

Manual

姓名：郭正康

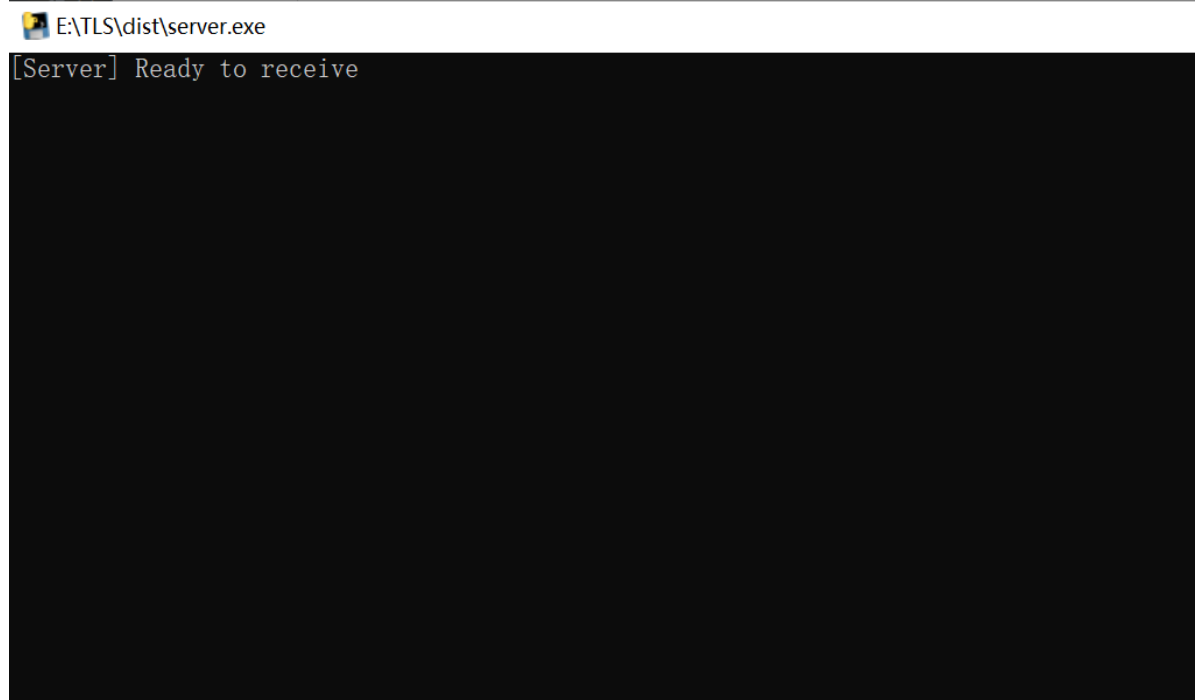
学号：20307130162

为了用户上帝般的使用体验，这将是一篇婴儿级呵护的使用手册！

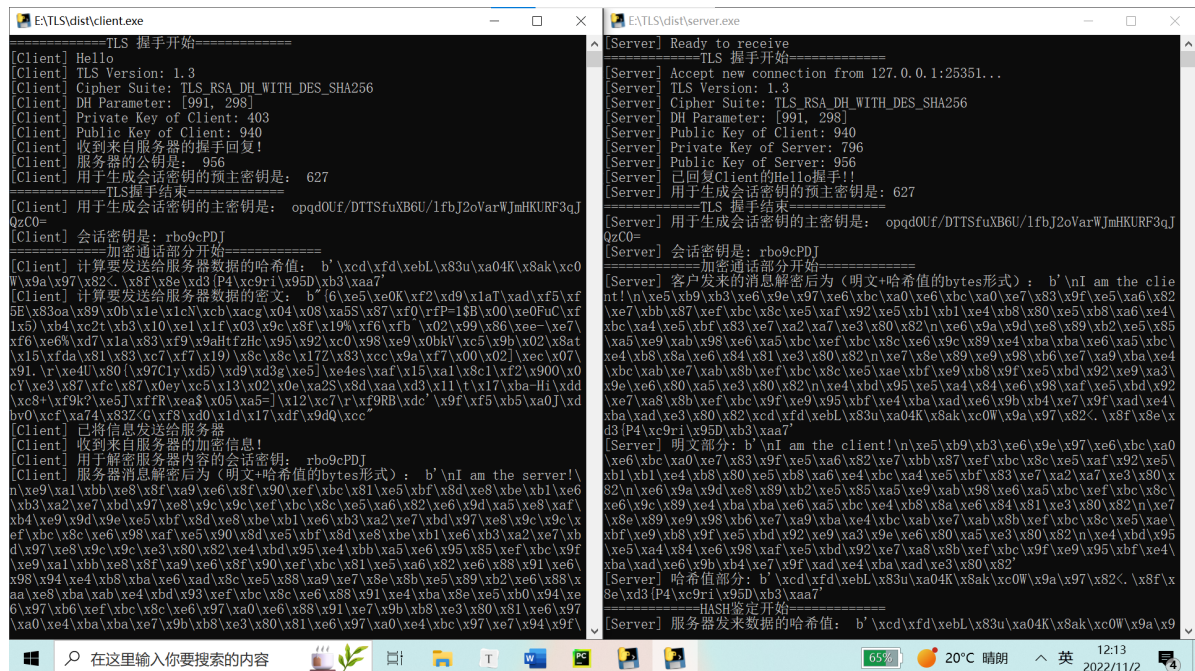
由于代码是用Python编写的，所以我提供了两种运行方式：

