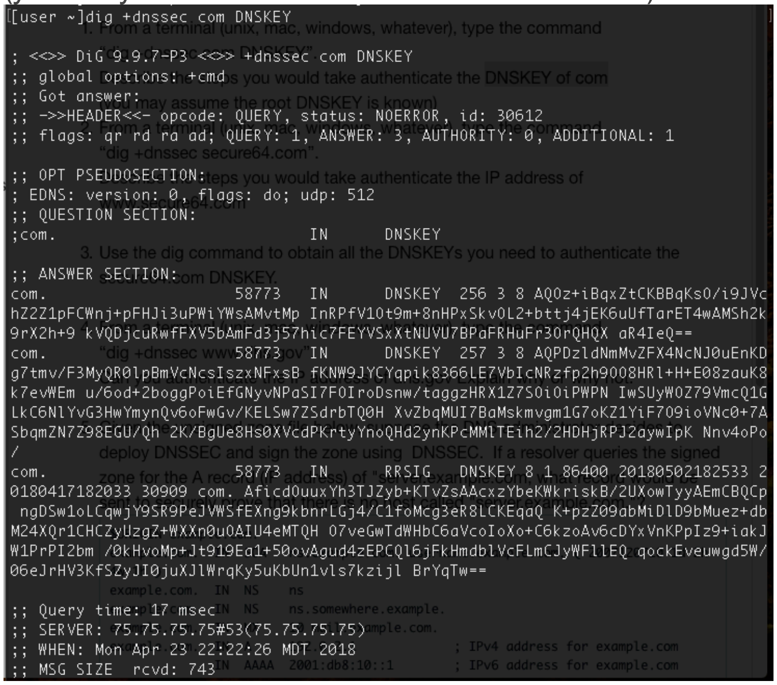
CSCI-3403 HW12
Chen Hao Cheng

Question not in the book:

1) From a terminal (unix, mac, windows, whatever), type the command “dig +dnssec com DNSKEY”. Describe the steps you would take authenticate the DNSKEY of com (you may assume the root DNSKEY is known)



```
[[user ~]dig +dnssec com DNSKEY

; <<>> DiG 9.9.7-P3 <<>> +dnssec com DNSKEY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30612
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;com.                           IN      DNSKEY

;; ANSWER SECTION:
com.                    58773   IN      DNSKEY  256 3 8 AQOz+iBqxZtCKBBqKs0/i9JVc
hZ2Z1pFCWnj+pFHJi3uPWiYWsAMvtMp InRPfV10t9m+8nHPxSkv0L2+bttj4jEK6uUfTarET4wAMSh2k
9rX2h+9 kVQDjcuRwfFXV5bAmFd3j57hic7FEYVSxXtNUVU7BPaFRHuFr30rQHQX aR4IeQ==
com.                    58773   IN      DNSKEY  257 3 8 AQPDzldNmMvZFX4NcNJ0uEnKD
g7tmv/F3MyQR0lpBmVcNcsIszxNFxsB fKNW9JYCYqpik8366LE7VbIcNRzfp2h9008HRl+H+E08zauK8
k7evWEm u/6od+2boggPoiEfGNyvNPaSI7F0IroDsnw/taggzHRX1Z7S0i0iPWPN IwSUyW0Z79VmcQ1G
LkC6NlYvG3HwYmynQv6oFwGv/KELSw7ZSdrbTQ0H XvZbqMUI7BaMskmvgm1G7oKZ1YiF709ioVNc0+7A
SbqmZN7Z98EGU/Qh 2K/BgUe8Hs0XVcdPKrtyYnoQHd2ynKPcMMlTEih2/2HDHjRPJ2aywIpK Nnv4oPo
/
com.                    58773   IN      RRSIG   DNSKEY 8 1 86400 20180502182533 2
0180417182033 30909 com. Aficd0uuxYh3TJZyb+KTvZsAAcxzYbeKWkriskB/2UXowTyyAEmCBQCp
 ngDSw1oLCqwjY9SR9PeJVWSfEXng9kbnrLGj4/C1foMcg3eR8LCKEqaQ K+pzZ09abMiDlD9bMuez+db
M24XQr1CHCZyUzgZ+WXXn0u0AIU4eMTQH 07veGwTdWHbC6aVcoIoXo+C6kzoAv6cDYxVnKPpIz9+iakJ
W1PrPI2bm /0kHvoMp+Jt919Ea1+50ovAgud4zEPCQl6jFkHmdblVcFLmCJyWFllEQ qockEveuwgd5W/
06eJrHV3KfSZyJI0juXJlWrqKy5uKbUn1vls7kzijl BrYqTw==

;; Query time: 17 msec
;; SERVER: 75.75.75.75#53(75.75.75.75)
;; WHEN: Mon Apr 23 22:22:26 MDT 2018
;; MSG SIZE  rcvd: 743
```

The QUESTION SECTION reaffirms what you went looking for – in this case, DIG went looking to an IPv4 address (DNSKEY layer/record) at .com.

