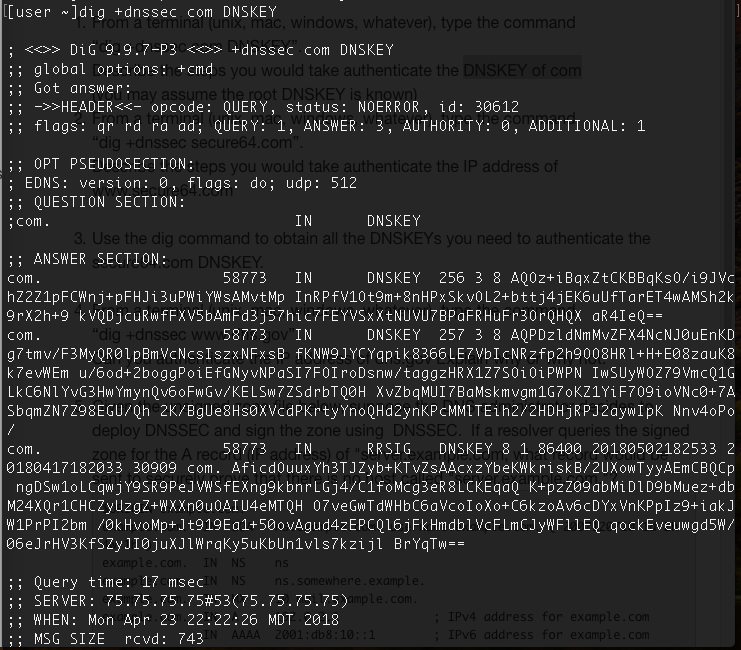
CSCI-3403 HW12

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)



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

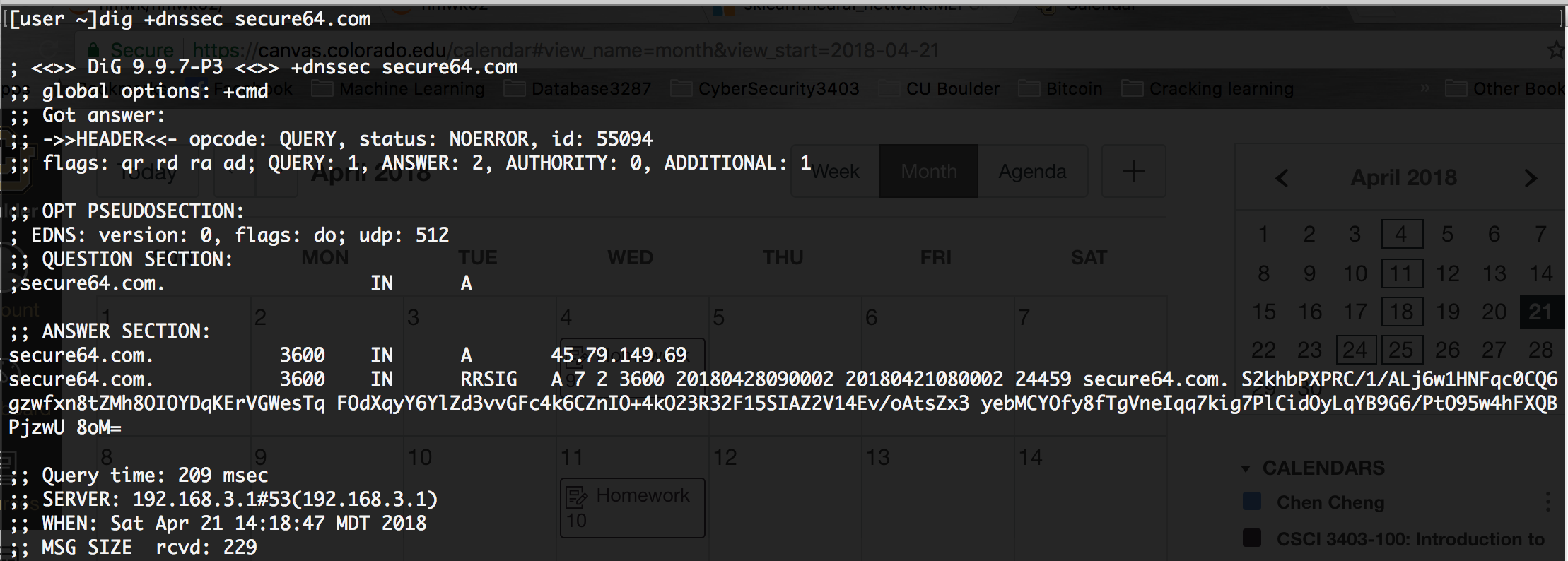
Query time shows how long it took to get the DNS response back from the server, which is listed on the next line.

