level02

This time around, we delved into something quite intriguing at home, a *.pcap* file. This file encapsulates packet data from a network, facilitating the analysis and management of network traffic and status.

```
level02@SnowCrash:~$ ls
level02.pcap
master:~$ scp -P 4242 level02@xxx.xxx.xxx.xxx:level02.pcap ./level02.pcap
```

In order to dissect this file, we scoured the internet for suitable software. Among the available options, *Wireshark* emerged as the most robust and user-friendly network protocol analyzer.
However, before diving into analysis, we had to transfer the .pcap file from the virtual machine to our local system. This was accomplished using the *"scp"* command, which stands for *Secure Copy Protocol*.

With the file on our local machine, we fired up Wireshark and initiated a thorough examination.
In Wireshark, by navigating through: *Right-click* > *Follow* > *TCP Stream*, we observed a user attempting a password entry, which was flagged as incorrect.

```
..wwwbugs login: l.le.ev.ve.el.lX.X
..
Password: ft_wandr...NDRel.L0L
.
..
Login incorrect
```

Upon closer inspection and after some tinkering, we discerned that the occurrences of "." within the password were actually representing backspace inputs. This led us to correct the password:

ft_wandr...NDRel.L0L -> ft_waNDReL0L

```
level02@SnowCrash:~$ su flag02
Password: ft_waNDReL0L
Don't forget to launch getflag !

flag02@SnowCrash:~$ getflag
Check flag.Here is your token : kooda2puivaav1idi4f57q8iq

flag02@SnowCrash:~$ su level03
Password: kooda2puivaav1idi4f57q8iq

level03@SnowCrash:~$
```