internsElite

NAME:-IBRAHIM KHAN

ROLL NO :-24/CS/J82

SUBMITTED TO:-

AMAN(MENTOR)

PROJECT:- MAJOR

Content pg.no

Nmap

Command prompt for network

Httrack

wireshark

Q 1:- use nmap tool for finding info,inside the network?

ANS:-

NMAP (Network Mapper)

- Network scanning software.
- Developed by Gordon Lyon.
- Written in C, C++, Python, Lua.
- Initial release: 1997.
- Latest version: 7.94
- Free and open-source.
- Compatible with Windows, Mac, Linux, etc.

- Security tool for network protection.

- Features:

  - Host discovery.

  - Port scanning.

  - Application name and version detection.

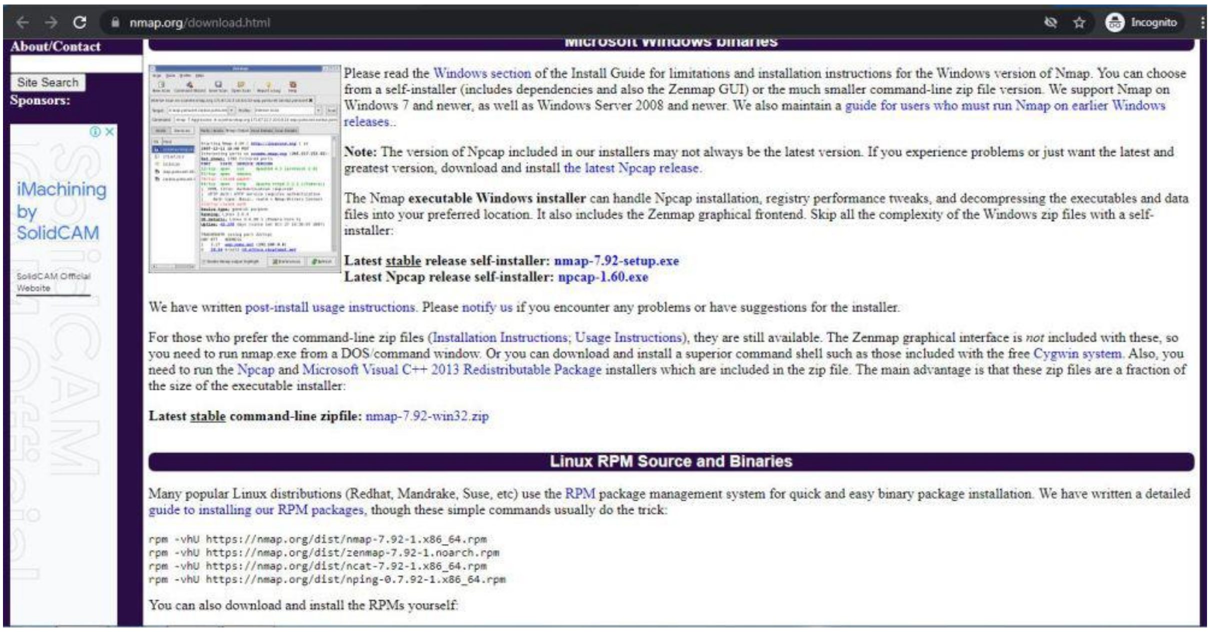
  - OS and hardware detection.

  - Scriptable interaction via NSE (Nmap Scripting Engine) and Lua.

Installing Nmap on Windows

Follow the below steps to install Nmap on Windows:

Step1: Visit the official website using the URL https://nmap.org/download#windows on any web browser the click on **nmap-7.94-setup.exe**. Downloading of this executable file will start soon. It is a 31.8 MB file so it will take some minutes.



Microsoft Windows binaries

Please read the Windows section of the Install Guide for limitations and installation instructions for the Windows version of Nmap. You can choose from a self-installer (includes dependencies and also the Zenmap GUI) or the much smaller command-line zip file version. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 and newer. We also maintain a guide for users who must run Nmap on earlier Windows releases..

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install the latest Npcap release.

The Nmap **executable Windows installer** can handle Npcap installation, registry performance tweaks, and decompressing the executables and data files into your preferred location. It also includes the Zenmap graphical frontend. Skip all the complexity of the Windows zip files with a self-installer:

Latest stable release self-installer: nmap-7.92-setup.exe
Latest Npcap release self-installer: npcap-1.60.exe

We have written post-install usage instructions. Please notify us if you encounter any problems or have suggestions for the installer.

For those who prefer the command-line zip files (Installation Instructions; Usage Instructions), they are still available. The Zenmap graphical interface is *not* included with these, so you need to run nmap.exe from a DOS/command window. Or you can download and install a superior command shell such as those included with the free Cygwin system. Also, you need to run the Npcap and Microsoft Visual C++ 2013 Redistributable Package installers which are included in the zip file. The main advantage is that these zip files are a fraction of the size of the executable installer:

Latest stable command-line zipfile: nmap-7.92-win32.zip

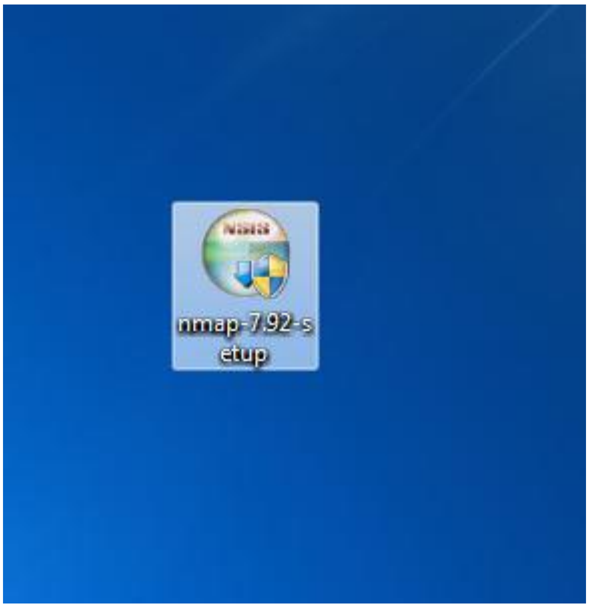
Linux RPM Source and Binaries

Many popular Linux distributions (Redhat, Mandrake, Suse, etc) use the RPM package management system for quick and easy binary package installation. We have written a detailed guide to installing our RPM packages, though these simple commands usually do the trick:

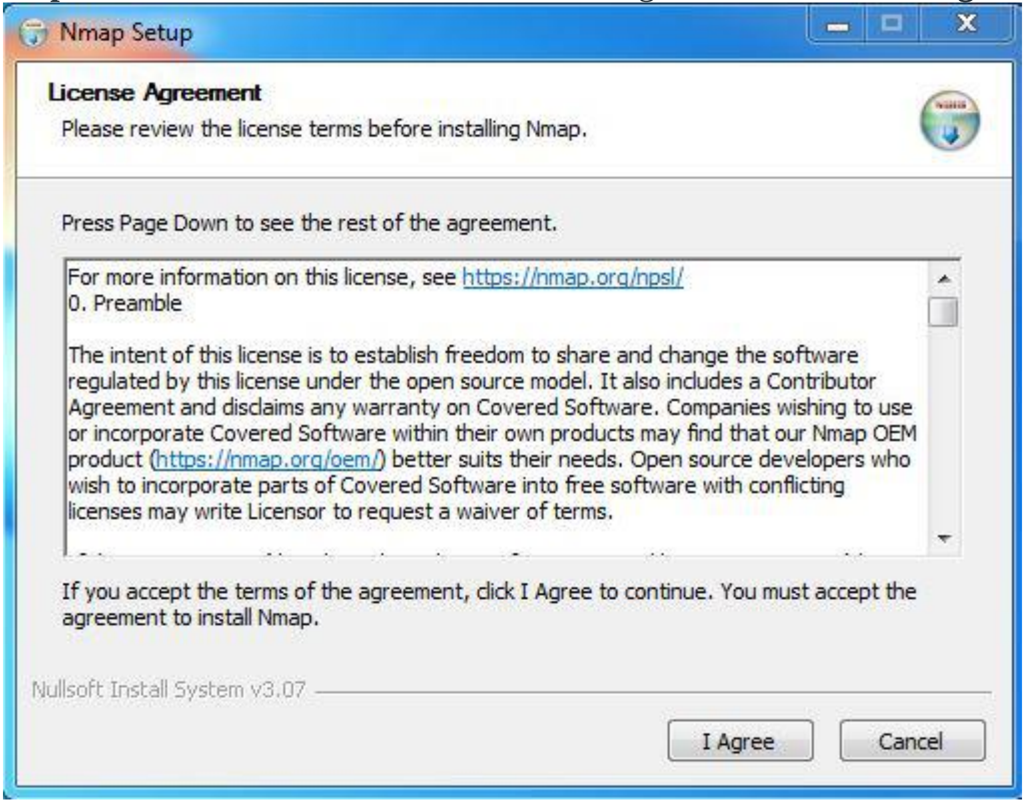
```
rpm -vhU https://nmap.org/dist/nmap-7.92-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/zenmap-7.92-1.noarch.rpm
rpm -vhU https://nmap.org/dist/ncat-7.92-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/nping-0.7.92-1.x86_64.rpm
```

You can also download and install the RPMs yourself:

Step 2: Now check for the executable file in downloads in your system and run it.



Step 3: It will prompt confirmation to make changes to your system. Click on **Yes**.
Step 4: The next screen will be of License Agreement, click on **I Agree**.



Nmap Setup

License Agreement

Please review the license terms before installing Nmap.

Press Page Down to see the rest of the agreement.

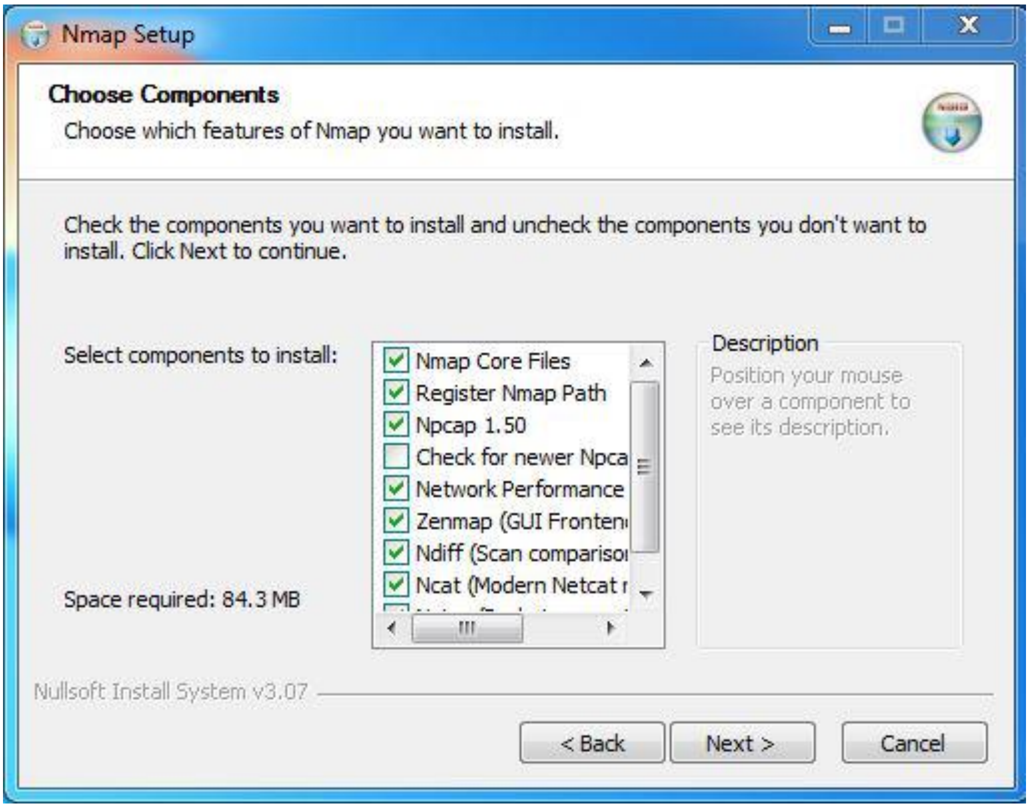
For more information on this license, see https://nmap.org/npsl/
0. Preamble

The intent of this license is to establish freedom to share and change the software regulated by this license under the open source model. It also includes a Contributor Agreement and disclaims any warranty on Covered Software. Companies wishing to use or incorporate Covered Software within their own products may find that our Nmap OEM product (https://nmap.org/oem/) better suits their needs. Open source developers who wish to incorporate parts of Covered Software into free software with conflicting licenses may write Licensor to request a waiver of terms.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.

Nullsoft Install System v3.07

Step 5: Next screen is of choosing components, all components are already marked so don’t change anything just click on the **Next** button.



Nmap Setup

Choose Components

Choose which features of Nmap you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

☑ Nmap Core Files
☑ Register Nmap Path
☑ Npcap 1.50
□ Check for newer Npca
☑ Network Performance
☑ Zenmap (GUI Fronten
☑ Ndiff (Scan compariso
☑ Ncat (Modern Netcat r

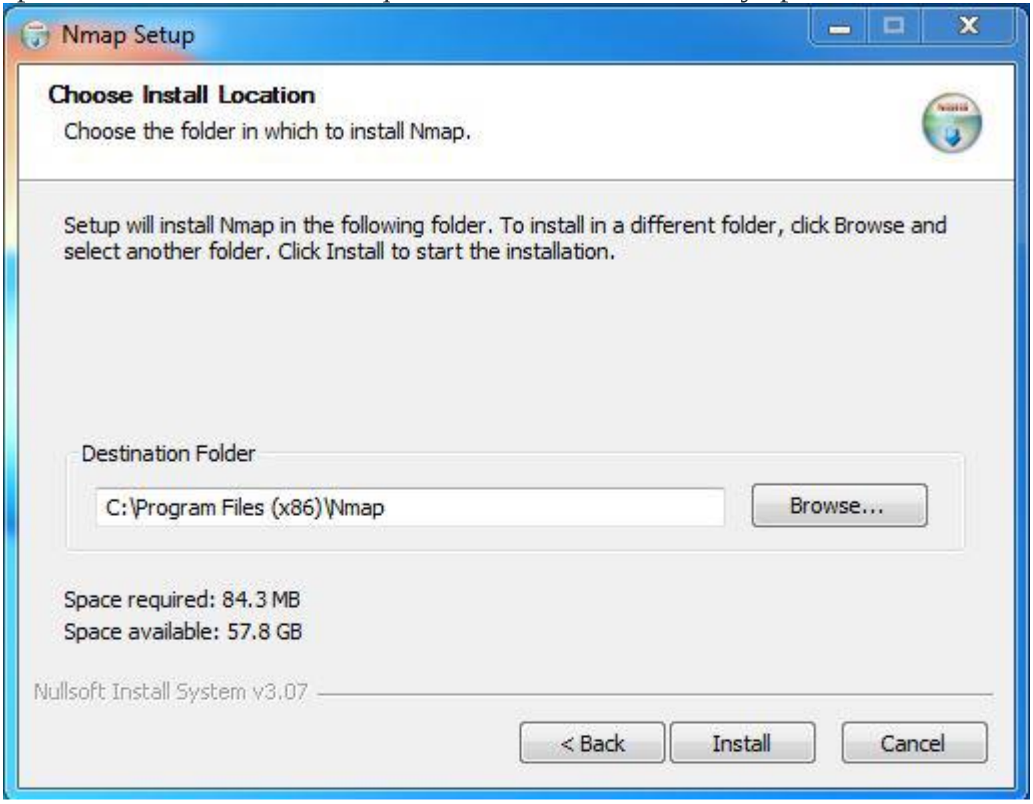
Description

Position your mouse over a component to see its description.

Space required: 84.3 MB

Nullsoft Install System v3.07

Step 6: In this step, we choose the installation location of Nmap. By default, it uses the C drive but you can change it into another drive that will have sufficient memory space for installation. It requires 84.3 MB of memory space.



Nmap Setup

Choose Install Location

Choose the folder in which to install Nmap.

Setup will install Nmap in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

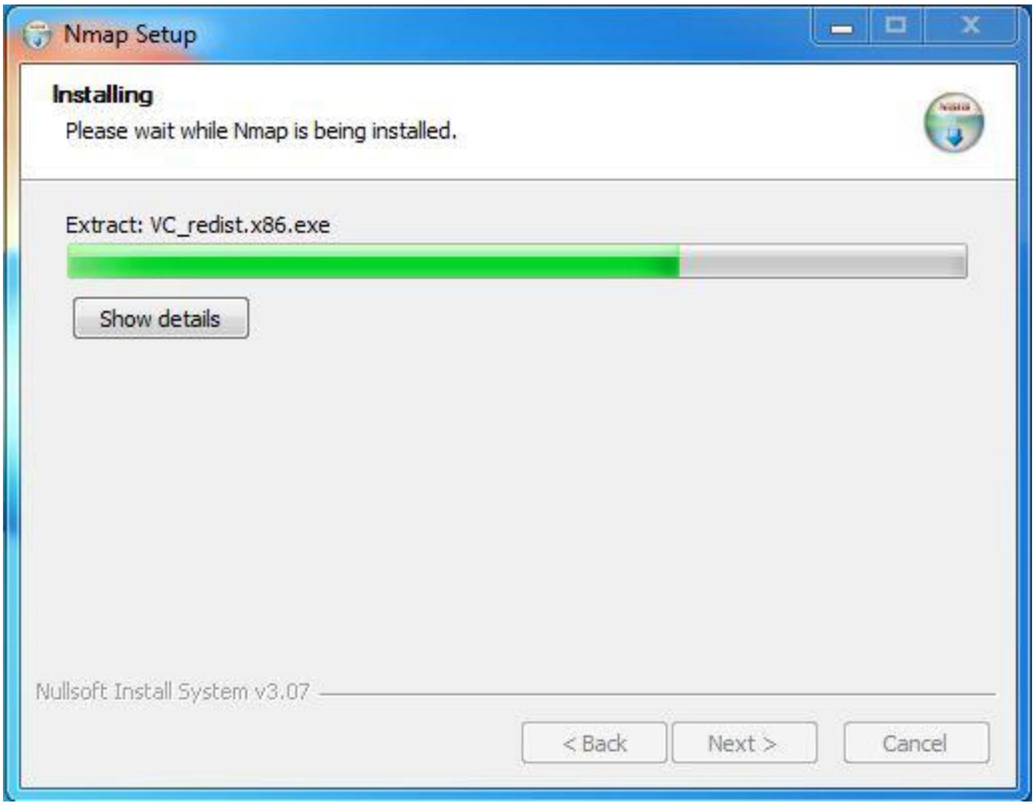
Destination Folder

C:\Program Files (x86)\Nmap

Space required: 84.3 MB
Space available: 57.8 GB

Nullsoft Install System v3.07

Step 7: After this installation process it will take a few minutes to complete the installation.



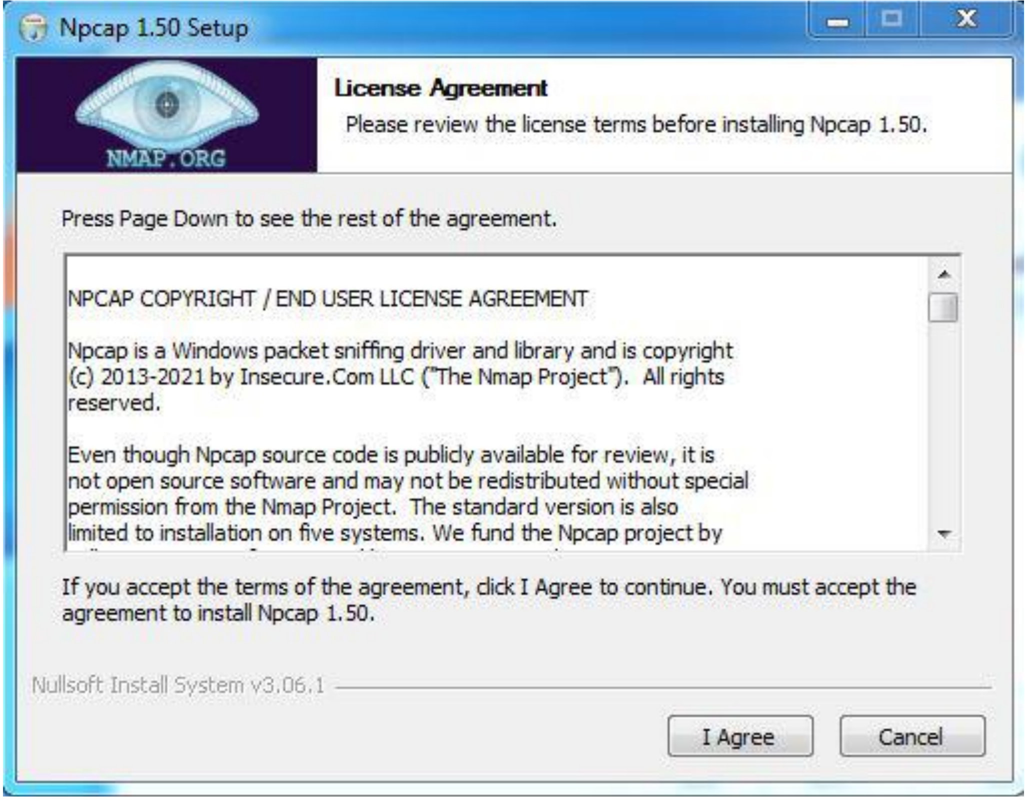
Nmap Setup

Installing

Please wait while Nmap is being installed.

Extract: VC_redist.x86.exe

Step 8: Npcap installation will also occur with it, the screen of License Agreement will appear, click on **I Agree**.



Npcap 1.50 Setup

License Agreement

Please review the license terms before installing Npcap 1.50.

Press Page Down to see the rest of the agreement.

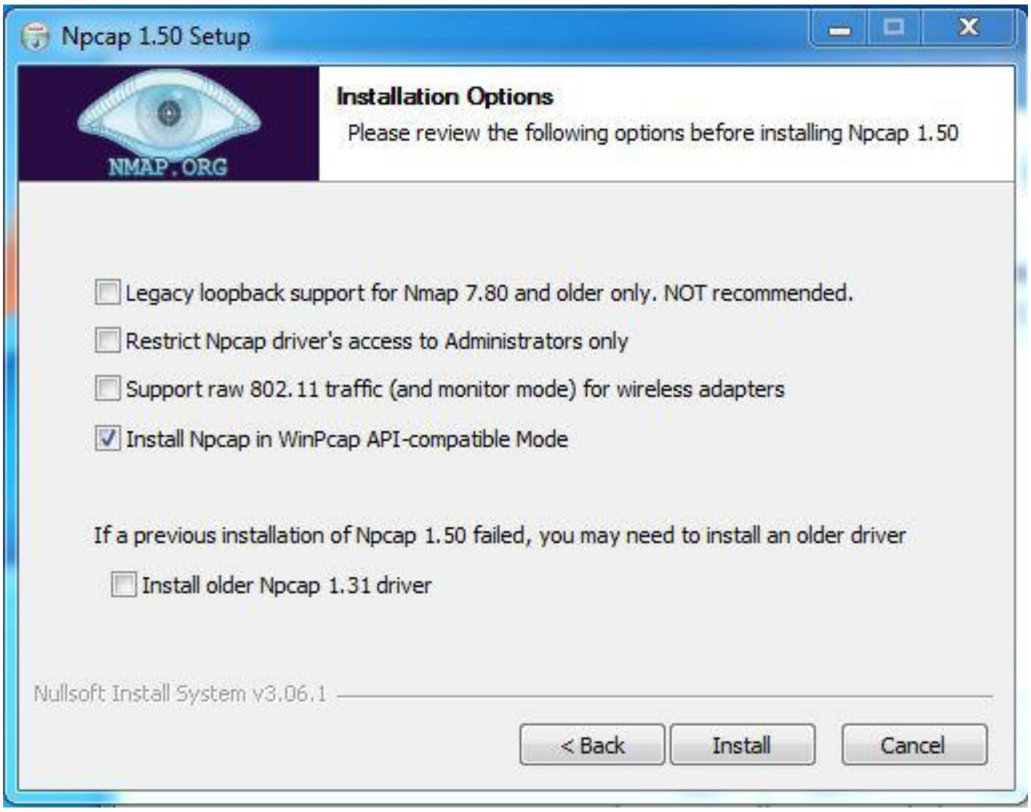
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT

Npcap is a Windows packet sniffing driver and library and is copyright (c) 2013-2021 by Insecure.Com LLC ("The Nmap Project"). All rights reserved.

Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed without special permission from the Nmap Project. The standard version is also limited to installation on five systems. We fund the Npcap project by

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 1.50.

Step 9: Next screen is of installation options don't change anything and click on the **Install** button.


Npcap 1.50 Setup

Installation Options

Please review the following options before installing Npcap 1.50

□ Legacy loopback support for Nmap 7.80 and older only. NOT recommended.

□ Restrict Npcap driver's access to Administrators only

□ Support raw 802.11 traffic (and monitor mode) for wireless adapters

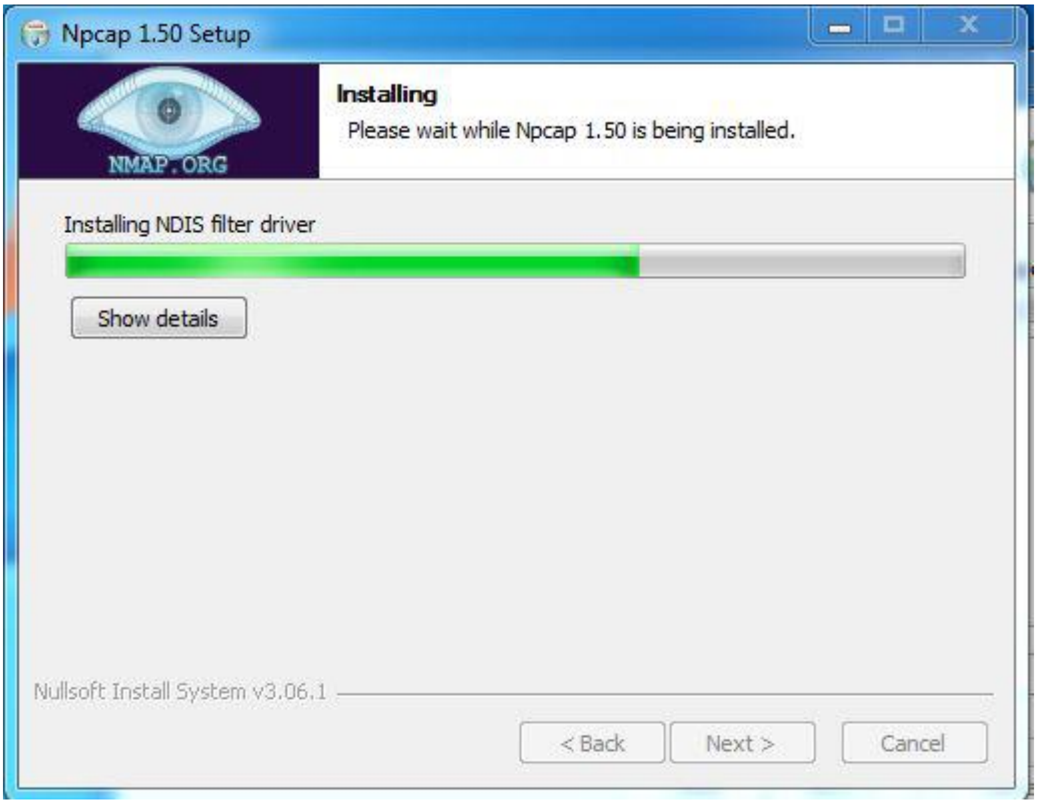
☑ Install Npcap in WinPcap API-compatible Mode

If a previous installation of Npcap 1.50 failed, you may need to install an older driver

□ Install older Npcap 1.31 driver

Nullsoft Install System v3.06.1

Step 10: After this installation process it will take a few minutes to complete the installation.


