

No.	Time	Source	Destination	Protocol	Length	Info
72	11.167636	192.168.1.49	128.119.245.12	HTTP	671	GET /wireshark-labs/INTRO-wireshark-file1.html

HTTP/1.1

Frame 72: 671 bytes on wire (5368 bits), 671 bytes captured (5368 bits) on interface \Device\NPF\_{E8F1393B-10D6-4491-A631-26A44CA59FE2}, id 0

Interface id: 0 (\Device\NPF\_{E8F1393B-10D6-4491-A631-26A44CA59FE2})  
 Interface name: \Device\NPF\_{E8F1393B-10D6-4491-A631-26A44CA59FE2}  
 Interface description: Wi-Fi  
 Encapsulation type: Ethernet (1)  
 Arrival Time: May 1, 2021 20:47:42.783660000 Финляндия (лето)  
 [Time shift for this packet: 0.000000000 seconds]  
 Epoch Time: 1619891262.783660000 seconds  
 [Time delta from previous captured frame: 0.001362000 seconds]  
 [Time delta from previous displayed frame: 0.000000000 seconds]  
 [Time since reference or first frame: 11.167636000 seconds]  
 Frame Number: 72  
 Frame Length: 671 bytes (5368 bits)  
 Capture Length: 671 bytes (5368 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: IntelCor\_88:6b:3e (c8:b2:9b:88:6b:3e), Dst: ASUSTekC\_e5:39:80 (18:31:bf:e5:39:80)

Destination: ASUSTekC\_e5:39:80 (18:31:bf:e5:39:80)  
 Address: ASUSTekC\_e5:39:80 (18:31:bf:e5:39:80)  
 .... 0. .... = LG bit: Globally unique address (factory default)  
 .... 0. .... = IG bit: Individual address (unicast)  
 Source: IntelCor\_88:6b:3e (c8:b2:9b:88:6b:3e)  
 Address: IntelCor\_88:6b:3e (c8:b2:9b:88:6b:3e)  
 .... 0. .... = LG bit: Globally unique address (factory default)  
 .... 0. .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.1.49, 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: 657

Identification: 0xc15e (49502)

Flags: 0x40, Don't fragment

0... .... = Reserved bit: Not set  
 .1.. .... = Don't fragment: Set  
 ..0. .... = More fragments: Not set

Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.49

Destination Address: 128.119.245.12

Transmission Control Protocol, Src Port: 57720, Dst Port: 80, Seq: 1, Ack: 1, Len: 617

Source Port: 57720

Destination Port: 80

[Stream index: 9]

[TCP Segment Len: 617]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1819868980

[Next Sequence Number: 618 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 2051680621

0101 .... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

000. .... = Reserved: Not set  
 ...0 .... = Nonce: Not set  
 .... 0... = Congestion Window Reduced (CWR): 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: 0x39e1 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[SEQ/ACK analysis]

[iRTT: 0.113949000 seconds]

[Bytes in flight: 617]

[Bytes sent since last PSH flag: 617]

[Timestamps]

[Time since first frame in this TCP stream: 0.115311000 seconds]

```
C:\Users\Tinkra\Downloads\LocalTemp\wireshark_wi-Fi-PCap_VH20.pcapng 221 total packets, 2 shown
[Time since previous frame in this TCP stream: 0.001362000 seconds]
TCP payload (617 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
Connection: keep-alive\r\n
Cache-Control: max-age=0\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/90.0.4430.72 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: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7,uk;q=0.6\r\n
If-None-Match: "51-5c13e6cd51121"\r\n
If-Modified-Since: Sat, 01 May 2021 05:59:01 GMT\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: 96]
No.      Time                Source                Destination            Protocol Length Info
  96 11.287712         128.119.245.12        192.168.1.49           HTTP      293    HTTP/1.1 304 Not Modified
Frame 96: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{E8F1393B-10D6-4491-A631-26A44CA59FE2}, id 0
  Interface id: 0 (\Device\NPF_{E8F1393B-10D6-4491-A631-26A44CA59FE2})
    Interface name: \Device\NPF_{E8F1393B-10D6-4491-A631-26A44CA59FE2}
    Interface description: Wi-Fi
  Encapsulation type: Ethernet (1)
  Arrival Time: May 1, 2021 20:47:42.903736000 Финляндия (лето)
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1619891262.903736000 seconds
  [Time delta from previous captured frame: 0.001980000 seconds]
  [Time delta from previous displayed frame: 0.120076000 seconds]
  [Time since reference or first frame: 11.287712000 seconds]
  Frame Number: 96
  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: ASUSTekC_e5:39:80 (18:31:bf:e5:39:80), Dst: IntelCor_88:6b:3e (c8:b2:9b:88:6b:3e)
  Destination: IntelCor_88:6b:3e (c8:b2:9b:88:6b:3e)
    Address: IntelCor_88:6b:3e (c8:b2:9b:88:6b:3e)
      .... 0. .... = LG bit: Globally unique address (factory default)
      .... 0 .... = IG bit: Individual address (unicast)
    Source: ASUSTekC_e5:39:80 (18:31:bf:e5:39:80)
      Address: ASUSTekC_e5:39:80 (18:31:bf:e5:39:80)
        .... 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: 192.168.1.49
  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)
    .... 000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 279
  Identification: 0xed9f (60831)
  Flags: 0x40, Don't fragment
    0... .... = Reserved bit: Not set
    1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  Fragment Offset: 0
  Time to Live: 45
  Protocol: TCP (6)
  Header Checksum: 0x27e4 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 128.119.245.12
  Destination Address: 192.168.1.49
Transmission Control Protocol, Src Port: 80, Dst Port: 57720, Seq: 1, Ack: 618, Len: 239
  Source Port: 80
  Destination Port: 57720
  [Stream index: 9]
  [TCP Segment Len: 239]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2051680621
  [Next Sequence Number: 240 (relative sequence number)]
  Acknowledgment Number: 618 (relative ack number)
  Acknowledgment number (raw): 1819869597
```

```
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
 000. .... = Reserved: Not set
...0 .... = Nonce: Not set
... 0... = Congestion Window Reduced (CWR): 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: 238
[Calculated window size: 30464]
[Window size scaling factor: 128]
Checksum: 0xd37a [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[SEQ/ACK analysis]
  [iRTT: 0.113949000 seconds]
  [BYTES in flight: 239]
  [Bytes sent since last PSH flag: 239]
[Timestamps]
  [Time since first frame in this TCP stream: 0.235387000 seconds]
  [Time since previous frame in this TCP stream: 0.001980000 seconds]
TCP payload (239 bytes)
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
    [HTTP/1.1 304 Not Modified\r\n]
    [Severity level: Chat]
    [Group: Sequence]
  Response Version: HTTP/1.1
  Status Code: 304
  [Status Code Description: Not Modified]
  Response Phrase: Not Modified
Date: Sat, 01 May 2021 17:47:42 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "51-5c13e6cd51121"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.120076000 seconds]
[Request in frame: 72]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```