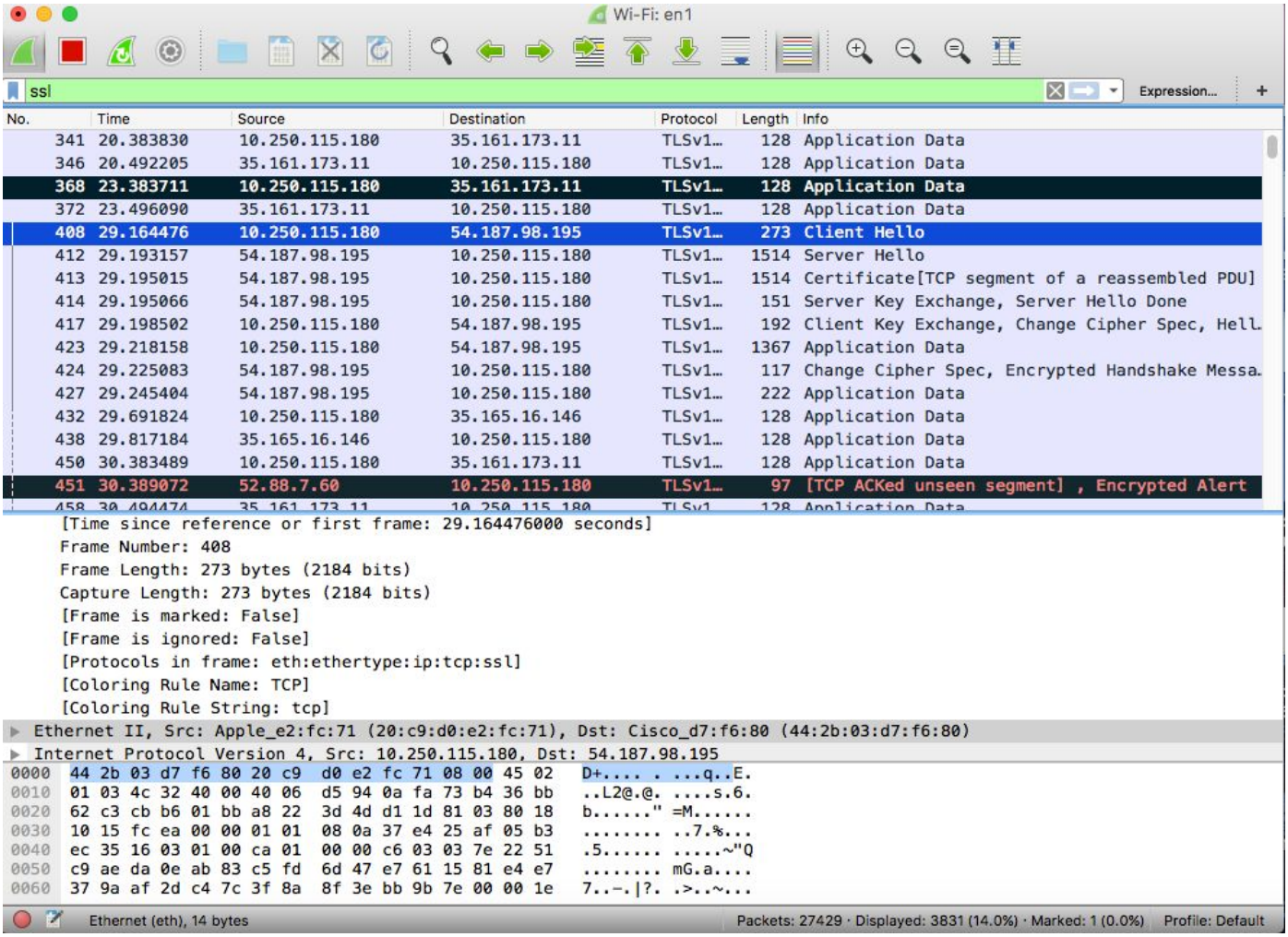
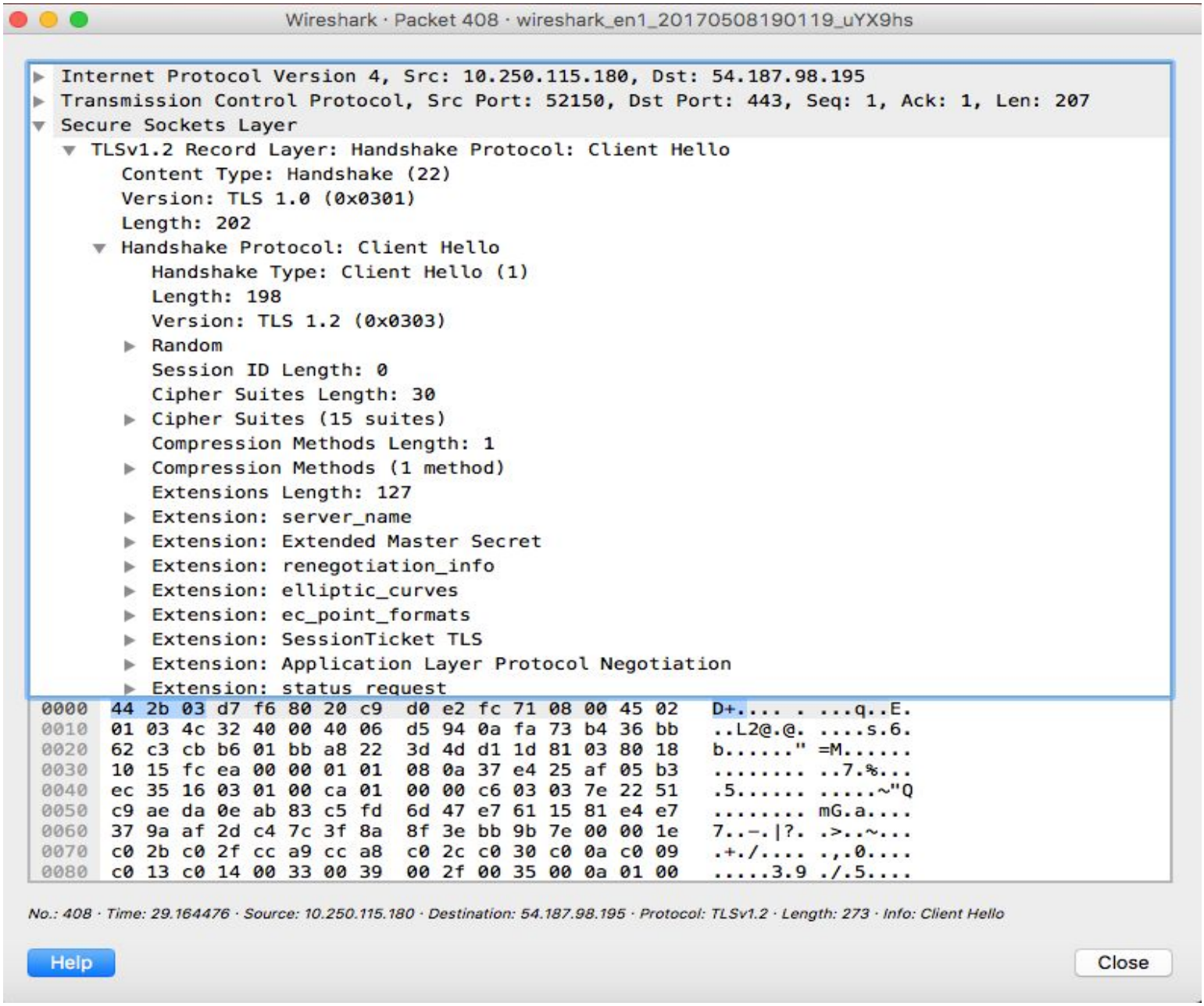
Paul Diaz
HW9
CS 166

