

# Tarefa Teórica - Handshake SSL/TLS(Secure Socket Layer/Transport Layer Security)

---

## Nomes

Bruno Aurélio Rôzza de Moura Campos (14104255)

Caio Cargnin Cardoso (09138003)

## PARTE 1

### Questão 1

É possível verificar as possibilidades do SSL/TLS do seu browser e do seu servidor. Cole os resultados (screenshot) aqui e comente o que chamou a sua atenção em cada um dos resultados.

**a. <https://www.ssllabs.com/> este site e teste o seu browser (diferentes tipos de browser podem ter resultados diferentes na sua máquina).**

**b. <https://www.ssllabs.com/> este site e teste um servidor que usa o SSL. Cuide para não acessar apenas um proxy de servidor real.**

**Obs.:** forward secrecy significa que se uma chave for comprometida durante uma sessão, esse conhecimento/fator não afeta a segurança de sessões anteriores. A troca de chaves RSA (RSA key Exchange) não fornece forward secrecy pois se alguma chave privada for comprometida, todo o tráfego anterior pode ser decifrado.

## Respostas

a.  
User Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.80 Safari/537.36



SSL/TLS Capabilities of Your Browser

[Other User Agents »](#)

User Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.80 Safari/537.36

Protocol Support

**Your user agent has good protocol support.**

Your user agent supports TLS 1.2, which is recommended protocol version at the moment.

Experimental: Your user agent supports TLS 1.3.

Logjam Vulnerability

**Your user agent is not vulnerable.**

For more information about the Logjam attack, please go to [weakdh.org](#).

To test manually, click [here](#). Your user agent is not vulnerable if it fails to connect to the site.

FREAK Vulnerability

**Your user agent is not vulnerable.**

For more information about the FREAK attack, please go to [www.freakattack.com](#).


To test manually, click [here](#). Your user agent is not vulnerable if it fails to connect to the site.

POODLE Vulnerability

**Your user agent is not vulnerable.**


For more information about the POODLE attack, please read [this blog post](#).

Protocol Features



Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No



Cipher Suites (in order of preference)

TLS_GREASE_4A (0x4a4a)	-
TLS_AES_128_GCM_SHA256 (0x1301) Forward Secrecy	128
TLS_AES_256_GCM_SHA384 (0x1302) Forward Secrecy	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Forward Secrecy	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc8) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128

TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) <b>WEAK</b>	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) <b>WEAK</b>	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) <b>WEAK</b>	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) <b>WEAK</b>	112

(1) When a browser supports SSL 2, its SSL 2-only suites are shown only on the very first connection to this site. To see the suites, close all browser windows, then open this exact page directly. Don't refresh.



Protocol Details

Server Name Indication (SNI)	Yes
Secure Renegotiation	Yes
<b>TLS compression</b>	<b>No</b>
Session tickets	Yes
OCSP stapling	Yes
Signature algorithms	SHA256/ECDSA, RSA_PSS_SHA256, SHA256/RSA, SHA384/ECDSA, RSA_PSS_SHA384, SHA384/RSA, RSA_PSS_SHA512, SHA512/RSA, SHA1/RSA
Named Groups	tls_grease_aaaa, x25519, secp256r1, secp384r1
Next Protocol Negotiation	No
Application Layer Protocol Negotiation	Yes h2 http/1.1
<b>SSL 2 handshake compatibility</b>	<b>No</b>

Mixed Content Handling



Mixed Content Tests

Images	Passive	<b>Yes</b>
CSS	Active	No
Scripts	Active	No
XMLHttpRequest	Active	No
WebSockets	Active	No
Frames	Active	No

- (1) These tests might cause a mixed content warning in your browser. That's expected.  
(2) If you see a failed test, try to reload the page. If the error persists, please get in touch.

Related Functionality

Upgrade Insecure Requests request header ( <a href="#">more info</a> )	Yes
--	-----

b.

