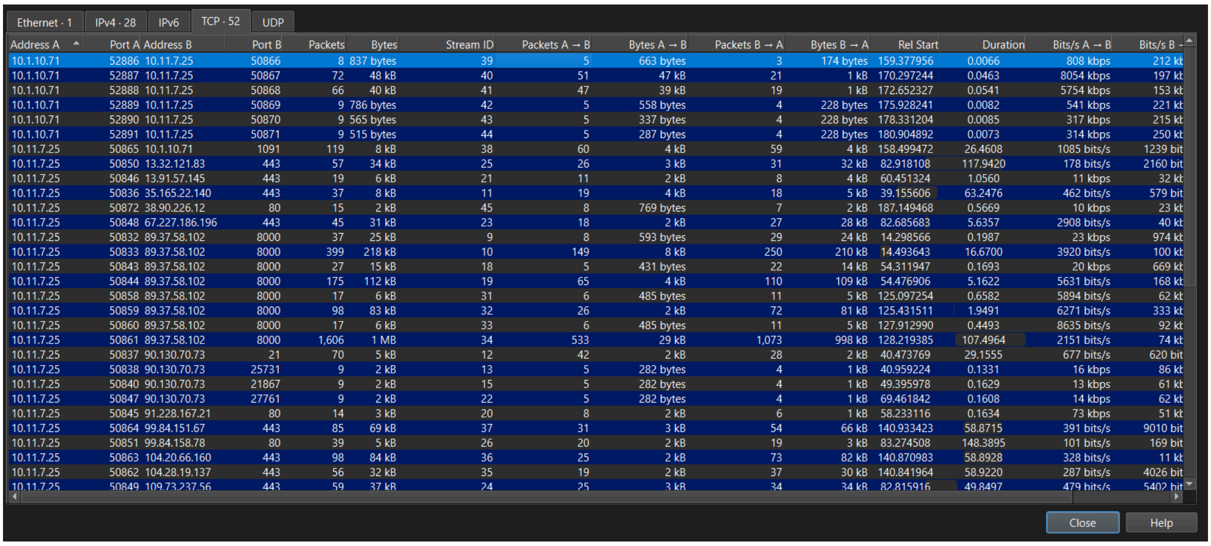
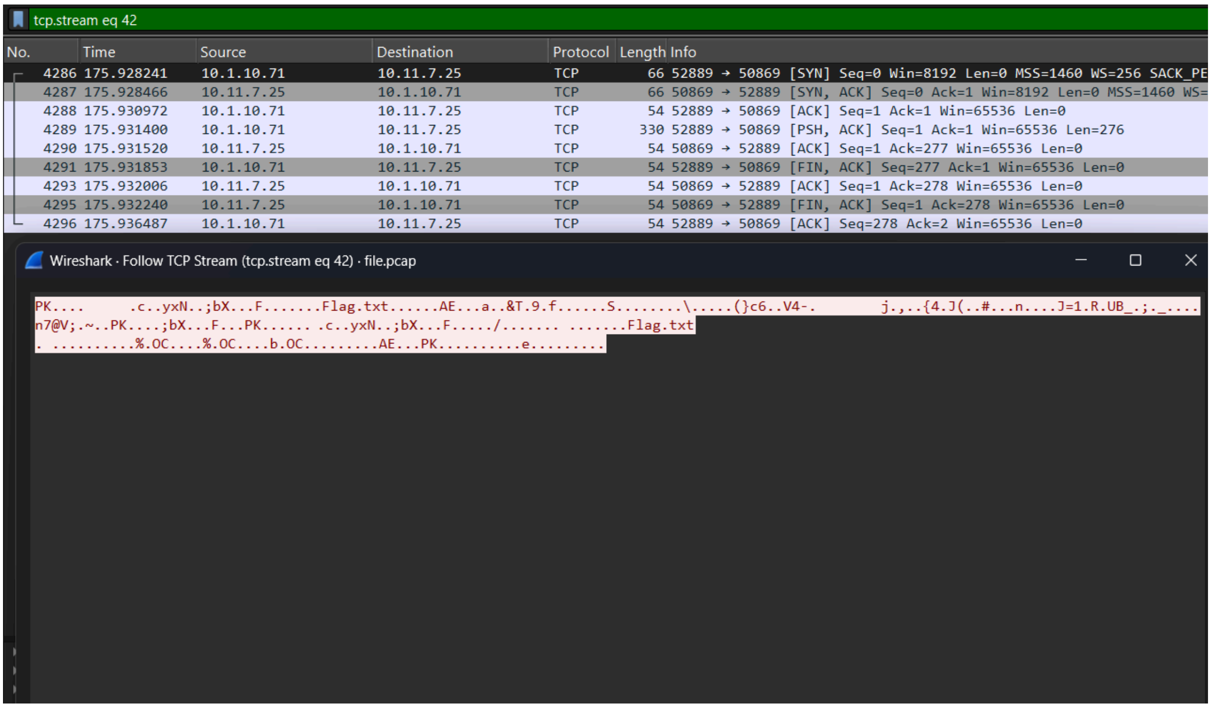
# I exported HTTP objects, I tried to open the **.img** files (useless), I searched for strings, I filtered by length. What this challenge is about is **tcp streams**. To see how many tcp streams are, go to **Statistics -> Conversations -> Select TCP**. In our case, you can see we have 52 TCP Streams :



