the address of the world's first-ever website and web server, running on a NeXT computer at CERN.

From human point of view we just got the response

```
maratmingazovr — -bash — 86x24
Last login: Fri Jan 22 15:43:03 on ttys001
(base) MBPmaraingazovr:~ maratmingazovr$ curl http://info.cern.ch
<html><head></head><body><header>
<title>http://info.cern.ch</title>
</header>

<h1>http://info.cern.ch - home of the first website</h1>
<p>From here you can:</p>
<ul>
<li><a href="http://info.cern.ch/hypertext/WWW/TheProject.html">Browse the first website</a></li>
<li><a href="http://line-mode.cern.ch/www/hypertext/WWW/TheProject.html">Browse the first website using the line-mode browser simulator</a></li>
<li><a href="http://home.web.cern.ch/topics/birth-web">Learn about the birth of the web</a></li>
<li><a href="http://home.web.cern.ch/about">Learn about CERN, the physics laboratory where the web was born</a></li>
</ul>
</body></html>
(base) MBPmaraingazovr:~ maratmingazovr$
```


But what's going on inside the network ?

Wi-Fi: en0

dns || ip.addr == 188.184.21.108

Source	SPort	Destination	DPort	Protocol	Length	Info
fe80::2e:fede...	61920	fe80::5ad5:6e...	53	DNS	92	Standard query 0x528c
fe80::5ad5:6e...	53	fe80::2e:fede...	61920	DNS	139	Standard query response
192.168.1.172	59515	188.184.21.108	80	TCP	78	59515 → 80 [SYN] Seq=0
188.184.21.108	80	192.168.1.172	59515	TCP	74	80 → 59515 [SYN, ACK]
192.168.1.172	59515	188.184.21.108	80	TCP	66	59515 → 80 [ACK] Seq=1
192.168.1.172	59515	188.184.21.108	80	HTTP	142	GET / HTTP/1.1
188.184.21.108	80	192.168.1.172	59515	HTTP	944	HTTP/1.1 200 OK (text)
188.184.21.108	80	192.168.1.172	59515	TCP	66	80 → 59515 [FIN, ACK]
192.168.1.172	59515	188.184.21.108	80	TCP	66	59515 → 80 [ACK] Seq=7
192.168.1.172	59515	188.184.21.108	80	TCP	66	59515 → 80 [FIN, ACK]
188.184.21.108	80	192.168.1.172	59515	TCP	66	80 → 59515 [ACK] Seq=880

▶ Frame 131: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0

▶ Ethernet II, Src: D-LinkIn_6e:78:99 (58:d5:6e:6e:78:99), Dst: Apple_b0:1a:69 (ac:bc:32:b0:1a:69)

▶ Internet Protocol Version 4, Src: 188.184.21.108, Dst: 192.168.1.172

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 59515, Seq: 880, Ack: 78, Len: 0

0020 01 ac 00 50 e8 7b 14 34 0a 16 4c 18 72 30 80 10 ...P.{.4..L.r0..

0030 00 e3 9a 6f 00 00 01 01 08 0a 1f 59 db a6 4b 0a ...o.....Y..K.

0040 3b 89 ;.

This TCP option's kind (tcp.option_kind), 1 byte • Packets: 6337 • Displayed: 160 (2.5%) • Ignored: 8 (0.1%) • Profile: Default

DNS request

Connection establishment
Three-way handshake

Client send GET request

Server send Response

Connection termination
Graceful Connection
Release

Step 1. Send DNS request.

The image shows a Wireshark packet capture window titled "Wi-Fi: en0". The filter bar at the top shows "dns || ip.addr == 188.184.21.108". The packet list shows five packets, with the second packet (a DNS query) selected. The packet details pane shows the structure of the DNS query, including the transaction ID, flags, and the query for "info.cern.ch". The packet bytes pane shows the raw data of the selected packet, with the domain name "info.cern.ch" highlighted in blue.

