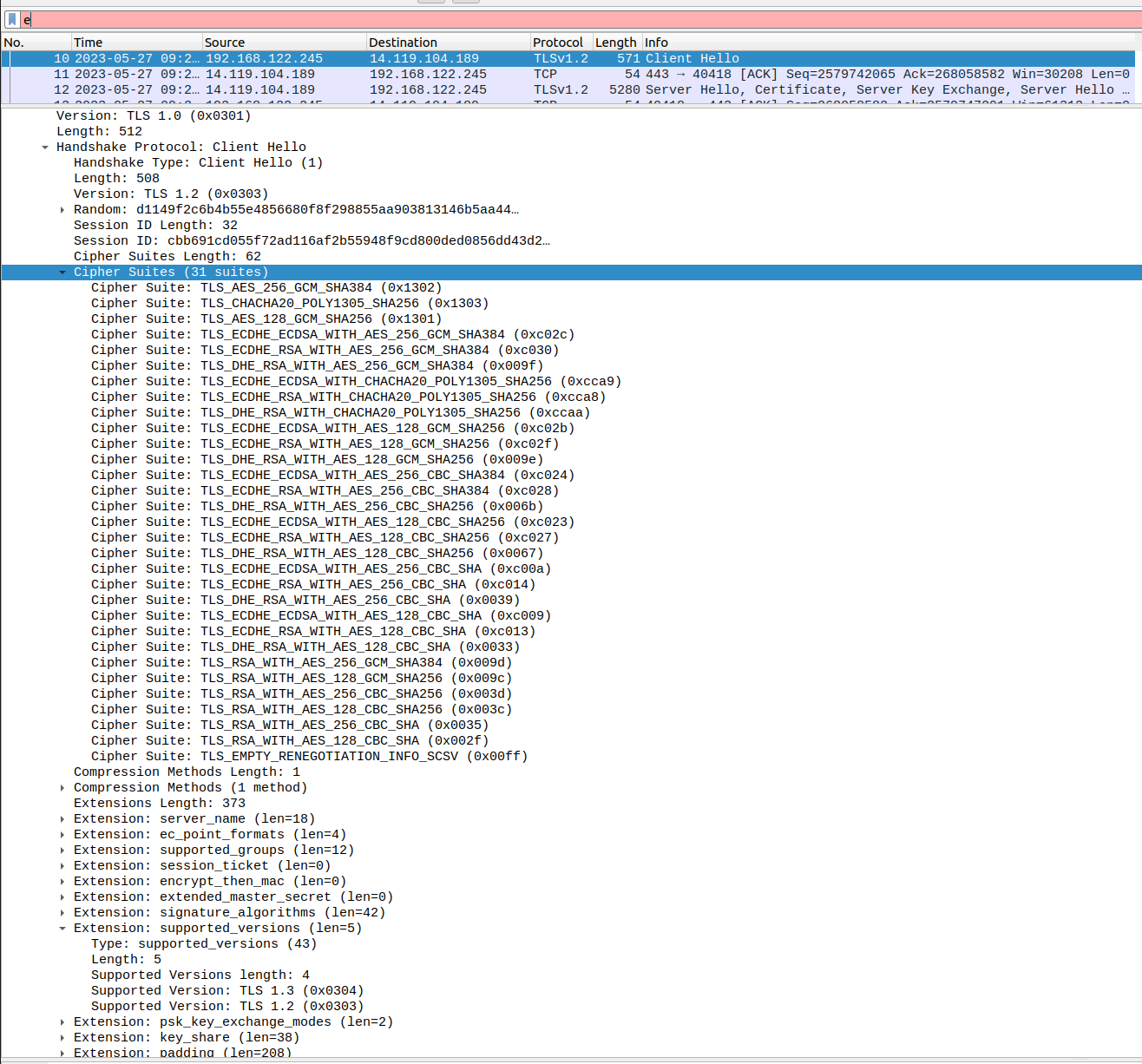
|  |
| --- |
| 哈尔滨工业大学(深圳) |
| **《网络与系统安全》 实验报告** |
|  |
| 实验五  TLS 实验  学 院: 计算机科学与技术学院   |  |  | | --- | --- | | 姓 名: | 梁鑫嵘 | | 学 号: | 200110619 | | 专 业: | 计算机科学与技术学院 | | 日 期: | 2023年4月 | |

