Wireshark Installation and Use.

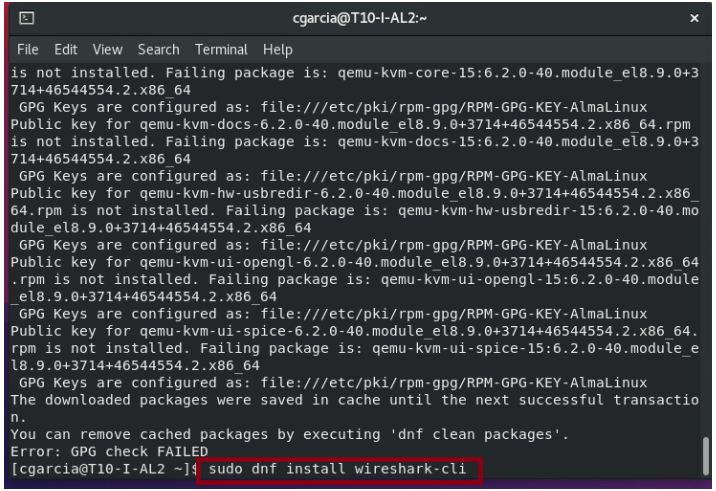
Carlos Gerez
January 2024

Wireshark installation from command line in Linux Alma:

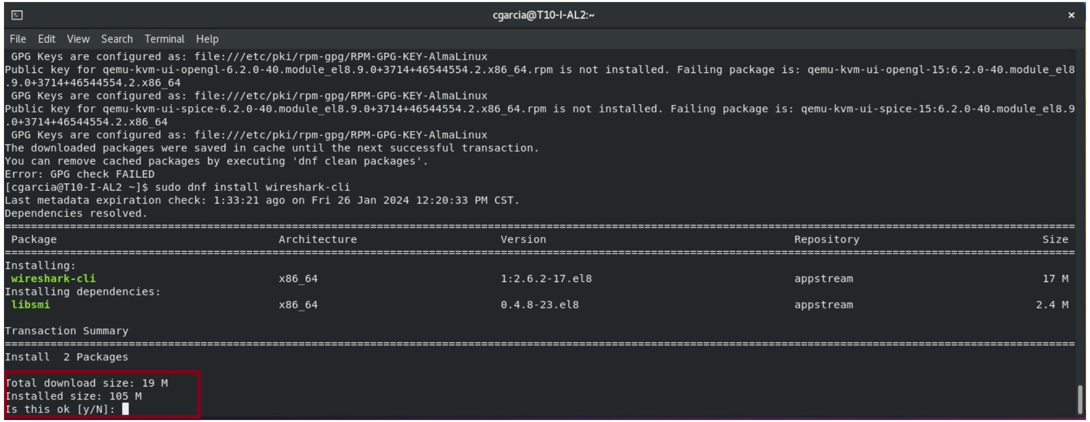
```
sudo dnf install wireshark
```

```
sudo dnf install wireshark-cli
```

```
sudo wireshark &
```

