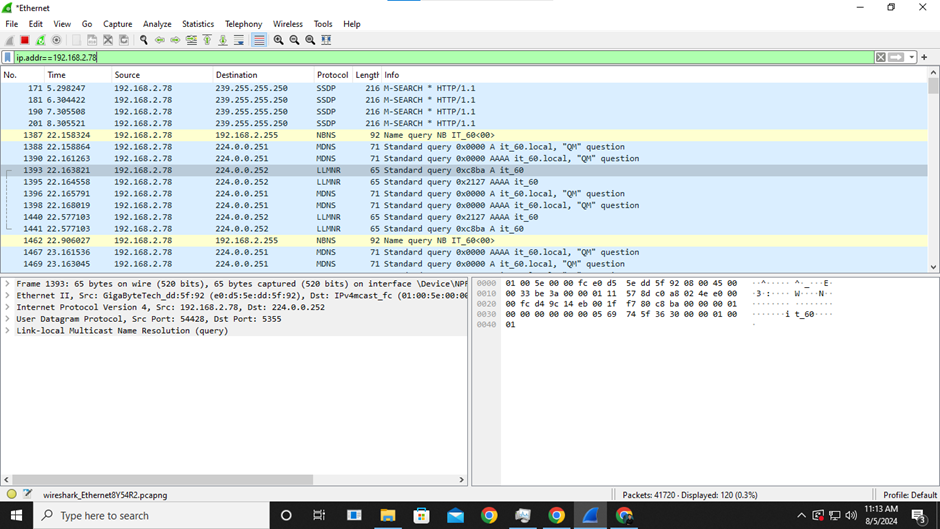
1. Inspect traffic for a specific IP address.

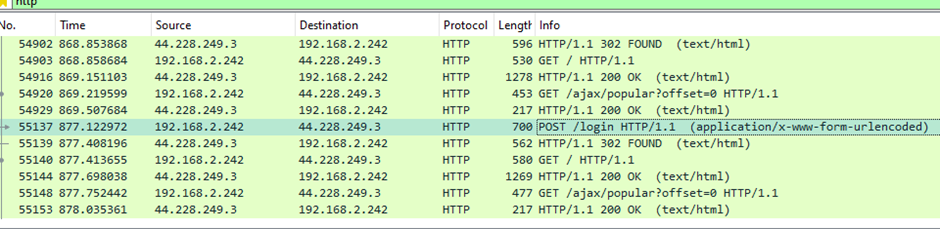
**Filter :** ip.addr==192.168.2.78

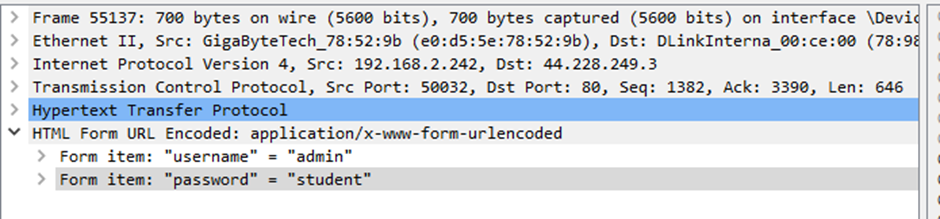


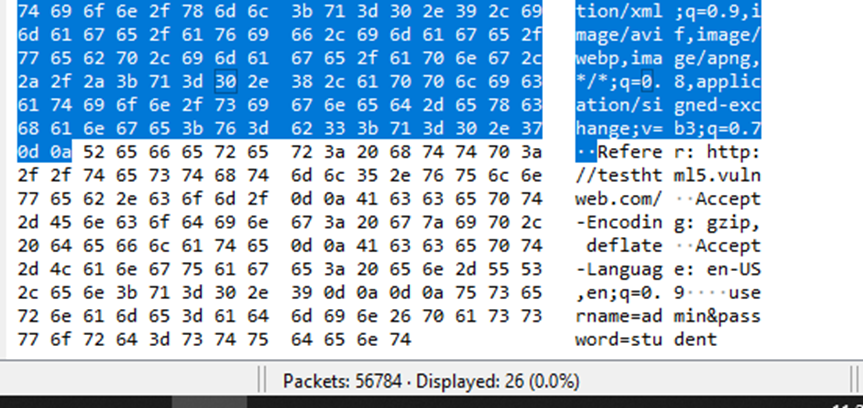
1. Sniff the credentials details from a vulnerable website:security tweets.com.

**Filter :** Keep scanning first. Goto website and then stop scanning and put filter “http”. Click the blue arrow at the side.