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



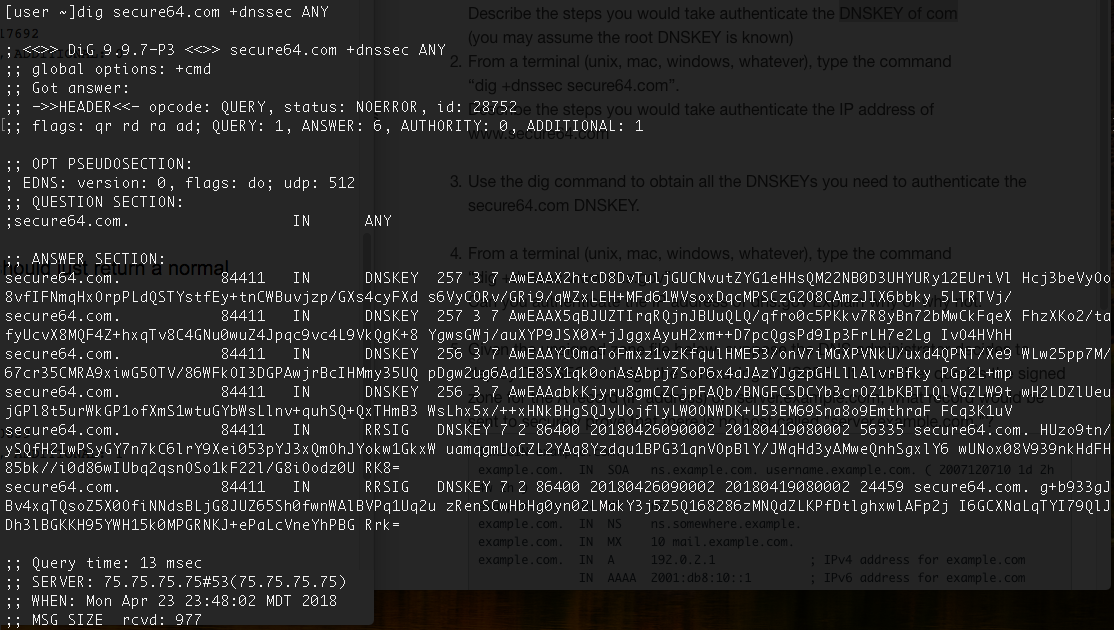
The QUESTION SECTION reaffirms what you went looking for – in this case, DIG went looking to an IPv4 address (A record) at 45.79.149.69

