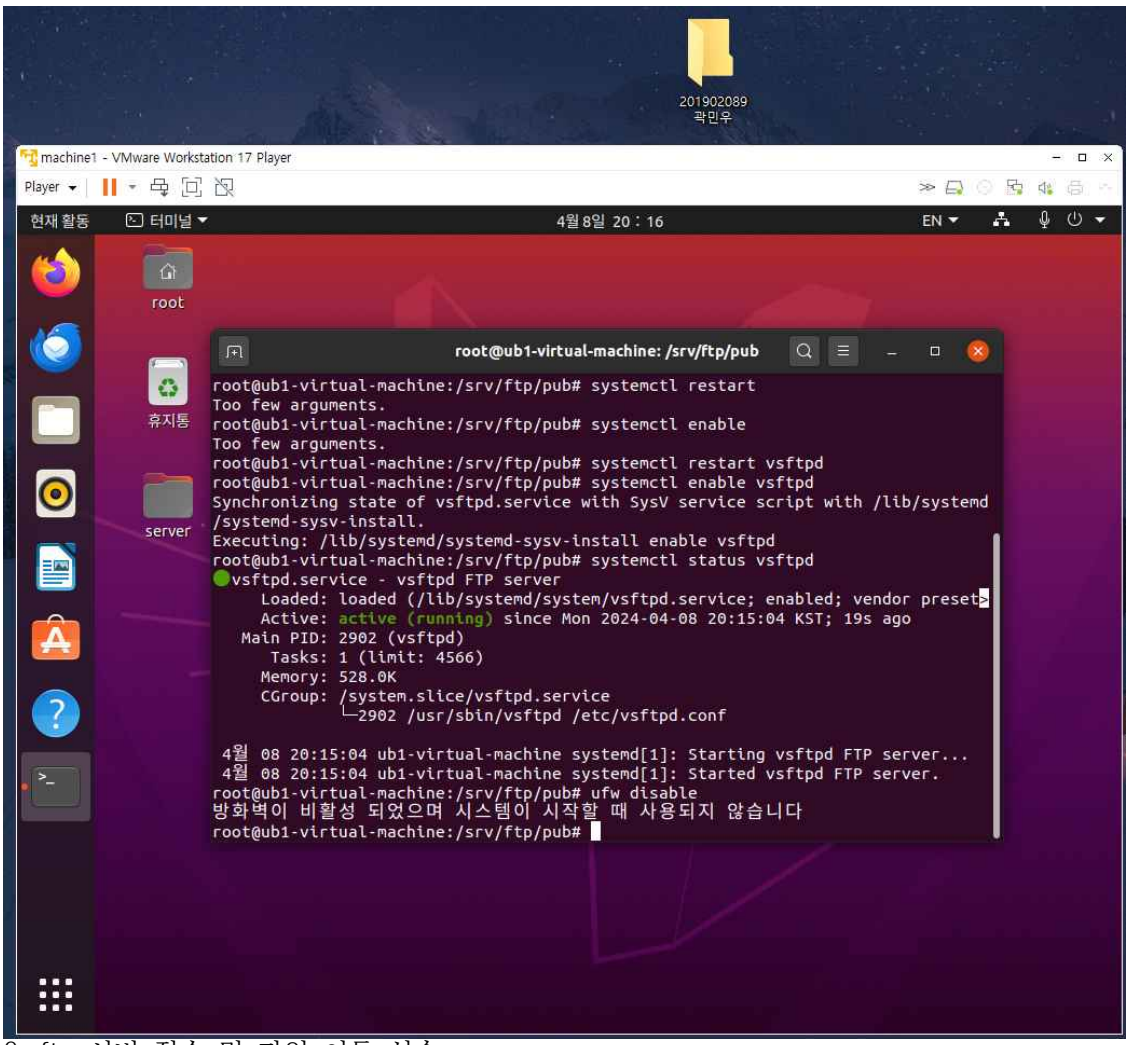
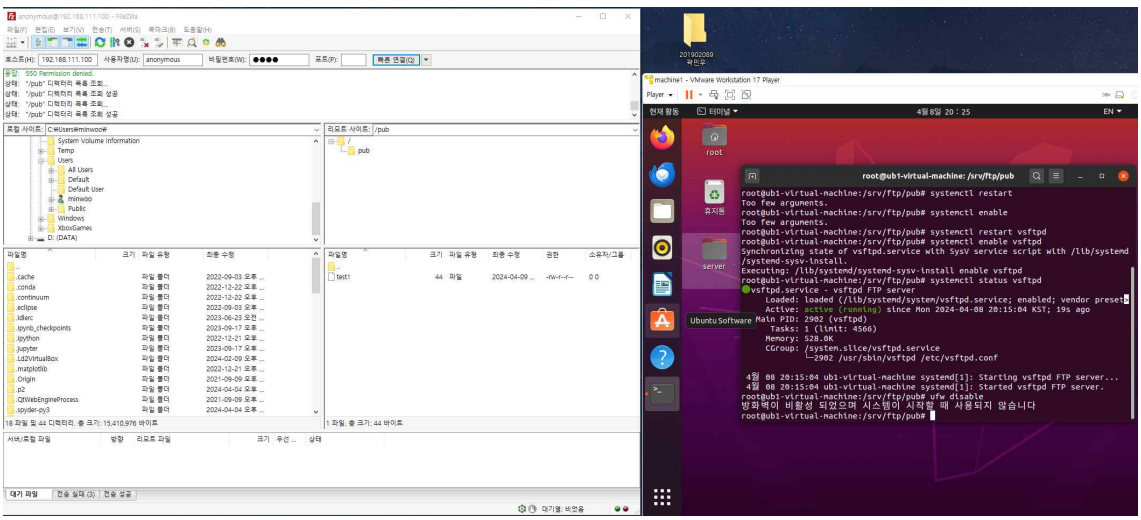
# FTP 서버 구축 및 실험

