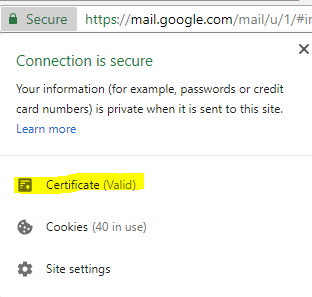
# Cryptography Homework 9: Digital Certificates

## Inspecting Certificates

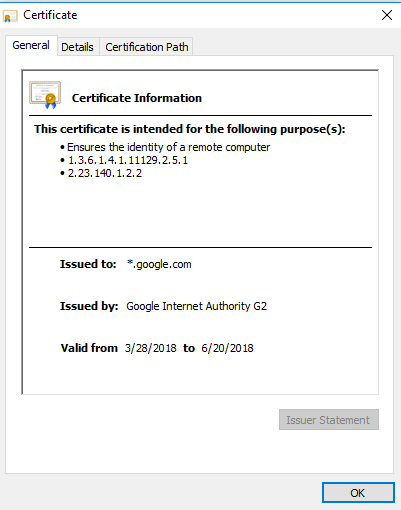
Download certificates from two web sites using the following instructions.

### Chrome

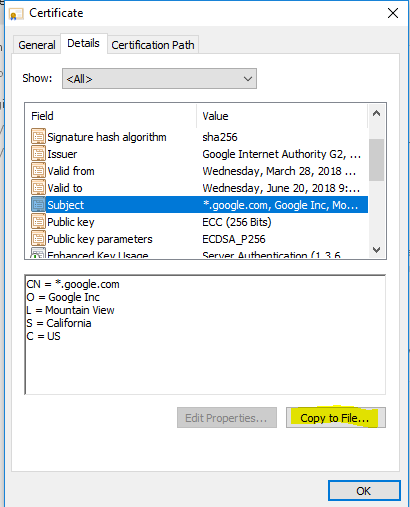
Chrome does not keep its own copy of certificates. Instead it uses the Microsoft Windows certificate store. The lock icon in the navigation bar displays certificate information.



Clicking on Certificate opens the Microsoft certificate dialog box.



The details tab allows you to view the contents of the certificate, and to download a copy.

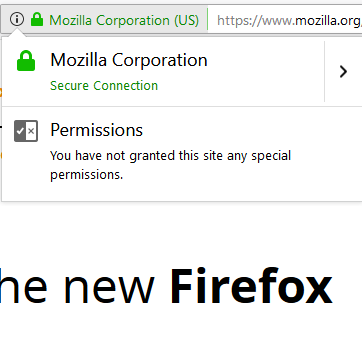
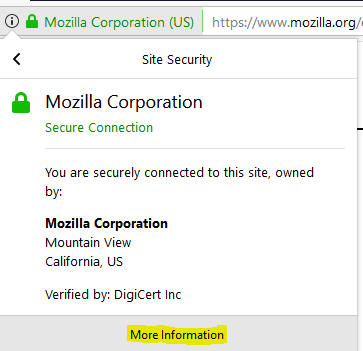


Copy the certificate to your desktop. Be sure to save the certificate in Base-64 encoded X.509 so that we can read it in Linux later on.

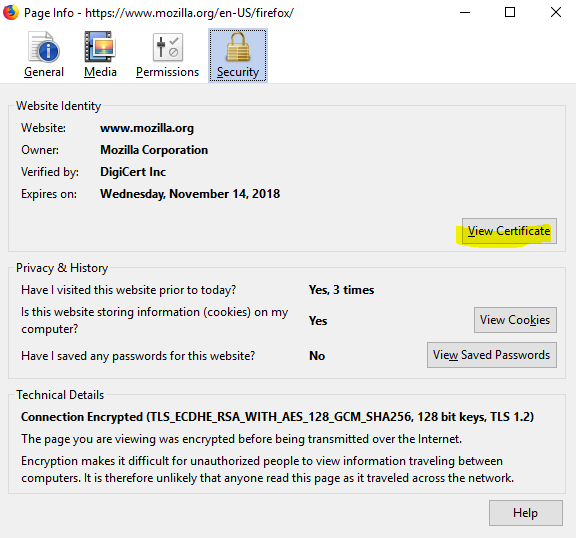
Also note the Certification Path tab. It shows the chain of certificates that leads to a root certificate authority (CA), assuming the certificate is valid. The CA must be trusted by your browser/operating system for the certificate to be listed as OK.

