Name: CHAN, Chun Hin

Student ID: 20853893

Email: chchanec@connect.ust.hk

Wireshark Lab: HTTP

*Part 2:*

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

A screenshot of a computer

Description automatically generated

Yes, the server explicitly return the contents of the file. It is because the status code I received is 200, and its corresponding status code description and phrase returned is “OK”. Also, I received a content length of 371 and a file data of 371 bytes, which implies the server is explicitly returning the contents of the html file.

**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.**

A screenshot of a computer

Description automatically generated

The HTTP status code returned from the server in response to the second HTTP GET is 304.

The phrase returned from the server in response to the second HTTP GET is “Not Modified”.

The server did not explicitly return the contents of the file, because based on the returned status code 304 and the corresponding phrase “Not Modified”, if the server knows that this website has not been modified, it will just returned the cached version of the same website to us instead.

*Part 4:*

**16. How many HTTP GET request messages did your browser send? To which**

**Internet addresses were these GET requests sent?**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

My browser sent 3 HTTP GET messages.

The first GET request is sent to the Internet address 128.119.245.12.

The second GET request is sent to the Internet address 128.119.245.12.

The third GET request is sent to the Internet address 178.79.137.164.

*Part 5:*

**18. What is the server’s response (status code and phrase) in response to the initial**

**HTTP GET message from your browser?**

A screenshot of a computer

Description automatically generated

The server’s status code is 401, and the phrase is “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?**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The new fields are Cache-Control and Authorization.

Wireshark Lab: DNS

*Part 3:*

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

The DNS query message sent to a IP address 143.89.14.7.

This is the IP address of my default local DNS server.

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

The “type” of DNS query is NS.

The query message does not 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 namesers?**

The response message provides 8 MIT nameservers, they are:

use5.akam.net

use2.akam.net

eur5.akam.net

ns1-173.akam.net

asia1.akam.net

ns1-37.akam.net

asia2.akam.net

usw2.akam.net

This response message also provides the IP address of the MIT nameservers, they are:

A screen shot of a computer

Description automatically generated

**19. Provide a screenshot.**

(The first screenshot is for Q16 – Q17, while the second to the fourth screenshots are for Q18 – Q19)

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated