

Санкт-Петербургский Политехнический Университет Петра Великого  
Институт компьютерных наук и технологий  
Кафедра компьютерных систем и программных технологий

# Сети и телекоммуникации

Отчет по лабораторной работе №1  
Программирование сокетов протоколов TCP и UDP

**Работу**  
**выполнил:**  
Коренёк Г.А.  
Группа: 43501/3  
**Преподаватель:**  
Алексюк А.О.

Санкт-Петербург  
2017

# Содержание

<b>1. Цель работы</b>	<b>2</b>
<b>2. Программа работы</b>	<b>2</b>
<b>3. Ход выполнения работы</b>	<b>2</b>
3.1. Простейшие клиент и сервер . . . . .	2
3.2. Индивидуальное задание . . . . .	2
3.2.1. Реализация на TCP . . . . .	3
3.2.2. Реализация на UDP . . . . .	4
3.3. Дополнительное задание . . . . .	4
3.3.1. Подключение к веб-серверу и запрос веб-страницы . . . . .	4
3.3.2. Запрос списка файлов и загрузка файла с ftp-сервера . . . . .	4
3.3.3. Отправка письма на SMTP-сервер . . . . .	6
3.3.4. Получение письма с POP3-сервера . . . . .	8
<b>4. Выводы</b>	<b>11</b>

# 1. Цель работы

Изучение принципов программирования сокетов протоколов TCP и UDP.

# 2. Программа работы

- разработать простейший клиент и сервер на основе протоколов TCP и UDP
- разработать прикладной протокол в соответствии с индивидуальным заданием, реализовать протокол в виде клиент-серверного приложения на основе протоколов TCP и UDP
- выполнить дополнительное задание

# 3. Ход выполнения работы

## 3.1. Простейшие клиент и сервер

Простейшие клиент и сервер были выполнены на основе протоколов TCP и UDP, а также адаптированы под ОС Windows и Linux. Сервер выполняет функции эхо-сервера, т.е. принимает сообщения от клиентов и посылает копии обратно. Клиент посылает сообщение, после чего завершается.

## 3.2. Индивидуальное задание

В качестве индивидуального задания была выбрана система обмена мгновенными сообщениями. Сервер реализован на Windows, клиент - на Linux.

Серверное приложение реализует следующие функции:

- Прослушивание определенного порта
- Обработка запросов на подключение по этому порту от клиентов
- Поддержка одновременной работы нескольких клиентов через механизм нитей
- Передача текстового сообщения одному клиенту
- Передача текстового сообщения всем клиентам
- Прием и ретрансляция входящих сообщений от клиентов
- Обработка запроса на отключение клиента
- Принудительное отключение указанного клиента

Клиентское приложение реализует следующие функции:

- Установление соединения с сервером
- Передача сообщения всем клиентам
- Передача сообщения указанному клиенту
- Прием сообщения от сервера с последующей индикацией

- Разрыв соединения
- Обработка ситуации отключения клиента сервером

Разработанное клиентское приложение предоставляет пользователю настройку IP-адреса или доменного имени сервера сообщений и номера порта сервера.

### 3.2.1. Реализация на ТСР

Для реализации данной системы был разработан текстовый асинхронный протокол. Его схема для реализации на ТСР представлена на рис. 3.1

Текстовый асинхронный протокол

источник	заголовок	опции	сообщение
клиент	Запрос на ретрансляцию сообщения (ret_msg)	Имя получателя, длина сообщения	Сообщение
	Запрос на ретрансляцию сообщения всем клиентам (ret_bcm)	Длина сообщения	Сообщение
	Запрос на отключение (dics_me)	-	-
	Запрос на авторизацию (auth_me)	Имя пользователя	-
сервер	Входящее сообщение (inc_msg)	Имя отправителя, длина сообщения	Сообщение
	Сообщение об ошибке (err_msg)	Длина сообщения	Сообщение

Рисунок 3.1. Схема прикладного протокола для реализации на ТСР

Сообщение всегда содержит, как минимум, поле заголовка, определяющее тип сообщения. Некоторые типы сообщений содержат также поле опций. Для типов сообщений, содержащих данные (собственно пользовательское сообщение), в поле опций, кроме прочего, указывается длина сообщения, чтобы принимающая сторона принимала нужное число символов.

Сервер имеет 1 слушающий порт, по которому принимает от клиентов запросы на соединение. При подсоединении очередного клиента, для связи с ним выделяется отдельный сокет, прием из которого осуществляется в отдельном потоке. Для дальнейшего управления порожденными потоками (например, завершение потока при получении от клиента запроса на отключение) при подключении клиента осуществляется вставка в хэш-таблицу id его сокета в качестве ключа и id потока в качестве значения.

После подключения клиента сервер ожидает приема 8 символов заголовка. Допустимые значения заголовков хранятся в хэш-таблице в качестве ключа. В качестве значения в ней хранятся ссылки на функции-обработчики. При совпадении принятого заголовка с имеющимся в таблице происходит вызов соответствующего обработчика.

Обработчик, в зависимости от соответствующего типа сообщения, может содержать вызовы для приема оставшейся части сообщения - опций и данных.

