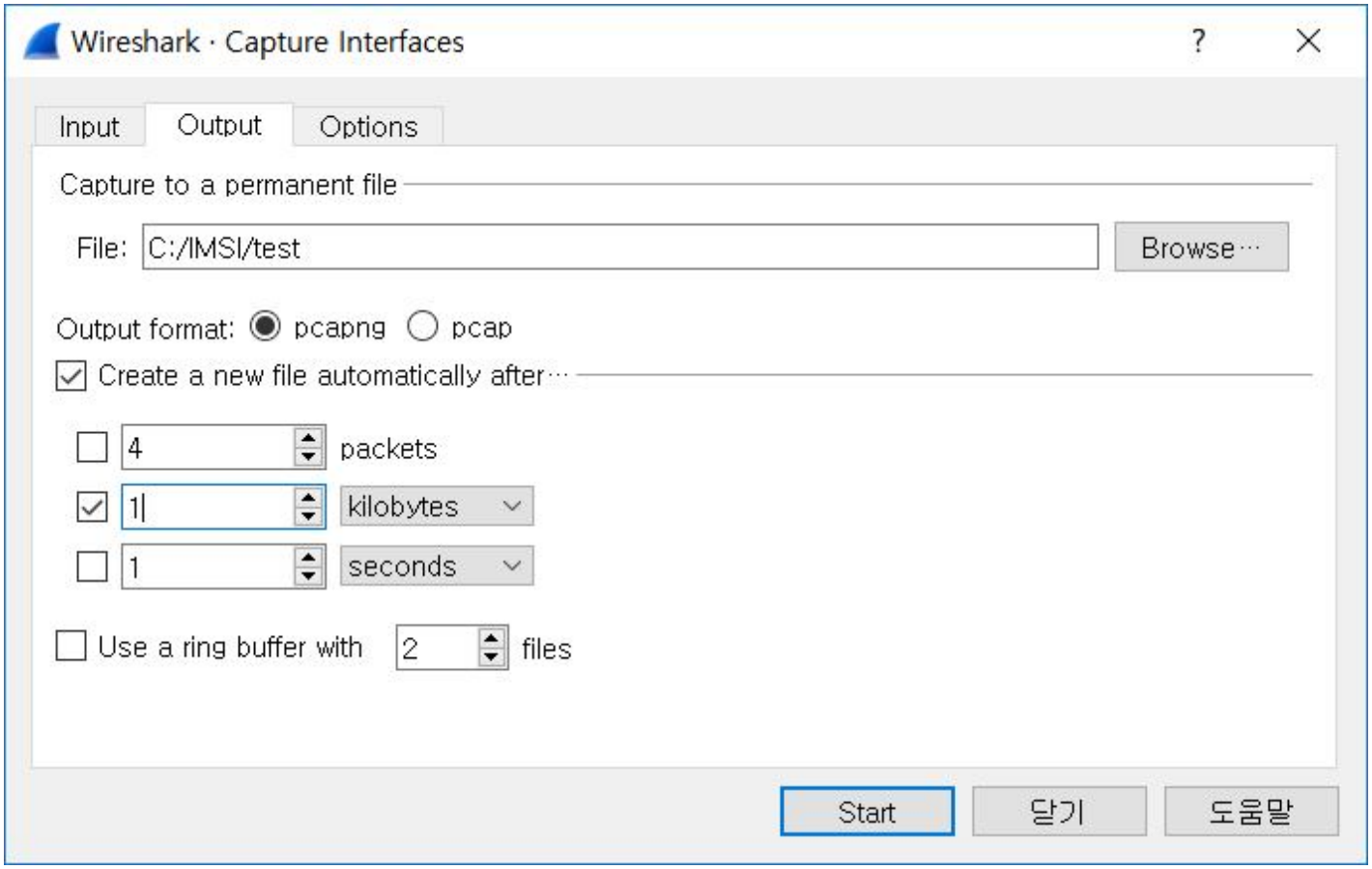
필터 사용

- **캡처 필터(Capture Filter)**
  - 패킷이 캡처될 때 지정
  - 지정된 표현식에 포함/제외된 패킷만 캡처

- **디스플레이 필터(Display Filter)**
  - 원하지 않는 패킷을 숨김
  - 지정된 표현식을 기반으로 원하는 패킷을 보기

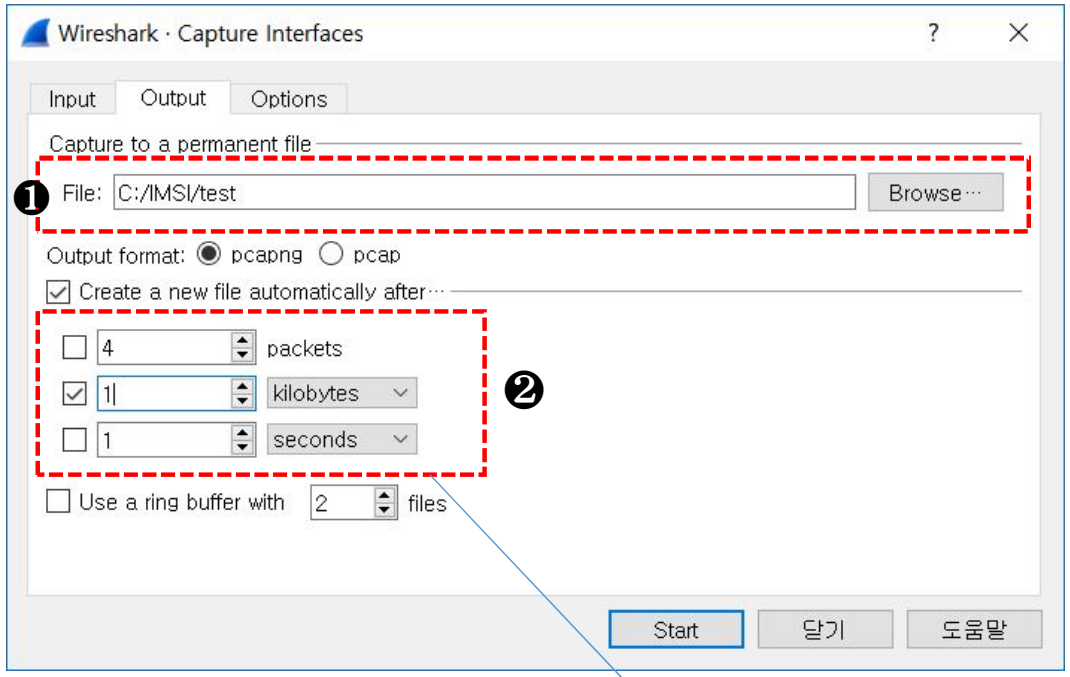
파일 집합으로 수집

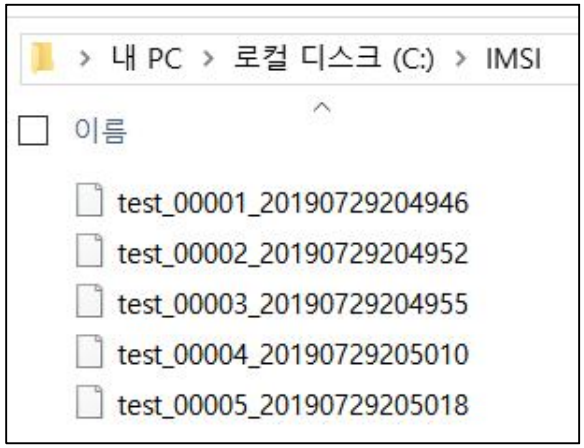
- Capture Options > Output Tab > Create a new file automatically after…



