System Programming & OS 실습

Network Protocol Practice

정지헌, 안석현, 김선재

Dankook University

{wlgjsjames7224, seokhyun, rlatjswo0824}@dankook.ac.kr

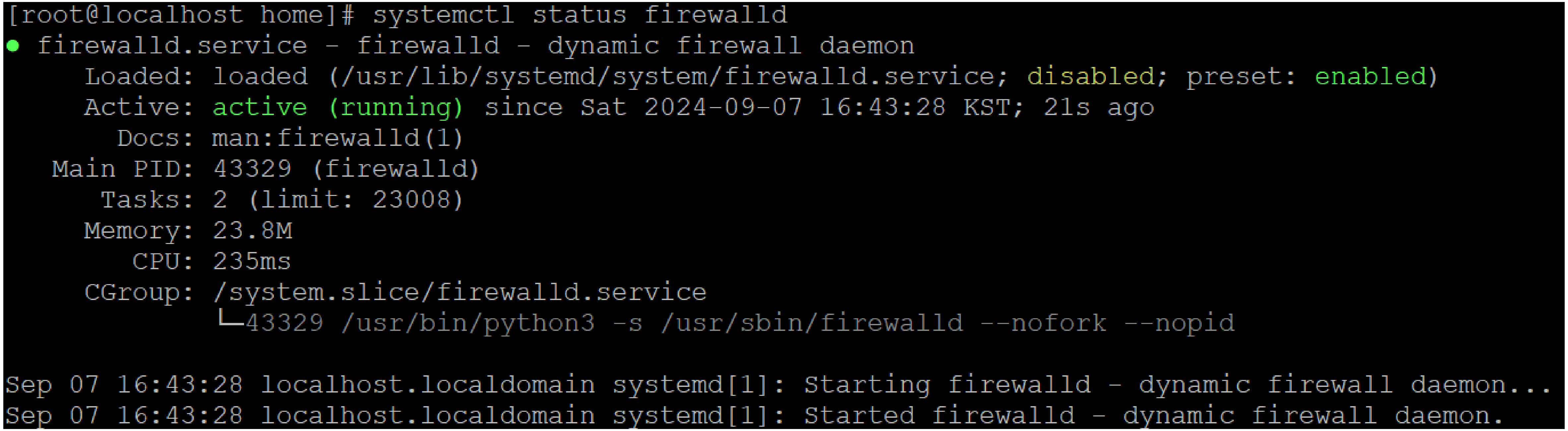
Index

- Telnet
- WireShark
- Network Packet Analysis

Telnet

❖ Telnet

- 방화벽 설정 확인
- systemctl status firewalld



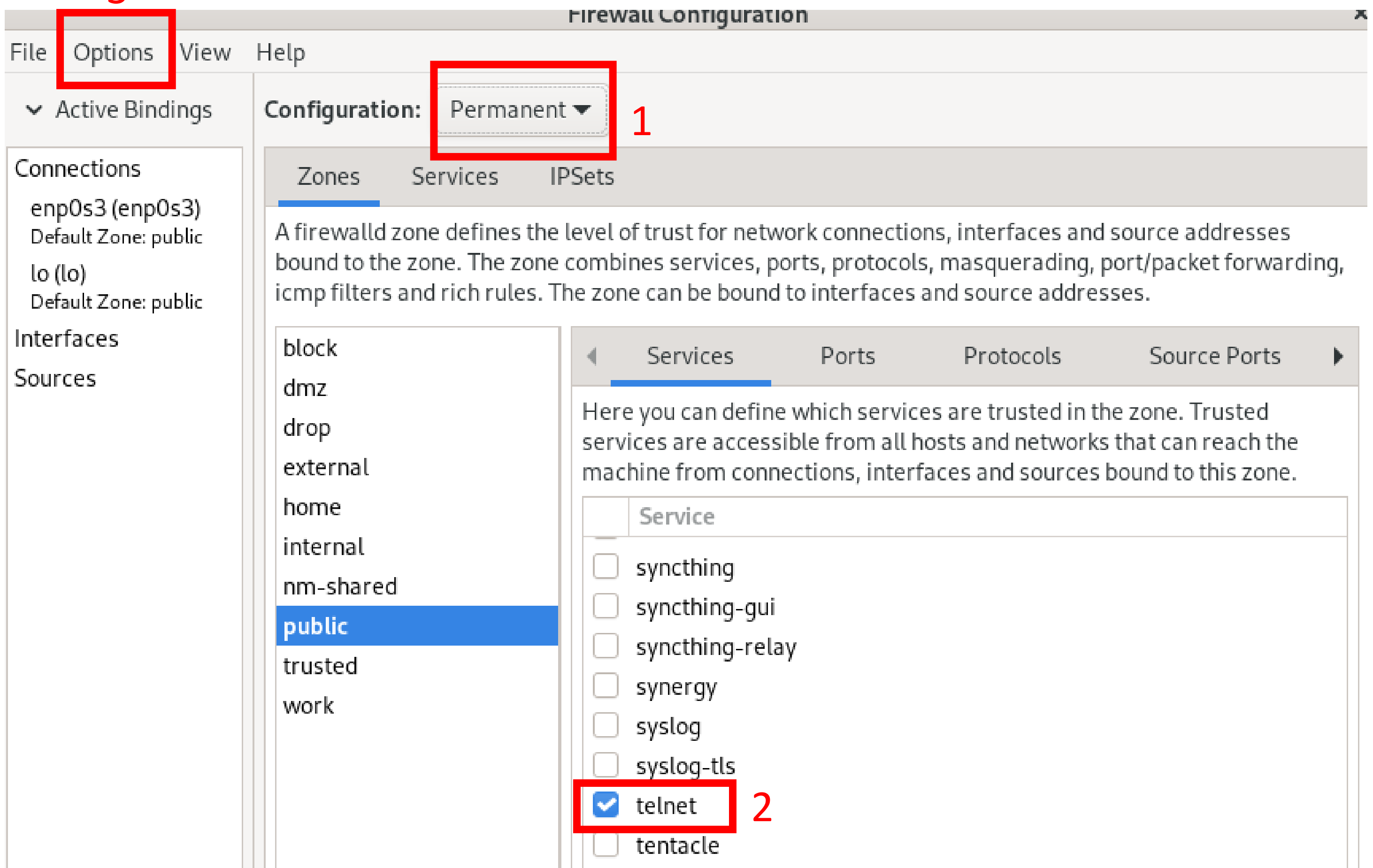
```
[root@localhost home]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; preset: enabled)
     Active: active (running) since Sat 2024-09-07 16:43:28 KST; 21s ago
       Docs: man:firewalld(1)
   Main PID: 43329 (firewalld)
      Tasks: 2 (limit: 23008)
     Memory: 23.8M
        CPU: 235ms
     CGroup: /system.slice/firewalld.service
             └─43329 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

Sep 07 16:43:28 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
Sep 07 16:43:28 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
```

Telnet

❖ Telnet

- 방화벽 설정을 위해 방화벽 GUI 불러오기

  firewall-config

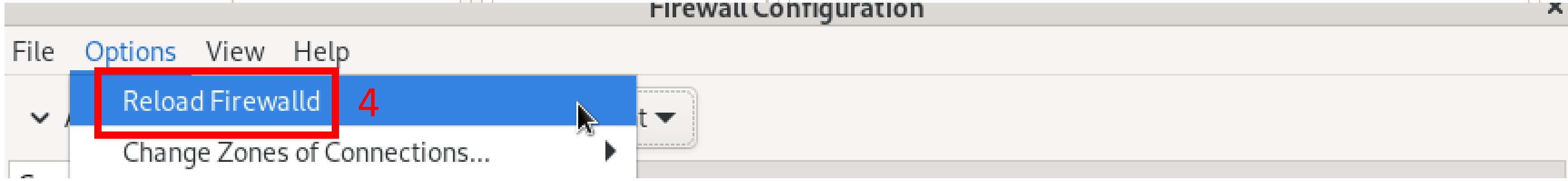


Configuration: Permanent

A firewalld zone defines the level of trust for network connections, interfaces and source addresses bound to the zone. The zone combines services, ports, protocols, masquerading, port/packet forwarding, icmp filters and rich rules. The zone can be bound to interfaces and source addresses.

Here you can define which services are trusted in the zone. Trusted services are accessible from all hosts and networks that can reach the machine from connections, interfaces and sources bound to this zone.