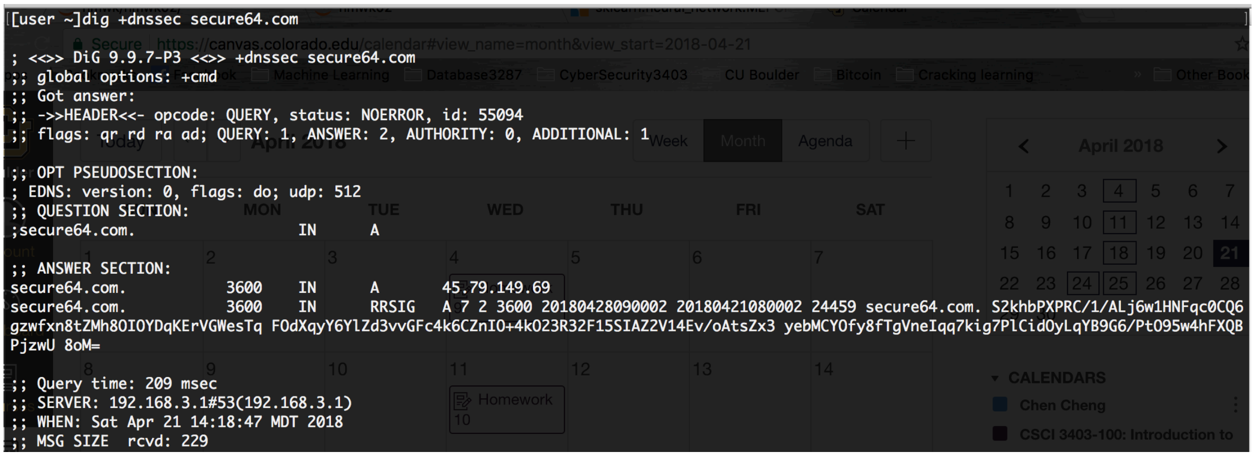
Query time shows how long it took to get the DNS response back from the server, which is listed on the next line.

DNSSEC is to add a layer of trust on top of DNS by providing authentication. When a DNS resolver is looking for some URL, the .com name servers help the resolver verify the records returned for cloudflare, and cloudflare helps verify the records returned for blog. The root DNS name servers help verify .com, and information published by the root is vetted by a thorough security procedure, including the Root Signing Ceremony.

Root Signing Ceremony - a rigorous procedure around signing the root DNS zone’s public keying information for the next few months. The private signing key used in this process is quite literally the key to the entire DNSSEC-protected Internet

DNSKEY holds the public key which resolvers use to verify. Public keys are stored in DNSKEY records inside of zone. To function key rollover, new keys are added ahead of time, while old keys remain in the zone until all entries have expired in the caches. the DNSKEY record is protected by an RRSIG, but this isn’t enough: The correctness of the DNSKEY record can be verified by the RRSIG, which can be verified by the DNSKEY! An additional mechanism to verify the DNSKEY is thus required. This is where the DS record comes in. It stores a summary of the DNSKEY in the *parent* zone, protected by the *parents* DNSKEY. This goes on in a tree-like structure, up to the root DNS zone. This root DNSKEY needs to be protected by some other means.

2) From a terminal (unix, mac, windows, whatever), type the command “dig +dnssec secure64.com”. Describe the steps you would take authenticate the IP address of www.secure64.com



```
[user ~]dig +dnssec secure64.com

; <<>> DiG 9.9.7-P3 <<>> +dnssec secure64.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55094
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;secure64.com.                  IN      A

;; ANSWER SECTION:
secure64.com.           3600    IN      A       45.79.149.69
secure64.com.           3600    IN      RRSIG   A 7 2 3600 20180428090002 20180421080002 24459 secure64.com. S2khbPXPRC/1/ALj6w1HNFqc0CQ6
gzwfxn8tZMh8OIOYDqKErVGWesTq FOdXqyY6YlZd3vvGFc4k6CZnIO+4kO23R32F15SIAZ2V14Ev/oAtsZx3 yebMCYOfy8fTgVneIqq7kig7PlCidOyLqYB9G6/PtO95w4hFXQB
PjzwU 8oM=

;; Query time: 209 msec
;; SERVER: 192.168.3.1#53(192.168.3.1)
;; WHEN: Sat Apr 21 14:18:47 MDT 2018
;; MSG SIZE  rcvd: 229
```

