

와이어샤크(Wireshark)는 자유 및 오픈 소스 패킷 분석 프로그램이다. 네트워크의 문제, 분석, 소프트웨어 및 통신 프로토콜 개발, 교육에 쓰인다. 원래 이름은 Ethereal이었으나 2006년 5월에 상표 문제로 말미암아 와이어샤크로 이름을 바꾸었다.

와이어샤크는 크로스 플랫폼으로, Qt 위젯 툴킷을 이용하여 사용자 인터페이스를 제공하며, pcap을 이용하여 패킷을 포획한다. 리눅스, 맥 OS X, BSD, 솔라리스를 포함한 다양한 유닉스 계열 운영 체제와 마이크로소프트 윈도에서 동작한다. GUI가 없는 터미널 기반 버전인 티샤크(TShark)도 제공한다. 와이어샤크, 또 TShark와 같은 프로그램과 함께 배포되는 여러 프로그램들은 자유 소프트웨어로, GNU 일반 공중 사용 허가서의 조건으로 공개된다.

기능

와이어샤크는 tcpdump와 매우 비슷하지만 그래픽 프론트엔드에 정렬, 필터링 옵션이 몇 가지 추가된 점이 다르다.

와이어샤크는 사용자가 무차별 모드(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 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 미러링이나 다양한 네트워크 탭을 이용하면 네트워크 상의 어느 지점으로까지 포획 범위를 넓힐 수 있다. 단순한 수동 탭(passive tap)은 악성 코드 탬퍼링 방지 기능이 매우 뛰어나다.

리눅스, BSD, 맥 OS X에서 libpcap 1.0.0 이후 버전으로 말미암아 와이어샤크 1.4 이후부터는 와이파이 어댑터를 감시 모드에 추가할 수 있게 되었다.

특징

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 pcap을 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, IEEE 802.11, PPP, 루프백을 포함한 수많은 네트워크로부터 읽을 수 있다.

포획한 네트워크 데이터는 GUI나 터미널 (명령 줄) 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 플러그인을 만들 수 있다.

포획한 트래픽 내의 VoIP 호출을 감지할 수 있다. 호환되는 인코딩으로 부호화되면 미디어 플로도 재생할 수 있다.

와이어샤크를 통해 순수 USB 트래픽을 포획할 수 있다.[2] 이 기능은 현재 리눅스에서만 이용할 수 있다.

와이어샤크의 순수 네트워크 추적 파일 포맷은 libpcap 및 WinPcap이 지원하는 libpcap 형식으로 되어 있으므로 tcpdump와 CA 넷마스터를 포함하여 동일한 포맷을 이용하는 다른 응용 프로그램들과 네트워크 추적 파일을 상호 이용할 수 있다. 또, snoop, 네트워크 제너럴의 스니퍼, 마이크로소프트 네트워크 모니터와 같은 다른 네트워크 가로채기 프로그램으로부터 포획한 데이터를 읽을 수도 있다.

출처 : 위키 백과-와이어샤크