

# Extract Certificate Information with OpenSSL

## Fetch the X.509 Public Key Certificate File

```
openssl s_client -connect google.com:443 -showcerts </dev/null | openssl x509 -outform pem > googlecert.pem
```

## Decode the Entire Certificate

```
openssl x509 -in googlecert.pem -noout -text
```

## Extract Specific Information from the Certificate

### Extract the Subject

```
openssl x509 -in googlecert.pem -noout -subject subject=CN = *.google.com
```

### Extract the Issuer

```
$ openssl x509 -in googlecert.pem -noout -issuer issuer=C = US, O = Google Trust Services LLC, CN = GTS CA 1C3
```

## Extracting the Extension Fields

```
$ openssl x509 -in googlecert.pem -noout -ext subjectAltName X509v3 Subject Alternative Name:  
DNS:*.google.com, DNS:*.appengine.google.com, DNS:*.bdn.dev, DNS:*.cloud.google.com,  
DNS:*.crowdsourcing.google.com, DNS:*.datacompute.google.com, ...(truncated)
```

---

Revision #1

Created 10 February 2023 14:04:29 by Dino Edwards

Updated 10 February 2023 14:14:55 by Dino Edwards