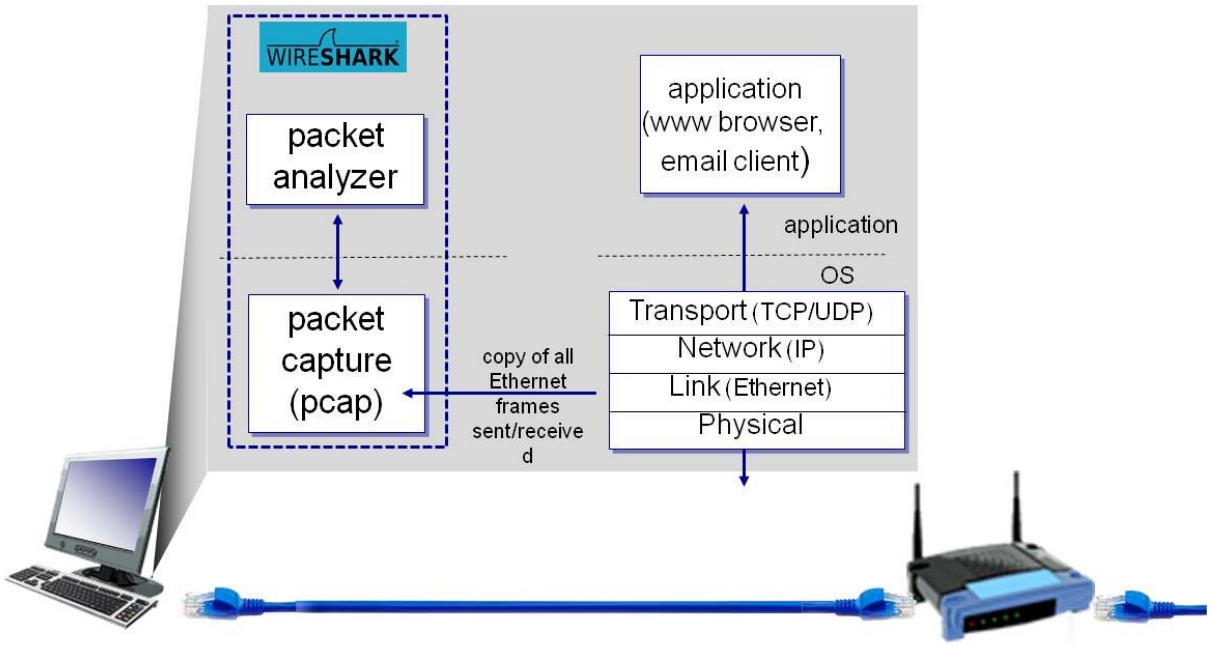
Wireshark 소개

순천향대학교 컴퓨터공학과
이 상 정

패킷 스니퍼 (Packet Sniffer) 소개

- 패킷 스니퍼 (packet sniffer)
  - 프로토콜을 실행하는 실체들 간에 교환되는 메시지를 관찰하는 도구
  - 컴퓨터에서 송수신되는 메시지를 캡처하고 저장
  - 캡처된 메시지의 프로토콜 필드들의 내용을 디스플레이
- 패킷 스니퍼는 두 부분으로 구성
  - 패킷 캡처 라이브러리 (packet capture library)
    - 컴퓨터에서 송수신되는 모든 링크 계층 프레임의 복사본을 수신
      - HTTP, FTP, TCP, UDP, DNS, IP 등 상위 계층 프로토콜의 메시지는 모두 링크 계층 프레임에 캡슐화
      - PC 상에서는 이더넷 프레임
  - 패킷 분석기 (packet analyzer)
    - 프로토콜 메시지 내의 모든 필드들의 내용을 분석하여 디스플레이

패킷 스니퍼 구조



Wireshark 패킷 스니퍼

❑ Wireshark 패킷 스니퍼

- http://www.wireshark.org/
- 다양한 계층의 프로토콜 스택에서 송수신되는 메시지의 내용을 디스플레이
- 엄밀한 의미에서 Wireshark는 패킷 분석기
  - 설치된 컴퓨터의 패킷 캡처 라이브러리를 이용
- 다양한 문서 및 매뉴얼: http://www.wireshark.org/docs/
  - 사용자 가이드 (User's Guide): http://www.wireshark.org/docs/wsug_html_chunked/
  - 매뉴얼 : http://www.wireshark.org/docs/man-pages/
  - FAQ: http://www.wireshark.org/faq.html
- 최근 버전은 Wireshark 2.4.1 (2017년 9월 현재)

