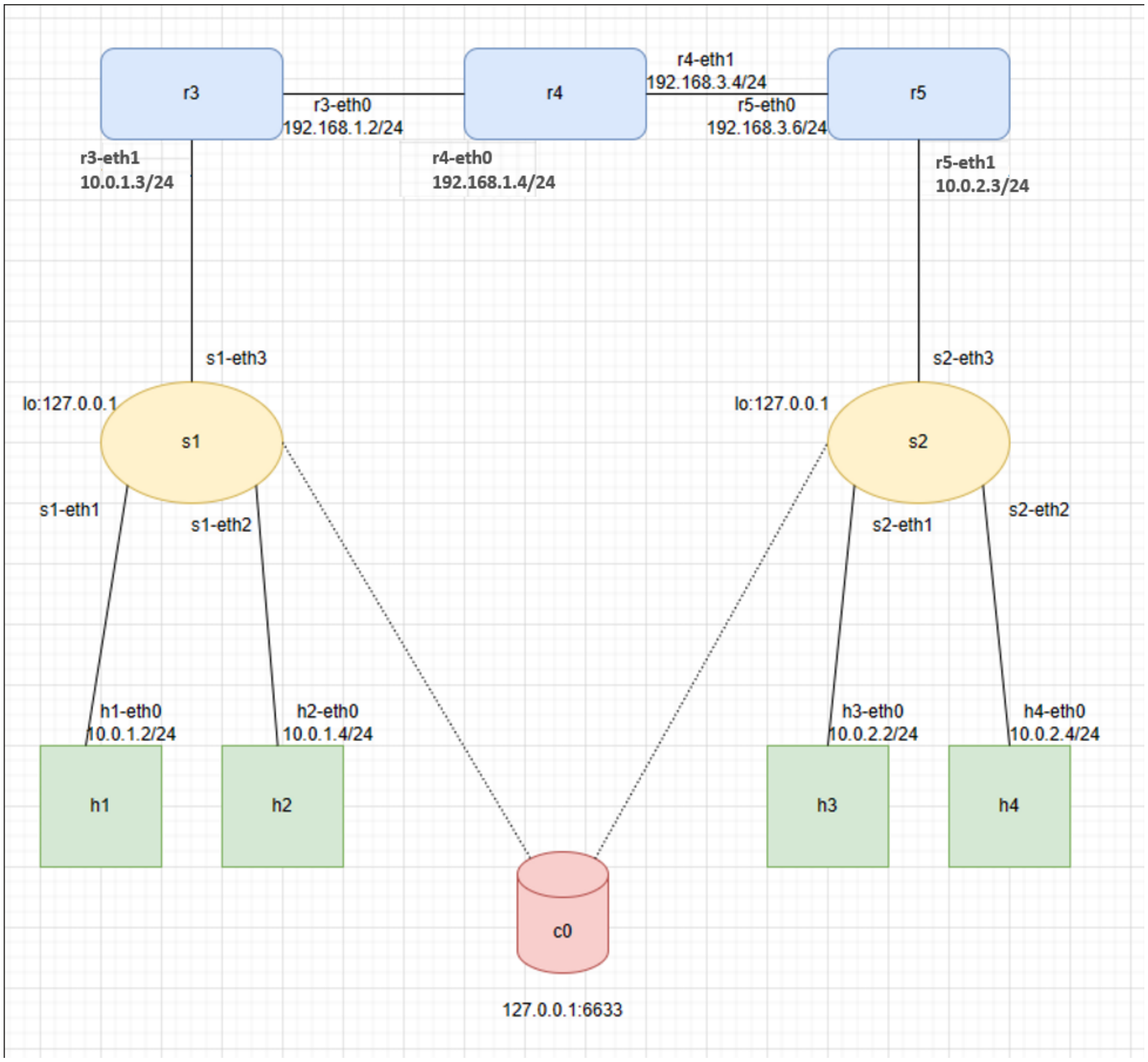
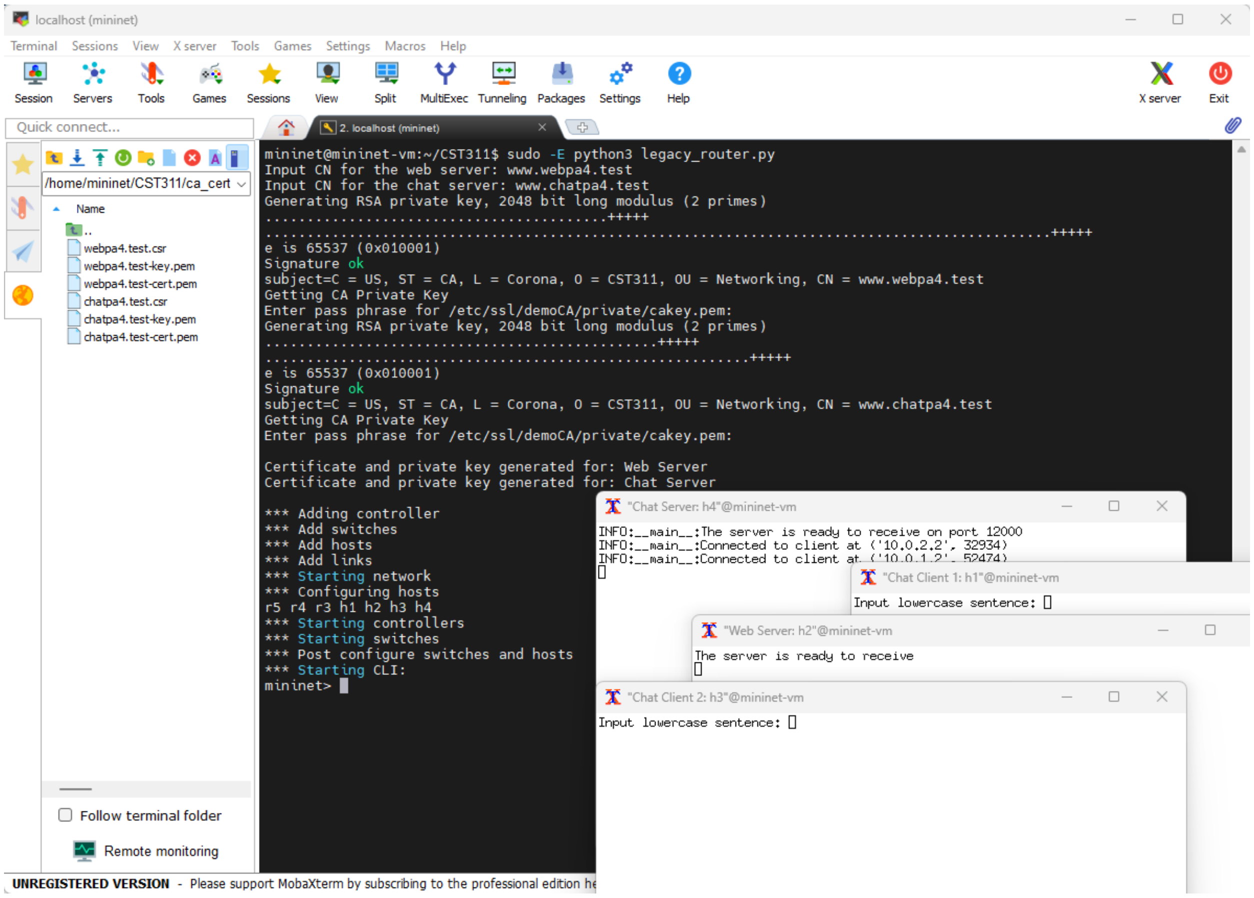
Diagram