Для управления сервером предусмотрен поток для опроса стандартного потока ввода. Его работа схожа с работой потока приема заголовков. Есть хэш-таблица с допустимыми командами в качестве ключа и обработчиками в качестве значения. При вводе команды вызывается обработчик. Обработчик может считывать со стандартного ввода необходимые дополнения для введенных команд.

Принцип работы клиента схож с принципом работы сервера. Основное отличие в том, что имеется только 1 поток для приема сообщений. Список допустимых принимаемых заголовков для клиента совпадает со списком посылаемых сервером заголовков, и наоборот. Отличается также список команд, принимаемых с клавиатуры.

### 3.2.2. Реализация на UDP

Реализация на UDP по структуре схожа с реализацией на TCP. Протокол отличается тем, что теперь не передается длина сообщения, но перед заголовком передается порядковый номер сообщения.

В отличие от варианта TCP, здесь не происходит установления соединения и все сообщения передаются через один сокет.

Сервер использует хэш-таблицу, в которой хранится сетевой адрес клиента (ключ) и соответствующий ему номер последнего принятого (в другой таблице отправленного) сообщения. При приеме (отправке) очередного сообщения его номер сравнивается с содержимым соответствующей таблицы, и, в случае нарушения порядка следования пакетов, сообщение об этом выводится в консоль.

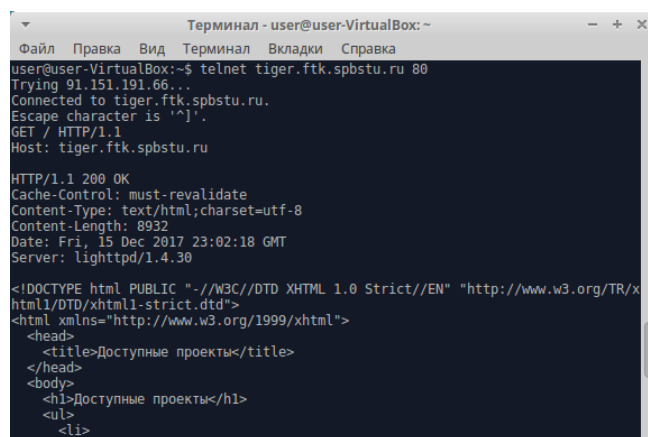
## 3.3. Дополнительное задание

В качестве дополнительного задания необходимо исследовать реальные прикладные протоколы. Необходимо "притвориться" клиентом и подключиться к одному из существующих общедоступных серверов.

В качестве утилиты для подключения к серверам была выбрана telnet.

### 3.3.1. Подключение к веб-серверу и запрос веб-страницы

Был произведен запрос веб-страницы с сервера tiger.ftk.spbstu.ru (рис. 3.2) Подключение производится по используемому протоколом http порту 80. Сервер вернул код 200 в заголовке ответа, что говорит об успешной обработке запроса.



```
Терминал - user@user-VirtualBox: ~
Файл  Правка  Вид  Терминал  Вкладки  Справка
user@user-VirtualBox:~$ telnet tiger.ftk.spbstu.ru 80
Trying 91.151.191.66...
Connected to tiger.ftk.spbstu.ru.
Escape character is '^]'.
GET / HTTP/1.1
Host: tiger.ftk.spbstu.ru

HTTP/1.1 200 OK
Cache-Control: must-revalidate
Content-Type: text/html; charset=utf-8
Content-Length: 8932
Date: Fri, 15 Dec 2017 23:02:18 GMT
Server: lighttpd/1.4.30

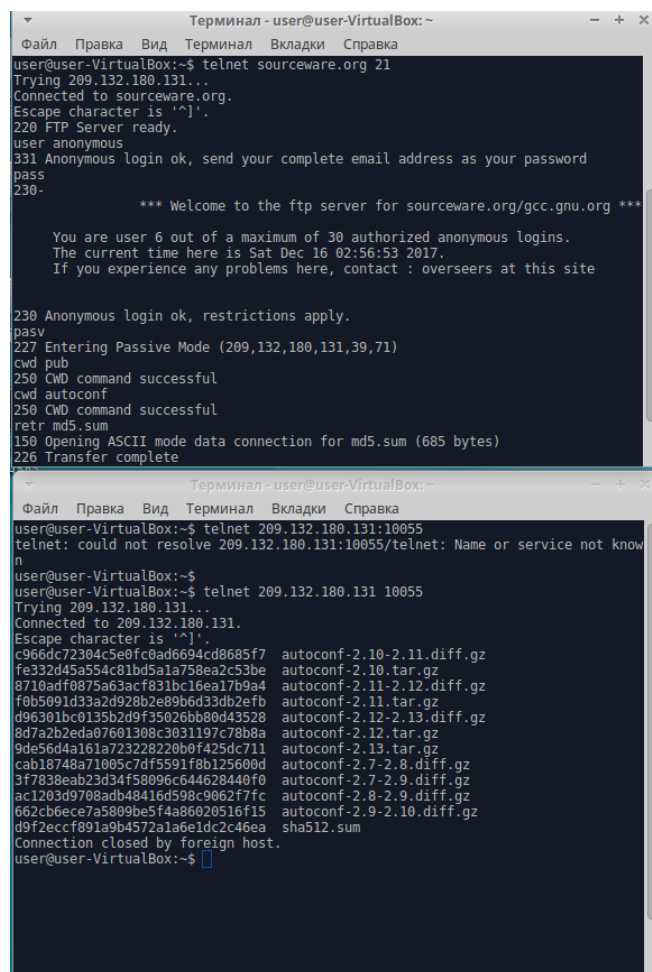
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Доступные проекты</title>
  </head>
  <body>
    <h1>Доступные проекты</h1>
    <ul>
      <li>
```

