

# Wireshark

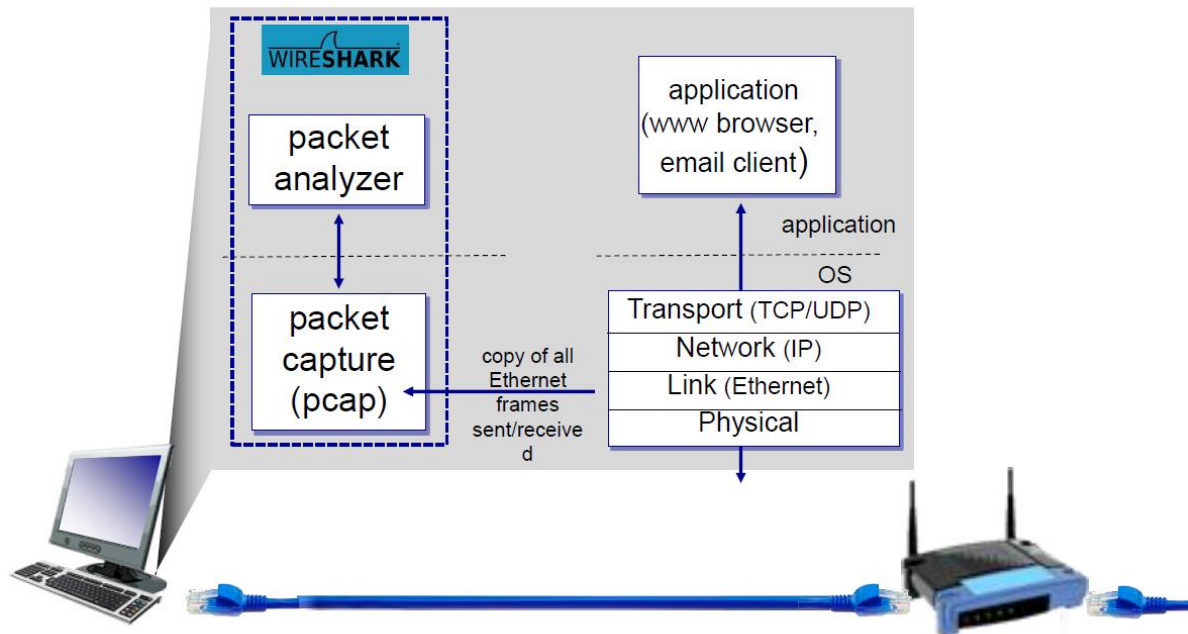
Packet Analysis Tool

# Category

1. 소개
2. 사용법
3. 과제 소개
  - Wireshark\_HTTP\_v7.0
  - Wireshark\_DNS\_v7.0

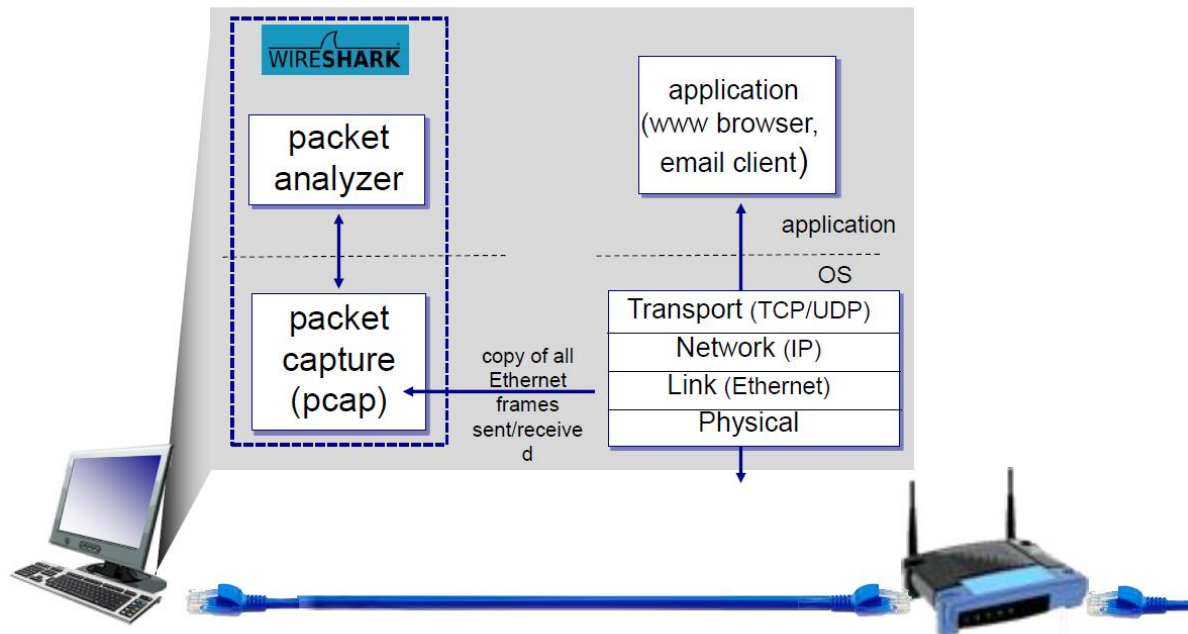
# Wireshark

- 패킷 캡처를 통한 패킷 분석 툴
- 네트워크 프로토콜에 대한 이해를 돕기 위해 사용됨
- Analyzing with data from packet capture(pcap) module built in OS
- 주기능 : 패킷 캡처, 필터링, 시각화



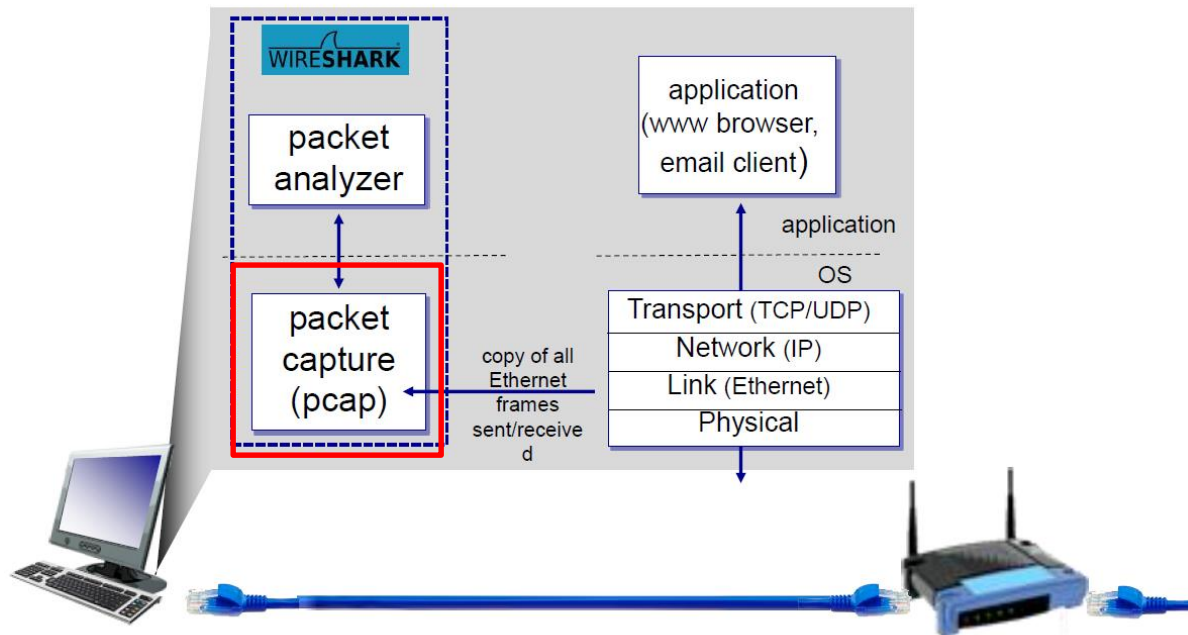
# Wireshark

- Packet Sniffer
  - 프로토콜 엔티티 사이에서 메시지가 변화하는것을 보기위한 도구
  - 다양한 프로토콜 필드에서 캡처한 메시지를 저장하고 보여줌



