

dropbear Connection to Android Userland Ubuntu

```
Activities Terminal Ahd 12 Nov, 10:13 userland@localhost: ~
hongwu@hongwu-Latitude-5480:~$ dbclient -p 2023 userland@192.168.17.174
userland@localhost:~$ ls -la
total 36989
drwxr-x---. 6 userland userland 3452 Nov 12 01:27 .
drwxr-xr-x. 3 userland userland 3452 Nov 11 08:45 ..
-rw-----. 1 userland userland 55 Nov 12 00:32 .Xauthority
-rw-----. 1 userland userland 43 Nov 12 01:27 .bash_history
-rw-r--r--. 1 userland userland 220 Jan 6 2022 .bash_logout
-rw-r--r--. 1 userland userland 3771 Jan 6 2022 .bashrc
drwx-----. 3 userland userland 3452 Nov 11 11:14 .config
-rw-----. 1 userland userland 20 Nov 12 00:12 .lessht
drwx-----. 3 userland userland 3452 Nov 11 10:55 .local
-rw-r--r--. 1 userland userland 807 Jan 6 2022 .profile
drwx-----. 2 userland userland 3452 Nov 11 11:13 .ssh
drwx-----. 2 userland userland 3452 Nov 12 00:32 .vnc
-rw-rw-r--. 1 userland userland 25 Nov 12 00:32 .vncrc
-rw-----. 1 userland userland 852 Nov 12 00:32 .xsession-errors
-rw-r--r--. 1 userland userland 5634423 Nov 11 11:07 dmeta-231111.tgz
-rwxr-xr-x. 1 userland userland 23986176 Nov 3 15:20 ngrok
-rw-r--r--. 1 userland userland 8161186 Nov 11 11:14 'ngrok-v3-stable-linux-arm64(1).tgz'
userland@localhost:~$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCrDzQ0PH+JK9nIEKRsX9IVXWS3GkQ9BWuWJ1t722BoQdoYY2olpPtlSjc9mHj89p0Au
E1DZvlk8T4yMHkEVCe8+ToYccLynRcOKBFLOxld7EXC+fXudWfE4KD2u2Y0aP9y0qelIbcFw2imwglLa27Ame000vHw7M/2U9GXhdAZzn
y1Ne7IqAvM2Df+16DTdMJfwGcPouAs1yavkgGT8suSejIrLviMkEf/nXRMW6wXegGsENIdcv1QDfM0FkUsFr9QgwWjmh9baGTMxGRCDW
35A3ovb9Sbsy7LP9rj1pxCYxsvvWXzVcrQfNdYtgch/T7p1N9B6jrmWG6G3QqYH/ hongwu@hongwu-Latitude-5480
userland@localhost:~$
```

In this tutorial, we demonstrate and explain how to set up dropbear (ssh clone) server in Userland Ubuntu (Userland = Linux virtual machine in Android, screenshot below), and connect to it using *dbclient* (screenshot above).

