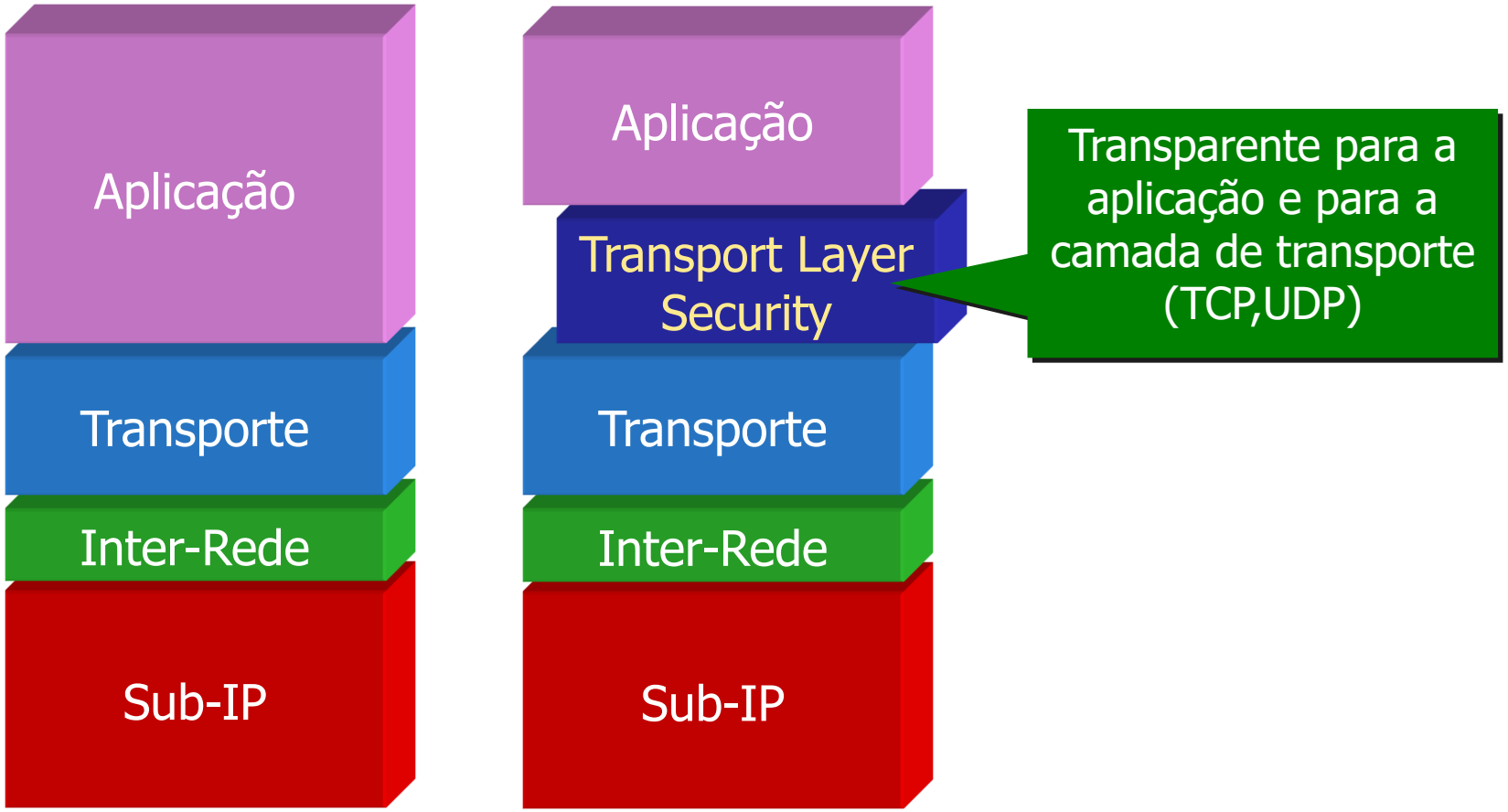
Criptologia Aplicada

SSL/TLS

Dênio Mariz
denio@ifpb.edu.br

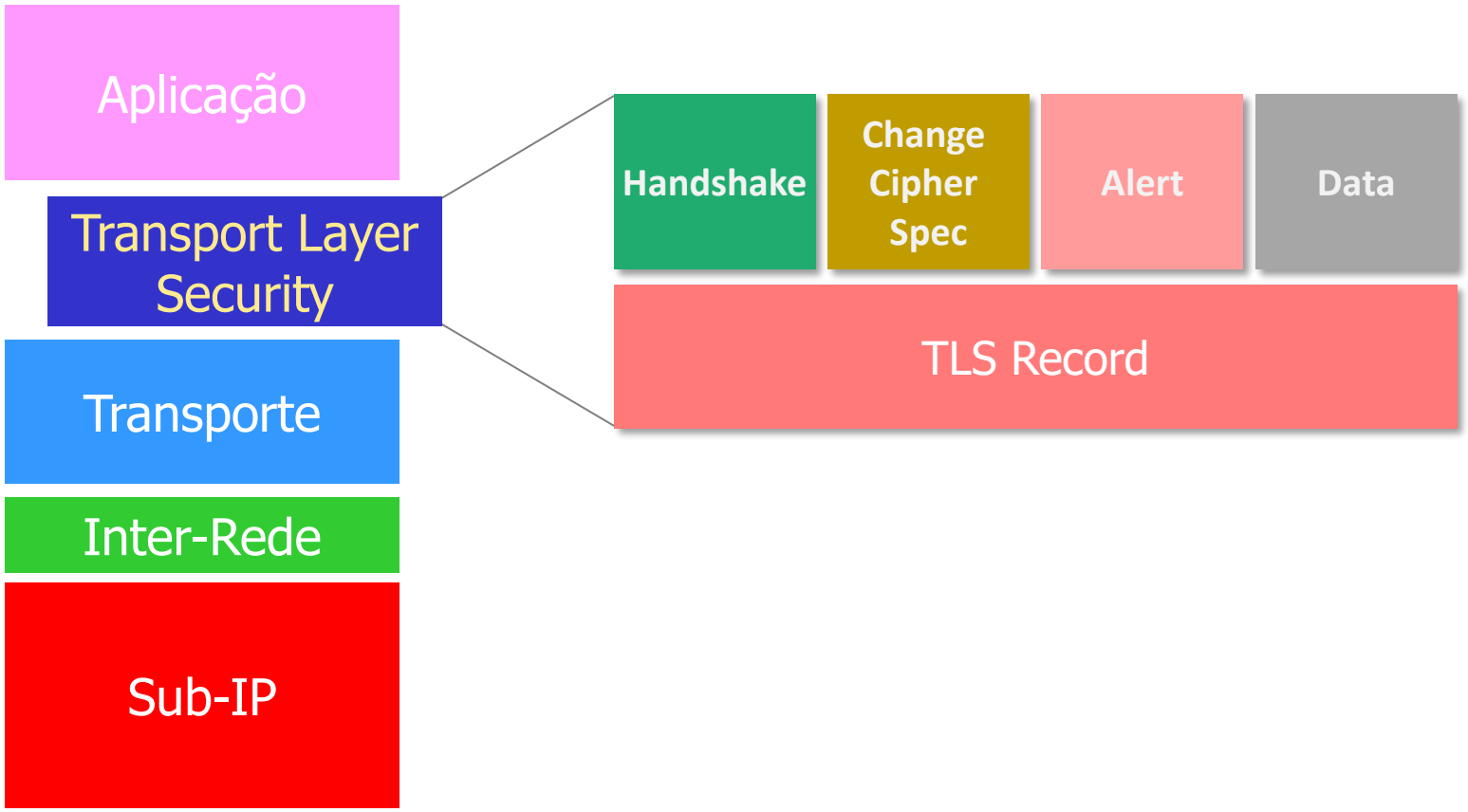
Modelo TCP/IP com Segurança



Modelo TCP/IP

Modelo TCP/IP com SSL/TLS

Modelo TCP/IP com Segurança



Modelo TCP/IP

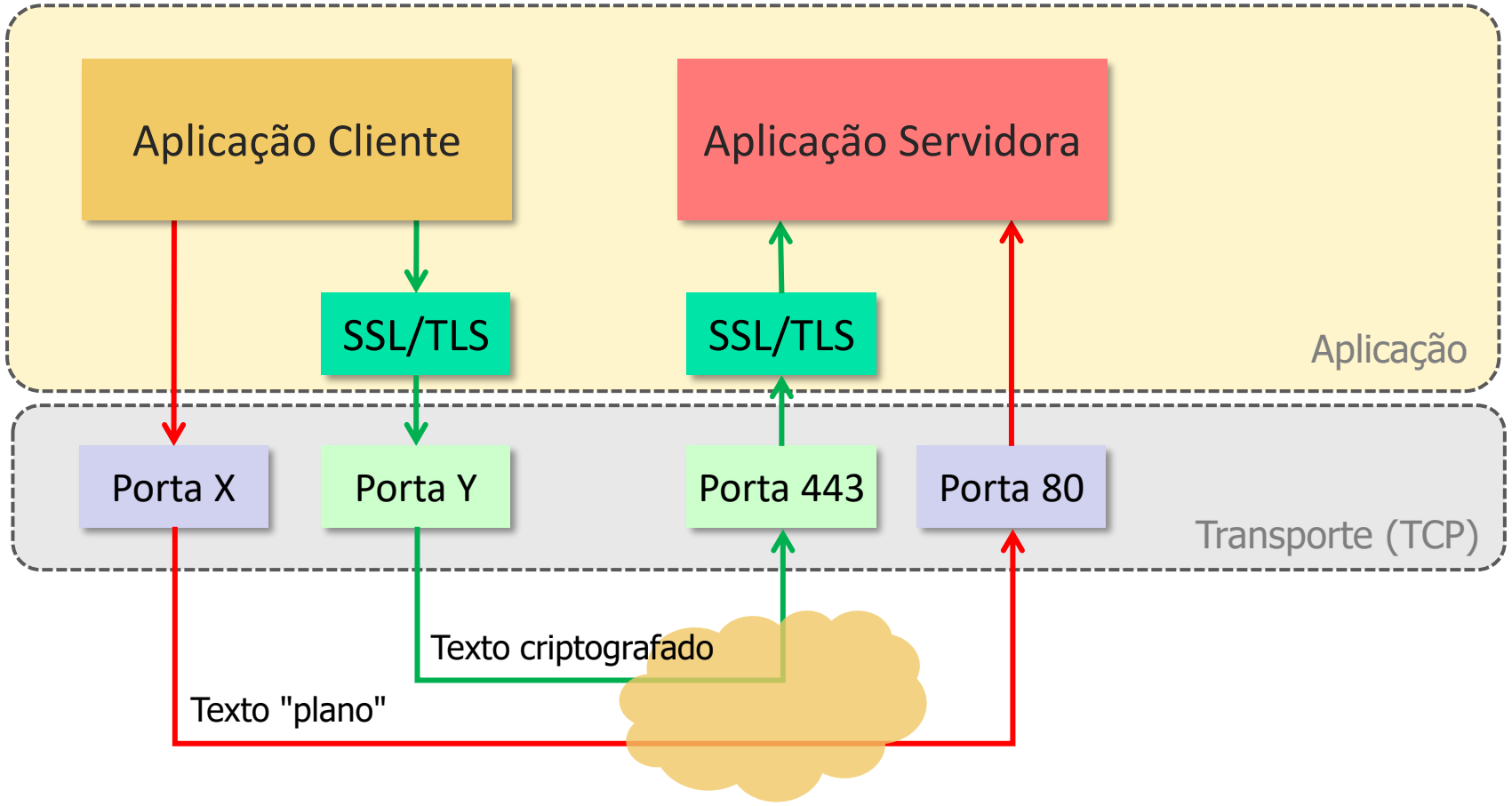
SSL/TLS – Visão Geral

- SSL: publicado pela Netscape em 1996
- TLS: publicado pelo IETF em 1999
  - Baseado no SSLv3
  - http://tim.dierks.org/2014/05/security-standards-and-name-changes-in.html
- Protocolos para troca de chaves e envio de mensagens confidenciais
  - Permitem autenticar o servidor para o cliente
  - Opcionalmente, permitem autenticar o cliente para o servidor
  - Estabelecem uma chave de sessão (secreta) usando um mecanismo de canal seguro (ex: RSA ou Diffie Helman)
  - Usam funções de hash para garantir integridade

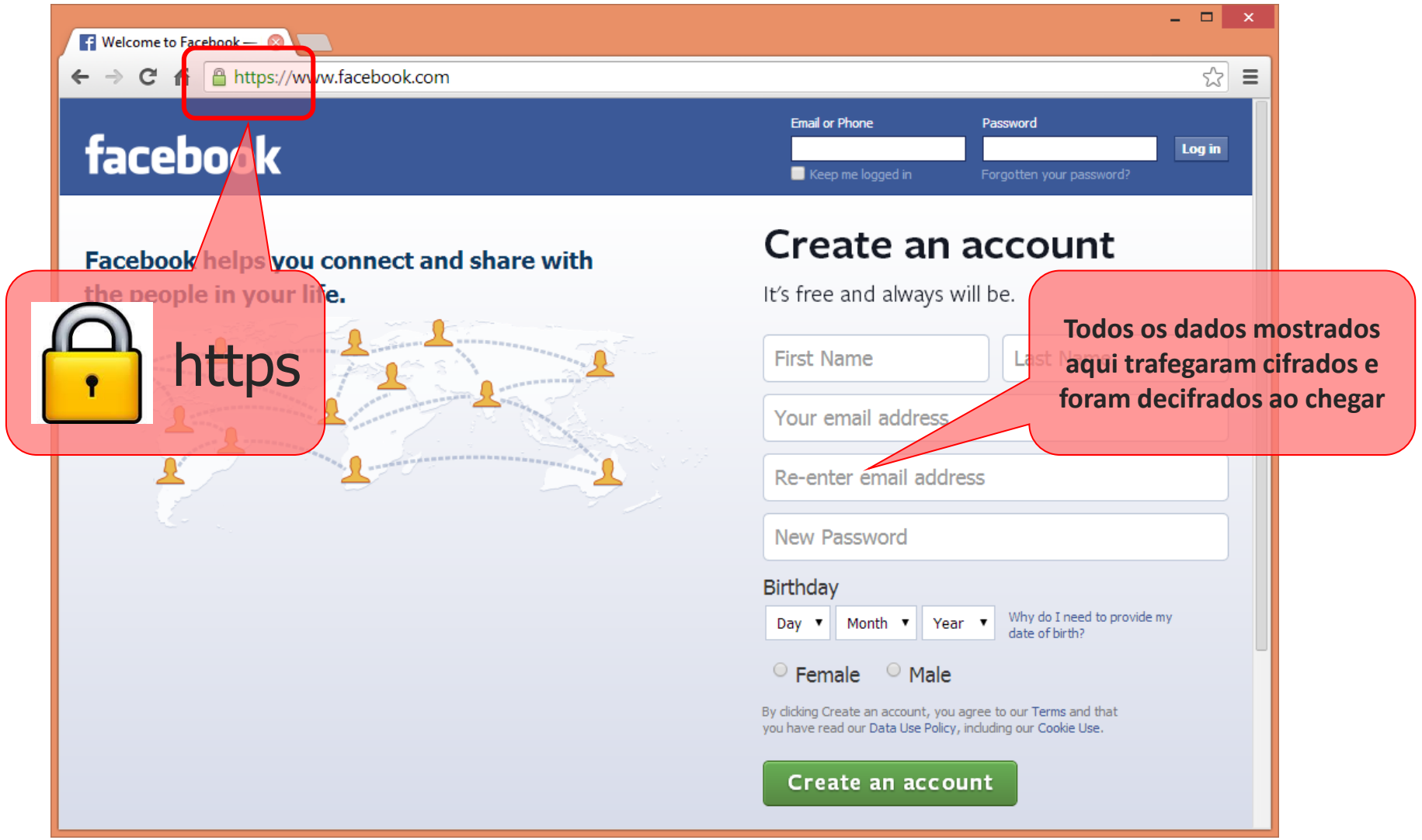
TLS – Transport Layer Security

- Em 1999 o IETF formou um grupo de trabalho para estabelecer um padrão de segurança de dados para a camada de transporte
- TLS 1.0 - RFC 2246 de 1999
  - Baseado no SSL 3.0
  - Algumas vulnerabilidades já conhecidas desde 2002
- TLS 1.1 - RFC 4346 de Abril 2006.
  - Proteção contra ataques de Cipher block chaining (CBC).
  - Melhorias no tratamento de de erros
  - Suporte para parâmetros registrados no IANA
- TLS 1.2 - RFC 5246 de Agosto 2008
  - Várias melhorias para descrição do hash usado pelo cliente e servidor
  - Adição de hash SHA-256
  - Expansão do suporte para authenticated encryption ciphers, Galois/Counter Mode (GCM)
  - Extensões para uso do AES
- Todas as versões do TLS foram refinadas na RFC 6176 de Março 2011
  - Remoção de compatibilidade para trás (ex: TLS não negocia mais o uso de SSL 2.0 nem 3.0)
- TLS 1.3 – Draft em andamento
  - Removerá suporte para MD5 e SHA-224 e algoritmos obsoletos, trará novos mecanismos

