LAPORAN RESMI
KEAMANAN JARINGAN

PRAKTIKUM 2

"Perbedaan Macam-Macam Tipe Jaringan pada Virtual Box dan Analisa Telnet dan SSH menggunakan Wireshark"

Oleh :
Teesa Wijayanti
3 D3 IT B
2103141036

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

Praktikum 1

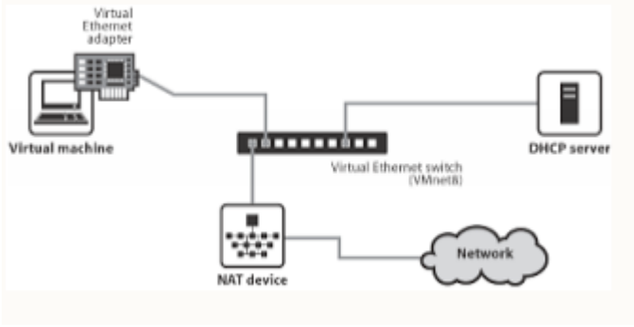
Perbedaan Macam-Macam Tipe Jaringan pada Virtual Box dan Analisa Telnet dan SSH menggunakan Wireshark

Soal :

1. Jelaskan perbedaan macam-macam tipe jaringan pada virtual box!
2. Install telnet dan ssh dengan menggunakan perintah sudo, lalu analisa paketnya dengan menggunakan wireshark!

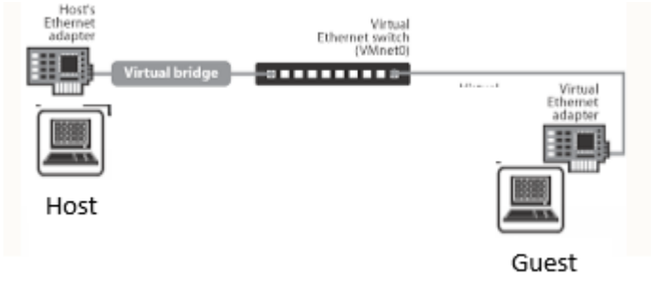
Pembahasan :

1. Macam-macam tipe jaringan pada virtual box :
   - Network Address Translation (NAT)



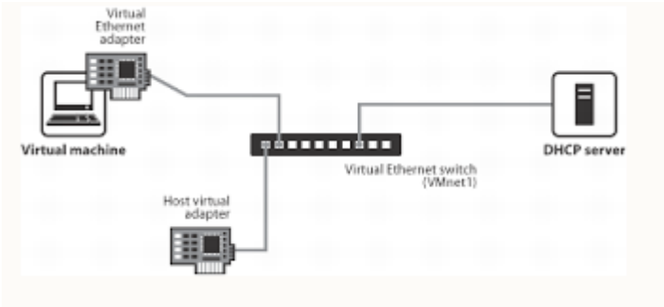
Prinsip kerja NAT yakni **OS virtual atau guest akan memiliki alamat IP yang samadengan host.** Apabila host terhubung dengan internet maka guest akan terhubung pula secara otomatis. Dan NAT yang terdapat didalam virtual box sama dengan NAT pada jaringan fisik.

   - Bridged Adapter



Dalam mode Bridged Adapter ini memungkinkan OS guest untuk merima data maupun mengirimkan data ke jaringan fisik. Jadi artinya **OS guest dan OS host adalah dua computer berbeda yang terhubung ke dalam jaringan yang sama.** Bila OS host memiliki lebih dari satu Ethernet maka kita harus memilih/menyetting ke jaringan mana virtual machine/OS guest akan disambungkan. Dan IP yang diberikan ke Vitual machine harus dari subnet yang sama dengan jaringan yang di pakai oleh OS host. Mode ini sangat cocok untuk membuat emulasi jaringan atau menjalankan server di dalam Virtualbox.

- Host-Only Adapter



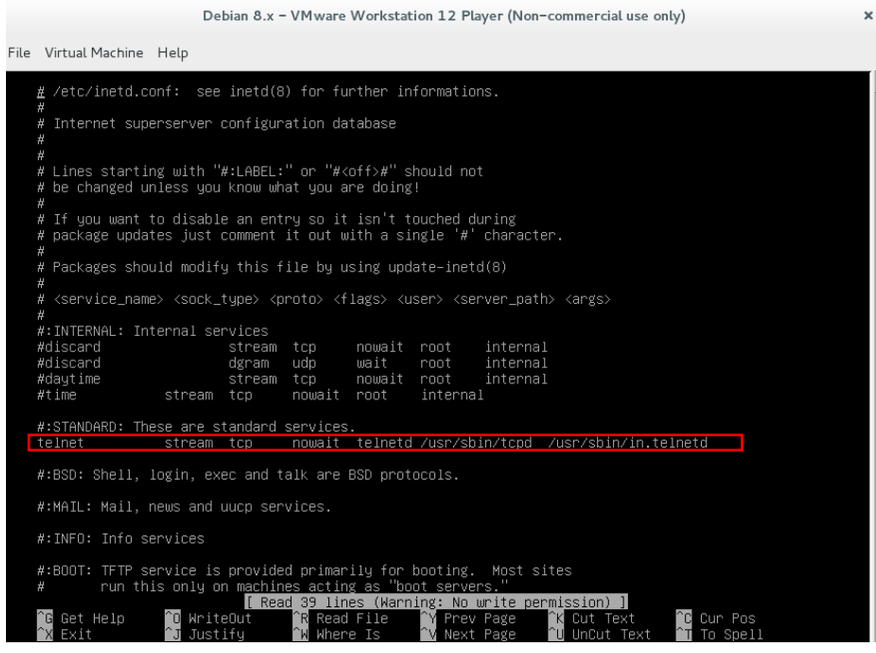
Dalam mode Host-only adapter ini dapat di artikan atau dianggap sebagai gabungan dari mode Bridged dan mode Internal network. Bedanya dengan bridged, host only hanya terbatas pada kelas-kelas yang sama. **Jaringan Host-hanya menyediakan koneksi jaringan antara mesin virtual dan host komputer**, menggunakan adaptor Ethernet virtual yang terlihat oleh sistem operasi host. **Pendekatan ini dapat berguna jika perlu untuk mendirikan sebuah jaringan virtual yang terisolasi.**

2. - Langkah-langkah install telnet menggunakan perintah sudo :

a. Gunakan perintah *sudo apt-get install telnetd* untuk menginstall server telnet.

```
student@debian:~$ sudo apt-get install telnetd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  openbsd-inetd
The following NEW packages will be installed:
  openbsd-inetd telnetd
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 79.0 kB of archives.
After this operation, 230 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kebo.pens.ac.id/debian/ jessie/main openbsd-inetd i386 0.20140418-2 [36.7 kB]
Get:2 http://kebo.pens.ac.id/debian/ jessie/main telnetd i386 0.17-36 [42.3 kB]
Fetched 79.0 kB in 0s (135 kB/s)
Selecting previously unselected package openbsd-inetd.
(Reading database ... 37707 files and directories currently installed.)
Preparing to unpack .../openbsd-inetd_0.20140418-2_i386.deb ...
Unpacking openbsd-inetd (0.20140418-2) ...
Selecting previously unselected package telnetd.
Preparing to unpack .../telnetd_0.17-36_i386.deb ...
Unpacking telnetd (0.17-36) ...
Processing triggers for systemd (215-17+deb8u4) ...
Processing triggers for man-db (2.7.0.2-5) ...
Setting up openbsd-inetd (0.20140418-2) ...
Setting up telnetd (0.17-36) ...
Adding user telnetd to group utmp
Processing triggers for systemd (215-17+deb8u4) ...
student@debian:~$
```

b. Edit file /etc/inetd.conf seperti dibawah ini.