Source	SPort	Destination	DPort	Protocol	Length	Info
fe80::2e:fede...	61920	fe80::5ad5:6e...	53	DNS	92	Standard query
fe80::5ad5:6e...	53	fe80::2e:fede...	61920	DNS	139	Standard query
192.168.1.172	59515	188.184.21.108	80	TCP	78	59515 → 80 [SYN
188.184.21.108	80	192.168.1.172	59515	TCP	74	80 → 59515 [SYN,
192.168.1.172	59515	188.184.21.108	80	TCP	66	59515 → 80 [ACK]

Transaction ID: 0x528c

- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
 - info.cern.ch: type A, class IN
 - Name: info.cern.ch
 - [Name Length: 12]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

[Response In: 114]

0020 fe de 13 21 98 23 fe 80 00 00 00 00 00 00 5a d5 ...!·#·...·Z·

0030 6e ff fe 6e 78 99 f1 e0 00 35 00 26 af c1 52 8c n··nx·...·5·&·R·

0040 01 00 00 01 00 00 00 00 00 00 04 69 6e 66 6f 04·info·

0050 63 65 72 6e 02 63 68 00 00 01 00 01 cern·ch·

Text item (text), 18 bytes Packets: 258610 · Displayed: 2286 (0.9%) · Ignored: 8 (0.0%) · Profile: Default

Step 2. DNS response give ip address of info.cern.ch

The image shows a Wireshark packet capture window titled "Wi-Fi: en0". The filter bar at the top shows "dns || ip.addr == 188.184.21.108". The packet list shows several packets, with the selected packet being a DNS response (Standard query response) from 188.184.21.108 to fe80::2e:fede... on port 53. The packet details pane shows the following information:

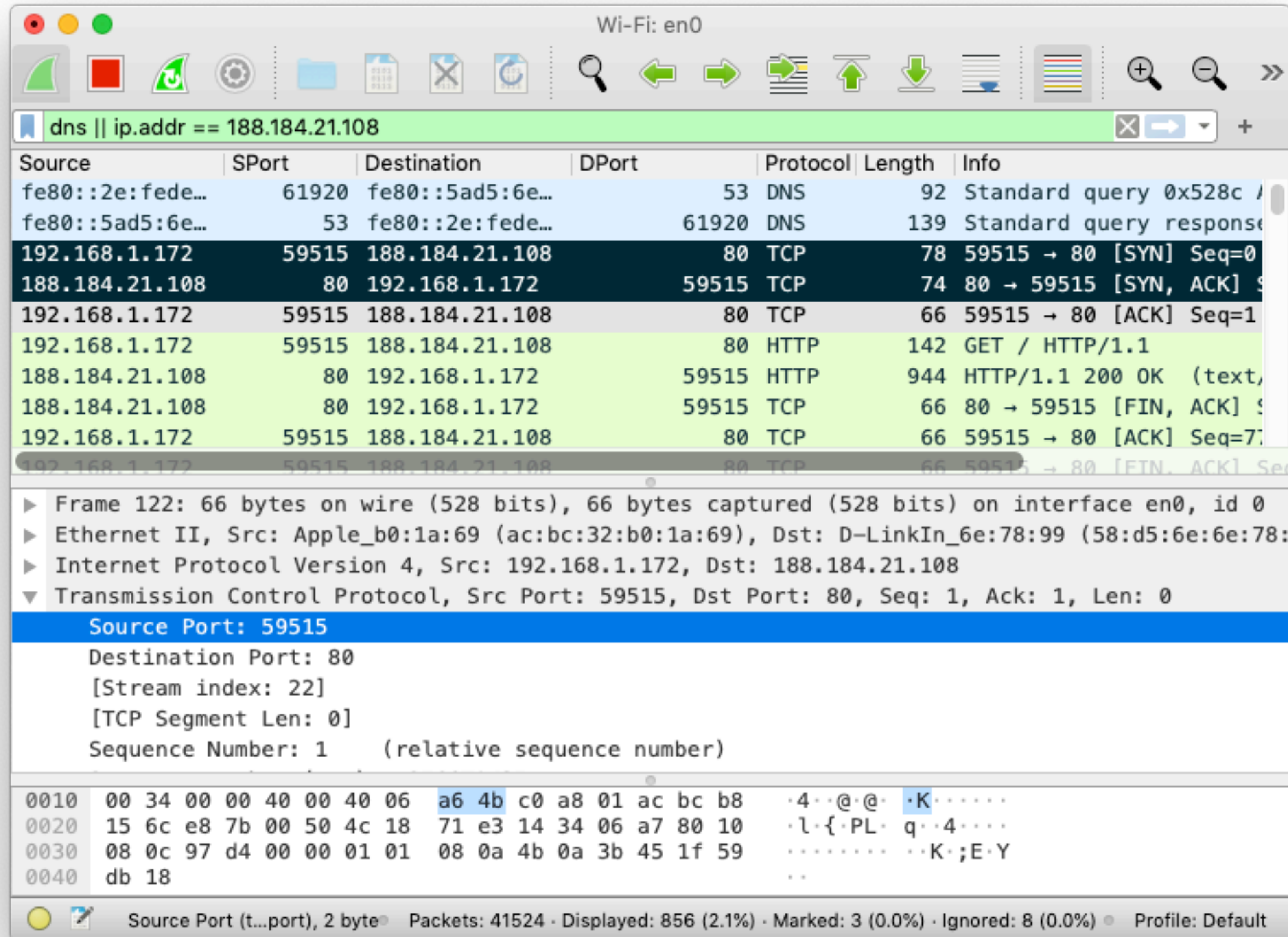
- Answers
 - info.cern.ch: type CNAME, class IN, cname webafs706.cern.ch
 - webafs706.cern.ch: type A, class IN, addr 188.184.21.108
 - Name: webafs706.cern.ch
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 6903 (1 hour, 55 minutes, 3 seconds)
 - Data length: 4
 - Address: 188.184.21.108

