

1. Wireshark UDP

1) Видим 4 поля в UDP-заголовке: src-port, dst-port, length, checksum:

322	0.637928934	192.168.10.100	192.168.10.1	DNS	75 Standard query 0xd11e HTTPS s7d1.scene7.com
338	0.642819883	192.168.10.1	192.168.10.100	DNS	503 Standard query response 0xfe03 A assets.adobedtm.com CNAME cn-asse
339	0.644593508	192.168.10.1	192.168.10.100	DNS	224 Standard query response 0x0380 HTTPS assets.adobedtm.com CNAME cn-i
340	0.644958092	192.168.10.100	192.168.10.1	DNS	85 Standard query 0x0089 HTTPS e7808.dscg.akamaiedge.net
341	0.651356570	192.168.10.1	192.168.10.100	DNS	149 Standard query response 0x0089 HTTPS e7808.dscg.akamaiedge.net SOA
344	0.655871879	192.168.10.100	64.233.161.95	UDP	75 48603 → 443 Len=33
345	0.657642568	64.233.161.95	192.168.10.100	UDP	66 443 → 48603 Len=24
370	0.666965518	192.168.10.1	192.168.10.100	DNS	496 Standard query response 0xee84 A s7d1.scene7.com CNAME wildcard.sc

▶ Frame 338: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits) on interface wlx7062b8b3c121, id 0
 ▶ Ethernet II, Src: Tp-LinkT_c4:83:be (c0:25:e9:c4:83:be), Dst: D-LinkIn_b3:c1:21 (70:62:b8:b3:c1:21)
 ▶ Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.100
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 40139

Source Port: 53
 Destination Port: 40139
 Length: 469
 Checksum: 0x25e5 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 7]
 [Timestamps]
 UDP payload (461 bytes)
 ▶ Domain Name System (response)

2) Длина каждого поля – два байта

322	0.637928934	192.168.10.100	192.168.10.1	DNS	75 Standard query 0xd11e HTTPS s7d1.scene7.com
338	0.642819883	192.168.10.1	192.168.10.100	DNS	503 Standard query response 0xfe03 A assets.adobedtm.com CNAME cn-asse
339	0.644593508	192.168.10.1	192.168.10.100	DNS	224 Standard query response 0x0380 HTTPS assets.adobedtm.com CNAME cn-i
340	0.644958092	192.168.10.100	192.168.10.1	DNS	85 Standard query 0x0089 HTTPS e7808.dscg.akamaiedge.net
341	0.651356570	192.168.10.1	192.168.10.100	DNS	149 Standard query response 0x0089 HTTPS e7808.dscg.akamaiedge.net SOA
344	0.655871879	192.168.10.100	64.233.161.95	UDP	75 48603 → 443 Len=33
345	0.657642568	64.233.161.95	192.168.10.100	UDP	66 443 → 48603 Len=24
370	0.666965518	192.168.10.1	192.168.10.100	DNS	496 Standard query response 0xee84 A s7d1.scene7.com CNAME wildcard.sc

▶ Frame 338: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits) on interface wlx7062b8b3c121, id 0
 ▶ Ethernet II, Src: Tp-LinkT_c4:83:be (c0:25:e9:c4:83:be), Dst: D-LinkIn_b3:c1:21 (70:62:b8:b3:c1:21)
 ▶ Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.100
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 40139

Source Port: 53
 Destination Port: 40139
 Length: 469
 Checksum: 0x25e5 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 7]
 [Timestamps]
 UDP payload (461 bytes)
 ▶ Domain Name System (response)

0020	0a 64 00 35 9c cb 01 d5 25 e5 fe 03 81 80 00 01	0d 15
0030	00 03 00 08 00 09 06 61 73 73 65 74 73 08 61 64a ssets:ad
0040	6f 62 65 64 74 6d 03 63 6f 6d 00 00 01 00 01 c0	obedtm.c om.....
0050	0c 00 05 00 01 00 00 00 2a 00 24 09 63 6e 2d 61*\$.cn-a
0060	73 73 65 74 73 08 61 64 6f 62 65 64 74 6d 03 63	ssets:ad obedtm.c

это соответствует спецификации UDP.

