

Terminal Shell Edit View Window Help Amreenie — bash — 200x54

```
Last login: Thu Apr 11 09:23:06 on ttys000
Amreens-MBP:~ Amreenie$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xffffffff
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
            nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 0
XHC0: flags=0<> mtu 0
XHC20: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 8c:85:90:8f:a7:36
        inet6 fe80::1086:4e3a:ce71:de02%en0 prefixlen 64 secured scopeid 0x6
            inet 192.168.1.167 netmask 0xffffffff broadcast 192.168.1.255
                nd6 options=201<PERFORMNUD,DAD>
                    media: autoselect
                    status: active
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=60<TS04,TS06>
    ether aa:00:75:09:48:01
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8863<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=60<TS04,TS06>
    ether aa:00:75:09:48:00
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=63<RXCSUM,TXCSUM,TS04,TS06>
    ether aa:00:75:09:48:01
    Configuration:
        id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
        maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
        root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
        ipfilter disabled flags 0x2
    member: en1 flags=3<LEARNING,DISCOVER>
        ifmaxaddr 0 port 7 priority 0 path cost 0
    member: en2 flags=3<LEARNING,DISCOVER>
        ifmaxaddr 0 port 8 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    ether 0e:85:90:8f:a7:36
        media: autoselect
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
    ether 9e:ed:0b:85:aa:1b
    inet6 fe80::9ced:bfef:fe85:aab%awdl0 prefixlen 64 scopeid 0xb
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

The dock features a variety of application icons, including Finder, Mail, Safari, iBooks, iTunes, iPhoto, iCal, Address Book, iMovie, iDVD, iWork (Pages, Numbers, Keynote), iLife (iPhoto, iMovie, iDVD), and a trash can icon.

1. What is the SSL/TLS version of the Client Hello frame?

The version of SSL/TLS is 1.2.

The screenshot shows a Wireshark capture of a TLS 1.2 Client Hello handshake. The timeline pane shows several frames, with frame 91 highlighted. The details pane shows the TLS 1.2 Record Layer: Handshake Protocol: Client Hello structure, specifically the Version field which is set to TLS 1.2 (0x0303). The bytes pane shows the raw hex and ASCII data for the Client Hello message, starting with FF FF 16 38 00 00 16 03 01 02 03 01 00 01 ff 03. The packet list pane shows the following sequence of frames:

No.	Time	Source	Destination	Protocol	Length	Info
17	1.943987	74.119.119.131	192.168.1.167	TLSv1.2	90	Application Data
24	2.803415	35.190.130.252	192.168.1.167	TLSv1.2	97	Encrypted Alert
28	2.804025	68.67.178.243	192.168.1.167	TLSv1.2	97	Encrypted Alert
42	3.651932	192.168.1.167	138.91.80.138	TLSv1.2	151	[TCP Previous segment not captured] , Application Data
43	3.653520	192.168.1.167	138.91.80.138	TLSv1.2	112	Application Data
45	3.719887	138.91.80.138	192.168.1.167	TLSv1.2	112	Application Data
47	3.733923	138.91.80.138	192.168.1.167	TLSv1.2	441	Application Data
49	3.734067	138.91.80.138	192.168.1.167	TLSv1.2	114	Application Data
91	4.170846	192.168.1.167	192.161.175.22	TLSv1.2	574	Client Hello
95	4.178611	192.168.1.167	192.161.175.22	TLSv1.2	574	Client Hello
105	4.238879	192.161.175.22	192.168.1.167	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
108	4.245054	192.161.175.22	192.168.1.167	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
110	4.245264	192.168.1.167	192.161.175.22	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
111	4.246146	192.168.1.167	192.161.175.22	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
113	4.246276	192.168.1.167	192.161.175.22	TLSv1.2	1412	Application Data

Frame 91: 574 bytes on wire (4592 bits), 574 bytes captured (4592 bits) on interface 0
Ethernet II, Src: Apple_8f:a7:36 (0c:85:90:8f:a7:36), Dst: Verizon_ea:f8:8e (48:5d:36:ea:f8:8e)
Internet Protocol Version 4, Src: 192.168.1.167, Dst: 192.161.175.22
Transmission Control Protocol, Src Port: 49876, Dst Port: 443, Seq: 1, Ack: 1, Len: 520
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 515
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 511
Version: TLS 1.2 (0x0303)
Random: 7f120e126773264ebd9c79ce73ae78860c9ad4c5a178056...
Session ID Length: 32
Session ID: 1798a085e66040f05d093281359656a6451758985416c806...
Cipher Suites Length: 34
Cipher Suites (17 suites)

Record layer version (ssl.record.version), 2 bytes

Packets: 4728 - Displayed: 1427 (30.2%) - Dropped: 0 (0.0%) Profile: Default

Mac OS X Dock icons include: Finder, App Store, iTunes, Mail, Safari, Google Chrome, iPhoto, Calendar, Mail, Word, PowerPoint, Numbers, iWork, Photos, News, Stocks, and iBooks.

2. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

The value of the content type is 22.

Wireshark Screenshot showing a network capture of an SSL/TLS handshake. The timeline shows several frames, with frame 91 highlighted as a Client Hello message. The details pane shows the structure of the TLSv1.2 record, specifically the Handshake Protocol: Client Hello section. The Content Type field is highlighted with a red box and labeled '(22)'. The value 22 corresponds to the 'Handshake' type. The bytes pane at the bottom shows the raw hex and ASCII representation of the Client Hello message.

Frame 91: 574 bytes on wire (4592 bits), 574 bytes captured (4592 bits) on interface 0

- ▶ Ethernet II, Src: Apple_8f:a7:36 (8c:85:90:8f:a7:36), Dst: Verizon_ea:f8:8e (48:5d:36:ea:f8:8e)
- ▶ Internet Protocol Version 4, Src: 192.168.1.167, Dst: 192.161.175.22
- ▶ Transmission Control Protocol, Src Port: 49876, Dst Port: 443, Seq: 1, Ack: 1, Len: 520
- Secure Sockets Layer
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - version: TLS 1.0 (0x0301)
 - Length: 515
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 511
 - Version: TLS 1.2 (0x0303)
 - Random: 7ff2d0e126f73284ebd9c79ce73ae78860c9ad4c5a178056...
 - Session ID Length: 32
 - Session ID: 1798a085e66040f05d093281359656a6451758985416c806...
 - Cipher Suites Length: 34
 - Cipher Suites (17 suites)

