

一个轻量级即时聊天程序设计与实现

整体设计

我的设计中，轻量级的服务端实际上只是为多个客户端提供鉴权、发现以及可靠的数据包转发服务，为客户端两两之间创建了可靠的端对端的数据包交换通道。几乎所有功能，包括聊天、“正在输入”的提示、文件传输和共享画板，均由客户端实现，封装到格式统一的数据包交给服务器进行转发，服务器无需理解包内容。此外，服务器在客户端不在线时还有缓存数据包的能力，能够在客户端上线的时候将缓存的数据包统一发给客户端。另外，服务器和客户端之间的通信还加入了TLS加密层，确保会话内容的保密性和完整性。

未来，还可以实现NAT穿透，进而为客户端真正创建端对端的直接通信，而无需经过中间服务器的转发。

协议

服务器与客户端之间的通信使用TCP，传递的数据以包为单位。一般来说，客户端与服务器的交互是请求—响应式的，同时为了提高聊天的实时性，也支持服务器主动推送消息数据包。

每一个数据包的格式统一如下：

```
0      3  4  5  ...
+-----+----+-----...
|  长度  | 类型 | 数据...
+-----+----+-----...
```

其中，`长度` 存放 `数据` 的长度（用于解决黏包问题，见下），`类型` 表示 `数据` 中存放的对象的类型，`数据` 存放使用protobuf序列化为字节串的对象，即数据包的实际内容。

根据类型的不同，数据包可分为以下几种：

- `LoginRequest`：客户端登录时发送此请求来登录。
- `LoginResponse`：服务器对登录请求的响应，告知客户端是否登录成功、用户未找到或者密码错误。
- `RegisterRequest`：客户端注册新用户请求。
- `RegisterResponse`：服务器对注册请求的响应，告知是否注册成功或者用户已存在。
- `ListUserRequest`：请求列出所有用户。
- `ListUserResponse`：所有用户的列表，包括用户名、用户号以及在线情况。
- `ListBuddyRequest`：请求列出所有好友。
- `ListBuddyResponse`：所有好友的列表，包括用户名、用户号以及在线情况。
- `AddBuddyRequest`：添加好友请求。
- `AddBuddyResponse`：服务器对添加好友请求的响应，告知是否成功，或者用户未找到等错误。
- `Message`：客户端之间通过服务器转发的数据包。

具体定义可以参见 `chat.proto`。

实际上，对于请求和响应（以结尾的 `Request` 或 `Response` 类型）类型的数据包，由于客户端一定发送请求，服务端一定发送响应，所以对于此类数据包，在 `类型` 中请求和响应可以使用相同的数值来表示。

Message 的特别说明

特别地，`Message` 数据包是本程序的核心，承载所有客户端到客户端的数据，它详细定义如下：

```
message Message {
    enum Type {
        MESSAGE = 0;
        FILE = 1;
        INPUTING = 2;
        GRAPHICS = 3;
    }
    uint32 uid = 1;
    uint64 timestamp = 2;
    Type type = 3;
    string msg = 4;
    bytes data = 5;
    string token = 6;
}
```

- `uid`：表示对端用户号，比如，客户端向服务器发送时，此字段表示目标用户号，服务器向客户端转发时，此字段则表示为源用户号。
- `timestamp`：一个Unix时间戳，服务器转发数据包时设置。
- `type`：这个数据包的类型，由客户端设置和解析。
- `msg`：字符串型数据。发送文件时，是文件的文件名。
- `data`：二进制字节串数据。发送文件时，是文件的内容。
- `token`：令牌（暂未使用）。

黏包与接收不全问题

由于TCP是可靠的面向字节流的传输层协议，它不保证保留消息边界，即多次 `send` 的数据可能一次 `recv` 就能够接收，或一次 `send` 的数据可能需要分多次 `recv` 接收。这里我采用“字符计数法”，发送时先发长度再发数据，接收的时候先接收长度，再循环接收，直到收到相应长度的数据才停止，就可以确保收到大小正确的应用层数据包了。

功能实现

即时聊天

这个功能使用 `MESSAGE` 类型的 `Message` 数据包实现，客户端发送数据包到另外一个客户端来完成聊天信息的发送，客户端收到数据包后显示出来完成聊天信息的接收与显示。

文件传输

这个功能实际上和“即时聊天”类似，只不过传输的内容由聊天文本信息变为文件名和文件内容。发送文件时，客户端提示用户选择需要发送的文件，然后读取文件内容并封装成消息数据包，交给服务器转发。若客户端收到一个文件类型的消息数据包，则提示用户保存文件，用户可以指定保存位置，或者选择不接收（不保存）。