r3
r4
r5
r3-eth0
192.168.1.2/24
r4-eth0
192.168.1.4/24
r4-eth1
192.168.3.4/24
r5-eth0
192.168.3.6/24
r3-eth1
10.0.1.3/24
r5-eth1
10.0.2.3/24
s1-eth3
s2-eth3
lo:127.0.0.1
s1
lo:127.0.0.1
s2
s1-eth1
s1-eth2
s2-eth1
s2-eth2
h1-eth0
10.0.1.2/24
h2-eth0
10.0.1.4/24
h3-eth0
10.0.2.2/24
h4-eth0
10.0.2.4/24
h1
h2
h3
h4
c0
127.0.0.1:6633

Screenshots

Screen capture of the program that runs with no Python errors:


localhost (mininet)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Quick connect...
2. localhost (mininet)
/home/mininet/CST311/ca_cert
Name
..
webpa4.test.csr
webpa4.test-key.pem
webpa4.test-cert.pem
chatpa4.test.csr
chatpa4.test-key.pem
chatpa4.test-cert.pem
Follow terminal folder
Remote monitoring
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition he

```
mininet@mininet-vm:~/CST311$ sudo -E python3 legacy_router.py
Input CN for the web server: www.webpa4.test
Input CN for the chat server: www.chatpa4.test
Generating RSA private key, 2048 bit long modulus (2 primes)
.........................................+++++
.............................................................................................+++++
e is 65537 (0x010001)
Signature ok
subject=C = US, ST = CA, L = Corona, O = CST311, OU = Networking, CN = www.webpa4.test
Getting CA Private Key
Enter pass phrase for /etc/ssl/demoCA/private/cakey.pem:
Generating RSA private key, 2048 bit long modulus (2 primes)
..............................................+++++
.........................................................+++++
e is 65537 (0x010001)
Signature ok
subject=C = US, ST = CA, L = Corona, O = CST311, OU = Networking, CN = www.chatpa4.test
Getting CA Private Key
Enter pass phrase for /etc/ssl/demoCA/private/cakey.pem:

Certificate and private key generated for: Web Server
Certificate and private key generated for: Chat Server

*** Adding controller
*** Add switches
*** Add hosts
*** Add links
*** Starting network
*** Configuring hosts
r5 r4 r3 h1 h2 h3 h4
*** Starting controllers
*** Starting switches
*** Post configure switches and hosts
*** Starting CLI:
mininet>
```

"Chat Server: h4"@mininet-vm

```
INFO:__main__:The server is ready to receive on port 12000
INFO:__main__:Connected to client at ('10.0.2.2', 32934)
INFO:__main__:Connected to client at ('10.0.1.2', 52474)
```

"Chat Client 1: h1"@mininet-vm

```
Input lowercase sentence:
```

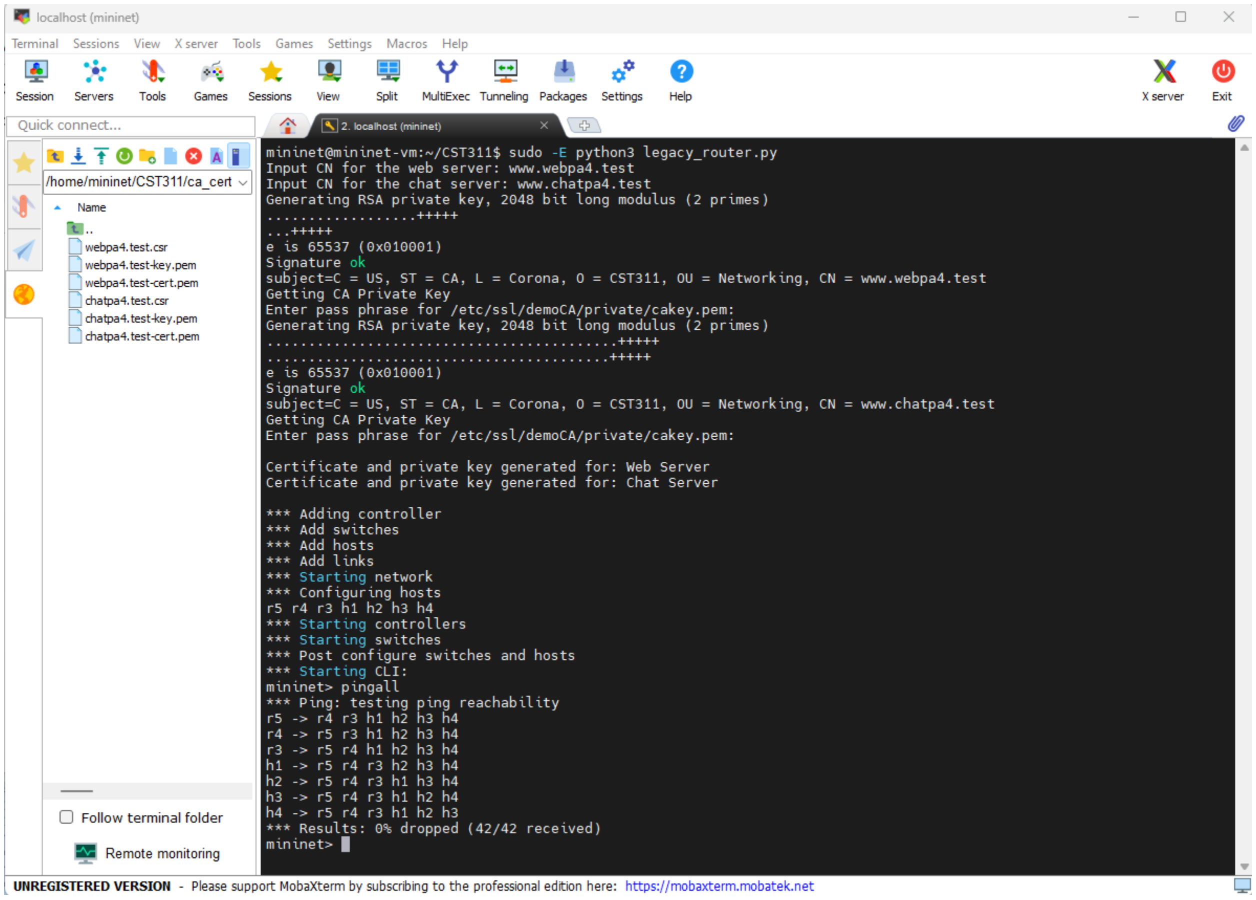
"Web Server: h2"@mininet-vm

```
The server is ready to receive
```

