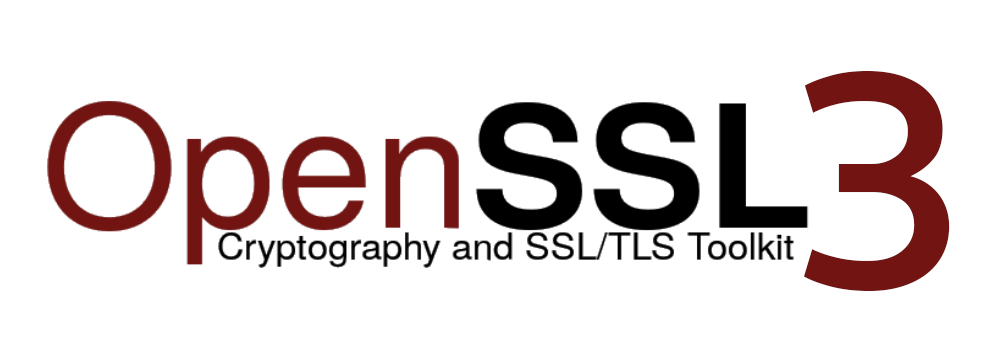
## Examining SSL Certificate



[Examining SSL Certificate 1](#_Toc167805184)

[Checking certificate validity 3](#_Toc167805185)

[Checking certificate expiry date 3](#_Toc167805186)

[Checking certificate extensions 3](#_Toc167805187)

[Checking deprecated TLS ciphers or versions 3](#_Toc167805188)

[Inspecting google.com certificate included with Mozilla. 3](#_Toc167805189)

[Inspecting online www.google.com certificate using Firefox 5](#_Toc167805190)

[Download PEM compare content with locally stored certificate 9](#_Toc167805191)

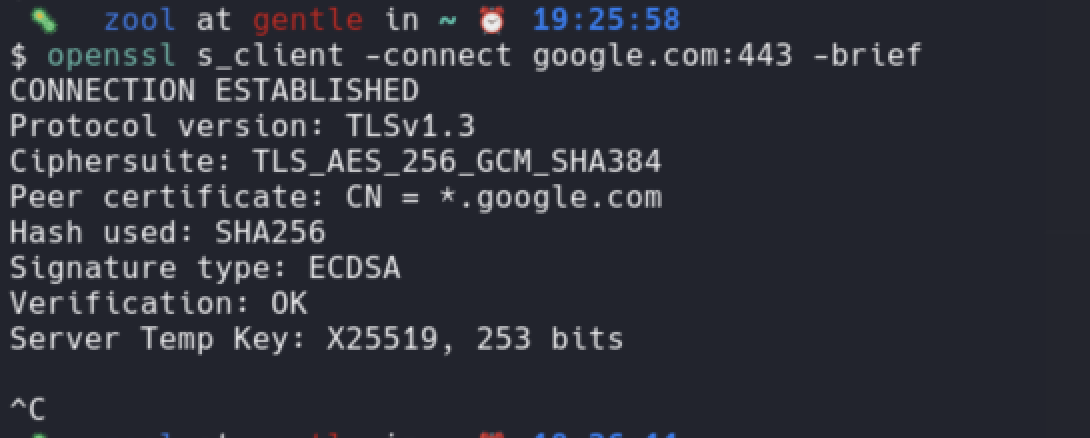
[Challange: 10](#_Toc167805192)

[Bonus challenge: 10](#_Toc167805193)

### Checking certificate validity

Let’s examine google.com certificate validity

***openssl s\_client -connect google.com:443 –brief***



Analyze output:

What hashing algorithm is used?

### Checking certificate expiry date

***echo | openssl s\_client -connect google.com:443 2>/dev/null | openssl x509 -noout -dates***

### Checking certificate extensions

***echo | openssl s\_client -connect google.com:443 2>/dev/null | openssl x509 -noout -ext subjectAltName***

### Checking deprecated TLS ciphers or versions

***openssl ciphers -s -tls1\_3***

### Inspecting google.com certificate included with Mozilla.

Let's examine one of certificates that are included with mozilla system.

