Wireshark 프로그램 이란?

[자유 및 오픈 소스](https://ko.wikipedia.org/wiki/%EC%9E%90%EC%9C%A0_%EB%B0%8F_%EC%98%A4%ED%94%88_%EC%86%8C%EC%8A%A4_%EC%86%8C%ED%94%84%ED%8A%B8%EC%9B%A8%EC%96%B4)[패킷 분석](https://ko.wikipedia.org/wiki/%ED%8C%A8%ED%82%B7_%EA%B0%80%EB%A1%9C%EC%B1%84%EA%B8%B0) 프로그램이다. [네트워크](https://ko.wikipedia.org/wiki/%EC%BB%B4%ED%93%A8%ED%84%B0_%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC)의 문제, 분석, 소프트웨어 및 [통신 프로토콜](https://ko.wikipedia.org/wiki/%ED%86%B5%EC%8B%A0_%ED%94%84%EB%A1%9C%ED%86%A0%EC%BD%9C) 개발, 교육에 쓰인다. 원래 이름은 **Ethereal**이었으나 2006년 5월에 상표 문제로 말미암아 와이어샤크로 이름을 바꾸었다.

와이어샤크는 [크로스 플랫폼](https://ko.wikipedia.org/wiki/%ED%81%AC%EB%A1%9C%EC%8A%A4_%ED%94%8C%EB%9E%AB%ED%8F%BC)으로, [Qt](https://ko.wikipedia.org/wiki/Qt_(%ED%94%84%EB%A0%88%EC%9E%84%EC%9B%8C%ED%81%AC))[위젯 툴킷](https://ko.wikipedia.org/wiki/%EC%9C%84%EC%A0%AF_%ED%88%B4%ED%82%B7)을 이용하여 사용자 인터페이스를 제공하며, [pcap](https://ko.wikipedia.org/wiki/Pcap)을 이용하여 패킷을 포획한다. [리눅스](https://ko.wikipedia.org/wiki/%EB%A6%AC%EB%88%85%EC%8A%A4), [맥 OS X](https://ko.wikipedia.org/wiki/%EB%A7%A5_OS_X), [BSD](https://ko.wikipedia.org/wiki/BSD), [솔라리스](https://ko.wikipedia.org/wiki/%EC%86%94%EB%9D%BC%EB%A6%AC%EC%8A%A4_(%EC%9A%B4%EC%98%81_%EC%B2%B4%EC%A0%9C))를 포함한 다양한 [유닉스 계열](https://ko.wikipedia.org/wiki/%EC%9C%A0%EB%8B%89%EC%8A%A4_%EA%B3%84%EC%97%B4)[운영 체제](https://ko.wikipedia.org/wiki/%EC%9A%B4%EC%98%81_%EC%B2%B4%EC%A0%9C)와 [마이크로소프트 윈도](https://ko.wikipedia.org/wiki/%EB%A7%88%EC%9D%B4%ED%81%AC%EB%A1%9C%EC%86%8C%ED%94%84%ED%8A%B8_%EC%9C%88%EB%8F%84)에서 동작한다. GUI가 없는 터미널 기반 버전인 티샤크(TShark)도 제공한다. 와이어샤크, 또 TShark와 같은 프로그램과 함께 배포되는 여러 프로그램들은 [자유 소프트웨어](https://ko.wikipedia.org/wiki/%EC%9E%90%EC%9C%A0_%EC%86%8C%ED%94%84%ED%8A%B8%EC%9B%A8%EC%96%B4)로, [GNU 일반 공중 사용 허가서](https://ko.wikipedia.org/wiki/GNU_%EC%9D%BC%EB%B0%98_%EA%B3%B5%EC%A4%91_%EC%82%AC%EC%9A%A9_%ED%97%88%EA%B0%80%EC%84%9C)의 조건으로 공개된다. 와이어샤크는 각기 다른 네트워크 프로토콜의 구조를 이해하는 소프트웨어이다. 그러므로 각기 다른 네트워크 프로토콜이 규정한 각기 다른 패킷의 의미와 더불어 필드와 요약 정보를 보여줄 수 있다. 와이어샤크는 [pcap](https://ko.wikipedia.org/wiki/Pcap)을 이용하여 캡처를 포획하므로 pcap이 지원하는 종류의 네트워크의 패킷만 포획할 수 있다.

