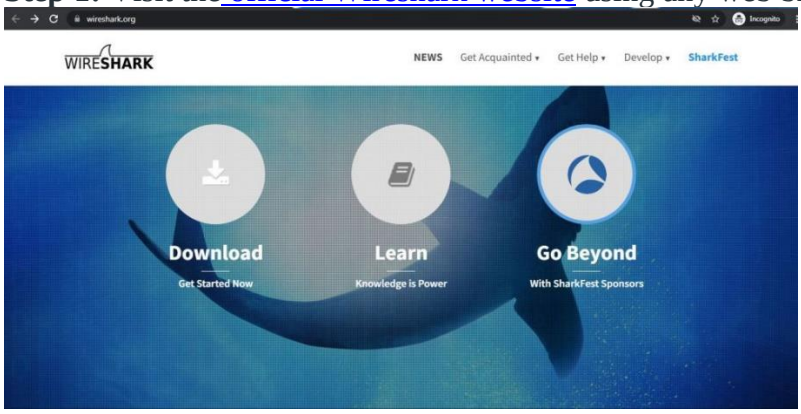
TASK-3

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.

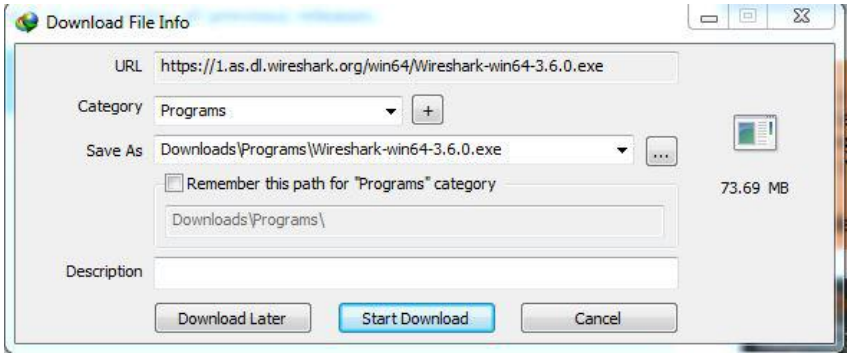
wireshark installation:-

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

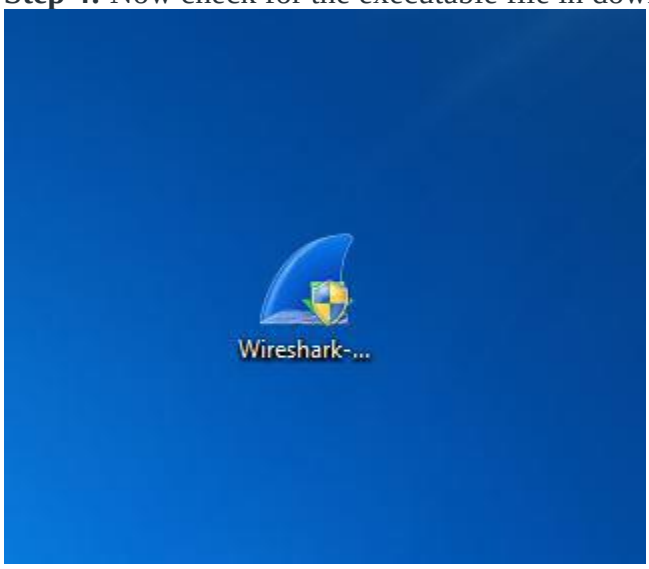


Step 2: Click on Download, a new webpage will open with different installers of Wireshark.

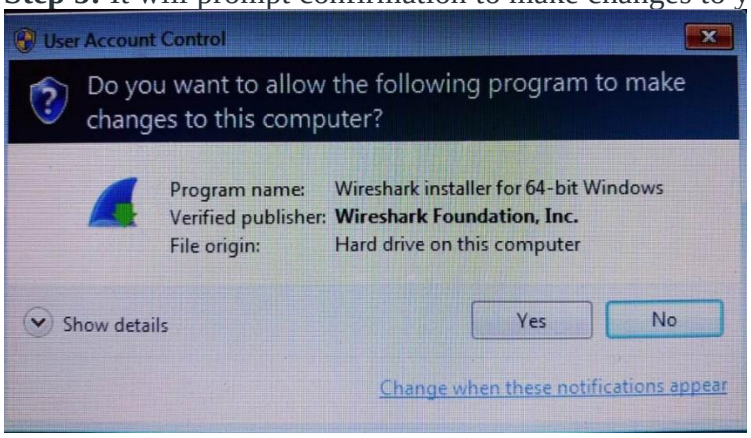
Step 3: Downloading of the executable file will start shortly. It is a small 73.69 MB file that will take some time.