The packet bytes pane shows the raw data of the DNS response, with the following hex and ASCII values:

```
0060 00 01 00 00 28 20 00 13 09 77 65 62 61 66 73 37 .....( ..webafs7
0070 30 36 04 63 65 72 6e 02 63 68 00 c0 2a 00 01 00 06.cern.ch.*...
0080 01 00 00 1a f7 00 04 bc b8 15 6c .....l
```

The status bar at the bottom shows "Response Address (dns.a), 4 bytes" and "Packets: 32970 · Displayed: 722 (2.2%) · Ignored: 8 (0.0%) · Profile: Default".

Step 3. TCP connection establishment. Three-way handshake



Wi-Fi: en0

dns || ip.addr == 188.184.21.108

Source	SPort	Destination	DPort	Protocol	Length	Info
fe80::2e:fede...	61920	fe80::5ad5:6e...	53	DNS	92	Standard query 0x528c /
fe80::5ad5:6e...	53	fe80::2e:fede...	61920	DNS	139	Standard query response
192.168.1.172	59515	188.184.21.108	80	TCP	78	59515 → 80 [SYN] Seq=0
188.184.21.108	80	192.168.1.172	59515	TCP	74	80 → 59515 [SYN, ACK] s
192.168.1.172	59515	188.184.21.108	80	TCP	66	59515 → 80 [ACK] Seq=1
192.168.1.172	59515	188.184.21.108	80	HTTP	142	GET / HTTP/1.1
188.184.21.108	80	192.168.1.172	59515	HTTP	944	HTTP/1.1 200 OK (text,
188.184.21.108	80	192.168.1.172	59515	TCP	66	80 → 59515 [FIN, ACK] s
192.168.1.172	59515	188.184.21.108	80	TCP	66	59515 → 80 [ACK] Seq=7
192.168.1.172	59515	188.184.21.108	80	TCP	66	59515 → 80 [FIN, ACK] Seq

▶ Frame 122: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0

▶ Ethernet II, Src: Apple_b0:1a:69 (ac:bc:32:b0:1a:69), Dst: D-LinkIn_6e:78:99 (58:d5:6e:6e:78:99)

▶ Internet Protocol Version 4, Src: 192.168.1.172, Dst: 188.184.21.108

▼ Transmission Control Protocol, Src Port: 59515, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 59515

Destination Port: 80

[Stream index: 22]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

0010	00 34 00 00 40 00 40 06	a6 4b c0 a8 01 ac bc b8	·4·@·@··K·
0020	15 6c e8 7b 00 50 4c 18	71 e3 14 34 06 a7 80 10	·l·{·PL·q·4·
0030	08 0c 97 d4 00 00 01 01	08 0a 4b 0a 3b 45 1f 59	······K·;E·Y
0040	db 18		··

Source Port (t...port), 2 byte · Packets: 41524 · Displayed: 856 (2.1%) · Marked: 3 (0.0%) · Ignored: 8 (0.0%) · Profile: Default

Step 4. Client send GET request.

