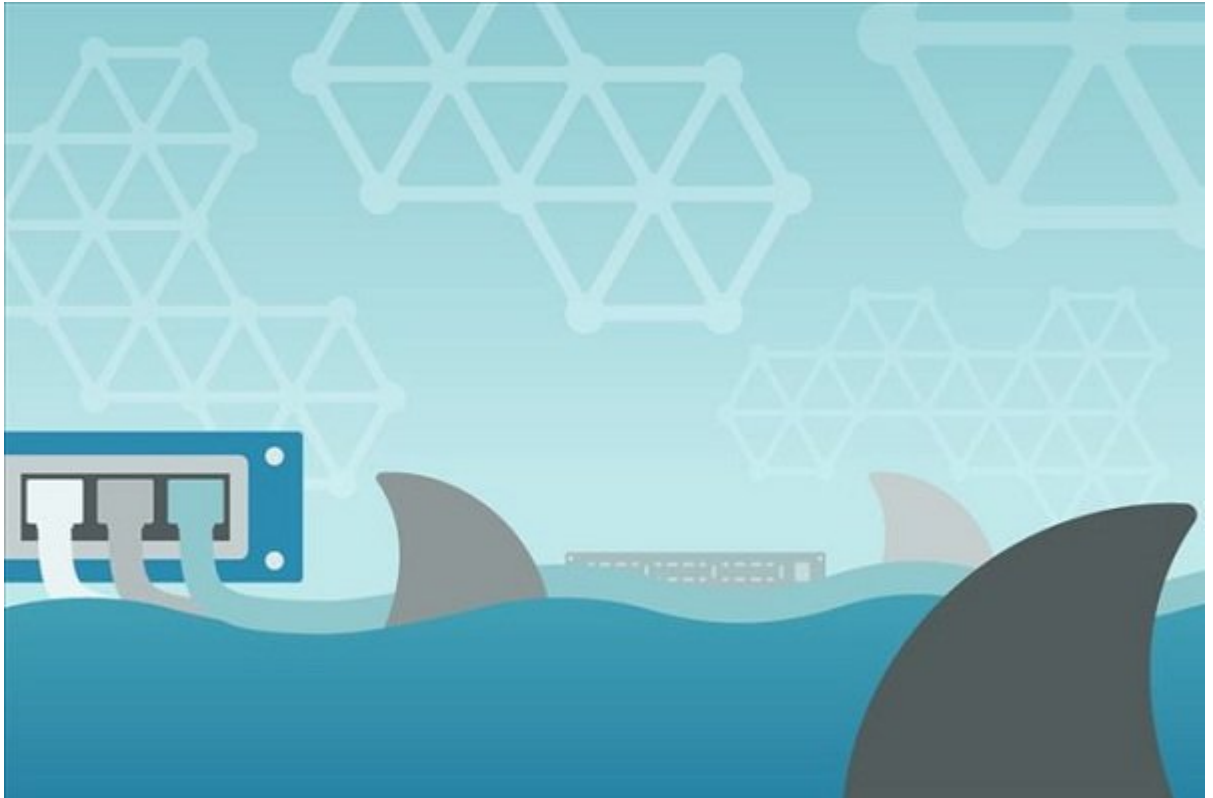


# 網路抓包工具 Wireshark 簡介



網路抓包工具 (Network Sniffing Tool) 是一種用於監控網路流量、分析網路封包的工具。它通常用於網路故障排除、安全分析、性能優化等場景。Wireshark 是目前最流行的網路抓包工具之一，它支援多種網路協議，並提供豐富的過濾和顯示功能。

網路抓包工具的原理是通過在網路介面卡 (NIC) 上安裝嗅探器 (Sniffer)，將經過該介面的所有網路封包抓取下來，並進行分析。Wireshark 支援多種網路協議，包括 TCP/IP、HTTP、FTP、SMTP、POP3、IMAP、LDAP、SMB、NFS、SSH、Telnet、FTP、SMTP、POP3、IMAP、LDAP、SMB、NFS、SSH、Telnet 等。它提供豐富的過濾和顯示功能，可以根據 IP 地址、端口、協議類型等條件進行過濾，並顯示抓取的封包內容。