**Output :**

****

****

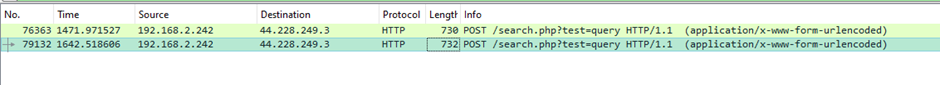
****

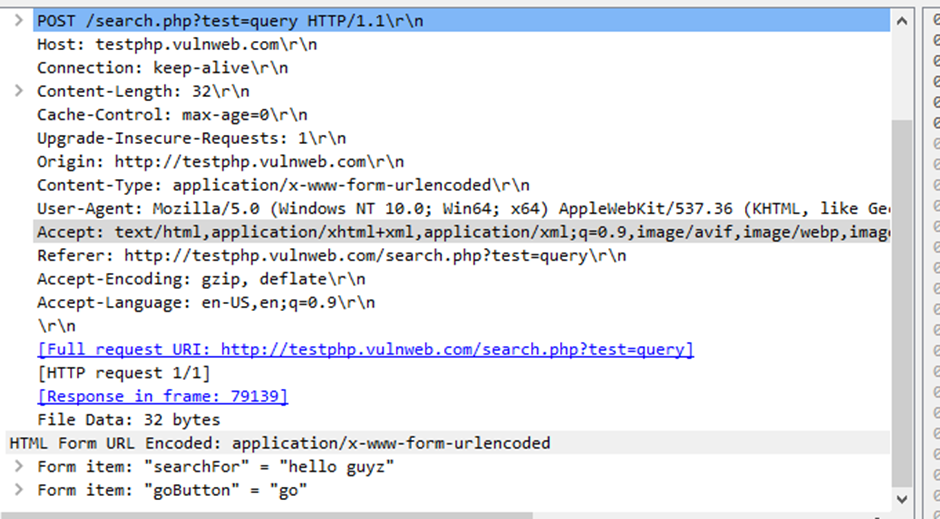
1. Check what user has typed in browser

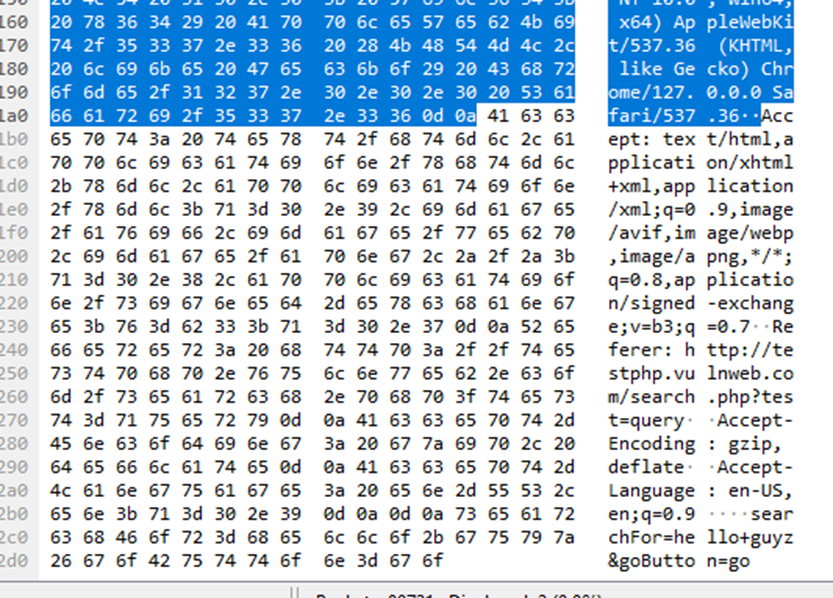
-http://test.vulnweb.com/search.php/

**Filter :** http.referer contains "http://test.vulnweb.com/search.php/"

**Output :**

****

****

****

1. Check what string user has passed in google search engine.

**Filter :** http.referer contains “search”

(here I used directly http as filter and then checked the console to get the details…see image 2 in output)

(First scan, then search on browser with word search in URL, then stop scanning and add filter)

**Output :**

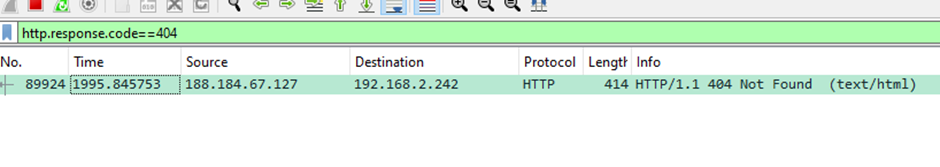
1. Find out packets which are getting the response as PAGE