***openssl x509 -text -noout -in /usr/share/ca-certificates/mozilla/GTS\_Root\_R1.crt***



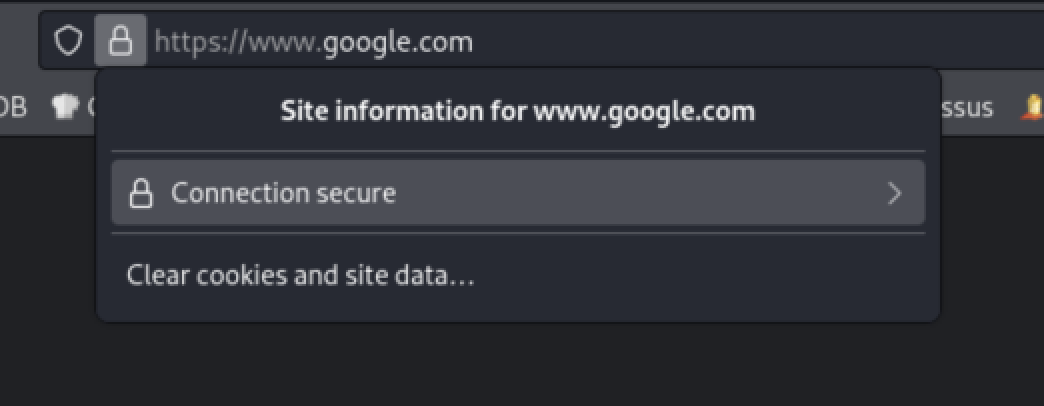
Examine content of:

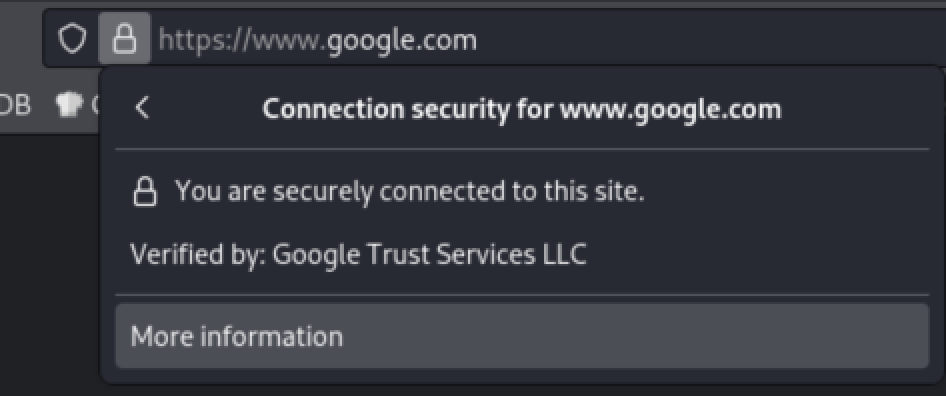
/usr/share/ca-certificates/mozilla/

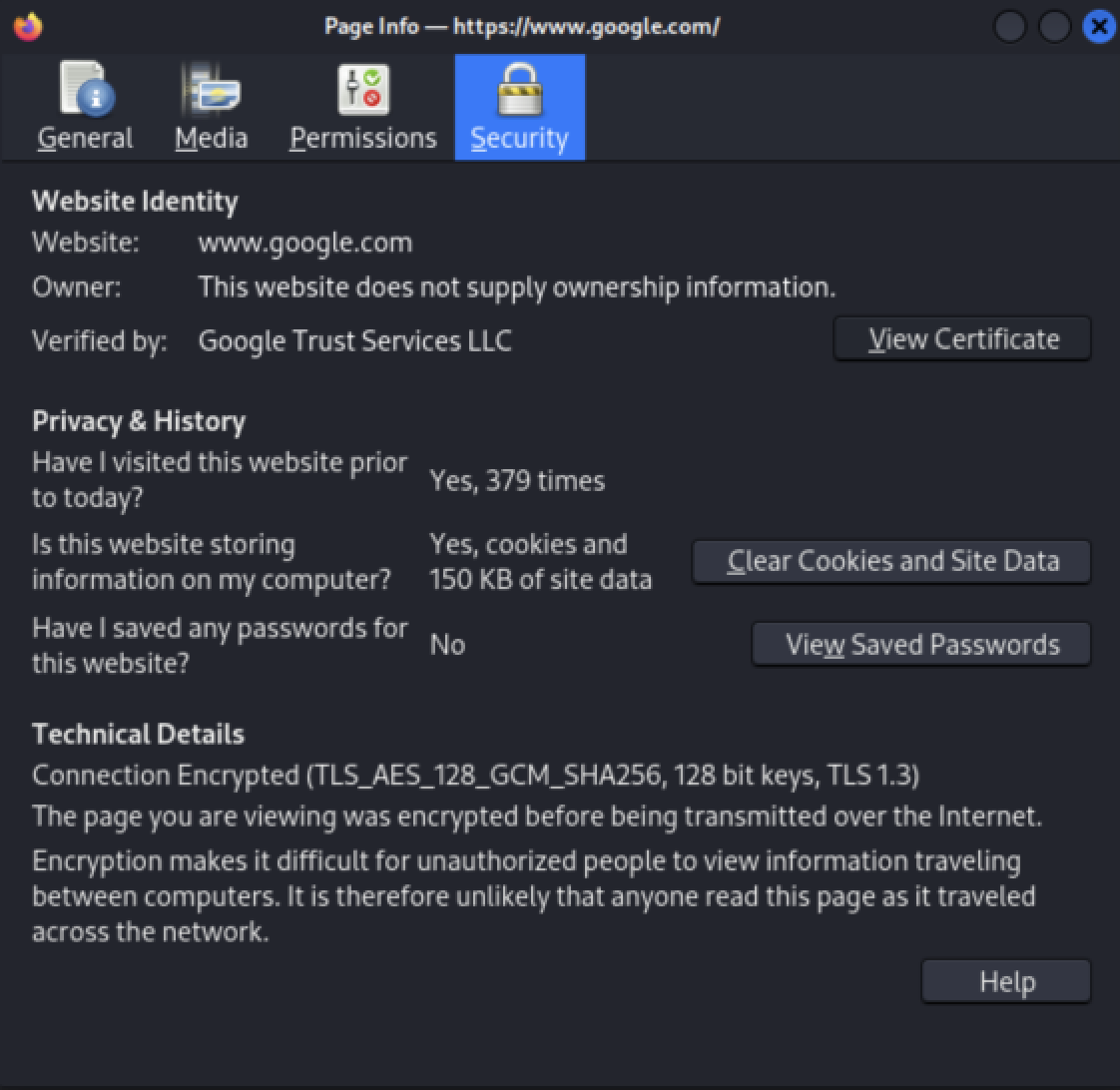
### Inspecting online www.google.com certificate using Firefox

