TLS (Transport Layer Security)

Fundamentos de Redes

- Guillermo Gómez Trenado
- Adrián Peláez Vegas
- José Antonio Ruiz Millán

Índice:

Definición e Historia

Índice:

1.a.- Evolución desde SSL hasta TLS

1. **Antecedentes**
2. Conceptos básicos
3. Historia

1.a.1. Antecedentes

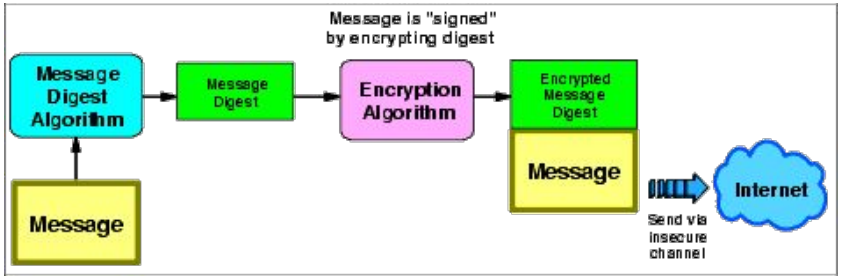
- [1994] Netscape. Protocolo seguro multipropósito (Netscape Communicator)
- Dificultad cifrado simétrico (Compartir)
- [1976] Whitfield Diffie y Martin Hellman desarrollan *Public Key Cryptography*. [Inteligencia británica ya lo había desarrollado y utilizado 1970-1974]

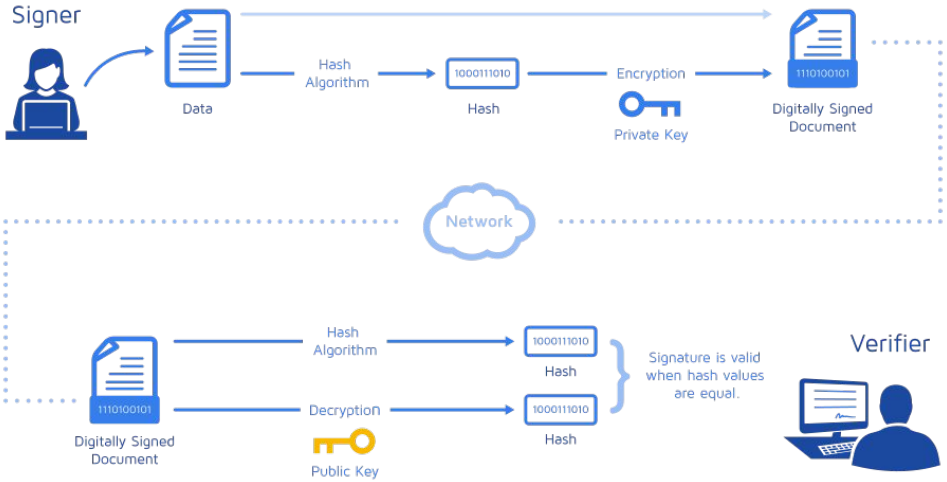
1.a.- Evolución desde SSL hasta TLS

1. Antecedentes
2. **Conceptos básicos**
3. Historia

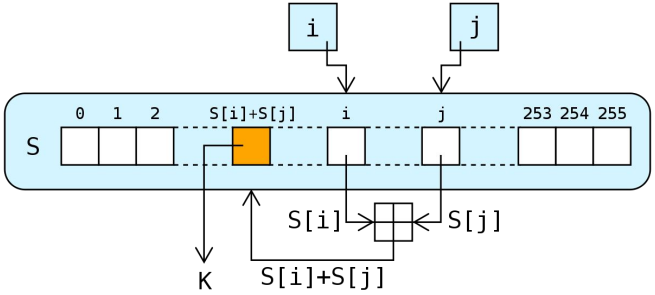
1.a.2. Conceptos básicos

A. **Encriptación**
B. **Message Digest**
C. **Firma digital**
D. **Certificado**





1.a.2. Conceptos básicos



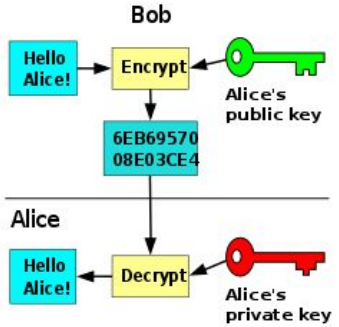
D. Encriptación Simétrica

1. **Stream Ciphers**
   a. RC4. Único de uso masivo (Junto a MAC)
2. **Block Ciphers**

   CBC->C[i]=E(K,M[i] xor C[i-1]) Evita analizar el tráfico con dos paquetes idénticos y reconocer patrones.

   a. DES (NSA asiste en su diseño) [56bits] Vulnerable meet-in-the-middle [WEAK]
   b. 3DES (DESx3) Ek1(Ek2(Ek3(M))) [WEAK]
   c. RC2 [64bit] 2^**40**(**Apto para exportación**) [WEAK]
   d. AES (TLS 1.1)
   e. Camellia (TLS 1.1)
   f. ARIA (TLS 1.1)
   g. ChaCha20 (TLS 1.2)
3. MAC (Integridad)
   a. MAC ad-hoc (inseguros), DES-MAC(lentos)
   b. HMAC. HMAC(K,M) = H(K xor (0x36||H(K xor 0x5x||M) H={MD5,SHA1,SHA256/384)
   c. AEAD (TLS 1.2)

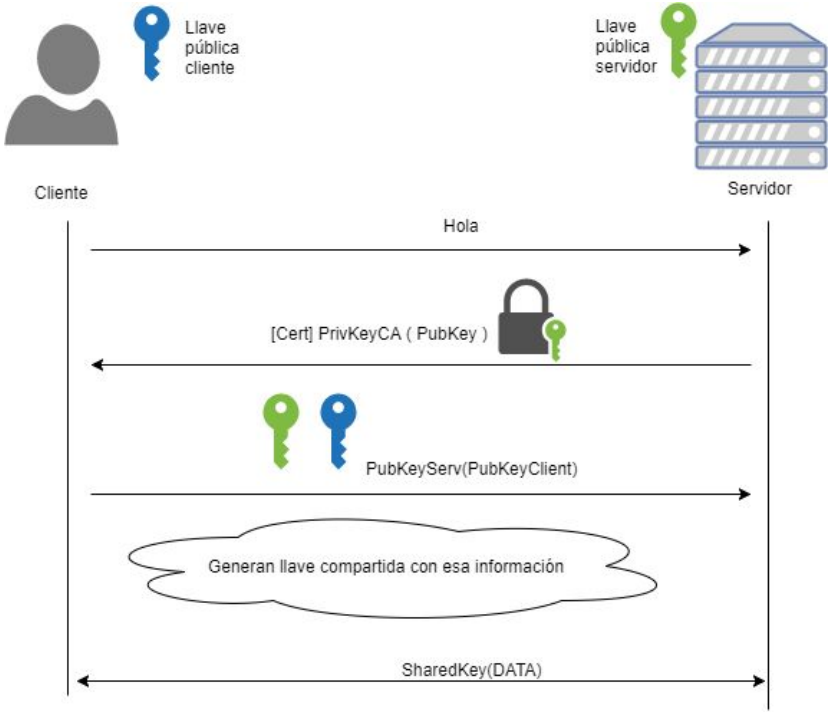
1.a.2. Conceptos básicos



E. Encriptación Asimétrica

1. **Generar clave simétrica**
   a. **RSA**.
      i. Priv: p,q,e. Pub: n, e. n=p*q, e primo relativo (p-1)*(q-1), e ~= {3,17,65537}
      ii. Client envía Session-key
   b. **Diffie-Hellman** DH.
      i. ZZ =[Sender] Yr^Xs mod p = Ys^Xr [Receiver] mod p. X=PrivKey, Y=PubKey, p=”gran primo”
      ii. Session-key se construye por separado
2. **Firma digital**
   a. RSA
      i. PrivK(MD(M)) = S -> PubK(S) == MD(M)
   b. DSS
      i. Parecido a DH

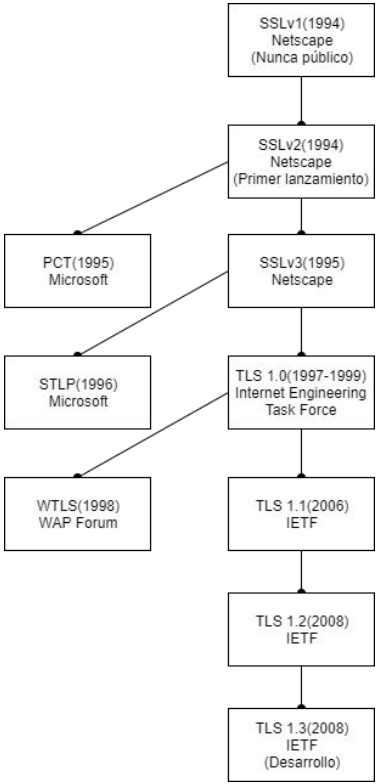
1.a.2. Conceptos básicos



1.a.- Evolución desde SSL hasta TLS

1. Antecedentes
2. Conceptos básicos
3. **Historia**

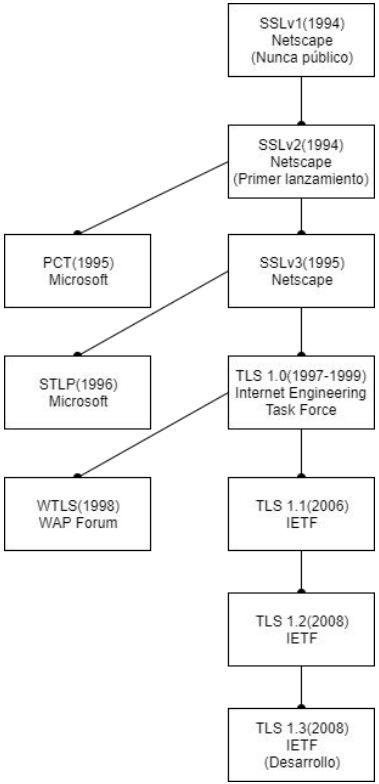
1.a.3. Historia



Objetivos

1. **Transparente** (Emular SOCKET TCP)
2. **Garantizar** (Tarjetas de crédito)
   a. **Confidencialidad**
   b. **Integridad**
   c. **Verificar partes** (Al menos al servidor)
   d. **Espontaneidad**
   e. **No repudio**

1.a.3. Historia



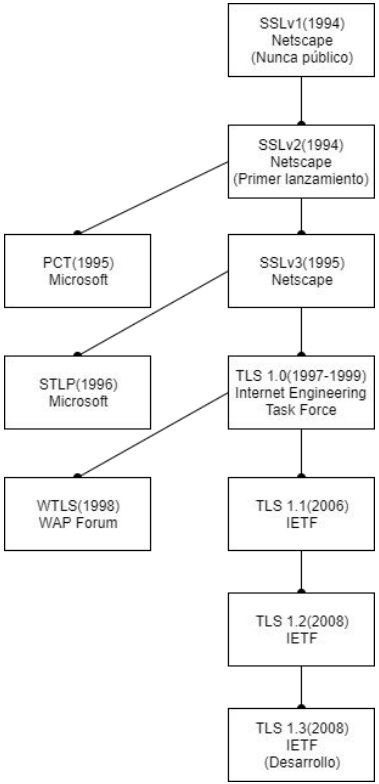
SSL 1.0 Nunca fue público | Tremendamente inseguro

1. **No integridad** (MAC)
2. RC4 (Stream Cipher sin integridad, realizar cambios)
3. Sin **número de secuencia** (reply attack)

SSL 2.0 (1995) [fallas de seguridad]:

1. **Primer ataque**: Wagner and Goldberd: RSA -> RNG seed hora y PID [Goldberg 1996]
2. Diferencias:
   a. Cliente elige cipher (respondidos por server)
3. Características que faltan:
   a. Encadenación de **certificados** (Sólo CA root)
   b. Mismo RSA para **exportación y uso doméstico** (américa)
4. Problemas de seguridad:
   1. Misma clave MAC y encriptación (Weak)
   2. MAC débil (MD5) -> **HMAC (SHA-1)**
   3. **Downgrade** (No SSL)
   4. **Truncation**

1.a.3. Historia



SSL 3.0 (1996) (**Desde 0**)

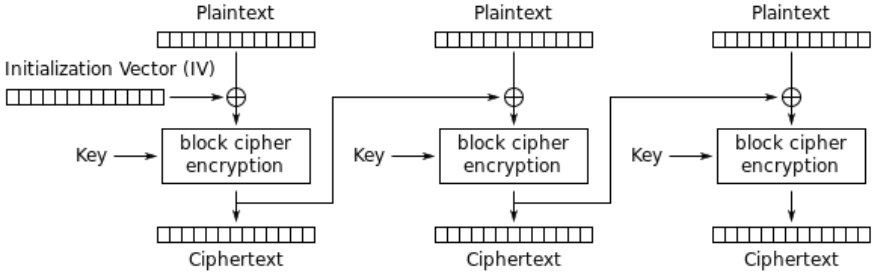
1. Auth-only
2. Nuevos ciphers
3. **Closure-handshake**

TLS 1.0 (IETF) [RFC 2246]

1. **IETF** con soporte Microsoft, Netscape principalmente (**Poco apoyo** cambios)
2. IETF Prioridad **seguridad**, EMPRESAS Prioridad **exportabilidad**.
3. **Nombre** del protocolo (Netscape SSL, Microsoft STLP)
4. Dificultades **retrocompatibilidad**
5. Mayores cambios, soporte **nuevos ciphers** (Problema **NSA**)
6. Tardó mucho en salir porque dependían de **X.509**