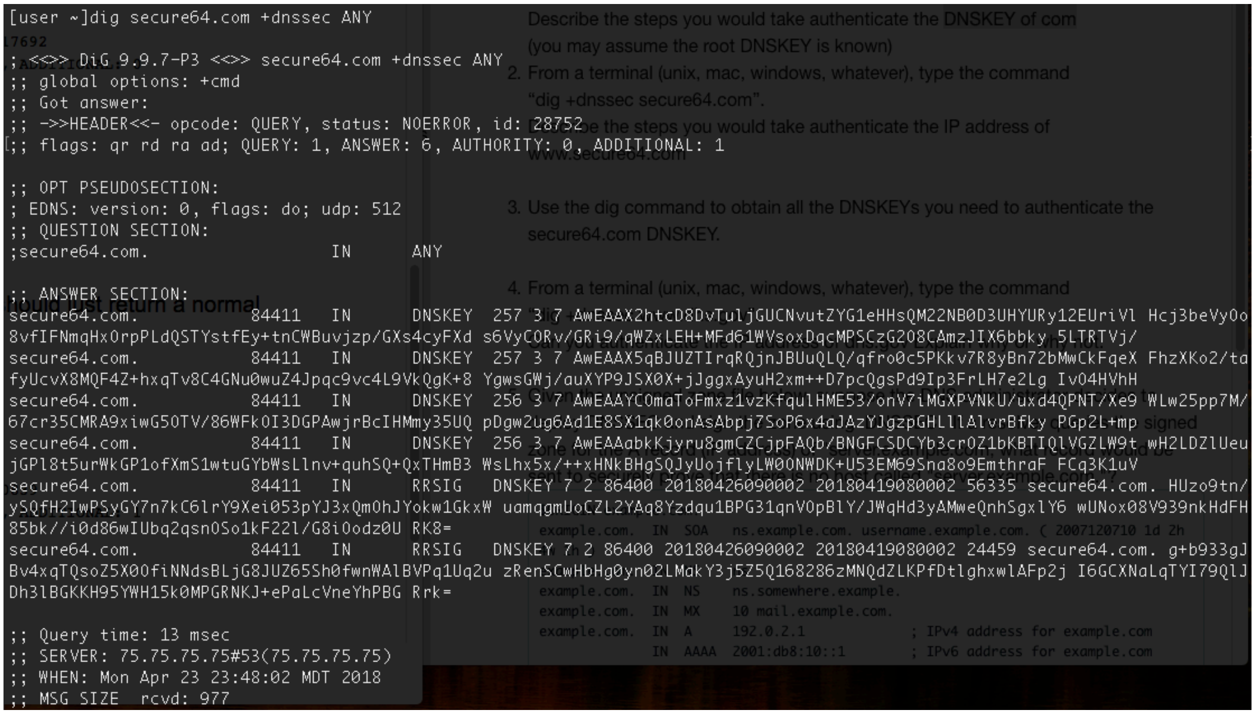
The QUESTION SECTION reaffirms what you went looking for – in this case, DIG went looking to an IPv4 address (A record) at 45.79.149.69

Query time shows how long it took to get the DNS response back from the server, which is listed on the next line.

DNSSEC is to add a layer of trust on top of DNS by providing authentication. When a DNS resolver is looking for some URL, the .com name servers help the resolver verify the records returned for cloudflare, and cloudflare helps verify the records returned for blog. The root DNS name servers help verify .com, and information published by the root is vetted by a thorough security procedure, including the Root Signing Ceremony.

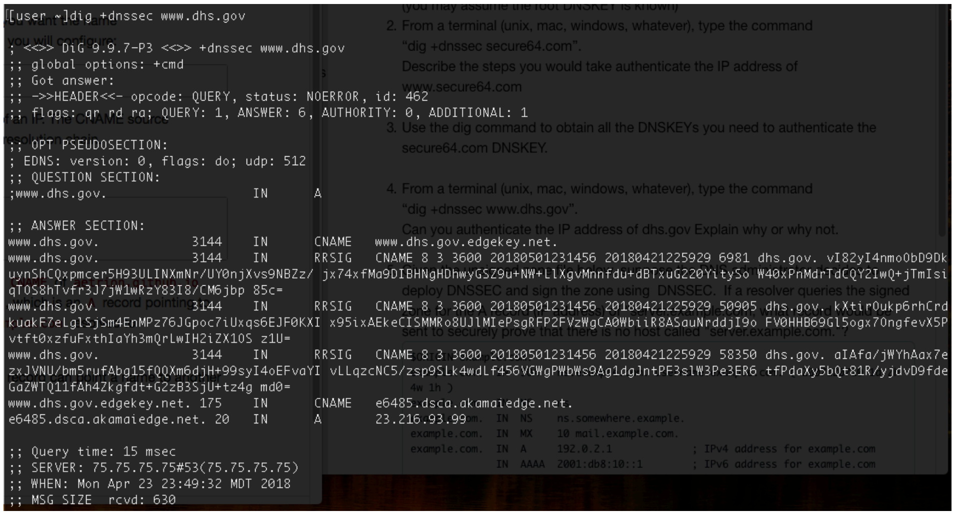
The server will send a request to cacheing resolver and ask for secure64.com., and cacheing resolver send to root(.), and the root reply to server, and the cacheing resolver will send the request to .com with DNSKEY, the DNSKEY holds the public key and .com will send back with DS and RRSIG record to verify.