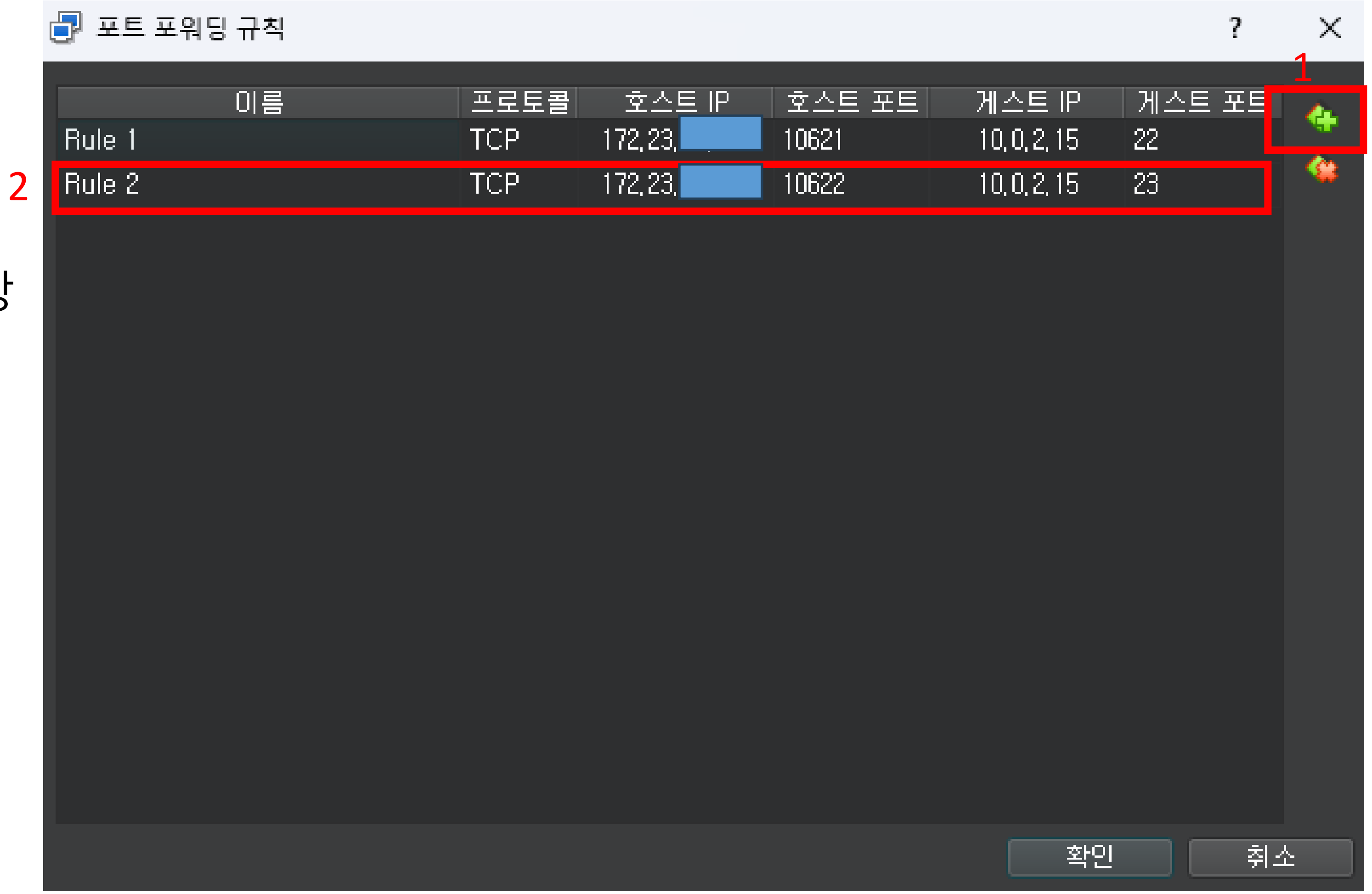
	Service
□	syncthing
□	syncthing-gui
□	syncthing-relay
□	synergy
□	syslog
□	syslog-tls
☑	telnet
□	tentacle



Telnet

❖ Telnet

- 포트포워딩 규칙 추가
- 텔넷은 기본적으로 23번 포트를 사용
- SSH 포트포워딩 규칙 추가하는 방법이랑 동일

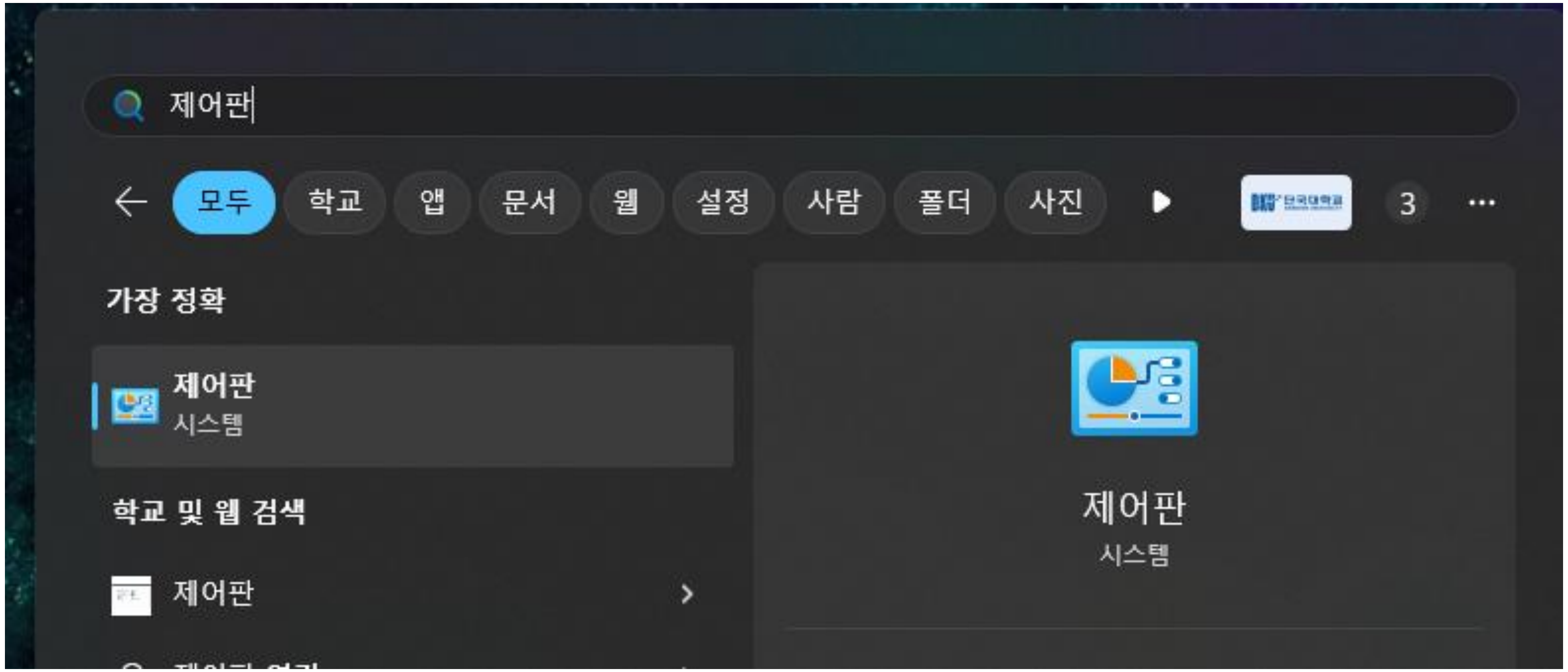


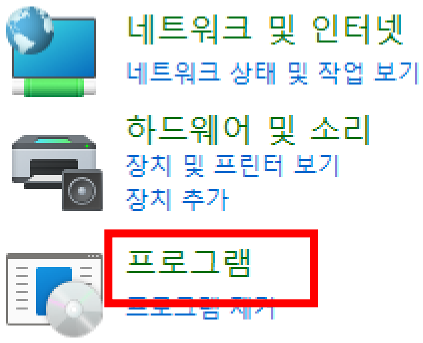
이름	프로토콜	호스트 IP	호스트 포트	게스트 IP	게스트 포트
Rule 1	TCP	172,23,[redacted]	10621	10,0,2,15	22
Rule 2	TCP	172,23,[redacted]	10622	10,0,2,15	23

Telnet

❖ 윈도우 설정

- 윈도우(노트북, 데스크탑) 설정
- 제어판 검색 후 프로그램 선택

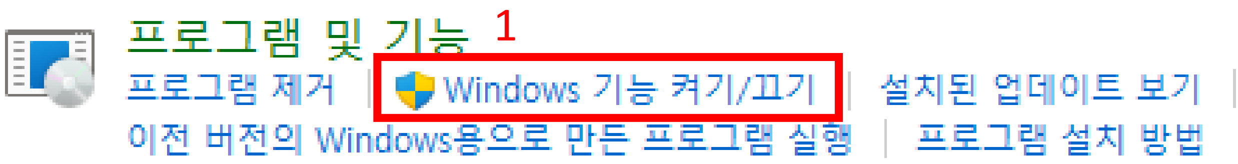




Telnet

❖ 윈도우 설정

- Window 기능 켜기/끄기 접속



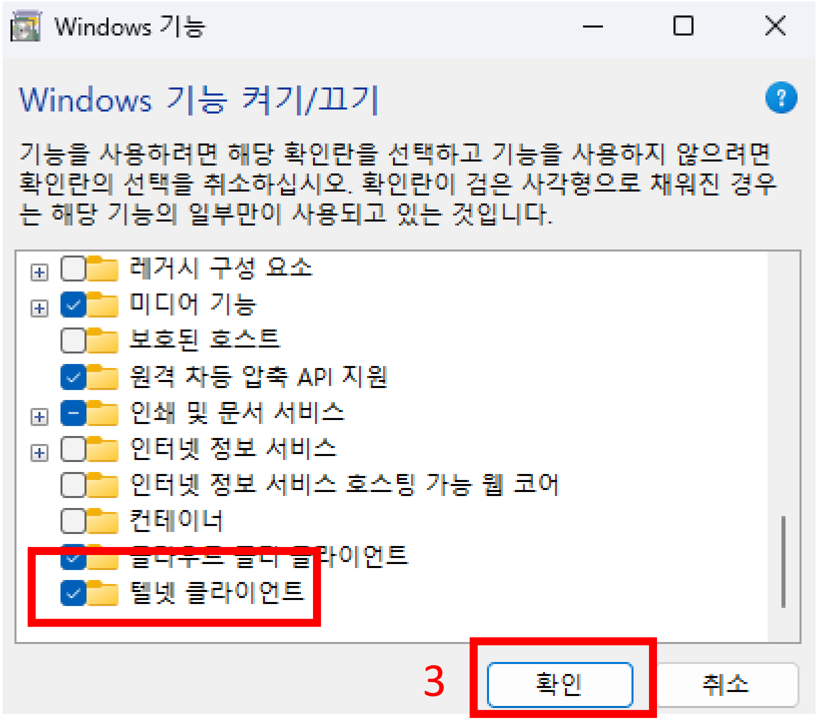
프로그램 및 기능

프로그램 제거 | Windows 기능 켜기/끄기 | 설치된 업데이트 보기 |
이전 버전의 Windows용으로 만든 프로그램 실행 | 프로그램 설치 방법

