LEVEL 02 :

```
level02@SnowCrash:~$ la -la
total 24
dr-x------ 1 level02 level02  120 Mar  5  2016 .
d--x--x--x 1 root    users    340 Aug 30  2015 ..
-r-x------ 1 level02 level02  220 Apr  3  2012 .bash_logout
-r-x------ 1 level02 level02 3518 Aug 30  2015 .bashrc
----r--r-- 1 flag02  level02 8302 Aug 30  2015 level02.pcap
-r-x------ 1 level02 level02  675 Apr  3  2012 .profile
level02@SnowCrash:~$
```

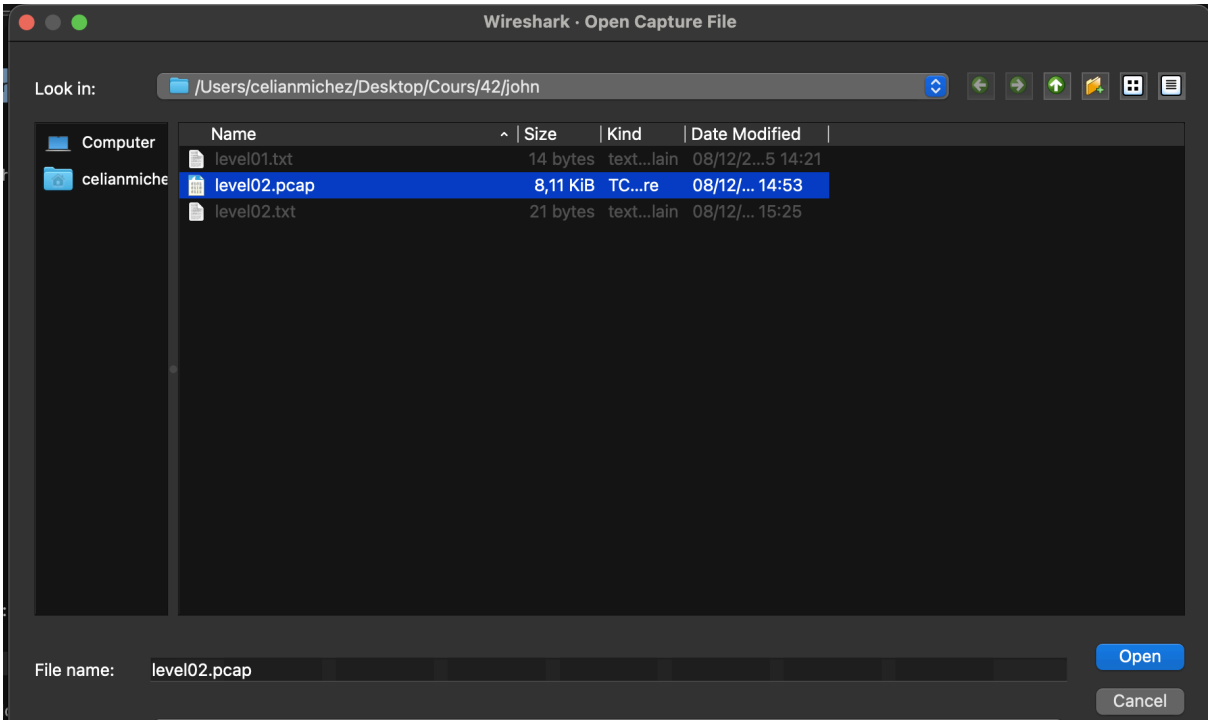
Dans le fichier home on a un .pcap. C'est une extension d'analyse de paquets.
On utilise donc wireshark pour lire ces paquets, pour cela on copie le fichier sur notre pc.

```
celianmichez@MacBook-Pro-de-Celian ~ % scp -P 4242 level02@10.18.196.83:/home/user/level02/level02.pcap .
         _____                      _____                 _
        / ____|                    / ____|               | |
       | (___  _ __   _____      _| |     _ __ __ _ ___| |__
        \___ \| '_ \ / _ \ \ /\ / / |    | '__/ _` / __| '_ \
        ____) | | | | (_) \ V  V /| |____| | | (_| \__ \ | | |
       |_____/|_| |_|\___/ \_/\_/  \_____|_|  \__,_|___/_| |_|

  Good luck & Have fun

          10.18.196.83
level02@10.18.196.83's password:
level02.pcap
celianmichez@MacBook-Pro-de-Celian ~ %
```