파일 집합으로 수집

- Capture Options > Output Tab > Create a new file automatically after…





- File > Open

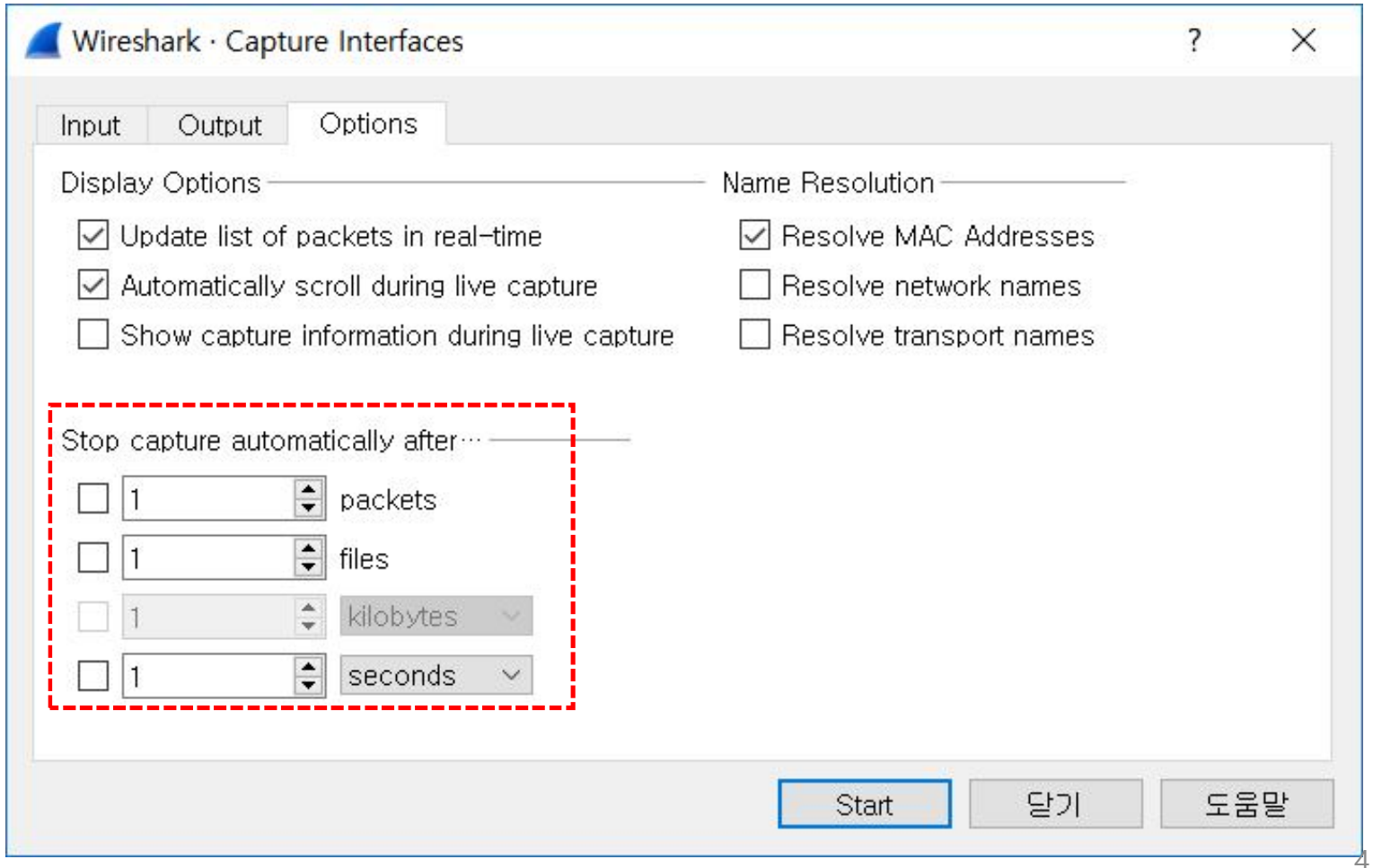
  - File > File set > List Files

파일당 4개의 패킷
1MB 파일 크기
1초마다

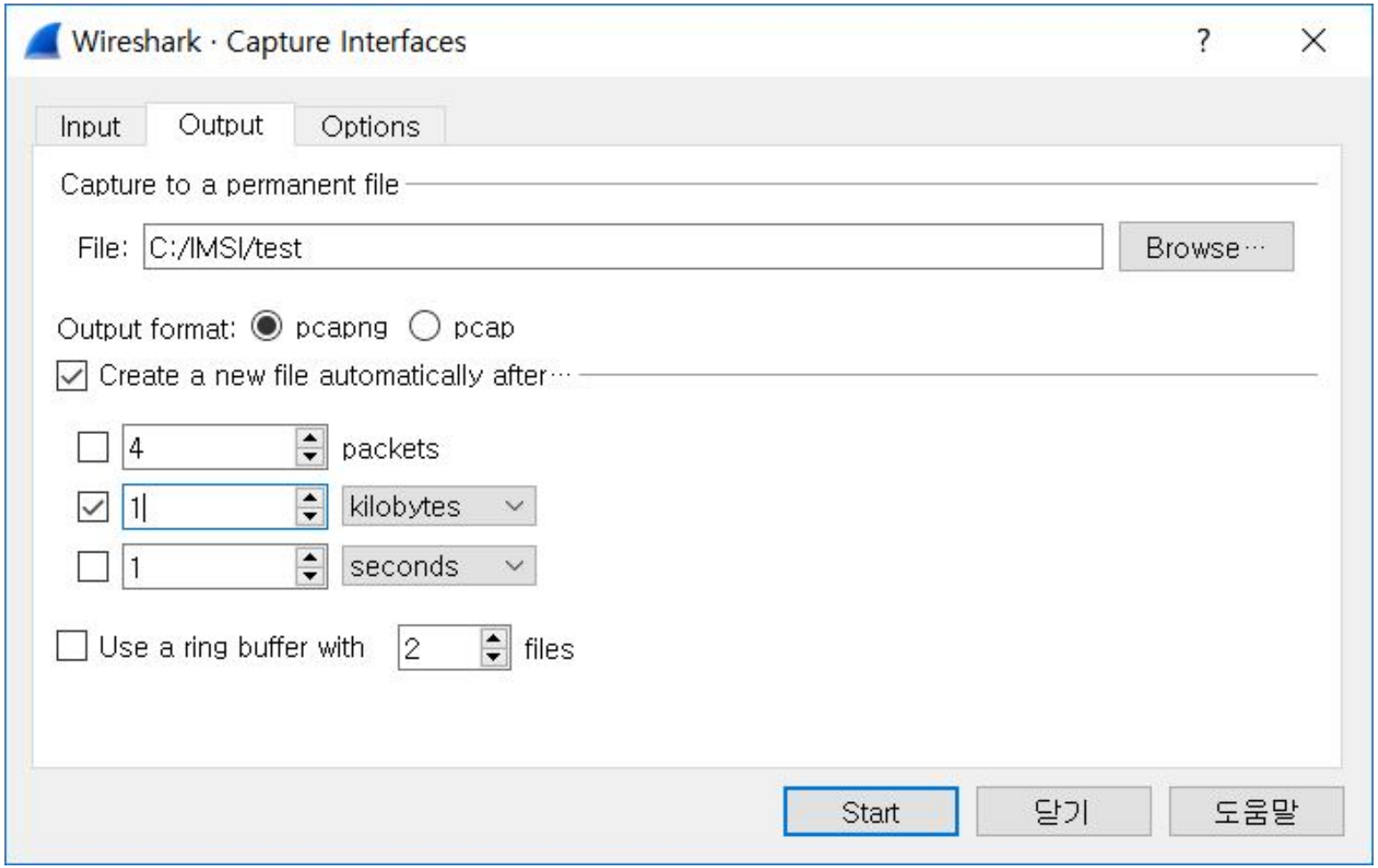
위의 어느 조건이든
먼저 만나면 파일 생성

파일 집합으로 수집

- Capture Options > Option Tab > Stop capture automatically after….

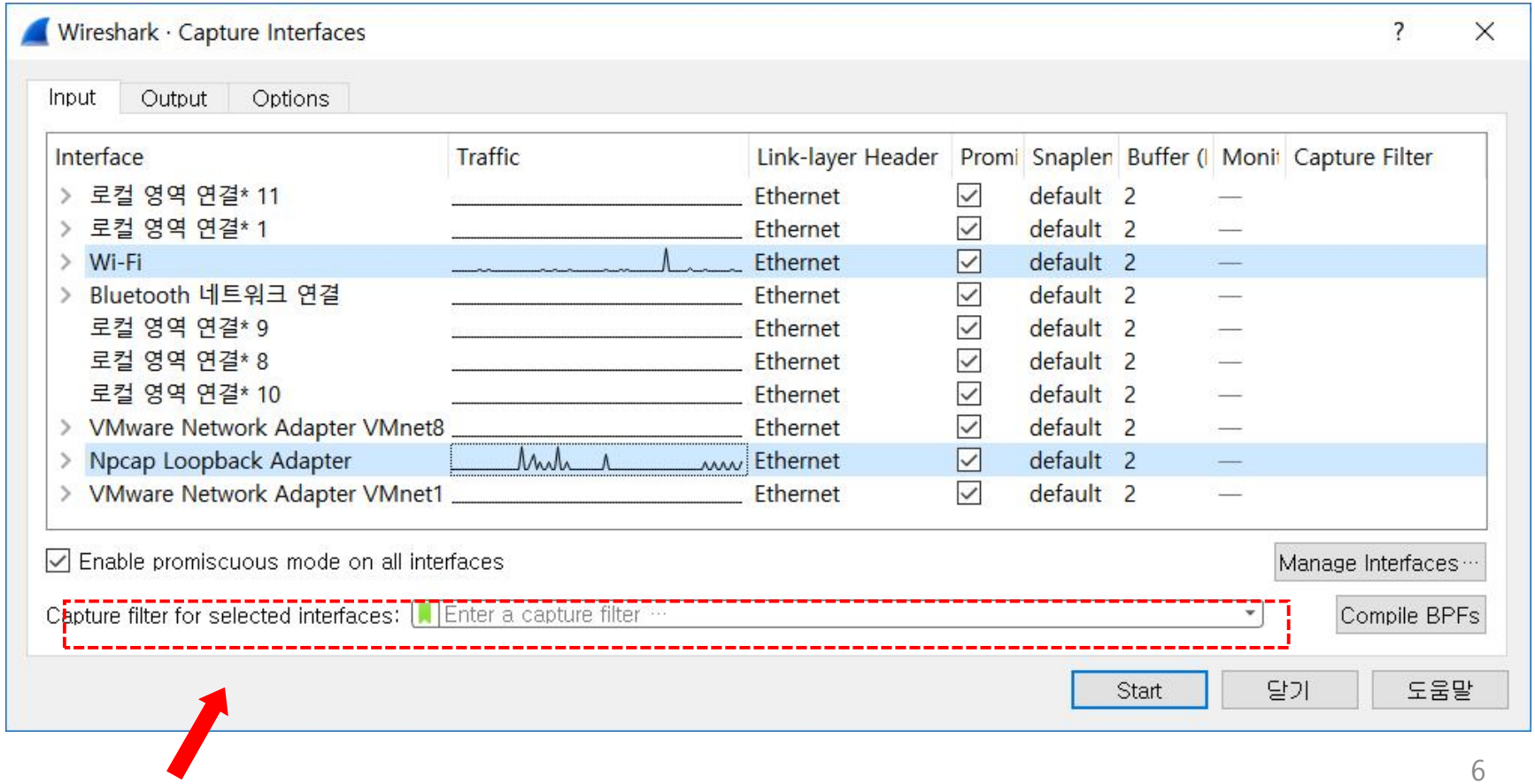


링 버퍼 사용


Wireshark · Capture Interfaces
Input
Output
Options
Capture to a permanent file
File: C:/IMSI/test
Browse…
Output format: pcapng pcap
Create a new file automatically after…
4 packets
1 kilobytes
1 seconds
Use a ring buffer with 2 files
Start
닫기
도움말

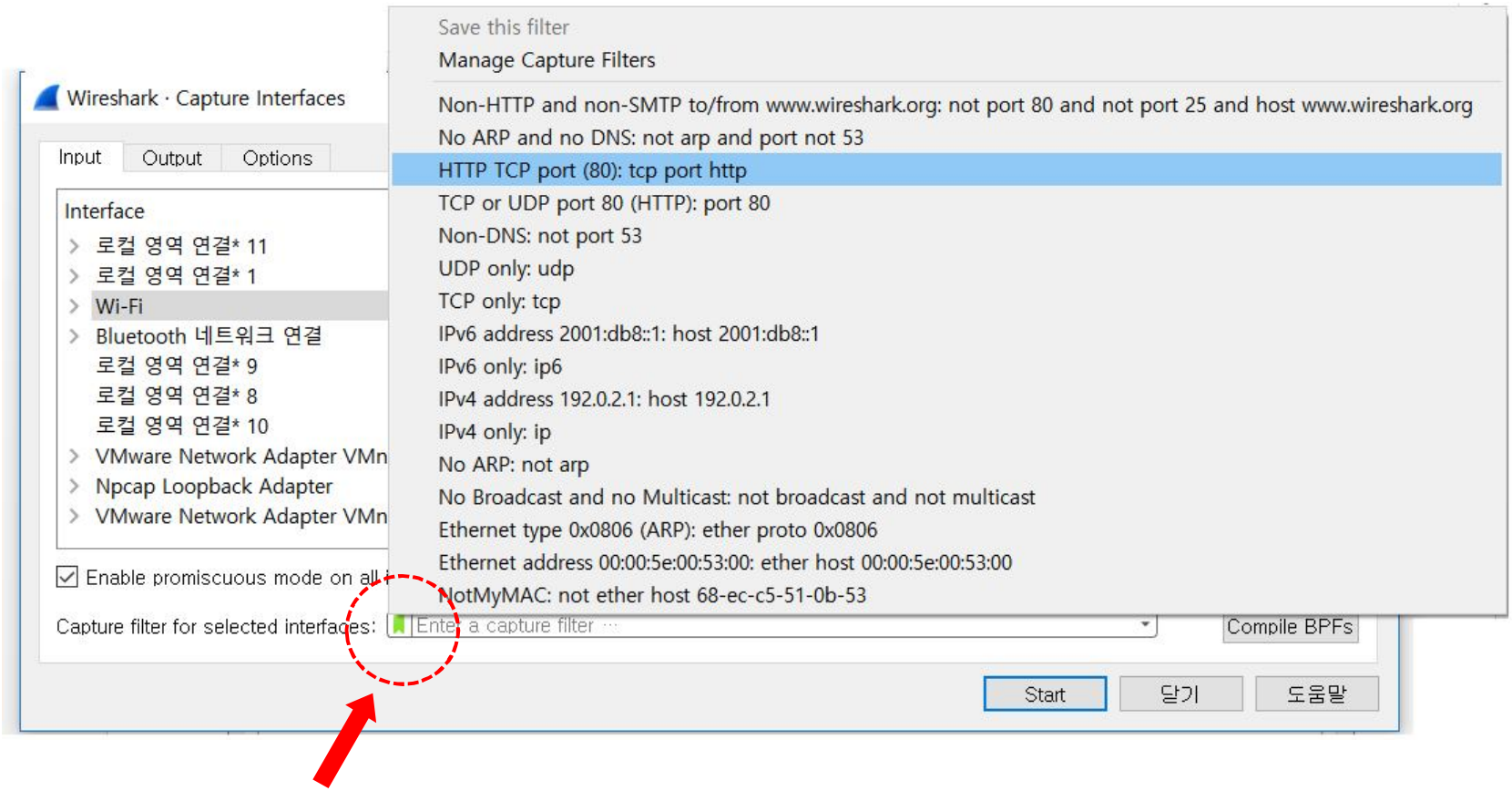
1) Capture Filter

- Capture Option 창에서 수집 필터 적용



Capture Option 창에서 수집 필터 적용

❶ Capture Option > 수집 필터 책갈피 화살표



수집 필터 책갈피 화살표

주소 기반의 트래픽 수집

❶ 특정 IP 주소에서/로 오는 트래픽 수집

- host 10.3.1.1
- host 2406:da00:ff00::6b16:f02d
- not host 10.3.1.1
- src host 10.3.1.1
- dst host 10.3.1.1
- host 10.3.1.1 or host 10.3.1.2
- host www.espn.com

