**Function Registers:**

**Arguments:** rdi, rsi, rdx, rcx, r8, r9

**Return Vals:** rax, rdx

**Callee Saved Registers:**  rbx, rsp, rbp, r12, r13, r14, r15

**Caller Saved Registers:** rax, rcx, rdx, rsi, rdi, r8, r9, r10, r11

**Segments:**

**Registers:** cs, ds, ss, es, gs, fs

Segment Selector (segment Index in segment descriptor table)

Privilege Levels (protection rings) are stored in the lowest two bits of **cs** or **ss**

**System Calls: man syscall**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Syscall | Arg1 | Arg2 | Arg3 | Arg4 | Arg5 | Arg6 |
| Rax | Rdi | Rsi | rdx | R10 | r8 | r9 |
| Write (1) | Where | Buf | size |  |  |  |
| Exit (60) | code |  |  |  |  |  |
| Read (2) | Where | Buf | size |  |  |  |

**Endianness:**

**demo3: dq 0x1234**

|  |  |  |
| --- | --- | --- |
| Address | Little Endian | Big Endian |
| Demo3 | 0x34 | 0x00 |
| Demo3 + 1 | 0x12 | 0x00 |
| Demo 3 + 2 | 0x00 | 0x00 |
| Demo3 + 3 | 0x00 | 0x00 |
| Demo3 + 4 | 0x00 | 0x00 |
| Demo3 + 5 | 0x00 | 0x00 |
| Demo3 + 6 | 0x00 | 0x12 |
| Demo3 + 7 | 0x00 | 0x34 |

**Div Example**

mov rax, 53 ; Bottom 32 bits of the number to be divided

mov rdx, 0 ; Top 32 bits of the number to be divided

mov r10, 10 ; The value we are diving by

div r10 ; divide rdx:rax by r10

; **rax** holds 5 (**value**), **rdx** holds 3 (**mod**)

**Register slices**

|  |  |  |  |
| --- | --- | --- | --- |
| 64 Bit Register | Lower 32 Bits | Lower 16 bits | Lower 8 bits |
| Rax | Eax | Ax | Al |
| Rbx | Ebx | Bx | Bl |
| Rcx | Ecx | Cx | Cl |
| Rdx | Edx | Dx | Dl |
| Rsi | Esi | Si | Sil |
| Rdi | Edi | Di | Dil |
| Rbp | Ebp | Bp | Bpl |
| Rsp | Esp | Sp | Spl |
| R[number] | R[number]d | R[number]w | R[number]b |

**processor modes**

* Real mode (oldest mode, 16 bit)
* Protected (commonly called 32 bit)
* Virtual (emulate real mode inside protected)
* System Management Mode (for sleep mode, power management, etc)
* Long mode, the one we are familiar with (64 bit)