1.在客户端容器中执行如下命令 ./handshake.py www.baidu.com根据执行结果回答下面三个问题。

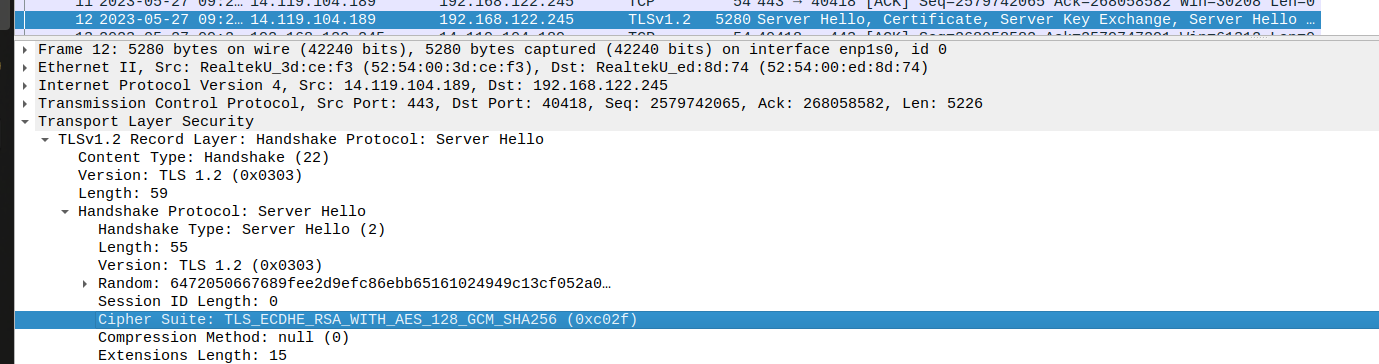
（1）客户端和服务器端使用的加密算法有哪些，分别起什么作用？

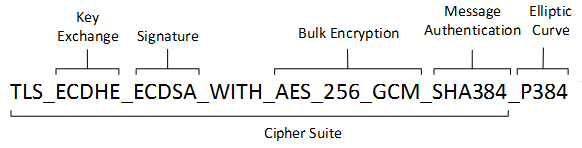
从Client Hello包得知，客户端支持的加密算法有：



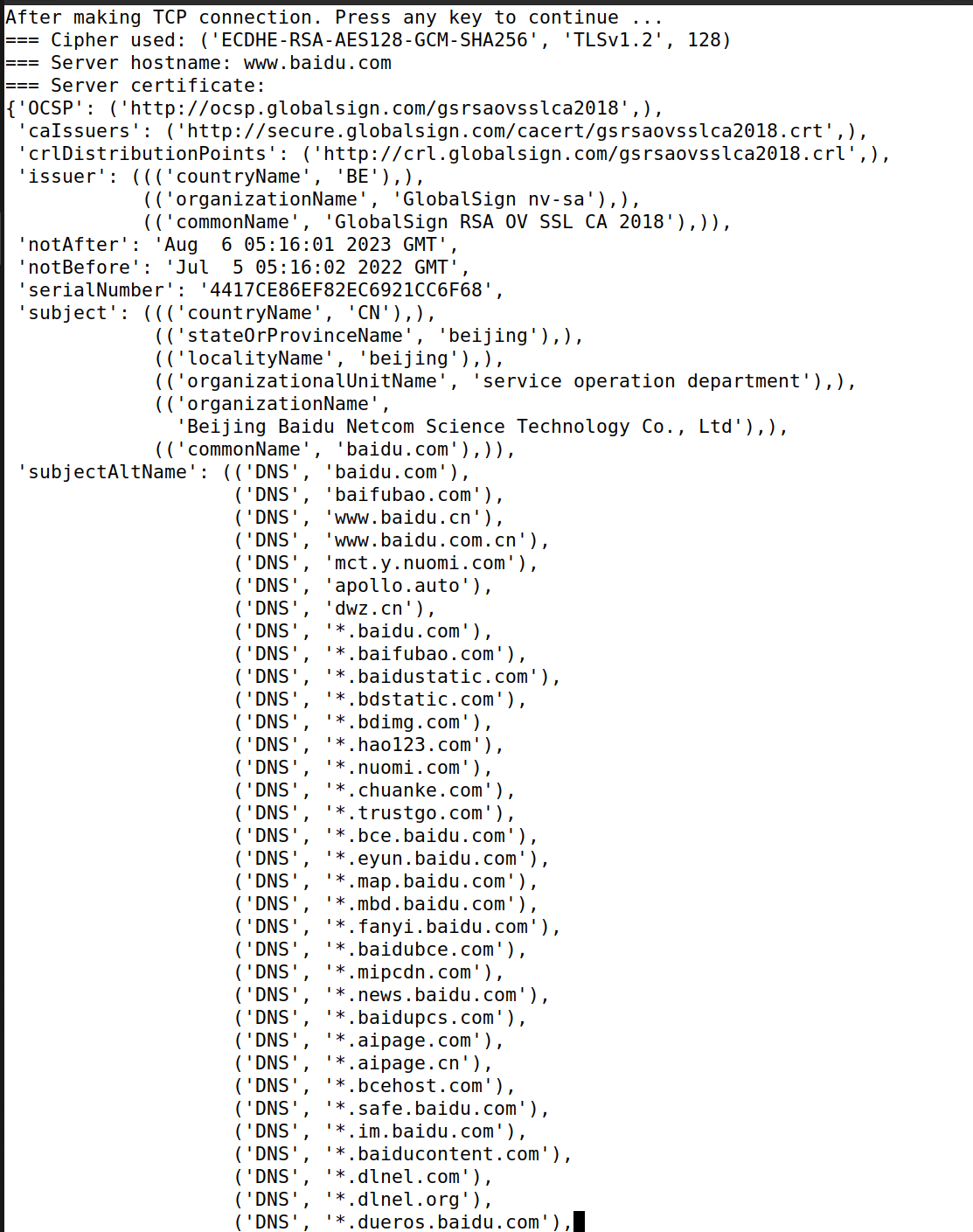
主要为AES、ECDSA、CHACHA20、RSA等。

从Server Hello包中得知，服务端使用的是TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256





（2）分析打印出来的服务器端证书

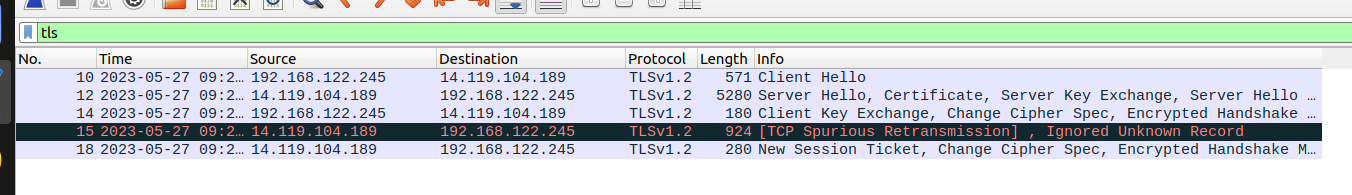


证书分析：

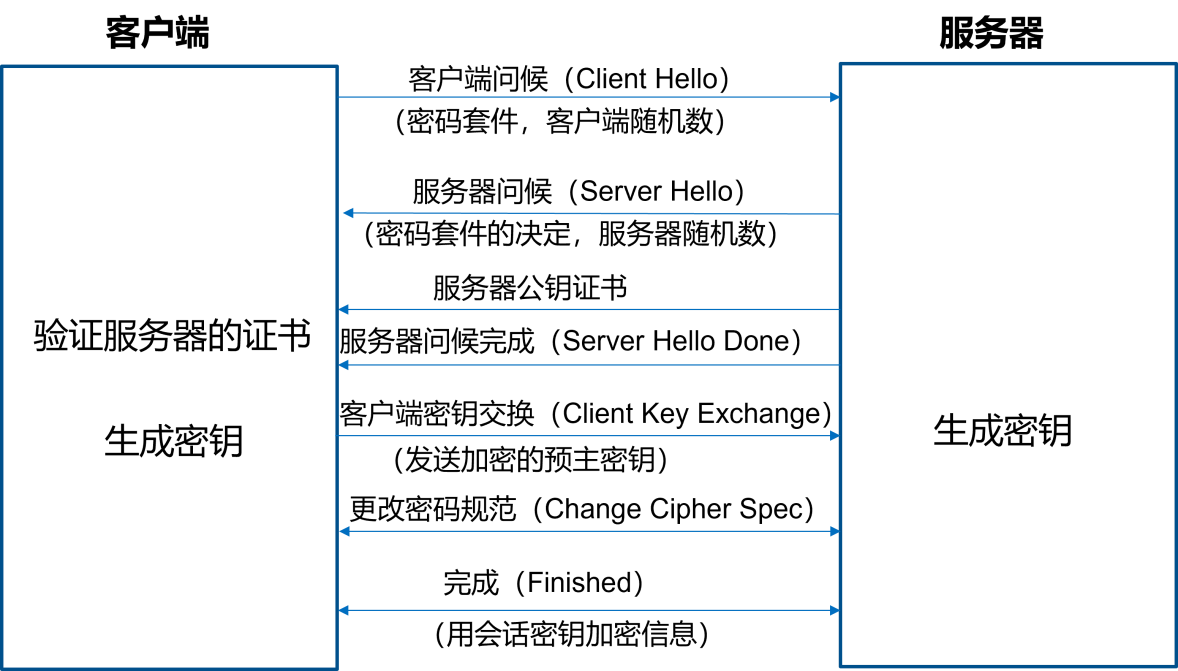
1. 颁发者是BE（比利时）的GlobalSign
2. 持有者是CN（中国）的Beijing Baidu Netcom Science Technology
3. 此证书对下列域名都有效

