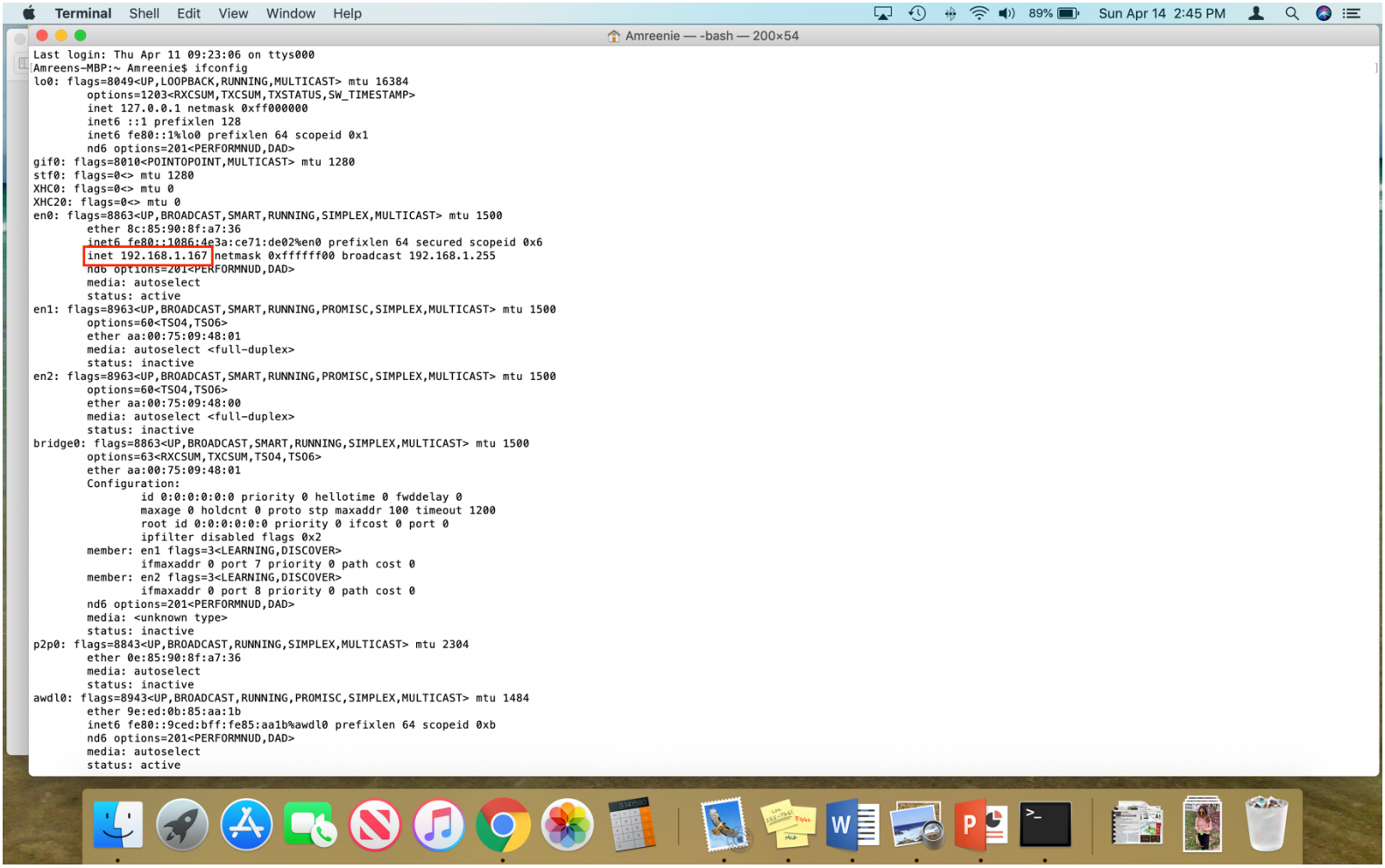