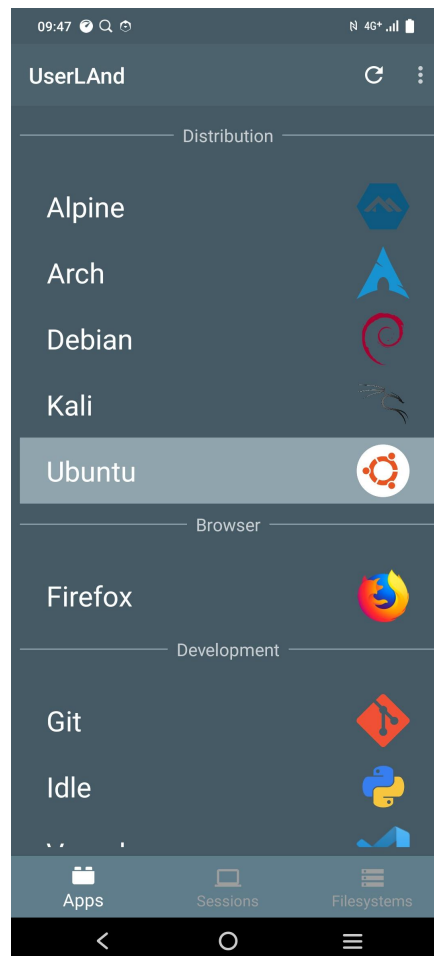


Figure 2

1. Install Userland from Google Play Store:

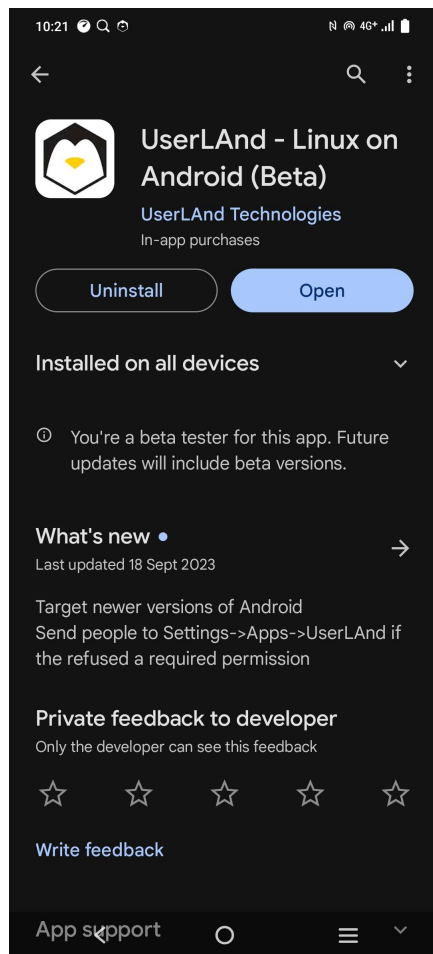


Figure 3

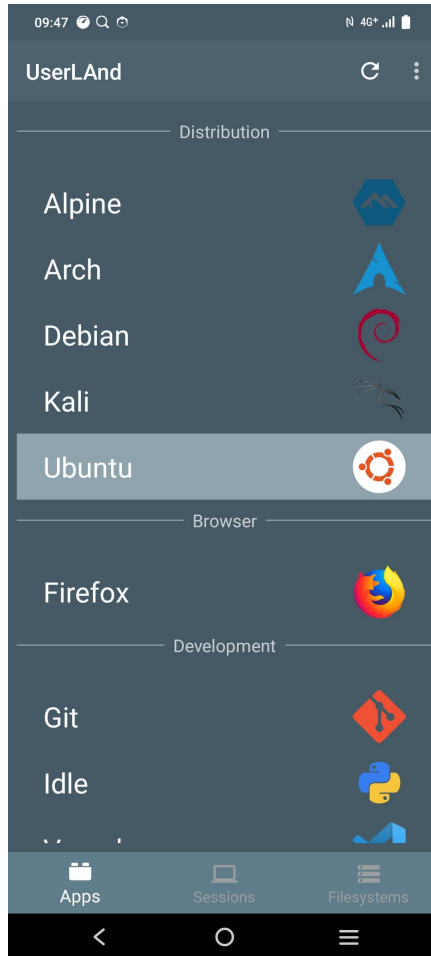


Figure 4

2. Click on Ubuntu in Figure 4. Choose Graphical mode when prompted.

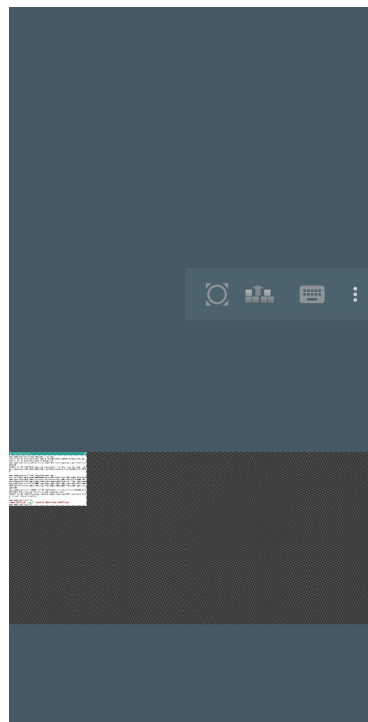


Figure 5



Figure 6

You will see something like shown in figure 5, expanded in figure 6.

