1. **Step 4 a through h for login.iastate.edu**
    a. **What version of TLS is being used to encrypt traffic?**
        TLS 1.3

    b. **What is the full name of the ciphersuite being used?**
        TLS_AES_256_GCM_SHA256

        i. **What key exchange protocol is used?**
            ECDHE

        ii. **What type of key (symmetric or asymmetric) does key exchange protocol exchange?**
            Asymmetric
        iii. **What type of key (symmetric or asymmetric) does key exchange protocol create?**
            Symmetric
        iv. **What is that created key used for? (Hint: There is another name for this key when we browse the web.)**
            Encrypting Traffic to and from the web server (Session key)

        v. **What is the cryptographic algorithm used for signing the certificate?**
            SHA-256 with RSA

        vi. **What is the block cipher used to encrypt the data?**
            AES
        vii. **How many bits are in the block cipher's key?**
            128 bits
        viii. **What is the block cipher mode being used?**
            GCM
        ix. **What is the hash function being used?**
            SHA2-256

    c. **Who is the certificate issued to (who is the owner)?**
        Iowa State University of Science and Technology
    d. **From what date to what date is the certificate valid?**
        Aug 18, 2021 to Aug 18, 2022
    e. **Who is the CA?**
        InCommon (UserTrust)
    f. **Is this a DV, OV, or EV certificate?**
        OV
    g. **What is the public exponent in the public key?**
        65537

(15 points)

2. **Screenshot of successful validation of login.iatate.edu certificate**
   (10 points)

```
cpre331@desktop:~/Downloads$ openssl verify -CAfile cert_bundle.pem login-iastate-edu.pem
login-iastate-edu.pem: OK
```