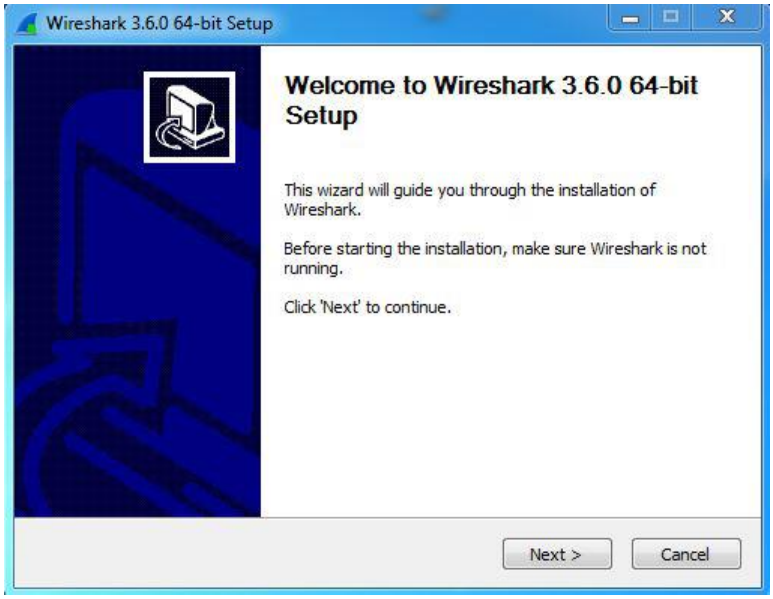
Step 4: Now check for the executable file in downloads in your system and run it.



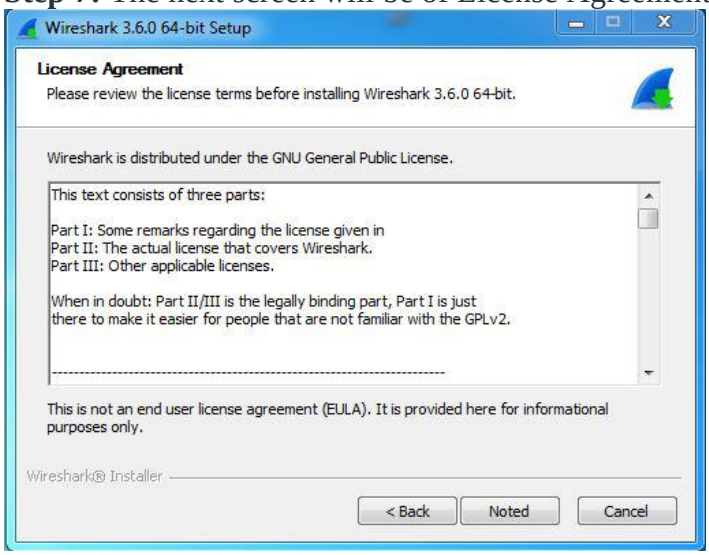
Step 5: It will prompt confirmation to make changes to your system. Click on Yes.



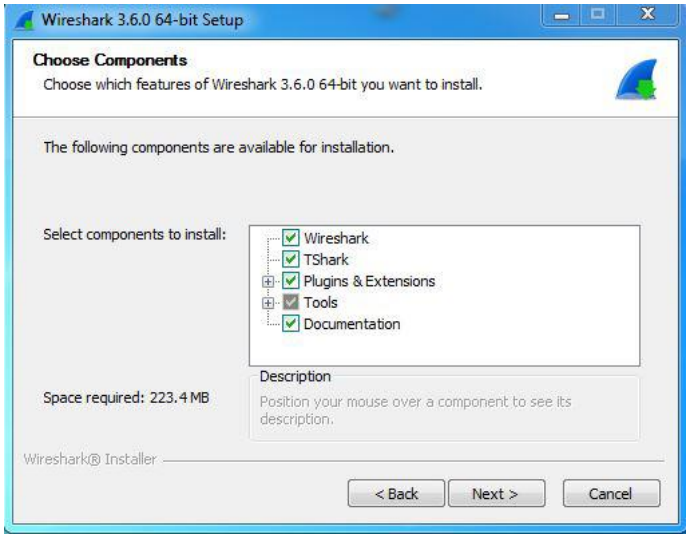
Step 6: Setup screen will appear, click on Next.



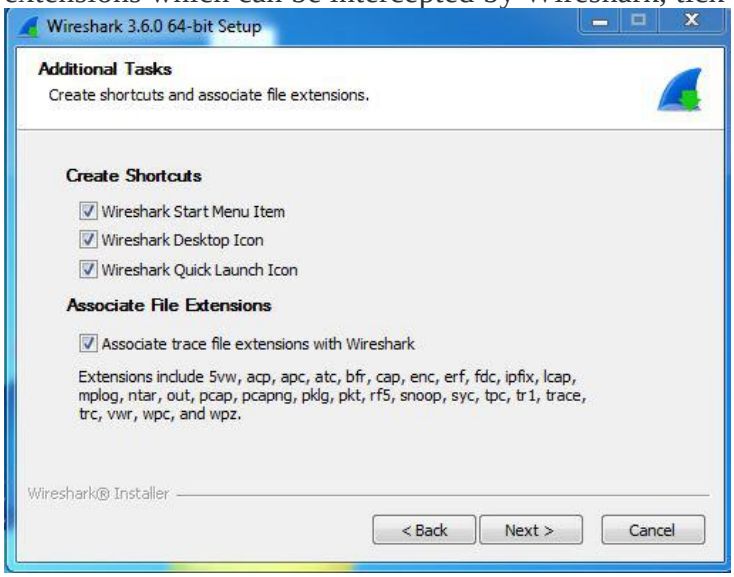
Step 7: The next screen will be of License Agreement, click on Noted.