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B -
10.1.10.71	52886	10.11.7.25	50866	8	837 bytes	39	5	663 bytes	3	174 bytes	159.377956	0.0066	808 kbps	212 kt
10.1.10.71	52887	10.11.7.25	50867	72	48 kB	40	51	47 kB	21	1 kB	170.297244	0.0463	8054 kbps	197 kt
10.1.10.71	52888	10.11.7.25	50868	66	40 kB	41	47	39 kB	19	1 kB	172.652327	0.0541	5754 kbps	153 kt
10.1.10.71	52889	10.11.7.25	50869	9	786 bytes	42	5	558 bytes	4	228 bytes	175.928241	0.0082	541 kbps	221 kt
10.1.10.71	52890	10.11.7.25	50870	9	565 bytes	43	5	337 bytes	4	228 bytes	178.331204	0.0085	317 kbps	215 kt
10.1.10.71	52891	10.11.7.25	50871	9	515 bytes	44	5	287 bytes	4	228 bytes	180.904892	0.0073	314 kbps	250 kt
10.11.7.25	50865	10.1.10.71	1091	119	8 kB	38	60	4 kB	59	4 kB	158.499472	26.4608	1085 bits/s	1239 bit
10.11.7.25	50850	13.32.121.83	443	57	34 kB	25	26	3 kB	31	32 kB	82.918108	117.9420	178 bits/s	2160 bit
10.11.7.25	50846	13.91.57.145	443	19	6 kB	21	11	2 kB	8	4 kB	60.451324	1.0560	11 kbps	32 kt
10.11.7.25	50836	35.165.22.140	443	37	8 kB	11	19	4 kB	18	5 kB	39.155606	63.2476	462 bits/s	579 bit
10.11.7.25	50872	38.90.226.12	80	15	2 kB	45	8	769 bytes	7	2 kB	187.149468	0.5669	10 kbps	23 kt
10.11.7.25	50848	67.227.186.196	443	45	31 kB	23	18	2 kB	27	28 kB	82.685683	5.6357	2908 bits/s	40 kt
10.11.7.25	50832	89.37.58.102	8000	37	25 kB	9	8	593 bytes	29	24 kB	14.298566	0.1987	23 kbps	974 kt
10.11.7.25	50833	89.37.58.102	8000	399	218 kB	10	149	8 kB	250	210 kB	14.493643	16.6700	3920 bits/s	100 kt
10.11.7.25	50843	89.37.58.102	8000	27	15 kB	18	5	431 bytes	22	14 kB	54.311947	0.1693	20 kbps	669 kt
10.11.7.25	50844	89.37.58.102	8000	175	112 kB	19	65	4 kB	110	109 kB	54.476906	5.1622	5631 bits/s	168 kt
10.11.7.25	50858	89.37.58.102	8000	17	6 kB	31	6	485 bytes	11	5 kB	125.097254	0.6582	5894 bits/s	62 kt
10.11.7.25	50859	89.37.58.102	8000	98	83 kB	32	26	2 kB	72	81 kB	125.431511	1.9491	6271 bits/s	333 kt
10.11.7.25	50860	89.37.58.102	8000	17	6 kB	33	6	485 bytes	11	5 kB	127.912990	0.4493	8635 bits/s	92 kt
10.11.7.25	50861	89.37.58.102	8000	1,606	1 MB	34	533	29 kB	1,073	998 kB	128.219385	107.4964	2151 bits/s	74 kt
10.11.7.25	50837	90.130.70.73	21	70	5 kB	12	42	2 kB	28	2 kB	40.473769	29.1555	677 bits/s	620 bit
10.11.7.25	50838	90.130.70.73	25731	9	2 kB	13	5	282 bytes	4	1 kB	40.959224	0.1331	16 kbps	86 kt
10.11.7.25	50840	90.130.70.73	21867	9	2 kB	15	5	282 bytes	4	1 kB	49.395978	0.1629	13 kbps	61 kt
10.11.7.25	50847	90.130.70.73	27761	9	2 kB	22	5	282 bytes	4	1 kB	69.461842	0.1608	14 kbps	62 kt
10.11.7.25	50845	91.228.167.21	80	14	3 kB	20	8	2 kB	6	1 kB	58.233116	0.1634	73 kbps	51 kt
10.11.7.25	50864	99.84.151.67	443	85	69 kB	37	31	3 kB	54	66 kB	140.933423	58.8715	391 bits/s	9010 bit
10.11.7.25	50851	99.84.158.78	80	39	5 kB	26	20	2 kB	19	3 kB	83.274508	148.3895	101 bits/s	169 bit
10.11.7.25	50863	104.20.66.160	443	98	84 kB	36	25	2 kB	73	82 kB	140.870983	58.8928	328 bits/s	11 kt
10.11.7.25	50862	104.28.19.137	443	56	32 kB	35	19	2 kB	37	30 kB	140.841964	58.9220	287 bits/s	4026 bit
10.11.7.25	50849	109.73.237.56	443	59	37 kB	24	25	3 kB	34	34 kB	82.815916	49.8497	479 bits/s	5402 bit