주소 기반의 트래픽 수집

❷ IP 주소 범위에서/로 오는 트래픽 수집

- net 10.3.0.0/16
- net 10.3.0.0 mask 255.255.0.0
- ipv6 net 2406:da00:ff00::/64
- not dst net 10.3.0.0/16
- dst net 10.3.0.0/16
- src net 10.3.0.0/16

주소 기반의 트래픽 수집

❸ 브로드캐스트 또는 멀티캐스트 트래픽 수집

- ip broadcast
- ip multicast
- dst host ff02::1
- dst host ff02::2

주소 기반의 트래픽 수집

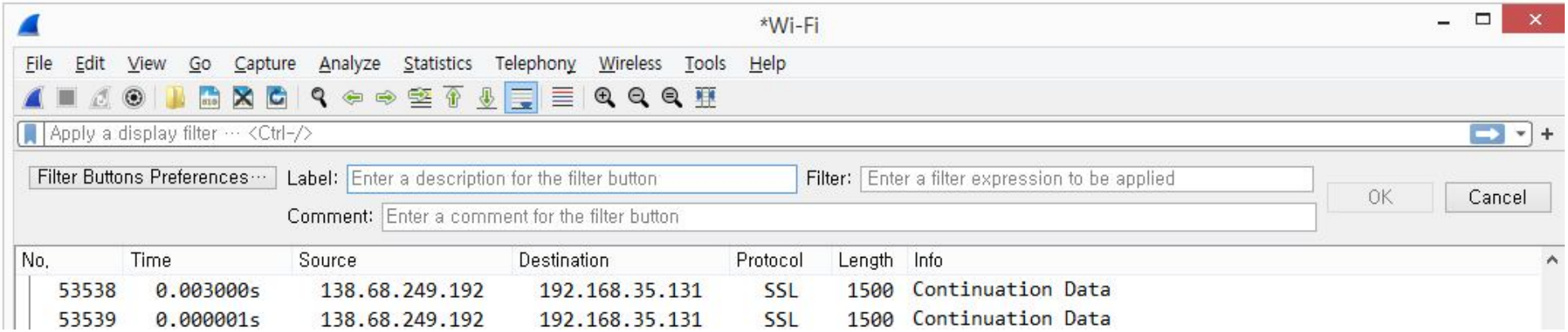
❹ MAC 주소 기반의 트래픽 수집

- ether host 00:08:15:00:08:15
- ether src 00:08:15:00:08:15
- ether dst 00:08:15:00:08:15
- not ether host 00:08:15:00:08:15

특정 애플리케이션에 대한 트래픽 수집

- port 53
- not port 53
- port 80
- udp port 67
- tcp port 21
- portrange 1-80
- tcp portrange 1-80
- port 20 or port 21
- host 10.3.1.1 and port 80
- host 10.3.1.1 and not port 80
- udp src port 68 and udp dst port 67

2) 디스플레이 필터


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
Filter Buttons Preferences···
Label: Enter a description for the filter button
Filter: Enter a filter expression to be applied
Comment: Enter a comment for the filter button
OK
Cancel
No. Time Source Destination Protocol Length Info
53538 0.003000s 138.68.249.192 192.168.35.131 SSL 1500 Continuation Data
53539 0.000001s 138.68.249.192 192.168.35.131 SSL 1500 Continuation Data

적절한 디스플레이 필터 문법 사용

- 간단한 디스플레이 필터 문법

  arp

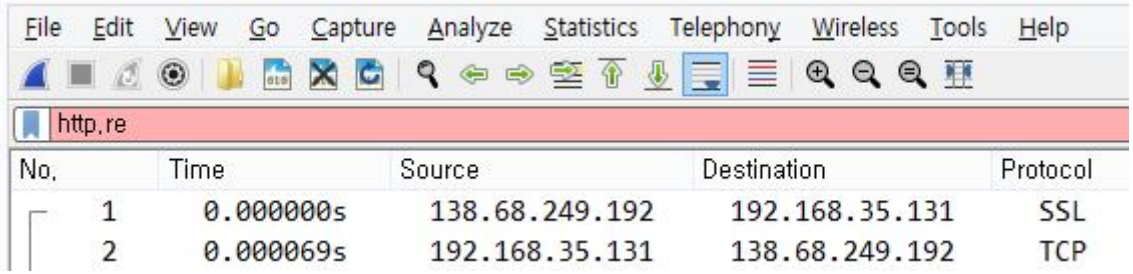
  ip

  ipv6

  tcp

적절한 디스플레이 필터 문법 사용

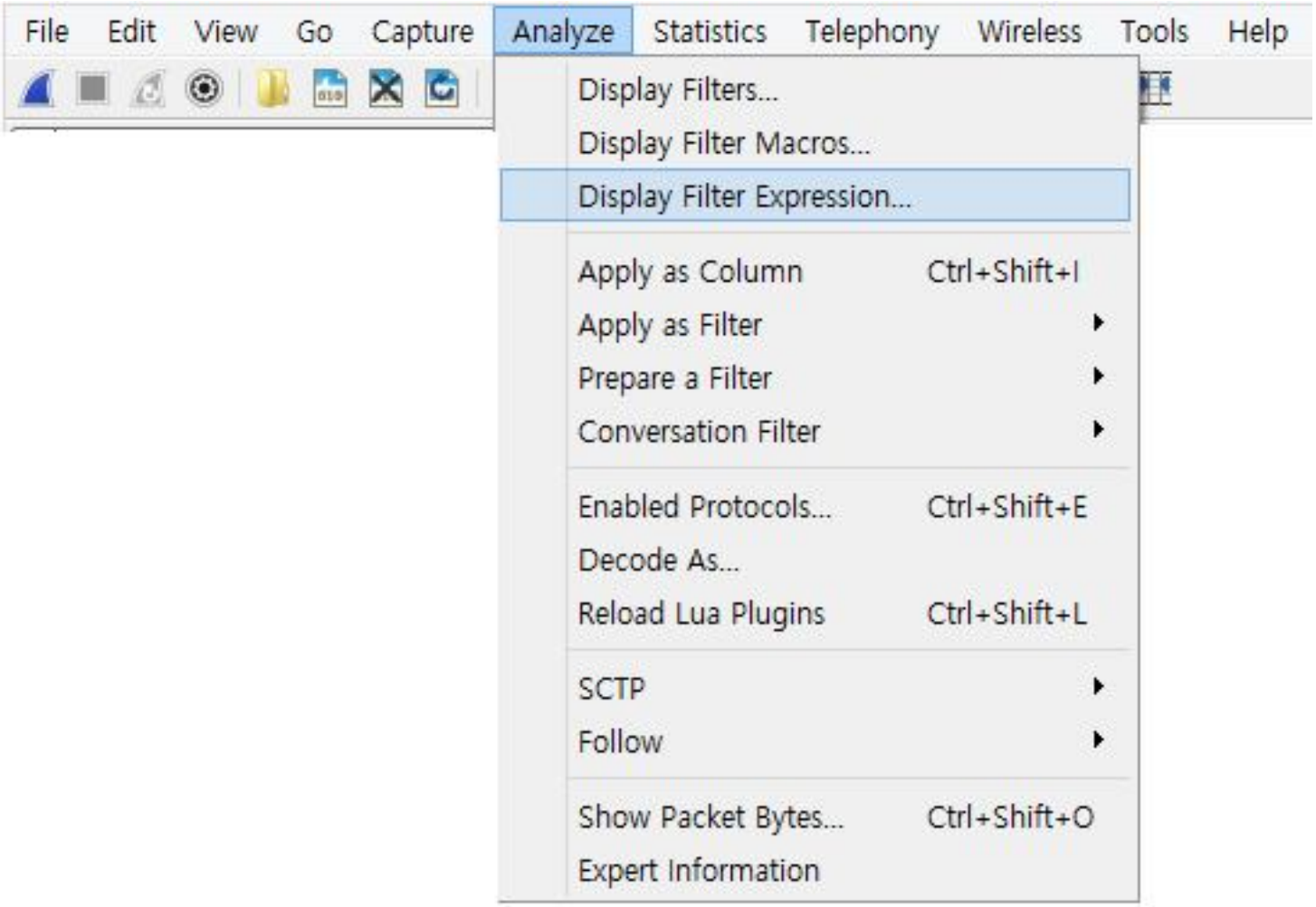
- **디스플레이 필터 오류 탐지 메커니즘**
  - 대소문자 구분
  - 적색 배경
    - 문법 검사 실패
    - 동작하지 않음
  - 녹색 배경
    - 문법 이상 없음
    - '논리 검사'는 하지 않음 (예) http && udp
  - 황색 배경
    - 필터가 원하는 대로 동작하지 않는 것을 경고 (예) ip.addr != 10.1.1.1



디스플레이필터와 연산자 비교

연산자	영어표기	예제
==	eq	ip.src == 10.2.2.2
!=	ne	tcp.srcport != 80
>	gt	frame.time_relative > 1
<	lt	tcp.window_size < 1460
>=	ge	dns.count.answers >=10
<=	lt	ip.ttl < 10
	contains	http contain “GET”

- 표현식을 사용한 디스플레이 필터 구축



캡처 필터 vs 디스플레이 필터

캡처 필터 구문 예제	디스플레이 필터 예제
host 172.16.1.1	ip.host == 172.16.1.1
src host 172.16.1.1	ip.src ==172.16.1.1
dst host 172.16.1.1	ip.dst ==172.16.1.1
port 8080	tcp.port == 8080
!port 8080	!tcp.port = 8080

❶ 단순 IP 주소 호스트에게/부터의 트래픽 필터링

- ip.addr == 10.3.1.1
- !ip.addr ==10.3.1.1
- ipv6.addr == 2406:da00:ff00::6b16:f02d
- ip.src==10.3.1.1
- ip.dst == 10.3.1.1
- ip.host == www.wireshark.org