24.04.08

1. FTP 설정(Linux Ubuntu)




2. ftp 서버 접속 및 파일 이동 실습



3. Wireshark 실습

(1)-1. window에서 Filezilla를 통한 ftp 서버 접속

| | | | | | | |
|---|---|---|---|---|---|---|
| 13 | 124.586… | 192.168.111.1 | 192.168.111.100 | TCP | 66 | 6972 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 14 | 124.587… | 192.168.111.100 | 192.168.111.1 | TCP | 66 | 21 → 6972 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128 |
| 15 | 124.587… | 192.168.111.1 | 192.168.111.100 | TCP | 54 | 6972 → 21 [ACK] Seq=1 Ack=1 Win=1051136 Len=0 |
| 16 | 124.588… | 192.168.111.100 | 192.168.111.1 | FTP | 74 | Response: 220 (vsFTPd 3.0.3) |
| 17 | 124.588… | 192.168.111.1 | 192.168.111.100 | FTP | 64 | Request: AUTH TLS |
| 18 | 124.588… | 192.168.111.100 | 192.168.111.1 | TCP | 60 | 21 → 6972 [ACK] Seq=21 Ack=11 Win=64256 Len=0 |
| 19 | 124.588… | 192.168.111.100 | 192.168.111.1 | FTP | 92 | Response: 530 Please login with USER and PASS. |
| 20 | 124.589… | 192.168.111.1 | 192.168.111.100 | FTP | 64 | Request: AUTH SSL |
| 21 | 124.589… | 192.168.111.100 | 192.168.111.1 | FTP | 92 | Response: 530 Please login with USER and PASS. |
| 22 | 124.600… | 192.168.111.1 | 192.168.111.100 | FTP | 70 | Request: USER anonymous |
| 23 | 124.600… | 192.168.111.100 | 192.168.111.1 | FTP | 88 | Response: 331 Please specify the password. |
| 24 | 124.600… | 192.168.111.1 | 192.168.111.100 | FTP | 65 | Request: PASS 1234 |
| 25 | 124.602… | 192.168.111.100 | 192.168.111.1 | FTP | 77 | Response: 230 Login successful. |
| 26 | 124.603… | 192.168.111.1 | 192.168.111.100 | FTP | 60 | Request: SYST |
| 27 | 124.603… | 192.168.111.100 | 192.168.111.1 | FTP | 73 | Response: 215 UNIX Type: L8 |
| 28 | 124.603… | 192.168.111.1 | 192.168.111.100 | FTP | 60 | Request: FEAT |
| 29 | 124.603… | 192.168.111.100 | 192.168.111.1 | FTP | 69 | Response: 211-Features: |
| 30 | 124.603… | 192.168.111.100 | 192.168.111.1 | FTP | 61 | Response:  EPRT |
| 31 | 124.603… | 192.168.111.1 | 192.168.111.100 | TCP | 54 | 6972 → 21 [ACK] Seq=60 Ack=195 Win=1050880 Len=0 |
| 32 | 124.603… | 192.168.111.100 | 192.168.111.1 | FTP | 61 | Response:  EPSV |
| 33 | 124.603… | 192.168.111.100 | 192.168.111.1 | FTP | 61 | Response:  MDTM |
| 34 | 124.603… | 192.168.111.1 | 192.168.111.100 | TCP | 54 | 6972 → 21 [ACK] Seq=60 Ack=209 Win=1050880 Len=0 |
| 35 | 124.603… | 192.168.111.100 | 192.168.111.1 | FTP | 61 | Response:  PASV |
| 36 | 124.603… | 192.168.111.100 | 192.168.111.1 | FTP | 68 | Response:  REST STREAM |