Wireshark 다운로드 및 설치

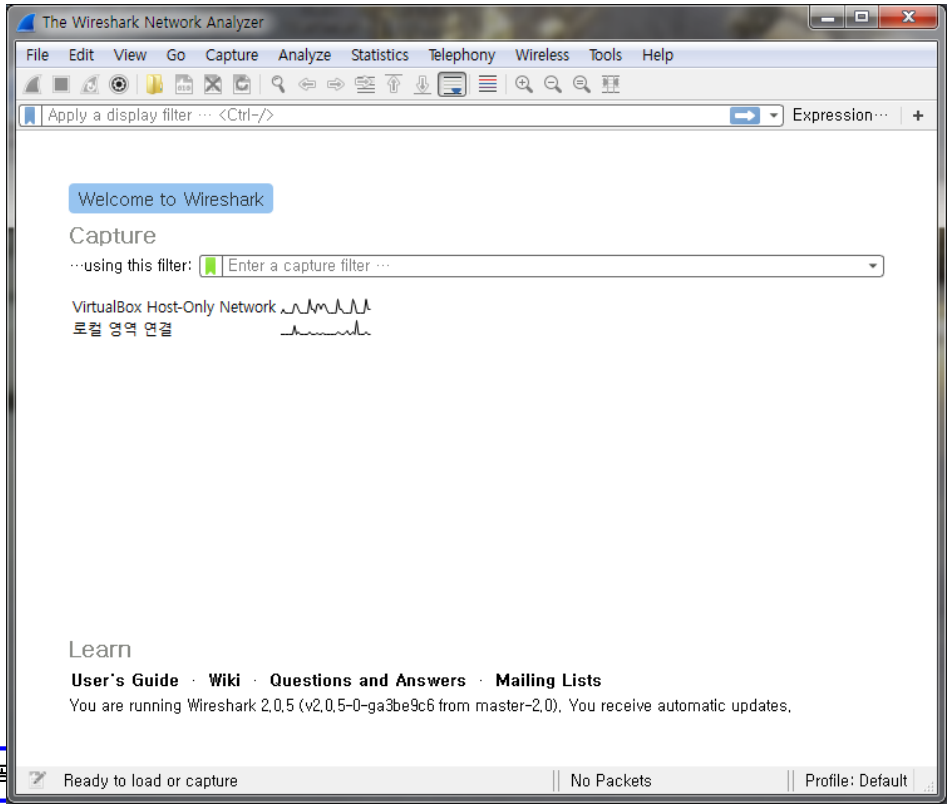
❑ 다운로드

- https://www.wireshark.org/#download 에서 다운로드
  - 운영체제 버전에 맞게 다운로드
    - Wireshark-win32-2.4.1.exe
    - Wireshark-win64-2.4.1.exe