- 기본적으로 윈도우에서는 telnet 접속

프로그램 기능이 꺼져있음

- 텔넷 클라이언트 활성화



Windows 기능

Windows 기능 켜기/끄기

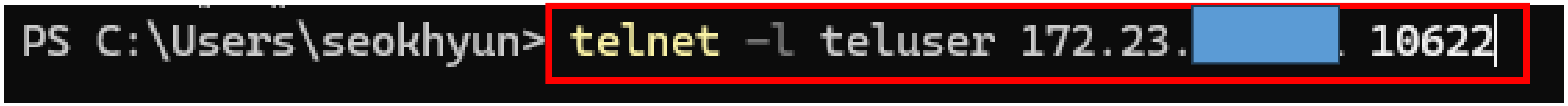
기능을 사용하려면 해당 확인란을 선택하고 기능을 사용하지 않으려면 확인란의 선택을 취소하십시오. 확인란이 검은 사각형으로 채워진 경우는 해당 기능의 일부만이 사용되고 있는 것입니다.

- ⊞ □ 레거시 구성 요소
- ⊞ ☑ 미디어 기능
- □ 보호된 호스트
- ☑ 원격 차등 압축 API 지원
- ⊞ ■ 인쇄 및 문서 서비스
- ⊞ □ 인터넷 정보 서비스
- □ 인터넷 정보 서비스 호스팅 가능 웹 코어
- □ 컨테이너
- ☑ 클라우드 폴더 클라이언트
- ☑ 텔넷 클라이언트

확인 취소

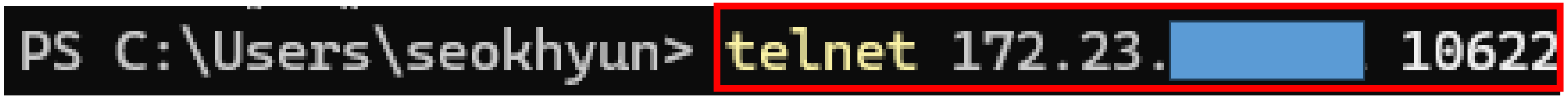
Telnet

❖ Window에서 접속 확인



```
PS C:\Users\seokhyun> telnet -l teluser 172.23.[redacted]. 10622
```

-> telnet –l [사용자이름] [HOST IP] [Port number]



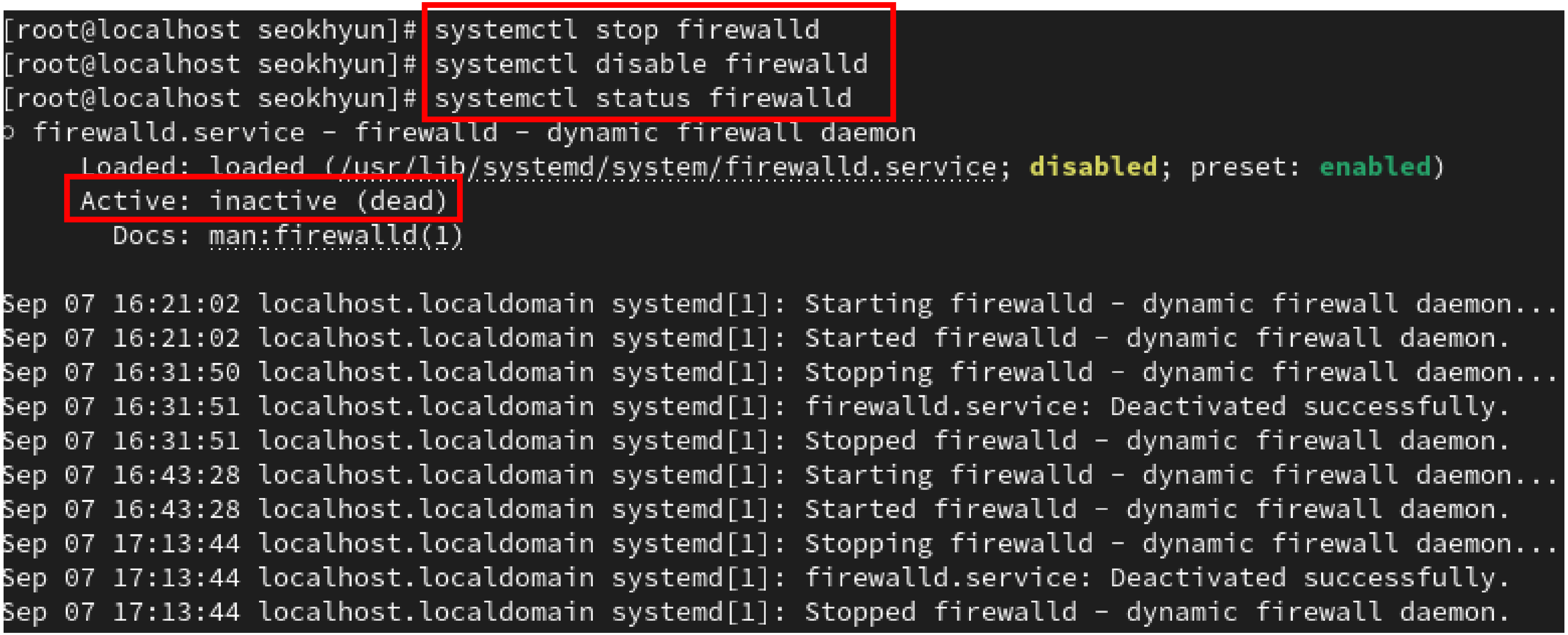
```
PS C:\Users\seokhyun> telnet 172.23.[redacted] 10622
```

-> telnet [HOST IP] [Port number]