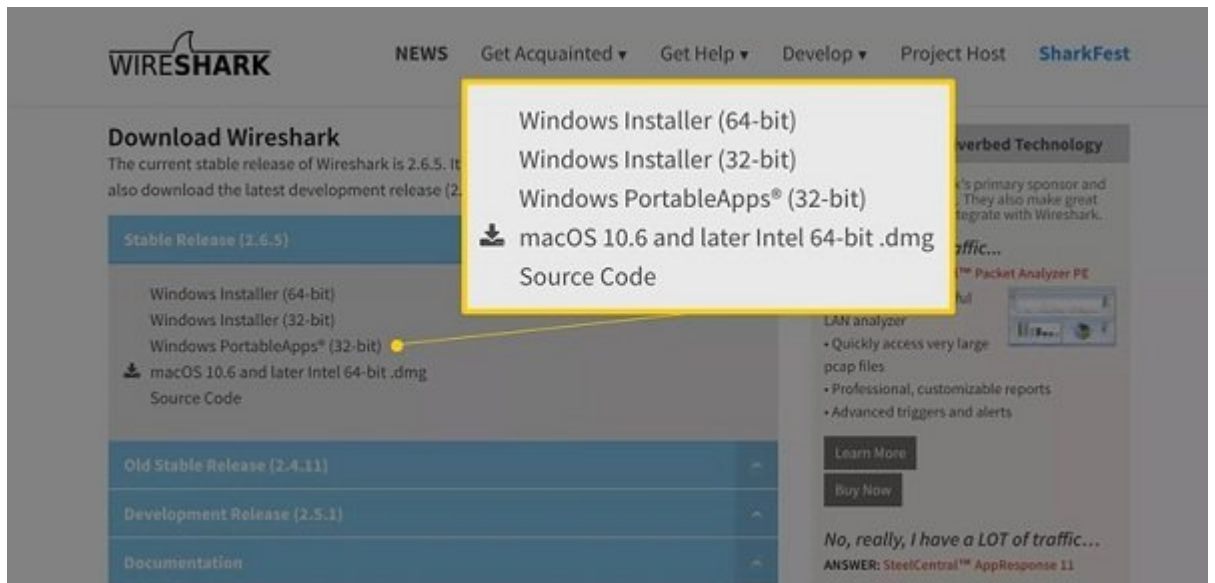
## Wireshark 簡介

Wireshark 是一個開源的網路抓包工具，它支援多種網路協議，並提供豐富的過濾和顯示功能。它通常用於網路故障排除、安全分析、性能優化等場景。Wireshark 支援多種網路協議，包括 TCP/IP、HTTP、FTP、SMTP、POP3、IMAP、LDAP、SMB、NFS、SSH、Telnet、FTP、SMTP、POP3、IMAP、LDAP、SMB、NFS、SSH、Telnet 等。它提供豐富的過濾和顯示功能，可以根據 IP 地址、端口、協議類型等條件進行過濾，並顯示抓取的封包內容。

OSI model layers. The first layer is the Physical layer, which deals with the physical transmission of data over a medium. The second layer is the Data Link layer, which deals with the reliable transfer of data between adjacent nodes. The third layer is the Network layer, which deals with the routing of data packets across multiple hops. The fourth layer is the Transport layer, which deals with the reliable end-to-end transfer of data. The fifth layer is the Session layer, which deals with the establishment, maintenance, and termination of a session between two communicating devices. The sixth layer is the Presentation layer, which deals with the representation of data. The seventh layer is the Application layer, which deals with the exchange of data between applications.

