

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FEELT – FACULDADE DE ENGENHARIA ELÉTRICA
ENGENHARIA DE COMPUTAÇÃO

LUCAS ALBINO MARTINS
12011ECP022
ALAN NICOLAS DE OLIVEIRA SILVA
12011ECP025

**REDES DE COMUNICAÇÕES II: Atividade Prática 5 - Tarefa de
Programação Wireshark SSL**

UBERLÂNDIA
2021

Atividade Prática 5 - Tarefa de Programação Wireshark SSL

1. For each of the first 8 Ethernet frames, specify the source of the frame (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a timing diagram between client and server, with one arrow for each SSL record.

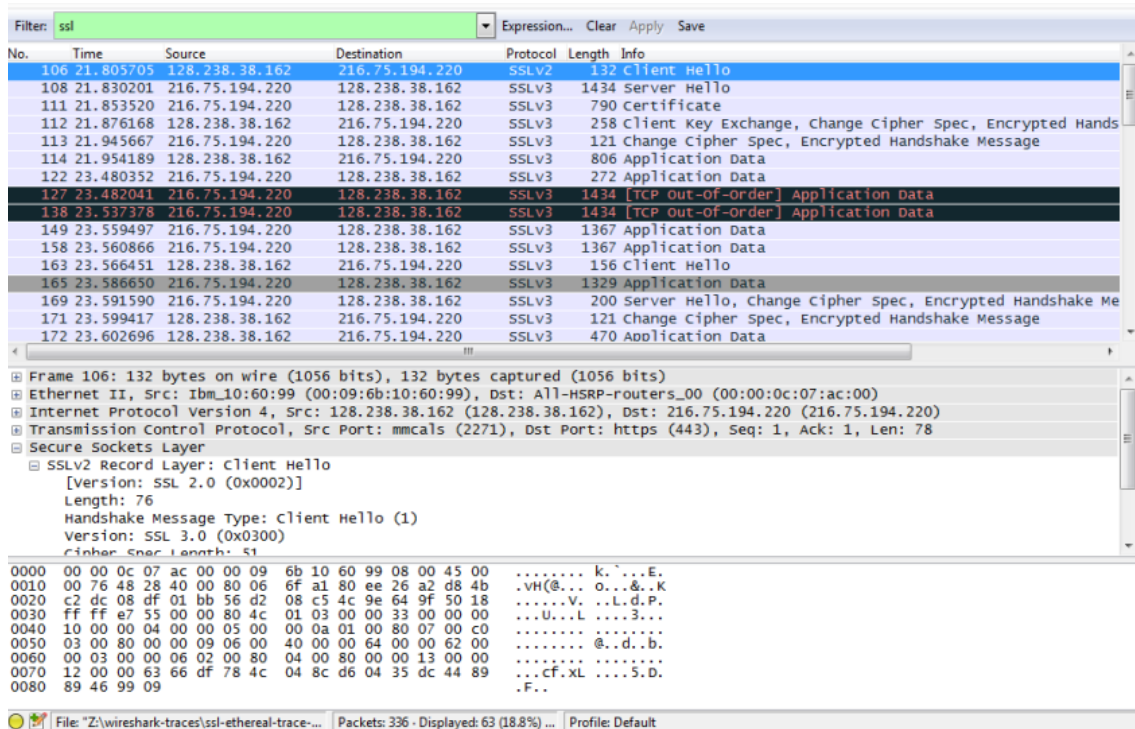


Figura 1 – Captura de tela wireshark.

Tabela 1 – SSL.

