Task 1

Question 1

A. What is your IP address, and

194.47.41.238

B. what is the corresponding MAC address?

60:dd:8e:b6:62:c8

C. How do you find them?

You find the ip adress in source column and the mac address in Ethernet II layer

Question 2

A. What is the port number for your browser to access the home page?

Port 80

B. What is the remote http server port number?

Port 54171

C. In which layer header does port numbers appear?

Layer 4

D. What are these port numbers used for?

To identify a particular application in a server.

Question 3

A. which transport layer protocol (UDP or TCP) was used to transport this GET message?

We used TCP.

B. the transport layer protocol data unit was encapsulated in an IP packet. Check the source and destination IP addresses in IP header. Is the source IP address your computer IP address?

Yes, it is.

C. the IP packet is encapsulated in a hardware frame. check the frame header, you can find the source MAC address and destination MAC address. Is the destination MAC address corresponding to the MAC address of remote web server? why and why not?

No, the destination MAC address in the frame header is not the MAC address of the remote web server. It's the MAC address of the next device within your local network that helps route the data toward its destination. The destination MAC address changes as data travels through different devices on its path to the remote server.

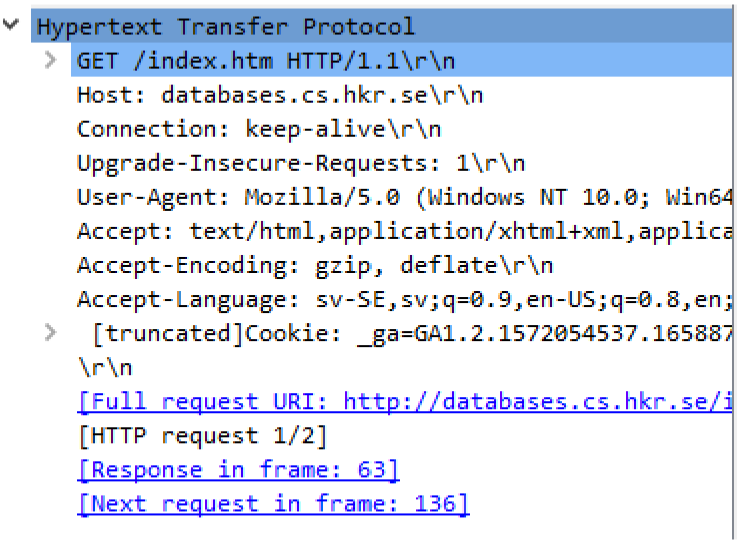
D. find or calculate the HTTP message size (length), TCP segment size(length), IP packet size and frame size.

HTTP message size:490 total length in Ip packet – 20 header size of ip packet – 20 header size of TCP segment = 450 size of http message, TCP segment size: 470, IP packet size: 490, frame size: 504

Question 4

A. How many header lines are there in this HTTP request message?

8 headers



```
Hypertext Transfer Protocol
  GET /index.htm HTTP/1.1\r\n
  Host: databases.cs.hkr.se\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64
  Accept: text/html,application/xhtml+xml,applica
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: sv-SE,sv;q=0.9,en-US;q=0.8,en;
   [truncated]Cookie: _ga=GA1.2.1572054537.165887
  \r\n
  [Full request URI: http://databases.cs.hkr.se/i
  [HTTP request 1/2]
  [Response in frame: 63]
  [Next request in frame: 136]
```

B. Does this http message contain any file data?

No, it does not contain any file data since the request is a GET request.

Question 5

A. Is your browser running HTTP version 1.0 or 1.1?

My browser runs HTTP1.1

B. What version of HTTP is the server running?

HTTP 1.1 is running on the server.

Question6

What languages does your browser indicate that it can accept to the server?

sv-SE,sv;q=0.9,en-US;q=0.8,en;q=0.7,ar;q=0.6, Swedish, English, and Arabic

Question 7

Does this HTTP request message contain payload data? How do you know?

No, it does not since there is no content-length variable in the HTTP layer and no data to show

Question 8

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

    200

B. What does the code mean?

The status code returned by the server indicates the outcome of the HTTP request. 200 status code means request was successful, and the server has returned the requested resource.

