OPEN SOURCES TECHNOLOGIES

CA: 3

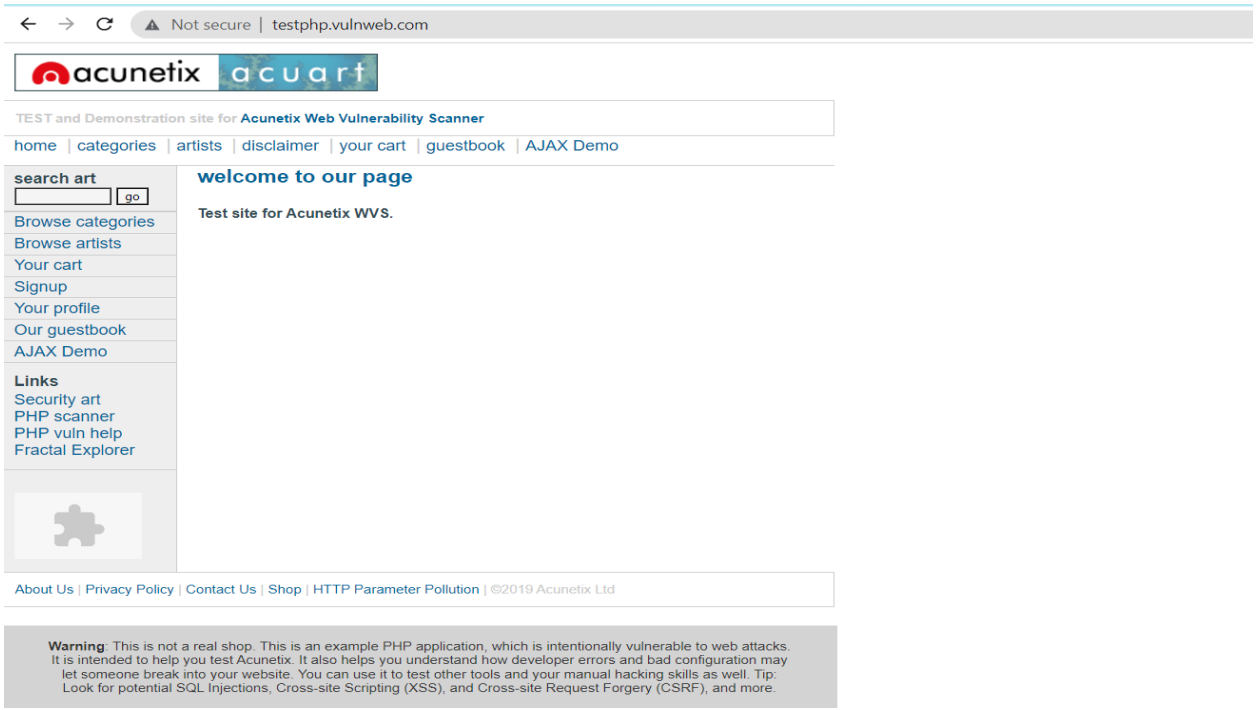
Name : Banagani Prashanth
Reg No : 11906733
Course Code : INT301
Roll No : 44
Section : KE011

Q : Suppose you are a network analyst and implemented the sensor inside the firewall, working in the Infotech department of LPU. You have been assigned the responsibility of inspecting HTTP Traffic and retrieving the Username and password from http://testphp.vulnweb.com/ website. Write the steps involved in scanning the port.

As network analysts, we can use a network protocol analyzer tool like Wireshark to inspect HTTP traffic and retrieve the username and password from the http://testphp.vulnweb.com/ website.

Wireshark is a free and open-source network protocol analyzer. It is used for network troubleshooting, analysis, software and communications protocol development.It can capture packets from a network connection in real-time and display them at a granular level. Once these packets are broken down, you can use them for real-time or offline analysis.