❷ 주소 범위에게/부터의 트래픽 필터링

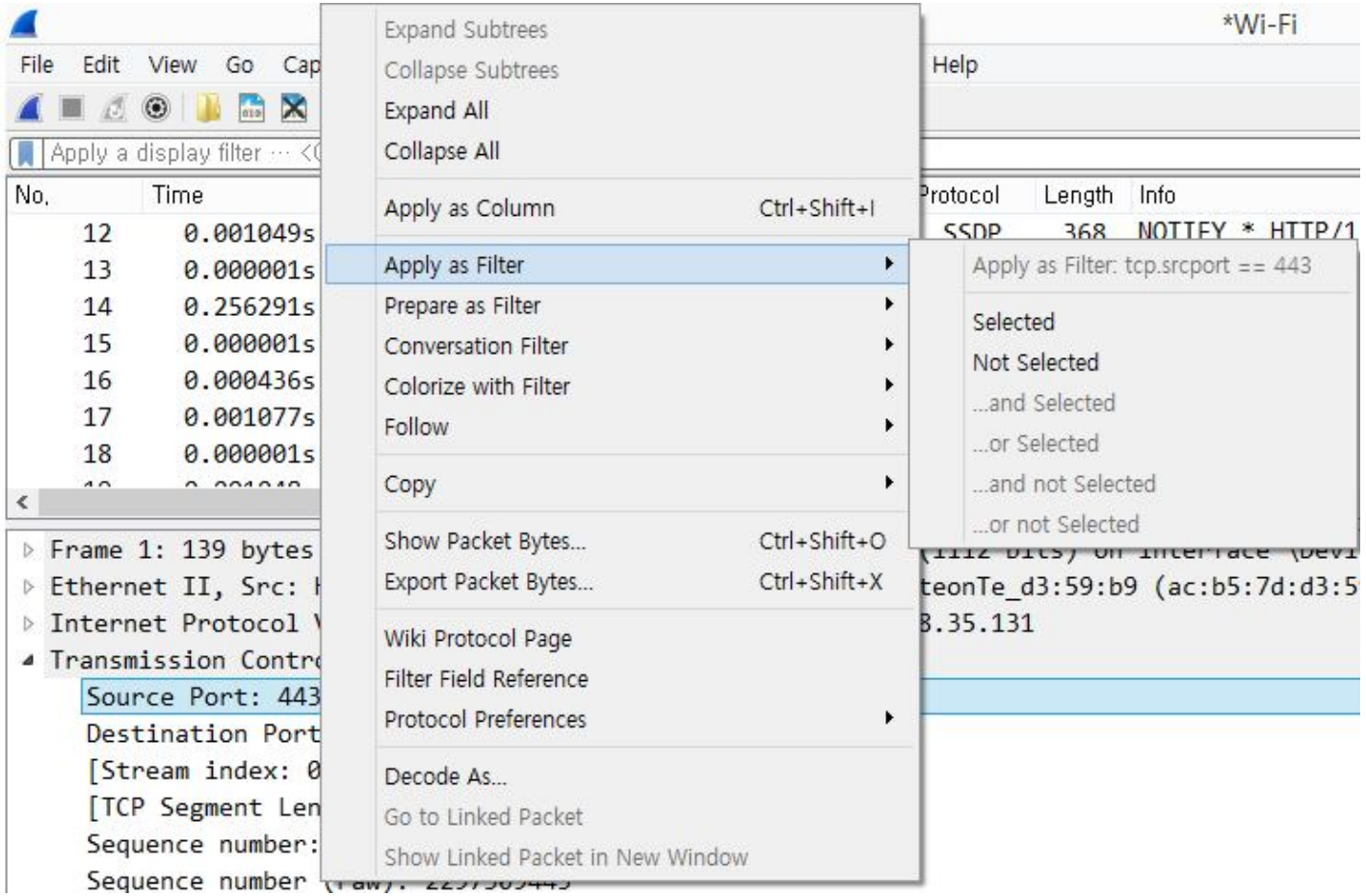
- ip.addr > 10.3.0.1 && ip.addr < 10.3.0.5
- (ip.addr >= 10.3.0.1 && ip.addr <= 10.3.0.6) && !ip.addr ==10.3.0.3
- ipv6.addr == fe80:: && ipv6.addr < fec0::

❸ IP 서브넷에서/으로부터 트래픽 필터링

- ip.addr == 10.3.0.0/16
- ip.addr == 10.3.0.0/16 && !ip.addr ==10.3.0.3
- !ip.addr == 10.3.0.0/16 && !ip.addr ==10.2.0.0/16

- Apply as Filter

- Prepare as Filter



Selected

A == B

Not Selected

!(A==B)

… and Selected

(A==B) && (C…)

... or Selected

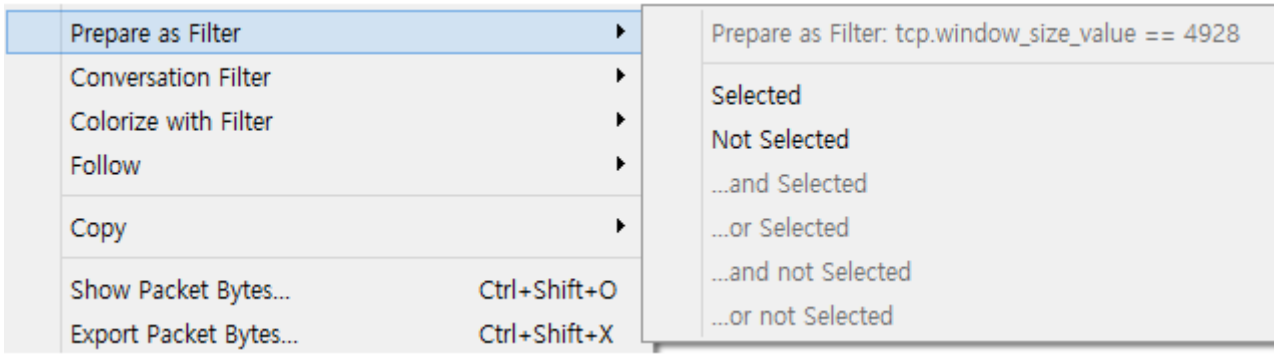
(A==B) || (C…)

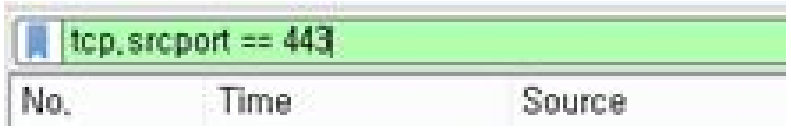
… and Not Selected

(A==B) && !(C…)

… or Not Selected

(A==B) || !(C…)





TCP/UDP Conversation Filter 방법

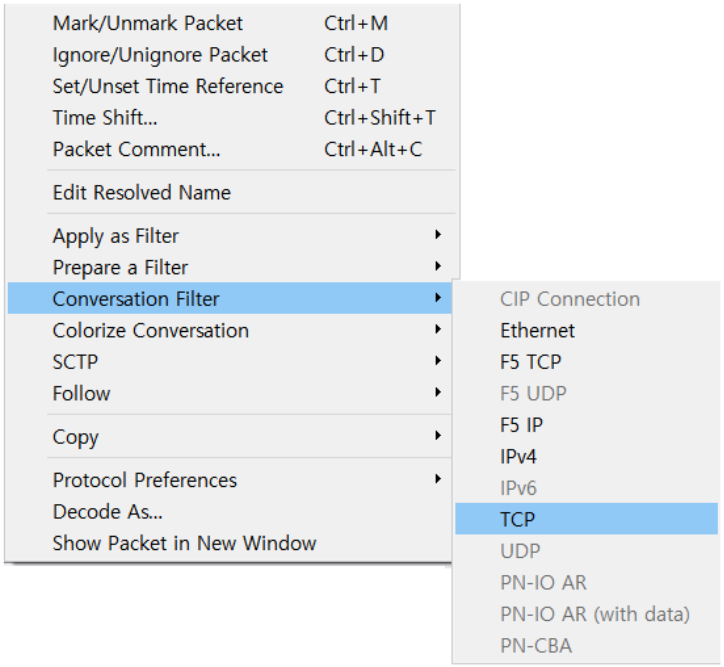
- 관심 있는 데이터를 빠르게 분석 가능
- 필터 방법 2가지

  - Conversation

  - Stream Follow

단일 TCP나 UDP 대화 필터링(Conversation Filtering)

❶ 패킷 리스트 > 패킷선택 > 오른쪽 마우스 클릭 > Conversation Filter > TCP



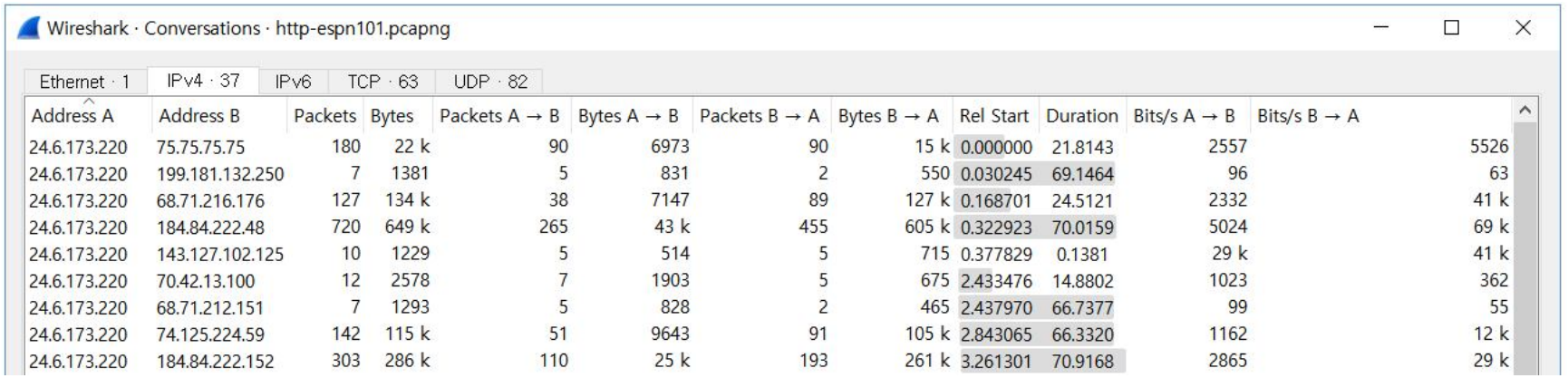
추적파일 : **http-espn101.pcapng**

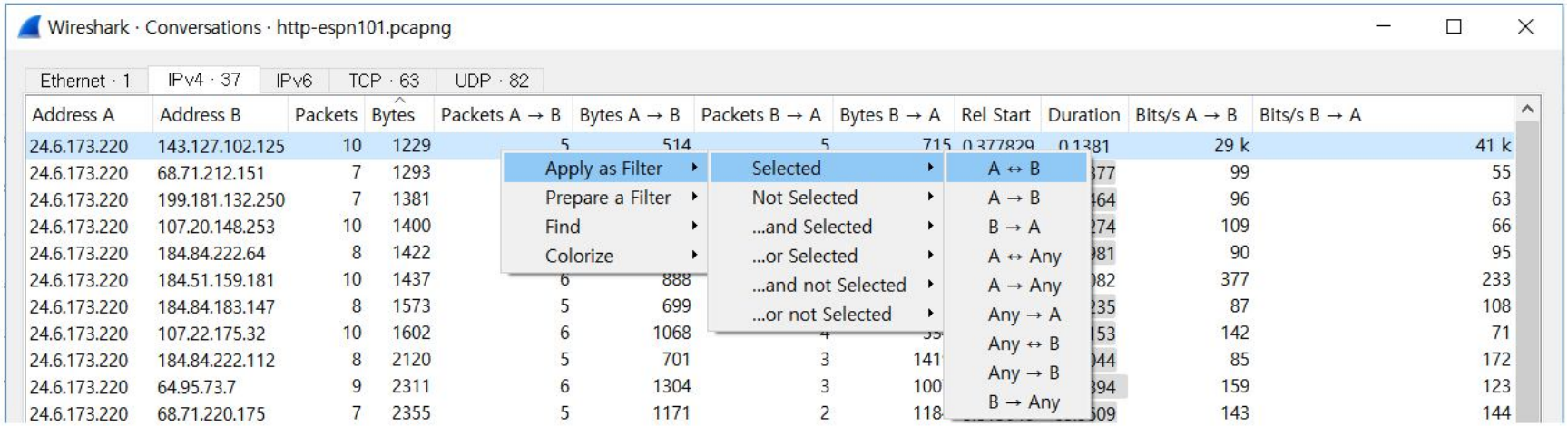
(ip.addr eq 24.6.173.220 and ip.addr eq 199.181.132.250) and (tcp.port eq 19941 and tcp.port eq 80)

