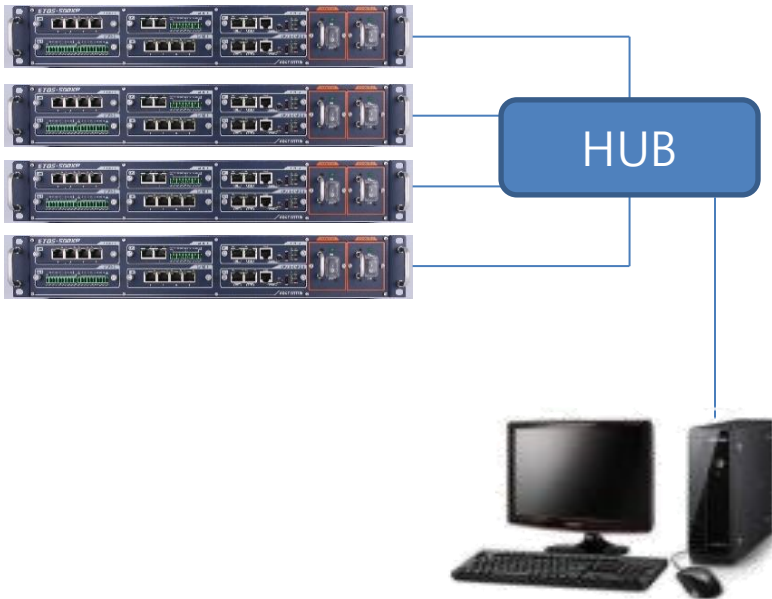


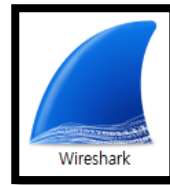
패킷 모니터링을 위한 PC 연결

Advanced Communication & Technology System

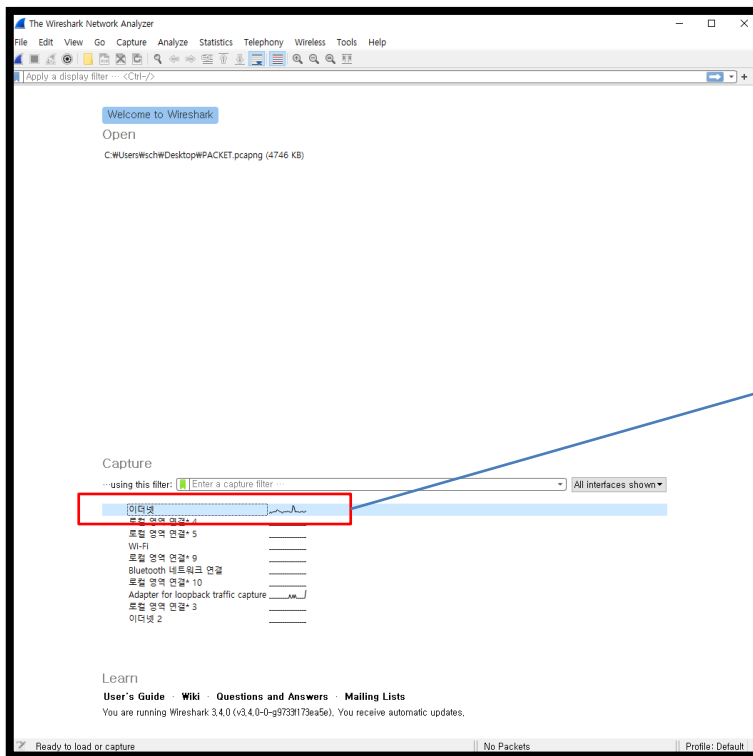
ETOS-500XP



왼쪽 구성과 같이 ETOS가 연결 되어있는 네트워크단에 PC를 연결하여 패킷 모니터링을 해야 하나 현장 여건이 불가 하다면 연결이 가능한 위치에서 진행 하시기 바랍니다.



Wireshark 프로그램을 설치 후 실행 합니다.