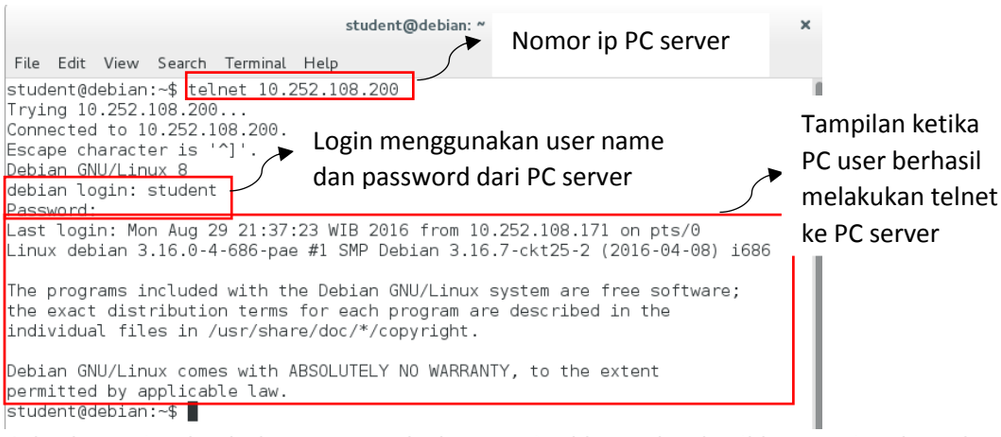


Hal ini akan menjadikan telnet berjalan lewat daemon xinetd yang akan membuat efisien memory karena pengaturan layanan telnet diatur oleh xinetd.

c. Restart service inetd menggunakan perintah /etc/init.d/openbsd-inetd restart

```
student@debian:~$ sudo /etc/init.d/openbsd-inetd restart
[ ok ] Restarting openbsd-inetd (via systemctl): openbsd-inetd.service.
student@debian:~$ _
```

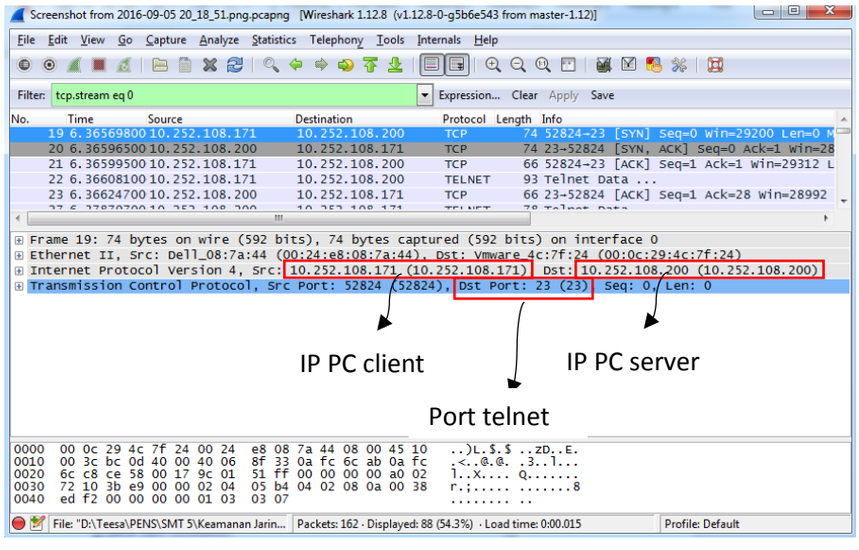
d. Jalankan telnet melalui komputer lain yang terhubung, dengan menggunakan perintah telnet **no ip PC server**, kemudian masukkan user name dan password dari komputer yang ingin di akses (PC client).



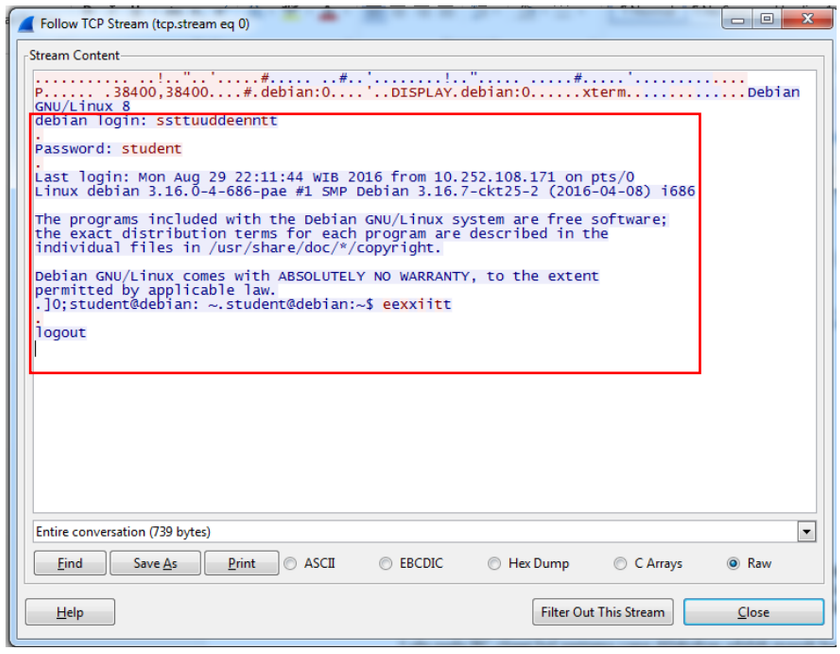
e. Jalankan wireshark dengan cara buka terminal baru dan ketikkan perintah *sudo wireshark*

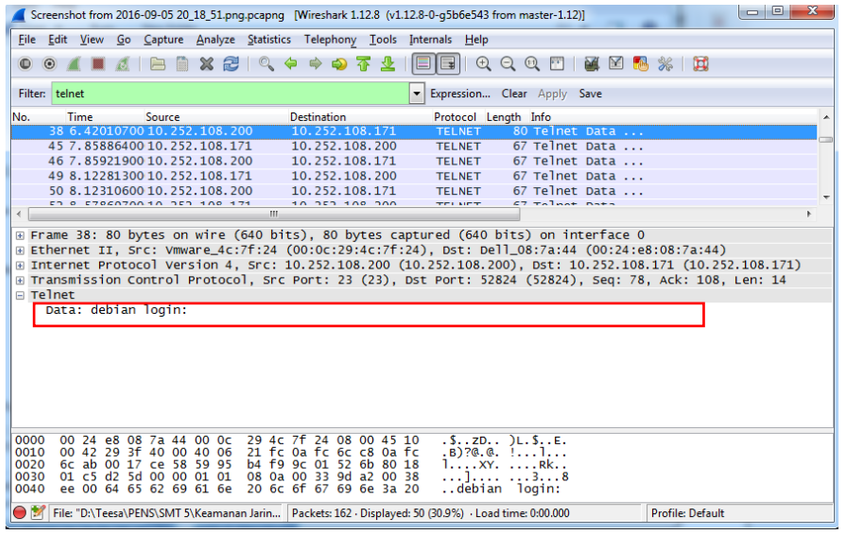
```
student@debian:~$ sudo wireshark
```

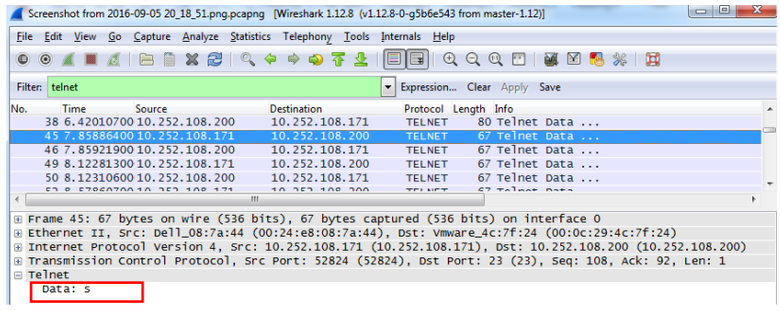
Kemudian wireshark akan terbuka lalu ketikkan **telnet** pada kolom filter, sehingga tampilannya seperti gambar di bawah ini:

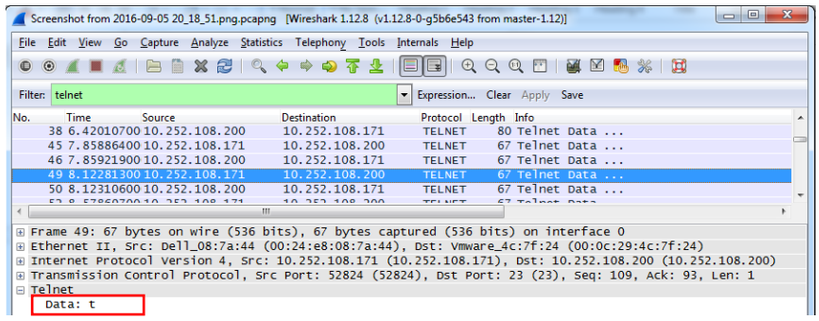


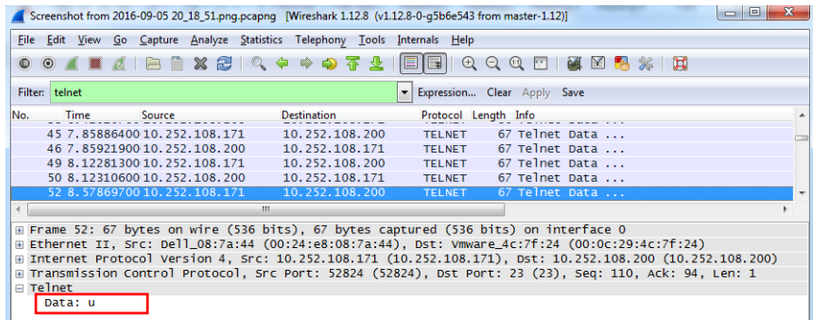
klik kanan pada salah satu paket data, lalu pilih **follow tcp stream** untuk dapat melihat berbagaimacam aksi yang dilakukan oleh user lain / PC client ke PC server yang **berhasil ditangkap oleh wireshark secara jelas termasuk password dari PC server yang dimasukkan oleh client.** Hal ini dikarenakan sifat telnet yang **mentransmisikan data dengan modus clear teks.**

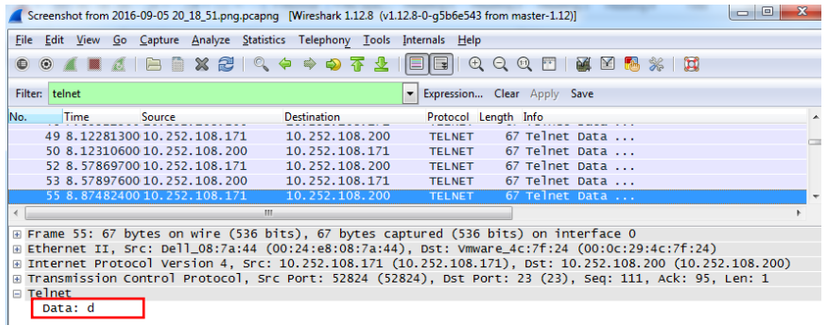

Follow TCP Stream (tcp.stream eq 0)
Stream Content
P..... .38400,38400....#.debian:0....'..DISPLAY.debian:0.....xterm.....Debian GNU/Linux 8
debian login: ssttuuddeenntt
Password: student
Last login: Mon Aug 29 22:11:44 WIB 2016 from 10.252.108.171 on pts/0
Linux debian 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt25-2 (2016-04-08) i686
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
.]0;student@debian: ~.student@debian:~$ eexxiitt
logout
Entire conversation (739 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close


Screenshot from 2016-09-05 20_18_51.png.pcapng [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: telnet
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
38 6.42010700 10.252.108.200 10.252.108.171 TELNET 80 Telnet Data ...
45 7.85886400 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
46 7.85921900 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
49 8.12281300 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
50 8.12310600 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
Frame 38: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
Ethernet II, Src: Vmware_4c:7f:24 (00:0c:29:4c:7f:24), Dst: Dell_08:7a:44 (00:24:e8:08:7a:44)
Internet Protocol Version 4, Src: 10.252.108.200 (10.252.108.200), Dst: 10.252.108.171 (10.252.108.171)
Transmission Control Protocol, Src Port: 23 (23), Dst Port: 52824 (52824), Seq: 78, Ack: 108, Len: 14
Telnet
Data: debian login:
0000 00 24 e8 08 7a 44 00 0c 29 4c 7f 24 08 00 45 10 .$..zD..)L.$..E.
0010 00 42 29 3f 40 00 40 06 21 fc 0a fc 6c c8 0a fc .B)?@.@. !...l...
0020 6c ab 00 17 ce 58 59 95 b4 f9 9c 01 52 6b 80 18 l....XY. ....Rk..
0030 01 c5 d2 5d 00 00 01 01 08 0a 00 33 9d a2 00 38 ...]..... ...3...8
0040 ee 00 64 65 62 69 61 6e 20 6c 6f 67 69 6e 3a 20 ..debian login:
File: "D:\Teesa\PENS\SMT 5\Keamanan Jarin... Packets: 162 · Displayed: 50 (30.9%) · Load time: 0:00.000 Profile: Default


Screenshot from 2016-09-05 20_18_51.png.pcapng [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: telnet
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
38 6.42010700 10.252.108.200 10.252.108.171 TELNET 80 Telnet Data ...
45 7.85886400 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
46 7.85921900 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
49 8.12281300 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
50 8.12310600 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
Frame 45: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: Dell_08:7a:44 (00:24:e8:08:7a:44), Dst: Vmware_4c:7f:24 (00:0c:29:4c:7f:24)
Internet Protocol Version 4, Src: 10.252.108.171 (10.252.108.171), Dst: 10.252.108.200 (10.252.108.200)
Transmission Control Protocol, Src Port: 52824 (52824), Dst Port: 23 (23), Seq: 108, Ack: 92, Len: 1
Telnet
Data: s


Screenshot from 2016-09-05 20_18_51.png.pcapng [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: telnet
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
38 6.42010700 10.252.108.200 10.252.108.171 TELNET 80 Telnet Data ...
45 7.85886400 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
46 7.85921900 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
49 8.12281300 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
50 8.12310600 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
Frame 49: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: Dell_08:7a:44 (00:24:e8:08:7a:44), Dst: Vmware_4c:7f:24 (00:0c:29:4c:7f:24)
Internet Protocol Version 4, Src: 10.252.108.171 (10.252.108.171), Dst: 10.252.108.200 (10.252.108.200)
Transmission Control Protocol, Src Port: 52824 (52824), Dst Port: 23 (23), Seq: 109, Ack: 93, Len: 1
Telnet
Data: t