3. **Screenshot of vi of PEM version of login.iastate.edu certificate (base64 encode information)**
   (10 points)

```
-----BEGIN CERTIFICATE-----
MIIGyzCCBbOgAwIBAgIQO77OY/LU1au7WwHJS8FcgjANBgkqhkiG9w0BAQsFADB2
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUkxEjAQBgNVBAcTCUFubiBBcmJvcjES
MBAGA1UEChMJSW50ZXJuZXQyMREwDwYDVQQLEwhJbkNvbW1vbjEfMB0GA1UEAxMW
SW5Db21tb24gUlNBIFNlcnZlciBDQTAeFw0yMTA4MTgwMDAwMDBaFw0yMjA4MTgy
MzU5NTlaMIGBMQswCQYDVQQGEwJVUzENMAsGA1UECBMESW93YTENMAsGA1UEBxME
QW1lczE4MDYGA1UEChMvSW93YSBTdGF0ZSBVbml2ZXJzaXR5IG9mIFNjaWVuY2Ug
YW5kIFRlY2hub2xvZ3kxGjAYBgNVBAMTEWxvZ2luLmlhc3RhdGUuZWR1MIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3Xk+bpFZw0bJXzYtLNdiBGBBXZiD
VMfxR2IsFGJT5pqC23iXmNnpHDQakdT+CWGqhiPp9onT3ob8Eoe+X5Xn01xIfle5
hi1u2I0A3g6hQ+xTBHtWG6kzw6LQfERhxH7f0MfCGPSy1P7M4QblWmbo/09w2W9y
21+Jfo+VfKI+UVxOducXzaLcPB4hC+PUzFLwS3E/HgetGhLheennYZD0LW0BjTV4
7H2tRrATIgTnY8TWfrpvTSoD8P1gMqWf35WJnFFcBLhr0eZMUN0vQEv6orLYNUpz
ykk9xVKNsSrebpz0PjJGX256VG3VxaRKa3ZgiLBIFcVXzPDyKVbD+wNYowIDAQAB
o4IDRzCCA0MwHwYDVR0jBBgwFoAUHgWjd49sluJbh0umtIascQAM5zgwHQYDVR0O
BBYEFFGajielzRZlU4Z1MxpoCrCGjrTWMA4GA1UdDwEB/wQEAwIFoDAMBgNVHRMB
Af8EAjAAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjBnBgNVHSAEYDBe
MFIGDCsGAQQBriMBBAMBATBCMEAGCCsGAQUFBwIBFjRodHRwczovL3d3dy5pbmNv
bW1vbi5vcmcvY2VydC9yZXBvc2l0b3J5L2Nwc19zc2wucGRmMAgGBmeBDAECAjBE
BgNVHR8EPTA7MDmgN6A1hjNodHRwOi8vY3JsLmluY29tbW9uLXJzYS5vcmcvSW5D
b21tb25SU0FTZXJ2ZXJDQS5jcmwwdQYIKwYBBQUHAQEEaTBnMD4GCCsGAQUFBzAC
hjJodHRwOi8vY3J0LnVzZXJ0cnVzdC5jb20vSW5Db21tb25SU0FTZXJ2ZXJDQV8y
LmNydDAlBggrBgEFBQcwAYYZaHR0cDovL29jc3AudXNlcnRydXN0LmNvbTAcBgNV
HREEFTATghFsb2dpbi5pYXN0YXRlLmVkdTCCAX4GCisGAQQB1nkCBAIEggFuBIIB
agFoAHYARqVV63X6kSAwtaKJafTzfREsQXS+/Um4havy/HD+bUcAAAF7WuzDCgAA
BAMARzBFAiBvXReh7LGC80opTvSxLRiDrlXozO8Ineg1QCBTbUP/6QIhALkECTtK
jbPGtPH2Ob6dnWSd5hh7enshLsq44fz30uw5AHYAQcjKsd8iRkoQxqE6CUKHXk4x
ixsD6+tLx2jwkGKWBvYAAAF7WuzCzAAABAMARzBFAiEAlBWmpIN6iZ3NkVYmoBr
1jQ8AxkxQoW+uCY5Mv37rpwCIBeIf2Z1bw1mkBZTYqeiCIasEEUEqq9eOGVwL9zD
6I0RAHYAKXm+8J45OSHwVnOfY6V35b5XfZxgCvj5TV0mXCVdx4QAAAF7WuzCqwAA
BAMARzBFAiAxPeOv+8la4Vzi5eSobVQ0VnwroEFfz6BS4YRdU3fNhAIhAJ9z3QWn
vpNNbLWfXzAfFn7gAEyfM2ebRSc0CRaFWylRMA0GCSqGSIb3DQEBCwUAA4IBAQCB
az/J+N0Oi5yDWj2Btu7E+phW43FrppUd6/zo/sRFy6aiuGaWmB8H3LaOCZKvsdEU
SeCvbSyYAFZbAOaa5Bx7bd5p7iMRXiUZeG01tvKNeMjQc4OvepFhsy6xHDmQlMIh
cscvPr+jtRJ4b/krUbW1/N5fqPeUjyWYE/FLpv3ZHr8FilBLvWUuDZa8ZEdKKA/w
1/u4YB/LmDQzu+h+Wbm366RZTFCNYDBGAw/p1rjS3aUHebH6uCwWhTXJReLC7vRX
jAC+9019Wl7mtNQwiyyvqYqzSGZSKgcR6PqLJovGSpQFNKsvR+FdOXTD4vIS6HB/
HEqY/yuHY042PYz5AsVf
-----END CERTIFICATE-----
```

