

Wireshark를 이용한 패킷 수집 및 분석

성결대학교 컴퓨터공학부
최정열 교수
(passjay0@naver.com)



Contents

❑ What is Wireshark ?

❑ Installation

❑ Get Started

❑ Menu and Functions

- Filter
- Statistics
- Telephony

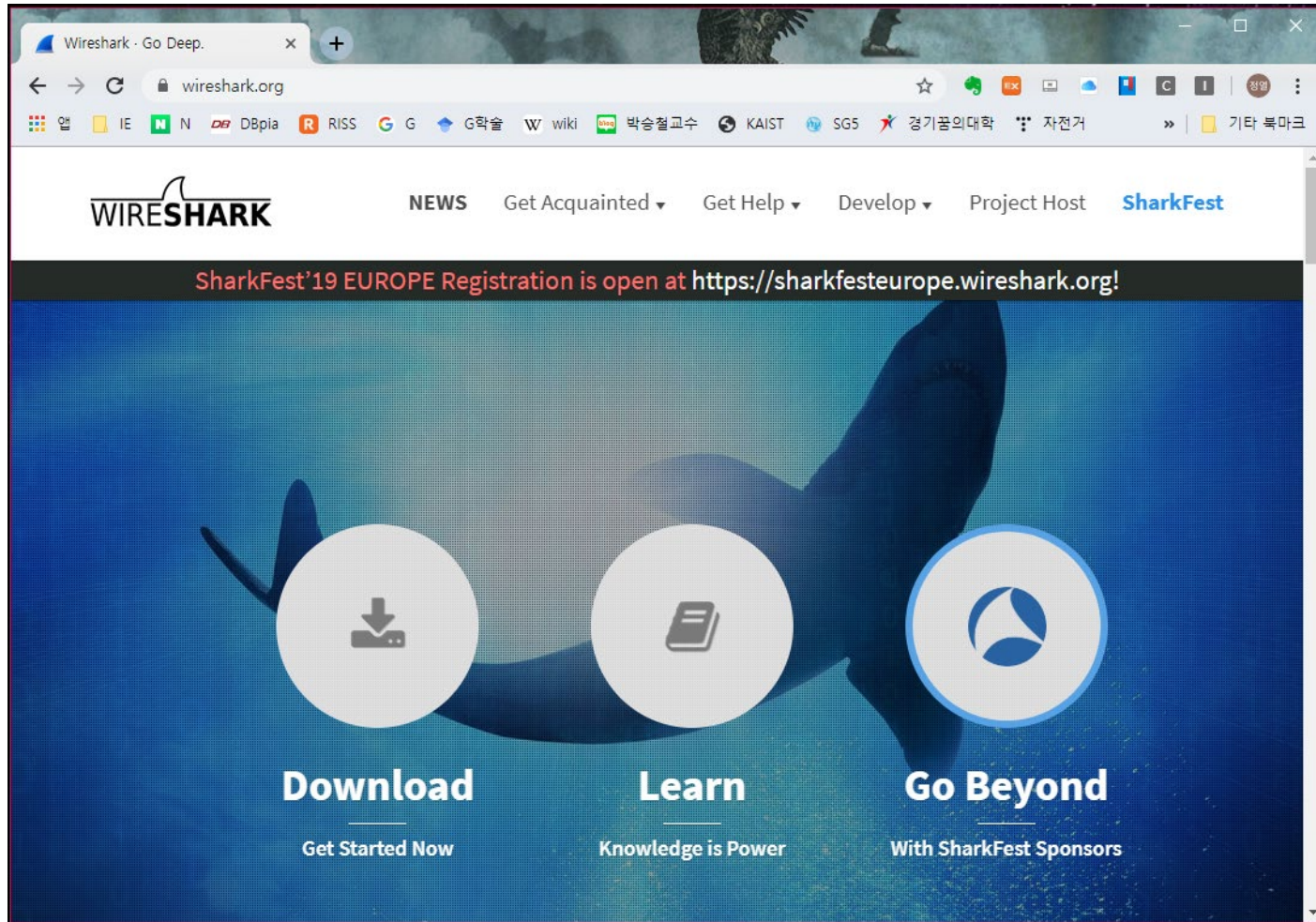
❑ Assignments

What is Wireshark

- ❑ 세계에서 가장 널리 쓰이는 네트워크(패킷) 분석 프로그램
- ❑ 수집한 패킷에 대한 네트워크/계층별 프로토콜 정보를 제공
- ❑ 패킷을 수집하기 위해서 pcap 네트워크 라이브러리를 사용
- ❑ 장점
 - 쉬운 설치
 - GUI 인터페이스를 이용한 간단한 사용법
 - 필터, 통계 등 다양한 기능 제공
 - 오픈 소스 기반의 프리웨어