“正在输入”的提示

这个功能使用 `INPUTING` 类型的 `Message` 数据包实现，当客户端检测到聊天窗口中待发送内容文本框的内容变化（即 `TextBox` 的 `TextChanged` 事件被触发）后，会给对方发送“正在输入”消息数据包，从而使得对方显示“正在输入...”字样。

为了减少网络使用，提高效率，“正在输入”的消息数据包隔至少一秒才发一次，同时，为确保显示的连续性，每次收到对方的“正在输入”消息数据包会持续显示“正在输入...”字样一秒。

共享画板

为了实现共享画板，需要实现绘画信息的传输。我的实现中，用户画的图线可分解为一个一个线段，每当用户画一笔，客户端就会将该线段的首末坐标封装成图形消息数据包发给服务器进行转发，同样，收到图形消息数据包后，解析其中线段的首末坐标，并绘制到界面上，从而完成画板的实时共享。

缓存数据包

服务器在客户端不在线时还有缓存数据包的能力，能够在客户端上线的时候将缓存的数据包统一发给客户端。这需要在服务器转发数据包时判断客户端是否在线，若不在线则存放到一个临时的队列或其他数据结构中，下次客户端登录时统一发给客户端即可。

唯一性保证

服务器能够保证已登录用户的唯一性，即某一个用户同一时间只能在一个客户端进程登录。若用户重复登录，服务器在登录时会将之前的会话杀死，维持唯一性。若没有唯一性保证，服务器在转发数据包时会发生混乱。

TLS

这个功能使用OpenSSL来实现，只需要在服务器或客户端程序开始运行时初始化SSL环境，创建连接的时候初始化SSL连接，以后发送或接收数据使用 `SSL_write` 或 `SSL_read` 替代 `send` 或 `recv` 即可。服务器还需要一个配有私钥的证书（可以是自签名的）用于非对称加密，客户端保存证书的SHA1指纹用于验证（安全性有待考证，比对整个证书来验证可能更安全）。证书使用OpenSSL命令行工具来生成。

为测试正确使用了TLS，我对客户端和服务器的连接进行了抓包。

未加密

```

00000000 00 00 00 2a ...*
00000004 fe 54 68 69 73 20 69 73 20 61 20 63 68 61 74 20 .This is
a chat
00000014 73 65 72 76 65 72 2e 20 48 65 6c 6c 6f 2c 20 31 server.
Hello, 1
00000024 39 32 2e 31 36 38 2e 31 2e 32 21 92.168.1
.2!
00000000 00 00 00 0e 00 .....
00000005 0a 04 74 77 64 32 12 06 31 32 33 34 35 36 ..twd2..
123456
0000002F 00 00 00 02 ....
00000033 00 10 01 00 00 00 16 03 0a 0a 08 01 12 04 74 77 .....
.....tw
00000043 64 32 18 01 0a 08 08 02 12 04 74 77 64 33 d2.....
..twd3
00000013 00 00 00 00 03 .....
00000051 00 00 00 16 ....
00000055 03 0a 0a 08 01 12 04 74 77 64 32 18 01 0a 08 08 .....t
wd2.....
00000065 02 12 04 74 77 64 33 ...twd3
00000018 00 00 00 00 03 .....
0000006C 00 00 00 16 ....
00000070 03 0a 0a 08 01 12 04 74 77 64 32 18 01 0a 08 08 .....t
wd2.....
00000080 02 12 04 74 77 64 33 ...twd3
0000001D 00 00 00 09 06 .....
00000022 08 02 1a 05 68 65 6c 6c 6f ....hell o
0000002B 00 00 00 00 03 .....
00000087 00 00 00 16 ....
0000008B 03 0a 0a 08 01 12 04 74 77 64 32 18 01 0a 08 08 .....t
wd2.....
0000009B 02 12 04 74 77 64 33 ...twd3
00000030 00 00 00 00 03 .....
000000A2 00 00 00 16 ....
000000A6 03 0a 0a 08 01 12 04 74 77 64 32 18 01 0a 08 08 .....t
wd2.....
000000B6 02 12 04 74 77 64 33 ...twd3
00000035 00 00 00 1d 06 .....
0000003A 08 02 1a 19 54 68 69 73 20 69 73 20 61 20 73 65 ....This is a
se
0000004A 63 72 65 74 20 6d 65 73 73 61 67 65 2e cret mes sage.
00000057 00 00 00 00 03 .....
000000BD 00 00 00 16 ....
000000C1 03 0a 0a 08 01 12 04 74 77 64 32 18 01 0a 08 08 .....t
wd2.....
000000D1 02 12 04 74 77 64 33 ...twd3