"Chat Client 2: h3"@mininet-vm

```
Input lowercase sentence:
```

Screen capture of successful pingall at the mininet> prompt:



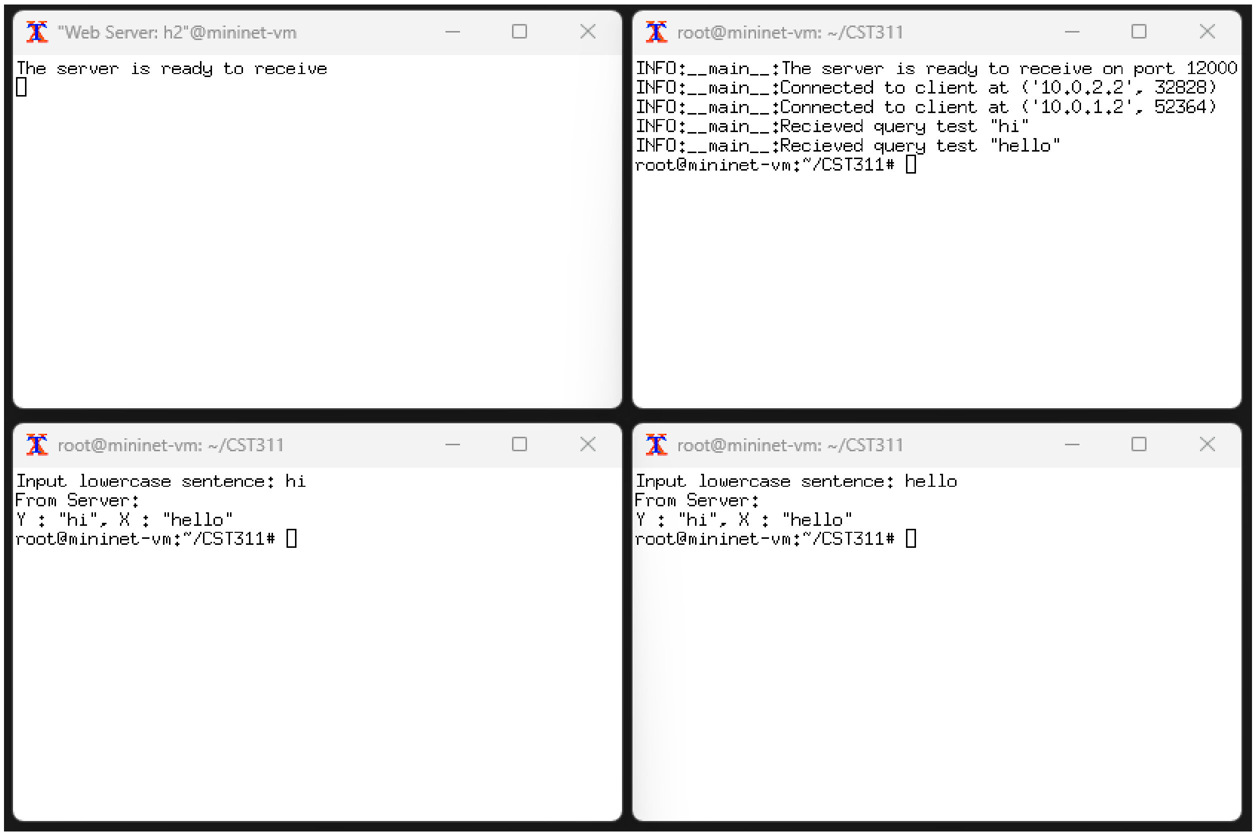
```
mininet@mininet-vm:~/CST311$ sudo -E python3 legacy_router.py
Input CN for the web server: www.webpa4.test
Input CN for the chat server: www.chatpa4.test
Generating RSA private key, 2048 bit long modulus (2 primes)
.................+++++
...+++++
e is 65537 (0x010001)
Signature ok
subject=C = US, ST = CA, L = Corona, O = CST311, OU = Networking, CN = www.webpa4.test
Getting CA Private Key
Enter pass phrase for /etc/ssl/demoCA/private/cakey.pem:
Generating RSA private key, 2048 bit long modulus (2 primes)
.........................................+++++
........................................+++++
e is 65537 (0x010001)
Signature ok
subject=C = US, ST = CA, L = Corona, O = CST311, OU = Networking, CN = www.chatpa4.test
Getting CA Private Key
Enter pass phrase for /etc/ssl/demoCA/private/cakey.pem:

Certificate and private key generated for: Web Server
Certificate and private key generated for: Chat Server

*** Adding controller
*** Add switches
*** Add hosts
*** Add links
*** Starting network
*** Configuring hosts
r5 r4 r3 h1 h2 h3 h4
*** Starting controllers
*** Starting switches
*** Post configure switches and hosts
*** Starting CLI:
mininet> pingall
*** Ping: testing ping reachability
r5 -> r4 r3 h1 h2 h3 h4
r4 -> r5 r3 h1 h2 h3 h4
r3 -> r5 r4 h1 h2 h3 h4
h1 -> r5 r4 r3 h2 h3 h4
h2 -> r5 r4 r3 h1 h3 h4
h3 -> r5 r4 r3 h1 h2 h4
h4 -> r5 r4 r3 h1 h2 h3
*** Results: 0% dropped (42/42 received)
mininet> 
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

Screen capture of a successful chat session between the two chat clients:


"Web Server: h2"@mininet-vm
root@mininet-vm: ~/CST311
root@mininet-vm: ~/CST311
root@mininet-vm: ~/CST311

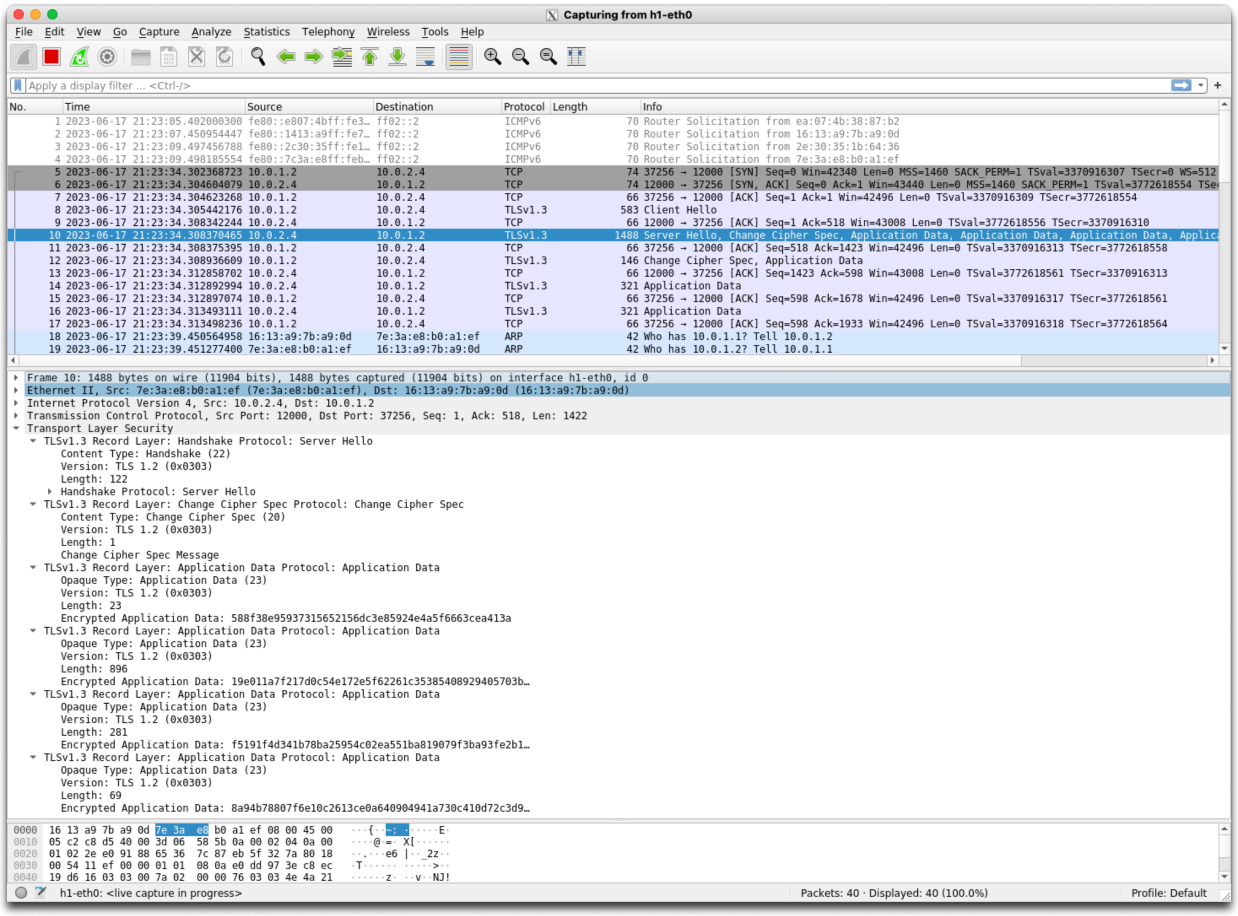
```
The server is ready to receive
```