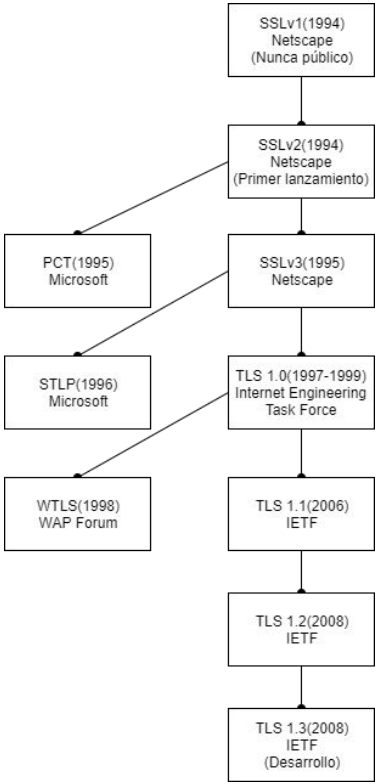
TLS 1.1 [RFC 4346]

1. Protección **Cipher block chaining [IV]**



Cipher Block Chaining (CBC) mode encryption

1.a.3. Historia



TLS 1.2 [RFC 5246]

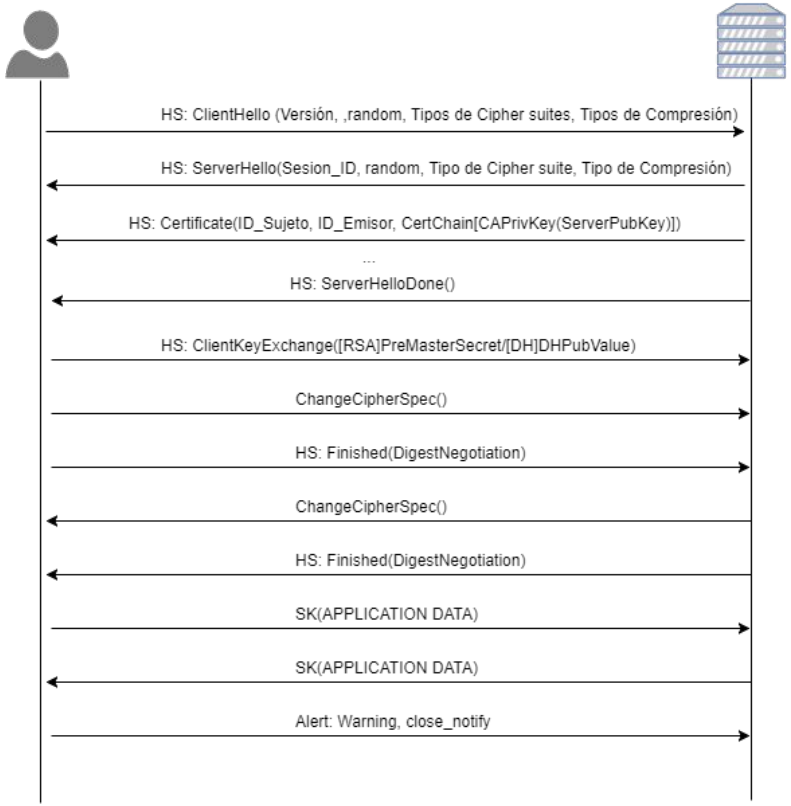
1. Desplazar **MD5 por SHA-256**
2. Mejoras acuerdo para elegir cifrado

TLS 1.3 (https://tools.ietf.org/html/draft-ietf-tls-tls13-21)

1. **Eliminar** soporte **MD5** y SHA-224 (MAC)
2. Eliminar soporte **compresión**
3. Eliminar soporte **cifrados** o configuraciones inseguras
4. Prohibir negociación de **SSL o RC4** para retrocompatibilidad (Problema servidores antiguos, RC4 actualmente usado para evitar BEAST Attack (CBC attack)

Índice:

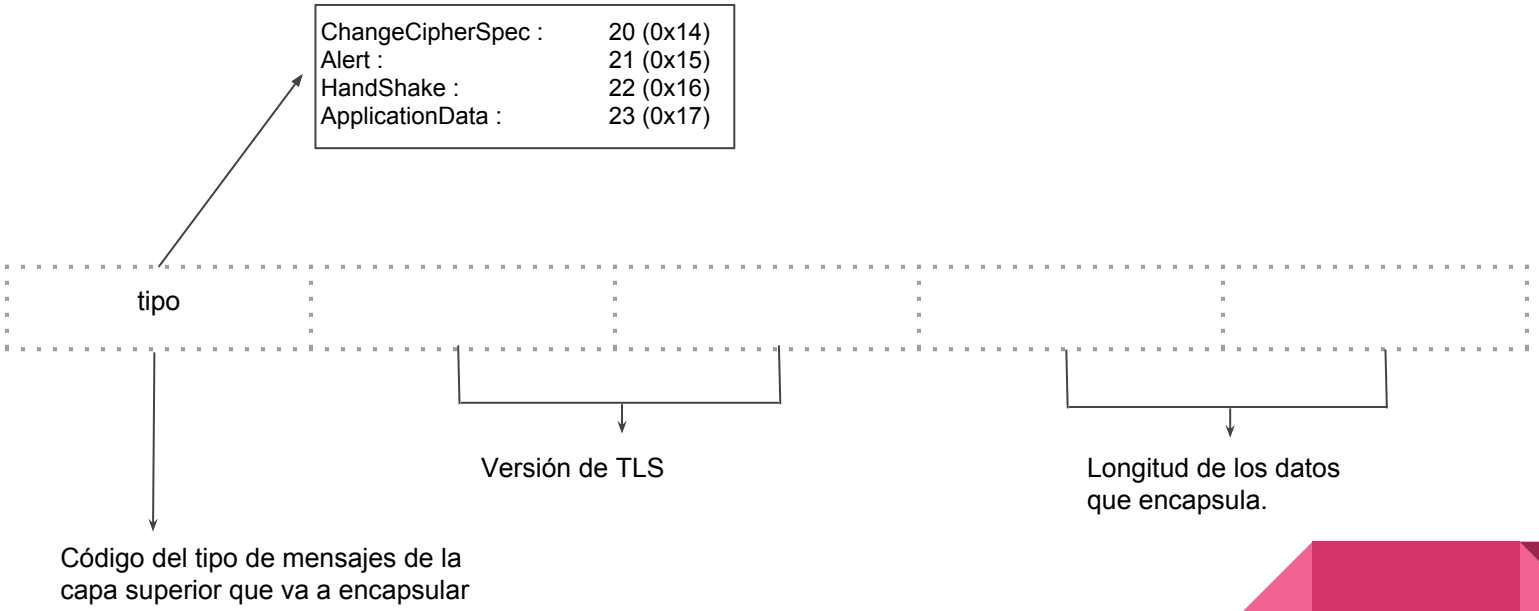
1.b.- Descripción TLS (Básico)



Análisis tráfico TLS (Wireshark)

Índice:

2.a.1. Record layer (capa inferior)



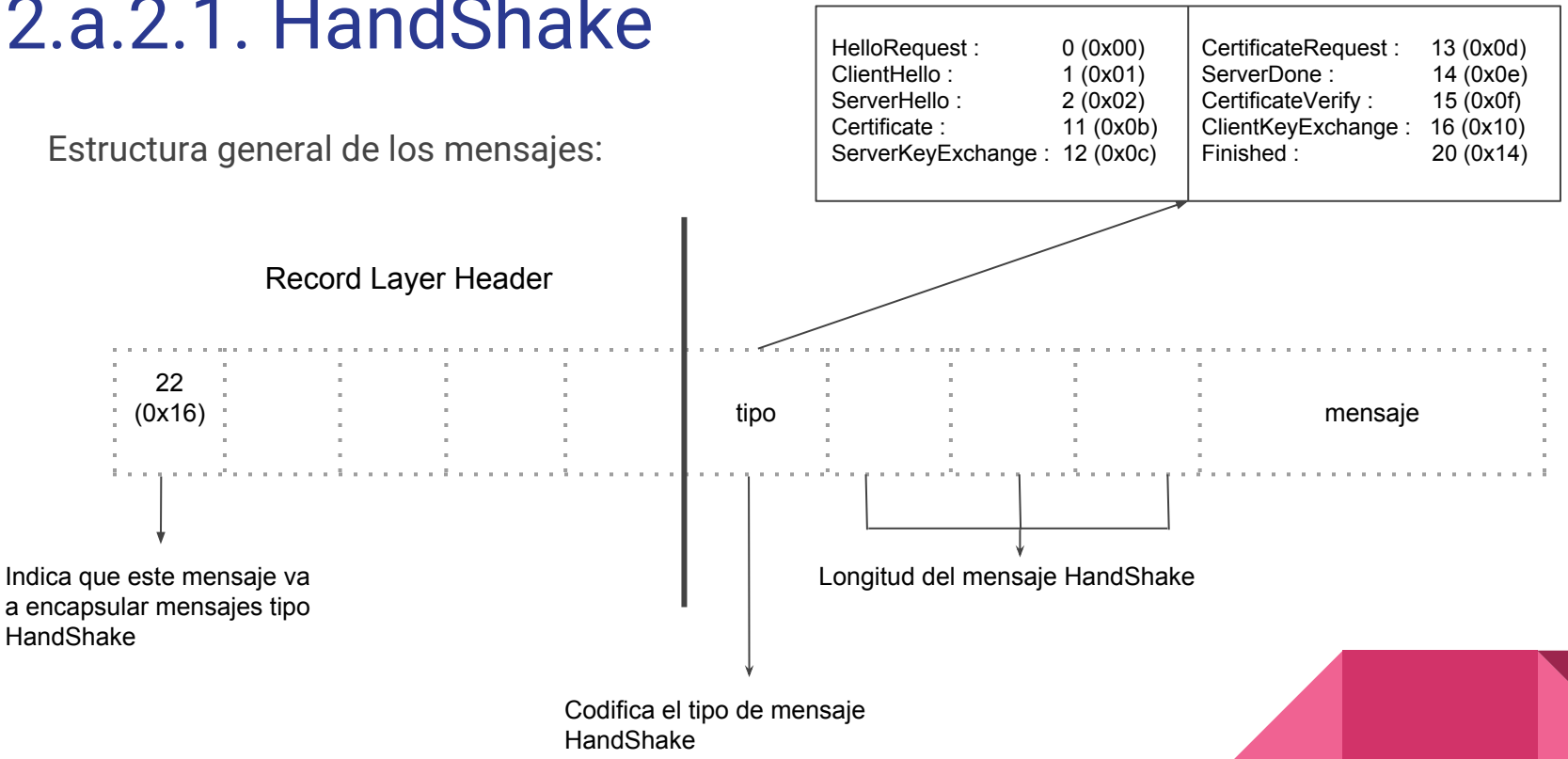
2.a.2. Higher layer (capa superior)

Esta capa se compone de 4 subprotocolos, cada uno de ellos con un propósito muy específico:

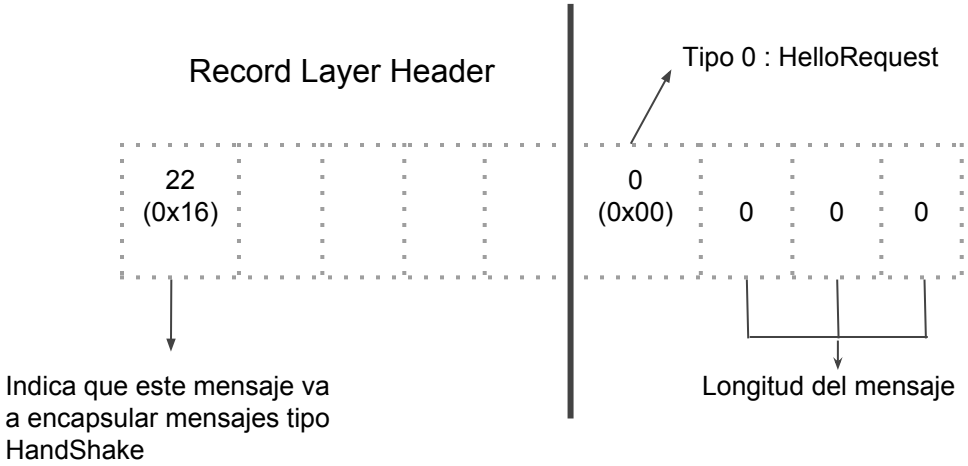
- HandShake
- ChangeCipherSpec
- Alert
- Application Data

2.a.2.1. HandShake

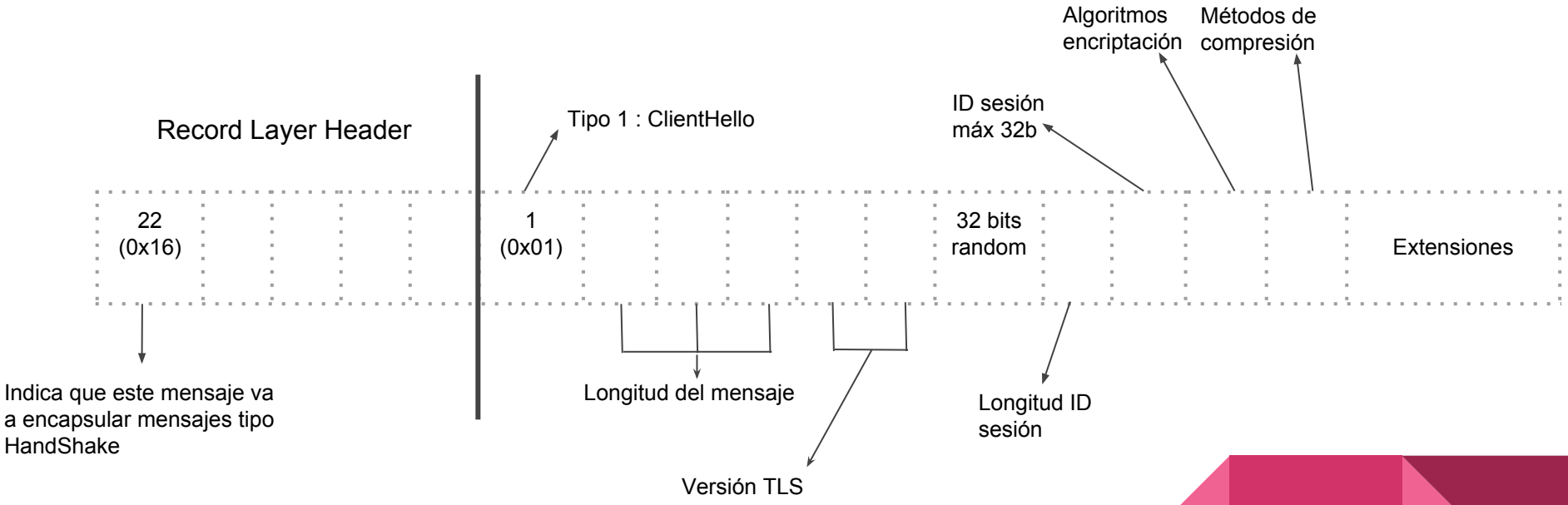
Estructura general de los mensajes:



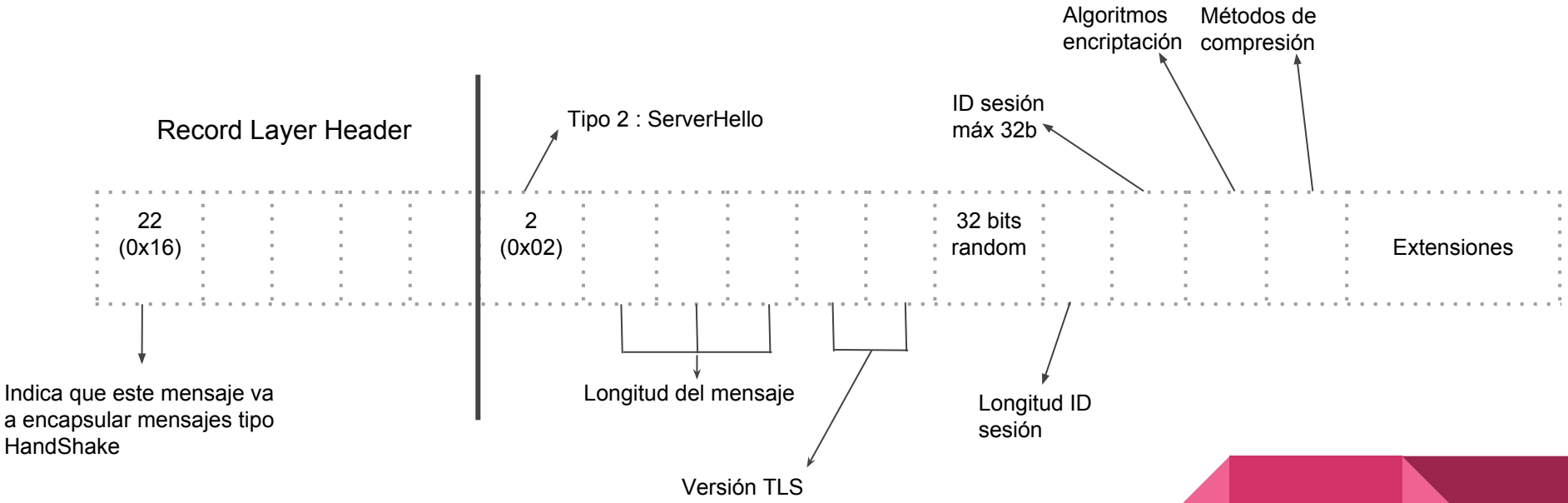
2.a.2.1.1. HandShake -> HelloRequest



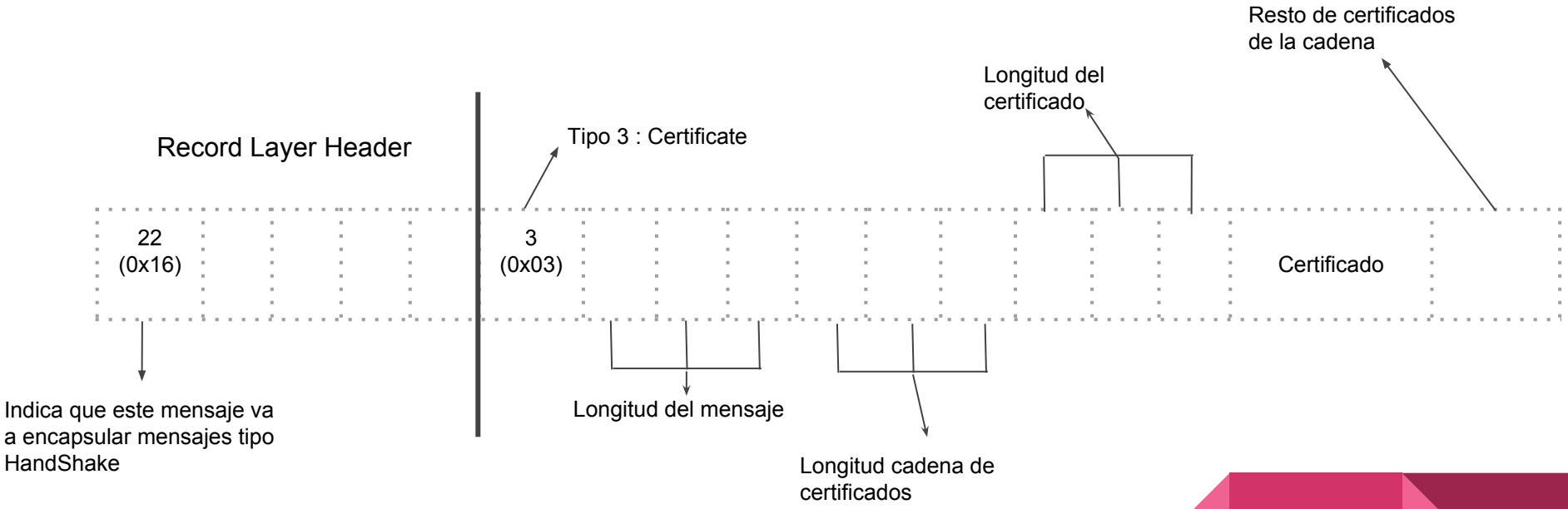
2.a.2.1.2. HandShake -> ClientHello



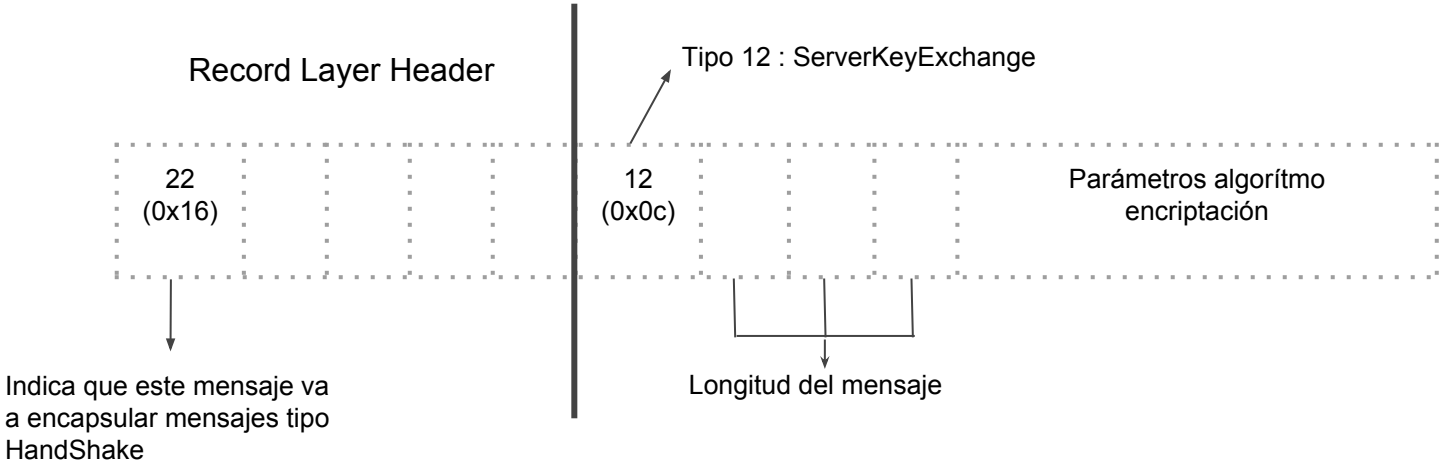
2.a.2.1.3. HandShake -> ServerHello



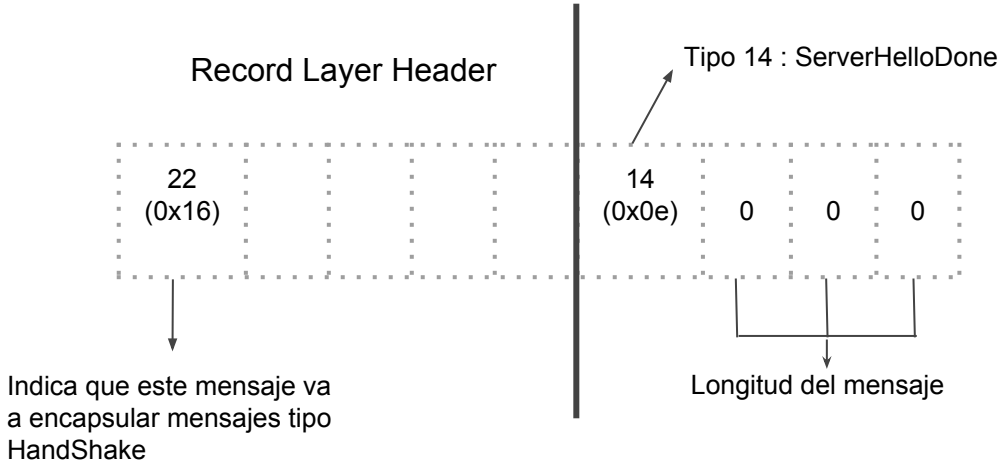
2.a.2.1.4. HandShake -> Certificate



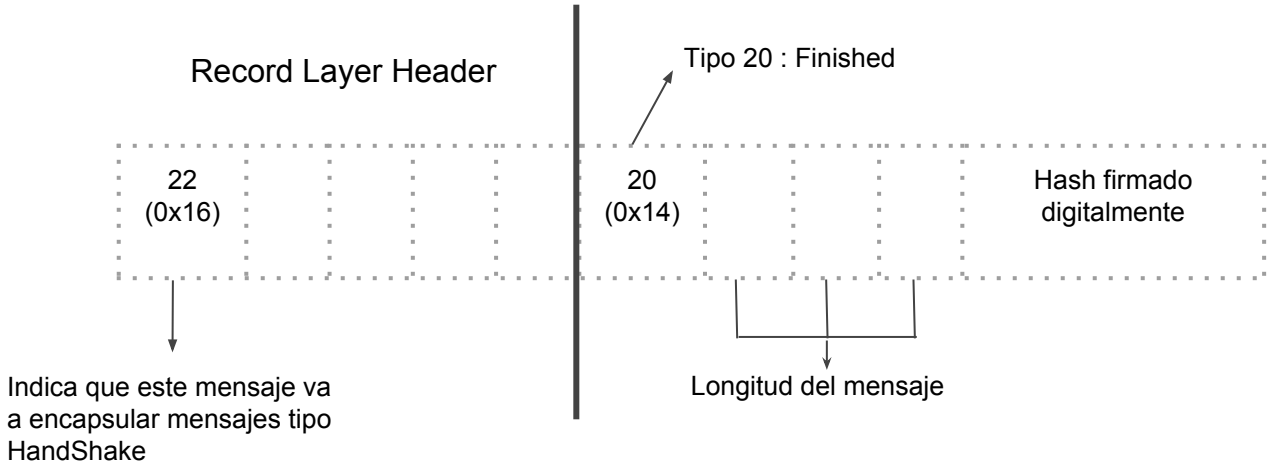
2.a.2.1.6. HandShake -> ServerKeyExchange ClientKeyExchange