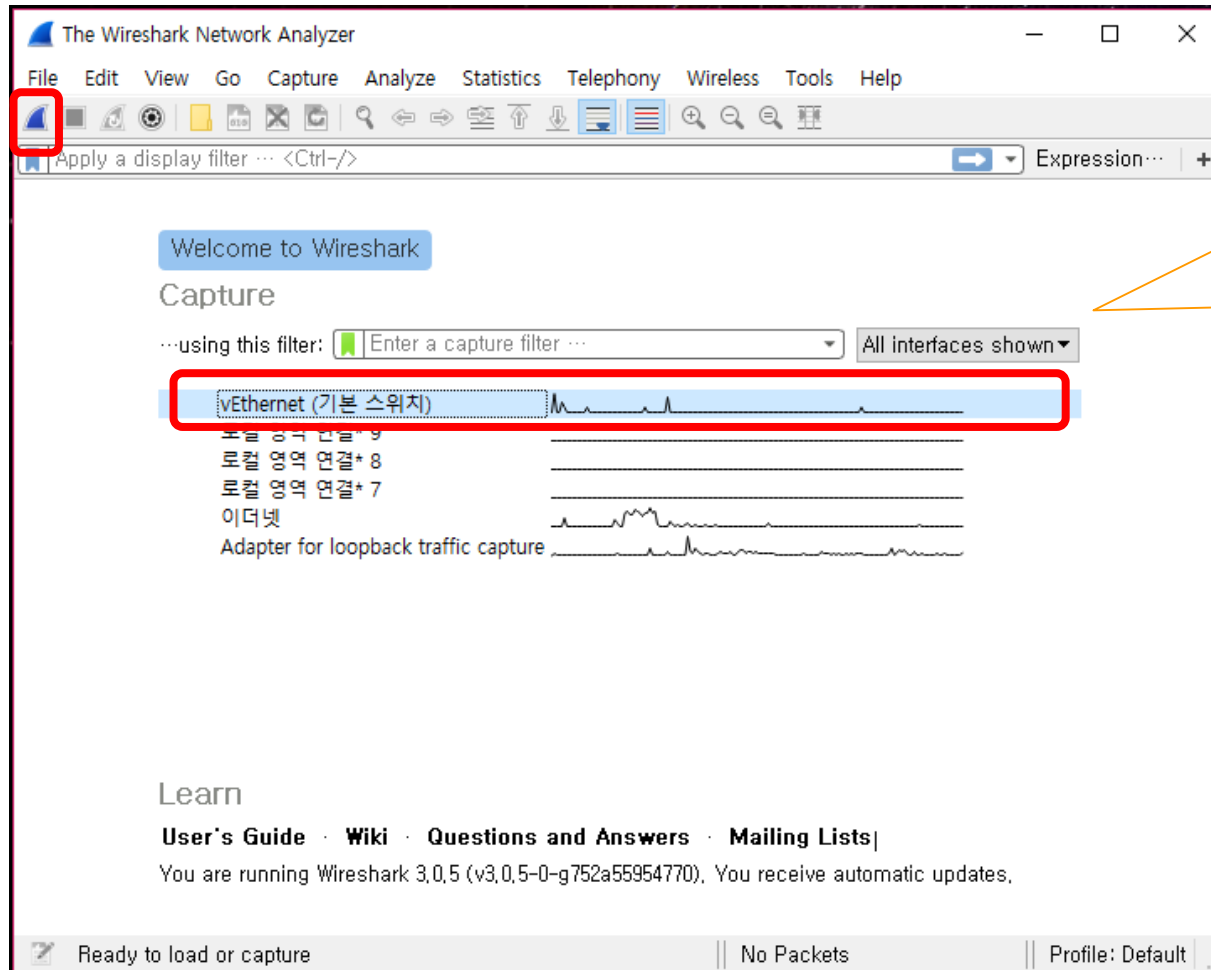
Installation

❑ <http://www.wireshark.org>



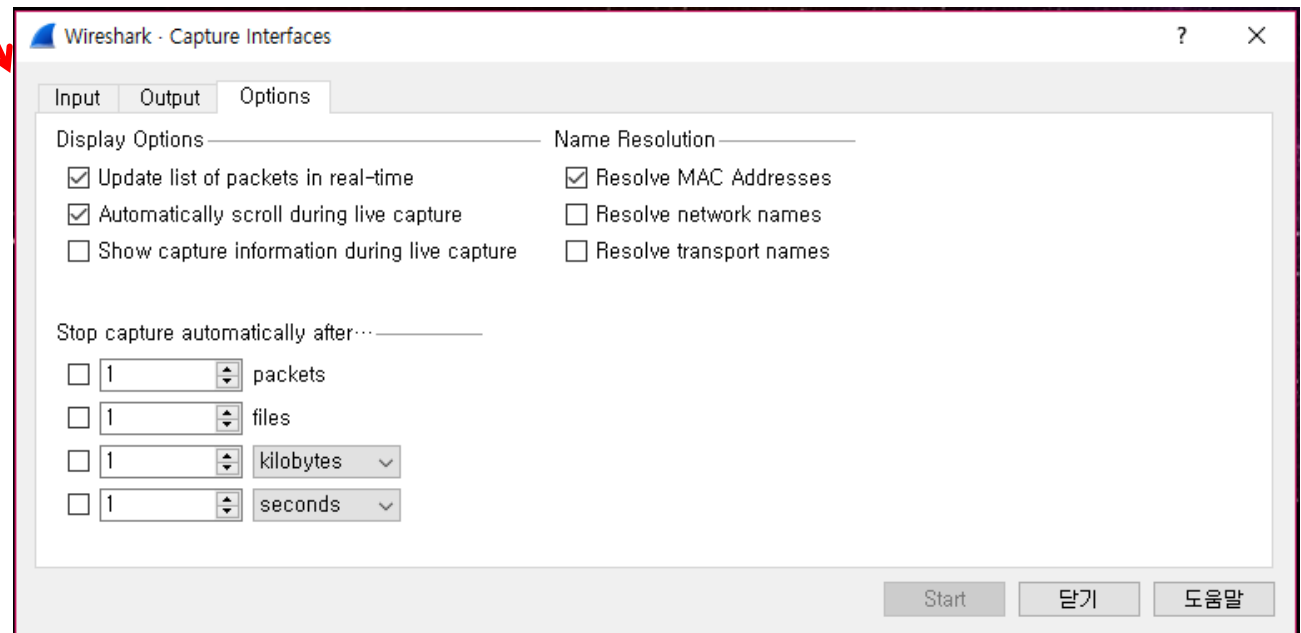
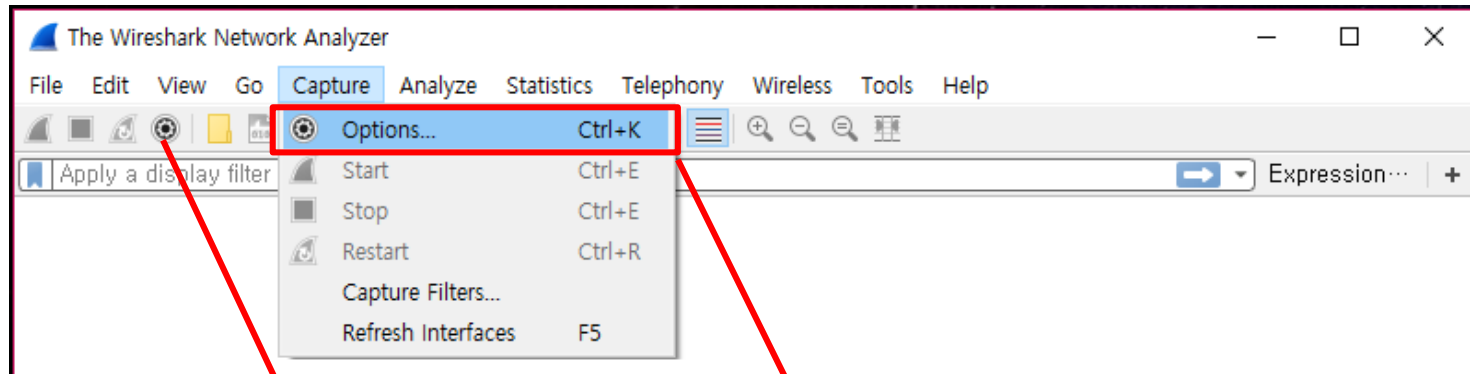
Get Started

❑ 네트워크 인터페이스를 선택하고 패킷을 캡처한다

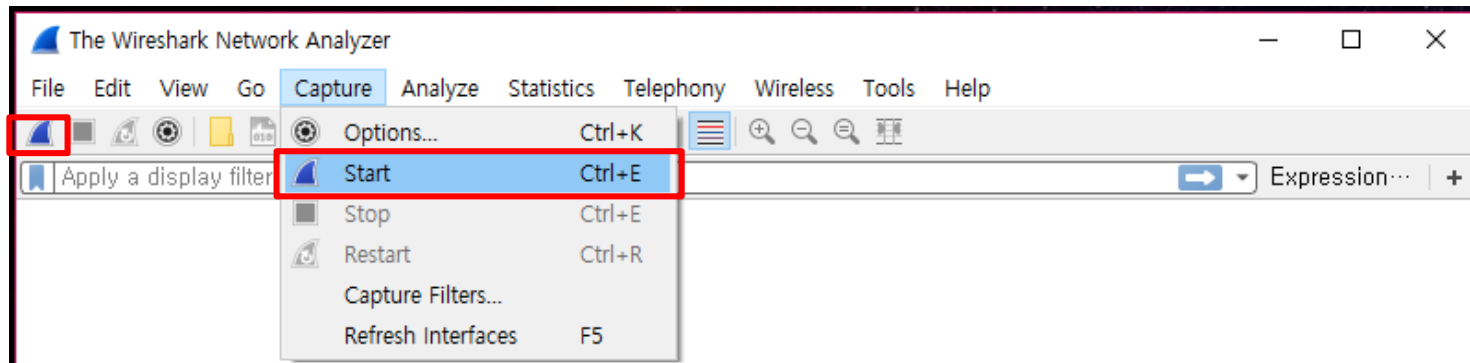


캡처 가능한
인터페이스가
안 보이면,
관리자 권한
으로 실행

❑ [Capture]-[Option] 메뉴에서 캡처 관련 여러가지 사항을 설정한다



- ❑ [Capture] 메뉴의 [Start] 버튼, 또는 캡처 인터페이스 창의 [Start] 버튼을 눌러 캡처를 시작한다



❑ 패킷 캡처 화면

- Menu
- Shortcuts
- Display Filter
- Packet List Pane
- Packet Details Pane
- Dissector Pane
- Misc.

The image shows the Wireshark network protocol analyzer interface. The title bar reads '*이더넷'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. Below the toolbar is a display filter set to 'http'. The packet list pane shows three captured packets, all of type HTTP. The first packet (No. 507) is a GET request to / HTTP/1.1. The second packet (No. 510) is an HTTP 302 response. The third packet (No. 2152) is a GET request to /?nil_prof. The packet details pane shows the structure of the selected packet (No. 507), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The dissector pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates the current protocol is Transmission Control Protocol (tcp), 20 bytes, with 9416 packets displayed and 6 (0.1%) dropped.

No.	Time	Source	Destination	Protocol	Length	Info
507	7.446691	192.168.0.56	203.133.167.212	HTTP	1240	GET / HTTP/1.1
510	7.450802	203.133.167.212	192.168.0.56	HTTP	193	HTTP/1.1 302 F
2152	29.350526	192.168.0.56	203.133.167.81	HTTP	1386	GET /?nil_prof

Frame 8732: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface 0

Ethernet II, Src: Micro-St_9e:6b:50 (30:9c:23:9e:6b:50), Dst: EfmNetwo_c3:c3:d0 (00:26:66:c3:c3:d0)

Internet Protocol Version 4, Src: 192.168.0.56, Dst: 125.209.254.194

Transmission Control Protocol, Src Port: 52485, Dst Port: 80, Seq: 1, Ack: 1, Len: 429

Hypertext Transfer Protocol

0020 fe c2 cd 05 00 50 b6 f3 29 72 27 ab fb 8e 50 18P..)r'...P.

