```
No.     Time            Source                Destination           Protocol Length Info
    177 1.821132        114.214.227.222       128.119.245.12        HTTP      545    GET /wireshark-labs/protected_pages/HTTP-
wireshark-file5.html HTTP/1.1
Frame 177: 545 bytes on wire (4360 bits), 545 bytes captured (4360 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.227.222, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 531
    Identification: 0x9f85 (40837)
    Flags: 0x40, Don't fragment
    ...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: 114.214.227.222
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 50363, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
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]
        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/94.0.4606.71 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: zh-CN,zh;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: 201]
No.     Time            Source                Destination           Protocol Length Info
    201 2.080870        128.119.245.12        114.214.227.222       HTTP      771    HTTP/1.1 401 Unauthorized  (text/html)
Frame 201: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.227.222
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 757
    Identification: 0x701d (28701)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 32
    Protocol: TCP (6)
    Header Checksum: 0x1bad [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 114.214.227.222
Transmission Control Protocol, Src Port: 80, Dst Port: 50363, Seq: 1, Ack: 492, Len: 717
Hypertext Transfer Protocol
    HTTP/1.1 401 Unauthorized\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
        Response Version: HTTP/1.1
        Status Code: 401
        [Status Code Description: Unauthorized]
        Response Phrase: Unauthorized
    Date: Fri, 16 Sep 2022 14:14:28 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 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
        [Content length: 381]
    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: 0.259738000 seconds]
    [Request in frame: 177]
    [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)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>401 Unauthorized</title>\n
    </head><body>\n
    <h1>Unauthorized</h1>\n
    <p>This server could not verify that you\n
    are authorized to access the document\n
    requested.  Either you supplied the wrong\n
    credentials (e.g., bad password), or your\n
    browser doesn't understand how to supply\n
    the credentials required.</p>\n
    </body></html>\n
No.     Time            Source                Destination          Protocol Length Info
    901 10.591197      114.214.227.222       128.119.245.12       HTTP     630    GET /wireshark-labs/protected_pages/HTTP-
wireshark-file5.html HTTP/1.1
Frame 901: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.227.222, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 616
    Identification: 0x9f8b (40843)
    Flags: 0x40, Don't fragment
    ...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: 114.214.227.222
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 51964, Dst Port: 80, Seq: 1, Ack: 1, Len: 576
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]
        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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\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/94.0.4606.71 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: zh-CN,zh;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 1/2]
    [Response in frame: 945]
    [Next request in frame: 947]
No.     Time            Source                Destination          Protocol Length Info
    945 10.866822      128.119.245.12        114.214.227.222      HTTP     544    HTTP/1.1 200 OK  (text/html)
Frame 945: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.227.222
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 530
    Identification: 0x89c2 (35266)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 33
    Protocol: TCP (6)
    Header Checksum: 0x01eb [validation disabled]
    [Header checksum status: Unverified]
```

Source Address: 128.119.245.12
        Destination Address: 114.214.227.222
Transmission Control Protocol, Src Port: 80, Dst Port: 51964, Seq: 1, Ack: 577, Len: 490
Hypertext Transfer Protocol
        HTTP/1.1 200 OK\r\n
                [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
                Response Version: HTTP/1.1
                Status Code: 200
                [Status Code Description: OK]
                Response Phrase: OK
        Date: Fri, 16 Sep 2022 14:14:36 GMT\r\n
        Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
        Last-Modified: Fri, 16 Sep 2022 05:59:02 GMT\r\n
        ETag: "84-5e8c50f0c2df2"\r\n
        Accept-Ranges: bytes\r\n
        Content-Length: 132\r\n
                [Content length: 132]
        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: 0.275625000 seconds]
        [Request in frame: 901]
        [Next request in frame: 947]
        [Next response in frame: 964]
        [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)
        \n
        <html>\n
        \n
        This page is password protected! If you're seeing this, you've downloaded the page correctly
\n
        Congratulations!\n
        </html>