HW7\_23102009\_ParkShinhyung

Step1.

Command: ROPgadget --binary libc.so.6

The following command was executed to find a gadget that sets the rdi register:

Step2.

The gadget was identified in the command output.



Explain how the gadget work?

**pop rdi**: Pops a value from the stack and stores it in the rdi register.

**ret**: Returns control flow to the next address on the stack. This gadget is essential in Return-Oriented Programming (ROP) to set the rdi register with a specific value before a function call.