```

使用TLS v1.2

```

00000000 16 03 03 00 9e 01 00 00 9a 03 03 5a 3d 3b 7a 4b .....
...Z=;zK
00000010 27 0f 2c 1c 84 e6 4d 2e 37 90 3d 52 29 e0 14 81 '.,...M.
7.=R)...
00000020 6c 33 89 0d ca a8 90 ba 5d 31 5a 00 00 3c c0 2c 13..... j1Z..
<.,
00000030 c0 2b c0 30 c0 2f 00 9f 00 9e c0 24 c0 23 c0 28 .+.0./..
...$.#.(
00000040 c0 27 c0 0a c0 09 c0 14 c0 13 00 39 00 33 00 9d .'.....
...9.3..
00000050 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 00 6a 00 40 ...=.<.5
./...j.@
00000060 00 38 00 32 00 13 00 05 00 04 01 00 00 35 00 0a .8.2....
.....5..
00000070 00 06 00 04 00 17 00 18 00 0b 00 02 01 00 00 0d .....
.....
00000080 00 14 00 12 06 01 06 03 04 01 05 01 02 01 04 03 .....
.....
00000090 05 03 02 03 02 02 00 23 00 00 00 17 00 00 ff 01 .....#
.....
000000A0 00 01 00 ...
00000000 16 03 03 00 35 02 00 00 31 03 03 ae 34 ee 8c bd ....5...
1...4...
00000010 83 65 93 00 62 da 4e 63 2e e1 ad 6c af 22 be f7 .e..b.Nc
...1."..
00000020 c0 c7 a0 fa 47 84 6e b0 07 62 81 00 00 9d 00 00 ....G.n.
.b.....
00000030 09 ff 01 00 01 00 00 23 00 00 16 03 03 03 0a 0b .....#
.....
00000040 00 03 06 00 03 03 00 03 00 30 82 02 fc 30 82 01 .....
.0...0..
00000050 e4 02 09 00 dd b1 31 a7 7b 2b 43 0f 30 0d 06 09 .....1.
{+C.0...
00000060 2a 86 48 86 f7 0d 01 01 0b 05 00 30 40 31 0b 30 *.H.....
...0@1.0
00000070 09 06 03 55 04 06 13 02 43 4e 31 0c 30 0a 06 03 ...U....
CN1.0...
00000080 55 04 08 0c 03 4e 2d 41 31 0d 30 0b 06 03 55 04 U....N-A
1.0...U.
00000090 0a 0c 04 74 77 64 32 31 14 30 12 06 03 55 04 03 ...twd21
.0...U..
000000A0 0c 0b 63 68 61 74 2e 73 65 72 76 65 72 30 1e 17 ..chat.s
erver0..
000000B0 0d 31 37 31 32 32 32 31 36 30 39 32 33 5a 17 0d .1712221
60923Z..
000000C0 32 37 31 32 32 30 31 36 30 39 32 33 5a 30 40 31 27122016
0923Z0@1
000000D0 0b 30 09 06 03 55 04 06 13 02 43 4e 31 0c 30 0a .0...U..
..CN1.0.

