

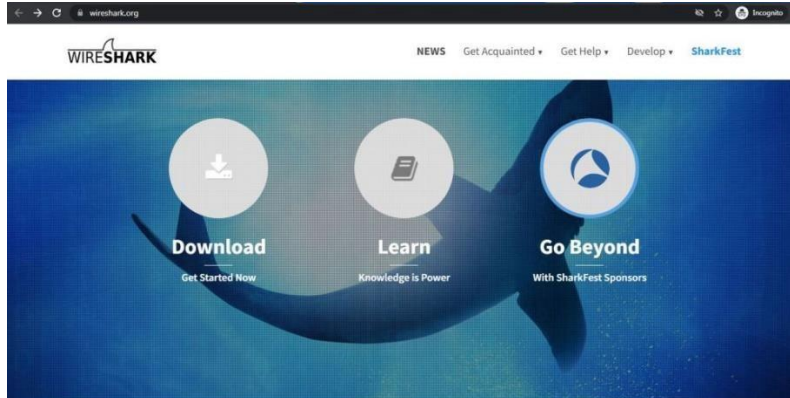
## Introduction to wireshark:-

Wireshark is **software that is widely used in the analysis of data packets in a network.**

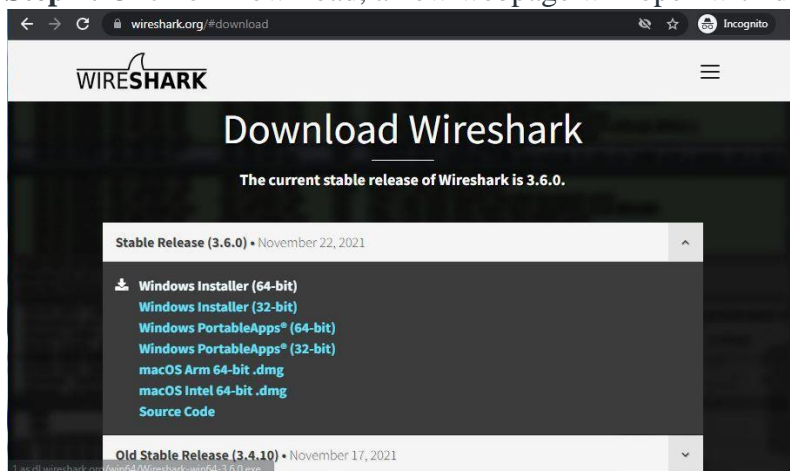
Wireshark is completely free and open source. This packet analyzer is used for a variety of purposes like troubleshooting networks, understanding communication between two systems, developing new protocols, etc.

## wireshark installation:-

**Step 1:** Visit the [official Wireshark website](https://www.wireshark.org) using any web browser.



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



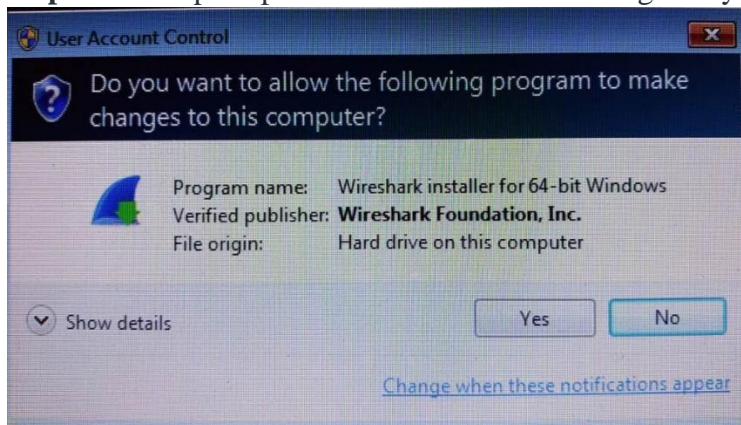
**Step 3:** Downloading of the executable file will start shortly. It is a small 73.69 MB file that will take some time.



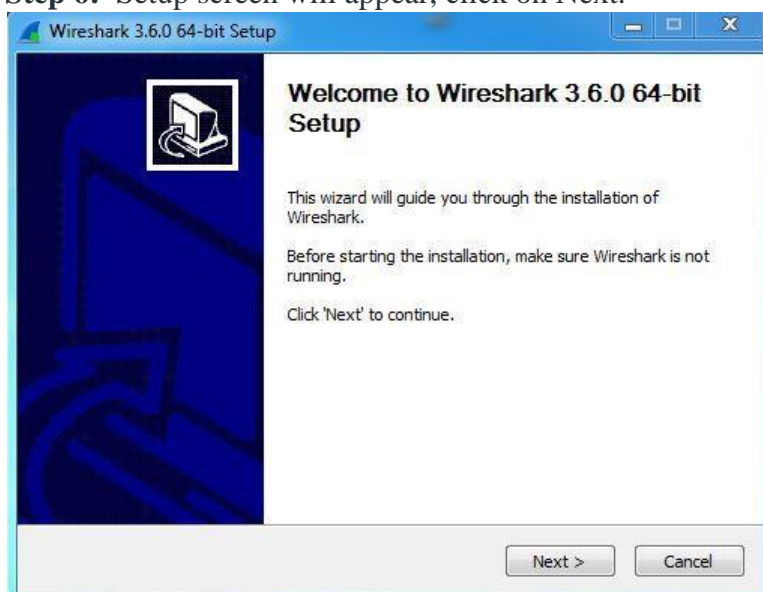
**Step 4:** Now check for the executable file in downloads in your system and run it.