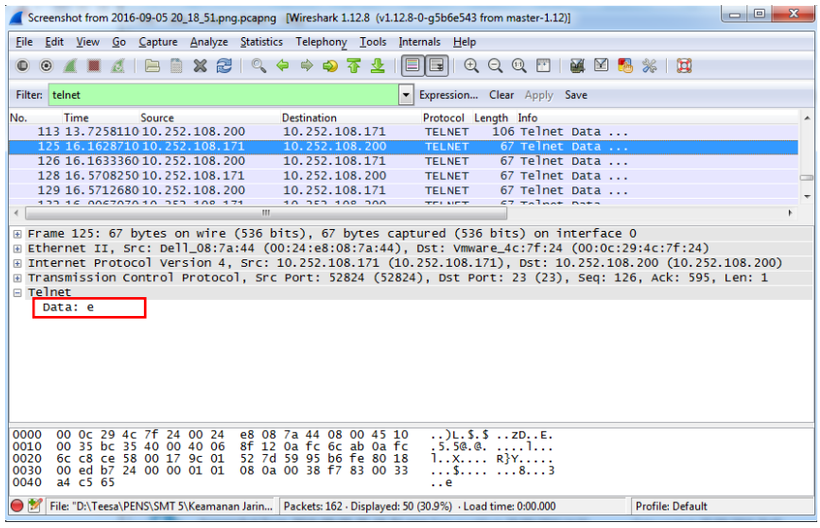


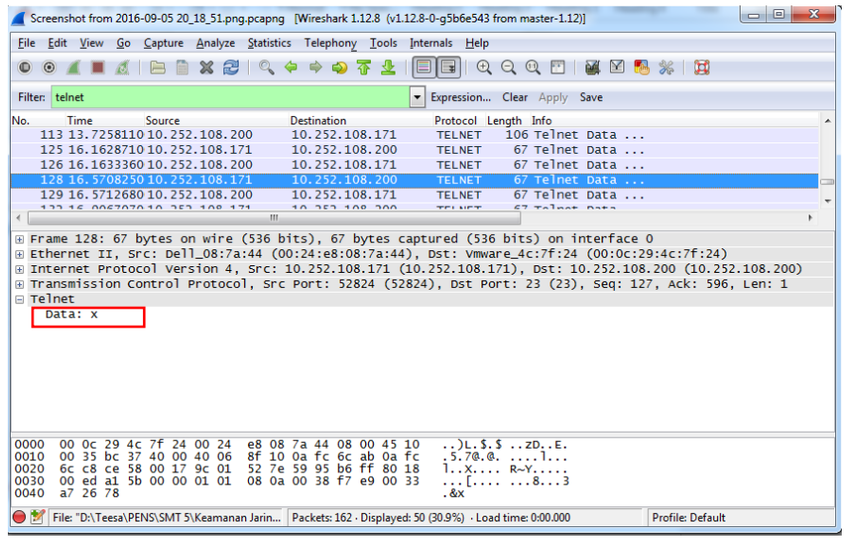
Pada gambar di atas dapat terihat bahwa paket data dikirimkan secara satu per satu, mulai dari s, t kemudian u dan seterusnya hingga membentuk suatu data yang utuh.

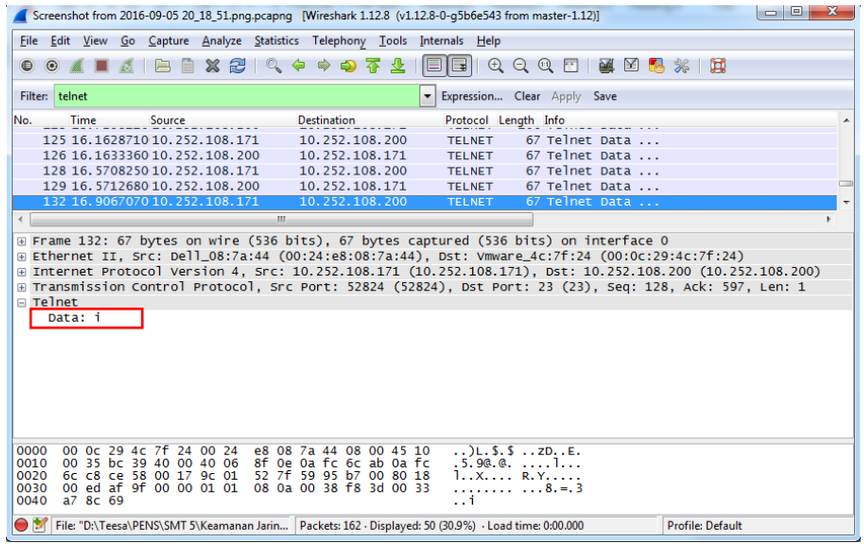
f. Kemudian ketikkan exit untuk keluar dari komputer server

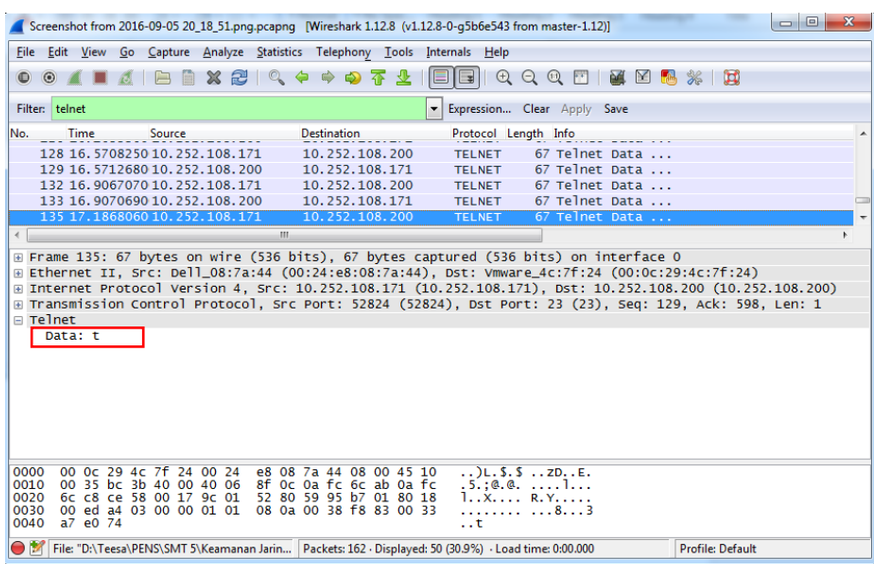
```
student@debian:~$ exit
logout
Connection closed by foreign host.
```

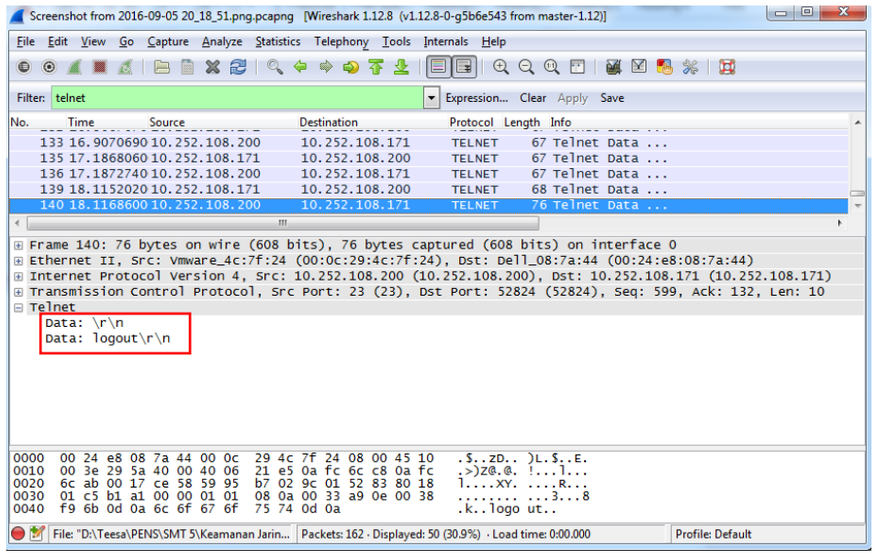
Ketika exit pun juga akan terlihat bahwa paket data dikirimkan secara satu per satu juga, seperti yang terlihat pada gambar di bawah ini :