0030 01 04 3f 3c 00 00 47 45 54 20 2f 6d 6f 76 69 65 ..?<...GE T /movie

0040 2f 32 30 31 32 2f 30 39 2f 62 67 5f 68 6f 6d 65 /2012/09 /bg_home

0050 2e 70 6e 67 20 48 54 54 50 2f 31 2e 31 0d 0a 48 .png HTTP/1.1..H

0060 6f 73 74 3a 20 73 74 61 74 69 63 2e 6e 61 76 65 ost: static.nave

0070 72 2e 6e 65 74 0d 0a 43 6f 6e 6e 65 63 74 69 6f r.net..C onnectio

0080 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep-alive..U

0090 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ser-Agent: Mozil

Transmission Control Protocol (tcp), 20 bytes | Packets: 9416 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

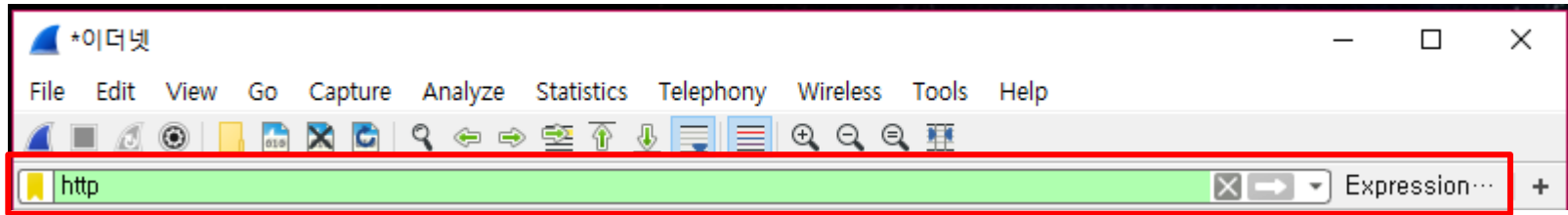
Menu and Functions

□ 메뉴

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

- File: 캡처 데이터를 열거나 저장합니다.
- Edit: 패킷을 찾거나 표시합니다. 프로그램 전역적인 속성들을 설정합니다.
- View: Wireshark 플랫폼의 보이는 모양을 설정합니다.
- Go: 캡처된 데이터의 특정 위치로 이동합니다.
- Capture: 캡처 필터 옵션을 설정하고 캡처를 시작합니다.
- Analyze: 분석 옵션(display)을 설정합니다.
- Statistics: Wireshark의 통계 데이터를 봅니다.
- Telephony: 인터넷전화 관련 트래픽 분석
- Wireless: Bluetooth, WLAN 트래픽 분석
- Tools
- Help: 오프라인 혹은 온라인 도움말을 봅니다.

❑ Display Filter



- Display Filter는 캡처된 로그 정보에서 데이터를 찾을 때 사용합니다.
 - Capture Filter vs Display Filter
- 필터가 문법에 맞게 설정되면 녹색으로 표시된다

❑ Packet List Pane

Time ↓	Source	Destination	Port	Protocol	Info
4.371799	192.168.1.2	84.16.81.23	80	HTTP	GET /image/bu_logo.jpg HTTP/1.1
4.384927	84.16.81.23	192.168.1.2	3296	HTTP	HTTP/1.1 304 Not Modified
4.397701	84.16.81.23	192.168.1.2	3293	HTTP	HTTP/1.1 304 Not Modified
4.419743	192.168.1.2	84.16.81.23	80	HTTP	GET /image/carre.gif HTTP/1.1
4.419911	192.168.1.2	84.16.81.23	80	HTTP	GET /image/carre_blanc.gif HTTP/1.1
4.444310	84.16.81.23	192.168.1.2	3296	HTTP	HTTP/1.1 304 Not Modified
4.444734	192.168.1.2	84.16.81.23	80	HTTP	GET /lookxp/lookxpback.gif HTTP/1.1
4.457367	84.16.81.23	192.168.1.2	3293	HTTP	HTTP/1.1 304 Not Modified
4.474045	84.16.81.23	192.168.1.2	3296	TCP	[TCP segment of a reassembled PDU]
4.477516	84.16.81.23	192.168.1.2	3296	TCP	[TCP segment of a reassembled PDU]

185.	Cisco-Li_2a:fb:9b	3Com_9b:47:f7	ARP	who has 192.168.1.2? Tell 192.168.1.1
185.	3Com_9b:47:f7	Cisco-Li_2a:fb:9b	ARP	192.168.1.2 is at 00:04:75:9b:47:f7

- packet list 패널은 캡처된 모든 패킷을 보여줍니다
 - Source/destination MAC/IP 주소, TCP /UDP 포트 번호, 프로토콜, 패킷 내용 등
- 열은 추가/삭제 할 수 있으며, [Edit]-[Preferences]에서 패널의 색상을 변경 할 수 있습니다:

❑ Packet Details Pane

Selected Packet

Time	Source	Destination	Port	Protocol	Info
59.3	192.168.1.2	84.16.81.23	80	HTTP	GET /wireshark_use.php HTTP/1.1
59.3	192.168.1.2	84.16.81.23	80	HTTP	GET /menu.js HTTP/1.1
59.4	84.16.81.23	192.168.1.2	1600	HTTP	HTTP/1.1 304 Not Modified
59.4	192.168.1.2	84.16.81.23	80	HTTP	GET /lookxp.css HTTP/1.1
59.5	84.16.81.23	192.168.1.2	1601	HTTP	HTTP/1.1 304 Not Modified

OSI Layer 2

OSI Layer 3

OSI Layer 4

OSI Layer 7

- Frame 152 (773 bytes on wire, 773 bytes captured)
- Ethernet II, Src: 3Com_9b:47:f7 (00:04:75:9b:47:f7), Dst: Cisco-Li_2a:fb:9b (00:18:39:2a:fb:9b)
- Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 84.16.81.23 (84.16.81.23)
- Transmission Control Protocol, Src Port: 1601 (1601), Dst Port: http (80), Seq: 1, Ack: 1, Len: 719
- Hypertext Transfer Protocol

- Frame 152 (773 bytes on wire, 773 bytes captured)
- Ethernet II, Src: 3Com_9b:47:f7 (00:04:75:9b:47:f7), Dst: Cisco-Li_2a:fb:9b (00:18:39:2a:fb:9b)
- Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 84.16.81.23 (84.16.81.23)
- Transmission Control Protocol, Src Port: 1601 (1601), Dst Port: http (80), Seq: 1, Ack: 1, Len: 719
- Hypertext Transfer Protocol
- GET /lookxp.css HTTP/1.1\r\n
 Accept: */*\r\n
 Referer: http://www.openmaniak.com/wireshark_use.php\r\n
 Accept-Language: fr-ch\r\n
 Accept-Encoding: gzip, deflate\r\n
 If-Modified-Since: Tue, 27 Nov 2007 18:05:18 GMT\r\n
 If-None-Match: "1092c33-2590-474c5c5e"\r\n
 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727)\r\n
 Host: www.openmaniak.com\r\n
 Connection: Keep-Alive\r\n
 Cookie: __utmc=196743026; __utma=196743026.531070789.1188047094.1196949120.1196949190.96; __utmz=196743026.1196949190.96.17.utmcc\r\n

- 패킷 리스트에서 선택한 패킷에 대한 상세한 정보 제공
 - 계층별로 표시

❑ Dissector Pane

```
+ Frame 152 (773 bytes on wire, 773 bytes captured)
+ Ethernet II, Src: 3Com_9b:47:f7 (00:04:75:9b:47:f7), Dst: Cisco-Li_2a:fb:9b (00:18:39:2a:fb:9b)
+ Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 84.16.81.23 (84.16.81.23)
- Transmission Control Protocol, Src Port: 1601 (1601), Dst Port: http (80), Seq: 1, Ack: 1, Len: 719
  Source port: 1601 (1601)
  Destination port: http (80)
  Sequence number: 1 (Initial sequence number)

0010  02 f7 82 ae 40 00 80 06 0e 81 c0 a8 01 02 54 10  ....@... ..T.
0020  51 17 06 41 00 50 69 66 8c 75 94 d2 db f6 50 18  Q..A.Pif .u...P.
0030  ff ff 69 bb 00 00 47 45 54 20 2f 6c 6f 6f 6b 78  ..i...GE T /lookx
0040  70 2e 63 73 73 20 48 54 54 50 2f 31 2e 31 0d 0a  p.css HT TP/1.1..
0050  41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 52 65 66  Accept: */*..Ref
```

- "packet bytes 패널"이라고도 하는 dissector 패널은 packet details 패널과 내용은 같지만 데이터를 16진수로 나타내줍니다.
- 위에 보여진 예에서, packet details 패널에서 TCP 포트(80)을 선택하였고, 그에 대한 16진수 정보가 dissector 패널에 자동으로 표시됩니다.(0050)

□ 프로그램 하단 정보

Network Interface	Capture state	Capture file	Capture size	P	D	M
3Com EtherLink PCI (Microsoft's Packet Scheduler) : <live capture in progress> File: C:\DOCUME~1\admin\LOCAL5~1\Temp\etherXXXXa01768 9677 KB						
				P: 34239	D: 3481	M: 0

- 캡처하는데 사용된 네트워크 카드
- 캡처 동작이 진행 혹은 정지 상태 여부
- 캡처된 정보가 하드 디스크의 어느 위치에 저장되는지
- 캡처 사이즈
- 캡처된 패킷수(P)
- 화면에 표시된 패킷수(display filter에 매칭되는 패킷들)
- 표시된 패킷수(M)

