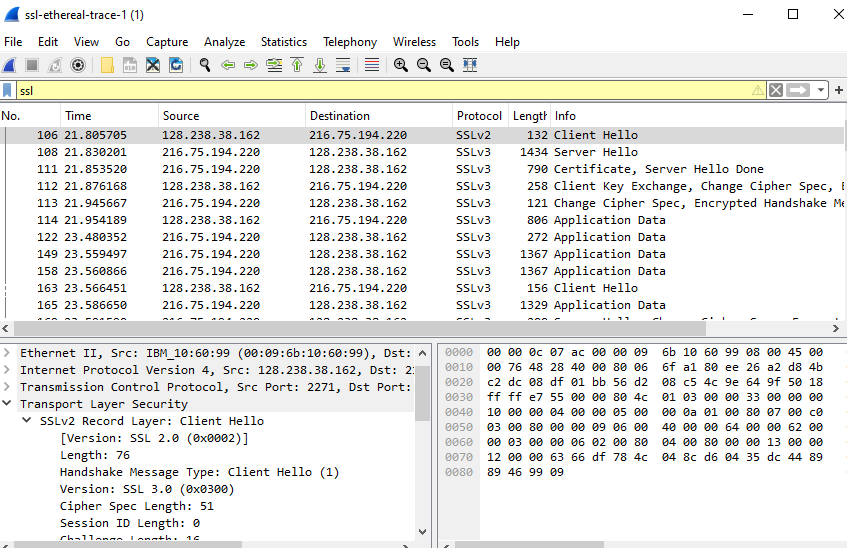
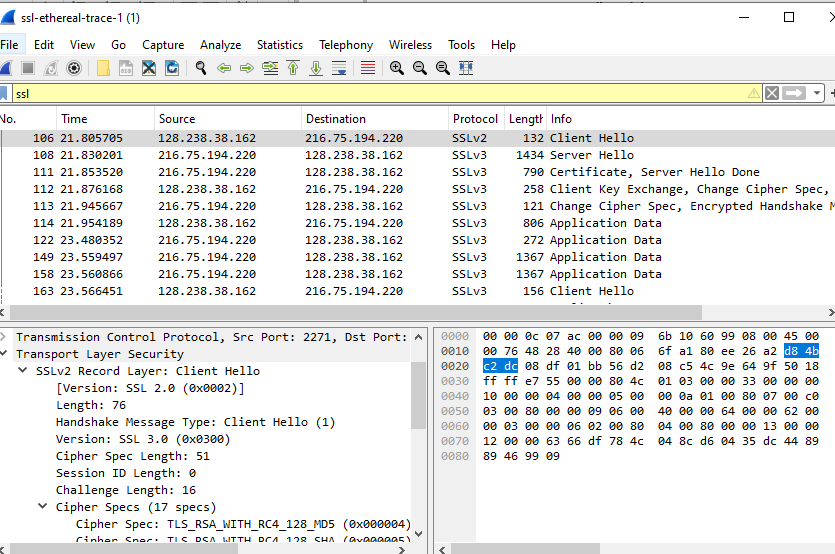
**Task 3: Investigating the Secure Sockets Layer (SSL) protocol**

SSL is a mechanism for securing the Internet that is based on encryption. The Secure Sockets Layer (SSL) protocol initiates a process of authentication known as a handshake between two communicating devices in order to verify that both devices are in fact indeed who they claim to be. In addition, SSL digitally signs data in order to ensure the integrity of the data. This ensures that the data has not been altered in any way before it is delivered to the person who is supposed to receive it.

