Ubuntu 리눅스에서 wireshark

김 솔

TABLE OF CONTENTS

01 Ubuntu

02 wireshark

• Ubuntu

사용 편의성에 초점을 맞춘 리눅스 배포판

-장점

- Windows, 맥 OS와 같은 그래픽 환경
- 배포판을 수정하거나 수정한 것을 재배포할 수 있는 자유 소프트웨어
- 오픈 소스, 55개 언어 지원
- sudo 도구사용

-단점

- 6개월에 한번 업그레이드

ubuntu

- apt

(Avanced Pakage Tool)

```
tik@tik-VirtualBox:~$ apt
apt 2.0.4 (amd64)
사용법: apt [options] command

apt는 패키지에 대해 정보 표시, 검색, 관리 등의
명령어를 제공하는 명령줄 패키지 관리자입니다.
apt는 apt-get과 apt-cache와 같이 특화된 APT 도구들과
동등한 기능들을 제공하지만, 기본적으로 상호작용적인
사용을 위해 적합한 옵션을 활성화합니다.

자주 사용되는 명령어:
  list - 패키지 이름을 기반으로 패키지를 나열합니다
  search - 패키지 설명에서 키워드를 검색합니다
  show - 패키지의 정보를 표시합니다
  install - 패키지를 설치합니다
  reinstall - 패키지를 재설치합니다
  remove - 패키지를 제거합니다
  autoremove - 사용하지 않는 패키지를 자동으로 전부 지웁니다
  update - 사용 가능한 패키지의 목록을 업데이트합니다
  upgrade - 패키지를 설치/업그레이드해 시스템을 업그레이드합니다
  full-upgrade - 패키지를 삭제/설치/업그레이드해 시스템을 업그레이드합니다
  edit-sources - 소스 정보 파일을 편집합니다
  satisfy - satisfy dependency strings

이용 가능한 명령에 대한 더 많은 정보를 얻고자 한다면 apt(8)를 보십시오.
Configuration options and syntax is detailed in apt.conf(5).
Information about how to configure sources can be found in sources.list(5).
Package and version choices can be expressed via apt_preferences(5).
Security details are available in apt-secure(8).
                    이 APT는 Super Cow Powers로 무장했습니다.
tik@tik-VirtualBox:~$
```

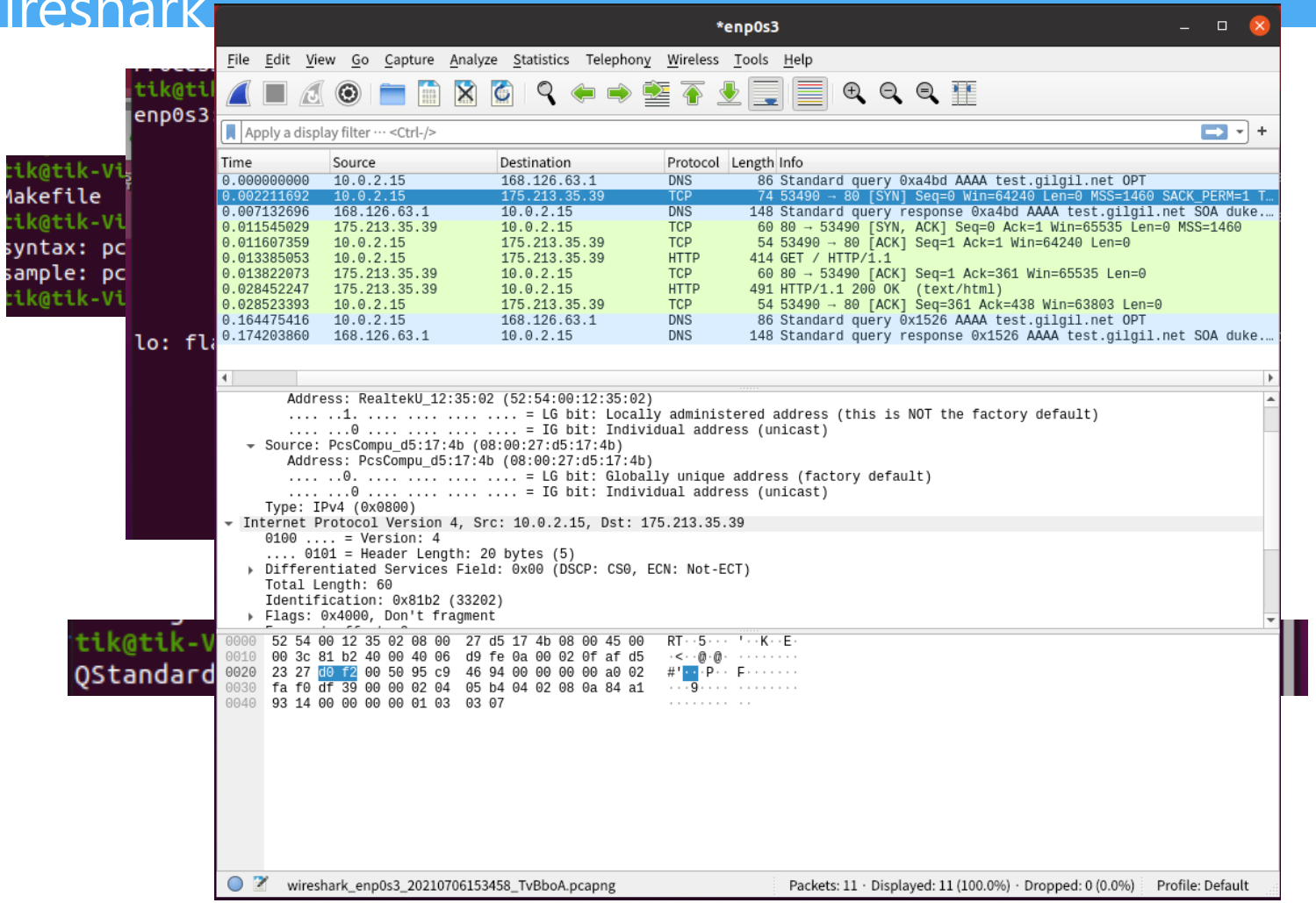
- sudo

```
tik@tik-VirtualBox:~$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
            [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
            prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
            prompt] [-T timeout] [-u user] file ...
tik@tik-VirtualBox:~$
```

```
sudo apt install net-tools
```