 실시간 네트워크 연결의 유선으로부터 데이터를 포획하고, 이미 포획한 패킷을 기록해둔 파일로부터 데이터를 읽을 수 있다.

 실시간 데이터를 [이더넷](https://ko.wikipedia.org/wiki/%EC%9D%B4%EB%8D%94%EB%84%B7), [IEEE 802.11](https://ko.wikipedia.org/wiki/IEEE_802.11), [PPP](https://ko.wikipedia.org/wiki/%EC%A0%90%EB%8C%80%EC%A0%90_%ED%94%84%EB%A1%9C%ED%86%A0%EC%BD%9C), [루프백](https://ko.wikipedia.org/wiki/%EB%A3%A8%ED%94%84%EB%B0%B1)을 포함한 수많은 네트워크로부터 읽을 수 있다.

 포획한 네트워크 데이터는 [GUI](https://ko.wikipedia.org/wiki/%EA%B7%B8%EB%9E%98%ED%94%BD_%EC%82%AC%EC%9A%A9%EC%9E%90_%EC%9D%B8%ED%84%B0%ED%8E%98%EC%9D%B4%EC%8A%A4)나 터미널 ([명령 줄](https://ko.wikipedia.org/wiki/%EB%AA%85%EB%A0%B9_%EC%A4%84_%EC%9D%B8%ED%84%B0%ED%8E%98%EC%9D%B4%EC%8A%A4)) 버전의 유틸리티 TShark를 통해 탐색할 수 있다.

 포획한 파일들은 editcap 프로그램으로의 명령 줄 스위치를 통하여 프로그래밍하듯이 편집하거나 변환할 수 있다.

 데이터 표현은 디스플레이 필터를 이용하여 정리할 수 있다.

 새로운 프로토콜 분석을 위해 [플러그인](https://ko.wikipedia.org/wiki/%ED%94%8C%EB%9F%AC%EA%B7%B8%EC%9D%B8)을 만들 수 있다.

 포획한 트래픽 내의 [VoIP](https://ko.wikipedia.org/wiki/VoIP) 호출을 감지할 수 있다. 호환되는 인코딩으로 부호화되면 미디어 플로도 재생할 수 있다.

 와이어샤크를 통해 순수 [USB](https://ko.wikipedia.org/wiki/USB) 트래픽을 포획할 수 있다.[[2]](https://ko.wikipedia.org/wiki/%EC%99%80%EC%9D%B4%EC%96%B4%EC%83%A4%ED%81%AC#cite_note-2) 이 기능은 현재 리눅스에서만 이용할 수 있다.

와이어샤크의 순수 네트워크 추적 파일 포맷은 [libpcap 및 WinPcap](https://ko.wikipedia.org/wiki/Pcap)이 지원하는 libpcap 형식으로 되어 있으므로 [tcpdump](https://ko.wikipedia.org/wiki/Tcpdump)와 [CA](https://ko.wikipedia.org/w/index.php?title=CA_(%EA%B8%B0%EC%97%85)&action=edit&redlink=1)[넷마스터](https://ko.wikipedia.org/w/index.php?title=%EB%84%B7%EB%A7%88%EC%8A%A4%ED%84%B0&action=edit&redlink=1)를 포함하여 동일한 포맷을 이용하는 다른 응용 프로그램들과 네트워크 추적 파일을 상호 이용할 수 있다. 또, [snoop](https://ko.wikipedia.org/w/index.php?title=Snoop&action=edit&redlink=1), 네트워크 제너럴의 스니퍼, [마이크로소프트 네트워크 모니터](https://ko.wikipedia.org/w/index.php?title=%EB%A7%88%EC%9D%B4%ED%81%AC%EB%A1%9C%EC%86%8C%ED%94%84%ED%8A%B8_%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC_%EB%AA%A8%EB%8B%88%ED%84%B0&action=edit&redlink=1)와 같은 다른 네트워크 가로채기 프로그램으로부터 포획한 데이터를 읽을 수도 있다.

Wireshark는 어떠한 라이브러리를 사용하는가?

패킷 캡쳐시 리눅스 상에서는 Libpcap, 윈도우 상에서는 Winpcap 라이브러리를 사용하여 패킷을 수집할 경우, 확장자가 .PCAP이라는 파일 포맷(File Format)으로 처리된다.