SSL/TLS na aplicação



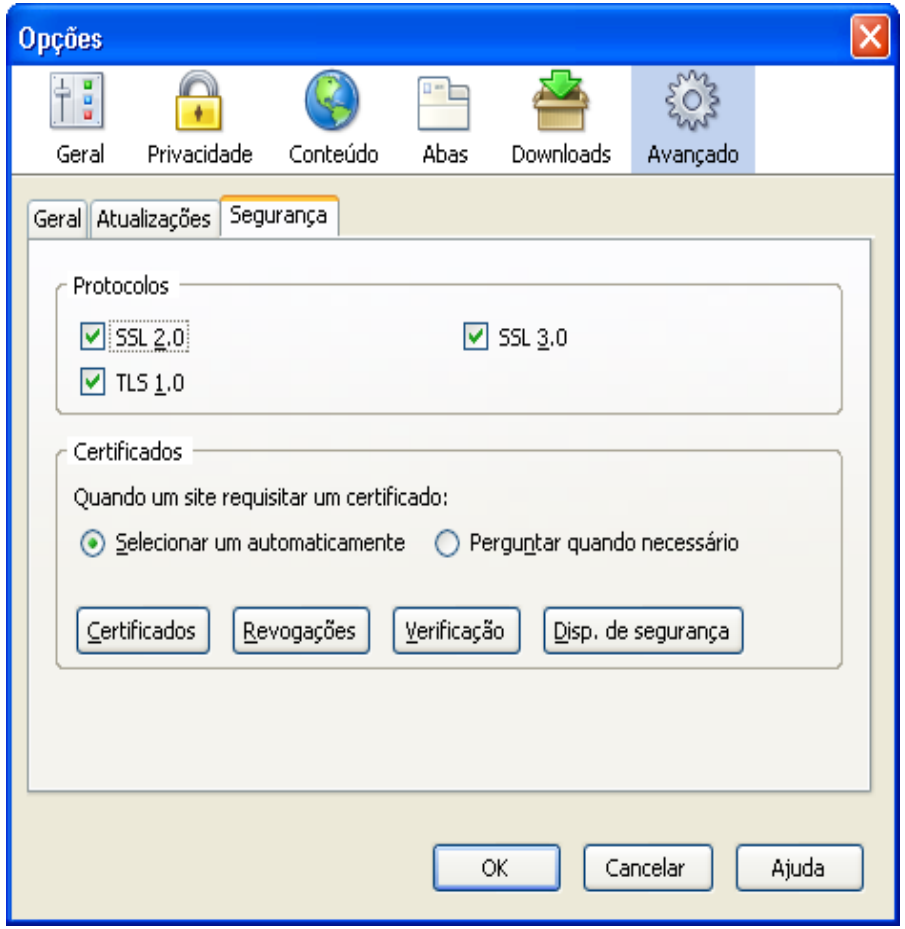
TLS/SSL no Mundo Real



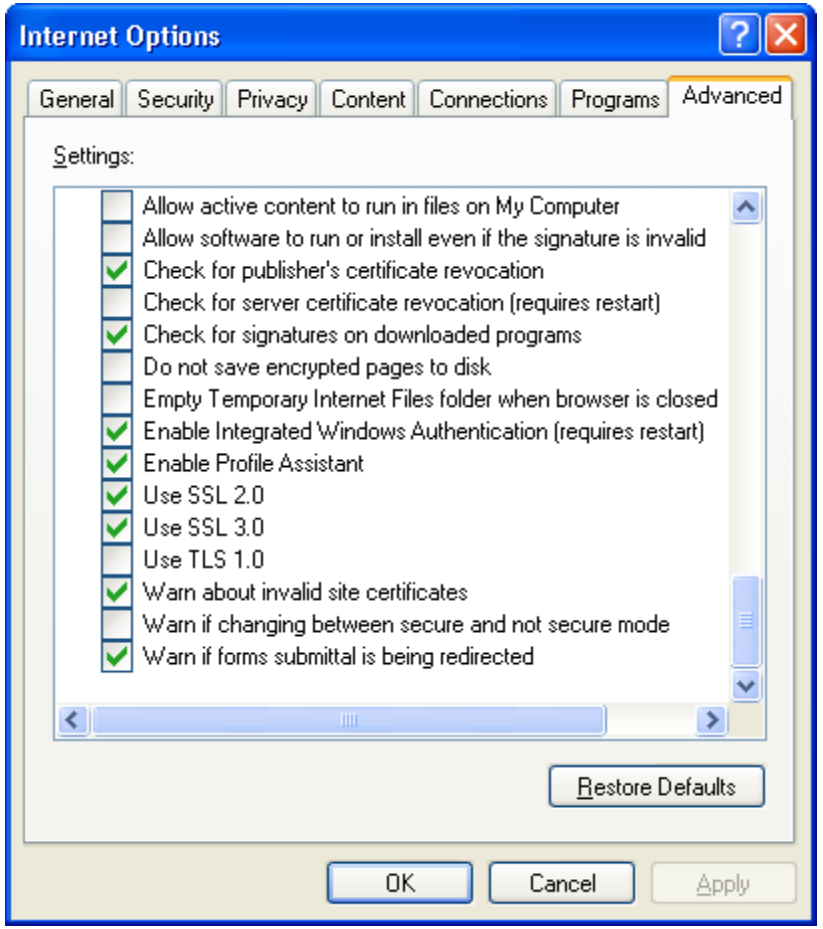
Confidencialidade

- Criptografia Simétrica ou Assimétrica: qual usar?
  - Sistemas assimétricos: Confidencialidade, Autenticação e não-repúdio
  - Sistemas simétricos: confidencialidade, desempenho
- TLS usa solução Híbrida (ambas as criptografias)
  - Chaves pública e privada para cifrar/decifrar uma chave simétrica (chave de sessão)
  - Chave simétrica para cifrar/decifrar os dados

SSL, TLS – Suportado pelos Browsers

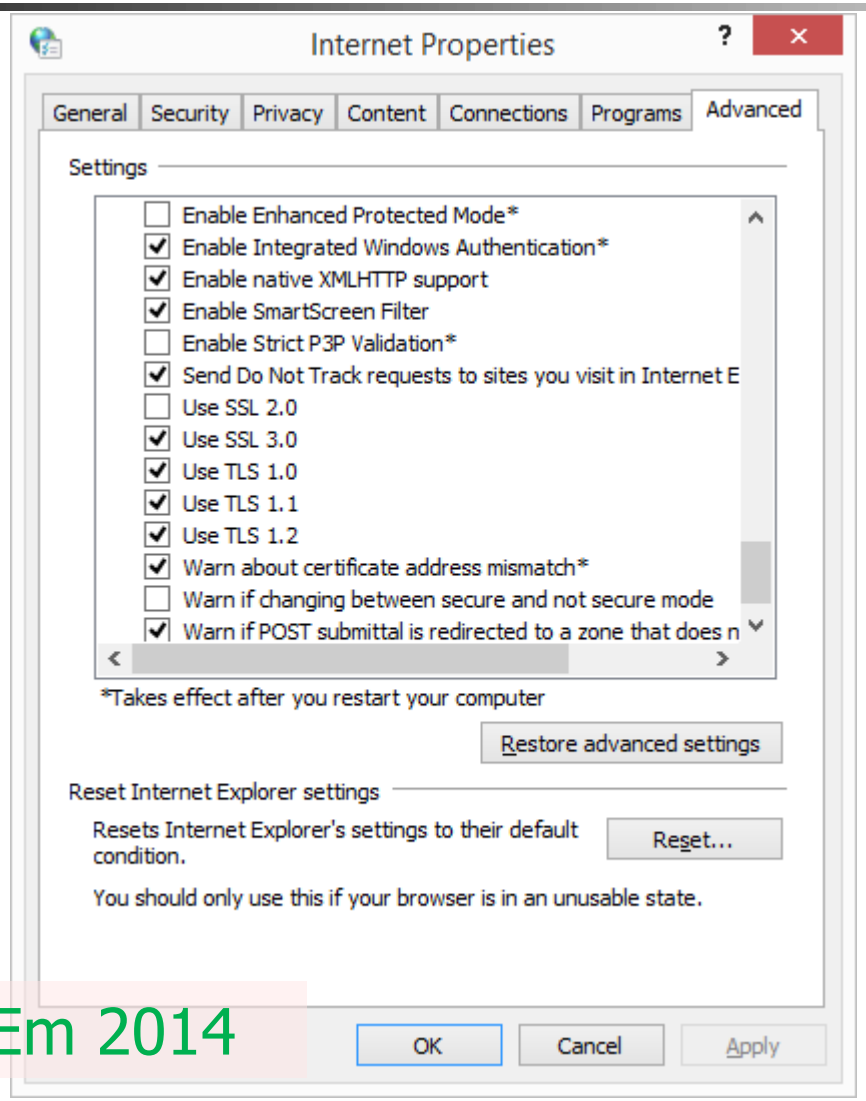


Mozilla Firefox

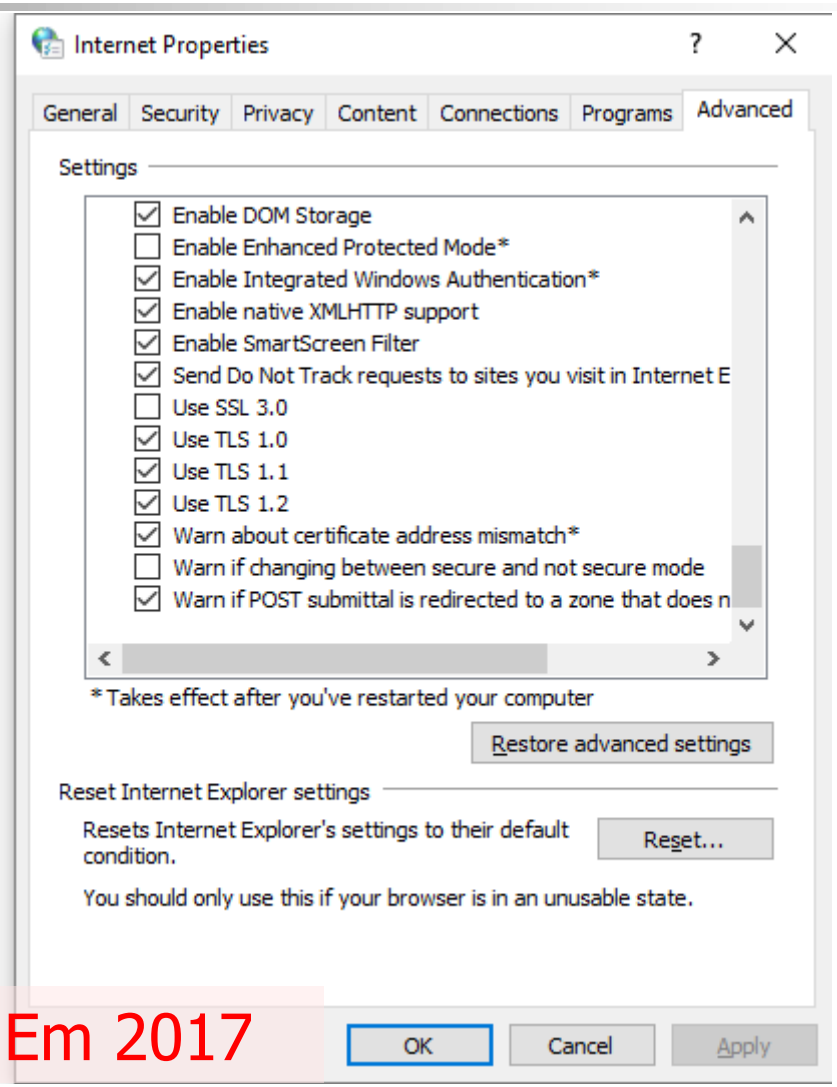


Internet Explorer

Opções da Internet (windows 8,10)