It is actually an X terminal (white background, green tab at the top) on a X window background (grey black texture).

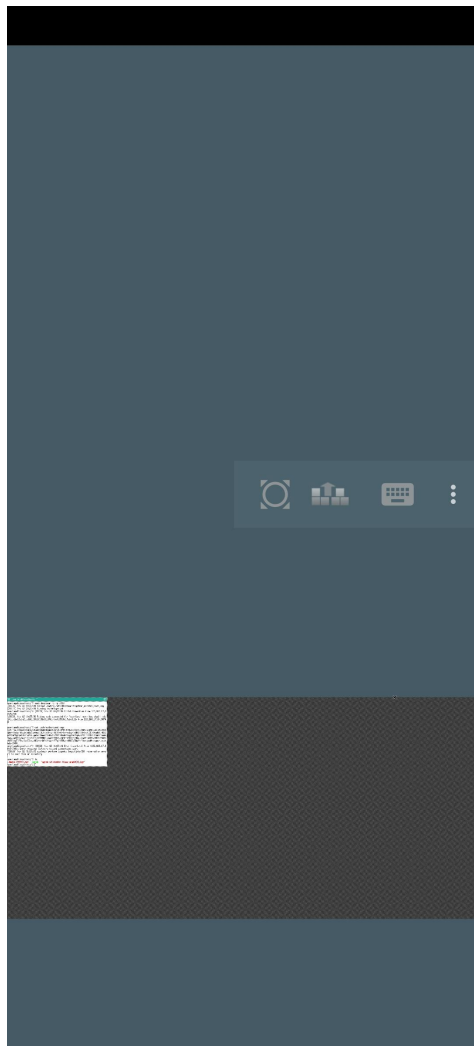


Figure 7

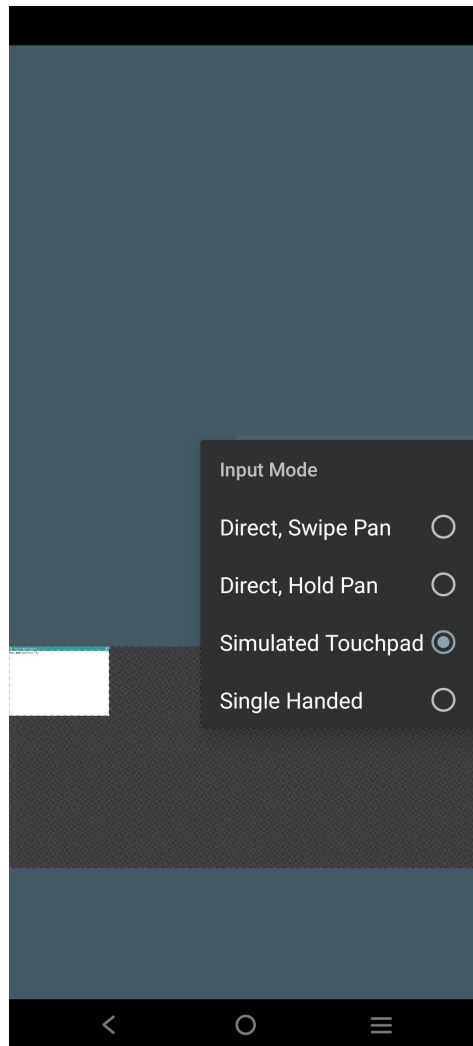


Figure 8

3. In order to zoom in, tap on the screen in Figure 7, so that the screen control icons (middle right of the screen) appear, then press the three vertical dots icon, and choose “Simulated Touchpad”. Then you will be able to zoom in by placing two fingers on the screen and extending the distance between your fingers. Then you may move the mouse pointer by dragging your fingers on the screen like a touchpad.

At this point, you may be wondering why on Earth does such user unfriendly software still exist in 2023 (going to be 2024 soon)? The answer is a long story, but the solution we are offering is based on the fundamental and ubiquitous hash function, which surely every programmer knows, which then raises more questions (see Appendix A for DMeta Hash Contract: Creating Contracts using Hash Values.)

- This tutorial is part of DMeta Decentralised Metaverse, a collaboration project for all free software programmers and individual users to use DMeta Hash Contract to mark ownership of source code and private data, and building a “decentralised metaverse”

owned and operated by “the people”, using building blocks marked with DMeta Hash Contract.