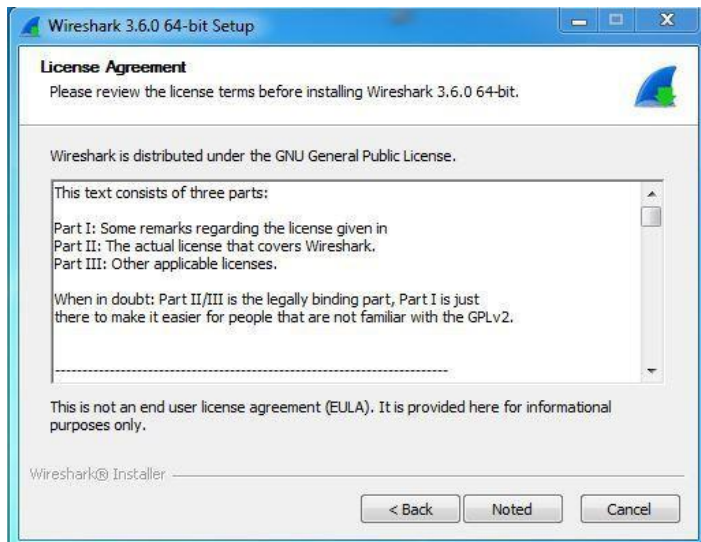
**Step 5:** It will prompt confirmation to make changes to your system. Click on Yes.



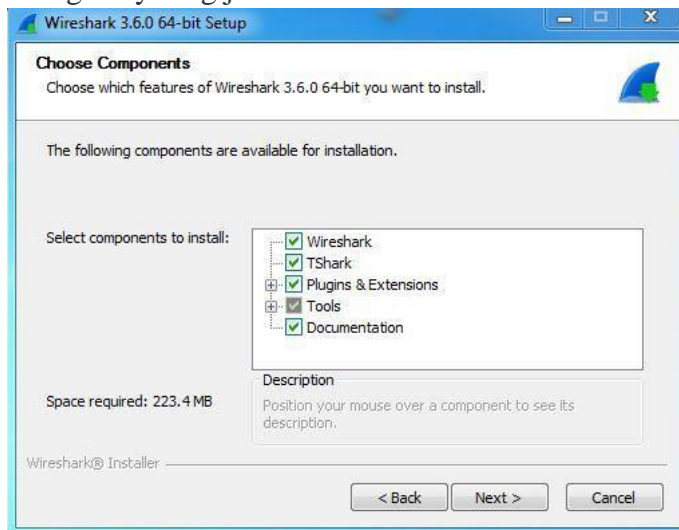
**Step 6:** Setup screen will appear, click on Next.



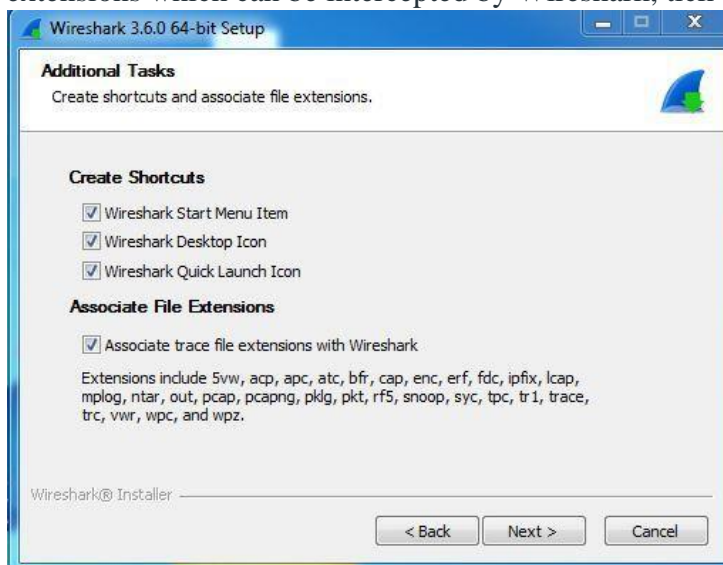
**Step 7:** The next screen will be of License Agreement, click on Noted.



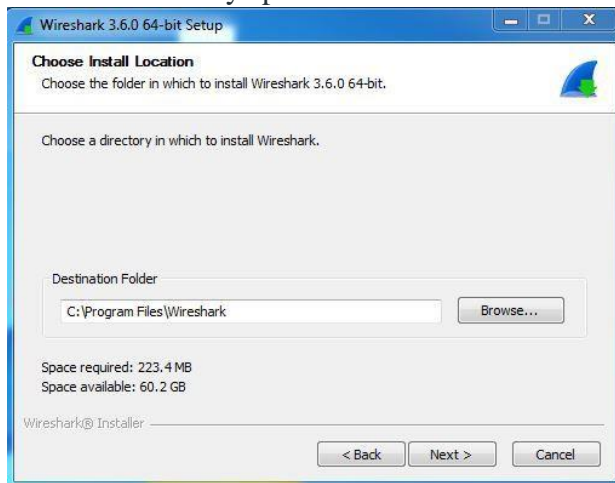
**Step 8:** This screen is for choosing components, all components are already marked so don't change anything just click on the Next button.



**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.



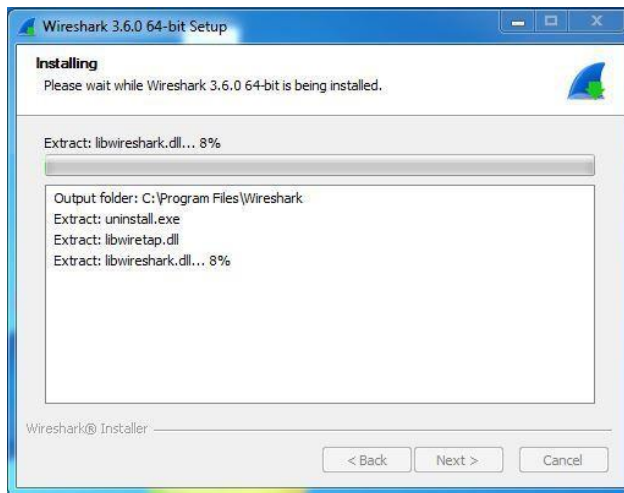
**Step 11:** Next screen has an option to install Npcap which is used with Wireshark to capture packets *pcap* means packet capture so the install option is already checked don't change anything and click the next button.