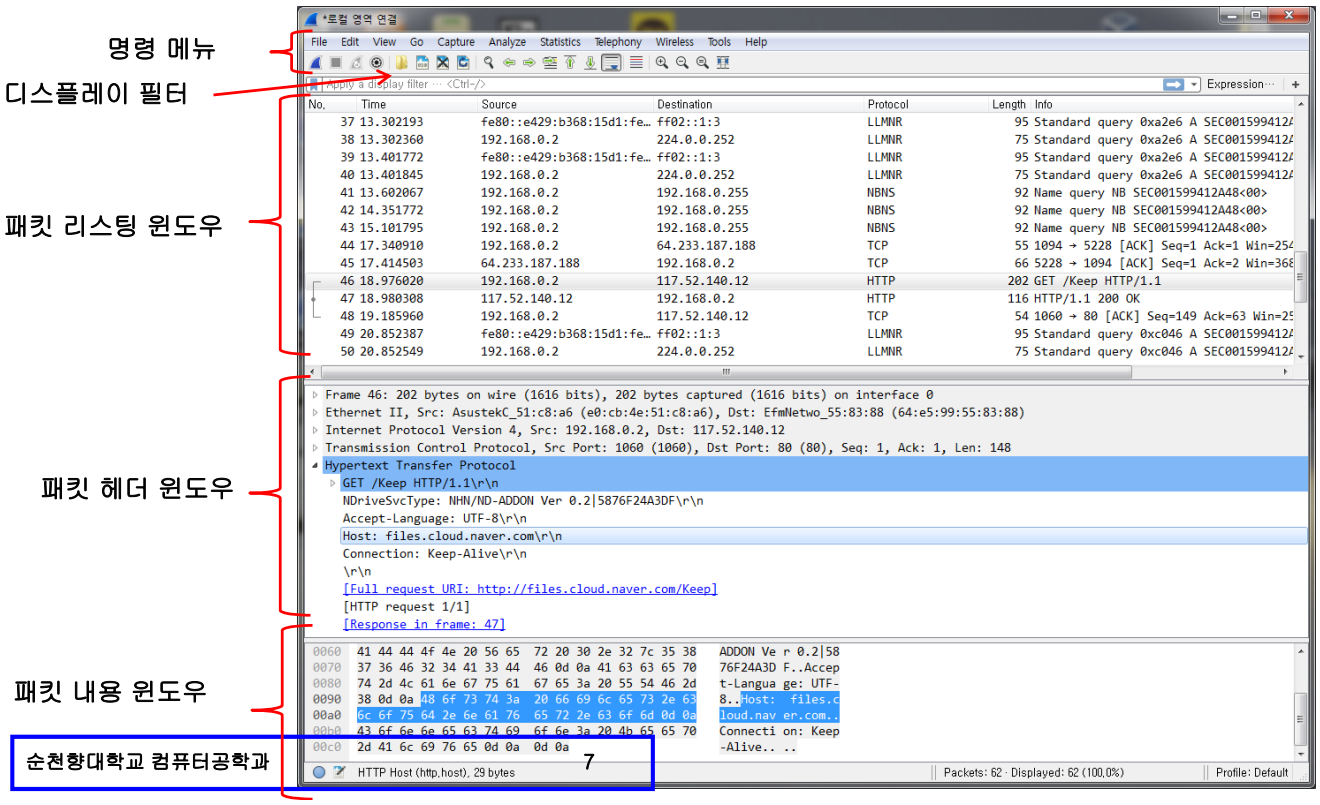
❑ 설치

- 다운로드 파일 실행하여 설치
- 설치 시 운영체제에 패킷 캡처 라이브러리가 없으면 자동으로 설치

초기 실행 화면

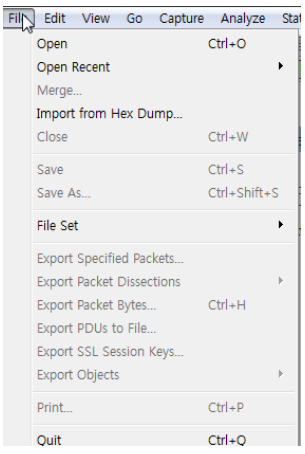


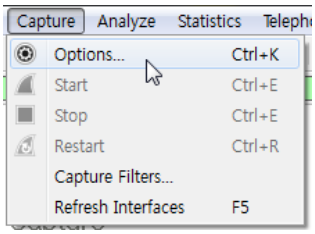
Wireshark 인터페이스 (1)



Wireshark 인터페이스 (2)

- 명령 메뉴 (command menu)
  - File 메뉴
    - 캡처된 패킷을 저장
    - 이전에 저장된 패킷들을 오픈
    - Wireshark 종료
  - Capture 메뉴
    - 패킷 캡처를 시작
      - Options – Start