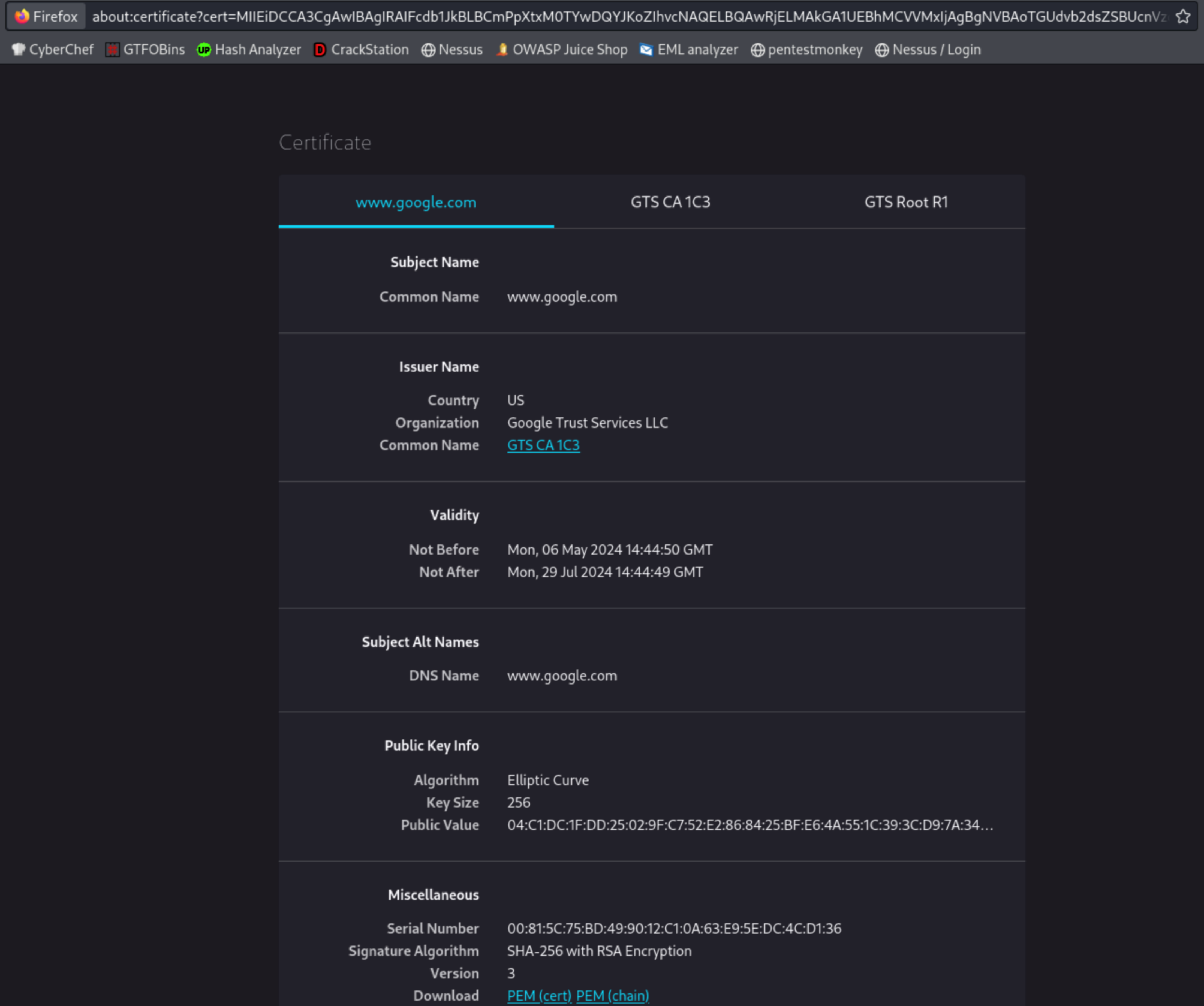
Open Firefox and navigate to [www.google.com](http://www.google)