Npcap 1.50 Setup

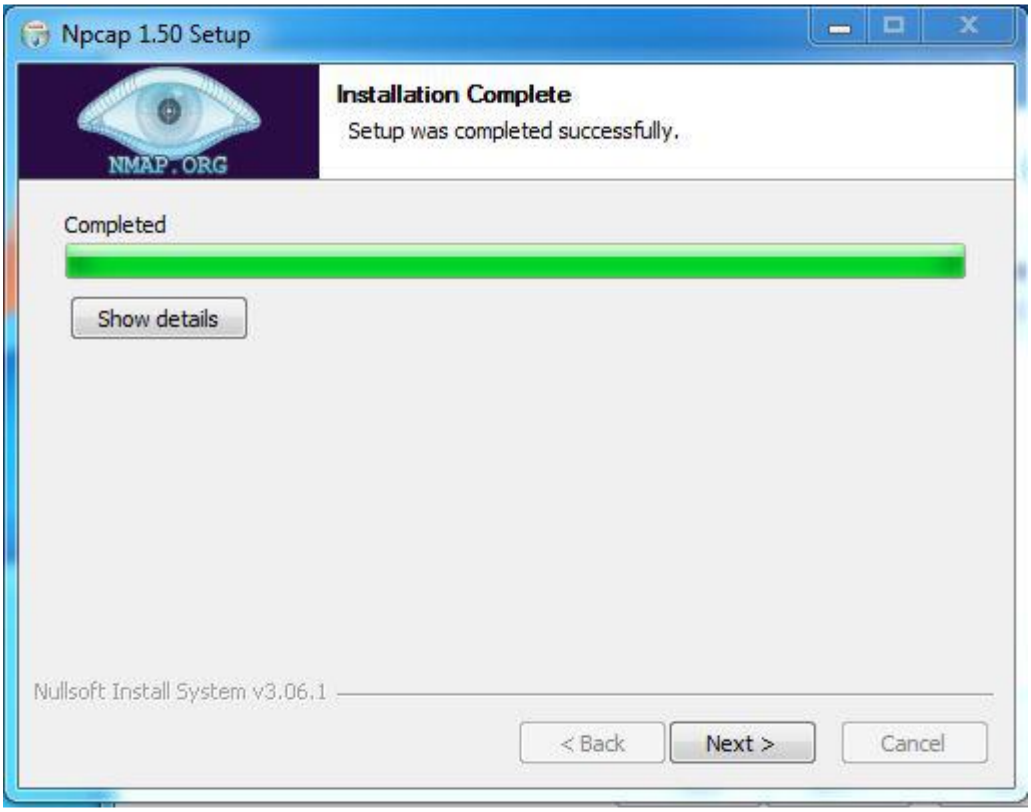
Installing

Please wait while Npcap 1.50 is being installed.

Installing NDIS filter driver

Nullsoft Install System v3.06.1

Step 11: After completion of installation click on the **Next** button.



Npcap 1.50 Setup

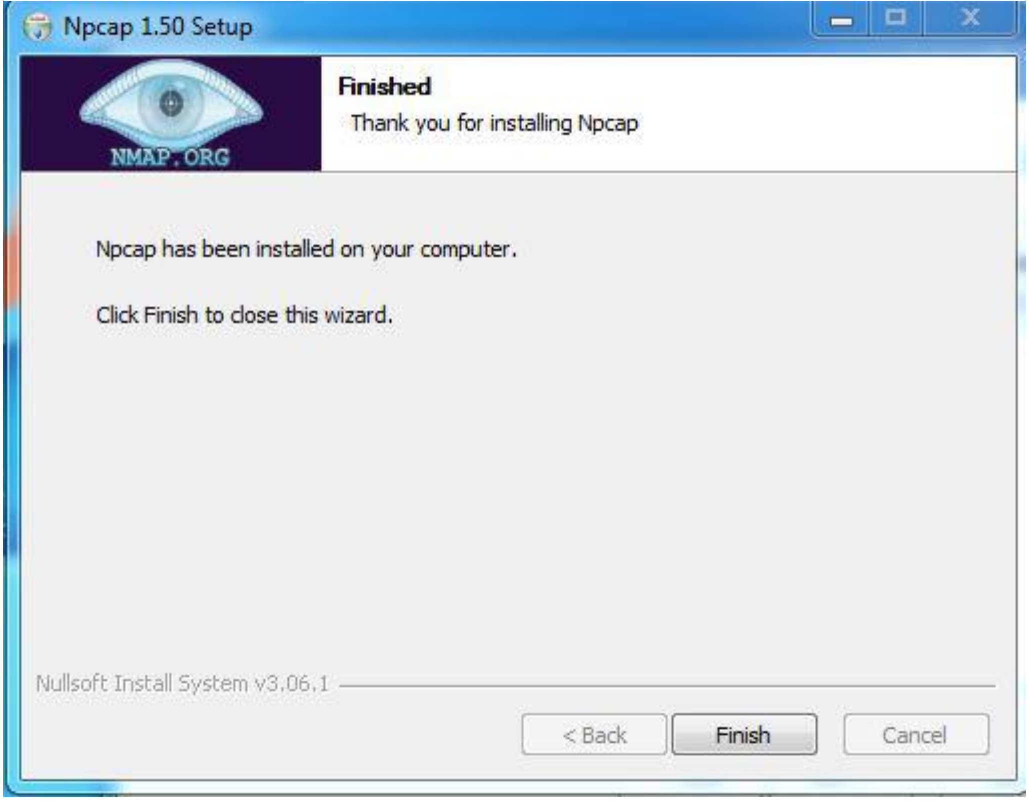
Installation Complete

Setup was completed successfully.

Completed

Nullsoft Install System v3.06.1

Step 12: Click on the **Finish** button to finish the installation of Npcap.



Npcap 1.50 Setup

Finished

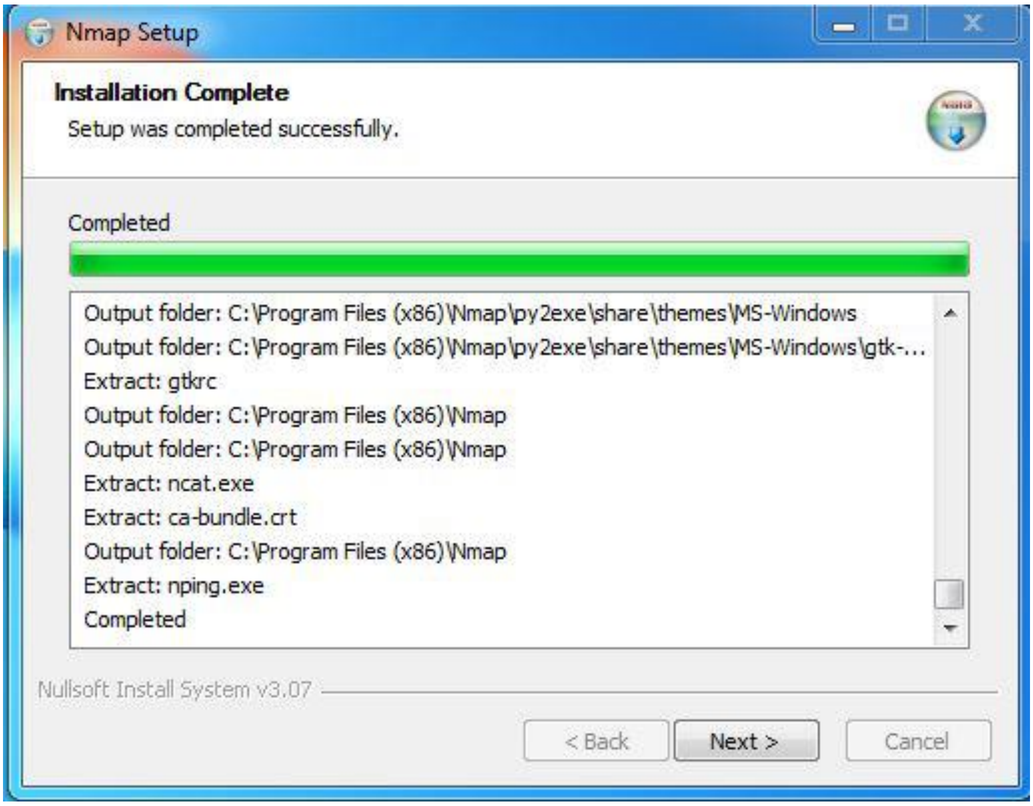
Thank you for installing Npcap

Npcap has been installed on your computer.

Click Finish to close this wizard.

Nullsoft Install System v3.06.1

Step 13: After completion of the installation of Nmap click on **Next** button.


Nmap Setup

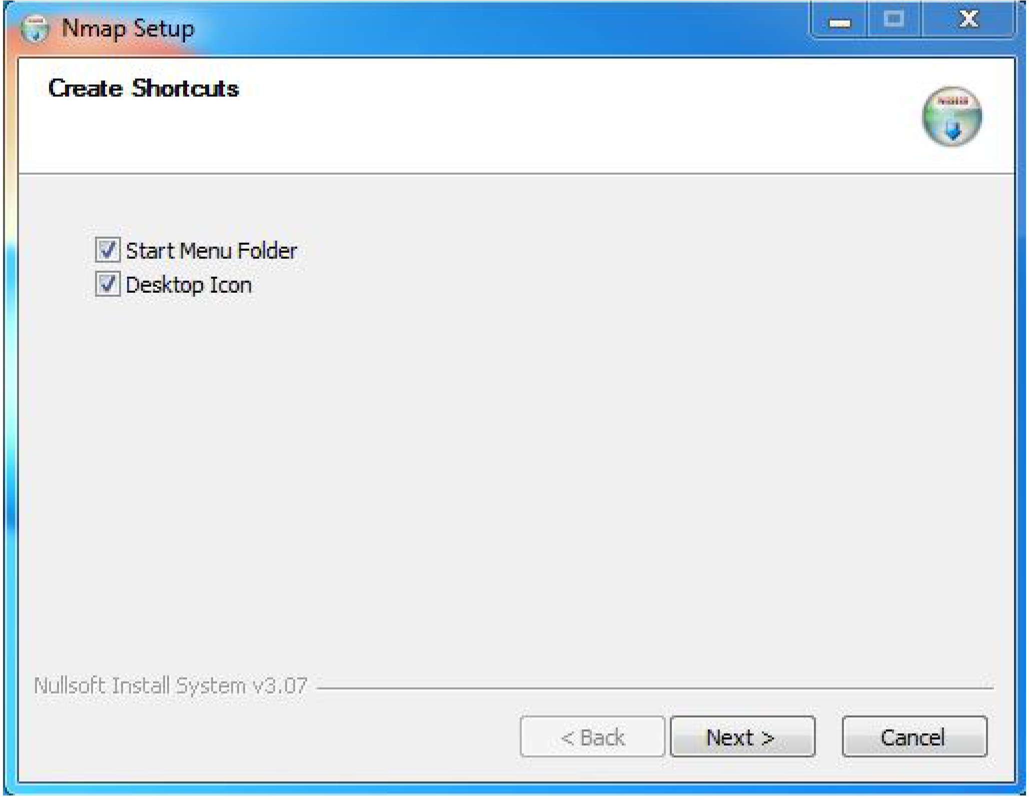
Installation Complete

Setup was completed successfully.

Completed

```
Output folder: C:\Program Files (x86)\Nmap\py2exe\share\themes\MS-Windows
Output folder: C:\Program Files (x86)\Nmap\py2exe\share\themes\MS-Windows\gtk-...
Extract: gtkrc
Output folder: C:\Program Files (x86)\Nmap
Output folder: C:\Program Files (x86)\Nmap
Extract: ncat.exe
Extract: ca-bundle.crt
Output folder: C:\Program Files (x86)\Nmap
Extract: nping.exe
Completed
```

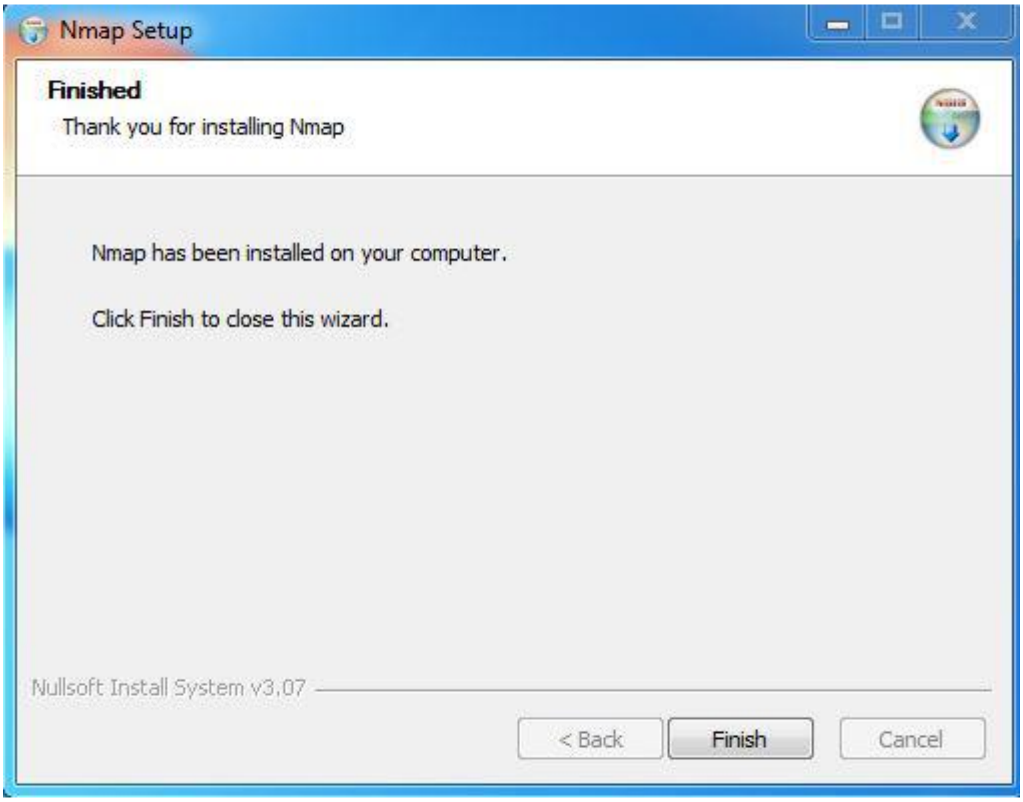
Step 14: Screen for creating shortcut will appear, click on **Next** button.


Nmap Setup

Create Shortcuts

☑ Start Menu Folder
☑ Desktop Icon

Step 15: Click on the **Finish** button to finish the installation of Nmap.



Nmap Setup

Finished

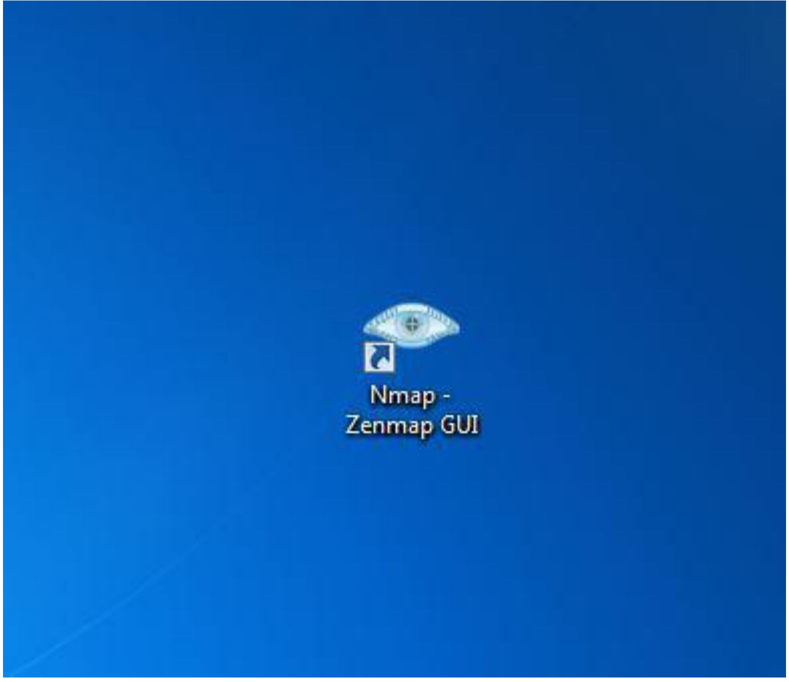
Thank you for installing Nmap

Nmap has been installed on your computer.

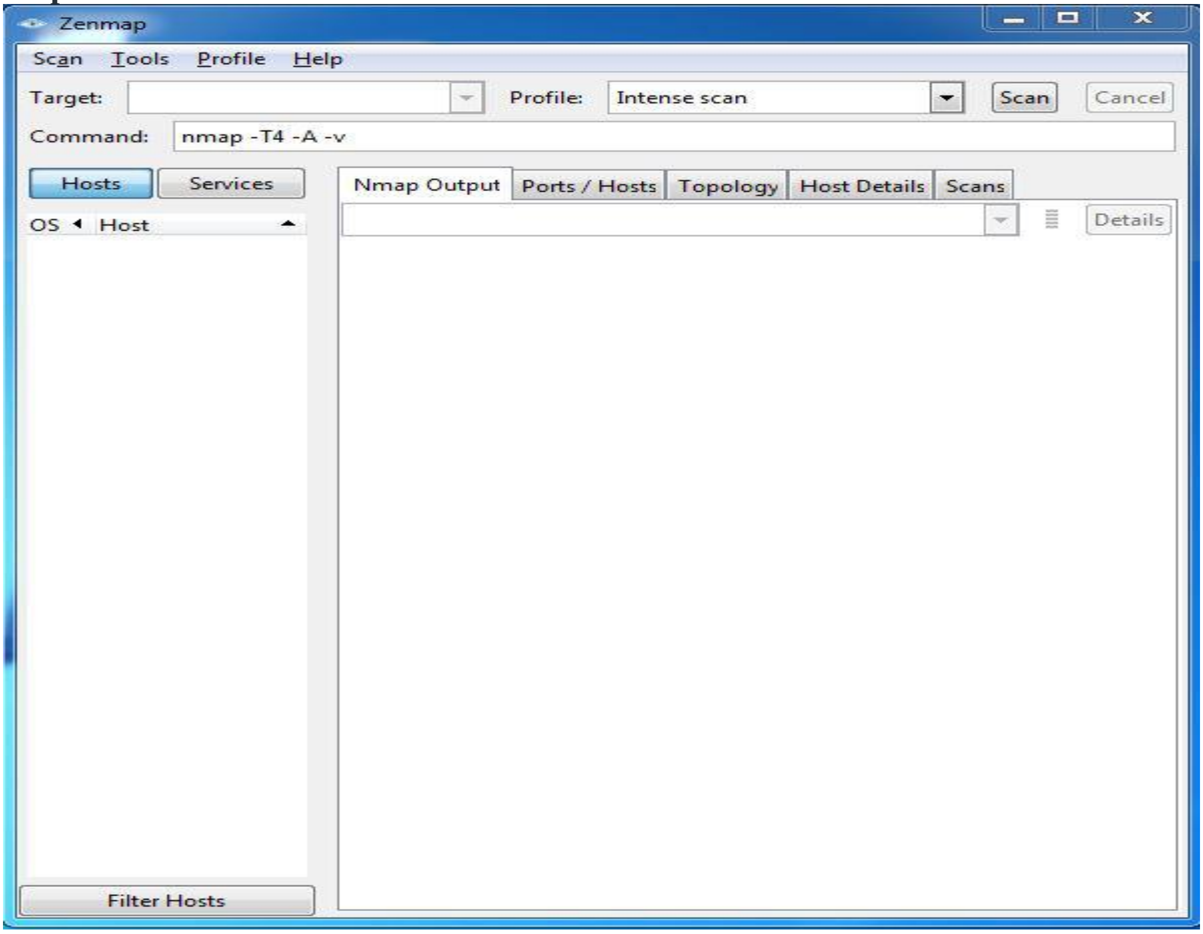
Click Finish to close this wizard.

Nullsoft Install System v3.07

Step 16: Nmap is successfully installed on the system and an icon is created on the desktop.



Step 17:- Run the software and see the interface



Target:

Profile: Intense scan

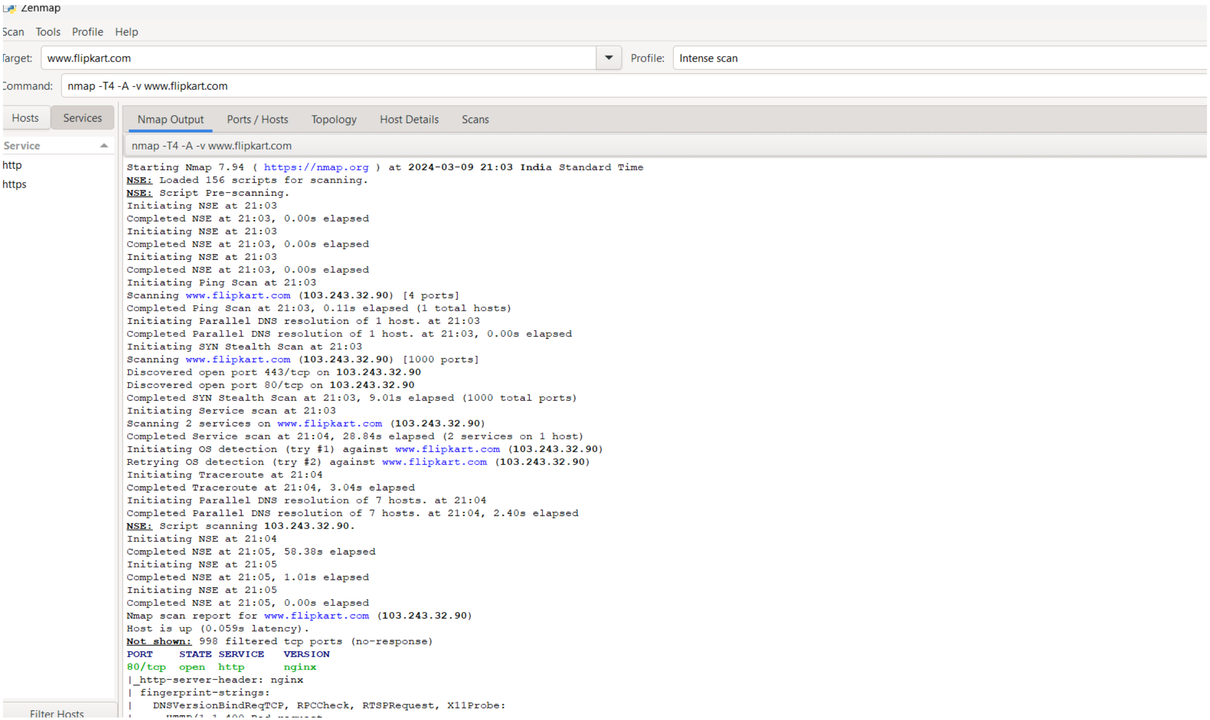
Command: nmap -T4 -A -v

So this is how you have successfully installed Nmap on your windows system.

DISCLAIMER

This material is intended for educational purposes only. Any unlawful use is strictly prohibited. Users are solely responsible for their actions.

(Zoom it u will see clearly)