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.secnet.com.br](#)

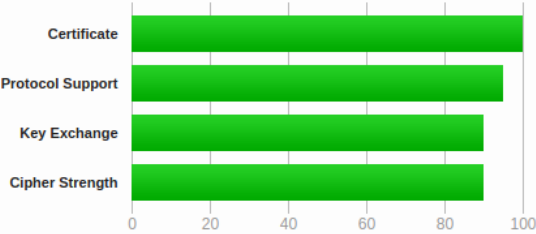
SSL Report: [www.secnet.com.br](#) (50.116.50.47)

Assessed on: Sun, 16 Jun 2019 23:06:54 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1



Subject	*.secnet.com.br Fingerprint SHA256: 6899dfc1e8ab548ebd9b2b39a9efc8734221f0ef3a20076ee2e4630523200810 Pin SHA256: AHZMZ1PW29g9A09cJYiwOQPnk44WnGP1RoAUzp+Pb00=
Common names	*.secnet.com.br
Alternative names	*.secnet.com.br secnet.com.br
Serial Number	00efbf7246d521fd30266b650140e7e824
Valid from	Fri, 09 Jun 2017 00:00:00 UTC
Valid until	Sun, 05 Jul 2020 23:59:59 UTC (expires in 1 year)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	COMODO RSA Domain Validation Secure Server CA AIA: http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSF Must Staple	No
Revocation information	CRL, OCSF CRL: http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl OCSF: http://ocsp.comodoca.com
Revocation status	Good (not revoked)
DNS CAA	No ( <a href="#">more info</a> )
Trusted	Yes Mozilla Apple Android Java Windows



## Additional Certificates (if supplied)



Certificates provided 4 (5399 bytes)

Chain issues Contains anchor

## #2

Subject	COMODO RSA Domain Validation Secure Server CA Fingerprint SHA256: 02ab57e4e67a0cb48dd2ff34830e8ac40f4476fb08ca6be3f5cd846f646840f0 Pin SHA256: kIO23nT2ehFDXCf3eHTDRESMz3asj1muO+4aidjiuY=
Valid until	Sun, 11 Feb 2029 23:59:59 UTC (expires in 9 years and 7 months)
Key	RSA 2048 bits (e 65537)
Issuer	COMODO RSA Certification Authority
Signature algorithm	SHA384withRSA

## #3

Subject	COMODO RSA Certification Authority Fingerprint SHA256: 4f32d5dc00f715250abcc486511e37f501a899deb3bf7ea8adbbd3aef1c412da Pin SHA256: grX4Ta9Hpz6tSHkmCrvpApTQGo67CYDnvpRLg5yRME=
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 11 months and 13 days)
Key	RSA 4096 bits (e 65537)
Issuer	AddTrust External CA Root
Signature algorithm	SHA384withRSA

## #4

Subject	AddTrust External CA Root <span>In trust store</span> Fingerprint SHA256: 687fa451382278ff0c8b11f8d43d576671c6eb2bceab413fb83d965d06d2ff2 Pin SHA256: lCpPFqbkrIJ3EcVFAkeip0+44VaoJUymbnOaEuk7iEU=
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 11 months and 13 days)
Key	RSA 2048 bits (e 65537)
Issuer	AddTrust External CA Root Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate



## Certification Paths



Mozilla Apple Android **Java** Windows

### Path #1: Trusted



1	Sent by server	*.secnet.com.br Fingerprint SHA256: 6899dfc1e8ab548ebd9b2b39a9efc8734221f0ef3a20076ee2e4630523200810 Pin SHA256: AHZMZ1PW29g9A09cJYiwOQPnk44WnGP1RoAUzp+Pb00= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	COMODO RSA Domain Validation Secure Server CA Fingerprint SHA256: 02ab57e4e67a0cb48dd2ff34830e8ac40f4476fb08ca6be3f5cd846f646840f0 Pin SHA256: kO23nT2ehFDXcf3eHTDRESMz3asj1muO+4aldjiuY= RSA 2048 bits (e 65537) / SHA384withRSA
3	In trust store	COMODO RSA Certification Authority Self-signed Fingerprint SHA256: 52f0e1c4e58ec629291b60317f074671b85d7ea80d5b07273463534b32b40234 Pin SHA256: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME= RSA 4096 bits (e 65537) / SHA384withRSA

