Wireshark Practical

Practical no 10

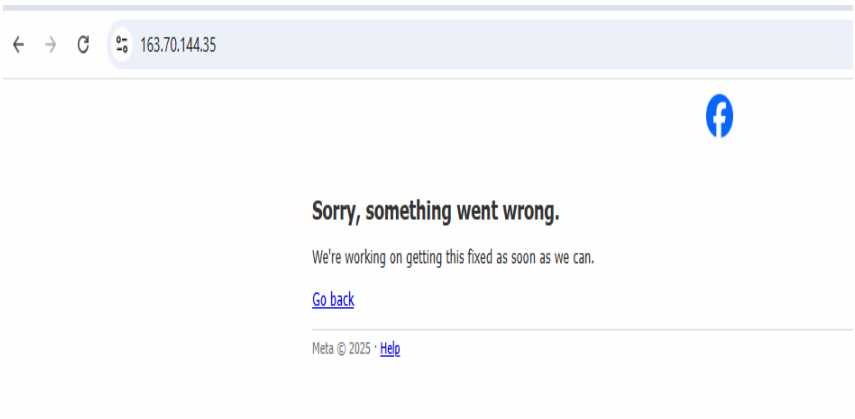
A. Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account

MUST Create your own Facebook account

1. Open Wireshark on your system.
2. Select the active network interface (Ethernet or Wi-Fi).
3. Once selected, Wireshark will start capturing packets.
4. Log in to your Facebook account only after Wireshark is running.
5. Open the Command Prompt and run:

ping facebook.com this will give you Facebook address
(eg for my machine 163.70.144.35 / 157.240.237.35)

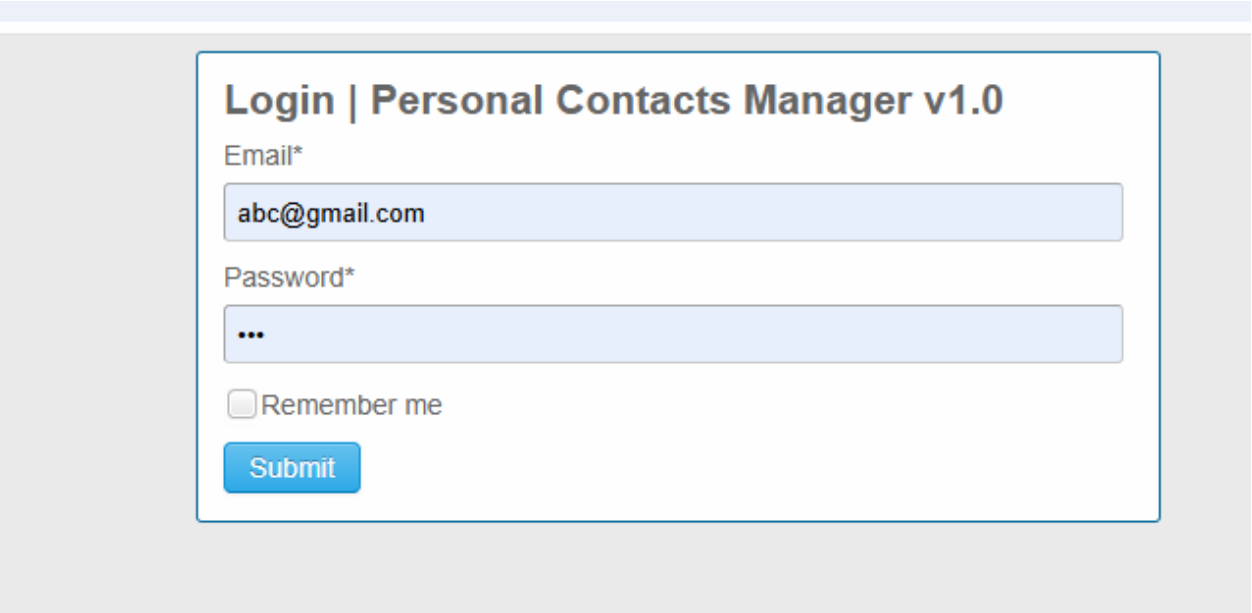
6. In Wireshark, apply a filter to capture only Facebook packets**:**
   tcp && ip.addr == 163.70.144.35 (Facebook id)
7. To verify, open your browser and enter the same IP address. If it opens Facebook, you know the captured packets belong to Facebook**.**



