**CS 6043: Computer Networking**

**SPRING 2016**

**PROJECT 1**

**Given: Jan. 17, 2016**

**Due: Feb. 12 (Friday), 2016 (NO LATER THAN 11:59PM)**

**Submission Instructions:**

1. Submit only on-line files on Blackboard before midnight. No hard copy will be accepted.

2. For students who are working in a team, *one* submission for the team is sufficient.

3. Wireshark files for this project can be found in the zip file “Project\_1\_Wireshark\_Traces.zip”.

**Part I: HTTP**

1. Load the file ‘http-ethereal-trace-1’ in Wireshark and answer the following questions. The traces were collected when a simple and very short HTML file was downloaded.
2. What version of HTTP is being run by your browser and the server?

Answer: HTTP 1.1

1. What is the status code returned from the server to your browser? What is its significance?

Answer: Status displayed is 1.1 200 OK

1. Load the file ‘http-ethereal-trace-2’ in Wireshark and answer the following questions. The traces were collected when a particular web page is accessed twice from the browser within a short interval.
2. Inspect the contents of the first server response. Did the server explicitly return the contents of the file? If so, what was returned?

Answer: Yes. It returned the contents of the file. It displayed ‘Congratulations again! Now you've downloaded the file lab2-2.html.’

1. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Answer: The message received was ‘304 Not Modified’. It did not receive the contents of the file and the document hasn’t been modified. Hence the status.

1. Load the file ‘http-ethereal-trace-3’ in Wireshark and answer the following question.

The traces were collected when a HTML document with embedded objects (images in this case) were accessed via the web browser. The HTML file contains the URLs of the images, not the images themselves. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

Answer: They are in series because the first image was requested and sent before the second.

1. Enter the following URL into your browser and type the requested user name and password into the pop up box.

<http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html>

The username is “wireshark-students”, and the password is “network” (without the quotes).

1. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

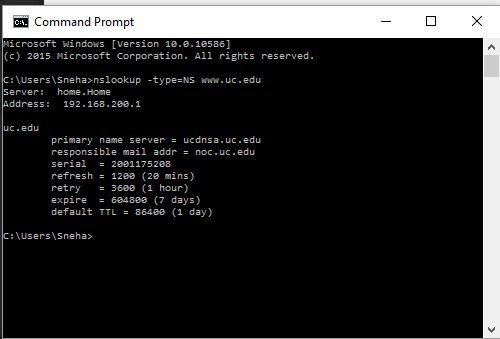
Answer: http /1.1 401 Unauthorized

1. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

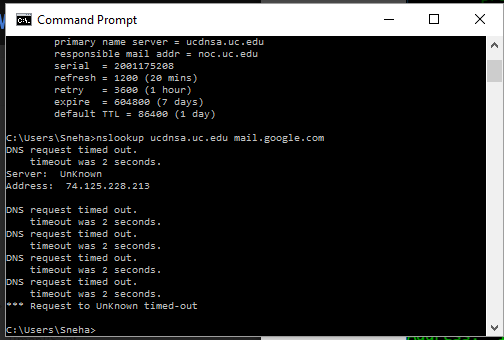
Answer: Authorization:basic is the new field added.

**Part II: DNS**

1. Run *nslookup* to determine the authoritative DNS servers for University of Cincinnati. Please include screenshot in your answer.



1. Run *nslookup* so that the DNS servers obtained in Question 1 is queried for the mail servers for Gmail. What is its IP address? Please include screenshot in your answer.



1. Load the file ‘dns-ethereal -trace-1’ in Wireshark and answer the following questions.
2. Locate the DNS query and response messages. Are they sent over UDP or TCP? What is the destination port for the DNS query message and the source port of DNS response message?

Answer: The messages are sent over UDP. Source port is 3163 and destination port is 53.

1. Examine the DNS query message. What “Type” of DNS query is it?

Answer: This query was type A.

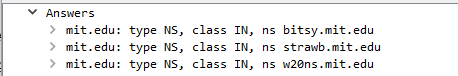
1. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

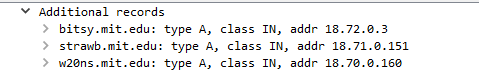
Answer: It provided two answers, which contained IP addresses

1. Load the file ‘dns-ethereal -trace-3’ in Wireshark and answer the following questions.
2. Examine the last (no. 493) DNS response message. What MIT nameservers does the response message provide?

Answer:

mit.edu, bitsy.mit.edu, strawb.mit.edu, w20ns.mit.edu





1. Does this response message also provide the IP addresses of the MIT nameservers? If yes, what are they?

Answer:

Yes.

18.72.0.3, 18.71.0.151 and 18.70.0.160