### Firefox

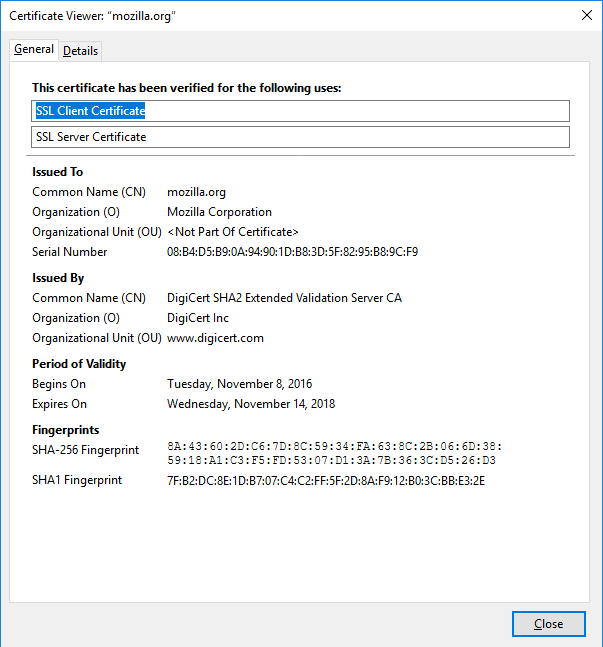
Firefox maintains its own certificate store. Therefore, the dialog boxes look slightly different. Select the lock icon in the browser navigation bar, then select More Information.

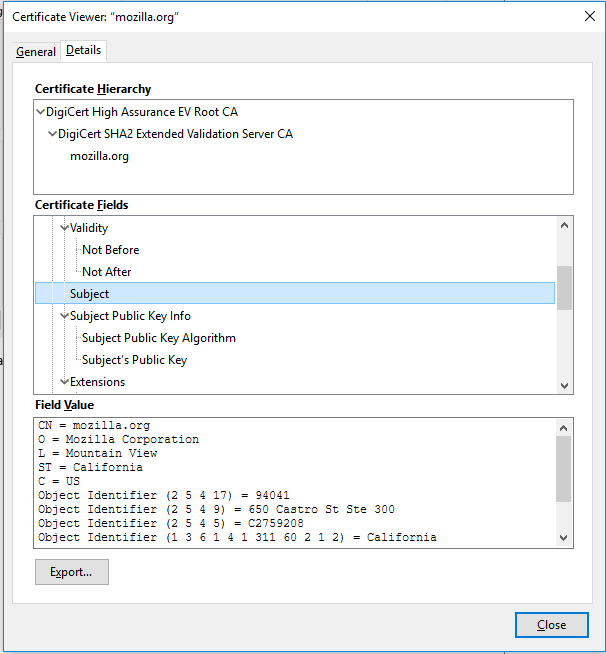
 

The dialog box shows web site information and allows you to save the certificate.



The Certificate Viewer shows detailed information about the certificate and allows you to export (save a copy) the certificate.