（3）抓包分析TLS握手协议

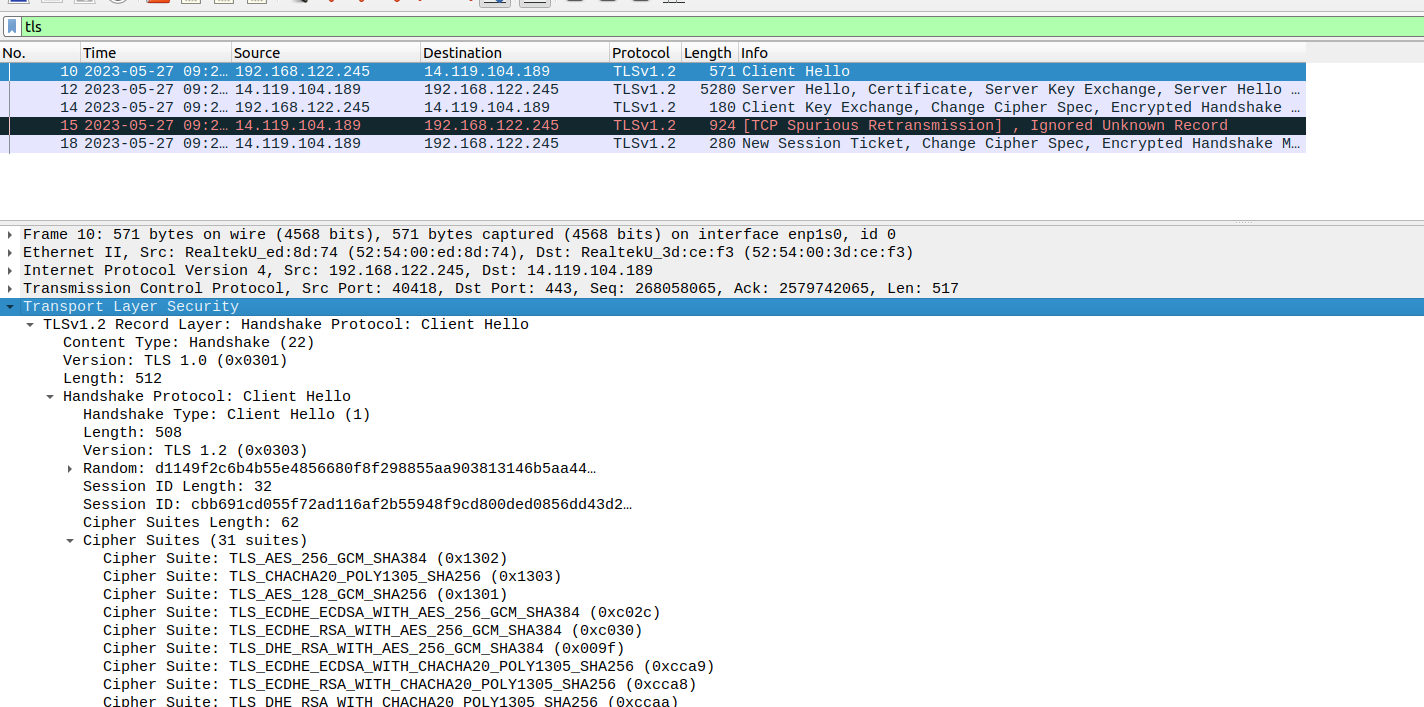
对脚本运行过程抓包：



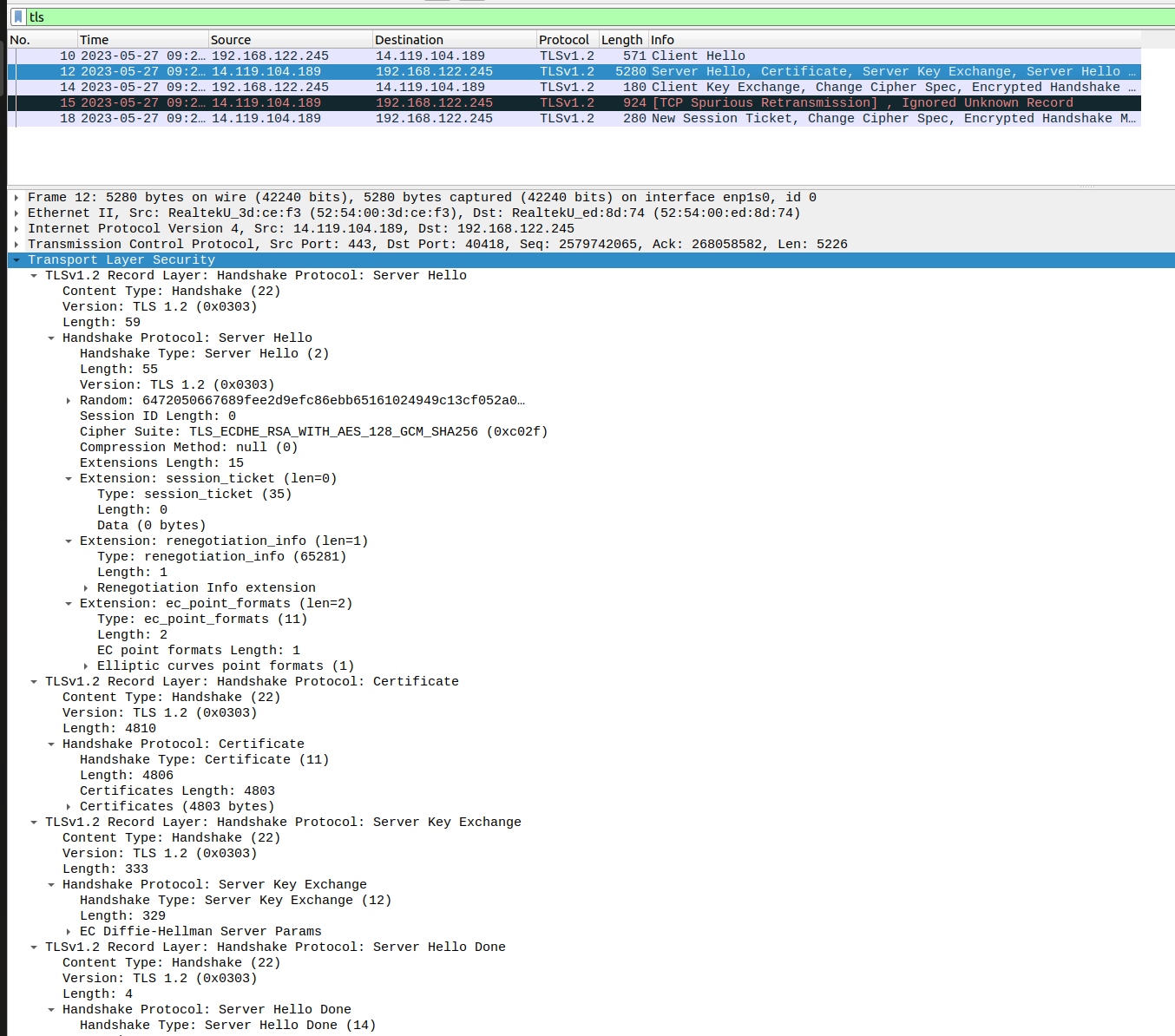
运行结束后有4个TLSv1.2导书的TLS握手过程：

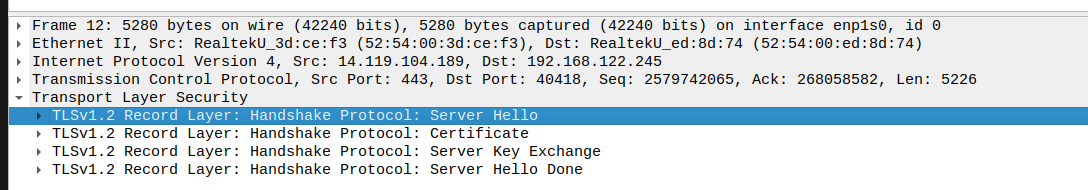


Client Hello：