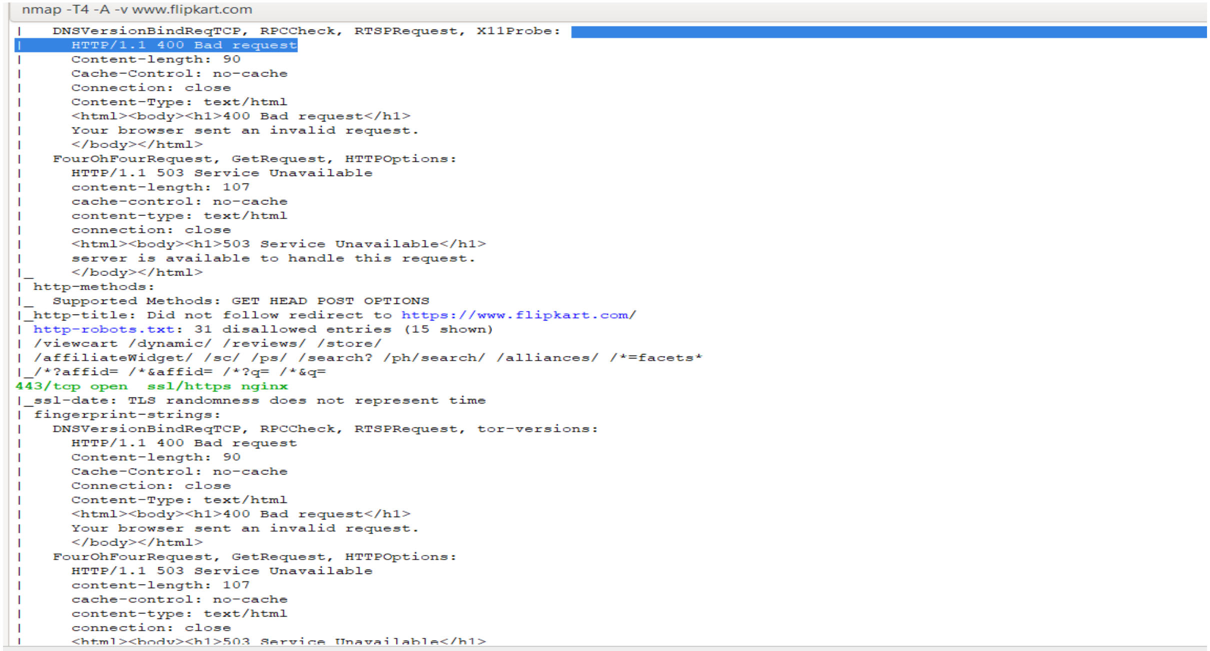


Target: www.flipkart.com

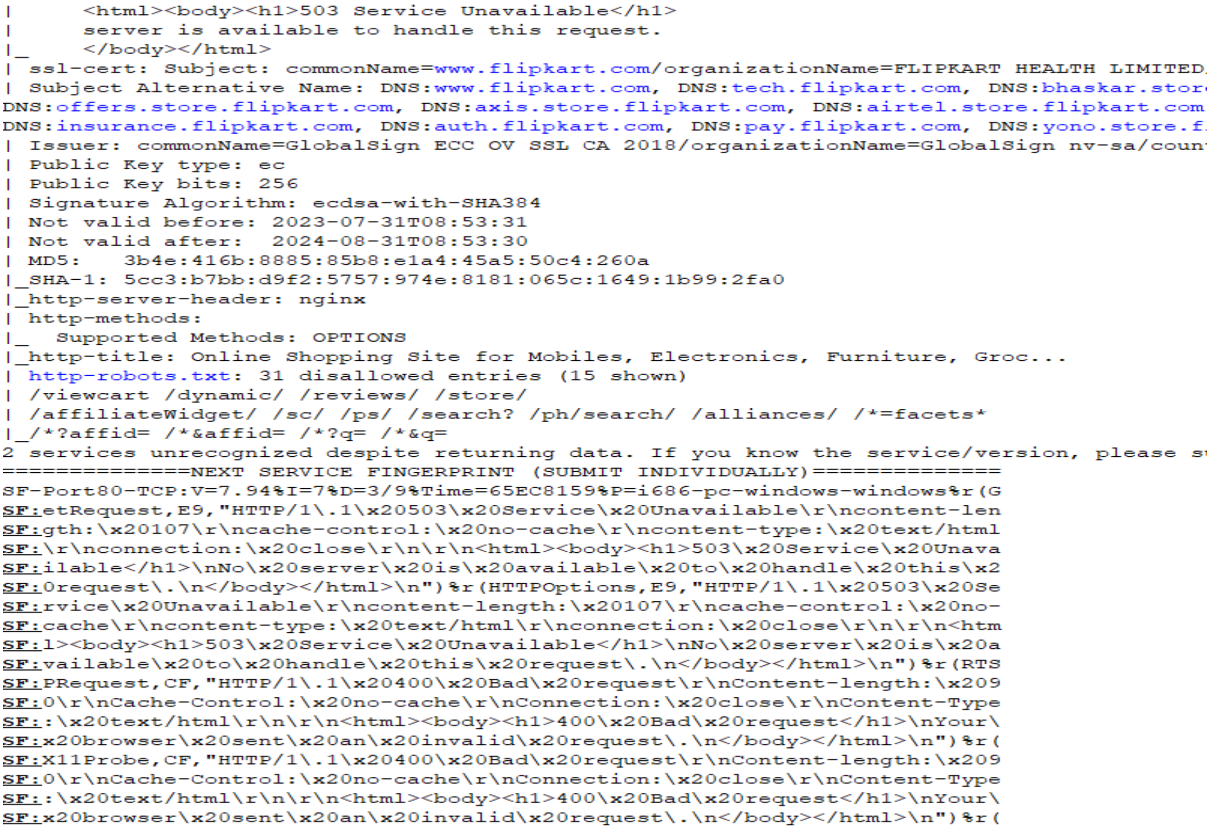
Profile: Intense scan

Command: nmap -T4 -A -v www.flipkart.com

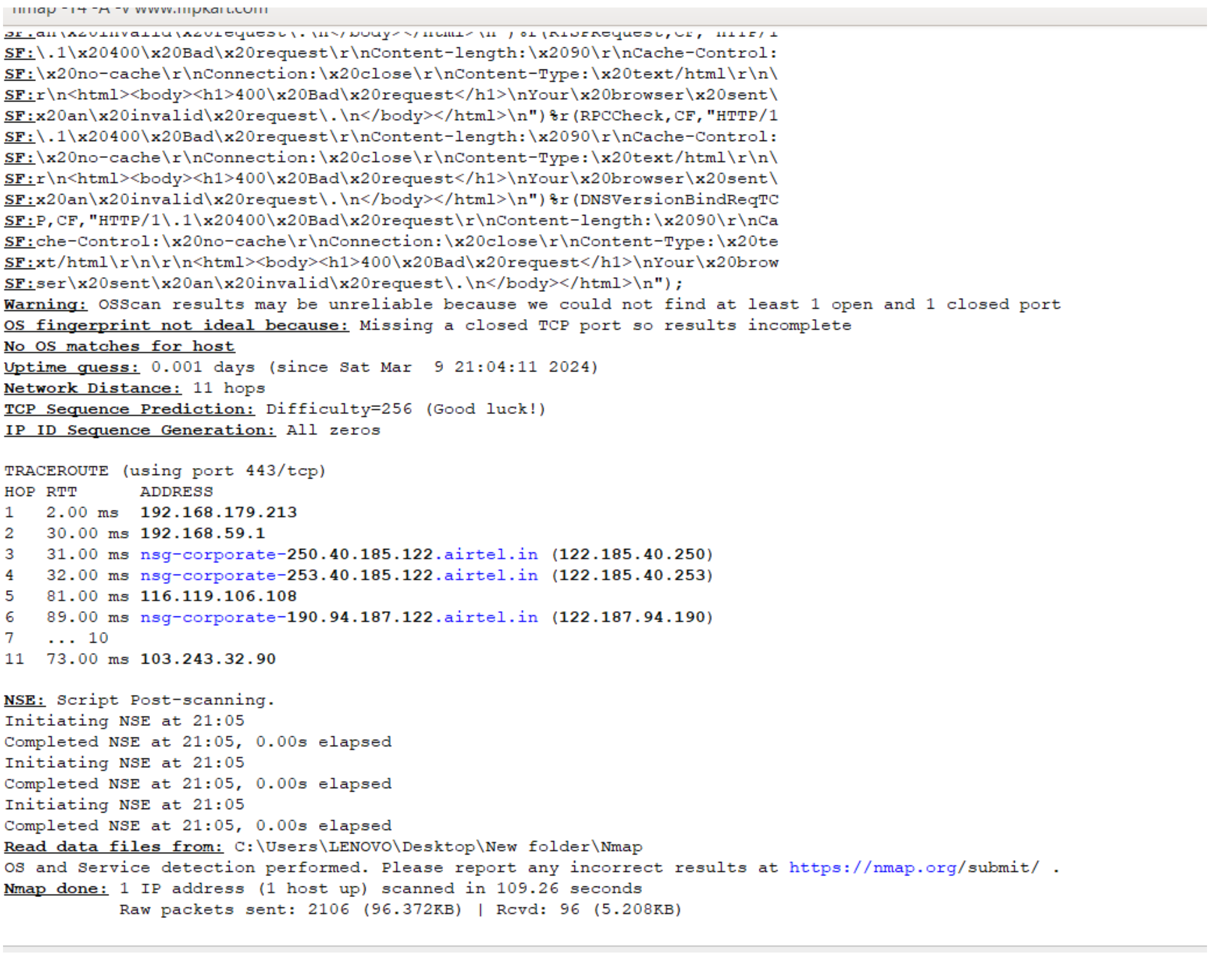
```
nmap -T4 -A -v www.flipkart.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-09 21:03 India Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:03
Completed NSE at 21:03, 0.00s elapsed
Initiating NSE at 21:03
Completed NSE at 21:03, 0.00s elapsed
Initiating NSE at 21:03
Completed NSE at 21:03, 0.00s elapsed
Initiating Ping Scan at 21:03
Scanning www.flipkart.com (103.243.32.90) [4 ports]
Completed Ping Scan at 21:03, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:03
Completed Parallel DNS resolution of 1 host. at 21:03, 0.00s elapsed
Initiating SYN Stealth Scan at 21:03
Scanning www.flipkart.com (103.243.32.90) [1000 ports]
Discovered open port 443/tcp on 103.243.32.90
Discovered open port 80/tcp on 103.243.32.90
Completed SYN Stealth Scan at 21:03, 9.01s elapsed (1000 total ports)
Initiating Service scan at 21:03
Scanning 2 services on www.flipkart.com (103.243.32.90)
Completed Service scan at 21:04, 28.84s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.flipkart.com (103.243.32.90)
Retrying OS detection (try #2) against www.flipkart.com (103.243.32.90)
Initiating Traceroute at 21:04
Completed Traceroute at 21:04, 3.04s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 21:04
Completed Parallel DNS resolution of 7 hosts. at 21:04, 2.40s elapsed
NSE: Script scanning 103.243.32.90.
Initiating NSE at 21:04
Completed NSE at 21:05, 58.38s elapsed
Initiating NSE at 21:05
Completed NSE at 21:05, 1.01s elapsed
Initiating NSE at 21:05
Completed NSE at 21:05, 0.00s elapsed
Nmap scan report for www.flipkart.com (103.243.32.90)
Host is up (0.059s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
|_http-server-header: nginx
| fingerprint-strings:
|   DNSVersionBindReqTCP, RPCCheck, RTSPRequest, X11Probe:
|     HTTP/1.1 400 Bad request
```



```
nmap -T4 -A -v www.flipkart.com
|   DNSVersionBindReqTCP, RPCCheck, RTSPRequest, X11Probe:
|     HTTP/1.1 400 Bad request
|     Content-length: 90
|     Cache-Control: no-cache
|     Connection: close
|     Content-Type: text/html
|     <html><body><h1>400 Bad request</h1>
|     Your browser sent an invalid request.
|     </body></html>
|   FourOhFourRequest, GetRequest, HTTPOptions:
|     HTTP/1.1 503 Service Unavailable
|     content-length: 107
|     cache-control: no-cache
|     content-type: text/html
|     connection: close
|     <html><body><h1>503 Service Unavailable</h1>
|     server is available to handle this request.
|_    </body></html>
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://www.flipkart.com/
| http-robots.txt: 31 disallowed entries (15 shown)
| /viewcart /dynamic/ /reviews/ /store/
| /affiliateWidget/ /sc/ /ps/ /search? /ph/search/ /alliances/ /*=facets*
|_/*?affid= /*&affid= /*?q= /*&q=
443/tcp open  ssl/https nginx
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   DNSVersionBindReqTCP, RPCCheck, RTSPRequest, tor-versions:
|     HTTP/1.1 400 Bad request
|     Content-length: 90
|     Cache-Control: no-cache
|     Connection: close
|     Content-Type: text/html
|     <html><body><h1>400 Bad request</h1>
|     Your browser sent an invalid request.
|     </body></html>
|   FourOhFourRequest, GetRequest, HTTPOptions:
|     HTTP/1.1 503 Service Unavailable
|     content-length: 107
|     cache-control: no-cache
|     content-type: text/html
|     connection: close
|     <html><body><h1>503 Service Unavailable</h1>
```



```
|      <html><body><h1>503 Service Unavailable</h1>
|      server is available to handle this request.
|_     </body></html>
| ssl-cert: Subject: commonName=www.flipkart.com/organizationName=FLIPKART HEALTH LIMITED
| Subject Alternative Name: DNS:www.flipkart.com, DNS:tech.flipkart.com, DNS:bhaskar.stor
DNS:offers.store.flipkart.com, DNS:axis.store.flipkart.com, DNS:airtel.store.flipkart.com
DNS:insurance.flipkart.com, DNS:auth.flipkart.com, DNS:pay.flipkart.com, DNS:yono.store.f
| Issuer: commonName=GlobalSign ECC OV SSL CA 2018/organizationName=GlobalSign nv-sa/coun
| Public Key type: ec
| Public Key bits: 256
| Signature Algorithm: ecdsa-with-SHA384
| Not valid before: 2023-07-31T08:53:31
| Not valid after:  2024-08-31T08:53:30
| MD5:   3b4e:416b:8885:85b8:e1a4:45a5:50c4:260a
|_SHA-1: 5cc3:b7bb:d9f2:5757:974e:8181:065c:1649:1b99:2fa0
|_http-server-header: nginx
| http-methods:
|_  Supported Methods: OPTIONS
|_http-title: Online Shopping Site for Mobiles, Electronics, Furniture, Groc...
| http-robots.txt: 31 disallowed entries (15 shown)
| /viewcart /dynamic/ /reviews/ /store/
| /affiliateWidget/ /sc/ /ps/ /search? /ph/search/ /alliances/ /*=facets*
|_/*?affid= /*&affid= /*?q= /*&q=
2 services unrecognized despite returning data. If you know the service/version, please s
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94%I=7%D=3/9%Time=65EC8159%P=i686-pc-windows-windows%r(G
SF:etRequest,E9,"HTTP/1\.1\x20503\x20Service\x20Unavailable\r\ncontent-len
SF:gth:\x20107\r\ncache-control:\x20no-cache\r\ncontent-type:\x20text/html
SF:\r\nconnection:\x20close\r\n\r\n<html><body><h1>503\x20Service\x20Unava
SF:ilable</h1>\nNo\x20server\x20is\x20available\x20to\x20handle\x20this\x2
SF:0request\.\n</body></html>\n")%r(HTTPOptions,E9,"HTTP/1\.1\x20503\x20Se
SF:rvice\x20Unavailable\r\ncontent-length:\x20107\r\ncache-control:\x20no-
SF:cache\r\ncontent-type:\x20text/html\r\nconnection:\x20close\r\n\r\n<htm
SF:l><body><h1>503\x20Service\x20Unavailable</h1>\nNo\x20server\x20is\x20a
SF:vailable\x20to\x20handle\x20this\x20request\.\n</body></html>\n")%r(RTS
SF:PRequest,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-length:\x209
SF:0\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-Type
SF::\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1>\nYour\
SF:x20browser\x20sent\x20an\x20invalid\x20request\.\n</body></html>\n")%r(
SF:X11Probe,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-length:\x209
SF:0\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-Type
SF::\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1>\nYour\
SF:x20browser\x20sent\x20an\x20invalid\x20request\.\n</body></html>\n")%r(
```



```
nmap -T4 -A -v www.flipkart.com
SF:an\x20invalid\x20request\.\n</body></html>\n")%r(RTSPRequest,CF,"HTTP/1
SF:\.1\x20400\x20Bad\x20request\r\nContent-length:\x2090\r\nCache-Control:
SF:\x20no-cache\r\nConnection:\x20close\r\nContent-Type:\x20text/html\r\n\
SF:r\n<html><body><h1>400\x20Bad\x20request</h1>\nYour\x20browser\x20sent\
SF:x20an\x20invalid\x20request\.\n</body></html>\n")%r(RPCCheck,CF,"HTTP/1
SF:\.1\x20400\x20Bad\x20request\r\nContent-length:\x2090\r\nCache-Control:
SF:\x20no-cache\r\nConnection:\x20close\r\nContent-Type:\x20text/html\r\n\
SF:r\n<html><body><h1>400\x20Bad\x20request</h1>\nYour\x20browser\x20sent\
SF:x20an\x20invalid\x20request\.\n</body></html>\n")%r(DNSVersionBindReqTC
SF:P,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-length:\x2090\r\nCa
SF:che-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-Type:\x20te
SF:xt/html\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1>\nYour\x20brow
SF:ser\x20sent\x20an\x20invalid\x20request\.\n</body></html>\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Uptime guess: 0.001 days (since Sat Mar  9 21:04:11 2024)
Network Distance: 11 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   2.00 ms  192.168.179.213
2   30.00 ms 192.168.59.1
3   31.00 ms nsg-corporate-250.40.185.122.airtel.in (122.185.40.250)
4   32.00 ms nsg-corporate-253.40.185.122.airtel.in (122.185.40.253)
5   81.00 ms 116.119.106.108
6   89.00 ms nsg-corporate-190.94.187.122.airtel.in (122.187.94.190)
7   ... 10
11  73.00 ms 103.243.32.90

NSE: Script Post-scanning.
Initiating NSE at 21:05
Completed NSE at 21:05, 0.00s elapsed
Initiating NSE at 21:05
Completed NSE at 21:05, 0.00s elapsed
Initiating NSE at 21:05
Completed NSE at 21:05, 0.00s elapsed
Read data files from: C:\Users\LENOVO\Desktop\New folder\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.26 seconds
           Raw packets sent: 2106 (96.372KB) | Rcvd: 96 (5.208KB)
```

some information about targets www.flipkart.com:

1. **Host Information**:
   - IP Address: 103.243.32.90
   - Host is up with a latency of 0.078 seconds.

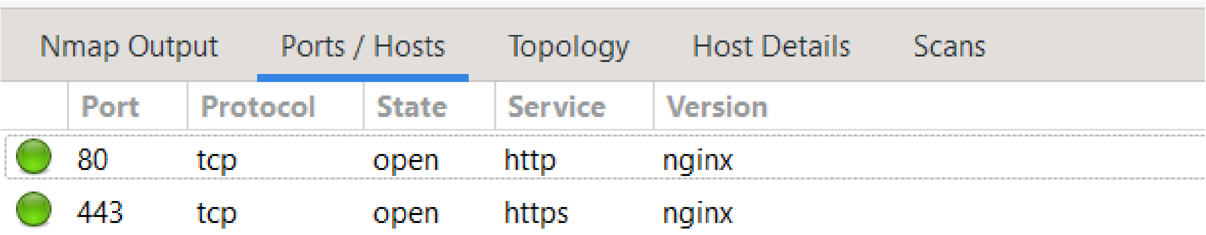
2. **Open Ports**:
   - Port 80/tcp: Open, running HTTP service (nginx).
   - Port 443/tcp: Open, running SSL/HTTPS service (nginx).

3. **HTTP Service** (Port 80/tcp):
   - Server: nginx
   - Supported HTTP Methods: GET, HEAD, POST, OPTIONS
   - HTTP Title: The scan did not follow the redirect to https://www.flipkart.com/
   - Robots.txt Disallowed Entries: 31 entries

4. **HTTPS Service** (Port 443/tcp):
   - Server: nginx
   - SSL Certificate Information:
     - Subject: CommonName=www.flipkart.com, OrganizationName=FLIPKART HEALTH LIMITED, StateOrProvinceName=West Bengal, CountryName=IN
     - Subject Alternative Name: Various subdomains of flipkart.com
     - Issuer: CommonName=GlobalSign ECC OV SSL CA 2018, OrganizationName=GlobalSign nv-sa, CountryName=BE
     - Validity: From July 31, 2023, to August 31, 2024

5. **Operating System Detection**:
   - Device Type: General purpose
   - Running OS (Guessed): OpenBSD
   - Aggressive OS Guess: OpenBSD
   - Uptime Guess: 0.001 days

6. **Network Distance**: 11 hops



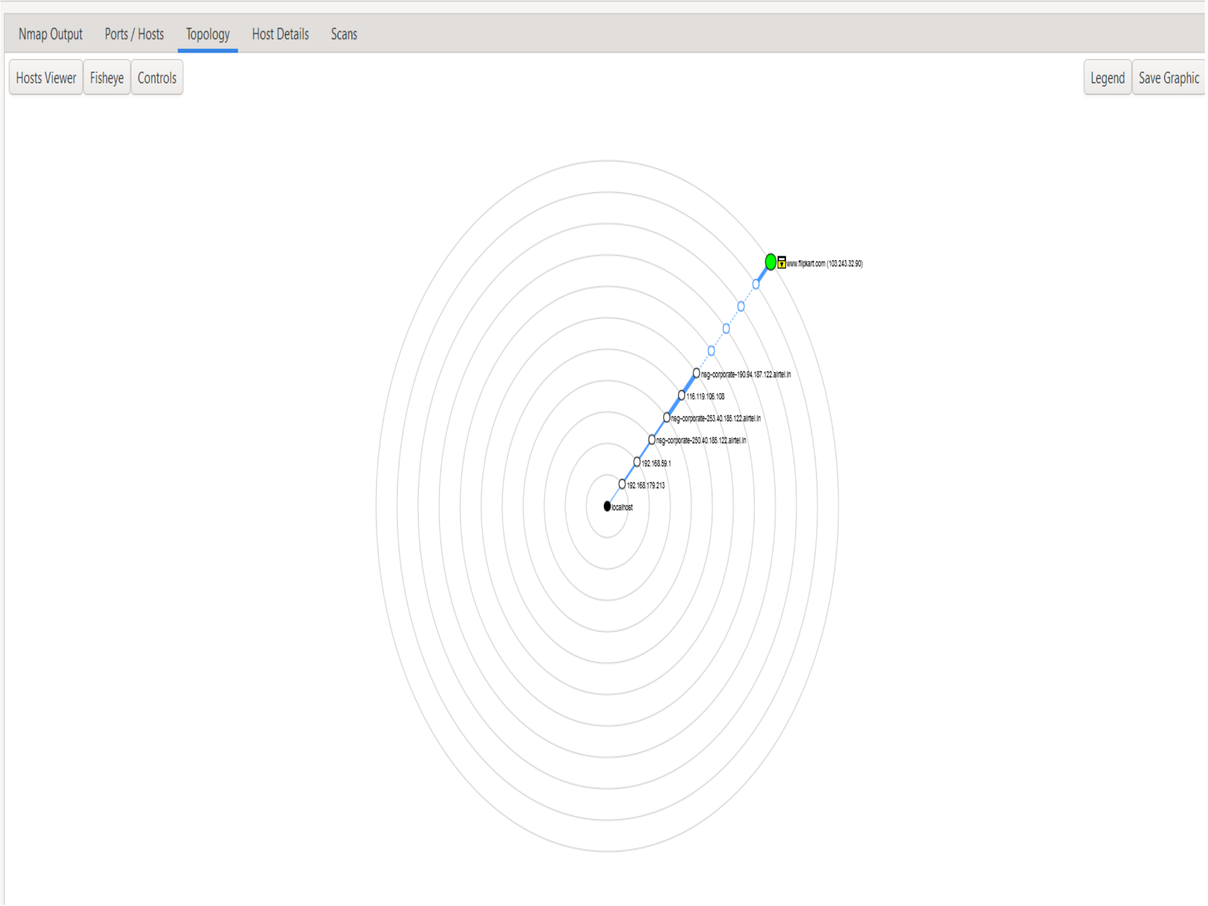
	Port	Protocol	State	Service	Version
●	80	tcp	open	http	nginx
●	443	tcp	open	https	nginx

- **Hosts**: Devices like computers, servers, or smartphones on a network.
- **Ports**: Channels on a host through which network traffic flows, allowing different types of communication.

Here are the ports and hosts provided:

- **Port 80**:
  - Protocol: TCP
  - State: Open
  - Service: HTTP

- **Port 443**:
  - Protocol: TCP
  - State: Open
  - Service: HTTPS


Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
www.flipkart.com (103.243.32.90)
nsg-corporate-190.94.187.122.airtel.in
116.119.106.108
nsg-corporate-253.40.185.122.airtel.in
nsg-corporate-250.40.185.122.airtel.in
192.168.59.1
192.168.179.213
localhost

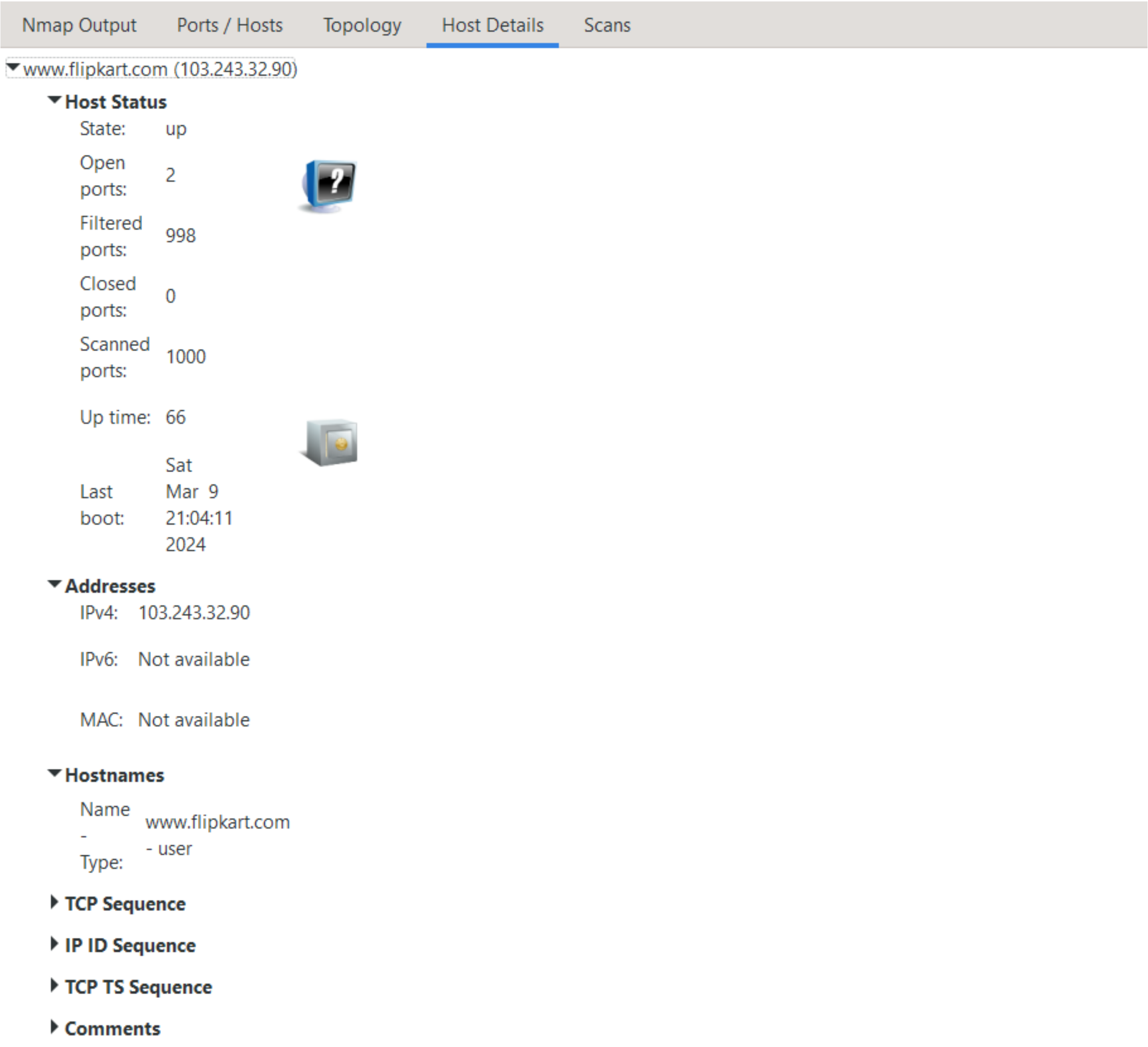
Topology refers to the arrangement or structure of interconnected elements within a system, such as a network.

Hosts Viewer allows you to view and manage information about scanned hosts, including their IP addresses, hostnames, open ports, and other details.

Fisheye is a feature in Nmap that provides a broad overview of the results of a scan, allowing you to quickly identify patterns or anomalies in the data.

Controls in Nmap refer to various options and parameters that you can use to customize and control the behavior of the scan. This includes options like specifying target hosts, scan types, timing options, output formats, and more.

- www.flipkart.com **(105.243.32.90)**: This is the target host being scanned.
- **nsg-corporate-190.94.107.122.airtel.in**: This appears to be a router or gateway device (nsg-corporate) within the Airtel network (airtel.in), with the IP address 190.94.107.122.
- **116.119.106.105**: This is another intermediate device with the IP address 116.119.106.105.
- **nsg-corporate-253.40.105.122.airtel.in**: Similar to the first one, this seems to be another router or gateway device within the Airtel network, with the IP address 40.105.122.
- **nsg-corporate-254.40.185.122.airtel.in**: Another router or gateway device within the Airtel network, with the IP address 40.185.122.
- **192.168.59.1 and 192.168.179.213**: These are private IP addresses, likely representing local devices within a private network.
- **localhost**: This typically refers to the local machine or device on which the Nmap scan is being executed.



www.flipkart.com (103.243.32.90)

Host Status

State: up

Open ports: 2

Filtered ports: 998

Closed ports: 0

Scanned ports: 1000

Up time: 66

Last boot: Sat Mar 9 21:04:11 2024

Addresses

IPv4: 103.243.32.90

IPv6: Not available

MAC: Not available

Hostnames

Name - Type: www.flipkart.com - user

TCP Sequence

IP ID Sequence

TCP TS Sequence

Comments

- **Host Status**:

  - The host is **open**, indicating it's accessible.

  - **Filtered ports**: Some ports couldn't be reached due to filtering.

  - **Closed ports**: No services found on these ports.

- **Ports Scanned**:

  - A total of 1000 ports were scanned.

  - Only 2 ports were found to be up and responsive.

- **Uptime**:

  - The host has been up for 66 seconds.

  - Last booted on March 9, 2024, at 21:04:11.

- **Addresses**:

  - IPv4 address: 103.243.32.90

  - IPv6 address: Not available

  - MAC address: Not available

- **Hostnames**:

  - The hostname is www.flipkart.com, representing the target.

