

No.	Time	Source	Destination	Length	Protocol
39	2023-09-22 14:05:14.358687	10.12.92.76	128.119.245.12	558	HTTP

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 39: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface en0, id 0
Section number: 1
Interface id: 0 (en0)
Interface name: en0
Interface description: Wi-Fi
Encapsulation type: Ethernet (1)
Arrival Time: Sep 22, 2023 14:05:14.358687000 MDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1695413114.358687000 seconds
[Time delta from previous captured frame: 0.000113000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 5.823968000 seconds]
Frame Number: 39
Frame Length: 558 bytes (4464 bits)
Capture Length: 558 bytes (4464 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: Apple_8d:db:36 (f4:d4:88:8d:db:36), Dst: Cisco_80:9b:df (6c:8b:d3:80:9b:df)
Destination: Cisco_80:9b:df (6c:8b:d3:80:9b:df)
Address: Cisco_80:9b:df (6c:8b:d3:80:9b:df)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Source: Apple_8d:db:36 (f4:d4:88:8d:db:36)
Address: Apple_8d:db:36 (f4:d4:88:8d:db:36)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.12.92.76, Dst: 128.119.245.12
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 544
Identification: 0x0000 (0)
010. = Flags: 0x2, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x5cfc [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.12.92.76
Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 57672, Dst Port: 80, Seq: 1, Ack: 1, Len: 504
Source Port: 57672
Destination Port: 80
[Stream index: 9]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 504]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 364782832
[Next Sequence Number: 505 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3714818623
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
 000. = Reserved: Not set
 ...0 = Accurate ECN: Not set
 0... = Congestion Window Reduced: Not set
 0.. = ECN-Echo: Not set
 0. = Urgent: Not set
 1 = Acknowledgment: Set
 1... = Push: Set
 0.. = Reset: Not set
 0. = Syn: Not set
 0 = Fin: Not set
 [TCP Flags:AP...]
Window: 4096
[Calculated window size: 262144]
[Window size scaling factor: 64]
Checksum: 0x9eaa [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
 [Time since first frame in this TCP stream: 0.067714000 seconds]
 [Time since previous frame in this TCP stream: 0.000113000 seconds]
[SEQ/ACK analysis]
 [iRTT: 0.067601000 seconds]
 [Bytes in flight: 504]
 [Bytes sent since last PSH flag: 504]
TCP payload (504 bytes)
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
 [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
 [Severity level: Chat]
 [Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/INTRO-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
If-None-Match: "51-605d8305477ae"\r\n
Upgrade-Insecure-Requests: 1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
If-Modified-Since: Thu, 21 Sep 2023 05:59:02 GMT\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.6 Safari/605.1.15\r\n
Accept-Language: en-CA,en-US;q=0.9,en;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 41]

No.	Time	Source	Destination	Length	Protocol
41	2023-09-22 14:05:14.430055	128.119.245.12	10.12.92.76	492	HTTP

HTTP/1.1 200 OK (text/html)
Frame 41: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface en0, id 0
Section number: 1
Interface id: 0 (en0)
Interface name: en0
Interface description: Wi-Fi
Encapsulation type: Ethernet (1)

```
Arrival Time: Sep 22, 2023 14:05:14.430055000 MDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1695413114.430055000 seconds
[Time delta from previous captured frame: 0.000774000 seconds]
[Time delta from previous displayed frame: 0.071368000 seconds]
[Time since reference or first frame: 5.895336000 seconds]
Frame Number: 41
Frame Length: 492 bytes (3936 bits)
Capture Length: 492 bytes (3936 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Cisco_80:9b:df (6c:8b:d3:80:9b:df), Dst: Apple_8d:db:36 (f4:d4:88:8d:db:36)
Destination: Apple_8d:db:36 (f4:d4:88:8d:db:36)
Address: Apple_8d:db:36 (f4:d4:88:8d:db:36)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ..0 .... = IG bit: Individual address (unicast)
Source: Cisco_80:9b:df (6c:8b:d3:80:9b:df)
Address: Cisco_80:9b:df (6c:8b:d3:80:9b:df)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ..0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.12.92.76
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 478
Identification: 0x072a (1834)
010. .... = Flags: 0x2, Don't fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 32
Protocol: TCP (6)
Header Checksum: 0x7614 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 10.12.92.76
Transmission Control Protocol, Src Port: 80, Dst Port: 57672, Seq: 1, Ack: 505, Len: 438
Source Port: 80
Destination Port: 57672
[Stream index: 9]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 438]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3714818623
[Next Sequence Number: 439 (relative sequence number)]
Acknowledgment Number: 505 (relative ack number)
Acknowledgment number (raw): 364783336
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ....1 .... = Acknowledgment: Set
```

.... 1... = Push: Set
.... .0.. = Reset: Not set
.... ..0. = Syn: Not set
.... ...0 = Fin: Not set
[TCP Flags:AP...]

Window: 237

[Calculated window size: 30336]

[Window size scaling factor: 128]

Checksum: 0xbcf9 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[Time since first frame in this TCP stream: 0.139082000 seconds]

[Time since previous frame in this TCP stream: 0.000774000 seconds]

[SEQ/ACK analysis]

[iRTT: 0.067601000 seconds]

[Bytes in flight: 438]

[Bytes sent since last PSH flag: 438]

TCP payload (438 bytes)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

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

[HTTP/1.1 200 OK\r\n\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Fri, 22 Sep 2023 20:05:14 GMT\r\n

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

Last-Modified: Fri, 22 Sep 2023 05:59:01 GMT\r\n

ETag: "51-605ec4e276cfa"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\r\n

[Content length: 81]

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 1/1]

[Time since request: 0.071368000 seconds]

[Request in frame: 39]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

File Data: 81 bytes

Line-based text data: text/html (3 lines)

<html>\n

Congratulations! You've downloaded the first Wireshark lab file!\n

</html>\n