3) Use the dig command to obtain all the DNSKEYs you need to authenticate the secure64.com DNSKEY.



```
[user ~]dig secure64.com +dnssec ANY

; <<>> DiG 9.9.7-P3 <<>> secure64.com +dnssec ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28752
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;secure64.com.                  IN      ANY

;; ANSWER SECTION:
secure64.com.           84411   IN      DNSKEY  257 3 7 AwEAAX2htcD8DvTuljGUCNvutZYG1eHHsQM22NB0D3UHYURy12EUriVl Hcj3beVy0o
8vfIFNmqHx0rpPLdQSTYstfEy+tnCWBuvjzp/GXs4cyFXd s6VyC0Rv/GRi9/qWZxLEH+MFd61WVsoxDqcMPSCzG208CAmzJIX6bbky 5LTRTVj/
secure64.com.           84411   IN      DNSKEY  257 3 7 AwEAAX5qBJUZTIrqRQjnJBUuQLQ/qfro0c5PKkv7R8yBn72bMwCkFqeX FhzXKo2/ta
fyUcvX8MQF4Z+hxqTv8C4GNu0wuZ4Jpqc9vc4L9VkQgK+8 YgwsGWj/auXYP9JSX0X+jJggxAyuH2xm++D7pcQgsPd9Ip3FrLH7e2Lg Iv04HVhH
secure64.com.           84411   IN      DNSKEY  256 3 7 AwEAAYC0maToFmxz1vzKfqulHME53/onV7iMGXPVNkU/uxd4QPNT/Xe9 WLw25pp7M/
67cr35CMRA9xiwG50TV/86WFk0I3DGPAwjrBcIHMmy35UQ pDgw2ug6Ad1E8SX1qk0onAsAbpj7SoP6x4aJAzYJgzpGHLllAlvrBfky PGp2L+mp
secure64.com.           84411   IN      DNSKEY  256 3 7 AwEAAabkKjyru8gmCZCjpFAQb/BNGFCSDCYb3cr0Z1bKBTIQlVGZLW9t wH2LDZlUeu
jGPl8t5urWkGP1ofXmS1wtuGYbWsLlnv+quhSQ+QxTHmB3 WsLhx5x/++xHNkBHgSQJyUojflyLW0ONWDK+U53EM69Sna8o9EmthraF FCq3K1uV
secure64.com.           84411   IN      RRSIG   DNSKEY 7 2 86400 20180426090002 20180419080002 56335 secure64.com. HUzo9tn/
ySQfH2IwPSyGY7n7kC6lrY9Xei053pYJ3xQm0hJYokw1GkxW uamqgmUoCZL2YAq8Yzdqu1BPG31qnV0pBlY/JWqHd3yAMweQnhSgxlY6 wUNox08V939nkHdFH
85bk//i0d86wIUbq2qsnOSo1kF22l/G8iOodz0U RK8=
secure64.com.           84411   IN      RRSIG   DNSKEY 7 2 86400 20180426090002 20180419080002 24459 secure64.com. g+b933gJ
Bv4xqTQsoZ5X0OfiNNdsBLjG8JUZ65Sh0fwnWAlBVPq1Uq2u zRenSCwHbHg0yn02LMakY3j5Z5Q168286zMNQdZLKPfDtlghxwlAFp2j I6GCXNaLqTYI79QlJ
Dh3lBGKKH95YWH15k0MPGRNKJ+ePaLcVneYhPBG Rrk=

;; Query time: 13 msec
;; SERVER: 75.75.75.75#53(75.75.75.75)
;; WHEN: Mon Apr 23 23:48:02 MDT 2018
;; MSG SIZE  rcvd: 977
```

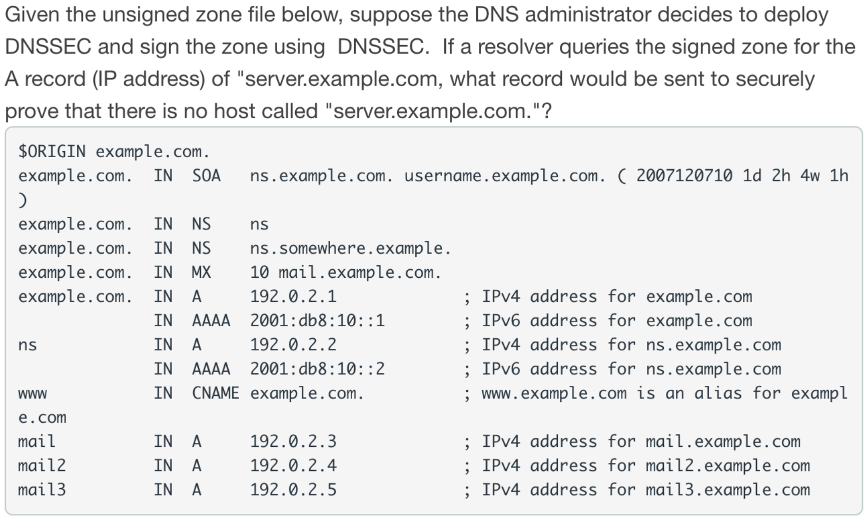
4) From a terminal (unix, mac, windows, whatever), type the command “dig +dnssec www.dhs.gov”. Can you authenticate the IP address of dhs.gov Explain why or why not.



```
[user ~]dig +dnssec www.dhs.gov

; <<>> DiG 9.9.7-P3 <<>> +dnssec www.dhs.gov
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 462
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;www.dhs.gov.                   IN      A

;; ANSWER SECTION:
www.dhs.gov.            3144    IN      CNAME   www.dhs.gov.edgekey.net.
www.dhs.gov.            3144    IN      RRSIG   CNAME 8 3 3600 20180501231456 20180421225929 6981 dhs.gov. vI82yI4nmo0bD9Dk
uynShCQxpmcer5H93ULINXmNr/UY0njXvs9NBZz/ jx74xfMa9DIBHNgHDhwyGSZ9u+NW+LlXgvMnnfdu+dBTxuG220YitySo W40xPnMdrTdCQY2IwQ+jTmIsi
qTOS8hTvfr3J7jW1wRzY83I8/CM6jbp 85c=
www.dhs.gov.            3144    IN      RRSIG   CNAME 8 3 3600 20180501231456 20180421225929 50905 dhs.gov. kXtirOukp6rhCrd
kuakF7eLglSjSm4EnMPz76JGpoc7iUxqs6EJF0KXI x95ixAEkeCISMMRo8UJlMIePsgRFP2FVzWgCA0WbiiR8ASauNrddjI9o FV0HHB69Gl5ogx70ngfevX5P
vtft0xzfuFxthIaYh3mQrLwIH2iZX10S z1U=
www.dhs.gov.            3144    IN      RRSIG   CNAME 8 3 3600 20180501231456 20180421225929 58350 dhs.gov. aIAfa/jWYhAax7e
zxJVNU/bm5rufAbg15fQQXm6djH+99syI4oEFvaYI vLLqzcNC5/zsp9SLk4wdLf456VGWgPWbWs9Ag1dgJntPF3slW3Pe3ER6 tfPdaXy5bQt81R/yjdvD9fde
GaZWTQ11fAh4Zkgfdt+G2zB3SjU+tz4g md0=
www.dhs.gov.edgekey.net. 175    IN      CNAME   e6485.dsca.akamaiedge.net.
e6485.dsca.akamaiedge.net. 20   IN      A       23.216.93.99

;; Query time: 15 msec
;; SERVER: 75.75.75.75#53(75.75.75.75)
;; WHEN: Mon Apr 23 23:49:32 MDT 2018
;; MSG SIZE  rcvd: 630
```