```

000000E0	06 03 55 04 08 0c 03 4e 2d 41 31 0d 30 0b 06 03	..U....N -
A1.0...		
000000F0	55 04 0a 0c 04 74 77 64 32 31 14 30 12 06 03 55	U....twd
21.0...U		
00000100	04 03 0c 0b 63 68 61 74 2e 73 65 72 76 65 72 30chat
.server0		
00000110	82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01	.."0...*
.H.....		
00000120	05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 000
.....		
00000130	ac d2 60 ca e0 35 ff a1 b9 5e 26 c1 68 27 b2 fd	..`.5..
.^&.h'..		
00000140	e7 7e a2 1d 56 91 16 93 2d fd 93 e1 33 9b 81 b7	~..V...
....3...		
00000150	b0 3b 40 3a 59 e3 64 4a 8d aa 6a 2c 3f eb 3f b8	.;@:Y.dJ
..j,?.?.		
00000160	66 63 53 26 22 eb 4f 88 cd 10 29 56 a6 02 3f 1c	fcS&".O.
..)V...?.		
00000170	8b c9 ee c7 50 79 ac 45 f1 75 5e 88 17 e8 c0 75Py.E
.u^.....u		
00000180	04 a8 d2 46 b1 c4 44 01 93 b9 48 b1 64 0f 93 b8	...F...D.
..H.d...		
00000190	b4 74 26 6c a6 e8 82 7e 60 76 2b e4 5d 44 71 32	.t&l....~
`v+.]Dq2		
000001A0	f0 85 79 c4 9b 59 f1 a9 e3 da d5 7f d5 be 35 94	..y..Y..
.....5.		
000001B0	7d 7d 74 d0 96 7e f5 cb 35 cd a8 e3 ff 31 e8 c1	}}t...~..
5....1..		
000001C0	a0 22 44 30 bd e2 b3 c5 3d 07 0c b8 49 51 37 db	."D0....
=...IQ7.		
000001D0	ee 74 a3 c9 d7 69 ff 11 f2 4f b7 94 f2 42 dd 48	.t...i..
.O...B.H		
000001E0	c9 86 4d b1 52 bc 00 2e 78 51 02 86 61 3d 3c a2	..M.R...
xQ...a=<.		
000001F0	00 f3 c9 3d d1 8e c8 9e 1e 53 1e fc 26 9f 74 b6	...=....
.S...&.t.		
00000200	c2 3e 5d 89 3a 85 fb 53 f9 fd 56 35 af 35 e5 2e	.>]...:S
..V5.5..		
00000210	01 83 4f aa cc 2d 35 6f b4 34 7b 4f 1b 82 f2 ab	..O...-5o
.4{O....		
00000220	e3 24 80 4d e1 0b d9 ec 3d 8d 97 56 0a cd 72 e5	.\$..M....
=..V...r.		
00000230	02 03 01 00 01 30 0d 06 09 2a 86 48 86 f7 0d 010..
.*.H....		
00000240	01 0b 05 00 03 82 01 01 00 8a 90 3c 4b 2a bc a7
...<K*..		
00000250	eb e8 8e 63 65 02 56 4d 5f 76 04 48 c7 5f a5 be	...ce.VM
v.H...		

```

00000260 2e 02 60 3f cb 0f 5a df 75 ba a7 61 53 7f 3b 5e ..`?...Z.
u..aS.;^
00000270 1c 0a f3 f5 81 34 1f 4d 80 c5 39 1c f6 c1 58 a3 .....4.M
..9...X.
00000280 67 11 84 9f 2c 91 93 90 2d 1b 4f 87 53 4a ef f0 g....,...
-.O.SJ..
00000290 3a c9 f5 5e 73 ad 19 6b 0c 0b ac 77 db 51 bd 85 :...^s..k
...w.Q..
000002A0 bb ec 18 39 68 d2 bf a6 b6 8f 4f f0 5d 5a 22 71 ...9h...
..O.]Z"q
000002B0 fd 5f c0 28 61 9c 2c a2 fa 77 5c 39 2a 7d dc 05 .._(a.,.
.w\9*}..
000002C0 c6 85 5c 97 a0 4a c8 7d 7b 4a 7f b8 a3 53 ff 58 ..\...J.}
{J...S.X
000002D0 9f 9c 8c fa 1c 63 97 e1 ec 60 fb 0b f5 a6 ce ff .....c..
..`.....
000002E0 c2 f0 90 17 30 95 35 d1 e3 9e ae f0 5f 40 6e 02 ....0.5.
...._@n.
000002F0 45 cc e2 d2 08 72 54 d0 42 ae 37 d0 18 95 0b 61 E....rT.
B.7....a
00000300 49 70 11 59 c7 0a 9d 89 ae af 8e 80 5a 06 3d 80 Ip.Y....
....Z.=.
00000310 63 b4 26 fc 11 28 5a 6d 68 24 ce cf eb bf 6b 0e c.&...(Zm
h$.k.
00000320 5d 2e 05 bf 4c 65 79 8c b4 2f 47 1e 84 a7 f0 15 ]...Ley.
./G.....
00000330 32 b0 77 15 a5 ca 2f 6f 1d 30 8b b0 84 af fd 37 2.w.../o
.0.....7
00000340 ae 24 64 43 82 e1 0e 94 99 16 03 03 00 04 0e 00 .$dC....
.....
00000350 00 00 ..
000000A3 16 03 03 01 06 10 00 01 02 01 00 7d c4 4b 6c 52 .....
...}.KlR
000000B3 27 b7 19 f9 39 bc e2 1c 19 7b 4f c0 fb 5a 54 50 '...9... .
{O..ZTP
000000C3 85 e0 b6 93 7c 86 29 8d 57 34 1b 44 34 5f 7b cd ....|.)).
W4.D4_{.
000000D3 d8 c9 68 cb ff 77 35 9c 8e ba 45 90 ba 62 8c 35 ..h..w5.
..E..b.5
000000E3 10 66 00 f8 d1 86 e7 ee 35 d6 9d 38 6b b5 0e 46 .f.....
5..8k..F
000000F3 c2 f4 46 a4 1d 99 28 1e c2 0f 9d 81 c0 62 bf 46 ..F...(.
....b.F
00000103 75 d6 46 b8 c0 b9 48 42 d7 e2 9b a9 b2 59 af b5 u.F...HB
.....Y..
00000113 57 4a cd 61 87 d2 d3 77 3a 23 2f d2 7d 95 5c 16 WJ.a...w
:#/.)\..
00000123 22 bd 2f 66 0a 5b a3 37 6d c9 ab 8d 0b 11 33 17 "./f.[.7
m.....3.