Telnet

❖ Window에서 접속 불가 시

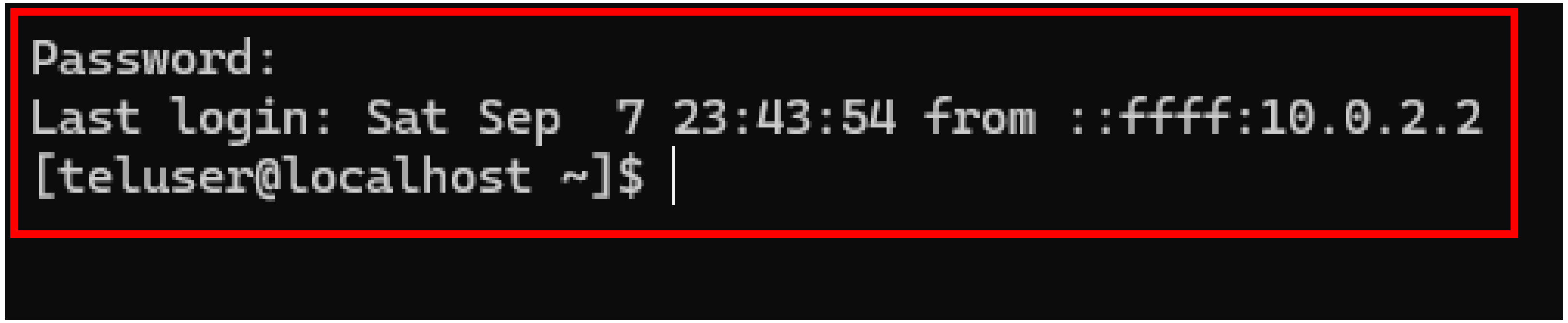
- 실습 진행을 위해 방화벽 기능 off



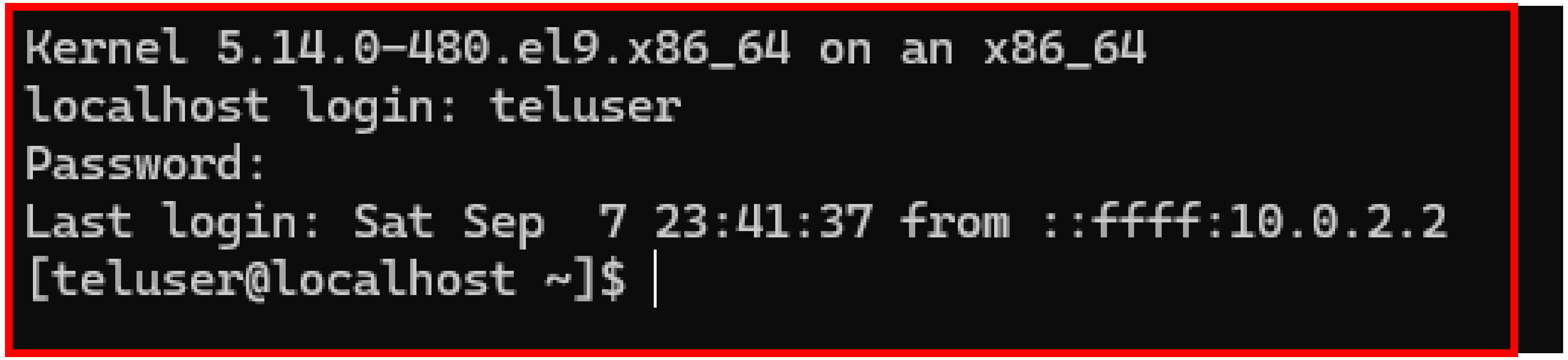
```
[root@localhost seokhyun]# systemctl stop firewalld
[root@localhost seokhyun]# systemctl disable firewalld
[root@localhost seokhyun]# systemctl status firewalld
○ firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; preset: enabled)
     Active: inactive (dead)
       Docs: man:firewalld(1)

Sep 07 16:21:02 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
Sep 07 16:21:02 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
Sep 07 16:31:50 localhost.localdomain systemd[1]: Stopping firewalld - dynamic firewall daemon...
Sep 07 16:31:51 localhost.localdomain systemd[1]: firewalld.service: Deactivated successfully.
Sep 07 16:31:51 localhost.localdomain systemd[1]: Stopped firewalld - dynamic firewall daemon.
Sep 07 16:43:28 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
Sep 07 16:43:28 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
Sep 07 17:13:44 localhost.localdomain systemd[1]: Stopping firewalld - dynamic firewall daemon...
Sep 07 17:13:44 localhost.localdomain systemd[1]: firewalld.service: Deactivated successfully.
Sep 07 17:13:44 localhost.localdomain systemd[1]: Stopped firewalld - dynamic firewall daemon.
```

Telnet

❖ Window에서 접속 확인



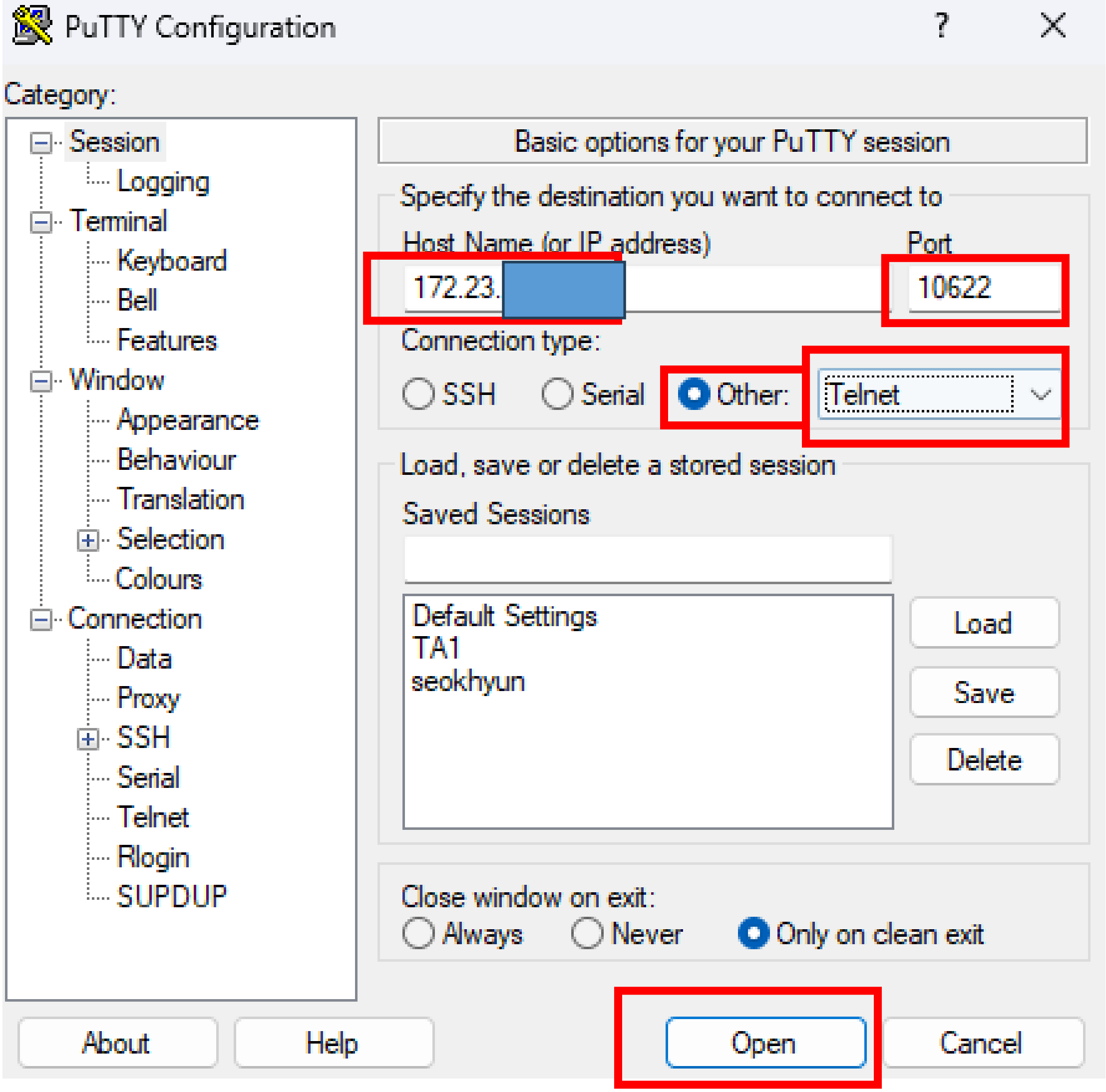
```
Password:
Last login: Sat Sep  7 23:43:54 from ::ffff:10.0.2.2
[teluser@localhost ~]$ 
```



```
Kernel 5.14.0-480.el9.x86_64 on an x86_64
localhost login: teluser
Password:
Last login: Sat Sep  7 23:41:37 from ::ffff:10.0.2.2
[teluser@localhost ~]$ 
```

Telnet

❖ putty를 통한 접속



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 172.23.[redacted]

Port: 10622

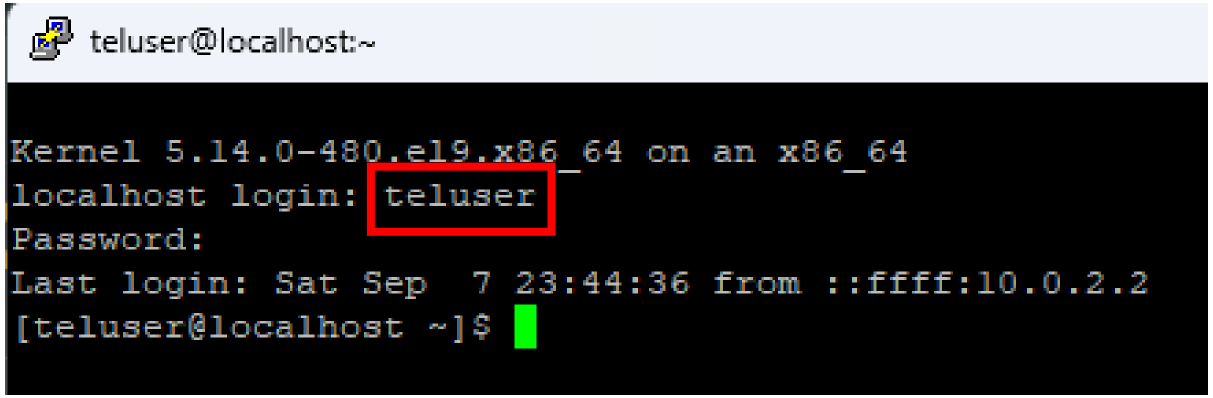
Connection type: ○ SSH ○ Serial ● Other: Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings
TA1
seokhyun