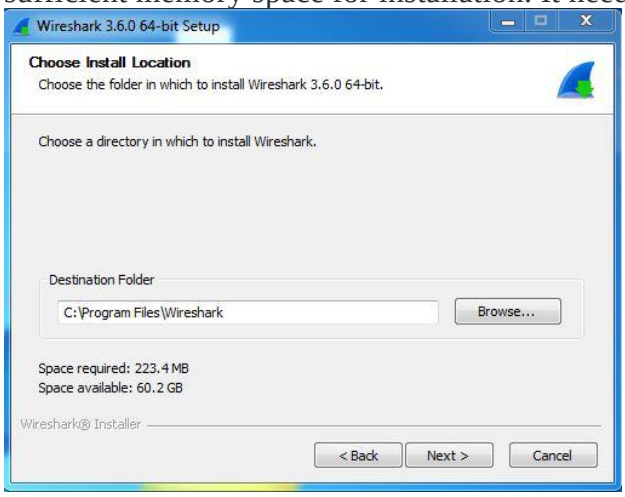
Step 8: This screen is for choosing components, all components are already marked so don't change anything just click on the Next button.



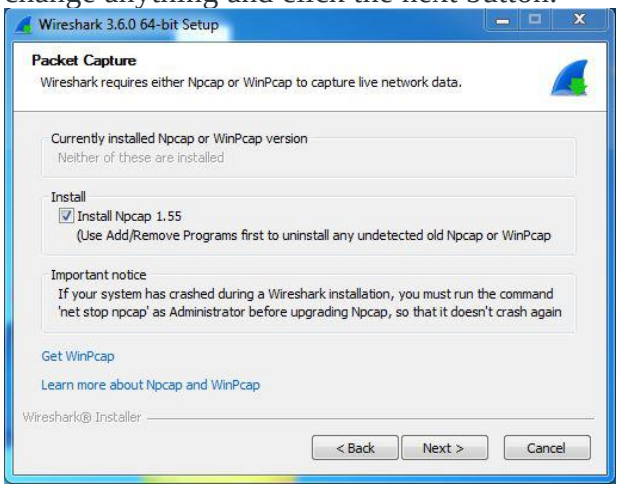
Step 9: This screen is of choosing shortcuts like start menu or desktop icon along with file extensions which can be intercepted by Wireshark, tick all boxes and click on Next button.



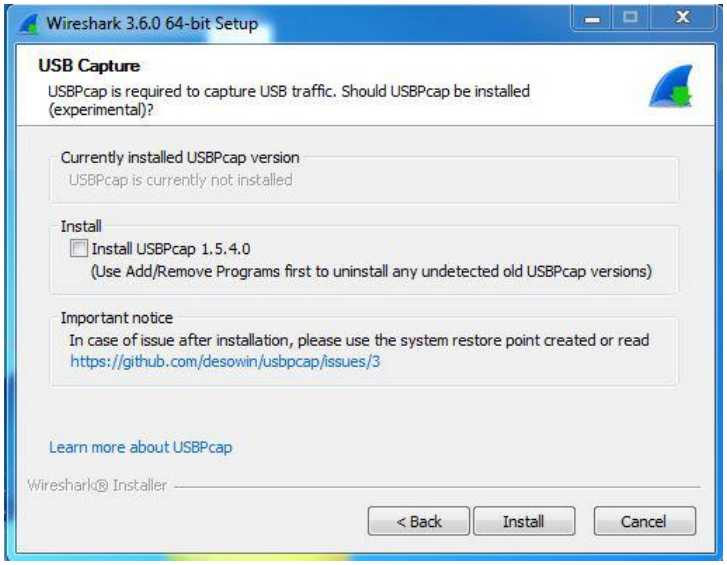
Step 10: The next screen will be of installing location so choose the drive which will have sufficient memory space for installation. It needed only a memory space of 223.4 MB.