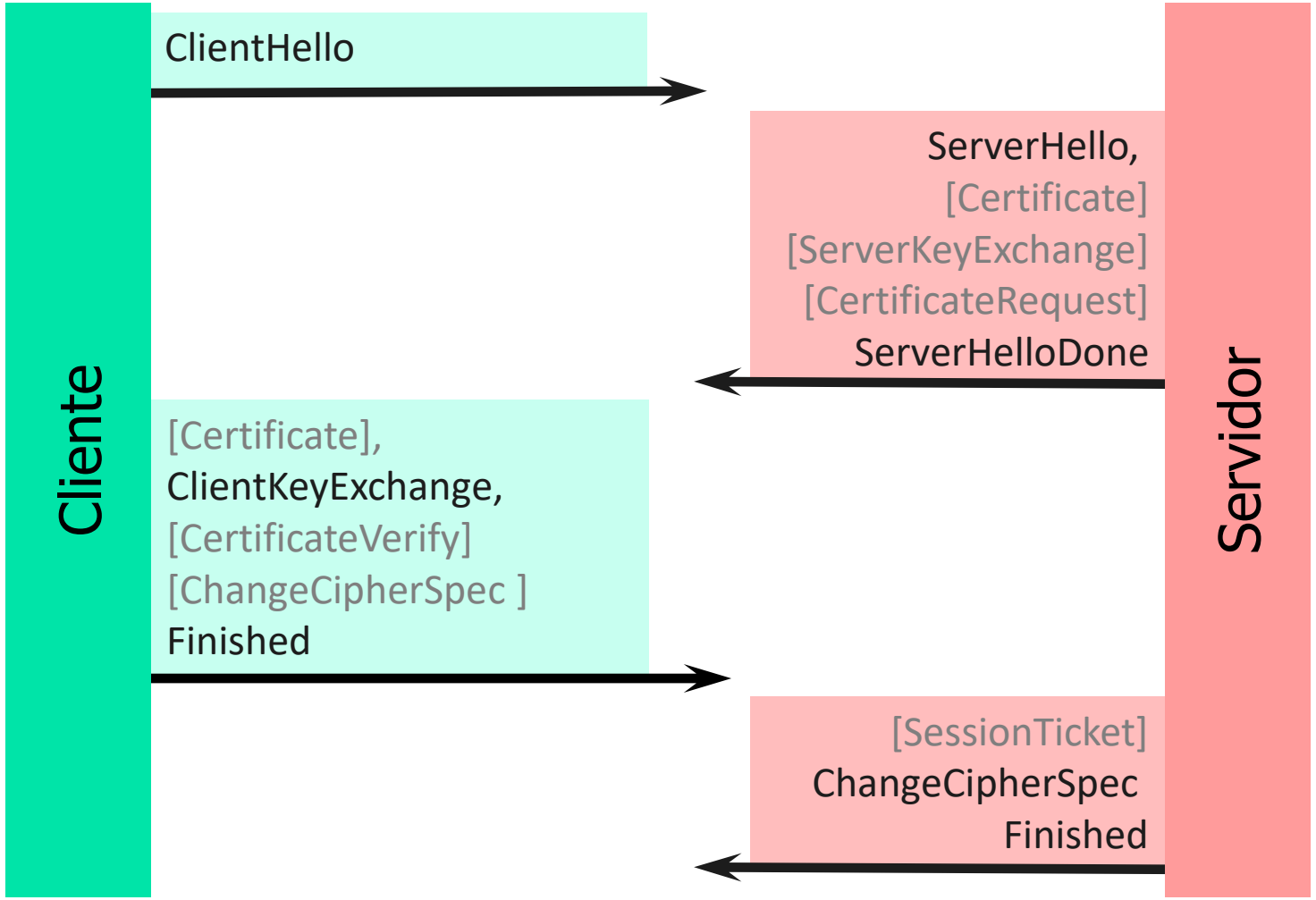
Em 2014



Em 2017

Control Panel → Internet Options

TLS Handshake Protocol 1.2



Mensagens do TLS handshake 1/4

- ClientHello
  - Version: Versão do protocol TLS do cliente
  - Client Random: Número pseudorandomico de 28 bytes para cálculo do “Master secret” (a ser usado na criação da chave se sessão)
  - Session ID: Identificador único da sessão para o cliente
  - Cipher Suite: A suite de cifras suportada pelo cliente, em ordem de preferência
  - Compression Method: Método de compressão selecionado (opcional, normalmente null)

Mensagens do TLS handshake 2/4

- ServerHello
  - Server Version: A maior versão TLS do servidor que seja suportada pelo cliente
  - Server Random: Número pseudorandômico de 28 bytes para cálculo do “Master secret”
  - Session ID: Identificador único da sessão para o servidor
  - Cipher Suite: Apenas uma das suites de cifras selecionada (normalmente a mais forte). Se nenhuma for suportada, um alerta é Gerado e o handshake falha.
  - Compression Method: Método de compressão selecionado (opcional, normalmente null)
- Server Certificate
  - Envia a cadeia de certificados do servidor para o cliente (X.509v3)
  - Não enviada apenas quando a cifra não exige um certificado (ex: DH)

Mensagens do TLS handshake 3/4

- ServerKeyExchange
  - Informações adicionais para estabelecimento da chave (apenas para alguns algoritmos específicos – e.g. Diffie Hellman)
- CertificateRequest
  - Servidor solicita o certificado do cliente (opcional)
  - Inclui nomes das autoridades raiz confiáveis do servidor
- ServerHelloDone
  - Avisa ao cliente do fim do ServerHello
- Certificate (client)
  - Envia cadeia de certificados do cliente para o servidor (se solicitado por CertificateRequest)
- ClientKeyExchange
  - A chave simétrica secreta é estabelecida pelo cliente (fase final do DH ou envio via RSA cifrada com a pública do servidor)

Mensagens do TLS handshake 4/4

- CertificateVerify
  - Envia uma assinatura digital para todas as mensagens trocadas até então para verificação por parte do servidor
  - Serve para provar ao servidor que o cliente realmente é o dono da chave pública
  - Apenas quando o certificado do cliente é enviado para o servidor e tem capacidade de assinatura
- Session Ticket
  - Servidor envia um "Ticket de Sessão" que é a chave da sessão cifrada com uma chave que somente o servidor possui (*Session Ticket Encryption Key - STEK*). Isso permitirá a um cliente "retomar" uma sessão reduzindo a sobrecarga do handshake.
- ChangeCipherSpec (client, Server)
  - Notifica o parceiro que as mensagens subseqüentes serão protegidos com algoritmos e chaves recém-negociados.
  - Mensagens seguintes serão cifradas com o algoritmo simétrico negociado
- Finished (client, server)
  - (Também chamada de Encrypted Handshake Message)
  - É um hash de toda a conversa anterior.
  - É a primeira mensagem cifrada pelos algoritmos negociados. Parceiro deve verificar a corretude.
  - Após enviar a sua e conferir a do parceiro, dados podem ser enviados protegidos pelo mesmo mecanismo.

SSL/TLS – Detalhes do Handshake

- Mensagem "ServerHello"
  - Algoritmos de criptografia mais fortes dentre os sugeridos pelo cliente
- Mensagem “Certificate"
  - Envio do Certificado
  - Certificado assinado por uma autoridade certificadora
  - Cliente checa se o CA é confiável (interno no browser)
  - Servidor pode opcionalmente solicitar o Certificado do cliente
    - Não é prático para comércio eletrônico
    - Usuário pode usar o número de cartão de crédito para isto

Passos da Sessão TLS (resumo) 1/2

- O cliente envia uma mensagem "Client hello" para o servidor, juntamente com o valor aleatório do cliente e suites de cifra suportadas.
- O servidor responde enviando uma mensagem "Server hello" com o valor aleatório do servidor e as cifras selecionadas.
- O servidor envia seu certificado ao cliente para autenticação e pode opcionalmente solicitar um certificado do cliente com uma mensagem CertificateRequest.
- O servidor envia a mensagem "Server hello done".
- Se o servidor solicitou um certificado do cliente, o cliente o envia em uma mensagem Certificate.
- O cliente cria um *premaster secret* (número aleatório) e criptografa-o com a chave pública do servidor, enviando o *premaster secret* criptografado para o servidor na mensagem ClientKeyExchange.

Passos da Sessão TLS (resumo) 2/2

- O servidor recebe o *premaster secret*. Ambos geram o *Master Secret* com base no *premaster secret* e nos valores randômicos `ClientHello.random` e `ServerHello.random`
- O cliente envia notificação "Change Cipher Spec" para o servidor para indicar que o cliente começará a usar as novas chaves de sessão para hashing e mensagens cifradas. O cliente envia a mensagem "Finish".
- O servidor recebe "Change Cipher Spec" e muda seu estado para criptografia simétrica usando as chaves de sessão. O servidor envia a mensagem "Finish" para o cliente.
- Cliente e servidor agora podem trocar dados pelo canal seguro que estabeleceram. Todas as mensagens enviadas entre o cliente e o servidor são criptografadas usando a chave da sessão.

TLS – Cipher Suite

- Um identificador de 3 bytes que define um conjunto de algoritmos (cipher suite) necessários para proteger uma conexão TLS
- Formato: PROTO_KX[AU]_WITH_ENC_MAC
  - PROTO – protocolo (TLS, SSL, SSL2)
  - KX – algoritmo para troca de chaves
  - AU – algoritmo de autenticação (opcional)
  - ENC – algoritmo de criptografia simétrica
  - MAC – algoritmo de hash (integridade)
- Existem mais de 200 cipher suites.
- KX = {RSA, DH, DHE, ECDHE}

Exemplo de cifra TLS

- TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS = o protocolo TLS
  - RSA = RSA para troca de chave
  - RSA = RSA para autenticação
  - AES_128_CBC = AES 128 no modo "cipher block chaining"
  - SHA= algoritmo de hash

→ TLS_RSA_WITH_AES_128_CBC_SHA é obrigatória no TLS 1.2

TLS Cipher Suites: algoritmos disponíveis

Key exchange and Authentication

SIGLA	Algoritmo
RSA	Rivest, Shamir, Adleman
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
ECDH	Elliptic-Curve Diffie-Hellman
KRB5	Kerberos
SRP	Secure Remote Password Protocol
PSK	Pre-shared key
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
DSS	Digital Signature Standard

Encryption and MAC

SIGLA	Algoritmo
3DES	**Tripple Data Encryption Algorithm**
AES	**Advanced Encryption Standard**
Camelia	**Block cipher developed by Mitsubishi and NTT**
DES	**Data Encryption Standard**
Fortezza	**Security token based cipher**
GOST	**Block cipher developed in USSR**
IDEA	**International Data Encryption Algorithm**
~~**RC2**~~	~~**Rivest Cipher 2**~~
~~**RC4**~~	~~**Rivest Cipher 4**~~
SEED	**Block cipher developed by Korean Information Security Agency**
SHA	**Secure Hash Algorithm**
MD5	**Message Digiest algorithm 5**