## Wireshark Installation

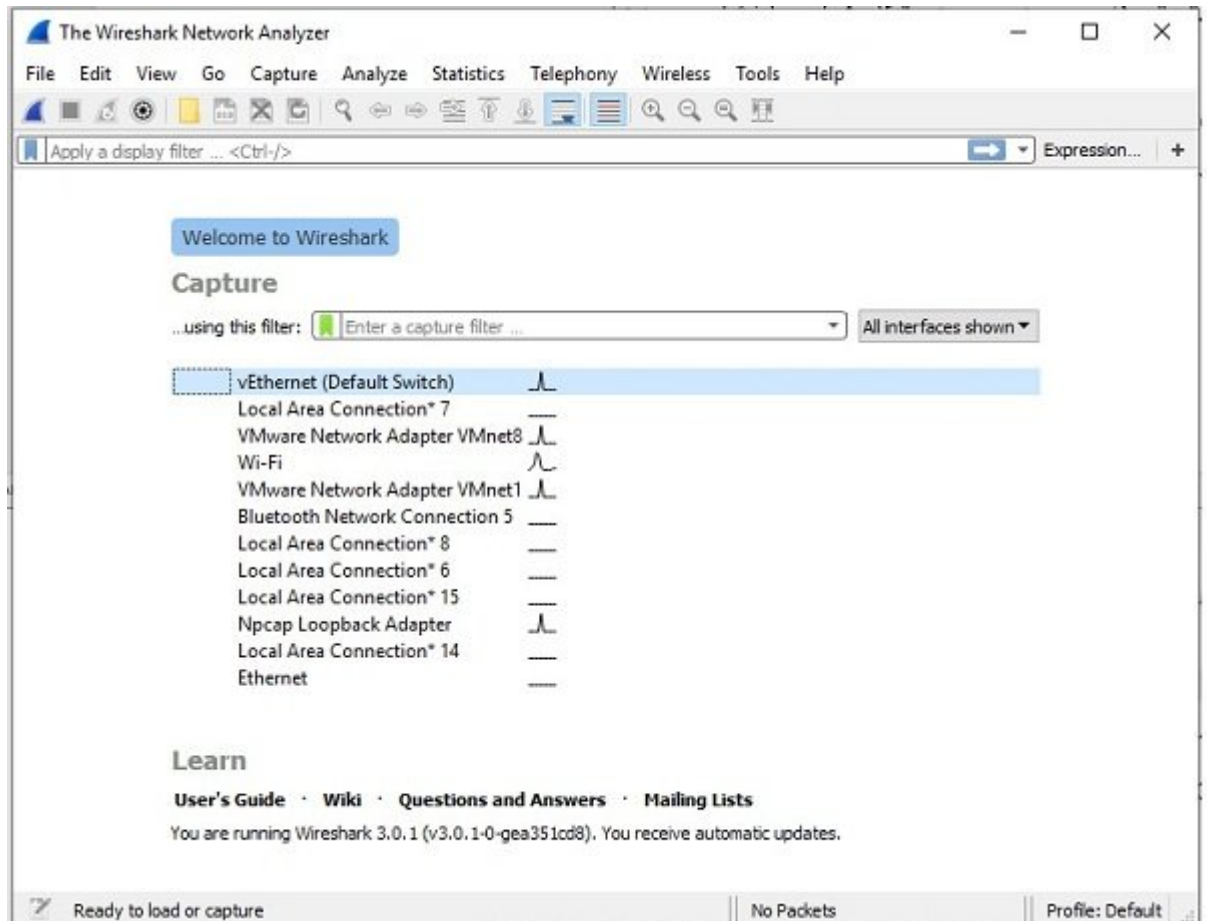
Wireshark is a free and open-source network protocol analyzer. It is used for capturing and analyzing network traffic. The first step in installing Wireshark is to visit the Wireshark Foundation website (1 link).



WinPcap is a free and open-source library for capturing network traffic. It is used for capturing and analyzing network traffic. The first step in installing WinPcap is to visit the WinPcap website. The website provides download links for Windows, Linux, and FreeBSD. The Windows download link is for the WinPcap 4.0.2 setup. The Linux download link is for the WinPcap 4.0.2 source code. The FreeBSD download link is for the WinPcap 4.0.2 source code. The third step is to install WinPcap. The installation process is simple and can be completed in a few minutes.

