

No.	Time	Source	Destination	Protocol	Length	Info
1359	31.775342	128.119.245.12	192.168.86.60	HTTP	492	HTTP/1.1 200 OK (text/html)

Frame 1359: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{9F22B204-A636-4207-9867-4DE0B9A70F3B}, id 0

Section number: 1

Interface id: 0 (\Device\NPF_{9F22B204-A636-4207-9867-4DE0B9A70F3B})

Interface name: \Device\NPF_{9F22B204-A636-4207-9867-4DE0B9A70F3B}

Interface description: Ethernet

Encapsulation type: Ethernet (1)

Arrival Time: Sep 18, 2023 20:33:13.450458000 Mountain Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1695090793.450458000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.096364000 seconds]

[Time since reference or first frame: 31.775342000 seconds]

Frame Number: 1359

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: Google_f3:81:73 (28:bd:89:f3:81:73), Dst: Micro-St_83:7c:a3 (2c:f0:5d:83:7c:a3)

Destination: Micro-St_83:7c:a3 (2c:f0:5d:83:7c:a3)

Address: Micro-St_83:7c:a3 (2c:f0:5d:83:7c:a3)

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

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

Source: Google_f3:81:73 (28:bd:89:f3:81:73)

Address: Google_f3:81:73 (28:bd:89:f3:81:73)

.... 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: 192.168.86.60

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: 0x1add (6877)

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: 45

Protocol: TCP (6)

Header Checksum: 0xa4d4 [validation disabled]

[Header checksum status: Unverified]

Source Address: 128.119.245.12

Destination Address: 192.168.86.60

Transmission Control Protocol, Src Port: 80, Dst Port: 53278, Seq: 1, Ack: 507, Len: 438

Source Port: 80

Destination Port: 53278

[Stream index: 25]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 438]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2728030336

[Next Sequence Number: 439 (relative sequence number)]

Acknowledgment Number: 507 (relative ack number)

Acknowledgment number (raw): 2646585425

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: 0x370c [unverified]

```
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
  [Time since first frame in this TCP stream: 0.182936000 seconds]
  [Time since previous frame in this TCP stream: 0.000000000 seconds]
[SEQ/ACK analysis]
  [iRTT: 0.086455000 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]
    [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: Tue, 19 Sep 2023 02:33:13 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: Mon, 18 Sep 2023 05:59:02 GMT\r\n
ETag: "51-6059bd6cfb860"\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 1/2]
[Time since request: 0.096364000 seconds]
[Request in frame: 1339]
[Next request in frame: 1364]
[Next response in frame: 1366]
[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
```