### Path #2: Trusted



1	Sent by server	*.secnet.com.br Fingerprint SHA256: 6899dfc1e8ab548ebd9b2b39a9efc8734221f0ef3a20076ee2e4630523200810 Pin SHA256: AHZMZ1PW29g9A09cJYiwOQPnk44WnGP1RoAUzp+Pb00= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	COMODO RSA Domain Validation Secure Server CA Fingerprint SHA256: 02ab57e4e67a0cb48dd2ff34830e8ac40f4476fb08ca6be3f5cd846f646840f0 Pin SHA256: kO23nT2ehFDXcf3eHTDRESMz3asj1muO+4aldjiuY= RSA 2048 bits (e 65537) / SHA384withRSA
3	Sent by server	COMODO RSA Certification Authority Fingerprint SHA256: 4f32d5dc00f715250abcc486511e37f501a899deb3bf7ea8adbbd3aef1c412da Pin SHA256: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME= RSA 4096 bits (e 65537) / SHA384withRSA
4	Sent by server In trust store	AddTrust External CA Root Self-signed Fingerprint SHA256: 687fa51382278ff0c8b11f8d43d576671c6eb2bceab413fb83d965d06d2ff2 Pin SHA256: lCpPFqbkrU3EcVFAkeip0+44VaoJUymbnOaEuk7IEU= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

## Configuration



### Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we only support RFC 8446.



### Cipher Suites

#### # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128 WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128 WEAK
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 WEAK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 WEAK
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH secp256r1 (eq. 3072 bits RSA) FS	112 WEAK
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	WEAK	112

#### # TLS 1.1 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128 WEAK
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 WEAK
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH secp256r1 (eq. 3072 bits RSA) FS	112 WEAK
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	WEAK	112

#### # TLS 1.0 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128 WEAK
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 WEAK
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH secp256r1 (eq. 3072 bits RSA) FS	112 WEAK
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	WEAK	112





## Handshake Simulation

<a href="#">Android 2.3.7</a> <span>No SNI <sup>2</sup></span>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
<a href="#">Android 4.0.4</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.1.1</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.2.2</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.3</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 5.0.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 6.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 7.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Baidu Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Chrome 69 / Win 7</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Chrome 70 / Win 10</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Firefox 47 / Win 7</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Firefox 62 / Win 7</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Googlebot Feb 2018</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">IE 7 / Vista</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
<a href="#">IE 8 / XP</a> <span>No FS <sup>1</sup> No SNI <sup>2</sup></span>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA	
<a href="#">IE 8-10 / Win 7</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
<a href="#">IE 11 / Win 7</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
<a href="#">IE 11 / Win 8.1</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
<a href="#">IE 10 / Win Phone 8.0</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
<a href="#">IE 11 / Win Phone 8.1</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
<a href="#">IE 11 / Win Phone 8.1 Update</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
<a href="#">IE 11 / Win 10</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Edge 15 / Win 10</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Edge 13 / Win Phone 10</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Java 6u45</a> <span>No SNI <sup>2</sup></span>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
<a href="#">Java 7u25</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
<a href="#">Java 8u161</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">OpenSSL 0.9.8y</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
<a href="#">OpenSSL 1.0.1j</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">OpenSSL 1.0.2e</a> <span>R</span>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS

<a href="#">Safari 5.1.9 / OS X 10.6.8</a>	RSA 2048 (SHA256)	<b>TLS 1.0</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	<b>FS</b>
<a href="#">Safari 6 / iOS 6.0.1</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	<b>FS</b>
<a href="#">Safari 6.0.4 / OS X 10.8.4</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.0</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	<b>FS</b>
<a href="#">Safari 7 / iOS 7.1</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	<b>FS</b>
<a href="#">Safari 7 / OS X 10.9</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	<b>FS</b>
<a href="#">Safari 8 / iOS 8.4</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	<b>FS</b>
<a href="#">Safari 8 / OS X 10.10</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	<b>FS</b>
<a href="#">Safari 9 / iOS 9</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	<b>FS</b>
<a href="#">Safari 9 / OS X 10.11</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	<b>FS</b>
<a href="#">Safari 10 / iOS 10</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	<b>FS</b>
<a href="#">Safari 10 / OS X 10.12</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	<b>FS</b>
<a href="#">Apple ATS 9 / iOS 9</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	<b>FS</b>
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	<b>FS</b>
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	<b>FS</b>

#### # Not simulated clients (Protocol mismatch)


**IE 6 / XP** **No FS** <sup>1</sup> **No SNI** <sup>2</sup> Protocol mismatch (not simulated)

- (1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.  
 (2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.  
 (3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.  
 (R) Denotes a reference browser or client, with which we expect better effective security.  
 (All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).  
 (All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.




