This program is designed to find the OS of a machine if they are running FreeBSD or Linux. In order to run this program you must first make sure the machine you want to check is up and running then you type in the command “sudo ./Lab5.py <IP address> with the IP address being the IP of the machine you want to test. To check if the OS is freeBSD I send one ICMP packet and take in its ID, then I send ten ICMP packets from a different src IP, then I send one more ICMP packet from my machine and compare the IDs from the first ICMP packet I sent from my machine to the second one I sent from my machine. Now the IDs are globally incrementing but every now and then FreeBSD throws a random number in as the ID so I had to give some wiggle room when comparing the IDs of the two ICMP packets sent from my machine. So when comparing them I checked to make sure they were around 10 away from each other since they probably weren’t going to be exactly ten away due to the random id every now and then. Then I due the comparison ten times and if the majority of the comparisons match the criteria then I assume the OS is FreeBSD. If those criteria aren’t met then I go on to check if it is a Linux machine. Since linux has a little harder to predict IPID incrementation I used the checksum portion of the header to guess the OS here. I noticed that the difference in checksum from the two ICMP packets from my machine were always between 1 and 25. So I did the same thing as before where I send an ICMP packet from my machine then send one from a spoofed address and then send one more from my machine again. I then compare the difference in the checksums of the two ICMP packets sent from my machine and if the difference is in the range 1-25 then I can assume it is a Linux machine. If neither of these are found then the program prints out “OS was not found”.

FreeBSD probably wouldn’t be able to be used as a zombie because of the random number thrown in every so often. If they didn’t have that it would be very easy to predict the IPID for each connection but since they have that it makes it very difficult to predict what number is going to be next over multiple connections because you know that eventually it’ll be wrong.