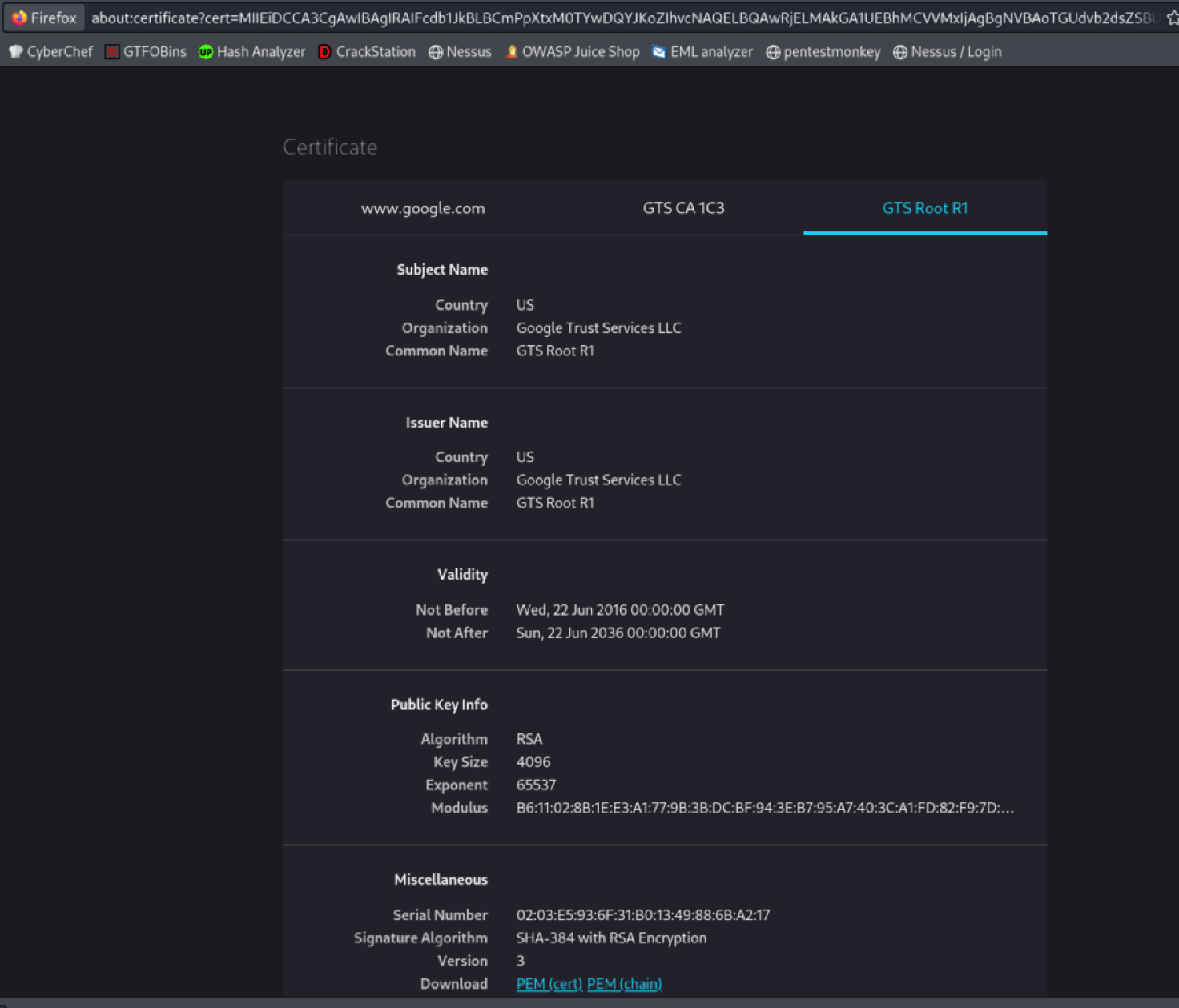
Click on padlock and follows screenshots.







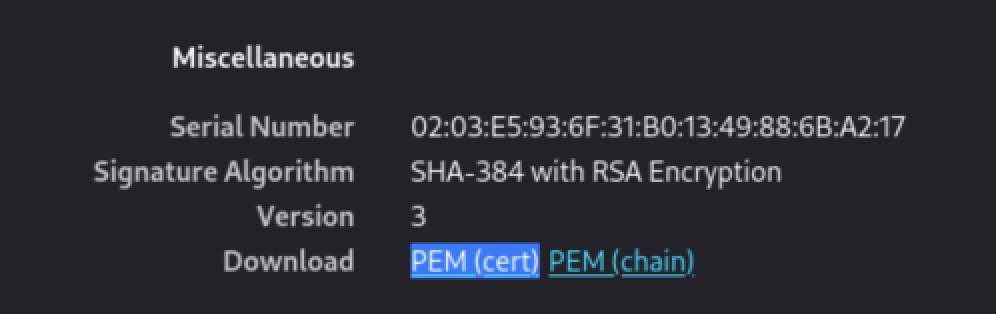




Download PEM

Compare Serial Number and other fields between locally stored and online certificate

