**와이어샤크 WireShark**

***Signed by HyeonGyu(Member1)***

**소개**

**와이어샤크(Wireshark)**는 [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 Ethereal이었으나 2006년 5월에 상표 문제로 말미암아 와이어샤크로 이름을 바꾸었다. GUI지원 및 크로스플랫폼으로 윈도우 32bit, 64bit, 리눅스, 유닉스, 솔라리스 등등 거의 모든 운영체제를 지원한다. 무료이며 막강한 기능으로 네크워크 패킷 감시용으로는 최고 프로그램이다.

**기능**

**와이어샤크**는 [tcpdump](https://ko.wikipedia.org/wiki/Tcpdump" \o "Tcpdump)와 매우 비슷하지만 [그래픽](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) [프론트엔드](https://ko.wikipedia.org/wiki/%ED%94%84%EB%A1%A0%ED%8A%B8%EC%97%94%EB%93%9C%EC%99%80_%EB%B0%B1%EC%97%94%EB%93%9C)에 정렬, 필터링 옵션이 몇 가지 추가된 점이 다르다. 와이어샤크는 사용자가 [무차별 모드](https://ko.wikipedia.org/w/index.php?title=%EB%AC%B4%EC%B0%A8%EB%B3%84_%EB%AA%A8%EB%93%9C&action=edit&redlink=1)(promiscuous mode)를 지원하는 네트워크 인터페이스를 해당 모드에 추가할 수 있는 기능을 제공한다. 이로써 인터페이스의 구성 주소와 브로드캐스트/멀티캐스트 트래픽을 포함한 모든 트래픽이 해당 인터페이스에 나타난다. 그러나 [네트워크 스위치](https://ko.wikipedia.org/wiki/%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC_%EC%8A%A4%EC%9C%84%EC%B9%98) 포트의 무차별 모드에서 패킷 가로채기로 말미암아 포획을 할 때 스위치를 통하는 모든 트래픽이 꼭 포획하는 포트를 거치는 것은 아니다. 그러므로 무차별 모드에서의 포획은 네트워크의 트래픽을 모두 확인하지는 못한다. [포트 미러링](https://ko.wikipedia.org/wiki/%ED%8F%AC%ED%8A%B8_%EB%AF%B8%EB%9F%AC%EB%A7%81)이나 다양한 [네트워크 탭](https://ko.wikipedia.org/w/index.php?title=%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC_%ED%83%AD&action=edit&redlink=1)을 이용하면 네트워크 상의 어느 지점으로까지 포획 범위를 넓힐 수 있다. 단순한 수동 탭(passive tap)은 [악성 코드](https://ko.wikipedia.org/wiki/%EC%95%85%EC%84%B1_%EC%BD%94%EB%93%9C) [탬퍼링 방지](https://ko.wikipedia.org/wiki/%ED%83%AC%ED%8D%BC%EB%A7%81_%EB%B0%A9%EC%A7%80) 기능이 매우 뛰어나다. [리눅스](https://ko.wikipedia.org/wiki/%EB%A6%AC%EB%88%85%EC%8A%A4), [BSD](https://ko.wikipedia.org/wiki/BSD), [맥 OS X](https://ko.wikipedia.org/wiki/%EB%A7%A5_OS_X)에서 [libpcap](https://ko.wikipedia.org/wiki/Pcap" \o "Pcap) 1.0.0 이후 버전으로 말미암아 와이어샤크 1.4 이후부터는 [와이파이](https://ko.wikipedia.org/wiki/%EC%99%80%EC%9D%B4%ED%8C%8C%EC%9D%B4) 어댑터를 감시 모드에 추가할 수 있게 되었다.

**특징**

**와이어샤크**는 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" \o "Pcap)을 이용하여 캡처를 포획하므로 pcap이 지원하는 종류의 네트워크의 패킷만 포획할 수 있다. 와이어샤크의 순수 네트워크 추적 파일 포맷은 [libpcap 및 WinPcap](https://ko.wikipedia.org/wiki/Pcap" \o "Pcap)이 지원하는 libpcap 형식으로 되어 있으므로 [tcpdump](https://ko.wikipedia.org/wiki/Tcpdump" \o "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.