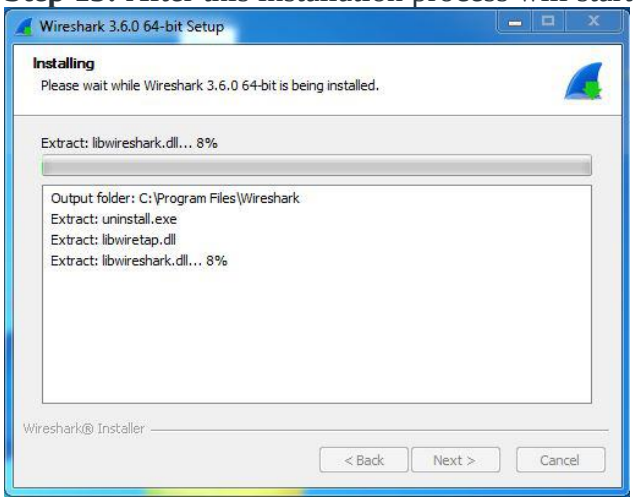
Step 11: Next screen has an option to install Npcap which is used with Wireshark to capture packets *pcap* means packet capture so the install option is already checked don't change anything and click the next button.



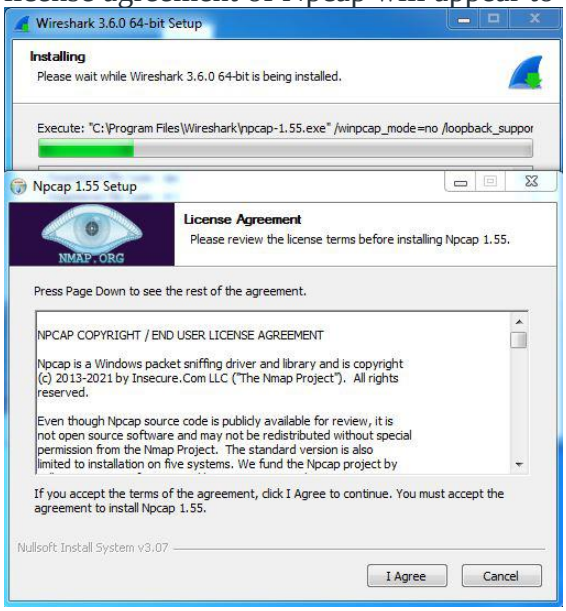
Step 12: Next screen is about USB network capturing so it is one's choice to use it or not, click on Install.



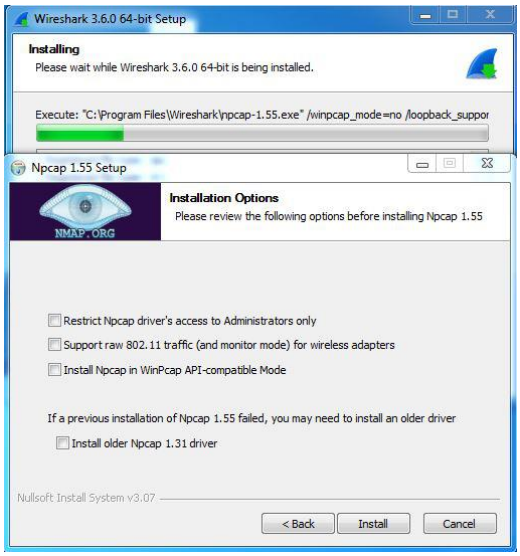
Step 13: After this installation process will start.



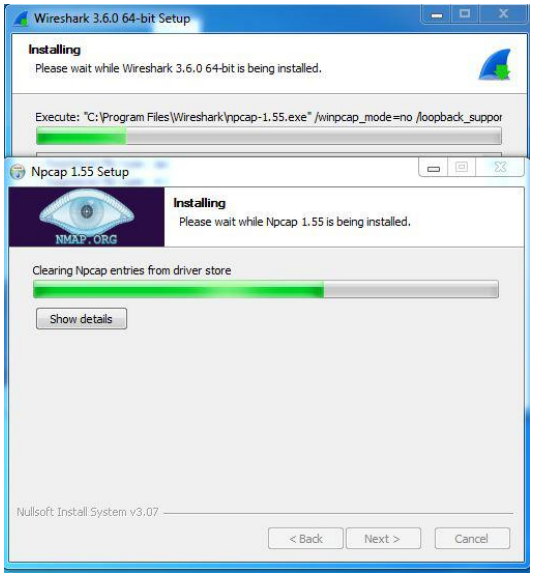
Step 14: This installation will prompt for Npcap installation as already checked so the license agreement of Npcap will appear to click on the *I Agree* button.



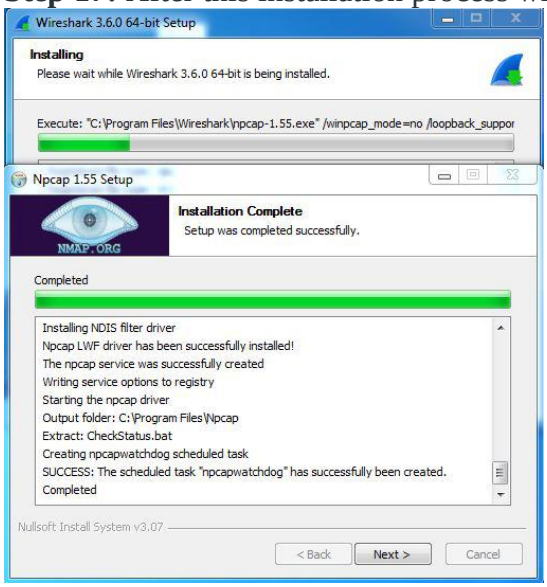
Step 15: Next screen is about different installing options of *npcap*, don't do anything click on Install.