Click on

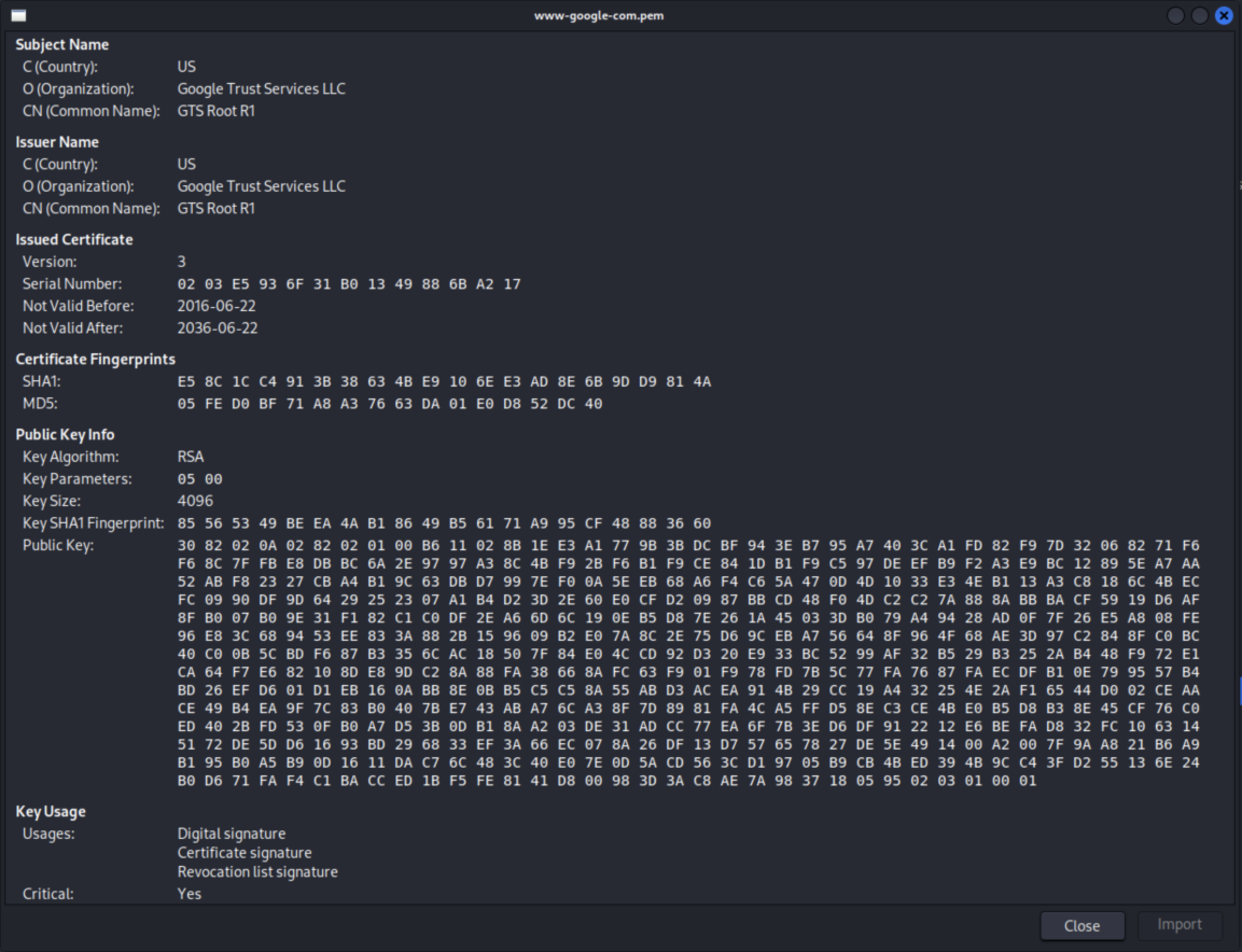


### Download PEM compare content with locally stored certificate

PEM:

“Privacy-Enhanced Mail (PEM) is a de facto file format for storing and sending cryptographic keys, certificates, and other data, based on a set of 1993 IETF standards defining "privacy-enhanced mail." While the original standards were never broadly adopted and were supplanted by PGP and S/MIME, the textual encoding they defined became very popular. The PEM format was eventually formalized by the IETF in RFC 7468.[1]”

Reference: <https://en.wikipedia.org/wiki/Privacy-Enhanced_Mail>



### Challange:

Using cli tools of your choice crate file named crt\_list.txt on your desktop.

### Bonus challenge:

Command needs to be one liner.