CROUZET Zoé

DEVERGNE Noémie

BEHERAY Hugo

**Network Security – lab4**

**Q1)**

By doing *nslookup amazon.fr* we get this:

Une image contenant texte

Description générée automatiquement

Then by doing dig amazon.fr we get this:

Une image contenant texte

Description générée automatiquement

By using the filter on wireshark we get:

Une image contenant table

Description générée automatiquement

Q2)

We got the ip address of my amazon server by doing the dig command. The ip is 192.168.1.254.

Une image contenant texte

Description générée automatiquement

To get the ip address of amazon :

Une image contenant table

Description générée automatiquement

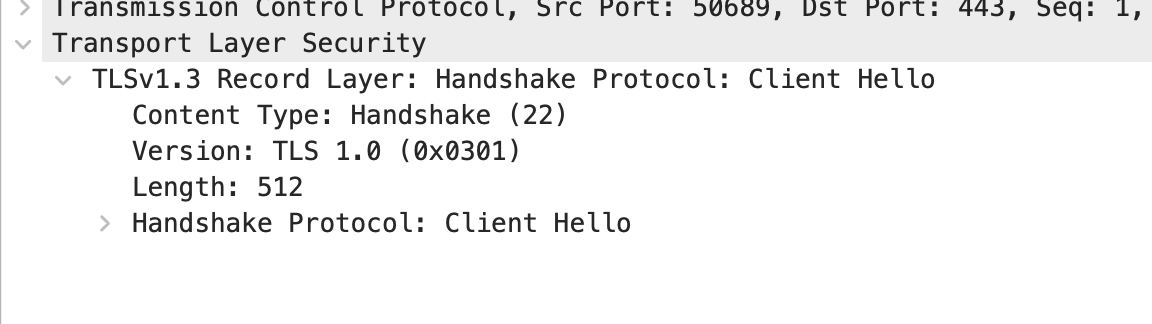
The ip address is 142.250.178.142.

Q3)

Une image contenant table

Description générée automatiquement

Q4)



Here we can see that the version of TLS is 1.0.

Q5)

Q6)

There are 3 fields :

* Content type = 1 Byte
* Version = 2 bytes
* Length = 2 bytes

Q7)

For the Client hello : Une image contenant texte

Description générée automatiquement

For the server Hello :

Une image contenant texte

Description générée automatiquement

Q8)

Une image contenant texte

Description générée automatiquement

Yes it does, the value is highlighted in blue on the screenshot.

Q9)

Une image contenant texte

Description générée automatiquement

Yes it does, it is 32 bits long and is used for preventing cyberattacks.

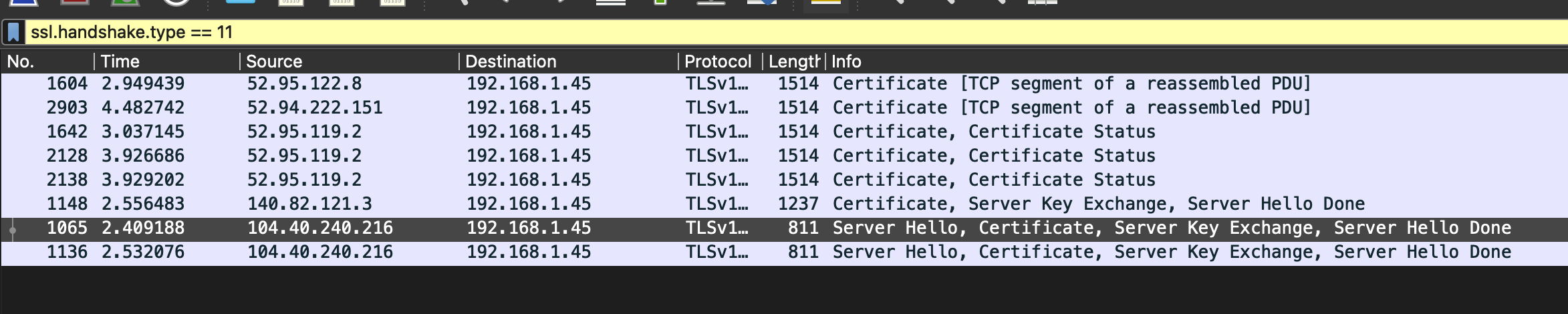
Q10)

On the previous screen (Q9) we can see that it contains a Session ID of 32 bits. It is used to create a secure session between server and client.

Q11)

There is no certificate in this record, they are in another one.

We can see here that they are in a single frame because of the length, which is the same everytime.



Q12)

Yes, the record is supposed to contain a pre master secret. It is used to create the master secret. The master key is used to create a session key.

Q13)

The change Cipher Spec Record indicates that the content of the SSL record will be encrypted. It is 6 bytes long.

Q14)

The handshake messages and MAC addresses are being encrypted when sent to the server.

Q15)

Q16)

We encrypt application data using symmetric encryption algorithm. It includes a MAC but wireshark does not distinguish the MAC and the encrypted application

Q17)