Yes, you can. We set www.dhs.gov as a CNAME of www.dhs.gov.edgekey.net, which in turns is itself a CNAME of dhs.gov 3 times and in turns is itself a CNAME of e6485.dsca.akamaiedge.net, which is an A record pointing to 23.216.93.99. Before sending back to 23.216.93.99, there is DNSEKY with public key.

5)



Given the unsigned zone file below, suppose the DNS administrator decides to deploy DNSSEC and sign the zone using DNSSEC. If a resolver queries the signed zone for the A record (IP address) of "server.example.com, what record would be sent to securely prove that there is no host called "server.example.com."?

```
$ORIGIN example.com.
example.com.  IN  SOA   ns.example.com. username.example.com. ( 2007120710 1d 2h 4w 1h
)
example.com.  IN  NS    ns
example.com.  IN  NS    ns.somewhere.example.
example.com.  IN  MX    10 mail.example.com.
example.com.  IN  A     192.0.2.1             ; IPv4 address for example.com
              IN  AAAA  2001:db8:10::1        ; IPv6 address for example.com
ns            IN  A     192.0.2.2             ; IPv4 address for ns.example.com
              IN  AAAA  2001:db8:10::2        ; IPv6 address for ns.example.com
www           IN  CNAME example.com.          ; www.example.com is an alias for exampl
e.com
mail          IN  A     192.0.2.3             ; IPv4 address for mail.example.com
mail2         IN  A     192.0.2.4             ; IPv4 address for mail2.example.com
mail3         IN  A     192.0.2.5             ; IPv4 address for mail3.example.com
```

Since there no ‘server.example.com’ so NSEC record should be sent to securely prove that there is no host called “server.example.com.”.

Review Question Chapter 23

23.9)

What is a public key infrastructure (PKI)?

An asymmetric cryptographic based digital signatures which store, revoke, create, manage and distribute to a set of people, software, hardware, procedures and policies are called as public-key infrastructure.

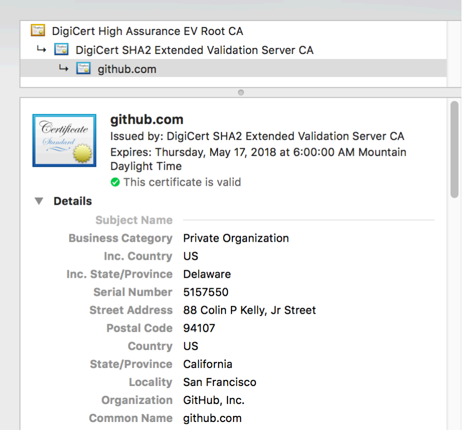
- The combination of public-key encryption and digital signature service is known as PKI
- Enabling a secure , convenient, and efficient acquisition of public key is the principal objective for developing a PKI

<u>Problems Chapter 23</u>

23.3)

a)

Owner name: Github is an organization so it’s owned by Github, Inc.



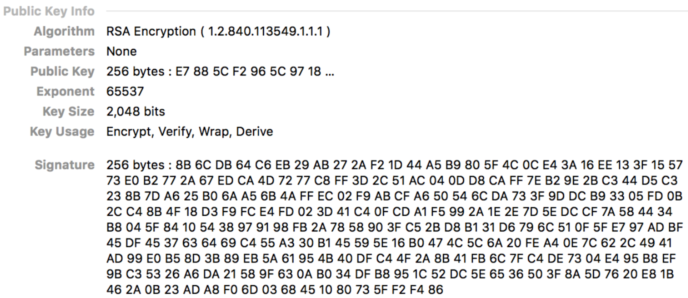
DigiCert High Assurance EV Root CA
↳ DigiCert SHA2 Extended Validation Server CA
↳ github.com

github.com
Issued by: DigiCert SHA2 Extended Validation Server CA
Expires: Thursday, May 17, 2018 at 6:00:00 AM Mountain Daylight Time
This certificate is valid

▼ **Details**

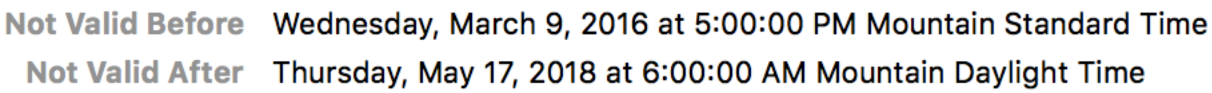
Subject Name	
Business Category	Private Organization
Inc. Country	US
Inc. State/Province	Delaware
Serial Number	5157550
Street Address	88 Colin P Kelly, Jr Street
Postal Code	94107
Country	US
State/Province	California
Locality	San Francisco
Organization	GitHub, Inc.
Common Name	github.com

