获得TLS信息课程报告

需求：编写程序获得https服务器的密码套件和和证书等服务信息。

解决思路：利用python的ssl和socket库与https服务器建立连接，从而可以获得TLS的配置信息。

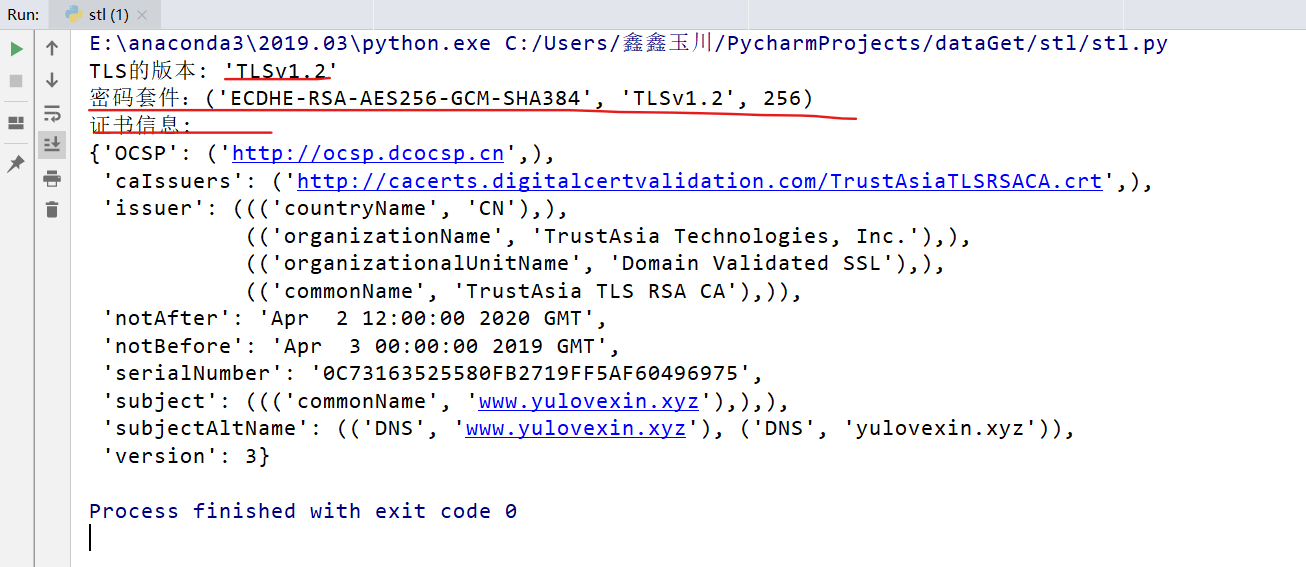
语言：python

使用库：ssl，socket

代码：

|  |
| --- |
| import socket  import ssl  import pprint  hostname = 'www.yulovexin.xyz'  context = ssl.create\_default\_context()  with socket.create\_connection((hostname, 443)) as sock:  with context.wrap\_socket(sock, server\_hostname=hostname) as ssock:  print("TLS的版本: ",end='')  pprint.pprint(ssock.version())  print("密码套件：", end='')  pprint.pprint(ssock.cipher())  print("证书信息:")  pprint.pprint(ssock.getpeercert()) |

代码流程大概为与host建立连接，把连接结果封装成一个对象，通过这个对象可以获得配置信息。

结果图如下：

|  |
| --- |
| TLS的版本: 'TLSv1.2'  密码套件：('ECDHE-RSA-AES256-GCM-SHA384', 'TLSv1.2', 256)  证书信息:  {'OCSP': ('http://ocsp.dcocsp.cn',),  'caIssuers': ('http://cacerts.digitalcertvalidation.com/TrustAsiaTLSRSACA.crt',),  'issuer': ((('countryName', 'CN'),),  (('organizationName', 'TrustAsia Technologies, Inc.'),),  (('organizationalUnitName', 'Domain Validated SSL'),),  (('commonName', 'TrustAsia TLS RSA CA'),)),  'notAfter': 'Apr 2 12:00:00 2020 GMT',  'notBefore': 'Apr 3 00:00:00 2019 GMT',  'serialNumber': '0C73163525580FB2719FF5AF60496975',  'subject': ((('commonName', 'www.yulovexin.xyz'),),),  'subjectAltName': (('DNS', 'www.yulovexin.xyz'), ('DNS', 'yulovexin.xyz')),  'version': 3} |

到此结果正确，实验成功。