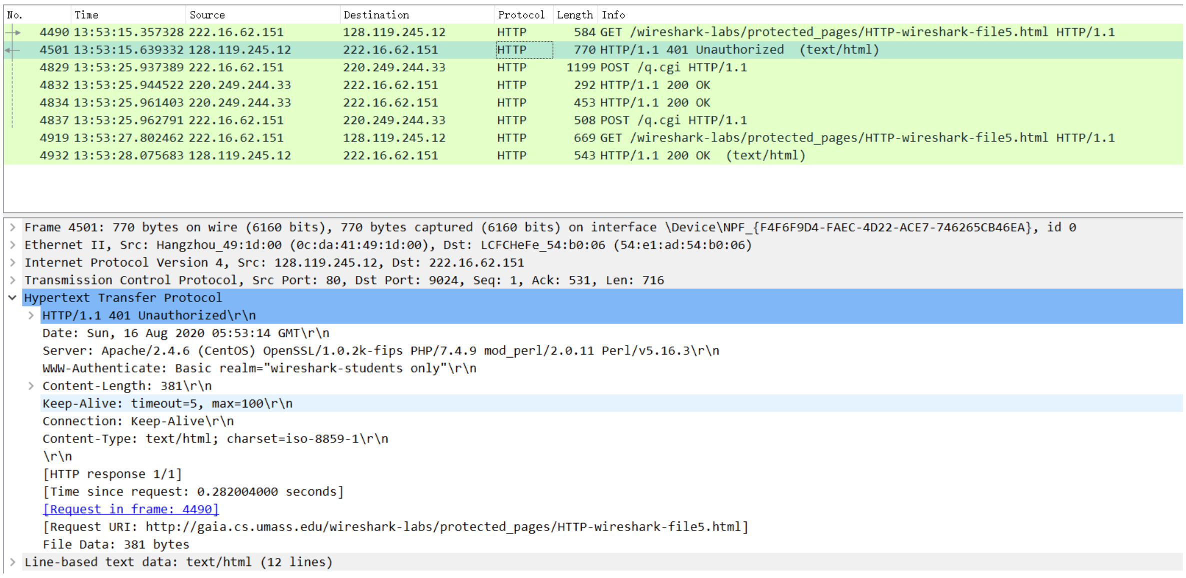
5. HTTP Authentication

Answer the following questions:

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

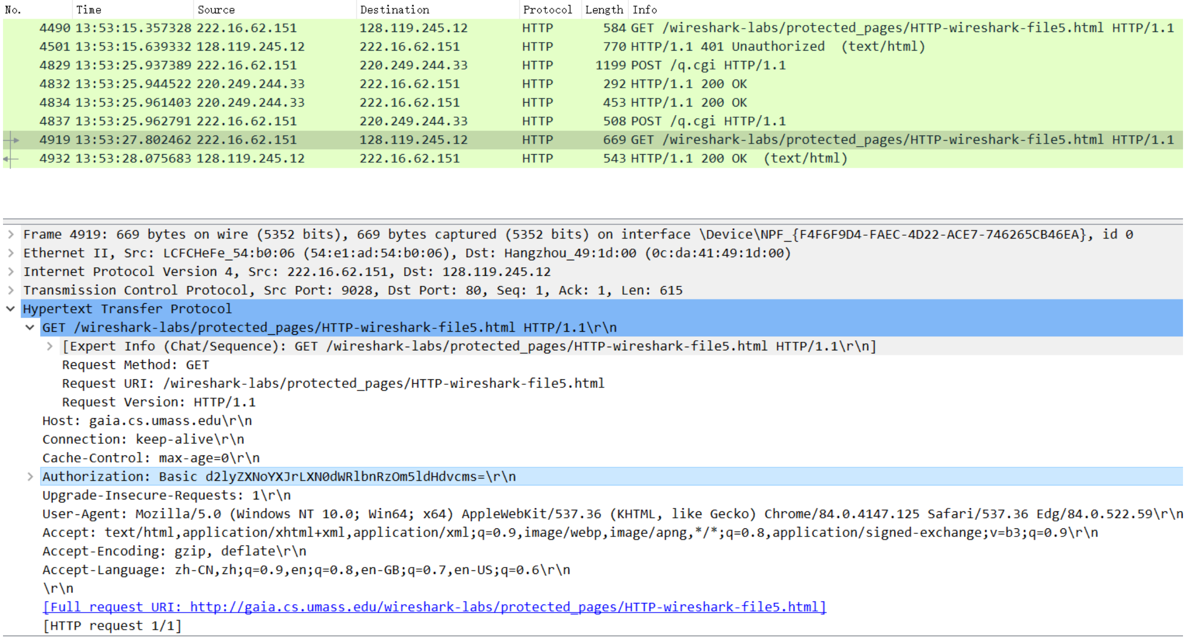
18. **Answer: First response's status code is 401 Unauthorized**



```
No.     Time            Source          Destination     Protocol Length Info
4490 13:53:15.357328 222.16.62.151    128.119.245.12    HTTP      584 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
4501 13:53:15.639332 128.119.245.12   222.16.62.151     HTTP      770 HTTP/1.1 401 Unauthorized  (text/html)
4829 13:53:25.937389 222.16.62.151    220.249.244.33    HTTP     1199 POST /q.cgi HTTP/1.1
4832 13:53:25.944522 220.249.244.33   222.16.62.151     HTTP      292 HTTP/1.1 200 OK
4834 13:53:25.961403 220.249.244.33   222.16.62.151     HTTP      453 HTTP/1.1 200 OK
4837 13:53:25.962791 222.16.62.151    220.249.244.33    HTTP      508 POST /q.cgi HTTP/1.1
4919 13:53:27.802462 222.16.62.151    128.119.245.12    HTTP      669 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
4932 13:53:28.075683 128.119.245.12   222.16.62.151     HTTP      543 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 4501: 770 bytes on wire (6160 bits), 770 bytes captured (6160 bits) on interface \Device\NPF_{F4F6F9D4-FAEC-4D22-ACE7-746265CB46EA}, id 0
> Ethernet II, Src: Hangzhou_49:1d:00 (0c:da:41:49:1d:00), Dst: LCFCHeFe_54:b0:06 (54:e1:ad:54:b0:06)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 222.16.62.151
> Transmission Control Protocol, Src Port: 80, Dst Port: 9024, Seq: 1, Ack: 531, Len: 716
v Hypertext Transfer Protocol
  > HTTP/1.1 401 Unauthorized\r\n
    Date: Sun, 16 Aug 2020 05:53:14 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9 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: 0.282004000 seconds]
    [Request in frame: 4490]
    [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)
```

19. **Answer: There is an Authorization in HTTP GET message**



```
No.     Time            Source          Destination     Protocol Length Info
4490 13:53:15.357328 222.16.62.151    128.119.245.12    HTTP      584 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
4501 13:53:15.639332 128.119.245.12   222.16.62.151     HTTP      770 HTTP/1.1 401 Unauthorized  (text/html)
4829 13:53:25.937389 222.16.62.151    220.249.244.33    HTTP     1199 POST /q.cgi HTTP/1.1
4832 13:53:25.944522 220.249.244.33   222.16.62.151     HTTP      292 HTTP/1.1 200 OK
4834 13:53:25.961403 220.249.244.33   222.16.62.151     HTTP      453 HTTP/1.1 200 OK
4837 13:53:25.962791 222.16.62.151    220.249.244.33    HTTP      508 POST /q.cgi HTTP/1.1
4919 13:53:27.802462 222.16.62.151    128.119.245.12    HTTP      669 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
4932 13:53:28.075683 128.119.245.12   222.16.62.151     HTTP      543 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 4919: 669 bytes on wire (5352 bits), 669 bytes captured (5352 bits) on interface \Device\NPF_{F4F6F9D4-FAEC-4D22-ACE7-746265CB46EA}, id 0
> Ethernet II, Src: LCFCHeFe_54:b0:06 (54:e1:ad:54:b0:06), Dst: Hangzhou_49:1d:00 (0c:da:41:49:1d:00)
> Internet Protocol Version 4, Src: 222.16.62.151, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 9028, Dst Port: 80, Seq: 1, Ack: 1, Len: 615
v Hypertext Transfer Protocol
  v 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/84.0.4147.125 Safari/537.36 Edg/84.0.522.59\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
```

Conclusion:

The username (wireshark-students) and password (network) that you entered are encoded in the string of characters (d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=) following the “Authorization: Basic” header in the client’s HTTP GET message.