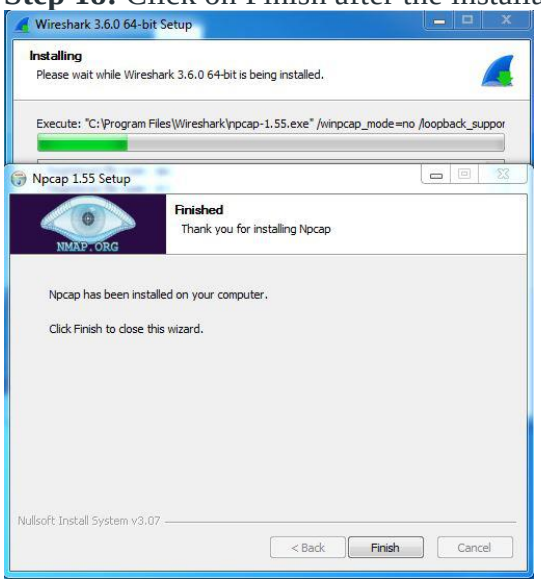
Step 16: After this installation process will start which will take only a minute.



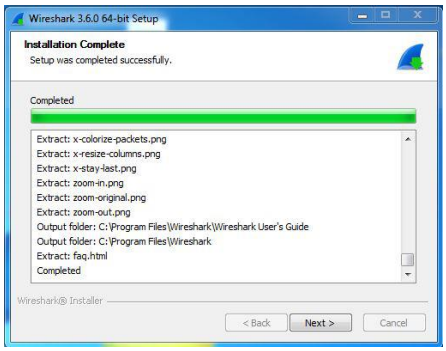
Step 17: After this installation process will complete click on the Next button.



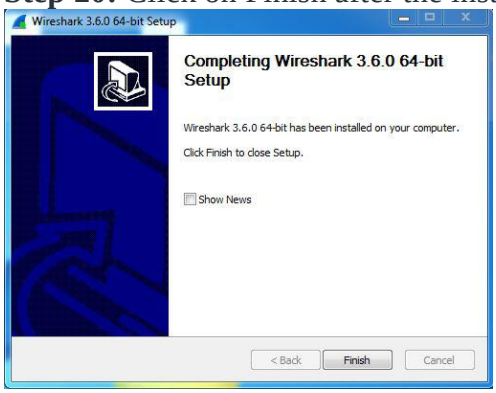
Step 18: Click on Finish after the installation process is complete.



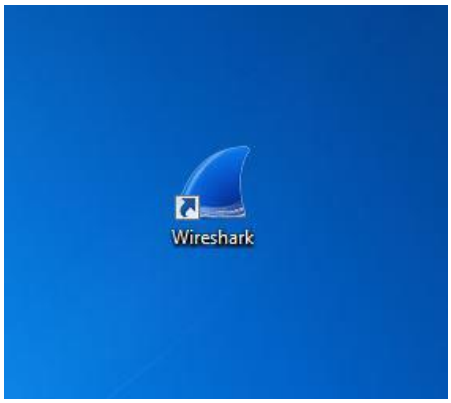
Step 19: After this installation process of Wireshark will complete click on the Next button.



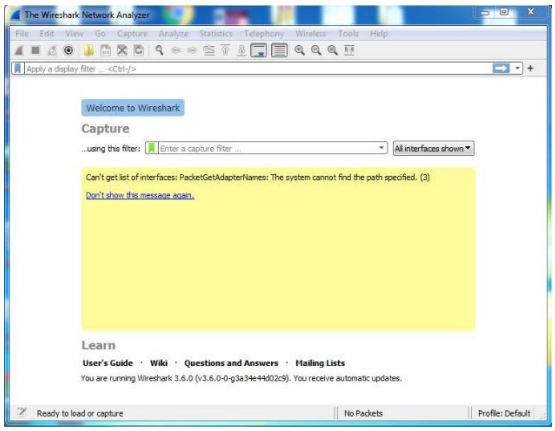
Step 20: Click on Finish after the installation process of Wireshark is complete.