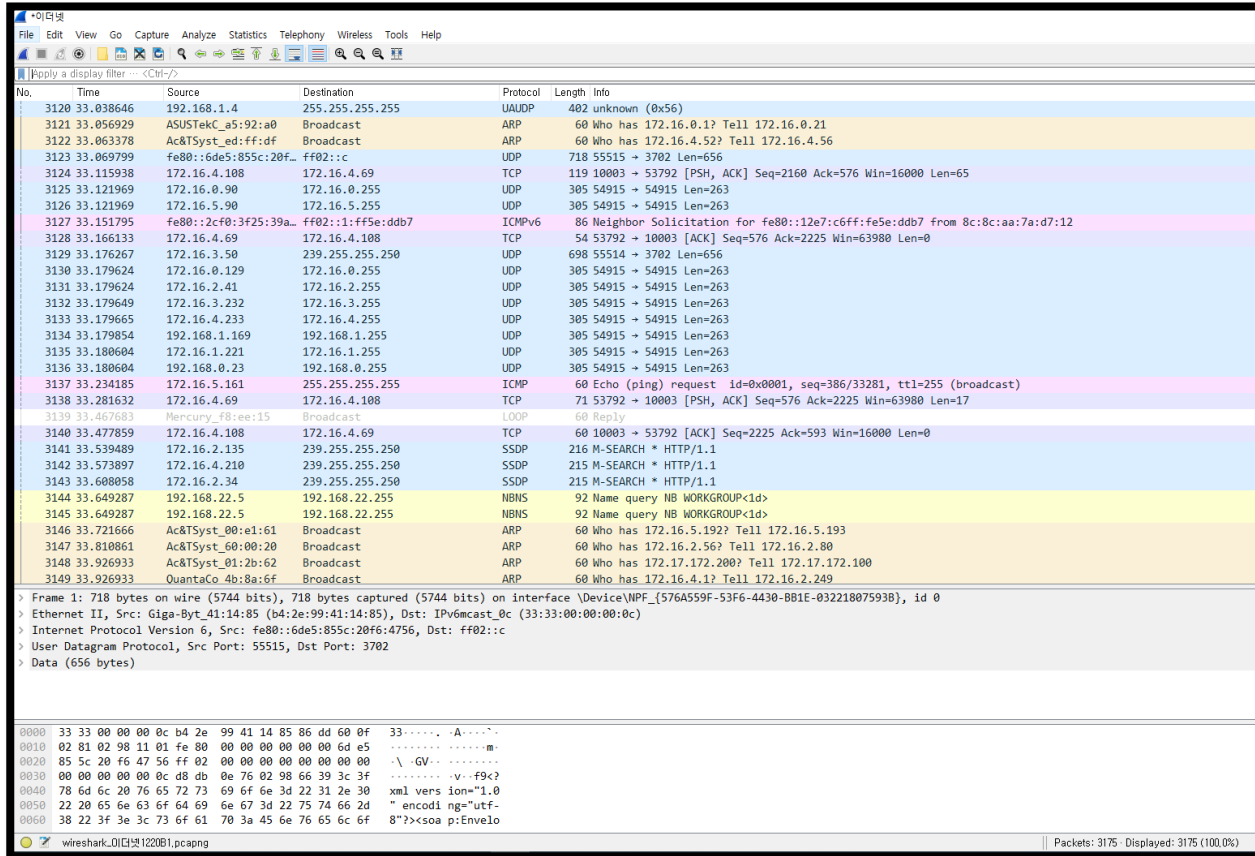


처음 화면에서 이더넷 또는 랜카드 항목 우측에 그래프가 진행되는 항목을 더블클릭 합니다.

이더넷

Wireshark 사용 방법

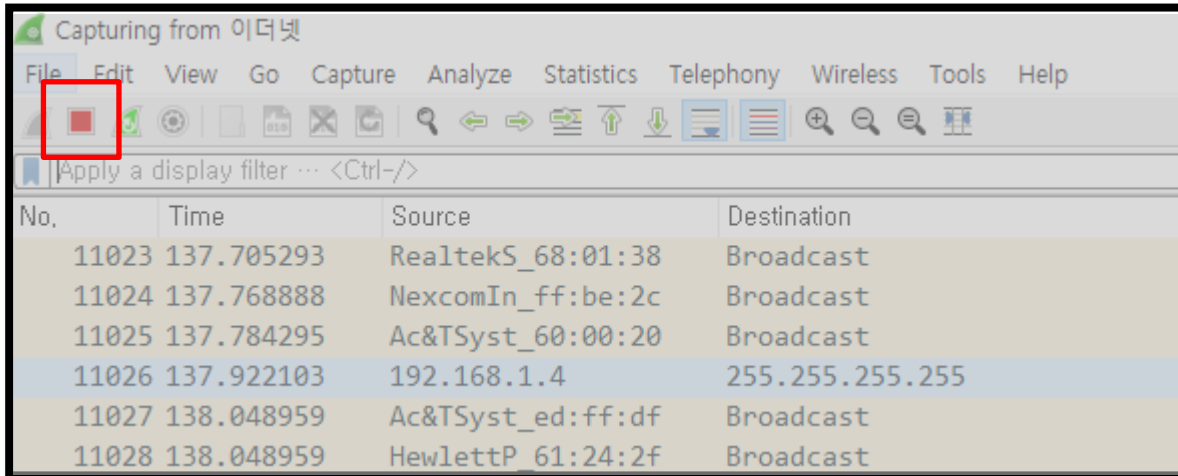
Advanced Communication & Technology System



그림과 같이 네트워크 패킷이 모니터링 됩니다.
1~2분정도 진행 상황을 모니터링 합니다.

