WHAT IS WIRESHARK ?

Wireshark is an open source network packet analyzer used to analyze a network or network protocol. It helps to analyze all TCP/IP data connected to the computer.

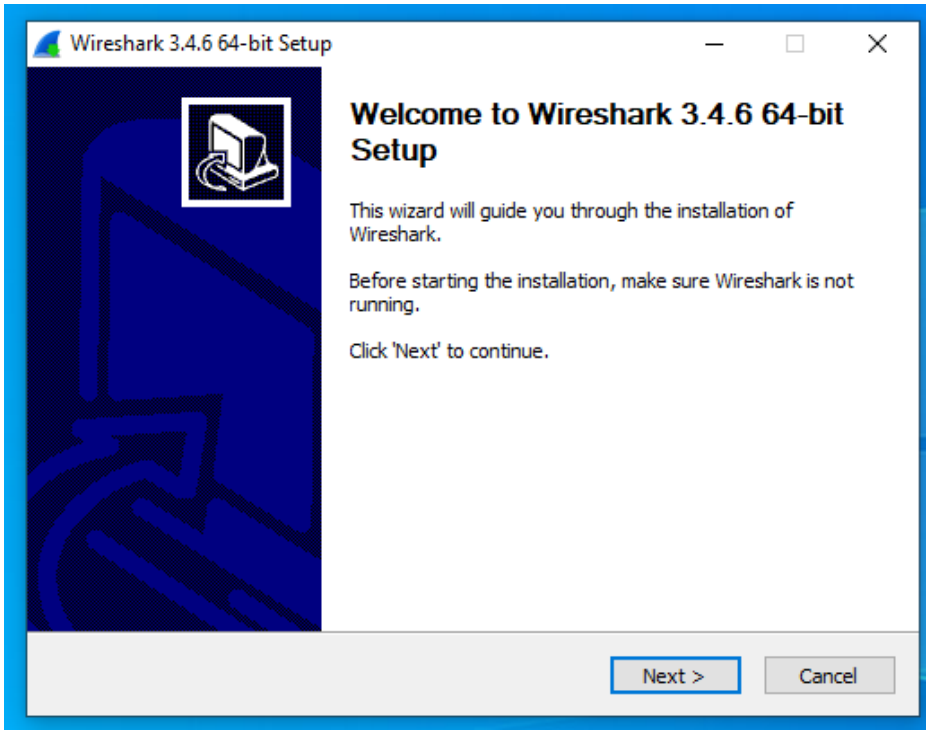
Wireshark can be used on Unix/Linux and Windows operating systems.

Features of Wireshark

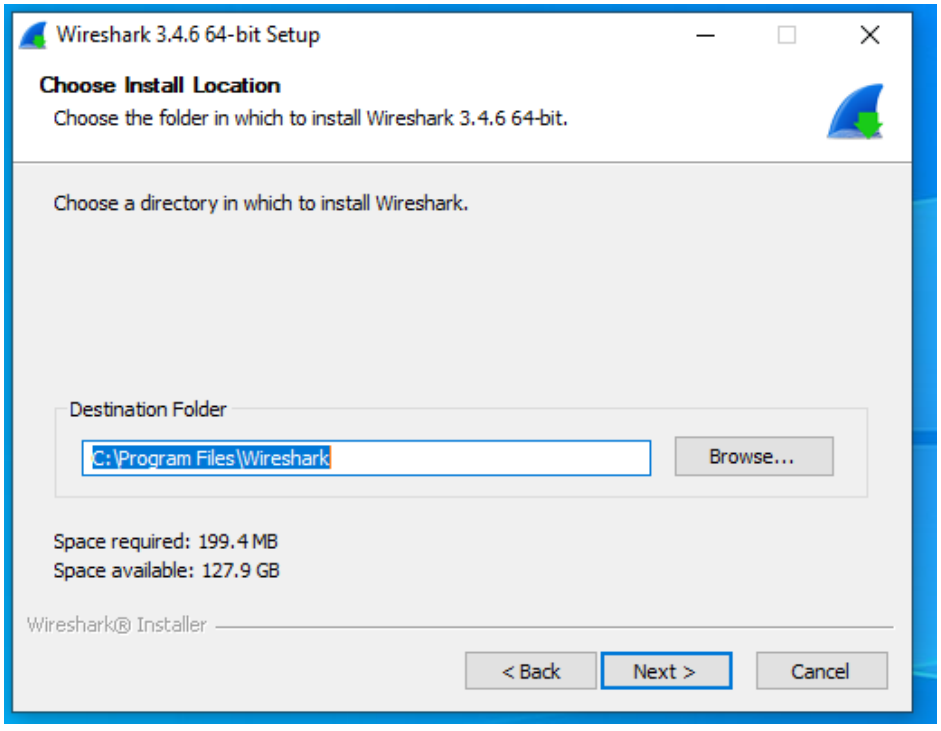
- Wireshark can be used on Unix/Linux and Windows operating systems.
- Keeps packets on the local network and displays them in detail to the user.
- There is decryption support for protocols. These protocols :
  - IPsec , Internet Protocol Security
  - SSL, Secure Sockets Layer
  - TLS, Transport Layer Security
  - WEP, Wired Equivalent Privacy