```
INFO:__main__:The server is ready to receive on port 12000
INFO:__main__:Connected to client at ('10.0.2.2', 32828)
INFO:__main__:Connected to client at ('10.0.1.2', 52364)
INFO:__main__:Recieved query test "hi"
INFO:__main__:Recieved query test "hello"
root@mininet-vm:~/CST311#
```

```
Input lowercase sentence: hi
From Server:
Y : "hi", X : "hello"
root@mininet-vm:~/CST311#
```

```
Input lowercase sentence: hello
From Server:
Y : "hi", X : "hello"
root@mininet-vm:~/CST311#
```

Screen capture of a Wireshark trace of the communication between a chat client and the chat server:


Capturing from h1-eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

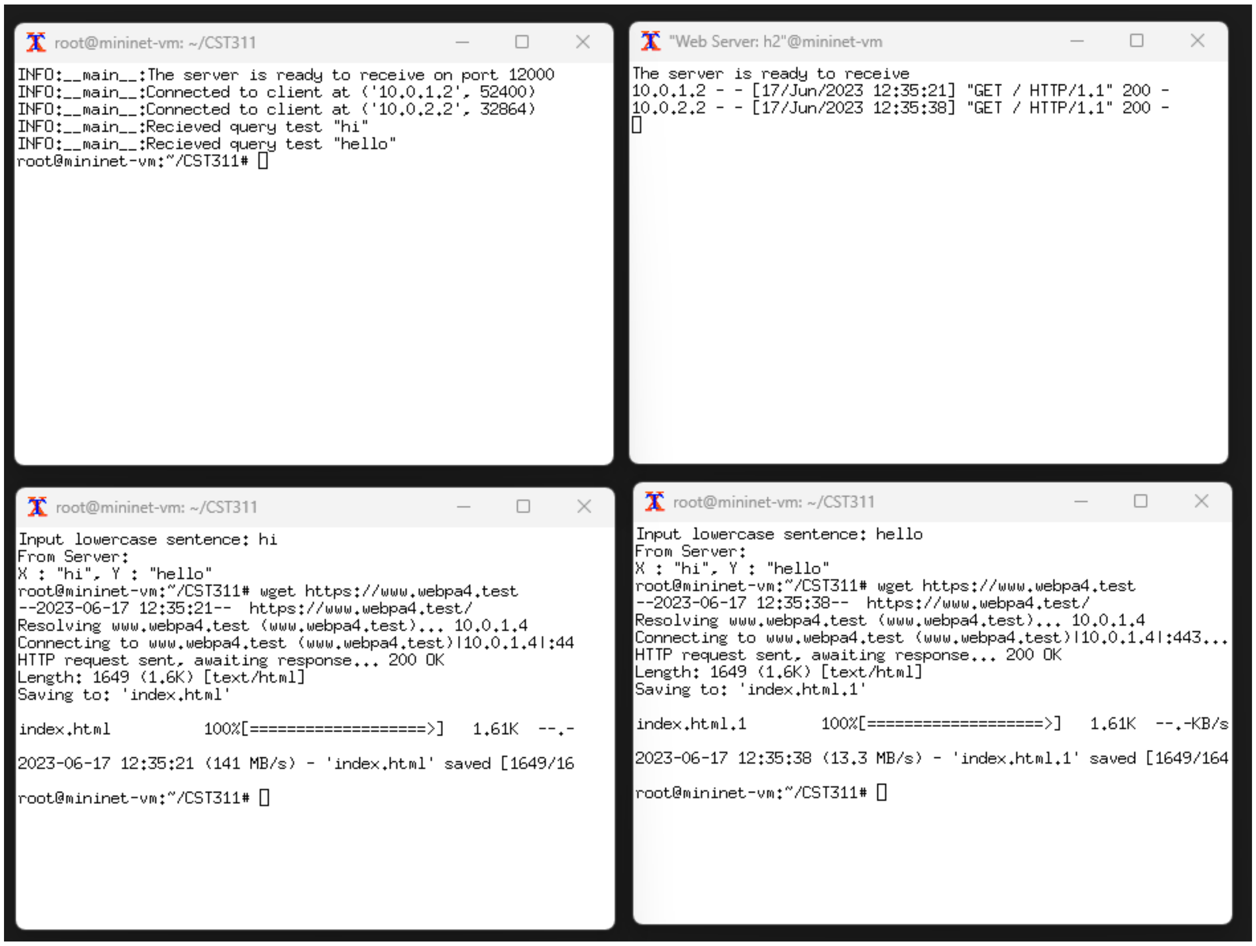
```
No.  Time                           Source                    Destination         Protocol Length Info
   1 2023-06-17 21:23:05.402000300 fe80::e807:4bff:fe3… ff02::2             ICMPv6     70 Router Solicitation from ea:07:4b:38:87:b2
   2 2023-06-17 21:23:07.450954447 fe80::1413:a9ff:fe7… ff02::2             ICMPv6     70 Router Solicitation from 16:13:a9:7b:a9:0d
   3 2023-06-17 21:23:09.497456788 fe80::2c30:35ff:fe1… ff02::2             ICMPv6     70 Router Solicitation from 2e:30:35:1b:64:36
   4 2023-06-17 21:23:09.498185554 fe80::7c3a:e8ff:feb… ff02::2             ICMPv6     70 Router Solicitation from 7e:3a:e8:b0:a1:ef
   5 2023-06-17 21:23:34.302368723 10.0.1.2             10.0.2.4            TCP        74 37256 → 12000 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM=1 TSval=3370916307 TSecr=0 WS=512
   6 2023-06-17 21:23:34.304604079 10.0.2.4             10.0.1.2            TCP        74 12000 → 37256 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1460 SACK_PERM=1 TSval=3772618554 TSe
   7 2023-06-17 21:23:34.304623268 10.0.1.2             10.0.2.4            TCP        66 37256 → 12000 [ACK] Seq=1 Ack=1 Win=42496 Len=0 TSval=3370916309 TSecr=3772618554
   8 2023-06-17 21:23:34.305442176 10.0.1.2             10.0.2.4            TLSv1.3   583 Client Hello
   9 2023-06-17 21:23:34.308342244 10.0.2.4             10.0.1.2            TCP        66 12000 → 37256 [ACK] Seq=1 Ack=518 Win=43008 Len=0 TSval=3772618556 TSecr=3370916310
  10 2023-06-17 21:23:34.308370465 10.0.2.4             10.0.1.2            TLSv1.3  1488 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Applica
  11 2023-06-17 21:23:34.308375395 10.0.1.2             10.0.2.4            TCP        66 37256 → 12000 [ACK] Seq=518 Ack=1423 Win=42496 Len=0 TSval=3370916313 TSecr=3772618558
  12 2023-06-17 21:23:34.308936609 10.0.1.2             10.0.2.4            TLSv1.3   146 Change Cipher Spec, Application Data
  13 2023-06-17 21:23:34.312858702 10.0.2.4             10.0.1.2            TCP        66 12000 → 37256 [ACK] Seq=1423 Ack=598 Win=43008 Len=0 TSval=3772618561 TSecr=3370916313
  14 2023-06-17 21:23:34.312892994 10.0.2.4             10.0.1.2            TLSv1.3   321 Application Data
  15 2023-06-17 21:23:34.312897074 10.0.1.2             10.0.2.4            TCP        66 37256 → 12000 [ACK] Seq=598 Ack=1678 Win=42496 Len=0 TSval=3370916317 TSecr=3772618561