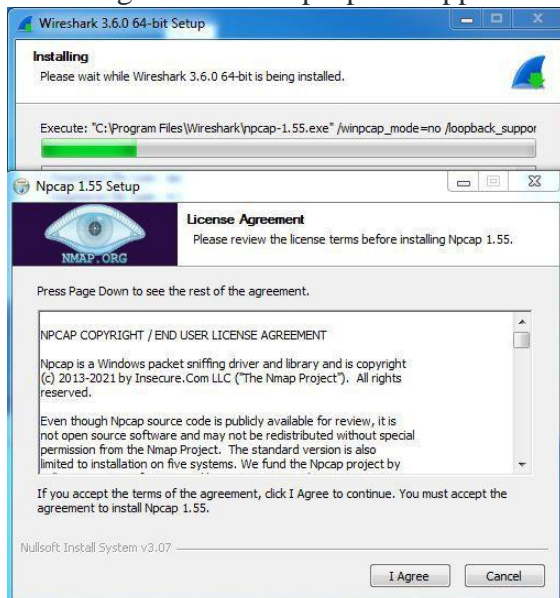
**Step 12:** Next screen is about USB network capturing so it is one's choice to use it or not, click on Install.



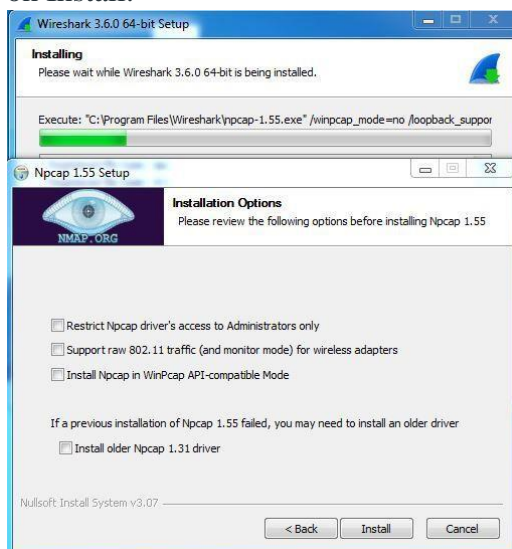
**Step 13:** After this installation process will start.



**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.

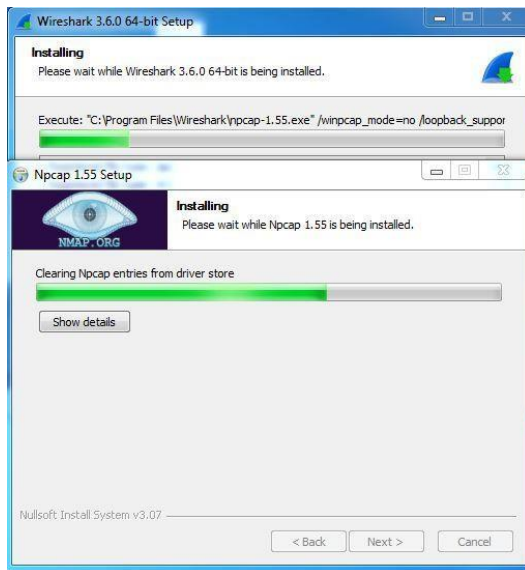


**Step 15:** Next screen is about different installing options of *npcap*, don't do anything click on Install.

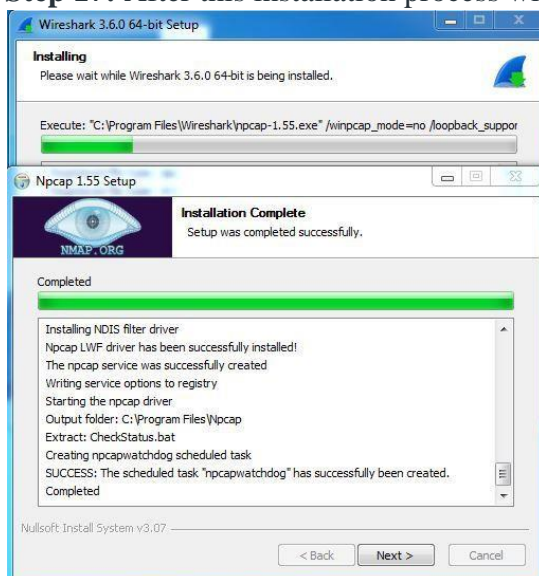


**Step 16:** After this installation process will start which will take only a minute.





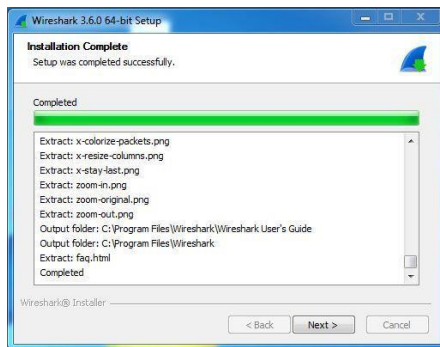
**Step 17:** After this installation process will complete click on the Next button.



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



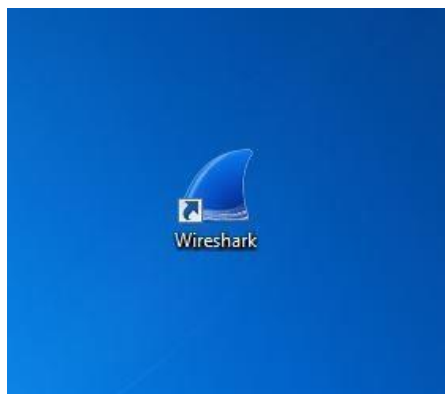
**Step 19:** After this installation process of Wireshark will complete click on the Next button.



