Ivan Cruz

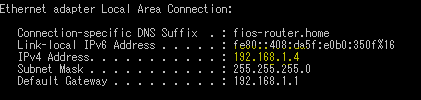
Prof. Waziri

IT-520

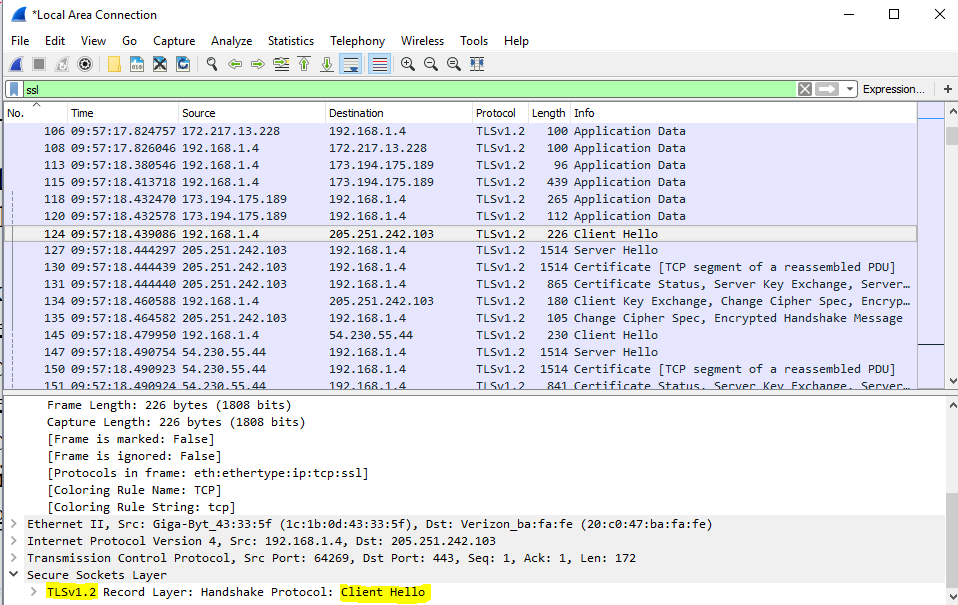
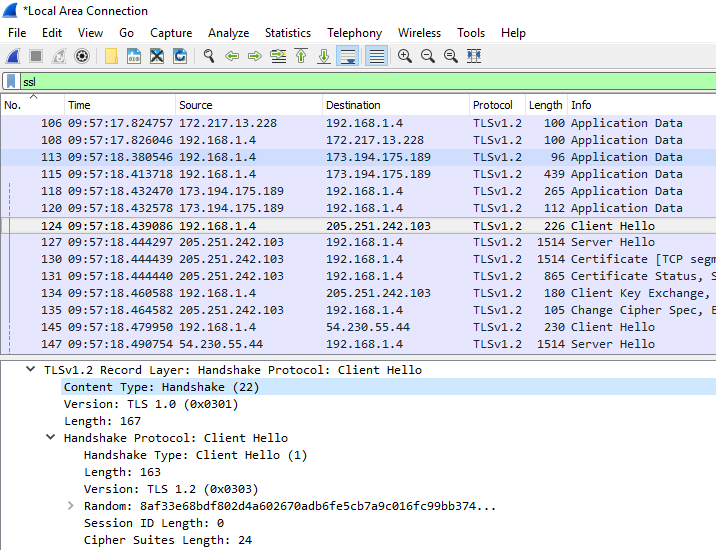
April 17, 2018