B. Capture all HTTP traffic to/from Facebook (other website), when you log in to your Facebook account

1. 1st you need to open http website like techpanda.org

2. you have to enter any sample email & enter password and click on submit



3. You will get

Dashboard | Personal Contacts Manager v1.0

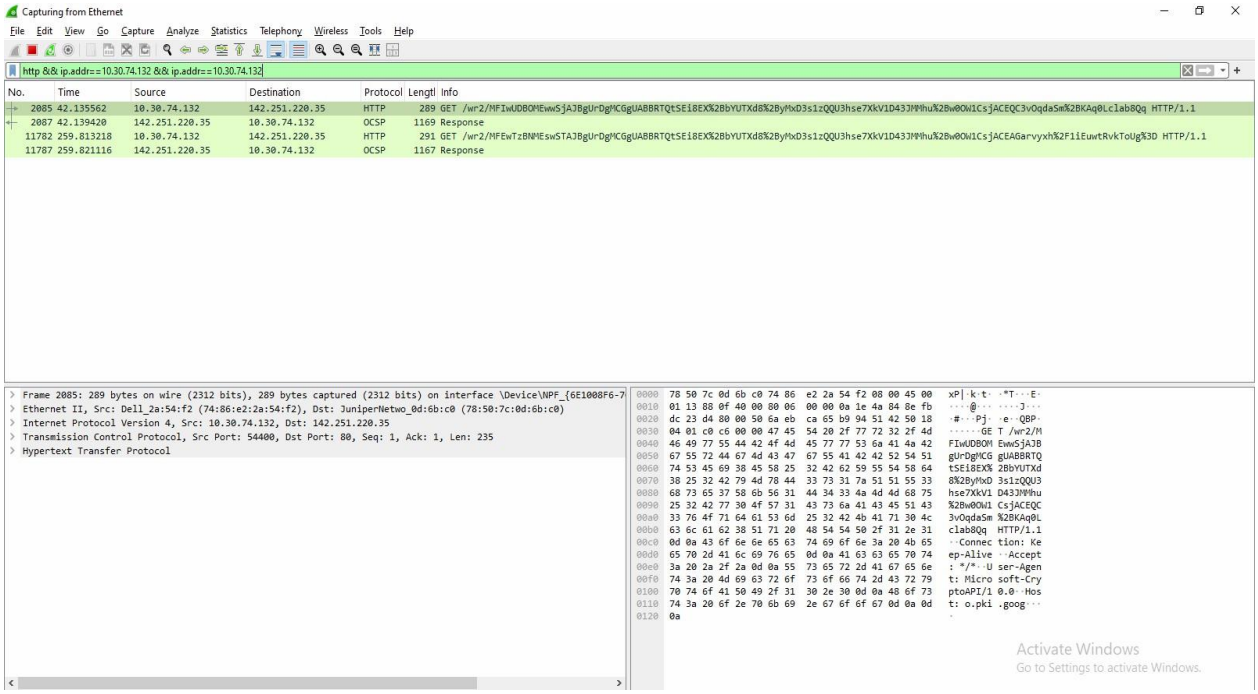
Add New Contact | Log Out

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
99213	asfe	liilhl	13230842384	admin@example.com	Edit
99214	shreya	shinde	8999235684	shrreyanb@gmail.com	Edit
99215	Bhupiiindra	JOGIIIII	828282828282	bhupjaaaaa2@jaa2.com	Edit
99216	Sandesh	Pawar	9999999999	sandesh@snapchat.com	Edit
99217	Yash	Pawar	9658741230	yash16@gmail.com	Edit
99218	protagonist	netent	946987582315	admin@google.com	Edit
99219	anurag	Satav	0000000000	admin@google.com	Edit
99220	j	s	123	j@gmail.com	Edit
99221	jy	sh	456	js@gmail.com	Edit
99222	Jack	Sparrow	0987654321	Captain@gmail.com	Edit
99223	ksjbdck	sdvcS	65846345435	abc@gmail.com	Edit
99224	Jaaxfgnb rmtdgsncv wswjodw1	aq	zsGTRY	hiray@info.com	Edit
99225	tgfse	Patel	73839903	sheikhnamra42@gmail.com	Edit
99226	soooo	hammmm	5465891265	admin@google.com	Edit
99227	Dark	lewis	1234567	admin@xyz.com	Edit