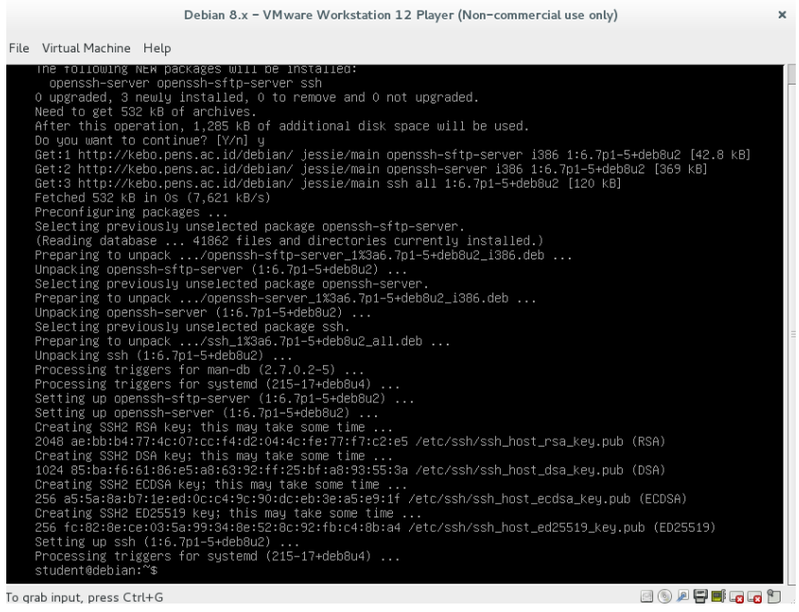

Screenshot from 2016-09-05 20_18_51.png.pcapng [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: telnet
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
113 13.7258110 10.252.108.200 10.252.108.171 TELNET 106 Telnet Data ...
125 16.1628710 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
126 16.1633360 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
128 16.5708250 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
129 16.5712680 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
Frame 128: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: Dell_08:7a:44 (00:24:e8:08:7a:44), Dst: Vmware_4c:7f:24 (00:0c:29:4c:7f:24)
Internet Protocol Version 4, Src: 10.252.108.171 (10.252.108.171), Dst: 10.252.108.200 (10.252.108.200)
Transmission Control Protocol, Src Port: 52824 (52824), Dst Port: 23 (23), Seq: 127, Ack: 596, Len: 1
Telnet
Data: x
0000 00 0c 29 4c 7f 24 00 24 e8 08 7a 44 08 00 45 10 ..)L.$.$ ..zD..E.
0010 00 35 bc 37 40 00 40 06 8f 10 0a fc 6c ab 0a fc .5.7@.@. ....l...
0020 6c c8 ce 58 00 17 9c 01 52 7e 59 95 b6 ff 80 18 l..X.... R~Y.....
0030 00 ed a1 5b 00 00 01 01 08 0a 00 38 f7 e9 00 33 ...[.... ...8...3
0040 a7 26 78 .&x
File: "D:\Teesa\PENS\SMT 5\Keamanan Jarin... Packets: 162 · Displayed: 50 (30.9%) · Load time: 0:00.000 Profile: Default


Screenshot from 2016-09-05 20_18_51.png.pcapng [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: telnet
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
125 16.1628710 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
126 16.1633360 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
128 16.5708250 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
129 16.5712680 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
132 16.9067070 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
Frame 132: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: Dell_08:7a:44 (00:24:e8:08:7a:44), Dst: Vmware_4c:7f:24 (00:0c:29:4c:7f:24)
Internet Protocol Version 4, Src: 10.252.108.171 (10.252.108.171), Dst: 10.252.108.200 (10.252.108.200)
Transmission Control Protocol, Src Port: 52824 (52824), Dst Port: 23 (23), Seq: 128, Ack: 597, Len: 1
Telnet
Data: i
0000 00 0c 29 4c 7f 24 00 24 e8 08 7a 44 08 00 45 10 ..)L.$.$ ..zD..E.
0010 00 35 bc 39 40 00 40 06 8f 0e 0a fc 6c ab 0a fc .5.9@.@. ....l...
0020 6c c8 ce 58 00 17 9c 01 52 7f 59 95 b7 00 80 18 l..X.... R.Y.....
0030 00 ed af 9f 00 00 01 01 08 0a 00 38 f8 3d 00 33 ....8.=.3
0040 a7 8c 69 ..i
File: "D:\Teesa\PENS\SMT 5\Keamanan Jarin... Packets: 162 · Displayed: 50 (30.9%) · Load time: 0:00.000 Profile: Default


Screenshot from 2016-09-05 20_18_51.png.pcapng [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: telnet
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
128 16.5708250 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
129 16.5712680 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
132 16.9067070 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
133 16.9070690 10.252.108.200 10.252.108.171 TELNET 67 Telnet Data ...
135 17.1868060 10.252.108.171 10.252.108.200 TELNET 67 Telnet Data ...
Frame 135: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: Dell_08:7a:44 (00:24:e8:08:7a:44), Dst: Vmware_4c:7f:24 (00:0c:29:4c:7f:24)
Internet Protocol Version 4, Src: 10.252.108.171 (10.252.108.171), Dst: 10.252.108.200 (10.252.108.200)
Transmission Control Protocol, Src Port: 52824 (52824), Dst Port: 23 (23), Seq: 129, Ack: 598, Len: 1
Telnet
Data: t
0000 00 0c 29 4c 7f 24 00 24 e8 08 7a 44 08 00 45 10 ..)L.$.$ ..zD..E.
0010 00 35 bc 3b 40 00 40 06 8f 0c 0a fc 6c ab 0a fc .5.;@.@. ....l...
0020 6c c8 ce 58 00 17 9c 01 52 80 59 95 b7 01 80 18 l..X.... R.Y.....
0030 00 ed a4 03 00 00 01 01 08 0a 00 38 f8 83 00 33 ....8...3
0040 a7 e0 74 ..t
File: "D:\Teesa\PENS\SMT 5\Keamanan Jarin... Packets: 162 · Displayed: 50 (30.9%) · Load time: 0:00.000 Profile: Default



- Langkah-langkah install ssh menggunakan perintah sudo :
  a. Gunakan perintah *sudo apt-get install ssh* untuk menginstall ssh.



  b. Jalankan ssh melalui komputer lain yang terhubung, dengan menggunakan perintah ssh **no ip PC server**, kemudian masukkan password dari komputer yang ingin di akses (PC client).

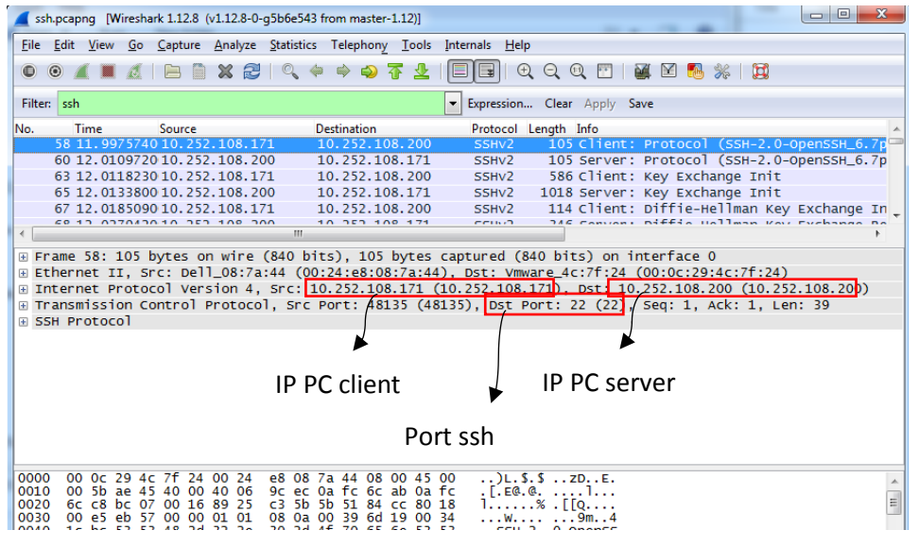
```
student@debian:~$ ssh 10.252.108.200
student@10.252.108.200's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Aug 29 21:55:19 2016 from 10.252.108.171
student@debian:~$
```