pcap 패킷 캡처용 라이브러리

- Wireshark


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
Time Source Destination Protocol Length Info
0.000000000 10.0.2.15 168.126.63.1 DNS 86 Standard query 0xa4bd AAAA test.gilgil.net OPT
0.002211692 10.0.2.15 175.213.35.39 TCP 74 53490 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
0.007132696 168.126.63.1 10.0.2.15 DNS 148 Standard query response 0xa4bd AAAA test.gilgil.net SOA duke.…
0.011545029 175.213.35.39 10.0.2.15 TCP 60 80 → 53490 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
0.011607359 10.0.2.15 175.213.35.39 TCP 54 53490 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
0.013385053 10.0.2.15 175.213.35.39 HTTP 414 GET / HTTP/1.1
0.013822073 175.213.35.39 10.0.2.15 TCP 60 80 → 53490 [ACK] Seq=1 Ack=361 Win=65535 Len=0
0.028452247 175.213.35.39 10.0.2.15 HTTP 491 HTTP/1.1 200 OK (text/html)
0.028523393 10.0.2.15 175.213.35.39 TCP 54 53490 → 80 [ACK] Seq=361 Ack=438 Win=63803 Len=0
0.164475416 10.0.2.15 168.126.63.1 DNS 86 Standard query 0x1526 AAAA test.gilgil.net OPT
0.174203860 168.126.63.1 10.0.2.15 DNS 148 Standard query response 0x1526 AAAA test.gilgil.net SOA duke.…
Address: RealtekU_12:35:02 (52:54:00:12:35:02)
.... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
....0 .... = IG bit: Individual address (unicast)
Source: PcsCompu_d5:17:4b (08:00:27:d5:17:4b)
Address: PcsCompu_d5:17:4b (08:00:27:d5:17:4b)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 175.213.35.39
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x81b2 (33202)
Flags: 0x4000, Don't fragment
0000 52 54 00 12 35 02 08 00 27 d5 17 4b 08 00 45 00
0010 00 3c 81 b2 40 00 40 06 d9 fe 0a 00 02 0f af d5
0020 23 27 d0 f2 00 50 95 c9 46 94 00 00 00 00 a0 02
0030 fa f0 df 39 00 00 02 04 05 b4 04 02 08 0a 84 a1
0040 93 14 00 00 00 00 01 03 03 07
wireshark_enp0s3_20210706153458_TvBboA.pcapng
Packets: 11 · Displayed: 11 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

• Wireshark

- 자유 및 오픈 소스 패킷 분석 프로그램
- 크로스 플랫폼으로, Qt 위젯 툴킷을 이용하여 사용자 인터페이스를 제공, pcap을 이용하여 패킷을 포획
- 포획한 네트워크 데이터는 GUI나 터미널 버전의 유틸리티 TShark를 통해 탐색할 수 있다.

그래픽 사용자 인터페이스(graphical user interface, **GUI**) 사용자가 편리하게 사용할 수 있도록 입출력 등의 기능을 알기 쉬운 아이콘 따위의 그래픽으로 나타낸 것

Thank you.