```

00000133 b2 6d 63 26 a3 fc 23 97 9b 32 c8 3b 37 c1 47 6d .mc&...#. .2.;7.Gm
00000143 76 95 3b 78 a1 eb 4c 04 c4 8e 8d 03 0a 4f c4 41 v.;x...L.O.A
00000153 13 21 9f 9a a9 ec 0e 75 df f9 33 ab 96 e3 b8 e4 .!.....u ..3.....
00000163 83 ba 0a df 2c c1 62 7a 56 92 83 41 a3 44 91 a2,bz V..A.D..
00000173 2f 04 6c ba 55 eb 8b 93 bd 44 d0 cf 93 cf e3 3a /.1.U... .D.....:
00000183 98 66 b6 a0 90 e6 f9 4d 49 4e e9 54 5b a6 32 61 .f.....M IN.T[.2a
00000193 73 3f 15 d4 bb 27 e2 09 0a 7f ab 15 cd a6 4c 4e s?...'.LN
000001A3 39 8b 69 3c c4 31 b7 9c 3e f8 15 14 03 03 00 01 9.i<.1.. >.....
000001B3 01 16 03 03 00 28 00 00 00 00 00 00 00 00 6a 46,jF
000001C3 c0 e6 ac 02 0a 65 66 15 43 bf 8b 19 99 3c cd e2ef. C.... <..
000001D3 00 bd eb af f2 67 98 29 e7 e3 27 db 15 dag.) ..'...
00000352 16 03 03 00 aa 04 00 00 a6 00 00 1c 20 00 a0 43C
00000362 6e 90 7e 67 7e f9 63 04 04 af b4 07 23 e7 02 2e n.~g~.c.#...
00000372 a0 49 00 14 5f c2 e0 5c 58 f9 5a d5 9d 44 27 12 .I..._.. \ X.Z..D'.
00000382 ba dc 5a a9 ce be 83 d3 d4 a1 d6 5b 9d 54 63 8f ..Z..... ...[.Tc.
00000392 54 b3 b4 24 cb 94 75 18 b9 46 12 6b 63 64 db 17 T..\$.u. .F.kcd..
000003A2 80 a2 ac b8 4d 8b c2 f8 a8 fe 67 ee 51 86 07 48M... ..g.Q..H
000003B2 fe c3 83 1d 56 08 41 38 3a f9 9f 02 a0 50 3b 07V.A8 :....P;..
000003C2 97 62 f0 ce 2c 1b c4 3c 29 9f 50 e2 88 4f 85 17 .b...,...<).P..O..
000003D2 87 84 45 12 78 ca dc 62 8a ee 81 13 e2 c1 29 64 ..E.x..b)d
000003E2 e0 d8 cc bf 3c 13 9f 4d 39 23 da 04 10 7b 45 0e<..M 9#...{E.
000003F2 72 66 c0 fa 73 e9 fe 3b 52 b5 91 ee 71 36 65 14 rf..s...; R...q6e.
00000402 03 03 00 01 01 16 03 03 00 28 6e e1 82 99 4b 71 (n...Kq
00000412 5c bc 3c 5d 27 a5 2b d1 e3 30 f1 28 c7 8e 8d 9c \.<]'..+. .0.(....


```

00000422 31 07 65 6d f5 22 83 6e 2a db 74 b1 78 df f8 0a 1.em."n
*.t.x...
00000432 78 44 xD
00000434 17 03 03 00 1c 6e e1 82 99 4b 71 5c bd d0 d7 eb .....n..
.Kq\....
00000444 83 54 71 80 b6 11 6f 74 82 9d 10 05 f8 ad 33 ad .Tq...ot
.....3.
00000454 d6 17 03 03 00 19 6e e1 82 99 4b 71 5c be a5 6b .....n.
..Kq\..k
00000464 3d f3 b3 bf a9 76 37 4c 22 d2 67 e8 46 dd e4 17 =....v7L
".g.F...
00000474 03 03 00 42 6e e1 82 99 4b 71 5c bf d0 e5 4c 95 ...Bn...
Kq\...L.
00000484 de 14 1d a8 6c 9c 58 05 5a d6 56 52 c6 d7 8e 85 ....l.X.
Z.VR....
00000494 3f 52 07 42 21 bd ca 32 50 35 86 a7 71 38 b2 ed ?R.B!...2
P5..q8..
000004A4 3e 4e 44 96 0e e8 2a 45 a2 4f ec 7f 41 41 d5 ad >ND...*E
.O..AA..
000004B4 b4 d2 27 db b4 0e ...'...
000001E1 17 03 03 00 1d 00 00 00 00 00 00 00 01 4e 85 33 .....
.....N.3
000001F1 b4 f1 cb 4d 07 a6 00 18 3d 29 11 28 4e 4d ea e1 ...M.... =).
(NM..
00000201 2f 7c /|
00000203 17 03 03 00 26 00 00 00 00 00 00 00 02 57 2d 24 ....&...
.....W-$
00000213 55 78 df ab ab 49 c1 fa 9f 13 b0 f4 fd 4a 55 7a Ux...I..
.....JUz
00000223 2d 7f aa 59 ae 75 3a 44 88 41 23 -..Y.u:D .A#
000004BA 17 03 03 00 1c 6e e1 82 99 4b 71 5c c0 9e ce 0d .....n..
.Kq\....
000004CA 25 35 3c 0a b9 b9 74 64 85 a0 51 9e a1 c9 19 26 %5<...td
..Q....&
000004DA 9a .
000004DB 17 03 03 00 19 6e e1 82 99 4b 71 5c c1 a4 10 ff .....n..
.Kq\....
000004EB f5 0d 07 e6 c3 9d 9a fc fc 35 33 9c 26 d5 17 03 .....
.53.&...
000004FB 03 00 1a 6e e1 82 99 4b 71 5c c2 8f c4 82 17 9d ...n...K
q\.....
0000050B bc 4b 9c fe 9f 64 97 6c 07 ad 74 ea fc 17 03 03 .K...d.l
..t.....
0000051B 00 1c 6e e1 82 99 4b 71 5c c3 4f ac dd 25 f0 03 ..n...Kq
\..O..%..
0000052B 71 e8 58 17 fb a6 2b 7d ed 25 47 ba e3 56 17 03 q.X...+}
.%G..V..
0000053B 03 00 19 6e e1 82 99 4b 71 5c c4 15 1b e8 4a b5 ...n...K
q\....J.