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

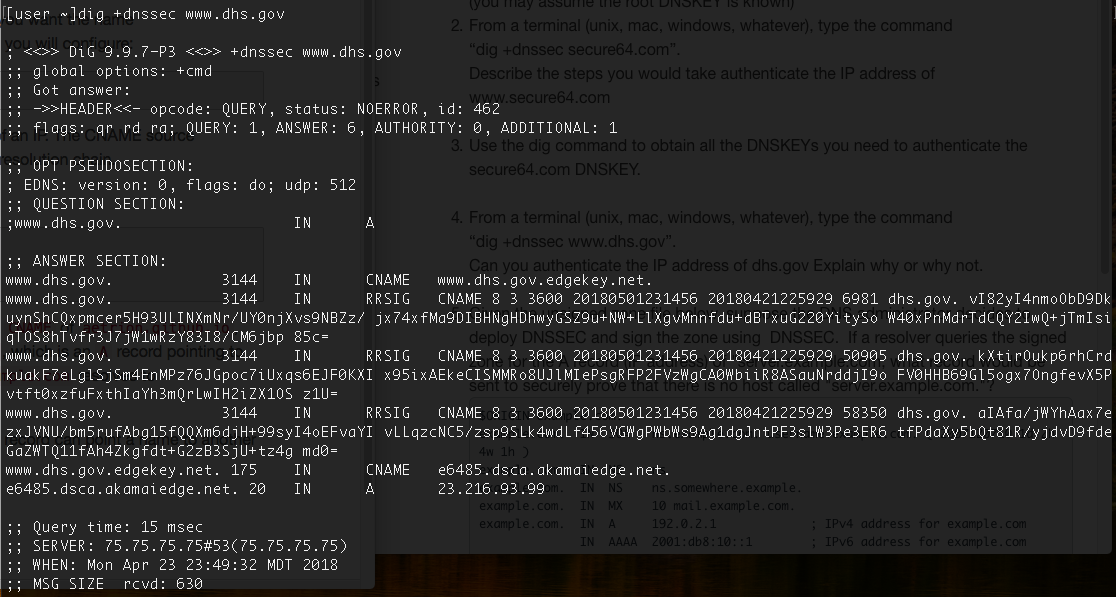
DNSSEC is to add a layer of trust on top of DNS by providing authentication. When a DNS resolver is looking for some URL, the .com name servers help the resolver verify the records returned for cloudflare, and cloudflare helps verify the records returned for blog. The root DNS name servers help verify .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.

