Matei Teodor – 323 CA

Exercitiul 1

Cifru folosit: TLS\_AES\_256\_GCM\_SHA384

Validity

Not Before: Jun 15 00:00:42 2017 GMT

Not After : Dec 15 00:00:42 2021 GMT

Issuer: OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:d0:18:cf:45:d4:8b:cd:d3:9c:e4:40:ef:7e:b4:

dd:69:21:1b:c9:cf:3c:8e:4c:75:b9:0f:31:19:84:

3d:9e:3c:29:ef:50:0d:10:93:6f:05:80:80:9f:2a:

a0:bd:12:4b:02:e1:3d:9f:58:16:24:fe:30:9f:0b:

74:77:55:93:1d:4b:f7:4d:e1:92:82:10:f6:51:ac:

0c:c3:b2:22:94:0f:34:6b:98:10:49:e7:0b:9d:83:

39:dd:20:c6:1c:2d:ef:d1:18:61:65:e7:23:83:20:

a8:23:12:ff:d2:24:7f:d4:2f:e7:44:6a:5b:4d:d7:

50:66:b0:af:9e:42:63:05:fb:e0:1c:c4:63:61:af:

9f:6a:33:ff:62:97:bd:48:d9:d3:7c:14:67:dc:75:

dc:2e:69:e8:f8:6d:78:69:d0:b7:10:05:b8:f1:31:

c2:3b:24:fd:1a:33:74:f8:23:e0:ec:6b:19:8a:16:

c6:e3:cd:a4:cd:0b:db:b3:a4:59:60:38:88:3b:ad:

1d:b9:c6:8c:a7:53:1b:fc:bc:d9:a4:ab:bc:dd:3c:

61:d7:93:15:98:ee:81:bd:8f:e2:64:47:20:40:06:

4e:d7:ac:97:e8:b9:c0:59:12:a1:49:25:23:e4:ed:

70:34:2c:a5:b4:63:7c:f9:a3:3d:83:d1:cd:6d:24:

ac:07

Exponent: 65537 (0x10001)

Cifru folosit: TLS\_AES\_256\_GCM\_SHA384

Issuer: C = US, O = Google Trust Services, CN = GTS CA 1O1

Validity

Not Before: Apr 15 20:16:47 2020 GMT

Not After : Jul 8 20:16:47 2020 GMT

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

04:8e:a4:03:0d:0c:a7:1d:52:28:80:ba:89:51:b9:

45:7a:7a:60:33:a5:ab:25:a4:05:c8:32:d9:b6:5c:

2b:ba:05:a7:6d:2d:e1:66:36:48:30:da:5b:27:28:

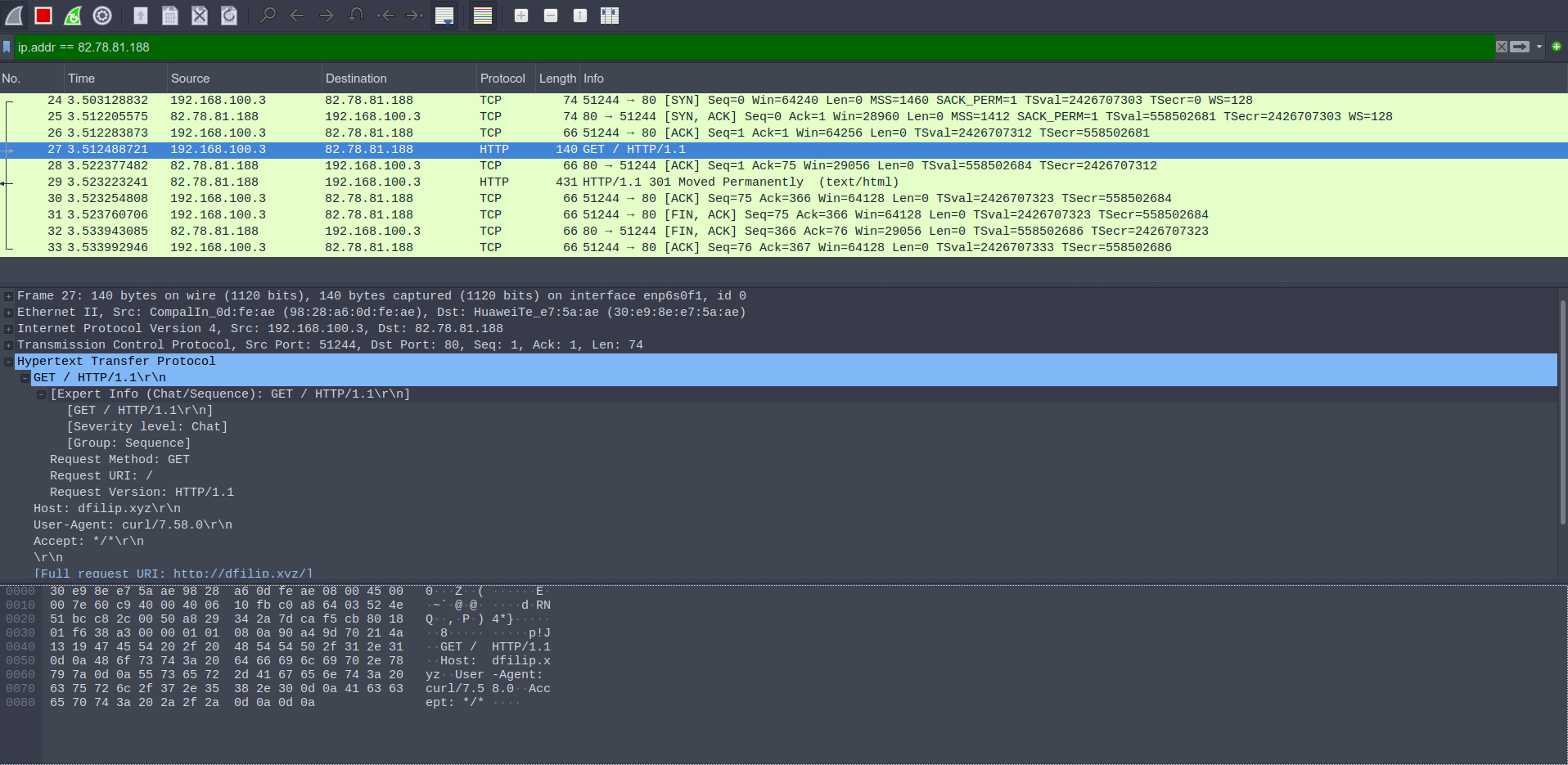
08:45:60:83:90:67:3b:51:ef:d0:e2:85:81:9b:49:

c3:50:56:d8:a9

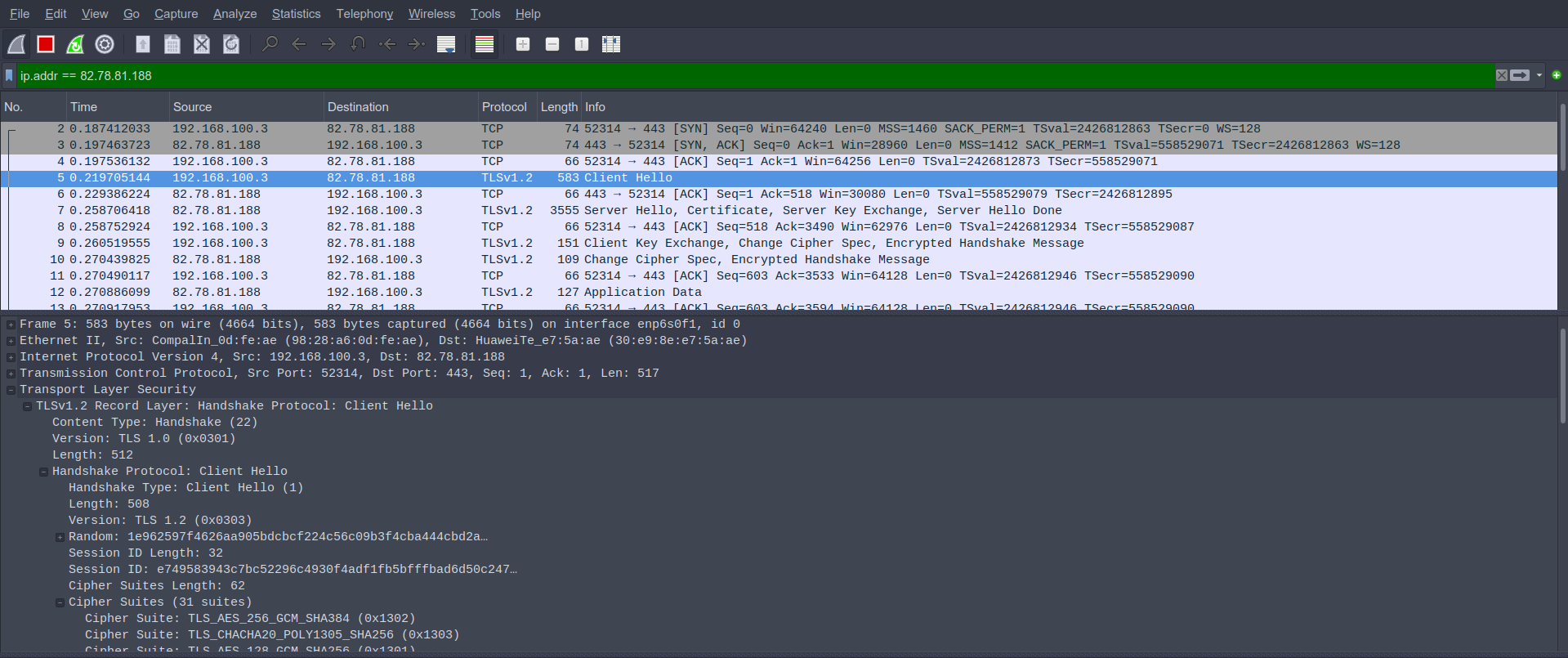
ASN1 OID: prime256v1

NIST CURVE: P-256

Exercitiul 2

Captura pentru logare pe http:

Captura pentru logare pe https:



Exercitiul 3

Versiune TLS: TLS 1.2 (0x0303)

Cipher Suites (31 suites)

Cipher Suite: TLS\_AES\_256\_GCM\_SHA384 (0x1302)

Cipher Suite: TLS\_CHACHA20\_POLY1305\_SHA256 (0x1303)

Cipher Suite: TLS\_AES\_128\_GCM\_SHA256 (0x1301)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009f)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca9)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca8)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xccaa)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009e)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc024)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x006b)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc023)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc027)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x0067)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc00a)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0039)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA (0xc009)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x0033)

Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009d)

Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009c)

Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003d)

Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003c)

Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)

Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f)

Cipher Suite: TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV (0x00ff)

Cifrul serverului:

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca8)

Exercitiul 4

M-am logat pe grid si am trimis cateva comenzi in terminal, se observa ca toate sunt criptate.

