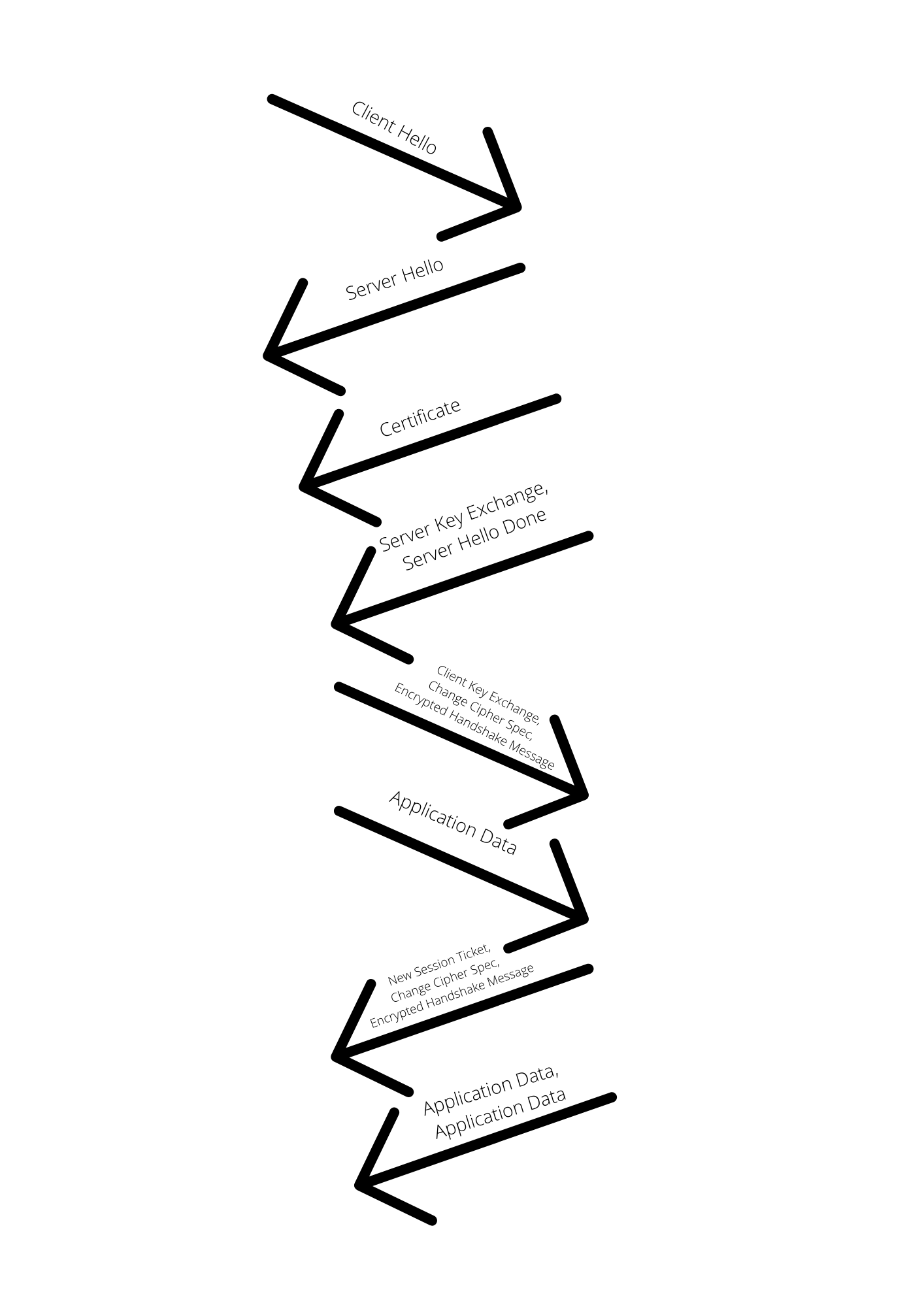
Aluno:

Matrícula:

1 -

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | ORIGEM | CONTADOR TLS | TIPO |
| 1 | Cliente | 1 | Client Hello |
| 2 | Servidor | 1 | Server Hello |
| 3 | Servidor | 1 | Certificate |
| 4 | Servidor | 2 | Server Key Exchange, Server Hello Done |
| 5 | Cliente | 3 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 6 | Cliente | 1 | Application Data |
| 7 | Servidor | 3 | New Session Ticket, Change Cipher Spec, Encrypted Handshake Message |
| 8 | Servidor | 2 | Application Data, Application Data |

