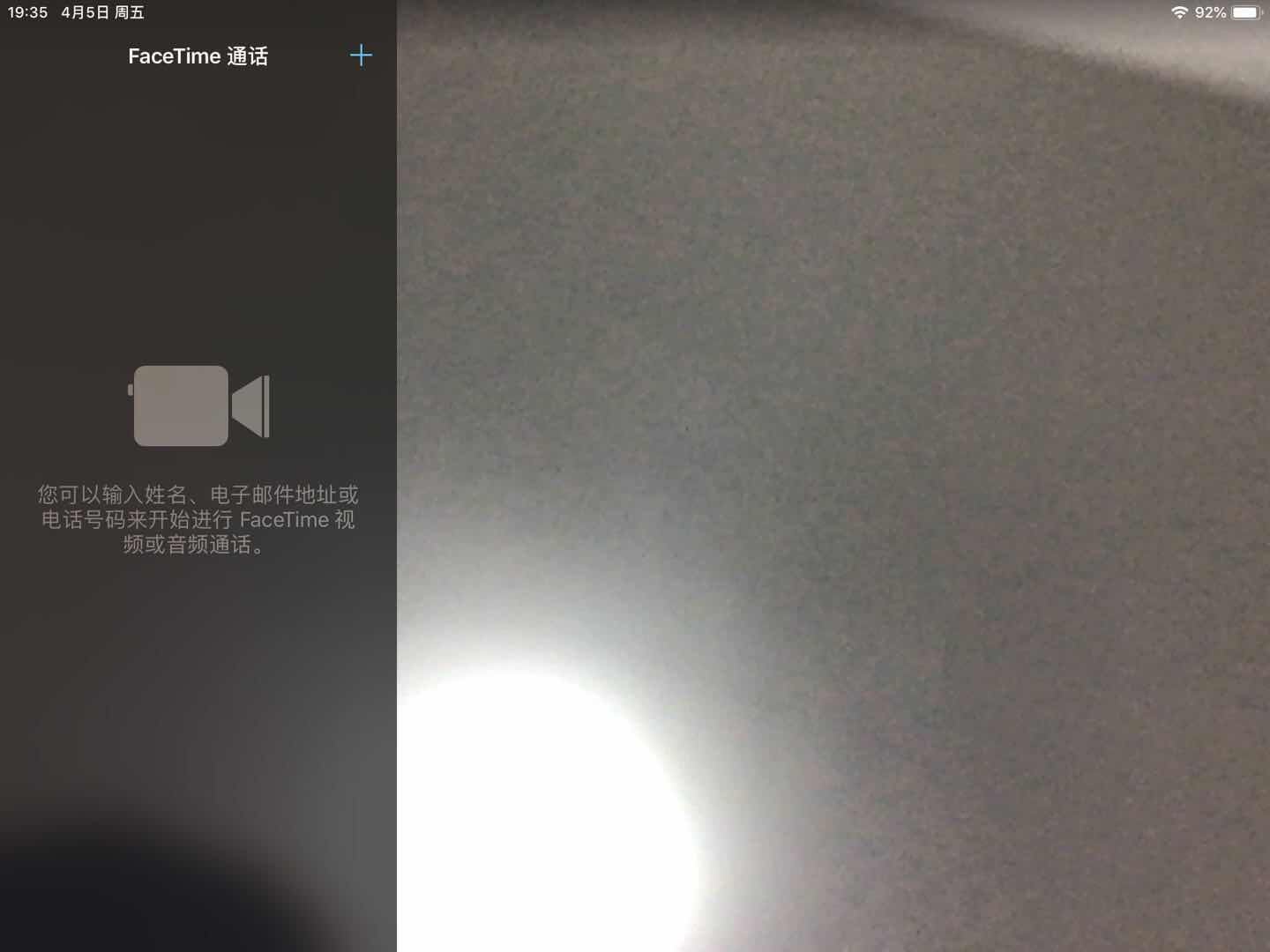
Youtube分析报告

陈力恒 201828015029025 软件所

# 简介

FaceTime是苹果公司iOS和Mac OS X内置的一款视频通话软件，通过Wi-Fi或者蜂窝数据接入互联网，在两个装有FaceTime的设备之间实现视频通话。其要求通话双方均具有装有FaceTime的苹果设备，苹果ID以及可接入互联网的3G/4G或者Wi-Fi网络。

FaceTime界面如图：



# 软件使用情况

本次分析针对IPad端IOS中的Facetime进行，分析其中TLS流量。

# 测试环境搭建

受测操作系统：IOS 12.2

受测软件：Facetime

操作系统：Windows 10

抓包软件：Wireshark Version 3.0.0 (v3.0.0-0-g937e33de)

Fiddler v5.0.20182.28034 for .NET 4

编程软件：Visual Studio 2017

其他：Winpcap库

# 分析工具及要求

PC端开启热点，IOS设备连接热点，Wireshark进行抓包，保存至Pcap文件，用Fiddler对密文解密。利用Visual Studio 开发程序对Pcap文件进行深度分析。对TLS中的可提取的明文信息进行提取。