  16 2023-06-17 21:23:34.313493111 10.0.2.4             10.0.1.2            TLSv1.3   321 Application Data
  17 2023-06-17 21:23:34.313498236 10.0.1.2             10.0.2.4            TCP        66 37256 → 12000 [ACK] Seq=598 Ack=1933 Win=42496 Len=0 TSval=3370916318 TSecr=3772618564
  18 2023-06-17 21:23:39.450564958 16:13:a9:7b:a9:0d    7e:3a:e8:b0:a1:ef   ARP        42 Who has 10.0.1.1? Tell 10.0.1.2
  19 2023-06-17 21:23:39.451277400 7e:3a:e8:b0:a1:ef    16:13:a9:7b:a9:0d   ARP        42 Who has 10.0.1.2? Tell 10.0.1.1
```

```
Frame 10: 1488 bytes on wire (11904 bits), 1488 bytes captured (11904 bits) on interface h1-eth0, id 0
Ethernet II, Src: 7e:3a:e8:b0:a1:ef (7e:3a:e8:b0:a1:ef), Dst: 16:13:a9:7b:a9:0d (16:13:a9:7b:a9:0d)
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.1.2
Transmission Control Protocol, Src Port: 12000, Dst Port: 37256, Seq: 1, Ack: 518, Len: 1422
Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 122
    Handshake Protocol: Server Hello
  TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
  TLSv1.3 Record Layer: Application Data Protocol: Application Data
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 23
    Encrypted Application Data: 588f38e95937315652156dc3e85924e4a5f6663cea413a
  TLSv1.3 Record Layer: Application Data Protocol: Application Data
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 896
    Encrypted Application Data: 19e011a7f217d0c54e172e5f62261c35385408929405703b…
  TLSv1.3 Record Layer: Application Data Protocol: Application Data
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 281
    Encrypted Application Data: f5191f4d341b78ba25954c02ea551ba819079f3ba93fe2b1…
  TLSv1.3 Record Layer: Application Data Protocol: Application Data
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 69
    Encrypted Application Data: 8a94b78807f6e10c2613ce0a640904941a730c410d72c3d9…
```

```
0000  16 13 a9 7b a9 0d 7e 3a  e8 b0 a1 ef 08 00 45 00   ···{··~:·····E·
0010  05 c2 c8 d5 40 00 3d 06  58 5b 0a 00 02 04 0a 00   ····@·=· X[······
0020  01 02 2e e0 91 88 65 36  7c 87 eb 5f 32 7a 80 18   ··.···e6 |··_2z··
0030  00 54 11 ef 00 00 01 01  08 0a e0 dd 97 3e c8 ec   ·T······ ·····>··
0040  19 d6 16 03 03 00 7a 02  00 00 76 03 03 4e 4a 21   ······z· ··v··NJ!
```

h1-eth0: <live capture in progress>   Packets: 40 · Displayed: 40 (100.0%)   Profile: Default

Screen capture of the successful wget (or curl) of the web server index file:



root@mininet-vm: ~/CST311

```
INFO:__main__:The server is ready to receive on port 12000
INFO:__main__:Connected to client at ('10.0.1.2', 52400)
INFO:__main__:Connected to client at ('10.0.2.2', 32864)
INFO:__main__:Recieved query test "hi"
INFO:__main__:Recieved query test "hello"
root@mininet-vm:~/CST311#
```

"Web Server: h2"@mininet-vm

```
The server is ready to receive
10.0.1.2 - - [17/Jun/2023 12:35:21] "GET / HTTP/1.1" 200 -
10.0.2.2 - - [17/Jun/2023 12:35:38] "GET / HTTP/1.1" 200 -
```

root@mininet-vm: ~/CST311