4. **Screenshot of text information of login.iastate.edu certificate** (5 points)

```
cpre331@desktop:~/Downloads$ openssl x509 -in login-iastate-edu.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            3b:be:ce:63:f2:d4:d5:ab:bb:5b:01:c9:4b:c1:5c:82
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = MI, L = Ann Arbor, O = Internet2, OU = InCommon, CN = InCommon RSA Server CA
        Validity
            Not Before: Aug 18 00:00:00 2021 GMT
            Not After : Aug 18 23:59:59 2022 GMT
        Subject: C = US, ST = Iowa, L = Ames, O = Iowa State University of Science and Technology, CN = login.iastate.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:dd:79:3e:6e:91:59:c3:46:c9:5f:36:2d:2c:d7:
                    62:04:60:41:5d:98:83:54:c7:f1:47:62:2c:14:62:
                    53:e6:9a:82:db:78:97:98:d9:e9:1c:34:1a:91:d4:
                    fe:09:61:aa:86:23:e9:f6:89:d3:de:86:fc:12:87:
                    be:5f:95:e7:d3:5c:48:7e:57:b9:86:2d:6e:d8:8d:
                    00:de:0e:a1:43:ec:53:04:7b:56:1b:a9:33:c3:a2:
                    d0:7c:44:61:c4:7e:df:d0:c7:c2:18:f4:b2:d4:fe:
                    cc:e1:06:e5:5a:66:e8:ff:4f:70:d9:6f:72:db:5f:
                    89:7e:8f:95:7c:a2:3e:51:5c:4e:76:e7:17:cd:a2:
                    dc:3c:1e:21:0b:e3:d4:cc:52:f0:4b:71:3f:1e:07:
                    ad:1a:12:e1:79:e9:e7:61:90:f4:2d:6d:01:8d:35:
                    78:ec:7d:ad:46:b0:13:22:04:e7:63:c4:d6:7e:ba:
                    6f:4d:2a:03:f0:fd:60:32:a5:9f:df:95:89:9c:51:
                    5c:04:b8:6b:d1:e6:4c:50:dd:2f:40:4b:fa:a2:b2:
                    d8:35:4a:73:ca:49:3d:c5:52:8d:b1:2a:de:6e:9c:
                    f4:3e:32:46:5f:6e:7a:54:6d:d5:c5:a4:4a:6b:76:
                    60:88:b0:48:15:c5:57:cc:f0:f2:29:56:c3:fb:03:
                    58:a3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:1E:05:A3:77:8F:6C:96:E2:5B:87:4B:A6:B4:86:AC:71:00:0C:E7:38

            X509v3 Subject Key Identifier:
                51:9A:8E:27:A5:CD:16:65:53:86:75:33:1A:68:0A:B0:86:8E:B4:D6
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
```

```
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
    X509v3 Certificate Policies:
        Policy: 1.3.6.1.4.1.5923.1.4.3.1.1
          CPS: https://www.incommon.org/cert/repository/cps_ssl.pdf
        Policy: 2.23.140.1.2.2

    X509v3 CRL Distribution Points:

        Full Name:
          URI:http://crl.incommon-rsa.org/InCommonRSAServerCA.crl

    Authority Information Access:
        CA Issuers - URI:http://crt.usertrust.com/InCommonRSAServerCA_2.crt
        OCSP - URI:http://ocsp.usertrust.com

    X509v3 Subject Alternative Name:
        DNS:login.iastate.edu
    CT Precertificate SCTs:
        Signed Certificate Timestamp:
            Version   : v1 (0x0)
            Log ID    : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
                        11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
            Timestamp : Aug 18 20:21:11.050 2021 GMT
            Extensions: none
            Signature : ecdsa-with-SHA256
                        30:45:02:20:6F:5D:17:A1:EC:B1:82:F3:4A:29:4E:F4:
                        B1:2D:18:83:AE:55:E8:CC:EF:08:9D:E8:35:40:20:53:
                        6D:43:FF:E9:02:21:00:B9:04:09:3B:4A:8D:B3:C6:B4:
                        F1:F6:39:BE:9D:9D:64:9D:E6:18:7B:7A:7B:21:2E:CA:
                        B8:E1:FC:F7:D2:EC:39
        Signed Certificate Timestamp:
            Version   : v1 (0x0)
            Log ID    : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
                        4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
            Timestamp : Aug 18 20:21:10.988 2021 GMT
            Extensions: none
            Signature : ecdsa-with-SHA256
                        30:45:02:21:00:94:15:A6:9A:92:0D:EA:26:77:36:45:
                        58:9A:80:6B:D6:34:3C:03:19:31:42:85:BE:B8:26:39:
                        32:FD:FB:AE:9C:02:20:17:88:7F:66:75:6F:0D:66:90:
                        16:53:62:A7:A2:08:86:AC:10:45:04:AA:AF:5E:38:65:
                        70:2F:DC:C3:E8:8D:11
        Signed Certificate Timestamp:
```

```
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
                            BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
                Timestamp : Aug 18 20:21:10.955 2021 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:45:02:20:31:3D:E3:AF:FB:C9:5A:E1:5C:E2:E5:E4:
                            A8:6D:54:34:56:7C:2B:A0:41:5F:CF:A0:52:E1:84:5D:
                            53:77:CD:84:02:21:00:9F:73:DD:05:A7:BE:93:4D:6C:
                            B5:9F:5F:30:1F:16:7E:E0:00:4C:9F:33:67:9B:45:27:
                            34:09:16:85:5B:29:51
Signature Algorithm: sha256WithRSAEncryption
     81:6b:3f:c9:f8:dd:0e:8b:9c:83:5a:3d:81:b6:ee:c4:fa:98:
     56:e3:71:6b:a6:95:1d:eb:fc:e8:fe:c4:45:cb:a6:a2:b8:66:
     96:98:1f:07:dc:b6:8e:09:92:af:b1:d1:14:49:e0:af:6d:2c:
     98:00:56:5b:00:e6:9a:e4:1c:7b:6d:de:69:ee:23:11:5e:25:
     19:78:6d:35:b6:f2:8d:78:c8:d0:73:83:af:7a:91:61:b3:2e:
     b1:1c:39:90:94:c2:21:72:c7:2f:3e:bf:a3:b5:12:78:6f:f9:
     2b:51:b5:b5:fc:de:5f:a8:f7:94:8f:25:98:13:f1:4b:a6:fd:
     d9:1e:bf:05:8a:50:4b:bd:65:2e:0d:96:bc:64:47:4a:28:0f:
     f0:d7:fb:b8:60:1f:cb:98:34:33:bb:e8:7e:59:b9:b7:eb:a4:
     59:4c:50:8d:60:30:46:03:0f:e9:d6:b8:d2:dd:a5:07:79:b1:
     fa:b8:2c:16:85:35:c9:45:e2:c2:ee:f4:57:8c:00:be:f7:4d:
     7d:5a:5e:e6:b4:d4:30:8b:2c:af:a9:8a:b3:48:66:52:2a:07:
     11:e8:fa:8b:26:8b:c6:4a:94:05:34:ab:2f:47:e1:5d:39:74:
     c3:e2:f2:12:e8:70:7f:1c:4a:98:ff:2b:87:63:4e:36:3d:8c:
     f9:02:c5:5f
```