```

0000054B 44 e7 c6 6a 4f 53 42 b7 10 ae 9e 55 17 03 03 00 D..jOSB.
...U....
0000055B 2e 6e e1 82 99 4b 71 5c c5 38 7c 51 ce 61 dc b5 .n...Kq\
.8|Q.a..
0000056B 74 6e d1 48 0b dd 14 65 38 ea 2a f7 2e 2a 3d 91 tn.H...e
8.*...*=.
0000057B 3c 61 f1 fd ff 2f 54 34 d7 84 e5 eb df 95 e9 <a.../T4
.....
0000022E 17 03 03 00 1d 00 00 00 00 00 00 00 03 c4 6c d1
.....l.
0000023E 52 12 dd 39 4c dd cb 4c 5b f4 45 60 eb 62 36 66 R..9L..L
[.E`.b6f
0000024E 0b 76 .v
0000058A 17 03 03 00 1c 6e e1 82 99 4b 71 5c c6 05 bc 99n..
.Kq\....
0000059A 23 82 72 d0 84 ae c6 51 bf 65 ff ec 77 78 d6 60 #.r....Q
.e..wx.`
000005AA d6 .
00000250 17 03 03 00 18 00 00 00 00 00 00 00 04 7b 40 d7
{@.
00000260 dc 12 a4 da 3f d4 bb 11 9f f5 04 fd 2b?... ..+
000005AB 17 03 03 00 19 6e e1 82 99 4b 71 5c c7 3f 43 b9n..
.Kq\.?C.
000005BB 3c 0e 68 73 72 79 0a 7c 02 10 8d 5e 39 28 <.hsry.|
...^9(
000005C9 17 03 03 00 2e 6e e1 82 99 4b 71 5c c8 ce e3 7dn..
.Kq\...}
000005D9 3c e5 c0 84 98 eb c1 39 02 1c d9 9e a8 1f 87 25 <.....9
.....%
000005E9 4e 7e d7 96 7d 28 ad d3 2d e4 a8 03 4a bb 1a 1c N~..}{(..
-...J...
000005F9 fc 25 9f .%.
0000026D 17 03 03 00 1d 00 00 00 00 00 00 00 05 cd 7a e1
.....z.
0000027D c1 3d 23 6b 79 53 d6 4e f4 ba a3 a4 1b e7 36 9f .=#kyS.N
.....6.
0000028D e8 64 .d
000005FC 17 03 03 00 1c 6e e1 82 99 4b 71 5c c9 e5 f4 6en..
.Kq\...n
0000060C 9d 22 7e 3a f3 8d 45 83 cd 0a 9f d4 32 58 20 2e ."~:...E.
....2X .
0000061C 86 .
0000028F 17 03 03 00 18 00 00 00 00 00 00 00 06 44 5f 64
.....D_d
0000029F d9 f2 11 98 e9 31 a9 99 3d b9 0b de 941.. =....
0000061D 17 03 03 00 19 6e e1 82 99 4b 71 5c ca 4e c2 63n..
.Kq\..N.c
0000062D eb 5b 30 28 15 33 03 c9 c0 fb d5 be cc aa 17 03 .[0(.3..
.....

```
0000063D 03 00 2e 6e e1 82 99 4b 71 5c cb bf 50 68 ce a0 ...n...K
q\..Ph..
0000064D a2 5f f5 40 ef c8 7e 76 41 32 f9 00 c3 28 00 71 ...@...~v
A2...(.q
0000065D 7f e5 fd 48 96 cb 5e 3b 17 f7 7f 3a a6 96 8e 20 ...H...^;
....:....
0000066D 74 t
000002AC 17 03 03 00 1d 00 00 00 00 00 00 00 07 d5 a0 82 .....
.....
000002BC 45 db 80 d6 62 3b 7e ef ba e3 5c fc 32 04 5c a6 E...b;~.
..\2.\.
000002CC 7b 0e {.
000002CE 17 03 03 00 21 00 00 00 00 00 00 00 08 c6 53 c9 ....!...
.....S.
000002DE 12 26 e3 19 9f e6 f8 da 36 e2 e0 cd 06 9c 08 f5 .&.....
6.....
000002EE 5a 54 53 fe e7 33 ZTS..3
000002F4 17 03 03 00 1d 00 00 00 00 00 00 00 09 ab b7 bc .....
.....
00000304 c5 98 e0 da 59 b7 bf 65 19 0a be 3b 9f 39 23 3f ....Y...e
...;.9#?
00000314 81 60 .^
00000316 17 03 03 00 18 00 00 00 00 00 00 00 0a d6 42 28 .....
.....B(
00000326 07 43 7d 85 17 41 af 35 a7 d4 f0 87 dd .C}..A.5 .....