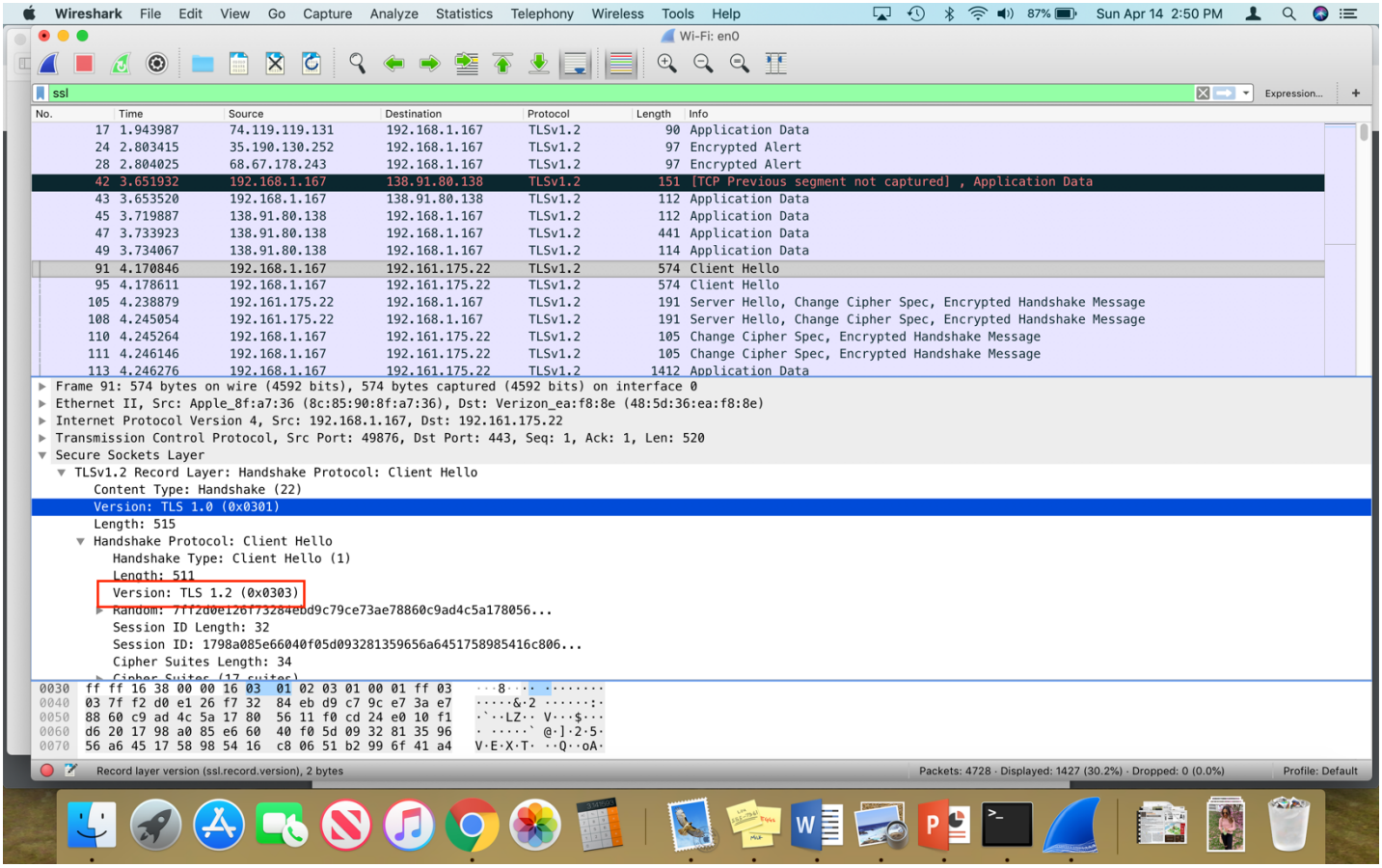

