

```
No.      Time                Source                Destination          Protocol Length Info
505 2023-02-13 20:26:00.776688 10.162.31.137        128.119.245.12      HTTP                542      GET /wireshark-labs/protected_pages/HTTP-
wireshark-file5.html HTTP/1.1
Frame 505: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface \Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC}, id 0
Section number: 1
Interface id: 0 (\Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC})
Interface name: \Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC}
Interface description: Ethernet
Encapsulation type: Ethernet (1)
Arrival Time: Feb 13, 2023 20:26:00.776688000 Eastern Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1676337960.776688000 seconds
[Time delta from previous captured frame: 0.000358000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 6.080940000 seconds]
Frame Number: 505
Frame Length: 542 bytes (4336 bits)
Capture Length: 542 bytes (4336 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: Micro-St_06:51:9e (00:d8:61:06:51:9e), Dst: Routerbo_eb:56:c3 (08:55:31:eb:56:c3)
Destination: Routerbo_eb:56:c3 (08:55:31:eb:56:c3)
Address: Routerbo_eb:56:c3 (08:55:31:eb:56:c3)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0 .... = IG bit: Individual address (unicast)
Source: Micro-St_06:51:9e (00:d8:61:06:51:9e)
Address: Micro-St_06:51:9e (00:d8:61:06:51:9e)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.162.31.137, 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: 528
Identification: 0x6732 (26418)
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: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.162.31.137
Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 61547, Dst Port: 80, Seq: 1, Ack: 1, Len: 488
Source Port: 61547
Destination Port: 80
[Stream index: 22]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 488]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3677443687
[Next Sequence Number: 489 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3193535080
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: 1026
[Calculated window size: 262656]
[Window size scaling factor: 256]
Checksum: 0xa1b1 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.024807000 seconds]
[Time since previous frame in this TCP stream: 0.000358000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.024449000 seconds]
```

```
[Bytes in flight: 488]
[Bytes sent since last PSH flag: 488]
TCP payload (488 bytes)
Hypertext Transfer Protocol
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
[GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.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/109.0.0.0 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: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/1]
[Response in frame: 509]
No.      Time                               Source                               Destination                           Protocol Length Info
509 2023-02-13 20:26:00.801327      128.119.245.12                       10.162.31.137                         HTTP      771      HTTP/1.1 401 Unauthorized (text/html)
Frame 509: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC}, id 0
Section number: 1
Interface id: 0 (\Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC})
Interface name: \Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC}
Interface description: Ethernet
Encapsulation type: Ethernet (1)
Arrival Time: Feb 13, 2023 20:26:00.801327000 Eastern Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1676337960.801327000 seconds
[Time delta from previous captured frame: 0.000307000 seconds]
[Time delta from previous displayed frame: 0.024639000 seconds]
[Time since reference or first frame: 6.105579000 seconds]
Frame Number: 509
Frame Length: 771 bytes (6168 bits)
Capture Length: 771 bytes (6168 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: Routerbo_eb:56:c3 (08:55:31:eb:56:c3), Dst: Micro-St_06:51:9e (00:d8:61:06:51:9e)
Destination: Micro-St_06:51:9e (00:d8:61:06:51:9e)
Address: Micro-St_06:51:9e (00:d8:61:06:51:9e)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0. .... = IG bit: Individual address (unicast)
Source: Routerbo_eb:56:c3 (08:55:31:eb:56:c3)
Address: Routerbo_eb:56:c3 (08:55:31:eb:56:c3)
.... 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: 10.162.31.137
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: 757
Identification: 0xf0e5 (61669)
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: 48
Protocol: TCP (6)
Header Checksum: 0xb76e [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 10.162.31.137
Transmission Control Protocol, Src Port: 80, Dst Port: 61547, Seq: 1, Ack: 489, Len: 717
Source Port: 80
Destination Port: 61547
[Stream index: 22]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 717]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3193535080
[Next Sequence Number: 718 (relative sequence number)]
Acknowledgment Number: 489 (relative ack number)
Acknowledgment number (raw): 3677444175
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: 0x0cc3 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
  [Time since first frame in this TCP stream: 0.049446000 seconds]
  [Time since previous frame in this TCP stream: 0.000307000 seconds]
[SEQ/ACK analysis]
  [iRTT: 0.024449000 seconds]
  [Bytes in flight: 717]
  [Bytes sent since last PSH flag: 717]
TCP payload (717 bytes)
Hypertext Transfer Protocol
HTTP/1.1 401 Unauthorized\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
  [HTTP/1.1 401 Unauthorized\r\n]
  [Severity level: Chat]
  [Group: Sequence]
Response Version: HTTP/1.1
Status Code: 401
[Status Code Description: Unauthorized]
Response Phrase: Unauthorized
Date: Tue, 14 Feb 2023 01:26:00 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
WWW-Authenticate: Basic realm="wireshark-students only"\r\n
Content-Length: 381\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.024639000 seconds]
[Request in frame: 505]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
File Data: 381 bytes