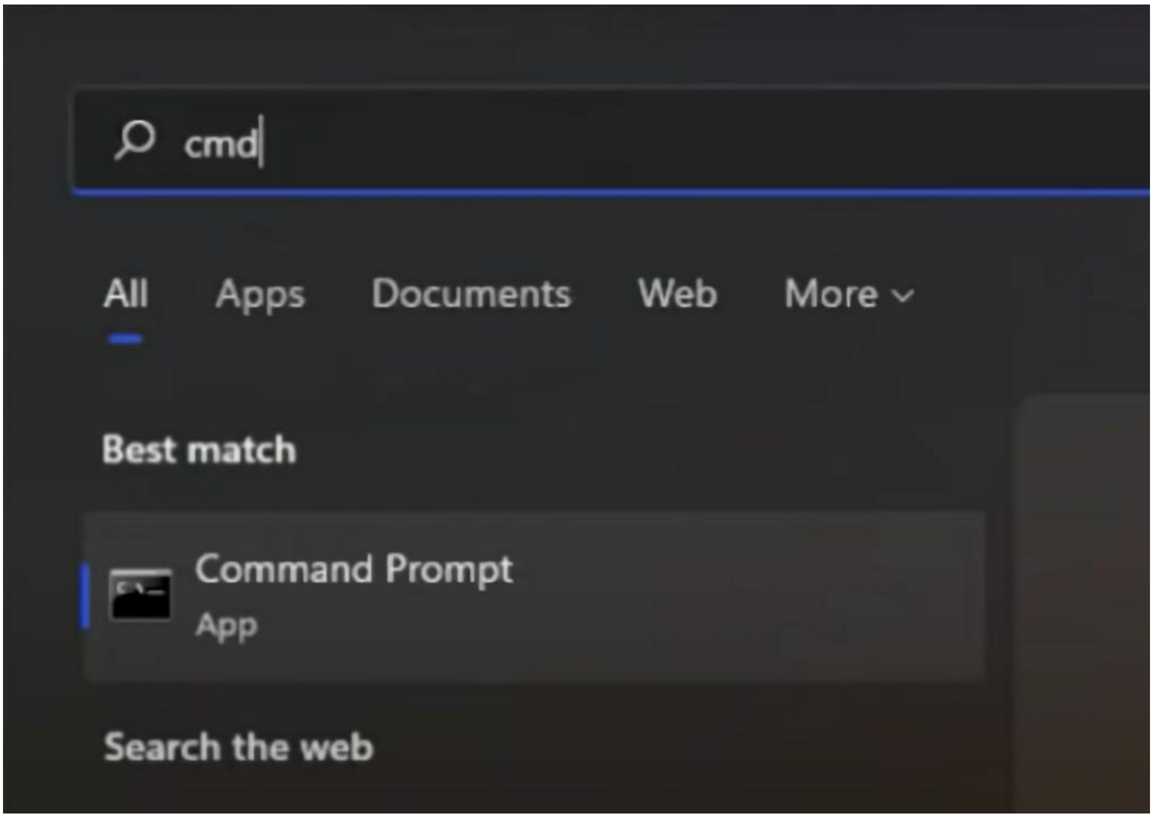
- **Comments**:

  - Additional information such as TCP sequence and IP ID sequence is available but not specified.

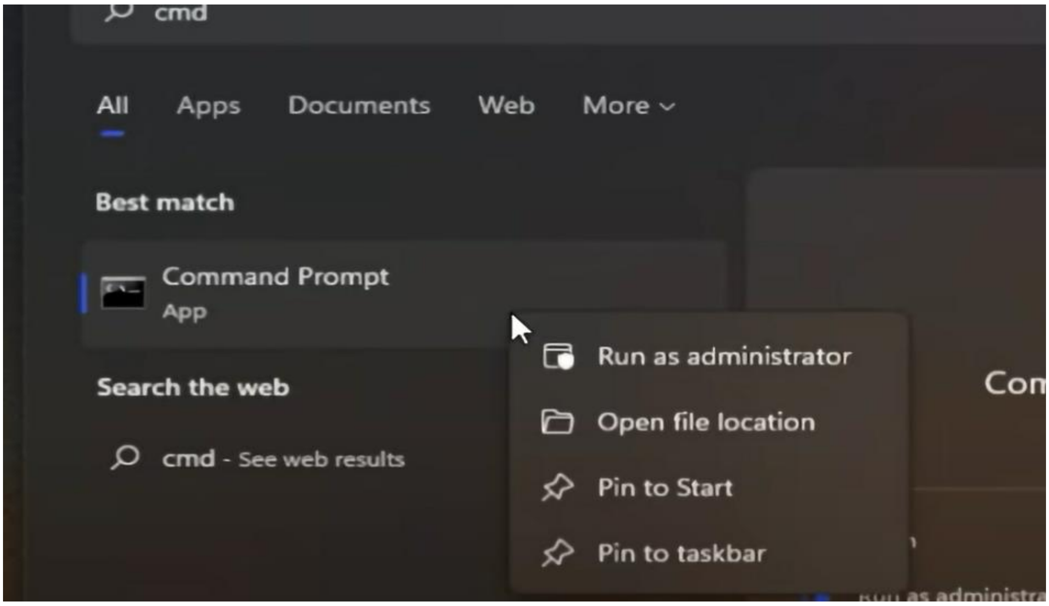
Q 2:- write and explain commands in window command prompt for network/service details?

ANS:-

Step 1:- go to the search bar of your computer and search cmd

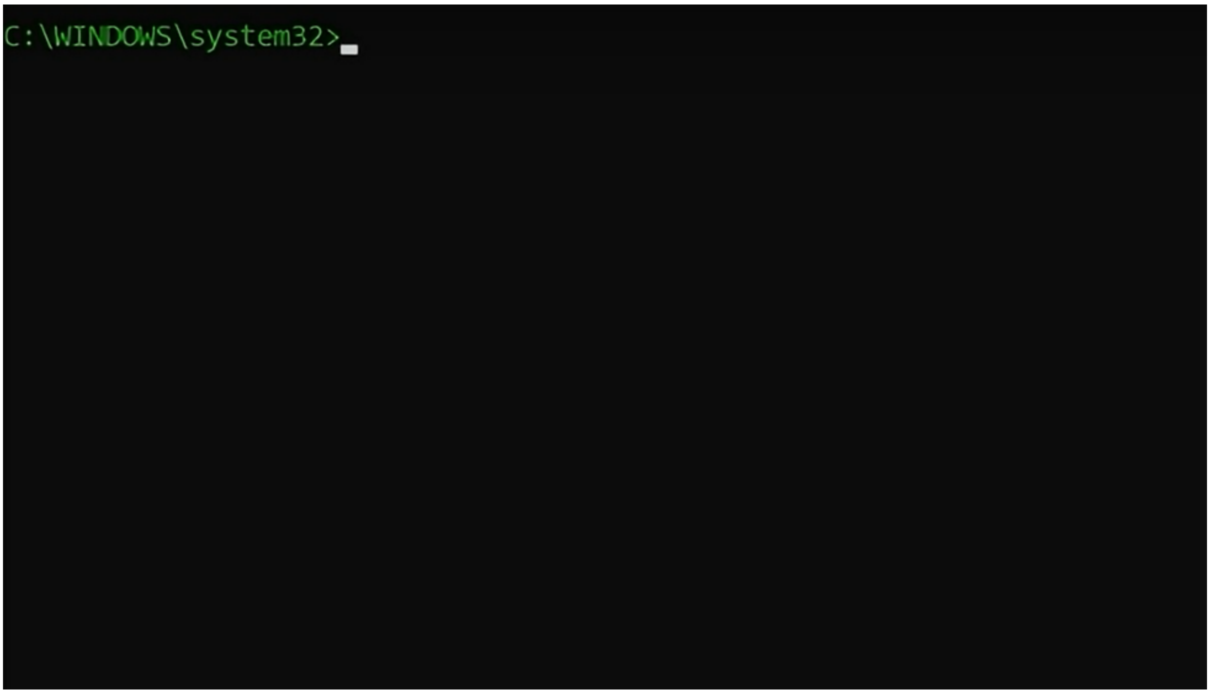


Step 2:- right click and put the mouse



click to run administrator.

Step2:- your cmd command prompt will open

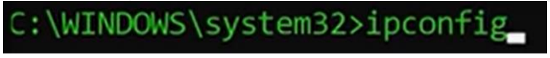


```
C:\WINDOWS\system32>_
```

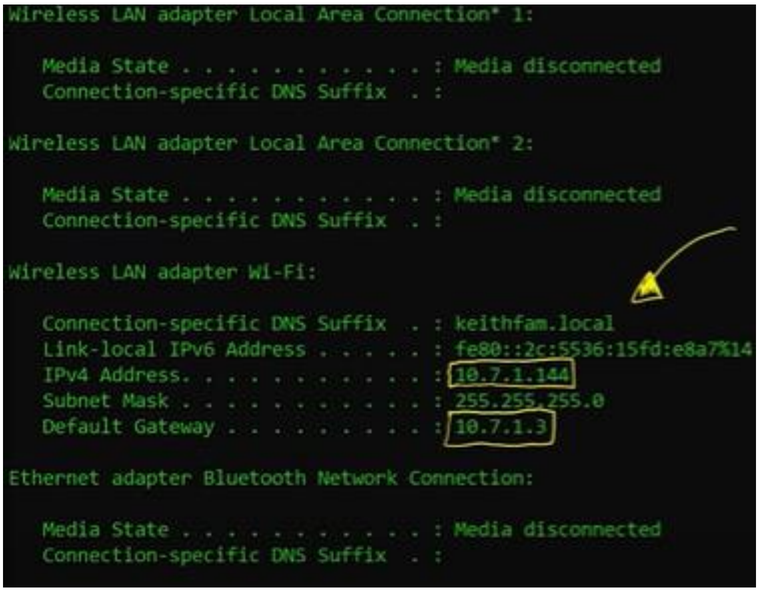
ipconfig:

- **Explanation**: Displays the current TCP/IP network configuration values. This includes IP address, subnet mask, default gateway, etc.
- **When to use**:
  - Troubleshooting network connectivity issues.
  - Verifying network settings.

    - Renewing or releasing IP addresses.



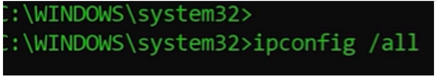
```
C:\WINDOWS\system32>ipconfig_
```



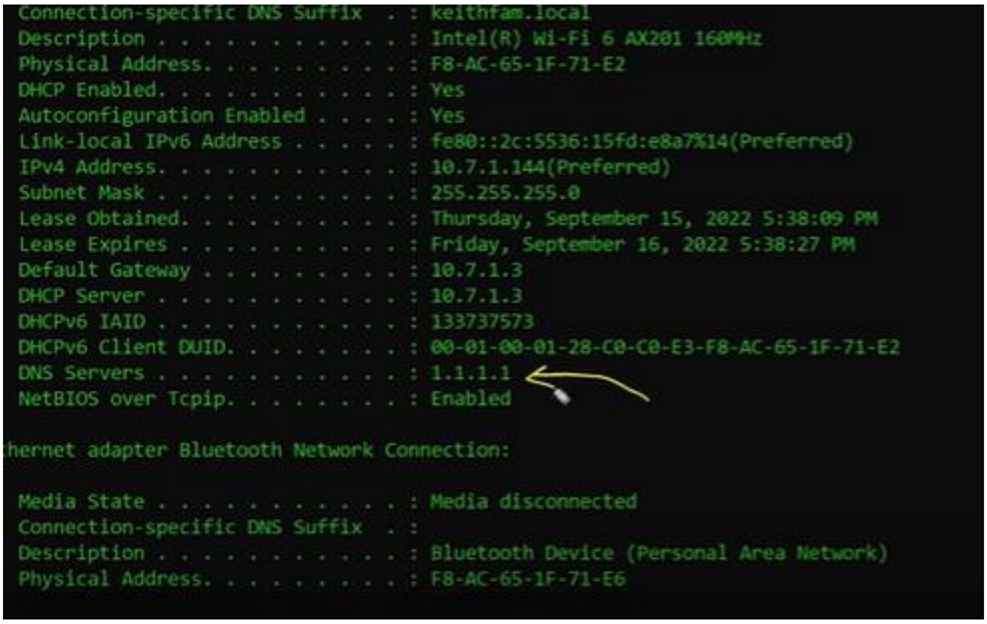
```
Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : keithfam.local
   Link-local IPv6 Address . . . . . : fe80::2c:5536:15fd:e8a7%14
   IPv4 Address. . . . . . . . . . . : 10.7.1.144
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.7.1.3

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

ipconfig /all:

- **Explanation**: Provides detailed information about the network configuration, including DNS servers, DHCP server, MAC address, etc.
- **When to use**:
    - Diagnosing complex network issues.
    - Gathering detailed network information.



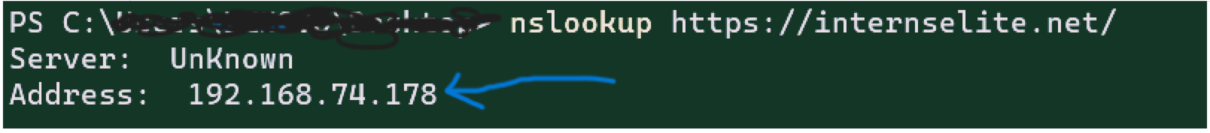
```
:\WINDOWS\system32>
:\WINDOWS\system32>ipconfig /all
```



```
   Connection-specific DNS Suffix  . : keithfam.local
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : F8-AC-65-1F-71-E2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2c:5536:15fd:e8a7%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.7.1.144(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, September 15, 2022 5:38:09 PM
   Lease Expires . . . . . . . . . . : Friday, September 16, 2022 5:38:27 PM
   Default Gateway . . . . . . . . . : 10.7.1.3
   DHCP Server . . . . . . . . . . . : 10.7.1.3
   DHCPv6 IAID . . . . . . . . . . . : 133737573
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-C0-C0-E3-F8-AC-65-1F-71-E2
   DNS Servers . . . . . . . . . . . : 1.1.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

hernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : F8-AC-65-1F-71-E6
```

nslookup:

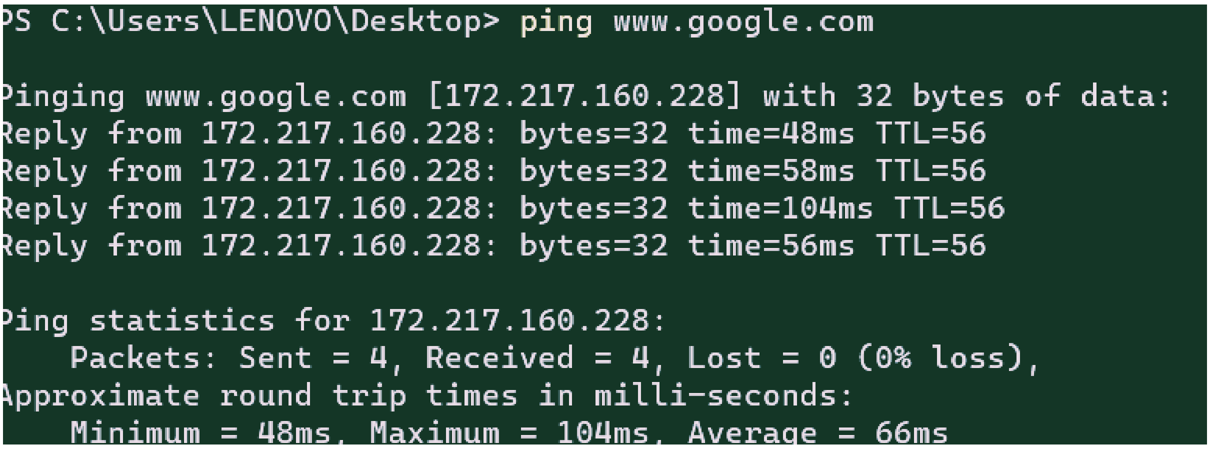
- **Explanation**: A network administration command-line tool used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records.
- **When to use**:
  - Troubleshooting DNS-related issues.
  - Checking DNS records for a domain.
  - Verifying DNS resolution.



```
PS C:\[redacted] nslookup https://internselite.net/
Server:  UnKnown
Address:  192.168.74.178
```

ping:

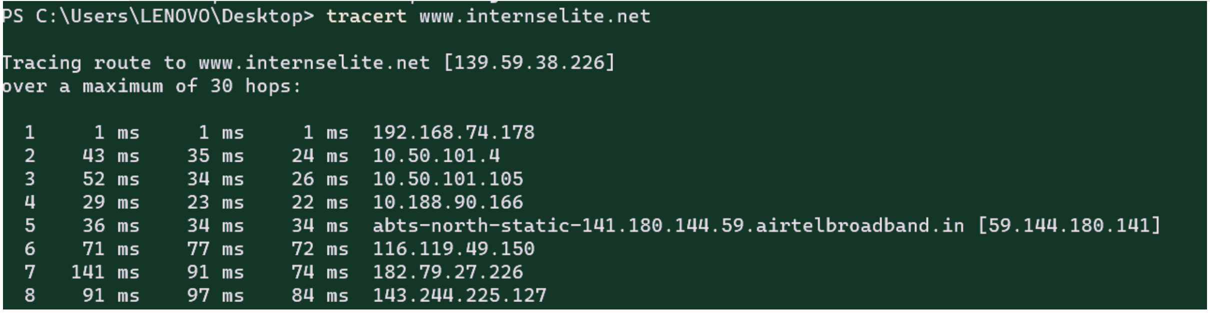
- **Explanation**: Sends ICMP Echo Request messages to a specified network host to check if it's reachable and measure the round-trip time.
- **When to use**:
  - Testing connectivity to a remote host.
  - Diagnosing network latency issues.
  - Verifying network availability.



```
PS C:\Users\LENOVO\Desktop> ping www.google.com

Pinging www.google.com [172.217.160.228] with 32 bytes of data:
Reply from 172.217.160.228: bytes=32 time=48ms TTL=56
Reply from 172.217.160.228: bytes=32 time=58ms TTL=56
Reply from 172.217.160.228: bytes=32 time=104ms TTL=56
Reply from 172.217.160.228: bytes=32 time=56ms TTL=56

Ping statistics for 172.217.160.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 48ms, Maximum = 104ms, Average = 66ms
```

tracert:

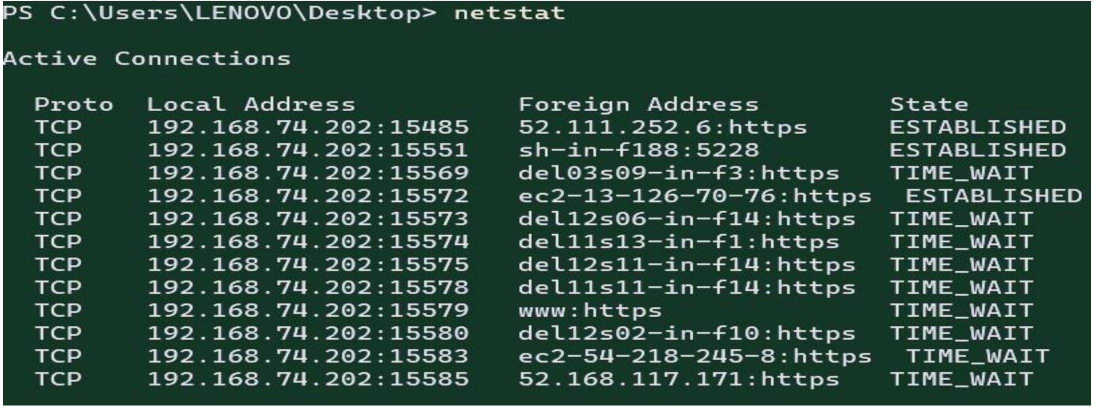
- **Explanation**: Traces the route taken by packets from the source to the destination, showing the number of hops and the time taken by each.
- **When to use**:
  - Identifying network routing issues.
  - Troubleshooting slow network connections.
  - Analyzing network paths.



```
PS C:\Users\LENOVO\Desktop> tracert www.internselite.net

Tracing route to www.internselite.net [139.59.38.226]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.74.178
  2    43 ms    35 ms    24 ms  10.50.101.4
  3    52 ms    34 ms    26 ms  10.50.101.105
  4    29 ms    23 ms    22 ms  10.188.90.166
  5    36 ms    34 ms    34 ms  abts-north-static-141.180.144.59.airtelbroadband.in [59.144.180.141]
  6    71 ms    77 ms    72 ms  116.119.49.150
  7   141 ms    91 ms    74 ms  182.79.27.226
  8    91 ms    97 ms    84 ms  143.244.225.127
```

netstat:

- **Explanation**: Displays active network connections, routing tables, interface statistics, masquerade connections, multicast memberships, and other network-related information.
- **When to use**:
  - Monitoring network connections.
  - Identifying network usage.
  - Diagnosing network performance issues.