Terminal Shell Edit View Window Help
89% Sun Apr 14 2:45 PM
Amreenie — -bash — 200×54
Last login: Thu Apr 11 09:23:06 on ttys000
Amreens-MBP:~ Amreenie$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
inet 127.0.0.1 netmask 0xff000000
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
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 0xffffff00 broadcast 192.168.1.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
options=60<TSO4,TSO6>
ether aa:00:75:09:48:01
media: autoselect <full-duplex>
status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
options=60<TSO4,TSO6>
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,TSO4,TSO6>
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:bff:fe85:aa1b%awdl0 prefixlen 64 scopeid 0xb
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active

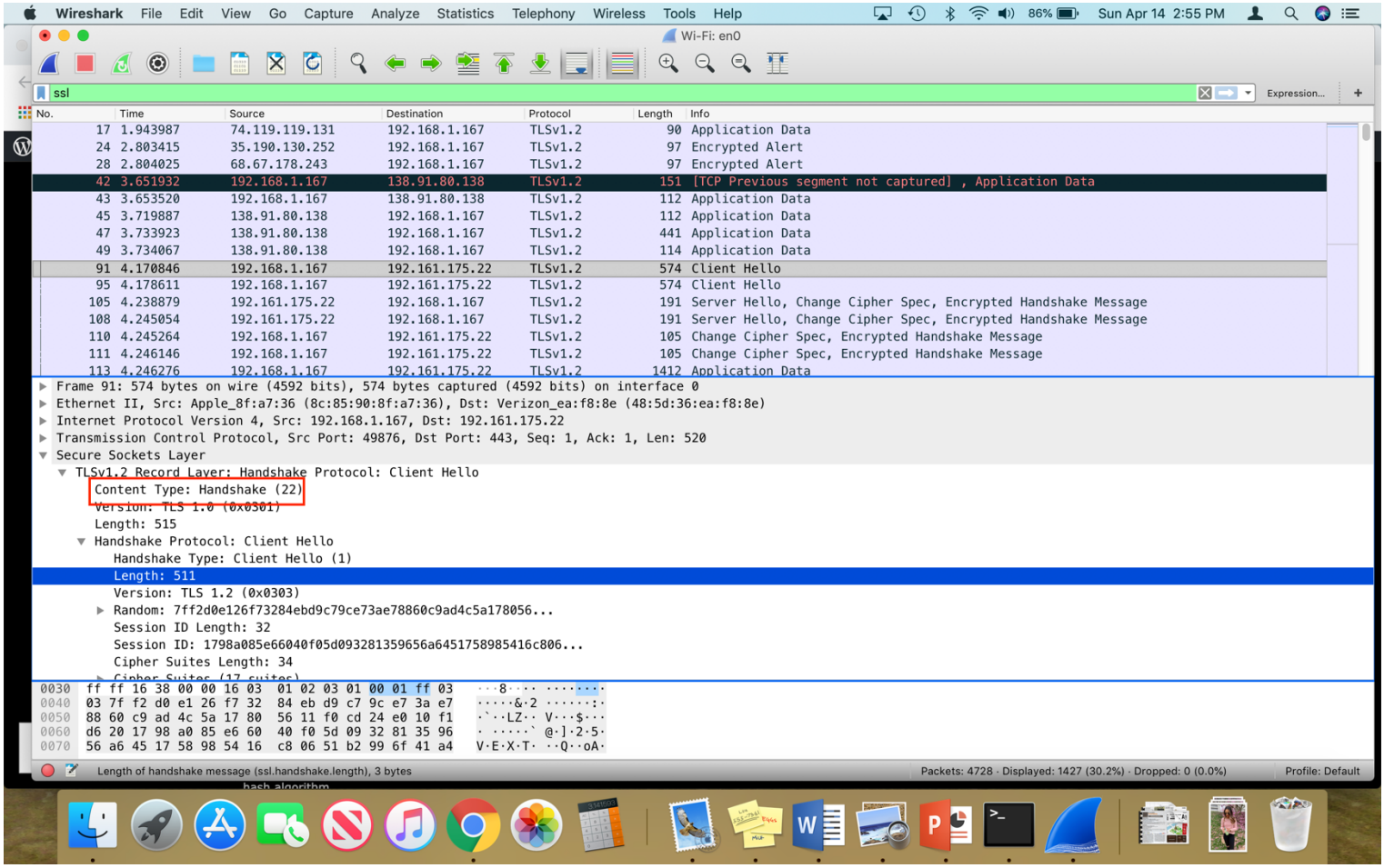
1. What is the SSL/TLS version of the of the Client Hello frame?

