I installed wireShark and sniffed IP/DNS/HTTP/UDP/SSL traffic on my local Ethernet network, and then I did all the assignment questions.

Here is some particular knowledge that I didn't know before.

IP/UDP and DNS section

I learned datagram fragmentation. Ethernet frame is 1500, subtract the 20 size header, the IP MTU(Maximum Transmission Unit) is 1480, and for UDP ,the MTU is 1472.

I also learned that DNS query is reversed. And because my machine is in a windows domain, dns client send out multiple requests for the name, because it didn't know which machine+domain I am refer to.

Http Section.

I learned that

For long document, there are a lot of continuation responses.

For each authentication, client resend request, with encoded user/pass in the header.

SSL section

After solved all questions in assignment, I visited eBay and amazon https site, to check their security level.

I found out that their Cipher Suite is also vulnerable and could get attacked.

My browser client asks Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)

Amazon server:

TLS v1.0, Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005).

EBay server:

TLS v1.0, Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004)

TLS v.10 and RC4 128bit are all considered vulnerable now days.

People have published paper regarding succeeded attack to TLS v1.0 like 3 years ago, and to RC4 about 1 year ago.

The succeed attack to RC4 is steal cookies from PayPal; I think EBay really should improve their security level.