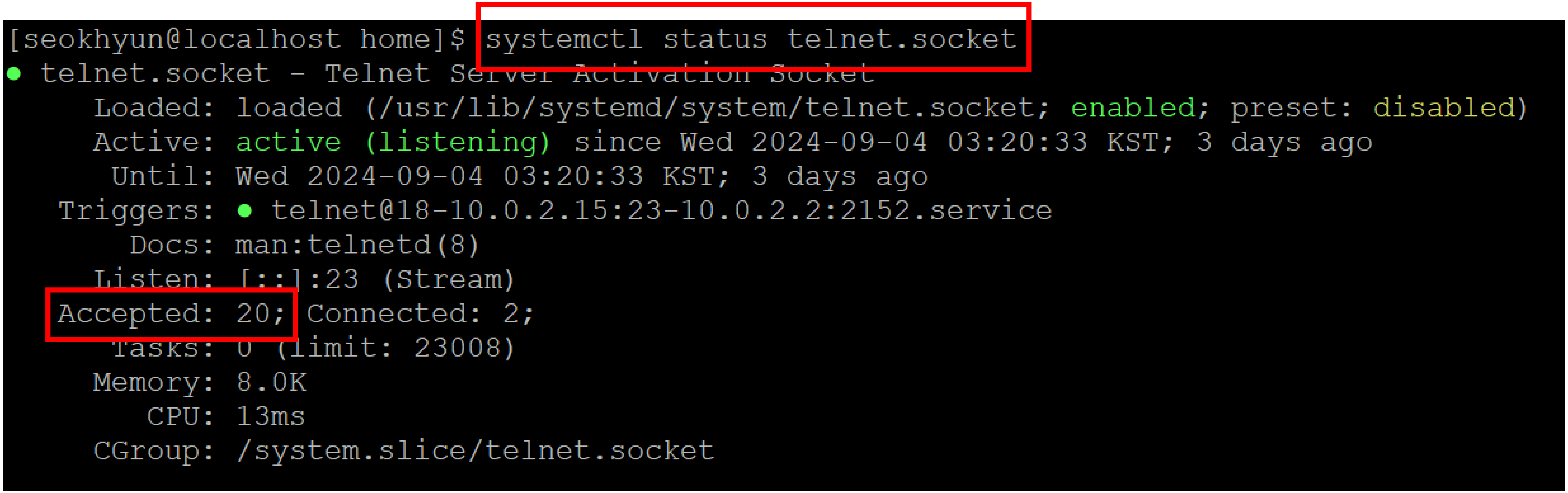
Close window on exit: ○ Always ○ Never ● Only on clean exit



```
Kernel 5.14.0-480.el9.x86_64 on an x86_64
localhost login: teluser
Password:
Last login: Sat Sep  7 23:44:36 from ::ffff:10.0.2.2
[teluser@localhost ~]$ 
```

Telnet

❖ putty를 통한 접속

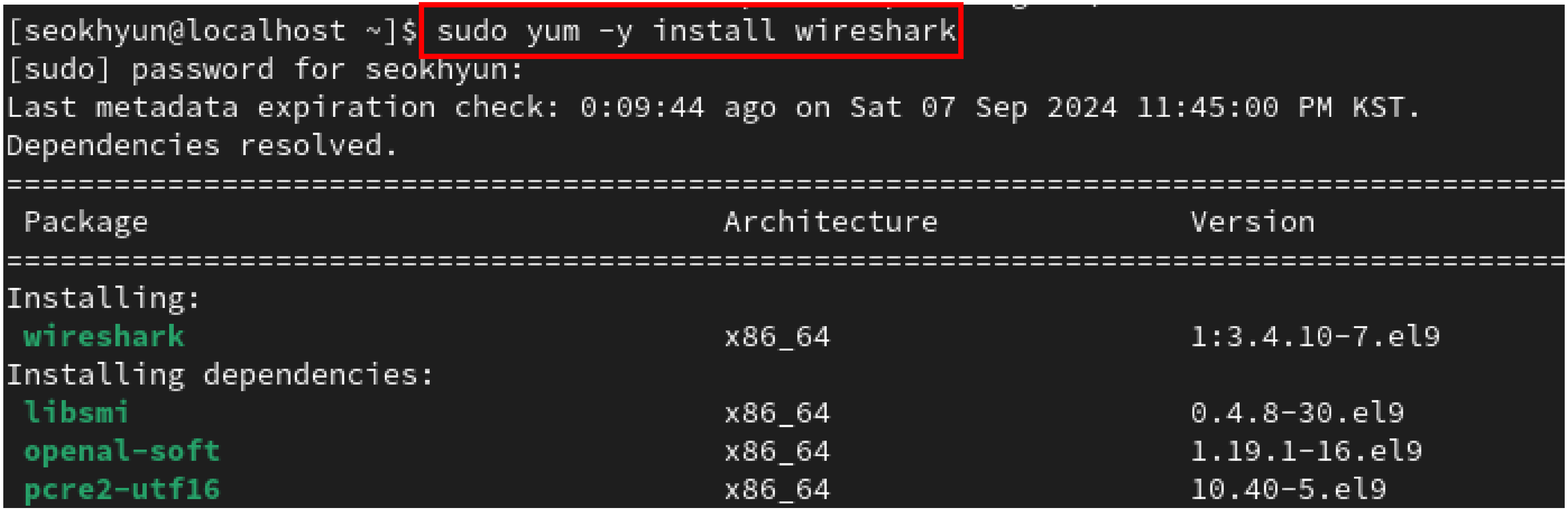


```
[seokhyun@localhost home]$ systemctl status telnet.socket
● telnet.socket - Telnet Server Activation Socket
     Loaded: loaded (/usr/lib/systemd/system/telnet.socket; enabled; preset: disabled)
     Active: active (listening) since Wed 2024-09-04 03:20:33 KST; 3 days ago
      Until: Wed 2024-09-04 03:20:33 KST; 3 days ago
   Triggers: ● telnet@18-10.0.2.15:23-10.0.2.2:2152.service
       Docs: man:telnetd(8)
     Listen: [::]:23 (Stream)
   Accepted: 20; Connected: 2;
      Tasks: 0 (limit: 23008)
     Memory: 8.0K
        CPU: 13ms
     CGroup: /system.slice/telnet.socket
```

WireShark

❖ WireShark 설치

- sudo yum –y install wireshark
- sudo yum –y install wireshark-gnome (첫 번째 명령어로 설치가 안될 시)

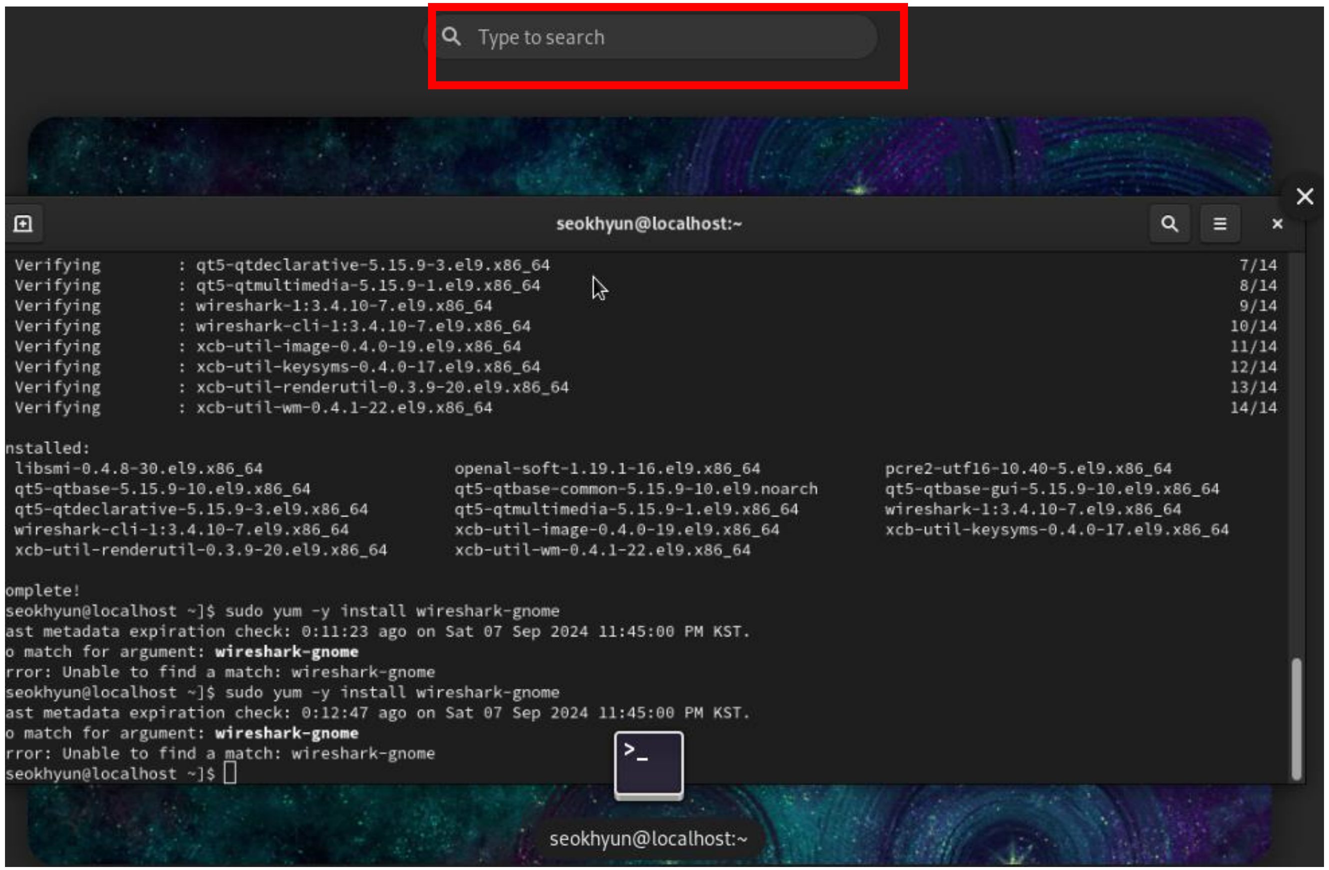


```
[seokhyun@localhost ~]$ sudo yum -y install wireshark
[sudo] password for seokhyun:
Last metadata expiration check: 0:09:44 ago on Sat 07 Sep 2024 11:45:00 PM KST.
Dependencies resolved.
==========================================================================================
 Package                                Architecture              Version
==========================================================================================
Installing:
 wireshark                              x86_64                    1:3.4.10-7.el9
Installing dependencies:
 libsmi                                 x86_64                    0.4.8-30.el9
 openal-soft                            x86_64                    1.19.1-16.el9
 pcre2-utf16                            x86_64                    10.40-5.el9
```

