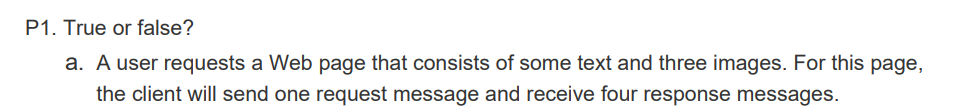
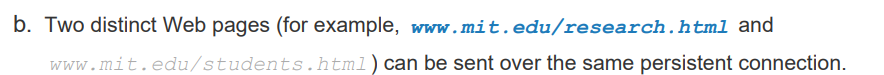
Text

Description automatically generated



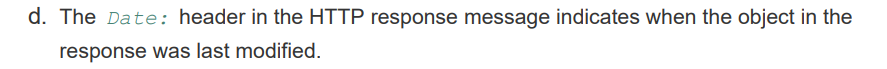
False



True



False

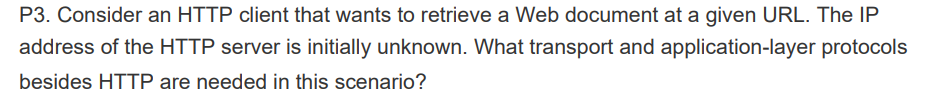


False



False





DNS will be needed since we don’t have the URL cached on the local host. So, a DNS request is sent to obtain the host name. for mapping. Now, DNS runs over UDP. With the mapping done the HTTP client makes a TCP connection with the server. After establishing this connection, the request for the website is sent over the connection.



Text

Description automatically generated with medium confidence

Diagram

Description automatically generated

Text, letter

Description automatically generated



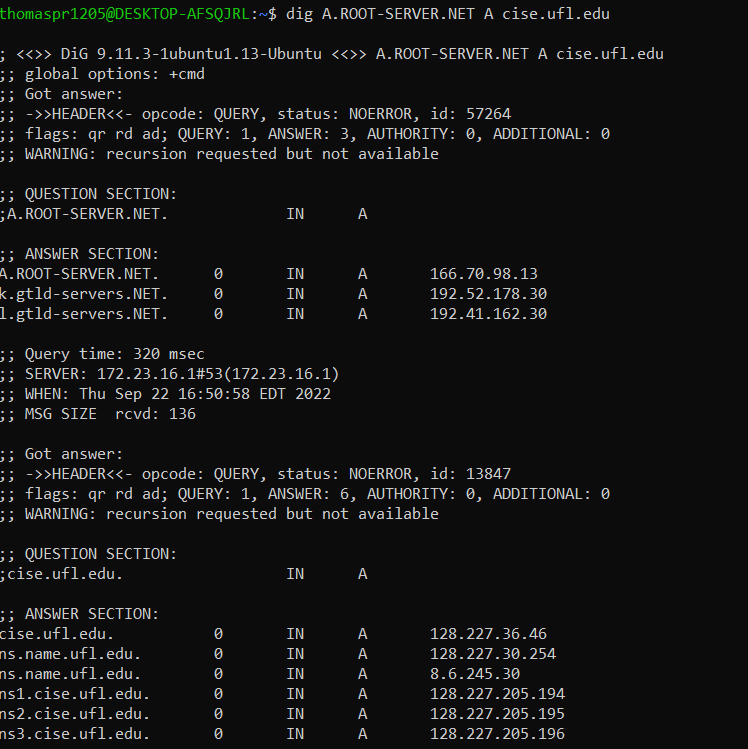
Text

Description automatically generated

Diagram

Description automatically generated

a)



b)

Text

Description automatically generatedText

Description automatically generated

Wireshark Lab (35 points)

**HTTP**

**1. The Basic HTTP GET/response interaction**

Graphical user interface, text, application, email

Description automatically generated

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the   
   server running?

Both my browser and the server area running 1.1

1. What languages (if any) does your browser indicate that it can accept to the   
   server?

Spanish and English from the server

1. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Computer: 192.168.1.112

gaia.cs.umass.edu.server: 128.119.245.12

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

200 OK

1. When was the HTML file that you are retrieving last modified at the server?

Graphical user interface, application, Word

Description automatically generated

1. How many bytes of content are being returned to your browser?   
   128
2. By inspecting the raw data in the packet content window, do you see any headers   
   within the data that are not displayed in the packet-listing window? If so, name   
   one.