IP PC server

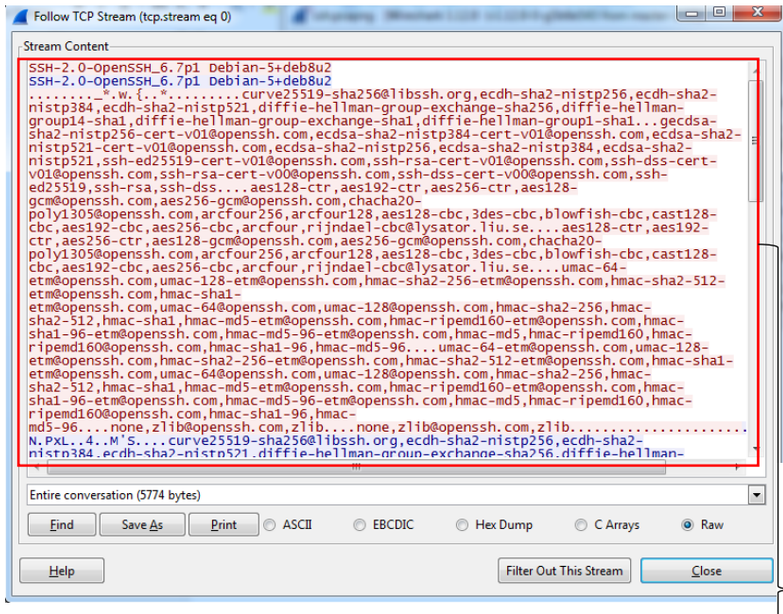
  c. Jalankan wireshark dengan cara buka terminal baru dan ketikkan perintah *sudo wireshark*

```
student@debian:~$ sudo wireshark
```

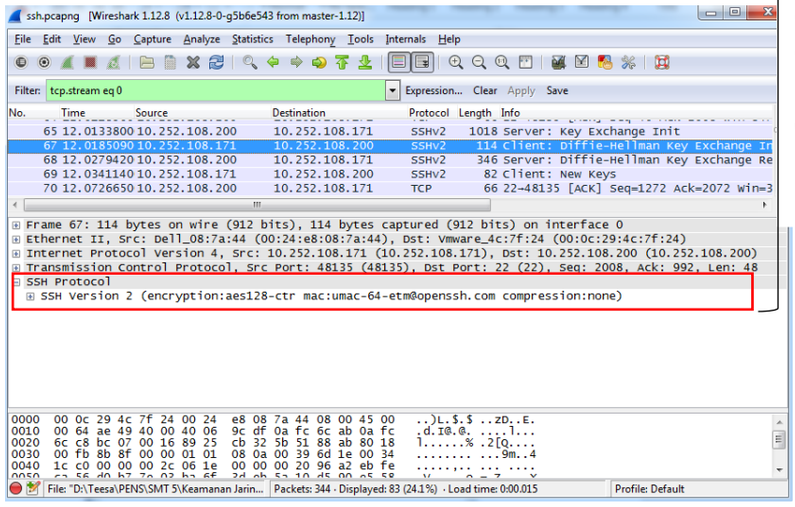
Kemudian wireshark akan terbuka lalu ketikkan **ssh** pada kolom filter, sehingga tampilannya seperti gambar di bawah ini:



klik kanan pada salah satu paket data, lalu pilih **follow tcp stream** untuk dapat melihat berbagaimacam aksi yang dilakukan oleh user lain / PC client ke PC server yang **berhasil ditangkap oleh wireshark secara jelas.** Namun berbeda dengan telnet, ssh mempunyai sifat ssh yang lebih aman dibandingkan telnet, karena ssh **mendukung enkripsi / otentikasi terhadap remote host.** Sehingga, berbagaimacam aksi yang dilakukan oleh client tersebut termasuk password dan username tidak dapat terlihat secara jelas.



User name, password dan berbagaimacam aksi yang dilakukan PC client terhadap PC server **tidak dapat terlihat pada wireshark**



d. Kemudian ketikkan exit untuk keluar dari komputer server

```
student@debian:~$ exit
logout
Connection closed by foreign host.
```

3. Cara lain install server ssh dengan menggunakan perintah *$sudo apt-get install openssh-server*

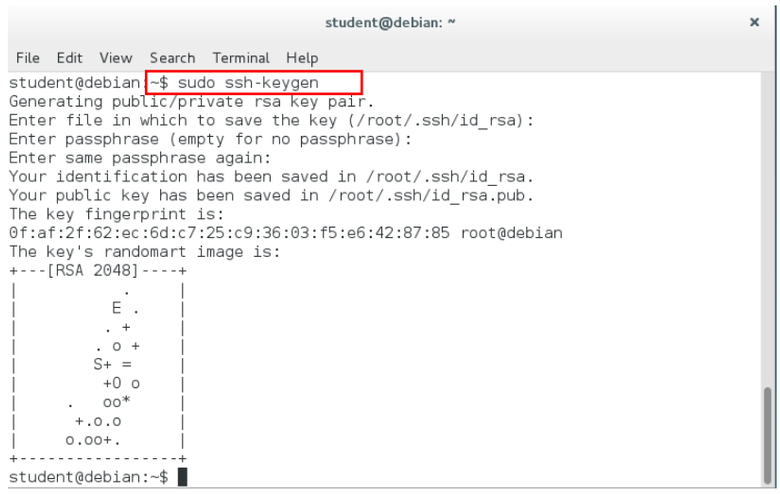
```
student@debian:~$ sudo apt-get install openssh-server
[sudo] password for student:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  openssh-sftp-server
Suggested packages:
  ssh-askpass rssh molly-guard ufw monkeysphere
The following NEW packages will be installed:
  openssh-server openssh-sftp-server
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 369 kB of archives.
After this operation, 952 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kebo.pens.ac.id/debian/ jessie/main openssh-sftp-server amd64 1:6.7p1-5+deb8u2 [37.9 kB]
Get:2 http://kebo.pens.ac.id/debian/ jessie/main openssh-server amd64 1:6.7p1-5+deb8u2 [331 kB]
Fetched 369 kB in 0s (3,690 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openssh-sftp-server.
(Reading database ... 154218 files and directories currently installed.)
Preparing to unpack .../openssh-sftp-server_1%3a6.7p1-5+deb8u2_amd64.deb ...
Unpacking openssh-sftp-server (1:6.7p1-5+deb8u2) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a6.7p1-5+deb8u2_amd64.deb ...
Unpacking openssh-server (1:6.7p1-5+deb8u2) ...
Processing triggers for man-db (2.7.0.2-5) ...
Processing triggers for systemd (215-17+deb8u4) ...
Setting up openssh-sftp-server (1:6.7p1-5+deb8u2) ...
Setting up openssh-server (1:6.7p1-5+deb8u2) ...
Creating SSH2 RSA key; this may take some time ...
2048 fd:63:4a:4d:74:41:5f:22:8e:65:63:76:fc:75:1e:57 /etc/ssh/ssh_host_rsa_key.pub (RSA)
Creating SSH2 DSA key; this may take some time ...
1024 57:b8:3a:68:3d:65:fe:bc:f2:0b:86:53:0f:a2:c1:f6 /etc/ssh/ssh_host_dsa_key.pub (DSA)
Creating SSH2 ECDSA key; this may take some time ...
256 ea:1b:f8:79:0f:86:f0:0b:75:d9:4b:dc:b5:fb:f2:a4 /etc/ssh/ssh_host_ecdsa_key.pub (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 35:70:4b:39:d7:4c:68:19:b0:37:b3:d0:a5:2c:58:9c /etc/ssh/ssh_host_ed25519_key.pub (ED25519)
Processing triggers for systemd (215-17+deb8u4) ...
student@debian:~$
```

OpenSSH adalah versi bebas tersedia dari keluarga (SSH) protokol Secure Shell sebagai alat untuk mengendalikan komputer secara jauh atau mentransfer file antara komputer. OpenSSH **menyediakan daemon server dan alat klien** untuk memfasilitasi secara aman dengan cara remote control dienkripsi dan operasi file transfer.