Total Records Count: 16

3. Open cmd and give command and ping techpanda.org then you will get connectivity with

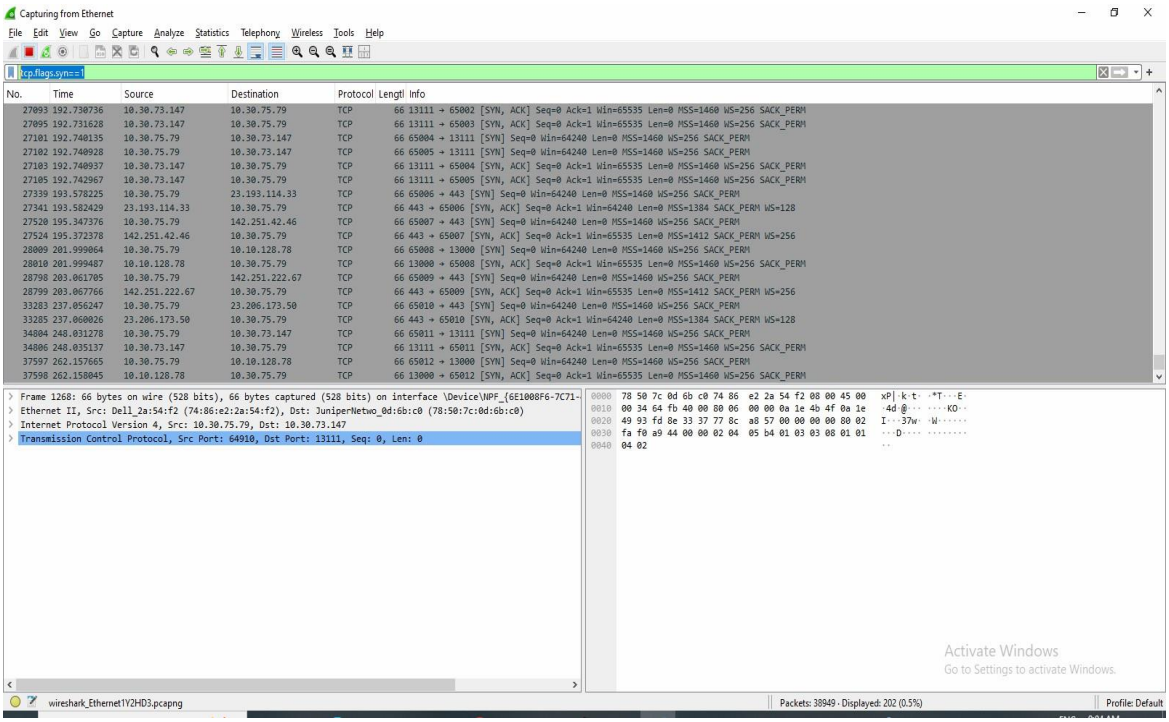
5. http && ip.addr==10.30.74.132 (Machine IP) && ip.addr==271.174.153.52 (techpanda.org ip) (imp command)



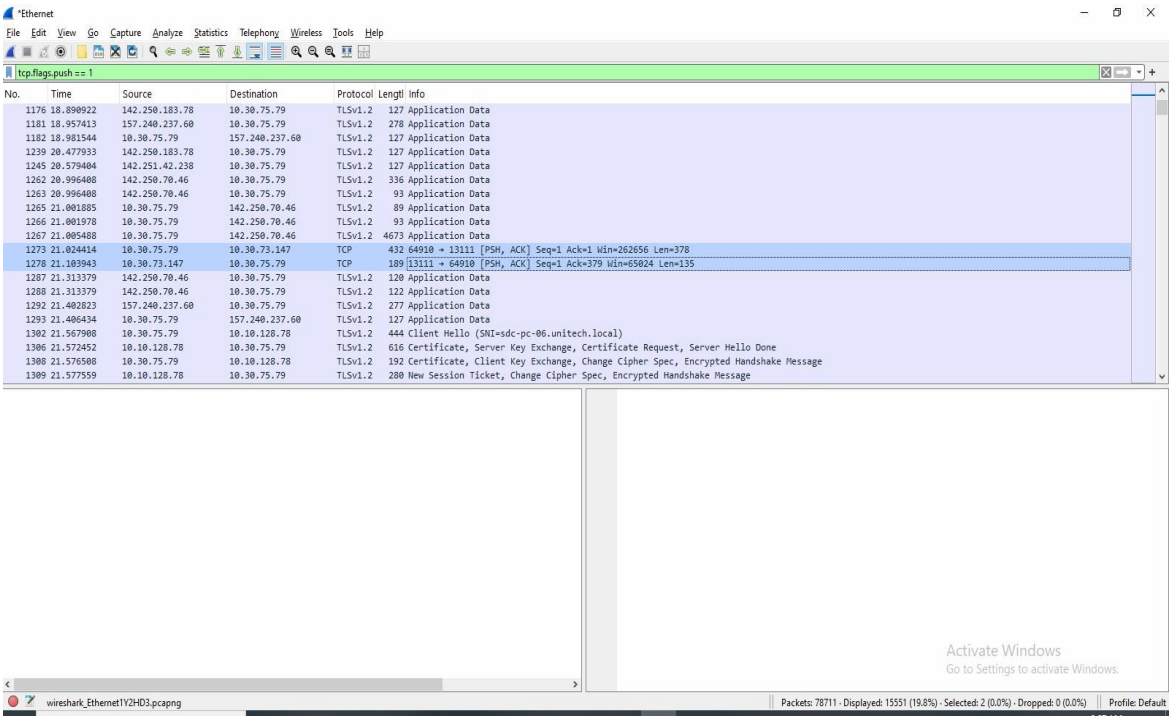
3 & 4. Write a DISPLAY filter expression to count all TCP packets (captured under item #1)

that have the flags SYN, PSH, and RST set. Show the fraction of packets that had each flag set.

tcp.flags.syn==1



tcp.flags.push == 1



tcp.flags.reset == 1