

Wireshark Practical

Practical no 10

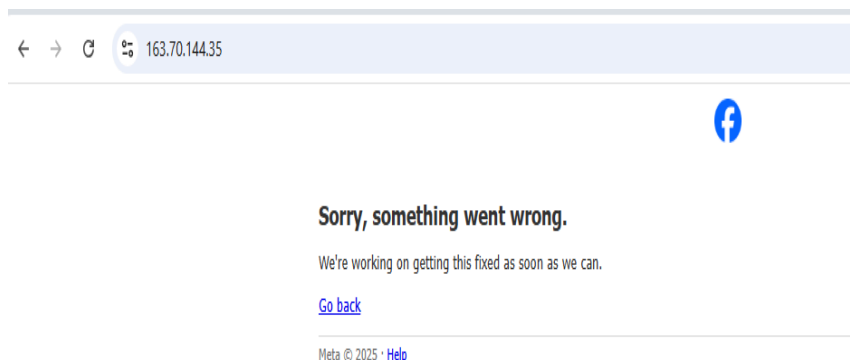
A. Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account

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)**

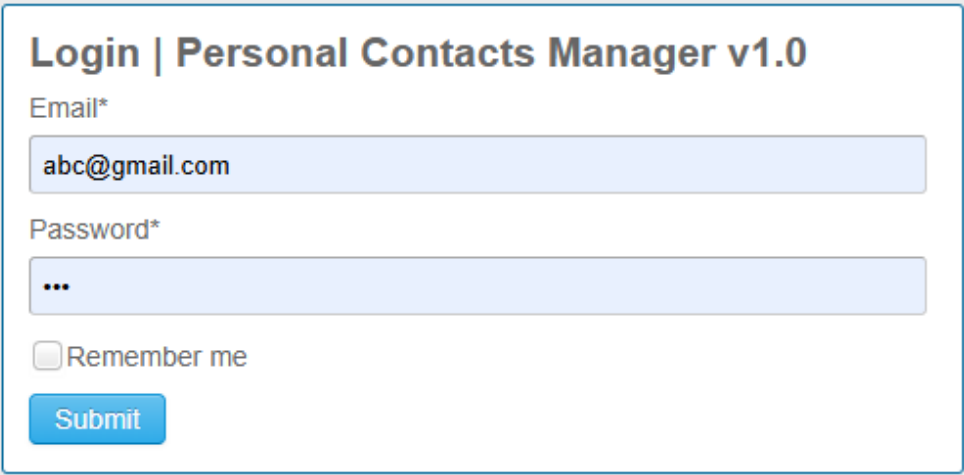
6. In Wireshark, apply a filter to capture only Facebook packets:
tcp && ip.addr == 163.70.144.35 (Facebook id)
7. To verify, open your browser and enter the same IP address. If it opens Facebook, you know the captured packets belong to Facebook.



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



The image shows a login form titled "Login | Personal Contacts Manager v1.0". It contains two input fields: "Email*" with the value "abc@gmail.com" and "Password*" with masked characters "...". Below the password field is a checkbox labeled "Remember me" which is unchecked. At the bottom is a blue "Submit" button.

Login | Personal Contacts Manager v1.0

Email*

abc@gmail.com

Password*

...

☐ Remember me

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	liihl	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 && ip.addr==10.30.74.132` (imp command)

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http && ip.addr==10.30.74.132 && ip.addr==10.30.74.132

No.	Time	Source	Destination	Protocol	Length	Info
2885	42.135562	10.30.74.132	142.251.220.35	HTTP	289	GET /nr2/HPFWU0B0HEws5JA3B9UrDgKCGuABBRQTcSE18EXK28yYUTXd8X28yPhd3s1zQQU3hse7Xkv1D43JfPhuK28w0W1CsJACEQC3vQqda5mK28KAq0Lc1ab8Qq HTTP/1.1
2887	42.139428	142.251.220.35	10.30.74.132	OCSP	1169	Response
11782	259.813218	10.30.74.132	142.251.220.35	HTTP	291	GET /nr2/HPFWTzBNPESw5TA3B9UrDgKCGuABBRQTcSE18EXK28yYUTXd8X28yPhd3s1zQQU3hse7Xkv1D43JfPhuK28w0W1CsJACEAGarvyxhK2F11EwtrRvkt0UgK3D HTTP/1.1
11787	259.821116	142.251.220.35	10.30.74.132	OCSP	1167	Response

> Frame 2885: 289 bytes on wire (2312 bits), 289 bytes captured (2312 bits) on interface \Device\NPF_{6E1008F6-7...}

> Ethernet II, Src: Dell_2a:54:f2 (74:86:e2:2a:54:f2), Dst: JuniperNetwo_0d:6b:c0 (78:50:17:c0:d6:c0)

> Internet Protocol Version 4, Src: 10.30.74.132, Dst: 142.251.220.35

> Transmission Control Protocol, Src Port: 54400, Dst Port: 80, Seq: 1, Ack: 1, Len: 235

> Hypertext Transfer Protocol

0000 78 50 7c 0d 6b c0 74 86 e2 2a 54 f2 08 00 45 00 xP|k:t...T...E
0010 01 13 88 0f 40 00 80 06 00 00 0a 1e 4a 84 8e fb ...@...J...
0020 dc 23 04 00 00 50 6a eb ca 65 b9 94 51 42 50 18 #...PJ...e-QBP
0030 04 01 c0 c0 00 00 47 45 54 20 2f 77 72 32 2f 4dGE T /nr2/H
0040 46 49 77 55 44 42 4f 4d 45 77 77 53 6a 41 4a 42 F1wU0B0H Ews5JA3B
0050 67 55 72 44 67 4d 43 47 67 55 41 42 42 52 54 51 gUrDgKCG gUABBRQT
0060 74 53 45 69 38 45 58 25 32 42 62 59 55 54 58 64 tSE18EXK 28yYUTXd
0070 38 25 32 42 79 4d 78 44 33 73 31 7a 51 51 55 33 8X28yPhd 3s1zQQU3
0080 68 73 65 37 58 6b 56 31 44 34 33 4a 4d 4d 68 75 hse7Xkv1 D43JfPhu
0090 25 32 42 77 30 4f 57 31 43 73 6a 41 43 45 51 43 K28w0W1L CsJACEQC
00a0 33 76 4f 71 64 61 53 6d 25 32 42 4b 41 71 30 4c 3vQqda5m K28KAq0L
00b0 63 6c 61 62 38 51 71 20 48 54 54 50 2f 31 2e 31 c1ab8Qq HTTP/1.1
00c0 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 ..Connec tion: Ke
00d0 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65 70 74 ep-alive -Accept
00e0 3a 20 2a 2f 2a 0d 0a 55 73 65 72 2d 41 67 65 6e : */* -U ser-Agen
00f0 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 43 72 79 t: Micro soft-Cry
0100 70 74 6f 41 50 49 2f 31 30 2e 30 0d 0a 48 6f 73 ptoAPL/1 0.0 -Hos
0110 74 3a 20 6f 2e 70 6b 69 2e 67 6f 6f 67 0d 0a 0d t: o.pki .goog ..
0120 0a

Activate Windows
Go to Settings to activate Windows.

3.

tcp.flags.syn==1 && ip.addr ==10.30.74.132 && ip.addr ==157.240.242.14