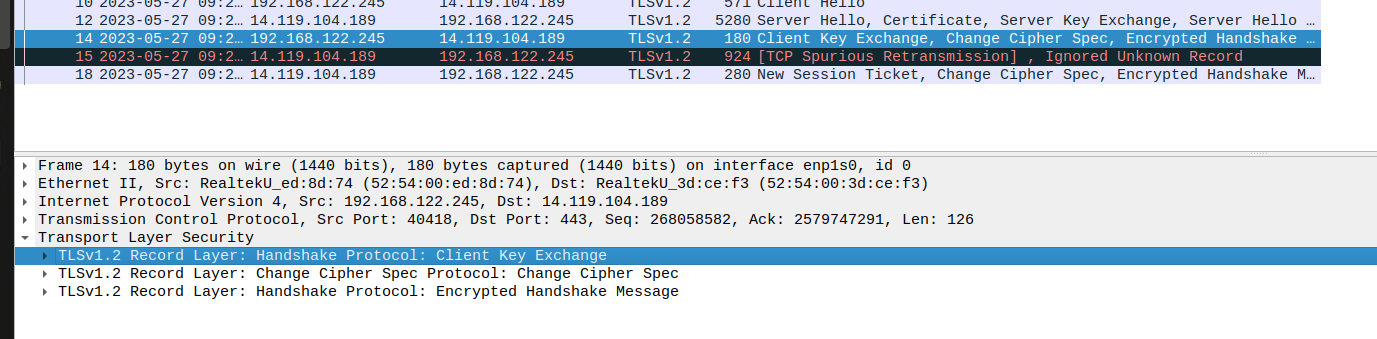
Server Hello：

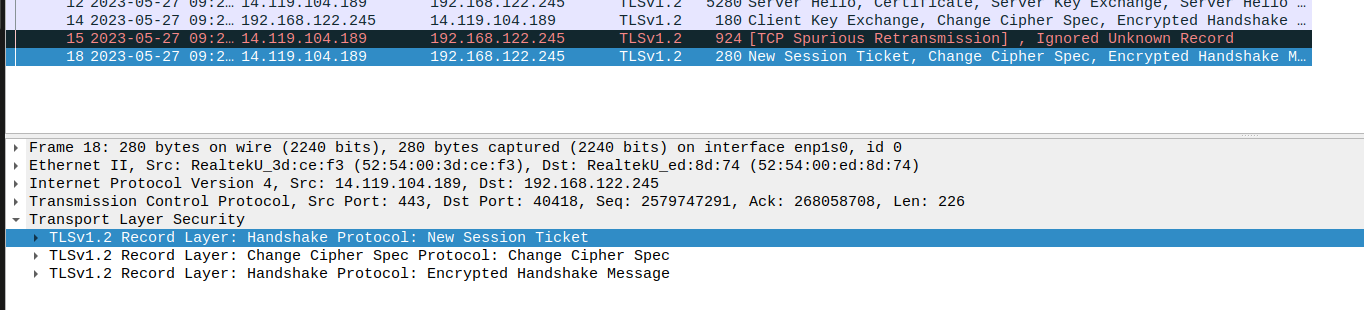


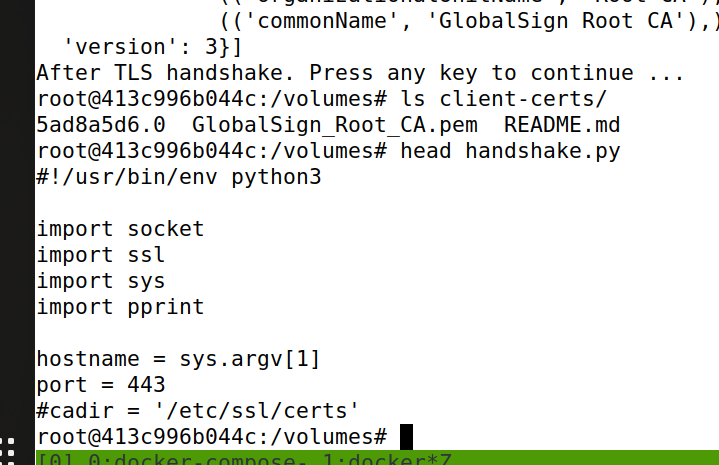


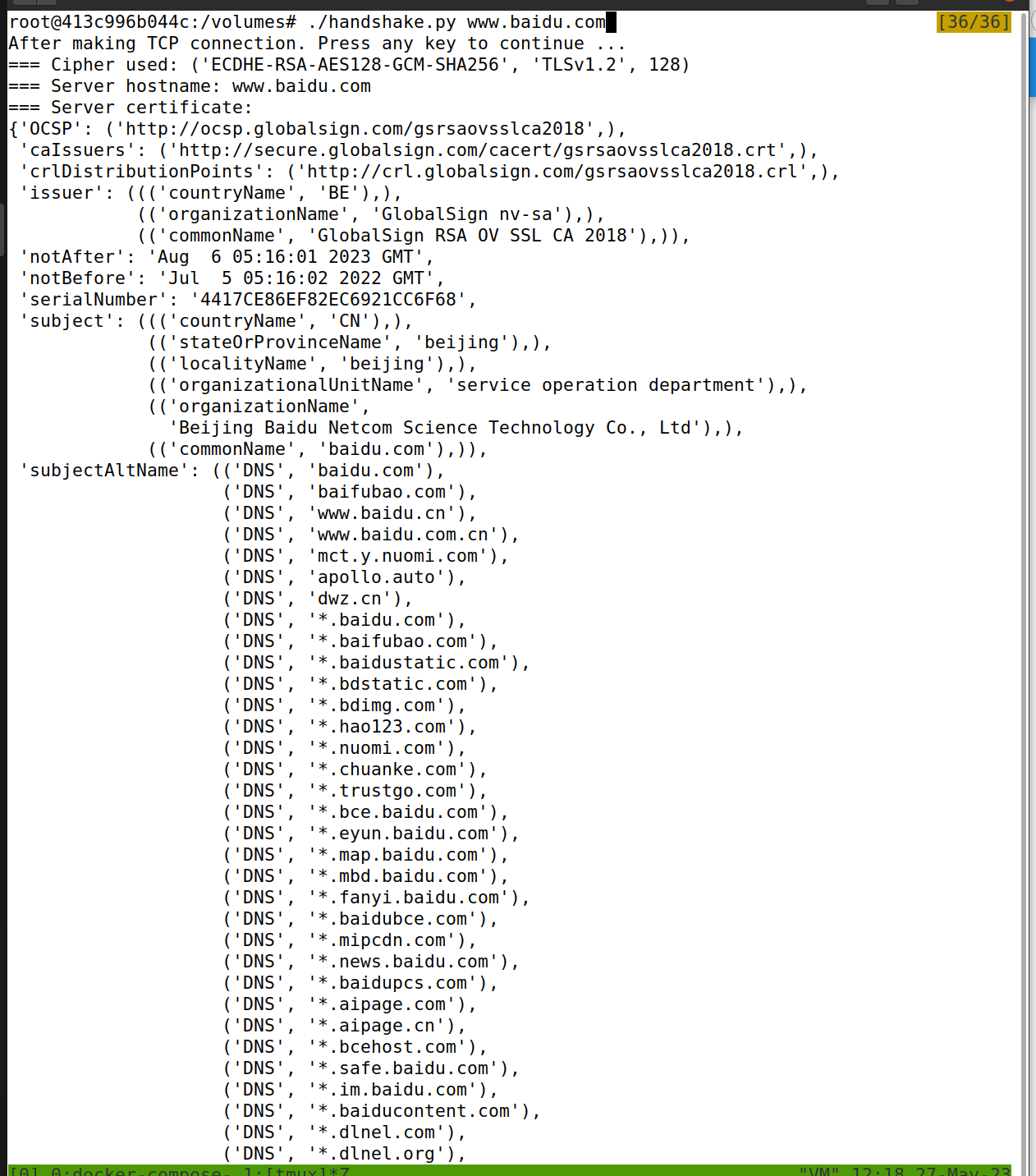
此时一次传输了Server Hello、服务器证书、服务器密钥交换、服务器问候完成。