Filtering

□ 필터

- 방대한 자료 중에서 원하는 데이터를 찾을 수 있게 함
- Capture Filter
 - 로그에 기록되는 데이터를 선택
 - 로그의 크기를 줄이는 것이 목적
- Display Filter
 - 캡처된 로그에서 데이터를 찾을 때 사용
 - 데이터를 캡처하는 동안 수정 가능
 - 원하는 데이터를 검색

❑ Capture Filters

- 설정 방법: [Capture]-[Capture Filters]
- 사용 예

Syntax:	Protocol	Direction	Host(s)	Value	Logical Operations	Other expression
Example:	tcp	dst	10.1.1.1	80	and	tcp dst 10.2.2.2 3128

- Protocol: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp udp
 - 프로토콜을 지정하지 않으면 모든 프로토콜을 사용
- Direction: src, dst, src and dst, src or dst
 - 출발지나 목적지를 지정하지 않으면 "src or dst" 키워드를 사용
 - 예) "host 10.2.2.2"은 "src or dst host 10.2.2.2"을 의미함
- Host(s): net, port, host, portrange.
 - 호스트를 지정하지 않으면 "host" 키워드를 사용
 - 예) "src 10.1.1.1"은 "src host 10.1.1.1"과 같은 의미
- Logical Operations: not, and, or.
 - "not"이 가장 높은 우선순위. "or"과 "and"는 같은 우선순위. 왼쪽에서 오른쪽으로 처리
 - 예) "not tcp port 3128 and tcp port 23"은 "(not tcp port 3128) and tcp port 23"과 동일
"not (tcp port 3128 and tcp port 23)"과는 동일하지 않음

● 사용 예

– **tcp dst port 3128**

- 목적지가 TCP 포트 3128인 패킷을 보여줌

– **ip src host 10.1.1.1**

- 출발지 IP 주소가 10.1.1.1인 패킷을 보여줌

– **host 10.1.2.3**

- 출발지와 목적지 IP 주소가 10.1.1.1인 패킷을 보여줌

– **src portrange 2000-2500**

- 출발지의 UDP, TCP 포트가 2000-2500 사이인 패킷을 보여줌

– **not icmp**

- icmp 패킷을 제외한 모든 패킷을 보여줌

– **src host 10.7.2.12 and not dst net 10.200.0.0/16**

- 출발지 IP 주소가 10.7.2.12이면서, 목적지 IP 네트워크가 10.200.0.0/16이 아닌 패킷을 보여줌

– **(src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst portrange 200-10000 and dst net 10.0.0.0/8**

- 출발지 IP 주소가 10.4.1.12이거나, 출발지 네트워크가 10.6.0.0/16인 패킷 중에서 목적지 TCP 포트 범위가 200-10000이면서, 목적지 IP 네트워크가 10.0.0.0/8인 패킷을 보여줌

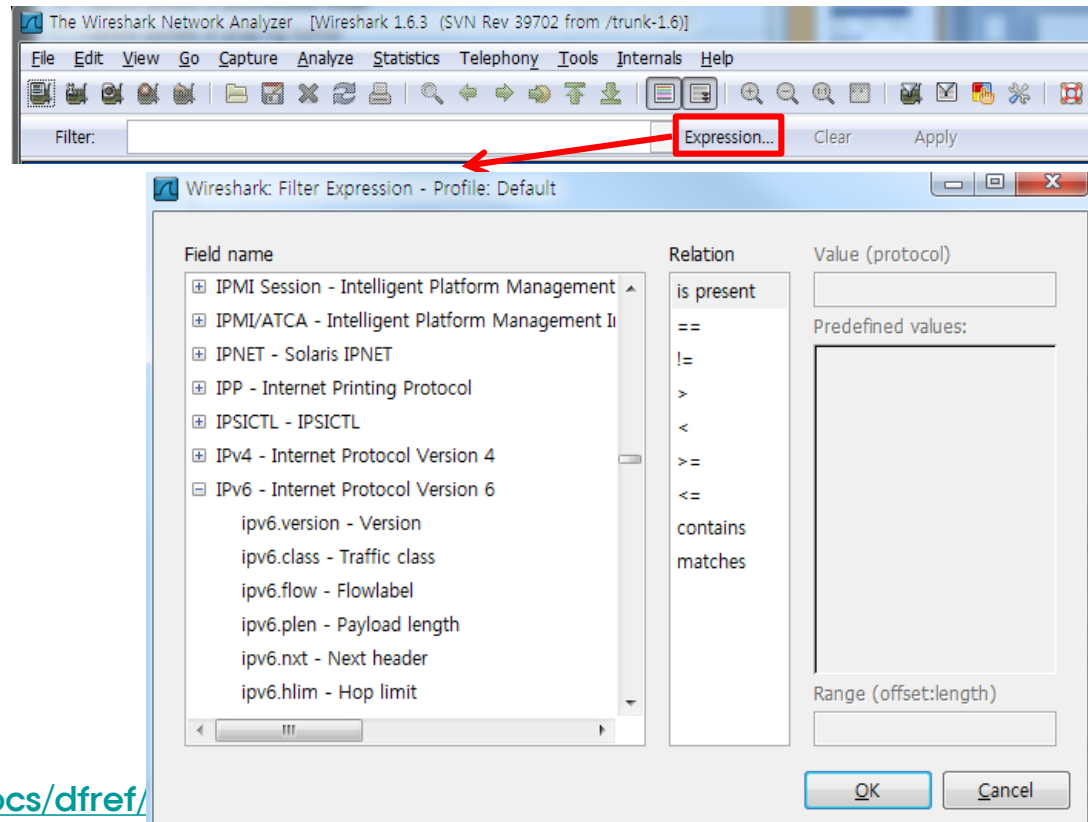
❑ Display Filters

- 설정방법: [Analyze]-[Display Filters]
- 사용 예

Syntax: **Protocol** . **String 1** . **String 2** **Comparison operator** **Value** **Logical Operations** **Other expression**