# Now go to Wireshark and filter **tcp.stream eq {number}** and then **select packets (right click) -> Follow -> TCP Stream.** At **tcp.stream eq 42** we got an archive :



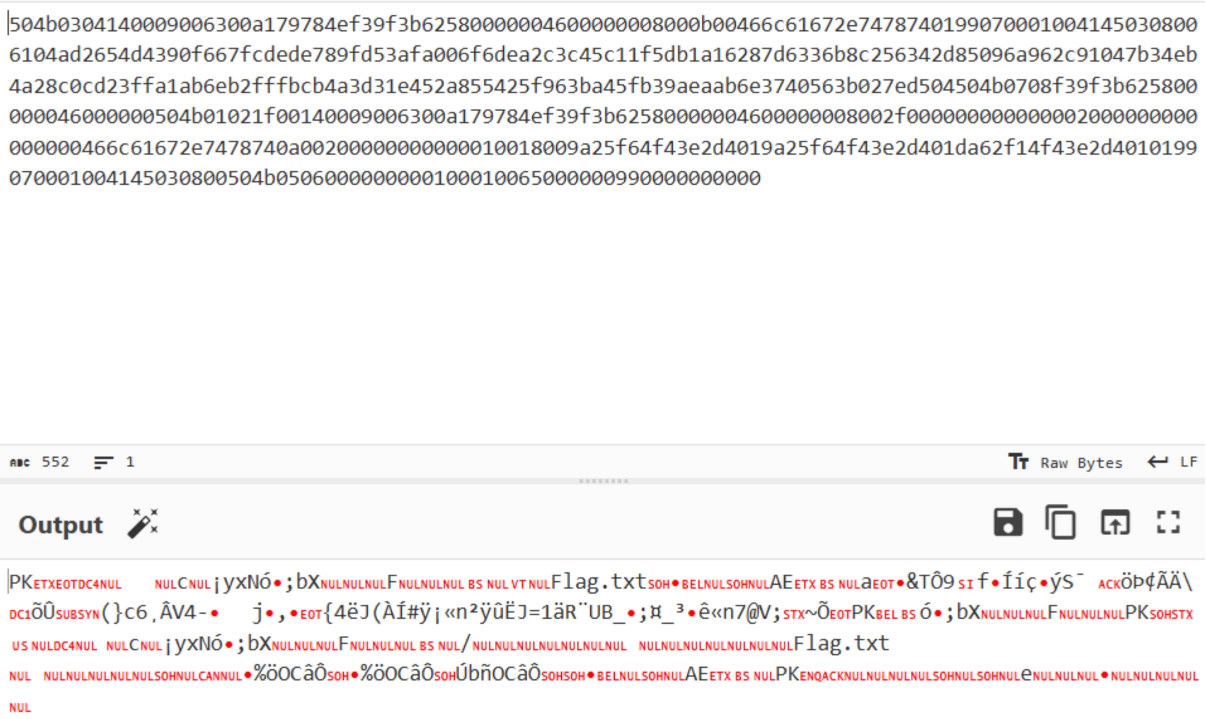
tcp.stream eq 42

No.	Time	Source	Destination	Protocol	Length	Info
4286	175.928241	10.1.10.71	10.11.7.25	TCP	66	52889 → 50869 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE
4287	175.928466	10.11.7.25	10.1.10.71	TCP	66	50869 → 52889 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=
4288	175.930972	10.1.10.71	10.11.7.25	TCP	54	52889 → 50869 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4289	175.931400	10.1.10.71	10.11.7.25	TCP	330	52889 → 50869 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=276
4290	175.931520	10.11.7.25	10.1.10.71	TCP	54	50869 → 52889 [ACK] Seq=1 Ack=277 Win=65536 Len=0
4291	175.931853	10.1.10.71	10.11.7.25	TCP	54	52889 → 50869 [FIN, ACK] Seq=277 Ack=1 Win=65536 Len=0
4293	175.932006	10.11.7.25	10.1.10.71	TCP	54	50869 → 52889 [ACK] Seq=1 Ack=278 Win=65536 Len=0
4295	175.932240	10.11.7.25	10.1.10.71	TCP	54	50869 → 52889 [FIN, ACK] Seq=1 Ack=278 Win=65536 Len=0
4296	175.936487	10.1.10.71	10.11.7.25	TCP	54	52889 → 50869 [ACK] Seq=278 Ack=2 Win=65536 Len=0

Wireshark · Follow TCP Stream (tcp.stream eq 42) · file.pcap

```
PK....      .c..yxN..;bX...F.......Flag.txt......AE...a..&T.9.f......S........\.....(}c6..V4-.       j.,..{4.J(..#...n....J=1.R.UB_.;._....
n7@V;.~..PK....;bX...F...PK...... .c..yxN..;bX...F...../....... .......Flag.txt
. ..........%.OC....%.OC....b.OC.........AE...PK..........e.........
```

# If we export the archive, it’s corrupted. So, I selected **Show as Raw.** Now, go to Cyberchef and upload the hex and save the archive :



```