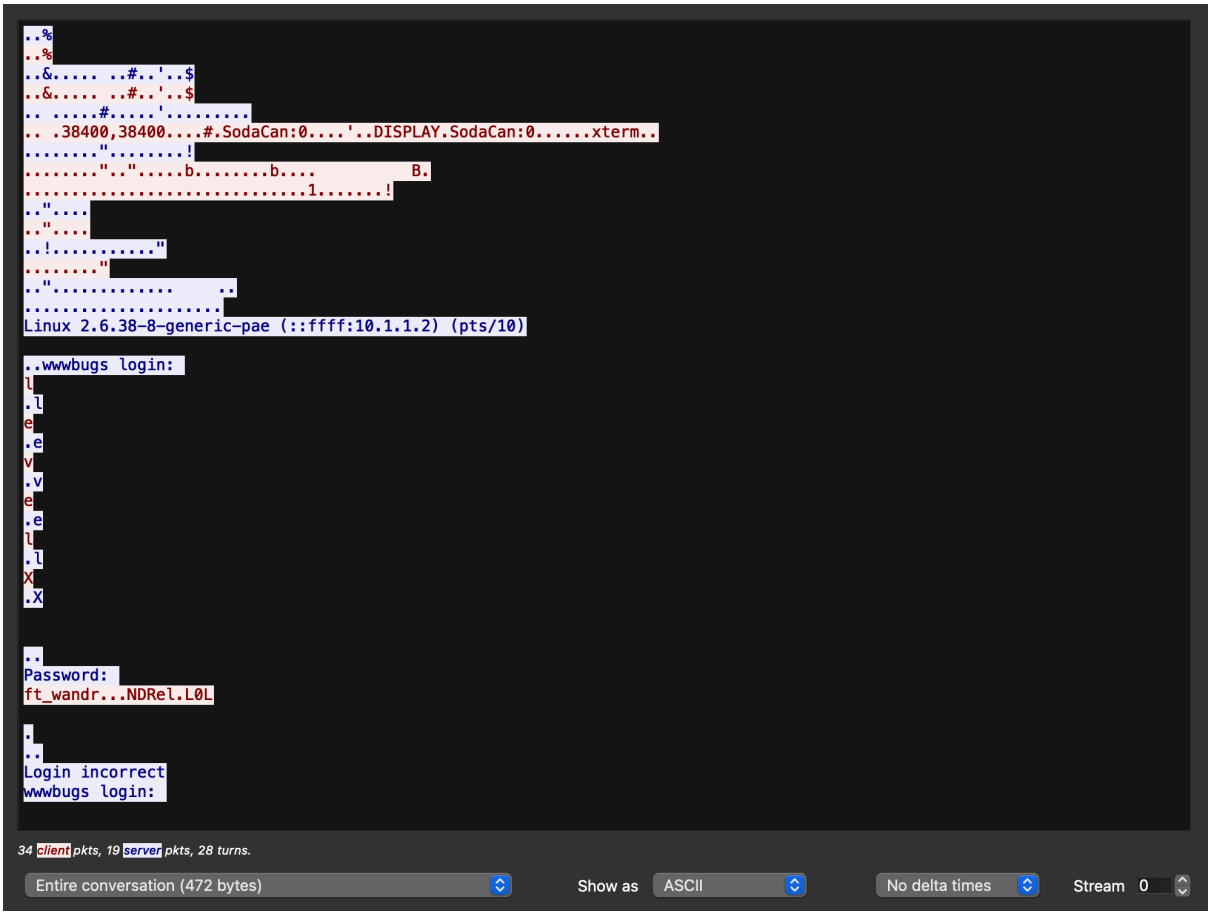
Maintenant on peut l'ouvrir avec Wireshark



