Final Exam

Question 2

< **Back to the Question**

The correct command is:

```
$ openssl x509 -in ~/shared/certs/client.pem -inform PEM -nameopt RFC2253 -text
```
COPY

Which will output:

```
                                                    COPY

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 266611 (0x41173)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US,ST=New York,L=New York City,O=MongoDB,OU=University,CN=localhost
```

```
        Validity
            Not Before: Nov  7 20:03:00 2016 GMT
            Not After : Nov  7 20:03:00 2036 GMT
        Subject: C=US,ST=New York,L=New York City,O=MongoDB,OU=University2,CN=M310 Client
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:94:45:9e:e1:54:26:69:2c:d7:c5:a4:f8:f5:17:
                    52:07:80:77:23:a0:7a:10:3e:ae:11:54:5d:3e:05:
                    96:f4:4e:44:22:89:9a:cc:ae:ef:ba:a3:92:e6:b7:
                    f7:13:3b:b6:95:8e:f0:7f:04:75:b1:c8:65:e3:d2:
                    04:22:76:99:2c:d6:5d:54:83:4a:83:43:b5:25:99:
                    df:d2:fd:51:64:d0:b9:d9:66:0a:8f:65:c7:69:70:
                    6f:13:9c:71:f4:08:06:b5:da:40:66:3d:a9:9d:ed:
                    a8:c7:81:df:3d:3a:b6:47:21:39:de:a5:83:f1:c2:
                    15:07:86:0e:74:26:ee:0e:67:07:6b:c0:9f:aa:91:
                    ee:14:77:28:67:e0:ae:95:29:c8:91:dc:55:a9:4f:
                    cc:98:b8:34:fe:87:c7:f5:c4:84:4c:d4:2e:d6:e5:
                    45:55:f6:0e:dd:16:fb:bb:d1:3c:e0:d8:fc:0b:d6:
                    8f:79:19:42:56:38:35:27:c6:3e:6f:85:e9:39:3e:
                    4a:e8:26:f5:e3:36:c5:15:0d:5c:6e:bf:df:21:31:
                    e9:f9:d1:69:00:ba:ae:ab:73:90:c3:96:02:3d:b3:
                    6d:c6:58:14:35:f9:1f:79:88:03:71:83:67:62:d1:
                    a1:e4:4e:4d:3f:f2:c2:09:fd:00:af:dc:b6:0a:2c:
                    a0:ed
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:localhost, IP Address:127.0.0.1, DNS:database.m310.mongodb.university,
DNS:infrastructure.m310.mongodb.university
```

```
    Signature Algorithm: sha1WithRSAEncryption
        01:90:dc:e0:2b:04:5d:9e:f0:ba:66:ee:cf:db:63:ee:dc:96:
        ba:6e:3c:d3:e6:74:1b:17:11:1c:98:a0:1b:97:d1:54:a4:3d:
        a9:99:14:5c:b2:22:97:56:5b:aa:d2:83:5a:37:c4:7d:73:73:
        8a:dd:7b:21:b9:9f:a4:dc:f2:b4:5e:42:39:ad:20:98:51:b9:
        d9:aa:e9:1f:3d:ac:5a:55:df:01:2b:93:45:ac:c3:43:c3:5e:
        58:5c:98:fa:e7:07:8c:c6:f7:3d:f4:44:32:28:d5:e7:7b:ae:
        f0:9f:46:fb:b4:17:92:55:c2:fa:b9:ac:65:89:ae:55:0b:ee:
        6c:25:05:3c:4b:87:1b:4e:d2:72:9d:c0:07:76:30:5f:e2:ed:
        aa:f5:61:af:92:20:5e:ff:71:c5:5d:51:54:2c:92:4e:0e:70:
        5b:c4:00:81:5f:9b:07:3d:98:7a:b5:2f:c3:fd:a3:3b:14:c8:
        a6:7c:ff:b7:dd:c6:c3:f3:17:aa:d5:c6:88:22:d7:ee:c2:25:
        cf:9f:80:96:cf:c6:a2:86:65:4c:69:21:9b:06:a8:ab:6a:da:
        bf:a6:6f:9c:3a:f5:d6:18:62:32:89:29:bb:f3:3b:84:f0:a3:
        18:4d:a5:16:8c:04:c8:34:68:f7:09:f0:e9:0d:67:8d:9b:a2:
        e3:37:b4:9a
-----BEGIN CERTIFICATE-----
MIIDzjCCAragAwIBAgIDBBFzMA0GCSqGSIb3DQEBBQUAMHMxEjAQBgNVBAMTCWxv
Y2FsaG9zdDETMBEGA1UECxMKVW5pdmVyc2l0eTEQMA4GA1UEChMHTW9uZ29EQjEW
MBQGA1UEBxMNTmV3IFlvcmsgQ2l0eTERMA8GA1UECBMITmV3IFlvcmsxCzAJBgNV
BAYTAlVTMB4XDTE2MTEwNzIwMDMwMFoXDTM2MTEwNzIwMDMwMFowdjEUMBIGA1UE
AxMLTTMxMCBDbGllbnQxFDASBgNVBAsTC1VuaXZlcnNpdHkyMRAwDgYDVQQKEwdN
b25nb0RCMRYwFAYDVQQHEw1OZXcgWW9yayBDaXR5MREwDwYDVQQIEwhOZXcgWW9y
azELMAkGA1UEBhMCVVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCU
RZ7hVCZpLNfFpPj1F1IHgHcjoHoQPq4RVF0+BZb0TkQiiZrMru+6o5Lmt/cTO7aV
jvB/BHWxyGXj0gQidpks1l1Ug0qDQ7Ulmd/S/VFk0LnZZgqPZcdpcG8TnHH0CAa1
2kBmPamd7ajHgd89OrZHITnepYPxwhUHhg50Ju4OZwdrwJ+qke4Udyhn4K6VKciR
3FWpT8yYuDT+h8f1xIRM1C7W5UVV9g7dFvu70Tzg2PwL1o95GUJWODUnxj5vhek5
PkroJvXjNsUVDVxuv98hMen50WkAuq6rc5DDlgI9s23GWBQ1+R95iANxg2di0aHk
Tk0/8sIJ/QCv3LYKLKDtAgMBAAGjaDBmMGQGA1UdEQRdMFuCCWxvY2FsaG9zdIcE
fwAAAYIgZGF0YWJhc2UuubTMxMC5tb25nb2RiLnVuaXZlcnNpdHmCJmluZnJhc3Ry
```

dWN0dXJlLm0zMTAubW9uZ29kYi51bml2ZXJzaXR5MA0GCSqGSIb3DQEBBQUAA4IB
AQABkNzgKwRdnvC6Zu7P22Pu3Ja6bjzT5nQbFxEcmKAbl9FUpD2pmRRcsiKXVluq
0oNaN8R9c3OK3XshuZ+k3PK0XkI5rSCYUbnZqukfPaxaVd8BK5NFrMNDw15YXJj6
5weMxvc99EQyKNXne67wn0b7tBeSVcL6uaxlia5VC+5sJQU8S4cbTtJyncAHdjBf
4u2q9WGvkiBe/3HFXVFULJJODnBbxACBX5sHPZh6tS/D/aM7FMimfP+33cbD8xeq
1caIItfuwiXPn4CWz8aihmVMaSGbBqiratq/pm+cOvXWGGIyiSm78zuE8KMYTaUW
jATINGj3CfDpDWeNm6LjN7Sa
-----END CERTIFICATE-----

Proceed to next section