```

0030 ff ff 16 38 00 00 16 03 01 02 03 01 00 01 ff 03  ..8.... .....
0040 03 7f f2 d0 e1 26 f7 32 84 eb d9 c7 9c e7 3a e7  ....&2.....
0050 88 60 c9 ad 4c 5a 17 80 56 11 f0 cd 24 e0 10 f1  `..LZ.. V...$...
0060 d6 20 17 98 a0 85 e6 60 40 f0 5d 09 32 81 35 96  . ....` @]~2.5.
0070 56 a6 45 17 58 98 54 16 c8 06 51 b2 99 6f 41 a4  V.E-X-T. ..Q..oA.

```

Packets: 4728 - Displayed: 1427 (30.2%) - Dropped: 0 (0.0%) Profile: Default

3. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

There is no challenge.

Screenshot of Wireshark showing network traffic and a detailed analysis of a TLSv1.2 Client Hello message.

The packet list shows several frames, with frame 42 (Client Hello) highlighted in blue. The details pane shows the structure of the Client Hello message:

- Transmission Control Protocol:** Src Port: 49876, Dst Port: 443, Seq: 1, Ack: 1, Len: 520
- Secure Sockets Layer**
- TLSv1.2 Record Layer:** Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 515
- Handshake Protocol: Client Hello**
 - Handshake Type: Client Hello (1)
 - Length: 511
 - Version: TLS 1.2 (0x0303)
 - Random: 7ff2d0e126f73284ebd9c79ce73ae78860c9ad4c5a178056...
 - Session ID Length: 32
 - Session ID: 1798a085e66040f05d093281359656a6451758985416c806...
 - Cipher Suites Length: 34
 - Cipher Suites (17 suites)
 - Compression Methods Length: 1
 - Compression Methods (1 method)**
 - Extensions Length: 404
 - Extension: Reserved (GREASE) (len=0)
 - Extension: server_name (len=20)
 - Extension: extended_master_secret (len=0)
 - Extension: renegotiation_info (len=1)

The bytes pane shows the raw hex and ASCII data for the compression methods extension:

```

00a0  00 2f 00 35 00 00 01 00  01 94 6a 6a 00 00 00 00  ./-5.... jj....
00b0  00 14 00 12 00 00 0f 77  77 77 2e 72 65 76 6f 6c  .....w www.revol
00c0  76 65 2e 63 6f 6d 00 17  00 00 ff 01 00 01 00 00 ve.com. .....
00d0  0a 00 0a 00 08 4a 4a 00  1d 00 17 00 18 00 0b 00 .....JJ. .....
00e0  02 01 00 00 23 00 d0 87  62 a8 bc ca 33 c3 ce 18 .....#... b...3...

```

At the bottom, there is a toolbar with various application icons and a status bar indicating 4728 packets displayed, 1427 (30.2%) dropped, and 0 (0.0%) error.

4. Does the ClientHello record advertise the cipher suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

The ClientHello does record the cipher suites.

Public-key: RSA

Symmetric-Key: AES128 and AES 256

Hash: SHA

Wireshark Screenshot showing a TLS handshake:

- Session ID Length:** 32
- Session ID:** 1798a085e66040f05d093281359656a6451758985416c806...
- Cipher Suites Length:** 34
- Cipher Suites (17 suites):**
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca8)
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc02c)
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca9)
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca8)
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca9)
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca8)
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca9)
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca9)
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- Compression Methods Length:** 1

Packets: 4728 - Displayed: 1427 (30.2%) - Dropped: 0 (0.0%)

Profile: Default

1. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

Yes, it does. It uses RSA for public key, AES for symmetric key, and SHA for hash.

The screenshot shows a Wireshark capture of network traffic. The timeline pane at the top shows several application-layer packets (Protocol: TLSv1.2) exchanged between 192.168.1.167 and 192.168.1.167. The details pane displays the structure of a Server Hello message (packet 105). The 'Cipher Suite' field is highlighted with a red box and contains the value `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)`. The bytes pane at the bottom shows the raw hex and ASCII representation of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
45	3.719887	138.91.80.138	192.168.1.167	TLSv1.2	112	Application Data
47	3.733923	138.91.80.138	192.168.1.167	TLSv1.2	441	Application Data
49	3.734067	138.91.80.138	192.168.1.167	TLSv1.2	114	Application Data
91	4.170846	192.168.1.167	192.161.175.22	TLSv1.2	574	Client Hello
95	4.178611	192.168.1.167	192.161.175.22	TLSv1.2	574	Client Hello
105	4.238879	192.161.175.22	192.168.1.167	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
108	4.245054	192.161.175.22	192.168.1.167	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
110	4.245264	192.168.1.167	192.161.175.22	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
111	4.246146	192.168.1.167	192.161.175.22	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
113	4.246276	192.168.1.167	192.161.175.22	TLSv1.2	1412	Application Data
114	4.274163	199.187.193.130	192.168.1.167	TLSv1.2	97	Encrypted Alert

Selected packet details:

- Handshake Protocol: Server Hello
- Handshake Type: Server Hello (2)
- Length: 77
- Version: TLS 1.2 (0x0303)
- Random: 80ae980a3679b4f073c2b7e46f582982db631f0efc826dde...
- Session ID Length: 32
- Session ID: 1798a085e66040f05d093281359656a6451758985416c806...
- Cipher Suite: `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)`
- Compression Method: null (0)
- Extensions Length: 5
- Extension: renegotiation_info (len=1)

Selected packet bytes:

```

0070  56 a6 45 17 58 98 54 16 c8 06 51 b2 99 6f 41 a4 V·E·X·T· ··Q··o··
0080  f7 2c c0 30 00 05 ff 01 00 01 00 14 03 03 00 ..·0··· ···· ···· ····
0090  01 01 16 03 03 00 28 29 93 b8 59 3c 00 19 ad 56 ····() ···Y<···V
00a0  b3 11 31 2a f1 25 86 96 e2 f4 92 7e c1 95 8f f8 ···1*%·· ···· ····
00b0  76 bd 05 85 5b 96 89 86 17 d4 cd 3c 52 b8 3f v···[·· ···<R·?

```

Packets: 4728 · Displayed: 1427 (30.2%) · Dropped: 0 (0.0%) · Profile: Default

HTTP OK Message:

I didn't have a HTTP ok message, so I am including a screenshot of that.

The screenshot shows a Wireshark capture window titled "Wireshark Lab 8.pcapng". The "http" protocol column is selected. Two frames are visible:

- Frame 3519: An HTTP GET request from 192.168.1.167 to 72.21.91.29. The "Info" column shows the full URL: "/MFYwVKADAgEAME0wSzBJMAkGBSs0AwIaBQAEFEn0vYoYv3YGmMXe0C1o03Fq50aGBB0901Cl1qCt7vNKYAp...".
- Frame 3521: An OCSP response from 72.21.91.29 to 192.168.1.167. The "Info" column shows the response body.

The details pane displays the full request and response messages. The request includes headers such as Host, Accept, Accept-Language, Connection, Accept-Encoding, and User-Agent. The response is a standard OCSP response.

The bottom of the screenshot shows the Mac OS X Dock with various application icons.