3) Значение поля length – длина заголовка + длина (размер) тела udp-пакета.

В моем пакете length – 469, значит, сами данные занимают 469 – 8 байт

4) Теоретически, без учета размера TCP-заголовка, так как максимальное значение поля length – $2^{16} - 1$ и длина заголовка – 8 байт, то $2^{16} - 1 - 8$ (65527)

5) Очевидно, $2^{16} - 1$

6) В поле Protocol заголовка TCP находится значение 17:

322	0.637928934	192.168.10.100	192.168.10.1	DNS	75 Standard query 0xd11e HTTPS s7d1.scene7.com
338	0.642819883	192.168.10.1	192.168.10.100	DNS	503 Standard query response 0xfe03 A assets.adobedtm.com CNAME cn-asse
339	0.644593508	192.168.10.1	192.168.10.100	DNS	224 Standard query response 0x0380 HTTPS assets.adobedtm.com CNAME cn-
340	0.644958092	192.168.10.100	192.168.10.1	DNS	85 Standard query 0x0089 HTTPS e7808.dscg.akamaiedge.net
341	0.651356570	192.168.10.1	192.168.10.100	DNS	149 Standard query response 0x0089 HTTPS e7808.dscg.akamaiedge.net SOA
344	0.655871879	192.168.10.100	64.233.161.95	UDP	75 48603 → 443 Len=33
345	0.657642568	64.233.161.95	192.168.10.100	UDP	66 443 → 48603 Len=24
370	0.666965518	192.168.10.1	192.168.10.100	DNS	496 Standard query response 0xee84 A s7d1.scene7.com CNAME wildcard.sc
▶ Frame 338: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits) on interface wlx7062b8b3c121, id 0 Ethernet II, Src: Tp-LinkT_c4:83:be (c0:25:e9:c4:83:be), Dst: D-LinkIn_b3:c1:21 (70:62:b8:b3:c1:21) Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.100 0100 = Version: 4 0101 = Header Length: 20 bytes (5) ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 489 Identification: 0x0000 (0) ▶ Flags: 0x40, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 63 Protocol: UDP (17) Header Checksum: 0xa44e [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.10.1 Destination Address: 192.168.10.100 User Datagram Protocol, Src Port: 53, Dst Port: 40120					
0010	01 e9 00 00 40 00 3f 11	a4 4e c0 a8 0a 01 c0 a8	...	0 ?	N
0020	0a 64 00 35 9c cb 01 d5	25 e5 fe 03 81 80 00 01	...	d 5	%
0030	00 03 00 08 00 09 06 61	73 73 65 74 73 08 61 64	...	a	ssets:ad
0040	6f 62 65 64 74 6d 03 63	6f 6d 00 00 01 00 01 c0	...	obedtm:c	om
0050	0c 00 05 00 01 00 00 00	2a 00 24 09 63 6e 2d 61	...	*	\$.cn-a