Wireshark 사용 방법

Advanced Communication & Technology System



정지 버튼을 클릭합니다.

Wireshark 사용 방법

Advanced Communication & Technology System

PACKET.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
19491	260.136434	172.16.2.157	172.16.2.255	UDP	82	58242 → 1947 Len=40
19492	260.148055	172.16.4.69	172.16.4.108	TCP	54	53792 → 10003 [ACK] Seq=4449 Ack=16
19493	260.214633	172.16.3.36	172.16.3.255	UDP	170	65521 → 50007 Len=128
19494	260.246464	Netgear_e8:59:4b	Broadcast	0x8899	60	Realtek Layer 2 Protocols
19495	260.250372	172.16.0.129	172.16.0.255	UDP	305	54915 → 54915 Len=263
19496	260.250372	172.16.2.41	172.16.2.255	UDP	305	54915 → 54915 Len=263
19497	260.250403	172.16.4.233	172.16.4.255	UDP	305	54915 → 54915 Len=263
19498	260.250406	172.16.1.221	172.16.1.255	UDP	305	54915 → 54915 Len=263
19499	260.250406	192.168.0.23	192.168.0.255	UDP	305	54915 → 54915 Len=263
19500	260.250878	172.16.3.232	172.16.3.255	UDP	305	54915 → 54915 Len=263
19501	260.250878	192.168.1.169	192.168.1.255	UDP	305	54915 → 54915 Len=263
19502	260.365418	LSLGIndu_73:10:5d	Broadcast	ARP	64	Who has 172.16.0.1? Tell 172.16.0.7
19503	260.365418	LGElectr_f9:2c:93	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.6
19504	260.365418	IntelCor_2c:1a:eb	Broadcast	ARP	60	Who has 30.30.30.1? Tell 30.30.30.2
19505	260.404444	172.16.4.69	172.16.4.108	TCP	71	53792 → 10003 [PSH, ACK] Seq=4449 A
19506	260.496029	172.16.5.130	172.16.5.255	NBNS	92	Name query NB WORKGROUP<1b>
19507	260.496949	192.168.22.5	192.168.22.255	BROWSER	225	Browser Election Request
19508	260.604098	172.16.4.108	172.16.4.69	TCP	60	10003 → 53792 [ACK] Seq=16994 Ack=4
19509	260.622855	Ac&TSyst_01:2b:62	Broadcast	ARP	60	Who has 172.17.172.200? Tell 172.17
19510	260.625754	fe80::2cf0:3f25:39a...	ff02::1:ff5e:ddb7	ICMPv6	86	Neighbor Solicitation for fe80::12e
19511	260.658533	172.16.3.40	172.16.3.255	UDP	608	55023 → 3703 Len=656

> Frame 19503: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{576A559F-53F6-4430-BB1E-032} ...

Ethernet II, Src: LGElectr_f9:2c:93 (14:c9:13:f9:2c:93), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

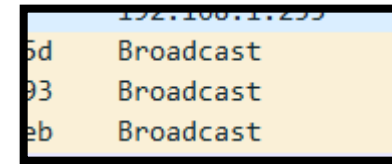
Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Address: Broadcast (ff:ff:ff:ff:ff:ff)

....1. = LG bit: Locally administered address (this is NOT the factory default)

0000 ff ff ff ff ff ff 14 c9 13 f9 2c 93 08 06 00 01
0010 08 00 06 04 00 01 14 c9 13 f9 2c 93 ac 10 00 44D
0020 00 00 00 00 00 00 ac 10 00 01 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00