0000066E 17 03 03 00 1c 6e e1 82 99 4b 71 5c cc 86 0b 90 .....n..
.Kq\....
0000067E a9 6d 2b e2 86 c3 02 c9 e0 1b 75 ab 06 87 c5 9d .m+.....
..u.....
0000068E 68 h
0000068F 17 03 03 00 19 6e e1 82 99 4b 71 5c cd a3 ec 92 .....n..
.Kq\....
0000069F 9c 57 02 89 9d 44 a5 d7 d1 c1 05 54 5a e7 17 03 .W...D..
...TZ...
000006AF 03 00 2e 6e e1 82 99 4b 71 5c ce 06 33 aa 5c ac ...n...K
q\..3.\.
000006BF 8b 6f 0e 20 e7 cf 00 68 8d 89 7a b4 76 3a 28 1f .o. ...h
..z.v:(.
000006CF 73 b6 d4 c1 b6 c0 2b 91 2b e6 e2 75 9d e1 61 57 s.....+.
+..u...aW
000006DF 32 2
00000333 17 03 03 00 1d 00 00 00 00 00 00 00 0b 72 b2 5a .....
.....r.Z
00000343 6b bf a5 83 e5 e2 67 38 85 1f ba 44 84 7d 9b e1 k.....g8
...D.}..
00000353 89 4a .J
000006E0 17 03 03 00 1c 6e e1 82 99 4b 71 5c cf 8d 40 2d .....n..
.Kq\...@-
```

```

000006F0 07 bf d5 b0 45 66 c9 03 ea 9d 04 c3 be d7 c7 8b ....Ef..
.....
00000700 f3 .
00000355 17 03 03 00 18 00 00 00 00 00 00 00 0c b0 9a 54 .....
.....T
00000365 ff 65 99 bb 17 b1 e9 a3 fd c6 38 e6 4d .e..... ..8.M
00000701 17 03 03 00 19 6e e1 82 99 4b 71 5c d0 b4 cc 38 .....n..
.Kq\...8
00000711 c9 79 07 fd c0 32 24 ca 29 a7 44 fc 0a ab 17 03 .y...2$.
).D.....
00000721 03 00 2e 6e e1 82 99 4b 71 5c d1 72 ce 9e 08 95 ...n...K
q\.r....
00000731 ae 21 a6 c0 a7 c8 b1 8c 5f 37 b9 de 1d 0a 23 d3 .!.....
_7....#.
00000741 0f fd 13 d2 0f 06 97 11 a6 51 94 42 28 93 da d6 .....
.Q.B(...)
00000751 db .
00000372 17 03 03 00 1d 00 00 00 00 00 00 00 0d 06 8d 1d .....
.....
00000382 d8 27 9d 16 13 86 2c cf 4b c8 c3 f3 3a ba 91 83 .'.....,
K...:...
00000392 74 ec t.
00000394 17 03 03 00 35 00 00 00 00 00 00 00 0e 16 c5 a5 ....5...
.....
000003A4 87 ed 49 dd 26 6d 79 da e4 4b bc 77 da 14 6b 47 ..I.&my.
.K.w..kG
000003B4 37 0c 44 8c a4 8a ed 85 db 06 96 ff d1 e0 8c c8 7.D.....
.....
000003C4 3f 0c ee 08 1a 84 9c d4 74 7d ?..... t}
000003CE 17 03 03 00 1d 00 00 00 00 00 00 00 0f ff e1 84 .....
.....
000003DE 5e 5c 94 fd 16 28 bc 8e 97 cd 4a 3d a4 0a fd 46 ^\...(..
..J=...F
000003EE 66 5d f]
000003F0 17 03 03 00 18 00 00 00 00 00 00 00 10 5b c8 96 .....
[...
00000400 7e 6f ea e6 4e 7e a8 9f e2 2a c3 3c 3e ~o..N~... *.<>
00000752 17 03 03 00 1c 6e e1 82 99 4b 71 5c d2 f2 72 16 .....n..
.Kq\..r.
00000762 2f 07 af 09 b9 31 93 3d 56 56 d6 fb 7d 67 7e 54 /....1.=
VV..}g~T
00000772 be .
00000773 17 03 03 00 19 6e e1 82 99 4b 71 5c d3 30 52 5a .....n..
.Kq\..0RZ
00000783 7c 53 63 22 54 05 1c 0d 36 57 7b 05 1b 5d 17 03 |Sc"T...
6W{...}..
00000793 03 00 2e 6e e1 82 99 4b 71 5c d4 17 72 f9 71 1e ...n...K
q\..r.q.

