Wireshark

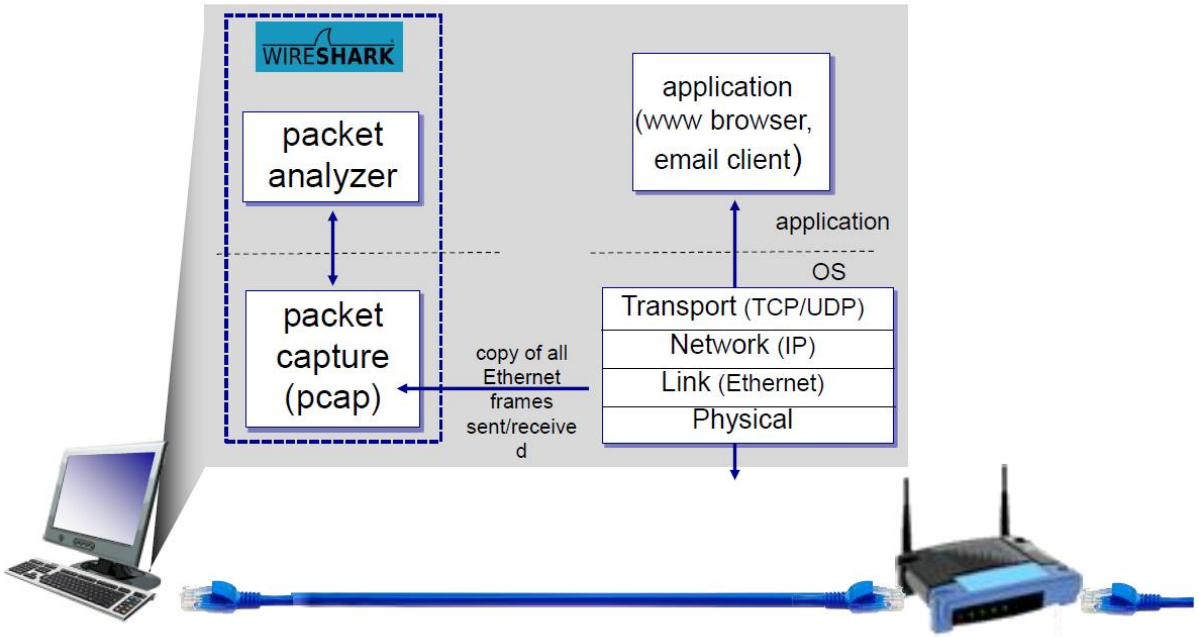
Packet Analysis Tool

Category

1. 소개
2. 사용법
3. 과제 소개
   - Wireshark_HTTP_v7.0
   - Wireshark_DNS_v7.0

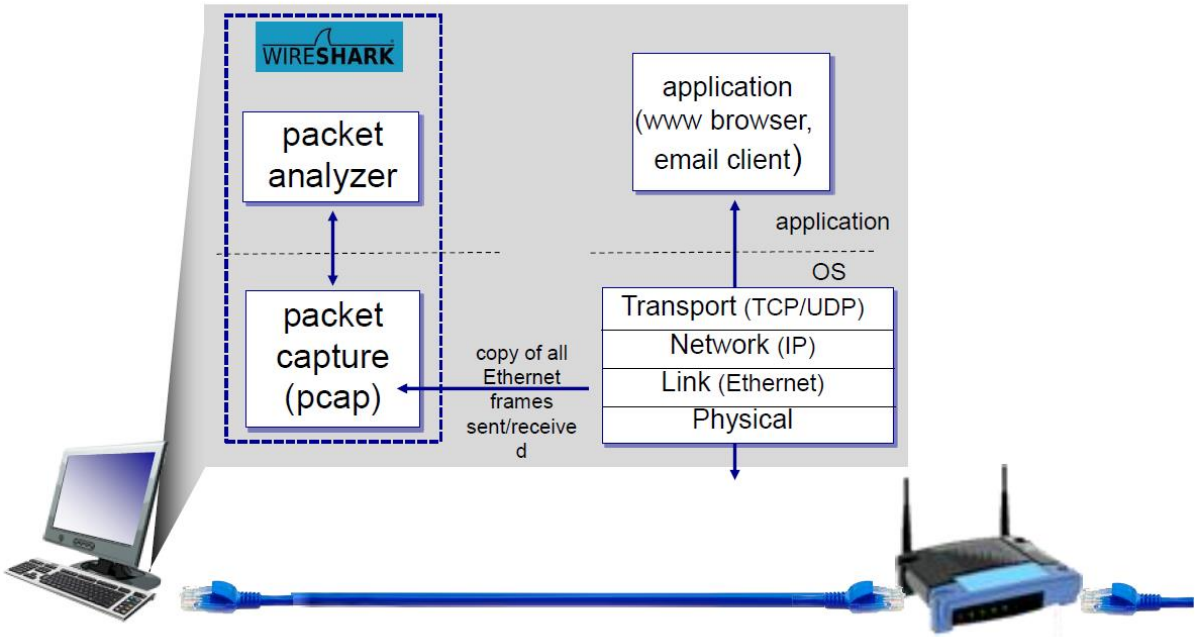
Wireshark

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



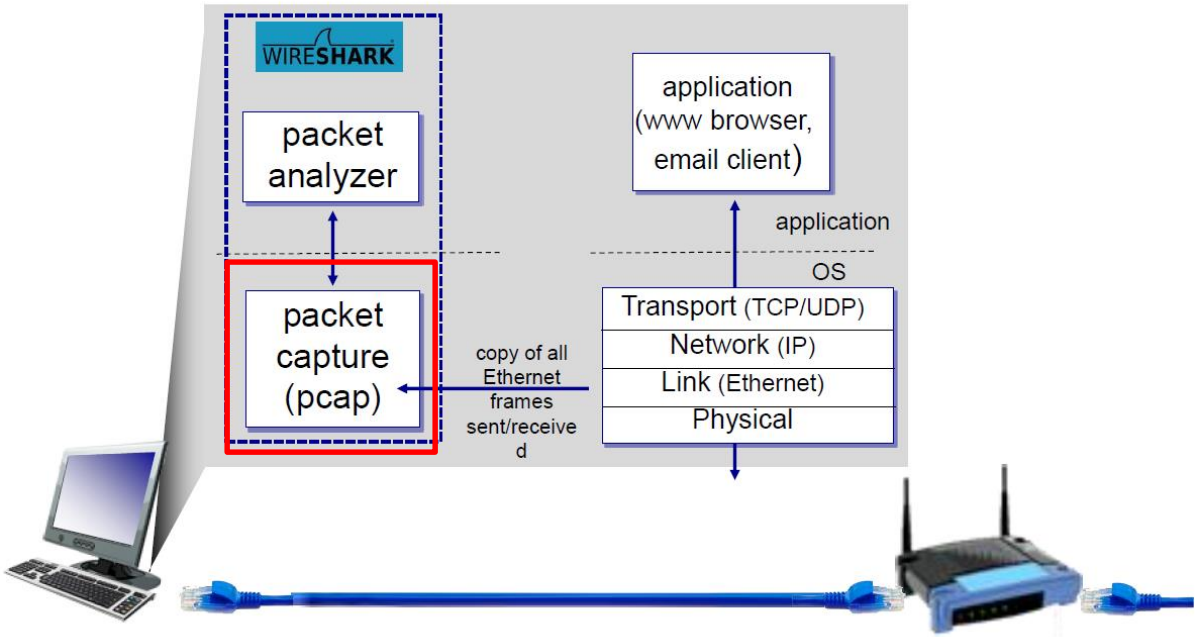
Wireshark

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



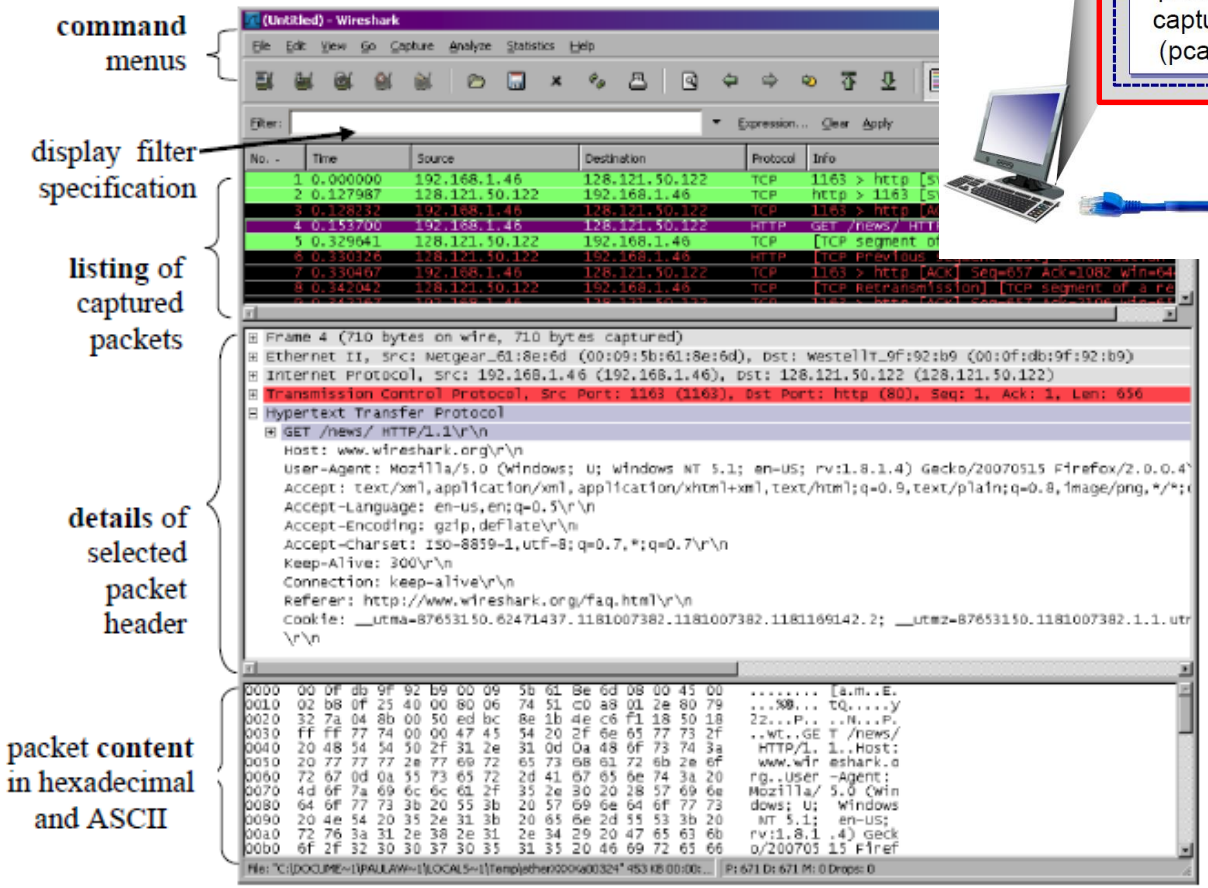
Wireshark

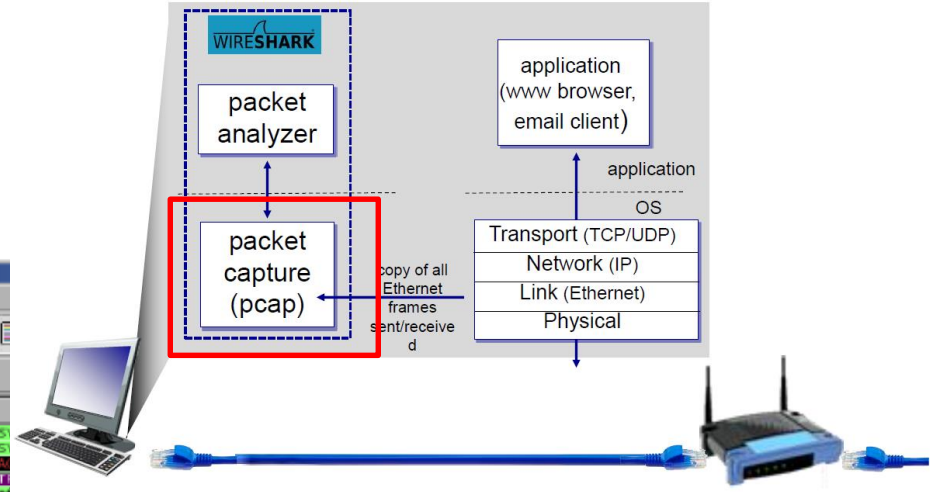
- Packet Capture Library
  - 컴퓨터가 전송하거나, 전송받은 모든 링크 레이어 프레임의 사본을 수신



Wireshark

- Packet analyzer
  - 프로토콜 메시지와 함께 모든 필드의 콘텐츠를 시각화





예시화면

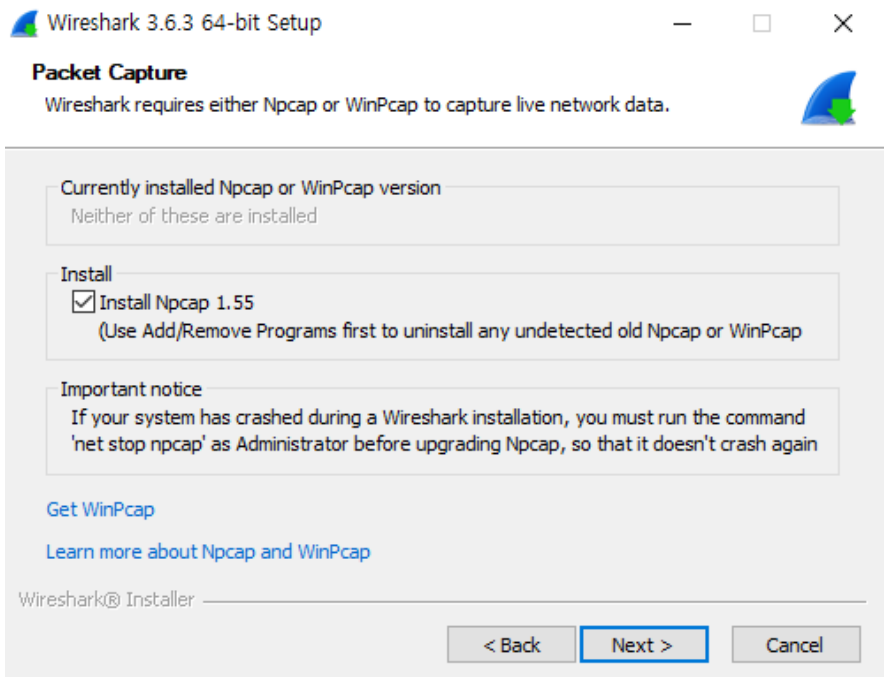
HTTP 프로토콜에 의해 변화되는 메시지 안에 있는 다양한 필드에 대한 시각화

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
v 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
v 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)
v 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

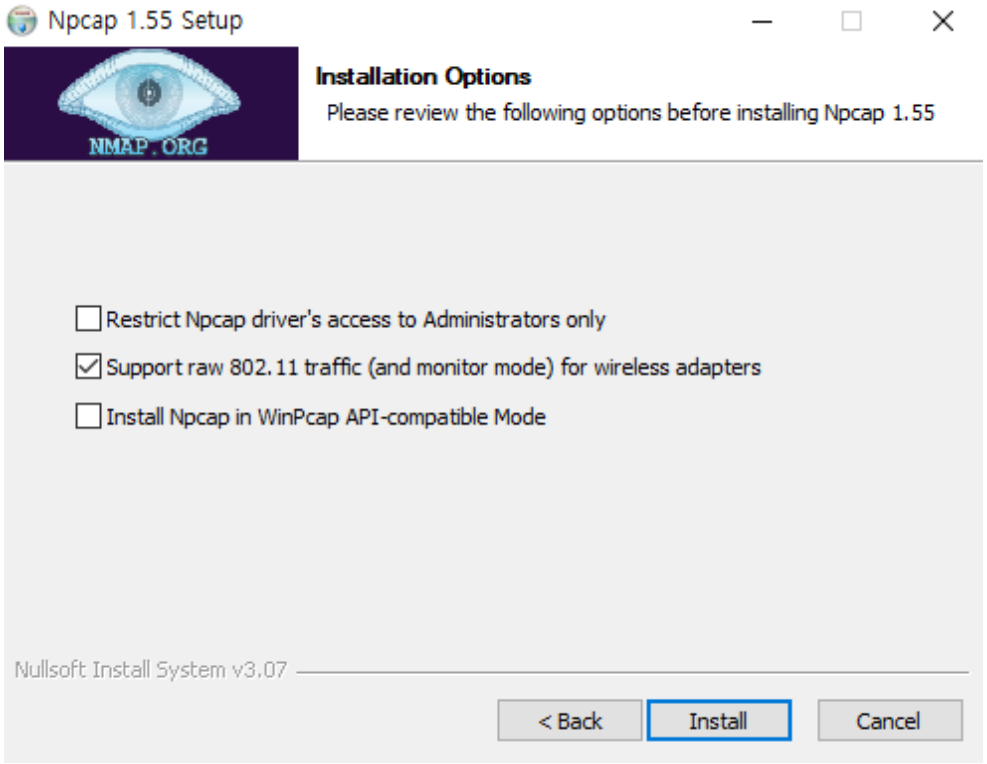
- Wireshark 다운로드: http://www.wireshark.org/download.html
- Wireshark 사용을 위해 Libcap 혹은 WinPCap 패킷 캡쳐 라이브러리를 지원해야함
- WinPCap 다운로드 : https://www.winpcap.org/install/default.htm
- Wireshark 설치과정중 Npcap 을 설치 할 것이냐, 라는 체크박스가 나옴
- 자료화면은 현재 WinPcap 혹은 Npcap 이 설치되어 있다면 그에 대한 버전을 보여주며, 없을 경우 Npcap 을 설치 선택 화면
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



Wireshark

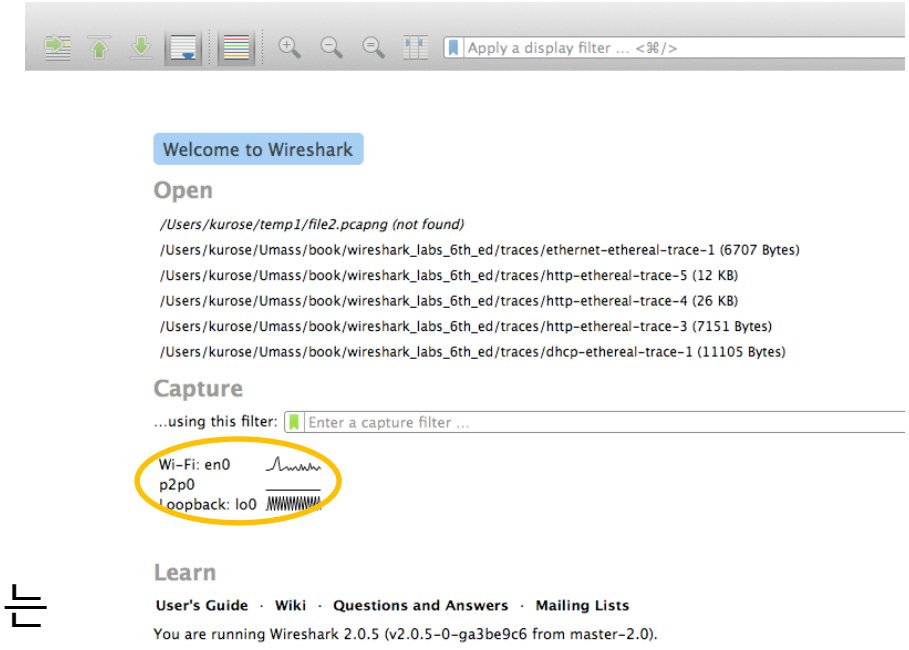
유선 사용시에는 상관없음.
무선 사용시에 이 실험을 진행하기 위해 추가 설정 내용으로 변경

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

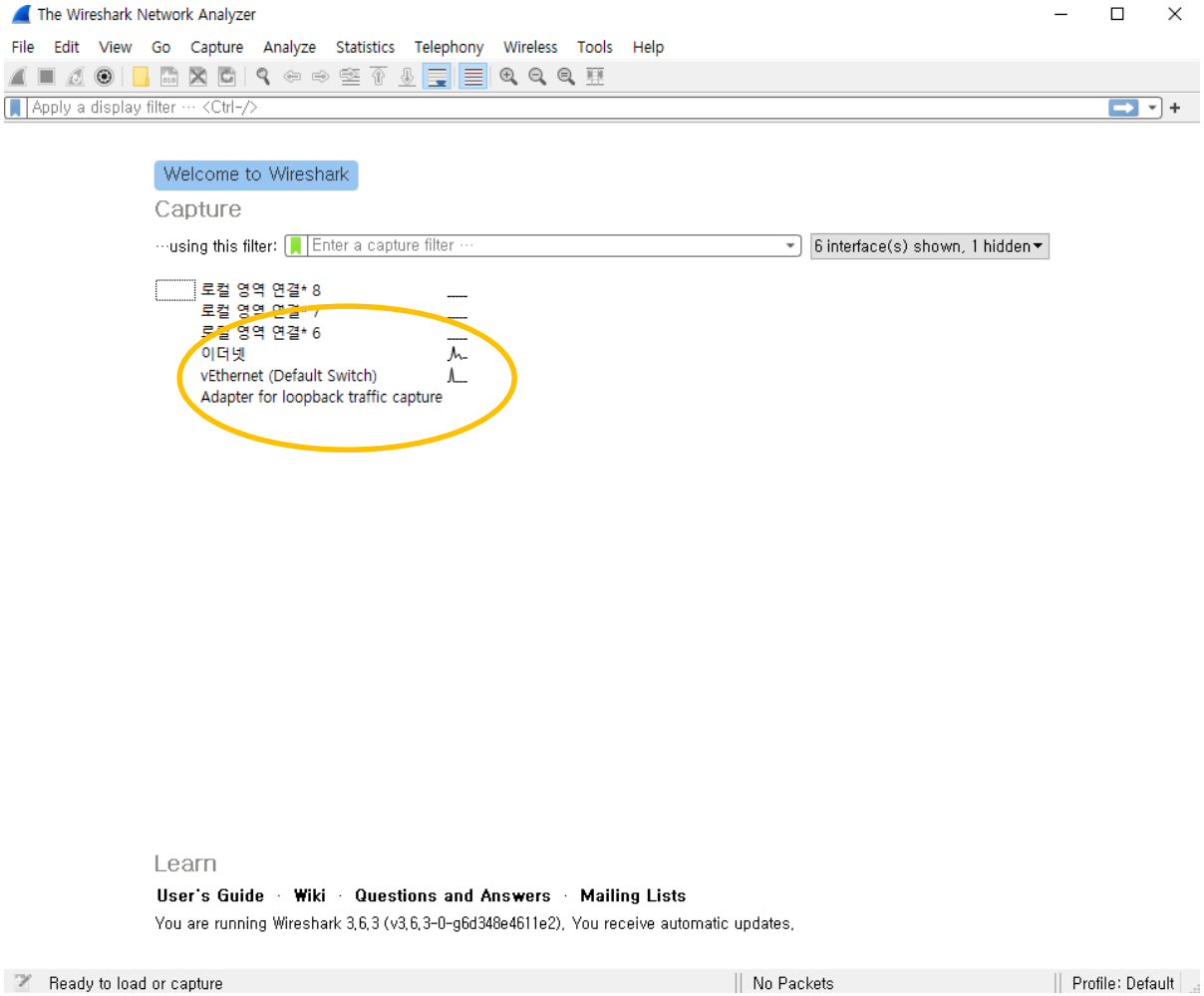
자료화면은 wi-fi 를 사용중인 환경에서 wireshark 를 실행시켰을때의 모습

이더넷을 사용할 경우 이더넷에 해당하는 항목이 인식됨

해당 인터페이스를 더블클릭 할 경우 패킷캡쳐를 시작

Wireshark 사용법

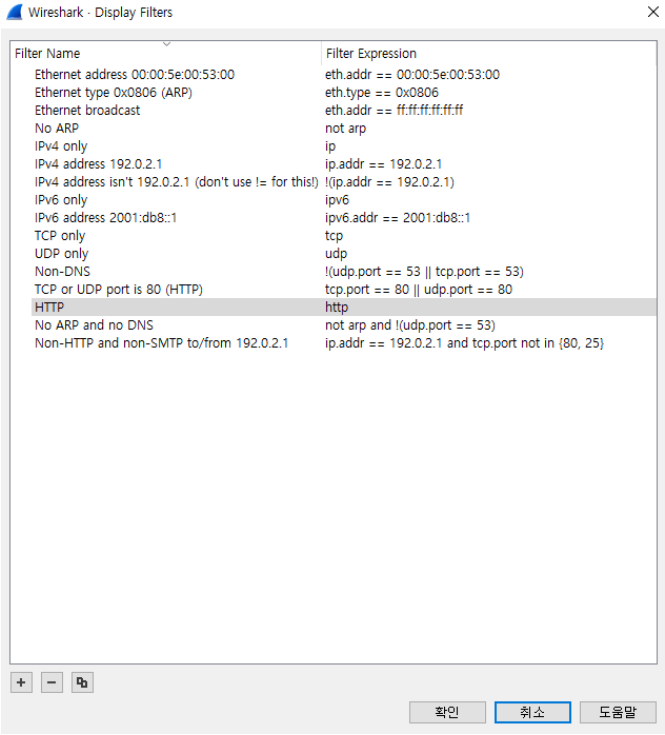
- 해당 자료화면은 이더넷을 사용중인 화면
- 사용하고 있는 모든 어댑터의 정보가 나옴



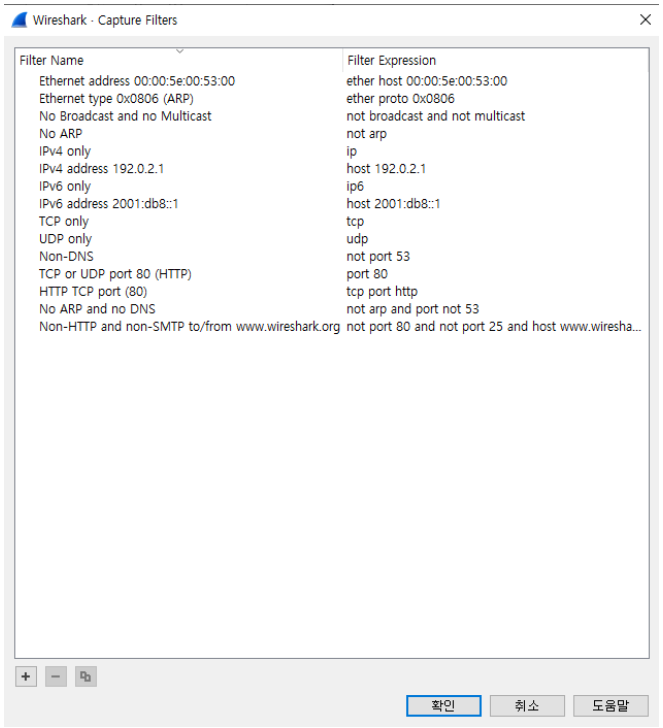
Wireshark 사용법

주기능 중 하나인 필터링

Analyze_Display Filters.. 을 선택 시 Diplay 할 내용에 대한 filter 가 나옴 좌측 하단의 + 와 – 를 통해 원하는 필터 추가/삭제 가능



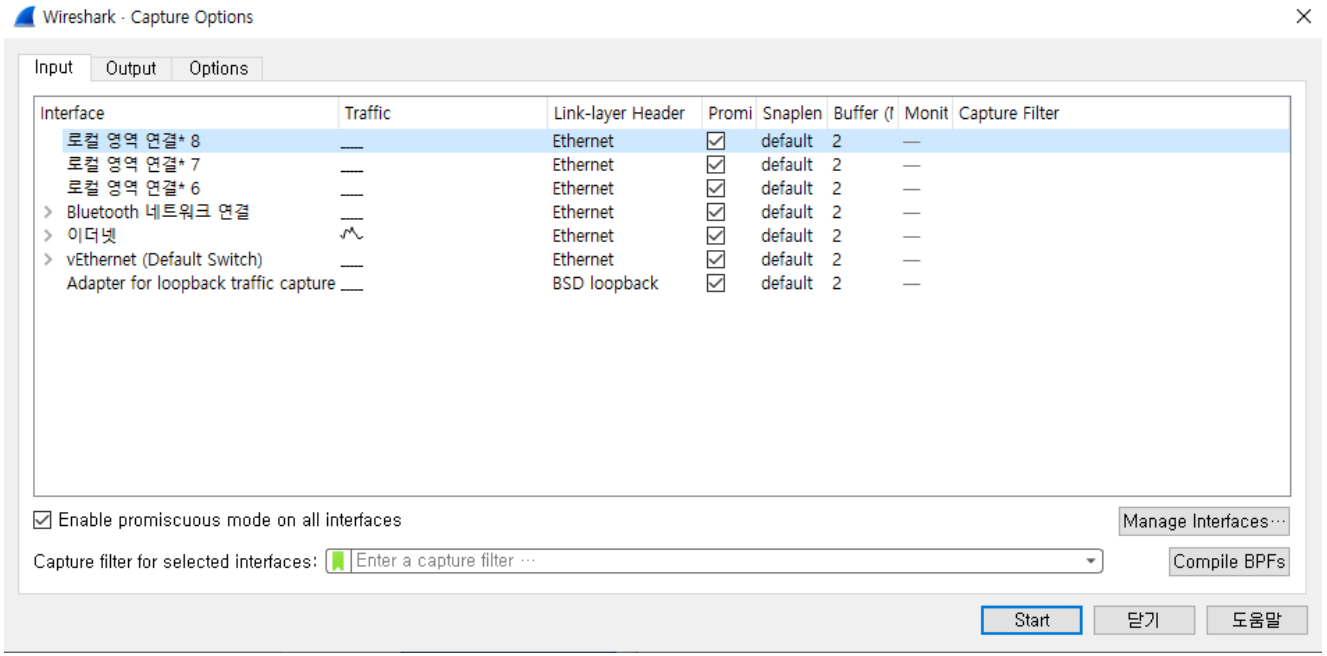
Capture_Capture Filters..을 선택 시 Capture 할 내용에 대한 filter 가 나옴 좌측 하단의 + 와 – 를 통해 원하는 필터 추가/삭제 가능



Wireshark 사용법

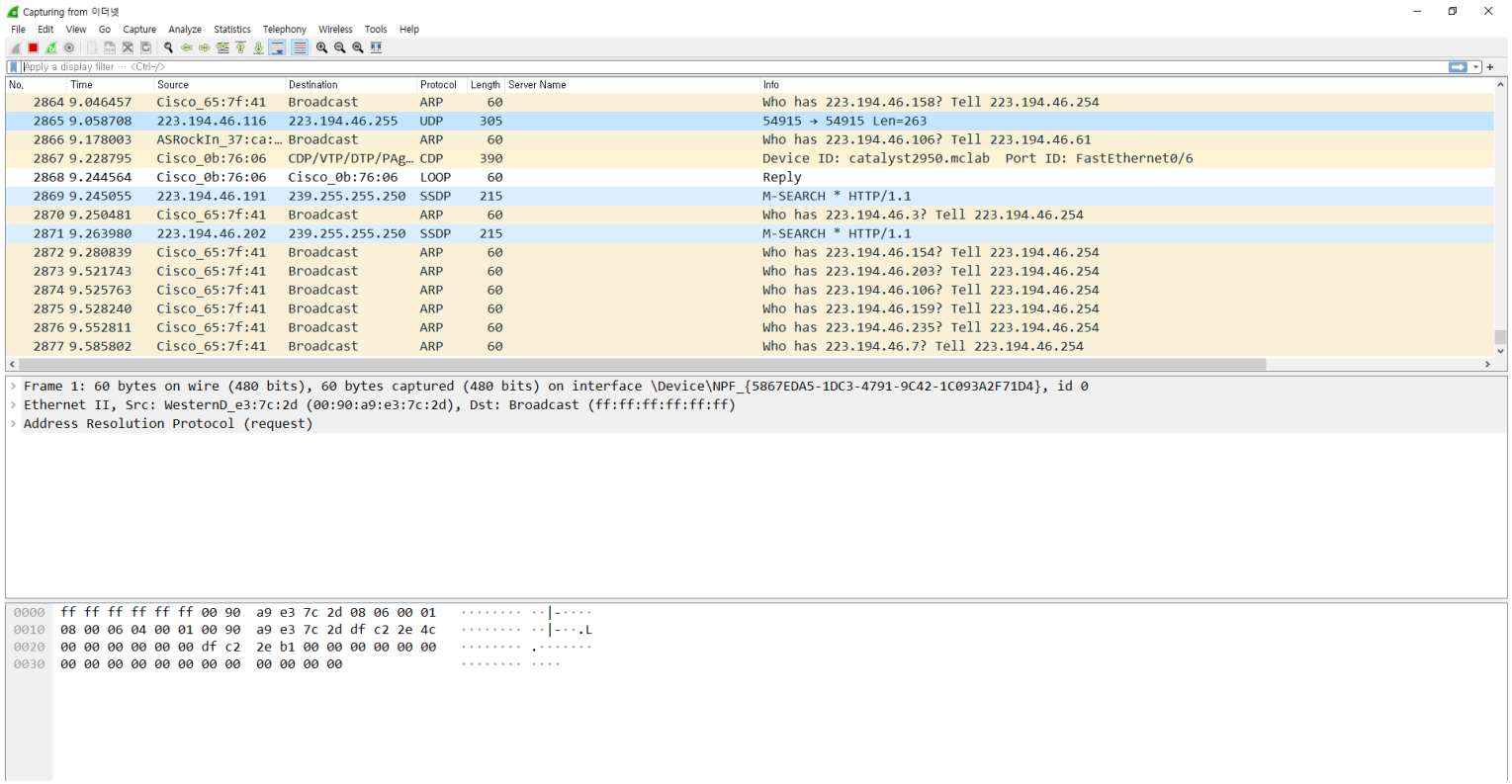
상단 메뉴에서 Capture_Options 를 클릭 할 경우(자료화면)

원하는 인터페이스를 선택하고 Start 를 눌러 패킷캡쳐를 실행 가능



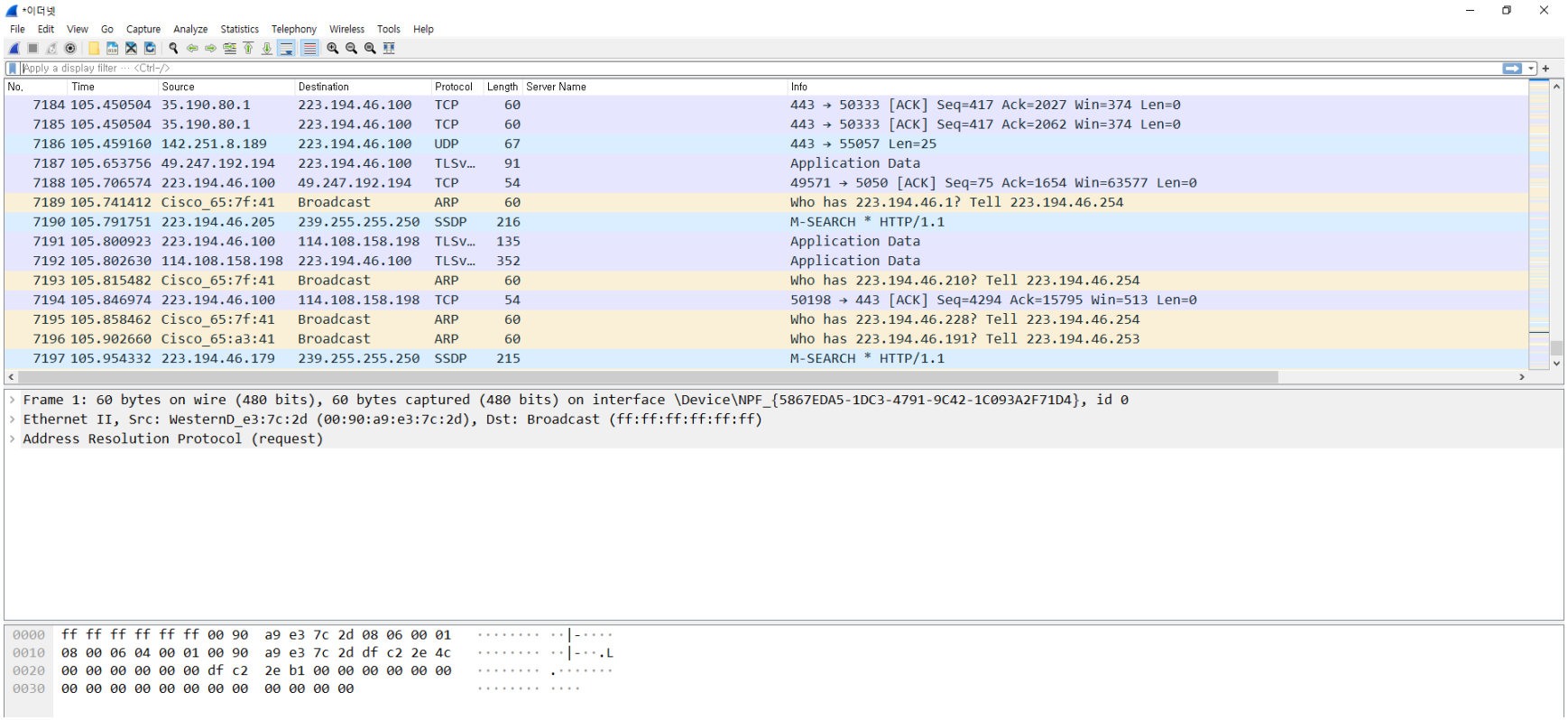
Wireshark 사용법

이더넷을 선택할 경우의 화면



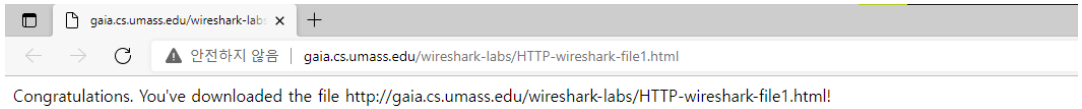
Wireshark 사용법

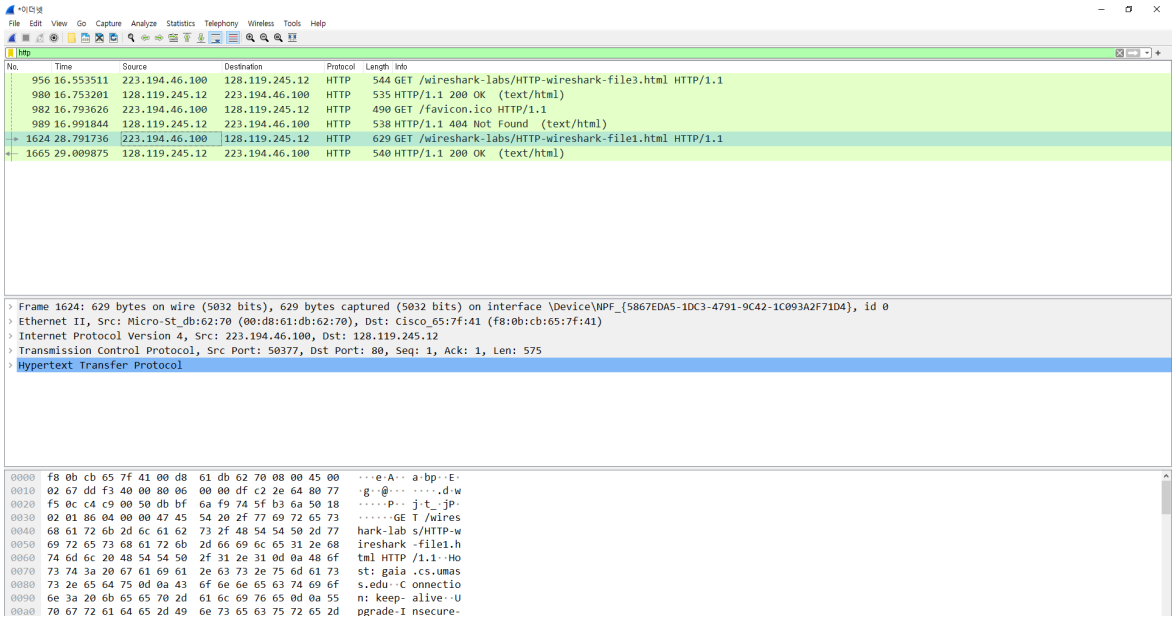
이전 화면과 차이점 :
좌측 상단의 적색 사각형 버튼을 누름으로 인해 패킷 캡쳐를 정지하여 현재까지 캡쳐한 정보만을 보여줌



Wireshark 사용법

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

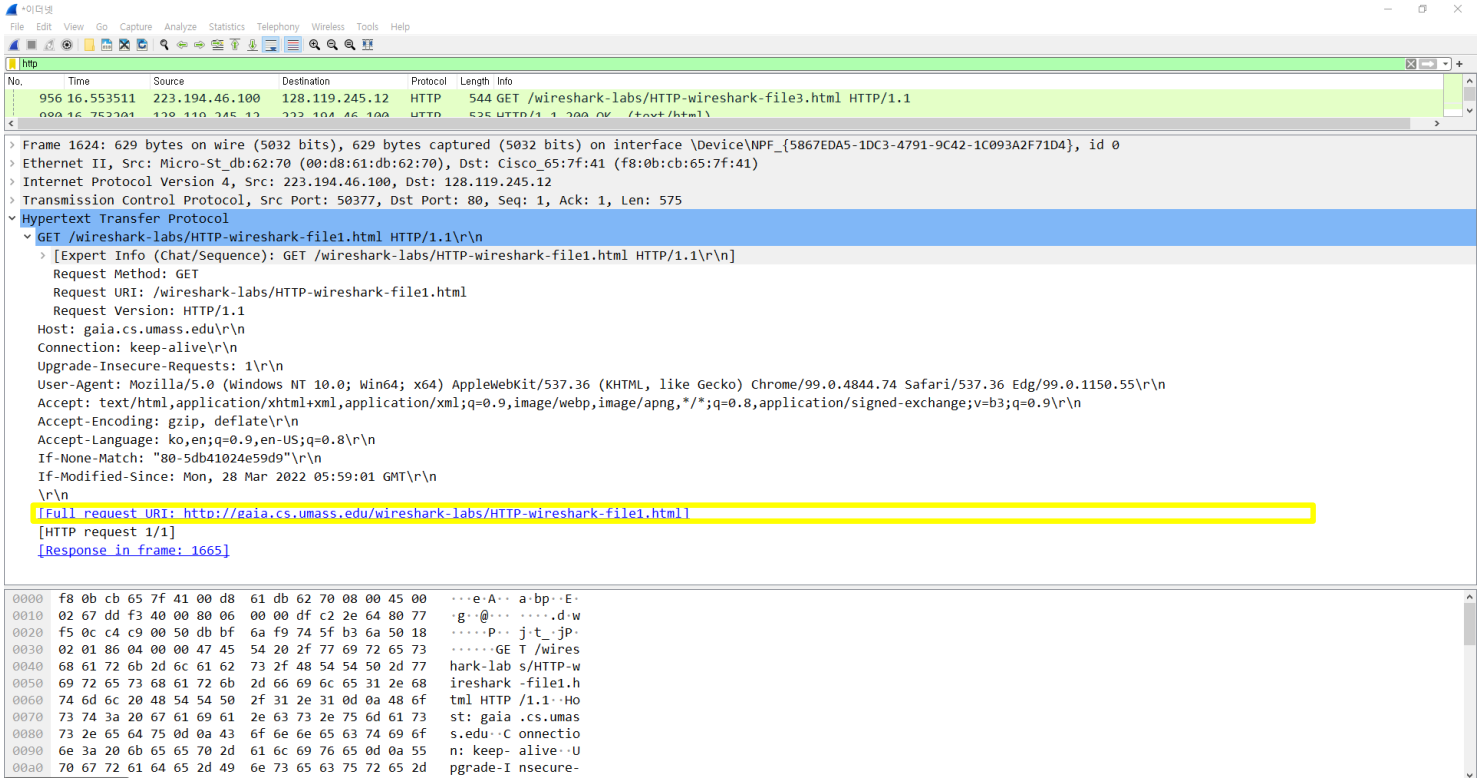




wireshark display filter 를 이용하여, http 에 관련한 정보만을 display

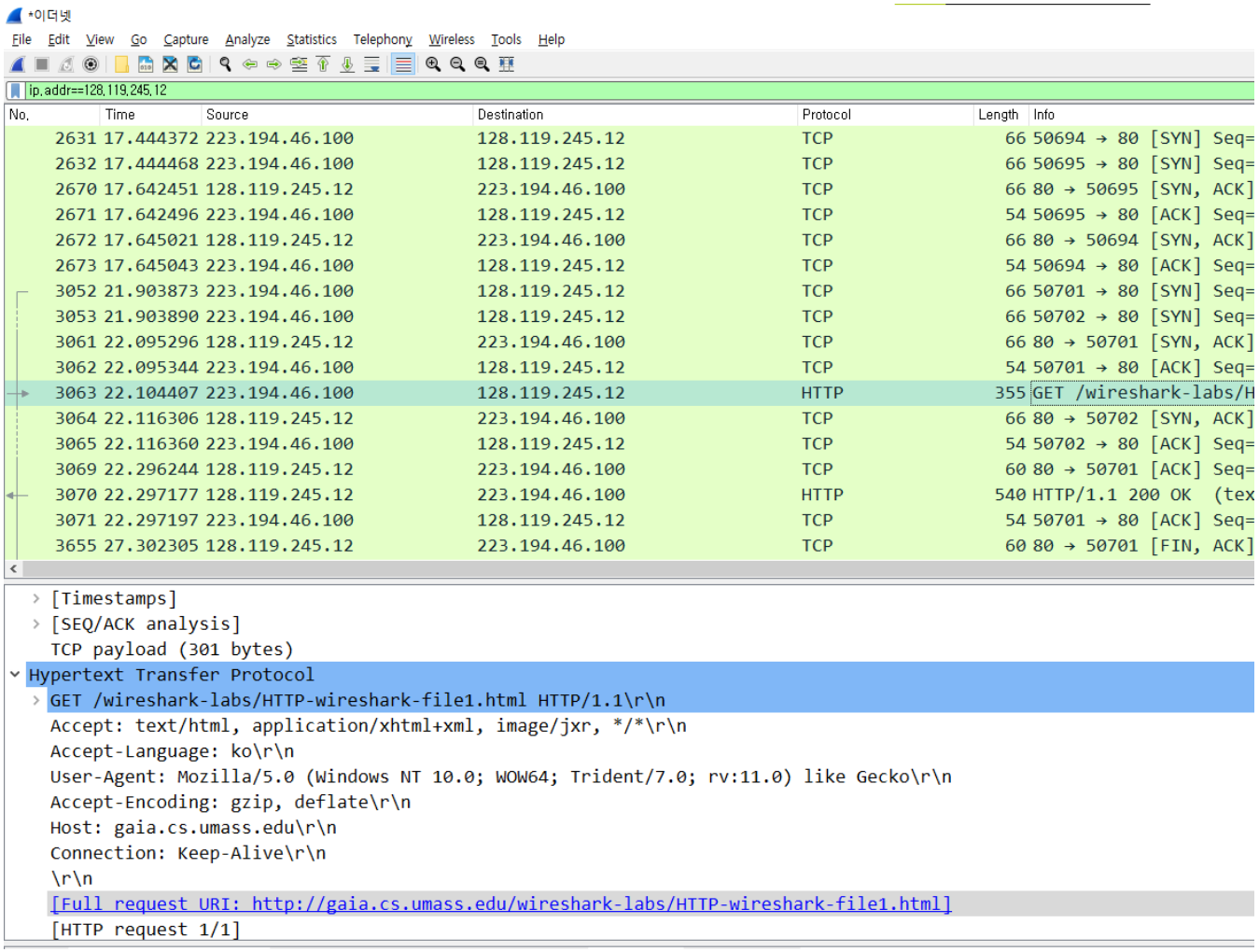
Wireshark 사용법

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



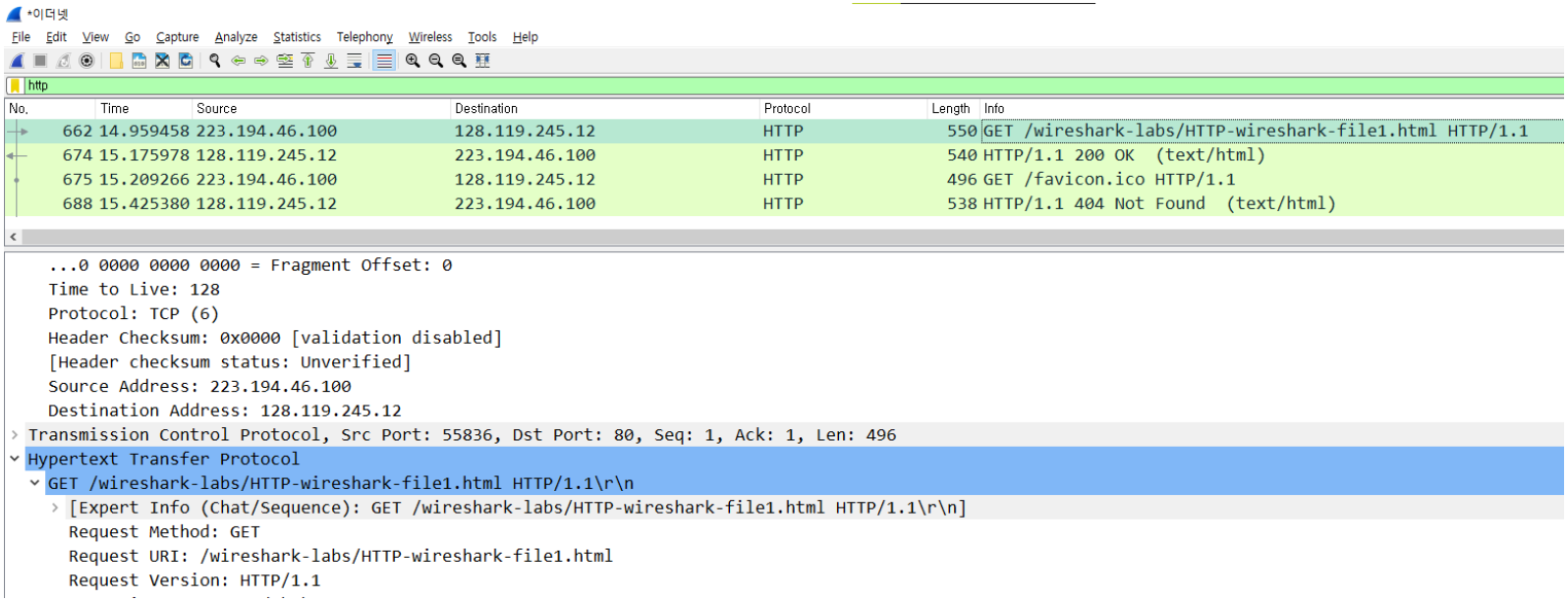
Wireshark 사용법

Wireshark display 필터를 이용하여,
IP주소를 기준으로 필터링 한 모습



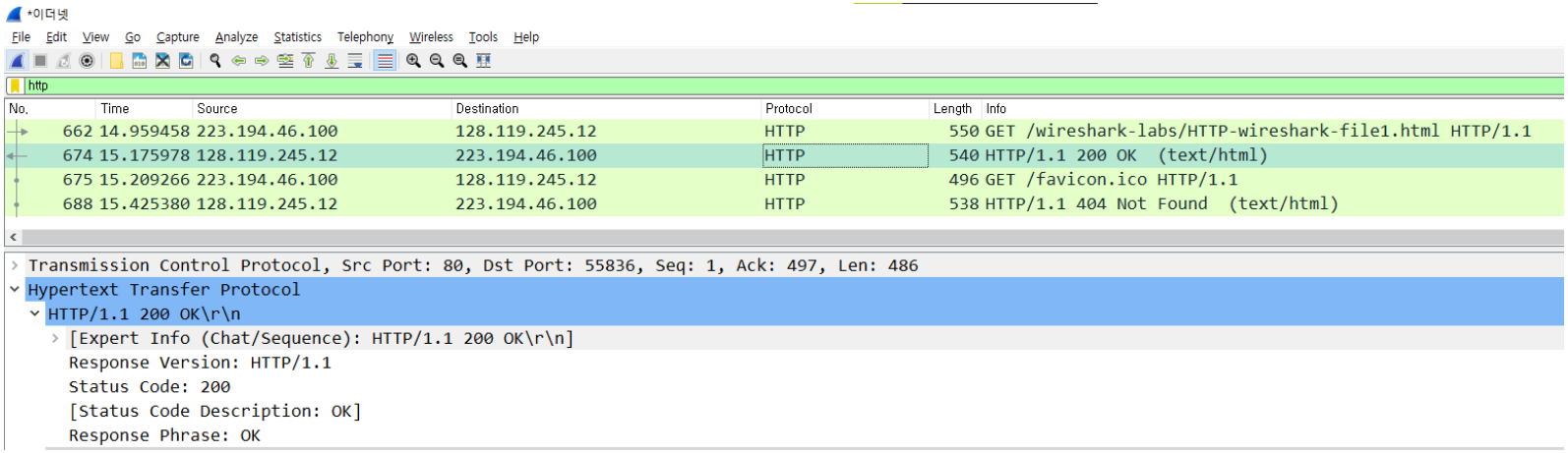
Wireshark 사용법

223.194.46.100 에서 128.119.245.12 로 request 를 보낸 모습

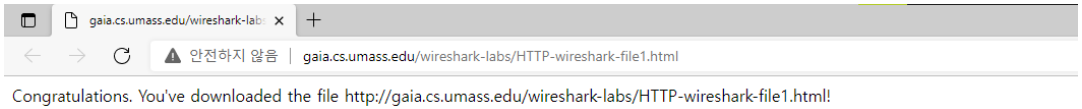


Wireshark 사용법

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 캡쳐를 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'

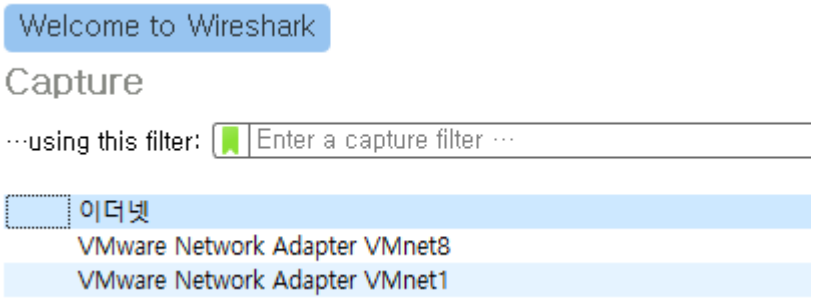
Question #1

- CMD 혹은 terminal 에서 IP 화면 캡쳐하기.
- 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 보여주기 위해 사용됨

Question #1

- PC 에서 동작중인 Wireshark 화면 캡쳐



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	[redacted]	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	[redacted]	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

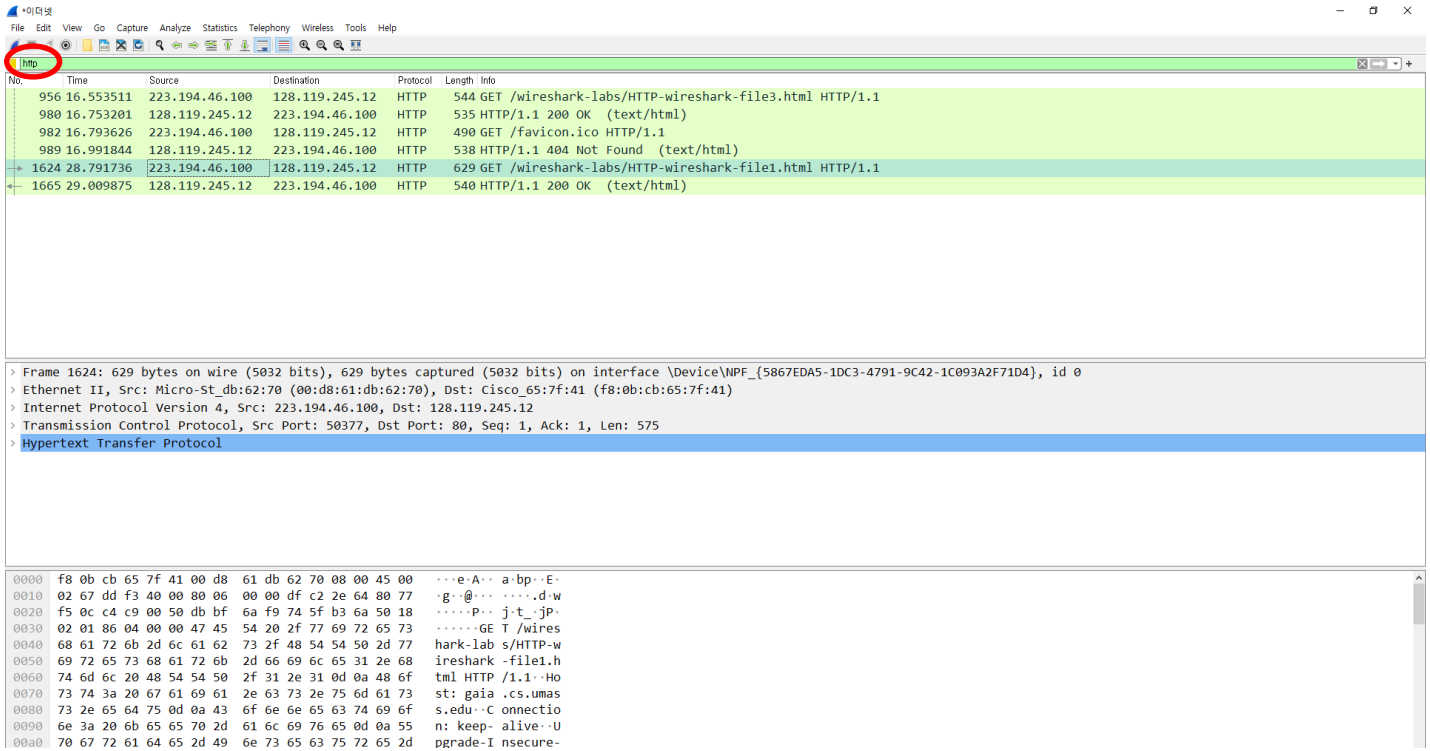
결과 화면 캡쳐 및 해당 캡쳐 화면에 대한 설명 서술 필수

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

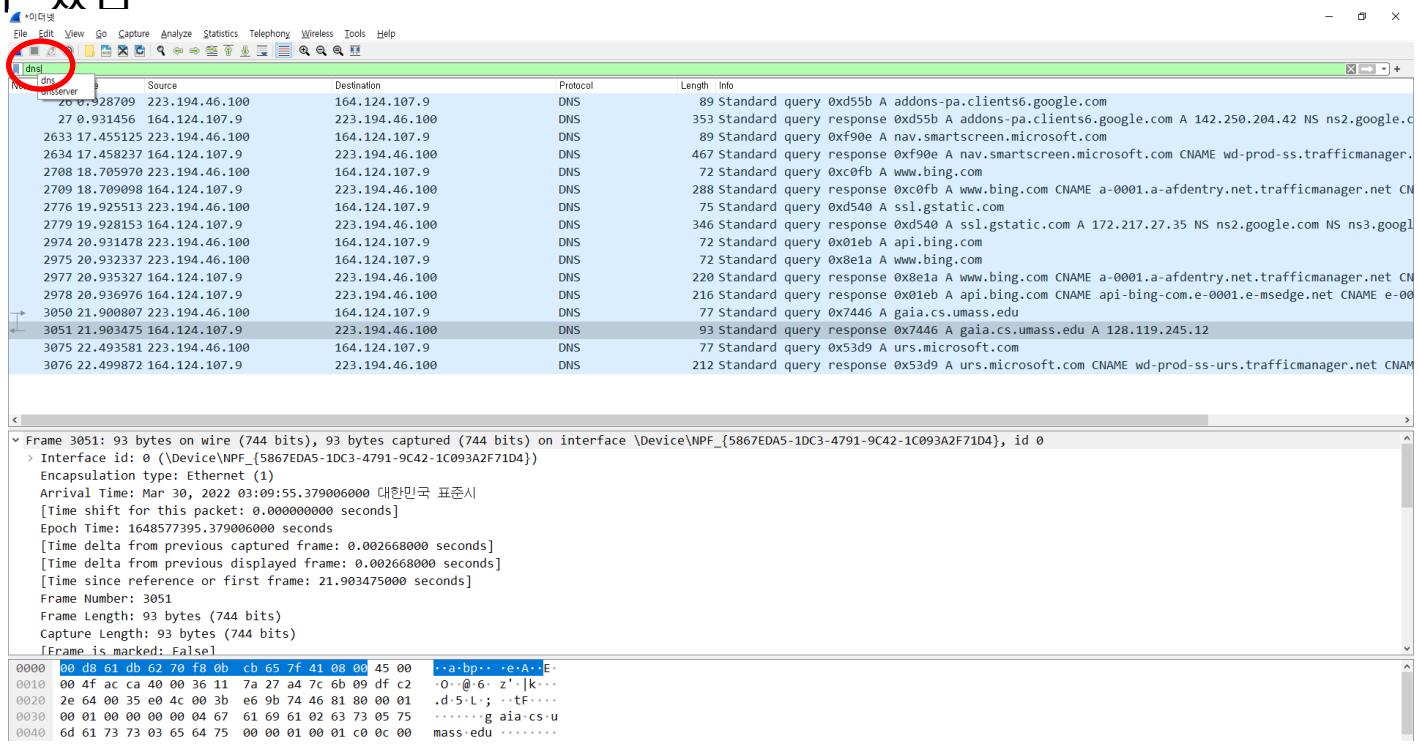
결과 화면 캡쳐 및 해당 캡쳐 화면에 대한 설명 서술 필수

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

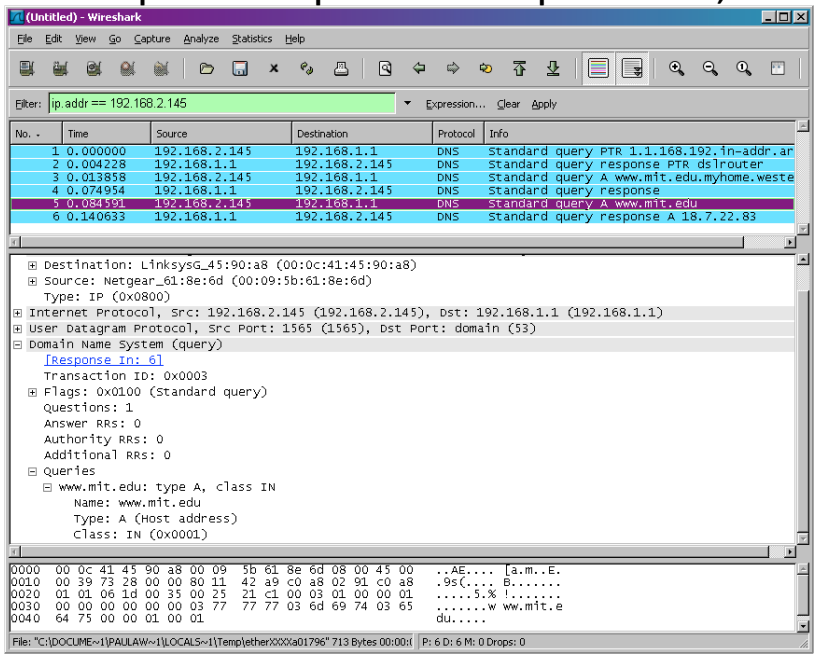


Wireshark_DNS_v7.0

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 포멧: **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 캡쳐 및 해당 화면에 대한 설명
- 결론 및 고찰
  → 5 줄 이상

질문