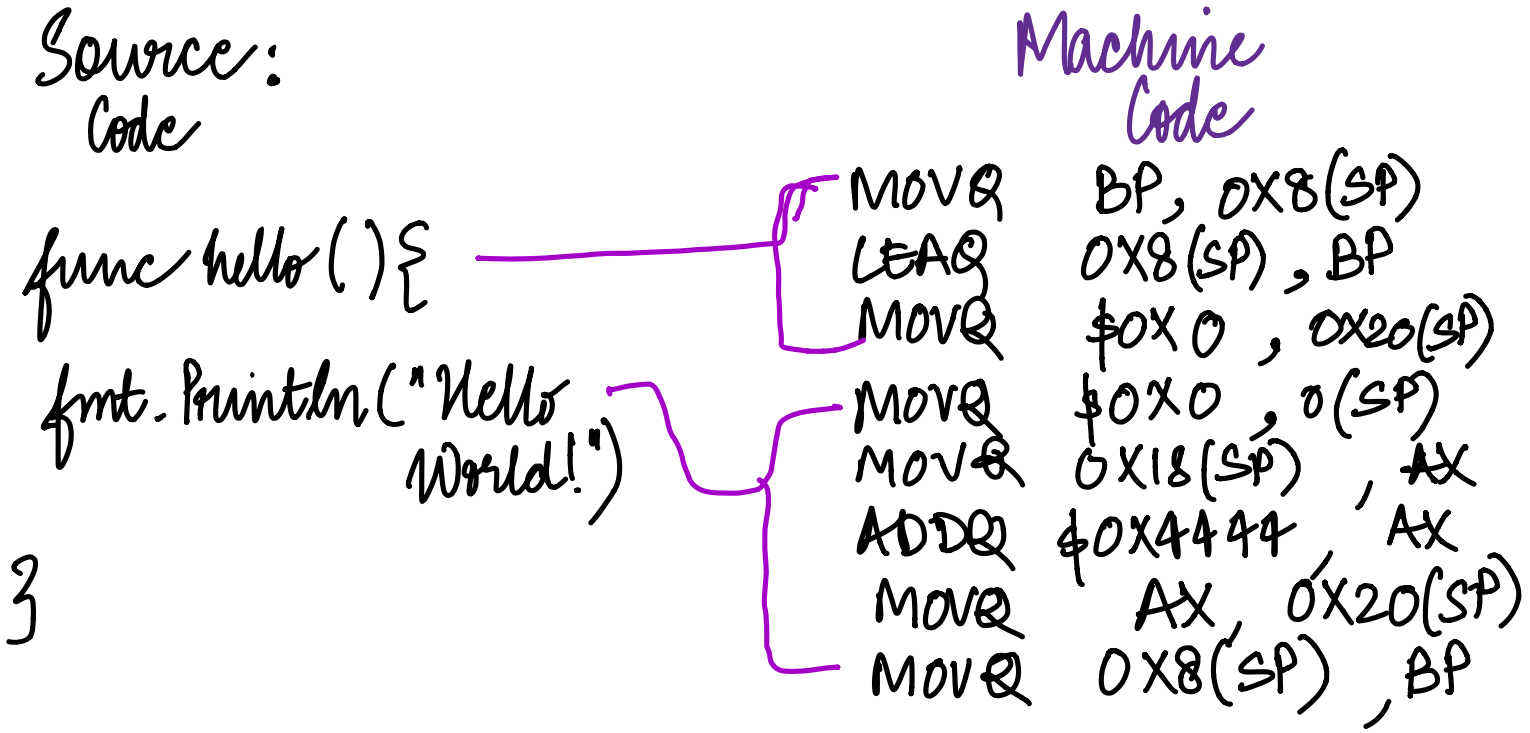