```

```
000007A3 b9 09 3f 83 21 81 f6 80 df 9e 7a c7 93 ba 89 a8 ..?.!...
..z.....
000007B3 cc ca 38 31 3e 33 bd 96 e3 cc 41 64 57 8f cb 96 ..81>3..
..AdW...
000007C3 5a                                     Z
```

可以看出，在未加密的时候，用户登录的密码以及秘密消息均为明文，加密后就看不出来了。可见，确实成功加密了。

思考题

1. Socket与文件的关系

在调用 `socket(2)` 创建socket时，内核会创建一个socket内核对象，同时分配一个文件描述符并将其映射到这个socket内核对象。之后调用 `write(2)` 或 `read(2)` (`send(2)` 以及 `recv(2)` 只是多了标志位、地址等参数) 进行写或者读操作的时候就可以利用文件描述符，像访问通过 `open(2)` 打开的文件一样访问socket了。

2. 服务器程序的角色

在设计思路中已经说明，服务器程序的核心角色就是包转发器。

3. 服务器端口与客户端连接个数的关系

在本程序中，服务器使用TCP的1025端口监听客户端的连接请求，和客户端进行通信；客户端则通过一个临时的端口和服务器创建连接。无论有多少客户端，服务器都使用相同的端口发送和接收数据，而用对方的地址和对方的端口号来唯一标识每一个连接。

总结和收获

这个实验算是本课程的大实验，我在完成这个实验的过程中用到了socket、C++ 11的多线程及互斥体、protobuf库以及OpenSSL库。

Socket是网络开发一定会使用的，而多线程是并发程序的关键，也是网络程序的关键，通过使用它们来完成本次实验，我对于网络程序的开发及其设计思想的理解更加深刻了。

此外，这一次我还尝试使用了两个外部库，protobuf以及OpenSSL，方便快捷地实现了数据对象的序列化以及TLS加密层的安装，加强了我使用外部网络库的能力。