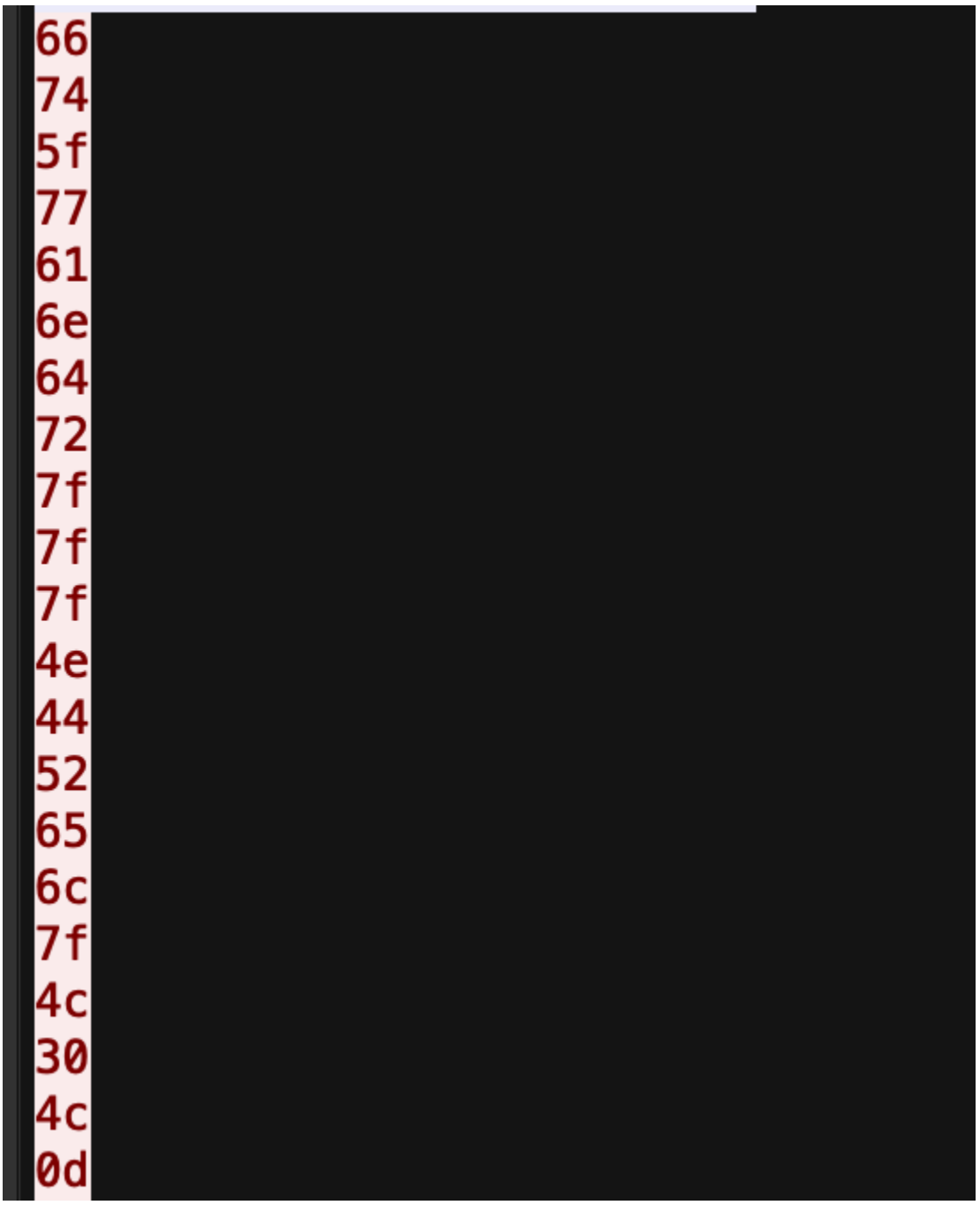
On a donc une liste de paquets.

