

No.	Time	Source	Destination	Protocol	Length	Info
187	5.281952	10.13.166.59	128.119.245.12	HTTP	541	GET /wireshark-labs/INTRO-wireshark-file1.html

HTTP/1.1

Frame 187: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface \Device\NPF_{5704ECEF-85EA-4BEA-9BCF-1A1F89899944}, id 0

Section number: 1

Interface id: 0 (\Device\NPF_{5704ECEF-85EA-4BEA-9BCF-1A1F89899944})

Interface name: \Device\NPF_{5704ECEF-85EA-4BEA-9BCF-1A1F89899944}

Interface description: Wi-Fi

Encapsulation type: Ethernet (1)

Arrival Time: Sep 25, 2024 08:30:31.280248000 Mountain Daylight Time

UTC Arrival Time: Sep 25, 2024 14:30:31.280248000 UTC

Epoch Arrival Time: 1727274631.280248000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.010948000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 5.281952000 seconds]

Frame Number: 187

Frame Length: 541 bytes (4328 bits)

Capture Length: 541 bytes (4328 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: AzureWaveTec_c1:d1:21 (70:66:55:c1:d1:21), Dst: Cisco_94:75:1f (6c:8b:d3:94:75:1f)

Destination: Cisco_94:75:1f (6c:8b:d3:94:75:1f)

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

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

Source: AzureWaveTec_c1:d1:21 (70:66:55:c1:d1:21)

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

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

Type: IPv4 (0x0800)

[Stream index: 0]

Internet Protocol Version 4, Src: 10.13.166.59, 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: 527

Identification: 0xa589 (42377)

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: 0x2d93 [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.13.166.59

Destination Address: 128.119.245.12

[Stream index: 8]

Transmission Control Protocol, Src Port: 64927, Dst Port: 80, Seq: 1, Ack: 1, Len: 487

Source Port: 64927

Destination Port: 80

[Stream index: 9]

[Stream Packet Number: 4]

[Conversation completeness: Complete, WITH_DATA (63)]

..1. = RST: Present

...1 = FIN: Present

.... 1... = Data: Present

.... .1.. = ACK: Present

.... ..1. = SYN-ACK: Present

.... ...1 = SYN: Present

[Completeness Flags: RFDASS]

[TCP Segment Len: 487]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 926447928

[Next Sequence Number: 488 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 1424090542

```
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: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x5813 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
  [Time since first frame in this TCP stream: 0.093320000 seconds]
  [Time since previous frame in this TCP stream: 0.014185000 seconds]
[SEQ/ACK analysis]
  [iRTT: 0.079135000 seconds]
  [Bytes in flight: 487]
  [Bytes sent since last PSH flag: 487]
TCP payload (487 bytes)
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
  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
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
Edg/129.0.0.0\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=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Response in frame: 218]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
No.      Time      Source      Destination      Protocol  Length Info
218 5.362832 128.119.245.12 10.13.166.59 HTTP 492 HTTP/1.1 200 OK (text/html)
Frame 218: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface
\Device\NPF_{5704ECEF-85EA-4BEA-9BCF-1A1F89899944}, id 0
  Section number: 1
  Interface id: 0 (\Device\NPF_{5704ECEF-85EA-4BEA-9BCF-1A1F89899944})
  Interface name: \Device\NPF_{5704ECEF-85EA-4BEA-9BCF-1A1F89899944}
  Interface description: Wi-Fi
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 25, 2024 08:30:31.361128000 Mountain Daylight Time
  UTC Arrival Time: Sep 25, 2024 14:30:31.361128000 UTC
  Epoch Arrival Time: 1727274631.361128000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.001185000 seconds]
  [Time delta from previous displayed frame: 0.000880000 seconds]
  [Time since reference or first frame: 5.362832000 seconds]
  Frame Number: 218
  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_94:75:1f (6c:8b:d3:94:75:1f), Dst: AzureWaveTec_c1:d1:21 (70:66:55:c1:d1:21)
  Destination: AzureWaveTec_c1:d1:21 (70:66:55:c1:d1:21)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ...0 .... = IG bit: Individual address (unicast)
  Source: Cisco_94:75:1f (6c:8b:d3:94:75:1f)
```

```

    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.13.166.59
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: 0x65ca (26058)
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: 35
Protocol: TCP (6)
Header Checksum: 0xca83 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 10.13.166.59
[Stream index: 8]
Transmission Control Protocol, Src Port: 80, Dst Port: 64927, Seq: 1, Ack: 488, Len: 438
Source Port: 80
Destination Port: 64927
[Stream index: 9]
[Stream Packet Number: 6]
[Conversation completeness: Complete, WITH_DATA (63)]
    ..1. .... = RST: Present
    ...1 .... = FIN: Present
    .... 1... = Data: Present
    .... .1.. = ACK: Present
    .... ..1. = SYN-ACK: Present
    .... ...1 = SYN: Present
[Completeness Flags: RFDASS]
[TCP Segment Len: 438]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1424090542
[Next Sequence Number: 439 (relative sequence number)]
Acknowledgment Number: 488 (relative ack number)
Acknowledgment number (raw): 926448415
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: 30016
[Calculated window size: 30016]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0xe22e [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
    [Time since first frame in this TCP stream: 0.174200000 seconds]
    [Time since previous frame in this TCP stream: 0.001185000 seconds]
[SEQ/ACK analysis]
    [iRTT: 0.079135000 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
    Response Version: HTTP/1.1
```

C:\Users\gerar\AppData\Local\Temp\wireshark_Wi-Fi9M3LU2.pcapng 1213 total packets, 2 shown

```
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Wed, 25 Sep 2024 14:30:31 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: Wed, 25 Sep 2024 05:59:01 GMT\r\n
ETag: "51-622eb51973b01"\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
[Request in frame: 187]
[Time since request: 0.080880000 seconds]
[Request URI: /wireshark-labs/INTRO-wireshark-file1.html]
[Full 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
```