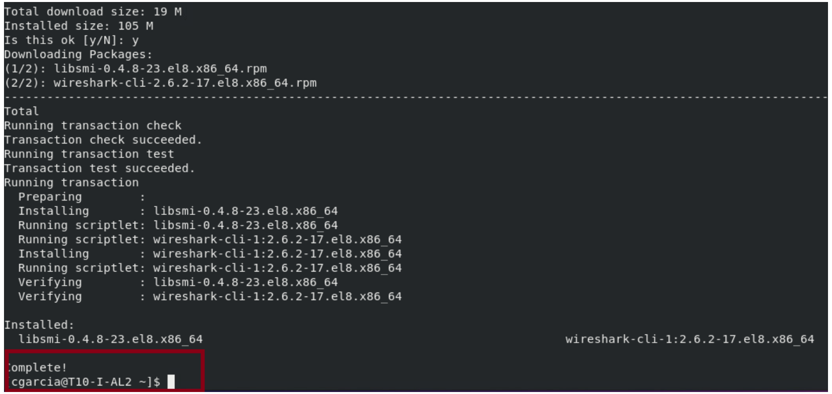


```
is not installed. Failing package is: qemu-kvm-core-15:6.2.0-40.module_el8.9.0+3
714+46544554.2.x86_64
 GPG Keys are configured as: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-AlmaLinux
Public key for qemu-kvm-docs-6.2.0-40.module_el8.9.0+3714+46544554.2.x86_64.rpm
is not installed. Failing package is: qemu-kvm-docs-15:6.2.0-40.module_el8.9.0+3
714+46544554.2.x86_64
 GPG Keys are configured as: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-AlmaLinux
Public key for qemu-kvm-hw-usbredir-6.2.0-40.module_el8.9.0+3714+46544554.2.x86_
64.rpm is not installed. Failing package is: qemu-kvm-hw-usbredir-15:6.2.0-40.mo
dule_el8.9.0+3714+46544554.2.x86_64
 GPG Keys are configured as: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-AlmaLinux
Public key for qemu-kvm-ui-opengl-6.2.0-40.module_el8.9.0+3714+46544554.2.x86_64
.rpm is not installed. Failing package is: qemu-kvm-ui-opengl-15:6.2.0-40.module
_el8.9.0+3714+46544554.2.x86_64
 GPG Keys are configured as: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-AlmaLinux
Public key for qemu-kvm-ui-spice-6.2.0-40.module_el8.9.0+3714+46544554.2.x86_64.
rpm is not installed. Failing package is: qemu-kvm-ui-spice-15:6.2.0-40.module_e
l8.9.0+3714+46544554.2.x86_64
 GPG Keys are configured as: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-AlmaLinux
The downloaded packages were saved in cache until the next successful transactio
n.
You can remove cached packages by executing 'dnf clean packages'.
Error: GPG check FAILED
[cgarcia@T10-I-AL2 ~]$ sudo dnf install wireshark-cli
```

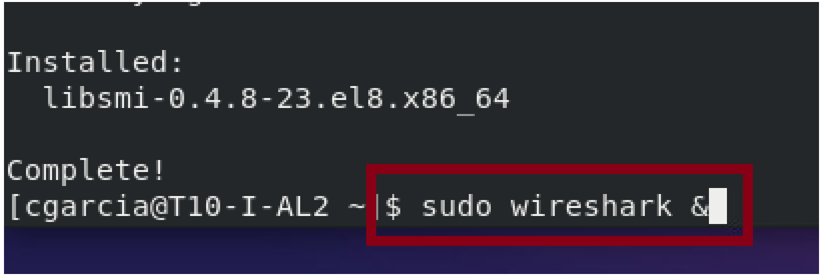


```
 GPG Keys are configured as: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-AlmaLinux
Public key for qemu-kvm-ui-opengl-6.2.0-40.module_el8.9.0+3714+46544554.2.x86_64.rpm is not installed. Failing package is: qemu-kvm-ui-opengl-15:6.2.0-40.module_el8
.9.0+3714+46544554.2.x86_64
 GPG Keys are configured as: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-AlmaLinux
Public key for qemu-kvm-ui-spice-6.2.0-40.module_el8.9.0+3714+46544554.2.x86_64.rpm is not installed. Failing package is: qemu-kvm-ui-spice-15:6.2.0-40.module_el8.9
.0+3714+46544554.2.x86_64
 GPG Keys are configured as: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-AlmaLinux
The downloaded packages were saved in cache until the next successful transaction.
You can remove cached packages by executing 'dnf clean packages'.
Error: GPG check FAILED
[cgarcia@T10-I-AL2 ~]$ sudo dnf install wireshark-cli
Last metadata expiration check: 1:33:21 ago on Fri 26 Jan 2024 12:20:33 PM CST.
Dependencies resolved.
=========================================================================================================================================================================
 Package                              Architecture                   Version                                         Repository                                     Size
=========================================================================================================================================================================
Installing:
 wireshark-cli                        x86_64                         1:2.6.2-17.el8                                  appstream                                      17 M
Installing dependencies:
 libsmi                               x86_64                         0.4.8-23.el8                                    appstream                                     2.4 M

Transaction Summary
=========================================================================================================================================================================
Install  2 Packages

Total download size: 19 M
Installed size: 105 M
Is this ok [y/N]: 
```

Wireshark installation from command line in Linux Alma:

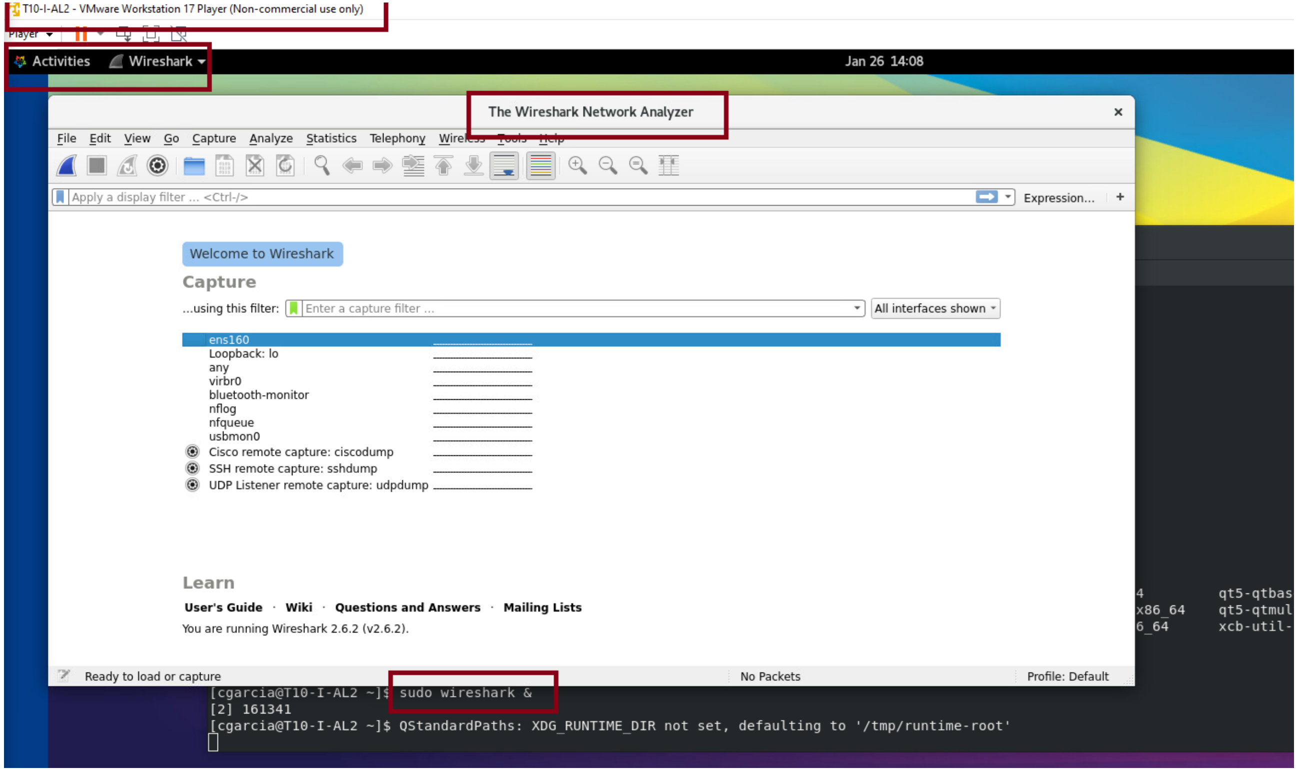


```
Total download size: 19 M
Installed size: 105 M
Is this ok [y/N]: y
Downloading Packages:
(1/2): libsmi-0.4.8-23.el8.x86_64.rpm
(2/2): wireshark-cli-2.6.2-17.el8.x86_64.rpm
------------------------------------------------------------------------------------------------------------------------
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
  Installing       : libsmi-0.4.8-23.el8.x86_64
  Running scriptlet: libsmi-0.4.8-23.el8.x86_64
  Running scriptlet: wireshark-cli-1:2.6.2-17.el8.x86_64
  Installing       : wireshark-cli-1:2.6.2-17.el8.x86_64
  Running scriptlet: wireshark-cli-1:2.6.2-17.el8.x86_64
  Verifying        : libsmi-0.4.8-23.el8.x86_64
  Verifying        : wireshark-cli-1:2.6.2-17.el8.x86_64

Installed:
  libsmi-0.4.8-23.el8.x86_64                                                     wireshark-cli-1:2.6.2-17.el8.x86_64

:omplete!
 cgarcia@T10-I-AL2 ~]$
```



```
Installed:
  libsmi-0.4.8-23.el8.x86_64

Complete!
[cgarcia@T10-I-AL2 ~]$ sudo wireshark &
```