# 测试条件

PC端开启热点供IOS设备连接。

# 主要功能及其使用

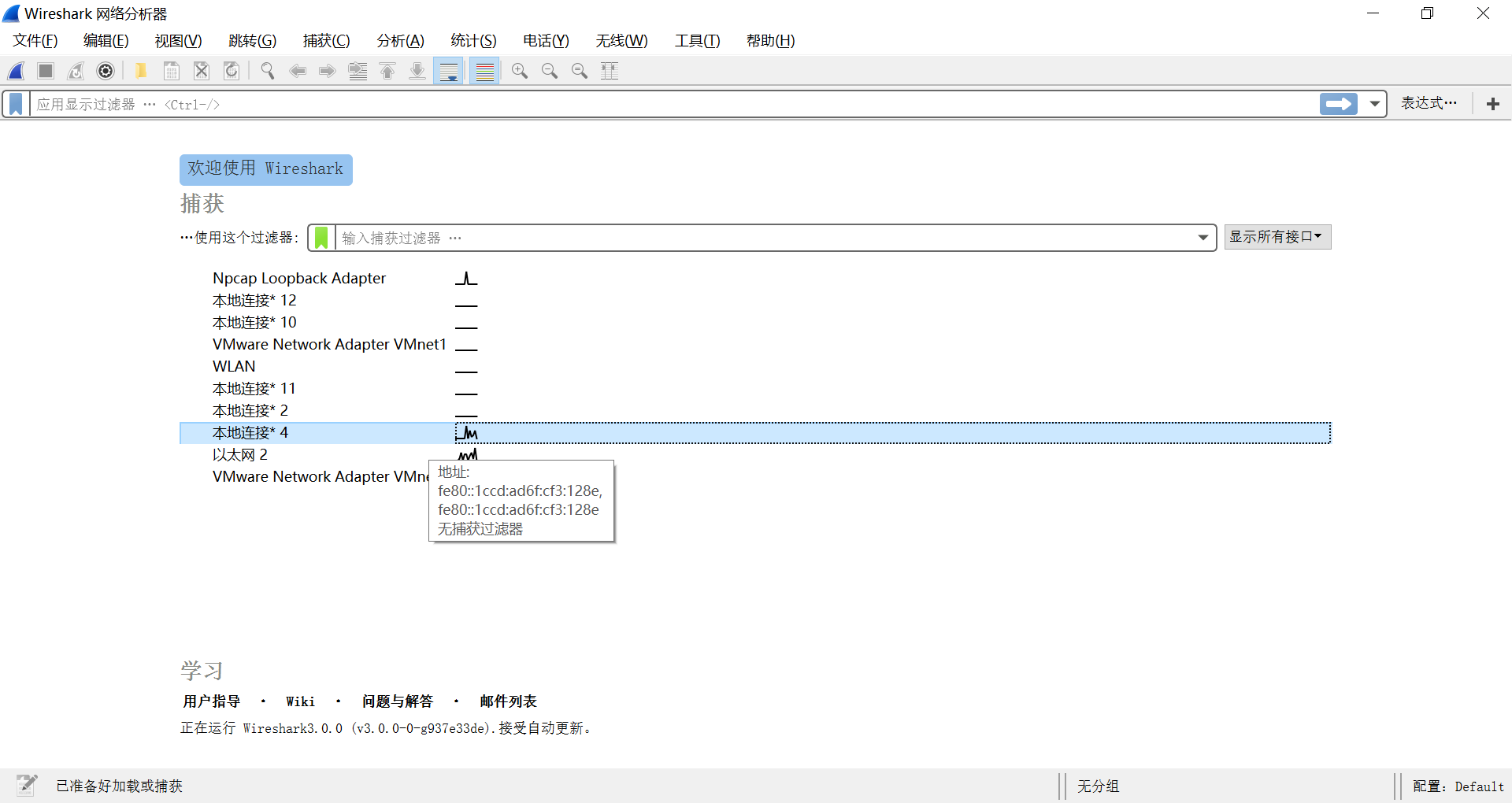
打开Facetime，添加好友，进行视频通话。

# 抓包过程

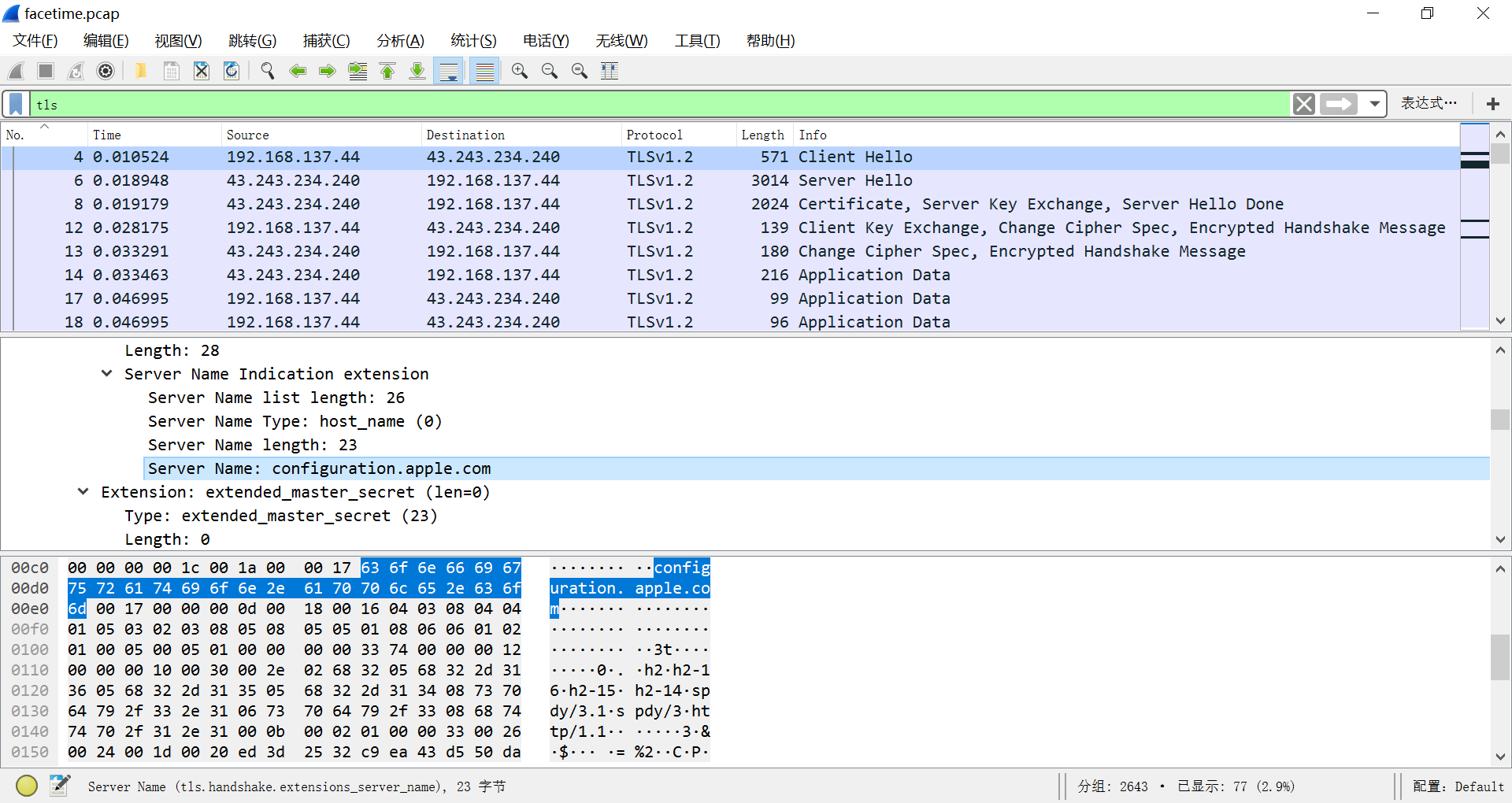