```
Input lowercase sentence: hi
From Server:
X : "hi", Y : "hello"
root@mininet-vm:~/CST311# wget https://www.webpa4.test
--2023-06-17 12:35:21--  https://www.webpa4.test/
Resolving www.webpa4.test (www.webpa4.test)... 10.0.1.4
Connecting to www.webpa4.test (www.webpa4.test)|10.0.1.4|:44
HTTP request sent, awaiting response... 200 OK
Length: 1649 (1.6K) [text/html]
Saving to: 'index.html'

index.html          100%[===================>]   1.61K  --.-

2023-06-17 12:35:21 (141 MB/s) - 'index.html' saved [1649/16

root@mininet-vm:~/CST311#
```

root@mininet-vm: ~/CST311

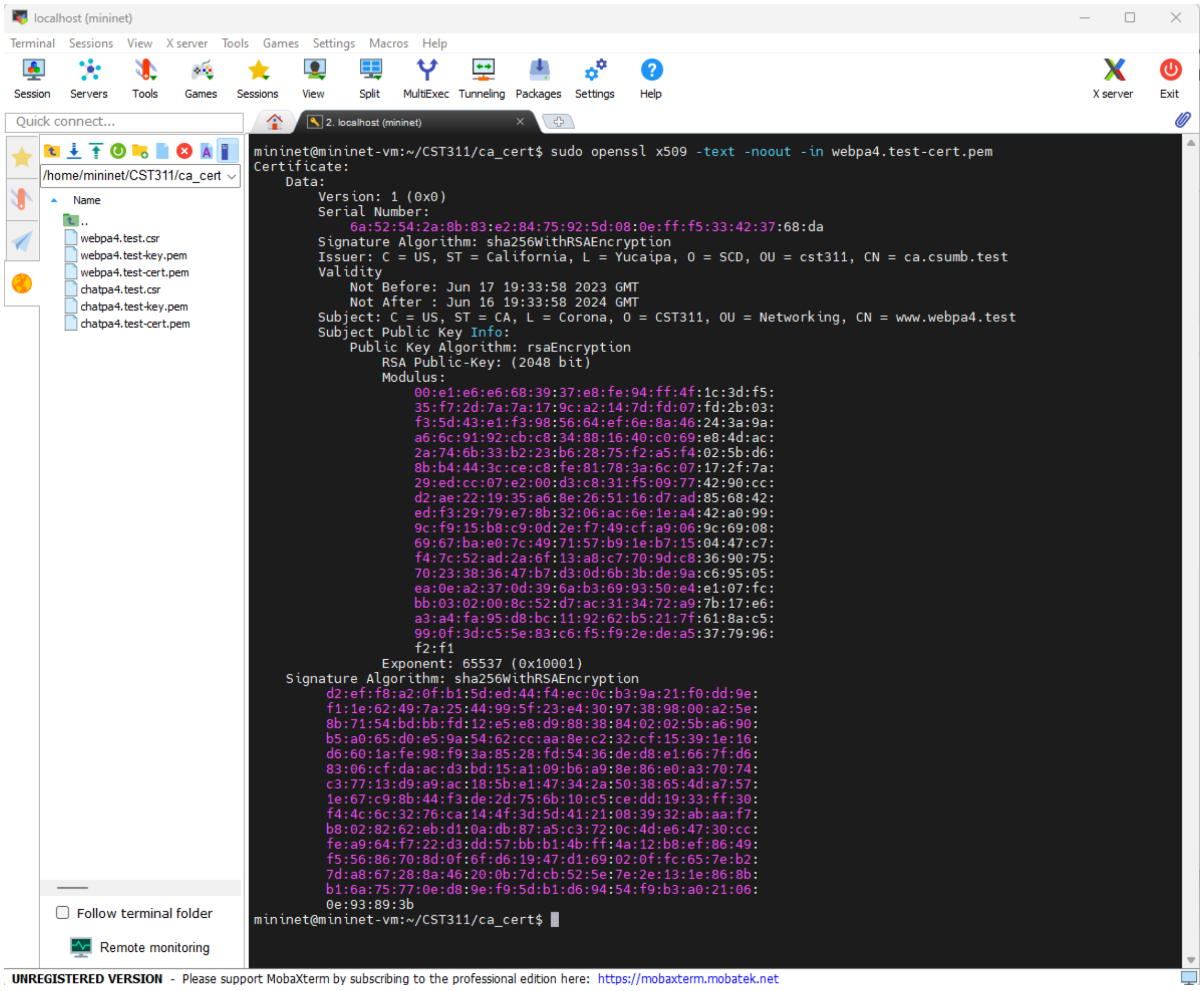
```
Input lowercase sentence: hello
From Server:
X : "hi", Y : "hello"
root@mininet-vm:~/CST311# wget https://www.webpa4.test
--2023-06-17 12:35:38--  https://www.webpa4.test/
Resolving www.webpa4.test (www.webpa4.test)... 10.0.1.4
Connecting to www.webpa4.test (www.webpa4.test)|10.0.1.4|:443...
HTTP request sent, awaiting response... 200 OK
Length: 1649 (1.6K) [text/html]
Saving to: 'index.html.1'