Wireshark can be open from the command line or from the gui

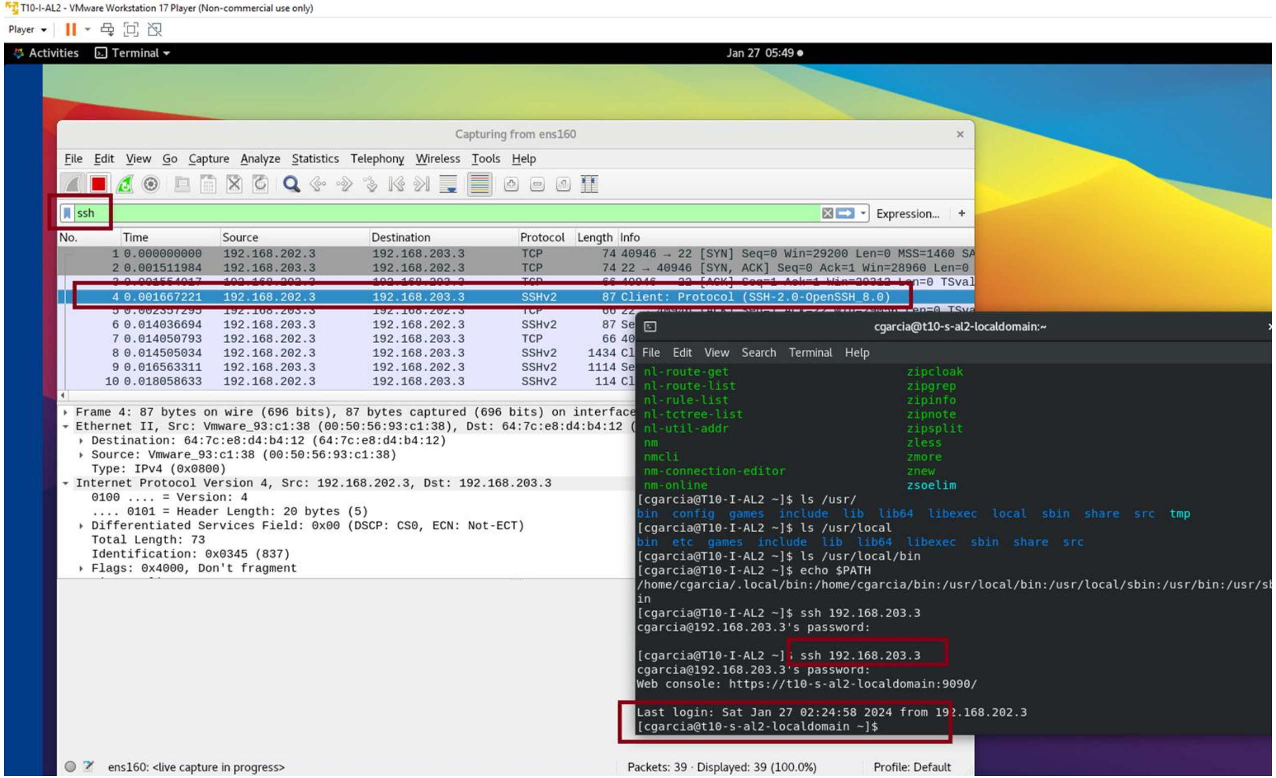

T10-I-AL2 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Wireshark
Jan 26 14:08
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
ens160
Loopback: lo
any
virbr0
bluetooth-monitor
nflog
nfqueue
usbmon0
Cisco remote capture: ciscodump
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Ready to load or capture
No Packets
Profile: Default