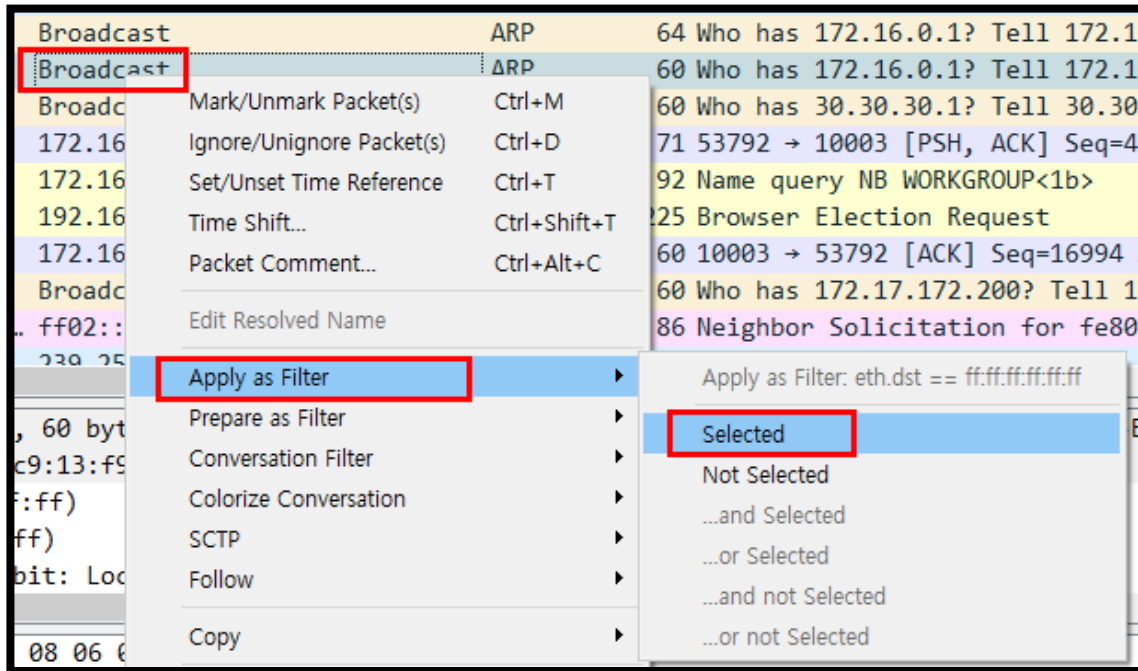
Source or Destination Hardware Address (eth.addr), 6 byte(s) | Packets: 19519 · Displayed: 19519 (100.0%) · Dropped: 0 (0.0%) | Profile: Default



Destination 항목에 Broadcast 항목을
우클릭 합니다.

Wireshark 사용 방법

Advanced Communication & Technology System



그림의 경로를 따라 Selected를 선택 합니다.

Wireshark 사용 방법

Advanced Communication & Technology System

The image shows the Wireshark interface with a packet capture file named 'PACKET.pcapng'. The packet list on the left shows various ARP and UDP packets. The packet details pane on the right shows the structure of a selected packet (Frame 19503), including Ethernet II, Destination, and Address fields. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. A status bar at the bottom indicates 'Packets: 19519 · Displayed: 6989 (35,8%) · Dropped: 0 (0,0%)'.

No.	Time	Source	Destination	Protocol	Length	Info
19479	259.940032	Ac&TSyst_00:aa:05	Broadcast	ARP	60	Who has 192.168.99.107? Tell 192.168.99.107
19480	259.940032	8c:8c:aa:7a:d7:12	Broadcast	ARP	60	Who has 172.16.5.1? Tell 172.16.5.1
19481	259.940032	8c:8c:aa:7a:d7:12	Broadcast	ARP	60	Who has 172.20.120.1? Tell 172.16.5.1
19482	260.051713	Ac&TSyst_ed:ff:df	Broadcast	ARP	60	Who has 172.16.4.52? Tell 172.16.4.52
19483	260.094222	172.16.0.90	172.16.0.255	UDP	305	54915 → 54915 Len=263
19484	260.094371	172.16.5.90	172.16.5.255	UDP	305	54915 → 54915 Len=263
19485	260.105841	172.16.2.157	172.16.2.255	UDP	82	58239 → 1947 Len=40
19487	260.105841	172.16.2.157	255.255.255.255	UDP	82	58241 → 1947 Len=40
19490	260.136386	172.16.2.157	255.255.255.255	UDP	82	58244 → 1947 Len=40
19491	260.136434	172.16.2.157	172.16.2.255	UDP	82	58242 → 1947 Len=40
19493	260.214633	172.16.3.36	172.16.3.255	UDP	170	65521 → 50007 Len=128
19494	260.246464	Netgear_e8:59:4b	Broadcast	0x8899	60	Realtek Layer 2 Protocols
19495	260.250372	172.16.0.129	172.16.0.255	UDP	305	54915 → 54915 Len=263
19496	260.250372	172.16.2.41	172.16.2.255	UDP	305	54915 → 54915 Len=263
19497	260.250403	172.16.4.233	172.16.4.255	UDP	305	54915 → 54915 Len=263
19498	260.250406	172.16.1.221	172.16.1.255	UDP	305	54915 → 54915 Len=263
19499	260.250406	192.168.0.23	192.168.0.255	UDP	305	54915 → 54915 Len=263
19500	260.250878	172.16.3.232	172.16.3.255	UDP	305	54915 → 54915 Len=263
19501	260.250878	192.168.1.169	192.168.1.255	UDP	305	54915 → 54915 Len=263
19502	260.365418	LSLGIndu_73:10:5d	Broadcast	ARP	64	Who has 172.16.0.1? Tell 172.16.0.1
19503	260.365418	LGElectr_f9:2c:93	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.1

