

Experiment 10

Learning Objective: Use of tools like Wireshark and Ettercap and it will help you to capture network packets and display them at a granular level and analyze it.

Tools: Wireshark, and Ettercap.

Theory:

What Is Wireshark?

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

Packet Capture: Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.

Filtering: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.

Visualization: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

What Is Wireshark Used For?

Wireshark has many uses, including troubleshooting networks that have performance issues. Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic. It's a major part of any IT pro's toolkit – and hopefully, the IT pro has the knowledge to use it.

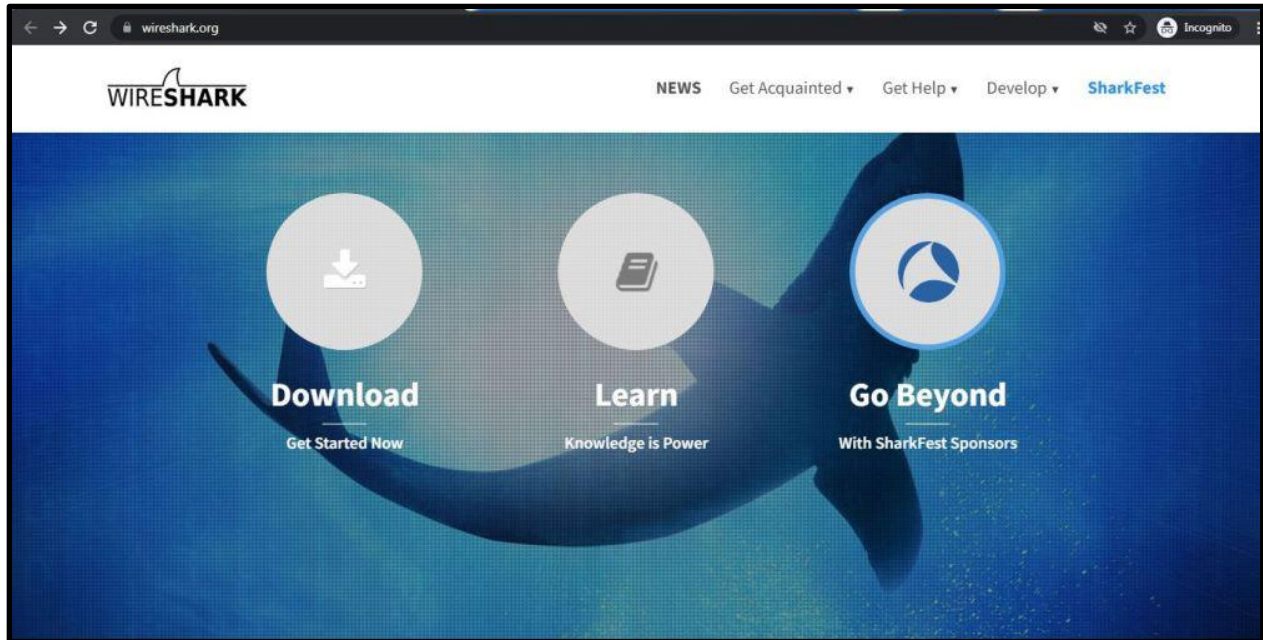
Wireshark History.

Wireshark is software that is widely used in the analysis of data packets in a network. Wireshark is completely free and open source. This packet analyzer is used for a variety of purposes like troubleshooting networks, understanding communication between two systems, developing new protocols, etc. The original name of Wireshark was Ethereal which was changed in 2006 due to some company's copyright issues. This software is written in C and C++, and its initial release was in the year 1998. Its latest release is 3.6.0 which got released on 22 November 2021. Wireshark is a cross-platform software, it can be run on Linux, windows, mac, and any other operating system.

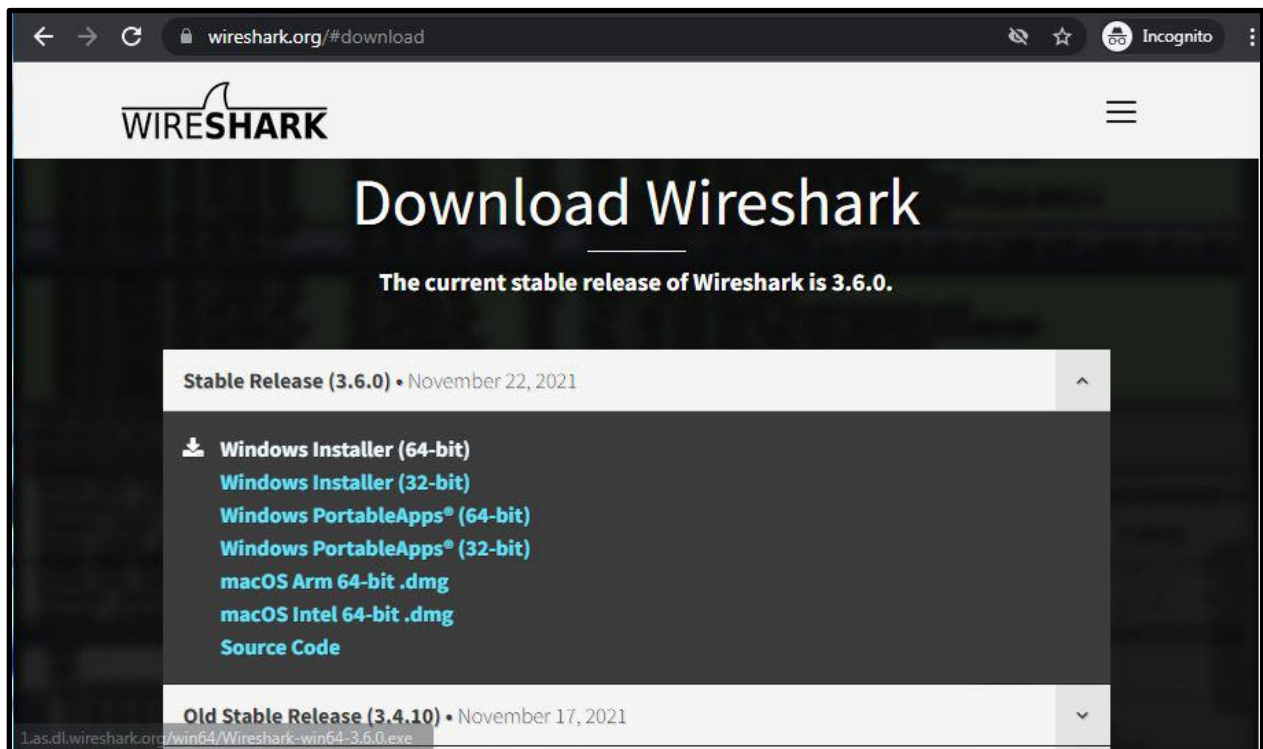
Learning Object 01: Installing Wireshark and Sniffing HTTP request.