1) 省心运行：

这种方法只需要先点击server.exe文件，会显示如下：



再点击client.exe文件即可，效果如下：



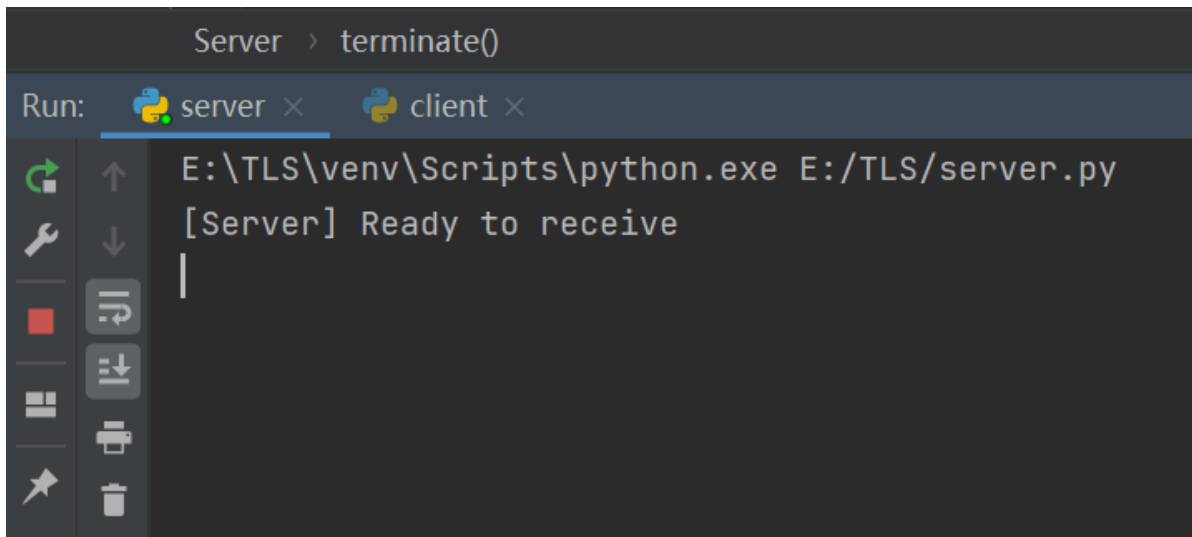
最后只需要在两个窗口各自按一下回车即可关闭运行窗口。

2) 实操运行:

这种方式需要运行server.py和client.py两个源代码文件，您可以体验程序员de完所有bug之后运行成功的那一刻喜悦！

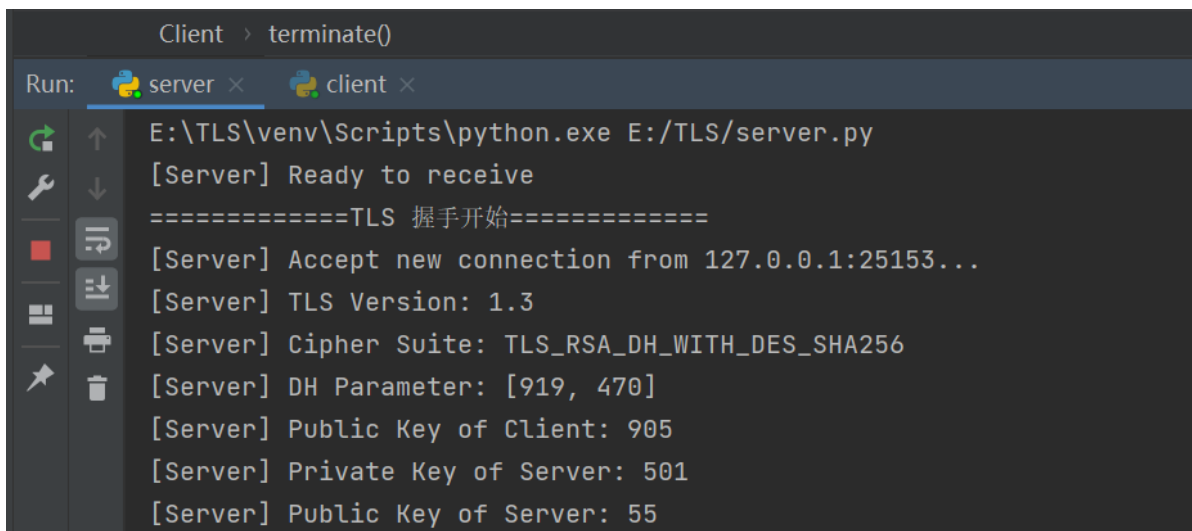
注意：采用这种方法可能需要下载一些库以确保程序可以运行，比如：`pip install hkdf`。如果程序还报错缺少哪个模块，那要劳烦您多执行几次 `pip install + 库名`

先运行server.py文件，会在运行窗口看到如下情形：



```
Server > terminate()
Run: server x client x
E:\TLS\venv\Scripts\python.exe E:/TLS/server.py
[Server] Ready to receive
|
```

然后再运行client.py文件，client和server的运行窗口就会各自打印出整个运行过程！！如下：



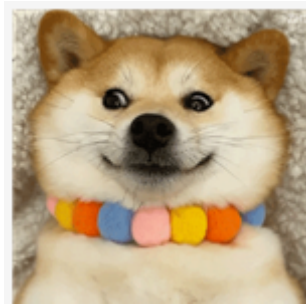
```
Client > terminate()
Run: server x client x
E:\TLS\venv\Scripts\python.exe E:/TLS/server.py
[Server] Ready to receive
====TLS 握手开始====
[Server] Accept new connection from 127.0.0.1:25153...
[Server] TLS Version: 1.3
[Server] Cipher Suite: TLS_RSA_DH_WITH_DES_SHA256
[Server] DH Parameter: [919, 470]
[Server] Public Key of Client: 905
[Server] Private Key of Server: 501
[Server] Public Key of Server: 55
```

```
Client > terminate()

Run: server × client ×

E:\TLS\venv\Scripts\python.exe E:/TLS/client.py
=====TLS 握手开始=====
[Client] Hello
[Client] TLS Version: 1.3
[Client] Cipher Suite: TLS_RSA_DH_WITH_DES_SHA256
[Client] DH Parameter: [919, 470]
[Client] Private Key of Client: 865
[Client] Public Key of Client: 905
[Client] 收到来自服务器的握手回复!
[Client] 服务器的公钥是: 55
[Client] 用于生成会话密钥的预主密钥是: 590
```

为了您宝贵的时间，我诚心推荐您采用第一种极致追求用户体验的方法，当然，如果您愿意，也可以选择方法二，它并不会麻烦多少



如果您有任何问题或不解，请联系客服小郭同学：18817238652/20307130162@fudan.edu.cn 客服24小时除了睡觉都在线！