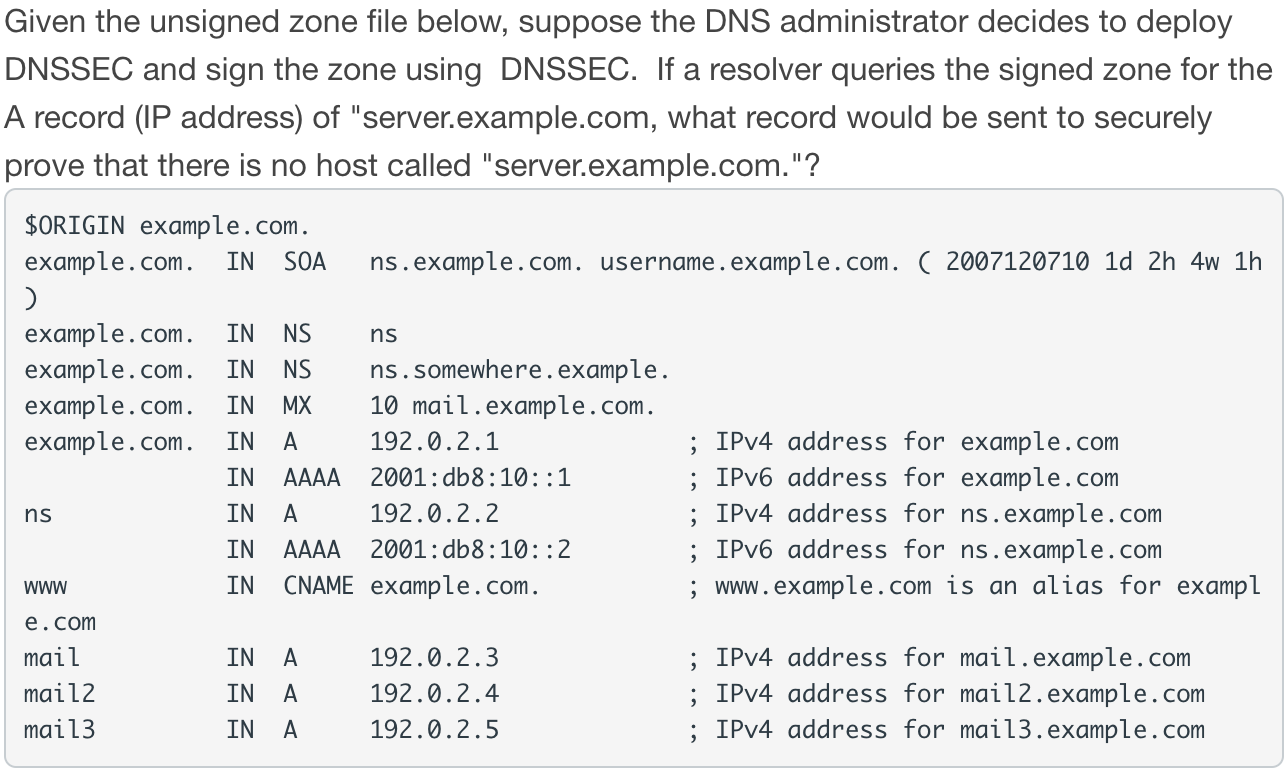


4) From a terminal (unix, mac, windows, whatever), type the command “dig +dnssec www.dhs.gov”. Can you authenticate the IP address of dhs.gov Explain why or why not.



Yes, you can. We set [www.dhs.gov](http://www.dhs.gov) as a CNAME of [www.dhs.gov.edgekey.net](http://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)



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.

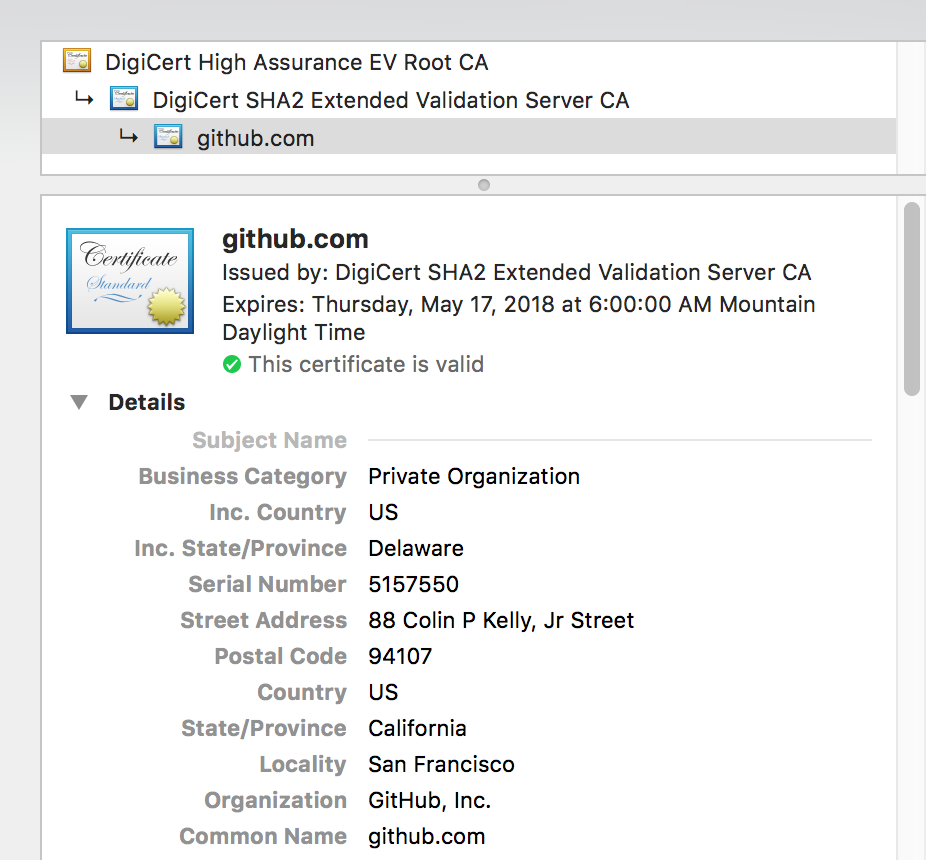
* The combination of public-key encryption and digital signature service is known as PKI
* Enabling a secure , convenient, and efficient acquisition of public key is the principal objective for developing a PKI