No.	Time	Source	Destination	Protocol	Length	Info
5	0.000000	24.6.173.220	199.181.132.250	TCP	66	19941 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=
6	0.031335	199.181.132.250	24.6.173.220	TCP	66	80 → 19941 [SYN, ACK] Seq=0 Ack=1 Win=4380
7	0.000126	24.6.173.220	199.181.132.250	TCP	54	19941 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len
8	0.000665	24.6.173.220	199.181.132.250	HTTP	603	GET / HTTP/1.1
9	0.041099	199.181.132.250	24.6.173.220	HTTP	484	HTTP/1.1 301 Moved Permanently (text/html
31	0.199860	24.6.173.220	199.181.132.250	TCP	54	19941 → 80 [ACK] Seq=550 Ack=431 Win=65268
4891	68.873340	24.6.173.220	199.181.132.250	TCP	54	19941 → 80 [RST, ACK] Seq=550 Ack=431 Win=

❷ Statistics > Conversation Filter

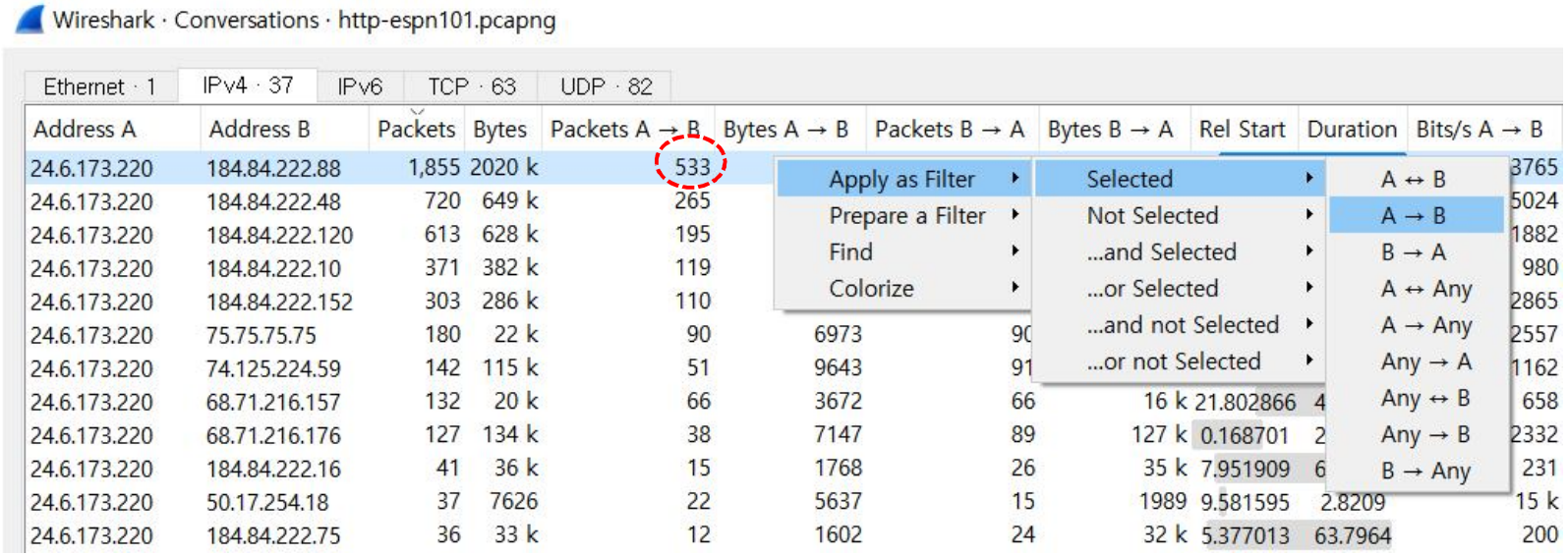
추적파일 : http-espn101.pcapng



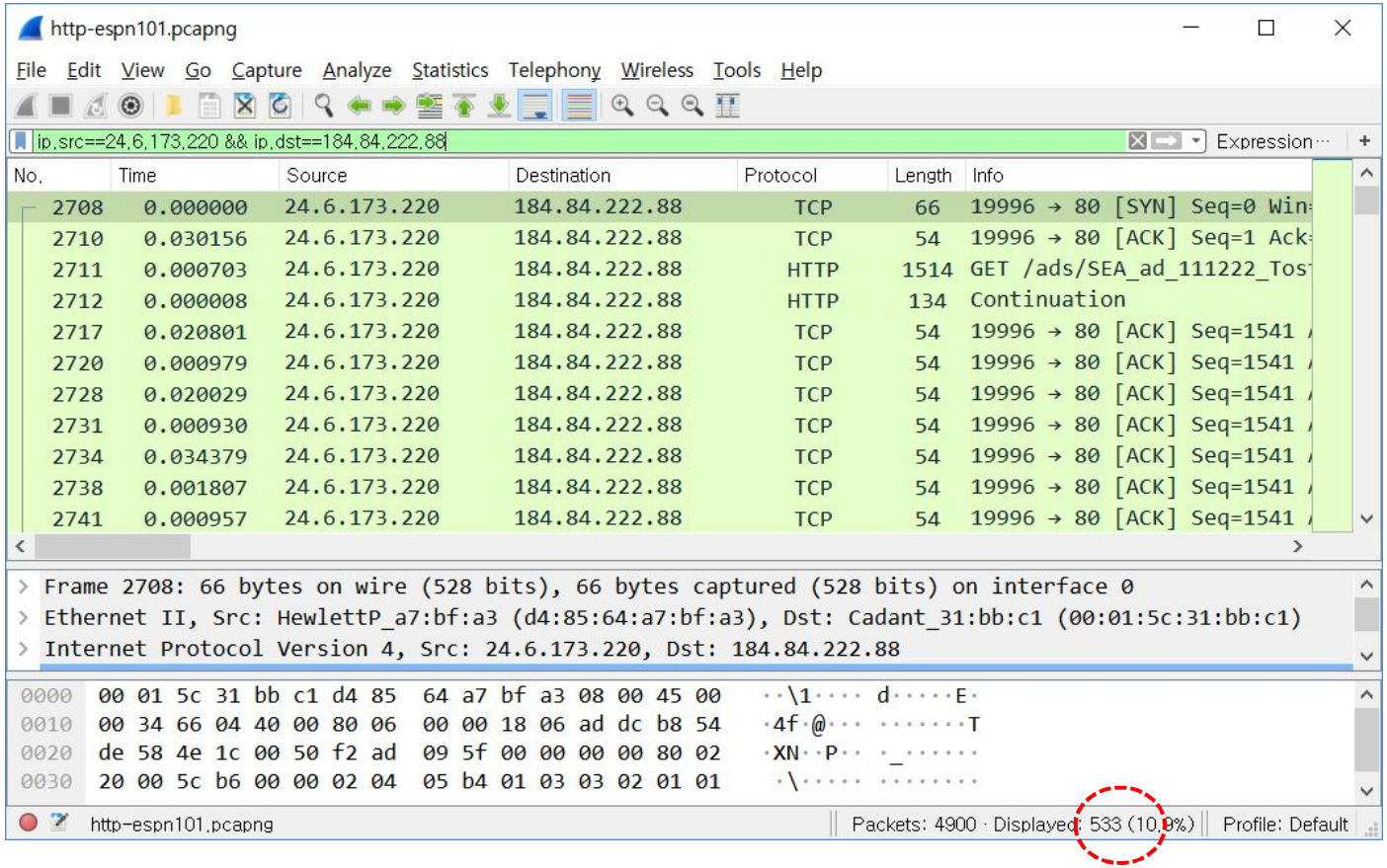


❷ Statistics > Conversation Filter

- Packets 필드를 기준으로 내림 차순으로 정렬
- 첫 번째 패킷 선택
- 오른쪽 마우스 클릭 > Apply as Filter > Selected > A→ B

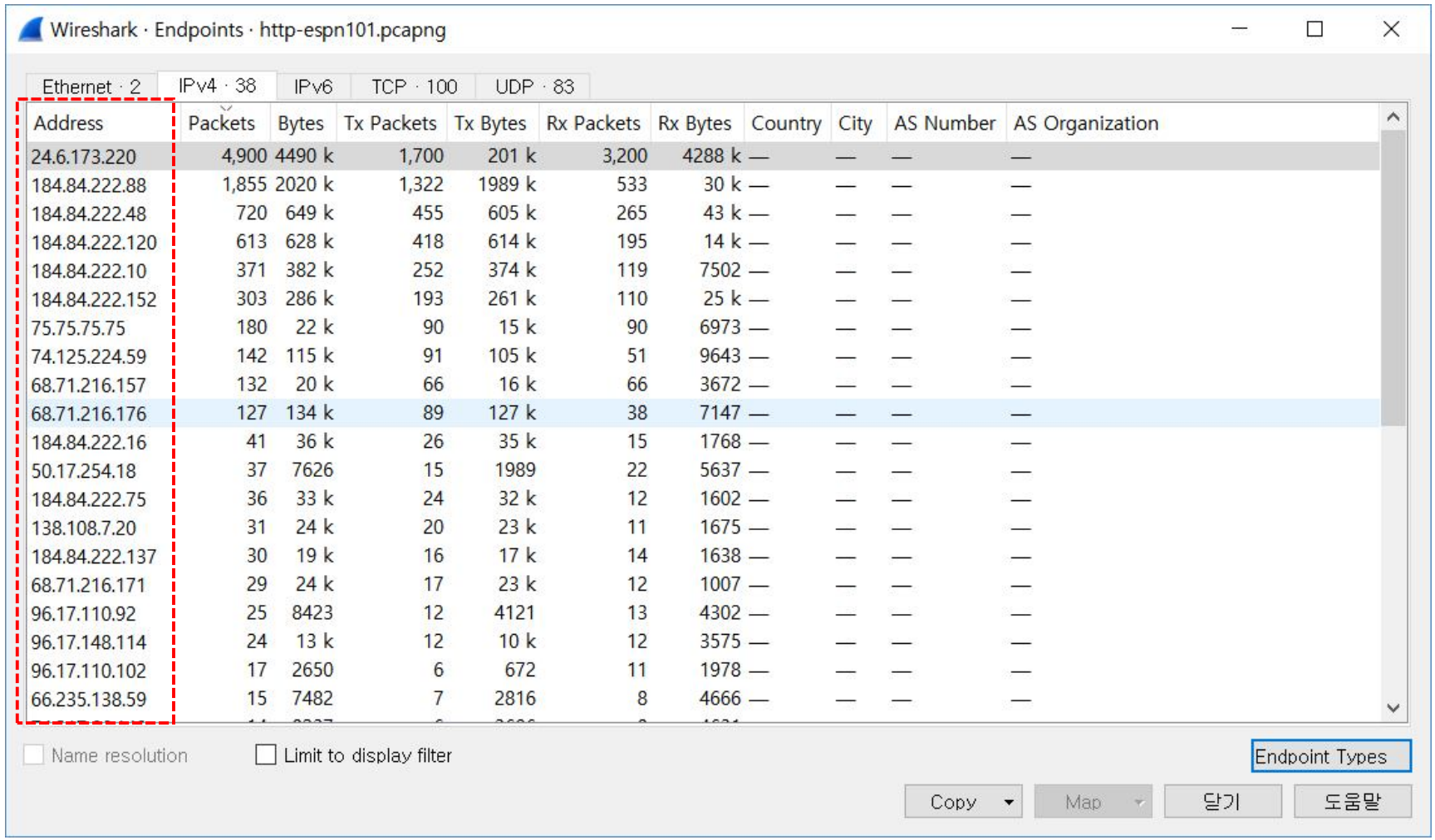


❷ Statistics > **Conversation Filter**



[참고] Endpoints

Statistics > Endpoints



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
24.6.173.220	4,900	4490 k	1,700	201 k	3,200	4288 k	—	—	—	—
184.84.222.88	1,855	2020 k	1,322	1989 k	533	30 k	—	—	—	—
184.84.222.48	720	649 k	455	605 k	265	43 k	—	—	—	—
184.84.222.120	613	628 k	418	614 k	195	14 k	—	—	—	—
184.84.222.10	371	382 k	252	374 k	119	7502	—	—	—	—
184.84.222.152	303	286 k	193	261 k	110	25 k	—	—	—	—
75.75.75.75	180	22 k	90	15 k	90	6973	—	—	—	—
74.125.224.59	142	115 k	91	105 k	51	9643	—	—	—	—
68.71.216.157	132	20 k	66	16 k	66	3672	—	—	—	—
68.71.216.176	127	134 k	89	127 k	38	7147	—	—	—	—
184.84.222.16	41	36 k	26	35 k	15	1768	—	—	—	—
50.17.254.18	37	7626	15	1989	22	5637	—	—	—	—
184.84.222.75	36	33 k	24	32 k	12	1602	—	—	—	—
138.108.7.20	31	24 k	20	23 k	11	1675	—	—	—	—
184.84.222.137	30	19 k	16	17 k	14	1638	—	—	—	—
68.71.216.171	29	24 k	17	23 k	12	1007	—	—	—	—
96.17.110.92	25	8423	12	4121	13	4302	—	—	—	—
96.17.148.114	24	13 k	12	10 k	12	3575	—	—	—	—
96.17.110.102	17	2650	6	672	11	1978	—	—	—	—
66.235.138.59	15	7482	7	2816	8	4666	—	—	—	—