I don’t see any differences

**2. The HTTP CONDITIONAL GET/response interaction**  
Graphical user interface, text, application, email

Description automatically generated

8. Inspect the contents of the first HTTP GET request from your browser to the   
server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

There is no “IF-MODIFIED-Since”

9. Inspect the contents of the server response. Did the server explicitly return the   
contents of the file? How can you tell?

Graphical user interface, text, application

Description automatically generated

10. Now inspect the contents of the second HTTP GET request from your browser to   
the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If   
so, what information follows the “IF-MODIFIED-SINCE:” header?

Graphical user interface, text, application

Description automatically generated

If there is a modification then a new connection is established, if not used the previous frame

11. 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.

Graphical user interface, text, application

Description automatically generated

Code: 304 not modified

The server didn’t explicitly return the contents of the file

**3. Retrieving Long Documents**

**Graphical user interface, text, application, Word

Description automatically generated**

12. How many HTTP GET request messages did your browser send? Which packet   
number in the trace contains the GET message for the Bill or Rights?

GET requests: 1

Packet number: 538

13. Which packet number in the trace contains the status code and phrase associated   
with the response to the HTTP GET request?

Packet number: 557

14. What is the status code and phrase in the response?

Status code: 200 OK  
15. How many data-containing TCP segments were needed to carry the single HTTP   
response and the text of the Bill of Rights?

Graphical user interface, application, Word

Description automatically generated

TCP segments: 4

**4. HTML Documents with Embedded Objects**

Graphical user interface, application

Description automatically generated

16. How many HTTP GET request messages did your browser send? To which   
Internet addresses were these GET requests sent?

GET Request: 3

Wireshark-labs/HTTP-wireshark-file4.html

Pearson.png

8E\_cover\_small.png

17. Can you tell whether your browser downloaded the two images serially, or   
whether they were downloaded from the two web sites in parallel? Explain.

The browser downloaded the images serially. The GET requests are in different packets, but before the second GET request is sent, the response from the first GET is received. If they were running in parallel, both files would have been requested, before getting a response.

**5 HTTP Authentication**

**Graphical user interface, text, application

Description automatically generated**

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

Status Code: 401 Unauthorized

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

Graphical user interface, text, application, email

Description automatically generated

The new field is the authorization field. This is due to the fact we include the username and password with the request.

**DNS**

1. **Nslookup**

Run nslookup to obtain the IP address of a Web server in Asia. What is the IP   
address of that server?

Text

Description automatically generated

Ip address: 58.229.6.225

2. Run nslookup to determine the authoritative DNS servers for a university in   
Europe.

Graphical user interface, text

Description automatically generated

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for   
the mail servers for Yahoo! mail. What is its IP address?

Text

Description automatically generated

1. **Ipconfig**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

1. **Tracing DNS with Wireshark**
2. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Graphical user interface, application