Problems Chapter 23

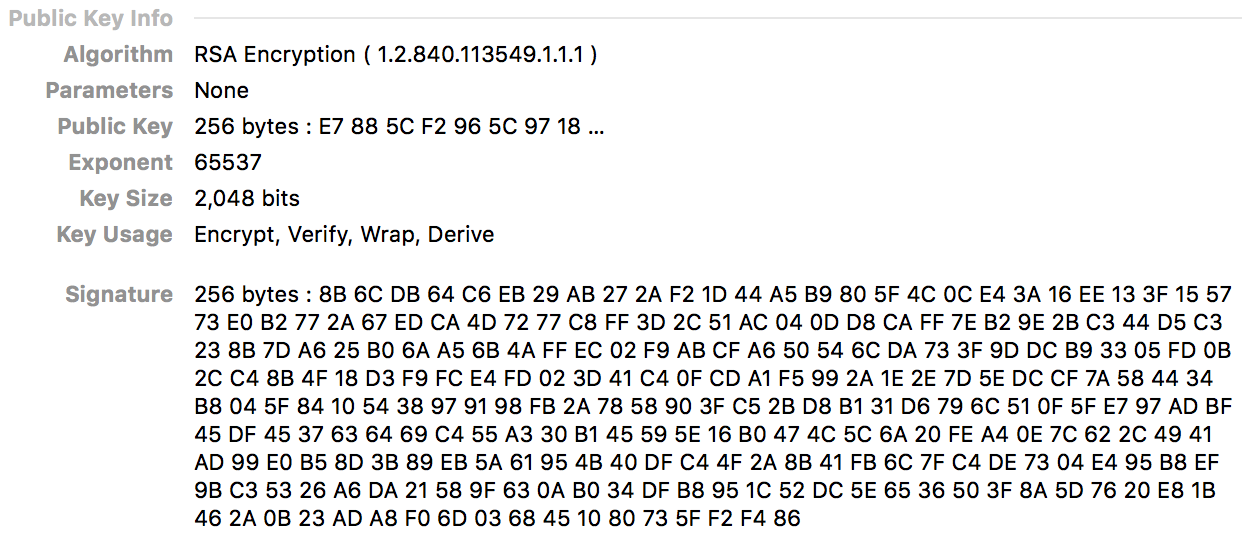
23.3)

a)

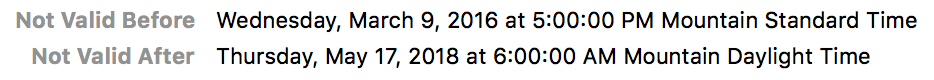
Owner name: Github is an organization so it’s owned by Github, Inc.

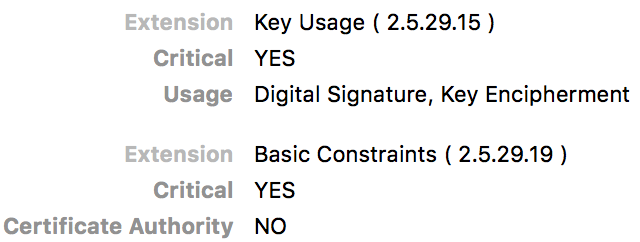


Public key:

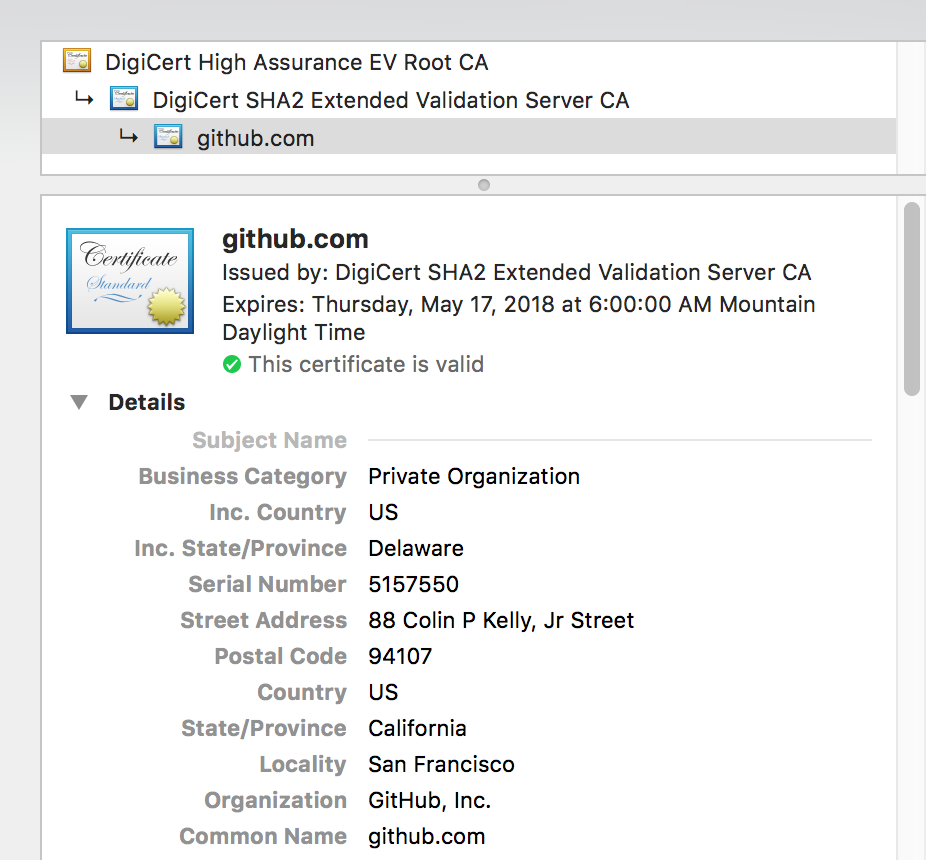


Validate date:





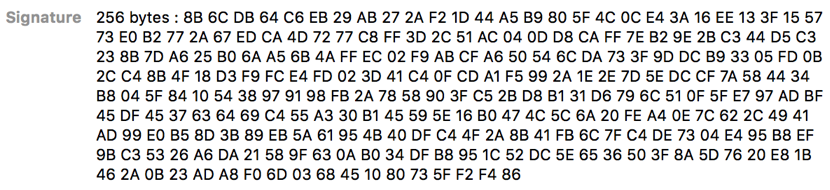
CA: In above picture, it shows there is no CA, but if we look at the follow picture, the CA is

 DigiCert SHA2 Extended Validation Server CA

Type of signature:

RSA algorithm with 2048 bits

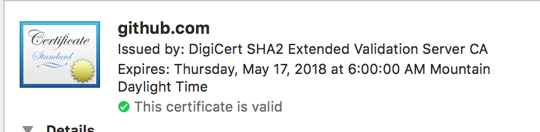
Value of signature:



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



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

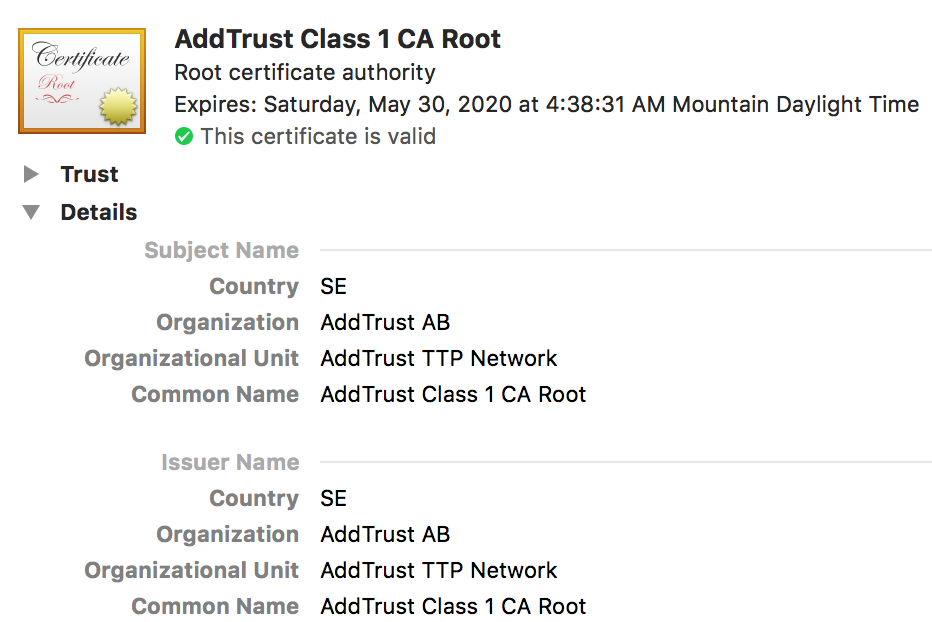
d) State whether there are any other obvious problems with the algorithm used in this certificate

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.