Example: ftp passive ip == 10.2.3.4 xor icmp.type

- Protocol:
 - 프로토콜을 선택
- String1, 2: optional
 - 프로토콜의 하위 카테고리



❖ 지원 프로토콜: <http://www.wireshark.org/docs/dfref/>

- Comparison operator

영문 표기:	C언어 표기:	의미:
eq	==	같다
ne	!=	틀리다
gt	>	크다
lt	<	작다
ge	>=	크거나 같다
le	<=	작거나 같다

- Logical Operations

영문 표기:	C언어 표기:	의미:
and	&&	논리곱
or		논리합
xor	^^	배타적 논리합
not	!	부정

● 사용 예

- **snmp || dns || icmp**

- SNMP 혹은 DNS 혹은 ICMP 트래픽을 보여줌

- **ip.addr == 10.1.1.1**

- 출발지나 목적지의 IP 주소가 10.1.1.1인 패킷을 보여줌

- **ip.src != 10.1.2.3 or ip.dst != 10.4.5.6**

- 출발지의 IP 주소가 10.1.2.3이 아니거나 목적지의 IP 주소가 10.4.5.6이 아닌 패킷을 보여줌

- **ip.src != 10.1.2.3 and ip.dst != 10.4.5.6**

- 출발지 IP 주소가 10.1.2.3이 아니면서, 목적지 IP 주소가 10.4.5.6이 아닌 패킷을 보여줌

- **tcp.port == 25**

- 출발지와 목적지의 TCP 포트가 25인 패킷을 보여줌

- **tcp.dstport == 25**

- 목적지의 TCP 포트가 25인 패킷을 보여줌

- **tcp.flags**

- TCP 플래그를 가지고 있는 패킷을 보여줌

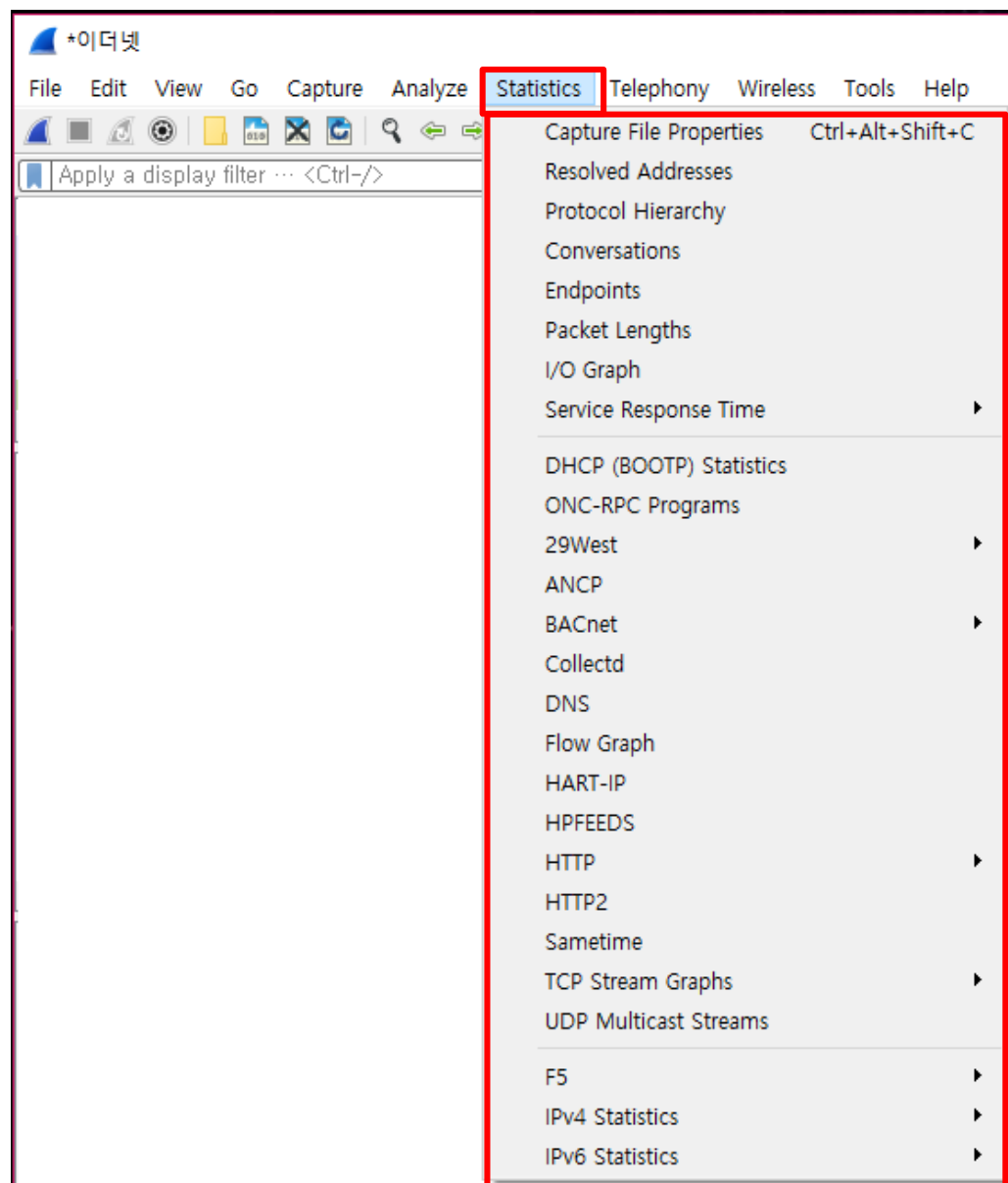
- **tcp.flags.syn == 0x02**

- TCP SYN 플래그를 가지고 있는 패킷을 보여줌

- 필터 구문에 문제가 없다면, 녹색으로 하이라이트 될 것이며, 잘못됐다면 붉은색으로 하이라이트 될 것입니다.



Statistics



❑ Protocol Hierarchy

- 계층별 데이터 확인

Wireshark: Protocol Hierarchy Statistics

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	36227	36274768	0.438	0	0	0.000
Ethernet	100.00%	36227	36274768	0.438	0	0	0.000
Internet Protocol IP	100.00%	36227	36274768	0.438	0	0	0.000
Transmission Control Protocol TCP	99.74%	36134	36265227	0.438	35819	36068887	0.435
Data	0.08%	28	4860	0.000	28	4860	0.000
Hypertext Transfer Protocol HTTP	0.75%	273	181506	0.002	236	161226	0.002
CompuServe GIF	0.03%	11	5868	0.000	11	5868	0.000
Line-based text data	0.04%	16	7603	0.000	16	7603	0.000
Portable Network Graphics	0.03%	10	6809	0.000	10	6809	0.000
User Datagram Protocol UDP	0.13%	47	6137	0.000	0	0	0.000
Domain Name Service	0.04%	14	1431	0.000	14	1431	0.000
Data	0.08%	29	4187	0.000	29	4187	0.000
NetBIOS Name Service	0.01%	3	276	0.000	3	276	0.000
NetBIOS Datagram Service NetBIOS	0.00%	1	243	0.000	0	0	0.000
SMB (Server Message Block Protocol)	0.00%	1	243	0.000	0	0	0.000
SMB MailSlot Protocol	0.00%	1	243	0.000	0	0	0.000
Microsoft Windows Browser Protocol	0.00%	1	243	0.000	1	243	0.000
Internet Control Message Protocol ICMP	0.13%	46	3404	0.000	46	3404	0.000

OSI Layer 2: Ethernet
OSI Layer 3: IP, ICMP
OSI Layer 4: TCP, UDP
OSI Layer 5 to 7: HTTP, NetBIOS, SMB, etc.

❑ Conversation

- 두 호스트 사이의 트래픽
- 프로토콜 명 옆의 숫자: conversation의 수

Conversations: Realtek RTL8168D/8111D PCI-E Gigabit Ethernet NIC

Ethernet: 398 | Fibre Channel | FDDI | IPv4: 266 | IPv6: 91 | IPX: 6 | JXTA | NCP | RSVP | SCTP | TCP: 23 | Token Ring | UDP: 517 | USB | WLAN

Ethernet Conversations

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B
Micro-St_50:df:cf	Broadcast	7	887	7	887	0	0
Micro-St_50:df:48	Broadcast	22	1 933	22	1 933	0	0
Micro-St_85:dd:49	Broadcast	26	3 294	26	3 294	0	0
SamsungE_33:24:23	Broadcast	73	6 684	73	6 684	0	0
Wistron_83:58:1e	Broadcast	261	15 660	261	15 660	0	0
BrocadeC_9b:9b:00	Broadcast	14 253	855 180	14 253	855 180	0	0
Micro-St_50:df:4d	Broadcast	250	22 488	250	22 488	0	0
Giga-Byt_9f:cb:0b	Broadcast	35	2 100	35	2 100	0	0
ScopeInf_03:01:26	Broadcast	2 104	126 240	2 104	126 240	0	0
ScopeInf_03:01:26	Portwell_2c:61:d6	129	7 740	129	7 740	0	0
JuniperN_59:74:db	Portwell_2c:61:d6	125	7 502	125	7 502	0	0
Hewlett_82:95:ac	Broadcast	378	35 568	378	35 568	0	0

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Stream Close

❑ Endpoints

- 각 장치별로 주고 받은 데이터에 대한 통계 정보
- 프로토콜 명 옆의 숫자: Endpoints의 수

Endpoints: Realtek RTL8168D/8111D PCI-E Gigabit Ethernet NIC

Ethernet: 270 | Fibre Channel | FDDI | IPv4: 213 | IPv6: 59 | IPX: 7 | JXTA | NCP | RSVP | SCTP | TCP: 38 | Token Ring | UDP: 549 | USB | WLAN

Ethernet Endpoints

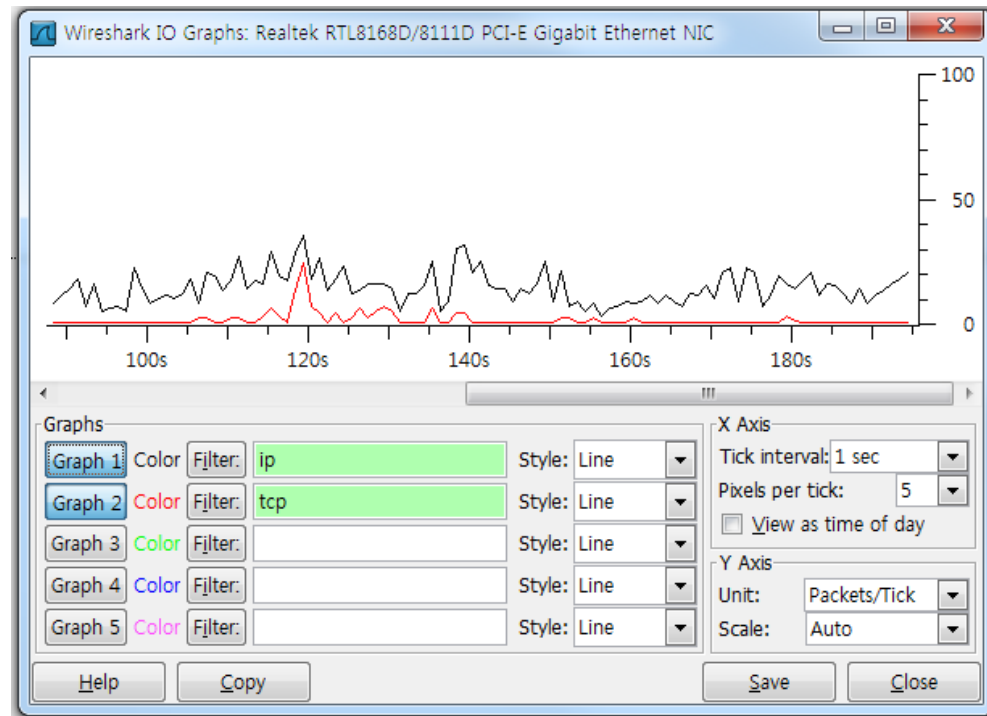
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
Micro-St_50:df:cf	7	887	7	887	0	0
Broadcast	19 944	1 285 463	0	0	19 944	1 285 463
Micro-St_50:df:48	22	1 933	22	1 933	0	0
Micro-St_85:dd:49	57	8 154	57	8 154	0	0
SamsungE_33:24:23	178	15 497	178	15 497	0	0
Wistron_83:58:1e	261	15 660	261	15 660	0	0
BrocadeC_9b:9b:00	14 611	936 626	14 434	911 951	177	24 675
Micro-St_50:df:4d	250	22 488	250	22 488	0	0
Giga-Byt_9f:cb:0b	35	2 100	35	2 100	0	0
ScopeInf_03:01:26	2 239	134 354	2 238	134 312	1	42
Portwell_2c:61:d6	254	15 242	0	0	254	15 242
JuniperN_59:74:db	272	16 322	272	16 322	0	0
Hewlett_82:95:ac	378	35 568	378	35 568	0	0

☒ Name resolution ☐ Limit to display filter

Help Copy Map Close

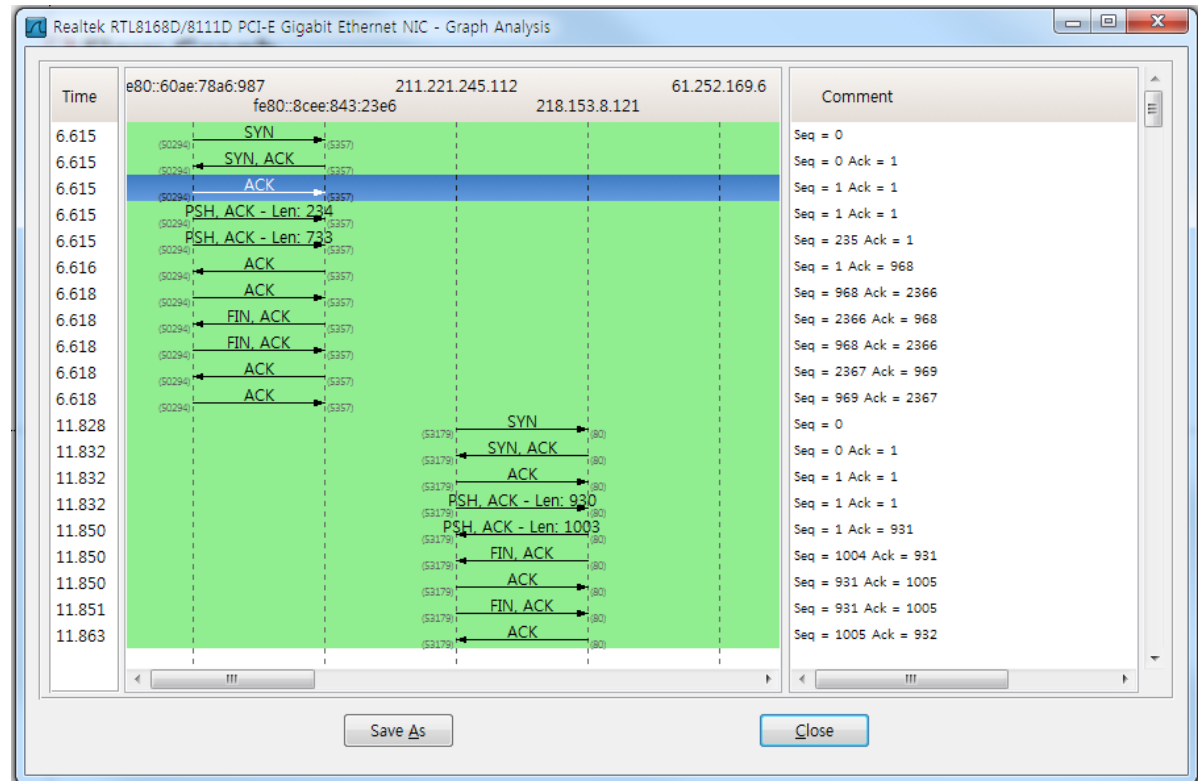
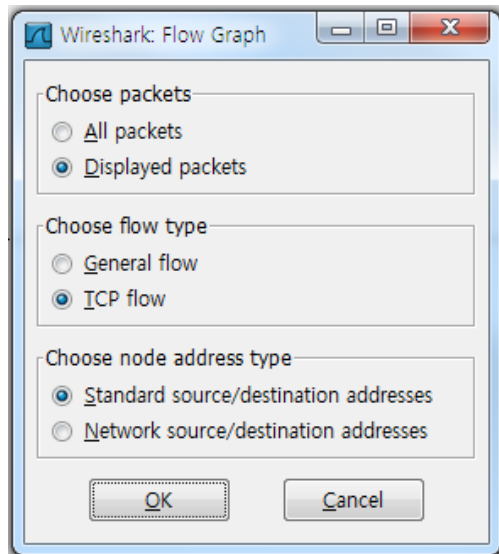
❑ IO Graphs

- 입출력 트래픽 상황을 그래프로 표시
- 필터 이용 가능



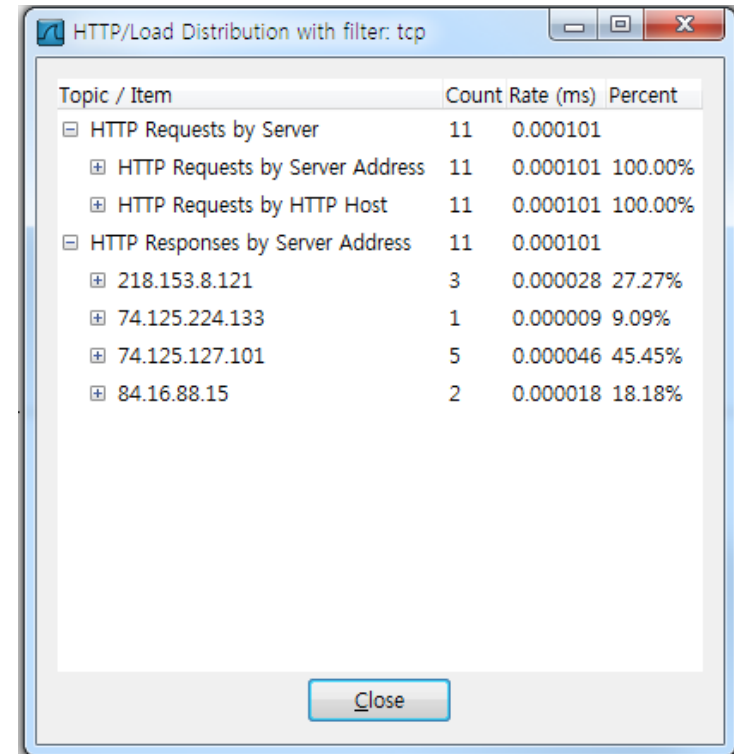
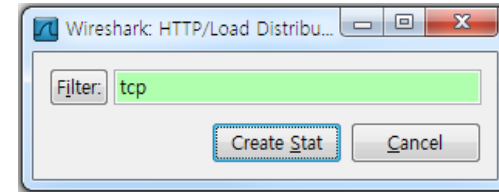
❑ Flow Graph

- TCP 연결 정보 분석



□ HTTP

- Load Distribution
 - 웹서버별 부하 분포도를 보여줌
- Packet Counter
 - HTTP 요청과 응답을 보여줌
- Requests
 - 웹서버에서 요청받은 파일들을 보여줌



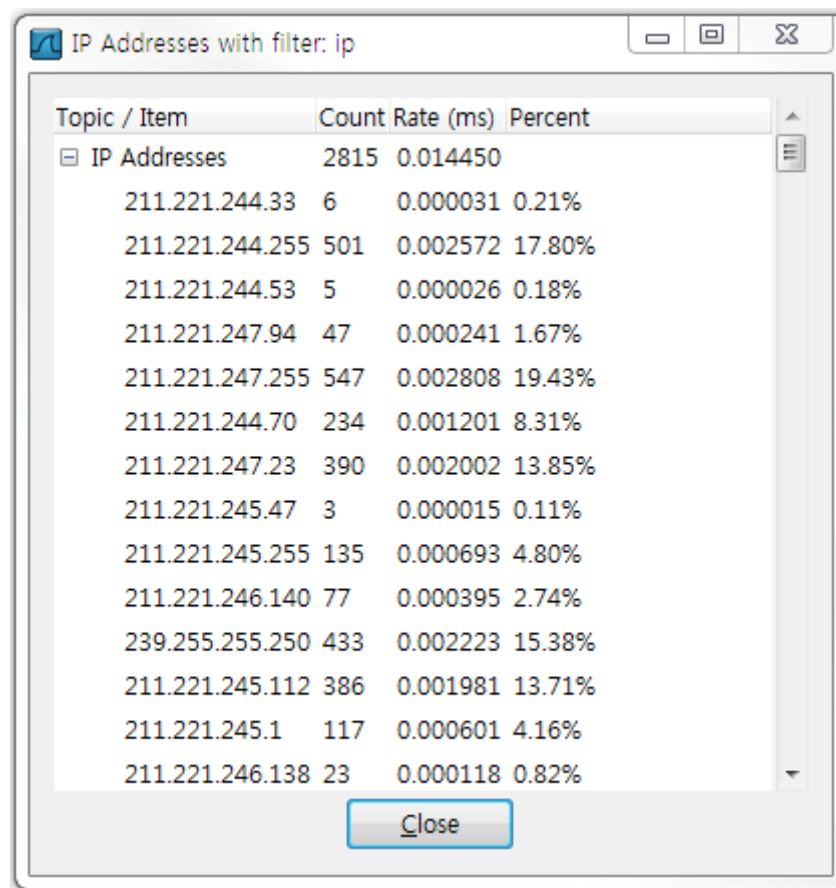
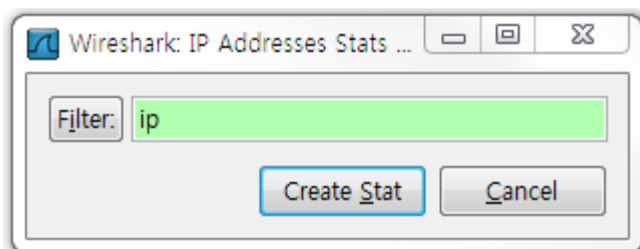
A window titled "HTTP/Load Distribution with filter: tcp". It displays a table with the following data:

Topic / Item	Count	Rate (ms)	Percent
[-] HTTP Requests by Server	11	0.000101	
[+] HTTP Requests by Server Address	11	0.000101	100.00%
[+] HTTP Requests by HTTP Host	11	0.000101	100.00%
[-] HTTP Responses by Server Address	11	0.000101	
[+] 218.153.8.121	3	0.000028	27.27%
[+] 74.125.224.133	1	0.000009	9.09%
[+] 74.125.127.101	5	0.000046	45.45%
[+] 84.16.88.15	2	0.000018	18.18%

At the bottom of the window is a "Close" button.

❑ IP address

- 패킷의 출발지/목적지 IP 주소를 보여줌

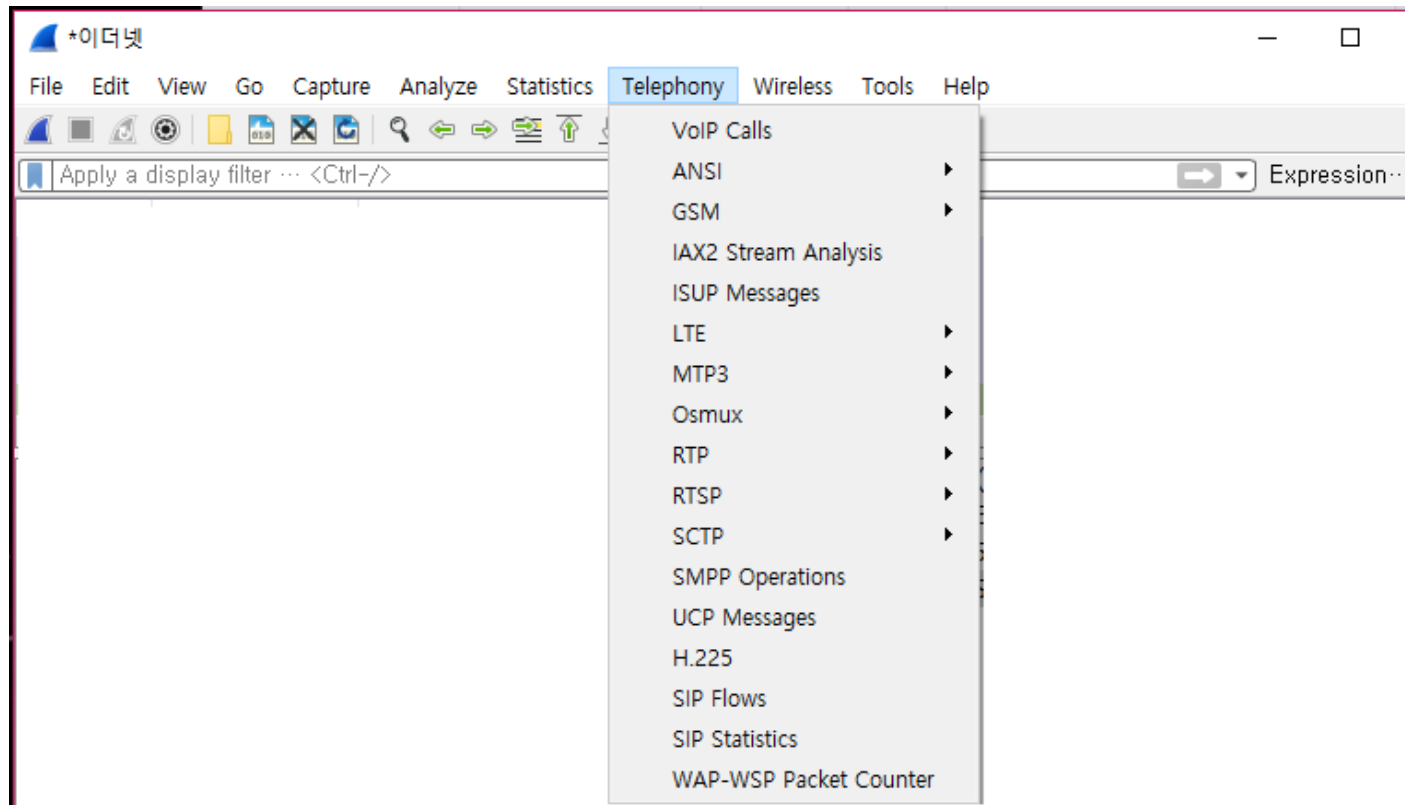


The image shows the 'IP Addresses with filter: ip' window. It displays a table with the following data:

Topic / Item	Count	Rate (ms)	Percent
IP Addresses	2815	0.014450	
211.221.244.33	6	0.000031	0.21%
211.221.244.255	501	0.002572	17.80%
211.221.244.53	5	0.000026	0.18%
211.221.247.94	47	0.000241	1.67%
211.221.247.255	547	0.002808	19.43%
211.221.244.70	234	0.001201	8.31%
211.221.247.23	390	0.002002	13.85%
211.221.245.47	3	0.000015	0.11%
211.221.245.255	135	0.000693	4.80%
211.221.246.140	77	0.000395	2.74%
239.255.255.250	433	0.002223	15.38%
211.221.245.112	386	0.001981	13.71%
211.221.245.1	117	0.000601	4.16%
211.221.246.138	23	0.000118	0.82%

