Monitoring a TLS Handshake

Getting started

This exercise assumes you have installed [WireShark](https://www.wireshark.org/download.html) on Kali-linux running in VirtualBox.

* Open Firefox and clear "Cookies and Site Data" and "Clear history"
* Type this URL in the browser <https://cphbusiness.dk>   (or any URL, that will redirect to a secure connection)  **DO NOT HIT ENTER** yet.

Performing the capture

* In Wireshark start a new capture, and when started, go to the browser and hit ENTER.
* When the secure page is loaded (you have a chain lock in your browser) stop the capture.

Observe the captured traffic

* Type **tls** in the display filter box
* Identify the Client Hello package (If there is more than one, pick the last one you find)
* Right-click this package → Select Follow → TLS Stream. Just close the window that pops up
* Add this to the filter string **&& tls**

Et billede, der indeholder ur, telefon, computer

Automatisk genereret beskrivelse

*For the next questions, you should focus only on the packages between the Client Hello message, and the first Application Data message (the SSL handshake)*

* How many of the messages from this figure, taken from the slides, can you identify in the captured traffic?
* How many of the terms listed in the top of this exercise can you identify in the captured traffic (You need to open the Secure Socket Layer Packets) in the bottom window?
* How many Cipher Suites did the Client (browser) support?
* Which of the Cipher Suites, supported by the client, was chosen by the server?
* Open one of the Secure Socket Layer packages for an Application Data request. Hopefully, you will observe that you cannot read the content - **it's encrypted** :-)
* Which overall strategy was used to encrypt the “Application Data” packages: Symmetric or Asymmetric (public key) encryption?