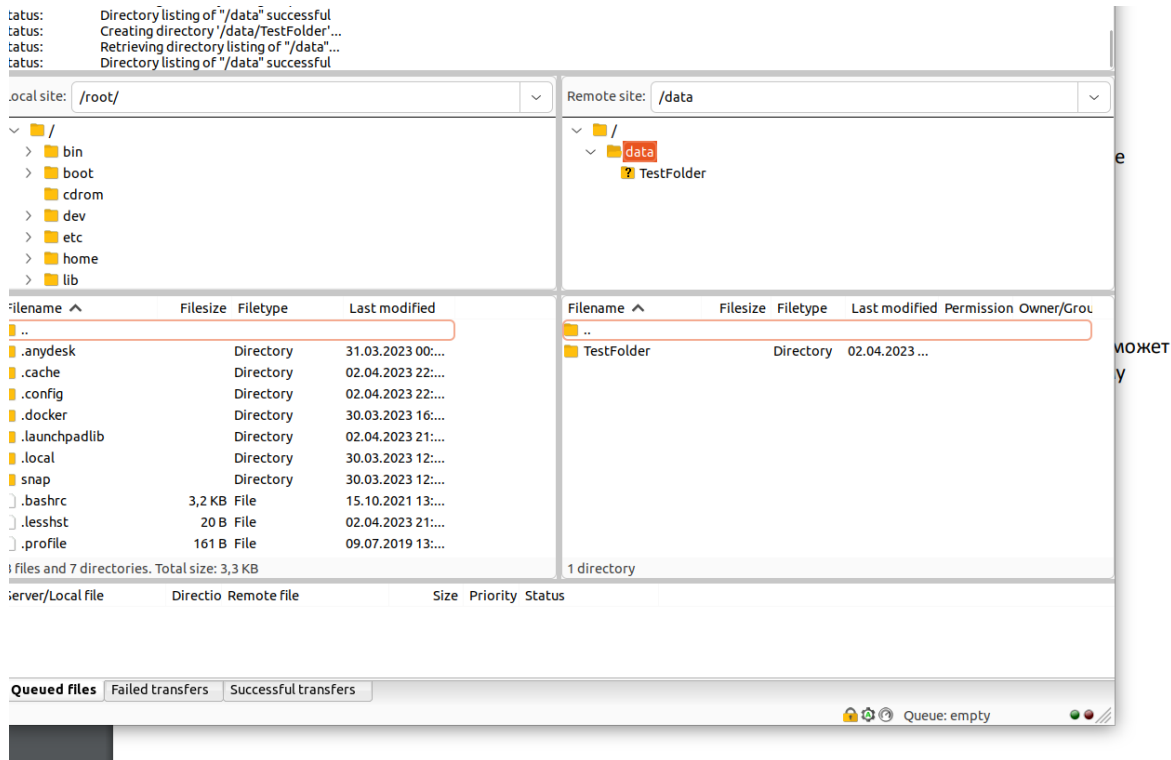
7) Порты назначения и отправителя в этих двух пакетах меняются местами:

14	0.323119400	192.168.10.1	192.168.10.100	DNS	219 Standard query response 0x700d HTTPS www.mcdonalds.com CNAME direct
15	0.323790527	192.168.10.100	192.168.10.1	DNS	83 Standard query 0xefb4 HTTPS e10723.b.akamaiedge.net
16	0.327520655	192.168.10.1	192.168.10.100	DNS	144 Standard query response 0xefb4 HTTPS e10723.b.akamaiedge.net SOA n
35	0.400051185	192.168.10.100	142.250.150.99	UDP	666 42977 → 443 Len=624
40	0.414186073	142.250.150.99	192.168.10.100	UDP	72 443 → 42977 Len=30
41	0.416018690	192.168.10.100	142.250.150.99	UDP	389 42977 → 443 Len=347
42	0.418300235	192.168.10.100	142.250.150.99	UDP	252 42977 → 443 Len=210
44	0.429535112	142.250.150.99	192.168.10.100	UDP	73 443 → 42977 Len=31
45	0.431559338	142.250.150.99	192.168.10.100	UDP	73 443 → 42977 Len=31
46	0.433193178	192.168.10.100	142.250.150.99	UDP	75 42977 → 443 Len=33
49	0.438114311	142.250.150.99	192.168.10.100	UDP	281 443 → 42977 Len=239
50	0.438361198	142.250.150.99	192.168.10.100	UDP	69 443 → 42977 Len=27
.... 0101 = Header Length: 20 bytes (5) ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 69 Identification: 0xb5df (46559) ▶ Flags: 0x00 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 64 Protocol: UDP (17) Header Checksum: 0x2f13 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.10.100 Destination Address: 192.168.10.1 User Datagram Protocol, Src Port: 33509, Dst Port: 53 Source Port: 33509 Destination Port: 53 Length: 49 Checksum: 0x5644 [unverified] [Checksum Status: Unverified] [Stream index: 2] ▶ [Timestamps] UDP payload (41 bytes) Domain Name System (query)					
14	0.323119400	192.168.10.1	192.168.10.100	DNS	219 Standard query response 0x700d HTTPS www.mcdonalds.com CNAME direct
15	0.323790527	192.168.10.100	192.168.10.1	DNS	83 Standard query 0xefb4 HTTPS e10723.b.akamaiedge.net
16	0.327520655	192.168.10.1	192.168.10.100	DNS	144 Standard query response 0xefb4 HTTPS e10723.b.akamaiedge.net SOA n
35	0.400051185	192.168.10.100	142.250.150.99	UDP	666 42977 → 443 Len=624
40	0.414186073	142.250.150.99	192.168.10.100	UDP	72 443 → 42977 Len=30
41	0.416018690	192.168.10.100	142.250.150.99	UDP	389 42977 → 443 Len=347
42	0.418300235	192.168.10.100	142.250.150.99	UDP	252 42977 → 443 Len=210
44	0.429535112	142.250.150.99	192.168.10.100	UDP	73 443 → 42977 Len=31
45	0.431559338	142.250.150.99	192.168.10.100	UDP	73 443 → 42977 Len=31
46	0.433193178	192.168.10.100	142.250.150.99	UDP	75 42977 → 443 Len=33
49	0.438114311	142.250.150.99	192.168.10.100	UDP	281 443 → 42977 Len=239
50	0.438361198	142.250.150.99	192.168.10.100	UDP	69 443 → 42977 Len=27
.... 0101 = Header Length: 20 bytes (5) ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 130 Identification: 0x0000 (0) ▶ Flags: 0x40, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 63 Protocol: UDP (17) Header Checksum: 0xa5b5 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.10.1 Destination Address: 192.168.10.100 User Datagram Protocol, Src Port: 53, Dst Port: 33509 Source Port: 53 Destination Port: 33509 Length: 110 Checksum: 0xff7e [unverified] [Checksum Status: Unverified] [Stream index: 2] ▶ [Timestamps] UDP payload (102 bytes) Domain Name System (response)					