* 笔记本开启热点，让IPad连接。



* 本地连接4，就是IPad的上网流量。



* 进入后便开始抓包。



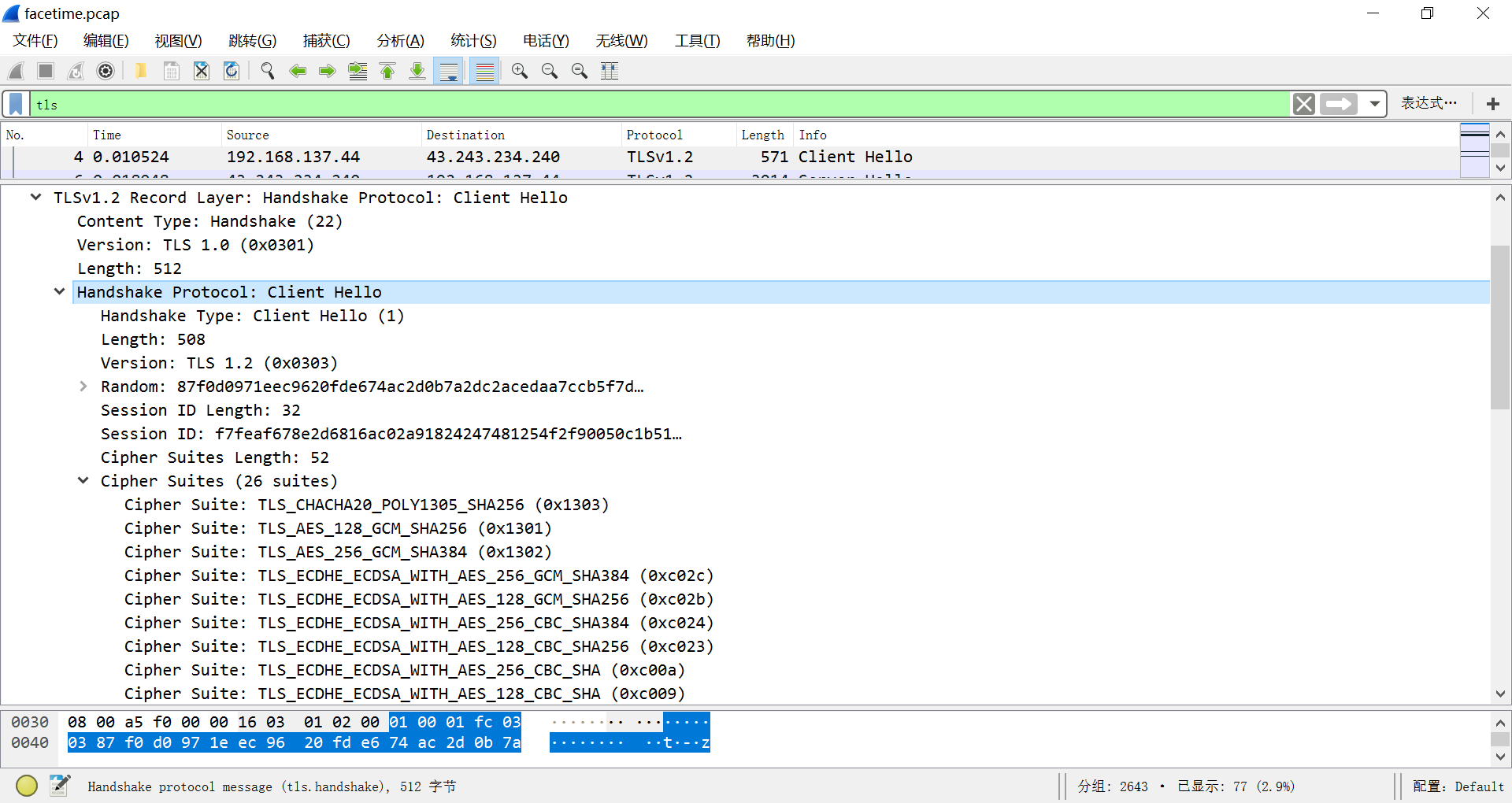
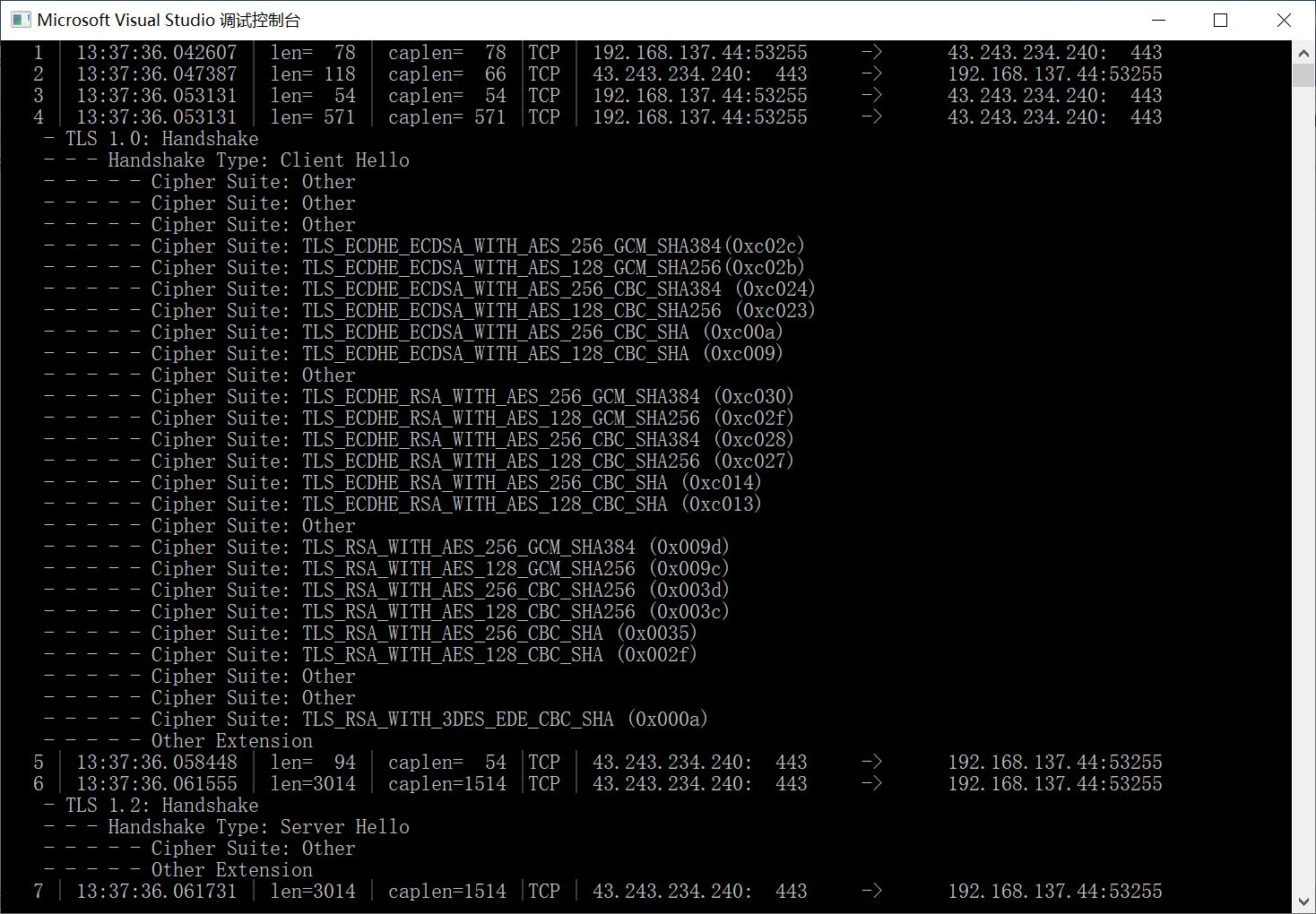
* 保存成facetime.pcap文件。