2.a.2.1.7. HandShake -> ServerHelloDone

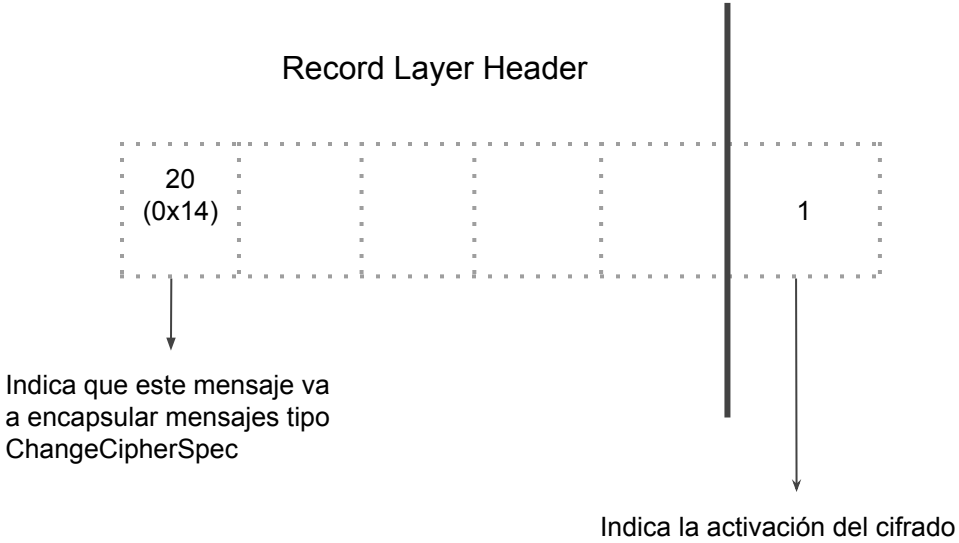


2.a.2.1.8. HandShake -> Finished



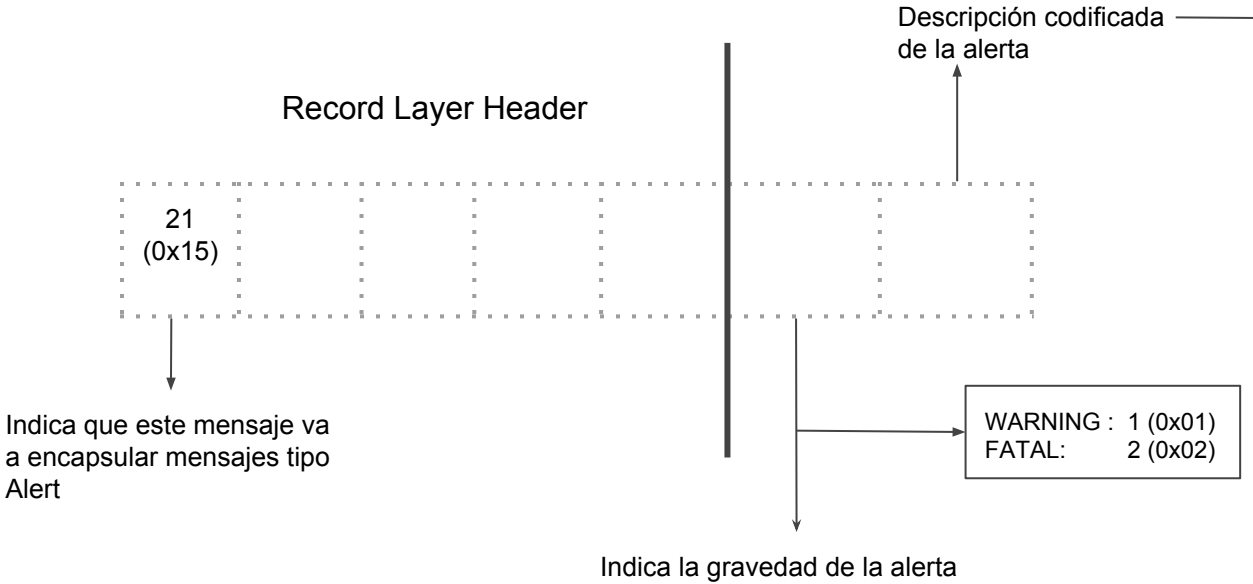
2.a.2.2. ChangeCipherSpec

Estructura general de los mensajes:



2.a.2.3. Alert

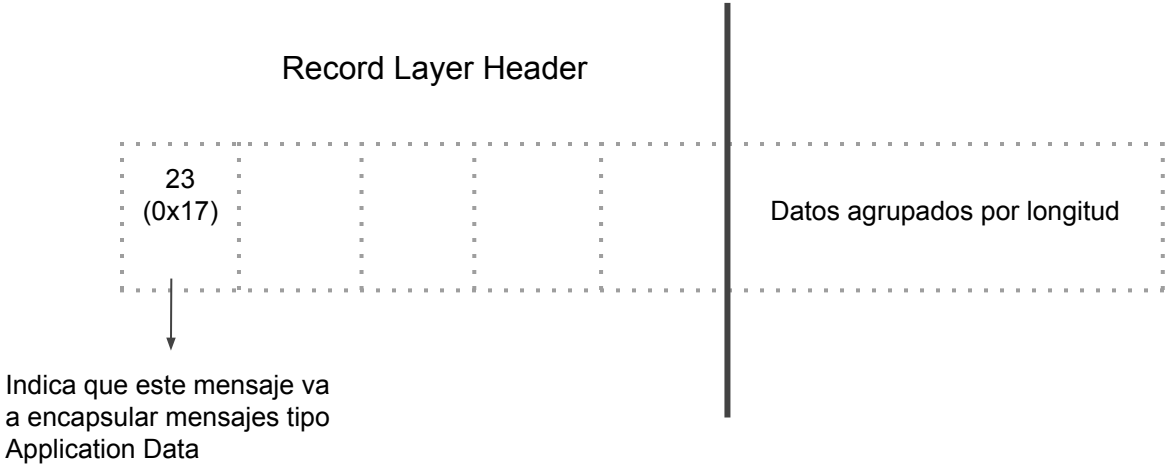
Estructura general de los mensajes:



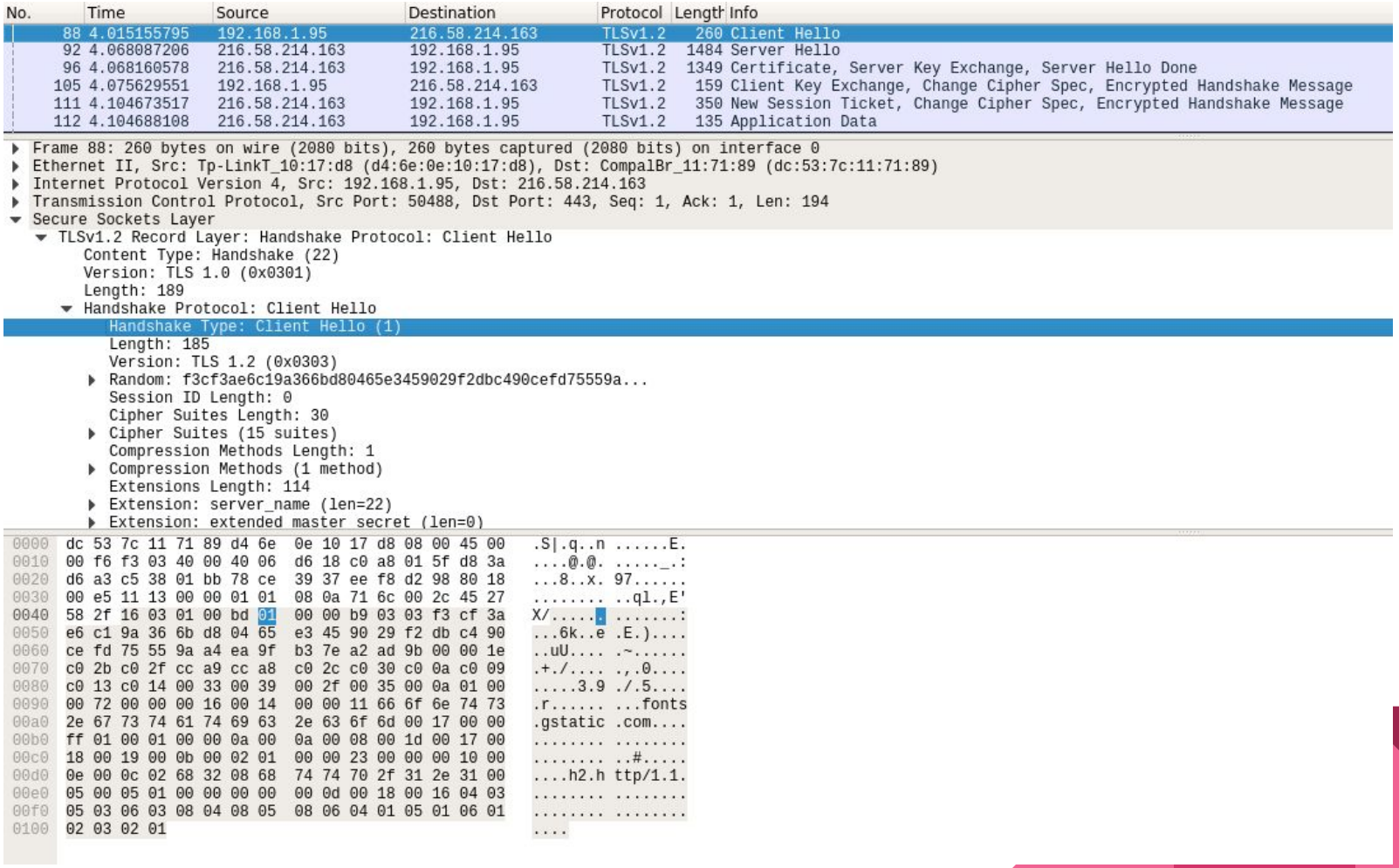
CLOSE_NOTIFY	0	0x00
UNEXPECTED_MESSAGE	10	0x0A
BAD_RECORD_MAC	20	0x14
DECRYPTION_FAILED	21	0x15
RECORD_OVERFLOW	22	0x16
DECOMPRESSION_FAILURE	30	0x1E
HANDSHAKE_FAILURE	40	0x28
NO_CERTIFICATE	41	0x29
BAD_CERTIFICATE	42	0x2A
UNSUPPORTED_CERTIFICATE	43	0x2B
CERTIFICATE_REVOKED	44	0x2C
CERTIFICATE_EXPIRED	45	0x2D
CERTIFICATE_UNKNOWN	46	0x2E
ILLEGAL_PARAMETER	47	0x2F
UNKNOWN_CA	48	0x30
ACCESS_DENIED	49	0x31
DECODE_ERROR	50	0x32
DECRYPT_ERROR	51	0x33
EXPORT_RESTRICTION	60	0x3C
PROTOCOL_VERSION	70	0x46
INSUFFICIENT_SECURITY	71	0x47
INTERNAL_ERROR	80	0x50
USER_CANCELLED	90	0x5A
NO_RENEGOTIATION	100	0x64