3) 스트림 따라가기(Stream Follow)

- 여러 패킷의 데이터를 통합해 쉽게 읽을 수 있는 형식으로 재구성 (재조립)
- 4가지 유형의 스트림

  - TCP stream

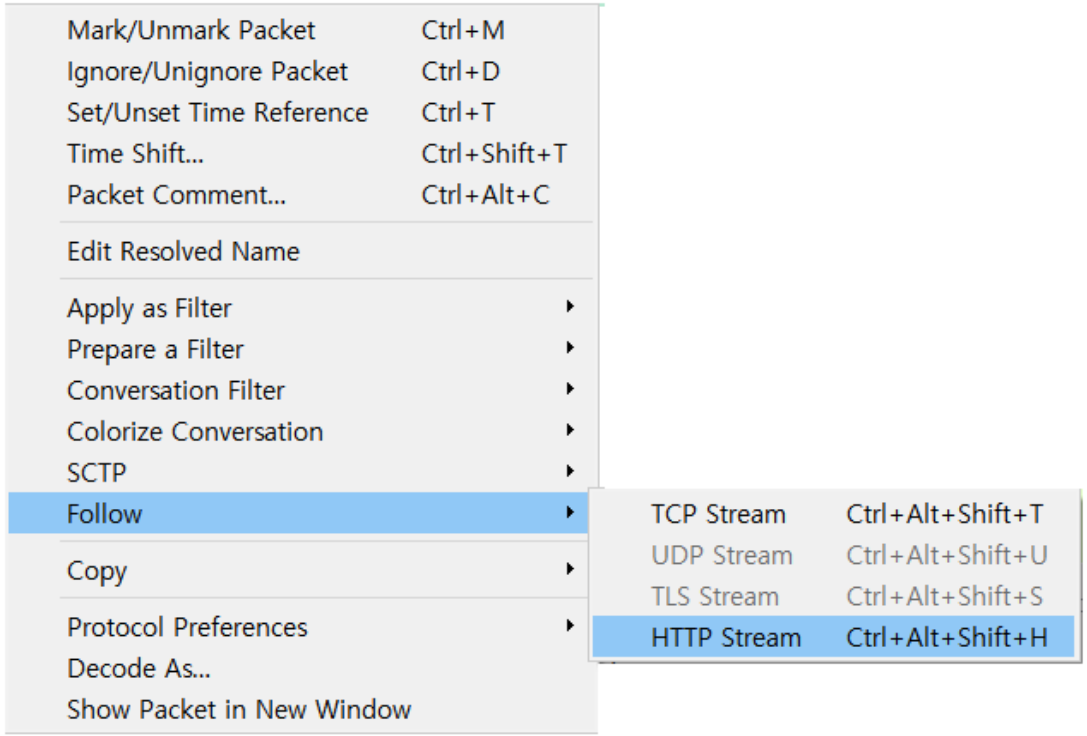
  - UDP Stream

  - SSL Stream

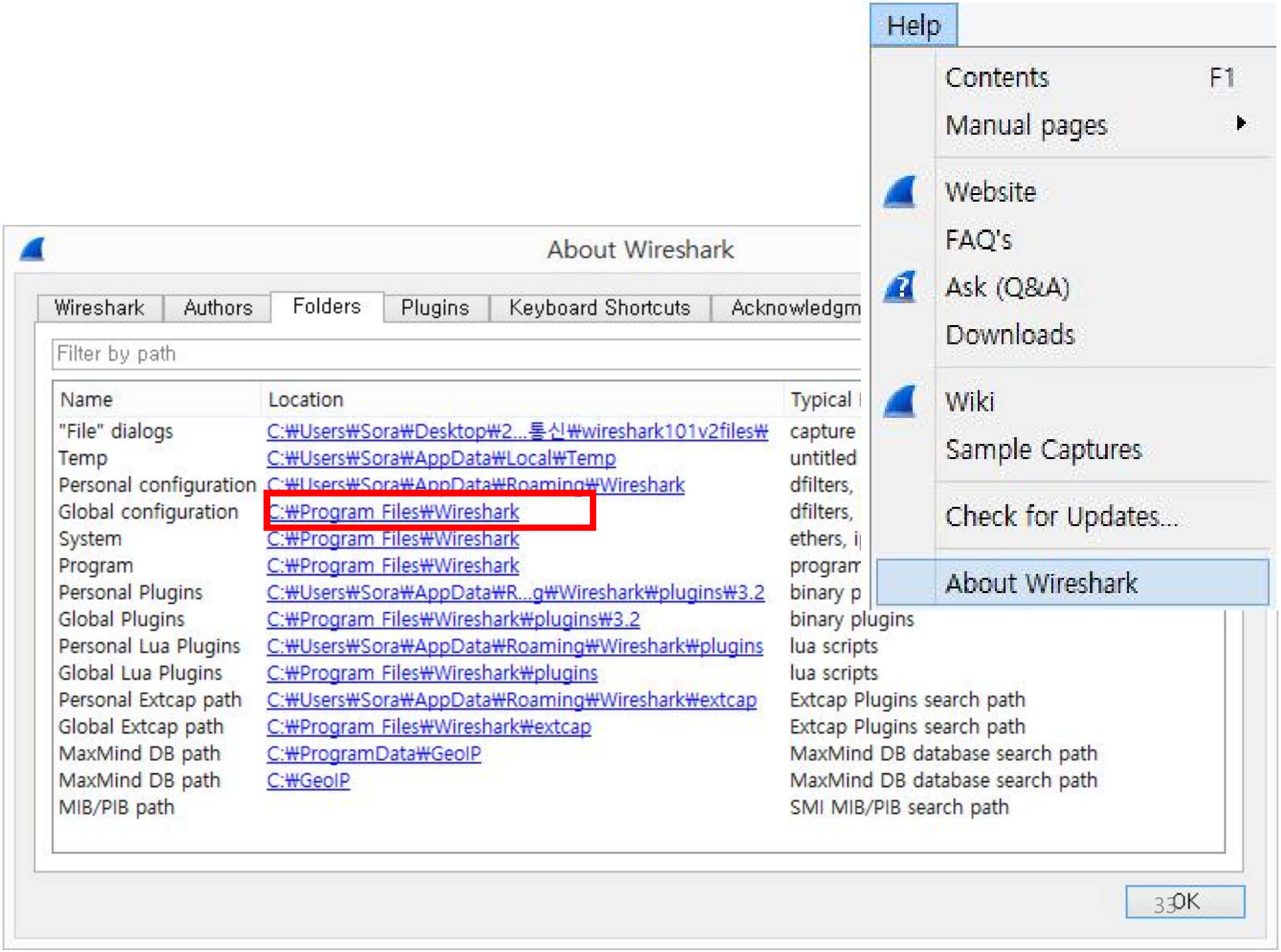
  - HTTP Stream

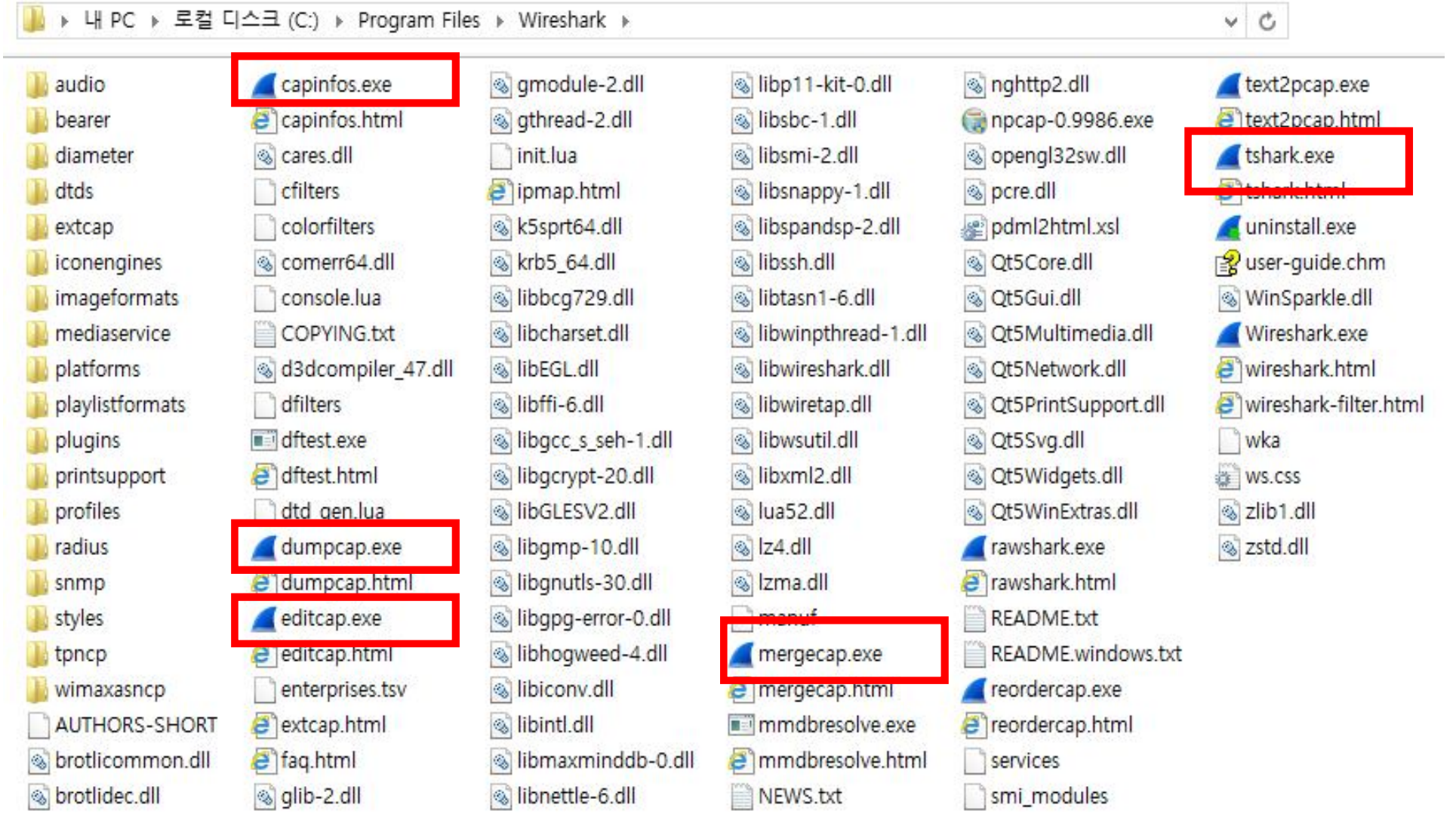
* 단일 TCP나 UDP 대화 필터링

TCP 또는 HTTP 패킷 선택 > 오른쪽 마우스 클릭 > Follow > HTTP Stream



	LINUX	MS-Window
패킷수집	TCPdump	TShark
패킷분석	Wireshark	


Help
Contents F1
Manual pages
Website
FAQ's
Ask (Q&A)
Downloads
Wiki
Sample Captures
Check for Updates...
About Wireshark
About Wireshark
Wireshark Authors Folders Plugins Keyboard Shortcuts Acknowledgm
Filter by path
Name Location Typical
"File" dialogs C:₩Users₩Sora₩Desktop₩2...통신₩wireshark101v2files₩ capture
Temp C:₩Users₩Sora₩AppData₩Local₩Temp untitled
Personal configuration C:₩Users₩Sora₩AppData₩Roaming₩Wireshark dfilters,
Global configuration C:₩Program Files₩Wireshark dfilters,
System C:₩Program Files₩Wireshark ethers, i
Program C:₩Program Files₩Wireshark program
Personal Plugins C:₩Users₩Sora₩AppData₩R...g₩Wireshark₩plugins₩3.2 binary p
Global Plugins C:₩Program Files₩Wireshark₩plugins₩3.2 binary plugins
Personal Lua Plugins C:₩Users₩Sora₩AppData₩Roaming₩Wireshark₩plugins lua scripts
Global Lua Plugins C:₩Program Files₩Wireshark₩plugins lua scripts
Personal Extcap path C:₩Users₩Sora₩AppData₩Roaming₩Wireshark₩extcap Extcap Plugins search path
Global Extcap path C:₩Program Files₩Wireshark₩extcap Extcap Plugins search path
MaxMind DB path C:₩ProgramData₩GeoIP MaxMind DB database search path
MaxMind DB path C:₩GeoIP MaxMind DB database search path
MIB/PIB path SMI MIB/PIB search path
OK


내 PC ▸ 로컬 디스크 (C:) ▸ Program Files ▸ Wireshark ▸
audio
bearer
diameter
dtds
extcap
iconengines
imageformats
mediaservice
platforms
playlistformats
plugins
printsupport
profiles
radius
snmp
styles
tpncp
wimaxasncp
AUTHORS-SHORT
brotlicommon.dll
brotlidec.dll
capinfos.exe
capinfos.html
cares.dll
cfilters
colorfilters
comerr64.dll
console.lua
COPYING.txt
d3dcompiler_47.dll
dfilters
dftest.exe
dftest.html
dtd_gen.lua
dumpcap.exe
dumpcap.html
editcap.exe
editcap.html
enterprises.tsv
extcap.html
faq.html
glib-2.dll
gmodule-2.dll
gthread-2.dll
init.lua
ipmap.html
k5sprt64.dll
krb5_64.dll
libbcg729.dll
libcharset.dll
libEGL.dll
libffi-6.dll
libgcc_s_seh-1.dll
libgcrypt-20.dll
libGLESV2.dll
libgmp-10.dll
libgnutls-30.dll
libgpg-error-0.dll
libhogweed-4.dll
libiconv.dll
libintl.dll
libmaxminddb-0.dll
libnettle-6.dll
libp11-kit-0.dll
libsbc-1.dll
libsmi-2.dll
libsnappy-1.dll
libspandsp-2.dll
libssh.dll
libtasn1-6.dll
libwinpthread-1.dll
libwireshark.dll
libwiretap.dll
libwsutil.dll
libxml2.dll
lua52.dll
lz4.dll
lzma.dll
manuf
mergecap.exe
mergecap.html
mmdbresolve.exe
mmdbresolve.html
NEWS.txt
nghttp2.dll
npcap-0.9986.exe
opengl32sw.dll
pcre.dll
pdml2html.xsl
Qt5Core.dll
Qt5Gui.dll
Qt5Multimedia.dll
Qt5Network.dll
Qt5PrintSupport.dll
Qt5Svg.dll
Qt5Widgets.dll
Qt5WinExtras.dll
rawshark.exe
rawshark.html
README.txt
README.windows.txt
reordercap.exe
reordercap.html
services
smi_modules
text2pcap.exe
text2pcap.html
tshark.exe
tshark.html
uninstall.exe
user-guide.chm
WinSparkle.dll
Wireshark.exe
wireshark.html
wireshark-filter.html
wka
ws.css
zlib1.dll
zstd.dll

커맨드라인에서 트래픽 수집

- dumpcap.exe나 tshark.exe를 이용해 커맨드 라인으로 트래픽 수집

  - Tshark를 구동하면 dumpcap.exe를 호출해서 수집 기능을 활용

```
C:₩Program Files₩Wireshark>dir dumpcap.exe

 C:₩Program Files₩Wireshark 디렉터리

2020-02-27  오전 05:47           420,416 dumpcap.exe
               1개 파일             420,416 바이트
               0개 디렉터리  86,740,180,992 바이트 남음

C:₩Program Files₩Wireshark>dir tshark.exe

 C:₩Program Files₩Wireshark 디렉터리

2020-02-27  오전 05:47           582,720 tshark.exe
               1개 파일             582,720 바이트
               0개 디렉터리  86,740,180,992 바이트 남음
```

❶ tshark –h

```
C:\Program Files\Wireshark>tshark -h
TShark (Wireshark) 3.0.3 (v3.0.3-0-g6130b92b0ec6)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: tshark [options] ...
```

❷ tshark –D

```
C:\Program Files\Wireshark>tshark -D
1.  \Device\NPF_{5256CF9B-1707-460C-B397-669CE852CFDE}
2.  \Device\NPF_{A378EED4-AC87-4168-8B22-DFDD0B9EC62E}