# 编程分析Pcap

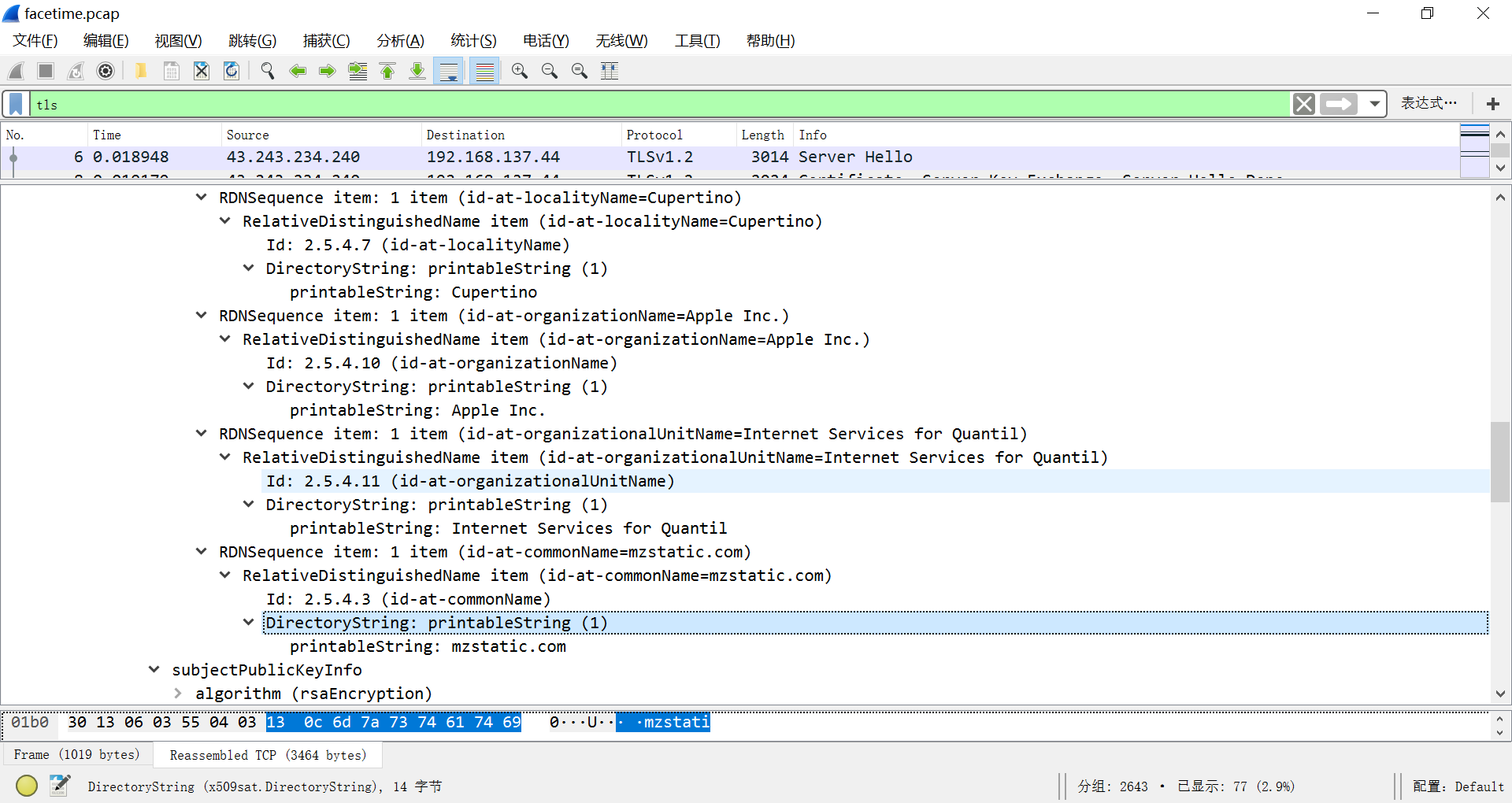
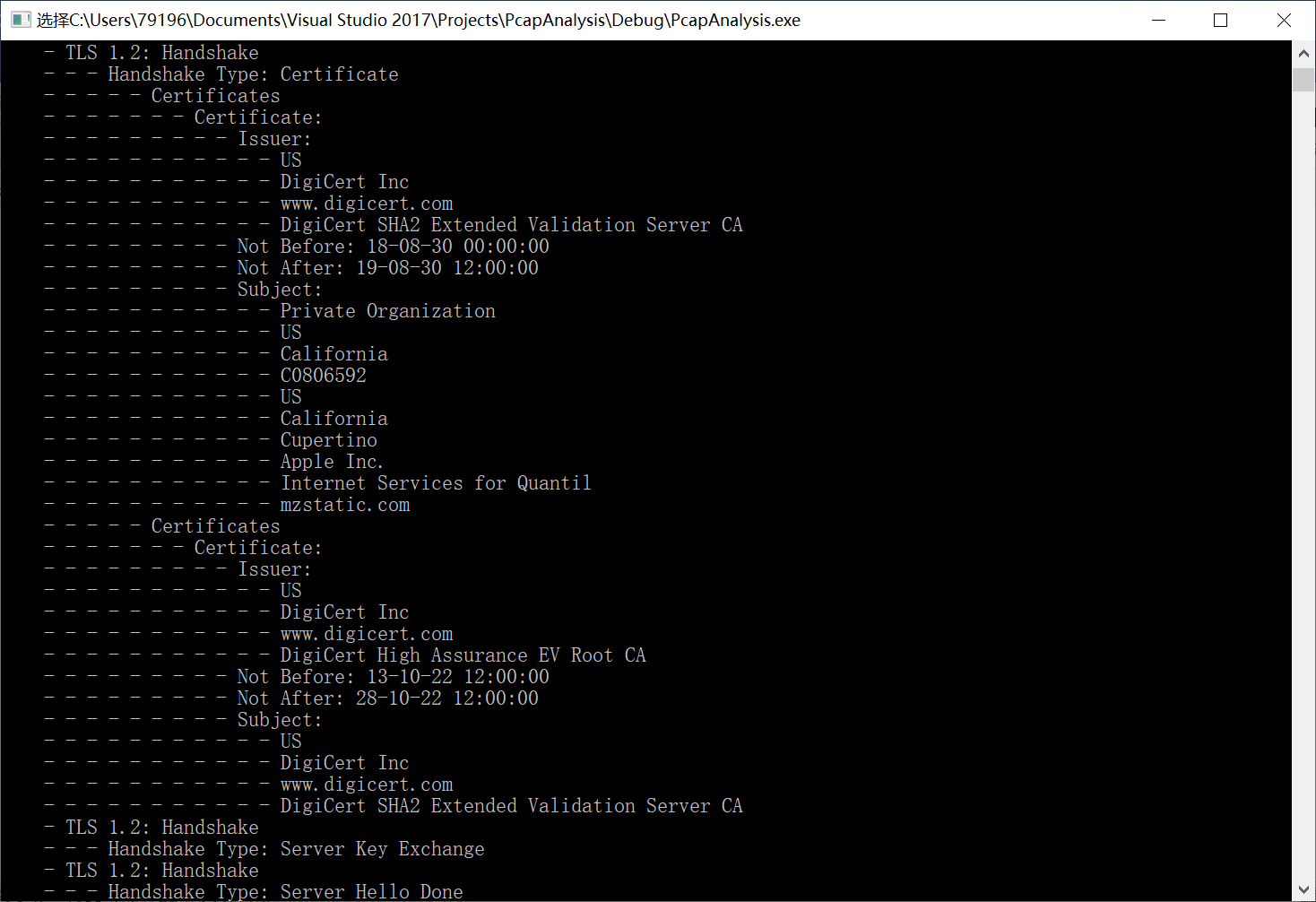
* 通过Winpcap Api，在pcap\_loop和packet\_handler实现对Pcap文件中每一个数据包的捕获。然后利用每一个数据中的数据逐Bit的对协议进行分析，从链接层的Loopback和Ethernet的区分到IP层协议的分析，到TCP层协议的分析，再到Socks、TLS1.2协议的分析。由于TCP层是不标志出应用层的具体协议，因此通过TCP载荷的第一个字节来判断，0x05对应Socks Version5，0x14-0x17对应不同类型的TLS1.2的Record包。
* Socks中关键是对Socks状态的分析，并从中可以提取如请求的域名端口、回复的地址端口。
* 最为困难的还是TLS1.2的分析，因为其过于繁复，需要耐着心一步一步分析。首先可以通过标志0x14-0x17确认TLS包是Change Cipher Spec、Alter、Handshake、Application中的一种。
* 其中Handshake是本次编程中处理细节最多的一个。同样通过标志区分具体的类型0x01对应Client Hello，0x02对应Server Hello等等。接下来依然是对不同的包进行进一层的分析。
* 值得注意的是，在分析Certificate这个Handshake类型的时候，我发现它的证书的数据流是分段的，往往一部分在上一个包Server Hello之后，第二部分在新的一个TLS包中。因此需要设立一个缓冲区将两个段合在一个进行分析。深层的原因应该是：TCP其实并不考虑具体的应用层协议，因此，一个很长的TLS证书，一个TCP包无法装载的下，因此会通过连续若干个TCP包传输。
* 在具体编程过程中，由于Byte众多，一开始经常看错位，因此后来使用Offset来保存并指明当前分析到哪一个字节。这也可以算一个小技巧。
* 另一个值得注意的是，协议类型中的抓包工具显示的很多可见都是从一个字节去对应具体的值（如0x01对应Client Hello），然后显示出来，往往只有域名才在协议中用字符串的ASCII进行传输。