Рисунок 3.2. Запрос веб-страницы

### 3.3.2. Запрос списка файлов и загрузка файла с ftp-сервера

Протокол FTP использует 2 соединения - для передачи команд и для передачи данных. Поэтому подключение к нему производится в 2 этапа: сначала производится подключение

к порту 21 (для передачи команд) и авторизация, затем переход в пассивный режим и подключение из другого терминала к порту, указанному сервером (рис. 3.3 - 3.4)



```
Терминал - user@user-VirtualBox: ~
Файл  Правка  Вид  Терминал  Вкладки  Справка
user@user-VirtualBox:~$ telnet sourceware.org 21
Trying 209.132.180.131...
Connected to sourceware.org.
Escape character is '^J'.
220 FTP Server ready.
User anonymous
331 Anonymous login ok, send your complete email address as your password
pass
230-
*** Welcome to the ftp server for sourceware.org/gcc.gnu.org ***

You are user 6 out of a maximum of 30 authorized anonymous logins.
The current time here is Sat Dec 16 02:56:53 2017.
If you experience any problems here, contact : overseers at this site

230 Anonymous login ok, restrictions apply.
pasv
227 Entering Passive Mode (209,132,180,131,39,71)
cwd pub
250 CWD command successful
cwd autoconf
250 CWD command successful
retr md5.sum
150 Opening ASCII mode data connection for md5.sum (685 bytes)
226 Transfer complete

Терминал - user@user-VirtualBox: ~
Файл  Правка  Вид  Терминал  Вкладки  Справка
user@user-VirtualBox:~$ telnet 209.132.180.131:10055
telnet: could not resolve 209.132.180.131:10055/telnet: Name or service not known
user@user-VirtualBox:~$ telnet 209.132.180.131 10055
Trying 209.132.180.131...
Connected to 209.132.180.131.
Escape character is '^J'.
c966dc72204c5e0fc0ad6694cd8685f7 autoconf-2.10-2.11.diff.gz
fe332d45a554c01bd5a1a758ea2c53be autoconf-2.10.tar.gz
8710adf0875a63acf831bc16ea17b9a4 autoconf-2.11-2.12.diff.gz
f0b5091d33a2d928b2e89b6d33db2efb autoconf-2.11.tar.gz
d96301bc0135b2d9f35026bb80d43528 autoconf-2.12-2.13.diff.gz
8d7a2b2eda07601308c3031197c78b8a autoconf-2.12.tar.gz
9de56d4a161a723228228b0f425dc711 autoconf-2.13.tar.gz
cab18748a71005c7df5591f8b125600d autoconf-2.7-2.8.diff.gz
3f7830eab23d34f58096c644628440f0 autoconf-2.7-2.9.diff.gz
ac1203d9708adb48416d598c9062f7fc autoconf-2.8-2.9.diff.gz
662cb6ece7a5809be5f4a86020516f15 autoconf-2.9-2.10.diff.gz
d9f2eccf891a9b4572a1a6e1dc2c46ea sha512.sum
Connection closed by foreign host.
user@user-VirtualBox:~$
```

Рисунок 3.3. Запрос списка файлов и загрузка файла с ftp-сервера

```
Терминал - user@user-VirtualBox: ~
Файл  Правка  Вид  Терминал  Вкладки  Справка
user@user-VirtualBox:~$ telnet sourceware.org 21
Trying 209.132.180.131...
Connected to sourceware.org.
Escape character is '^]'.
220 FTP Server ready.
user anonymous
331 Anonymous login ok, send your complete email address as your password
pass
230-
*** Welcome to the ftp server for sourceware.org/gcc.gnu.org ***

You are user 10 out of a maximum of 30 authorized anonymous logins.
The current time here is Sat Dec 16 03:02:31 2017.
If you experience any problems here, contact : overseers at this site

230 Anonymous login ok, restrictions apply.
pasv
227 Entering Passive Mode (209,132,180,131,39,254)
list
150 Opening ASCII mode data connection for file list
226 Transfer complete

Терминал - user@user-VirtualBox: ~
Файл  Правка  Вид  Терминал  Вкладки  Справка
user@user-VirtualBox:~$ telnet 209.132.180.131 10238
Trying 209.132.180.131...
Connected to 209.132.180.131.
Escape character is '^]'.
drwxr-xr-x  9 ftp      ftp      4096 Mar 22  2013 .
drwxr-xr-x  9 ftp      ftp      4096 Mar 22  2013 ..
-r--r--r--  1 ftp      ftp      4096 Oct 22  1999 .notar
lrwxrwxrwx  1 ftp      ftp      4096 Mar 19  2013 anonftp -> .
dr-xr-xr-x  2 ftp      ftp      4096 Feb 14  2004 bin
dr-xr-xr-x  2 ftp      ftp      4096 Feb 14  2004 etc
drwxr-xr-x  2 ftp      ftp      4096 Feb 14  2004 lib
drwxrwsr-x 55 ftp      ftp      4096 Jun  2  2017 pub
d-wx-wx--x  2 ftp      ftp      4096 Jan 20  2012 uploads
drwxr-xr-x  3 ftp      ftp      4096 Nov  8  1999 usr
-rw-r--r--  1 ftp      ftp      4096 Mar 26  2006 welcome.msg
drwxr-xr-x  3 ftp      ftp      4096 Dec  7  2001 www
Connection closed by foreign host.
user@user-VirtualBox:~$
```