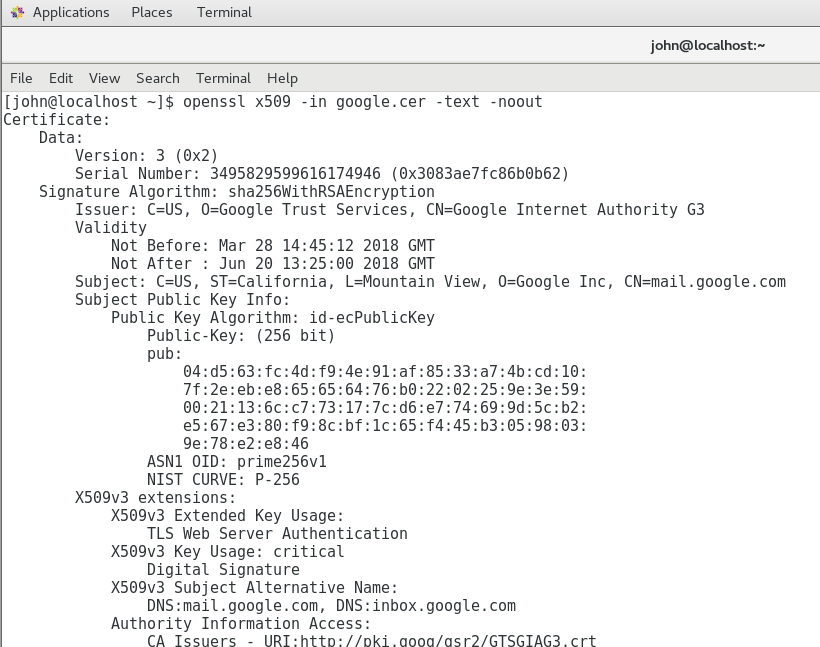


Note: Firefox maintains its own certificate store, separate from the Windows certificate store.

## Viewing Certificate Details with openssl

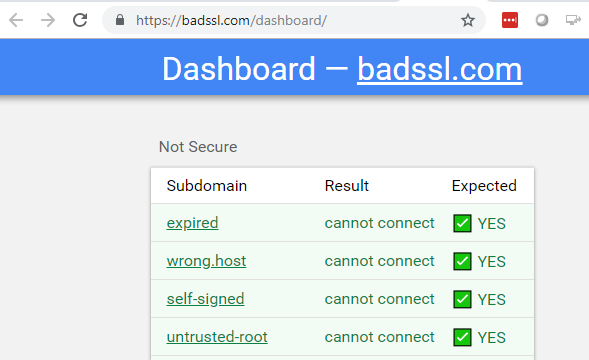
Linux usually has openssl installed by default. It displays the contents of certificates with this command:  
openssl x509 -in google.cer -text -noout

This command says that the certificate follows the X509 format, the input file is google.cer, we want text output to the screen, and we won’t be saving any files or modified versions of the certificate.



Copy one of the certificates you saved to your Linux VM and examine it with openssl.

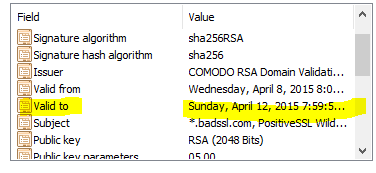
## Bad certificates--Hand in

The URL, <https://badssl.com/dashboard/>, allows you to examine several bad certificates.  


You should be able to tell what is wrong with the certificate by the title of the link you click on. The “expired” link has an expired cert. Therefore, click on each link, examine the certificate, and submit a screenshot of the part that you think is failing.

### Expired Certificate

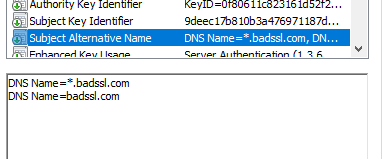
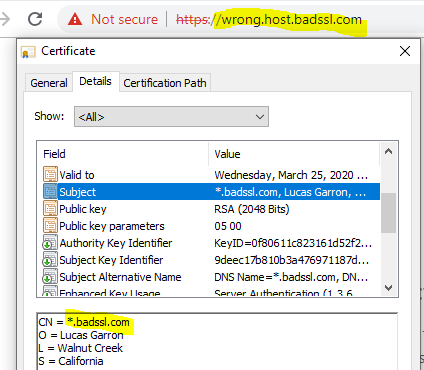
You should be able to find a problem with the valid dates in the Details tab of the Microsoft Certificate Window.

The certificate expired in 2015  


### Wrong Host

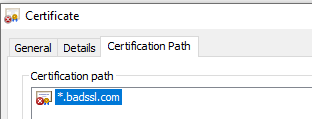
For this one you’ll need to look at the browser navigation bar, the Subject, and Subject Alternative Name of the certificate. Note: \*.whoops.ssl works for any letters “x” in xxx.whoops.ssl. It does not work for morestuff.xxx.whoops.ssl.

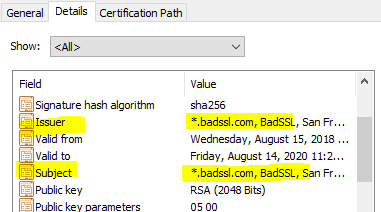
The certificate is for \*.badssl.com. host.badssl.com will pass, but wrong.host.badssl.com will not.