3.  \Device\NPF_{557124E1-28F6-4C2F-BDCE-1DFD75D011CE} (Wi-Fi)
4.  \Device\NPF_{630C09BF-1CAB-457F-978E-7A0BBEE76CF5}
5.  \Device\NPF_{E8E017EF-FC6D-4933-BD98-9AEC5CB26CF6}
6.  \Device\NPF_{27056470-1B11-4C61-8E92-0B25B7CB57C9}
7.  \Device\NPF_{DFBA2BCB-8989-40B4-873C-8CF862935F18}
8.  \Device\NPF_{6EC32DD5-41B3-45FF-B701-BB15DC1E7E45}
9.  \Device\NPF_{23E2556A-B636-483F-A13E-C3E889DD3825}
10.  \Device\NPF_{415D90F5-DFA5-426C-ABFE-BCCAB1542370}
```

❸ tshark –i 3

```
C:\Program Files\Wireshark>tshark -i 3
Capturing on 'Wi-Fi'
    1   0.000000 192.168.35.145 → 69.167.144.15 66 65160 64020 → https(443) [SYN] Seq=0 Win=65160 Len=0 MSS=1460 WS=256 SACK_PERM=1
    2   3.816065 192.168.35.145 → 121.53.202.218 66 65535 64021 → https(443) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
    3   3.816070 192.168.35.145 → 121.53.202.218 66 65535 64022 → https(443) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
    4   3.818776 121.53.202.218 → 192.168.35.145 66 8190 https(443) → 64022 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460 WS=16 SACK_PERM=1
    5   3.818895 192.168.35.145 → 121.53.202.218 54 1024 64022 → https(443) [ACK] Seq=1 Ack=1 Win=262144 Len=0
    6   3.819200 121.53.202.218 → 192.168.35.145 66 8190 https(443) → 64021 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460 WS=16 SACK_PERM=1
    7   3.819311 192.168.35.145 → 121.53.202.218 54 1024 64021 → https(443) [ACK] Seq=1 Ack=1 Win=262144 Len=0
    8   3.819713 192.168.35.145 → 121.53.202.218 295 1024 Client Hello
    9   3.819864 192.168.35.145 → 121.53.202.218 295 1024 Client Hello
```

* Ctrl+C 로 중단

❹ tshark –i 3 –w TST.pcapng

```
C:\Program Files\Wireshark>tshark -i 3 -w TST.pcapng
Capturing on 'Wi-Fi'
2472

C:\Program Files\Wireshark>
```

❺ tshark –r TST.pcapng

```
C:\Program Files\Wireshark>tshark -r TST.pcapng
    1   0.000000 192.168.35.145 → 69.167.144.15 74 65160 64159 → ht
    2   0.749769 192.168.35.145 → 104.74.232.184 54 256 64153 → htt
    3   0.752502 104.74.232.184 → 192.168.35.145 54 237 http(80) →
    4   0.752540 192.168.35.145 → 104.74.232.184 54 256 64153 → htt
    5   1.055385 192.168.35.145 → 110.76.141.124 66 64240 64160 → h
    6   1.058892 110.76.141.124 → 192.168.35.145 66 29200 https(443)
    7   1.058938 192.168.35.145 → 110.76.141.124 54 256 64160 → htt
    8   1.059047 192.168.35.145 → 110.76.141.124 256 256 Client Hell
```

❻ tshark –i 3 –a files:3 –b duration:10 –w myshark.pcapng

```
C:\Program Files\Wireshark>tshark -i 3 -a files:3 -b duration:10 -w myshark.pcapng
Capturing on 'Wi-Fi'
4464

C:\Program Files\Wireshark>dir myshark*
 C 드라이브의 볼륨에는 이름이 없습니다.
 볼륨 일련 번호: BCF8-FA59

 C:\Program Files\Wireshark 디렉터리

2018-08-12  오전 12:46           679,312 myshark_00001_20190801004608.pcapng
2018-08-12  오전 12:46         1,269,276 myshark_00002_20190801004618.pcapng
2018-08-12  오전 12:46           937,040 myshark_00003_20190801004629.pcapng
               3개 파일           2,885,628 바이트
               0개 디렉터리  126,970,032,128 바이트 남음
```

-a file:3 3개 파일 수집 후 자동 정지

-b duration:10 10초후에 다음 파일을 생성

-w myshark.pcapng 추적파일명

커맨드라인 수집 과정에서 수집 필터(캡처필터)

❶ **tshark –i 3 –f "tcp port 443" –w mysecport443.pcapng**

```
C:\Program Files\Wireshark>tshark -i 3 -f "tcp port 443" -w mysecport443.pcapng
Capturing on 'Wi-Fi'
2734

C:\Program Files\Wireshark>tshark -r mysecport443.pcapng
    1   0.000000 192.168.35.145 → 69.167.144.15 74 65160 64805 → https(443) [SYN] Seq=0 W
    2   3.010265 192.168.35.145 → 69.167.144.15 74 65160 [TCP Retransmission] 64805 → htt
    3   3.627403 192.168.35.145 → 52.175.23.79 66 64240 64806 → https(443) [SYN] Seq=0 Wi
    4   3.710985 52.175.23.79 → 192.168.35.145 66 8192 https(443) → 64806 [SYN, ACK] Seq=
    5   3.711076 192.168.35.145 → 52.175.23.79 54 258 64806 → https(443) [ACK] Seq=1 Ack=
    6   3.711563 192.168.35.145 → 52.175.23.79 274 258 Client Hello
    7   3.792328 52.175.23.79 → 192.168.35.145 1514 1026 [TCP segment of a reassembled PDU
    8   3.792330 52.175.23.79 → 192.168.35.145 1514 1026 https(443) → 64806 [ACK] Seq=146
    9   3.792335 52.175.23.79 → 192.168.35.145 538 1026 Server Hello, Certificate, Server
```