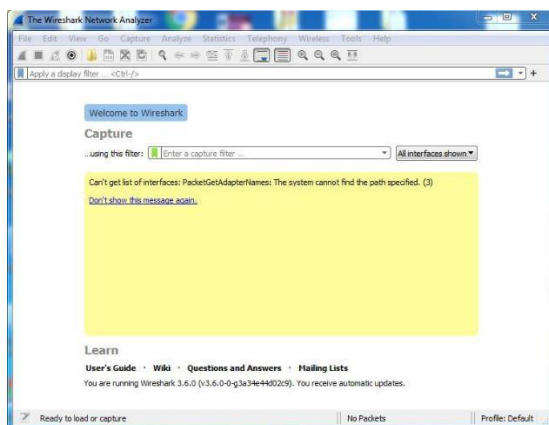
**Step 20:** Click on Finish after the installation process of Wireshark is complete.



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

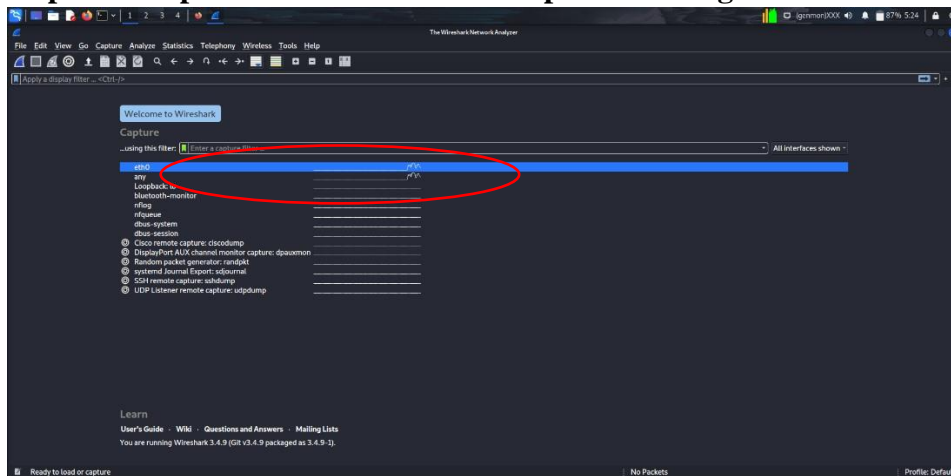


Now run the software and see the interface.

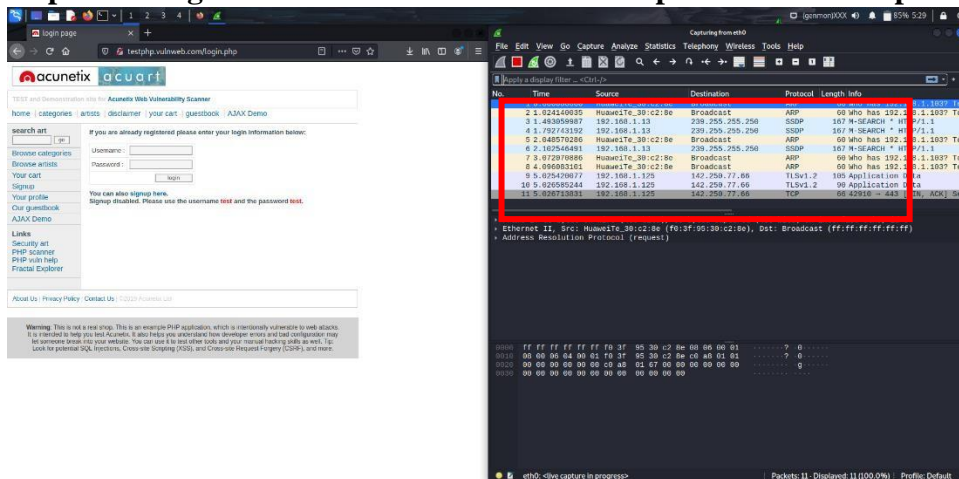


# Sniffing http packets using wireshark:-

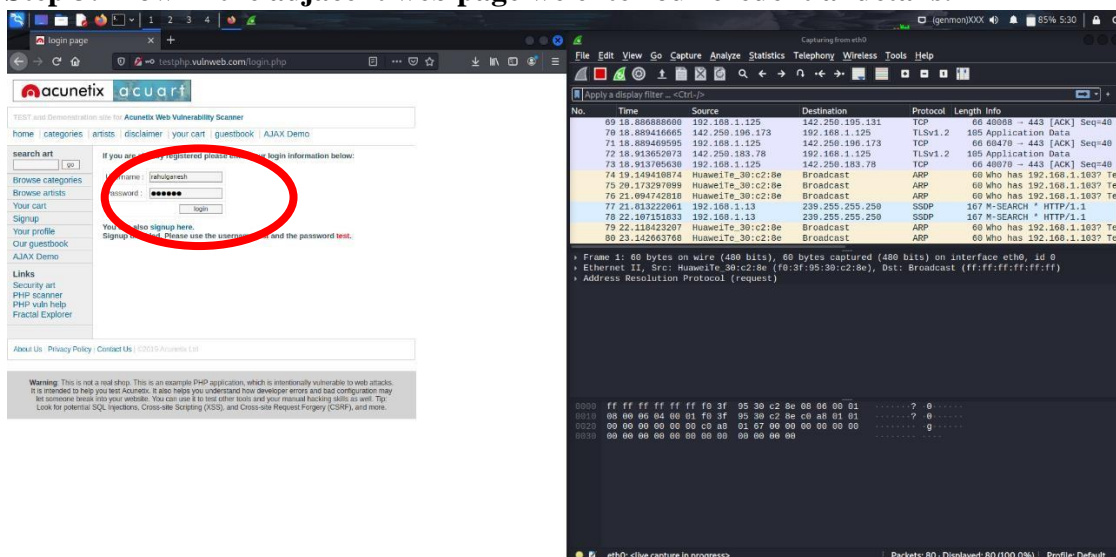
Step 1:- we open wireshark and see the pulse running on the network connection.