## Wireshark Configuration

Wireshark is a free and open-source network protocol analyzer. It is used for capturing and analyzing network traffic. The first step in configuring Wireshark is to install the WinPcap library. The second step is to configure the network interface. The third step is to configure the capture filter. The fourth step is to configure the display filter. The fifth step is to configure the packet list. The sixth step is to configure the packet details. The seventh step is to configure the packet bytes. The eighth step is to configure the packet capture. The ninth step is to configure the packet analysis. The tenth step is to configure the packet display. The eleventh step is to configure the packet capture. The twelfth step is to configure the packet analysis. The thirteenth step is to configure the packet display. The fourteenth step is to configure the packet capture. The fifteenth step is to configure the packet analysis. The sixteenth step is to configure the packet display. The seventeenth step is to configure the packet capture. The eighteenth step is to configure the packet analysis. The nineteenth step is to configure the packet display. The twentieth step is to configure the packet capture. The twenty-first step is to configure the packet analysis. The twenty-second step is to configure the packet display. The twenty-third step is to configure the packet capture. The twenty-fourth step is to configure the packet analysis. The twenty-fifth step is to configure the packet display. The twenty-sixth step is to configure the packet capture. The twenty-seventh step is to configure the packet analysis. The twenty-eighth step is to configure the packet display. The twenty-ninth step is to configure the packet capture. The thirtieth step is to configure the packet analysis. The thirty-first step is to configure the packet display. The thirty-second step is to configure the packet capture. The thirty-third step is to configure the packet analysis. The thirty-fourth step is to configure the packet display. The thirty-fifth step is to configure the packet capture. The thirty-sixth step is to configure the packet analysis. The thirty-seventh step is to configure the packet display. The thirty-eighth step is to configure the packet capture. The thirty-ninth step is to configure the packet analysis. The fortieth step is to configure the packet display. The forty-first step is to configure the packet capture. The forty-second step is to configure the packet analysis. The forty-third step is to configure the packet display. The forty-fourth step is to configure the packet capture. The forty-fifth step is to configure the packet analysis. The forty-sixth step is to configure the packet display. The forty-seventh step is to configure the packet capture. The forty-eighth step is to configure the packet analysis. The forty-ninth step is to configure the packet display. The fiftieth step is to configure the packet capture. The fifty-first step is to configure the packet analysis. The fifty-second step is to configure the packet display. The fifty-third step is to configure the packet capture. The fifty-fourth step is to configure the packet analysis. The fifty-fifth step is to configure the packet display. The fifty-sixth step is to configure the packet capture. The fifty-seventh step is to configure the packet analysis. The fifty-eighth step is to configure the packet display. The fifty-ninth step is to configure the packet capture. The sixtieth step is to configure the packet analysis. The sixty-first step is to configure the packet display. The sixty-second step is to configure the packet capture. The sixty-third step is to configure the packet analysis. The sixty-fourth step is to configure the packet display. The sixty-fifth step is to configure the packet capture. The sixty-sixth step is to configure the packet analysis. The sixty-seventh step is to configure the packet display. The sixty-eighth step is to configure the packet capture. The sixty-ninth step is to configure the packet analysis. The seventieth step is to configure the packet display. The seventy-first step is to configure the packet capture. The seventy-second step is to configure the packet analysis. The seventy-third step is to configure the packet display. The seventy-fourth step is to configure the packet capture. The seventy-fifth step is to configure the packet analysis. The seventy-sixth step is to configure the packet display. The seventy-seventh step is to configure the packet capture. The seventy-eighth step is to configure the packet analysis. The seventy-ninth step is to configure the packet display. The eightieth step is to configure the packet capture. The eighty-first step is to configure the packet analysis. The eighty-second step is to configure the packet display. The eighty-third step is to configure the packet capture. The eighty-fourth step is to configure the packet analysis. The eighty-fifth step is to configure the packet display. The eighty-sixth step is to configure the packet capture. The eighty-seventh step is to configure the packet analysis. The eighty-eighth step is to configure the packet display. The eighty-ninth step is to configure the packet capture. The ninetieth step is to configure the packet analysis. The ninety-first step is to configure the packet display. The ninety-second step is to configure the packet capture. The ninety-third step is to configure the packet analysis. The ninety-fourth step is to configure the packet display. The ninety-fifth step is to configure the packet capture. The ninety-sixth step is to configure the packet analysis. The ninety-seventh step is to configure the packet display. The ninety-eighth step is to configure the packet capture. The ninety-ninth step is to configure the packet analysis. The hundredth step is to configure the packet display.



