

No.	Time	Source	Destination	Protocol	Length	Info
	22 2018-10-07 14:37:00.007768	10.173.21.117	128.119.245.12	HTTP	482	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1

Frame 22: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 7, 2018 14:37:00.007768000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1538894220.007768000 seconds

[Time delta from previous captured frame: 0.000373000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 6.284242000 seconds]

Frame Number: 22

Frame Length: 482 bytes (3856 bits)

Capture Length: 482 bytes (3856 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoe:ppp:ip:tcp:http]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

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

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

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

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

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

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

0001 = Version: 1

.... 0001 = Type: 1

Code: Session Data (0x00)

Session ID: 0x88b3

Payload Length: 462

Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 10.173.21.117, 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: 460

Identification: 0x4343 (17219)

Flags: 0x4000, 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: 0x6043 [validation disabled]

[Header checksum status: Unverified]

Source: 10.173.21.117

Destination: 128.119.245.12

Transmission Control Protocol, Src Port: 1347, Dst Port: 80, Seq: 1, Ack: 1, Len: 420

Source Port: 1347

Destination Port: 80

[Stream index: 2]

[TCP Segment Len: 420]

Sequence number: 1 (relative sequence number)

[Next sequence number: 421 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

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 size value: 258
[Calculated window size: 66048]
[Window size scaling factor: 256]
Checksum: 0x8acf [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
  [iRTT: 0.379687000 seconds]
  [Bytes in flight: 420]
  [Bytes sent since last PSH flag: 420]
[Timestamps]
  [Time since first frame in this TCP stream: 0.380060000 seconds]
  [Time since previous frame in this TCP stream: 0.000373000 seconds]
TCP payload (420 bytes)
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
  [GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
  [Severity level: Chat]
  [Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file4.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2\r\n
Accept-Encoding: gzip, deflate\r\n
DNT: 1\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
[HTTP request 1/1]
[Response in frame: 28]
```