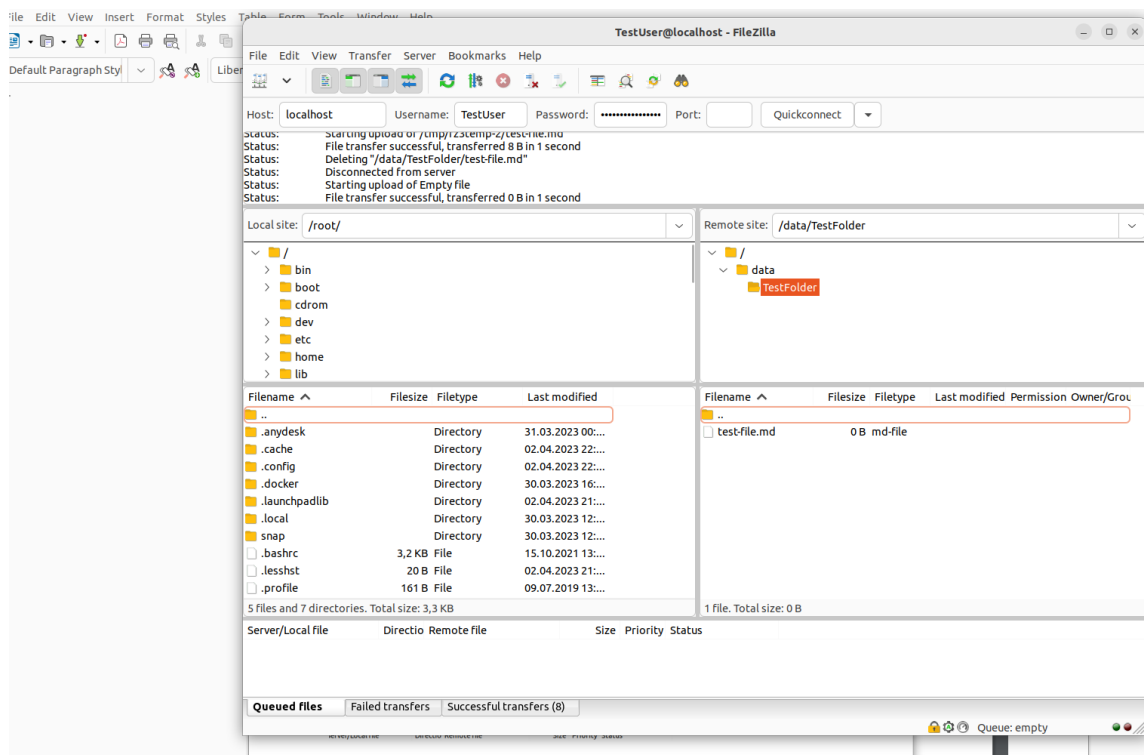
потому что первый запрос отправило приложение через порт 33509 на порт 53 получатель, а получатель с 53 порта отправил идр-датаграмму на порт 33509 на мой компьютер.