客户端密钥交换、更改密码规范、传递加密信息：



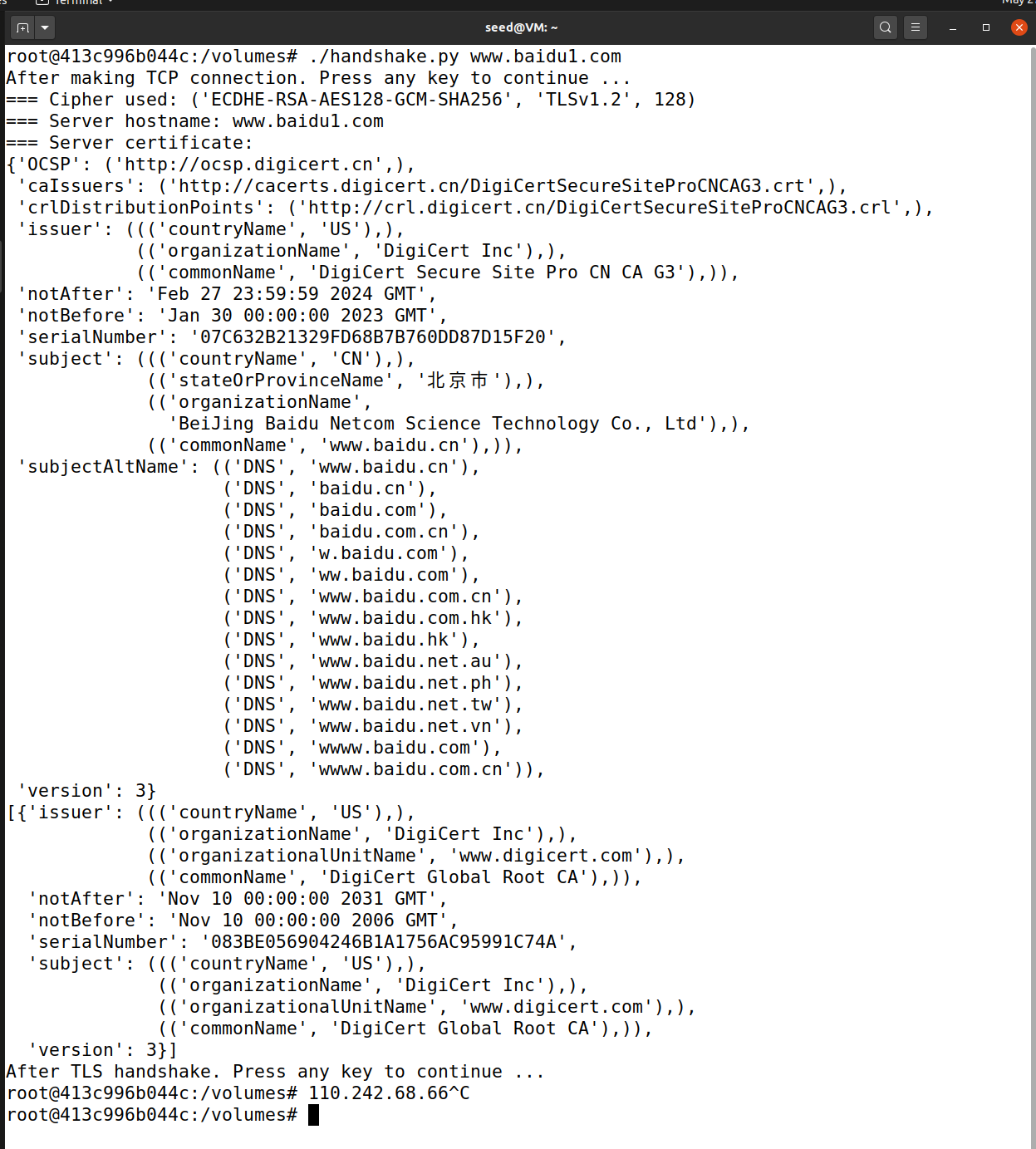


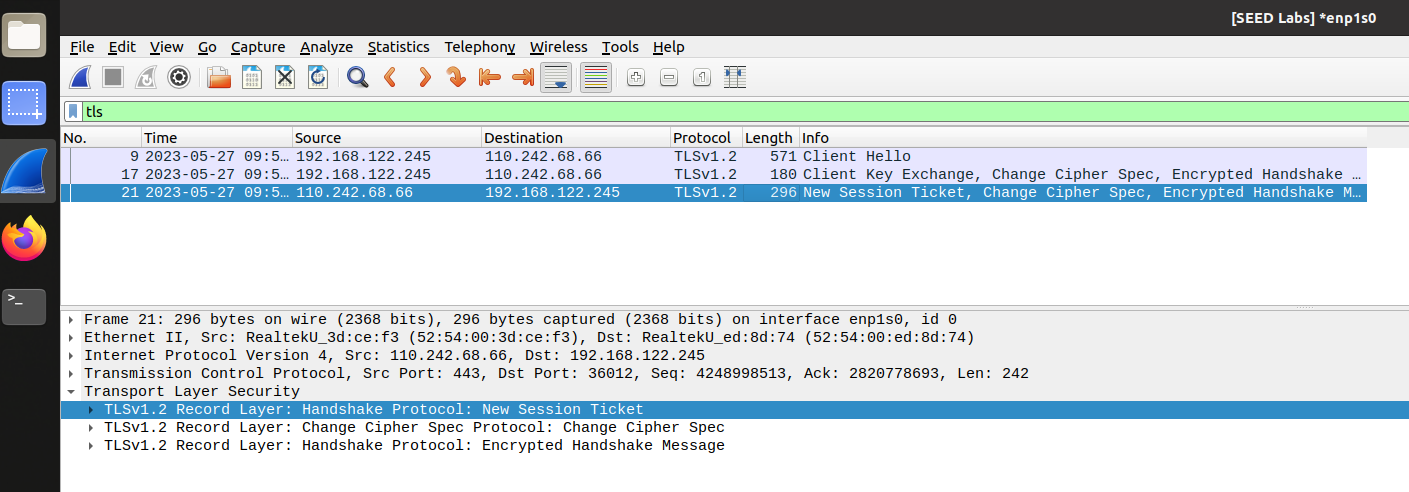
1. 更改证书文件路径，请同学们将www.baidu.com网站的测试过程截图保存（如果不将证书拷贝过来应该有报错信息，拷贝过来之后应该正常），也可选用其他网站做测试。
2. 