Installing Wireshark on Windows:

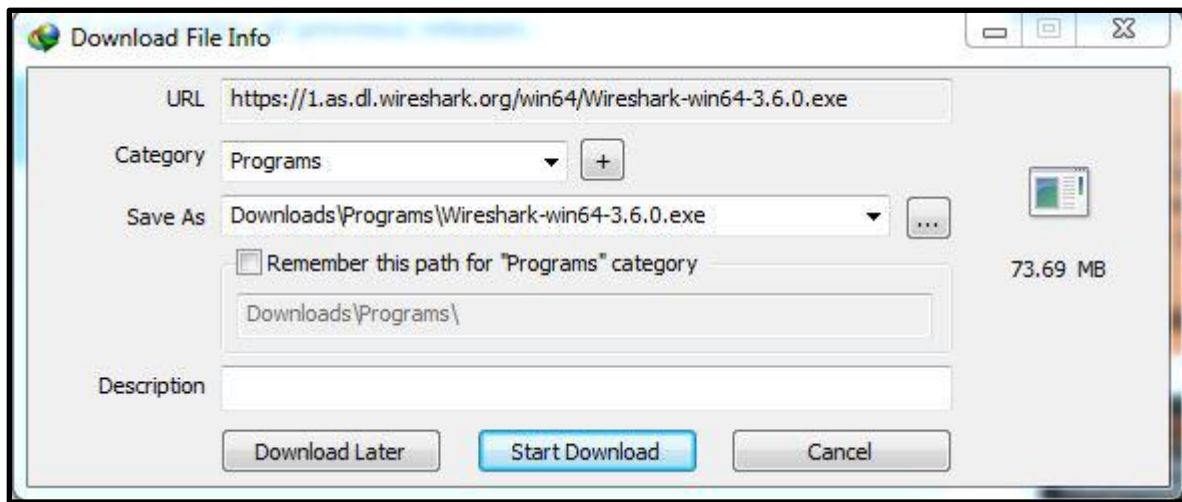
Step 1: Visit the official Wireshark website: - <https://www.wireshark.org/>



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



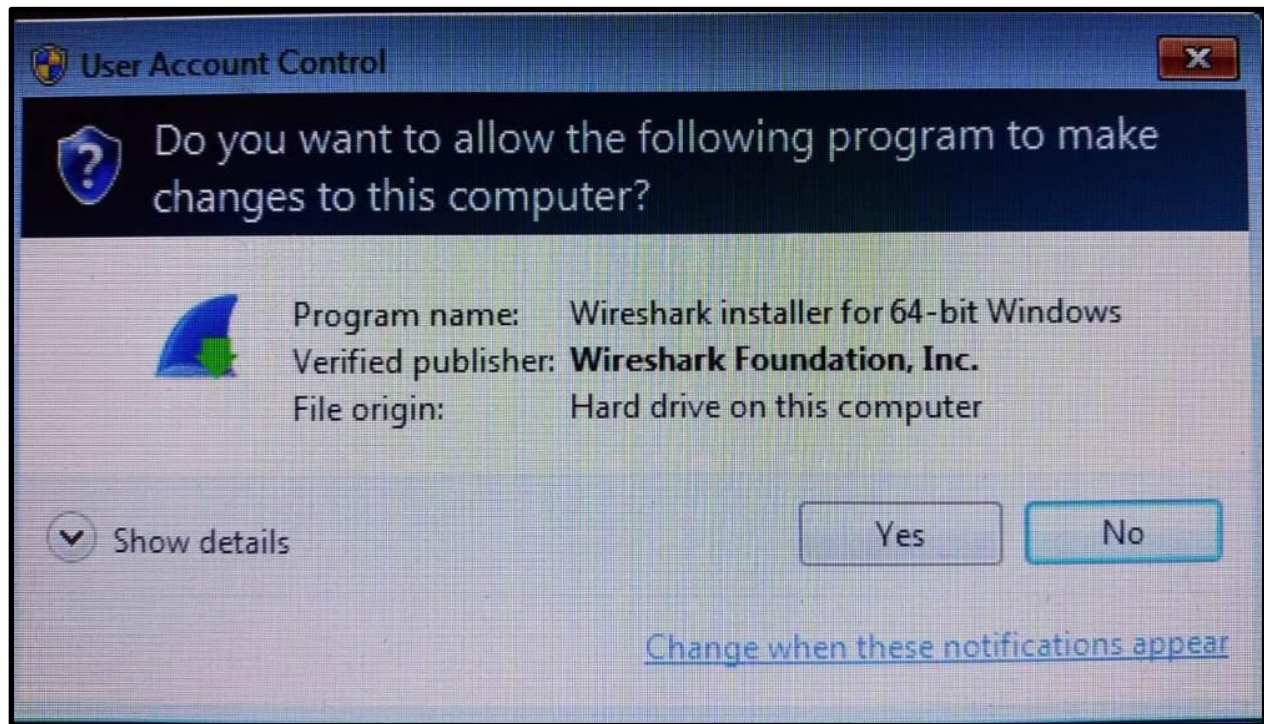
Step 3: Downloading of the executable file will start shortly. It is a small 73.69 MB file that will take some time.



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



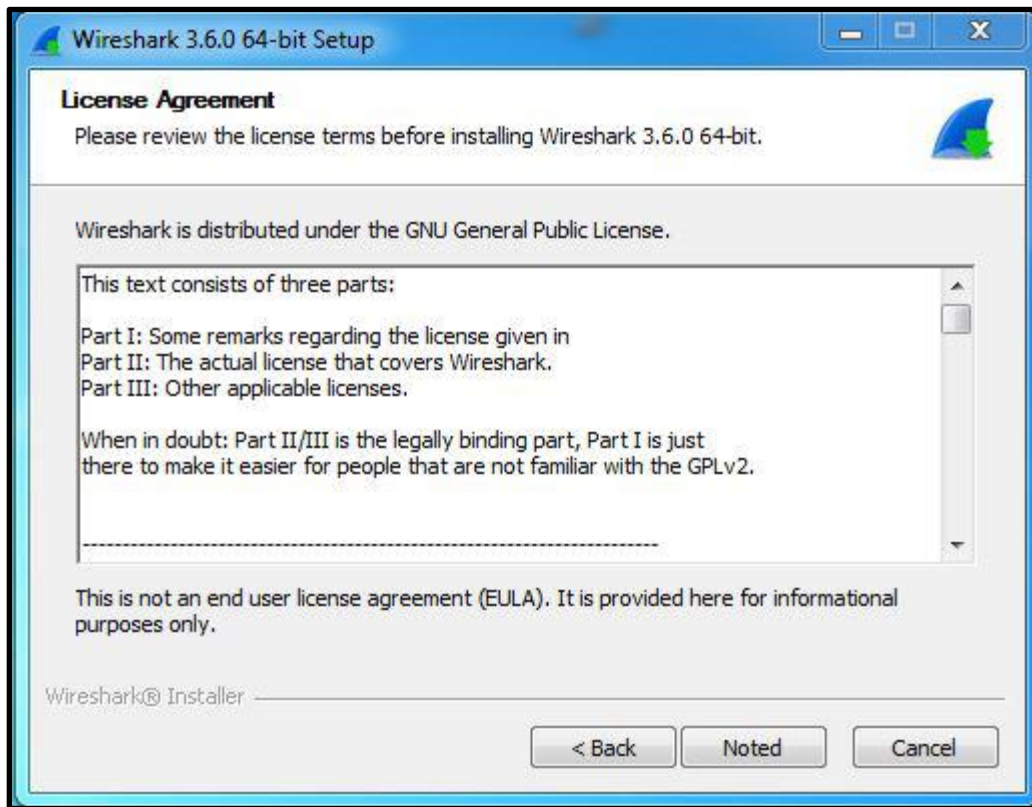
Step 5: It will prompt confirmation to make changes to your system. Click on **Yes**.