Рисунок 3.4. Запрос списка файлов и загрузка файла с ftp-сервера

### 3.3.3. Отправка письма на SMTP-сервер

Попытаемся авторизоваться на SMTP-сервере gmail (рис. 3.5)

```
Терминал - user@user-VirtualBox: ~
Файл  Правка  Вид  Терминал  Вкладки  Справка
user@user-VirtualBox:~$ telnet smtp.gmail.com 587
Trying 64.233.161.108...
Connected to gmail-smtp-msa.l.google.com.
Escape character is '^]'.
220 smtp.gmail.com ESMTP r7sm1493146lja.32 - gsmt
ehlo a
250-smtp.gmail.com at your service, [188.170.82.197]
250-SIZE 35882577
250-8BITMIME
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
auth plain AGx
530 5.7.0 Must issue a STARTTLS command first. r7sm1493146lja.32 - gsmt
```

Рисунок 3.5. Отправка письма на SMTP-сервер без использования шифрования

Как видно, данный сервер требует обязательного использования TLS. Установим защищенное соединение с помощью утилиты openssl (рис. 3.6 - 3.7)

```
Терминал - user@user-VirtualBox: ~
Файл Правка Вид Терминал Вкладки Справка
user@user-VirtualBox:~$ openssl s_client -starttls smtp -crlf -connect smtp.gmail.com:587
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = Google Internet Authority G3
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = smtp.gmail.com
verify return:1
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=smtp.gmail.com
 1 s:/C=US/O=Google Trust Services/CN=Google Internet Authority G3
 1 s:/C=US/O=Google Trust Services/CN=Google Internet Authority G3
 1 i:/OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEGjCCA2qgAwIBAgITdzikJzCrDj4wDQYJKoZIhvcNAQELBQAwVDELMAkGA1UE
BhMCVVMxHjAcBgNVBAoTFUdvb2dsZS5BUcnVzdCBTZXJ2aWNlczElMCMGA1UEAxMc
R29vZ2xlIEludG9ybWV0IEF1dGhvcml0eSBHMzAeFw0xNzEyMDUxMDE2M0laFw0x
ODAyMjcwOTI1MDBaMG9xZzA3BgtNVBAYTALVTMRMwEQYDVQIDApDyWxpZm9ybmlh
MRVwFAYDVQQDA1N3VudGFpb1BwV3MRMwEQYDVQIDApHb29nbGUgSw5jMRcw
FQYDVQDDA5zbXRwLmdtYWwLsLmNvbnVtTCCASwEQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAs95vMtrTHpAnpa4jXG8tpViE17nDHG6TQv4ZboMhqwH5Kz93jnbGsn
DutTCvsLV7jhc97q08sD1sX8HFUnQ2TfuRnj/MNsnl69r0AfLRIYKw5C8mqEsYUM
lhW0t3j1Hx5Suz0q2c3NznBf5fKHVR06ZLIQwXqZe4yyiyGjJiVV+hfiS83zr8
X0Zs7/N35op3IPPRY827/uu+ouTjQank9JGdTpFR0U+LzLuKmp9NJjFbBSKrK+eG
MtwWnsX7TTQpNmgqERhd5TB5NIYQ0XmiY3rjG2Q48HWFcUYTr5JXBS2gxEKJ0d1M
6BYzXxOuTldsm0S+SbwGxGqVtsIcGbECaWEAA0CAUIwggE+MBMGA1UdJQQMMAoG
CCsGAQUFBwMBMBKgA1UdEQSMBCDnNtdHauZ21haWwUy29tMGgGCCsGAQUFBwEB
BFwwWjAtBggrBgEFBQcwAoYhaHR0cDovL3BraS5nb29nL2dzcjIvR1RTR0lBRzMu
Y3J0MCKGCCsGAQUFBzABhh1odHRwOi8vb2NzcC5wa2kuZ29vZy9HVFNHNSUHFHMzAd
BgNVHQ4EFgQUHwTh0jn9lnb5d5NezXJ2wBbA3aMwDAYDVR0TAQH/BAIwADAfBgNV
HSMEGDAwBR3wrhQmm2drEtWobQg6B+pn66SzAhBgNVHSAEGjAYMAwGC1sGAQ0B
InkCBQMWCAyGZ4EQAQICMDEGA1UdHwQqMgJqAKoCKGh0dHA6Ly9jcmwucGtp
Lmdvb2cvR1RTR0lBRzMuY3J0MCKGCCsGAQUFBzABh3DQEBcUAA4IBAQAxNVxTDvtUSuZE
HQSyhwLCrF9uv04nbGdk/7gxKFb3H6LKlncLzNDUevATUMiPANETRwtwr7b560t
p61h3Z1uzqQhx1+XuL0cLiWm/taEx/IsKEFABiuWrZEbq25B0ZHLTHS/rXdsJ900
0SvIU1Mle9bWws0vFtKI0+IfdRCAuywDZir/kucJ3/PYrJKZrflJajCX7Pf1SuF4
C2Pu/u4qHwZ3BpM5e1u3B3fSGfwVWP1rCDPIFRjnS7JH6B2A61aCR0f1Gub8+ums
dIPVoIY16vXhroLP4jcoQlB0rVSh9zmRk1NzrQZffSpFz6gdcD8XC659Y1LzeVP
KprRPbe/
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=smtp.gmail.com
Issuer=/C=US/O=Google Trust Services/CN=Google Internet Authority G3
---
No client certificate CA names sent
Peer signing digest: SHA256
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 3239 bytes and written 466 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
```