How To Setup Wireshark ?

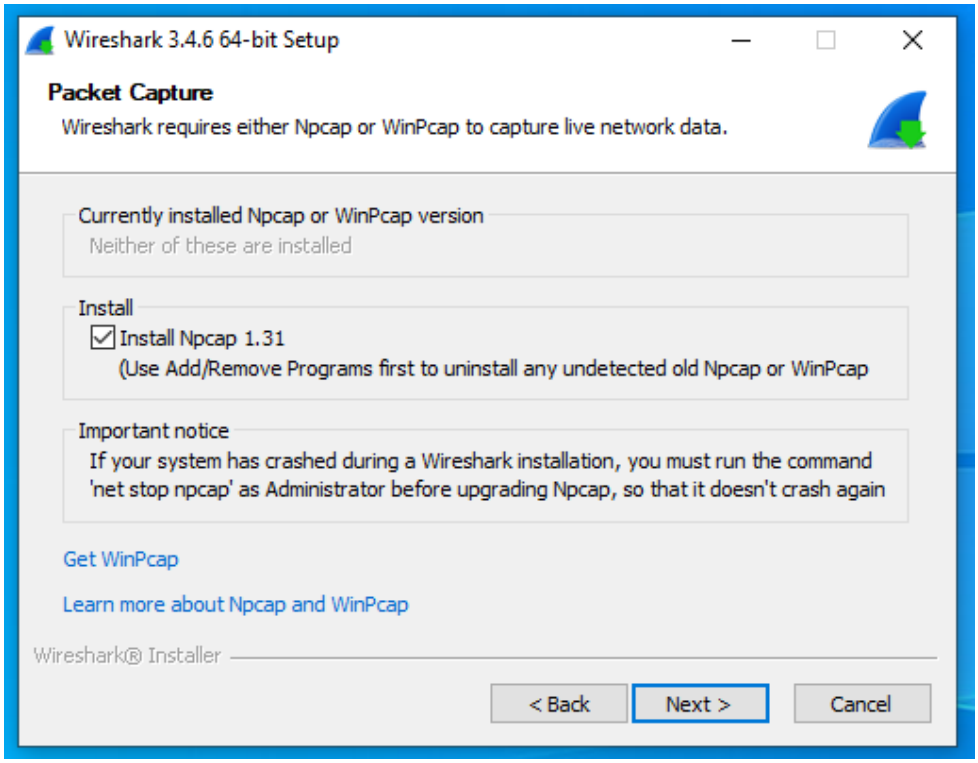
1. According to the operating system used, the download is made from wireshark's own site.
2. The downloaded setup file is run as administrator.
3. Continue by clicking the Next button in the installation wizard.