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	59.233.235.218	59.233.235.223	TCP	74	39247 → 12121 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM TSval=18592800 TSecr=0 WS=128
2	0.000128	59.233.235.223	59.233.235.218	TCP	74	12121 → 39247 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=46280417 TSecr=18592800 WS=32
3	0.000390	59.233.235.218	59.233.235.223	TCP	66	39247 → 12121 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=18592800 TSecr=46280417
4	0.036008	59.233.235.223	59.233.235.218	TCP	69	12121 → 39247 [PSH, ACK] Seq=1 Ack=1 Win=14496 Len=3 TSval=46280426 TSecr=18592800
5	0.036255	59.233.235.218	59.233.235.223	TCP	66	39247 → 12121 [ACK] Seq=1 Ack=4 Win=14720 Len=0 TSval=18592804 TSecr=46280426
6	0.036276	59.233.235.218	59.233.235.223	TCP	69	39247 → 12121 [PSH, ACK] Seq=1 Ack=4 Win=14720 Len=3 TSval=18592804 TSecr=46280426
7	0.036396	59.233.235.223	59.233.235.218	TCP	66	12121 → 39247 [ACK] Seq=4 Ack=4 Win=14496 Len=0 TSval=46280426 TSecr=18592804
8	0.036581	59.233.235.223	59.233.235.218	TCP	84	12121 → 39247 [PSH, ACK] Seq=4 Ack=4 Win=14496 Len=18 TSval=46280426 TSecr=18592804
9	0.036698	59.233.235.218	59.233.235.223	TCP	84	39247 → 12121 [PSH, ACK] Seq=4 Ack=22 Win=14720 Len=18 TSval=18592804 TSecr=46280426
10	0.036859	59.233.235.223	59.233.235.218	TCP	90	12121 → 39247 [PSH, ACK] Seq=22 Ack=22 Win=14496 Len=24 TSval=46280426 TSecr=18592804
11	0.037039	59.233.235.218	59.233.235.223	TCP	133	39247 → 12121 [PSH, ACK] Seq=22 Ack=46 Win=14720 Len=67 TSval=18592804 TSecr=46280426
12	0.039170	59.233.235.223	59.233.235.218	TCP	84	12121 → 39247 [PSH, ACK] Seq=46 Ack=89 Win=14496 Len=18 TSval=46280427 TSecr=18592804
13	0.039392	59.233.235.218	59.233.235.223	TCP	140	39247 → 12121 [PSH, ACK] Seq=89 Ack=64 Win=14720 Len=74 TSval=18592804 TSecr=46280427
14	0.039704	59.233.235.223	59.233.235.218	TCP	73	12121 → 39247 [PSH, ACK] Seq=64 Ack=163 Win=14496 Len=7 TSval=46280427 TSecr=18592804
15	0.039842	59.233.235.218	59.233.235.223	TCP	73	39247 → 12121 [PSH, ACK] Seq=163 Ack=71 Win=14720 Len=7 TSval=18592804 TSecr=46280427
16	0.040138	59.233.235.223	59.233.235.218	TCP	81	12121 → 39247 [PSH, ACK] Seq=71 Ack=170 Win=14496 Len=15 TSval=46280427 TSecr=18592804
17	0.040277	59.233.235.218	59.233.235.223	TCP	75	39247 → 12121 [PSH, ACK] Seq=170 Ack=86 Win=14720 Len=9 TSval=18592804 TSecr=46280427
18	0.040450	59.233.235.223	59.233.235.218	TCP	107	12121 → 39247 [PSH, ACK] Seq=86 Ack=179 Win=14496 Len=41 TSval=46280427 TSecr=18592804
19	0.071743	59.233.235.218	59.233.235.223	TCP	66	39247 → 12121 [ACK] Seq=179 Ack=127 Win=14720 Len=0 TSval=18592808 TSecr=46280427
20	0.071825	59.233.235.223	59.233.235.218	TCP	141	12121 → 39247 [PSH, ACK] Seq=127 Ack=179 Win=14496 Len=75 TSval=46280435 TSecr=18592808

On peut voir le “resume” des paquets en faisant click droit, follow, tcp streams.



On peut voir le mot de passe ici. Le soucis c’est les “.” qui peuvent etre des caracteres non imprimables. Pour voir ca on va passer du mode ASCII a RAW.



On peut voir que les 3 “.” sont des 7F, se qui correspond au caractere DEL.
Du coup apres une petite manipulation de la chaine de caracteres on a : ft_waNDReL0L

```
level02@SnowCrash:~$ su flag02
Password:
Don't forget to launch getflag !
flag02@SnowCrash:~$ getflag
Check flag.Here is your token : kooda2puivaav1idi4f57q8iq
flag02@SnowCrash:~$
```

Le flag est donc : kooda2puivaav1idi4f57q8iq