# 编程分析结果的验证

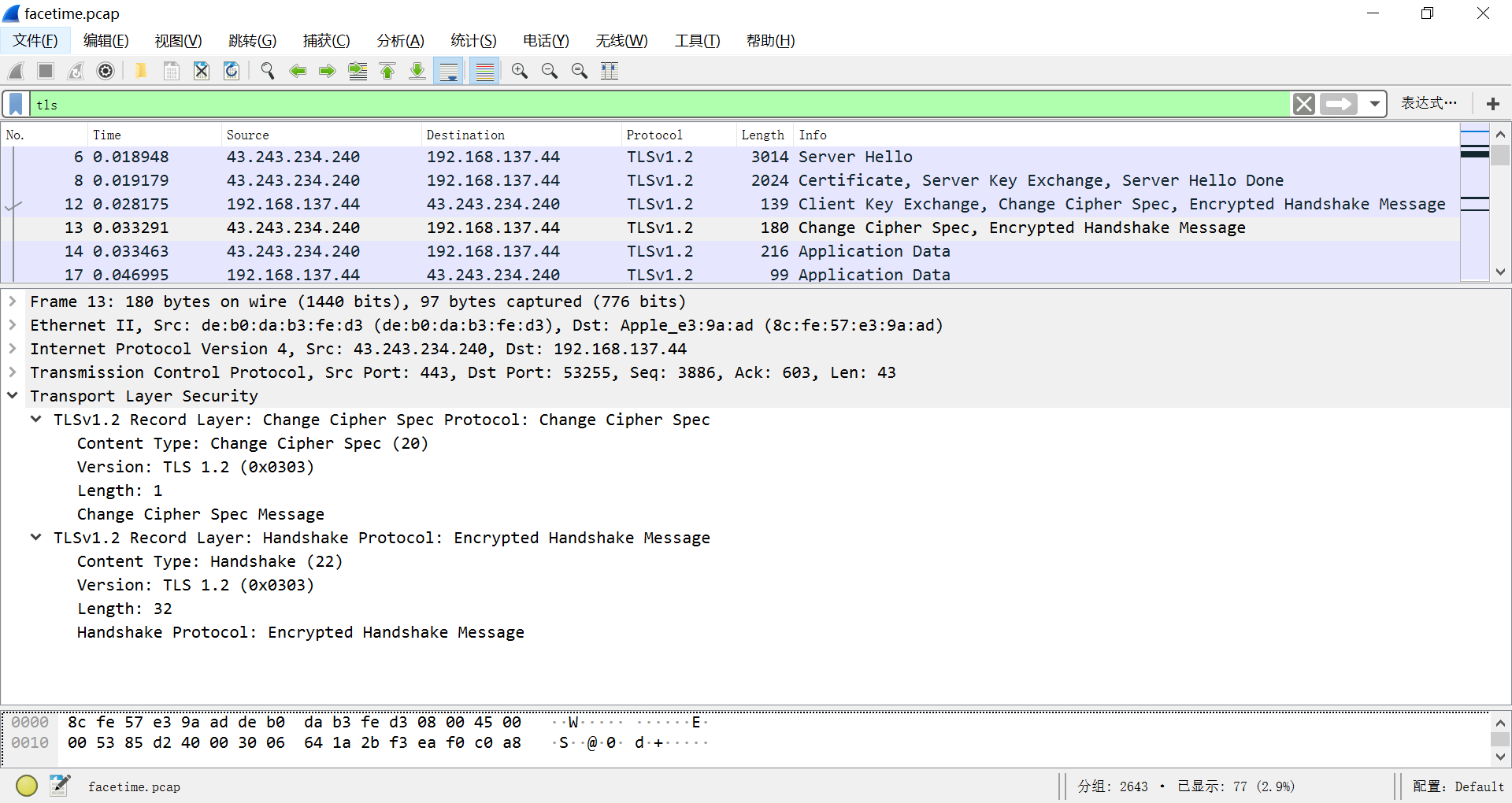
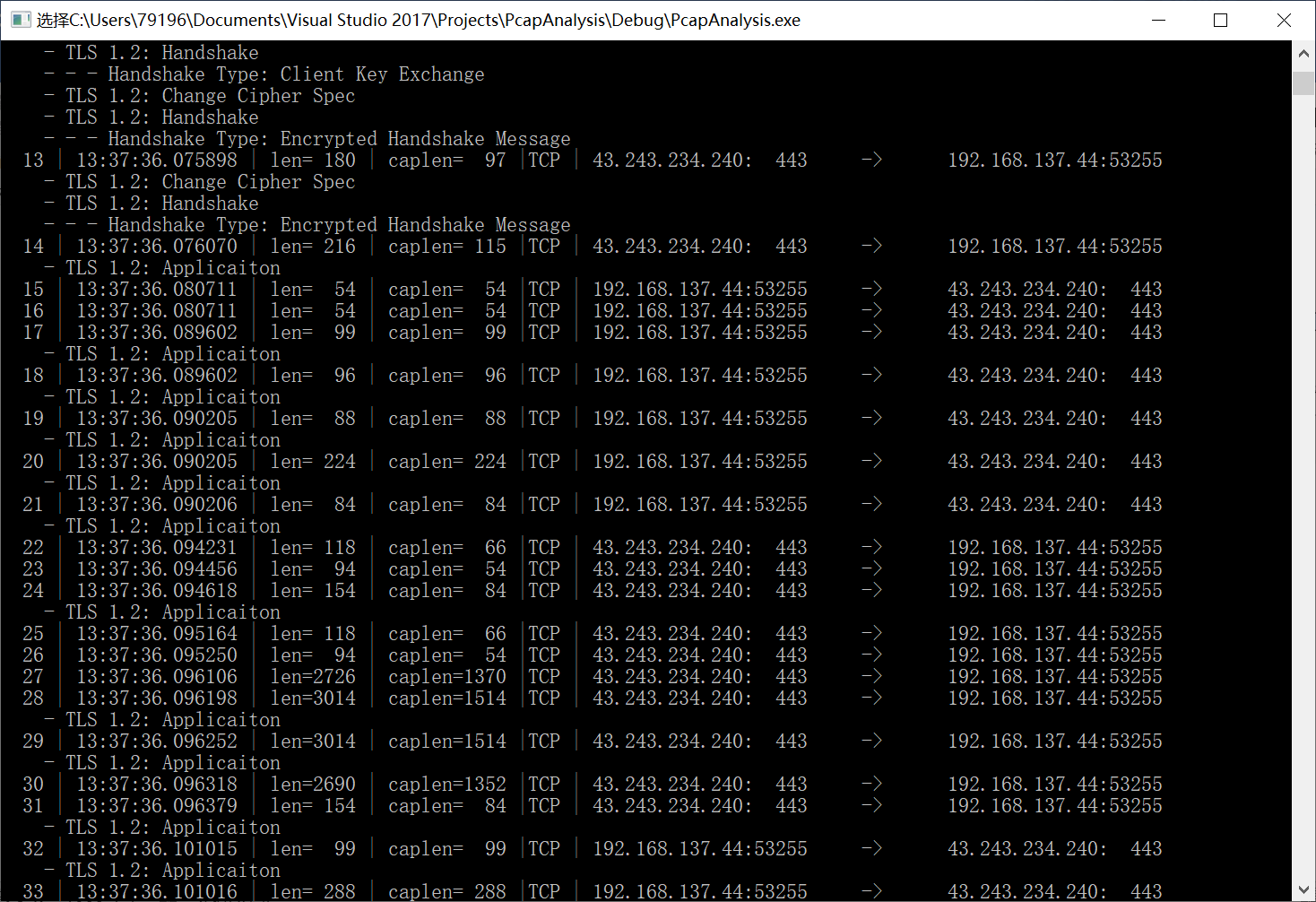
* Client Hello、Server Hello一致。



* 证书信息一致。Certificates、Server Exchange、Server Hello Done一致。



* Change Cipher Spec、Encrypted Handshake Message、Application一致。



* TLS握手和传输一致。验证通过。

# 密文解析

利用Fiddler对各个连接（configuration.apple.com、cma.itunes.apple.com、ftreporter.push.apple.com）中的密文进行解析。

## configuration.apple.com

"CONNECT 43.243.234.240:443 HTTP/1.1

Host: 43.243.234.240:443

Fiddler-Import: Packet capture contained HTTPS traffic. Parsing HTTPS Handshake to show this mock Session.

