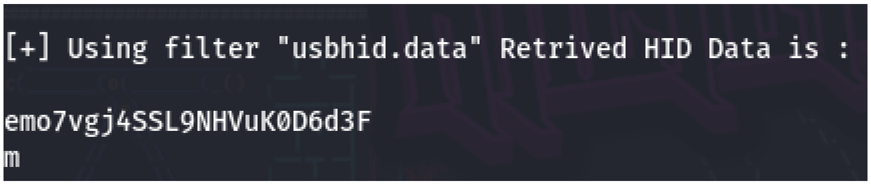
After opening the tshark, I get the feeling it might be some sort of keylogger since there is only USB traffic.

Credits to https://github.com/5h4rrK/CTF-Usb_Keyboard_Parser/blob/main/Usb_Keyboard_Parser.py

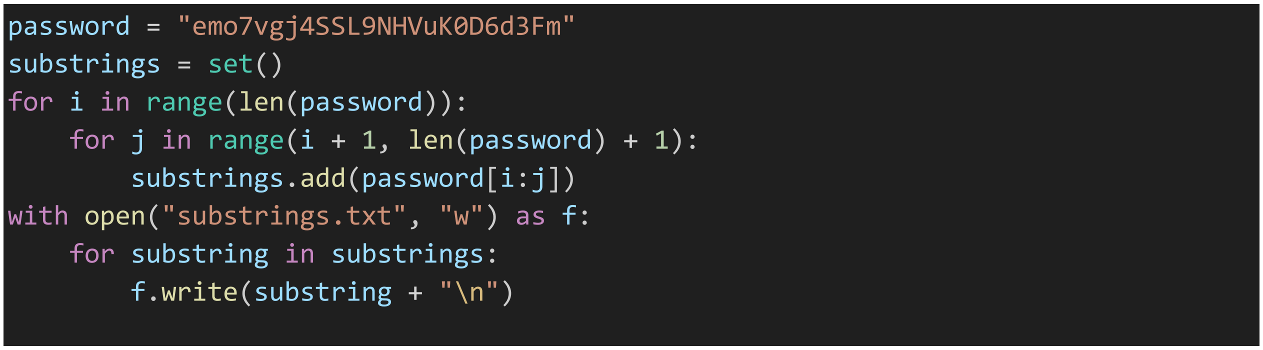


```
[+] Using filter "usbhid.data" Retrived HID Data is :

emo7vgj4SSL9NHVuK0D6d3F
m
```

I also ran binwalk to see if there is any hidden file, and I found a zip which I quickly retrieved.

The password we found doesn’t work, meaning that the script must have extracted some extra characters



```
password = "emo7vgj4SSL9NHVuK0D6d3Fm"
substrings = set()
for i in range(len(password)):
    for j in range(i + 1, len(password) + 1):
        substrings.add(password[i:j])
with open("substrings.txt", "w") as f:
    for substring in substrings:
        f.write(substring + "\n")
```

Now that we generated all possible passwords, we use fcrack to break it, get the password and the flag.

Made with love by: AndreiCat