5. **Screenshot of the SHA1 and SHA256 hashes of login.iastate.edu certificate, compare with fingerprints**
   (10 points)

```
cpre331@desktop:~/Downloads$ openssl x509 -in login-iastate-edu.pem -outform der -out login-iastate-edu.der
cpre331@desktop:~/Downloads$ sha1sum login-iastate-edu.der
c4a4ad240744d572db4135e917dd8e2dc99cb633  login-iastate-edu.der
cpre331@desktop:~/Downloads$ sha256sum login-iastate-edu.der
6906b08195fd42b159131ac28f02de5f517751099f7b2d9dc9e660440611be45  login-iastate-edu.der
```

6. **Step 4 a through h for canvas.iastate.edu**
   a. **What version of TLS is being used to encrypt traffic?**
      TLS 1.2

   b. **What is the full name of the ciphersuite being used?**
      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA256
      i. **What key exchange protocol is used?**
         ECDHE
      ii. **What type of key (symmetric or asymmetric) does key exchange protocol exchange?**
         Asymmetric
      iii. **What type of key (symmetric or asymmetric) does key exchange protocol create?**
         Symmetric
      iv. **What is that created key used for? (Hint: There is another name for this key when we browse the web.)**
         Encrypting Traffic to and from the web server (Session key)

      v. **What is the cryptographic algorithm used for signing the certificate?**
         SHA-256 with RSA

      vi. **What is the block cipher used to encrypt the data?**
         AES
      vii. **How many bits are in the block cipher's key?**
         256 bits
      viii. **What is the block cipher mode being used?**
         GCM
      ix. **What is the hash function being used?**
         SHA2-256

   c. **Who is the certificate issued to (who is the owner)?**
      Instructure, Inc
   d. **From what date to what date is the certificate valid?**
      Jun 26, 2020 to Jun 30, 2022

e. **Who is the CA?**
DigiCert

f. **Is this a DV, OV, or EV certificate?**
OV

g. **What is the public exponent in the public key?**
65537

(15 points)

7. **Screenshot of successful validation of canvas.iastate.edu certificate** (10 points)

```
cpre331@desktop:~/Downloads$ openssl verify -CAfile cert_bundle_canvas.pem canvas-iastate-edu.pem
canvas-iastate-edu.pem: OK
cpre331@desktop:~/Downloads$
```

