

ECSC Estonia Prequalifier - covertchannel2

We are given a pcap file and wished good luck.

Opening it in wireshark all the packets seem fairly identical, a `lorem ipsum` text is transferred byte by byte through tcp payloads, but that does not seem to be the flag. Scrolling through the packets, `Wireshark` says that some packets have the `Urgent pointer` value set, but not the `Urgent bit`. This is probably a clue.

Using `tshark` to dump all the values of urgent pointers (I don't remember command, google it) we get values that look like this:

```
1088
1088
1072
1968
1776
1632
1632
1520
1568
...
```

Look fairly random at first, but when I thought about the flag format, which is `DDC{...}`, then the first two numbers being the same makes sense.

I tried dividing `1088` by the ASCII decimal value of `D`, which resulted in the value `16`. After dividing all the numbers by 16 and converting the decimals to ascii characters, we get the flag.