# 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 user interface and the Windows certificate store. The lock icon in the navigation bar displays certificate information.

A picture containing graphical user interface

Description automatically generated

Clicking on Certificate opens the Microsoft certificate dialog box.

Graphical user interface, text, application

Description automatically generated Text

Description automatically generated with low confidence

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

Graphical user interface, text, application, email

Description automatically generated

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.

Graphical user interface, text

Description automatically generated

Note the Certificate Hierarchy field. It shows the chain of certificates that leads to a root certificate authority (CA), assuming the certificate is valid. The root 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 Connection secure, then select More Information.

Graphical user interface, text, application, chat or text message

Description automatically generatedGraphical user interface, text, application, chat or text message

Description automatically generated

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

Graphical user interface, text, application, email

Description automatically generated

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

Graphical user interface, application

Description automatically generated

<snip>

Graphical user interface, text, application, email

Description automatically generated

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

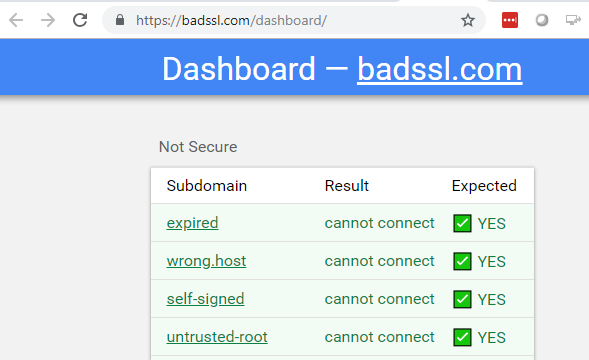
This command says that the certificate follows the X509 format, the input file is google.cer, we want text output to the screen, and we won’t be saving any files or modified versions of the certificate.

Text

Description automatically generated  
<snip>

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.

Your browser will complain that the site you are going to is unsafe. Normally you should heed the warning and go no further.  
Graphical user interface, text, application, email

Description automatically generated

We want to go to the site so we can examine the certificate and see what is wrong. Click on the Advanced button and proceed boldly to the site. The behavior of Chrome and Firefox differs, but both will allow you to click through the warnings to go to the site. Firefox gives you an option to view the certificate before proceeding to the site, which is nice.

### Expired Certificate

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

### 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.

### 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.

### Untrusted root

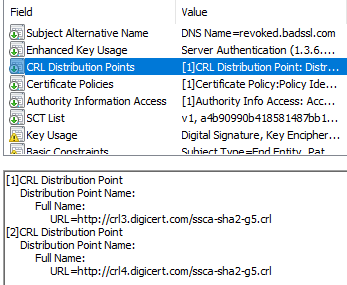
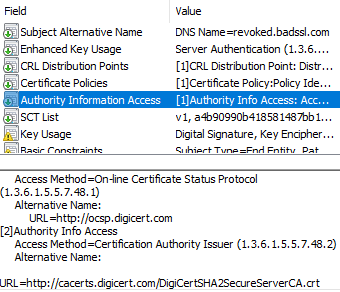
This one looks a lot like the Self-signed certificate. Make the same checks as on the self-signed certificate. It will be slightly different in the Issuer field because the certificate was issued by a CA, we just don’t trust it.

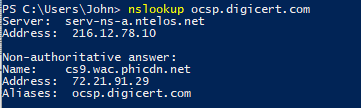
### Revoked

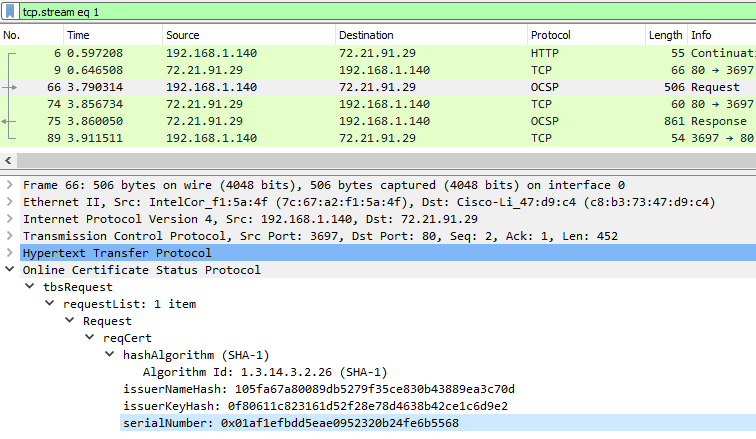
Note: The site has not been updated recently, and the certificate revoked.badssl.com has expired. So just read the following, you don't have to do anything. To determine whether a certificate is revoked you must follow the procedure the browser follows. In the text below, we follow along with the browser in Wireshark as we:

1. Find the URL for the old-style Certificate Revocation List
2. Find the URL for the newer OCSP (under Authority Information Access in the certificate.)
3. Find the IP for the above
4. Find the browser's request to either the CRL or OCSP in the Wireshark traffic
5. Find the response—is it ok or revoked?

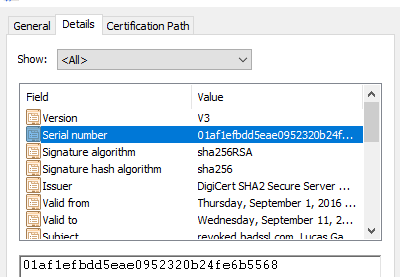
You won’t find anything wrong with this certificate--it is a valid certificate that has been revoked by the CA. When the browser checks with the CA, it will find the certificate has been revoked and you won’t see an error until then. If you like, you can start a packet capture before you click on the 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 certificate

.  


Here is the response, revoked.  