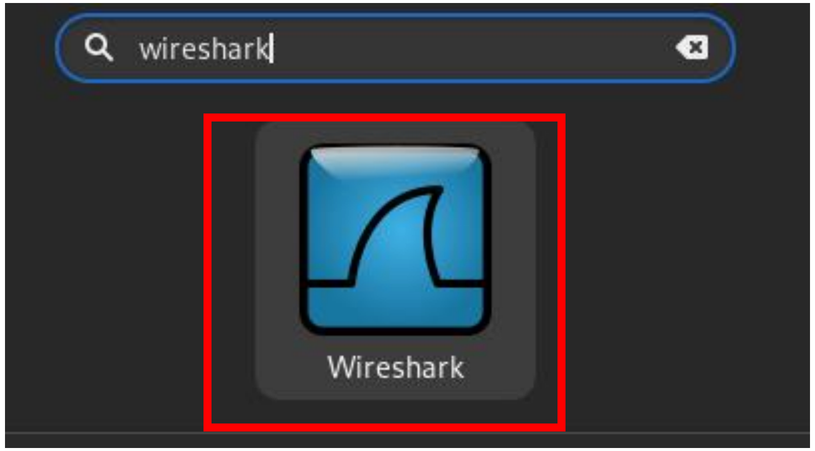
WireShark

❖ WireShark GUI

- wireshark & (실행이 가능)

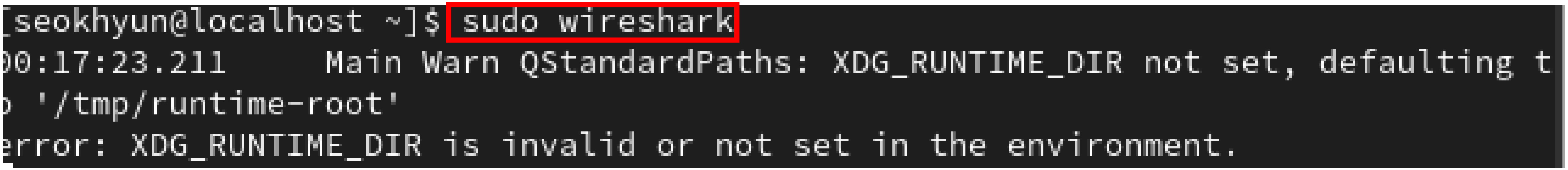


```
 Verifying        : qt5-qtdeclarative-5.15.9-3.el9.x86_64                                      7/14
 Verifying        : qt5-qtmultimedia-5.15.9-1.el9.x86_64                                       8/14
 Verifying        : wireshark-1:3.4.10-7.el9.x86_64                                            9/14
 Verifying        : wireshark-cli-1:3.4.10-7.el9.x86_64                                       10/14
 Verifying        : xcb-util-image-0.4.0-19.el9.x86_64                                        11/14
 Verifying        : xcb-util-keysyms-0.4.0-17.el9.x86_64                                      12/14
 Verifying        : xcb-util-renderutil-0.3.9-20.el9.x86_64                                   13/14
 Verifying        : xcb-util-wm-0.4.1-22.el9.x86_64                                           14/14

nstalled:
 libsmi-0.4.8-30.el9.x86_64              openal-soft-1.19.1-16.el9.x86_64          pcre2-utf16-10.40-5.el9.x86_64
 qt5-qtbase-5.15.9-10.el9.x86_64         qt5-qtbase-common-5.15.9-10.el9.noarch    qt5-qtbase-gui-5.15.9-10.el9.x86_64
 qt5-qtdeclarative-5.15.9-3.el9.x86_64   qt5-qtmultimedia-5.15.9-1.el9.x86_64      wireshark-1:3.4.10-7.el9.x86_64
 wireshark-cli-1:3.4.10-7.el9.x86_64     xcb-util-image-0.4.0-19.el9.x86_64        xcb-util-keysyms-0.4.0-17.el9.x86_64
 xcb-util-renderutil-0.3.9-20.el9.x86_64 xcb-util-wm-0.4.1-22.el9.x86_64

omplete!
seokhyun@localhost ~]$ sudo yum -y install wireshark-gnome
ast metadata expiration check: 0:11:23 ago on Sat 07 Sep 2024 11:45:00 PM KST.
o match for argument: wireshark-gnome
rror: Unable to find a match: wireshark-gnome
seokhyun@localhost ~]$ sudo yum -y install wireshark-gnome
ast metadata expiration check: 0:12:47 ago on Sat 07 Sep 2024 11:45:00 PM KST.
o match for argument: wireshark-gnome
rror: Unable to find a match: wireshark-gnome
seokhyun@localhost ~]$ 
```

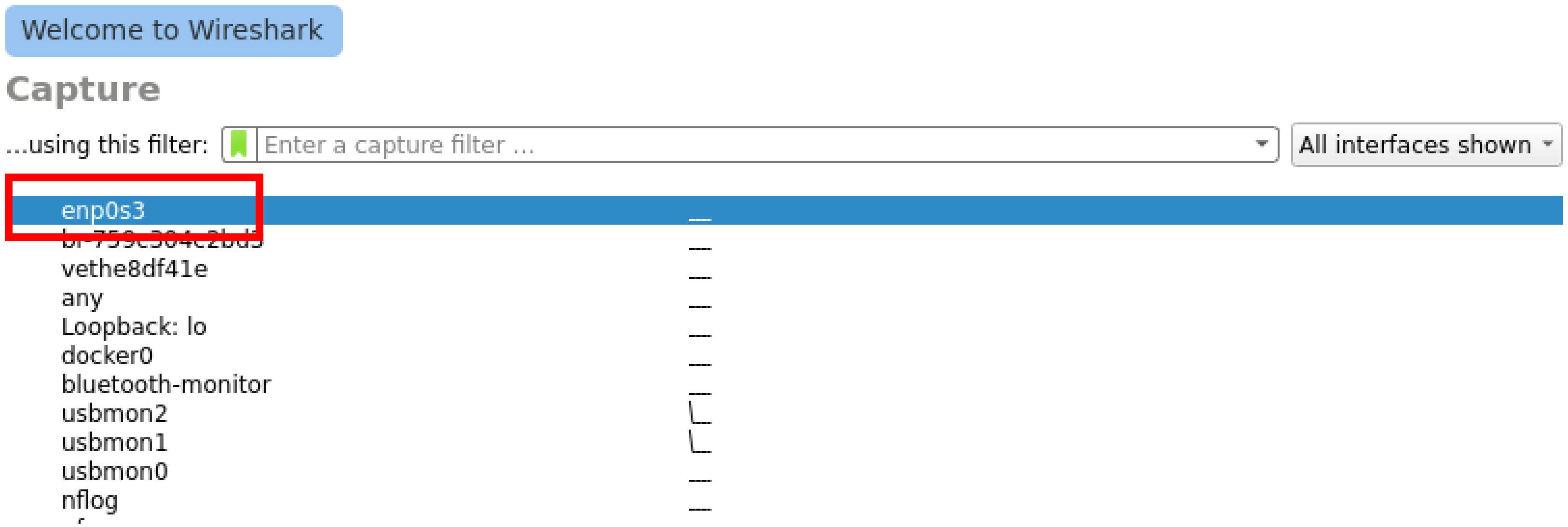


WireShark

- WireShark GUI
  - sudo wireshark



```
[seokhyun@localhost ~]$ sudo wireshark
00:17:23.211      Main Warn QStandardPaths: XDG_RUNTIME_DIR not set, defaulting t
o '/tmp/runtime-root'
error: XDG_RUNTIME_DIR is invalid or not set in the environment.
```



