

Wireshark 기초

송실대
정 규식

Wireshark ?

- [자유 및 오픈 소스 패킷 분석](#) 프로그램이다. [네트워크](#)의 문제, 분석, 소프트웨어 및 [통신 프로토콜](#) 개발, 교육에 쓰인다. 원래 이름은 **Ethereal**이었으나 2006년 5월에 상표 문제로 말미암아 와이어샤크로 이름을 바꾸었다.
- 와이어샤크는 [크로스 플랫폼](#)으로, [GTK+](#) [위젯 툴킷](#)을 이용하여 사용자 인터페이스를 제공하며, [pcap](#)을 이용하여 패킷을 포획한다. [리눅스](#), [맥 OS X](#), [BSD](#), [솔라리스](#)를 포함한 다양한 [유닉스 계열 운영 체제](#)와 [마이크로소프트 윈도우](#)에서 동작한다. GUI가 없는 터미널 기반 버전인 티샤크(TShark)도 제공한다. 와이어샤크, 또 TShark와 같은 프로그램과 함께 배포되는 여러 프로그램들은 [자유 소프트웨어](#)로, [GNU 일반 공중 사용 허가서](#)의 조건으로 공개된다.

목차

- 설치과정
- 핵심요소
- 패킷캡쳐
- 패킷필터
- 트래픽분석
- HTTP 패킷 따라가기

V 3.0.4 설치과정

1. <https://www.wireshark.org/download.html>
에 접속
2. 자신의 컴퓨터 운영체제에 맞는 옵션 선택
및 다운로드
3. 계속 next 선택
4. Packet Capture 설치단계에서 next 선택
5. 그냥 install 선택

<https://www.wireshark.org/download.html>에서 installer download

wireshark.org/download.html



NEWS

Get Acquainted ▾

Get Help ▾

Develop ▾

Project Host

SharkFest

Download Wireshark

The current stable release of Wireshark is 3.0.4. It supersedes all previous releases. You can also download the latest development release (3.1.0) and documentation.

Stable Release (3.0.4)

 **Windows Installer (64-bit)**

Windows Installer (32-bit)

Windows PortableApps® (32-bit)

macOS 10.12 and later Intel 64-bit .dmg

Source Code

Old Stable Release (2.6.11)

Development Release (3.1.0)

Documentation

Having Problems?

[Explore our download area](#) or look in our [third party package list](#) below.

Installation Notes

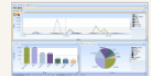
Go Beyond with Riverbed Technology

Riverbed is Wireshark's primary sponsor and provides our funding. They also make great products that fully integrate with Wireshark.

I have a lot of traffic...

ANSWER: SteelCentral™ Packet Analyzer PE

- Visually rich, powerful LAN analyzer
- Quickly access very large pcap files
- Professional, customizable reports
- Advanced triggers and alerts



[Learn More](#)

[Buy Now](#)

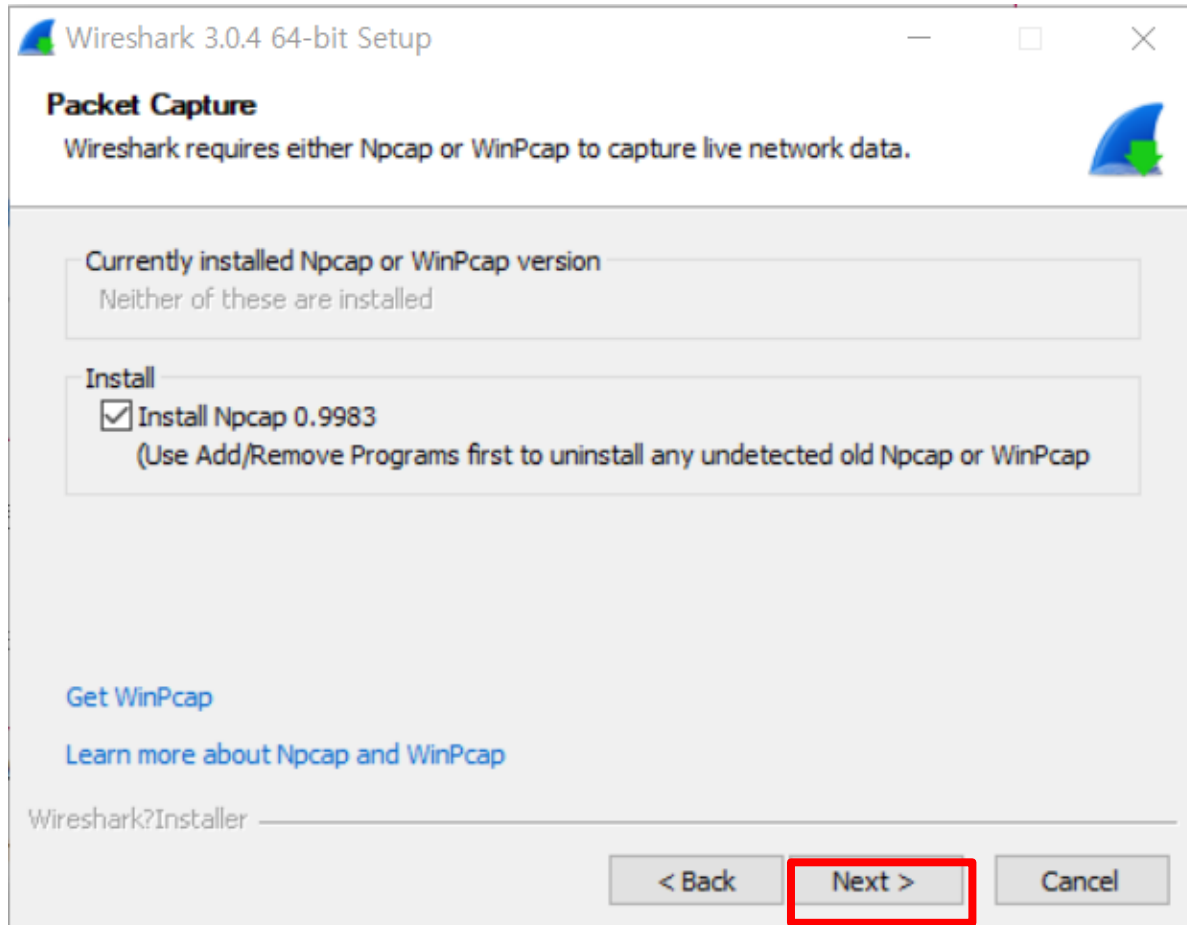
No, really, I have a LOT of traffic...

ANSWER: SteelCentral™ AppResponse 11

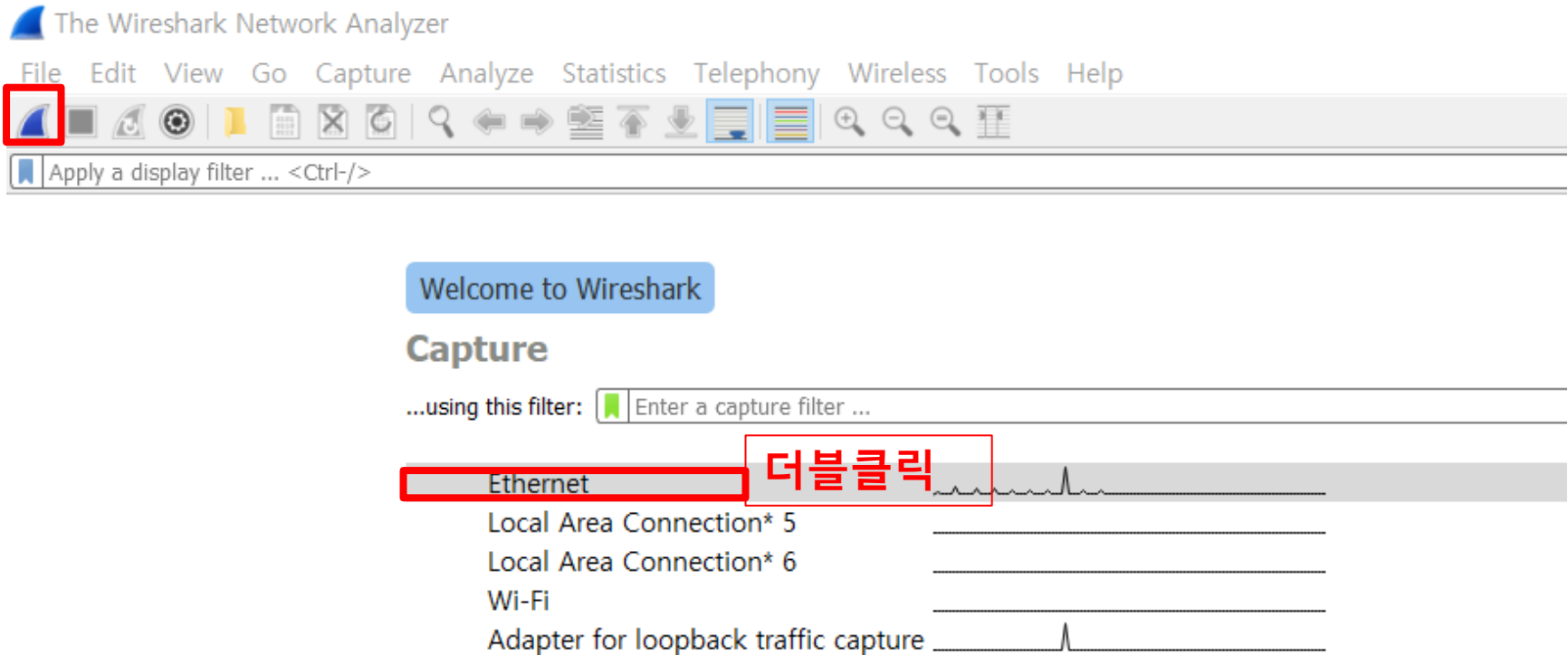
- Full stack analysis – from packets to pages
- Rich performance metrics & pre-defined insights for fast problem identification/resolution
- Modular, flexible solution for deeply-analyzing network & application performance

[Learn More](#)

설치과정중



설치후 초기화면



캡처 시작화면(예)

The screenshot displays the Microsoft Wi-Fi capture tool interface. The title bar reads "Capturing from Microsoft: Wi-Fi". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for capture and analysis, with a red square icon highlighted. Below the toolbar is a filter bar with the text "Apply a display filter ... <Ctrl-/>" and an "Expression..." field. The main packet list shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
53	8.986970	192.168.35.1	239.255.255.250	SSDP	384	NOTIFY * HTTP/1.1
54	10.009683	192.168.35.110	192.168.35.203	TCP	171	50531 → 8009 [PSH, ACK] Seq=235 Ack=235 Win=256 Len=117 [TCP segment of a reass...
55	10.015089	192.168.35.203	192.168.35.110	TCP	171	8009 → 50531 [PSH, ACK] Seq=235 Ack=352 Win=279 Len=117 [TCP segment of a reass...
56	10.056430	192.168.35.110	192.168.35.203	TCP	54	50531 → 8009 [ACK] Seq=352 Ack=352 Win=255 Len=0
57	15.017718	192.168.35.110	192.168.35.203	TCP	171	50531 → 8009 [PSH, ACK] Seq=352 Ack=352 Win=255 Len=117 [TCP segment of a reass...
58	15.020766	192.168.35.203	192.168.35.110	TCP	171	8009 → 50531 [PSH, ACK] Seq=352 Ack=469 Win=279 Len=117 [TCP segment of a reass...
59	15.062480	192.168.35.110	192.168.35.203	TCP	54	50531 → 8009 [ACK] Seq=469 Ack=469 Win=255 Len=0

Below the packet list, the details for Frame 1 are shown:

- > Frame 1: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface 0
- > Ethernet II, Src: IntelCor_03:10:f1 (b4:b6:76:03:10:f1), Dst: Google_b2:44:97 (30:fd:38:b2:44:97)
- > Internet Protocol Version 4, Src: 192.168.35.110, Dst: 192.168.35.203
- > Transmission Control Protocol, Src Port: 50531, Dst Port: 8009, Seq: 1, Ack: 1, Len: 117

The bottom section displays the raw packet data in hexadecimal and ASCII format. The status bar at the bottom indicates "Microsoft: Wi-Fi: <live capture in progress>", "Packets: 59 · Displayed: 59 (100.0%)", and "Profile: Default".

캡처 중지화면 (예)

*Microsoft: Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1508	51.221848	192.168.35.110	211.115.106.191	TCP	54	49792 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1509	51.223088	192.168.35.110	211.115.106.191	HTTP	427	GET /jk?c=62&p=GKKUEAKYH1ekm76UZGhRzxWngvYXOEQLKMBdLFw1WIg=&k=1 HTTP/1.1
1510	51.223089	192.168.35.110	211.115.106.191	HTTP	427	GET /jk?c=62&p=GKKUEAKYH1ekm76UZGhRzxWngvYXOEQLKMBdLFw1WIg=&k=1 HTTP/1.1
1511	51.227328	211.115.106.191	192.168.35.110	TCP	60	80 → 49792 [ACK] Seq=1 Ack=374 Win=30720 Len=0
1512	51.227900	211.115.106.191	192.168.35.110	TCP	60	80 → 49791 [ACK] Seq=1 Ack=374 Win=30720 Len=0
1513	51.230308	128.119.245.12	192.168.35.110	TCP	66	80 → 49790 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
1514	51.230466	192.168.35.110	128.119.245.12	TCP	54	49790 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1515	51.234052	211.115.106.191	192.168.35.110	HTTP	406	HTTP/1.1 200 OK

> Frame 59: 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits) on interface 0

> Ethernet II, Src: IntelCor_03:10:f1 (b4:b6:76:03:10:f1), Dst: Hfr_41:19:50 (00:23:aa:41:19:50)

> Internet Protocol Version 4, Src: 192.168.35.110, Dst: 211.115.106.206

> Transmission Control Protocol, Src Port: 49741, Dst Port: 80, Seq: 1, Ack: 1, Len: 333

> Hypertext Transfer Protocol

```
0000 00 23 aa 41 19 50 b4 b6 76 03 10 f1 08 00 45 00  ·#·A·P···v·····E·
0010 01 75 11 f6 40 00 80 06 c5 34 c0 a8 23 6e d3 73  ·u··@····4··#n·s
0020 6a ce c2 4d 00 50 f1 27 c3 90 d1 3b 5a 54 50 18  j··M·P·'···;ZTP·
0030 01 00 11 fd 00 00 47 45 54 20 2f 6a 6b 3f 63 3d  ·····GE T /jk?c=
0040 32 38 26 70 3d 47 4b 4b 55 45 41 6b 59 48 31 65  28&p=GKK UEAKYH1e
0050 6b 6d 37 36 55 5a 47 68 52 7a 78 57 6e 67 76 59  km76UZGh RzxWngvY
0060 58 4f 45 51 4c 4b 4d 42 64 4c 46 77 31 57 49 67  XOEQLKMB dLFw1WIg
0070 3d 26 6b 3d 31 20 48 54 54 50 2f 31 2e 31 0d 0a  =&k=1 HT TP/1.1·
0080 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 55 73 65  Accept: */*·Use
0090 72 2d 41 67 65 6e 74 3a 20 4d 65 44 43 6f 72 65  r-Agent: MeDCore
```

http filter 적용한 화면 (예)

The screenshot displays the Microsoft Wi-Fi network analysis tool interface. The top 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. The main window is divided into three sections: a packet list, a packet details pane, and a packet bytes pane.

The packet list section shows a table of captured packets. The 'http' filter is applied, as indicated by the red box around the filter name in the toolbar. The table columns are No., Time, Source, Destination, Protocol, Length, and Info. The packets are filtered to show only HTTP traffic.

No.	Time	Source	Destination	Protocol	Length	Info
59	2.784291	192.168.35.110	211.115.106.206	HTTP	387	GET /jk?c=28&p=GKKUEAkYH1ekm76UZGhRzxWngvYXOEQLKMBdLFw1WIg=&k=1 HTTP/1.1
61	2.787796	211.115.106.206	192.168.35.110	HTTP	367	HTTP/1.1 200 OK
74	8.434232	192.168.35.110	211.115.106.206	HTTP	387	GET /jk?c=28&p=GKKUEAkYH1ekm76UZGhRzxWngvYXOEQLKMBdLFw1WIg=&k=1 HTTP/1.1
76	8.440615	211.115.106.206	192.168.35.110	HTTP	367	HTTP/1.1 200 OK
83	9.327803	192.168.35.110	192.168.35.1	HTTP	252	GET /rootDesc.xml HTTP/1.1
87	9.332733	192.168.35.1	192.168.35.110	HTTP/...	403	HTTP/1.1 200 OK
95	9.639627	192.168.35.110	192.168.35.1	HTTP	252	GET /rootDesc.xml HTTP/1.1
99	9.642015	192.168.35.1	192.168.35.110	HTTP/...	403	HTTP/1.1 200 OK

The packet details pane shows the details for the selected packet (Frame 59). It includes the following information:

- Frame 59: 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits) on interface 0
- Ethernet II, Src: IntelCor_03:10:f1 (b4:b6:76:03:10:f1), Dst: Hfr_41:19:50 (00:23:aa:41:19:50)
- Internet Protocol Version 4, Src: 192.168.35.110, Dst: 211.115.106.206
- Transmission Control Protocol, Src Port: 49741, Dst Port: 80, Seq: 1, Ack: 1, Len: 333
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the selected packet in hexadecimal and ASCII format.

```
0000 00 23 aa 41 19 50 b4 b6 76 03 10 f1 08 00 45 00  ·#·A·P···v·····E·
0010 01 75 11 f6 40 00 80 06 c5 34 c0 a8 23 6e d3 73  ·u··@··· ·4··#n·s
0020 6a ce c2 4d 00 50 f1 27 c3 90 d1 3b 5a 54 50 18  j··M·P·'···;ZTP·
0030 01 00 11 fd 00 00 47 45 54 20 2f 6a 6b 3f 63 3d  ······GE T /jk?c=
0040 32 38 26 70 3d 47 4b 4b 55 45 41 6b 59 48 31 65  28&p=GKK UEAkYH1e
0050 6b 6d 37 36 55 5a 47 68 52 7a 78 57 6e 67 76 59  km76UZGh RzxWngvY
0060 58 4f 45 51 4c 4b 4d 42 64 4c 46 77 31 57 49 67  XOEQLKMB dLFw1WIg
0070 3d 26 6b 3d 31 20 48 54 54 50 2f 31 2e 31 0d 0a  =&k=1 HT TP/1.1·
0080 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 55 73 65  Accept: /*···Use
0090 72 2d 41 67 65 6e 74 3a 20 4d 65 44 43 6f 72 65  r-Agent: MeDCore
```

HTTP GET 패킷 클릭 (예)

The image shows a Wireshark packet capture window. The main pane displays a list of captured packets. Packet 1502 is selected, and its details pane is expanded to show the Hypertext Transfer Protocol section. The packet list pane shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
1381	43.644810	192.168.35.110	211.115.106.191	HTTP	387	GET /jk?c=43&p=GKKUEAKYH1ekm76UZGhRzxWngvYXOEQLKMBdLFw1Wlg=&k=1 HTTP/1.1
1383	43.650000	211.115.106.191	192.168.35.110	HTTP	244	HTTP/1.1 200 OK
1502	51.213339	192.168.35.110	128.119.245.12	HTTP	587	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

The details pane for packet 1502 shows the following structure:

- Frame 1502: 587 bytes on wire (4696 bits), 587 bytes captured (4696 bits) on interface 0
- Ethernet II, Src: IntelCor_03:10:f1 (b4:b6:76:03:10:f1), Dst: Hfr_41:19:50 (00:23:aa:41:19:50)
- Internet Protocol Version 4, Src: 192.168.35.110, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 49788, Dst Port: 80, Seq: 1, Ack: 1, Len: 533
- Hypertext Transfer Protocol

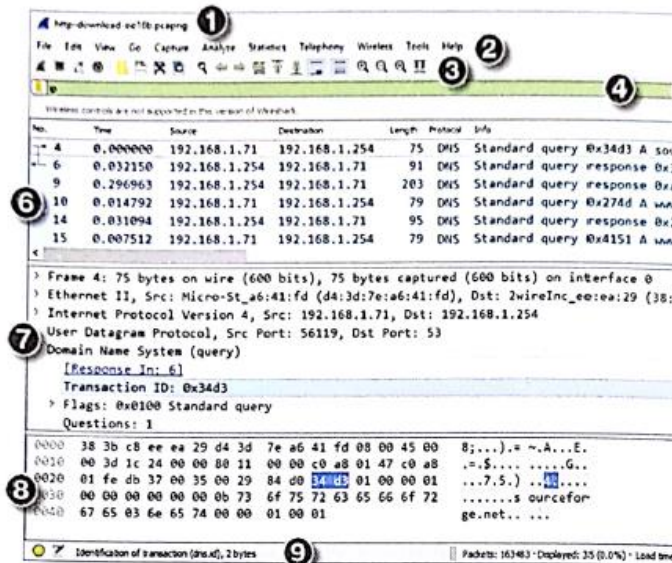
The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII column shows the following text:

```
..#A.P.. v....E-  
..=Qg@... M...#n-w  
...|.P^...z P-  
.....GE T /wires  
hark-lab s/INTRO-  
wireshar k-file1.  
html HTTP/1.1..H  
ost: gai a.cs.uma  
ss.edu.. Connecti  
on: keep -alive..  
Upgrade- Insecure
```

목차

- 설치과정
- 핵심요소
- 패킷캡쳐
- 패킷필터
- 트래픽분석
- HTTP 패킷 따라가기

주요 GUI 요소
















- ❶ 타이틀 바(Title Bar) 추적 파일 이름, 캡처 소스 또는 'The Wireshark Network Analyzer'라는 제목이 나타난다.
- ❷ 메인 메뉴(Main Menu) 표준 메뉴가 나타난다.
- ❸ 메인 툴바(Main Toolbar) 이 아이콘 버튼을 사용하려면 배워야 한다.
- ❹ 디스플레이 필터 영역과 필터 표현식 영역(Display Filter Area and Filter Expressions Area) 특정 트래픽에 초점을 맞춘다.
- ❺ 무선 툴바(Wireless Toolbar) 802.11 설정을 규정한다.
- ❻ 패킷 목록 창(Packet List Pane) 프레임 관련 지시기와 각 프레임을 요약한다.
- ❼ 패킷 상세 창(Packet Details Pane) 분석된 프레임들이 나타난다.
- ❽ 패킷 바이트 창(Packet Bytes Pane) 16진수와 ASCII 값으로 표현된 상세한 내용이 나타난다.
- ❾ 상태 바(Status Bar) 전문가, 주식, 패킷 개수, 프로파일에 대한 액세스가 나타난다.

Wireshark main menu

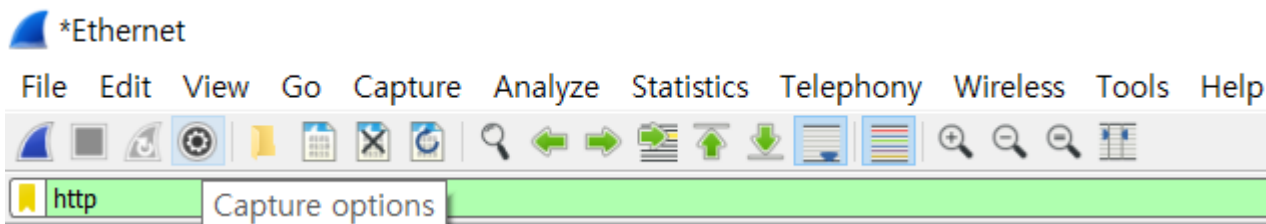
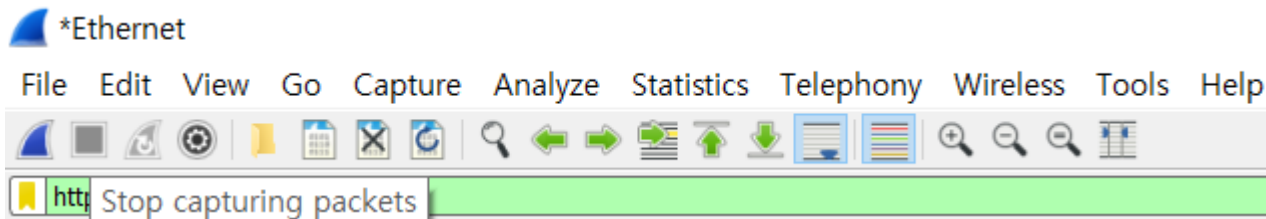
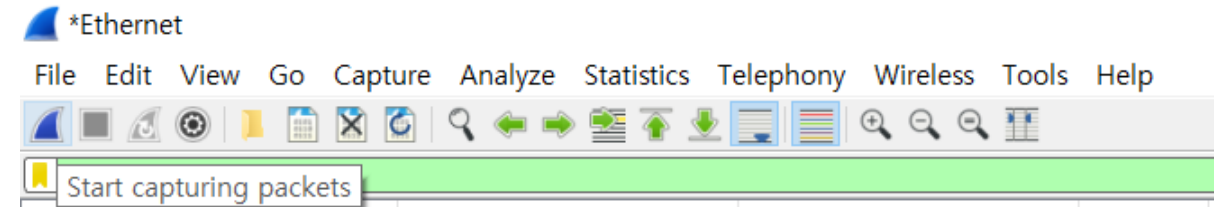
File Edit View Go Capture Analyze Statistics Telephony Tools Help

- File : 캡처 파일 관련 메뉴 (열기, 저장, 합치기 등)
- Edit : 패킷의 내용을 찾거나 각 패킷을 체크하여 따로 저장하는 기능 관련 메뉴
(검색 시 Hex, String등으로 원하는 패킷을 찾을 수 있음
패킷을 토글(체크)하여 File 메뉴에서 토글 한 패킷만 따로 저장 가능)
- View : 보기 관련 메뉴 (GUI 설정, 패킷 색깔 표시 설정등)
- Go : 패킷 이동 관련 메뉴 (위아래, 맨처음 , 맨끝 패킷으로 이동)
- Capture : 캡처 관련 메뉴 (카드 선택, 옵션 설정, 필터, 시작, 멈춤, 재시작)
- Analyze : 패킷 분석 관련 메뉴 (화면 출력 필터, 디코딩, 스트림 추적등)
- Statistic : 통계 관련 메뉴 (요약, 프로토콜별 통계, 입출력 그래프, 응답시간, 패킷길이 등)
- Telephony : 전화 관련 메뉴 (각종 음성관련 프로토콜 패킷을 분석)
- Tools : 방화벽 정책 생성 메뉴
- Help : 도움말 관련 메뉴

Wireshark main toolbar

-  Start : 캡처를 시작한다.
-  Stop : 캡처를 중지한다.
-  Restart : 캡처를 다시 시작한다.
-  Open : 저장된 파일을 열때 사용한다.
-  Open Recent : 최근에 열었던 파일을 열때 사용한다.
-  Close : 현재 캡처 하고 있는 화면을 닫는다.
-  Reload this capture file : pcap파일을 새로고침한다.
-  Find Packet.. : 특정 패킷을 찾을수 있다.
-  Back : 이전에 선택된 패킷으로 돌아간다.
-  Forward : 돌아오기전에 선택되었던 앞의 패킷으로 돌아간다.
-  Go to Packet... : Packet 의 앞부분에 써있는 Number 로 Packet 을 찾을수 있다.
-  First Packet : 모든 패킷의 가장 상단 패킷으로 이동한다.
-  Last Packet : 모든 패킷의 가장 하단 패킷으로 이동한다.

Wireshark main toolbar



Packet Pane(창)

The screenshot displays the Wireshark interface with the Packet Pane expanded. The top section, labeled "Packet List Pane", shows a list of captured packets. The second packet is selected, and its details are shown in the "Packet Details Pane". The raw packet bytes are displayed in the "Packet Bytes Pane" at the bottom.

Packet List Pane

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.173.220	75.75.75.75	DNS	74	Standard query 0xae0b A www.
2	0.013237	75.75.75.75	24.6.173.220	DNS	154	Standard query response 0xae0b
3	0.013971	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x4552 AAAA ..
4	0.027695	75.75.75.75	24.6.173.220	DNS	102	Standard query response 0x4552
5	0.028699	24.6.173.220	74.125.224.80	TCP	66	35145 → 80 [SYN, ACK] Seq=0 /
6	0.046071	74.125.224.80	24.6.173.220	TCP	66	80 → 35145 [SYN, ACK] Seq=0 /
7	0.046258	24.6.173.220	74.125.224.80	TCP	54	35145 → 80 [ACK] Seq=1 Ack=1
8	0.046998	24.6.173.220	74.125.224.80	HTTP	342	GET / HTTP/1.1

Packet Details Pane

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on inter...
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:..
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 51724 (51724), Dst Port: 53 (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0xae0b
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0

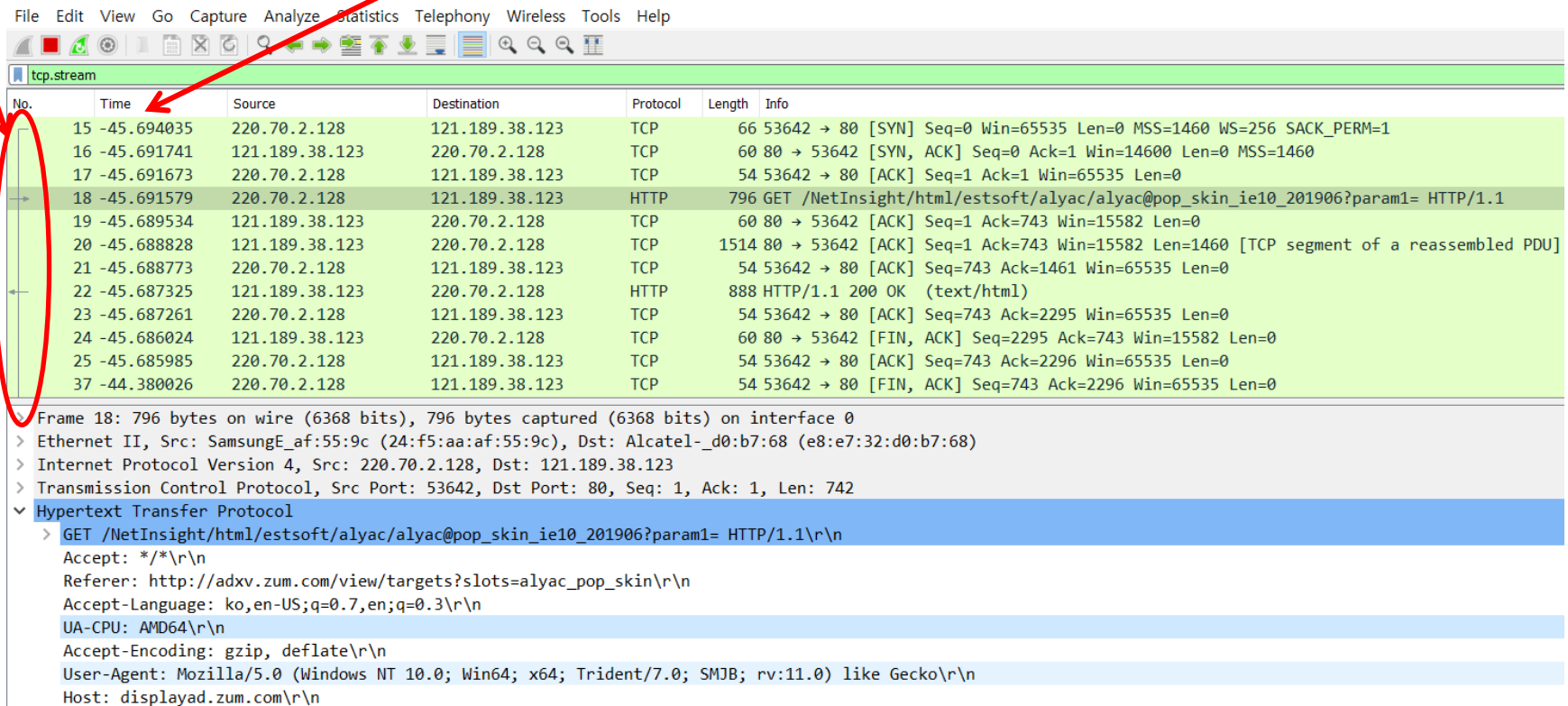
Packet Bytes Pane

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..\1.... d....E.
0010 00 3c 08 3d 00 00 80 11 00 00 18 06 ad dc 4b 4b ..K..
0020 4b 4b ca 0c 00 35 00 28 5c b2 ae 0b 01 00 00 ..K..
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 ..
0040 65 03 63 6f 6d 00 00 01 00 01 ..e.com... ..

Packet List Pane

Time 정보: No=1 패킷 도착 시점을 기준으로 상대적인 delay

패킷지시기



tcp.stream

No.	Time	Source	Destination	Protocol	Length	Info
15	-45.694035	220.70.2.128	121.189.38.123	TCP	66	53642 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	-45.691741	121.189.38.123	220.70.2.128	TCP	60	80 → 53642 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
17	-45.691673	220.70.2.128	121.189.38.123	TCP	54	53642 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
18	-45.691579	220.70.2.128	121.189.38.123	HTTP	796	GET /NetInsight/html/estsoft/alyac/alyac@pop_skin_ie10_201906?param1= HTTP/1.1
19	-45.689534	121.189.38.123	220.70.2.128	TCP	60	80 → 53642 [ACK] Seq=1 Ack=743 Win=15582 Len=0
20	-45.688828	121.189.38.123	220.70.2.128	TCP	1514	80 → 53642 [ACK] Seq=1 Ack=743 Win=15582 Len=1460 [TCP segment of a reassembled PDU]
21	-45.688773	220.70.2.128	121.189.38.123	TCP	54	53642 → 80 [ACK] Seq=743 Ack=1461 Win=65535 Len=0
22	-45.687325	121.189.38.123	220.70.2.128	HTTP	888	HTTP/1.1 200 OK (text/html)
23	-45.687261	220.70.2.128	121.189.38.123	TCP	54	53642 → 80 [ACK] Seq=743 Ack=2295 Win=65535 Len=0
24	-45.686024	121.189.38.123	220.70.2.128	TCP	60	80 → 53642 [FIN, ACK] Seq=2295 Ack=743 Win=15582 Len=0
25	-45.685985	220.70.2.128	121.189.38.123	TCP	54	53642 → 80 [ACK] Seq=743 Ack=2296 Win=65535 Len=0
37	-44.380026	220.70.2.128	121.189.38.123	TCP	54	53642 → 80 [FIN, ACK] Seq=743 Ack=2296 Win=65535 Len=0

Frame 18: 796 bytes on wire (6368 bits), 796 bytes captured (6368 bits) on interface 0

- > Ethernet II, Src: SamsungE_af:55:9c (24:f5:aa:af:55:9c), Dst: Alcatel-_d0:b7:68 (e8:e7:32:d0:b7:68)
- > Internet Protocol Version 4, Src: 220.70.2.128, Dst: 121.189.38.123
- > Transmission Control Protocol, Src Port: 53642, Dst Port: 80, Seq: 1, Ack: 1, Len: 742
- > Hypertext Transfer Protocol
 - > GET /NetInsight/html/estsoft/alyac/alyac@pop_skin_ie10_201906?param1= HTTP/1.1\r\n
 - Accept: */*\r\n
 - Referer: http://adxv.zum.com/view/targets?slots=alyac_pop_skin\r\n
 - Accept-Language: ko,en-US;q=0.7,en;q=0.3\r\n
 - UA-CPU: AMD64\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; SMJB; rv:11.0) like Gecko\r\n
 - Host: displayad.zum.com\r\n

패킷지시기

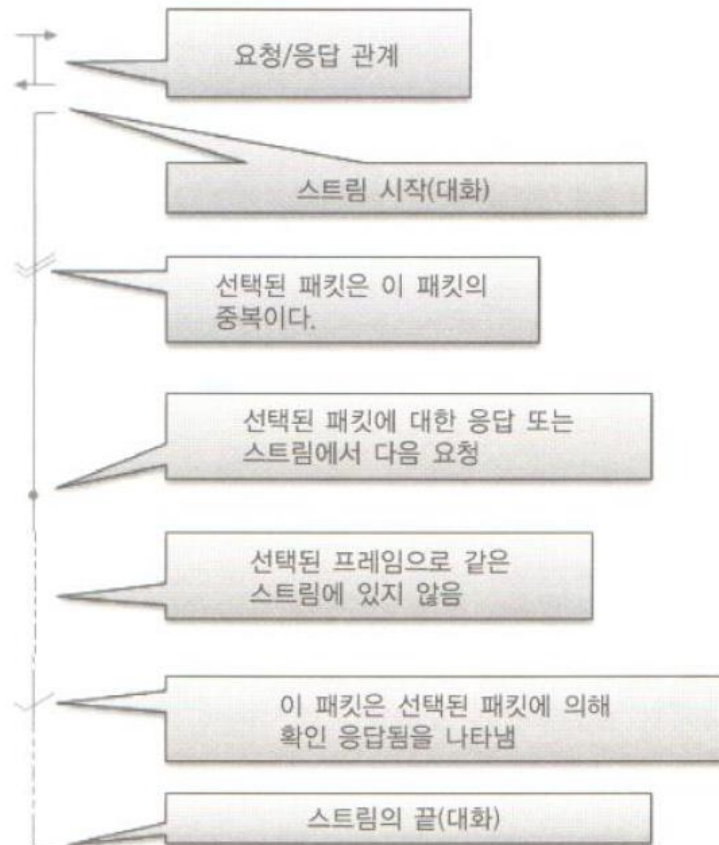


그림 13 관련된 패킷 지시기는 관련 패킷을 빨리 찾는 데 도움이 된다.

Packet Details Pane

```

+ Frame 1827: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0
+ Ethernet II, Src: DellEsgP_94:d1:3f (00:0f:1f:94:d1:3f), Dst: Elitegro_5f:20:e5 (c8:9c:dc:5
+ Internet Protocol Version 4, Src: 10.56.208.251 (10.56.208.251), Dst: 10.56.208.216 (10.56.
+ Transmission Control Protocol, Src Port: 9082 (9082), Dst Port: 49168 (49168), Seq: 1, Ack:
+ Hypertext Transfer Protocol
  
```

프레임 섹션은
와이어샹크가
보여주는
메타데이터가
들어있다.

패킷

세그먼트

```

* Frame 2284: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on
  Interface id: 0 (\Device\NPF_{98657C67-2DE2-4C46-B5FE-5101D6F0227D})
  Encapsulation type: Ethernet (1)
  Arrival Time: Dec 2, 2015 19:14:36.182840000 Pacific Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1449112476.182840000 seconds
  [Time delta from previous captured frame: 0.000139000 seconds]
  [Time delta from previous displayed frame: 2.561500000 seconds]
  [Time since reference or first frame: 10.111596000 seconds]
  Frame Number: 2284
  Frame Length: 345 bytes (2760 bits)
  Capture Length: 345 bytes (2760 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
  * Ethernet II, Src: GemtekTe_cc:7d:da (20:10:7a:cc:7d:da), Dst: HonHaiPr_fa:0e
  * Internet Protocol Version 4, Src: 192.168.44.7, Dst: 198.66.239.146
  * Transmission Control Protocol, Src Port: 26170 (26170), Dst Port: 80 (80), S
  * Hypertext Transfer Protocol
    GET / HTTP/1.1\r\n
    Host: www.chappellu.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:42.0) Gecko/20100101 Fi
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.chappellu.com/]
  
```

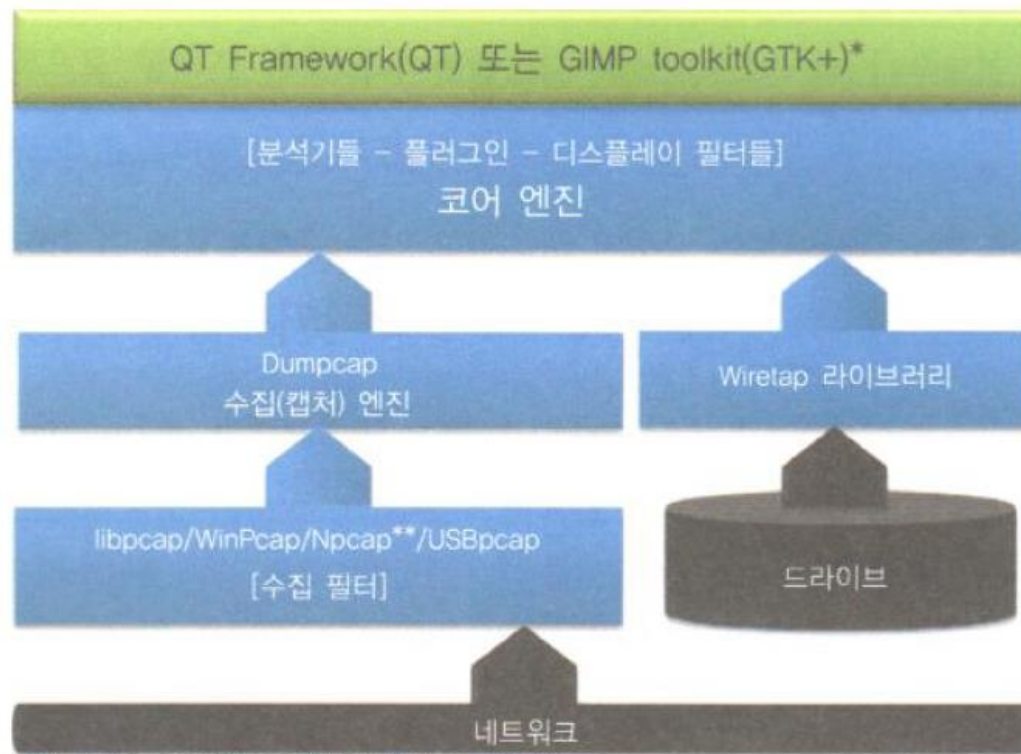

Packet Bytes Pane

0000	d8	cb	8a	c7	81	76	00	90	0b	26	c7	e5	08	00	45	00v...&....E.
0010	01	d8	2c	0a	40	00	34	06	28	b6	67	06	ae	11	0a	38	...,.@.4. (.g....8
0020	d1	10	00	50	c2	37	06	11	61	ac	1c	96	9b	bb	50	18	...P.7.. a.....P.
0030	00	87	70	81	00	00	48	54	54	50	2f	31	2e	31	20	32	..p...HT TP/1.1 2
0040	30	30	20	4f	4b	0d	0a	44	61	74	65	3a	20	57	65	64	00 OK..D ate: wed
0050	2c	20	32	33	20	44	65	63	20	32	30	31	35	20	30	34	, 23 Dec 2015 04
0060	3a	33	39	3a	32	38	20	47	4d	54	0d	0a	53	65	72	76	:39:28 G MT..Serv
0070	65	72	3a	20	41	70	61	63	68	65	0d	0a	43	61	63	68	er: Apac he..Cach
0080	65	2d	63	6f	6e	74	72	6f	6c	3a	20	6e	6f	2d	63	61	e-contro l: no-ca
0090	63	68	65	2c	20	6e	6f	2d	73	74	6f	72	65	2c	20	6d	che, no- store, m
00a0	75	73	74	2d	72	65	76	61	6c	69	64	61	74	65	0d	0a	ust-reva lidaate..
00b0	50	72	61	67	6d	61	3a	20	6e	6f	2d	63	61	63	68	65	Pragma: no-cache
00c0	0d	0a	50	33	50	3a	20	43	50	3d	22	41	4c	4c	20	43	..P3P: C P="ALL C
00d0	55	52	61	20	41	44	4d	61	20	44	45	56	61	20	54	41	URa ADMa DEVa TA
00e0	49	61	20	4f	55	52	20	42	55	53	20	49	4e	44	20	50	Ia OUR B US IND P



Wireshark 내부구조

- 수집(캡처) 프로세스는 특수 링크 계층 드라이버에 의존
- Dumpcap 수집엔진은 정지조건을 지정



* GTK 지원은 와이어샤크 v2에서 언젠가는 중지될 것이다.

** 와이어샤크 v2의 초기 버전은 Npcap이 포함돼 있지 않다(자세한 정보는 Npcap.org를 방문하라).

목차

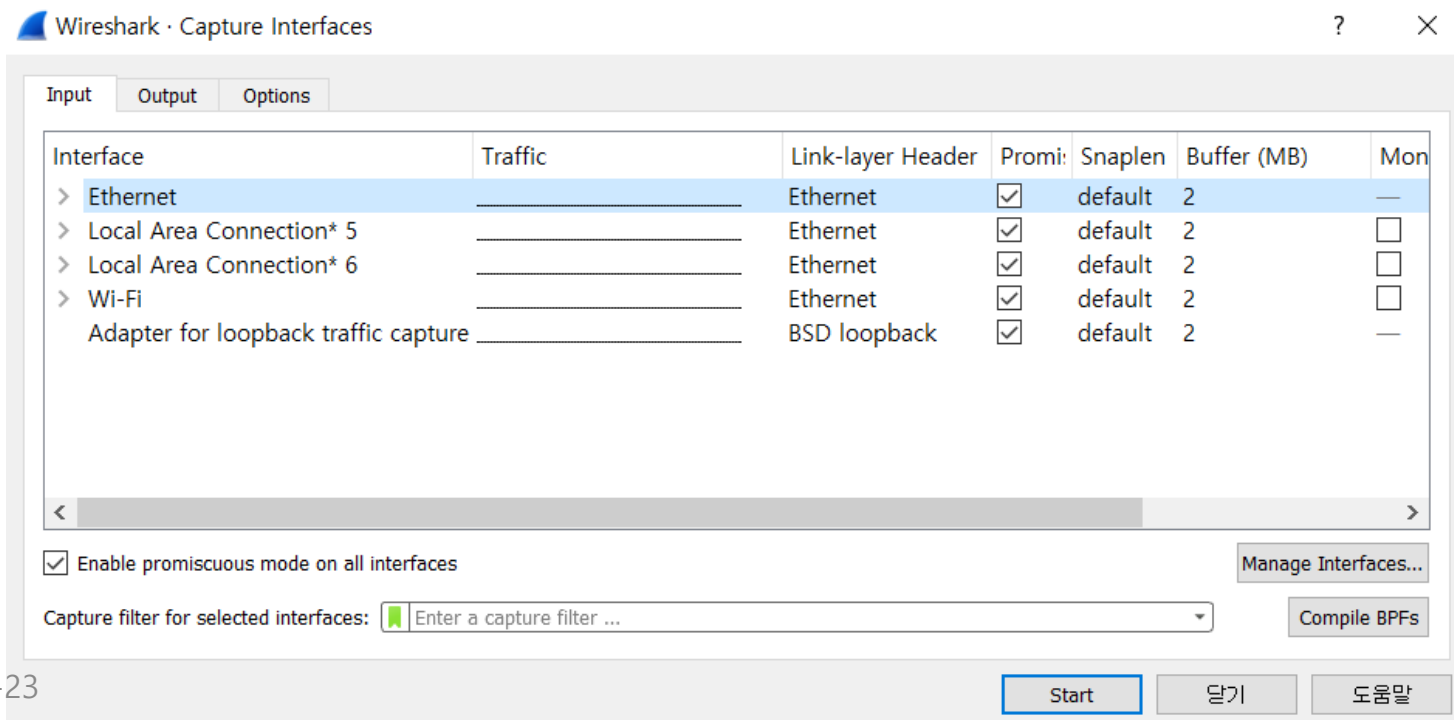
- 설치과정
- 핵심요소
- 패킷캡쳐
- 패킷필터
- 트래픽분석
- HTTP 패킷 따라가기

패킷캡쳐

1. 실시간 캡쳐
 2. 저장된 file 불러오기
(**확장자 pcap or pcapng**)
- 캡쳐후 GUI 화면 나옴

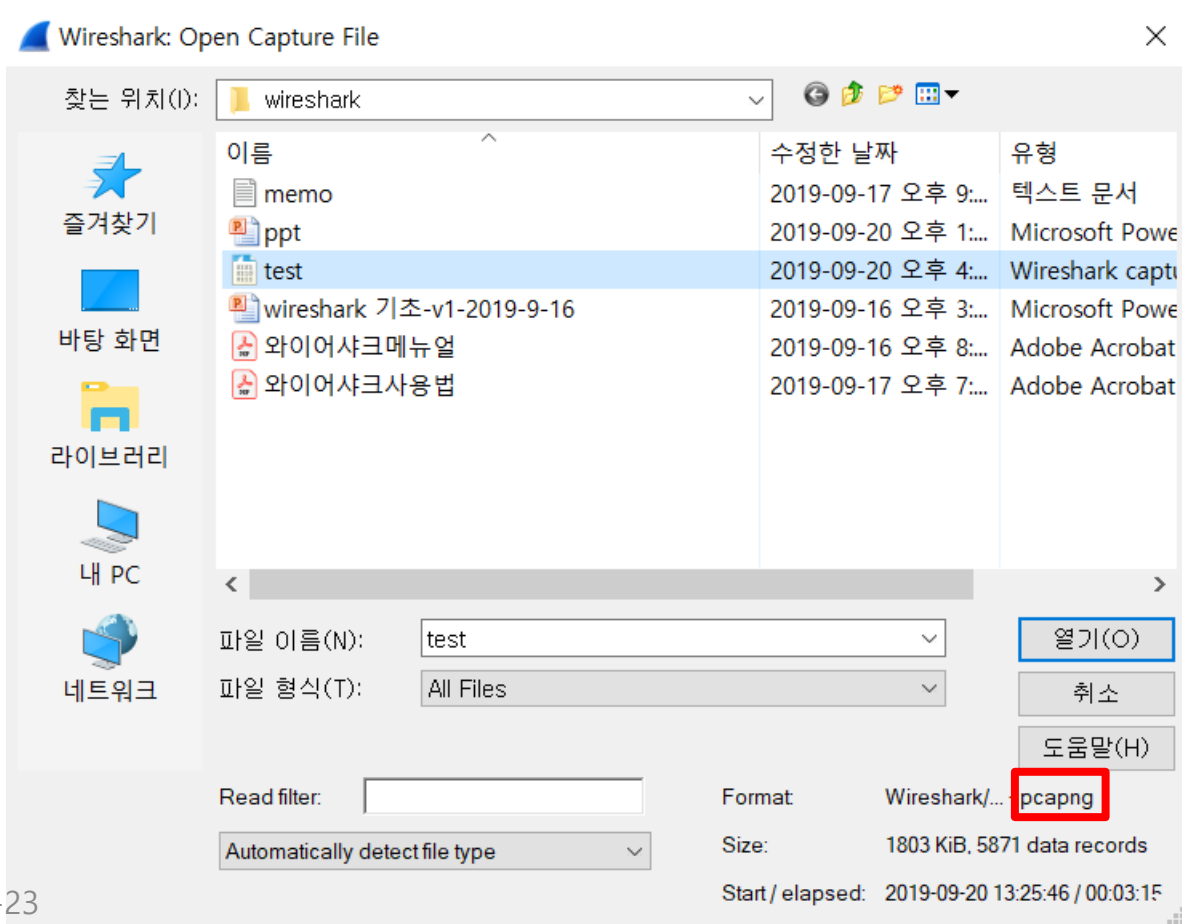
실시간 패킷캡처

- Main 화면에서  단축키 누르기
- Main menu에서 capture – options 선택후 Start 클릭



캡처된 file 불러오기 (확장자: pcapng)

- Main menu에서 File - open 선택



목차

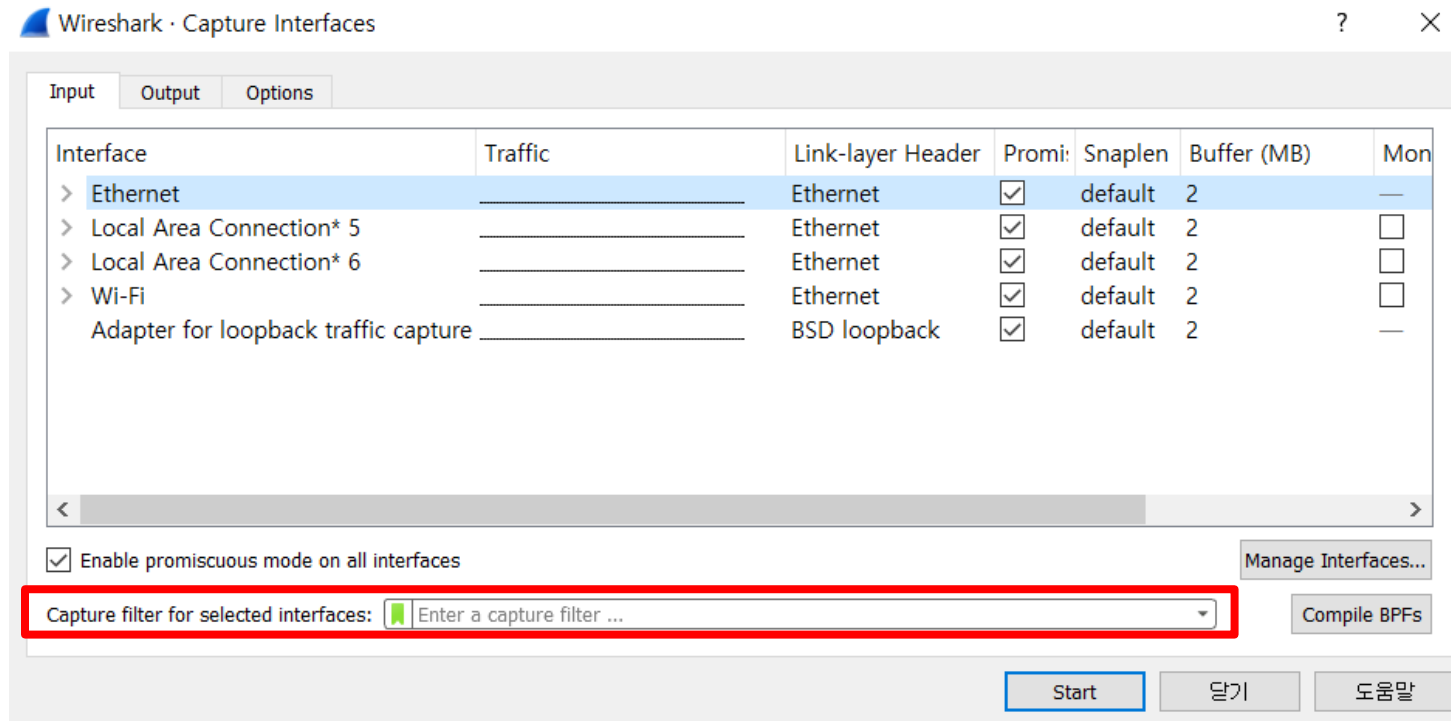
- 설치과정
- 핵심요소
- 패킷캡쳐
- 패킷필터
- 트래픽분석
- HTTP 패킷 따라가기

패킷 필터

1. 캡처시 필터
2. 화면 display시 필터

캡처시 패킷필터

- Main menu에서 capture – options



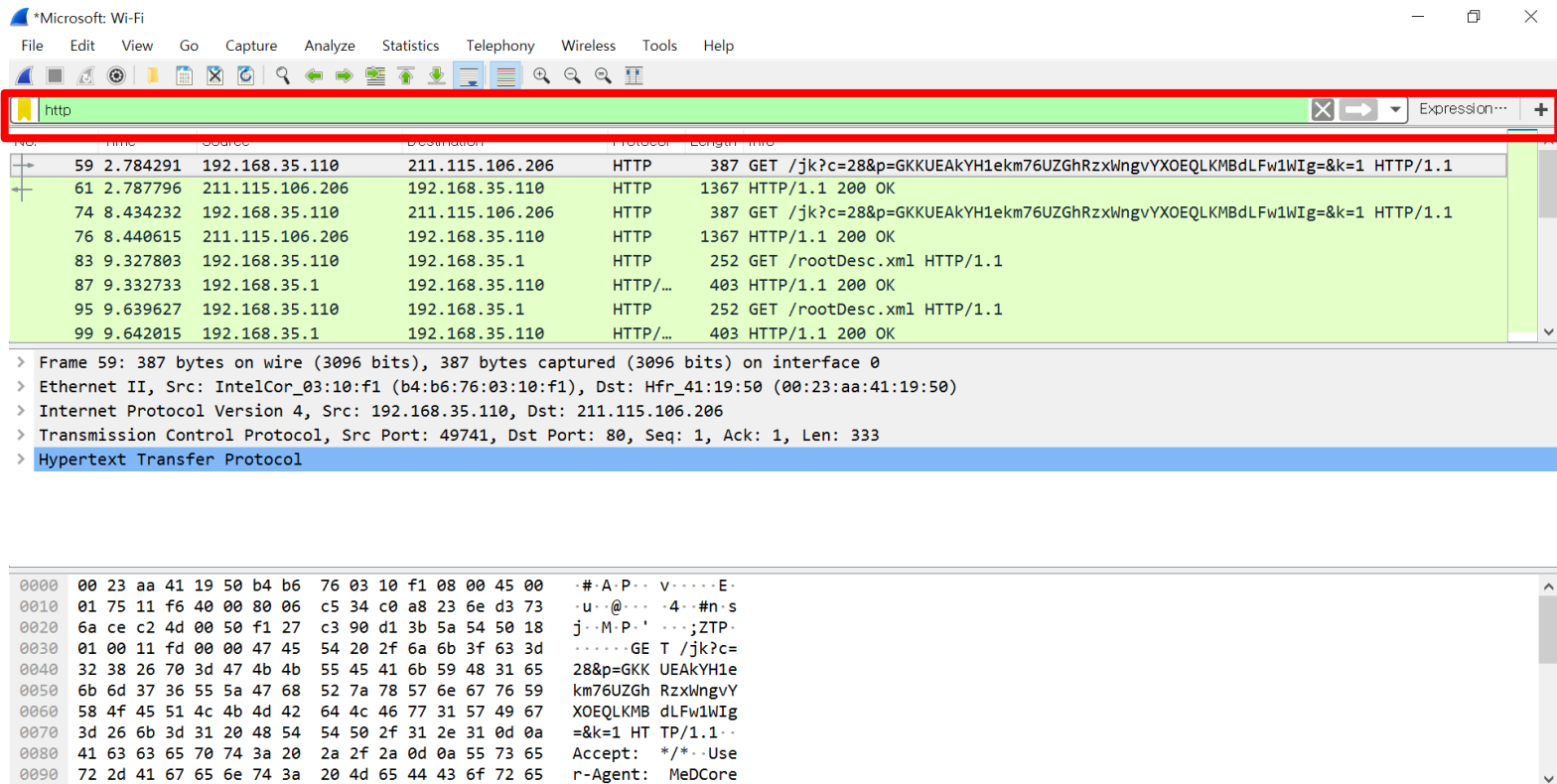
필터링 캡처 예제

- 특정 호스트의 패킷 캡처
 - host 10.10.50.170
- 특정 두 호스트의 통신 패킷 캡처
 - host 10.10.50.170 and host 10.10.50.15
- 특정 포트 패킷 캡처
 - port 80
- 특정 두 포트 전부 패킷 캡처
 - port 80 or port 1770
- 특정 호스트의 특정 포트 패킷 캡처
 - host 10.10.50.170 and port 80
- 특정 패킷만 캡처 안함
 - not arp

➤ 더 많은 예제는 다음 링크를 참조한다.
<http://wiki.wireshark.org/CaptureFilters>

화면 display시 패킷필터

- Main menu에서 analyze – Display Filters



Display 필터 툴바 사용법

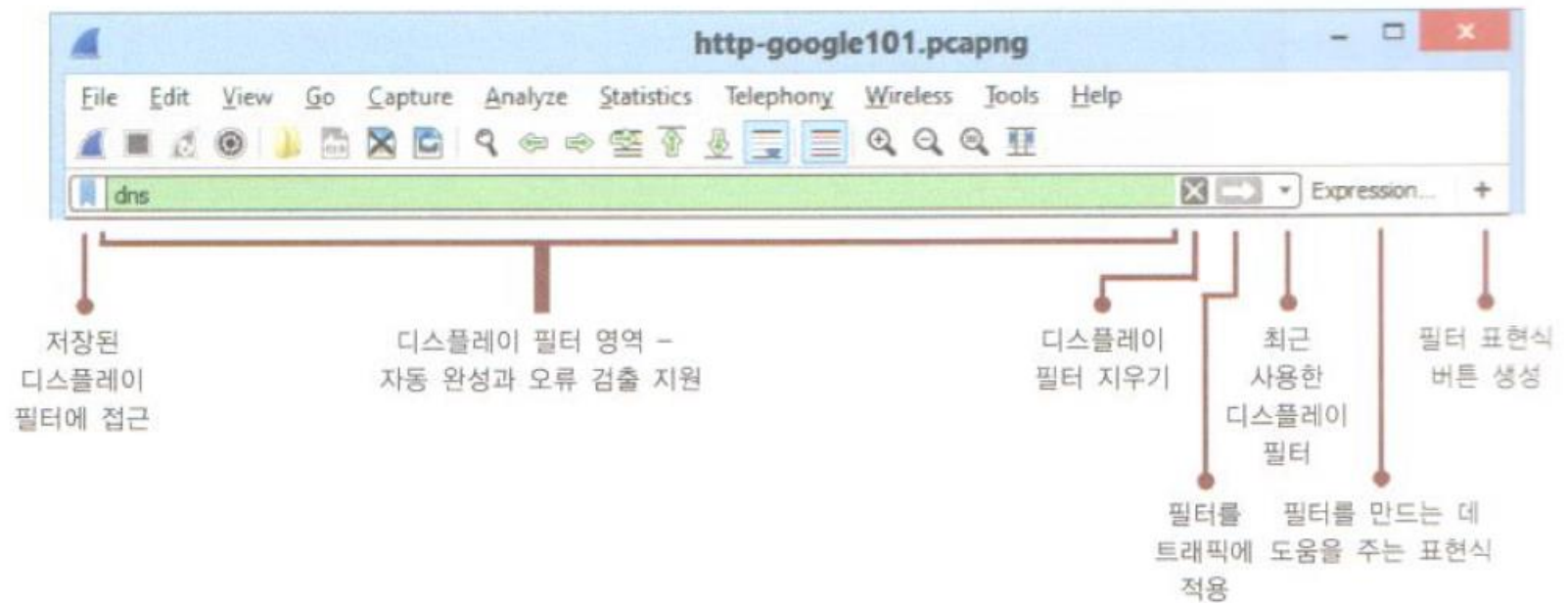


그림 10 트래픽 분석 시간을 줄이려면 디스플레이 필터 툴바의 사용법을 배우라.

상태 바 활용

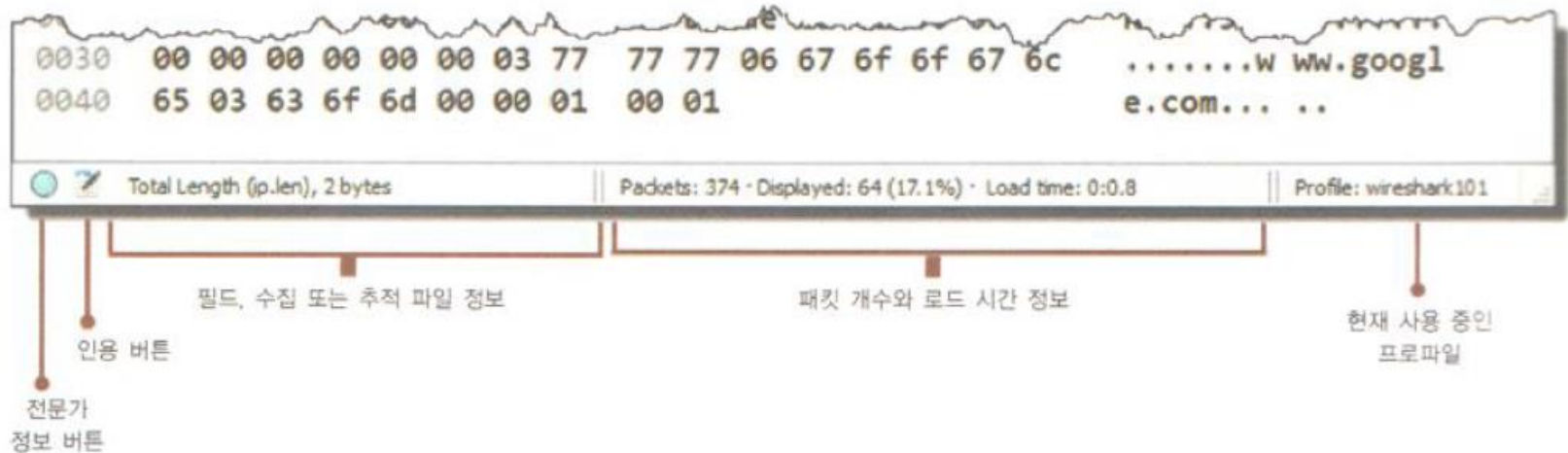


그림 20 상태 바 내용은 패킷 목록 창이나 패킷 상세 창 안에서 무엇을 클릭하는가에 따라 변한다.

화면 필터 예제

- 특정 호스트의 패킷 캡처
 - `ip.addr == 10.10.50.15`
 - 특정 두 호스트의 통신 패킷 캡처
 - `host 10.10.50.170 and host 10.10.50.15`
 - 특정 포트 패킷 캡처
 - `tcp.port == 80`
 - 특정 두 포트 전부 패킷 캡처
 - `tcp.port == 80 or tcp.port == 1770`
 - 특정 호스트의 특정 포트 패킷 캡처
 - `ip.addr == 10.10.50.170 and tcp.port == 80`
 - 특정 패킷만 캡처 안함
 - `not arp`
- 더 많은 예제는 다음 링크를 참조한다.
<http://wiki.wireshark.org/DisplayFilters>

자주 쓰이는 필터 예제(1/2)

우선 필터 구문을 작성해야 한다. 필터 구문의 형식은 다음과 같다.

문법:	프로토콜	.	속성 1	.	속성 2	비교 연산자	값	논리 연산자	그 다음 필터 구문
예:	http		request		full_uri	contains	"google"	or	ssl

http.request.full_uri contains "google" or ssl

“HTTP Request의 Full URI에 “google”이 포함되거나 SSL 프로토콜을 사용하는
패킷”

자주 쓰이는 필터 예제(2/2)

ip.addr == 127.0.0.1

ip.dst == 127.0.0.1 or ip.src == 127.0.0.1과 같은 구문이다. 이 표현을 사용할 때 주의해야 할 점은

ip.addr != 127.0.0.1과 같은 표현은 **ip.src**와 **ip.dst** 모두 127.0.0.1인 패킷만 제외한다는 것이다. 만약 127.0.0.1에서 오거나 간 패킷을 모두 제외하고 싶다면 **!(ip.addr == 127.0.0.1)**을 사용해야 한다.

ip.addr == 10.56.208.213 && ip.addr == 64.233.189.99

10.56.208.213과 64.233.189.99 사이의 통신 내역만을 출력한다. 두 단말 사이에서 어떤 데이터가 오갔는지 관찰할 때에 유용하다.

http

위에서도 언급했듯이 아무 비교 연산자 없이 프로토콜 이름만 쓰면 http 프로토콜을 사용한 패킷만을 캡처하게 된다.

HTTP 트래픽의 적절한 필터링

- 2가지 방법이 존재
 - HTTP
 - `tcp.port == xx` (여기서 `xx`는 사용중인 HTTP 포트다): tcp connection 과정까지 확인가능

TCP 포트 번호 기반의 필터 사용사례

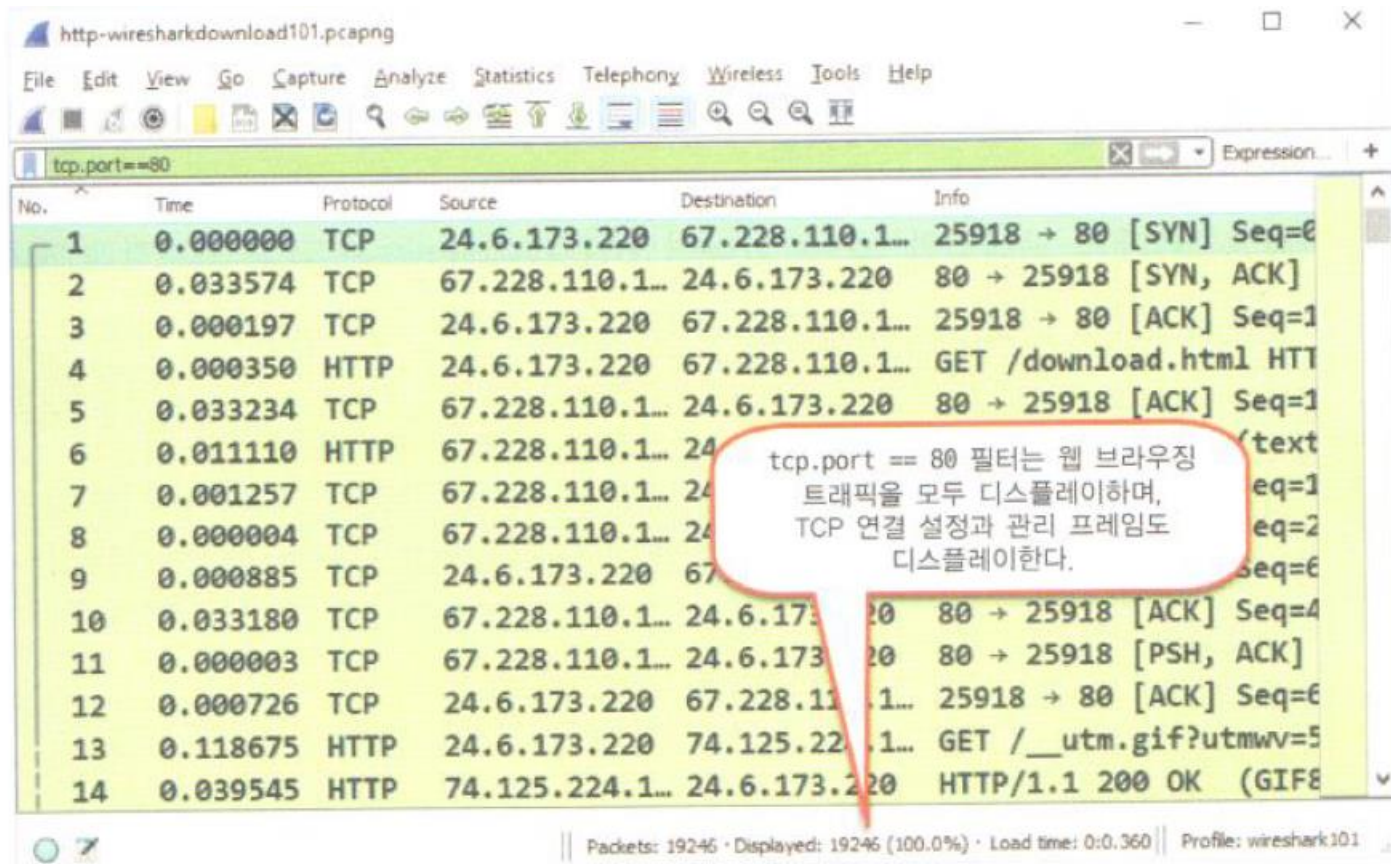


그림 65 포트 번호 기반 필터는 이 wireshark.org 브라우징 세션 안의 패킷을 모두 디스플레이한다.

HTTP 필터 사용 사례

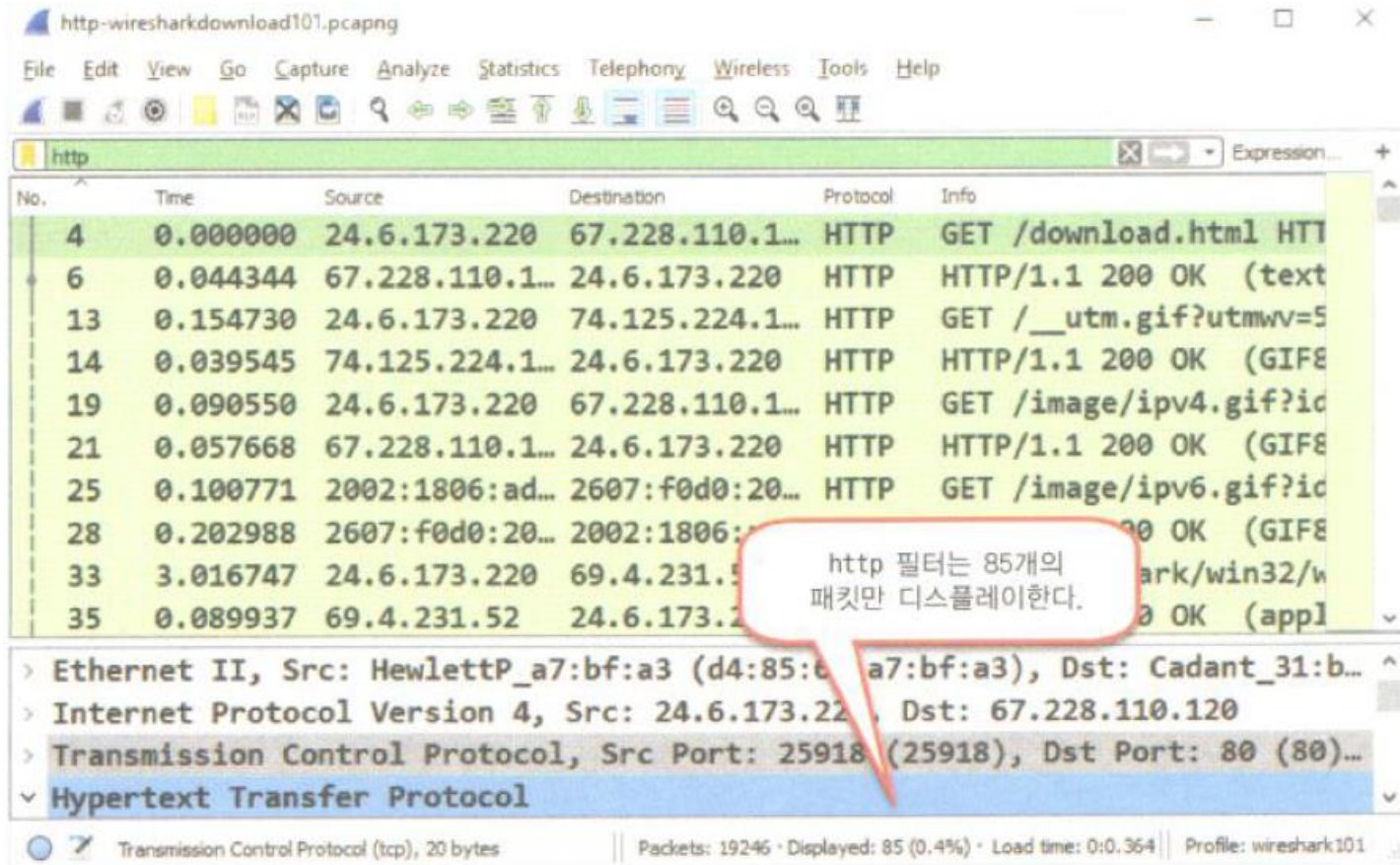


그림 66 http 필터는 TCP 핸드셰이크, ACK, 연결 해제 프로세스를 보여주지 않는다.

목차

- 설치과정
- 핵심요소
- 패킷캡쳐
- 패킷필터
- **트래픽분석**
- HTTP 패킷 따라가기

웹브라우저링 세션 재조립

- 패킷목록창에서 HTTP 패킷을 오른쪽 클릭 하세요
- Follow > TCP stream을 선택한다.
- 호스트간 나눴던 대화가 나온다. (다다음장에 나온 예제)

패킷목록창에서 어떤 패킷이든지 오른쪽 클릭하시오.

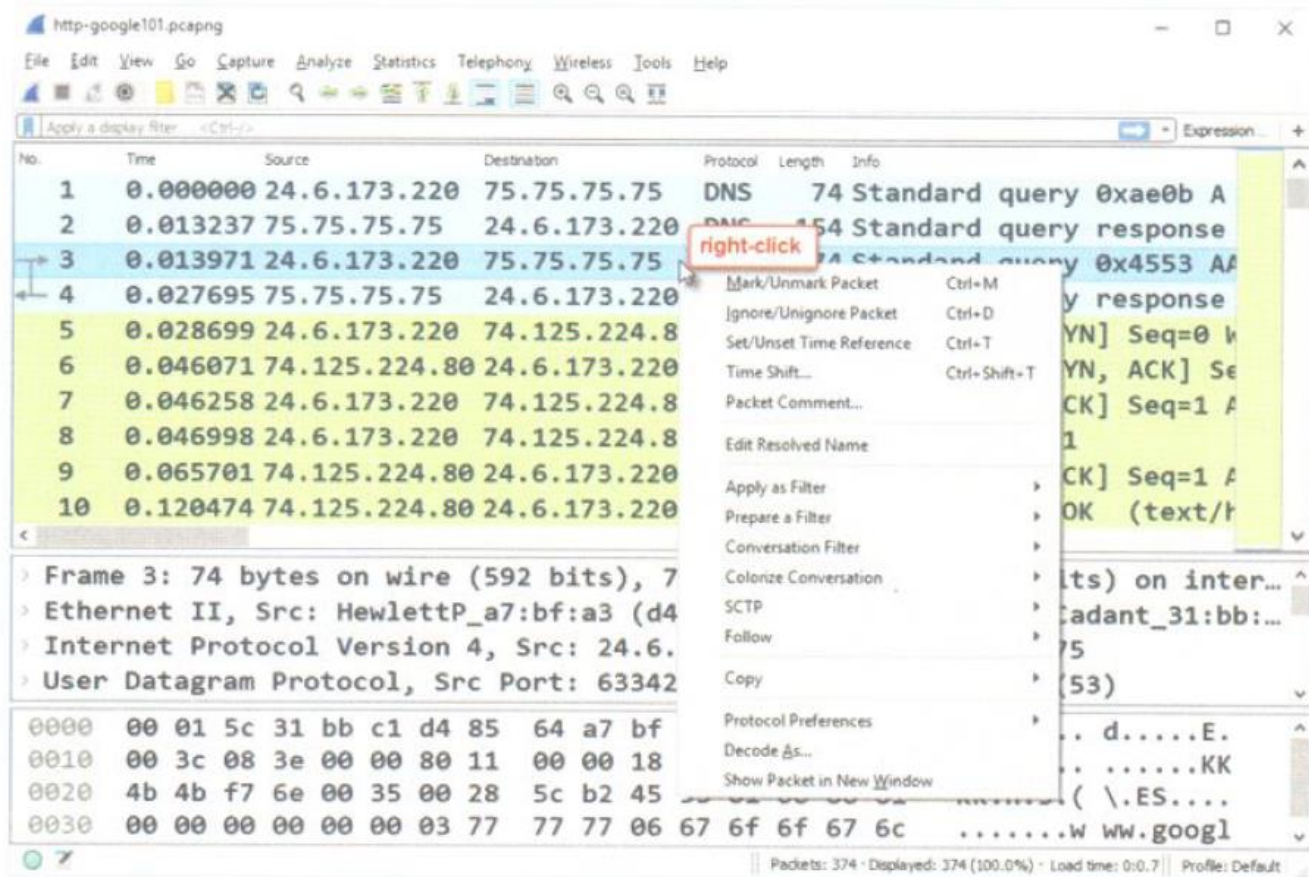


그림 17 이용 가능한 기능을 보려면 패킷 목록 창에서 어떤 패킷이든 오른쪽 클릭하라.

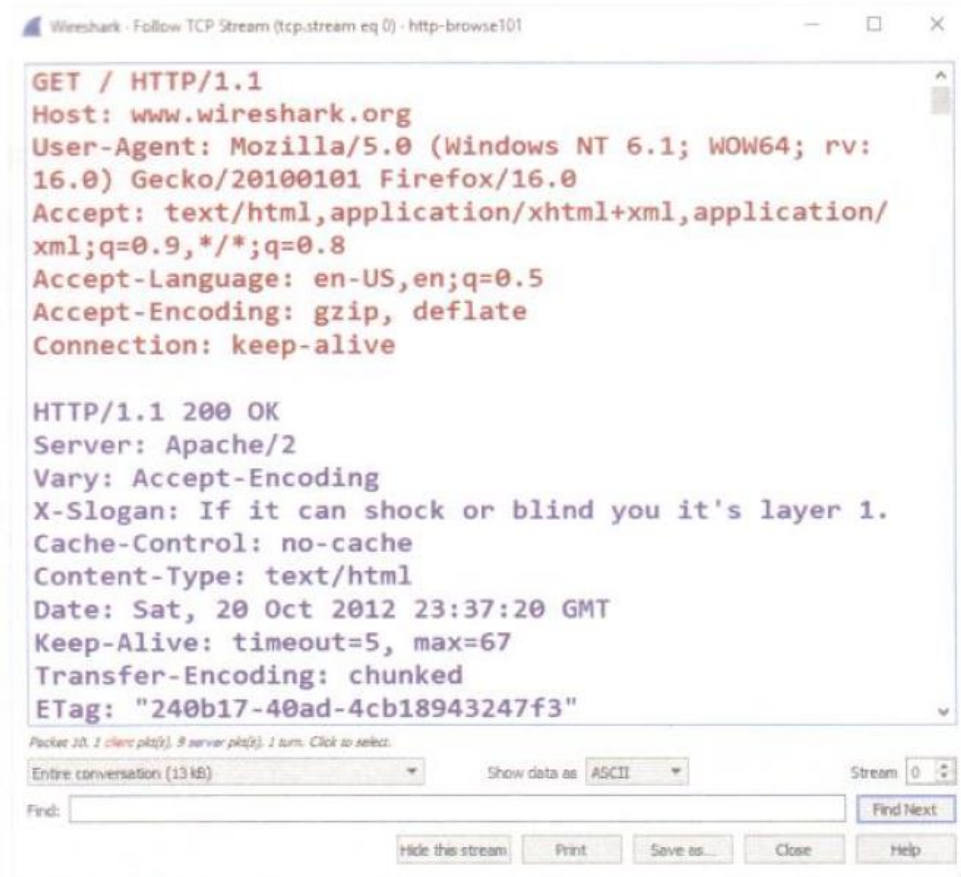


그림 111 스트림을 따라가 보면 대화가 훨씬 명확해진다. [http-browse101.pcapng]

Wireshark wiki page 접근

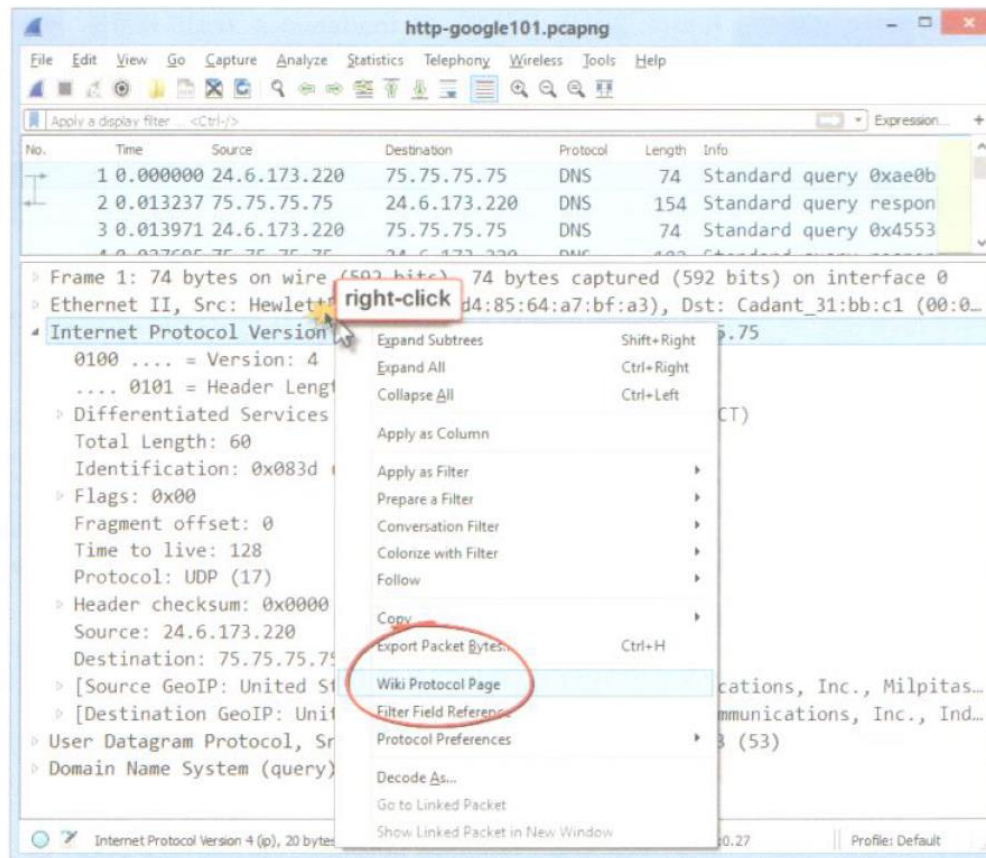


그림 5 패킷 상세 창에 나타난 프로토콜에서 오른쪽 클릭하면 관련된 위키 프로토콜 페이지를 시작한다.

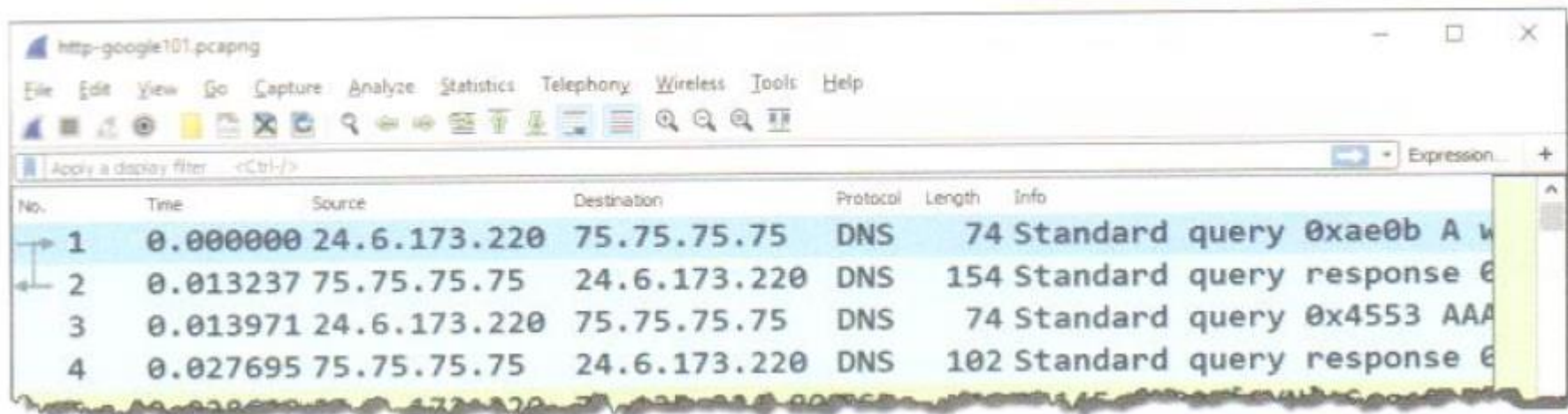
[http-google101.pcapng]

웹브라우저 트래픽 분석(1/4)

http-google101.pcapng¹¹를 열고 누군가가 www.google.com¹²을 방문할 때 생성되는 트래픽을 따라가면서 살펴보자.

전형적인 웹 브라우징 세션에서 추적 파일은 호스트 이름('A' 레코드로 언급된다)을 IP 주소로 변환하기 위한 DNS 요청(프레임 1)을 포함할 것이다. DNS 응답은 최소한 해당 호스트 이름과 관련된 하나의 IP 주소(프레임 2)를 돌려보낼 것이다.

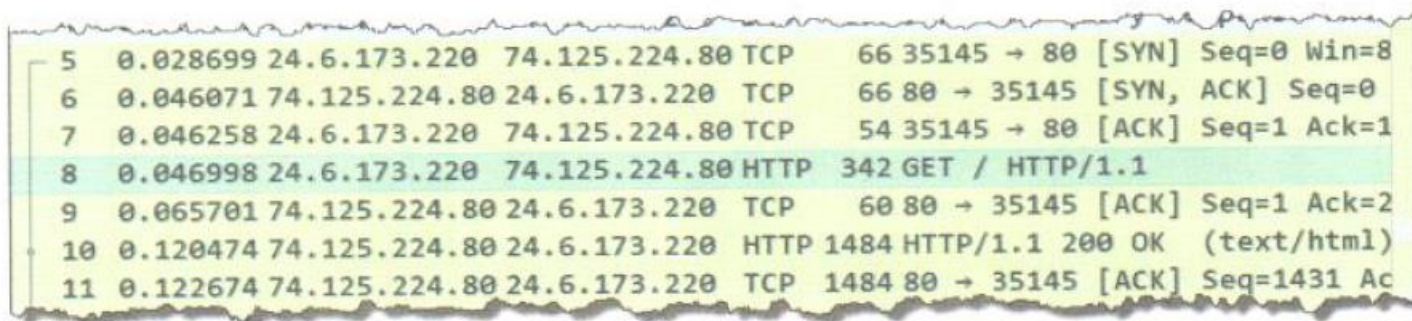
클라이언트가 IPv4와 IPv6를 모두 지원한다면 IPv6 주소('AAAA' 레코드로 언급된다)를 찾기 위한 요청을 발견할 것이다(프레임 3). DNS 서버는 IPv6 주소나 부가적인 정보(프레임 4) 중 하나로 응답할 것이다.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.173.220	75.75.75.75	DNS	74	Standard query 0xae0b A w
2	0.013237	75.75.75.75	24.6.173.220	DNS	154	Standard query response 6
3	0.013971	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x4553 AAA
4	0.027695	75.75.75.75	24.6.173.220	DNS	102	Standard query response 6

웹브라우저 트래픽 분석(2/4)

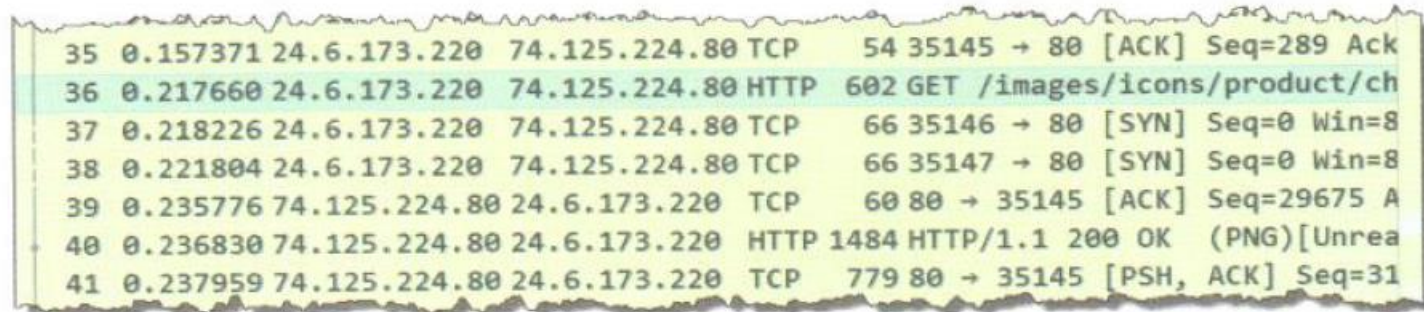
다음에 클라이언트와 웹 서버(프레임 5, 6, 7) 간의 TCP 3 방향 핸드셰이크를 보고, 그 후에 메인 페이지("/")를 GET하기 위한 클라이언트의 요청을 본다(프레임 8). 서버는 요청의 수신을 확인 응답하고(프레임 9), OK 회신을 보낸다(프레임 10).¹³ 이제 서버는 클라이언트에게 메인 페이지를 보내기 시작한다(프레임 11).



5	0.028699	24.6.173.220	74.125.224.80	TCP	66	35145 → 80	[SYN] Seq=0 Win=8
6	0.046071	74.125.224.80	24.6.173.220	TCP	66	80 → 35145	[SYN, ACK] Seq=0
7	0.046258	24.6.173.220	74.125.224.80	TCP	54	35145 → 80	[ACK] Seq=1 Ack=1
8	0.046998	24.6.173.220	74.125.224.80	HTTP	342	GET / HTTP/1.1	
9	0.065701	74.125.224.80	24.6.173.220	TCP	60	80 → 35145	[ACK] Seq=1 Ack=2
10	0.120474	74.125.224.80	24.6.173.220	HTTP	1484	HTTP/1.1 200 OK (text/html)	
11	0.122674	74.125.224.80	24.6.173.220	TCP	1484	80 → 35145	[ACK] Seq=1431 Ac

웹브라우저 트래픽 분석(3/4)

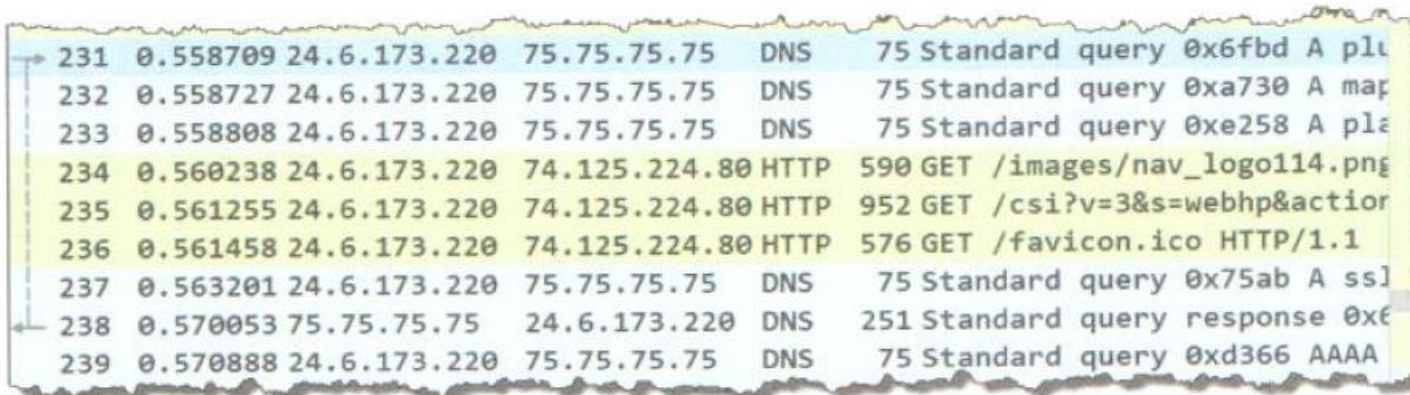
주기적으로 클라이언트는 동일 서버인 `www.google.com` 페이지(프레임 36)의 다른 요소를 요청한다.



35	0.157371	24.6.173.220	74.125.224.80	TCP	54	35145 → 80	[ACK] Seq=289 Ack
36	0.217660	24.6.173.220	74.125.224.80	HTTP	602	GET /images/icons/product/ch	
37	0.218226	24.6.173.220	74.125.224.80	TCP	66	35146 → 80	[SYN] Seq=0 Win=8
38	0.221804	24.6.173.220	74.125.224.80	TCP	66	35147 → 80	[SYN] Seq=0 Win=8
39	0.235776	74.125.224.80	24.6.173.220	TCP	60	80 → 35145	[ACK] Seq=29675 A
40	0.236830	74.125.224.80	24.6.173.220	HTTP	1484	HTTP/1.1 200 OK (PNG)[Unrea	
41	0.237959	74.125.224.80	24.6.173.220	TCP	779	80 → 35145	[PSH, ACK] Seq=31

웹브라우저 트래픽 분석(4/4)

뿐만 아니라 www.google.com 상에 또 다른 웹사이트로 링크가 있을 때 클라이언트는 그다음 사이트(예를 들어 프레임 231, 232, 233에서처럼)에 대한 DNS 질의를 만들 것이다. 이러한 DNS 질의는 자바스크립트 메뉴바가 로드될 때 트리거된다. DNS 요청을 클릭하면 관련 패킷 지시기는 DNS 응답을 가리킨다.



231	0.558709	24.6.173.220	75.75.75.75	DNS	75 Standard query 0x6fbd A plu
232	0.558727	24.6.173.220	75.75.75.75	DNS	75 Standard query 0xa730 A map
233	0.558808	24.6.173.220	75.75.75.75	DNS	75 Standard query 0xe258 A pla
234	0.560238	24.6.173.220	74.125.224.80	HTTP	590 GET /images/nav_logo114.png
235	0.561255	24.6.173.220	74.125.224.80	HTTP	952 GET /csi?v=3&s=webhp&action
236	0.561458	24.6.173.220	74.125.224.80	HTTP	576 GET /favicon.ico HTTP/1.1
237	0.563201	24.6.173.220	75.75.75.75	DNS	75 Standard query 0x75ab A ssl
238	0.570053	75.75.75.75	24.6.173.220	DNS	251 Standard query response 0x6
239	0.570888	24.6.173.220	75.75.75.75	DNS	75 Standard query 0xd366 AAAA

목차

- 설치과정
- 핵심요소
- 패킷캡쳐
- 패킷필터
- 트래픽분석
- HTTP 패킷 따라가기

HTTP 패킷 따라가기(1/4)

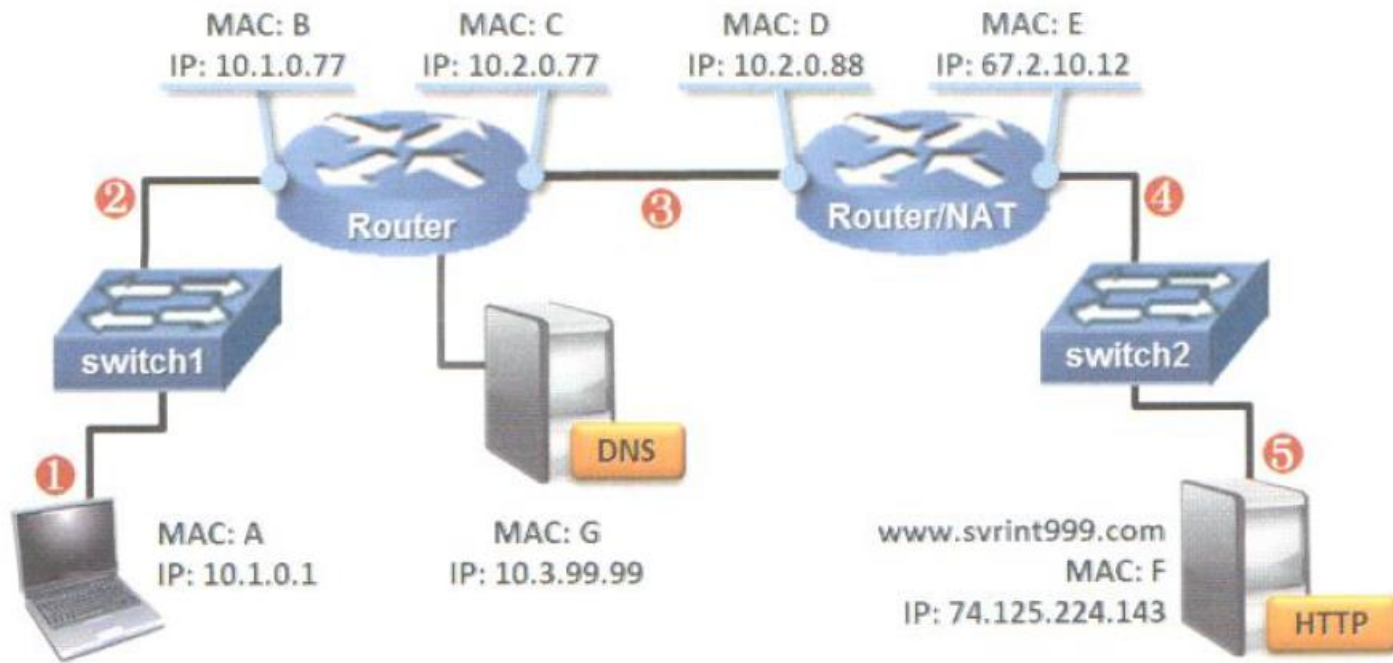
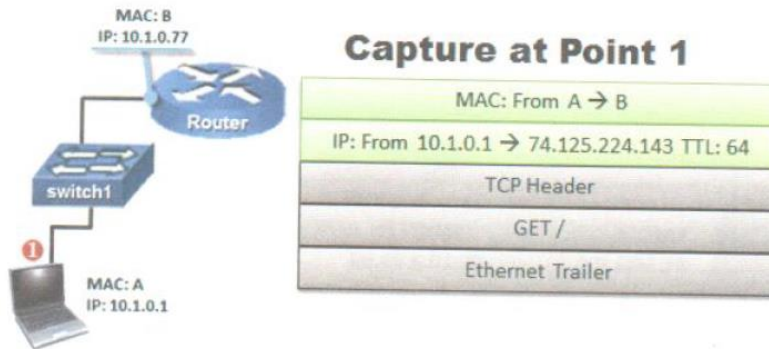


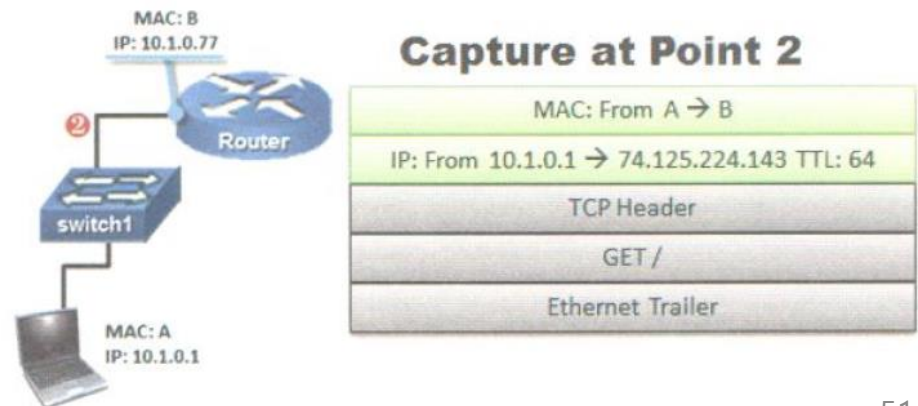
그림 3 이 장치들이 경로를 따라 전달되는 프레임 형식에 어떻게 영향을 끼치는가?

HTTP 패킷 따라가기(2/4)

포인트 1: 클라이언트에서 무엇을 볼 것인가?

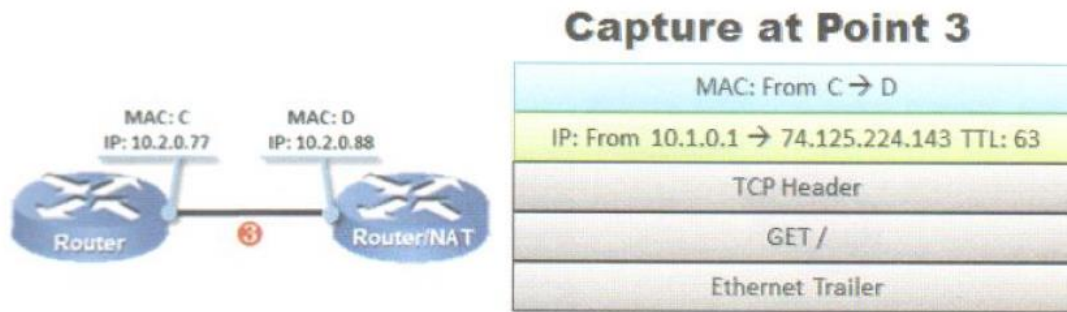


포인트 2: 첫 번째 스위치의 뒤쪽에서 무엇을 볼 수 있는가?

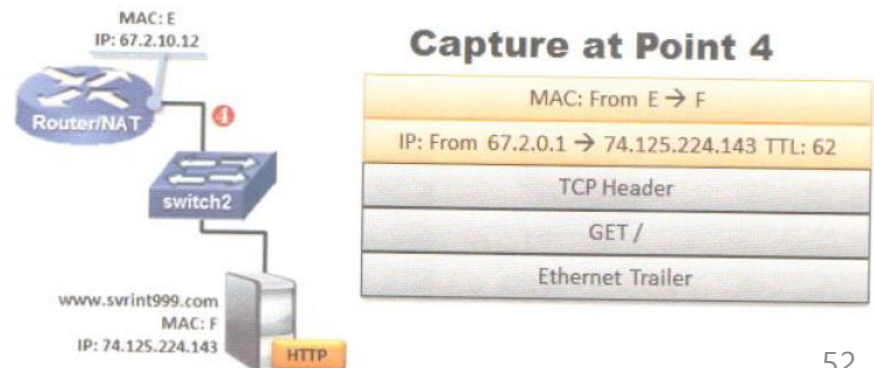


HTTP 패킷 따라가기(3/4)

포인트 3: 라우터의 다른 쪽에서 무엇을 볼 수 있는가?

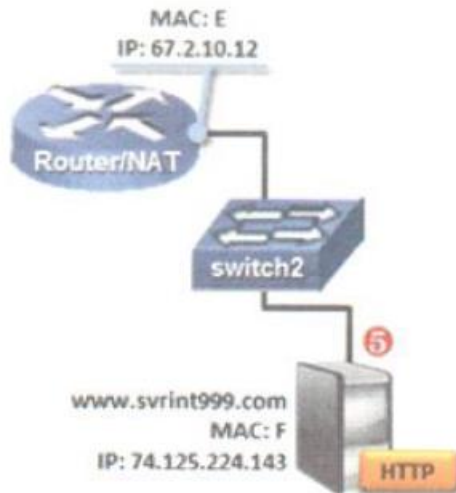


포인트 4: 라우터/NAT 장치의 다른 쪽에서 무엇을 볼 수 있는가?



HTTP 패킷 따라가기(4/4)

포인트 5: 서버에서 무엇을 볼 것인가?



Capture at Point 5

MAC: From E → F
IP: From 67.2.0.1 → 74.125.224.143 TTL: 62
TCP Header
GET /
Ethernet Trailer

참고문헌

- 이재광(역), 로라채움(원저), "와이어샹크 개론", 2nd ed., 에이콘, 2018
- <https://blog.naver.com/haebongru2017/221559789541>
- <http://halra.knuw.ac.kr/networksecurity/와이어샹크사용법.pdf>
- <https://jeong-pro.tistory.com/155>
- <http://cfile2.uf.tistory.com/attach/2604084E568041721D4B36>

Trace files 예제

chappell-university.com/traces

Student Portal

Welcome to the Chappell University Student Portal. We have hundreds of trace files to help our students and instructors.

Download Instructions:

FTP or Browser Access

Site: wiresharktraces.com

Username: traces@wiresharktraces.com

Password: wireshark2020