```
PS C:\Users\LENOVO\Desktop> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.74.202:15485   52.111.252.6:https     ESTABLISHED
  TCP    192.168.74.202:15551   sh-in-f188:5228        ESTABLISHED
  TCP    192.168.74.202:15569   del03s09-in-f3:https   TIME_WAIT
  TCP    192.168.74.202:15572   ec2-13-126-70-76:https  ESTABLISHED
  TCP    192.168.74.202:15573   del12s06-in-f14:https  TIME_WAIT
  TCP    192.168.74.202:15574   del11s13-in-f1:https   TIME_WAIT
  TCP    192.168.74.202:15575   del12s11-in-f14:https  TIME_WAIT
  TCP    192.168.74.202:15578   del11s11-in-f14:https  TIME_WAIT
  TCP    192.168.74.202:15579   www:https              TIME_WAIT
  TCP    192.168.74.202:15580   del12s02-in-f10:https  TIME_WAIT
  TCP    192.168.74.202:15583   ec2-54-218-245-8:https  TIME_WAIT
  TCP    192.168.74.202:15585   52.168.117.171:https   TIME_WAIT
```

Q 3:- use website copying tool for website copy (Httrack)?

ANS 3)

HTTRACK

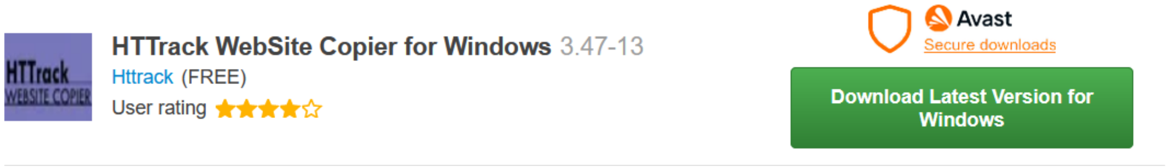
HTTrack is a popular website copying tool that allows users to download entire websites for offline browsing. Here are the key points about HTTrack:

1. **Website Mirroring**: HTTrack allows users to duplicate entire websites onto their local storage, capturing HTML, images, CSS, JavaScript, and other resources.
2. **Offline Browsing**: Users can access the mirrored version of websites offline, offering convenient browsing when internet connectivity is unavailable or unreliable.
3. **Recursive Retrieval**: Employing a recursive retrieval algorithm, HTTrack systematically follows links within a website, downloading all associated pages and resources to ensure a comprehensive copy.
4. **Customizable Settings**: HTTrack offers flexible configuration options, enabling users to specify parameters such as link depth, file types for download, and bandwidth limits.
5. **HTML Parsing**: HTTrack parses HTML files to adjust links and resources, ensuring seamless functionality of the mirrored website offline, even when the original website employs absolute URLs.

Installation

Step1:-Go to the website: https://filehippo.com/download_httrack-website-copier/

And Press the download button.

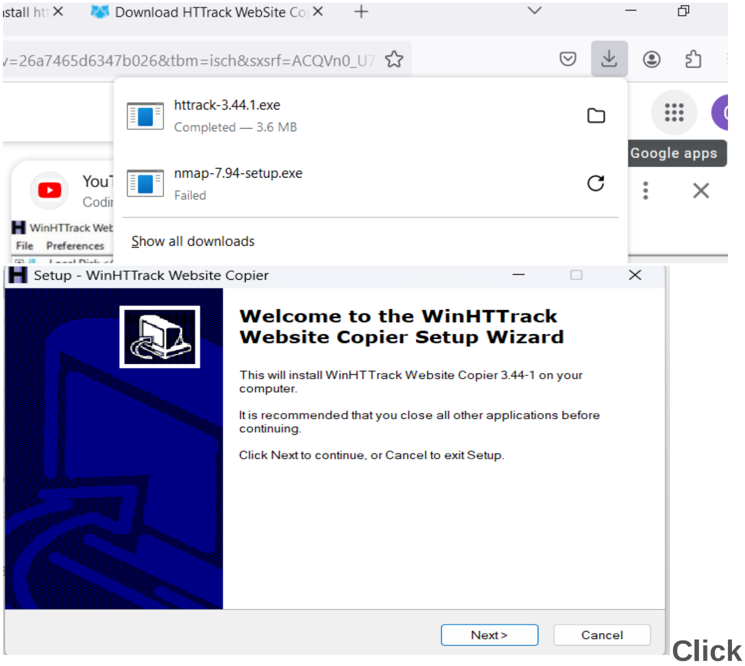


HTTrack WebSite Copier for Windows 3.47-13

Httrack (FREE)

User rating ★★★★☆

Step2:- Go to the download section and click on the downloaded file to begin the installation process.



Setup - WinHTTrack Website Copier

Welcome to the WinHTTrack Website Copier Setup Wizard

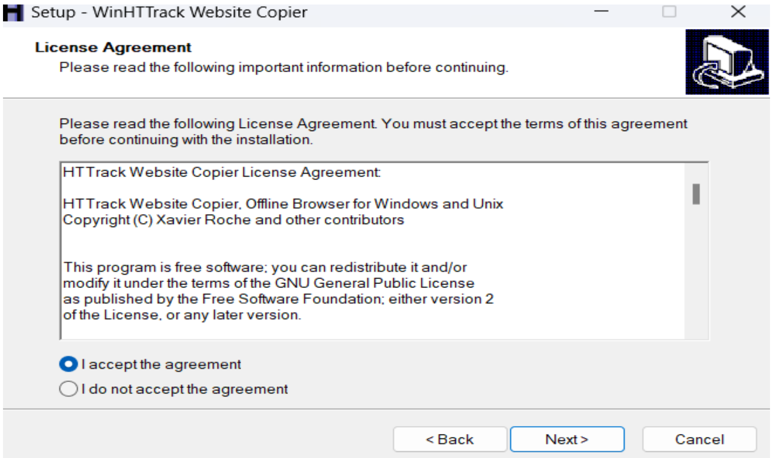
This will install WinHTTrack Website Copier 3.44-1 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Click Next.

Step3:- Accept the agreement



Setup - WinHTTrack Website Copier

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

HTTrack Website Copier License Agreement

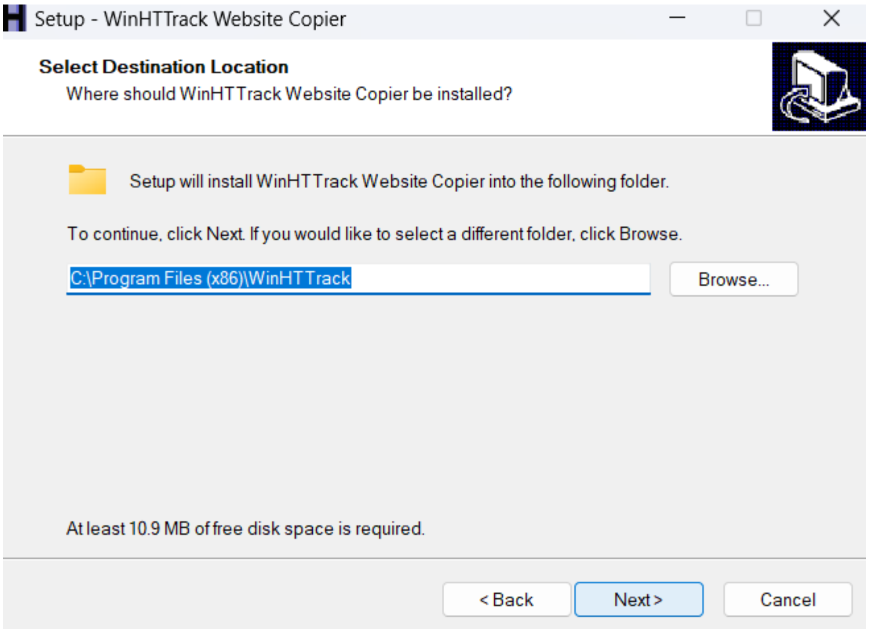
HTTrack Website Copier, Offline Browser for Windows and Unix
Copyright (C) Xavier Roche and other contributors

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version.

● I accept the agreement
○ I do not accept the agreement

Click Next.

Step4:- Choose the browser section or set it as default


Setup - WinHTTrack Website Copier

Select Destination Location

Where should WinHTTrack Website Copier be installed?

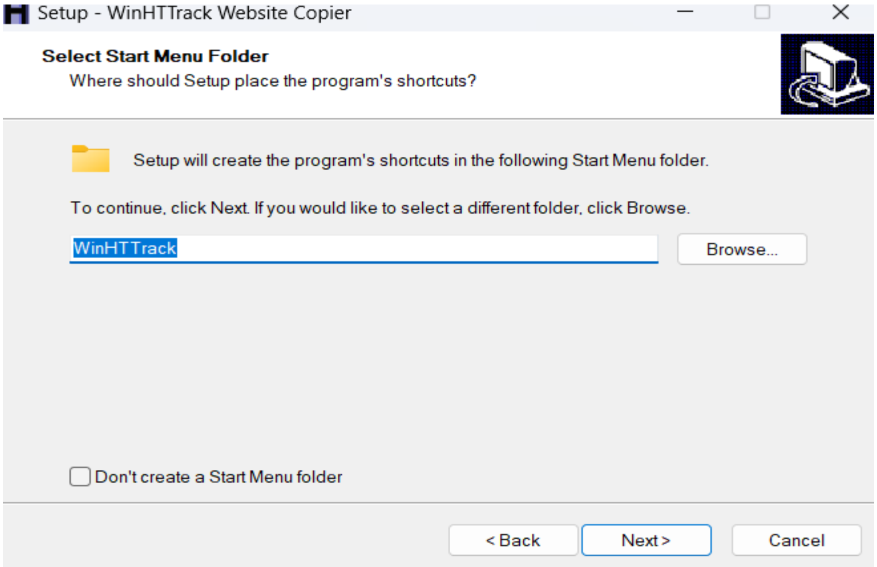
Setup will install WinHTTrack Website Copier into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\WinHTTrack

At least 10.9 MB of free disk space is required.

Click Next.


Setup - WinHTTrack Website Copier

Select Start Menu Folder

Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

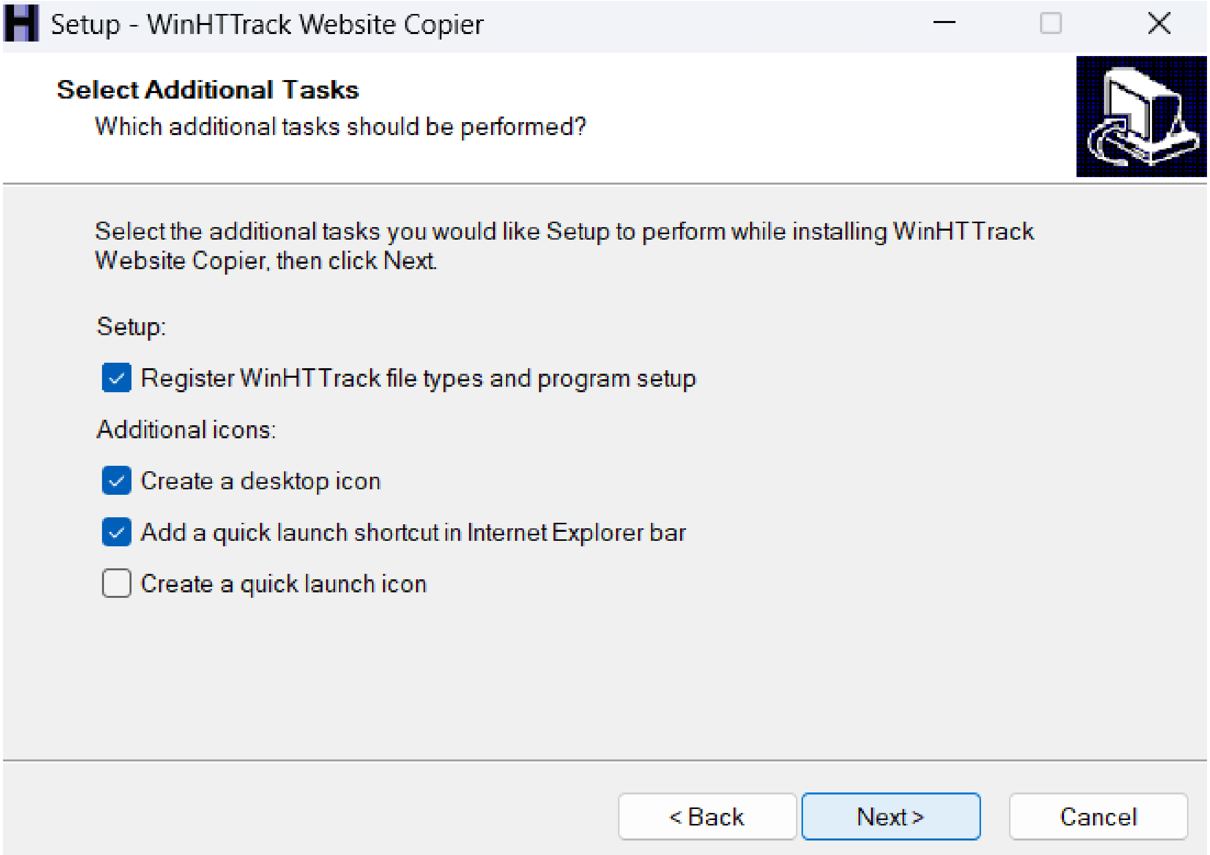
To continue, click Next. If you would like to select a different folder, click Browse.

WinHTTrack

□ Don't create a Start Menu folder

Click Next.

Step5:-chose the option if u need destop icon



Select Additional Tasks

Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing WinHTTrack Website Copier, then click Next.

Setup:

☑ Register WinHTTrack file types and program setup

Additional icons:

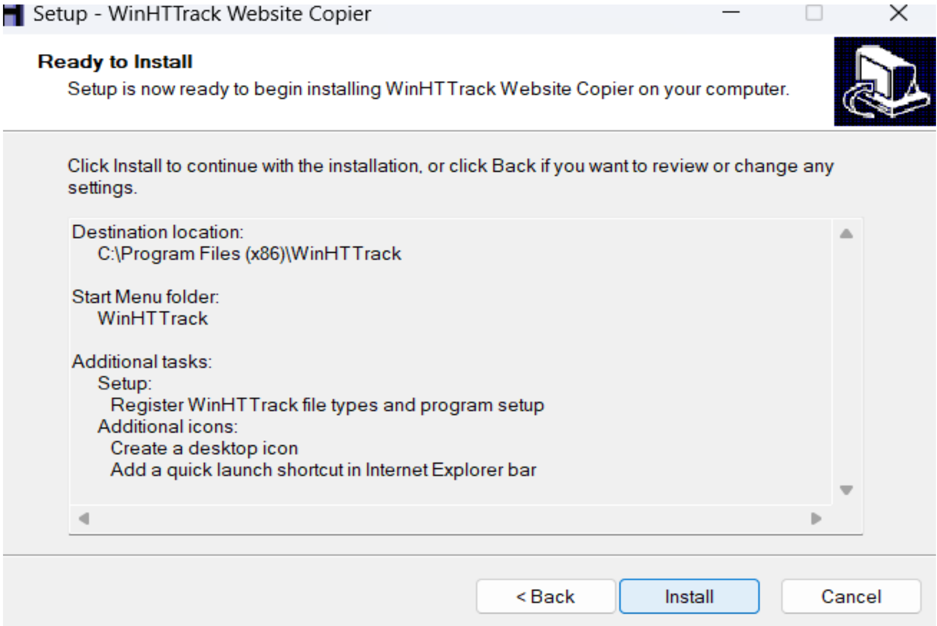
☑ Create a desktop icon

☑ Add a quick launch shortcut in Internet Explorer bar

□ Create a quick launch icon

Click Next.

Step6:- it is ready to install and press finish



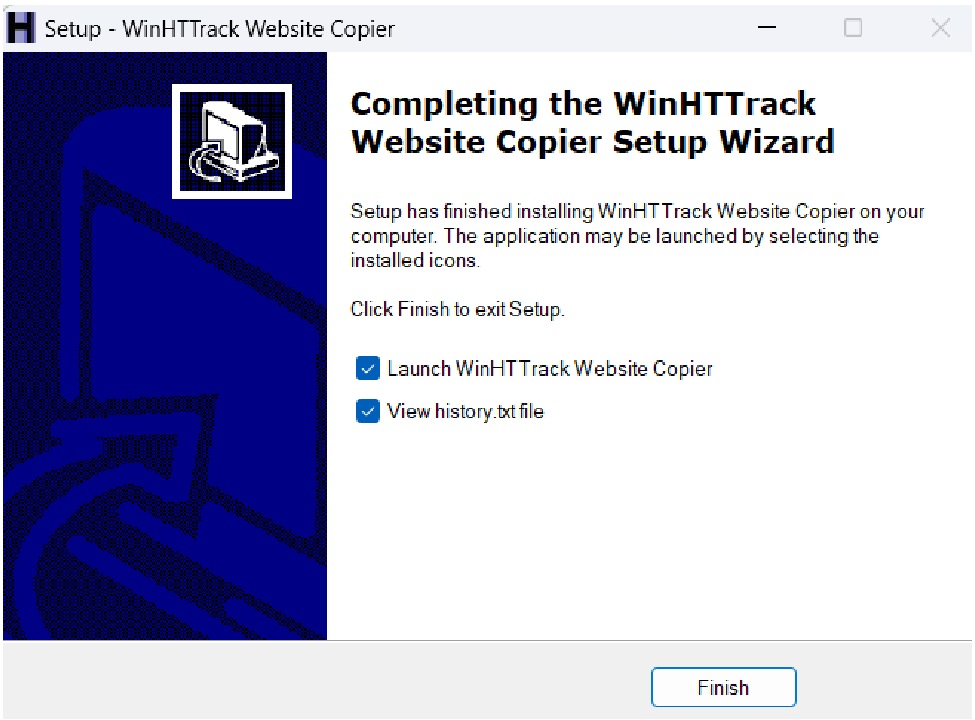
Ready to Install

Setup is now ready to begin installing WinHTTrack Website Copier on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
    C:\Program Files (x86)\WinHTTrack

Start Menu folder:
    WinHTTrack

Additional tasks:
    Setup:
      Register WinHTTrack file types and program setup
    Additional icons:
      Create a desktop icon
      Add a quick launch shortcut in Internet Explorer bar
```

click install



Completing the WinHTTrack Website Copier Setup Wizard

Setup has finished installing WinHTTrack Website Copier on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

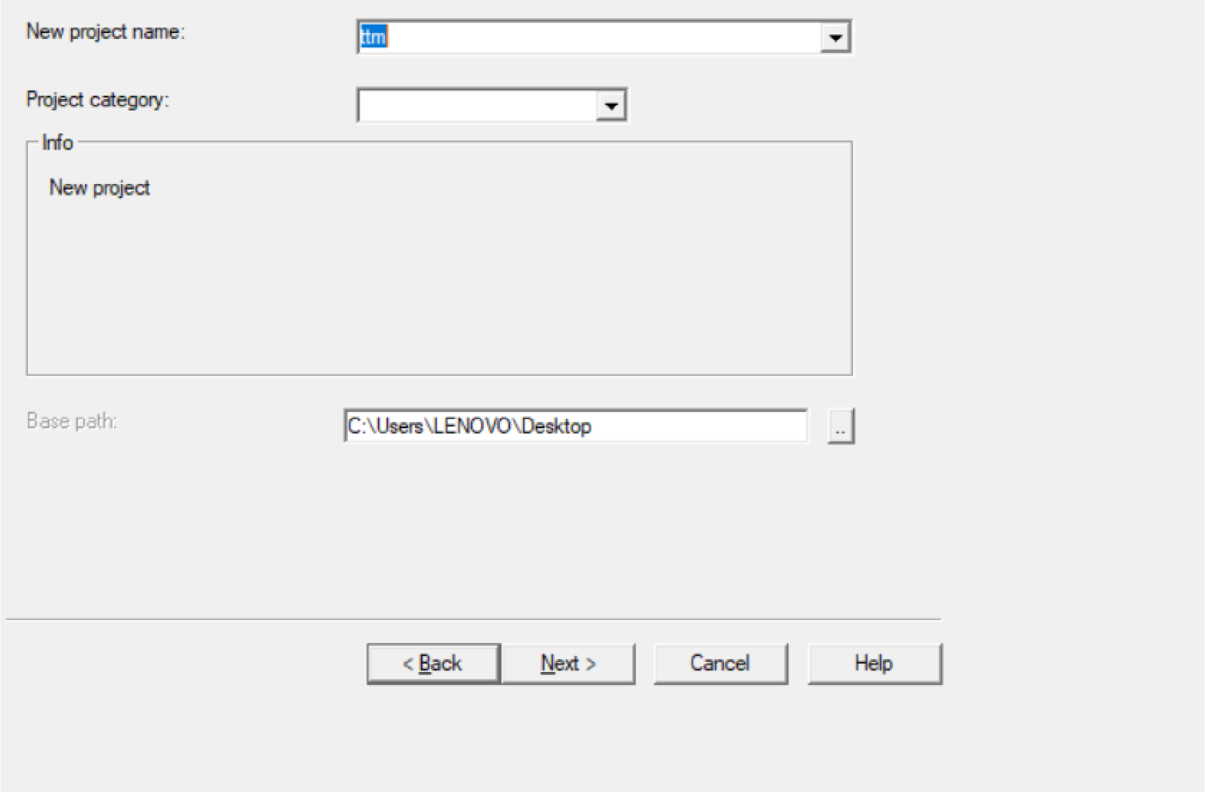
☑ Launch WinHTTrack Website Copier

☑ View history.txt file

install

How to perform httrack

Step1:-Open HTTrack and choose a project name. This will be the name of the folder containing your project. One project can include copies of multiple websites.



New project name: ttm

Project category:

Info

New project

Base path: C:\Users\LENOVO\Desktop

Click Next.

Step2:-

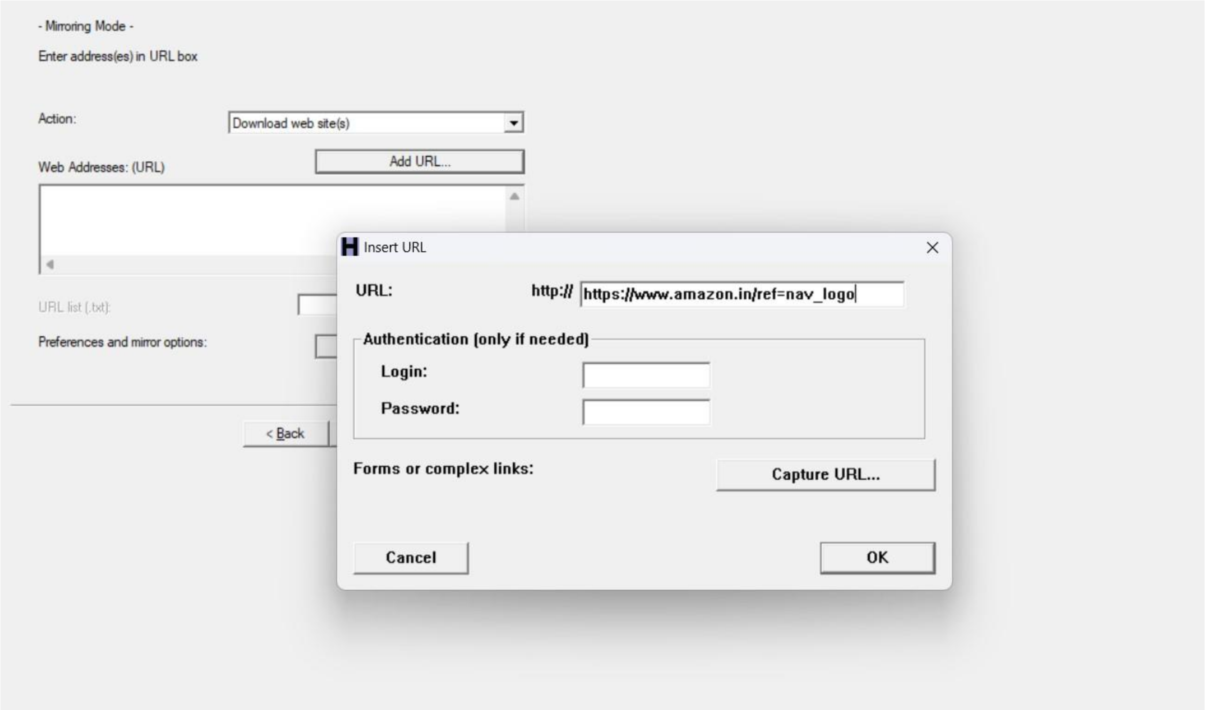
Select an action. Click the menu at the top, and choose the option that fits what you want to do. The most common options are:

- Chose **Download web site(s)** to mirror a website with its default options.

Choose **Download website(s) + questions** if you want to be prompted about links to download.[1]

Enter the URL(s) of the websites you want to mirror. If you're downloading multiple websites, place each URL on a separate line.

- You can click **Set options…** to choose other options, including certain file types to download or skip, recursion preferences, and the address of your proxy server.



- Mirroring Mode -

Enter address(es) in URL box

Action: Download web site(s)

Web Addresses: (URL)

URL list (.txt):

Preferences and mirror options:

Insert URL

URL: http:// https://www.amazon.in/ref=nav_logo

Authentication (only if needed)

Login:

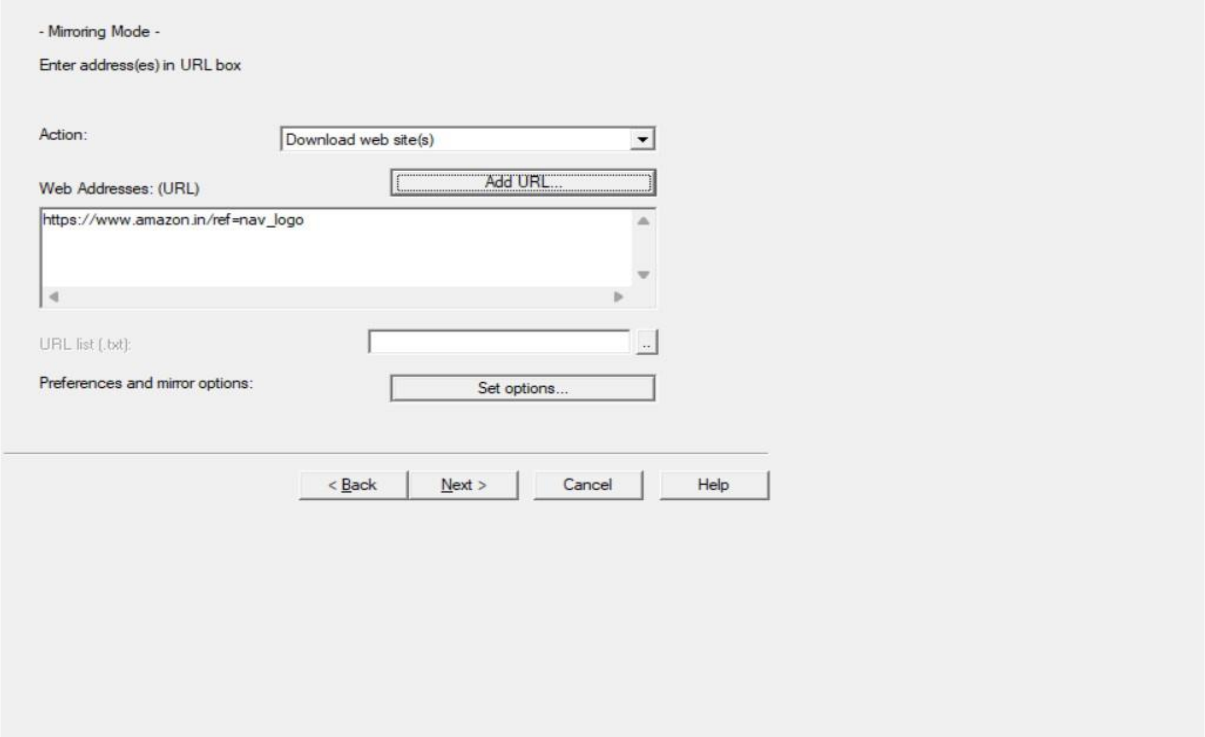
Password:

Forms or complex links:

Click ok

Step 3:-

Choose your final preferences and click Finish. If you want, you can choose options such as delaying the start of the downloading or disconnecting when finished first.



- Mirroring Mode -

Enter address(es) in URL box

Action: Download web site(s)

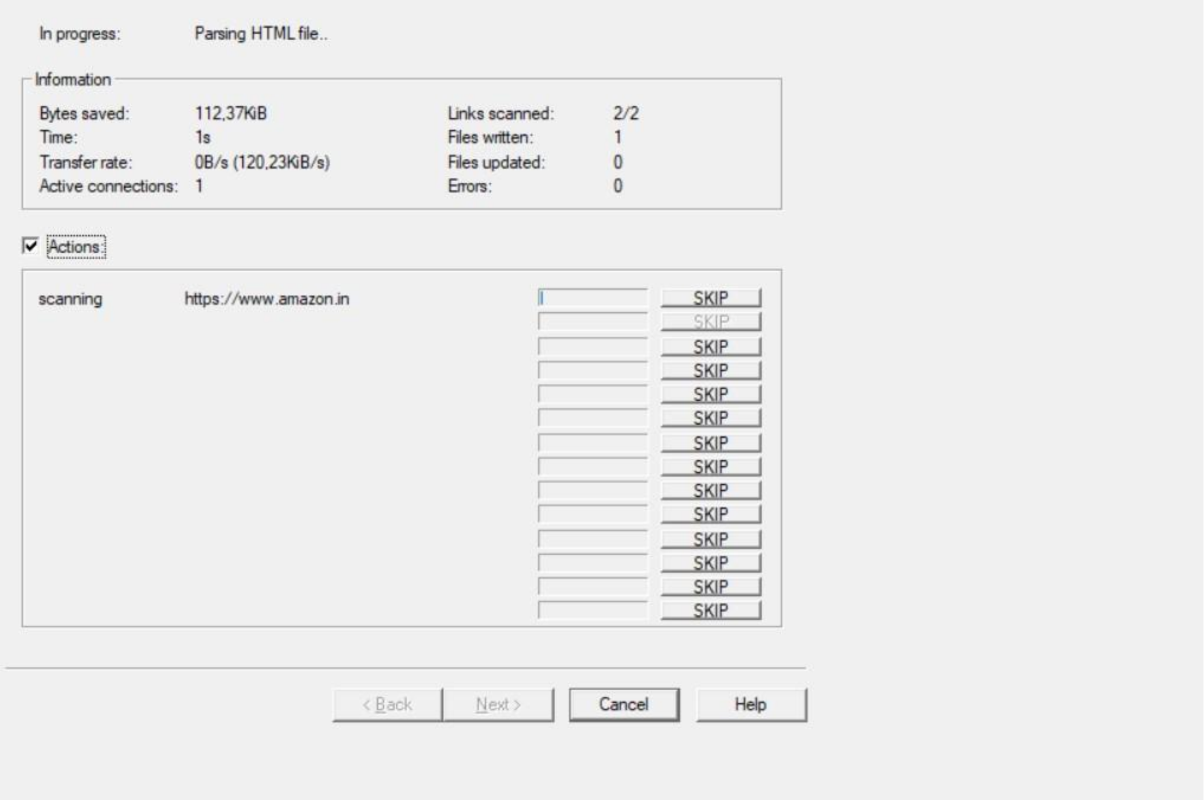
Web Addresses: (URL)

https://www.amazon.in/ref=nav_logo

URL list (.txt):

Preferences and mirror options:

Step4:- Watch the site(s) download in real time. HTTrack will now download the websites you entered with your preferred preferences.



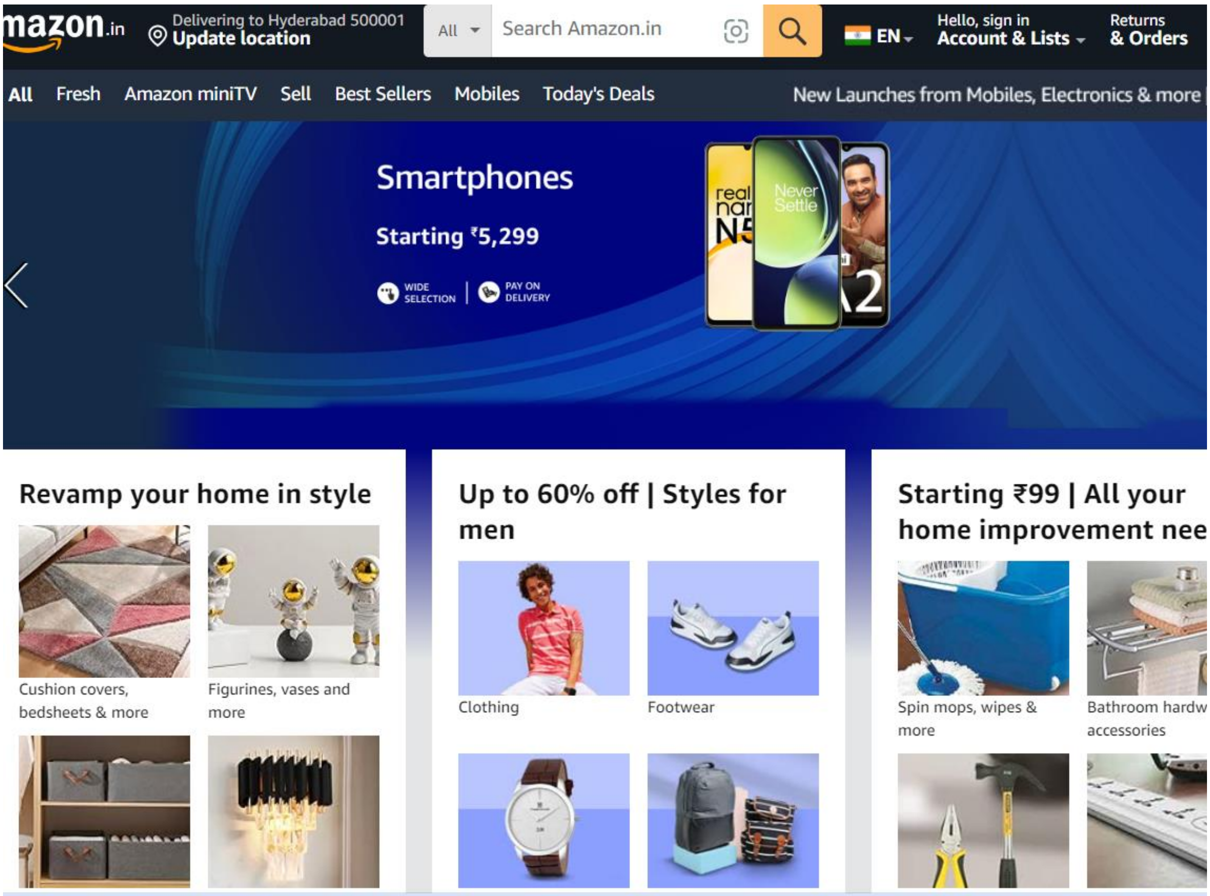
In progress: Parsing HTML file..

Information

Bytes saved:	112,37KiB	Links scanned:	2/2
Time:	1s	Files written:	1
Transfer rate:	0B/s (120,23KiB/s)	Files updated:	0
Active connections:	1	Errors:	0

☑ Actions

scanning https://www.amazon.in



Revamp your home in style

Cushion covers, bedsheets & more

Figurines, vases and more

Up to 60% off | Styles for men

Clothing

Footwear

Starting ₹99 | All your home improvement nee

Spin mops, wipes & more

Bathroom hardw accessories

Q 4:- use wireshark tool for packet capturing?