8. **Screenshot of vi of PEM version of canvas.iastate.edu certificate (base64 encode information)** (10 points)

```
-----BEGIN CERTIFICATE-----
MIIGpzCCBY+gAwIBAgIQBGq/qa7h5vS1nrfYjqDuHDANBgkqhkiG9w0BAQsFADBN
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMScwJQYDVQQDEx5E
aWdpQ2VydCBTSEEyIFNlY3VyZSBTZXJ2ZXIgQ0EwHhcNMjAwNjI2MDAwMDAwWhcN
MjIwNjMwMTIwMDAwWjByMQswCQYDVQQGEwJVUzENMAsGA1UECBMEVXRhaDEbMBkG
A1UEBxMSQ290dG9ud29vZCBIZWlnaHRzMRowGAYDVQQKExFJbnN0cnVjdHVyZSwg
SW5jLjEbMBkGA1UEAxMSY2FudmFzLmlhc3RhdGUuZWR1MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAvW6lHzRvIR6y9Pa+g5AcpK2oI3sX4VEsA9Ev7UGf
C6nKqlaTs99YbsjAjWW/u9sd9T/5QXmADmYY4mzrptaGxoAWOFlZWUDRd7MtlioC
Wkz5bBoAW4ydMd8lic6qT61e2gMcDDenGFOpg7qSpropIN+31M66avBlJ5/EjOB9
cObj08fThTvJ5AFl3TKpWgekcv7SzsoNIKjb0skz9CFWOPRpXvDasCZHMyd05x6O
9qPgRMnzoT9v44w3mGOS5lF4kY9jo5YOLdrjjIQI6GHp1Uzn1H1SfJ7kOTb56JFJ
75aJKPuxpsbBTadrNmSzcQ7w7+PgQmLGId7gJqugDvjzLwIDAQABo4IDXDCCA1gw
HwYDVR0jBBgwFoAUD4BhHIIxYdUvKOeNRji0LOHG2eIwHQYDVR0OBBYEFLU3BOrj
F9ycFfvKtMtnjSiQ5qPlMB0GA1UdEQQWMBSCEmNhbnZhcy5pYXN0YXRlLmVkdTAO
BgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMGsG
A1UdHwRkMGIwL6AtoCuGKWh0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9zc2NhLXNo
YTItZzYuY3JsMC+gLaArhilodHRwOi8vY3JsNC5kaWdpY2VydC5jb20vc3NjYS1z
aGEyLWc2LmNybDBMBgNVHSAERTBDMDcGCWCGSAGG/WwBATAqMCgGCCsGAQUFBwIB
FhxodHRwczovL3d3dy5kaWdpY2VydC5jb20vQ1BTMAgGBmeBDAECAjB8BggrBgEF
BQcBAQRwMG4wJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBG
BggrBgEFBQcwAoY6aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0
U0hBMlNlY3VyZVNlcnZlckNBLmNydDAMBgNVHRMBAf8EAjAAMIIBfwYKKwYBBAHW
eQIEAgSCAW8EggFrAWkAdwBGpVXrdfqRIDC1oolp9PN9ESxBdL79SbiFq/L8cP5t
RwAAAXLuMFCmAAAEAwBIMEYCIQC3St+w1Rabx6wTfs2d6/6mPss876rRFTJDSrMV
9NAApAIhAI1LsSYMC86w1Qw1M2/vsR1lxp1kZsL5A7nd3nun+p/hAHYAIkVFB1lV
JFaWP6Ev8fdthuAjJmOtwEt/XcaDXG7iDwIAAAFy7jBQggAABAMARzBFAiBBmTgE
5lrwccpg9KjH9NTUYyygMwZMXmih6nbWDAsL6AIhAM06T0xe8oeInX3UBiQppS44
2GCHKj/PhW6qTYa7JZJ4AHYAUaOw9f0BeZxWbbg3eI8MpHrMGyfL956IQpoN/tSL
BeUAAAFy7jBQ0AAABAMARzBFAiEAqnktZTlzC1s2fAWhp3Im9Yx48cZ9UEFX4ZFG
1RiYo90CIB4SnkgfxMvvwTz26hgJiexgk0BTY5xedDFPMpYDQ0U3MA0GCSqGSIb3
DQEBCwUAA4IBAQBl+dKUocHDSzQ87N7WXq+sMf5BBYPnjPs28i41KzEO8+QbD0mi
nYqHgVeRu9Wh1L5NzYkC96FIBKzAj5I1tRQMI66EenrgUyDBndURRgPX5CgAVV7O
7y4ogIxAgFk62NEmjh53uugn4IQRU9FX2Tr3xZdLe/p1zZ3cqweAWCoY3C2CmwNV
ZqyvFM0HlJN5k/Fkh+2jSJ0L/EoMnHPivFyU5x+lQTPswcNwFp7paMe+C8rAWWHt
CkLJ1g/Iw6kWlwNhjXxOb9MHY6+hL7jvF2Ewj4tqXdCqKGX5lmWrs1yX3RMkRfzF
IABoFZwwVImIQ5Sl7a8Y6yaPdunDpq50g+n9
-----END CERTIFICATE-----
```