## Protocol Details

	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read <a href="#">this longer explanation</a> (2) Key usage data kindly provided by the <a href="#">Censys</a> network search engine; original DROWN website <a href="#">here</a> (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
<b>DROWN</b>	
<b>Secure Renegotiation</b>	<b>Supported</b>
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side ( <a href="#">more info</a> ) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )
Zombie POODLE	No ( <a href="#">more info</a> ) TLS 1.2: 0xc027
GOLDENDOODLE	No ( <a href="#">more info</a> ) TLS 1.2: 0xc027
OpenSSL 0-Length	No ( <a href="#">more info</a> ) TLS 1.2: 0xc027
Sleeping POODLE	No ( <a href="#">more info</a> ) TLS 1.2: 0xc027
<b>Downgrade attack prevention</b>	<b>Yes, TLS_FALLBACK_SCSV supported</b> ( <a href="#">more info</a> )
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No ( <a href="#">more info</a> )
Ticketbleed (vulnerability)	No ( <a href="#">more info</a> )
OpenSSL CCS vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No ( <a href="#">more info</a> )
ROBOT (vulnerability)	No ( <a href="#">more info</a> )
Forward Secrecy	With modern browsers ( <a href="#">more info</a> )
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
<b>OCSP stapling</b>	<b>Yes</b>
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No ( <a href="#">more info</a> )
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No ( <a href="#">more info</a> )
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	secp256r1, secp521r1, secp384r1, secp256k1 (server preferred order)
SSL 2 handshake compatibility	Yes




### HTTP Requests



1

https://www.secnet.com.br/ (HTTP/1.1 200 OK)

Date	Sun, 16 Jun 2019 23:04:26 GMT
Server	Apache
Accept-Ranges	bytes
Vary	Accept-Encoding,User-Agent
X-Mod-Pagespeed	1.13.35.2-0
Cache-Control	max-age=0, no-cache
X-Server	High Performance Servers - www.secnet.com.br
Referrer-Policy	
Pragma	public
Content-Length	219585
Connection	close
Content-Type	text/html; charset=UTF-8



### Miscellaneous

Test date	Sun, 16 Jun 2019 23:04:49 UTC
Test duration	124.894 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	cloud.secnet.host

## 2. Questão

Leia as recomendações da página <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices> e faça um pequeno resumo das seções 1 e 2 dessas recomendações.

## Respostas

### Chave privada e certificado

O TLS começa com a identificação criptográfica do servidor. Para isso, é usado uma chave privada forte afim de evitar ataques de falsificação de identidade. Para garantir a segurança, há algumas dicas como:

- **Use chaves particulares de 2048 bits:** Para grande parte dos sites, chaves RSA de 2048 já são o suficiente.
- **Proteger Chaves Privadas:** Restringindo o acesso, gerando chaves com entropia suficiente.
- **Garantir cobertura suficiente de Hostname:** É uma forma de garantir que todas as rotas estão acessíveis e evitar avisos de certificados inválidos.
- **Obter certificados de uma CA confiável:** Isso é, escolher uma Autoridade de Certificação (CA) que seja confiável e séria. Para escolher uma CA, deve-se levar em consideração:
  - **Postura de segurança:** uma opção é examinar seu histórico de segurança.
  - **As CAs com foco nos negócios:** cujas atividades constituem uma parte substancial de seus negócios, têm tudo a perder se algo der errado

- **Serviços oferecidos:** No mínimo, sua AC selecionada deve fornecer suporte para os métodos de revogação da Lista de Revogação de Certificados (CRL) e do Protocolo de Status de Certificados Online (OCSP), com disponibilidade e desempenho de rede sólidos.
- **Opções de gerenciamento de certificados** se for necessário operar um grande número de certificados e operar em um ambiente complexo, escolha uma autoridade de certificação que ofereça boas ferramentas para gerenciá-los.
- **Suporte** é uma tranquilidade ter um bom suporte.
- **Use Algoritmos de Assinatura de Certificado Forte:** A segurança do certificado depende (1) da força da chave privada que foi usada para assinar o certificado e (2) da força da função de hash usada na assinatura.