RC4 obsoleto (RFC7465)

Cipher-String	OpenSSL syntax
Advanced (A)	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
Broad Compatibility (B)	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256
Widest Compatibility (C)	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
Legacy (D)	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES128-SHA:AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256:AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA

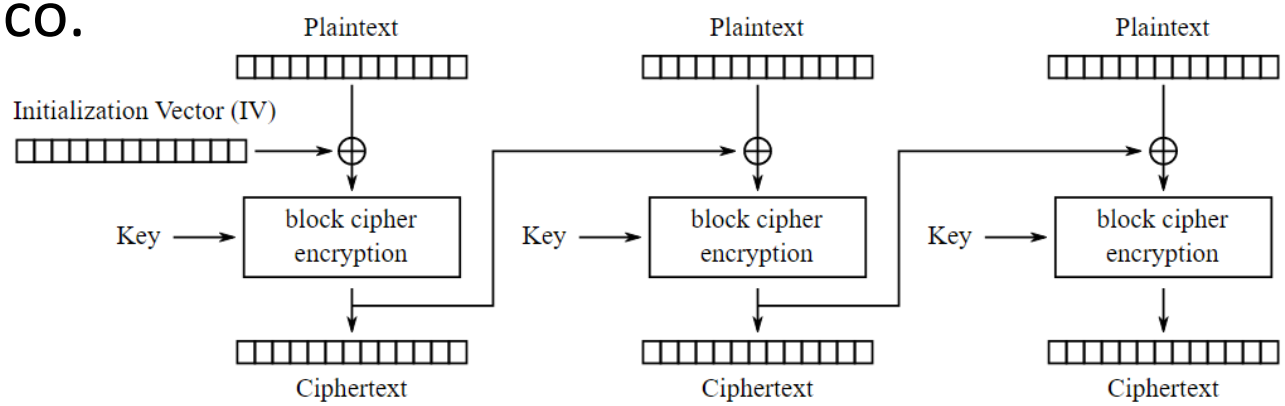
https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html

Exemplo de conjuntos de cifras TLS

Cipher ID	Name	Key Exchange	Authentication	Encryption	Bits	MAC
0x000000	TLS_NULL_WITH_NULL_NULL	NULL	NULL	NULL	0	NULL
0x000001	TLS_RSA_WITH_NULL_MD5	RSA	RSA	NULL	0	MD5
...	...	...	...	...	...	...
0x00002E	TLS_RSA_PSK_WITH_NULL_SHA	RSA	PSK	NULL	0	SHA
0x00002F	TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES_128_CBC	128	SHA
0x000030	TLS_DH_DSS_WITH_AES_128_CBC_SHA	DH	DSS	AES_128_CBC	128	SHA
0x000031	TLS_DH_RSA_WITH_AES_128_CBC_SHA	DH	RSA	AES_128_CBC	128	SHA
0x000032	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE	DSS	AES_128_CBC	128	SHA
0x000033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE	RSA	AES_128_CBC	128	SHA
0x000034	TLS_DH_Anon_WITH_AES_128_CBC_SHA	DH	Anon	AES_128_CBC	128	SHA
0x000035	TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES_256_CBC	256	SHA
0x000036	TLS_DH_DSS_WITH_AES_256_CBC_SHA	DH	DSS	AES_256_CBC	256	SHA
0x000037	TLS_DH_RSA_WITH_AES_256_CBC_SHA	DH	RSA	AES_256_CBC	256	SHA
0x000038	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE	DSS	AES_256_CBC	256	SHA
...	...	...	...	...	...	...

Cipher Block Chaining

- Antes de cifrar o texto plano, um XOR é feito entre o texto plano e o texto cifrado anterior
  - Cada bloco de texto cifrado depende de todos os blocos de texto plano processados até esse ponto.
  - Um vetor de inicialização deve ser usado no primeiro bloco.



Cipher Block Chaining (CBC) mode encryption

Fonte: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

MAC – Message Authentication Code

- Informação que confirma se a mensagem veio do remetente declarado (autenticidade) e não foi alterada (integridade)
- Requer:
  - Chave simétrica
  - Algoritmo para assinatura
  - Algoritmo de hash
- Diferente de assinatura digital
  - Assinatura digital requer chaves assimétricas e a certeza de que a chave pública é correta
  - MAC usa chave simétrica (requer apenas a garantia de que a chave é conhecida entre os parceiros)

Avaliação da Segurança do SSL/TLS

Cipher			Protocol version						Status
Type	Algorithm	Nominal strength (bits)	SSL 2.0	SSL 3.0 [n 1][n 2][n 3][n 4]	TLS 1.0 [n 1][n 3]	TLS 1.1 [n 1]	TLS 1.2 [n 1]	TLS 1.3 (Draft)	
Block cipher with mode of operation	AES GCM[32][n 5]	256, 128	N/A	N/A	N/A	N/A	Secure	Secure	Defined for TLS 1.2 in RFCs
	AES CCM[33][n 5]		N/A	N/A	N/A	N/A	Secure	Secure	
	AES CBC[n 6]		N/A	N/A	Depends on mitigations	Secure	Secure	N/A	
	Camellia GCM[34][n 5]	256, 128	N/A	N/A	N/A	N/A	Secure	Secure	
	Camellia CBC[35][n 6]		N/A	N/A	Depends on mitigations	Secure	Secure	N/A	
	ARIA GCM[36][n 5]	256, 128	N/A	N/A	N/A	N/A	Secure	Secure	
	ARIA CBC[36][n 6]		N/A	N/A	Depends on mitigations	Secure	Secure	N/A	
	SEED CBC[37][n 6]	128	N/A	N/A	Depends on mitigations	Secure	Secure	N/A	
	3DES EDE CBC[n 6][n 7]	112[n 8]	Insecure	Insecure	Insecure	Insecure	Insecure	N/A	
	GOST 28147-89 CNT[31][n 7]	256	N/A	N/A	Insecure	Insecure	Insecure		Defined in RFC 4357
	IDEA CBC[n 6][n 7][n 9]	128	Insecure	Insecure	Insecure	Insecure	N/A	N/A	Removed from TLS 1.2
	DES CBC[n 6][n 7][n 9]	56	Insecure	Insecure	Insecure	Insecure	N/A	N/A	
		40[n 10]	Insecure	Insecure	Insecure	N/A	N/A	N/A	Forbidden in TLS 1.1 and later
	RC2 CBC[n 6][n 7]	40[n 10]	Insecure	Insecure	Insecure	N/A	N/A	N/A	
Stream cipher	ChaCha20-Poly1305[42][n 5]	256	N/A	N/A	N/A	N/A	Secure	Secure	Defined for TLS 1.2 in RFCs
	RC4[n 11]	128	Insecure	Insecure	Insecure	Insecure	Insecure	N/A	Prohibited in all versions of TLS by RFC 7465
		40[n 10]	Insecure	Insecure	Insecure	N/A	N/A	N/A	
None	Null[n 12]	-	N/A	Insecure	Insecure	Insecure	Insecure	Insecure	Defined for TLS 1.2 in RFCs

Fonte: http://en.wikipedia.org/wiki/Transport_Layer_Security (Mar-2017)