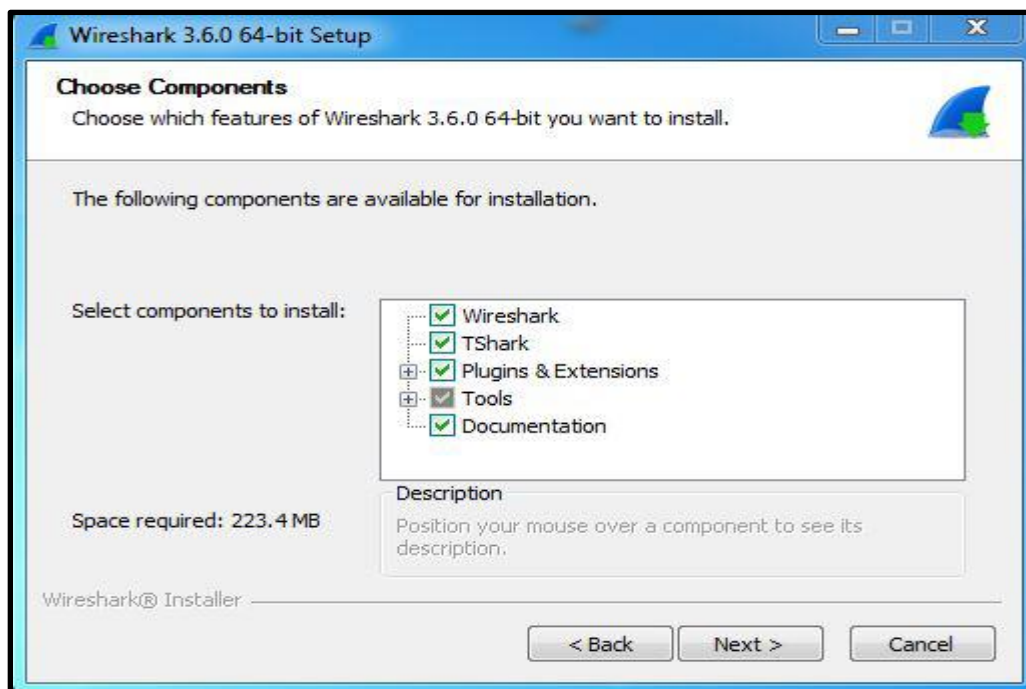
Step 6: Setup screen will appear, click on **Next**.



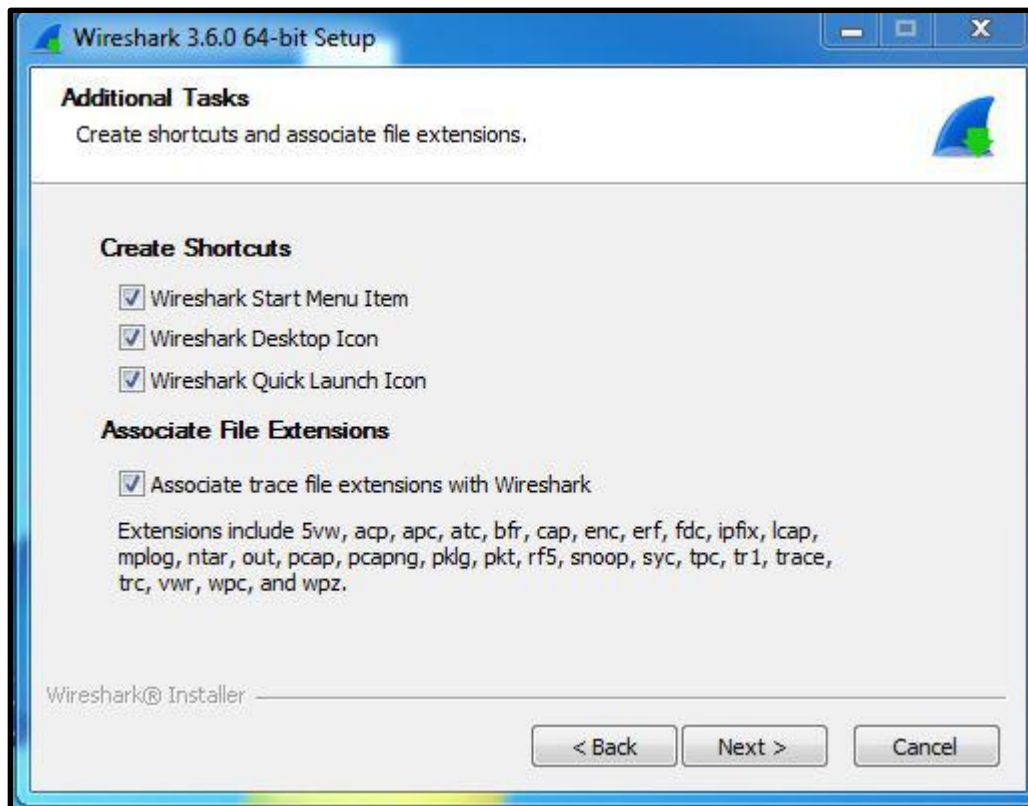
Step 7: The next screen will be of License Agreement, click on **Noted**.



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



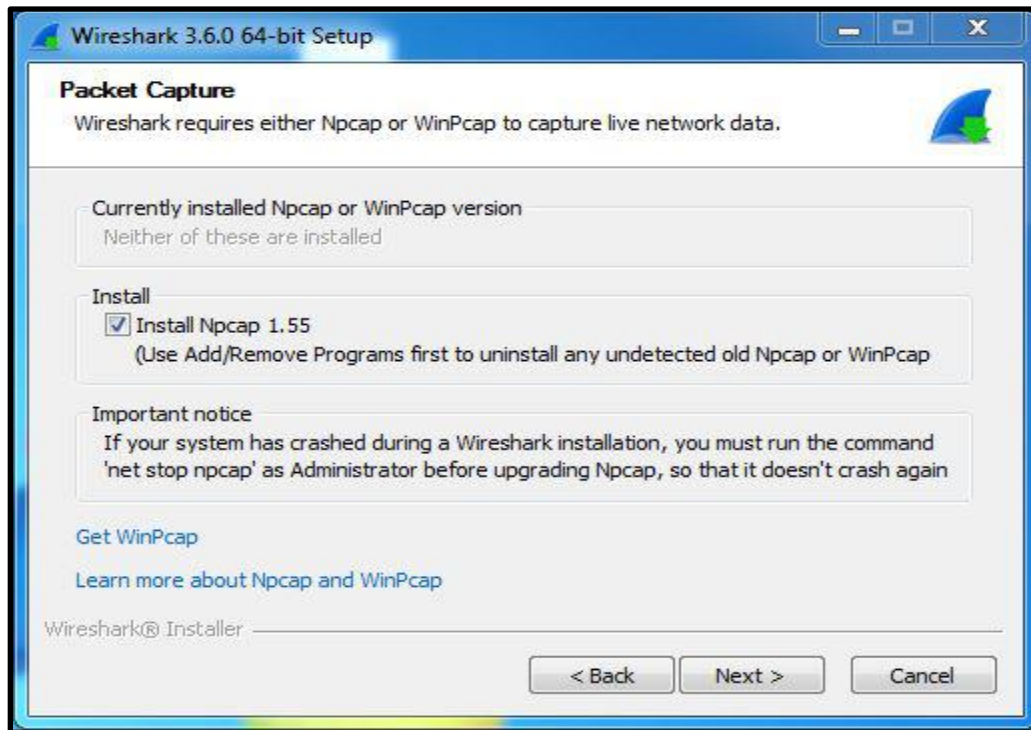
Step 9: This screen is of choosing shortcuts like start menu or desktop icon along with file extensions which can be intercepted by Wireshark, tick all boxes, and click on **Next button**.



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.



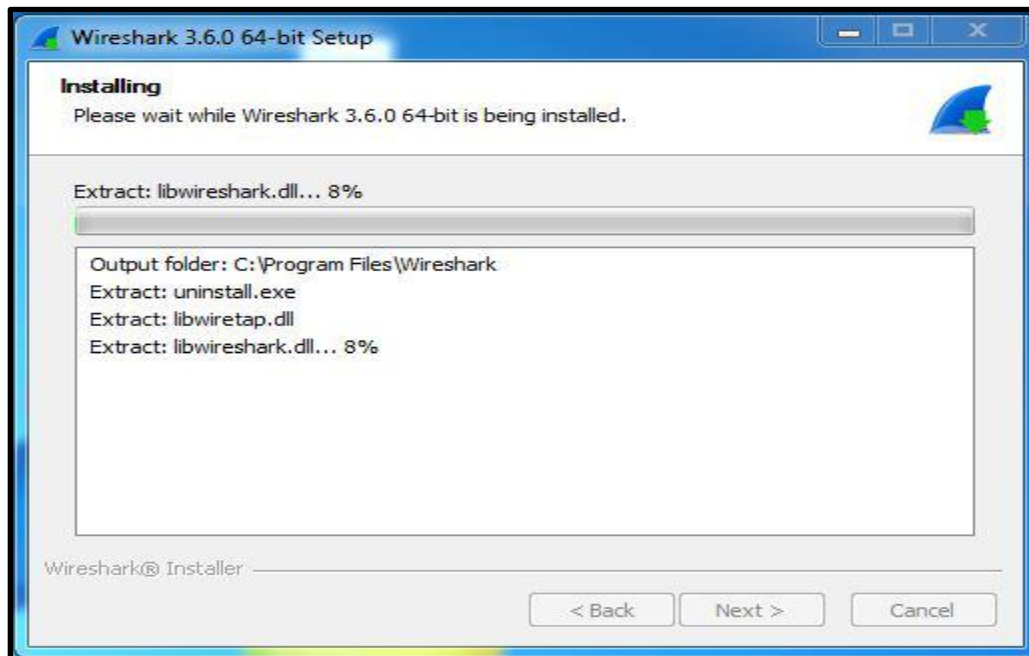
Step 11: Next screen has an option to install Npcap which is used with Wireshark to capture packets pcap means packet capture, so the install option is already checked don't change anything and click the next button.