❷ **tshark –i 3 –f "tcp port 443 and host 192.168.1.1" –w my443.pcapng**

커맨드라인 수집 과정에서 디스플레이 필터

❶ **tshark –r "mysecport443.pcapng" –Y "tcp.analysis.flags"**

```
C:\Program Files\Wireshark>tshark -r "mysecport443.pcapng" -Y "tcp.analysis.flags"
    2    3.010265 192.168.35.145 → 69.167.144.15 74 65160 [TCP Retransmission] 64805 → https(443)
 1113    9.019700 192.168.35.145 → 69.167.144.15 66 65160 [TCP Retransmission] 64805 → https(443)
 2734   24.038230 192.168.35.145 → 69.167.144.15 74 65160 [TCP Retransmission] 64898 → https(443)
```

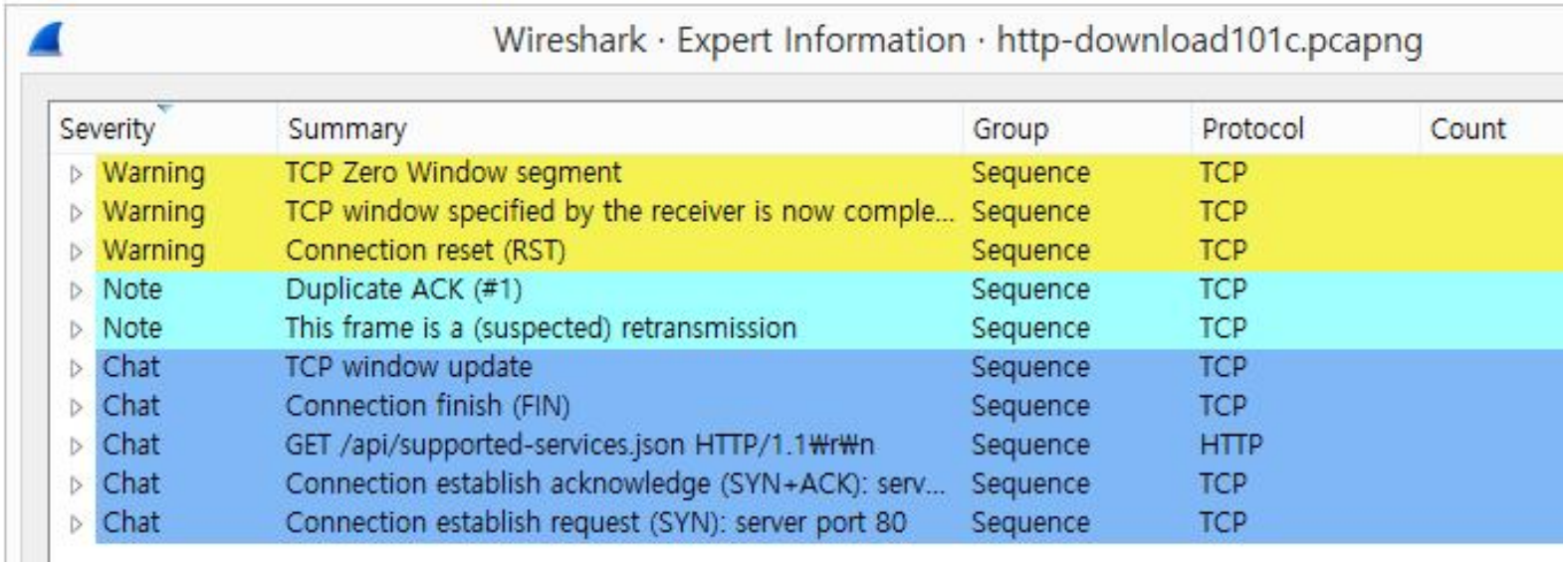
❷ **tshark –r "mysecport443.pcapng" –Y "tcp.analysis.flags" –w tcpflag.pcapng**

❸ **tshark –r "mysecport443.pcapng" –Y "http.request.method == GET"**

❹ tshark –i 3 –qz hosts

접속한 호스트 목록 확인

```
C:₩Program Files₩Wireshark>tshark -i3 -qz hosts
Capturing on 'Wi-Fi'
5681 packets captured
# TShark hosts output
#
# Host data gathered from the temporary capture file

125.209.222.142 www.naver.com.nheos.com
125.209.254.155 s1.e.navercdn.com
43.250.152.43   s2.e.navercdn.com
210.89.172.40   kr-lcs.naver.com.akadns.net
125.209.210.116 kr-cc.naver.com.akadns.net
13.107.21.200   dual-a-0001.a-msedge.net
125.209.254.162 s1.e.navercdn.com
168.63.154.101  wd-prod-ss-as-east-2-fe.eastasia.cloudapp.azure.com
125.209.230.195 l.www.naver.com
43.250.152.50   s2.e.navercdn.com
```



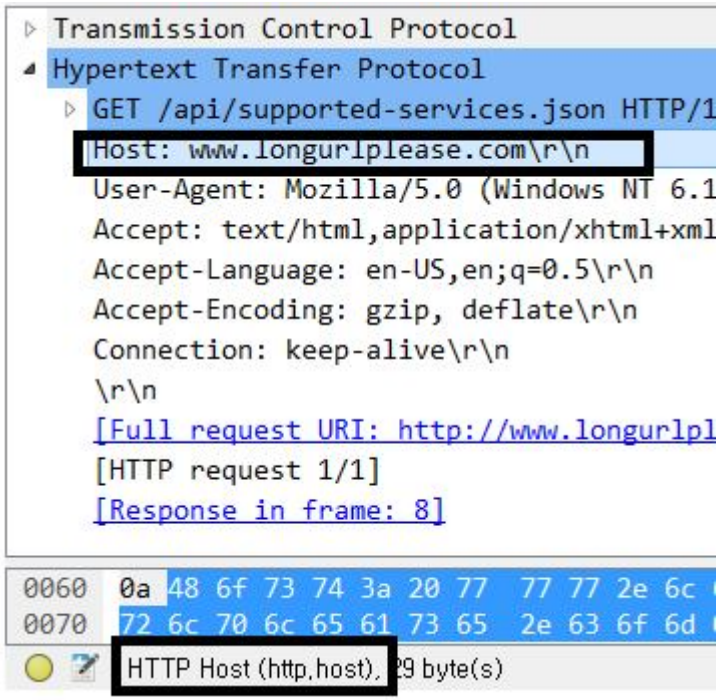
Severity	Summary	Group	Protocol	Count
Warning	TCP Zero Window segment	Sequence	TCP	
Warning	TCP window specified by the receiver is now comple...	Sequence	TCP	
Warning	Connection reset (RST)	Sequence	TCP	
Note	Duplicate ACK (#1)	Sequence	TCP	
Note	This frame is a (suspected) retransmission	Sequence	TCP	
Chat	TCP window update	Sequence	TCP	
Chat	Connection finish (FIN)	Sequence	TCP	
Chat	GET /api/supported-services.json HTTP/1.1₩r₩n	Sequence	HTTP	
Chat	Connection establish acknowledge (SYN+ACK): serv...	Sequence	TCP	
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	

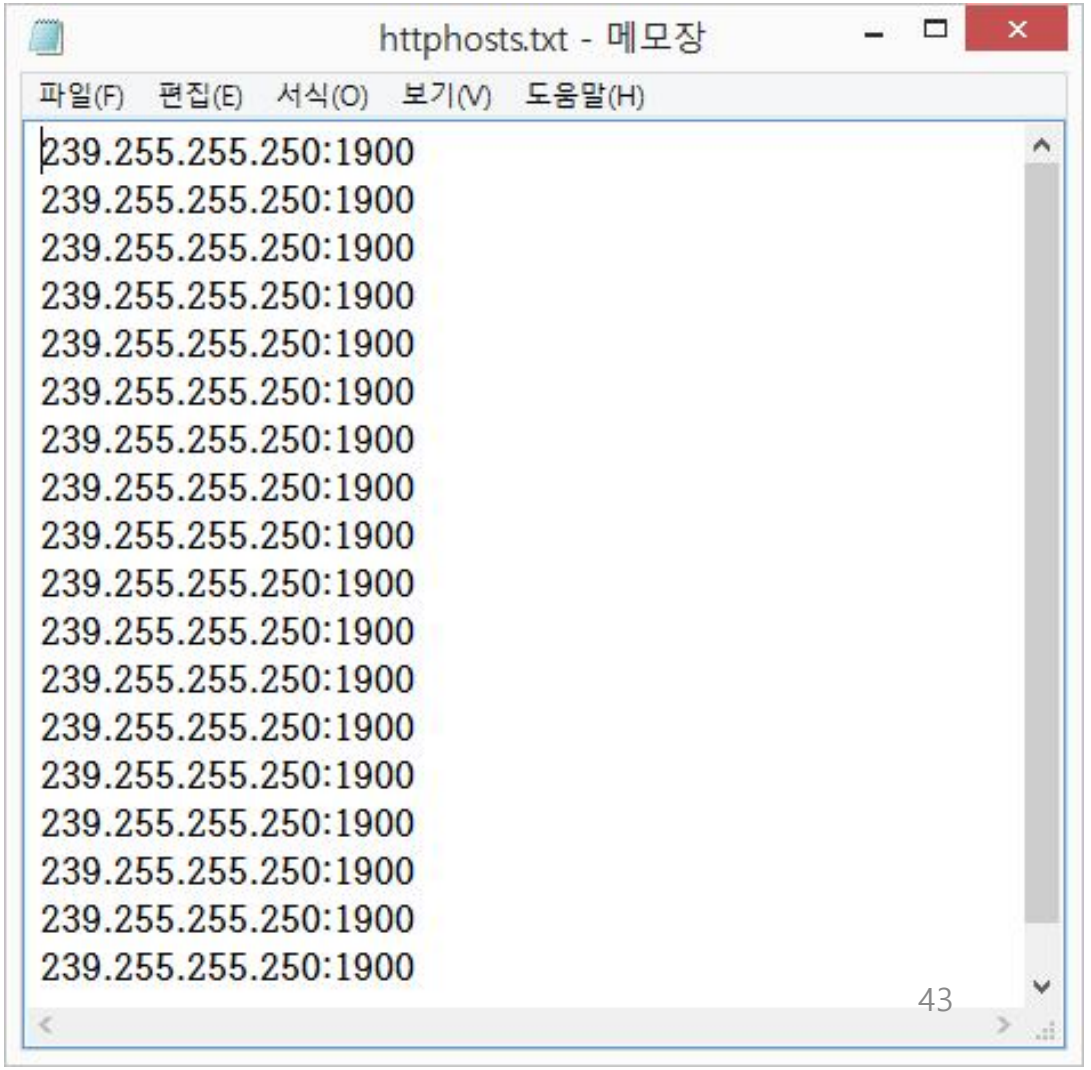
❺ tshark –r “http-download101c.pcapng” –qz expert,warns

```
C:\Program Files\Wireshark>tshark -r "mysecport443.pcapng" -qz expert.warns

Warns (30)
==========
   Frequency      Group          Protocol  Summary
          30   Sequence               TCP  Connection reset (RST)

Notes (35)
==========
   Frequency      Group          Protocol  Summary
           3   Sequence               TCP  This frame is a (suspected) retransmission
          32   Sequence               TLS  This session reuses previously negotiated keys (Session resumption)

Chats (271)
==========
   Frequency      Group          Protocol  Summary
          96   Sequence               TCP  Connection establish request (SYN): server port 443
          91   Sequence               TCP  Connection establish acknowledge (SYN+ACK): server port 443
          84   Sequence               TCP  Connection finish (FIN)
```

❻ tshark -i 3 –Y “http.host” –T fields –e http.host > httphosts.txt

실시간으로 관찰된 특정 필드 값을 텍스트 파일로 저장





❹ tshark –i 3 –qz hosts