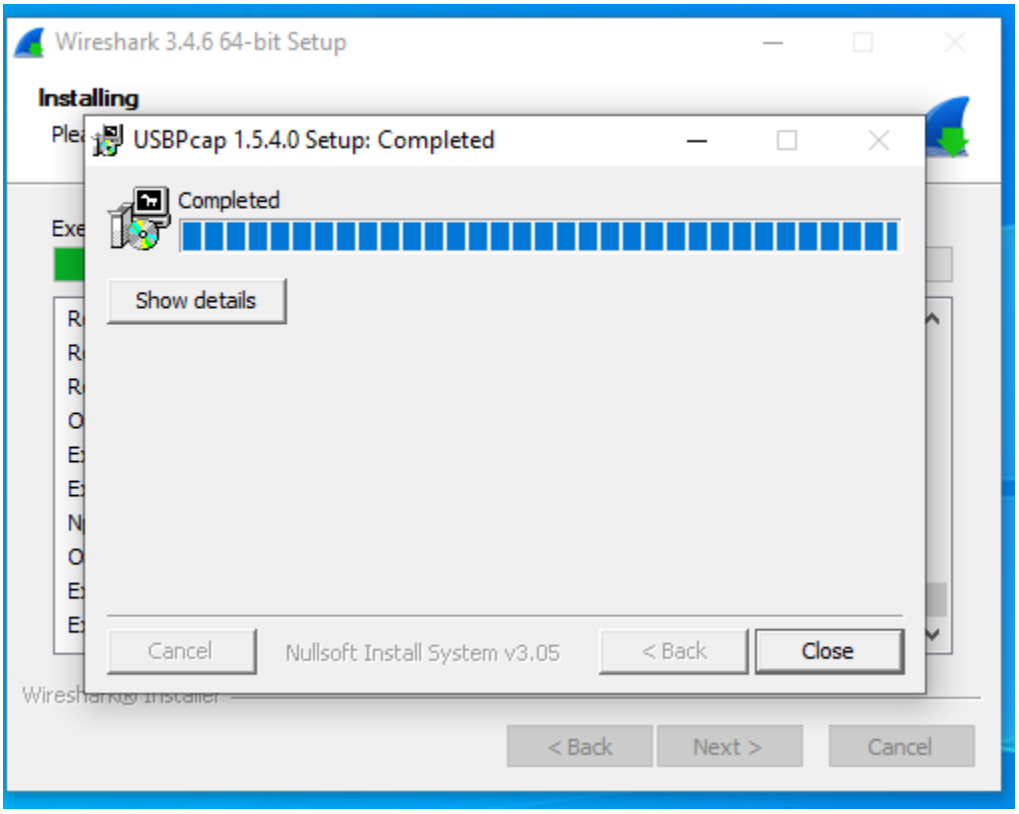
4. The installation location is left as default and continued.



