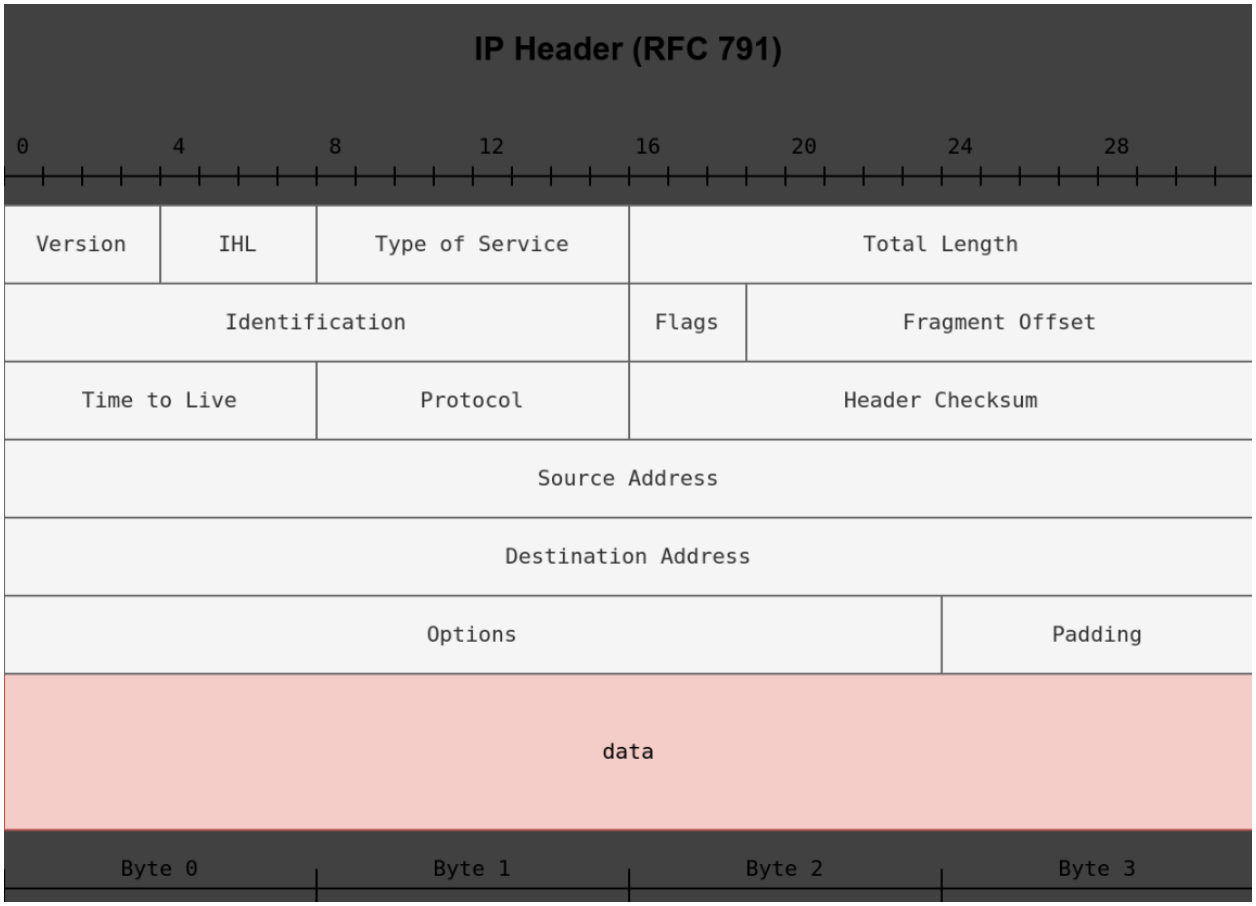
Nmap Fragmented Packets

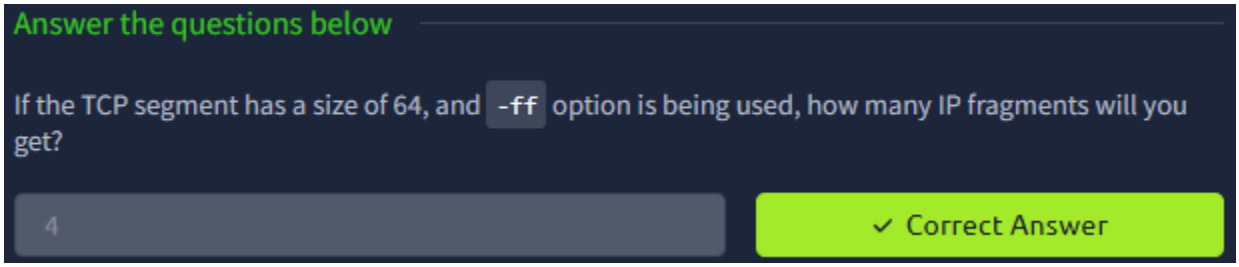
Firewall:
A firewall is a piece of software or hardware that permits/blocks packets. It functions based on **rules** that configure its ability to block or permit traffic based on the configuration. It may also contain exceptions, such as blocking all traffic except those coming to your web browser. A **traditional firewall inspects, IP header, and transport header** but a more **sophisticated firewall may try to examine data carried by the transport layer.**

IDS:
Intrusion Detection System, **inspects network packets for behavioural patterns or specific signatures.** It raises alerts whenever a malicious rule is met. In additional to the IP header and transport layer header the IDS **would also inspect data contents in the transport layer and check if it matches malicious patterns.** So the question I have is how to make it less likely to be flagged? The idea is sending it in much smaller packets.

Fragmented Packets:
Nmap provides the option to fragment packets **-f** to achieve this. Once chosen the IP data will be divided into 8 bytes or less… **Adding another -f (-f -f) or -ff will split the data into 16 bytes fragmented instead of 8.** You can change the value to –mtu **however you should ALWAYS choose a multiple of 8.**

To understand fragmentation, we need to look at the IP header. Notice the source address is taking 32bits (4 bytes) on the 4th row. Destination address is taking another 4bytes for the 5th row. The data that we will fragment across multiple packets is highlighted in red. IP uses the identification (ID) fragment offset show in the second row.





The answer is 4 because remembering the rule -ff where each f represents 8 bytes. -f would represent 8 bytes, and -ff is 16 bytes. So it would be 64 divided by 16bytes, creating 4 segments.