We need to open the website in our search engine to verify its IP address while performing these tasks



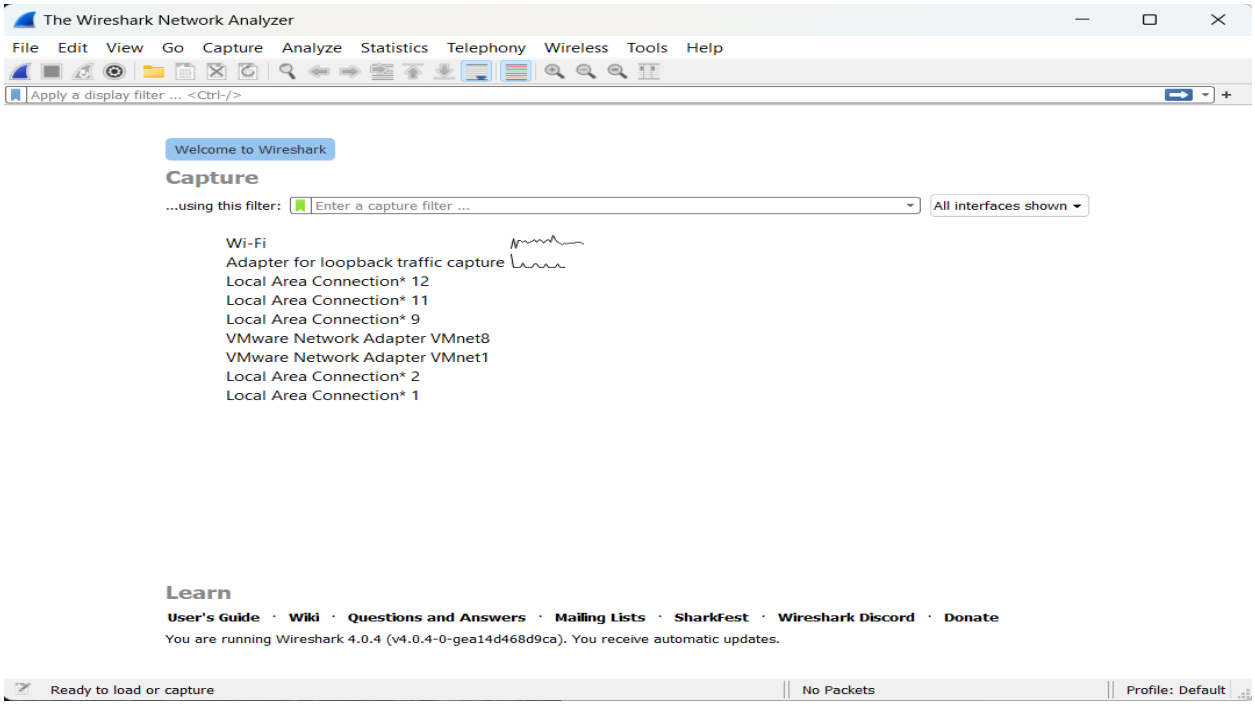
To check the IP address of the website, we are going to use the ping command through the command prompt.

Command : ping testphp.vulnweb.com

```
Command Prompt

Microsoft Windows [Version 10.0.22621.1413]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Asus>ping testphp.vulnweb.com

Pinging testphp.vulnweb.com [44.228.249.3] with 32 bytes of data:
Reply from 44.228.249.3: bytes=32 time=367ms TTL=34
Reply from 44.228.249.3: bytes=32 time=339ms TTL=34
Reply from 44.228.249.3: bytes=32 time=331ms TTL=34
Reply from 44.228.249.3: bytes=32 time=299ms TTL=34

Ping statistics for 44.228.249.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 299ms, Maximum = 367ms, Average = 334ms

C:\Users\Asus>
```

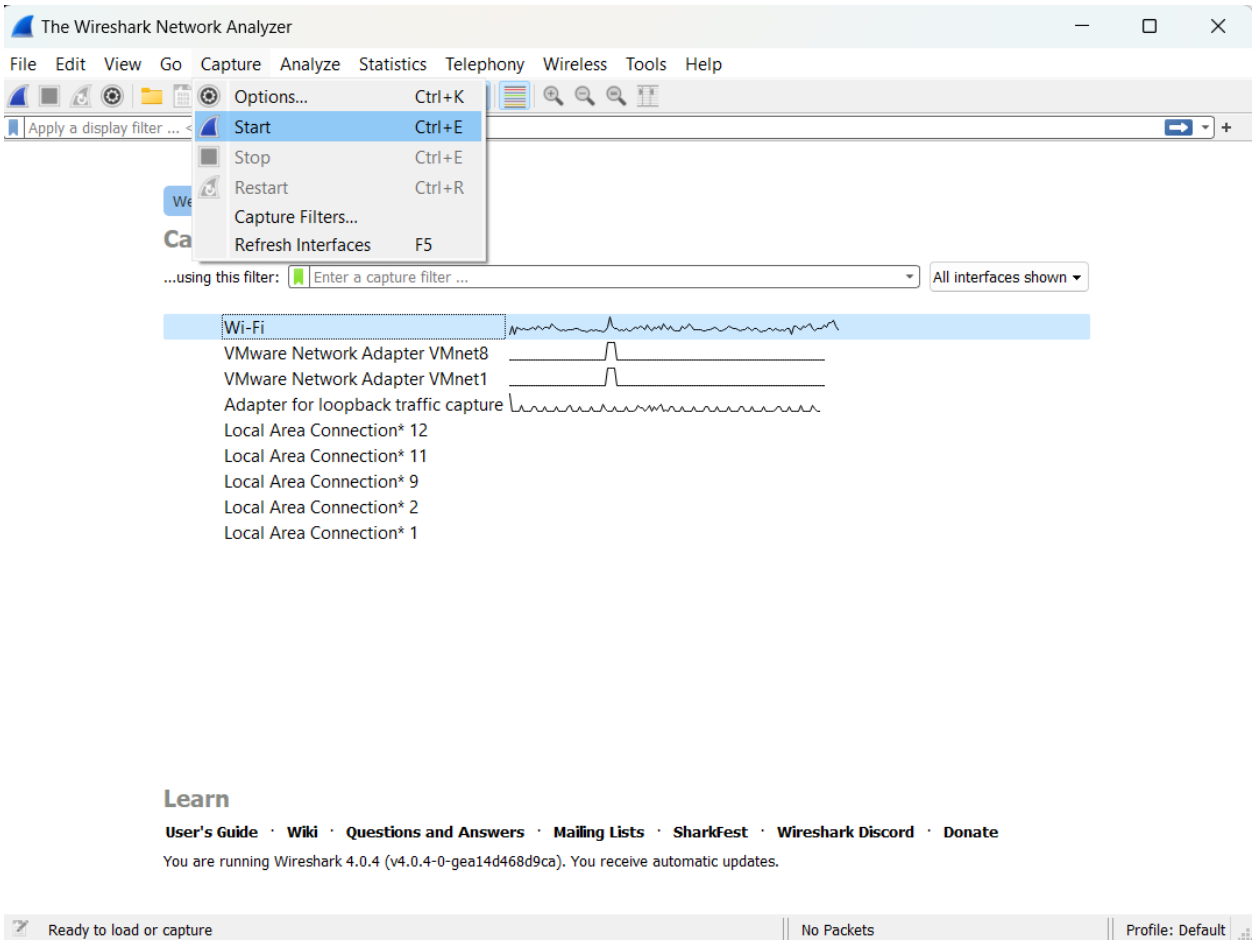
Follow these steps to inspect HTTP traffic and retrieve the username and password from the website:

1.Open Wireshark.

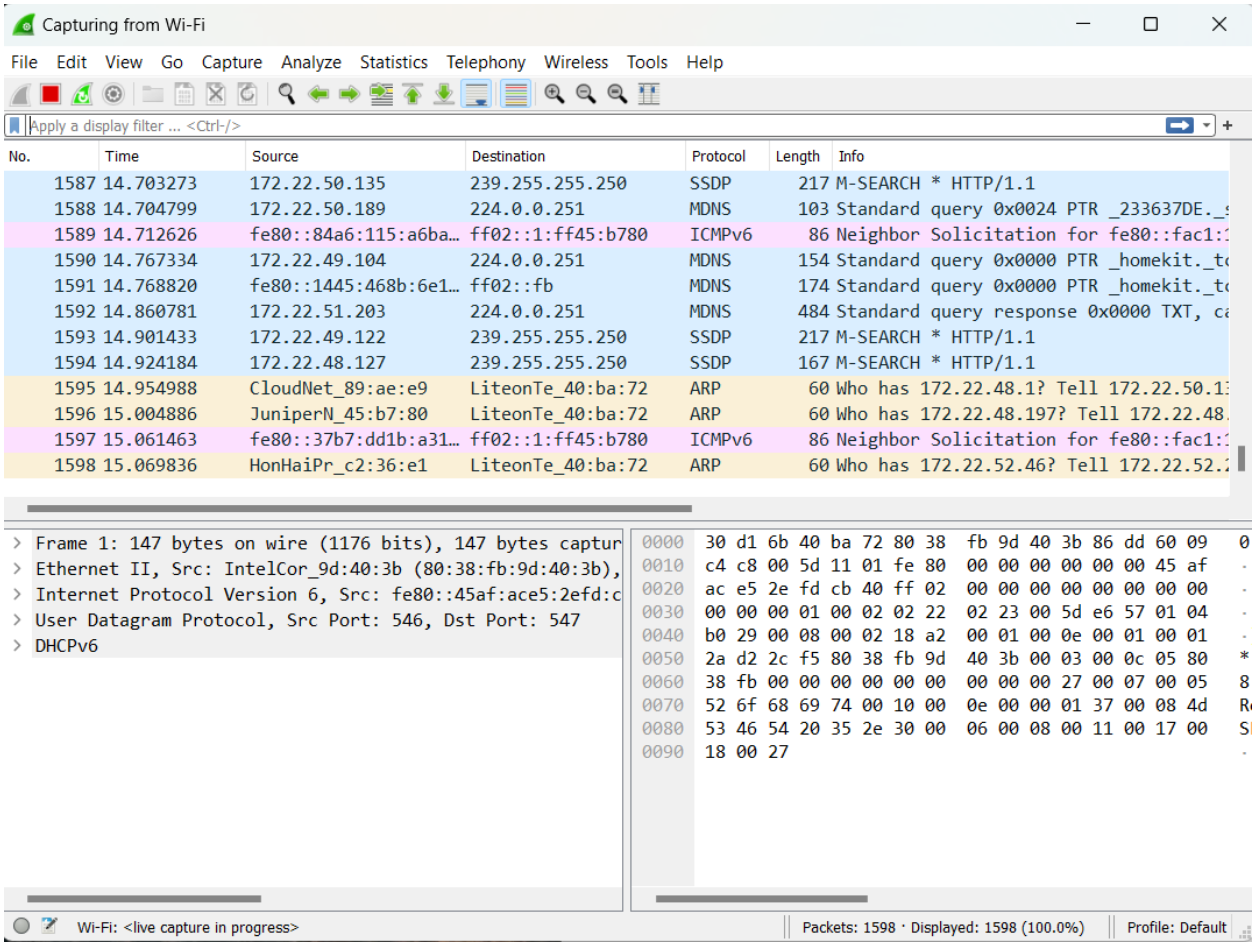


1. In the main window, you will see a list of available network interfaces under the “Capture” section.
2. Identify the network interface that is connected to the internet. It could be a wired or wireless connection and is usually labeled as “Ethernet” or “Wi-Fi”.
3. Click on the interface to select it.

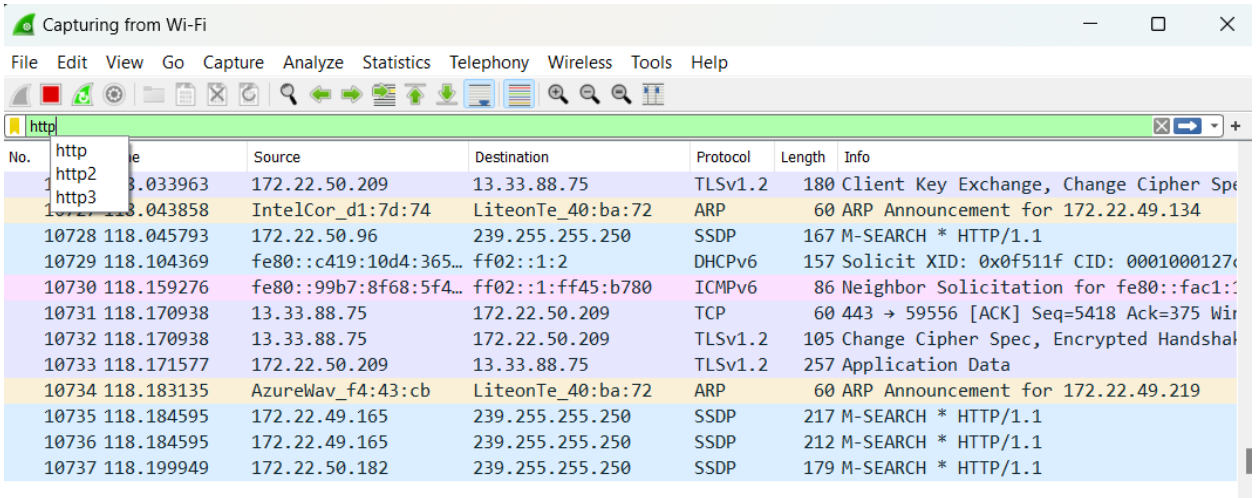
Once you have selected the network interface, you can start capturing packets by clicking on the “Start Capture” button.



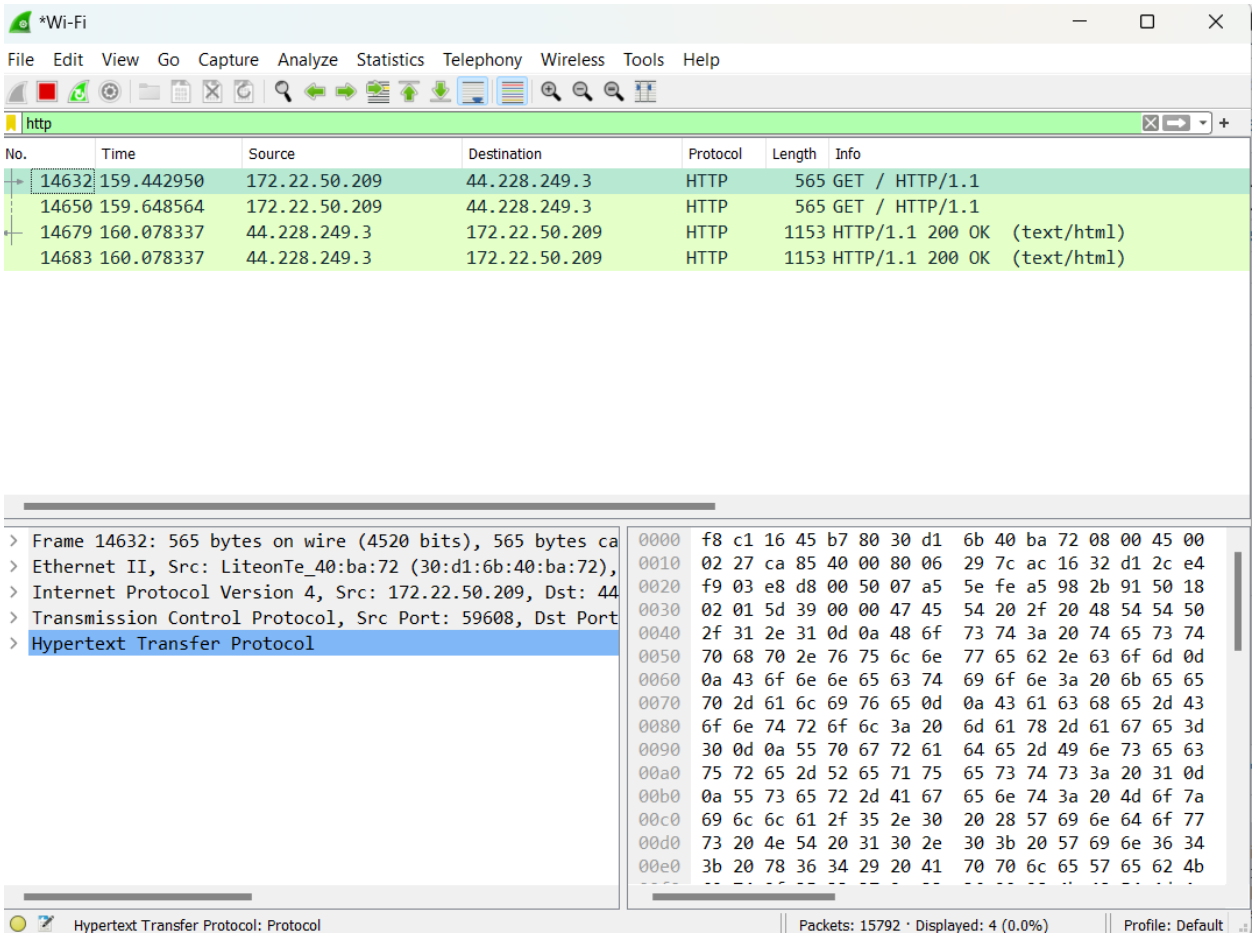
After Clicking on start capture button:



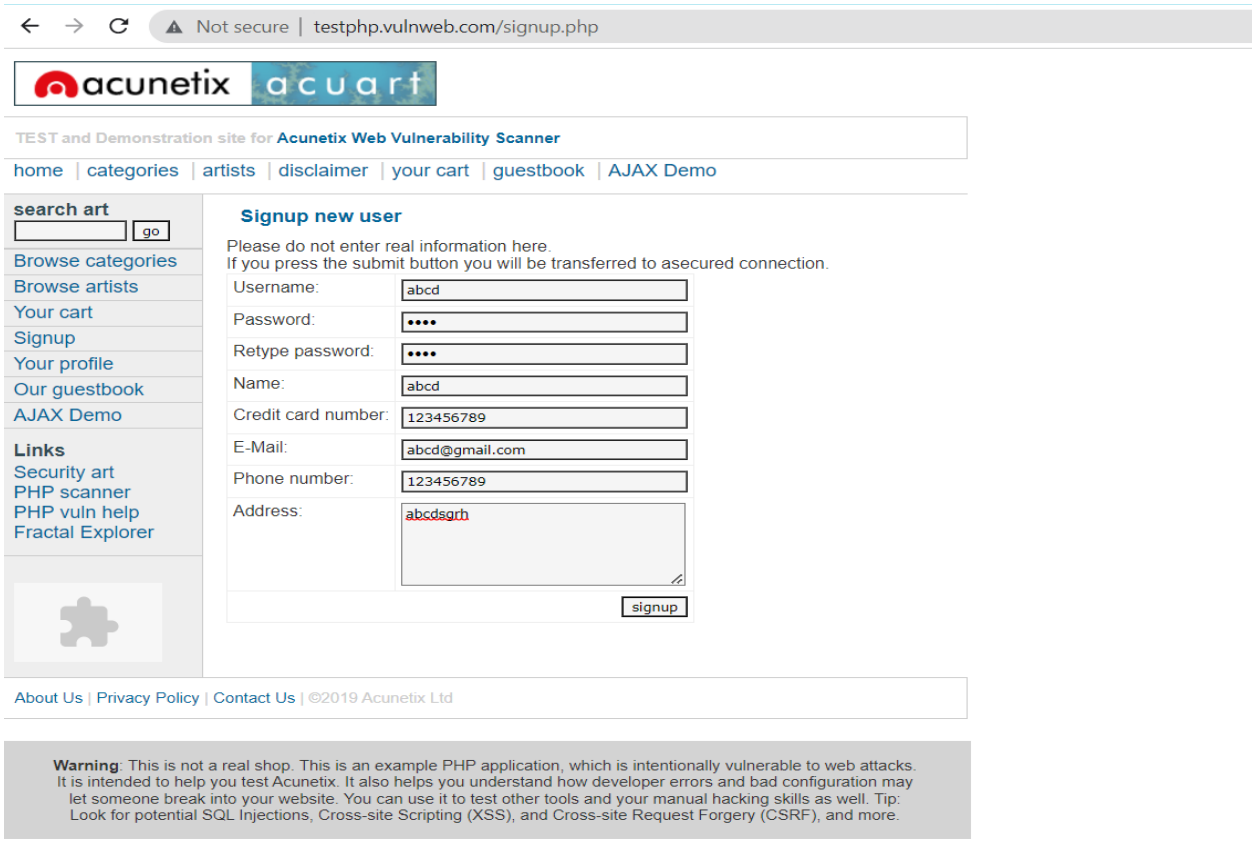
After you have started capturing packets and entered “http” in the filter bar to display only HTTP traffic, look for packets in the packet list pane that have the “POST” method in the “Info” column.



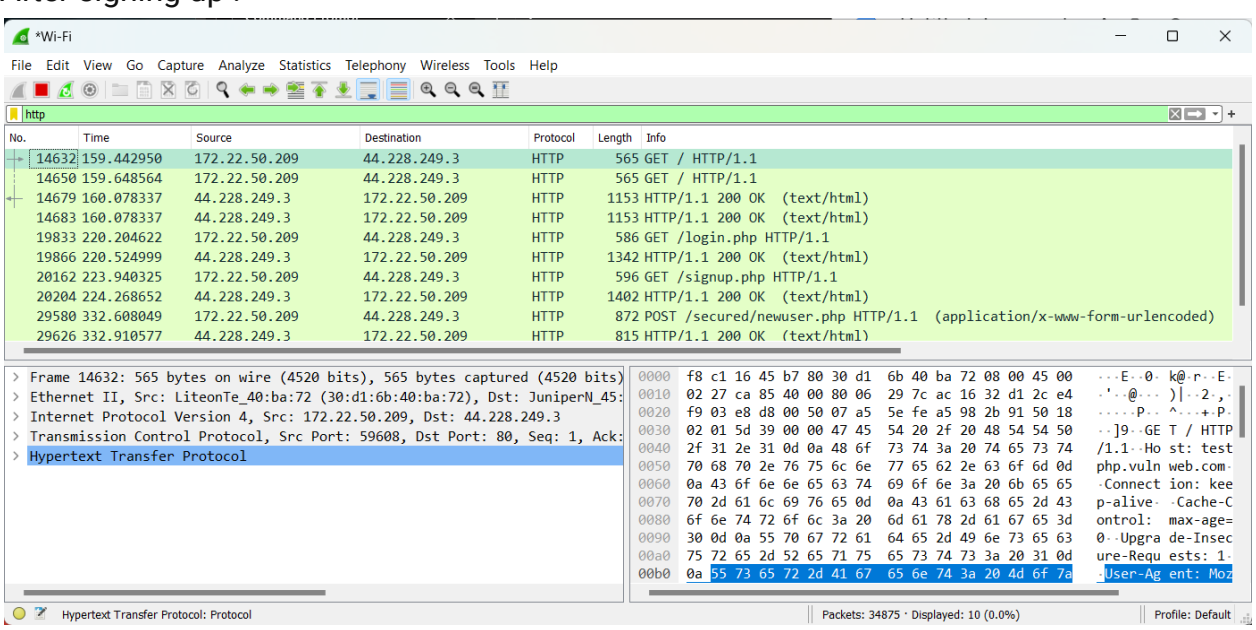
If you see a packet with the “POST” method, select it by clicking on it.



If you don’t see any packets with the “POST” method while capturing HTTP traffic in Wireshark, it could mean that no data is being sent to the server from the website you are trying to inspect.Try refreshing the website or performing an action on the website that would send data to the server, such as submitting a form or logging in.

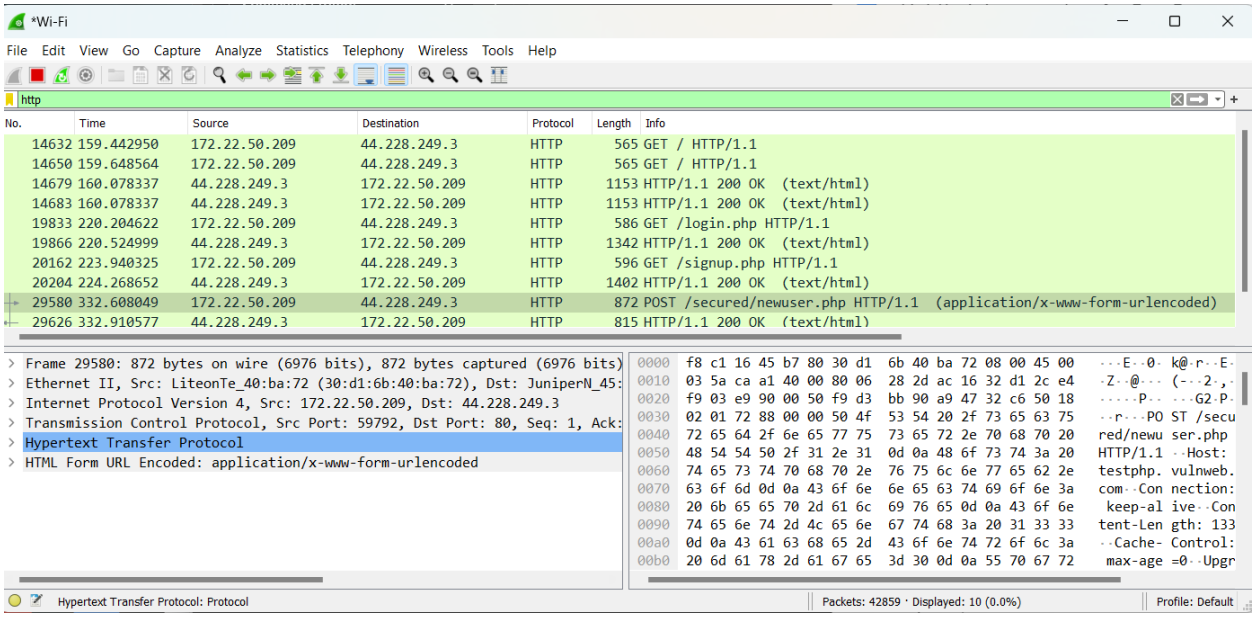


After signing up :

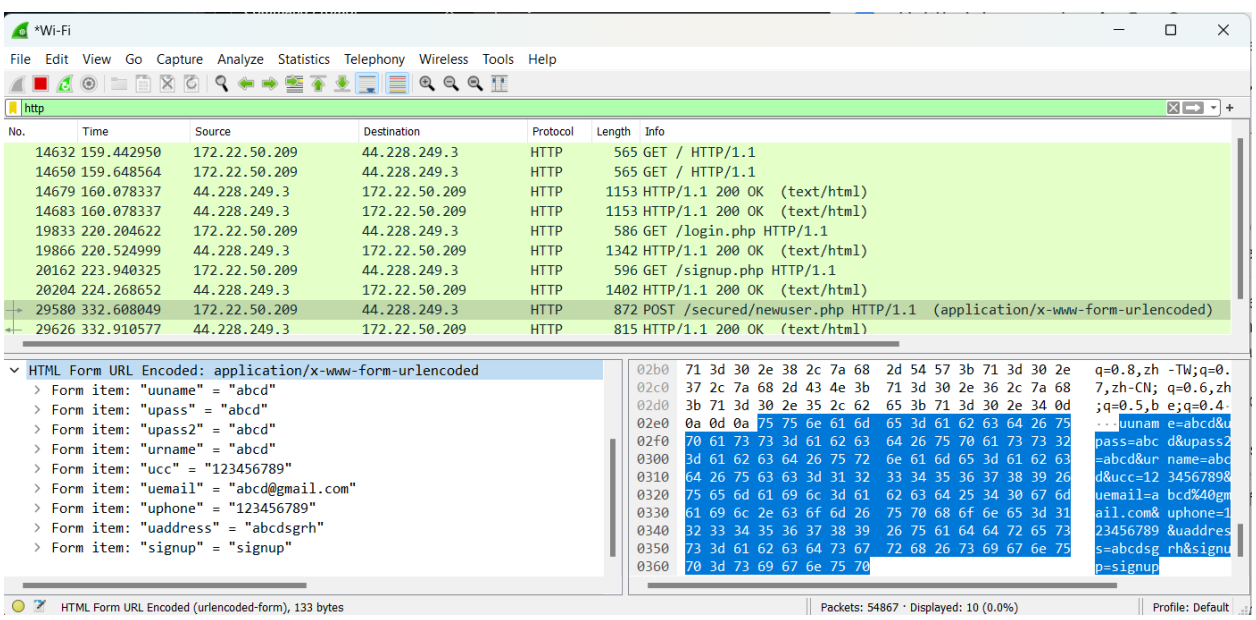


Now that you can see packets with the “POST” method in Wireshark, you can proceed to the next step which is to select the packet and expand the “Hypertext Transfer Protocol” section in the packet details pane. Here’s how you can do it:

1. Select the packet with the “POST” method by clicking on it in the packet list pane.
2. In the packet details pane, look for the “Hypertext Transfer Protocol” section and click on the “>” icon next to it to expand it.



3. Look for the “Form item” field which contains the username and password



The “Form item” field in the “Hypertext Transfer Protocol” section of a packet in Wireshark displays the data that is being sent to the server from a form on a website.

The field is usually labeled with the name of the form input element, such as “username” or “password”.

To identify which “Form item” field contains the username and password, you can look for fields that are labeled with names that are commonly used for username and password input elements, such as “username”, “user”, “email”, “login”, “password”, “pass”, etc.

Once you have identified the “Form item” fields that contain the username and password, you can view their values to retrieve the information.

Wireshark is a powerful tool that can be used to inspect HTTP traffic and retrieve information such as usernames and passwords from websites. By following the steps outlined in this report, a network analyst can successfully use Wireshark to capture packets, filter HTTP traffic, and identify packets with the “POST” method to retrieve the desired information. This demonstrates the usefulness of Wireshark as a network protocol analyzer for troubleshooting and analysis purposes.