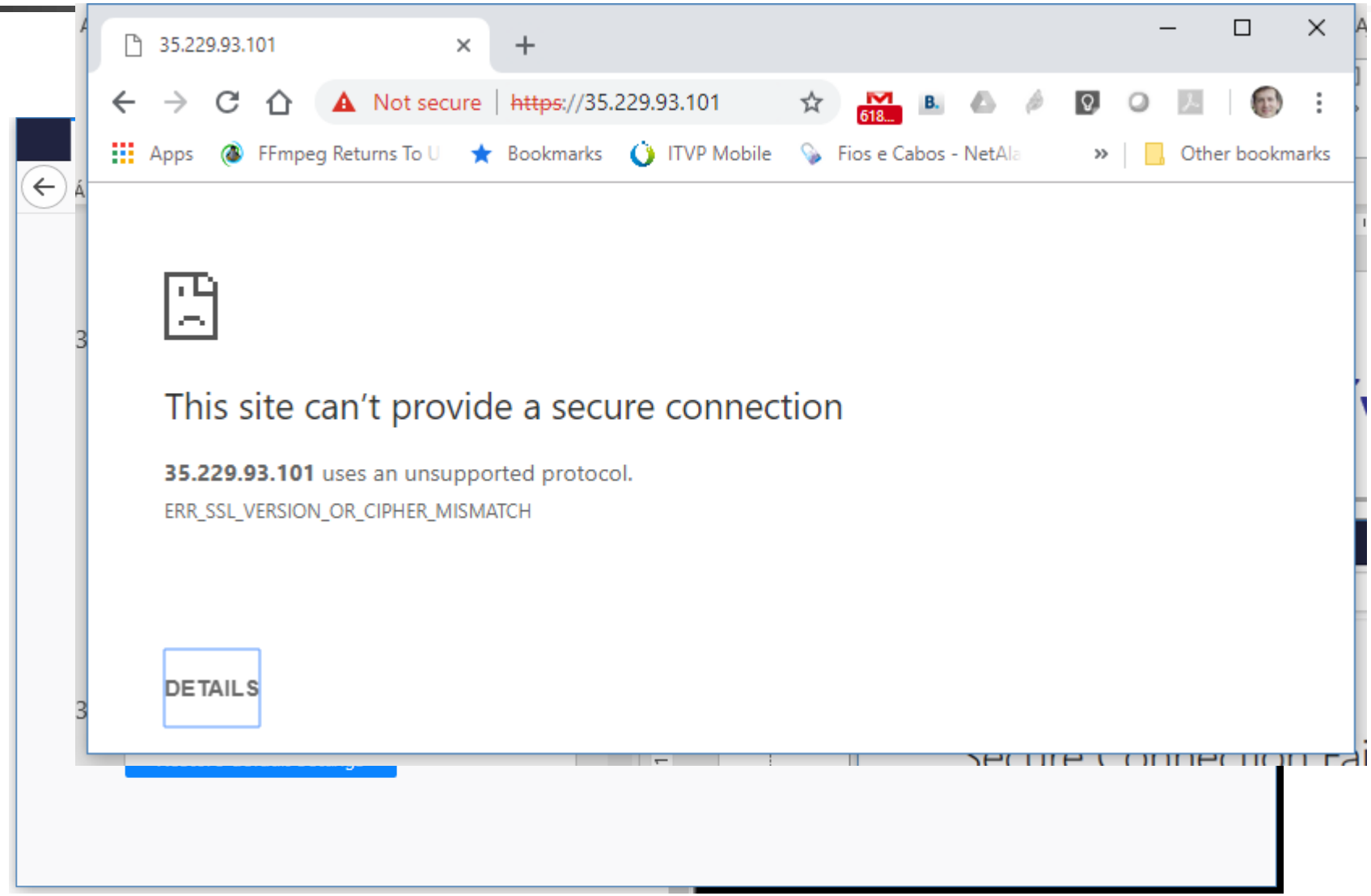
Testando TLS

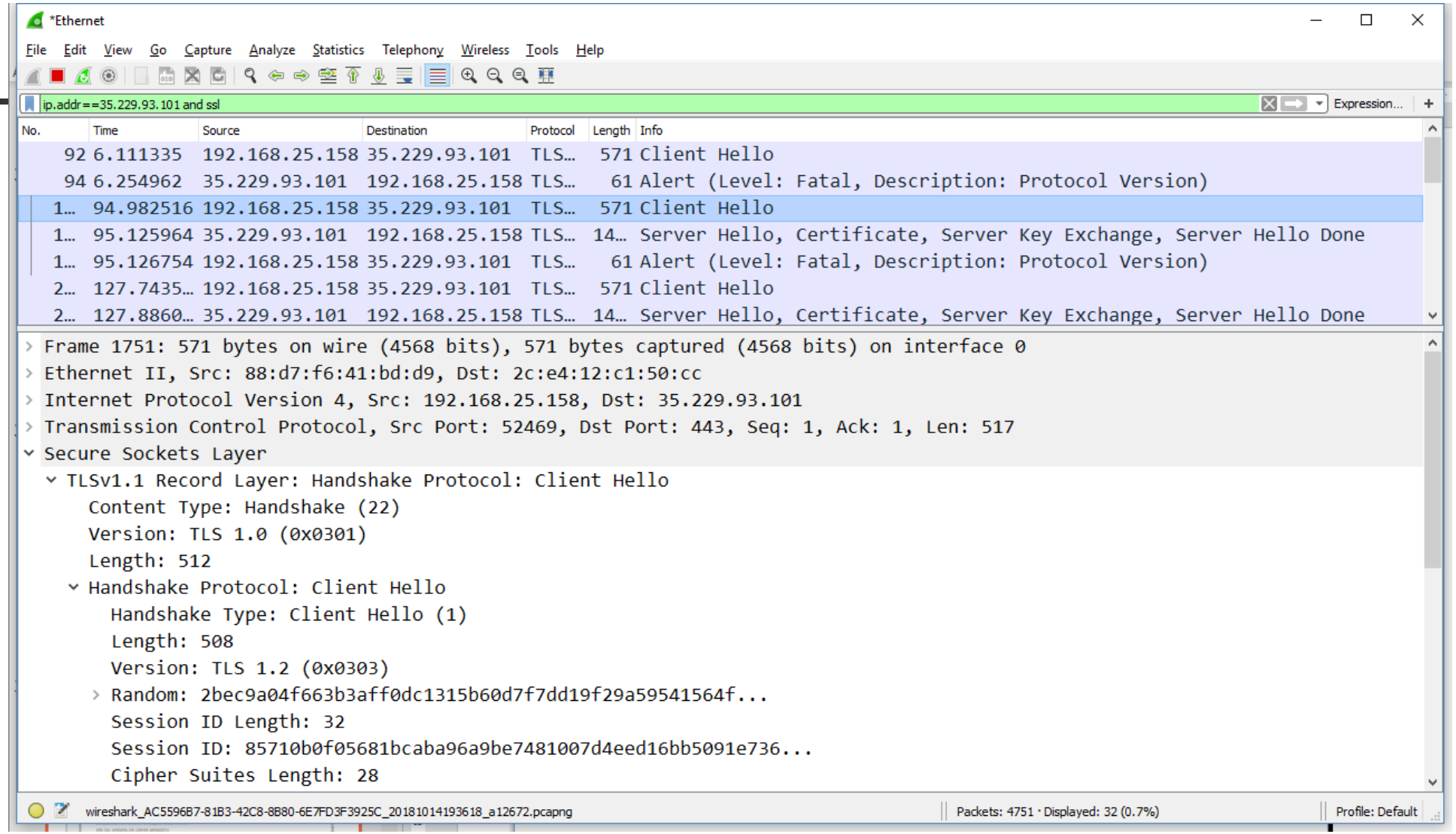
- Testando TLS
  - www.ssllabs.com/ssltest
- TLS
  - https://technet.microsoft.com/en-us/library/cc785811.aspx
  - https://sites.google.com/site/tlsssloverview/handshake-process
  - https://hpbn.co/transport-layer-security-tls/
  - http://www.pierobon.org/ssl/ch2/detail.htm
- Resumo de ataques TLS
  - https://tools.ietf.org/html/rfc7457