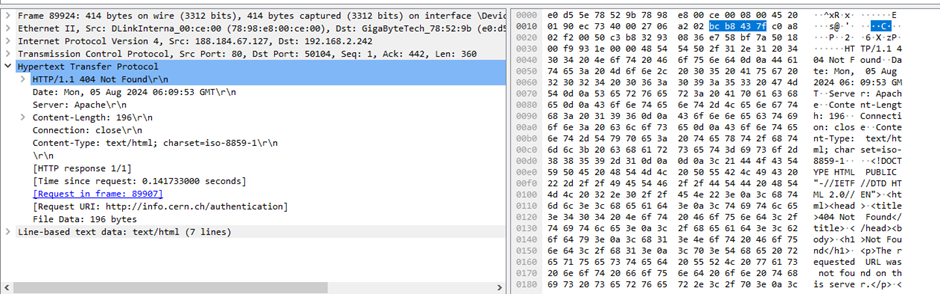
NOT FOUND.

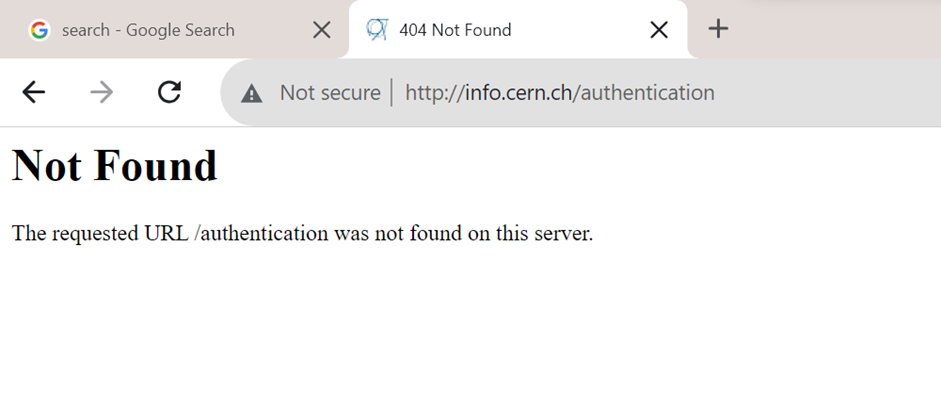
**URL used :** http://info.cern.ch/authentication

