

Experiment Number:7

Aim: Study of packet sniffer tool **Wireshark**

- A. Observer performance in **promiscuous** as well as **non-promiscuous** mode
- B. Show the packets can be traced base on different **filters**

Date of Performance: 20-8-2020

Date of Submission: 27-9-2020

Grade:

Sign:



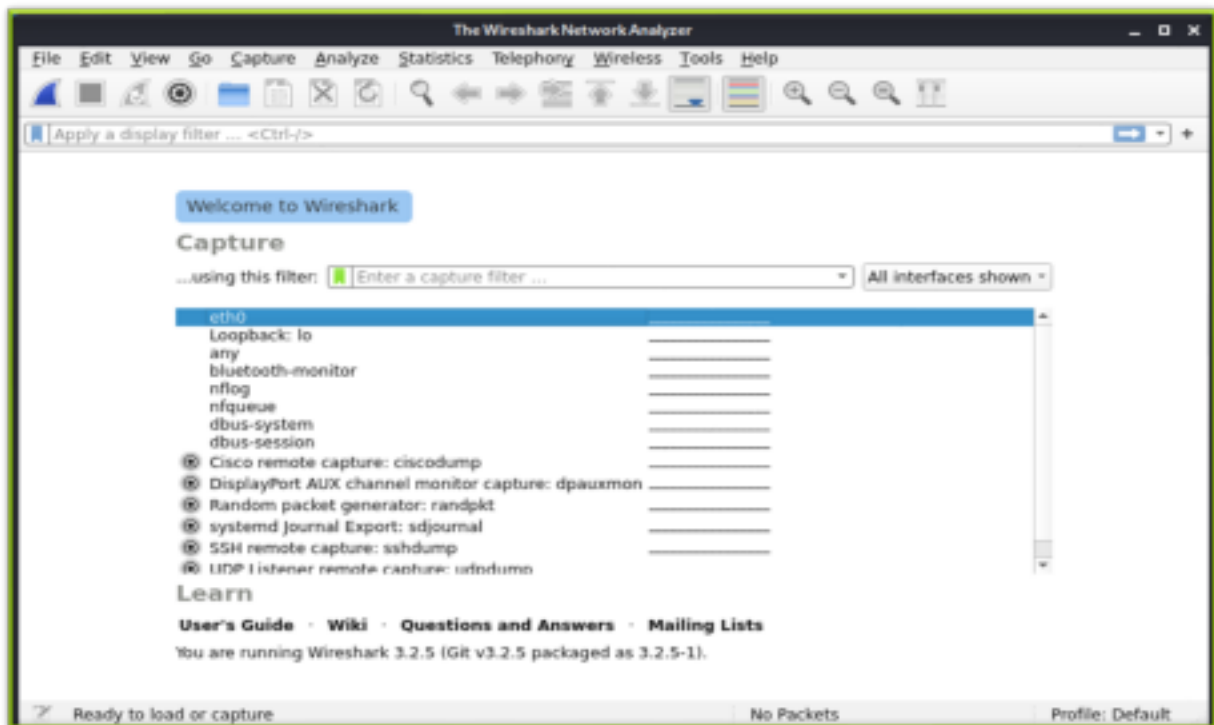
Name :

Bhagyashri Nitin Patil

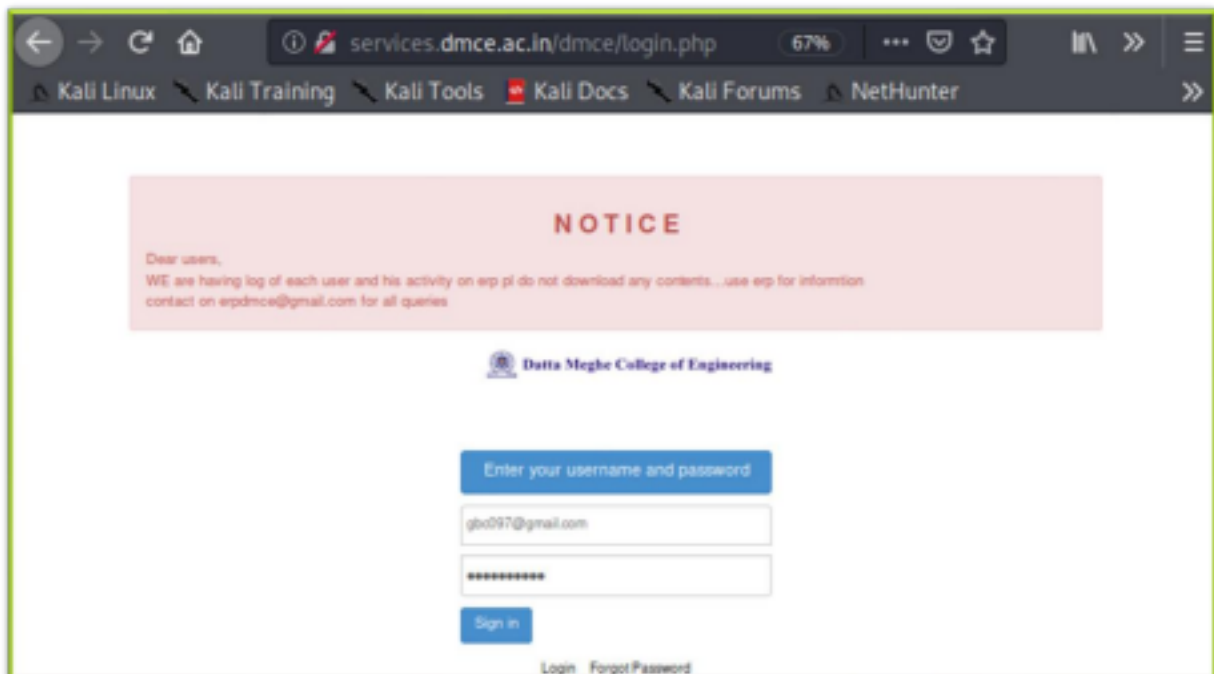
Roll Number: **50**

✚ Username and Password Capturing in Wireshark 1.

Open Wireshark and click on start packet capturing

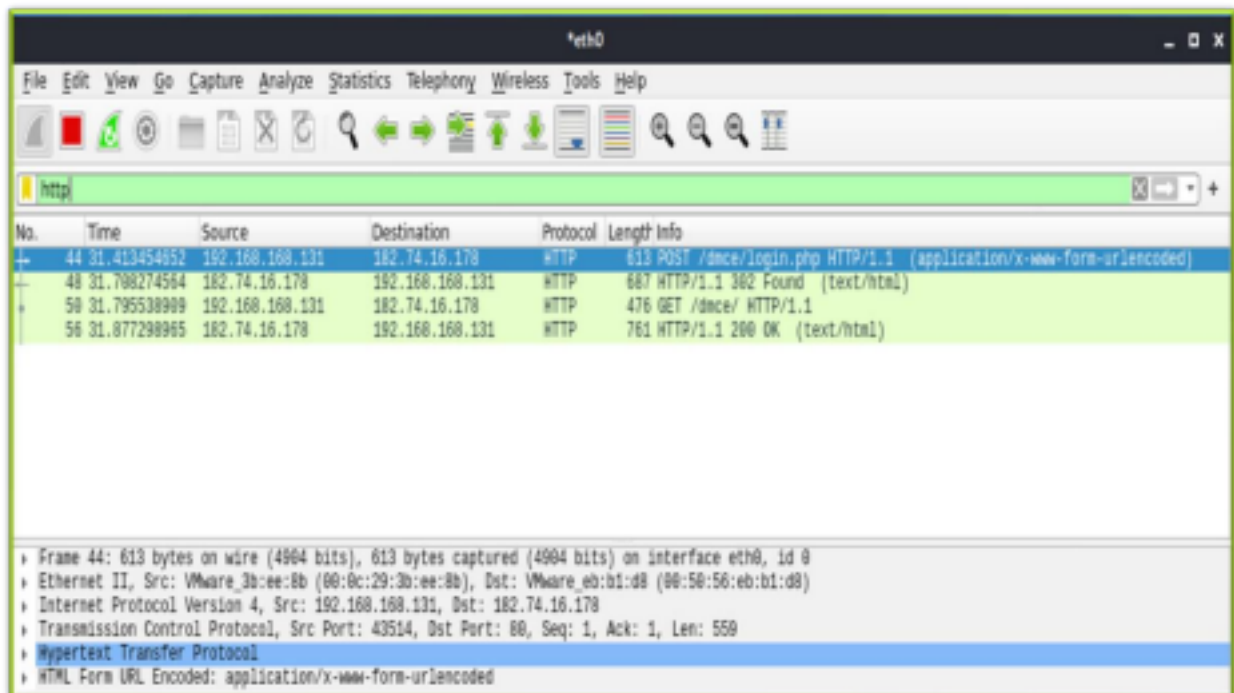


2. ERP login

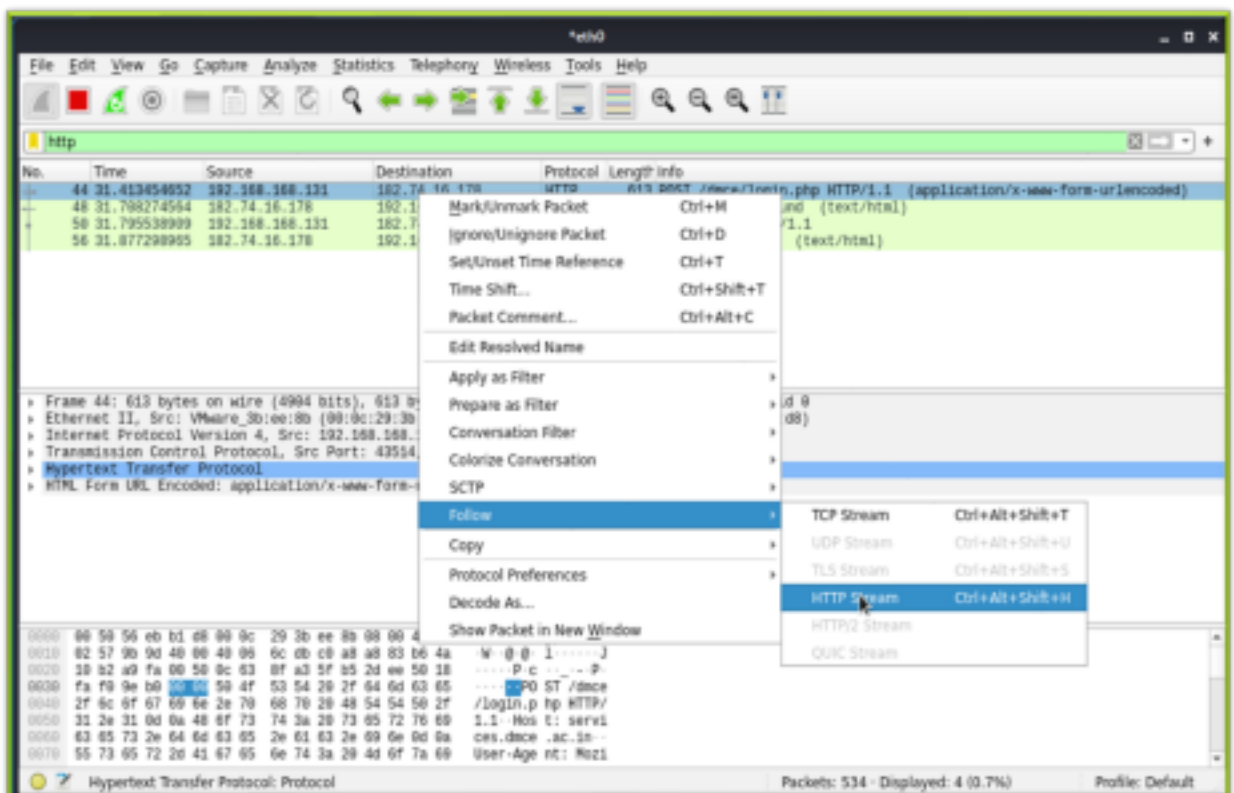


CNS (Roll_50)

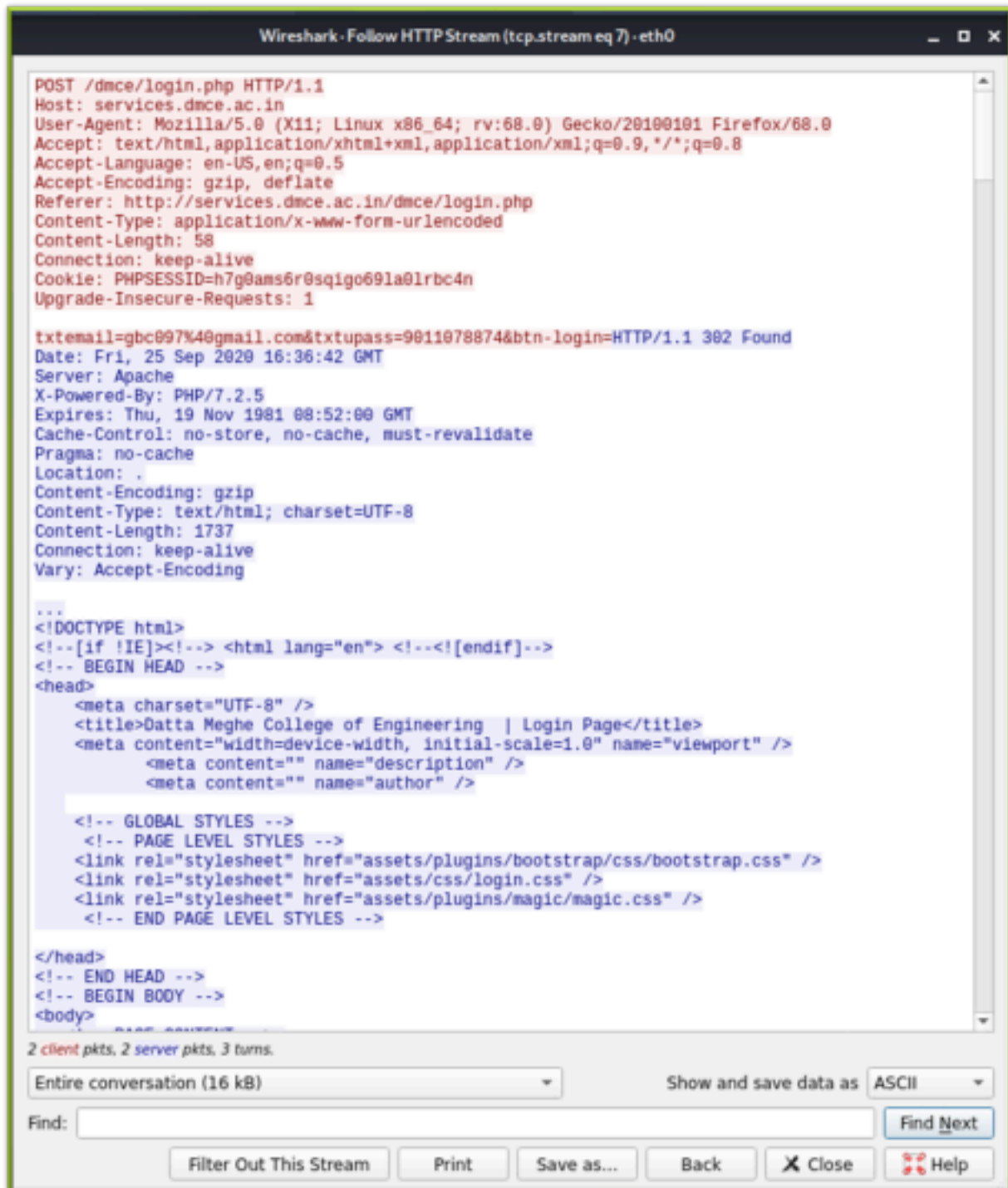
3. Apply http filter and Observe POST Method



4. Right click on highlight line & Click Follow->HTTP Stream



5. Username and Password displayed. [txtemail]



```
Wireshark · Follow HTTP Stream (tcp.stream eq 7) · eth0

POST /dmce/login.php HTTP/1.1
Host: services.dmce.ac.in
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://services.dmce.ac.in/dmce/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Connection: keep-alive
Cookie: PHPSESSID=h7g0ams6r0sqigo69la01rbc4n
Upgrade-Insecure-Requests: 1

txtemail=gbc097%40gmail.com&txtupass=9011078874&btn-login=HTTP/1.1 302 Found
Date: Fri, 25 Sep 2020 16:36:42 GMT
Server: Apache
X-Powered-By: PHP/7.2.5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: .
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Content-Length: 1737
Connection: keep-alive
Vary: Accept-Encoding

...
<!DOCTYPE html>
<!--[if !IE]><!--> <html lang="en"> <!--<![endif]>>
<!-- BEGIN HEAD -->
<head>
  <meta charset="UTF-8" />
  <title>Datta Meghe College of Engineering | Login Page</title>
  <meta content="width=device-width, initial-scale=1.0" name="viewport" />
  <meta content="" name="description" />
  <meta content="" name="author" />

  <!-- GLOBAL STYLES -->
  <!-- PAGE LEVEL STYLES -->
  <link rel="stylesheet" href="assets/plugins/bootstrap/css/bootstrap.css" />
  <link rel="stylesheet" href="assets/css/login.css" />
  <link rel="stylesheet" href="assets/plugins/magic/magic.css" />
  <!-- END PAGE LEVEL STYLES -->

</head>
<!-- END HEAD -->
<!-- BEGIN BODY -->
<body>
```

2 client pkts, 2 server pkts, 3 turns.

Entire conversation (16 kB) Show and save data as ASCII

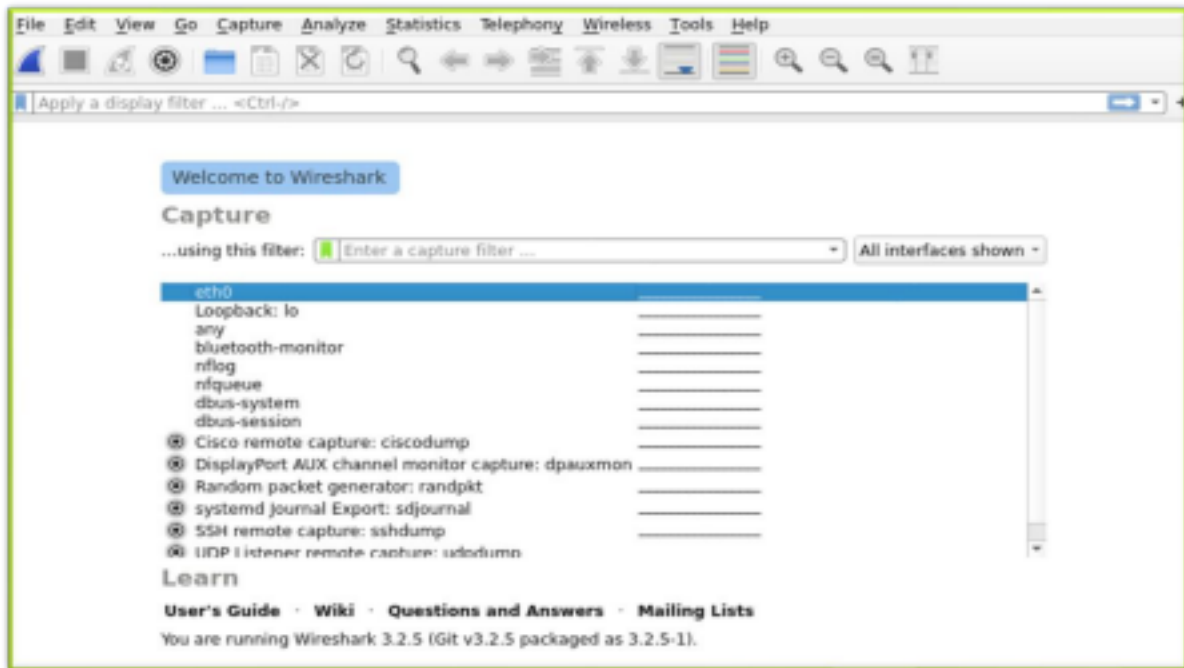
Find: Find Next

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

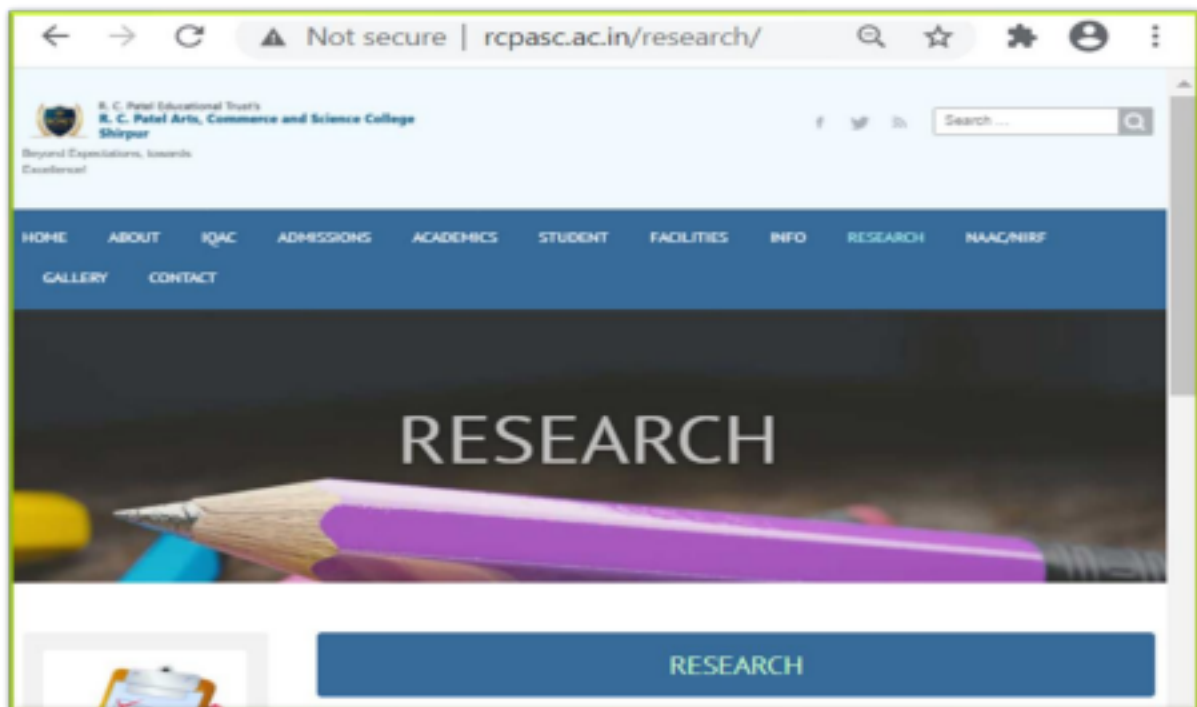
CNS (Roll_50)

📌 Image Capturing in Wireshark

1. Open Wireshark and click on start packet capturing

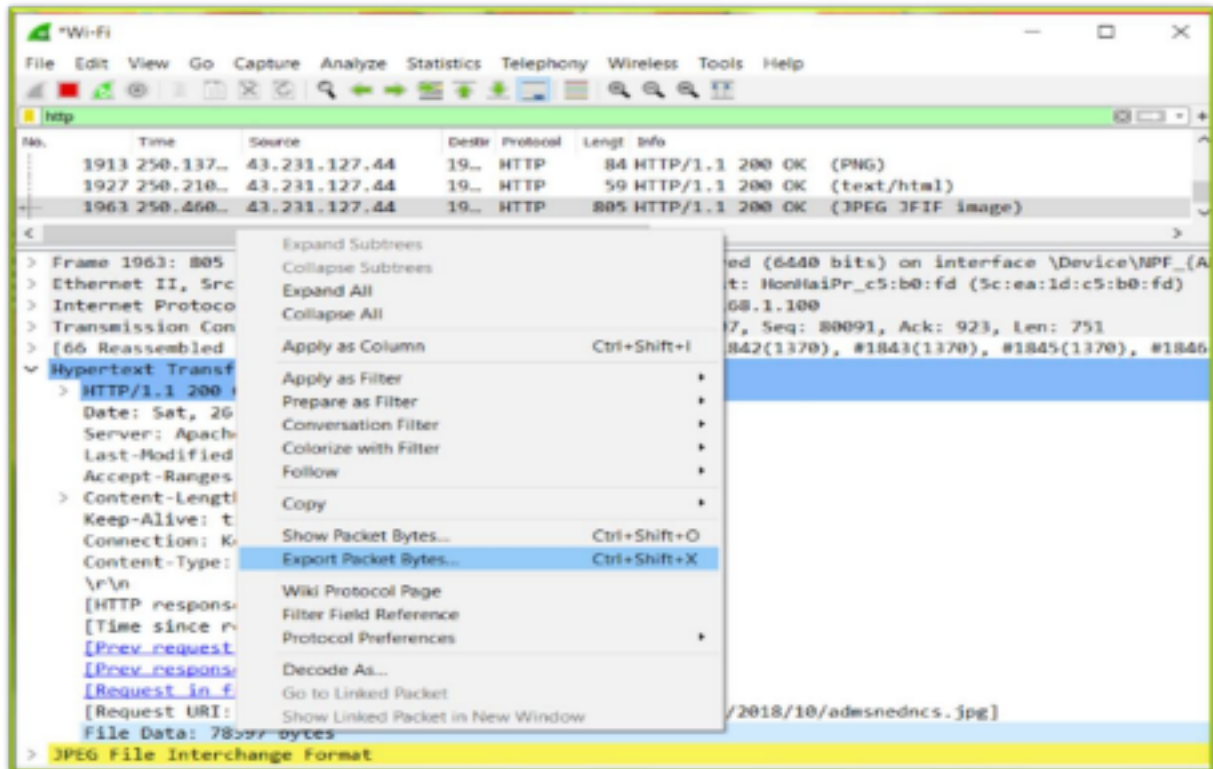


2. Open browser and browse a website

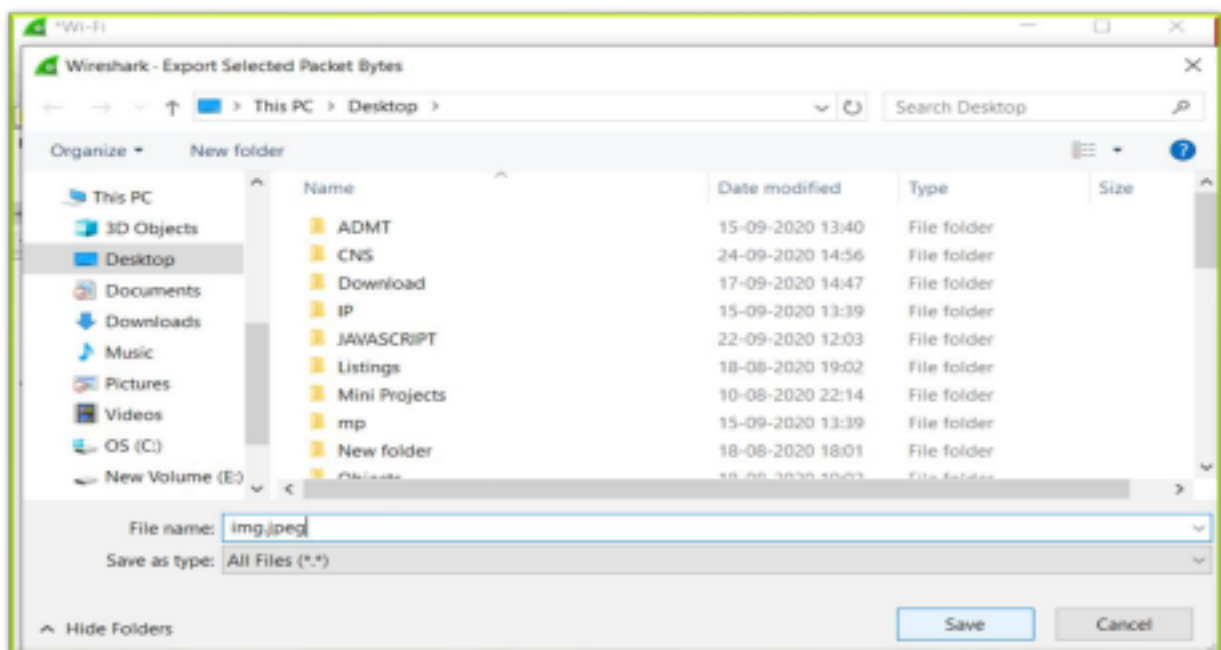


CNS (Roll_50)

3. Open Filter box and type http In packet description,click Hypertext Protocol ,scroll down and find file size



5. Save File as img.jpeg on Desktop



CNS (Roll_50)

6. Open File img.jpeg which is saved on Desktop in step 5
It is captured image through wireshark



CNS (Roll_50)

☐ Video Capturing in Wireshark

1. Open Wireshark and click on start packet capturing



2. Open browser and browse a website and play video



CNS (Roll_50)

3. Pause video after few minutes



4. Type UDP in filter box and Observe packet details



CNS (Roll_50)

5. Click on Statistics and select Conversations option



6. Click on Follow Stream button





7. Save file as videpcaptured.mp4 on desktop



8. Play videpcaptured.mp4 file in VLC media player

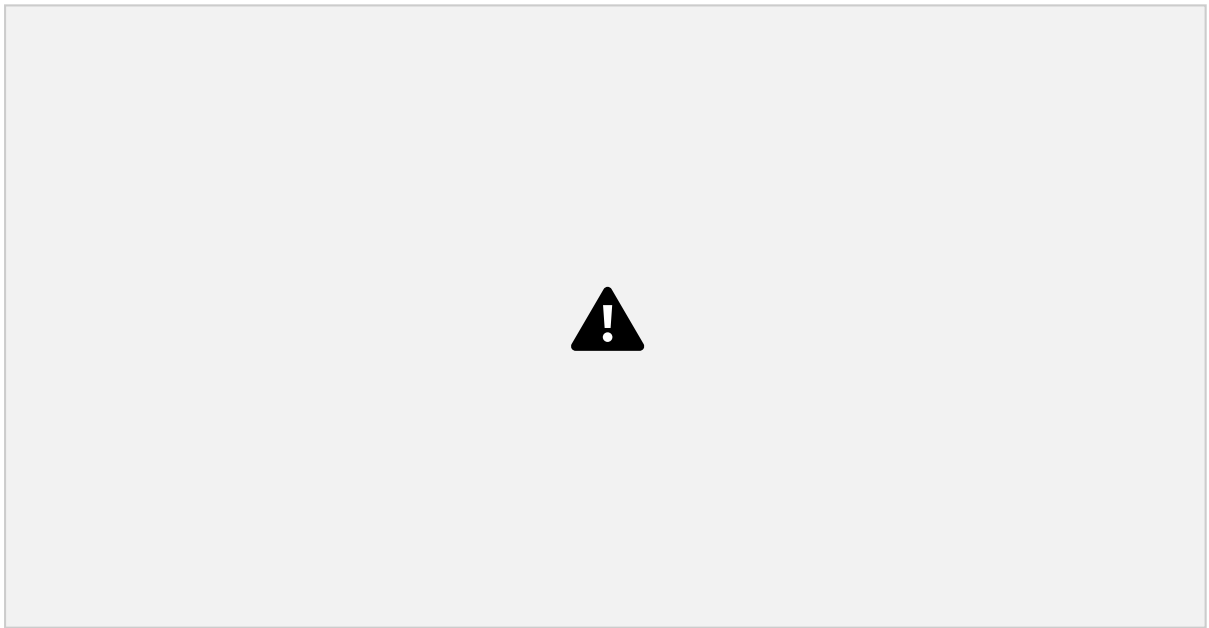


Filters

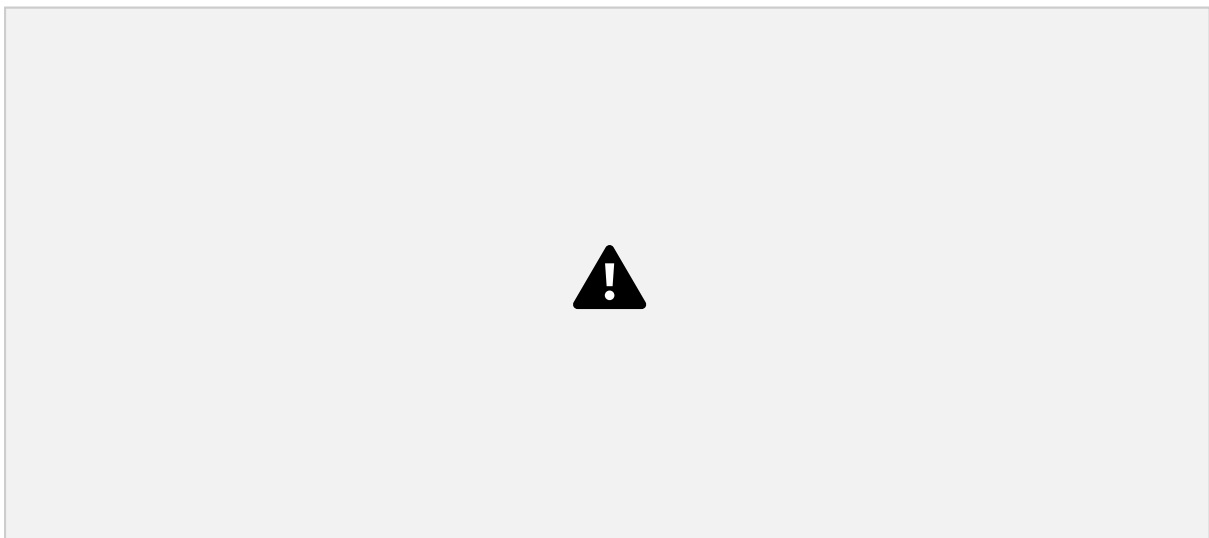
❖ Capture Filter

- Port 80

1. Open wireshark,select Wifi & type port 80 in capture filter
And click start symbol

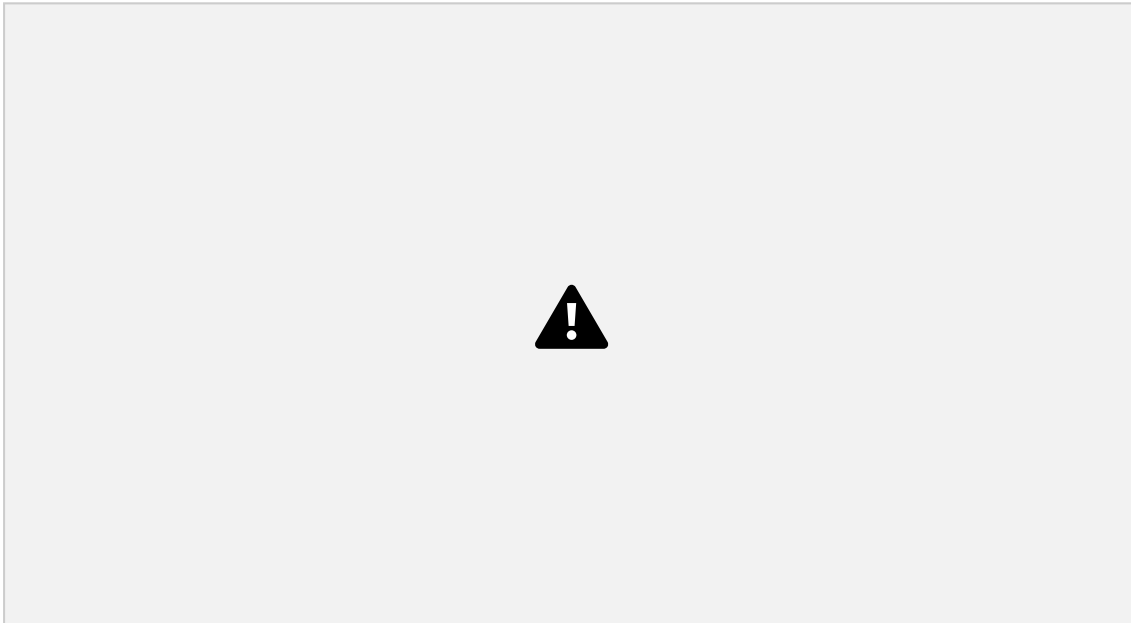


2. In Filtered traffic and only TCP packet displayed

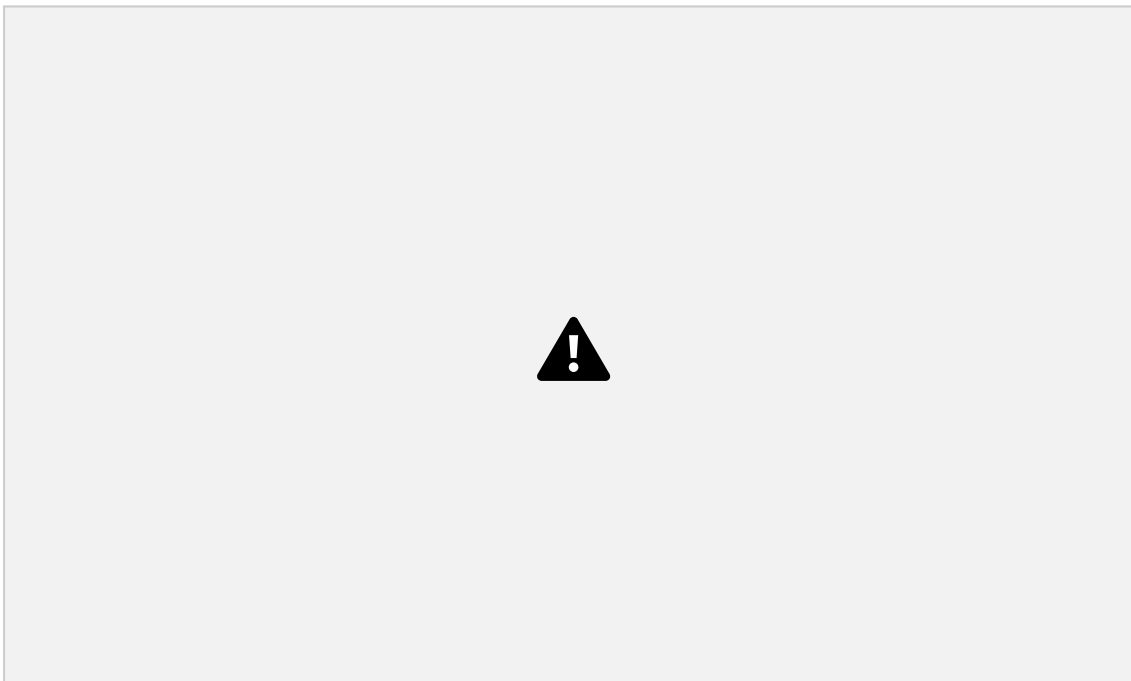


- src 192.168.1.100

1. Open wireshark,select Wifi & type src in capture filter and click start symbol

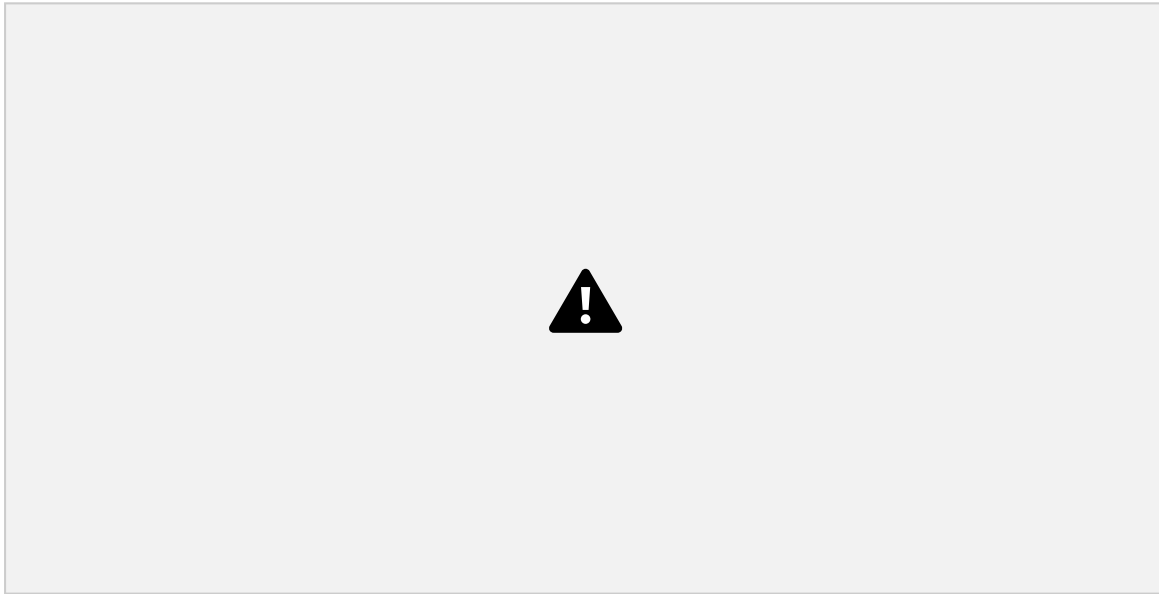


2. In Filtered traffic only packet displayed which arrived from 192.168.1.100 source.

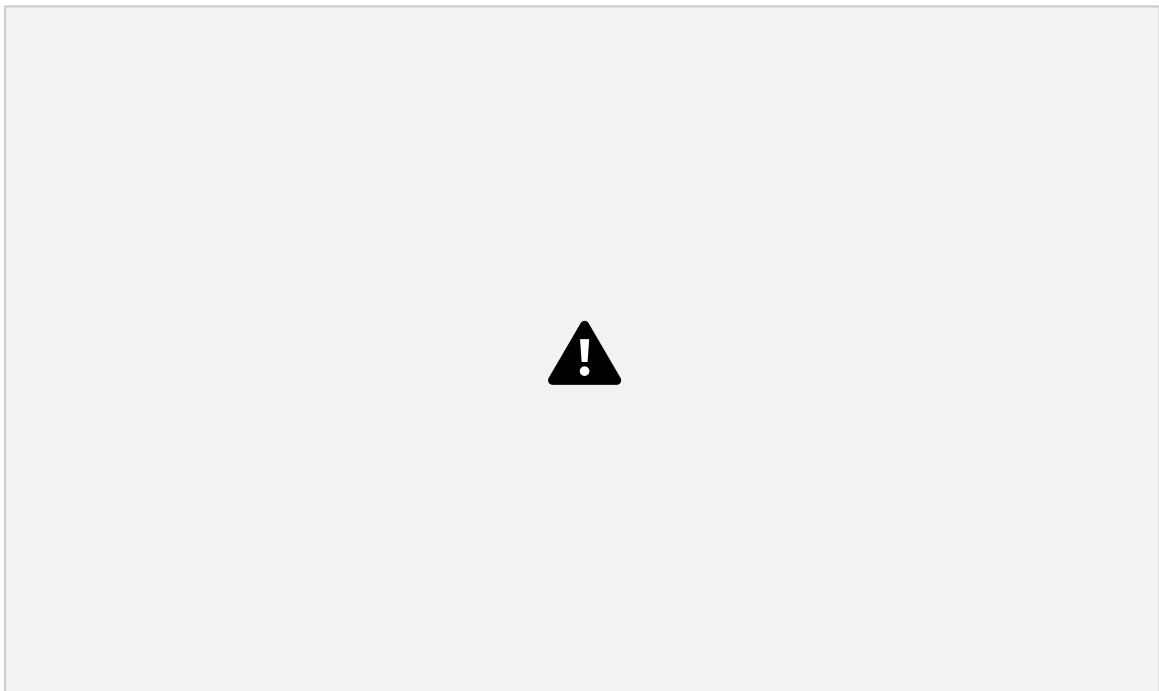


- dst 172.217.165.35

1. Open wireshark,select Wifi & type src in capture filter and click start symbol

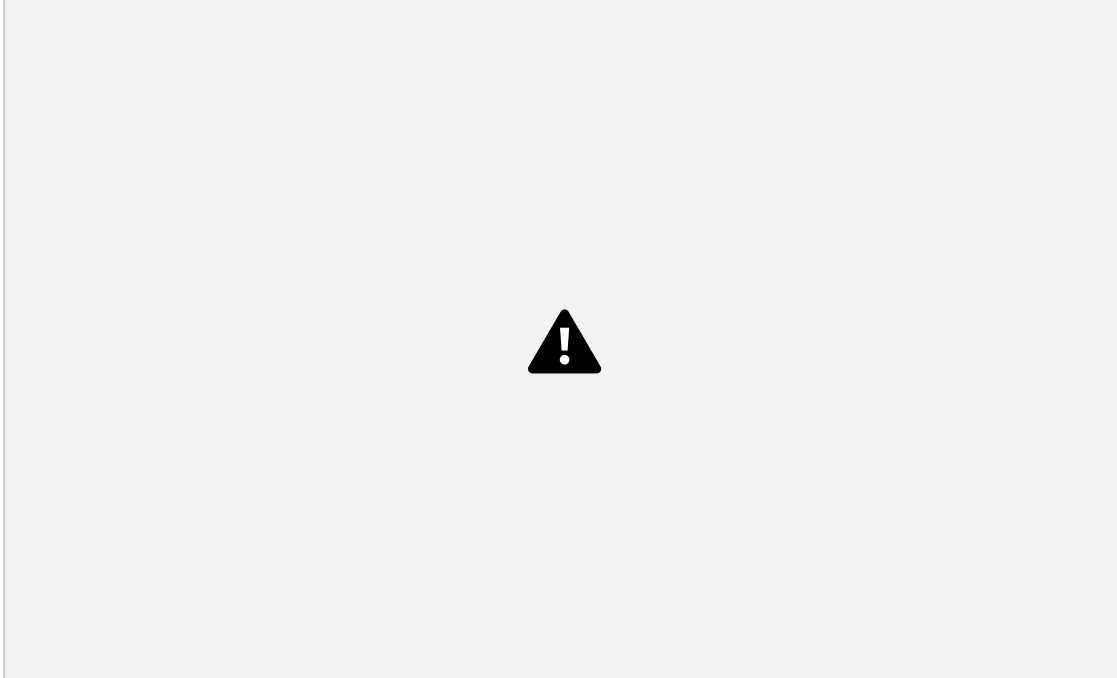


2. In Filtered traffic only packet displayed which goes to 172.217.166.35 source.

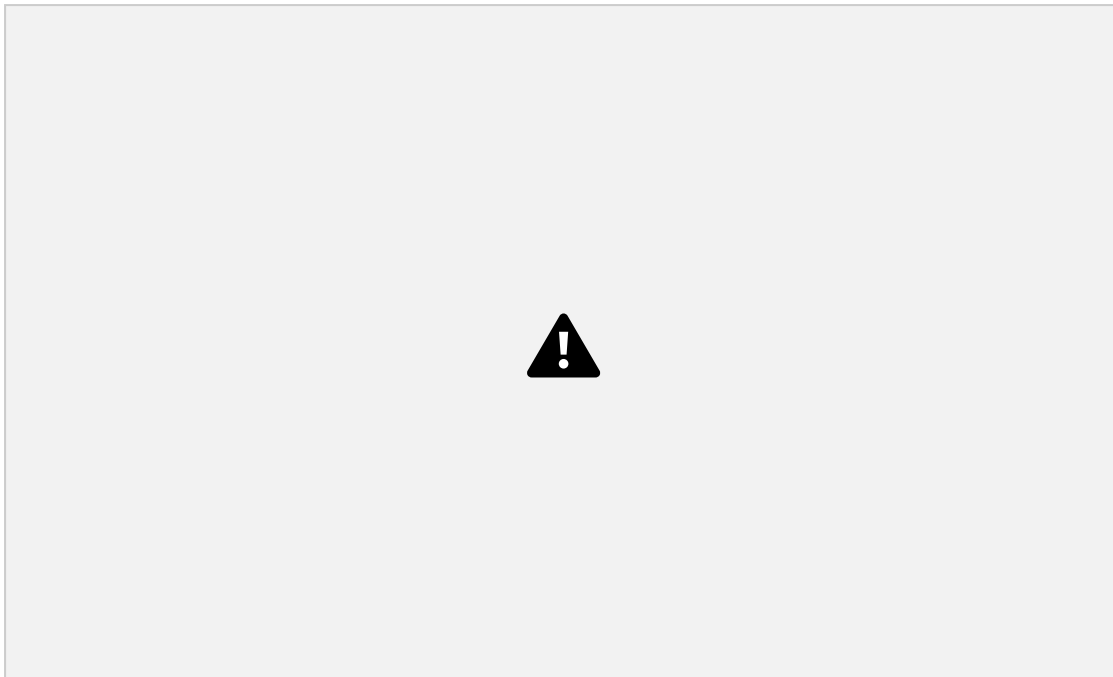


- host 192.168.1.100

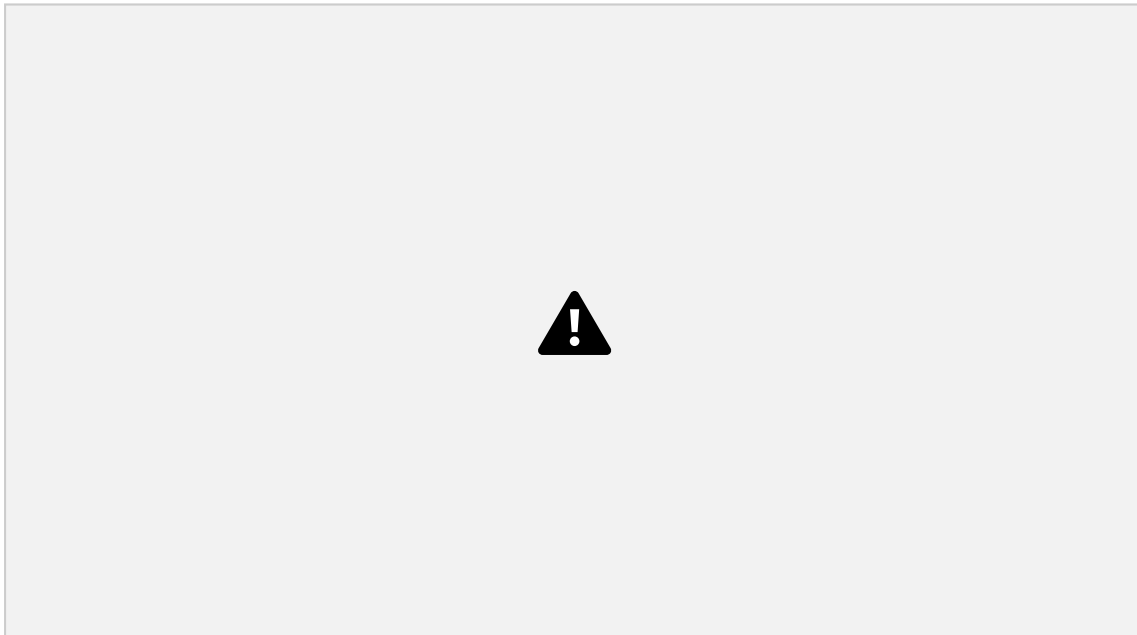
1. Open wireshark,select Wifi & press ctrl+K



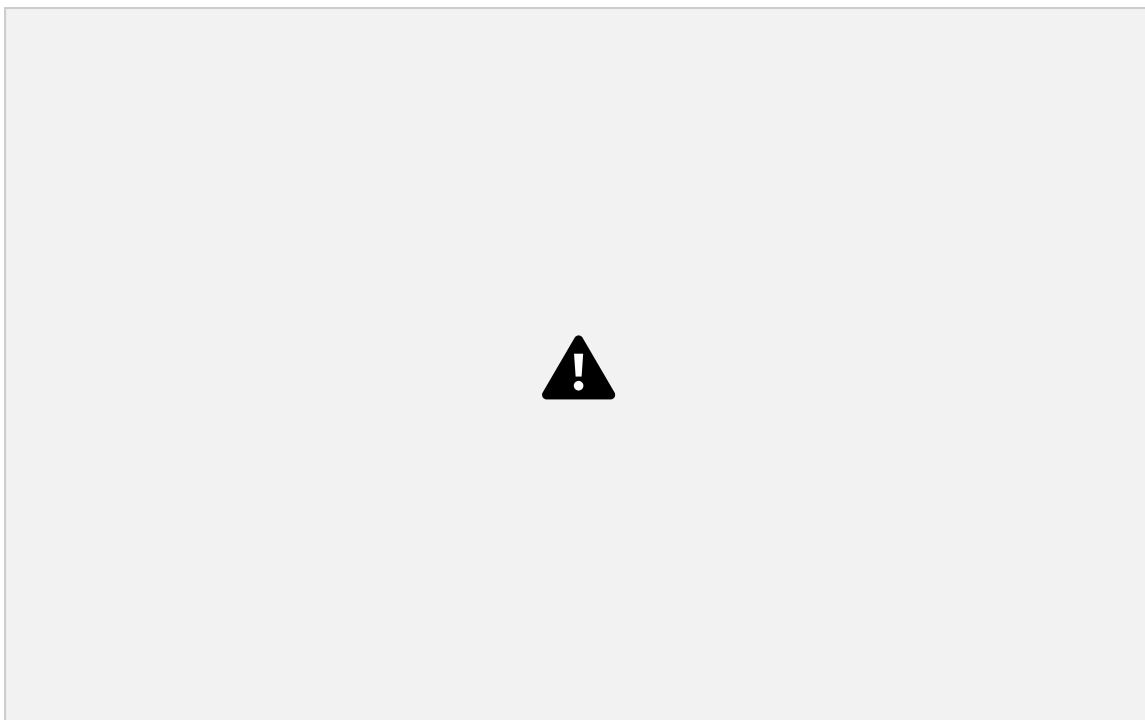
2. Check Promiscuous boxes and Type host 192.168.1.100 in captured filter box and click start option



3. Observed traffic on host

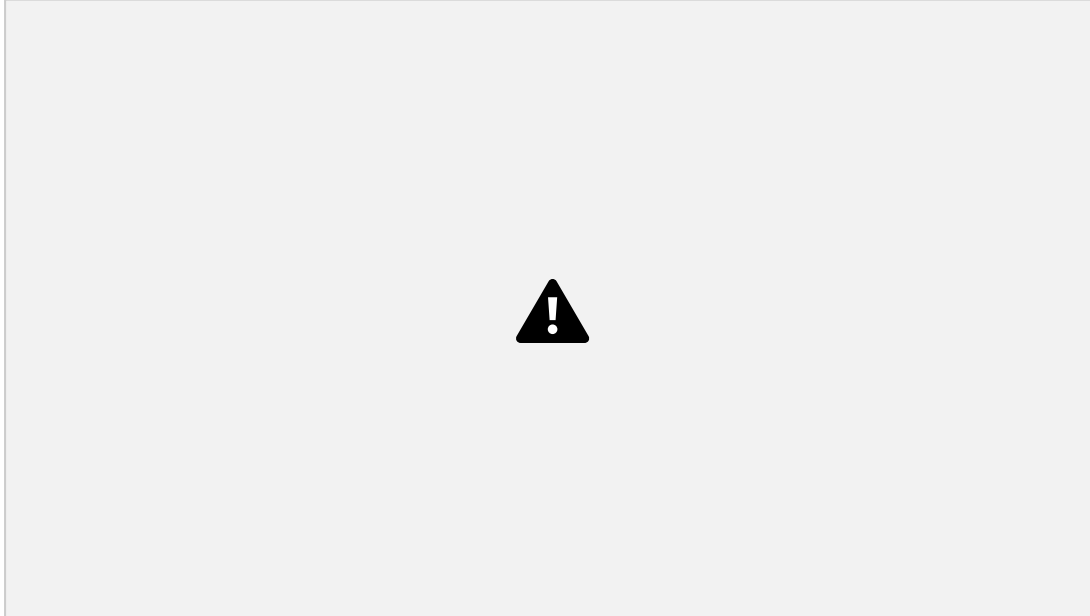


----- ➤ Open browser
and Go to website testing
ground.scraping.pro and login

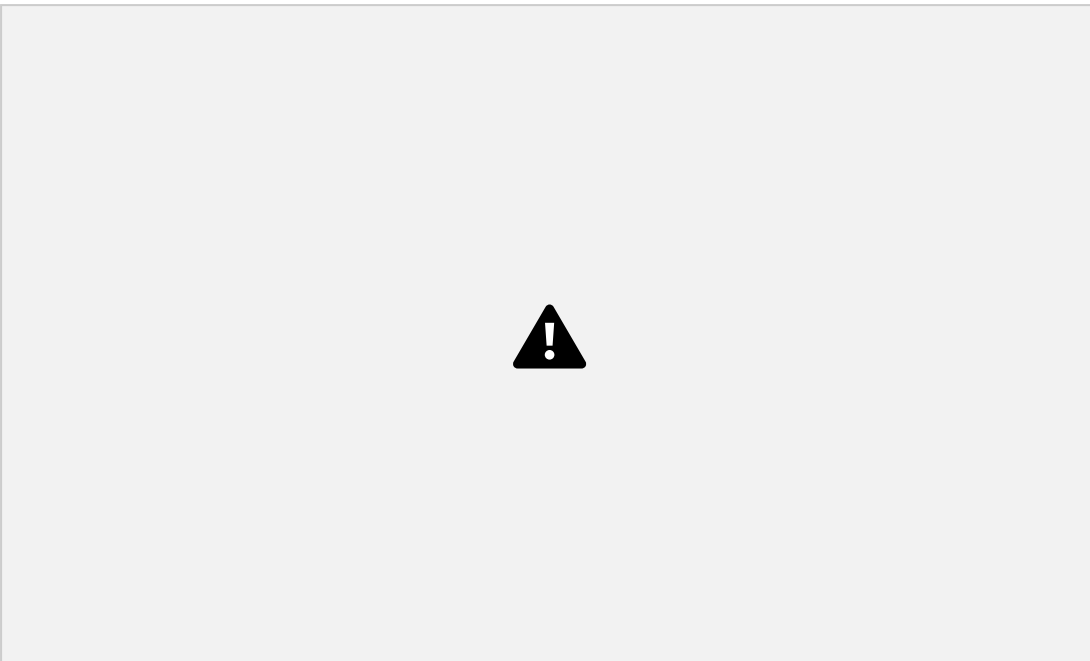


❖ Display Filter

1. Open wireshark and select wi-fi

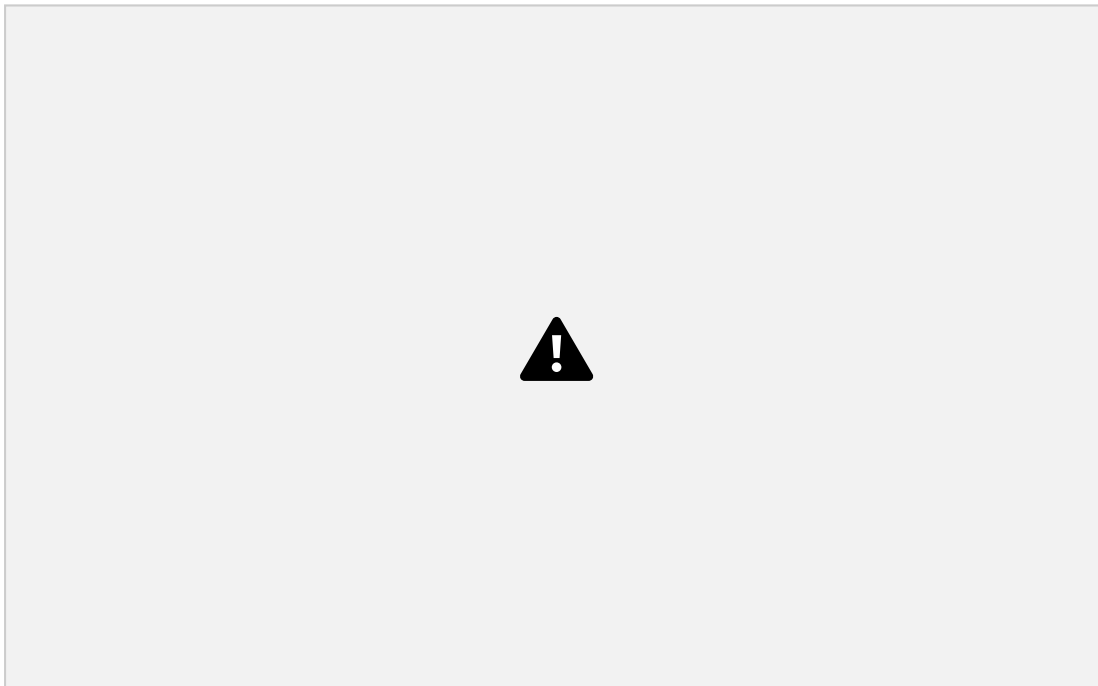


2. Press Ctrl+K and Check Promiscuous modes, click start

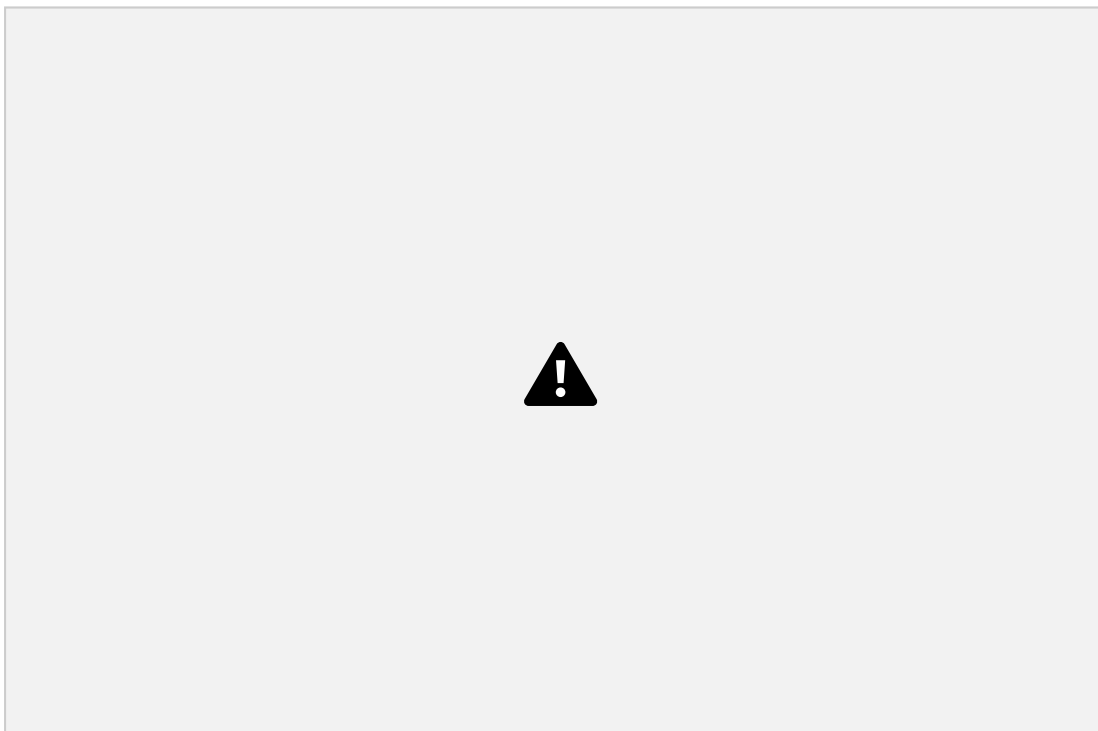


CNS (Roll_50)

3. Type http in display filter box and press enter



4. Go to Analyze tab and select display filters



CNS (Roll_50)

5. Display filter dialogue box opened and see details and click ok



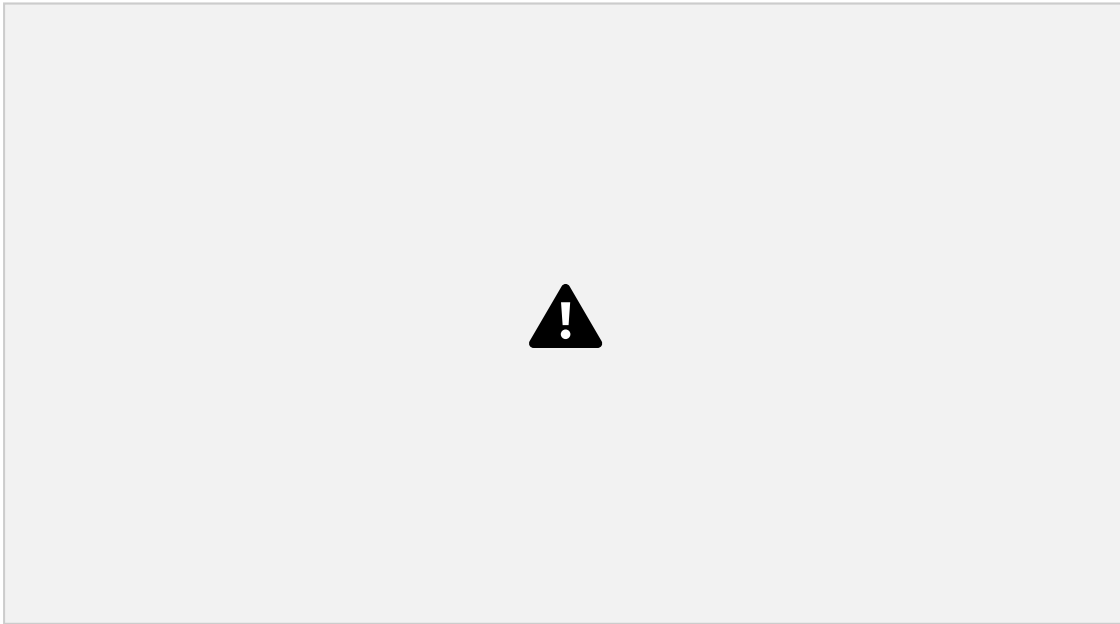
6.

Goto Analyze tab and select follow → HTTP Stream option

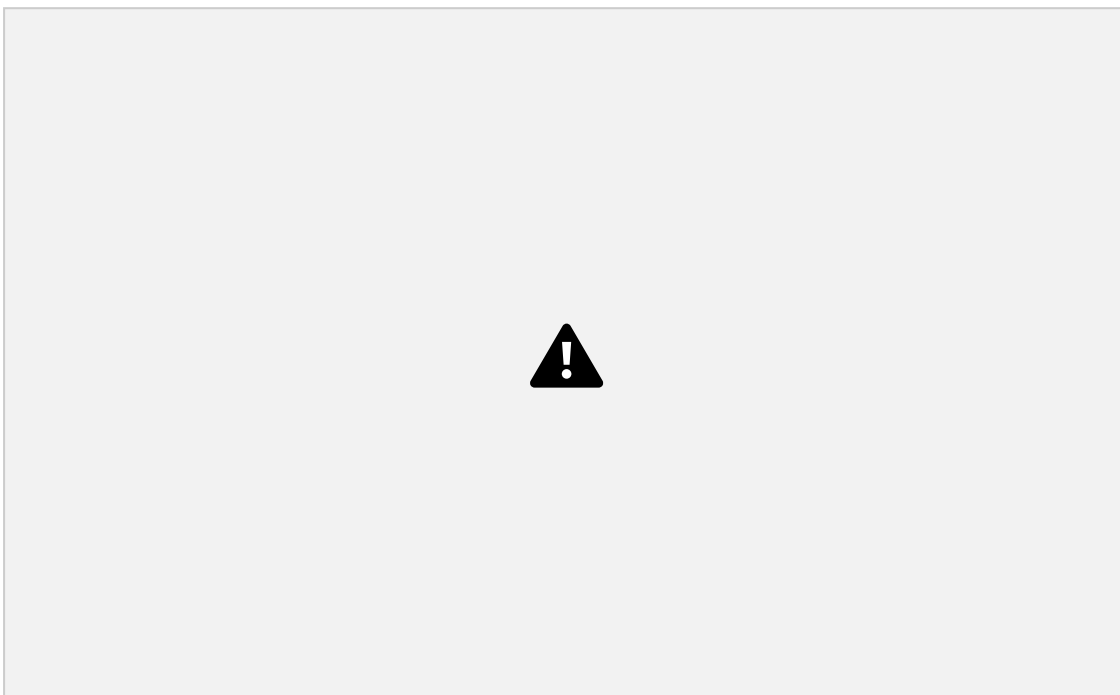


CNS (Roll_50)

7. Displayed full conversation information between client and server
(username & password noticed)



8. Filter applied automatically in above step. Displayed all packets that make up the conservation.



CNS (Roll_50)

9. Use another way to apply filter as right-click one of the detail and use the Apply as filter -> select



10. [http automatically displayed in display filter box](#)

