1. برای پیدا کردن flag ها، اول به نوع بندی تمام دیتا ها میشود پرداخت.
بعد از پیدا کردن انوع مختلف میشود انها را به تعداد تغییراتشان نوع بندی کرد
بعد میتوان با دنبال کردن منابع و دیتاهایی که این منابع حمل میکنند، میتوان flag ها را پیدا کرد.

Flag{778LQJ8}

Flag در پکتی با پروتکل TCP و length برابر با 13 و source port برابر با 20 و destination port برابر با 80 قرار دارد.

2.

TCP Packets : 26 packets, 25 with length of 0, with length of 13 containing the flag. The flag containing TCP packets has the source: 139.108.230.37 with port: 20, and the destination: 116.227.202.204 with port: 80.

UDP Packets: 30 packets with length of 8 just for the header and 0 in the message or data that they're transmitting. The packets are between different sources and destinations but in the same source port and destination port, each pair, both in 53.

ICMP Packets: 32 packets with length 28 in data and 5 for the headers. All the packets contain pinging requests which all but one have no response for. The only one with the multicast info, has the source of 7.157.46.241 and the destination of 238.16.112.231.