**1: Capturing packets in an SSL Session**



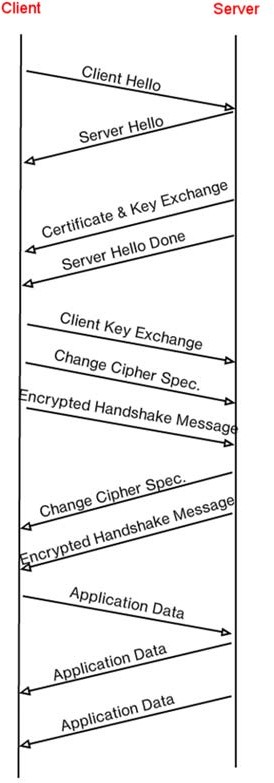
**2: Captured Trace**



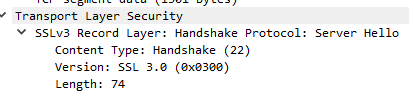
**1: Table for the 8 Ethernet Frames**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Time | Source | Destination | Info |
| 106 | 21.80571 | 128.238.38.162 | 216.75.194.220 | Client Hello |
| 108 | 21.8302 | 216.75.194.220 | 128.238.38.162 | Server Hello |
| 111 | 21.85352 | 216.75.194.220 | 128.238.38.162 | Certificate, Server Hello Done |
| 112 | 21.87617 | 128.238.38.162 | 216.75.194.220 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 113 | 21.94567 | 216.75.194.220 | 128.238.38.162 | Change Cipher Spec, Encrypted Handshake Message |
| 114 | 21.95419 | 128.238.38.162 | 216.75.194.220 | Application Data |
| 122 | 23.48035 | 216.75.194.220 | 128.238.38.162 | Application Data |
| 149 | 23.5595 | 216.75.194.220 | 128.238.38.162 | SSLv3 |

**Timing Diagram**

****

**2: SSL records begins with the same three fields as shown in the diagram:**

****

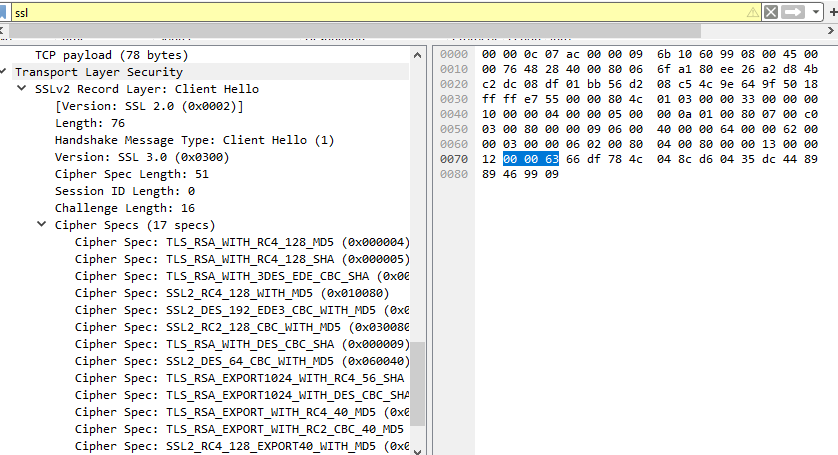
Content type = 1 byte

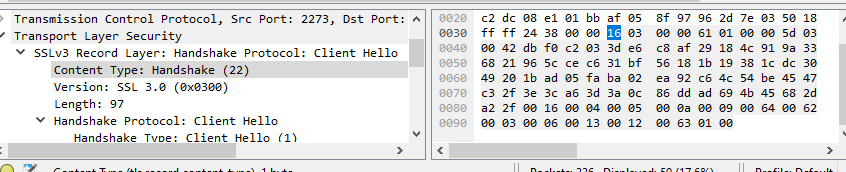
Version = 2 byte

Length = 2 byte

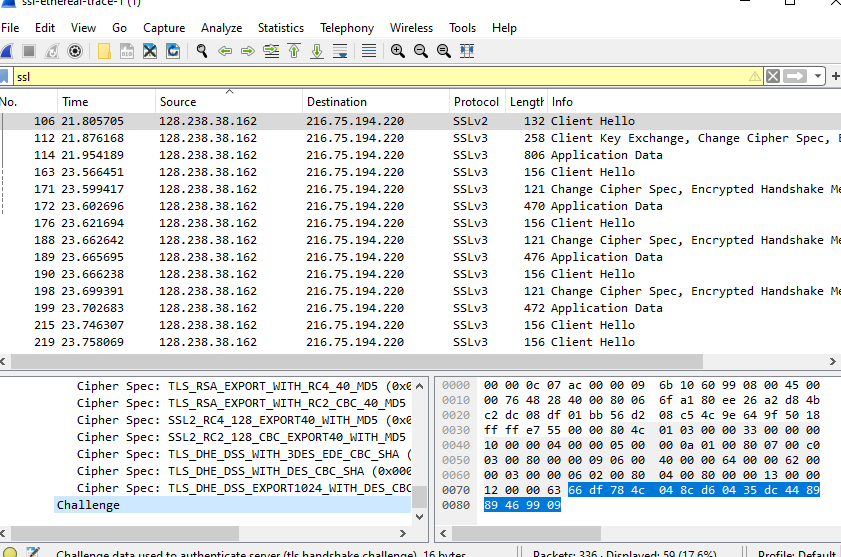
**3: HelloClient Record**

**The content type is 22.**

****

****

**4: Hexadecimal notation value:**

****

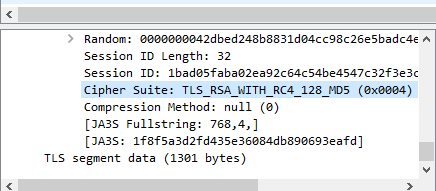
**5: Algorithms**

Public key algorithm: RSA

Symmetric key algorithm: RC4

Hash algorithm: MD5

**6: Cipher suit Algorithms on ServerHello SSL Record:**



**7: The purpose of client and Server nonces in SSL:**

Yes. It is used for attack preventing and it is 32 bit long i.e., 28bits data and 4bits time.