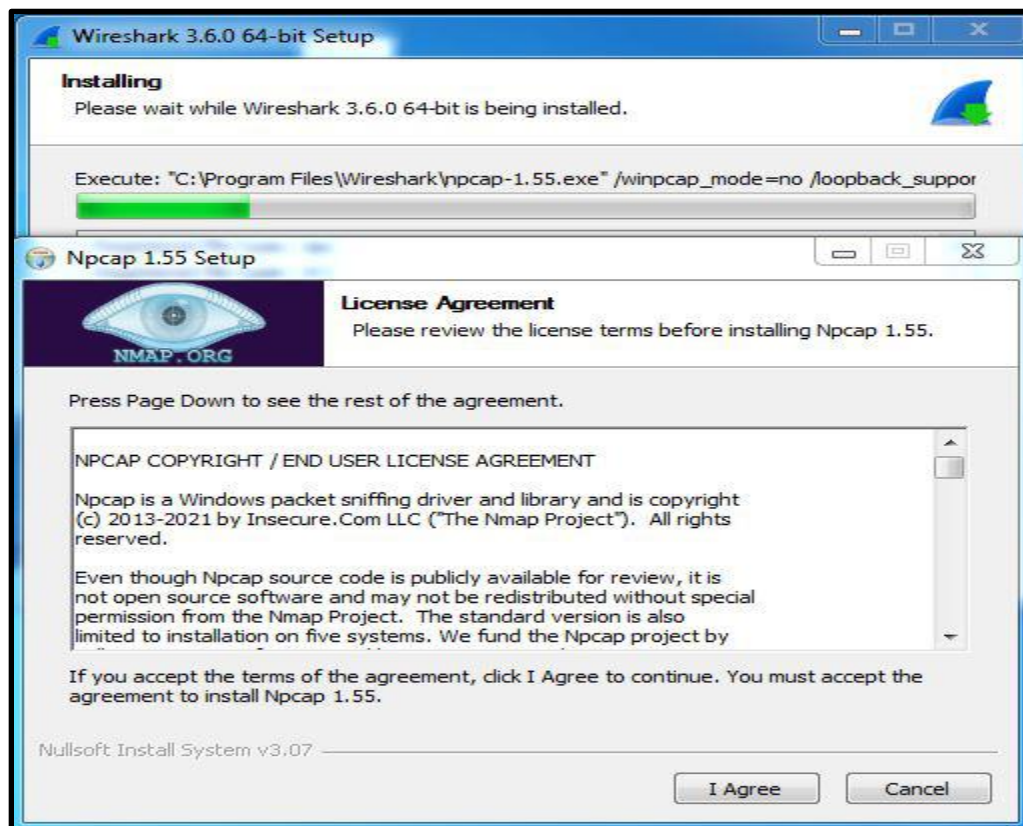
Step 12: Next screen is about USB network capturing so it is one's choice to use it or not, click on **Install**.



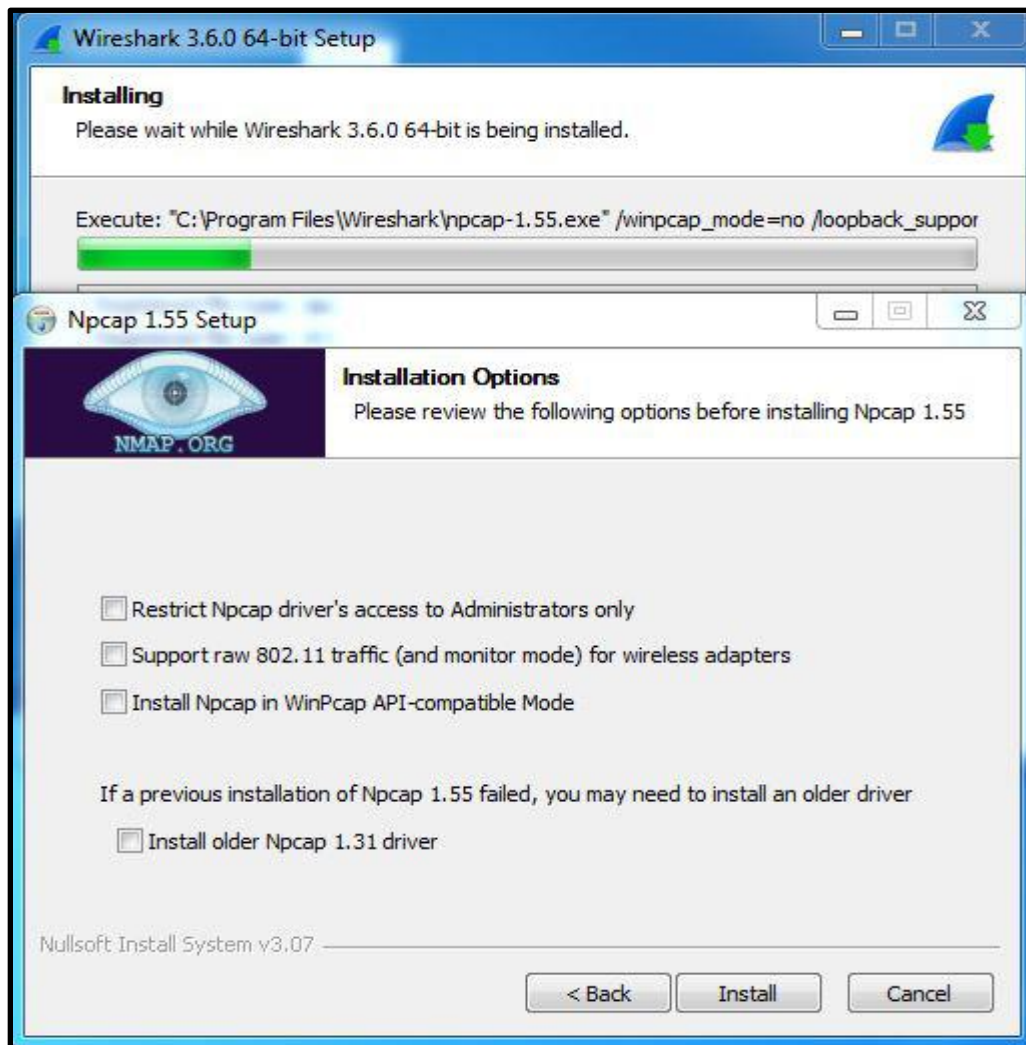
Step 13: After this, installation process will start.