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

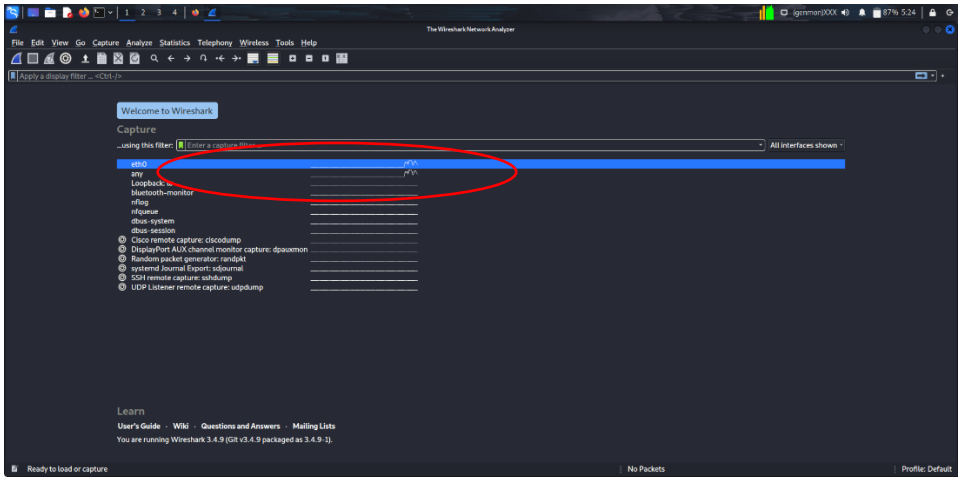


Now run the software and see the interface.

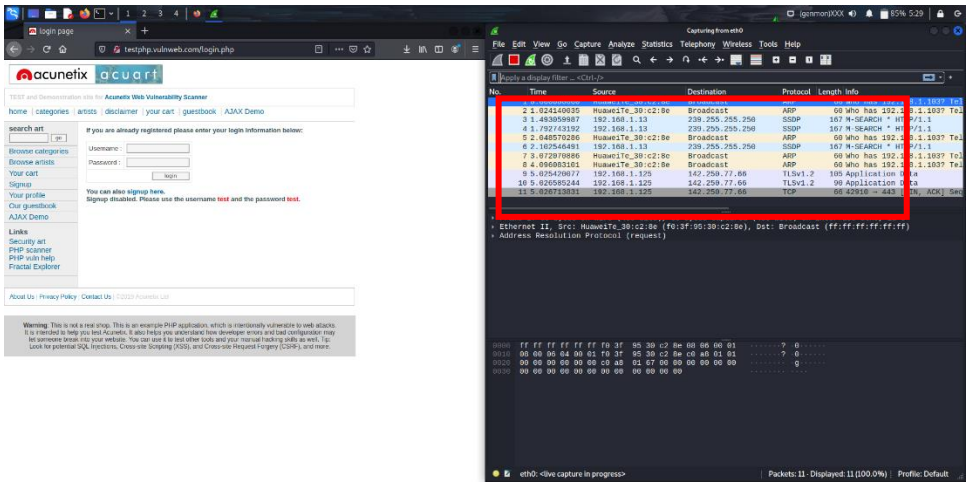


Sniffing http packets using wireshark:-

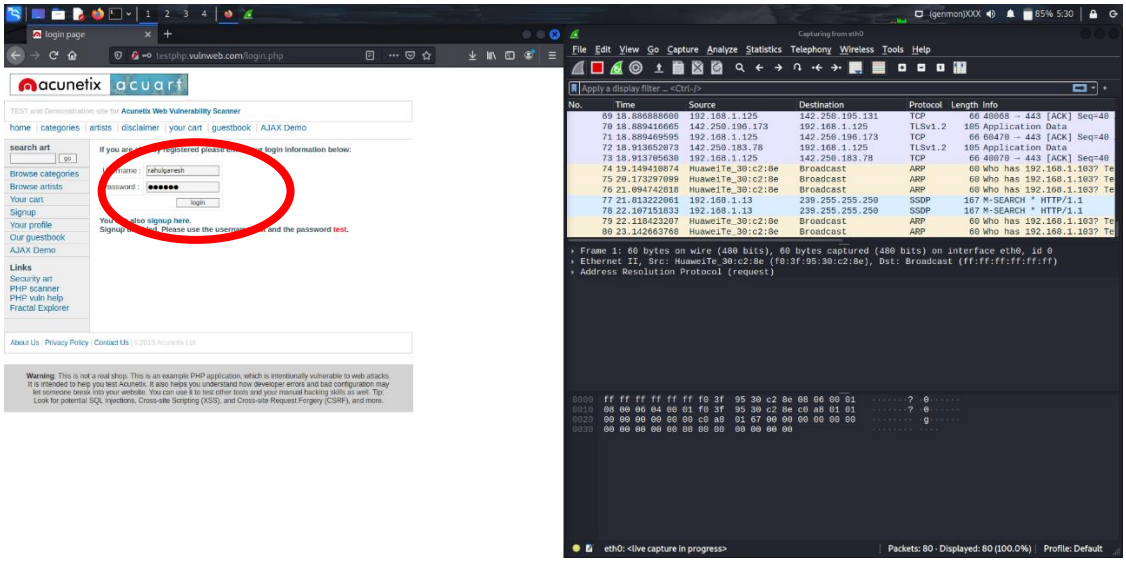
Step 1:- we open wireshark and see the pulse running on the network connection.