1.Filezilla сервер и клиент

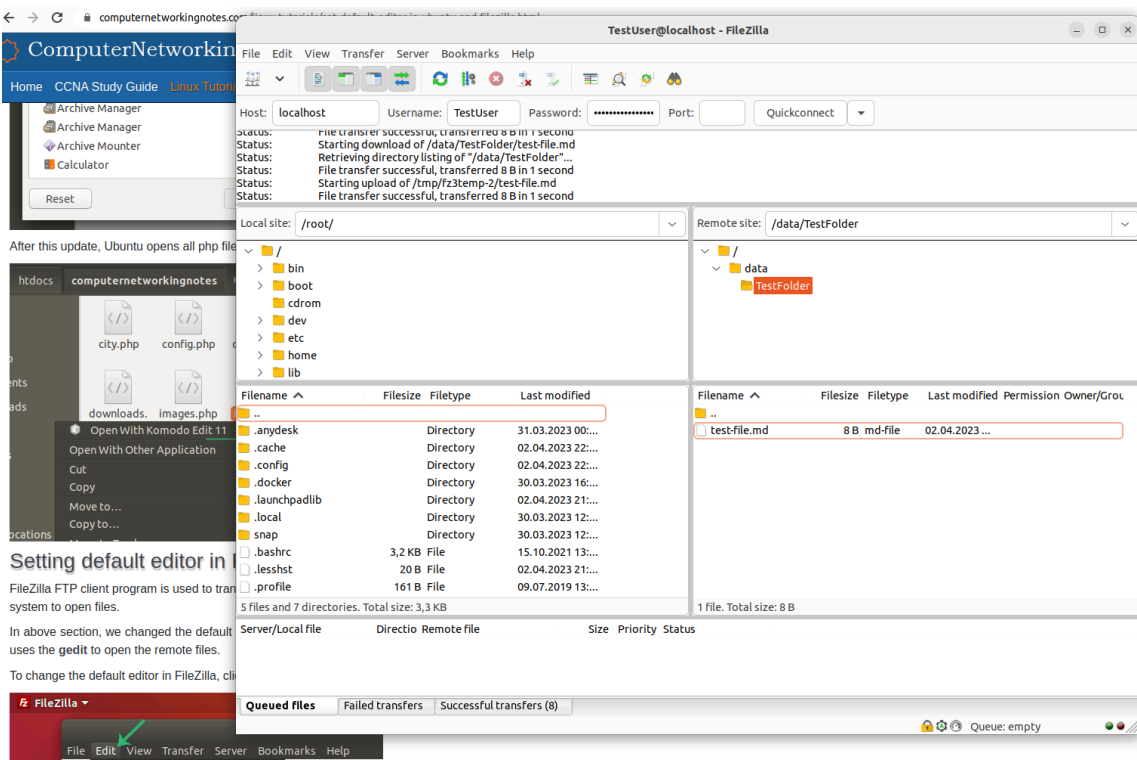
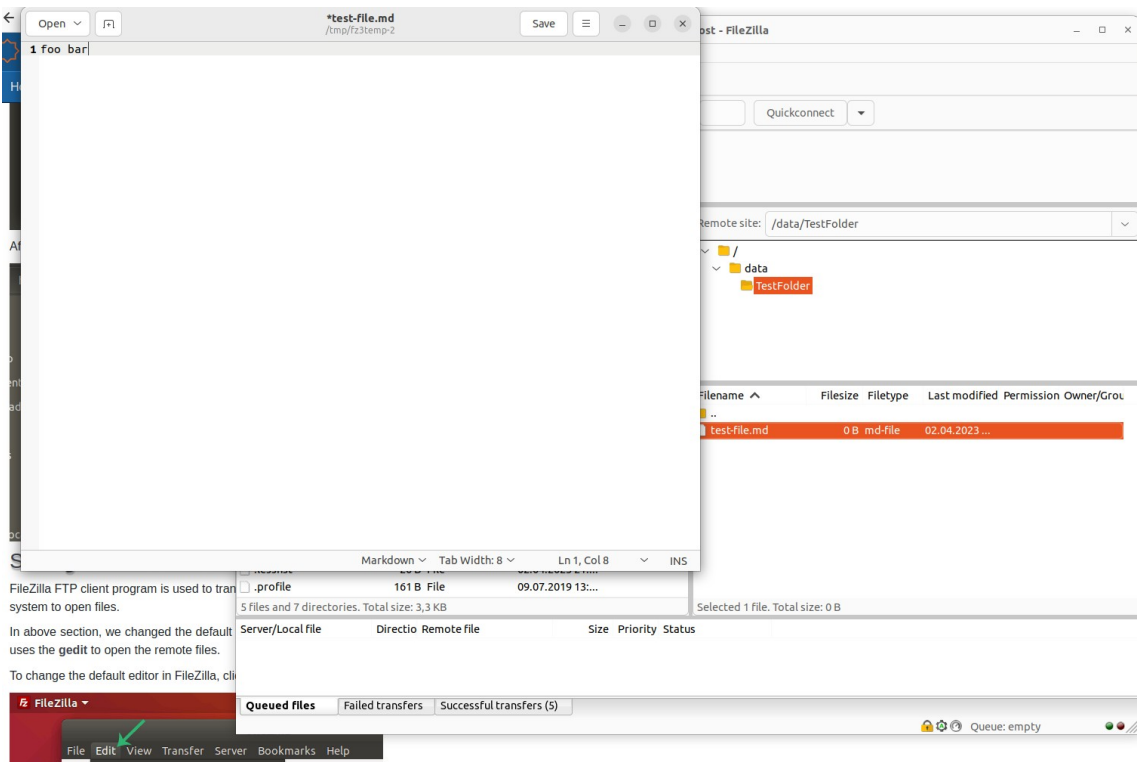
Создадим папку TestFolder:



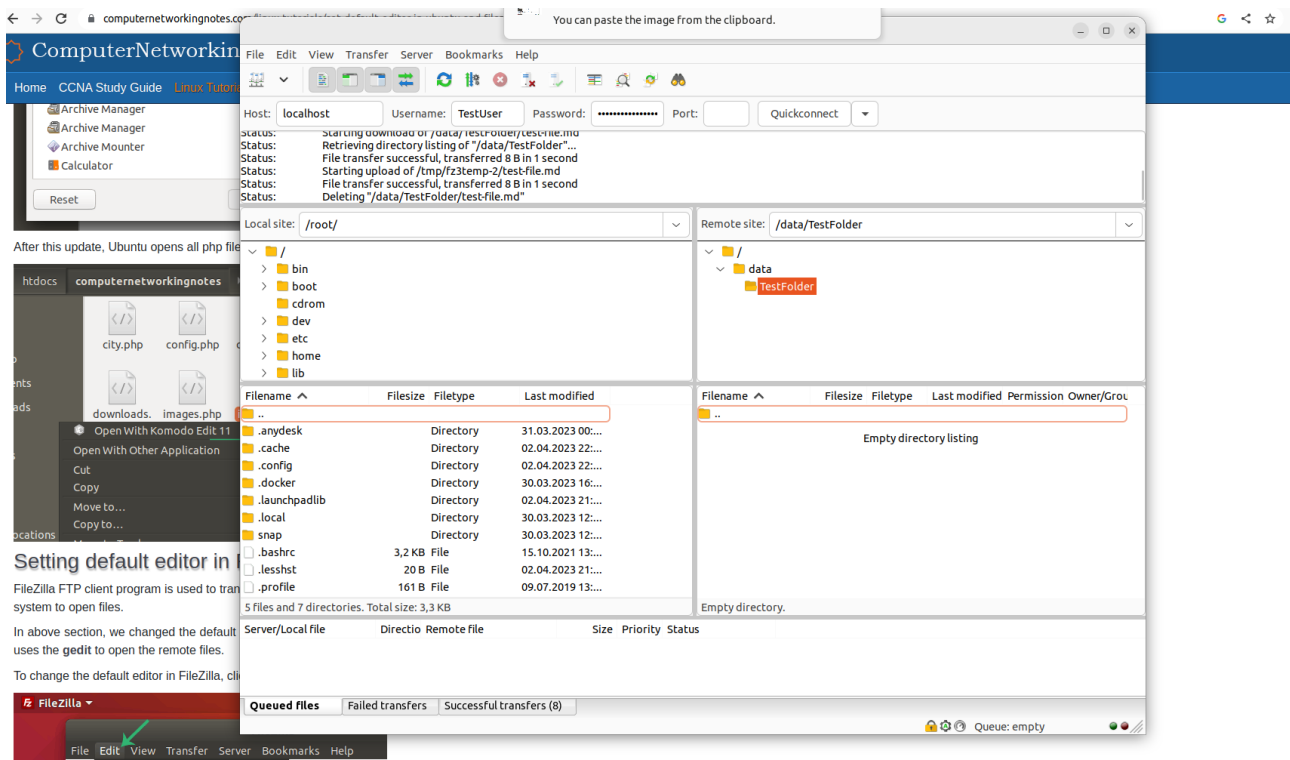
Создадим файл test-file.md



Обновим содержимое файла:



Теперь удалим тестовый файл:



2. FTP-клиент

ruby client.rb -h (справка)

ruby client.rb --host localhost --port 21 --username myusername --password mypassword

```
viralpraxis@primary: ~/Documents/spbu/2023-spring/networks/spbu-masters-compnet/homeworks/06$ ls
assets ftp report.odt report.pdf
viralpraxis@primary:~/Documents/spbu/2023-spring/networks/spbu-masters-compnet/homeworks/06$ ruby ftp/client.rb
CONNECTED
/: ls
swapfile
proc
root
dev
lib32
etc
cdrom
bin
snap
run
boot
sbin
lib64
srv
lost+found
sys
lib
mnt
tmp
var
libx32
media
opt
usr
home
/:
```