The version of SSL/TLS is 1.2.



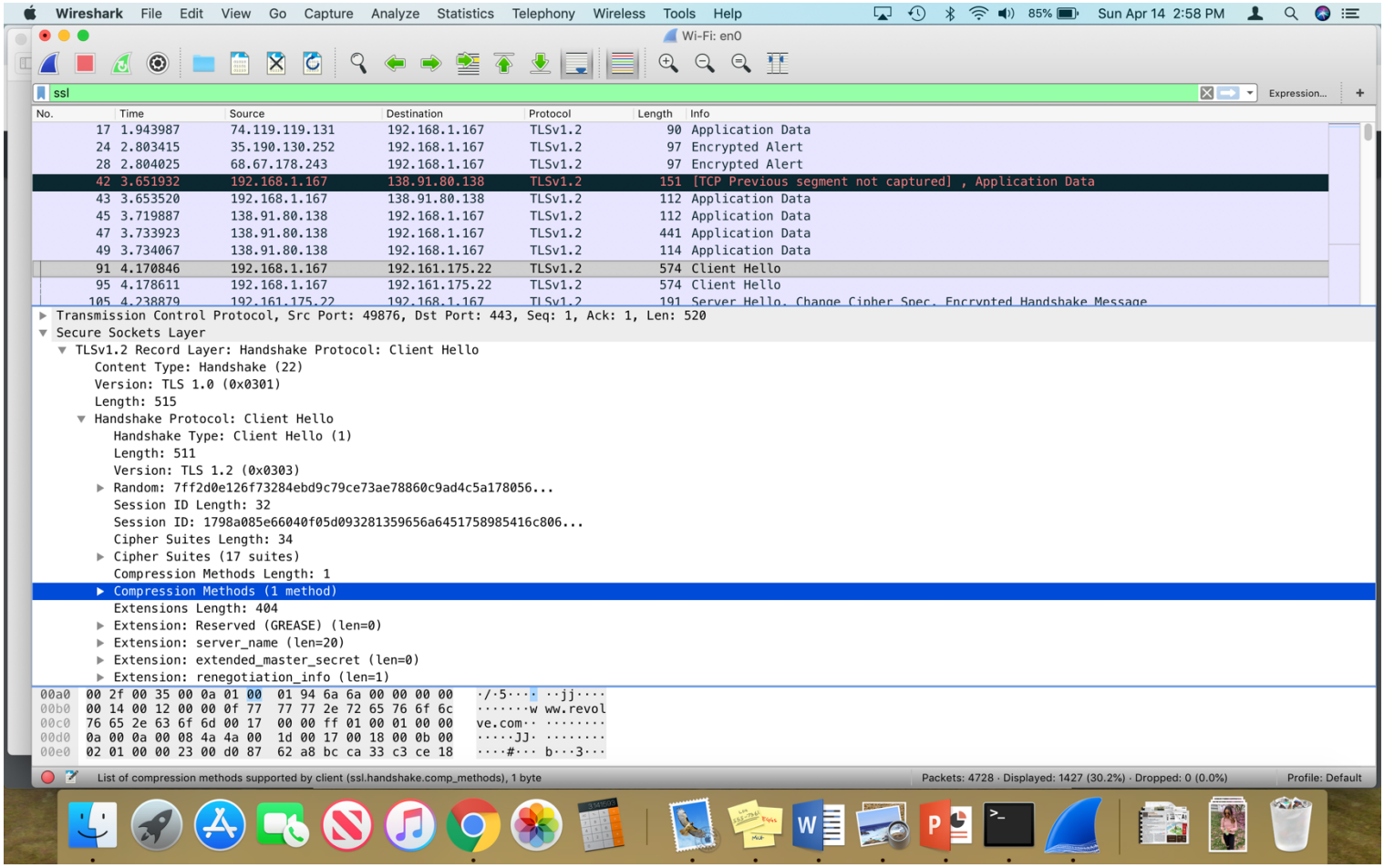
2. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

The value of the content type is 22.