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



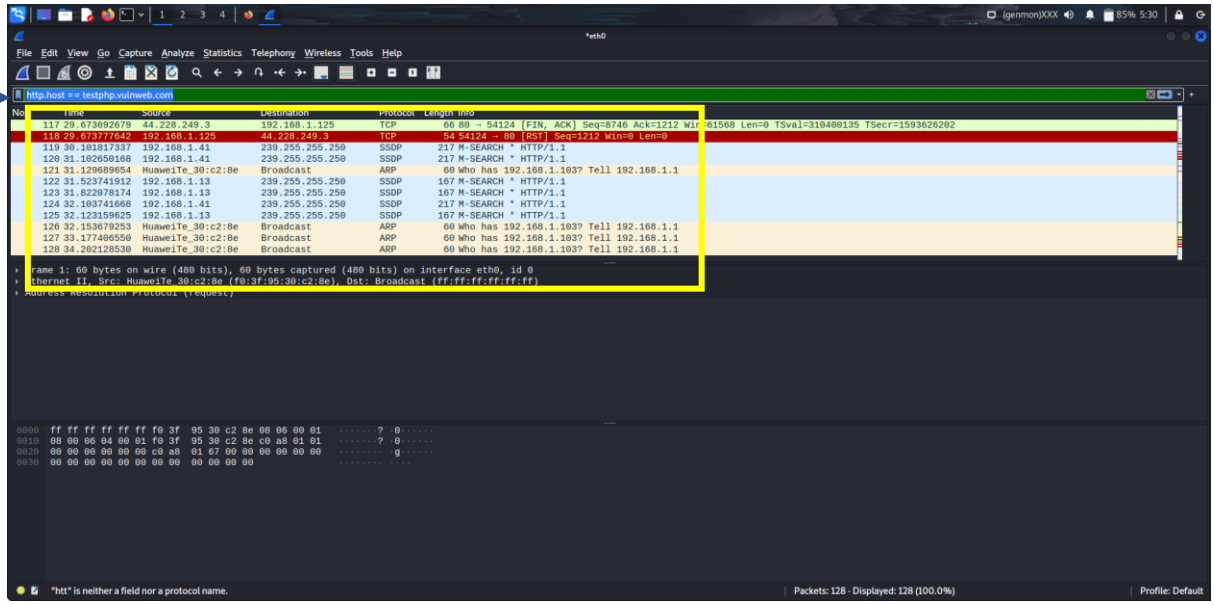
Step 3:- now in the adjacent web page we enter our credential details.

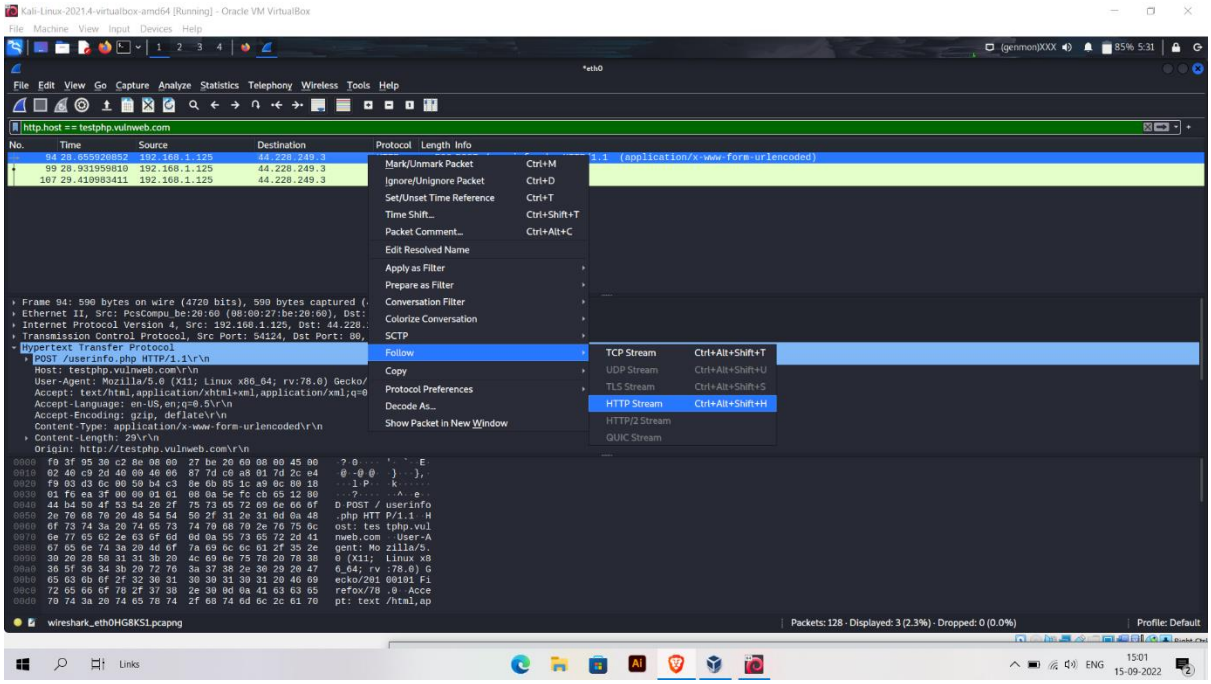


Step 4:- we hit enter and stop the wireshark, so that it stops to capture the packets. And now we filter the packets in the filter box, by giving <protocol>.host == <domain name>