Generating RSA keypair for dropbear

1. The following are screenshots of “man dropbearkey” (man = manual pages in Linux).



```
dropbearkey(1)                                General Commands Manual                                dropbearkey(1)

NAME
    dropbearkey - create private keys for the use with dropbear(8) or dbclient(1)

SYNOPSIS
    dropbearkey -t type -f file [-s bits] [-y]

DESCRIPTION
    dropbearkey generates a RSA, DSS, or ECDSA format SSH private key, and saves it to a file for
    the use with the Dropbear client or server. Note that some SSH implementations use the term
    "DSA" rather than "DSS", they mean the same thing.

OPTIONS
    -t type
        Type of key to generate. Must be one of rsa ecdsa or dss.

    -f file
        Write the secret key to the file file. For client authentication ~/.ssh/id_dropbear is
        loaded by default

    -s bits
        Set the key size to bits bits, should be multiple of 8 (optional).

    -y
        Just print the publickey and fingerprint for the private key in file.

Manual page dropbearkey(1) line 1 (press h for help or q to quit)
```

Figure 9



```
        Set the key size to bits bits, should be multiple of 8 (optional).

    -y
        Just print the publickey and fingerprint for the private key in file.

NOTES
    The program dropbearconvert(1) can be used to convert between Dropbear and OpenSSH key formats.

    Dropbear does not support encrypted keys.

EXAMPLE
    generate a host-key:
    # dropbearkey -t rsa -f /etc/dropbear/dropbear_rsa_host_key

    extract a public key suitable for authorized_keys from private key:
    # dropbearkey -y -f id_rsa | grep "^ssh-rsa " >> authorized_keys

AUTHOR
    Matt Johnston (matt@ucc.asn.au).
    Gerrit Pape (pape@smarden.org) wrote this manual page.

SEE ALSO
    dropbear(8), dbclient(1), dropbearconvert(1)

    https://matt.ucc.asn.au/dropbear/dropbear.html

dropbearkey(1)

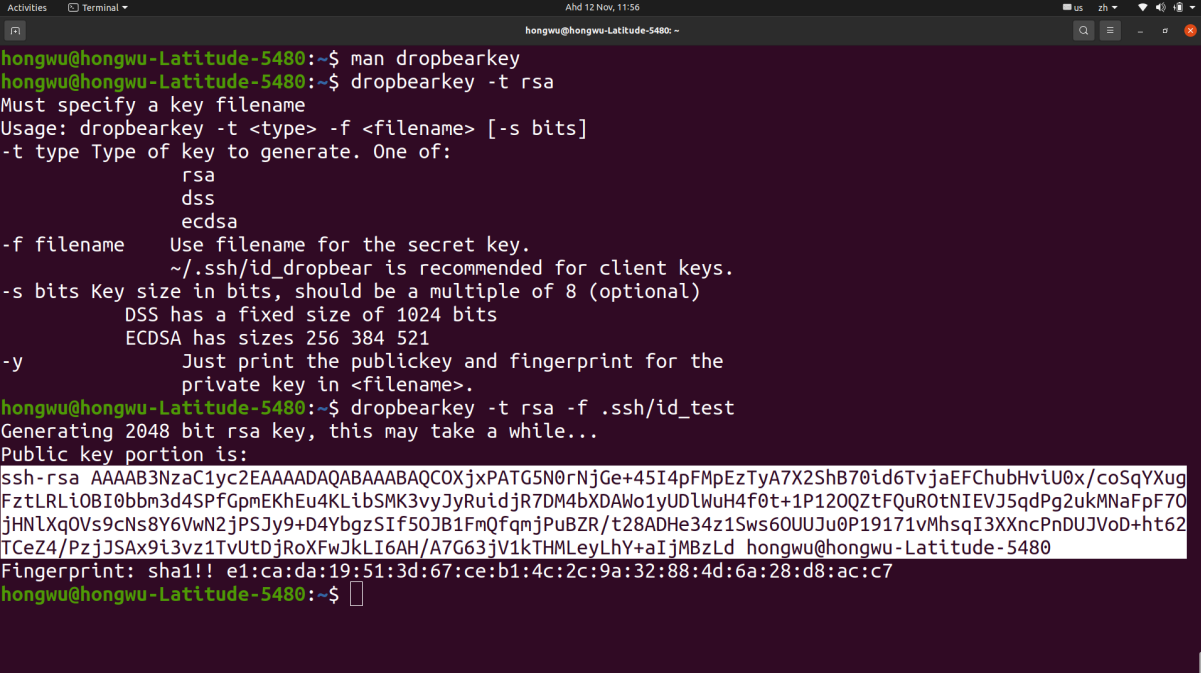
Manual page dropbearkey(1) line 23/48 (END) (press h for help or q to quit)
```