3. 请同学们将修改 www.baidu.com 网站主机名的测试过程截图保存在报告里并分析执行的结果，也可选用其他网站做测试。

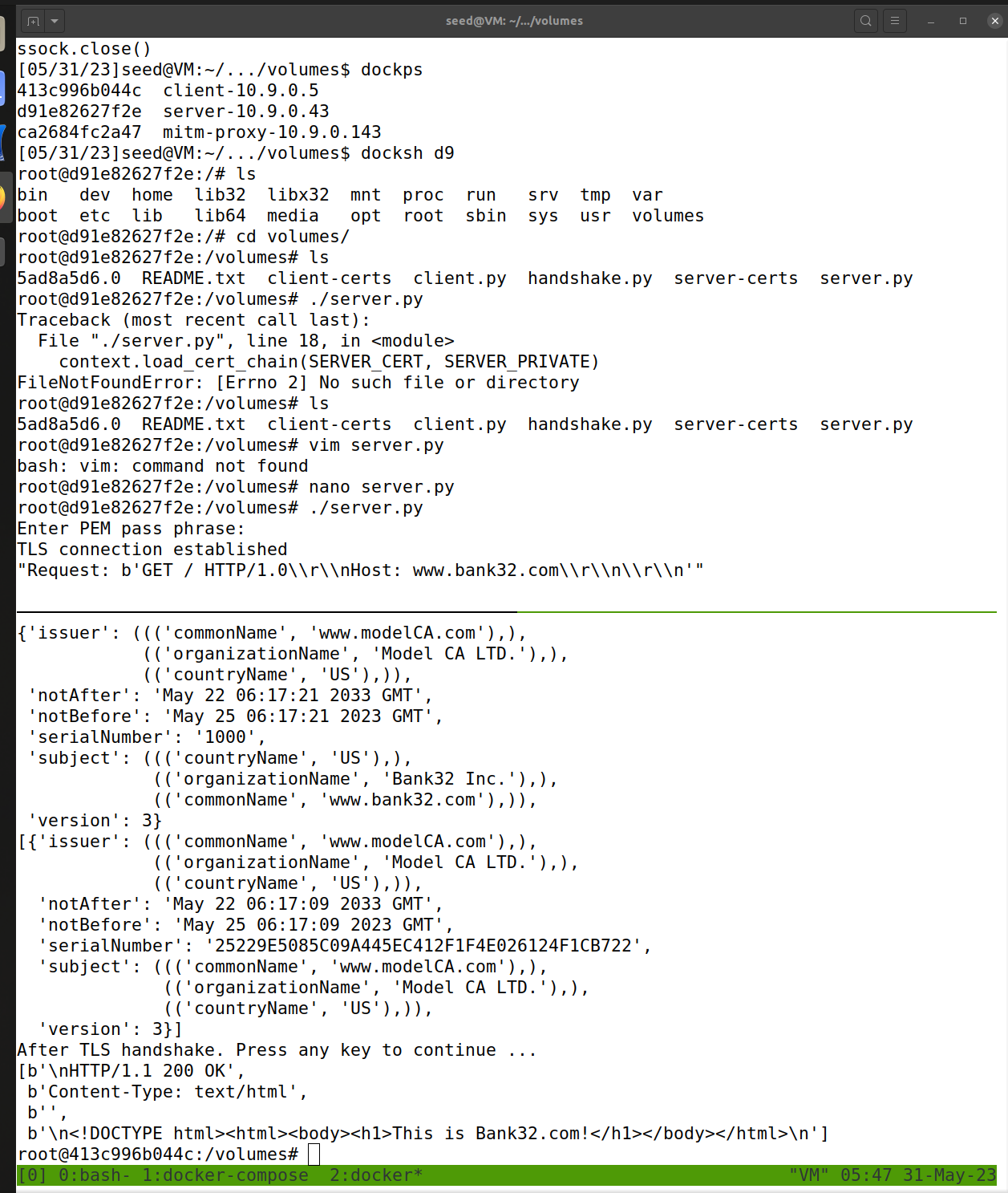
修改hosts后，由于没有校验域名正确性，所以整个流程可以顺利进行。



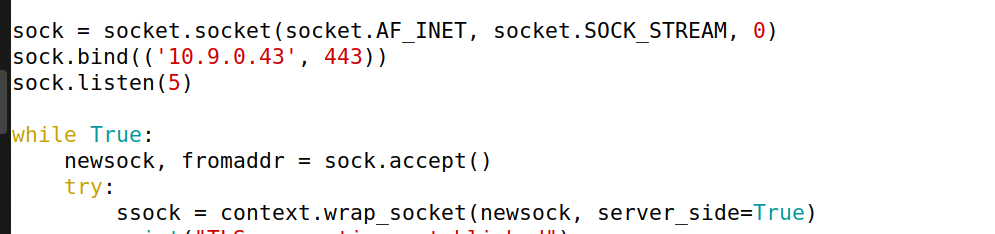


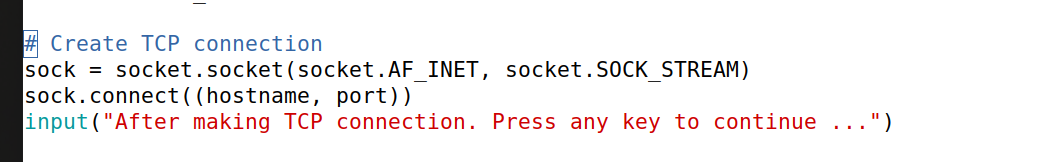
4.请分析TLS客户端编程和server.py的代码，说明客户端和服务器程序的关键步骤。

