CA1 Wireshark – HTTP Marks 30

Eoin Fitzsimons – X23151374

Before you begin, please ensure that you have Wireshark fully installed on your computer

Once you have opened Wireshark, proceed to complete the below steps and answer the below questions.

**Please note:** This is an individual assignment. Any evidence of plagiarism will result in zero grade for this lab. Please ensure you work on your own to answer the below questions. The use of any online tools is prohibited from use in this assignment.

# Instructions:

1. Log in to Moodle
2. Go to CA Activities
3. Download the two Wireshark files
4. Open the files in Wireshark (double click should open it automatically)
5. Answer the questions for each file

Edit this word document and upload your answers.

# Tips:

1. Wireshark is an intelligent tool that has features that help to identify packets and the corresponding requests/responses. So do not ignore as it is much easier to use what is available than it is to manually search through packets.
2. Use Wireshark filters to narrow down your search.
3. Use ‘right click’ > expand all – to make it easier to view all header information without having to click on individual items.

# Questions:

# Wireshark HTTP file.

## Find the first HTTP GET request, expand the HTTP headers section, and answer the following

* 1. TIP: use filters to narrow your search

### What is the user agent of the client the sent this HTTP request packet?

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n

### What is the hostname?

Host: apache.org\r\n

### What media formats will be accepted in the response?

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

### What is the default language that is accepted by the client?

Accept-Language: en-US,en;q=0.9\r\n

### What types of encoding (usually compression algorithms) can the client accept?

Accept-Encoding: gzip, deflate\r\n

## Find the corresponding response packet to the GET packet that you found above and answer the following questions:

### What content encoding was provided by the server?

Content-Encoding: gzip\r\n

### When does the content expire?

Expires: Wed, 13 Oct 2021 16:29:02 GMT\r\n

### What is the content length?

[Content length: 17011]

### How many cache hits were there in the response?

X-Cache-Hits: 6, 0\r\n

## Using the same response packet as above - Expand the IPv4 and TCP header sections and answer the following questions

### What is the IP address of the server?

Source Address: 151.101.2.132

### What is the IP address of the client?

Destination Address: 192.168.1.6

### What is the client port number used?

Destination Port: 62626

### What is the server port number used?

Source Port: 80

# monday pcap file

## Which domains were visited by the user?

Host: [www.msftncsi.com\r\n](http://www.msftncsi.com\r\n)  
Host: httpforever.com\r\n  
Host: www.computerweb4u.ie\r\n

## Find the HTTP GET request for computerweb4u.ie

### What is the IP address of the server?

Destination Address: 78.137.164.70

### What is the IP address of the client?

Source Address: 192.168.101.131

### What is the client port number used?

Source Port: 54245

### What is the server port number used?

Destination Port: 80