# Wireshark

- Packet Capture Library
  - 컴퓨터가 전송하거나, 전송받은 모든 링크 레이어 프레임의 사본을 수신



# Wireshark

- Packet analyzer
  - 프로토콜 메시지와 함께 모든 필드의 콘텐츠를 시각화

**command menus**

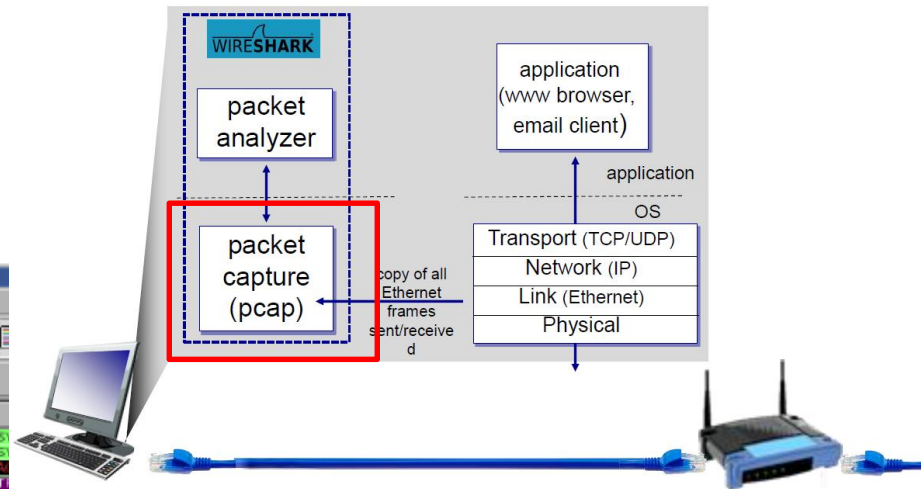
**display filter specification**

**listing of captured packets**

**details of selected packet header**

**packet content in hexadecimal and ASCII**

The screenshot shows the Wireshark interface with a list of captured packets. The selected packet (Frame 4) is an HTTP GET request to www.wireshark.org. The details pane shows the packet structure: Ethernet II, Internet Protocol, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet content is displayed in both hexadecimal and ASCII.



# 예시화면

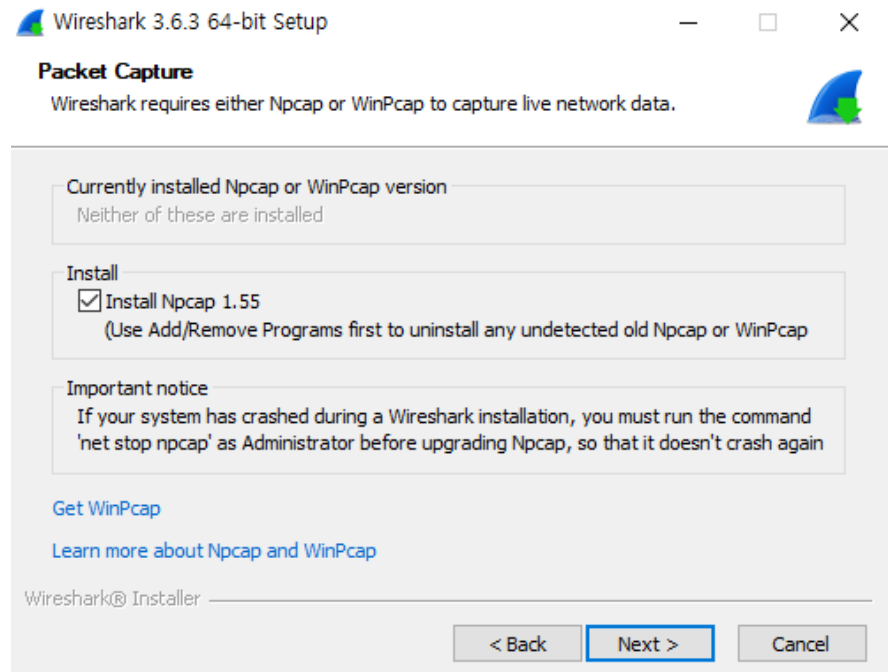
## HTTP 프로토콜에 의해 변화되는 메시지 안에 있는 다양한 필드에 대한 시각화

```
Wireshark - Packet 3063 - 이더넷

> Frame 3063: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface \Device\NPF_{5867EDA5-1DC3-4791-9C42-1C093A2F71D4}, id 0
  > Ethernet II, Src: Micro-St_db:62:70 (00:d8:61:db:62:70), Dst: Cisco_65:7f:41 (f8:0b:cb:65:7f:41)
    > Destination: Cisco_65:7f:41 (f8:0b:cb:65:7f:41)
    > Source: Micro-St_db:62:70 (00:d8:61:db:62:70)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 223.194.46.100, Dst: 128.119.245.12
  > Transmission Control Protocol, Src Port: 50701, Dst Port: 80, Seq: 1, Ack: 1, Len: 301
    Source Port: 50701
    Destination Port: 80
    [Stream index: 35]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 301]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 1729099972
    [Next Sequence Number: 302 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 1934878237
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1024
    [Calculated window size: 262144]
    [Window size scaling factor: 256]
    Checksum: 0x84f2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (301 bytes)
  > Hypertext Transfer Protocol
    > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
      Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
      Accept-Language: ko\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
      Accept-Encoding: gzip, deflate\r\n
      Host: gaia.cs.umass.edu\r\n
      Connection: Keep-Alive\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
      [HTTP request 1/1]
```

# Wireshark 사용법

- Wireshark 다운로드: <http://www.wireshark.org/download.html>
- Wireshark 사용을 위해 Libcap 혹은 WinPCap 패킷 캡처 라이브러리를 지원해야함
- WinPCap 다운로드 : <https://www.winpcap.org/install/default.htm>
- Wireshark 설치과정중 Npcap 을 설치 할 것이냐, 라는 체크박스가 나옴
- 자료화면은 현재 WinPcap 혹은 Npcap 이 설치되어 있다면 그에 대한 버전을 보여주며, 없을 경우 Npcap 을 설치 선택 화면  
체크 후 설치



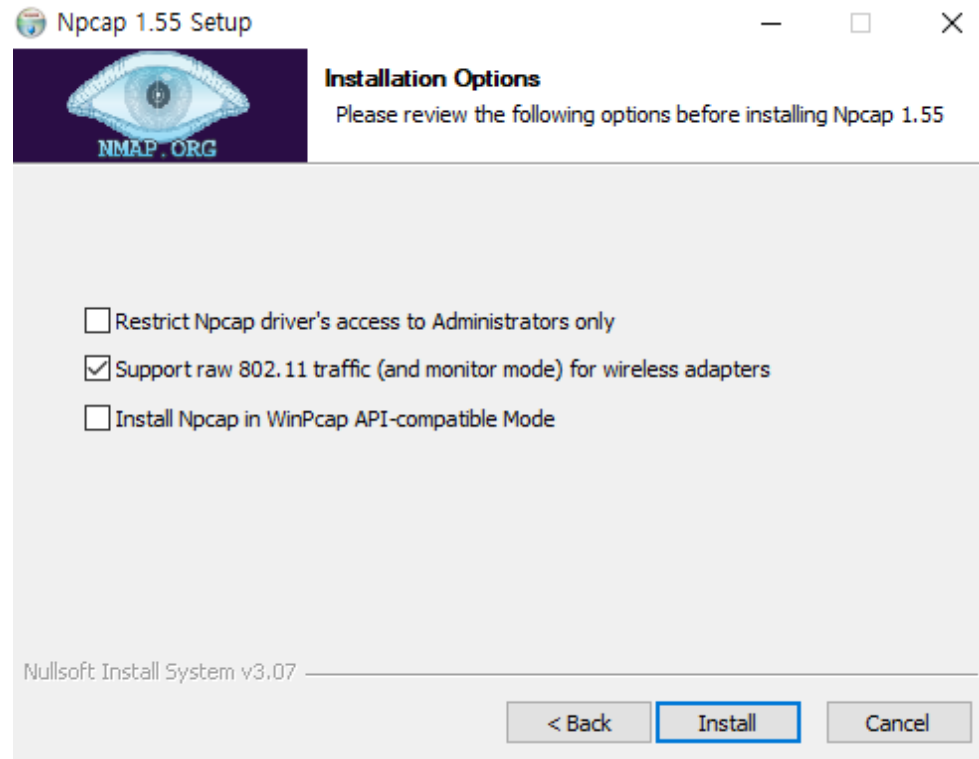


# Wireshark

유선 사용시에는 상관없음.

무선 사용시에 이 실험을 진행하기 위해 추가 설정 내용으로 변경

아래의 Support raw 802.11 traffic (and monitor mode) for wireless 체크하면, Npcap을 통해 지원되지 않는 무선 어댑터를 사용할 때 802.11 패킷을 캡처할 수 있습니다.



# Wireshark 사용법

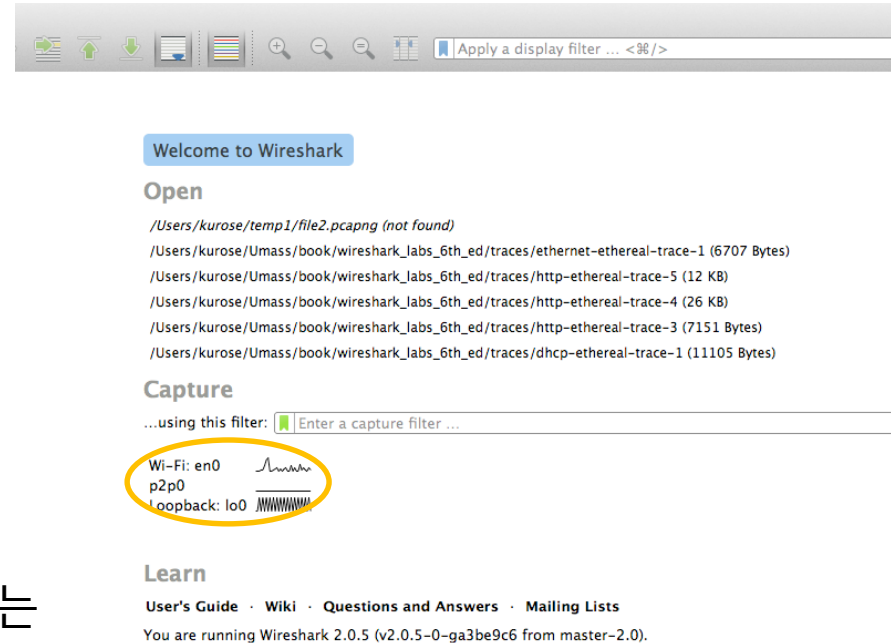
## Wireshark 실행시 초기화면

해당 화면은 OS 나 wireshark 의 버전에 따라 GUI가 다르므로 실제 과제를 진행하며 보는 Wireshark 초기화면과 자료화면에는 차이가 있을 수 있음

자료화면은 wi-fi 를 사용중인 환경에서 wireshark 를 실행시켰을때의 모습

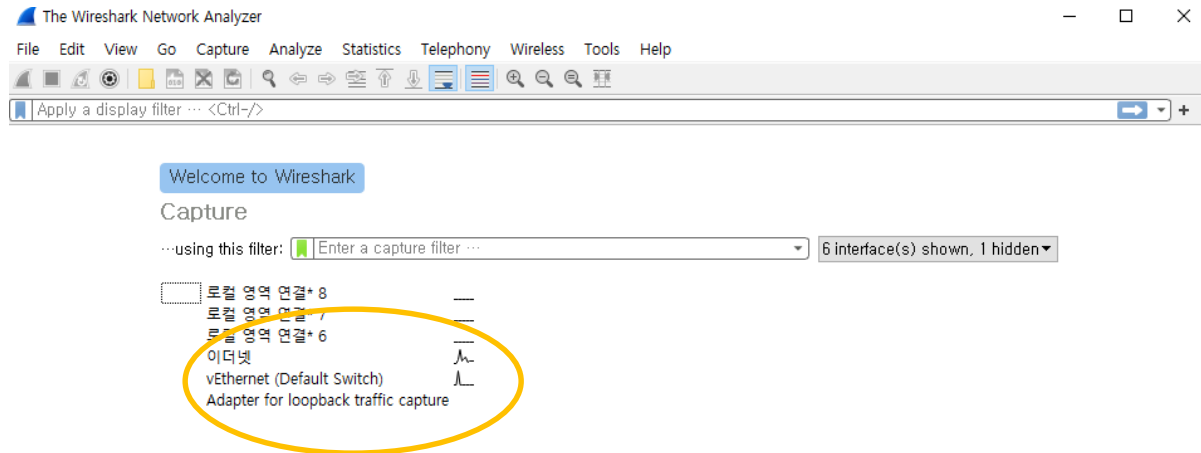
이더넷을 사용할 경우 이더넷에 해당하는 항목이 인식됨

해당 인터페이스를 더블클릭 할 경우 패킷캡처를 시작



# Wireshark 사용법

- 해당 자료화면은 이더넷을 사용중인 화면
- 사용하고 있는 모든 어댑터의 정보가 나옴



## Learn

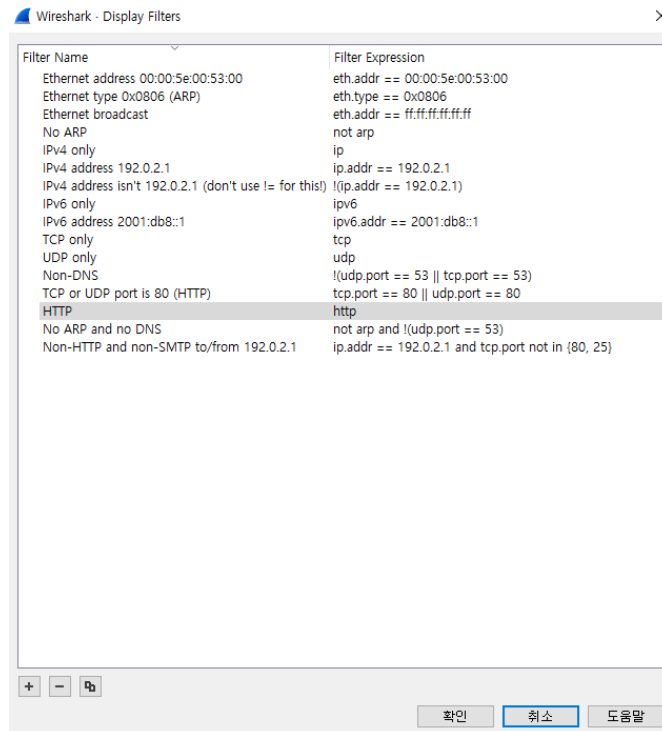
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.6.3 (v3.6.3-0-g6d348e4611e2). You receive automatic updates.

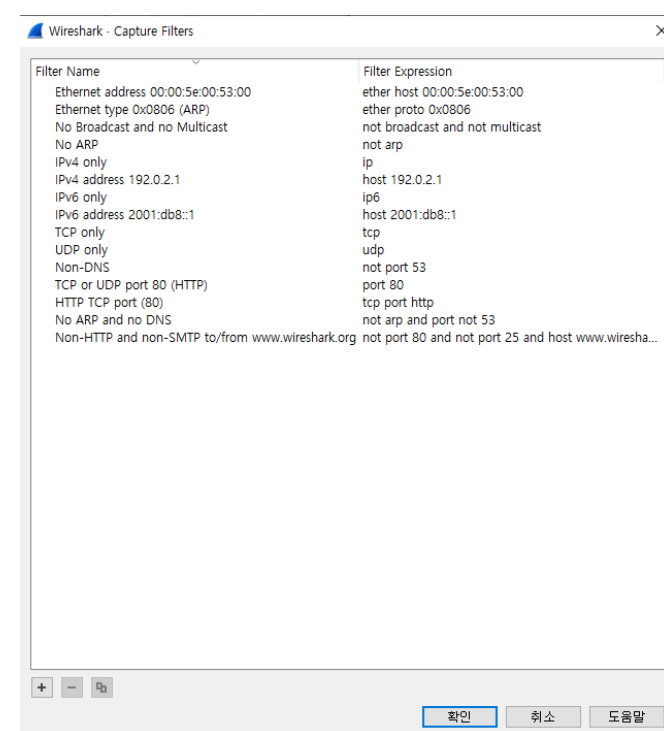
# Wireshark 사용법

## 주기능 중 하나인 필터링

Analyze\_Display Filters..을 선택 시  
Display 할 내용에 대한 filter 가 나옴  
좌측 하단의 + 와 - 를 통해 원하는  
필터 추가/삭제 가능



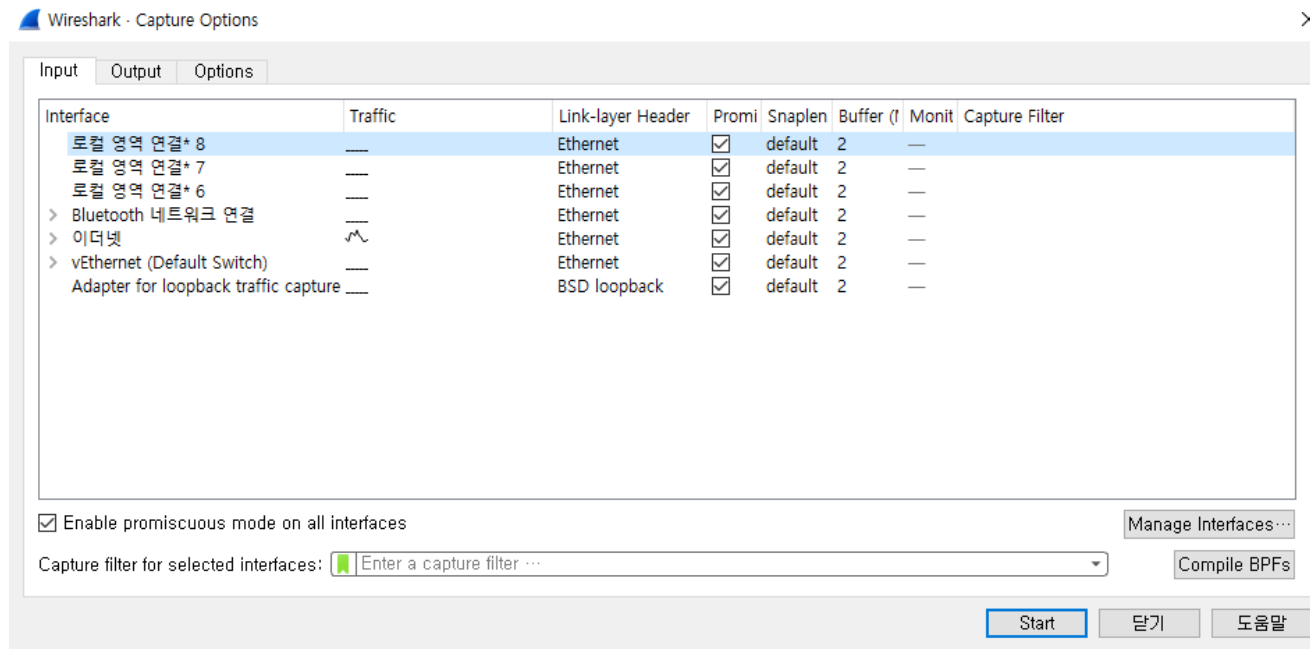
Capture\_Capture Filters..을 선택 시  
Capture 할 내용에 대한 filter 가 나옴  
좌측 하단의 + 와 - 를 통해 원하는  
필터 추가/삭제 가능



# Wireshark 사용법

상단 메뉴에서 Capture\_Options 를 클릭 할 경우(자료화면)

원하는 인터페이스를 선택하고 Start 를 눌러 패킷캡처를 실행 가능



# Wireshark 사용법

## 이더넷을 선택할 경우의 화면

Capturing from 이더넷

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Server Name	Info
2864	9.046457	Cisco_65:7f:41	Broadcast	ARP	60		Who has 223.194.46.158? Tell 223.194.46.254
2865	9.058708	223.194.46.116	223.194.46.255	UDP	305		54915 → 54915 Len=263
2866	9.178003	ASRockIn_37:ca:...	Broadcast	ARP	60		Who has 223.194.46.106? Tell 223.194.46.61
2867	9.228795	Cisco_0b:76:06	CDP/VTP/DTP/PAG...	CDP	390		Device ID: catalyst2950.mclab Port ID: FastEthernet0/6
2868	9.244564	Cisco_0b:76:06	Cisco_0b:76:06	LOOP	60		Reply
2869	9.245055	223.194.46.191	239.255.255.250	SSDP	215		M-SEARCH * HTTP/1.1
2870	9.250481	Cisco_65:7f:41	Broadcast	ARP	60		Who has 223.194.46.3? Tell 223.194.46.254
2871	9.263980	223.194.46.202	239.255.255.250	SSDP	215		M-SEARCH * HTTP/1.1
2872	9.280839	Cisco_65:7f:41	Broadcast	ARP	60		Who has 223.194.46.154? Tell 223.194.46.254
2873	9.521743	Cisco_65:7f:41	Broadcast	ARP	60		Who has 223.194.46.203? Tell 223.194.46.254
2874	9.525763	Cisco_65:7f:41	Broadcast	ARP	60		Who has 223.194.46.106? Tell 223.194.46.254
2875	9.528240	Cisco_65:7f:41	Broadcast	ARP	60		Who has 223.194.46.159? Tell 223.194.46.254
2876	9.552811	Cisco_65:7f:41	Broadcast	ARP	60		Who has 223.194.46.235? Tell 223.194.46.254
2877	9.585802	Cisco_65:7f:41	Broadcast	ARP	60		Who has 223.194.46.7? Tell 223.194.46.254

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{5867EDA5-1DC3-4791-9C42-1C093A2F71D4}, id 0

> Ethernet II, Src: WesternD\_e3:7c:2d (00:90:a9:e3:7c:2d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Address Resolution Protocol (request)

```
0000  ff ff ff ff ff ff 00 90 a9 e3 7c 2d 08 06 00 01  .....L
0010  08 00 06 04 00 01 00 90 a9 e3 7c 2d df c2 2e 4c  .....L
0020  00 00 00 00 00 00 df c2 2e b1 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

# Wireshark 사용법

이전 화면과 차이점 :

좌측 상단의 적색 사각형 버튼을 누름으로 인해 패킷 캡처를 정지하여 현재까지 캡처한 정보만을 보여줌

Wireshark interface showing a packet capture. The top pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, Server Name, and Info. The middle pane shows the details of the selected packet (Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{5867EDA5-1DC3-4791-9C42-1C093A2F71D4}, id 0). The bottom pane shows the raw packet data in hexadecimal and ASCII.

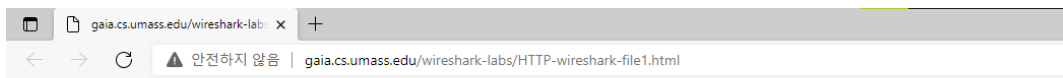
No.	Time	Source	Destination	Protocol	Length	Server Name	Info
7184	105.450504	35.190.80.1	223.194.46.100	TCP	60		443 → 50333 [ACK] Seq=417 Ack=2027 Win=374 Len=0
7185	105.450504	35.190.80.1	223.194.46.100	TCP	60		443 → 50333 [ACK] Seq=417 Ack=2062 Win=374 Len=0
7186	105.459160	142.251.8.189	223.194.46.100	UDP	67		443 → 55057 Len=25
7187	105.653756	49.247.192.194	223.194.46.100	TLSv...	91		Application Data
7188	105.706574	223.194.46.100	49.247.192.194	TCP	54		49571 → 5050 [ACK] Seq=75 Ack=1654 Win=63577 Len=0
7189	105.741412	Cisco_65:7f:41	Broadcast	ARP	60		who has 223.194.46.1? Tell 223.194.46.254
7190	105.791751	223.194.46.205	239.255.255.250	SSDP	216		M-SEARCH * HTTP/1.1
7191	105.800923	223.194.46.100	114.108.158.198	TLSv...	135		Application Data
7192	105.802630	114.108.158.198	223.194.46.100	TLSv...	352		Application Data
7193	105.815482	Cisco_65:7f:41	Broadcast	ARP	60		who has 223.194.46.210? Tell 223.194.46.254
7194	105.846974	223.194.46.100	114.108.158.198	TCP	54		50198 → 443 [ACK] Seq=4294 Ack=15795 Win=513 Len=0
7195	105.858462	Cisco_65:7f:41	Broadcast	ARP	60		who has 223.194.46.228? Tell 223.194.46.254
7196	105.902660	Cisco_65:a3:41	Broadcast	ARP	60		who has 223.194.46.191? Tell 223.194.46.253
7197	105.954332	223.194.46.179	239.255.255.250	SSDP	215		M-SEARCH * HTTP/1.1

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{5867EDA5-1DC3-4791-9C42-1C093A2F71D4}, id 0  
> Ethernet II, Src: WesternD\_e3:7c:2d (00:90:a9:e3:7c:2d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Address Resolution Protocol (request)

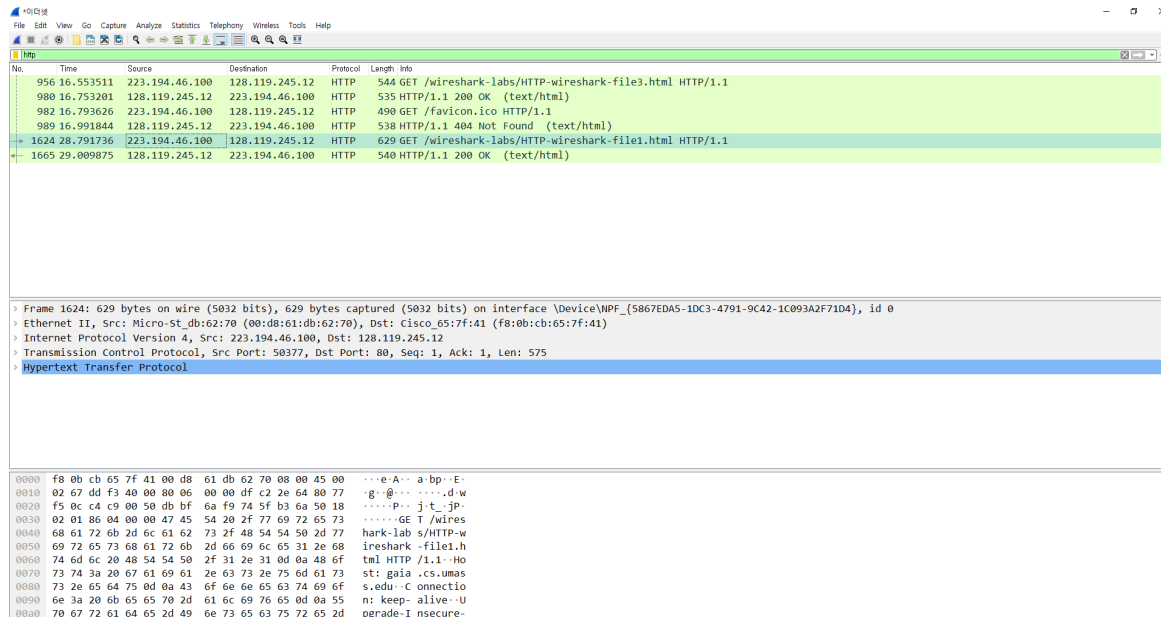
```
0000  ff ff ff ff ff 00 90 a9 e3 7c 2d 08 06 00 01  .......|.....
0010  08 00 06 04 00 01 00 90 a9 e3 7c 2d df c2 2e 4c  .......|....L
0020  00 00 00 00 00 00 df c2 2e b1 00 00 00 00 00 00  .......
0030  00 00 00 00 00 00 00 00 00 00 00 00  .......
```

# Wireshark 사용법

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html> 접속



Congratulations. You've downloaded the file <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>!

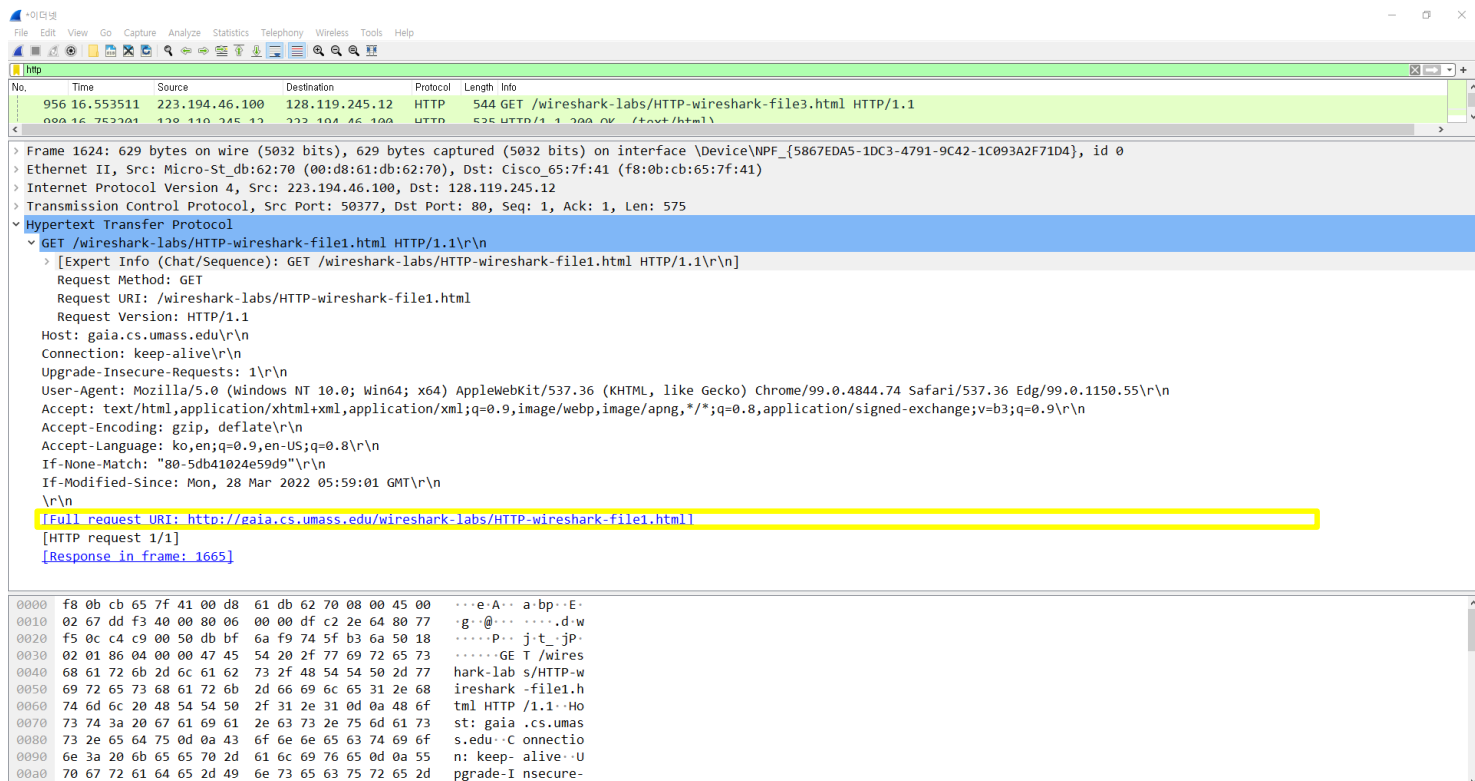


wireshark display filter 를 이용하여, http 에 관련한 정보만을 display



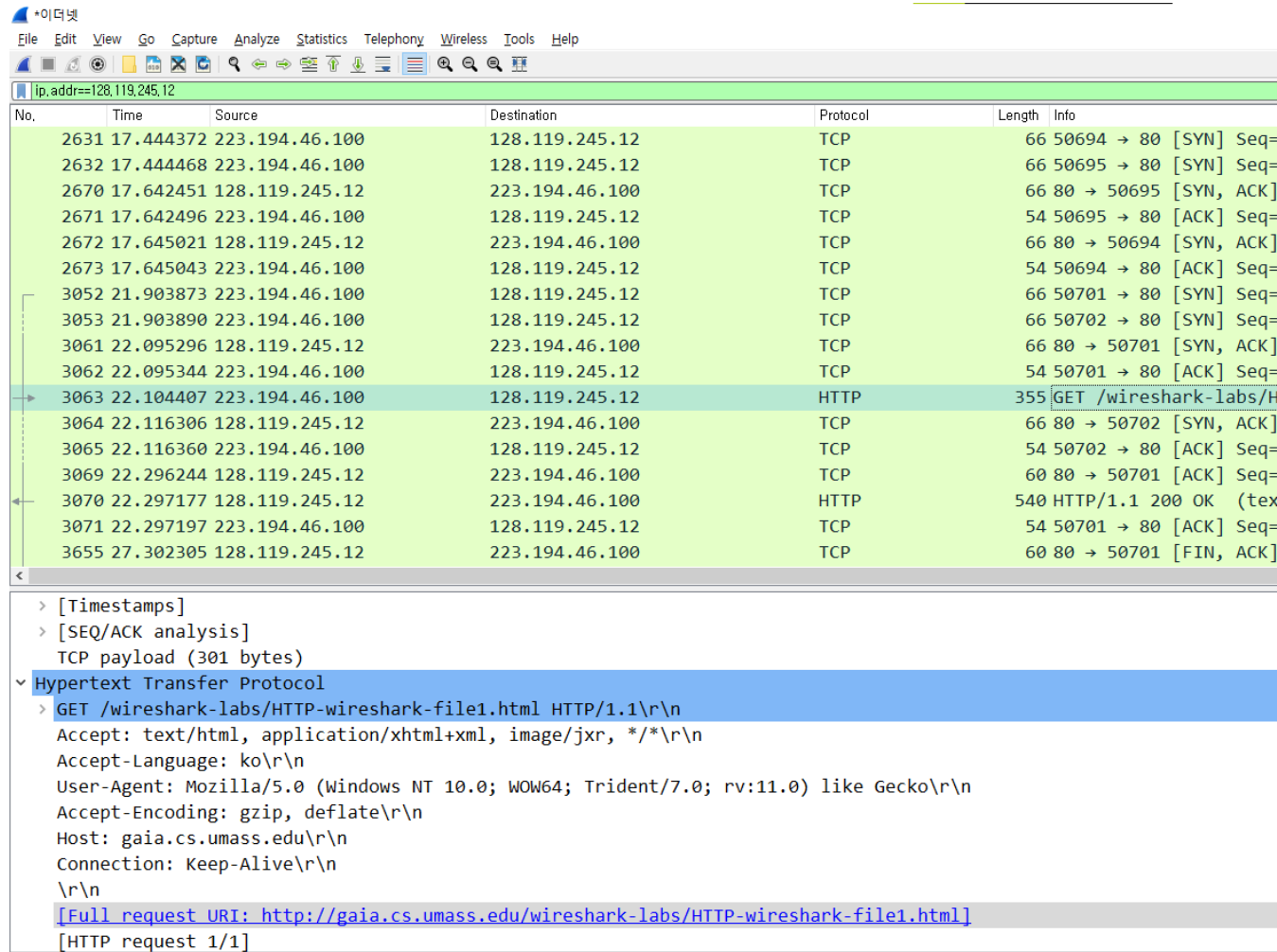
# Wireshark 사용법

[Full request URI : <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>]  
로 접속한 사이트와 같은 주소와 동일함을 확인



# Wireshark 사용법

Wireshark display 필터를 이용하여,  
IP주소를 기준으로 필터링 한 모습



Wireshark interface showing a packet capture filtered by IP address. The packet list shows various TCP and HTTP packets. The selected packet (No. 3063) is an HTTP GET request, and its details are expanded in the packet details pane.

No.	Time	Source	Destination	Protocol	Length	Info
2631	17.444372	223.194.46.100	128.119.245.12	TCP	66	50694 → 80 [SYN] Seq=
2632	17.444468	223.194.46.100	128.119.245.12	TCP	66	50695 → 80 [SYN] Seq=
2670	17.642451	128.119.245.12	223.194.46.100	TCP	66	80 → 50695 [SYN, ACK] Seq=
2671	17.642496	223.194.46.100	128.119.245.12	TCP	54	50695 → 80 [ACK] Seq=
2672	17.645021	128.119.245.12	223.194.46.100	TCP	66	80 → 50694 [SYN, ACK] Seq=
2673	17.645043	223.194.46.100	128.119.245.12	TCP	54	50694 → 80 [ACK] Seq=
3052	21.903873	223.194.46.100	128.119.245.12	TCP	66	50701 → 80 [SYN] Seq=
3053	21.903890	223.194.46.100	128.119.245.12	TCP	66	50702 → 80 [SYN] Seq=
3061	22.095296	128.119.245.12	223.194.46.100	TCP	66	80 → 50701 [SYN, ACK] Seq=
3062	22.095344	223.194.46.100	128.119.245.12	TCP	54	50701 → 80 [ACK] Seq=
3063	22.104407	223.194.46.100	128.119.245.12	HTTP	355	GET /wireshark-labs/H
3064	22.116306	128.119.245.12	223.194.46.100	TCP	66	80 → 50702 [SYN, ACK] Seq=
3065	22.116360	223.194.46.100	128.119.245.12	TCP	54	50702 → 80 [ACK] Seq=
3069	22.296244	128.119.245.12	223.194.46.100	TCP	60	80 → 50701 [ACK] Seq=
3070	22.297177	128.119.245.12	223.194.46.100	HTTP	540	HTTP/1.1 200 OK (tex
3071	22.297197	223.194.46.100	128.119.245.12	TCP	54	50701 → 80 [ACK] Seq=
3655	27.302305	128.119.245.12	223.194.46.100	TCP	60	80 → 50701 [FIN, ACK]

Packet details for selected packet (No. 3063):

- [Timestamps]
- [SEQ/ACK analysis]
  - TCP payload (301 bytes)
- Hypertext Transfer Protocol
  - GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  - Accept: text/html, application/xhtml+xml, image/jxr, \*/\*\r\n
  - Accept-Language: ko\r\n
  - User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
  - Accept-Encoding: gzip, deflate\r\n
  - Host: gaia.cs.umass.edu\r\n
  - Connection: Keep-Alive\r\n
  - \r\n
  - [Full request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>]
  - [HTTP request 1/1]

# Wireshark 사용법

223.194.46.100 에서 128.119.245.12 로 request 를 보낸 모습

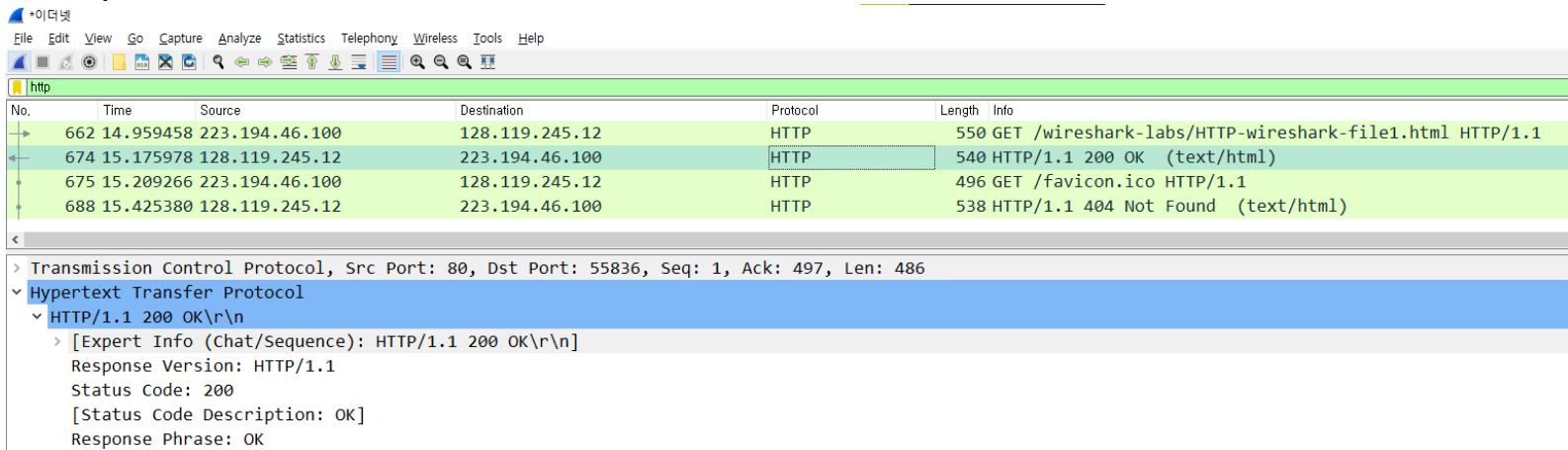
The image shows a Wireshark capture of network traffic. The top pane displays a list of captured packets. The second pane shows the details of the selected packet (No. 662), including the IP header and the Hypertext Transfer Protocol (HTTP) section.

No.	Time	Source	Destination	Protocol	Length	Info
662	14.959458	223.194.46.100	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
674	15.175978	128.119.245.12	223.194.46.100	HTTP	540	HTTP/1.1 200 OK (text/html)
675	15.209266	223.194.46.100	128.119.245.12	HTTP	496	GET /favicon.ico HTTP/1.1
688	15.425380	128.119.245.12	223.194.46.100	HTTP	538	HTTP/1.1 404 Not Found (text/html)

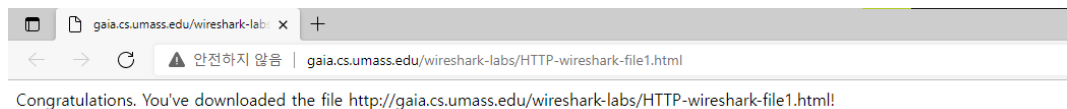
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 128  
Protocol: TCP (6)  
Header Checksum: 0x0000 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 223.194.46.100  
Destination Address: 128.119.245.12  
> Transmission Control Protocol, Src Port: 55836, Dst Port: 80, Seq: 1, Ack: 1, Len: 496  
v Hypertext Transfer Protocol  
v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n  
v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n  
Request Method: GET  
Request URI: /wireshark-labs/HTTP-wireshark-file1.html  
Request Version: HTTP/1.1

# Wireshark 사용법

128.119.245.12 에서 223.194.46.100 에 response 를 보낸 모습  
Response 의 status code 는 200 이며 OK 임을 볼 수 있음



response 를 보내는 Source 는 request 의 대상이 되는것을 볼 수 있다.  
해당 response 의 결과화면



## 질문

# Homework #1

- Wireshark\_Intro\_v7.0
- Wireshark\_HTTP\_v7.0
- Wireshark\_DNS\_v7.0
- 과제 제출기한 : ~ 2022/04/13 23:59

## 과제 주의사항

- 와이어 샤크가 패킷을 캡처를 실패할 경우.
  1. 관리자 권한으로 실행  
(MAC, ubuntu 의 경우 'sudo' 사용)
  2. 1번으로 해결 불가 -> packet capture (pcap) 가 설치되지 않은것이므로, WinPcap 설치
    - WinPcap : <https://www.winpcap.org/install/default.htm>
    - Ubuntu : `sudo apt-get install libpcap-dev`
- 질문
  1. E-mail : gggg865 @gmail.com (김동주조교)
  2. klas.kw.ac.kr -> 강의 종합 정보 -> 학습 지원실 -> '강의 묻고 답하기'

## Question #1

- CMD 혹은 terminal 에서 IP 화면 캡처하기.
- Windows : Win + R -> cmd -> ipconfig  
Linux : Open Terminal -> ifconfig
- Ipconfig 와 ifconfig는 같은 역할을 한다.
- 호스트에서 네트워크 이슈를 디버깅하기에 유용한 기능
- Ipconfig 는 DNS 서버 주소, 주소, 어댑터 타입을 포함하는 현재 TCP/IP 정보를 보여주기에 사용됨

```
C:\Users\MMALID>ipconfig

Windows IP 구성

이더넷 어댑터 이더넷:

    연결별 DNS 접미사. . . . . : 
    링크-로컬 IPv6 주소. . . . . : 8e59:4a01%16
    IPv4 주소. . . . . : 223.194.46.202
    서브넷 마스크. . . . . : 
    기본 게이트웨이. . . . . : 223.194.46.254
```



# Question #1

- PC 에서 동작중인 Wireshark 화면 캡처

Welcome to Wireshark

Capture

...using this filter:

☒ 이더넷

VMware Network Adapter VMnet8

VMware Network Adapter VMnet1

No.	Time	Source	Destination	Protocol	Length	Info
13	0.441737	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.102? Tell 223.194.46.254
14	0.455456	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.164? Tell 223.194.46.254
15	0.562932	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.215? Tell 223.194.46.254
16	0.569920	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.228? Tell 223.194.46.254
17	0.575260	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.45? Tell 223.194.46.254
18	0.599365	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.5? Tell 223.194.46.254
19	0.712305	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.180? Tell 223.194.46.254
20	0.733979	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.140? Tell 223.194.46.254
21	0.747534	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.126? Tell 223.194.46.254
22	0.822331	Cisco_0b:76:13	Spanning-tree-(for-...	STP	60	Conf. Root = 4096/46/f8:0b:cb:65:7f:00 Cost = 3019 Port = 0...
23	0.827761	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.230? Tell 223.194.46.254
24	0.921524		75.126.39.117	TCP	58	[TCP Retransmission] 443 → 80 [SYN, ACK] Seq=0 Ack=2916875119...
25	0.973112	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.221? Tell 223.194.46.254
26	1.034515	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.70? Tell 223.194.46.254
27	1.041733	Cisco_65:7f:41	Broadcast	ARP	60	Who has 223.194.46.3? Tell 223.194.46.254
28	1.055514	75.126.39.117	223.194.46.202	TCP	60	[TCP Port numbers reused] 80 → 443 [SYN] Seq=0 Win=5840 Len=0
29	1.055535		75.126.39.117	TCP	58	[TCP ACKed unseen segment] 443 → 80 [SYN, ACK] Seq=0 Ack=3784...

## Question #2

- Wireshark\_HTTP\_v7.0.pdf의 19개 문제 풀이

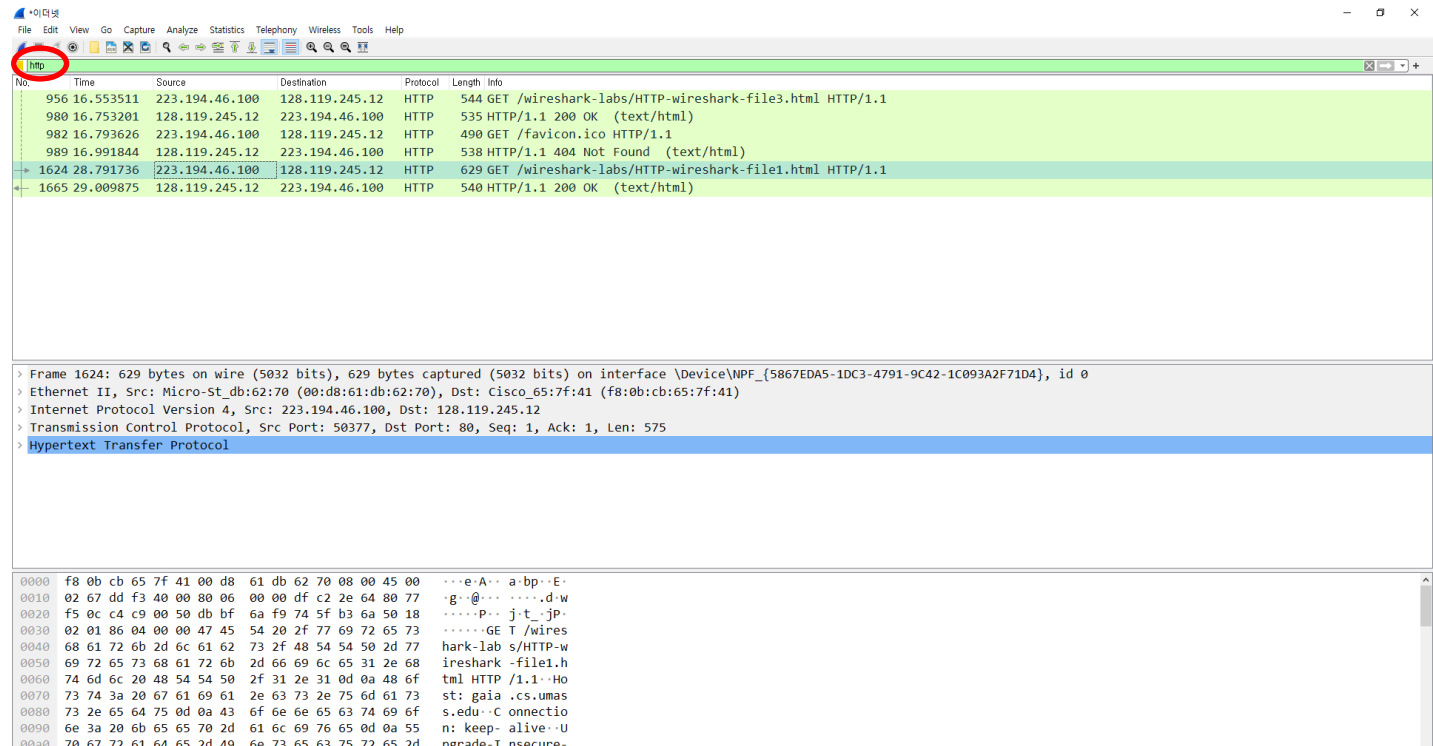
**결과 화면 캡처 및 해당 캡처 화면에 대한 설명 서술 필수**

# Wireshark\_HTTP\_v7.0

HTTP : Hypertext Transfer Protocol

인터넷에서 데이터를 주고받을 수 있는 규칙

Wireshark 에서 filter 에 http 를 입력해서 http protocol 에 해당하는 내용만을 볼 수 있음



## Wireshark\_HTTP\_v7.0

1 ~ 7 번 문제 : By looking at the information in the HTTP GET and response messages, answer the following questions. When answering the following questions, you should print out the GET and response messages (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the message you've found the information that answers the following questions. When you hand in your assignment, annotate the output so that it's clear where in the output you're getting the information for your answer (e.g., for our classes, we ask that students markup paper copies with a pen, or annotate electronic copies with text in a colored font).