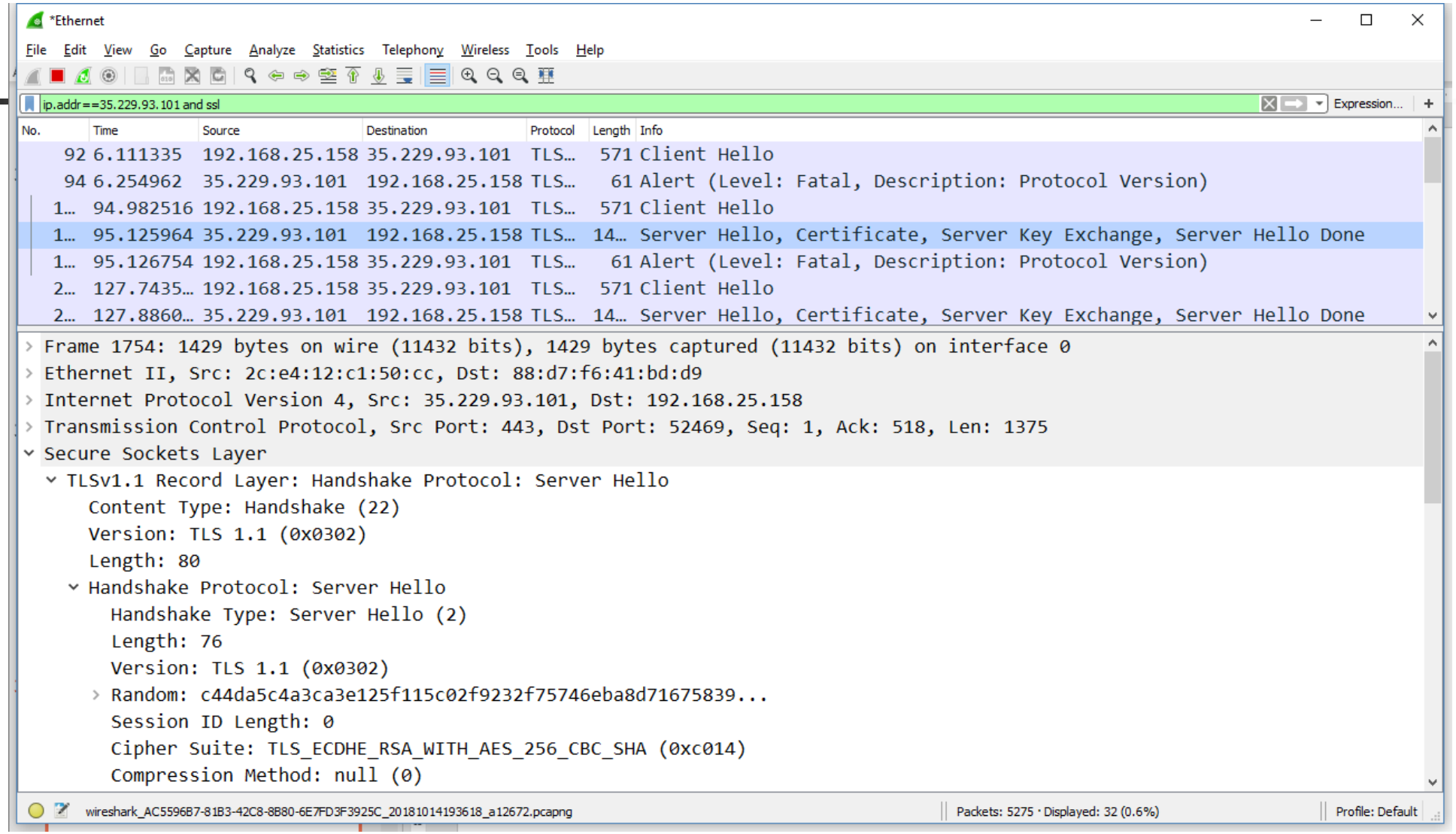
Referências

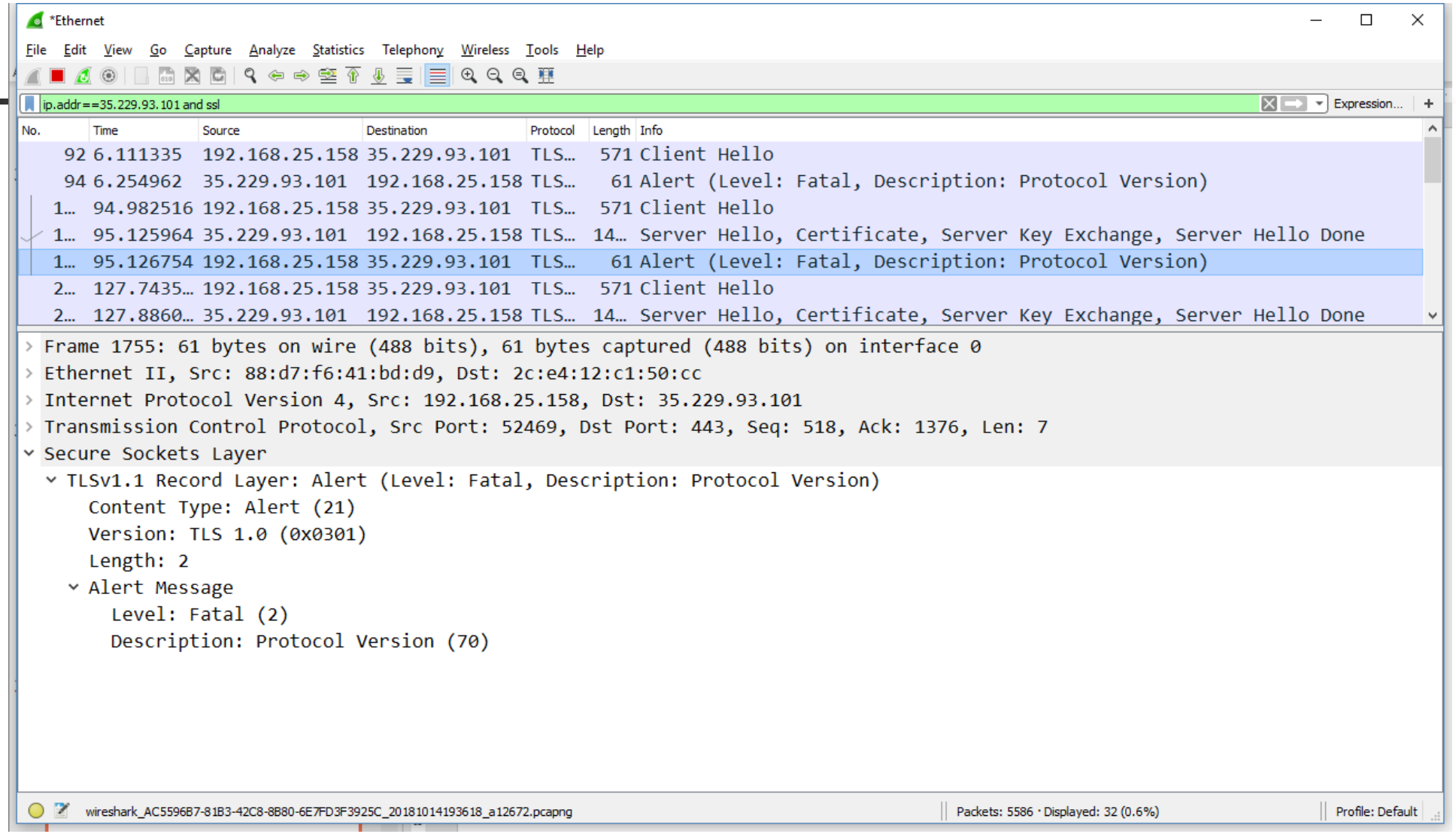
- MAC
  - https://en.wikipedia.org/wiki/Message_authentication_code
- Cipher Suites
  - http://www.thesprawl.org/research/tls-and-ssl-cipher-suites/
- TLS
  - http://blog.catchpoint.com/2017/05/12/dissecting-tls-using-wireshark/
  - https://tools.ietf.org/html/rfc5246