Figure 10

2. Generate RSA keypair (private key and public key):


```
$ dropbearkey -t rsa -f .ssh/id_test
```

Public key portion will be shown, as highlighted in the screenshot below. Copy the whole line (one very long line spanning 4 lines on screen in figure 11, starting with “ssh-rsa” ending with user@host) and paste it into your Gmail account, or any other app, that you can open on your Userland mobile phone, so that you can paste this public key into ~/.ssh/authorized_keys file (figure 12).



```
hongwu@hongwu-Latitude-5480:~$ man dropbearkey
hongwu@hongwu-Latitude-5480:~$ dropbearkey -t rsa
Must specify a key filename
Usage: dropbearkey -t <type> -f <filename> [-s bits]
-t type Type of key to generate. One of:
    rsa
    dss
    ecdsa
-f filename Use filename for the secret key.
    ~/.ssh/id_dropbear is recommended for client keys.
-s bits Key size in bits, should be a multiple of 8 (optional)
    DSS has a fixed size of 1024 bits
    ECDSA has sizes 256 384 521
-y Just print the publickey and fingerprint for the
    private key in <filename>.
hongwu@hongwu-Latitude-5480:~$ dropbearkey -t rsa -f .ssh/id_test
Generating 2048 bit rsa key, this may take a while...
Public key portion is:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCOXjxPATG5N0rNjGe+45I4pFMpEzTyA7X2ShB70id6TvjaEFChubHviU0x/coSqYXug
FztLRLi0BI0bbm3d4SPfGpmEKHEu4KLibSMK3vyJyRuidjR7DM4bXDAWo1yUDLWuH4f0t+1P120QZtFQuR0tNIEVJ5qdPg2ukMNaFpF70
jHNLXq0Vs9cNs8Y6VwN2jPSJy9+D4YbgzSIf50JB1FmQfQmjPuBZR/t28ADHe34z1Sws60UUJ0P19171vMhsqI3XXncPnDUJVoD+ht62
TCeZ4/PzjJSAx9i3vz1TvUtdjRoXFWJkLI6AH/A7G63jV1kTHMLeyLHy+aIjMBzLd hongwu@hongwu-Latitude-5480
Fingerprint: sha1!! e1:ca:da:19:51:3d:67:ce:b1:4c:2c:9a:32:88:4d:6a:28:d8:ac:c7
hongwu@hongwu-Latitude-5480:~$
```