| 37 | 124.603… | 192.168.111.1 | 192.168.111.100 | TCP | 54 | 6972 → 21 [ACK] Seq=60 Ack=230 Win=1050880 Len=0 |
| 38 | 124.603… | 192.168.111.100 | 192.168.111.1 | FTP | 61 | Response:  SIZE |
| 39 | 124.603… | 192.168.111.100 | 192.168.111.1 | FTP | 61 | Response:  TVFS |
| 40 | 124.603… | 192.168.111.1 | 192.168.111.100 | TCP | 54 | 6972 → 21 [ACK] Seq=60 Ack=244 Win=1050880 Len=0 |
| 41 | 124.603… | 192.168.111.100 | 192.168.111.1 | FTP | 63 | Response: 211 End |
| 42 | 124.606… | 192.168.111.1 | 192.168.111.100 | FTP | 59 | Request: PWD |
| 43 | 124.606… | 192.168.111.100 | 192.168.111.1 | FTP | 88 | Response: 257 "/" is the current directory |
| 44 | 124.606… | 192.168.111.1 | 192.168.111.100 | FTP | 62 | Request: TYPE I |
| 45 | 124.606… | 192.168.111.100 | 192.168.111.1 | FTP | 85 | Response: 200 Switching to Binary mode. |
| 46 | 124.606… | 192.168.111.1 | 192.168.111.100 | FTP | 60 | Request: PASV |
| 47 | 124.606… | 192.168.111.100 | 192.168.111.1 | FTP | 108 | Response: 227 Entering Passive Mode (192,168,111,100,139,162). |
| 48 | 124.607… | 192.168.111.1 | 192.168.111.100 | FTP | 60 | Request: LIST |
| 49 | 124.607… | 192.168.111.1 | 192.168.111.100 | TCP | 66 | 6973 → 35746 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM |
| 50 | 124.607… | 192.168.111.100 | 192.168.111.1 | TCP | 66 | 35746 → 6973 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128 |
| 51 | 124.607… | 192.168.111.1 | 192.168.111.100 | TCP | 54 | 6973 → 35746 [ACK] Seq=1 Ack=1 Win=4194304 Len=0 |
| 52 | 124.607… | 192.168.111.100 | 192.168.111.1 | FTP | 93 | Response: 150 Here comes the directory listing. |
| 53 | 124.607… | 192.168.111.100 | 192.168.111.1 | FTP-DA… | 115 | FTP Data: 61 bytes (PASV) (LIST) |
| 54 | 124.607… | 192.168.111.100 | 192.168.111.1 | TCP | 60 | 35746 → 6973 [FIN, ACK] Seq=62 Ack=1 Win=64256 Len=0 |
| 55 | 124.607… | 192.168.111.1 | 192.168.111.100 | TCP | 54 | 6973 → 35746 [ACK] Seq=1 Ack=63 Win=4194176 Len=0 |
| 56 | 124.607… | 192.168.111.1 | 192.168.111.100 | TCP | 54 | 6973 → 35746 [FIN, ACK] Seq=1 Ack=63 Win=4194176 Len=0 |
| 57 | 124.607… | 192.168.111.100 | 192.168.111.1 | TCP | 60 | 35746 → 6973 [ACK] Seq=63 Ack=2 Win=64256 Len=0 |
| 58 | 124.607… | 192.168.111.100 | 192.168.111.1 | FTP | 78 | Response: 226 Directory send OK. |
| 59 | 124.607… | 192.168.111.1 | 192.168.111.100 | TCP | 54 | 6972 → 21 [ACK] Seq=85 Ack=435 Win=1050624 Len=0 |