Рисунок 3.6. Отправка письма на SMTP-сервер через TLS-подключение



```
Терминал - user@user-VirtualBox: ~
Файл  Правка  Вид  Терминал  Вкладки  Справка

Session-ID: 6A0486720E1C63481F1C082CC9CD6E51B5C42E94E3D70A6FA6D5BF21E655B160
Session-ID-ctx:
Master-Key: 4E5744D58992FC6BFA5D9E0CAB553D5E5D23774782343AABC544AC5348AD8547
35A458F6F301A3A36AAE47643A27F8BC
Key-Arg : None
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 100800 (seconds)
TLS session ticket:
0000 - 00 8d e4 8d 09 b7 74 e0-da 21 96 7d 02 61 98 8a .....t...!..a..
0010 - 64 62 04 6e 54 77 cf 29-f3 08 be ed b9 43 b8 28 db.nTw.)....C.(
0020 - 89 ba eb af c0 25 29 ec-b1 9f ab 60 91 a9 9a 66 .....%).....f
0030 - ef 9c 1a 96 10 7b 69 2e-e0 f0 2e b6 8e 54 2b 3b .....{i.....T+;
0040 - 9e 87 d4 42 64 5b e1 6f-f2 0d 14 78 d7 fa a0 3b ...Bd[.o...x...;
0050 - 88 4e 79 6d 40 ae 57 ce-a3 0d 2d 8e 9c 4f fd bd .Nym@.W.....0..
0060 - 5d 67 92 a9 21 d4 c1 d9-d8 a1 b0 a8 f4 45 e5 68 ]g..f.....E.h
0070 - f8 76 e6 41 56 24 c6 c0-7c 64 ce 61 d5 52 01 5e .v.AV$.|d.a.R.^
0080 - cf 42 6e 87 d5 f1 0b b8-ee 26 b9 a3 28 2e d8 a1 .Bn.....&.(...
0090 - 60 c9 52 5a ec 76 03 6c-f2 13 4c 4f 74 4a b1 de ^.RZ.v.l.L0tJ..
00a0 - 50 18 88 21 05 4a 46 85-13 25 b7 18 9c 18 2f 66 P..!JF.%....f
00b0 - 26 bf 97 fa e7 1b e7 92-7e 26 be e9 9a 14 a7 55 &.....&.....U
00c0 - d9 ff 0f 39 b4 85 93 ca-34 c8 98 8c 78 e3 e2 4a ...9....4...x..J
00d0 - da 4d 93 1c 48 .M..H

Start Time: 1513389854
Timeout : 300 (sec)
Verify return code: 0 (ok)
---
250 SMTPUTF8
ehlo a
250-smtp.gmail.com at your service, [188.170.82.197]
250-SIZE 35882577
250-8BITIME
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
auth plain AGx1
235 2.7.0 Accepted
mail from:<lugakorrav@gmail.com>
250 2.1.0 OK h75sm1474953ljf.36 - gsmt
rcpt to:<impacthammer218@gmail.com>
250 2.1.5 OK h75sm1474953ljf.36 - gsmt
data
354 Go ahead h75sm1474953ljf.36 - gsmt
subject:
test message

Korenek Grigory

250 2.0.0 OK 1513389904 h75sm1474953ljf.36 - gsmt
quit
221 2.0.0 closing connection h75sm1474953ljf.36 - gsmt
read:errno=0
user@user-VirtualBox:~$
```

Рисунок 3.7. Отправка письма на SMTP-сервер через TLS-подключение

Сервер сообщил, что сообщение успешно отправлено. Убедимся в этом, зайдя на gmail.com (рис. 3.8)