You are running Wireshark 2.6.2 (v2.6.2).

```
4        qt5-qtbas
x86_64   qt5-qtmul
6_64     xcb-util-
```

```
[cgarcia@T10-I-AL2 ~]$ sudo wireshark &
[2] 161341
[cgarcia@T10-I-AL2 ~]$ QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

We had connectivities problems in our network and want to know if we lack connectivity to another computer while connecting with ssh or it was a problem in the settings of the machine. We can capture traffic filtering what is of interest to isolate problems in this case.
We tried ssh from 192.168.203.3 towards our machine 192.168.202.3


T10-I-AL2 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Jan 27 05:49
Capturing from ens160
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
cgarcia@t10-s-al2-localdomain:~
File Edit View Search Terminal Help

ssh

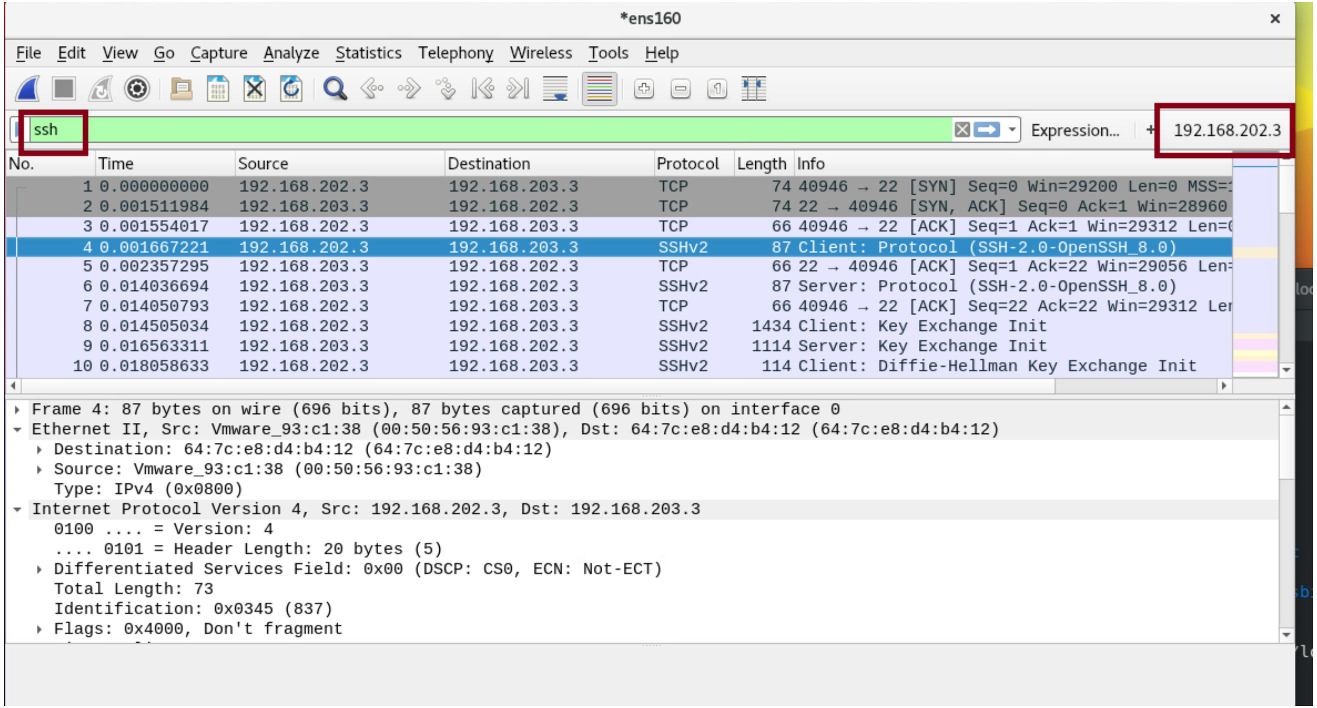
```
No.  Time          Source          Destination     Protocol  Length Info
   1 0.000000000   192.168.202.3   192.168.203.3   TCP         74 40946 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SA
   2 0.001511984   192.168.203.3   192.168.202.3   TCP         74 22 → 40946 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
   3 0.001554017   192.168.202.3   192.168.203.3   TCP         66 40946 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval
   4 0.001667221   192.168.202.3   192.168.203.3   SSHv2       87 Client: Protocol (SSH-2.0-OpenSSH_8.0)
   5 0.002357295   192.168.203.3   192.168.202.3   TCP         66 22 → 40946 [ACK] Seq=1 Ack=22 Win=29056 Len=0 TSva
   6 0.014036694   192.168.203.3   192.168.202.3   SSHv2       87 Se
   7 0.014050793   192.168.202.3   192.168.203.3   TCP         66 40
   8 0.014505034   192.168.202.3   192.168.203.3   SSHv2     1434 Cl
   9 0.016563311   192.168.203.3   192.168.202.3   SSHv2     1114 Se
  10 0.018058633   192.168.202.3   192.168.203.3   SSHv2      114 Cl
```