Nº	Frame	Origem	Destino	Nº de SSL	Tipo de SSL
1	106	128.238.38.162	216.75.194.220	1	Client Hello
2	108	216.75.194.220	128.238.38.162	1	Server Hello
3	111	216.75.194.220	128.238.38.162	2	Server Hello Done
4	112	128.238.38.162	216.75.194.220	3	Client Key Exchange
5	113	216.75.194.220	128.238.38.162	2	Change Cipher Spec
6	114	128.238.38.162	216.75.194.220	1	Application Data
7	122	216.75.194.220	128.238.38.162	1	Application Data
8	127	216.75.194.220	128.238.38.162	1	Application Data

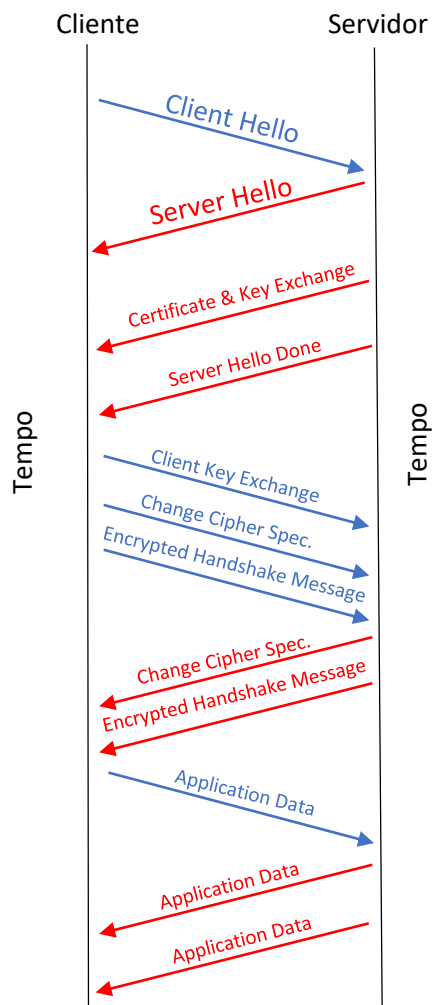


Figura 2 – Diagrama de tempo(Cliente x Servidor).

2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is “content type”and has length of one byte. List all three fields and their lengths.

```

Frame 112: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)
Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
Internet Protocol Version 4, Src: 128.238.38.162 (128.238.38.162), Dst: 216.75.194.220 (216.75.194.220)
Transmission Control Protocol, Src Port: mmcals (2271), Dst Port: https (443), Seq: 79, Ack: 2785, Len: 204
Secure Sockets Layer
  SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: SSL 3.0 (0x0300)
    Length: 132
  Handshake Protocol: Client Key Exchange
    Handshake Type: Client Key Exchange (16)
    Length: 128
  SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
0000  00 00 0c 07 ac 00 00 09 6b 10 60 99 08 00 45 00  ..... k. ^...E.
0010  00 f4 48 2c 40 00 80 06 6f 1f 80 ee 26 a2 d8 4b  ..H.@... o...&..K
0020  c2 dc 08 df 01 bb 56 d2 09 13 4c 9e 6f 7f 50 18  .....V.  ..L.O.P.
0030  fd 1f c2 d9 00 00 16 03 00 00 84 10 00 00 80 bc  .....
0040  49 49 47 29 aa 25 90 47 7f d0 59 05 6a e7 89 56  IIG).%.G  ..Y.j..V
0050  c7 7b 17 cf 08 b4 7c 60 0c 61 f1 04 b0 fb f8 3c  .....
File: "Z:\wireshark-traces\ssl-ethereal-trace-...  Packets: 336 - Displayed: 63 (18.8%) ...  Profile: Default

```

Figura 3 – Informações sobre os três campos e seus comprimentos para o frame número 112.

Os campos de comprimento são:

- 1) Content Type = 1 byte
- 2) Version = 2 bytes
- 3) Length = 2 bytes

3. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

The image shows a Wireshark packet capture of an SSLv2 Client Hello record. The packet list shows a single packet of type SSLv2, length 132, containing a Client Hello. The packet details pane shows the following structure:

- Transmission Control Protocol, Src Port: mmcals (22/1), Dst Port: nttps (443), Seq: 1, ACK: 1, Len: 78
- Secure Sockets Layer
 - SSLv2 Record Layer: Client Hello
 - [Version: SSL 2.0 (0x0002)]
 - Length: 76
 - Handshake Message Type: Client Hello (1)
 - Version: SSL 3.0 (0x0300)
 - Cipher Spec Length: 51
 - Session ID Length: 0
 - Challenge Length: 16
 - Cipher Specs (17 specs)
 - Cipher Spec: TLS_RSA_WITH_RC4_128_MD5 (0x000004)
 - Cipher Spec: TLS_RSA_WITH_RC4_128_SHA (0x000005)
 - Cipher Spec: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00000a)
 - Cipher Spec: SSL2_RC4_128_WITH_MD5 (0x010080)
 - Cipher Spec: SSL2_DES_192_EDE3_CBC_WITH_MD5 (0x0700c0)
 - Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x030080)
 - Cipher Spec: TLS_RSA_WITH_DES_CBC_SHA (0x000009)
 - Cipher Spec: SSL2_DES_64_CBC_WITH_MD5 (0x060040)
 - Cipher Spec: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x000064)
 - Cipher Spec: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x000062)
 - Cipher Spec: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x000003)
 - Cipher Spec: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x000006)
 - Cipher Spec: SSL2_RC4_128_EXPORT40_WITH_MD5 (0x020080)
 - Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x040080)
 - Cipher Spec: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x000013)
 - Cipher Spec: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x000012)
 - Cipher Spec: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x000063)
 - Challenge

The challenge field is highlighted in blue, showing the hex value 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 09. The packet bytes pane shows the raw data of the challenge field, which is 16 bytes long.

Figura 4 – Campo Content Type para o frame de Client Hello.

Resp.: O valor é 22, correspondendo a uma Handshake Message.

4. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

Sim, possui um nonce. O valor do Challenge é: 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 09

5. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

Sim, há especificação dos Cyber Suites. Os três algoritmos são:

- Algoritmo de chave pública: RSA
- Algoritmo de chave simétrica RC4
- Algoritmo de hash: MD5

6. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

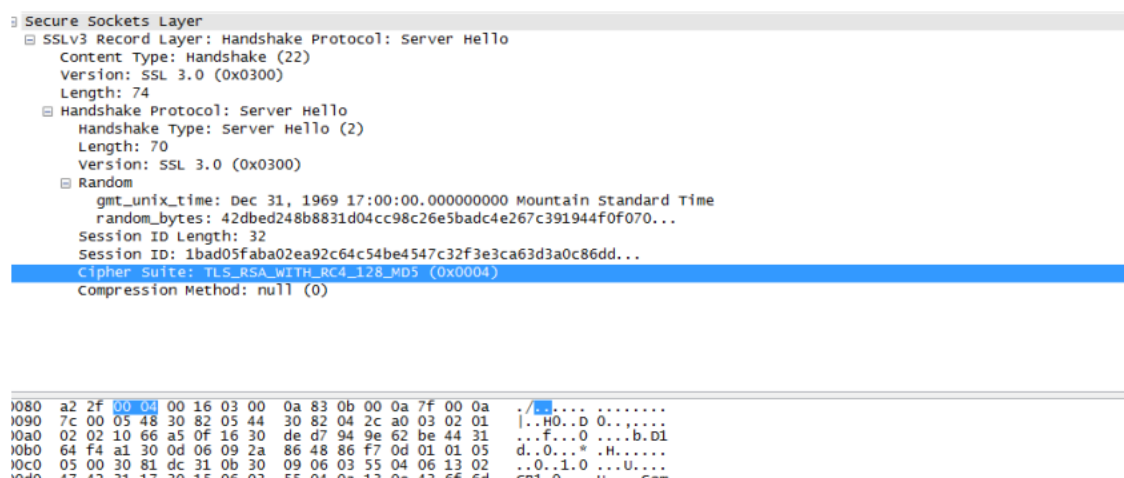


Figura 5 – Cipher Suites.

Sim, há especificação dos Cyber Suites. Os três algoritmos são:

- Algoritmo de chave pública: RSA
- Algoritmo de chave simétrica RC4
- Algoritmo de hash: MD5

7. Does this record include a nonce? If so, how long is it? What is the purpose of the client and server nonces in SSL?

Sim, possui um nonce de 32 bits (28bits data + 4 bits time), ele é usado para prevenir ataques.