Step 2:- we right click and see that the network packets will be captured by wireshark.



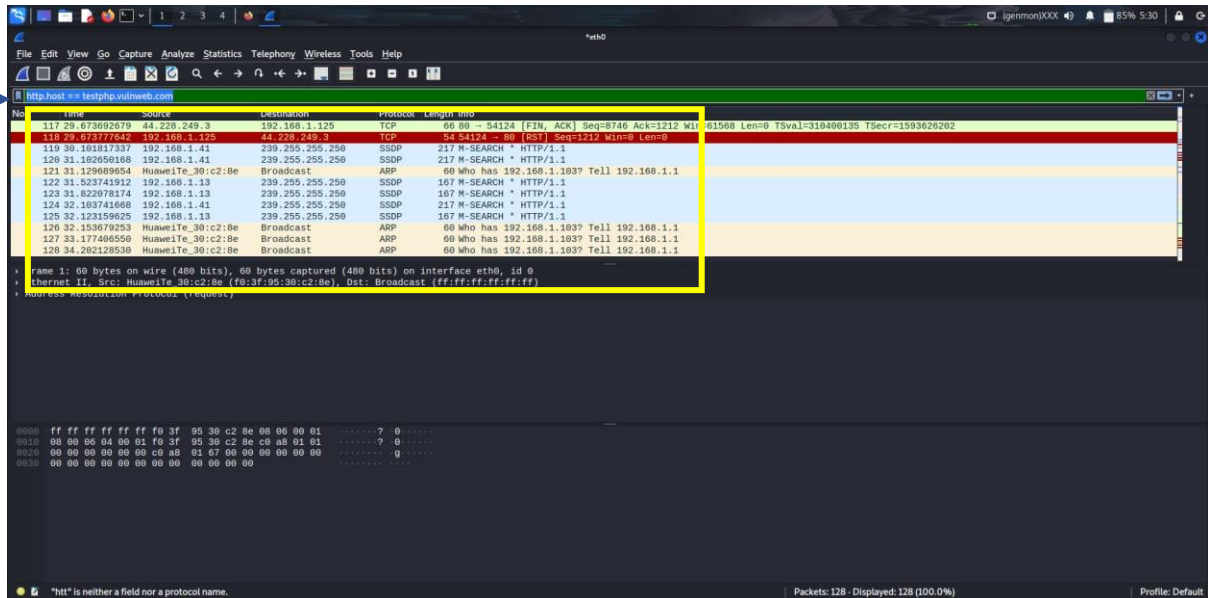
Step 3:- now in the adjacent web page we enter our credential details.



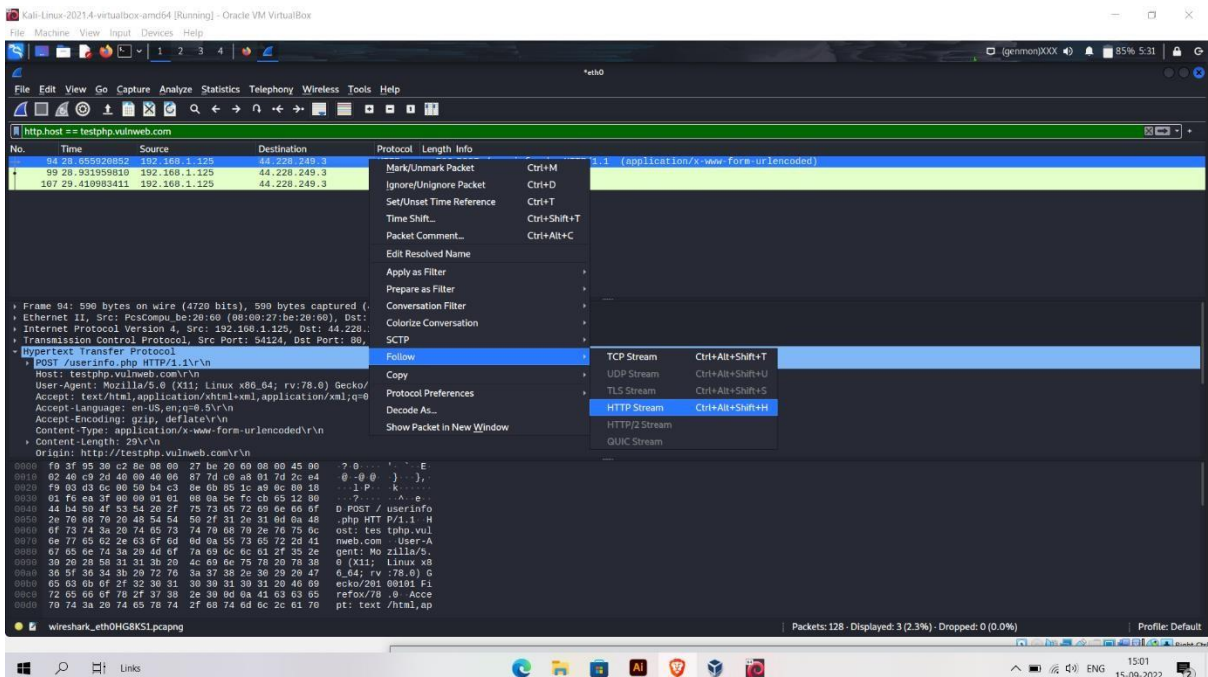


**Step 4:-** we hit enter and stop the wireshark, so that it stops to capture the packets. And now we filter the packets in the filter box, by giving <protocol>.host == <domain name>