Frame 19503: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{576A559F-53F6-4430-BB1E-032}^

Ethernet II, Src: LGElectr_f9:2c:93 (14:c9:13:f9:2c:93), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Address: Broadcast (ff:ff:ff:ff:ff:ff)

.....1. = LG bit: Locally administered address (this is NOT the factory default)

0000 ff ff ff ff ff ff 14 c9 13 f9 2c 93 08 06 00 01
0010 08 00 06 04 00 01 14 c9 13 f9 2c 93 ac 10 00 44
0020 00 00 00 00 00 00 ac 10 00 01 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00

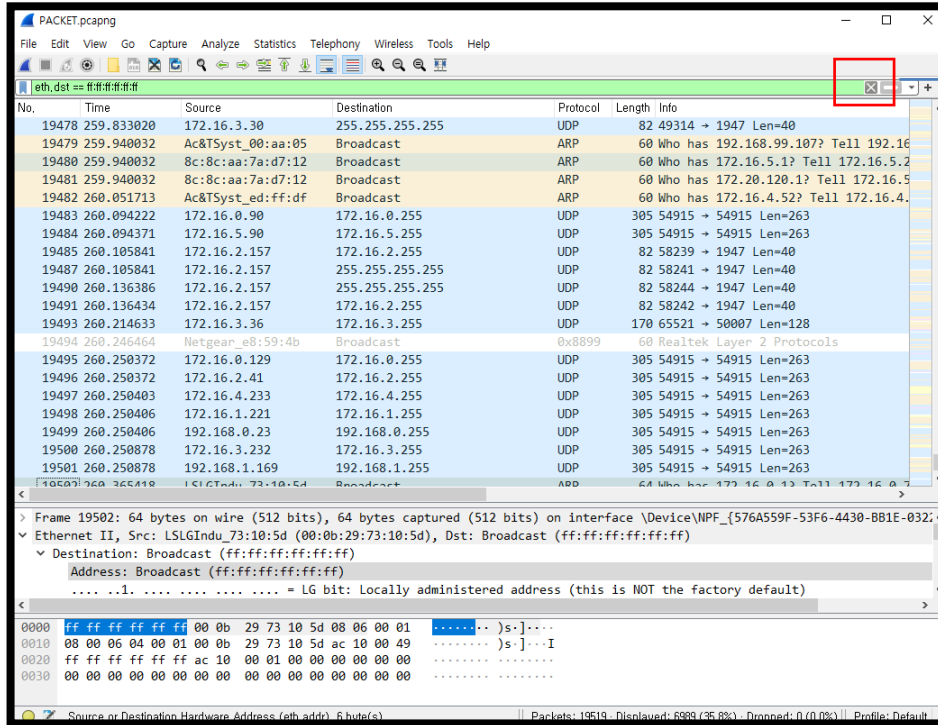
Source or Destination Hardware Address (eth,addr), 6 byte(s) Packets: 19519 · Displayed: 6989 (35,8%) · Dropped: 0 (0,0%) Profile: Default

Packets: 19519 · Displayed: 6989 (35,8%) · Dropped: 0 (0,0%)

프로그램 하단의 패킷량 % 량을 확인 합니다.