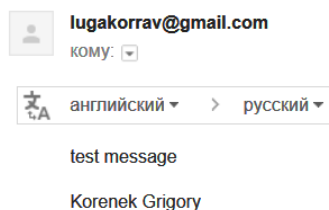


Рисунок 3.8. Отправленное письмо

### 3.3.4. Получение письма с POP3-сервера

Проверим почту и получим письмо (рис. 3.9 - 3.11)

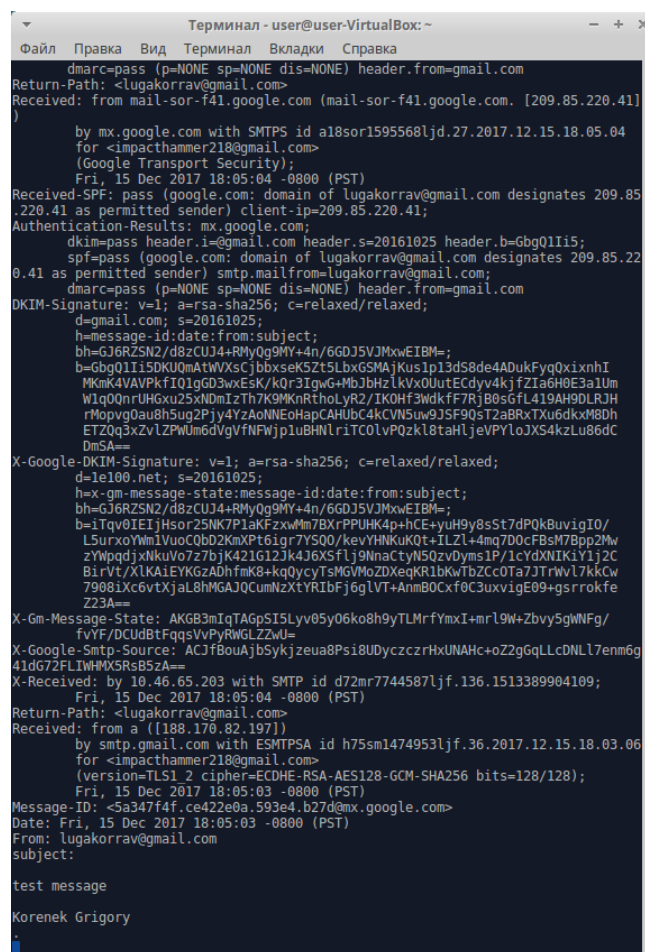
```
Терминал - user@user-VirtualBox: ~
Файл Правка Вид Терминал Вкладки Справка
user@user-VirtualBox:~$ openssl s_client -connect pop.gmail.com:995
CONNECTED(00000000)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = Google Internet Authority G3
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = pop.gma
il.com
verify return:1
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=pop.gmail.com
i:/C=US/O=Google Trust Services/CN=Google Internet Authority G3
1 s:/C=US/O=Google Trust Services/CN=Google Internet Authority G3
i:/OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEgDCCA2igAwIBAgIIV0cZyXvY4LcwDQYJKoZIhvcNAQELBQAwVDELMAkGA1UE
BhMCVVMxHjAcBgNVBAoTFUdvb2dsZS5SUcnVzdCBTZXJ2aWNLczELMCMGA1UEAxMc
R29vZ2x1IEludGVybmV0IEF1dGhvcml0eSBHMzAeFw0xNzEyMDUxMDE3MzZaFw0x
ODAyMjcwOTI5MDBaMGcxZzA1BGNVBAZTA1VTMRMwEQYDVQIDApDyWxpZm9ybmRh
MRYwFAYDVQQHDA1Nb3VudGFpb1BwaWwV3MRMwEQYDVQIDApHb29nbGUgSW5jMRYw
FAYDVQDDDA1w3AuZ21haWwY29tMIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA1Nn0wiRPM+Mi0ltZdaom+h96046kcbhldj6xw0DqAMDfLd0WM2Dkcxi
CX7z4C/TIBX0AHjXKQz9mdqaxVzBh0ycXu8ZHW2VRs+bbLbo/DL97YvumrjpiBL
7Kp9ieQ5WmQUnSgM15rzozcJ79kFgW0+5X0JIqp/vKam4yWAv/I4FKdQmZwFtZ86
D0An6dJ5IDb/Y0cX1sFRAmUiEviaJczAMpJzsqh1mqP9Epb/0/yBcoYLDhEvacBL
Z0uaBYcG1fag5rF/rMogZq1UM3w9ITl1kKRd5RqcS6PxMC7aq/Pm4r3ULlGbRT+w
ze2IpdmlQ0tJDwJMb3mwoyyHTHwnuQIDAQABo4IBQTCAT0wEwYDVR0LBAwwCgYI
KwYBBQUHAEwEwGAYDVR0RBBEwD4INcG9wLmdtYwLsLmNvbTB0BggrBgEFBQcBAQRc
MFowLQYIKwYBBQUHMAKIWh0dHA6Ly9wa2kuZ29vZy9nc3IyL0dUU0dJQUczLmNy
dApBggrBgEFBQcwAYYdaHR0cDovL29jc3AucGtpLmdvb2c2vR1RTR0lBRzMuHQYD
VR0BBYEFLGR1+GLYRF5Psa7GTCWruyRCHLWMAwGA1UdEwEB/wQCMAAwHwYDVR0j
BBgwFoAUd8K4UJpndnaxLcKGIOgfqZ+ukswIQYDVR0gBBowGDAwBggrBgEEAdZ5
AgUDMAgGBmeBDAECAjAxBgNVHR8EKjAocMCAgJKA1h1BodHRwOi8vY3JsLnBraS5N
b29nL0dUU0dJQUczLmNyYDANBgkqhkiG9w0BAQsFAAOCAQEAUUI5SRsXf0GaLLIIE
4IPg2R65CjoTD971T7LHD1Ys0nxLcI60610uEh1YwCjmxrTb51fKG+Uk6X5NY40x
voNXfn6/cNNQ/ne+UKEYI0IwuhQju65FhSMkRhJB7QMB/11Hr0sWaRkpSEKII7np
vUUXHZ+J01k/pi4CMd1AreHw/5gXIEqFYOKkh82cU01GLsLZV20PzpprZ80BBRNQ
ohUUIGy4VS+2bp4sth7DGChzR3tL2X14+9GKS0b1iU0IA2Jc3uok53bL5uoJmRN
BjRcZodyzKkR5fR0Qo3h7Rmef0vVrjCj6CEujmotdU0dtsNJNmu90n9fRA5byNzL
YhhL5w==
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=pop.gmail.com
issuer=/C=US/O=Google Trust Services/CN=Google Internet Authority G3
---
No client certificate CA names sent
Peer signing digest: SHA256
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 2984 bytes and written 431 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
```