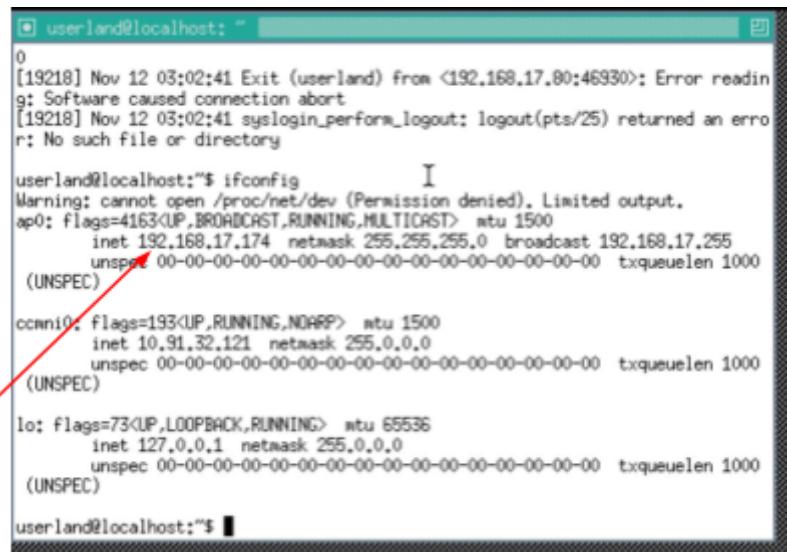
Figure 11



```
userland@localhost:~$ sudo dropbear -E -p 2023
[28826] Nov 12 00:33:28 Failed loading /etc/dropbear.
[28827] Nov 12 00:33:28 Running in background
userland@localhost:~$ [28828] Nov 12 00:33:36 Child i
0:50748
[28828] Nov 12 00:33:36 Pubkey auth succeeded for 'u:
14:da:bd:5a:a2:cd:61:20:b5:5b:8d:89:a0:e0:35:8d:7a:el
8
userland@localhost:~$ cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCOXjxPATG5N0rNjGe+45I4pFMpEzTyA7X2ShB70id6TvjaEFChubHviU0x/coSqYXug
FztLRLi0BI0bbm3d4SPfGpmEKHEu4KLibSMK3vyJyRuidjR7DM4bXDAWo1yUDLWuH4f0t+1P120QZtFQuR0tNIEVJ5qdPg2ukMNaFpF70
jHNLXq0Vs9cNs8Y6VwN2jPSJy9+D4YbgzSIf50JB1FmQfQmjPuBZR/t28ADHe34z1Sws60UUJ0P19171vMhsqI3XXncPnDUJVoD+ht62
TCeZ4/PzjJSAx9i3vz1TvUtdjRoXFWJkLI6AH/A7G63jV1kTHMLeyLHy+aIjMBzLd hongwu@hongwu-Latitude-5480
userland@localhost:~$
```

Figure 12

3. Finding out IP address of Userland Ubuntu server with “ifconfig”:



```

userland@localhost: ~
0
[19218] Nov 12 03:02:41 Exit (userland) from <192.168.17.80:46930>; Error readin
g: Software caused connection abort
[19218] Nov 12 03:02:41 syslogin_perform_logout: logout(pts/25) returned an erro
r: No such file or directory

userland@localhost:~$ ifconfig
Warning: cannot open /proc/net/dev (Permission denied). Limited output.
ap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.17.174 netmask 255.255.255.0 broadcast 192.168.17.255
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000
    (UNSPEC)
ccn0: flags=193<UP,RUNNING,NOARP> mtu 1500
    inet 10.91.32.121 netmask 255.0.0.0
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000
    (UNSPEC)
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000
    (UNSPEC)
userland@localhost:~$
  
