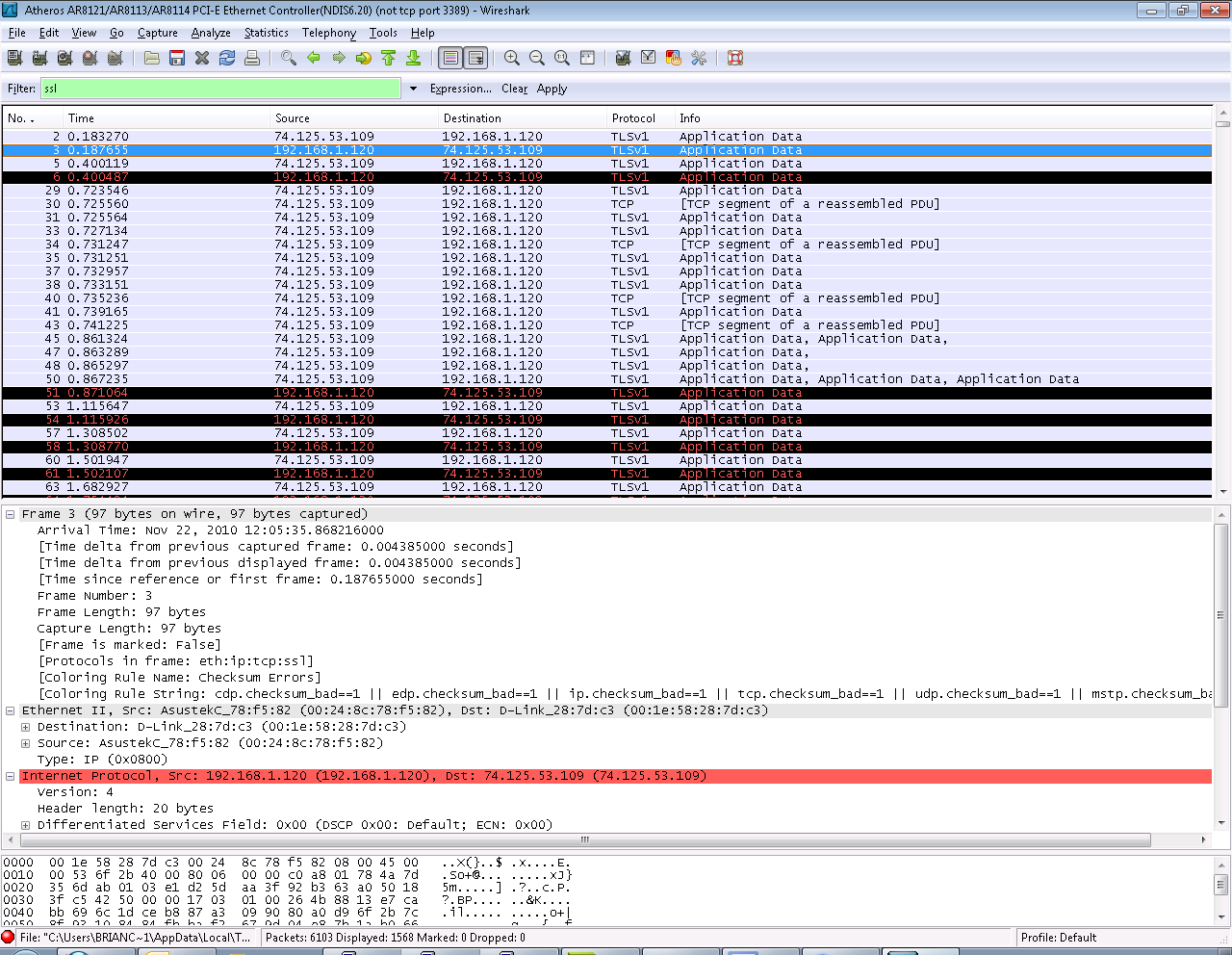
Brian Cullinan

11/22/2010

Project 4



* 1. Source:192.168.1.120, Count: 1 record, Types: Client Hello
  2. Source:72.21.214.128, Count: 1 record, Types: Server Hello, Certificate
  3. Source:192.168.1.120, Count: 3 records, Types: Handshake, Client key exchange, Encrypted handshake
  4. Source:72.21.214.128, Count: 2 records, Types: Change cipher spec, Encrypted handshake
  5. Source:192.168.1.120, Count: 1 record, Types: Application Data
  6. Source:72.21.214.128, Count: 1 record, Types: Application Data
  7. Source:72.21.214.128, Count: 1 record, Types: Application Data
  8. Source:192.168.1.120, Count: 1 record, Types: Application Data

1. The 3 different fields are as follows:
   1. Content Type: 1 byte
   2. Version: 2 bytes
   3. Length: 2 bytes
2. The content type for the client hello is Handshake
3. No, there does not appear to be a challenge
4. Yes, RSA, AES, SHA
5. Yes, TLS\_RSA\_WITH\_RC4\_128\_MD5
6. No, there does not appear to be a challenge in this record
7. Yes, it’s includes a session ID of length 32, the point is so the server can keep track of who is connected
8. Yes, it includes a certificate and it fits in to one frame.
9. It does not appear to contain a pre-master secret, no.
10. This message tells the server and client that all messages will use the encryption algorithm that was just decided on, this is a length of 1 byte
11. A RC4 key used throughout the session, using the newly decided encryption mode in this case RSA
12. Yes, they seem to be formatted exactly the same way but the content of the handshake is different
13. The application data is being encrypted with RSA. It looks like each application data record also has a MAC associated with it. No, it does not distinguish between the two.
14. I found it interested that Wireshark can list the data protocol used for each TLS message. The working protocols are all http, but I saw some other imap TLS messages for when I was checking my e-mail during the capture.