Heterograms

I completed this challenge with a combination of static and dynamic analysis. I used static analysis to first understand what the program was asking for and then used dynamic analysis to see where my input was failing and correct my input. The goal of this program is to make globalstate == 7, which will then return 1 and give you the flag. Globalstate starts at 0, and each time you send a successful packet (that is not for clearing out variables), globalstate increases by 1.

Packets can be separated into 2 types: packets that clear the array_buff and packets that set the array_buff.

All packets (both packets that clear the array_buff and packets that set the array_buff) have the following contents:

(*The first 2 bytes are fixed, but other values can be sent in different orders as long as values follow indications)

Byte	content
0	Length of payload (excluding this value)
1	Checksum (excluding this value)
2	Indication that following byte is the operation done on the array (Value = \x02)
3	Operation on array (0 for checking, 2 for erasing)
4	Indication that following byte is the value of globalstate from the user (Value = \x00)
5	globalstate

Packets that set the array_buff have a payload section with the following format:

Byte	content
6	Indication that following byte marks the start of payload (Value = \x01)
7	Length of payload
8-end of payload	payload

You can figure out the payload of a successful packet by analyzing strings in the binary. There are 7 strings to be analyzed in this program. This program wants the user to send packets that will set an array_buff for every string. Consider the mapping a->0, b->1, c->2, d->3,…, z->25. array_buff[x] needs to be set to 1 if the letter corresponding to x in the mapping is present in the string. The user constructs this array_buff by indicating at which indices the array_buff should be set to 1 through the payload.

After setting array_buff, the user also needs to be able to reset it so that it can be set again, which can be done by sending a packet without a payload that sticks to the conventions outlined in the tables above.

For each string successfully analyzed, globalstate increases by 1 and eventually hits 7, causing the program to return the flag.