Wireshark 사용 방법

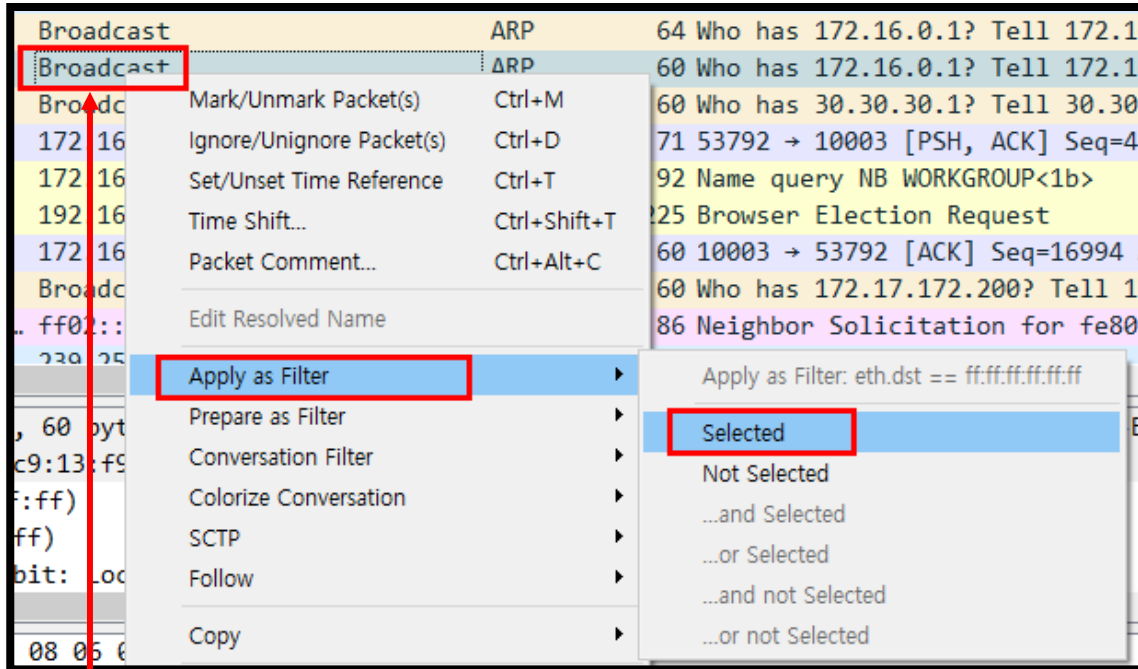
Advanced Communication & Technology System



X 를 클릭하여 필터를 해제 합니다.

Wireshark 사용 방법

Advanced Communication & Technology System

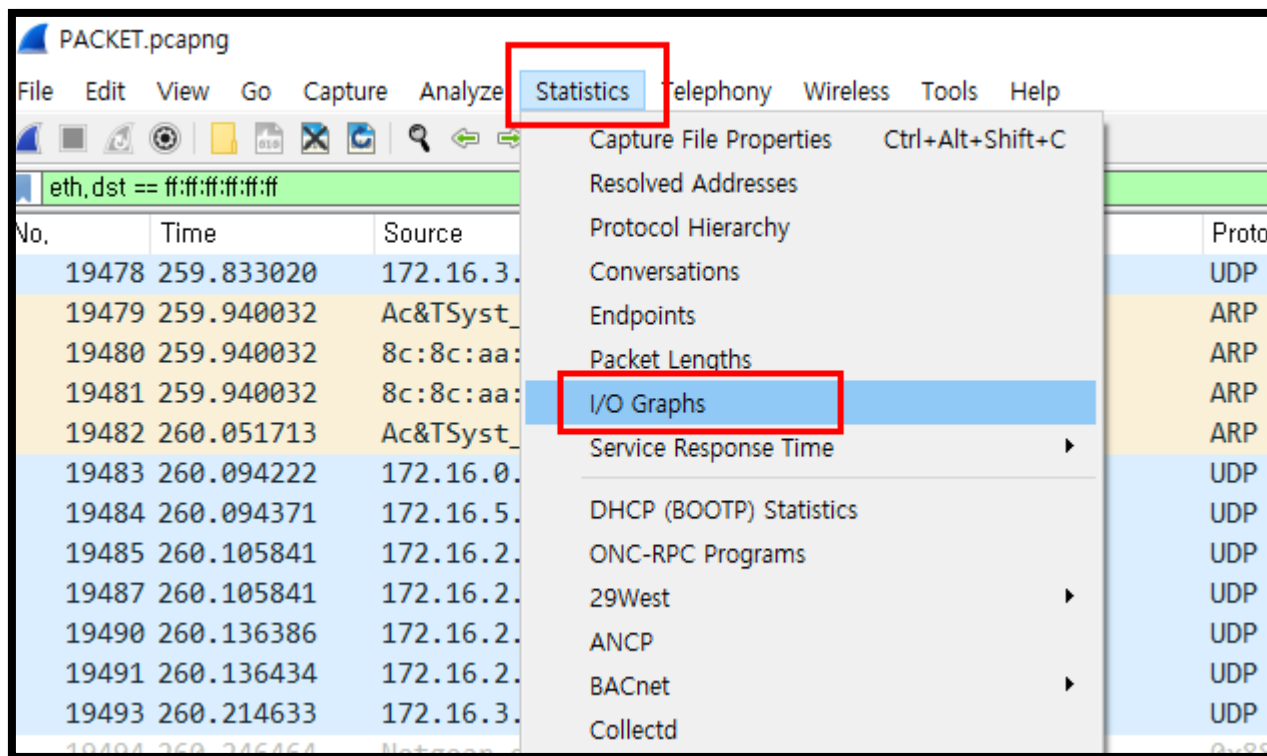


저희 사내망에서는 멀티캐스트 패킷이 없어
브로드 캐스트 필터링 화면으로 대체 하였으니
참고 하시기 바랍니다.

