21BCE7371
RADHA KRISHNA GARG

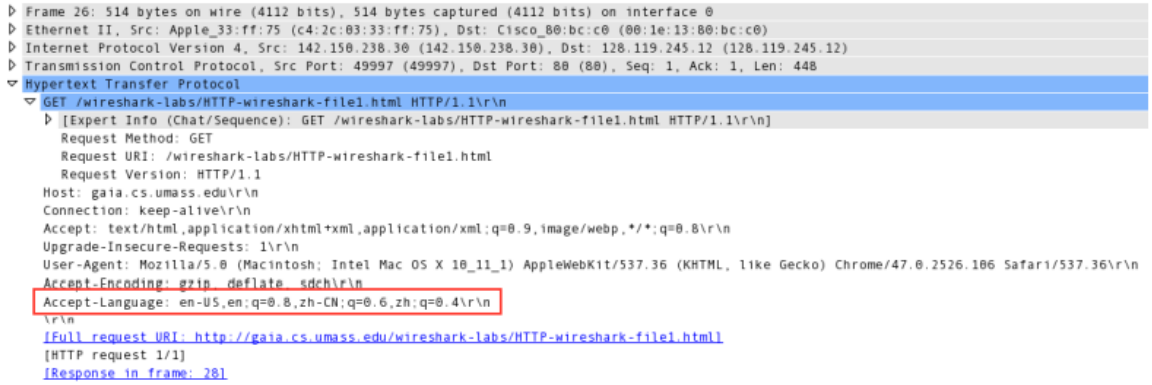
CN LAB ASSIGNMENT-11

ANS-2

Solution:

en-US and zh-CN

(languages information is listed in the item ‘Accept-Language’ in the HTTP GET
message)

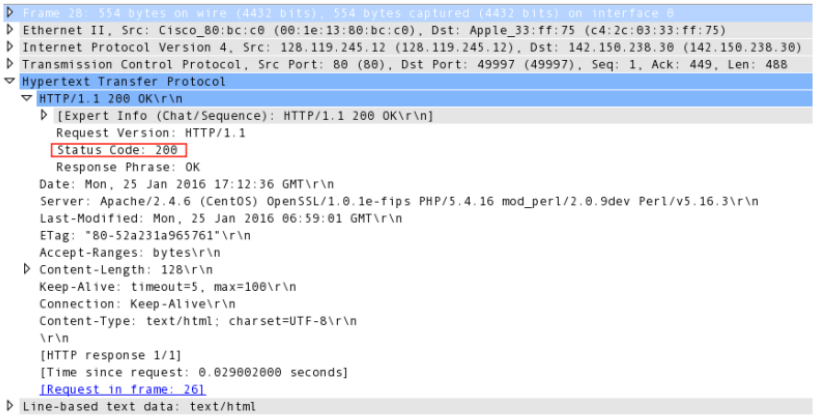


ANS-4

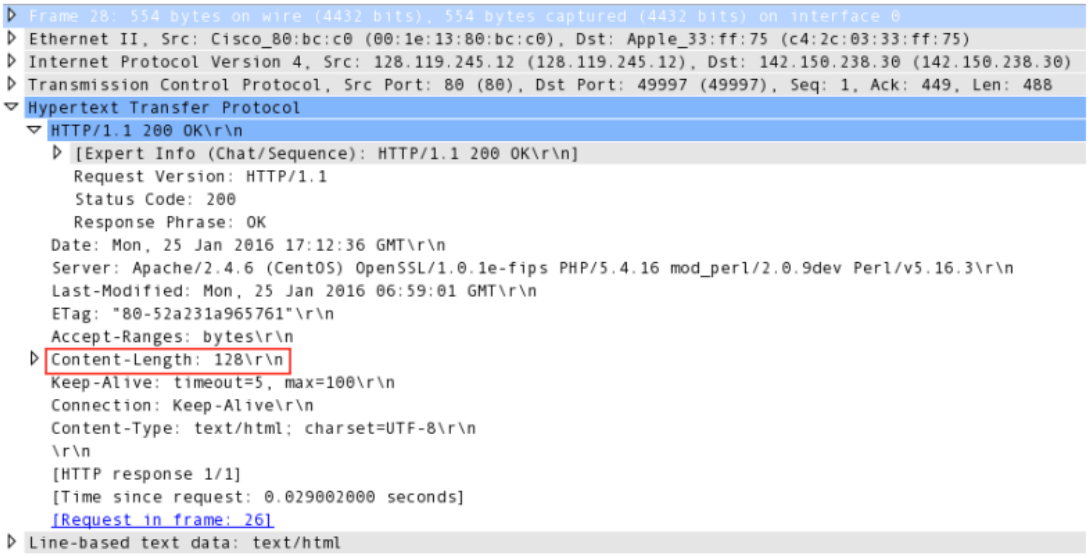
Solution:

status code:200

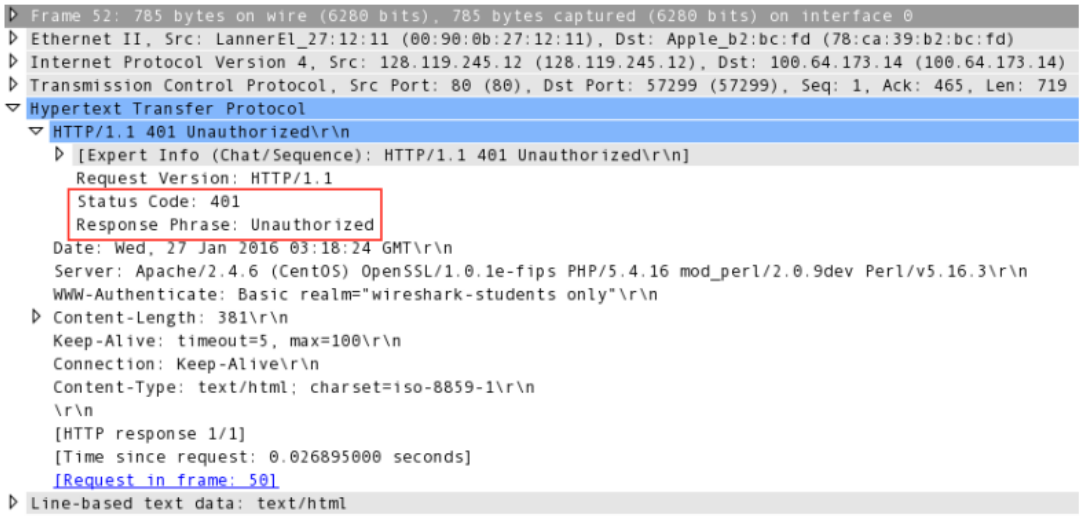
(status code information is listed in the HTTP OK message)



ANS-6
Solution:
Content length: 128
(Content length information is listed in the item ‘Content-Length’ in the HTTP OK
message)



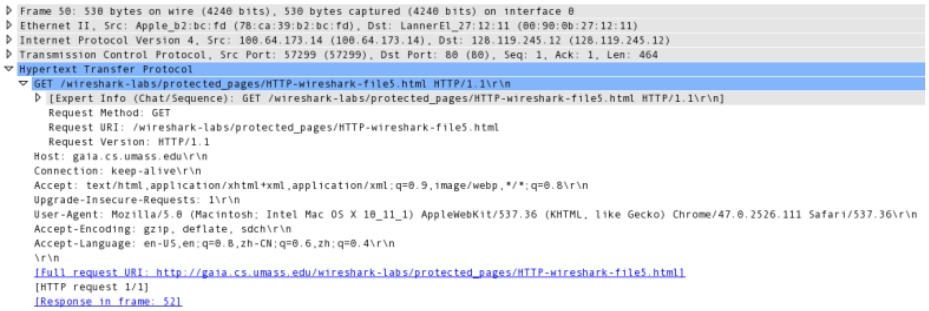
ANS-7
Solution:
We got a response that said ‘HTTP/1.1 401 Unauthorized’.
Status code: 401
Response phrase: Unauthorized



ANS-8

Solution:

The screenshot of first HTTP GET message:



The screenshot of second HTTP GET message:

Comparing these two HTTP GET messages, it is easy to find that the second HTTP GET message contains the ‘Authorization’ field. 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. While it may appear that your username and password are encrypted, they are simply encoded in a format known as Base64 format. The username and password are not encrypted! To see this, go to **http://www.motobit.com/util/base64-decoder-encoder.asp** and enter the base64- encoded string d2lyZXNoYXJrLXN0dWRlbnRz and decode. Voila! You have translated from Base64 encoding to ASCII encoding, and thus should see your username! To view the password, enter the remainder of the string Om5ldHdvcms= and press decode. Since anyone can download a tool like Wireshark and sniff packets (not just their own) passing by their network adaptor, and anyone can translate from Base64 to ASCII (you just did it!), it should be clear to you that simple passwords on WWW sites are not secure unless additional measures are taken.