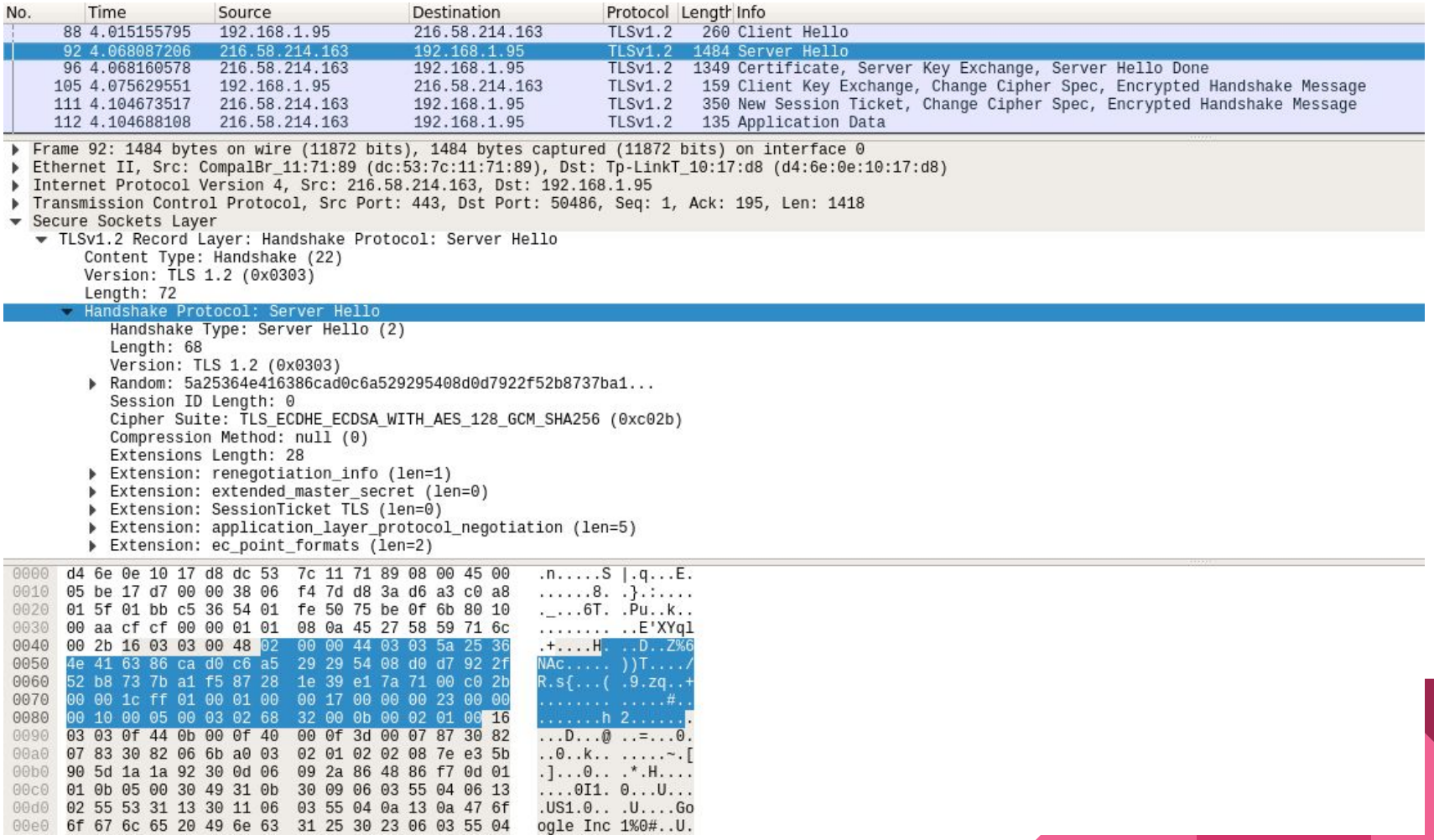
2.a.2.4. Application Data

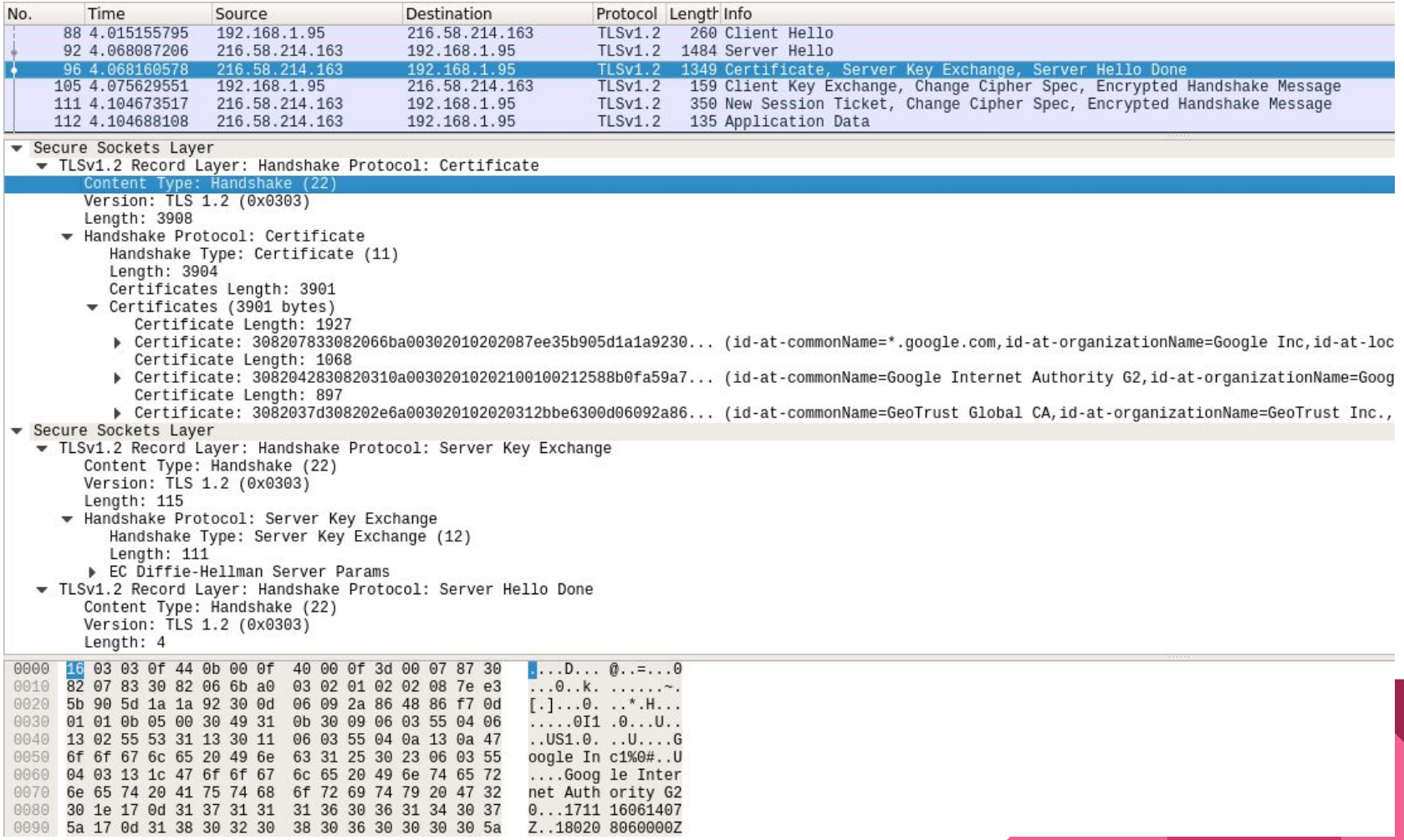
Estructura general de los mensajes:

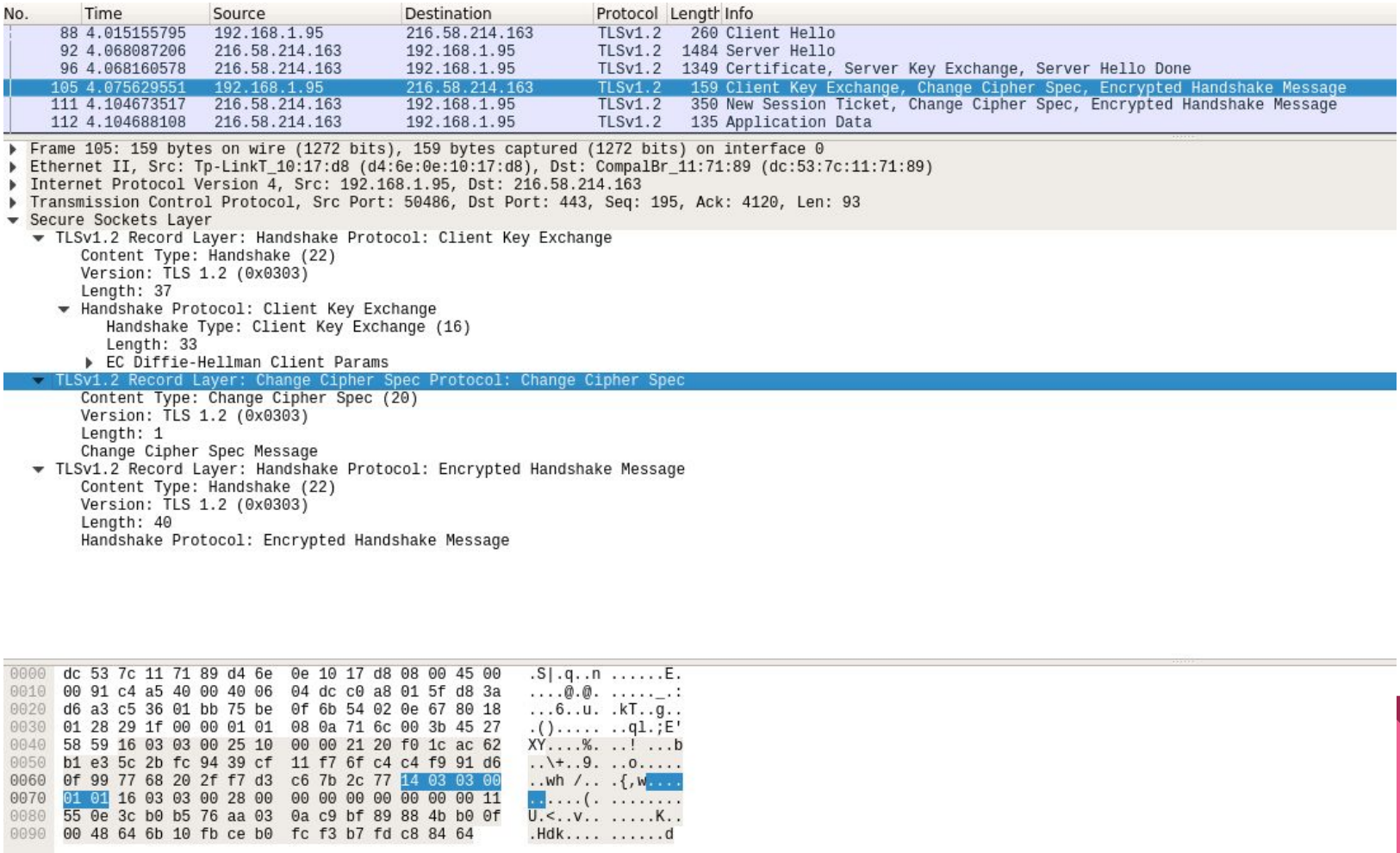


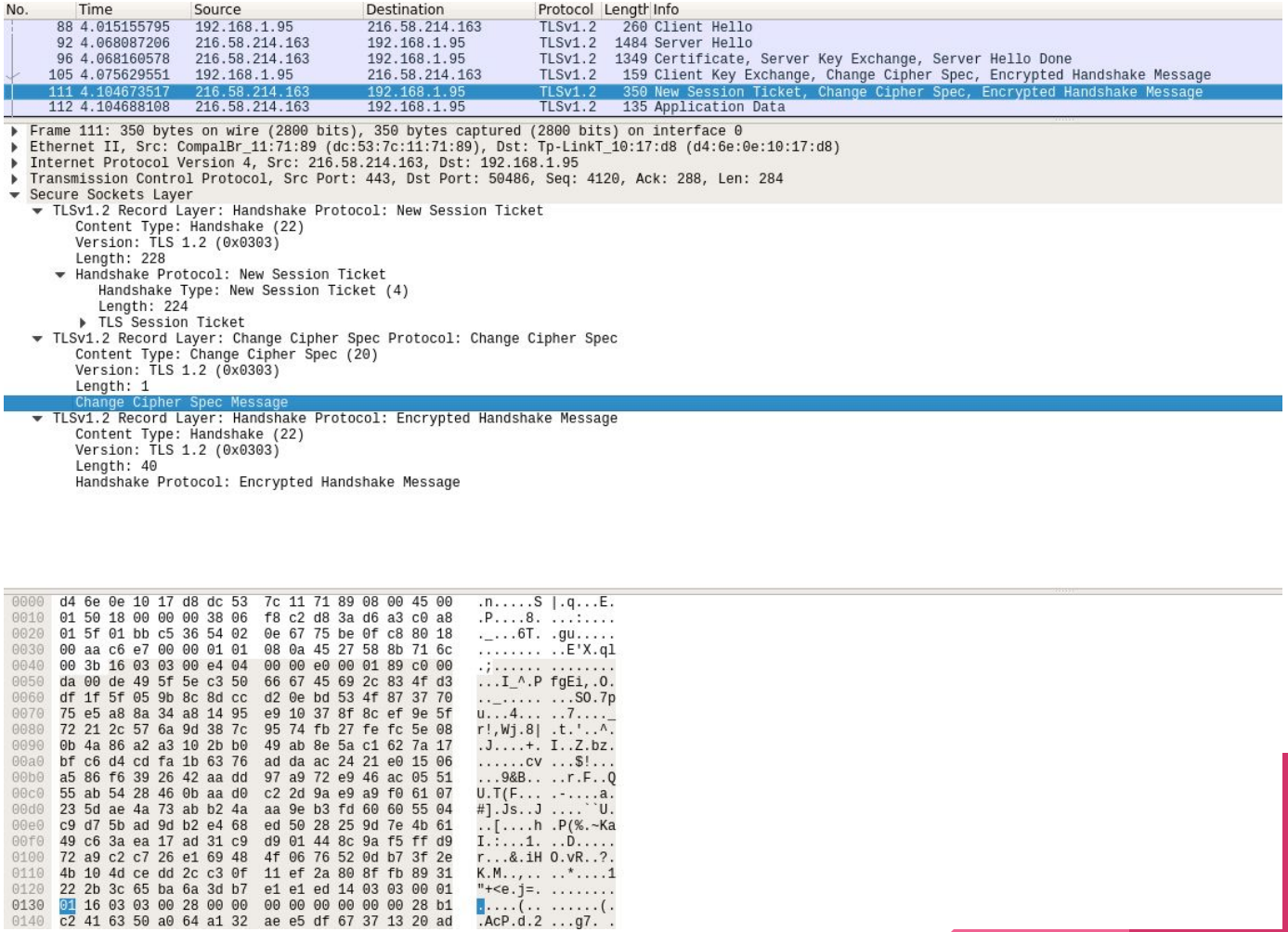
Índice:

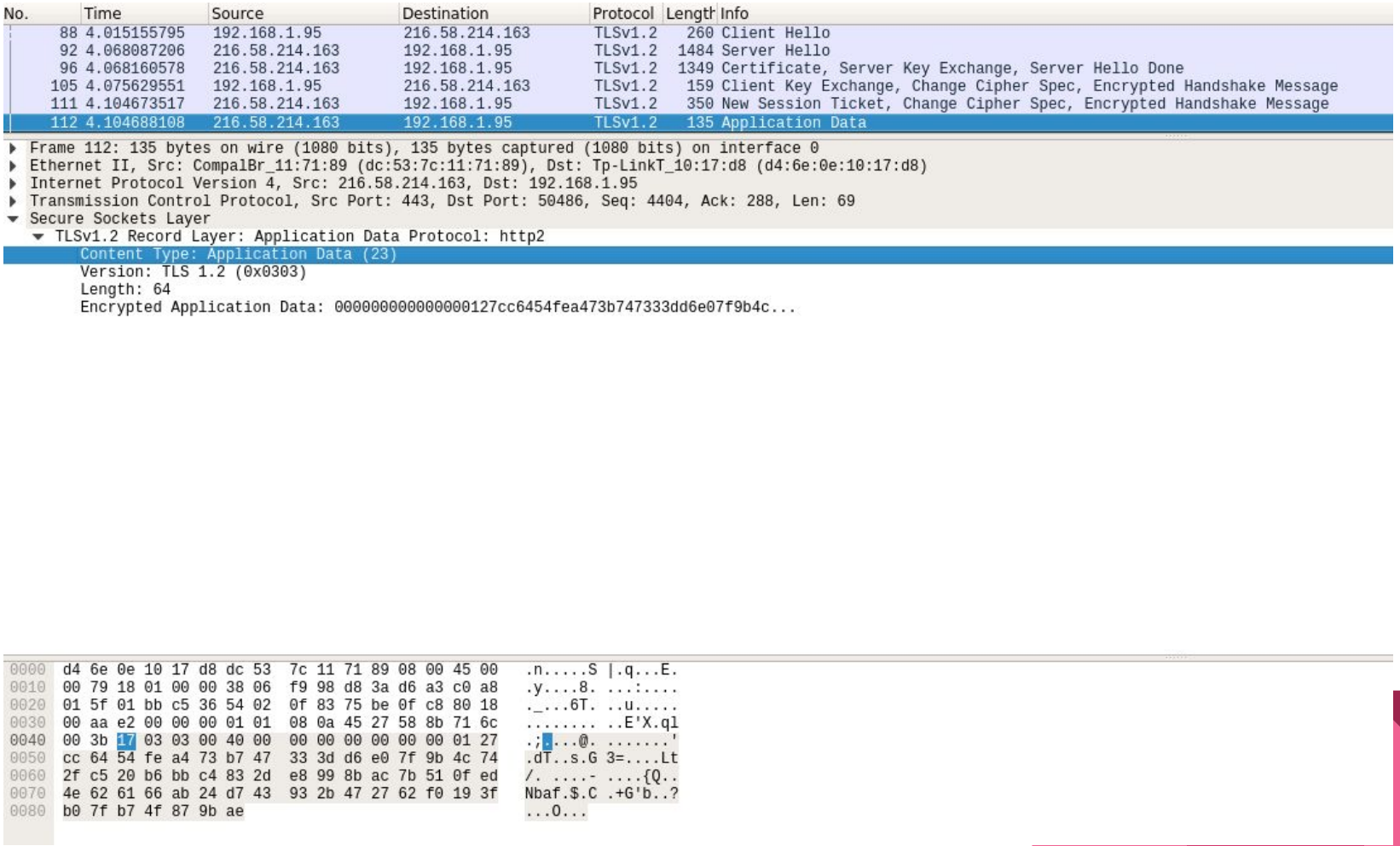

No. Time Source Destination Protocol Length Info
88 4.015155795 192.168.1.95 216.58.214.163 TLSv1.2 260 Client Hello
92 4.068087206 216.58.214.163 192.168.1.95 TLSv1.2 1484 Server Hello
96 4.068160578 216.58.214.163 192.168.1.95 TLSv1.2 1349 Certificate, Server Key Exchange, Server Hello Done
105 4.075629551 192.168.1.95 216.58.214.163 TLSv1.2 159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
111 4.104673517 216.58.214.163 192.168.1.95 TLSv1.2 350 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
112 4.104688108 216.58.214.163 192.168.1.95 TLSv1.2 135 Application Data
Frame 88: 260 bytes on wire (2080 bits), 260 bytes captured (2080 bits) on interface 0
Ethernet II, Src: Tp-LinkT_10:17:d8 (d4:6e:0e:10:17:d8), Dst: CompalBr_11:71:89 (dc:53:7c:11:71:89)
Internet Protocol Version 4, Src: 192.168.1.95, Dst: 216.58.214.163
Transmission Control Protocol, Src Port: 50488, Dst Port: 443, Seq: 1, Ack: 1, Len: 194
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 189
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 185
Version: TLS 1.2 (0x0303)
Random: f3cf3ae6c19a366bd80465e3459029f2dbc490cefd75559a...
Session ID Length: 0
Cipher Suites Length: 30
Cipher Suites (15 suites)
Compression Methods Length: 1
Compression Methods (1 method)
Extensions Length: 114
Extension: server_name (len=22)
Extension: extended master secret (len=0)
0000 dc 53 7c 11 71 89 d4 6e 0e 10 17 d8 08 00 45 00 .S|.q..n ......E.
0010 00 f6 f3 03 40 00 40 06 d6 18 c0 a8 01 5f d8 3a ....@.@. ....._.:
0020 d6 a3 c5 38 01 bb 78 ce 39 37 ee f8 d2 98 80 18 ...8..x. 97......
0030 00 e5 11 13 00 00 01 01 08 0a 71 6c 00 2c 45 27 ....ql.,E'
0040 58 2f 16 03 01 00 bd 01 00 00 b9 03 03 f3 cf 3a X/...... ....:
0050 e6 c1 9a 36 6b d8 04 65 e3 45 90 29 f2 db c4 90 ...6k..e .E.)....
0060 ce fd 75 55 9a a4 ea 9f b3 7e a2 ad 9b 00 00 1e ..uU.... .~......
0070 c0 2b c0 2f cc a9 cc a8 c0 2c c0 30 c0 0a c0 09 .+./.... .,.0....
0080 c0 13 c0 14 00 33 00 39 00 2f 00 35 00 0a 01 00 .....3.9 ./.5....
0090 00 72 00 00 00 16 00 14 00 00 11 66 6f 6e 74 73 .r..... ...fonts
00a0 2e 67 73 74 61 74 69 63 2e 63 6f 6d 00 17 00 00 .gstatic .com....
00b0 ff 01 00 01 00 00 0a 00 0a 00 08 00 1d 00 17 00 ....
00c0 18 00 19 00 0b 00 02 01 00 00 23 00 00 00 10 00 ....#.....
00d0 0e 00 0c 02 68 32 08 68 74 74 70 2f 31 2e 31 00 ....h2.h ttp/1.1.
00e0 05 00 05 01 00 00 00 00 00 0d 00 18 00 16 04 03 ....
00f0 05 03 06 03 08 04 08 05 08 06 04 01 05 01 06 01 ....
0100 02 03 02 01 ....

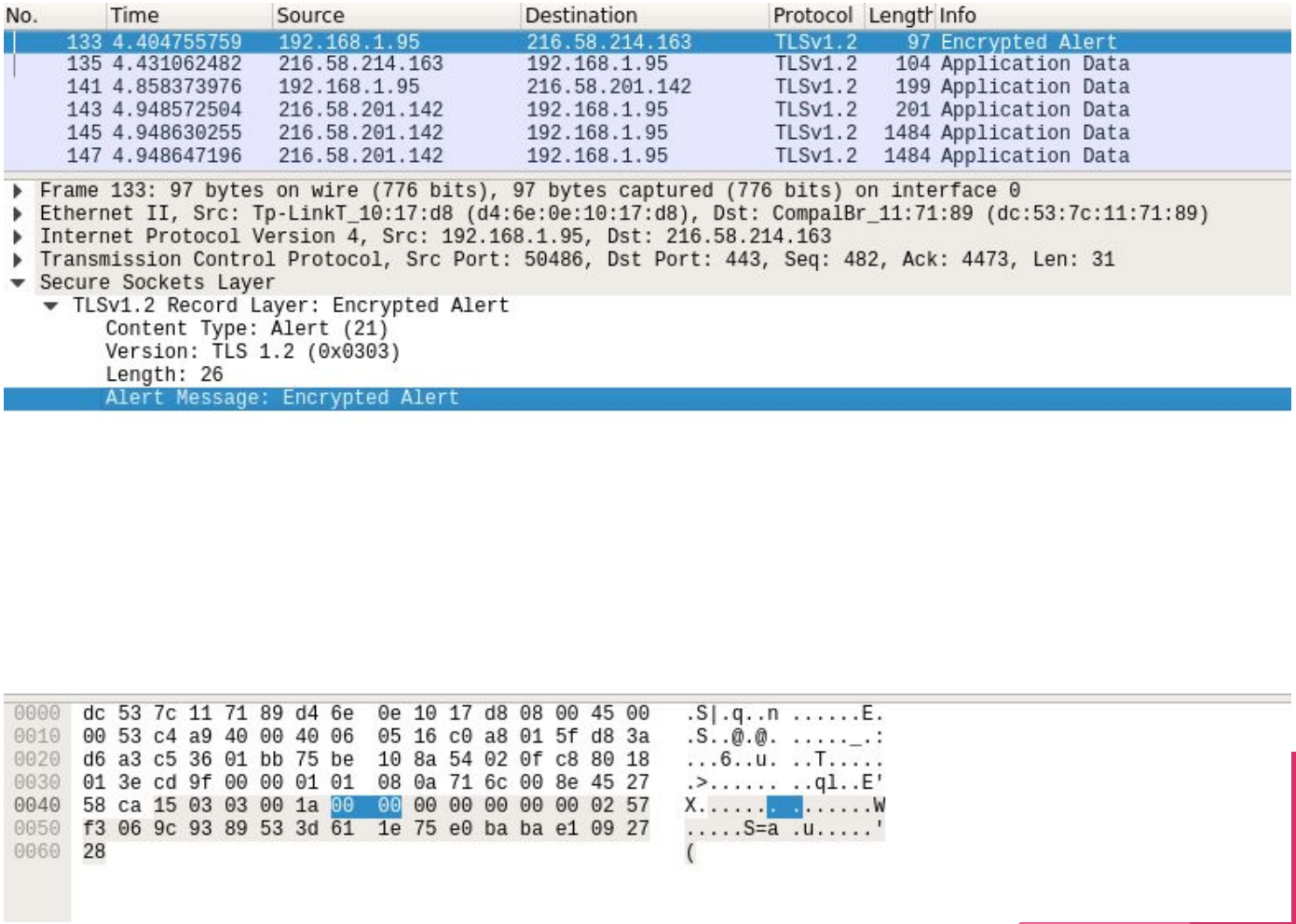

No. Time Source Destination Protocol Length Info
88 4.015155795 192.168.1.95 216.58.214.163 TLSv1.2 260 Client Hello
92 4.068087206 216.58.214.163 192.168.1.95 TLSv1.2 1484 Server Hello
96 4.068160578 216.58.214.163 192.168.1.95 TLSv1.2 1349 Certificate, Server Key Exchange, Server Hello Done
105 4.075629551 192.168.1.95 216.58.214.163 TLSv1.2 159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
111 4.104673517 216.58.214.163 192.168.1.95 TLSv1.2 350 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
112 4.104688108 216.58.214.163 192.168.1.95 TLSv1.2 135 Application Data
Frame 92: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interface 0
Ethernet II, Src: CompalBr_11:71:89 (dc:53:7c:11:71:89), Dst: Tp-LinkT_10:17:d8 (d4:6e:0e:10:17:d8)
Internet Protocol Version 4, Src: 216.58.214.163, Dst: 192.168.1.95
Transmission Control Protocol, Src Port: 443, Dst Port: 50486, Seq: 1, Ack: 195, Len: 1418
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 72
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 68
Version: TLS 1.2 (0x0303)
Random: 5a25364e416386cad0c6a529295408d0d7922f52b8737ba1...
Session ID Length: 0
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Compression Method: null (0)
Extensions Length: 28
Extension: renegotiation_info (len=1)
Extension: extended_master_secret (len=0)
Extension: SessionTicket TLS (len=0)
Extension: application_layer_protocol_negotiation (len=5)
Extension: ec_point_formats (len=2)
0000 d4 6e 0e 10 17 d8 dc 53 7c 11 71 89 08 00 45 00 .n.....S |.q...E.
0010 05 be 17 d7 00 00 38 06 f4 7d d8 3a d6 a3 c0 a8 ......8. .}.:....
0020 01 5f 01 bb c5 36 54 01 fe 50 75 be 0f 6b 80 10 ._...6T. .Pu..k..
0030 00 aa cf cf 00 00 01 01 08 0a 45 27 58 59 71 6c ....E'XYql
0040 00 2b 16 03 03 00 48 02 00 00 44 03 03 5a 25 36 .+....H. ..D..Z%6
0050 4e 41 63 86 ca d0 c6 a5 29 29 54 08 d0 d7 92 2f NAc.....))T..../
0060 52 b8 73 7b a1 f5 87 28 1e 39 e1 7a 71 00 c0 2b R.s{...(.9.zq..+
0070 00 00 1c ff 01 00 01 00 00 17 00 00 00 23 00 00 ....#..
0080 00 10 00 05 00 03 02 68 32 00 0b 00 02 01 00 16 ....h 2.......
0090 03 03 0f 44 0b 00 0f 40 00 0f 3d 00 07 87 30 82 ...D...@ ..=...0.
00a0 07 83 30 82 06 6b a0 03 02 01 02 02 08 7e e3 5b ..0..k.. .....~.[
00b0 90 5d 1a 1a 92 30 0d 06 09 2a 86 48 86 f7 0d 01 .]...0.. .*.H....
00c0 01 0b 05 00 30 49 31 0b 30 09 06 03 55 04 06 13 ....0I1. 0...U...
00d0 02 55 53 31 13 30 11 06 03 55 04 0a 13 0a 47 6f .US1.0.. .U....Go
00e0 6f 67 6c 65 20 49 6e 63 31 25 30 23 06 03 55 04 ogle Inc 1%0#..U.


No. Time Source Destination Protocol Length Info
88 4.015155795 192.168.1.95 216.58.214.163 TLSv1.2 260 Client Hello
92 4.068087206 216.58.214.163 192.168.1.95 TLSv1.2 1484 Server Hello
96 4.068160578 216.58.214.163 192.168.1.95 TLSv1.2 1349 Certificate, Server Key Exchange, Server Hello Done
105 4.075629551 192.168.1.95 216.58.214.163 TLSv1.2 159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
111 4.104673517 216.58.214.163 192.168.1.95 TLSv1.2 350 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
112 4.104688108 216.58.214.163 192.168.1.95 TLSv1.2 135 Application Data
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 3908
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 3904
Certificates Length: 3901
Certificates (3901 bytes)
Certificate Length: 1927
Certificate: 308207833082066ba00302010202087ee35b905d1a1a9230... (id-at-commonName=*.google.com,id-at-organizationName=Google Inc,id-at-loc
Certificate Length: 1068
Certificate: 3082042830820310a003020102021001002125 88b0fa59a7... (id-at-commonName=Google Internet Authority G2,id-at-organizationName=Goog
Certificate Length: 897
Certificate: 3082037d308202e6a003020102020312bbe6300d06092a86... (id-at-commonName=GeoTrust Global CA,id-at-organizationName=GeoTrust Inc.,
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 115
Handshake Protocol: Server Key Exchange
Handshake Type: Server Key Exchange (12)
Length: 111
EC Diffie-Hellman Server Params
TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 4
0000 16 03 03 0f 44 0b 00 0f 40 00 0f 3d 00 07 87 30 ....D... @..=...0
0010 82 07 83 30 82 06 6b a0 03 02 01 02 02 08 7e e3 ...0..k. ......~.
0020 5b 90 5d 1a 1a 92 30 0d 06 09 2a 86 48 86 f7 0d [.]...0. ..*.H...
0030 01 01 0b 05 00 30 49 31 0b 30 09 06 03 55 04 06 .....0I1 .0...U..
0040 13 02 55 53 31 13 30 11 06 03 55 04 0a 13 0a 47 ..US1.0. ..U....G
0050 6f 6f 67 6c 65 20 49 6e 63 31 25 30 23 06 03 55 oogle In c1%0#..U
0060 04 03 13 1c 47 6f 6f 67 6c 65 20 49 6e 74 65 72 ....Goog le Inter
0070 6e 65 74 20 41 75 74 68 6f 72 69 74 79 20 47 32 net Auth ority G2
0080 30 1e 17 0d 31 37 31 31 31 36 30 36 31 34 30 37 0...1711 16061407
0090 5a 17 0d 31 38 30 32 30 38 30 36 30 30 30 30 5a Z..18020 8060000Z