Broadcast를 Select 한 것 과 같이 MultyCast 항목
을 Select 하여 패킷량 %를 확인 합니다.

Wireshark 사용 방법

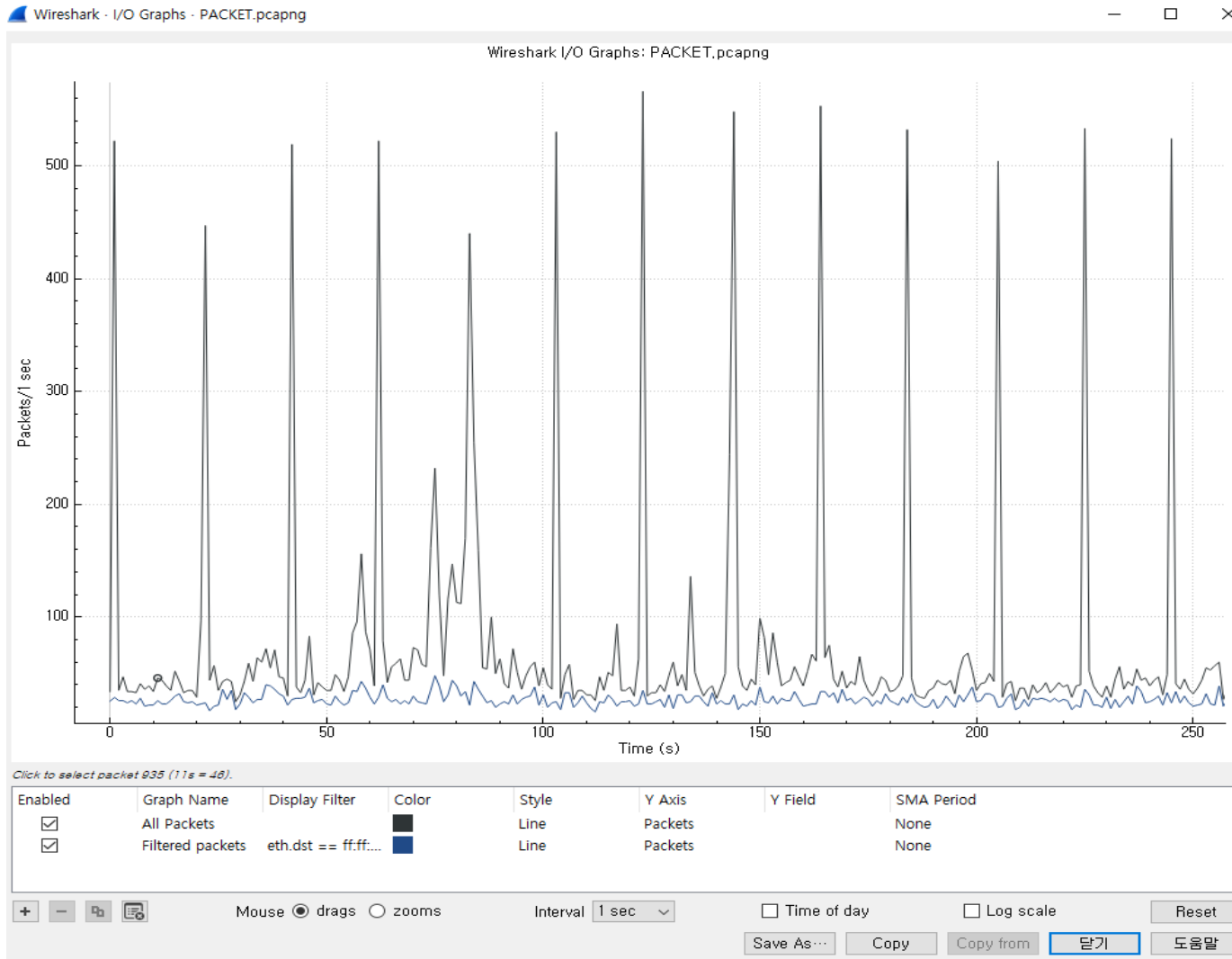
Advanced Communication & Technology System



I/O 그래프 화면으로 이동합니다.