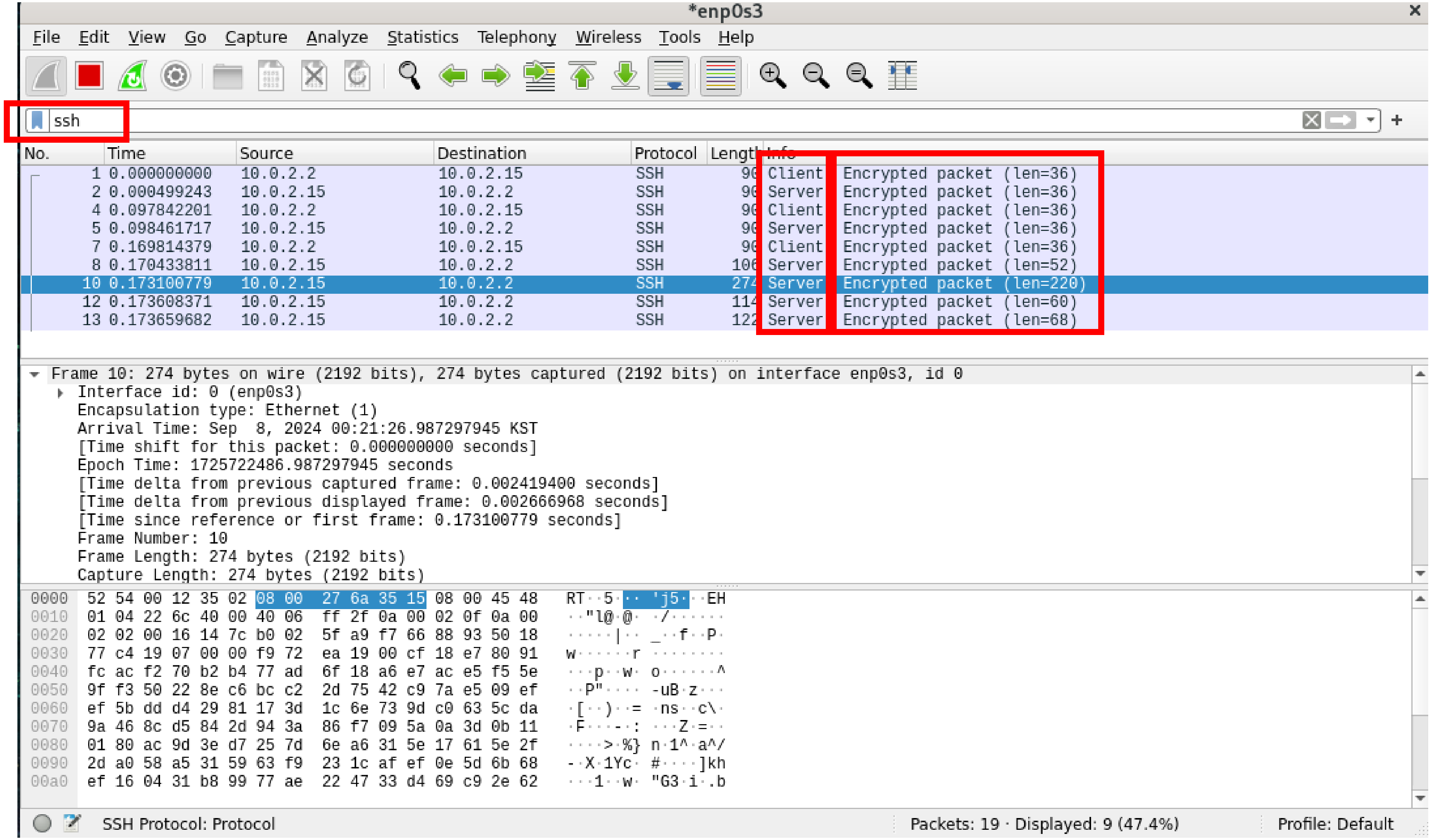
Capture

...using this filter: Enter a capture filter ... All interfaces shown

```
enp0s3
br-759c304c2bd5
vethe8df41e
any
Loopback: lo
docker0
bluetooth-monitor
usbmon2
usbmon1
usbmon0
nflog
```

Network Packet Analysis

❖ ssh network packet 확인


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: ssh

```
No.   Time          Source       Destination  Protocol Length Info
    1 0.000000000   10.0.2.2     10.0.2.15    SSH      90  Client  Encrypted packet (len=36)
    2 0.000499243   10.0.2.15    10.0.2.2     SSH      90  Server  Encrypted packet (len=36)
    4 0.097842201   10.0.2.2     10.0.2.15    SSH      90  Client  Encrypted packet (len=36)
    5 0.098461717   10.0.2.15    10.0.2.2     SSH      90  Server  Encrypted packet (len=36)
    7 0.169814379   10.0.2.2     10.0.2.15    SSH      90  Client  Encrypted packet (len=36)
    8 0.170433811   10.0.2.15    10.0.2.2     SSH      106 Server  Encrypted packet (len=52)
   10 0.173100779   10.0.2.15    10.0.2.2     SSH      274 Server  Encrypted packet (len=220)
   12 0.173608371   10.0.2.15    10.0.2.2     SSH      114 Server  Encrypted packet (len=60)
   13 0.173659682   10.0.2.15    10.0.2.2     SSH      122 Server  Encrypted packet (len=68)
```

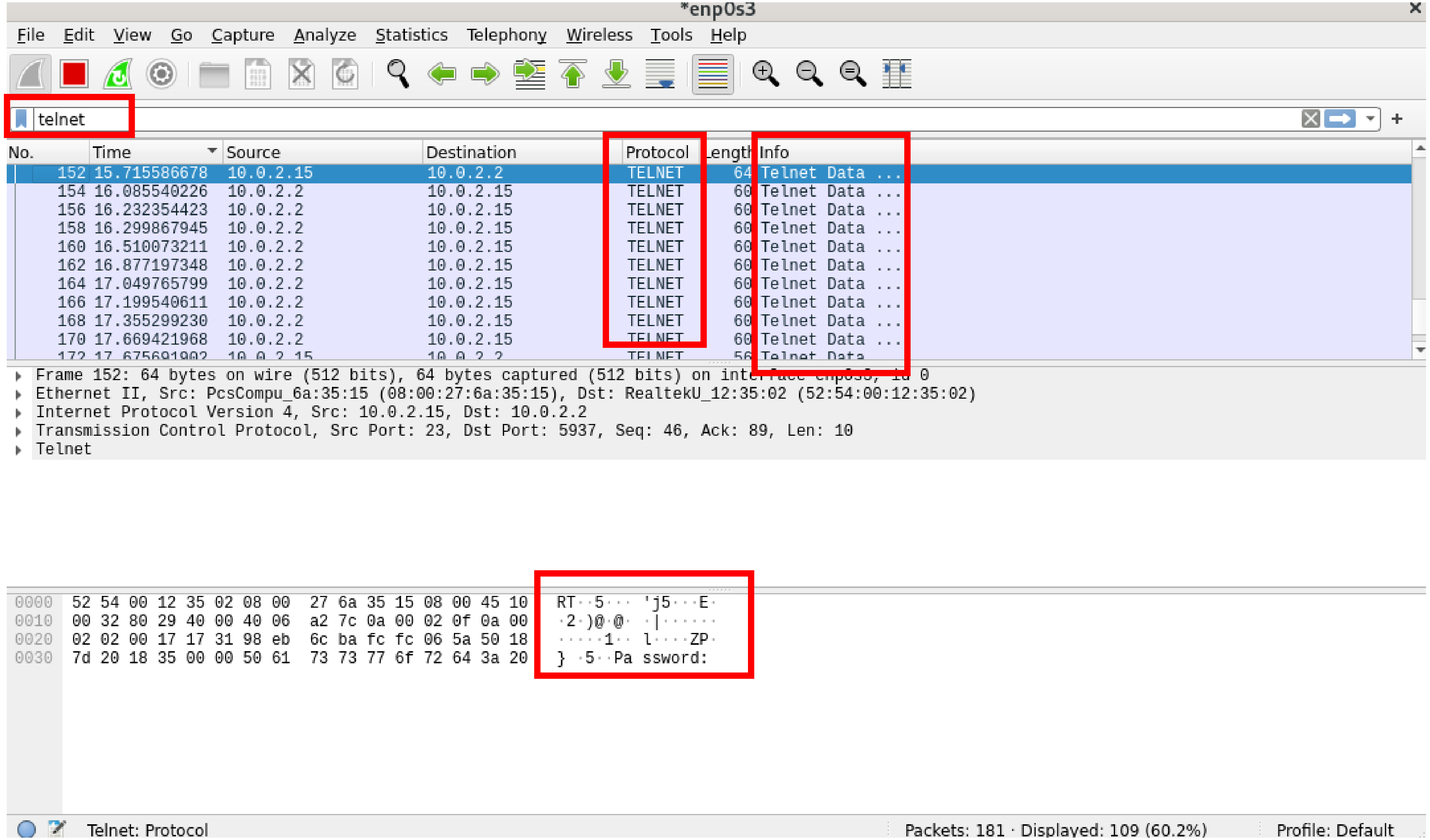
```
▾ Frame 10: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits) on interface enp0s3, id 0
  ▸ Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep  8, 2024 00:21:26.987297945 KST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1725722486.987297945 seconds
    [Time delta from previous captured frame: 0.002419400 seconds]
    [Time delta from previous displayed frame: 0.002666968 seconds]
    [Time since reference or first frame: 0.173100779 seconds]
    Frame Number: 10
    Frame Length: 274 bytes (2192 bits)
    Capture Length: 274 bytes (2192 bits)
```

```
0000  52 54 00 12 35 02 08 00  27 6a 35 15 08 00 45 48   RT··5···'j5···EH
0010  01 04 22 6c 40 00 40 06  ff 2f 0a 00 02 0f 0a 00   ··"l@·@··/······
0020  02 02 00 16 14 7c b0 02  5f a9 f7 66 88 93 50 18   ·····|··_··f··P·
0030  77 c4 19 07 00 00 f9 72  ea 19 00 cf 18 e7 80 91   w······r········
0040  fc ac f2 70 b2 b4 77 ad  6f 18 a6 e7 ac e5 f5 5e   ···p··w·o······^
0050  9f f3 50 22 8e c6 bc c2  2d 75 42 c9 7a e5 09 ef   ··P"····-uB·z···
0060  ef 5b dd d4 29 81 17 3d  1c 6e 73 9d c0 63 5c da   ·[··)··=·ns··c\·
0070  9a 46 8c d5 84 2d 94 3a  86 f7 09 5a 0a 3d 0b 11   ·F···-·:···Z·=··
0080  01 80 ac 9d 3e d7 25 7d  6e a6 31 5e 17 61 5e 2f   ····>·%}n·1^·a^/
0090  2d a0 58 a5 31 59 63 f9  23 1c af ef 0e 5d 6b 68   -·X·1Yc·#····]kh
00a0  ef 16 04 31 b8 99 77 ae  22 47 33 d4 69 c9 2e 62   ···1··w·"G3·i·.b
```

