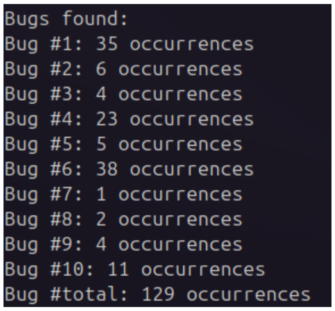
Design

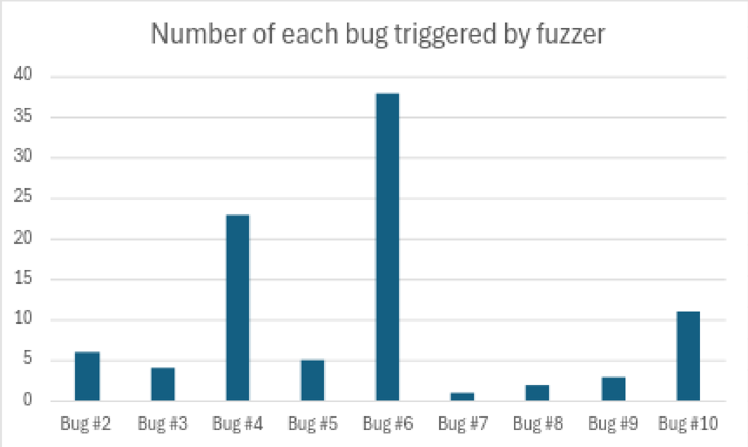
I designed my fuzzer in python. My original intent for the script was to mutate a random number of bytes in cross.jpg, but I have now realized that lines 67 and 68 are not doing what I thought they were. Regardless, I have sucessfully output all 10 bugs with my code. Instead, it is mutating one byte at a random position in cross.jpg with a new random value. My code does not use any rules, only random changes as it suffices in this use case. It then runs the application and outputs which bug was found. The code only saves the most recent bugged_input, as I do not need many of the same bug. This all repeats 1000 times.

Experimental Results

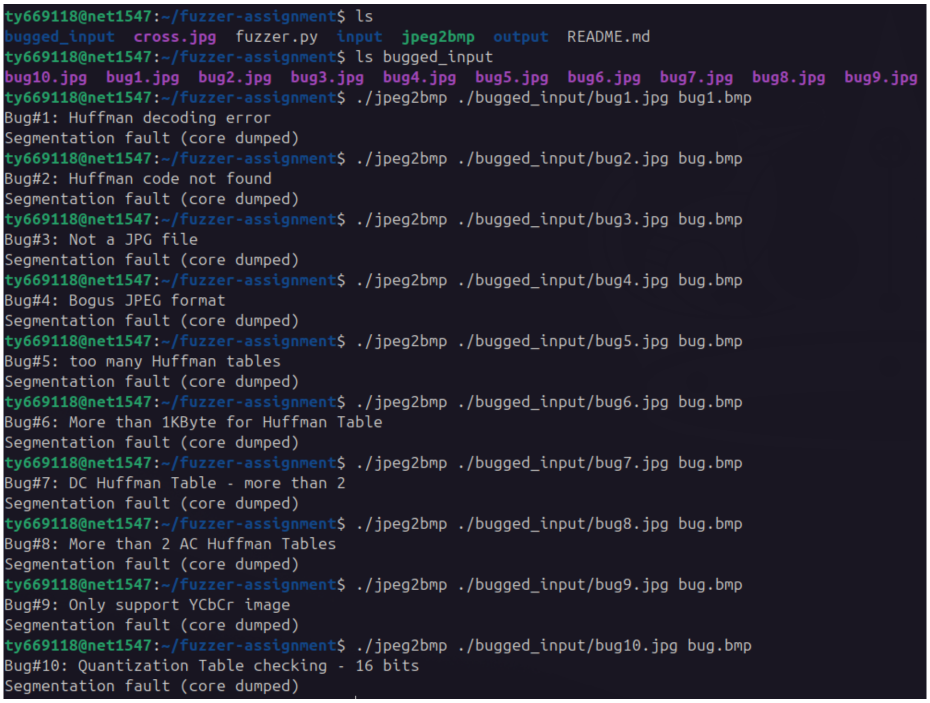


```
Bugs found:
Bug #1: 35 occurrences
Bug #2: 6 occurrences
Bug #3: 4 occurrences
Bug #4: 23 occurrences
Bug #5: 5 occurrences
Bug #6: 38 occurrences
Bug #7: 1 occurrences
Bug #8: 2 occurrences
Bug #9: 4 occurrences
Bug #10: 11 occurrences
Bug #total: 129 occurrences
```

	Bug #1	Bug #2	Bug #3	Bug #4	Bug #5	Bug #6	Bug #7	Bug #8	Bug #9	Bug #10
# of crashes triggered	35	6	4	23	5	38	1	2	3	11



Proof



```
ty669118@net1547:~/fuzzer-assignment$ ls
bugged_input  cross.jpg  fuzzer.py  input  jpeg2bmp  output  README.md
ty669118@net1547:~/fuzzer-assignment$ ls bugged_input
bug10.jpg  bug1.jpg  bug2.jpg  bug3.jpg  bug4.jpg  bug5.jpg  bug6.jpg  bug7.jpg  bug8.jpg  bug9.jpg
ty669118@net1547:~/fuzzer-assignment$ ./jpeg2bmp ./bugged_input/bug1.jpg bug1.bmp
Bug#1: Huffman decoding error
Segmentation fault (core dumped)
ty669118@net1547:~/fuzzer-assignment$ ./jpeg2bmp ./bugged_input/bug2.jpg bug.bmp
Bug#2: Huffman code not found
Segmentation fault (core dumped)
ty669118@net1547:~/fuzzer-assignment$ ./jpeg2bmp ./bugged_input/bug3.jpg bug.bmp
Bug#3: Not a JPG file
Segmentation fault (core dumped)
ty669118@net1547:~/fuzzer-assignment$ ./jpeg2bmp ./bugged_input/bug4.jpg bug.bmp
Bug#4: Bogus JPEG format
Segmentation fault (core dumped)
ty669118@net1547:~/fuzzer-assignment$ ./jpeg2bmp ./bugged_input/bug5.jpg bug.bmp
Bug#5: too many Huffman tables
Segmentation fault (core dumped)
ty669118@net1547:~/fuzzer-assignment$ ./jpeg2bmp ./bugged_input/bug6.jpg bug.bmp
Bug#6: More than 1KByte for Huffman Table
Segmentation fault (core dumped)
ty669118@net1547:~/fuzzer-assignment$ ./jpeg2bmp ./bugged_input/bug7.jpg bug.bmp
Bug#7: DC Huffman Table - more than 2
Segmentation fault (core dumped)
ty669118@net1547:~/fuzzer-assignment$ ./jpeg2bmp ./bugged_input/bug8.jpg bug.bmp
Bug#8: More than 2 AC Huffman Tables
Segmentation fault (core dumped)
ty669118@net1547:~/fuzzer-assignment$ ./jpeg2bmp ./bugged_input/bug9.jpg bug.bmp
Bug#9: Only support YCbCr image
Segmentation fault (core dumped)
ty669118@net1547:~/fuzzer-assignment$ ./jpeg2bmp ./bugged_input/bug10.jpg bug.bmp
Bug#10: Quantization Table checking - 16 bits
Segmentation fault (core dumped)
```