- 맨 처음 6972 -> 21인 것을 보아 client는 port number를 6972로 설정한 것으로 보임
- 13, 14, 15번 packet을 보아 client와 server간 3-way-handshake를 한 것을 볼 수 있음 (Client의 active open). (하지만 server가 passive open 하는 과정은 보이지 않아서 캡처하지 못했습니다.)

Client : 192.168.111.1, Server : 192.168.111.100

(1)-2. packet 별 분석(이하 packet은 모두 Control Connection)

| No. | Src, Dst | Message | Meaning |
|---|---|---|---|
| 16 | Ser->Cli | Response : 220 | Service for new user |
| 17 | Cli->Ser | Request : AUTH TLS | Transport Layer Security Auth |
| 18 | Ser->Cli | ACK | ACK of No.17 |
| 19 | Ser->Cli | Response : 530 | Please login with USER and PASS |
| 20 | Cli->Ser | Request : AUTH SSL | Secure sockets Layer Auth |
| 21 | Ser->Cli | Response : 530 | Please login with USER and PASS |
| 22 | Cli->Ser | Request | USER anonymous |
| 23 | Ser->Cli | Response : 331 | please specify the password. |
| 24 | Cli->Ser | Request | PASS 1234 |
| 25 | Ser->Cli | Response : 230 | Login Successful. |
| 26 | Cli->Ser | Request : SYST | System Type? |
| 27 | Ser->Cli | Response : 215 | UNIX TYPE : L8 |
| 28 | Cli->Ser | Request: FEAT | System Features? |
| 29 | Ser->Cli | Response : 211-Features | System Features are... |
| 30 | Ser->Cli | System의 Feature를 특정하는 packet들이 오고 가는 과정. client는 특징 하나를 받을 때마다 ACK를 server에 전송 | |
| 31 | Cli->Ser | | |
| 32 | Ser->Cli | | |
| 33 | Ser->Cli | | |
| 34 | Cli->Ser | | |
| 35 | Ser->Cli | | |
| 36 | Ser->Cli | | |
| 37 | Cli->Ser | | |
| 38 | Ser->Cli | | |
| 39 | Ser->Cli | | |
| 40 | Cli->Ser | | |
| 41 | Ser->Cli | Response : 211 End | System Features End |
| 42 | Cli->Ser | Request : PWD | 현재 디렉토리 경로 이름? |
| 43 | Ser->Cli | Response : 257 | '/' is the current directory |
| 44 | Cli->Ser | Request : Type I | Want to Change into Binary mode |
| 45 | Ser->Cli | Response : 200(OK) | Switching to Binary mode |
| 46 | Cli->Ser | Request: PASV | Want to change into PASV mode |
| 47 | Ser->Cli | Response : 227 (192,168,111,100,139,162) | Entering Passive mode, IP 주소와 port number를 전송한다. IP : 192.168.111.100 Port Number : 35746 |
| 48 | Cli->Ser | Request : LIST | 파일 목록 표시 |

이후 Client는 35746번 port를 이용해 Active open을 수행한다. (packet 49~51번)

| | | | |
|---|---|---|---|
| 52 | Ser->Cli | Response : 150 | Here comes the Directory Listing |
| 53 | Ser->Cli | FTP data : 61bytes | 하단 캡처 참조 |
| 54 | 4-way-handshaking<br>Connection closing | | |
| 55 | | | |
| 56 | | | |
| 57 | | | |
| 58 | Ser->Cli | Response : 226(Closing) | Directory Send OK. |
| 59 | Cli->Ser | ACK | ACK of No. 58 |

※ 53~57번은 6973 <-> 35746 간의 data connection 과정이다.