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?

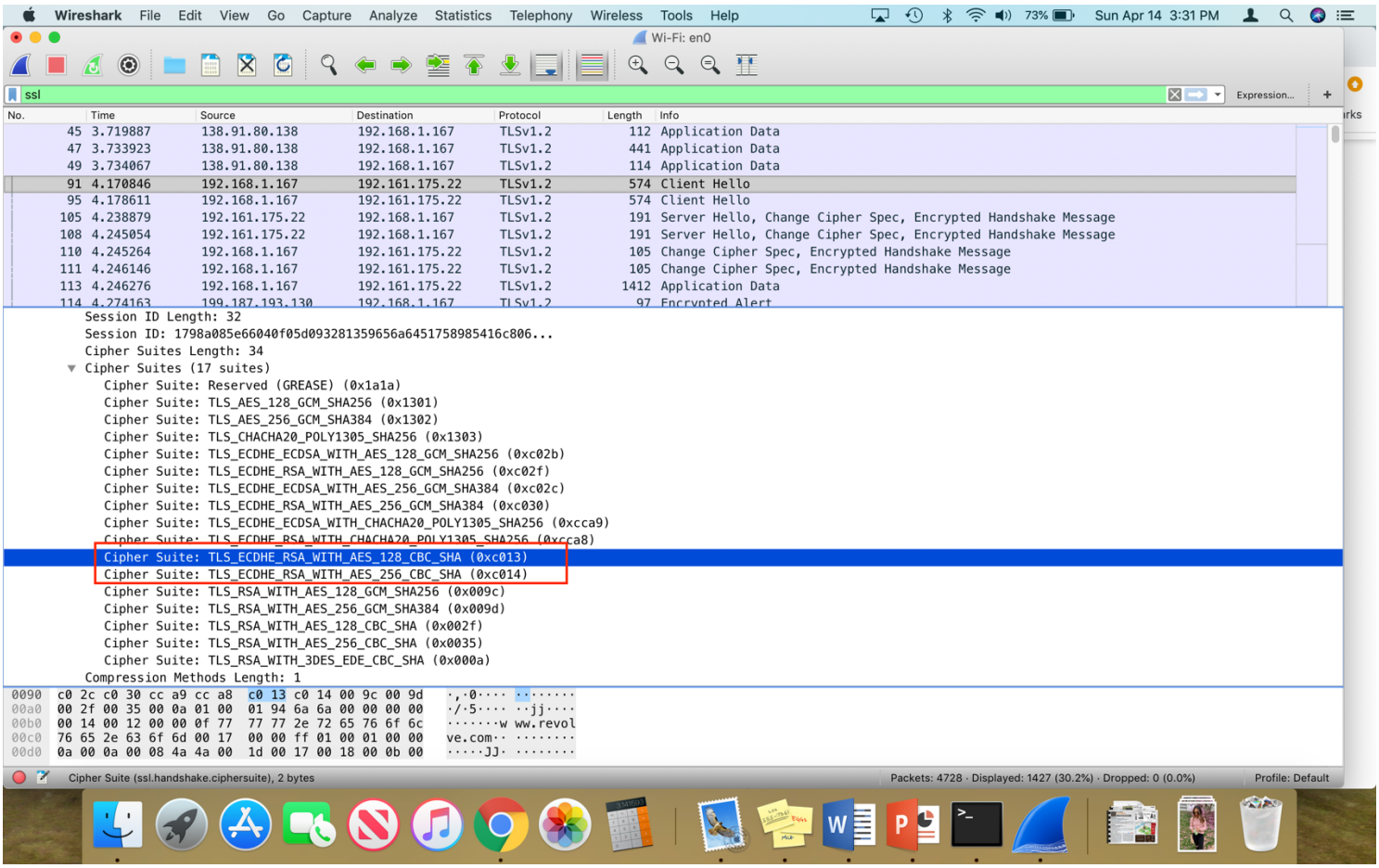
There is no challenge.