The image shows a Wireshark packet capture window titled "Wi-Fi: en0". The packet list pane shows a single packet, packet 124, which is a GET request from 192.168.1.172 to 188.184.21.108 on port 80. The packet details pane shows the structure of the request, including the GET method, host, user-agent, and accept headers. The packet bytes pane shows the raw data of the request, including the GET method, host, user-agent, and accept headers.

dns || ip.addr == 188.184.21.108

Source	SPort	Destination	DPort	Protocol	Length	Info
192.168.1.172	59515	188.184.21.108	80	HTTP	142	GET / HTTP/1.1

▶ Frame 124: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface en0, id 124

- ▶ Ethernet II, Src: Apple_b0:1a:69 (ac:bc:32:b0:1a:69), Dst: D-LinkIn_6e:78:99 (58:d5:6e:6e:78:99)
- ▶ Internet Protocol Version 4, Src: 192.168.1.172, Dst: 188.184.21.108
- ▶ Transmission Control Protocol, Src Port: 59515, Dst Port: 80, Seq: 1, Ack: 1, Len: 76

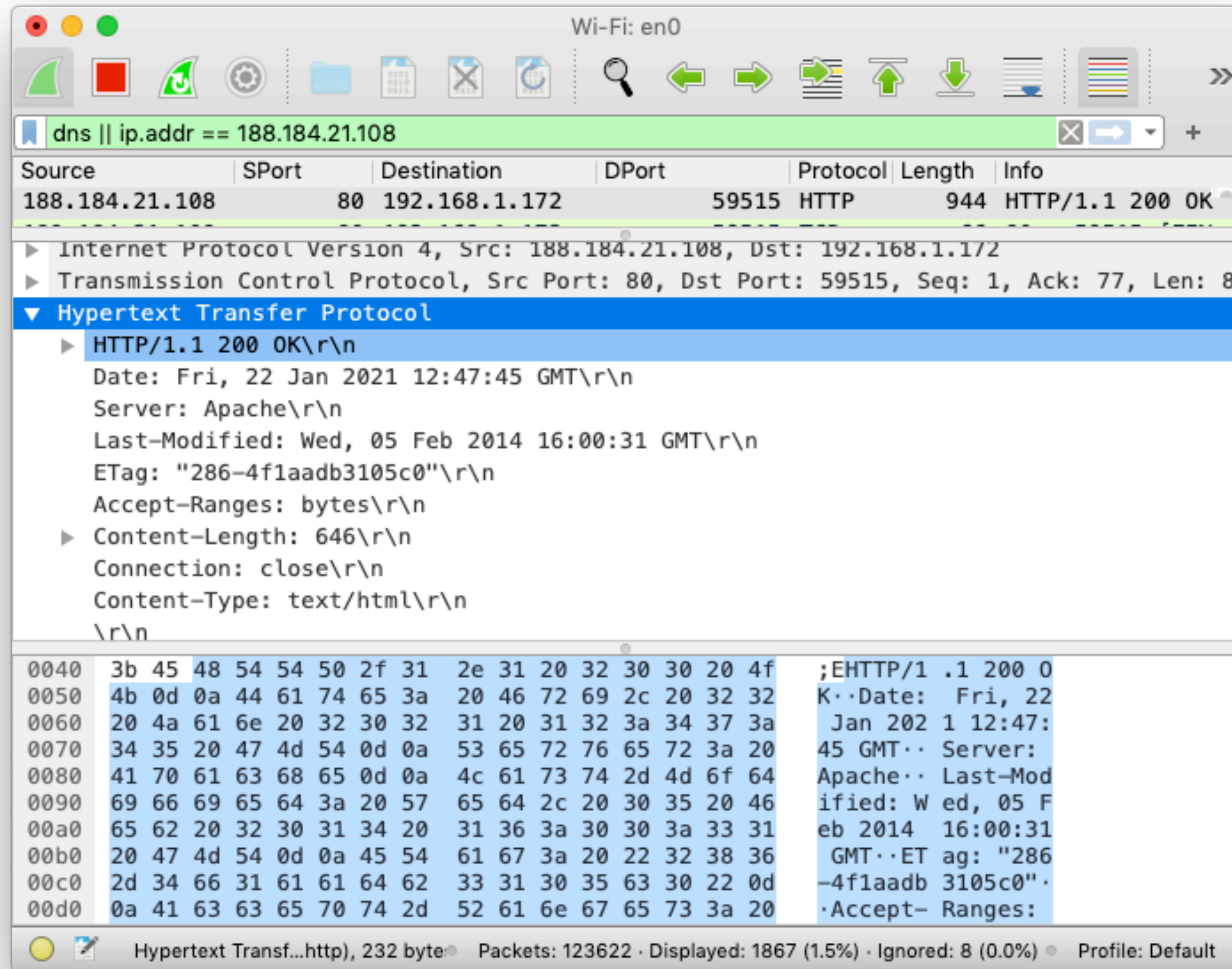
▼ Hypertext Transfer Protocol

- ▶ GET / HTTP/1.1\r\n
- Host: info.cern.ch\r\n
- User-Agent: curl/7.68.0\r\n
- Accept: */*\r\n
- \r\n
- [Full request URI: <http://info.cern.ch/>]
- [HTTP request 1/1]
- [Response in frame: 126]

Offset	Hex	ASCII
0000	58 d5 6e 6e 78 99 ac bc 32 b0 1a 69 08 00 45 00	X·nnx··· 2··i··E·
0010	00 80 00 00 40 00 40 06 a5 ff c0 a8 01 ac bc b8	····@·@· ······