Line-based text data: text/html (12 lines)
No.      Time                               Source                Destination            Protocol Length Info
 1834 2023-02-13 20:26:18.994612      10.162.31.137          128.119.245.12         HTTP      627      GET /wireshark-labs/protected_pages/HTTP-
wireshark-file5.html HTTP/1.1
Frame 1834: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface \Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC}, id 0
Section number: 1
Interface id: 0 (\Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC})
Interface name: \Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC}
Interface description: Ethernet
Encapsulation type: Ethernet (1)
Arrival Time: Feb 13, 2023 20:26:18.994612000 Eastern Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1676337978.994612000 seconds
[Time delta from previous captured frame: 0.000502000 seconds]
[Time delta from previous displayed frame: 18.193285000 seconds]
[Time since reference or first frame: 24.298864000 seconds]
Frame Number: 1834
Frame Length: 627 bytes (5016 bits)
Capture Length: 627 bytes (5016 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: Micro-St_06:51:9e (00:d8:61:06:51:9e), Dst: Routerbo_eb:56:c3 (08:55:31:eb:56:c3)
Destination: Routerbo_eb:56:c3 (08:55:31:eb:56:c3)
Address: Routerbo_eb:56:c3 (08:55:31:eb:56:c3)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ...0 .... = IG bit: Individual address (unicast)
Source: Micro-St_06:51:9e (00:d8:61:06:51:9e)
Address: Micro-St_06:51:9e (00:d8:61:06:51:9e)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ...0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.162.31.137, 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: 613
Identification: 0x6738 (26424)
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: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.162.31.137
Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 61548, Dst Port: 80, Seq: 1, Ack: 1, Len: 573
Source Port: 61548
Destination Port: 80
[Stream index: 23]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 573]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2965916994
[Next Sequence Number: 574 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1965266900
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: 1026
[Calculated window size: 262656]
[Window size scaling factor: 256]
Checksum: 0xa206 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 18.240093000 seconds]
[Time since previous frame in this TCP stream: 18.215606000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.024487000 seconds]
[Bytes in flight: 573]
[Bytes sent since last PSH flag: 573]
TCP payload (573 bytes)
Hypertext Transfer Protocol
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
[GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm0=\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/109.0.0.0 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: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/1]
[Response in frame: 1840]
No.      Time                               Source                Destination           Protocol Length Info
1840 2023-02-13 20:26:19.021997      128.119.245.12        10.162.31.137         HTTP      544      HTTP/1.1 200 OK (text/html)
Frame 1840: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface \Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC}, id 0
Section number: 1
Interface id: 0 (\Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC})
Interface name: \Device\NPF_{1DD7923C-13AB-467D-9439-E2A4D71AF3BC}
Interface description: Ethernet
Encapsulation type: Ethernet (1)
Arrival Time: Feb 13, 2023 20:26:19.021997000 Eastern Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1676337979.021997000 seconds

```

```
[Time delta from previous captured frame: 0.002826000 seconds]
[Time delta from previous displayed frame: 0.027385000 seconds]
[Time since reference or first frame: 24.326249000 seconds]
Frame Number: 1840
Frame Length: 544 bytes (4352 bits)
Capture Length: 544 bytes (4352 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: Routerbo_eb:56:c3 (08:55:31:eb:56:c3), Dst: Micro-St_06:51:9e (00:d8:61:06:51:9e)
Destination: Micro-St_06:51:9e (00:d8:61:06:51:9e)
Address: Micro-St_06:51:9e (00:d8:61:06:51:9e)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0 .... = IG bit: Individual address (unicast)
Source: Routerbo_eb:56:c3 (08:55:31:eb:56:c3)
Address: Routerbo_eb:56:c3 (08:55:31:eb:56:c3)
.... 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: 10.162.31.137
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: 530
Identification: 0x4663 (18019)
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: 49
Protocol: TCP (6)
Header Checksum: 0x61d4 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 10.162.31.137
Transmission Control Protocol, Src Port: 80, Dst Port: 61548, Seq: 1, Ack: 574, Len: 490
Source Port: 80
Destination Port: 61548
[Stream index: 23]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 490]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1965266900
[Next Sequence Number: 491 (relative sequence number)]
Acknowledgment Number: 574 (relative ack number)
Acknowledgment number (raw): 2965917567
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: 238
[Calculated window size: 30464]
[Window size scaling factor: 128]
Checksum: 0x9032 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 18.267478000 seconds]
[Time since previous frame in this TCP stream: 0.002826000 seconds]
[SEQ/ACK analysis]
[iRTT: 0.024487000 seconds]
[Bytes in flight: 490]
[Bytes sent since last PSH flag: 490]
TCP payload (490 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, 14 Feb 2023 01:26:18 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, 13 Feb 2023 06:59:02 GMT\r\n
ETag: "84-5f48f61cf4901"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 132\r\n
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 1/1]
[Time since request: 0.027385000 seconds]
[Request in frame: 1834]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
File Data: 132 bytes
Line-based text data: text/html (6 lines)
```