从客户端访问服务端：

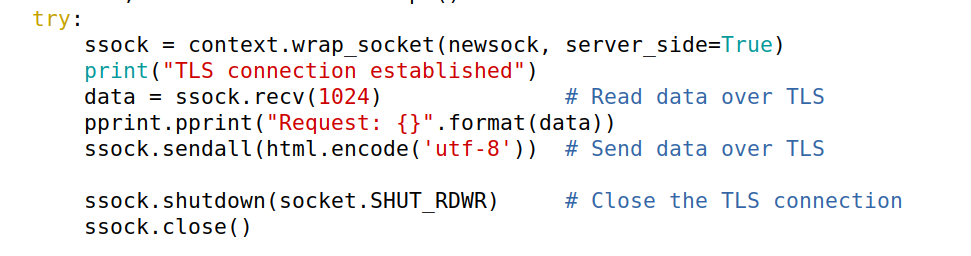


1. TCP 连接

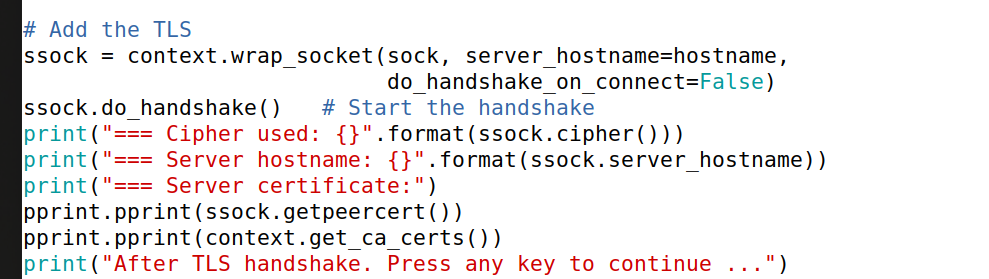




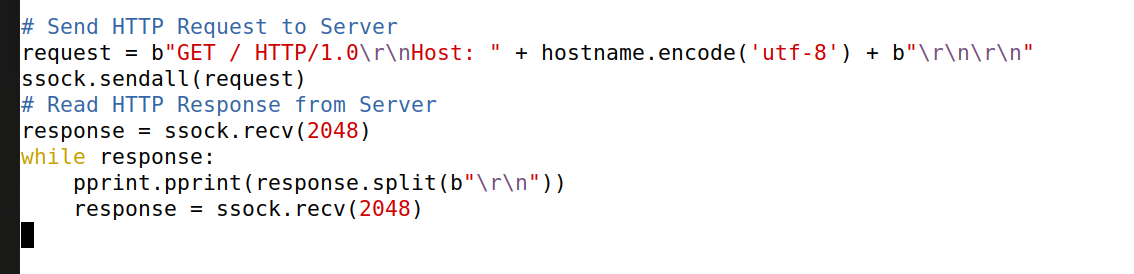
1. 数据传输
   1. 服务端TLS



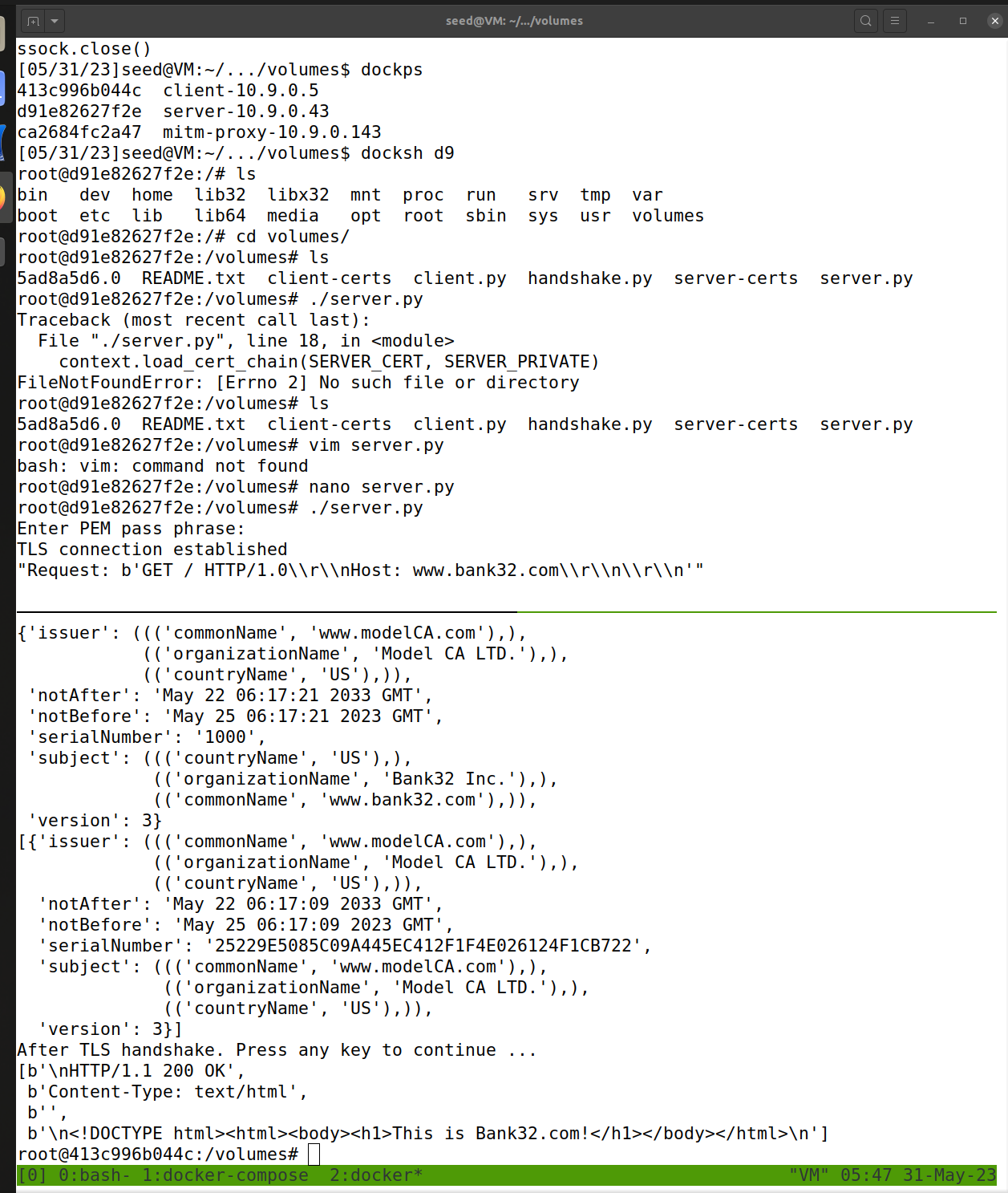