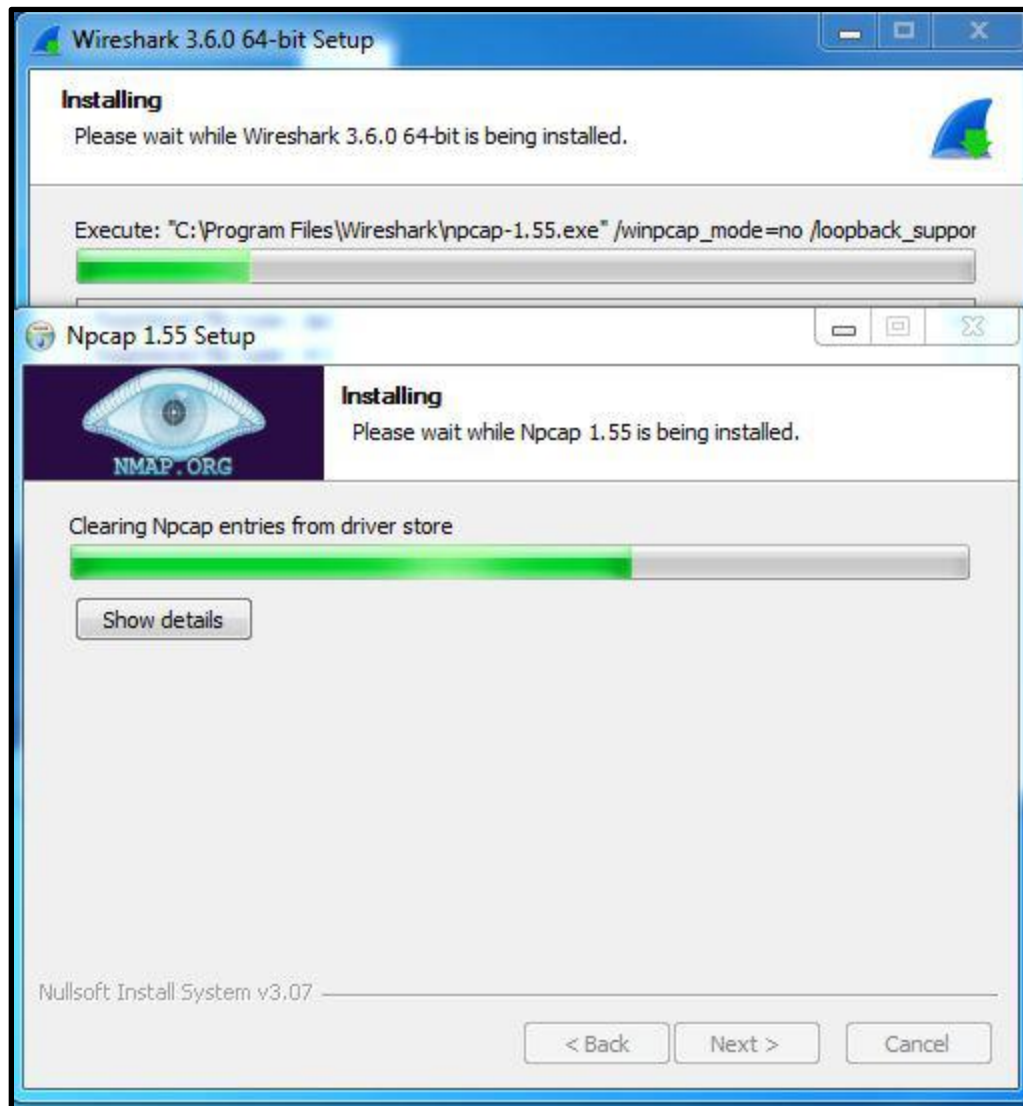
Step 14: This installation will prompt for Npcap installation as already checked so the license agreement of Npcap will appear to click on the **I Agree** button.



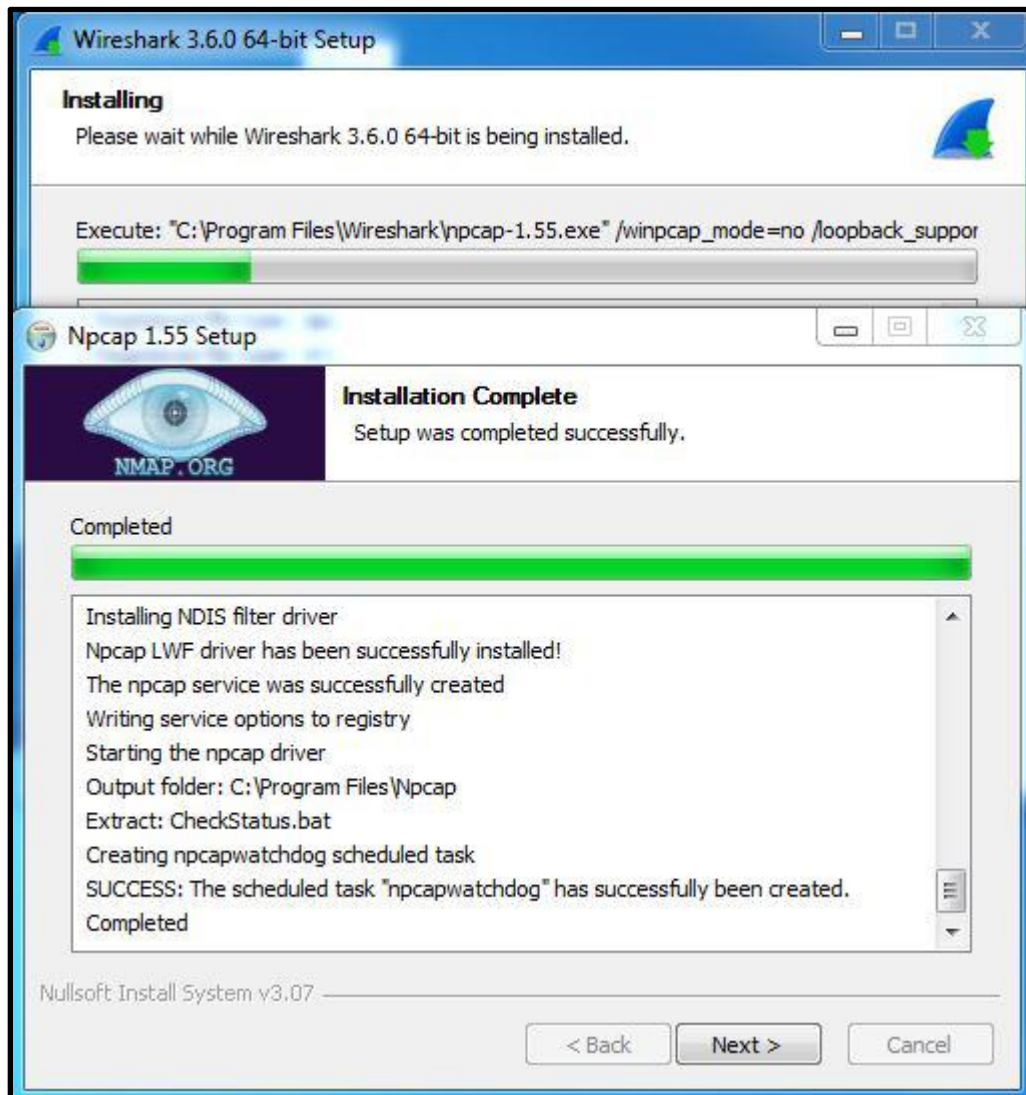
Step 15: Next screen is about different installing options of npcap, don't do anything click on Install.