```

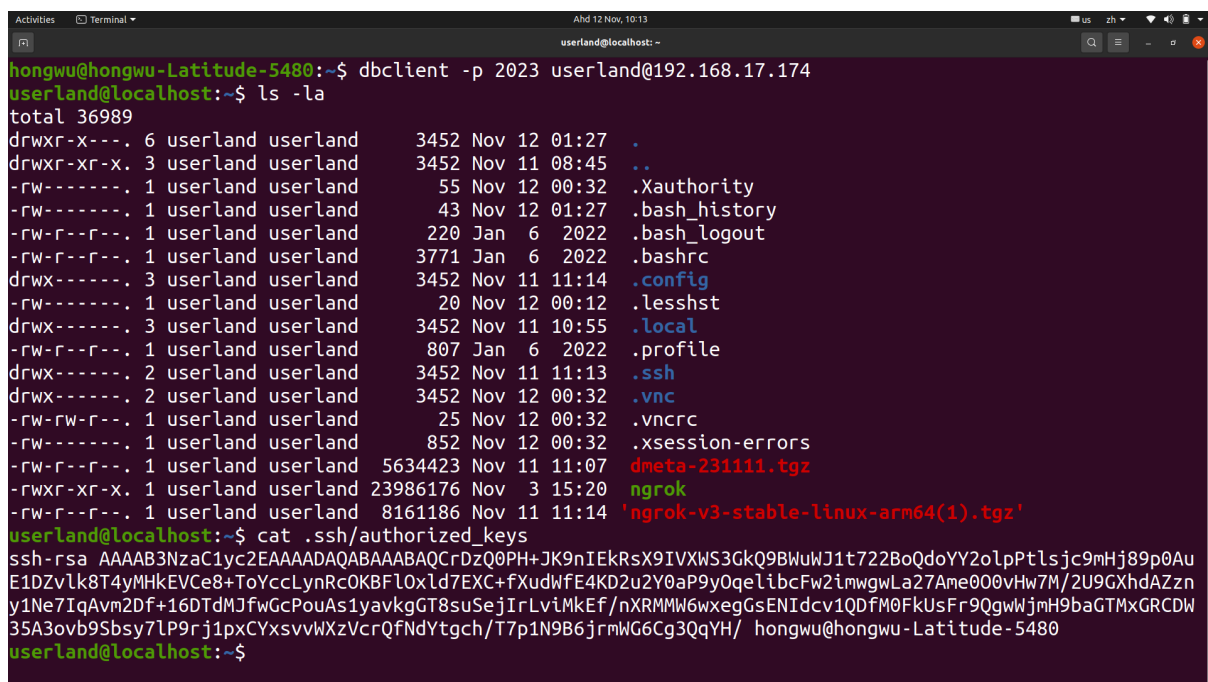
Figure 13

4. Start dropbear server (figure 12):

```
$ sudo dropbear -E -p 2023
```

5. Connect from Ubuntu desktop (hongwu-Latitude-5480) using *dbclient*.

```
$ dbclient -p 2023 userland@192.168.17.174
```



```

Activities  Terminal
Ald 12 Nov, 10:13
userland@localhost: ~
hongwu@hongwu-Latitude-5480:~$ dbclient -p 2023 userland@192.168.17.174
userland@localhost:~$ ls -la
total 36989
drwxr-x---. 6 userland userland 3452 Nov 12 01:27 .
drwxr-xr-x. 3 userland userland 3452 Nov 11 08:45 ..
-rw-r-----. 1 userland userland 55 Nov 12 00:32 .Xauthority
-rw-r-----. 1 userland userland 43 Nov 12 01:27 .bash_history
-rw-r-----. 1 userland userland 220 Jan 6 2022 .bash_logout
-rw-r-----. 1 userland userland 3771 Jan 6 2022 .bashrc
drwx-----. 3 userland userland 3452 Nov 11 11:14 .config
-rw-r-----. 1 userland userland 20 Nov 12 00:12 .lessshst
drwx-----. 3 userland userland 3452 Nov 11 10:55 .local
-rw-r-----. 1 userland userland 807 Jan 6 2022 .profile
drwx-----. 2 userland userland 3452 Nov 11 11:13 .ssh
drwx-----. 2 userland userland 3452 Nov 12 00:32 .vnc
-rw-rw-r--. 1 userland userland 25 Nov 12 00:32 .vncrc
-rw-r-----. 1 userland userland 852 Nov 12 00:32 .xsession-errors
-rw-r-----. 1 userland userland 5634423 Nov 11 11:07 dmeta-231111.tgz
-rwxr-xr-x. 1 userland userland 23986176 Nov 3 15:20 ngrok
-rw-r-----. 1 userland userland 8161186 Nov 11 11:14 'ngrok-v3-stable-linux-arm64(1).tgz'
userland@localhost:~$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCrDzQ0PH+JK9nIEkrsX9IVXWS3GkQ9BWuWJ1t722BoQdoYY2olpPtlSjc9mHj89p0Au
E1DZvlk8T4yMHkEVCe8+ToYccLynRcOKBFLOxld7EXC+fxudwFE4KD2u2Y0aP9y0qelIbcFw2imwglA27Ame000vHw7M/2U9GXhdAZzn
y1Ne7IqAvm2Df+16DTdMJfwGcPouAs1yavkgGT8suSejIrLvIMkEf/nXRMMW6wxegGsENIdcv1QDfM0FkUsFr9QgwWjmH9baGTmxGRCDW
35A3ovb9Sbsy7LP9rj1pxCYxsvvWxzVcrQfNdYtgch/T7p1N9B6jrmW6G6G3QqYH/ hongwu@hongwu-Latitude-5480
userland@localhost:~$
  
```

Figure 14