Task 1

I have no idea what is that, and I don’t know how to do it.

Task 2

The protocol is TLS v1.2, that can be identified by the protocols shown in the software.

The destination host is 129.78.110 .124, and the message ‘server hello’ is sent to this address, and the message ‘client hello’ is sent from this address.

Because that can allow one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.

The certificate is issues from the server128.65.210.8, to the client.

There is one certificate.

The handshake protocol was used.

It was not signed, as the transmission between server and client was established in a safe environment, and identities verified.