8. Does this record include a session ID? What is the purpose of the session ID?

Sim, o ID da sessão no registro é um identificador para a sessão SSL. Este ID pode permitir que o cliente retome a sessão mais tarde usando o ID da sessão.

9. Does this record contain a certificate, or is the certificate included in a separate record. Does the certificate fit into a single Ethernet frame?

Não, não há certificado neste registro. O certificado está no registro separado. Sim o certificado caber em um único quadro Ethernet.

10. Locate the client key exchange record. Does this record contain a pre-master secret? What is this secret used for? Is the secret encrypted? If so, how? How long is the encrypted secret?

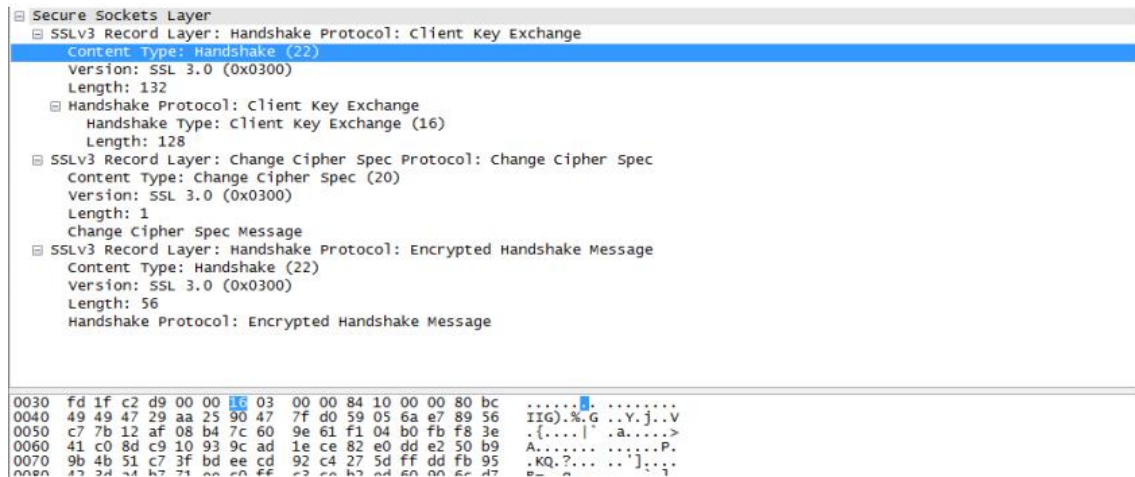


Figura 6 – PreMaster Secret.

Sim, este registro contém um segredo pré-mestre. O segredo mestre é criado usando este pré-mestre segredo. A chave mestra é usada para criar a chave de sessão. O segredo é criptografado por chave pública, o segredo criptografado é de 120 bytes.

11. What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?

O registro Change Cipher Spec é usado para indicar que o conteúdo dos próximos registros SSL será criptografado. São 6 bytes.

12. In the encrypted handshake record, what is being encrypted? How?

Todas as mensagens de handshake e endereços MAC são concatenados e criptografados. Eles são enviados para o servidor.

13. Does the server also send a change cipher record and an encrypted handshake record to the client? How are those records different from those sent by the client?

Sim, o handshake criptografado do servidor contém todas as mensagens de handshake enviadas do servidor. Outro contém mensagens enviadas do cliente.

14. How is the application data being encrypted? Do the records containing application data include a MAC? Does Wireshark distinguish between the encrypted application data and the MAC?

O algoritmo de criptografia simétrica é usado para criptografar os dados do aplicativo. Sim, os registros contendo dados de aplicativos incluem um MAC. Não, o Wireshark não fez distinção entre os dados de aplicativos criptografados e o MAC.

15. Comment on and explain anything else that you found interesting in the trace.

Baseando nas questões 3,4 e 5 foram utilizados dois pacotes diferentes para analisar os registros do tipo ClientHello, pois o primeiro ClientHello apresentava SSLv2, enquanto os demais apresentavam SSLv3. Sendo assim, alguns campos eram distintos entre os dois, de forma que não foi possível fazer a análise completa apenas com o primeiro ClientHello conforme pedido nas questões.