This Flag we were on the ip 10.162.2.83 from the previous flag we got root privilege, on the machine we created **ssh private and public keys** and downloaded the private key on the kali machine.

From here we could connect with **ssh -i raskey.priv root@10.162.2.83** and connect to the ip. To sniff the packets at the machine we used the command
**tcpdump -i any -w tecpdump.pcap** this command dumps the packets from any (all) the interfaces on the ip. We connected to the machine with another shell to send some more traffic to the machine, e.g ssh login traffic, dns lookup, browsing the cuiteur website etc.

We then transferred this pcap file to our machine by on the target opening a simple python server with:

**python3 -m http.server 8000**

We could then do:

**wget http://10.162.2.83:8000/tecdump.pcap**

To download the file to our system.

With wireshark we could list the collected files, saw a http get request and in the response packet the flag was found. For finding it in the packets you can either do Ctrl+F and search for a string value in packet details or just follow tcp stream and switch between streams.
**X-Ethhak-Flag-Content: flag{14ce187311d0a4b945cc84d604e6c3f89939c7d272feaf}**

We tried to capture traffic under many different circumstances. For example, we saw that 127.0.0.53 was listening/an open connection(with command **ss -tlnp**), so doing a dns lookup triggered the http traffic which contained the flag in the header. We also tried to just login via ssh which also triggered it. The most important part seems to be that the -i any flag is set on the tcpdump command since you then listen on all interfaces.