**8: Purpose of ID session**

The Server Hello message at frame 108 has a session ID. Clients receive unique SSL session IDs from the server to simplify session restart.   
  
The session ID lets the client and server restart a terminated SSL session without a handshake. Customers might receive a session ID in the Server Hello message upon connecting. Use the session ID to request the session if the client can continue and has previously created a session with the server. This method speed up and reduce the cost of creating a new SSL session for client-server communications.   
 **9: Certificate:**

No, this document does not contain any certificates of any kind. There is a separate record that contains the certificate. The certificate was able to fit into a single Ethernet frame.

**10: Pre-Master Secret**

This record have a pre-master secret, as the statement would imply. It is via the utilization of this pre-master secret that the master secret is created. Master key helps generate session key. After encryption with the public key, the secret is 120 bytes.

**11: Purpose of the Change Cipher Spec Record**

Change Cipher Spec records are necessary for SSL/TLS handshakes to take place. Following the completion of encryption negotiation, it signifies the beginning of secure communication. One byte of the message contains information on the cipher suite, key exchange, and changes to the encryption key. Once the recipient has obtained this record, they immediately begin the process of encrypting and decrypting data using the improved security parameters. The establishment of a safe network path for the transmission of confidential data is made possible by this crucial document. It is 6 bytes.

**12: Encrypted Handshake Record:**

The handshake messages sent during the SSL/TLS handshake protocol are encrypted in the encrypted handshake record using specific encryption algorithms, such as symmetric (e.g., AES) and authenticated (e.g., HMAC). This ensures the confidentiality and accuracy of the handshake messages sent between the client and server.

**13: Server send a Change Cipher Record:**

Yes the server’s encrypted handshake contains all the handshake messages that are sent from the server to the clients. From the server's point of view, the Change Cipher Spec record signifies the shift to using the previously set encryption parameters for future communication. During an encrypted handshake, the server and client exchange messages such as ServerHello, ServerKeyExchange, and CertificateRequest. These messages are then included in the encrypted handshake record. From the perspective of the server, these records are just as useful as the ones given by the client.

**14: Application Data**

During an SSL/TLS connection, application data is encrypted using a negotiated encryption technology (such as AES) and protected by a Message Authentication Code. The encrypted data's message authentication code (MAC) was calculated from the plaintext data before encryption. In packet analysis, Wireshark may provide fields for each component in the packet details window, but it does not readily distinguish between the MAC and encrypted application data. Despite its inability to discern between the two. Wireshark usually presents the packet as encrypted, but decryption is needed to view the plaintext, which includes the MAC address.

**15: Finding in the Trace:**

The existence of the SSLv3 protocol version in the current trace is not important as it demonstrates continued usage despite known vulnerabilities.

**Conclusion:**

The SSL/TLS handshake protocol and encrypted communication in the trace showed that encryption parameters were carefully negotiated and secure channels were established between clients and servers. With trace analysis, this was achieved. In particular, the use of SSLv3, despite its flaws, shows how important it is to identify and mitigate network communication security concerns. Handshake records, encryption techniques, and message authentication procedures can help you understand secure communication protocols. Integrity verification and encryption are crucial to protecting sensitive network data.   
  
**References**

Alnatheer, M. A. (2014). Secure socket layer (SSL) impact on web server performance. *Journal of Advances in Computer Networks*, *2*(3), 211-217.

Charjan, D. M., Bochare, P. M., & Bhuyar, Y. R. (2013). An overview of secure sockets layer. *Int. J. Comput. Sci. Appl*, *6*(2), 388-393.

Dastres, R., & Soori, M. (2020). Secure socket layer (SSL) in the network and web security. *International Journal of Computer and Information Engineering*, *14*(10), 330-333.

Bhatt, D. V., Schulze, S., & Hancke, G. P. (2006). Secure Internet access to gateway using secure socket layer. *IEEE transactions on instrumentation and measurement*, *55*(3), 793-800.

Jha, R. K., & Khurshid, F. (2014, December). Performance analysis of enhanced secure socket layer protocol. In *2014 International Conference on Communication and Network Technologies* (pp. 319-323). IEEE.