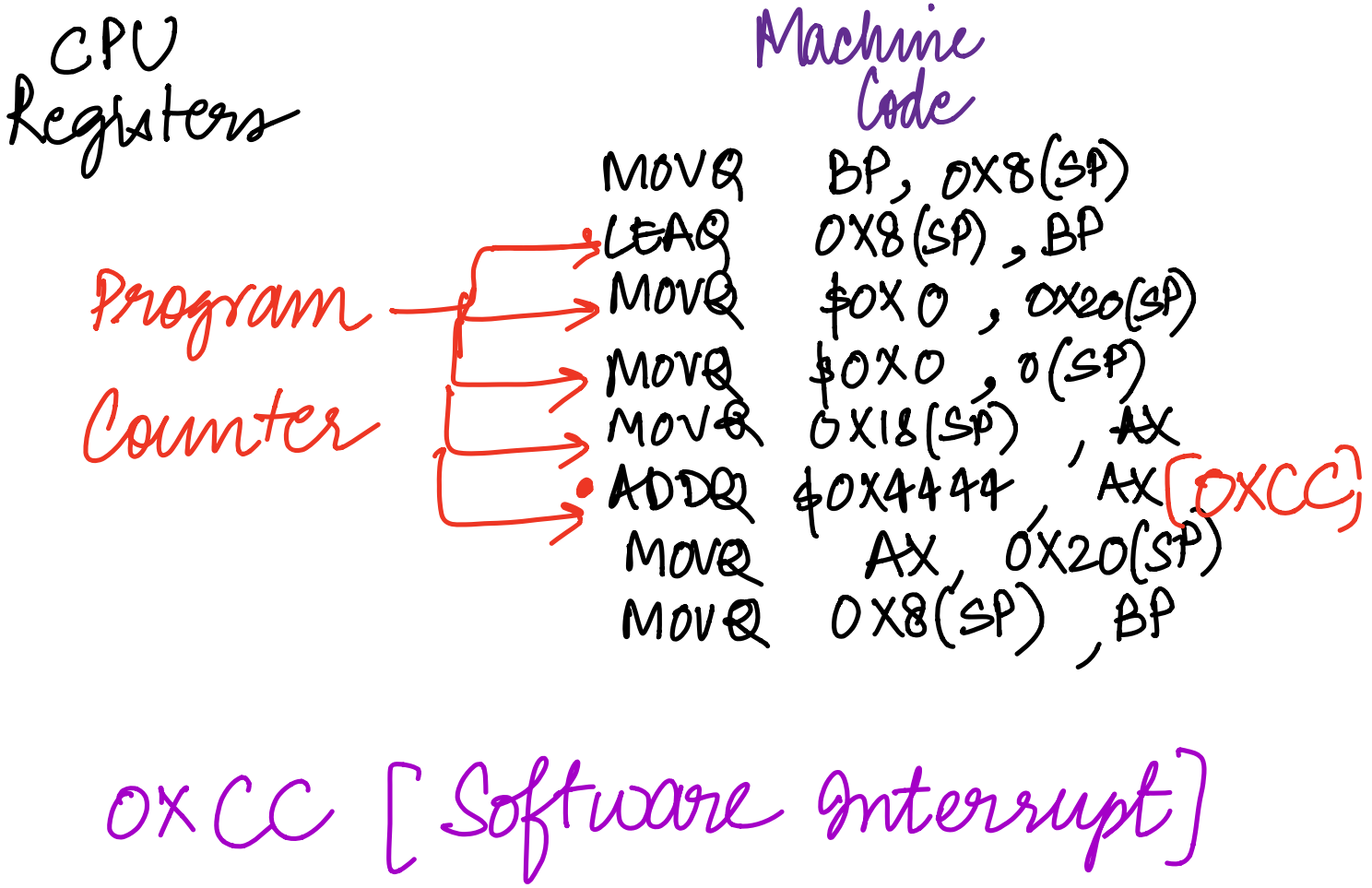
Debugger From Scratch.