0020	15 6c e8 7b 00 50 4c 18 71 e3 14 34 06 a7 80 18	·l·{·PL· q··4···
0030	08 0c 49 2e 00 00 01 01 08 0a 4b 0a 3b 45 1f 59	··I· ···· ··K·;E·Y
0040	db 18 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31	··GET / HTTP/1.1
0050	0d 0a 48 6f 73 74 3a 20 69 6e 66 6f 2e 63 65 72	··Host: info.cer
0060	6e 2e 63 68 0d 0a 55 73 65 72 2d 41 67 65 6e 74	n.ch··Us er-Agent
0070	3a 20 63 75 72 6c 2f 37 2e 36 38 2e 30 0d 0a 41	: curl/7 .68.0··A
0080	63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d 0a	ccept: * /*····

Hypertext Transfer Protocol (http), 76 bytes · Packets: 47480 · Displayed: 957 (2.0%) · Ignored: 8 (0.0%) · Profile: Default

Step 5. Server send Response (Header).



Wi-Fi: en0

dns || ip.addr == 188.184.21.108

Source	SPort	Destination	DPort	Protocol	Length	Info
188.184.21.108	80	192.168.1.172	59515	HTTP	944	HTTP/1.1 200 OK

Internet Protocol Version 4, Src: 188.184.21.108, Dst: 192.168.1.172

Transmission Control Protocol, Src Port: 80, Dst Port: 59515, Seq: 1, Ack: 77, Len: 8

Hypertext Transfer Protocol

- HTTP/1.1 200 OK\r\n
- Date: Fri, 22 Jan 2021 12:47:45 GMT\r\n
- Server: Apache\r\n
- Last-Modified: Wed, 05 Feb 2014 16:00:31 GMT\r\n
- ETag: "286-4f1aadb3105c0"\r\n
- Accept-Ranges: bytes\r\n
- Content-Length: 646\r\n
- Connection: close\r\n
- Content-Type: text/html\r\n
- \r\n

0040 3b 45 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f ;EHTTP/1 .1 200 0