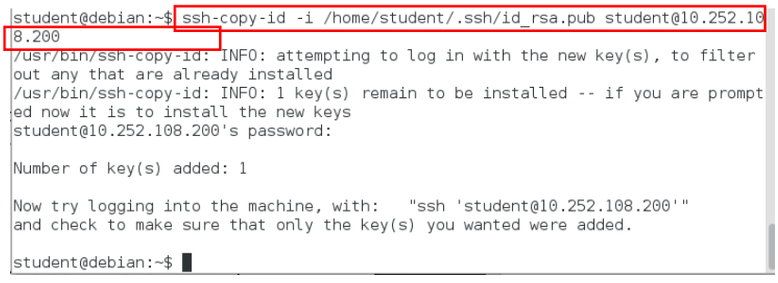
Komponen server OpenSSH, sshd, mendengarkan terus menerus selama koneksi klien dari salah satu alat klien. Ketika permintaan koneksi terjadi, sshd mendirikan sambungan yang benar tergantung pada jenis alat menghubungkan klien. Sebagai contoh, jika komputer remote menghubungkan dengan aplikasi ssh klien, server OpenSSH membuat sebuah sesi remote control setelah otentikasi. Jika remote user terhubung ke server OpenSSH dengan scp, daemon OpenSSH server memulai salinan aman file antara server dan klien setelah otentikasi. OpenSSH dapat menggunakan metode otentikasi, termasuk kata sandi polos, dan kunci publik.

Pengamatan data dengan menggunakan wireshark dapat dilihat pada gambar nomor 2 di atas.

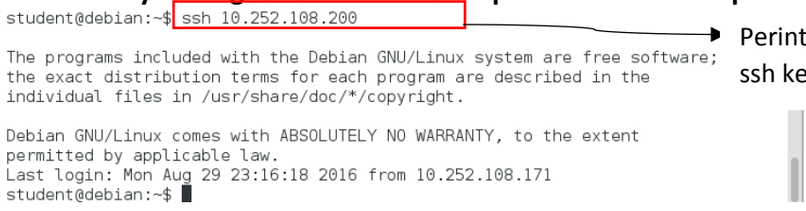
4. Jelaskan langkah-langkah install ssh tanpa password!
   - Langkah-langkah install ssh tanpa password :
     a. Gunakan perintah *sudo ssh-keygen.* Selama installasi akan **diminta memasukkan passharse/key, jika ingin pengaturan default cukup tekan enter saja.**



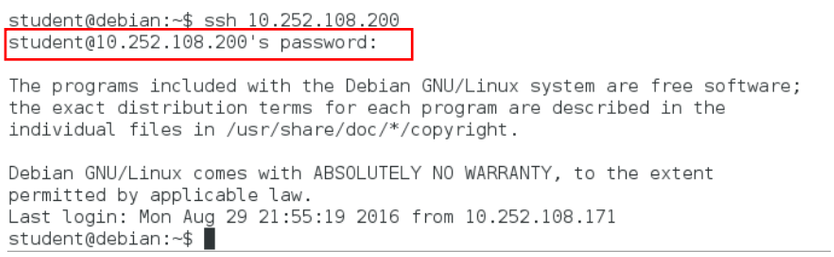
     b. Kopikan public key user ke komputer lain dengan menggunakan perintah *ssh-copy-id –i /home/student/ .ssh/id_rsa.pub username@alamat ip tujuan*. Sebelumnya pastikan terdapat nama user yang sama antar dua komputer yang akan terkoneksi ssh. Jika belum ada user yang sama, maka buat user terlebih dahulu.



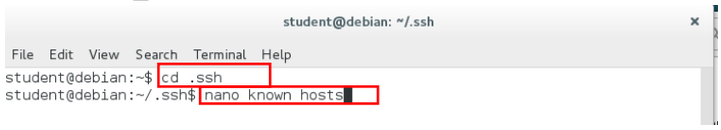
     c. Coba melakukan login ssh ke komputer tujuan. Jika installasi berhasil **maka tidak akan ditanya mengenai username dan password dari komputer tujuan.**

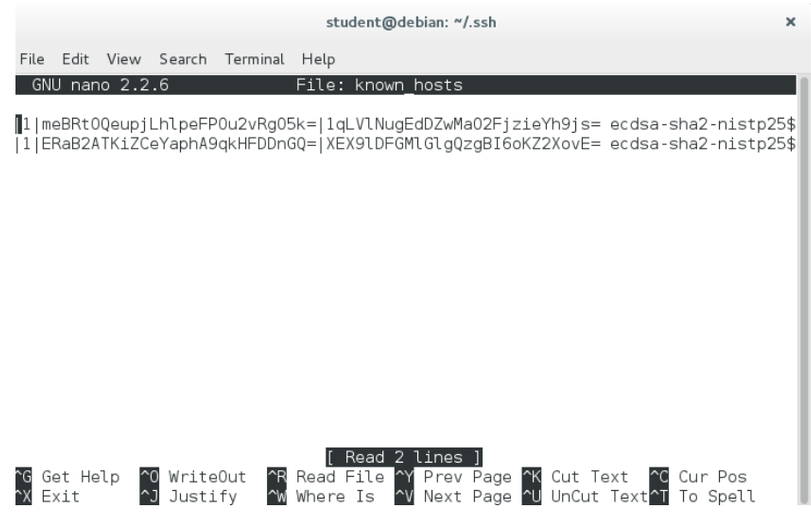


Bandingkan dengan gambar di bawah yang belum dilakukan pengaturan ssh tanpa password, dimana user **masih diminta untuk memasukkan password** dari komputer tujuan.

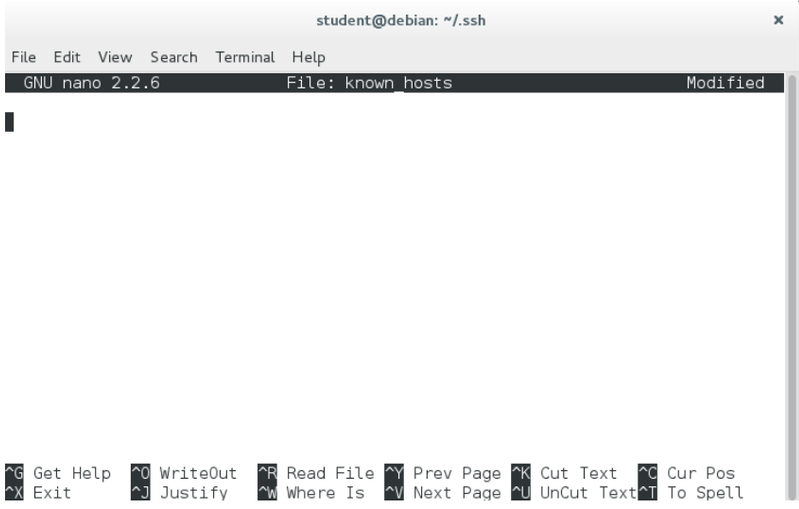


5. Hapus isi file ~/.ssh/known_hosts dan amati perubahannya!
   - Langkah-langkahnya :
     a. Masuk ke direktori .ssh dengan menggunakan parintah *$ cd .ssh* kemudian ketikkan perintah *$ nano known_hosts* untuk dapat menghapus/mengedit isi dari file known_host tersebut.