### Self-signed

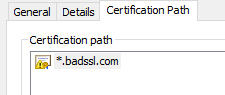
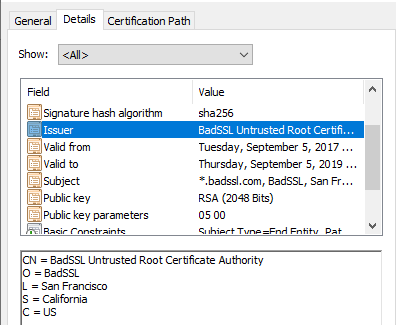
For this one, look in the Certification Path tab. The Certificate status: field at the bottom has useful info too. Also look at the Issuer and Subject fields in the Details tab.

Where the root CA should be, it shows \*.badssl.com  


Issuer and Subject are the same.  


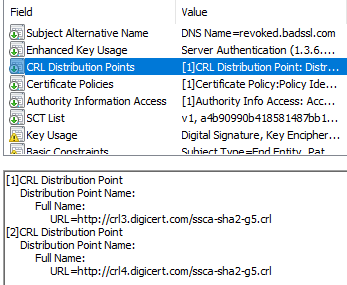
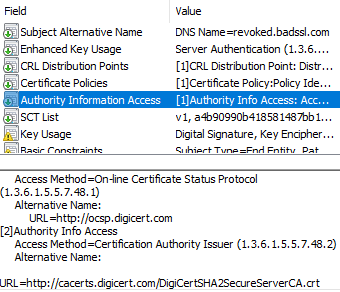
### Untrusted root

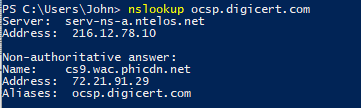
This one looks a lot like the Self-signed certificate. Make the same checks as on the self-signed certificate. It will be slightly different in the Issuer field because the certificate was issued by a CA, we just don’t trust it.

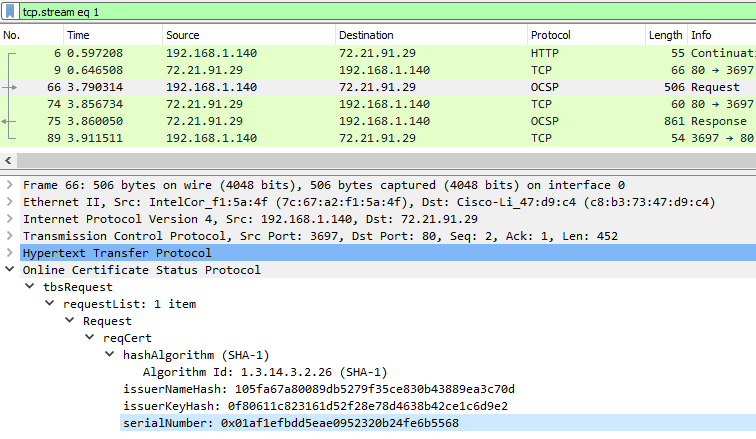
The Issuer is BadSSL Untrusted Root Certificate Authority. We don’t trust it. 

### Revoked

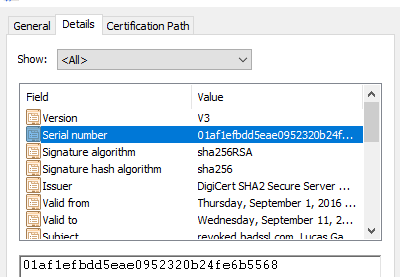
You won’t find anything wrong with this certificate--it is a valid certificate that has been revoked by the CA. When the browser checks with the CA, it will find the certificate has been revoked and you won’t see an error until then. If you like, you can start a packet capture before you click on the link and you may be able to find your browser checking to see if the certificate is revoked. The traffic will be to one of the URLs in the CRL Distribution Points or Authority Information Access fields of the certificate. This one is hard to catch, so I’ll show you what it looks like.

Here are the CRL and OCSP servers for that certificate.  
 

The browser may go to one of the addresses for crl3.digicert.com, crl4.digicert.com, ocsp.digicert.com, or cacerts.digicert.com. Here’s an nslookup query to find the IP address for ocsp.digicert.com.  


Here is the browser’s request to the IP address for ocsp.digicert.com.  


Here’s the certificate serial number, which matches the one in the request

.  


Here is the response, revoked.  