1. Use Wireshark to capture SSL authentication packets.



a. **The communication starts off by Alice saying “Can we talk” which is “Client Hello” highlighted in blue — source 10.250.115.180. Then server says hello back which is “Server Hello” in wireshark — source 35.161.173.11 then sends Certificate[TCP segment of reassembled PDU] and Server Key Exchange, Hello Done. Then client responds back by sending Client Key Exchange, Change Cipher spec, Hello. Then server sends Change Cipher Spec, Encrypted Handshake Message, then Encrypted Alert.**

b. **SSL packets contain the following — One packet contains Handshake protocol that contains handshake type, length, and version. It also contains random session ID length, cipher suites length, compression method and its length, extension server name, and others (please see pic attached).**



2. SSL and IPSec are both designed to provide security over the network.

    a. **The purpose of SSL is similar to IPsec, namely, security over the network and accomplish the same thing: authentication, session key, and more. They both provide encryption, integrity protection, and authentication.**
    b. **In terms of implementation, SSL is relatively simple while IPSec is complex. SSL lives at the socket layer, as a result, SSL resides in user space, while IPSec lives at the network layer — not directly accessible from user space.**
3. Suppose we use symmetric keys for authentication and each of N users must be able to authenticate any of the other N -1 users. Evidently, such a system requires one symmetric key for each pair of users, or on the order of N^2 keys. On the other hand, if we use public keys, only N key are required , but we must then deal with PKI issues.
    a. **Kerberos requires N symmetric keys for N users. Users do not share keys with each other. Instead each user shares one key with the KDC, that is, Alice and the KDC share K_A , Bob and the KDC share K_B, Carol and the KDC share K_C, and so on. Then the KDC acts as a go-between that enables any pair of users to communicate securely with each other. The bottom line is that Kerberos uses symmetric keys in a way that doe scale.**
    b. **In Kerberos, no PKI is required, but TTP plays a similar role as a certificated authority in a public key system. Kerberos TTP is known as the key distribution center, or KDC. Since the KDC acts as a TTP, if it's compromised, the security of the entire system is compromised.**
4. IKE has two phases, Phase 1 and Phase 2. In IKE Phase 1, there are four key options and for each of these, there i s a main mode and aggressive model
    a. **As with the digital signature variant, the main difference from main mode is that aggressive mode does not attempt to hide identities while main mode does. Main mode MUST be implemented, while aggressive mode SHOULD be implemented. Aggressive mode should be implemented.**
    b. **The primary advantage of the Phase 1 digital signature key option is that, it can start the protocol without waiting to obtain the other side's public key. This is true since it doesn't need to know anyone's public key — since everyone knows their private keys. However along the process of this protocol, it needs to obtain the other party's public key, in order to verify him/her as a proof, but this can be done in parallel during the process of the this protocol.**