* 1. 客户端 TLS

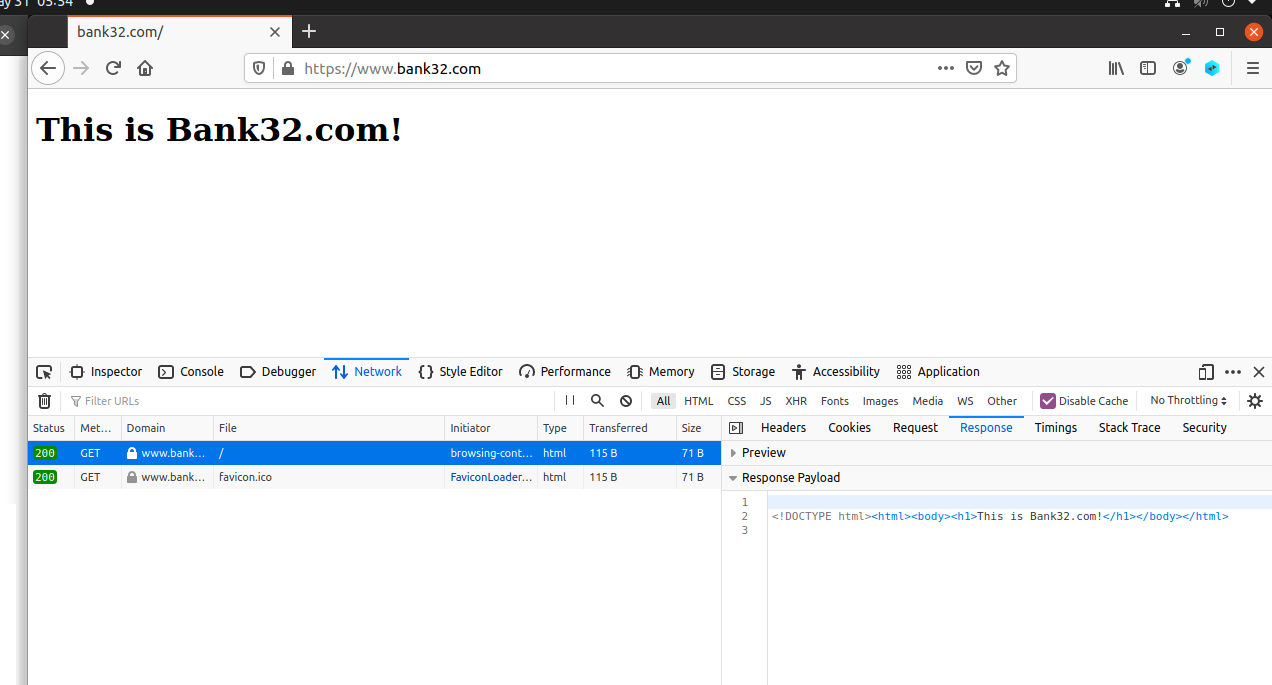


1. 客户端HTTP请求 Over TLS



5.请分别用client.py和浏览器两种方式访问服务器，并记录你观察的结果（截图）





现象：

client.py能够正确获取服务器的网页，

浏览器也能够正常请求服务器网页并显示。