Tampilan ketika isi file .ssh/known_hosts dihapus



Fungsi dari file .ssh/known_hosts adalah untuk menyimpan key yang mencakup alamat IP server dan password, dimana setiap SSH client yang melakukan koneksi ke server akan diberikan key berupa host ID yang telah digenerate dan dienkripsi oleh server. Oleh client key ini disimpan dalam dalam file .ssh/known_hosts **di dalam folder home milik user.** File ini **tidak hanya** digunakan untuk menyimpan **key dari satu server** ssh tetapi **key dari seluruh server** yang pernah komputer tersebut masuki menggunakan remote login ssh. Jadi, setiap kita akan masuk ke sebuah server, server tujuan akan memberikan kita key, yang kemudian akan dicocokkan dengan key yang telah kita simpan. **Apabila belum pernah masuk ke server tujuan, maka** kita akan diminta untuk menyimpan key yang diberikan. Dan jika kita **sudah pernah masuk ke server tersebut, maka** key yang pernah kita simpan akan dicocokkan dengan key yang diberikan oleh server. Jika key yang

diberikan oleh server tidak cocok dengan key yang disimpan, maka **client akan memutus** proses konektifitas tersebut karena ditakutkan server tujuan yang akan kita masuki **merupakan jebakan** yang dibuat **untuk mencuri username dan password milik client.**

Dan jika kita **ingin meyakinkan** bahwa **server** tersebut benar-benar **yang kita akses maka** kita dapat **menghapus key remote host identification yang telah tersimpan di komputer client,** yang berada pada file .ssh/known_hosts**.**

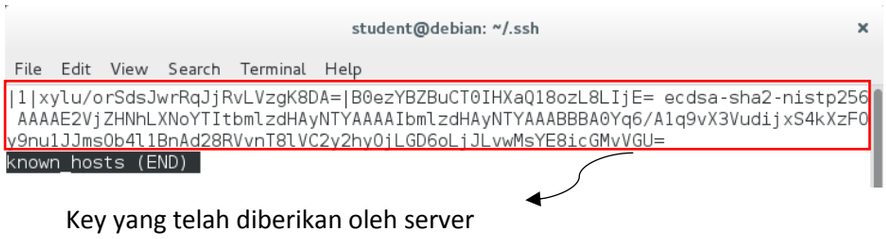
b. Kemudian lakukan ssh ke server

```
student@debian:~$ ssh 10.252.108.131
The authenticity of host '10.252.108.131 (10.252.108.131)' can't be established.
ECDSA key fingerprint is a5:5a:8a:b7:1e:ed:0c:c4:9c:90:dc:eb:3e:a5:e9:1f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.252.108.131' (ECDSA) to the list of known hosts.
student@10.252.108.131's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep  5 15:03:51 2016 from 10.252.108.249
student@debian:~$
```

Dapat dilihat pada gambar diatas bahwa client akan diminta untuk menyimpan key yang diberikan oleh server dan diminta untuk memasukkan password lagi, karena key yang sebelumnya telah dihapus.

c. Kemudian lihat lagi isi file *.ssh/known_hosts* dengan menggunakan perintah *$less known_hosts* maka akan tampil key berupa host ID yang telah digenerate dan dienkripsi oleh server yang telah kita akses.

```
student@debian:~/.ssh$ less known_hosts
```



Key yang telah diberikan oleh server yang kita akses, dan telah digenerate dan dienkripsi yang mencakup alamat IP server dan password

6. Gunakan perintah scp!

```
student@debian:~$ scp file.txt student@10.252.108.131:file.txt
student@10.252.108.131's password:
file.txt                                      100%    5     0.0KB/s   00:00
student@debian:~$ ls
\                   known_hosts
coba.c              mamot.py
febrigendut.txt     Masih gendutan febri daripada mammoth.py
file.txt            motty.py
frindzone mamot.py
student@debian:~$
```

File yang terdapat pada client

SCP (Secure Copy) adalah sebuah program yang merupakan bagian yang terintegrasi pada paket OpenSSH, yang berfungsi untuk menyediakan secure line transmisi antara 2 system dan dapat digunakan untuk transfer file. Keceptan SCP tidak secepat FTP dan penyajian data log server yang tidak bersifat realtime. Selain itu, kelemahan scp ini **kita juga harus mengetahui letak folder yang ingin kita tuju untuk menaruh file/data yang kita kirim.**

Berbagai macam perintah yang dapat dilakukan dengan menggunakan perintah scp :

- Perintah untuk mengcopy file dari komputer client ke komputer remote/server :

  scp namafile.ekstensi username@alamat ip tujuan:/nama/folder/tujuan

  contohnya seperti pada gambar di atas : *scp file.txt student@10.252.108.131:file.txt*

  Artinya, mengcopy file `file.txt` dari komputer lokal/ client ke komputer server dengan ip address 10.252.108.131 dan username student pada file `file.txt`.

- Perintah untuk mengambil File/Folder dari komputer server ke komputer client: ***scp username@alamat ip server:/nama/folder/asal/namafile.ekstensi/folder/tujuan/lokal***
- Selain transfer antar server-klien, dapat juga dilakukan transfer antara server-server. Berikut perintahnya :
  scp username@ip_tempat_file:/folder/tempat/menyimpan/nama/file username@ip_tujuan:/folder/tempat/menyimpan/nama/file

Semua perintah diatas dijalankan pada saat kita sedang me-remote komputer server. Jadi kita menggunakan port 22 sebagai port SSH. Namun, **jika ternyata bukan port 22 yang digunakan**, perintah SCP nya seperti dibawah ini :

scp -P port_ssh username@ip_tujuan:/folder/tempat/menyimpan

7. Gunakan perintah SFTP !

```
student@debian:~$ sftp 10.252.108.171
student@ 10.252.108.171's password:
Connected to 10.252.108.171
sftp> mget /home/student/.ssn/known_hosts
Fetching /home/student/.ssh/known_hosts to known_hosts
/home/student/.ssh/known_hosts                100%  222     0.2KB/s   00:00
sftp> quit
```

Secure FTP (SFTP) adalah program transfer file, sama seperti program FTP. SFTP lebih banyak digunakan karena data yang ditransfer dienkrip menggunakan enkripsi SSH sehingga lebih aman ketika dikirim melalui jaringan. Format perintah SFTP lebih sederhana dari pada SCP yaitu:

sftp namahost atau ***sftp namauser@hostname***

Dengan SFTP, kita harus login terlebih dahulu ke PC yang kita inginkan/ komputer server, selanjutnya kita dapat melakukan perintah-perintah SFTP. Tidak seperti pada FTP yang memungkinkan penggunaan anonymous user, pada SFTP username harus memiliki password.

Berbagai macam perintah yang dapat dilakukan dengan menggunakan perintah sftp :

- Perintah untuk mendownload file :
  get namafile.ekstensi atau ***mget namafile.ekstensi***

  Contohnya seperti yang terlihat pada gambar di atas menggunakan perintah *$sftp 10.252.108.171* dimana *10.252.108.171* merupakan alamat ip client, dan *mget /home/student/.ssh/known_hosts* artinya adalah, komputer server mendownload file dari direktori */home/student/.ssh/* dengan nama file *known_hosts* yang berada pada komputer client.
- Perintah untuk mengupload file :
  put namafile.ekstensi atau ***mput namafile.ekstensi***

Dan setelah server mendownload file `known_host` dari komputer client dapat dilihat dengan menggunakan perintah **ls** untuk membuktikan bahwa file `known_host` tersebut telah berhasil di download, seperti pada gambar dibawah ini :