Description automatically generated

They are sent over UDP

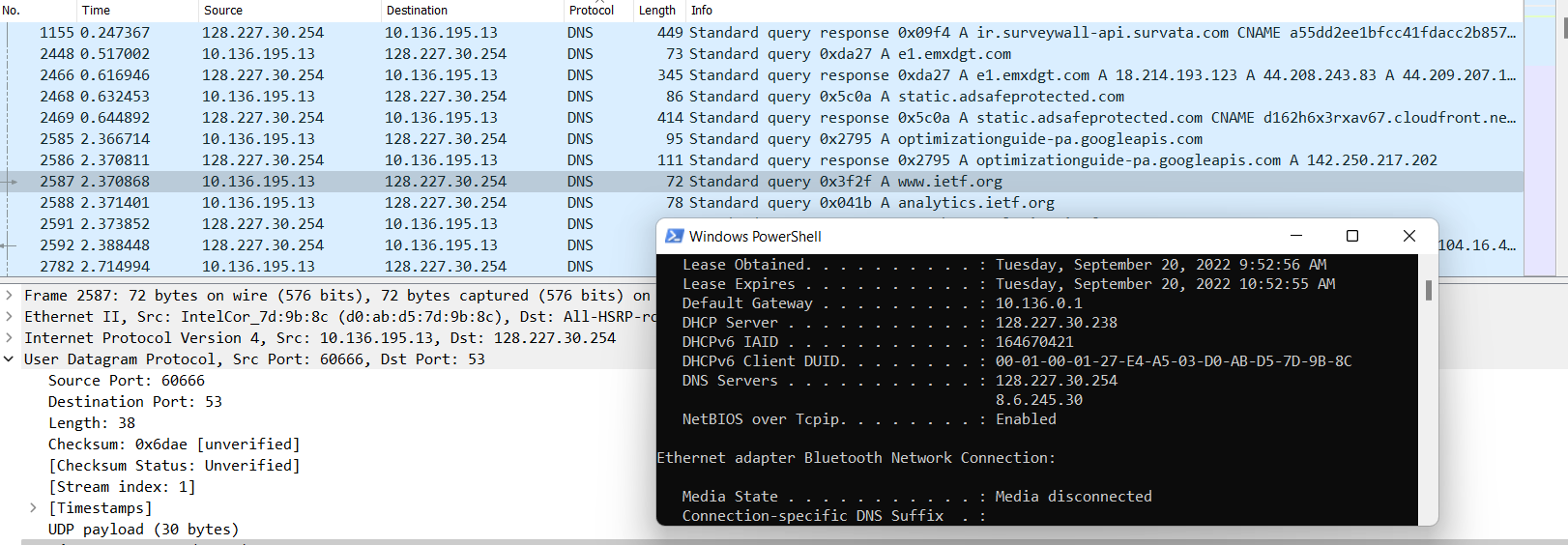
1. What is the destination port for the DNS query message? What is the source port   
   of DNS response message?   
   Graphical user interface, application

   Description automatically generated

Destination port: 53

Source port: 60666

1. To what IP address is the DNS query message sent? Use ipconfig to determine the   
   IP address of your local DNS server. Are these two IP addresses the same?



They are the same

1. Examine the DNS query message. What “Type” of DNS query is it? Does the   
   query message contain any “answers”?

Graphical user interface, application, Word

Description automatically generated

It is Type A, it does not contain any answers

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

Graphical user interface, application

Description automatically generated

There are 3 answers, containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.

Consider the subsequent TCP SYN packet sent by your host. Does the destination   
IP address of the SYN packet correspond to any of the IP addresses provided in   
the DNS response message?

Application

Description automatically generated with medium confidence

Yes, the destination address corresponds to the address provided in DNS response message (Address: 104.16.44.99)

10. This web page contains images. Before retrieving each image, does your host   
issue new DNS queries?

No, I didn’t find any new DNS queries to retrieve images

1. What is the destination port for the DNS query message? What is the source port   
   of DNS response message?

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

12. To what IP address is the DNS query message sent? Is this the IP address of your   
default local DNS server?

Graphical user interface, application

Description automatically generated

Text

Description automatically generated

It is sent to the local DNS server

1. Examine the DNS query message. What “Type” of DNS query is it? Does the   
   query message contain any “answers”?

Graphical user interface, text, application

Description automatically generated

It is type A and does not contain any answers

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

Graphical user interface, text, application, email

Description automatically generated

There are two answers provided, containing name of the host, the type of address, the class, and the IP address

15. Provide a screenshot.

Text

Description automatically generated

16. To what IP address is the DNS query message sent? Is this the IP address of your   
default local DNS server?

Graphical user interface, text, application

Description automatically generated

It was sent to my default DNS server  
17. Examine the DNS query message. What “Type” of DNS query is it? Does the   
query message contain any “answers”?

It’s a type NS query that contains one question and it doesn’t contain any answers.

18. Examine the DNS response message. What MIT nameservers does the response   
message provide? Does this response message also provide the IP addresses of the   
MIT nameservers?

Graphical user interface, text

Description automatically generated  
19. Provide a screenshot

See question above

20. To what IP address is the DNS query message sent? Is this the IP address of your   
default local DNS server? If not, what does the IP address correspond to?

Graphical user interface, application, Word

Description automatically generated

The query is sent to the MIT bitsy server

21. Examine the DNS query message. What “Type” of DNS query is it? Does the   
query message contain any “answers”?

Graphical user interface, application, Word

Description automatically generated

Type A, no answers, one question  
22. Examine the DNS response message. How many “answers” are provided? What   
does each of these answers contain?

Graphical user interface, text, application, email

Description automatically generated

There is only one answer, it contains, name, type, class, time to live, data length, and address

23. Provide a screenshot.

See question above