※ 53번 Packet

```
Frame 53: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface \Device\NPF_
Ethernet II, Src: VMware_b5:3a:45 (00:0c:29:b5:3a:45), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
Internet Protocol Version 4, Src: 192.168.111.100, Dst: 192.168.111.1
Transmission Control Protocol, Src Port: 35746, Dst Port: 6973, Seq: 1, Ack: 1, Len: 61
FTP Data (61 bytes data)
[Setup frame: 47]
[Setup method: PASV]
[Command: LIST]
Command frame: 48
[Current working directory: /]
Line-based text data (1 lines)
  drwxrwxrwx    2 0        0            4096 Apr 08 20:25 pub\r\n
```

가장 밑에 파일의 정보가 나와 있다.

(2)-1. 파일 전송

| | | | | | |
|---|---|---|---|---|---|
| 43 | 17.699930 | 192.168.111.1 | 192.168.111.100 | TCP | 66 9395 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 44 | 17.700044 | 192.168.111.100 | 192.168.111.1 | TCP | 66 21 → 9395 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128 |
| 45 | 17.700091 | 192.168.111.1 | 192.168.111.100 | TCP | 54 9395 → 21 [ACK] Seq=1 Ack=1 Win=1051136 Len=0 |
| 46 | 17.702386 | 192.168.111.100 | 192.168.111.1 | FTP | 74 Response: 220 (vsFTPd 3.0.3) |
| 47 | 17.702460 | 192.168.111.1 | 192.168.111.100 | FTP | 64 Request: AUTH TLS |
| 48 | 17.702541 | 192.168.111.100 | 192.168.111.1 | TCP | 60 21 → 9395 [ACK] Seq=21 Ack=11 Win=64256 Len=0 |
| 49 | 17.702598 | 192.168.111.100 | 192.168.111.1 | FTP | 92 Response: 530 Please login with USER and PASS. |
| 50 | 17.702660 | 192.168.111.1 | 192.168.111.100 | FTP | 64 Request: AUTH SSL |
| 51 | 17.702771 | 192.168.111.100 | 192.168.111.1 | FTP | 92 Response: 530 Please login with USER and PASS. |
| 52 | 17.705191 | 192.168.111.1 | 192.168.111.100 | FTP | 70 Request: USER anonymous |
| 53 | 17.705260 | 192.168.111.100 | 192.168.111.1 | FTP | 88 Response: 331 Please specify the password. |
| 54 | 17.705357 | 192.168.111.1 | 192.168.111.100 | FTP | 65 Request: PASS 1234 |
| 55 | 17.707714 | 192.168.111.100 | 192.168.111.1 | FTP | 77 Response: 230 Login successful. |
| 56 | 17.709583 | 192.168.111.1 | 192.168.111.100 | FTP | 64 Request: CWD /pub |
| 57 | 17.709664 | 192.168.111.100 | 192.168.111.1 | FTP | 91 Response: 250 Directory successfully changed. |
| 58 | 17.709729 | 192.168.111.1 | 192.168.111.100 | FTP | 59 Request: PWD |
| 59 | 17.709813 | 192.168.111.100 | 192.168.111.1 | FTP | 91 Response: 257 "/pub" is the current directory |
| 60 | 17.710440 | 192.168.111.1 | 192.168.111.100 | FTP | 62 Request: TYPE A |
| 61 | 17.710509 | 192.168.111.100 | 192.168.111.1 | FTP | 84 Response: 200 Switching to ASCII mode. |
| 62 | 17.710549 | 192.168.111.1 | 192.168.111.100 | FTP | 60 Request: PASV |
| 63 | 17.710817 | 192.168.111.100 | 192.168.111.1 | FTP | 108 Response: 227 Entering Passive Mode (192,168,111,100,196,202). |
| 64 | 17.710913 | 192.168.111.1 | 192.168.111.100 | FTP | 66 Request: RETR test1 |
| 65 | 17.711125 | 192.168.111.1 | 192.168.111.100 | TCP | 66 9396 → 50378 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM |
| 66 | 17.711186 | 192.168.111.100 | 192.168.111.1 | TCP | 66 50378 → 9396 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128 |
| 67 | 17.711208 | 192.168.111.1 | 192.168.111.100 | TCP | 54 9396 → 50378 [ACK] Seq=1 Ack=1 Win=4194304 Len=0 |
| 68 | 17.711321 | 192.168.111.100 | 192.168.111.1 | FTP | 117 Response: 150 Opening BINARY mode data connection for test1 (44 bytes). |
| 69 | 17.711393 | 192.168.111.100 | 192.168.111.1 | FTP-DA… | 98 FTP Data: 44 bytes (PASV) (RETR test1) |
| 70 | 17.711437 | 192.168.111.100 | 192.168.111.1 | TCP | 60 50378 → 9396 [FIN, ACK] Seq=45 Ack=1 Win=64256 Len=0 |
| 71 | 17.711450 | 192.168.111.1 | 192.168.111.100 | TCP | 54 9396 → 50378 [ACK] Seq=1 Ack=46 Win=4194176 Len=0 |
| 72 | 17.711522 | 192.168.111.100 | 192.168.111.1 | FTP | 78 Response: 226 Transfer complete. |
| 73 | 17.711534 | 192.168.111.1 | 192.168.111.100 | TCP | 54 9395 → 21 [ACK] Seq=89 Ack=399 Win=1050624 Len=0 |
| 74 | 17.711563 | 192.168.111.1 | 192.168.111.100 | TCP | 54 9396 → 50378 [FIN, ACK] Seq=1 Ack=46 Win=4194176 Len=0 |
| 75 | 17.711594 | 192.168.111.100 | 192.168.111.1 | TCP | 60 50378 → 9396 [ACK] Seq=46 Ack=2 Win=64256 Len=0 |