index.html.1        100%[===================>]   1.61K  --.-KB/s

2023-06-17 12:35:38 (13.3 MB/s) - 'index.html.1' saved [1649/164

root@mininet-vm:~/CST311#
```

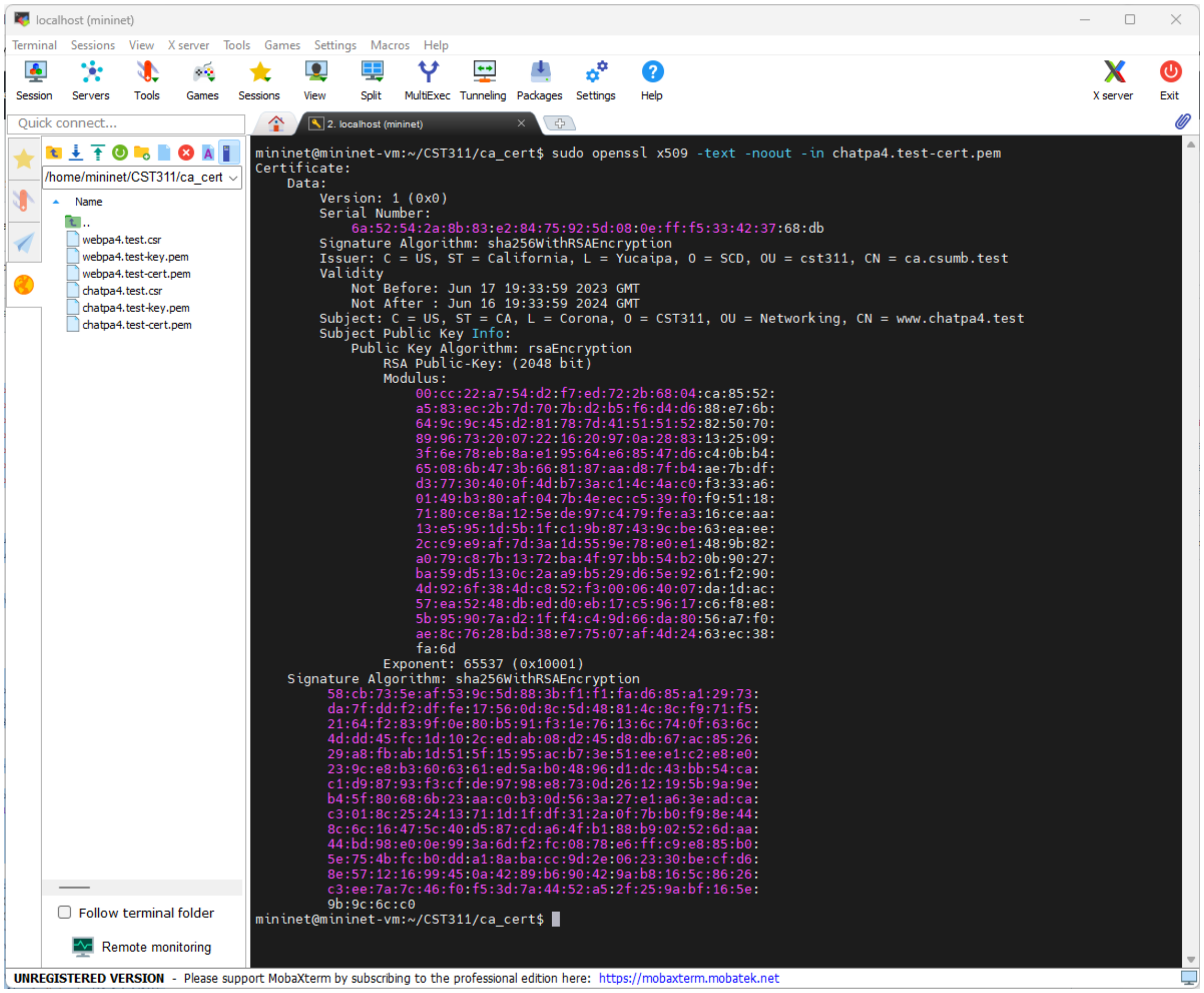
Screenshot of both decrypted server (web and chat) certificates.
Web server certificate:



localhost (mininet)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Quick connect...
2. localhost (mininet)
/home/mininet/CST311/ca_cert
Name
..
webpa4.test.csr
webpa4.test-key.pem
webpa4.test-cert.pem
chatpa4.test.csr
chatpa4.test-key.pem
chatpa4.test-cert.pem
Follow terminal folder
Remote monitoring
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
mininet@mininet-vm:~/CST311/ca_cert$ sudo openssl x509 -text -noout -in webpa4.test-cert.pem
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            6a:52:54:2a:8b:83:e2:84:75:92:5d:08:0e:ff:f5:33:42:37:68:da
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = Yucaipa, O = SCD, OU = cst311, CN = ca.csumb.test
        Validity
            Not Before: Jun 17 19:33:58 2023 GMT
            Not After : Jun 16 19:33:58 2024 GMT
        Subject: C = US, ST = CA, L = Corona, O = CST311, OU = Networking, CN = www.webpa4.test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:e1:e6:e6:68:39:37:e8:fe:94:ff:4f:1c:3d:f5:
                    35:f7:2d:7a:7a:17:9c:a2:14:7d:fd:07:fd:2b:03:
                    f3:5d:43:e1:f3:98:56:64:ef:6e:8a:46:24:3a:9a:
                    a6:6c:91:92:cb:c8:34:88:16:40:c0:69:e8:4d:ac:
                    2a:74:6b:33:b2:23:b6:28:75:f2:a5:f4:02:5b:d6:
                    8b:b4:44:3c:ce:c8:fe:81:78:3a:6c:07:17:2f:7a:
                    29:ed:cc:07:e2:00:d3:c8:31:f5:09:77:42:90:cc:
                    d2:ae:22:19:35:a6:8e:26:51:16:d7:ad:85:68:42:
                    ed:f3:29:79:e7:8b:32:06:ac:6e:1e:a4:42:a0:99:
                    9c:f9:15:b8:c9:0d:2e:f7:49:cf:a9:06:9c:69:08:
                    69:67:ba:e0:7c:49:71:57:b9:1e:b7:15:04:47:c7:
                    f4:7c:52:ad:2a:6f:13:a8:c7:70:9d:c8:36:90:75:
                    70:23:38:36:47:b7:d3:0d:6b:3b:de:9a:c6:95:05:
                    ea:0e:a2:37:0d:39:6a:b3:69:93:50:e4:e1:07:fc:
                    bb:03:02:00:8c:52:d7:ac:31:34:72:a9:7b:17:e6:
                    a3:a4:fa:95:d8:bc:11:92:62:b5:21:7f:61:8a:c5:
                    99:0f:3d:c5:5e:83:c6:f5:f9:2e:de:a5:37:79:96:
                    f2:f1
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         d2:ef:f8:a2:0f:b1:5d:ed:44:f4:ec:0c:b3:9a:21:f0:dd:9e:
         f1:1e:62:49:7a:25:44:99:5f:23:e4:30:97:38:98:00:a2:5e:
         8b:71:54:bd:bb:fd:12:e5:e8:d9:88:38:84:02:02:5b:a6:90:
         b5:a0:65:d0:e5:9a:54:62:cc:aa:8e:c2:32:cf:15:39:1e:16:
         d6:60:1a:fe:98:f9:3a:85:28:fd:54:36:de:d8:e1:66:7f:d6:
         83:06:cf:da:ac:d3:bd:15:a1:09:b6:a9:8e:86:e0:a3:70:74:
         c3:77:13:d9:a9:ac:18:5b:e1:47:34:2a:50:38:65:4d:a7:57:
         1e:67:c9:8b:44:f3:de:2d:75:6b:10:c5:ce:dd:19:33:ff:30:
         f4:4c:6c:32:76:ca:14:4f:3d:5d:41:21:08:39:32:ab:aa:f7:
         b8:02:82:62:eb:d1:0a:db:87:a5:c3:72:0c:4d:e6:47:30:cc:
         fe:a9:64:f7:22:d3:dd:57:bb:b1:4b:ff:4a:12:b8:ef:86:49:
         f5:56:86:70:8d:0f:6f:d6:19:47:d1:69:02:0f:fc:65:7e:b2:
         7d:a8:67:28:8a:46:20:0b:7d:cb:52:5e:7e:2e:13:1e:86:8b:
         b1:6a:75:77:0e:d8:9e:f9:5d:b1:d6:94:54:f9:b3:a0:21:06:
         0e:93:89:3b
mininet@mininet-vm:~/CST311/ca_cert$
```