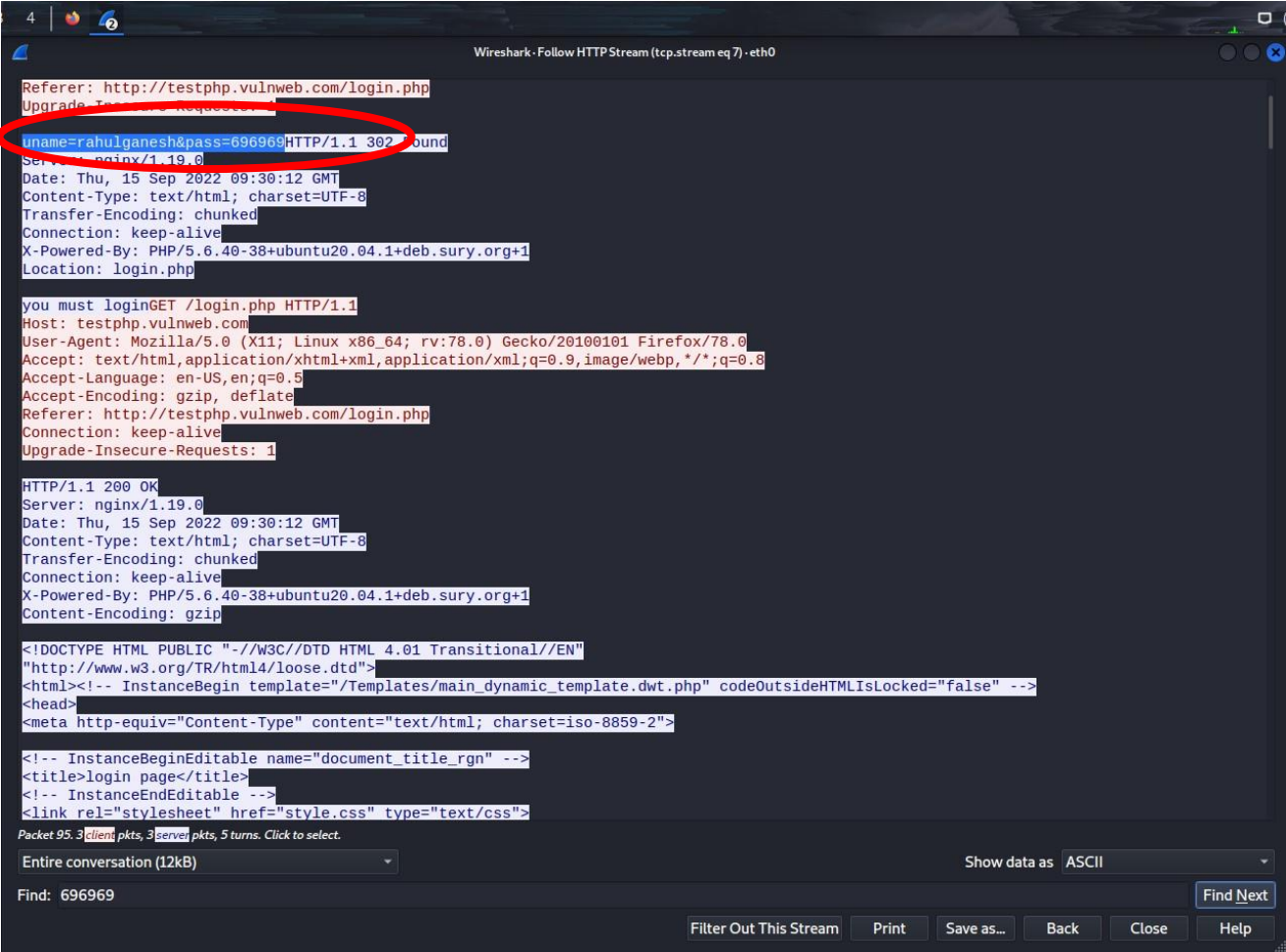
**Ex:-** “http.host==testphp.vulnweb.com”.



And we see the filtered packets that are required.



**Step 5:-** Now if we right click on any packet and > follow > http stream, we will see something like this where all our credentials entered in that particular web page are seen.



The screenshot shows the Wireshark interface with the 'Follow HTTP Stream' window open for packet 95. The stream is titled 'Follow HTTP Stream (tcp.stream eq 7) - eth0'. The request line is highlighted with a red circle: `uname=rahulganeshe&pass=696969 HTTP/1.1 302 Found`. The response status is `HTTP/1.1 200 OK`. The HTML content is visible below the headers.

```
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
uname=rahulganeshe&pass=696969 HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Thu, 15 Sep 2022 09:30:12 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php

you must loginGET /login.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 15 Sep 2022 09:30:12 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
```

Packet 95. 3 client pkts, 3 server pkts, 5 turns. Click to select.

Entire conversation (12kB) Show data as ASCII

Find: 696969 Find Next

Filter Out This Stream Print Save as... Back Close Help

## The Windows Security Log:-

The Windows Security Log, which you can find under Event Viewer, records critical user actions such as logons and logoffs, account management, object access, and more. Microsoft describes the Windows Security Log as "your best and last defense," and rightly so. The Security Log helps detect potential security problems, ensures user accountability, and serves as evidence during security breaches.

### What makes a Windows security event critical?

Among the multitude of Windows security events, the few that can be deemed critical can be broadly classified into two groups:

Events whose single occurrence indicates malicious activity. For example, a normal end-user account getting unexpectedly added to a sensitive security group.

Events whose successive occurrence above an accepted baseline indicates malicious activity. For example, an abnormally large number of failed logons.