## Wireshark\_HTTP\_v7.0

8 ~ 11 번 문제 : Before performing the steps below, make sure your browser's cache is empty. Enter the following URL into your browser <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html> Your browser should display a very simple five-line HTML file. Quickly enter the same URL into your browser again (or simply select the refresh button on your browser) Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

12 ~ 15 번 문제 : Let's next see what happens when we download a long HTML file. In the packet-listing window, you should see your HTTP GET message, followed by a multiple-packet TCP response to your HTTP GET request. This multiple-packet response deserves a bit of explanation. The HTTP response message consists of a status line, followed by header lines, followed by a blank line, followed by the entity body. In the case of our HTTP GET, the entity body in the response is the *entire* requested HTML file. In our case here, the HTML file is rather long, and at 4500 bytes is too large to fit in one TCP packet. The single HTTP response message is thus broken into several pieces by TCP, with each piece being contained within a separate TCP segment

## Wireshark\_HTTP\_v7.0

16,17 번 문제 : Now that we've seen how Wireshark displays the captured packet traffic for large HTML files, we can look at what happens when your browser downloads a file with embedded objects, i.e., a file that includes other objects (in the example below, image files) that are stored on another server

18,19번 문제 : So let's access this "secure" password-protected site

## Question #3

- Wireshark\_DNS\_v7.0.pdf의 23개 문제 풀이

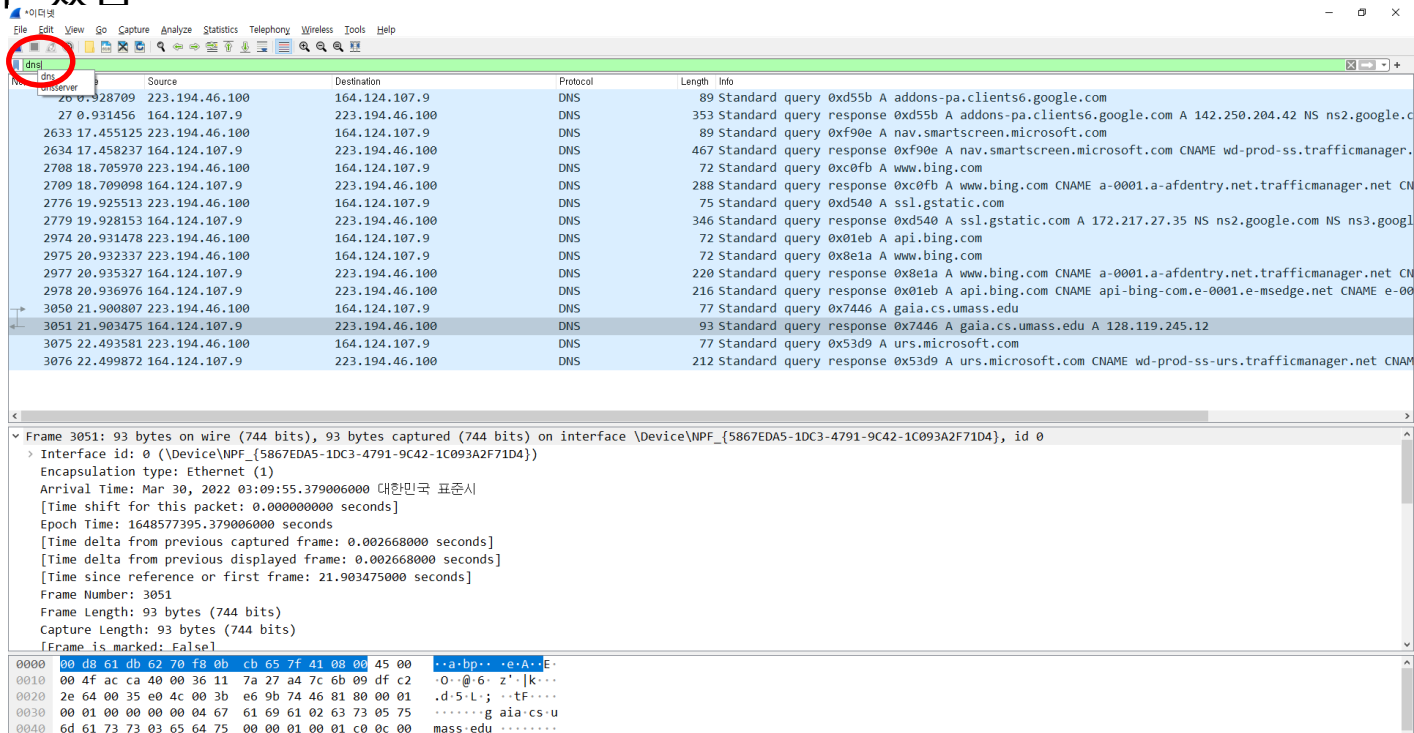
**결과 화면 캡처 및 해당 캡처 화면에 대한 설명 서술 필수**

# Wireshark\_DNS\_v7.0

## DNS : Domain Name System

IP 주소 대신 도메인 이름을 통해 원하는 사이트에 연결할 수 있도록 하는 프로토콜

Wireshark 에서는 filter 에 DNS 를 입력해서 DNS protocol 에 해당하는 내용만을 볼 수 있음



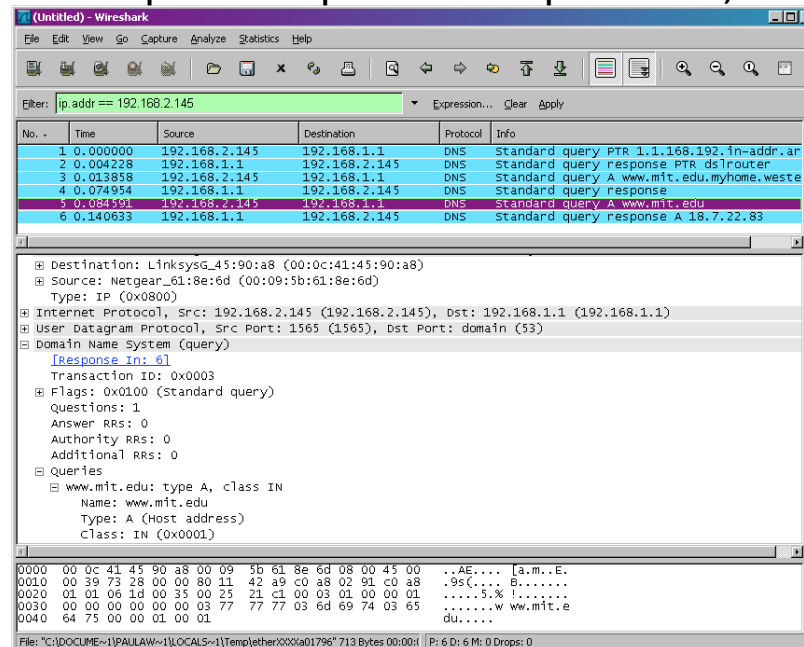


# Wireshark\_DNS\_v7.0

1 ~ 3 번 문제 : Now that we have provided an overview of *nslookup*, it is time for you to test drive it yourself

11 ~ 15 번 문제 : We see from the screenshot that *nslookup* actually sent three DNS queries and received three DNS responses. For the purpose of this assignment, in answering the following questions, ignore the first two sets of queries/responses, as they are specific to *nslookup* and are not normally generated by standard Internet applications. You should instead focus on the last query and response messages.

16 ~ 23 번 문제 : Now repeat the previous experiment, but instead issue the command



# Wireshark Assignment

Due date: 2022/04/13 23:59

## 업로드 파일 포맷: PDF

- 파일 명: 학번\_Ass1\_이름.pdf
- 예시: 2020202000\_Ass1\_홍길동.pdf

## 업로드 양식(언어: 한국어, 영어)

- 표지
  - 강의명, 강의 시간, 교수님 성함, 본인 학번, 본인 성명, 소속, 제출일
- 서론
  - 5 줄 이상
- 본문
  - Wireshark 화면 캡처 및 해당 화면에 대한 설명
- 결론 및 고찰
  - 5 줄 이상

## 질문