Wireshark 사용 방법

Advanced Communication & Technology System

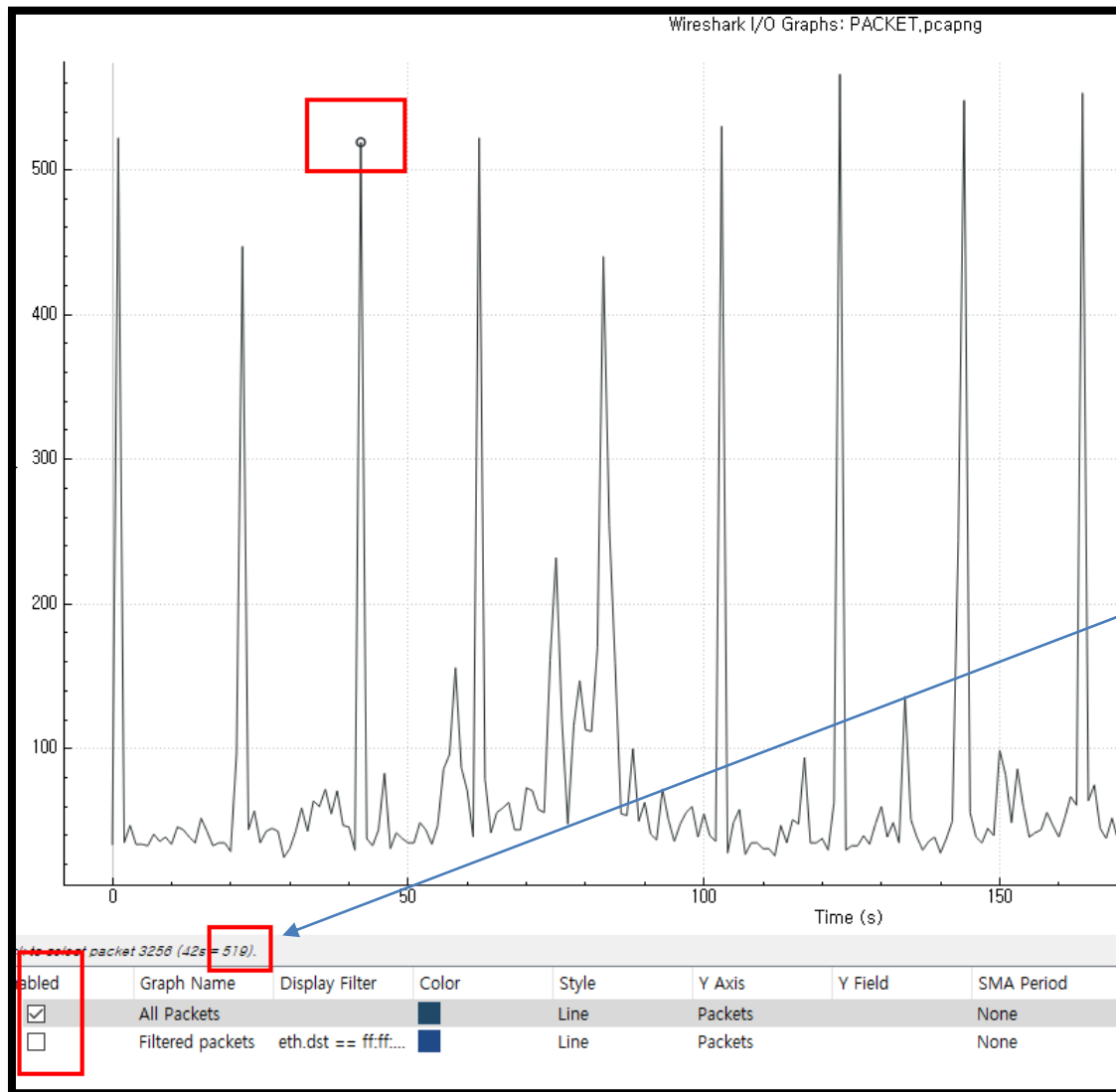


전체 패킷량.
필터링한
Broadcast, Multycst
패킷의 초당 발생량을
확인 할 수 있습니다.

그래프는 아래의 컬러
구분으로 확인이 가능
합니다.

Wireshark 사용 방법

Advanced Communication & Technology System



좌측 하단의 Enable 항목을 1개만 체크한 상태에서 그래프부분에 마우스를 움직이면 상단의 동그란 표시가 마우스와 그래프를 따라 이동하는 것을 확인 할 수 있습니다.

그래프의 최 상단에 위치할때 아래쪽에 패킷량이 얼마인지 확인이 가능합니다.

필터링 되어있는 항목 1개씩 반복하여 패킷량을 확인 합니다.