The eight most critical Windows security event IDs

Serial Category Number	Event ID and description	Reasons to monitor (by no means exhaustive)
(1) & (2)	Logon and logoff	4624 (Successful logon)
		<ul style="list-style-type: none"><li>• To detect abnormal and possibly unauthorized insider activity, like a logon from an inactive or restricted account, users logging on outside of normal working hours, concurrent logons to many resources, etc.</li><li>• To get information on user behavior like user attendance, user working hours, etc.</li></ul>

		<b>4625</b> (Failed logon)	<ul style="list-style-type: none"> <li>• To detect possible brute-force, dictionary, and other password guess attacks, which are characterized by a sudden spike in failed logons.</li> <li>• To arrive at a benchmark for the account lockout threshold policy setting.</li> </ul>
--	--	----------------------------	---

(3), (4), and (5)	<b>Account management</b>	<b>4728</b> (Member added to securityenabled global group)	<ul style="list-style-type: none"> <li>• To ensure group membership for privileged users, who hold the “keys to the kingdom,” is scrutinized regularly. This is especially true for security group membership additions.</li> <li>• To detect privilege abuse by users who are responsible for unauthorized additions.</li> <li>• To detect accidental additions.</li> </ul>
		<b>4732</b> (Member added to securityenabled local group)	
		<b>4756</b> (Member added to securityenabled universal group)	

(6)	<b>Event log</b>	<p><b>1102</b> (Log cleared) (Alternatively the event log service can also be disabled which results in the logs not getting recorded. This is done by the system audit policy, in which case event <b>4719</b> gets recorded.)</p>	<ul style="list-style-type: none"> <li>• To spot users with malicious intent, such as those responsible for tampering with event logs.</li> </ul>
(7)	<b>Account management</b>	<b>4740</b> (User account locked out)	<ul style="list-style-type: none"> <li>• To detect possible brute-force, dictionary, and other password guess attacks, which are characterized by a sudden spike in failed logons.</li> <li>• To mitigate the impact of legitimate users getting locked out and being unable to carry out their work.</li> </ul>
(8)	<b>Object access</b>	<b>4663</b> (Attempt made to access object)	<ul style="list-style-type: none"> <li>• To detect unauthorized attempts to access files and folders.</li> </ul>

## Monitor logs in windows:-

Log monitoring is a practice used by IT administrators to organize, analyze, and understand a network's performance. All network devices, including applications and hardware, create



logs as they perform operations. Logs are like a device's diary—they record every event and its critical information like user IP address, date and time, request time, and more. Log data can help you discover and troubleshoot issues, understand your infrastructure's daily activities, and optimize functionality across platforms.

Since each individual network device has its own logs, logging protocols are often used to standardize various log data. Syslog, which stands for System Logging Protocol, is a standard protocol that sends event logs to a specific server known as a syslog server. A syslog server is designed to bring all network logs to a single location, making it easier to manage and make sense of valuable syslog data.

Effective syslog monitoring can help you safely and accurately gather, analyze, and transmit data throughout your IT infrastructure. There are many syslog servers available today, and in this article, we'll examine a handful of excellent log monitoring tools.

## **Log Monitoring Tips and Best Practices:-**

It's essential to monitor log events on your network. Log monitoring can help you gain vital understandings of network performance, which can inform decisions to optimize network functionality. However, it can be difficult—not to mention overwhelming—to efficiently and accurately decipher the thousands of log events created daily.

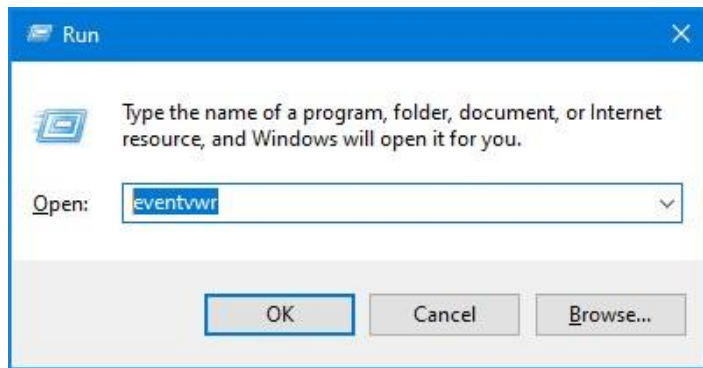
Log monitoring software is built to perform essential event log monitoring tasks consistently and accurately. You can use log monitoring tools to detect suspicious activity as soon as it occurs, then use related log data to uncover root sources and begin efficient troubleshooting. Syslog monitoring software is also designed to contrast real-time metrics with historical metrics to provide an in-depth understanding of a network's performance over time. Log monitoring tools allow you to generate alerts and reports to help you stay on top of log monitoring and create clear visualizations for at-a-glance insights into network performance.