0050 4b 0d 0a 44 61 74 65 3a 20 46 72 69 2c 20 32 32 K·Date: Fri, 22

0060 20 4a 61 6e 20 32 30 32 31 20 31 32 3a 34 37 3a Jan 2021 12:47:

0070 34 35 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 45 GMT· Server:

0080 41 70 61 63 68 65 0d 0a 4c 61 73 74 2d 4d 6f 64 Apache· Last-Mod

0090 69 66 69 65 64 3a 20 57 65 64 2c 20 30 35 20 46 ified: Wed, 05 F

00a0 65 62 20 32 30 31 34 20 31 36 3a 30 30 3a 33 31 eb 2014 16:00:31

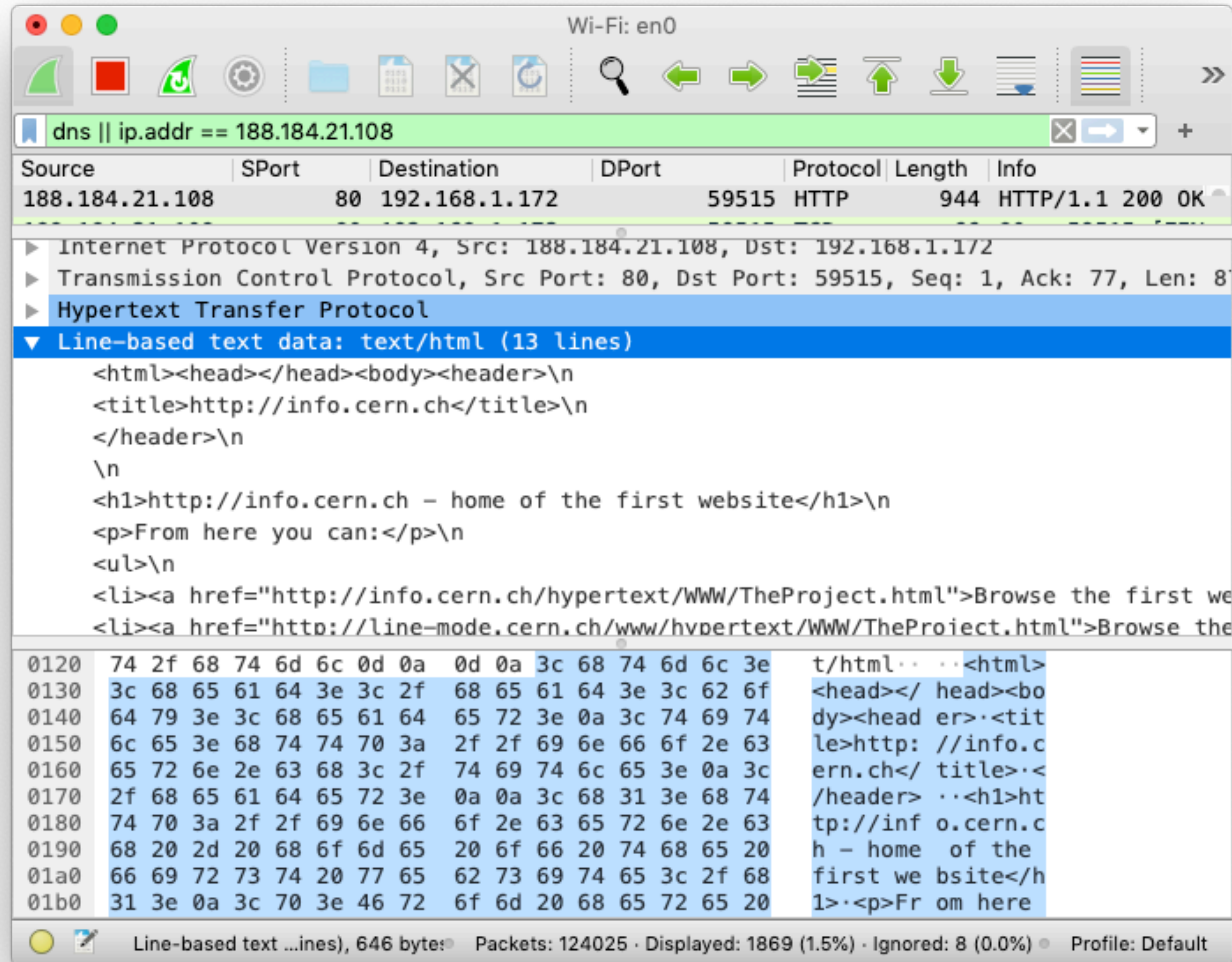
00b0 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 32 38 36 GMT·ET ag: "286