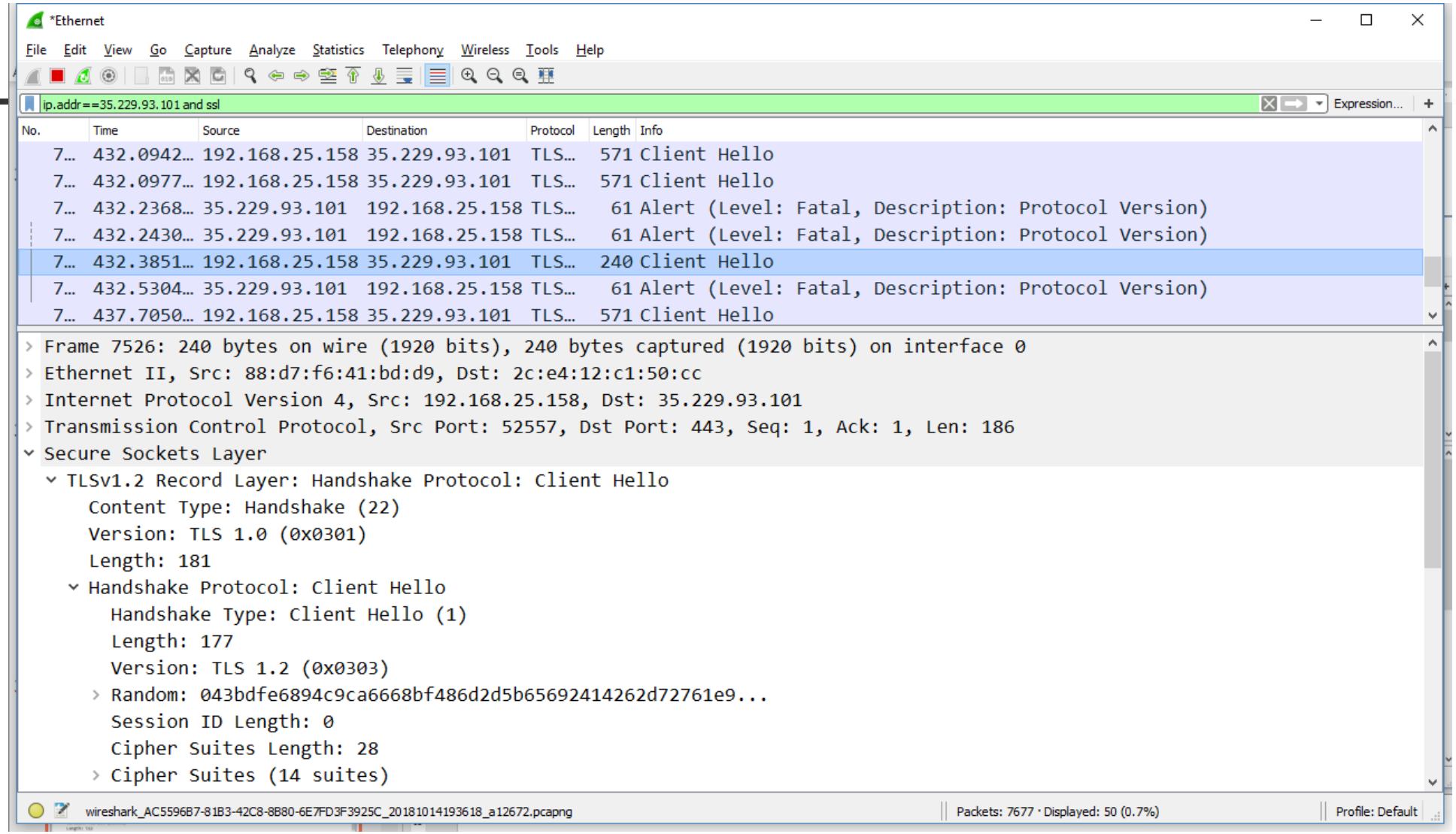
Versão incompatível do TLS

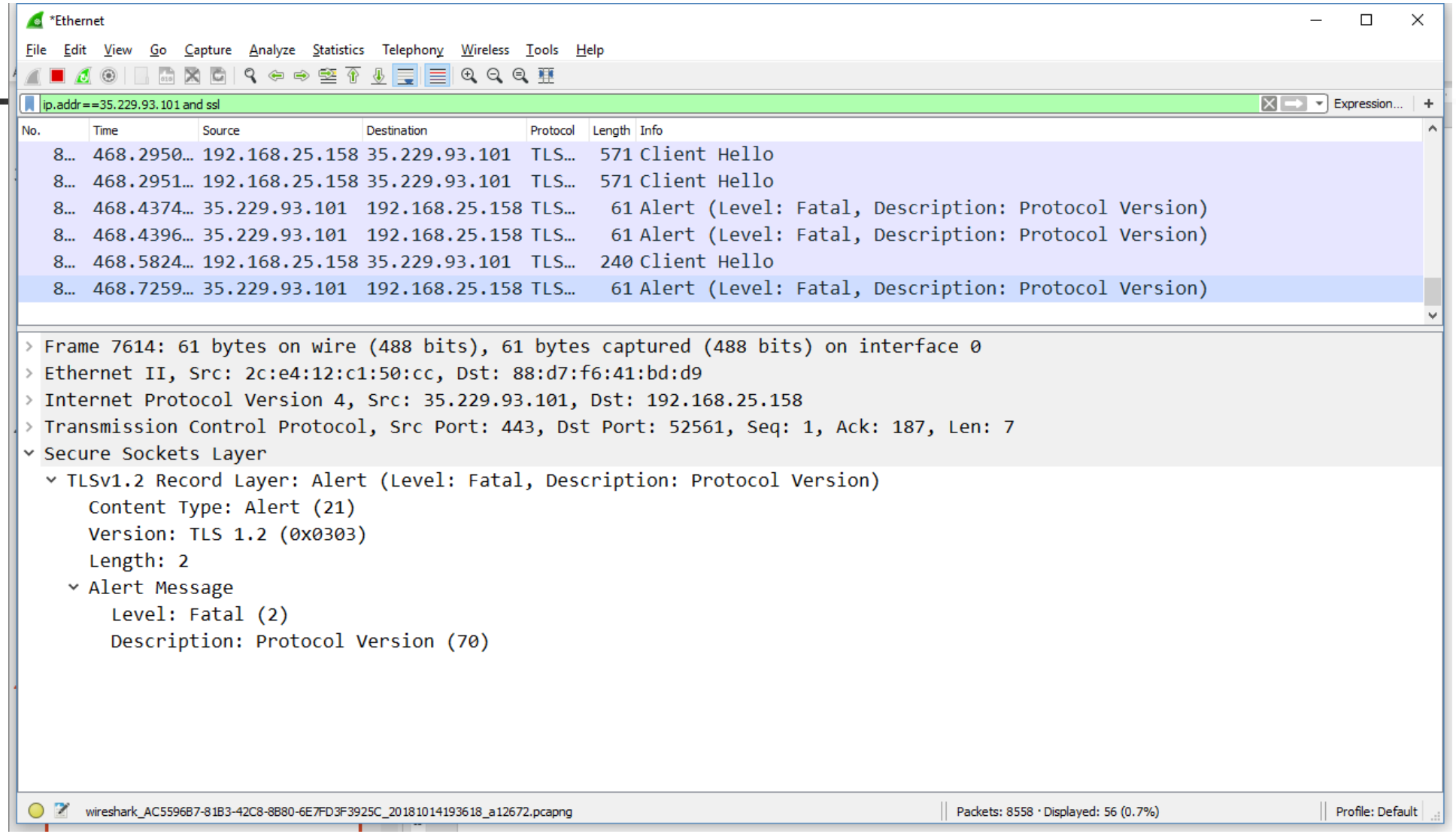



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==35.229.93.101 and ssl
Expression...
No. Time Source Destination Protocol Length Info
92 6.111335 192.168.25.158 35.229.93.101 TLS… 571 Client Hello
94 6.254962 35.229.93.101 192.168.25.158 TLS… 61 Alert (Level: Fatal, Description: Protocol Version)
1… 94.982516 192.168.25.158 35.229.93.101 TLS… 571 Client Hello
1… 95.125964 35.229.93.101 192.168.25.158 TLS… 14… Server Hello, Certificate, Server Key Exchange, Server Hello Done
1… 95.126754 192.168.25.158 35.229.93.101 TLS… 61 Alert (Level: Fatal, Description: Protocol Version)
2… 127.7435… 192.168.25.158 35.229.93.101 TLS… 571 Client Hello
2… 127.8860… 35.229.93.101 192.168.25.158 TLS… 14… Server Hello, Certificate, Server Key Exchange, Server Hello Done
Frame 1751: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0
Ethernet II, Src: 88:d7:f6:41:bd:d9, Dst: 2c:e4:12:c1:50:cc
Internet Protocol Version 4, Src: 192.168.25.158, Dst: 35.229.93.101
Transmission Control Protocol, Src Port: 52469, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Secure Sockets Layer
TLSv1.1 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: 2bec9a04f663b3aff0dc1315b60d7f7dd19f29a59541564f...
Session ID Length: 32
Session ID: 85710b0f05681bcaba96a9be7481007d4eed16bb5091e736...
Cipher Suites Length: 28
wireshark_AC5596B7-81B3-42C8-8B80-6E7FD3F3925C_20181014193618_a12672.pcapng
Packets: 4751 · Displayed: 32 (0.7%)
Profile: Default


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==35.229.93.101 and ssl
Expression...
No. Time Source Destination Protocol Length Info
92 6.111335 192.168.25.158 35.229.93.101 TLS… 571 Client Hello
94 6.254962 35.229.93.101 192.168.25.158 TLS… 61 Alert (Level: Fatal, Description: Protocol Version)
1… 94.982516 192.168.25.158 35.229.93.101 TLS… 571 Client Hello
1… 95.125964 35.229.93.101 192.168.25.158 TLS… 14… Server Hello, Certificate, Server Key Exchange, Server Hello Done
1… 95.126754 192.168.25.158 35.229.93.101 TLS… 61 Alert (Level: Fatal, Description: Protocol Version)
2… 127.7435… 192.168.25.158 35.229.93.101 TLS… 571 Client Hello
2… 127.8860… 35.229.93.101 192.168.25.158 TLS… 14… Server Hello, Certificate, Server Key Exchange, Server Hello Done
Frame 1754: 1429 bytes on wire (11432 bits), 1429 bytes captured (11432 bits) on interface 0
Ethernet II, Src: 2c:e4:12:c1:50:cc, Dst: 88:d7:f6:41:bd:d9
Internet Protocol Version 4, Src: 35.229.93.101, Dst: 192.168.25.158
Transmission Control Protocol, Src Port: 443, Dst Port: 52469, Seq: 1, Ack: 518, Len: 1375
Secure Sockets Layer
TLSv1.1 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.1 (0x0302)
Length: 80
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 76
Version: TLS 1.1 (0x0302)
Random: c44da5c4a3ca3e125f115c02f9232f75746eba8d71675839...
Session ID Length: 0
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Compression Method: null (0)
wireshark_AC5596B7-81B3-42C8-8B80-6E7FD3F3925C_20181014193618_a12672.pcapng
Packets: 5275 · Displayed: 32 (0.6%)
Profile: Default


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==35.229.93.101 and ssl
Expression...
No. Time Source Destination Protocol Length Info
92 6.111335 192.168.25.158 35.229.93.101 TLS… 571 Client Hello
94 6.254962 35.229.93.101 192.168.25.158 TLS… 61 Alert (Level: Fatal, Description: Protocol Version)
1… 94.982516 192.168.25.158 35.229.93.101 TLS… 571 Client Hello
1… 95.125964 35.229.93.101 192.168.25.158 TLS… 14… Server Hello, Certificate, Server Key Exchange, Server Hello Done
1… 95.126754 192.168.25.158 35.229.93.101 TLS… 61 Alert (Level: Fatal, Description: Protocol Version)
2… 127.7435… 192.168.25.158 35.229.93.101 TLS… 571 Client Hello
2… 127.8860… 35.229.93.101 192.168.25.158 TLS… 14… Server Hello, Certificate, Server Key Exchange, Server Hello Done
Frame 1755: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface 0
Ethernet II, Src: 88:d7:f6:41:bd:d9, Dst: 2c:e4:12:c1:50:cc
Internet Protocol Version 4, Src: 192.168.25.158, Dst: 35.229.93.101
Transmission Control Protocol, Src Port: 52469, Dst Port: 443, Seq: 518, Ack: 1376, Len: 7
Secure Sockets Layer
TLSv1.1 Record Layer: Alert (Level: Fatal, Description: Protocol Version)
Content Type: Alert (21)
Version: TLS 1.0 (0x0301)
Length: 2
Alert Message
Level: Fatal (2)
Description: Protocol Version (70)
wireshark_AC5596B7-81B3-42C8-8B80-6E7FD3F3925C_20181014193618_a12672.pcapng
Packets: 5586 · Displayed: 32 (0.6%)
Profile: Default


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==35.229.93.101 and ssl
Expression...
No. Time Source Destination Protocol Length Info
7... 432.0942... 192.168.25.158 35.229.93.101 TLS... 571 Client Hello
7... 432.0977... 192.168.25.158 35.229.93.101 TLS... 571 Client Hello
7... 432.2368... 35.229.93.101 192.168.25.158 TLS... 61 Alert (Level: Fatal, Description: Protocol Version)
7... 432.2430... 35.229.93.101 192.168.25.158 TLS... 61 Alert (Level: Fatal, Description: Protocol Version)
7... 432.3851... 192.168.25.158 35.229.93.101 TLS... 240 Client Hello
7... 432.5304... 35.229.93.101 192.168.25.158 TLS... 61 Alert (Level: Fatal, Description: Protocol Version)
7... 437.7050... 192.168.25.158 35.229.93.101 TLS... 571 Client Hello
Frame 7526: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits) on interface 0
Ethernet II, Src: 88:d7:f6:41:bd:d9, Dst: 2c:e4:12:c1:50:cc
Internet Protocol Version 4, Src: 192.168.25.158, Dst: 35.229.93.101
Transmission Control Protocol, Src Port: 52557, Dst Port: 443, Seq: 1, Ack: 1, Len: 186
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 181
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 177
Version: TLS 1.2 (0x0303)
Random: 043bdfe6894c9ca6668bf486d2d5b65692414262d72761e9...
Session ID Length: 0
Cipher Suites Length: 28
Cipher Suites (14 suites)
wireshark_AC5596B7-81B3-42C8-8B80-6E7FD3F3925C_20181014193618_a12672.pcapng
Packets: 7677 · Displayed: 50 (0.7%)
Profile: Default


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==35.229.93.101 and ssl
Expression...
No. Time Source Destination Protocol Length Info
8... 468.2950... 192.168.25.158 35.229.93.101 TLS... 571 Client Hello
8... 468.2951... 192.168.25.158 35.229.93.101 TLS... 571 Client Hello
8... 468.4374... 35.229.93.101 192.168.25.158 TLS... 61 Alert (Level: Fatal, Description: Protocol Version)
8... 468.4396... 35.229.93.101 192.168.25.158 TLS... 61 Alert (Level: Fatal, Description: Protocol Version)
8... 468.5824... 192.168.25.158 35.229.93.101 TLS... 240 Client Hello
8... 468.7259... 35.229.93.101 192.168.25.158 TLS... 61 Alert (Level: Fatal, Description: Protocol Version)
Frame 7614: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface 0
Ethernet II, Src: 2c:e4:12:c1:50:cc, Dst: 88:d7:f6:41:bd:d9
Internet Protocol Version 4, Src: 35.229.93.101, Dst: 192.168.25.158
Transmission Control Protocol, Src Port: 443, Dst Port: 52561, Seq: 1, Ack: 187, Len: 7
Secure Sockets Layer
TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Protocol Version)
Content Type: Alert (21)
Version: TLS 1.2 (0x0303)
Length: 2
Alert Message
Level: Fatal (2)
Description: Protocol Version (70)
wireshark_AC5596B7-81B3-42C8-8B80-6E7FD3F3925C_20181014193618_a12672.pcapng
Packets: 8558 · Displayed: 56 (0.7%)
Profile: Default