Рисунок 3.9. Получение письма с POP3-сервера

```
Терминал - user@user-VirtualBox: ~
Файл Правка Вид Терминал Вкладки Справка
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol : TLSv1.2
  Cipher   : ECDHE-RSA-AES128-GCM-SHA256
  Session-ID: 81AAEA1E51C65C38B83310B4A1540836E57FC0F8CC140C29EB18780AA5570957
  Session-ID-ctx:
  Master-Key: D3E73E488EE4CC7F1A9934B9E6506D937EDD08AB088871EDE36BF8687C1CC165
  6B23206C7112D017B01B3E82A7C027B2
  Key-Arg : None
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 100800 (seconds)
  TLS session ticket:
    0000 - 00 8d e4 8d 09 b7 74 e0-da 21 96 7d 02 61 98 8a .....t...}.a..
    0010 - c7 ed d6 f0 cf 83 a8 a0-07 c4 58 5d 6f d7 25 c1 .....X]o.%.
    0020 - 14 86 4c 82 b0 a7 a6 db-18 36 6f ef f3 08 10 75 ..L.....6o...u
    0030 - 06 7e f2 dc cd 77 17 ac-70 59 93 57 e3 ff 8c ca ~...w...pY.W....
    0040 - 00 1c fd 2c 7b c1 34 b0-f0 22 30 72 6c 32 a5 4f ...,{.4..0rl2.0
    0050 - f0 7f d7 79 fe 5f 1b 72-ea aa 69 45 05 9b e5 ae ...y...r..iE....
    0060 - 8f 07 44 51 90 41 f0 7d-83 f5 6f 26 6d 77 1d 98 ..DQ.A)...oSmw..
    0070 - 75 c9 4c 8d 06 f3 3f 8e-d8 10 e1 b2 63 d2 fe 77 u.L...?...C..w
    0080 - 17 23 49 e3 d4 c8 e9 bf-22 f7 4b 7e af 25 f4 e4 .#I...?...K~.%..
    0090 - 80 69 30 79 27 16 e3 0b-d1 95 69 f7 05 54 cc bb .i0y'.....i..T..
    00a0 - a2 08 3c 82 0c 8e e2 9a-7a 03 f6 c1 3c d1 c1 43 ..<.....Z...<..C
    00b0 - ad b4 40 13 1a 35 f8 6b-0c 91 cd a5 16 10 e7 b8 ..@..5.k.....
    00c0 - 56 7e ec 4f 02 c1 84 78-84 cc b3 aa bf 60 b8 c4 V~.0...x.....'..
    00d0 - da 10 30 8b 97 ..0..

  Start Time: 1513390375
  Timeout : 300 (sec)
  Verify return code: 0 (ok)
---
+OK Gpop ready for requests from 188.170.82.197 e19mb158308172lja
user impacthammer218
+OK send PASS
pass [REDACTED]
+OK Welcome.
stat
+OK 3 52566
list
+OK 3 messages (52566 bytes)
1 43367
2 4593
3 4606
.
retr 3
+OK message follows
Delivered-To: impacthammer218@gmail.com
Received: by 10.37.100.14 with SMTP id y14csp262974ybb;
Fri, 15 Dec 2017 18:05:04 -0800 (PST)
X-Received: by 10.25.150.137 with SMTP id y131mr6797320lfd.91.1513389904509;
Fri, 15 Dec 2017 18:05:04 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1513389904; cv=none;
d=google.com; s=arc-20160816;
```