00c0 2d 34 66 31 61 61 64 62 33 31 30 35 63 30 22 0d -4f1aadb 3105c0"

00d0 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 ·Accept- Ranges:

Hypertext Transf...http), 232 byte · Packets: 123622 · Displayed: 1867 (1.5%) · Ignored: 8 (0.0%) · Profile: Default

Step 5. Server send Response (Body).



Wi-Fi: en0

dns || ip.addr == 188.184.21.108

Source	SPort	Destination	DPort	Protocol	Length	Info
188.184.21.108	80	192.168.1.172	59515	HTTP	944	HTTP/1.1 200 OK

Internet Protocol Version 4, Src: 188.184.21.108, Dst: 192.168.1.172

Transmission Control Protocol, Src Port: 80, Dst Port: 59515, Seq: 1, Ack: 77, Len: 8

Hypertext Transfer Protocol

Line-based text data: text/html (13 lines)

```
<html><head></head><body><header>\n<title>http://info.cern.ch</title>\n</header>\n\n<h1>http://info.cern.ch - home of the first website</h1>\n<p>From here you can:</p>\n<ul>\n<li><a href="http://info.cern.ch/hypertext/WWW/TheProject.html">Browse the first we</li><a href="http://line-mode.cern.ch/www/hypertext/WWW/TheProject.html">Browse the
```

0120 74 2f 68 74 6d 6c 0d 0a 0d 0a 3c 68 74 6d 6c 3e t/html... <html>
0130 3c 68 65 61 64 3e 3c 2f 68 65 61 64 3e 3c 62 6f <head></ head><bo
0140 64 79 3e 3c 68 65 61 64 65 72 3e 0a 3c 74 69 74 dy><head er>·<tit
0150 6c 65 3e 68 74 74 70 3a 2f 2f 69 6e 66 6f 2e 63 le>http: //info.c
0160 65 72 6e 2e 63 68 3c 2f 74 69 74 6c 65 3e 0a 3c ern.ch</ title>·<
0170 2f 68 65 61 64 65 72 3e 0a 0a 3c 68 31 3e 68 74 /header> ··<h1>ht
0180 74 70 3a 2f 2f 69 6e 66 6f 2e 63 65 72 6e 2e 63 tp://inf o.cern.c
0190 68 20 2d 20 68 6f 6d 65 20 6f 66 20 74 68 65 20 h - home of the
01a0 66 69 72 73 74 20 77 65 62 73 69 74 65 3c 2f 68 first we bsite</h
01b0 31 3e 0a 3c 70 3e 46 72 6f 6d 20 68 65 72 65 20 l>·<p>Fr om here

Line-based text ...ines), 646 bytes · Packets: 124025 · Displayed: 1869 (1.5%) · Ignored: 8 (0.0%) · Profile: Default

Step 6. Connection termination.

The image shows a Wireshark packet capture window titled "Wi-Fi: en0". The filter bar shows "dns || ip.addr == 188.184.21.108". The packet list displays four packets related to a TCP connection termination:

Source	SPort	Destination	DPort	Protocol	Length	Info
188.184.21.108	80	192.168.1.172	59515	TCP	66	80 → 59515 [FIN
192.168.1.172	59515	188.184.21.108	80	TCP	66	59515 → 80 [ACK
192.168.1.172	59515	188.184.21.108	80	TCP	66	59515 → 80 [FIN
188.184.21.108	80	192.168.1.172	59515	TCP	66	80 → 59515 [ACK

The packet details pane for the selected packet (Frame 127) shows:

- Frame 127: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0
- Ethernet II, Src: D-LinkIn_6e:78:99 (58:d5:6e:6e:78:99), Dst: Apple_b0:1a:69 (ac:bc:32:b0:1a:69)
- Internet Protocol Version 4, Src: 188.184.21.108, Dst: 192.168.1.172
- Transmission Control Protocol, Src Port: 80, Dst Port: 59515, Seq: 879, Ack: 77, Len: 0

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  ac bc 32 b0 1a 69 58 d5 6e 6e 78 99 08 00 45 00  ..2..iX. nnx...E.
0010  00 34 dd fa 40 00 2c 06 dc 50 bc b8 15 6c c0 a8  .4..@.,. .P...l..
0020  01 ac 00 50 e8 7b 14 34 0a 15 4c 18 72 2f 80 11  ...P.{.4 ..L.r/..
0030  00 e3 9a fa 00 00 01 01 08 0a 1f 59 db 60 4b 0a  .....Y.`K.
0040  3b 45 ;E
```

The status bar at the bottom indicates: wireshark_Wi-FiKBSOX0.pcapng • Packets: 257293 • Displayed: 2262 (0.9%) • Ignored: 8 (0.0%) • Profile: Default

Task 2. Explore persistent and non-persistent http connection

1 - Establish persistent http connection

curl http://info.cern.ch

-H "Connection: keep-alive"

-H "Keep-Alive: timeout=5, max=100"

2 - Establish non-persistent http connection:

curl http://info.cern.ch

-H "Connection: close"

3 - Compare this two connection in terms of WireShark packets.

Task 3. Explore **https** connection

- 1 - Send https request **curl https://www.google.com/**
- 2 - Compare http and https packets. What is the difference ?

Wi-Fi: en0

ip.addr == 173.194.73.147

Source	SPort	Destination	DPort	Protocol	Length	Info
192.168.1.172	63173	173.194.73.147	443	TCP	78	63173 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=
173.194.73.147	443	192.168.1.172	63173	TCP	74	443 → 63173 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1436
192.168.1.172	63173	173.194.73.147	443	TCP	66	63173 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=127131
192.168.1.172	63173	173.194.73.147	443	TLSv1...	583	Client Hello
173.194.73.147	443	192.168.1.172	63173	TLSv1...	1484	Server Hello, Change Cipher Spec
173.194.73.147	443	192.168.1.172	63173	TLSv1...	1302	Application Data

▶ Frame 52: 1302 bytes on wire (10416 bits), 1302 bytes captured (10416 bits) on interface en0, id 0

▶ Ethernet II, Src: D-LinkIn_6e:78:99 (58:d5:6e:6e:78:99), Dst: Apple_b0:1a:69 (ac:bc:32:b0:1a:69)

▶ Internet Protocol Version 4, Src: 173.194.73.147, Dst: 192.168.1.172

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 63173, Seq: 1419, Ack: 518, Len: 1236

▶ [2 Reassembled TCP Segments (2521 bytes): #51(1285), #52(1236)]

▼ Transport Layer Security

▼ TLSv1.3 Record Layer: Application Data Protocol: http-over-tls

Opaque Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 2516

Encrypted Application Data: 05e647cd8f147c7655faad582a862853a35cb16b9d1c85052ee03d0c8005abe5929de3cc...

[Application Data Protocol: http-over-tls]

Offset	Hex	ASCII
0000	17 03 03 09 d4 05 e6 47 cd 8f 14 7c 76 55 fa adG... vU..
0010	58 2a 86 28 53 a3 5c b1 6b 9d 1c 85 05 2e e0 3d	X*(S\ k.....=
0020	0c 80 05 ab e5 92 9d e3 cc 87 7c 94 33 fa 17 b0 3...
0030	82 0c 05 82 40 cd a0 44 3c 49 ab bc 42 61 b2 9f	...@D <I Ba...
0040	05 2c 2a 13 b1 40 1e c9 c2 82 a4 ed d5 07 c2 b0	,*...@.....

Frame (1302 bytes) Reassembled TCP (2521 bytes)

Payload is encrypted application data (tls.app_data), 2,516 bytes

Packets: 6392 · Displayed: 89 (1.4%) · Ignored: 1 (0.0%) · Profile: Default