### Configuração

É uma garantia que as credenciais sejam apresentadas corretamente aos visitantes do site. Há uma série de medidas para ser levado em conta:

- **Use protocolos seguros:** Na maioria das implantações, o certificado do servidor sozinho é insuficiente; Dois ou mais certificados são necessários para construir uma cadeia completa de confiança.
- **Use Conjuntos de Codificação Segura** Existem cinco protocolos na família SSL / TLS: SSL v2, SSL v3, TLS v1.0, TLS v1.1 e TLS v1.2:
  - O SSL v2 é inseguro e não deve ser usado.
  - O SSL v3 é inseguro quando usado com HTTP (o ataque POODLE).
  - O TLS v1.0 também é um protocolo legado que não deve ser usado.
  - O TLS v1.1 e v1.2 são ambos sem problemas de segurança conhecidos
  - O TLS v1.2 deve ser seu protocolo principal porque é a única versão que oferece criptografia autenticada moderna
- **Use Conjuntos de Codificação Segura:** Em SSL e TLS, os conjuntos de criptografia definem como a comunicação segura ocorre. Eles são compostos de diferentes blocos de construção com a idéia de alcançar a segurança através da diversidade. Se um dos blocos de construção for fraco ou inseguro, é possível mudar para outro.
- **Selecione as melhores suítes de codificação:** Ter servidores selecionando ativamente o melhor conjunto de criptografia disponível é fundamental para obter a melhor segurança.
- **Use o sigilo antecipado:** O sigilo de encaminhamento (às vezes também chamado de sigilo de encaminhamento perfeito) é um recurso de protocolo que permite conversas seguras que não dependem da chave privada do servidor.
- **Use troca de chaves forte:** Para a troca de chaves, os sites públicos normalmente podem escolher entre a troca de chaves Diffie-Hellman (DHE) efêmera clássica e sua variante de curva elíptica, ECDHE.
- **Mitigar Problemas Conhecidos:** Nada é perfeitamente seguro, e é por isso que é uma boa prática ficar de olho no que acontece na segurança. Aplique prontamente correções de fornecedores se e

quando elas estiverem disponíveis; caso contrário, confie em soluções alternativas para mitigação.

### 3. Questão

Explique de forma geral as quatro fases do handshake de acordo com as páginas do livro do Stallings 386, 387, 388 e 389 (o pdf do capítulo está anexado junto na tarefa).