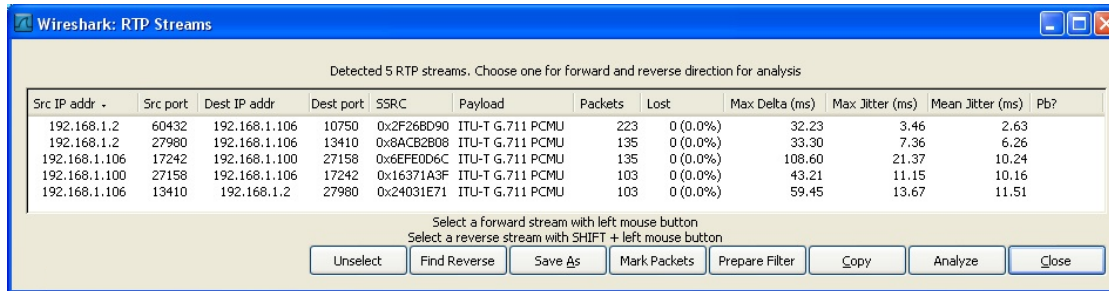
Telephony

❑ VoIP 트래픽 분석용 툴을 제공

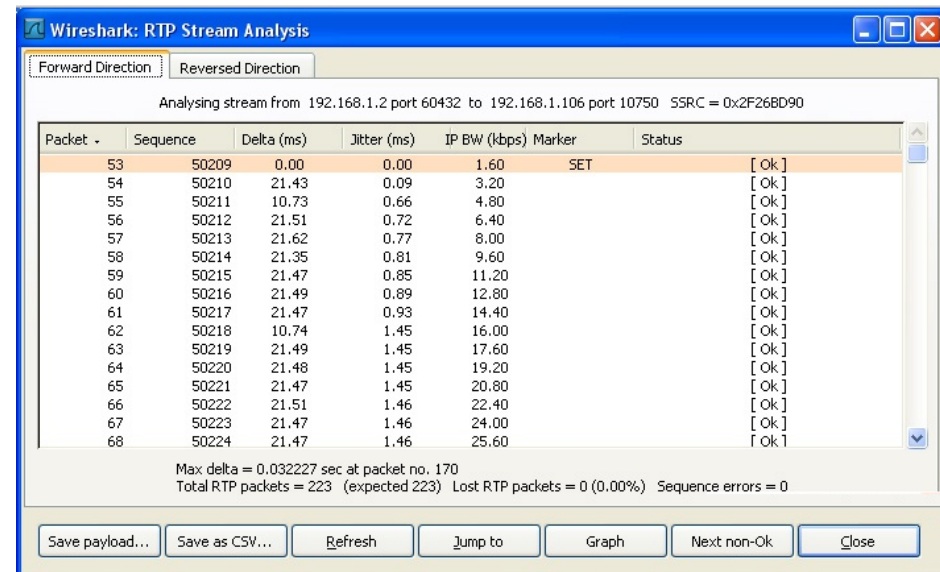


❑ RTP

- 음성/영상 통신용 프로토콜
 - UDP 위에서 실행
- signaling 작업을 제공하는 SIP나 H.323과 함께 연결하기 위해 종종 사용



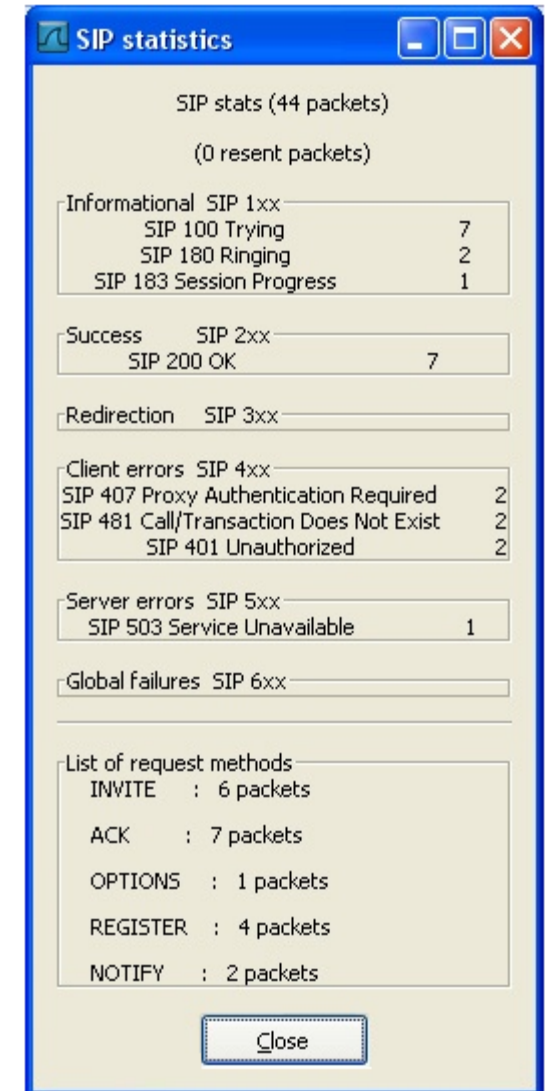
모든 스트림 보기



스트림 분석

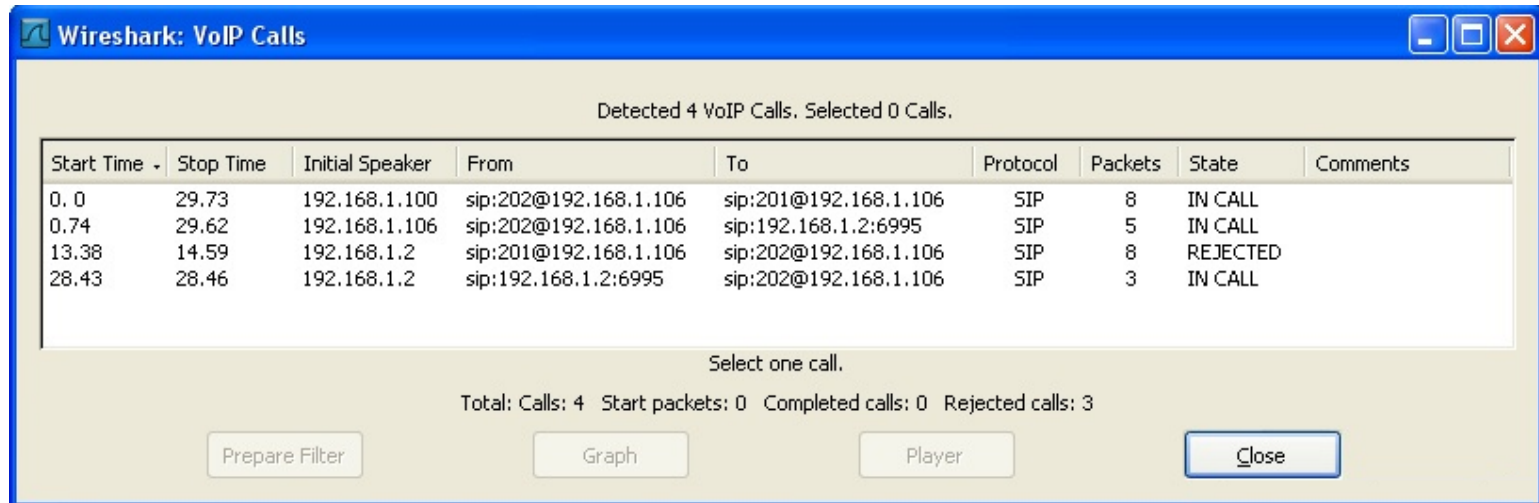
❑ SIP(Session Initiation Protocol)

- VoIP, 비디오 세션을 열기 위한 시그널링 프로토콜
- 멀티미디어 데이터 전송을 위한 RTP 프로토콜과 함께 동작



❑ VoIP Calls

- 시그널링 프로토콜: SIP, H.323
- 데이터 전송용 프로토콜: RTP



Wireshark: VoIP Calls

Detected 4 VoIP Calls. Selected 0 Calls.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
0.0	29.73	192.168.1.100	sip:202@192.168.1.106	sip:201@192.168.1.106	SIP	8	IN CALL	
0.74	29.62	192.168.1.106	sip:202@192.168.1.106	sip:192.168.1.2:6995	SIP	5	IN CALL	
13.38	14.59	192.168.1.2	sip:201@192.168.1.106	sip:202@192.168.1.106	SIP	8	REJECTED	
28.43	28.46	192.168.1.2	sip:192.168.1.2:6995	sip:202@192.168.1.106	SIP	3	IN CALL	

Select one call.

Total: Calls: 4 Start packets: 0 Completed calls: 0 Rejected calls: 3

Prepare Filter Graph Player Close

Assignment

❑ 웹 브라우저에서 어떤 홈페이지의 첫 페이지가 화면에 나오는 과정을 프로토콜 동작 관점에서 분석하시오

- 수업자료 2장(응용 계층) 20번 슬라이드 순서에 따라서 패킷을 분석한다
 - DNS 서버로부터 IP 주소 번역(DNS 메시지 송수신 과정)
 - 웹서버와 TCP 연결 설정(TCP three-way handshaking)
 - 수업자료 3장(전송 계층) 32~33번 슬라이드 참조
 - 웹서버로부터 http 프로토콜을 이용하여 메시지 송수신
 - 수업자료 2장 24, 26~32번 슬라이드 참조
 - 웹서버와 TCP 연결 해제 과정
 - 수업자료 3장 34~35번 슬라이드 참조
- 보고서 작성 방법
 - 10쪽 이내로 작성한다
 - 패킷 송수신 과정을 먼저 제시하고(흐름도), 각 패킷에서 중요한 필드를 설명한다
 - 모든 패킷을 분석할 필요는 없다
 - 장절/그림/표 목차, 맞춤법, 폰트 등 보고서 형식을 잘 갖출 것
- 참고
 - Wireshark를 실행하기 전에 인터넷 브라우저의 캐시를 삭제한다

□ 과제물 제출

- 팀 과제
- 배점: 10점
- 과제 제출 기한: 11월 24일(일) 자정
- 제출 방식
 - 사이버캠퍼스에 제출
 - 게시글 및 파일 이름은 아래 형식을 따름 (1인만 제출하면 됨)
 - 컴넷2019A_패킷분석_홍길동이순신 또는 컴넷2019B_패킷분석_홍길동이순신

Reference

- ❑ 와이어샹크를 이용한 네트워크 분석, 이재광, 맥그로힐
- ❑ 와이어샹크 네트워크 완전 분석, 에이콘출판사
- ❑ 와이어샹크를 활용한 실전 패킷 분석, 에이콘출판사
- ❑ <https://www.wireshark.org/docs/>