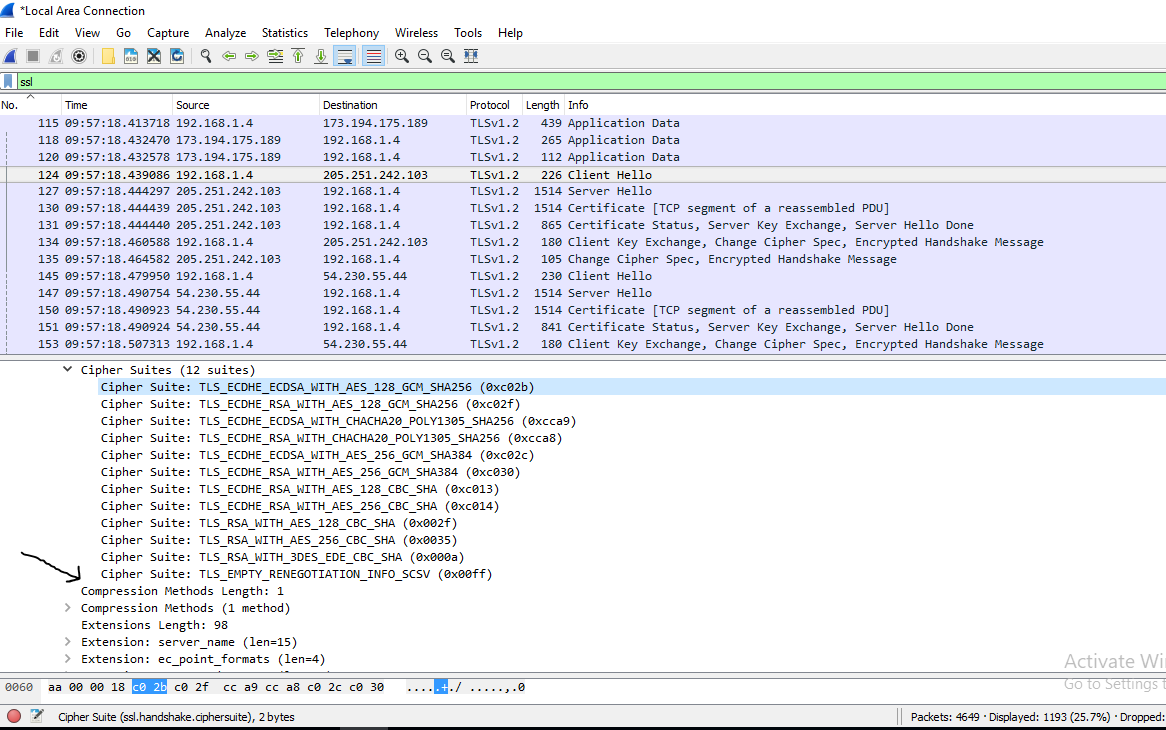
**Lab 8**

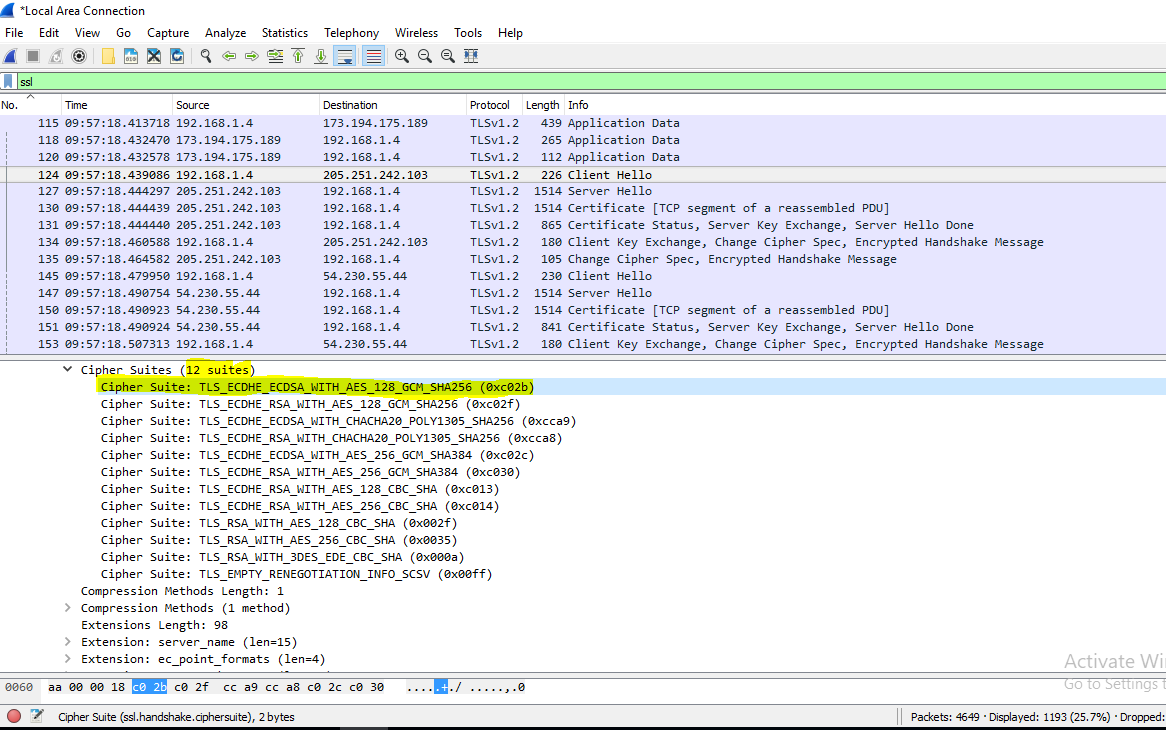
* Screenshot of my IP Address



Client Hello Record

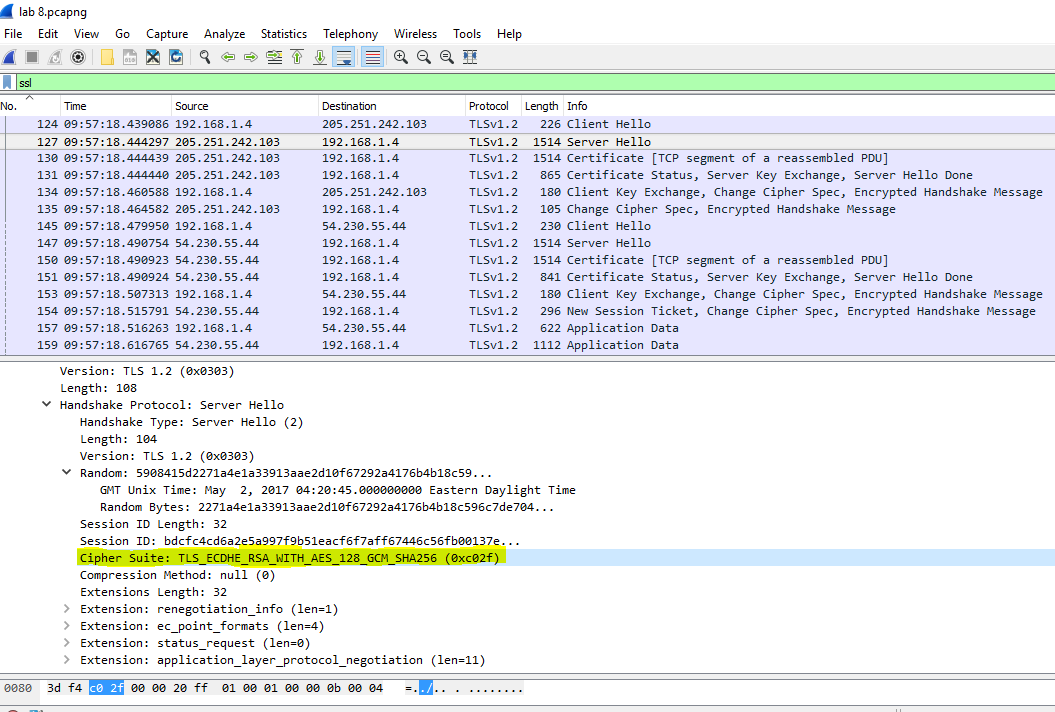
1. The Transport Layer Socket (TLS) version is 1.2 for the Client Hello frame
2. The value of the content type is 22
3. There is no challenge for this communication. If a challenge were present, it would normally be under the Cipher suite (arrow indicates the typical location of the challenge).



1. The ClientHello supports 12 different cipher suites. The first Cipher suite is TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 
   * This Cipher Suite uses private-public key algorithms: Elliptical Curve Digital Signature Algorithm (ECDSA) and Elliptical Curve Diffie-Hellman Exchange (ECDHE).
   * ECDHE is the symmetric-key algorithm
   * The hash algorithm is SHA256

Server Hello Record

1. TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 was chosen for this connection.



* + ECDHE and RSA are the algorithms used for the public-private key exchange
  + AES-128 and GCM are used to encrypt the data via bulk encryption
  + SHA256 is the hash algorithm