A SSLv3-compatible ClientHello handshake was found. Fiddler extracted the parameters below.

Version: 3.3 (TLS/1.2)

Random: 87 F0 D0 97 1E EC 96 20 FD E6 74 AC 2D 0B 7A 2D C2 AC ED AA 7C CB 5F 7D 90 B4 37 21 0D F0 78 88

""Time"": 2050/9/18 2:37:59

SessionID: F7 FE AF 67 8E 2D 68 16 AC 02 A9 18 24 24 74 81 25 4F 2F 90 05 0C 1B 51 BD A0 0C 4E 9D ED CF 83

Extensions:

renegotiation\_info 00

server\_name configuration.apple.com

extended\_master\_secret empty

signature\_algs sha256\_ecdsa, Unknown[0x8]\_Unknown[0x4], sha256\_rsa, sha384\_ecdsa, sha1\_ecdsa, Unknown[0x8]\_Unknown[0x5], Unknown[0x8]\_Unknown[0x5], sha384\_rsa, Unknown[0x8]\_Unknown[0x6], sha512\_rsa, sha1\_rsa

status\_request OCSP - Implicit Responder

NextProtocolNego empty

SignedCertTimestamp (RFC6962) empty

ALPN h2, h2-16, h2-15, h2-14, spdy/3.1, spdy/3, http/1.1

ec\_point\_formats uncompressed [0x0]

0x0033 00 24 00 1D 00 20 ED 3D 25 32 C9 EA 43 D5 50 DA FE 30 E7 51 11 4E 50 11 C5 AB 00 0C 8B 8F 78 42 3C 72 7C 13 D3 49

0x002d 01 01

0x002b 08 03 04 03 03 03 02 03 01

elliptic\_curves unknown [0x1D), secp256r1 [0x17], secp384r1 [0x18], secp521r1 [0x19]

padding 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Ciphers:

[1303] Unrecognized cipher - See http://www.iana.org/assignments/tls-parameters/

[1301] Unrecognized cipher - See http://www.iana.org/assignments/tls-parameters/

[1302] Unrecognized cipher - See http://www.iana.org/assignments/tls-parameters/

[C02C] TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

[C02B] TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

[C024] TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384

[C023] TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256

[C00A] TLS1\_CK\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA

[C009] TLS1\_CK\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA

[CCA9] TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256

[C030] TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

[C02F] TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

[C028] TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384

[C027] TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

[C014] TLS1\_CK\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

[C013] TLS1\_CK\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

[CCA8] TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256

[009D] TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

[009C] TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

[003D] TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256

[003C] TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

[0035] TLS\_RSA\_AES\_256\_SHA

[002F] TLS\_RSA\_AES\_128\_SHA

[C008] TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA

[C012] TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

[000A] SSL\_RSA\_WITH\_3DES\_EDE\_SHA

Compression:

[00] NO\_COMPRESSION

HTTP/1.1 200 Emulated CONNECT Tunnel

A SSLv3-compatible ServerHello handshake was found. Fiddler extracted the parameters below.

Version: 3.3 (TLS/1.2)

SessionID: DF F2 EB 31 AD 72 B4 23 A5 26 EF 81 B8 81 09 2E 6B 5A F1 6B 1D EB A9 81 3C 0A 83 A5 2C 7C FA 9F

Random: 27 8A CA FF AE BB 28 1C 62 FA 28 45 E8 08 49 A1 54 7A 5C 92 87 69 EC 1E 86 58 68 23 0E A2 6E 64

Cipher: TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 [0xCCA8]

CompressionSuite: NO\_COMPRESSION [0x00]

Extensions:

renegotiation\_info 00

ec\_point\_formats uncompressed [0x0], ansiX962\_compressed\_prime [0x1], ansiX962\_compressed\_char2 [0x2]

ALPN h2

extended\_master\_secret empty

"

## cma.itunes.apple.com

"CONNECT 42.101.76.4:443 HTTP/1.1

Host: 42.101.76.4:443

Fiddler-Import: Packet capture contained HTTPS traffic. Parsing HTTPS Handshake to show this mock Session.

A SSLv3-compatible ClientHello handshake was found. Fiddler extracted the parameters below.

Version: 3.3 (TLS/1.2)

Random: 33 F1 14 DF DA 28 D4 45 B0 C8 E2 00 71 CB A0 CB 2D 2E A6 E9 22 3D F1 2D 86 4C E4 8E 70 D9 8E ED

""Time"": 2088/8/7 12:33:55

SessionID: F9 00 C8 39 C3 48 39 2C 9A C2 C3 E2 82 C3 44 13 36 A3 CA 4F 8E BF BA 90 76 0C 6E C6 E5 76 EE FC

Extensions:

renegotiation\_info 00

server\_name cma.itunes.apple.com

extended\_master\_secret empty

signature\_algs sha256\_ecdsa, Unknown[0x8]\_Unknown[0x4], sha256\_rsa, sha384\_ecdsa, sha1\_ecdsa, Unknown[0x8]\_Unknown[0x5], Unknown[0x8]\_Unknown[0x5], sha384\_rsa, Unknown[0x8]\_Unknown[0x6], sha512\_rsa, sha1\_rsa

status\_request OCSP - Implicit Responder

NextProtocolNego empty

SignedCertTimestamp (RFC6962) empty

ALPN h2, h2-16, h2-15, h2-14, spdy/3.1, spdy/3, http/1.1

ec\_point\_formats uncompressed [0x0]

0x0033 00 24 00 1D 00 20 E1 00 BA 63 CA 97 76 8F B5 53 2C 5F 17 20 4C 38 58 2A 67 96 E9 97 21 91 DF 57 22 13 17 DC 57 3B

0x002d 01 01

0x002b 08 03 04 03 03 03 02 03 01

elliptic\_curves unknown [0x1D), secp256r1 [0x17], secp384r1 [0x18], secp521r1 [0x19]

padding 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Ciphers:

[1303] Unrecognized cipher - See http://www.iana.org/assignments/tls-parameters/

[1301] Unrecognized cipher - See http://www.iana.org/assignments/tls-parameters/

[1302] Unrecognized cipher - See http://www.iana.org/assignments/tls-parameters/

[C02C] TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

[C02B] TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

[C024] TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384

[C023] TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256

[C00A] TLS1\_CK\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA

[C009] TLS1\_CK\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA

[CCA9] TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256

[C030] TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

[C02F] TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

[C028] TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384

[C027] TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

[C014] TLS1\_CK\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

[C013] TLS1\_CK\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

[CCA8] TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256

[009D] TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

[009C] TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

[003D] TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256

[003C] TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

[0035] TLS\_RSA\_AES\_256\_SHA

[002F] TLS\_RSA\_AES\_128\_SHA

[C008] TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA

[C012] TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

[000A] SSL\_RSA\_WITH\_3DES\_EDE\_SHA

Compression:

[00] NO\_COMPRESSION

HTTP/1.1 200 Emulated CONNECT Tunnel

A SSLv3-compatible ServerHello handshake was found. Fiddler extracted the parameters below.

Version: 3.3 (TLS/1.2)

SessionID: 77 17 3F EE CC 7B 61 2A A6 20 DD BD 7C 4B F0 71 39 89 A0 C8 04 EE C2 56 BA 22 65 16 E2 B7 66 D4

Random: AF A5 58 A0 A1 F8 BF 34 92 19 56 D9 7C 56 A3 D6 EC 63 3A C1 EA 85 B7 37 30 4E CA 4B 2E D0 64 59

Cipher: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 [0xC030]

CompressionSuite: NO\_COMPRESSION [0x00]

Extensions:

renegotiation\_info 00

ec\_point\_formats uncompressed [0x0], ansiX962\_compressed\_prime [0x1], ansiX962\_compressed\_char2 [0x2]

ALPN http/1.1

extended\_master\_secret empty

"

## ftreporter.push.apple.com

"CONNECT 17.188.161.214:443 HTTP/1.1

Host: 17.188.161.214:443

Fiddler-Import: Packet capture contained HTTPS traffic. Parsing HTTPS Handshake to show this mock Session.

A SSLv3-compatible ClientHello handshake was found. Fiddler extracted the parameters below.

Version: 3.3 (TLS/1.2)

Random: 3E 03 69 6B 72 A7 BF 8D 03 E1 37 D3 D1 8C A5 5A 3C 09 52 FE 3F 0C AD 75 49 78 C6 05 F5 A5 92 B0

""Time"": 2027/2/8 7:50:22

SessionID: A1 73 1C 26 D9 7E 3A 7E 0C F2 03 67 D3 8A 27 CB 9E AA 1D 44 8D 12 F1 38 1F 5B 2E 3B 35 21 72 C7

Extensions:

renegotiation\_info 00

server\_name ftreporter.push.apple.com

extended\_master\_secret empty

signature\_algs sha256\_ecdsa, Unknown[0x8]\_Unknown[0x4], sha256\_rsa, sha384\_ecdsa, sha1\_ecdsa, Unknown[0x8]\_Unknown[0x5], Unknown[0x8]\_Unknown[0x5], sha384\_rsa, Unknown[0x8]\_Unknown[0x6], sha512\_rsa, sha1\_rsa

status\_request OCSP - Implicit Responder

NextProtocolNego empty

SignedCertTimestamp (RFC6962) empty

ALPN h2, h2-16, h2-15, h2-14, spdy/3.1, spdy/3, http/1.1

ec\_point\_formats uncompressed [0x0]

0x0033 00 24 00 1D 00 20 5F 17 CD E0 74 0B 93 A5 3C AD 43 C7 0F 63 1A 9B E1 2B 96 EC 85 9E E8 1D EC BA AE 5C AA E5 87 72

0x002d 01 01

0x002b 08 03 04 03 03 03 02 03 01

elliptic\_curves unknown [0x1D), secp256r1 [0x17], secp384r1 [0x18], secp521r1 [0x19]

padding 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Ciphers:

[1303] Unrecognized cipher - See http://www.iana.org/assignments/tls-parameters/

[1301] Unrecognized cipher - See http://www.iana.org/assignments/tls-parameters/

[1302] Unrecognized cipher - See http://www.iana.org/assignments/tls-parameters/

[C02C] TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

[C02B] TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

[C024] TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384

[C023] TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256

[C00A] TLS1\_CK\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA

[C009] TLS1\_CK\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA

[CCA9] TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256

[C030] TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

[C02F] TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

[C028] TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384

[C027] TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

[C014] TLS1\_CK\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

[C013] TLS1\_CK\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

[CCA8] TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256

[009D] TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

[009C] TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

[003D] TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256

[003C] TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

[0035] TLS\_RSA\_AES\_256\_SHA

[002F] TLS\_RSA\_AES\_128\_SHA

[C008] TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA

[C012] TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

[000A] SSL\_RSA\_WITH\_3DES\_EDE\_SHA

Compression:

[00] NO\_COMPRESSION

HTTP/1.1 200 Emulated CONNECT Tunnel

A SSLv3-compatible ServerHello handshake was found. Fiddler extracted the parameters below.

Version: 3.3 (TLS/1.2)

SessionID: 6F 05 42 E8 6E D4 74 A2 32 C6 72 76 14 05 61 A4 7F 21 7E 9A BB DD DF 86 1F 59 25 AF F5 E5 86 E3

Random: 5C 9C 5D CB 9D D3 99 3C DC 9B AB 25 1C D6 08 98 FF 7E 80 B9 B1 2D F2 00 D6 39 EE 02 66 E1 5F B2

Cipher: TLS\_RSA\_AES\_256\_SHA [0x0035]

CompressionSuite: NO\_COMPRESSION [0x00]

Extensions:

renegotiation\_info 00

server\_name empty

extended\_master\_secret empty

"

# 总结

* IPad软件抓包需要通过连接PC端热点来进行流量捕获
* 由于传输采用TLS协议，本实验旨在对TLS协议如握手、证书等可提取的信息进行分析并编程显示。此外，也对Socks协议进行了提取、分析和显示。
* 本文对编程细节进行了一定阐述。
* 对于具体的密文载荷，通过Fiddler进行分析便可识别。
* 展示了所开发的软件的显示结果。