파일 전송을 하기 위해선 로그인을 다시 시도해야 했습니다. 55번 packet까지는 같습니다. Client port number : 9395, 그리고 ASCII mode로 전환하는 것에서 차이가 있습니다. (No. 60 Packet)

(2)-2 Packet 분석

| | | | |
|---|---|---|---|
| 64 | Cli->Ser | Request : RETR test1 | test1 파일 전송 바람 |
| 65 | Active Open by 3-way-handshaking (Client Port : 9396, Server port : 50378) | | |
| 66 | | | |
| 67 | | | |
| 68 | Ser->Cli | Response: 150 | 파일 여는 중: Into Binary |
| 69 | Ser->Cli | FTP data: 44 Bytes | 하단 캡처 참조 |
| 70 | Server -> Client 방향 Connection 종료(2-way) | | |
| 71 | | | |
| 72 | Ser->Cli | Response : 226 | Transfer Complete. |
| 73 | Cli->Ser | ACK | ACK of No. 72 |
| 74 | Client -> Server 방향 Connection 종료(2-way) | | |
| 75 | | | |

※ 69번 Packet

```
Frame 69: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{B
Ethernet II, Src: VMware_b5:3a:45 (00:0c:29:b5:3a:45), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
Internet Protocol Version 4, Src: 192.168.111.100, Dst: 192.168.111.1
Transmission Control Protocol, Src Port: 50378, Dst Port: 9396, Seq: 1, Ack: 1, Len: 44
FTP Data (44 bytes data)
[Setup frame: 63]
[Setup method: PASV]
[Command: RETR test1]
Command frame: 64
[Current working directory: /pub]
Line-based text data (2 lines)
    testfile 1, 2, 3\n
    qwertyuiopasdfghjklzxcvbnm\n
```

※ 실제 test1 파일 내용

```
열기(O)                    test1
                           /srv/ftp/pub
1 testfile 1, 2, 3
2 qwertyuiopasdfghjklzxcvbnm
```