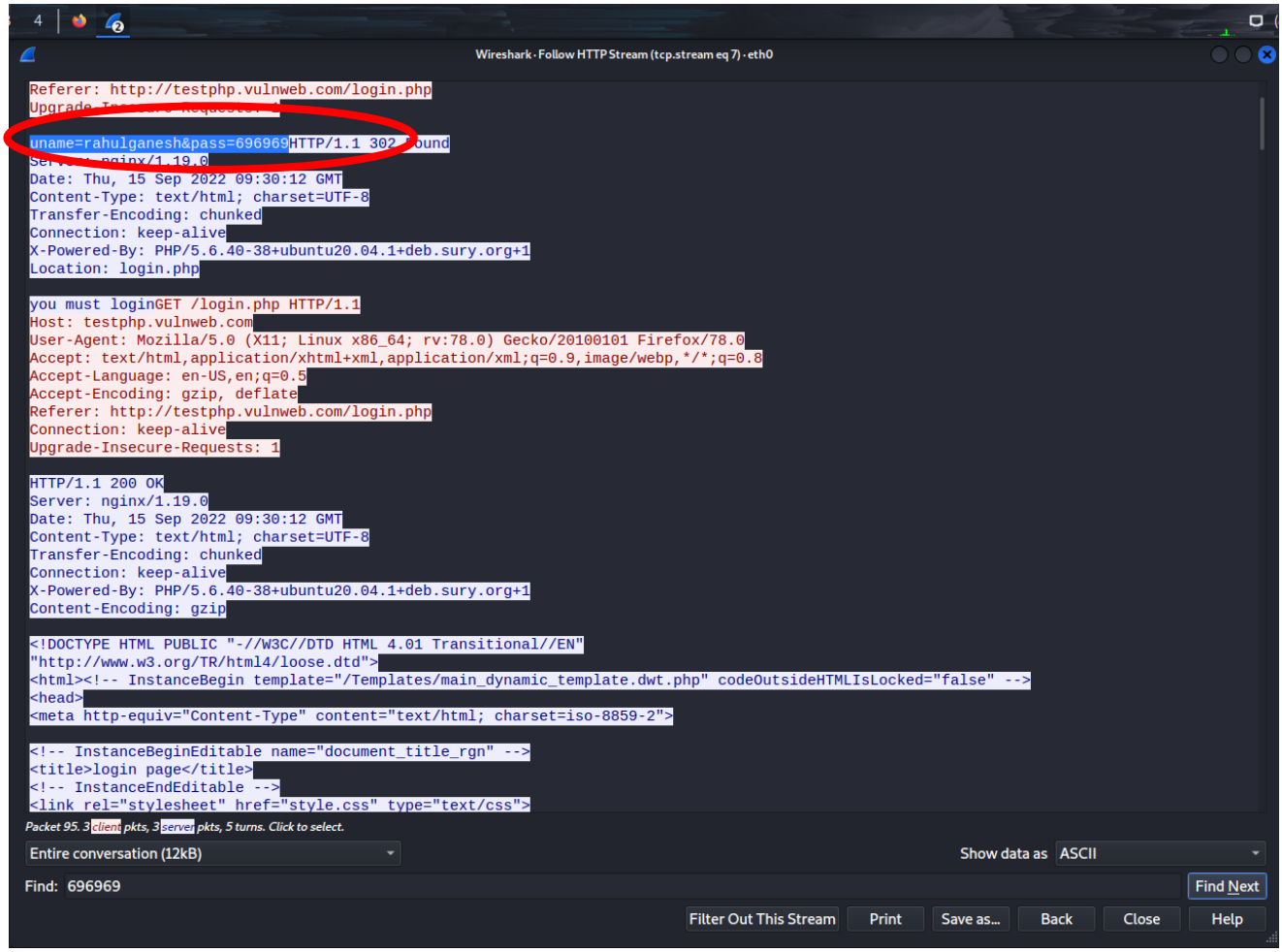
Ex:- “http.host==testphp.vulnweb.com”.

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.


Wireshark · Follow HTTP Stream (tcp.stream eq 7) · eth0
Referer: http://testphp.vulnweb.com/login.php
uname=rahulganesh&pass=696969HTTP/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" codeOutsideHTMLIsLocked="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