## **Ways to Quickly Clear All Event Logs in Windows 10:-**

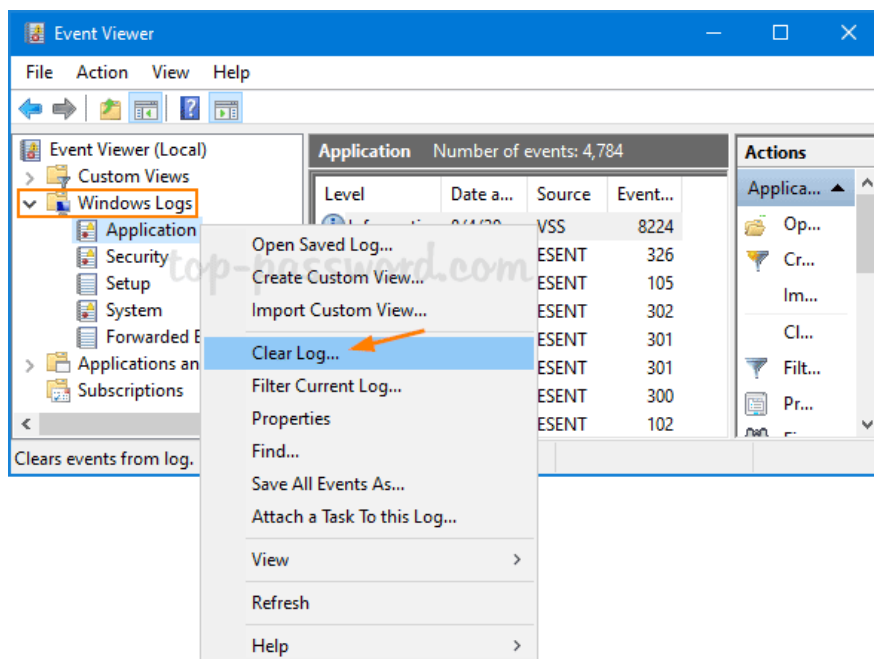
Event Viewer is a built-in Windows application that lets you view all the important events that occur on your PC. Sometimes, you may need to delete old event logs at once if nothing has gone wrong. In this tutorial we'll show you 3 ways to quickly clear all event logs in Windows 10 Event Viewer.

### **Method 1: Clear Windows Event Logs Using Event Viewer:-**

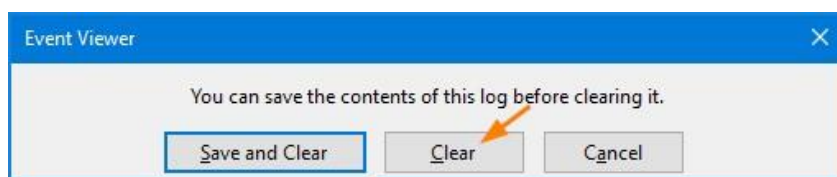
Press the Windows + R keys to open the Run dialog, type **eventvwr.msc** and click OK to [open Event Viewer](#).



On the left sidebar of Event Viewer, expand “Windows Logs” and right-click one of the events categories, then select **Clear Log** from the menu that comes up.



Click either the “**Save and Clear**” or the **Clear** button to confirm.

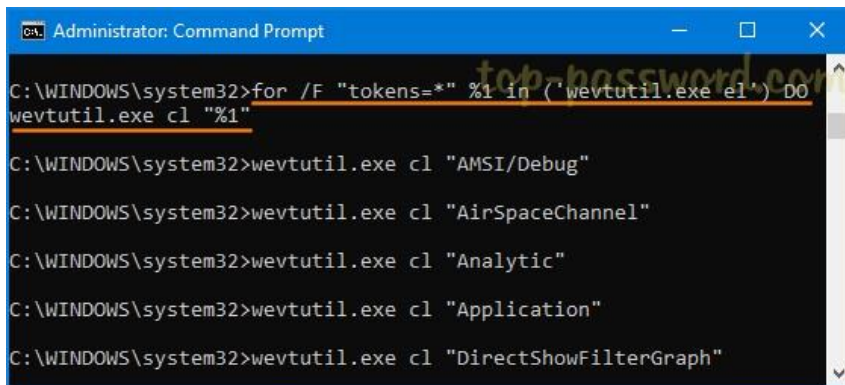


The event logs will be cleared immediately.

Method 2: Clear Windows Event Logs Using Command Prompt:-

Open an elevated Command Prompt window. Copy and paste the following command into the Command Prompt, and then hit Enter.

`for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"`



```
Administrator: Command Prompt
C:\WINDOWS\system32>for /F "tokens=* %1 in ( wevtutil.exe el ) DO
wevtutil.exe cl "%1"
C:\WINDOWS\system32>wevtutil.exe cl "AMSI/Debug"
C:\WINDOWS\system32>wevtutil.exe cl "AirSpaceChannel"
C:\WINDOWS\system32>wevtutil.exe cl "Analytic"
C:\WINDOWS\system32>wevtutil.exe cl "Application"
C:\WINDOWS\system32>wevtutil.exe cl "DirectShowFilterGraph"
```

This will delete all types of Windows event logs at once.

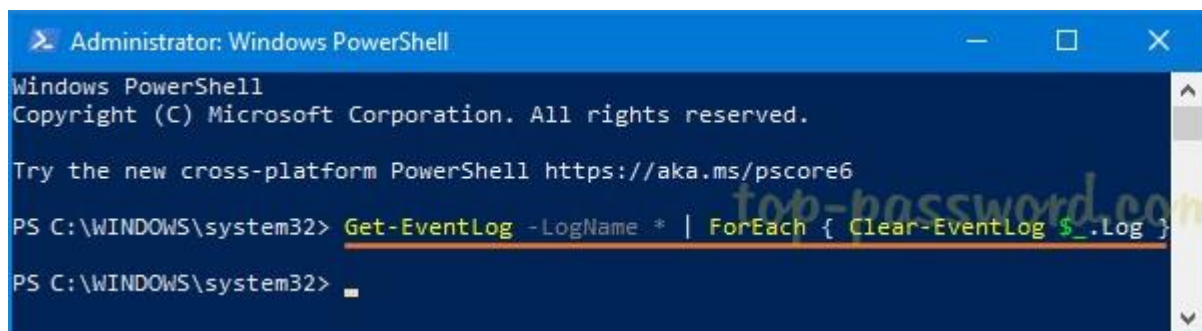
### Method 3: Clear Windows Event Logs Using PowerShell:-

Press the Windows logo key + X to open the Quick Link menu, and then click on “**Windows PowerShell (Admin)**”.



To clear all event logs in Windows 10, just enter the below command and press Enter.

**Get-EventLog -LogName \* | ForEach { Clear-EventLog \$\_.Log }**



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\WINDOWS\system32> Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }
PS C:\WINDOWS\system32> 
```