```
› Frame 4: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface
⌄ Ethernet II, Src: Vmware_93:c1:38 (00:50:56:93:c1:38), Dst: 64:7c:e8:d4:b4:12 (
  › Destination: 64:7c:e8:d4:b4:12 (64:7c:e8:d4:b4:12)
  › Source: Vmware_93:c1:38 (00:50:56:93:c1:38)
    Type: IPv4 (0x0800)
⌄ Internet Protocol Version 4, Src: 192.168.202.3, Dst: 192.168.203.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 73
    Identification: 0x0345 (837)
  › Flags: 0x4000, Don't fragment
```

```
nl-route-get                             zipcloak
nl-route-list                            zipgrep
nl-rule-list                             zipinfo
nl-tctree-list                           zipnote
nl-util-addr                             zipsplit
nm                                       zless
nmcli                                    zmore
nm-connection-editor                     znew
nm-online                                zsoelim
[cgarcia@T10-I-AL2 ~]$ ls /usr/
bin  config  games  include  lib  lib64  libexec  local  sbin  share  src  tmp
[cgarcia@T10-I-AL2 ~]$ ls /usr/local
bin  etc  games  include  lib  lib64  libexec  sbin  share  src
[cgarcia@T10-I-AL2 ~]$ ls /usr/local/bin
[cgarcia@T10-I-AL2 ~]$ echo $PATH
/home/cgarcia/.local/bin:/home/cgarcia/bin:/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sb
in
[cgarcia@T10-I-AL2 ~]$ ssh 192.168.203.3
cgarcia@192.168.203.3's password:

[cgarcia@T10-I-AL2 ~]$ ssh 192.168.203.3
cgarcia@192.168.203.3's password:
Web console: https://t10-s-al2-localdomain:9090/

Last login: Sat Jan 27 02:24:58 2024 from 192.168.202.3
[cgarcia@t10-s-al2-localdomain ~]$
```

ens160: <live capture in progress>   Packets: 39 · Displayed: 39 (100.0%)   Profile: Default

To isolate the problem we used Wireshark filtering the ssh connections from and to our machine to see if firewalls allow connections. Here we apply 2 filters, one to ssh connections and the other to the address 192.168.202.3 of our machine. We see that connections are working well, then the problem was located later in the $PATH variable of our Linux.



ssh

192.168.202.3

```
No.  Time          Source          Destination     Protocol  Length Info
   1 0.000000000   192.168.202.3   192.168.203.3   TCP         74 40946 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=
   2 0.001511984   192.168.203.3   192.168.202.3   TCP         74 22 → 40946 [SYN, ACK] Seq=0 Ack=1 Win=28960
   3 0.001554017   192.168.202.3   192.168.203.3   TCP         66 40946 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=
   4 0.001667221   192.168.202.3   192.168.203.3   SSHv2       87 Client: Protocol (SSH-2.0-OpenSSH_8.0)
   5 0.002357295   192.168.203.3   192.168.202.3   TCP         66 22 → 40946 [ACK] Seq=1 Ack=22 Win=29056 Len=
   6 0.014036694   192.168.203.3   192.168.202.3   SSHv2       87 Server: Protocol (SSH-2.0-OpenSSH_8.0)
   7 0.014050793   192.168.202.3   192.168.203.3   TCP         66 40946 → 22 [ACK] Seq=22 Ack=22 Win=29312 Le
   8 0.014505034   192.168.202.3   192.168.203.3   SSHv2     1434 Client: Key Exchange Init
   9 0.016563311   192.168.203.3   192.168.202.3   SSHv2     1114 Server: Key Exchange Init
  10 0.018058633   192.168.202.3   192.168.203.3   SSHv2      114 Client: Diffie-Hellman Key Exchange Init
```

```
› Frame 4: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0
˅ Ethernet II, Src: Vmware_93:c1:38 (00:50:56:93:c1:38), Dst: 64:7c:e8:d4:b4:12 (64:7c:e8:d4:b4:12)
  › Destination: 64:7c:e8:d4:b4:12 (64:7c:e8:d4:b4:12)
  › Source: Vmware_93:c1:38 (00:50:56:93:c1:38)
    Type: IPv4 (0x0800)
˅ Internet Protocol Version 4, Src: 192.168.202.3, Dst: 192.168.203.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 73
    Identification: 0x0345 (837)
  › Flags: 0x4000, Don't fragment
```