Ans:-

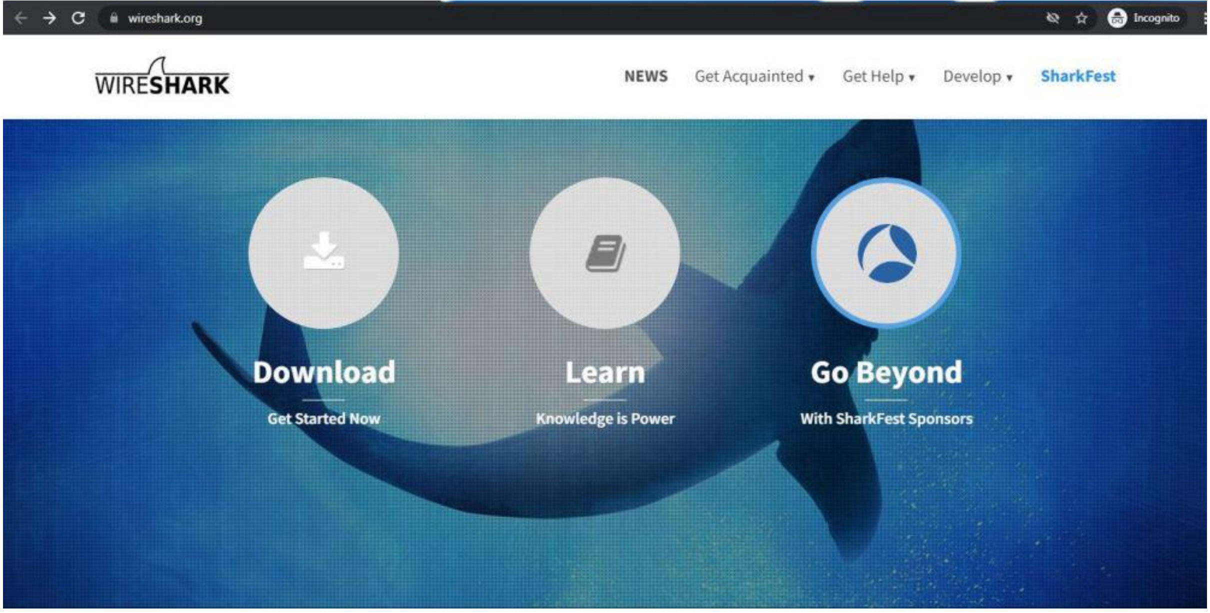
Wireshark is a widely-used network protocol analyzer. It allows users to capture and interactively browse the traffic running on a computer network. Here are some key points about Wireshark and why it's used

1. **Packet Analysis**: Captures and presents network packets in human-readable format.
2. **Protocol Analysis**: Supports a wide range of network protocols for detailed analysis.
3. **Troubleshooting**: Essential for diagnosing network issues like slow response times or packet loss.
4. **Security Analysis**: Detects network intrusions, analyzes malware traffic, and investigates security incidents.
5. **Network Monitoring**: Monitors network performance and usage, aiding in resource optimization and anomaly detection.
6. **Education and Training**: Used in educational settings to teach networking concepts and packet analysis techniques.
7. **Open Source**: Free and open-source under the GNU GPL, accessible to a broad user community for customization and extension

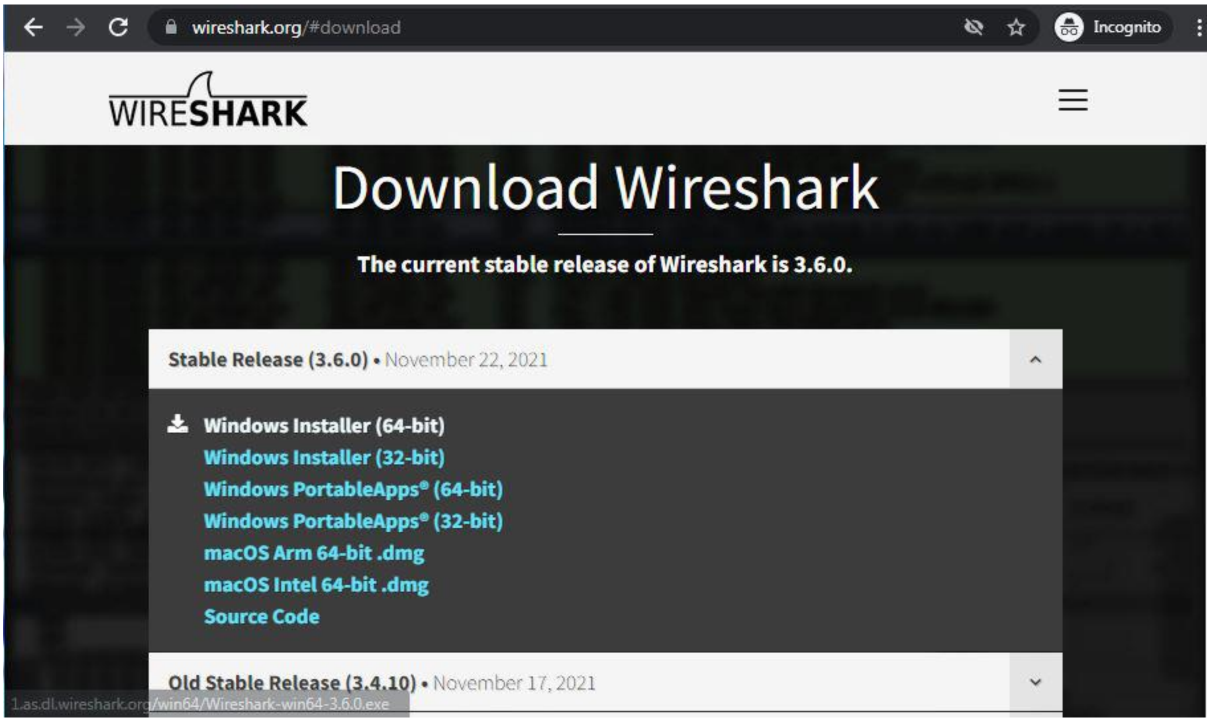
Installing Wireshark on Windows:

Follow the below steps to install Wireshark on Windows:

Step 1: Visit the official Wireshark website using any web browser.



Step 2: Click on Download, a new webpage will open with different installers of Wireshark.



Download Wireshark

The current stable release of Wireshark is 3.6.0.

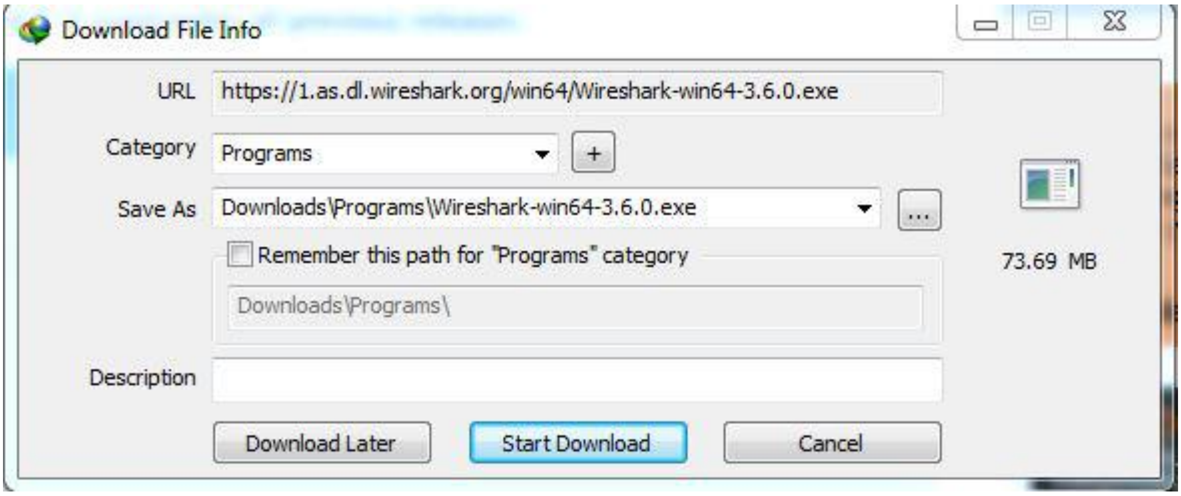
Stable Release (3.6.0) • November 22, 2021

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (64-bit)
- Windows PortableApps® (32-bit)
- macOS Arm 64-bit .dmg
- macOS Intel 64-bit .dmg
- Source Code

Old Stable Release (3.4.10) • November 17, 2021

1.as.dl.wireshark.org/win64/Wireshark-win64-3.6.0.exe

Step 3: Downloading of the executable file will start shortly. It is a small 73.69 MB file that will take some time.



Download File Info

URL https://1.as.dl.wireshark.org/win64/Wireshark-win64-3.6.0.exe

Category Programs

Save As Downloads\Programs\Wireshark-win64-3.6.0.exe

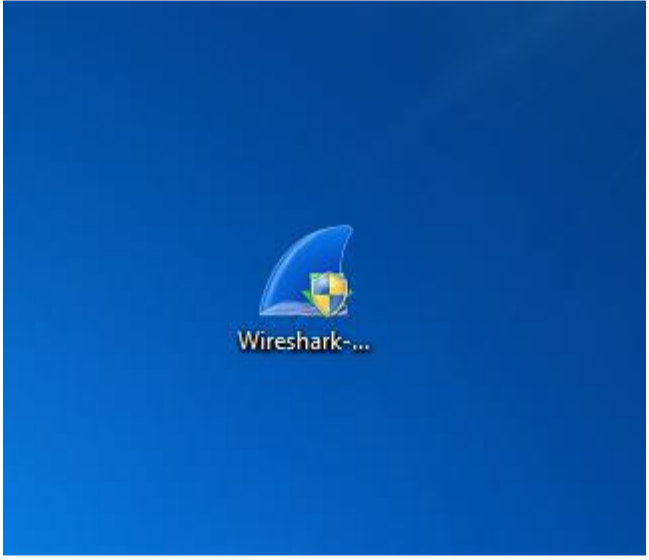
□ Remember this path for "Programs" category

Downloads\Programs\

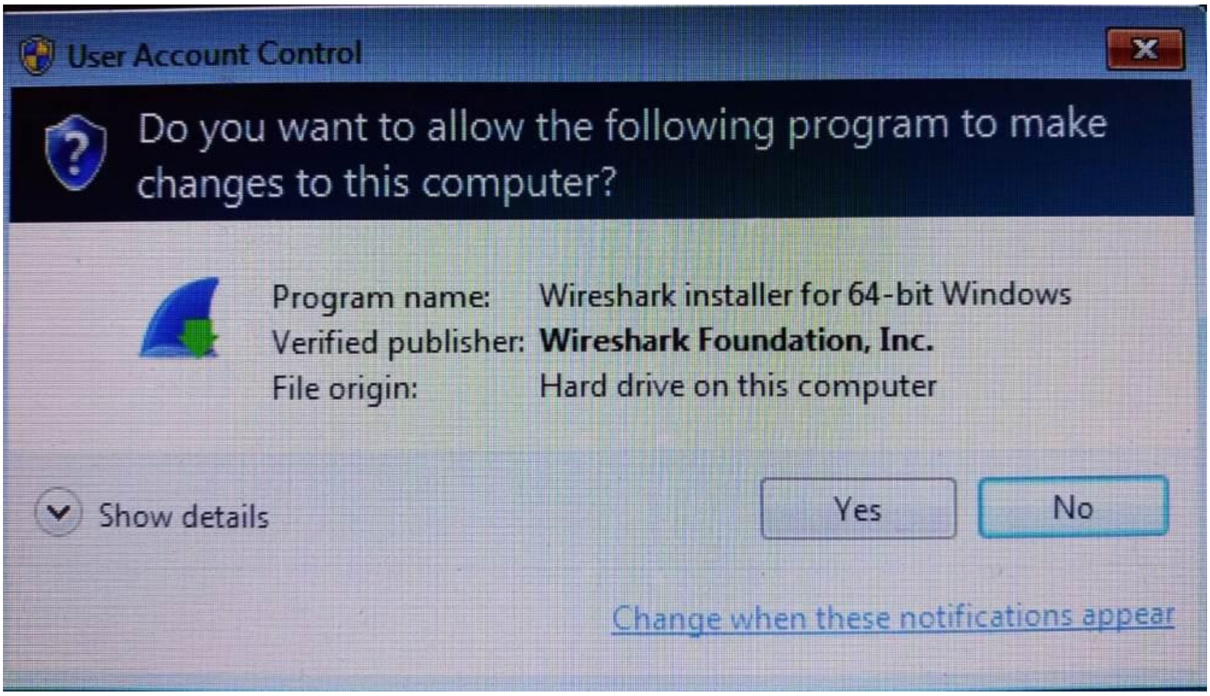
Description

73.69 MB

Step 4: Now check for the executable file in downloads in your system and run it.



Step 5: It will prompt confirmation to make changes to your system. Click on Yes.



User Account Control

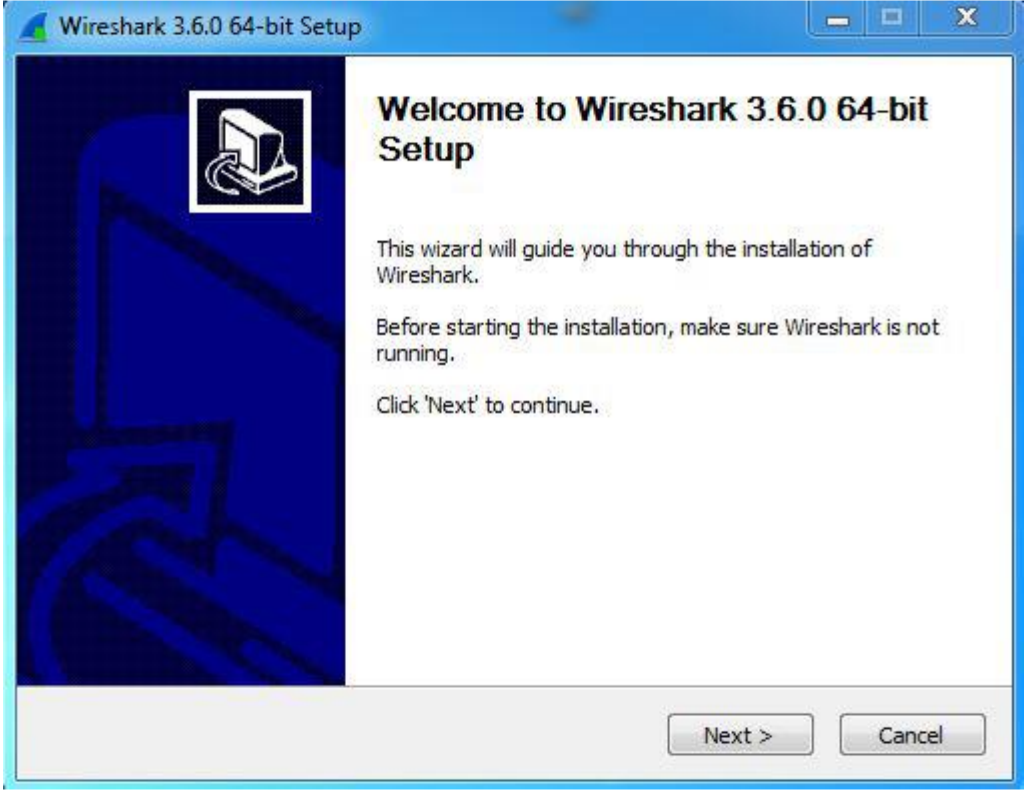
Do you want to allow the following program to make changes to this computer?

Program name: Wireshark installer for 64-bit Windows

Verified publisher: Wireshark Foundation, Inc.

File origin: Hard drive on this computer

Step 6: Setup screen will appear, click on Next.



Wireshark 3.6.0 64-bit Setup

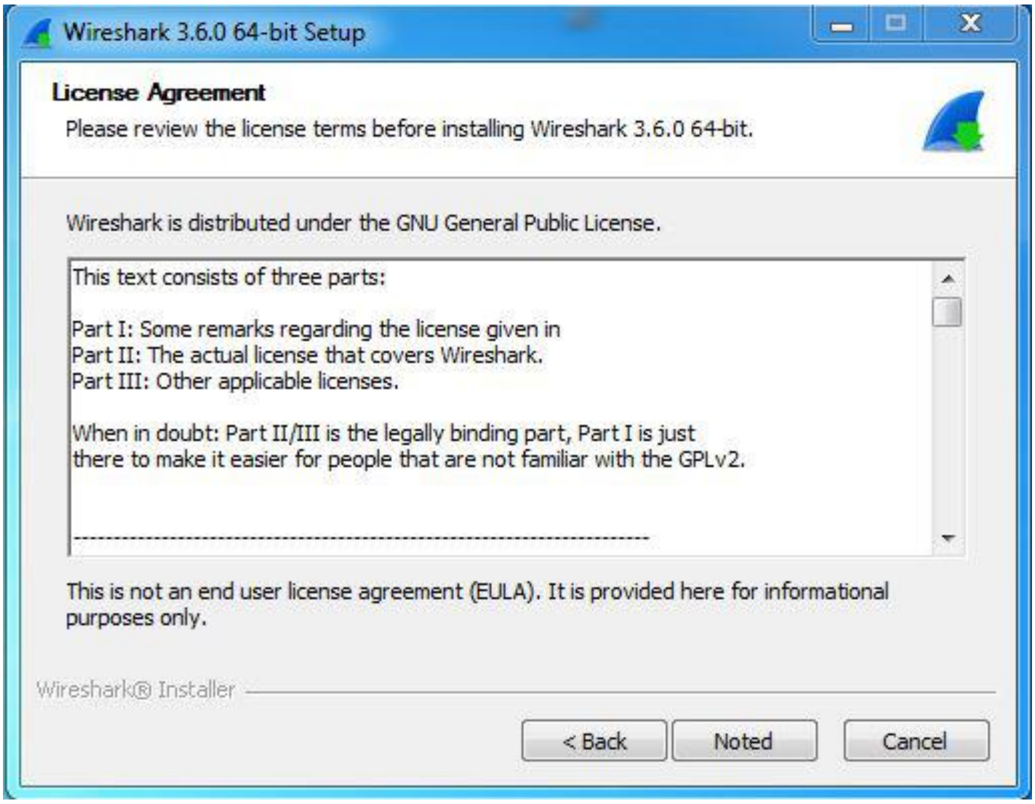
Welcome to Wireshark 3.6.0 64-bit Setup

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

Step 7: The next screen will be of License Agreement, click on Noted.



License Agreement

Please review the license terms before installing Wireshark 3.6.0 64-bit.

Wireshark is distributed under the GNU General Public License.

This text consists of three parts:

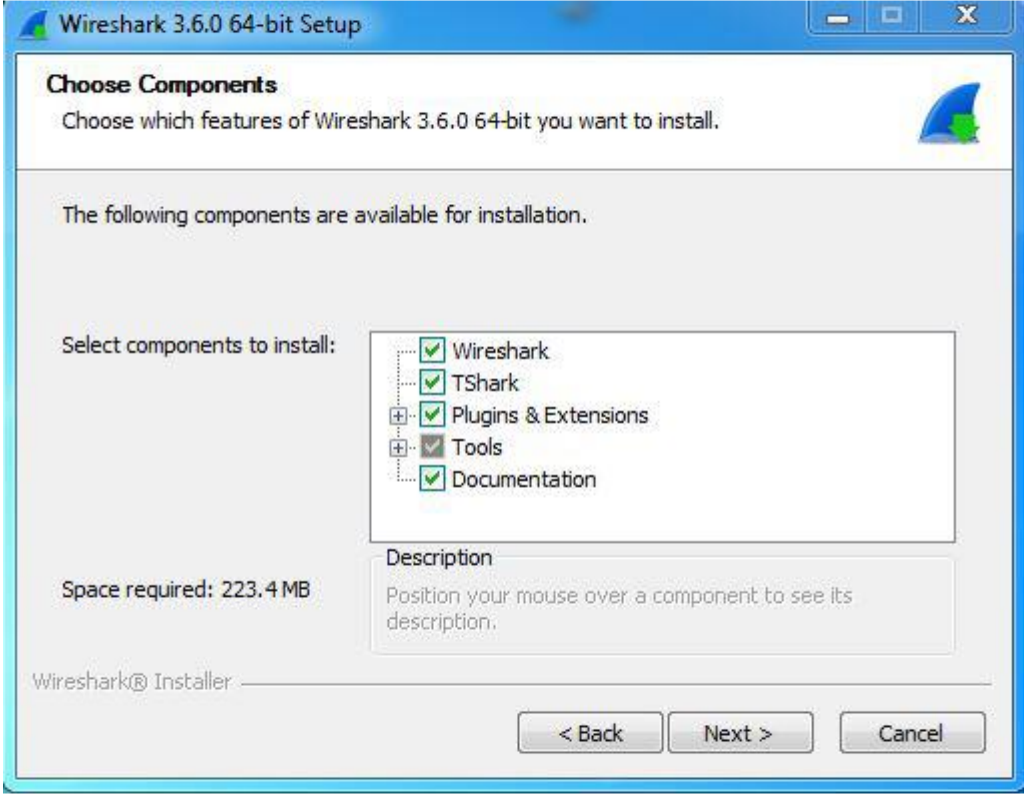
Part I: Some remarks regarding the license given in
Part II: The actual license that covers Wireshark.
Part III: Other applicable licenses.

When in doubt: Part II/III is the legally binding part, Part I is just
there to make it easier for people that are not familiar with the GPLv2.

This is not an end user license agreement (EULA). It is provided here for informational purposes only.

Wireshark® Installer

Step 8: This screen is for choosing components, all components are already marked so don't change anything just click on the Next button.



Choose Components

Choose which features of Wireshark 3.6.0 64-bit you want to install.

The following components are available for installation.

Select components to install:

- ☑ Wireshark
- ☑ TShark
- ☑ Plugins & Extensions
- ☑ Tools
- ☑ Documentation

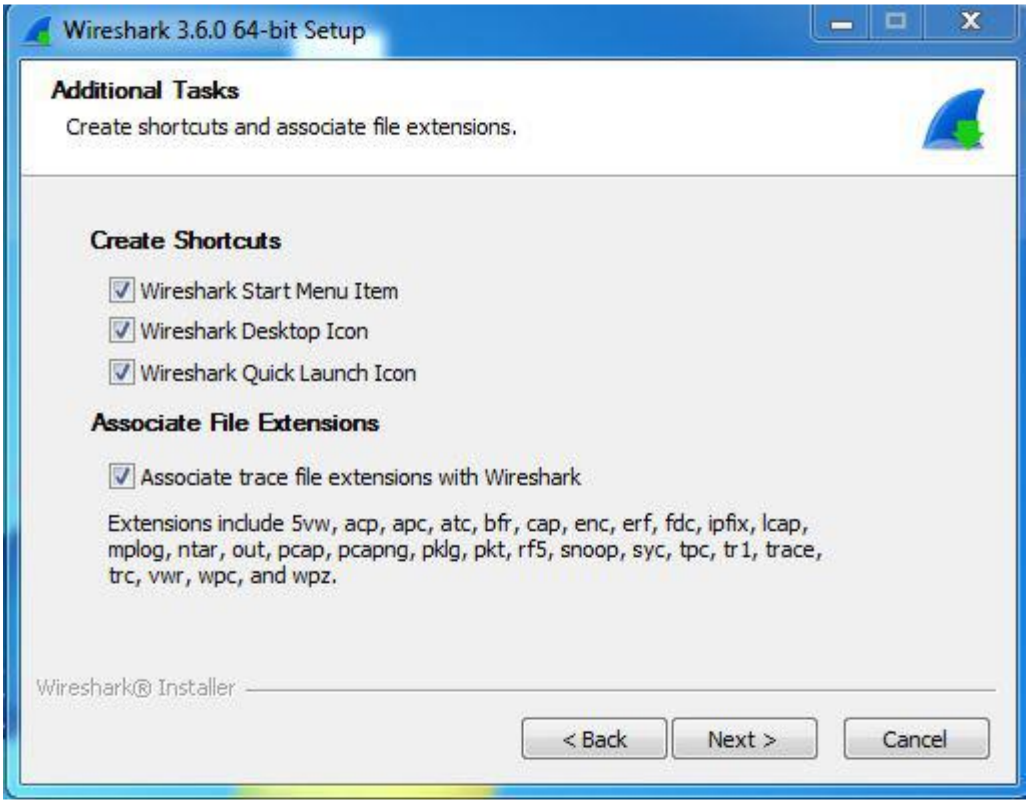
Space required: 223.4 MB

Description

Position your mouse over a component to see its description.

Wireshark® Installer

Step 9: This screen is of choosing shortcuts like start menu or desktop icon along with file extensions which can be intercepted by Wireshark, tick all boxes and click on Next button.



Wireshark 3.6.0 64-bit Setup

Additional Tasks

Create shortcuts and associate file extensions.

Create Shortcuts

☑ Wireshark Start Menu Item

☑ Wireshark Desktop Icon

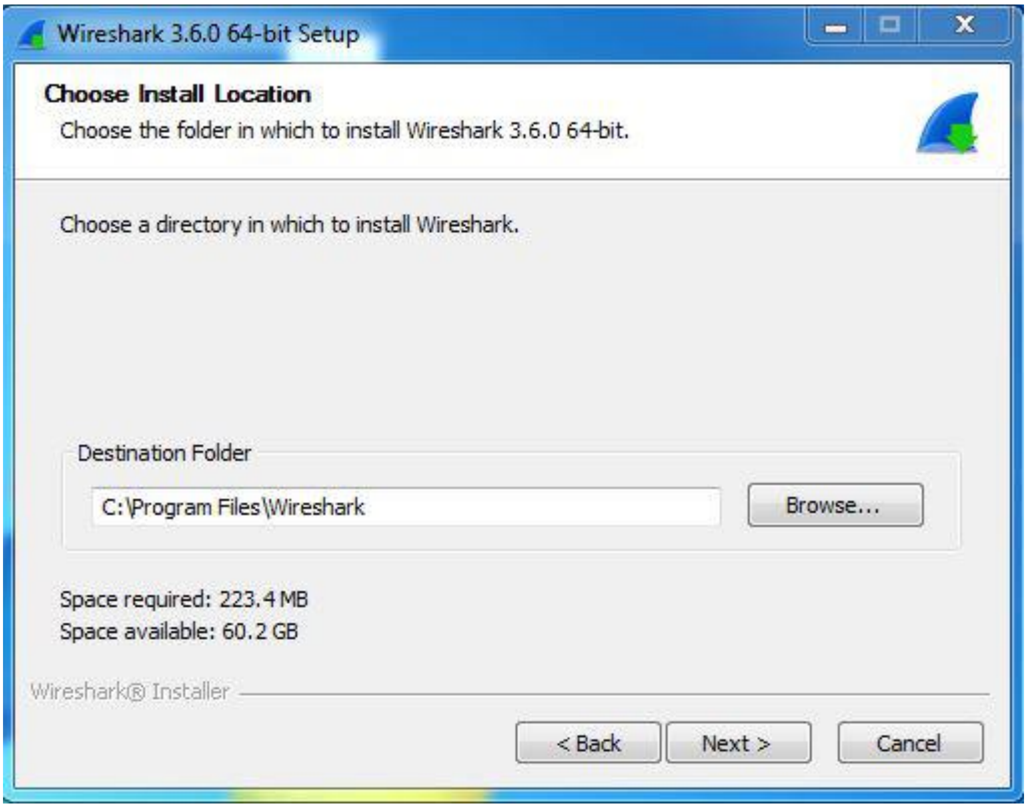
☑ Wireshark Quick Launch Icon

Associate File Extensions

☑ Associate trace file extensions with Wireshark

Extensions include 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, lcap, mplog, ntar, out, pcap, pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, and wpz.

