

No.	Time	Source	Destination	Protocol	Length	Info
539	11.969677	202.141.180.194	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 539: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface \Device\NPF_{8F4CCA7D-037E-4F4A-A903-982EA39577AF}, id 0

Section number: 1

Interface id: 0 (\Device\NPF_{8F4CCA7D-037E-4F4A-A903-982EA39577AF})

Interface name: \Device\NPF_{8F4CCA7D-037E-4F4A-A903-982EA39577AF}

Interface description: WLAN

Encapsulation type: Ethernet (1)

Arrival Time: Oct 5, 2023 13:55:56.146190000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1696485356.146190000 seconds

[Time delta from previous captured frame: 0.000193000 seconds]

[Time delta from previous displayed frame: 5.443559000 seconds]

[Time since reference or first frame: 11.969677000 seconds]

Frame Number: 539

Frame Length: 566 bytes (4528 bits)

Capture Length: 566 bytes (4528 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: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3), Dst: VMware_9f:00:7f (00:50:56:9f:00:7f)

Destination: VMware_9f:00:7f (00:50:56:9f:00:7f)

Address: VMware_9f:00:7f (00:50:56:9f:00:7f)

.... 0. = LG bit: Globally unique address (factory default)

.... 0 = IG bit: Individual address (unicast)

Source: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3)

Address: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3)

.... 0. = LG bit: Globally unique address (factory default)

.... 0 = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 202.141.180.194, 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: 552

Identification: 0xc4f1 (50417)

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: 128

Protocol: TCP (6)

Header Checksum: 0x3f0a [validation disabled]

[Header checksum status: Unverified]

Source Address: 202.141.180.194

Destination Address: 128.119.245.12

Transmission Control Protocol, Src Port: 50392, Dst Port: 80, Seq: 1, Ack: 1, Len: 512

Source Port: 50392

Destination Port: 80

[Stream index: 10]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 512]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 4144067985

[Next Sequence Number: 513 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 2273301255

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: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x18c6 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.275645000 seconds]
[Time since previous frame in this TCP stream: 0.000193000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.275452000 seconds]
[Bytes in flight: 512]
[Bytes sent since last PSH flag: 512]
TCP payload (512 bytes)
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
[GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0
Safari/537.36 Edg/117.0.2045.47\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/3]
[Response in frame: 562]
[Next request in frame: 574]
No.      Time           Source           Destination      Protocol Length Info
 562 12.258395    128.119.245.12   202.141.180.194  HTTP      784    HTTP/1.1 200 OK (text/html)
Frame 562: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{8F4CCA7D-037E-4F4A-A903-982EA39577AF}, id 0
Section number: 1
Interface id: 0 (\Device\NPF_{8F4CCA7D-037E-4F4A-A903-982EA39577AF})
Interface name: \Device\NPF_{8F4CCA7D-037E-4F4A-A903-982EA39577AF}
Interface description: WLAN
Encapsulation type: Ethernet (1)
Arrival Time: Oct 5, 2023 13:55:56.434908000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1696485356.434908000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.288718000 seconds]
[Time since reference or first frame: 12.258395000 seconds]
Frame Number: 562
Frame Length: 784 bytes (6272 bits)
Capture Length: 784 bytes (6272 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: VMWare_9f:00:7f (00:50:56:9f:00:7f), Dst: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3)
Destination: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3)
Address: LiteonTe_9d:af:b3 (74:4c:a1:9d:af:b3)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0. .... = IG bit: Individual address (unicast)
Source: VMWare_9f:00:7f (00:50:56:9f:00:7f)
Address: VMWare_9f:00:7f (00:50:56:9f:00:7f)
.... 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: 202.141.180.194
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
```

```
Differentiated Services Field: 0x04 (DSCP: LE, ECN: Not-ECT)
  0000 01.. = Differentiated Services Codepoint: Lower Effort (1)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 770
Identification: 0x125d (4701)
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: 34
Protocol: TCP (6)
Header Checksum: 0x4ec1 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 202.141.180.194
Transmission Control Protocol, Src Port: 80, Dst Port: 50392, Seq: 1, Ack: 513, Len: 730
Source Port: 80
Destination Port: 50392
[Stream index: 10]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 730]
Sequence Number: 1      (relative sequence number)
Sequence Number (raw): 2273301255
[Next Sequence Number: 731      (relative sequence number)]
Acknowledgment Number: 513      (relative ack number)
Acknowledgment number (raw): 4144068497
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: 0x02a0 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
  [Time since first frame in this TCP stream: 0.564363000 seconds]
  [Time since previous frame in this TCP stream: 0.001477000 seconds]
[SEQ/ACK analysis]
  [iRTT: 0.275452000 seconds]
  [Bytes in flight: 730]
  [Bytes sent since last PSH flag: 730]
TCP payload (730 bytes)
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, 05 Oct 2023 05:55:56 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: Thu, 05 Oct 2023 05:55:02 GMT\r\n
ETag: "173-606f1c3d0b269"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 371\r\n
  [Content length: 371]
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 1/3]
[Time since request: 0.288718000 seconds]
[Request in frame: 539]
[Next request in frame: 574]
[Next response in frame: 591]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
Line-based text data: text/html (10 lines)
\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
```