Wireshark은 네트워크 트래픽을 캡처하고 분석하는 데 사용되는 오픈 소스 소프트웨어입니다. 이 도구를 사용하여 네트워크 문제 해결, 보안 감사 및 성능 모니터링을 수행할 수 있습니다.

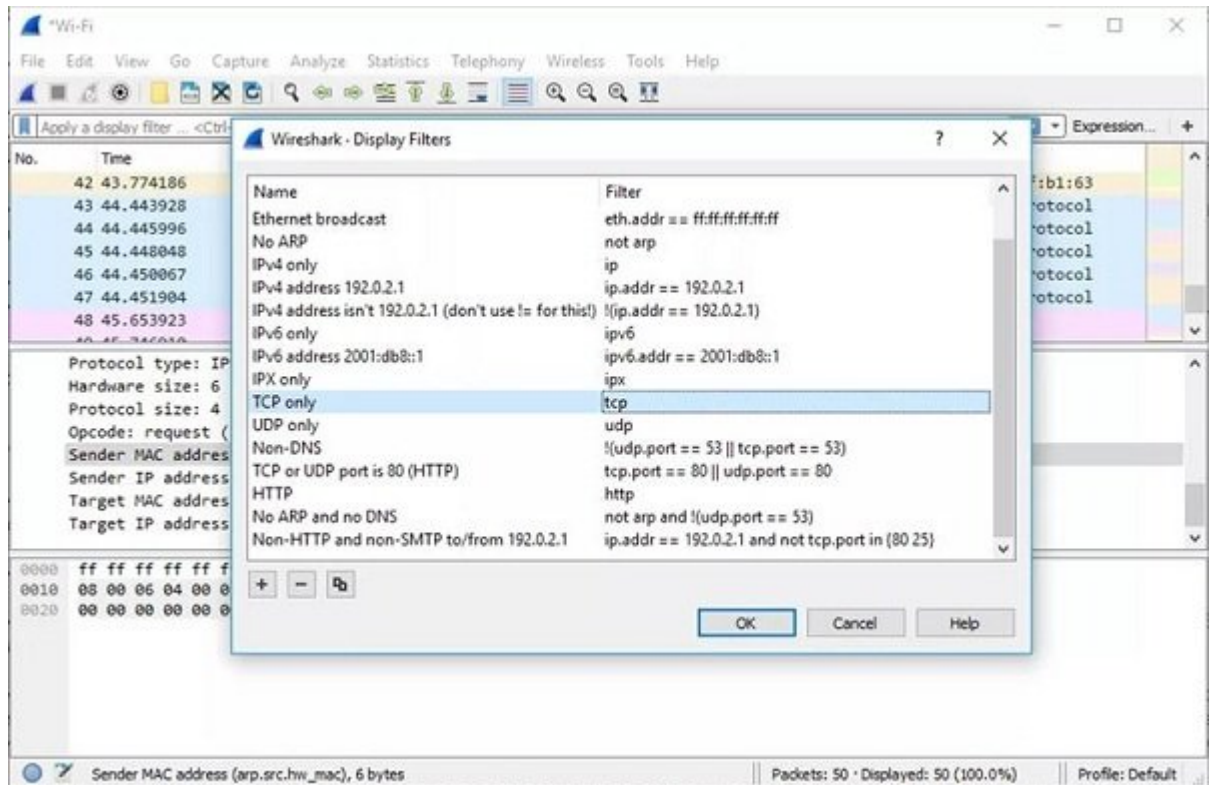
Wireshark를 사용하여 네트워크 트래픽을 캡처하고 분석하는 방법을 알아보겠습니다.