No. Time Source Destination Protocol Length Info
88 4.015155795 192.168.1.95 216.58.214.163 TLSv1.2 260 Client Hello
92 4.068087206 216.58.214.163 192.168.1.95 TLSv1.2 1484 Server Hello
96 4.068160578 216.58.214.163 192.168.1.95 TLSv1.2 1349 Certificate, Server Key Exchange, Server Hello Done
105 4.075629551 192.168.1.95 216.58.214.163 TLSv1.2 159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
111 4.104673517 216.58.214.163 192.168.1.95 TLSv1.2 350 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
112 4.104688108 216.58.214.163 192.168.1.95 TLSv1.2 135 Application Data
Frame 105: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface 0
Ethernet II, Src: Tp-LinkT_10:17:d8 (d4:6e:0e:10:17:d8), Dst: CompalBr_11:71:89 (dc:53:7c:11:71:89)
Internet Protocol Version 4, Src: 192.168.1.95, Dst: 216.58.214.163
Transmission Control Protocol, Src Port: 50486, Dst Port: 443, Seq: 195, Ack: 4120, Len: 93
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 37
Handshake Protocol: Client Key Exchange
Handshake Type: Client Key Exchange (16)
Length: 33
EC Diffie-Hellman Client Params
TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.2 (0x0303)
Length: 1
Change Cipher Spec Message
TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 40
Handshake Protocol: Encrypted Handshake Message
0000 dc 53 7c 11 71 89 d4 6e 0e 10 17 d8 08 00 45 00 .S|.q..n ......E.
0010 00 91 c4 a5 40 00 40 06 04 dc c0 a8 01 5f d8 3a ....@.@. ....._.:
0020 d6 a3 c5 36 01 bb 75 be 0f 6b 54 02 0e 67 80 18 ...6..u. .kT..g..
0030 01 28 29 1f 00 00 01 01 08 0a 71 6c 00 3b 45 27 .()..... ..ql.;E'
0040 58 59 16 03 03 00 25 10 00 00 21 20 f0 1c ac 62 XY....%. ..! ...b
0050 b1 e3 5c 2b fc 94 39 cf 11 f7 6f c4 c4 f9 91 d6 ..\+..9. ..o.....
0060 0f 99 77 68 20 2f f7 d3 c6 7b 2c 77 14 03 03 00 ..wh /.. .{,w....
0070 01 01 16 03 03 00 28 00 00 00 00 00 00 00 11 ......(. ....
0080 55 0e 3c b0 b5 76 aa 03 0a c9 bf 89 88 4b b0 0f U.<..v.. .....K..
0090 00 48 64 6b 10 fb ce b0 fc f3 b7 fd c8 84 64 .Hdk.... ......d


No. Time Source Destination Protocol Length Info
88 4.015155795 192.168.1.95 216.58.214.163 TLSv1.2 260 Client Hello
92 4.068087206 216.58.214.163 192.168.1.95 TLSv1.2 1484 Server Hello
96 4.068160578 216.58.214.163 192.168.1.95 TLSv1.2 1349 Certificate, Server Key Exchange, Server Hello Done
105 4.075629551 192.168.1.95 216.58.214.163 TLSv1.2 159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
111 4.104673517 216.58.214.163 192.168.1.95 TLSv1.2 350 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
112 4.104688108 216.58.214.163 192.168.1.95 TLSv1.2 135 Application Data
Frame 111: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface 0
Ethernet II, Src: CompalBr_11:71:89 (dc:53:7c:11:71:89), Dst: Tp-LinkT_10:17:d8 (d4:6e:0e:10:17:d8)
Internet Protocol Version 4, Src: 216.58.214.163, Dst: 192.168.1.95
Transmission Control Protocol, Src Port: 443, Dst Port: 50486, Seq: 4120, Ack: 288, Len: 284
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 228
Handshake Protocol: New Session Ticket
Handshake Type: New Session Ticket (4)
Length: 224
TLS Session Ticket
TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.2 (0x0303)
Length: 1
Change Cipher Spec Message
TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 40
Handshake Protocol: Encrypted Handshake Message
0000 d4 6e 0e 10 17 d8 dc 53 7c 11 71 89 08 00 45 00 .n.....S |.q...E.
0010 01 50 18 00 00 00 38 06 f8 c2 d8 3a d6 a3 c0 a8 .P....8. ...:....
0020 01 5f 01 bb c5 36 54 02 0e 67 75 be 0f c8 80 18 ._...6T. .gu.....
0030 00 aa c6 e7 00 00 01 01 08 0a 45 27 58 8b 71 6c ....E'X.ql
0040 00 3b 16 03 03 00 e4 04 00 00 e0 00 01 89 c0 00 .;...... ....
0050 da 00 de 49 5f 5e c3 50 66 67 45 69 2c 83 4f d3 ...I_^.P fgEi,.O.
0060 df 1f 5f 05 9b 8c 8d cc d2 0e bd 53 4f 87 37 70 .._..... ...SO.7p
0070 75 e5 a8 8a 34 a8 14 95 e9 10 37 8f 8c ef 9e 5f u...4... ..7...._
0080 72 21 2c 57 6a 9d 38 7c 95 74 fb 27 fe fc 5e 08 r!,Wj.8| .t.'..^.
0090 0b 4a 86 a2 a3 10 2b b0 49 ab 8e 5a c1 62 7a 17 .J....+. I..Z.bz.
00a0 bf c6 d4 cd fa 1b 63 76 ad da ac 24 21 e0 15 06 ......cv ...$!...
00b0 a5 86 f6 39 26 42 aa dd 97 a9 72 e9 46 ac 05 51 ...9&B.. ..r.F..Q
00c0 55 ab 54 28 46 0b aa d0 c2 2d 9a e9 a9 f0 61 07 U.T(F... .-....a.
00d0 23 5d ae 4a 73 ab b2 4a aa 9e b3 fd 60 60 55 04 #].Js..J ....``U.
00e0 c9 d7 5b ad 9d b2 e4 68 ed 50 28 25 9d 7e 4b 61 ..[....h .P(%.~Ka
00f0 49 c6 3a ea 17 ad 31 c9 d9 01 44 8c 9a f5 ff d9 I.:...1. ..D.....
0100 72 a9 c2 c7 26 e1 69 48 4f 06 76 52 0d b7 3f 2e r...&.iH O.vR..?.
0110 4b 10 4d ce dd 2c c3 0f 11 ef 2a 80 8f fb 89 31 K.M..,.. ..*....1
0120 22 2b 3c 65 ba 6a 3d b7 e1 e1 ed 14 03 03 00 01 "+<e.j=. ....
0130 01 16 03 03 00 28 00 00 00 00 00 00 00 00 28 b1 .....(.. ......(.
0140 c2 41 63 50 a0 64 a1 32 ae e5 df 67 37 13 20 ad .AcP.d.2 ...g7. .


No. Time Source Destination Protocol Length Info
88 4.015155795 192.168.1.95 216.58.214.163 TLSv1.2 260 Client Hello
92 4.068087206 216.58.214.163 192.168.1.95 TLSv1.2 1484 Server Hello
96 4.068160578 216.58.214.163 192.168.1.95 TLSv1.2 1349 Certificate, Server Key Exchange, Server Hello Done
105 4.075629551 192.168.1.95 216.58.214.163 TLSv1.2 159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
111 4.104673517 216.58.214.163 192.168.1.95 TLSv1.2 350 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
112 4.104688108 216.58.214.163 192.168.1.95 TLSv1.2 135 Application Data
Frame 112: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface 0
Ethernet II, Src: CompalBr_11:71:89 (dc:53:7c:11:71:89), Dst: Tp-LinkT_10:17:d8 (d4:6e:0e:10:17:d8)
Internet Protocol Version 4, Src: 216.58.214.163, Dst: 192.168.1.95
Transmission Control Protocol, Src Port: 443, Dst Port: 50486, Seq: 4404, Ack: 288, Len: 69
Secure Sockets Layer
TLSv1.2 Record Layer: Application Data Protocol: http2
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 64
Encrypted Application Data: 00000000000000127cc6454fea473b747333dd6e07f9b4c...
0000 d4 6e 0e 10 17 d8 dc 53 7c 11 71 89 08 00 45 00 .n.....S |.q...E.
0010 00 79 18 01 00 00 38 06 f9 98 d8 3a d6 a3 c0 a8 .y....8. ...:....
0020 01 5f 01 bb c5 36 54 02 0f 83 75 be 0f c8 80 18 ._...6T. ..u.....
0030 00 aa e2 00 00 00 01 01 08 0a 45 27 58 8b 71 6c ....E'X.ql
0040 00 3b 17 03 03 00 40 00 00 00 00 00 00 00 01 27 .;....@. ....'
0050 cc 64 54 fe a4 73 b7 47 33 3d d6 e0 7f 9b 4c 74 .dT..s.G 3=....Lt
0060 2f c5 20 b6 bb c4 83 2d e8 99 8b ac 7b 51 0f ed /. ....- ....{Q..
0070 4e 62 61 66 ab 24 d7 43 93 2b 47 27 62 f0 19 3f Nbaf.$.C .+G'b..?
0080 b0 7f b7 4f 87 9b ae ...O...


No. Time Source Destination Protocol Length Info
133 4.404755759 192.168.1.95 216.58.214.163 TLSv1.2 97 Encrypted Alert
135 4.431062482 216.58.214.163 192.168.1.95 TLSv1.2 104 Application Data
141 4.858373976 192.168.1.95 216.58.201.142 TLSv1.2 199 Application Data
143 4.948572504 216.58.201.142 192.168.1.95 TLSv1.2 201 Application Data
145 4.948630255 216.58.201.142 192.168.1.95 TLSv1.2 1484 Application Data
147 4.948647196 216.58.201.142 192.168.1.95 TLSv1.2 1484 Application Data
Frame 133: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0
Ethernet II, Src: Tp-LinkT_10:17:d8 (d4:6e:0e:10:17:d8), Dst: CompalBr_11:71:89 (dc:53:7c:11:71:89)
Internet Protocol Version 4, Src: 192.168.1.95, Dst: 216.58.214.163
Transmission Control Protocol, Src Port: 50486, Dst Port: 443, Seq: 482, Ack: 4473, Len: 31
Secure Sockets Layer
TLSv1.2 Record Layer: Encrypted Alert
Content Type: Alert (21)
Version: TLS 1.2 (0x0303)
Length: 26
Alert Message: Encrypted Alert
0000 dc 53 7c 11 71 89 d4 6e 0e 10 17 d8 08 00 45 00 .S|.q..n ......E.
0010 00 53 c4 a9 40 00 40 06 05 16 c0 a8 01 5f d8 3a .S..@.@. ....._.:
0020 d6 a3 c5 36 01 bb 75 be 10 8a 54 02 0f c8 80 18 ...6..u. ..T.....
0030 01 3e cd 9f 00 00 01 01 08 0a 71 6c 00 8e 45 27 .>...... ..ql..E'
0040 58 ca 15 03 03 00 1a 00 00 00 00 00 00 00 02 57 X..... . .....W
0050 f3 06 9c 93 89 53 3d 61 1e 75 e0 ba ba e1 09 27 .....S=a .u.....'
0060 28 (

Vulnerabilidades TLS

Índice:

3.a.- Tipos de ataques conocidos

1. **Ataques de renegociación**
2. Ataque de reversión de versiones
3. Ataque de relleno
4. Ataque RC4
5. Ataque de truncamiento

3.a.1.- Ataque de renegociación

Un ataque descubierto en 2009 (CVE-2009-3555) que permite inyectar información en conexiones “no propias” de un cliente con el servidor. Este problema afecta a las versiones 3.0 de SSL y todas las versiones actuales de TLS.

Podríamos interceptar (MitM) una conexión SSL y hacer nuestra propia conexión con el servidor mandando datos arbitrarios y desencadenar una renegociación utilizando la conexión original del cliente.

3.a.- Tipos de ataques conocidos

1. Ataques de renegociación
2. **Ataque de reversión de versiones**
3. Ataque de relleno
4. Ataque RC4
5. Ataque de truncamiento

3.a.2.- Ataque de reversión de versiones

Este tipo de ataque se realiza en la conexión del cliente con el servidor (MitM) para intentar rebajar el método de cifrado o la versión en sí, para así poder descifrar más fácilmente esta conexión. Un ataque muy explotado es conocido como POODLE (CVE-2014-3566).

3.a.- Tipos de ataques conocidos

1. Ataques de renegociación
2. Ataque de reversión de versiones
3. **Ataque de relleno**
4. Ataque RC4
5. Ataque de truncamiento

3.a.3.- Ataque de relleno

Algunos algoritmos de cifrado necesitan insertar bytes de relleno para completar los bloques. Es por ello, que en 2003 (CVE-2003-0078) se consiguió a través de un algoritmo, diferenciar la parte de relleno con la parte de información. En 2016 (CVE-2016-2107) se encontró una vulnerabilidad que permite descifrar (MitM) el tráfico cuando la conexión utiliza cifrado AES CBC y el servidor admite AES-NI.

3.a.- Tipos de ataques conocidos

1. Ataques de renegociación
2. Ataque de reversión de versiones
3. Ataque de relleno
4. **Ataque RC4**
5. Ataque de truncamiento

3.a.4.- Ataque RC4

El algoritmo RC4, como se usa en el protocolo TLS y protocolo SSL, no combina adecuadamente datos de estado con datos clave durante la fase de inicialización, lo que facilita a los atacantes remotos realizar ataques de recuperación de texto plano contra los bytes iniciales de una secuencia olfateando tráfico de red que de vez en cuando se basa en claves afectadas por la Debilidad de Invariancia, y luego usa un enfoque de fuerza bruta que involucra valores LSB.

