

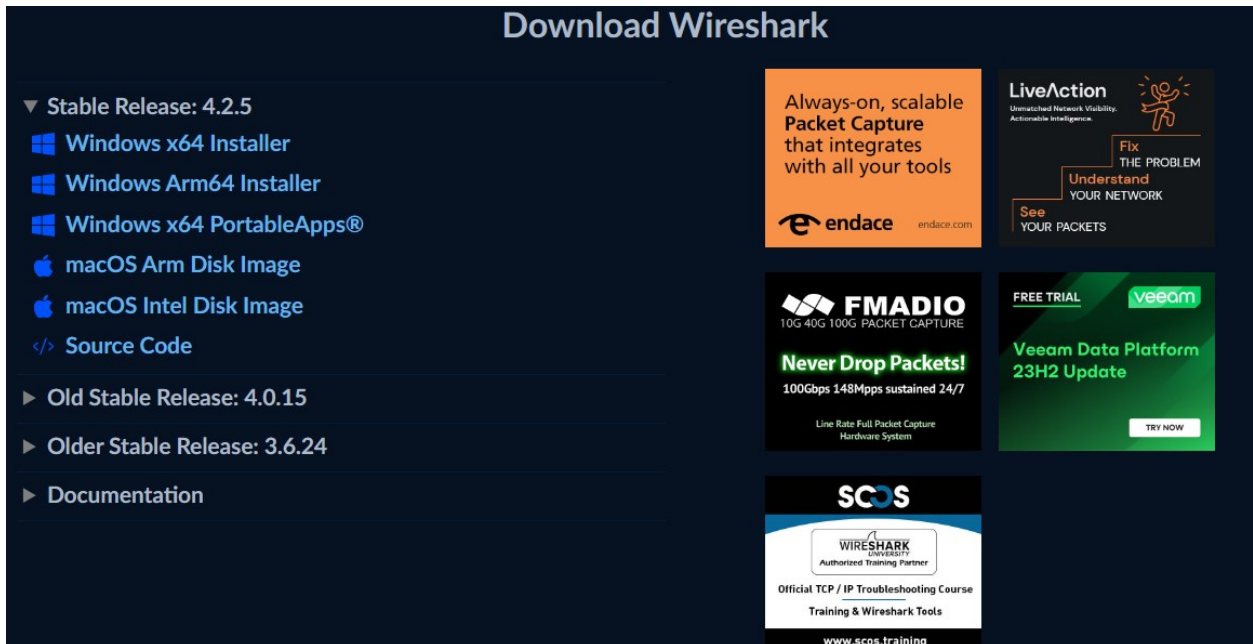
PRACTICAL PROJECT – WIRESHARK

Using Wireshark to find out the weak encryption data

URL: <https://www.wireshark.org/>

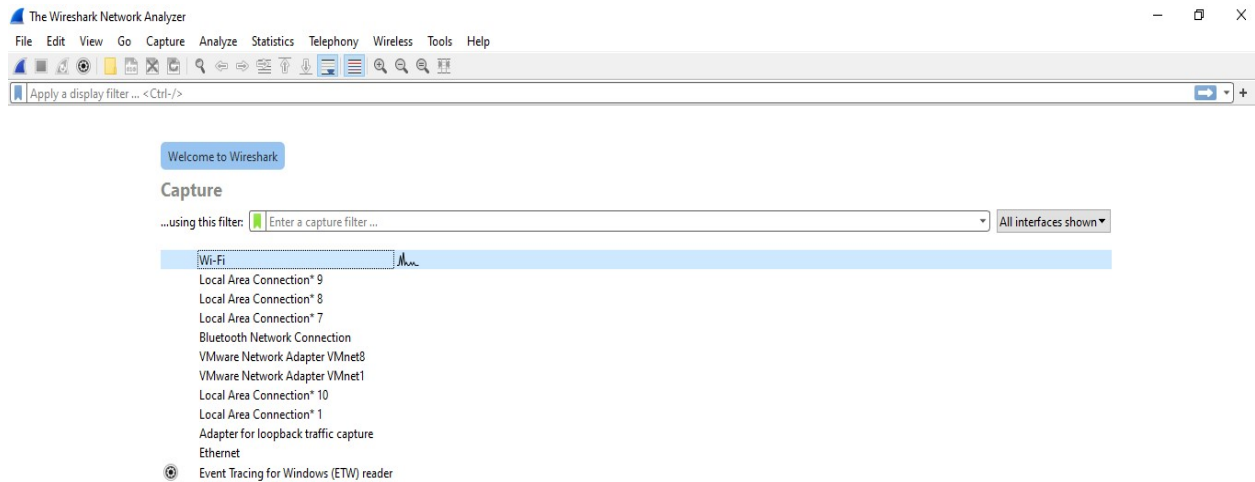


The image shows the Wireshark website homepage. At the top, there is a navigation bar with links: News, Learn, SharkFest, Get Acquainted, Get Help, Develop, Shop, and Members. A 'Donate' button is on the right. The main content area features a large blue banner with the Wireshark logo and the text 'Download Wireshark Now →'. Below this, it says 'The world's most popular network protocol analyzer' and 'Get started with Wireshark today and see why it is the standard across many commercial and non-profit enterprises.' There are two buttons: 'Get started' and 'Donate'. To the right, there is a graphic for 'Wireshark 4.0 Overview' with a shark fin icon.

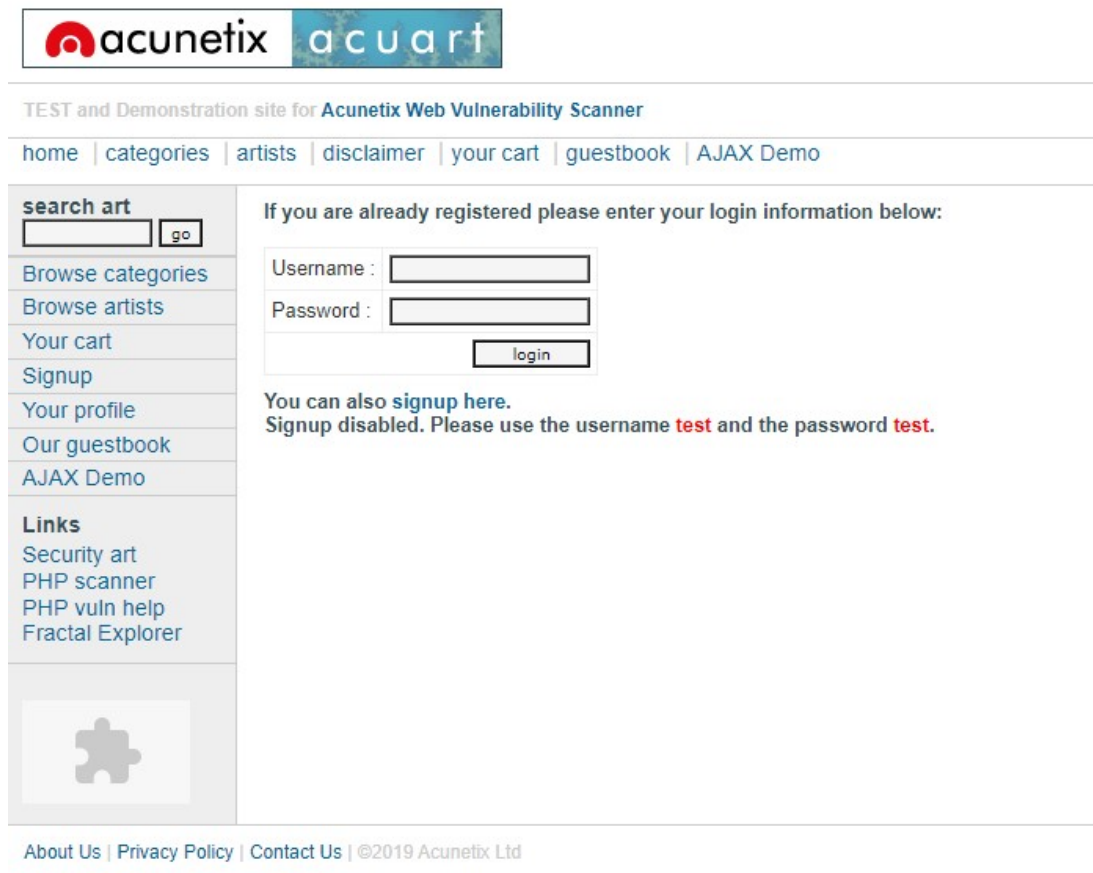


The image shows the 'Download Wireshark' page. The title 'Download Wireshark' is at the top. On the left, there is a list of download links: 'Stable Release: 4.2.5' (with sub-links for Windows x64 Installer, Windows Arm64 Installer, Windows x64 PortableApps®, macOS Arm Disk Image, macOS Intel Disk Image, and Source Code), 'Old Stable Release: 4.0.15', 'Older Stable Release: 3.6.24', and 'Documentation'. On the right, there are several promotional banners: 'endace' (Always-on, scalable Packet Capture), 'LiveAction' (Unmatched Network Visibility, Automatable Intelligence), 'FMADIO' (10G 40G 100G PACKET CAPTURE, Never Drop Packets!), 'Veeam' (FREE TRIAL, Veeam Data Platform 23H2 Update), and 'SCOS' (Wireshark University Authorized Training Partner, Official TCP / IP Troubleshooting Course).

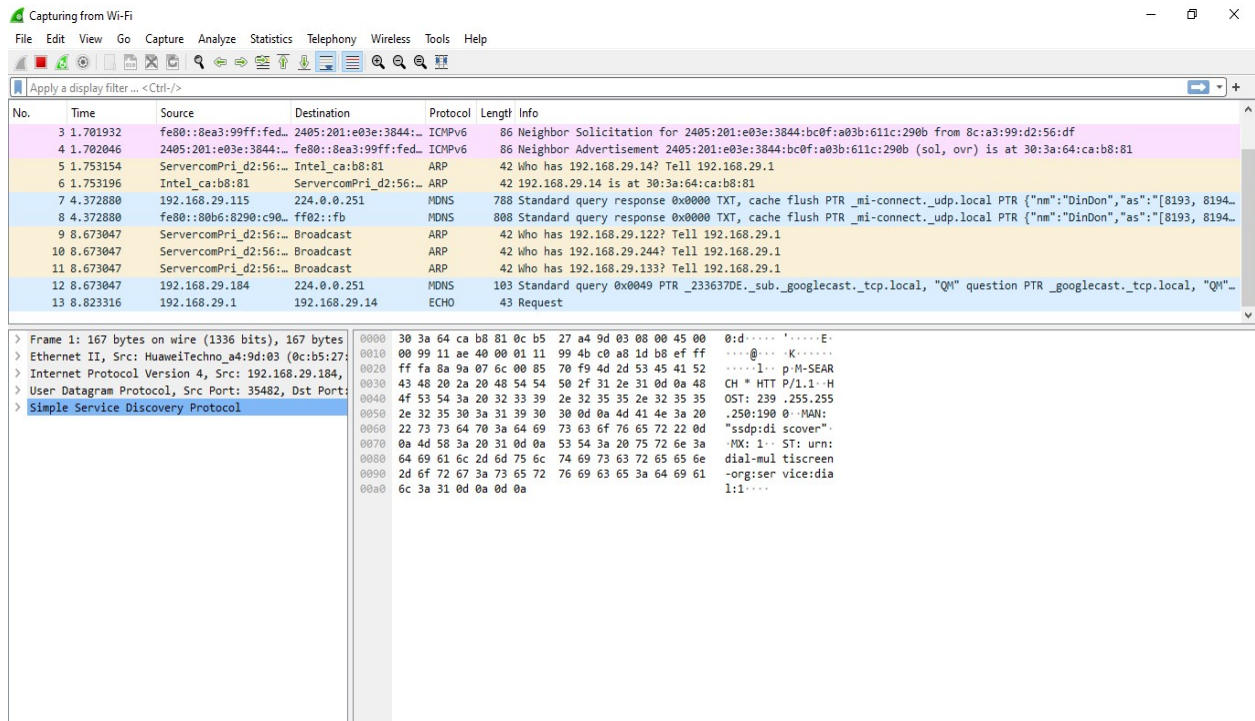
Step 1: Start Wireshark and click on Wi-Fi as shown in picture



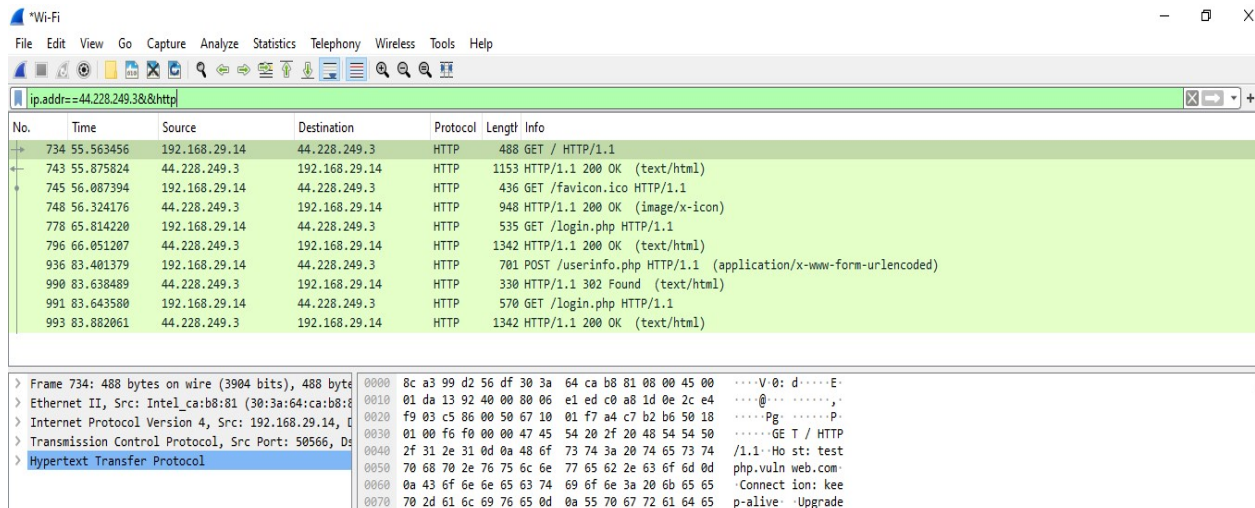
Step 2: Open the browser and open website testphp.vulnweb.com. Navigate to signin page and enter any credentials.



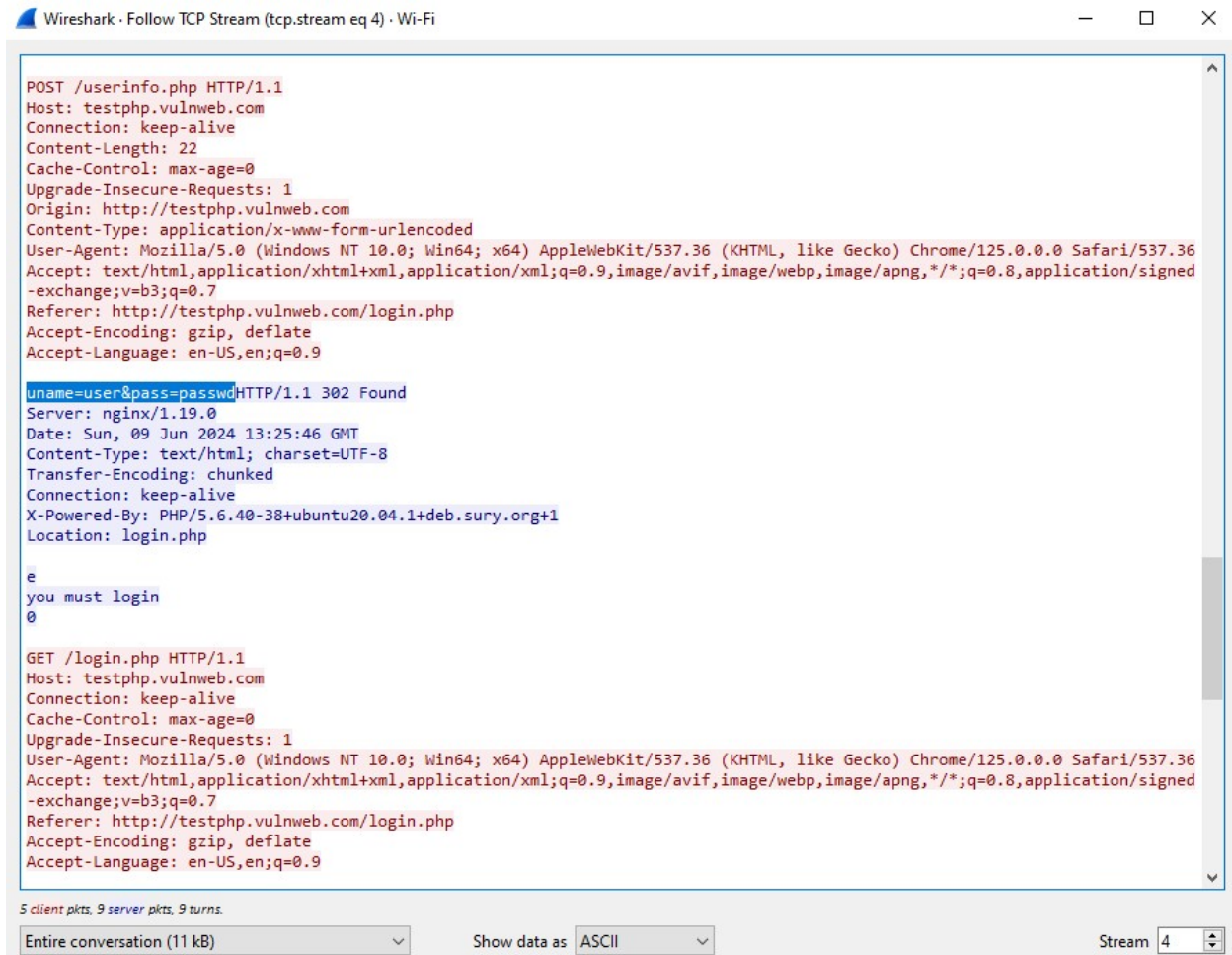
Step 3: Once the request is captured, go back to Wireshark and click on stop button.



Step 4: In filter write ip.addr==44.228.249.3&&http and click on search. Right click and follow TCP stream.



Step 5: A new window will open, go through the content and check we will be able to see the username and password in clear text (Here, uname=user&pass=passwd)



Wireshark · Follow TCP Stream (tcp.stream eq 4) · Wi-Fi

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 22
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

uname=user&pass=passwdHTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Sun, 09 Jun 2024 13:25:46 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

e
you must login
0

GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

5 client pkts, 9 server pkts, 9 turns.

Entire conversation (11 kB) Show data as ASCII Stream 4