Ex No-3: **Password Capturing using Wireshark**

Aim:

To capture and analyze network packets using Wireshark.

Requirements:

- Wireshark
- Windows
- Active internet connection or local network traffic

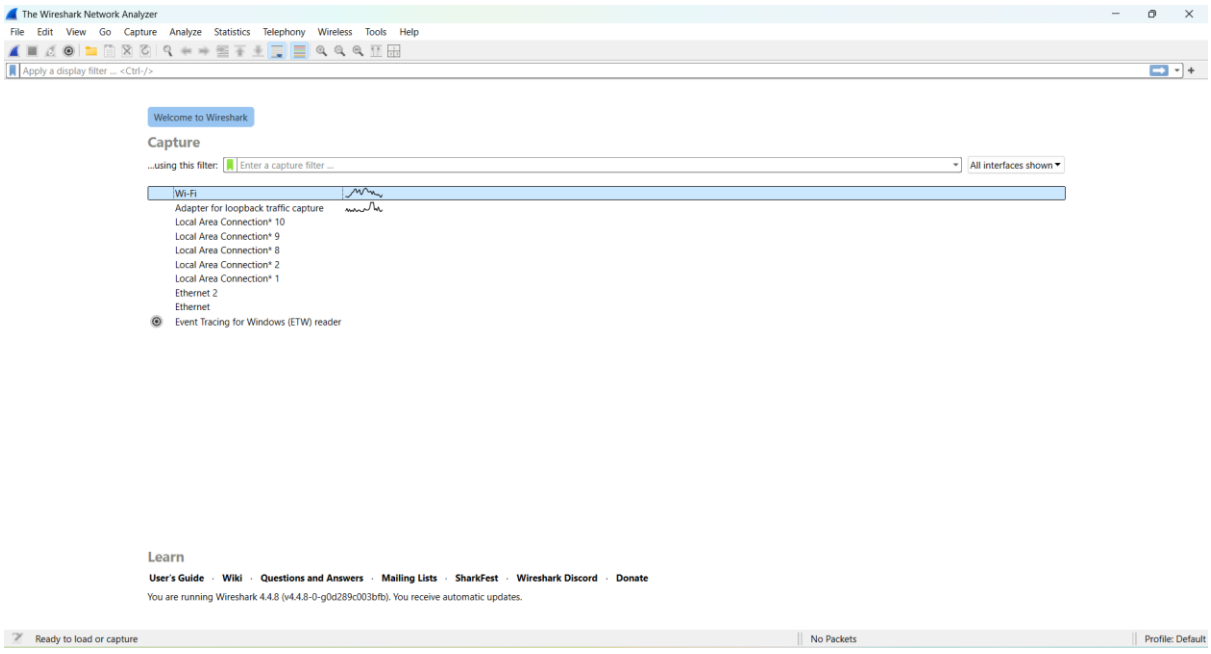
Description:

Wireshark is a popular open-source network protocol analyzer.

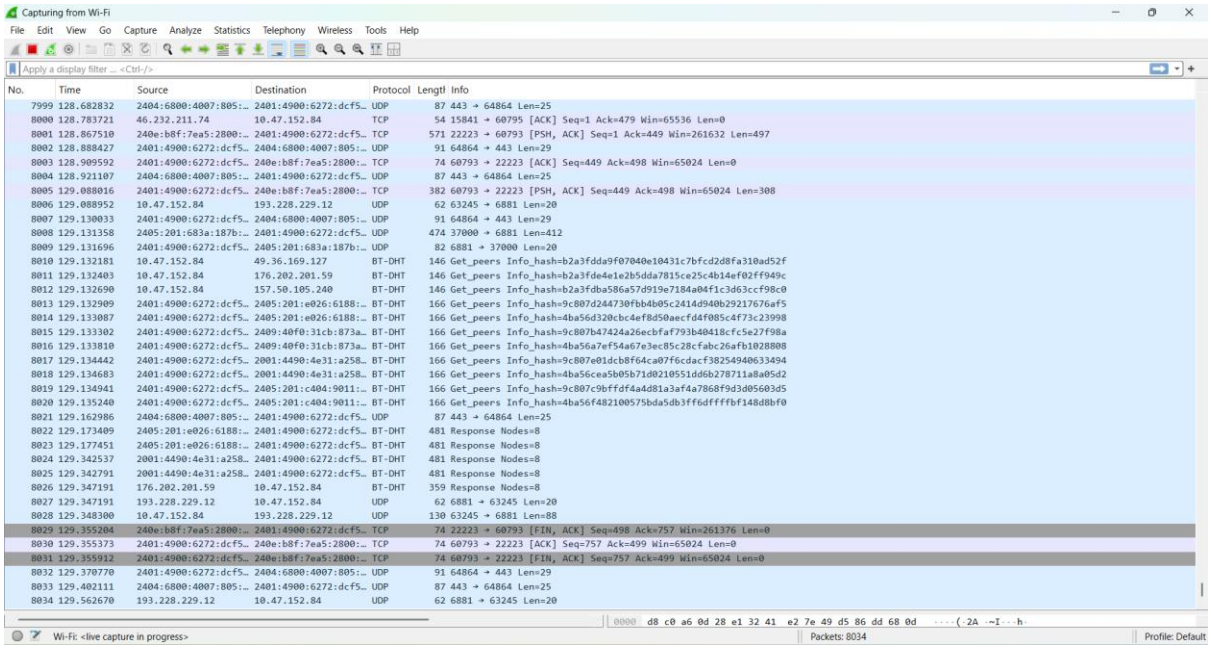
It allows forensic investigators and security analysts to:

- Capture live network traffic
- Inspect packet contents (headers & payloads)
- Filter and search packets (e.g., HTTP, DNS, TCP, ICMP, ARP)
- Detect suspicious or malicious activity
- Reconstruct sessions (e.g., HTTP requests, TCP streams

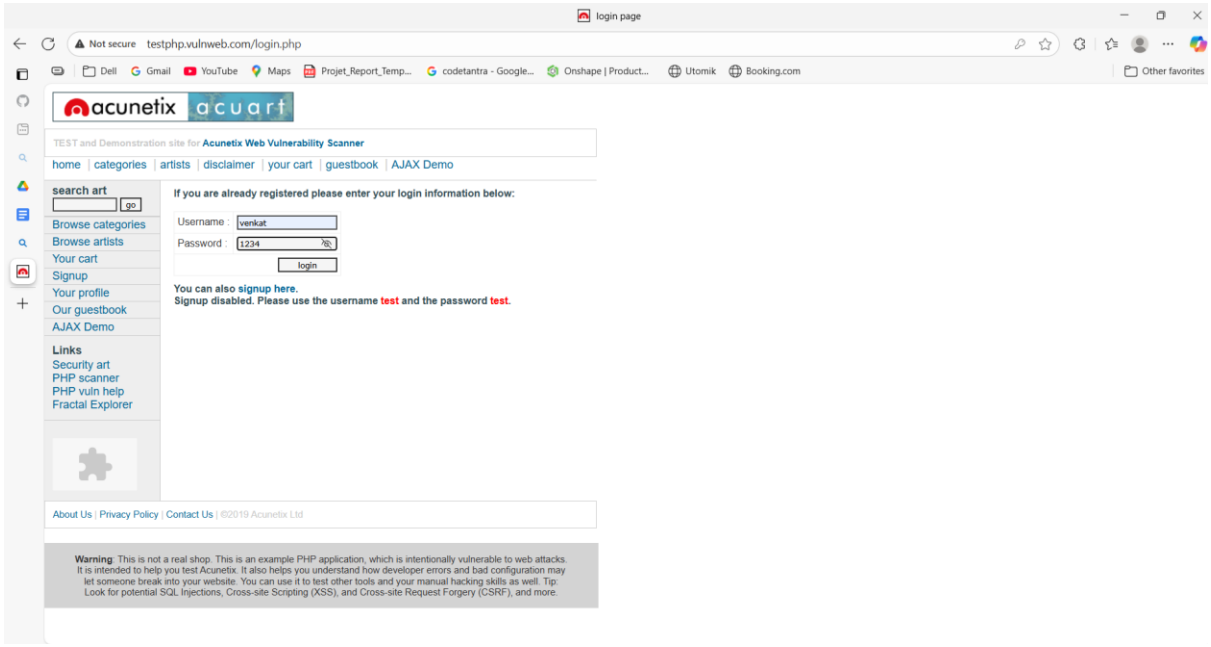
Step-1: Open the Wireshark, there you will see the different types of networks. Select the network that is connected to your network, in this case it is Wi-Fi



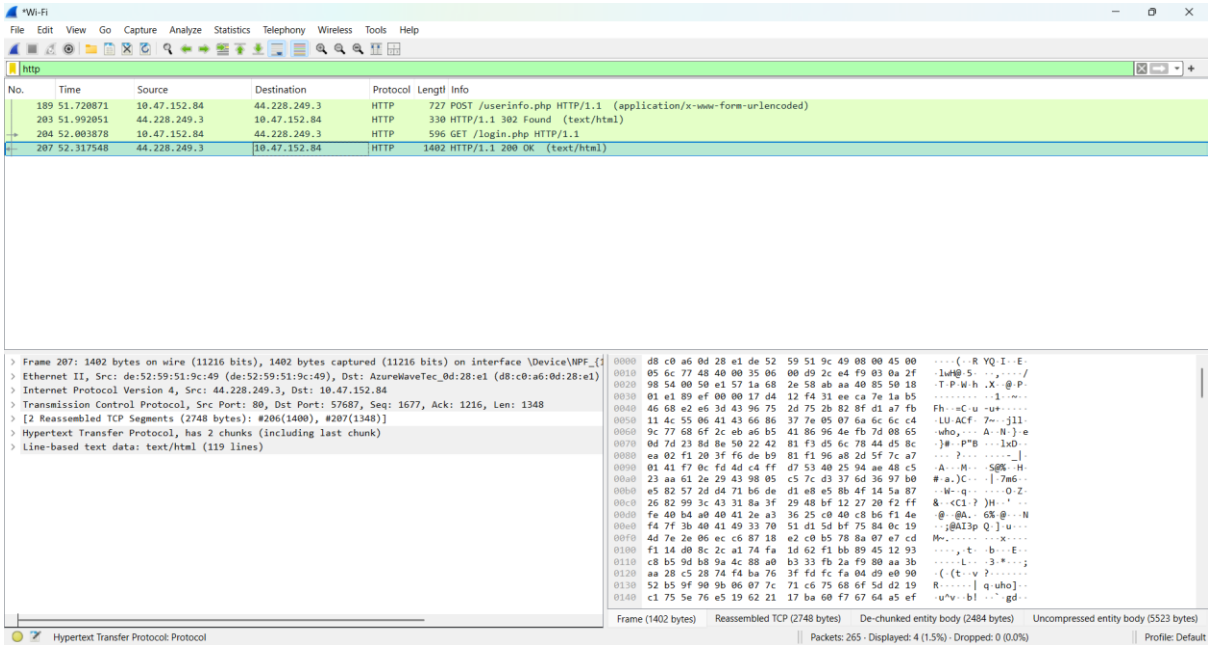
Step-2: On the top right corner you will see blue shark fin, just press the button and Wireshark begins capturing live traffic packets appear in real-time.



Step-3: After starting the packet capturing we will go to the website and login the credential on that website



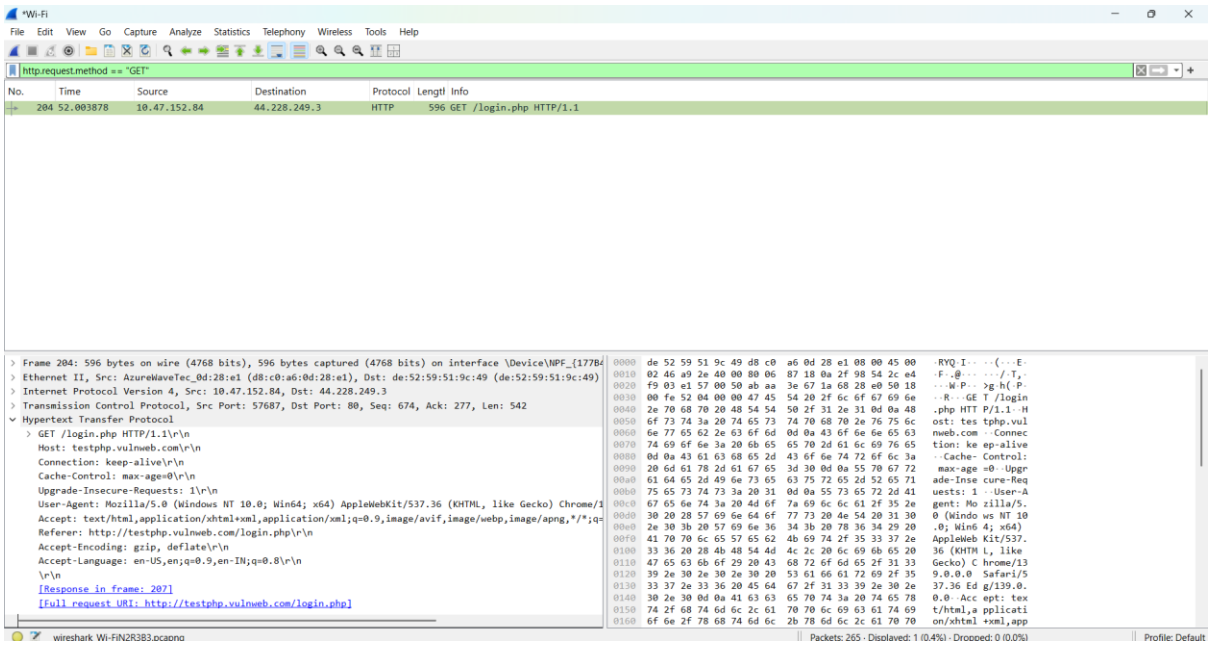
Step-4: Now go to Wireshark tool and apply some filters like HTTP to find the HTTP packets on the network.



Step-5: So, there are some HTTP packets are captured but we specifically looking for form data that the user submitted to the website.

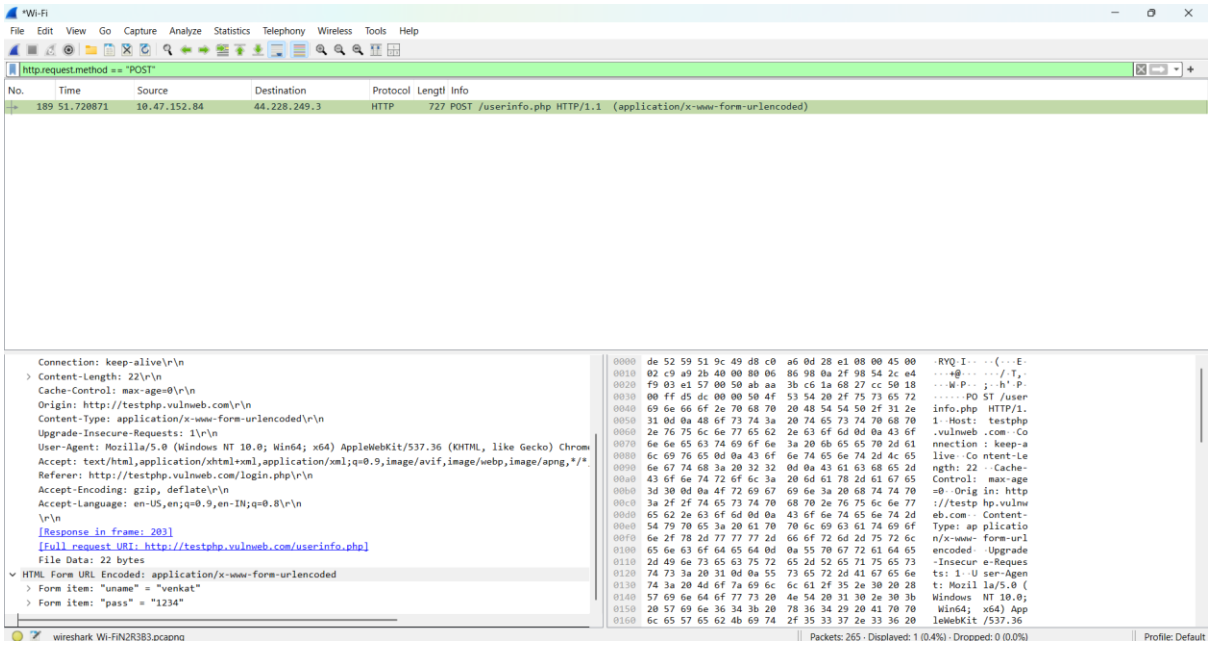
We have main two methods used for submitting form data from web pages like login forms to the server. They are ‘GET’ & ‘POST’

Step-6: So, firstly for knowing the credential we use the first method and apply the filter for the GET methods. http.request.method == “GET”



Step-7: Now after checking the GET method if we didn't find the form data, then we will try the POST method for that we will apply the filter on Wireshark

http.request.method == "POST"



As you can see the HTML form just click that form you can see the user credentials like username and password

Form item: "uname" = "venkat"

Form item: "pass" = "1234"