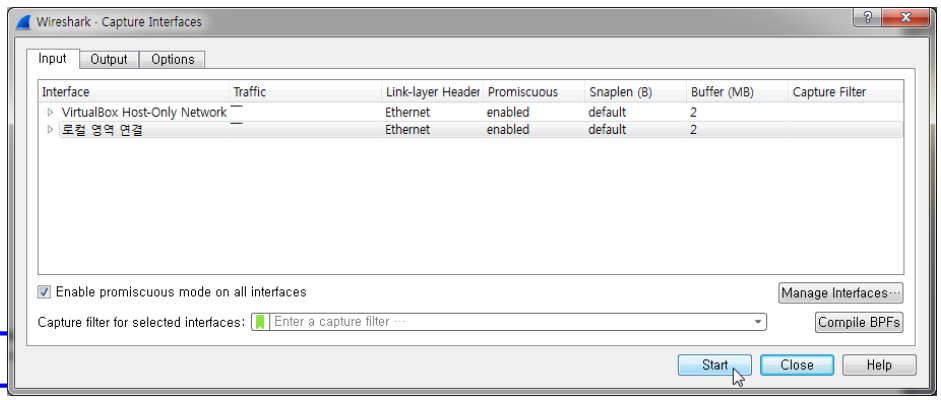
- 패킷 리스팅 윈도우 (packet-listing window)
  - 캡처된 패킷의 한 줄 요약을 디스플레이
  - 패킷 캡처 시간, 소스와 목적지 주소, 프로토콜 종류 등을 기술

Wireshark 인터페이스 (3)

- 패킷 헤더 윈도우 (packet-header details window)
  - 패킷 리스팅 윈도우에서 선택된 패킷에 대한 상세한 내용을 표시
  - 이 패킷을 포함하는 이더넷, IP 프레임 표시
  - +, – 박스 선택하여 확장, 축소 가능
- 패킷 내용 윈도우 (packet-contents window)
  - 캡처된 프레임 전체를 ASCII, 16진수로 표시
- 패킷 디스플레이 필터 (packet display filter) 필드
  - 프로토콜를 입력하여 패킷 리스팅 윈도우에 디스플레이 되는 정보를 필터링

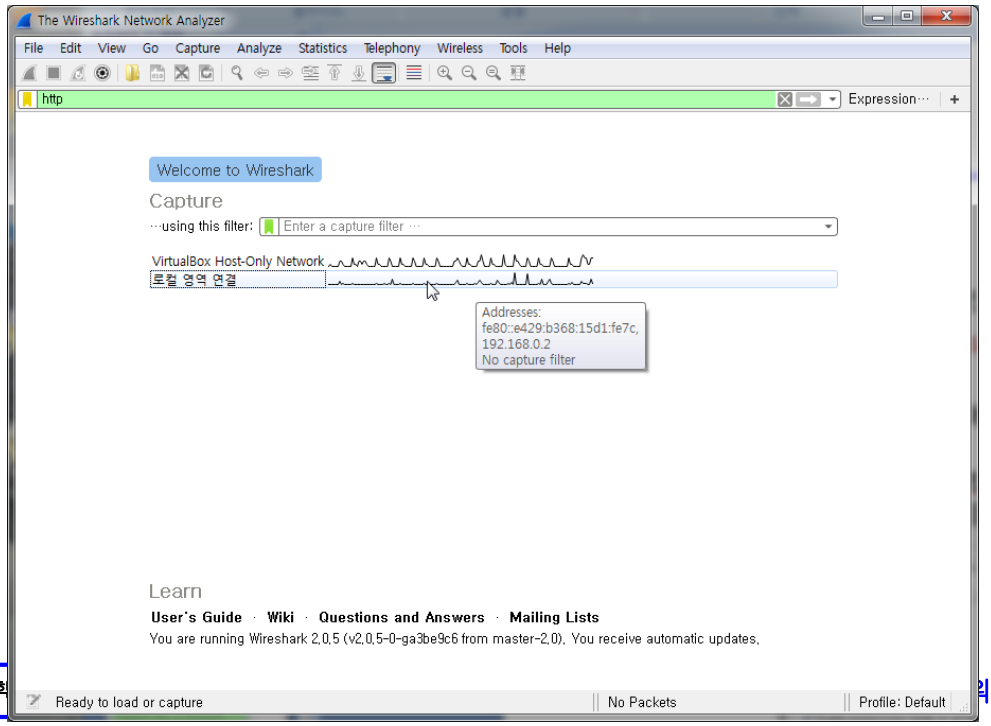
Wireshark 실행 예 (1)

1. Wireshark 실행
2. 패킷 캡처 옵션 설정 및 실행
   - Caputre –Options 메뉴 선택
   - Capture Options 윈도우
     - 대부분 디폴트 선택
     - 컴퓨터에 네트워크 인터페이스가 여러 개인 경우 캡처할 인터페이스 하나 선택
     - Start 버튼 클릭하여 패킷 캡처 시작