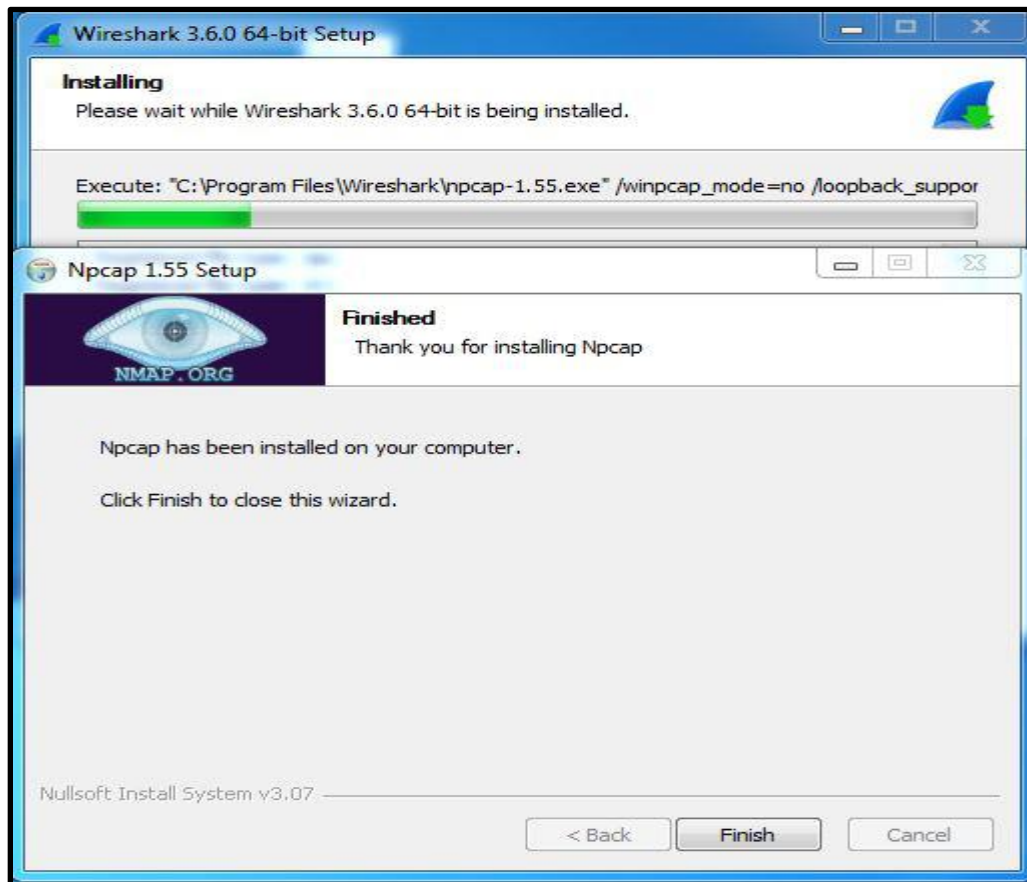
Step 16: After this, installation process will start which will take only a minute.



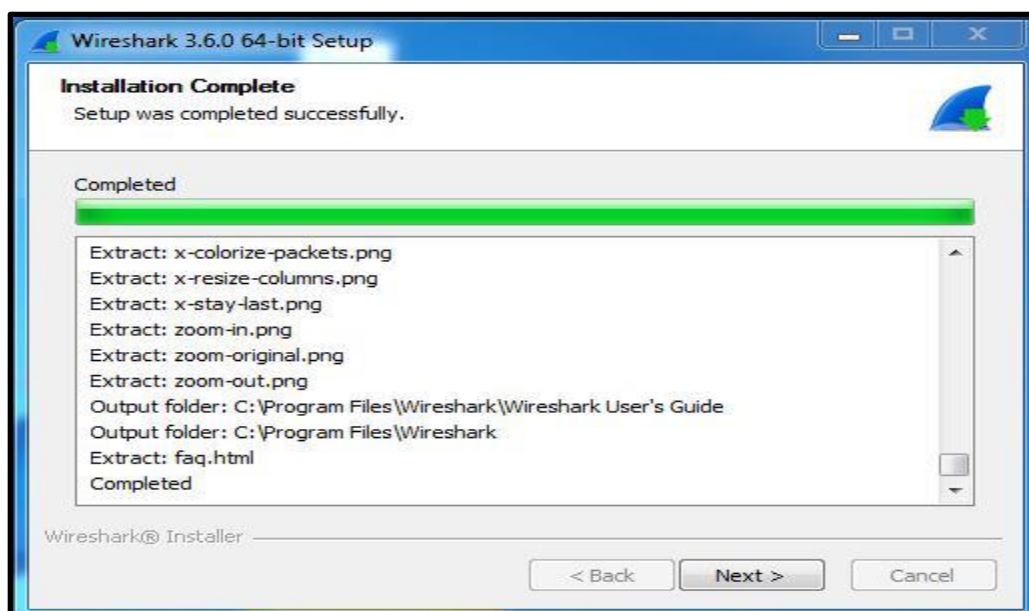
Step 17: After this, the installation process will be completed. Please click on the "Next" button.



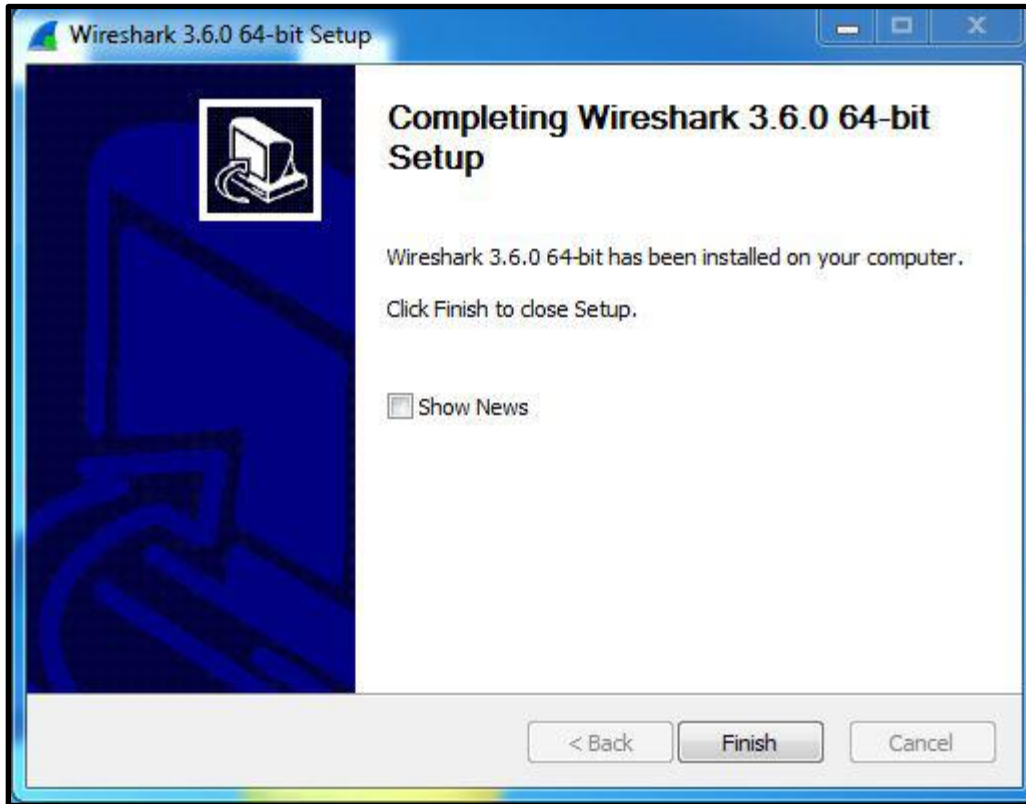
Step 18: Click on **Finish** after the installation process is completed.



Step 19: After this, the installation process of Wireshark will be completed. Please click on the "Next" button.