Question 9

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

    Mon, 18 ape 2016

B. Why does the server indicate the last modified date stamp?

helps optimize web performance, reduce server load, and improve user experiences by enabling efficient caching and resource management.

Question 10

A. How long in bytes is the payload data in this HTTP message?

    371 bytes zipped, 638 unzipped

B. How big in bytes is the requested home page?

    638 bytes

C. Do you find the "content-encoding: " header line? what is this line used for?

The "Content-Encoding" header is an HTTP response header that indicates how the content of the response has been encoded or compressed before it was sent by the server. This header informs the client about the encoding applied to the response body so that the client can properly decode and display or process the content. gzip: Indicates that the content has been compressed using the gzip compression algorithm.

Question 11

A. By inspecting the raw data in the packet content window, do you see any other information in HTTP header that are not displayed in the packet-listing window? If so, name one.

   The information that are in [], [Time since request:]

B. In both plain text and binary

Question 12

What is the file favicon.ico?

The "favicon.ico" file is typically a small image file that represents a website's icon. It is displayed in the browser's address bar, bookmarks, tabs, and other places to help users identify the website. This file is often referred to as a "favicon."

Question 13

How long in bytes for this http response message and how do you find it out?

1150 bytes, you find the size by looking at content-length line in the HTTTP header of the response of the favicon request.

Task 2

Question 14

A. Which frame (packet) number contains the HTTP GET command to download the file sunrise.gif?

   Frame 3

B. Inspect the contents of this HTTP GET request. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

   NO

Question 15 Inspect the contents of the server response to this GET command:

A. How big in bytes is this HTTP response message (the whole message = http header + payload)?

   1193 Bytes

B. How big is the file (image) in bytes (the actual file size)?

   1193 Bytes

C. How many bytes does this HTTP message header contain (only the header of http message)?

192 Bytes

Question 16

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

Yes, the value: If-Modified-Since: Fri, 19 Mar 2021 17:47:14 GMT

Question 17

A. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET image?

   304 not modified

B. How big in bytes is the HTTP response message?

   Not defined, no content-length or File data variables in the http layer

C. Did this response contain the file data?

   NO

D. Compare the sizes of the HTTP responses to the first and second GET sunrise.gif commands.

First GET response: 317051 bytes

Second GET response: No size defined

Question 18

The response time is the time duration from a request is sent and until a response to the request is received. What are response times for downloading the image with first and second HTTP GET image commands?

First GET: 0.20728800 sec

Second GET: 0.019241000 sec

Question 19

Write a reflection on how HTTP protocol with IF-MODIFIED-SINCE:” header enables the caching in a web browser. Discuss why the browser do not cache small objects.

The "IF-MODIFIED-SINCE" header in the HTTP protocol helps browsers save time by storing web page information. When you revisit a page, it checks if it has changed since your last visit. If not, the browser uses the saved data.

But, for very small items, like tiny images or icons, it's not worth the effort to save and check them in the cache. It's like trying to save a penny when it costs more to keep track of it than it's worth. So, browsers usually don't bother caching such small stuff.

Question 20

Write a reflection on how HTTP client(browser) and HTTP server (web server) interact via HTTP messages, and how the header lines in http messages are used to inform each other about the information carried in the messages. A good understanding about this would help to design your own application protocols in the future work.

HTTP clients, like web browsers, and HTTP servers, such as web servers, talk to each other using HTTP messages. These messages are like a digital chat, and the header lines in them are like short descriptions that tell what's inside.

Task 3

Question 21

A. Does HTTP send the password in plain text?

   Plain Text

B. When you visit a web site that uses HTTP protocol, should you enter your username and password if you are asked?

   No, because the data is not encrypted when it’s sent to the server.

Provide reflection on the captured data and observed results.

The captured data shows important things about how computers talk to each other on a network:

Addresses: Devices on a network have special numbers (IP and MAC addresses) that help them find each other.

Port Numbers: These are like door numbers for different services on devices.

Protocols: TCP makes sure data gets to its destination safely.

HTTP Headers: They contain extra info, like language preferences and how data is compressed.

Status Codes: "200" means everything went well when asking for a webpage.

Caching: Servers use dates to make websites load faster.

Security: Don't type in passwords on unsecured websites (HTTP).

Knowing these things helps make the internet work better and keeps your data safe.