**LAB 21**

**HTTP(S)**

1. Open the capture file called “Lab 21 – HTTP capture.pcapng”.
2. Filter this capture so that only HTTP packets are displayed and answer the following questions about the second http packet:

* What frame number does this packet have in this capture file?

220

* Is this an http request or an http response packet?

HTTP-request (get)

* Write down the http client socket that is used

178.117.177.241

* Write down the http server socket that is used

193.191.136.205

* Write down the hostname of the server

www.howest.be

* Write down below the name (full path) of the requested document on that website

/shadowbox.css

1. Select the TCP stream to which the second HTTP packet belongs and answer the following questions about that TCP stream:

* What is the stream number of the TCP stream to which this packet belongs?

21

* How many segments does this stream contain?

25

* Note below the numbers of the segments that initialized this TCP stream using the 3-way TCP handshake.

152-171-172

1. Since HTTP version 1.1, a single TCP session (stream) may contain more than one HTTP transaction (consisting of an HTTP request and a corresponding HTTP response). This is also the case for the TCP stream you are currently looking at.

Further refine the filter of the previous question, to only show the HTTP packets within the current TCP stream.

How many HTTP transactions does this TCP session contain according to this new filter?

**Number of HTTP transactions =** 12

1. Note that you can track any HTTP transaction via the additional window that opens when you right click on an HTTP packet and choose Follow > HTTP stream.

Do this for the first HTTP packet in the packets you filtered with the previous command and note below which colors are used in this extra window:

**Color for the HTTP requests =** brown/red

**Color for the HTTP responses =** blue

By looking closely at this extra window you can find out which web server was contacted during this transaction: Nginx, IIS or Apache.

**Web server =** IIS

1. Answer the questions below about the object that was requested from a web server in frame number 572 via http.

* What is the name of the file in which this object is located? (only the name, not the complete path)

Diploma.jpg

* So what kind of object is this?

JPG-image

Because the object to retrieve does not consist of readable text, you cannot view it via Follow HTTP Stream. If you want to be able to view the object, you first need to find in the details window of your packet which frame the response is to be found. Write down the number of the frame below.

**Frame number with response = 602**

By double clicking on the hyperlink with this number, you go straight to the indicated frame number. Do it!

You can now download the requested object by right clicking on the last line in the details window of this HTTP response (titled “JPEG File Interchange Format”) and selecting the option “Export packet bytes”. Enter a filename and save the image to disk.

Then open this saved file.

Paste a screenshot of this image below.



1. An object that is requested via http is usually too large to be sent via a single frame. The frame number with the response you had to fill in in the previous command is usually not the only number that contains “response bytes”.

In the details window of the “response-frame” you can see which frames contain response-bytes. Write these down below.

**Frame numbers with response-bytes =** 524 – 602 – 607

Conclusion: The response frame to which Wireshark refers in the http request is always the last frame of all frames with “response bytes”.

Note that Wireshark notes the size (in bytes) of these frames behind each frame number with “response bytes”. Why aren't these all the same size?

First frame will have the maximum size, following frames will probably be smaller

1. You have already exported an image from this capture file which was downloaded within one specific TCP conversation. In this Wireshark capture file, however, several TCP conversations were captured in which several objects were downloaded via HTTP.

To get an overview of all objects downloaded from a web server during a capture session, you can use the File menu in Wireshark and then select “*Export Objects”* and then “*HTTP”*.

Use this method to save the image with the name “wegenwerken.jpg” on your laptop. Paste a screenshot of this image below.



1. Apply a filter expression to request all HTTP GET requests sent during this capture session.

http.request.method eq GET

So how many such requests are there?

40

Write down the filter expression below to find all HTTP responses that do not have an OK code. (See lecture slides for the OK code.)

http.response && !(http.response.code==200)

So how many responses are there?

5

1. How many segments in the capture file use HTTPS?

Hint: filter on the protocol used by HTTPS to make it secure (use the newest protocol).

102

1. Follow the TLS stream to which frame number 26 belongs.

What is shown in the opened extra window? Why is that so?

Empty window because traffic is encrypted

Close this extra window and return to the set filter. What is the stream number of the TCP session to which this TLS session belongs?

7

Enter the number of the frame in which the contacted HTTPS server sends its SSL certificate to the client.

32