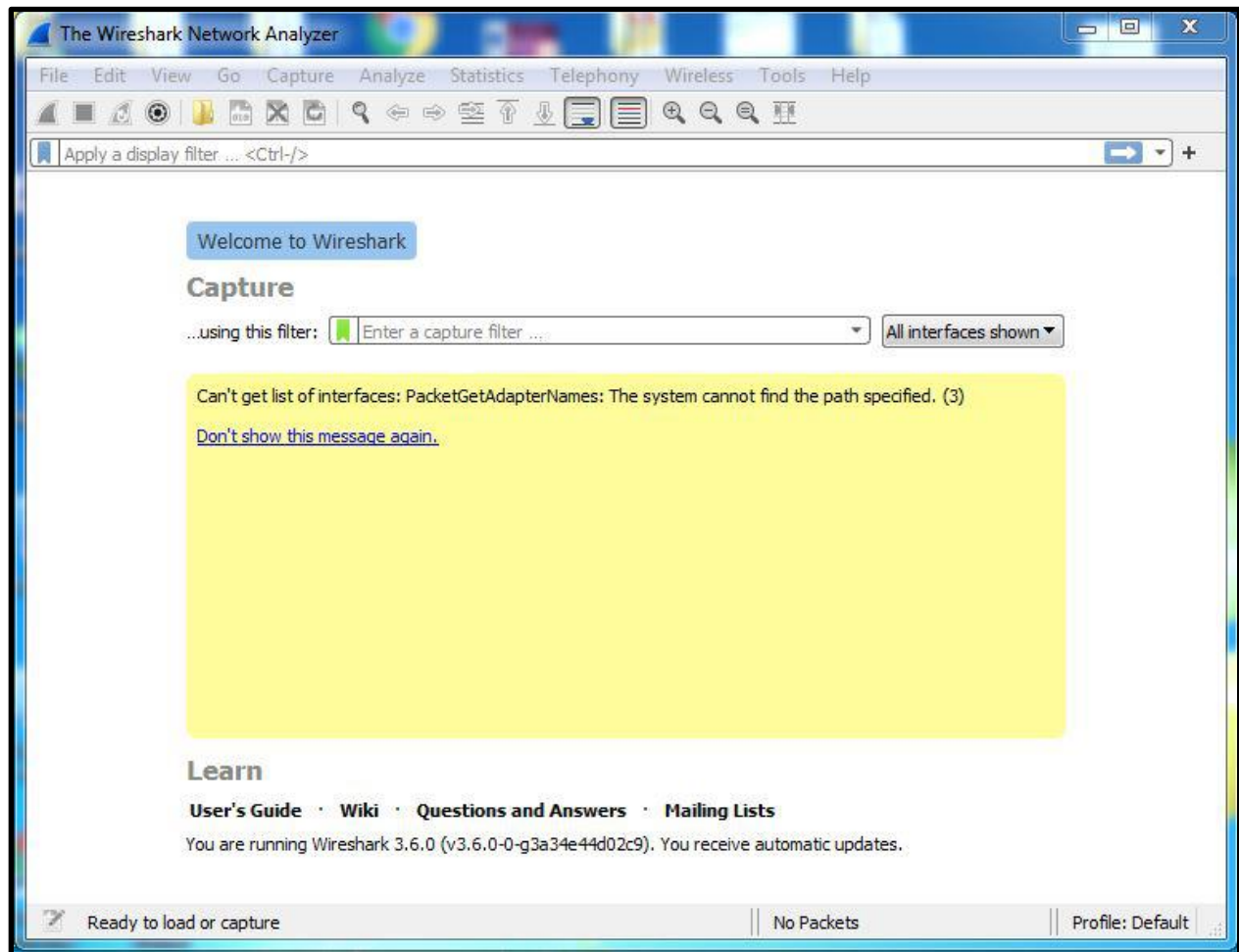
Step 20: Click on **Finish** after the installation process of Wireshark is completed.



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.



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

Sniffing HTTP Traffic

To test whether the sniffing works open the web browser and search for a random HTTP login website. For this demo, I have chosen <http://testphp.vulnweb.com/login.php> website to test.


TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)

Links
[Security art](#)
[PHP scanner](#)
[PHP vuln help](#)
[Fractal Explorer](#)



If you are already registered please enter your login information below:

Username :



Password :

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Next, go to the test website and enter some login info and click on login button.

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)


Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)



If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

After submitting the login info, it will be captured by the Attacker through the Wireshark application. Under **HTML Form URL Encoded** you could observe the login username and password.

http.request.method==POST

No.	Time	Source	Destination	Protocol	Length	Info
50	21.067432	192.168.8.188	44.228.249.3	HTTP	746	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

> Frame 50: 746 bytes on wire (5968 bits), 746 bytes captured (5968 bits) on interface \Device\NPF_{0E7C0E45-1308-4A6E-9250-7B07746EC0BA}, id 0
 > Ethernet II, Src: CyberTAN_80:02:cf (00:45:e2:80:02:cf), Dst: Shenzhen_09:f4:01 (d8:d8:66:09:f4:01)
 > Internet Protocol Version 4, Src: 192.168.8.188, Dst: 44.228.249.3
 > Transmission Control Protocol, Src Port: 58681, Dst Port: 80, Seq: 1, Ack: 1, Len: 692
 > Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

- > Form item: "uname" = "hello"
- > Form item: "pass" = "hello"

```

01b0 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,application
01c0 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml+xml,appl
01d0 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/xml;q=0.
01e0 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 9,image/avif,ima
01f0 67 65 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 ge/webp,image/ap
0200 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 ng,*/;q=0.8,app
0210 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e 65 64 2d lication/signed-
0220 65 78 63 68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d exchange;v=b3;q=
0230 30 2e 39 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 0.9;Referrer:ht
0240 74 70 3a 2f 2f 74 65 73 74 70 68 70 2e 76 75 6c tp://tes tphp.vul
0250 6e 77 65 62 2e 63 6f 6d 2f 6c 6f 67 69 6e 2e 70 nweb.com/login.p
0260 68 70 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 hp;Accept-Encod
0270 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 ing:gzip,defla
0280 74 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 te;Accept-Langu
0290 61 67 65 3a 20 65 6e 2d 47 42 2c 65 6e 2d 55 53 age:en-GB,en-US
02a0 3b 71 3d 30 2e 39 2c 65 6e 3b 71 3d 30 2e 38 2c ;q=0.9,en;q=0.8,
02b0 73 69 3b 71 3d 30 2e 37 2c 66 72 3b 71 3d 30 2e s;q=0.7,fr;q=0.
02c0 36 0d 0a 73 61 76 65 2d 64 61 74 61 3a 20 6f 6e 6;save-data:on
02d0 0d 0a 0d 0a 75 6e 61 6d 65 3d 68 65 6c 6c 6f 2d ...uname=hello&
02e0 70 61 73 73 3d 68 65 6c 6c 6f pass=hel lo
  
```


Learning Object 02: Sniffing HTTP request using Ettercap.

Sniff Login Credentials using Ettercap.

What is Ettercap?

Ettercap is an open-source tool that can be used to support man-in-the-middle attacks on networks. Ettercap can capture packets and then write them back onto the network. Ettercap enables the diversion and alteration of data virtually in real-time. Ettercap can also be used for the protocol analysis necessary to analyze network traffic.

Ettercap has a nice Graphical User Interface (GUI) as well as a command line interface. While Ettercap can support network traffic analysis, the most frequent use of Ettercap is to set up man-in-the-middle attacks using ARP poisoning. Penetration testing you can emulate includes man-in-the-middle attacks, credentials capture, DNS spoofing, and DoS attack.

Ettercap also supports both active and passive deep analysis of many protocols and includes many features for network and host analysis. Many “sniffing” modes are available – this includes MAC based, IP based, ARP based (full duplex), and Public ARP based (half duplex). Ettercap can also detect a switched local area network (LAN) and use the OS fingerprints to determine the total geometry of the LAN.

Perform the attack.