504b0304140009006300a179784ef39f3b625800000046000000008000b00466c61672e7478740199070001004145030800
6104ad2654d4390f667fcdede789fd53afa006f6dea2c3c45c11f5db1a16287d6336b8c256342d85096a962c91047b34eb
4a28c0cd23ffa1ab6eb2fffbcb4a3d31e452a855425f963ba45fb39aeaab6e3740563b027ed504504b0708f39f3b625800
000046000000504b01021f00140009006300a179784ef39f3b62580000004600000008002f000000000000002000000000
000000466c61672e7478740a00200000000000010018009a25f64f43e2d4019a25f64f43e2d401da62f14f43e2d4010199
070001004145030800504b05060000000000100010065000000990000000000
```

```
PKETXEOTDC4NUL    NULCNUL¡yxNó•;bXNULNULNULFNULNULNUL BS NUL VT NULFlag.txtSOH•BELNULSOHNULAEETX BS NULaEOT•&TÔ9 SI f•Íîç•ýS¯ ACKÖÞ¢ÃÄ\
DC1ÕÛSUBSYN()}c6¸ÂV4-•   j•,•EOT{4ëJ(ÀÍ#ÿ¡«n²ÿûËJ=1äR¨UB_•;¤_³•ê«n7@V;STX~ÕEOTPKBEL BS ó•;bXNULNULNULFNULNULNULPKSOHSTX
US NULDC4NUL NULCNUL¡yxNó•;bXNULNULNULFNULNULNUL BS NUL/NULNULNULNULNULNULNUL NULNULNULNULNULNULNULFlag.txt
NUL NULNULNULNULNULSOHNULCANNUL•%öOCâÔSOH•%öOCâÔSOHÚbñOCâÔSOHSOH•BELNULSOHNULAEETX BS NULPKENQACKNULNULNULNULSOHNULSOHNULeNULNULNUL•NULNULNULNUL
NUL
```

# Now, the archive is protected with a password. Because, probably, it was in a previous tcp stream (because it didn't find it from 42 to 51) I tried to find the password with **strings** :

strings file.pcap | grep PASS

```
#PASS mozilla@example.com
#PASS mozilla@example.com
#PASS VADPRDqid4TaB0r5a2B0n9wLp
#PASS ftpuser
#PASS mozilla@example.com
#PASS password
```

# I was lucky. I also tried with **pass, password, PASSWORD**. Unzip the archive

THE FLAG :
ECSC{AC0DFD65CA16813A6AD68C4BA55F8C607496D93E2408EE0B5EF6F1B9ACCE0BC9}
~Z4que