Chat server certificate:


localhost (mininet)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Quick connect...
2. localhost (mininet)
/home/mininet/CST311/ca_cert
Name
..
webpa4.test.csr
webpa4.test-key.pem
webpa4.test-cert.pem
chatpa4.test.csr
chatpa4.test-key.pem
chatpa4.test-cert.pem
Follow terminal folder
Remote monitoring
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
mininet@mininet-vm:~/CST311/ca_cert$ sudo openssl x509 -text -noout -in chatpa4.test-cert.pem
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            6a:52:54:2a:8b:83:e2:84:75:92:5d:08:0e:ff:f5:33:42:37:68:db
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = Yucaipa, O = SCD, OU = cst311, CN = ca.csumb.test
        Validity
            Not Before: Jun 17 19:33:59 2023 GMT
            Not After : Jun 16 19:33:59 2024 GMT
        Subject: C = US, ST = CA, L = Corona, O = CST311, OU = Networking, CN = www.chatpa4.test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cc:22:a7:54:d2:f7:ed:72:2b:68:04:ca:85:52:
                    a5:83:ec:2b:7d:70:7b:d2:b5:f6:d4:d6:88:e7:6b:
                    64:9c:9c:45:d2:81:78:7d:41:51:51:52:82:50:70:
                    89:96:73:20:07:22:16:20:97:0a:28:83:13:25:09:
                    3f:6e:78:eb:8a:e1:95:64:e6:85:47:d6:c4:0b:b4:
                    65:08:6b:47:3b:66:81:87:aa:d8:7f:b4:ae:7b:df:
                    d3:77:30:40:0f:4d:b7:3a:c1:4c:4a:c0:f3:33:a6:
                    01:49:b3:80:af:04:7b:4e:ec:c5:39:f0:f9:51:18:
                    71:80:ce:8a:12:5e:de:97:c4:79:fe:a3:16:ce:aa:
                    13:e5:95:1d:5b:1f:c1:9b:87:43:9c:be:63:ea:ee:
                    2c:c9:e9:af:7d:3a:1d:55:9e:78:e0:e1:48:9b:82:
                    a0:79:c8:7b:13:72:ba:4f:97:bb:54:b2:0b:90:27:
                    ba:59:d5:13:0c:2a:a9:b5:29:d6:5e:92:61:f2:90:
                    4d:92:6f:38:4d:c8:52:f3:00:06:40:07:da:1d:ac:
                    57:ea:52:48:db:ed:d0:eb:17:c5:96:17:c6:f8:e8:
                    5b:95:90:7a:d2:1f:f4:c4:9d:66:da:80:56:a7:f0:
                    ae:8c:76:28:bd:38:e7:75:07:af:4d:24:63:ec:38:
                    fa:6d
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         58:cb:73:5e:af:53:9c:5d:88:3b:f1:f1:fa:d6:85:a1:29:73:
         da:7f:dd:f2:df:fe:17:56:0d:8c:5d:48:81:4c:8c:f9:71:f5:
         21:64:f2:83:9f:0e:80:b5:91:f3:1e:76:13:6c:74:0f:63:6c:
         4d:dd:45:fc:1d:10:2c:ed:ab:08:d2:45:d8:db:67:ac:85:26:
         29:a8:fb:ab:1d:51:5f:15:95:ac:b7:3e:51:ee:e1:c2:e8:e0:
         23:9c:e8:b3:60:63:61:ed:5a:b0:48:96:d1:dc:43:bb:54:ca:
         c1:d9:87:93:f3:cf:de:97:98:e8:73:0d:26:12:19:5b:9a:9e:
         b4:5f:80:68:6b:23:aa:c0:b3:0d:56:3a:27:e1:a6:3e:ad:ca:
         c3:01:8c:25:24:13:71:1d:1f:df:31:2a:0f:7b:b0:f9:8e:44:
         8c:6c:16:47:5c:40:d5:87:cd:a6:4f:b1:88:b9:02:52:6d:aa:
         44:bd:98:e0:0e:99:3a:6d:f2:fc:08:78:e6:ff:c9:e8:85:b0:
         5e:75:4b:fc:b0:dd:a1:8a:ba:cc:9d:2e:06:23:30:be:cf:d6:
         8e:57:12:16:99:45:0a:42:89:b6:90:42:9a:b8:16:5c:86:26:
         c3:ee:7a:7c:46:f0:f5:3d:7a:44:52:a5:2f:25:9a:bf:16:5e:
         9b:9c:6c:c0
mininet@mininet-vm:~/CST311/ca_cert$
```

List of lines that were changed and why:
The lines that add the routers (r1, r2, and r3) (lines 40-45) were updated to have a valid IP address with their subnet mask, which is needed to identify each router. The subnet mask allows the routers to be on the same network since the first 24 bits of their IP address are the same.
The lines that add the hosts (h1, h2, h3, and h4) (lines 48-51) were updated to include the subnet mask as well and the default route for each host. The subnet masks were added to also allow the hosts to be on the same network since the first 24 bits of their IP addresses will be the same. The hosts will also be on the same network as the routers since they are both given the same subnet mask. Default routes are given to forward a packet to a location if the packet does not have the same local subnet.
The lines 58-61 were modified to assign IP addresses to the links between the routers and switches. Without these IP addresses the routers and switches would not be connected together.
The lines to create 6 static routes were added in lines 66-82 to provide static routes between the routers. The static routes allow the packets to have a path from one host to another host.

Questions:

1. What were any interesting findings and lessons learned?
   We learned that configuring IP addresses and routes are important in order for the network to function correctly. Static routes need to have subnets and the next hop in order to route properly. It is also important for the newly created certificate and key to be placed in the same path that the web and chat server have in order for the servers to use the certificate. We also learned that the makeTerm function allows for hosts to run commands that are given to it so the user does not have to manually input the commands.
2. Why didn't the original program forward packets between the hosts?
   The original program does not forward packets because the IP addresses in lines 26, 30, and 32 are '0.0.0.0'. If all the routers had the same IP address of 0.0.0.0, packets will not be able to be forward to a specific router, but providing a specific IP fixes this. There are also no routing algorithms in the original program so the packets are not directed where to go.
3. Is the line ' r3.cmd('sysctl -w net.ipv4.ip_forward=1') ' required?
   The line is required because it allows packets to be forward onto the network. This line allows the packets to move past r3. Without this line the packets would not be forward to the next router which would cause the packets to never get to the destination. This would cause routing issues and h3 and h4 would never receive the packets from h1 and h2. If packets are not able to reach their destination, then the networks would not communicate properly and the "internet" would not work.
4. Intentionally break your working program, e.g.: change a subnet length, IP address, or default route for a host. Explain why your change caused the network to break.
   Changing any one of these examples would cause the network to break because the packets would not be routed correctly. If s subnet length is changed then the subnet of the

hosts would not match. Changing the IP address would cause a routing issue because the packet would not be sent to the correct location or the packet might not be sent anywhere if the IP address is invalid. Changing a default route for a host would cause the network to break because packets will not be forwarded correctly to the next hop.