**Filter :** http.response.code==404

**Output :**



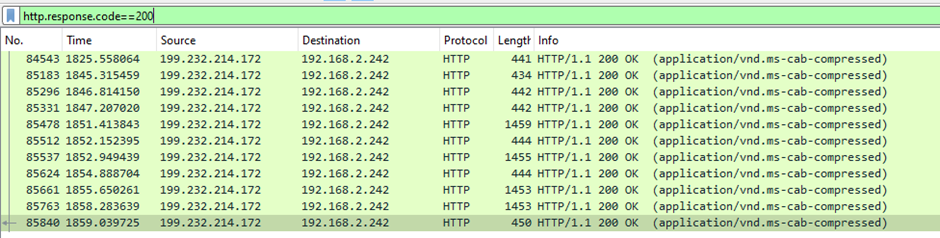


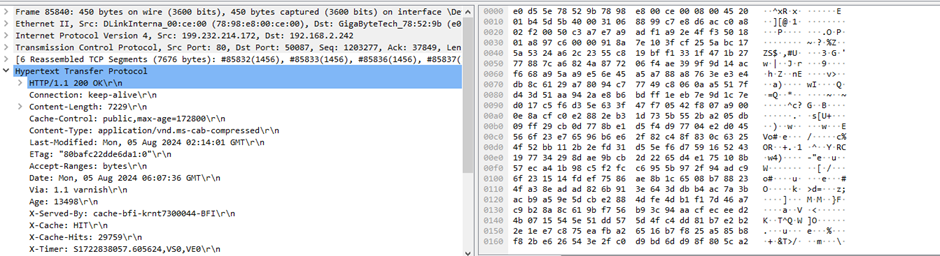


1. Find out those packets which are getting response.

**Filter :** http.response.code==200

**Output :**

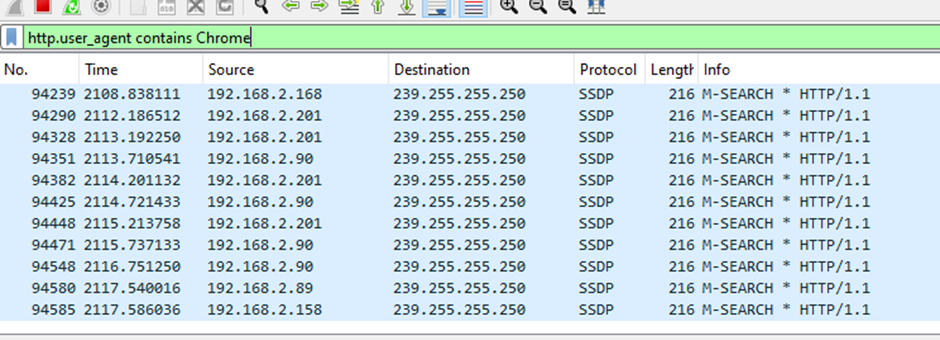
****

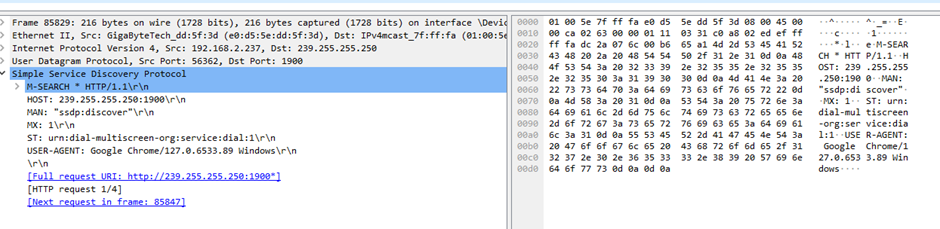
****

1. Find Packets-: Browser Specific.

**Filter :** http.user\_agent contains Chrome

**Output :**





**Codes for server.py and client.py :**

**Server.py :**

import socket

s=socket.socket()

print("Socket created successfully !")

port=8080

s.bind(('192.168.2.78',port))

print("Socket binded to %s"%(port))

s.listen(5)

print("Socket is listening...")

while True:

c,addr=s.accept()

print("Got connection from ",addr)

c.sendall('Thank you for connectiong! '.encode())

c.close()

**Client.py :**

import socket

s=socket.socket()

port=8080

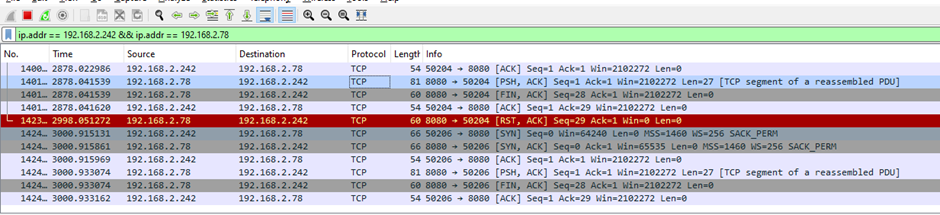
s.connect(('192.168.2.78',port))

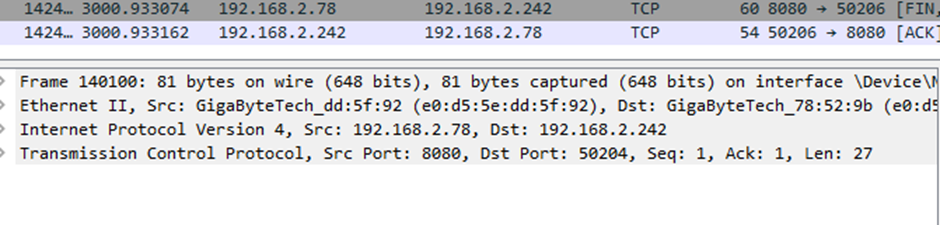
print(s.recv(1024).decode())

1. Inspect traffic between specific source and destination

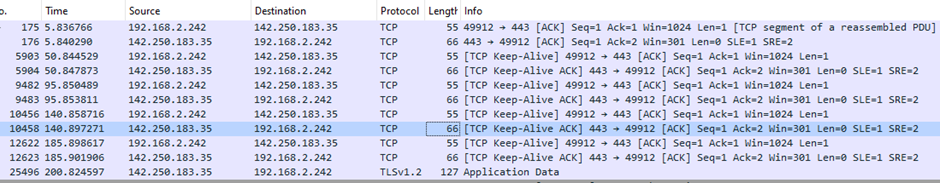
**Filter :** ip.aadr==192.168.2.78 && ip.addr==192.168.2.242

**Output :**





1. To sniff communication between client and server

****