Походим по папкам, зайдем в /tmp и сделаем ls (FTP-команда LIST/NSLT):

```

/: cd home
/home: ls
testuser
viralpraxis
/home: cd /tmp
/tmp: ls
systemd-private-3800c3fe2aea49d581545aeba723e16f-power-profiles-daemon.service-sD0Smp
.X11-unix
tracker-extract-3-files.128
snap-private-tmp
OSL_PIPE_1000_SingleOfficeIPC_eca9f176fb834e1317cb1c20b7a3
systemd-private-3800c3fe2aea49d581545aeba723e16f-ModemManager.service-5VdB02
.org.chromium.Chromium.SbmQX
systemd-private-3800c3fe2aea49d581545aeba723e16f-bluetooth.service-Nds0an
.X1024-lock
systemd-private-3800c3fe2aea49d581545aeba723e16f-switcheroo-control.service-KH8aMg
.com.google.Chrome.q5JDMD
.XIM-unix
.font-unix
ad_mailbox_2351_0_1_evt_subevt_0
.X0-lock
.ICE-unix
systemd-private-3800c3fe2aea49d581545aeba723e16f-systemd-resolved.service-HznICp
ad_mailbox_2351_0_0_evt_subevt_0
.X1-lock
ad_621_lsysten_evt_subevt_0
systemd-private-3800c3fe2aea49d581545aeba723e16f-upower.service-nWfNUp
scoped_diruzXRq0
systemd-private-3800c3fe2aea49d581545aeba723e16f-systemd-logind.service-GjsExh
.X1025-lock
systemd-private-3800c3fe2aea49d581545aeba723e16f-systemd-timesyncd.service-g75tdB
ad_connect_queue_865_0_evt_subevt_0
.Test-unix
lu241637lh6.tmp
data.txt
tracker-extract-3-files.1000
ad_621_gsystem_evt_subevt_0
systemd-private-3800c3fe2aea49d581545aeba723e16f-colord.service-lIdFEW
systemd-private-3800c3fe2aea49d581545aeba723e16f-systemd-oomd.service-sXGfVx
systemd-private-3800c3fe2aea49d581545aeba723e16f-fwupd.service-8Ei9gl
/tmp: █

```

В /tmp на сервер есть файл data.txt:

```

[sudo] password for viralpraxis:
viralpraxis@primary:/tmp$ cat data.txt
123
456
789
viralpraxis@primary:/tmp$

```

Скачаем этот файл:

```

systemd-private-3800c3fe2aea49d581545aeba723e16f-systemd-oomd.service-sXGfVx
systemd-private-3800c3fe2aea49d581545aeba723e16f-fwupd.service-8Ei9gl
/tmp: get data.txt downloaded-file.txt
[INFO] opened TCP connection with 127.0.0.1/41831
/tmp: █

```

```

viralpraxis@primary:~/Documents/spbu/2023-spring/networks/spbu-masters-compnet/homeworks/06$ ls
assets downloaded-file.txt ftp report.odt report.pdf
viralpraxis@primary:~/Documents/spbu/2023-spring/networks/spbu-masters-compnet/homeworks/06$ cat downloaded-file.txt
123
456
789
viralpraxis@primary:~/Documents/spbu/2023-spring/networks/spbu-masters-compnet/homeworks/06$ █

```

теперь закачаем этот файл по пути “/tmp/upload.txt” на сервер:

```

systemd-private-3800c3fe2aea49d581545aeba723e16f-colord.service-lIdFEW upload.txt
viralpraxis@primary:/tmp$ ls | grep txt
data.txt
upload.txt
viralpraxis@primary:/tmp$ cat upload.txt
123
456
789
viralpraxis@primary:/tmp$ █

```

```

[INFO] opened TCP connection with 127.0.0.1/41831
/tmp: put downloaded-file.txt upload.txt
[INFO] opened TCP connection with 127.0.0.1/60775
/tmp:

```