★★ Star of the show ★★

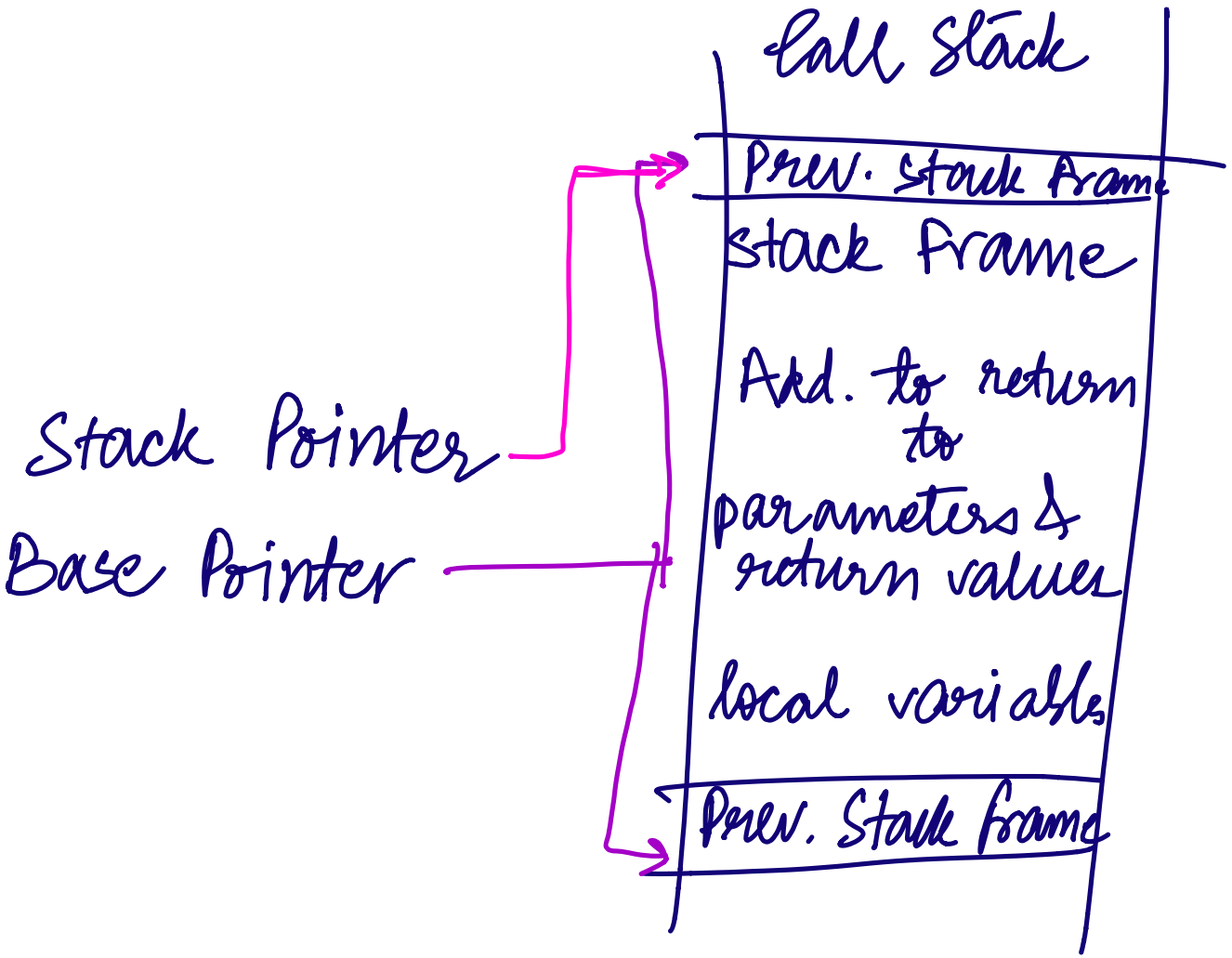
ptrace

- a system call
- allows one process (tracer) to control the execution of another process (tracee)
- allows examining & changing memory & registers


Source Code:
func hello(){
fmt.Println("Hello World!")
}
Machine Code
MOVQ BP, 0X8(SP)
LEAQ 0X8(SP), BP
MOVQ $0X0, 0X20(SP)
MOVQ $0X0, 0(SP)
MOVQ 0X18(SP), AX
ADDQ $0X4444, AX
MOVQ AX, 0X20(SP)
MOVQ 0X8(SP), BP



0xCC [Software Interrupt]


Call Stack
Prev. Stack Frame
stack frame
Add. to return to
parameters &
return values
local variables
Prev. Stack Frame
Stack Pointer
Base Pointer

"ELF & DWARF"

- Executable Link Format

```
$ readelf -h hello
ELF Header:
 Magic: 7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
 Class: ELF64
 Data: 2's complement, little endian
 Version: 1 (current)
 OS/ABI: UNIX - System V
 ABI Version: 0
 Type: EXEC (Executable file)
 Machine: Advanced Micro Devices X86-64
 Version: 0x1
 Entry point address: 0x456420
 Start of program headers: 64 (bytes into file)
 Start of section headers: 456 (bytes into file)
 Flags: 0x0
 Size of this header: 64 (bytes)
 Size of program headers: 56 (bytes)
 Number of program headers: 7
 Size of section headers: 64 (bytes)
 Number of section headers: 23
 Section header string table index: 3
```

. Section Headers

```
readelf -S hello/hello
There are 23 section headers, starting at offset 0x1c8:
```

```
Section Headers:
 [Nr] Name Type Address Offset Size EntSize Flags Link Info
Align
 [ 0] NULL 0000000000000000 00000000 0000000000000000
0000000000000000 0 0 0
…
 [ 6] .gosymtab PROGBITS 00000000004deae8 000deae8
0000000000000000 0000000000000000 A 0 0 1
 [ 7] .gopclntab PROGBITS 00000000004deb00 000deb00
000000000005324b 0000000000000000 A 0 0 32
…
```

• DWARF

- Debugging Data format
- uses a "data structure" to represent each variable, type, procedure

```
hello.c:
       1: int main()
       2: {
       3:   printf("Hello World!\n");
       4:   return 0;
       5: }
```

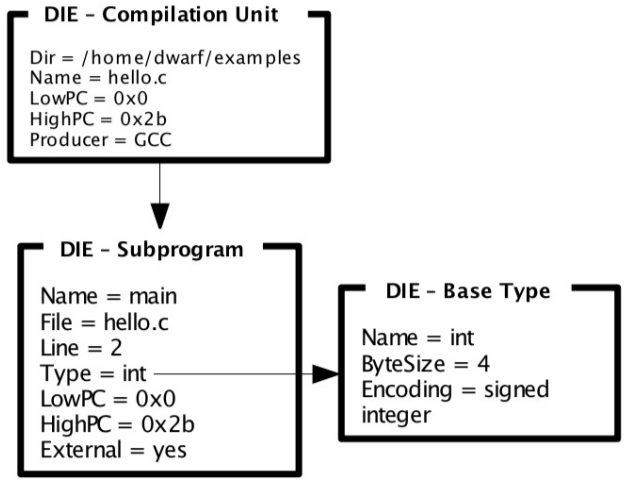


Figure 1. Graphical representation of DWARF data