Algunos ejemplos: **CVE-2013-2566** - **CVE-2015-2808**

3.a.- Tipos de ataques conocidos

1. Ataques de renegociación
2. Ataque de reversión de versiones
3. Ataque de relleno
4. Ataque RC4
5. **Ataque de truncamiento**

3.a.5.- Ataque de truncamiento

Un ataque de truncamiento de TLS bloquea las solicitudes de cierre de sesión de la cuenta de la víctima para que el usuario permanezca, sin saberlo, conectado a un servicio web. Cuando se envía la solicitud de cierre de sesión, el atacante inyecta un mensaje TCP FIN no cifrado para cerrar la conexión. Por lo tanto, el servidor no recibe la solicitud de cierre de sesión y no tiene conocimiento de la finalización anormal.

Este fallo llevó en julio de 2013 a que servicios web como Gmail o Hotmail tuvieran que mostrar una página indicando que la sesión ha finalizado para asegurarnos de esto.

Índice:

3.b.- Ataques más importantes

1. **Ataque CRIME**
2. Ataque Heartbleed
3. Ataque POODLE

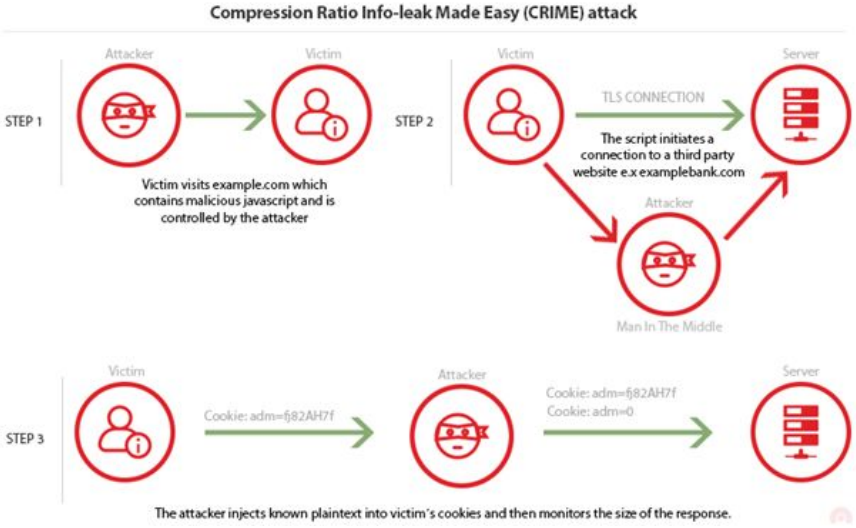
3.b.1.1.- Ataque CRIME (CVE-2012-4929)

CRIME (Compression Ratio Info-leak Made Easy) es una vulnerabilidad que se encuentra en la compresión de TLS. El método de compresión se incluye en el mensaje *ClientHello* y es opcional, lo que significa que la conexión se puede establecer sin compresión. El objetivo de la comprensión es reducir el uso de ancho de banda al tiempo que se preserva la integridad y seguridad cuando se intercambian grandes cantidades de información. DEFLATE es el algoritmo de compresión más conocido.

Una de las técnicas más usadas en compresión de archivos consiste en reemplazar bytes repetidos con un puntero a la primera instancia de ese byte.

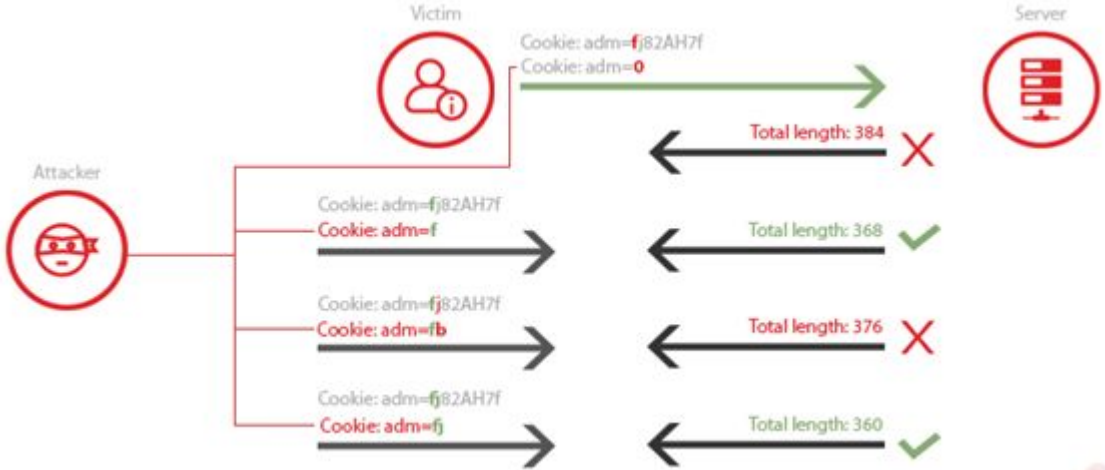
3.b.1.2.- Ataque CRIME (CVE-2012-4929)

Supongamos que el atacante quiere obtener una cookie de la víctima. Se sabe que para la sesión, el sitio web específico (ejemplo.com) crea una cookie llamada "adm". Sabiendo que el método de compresión DEFLATE reemplaza bytes repetidos, si el atacante inyecta *"Cookie: adm = 0"* en la cookie de la víctima, el servidor solo anexará 0 a la respuesta comprimida ya que *"Cookie: adm ="* ya se envió en la cookie de la víctima y se repite.



3.b.1.3.- Ataque CRIME (CVE-2012-4929)

Todo lo que el atacante debe hacer es inyectar diferentes caracteres y luego controlar el tamaño de la respuesta. Si el tamaño de la respuesta es menor que la inicial, significa que el carácter que inyectó está contenido en el valor de la cookie y, por lo tanto, se comprime, lo que equivale a una coincidencia. Si el carácter no está en el valor de la cookie, el tamaño de la respuesta será mayor.



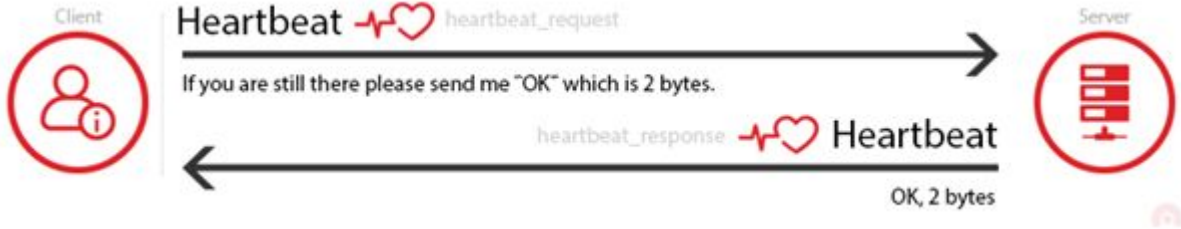
3.b.- Ataques más importantes

1. Ataque CRIME
2. **Ataque Heartbleed**
3. Ataque POODLE

3.b.2.1.- Ataque Heartbleed (CVE-2014-0160)

Heartbleed era una vulnerabilidad crítica, simple de explotar, que se encuentra en la “extensión de latido” de la popular biblioteca de criptografía OpenSSL. Este ataque aprovecha la “extensión de latido” TLS, que se usa principalmente como método para mantener viva la conexión entre dos partes siempre y cuando las dos partes estén disponibles.

La solicitud de latido funciona de la siguiente manera. El cliente envía un mensaje de "latido" al servidor con una carga útil que contiene datos + tamaño de los datos (y relleno). El servidor debe responder con la misma solicitud de "latido", que contiene los datos + tamaño de los datos que el cliente envió.



3.b.2.2.- Ataque Heartbleed (CVE-2014-0160)

El problema era que, si el cliente enviaba datos falsos, el servidor respondería con los datos recibidos por el cliente + datos aleatorios de su memoria para cumplir con los requisitos de longitud especificados por el remitente aunque los datos fueran más pequeños que la longitud especificada.

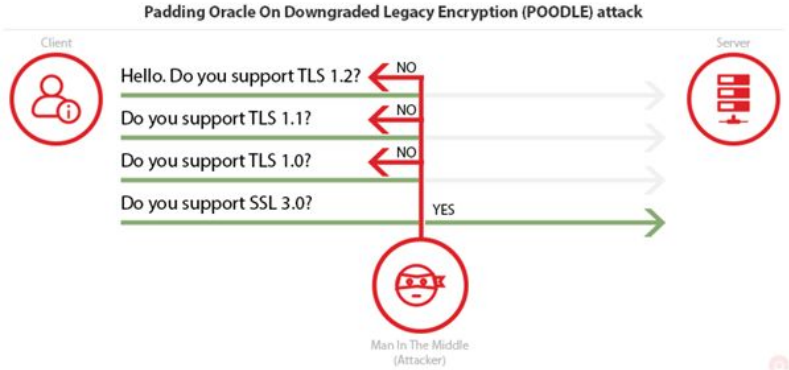
3.b.- Ataques más importantes

1. Ataque CRIME
2. Ataque Heartbleed
3. **Ataque POODLE**

3.b.3.1.- Ataque POODLE (CVE-2014-3566)

POODLE (Padding Oracle On Downgraded Legacy Encryption) se publicó en octubre de 2014 y aprovecha dos factores. El primero es el hecho de que algunos servidores/clientes todavía admiten SSL 3.0 para la interoperabilidad y compatibilidad con sistemas que usan versiones antiguas. El segundo factor es una vulnerabilidad que existe en SSL 3.0 que está relacionada con el relleno del bloque.

El cliente inicia el protocolo de enlace y envía la lista de las versiones SSL/TLS admitidas. Un atacante intercepta el tráfico, realiza un ataque MitM y se hace pasar por el servidor hasta que el cliente acepte degradar la conexión al vulnerable SSL 3.0



3.b.3.2.- Ataque POODLE (CVE-2014-3566)

Ahora que la conexión entre el Cliente y el Servidor está establecida en una versión vulnerable de SSL, el atacante puede realizar el ataque real de POODLE. La vulnerabilidad existe en el modo de encadenamiento de bloques de cifrado. Como las cifras de bloque tienen una longitud fija, si los datos en el último bloque no son un múltiplo de su tamaño, entonces se agrega relleno para llenar el espacio adicional. Uno de los problemas es que el servidor ignora el valor de relleno y solo verifica si la longitud del relleno es correcta, así como el Código de Autenticación de Mensaje (MAC) del texto plano. Eso significa que el receptor (Servidor) no puede verificar si el valor de relleno se ha modificado.

Un atacante puede descifrar el valor del texto plano de un bloque cifrado modificando los bytes de relleno y luego viendo la respuesta correspondiente del servidor. Se necesitan un máximo de 256 solicitudes SSL 3.0 para descifrar un solo byte.

Esto significa que una vez cada 256 solicitudes, el servidor aceptará el valor modificado. El atacante no necesita conocer el método o la clave de cifrado para realizar este ataque. Usando herramientas automatizadas, un atacante puede recuperar el texto plano carácter a carácter. Esto podría ser fácilmente una contraseña, una cookie, una sesión u otros datos confidenciales.

3.- Vulnerabilidades TLS: Estudio de sitios web.

Octubre 2016:

Ataques	Inseguro		Depende	Seguro	Otro
Ataque de renegociación	1.2% soporta renegociación insegura		0.4% soporta ambos	96.2% soporta renegociación segura	2.2% sin soporte
Ataque RC4	<0.1% permite sólo cifrados RC4	6.0% permite cifrados RC4 usado con navegadores modernos	28.5% soporta algunos cifrados RC4	65.5% sin soporte	
Ataque CRIME	2.4% vulnerable				
Heartbleed	0.1% vulnerable				
POODLE	2.1% vulnerable y explotable			97.1% no vulnerable	0.8% desconocido
Reversión de versiones	23.2% TLS_FALLBACK_SCSV no soportado			67.6% TLS_FALLBACK_SCSV soportado	9.1% desconocido

3.- Vulnerabilidades TLS: Ejemplos

Qualys SSL Labs

Índice:

4.- Caso práctico:

- Sistema Operativo: Ubuntu 12.04
- Versión OpenSSL: 1.0.1
- Version Apache: 2.2.22
- Versión Kali Linux: 2017.3

Pasos atacante:

- nmap -d --script=ssl-heartbleed --script-args=vulns.showall <TARGET>
- msgconsole
- use auxiliary/scanner/ssl/openssl_heartbleed
- set RHOSTS <TARGET>
- set verbose true
- exploit

Índice:

5.- Bibliografía

- Algoritmo DEFLATE: http://www.gzip.org/algorithm.txt Visitado por última vez 03-12-2017
- Vulnerabilidades: https://www.openssl.org/news/vulnerabilities.html Visitado por última vez 03-12-2017
- POST sobre TLS de Agathoklis Prodromou el 22 de Marzo de 2017:
  - https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/ Visitado por última vez 03-12-2017
- Chequeo TLS/SSL Web/navegador: https://www.ssllabs.com/ Visitado por última vez 03-12-2017
- RC4: https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_ssl_rc4_cipher_suites_supported Visitado por última vez 03-12-2017
- Post sobre ataque de truncamiento de John Leyden el 1 de Agosto de 2013:
  - http://www.theregister.co.uk/2013/08/01/gmail_hotmail_hijacking/ Visitado por última vez 03-12-2017
- RFC2246 https://tools.ietf.org/html/rfc2246 Visitado por última vez 03-12-2017
- RFC 4346 https://tools.ietf.org/html/rfc4346 Visitado por última vez 03-12-2017
- RFC 5246 https://tools.ietf.org/html/rfc5246 Visitado por última vez 03-12-2017
- TLS 1.3 Draft https://tools.ietf.org/html/draft-ietf-tls-tls13-21 Visitado por última vez 03-12-2017
- E.Rescorla. SSL and TLS: Designing and Building Secure Systems (2001)