Public key:

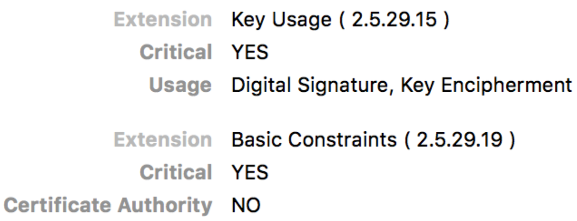


Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes : E7 88 5C F2 96 5C 97 18 …
Exponent	65537
Key Size	2,048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	256 bytes : 8B 6C DB 64 C6 EB 29 AB 27 2A F2 1D 44 A5 B9 80 5F 4C 0C E4 3A 16 EE 13 3F 15 57 73 E0 B2 77 2A 67 ED CA 4D 72 77 C8 FF 3D 2C 51 AC 04 0D D8 CA FF 7E B2 9E 2B C3 44 D5 C3 23 8B 7D A6 25 B0 6A A5 6B 4A FF EC 02 F9 AB CF A6 50 54 6C DA 73 3F 9D DC B9 33 05 FD 0B 2C C4 8B 4F 18 D3 F9 FC E4 FD 02 3D 41 C4 0F CD A1 F5 99 2A 1E 2E 7D 5E DC CF 7A 58 44 34 B8 04 5F 84 10 54 38 97 91 98 FB 2A 78 58 90 3F C5 2B D8 B1 31 D6 79 6C 51 0F 5F E7 97 AD BF 45 DF 45 37 63 64 69 C4 55 A3 30 B1 45 59 5E 16 B0 47 4C 5C 6A 20 FE A4 0E 7C 62 2C 49 41 AD 99 E0 B5 8D 3B 89 EB 5A 61 95 4B 40 DF C4 4F 2A 8B 41 FB 6C 7F C4 DE 73 04 E4 95 B8 EF 9B C3 53 26 A6 DA 21 58 9F 63 0A B0 34 DF B8 95 1C 52 DC 5E 65 36 50 3F 8A 5D 76 20 E8 1B 46 2A 0B 23 AD A8 F0 6D 03 68 45 10 80 73 5F F2 F4 86

Validate date:

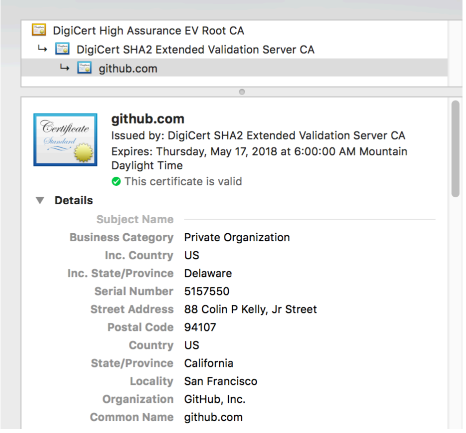


Not Valid Before	Wednesday, March 9, 2016 at 5:00:00 PM Mountain Standard Time
Not Valid After	Thursday, May 17, 2018 at 6:00:00 AM Mountain Daylight Time



Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Digital Signature, Key Encipherment
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO

CA: In above picture, it shows there is no CA, but if we look at the follow picture, the CA is



DigiCert High Assurance EV Root CA
↳ DigiCert SHA2 Extended Validation Server CA
↳ github.com

github.com
Issued by: DigiCert SHA2 Extended Validation Server CA
Expires: Thursday, May 17, 2018 at 6:00:00 AM Mountain Daylight Time
✓ This certificate is valid

▼ **Details**

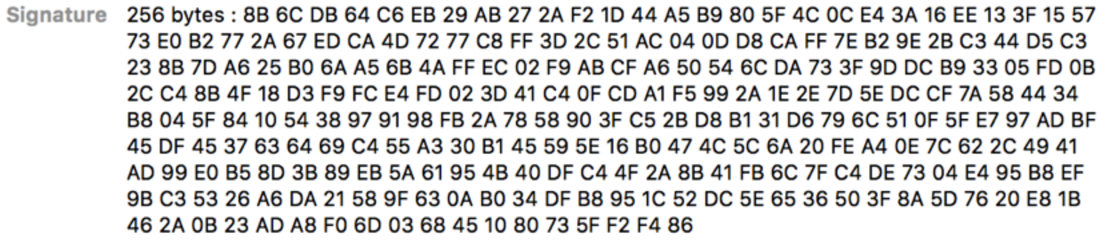
Subject Name	
Business Category	Private Organization
Inc. Country	US
Inc. State/Province	Delaware
Serial Number	5157550
Street Address	88 Colin P Kelly, Jr Street
Postal Code	94107
Country	US
State/Province	California
Locality	San Francisco
Organization	GitHub, Inc.
Common Name	github.com

DigiCert SHA2 Extended Validation Server CA

Type of signature:

RSA algorithm with 2048 bits

Value of signature:

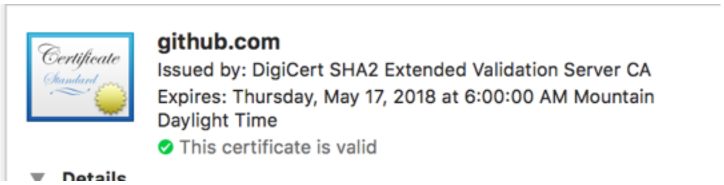


```
Signature  256 bytes : 8B 6C DB 64 C6 EB 29 AB 27 2A F2 1D 44 A5 B9 80 5F 4C 0C E4 3A 16 EE 13 3F 15 57
           73 E0 B2 77 2A 67 ED CA 4D 72 77 C8 FF 3D 2C 51 AC 04 0D D8 CA FF 7E B2 9E 2B C3 44 D5 C3
           23 8B 7D A6 25 B0 6A A5 6B 4A FF EC 02 F9 AB CF A6 50 54 6C DA 73 3F 9D DC B9 33 05 FD 0B
           2C C4 8B 4F 18 D3 F9 FC E4 FD 02 3D 41 C4 0F CD A1 F5 99 2A 1E 2E 7D 5E DC CF 7A 58 44 34
           B8 04 5F 84 10 54 38 97 91 98 FB 2A 78 58 90 3F C5 2B D8 B1 31 D6 79 6C 51 0F 5F E7 97 AD BF
           45 DF 45 37 63 64 69 C4 55 A3 30 B1 45 59 5E 16 B0 47 4C 5C 6A 20 FE A4 0E 7C 62 2C 49 41
           AD 99 E0 B5 8D 3B 89 EB 5A 61 95 4B 40 DF C4 4F 2A 8B 41 FB 6C 7F C4 DE 73 04 E4 95 B8 EF
           9B C3 53 26 A6 DA 21 58 9F 63 0A B0 34 DF B8 95 1C 52 DC 5E 65 36 50 3F 8A 5D 76 20 E8 1B
           46 2A 0B 23 AD A8 F0 6D 03 68 45 10 80 73 5F F2 F4 86
```

b) State whether this is a CA or end-user certificate, and why

This is a CA because it's issued by DigCert SHA2 Extended Validation Server CA

c) Indicate whether the certificate is valid or not, and why



github.com
Issued by: DigiCert SHA2 Extended Validation Server CA
Expires: Thursday, May 17, 2018 at 6:00:00 AM Mountain Daylight Time
✓ This certificate is valid

▼ **Details**

The certificate is valid, see the picture and it's not expired.

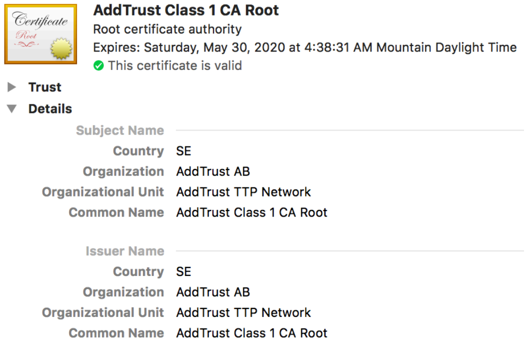
d) State whether there are any other obvious problems with the algorithm used in this certificate

There is no problems because it is no longer to use SHA1 nowadays issuing by the government. The 2048 bits long field is a container for the results of the hash function.

23.4)

a) Identify the key elements in this certificate, including owner's name and public key, its validity dates, the name of the CA that signed it, and the type and value of signature.

Owner's name: This is same as the same name organization as AddTrust AB



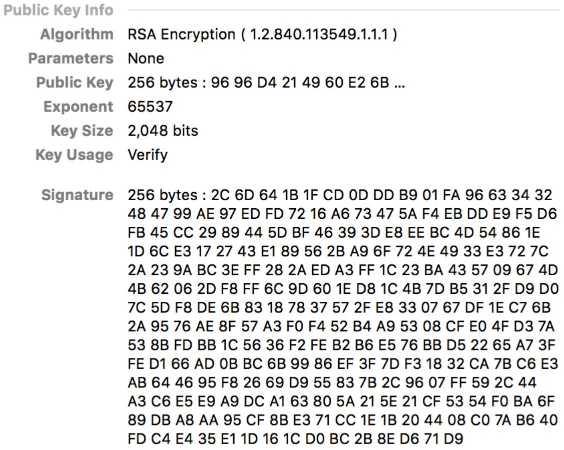
AddTrust Class 1 CA Root
Root certificate authority
Expires: Saturday, May 30, 2020 at 4:38:31 AM Mountain Daylight Time
✓ This certificate is valid

▶ Trust
▼ Details

Subject Name
Country SE
Organization AddTrust AB
Organizational Unit AddTrust TTP Network
Common Name AddTrust Class 1 CA Root

Issuer Name
Country SE
Organization AddTrust AB
Organizational Unit AddTrust TTP Network
Common Name AddTrust Class 1 CA Root

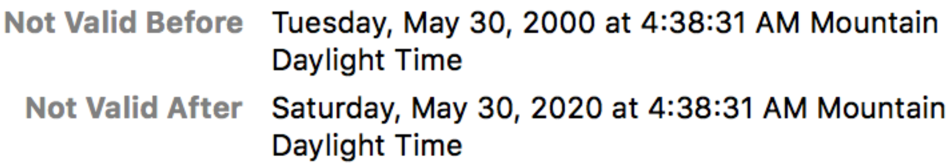
Public-key:



Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters None
Public Key 256 bytes : 96 96 D4 21 49 60 E2 6B ...
Exponent 65537
Key Size 2,048 bits
Key Usage Verify

```
Signature 256 bytes : 2C 6D 64 1B 1F CD 0D DD B9 01 FA 96 63 34 32
          48 47 99 AE 97 ED FD 72 16 A6 73 47 5A F4 EB DD E9 F5 D6
          FB 45 CC 29 89 44 5D BF 46 39 3D E8 EE BC 4D 54 86 1E
          1D 6C E3 17 27 43 E1 89 56 2B A9 6F 72 4E 49 33 E3 72 7C
          2A 23 9A BC 3E FF 28 2A ED A3 FF 1C 23 BA 43 57 09 67 4D
          4B 62 06 2D F8 FF 6C 9D 60 1E D8 1C 4B 7D B5 31 2F D9 D0
          7C 5D F8 DE 6B 83 18 78 37 57 2F E8 33 07 67 DF 1E C7 6B
          2A 95 76 AE 8F 57 A3 F0 F4 52 B4 A9 53 08 CF E0 4F D3 7A
          53 8B FD BB 1C 56 36 F2 FE B2 B6 E5 76 BB D5 22 65 A7 3F
          FE D1 66 AD 0B BC 6B 99 86 EF 3F 7D F3 18 32 CA 7B C6 E3
          AB 64 46 95 F8 26 69 D9 55 83 7B 2C 96 07 FF 59 2C 44
          A3 C6 E5 E9 A9 DC A1 63 80 5A 21 5E 21 CF 53 54 F0 BA 6F
          89 DB A8 AA 95 CF 8B E3 71 CC 1E 1B 20 44 08 C0 7A B6 40
          FD C4 E4 35 E1 1D 16 1C D0 BC 2B 8E D6 71 D9
```

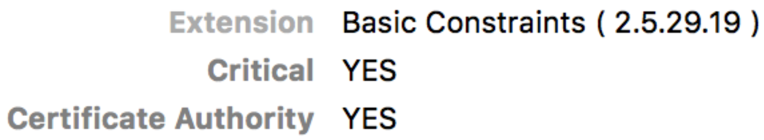
Validity dates:



Not Valid Before Tuesday, May 30, 2000 at 4:38:31 AM Mountain Daylight Time

Not Valid After Saturday, May 30, 2020 at 4:38:31 AM Mountain Daylight Time

CA:



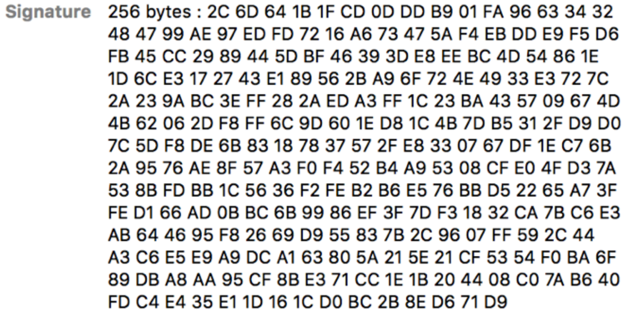
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES

It is also Root Certificate Authority

Type of signature:

RSA Encryption with 2048 bits

Value of signature:

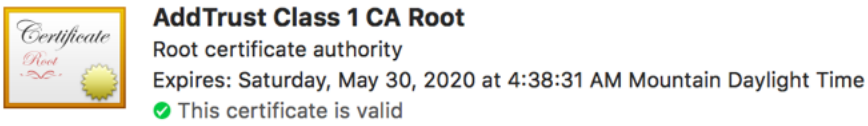


```
Signature   256 bytes : 2C 6D 64 1B 1F CD 0D DD B9 01 FA 96 63 34 32
            48 47 99 AE 97 ED FD 72 16 A6 73 47 5A F4 EB DD E9 F5 D6
            FB 45 CC 29 89 44 5D BF 46 39 3D E8 EE BC 4D 54 86 1E
            1D 6C E3 17 27 43 E1 89 56 2B A9 6F 72 4E 49 33 E3 72 7C
            2A 23 9A BC 3E FF 28 2A ED A3 FF 1C 23 BA 43 57 09 67 4D
            4B 62 06 2D F8 FF 6C 9D 60 1E D8 1C 4B 7D B5 31 2F D9 D0
            7C 5D F8 DE 6B 83 18 78 37 57 2F E8 33 07 67 DF 1E C7 6B
            2A 95 76 AE 8F 57 A3 F0 F4 52 B4 A9 53 08 CF E0 4F D3 7A
            53 8B FD BB 1C 56 36 F2 FE B2 B6 E5 76 BB D5 22 65 A7 3F
            FE D1 66 AD 0B BC 6B 99 86 EF 3F 7D F3 18 32 CA 7B C6 E3
            AB 64 46 95 F8 26 69 D9 55 83 7B 2C 96 07 FF 59 2C 44
            A3 C6 E5 E9 A9 DC A1 63 80 5A 21 5E 21 CF 53 54 F0 BA 6F
            89 DB A8 AA 95 CF 8B E3 71 CC 1E 1B 20 44 08 C0 7A B6 40
            FD C4 E4 35 E1 1D 16 1C D0 BC 2B 8E D6 71 D9
```

b) State whether this is a CA or end-user certificate, and why

End-user certificate because this is from root of local machine. It's not issued by the government

c) Indicate whether the certificate is valid or not, and why



AddTrust Class 1 CA Root

Root certificate authority

Expires: Saturday, May 30, 2020 at 4:38:31 AM Mountain Daylight Time

✓ This certificate is valid

It shows the certificate is valid and it's not expired

d) State whether there are any other obvious problems with the algorithm used in this certificate

Even if there is a RSA algorithm but there is no SHA2