9. **Screenshot of text information of canvas.iastate.edu certificate**
(5 points)

```
cpre331@desktop:~/Downloads$ openssl x509 -in canvas-iastate-edu.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:6a:bf:a9:ae:e1:e6:f4:b5:9e:b7:d8:8e:a0:ee:1c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = DigiCert Inc, CN = DigiCert SHA2 Secure Server CA
        Validity
            Not Before: Jun 26 00:00:00 2020 GMT
            Not After : Jun 30 12:00:00 2022 GMT
        Subject: C = US, ST = Utah, L = Cottonwood Heights, O = "Instructure, Inc.", CN = canvas.iastate.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bd:6e:a5:1f:34:6f:21:1e:b2:f4:f6:be:83:90:
                    1c:a4:ad:a8:23:7b:17:e1:51:2c:03:d1:2f:ed:41:
                    9f:0b:a9:ca:aa:56:93:b3:df:58:6e:c8:c0:8d:65:
                    bf:bb:db:1d:f5:3f:f9:41:79:80:0e:66:18:e2:6c:
                    eb:a6:d6:86:c6:80:16:38:59:59:59:40:d1:77:b3:
                    2d:96:2a:02:5a:4c:f9:6c:1a:00:5b:8c:9d:31:df:
                    25:89:ce:aa:4f:ad:5e:da:03:1c:0c:37:a7:18:53:
                    a9:83:ba:92:a6:ba:29:20:df:b7:d4:ce:ba:6a:f0:
                    65:27:9f:c4:8c:e0:7d:70:e6:e3:d3:c7:d3:85:3b:
                    c9:e4:01:65:dd:32:a9:5a:07:a4:72:fe:d2:ce:ca:
                    0d:20:a8:db:d2:c9:33:f4:21:56:38:f4:69:5e:f0:
                    da:b0:26:47:33:27:74:e7:1e:8e:f6:a3:e0:44:c9:
                    f3:a1:3f:6f:e3:8c:37:98:63:92:e6:51:78:91:8f:
                    63:a3:96:0e:2d:da:e3:8c:84:08:e8:61:e9:d5:4c:
                    e7:d4:7d:52:7c:9e:e4:39:36:f9:e8:91:49:ef:96:
                    89:28:fb:b1:a6:c6:c1:4d:a7:6b:36:64:b3:71:0e:
                    f0:ef:e3:e0:42:62:c6:21:de:e0:26:ab:a0:0e:f8:
                    f3:2f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:0F:80:61:1C:82:31:61:D5:2F:28:E7:8D:46:38:B4:2C:E1:C6:D9:E2

            X509v3 Subject Key Identifier:
                B5:37:04:EA:E3:17:DC:9C:15:FB:CA:B4:CB:67:8D:28:90:E6:A3:E5
            X509v3 Subject Alternative Name:
                DNS:canvas.iastate.edu
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
```

```
X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
X509v3 CRL Distribution Points:

    Full Name:
      URI:http://crl3.digicert.com/ssca-sha2-g6.crl

    Full Name:
      URI:http://crl4.digicert.com/ssca-sha2-g6.crl

X509v3 Certificate Policies:
    Policy: 2.16.840.1.114412.1.1
      CPS: https://www.digicert.com/CPS
    Policy: 2.23.140.1.2.2

Authority Information Access:
    OCSP - URI:http://ocsp.digicert.com
    CA Issuers - URI:http://cacerts.digicert.com/DigiCertSHA2SecureServerCA.crt

X509v3 Basic Constraints: critical
    CA:FALSE
CT Precertificate SCTs:
    Signed Certificate Timestamp:
        Version   : v1 (0x0)
        Log ID    : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
                    11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
        Timestamp : Jun 26 01:14:03.302 2020 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:46:02:21:00:B7:4A:DF:B0:D5:16:9B:C7:AC:13:7E:
                    CD:9D:EB:FE:A6:3E:CB:3C:EF:AA:D1:15:32:43:4A:B3:
                    15:F4:D0:00:A4:02:21:00:8D:4B:B1:26:0C:0B:CE:B0:
                    D5:0C:35:33:6F:EF:B1:1D:65:C6:9D:64:66:C2:F9:03:
                    B9:DD:DE:7B:A7:FA:9F:E1
    Signed Certificate Timestamp:
        Version   : v1 (0x0)
        Log ID    : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
                    E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
        Timestamp : Jun 26 01:14:03.266 2020 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:45:02:20:41:99:38:04:E6:5A:F0:71:CA:60:F4:A8:
                    C7:F4:D4:D4:63:2C:A0:33:06:4C:5E:68:A1:EA:76:D6:
                    0C:0B:0B:E8:02:21:00:CD:3A:4F:4C:5E:F2:87:88:9D:
                    7D:D4:06:24:29:A5:2E:38:D8:60:87:2A:3F:CF:85:6E:
                    AA:4D:86:BB:25:92:78
```

```
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 51:A3:B0:F5:FD:01:79:9C:56:6D:B8:37:78:8F:0C:A4:
                            7A:CC:1B:27:CB:F7:9E:88:42:9A:0D:FE:D4:8B:05:E5
                Timestamp : Jun 26 01:14:03.344 2020 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:45:02:21:00:AA:79:2D:65:39:73:0B:5B:36:7C:05:
                            A1:A7:72:26:F5:8C:78:F1:C6:7D:50:41:57:E1:91:46:
                            D5:18:98:A3:DD:02:20:1E:12:9E:48:1F:C4:CB:EF:C1:
                            3C:F6:EA:18:09:89:EC:60:93:40:53:63:9C:5E:74:31:
                            4F:32:96:03:43:45:37
    Signature Algorithm: sha256WithRSAEncryption
         65:f9:d2:94:a1:c1:c3:4b:34:3c:ec:de:d6:5e:af:ac:31:fe:
         41:05:83:e7:8c:fb:36:f2:2e:35:2b:31:0e:f3:e4:1b:0f:49:
         a2:9d:8a:87:81:57:91:bb:d5:a1:d4:be:4d:cd:89:02:f7:a1:
         48:04:ac:c0:8f:92:35:b5:14:0c:23:ae:84:7a:7a:e0:53:20:
         c1:9d:d5:11:46:03:d7:e4:28:00:55:5e:ce:ef:2e:28:80:8c:
         40:80:59:3a:d8:d1:26:8e:1e:77:ba:e8:27:e0:84:11:53:d1:
         57:d9:3a:f7:c5:97:4b:7b:fa:75:cd:9d:dc:ab:07:80:58:2a:
         18:dc:2d:82:9b:03:55:66:ac:af:14:cd:07:94:93:79:93:f1:
         64:87:ed:a3:48:9d:0b:fc:4a:0c:9c:73:e2:bc:5c:94:e7:1f:
         a5:41:33:ec:c1:c3:70:16:9e:e9:68:c7:be:0b:ca:c0:59:61:
         ed:0a:42:c9:d6:0f:c8:c3:a9:16:97:03:61:8d:7c:4e:6f:d3:
         07:63:af:a1:2f:b8:ef:17:61:30:8f:8b:6a:5d:d0:aa:28:65:
         f9:96:65:ab:b3:5c:97:dd:13:24:45:fc:c5:20:00:68:15:9c:
         30:54:89:88:43:94:a5:ed:af:18:eb:26:8f:76:e9:c3:a6:ae:
         74:83:e9:fd
```

10. **Screenshot of the SHA1 and SHA256 hashes of canvas.iastate.edu certificate, compare with fingerprints**
    (10 points)

```
cpre331@desktop:~/Downloads$ openssl x509 -in canvas-iastate-edu.pem -outform der -out canvas-iastate-edu.der
cpre331@desktop:~/Downloads$ sha1sum canvas-iastate-edu.der
4d82711939798bb9cbd922928fa72de77e8139ad  canvas-iastate-edu.der
cpre331@desktop:~/Downloads$ sha256sum canvas-iastate-edu.der
6b867323a038488b12c7651691b533c8a0ab9aec7900f186ea692d4513ad0a33  canvas-iastate-edu.der
cpre331@desktop:~/Downloads$
```