#### Respostas

- 1. Estabelecer capacidades de segurança:** É a fase que inicia a comunicação. O cliente envia mensagem contendo alguns parâmetros:
  - versão do SSL
  - ID da sessão
  - Conjunto de cifras (cipherSuite) - é uma lista contendo algoritmo de troca de chave. Por exemplo, RSA, Diffie-Hellman, Diffie-Hellman anônimo Fortezza
  - Método de compactação(compression method) - é uma lista dos métodos de compactação que o cliente admite Em seguida, o cliente aguarda a resposta do servidor.
- 2. Autenticação de servidor e troca de chaves:** Nesta etapa, o servidor encaminha seus certificados, se necessário autenticar. A mensagem de certificado é exigida para qualquer troca de chaves que tenham sido acordadas, exceto se for Diffie-Hellman anônimo. A mensagem final desta fase é sempre exigida, é uma mensagem `server_done` enviada pelo servidor para indicar o final da resposta dele. Em seguida, o servidor aguardará uma resposta do cliente
- 3. Autenticação do cliente e troca de chaves:** Quando o cliente recebe uma mensagem `server_done` ele verifica se o certificado é válido e se os parâmetros `server_hello` são aceitáveis. Se tudo ok, o cliente responde seja com uma mensagem `certificate` ou `no_certificate`. Na sequência, é recebido uma mensagem `client_key_exchange` contendo algum conjunto de cifras:
  - RSA
  - Diffie-Hellman anônimo ou efêmero
  - Diffie-Hellman fixo
  - Fortezza No fim desta fase, o cliente pode enviar uma mensagem `certificate_verify` para oferecer uma certificação explícita de um certificado. Contudo, essa mensagem só é enviada após qualquer certificado que tenha capacidade de assinatura, ou seja qualquer certificado menos Diffie-Hellman fixo
- 4. Término:** Na última etapa, o cliente envia uma mensagem `change_cipher_spec`. Cabe notar que essa mensagem não é considerada parte do protocolo de estabelecimento de sessão mas sim enviada usando o protocolo de mudança de especificação de cifra. Além da mensagem anterior, o cliente encaminha a mensagem `finished_message` sob os novos algoritmos, chaves e segredos. Em resposta, o servidor envia sua mensagem `change_cipher_spec`, transfere o CipherSpec pendente para o atual e envia sua `finished_message`. A partir daqui, o cliente e servidor podem trocar dados na camada de aplicação.

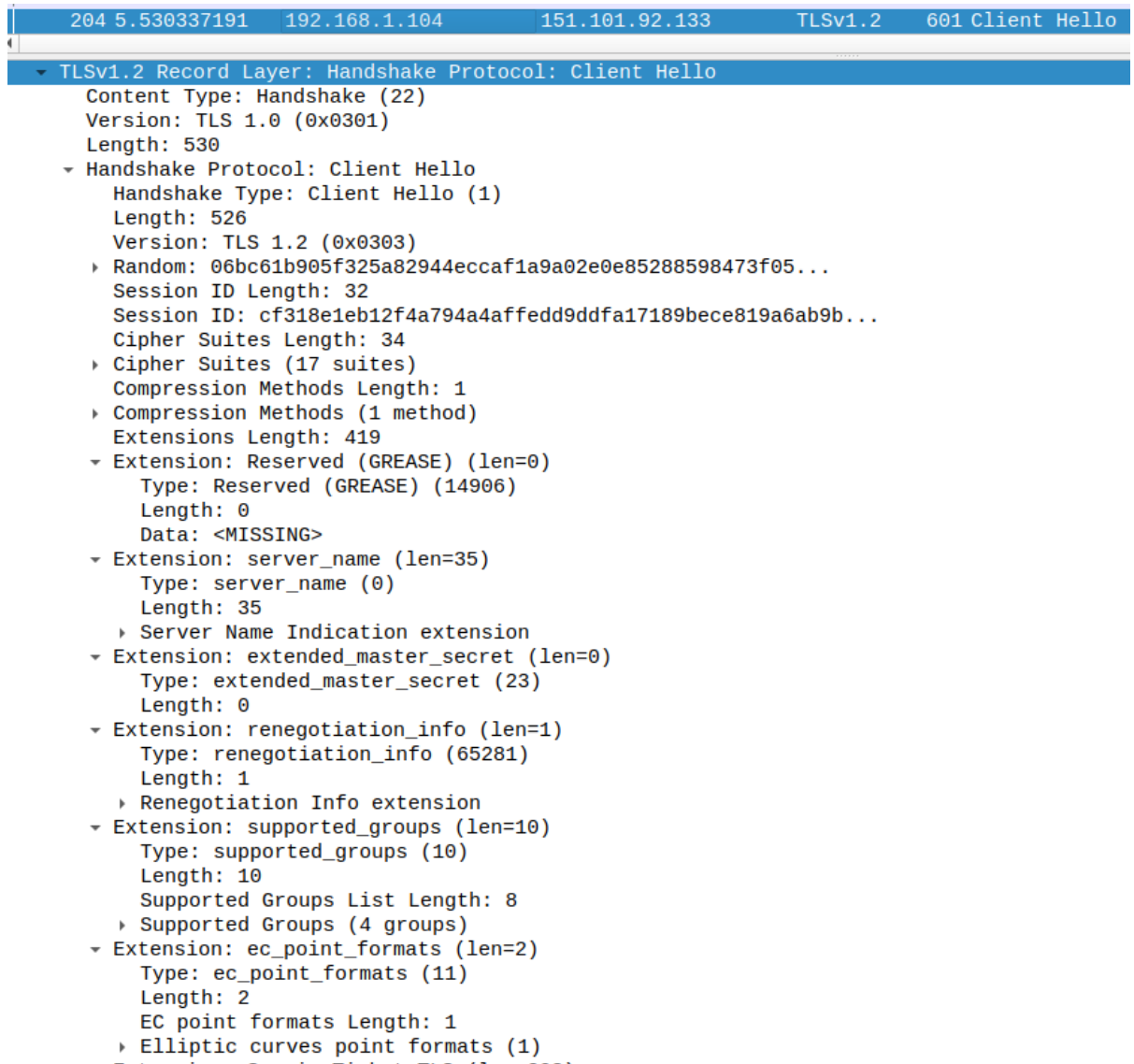
### 4. Questão - Coleta de um tráfego de handshake TLS