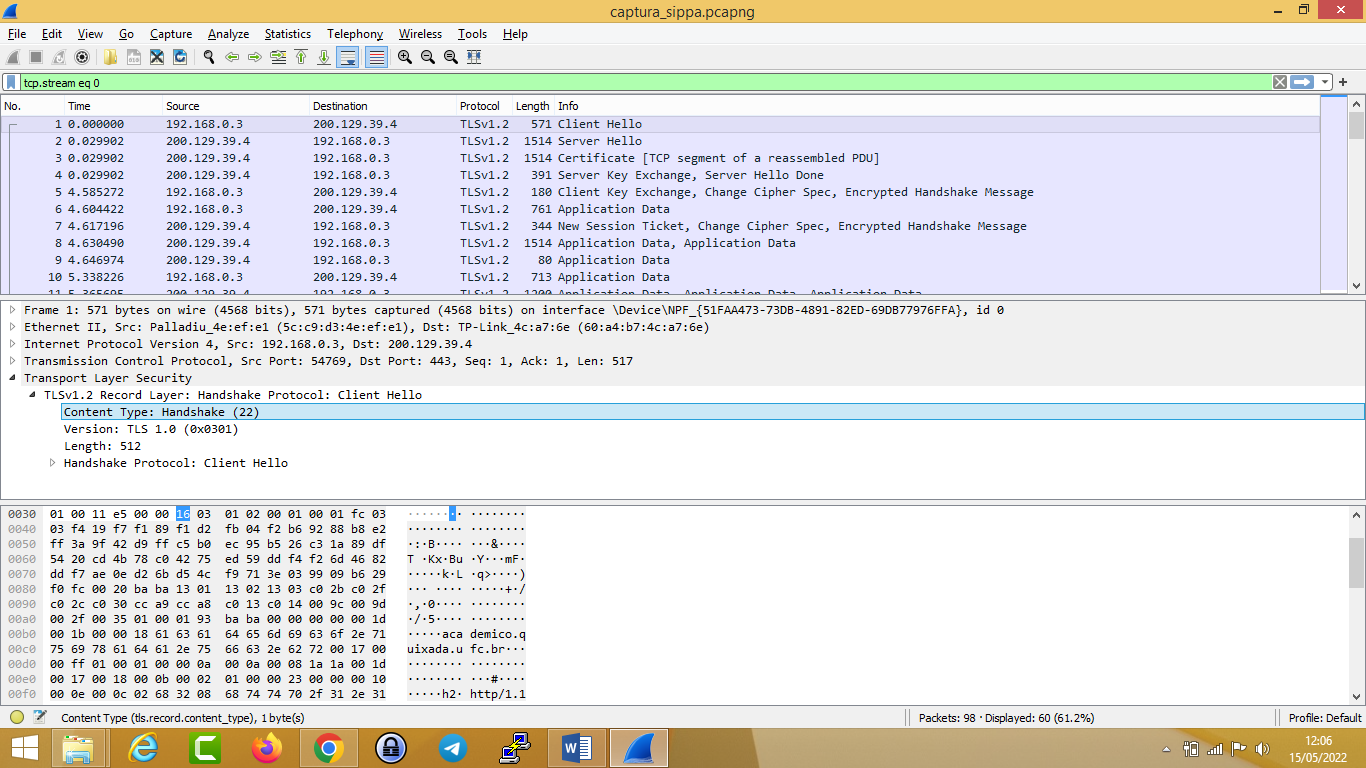


2 –

Content Type: 1 byte

Version: 2 bytes

Length: 2 bytes



3 – Content Type: Handshake (22)

4 – Sim, com o valor de:

Random: f419f7f189f1d2fb04f2b69288b8e2ff3a9f42d9ffc5b0ec95b526c31a89df54

5 – Sim, ele lista vários.

6 – Sim, foi utilizado os seguintes algoritmos: RSA, AES e SHA256.

7 – Sim, contendo um tamanho de 32 bytes de dados, sendo eles 28 para dados e 4 bytes para o tempo, com isso busca-se evitar ataques de reprodução.

8 – Não. Sua função é atribuir um identificador para cada sessão.

9 – Não há certificado, ele está em outro pacote e sozinho.

10 - Sim, ela usada por ambos para gerar chaves de sessão, sendo criptografado usando a chave pública do servidor usando 126 bytes. \*

11 – É indicar que os registros enviados pelo o TLS serão criptografados, este registro apresenta 6 byes, sendo 5 para o header e 1 para o segmento de mensagem.

12 – Uma junção das mensagens de handshake anteriores enviadas para o cliente é gerada e enviada para o servidor.

13 – Sim, o servidor envia, sendo o mesmo criptografado, é diferente pois contém a junção de todas as mensagens de handshake enviadas pelo o servidor.

14 – Está sendo usado o AES. A chave de criptografia do cliente é usada para criptografar dados do cliente para o servidor, e com o servidor acontece o contrário.