Wireshark를 설치하고 실행한 후, 'Capture' 메뉴를 클릭하여 인터페이스를 선택합니다. 이 예에서는 'vEthernet (Default Switch)'가 선택되어 있습니다. 'Capture' 버튼을 클릭하여 트래픽 캡처를 시작합니다. 트래픽이 캡처되면, 'Analyze' 메뉴를 클릭하여 트래픽을 분석합니다. 트래픽이 분석되면, 'Statistics' 메뉴를 클릭하여 트래픽 통계 정보를 확인합니다. 트래픽 통계 정보는 트래픽의 종류, 크기, 방향 등을 보여줍니다. 트래픽을 분석하고 통계 정보를 확인한 후, 'File' 메뉴를 클릭하여 트래픽을 저장합니다. 트래픽은 Wireshark의 기본 형식인 PCAP 형식으로 저장됩니다. 트래픽을 저장한 후, 다른 도구와 함께 사용할 수 있습니다.





이 단계를 완료하면 Wireshark의 필터링 기능이 활성화됩니다. 이 기능을 사용하여 네트워크 트래픽을 필터링하고, 특정 프로토콜이나 주소에 대한 트래픽을 표시할 수 있습니다. Wireshark의 필터링 기능을 사용하여, 특정 프로토콜이나 주소에 대한 트래픽을 표시할 수 있습니다. Wireshark의 필터링 기능을 사용하여, 특정 프로토콜이나 주소에 대한 트래픽을 표시할 수 있습니다.



이 단계를 완료하면 Wireshark의 필터링 기능이 활성화됩니다.

이 단계를 완료하면 Wireshark의 필터링 기능이 활성화됩니다. 이 기능을 사용하여 네트워크 트래픽을 필터링하고, 특정 프로토콜이나 주소에 대한 트래픽을 표시할 수 있습니다. Wireshark의 필터링 기능을 사용하여, 특정 프로토콜이나 주소에 대한 트래픽을 표시할 수 있습니다. Wireshark의 필터링 기능을 사용하여, 특정 프로토콜이나 주소에 대한 트래픽을 표시할 수 있습니다.





## معماری شبکه های رایانه ای

این کتاب، معماری شبکه های رایانه ای را به گونه ای ساده و قابل فهم برای دانشجویان و متخصصان حوزه شبکه های رایانه ای و مهندسی کامپیوتر، طراحی کرده است. در این کتاب، به بررسی مفاهیم پایه شبکه های رایانه ای، از جمله انواع شبکه ها، پروتکل ها، و روش های انتقال داده ها، پرداخته شده است. همچنین، به بررسی معماری شبکه های رایانه ای، از جمله انواع معماری ها، از جمله معماری های متمرکز، غیرمتمرکز، و ترکیبی، پرداخته شده است. این کتاب، به گونه ای طراحی شده است که بتواند به عنوان یک منبع آموزشی و مرجع برای دانشجویان و متخصصان حوزه شبکه های رایانه ای و مهندسی کامپیوتر، مورد استفاده قرار گیرد.

:معماری شبکه

معماری شبکه های رایانه ای

:معماری شبکه

معماری شبکه های رایانه ای

:معماری شبکه

11:55 - 08/05/1398

:معماری شبکه

معماری - معماری شبکه های رایانه ای - معماری شبکه های رایانه ای - Wireshark - معماری شبکه های رایانه ای

معماری

<https://www.shabakeh-mag.com/cover-story/15701/%D8%B1%D8%A7%D9%87%D9%86%D9%85%D8%A7%DB%8C-%D8%AC%D8%A7%D9%85%D8%B9-%D8%A8%D9%87%E2%80%8C%D8%A9%D8%A7%D8%B1%DA%AF%DB%8C%D8%B1%DB%8C-wireshark-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%86%D8%B8%D8%A7%D8%B1%D8%AA-%D8%A8%D8%B1-%D8%AA%D8%B1%D8%A7%D9%81%DB%8C%DA%A9-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7>