Wireshark 실행 예 (2)

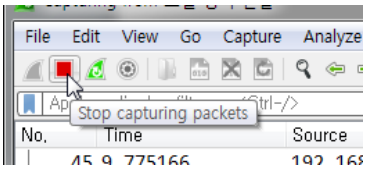
- 또는 배경 화면의 Interface 선택하여 패킷 캡처 시작

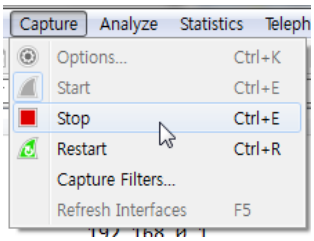


컴퓨터 네트워크

Wireshark 실행 예 (2)

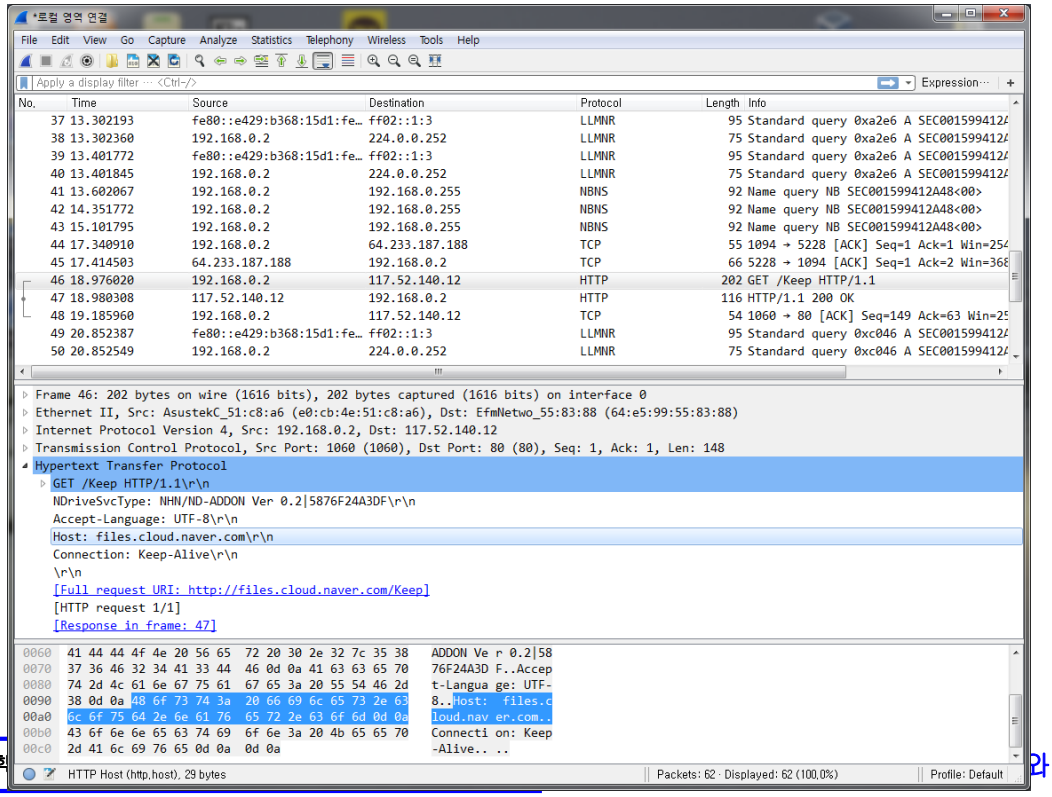
3. Wireshark 실행 중에 특정 웹 페이지에 접속
4. 웹 페이지가 브라우저에 표시되면 패킷 캡처 요약 윈도우에서 Stop 버튼을 클릭하여 패킷 캡처를 중지
   - 패킷이 캡처된 Wireshark 메인 윈도우 표시





6. 메인 윈도우 "디스플레이 필터"에 http 입력 후 Apply 클릭
   - 패킷 리스팅 윈도우에 HTTP 메시지만 표시
7. 패킷 리스팅 윈도우에서 첫 번째 http 메시지(GET 메시지)를 선택하면 패킷 헤더 윈도우에 HTTP GET 메시지 표시
8. Wireshark 종료

패킷이 캡처된 메인 윈도우



패킷이 필터된 메인 윈도우