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

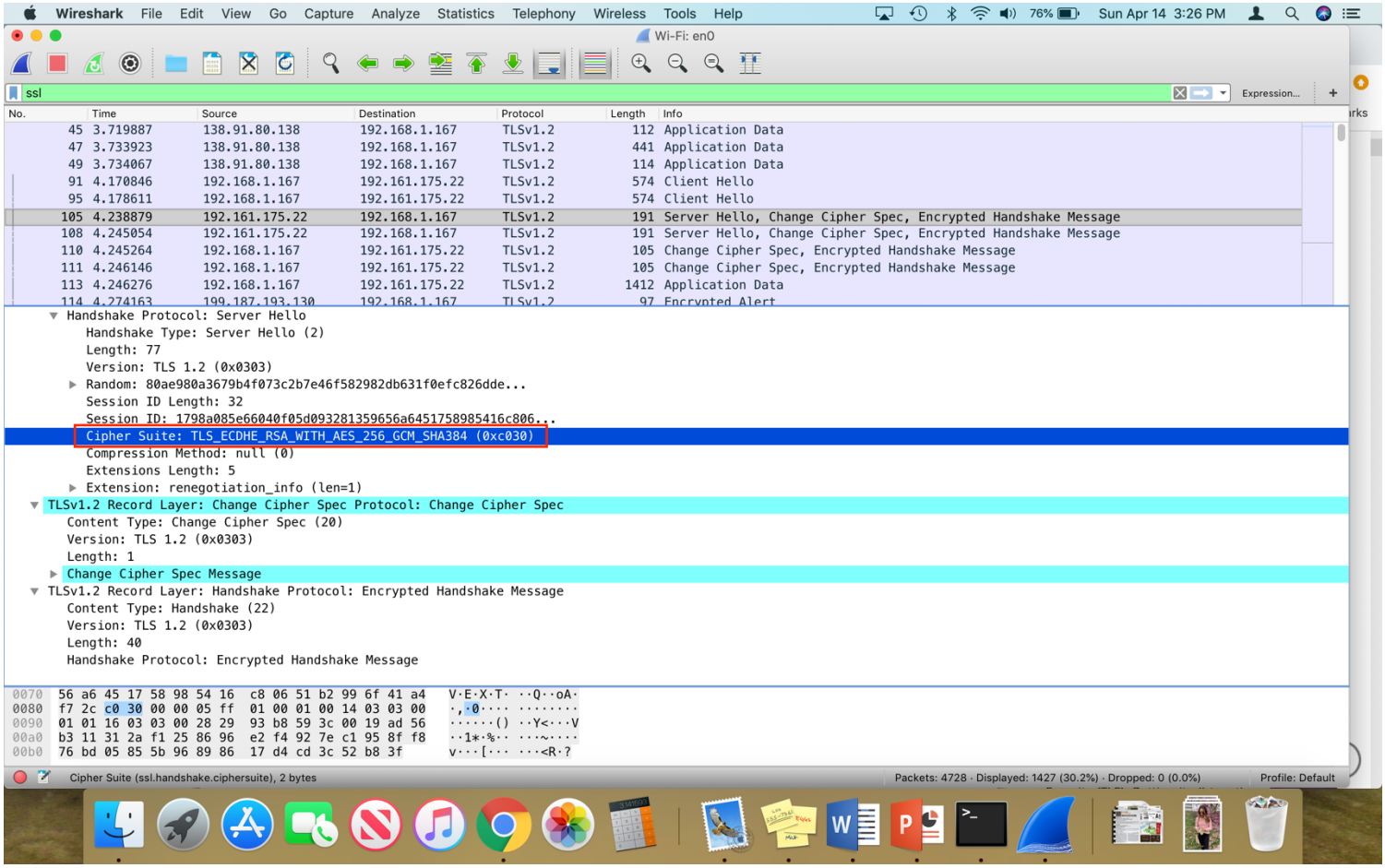
The ClientHello does record the cyber suites.

Public-key: RSA
Symmetric-Key: AES128 and AES 256
Hash: SHA



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.



HTTP OK Message:

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