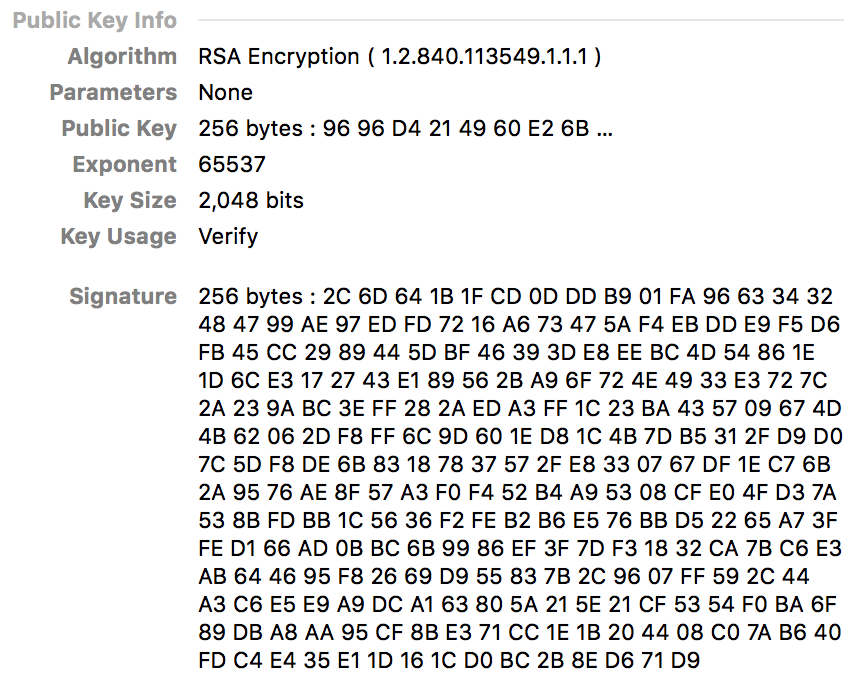
23.4)

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.

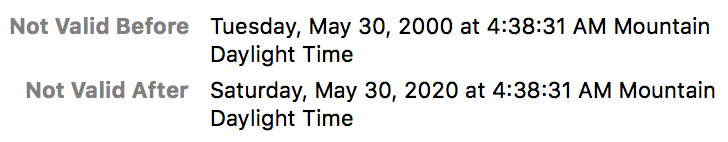
Owner’s name: This is same as the same name organization as AddTrust AB



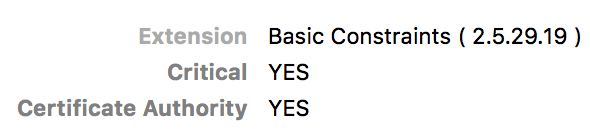
Public-key:



Validity dates:



CA:

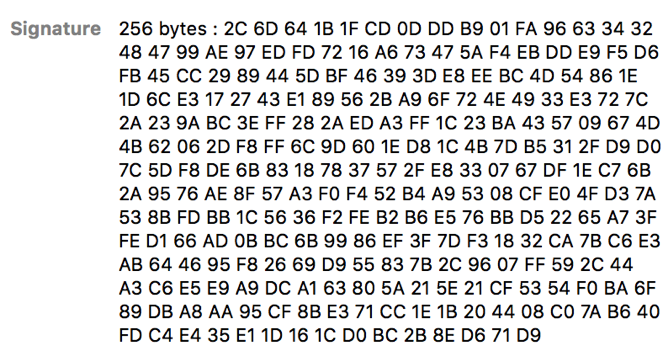


It is also Root Certificate Authority

Type of signature:

RSA Encryption with 2048 bits

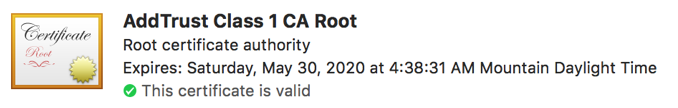
Value of signature:



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



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