Você deve capturar um handshake do TLS no Wireshark: ative a captura de pacotes no Wireshark, abra a conexão com um site que usa HTTPS e capture o tráfego. Depois de estabelecer a conexão segura, pare a

captura, salve a capture com seu nome (para entregar no moodle o arquivo). Comente um pouco o handshake do seu tráfego.

## Respostas

- A comunicação foi estabelecida com o endereço: <https://github.com/>
- É possível notar claramente as 4 etapas do handshake em cada mensagem
  - Estabelecer capacidades de segurança



- Autenticação de servidor e troca de chaves

▼ TLSv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)  
Version: TLS 1.2 (0x0303)  
Length: 122

▼ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)  
Length: 118  
Version: TLS 1.2 (0x0303)  
Random: a1bb5c307b39e98a850047f6b03a38fb58c421615883ba42...  
Session ID Length: 32  
Session ID: d3dcf0a0d0ef6be176c05a3e3d4b65f3829e41f6e8c102ef...  
Cipher Suite: TLS\_AES\_128\_GCM\_SHA256 (0x1301)  
Compression Method: null (0)  
Extensions Length: 46

▼ Extension: supported\_versions (len=2)

Type: supported\_versions (43)  
Length: 2  
Supported Version: TLS 1.3 (0x0304)

▼ Extension: key\_share (len=36)

Type: key\_share (51)  
Length: 36

▼ Key Share extension

► Key Share Entry: Group: x25519. Key Exchange length: 32

54.2.77.6633560	185.199.110.154	192.168.1.104	TLSv1.2	1091	Certificate, Certificate Status, Server Key Exchange
▼ Secure Sockets Layer					
▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate					
Content Type: Handshake (22)					
Version: TLS 1.2 (0x0303)					
Length: 2991					
► Handshake Protocol: Certificate					
▼ Secure Sockets Layer					
▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate Status					
Content Type: Handshake (22)					
Version: TLS 1.2 (0x0303)					
Length: 479					
▼ Handshake Protocol: Certificate Status					
Handshake Type: Certificate Status (22)					
Length: 475					
Certificate Status Type: OCSP (1)					
OCSP Response Length: 471					
► OCSP Response					
▼ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange					
Content Type: Handshake (22)					
Version: TLS 1.2 (0x0303)					
Length: 300					
► Handshake Protocol: Server Key Exchange					
▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done					
Content Type: Handshake (22)					
Version: TLS 1.2 (0x0303)					
Length: 4					
▼ Handshake Protocol: Server Hello Done					
Handshake Type: Server Hello Done (14)					
Length: 0					

- Autenticação do cliente e troca de chaves

#### Secure Sockets Layer

#### ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 70

#### ▼ Handshake Protocol: Client Key Exchange

Handshake Type: Client Key Exchange (16)

Length: 66

#### ▼ EC Diffie-Hellman Client Params

Pubkey Length: 65

Pubkey: 046715fa4feb481f9d9fb1b847330fa38d3baf001bbb38eb...