Step 10: The next screen will be of installing location so choose the drive which will have sufficient memory space for installation. It needed only a memory space of 223.4 MB.



Wireshark 3.6.0 64-bit Setup

Choose Install Location

Choose the folder in which to install Wireshark 3.6.0 64-bit.

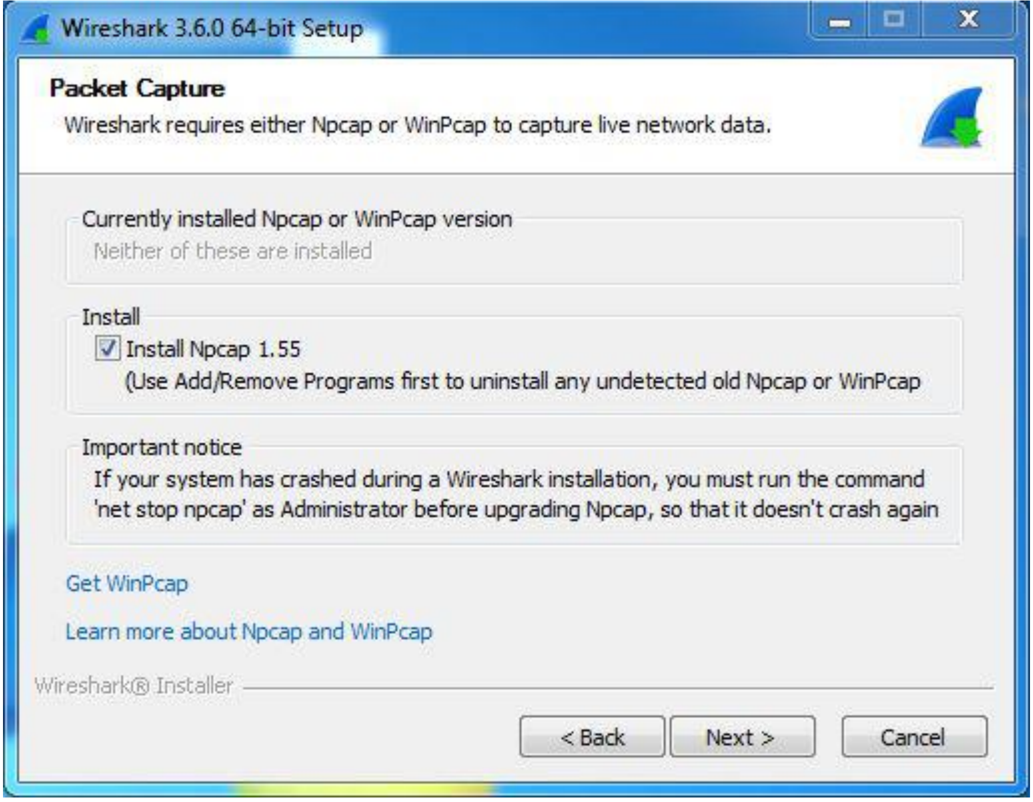
Choose a directory in which to install Wireshark.

Destination Folder: C:\Program Files\Wireshark

Space required: 223.4 MB

Space available: 60.2 GB

Step 11: Next screen has an option to install Npcap which is used with Wireshark to capture packets *pcap* means packet capture so the install option is already checked don't change anything and click the next button.



Wireshark 3.6.0 64-bit Setup

Packet Capture

Wireshark requires either Npcap or WinPcap to capture live network data.

Currently installed Npcap or WinPcap version

Neither of these are installed

Install

☑ Install Npcap 1.55

(Use Add/Remove Programs first to uninstall any undetected old Npcap or WinPcap

Important notice

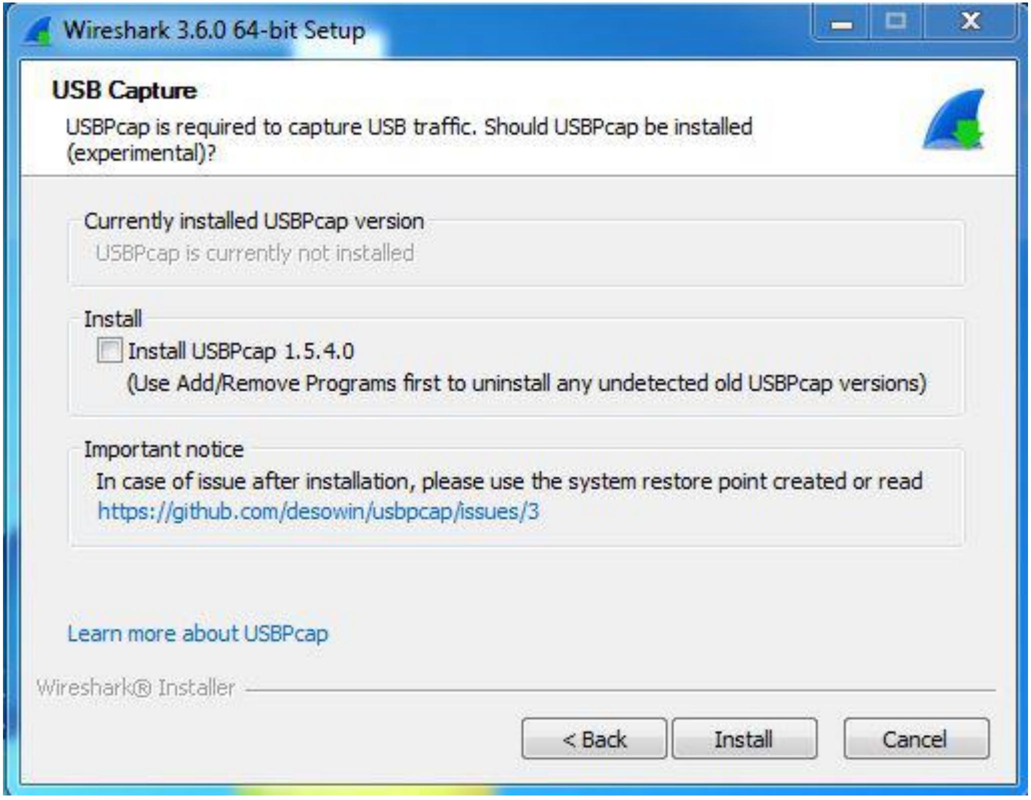
If your system has crashed during a Wireshark installation, you must run the command 'net stop npcap' as Administrator before upgrading Npcap, so that it doesn't crash again

Get WinPcap

Learn more about Npcap and WinPcap

Wireshark® Installer

Step 12: Next screen is about USB network capturing so it is one's choice to use it or not, click on Install.



Wireshark 3.6.0 64-bit Setup

USB Capture

USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?

Currently installed USBPcap version

USBPcap is currently not installed

Install

□ Install USBPcap 1.5.4.0

(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)

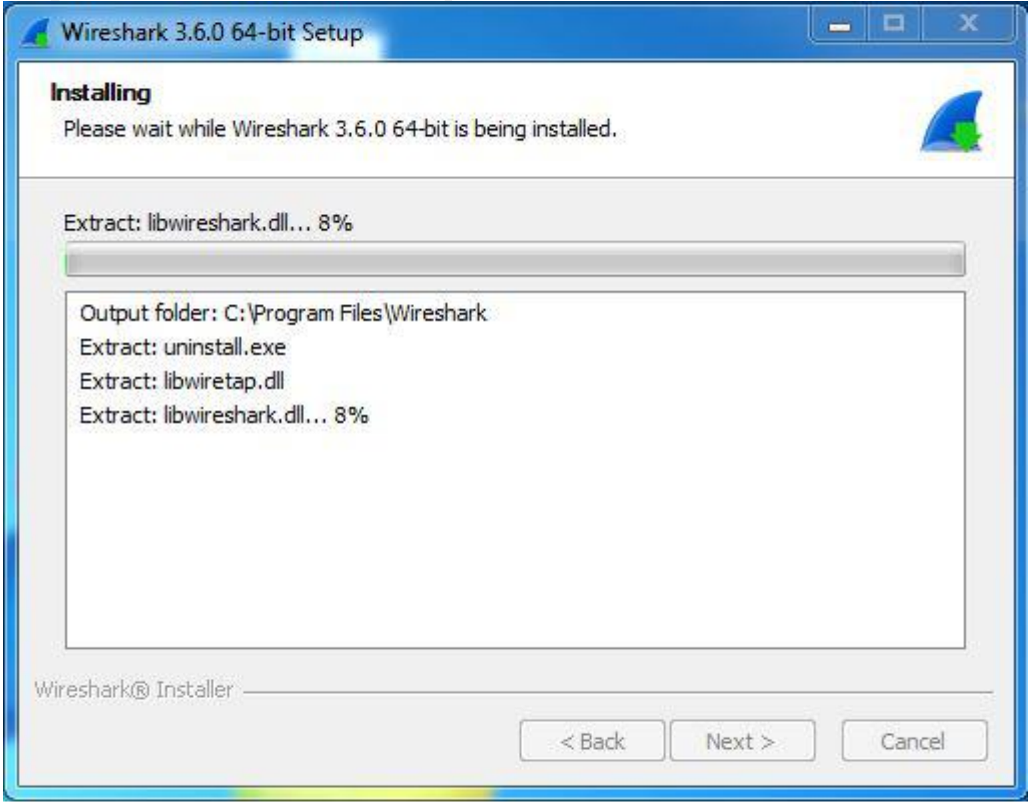
Important notice

In case of issue after installation, please use the system restore point created or read https://github.com/desowin/usbpcap/issues/3

Learn more about USBPcap

Wireshark® Installer

Step 13: After this installation process will start.



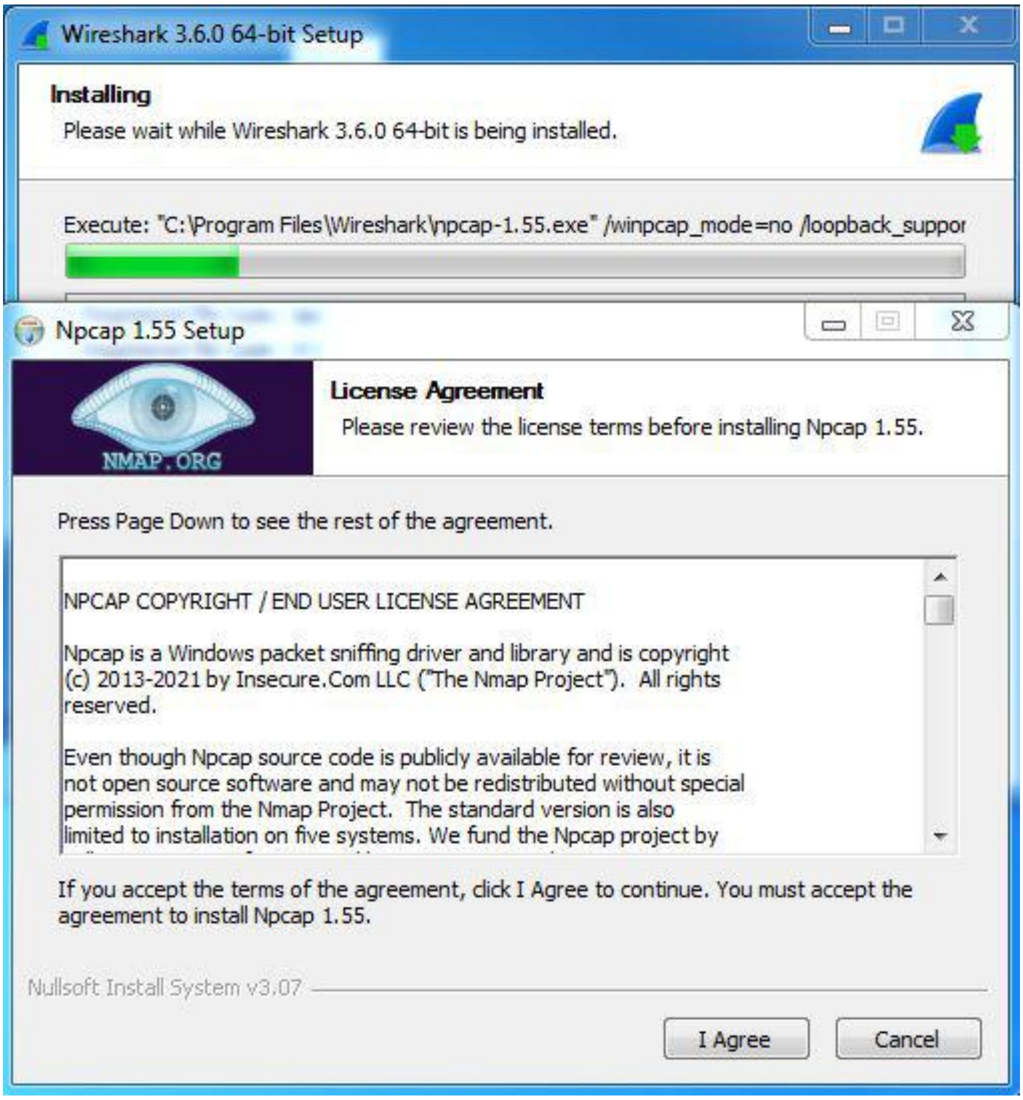
Installing

Please wait while Wireshark 3.6.0 64-bit is being installed.

Extract: libwireshark.dll... 8%

```
Output folder: C:\Program Files\Wireshark
Extract: uninstall.exe
Extract: libwiretap.dll
Extract: libwireshark.dll... 8%
```

Step 14: This installation will prompt for Npcap installation as already checked so the license agreement of Npcap will appear to click on the *I Agree* button.


Wireshark 3.6.0 64-bit Setup
Installing
Please wait while Wireshark 3.6.0 64-bit is being installed.

Execute: "C:\Program Files\Wireshark\npcap-1.55.exe" /winpcap_mode=no /loopback_suppor

Npcap 1.55 Setup
NMAP.ORG
License Agreement
Please review the license terms before installing Npcap 1.55.
Press Page Down to see the rest of the agreement.

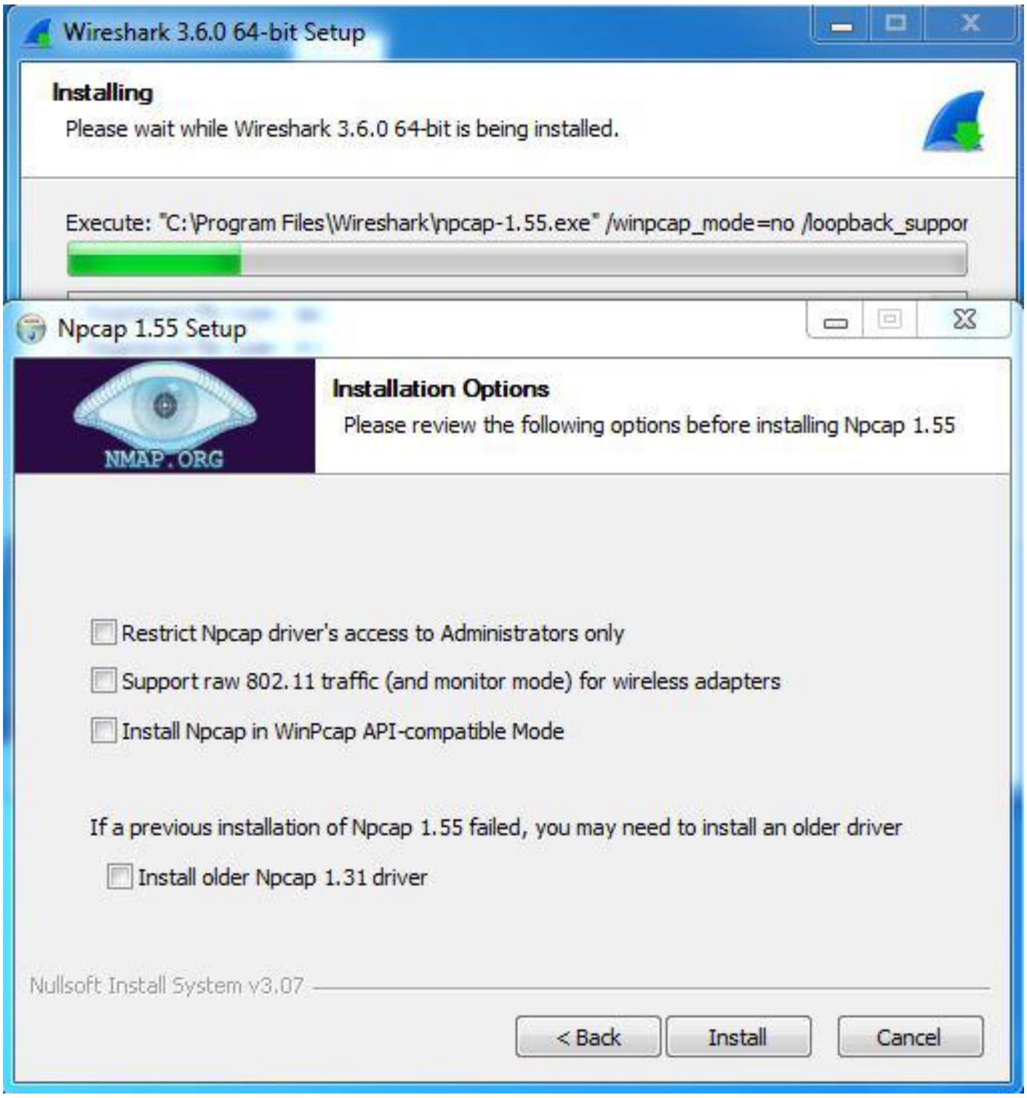
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT

Npcap is a Windows packet sniffing driver and library and is copyright (c) 2013-2021 by Insecure.Com LLC ("The Nmap Project"). All rights reserved.

Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed without special permission from the Nmap Project. The standard version is also limited to installation on five systems. We fund the Npcap project by

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 1.55.

Step 15: Next screen is about different installing options of *npcap*, don’t do anything click on Install.



Installing

Please wait while Wireshark 3.6.0 64-bit is being installed.

Execute: "C:\Program Files\Wireshark\npcap-1.55.exe" /winpcap_mode=no /loopback_suppor

Installation Options

Please review the following options before installing Npcap 1.55

□ Restrict Npcap driver's access to Administrators only

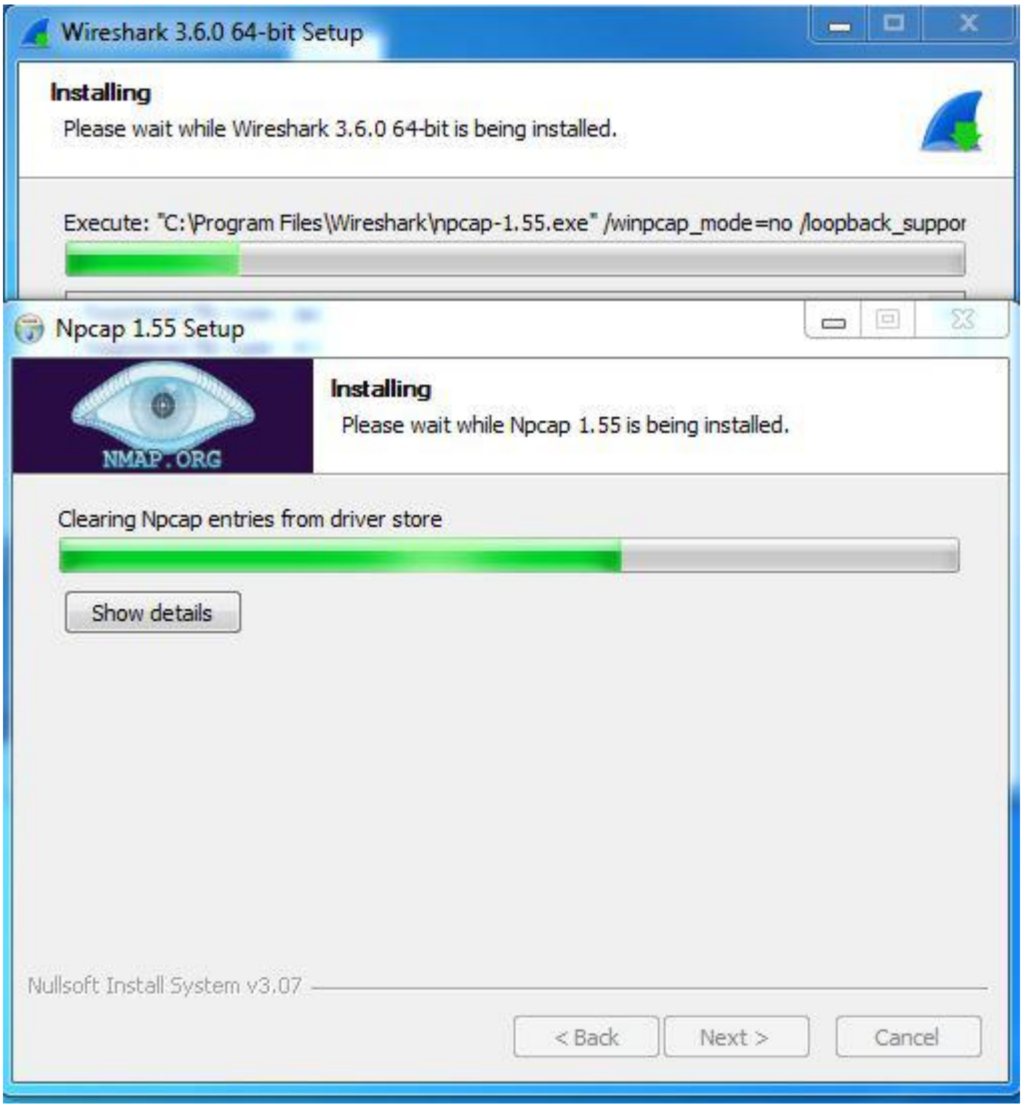
□ Support raw 802.11 traffic (and monitor mode) for wireless adapters

□ Install Npcap in WinPcap API-compatible Mode

If a previous installation of Npcap 1.55 failed, you may need to install an older driver

□ Install older Npcap 1.31 driver

Step 16: After this installation process will start which will take only a minute.



Wireshark 3.6.0 64-bit Setup

Installing

Please wait while Wireshark 3.6.0 64-bit is being installed.

Execute: "C:\Program Files\Wireshark\npcap-1.55.exe" /winpcap_mode=no /loopback_suppor

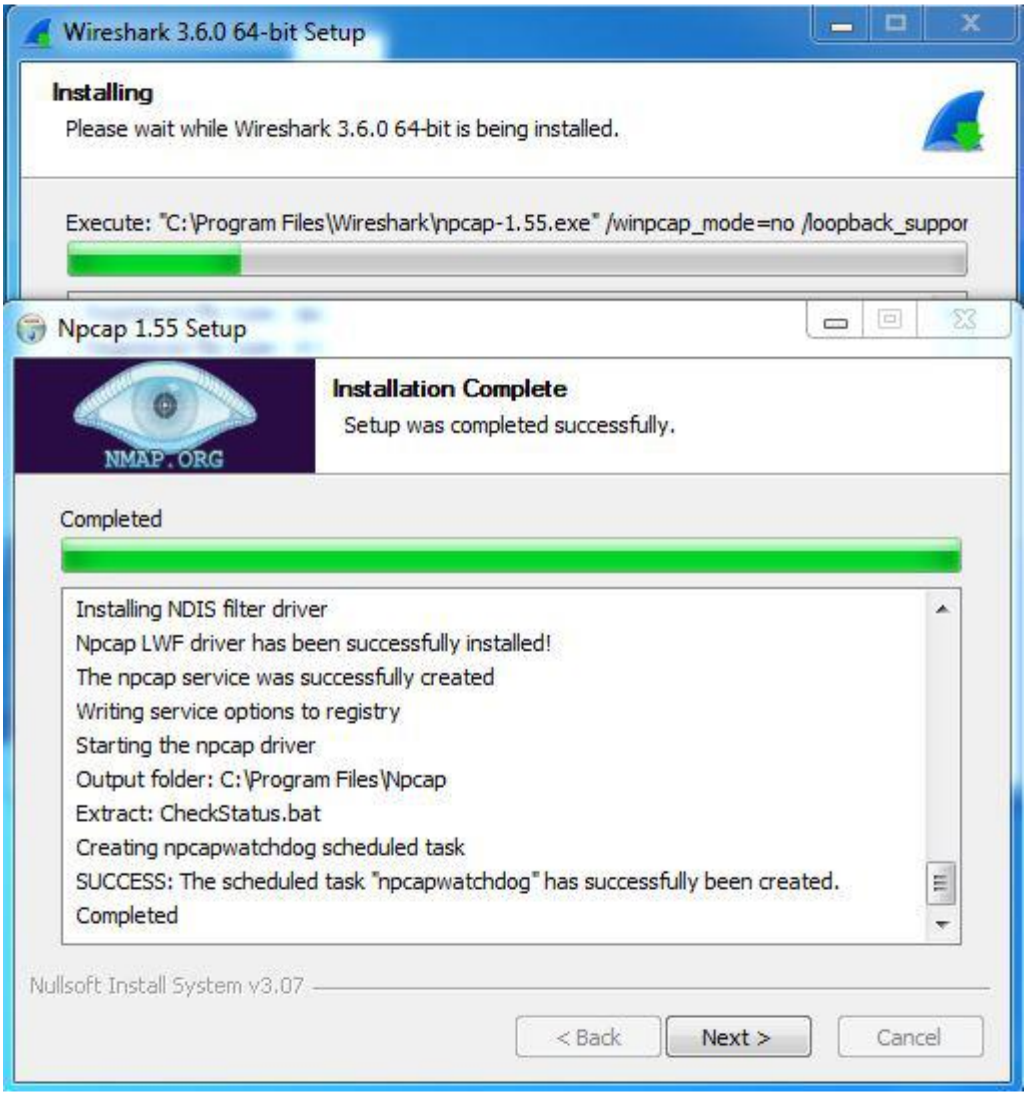
Npcap 1.55 Setup

Installing

Please wait while Npcap 1.55 is being installed.

Clearing Npcap entries from driver store

Step 17: After this installation process will complete click on the Next button.