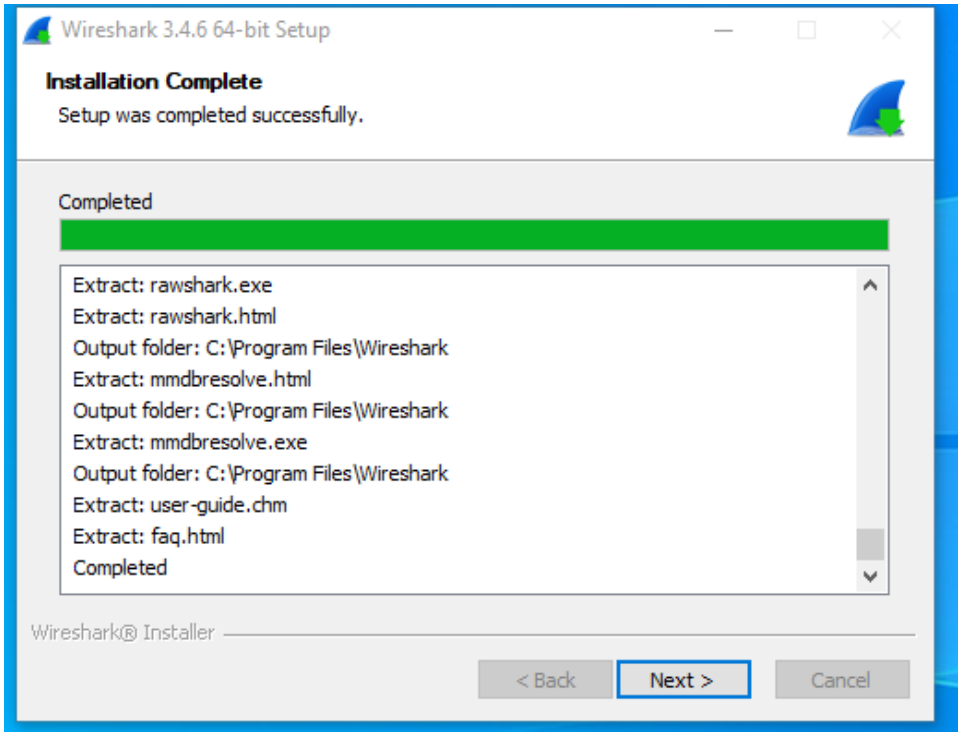
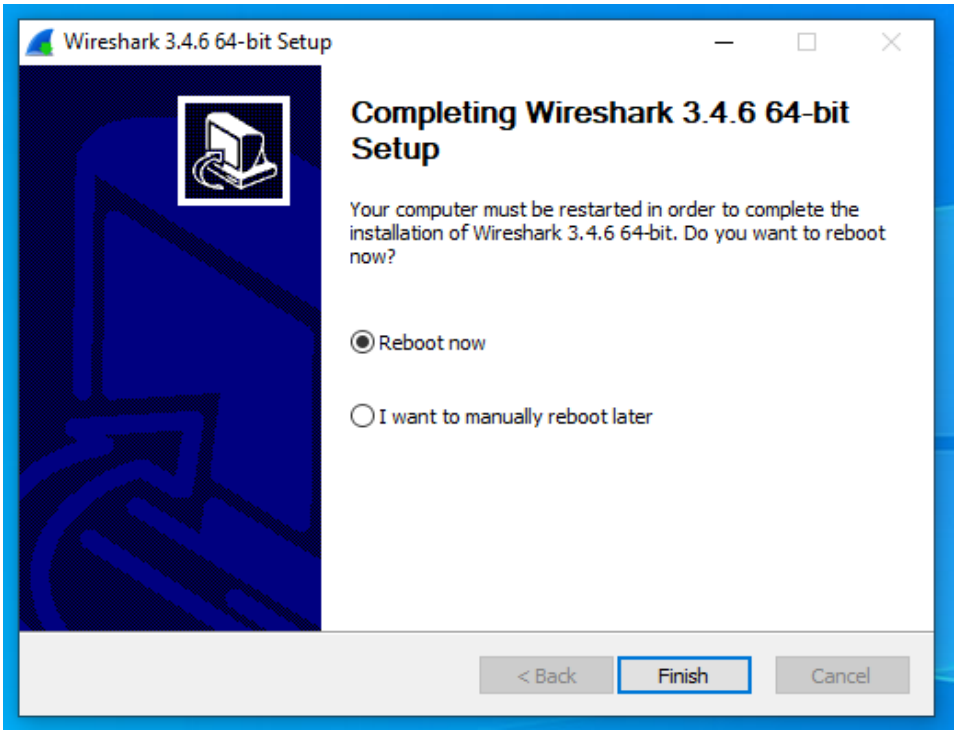
5. The most important utility of this software is the WinPcap program. Select Install WinPcap and press the next button.



6. The necessary files are extracted and the installation begins.
7. The USBPcap program is required to capture USB devices.



8. After the installation is complete, the wizard continues for the installation.
9. The network analysis program is installed.



10. The computer then restarts for the changes to be saved.