Рисунок 3.10. Получение письма с POP3-сервера



```
Терминал - user@user-VirtualBox: ~
Файл  Правка  Вид  Терминал  Вкладки  Справка

dmarc-pass (p=NONE sp=NONE dis=NONE) header.from=gmail.com
Return-Path: <lugakorrav@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
    by mx.google.com with SMTPS id a18sor1595568lj.27.2017.12.15.18.05.04
    for <impacthammer218@gmail.com>
    (Google Transport Security);
    Fri, 15 Dec 2017 18:05:04 -0800 (PST)
Received-SPF: pass (google.com: domain of lugakorrav@gmail.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
    dkim=pass header.i=@gmail.com header.s=20161025 header.b=Gbg01Ii5;
    spf=pass (google.com: domain of lugakorrav@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=lugakorrav@gmail.com;
    dmarc-pass (p=NONE sp=NONE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    d=gmail.com; s=20161025;
    h=message-id:date:from:subject;
    bh=GJ6RZSN2/d8zCUJ4+RMvOg9MY+4n/6GDJ5VJMxwEIBM=;
    b=Gbg01Ii5DKUQmAtwXsCjbbxseK5Zt5LbxGSMajKuslp13dS8de4ADukFyQ0xixnhI
    MkmK4VAVPki01gGD3vxESK/k0r3IgwG+MbJbHzlkVx0UutECdyv4kjfZia6H0E3a1Um
    Wlq0Q0nrUHGxu25xNDmIzTh7K9MKnRthoLyR2/IK0Hf3WdkfF7RjB0sGfL419AH9DLRJH
    rMopvg0au8hSug2Pjy4YzAoNNEoHapCAHUBC4kCVN5uw9J5F9QsT2aBRxTXu6dkxM8Dh
    ETZ0q3xZvLZPWUm6dVgVfNFwjp1uBHNlriTC0lvPQzkL8taHljvPYLoJXS4kzLu866C
    DmSA==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    d=1e100.net; s=20161025;
    h=x-gm-message-state:message-id:date:from:subject;
    bh=GJ6RZSN2/d8zCUJ4+RMvOg9MY+4n/6GDJ5VJMxwEIBM=;
    b=ITqv0IEIjHs0r25NK7P1aKfzxMm7BxrPPUHK4p+hCE+yuH9y8St7dPQkBuviG10/
    L5urxoYmI1Vu0CQbD2KmxPt6igr7YS00/kevYHNKuKQt+ILZL+4mq7D0cFBsM7Bpp2Mw
    zYwpgdjxNkuVo7z7bjK421G12Jk4J6XSflj9NnaCtyN5QzvDyms1P/1cYdXNKiY1j2C
    BirVt/XLKaiEYKgzAdhfmK8+kq0ycyTSMGVMoZDxeqKR1bKwTbZCc0Ta7JTrwL7kkCw
    7908IXc6vtXjaL8HMGAJQCumNzXtYRiBfj6glVT+AnmB0Cxf0C3uxvigE09+gsrrrkfe
    Z23A==
X-Gm-Message-State: AKGB3mIqTAGpSI5Lyv05y06ko8h9yTLMrfYmxI+mrl9W+Zbvy5gWNFg/
    fvYF/DCUdBTfQqsVvPyRWGLZzwU=
X-Google-Smtp-Source: ACJfBouAjb5Ykjzeua8PSi8UDyczcZrHxUNAHc+oZ2gGqLLcDNL1enm6g
    41dG72FLIWMXSRsB5ZA==
X-Received: by 10.46.65.203 with SMTP id d72mr7744587ljf.136.1513389904109;
    Fri, 15 Dec 2017 18:05:04 -0800 (PST)
Return-Path: <lugakorrav@gmail.com>
Received: from a ([188.170.82.197])
    by smtp.gmail.com with ESMTPSA id h75sm1474953ljf.36.2017.12.15.18.03.06
    for <impacthammer218@gmail.com>
    (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
    Fri, 15 Dec 2017 18:05:03 -0800 (PST)
Message-ID: <5a347f4f.ce422e0a.593e4.b27d@mx.google.com>
Date: Fri, 15 Dec 2017 18:05:03 -0800 (PST)
From: lugakorrav@gmail.com
Subject:
test message

Korenek Grigory
```

Рисунок 3.11. Получение письма с POP3-сервера

## 4. Выводы

В ходе работы был разработан и реализован в виде приложения прикладной протокол. В результате этого были изучены принципы программирования сокетов TCP и UDP. Основной проблемой при реализации приложения на TCP была необходимость контроля длины послыки. Ее решением стало добавление длины послыки в поле опций. После приема послыки принимающая сторона ожидает приема указанного числа символов. Проблема контроля потоков опроса клиентов решилась сохранением в хэш-таблице сокетов клиентов и соответствующих id потоков.

При реализации на UDP требовалось определять ситуации перемешивания и потери пакетов. Для этого на сервере создавались хэш-таблицы, хранящие адреса клиентов (ключи) и соответствующие номера отправляемых (принимаемых) пакетов. Для клиента с этой целью требовалось хранить только 2 переменные.

Также были исследованы прикладные протоколы. Как выяснилось, почтовые сервера могут требовать обязательного использования защищенного подключения.