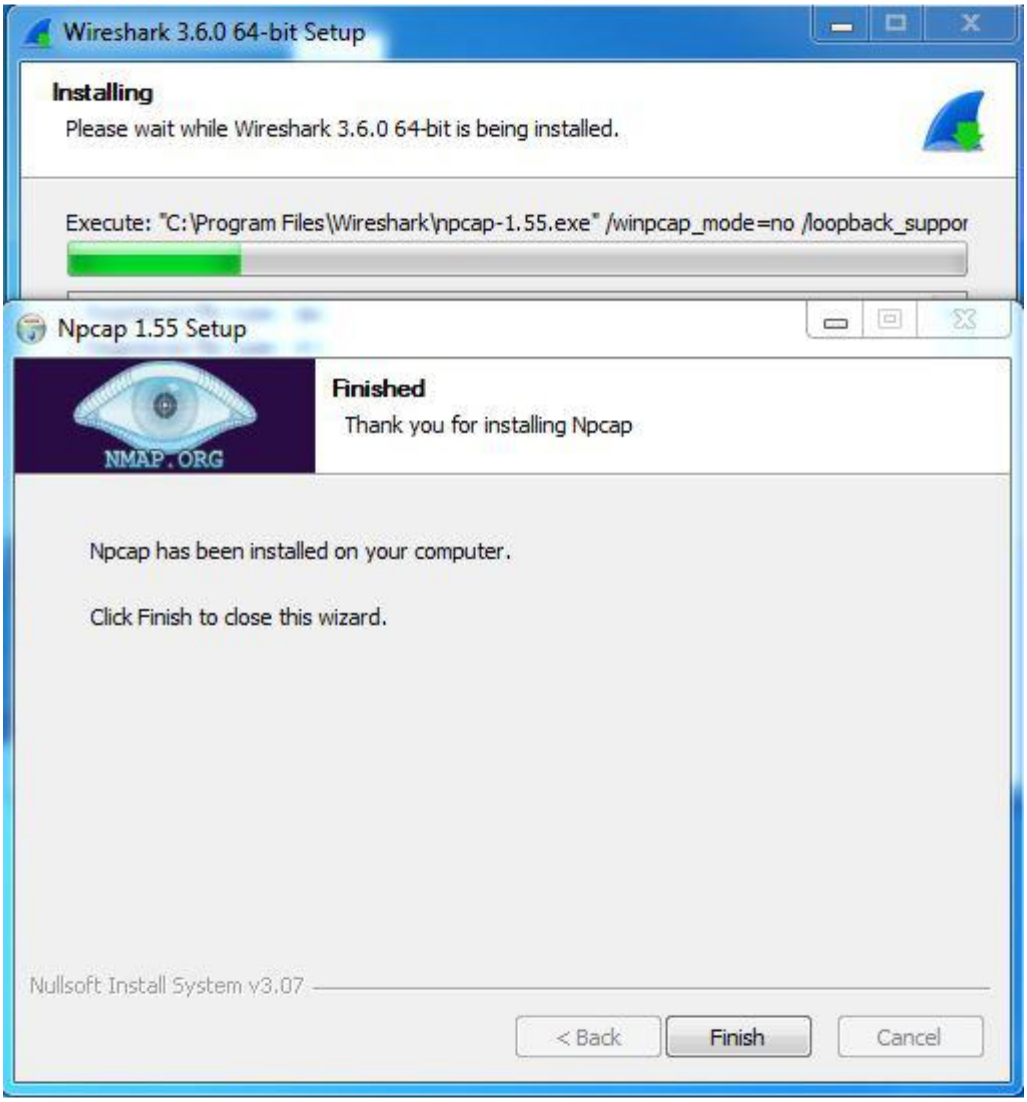


Wireshark 3.6.0 64-bit Setup
Installing
Please wait while Wireshark 3.6.0 64-bit is being installed.
Npcap 1.55 Setup
NMAP.ORG
Installation Complete
Setup was completed successfully.
Completed
Nullsoft Install System v3.07
< Back
Next >
Cancel

```
Execute: "C:\Program Files\Wireshark\npcap-1.55.exe" /winpcap_mode=no /loopback_suppor
```

```
Installing NDIS filter driver
Npcap LWF driver has been successfully installed!
The npcap service was successfully created
Writing service options to registry
Starting the npcap driver
Output folder: C:\Program Files\Npcap
Extract: CheckStatus.bat
Creating npcapwatchdog scheduled task
SUCCESS: The scheduled task "npcapwatchdog" has successfully been created.
Completed
```

Step 18: Click on Finish after the installation process is complete.



Wireshark 3.6.0 64-bit Setup

Installing

Please wait while Wireshark 3.6.0 64-bit is being installed.

Execute: "C:\Program Files\Wireshark\npcap-1.55.exe" /winpcap_mode=no /loopback_suppor

Npcap 1.55 Setup

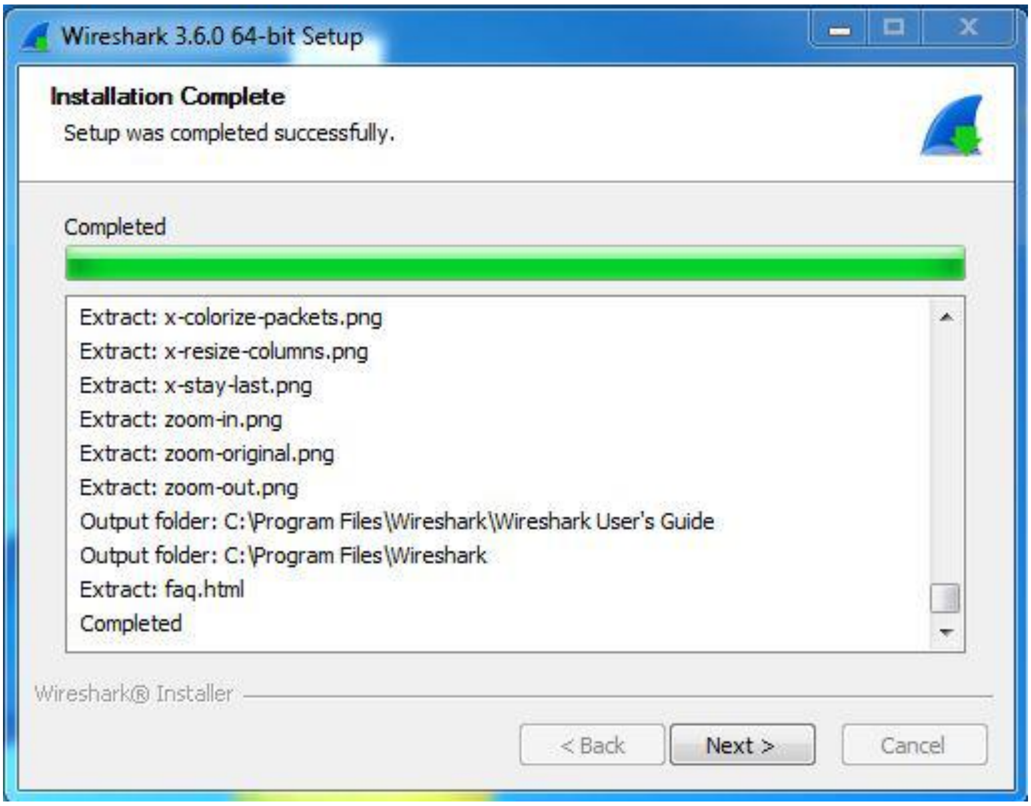
Finished

Thank you for installing Npcap

Npcap has been installed on your computer.

Click Finish to close this wizard.

Step 19: After this installation process of Wireshark will complete click on the Next button.



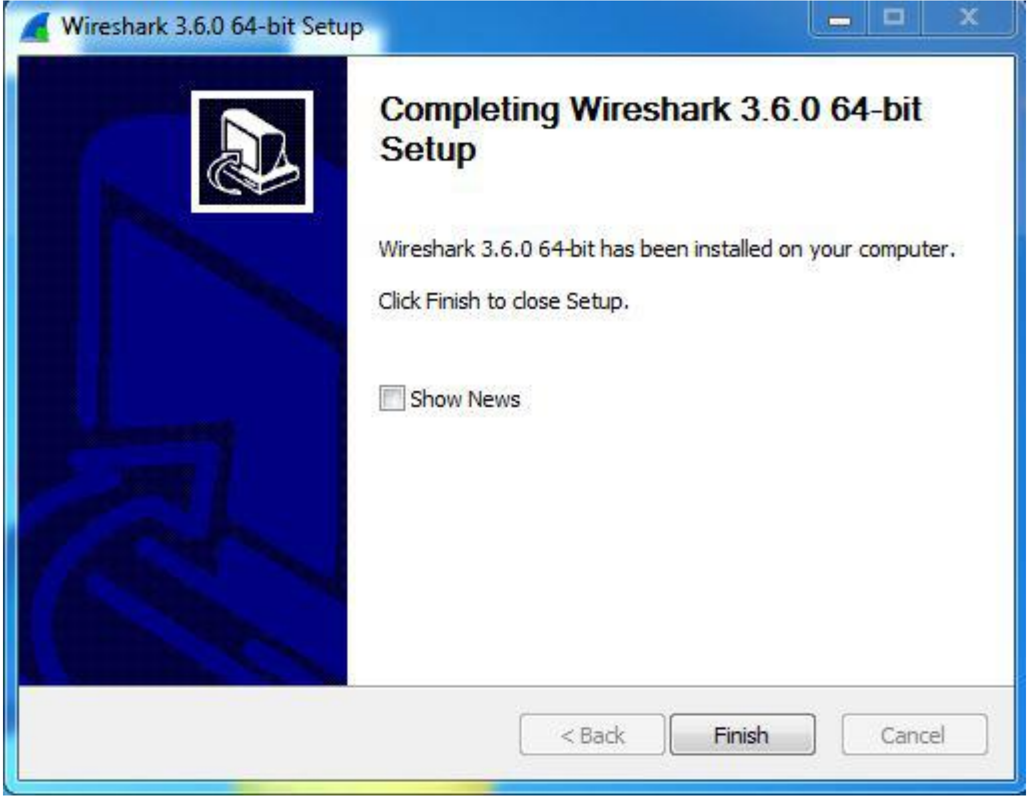
Installation Complete

Setup was completed successfully.

Completed

```
Extract: x-colorize-packets.png
Extract: x-resize-columns.png
Extract: x-stay-last.png
Extract: zoom-in.png
Extract: zoom-original.png
Extract: zoom-out.png
Output folder: C:\Program Files\Wireshark\Wireshark User's Guide
Output folder: C:\Program Files\Wireshark
Extract: faq.html
Completed
```

Step 20: Click on Finish after the installation process of Wireshark is complete.



Completing Wireshark 3.6.0 64-bit Setup

Wireshark 3.6.0 64-bit has been installed on your computer.

Click Finish to close Setup.

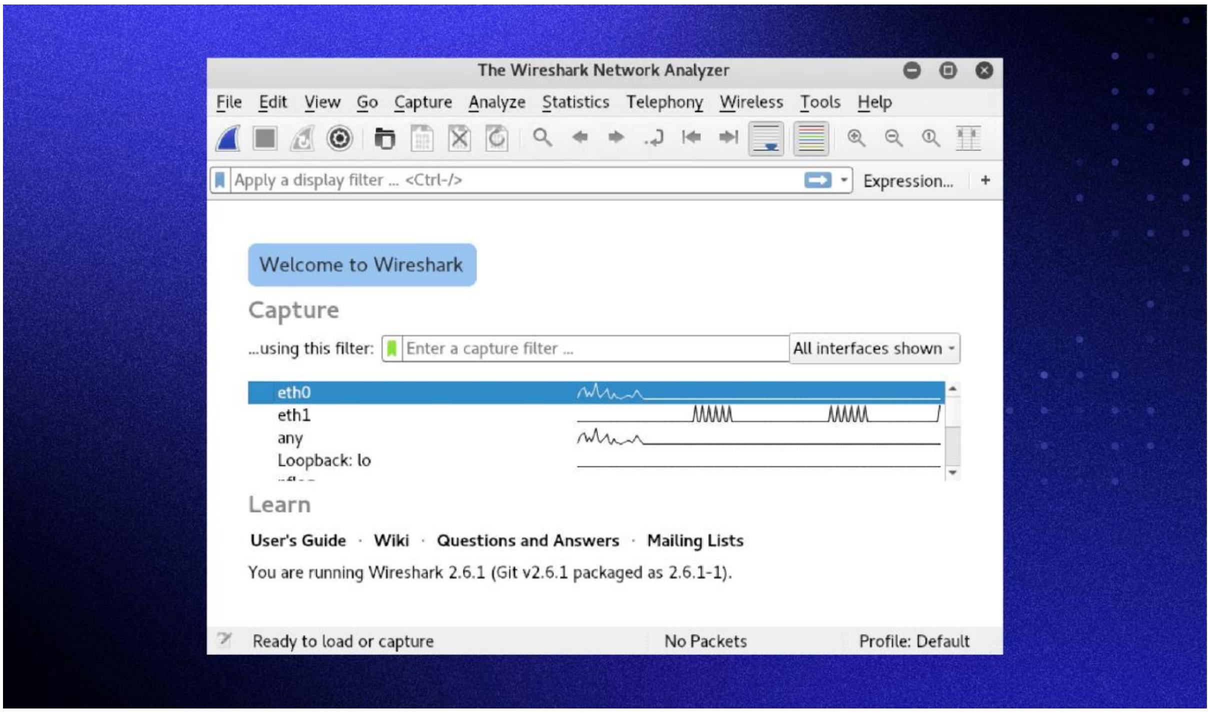
□ Show News

Wireshark is successfully installed on the system and an icon is created on the desktop as shown below:

Now run the software and see the interface.

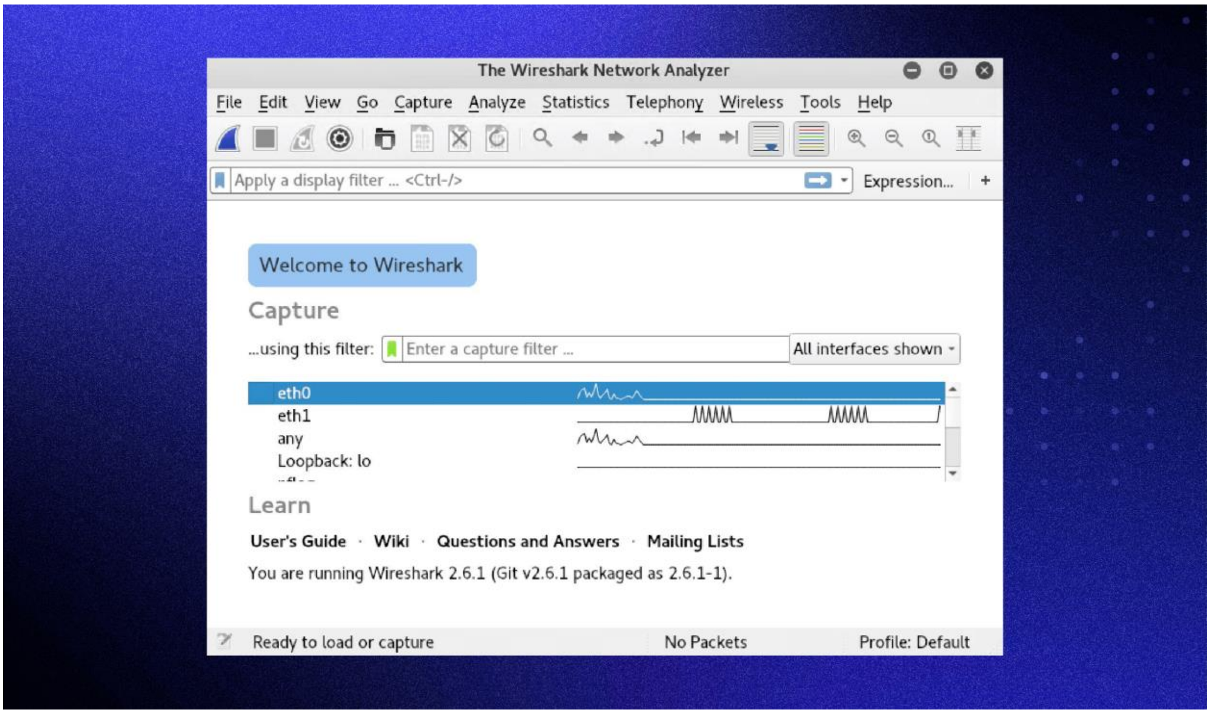
Congratulations!! At this point, you have successfully installed Wireshark on your windows system.

Perform wireshark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
eth1
any
Loopback: lo
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Ready to load or capture
No Packets
Profile: Default

You are running Wireshark 2.6.1 (Git v2.6.1 packaged as 2.6.1-1).

When you open Wireshark, you see a screen showing you a list of all the network connections you can monitor. You also have a capture filter field to only capture the network traffic you want to see.

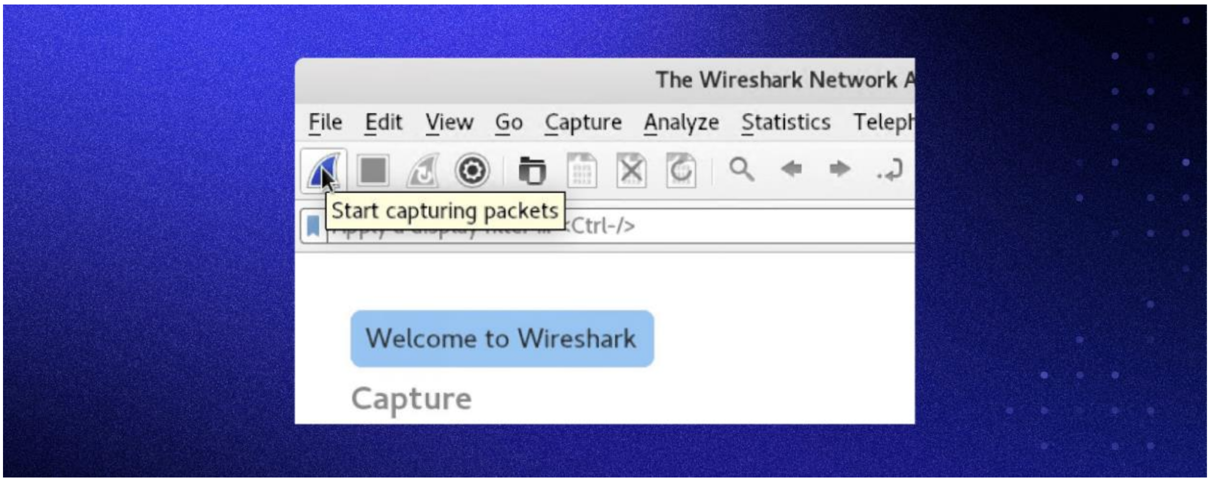

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
eth1
any
Loopback: lo
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.6.1 (Git v2.6.1 packaged as 2.6.1-1).

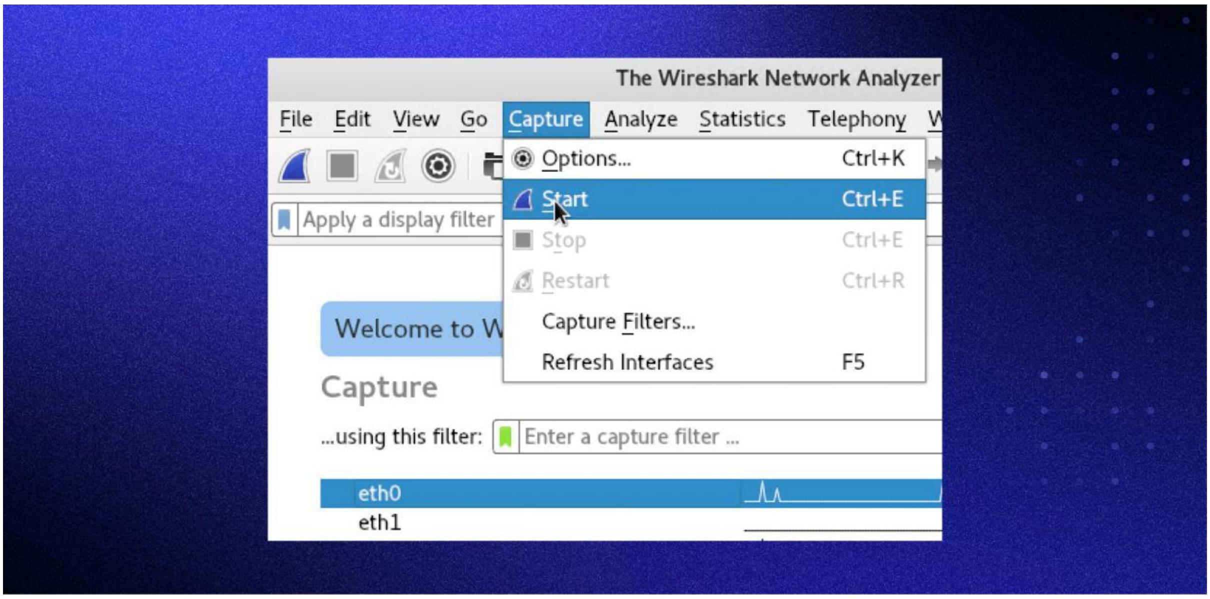
Ready to load or capture | No Packets | Profile: Default

You can select one or more of the network interfaces using shift+left-click. Once select the network interface, you can start the capture, and there are several ways to do that.

Click the first button on the toolbar, titled “Start capturing packets.”

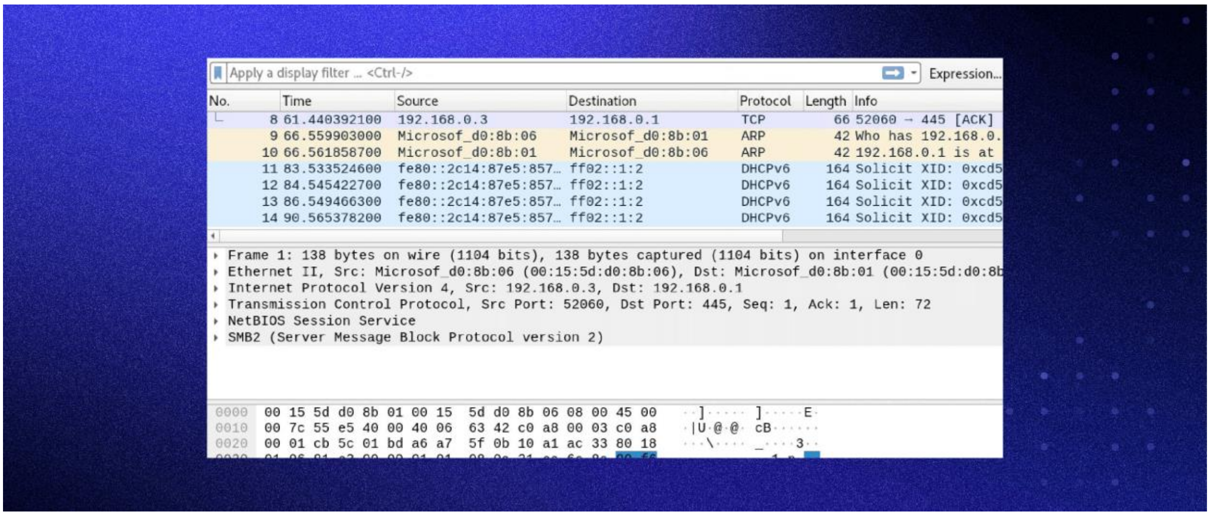


You can select the menu item Capture -> Start.



Or you could use the keystroke Control+E.

During the capture, Wireshark will show you the packets captured in real-time.



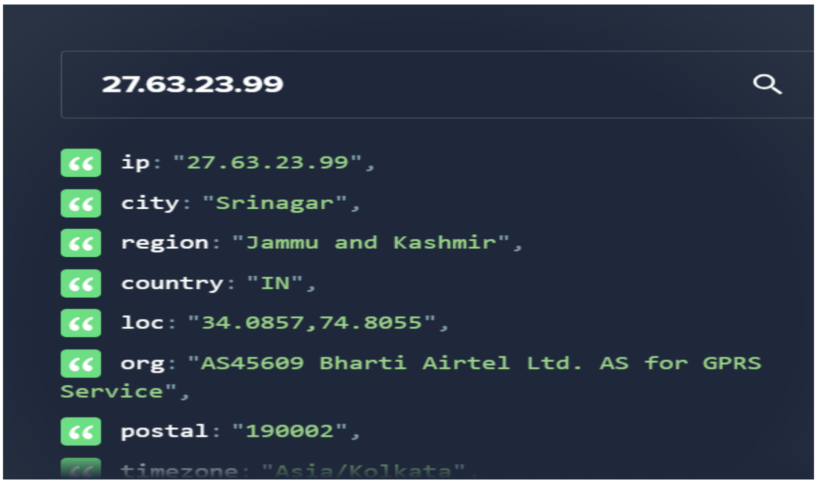
```
No.      Time          Source                 Destination        Protocol  Length Info
      8 61.440392100  192.168.0.3            192.168.0.1        TCP          66 52060 → 445 [ACK]
      9 66.559903000  Microsof_d0:8b:06      Microsof_d0:8b:01  ARP          42 Who has 192.168.0.
     10 66.561858700  Microsof_d0:8b:01      Microsof_d0:8b:06  ARP          42 192.168.0.1 is at
     11 83.533524600  fe80::2c14:87e5:857…   ff02::1:2          DHCPv6      164 Solicit XID: 0xcd5
     12 84.545422700  fe80::2c14:87e5:857…   ff02::1:2          DHCPv6      164 Solicit XID: 0xcd5
     13 86.549466300  fe80::2c14:87e5:857…   ff02::1:2          DHCPv6      164 Solicit XID: 0xcd5
     14 90.565378200  fe80::2c14:87e5:857…   ff02::1:2          DHCPv6      164 Solicit XID: 0xcd5

› Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
› Ethernet II, Src: Microsof_d0:8b:06 (00:15:5d:d0:8b:06), Dst: Microsof_d0:8b:01 (00:15:5d:d0:8b
› Internet Protocol Version 4, Src: 192.168.0.3, Dst: 192.168.0.1
› Transmission Control Protocol, Src Port: 52060, Dst Port: 445, Seq: 1, Ack: 1, Len: 72
› NetBIOS Session Service
› SMB2 (Server Message Block Protocol version 2)

0000  00 15 5d d0 8b 01 00 15  5d d0 8b 06 08 00 45 00   ··]····· ]·····E·
0010  00 7c 55 e5 40 00 40 06  63 42 c0 a8 00 03 c0 a8   ·|U·@·@· cB······
0020  00 01 cb 5c 01 bd a6 a7  5f 0b 10 a1 ac 33 80 18   ···\···· _····3··
```

Once you have captured all the packets needed, use the same buttons or menu options to stop the capture as you did to begin.

Q 5:- tools for finding details of any network or server/website(ip loopup website)?

1. **IPinfo.io**: IPinfo.io offers comprehensive details about IP addresses, including geolocation data, ASN information, and company details associated with the IP.

ipinfo.io

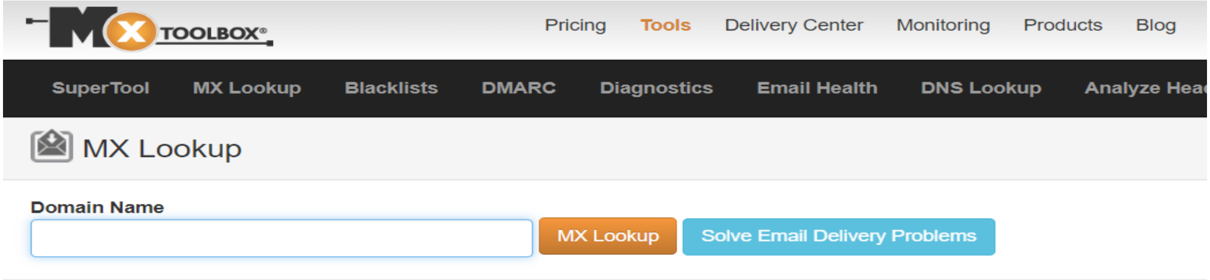


```
27.63.23.99

ip: "27.63.23.99",
city: "Srinagar",
region: "Jammu and Kashmir",
country: "IN",
loc: "34.0857,74.8055",
org: "AS45609 Bharti Airtel Ltd. AS for GPRS
Service",
postal: "190002",
timezone: "Asia/Kolkata",
```

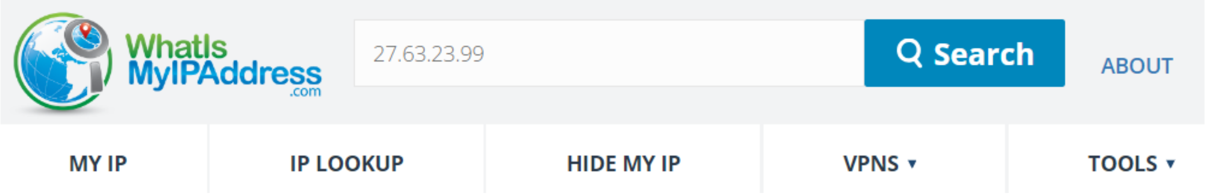
2. **IP2Location**: IP2Location provides geolocation data such as country, region, city, latitude, longitude, ZIP code, timezone, ISP, domain name, and connection type based on an IP address.

IP2LOCATION

3. **MXToolbox**: MXToolbox provides network diagnostic tools such as DNS lookup, blacklist check, SMTP diagnostics, and more.



4. **WhatIsMyIPAddress.com**: This website offers IP lookup, geolocation information, and other network tools.



------------------------------------ THANK YOU---