SSH Protocol: Protocol | Packets: 19 · Displayed: 9 (47.4%) | Profile: Default

Network Packet Analysis

❖ telnet network packet 확인



*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: telnet

```
No.   Time             Source      Destination  Protocol Length Info
  152 15.715586678  10.0.2.15   10.0.2.2     TELNET     64 Telnet Data ...
  154 16.085540226  10.0.2.2    10.0.2.15    TELNET     60 Telnet Data ...
  156 16.232354423  10.0.2.2    10.0.2.15    TELNET     60 Telnet Data ...
  158 16.299867945  10.0.2.2    10.0.2.15    TELNET     60 Telnet Data ...
  160 16.510073211  10.0.2.2    10.0.2.15    TELNET     60 Telnet Data ...
  162 16.877197348  10.0.2.2    10.0.2.15    TELNET     60 Telnet Data ...
  164 17.049765799  10.0.2.2    10.0.2.15    TELNET     60 Telnet Data ...
  166 17.199540611  10.0.2.2    10.0.2.15    TELNET     60 Telnet Data ...
  168 17.355299230  10.0.2.2    10.0.2.15    TELNET     60 Telnet Data ...
  170 17.669421968  10.0.2.2    10.0.2.15    TELNET     60 Telnet Data ...
  172 17.675691902  10.0.2.15   10.0.2.2     TELNET     56 Telnet Data
```

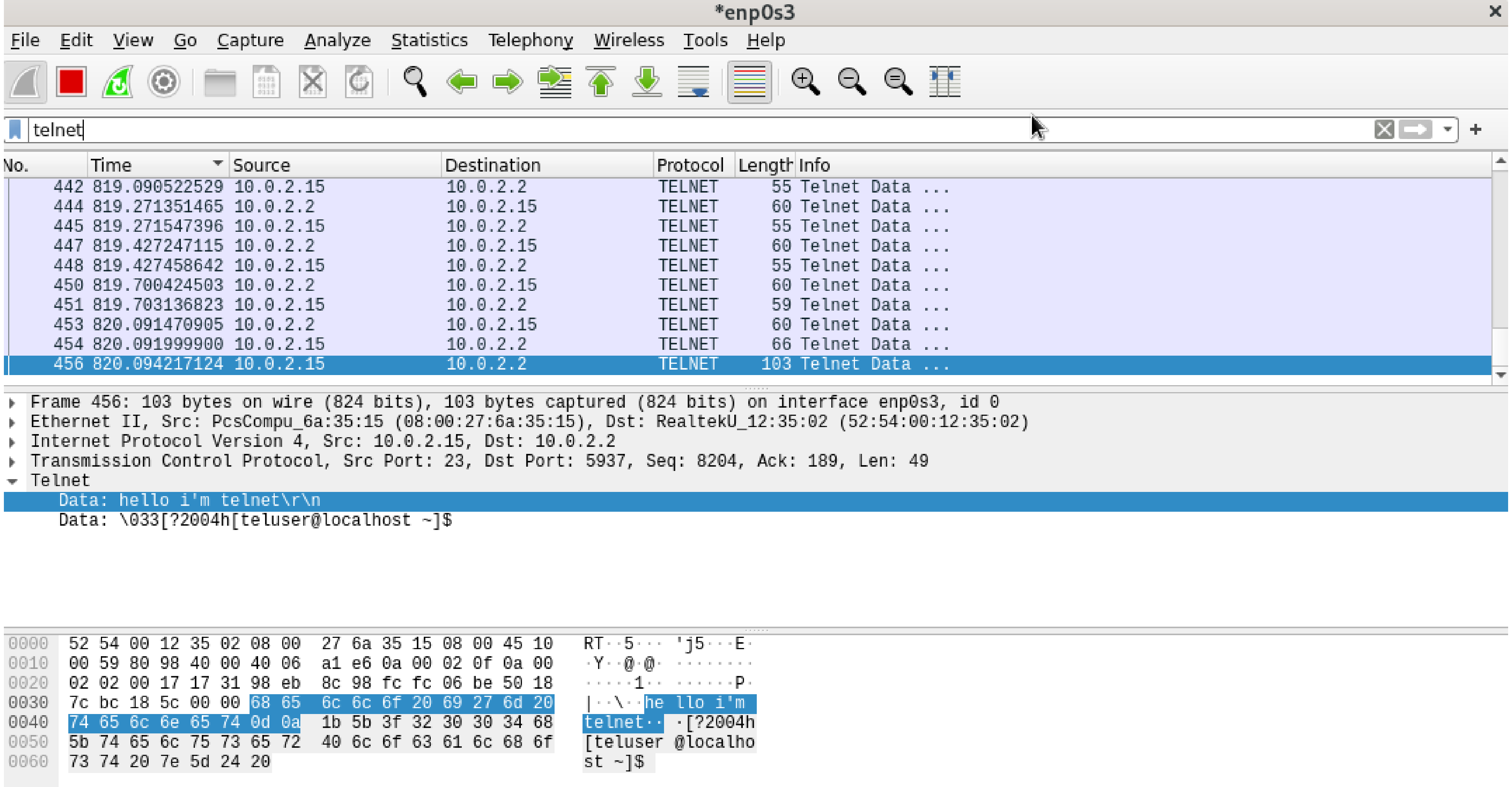
```
▸ Frame 152: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_6a:35:15 (08:00:27:6a:35:15), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.2
▸ Transmission Control Protocol, Src Port: 23, Dst Port: 5937, Seq: 46, Ack: 89, Len: 10
▸ Telnet
```

```
0000  52 54 00 12 35 02 08 00  27 6a 35 15 08 00 45 10   RT··5··· 'j5···E·
0010  00 32 80 29 40 00 40 06  a2 7c 0a 00 02 0f 0a 00   ·2·)@·@· ·|······
0020  02 02 00 17 17 31 98 eb  6c ba fc fc 06 5a 50 18   ·····1·· l····ZP·
0030  7d 20 18 35 00 00 50 61  73 73 77 6f 72 64 3a 20   } ·5··Pa ssword:
```

Telnet: Protocol   Packets: 181 · Displayed: 109 (60.2%)   Profile: Default

Network Packet Analysis

❖ telnet network packet 확인


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

```
No.    Time          Source       Destination   Protocol Length Info
   442 819.090522529 10.0.2.15    10.0.2.2      TELNET     55 Telnet Data ...
   444 819.271351465 10.0.2.2     10.0.2.15     TELNET     60 Telnet Data ...
   445 819.271547396 10.0.2.15    10.0.2.2      TELNET     55 Telnet Data ...
   447 819.427247115 10.0.2.2     10.0.2.15     TELNET     60 Telnet Data ...
   448 819.427458642 10.0.2.15    10.0.2.2      TELNET     55 Telnet Data ...
   450 819.700424503 10.0.2.2     10.0.2.15     TELNET     60 Telnet Data ...
   451 819.703136823 10.0.2.15    10.0.2.2      TELNET     59 Telnet Data ...
   453 820.091470905 10.0.2.2     10.0.2.15     TELNET     60 Telnet Data ...
   454 820.091999900 10.0.2.15    10.0.2.2      TELNET     66 Telnet Data ...
   456 820.094217124 10.0.2.15    10.0.2.2      TELNET    103 Telnet Data ...
```

```
▸ Frame 456: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_6a:35:15 (08:00:27:6a:35:15), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.2
▸ Transmission Control Protocol, Src Port: 23, Dst Port: 5937, Seq: 8204, Ack: 189, Len: 49
▾ Telnet
    Data: hello i'm telnet\r\n
    Data: \033[?2004h[teluser@localhost ~]$
```

```
0000  52 54 00 12 35 02 08 00  27 6a 35 15 08 00 45 10   RT··5··· 'j5···E·
0010  00 59 80 98 40 00 40 06  a1 e6 0a 00 02 0f 0a 00   ·Y··@·@· ········
0020  02 02 00 17 17 31 98 eb  8c 98 fc fc 06 be 50 18   ·····1·· ······P·
0030  7c bc 18 5c 00 00 68 65  6c 6c 6f 20 69 27 6d 20   |··\··he llo i'm 
0040  74 65 6c 6e 65 74 0d 0a  1b 5b 3f 32 30 30 34 68   telnet·· ·[?2004h
0050  5b 74 65 6c 75 73 65 72  40 6c 6f 63 61 6c 68 6f   [teluser @localho
0060  73 74 20 7e 5d 24 20                               st ~]$ 
```

Network Packet Analysis

❖ telnet network packet 실습 - 1

- 본인의 putty, powershell을 통해 telnet으로 접속
- ID, PW 입력
- Wireshark를 통해 ID, PW 네트워크 패킷 분석
- 각각 어떻게 패킷이 발생하는지 확인

Network Packet Analysis

❖ telnet network packet 실습 – 2

- test.txt 파일 생성
- “hello, I’m telnet” 작성 후 저장
- Wireshark를 통해 패킷 분석
- Cat test.txt 명령어 입력 후 wireshark를 통해 패킷 분석
- Root 권한 획득 후 패킷 분석