Writeup - LAN Party Panic

After opening the **capture.pcap** you can see many connection attempts, and no major data, so mostly something might be hidden in headers. Some clues, hints were given related to “fragmented packets” in the description, so if we look at IP Identification numbers more closely we will be able to see that for subnet 10.250. The IP Identification numbers were very random when compared to identification numbers to 192.168, so if we arrange the packets of 10.250 according in ascending time order and see IP Identification column we will be able to see that last 2 digits, when converted to ASCII gives us the flag

- tshark -r capture.pcap -T fields -e frame.time_epoch -e ip.src -e ip.id -E header=y -E separator=, > all_ids.csv
- awk -F, '$2 ~ /^10\.250\./ { print }' all_ids.csv > carriers.csv
- (head -n1 carriers.csv && tail -n +2 carriers.csv | sort -n -t, -k1,1) > carriers_sorted.csv
- awk -F ',' '{print $3}' carriers_sorted.csv