Step 01: Start your Kali Linux and open the Terminal in your Kali Linux. Type the following Command to open Ettercap GUI as shown below.

kali@kali:~\$ sudo ettercap -G



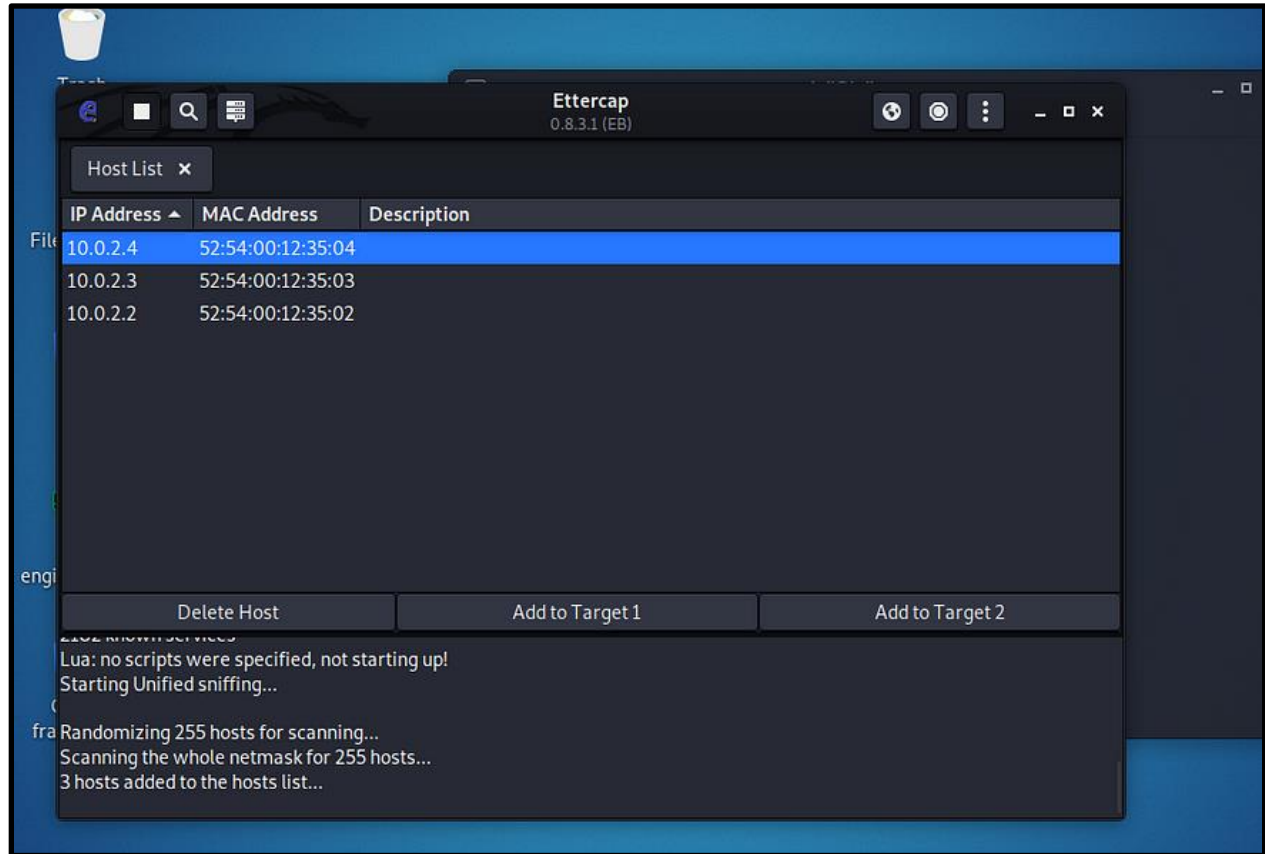
Step 02: Then Click on the **Tick icon** on the Top Bar and select Host.



Step 03: To find the hosts on the network. Click on the three dots and then **Host** you will see a menu that includes “**Scan for Hosts**”. Click on it and Ettercap will begin scanning the network for hosts.

Now, using that same “**Hosts**” tab, click on “**Hosts List**”. This will display all the hosts that Ettercap has discovered on your network.

So, you will see IP addresses and find your victims IP



Step 04: Go to the menu above and click on MITM tab and the drop-down menu will have a selection called.

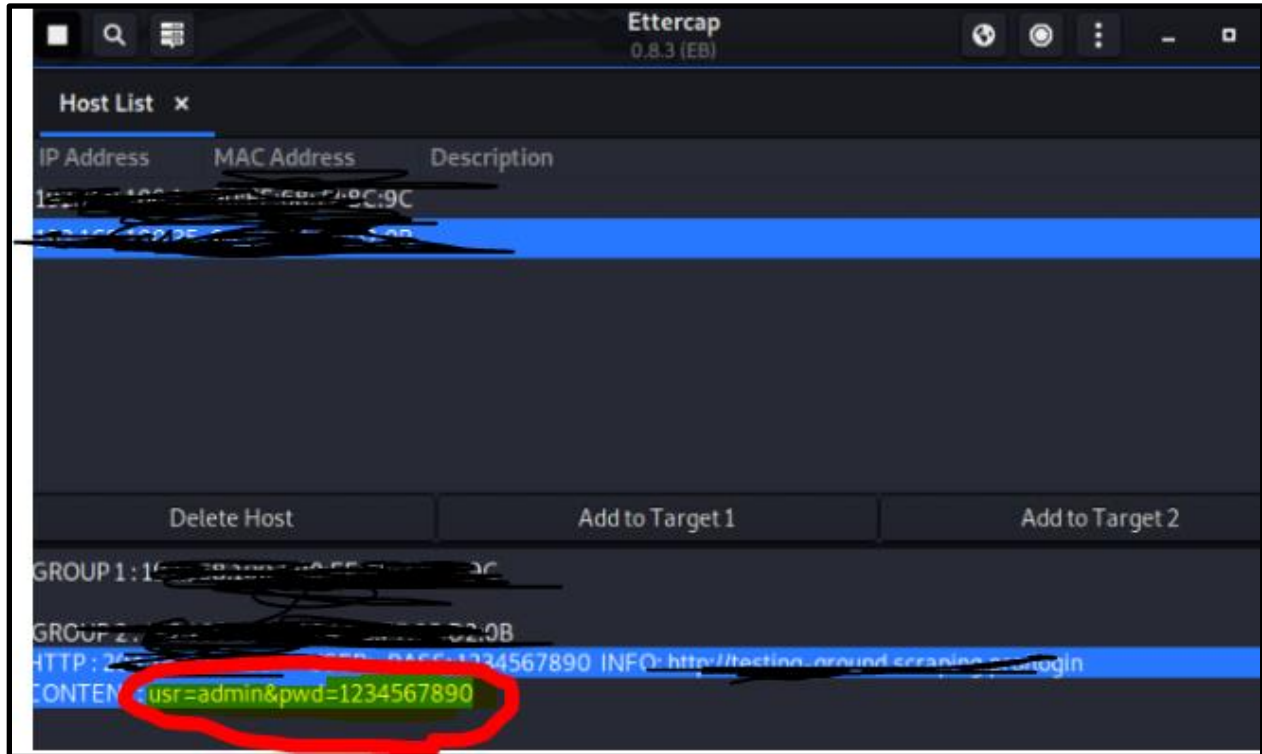
“ARP Poisoning”

Step 05: Select it and it will open a pop window like below. Select

“Sniff remote connections”.

And Press **OK**

Ettercap will begin ARP poisoning and you will see Ettercap respond in its main windows with the message below.



Now, we have successfully placed ourselves between the two targets systems and all their traffic must flow through us. This is where we can now.

1.Delete

2.Manipulate

3.Impersonate

4.View all their traffic

We have Successfully attempted the Sniffing & MITM attack using the Ettercap Tool.

Learning Outcomes: The student should have the ability to:

LO1: Perform Sniffing using Wireshark tool.

LO2: Perform Sniffing using Ettercap tool.

Course Outcomes: Upon completion of the course students will be able to understand the concept of Sniffing and ARP poisoning.

Conclusion: Through this experiment we learned the concept of sniffing and we used the Wireshark and Ettercap to sniff HTTP request.

For Faculty Use:

Correction Parameters	Formative Assessment [40%]	Timely completion of Practical [40%]	Attendance / Learning Attitude [20%]	
Marks Obtained				